Anonymity of NIST PQC Round-3 KEMs

Keita Xagawa[1][0000−0002−6832−9940]

NTT Social Informatics Laboratories, keita.xagawa.zv@hco.ntt.co.jp

Abstract. This paper investigates *anonymity* of all NIST PQC Round 3 KEMs: Classic McEliece, Kyber, NTRU, Saber, BIKE, FrodoKEM, HQC, NTRU Prime (Streamlined NTRU Prime and NTRU LPRime), and SIKE. We show the following results:

- NTRU is anonymous in the quantum random oracle model (QROM) if the underlying deterministic PKE is strongly disjoint-simulatable. NTRU is collision-free in the QROM. A hybrid PKE scheme constructed from NTRU as KEM and appropriate DEM is anonymous and robust. (Similar results for BIKE, FrodoKEM, HQC, NTRU LPRime, and SIKE hold except one of three parameter sets of HQC.)
- Classic McEliece is anonymous in the QROM if the underlying PKE is strongly disjoint-simulatable and a hybrid PKE scheme constructed from it as KEM and appropriate DEM is anonymous.
- Grubbs, Maram, and Paterson pointed out that Kyber and Saber have a gap in the current IND-CCA security proof in the QROM (EUROCRYPT 2022). We found that Streamlined NTRU Prime has another technical obstacle for the IND-CCA security proof in the QROM.

Those answer the open problem to investigate the anonymity and robustness of NIST PQC Round 3 KEMs posed by Grubbs, Maram, and Paterson (EUROCRYPT 2022).

We use strong disjoint-simulatability of the underlying PKE of KEM and strong pseudorandomness and smoothness/sparseness of KEM as the main tools, which will be of independent interest.

Keywords: anonymity, robustness, post-quantum cryptography, NIST PQC standardization, KEM, PKE, quantum random model

1 Introduction

Public-key encryption (PKE) allows us to send a message to a receiver confidentially if the receiver's public key is available. However, a ciphertext of PKE may reveal the receiver's public key, and the recipient of the ciphertext will be identified. This causes trouble in some applications, and researchers study the anonymity of PKE. Roughly speaking, PKE is said to be *anonymous* [7] if a ciphertext hides the receiver's information. Anonymous primitive is often used in the context of privacy-enhancing technologies.

A ciphertext of anonymous PKE indicates (computationally) no information of a receiver. Thus, when a receiver receives a ciphertext, it should

decrypt the ciphertext into a message and verify the message in order to check if the ciphertext is sent to the receiver or not. There may be a ciphertext from which two (or more) recipients can obtain messages in this situation, and this causes trouble in some applications, e.g., auction protocols [40]. Intuitively speaking, PKE is said to be *robust* [2] if only the intended receiver can obtain a meaningful message from a ciphertext. Both anonymity and robustness are important and useful properties beyond the standard IND-CCA security. Anonymous PKE is an important building primitive for anonymous credential systems [13], auction protocols [40], (weakly) anonymous authenticated key exchange [12, 20, 21, 43], and so on. Robust PKE has an application for searchable encryption [1] and auction [40].

Previous works on anonymity and robustness of KEM and hybrid PKE: Mohassel [36] studied the anonymity and robustness of a special KEM/DEM framework, a hybrid PKE with KEM that is implemented by a PKE with random plaintext. He showed that even if anonymous KEM and DEM sometimes fail to lead to an anonymous hybrid PKE by constructing a counterexample.
Grubbs, Maram, and Paterson [24] discussed anonymity and robustness of *post-quantum* KEM schemes and KEM/DEM framework in the quantum random oracle model (QROM). They also studied the anonymity and robustness of the hybrid PKE based on KEM with implicit rejection. On the variants of the Fujisaki-Okamoto (FO) transform [22, 23], they showed that anonymity and collision-freeness of KEMs obtained by the FO transform with implicit rejection and its variant[1], and they lead to anonymous, robust hybrid PKEs from appropriate assumptions. They also show anonymity and robustness of KEM obtained by a variant of the FO transform with explicit rejection and key-confirmation hash[2] and show that it leads to anonymous, robust hybrid PKE from appropriate assumptions.
They examined NIST PQC Standardization finalists (Classic McEliece [5], Kyber [42], NTRU [14], and Saber [18]). They showed the following results:

