




# Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model

Tsunekazu Saito<sup>(✉)</sup>, Keita Xagawa<sup>(✉)</sup> , and Takashi Yamakawa<sup>(✉)</sup>

NTT Secure Platform Laboratories, 3-9-11, Midori-cho,  
Musashino-shi, Tokyo 180-8585, Japan  
`{saito.tsunekazu,xagawa.keita,yamakawa.takashi}@lab.ntt.co.jp`

**Abstract.** Key-encapsulation mechanisms secure against chosen ciphertext attacks (IND-CCA-secure KEMs) in the quantum random oracle model have been proposed by Boneh, Dagdelen, Fischlin, Lehmann, Schafner, and Zhandry (CRYPTO 2012), Targhi and Unruh (TCC 2016-B), and Hofheinz, Hövelmanns, and Kiltz (TCC 2017). However, all are non-tight and, in particular, security levels of the schemes obtained by these constructions are less than half of original security levels of their building blocks.

In this paper, we give a conversion that tightly converts a weakly secure public-key encryption scheme into an IND-CCA-secure KEM in the quantum random oracle model. More precisely, we define a new security notion for deterministic public key encryption (DPKE) called the disjoint simulatability, and we propose a way to convert a disjoint simulatable DPKE scheme into an IND-CCA-secure key-encapsulation mechanism scheme without incurring a significant security degradation. In addition, we give DPKE schemes whose disjoint simulatability is tightly reduced to post-quantum assumptions. As a result, we obtain IND-CCA-secure KEMs tightly reduced to various post-quantum assumptions in the quantum random oracle model.

**Keywords:** Tight security · Chosen-ciphertext security  
Post-quantum cryptography · KEM

## 1 Introduction

### 1.1 Background

Indistinguishability against chosen ciphertext attacks (IND-CCA-security) is considered to be a *de facto* standard security notion of a public key encryption (PKE) and a key encapsulation mechanism (KEM). For constructing efficient IND-CCA-secure PKEs and KEMs, an idealized model called the random oracle model (ROM) [BR93] is often used. In the ROM, a hash function is idealized to be a publicly accessible oracle that simulates a truly random function. There are many known generic constructions of efficient IND-CCA-secure

PKE/KEM in the ROM; Bellare-Rogaway (BR) [BR93], OAEP [BR95, FOPS04], REACT [OP01], GEM [CHJ+02], Fujisaki-Okamoto (FO) [FO99, FO13], etc. KEM variants of these constructions were studied by Dent [Den03], which is summarized in Fig. 10 in Sect. B.

**Quantum Random Oracle Model.** Though the ROM has been widely used to heuristically analyze security of cryptographic primitives, Boneh et al. [BDF+11] pointed out that the ROM is rather problematic when considering a *quantum* adversary. The problem is that in the ROM, an adversary is only given a classical access to a random oracle. Since a random oracle is an idealization of a real hash function, a quantum adversary should be able to quantumly compute it. On the basis of this observation, they proposed a new model called the quantum random oracle model (QROM) where an adversary can quantumly access a random oracle. Since many techniques used in the ROM including adaptive programmability or extractability cannot be directly translated into the ones in the QROM, proving security in the QROM often requires different techniques from proofs in the ROM (see [BDF+11] for more details). Nonetheless, some above mentioned IND-CCA-secure PKE/KEMs in the ROM (and their variants) can be shown to also be secure in the QROM: Boneh et al. [BDF+11] proved that a variant of Bellare-Rogaway is IND-CCA-secure in the QROM. Targhi and Unruh [TU16] proposed variants of the Fujisaki-Okamoto and OAEP and proved that they are IND-CCA-secure in the QROM.

**Tight Security.** When proving the security of a primitive  $P$  under the hardness of a problem  $S$ , we usually construct a reduction algorithm  $\mathcal{R}$  that uses an adversary  $\mathcal{A}$  against the security of  $P$  as a subroutine and solves the problem  $S$ . Let  $(T, \epsilon)$  and  $(T', \epsilon')$  denote running times and success probabilities of  $\mathcal{A}$  and  $\mathcal{R}$ , respectively. We say that a reduction is tight if we have  $T' \approx T$  and  $\epsilon' \approx \epsilon$ . Tight security is desirable since it ensures that breaking the security of  $P$  is as hard as solving an underlying hard problem  $S$ . Conversely, if a security reduction is non-tight, we cannot immediately conclude that breaking the security of a primitive  $P$  is hard even if an underlying problem  $S$  is hard. For example, Menezes [Men12] shows an example of a provably secure primitive with non-tight security that is insecure with a realistic parameter setting. Therefore, tight security is important to ensure the real security of a primitive.

From that perspective, the above mentioned IND-CCA-secure PKE/KEMs in the QROM do not serve as satisfactory solutions for constructing post-quantum IND-CCA-secure PKE/KEMs because they are non-tight. To clarify this, we give more details on these results below, where  $(T, \epsilon)$  and  $(T', \epsilon')$  denote running times and success probabilities of an adversary and a reduction algorithm, respectively,  $q_H$  denotes the number of random oracle queries, and  $t_{RO}$  denotes the time needed to simulate one evaluation of a random oracle (for further explanation of  $t_{RO}$ , see Subsect. 2.2).

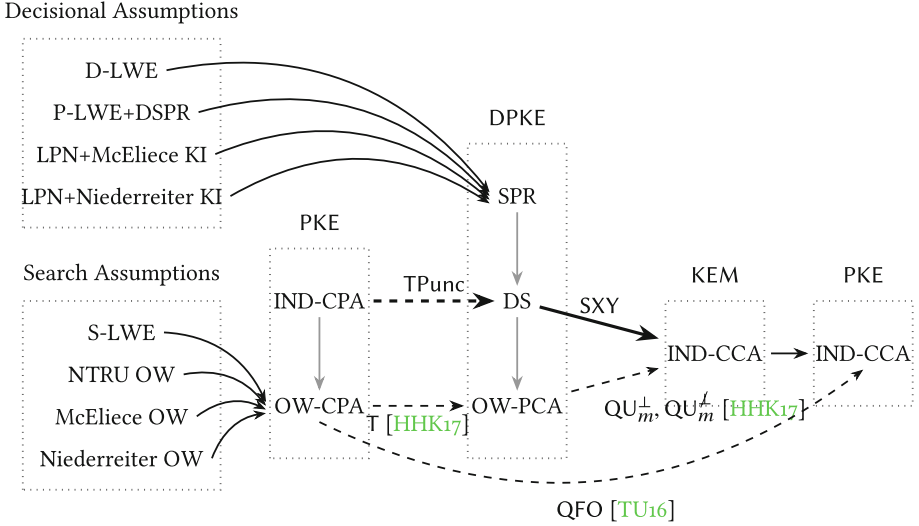
- Boneh et al. [BDF+11] proved that a KEM variant of Bellare-Rogaway based on a one-way trapdoor function is IND-CCA-secure in the QROM.<sup>1</sup> According to their security proof, we have  $T' \approx T + q_H \cdot t_F + (q_H + q_{\text{Dec}}) \cdot t_{\text{RO}}$  and  $\epsilon' \approx \epsilon^2/q_H^2$  where  $t_F$  denotes the time needed for evaluating an underlying one-way trapdoor function and  $q_{\text{Dec}}$  denotes the number of decryption queries.
- Targhi and Unruh [TU16] proposed a variant of Fujisaki-Okamoto and proved that their construction is secure in the QROM assuming OW-CPA security of an underlying PKE scheme. According to their security proof, we have  $T' \geq T + O(q_H^2)$  and  $\epsilon' \approx \epsilon^4/q_H^6$ . We note that Hofheinz et al. [HHK17] subsequently gave a modular analysis for the conversion but did not improve the tightness.
- Targhi and Unruh [TU16] proposed a variant of OAEP and proved that their construction is secure in the QROM assuming a partial domain one-way function. According to their security proof, we have  $T' \geq T + O(q_H^2)$  and  $\epsilon' \approx \epsilon^8/\text{poly}(q_H)$ .

As seen above, known constructions of IND-CCA-secure PKE/KEMs in the QROM incur at least quadratic security loss, and their security degrades rapidly as  $q_H$  grows. For example, in the Bellare-Rogaway KEM, if we start from a trapdoor function with 128-bit security (i.e.,  $\epsilon' = 2^{-128}$ ) and set  $q_H = 2^{60}$ , then the bound given by Boneh et al. [BDF+11] only ensures 4-bit security (i.e.,  $\epsilon = 2^{-4}$ ) for a resulting KEM. Conversely, if we want to ensure 128-bit security (i.e.,  $\epsilon = 2^{-128}$ ) for a resulting KEM, we have to start from a trapdoor function with 376-bit security ( $\epsilon' = 2^{-376}$ ) which incurs significant blowup of parameters. The other two constructions are even worse in regard to tightness. Therefore, to obtain an efficient construction of post-quantum IND-CCA-secure PKE/KEM, we need a construction with tighter security reduction that does not incur a quadratic security loss.

## 1.2 Our Contributions

In this paper, we give a construction of an IND-CCA-secure KEM based on a deterministic PKE (DPKE) scheme that satisfies a newly introduced security notion that we call the disjoint simulatability. Our security reduction is much tighter than those of existing constructions of IND-CCA-secure PKE schemes and does not incur quadratic security loss. By using the same notations as in the previous subsection, we have  $T' \approx T + q_H \cdot t_{\text{Enc}} + (q_H + q_{\text{Dec}}) \cdot t_{\text{RO}}$  and  $\epsilon' \approx \epsilon$  where  $t_{\text{Enc}}$  denotes a time needed for encryption of an underlying DPKE scheme. We note that  $t_{\text{Enc}}$  is a fixed polynomial of the security parameter, and thus we believe that this blowup is much less significant than the quadratic (or quartic/octic) blowup for  $\epsilon$  as in the previous constructions.

<sup>1</sup> More precisely, they proved that a hybrid encryption variant of the Bellare-Rogaway PKE scheme based on a one-way trapdoor function plus a CCA-secure symmetric-key encryption scheme is IND-CCA-secure in the QROM. Their proof is easily turned into the proof for the KEM variant of the Bellare-Rogaway conversion.



**Fig. 1.** Transformations among PKE, DPKE and KEM in the QROM: D-LWE and S-LWE denote the decisional and search learning-with-errors assumptions; P-LWE denotes the polynomial-LWE assumption; DSPR denotes the decisional small polynomial ratio assumption; LPN denotes the learning-parity-with-noise assumption; McEliece KI and Niederreiter KI denote the McEliece-key-indistinguishability and Niederreiter-key-indistinguishability assumptions, respectively; NTRU OW, McEliece OW, and Niederreiter OW denote onewayness of the NTRU, McEliece encryption, and Niederreiter encryption, respectively; OW-CPA, OW-PCA, IND-CPA, and IND-CCA denote onewayness under chosen-plaintext attacks, onewayness under plaintext-checking attacks, indistinguishability under chosen-plaintext attacks, and indistinguishability under chosen-ciphertext attacks, respectively; SPR denotes the sparse pseudorandomness; and DS denotes the disjoint simulatability. Solid arrows indicate quantum tight reductions, dashed arrows indicate quantum non-tight reductions, thin arrows indicate existing reductions, thick arrows indicate our new reductions, and gray arrows indicate trivial implications.

Moreover, we construct some DPKE schemes whose disjoint simulatabilities are tightly reduced to some post-quantum assumptions like learning with errors (LWE) and some other assumptions related to NTRU, the McEliece PKE, and the Niederreiter PKE. As a result, we obtain the first IND-CCA-secure KEMs that do not incur a quadratic security loss in the QROM based on these assumptions. We also construct a disjoint simulatable DPKE scheme from any IND-CPA-secure PKE scheme on an exponentially large message space with quadratic security loss. This gives a construction of an IND-CCA-secure KEM based on an IND-CPA-secure PKE scheme on an exponentially large message space with quadratic (rather than quartic as in previous works) security loss. Our results are summarized in Fig. 1.

We implement an instantiation based on NTRU-HRSS [HRSS17] on a desktop PC and a RasPi. Assuming that NTRU-HRSS is disjoint simulatable, the obtained KEM is CCA secure in the QROM. See Sect. 5.

### 1.3 Technical Overview

Here, we give a technical overview of our results.

**Disjoint Simulatability and Sparse Pseudorandomness.** Let  $\mathcal{D}_{\mathcal{M}}$  be a distribution over a message space  $\mathcal{M}$ . We say that a DPKE scheme is  $\mathcal{D}_{\mathcal{M}}$ -disjoint simulatable if a ciphertext of a message that is distributed according to  $\mathcal{D}_{\mathcal{M}}$  can be simulated by a simulator that does not know a message, and simulated ciphertext is invalid (i.e., out of the range of an encryption algorithm) with overwhelming probability. For an intermediate step to construct a disjoint simulatable DPKE scheme, we consider another security notion that we call sparse pseudorandomness and show that this is a sufficient condition for disjoint simulatability. We say that a DPKE scheme is  $\mathcal{D}_{\mathcal{M}}$ -sparse pseudorandom if a ciphertext of a message that is distributed according to  $\mathcal{D}_{\mathcal{M}}$  is pseudorandom and the range of an encryption algorithm is sparse in a ciphertext space. The  $\mathcal{D}_{\mathcal{M}}$ -sparse pseudorandomness implies the  $\mathcal{D}_{\mathcal{M}}$ -disjoint simulatability because if the sparse pseudorandomness is satisfied, then a simulator that simply outputs a random element of a ciphertext space suffices for the disjoint simulatability<sup>2</sup>.

**Instantiations of Disjoint Simulatable DPKE.** We construct DPKE schemes based on the concepts of the Gentry–Peikert–Vaikuntanathan (GPV) trapdoor function for LWE [GPV08], NTRU [HPS98], the McEliece PKE [McE78], and the Niederreiter PKE [Nie86] and prove that they are sparse pseudorandom (and thus disjoint simulatable) w.r.t. a certain message distribution under the LWE assumption, or other related assumptions to an underlying PKE scheme. Moreover, the reductions are tight. See Subsect. 3.3 for details of instantiations from concrete assumptions

We also construct a disjoint simulatable DPKE scheme based on any IND-CPA-secure PKE scheme with an exponentially large message space in the QROM. Unfortunately, this reduction is not tight and incurs a square security loss. See Subsect. 3.4 for details.

**Previous Construction: BR-KEM.** Before describing our construction, we review the construction and security proof of the Bellare-Rogaway KEM (BR-KEM), which was proven IND-CCA-secure in the QROM by Boneh et al. [BDF+11] because our construction is based on their idea. BR-KEM is a construction of an IND-CCA-secure KEM based on a one-way trapdoor function with an efficiently recognizable range<sup>3</sup>. For compatibility with ours, we treat a one-way trapdoor function as a perfectly correct OW-CPA-secure DPKE scheme by considering a function and an inversion to be an encryption and a

<sup>2</sup> In fact, we have to additionally assume that a ciphertext space is efficiently sampleable.

