Chosen-Ciphertext Secure Dual-Receiver Encryption in the Standard Model Based on Post-Quantum Assumptions

Laurin Benz^{2,3}, Wasilij Beskorovajnov¹, Sarai Eilebrecht¹, Roland Gröll¹ Maximilian Müller¹, and Jörn Müller-Quade^{2,3}

- ¹ FZI Forschungzentrum Informatik, Karlsruhe, Germany {beskorovajnov,eilebrecht,m.mueller,groell}@fzi.de
- ² Karlsruhe Institute of Technology, Karlsruhe, Germany
- ³ KASTEL Security Research Labs, Karlsruhe, Germany {laurin.benz,joern.mueller-quade}@kit.edu

Abstract. Dual-receiver encryption (DRE) is a special form of public key encryption (PKE) that allows a sender to encrypt a message for two recipients. Without further properties, the difference between DRE and PKE is only syntactical. One such important property is soundness, which requires that no ciphertext can be constructed such that the recipients decrypt to different plaintexts. Many applications rely on this property in order to realize more complex protocols or primitives. In addition, many of these applications explicitly avoid the usage of the random oracle, which poses an additional requirement on a DRE construction. We show that all of the IND-CCA2 secure standard model DRE constructions based on post-quantum assumptions fall short of augmenting the constructions with soundness and describe attacks thereon.

We then give an overview over all applications of IND-CCA2 secure DRE, group them into generic (i.e., applications using DRE as black-box) and non-generic applications and demonstrate that all generic ones require either soundness or public verifiability.

Conclusively, we identify the gap of sound and IND-CCA2 secure DRE constructions based on post-quantum assumptions in the standard model. In order to fill this gap we provide two IND-CCA2 secure DRE constructions based on the standard post-quantum assumptions, Normal Form Learning With Errors (NLWE) and Learning Parity with Noise (LPN).

Keywords: Dual-receiver encryption (DRE) \cdot Soundness \cdot Hybrid Encryption \cdot NLWE \cdot LPN \cdot Post-Quantum \cdot IND-CCA2 \cdot Standard Model

1 Introduction

Dual-receiver encryption (DRE) may be seen as a special case of Broadcast encryption (BE), where the number of recipients is constrained to two. Chow, Franklin, and Zhang [18] and Diament et al. [22] showed that DRE has plenty of applications, which impose different requirements on the used scheme. For some

applications the chosen plaintext attack (CPA) security is sufficient, whereas others require the stronger adaptive chosen ciphertext attack (CCA2) security. Furthermore, some applications require very specific DRE constructions using for example bilinear pairings. In this work we call such applications non-generic, as they make calls on internals routines of the employed DRE construction, preventing the use of DRE in a black-box manner within these applications.

Nevertheless, plenty of applications use DRE in a black-box manner and require only the property of soundness, for example [4, 8, 18, 20, 23, 44, 48]. This property requires that no adversary, even with knowledge of the secret keys of both recipients, is able to create a ciphertext that decrypts to two different plaintexts when decrypting with the secret keys of the recipients. Note that many of these applications are explicitly avoiding the use of the random oracle, which carries over to the employed DRE construction.

All standard model CCA2 secure DRE constructions based on post-quantum (PQ) assumptions [37, 54] are lattice-based and, as we show in this work, surprisingly fail at providing the soundness property. Moreover, Brendel et al. [14] mentions that amongst others, a CCA2 secure and sound PQ-instantiation did not yet appear in the literature. Thus, the aim of this work is to provide such DRE constructions, and therefore close this gap.

Contribution and Outline. Firstly, we conduct a literature review on—to the best of our knowledge—all applications requiring a sound CCA2 secure DRE in order to categorize them into generic and non-generic. Each application is explained shortly in Section 3.

- We identify the following generic applications requiring soundness: applications of CCA2 secure binding encryption [44], plaintext awareness via key registration [32], protocols for deniable authentication (DA) [23, 48], non-malleable commitments [19], and PKE schemes with non-interactive opening (PKENO) [20].
- The remaining applications are identified as non-generic: combined encryption schemes [22], protocols for secure group key management [12], tripartite key exchange [47], and schemes of dual receiver proxy re-encryption [9, 40].

Secondly, we conduct another literature review on—to the best of our knowledge—all constructions of CCA2 secure DRE in the standard model that may be used in a post-quantum setting and whether these constructions satisfy the soundness property. We present and explain our results in depth in Section 4. Our observation is that right now all of IND-CCA2 secure constructions are based on lattices and lack the soundness property.

Finally, in Section 5, we give efficient lattice- and LPN-based constructions in the standard model for IND-CCA2 secure and sound DRE schemes based on the hybrid encryption construction by Boyen, Izabachène, and Li [11] and the PKE construction by Kiltz, Masny, and Pietrzak [35], which can be used in any of the generic applications.

Moreover, we would like to point out that the employed trapdoor function in our lattice-based construction is from Micciancio and Peikert [42] and its ring and module variant was already implemented by Bert et al. [6, 7]. We therefore expect that our constructions are readily usable in prototypical implementations of generic applications from Section 3.

2 Preliminaries

Notations: For a positive integer k, [k] denotes the set $\{1, 2, \ldots, k\}$. We define the set of integers modulo q > 1 by \mathbb{Z}_q and the modular operation $(x \mod q)$ as mapping the integer x into [-q/2, q/2). Column-vectors are written as **bold** lower-case letters (e.g., v) and row-vectors are transposed column-vectors (e.g., \mathbf{v}^{\top}). The standard scalar product of the vectors \mathbf{x} and \mathbf{y} of the same dimension is denoted by $\langle \mathbf{x}, \mathbf{y} \rangle$. We denote matrices by **bold** upper-case letters (e.g., \mathbf{A}). The concatenation of two vectors \mathbf{v}_1 , \mathbf{v}_2 is denoted by $(\mathbf{v}_1, \mathbf{v}_2)$. By $\mathbf{v}[i]$ we refer to the *i*-th element of a vector \mathbf{v} and \mathbf{a}_i is the *i*-th column vector of a matrix **A.** The Euclidean norm of a vector \mathbf{v} is written as $\|\mathbf{v}\|$, its Hamming weight is denoted by $\|\mathbf{v}\|_{w}$, and |x| is the absolute value of a scalar x. Let S be an arbitrary set. By $s \leftarrow S$, we define the uniformly sampling of an element from S. If χ is a probability distribution, $x \leftarrow \chi$ denotes sampling an element according to the distribution. For a probabilistic algorithm R we denote by $y \leftarrow R(\mathbf{x})$ the result of one execution of R with input x. If an algorithm A has access to an oracle O, we write $\mathcal{A}^{\mathcal{O}}$. Our security parameter will always be called λ . We call a function $negl: \mathbb{N} \to \mathbb{R}$ negligible in λ , if for each positive integer k there exists an integer k_0 such that for all $\lambda > k_0 : |\text{negl}(\lambda)| < \lambda^{-k}$.

2.1 Definitions

We adapt the definition of DRE from Chow, Franklin, and Zhang [18] to a broader setting without the use of a common reference string (CRS). In many applications of DRE, the sender does not encrypt a message to two independent recipients. Instead, the sender interprets themselves as one of the recipients and encrypts the message under their own public key, too. Thus, we refer to the two receiving parties as receiver R and sender S with key pairs (sk^R, pk^R) and (sk^S, pk^S) , respectively.

Definition 1 (DRE). A public-key dual-receiver encryption scheme DRE = (gen, enc, dec) consists of the following algorithms:

- gen(1 $^{\lambda}$): The randomized *key generation* algorithm takes as input a unary encoding of the security parameter λ and outputs a public/secret key pair (pk, sk). We write (sk^R, pk^R) and (sk^S, pk^S) for the key pairs of two independent users.
- $enc(pk^R, pk^S, \mathbf{m})$: The randomized *encryption algorithm* takes as input two public keys pk^R and pk^S and a message \mathbf{m} , and outputs a ciphertext \mathbf{c} .
- $\operatorname{dec}(sk^i, pk^R, pk^S, \mathbf{c})$: The deterministic decryption algorithm takes one of the secret keys $sk^i (i \in \{R, S\})$, two public keys pk^R , pk^S , and a ciphertext \mathbf{c} as input, and outputs a message \mathbf{m}^i (which may be the special symbol \perp); we write $\mathbf{m}^i = \operatorname{dec}(sk^i, pk^R, pk^S, \mathbf{c})$.

4 L. Benz et al.

The usual IND-CCA2 security is somewhat different for a DRE scheme defined in Definition 2. However, when a DRE scheme already satisfies the soundness property from Definition 3 then the definition of IND-CCA2_{DRE} collapses to the standard definition of IND-CCA2.

Definition 2 (IND-CCA2_{DRE}). A DRE scheme is said to be indistinguishable under adaptive chosen ciphertext attack (IND-CCA2_{DRE} secure), if any probabilistic polynomial time (PPT) algorithm \mathcal{A} wins the IND-CCA2_{DRE} game in Figure 1 with probability at most $\frac{1}{2} + \mathtt{negl}(\lambda)$, i.e.,

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

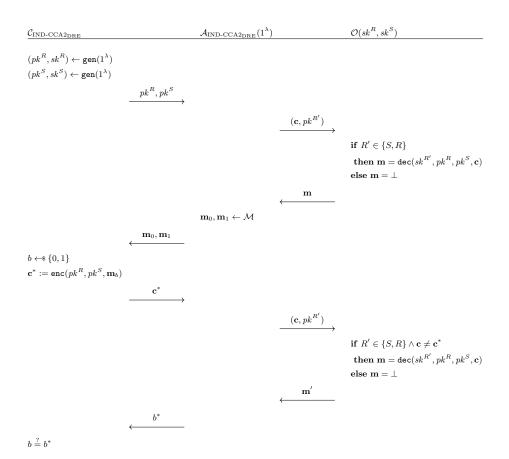


Fig. 1. Depiction of the IND-CCA2_{DRE} game.

The most important property of a DRE scheme is that of soundness, which states that every ciphertext will be decrypted to the same message from both

parties, even if it was maliciously made. Without this property every PKE scheme can also be used as a DRE scheme, simply by encrypting the message for both parties independently.

Definition 3 (Soundness for DRE [18]). Consider the experiment $\mathsf{Exp}^{\mathsf{sound}}_{\mathcal{E},\mathcal{A}}$ from Figure 2 for a DRE scheme \mathcal{E} and a PPT algorithm \mathcal{A} . A DRE scheme \mathcal{E} satisfies soundness if for any \mathcal{A} we have that $\mathsf{Adv}^{\mathsf{sound}}_{\mathcal{E},\mathcal{A}}$ is negligible in λ , i.e.,

$$\mathsf{Adv}^{\mathrm{sound}}_{\mathcal{E},\mathcal{A}}(\lambda) := \mathbb{P}\left[\mathsf{Exp}^{\mathrm{sound}}_{\mathcal{E},\mathcal{A}}(\lambda) = 1\right] \leq \mathtt{negl}(\lambda)\,.$$

Fig. 2. Depiction of the soundness game.

We will be constructing DRE schemes with the help of the hybrid encryption paradigm. For our constructions we require the following symmetric primitives and the according security definitions.

Definition 4 (SKE). A secret-key encryption (SKE) scheme is a pair of algorithms SKE = (SKE.enc, SKE.dec) with key space \mathcal{K}_{ske} and ciphertext space \mathcal{C}_{ske} with:

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

We require that for all $dk \in \mathcal{K}_{ske}$ it holds that

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

Definition 5 (OT-IND). A SKE scheme SKE is said to be one-time indistinguishable (OT-IND secure), if any PPT algorithm \mathcal{A} wins the OT-IND game in Figure 3 with probability at most $\frac{1}{2} + \mathtt{negl}(\lambda)$, i.e.,

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

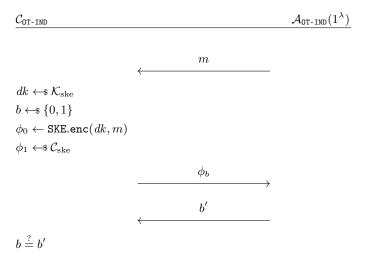


Fig. 3. Depiction of the OT-IND game.

A hash function is a function $\mathbb{H}: \{0,1\}^* \to \{0,1\}^\ell$ mapping bit strings of any length to bit strings of a fixed length ℓ .

Definition 6 (Collision Resistance). A family of hash functions $\{H_k\}_{k\in K}$ is said to be collision resistant (CR) if for all PPT algorithms \mathcal{A} the advantage $\mathsf{Adv}^{\mathrm{CR}}_{H,\mathcal{A}}(\lambda)$ is negligibly small, where

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

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.

Definition 7 (MAC). A message authentication code (MAC) scheme MAC with key space \mathcal{K}_{mac} consists of the two algorithms MAC = (MAC.sign, MAC.ver), where

- MAC.sign(mk, m): The randomized signing algorithm takes as input a signing key $mk \in \mathcal{K}_{mac}$ and a message m, and outputs a tag σ .
- MAC.ver (mk, \mathbf{m}, σ) : The deterministic verification algorithm takes as input a signing key $mk \in \mathcal{K}_{ske}$, a message \mathbf{m} and a tag σ , and outputs 1 if $\sigma \leftarrow \text{MAC.sign}(mk, \mathbf{m})$ and 0 otherwise.

Definition 8 (OT-SUF). A message authentication code scheme MAC is said to be one-time strongly unforgeable (OT-SUF secure) if any PPT algorithm \mathcal{A} wins the OT-SUF game in Figure 4 with at most negligible probability, i. e.,

$$\mathsf{Adv}^{\mathrm{OT\text{-}SUF}}_{\mathtt{MAC},\mathcal{A}}(\lambda) := \mathbb{P}\left[\mathsf{Exp}^{\mathrm{OT\text{-}SUF}}_{\mathtt{MAC},\mathcal{A}}(\lambda) = 1\right] \leq \mathtt{negl}(\lambda)\,.$$

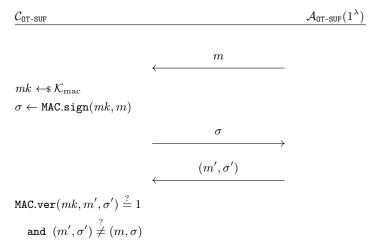


Fig. 4. Depiction of the OT-SUF game.

We use a key derivation function KDF: $\mathcal{K} \to \{0,1\}^n$ with key-space \mathcal{K} in order to generate the SKE- and MAC-keys from a short seed. We require for a KDF function to be IND secure according to Definition 9.

Definition 9 (IND KDF [11]). A key derivation function KDF is said to be IND secure if for all PPT algorithms \mathcal{A} the advantage $\mathsf{Adv}^{\mathsf{IND}}_{\mathsf{KDF},\mathcal{A}}(\lambda)$ is negligibly small, where

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

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

2.2 Assumptions and Lemmas

The following assumptions and lemmas are required in our proofs.