- Classic McEliece: They found that Classic McEliece is not collision-free. Since their anonymity proof in [24, Theorem 5] strongly depends on the collision-freeness of the underlying PKE, we cannot apply their anonymity proof to Classic McEliece. They also show that the hybrid PKE fails to achieve robustness since Classic McEliece is not collision-free.
- Kyber: They found that Kyber's anonymity (and even IND-CCA security) has two technical obstacles ('pre-key' and 'nested random oracles') in the QROM.
- NTRU: NTRU's anonymity has another technical obstacle: Their proof technique requires the computation of a key of KEM involving a message and a ciphertext, but, in NTRU, the computation of a

[1] A variant of the FO transform with implicit rejection using 'pre-key' technique. They wrote "a variant of the $\mathsf{FO}^{\not\perp}$ transform" in their paper.
[2] They modify 'key-confirmation hash' to involve a ciphertext on input.

key of NTRU involves only a message. The robustness of the hybrid PKE with NTRU is unclear.
- Saber: They insisted they show Saber's anonymity and IND-CCA security and the robustness of the hybrid PKE with Saber in the QROM, because they considered that Saber employs the FO transform with 'pre-key'. Unfortunately, Saber in [18] also uses both 'pre-key' and 'nested random oracles' as Kyber, and their proofs cannot be applied to Saber. See their slides [25]. (Fortunately, FrodoKEM can be shown anonymous and lead to anonymous, robust hybrid PKE, because FrodoKEM employs the FO transform with 'pre-key'.)

Unfortunately, we do not know whether all four finalists are anonymous or not, although the much effort of Grubbs et al. and their clean and modular framework. Grubbs et al. left several open problems: One of them is the anonymity and robustness of NTRU; the other important one is the anonymity of Classic McEliece.

1.1 Our Contribution

We investigate anonymity and robustness of *all* NIST PQC Round 3 KEM candidates and obtain Table 1. This answers the open problems posed by Grubbs et al.

In order to investigate anonymity, we first study strong pseudorandomness of PKE/KEM instead of studying anonymity directly. To show strong pseudorandomness of the hybird PKE, we study strong pseudorandomness and introduce smoothness and sparseness of KEM. We then show such properties of KEM obtained by the variants of the FO transform if the underlying deterministic PKE is strongly disjoint-simulatable. We finally study the properties of NIST PQC Round 3 KEM candidates. See the details in the following.

Anonymity through strong pseudorandomness, sparseness, and smoothness: Our starting point is *strong pseudorandomness* instead of anonymity. We say PKE/KEM/DEM is *strongly pseudorandom* if its ciphertext is indistinguishable from a random string chosen by a simulator on input the security parameter.[3] It is easy to show that strong pseudorandomness implies anonymity.

Using this notion, we attempt to follow the IND-CCA security proof of the KEM/DEM framework [16], that is, we try to show that the hybrid PKE from strongly pseudorandom KEM/DEM is also strongly pseudorandom, which implies that the hybrid PKE is anonymous. If we directly try to prove the ANON-CCA security of the hybrid PKE, then we will need to simulate *two* decryption oracles as Grubbs et al. Considering pseudorandomness allows us to treat a *single* key and oracle and simplifies the security proof. Unfortunately, we face another obstacle in the security proof when considering pseudorandomness.

To resolve the obstacle, we define *sparseness* of KEM with explicit rejection and *smoothness* of KEM with implicit rejection: We say KEM with explicit rejection is *sparse* if a ciphertext c chosen by a simulator is

[3] If the simulator can depend on an encryption key, then we just say pseudorandom.

Table 1. Summary of anonymity and robustness of NIST PQC Round 3 KEM candidates (finalists and alternate candidates) and the hybrid PKEs using them. In the first row, IND = Indistinguishability, SPR = Strong Pseudorandomness, ANO = Anonymity, CF = Collision Freeness, and ROB = Robustness under chosen-ciphertext attacks in the QROM. Y = Yes, N = No, ? = Unknown. The underline implies our new findings.

	KEM					Hybrid PKE	
Name	IND	SPR	ANO	CF	ROB	ANO	ROB
Classic McEliece [5]	Y	<u>Y</u>	<u>Y</u>	N	N	<u>Y</u>	N
Kyber [42]	?	?	?	?	N	?	?
NTRU [14]	Y	<u>Y</u>	<u>Y</u>	<u>Y</u>	N	<u>Y</u>	<u>Y</u>
Saber [18]	?	?	?	?	N	?	?
BIKE [6]	Y	<u>Y</u>	<u>Y</u>	<u>Y</u>	N	<u>Y</u>	<u>Y</u>
FrodoKEM [37]	Y	Y	Y	Y	N	Y	Y
HQC-128/192 [4]	Y	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>
HQC-256 [4]	Y	<u>N</u>	<u>N</u>	<u>Y</u>	<u>Y</u>	<u>N</u>	<u>Y</u>
Streamlined NTRU Prime [10]	<u>?</u>	?	?	?	N	?	?
NTRU LPRime [10]	Y	<u>Y</u>	<u>Y</u>	<u>Y</u>	N	<u>Y</u>	<u>Y</u>
SIKE [30]	Y	<u>Y</u>	<u>Y</u>	<u>Y</u>	N	<u>Y</u>	<u>Y</u>