<sup>3</sup> The efficient recognizability of a range was not explicitly assumed in [BDF+11] but is actually needed for their proof.

decryption, respectively. Let  $(\text{Gen}, \text{Enc}, \text{Dec})$  denote algorithms of an underlying DPKE scheme. Then  $\text{BR-KEM} = (\text{Gen}_{\text{BR}}, \text{Enc}_{\text{BR}}, \text{Dec}_{\text{BR}})$  is described as follows:

- $\text{Gen}_{\text{BR}}$  is exactly the same as  $\text{Gen}$ .
- $\text{Enc}_{\text{BR}}$ , given a public key  $ek$  as an input, chooses a randomness  $m$  from a message space uniformly at random, computes a ciphertext  $C := \text{Enc}(ek, m)$  and a key  $K := \text{H}(m)$  where  $\text{H}$  is a hash function modeled as a random oracle, and outputs  $(C, K)$ .
- $\text{Dec}_{\text{BR}}$ , given a ciphertext  $C$  and a decryption key  $dk$  as an input, checks if  $C$  is in the valid ciphertext space and returns  $\perp$  if not. Otherwise it computes  $K := \text{H}(\text{Dec}(dk, C))$  and returns  $K$ .

In the security proof in the QROM, we first replace a random oracle  $\text{H}$  with  $\text{H}_q \circ \text{Enc}(ek, \cdot)$  where  $\text{H}_q$  is another random oracle that is not given to an adversary. Since  $\text{Enc}(ek, \cdot)$  is injective due to its perfect correctness,  $\text{H}_q \circ \text{Enc}(ek, \cdot)$  still works as a random oracle from the view of an adversary. After this replacement, we notice that a decryption oracle can be simulated by using  $\text{H}_q$  without the help of a decryption key because we have  $\text{H}(\text{Dec}(dk, c)) = \text{H}_q \circ \text{Enc}(ek, \text{Dec}(dk, c)) = \text{H}_q(c)$ . For proving IND-CCA security, we have to prove that  $\text{H}_q(c^*)$  is pseudorandom from the view of an adversary. If we were in a classical world, then this could be proven quite easily: the only way for an adversary to obtain any information of  $\text{H}_q(c^*)$  is to query  $m^*$  such that  $c^* = \text{Enc}(ek, m^*)$ , in which case the adversary breaks the OW-CPA security of an underlying DPKE scheme. In a quantum world, things do not go as easily because even if an adversary queries a quantum state whose magnitude on  $m^*$  is large, a reduction algorithm cannot notice that immediately. Nonetheless, by using the One-Way to Hiding (OW2H) lemma proven by Unruh [Unr15] (Lemma 2.1), we can show that the advantage for an adversary to distinguish  $\text{H}_q(c^*)$  from a truly random string is at most a square root of the probability that measurement of a randomly chosen adversary's query to  $\text{H}$  is equal to  $m^*$ . Hence, we can reduce the IND-CCA security of BR-KEM to the OW-CPA security of the underlying DPKE scheme with a quadratic security loss. On the other hand, to avoid the quadratic security loss, it seems that we have to avoid the usage of the OW2H lemma because the lemma inherently incurs a quadratic security loss.

**Our Conversion, SXY.** In the above proof, we used the fact that the only way for an adversary to obtain any information of  $\text{H}_q(c^*)$  is to query  $m^*$  to  $\text{H}$  such that  $c^* = \text{Enc}(ek, m^*)$ . Our key idea is based on the observation that if such  $m^*$  does not exist, i.e.,  $c^*$  is out of the range of  $\text{Enc}(ek, \cdot)$ , then it is information-theoretically impossible for an adversary to obtain any information of  $\text{H}_q(c^*)$ . Indeed, though  $c^*$  is in the range of  $\text{Enc}(ek, \cdot)$  in the real game, if we choose an encryption randomness  $m$  according to a distribution  $\mathcal{D}_{\mathcal{M}}$ , then we can replace  $c^*$  with a simulated ciphertext that is out of the range of  $\text{Enc}(ek, \cdot)$  by using the  $\mathcal{D}_{\mathcal{M}}$ -disjoint simulatability. After replacing  $c^*$  with a simulated one, we can information-theoretically bound an adversary's advantage and need not use the OW2H lemma. This seems to simply resolve the problem, and we obtain an IND-CCA-secure KEM without a quadratic security loss. However, another problem arises here: a valid ciphertext

space of a disjoint simulatable DPKE scheme is inherently not efficiently recognizable (otherwise real and simulated ciphertexts are easy to distinguish), whereas the simulation of decryption algorithm has to first verify if a given ciphertext is valid or not. To resolve the problem, we modify the decryption algorithm so that if a ciphertext is invalid, then it returns a random value rather than  $\perp$ . In the security proof of BR-KEM, a decryption oracle is simulated just by evaluating a random oracle  $H_q$  for a ciphertext, and this enables a reduction algorithm to simulate a decryption oracle for both valid and invalid ciphertexts even though it cannot determine if a given ciphertext is valid. Hence, we can reduce the IND-CCA-security of the resulting KEM without using the OW2H lemma and thus without a quadratic security loss.

Curiously, this conversion is essentially the same as  $U_m^\chi$  in [HHK17]. This means that we can remove an “additional” hash from  $QU_m^\chi$  assuming a stronger underlying DPKE in the QROM. In addition, this means that the obtained KEM is tightly secure assuming that the underlying DPKE is OW-CPA secure in the ROM as shown in [HHK17].

## 1.4 Related Work

In a concurrent and independent work, Jiang, Zhang, Chen, Wang, and Ma [JZC+17] proposed two new constructions of an IND-CCA-secure KEM based on a OW-CPA-secure PKE scheme with quadratic security loss. However, both constructions incur quadratic security loss.

## 2 Preliminaries

### 2.1 Notation

A security parameter is denoted by  $\kappa$ . We use the standard  $O$ -notations:  $O$ ,  $\Theta$ ,  $\Omega$ , and  $\omega$ . DPT and PPT stand for deterministic polynomial time and probabilistic polynomial time. A function  $f(\kappa)$  is said to be *negligible* if  $f(\kappa) = \kappa^{-\omega(1)}$ . We denote a set of negligible functions by  $\text{negl}(\kappa)$ . For two finite sets  $\mathcal{X}$  and  $\mathcal{Y}$ ,  $\text{Map}(\mathcal{X}, \mathcal{Y})$  denote a set of all functions whose domain is  $\mathcal{X}$  and codomain is  $\mathcal{Y}$ .

For a distribution  $\chi$ , we often write “ $x \leftarrow \chi$ ,” which indicates that we take a sample  $x$  from  $\chi$ . For a finite set  $S$ ,  $U(S)$  denotes the uniform distribution over  $S$ . We often write “ $x \leftarrow S$ ” instead of “ $x \leftarrow U(S)$ .” For a set  $S$  and a deterministic algorithm  $A$ ,  $A(S)$  denotes the set  $\{A(x) \mid x \in S\}$ .

If  $\text{inp}$  is a string, then “ $\text{out} \leftarrow A(\text{inp})$ ” denotes the output of algorithm  $A$  when run on input  $\text{inp}$ . If  $A$  is deterministic, then  $\text{out}$  is a fixed value and we write “ $\text{out} := A(\text{inp})$ .” We also use the notation “ $\text{out} := A(\text{inp}; r)$ ” to make the randomness  $r$  explicit.

For the Boolean statement  $P$ ,  $\text{boole}(P)$  denotes the bit that is 1 if  $P$  is true, and 0 otherwise. For example,  $\text{boole}(b' \stackrel{?}{=} b)$  is 1 if and only if  $b' = b$ .

### 2.2 Quantum Computation

We refer to [NC00] for basic of quantum computation.

**Quantum Random Oracle Model.** Roughly speaking, the quantum random oracle model (QROM) is an idealized model where a hash function is modeled as a publicly and quantumly accessible random oracle. See [BDF+11] for a more detailed description of the model.

**Lemmas.** We review some useful lemmas regarding the quantum random oracles. The first one is called the oneway-to-hiding (OW2H) lemma, which is proven by Unruh [Unr15, Lemma 6.2]. Roughly speaking, the lemma states that if any quantum adversary issuing at most  $q$  queries to a quantum random oracle  $H$  can distinguish  $(x, H(x))$  from  $(x, y)$ , where  $y$  is chosen uniformly at random, then we can find  $x$  by measuring one of the adversary's queries even it causes a quadratic security loss. The lemma of the following form is taken from [HHK17].

**Lemma 2.1 (Algorithmic Oneway to Hiding [Unr15, HHK17]).** *Let  $H : \mathcal{X} \rightarrow \mathcal{Y}$  be a quantum random oracle, and let  $\mathcal{A}$  be an adversary issuing at most  $q$  queries to  $H$  that on input  $(x, y) \in \mathcal{X} \times \mathcal{Y}$  outputs either 0/1. For all (probabilistic) algorithms  $F$  whose input space is  $\mathcal{X} \times \mathcal{Y}$  and which do not make any hash queries to  $H$ , we have*

$$\left| \Pr[\mathcal{A}^H(\text{inp}) \rightarrow 1 \mid x \leftarrow \mathcal{X}; \text{inp} \leftarrow F(x, H(x))] - \Pr[\mathcal{A}^H(\text{inp}) \rightarrow 1 \mid (x, y) \leftarrow \mathcal{X} \times \mathcal{Y}; \text{inp} \leftarrow F(x, y)] \right| \leq 2q \cdot \sqrt{\Pr[\text{EXT}^{\mathcal{A}, H}(\text{inp}) \rightarrow x \mid (x, y) \leftarrow \mathcal{X} \times \mathcal{Y}; \text{inp} \leftarrow F(x, y)]},$$

where  $\text{EXT}$  picks  $i \leftarrow \{1, \dots, q\}$ , runs  $\mathcal{A}^H(\text{inp})$  until  $i$ -th query  $|\hat{x}\rangle$  to  $H$ , and returns  $x' := \text{Measure}(|\hat{x}\rangle)$  (when  $\mathcal{A}$  makes fewer than  $i$  queries,  $\text{EXT}$  outputs  $\perp \notin \mathcal{X}$ ).

(Unruh's original statement is recovered by letting  $F$  be an identity function.)

The second one claims that a random oracle can be used as a pseudorandom function even in the quantum setting.

**Lemma 2.2.** *Let  $\ell$  be an integer. Let  $H : \{0, 1\}^\ell \times \mathcal{X} \rightarrow \mathcal{Y}$  and  $H' : \mathcal{X} \rightarrow \mathcal{Y}$  be two independent random oracles. If an unbounded time quantum adversary  $\mathcal{A}$  makes a query to  $H$  at most  $q_H$  times, then we have*

$$\left| \Pr[\mathcal{A}^{H, H(s, \cdot)}() \rightarrow 1 \mid s \leftarrow \{0, 1\}^\ell] - \Pr[\mathcal{A}^{H, H'}() \rightarrow 1] \right| \leq q_H \cdot 2^{-\frac{\ell+1}{2}}$$

where all oracle accesses of  $\mathcal{A}$  can be quantum.

Though this seems to be a folklore, we give a proof of this lemma in Sect. C for completeness.<sup>4</sup>

**Simulation of Random Oracle.** In the original quantum random oracle model introduced by Boneh et al. [BDF+11], they do not allow a reduction algorithm to access a random oracle, so it has to simulate a random oracle by itself. In contrast, in this paper, we give a random oracle access to a reduction algorithm. We remark that this is just a convention and not a modification of the model since we can simulate a random oracle against quantum adversaries in several ways.

<sup>4</sup> Jiang et al. [JZC+17] also gave a proof of an essentially identical lemma.



1. The first way is a simulation by a  $2q$ -wise independent hash function, where  $q$  denotes the number of random oracle queries by an adversary, as introduced by Zhandry [Zha12b]. The simulation is perfect, that is, no adversary can distinguish the real QRO from the simulated one. A drawback of this simulation is a  $O(q^2)$  blowup for a running time of a reduction algorithm since it has to compute a  $2q$ -wise independent hash function for each random oracle query.
2. The second way is a simulation by a quantumly secure PRF as used in [BDF+11]. If we use this simulation, then the blowup of a running time of a reduction algorithm is  $O(q \cdot t_{\text{PRF}})$  where  $t_{\text{PRF}}$  is the time needed for evaluating a PRF, which is usually much smaller than  $O(q^2)$ . However, we have to additionally assume the existence of a quantumly secure PRF, which is known to exist if a quantumly secure one-way function exists [Zha12a].
3. The third way is a simulation by a real hash function like SHA-2 and to think that this is a “random oracle.” Since we adopt the QROM, we idealize a real hash function as a random oracle in the construction of primitives. Thus, it may be natural to assume the same thing even in a *reduction*, that is, the reduction algorithm implements the random oracle by a concrete hash function. If we use this simulation, then the blowup of a running time of a reduction algorithm is  $O(q \cdot t_{\text{hash}})$  where  $t_{\text{hash}}$  denotes a time to evaluate a hash function. This gives a tightest reduction at the expense of additional idealization of a hash function. We note that a similar convention is also used by Kiltz et al. [KLS17]. We finally note that this way strengthens the assumption, that is, we need to assume that some problem is hard *in the QROM*.

We use  $t_{\text{RO}}$  to denote a time needed to simulate a random oracle. We have  $t_{\text{RO}} = O(q)$ ,  $t_{\text{PRF}}$ , or  $t_{\text{hash}}$ , if we use the first, second, or third way, respectively. We note that in the proof of quantum variants of Fujisaki-Okamoto and OAEP [TU16, HHK17], we have to simulate a random oracle in the 1st way, because a simulator has to “invert” a random oracle in a simulation.

### 2.3 Public-Key Encryption

The model for PKE schemes is summarized as follows:

**Definition 2.1.** A PKE scheme PKE consists of the following triple of polynomial-time algorithms (Gen, Enc, Dec).

- $\text{Gen}(1^\kappa; r_g) \rightarrow (ek, dk)$ : a key-generation algorithm that on input  $1^\kappa$ , where  $\kappa$  is the security parameter, outputs a pair of keys  $(ek, dk)$ .  $ek$  and  $dk$  are called the encryption key and decryption key, respectively.
- $\text{Enc}(ek, m; r_e) \rightarrow c$ : an encryption algorithm that takes as input encryption key  $ek$  and message  $m \in \mathcal{M}$  and outputs ciphertext  $c \in \mathcal{C}$ .
- $\text{Dec}(dk, c) \rightarrow m/\perp$ : a decryption algorithm that takes as input decryption key  $dk$  and ciphertext  $c$  and outputs message  $m \in \mathcal{M}$  or a rejection symbol  $\perp \notin \mathcal{M}$ .

**Definition 2.2.** We say a PKE scheme PKE is deterministic if Enc is deterministic. DPKE stands for deterministic public key encryption.

**Definition 2.3 (Correctness).** We say  $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$  has perfect correctness if for any  $(ek, dk)$  generated by  $\text{Gen}$  and for any  $m \in \mathcal{M}$ , we have that

$$\Pr[\text{Dec}(dk, c) = m \mid c \leftarrow \text{Enc}(ek, m)] = 1.$$

An additional property,  $\gamma$ -spread, is in Sect. A

*Security:* Here, we define onewayness under chosen-plaintext attacks (OW-CPA), indistinguishability under chosen-plaintext attacks (IND-CPA), and indistinguishability under chosen-ciphertext attacks (IND-CCA) for a PKE.