Definition 10 (NLWE Problem [11]). Let $n = n(\lambda), m = m(\lambda), q = q(\lambda)$ be integers and χ be an error distribution. The advantage of a PPT adversary \mathcal{A} for the (normal-form) $\mathsf{NLWE}_{n,m,q,\chi}$ problem, denoted by $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{NLWE}_{n,m,q,\chi}}(\lambda)$, is defined as

$$\mathsf{Adv}^{\mathsf{NLWE}_{n,m,q,\chi}}_{\mathcal{A}}(\lambda) \coloneqq \big| \mathbb{P}\left[\mathcal{A}(\mathbf{A}, \mathbf{s}^{\top}\mathbf{A} + \mathbf{e}^{\top}) = 1\right] - \mathbb{P}\left[\mathcal{A}(\mathbf{A}, \mathbf{b}^{\top}) = 1\right] \big|,$$

where $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, $\mathbf{s} \leftarrow \chi^n$ and $\mathbf{e} \leftarrow \chi^m$. The $\mathsf{NLWE}_{n,m,q,\chi}$ problem is hard if $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{NLWE}_{n,m,q,\chi}}$ is negligible in λ for all PPT adversaries \mathcal{A}

Applebaum et al. [3, Lemma 2] proved that NLWE is equivalent to the standard form of LWE where the LWE secret **s** is sampled from \mathbb{Z}_q^n instead of χ^n .

Let Ber_p denote the Bernoulli distribution with parameter p, so $x \leftarrow \operatorname{Ber}_p$ is the random variable over $\{0,1\}$ with $\mathbb{P}[x=1]=p$.

Definition 11 (LPN Problem [35]). Let $n = n(\lambda), m = m(\lambda) \ge n$ as well as $0 \le p = p(\lambda) \le \frac{1}{2}$ be the Bernoulli parameter. The advantage of a PPT adversary \mathcal{A} for the LPN_{n,m,p} problem, denoted by $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{LPN}_{n,m,p}}(\lambda)$, is defined as

$$\mathsf{Adv}^{\mathsf{LPN}_{n,m,p}}_{\mathcal{A}}(\lambda) \coloneqq \big| \mathbb{P} \left[\mathcal{A}(\mathbf{A}, \mathbf{s}^{\top} \mathbf{A} + \mathbf{e}^{\top}) = 1 \right] - \mathbb{P} \left[\mathcal{A}(\mathbf{A}, \mathbf{b}^{\top}) = 1 \right] \big|,$$

where $\mathbf{A} \leftarrow \mathbb{Z}_2^{n \times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_2^n$ and $\mathbf{e} \leftarrow \mathrm{Ber}_p^m$. The $\mathsf{LPN}_{n,m,p}$ problem is hard if $\mathsf{Adv}_{\mathsf{A}}^{\mathsf{LPN}_{n,m,p}}$ is negligible in λ for all PPT adversaries \mathcal{A} .

The LPN assumption is equivalent to the hardness of decoding a random linear code, and it is believed to be post-quantum secure just like LWE. We also need two extended dual version of the LPN assumption, called Knapsack Learning Parity with Noise (KLPN) and Extended Knapsack Learning Parity with Noise (EKLPN).

Definition 12 (KLPN Problem [35]). Let $n = n(\lambda), m = m(\lambda) \ge 2n$ and $0 \le p = p(\lambda) \le \frac{1}{2}$ be the Bernoulli parameter. The advantage of a PPT adversary \mathcal{A} for the KLPN_{n,m,p} problem, denoted by $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{KLPN}_{n,m,p}}(\lambda)$, is defined as

$$\mathsf{Adv}^{\mathsf{KLPN}_{n,m,p}}_{\mathcal{A}}(\lambda) \coloneqq |\mathbb{P}\left[\mathcal{A}(\mathbf{A},\mathbf{AE}) = 1\right] - \mathbb{P}\left[\mathcal{A}(\mathbf{A},\mathbf{B}) = 1\right]|,$$

where $\mathbf{A}, \mathbf{B} \leftarrow \mathbb{Z}_2^{n \times m}$ and $\mathbf{E} \leftarrow \mathrm{Ber}_p^{m \times m}$.

Definition 13 (EKLPN Problem [35]). Let $n=n(\lambda), m=m(\lambda) \geq 2n$ and $0 \leq p=p(\lambda) \leq \frac{1}{2}$ be the Bernoulli parameter. The advantage of a PPT adversary \mathcal{A} for the $\mathsf{EKLPN}_{n,m,p}$ problem, denoted by $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{EKLPN}_{n,m,p}}(\lambda)$, is defined as

$$\mathsf{Adv}^{\mathsf{EKLPN}_{n,m,p}}_{\mathcal{A}}(\lambda) \coloneqq \big| \mathbb{P} \left[\mathcal{A}(\mathbf{A}, \mathbf{AE}, \mathbf{z}, \mathbf{z}^{\top}\mathbf{E}) = 1 \right] - \mathbb{P} \left[\mathcal{A}(\mathbf{A}, \mathbf{B}, \mathbf{z}, \mathbf{z}^{\top}\mathbf{E}) = 1 \right] \big|,$$

where $\mathbf{A}, \mathbf{B} \leftarrow \mathbb{Z}_2^{n \times m}, \mathbf{E} \leftarrow \mathrm{Ber}_p^{m \times m}$ and $\mathbf{z} \leftarrow \mathrm{Ber}_p^m$.

There is a reduction from EKLPN and KLPN to LPN by Kiltz, Masny, and Pietrzak [35] that states:

Lemma 1 ([35]). For all algorithms \mathcal{B} and \mathcal{B}' there exist algorithms \mathcal{A} and \mathcal{A}' that run in roughly the same time as \mathcal{B} , respectively \mathcal{B}' , and $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{LPN}_{m-n,m,p}} \geq \frac{1}{m}\mathsf{Adv}_{\mathcal{B}}^{\mathsf{KLPN}_{n,m,p}}$ as well as $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{LPN}_{m-n,m,p}} \geq \frac{1}{2m}\mathsf{Adv}_{\mathcal{B}}^{\mathsf{EKLPN}_{n,m,p}}$.

We also need efficient codes, which exist by the following lemma.

Lemma 2 ([34]). For any rate 0 < R < 1, there exists a binary linear error-correcting code family which is polynomial time constructible, encodable and decodable and can decode up to $\lfloor \frac{\delta n}{2} \rfloor$ errors where $\delta \approx \frac{1}{2}(1-R)$.

To carry out attacks against the soundness property of DRE schemes from the literature (Section 4), we need to construct a carefully chosen malicious LWE secret, called \mathbf{s}_2 in the following lemma.

Lemma 3. For all $\mathbf{d} \in \mathbb{Z}_q^n \setminus \{0\}$ and $\mathbf{s}_1 \in \mathbb{Z}_q^n$ there exists $\mathbf{s}_2 \in \mathbb{Z}_q^n$ such that

$$\langle \mathbf{d}, \mathbf{s}_1 - \mathbf{s}_2 \rangle \notin \left[-\frac{q}{4}, \frac{q}{4} \right).$$

Moreover, this \mathbf{s}_2 can be found efficiently.

Proof. Choose an index i such that $\mathbf{d}[i] \neq 0$. If there exists $x \in \mathbb{Z}_q$ such that $\mathbf{d}[i] \cdot x$ mod $q \notin [-\frac{q}{4}, \frac{q}{4})$ we can set $\mathbf{s}_2[i] = \mathbf{s}_1[i] - x$ and $\mathbf{s}_2[j] = \mathbf{s}_1[j]$ for all $j \in [n] \setminus \{i\}$. It then follows that $\langle \mathbf{d}, \mathbf{s}_1 - \mathbf{s}_2 \rangle = \mathbf{d}[i] \cdot x \notin [-\frac{q}{4}, \frac{q}{4})$, proving the lemma. To see that such an x exists let $m \in \mathbb{N}_0$ be minimal such that $\mathbf{d}[i] \cdot 2^m \notin [-\frac{q}{4}, \frac{q}{4})$. As m is minimal we know that $\mathbf{d}[i] \cdot 2^{\max(0, m-1)} \in [-\frac{q}{4}, \frac{q}{4})$, and thus $\mathbf{d}[i] \cdot 2^m \in [-\frac{q}{2}, \frac{q}{2})$. Therefore, $\mathbf{d}[i] \cdot 2^m$ is not affected by the modulus and $x = 2^m$ satisfies the constraint.

This x can be found in $\log q$ steps.

3 Applications of Dual-Receiver Encryption

In the following, we describe—to the best of our knowledge—all applications that are reportedly realized with a CCA2 secure DRE scheme.

This section is structured as follows: Firstly, we describe all applications that generically require a sound DRE scheme. Then we briefly describe, for the sake of completeness, two remaining generic applications where a CCA2 secure and sound DRE construction is either unnecessarily strong or requires a reformulation and an additional proof in the CRS model. Finally, we describe the remaining non-generic applications.

3.1 Applications of CCA2 secure DRE with Soundness

Applications of Binding Encryption. Binding Encryption schemes are a special case of Broadcast Encryption [28], where the property of strong or weak decryption consistency is guaranteed. DRE in turn is a special case of a binding encryption scheme with only two recipients. The definitions of (partial) soundness and (weak) strong decryption consistency are syntactically equivalent when constrained to the special case of two recipients. Conclusively, one may therefore use a binding encryption scheme constrained to two recipients with a suitable level of decryption consistency in any DRE scenario. This means that the most efficient construction of binding encryption by Noh et al. [44] is basically an IND-CPA DRE scheme with soundness as it guarantees strong decryption consistency.

In some cases, a DRE scheme can also be extended to a binding encryption scheme. Consider the case that a sound DRE scheme is scalable for up to n receivers, which is the case with our constructions in Section 5. Then the DRE scheme becomes a binding encryption scheme and can therefore be used for all of its applications. These observations are somewhat simple but surprisingly have not yet been mentioned in the literature.

Plaintext Awareness via Key Registration (PAvKR). One variant of plaintext-awareness is plaintext-awareness via key registration introduced by Herzog, Liskov, and Micali [32]. In this notion, both sender and receiver need a public/private-key pair. These key pairs are registered via a key registration authority that ensures that the owner of a public key has knowledge of the private key. DRE is a natural way to utilize such an authority to achieve PA.

PAvKR can be used to enforce the Dolev-Yao model [24]. It is a formal proof model in which automated theorem provers like TAMARIN [41] can be used.

Deniable Authenticated Key Exchange. DRE is used in [23, 48] to implement a special case of deniable authentication (DA) introduced by Dwork, Naor, and Sahai [26] called on-line deniability, which captures the fact that deniability should also apply when one of the parties cooperates with a third party during the protocol. Dodis et al. [23] proposed an asymmetric key exchange protocol for symmetric keys called key exchange with incriminating abort (KEIA), which is a weak form of a deniable key exchange protocol. Roughly said, KEIA enables deniability if the key exchange protocol is terminated successfully. Once a shared key is established, deniability is guaranteed, even if corruptions occur later on. An IND-CCA2 secure and sound DRE scheme is used together with non-committing encryption by Canetti et al. [16] to realize a key exchange with incriminating abort functionality \mathcal{F}_{keia} in the generalized universal composability (GUC) framework by Canetti et al. [15]. The soundness property is mandatory, as it allows to simulate specific actions with either S's or R's secret key.

PKE with Non-Interactive Opening. The notion of public-key encryption with non-interactive opening (PKENO) by Damgård et al. [20] allows a receiver of a message to publicly open, when the encryption is interpreted as a commitment scheme, a received ciphertext to its plaintext without the necessity to interact with the sender. As stated by Chow, Franklin, and Zhang [18], a DRE trivially implies a one-time PKENO: The encrypting party takes the public keys of both receivers and sends $c = \operatorname{enc}(pk^R, pk^T, \mathbf{m})$ to both receivers. One of the two receivers can then prove the validity of the ciphertext c by revealing \mathbf{m} and its secret key.

3.2 Applications of DRE with Public Verifiability

Some applications require the property of public verifiability for ciphertexts of a DRE scheme, which is another property of DRE beside soundness. This property requires the existence of a public algorithm verifying the validity of a given DRE ciphertext.

Threshold Decryption. Chow, Franklin, and Zhang [18] describe that a publicly verifiable DRE scheme can be augmented with a secret sharing protocol that distributes one of the receiver's secret key among n parties in order to enable the threshold decryption scenario with a distributed so-called supervision party. We are not aware of any literature that explores these kinds of constructions any further.

Public-Key Encryption with Plaintext Equality Test (PET). Chow, Franklin, and Zhang [18] note that each publicly verifiable DRE enables the notion of PET introduced by Yang et al. [53]. This allows one to check if any two independent ciphertexts encrypt the same message by providing an additional public test functionality. However, to the best of our knowledge, all the established DRE constructions that are used in PET realizations so far are based on bilinear pairings.

3.3 Applications of CPA secure DRE and the CRS Model

There are two generic applications that differ substantially from the others in regard to their requirements on the DRE or the model they are proven secure within.

Completely Non-Malleable DRE. Due to the impossibility results of the existence of a non-interactive completely non-malleable PKE that can be proven secure with a black-box simulation in the standard model from Fischlin [29]. Chow, Franklin, and Zhang [18] propose two constructions of a completely non-malleable DRE (CNM-DRE) scheme in the CRS model. This property requires that any adversary obtaining a ciphertext \mathbf{c} without knowing the corresponding plaintext \mathbf{m} is not able to create a ciphertext \mathbf{c}^* and a (new) key pair such that the message \mathbf{m}^* encrypted in \mathbf{c}^* under this key pair is related to \mathbf{m} in some way.

CNM-DRE schemes can be utilized to construct dual-receiver non-malleable commitments (DR-NMC). These are generalizations of normal commitment schemes introduced by Crescenzo, Ishai, and Ostrovsky [19] and enable the possibility of committing to a message in a non-malleable sense for two independent receivers such that both receivers are able to open the commitment and know that the other party obtained the same de-committed message. We leave it open for future work to check our constructions in regard to this security definition.

Construction of Secure Channels. A new security notion, called sender-binding chosen plaintext attack (SB-CPA), for a variant of PKE, namely sender-binding encryption (SBE), was introduced by Beskorovajnov et al. [8]. The reasoning behind this notion is a definition of minimal security for the public-key part of the encryption when used in conjunction with authenticated channels in order to realize a universally composable secure channel. The authors show that an IND-CPA secure and sound DRE can be used to construct an SB-CPA secure SBE when a key registration with knowledge (KRK) is available. Benz et al. [5] showed that the results carry over to the hybrid encryption or the key exchange setting by utilizing a CPA secure dual-receiver key encapsulation mechanism (KEM). Our constructions from Section 5 can be easily simplified to provide this lower security than CCA2 without losing the soundness property. Moreover, we note that our constructions can be easily adapted to provide a CPA secure dual-receiver KEM with soundness because they are constructed with the help of the hybrid encryption paradigm.

3.4 Non-Generic Applications

In this section, we briefly introduce non-generic applications of DRE. We denote that the use of DRE in these applications may be generalizable by finding a property that correctly describes the application's requirements on a DRE construction. However, we are not aware of any such property in the literature and therefore argue that declaring these applications non-generic at this point in time is justified. Securely modifying the use of DRE in these applications in order to make them generic is out of scope and left as an open question. Finally, all the following applications are build upon bilinear pairings inside the employed DRE construction.

Useful Security Puzzles. Computational puzzles can be used to protect servers from resource-heavy client requests. That is, a client has to solve a computationally expensive task which is easily verifiable by the server. However, we call a puzzle not useful if for example its only purpose is to rate-limit a client. In the work of Diament et al. [22], there are two scenarios with useful security puzzles proposed. In the first scenario, a file server can utilize DRE to rate-limit clients requesting encrypted files by outsourcing a huge part of the decryption to the clients. In another scenario, security puzzles might be used for DDoS protection in a TLS-like protocol. Note that this work has been revised in [21].