decapsulated into $\perp$ with overwhelming probability. We say KEM with implicit rejection is *smooth* if, given a ciphertext c chosen by a simulator, any efficient adversary cannot distinguish a random key from a decapsulated key. This definition imitates the smoothness of the hash proof system [16]. Those notions help us to prove the pseudorandomness of the hybrid PKE.

Pseudorandomness, smoothness, and collision-freeness of the FO variants: In order to treat the case for Classic McEliece and NTRU, in which the underlying PKE is deterministic, we treat SXY [39], variants of U [26], and variants of HU [32]. Modifying the IND-CCA security proofs of them, we show that the obtained KEM is strongly pseudorandom and smooth if the underlying PKE is strongly disjoint-simulatable [39]. We also show that the obtained KEM is collision-free if the underlying deterministic PKE is collision-free. We finally note that our reductions are *tight* as a bonus.

Grubbs et al. [24] discussed a barrier to show anonymity of NTRU (and Classic McEliece implicitly), which stems from the design choice $K = \mathsf{H}(\mu)$ instead of $K = \mathsf{H}(\mu, c)$. In addition, their proof technique requires the underlying PKE to be collision-free. Since the underlying PKE of Classic McEliece lacks collision freeness, they left the proof of anonymity of Classic McEliece as an open problem. Both barriers stem from the fact that we need to simulate *two* decapsulation oracles in the proof of ANON-CCA-security. We avoid those technical barriers by using a stronger notion, SPR-CCA security; in the proof of SPR-CCA-security, we only need to simulate a *single* decapsulation oracle.

Application to NIST PQC Round-3 KEM candidates: Using the above techniques, we solve open problems posed by Grubbs et al. and extend the study of finalists and alternative candidates of NIST PQC Round 3 KEMs as depicted in Table 1.
We found the following properties (we omit the detail of the assumptions):

- Classic McEliece is anonymous and the hybrid PKE using it is anonymous, which is in the full version.
- NTRU is anonymous and collision-free. The hybrid PKE using it is anonymous and robust. See Section 5. Similar results for BIKE, HQC (HQC-128 and HQC-196)[4], NTRU LPRime, and SIKE hold, which are in the full version.
- We found that Streamlined NTRU Prime has another technical obstacle for anonymity: the key and key-confirmation hash involves 'pre-key' problem.[5] While this is not a big problem for the IND-CCA security in the ROM, we fail to show the IND-CCA security in the QROM. We will discuss it in detail in the full version.

Remark 1. Bernstein [9] suggests to use *quantum indifferentiability* of the domain extension of quantum random oracles in [49, Section 5]. While we did not check the detail, this quantum indifferentiability would solve the problems on 'pre-key' of Kyber, Saber, and Streamlined NTRU Prime.

Open Problems: We leave showing anonymity and the IND-CCA security of Kyber, Saber, and Streamlined NTRU Prime in the QROM as an important open problem as Grubbs et al. posed.

Organization: Section 2 reviews the QROM, definitions of primitives, and the results of Grubbs et al. [24]. In addition, it also shows strong pseudorandomness implies anonymity. Section 3 studies the strong pseudorandomness of the KEM/DEM framework. Section 4 studies SXY's security properties. Section 5 examines the anonymity and robustness of NTRU. Due to the space limit, we omit a lot of contents from the conference version.

Appendix Highlights: The full version contains the missing proofs. Moreover, its appendices contain the properties of the variants of the FO transform (T, variants of U, and variants of HU) and examine the other NIST PQC Round-3 KEM candidates, Classic McEliece, Kyber, Saber, BIKE, FrodoKEM, HQC, NTRU Prime (Streamlined NTRU Prime and NTRU LPRime), and SIKE, as summarized in Table 1.

[4] HQC-256 is not anonymous because the parity of the ciphertext leaks the parity of the encapsulation key. See the full version for the detail.