**Definition 2.4 (Security notions for PKE).** For any adversary  $\mathcal{A}$ , we define its OW-CPA, IND-CPA, and IND-CCA advantages against a PKE scheme  $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$  as follows:

$$\begin{aligned} \text{Adv}_{\mathcal{A}, \text{PKE}}^{\text{ow-cpa}}(\kappa) &:= \Pr[\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ow-cpa}}(\kappa) = 1], \\ \text{Adv}_{\text{PKE}, \mathcal{A}}^{\text{ind-cpa}}(\kappa) &:= \left| 2 \Pr[\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ind-cpa}}(\kappa) = 1] - 1 \right|, \\ \text{Adv}_{\text{PKE}, \mathcal{A}}^{\text{ind-cca}}(\kappa) &:= \left| 2 \Pr[\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ind-cca}}(\kappa) = 1] - 1 \right|, \end{aligned}$$

where  $\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ow-cpa}}(\kappa)$ ,  $\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ind-cpa}}(\kappa)$ , and  $\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ind-cca}}(\kappa)$  are experiments described in Fig. 2. For  $\text{GOAL-ATK} \in \{\text{OW-CPA}, \text{IND-CPA}, \text{IND-CCA}\}$ , we say that PKE is GOAL-ATK-secure if  $\text{Adv}_{\mathcal{A}, \text{PKE}}^{\text{goal-atk}}(\kappa)$  is negligible for any PPT adversary  $\mathcal{A}$ .

Additional definitions are in Sect. A

$\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ow-cpa}}(\kappa)$	$\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ind-cpa}}(\kappa)$	$\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ind-cca}}(\kappa)$
$(ek, dk) \leftarrow \text{Gen}(1^\kappa)$	$b \leftarrow \{0, 1\}$	$b \leftarrow \{0, 1\}$
$m^* \leftarrow \mathcal{M}$	$(ek, dk) \leftarrow \text{Gen}(1^\kappa)$	$(ek, dk) \leftarrow \text{Gen}(1^\kappa)$
$c^* \leftarrow \text{Enc}(ek, m^*)$	$(m_0, m_1, st) \leftarrow \mathcal{A}_1(ek)$	$(m_0, m_1, st) \leftarrow \mathcal{A}_1^{\text{DEC}_\perp(\cdot)}(ek)$
$m' \leftarrow \mathcal{A}(ek, c^*)$	$c^* \leftarrow \text{Enc}(ek, m_b)$	$c^* \leftarrow \text{Enc}(ek, m_b)$
<b>return</b> $\text{boole}(m' \stackrel{?}{=} \text{Dec}(dk, c^*))$	$b' \leftarrow \mathcal{A}_2(c^*, st)$	$b' \leftarrow \mathcal{A}_2^{\text{DEC}_{c^*}(\cdot)}(c^*, st)$
	<b>return</b> $\text{boole}(b' \stackrel{?}{=} b)$	<b>return</b> $\text{boole}(b' \stackrel{?}{=} b)$
		$\text{DEC}_a(c)$
		if $c = a$ , return $\perp$
		$m := \text{Dec}(dk, c)$
		<b>return</b> $m$

**Fig. 2.** Games for PKE schemes

### 2.4 Key Encapsulation

The model for KEM schemes is summarized as follows:

**Definition 2.5.** A KEM scheme  $\text{KEM}$  consists of the following triple of polynomial-time algorithms  $(\text{Gen}, \text{Encaps}, \text{Decaps})$ :

- $\text{Gen}(1^\kappa; r_g) \rightarrow (ek, dk)$ : a key-generation algorithm that on input  $1^\kappa$ , where  $\kappa$  is the security parameter, outputs a pair of keys  $(ek, dk)$ .  $ek$  and  $dk$  are called the encapsulation key and decapsulation key, respectively.
- $\text{Encaps}(ek; r_e) \rightarrow (c, K)$ : an encapsulation algorithm that takes as input encapsulation key  $ek$  and outputs ciphertext  $c \in \mathcal{C}$  and key  $K \in \mathcal{K}$ .
- $\text{Decaps}(dk, c) \rightarrow K/\perp$ : a decapsulation algorithm that takes as input decapsulation key  $dk$  and ciphertext  $c$  and outputs key  $K$  or a rejection symbol  $\perp \notin \mathcal{K}$ .

**Definition 2.6 (Correctness).** We say  $\text{KEM} = (\text{Gen}, \text{Encaps}, \text{Decaps})$  has perfect correctness if for any  $(ek, dk)$  generated by  $\text{Gen}$ , we have that

$$\Pr[\text{Decaps}(dk, c) = K : (c, K) \leftarrow \text{Encaps}(ek)] = 1.$$

*Security:* We define indistinguishability under chosen-plaintext and chosen-ciphertext attacks (denoted by IND-CPA and IND-CCA) for KEM, respectively.

**Definition 2.7.** For any adversary  $\mathcal{A}$ , we define its IND-CPA and IND-CCA advantages against a KEM scheme  $\text{KEM} = (\text{Gen}, \text{Encaps}, \text{Decaps})$  as follows:

$$\text{Adv}_{\text{KEM}, \mathcal{A}}^{\text{ind-cpa}}(\kappa) := \left| 2 \Pr[\text{Expt}_{\text{KEM}, \mathcal{A}}^{\text{ind-cpa}}(\kappa) = 1] - 1 \right|,$$

$$\text{Adv}_{\text{KEM}, \mathcal{A}}^{\text{ind-cca}}(\kappa) := \left| 2 \Pr[\text{Expt}_{\text{KEM}, \mathcal{A}}^{\text{ind-cca}}(\kappa) = 1] - 1 \right|,$$

where  $\text{Expt}_{\text{KEM}, \mathcal{A}}^{\text{ind-cpa}}(\kappa)$  and  $\text{Expt}_{\text{KEM}, \mathcal{A}}^{\text{ind-cca}}(\kappa)$  are experiments described in Fig. 3.

$\text{Expt}_{\text{KEM}, \mathcal{A}}^{\text{ind-cpa}}(\kappa)$	$\text{Expt}_{\text{KEM}, \mathcal{A}}^{\text{ind-cca}}(\kappa)$	$\text{DEC}_{c^*}(c)$
$b \leftarrow \{0, 1\}$	$b \leftarrow \{0, 1\}$	if $c = c^*$ , return $\perp$
$(ek, dk) \leftarrow \text{Gen}(1^\kappa)$	$(ek, dk) \leftarrow \text{Gen}(1^\kappa)$	$K := \text{Decaps}(dk, c)$
$(c^*, K_0^*) \leftarrow \text{Encaps}(ek)$ ;	$(c^*, K_0^*) \leftarrow \text{Encaps}(ek)$ ;	<b>return</b> $K$
$K_1^* \leftarrow \mathcal{K}$	$K_1^* \leftarrow \mathcal{K}$	
$b' \leftarrow \mathcal{A}(ek, c^*, K_b^*)$	$b' \leftarrow \mathcal{A}^{\text{DEC}_{c^*}(\cdot)}(ek, c^*, K_b^*)$	
<b>return</b> $\text{boole}(b' \stackrel{?}{=} b)$	<b>return</b> $\text{boole}(b' \stackrel{?}{=} b)$	

**Fig. 3.** Games for KEM schemes

For  $\text{ATK} \in \{\text{CPA}, \text{CCA}\}$ , we say that  $\text{KEM}$  is  $\text{IND-ATK-secure}$  if  $\text{Adv}_{\mathcal{A}, \text{PKE}}^{\text{ind-atk}}(\kappa)$  is negligible for any PPT adversary  $\mathcal{A}$ .

## 2.5 eXtendable-Output Functions

An eXtendable-Output Function (XOF) is a function on input bit strings in which the output can be extended to an arbitrary desired length. An XOF is denoted by  $\text{XOF}(X, L)$ , where  $X$  is the input bit string and  $L$  is the desired output length. We modeled the XOF as a quantumly-accessible random oracle. We employ SHAKE256, standardized as an XOF by NIST [NIS15].

## 2.6 Assumptions

*Preliminaries:* Let  $\rho_s(x) = \exp(-\pi\|x\|^2/s^2)$  for  $x \in \mathbb{R}^n$  be a Gaussian function scaled by a factor  $s$ . For any real  $s > 0$  and lattice  $\Lambda$ , we define the discrete Gaussian distribution  $D_{\Lambda, s}$  over  $\Lambda$  with parameter  $s$  by

$$D_{\Lambda, s}(x) = \rho_s(x) / \rho_s(\Lambda) \text{ for } x \in \Lambda,$$

where  $\rho_s(\Lambda) = \sum_{x \in \Lambda} \rho_s(x)$ . The following norm bound is useful.

**Lemma 2.3 (Adapted version of [MR07, Lemma 4.4]).** For  $\sigma = \omega(\sqrt{\log(n)})$ , it holds that

$$\Pr_{e \leftarrow D_{\mathbb{Z}^n, \sigma}} [\|e\| > \sigma\sqrt{n}] \leq 2^{-n+1}.$$

*LWE and its variants:* We review the assumptions for lattice-based PKEs. The most basic one is the learning-with-errors (LWE) assumption [Reg09], which is a generalized version of the learning-parity-with-noise assumption [BFKL93, KSS10].

**Definition 2.8 (LWE assumption in matrix form).** For all  $\kappa$ , let  $n = n(\kappa)$  and  $q = q(\kappa)$  be integers and let  $\chi$  be a distribution over  $\mathbb{Z}$ .

The decisional learning-with-errors (LWE) assumption  $\text{LWE}_{n, q}$  states that, for any  $m = \text{poly}(\kappa)$ ,

the following two distributions are computationally hard to distinguish:

- $A, sA + e$ , where  $A \leftarrow \mathbb{Z}_q^{n \times m}$ ,  $s \leftarrow \mathbb{Z}_q^n$ , and  $e \leftarrow \chi^m$
- $A, u$ , where  $A \leftarrow \mathbb{Z}_q^{n \times m}$  and  $u \leftarrow \mathbb{Z}_q^m$ .

We also review its polynomial version [LPR10, BV11]. We here use the Hermite-normal form of the assumption [ACPS09, LPR10, BV11], where secret  $s$  is chosen from the noise distribution.

**Definition 2.9 (Poly-LWE assumption – Hermite normal form).** For all  $\kappa$ , let  $\Phi(x) = \Phi_\kappa(x) \in \mathbb{Z}[x]$  be a polynomial of degree  $n = n(\kappa)$ , let  $q = q(\kappa)$  be an integer, let  $R := \mathbb{Z}[x]/(\Phi(x))$  and  $R_q := \mathbb{Z}_q[x]/(\Phi(x))$ , and let  $\chi$  denote a distribution over the ring  $R$ .

The decisional polynomial learning-with-errors (Poly-LWE) assumption  $\text{PolyLWE}_{\Phi, q, \chi}$  states that, for any  $\ell = \text{poly}(\kappa)$ , the following two distributions are hard to distinguish:

- $\{(a_i, a_i s + e_i)\}_{i=1, \dots, \ell}$ , where  $a_i \leftarrow R_q, s, e_i \leftarrow \chi$
- $\{(a_i, u_i)\}_{i=1, \dots, \ell}$ , where  $a_i, u_i \leftarrow R_q$ .

Next, we recall the decisional small polynomial ratio (DSPR) assumption defined by López-Alt, Tromer, and Vaikuntanathan [LTV12]. We here employ an adapted version of the DSPR assumption.

**Definition 2.10 (DSPR assumption).** For all  $\kappa$ , let  $\Phi(x) = \Phi_\kappa(x) \in \mathbb{Z}[x]$  be a polynomial of degree  $n = n(\kappa)$ , let  $q = q(\kappa)$  be a positive integer, let  $R := \mathbb{Z}[x]/(\Phi(x))$  and  $R_q := \mathbb{Z}_q[x]/(\Phi(x))$ , and let  $\chi$  denote a distribution over the ring  $R$ .

The decisional small polynomial ratio (DSPR) assumption  $\text{DSPR}_{\Phi, q, \chi_g, \chi_f}$  says that the following two distributions are hard to distinguish:

- a polynomial  $h := g \cdot f^{-1} \in R_q$ , where  $g \leftarrow \chi_g$  and  $f \leftarrow \chi_f$ .
- a polynomial  $u \leftarrow R_q$ .

*Remark 2.1.* Stehlé and Steinfeld [SS11] showed that  $\text{DSPR}_{\Phi, q, \chi}$  is statistically hard if  $n$  is a power of two,  $\Phi(x) = x^n + 1$ , and  $\chi_g = \chi_f = D_{\mathbb{Z}^n, r}$  for  $r > \sqrt{q} \cdot \text{poly}(\kappa)$ .

### 3 Disjoint Simulatability of Deterministic PKE

Here, we define a new security notion, *disjoint simulatability*, for DPKE. We also define another security notion called *sparse pseudorandomness* and prove that it implies the disjoint simulatability. Then we give some instantiations of sparse pseudorandom (and thus disjoint simulatable) deterministic PKE schemes based on the LWE assumption or various assumptions related to NTRU, the McEliece PKE, and the Niederreiter PKE with tight reductions. We also construct a disjoint simulatable DPKE scheme from any IND-CPA-secure PKE scheme with a sufficiently large message space in the QROM, though the reduction is non-tight.

#### 3.1 Definition

We define a new security notion, *disjoint simulatability*, for DPKE. Intuitively, a deterministic PKE scheme is disjoint simulatable if there exists a simulator that is only given a public key and generates a “fake ciphertext” that is indistinguishable from a real ciphertext of a random message. Moreover, we require that a fake ciphertext falls in a valid ciphertext space with negligible probability. The formal definition is as follows.

**Definition 3.1 (Disjoint simulatability).** Let  $\mathcal{D}_{\mathcal{M}}$  denote an efficiently sampleable distribution on a set  $\mathcal{M}$ . A deterministic PKE scheme  $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$  with plaintext and ciphertext spaces  $\mathcal{M}$  and  $\mathcal{C}$  is  $\mathcal{D}_{\mathcal{M}}$ -disjoint simulatable if there exists a PPT algorithm  $\mathcal{S}$  that satisfies the following.

- (Statistical disjointness:)

$$\text{Disj}_{\text{PKE}, \mathcal{S}}(\kappa) := \max_{(ek, dk) \in \text{Gen}(1^\kappa; \mathcal{R})} \Pr[c \in \text{Enc}(ek, \mathcal{M}) \mid c \leftarrow \mathcal{S}(ek)]$$

is negligible, where  $\mathcal{R}$  denotes a randomness space for  $\text{Gen}$ .

- (Ciphertext-indistinguishability:) For any PPT adversary  $\mathcal{A}$ ,

$$\text{Adv}_{\text{PKE}, \mathcal{D}_{\mathcal{M}}, \mathcal{A}, \mathcal{S}}^{\text{ds-ind}}(\kappa) := \left| \Pr \left[ \mathcal{A}(ek, c^*) \rightarrow 1 \mid \begin{array}{l} (ek, dk) \leftarrow \text{Gen}(1^\kappa); m^* \leftarrow \mathcal{D}_{\mathcal{M}}; \\ c^* := \text{Enc}(ek, m^*) \end{array} \right] - \Pr \left[ \mathcal{A}(ek, c^*) \rightarrow 1 \mid (ek, dk) \leftarrow \text{Gen}(1^\kappa); c^* \leftarrow \mathcal{S}(ek) \right] \right|$$

is negligible.