Combined Encryption Schemes. DRE is utilized to construct combined encryption schemes in [18] and [21, 22]. In the latter two works, the scheme can be used for signing and encryption at the same time. Meanwhile the former construction offers the possibility to use a DRE and PKE scheme with the same keys.

Secure Group Key Management. The concept of secure group communication (SGC) allows a group of users to communicate such that only members of the group can decrypt messages. For this purpose, the group shares a secret called the group key. The most crucial problem is to solve the management of this group key. In SGC, new members can join, and existing members may leave the group. However, new members must not read old messages (backward secrecy), and ex-users are not allowed to decrypt messages after leaving the group (forward secrecy). Hence, the group key must be changed after each entry or exit. This process is called rekeying.

One possible way to manage group keys is to use *key graphs* [50]. BR and Amberker [12] use the DRE scheme of Diament et al. [22] to manage such a key graph and thus to enable SGC.

Tripartite Key Exchange. The protocols for authenticated key exchange (AKE) are used to share a key among multiple parties via unauthenticated channels. A special case is the three-party AKE (3KE). One of the special properties of a 3KE is called maximal-exposure-resilience (MEX-resilience). It roughly captures the fact that no information about the session key is exposed, even if an adversary is able to obtain any non-trivial combination of keys, that is, not all parties are completely corrupted.

Suzuki and Yoneyama [47] utilize a modified version of a DRE KEM construction from Chow, Franklin, and Zhang [18] to realize an *exposure-resilient* one-round 3KE in the standard model with the help of bilinear pairings. During the protocol, each party samples a random nonce and broadcasts it to the two other parties. Afterwards, each party aggregates the three plaintexts and derives a shared key via a pseudo-random key derivation function (KDF).

Dual-Receiver Proxy Re-Encryption (DR-PRE). The general notion of proxy re-encryption (PRE) from Blaze, Bleumer, and Strauss [9] and Mambo and Okamoto [40] allows one to transform a ciphertext that has been encrypted for one user into a ciphertext for a different party. In the case of dual-receiver proxy re-encryption (DR-PRE), a ciphertext encrypted for a single user, called the delegator, can be converted into a ciphertext so that it can be decrypted by two independent users, called the delegatees.

Originally, this task had to be done for each delegatee individually with different PREs and re-encryption keys. Patil and BR [45] however use DRE to accomplish this task with a dedicated DR-PRE construction. Both delegatees can decrypt the resulting ciphertext with their respective secret key. In this way computational and bandwidth costs can be saved.

4 Related Work on Post-Quantum DRE Constructions

In this section, we present all related works for post-quantum IND-CCA2_{DRE} secure DRE constructions in the standard model, that are [37, 54]. For both of these works, we show that they do not fulfill the soundness property.

We also consider constructions of broadcast encryption schemes as such constructions may be applied to the DRE setting and may have the property of strong decryption consistency that is equivalent to soundness, cf. the discussion from Section 3.1. Belonging to the list of broadcast encryption constructions that do not mention strong decryption consistency, there are six (identity-based) BE schemes [13, 30, 33, 39, 49, 52], one IND-CPA construction [10] and four generic constructions from Libert, Paterson, and Quaglia [36]. One exception is the binding encryption construction from Noh et al. [44], which explicitly proves the decryption consistency property. However, this construction is only IND-CPA secure.

For the sake of completeness, we also denote that there are four DRE schemes which are based on post-quantum assumptions satisfying the soundness property. However, they are only IND-CPA secure. The first is from a Master's Thesis by Gegier [31], which presents a generic construction of a DRE KEM from any deterministic PKE and trapdoor functions with hardcore functions. The second is from a Master's Thesis by Müller [43], which presents a lattice-based direct construction of a DRE PKE. The third and fourth are two McEliece-based constructions by Beskorovajnov et al. [8].

4.1 IND-CCA2 Secure DRE Schemes Without Soundness

There are two IND-CCA2_{DRE} secure DRE schemes in the standard model, one by Zhang et al. [54] and one by Liu et al. [37]. The constructions differ roughly only in the choice of hash functions. In this subsection, we will show that these schemes do not satisfy the soundness property due to the lack of structure checks. In order to explain the attack on the soundness of these schemes, we abstract the two schemes into one abstract template that covers both schemes:

- The parameters χ and χ' denote LWE error distributions.
- $OTS = (KGen_{OTS}, Sig_{OTS}, Vfy_{OTS})$ is a strongly unforgeable one-time signature scheme (see [54, Appendix B] for a definition).
- **H**^R, **H**^S are matrices generated by deterministic functions whose computation includes parts of the public key and a hash function depending on a verification key of OTS. These functions differ among both schemes, but are well-defined.
- The algorithm SampleLeft which occurs in line 4 of Figure 5 outputs on input (\mathbf{C}^R , \mathbf{d}_i , sk^R , s') a vector \mathbf{v}_i such that $\mathbf{C}^R\mathbf{v}_i = \mathbf{d}_i$. The vector \mathbf{d}_i is the *i*-th column vector of the matrix \mathbf{D} which is sampled uniformly random, part of the CRS of this scheme, and used as LWE-Matrix to disguise the message.

We omit the details of the key generation here. Roughly, a LWE-Matrix and a corresponding trapdoor is generated in it.

```
\frac{\mathsf{enc}(\mathbf{A}^R, \mathbf{A}^S, \mathbf{m} \in \{0,1\}^n)}{1: \quad \mathbf{s} \leftarrow \$ \, \mathbb{Z}_q^n, \mathbf{e}_{\mathrm{msg}} \leftarrow \chi^n, \mathbf{e}^R, \mathbf{e}^S \leftarrow {\chi'}^{2m}} \qquad \frac{\mathsf{dec}(sk^R, \mathbf{A}^R, \mathbf{A}^S, \mathbf{c})}{1: \quad \text{if } \mathsf{Vfy}_{\mathrm{OTS}}(vk, (\mathbf{c}^R, \mathbf{c}^S, c_{\mathrm{msg}}), \sigma) == \mathsf{false}}
  2: (vk, sk) \leftarrow \mathsf{KGen}_{\mathsf{OTS}}(1^{\lambda})
                                                                                                                                 3: for i \in [n]
  3: \mathbf{C}^R = [\mathbf{A}^R | \mathbf{H}^R]
                                                                                                                                 4: \mathbf{v}_i \leftarrow \mathtt{SampleLeft}(\mathbf{A}^R, \mathbf{H}^R, \mathbf{d}_i, sk^R, s')
  4: \mathbf{C}^S = [\mathbf{A}^S | \mathbf{H}^S]
                                                                                                                                 5: \mathbf{V}^R = [\mathbf{v}_1 \dots \mathbf{v}_n]
 5: \mathbf{c}^R = (\mathbf{C}^R)^{\top} \mathbf{s} + \mathbf{e}^R \in \mathbb{Z}_q^{2m}
                                                                                                                                                    /\!\!/ It holds \mathbf{C}^R \mathbf{V}^R = \mathbf{D}
  6: \mathbf{c}^S = (\mathbf{C}^S)^{\mathsf{T}} \mathbf{s} + \mathbf{e}^S \in \mathbb{Z}_q^{2m}
                                                                                                                                 6: \mathbf{m}' = \mathbf{c}_{\text{msg}} - (\mathbf{V}^R)^{\top} \mathbf{c}^R \stackrel{!}{\approx} [q/2] \mathbf{m}
  7: \mathbf{c}_{\text{msg}} = \mathbf{D}^{\top} \mathbf{s} + \mathbf{e}_{\text{msg}} + \lceil q/2 \rceil \mathbf{m} \in \mathbb{Z}_q^n
                                                                                                                                 7: \mathbf{m} \leftarrow \text{Round each element of } \mathbf{m}'
  8: \sigma \leftarrow \mathsf{Sig}_{\mathsf{OTS}}(\mathit{sk}, (\mathbf{c}^R, \mathbf{c}^S, \mathbf{c}_{\mathsf{msg}}))
                                                                                                                                  8: return m
  9: return \mathbf{c} = (\mathbf{c}^R, \mathbf{c}^S, \mathbf{c}_{\text{msg}}, \sigma)
```

Fig. 5. An abstract template of [37, 54].

Let us construct an adversary \mathcal{A} which breaks the soundness property with probability 1. It creates a ciphertext \mathbf{c} such that R decrypts 0 as the first bit of the message, whereas S obtains 1.

First, \mathcal{A} obtains the public keys \mathbf{A}^R and \mathbf{A}^S (the secret keys are not needed for this attack). \mathcal{A} runs $(vk, sk) \leftarrow \mathsf{KGen}_{OTS}$ and creates the LWE-matrices $\mathbf{C}^i = \lceil \mathbf{A}^i | \mathbf{H}^i \rceil$ for $i \in \{R, S\}$ where \mathbf{H}_i are deterministic evaluations of some

hash functions and other public information. Recall that \mathbf{d}_1 is the first column vector of \mathbf{D} . Sample $\mathbf{s}^R \leftarrow \mathbb{Z}_q^n$ and use Lemma 3 to choose $\mathbf{s}^S \in \mathbb{Z}_q^n$ such that $\langle \mathbf{d}_1, \mathbf{s}^R - \mathbf{s}^S \rangle \notin [-\frac{q}{4}, \frac{q}{4})$. The vector d_1 is not equal to zero with overwhelming probability since it was sampled from \mathbb{Z}_q^n uniformly at random. Now, \mathcal{A} can construct a malicious ciphertext part \mathbf{c}' as follows:

$$\mathbf{c}' = \begin{pmatrix} \mathbf{c}^R \\ \mathbf{c}^S \\ \mathbf{c}^{\mathrm{msg}} \end{pmatrix} = \begin{bmatrix} \left(\mathbf{C}^R \right)^\top \cdot \mathbf{s}^R \\ \left(\mathbf{C}^S \right)^\top \cdot \mathbf{s}^S \\ \mathbf{D}^\top \cdot \mathbf{s}^R \end{bmatrix} \in \mathbb{Z}_q^{2m+n}.$$

Note that we implicitly choose \mathbf{e}^R , $\mathbf{e}^S = \mathbf{0}^m$ and $\mathbf{e}^{\mathrm{msg}}$, $\mathbf{m} = 0^n$. To finish the encryption, \mathcal{A} runs $\sigma \leftarrow \mathsf{Sig}_{\mathrm{OTS}}(sk,\mathbf{c}')$ and returns the ciphertext $\mathbf{c} = (vk,\mathbf{c}',\sigma)$. A sketch of this game is given in Figure 6.

Challenger C

Adversary A

Fig. 6. Soundness attack against the schemes of [37, 54].

Let us discuss the respective decryptions. Since R does not use the malformed ciphertext part \mathbf{c}^S in the decryption algorithm and the signature σ

is valid, R decrypts 0^n as its message and thus 0 as the first bit. Now consider the decryption algorithm in the view of S, restricted to the first bit of \mathbf{m} . First, the signature check is successful since A made an honest signature. Next, SampleLeft($\mathbf{A}^S, \mathbf{H}^S, \mathbf{d}_1, sk^S, s'$) returns \mathbf{v}_1 such that $\mathbf{C}^S \mathbf{v}_1 = \mathbf{d}_1$. According to line 6 of the decryption algorithm from Figure 5, S obtains $\mathbf{m}'[1] = \mathbf{c}^{\text{msg}}[1] - \mathbf{v}_1^{\mathsf{T}}\mathbf{c}^S = \langle \mathbf{d}_1, \mathbf{s}^R \rangle - \mathbf{v}_1^{\mathsf{T}}(\mathbf{C}^S)^{\mathsf{T}} \cdot \mathbf{s}^S = \langle \mathbf{d}_1, \mathbf{s}^R \rangle - \mathbf{d}_1^{\mathsf{T}}\mathbf{s}^S = \langle \mathbf{d}_1, \mathbf{s}^R - \mathbf{s}^S \rangle \notin [-\frac{q}{4}, \frac{q}{4})$ and hence decrypts 1 as first bit. Thus, R and S decrypt different messages from the same ciphertext which breaks the soundness property.

4.2 Identity-based DRE Schemes Without Soundness

We now discuss identity-based DRE (IB-DRE) schemes. In identity based encryption (IBE), public information, such as an email address, called *identity*, is used for encryption instead of traditional public keys. Decryption is still performed with the help of a secret key. Such a secret key is attained from a key generation algorithm that takes a *master secret key* and an identity as input.

There are three works constructing post-quantum secure identity-based DRE schemes in the literature [37, 38, 54]. Zhang et al. [54] propose a generic construction, which is instantiated in the more recent work of Liu et al. [37]. Here, an additional primitive called *lattice-based programmable hash functions* is used. Liu et al. [38] use an injective map and a homomorphic computation technique due to Yamada [51].

Due to the huge storage costs of public parameters, IB-DRE schemes are impracticable in their current state. For example, in the recent work from Liu et al. [38], 70 public key matrices are demanded, leading to storage cost of approximately 1.2GB for a choice of n=284 (as suggested by Micciancio and Peikert [42]). Besides the huge storage costs, none of the three IB-DRE schemes satisfies the soundness property. From a structural perspective, all of these schemes use the same ideas as the schemes from Section 4.1 for encryption, and the decryption algorithm does not contain any soundness tests as well. Hence, an adversary can inject different LWE-secrets $\bf s$ in the encryption.

For an attack against the schemes of Liu et al. [38], we refer to Section 4.1 since the attacks are very similar. The attack on the schemes of Liu et al. [37] is slightly more involved and is discussed in Appendix A.

5 IND-CCA2_{DRE} Secure and Sound Hybrid DRE

Section 3 and Section 4 show that there is a need for efficient, post-quantum and IND-CCA2_{DRE} secure and sound constructions of DRE schemes in the standard model. In the following we present two constructions that meet this need.

For both constructions we need a full-rank difference encoding FRD^4 as well as a hash function $H: \{0,1\}^* \to \mathbb{Z}_q^n \setminus \{0\}$, a secret-key encryption system SKE, a message authentication code MAC and a key derivation function KDF.

⁴ A FRD is a function FRD: $\mathbb{Z}_q^n \to \mathbb{Z}_q^{n \times n}$ such that for any $x, y \in \mathbb{Z}_q^n, x \neq y$ we have FRD(x) - FRD(y) is invertible over $\mathbb{Z}_q^{n \times n}$. See the work of Agrawal, Boneh, and Boyen [2] for an example of such functions.

5.1 NLWE-Based Construction

By adapting the NLWE-based hybrid construction from Boyen, Izabachène, and Li [11] we are able to straightforwardly construct an NLWE-based DRE construction with soundness. As usual, $\mathcal{D}_{\mathbb{Z},\alpha q}$ denotes the discrete Gaussian distribution.

In our description in Figure 7 we only show the decryption for R, the decryption for S works exactly the same with swapped party identifiers.

 $\frac{\mathrm{gen}(\boldsymbol{1}^{\lambda})}{\boldsymbol{1}: \quad \mathbf{A} \leftarrow \!\! \$ \, \mathbb{Z}_q^{n \times m}, \mathbf{R} \leftarrow \mathcal{D}_{\mathbb{Z}, \omega(\sqrt{\log n})}^{m \times \overline{m}}}$

```
2: \mathbf{A}_1 = \mathbf{A} \cdot \mathbf{R}
                                                                3: return (pk, sk) := ((\mathbf{A}, \mathbf{A}_1), \mathbf{R})
\mathtt{enc}(\mathit{pk}^R,\mathit{pk}^S,\mathbf{M})
                                                                                                                           \operatorname{dec}(sk^R,pk^R,pk^S,\mathbf{C})
 1: parse pk^R = (\mathbf{A}^R, \mathbf{A}_1^R)
                                                                                                                             1: parse pk^R = (\mathbf{A}^R, \mathbf{A}_1^R)
 2: parse pk^S = (\mathbf{A}^S, \mathbf{A}_1^S)
                                                                                                                             2: parse pk^S = (\mathbf{A}^S, \mathbf{A}_1^S)
 3: \mathbf{k} \leftarrow \$ \{0,1\}^n
                                                                                                                            3: parse sk^R = (\mathbf{R}^R)
 4: \quad (dk, mk) := \mathtt{KDF}(\mathbf{k})
                                                                                                                             4: parse \mathbf{C} = (\mathbf{c}_0^R, \mathbf{c}_0^S, \mathbf{c}_1^R, \mathbf{c}_1^S, \phi, \sigma)
  5: \overline{\mathbf{s}} \leftarrow \mathcal{D}^m_{\mathbb{Z},\alpha q}, \ \mathbf{s} := \mathbf{k} \cdot \lfloor \frac{q}{2} \rfloor + \overline{\mathbf{s}}
                                                                                                                            \mathbf{5}:\ (\mathbf{s},\mathbf{e}_0^R,\mathbf{e}_1^R) \leftarrow \mathtt{Invert}(\mathbf{R},
                                                                                                                                        \left[\mathbf{A}^R \mid \mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0^R))\mathbf{G}\right], (\mathbf{c}_0^R, \mathbf{c}_1^R))
  6: \mathbf{e}_0^R, \mathbf{e}_0^S \leftarrow \mathcal{D}_{\mathbb{Z}, \alpha q}^m
  7: \mathbf{c}_0 = (\mathbf{s}^{\top} \mathbf{A}^R + \mathbf{e}_0^R, \mathbf{s}^{\top} \mathbf{A}^S + \mathbf{e}_0^S)
                                                                                                                             6: if \|\mathbf{e}_0^R\| > \alpha q \sqrt{m} output \perp
  8: \mathbf{e}_{1}^{R}, \mathbf{e}_{1}^{S} \leftarrow \mathcal{D}_{\mathbb{Z},s}^{\overline{m}},
                                                                                                                             7: if \|\mathbf{e}_1^R\| > \alpha q \sqrt{2m\overline{m}} \cdot \omega(\sqrt{\log n}) output \perp
              where s^2 = (\|\mathbf{e}_0\|^2 + m(\alpha q)^2) \cdot \omega(\sqrt{\log n})
                                                                                                                             8: if \|(\mathbf{c}_0^S)^\top - \mathbf{s}^\top \mathbf{A}^S\| > \alpha q \sqrt{m} output \bot
  9: \mathbf{c}_1 = \left(\mathbf{s}^{\top}(\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + \mathbf{e}_1^R\right)
            \mathbf{s}^{\top}(\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + \mathbf{e}_1^S)
                                                                                                                             9: if \left\| \left( \mathbf{c}_1^S \right)^\top - \mathbf{s}^\top (\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) \right\| >
10: \phi := SKE.enc(dk, \mathbf{M})
                                                                                                                                        \alpha q \sqrt{2m\overline{m}} \cdot \omega(\sqrt{\log n})output\bot
11: \sigma := MAC.sign(mk, (\mathbf{c}_0, \mathbf{c}_1, \phi))
                                                                                                                           10: for i \in [m] do
12: return \mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1, \phi, \sigma)
                                                                                                                                            \mathbf{k}[i] = \begin{cases} 0, \ \mathbf{s}[i] \in [-\frac{q}{4}, \frac{q}{4}) \\ 1, \ \mathbf{s}[i] \notin [-\frac{q}{4}, \frac{q}{4}) \end{cases}
                                                                                                                           11: if \|\mathbf{s} - \mathbf{k}\| > \alpha q \sqrt{n} output \perp
                                                                                                                           12: (dk, mk) = KDF(\mathbf{k})
                                                                                                                           13: if 1 == MAC.Vfy(mk, (\mathbf{c}_0, \mathbf{c}_1, \phi), \sigma)
                                                                                                                           14: return \mathbf{M} = SKE.dec(dk, \phi)
                                                                                                                            15: else return \mathbf{M} = \bot
```

Fig. 7. Description of $\Sigma_{LWE-DRE} = (gen, enc, dec)$.

Theorem 1. The DRE $\Sigma_{LWE-DRE} = (\text{gen, enc, dec})$ is correct.

The correctness proof carries over from the correctness of [11] since our construction does not change anything intrinsic.

Theorem 2. The DRE $\Sigma_{LWE-DRE} = (gen, enc, dec)$ is sound as in Definition 3.

The basic idea is a statistical one: for a given matrix \mathbf{A} , the LWE tuple (\mathbf{s}, \mathbf{e}) in $\mathbf{s}^{\top} \mathbf{A} + \mathbf{e}$ is unique with overwhelming probability, see for example the work of Zhang et al. [55]. Therefore, even for maliciously created ciphertexts, both parties will recover the same \mathbf{s} .

Proof. Assume the scheme is not sound. Then there exists an adversary \mathcal{A} with non-negligible advantage $\mathsf{Adv}^{\mathsf{dre}\text{-}\mathsf{sound}}_{\mathcal{E},\mathcal{A}}$ as in Definition 3. Thus, given two public keys $pk^R = (\mathbf{A}^R, \mathbf{A}_1^R)$ and $pk^S = (\mathbf{A}^S, \mathbf{A}_1^S)$, the adversary \mathcal{A} returns with non-negligible advantage a valid ciphertext \mathbf{c} such that $\mathsf{dec}(sk^R, pk^S, pk^R, \mathbf{c}) \neq \mathsf{dec}(sk^S, pk^S, pk^R, \mathbf{c})$.

At least one party has to accept the ciphertext as otherwise both parties would return \bot . Thus, we can assume without loss of generality that R outputs a message and therefore all checks are valid. In particular, we have $\left\|\mathbf{c}_1^{S^\top} - (\mathbf{s}^R)^\top (\mathbf{A}_1^S + \text{FRD}(\mathbf{H}(\mathbf{c}_0))\mathbf{G})\right\| \le \alpha q \sqrt{2m\overline{m}} \cdot \omega(\sqrt{\log n})$, where \mathbf{s}^R is the vector that R recovered in step 5. This means that $\mathbf{c}_1^{S^\top} = (\mathbf{s}^R)^\top (\mathbf{A}_1^S + \text{FRD}(\mathbf{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}_1')^\top$ with $\|\mathbf{e}_1'\| \le \alpha q \sqrt{2m\overline{m}} \cdot \omega(\sqrt{\log n})$. Similarly, we have $\mathbf{c}_0^{S^\top} = (\mathbf{s}^R)^\top \mathbf{A}^S + (\mathbf{e}_0')^\top$ with $\|\mathbf{e}_0'\| \le \alpha q \sqrt{m}$.

By Micciancio and Peikert [42, Theorem 5.4] this means that S recovers \mathbf{s}^R as well, succeeds with all checks and thus both parties recover the same \mathbf{k} , as well as the same (dk, mk) because the KDF is deterministic.

Finally, as our decryption algorithm as well as our verification algorithm are deterministic, it follows that both parties recover the same M.

Theorem 3. The DRE $\Sigma_{\mathit{LWE-DRE}} = (\text{gen}, \text{enc}, \text{dec})$ is $\mathit{IND-CCA2_{DRE}}$ -secure as in Definition 2 if $\mathit{NLWE}_{n,m,q,D_{\mathbb{Z},\alpha q}}$ is hard, and $\mathit{SKE}, \mathit{MAC}, \mathit{H}, \mathit{KDF}$ are all secure w.r.t. Definitions 5, 6, 8 and 9.

To prove this we adapt the proof of Boyen, Izabachène, and Li [11, Theorem 1]. Thus, for a more in-depth discussion we refer interested reader to that paper. Starting with the IND-CCA2_{DRE} game, we slowly replace parts of our scheme until we arrive at a game where any adversary cannot do better than guessing because the supposedly encrypted message is in fact only a random ciphertext. Our assumptions make sure that no adversary can differentiate the games with more than negligible probability and so this proves that our construction is indeed secure.

Proof. We start by giving a small overview of the games. Game 1 to 3 change the decryption oracle to make it easier for us to adapt the public keys in Game 4. Those changes aim to make sure that the adversary does not query ciphertexts using the challenge "tag" $FRD(H(\mathbf{c}_0^*))$. This in turn allows us to replace the binding parts \mathbf{c}_0 and \mathbf{c}_1 of \mathbf{k} by randomness in Game 5 and 6. Now, Game 7 replaces this key \mathbf{k} by randomness as well, and finally in Game 8 we replace the message encryption ϕ by a random ciphertext.

As usual, we denote by $\mathbb{P}[S_i]$ the probability, that the adversary outputs 1 in Game *i*.

Game 0: This game follows the IND-CCA2-DRE game. Here, \mathcal{A} gets two independently generated public keys, makes decryption queries to the oracle which can be honestly answered using the secret keys. After that, A submits two messages M_0, M_1 of equal length, after which the challenge ciphertext is computed by $\mathbf{c}^* = \text{enc}(pk^R, pk^S, M_b)$ for $b \leftarrow \$\{0, 1\}$. The adversary \mathcal{A} can now make further queries provided that the used public key is from the set $\{R,S\}$ and $\mathbf{c} \neq \mathbf{c}^*$. Finally, \mathcal{A} outputs b' and the game returns 1 if b=b'. By definition, we have

$$\mathbb{P}\left[S_{0}\right] = \mathbb{P}\left[\mathsf{Exp}_{\mathrm{DRE},\mathcal{A}}^{\mathrm{IND\text{-}CCA2}_{\mathrm{DRE}}}(\lambda) = 1\right].$$

Game 1: We now precompute \mathbf{c}_0^* before sending the two generated public keys to A. More specifically, steps 3 to 7 of the encoding in Figure 7 are now done before sending the public keys to A. As the precomputed \mathbf{c}_0^* is already unavailable to A until \mathbf{c}^* is released and nothing else changed we get

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

Game 2: This is identical to Game 1 except for the decryption oracle, which now rejects ciphertexts with $H(\mathbf{c}_0) = H(\mathbf{c}_0^*)$ in the first phase as well as ciphertexts with $\mathbf{c}_0 \neq \mathbf{c}_0^*$ and $\mathtt{H}(\mathbf{c}_0) = \mathtt{H}(\mathbf{c}_0^*)$ in the second phase. Using [11, Lemma 4] we get (for Q_1 being the number of decryption queries in the first phase)⁵

$$|\mathbb{P}\left[S_{2}\right]-\mathbb{P}\left[S_{1}\right]|\leq\frac{Q_{1}}{q^{n}}+\mathsf{Adv}_{\mathtt{H},\mathcal{B}_{1}(\lambda)}^{\mathrm{CR}}.$$

- **Game 3:** We now additionally forbid all decryption queries with $\mathbf{c}_0 = \mathbf{c}_0^*$ after the challenge ciphertext has been released. We can bound the probability that \mathcal{A} submits a valid decryption query $\mathbf{c} = (\mathbf{c}_0^*, \mathbf{c}_1, \phi, \sigma) \neq \mathbf{c}^*$ by two sub-events: (1) NoBind: a different key $\mathbf{k} \neq \mathbf{k}^*$ is associated to \mathbf{c}_0^* .

 - (2) Forge: the key \mathbf{k}^* from \mathbf{c}^* was used for \mathbf{c} .

Our definition of \mathbf{c}_0 (step 7 of Figure 7) and the uniqueness of LWE samples⁶ proves that $\mathbb{P}[NoBind]$ is negligible, and thus

$$|\mathbb{P}[S_4] - \mathbb{P}[S_3]| \leq \mathbb{P}[\text{Forge}_3] + \text{negl}(\lambda).$$

Game 4: We adapt the generation of both public keys, calculating \mathbf{c}_0^* before setting $\mathbf{A}_1^R = \mathbf{A}^R \mathbf{R}^R - \text{FRD}(\mathbb{H}(\mathbf{c}_0^*))\mathbf{G})$ and $\mathbf{A}_1^S = \mathbf{A}^S \mathbf{R}^S - \text{FRD}(\mathbb{H}(\mathbf{c}_0^*))\mathbf{G})$. As \mathbf{A}^S and \mathbf{A}^R are both uniformly random, the distribution of the public keys in Game 3 and Game 4 are statistically close. Also, the decryption oracle can handle the same set of decryption queries as in Game 3. Indeed, given $\mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1, \phi, \sigma)$ we have

$$\begin{split} \mathbf{c}_1 &= \left(\mathbf{s}^\top (\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + \mathbf{e}_1^R, \mathbf{s}^\top (\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + \mathbf{e}_1^S\right) \\ &= \left(\mathbf{s}^\top (\mathbf{A}^R \mathbf{R}^R + (\mathtt{FRD}(\mathtt{H}(\mathbf{c}_0)) - \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0^*)))\mathbf{G}) + \mathbf{e}_1^R, \\ &\mathbf{s}^\top (\mathbf{A}^S \mathbf{R}^S + (\mathtt{FRD}(\mathtt{H}(\mathbf{c}_0)) - \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0^*)))\mathbf{G}) + \mathbf{e}_1^S\right). \end{split}$$

⁵ Notice that Q_2 in [11, Lemma 4] is not needed: The reduction algorithm \mathcal{B}_1 always wins if a collision occurs.

⁶ See for example [55, Lemma 6].