### 3.2 Sufficient Condition: Sparse Pseudorandomness

Here, we define another security notion for DPKE called *sparse pseudorandomness*, which is a sufficient condition to be disjoint simulatable. Intuitively, a deterministic PKE scheme is sparse pseudorandom if valid ciphertexts are sparse in a ciphertext space and pseudorandom when a message is randomly chosen. In other words, an encryption algorithm can be seen as a pseudorandom generator (PRG). The formal definition is as follows.

**Definition 3.2 (Sparse pseudorandomness).** Let  $\mathcal{D}_{\mathcal{M}}$  denote an efficiently sampleable distribution on a set  $\mathcal{M}$ . A deterministic PKE scheme  $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$  with plaintext and ciphertext spaces  $\mathcal{M}$  and  $\mathcal{C}$  is  $\mathcal{D}_{\mathcal{M}}$ -sparse pseudorandom if the following two properties are satisfied.

- (Sparseness:)

$$\text{Sparse}_{\text{PKE}}(\kappa) := \max_{(ek, dk) \in \text{Gen}(1^\kappa; \mathcal{R})} \frac{|\text{Enc}(ek, \mathcal{M})|}{|\mathcal{C}|}$$

is negligible where  $\mathcal{R}$  denotes a randomness space for  $\text{Gen}$ .

- (Pseudorandomness:) For any PPT adversary  $\mathcal{A}$ ,

$$\text{Adv}_{\text{PKE}, \mathcal{D}_{\mathcal{M}}, \mathcal{A}}^{\text{pr}}(\kappa) := \left| \Pr \left[ \mathcal{A}(ek, c^*) \rightarrow 1 \mid \begin{array}{l} (ek, dk) \leftarrow \text{Gen}(1^\kappa); m^* \leftarrow \mathcal{D}_{\mathcal{M}}; \\ c^* := \text{Enc}(ek, m^*) \end{array} \right] - \Pr \left[ \mathcal{A}(ek, c^*) \rightarrow 1 \mid (ek, dk) \leftarrow \text{Gen}(1^\kappa), c^* \leftarrow \mathcal{C} \right] \right|$$

is negligible.

Then we prove that the sparse pseudorandomness implies the disjoint simulatability if a ciphertext space is efficiently sampleable.

**Lemma 3.1.** *If a deterministic PKE scheme  $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$  with plaintext and ciphertext spaces  $\mathcal{M}$  and  $\mathcal{C}$  is  $\mathcal{D}_{\mathcal{M}}$ -sparse pseudorandom and  $\mathcal{C}$  is efficiently sampleable, then PKE is also  $\mathcal{D}_{\mathcal{M}}$ -disjoint simulatable. In particular, there exists a PPT simulator  $\mathcal{S}$  such that  $\text{Disj}_{\text{PKE}, \mathcal{S}}(\kappa) = \text{Sparse}_{\text{PKE}}(\kappa)$  and  $\text{Adv}_{\text{PKE}, \mathcal{D}_{\mathcal{M}}, \mathcal{A}, \mathcal{S}}^{\text{ds-ind}}(\kappa) = \text{Adv}_{\text{PKE}, \mathcal{D}_{\mathcal{M}}, \mathcal{A}}^{\text{pr}}(\kappa)$ .*

*Proof.* Let  $\mathcal{S}$  be an algorithm that outputs a random element of  $\mathcal{C}$ . Then we clearly have  $\text{Disj}_{\text{PKE}, \mathcal{S}}(\kappa) = \text{Sparse}_{\text{PKE}}(\kappa)$  and  $\text{Adv}_{\text{PKE}, \mathcal{D}_{\mathcal{M}}, \mathcal{A}, \mathcal{S}}^{\text{ds-ind}}(\kappa) = \text{Adv}_{\text{PKE}, \mathcal{D}_{\mathcal{M}}, \mathcal{A}}^{\text{pr}}(\kappa)$ .  $\square$

### 3.3 Instantiations

Here, we give examples of a DPKE scheme that is disjoint simulatable. In particular, we construct a DPKE scheme that has the sparse pseudorandomness based on the LWE assumption or some other assumptions related to NTRU. (We further construct them based on the McEliece PKE and the Niederreiter PKE in the full version.) We remark that the reductions are tight. By combining those with Lemma 3.1, we obtain disjoint simulatable DPKE schemes based on any of these assumptions with tight security.

**LWE-based DPKE.** We review the GPV trapdoor function for LWE [GPV08, Pei09, MP12]. The LWE assumption (in matrix form) states that  $(A, sA + e)$  and  $(A, u)$  are computationally indistinguishable, where  $A \leftarrow \mathbb{Z}_q^{n \times m}$ ,  $s \leftarrow \mathbb{Z}_q^n$ ,  $e \leftarrow \chi^m$ , and  $u \leftarrow \mathbb{Z}_q^m$ . The GPV trapdoor function for LWE exploited that if we have a “short” matrix  $T$  satisfying  $AT \equiv O \pmod q$ , we can retrieve  $s$  and  $e$  from  $c = sA + e$ . The trapdoor  $T$  for  $A$  is generated by an algorithm  $\text{TrapGen}$ :

**Theorem 3.1** ([Ajt99, AP11]). *For any positive integers  $n$  and  $q \geq 3$ , any  $\delta > 0$  and  $m \geq (2 + \delta)n \lg q$ , there is a probabilistic polynomial-time algorithm  $\text{TrapGen}$  that outputs a pair  $T \in \mathbb{Z}^{m \times m}$  and  $A \in \mathbb{Z}_q^{n \times m}$  such that: the distribution of  $A$  is within a negligible statistical distance of uniform over  $\mathbb{Z}_q^{n \times m}$ ,  $T$  is non-singular (over the rationals),  $\|t_i\| \leq L = O(m \lg m)$  for every column vector  $t_i$  of  $T$ , and  $AT \equiv O \pmod q$ .*

Let us construct a DPKE scheme  $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$  as follows:

**Parameters:** We require several parameters: the dimension  $n = n(\kappa)$ , the modulus  $q = q(\kappa)$ , and  $m = m(\kappa)$ . We also employ  $L = O(m \lg m)$ ,  $\sigma = \omega(\sqrt{\lg n})$ ,  $\beta = \sigma\sqrt{n}$ .

We require that  $\beta L < q/2$  and  $q^m \gg q^n \cdot (2\beta + 1)^m$ .

- The plaintext space  $\mathcal{M} := \mathbb{Z}_q^n \times B_m(\beta)$ , where  $B_m(\beta) := \{e \in \mathbb{Z}^m \mid \|e\| \leq \beta\}$ .
- The sampler  $\mathcal{D}_{\mathcal{M}}$  samples  $s \leftarrow \mathbb{Z}_q^n$  and  $e \leftarrow D_{\mathbb{Z}^m, \sigma}$  conditioned on  $\|e\| \leq \beta$ .
- The ciphertext space  $\mathcal{C} := \mathbb{Z}_q^m$

**Key Generation:**  $\text{Gen}(1^\kappa)$  invokes  $\text{TrapGen}(1^n, 1^m, q)$  and obtains  $A \in \mathbb{Z}_q^{n \times m}$  and  $T \in \mathbb{Z}^{m \times m}$ . It outputs  $ek = A$  and  $dk = (A, T)$ .

**Encryption:**  $\text{Enc}(ek, (s, e))$  outputs  $c = sA + e \bmod q$ .

**Decryption:**  $\text{Dec}(dk, c)$  computes  $e = (c \cdot T \bmod q) \cdot T^{-1}$  and  $s = (c - e) \cdot A^+ \bmod q$ , where  $A^+ := A^\top \cdot (A \cdot A^\top) \in \mathbb{Z}_q^{m \times n}$ , the left inverse of  $A$ .

The properties of PKE are summarized as follows:

**Perfect Correctness:** We know  $c \cdot T \equiv sAT + eT \equiv eT \pmod{q}$ . If  $\|eT\|_\infty < q/2$ , then  $c \cdot T \bmod q = eT \in \mathbb{Z}^m$  holds and  $e$  is recovered by  $e = (c \cdot T \bmod q) \cdot T^{-1}$ . Once correct  $e$  is obtained,  $s$  is recovered by  $(c - e) \cdot A^+ \in \mathbb{Z}_q^n$ . The condition  $\|eT\|_\infty < q/2$  is satisfied because  $\|eT\|_\infty \leq \max_i \|e\| \cdot \|t_i\| \leq \beta L < q/2$ , where  $t_i$  is the column vectors of  $T$ .

**Sparseness:**  $|\mathcal{C}| = q^m$  and  $|\text{Enc}(ek, \mathcal{M})| \leq \mathcal{M} = |\mathbb{Z}_q^n \times B_m(\beta)| \leq q^n \cdot (2\beta + 1)^m$ . Sparseness follows from the fact  $q^m \gg q^n \cdot (2\beta + 1)^m$ .

**Pseudorandomness:** We consider the following hybrid games:

- (Original game 1:) The adversary is given  $(A, c^*)$ , where  $(A, T) \leftarrow \text{TrapGen}(1^n, 1^m, q)$ ,  $(s, e) \leftarrow \mathcal{D}_\mathcal{M}$ , and  $c^* \leftarrow \mathbb{Z}_q^m$ .
- (Hybrid game 1:) Let us replace the public key  $A$ . We consider  $(A, c^*)$ , where  $A \leftarrow \mathbb{Z}_q^{n \times m}$ ,  $(s, e) \leftarrow \mathcal{D}_\mathcal{M}$ , and  $c^* := sA + e \bmod q$ . This change is justified by Theorem 3.1.
- (Hybrid game 2:) Let us replace the sampler  $\mathcal{D}_\mathcal{M}$ . We consider  $(A, c^*)$ , where  $A \leftarrow \mathbb{Z}_q^{n \times m}$ ,  $(s, e) \leftarrow U(\mathbb{Z}_q^n) \times D_{\mathbb{Z}^m, \sigma}$ , and  $c^* := sA + e \bmod q$ . This replacement is justified by Lemma 2.3.
- (Hybrid game 3:) We next replace the ciphertext  $c^*$ . We consider  $(A, c^*)$ , where  $A \leftarrow \mathbb{Z}_q^{n \times m}$  and  $c^* \leftarrow \mathbb{Z}_q^m$ . This game is computationally indistinguishable from the previous game under the LWE assumption  $\text{LWE}_{n, q, D_{\mathbb{Z}, \sigma}}$ .
- (Original game 2:) We replace the public key  $A$ . We consider  $(A, c^*)$ , where  $(A, T) \leftarrow \text{TrapGen}(1^n, 1^m, q)$  and  $c^* := sA + e \bmod q$ . This change is justified by Theorem 3.1.

*Remark 3.1.* For simplicity, we employ the simple version of the GPV trapdoor function for LWE. Further improvements are available, e.g., [MP12, Section 5].

**NTRU-based DPKE.** We next review the original version of NTRUEncrypt [HPS98]. Let  $\Phi(x) = x^n - 1 \in \mathbb{Z}[x]$ , let  $p < q$  be positive integers with  $\gcd(p, q) = 1$ , and let  $R := \mathbb{Z}[x]/(\Phi(x))$  and  $R_q := \mathbb{Z}_q[x]/(\Phi(x))$ . We often set  $p = 3$  and  $q = 2^k$  for some  $k$ . Let  $\mathcal{T}$  be a set of ternary-coefficient polynomials in  $R$ , that is,  $\mathcal{T} := \{t = \sum_{i=0}^{n-1} t_i x^i \in R \mid t_i \in \{-1, 0, +1\}\}$ . Let  $\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_r, \mathcal{L}_m \subseteq \mathcal{T}$ . The public key is  $h = g/f$ , where  $f \leftarrow \mathcal{L}_f, g \leftarrow \mathcal{L}_g$  with  $f$  has inverses in  $R_p$  and  $R_q$ . The ciphertext of  $m \in \mathcal{L}_m$  with randomness  $r \in \mathcal{L}_r$  is  $c = prh + m$ . Roughly speaking, we can retrieve  $m$  if we know  $f$ ;  $cf = prg + mf \in R_q$  and it holds in  $R$ .

**Parameters:** We require that  $\|prg + mf \bmod q\|_\infty < q/2$  for any  $g, f, m, r$  in their domains, where, for  $t = \sum_{i=0}^{n-1} t_i x^i \in R$ , we define  $\|t\|_\infty := \max_i |t_i|$ . For simplicity, we assume that  $\mathcal{L}_m = \mathcal{L}_r$ .

- The plaintext space is  $\mathcal{M} := \mathcal{L}_m \times \mathcal{L}_r$ .



- The sampler  $\mathcal{D}_{\mathcal{M}}$  samples  $(m, r) \leftarrow \mathcal{L}_m \times \mathcal{L}_r$ .
- The ciphertext space is  $\mathcal{C} := R_q$ .

**Key Generation:**  $\text{Gen}()$  chooses  $g \leftarrow \mathcal{L}_g$  and  $f \leftarrow \mathcal{L}_f$  until  $f$  is invertible in  $R_q$  and  $R_p$ . It outputs  $ek = h = g/f \in R_q$  and  $dk = (h, f)$ .

**Encryption:**  $\text{Enc}(ek, (m, r))$  outputs  $c = prh + m \in R_q$ .

**Decryption:**  $\text{Dec}(sk, c)$  computes  $m := (fc \bmod q) \cdot f^{-1} \bmod p$  and  $r := (c - m) \cdot (ph)^{-1} \bmod q$ .

The properties of this DPKE are summarized as follows:

**Perfect correctness:** Note that  $fc \equiv prg + mf \pmod{q}$ . Since  $\|prg + mf \bmod q\|_\infty < q/2$  from our requirement, we have  $(fc \bmod q) = prg + mf \in R$ . Hence, we have  $(fc \bmod q) \cdot f^{-1} \equiv (prg + mf) \cdot f^{-1} \equiv m \pmod{p}$  as we wanted.  $r$  is also recovered because  $(c - m) \cdot (ph)^{-1} \equiv prh \cdot (ph)^{-1} \equiv r \pmod{q}$ .

**Sparseness:** Sparseness follows from  $|\mathcal{C}| = q^n \gg 3^{2n} = |\mathcal{T}^2| \geq |\mathcal{L}_m \times \mathcal{L}_r| = |\text{Enc}(ek, \mathcal{M})|$ .

**Pseudorandomness:** What we want to show is

$$(h, c = prh + m) \approx_c (h, u),$$

where  $h = g/f$  is a public key with  $f \leftarrow \mathcal{L}_f, g \leftarrow \mathcal{L}_g$  with condition  $f$  has inverses  $R_p$  and  $R_q$ ,  $(m, r) \leftarrow \mathcal{L}_m \times \mathcal{L}_r$ , and  $u \leftarrow R_q$ . Let  $\chi_g := U(\mathcal{L}_g)$  and  $\chi_f := U(\mathcal{L}_f \cap R_p^* \cap R_q^*)$ , where  $R_k^*$  for  $k \in \{p, q\}$  denotes  $\{f \in R \mid f \text{ has an inverse in } R_k\}$ . Let  $\chi := U(\mathcal{L}_m) = U(\mathcal{L}_r)$ .