As for all $\mathtt{H}(\mathbf{c}_0) \neq \mathtt{H}(\mathbf{c}_0^*)$ the difference $\mathtt{FRD}(\mathtt{H}(\mathbf{c}_0)) - \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0^*))$ is invertible by the definition of FRD, the trapdoor \mathbf{R}^S or \mathbf{R}^R can be used to decrypt the queries. The case $\mathtt{H}(\mathbf{c}_0) = \mathtt{H}(\mathbf{c}_0^*)$ was already rejected in Game 3 and so we get

$$|\mathbb{P}[S_4] - \mathbb{P}[S_3]| \le \text{negl}(\lambda) \quad \text{and} \quad |\mathbb{P}[\text{Forge}_4] - \mathbb{P}[\text{Forge}_3]| \le \text{negl}(\lambda).$$

Game 5: Here, instead of honestly generating \mathbf{c}_0^* and \mathbf{c}_1^* , we draw $\mathbf{c}_1^* \leftarrow \mathbb{Z}_q^{2\overline{m}}$ and $\tilde{\mathbf{c}}_0^{*R}, \tilde{\mathbf{c}}_0^{*S} \leftarrow \mathbb{Z}_q^m$ and set $\mathbf{c}_0^* = (\tilde{\mathbf{c}}_0^{*R} + (\mathbf{k}^* \cdot \lfloor q/2 \rfloor)^\top \mathbf{A}^R, \tilde{\mathbf{c}}_0^{*S} + (\mathbf{k}^* \cdot \lfloor q/2 \rfloor)^\top \mathbf{A}^S)$. We can then use [11, Lemma 5] to reduce this game-step to the NLWE-assumption with the only adaption being that we replace the definition of $(\mathbf{c}_1^*)^\top = (\mathbf{c}_0^*)^\top \mathbf{R} + \mathbf{v}^\top$ by $(\mathbf{c}_1^*)^\top = ((\mathbf{c}_0^{*R})^\top \mathbf{R}^R + \mathbf{v}^{R^\top}, (\mathbf{c}_0^{*S})^\top \mathbf{R}^S + \mathbf{v}^{S^\top})$. This results in

$$\begin{split} |\mathbb{P}\left[S_{5}\right] - \mathbb{P}\left[S_{4}\right]| &\leq \mathsf{Adv}^{\mathsf{NLWE}_{n,m,q,\chi}}_{\mathcal{B}_{2}}(\lambda) \quad \text{as well as} \\ |\mathbb{P}\left[\mathsf{Forge}_{5}\right] - \mathbb{P}\left[\mathsf{Forge}_{4}\right]| &\leq 2\mathsf{Adv}^{\mathsf{NLWE}_{n,m,q,\chi}}_{\mathcal{B}_{2}'}(\lambda). \end{split}$$

Game 6: We now replace \mathbf{c}_0^* of Game 5 with $\mathbf{c}_0^* \leftarrow \mathbb{Z}_q^{2m}$. As $\tilde{\mathbf{c}_0^*}$ was only used to generate \mathbf{c}_0^* and acted as a one-time-pad, the distributions of both games are identical and thus

$$\mathbb{P}\left[S_{6}\right] = \mathbb{P}\left[S_{5}\right] \quad \text{and} \quad \mathbb{P}\left[\text{Forge}_{6}\right] = \mathbb{P}\left[\text{Forge}_{5}\right].$$

Game 7: Instead of generating the signing key dk^* and the MAC key mk^* using the KDF, we just draw them from the key spaces of SKE and MAC uniformly. As \mathbf{k}^* is independent of \mathbf{c}^* since Game 6, this change can be reduced to the security of the KDF. More specifically, using [11, Lemma 6] we can show that

$$\begin{split} |\mathbb{P}\left[S_7\right] - \mathbb{P}\left[S_6\right]| &\leq \mathsf{Adv}^{\mathrm{IND}}_{\mathtt{KDF},\mathcal{B}_3'}(\lambda) \quad \mathrm{as \ well \ as} \\ |\mathbb{P}\left[\mathrm{Forge}_7\right] - \mathbb{P}\left[\mathrm{Forge}_6\right]| &\leq 2\mathsf{Adv}^{\mathrm{IND}}_{\mathtt{KDF},\mathcal{B}_3'}(\lambda). \end{split}$$

But as mk^* is now uniformly sampled and independent of $\mathbf{c}_0^*, \mathbf{c}_1^*$ and ϕ^* , $\mathbb{P}[\text{Forge}_7]$ can straightforwardly be bound by the security of the MAC using [11, Lemma 7] to arrive at

$$\mathbb{P}\left[\mathrm{Forge}_7\right] \leq Q_2 \cdot \mathsf{Adv}_{\mathtt{MAC},\mathcal{B}_4}^{\mathrm{OT\text{-}SUF}}(\lambda).$$

Game 8: Last but not least we replace the encrypted message ϕ^* of the challenge ciphertext by a random ciphertext. As dk^* is independently and randomly chosen, a straightforward reduction shows

$$|\mathbb{P}[S_8] - \mathbb{P}[S_7]| \leq \mathsf{Adv}_{\mathsf{SKE},\mathcal{B}_5}^{\mathrm{OT\text{-}IND}}(\lambda).$$

We note that in Game 8 the challenge ciphertext is independent of the chosen value b, and thus the adversary has no advantage in winning Game 8. Using our assumptions we finally see that the winning probability between all games only changes negligible, and thus

$$\mathsf{Adv}_{\mathrm{DRE},\mathcal{A}}^{\mathrm{IND\text{-}CCA2}_{\mathrm{DRE}}}(\lambda) \leq \frac{1}{2} + \mathtt{negl}(\lambda),$$

which finishes the proof.

5.2 Code-based Construction of a Sound and IND-CCA2_{DRE} Secure DRE

We adapt the LPN-based PKE from Kiltz, Masny, and Pietrzak [35] to create an IND-CCA2_{DRE} secure DRE scheme with soundness. The double trapdoor technique employed by the authors allows us to convert their PKE into a DRE construction, while actually reducing the public key by one matrix and only slightly increasing the ciphertext size.

We note here that Boyen, Izabachène, and Li [11] adapted the scheme of Kiltz, Masny, and Pietrzak [35] as well to create an IND-CCA2 secure hybrid encryption scheme based on LPN, which shares the symmetric part of our scheme.

As before only the decryption for R is described in Figure 8, but the decryption for S works exactly the same with swapped party identifiers. Also, everything happens in \mathbb{Z}_2 , and so the operations "+" and "-" can be used interchangeably.

In this scheme we use a constant 0 < c < 1/4 defining the Bernoulli parameter $p = \sqrt{c/m}$ and the bounding parameter $\beta = 2\sqrt{cm}$. Additionally, we use an efficient binary linear error-correcting code $\mathbf{G} : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ correcting up to αm errors for $4c < \alpha < 1$, which exists by Lemma 2.

```
\frac{\text{gen}(1^{\lambda})}{1: \quad \mathbf{A} \leftarrow \$ \mathbb{Z}_{2}^{n \times m}, \mathbf{R} \leftarrow \text{Ber}_{p}^{m \times m}}2: \quad \mathbf{A}_{1} = \mathbf{A} \cdot \mathbf{R}3: \quad \mathbf{return} \ (pk, sk) := ((\mathbf{A}, \mathbf{A}_{1}), \mathbf{R})
```

```
enc(pk^R, pk^S, \mathbf{M})
                                                                                                                        dec(sk^R, pk^R, pk^S, \mathbf{C})
  1: parse pk^R = (\mathbf{A}^R, \overline{\mathbf{A}_1^R})
                                                                                                                          1: parse pk^R = (\mathbf{A}^R, \mathbf{A}_1^R)
 2: parse pk^S = (\mathbf{A}^S, \mathbf{A}_1^S)
                                                                                                                         2: parse pk^S = (\mathbf{A}^S, \mathbf{A}_1^S)
 s \in \{0,1\}^n
                                                                                                                         3: parse sk^R = (\mathbf{R}^R)
  4: (dk, mk) := KDF(s)
                                                                                                                         4: parse \mathbf{C} = (\mathbf{c}_0^R, \mathbf{c}_0^S, \mathbf{c}_1^R, \mathbf{c}_1^S, \phi, \sigma)
  5: \mathbf{e}^R, \mathbf{e}^S \leftarrow \mathrm{Ber}_p^m
                                                                                                                         5: \mathbf{c}_t^R \coloneqq \mathbf{c}_1^R - \mathbf{c}_0^R \mathbf{R}^R
  6: \mathbf{c}_0 = (\mathbf{s}^{\top} \mathbf{A}^R + \mathbf{e}^R, \mathbf{s}^{\top} \mathbf{A}^S + \mathbf{e}^S)
                                                                                                                         6: \mathbf{s} \coloneqq \mathtt{decode}_{\mathbf{G}}\left(\mathbf{c}_{t}^{R}\right) \cdot \mathtt{FRD}(\mathtt{H}(\mathbf{c}_{0}))^{-1}
  7: \mathbf{T}^R, \mathbf{T}^S \leftarrow \mathrm{Ber}_n^{m \times m}
                                                                                                                         7: if \left\|\mathbf{c}_0^R - \mathbf{s}^\top \mathbf{A}^R\right\|_{\infty} > \beta output \perp
  8: \mathbf{c}_1 = (\mathbf{s}^{\top}(\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^R)^{\top}\mathbf{T}^R,
                                                                                                                         8: if \left\|\mathbf{c}_0^S - \mathbf{s}^\top \mathbf{A}^S\right\|_w > \beta output \perp
            \mathbf{s}^{\top}(\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^S)^{\top}\mathbf{T}^S)
          \phi := \texttt{SKE.enc}(dk, \mathbf{M})
                                                                                                                         9: if \left\|\mathbf{c}_1^R - \mathbf{s}^\top (\mathbf{A}_1^R + \text{FRD}(\mathbf{H}(\mathbf{c}_0))\mathbf{G})\right\|_w > \frac{\alpha m}{2}
10: \sigma := \mathtt{MAC.sign}(mk, (\mathbf{c}_0, \mathbf{c}_1, \phi))
                                                                                                                        10: if \|\mathbf{c}_1^S - \mathbf{s}^\top (\mathbf{A}_1^S + \text{FRD}(\mathbf{H}(\mathbf{c}_0))\mathbf{G})\|_{\infty} > \frac{\alpha m}{2}
11: return \mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1, \phi, \sigma)
                                                                                                                        11: (dk, mk) = KDF(s)
                                                                                                                        12: if 1 == MAC.Vfy(mk, (\mathbf{c}_0, \mathbf{c}_1, \phi), \sigma)
                                                                                                                        13: \mathbf{return} \ \mathbf{M} = \mathsf{SKE.dec}(dk, \phi)
                                                                                                                        14: else return \mathbf{M} = \bot
```

 $\textbf{Fig. 8.} \ \, \text{Description of} \ \, \boldsymbol{\Sigma}_{\texttt{LPN-DRE}} = (\texttt{gen}, \texttt{enc}, \texttt{dec})$

Theorem 4. The DRE $\Sigma_{LPN-DRE} = (gen, enc, dec)$ is correct.

Proof. As the same parameters are used, the proof of [35, Theorem 1] shows that

$$\underset{\mathbf{e} \leftarrow \operatorname{Ber}_p^m}{\mathbb{P}} \left[\| \mathbf{e} \|_w > \beta \right] < 2^{-\Theta(\sqrt{m})} \tag{1}$$

as well as

$$\mathbb{P}_{\mathbf{T} \leftarrow \operatorname{Ber}_{n}^{m \times m}} \left[\| \mathbf{T} \mathbf{e} \|_{w} > \frac{\alpha m}{2} \mid \| \mathbf{e} \|_{w} \le \beta \right] < 2^{-\Theta(m)}.$$
 (2)

Thus, for a properly generated ciphertext, it holds with overwhelming probability $1 - 2^{\Theta(\sqrt{m})}$ for $i \in \{R, S\}$ that

$$\left\|\mathbf{e}^i\right\|_w \leq \beta \ \wedge \ \left\|(\mathbf{e}^i)^\top \mathbf{T}^i\right\|_w \leq \frac{\alpha m}{2} \ \wedge \ \left\|(\mathbf{e}^i)^\top \mathbf{R}^i\right\|_w \leq \frac{\alpha m}{2}.$$

In this case, by the error correction property of the code G, the correct sis recovered from $\mathbf{c}_t^R = \mathbf{s}^{\top} \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0)) \mathbf{G} + (\mathbf{e}^R)^{\top} (\mathbf{T}^R - \mathbf{R}^R)$ as the error term satisfies $\|(\mathbf{e}^R)^{\top} (\mathbf{T}^R - \mathbf{R}^R)\|_w \leq \alpha m$ by Equation (2). Also, all decryption checks succeed and thus the correct message M is recovered by the determinism of KDF, MAC. Vfy and SKE.dec.

Theorem 5. The DRE $\Sigma_{LPN-DRE} = (\text{gen, enc, dec})$ is sound as in Definition 3.

The proof is similar to proof 2 but this time we use the decoding properties of G for the uniqueness of s.

Proof. Assume the scheme is not sound. Then there exists an adversary \mathcal{A} whose advantage $\mathsf{Adv}^{\mathsf{dre-sound}}_{\mathcal{E},\mathcal{A}}$ is non-negligible, where the advantage is defined as in Definition 3. Thus, given two public keys $pk^R = (\mathbf{A}^R, \mathbf{A}_1^R), pk^S = (\mathbf{A}^S, \mathbf{A}_1^S),$ the adversary \mathcal{A} returns with non-negligible advantage a valid ciphertext \mathbf{c} with $\operatorname{dec}(sk^R, \ pk^S, \ pk^R, \mathbf{c}) \neq \operatorname{dec}(sk^S, \ pk^S, \ pk^R, \ \mathbf{c}).$

At least one party has to accept the ciphertext as otherwise both parties would return \perp . Thus, we can assume without loss of generality that R outputs a message and therefore the decryption checks are valid. In particular, we have a message and therefore the decryption checks are valid. In particular, we have $\|\mathbf{c}_1^S - (\mathbf{s}^R)^\top (\mathbf{A}_1^S + \mathsf{FRD}(\mathsf{H}(\mathbf{c}_0))\mathbf{G})\|_w \leq \frac{\alpha m}{2}$, where \mathbf{s}^R is the vector that R recovered in step 6. This means that $\mathbf{c}_1^S = (\mathbf{s}^R)^\top (\mathbf{A}_1^S + \mathsf{FRD}(\mathsf{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}_1')^\top$ with $\|\mathbf{e}_1'\|_w \leq \frac{\alpha m}{2}$. Similarly, we have $\mathbf{c}_0^S = (\mathbf{s}^R)^\top \mathbf{A}^S + (\mathbf{e}_0')^\top$ with $\|\mathbf{e}_0'\|_w \leq \beta$. Therefore, it holds that $\mathbf{c}_t^S = \mathbf{c}_1^S - \mathbf{c}_0^S \mathbf{R}^S = \mathbf{s}^R \mathsf{FRD}(\mathsf{H}(c_0))\mathbf{G} + (\mathbf{e}_1')^\top - (\mathbf{e}_0')^\top \mathbf{R}^S$. As $\|\mathbf{e}_1'\|_w \leq \frac{\alpha m}{2}$ we only need to show $\|(\mathbf{e}_0')^\top \mathbf{R}^S\|_w \leq \frac{\alpha m}{2}$. Indeed, the decoding property of \mathbf{G} guarantees the correct decoding of \mathbf{g} is the inequality holds, and as the following of \mathbf{G} is a sum of \mathbf{G} and \mathbf{G} .

KDF, MAC. Vfy and SKE.dec are deterministic, both parties will decrypt the same

To show that $\|(\mathbf{e}_0')^{\top}\mathbf{R}\|_w \leq \frac{\alpha m}{2}$ with overwhelming probability, notice first that $\#\{\mathbf{e} \in \mathbb{Z}_2^m \mid \|\mathbf{e}\|_w \leq \beta\} = \sum_{i=0}^{\beta} {m \choose i} \leq 2^{\log(m)\mathcal{O}(\sqrt{m})}$ because $\beta = \Theta(\sqrt{m})$. Thus, taking the union bound over all $\mathbf{e} \in \mathbb{Z}_2^m$ with $\|\mathbf{e}\|_w \leq \beta$ we get

$$\underset{\mathbf{R}^{S}}{\mathbb{P}}\left[\left\langle \mathbf{e},\left\|\mathbf{e}\right\|_{w} \leq \beta: \left\|\mathbf{e}^{\top}\mathbf{R}^{S}\right\|_{w} \leq \frac{\alpha m}{2}\right] \geq 1 - 2^{\Theta(m)}$$

using Equation (2) as desired, which finishes the proof.

Theorem 6. The DRE $\Sigma_{\textit{LPN-DRE}} = (\text{gen}, \text{enc}, \text{dec})$ is IND-CCA2_{DRE}-secure as in Definition 2 if $\textit{LPN}_{n,m,p}$ is hard, and SKE, MAC, H, KDF are all secure w.r.t. Definitions 5, 6, 8 and 9.