- We first replace  $h = g/f$  with random  $h'$ , which is justified by the DSPR assumption  $\text{DSPR}_{\Phi, q, \chi_f, \chi_g}$ .
- We next replace  $c = prh' + m$  with random  $c'$ , which is justified by the Poly-LWE assumption  $\text{PolyLWE}_{\Phi, q, \chi}$ ; Given  $\tilde{h}$  and  $c = r\tilde{h} + m$  or random, we convert them into  $h' = p^{-1}\tilde{h}$  and  $c$ . Since  $p$  is co-prime to  $q$ ,  $h'$  is truly random. If  $c = r\tilde{h} + e$ , then  $c = pr \cdot p^{-1}\tilde{h} + e = prh' + e$  as we wanted.
- We then go backward by replacing random  $h'$  with  $h = g/f$ , which is justified by the DSPR assumption  $\text{DSPR}_{\Phi, q, \chi_f, \chi_g}$  again.

### 3.4 Generic Conversion from IND-CPA-Secure PKE

Here, we show that any perfectly-correct IND-CPA-secure PKE whose plaintext space is sufficiently large can be converted into a disjoint-simulatable DPKE scheme in the quantum random oracle model. We note that the conversion is *non-tight*.

Intuitively, we replace randomness of an underlying IND-CPA-secure PKE scheme with a hash value of a message similarly to the conversion  $\mathbb{T}$  given in [HHK17] (which is in turn based on the Fujisaki-Okamoto conversion). The difference from the conversion  $\mathbb{T}$  is that we “puncture” a message space by  $0^5$ . That is, if a message space of an underlying IND-CPA-secure PKE scheme is  $\mathcal{M}$ , then

<sup>5</sup> We assume that  $0 \in \mathcal{M}$ . In fact, we can replace  $0$  with an arbitrary message in  $\mathcal{M}$ . We assume that  $0 \in \mathcal{M}$  for notational simplicity.

$\text{Gen}_1(1^\kappa)$	$\text{Enc}_1(ek, m)$ , where $m \in \mathcal{M}'$	$\text{Dec}_1(dk, c)$
$(ek, dk) \leftarrow \text{Gen}(1^\kappa)$	$r := \text{G}(m)$	$m := \text{Dec}(dk, c)$
<b>return</b> $(ek, dk)$	$c := \text{Enc}(ek, m; r)$	<b>if</b> $m \notin \mathcal{M}'$ <b>return</b> $\perp$
	<b>return</b> $c$	<b>else return</b> $m$
$\mathcal{S}(ek)$		
$r \leftarrow \mathcal{R}$		
$c := \text{Enc}(ek, 0; r)$		
<b>return</b> $c$		

**Fig. 4.**  $\text{PKE}_1 = (\text{Gen}_1, \text{Enc}_1, \text{Dec}_1) = \text{TPunc}[\text{PKE}, \text{G}]$  with simulator  $\mathcal{S}$ .

a message space of the resulting scheme is  $\mathcal{M}' := \mathcal{M} \setminus \{0\}$ . In this meaning, we call our conversion  $\text{TPunc}$ . We give the concrete description of the conversion  $\text{TPunc}$  below.

Let  $\mathcal{M}$  and  $\mathcal{R}$  be the message and randomness spaces of  $\text{PKE}$ , respectively, and let  $\mathcal{M}' := \mathcal{M} \setminus \{0\}$ . Then the resulting DPKE scheme  $\text{PKE}_1 = \text{TPunc}[\text{PKE}, \text{G}]$  is described in Fig. 4 where  $\text{G}: \mathcal{M} \rightarrow \mathcal{R}$  denotes a random oracle. Here, we remark that the message space of  $\text{PKE}_1$  is restricted to  $\mathcal{M}' := \mathcal{M} \setminus \{0\}$ . The security of  $\text{PKE}_1$  is stated as follows.

**Theorem 3.2 (Security of  $\text{TPunc}$ ).** *Let  $\mathcal{S}$  be the algorithm described in Fig. 4. If  $\text{PKE}$  is perfectly correct, then we have  $\text{Disj}_{\text{PKE}_1, \mathcal{S}}(\kappa) = 0$ . Moreover, for any quantum adversary  $\mathcal{A}$  against  $\text{PKE}_1$  issuing at most  $q_{\text{G}}$  quantum queries to  $\text{G}$ , there exist quantum adversaries  $\mathcal{B}$  and  $\mathcal{C}$  against IND-CPA security of  $\text{PKE}$  such that*

$$\text{Adv}_{\text{PKE}_1, U_{\mathcal{M}'}, \mathcal{A}, \mathcal{S}}^{\text{ds-ind}}(\kappa) \leq 2q_{\text{G}} \sqrt{\text{Adv}_{\text{PKE}, \mathcal{B}}^{\text{ind-cpa}}(\kappa) + \frac{2}{|\mathcal{M}'|} + \text{Adv}_{\text{PKE}, \mathcal{C}}^{\text{ind-cpa}}(\kappa)}$$

where  $U_{\mathcal{M}'}$  denotes the uniform distribution on  $\mathcal{M}'$ , and  $\text{Time}(\mathcal{B}) \approx \text{Time}(\mathcal{C}) \approx \text{Time}(\mathcal{A}) + q_{\text{G}} \cdot t_{\text{RO}}$ .

**Security Proof.** We obviously have  $\text{Disj}_{\text{PKE}_1, \mathcal{S}}(\kappa) = 0$  since  $\text{PKE}$  is perfectly correct.

To prove the rest of the theorem, we consider the following sequence of games. See Table 1 for the summary of games and justifications.

**Game<sub>0</sub>:** This game is defined as follows:

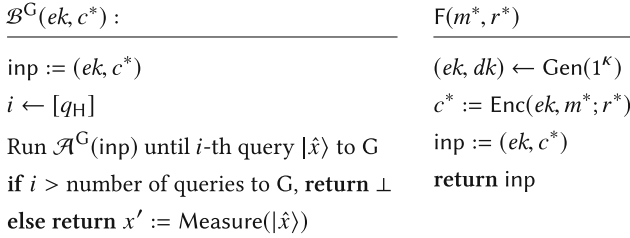
$$\begin{aligned} (ek, dk) &\leftarrow \text{Gen}(1^\kappa); m^* \leftarrow \mathcal{M}'; r^* \leftarrow \text{G}(m^*); c^* := \text{Enc}(ek, m^*; r^*); \\ b' &\leftarrow \mathcal{A}^{\text{G}(\cdot)}(ek, c^*); \text{return } b'. \end{aligned}$$

**Game<sub>1</sub>:** This game is the same as **Game<sub>0</sub>** except that a randomness to generate a challenge ciphertext is freshly generated:

$$\begin{aligned} (ek, dk) &\leftarrow \text{Gen}(1^\kappa); m^* \leftarrow \mathcal{M}'; r^* \leftarrow \mathcal{R}; c^* := \text{Enc}(ek, m^*; r^*); \\ b' &\leftarrow \mathcal{A}^{\text{G}(\cdot)}(ek, c^*); \text{return } b'. \end{aligned}$$

**Table 1.** Summary of games for the security proof of Theorem 3.2

Game	$m^*$	$r^*$	$c^*$	Justification
Game <sub>0</sub>	$\mathcal{M}'$	$G(m^*)$	$\text{Enc}(ek, m^*; r^*) = \text{Enc}_1(ek, m^*)$	
Game <sub>1</sub>	$\mathcal{M}'$	$r^*$	$\text{Enc}(ek, m^*; r^*)$	OW-CPA security of PKE and the OW2H lemma
Game <sub>2</sub>	0	$r^*$	$\text{Enc}(ek, 0; r^*) = \mathcal{S}(ek)$	IND-CPA security of PKE



**Fig. 5.** Adversary  $\mathcal{B}$  and Algorithm F

Game<sub>2</sub>: This game is the same as Game<sub>1</sub> except that a challenge ciphertext is generated by  $\text{Enc}(ek, m^*, r^*)$ , where  $m^* := 0$  rather than  $m^* \leftarrow \mathcal{M}'$ :

$(ek, dk) \leftarrow \text{Gen}(1^\kappa); r^* \leftarrow \mathcal{R}; c^* := \text{Enc}(ek, 0; r^*); b' \leftarrow \mathcal{A}^{G(\cdot)}(ek, c^*); \text{return } b'$ .

This completes the descriptions of games. It is easy to see that we have

$$\text{Adv}_{\text{PKE}_{1,U,\mathcal{M}',\mathcal{A},\mathcal{S}}}^{\text{ds-ind}}(\kappa) = |\text{Pr}[\text{Game}_0 = 1] - \text{Pr}[\text{Game}_2 = 1]|.$$

We give an upperbound for this by the following lemmas.

**Lemma 3.2.** *There exists an adversary  $\mathcal{B}$  such that*

$$|\text{Pr}[\text{Game}_0 = 1] - \text{Pr}[\text{Game}_1 = 1]| \leq 2q_G \sqrt{\text{Adv}_{\text{PKE}_{\mathcal{B}}}^{\text{ind-cpa}}(\kappa) + \frac{2}{|\mathcal{M}|}}$$

and  $\text{Time}(\mathcal{B}) \approx \text{Time}(\mathcal{A}) + q_G \cdot t_{\text{RO}}$ .

*Proof.* Let F be an algorithm described in Fig. 5. It is easy to see that Game<sub>0</sub> can be restated as

$m^* \leftarrow \mathcal{M}'; r^* \leftarrow G(m^*); \text{inp} := F(ek, m^*; r^*); b' \leftarrow \mathcal{A}^{G(\cdot)}(\text{inp}); \text{return } b'$ .

and Game<sub>1</sub> can be restated as

$m^* \leftarrow \mathcal{M}'; r^* \leftarrow \mathcal{R}; \text{inp} := F(ek, m^*; r^*); b' \leftarrow \mathcal{A}^{G(\cdot)}(\text{inp}); \text{return } b'$ .

Then applying the Algorithmic-OW2H lemma (Lemma 2.1) with  $\mathcal{X} = \mathcal{M}'$ ,  $\mathcal{Y} = \mathcal{R}$ ,  $x = m^*$ ,  $y = r^*$ , and algorithms  $\mathcal{A}$  and  $F$ , we have

$$|\Pr[\text{Game}_0 = 1] - \Pr[\text{Game}_1 = 1]| \leq 2q_G \sqrt{\Pr[m^* \leftarrow \mathcal{B}^G(ek, c^*)]}.$$

where  $\mathcal{B}^G$  is an algorithm described in Fig. 5,  $(ek, dk) \leftarrow \text{Gen}(1^\kappa)$ ,  $m^* \leftarrow \mathcal{M}'$ ,  $r^* \leftarrow \mathcal{R}$ , and  $c^* := \text{Enc}(ek, m^*, r^*)$ . Since the statistical distance between uniform distributions on  $\mathcal{M}$  and  $\mathcal{M}'$  is  $\frac{1}{|\mathcal{M}|}$ , we have  $\Pr[m^* \leftarrow \mathcal{B}^G(ek, c^*)] \leq \text{Adv}_{\text{PKE}, \mathcal{B}}^{\text{ow-cpa}}(\kappa) + \frac{1}{|\mathcal{M}|}$  where the probability in the left-hand side is taken as in the above. (Note that additional  $\frac{1}{|\mathcal{M}|}$  appears because  $m^*$  is taken from  $\mathcal{M}' = \mathcal{M} \setminus \{0\}$  in the left-hand side probability.) Moreover, we have  $\text{Adv}_{\text{PKE}, \mathcal{B}}^{\text{ow-cpa}}(\kappa) \leq \text{Adv}_{\text{PKE}, \mathcal{B}}^{\text{ind-cpa}}(\kappa) + \frac{1}{|\mathcal{M}|}$  in general. By combining these inequalities, the lemma is proven.  $\square$

**Lemma 3.3.** *There exists an adversary  $\mathcal{C}$  such that  $|\Pr[\text{Game}_1 = 1] - \Pr[\text{Game}_2 = 1]| \leq \text{Adv}_{\text{PKE}, \mathcal{C}}^{\text{ind-cpa}}(\kappa)$  and  $\text{Time}(\mathcal{C}) \approx \text{Time}(\mathcal{A}) + q_G \cdot t_{\text{RO}}$ .*

*Proof.* We construct an adversary  $\mathcal{C}$  against the IND-CPA security of PKE as follows.

$\mathcal{C}^G(ek)$ : It chooses  $m_0 \leftarrow \mathcal{M}'$  and sets  $m_1 := 0$ . Then it queries  $(m_0, m_1)$  to its challenge oracle and obtains  $c^* \leftarrow \text{Enc}(ek, m^*; r^*)$ , where  $m^*$  is  $m_b$  for a random bit  $b$  chosen by the challenger. It invokes  $b' \leftarrow \mathcal{A}^G(ek, c^*)$  and outputs  $b'$ .

This completes the description of  $\mathcal{C}$ . It is obvious that  $\mathcal{C}$  perfectly simulates  $\text{Game}_{b+1}$  depending on the challenge bit  $b \in \{0, 1\}$ . Therefore, we have

$$\begin{aligned} \text{Adv}_{\text{PKE}, \mathcal{C}}^{\text{ind-cpa}}(\kappa) &= |2 \Pr[b' = b] - 1| \\ &= |(1 - \Pr[b' = 1 \mid b = 0]) + \Pr[b' = 1 \mid b = 1] - 1| \\ &= |1 - \Pr[\text{Game}_1 = 1] + \Pr[\text{Game}_2 = 1] - 1| \\ &= |\Pr[\text{Game}_2 = 1] - \Pr[\text{Game}_1 = 1]| \end{aligned}$$

as we wanted.  $\square$

## 4 Conversion from Disjoint Simulatability to IND-CCA

In this section, we convert a disjoint simulatable DPKE scheme into an IND-CCA-secure KEM. Let  $\text{PKE}_1 = (\text{Gen}_1, \text{Enc}_1, \text{Dec}_1)$  be a deterministic PKE scheme and let  $H: \mathcal{M} \rightarrow \mathcal{K}$  and  $H': \{0, 1\}^\ell \times \mathcal{C} \rightarrow \mathcal{K}$  be random oracles. Our conversion SXY is described in Fig. 6. The securities of our conversion can be stated as follows.

**Theorem 4.1 (Security of SXY in the ROM (an adapted version of [HHK17, Theorem 3.6])).** *Let  $\text{PKE}_1$  be a perfectly correct DPKE scheme.*

$\overline{\text{Gen}}(1^\kappa)$	$\overline{\text{Enc}}(ek')$	$\overline{\text{Dec}}(dk, c)$ , where $dk = (dk', ek', s)$
$(ek', dk') \leftarrow \text{Gen}_1(1^\kappa)$	$m \leftarrow \mathcal{D}_{\mathcal{M}}$	$m := \text{Dec}_1(dk', c)$
$s \leftarrow \{0, 1\}^\ell$	$c := \text{Enc}_1(ek', m)$	if $m = \perp$ , <b>return</b> $K := H'(s, c)$
$dk \leftarrow (dk', ek', s)$	$K := H(m)$	if $c \neq \text{Enc}_1(ek', m)$ , <b>return</b> $K := H'(s, c)$
<b>return</b> $(ek', dk)$	<b>return</b> $(K, c)$	<b>else return</b> $K := H(m)$

**Fig. 6.**  $\text{KEM} := \text{SXY}[\text{PKE}_1, H, H']$ .

For any IND-CCA adversary  $\mathcal{A}$  against KEM issuing  $q_H$  and  $q_{H'}$  quantum random oracle queries to  $H$  and  $H'$  and  $q_{\overline{\text{Dec}}}$  decryption queries, there exists an OW-CPA adversary  $\mathcal{B}$  against  $\text{PKE}_1$ , such that

$$\text{Adv}_{\text{KEM}, \mathcal{A}}^{\text{ind-cca}}(\kappa) \leq \text{Adv}_{\text{PKE}_1, \mathcal{B}}^{\text{ow-cpa}}(\kappa) + q_{H'} \cdot 2^{-\ell}$$

and  $\text{Time}(\mathcal{B}) \approx \text{Time}(\mathcal{A}) + q_H \cdot \text{Time}(\text{Enc}_1) + (q_H + q_{H'} + q_{\overline{\text{Dec}}}) \cdot t_{\text{CRO}}$ , where  $t_{\text{CRO}}$  is the running time to simulate the classical random oracle.