To prove this we use ideas of Boyen, Izabachène, and Li [11, Theorem 1] and Kiltz, Masny, and Pietrzak [35, Theorem 2]. Therefore, this proof shares its structure with proof 3, and for faster understanding, games that differ from aforementioned proof are highlighted by underscoring them.

Proof. Game 0: This game follows the IND-CCA2-DRE game. So again, \mathcal{A} gets two independently generated public keys, makes decryption queries to the oracle which can be honestly answered using the secret keys. After that, \mathcal{A} submits two messages M_0, M_1 of equal length, after which the challenge ciphertext is computed by $\mathbf{c}^* = \text{enc}(pk^R, pk^S, M_b)$ for $b \leftarrow \{0, 1\}$. The adversary \mathcal{A} can now make further queries provided that the used public key is from the set $\{R, S\}$ and $\mathbf{c} \neq \mathbf{c}^*$. Finally, \mathcal{A} outputs b' and the game returns 1 if b = b'. By definition, we have

$$\mathbb{P}\left[S_{0}\right] = \mathbb{P}\left[\mathsf{Exp}_{\mathrm{DRE},\mathcal{A}}^{\mathrm{IND\text{-}CCA2}_{\mathrm{DRE}}}(\lambda) = 1\right].$$

Game 1: In this game, \mathbf{c}_0^* is precomputed before sending the two generated public keys to \mathcal{A} . More specifically, steps 3 to 6 of the encoding in Figure 8 are now done before sending the public keys to \mathcal{A} . As the precomputed \mathbf{c}_0^* is already unavailable to \mathcal{A} until \mathbf{c}^* is released and nothing else changed we get

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

Game 2: This is identical to Game 1 except for the decryption oracle, which now rejects ciphertexts with $H(\mathbf{c}_0) = H(\mathbf{c}_0^*)$ in the first phase as well as ciphertexts with $\mathbf{c}_0 \neq \mathbf{c}_0^*$ and $H(\mathbf{c}_0) = H(\mathbf{c}_0^*)$ in the second phase. Using [11, Lemma 4] we get (for Q_1 being the number of decryption queries in the first phase)

$$|\mathbb{P}\left[S_{2}\right] - \mathbb{P}\left[S_{1}\right]| \leq \frac{Q_{1}}{q^{n}} + \mathsf{Adv}_{\mathtt{H},\mathcal{B}_{1}(\lambda)}^{\mathrm{CR}}.$$

<u>Game 3:</u> We now additionally forbid all decryption queries with $\mathbf{c}_0 = \mathbf{c}_0^*$ after the challenge ciphertext has been released. We can bound the probability that \mathcal{A} submits a valid decryption query $\mathbf{c} = (\mathbf{c}_0^*, \mathbf{c}_1, \phi, \sigma) \neq \mathbf{c}^*$ by two sub-events:

- (1) NoBind: a different key $\mathbf{s} \neq \mathbf{s}^*$ is associated to \mathbf{c}_0^* .
- (2) Forge: the key \mathbf{s}^* from \mathbf{c}^* was used for \mathbf{c} .

Our definition of \mathbf{c}_0 (step 6 of Figure 8) and the uniqueness of LPN samples⁷ proves that \mathbb{P} [NoBind] is negligible, and thus

$$|\mathbb{P}[S_4] - \mathbb{P}[S_3]| \leq \mathbb{P}[\text{Forge}_3] + \text{negl}(\lambda).$$

⁷ See for example [25, Lemma 3.2].

<u>Game 4:</u> Our goal again is to set $\mathbf{A}_1^R = \mathbf{A}^R \mathbf{R}^R - \text{FRD}(\mathbf{H}(\mathbf{c}_0^*))\mathbf{G}$ as well as $\mathbf{A}_1^S = \mathbf{A}^S \mathbf{R}^S - \text{FRD}(\mathbf{H}(\mathbf{c}_0^*))\mathbf{G}$. Because of the low noise rate of the private keys, \mathbf{A}_1^R and \mathbf{A}_1^S are only computationally indistinguishable from uniformly random matrices based on the KLPN problem (whereas those matrices were statistically close to uniform in our LWE construction from Section 5.1). To solve this we split this game into multiple smaller steps. The idea is to use the double trapdoor already present in the DRE scheme because of the (sound) encryption for both parties to first adapt sk^R and then sk^S . In the process we also adapt \mathbf{c}^* so that later we can use an LPN sample to hide the challenge bit. A recap of the changes can be found before Game 5.

Game 4.1: All decryption queries are answered using sk^S . By the soundness property of our construction (see Theorem 5) we have

$$|\mathbb{P}\left[S_{4.1}\right] - \mathbb{P}\left[S_{3}\right]| \leq \mathtt{negl}(\lambda) \ \ \mathrm{and} \ \ \ |\mathbb{P}\left[\mathrm{Forge}_{4.1}\right] - \mathbb{P}\left[\mathrm{Forge}_{3}\right]| \leq \mathtt{negl}(\lambda).$$

Game 4.2: We replace \mathbf{A}_1^R by a random matrix. This can be reduced to the KLPN assumption: Assume we have a distinguisher \mathcal{D} between Game 4.1 and 4.2. Our attacker \mathcal{A}_1 on KLPN gets (\mathbf{A}, \mathbf{B}) and has to decide whether $\mathbf{B} \leftarrow \mathbb{S} \mathbb{Z}_2^{n \times m}$ or $\mathbf{B} = \mathbf{A}\mathbf{E}$ for $\mathbf{A} \leftarrow \mathbb{S} \mathbb{Z}_2^{n \times m}$ and $\mathbf{E} \leftarrow \mathrm{Ber}_p^{m \times m}$. It simulates Game 4.1 but instead of generating \mathbf{A}^R and \mathbf{A}_1^R it sets $\mathbf{A}^R \coloneqq \mathbf{A}$ and $\mathbf{A}_1^R \coloneqq \mathbf{B}$. As sk^R is not used anymore this does not change the decryption capabilities of the oracle, and so if $\mathbf{B} \leftarrow \mathbb{S} \mathbb{Z}_2^{n \times m}$ this perfectly simulates Game 4.2, while if $\mathbf{B} = \mathbf{A}\mathbf{E}$ this perfectly simulates Game 4.1. Thus, the advantage of \mathcal{A}_1 is that of \mathcal{D} , and so we have

$$|\mathbb{P}\left[S_{4.2}\right] - \mathbb{P}\left[S_{4.1}\right]| \leq \mathsf{Adv}_{\mathcal{A}_1}^{\mathsf{KLPN}_{n,m,p}}(\lambda).$$

For the Forge probabilities, the adversary \mathcal{A}_2 follows the same game as above, but for every decryption query $\mathbf{c} = (\mathbf{c}_0^*, \mathbf{c}_1, \phi, \sigma) \neq \mathbf{c}^*$ it checks if MAC.Vfy $(mk^*, (\mathbf{c}_0, \mathbf{c}_1, \phi), \sigma) = 1$. In this case, it outputs 1 to the KLPN challenger, otherwise it replies with \bot to the decryption query. If this never happens \mathcal{A}_2 outputs a random bit. As in [11, Lemma 5] this results in

$$|\mathbb{P}\left[\mathrm{Forge}_{4.2}\right] - \mathbb{P}\left[\mathrm{Forge}_{4.1}\right]| \leq 2\mathsf{Adv}_{\mathcal{A}_2}^{\mathsf{KLPN}_{n,m,p}}(\lambda).$$

Game 4.3: In this game $\mathbf{A}_1^R = \mathbf{B}$ is replaced by $\mathbf{A}_1^R = \mathbf{B} - \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0^*))\mathbf{G}$ for $\mathbf{B} \leftarrow \mathbb{Z}_2^{n \times m}$. As \mathbf{B} is a one time pad this does not change the distributions, and so

$$\mathbb{P}[S_{4,3}] = \mathbb{P}[S_{4,2}]$$
 and $\mathbb{P}[\text{Forge}_{4,3}] = \mathbb{P}[\text{Forge}_{4,2}]$.

Game 4.4: We now replace $\mathbf{A}_1^R = \mathbf{B} - \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0^*))$ by our secret key trapdoor $\mathbf{A}_1^R = \mathbf{A}^R \mathbf{R}^R - \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0^*)) \mathbf{G}$. We also adapt \mathbf{c}_1^{*R} such that instead of sampling \mathbf{T}^R and honestly generating \mathbf{c}_1^{*R} we instead replace it by $\mathbf{c}_1^{*R} := \mathbf{s}^\top (\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0^*)) \mathbf{G}) + (\mathbf{e}^R)^\top \mathbf{R}^R$. Similar to Game 4.2 this can be reduced to the EKLPN assumption. For this, assume that there is a distinguisher \mathcal{D} between Game 4.4 and 4.3. The adversary \mathcal{A}_3 on

EKLPN gets $(\mathbf{A}, \mathbf{B}, \mathbf{z}, \mathbf{u})$ and has to decide whether $\mathbf{B} \leftarrow \mathbb{Z}_2^{n \times m}$ or $\mathbf{B} = \mathbf{A}\mathbf{E}$ for $\mathbf{A} \leftarrow \mathbb{Z}_2^{n \times m}, \mathbf{E} \leftarrow \operatorname{Ber}_p^{m \times m}, \mathbf{z} \leftarrow \operatorname{Ber}_p^m$ and $\mathbf{u} = \mathbf{z}^{\top}\mathbf{E}$. It then simulates Game 4.3 but sets $\mathbf{A}^R := \mathbf{A}, \mathbf{A}_1^R := \mathbf{B}, \mathbf{c_0}^{*R} := \mathbf{s}^{\top}\mathbf{A}^R + \mathbf{z}$ and $\mathbf{c_1^*}^R \coloneqq \mathbf{s}^\top (\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0^*))\mathbf{G}) + \mathbf{u}.$

Now, if $\mathbf{B} \leftarrow \mathbb{Z}_2^{n \times m}$ this perfectly simulates Game 4.3 because \mathbf{E} and \mathbf{T}^{R} have the same distribution and both are not used outside of the error generation, whereas if $\mathbf{B} = \mathbf{A}\mathbf{E}$ the construction perfectly simulates Game 4.4. As before, together this gives us

$$\begin{split} |\mathbb{P}\left[S_{4.4}\right] - \mathbb{P}\left[S_{4.3}\right]| &\leq \mathsf{Adv}_{\mathcal{A}_3}^{\mathsf{EKLPN}_{n,m,p}}(\lambda) \quad \text{and} \\ |\mathbb{P}\left[\mathsf{Forge}_{4.4}\right] - \mathbb{P}\left[\mathsf{Forge}_{4.3}\right]| &\leq 2\mathsf{Adv}_{\mathcal{A}_4}^{\mathsf{EKLPN}_{n,m,p}}(\lambda). \end{split}$$

Game 4.5: Decryption is now always done via sk^R instead of sk^S . The decryption oracle can still handle the same set of decryption queries. Indeed, given a valid $\mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1, \phi, \sigma)$ we have

$$\begin{split} \mathbf{c}_1^{R^\top} = & \mathbf{s}^\top (\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^R)^\top \mathbf{T}^R \\ = & \mathbf{s}^\top (\mathbf{A}^R \mathbf{R}^R + (\mathtt{FRD}(\mathtt{H}(\mathbf{c}_0)) - \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0^*)))\mathbf{G}) + (\mathbf{e}^R)^\top \mathbf{T}^R. \end{split}$$

As for all $H(\mathbf{c}_0) \neq H(\mathbf{c}_0^*)$ the difference $FRD(H(\mathbf{c}_0)) - FRD(H(\mathbf{c}_0^*))$ is invertible by the definition of FRD, the trapdoor \mathbf{R}^R can be used to decrypt the queries. The case $H(\mathbf{c}_0) = H(\mathbf{c}_0^*)$ was already rejected from Game 3 on. Also, by the soundness the difference between using sk^R or sk^S is negligible, and so we get

$$|\mathbb{P}\left[S_{4.5}\right] - \mathbb{P}\left[S_{4.4}\right]| \leq \mathtt{negl}(\lambda) \text{ and } |\mathbb{P}\left[\mathrm{Forge}_{4.5}\right] - \mathbb{P}\left[\mathrm{Forge}_{4.4}\right]| \leq \mathtt{negl}(\lambda).$$

Game 4.6: We repeat Game 4.2-Game 4.4 with sk^S . This results in $\mathbf{A}_1^S = \mathbf{A}^S \mathbf{R}^S - \text{FRD}(\mathbf{H}(\mathbf{c}_0^*))$ and $\mathbf{c_1^*}^S \coloneqq \mathbf{s}^\top (\mathbf{A}_1^S + \text{FRD}(\mathbf{H}(\mathbf{c}_0^*))\mathbf{G}) + (\mathbf{e}^S)^\top \mathbf{R}^S$ with probability differences

$$\begin{split} |\mathbb{P}\left[S_{4.6}\right] - \mathbb{P}\left[S_{4.5}\right]| &\leq \mathsf{Adv}_{\mathcal{A}_5}^{\mathsf{KLPN}_{n,m,p}}(\lambda) + \mathsf{Adv}_{\mathcal{A}_6}^{\mathsf{EKLPN}_{n,m,p}}(\lambda) \quad \text{and} \\ \mathbb{P}\left[\mathsf{Forge}_{4.6}\right] - \mathbb{P}\left[\mathsf{Forge}_{4.5}\right] &\leq 2\mathsf{Adv}_{\mathcal{A}_7}^{\mathsf{KLPN}_{n,m,p}}(\lambda) + 2\mathsf{Adv}_{\mathcal{A}_8}^{\mathsf{EKLPN}_{n,m,p}}(\lambda). \end{split}$$

After Game 4.6 we have (for $i \in \{R, S\}$) $\mathbf{A}_1^i + \text{FRD}(\mathbf{H}(\mathbf{c}_0^*))\mathbf{G} = \mathbf{A}^i\mathbf{R}^i$, and thus at this point the scheme differs in the following way from the original

- $(pk^i, sk^i) = ((\mathbf{A}^i, \mathbf{A}^i_1), \mathbf{R}^i)$ where $\mathbf{A}^i \leftarrow \mathbb{Z}_2^{n \times m}, \mathbf{R}^i \leftarrow \mathrm{Ber}_n^{m \times m}$ and then $\mathbf{A}_{1}^{i} := \mathbf{A}^{i} \mathbf{R}^{i} - \text{FRD}(\mathbf{H}(\mathbf{c}_{0}^{*})) \mathbf{G}$ $\bullet \ \mathbf{c}_{0}^{*} = (\mathbf{s}^{\top} \mathbf{A}^{R} + \mathbf{e}^{R}, \mathbf{s}^{\top} \mathbf{A}^{S} + \mathbf{e}^{S})$ $\bullet \ \mathbf{c}_{1}^{*} = (\mathbf{s}^{\top} \mathbf{A}^{R} \mathbf{R}^{R} + (\mathbf{e}^{R})^{\top} \mathbf{R}^{R}, \mathbf{s}^{\top} \mathbf{A}^{S} \mathbf{R}^{S} + (\mathbf{e}^{S})^{\top} \mathbf{R}^{S}).$

⁸ As \mathbf{c}_0^* is calculated after \mathbf{A}^i is generated but before \mathbf{A}_1^i is generated, it can be used to calculate \mathbf{A}_1^i .