**Theorem 4.2 (Security of SXY in the QROM).** Let  $\text{PKE}_1$  be a perfectly correct DPKE scheme that satisfies the  $\mathcal{D}_{\mathcal{M}}$ -disjoint simulatability with a simulator  $\mathcal{S}$ . For any IND-CCA quantum adversary  $\mathcal{A}$  against KEM issuing  $q_H$  and  $q_{H'}$  quantum random oracle queries to  $H$  and  $H'$  and  $q_{\overline{\text{Dec}}}$  decryption queries, there exists an adversary  $\mathcal{B}$  against the disjoint simulatability of  $\text{PKE}_1$  such that

$$\text{Adv}_{\text{KEM}, \mathcal{A}}^{\text{ind-cca}}(\kappa) \leq \text{Adv}_{\text{PKE}_1, \mathcal{D}_{\mathcal{M}}, \mathcal{S}, \mathcal{B}}^{\text{ds-ind}}(\kappa) + \text{Disj}_{\text{PKE}_1, \mathcal{S}}(\kappa) + q_{H'} \cdot 2^{-\frac{\ell+1}{2}}$$

and  $\text{Time}(\mathcal{B}) \approx \text{Time}(\mathcal{A}) + q_H \cdot \text{Time}(\text{Enc}_1) + (q_H + q_{H'} + q_{\overline{\text{Dec}}}) \cdot t_{\text{RO}}$ .

The proof of Theorem 4.2 follows.

*Remark 4.1.* We also note that our reduction enables the decapsulation oracle  $\overline{\text{Dec}}$  to quantumly queried.

**Security Proof.** We use game-hopping proof. The overview of all games is given in Table 2.

**Game<sub>0</sub>:** This is the original game,  $\text{Expt}_{\text{KEM}, \mathcal{A}}^{\text{ind-cca}}(\kappa)$ .

**Game<sub>1</sub>:** This game is the same as **Game<sub>0</sub>** except that  $H'(s, c)$  in the decryption oracle is replaced with  $H_q(c)$  where  $H_q : \mathcal{C} \rightarrow \mathcal{K}$  is another random oracle. We remark that  $\mathcal{A}$  is not given direct access to  $H_q$ .

**Game<sub>1.5</sub>:** This game is the same as **Game<sub>1</sub>** except that the random oracle  $H(\cdot)$  is simulated by  $H'_q(\text{Enc}_1(ek, \cdot))$  where  $H'_q$  is yet another random oracle. We remark that a decryption oracle and generation of  $K_0^*$  also use  $H'_q(\text{Enc}_1(ek, \cdot))$  as  $H(\cdot)$  and that  $\mathcal{A}$  is not given direct access to  $H'_q$ .

**Game<sub>2</sub>:** This game is the same as **Game<sub>1.5</sub>** except that the random oracle  $H(\cdot)$  is simulated by  $H_q(\text{Enc}_1(ek, \cdot))$  instead of  $H'_q(\text{Enc}_1(ek, \cdot))$ . We remark that a decryption oracle and generation of  $K_0^*$  also use  $H_q(\text{Enc}_1(ek, \cdot))$  as  $H(\cdot)$ .

**Table 2.** Summary of games for the proof of Theorem 4.2

Game	H	$c^*$	$K_0^*$	$K_1^*$	Decryption of		Justification
					valid $c$	invalid $c$	
Game <sub>0</sub>	H( $\cdot$ )	Enc <sub>1</sub> ( $ek', m^*$ )	H( $m^*$ )	random	H( $m$ )	H'(s, c)	
Game <sub>1</sub>	H( $\cdot$ )	Enc <sub>1</sub> ( $ek', m^*$ )	H( $m^*$ )	random	H( $m$ )	H <sub>q</sub> (c)	Lemma 2.2
Game <sub>1.5</sub>	H' <sub>q</sub> (Enc <sub>1</sub> ( $ek', \cdot$ ))	Enc <sub>1</sub> ( $ek', m^*$ )	H( $m^*$ )	random	H( $m$ )	H <sub>q</sub> (c)	Perfect correctness
Game <sub>2</sub>	H <sub>q</sub> (Enc <sub>1</sub> ( $ek', \cdot$ ))	Enc <sub>1</sub> ( $ek', m^*$ )	H( $m^*$ )	random	H( $m$ )	H <sub>q</sub> (c)	Conceptual
Game <sub>3</sub>	H <sub>q</sub> (Enc <sub>1</sub> ( $ek', \cdot$ ))	Enc <sub>1</sub> ( $ek', m^*$ )	H <sub>q</sub> ( $c^*$ )	random	H <sub>q</sub> (c)	H <sub>q</sub> (c)	Perfect correctness
Game <sub>4</sub>	H <sub>q</sub> (Enc <sub>1</sub> ( $ek', \cdot$ ))	$\mathcal{S}(ek')$	H <sub>q</sub> ( $c^*$ )	random	H <sub>q</sub> (c)	H <sub>q</sub> (c)	DS-IND

Game<sub>3</sub>: This game is the same as Game<sub>2</sub> except that  $K_0^*$  is set as  $H_q(c^*)$  and the decryption oracle always returns  $H_q(c)$  as long as  $c \neq c^*$ . We denote the modified decryption oracle by  $\overline{\text{Dec}}'$ .

Game<sub>4</sub>: This game is the same as Game<sub>3</sub> except that  $c^*$  is set as  $\mathcal{S}(ek')$ .

The above completes the descriptions of games. We clearly have

$$\text{Adv}_{\text{KEM}, \mathcal{A}}^{\text{ind-cca}}(\kappa) = |2 \Pr[\text{Game}_0 = 1] - 1|$$

by the definition. We upperbound this by the following lemmas.

**Lemma 4.1.** *We have*

$$|\Pr[\text{Game}_0 = 1] - \Pr[\text{Game}_1 = 1]| \leq q_H \cdot 2^{-\frac{\ell+1}{2}}.$$

*Proof.* This is obvious from Lemma 2.2. □

**Lemma 4.2.** *We have*

$$\Pr[\text{Game}_1 = 1] = \Pr[\text{Game}_{1.5} = 1].$$

*Proof.* Since we assume that PKE<sub>1</sub> has a perfect correctness, Enc<sub>1</sub>( $ek', \cdot$ ) is injective. Therefore, if H'<sub>q</sub>( $\cdot$ ) is a random function, then H'<sub>q</sub>(Enc<sub>1</sub>( $ek, \cdot$ )) is also a random function. Remarking that access to H'<sub>q</sub> is not given to  $\mathcal{A}$ , it causes no difference from the view of  $\mathcal{A}$  if we replace H( $\cdot$ ) with H'<sub>q</sub>(Enc<sub>1</sub>( $ek, \cdot$ )). □

**Lemma 4.3.** *We have*

$$\Pr[\text{Game}_{1.5} = 1] = \Pr[\text{Game}_2 = 1].$$

*Proof.* We call a ciphertext  $c$  valid if we have Enc<sub>1</sub>( $ek', \text{Dec}_1(dk', c)$ ) =  $c$  and invalid otherwise. We remark that H<sub>q</sub> is used only for decrypting an invalid ciphertext  $c$  as H<sub>q</sub>( $c$ ) in Game<sub>1.5</sub>. This means that a value of H<sub>q</sub>( $c$ ) for a valid  $c$  is not used at all in Game<sub>1.5</sub>. On the other hand, any output of Enc<sub>1</sub>( $ek', \cdot$ ) is valid due to the perfect correctness of PKE<sub>1</sub>. Since H'<sub>q</sub> is only used for evaluating an output of Enc( $ek', \cdot$ ), a value of H<sub>q</sub>( $c$ ) for a valid  $c$  is not used at all in Game<sub>1.5</sub>. Hence, it causes no difference from the view of  $\mathcal{A}$  if we use the same random oracle H<sub>q</sub> instead of two independent random oracles H<sub>q</sub> and H'<sub>q</sub>. □

**Lemma 4.4.** *We have*

$$\Pr[\text{Game}_2 = 1] = \Pr[\text{Game}_3 = 1].$$

*Proof.* Since we set  $H(\cdot) := H_q(\text{Enc}_1(ek', \cdot))$ , for any valid  $c$  and  $m := \text{Dec}_1(dk', c)$ , we have  $H(m) = H_q(\text{Enc}_1(ek', m)) = H_q(c)$ . Therefore, responses of the decryption oracle are unchanged. We also have  $H(m^*) = H_q(c^*)$  for a similar reason.  $\square$

**Lemma 4.5.** *There exists an adversary  $\mathcal{B}$  such that*

$$|\Pr[\text{Game}_3 = 1] - \Pr[\text{Game}_4 = 1]| \leq \text{Adv}_{\text{PKE}_1, \mathcal{D}_{\mathcal{M}}, \mathcal{S}, \mathcal{B}}^{\text{ds-ind}}(\kappa).$$

and  $\text{Time}(\mathcal{B}) \approx \text{Time}(\mathcal{A}) + q_H \cdot \text{Time}(\text{Enc}_1) + (q_H + q_{H'} + q_{\overline{\text{Dec}}}) \cdot t_{\text{RO}}$ .

*Proof.* We construct an adversary  $\mathcal{B}$ , which is allowed to access two random oracles  $H_q$  and  $H'$ , against the disjoint simulatability as follows<sup>6</sup>.

$\mathcal{B}^{H_q, H'}(ek', c^*)$  : It picks  $b \leftarrow \{0, 1\}$ , sets  $K_0^* := H_q(c^*)$  and  $K_1^* \leftarrow \mathcal{K}$ , and invokes  $b' \leftarrow \mathcal{A}^{H, H', \overline{\text{Dec}}'}(ek', c^*, K_b^*)$  where  $\mathcal{A}$ 's oracles are simulated as follows.

- $H(\cdot)$  is simulated by  $H_q(\text{Enc}_1(ek', \cdot))$ .
- $H'$  can be simulated because  $\mathcal{B}$  has access to an oracle  $H'$ .
- $\overline{\text{Dec}}'(\cdot)$  is simulated by forwarding to  $H_q(\cdot)$ .

Then  $\mathcal{B}$  returns  $\text{boole}(b \stackrel{?}{=} b')$ .

This completes the description of  $\mathcal{B}$ . It is easy to see that  $\mathcal{B}$  perfectly simulates  $\text{Game}_3$  if  $c^* = \text{Enc}_1(ek, m^*)$  and  $\text{Game}_4$  if  $c^* = \mathcal{S}(ek')$ . Therefore, we have

$$|\Pr[\text{Game}_3 = 1] - \Pr[\text{Game}_4 = 1]| \leq \text{Adv}_{\text{PKE}_1, \mathcal{D}_{\mathcal{M}}, \mathcal{S}, \mathcal{B}}^{\text{ds-ind}}(\kappa)$$

as wanted. Since  $\mathcal{B}$  invokes  $\mathcal{A}$  once,  $H$  is simulated by one evaluation of  $\text{Enc}_1$  plus one evaluation of a random oracle, and  $H'$  and  $\overline{\text{Dec}}'$  are simulated by one evaluation of random oracles, we have  $\text{Time}(\mathcal{B}) \approx \text{Time}(\mathcal{A}) + q_H \cdot \text{Time}(\text{Enc}_1) + (q_H + q_{H'} + q_{\overline{\text{Dec}}}) \cdot t_{\text{RO}}$ .  $\square$

**Lemma 4.6.** *We have*

$$|2 \Pr[\text{Game}_4 = 1] - 1| \leq \text{Disj}_{\text{PKE}_1, \mathcal{S}}(\kappa).$$

*Proof.* Let  $\text{Bad}$  denote an event in which  $c^* \in \text{Enc}_1(ek', \mathcal{M})$  in  $\text{Game}_4$ . It is easy to see that we have

$$\Pr[\text{Bad}] \leq \text{Disj}_{\text{PKE}_1, \mathcal{S}}(\kappa).$$

When  $\text{Bad}$  does not occur, i.e.,  $c^* \notin \text{Enc}_1(ek', \mathcal{M})$ ,  $\mathcal{A}$  obtains no information about  $K_0^* = H_q(c^*)$ . This is because queries to  $H$  only reveal  $H_q(c)$  for  $c \in \text{Enc}_1(ek', \mathcal{M})$ , and  $\overline{\text{Dec}}'(c)$  returns  $\perp$  if  $c = c^*$ . Therefore, we have

$$\Pr[\text{Game}_4 = 1 \mid \overline{\text{Bad}}] = 1/2.$$

---

<sup>6</sup> We allow a reduction algorithm to access the random oracles. See Subsect. 2.2 for details.

Combining the above, we have

$$\begin{aligned}
 & |2 \Pr[\text{Game}_4 = 1] - 1| \\
 &= |\Pr[\text{Bad}] \cdot (2 \Pr[\text{Game}_4 = 1 \mid \text{Bad}] - 1) + \Pr[\overline{\text{Bad}}] \\
 &\quad \cdot (2 \Pr[\text{Game}_4 = 1 \mid \overline{\text{Bad}}] - 1)| \\
 &\leq \Pr[\text{Bad}] + |2 \Pr[\text{Game}_4 = 1 \mid \overline{\text{Bad}}] - 1| \\
 &\leq \text{Disj}_{\text{PKE}_1, \mathcal{S}}(\kappa)
 \end{aligned}$$

as we wanted. □

## 5 Implementation

We report the implementation results on a desktop PC and on a RasPi, which are based on the previous implementation of a variant of NTRU [HRSS17].

### 5.1 NTRU-HRSS

We review a variant of NTRU, which we call  $\text{NTRU}_{\text{HRSS17}}$ , developed by Hülsing, Rijneveld, Schanck, and Schwabe [HRSS17].