Game 5: Instead of honestly generating \mathbf{c}_0^* and \mathbf{c}_1^* , we draw both $\mathbf{c}_0^{*R} \leftarrow \mathbb{Z}_2^m$ and $\mathbf{c}_0^{*S} \leftarrow \mathbb{Z}_2^m$ and set $\mathbf{c}_1^{*R} \coloneqq \mathbf{c}_0^{*R} \mathbf{R}^R$ as well as $\mathbf{c}_1^{*S} \coloneqq \mathbf{c}_0^{*S} \mathbf{R}^S$. This game step can be reduced to the LPN problem. So assume that there is a distinguisher \mathcal{D} between Game 5 and 4.6. Let \mathcal{A}_9 be an adversary to the LPN problem who gets $((\mathbf{A}^1, \mathbf{A}^2), (\mathbf{u}^1, \mathbf{u}^2))$ where $\mathbf{u}^i \leftarrow \mathbb{Z}_2^m$ or $\mathbf{u}^i = \mathbf{s}^\top \mathbf{A}^i + \mathbf{e}^i$ for $\mathbf{A}^i \leftarrow \mathbb{Z}_2^m$ and $\mathbf{e}^i \leftarrow \mathrm{Ber}_p^m$. It simulates Game 4.6 but sets $\mathbf{c}_0^{*R} = \mathbf{u}^1$, $\mathbf{c}_0^{*S} = \mathbf{u}^2$, $\mathbf{c}_1^{*R} = \mathbf{u}^1 \mathbf{R}^R$ and $\mathbf{c}_1^{*S} = \mathbf{u}^2 \mathbf{R}^S$. Now if $\mathbf{u}^i = \mathbf{s}^\top \mathbf{A}^i + \mathbf{e}^i$ this perfectly simulates Game 4.6 by our previous

Now if $\mathbf{u}^i = \mathbf{s}^{\top} \mathbf{A}^i + \mathbf{e}^i$ this perfectly simulates Game 4.6 by our previous comment, whereas if $\mathbf{u}^i \leftarrow \mathbb{Z}_2^m$ this simulates Game 5. As before that means we have

$$\begin{split} |\mathbb{P}\left[S_{5}\right] - \mathbb{P}\left[S_{4.6}\right]| &\leq \mathsf{Adv}^{\mathsf{LPN}_{n,2m,p}}_{\mathcal{A}_{9}}(\lambda) \quad \text{as well as} \\ |\mathbb{P}\left[\mathsf{Forge}_{5}\right] - \mathbb{P}\left[\mathsf{Forge}_{4.6}\right]| &\leq 2\mathsf{Adv}^{\mathsf{LPN}_{n,2m,p}}_{\mathcal{A}_{10}}(\lambda). \end{split}$$

Game 6: Instead of generating the signing key dk^* and the MAC key mk^* using the KDF, we just draw them from the key spaces of SKE and MAC uniformly. As \mathbf{s}^* is independent of \mathbf{c}^* since Game 5, this change can be reduced to the security of the KDF. More specifically, using [11, Lemma 6] we can show that

$$\begin{split} |\mathbb{P}\left[S_6\right] - \mathbb{P}\left[S_5\right]| &\leq \mathsf{Adv}^{\mathrm{IND}}_{\mathsf{KDF},\mathcal{B}_3'}(\lambda) \quad \text{as well as} \\ |\mathbb{P}\left[\mathrm{Forge}_6\right] - \mathbb{P}\left[\mathrm{Forge}_5\right]| &\leq 2\mathsf{Adv}^{\mathrm{IND}}_{\mathsf{KDF},\mathcal{B}_3'}(\lambda). \end{split}$$

But as mk^* is now uniformly sampled and independent of \mathbf{c}_0^* , \mathbf{c}_1^* and ϕ^* , $\mathbb{P}\left[\text{Forge}_6\right]$ can straightforwardly be bound by the security of the MAC using [11, Lemma 7] to arrive at

$$\mathbb{P}\left[\mathrm{Forge}_{6}\right] \leq Q_{2} \cdot \mathsf{Adv}_{\mathtt{MAC},\mathcal{B}_{4}}^{\mathtt{OT-SUF}}(\lambda).$$

Game 7: Last but not least we replace the encrypted message ϕ^* of the challenge ciphertext by a random ciphertext. As dk^* is independently and randomly chosen, a straightforward reduction shows

$$|\mathbb{P}\left[S_{7}\right] - \mathbb{P}\left[S_{6}\right]| \leq \mathsf{Adv}^{\mathrm{OT\text{-}IND}}_{\mathtt{SKE},\mathcal{B}_{5}}(\lambda)$$

We note that in Game 7 the challenge ciphertext is independent of the chosen value b, and thus the adversary has no advantage in winning Game 7. Using our assumptions we finally see that the winning probability between all games only changes negligible, and thus

$$\mathsf{Adv}_{\mathrm{DRE},\mathcal{A}}^{\mathrm{IND\text{-}CCA2}_{\mathrm{DRE}}}(\lambda) \leq \frac{1}{2} + \mathtt{negl}(\lambda),$$

which finishes the proof.

We discuss further observations that might be of independent interest in Section 6.

 $^{^{9}}$ Notice that this is actually an $\mathrm{LPN}_{n,2m,p}$ sample.

6 Discussion

Secure parameters for our schemes from Section 5 as well as their resulting sizes can be found in Appendix B.

Modular Hybrid Encryption: Boyen, Izabachène, and Li [11] mention that proving the security of the KEM-part in their construction is left for future work. Solving this task would be in fact an interesting result, which might lead to more efficient IND-CCA2 constructions of PKE or DRE in the standard model. For DRE, however, additional assumptions, such as correlated product security [46], are required as encrypting the same secret twice might in general counteract the one-wayness property as shown by Rosen and Segev [46] for the RSA one-way function. Our observation is that the security of the KEM part in the hybrid construction from Boyen, Izabachène, and Li [11] has to be weaker than the replayable chosen ciphertext attack (RCCA) security, which is defined for a PKE by Canetti, Krawczyk, and Nielsen [17] and adapted to the KEM definition from Abe, Gennaro, and Kurosawa [1]. In lattice- or LPN-based trapdoor functions an adversary may always manipulate the error such that the inversion outputs an $\mathbf{x} \neq \bot$. Consider having a validity oracle that on input **c** checks whether the ciphertext decrypts to \perp . Note that the decryption oracle from the RCCA-Game returning test is such an oracle. Then the adversary may obtain the error vector by manipulating c and testing, whether the RCCA oracle returns test.

Partial Soundness There are corner cases where a weaker variant of soundness is sufficient, i.e., partial soundness or weak decryption consistency, which are equivalent when constrained to two recipients. This allows one party to decrypt the ciphertext to a valid message while the other party outputs \perp . The formal definitions can be found in Beskorovajnov et al. [8] and Noh et al. [44].

If one for example skips either step 8 or 9 (but not both) of the decryption in the NLWE-based construction of Section 5.1 (only checking the error of either \mathbf{c}_0^S or \mathbf{c}_1^S) one gets a slightly more efficient partially sound DRE. Thus, while an attacker cannot create a valid ciphertext encrypting different messages to S and R, they can create a ciphertext which S decrypts to a valid message while R outputs \bot . Indeed, one can achieve this by creating a valid ciphertext and adding a big enough error term to either \mathbf{c}_0^S or \mathbf{c}_1^S such that S does not accept the ciphertext, whereas R accepts and decrypts the ciphertext because it does not check this error. Partial soundness still holds because of the injectivity of the LWE function.

7 Conclusion

We observe that the literature of IND-CCA2_{DRE} secure DRE constructions in the standard model based on post-quantum assumptions lacks constructions that guarantee soundness. However, most of the literature around applications that employ DRE in a generic way require this exact property. Our main result comprises two constructions that fill this gap.

We point out that applications identified by us as non-generic in Section 3.4 may be abstracted further in future work in order to use a DRE in a black-box manner. Finally, we note that a DRE construction based on a post-quantum assumption with public verifiability and soundness, which is required by applications from Section 3.2, is still an open question.

Acknowledgements. We thank the PKC 2024 anonymous reviewers for their valuable feedback. The work presented in this paper has been supported by Helmholtz Information, Program "Engineering Digital Futures", Topic "Engineering secure Systems.

References

- Abe, M., Gennaro, R., and Kurosawa, K.: Tag-KEM/DEM: A New Framework for Hybrid Encryption, Cryptology ePrint Archive, Report 2005/027. (2017). https://eprint.iacr.org/2005/027
- Agrawal, S., Boneh, D., and Boyen, X.: Efficient Lattice (H)IBE in the Standard Model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010). DOI: 10.1007/978-3-642-13190-5 28
- Applebaum, B., Cash, D., Peikert, C., and Sahai, A.: Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 595–618. Springer, Heidelberg (2009). DOI: 10.1007/978-3-642-03356-8 35
- Bellare, M., and Rogaway, P.: Optimal Asymmetric Encryption. In: Santis, A.D. (ed.) EUROCRYPT 1995. LNCS, vol. 950, pp. 92–111. Springer, Heidelberg (1994). DOI: 10.1007/BFb0053428
- Benz, L., Beskorovajnov, W., Eilebrecht, S., Müller-Quade, J., Ottenhues, A., and Schwerdt, R.: Sender-binding Key Encapsulation. In: Public-Key Cryptography– PKC 2023: 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, Atlanta, GA, USA, May 7–10, 2023, Proceedings, Part I, pp. 744– 773 (2023). DOI: 10.1007/978-3-031-31368-4 26
- Bert, P., Eberhart, G., Prabel, L., Roux-Langlois, A., and Sabt, M.: Implementation of Lattice Trapdoors on Modules and Applications. In: Cheon, J.H., and Tillich, J.-P. (eds.) Post-Quantum Cryptography 12th International Workshop, PQCrypto 2021. LNCS, vol. 12841, pp. 195–214. Springer, Heidelberg (2021). DOI: 10.1007/978-3-030-81293-5 11
- Bert, P., Fouque, P.-A., Roux-Langlois, A., and Sabt, M.: Practical Implementation of Ring-SIS/LWE Based Signature and IBE. In: Lange, T., and Steinwandt, R. (eds.) Post-Quantum Cryptography 9th International Conference, PQCrypto 2018. LNCS, vol. 10786, pp. 271–291. Springer, Heidelberg (2018). DOI: 10.1007/978-3-319-79063-3 13
- 8. Beskorovajnov, W., Gröll, R., Müller-Quade, J., Ottenhues, A., and Schwerdt, R.: A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels. In: Hanaoka, G., Shikata, J., and Watanabe, Y. (eds.) PKC 2022. LNCS, vol. 13178, pp. 316–344. Springer, Heidelberg (2022). DOI: 10.1007/978-3-030-97131-1 11

- 9. Blaze, M., Bleumer, G., and Strauss, M.: Divertible Protocols and Atomic Proxy Cryptography. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 127–144. Springer, Heidelberg (1998). DOI: 10.1007/BFb0054122
- Boneh, D., Kim, S., and Nikolaenko, V.: Lattice-Based DAPS and Generalizations: Self-Enforcement in Signature Schemes. In: Gollmann, D., Miyaji, A., and Kikuchi, H. (eds.) ACNS 17. LNCS, vol. 10355, pp. 457–477. Springer, Heidelberg (2017). DOI: 10.1007/978-3-319-61204-1 23
- Boyen, X., Izabachène, M., and Li, Q.: Secure Hybrid Encryption in the Standard Model from Hard Learning Problems. In: Cheon, J.H., and Tillich, J.-P. (eds.) Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021, pp. 399–418. Springer, Heidelberg (2021). DOI: 10.1007/978-3-030-81293-5 21
- 12. BR, P., and Amberker, B.: Secure Group Key Management Scheme Based on Dual Receiver Cryptosystem. In: AsiaPKC '13, pp. 45–50. ACM Press (2013). DOI: 10.1145/2484389.2484399
- Brakerski, Z., and Vaikuntanathan, V.: Lattice-Inspired Broadcast Encryption and Succinct Ciphertext-Policy ABE, Cryptology ePrint Archive, Report 2020/191. (2020). https://eprint.iacr.org/2020/191
- Brendel, J., Fiedler, R., Günther, F., Janson, C., and Stebila, D.: Post-quantum asynchronous deniable key exchange and the signal handshake. In: Public-Key Cryptography–PKC 2022: 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part II, pp. 3–34 (2022). DOI: 10.1007/978-3-030-97131-1
- 15. Canetti, R., Dodis, Y., Pass, R., and Walfish, S.: Universally Composable Security with Global Setup. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 61–85. Springer, Heidelberg (2007). DOI: 10.1007/978-3-540-70936-7 4
- Canetti, R., Feige, R., Goldreich, O., and Naor, M.: Adaptively Secure Multi-Party Computation. In: 28th ACM STOC, pp. 639–648. ACM Press (1996). DOI: 10.1145/237814.238015
- Canetti, R., Krawczyk, H., and Nielsen, J.B.: Relaxing Chosen-Ciphertext Security.
 In: Boneh, D. (ed.) CRYPTO 2003, pp. 565–582. Springer, Heidelberg (2003). DOI: 10.1007/978-3-540-45146-4 33
- Chow, S.S.M., Franklin, M.K., and Zhang, H.: Practical Dual-Receiver Encryption
 Soundness, Complete Non-malleability, and Applications. In: Benaloh, J. (ed.)
 CT-RSA 2014. LNCS, vol. 8366, pp. 85–105. Springer, Heidelberg (2014). DOI: 10.1007/978-3-319-04852-9 5
- 19. Crescenzo, G.D., Ishai, Y., and Ostrovsky, R.: Non-Interactive and Non-Malleable Commitment. In: 30th ACM STOC, pp. 141–150. ACM Press (1998). DOI: 10.1145/276698.276722
- Damgård, I., Hofheinz, D., Kiltz, E., and Thorbeck, R.: Public-Key Encryption with Non-Interactive Opening. In: Malkin, T. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 239–255. Springer, Heidelberg (2008). DOI: 10.1007/978-3-540-79263-5_15
- 21. Diament, T., Lee, H.K., Keromytis, A.D., and Yung, M.: The Efficient Dual Receiver Cryptosystem and its Applications. International Journal of Network Security 13(3), 135–151 (2011). DOI: 10.7916/D81R7100
- Diament, T., Lee, H.K., Keromytis, A.D., and Yung, M.: The Dual Receiver Cryptosystem and its Applications. In: Atluri, V., Pfitzmann, B., and McDaniel, P. (eds.) ACM CCS 2004, pp. 330–343. ACM Press (2004). DOI: 10.1145/1030083. 1030128

- 23. Dodis, Y., Katz, J., Smith, A., and Walfish, S.: Composability and On-Line Deniability of Authentication. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 146–162. Springer, Heidelberg (2009). DOI: 10.1007/978-3-642-00457-5 10
- Dolev, D., and Yao, A.: On the Security of Public Key Protocols. IEEE Transactions on Information Theory 29(2), 198–208 (1983). DOI: 10.1109/TIT.1983.1056650
- 25. Döttling, N.: Cryptography based on the Hardness of Decoding. PhD thesis, Karlsruhe, Karlsruher Institut für Technologie (KIT), Diss., 2014 (2014).
- Dwork, C., Naor, M., and Sahai, A.: Concurrent Zero-Knowledge. J. ACM 51(6), 851–898 (2004). DOI: 10.1145/1039488.1039489
- 27. Esser, A., Kübler, R., and May, A.: LPN Decoded. In: Katz, J., and Shacham, H. (eds.) Advances in Cryptology CRYPTO 2017, pp. 486–514. Springer International Publishing, Cham (2017)
- Fiat, A., and Naor, M.: Broadcast Encryption. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 480–491. Springer, Heidelberg (1993). DOI: 10.1007/3-540-48329-2 40
- Fischlin, M.: Completely non-malleable schemes. In: Automata, Languages and Programming: 32nd International Colloquium, ICALP 2005, Lisbon, Portugal, July 11-15, 2005. Proceedings 32, pp. 779–790 (2005). DOI: 10.1007/11523468 63
- Ge, A., and Wei, P.: Identity-Based Broadcast Encryption with Efficient Revocation.
 In: Lin, D., and Sako, K. (eds.) PKC 2019, Part I. LNCS, vol. 11442, pp. 405–435.
 Springer, Heidelberg (2019). DOI: 10.1007/978-3-030-17253-4 14
- Gegier, K.: On Novel Constructions of Dual Receiver Key Encapsulation Mechanisms Based on Deterministic Encryption. MA thesis, Karlsruhe Institute of Technology (KIT) (2020).
- 32. Herzog, J., Liskov, M., and Micali, S.: Plaintext Awareness Via Key Registration. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 548–564. Springer, Heidelberg (2003). DOI: 10.1007/978-3-540-45146-4 32
- Jinman, Z., and Qin, C.: Hierarchical Identity-Based Broadcast Encryption Scheme on Lattices. In: 2011 Seventh International Conference on Computational Intelligence and Security, pp. 944–948. IEEE (2011). DOI: 10.1109/CIS.2011.212
- 34. Justesen, J.: Class of constructive asymptotically good algebraic codes. IEEE Transactions on Information Theory 18(5), 652–656 (1972). DOI: 10.1109/TIT.1972. 1054893
- 35. Kiltz, E., Masny, D., and Pietrzak, K.: Simple Chosen-Ciphertext Security from Low-Noise LPN. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 1–18. Springer, Heidelberg (2014). DOI: 10.1007/978-3-642-54631-0 1
- 36. Libert, B., Paterson, K.G., and Quaglia, E.A.: Anonymous Broadcast Encryption: Adaptive Security and Efficient Constructions in the Standard Model. In: Fischlin, M., Buchmann, J., and Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 206–224. Springer, Heidelberg (2012). DOI: 10.1007/978-3-642-30057-8_13
- 37. Liu, Y., Zhang, D., Deng, Y., and Li, B.: (Identity-based) Dual Receiver Encryption from Lattice-Based Programmable Hash Functions with High Min-Entropy. Cybersecurity 2(1), 1–15 (2019). DOI: 10.1186/s42400-019-0034-y
- 38. Liu, Y., Wang, L., Shen, X., and Li, L.: New Constructions of Identity-Based Dual Receiver Encryption from Lattices. Entropy 22(6) (2020). DOI: 10.3390/e22060599
- Ma, F., and Zhandry, M.: Encryptor Combiners: A Unified Approach to Multiparty NIKE, (H)IBE, and Broadcast Encryption, Cryptology ePrint Archive, Report 2017/152. (2017). https://eprint.iacr.org/2017/152

- 40. Mambo, M., and Okamoto, E.: Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 80(1), 54–63 (1997)
- 41. Meier, S., Schmidt, B., Cremers, C., and Basin, D.: The TAMARIN Prover for the Symbolic Analysis of Security Protocols. In: Sharygina, N., and Veith, H. (eds.) DAV 13. LNCS, vol. 8044, pp. 696–701. Springer, Heidelberg (2013). DOI: 10.1007/978-3-642-39799-8 48
- Micciancio, D., and Peikert, C.: Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In: Pointcheval, D., and Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). DOI: 10.1007/978-3-642-29011-4
- 43. Müller, M.: On the Applicability of Dual-Receiver Encryption in a Post-Quantum World. MA thesis, Karlsruhe Institute of Technology (KIT) (2021).
- 44. Noh, G., Hong, D., Kwon, J.O., and Jeong, I.R.: A Strong Binding Encryption Scheme from Lattices for Secret Broadcast. IEEE communications letters 16(6), 781–784 (2012). DOI: 10.1109/LCOMM.2012.041112.112495
- 45. Patil, S.M., and BR, P.: DR-PRE: Dual Receiver Proxy Re-Encryption Scheme. Information Security Journal: A Global Perspective 29(2), 62–72 (2020). DOI: 10.1080/19393555.2020.1715515
- Rosen, A., and Segev, G.: Chosen-Ciphertext Security via Correlated Products. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 419–436. Springer, Heidelberg (2009). DOI: 10.1007/978-3-642-00457-5 25
- Suzuki, K., and Yoneyama, K.: Exposure-Resilient One-Round Tripartite Key Exchange Without Random Oracles. In: Jacobson Jr., M.J., Locasto, M.E., Mohassel, P., and Safavi-Naini, R. (eds.) ACNS 13. LNCS, vol. 7954, pp. 458–474. Springer, Heidelberg (2013). DOI: 10.1007/978-3-642-38980-1 29
- 48. Unger, N., and Goldberg, I.: Improved Strongly Deniable Authenticated Key Exchanges for Secure Messaging. PoPETs 2018(1), 21–66 (2018). DOI: 10.1515/popets-2018-0003
- Wang, J., and Bi, J.: Lattice-Based Identity-Based Broadcast Encryption, IACR ePrint Archive, Report 2010/288. (2010). https://eprint.iacr.org/2010/288
- 50. Wong, C.K., Gouda, M., and Lam, S.S.: Secure Group Communications Using Key Graphs. IEEE/ACM Transactions on Networking 8(1), 16–30 (2000). DOI: 10.1109/90.836475
- 51. Yamada, S.: Adaptively Secure Identity-Based Encryption from Lattices with Asymptotically Shorter Public Parameters. In: Fischlin, M., and Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 32–62. Springer, Heidelberg (2016). DOI: 10.1007/978-3-662-49896-5 2
- 52. Yang, C., Zheng, S., Wang, L., Lu, X., and Yang, Y.: Hierarchical Identity-Based Broadcast Encryption Scheme from LWE. Journal of Communications and Networks 16(3), 258–263 (2014). DOI: 10.1109/JCN.2014.000045
- 53. Yang, G., Tan, C.H., Huang, Q., and Wong, D.S.: Probabilistic Public-Key Encryption with Equality Test. In: Pieprzyk, J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 119–131. Springer, Heidelberg (2010). DOI: 10.1007/978-3-642-11925-5_9
- 54. Zhang, D., Zhang, K., Li, B., Lu, X., Xue, H., and Li, J.: Lattice-Based Dual Receiver Encryption and More. In: ACISP 18. LNCS, vol. 1172. Springer, Heidelberg (2018). DOI: 10.1007/978-3-319-93638-3_30
- 55. Zhang, J., Yu, Y., Fan, S., and Zhang, Z.: Improved Lattice-Based CCA2-Secure PKE in the Standard Model. Science China Information Sciences 63(182101), 1–22 (2020). DOI: 10.1007/s11432-019-9861-3

A Soundness Attack on the DRE scheme of Liu et al. [37]

Here, we describe a soundness attack on the scheme of Liu et al. [37]. The basic setup for this scheme is similar to the constructions of Section 4.1, but the ciphertext $\mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1)$ is constructed as follows:

$$\mathbf{c}_0 = \mathbf{D}^{\top} \mathbf{s} + \mathbf{e}_0 + \lceil q/2 \rceil \mathbf{m} \in \mathbb{Z}_q^n$$

$$\mathbf{c}_1 = \begin{pmatrix} \mathbf{c}_1^0 \\ \mathbf{c}_1^R \\ \mathbf{c}_1^S \end{pmatrix} = \begin{bmatrix} \mathbf{A}^{\top} \\ (\mathbf{A}^{id_R})^{\top} \\ (\mathbf{A}^{id_S})^{\top} \end{bmatrix} \mathbf{s} + \begin{pmatrix} \mathbf{e}_1^0 \\ \mathbf{e}_1^R \\ \mathbf{e}_1^S \end{pmatrix} \in \mathbb{Z}_q^{3m}.$$

The vectors \mathbf{e}_0 , \mathbf{e}_1^0 , \mathbf{e}_1^R , \mathbf{e}_1^S are LWE errors and the LWE-matrix \mathbf{D} which is part of the public parameters is used to disguise the message. The LWE-matrix \mathbf{A} is also part of the public parameters, whereas the matrices \mathbf{A}^{id_R} , \mathbf{A}^{id_S} arise from the identities id_R and id_S .

Decryption is possible due to the secret keys $sk^{id_i} = \mathbf{E}^{id_i}$ satisfying the equation $[\mathbf{A}|\mathbf{A}^{id_i}]\mathbf{E}^{id_i} = \mathbf{D}$ for $i \in \{R, S\}$. The message \mathbf{m} can be recovered by rounding the elements of $\mathbf{b} = \mathbf{c}_0 - (\mathbf{E}^{id_i})^{\top} \cdot \begin{bmatrix} \mathbf{c}_1^0 \\ \mathbf{c}_1^i \end{bmatrix}$ to 0 or 1.

The idea of the attack is the same as the idea of the attacks against the constructions in Section 4.1 by injecting different LWE secrets for the sender and receiver.

Indeed, an adversary can choose \mathbf{m} , \mathbf{e}_1^0 , \mathbf{e}_1^R , \mathbf{e}_1^S , $\mathbf{s}^R = \mathbf{0}$ (with appropriate dimensions) and \mathbf{s}^S such that $\mathbf{0} - (\mathbf{E}^{id_S})^{\top} \begin{bmatrix} \mathbf{0} \\ \mathbf{A}^{id_S} \cdot \mathbf{s}^S \end{bmatrix} \in \mathbb{Z}_q^{2m}$ contains an entry that is not in $[-\frac{q}{4}, \frac{q}{4}]$. This is possible due to Lemma 3 and the fact that $\mathbf{E}_2^{id_S} \mathbf{A}^{id_S}$ contains a non-zero column vector \mathbf{E}_j with overwhelming probability (for $[\mathbf{E}_1^{id_S} | \mathbf{E}_2^{id_S}] := \mathbf{E}^{id_S}$). Then the malicious ciphertext has the form

$$\begin{split} \mathbf{c}_0 &= \mathbf{D}^{\top} \mathbf{s}^R \\ \mathbf{c}_1 &= \begin{pmatrix} \mathbf{c}_1^0 \\ \mathbf{c}_1^R \\ \mathbf{c}_1^S \end{pmatrix} = \begin{bmatrix} \mathbf{A}^{\top} \cdot \mathbf{s}^R \\ (\mathbf{A}^{id_R})^{\top} \cdot \mathbf{s}^R \\ (\mathbf{A}^{id_S})^{\top} \cdot \mathbf{s}^S \end{bmatrix}. \end{split}$$

Due to the correctness of the scheme, R recovers 0^n as the message. However, we claim that S obtains 1 as the last bit of \mathbf{m} . Indeed, they calculate

$$\mathbf{b} = \mathbf{c}_0 - (\mathbf{E}^{id_S})^\top \cdot \begin{bmatrix} \mathbf{c}_1^0 \\ \mathbf{c}_1^R \end{bmatrix} = \mathbf{0} - (\mathbf{E}^{id_S})^\top \begin{bmatrix} 0 \\ (\mathbf{A}^{id_S})^\top \cdot \mathbf{s}^S \end{bmatrix}$$

in the decryption algorithm. For the j-th element of **b**, it holds that $\mathbf{b}[j] \notin [-\frac{q}{4}, \frac{q}{4})$ due to the choice of \mathbf{s}^S . Thus, S obtains 1 as j-th bit

In summary, S obtains 1 as j-th bit, while R obtaines 0 as j-th bit, and the soundness property is broken.

B Sizes of our constructions

In order to determine the size requirements in the constructions from Section 5, the following rough estimations based on common parameters that can be found in the literature are presented. The sizes of the symmetric primitives are kept out of the estimations, as the largest impact on the sizes is the public-key part of the constructions.

The following parameters determine the overall size dimensions.

- NLWE parameters
 - \circ n, m, q, α ensure the hardness of the $\mathsf{NLWE}_{n,m,q,\mathcal{D}_{\mathbb{Z},\alpha q}}$ problem.
 - $n = n(\lambda)$ is the main security parameter of the scheme.
 - $\circ q \geq 2\sqrt{n}/\alpha$ is the modulus of the scheme.
 - ∘ $m \ge n\lceil \log q \rceil + \omega(\sqrt{\log n})$ is the dimension of a lattice associated with **A**. ∘ $\bar{m} = n\lceil \log q \rceil$.
- For the LPN-based construction only n needs to be defined, as m=2n and $p=\sqrt{c/m}$ are fixed then.

For the NLWE-based construction we adopt the parameters from Frodo-1344¹⁰ as the authors use the concrete parameter estimations for the normal-form DLWE, which we reduce to as well. The parameters of the reduced LWE-instance from Frodo-1344 can be found already precomputed in the LWE-estimator repository¹¹.

For the security level 5, which corresponds to approximately 256 bits of security, the reduced NLWE instance yields the parameters $n=1344, q=2^{16}=65536, m=1344+16$, which leads to $\bar{m}=1344*16=21504$ for our construction. The resulting sizes are given in Table 1. Note that it is possible to choose the set $\{\pm 1,0\}$ as sample space for the error distribution (as stated by Micciancio and Peikert [42]), and therefore every element of the secret key can be stored within 2 bits.

Table 1. Sizes of $\Sigma_{\texttt{LWE-DRE}}$ from Figure 7 in Section 5.1

	pk for one party	sk	$ \mathbf{c} $
Generic sizes	$\lceil \log q \rceil \cdot (n \cdot (m + \bar{m}))$	$\lceil \log q \rceil \cdot (m \cdot \bar{m})$	$\lceil \log q \rceil \cdot (2 \cdot (m + \bar{m}))$
Exact sizes	61.45MB	58.49MB	91.45kB

Notice however that no optimizations were performed. So one could greatly reduce the storage costs by converting the scheme to ring or module-LWE just as the scheme of Boyen, Izabachène, and Li [11].

For the LPN construction we follow the analysis by Esser, Kübler, and May [27] that says for 256 bits of security in the low noise LPN setting we need to set n = 26500. The resulting sizes can be found in Table 2.

¹⁰ https://frodokem.org/

 $^{^{11}}$ https://github.com/malb/lattice-estimator/blob/main/estimator/schemes.py# L151

34 L. Benz et al.

Table 2. Sizes of $\Sigma_{\texttt{LPN-DRE}}$ from Figure 8 in Section 5.2.

	pk for one party	sk	$ \mathbf{c} $
Generic sizes	$2 \cdot n \cdot m$	m^2	$4 \cdot m$
Exact sizes	351.13MB	351.13MB	$26.5 \mathrm{kB}$

No optimizations where performed for this scheme either. As the secret key of our scheme is low noise, the storage requirement of the scheme could easily be reduced. We leave it open for future work to adapt the optimizations that are state of the art to both our constructions.

Also we note that the public key of the LPN-PKE by Kiltz, Masny, and Pietrzak [35] needs an extra matrix, making their public key bigger, while the ciphertext is nearly the same size thanks to the dual-receiver specific optimizations in our scheme.