Let  $\Phi_m(x) \in \mathbb{Z}[x]$  be the  $m$ -th cyclotomic polynomial. We have  $\Phi_1 = x - 1$ . If  $m$  is prime, then we have  $\Phi_m = 1 + x + \dots + x^{m-1}$ . Define  $S_n := \mathbb{Z}[x]/(\Phi_n)$  and  $R_n := \mathbb{Z}[x]/(x^n - 1)$ . For prime  $n$ , we have  $x^n - 1 = \Phi_1 \Phi_n$  and  $R_n \simeq S_1 \times S_n$ . We define  $\text{Lift}_p: S_n/(p) \rightarrow R_n$  as

$$\text{Lift}_p(v) := [\Phi_1[v/\Phi_1]_{(p, \Phi_n)}]_{(x^n - 1)}.$$

By definition, we have  $\text{Lift}_p(v) \equiv 0 \pmod{\Phi_1}$  and  $\text{Lift}_p(v) \equiv v \pmod{(p, \Phi_n)}$ . Let  $\mathfrak{p} = (p, \Phi_n)$  and  $\mathfrak{q} = (q, x^n - 1)$ . Let

$$\begin{aligned}
 \mathcal{T} &:= \{a \in \mathbb{Z}[x] : a = [a]_{\mathfrak{p}}\} = \{a \in \mathbb{Z}[x] : a_i \in (p) \text{ and } \deg(a) < \deg(\Phi_n)\}, \\
 \mathcal{T}_+ &:= \{a \in \mathcal{T} : \langle xa, a \rangle \geq 0\}.
 \end{aligned}$$

The definition of  $\text{NTRU}_{\text{HRSS17}}$  is in Fig. 7. Note that all ciphertexts are equivalent to 0 modulo  $(q, \Phi_1)$ , which prevents a trivial distinguishing attack.

Gen( $1^\kappa$ )	Enc( $h, m$ ), $m \in \mathcal{T}$	Dec( $f, c$ )
$g, f \leftarrow \mathcal{T}_+$	$r \leftarrow \mathcal{T}$	$m' := [[cf]_{\mathfrak{q}} f^{-1}]_{\mathfrak{p}}$
$f_q := [1/f]_{(q, \Phi_n)}$	$c := [prh + \text{Lift}_p(m)]_{\mathfrak{q}}$	<b>return</b> $m'$
$h := [\Phi_1 g f_q]_{\mathfrak{q}}$	<b>return</b> $c$	
<b>return</b> $dk = f, ek = h$		

**Fig. 7.**  $\text{NTRU}_{\text{HRSS17}}$



$\text{Gen}'(1^k) = \text{Gen}$	$\text{Enc}'(h, (m, r)), (m, r) \in \mathcal{T}^2$	$\text{Dec}'(f, c)$
$g, f \leftarrow \mathcal{T}_+$	$c := [prh + \text{Lift}_p(m)]_q$	$m' := [[cf]_q f^{-1}]_p$
$f_q := [1/f]_{(q, \Phi_n)}$	<b>return</b> $c$	$r' := \left[ [(c - \text{Lift}_p(m')) \cdot (ph)^{-1}]_q \right]_p$
$h := [\Phi_{1g} f_q]_q$		<b>return</b> $(m', r')$
<b>return</b> $dk = f, ek = h$		

**Fig. 8.** Our modification  $\text{NTRU}_{\text{HRSS17}'}$

Hülsing et al. choose  $(n, p, q) = (701, 3, 8192)$ : The scheme is perfectly correct, and they claimed 128-bit post-quantum security of this parameter set. The implementation of  $\text{NTRU}_{\text{HRSS17}}$  and  $\text{QFO}^\perp[\text{NTRU}_{\text{HRSS17}}, \text{G}, \text{H}, \text{H}']$  is reported in [HRSS17].

**Our Modification:** We want  $\text{PKE}_1$  to be *deterministic*. Hence, we consider a pair of  $(m, r)$  as a plaintext and make the decryption algorithm output  $(m, r)$  rather than  $m$ . The modification  $\text{NTRU}_{\text{HRSS17}'}$  is summarized in Fig. 8.

The properties of this DPKE are summarized as follows:

**Perfect Correctness:** This follows from the perfect correctness of the original PKE.

**Sparseness:** This follows from the parameter setting of the original PKE.

**Pseudorandomness:** We assume that the modified PKE  $\text{NTRU}_{\text{HRSS17}'}$  satisfies pseudorandomness.

We also implement  $\text{SXY}[\text{NTRU}_{\text{HRSS17}'}, \text{H}, \text{H}']$ , where  $\text{H}$  and  $\text{H}'$  are implemented by  $\text{SHAKE256}$ . We define

$$\text{H}(m, r) := \text{XOF}((r, m, 0), 256) \text{ and } \text{H}'(s, c) := \text{XOF}((c, (s\|00 \cdots 00), 1), 256),$$

where we treat  $r \in R_n/(q)$  and the last bit is the context string.

To avoid the inversion of polynomials in decapsulation, we add  $f^{-1}$  modulo  $p$  to  $dk$  as Hülsing et al. did [HRSS17]. This requires 139 extra bytes. In addition, we put  $(ph)^{-1}$  modulo  $q$  in  $dk$ , which requires 1140 extra bytes. Thus, our decapsulation key is 2557 bytes long.

## 5.2 Experimental Results

We preform the experiment with

- one core of an Intel Core i7-6700 at 3.40 GHz on a desktop PC with 8 GB memory and Ubuntu16.04 and
- a RasPi3 with 32-bit Rasbian.

We use `gcc` to compile the programs with option `-O3`. We generate 200 keys and ciphertexts to estimate the running time of key generation, encryption, and decryption. The experimental results are summarized

**Table 3.** Experimental results: We have  $|ek| = 1140$  bytes,  $|dk| = 2557$  bytes, and  $|c| = 1140$  bytes.

(a) Our Experiments on a PC				(b) Our Experiments on a RasPi					
	min	med.	avg.	max		min	med.	avg.	max
Gen <sub>1</sub>	1767	1778	1815	2592	Gen <sub>1</sub>	33 675	33 685	33 687	45 460
Enc <sub>1</sub>	327	329	328	331	Enc <sub>1</sub>	3 085	3 089	3 091	3 121
Dec <sub>1</sub>	958	959	959	1 021	Dec <sub>1</sub>	8 839	8 851	8 850	8 880
	min	med.	avg.	max		min	med.	avg.	max
$\overline{\text{Gen}}$	2565	2580	2579	2601	$\overline{\text{Gen}}$	49 151	49 169	49 174	49 263
$\overline{\text{Enc}}$	332	334	333	336	$\overline{\text{Enc}}$	3 200	3 205	3 207	3 232
$\overline{\text{Dec}}$	1280	1282	1282	1286	$\overline{\text{Dec}}$	11 837	11 841	11 843	11 888

in Table 3. (Gen<sub>1</sub>, Enc<sub>1</sub>, Dec<sub>1</sub>) and ( $\overline{\text{Gen}}$ ,  $\overline{\text{Enc}}$ ,  $\overline{\text{Dec}}$ ) indicate  $\text{NTRU}_{\text{HRSS17}'}$  and  $\text{SXY}[\text{NTRU}_{\text{HRSS17}'}]$ . The results reflect Hüsling et al.’s constant-time implementation and ours. Our conversion adds only small extra costs for hashing in encryption and adds about  $T_{\text{Enc}_1}$  for re-encrypting in decryption.

Note that our implementations are for reference and we did not optimize them. Further optimizations will speed up the algorithms as Hüsling et al. did [HRSS17]. The source code is available at <https://info.isl.ntt.co.jp/crypt/eng/archive/contents.html#sxy>.

**Acknowledgements.** We would like to thank anonymous reviewers of Eurocrypt 2018, Eike Kiltz, Daniel J. Bernstein, Edoardo Persichetti, and Joost Rijneveld for their insightful comments.

## A Missing Definitions

**Definition A.1 ( $\gamma$ -spread).** Let  $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$  be a PKE scheme. We say PKE is  $\gamma$ -spread if for every  $(ek, dk)$  generated by  $\text{Gen}(1^\kappa)$  and for any  $m \in \mathcal{M}$ , we have that

$$-\lg \left( \max_{c \in \mathcal{C}} \Pr_{r \leftarrow \mathcal{R}} [c = \text{Enc}(ek, m; r)] \right) \geq \gamma.$$

(In other words, the min entropy of  $\text{Enc}(ek, m; U(\mathcal{R}))$  is at least  $\gamma$ .) We say PKE is well-spread in  $\kappa$  if  $\gamma = \gamma(\kappa) = \omega(\lg \kappa)$ .

We additionally review the definitions of onewayness under validity-checking attacks (OW-VA), onewayness under plaintext-checking attacks (OW-PCA), and onewayness under plaintext and validity checking attacks (OW-PCVA) for PKE.

**Definition A.2 (Security notions for PKE).** Let  $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$  be a PKE scheme with message space  $\mathcal{M}$ . For any adversary  $\mathcal{A}$  and for  $\text{ATK} \in$

$\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ow-atk}}(\kappa)$	$\text{Pco}(m \in \mathcal{M}, c)$	$\text{Cvo}(c)$
$(ek, dk) \leftarrow \text{Gen}(1^\kappa)$	<b>return</b> boole( $m \stackrel{?}{=} \text{Dec}(dk, c)$ )	if $c = c^*$ , <b>return</b> $\perp$
$m^* \leftarrow \mathcal{M}$		$m := \text{Dec}(dk, c)$
$c^* \leftarrow \text{Enc}(ek, m^*)$		<b>return</b> boole( $m \in \mathcal{M}$ )
$m' \leftarrow \mathcal{A}^{\text{OATK}}(ek, c^*)$		
<b>return</b> boole( $m' \stackrel{?}{=} \text{Dec}(dk, c^*)$ )		

**Fig. 9.** Games for PKE schemes

$\{\text{VA}, \text{PCA}, \text{PCVA}\}$ , we define the experiments  $\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ow-va}}(\kappa)$ ,  $\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ow-pca}}(\kappa)$ , and  $\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ow-pcva}}(\kappa)$  as in Fig. 9, where

$$O_{\text{ATK}} := \begin{cases} \text{Cvo}(\cdot) & (\text{ATK} = \text{VA}) \\ \text{Pco}(\cdot, \cdot) & (\text{ATK} = \text{PCA}) \\ \text{Cvo}(\cdot), \text{Pco}(\cdot, \cdot) & (\text{ATK} = \text{PCVA}). \end{cases}$$

For any adversary  $\mathcal{A}$ , we define its OW-VA, OW-PCA, and OW-PCVA advantages as follows:

$$\begin{aligned} \text{Adv}_{\mathcal{A}, \text{PKE}}^{\text{ow-va}}(\kappa) &:= \Pr[\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ow-va}}(\kappa) = 1], \\ \text{Adv}_{\mathcal{A}, \text{PKE}}^{\text{ow-pca}}(\kappa) &:= \Pr[\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ow-pca}}(\kappa) = 1], \\ \text{Adv}_{\mathcal{A}, \text{PKE}}^{\text{ow-pcva}}(\kappa) &:= \Pr[\text{Expt}_{\text{PKE}, \mathcal{A}}^{\text{ow-pcva}}(\kappa) = 1]. \end{aligned}$$

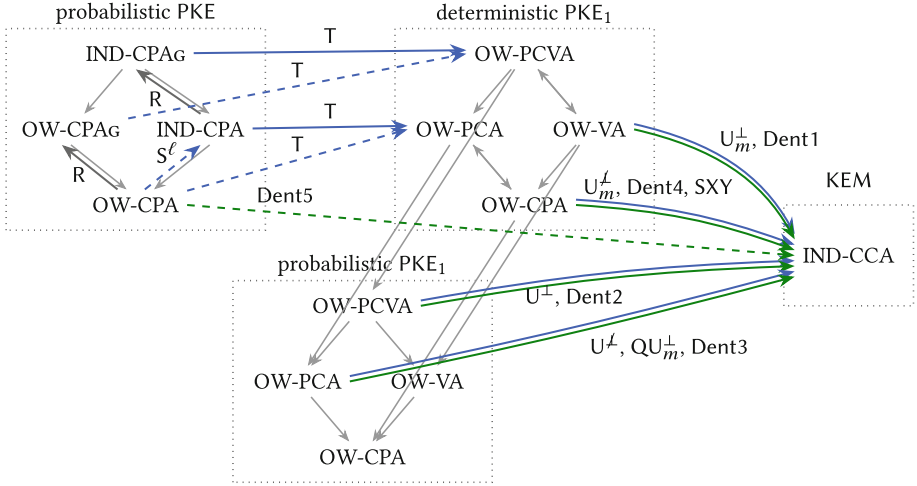
For  $\text{ATK} \in \{\text{VA}, \text{PCA}, \text{PCVA}\}$ , we say that PKE is OW-ATK-secure if  $\text{Adv}_{\mathcal{A}, \text{PKE}}^{\text{ow-atk}}(\kappa)$  is negligible for any PPT adversary  $\mathcal{A}$ .

## B Transformations in the Random Oracle Model

We summarize transformations among PKE, DPKE and KEM in the ROM in Fig. 10.

GOAL-ATTACKg indicate the class of PKEs that is GOAL-ATTACK-secure and  $2^{-\omega(\lg \kappa)}$ -uniformity [FO00, FO99], or equivalently  $\omega(\lg \kappa)$ -spreading [FO13]. Solid arrows indicate tight reductions, dashed arrows indicate non-tight reductions, thin arrows indicate trivial reductions, thick black arrows indicate reductions in [FO00], thick green arrows indicate reductions in [Den03], and thick blue arrows indicate reductions in [HHK17].

- The transformation R is in [FO00, Remark 5.5]; R converts  $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$  with randomness space  $\mathcal{R}$  into  $\text{PKE}' = (\text{Gen}', \text{Enc}', \text{Dec}')$  with randomness space  $\mathcal{R} \times \mathcal{R}'$ . They defined  $\text{Gen}' := \text{Gen}$ ,  $\text{Enc}'(ek, x; (r, r')) := (\text{Enc}(ek, x; r), r')$  and  $\text{Dec}'(dk, (c, r')) := \text{Dec}(dk, c)$ . This change amplifies  $\gamma$ -uniformity of PKE into  $(\gamma/|\mathcal{R}'|)$ -uniformity.



**Fig. 10.** Transformations in the ROM. GOAL-ATTACKg indicates the class of PKEs that is GOAL-ATTACK-secure and  $2^{-\omega(\lg \kappa)}$ -uniformity [FO00,FO99], or equivalently  $\omega(\lg \kappa)$ -spreading [FO13]. Solid arrows indicate tight reductions, dashed arrows indicate non-tight reductions, thin arrows indicate trivial reductions, thick black arrows indicate reductions in [FO00], thick green arrows indicate reductions in [Den03], and thick blue arrows indicate reductions in [HHK17]. The transformation R is in [FO00, Remark 5.5]. The transformations Dent1, Dent2, Dent3, Dent4, and Dent5 are given in [Den03]. The transformations  $S^\ell$ , T,  $U^\perp$ ,  $U^\ell$ ,  $U_m^\perp$ ,  $U_m^\ell$ , and  $QU_m^\perp$  are given in [HHK17]. (Color figure online)

- The transformations Dent1, Dent2, Dent3, Dent4, and Dent5 are given in [Den03].
- The transformations  $S^\ell$ , T,  $U^\perp$ ,  $U^\ell$ ,  $U_m^\perp$ ,  $U_m^\ell$ , and  $QU_m^\perp$  are given in [HHK17].

Note that  $\text{Dent1} \approx U_m^\perp$ , which is a KEM variant of BR93;  $\text{Dent2} \approx U^\perp$ , which is a KEM variant of REACT/GEM;  $\text{Dent4} \approx QU_m^\perp$ ;  $\text{Dent5} \approx FO_m^\perp = U_m^\perp \circ T$ , which is a KEM variant of FO.

Albrecht, Orsini, Paterson, Peer, and Smart [AOP+17] gave the tight security proof for Dent5 when the underlying PKE is a certain Ring-LWE-based PKE scheme. We also observe that Dent5 is decomposed into  $U_m^\perp \circ T$ . Thus, starting from IND-CPAg-secure PKE, we obtain the similar proof by combining reductions in [HHK17].

## C Omitted Proofs

### C.1 Proof of Lemma 2.2

Here, we prove Lemma 2.2. Before proving the lemma, we introduce another lemma, which gives a lower bound for a decisional variant of Grover’s search problem.

**Lemma C.1** ([SY17, Lemma C.1]). *Let  $g_s : \{0, 1\}^\ell \rightarrow \{0, 1\}$  denotes a function defined as  $g_s(s) := 1$  and  $g_s(s') := 0$  for all  $s' \neq s$ , and  $g_\perp : \{0, 1\}^\ell \rightarrow \{0, 1\}$  denotes a function that returns 0 for all inputs. Then for any unbounded time adversary  $\mathcal{A}$  that issues at most  $q$  quantum queries to its oracle, we have*

$$\Pr[1 \leftarrow \mathcal{A}^{g_s}() \mid s \leftarrow \{0, 1\}^\ell] - \Pr[1 \leftarrow \mathcal{A}^{g_\perp}()] \leq q \cdot 2^{-\frac{\ell+1}{2}}.$$

Then we prove Lemma 2.2 relying on the above lemma.

*Proof.* (of Lemma 2.2) To prove the theorem, we consider the following sequence of games for an algorithm  $\mathcal{A}$ .

**Game 0:** This game returns as  $\mathcal{A}^{\mathsf{H}, \mathsf{H}(s, \cdot)}()$  outputs, where  $s \leftarrow \{0, 1\}^\ell$  and  $\mathsf{H} : \{0, 1\}^\ell \times \mathcal{X} \rightarrow \mathcal{Y}$  are random functions.

**Game 1:** This game returns as  $\mathcal{A}^{O[s, \mathsf{H}_0, \mathsf{H}_1], \mathsf{H}_1(\cdot)}()$  outputs, where  $s \leftarrow \{0, 1\}^\ell$ ,  $\mathsf{H}_0 : \{0, 1\}^\ell \times \mathcal{X} \rightarrow \mathcal{Y}$  and  $\mathsf{H}_1 : \mathcal{X} \rightarrow \mathcal{Y}$  are independent random functions, and  $O[s, \mathsf{H}_0, \mathsf{H}_1]$  is a function defined as

$$O[s, \mathsf{H}_0, \mathsf{H}_1](s', x) := \begin{cases} \mathsf{H}_0(s', x) & \text{if } s' \neq s, \\ \mathsf{H}_1(x) & \text{if } s' = s. \end{cases} \quad (1)$$

**Game 2:** This game returns as  $\mathcal{A}^{\mathsf{H}_0, \mathsf{H}_1}()$  outputs, where  $\mathsf{H}_0 : \{0, 1\}^\ell \times \mathcal{X} \rightarrow \mathcal{Y}$  and  $\mathsf{H}_1 : \mathcal{X} \rightarrow \mathcal{Y}$  are independent random functions.

This completes the descriptions of games. We want to prove that  $|\Pr[\text{Game}_2 = 1] - \Pr[\text{Game}_0 = 1]| \leq q_{\mathsf{H}} \cdot 2^{-\frac{\ell+1}{2}}$ . It is easy to see that we have  $\Pr[\text{Game}_0 = 1] = \Pr[\text{Game}_1 = 1]$ . What is left is to prove that  $|\Pr[\text{Game}_2 = 1] - \Pr[\text{Game}_1 = 1]| \leq q_{\mathsf{H}} \cdot 2^{-\frac{\ell+1}{2}}$ . We prove this by a reduction to Lemma C.1. We consider the following algorithm  $\mathcal{B}$  that has access to  $g$  that is  $g_s$  for randomly chosen  $s \leftarrow \{0, 1\}^\ell$  or  $g_\perp$  where  $g_s$  and  $g_\perp$  are as defined in Lemma C.1.

$\mathcal{B}^g$ : It picks two random functions  $\mathsf{H}_0 : \{0, 1\}^\ell \times \mathcal{X} \rightarrow \mathcal{Y}$  and  $\mathsf{H}_1 : \mathcal{X} \rightarrow \mathcal{Y}$ , and runs  $\mathcal{A}^{O, \mathsf{H}_1}$  where  $\mathcal{B}$  simulates  $O$  as follows: If  $\mathcal{A}$  queries  $(s', x)$  to  $O$ ,  $\mathcal{B}$  queries  $s'$  to its own oracle  $g$  to obtain a bit  $b$ . If  $b = 0$ , then  $\mathcal{B}$  returns  $\mathsf{H}_0(s', x)$  to  $\mathcal{A}$  and if  $b = 1$ , then  $\mathcal{B}$  returns  $\mathsf{H}_1(x')$  to  $\mathcal{A}$ .

This completes the description of  $\mathcal{B}$ . It is easy to see that if  $g = g_s$  for randomly chosen  $s \leftarrow \{0, 1\}^\ell$ , then  $\mathcal{B}$  perfectly simulates  $\text{Game}_1$ , and if  $g = g_\perp$ , then  $\mathcal{B}$  perfectly simulates  $\text{Game}_2$ . Therefore, we have

$$|\Pr[\text{Game}_1 = 1] - \Pr[\text{Game}_2 = 1]| = \left| \Pr[1 \leftarrow \mathcal{B}^{g_s}() \mid s \leftarrow \{0, 1\}^\ell] - \Pr[1 \leftarrow \mathcal{B}^{g_\perp}()] \right|.$$

On the other hand, by Lemma C.1, we have

$$\left| \Pr[1 \leftarrow \mathcal{B}^{g_s}() \mid s \leftarrow \{0, 1\}^\ell] - \Pr[1 \leftarrow \mathcal{B}^{g_\perp}()] \right| \leq q_{\mathsf{H}} \cdot 2^{-\frac{\ell+1}{2}},$$

since the number of  $\mathcal{B}$ 's queries to its own oracle is exactly the same as the number of  $\mathcal{A}$ 's queries to  $O$ , which is equal to  $q_{\mathsf{H}}$ . This completes the proof of Lemma 2.2.  $\square$

## References

- [ACPS09] Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 595–618. Springer, Heidelberg (2009). [https://doi.org/10.1007/978-3-642-03356-8\\_35](https://doi.org/10.1007/978-3-642-03356-8_35)
- [Ajt99] Ajtai, M.: Generating hard instances of the short basis problem. In: Wiedermann, J., van Emde Boas, P., Nielsen, M. (eds.) ICALP 1999. LNCS, vol. 1644, pp. 1–9. Springer, Heidelberg (1999). [https://doi.org/10.1007/3-540-48523-6\\_1](https://doi.org/10.1007/3-540-48523-6_1)
- [AOP+17] Albrecht, M.R., Orsini, E., Paterson, K.G., Peer, G., Smart, N.P.: Tightly secure ring-LWE based key encapsulation with short ciphertexts. In: Foley, S.N., Gollmann, D., Sneekenes, E. (eds.) ESORICS 2017. LNCS, vol. 10492, pp. 29–46. Springer, Cham (2017). [https://doi.org/10.1007/978-3-319-66402-6\\_4](https://doi.org/10.1007/978-3-319-66402-6_4)
- [AP11] Alwen, J., Peikert, C.: Generating shorter bases for hard random lattices. *Theory Comput. Syst.* **48**(3), 535–553 (2011). A preliminary versions appeared in STACS 2009 (2009)
- [BDF+11] Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer, Heidelberg (2011). [https://doi.org/10.1007/978-3-642-25385-0\\_3](https://doi.org/10.1007/978-3-642-25385-0_3)
- [BFKL93] Blum, A., Furst, M., Kearns, M., Lipton, R.J.: Cryptographic primitives based on hard learning problems. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 278–291. Springer, Heidelberg (1994). [https://doi.org/10.1007/3-540-48329-2\\_24](https://doi.org/10.1007/3-540-48329-2_24)
- [BR93] Bellare, M., Rogaway, P.: Random oracle are practical: a paradigm for designing efficient protocols. In: CCS 1993, pp. 62–73. ACM (1993)
- [BR95] Bellare, M., Rogaway, P.: Optimal asymmetric encryption. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 92–111. Springer, Heidelberg (1995). <https://doi.org/10.1007/BFb0053428>
- [BV11] Brakerski, Z., Vaikuntanathan, V.: Fully homomorphic encryption from ring-LWE and security for key dependent messages. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 505–524. Springer, Heidelberg (2011). [https://doi.org/10.1007/978-3-642-22792-9\\_29](https://doi.org/10.1007/978-3-642-22792-9_29)
- [CHJ+02] Jean-Sébastien, C., Handschuh, H., Joye, M., Paillier, P., Pointcheval, D., Tymen, C.: GEM: a generic chosen-ciphertext secure encryption method. In: Preneel, B. (ed.) CT-RSA 2002. LNCS, vol. 2271, pp. 263–276. Springer, Heidelberg (2002). [https://doi.org/10.1007/3-540-45760-7\\_18](https://doi.org/10.1007/3-540-45760-7_18)
- [Den03] Dent, A.W.: A designer’s guide to KEMs. In: Paterson, K.G. (ed.) Cryptography and Coding 2003. LNCS, vol. 2898, pp. 133–151. Springer, Heidelberg (2003). [https://doi.org/10.1007/978-3-540-40974-8\\_12](https://doi.org/10.1007/978-3-540-40974-8_12)
- [FO99] Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg (1999). [https://doi.org/10.1007/3-540-48405-1\\_34](https://doi.org/10.1007/3-540-48405-1_34)
- [FO00] Fujisaki, E., Okamoto, T.: How to enhance the security of public-key encryption at minimum cost. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **83**(1), 24–32 (2000). A preliminary version appeared in PKC 1999 (1999)

- [FO13] Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. *J. Cryptol.* **26**(1), 80–101 (2013)
- [FOPS04] Fujisaki, E., Okamoto, T., Pointcheval, D., Stern, J.: RSA-OAEP is secure under the RSA assumption. *J. Cryptol.* **17**(2), 81–104 (2004)
- [GPV08] Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Dwork, C. (ed.) *STOC 2008*, pp. 197–206. ACM (2008). <https://eprint.iacr.org/2007/432>
- [HHK17] Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the fujisaki-okamoto transformation. In: Kalai, Y., Reyzin, L. (eds.) *TCC 2017, Part I*. LNCS, vol. 10677, pp. 341–371. Springer, Cham (2017). [https://doi.org/10.1007/978-3-319-70500-2\\_12](https://doi.org/10.1007/978-3-319-70500-2_12)
- [HPS98] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: a ring-based public key cryptosystem. In: Buhler, J.P. (ed.) *ANTS 1998*. LNCS, vol. 1423, pp. 267–288. Springer, Heidelberg (1998). <https://doi.org/10.1007/BFb0054868>
- [HRSS17] Hülsing, A., Rijneveld, J., Schanck, J., Schwabe, P.: High-speed key encapsulation from NTRU. In: Fischer, W., Homma, N. (eds.) *CHES 2017*. LNCS, vol. 10529, pp. 232–252. Springer, Cham (2017). [https://doi.org/10.1007/978-3-319-66787-4\\_12](https://doi.org/10.1007/978-3-319-66787-4_12)
- [JZC+17] Jiang, H., Zhang, Z., Chen, L., Wang, H., Ma, Z.: Post-quantum IND-CCA-secure KEM without additional hash. *IACR Cryptology ePrint Archive 2017/1096* (2017)
- [KLS17] Kiltz, E., Lyubashevsky, V., Schaffner, C.: A concrete treatment of fiat-shamir signatures in the quantum random-oracle model. *IACR Cryptology ePrint Archive 2017/916* (2017)
- [KSS10] Katz, J., Shin, J.S., Smith, A.: Parallel and concurrent security of the HB and HB<sup>+</sup> protocols. *J. Cryptology* **23**(3), 402–421 (2010)
- [LPR10] Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) *EUROCRYPT 2010*. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010). [https://doi.org/10.1007/978-3-642-13190-5\\_1](https://doi.org/10.1007/978-3-642-13190-5_1)
- [LTV12] López-Alt, A., Tromer, E., Vaikuntanathan, V.: On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Karloff, H.J., Pitassi, T. (eds.) *STOC 2012*, pp. 1219–1234. ACM (2012)
- [McE78] McEliece, R.J.: A public key cryptosystem based on algebraic coding theory. Technical report, DSN progress report (1978)
- [Men12] Menezes, A.: Another look at provable security. In: Pointcheval, D., Johansson, T. (eds.) *EUROCRYPT 2012*. LNCS, vol. 7237, p. 8. Springer, Heidelberg (2012). [https://doi.org/10.1007/978-3-642-29011-4\\_2](https://doi.org/10.1007/978-3-642-29011-4_2)
- [MP12] Micciancio, D., Peikert, C.: Trapdoors for lattices: simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) *EUROCRYPT 2012*. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). [https://doi.org/10.1007/978-3-642-29011-4\\_41](https://doi.org/10.1007/978-3-642-29011-4_41)
- [MR07] Micciancio, D., Regev, O.: Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.* **37**(1), 267–302 (2007). A preliminary version appeared in *FOCS 2004* (2004)
- [NC00] Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge (2000)
- [Nie86] Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. *Probl. Control Inf. Theory* **15**, 159–166 (1986)

- [NIS15] Fips 202: Sha-3 standard: Permutation-based hash and extendable-output functions. U.S.Department of Commerce/National Institute of Standards and Technology (2015)
- [OP01] Okamoto, T., Pointcheval, D.: REACT: rapid enhanced-security asymmetric cryptosystem transform. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 159–174. Springer, Heidelberg (2000). [https://doi.org/10.1007/3-540-45353-9\\_13](https://doi.org/10.1007/3-540-45353-9_13)
- [Pei09] Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In: Mitzenmacher, M. (ed.) STOC 2009, pp. 333–342. ACM (2009)
- [Reg09] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. *J. ACM* **56**(6), Article 34 (2009). A preliminary version appeared in STOC 2005 (2005)
- [SS11] Stehlé, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 27–47. Springer, Heidelberg (2011)
- [SY17] Song, F., Yun, A.: Quantum security of NMAC and related constructions. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10402, pp. 283–309. Springer, Cham (2017). [https://doi.org/10.1007/978-3-319-63715-0\\_10](https://doi.org/10.1007/978-3-319-63715-0_10)
- [TU16] Targhi, E.E., Unruh, D.: Post-quantum security of the fujisaki-okamoto and OAEP transforms. In: Hirt, M., Smith, A. (eds.) TCC 2016. LNCS, vol. 9986, pp. 192–216. Springer, Heidelberg (2016). [https://doi.org/10.1007/978-3-662-53644-5\\_8](https://doi.org/10.1007/978-3-662-53644-5_8)
- [Unr15] Unruh, D.: Revocable quantum timed-release encryption. *J. ACM* **62**(6), No. 49 (2015). The preliminary version appeared in EUROCRYPT 2014. <https://eprint.iacr.org/2013/606>
- [Zha12a] Zhandry, M.: How to construct quantum random functions. In: 53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, pp. 679–687, 20–23 October 2012
- [Zha12b] Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 758–775. Springer, Heidelberg (2012). [https://doi.org/10.1007/978-3-642-32009-5\\_44](https://doi.org/10.1007/978-3-642-32009-5_44)