[5] The key and key-confirmation value on a plaintext μ and an encapsulation key ek is computed as $K = \mathsf{H}(k, c_0, c_1)$ and $h = \mathsf{F}(k, \mathsf{Hash}(ek))$, where $k = \mathsf{H}_3(\mu)$ and (c_0, c_1) is a main body of a ciphertext.

2 Preliminaries

Notations: A security parameter is denoted by κ. We use the standard O-notations. DPT, PPT, and QPT stand for a deterministic polynomial time, probabilistic polynomial time, and quantum polynomial time, respectively. A function $f(\kappa)$ is said to be *negligible* if $f(\kappa) = \kappa^{-\omega(1)}$. We denote a set of negligible functions by $\mathsf{negl}(\kappa)$. For a distribution χ, we often write "$x \leftarrow \chi$," which indicates that we take a sample x according to χ. 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, $\mathsf{A}(S)$ denotes the set $\{\mathsf{A}(x) \mid x \in S\}$. If inp is a string, then "$\mathsf{out} \leftarrow \mathsf{A}(\mathsf{inp})$" denotes the output of algorithm A when run on input inp. If A is deterministic, then out is a fixed value and we write "$\mathsf{out} := \mathsf{A}(\mathsf{inp})$." We also use the notation "$\mathsf{out} := \mathsf{A}(\mathsf{inp}; r)$" to make the randomness r explicit.
For a statement P (e.g., $r \in [0,1]$), we define $\mathsf{boole}(P) = 1$ if P is satisfied and 0 otherwise.
For two finite sets $\mathcal{X}$ and $\mathcal{Y}$, $\mathcal{F}(\mathcal{X}, \mathcal{Y})$ denotes a set of all mapping from $\mathcal{X}$ to $\mathcal{Y}$.

Lemma 1 (Generic distinguishing problem with bounded probabilities [29, Lemma 2.9], adapted). *Let $\mathcal{X}$ be a finite set. Let $\delta \in [0,1]$. Let $\mathsf{F}\colon \mathcal{X} \to \{0,1\}$ be the following function: for each $x \in \mathcal{X}$, $\mathsf{F}(x) = 1$ with probability $\delta_x \leq \delta$ and $\mathsf{F}(x) = 0$ else. Let $\mathsf{Z}\colon \mathcal{X} \to \{0,1\}$ be the zero function, that is, $\mathsf{Z}(x) = 0$ for all x. If an unbounded-time quantum adversary $\mathcal{A}$ makes a query to F or Z at most Q times, then we have*

$$\left|\Pr[b \leftarrow \mathcal{A}^{\mathsf{F}(\cdot)}() : b = 1] - \Pr[b \leftarrow \mathcal{A}^{\mathsf{Z}(\cdot)}() : b = 1]\right| \leq 8(Q+1)^2\delta.$$

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

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. In this paper, we model a quantum oracle O as a mapping $|x\rangle|y\rangle \mapsto |x\rangle|y \oplus O(x)\rangle$, where $x \in \{0,1\}^n$, $y \in \{0,1\}^m$, and $O\colon \{0,1\}^n \to \{0,1\}^m$. See [11] for a more detailed description of the model.

Lemma 2 (QRO is PRF). *Let ℓ be a positive integer. Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. Let $\mathsf{H}_{\mathsf{prf}}\colon \{0,1\}^\ell \times \mathcal{X} \to \mathcal{Y}$ and $\mathsf{H}_q\colon \mathcal{X} \to \mathcal{Y}$ be two independent random oracles. If an unbounded-time quantum adversary $\mathcal{A}$ makes a query to the random oracles at most Q times, then we have*

$$\left|\begin{array}{c}\Pr[s \leftarrow \mathcal{M}, b \leftarrow \mathcal{A}^{\mathsf{H}_{\mathsf{prf}}(\cdot,\cdot),\mathsf{H}_{\mathsf{prf}}(s,\cdot)}() : b = 1] \\ -\Pr[b \leftarrow \mathcal{A}^{\mathsf{H}_{\mathsf{prf}}(\cdot,\cdot),\mathsf{H}_q(\cdot)}() : b = 1]\end{array}\right| \leq 2Q \cdot 2^{-\ell/2}$$

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

See [39] and [31] for the proof.

Lemma 3 (QRO is collision-resistant [48, Theorem 3.1]). *There is a universal constant C such that the following holds: Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. Let $\mathsf{H}\colon \mathcal{X} \to \mathcal{Y}$ be a random oracle. If an unbounded time quantum adversary $\mathcal{A}$ makes a query to H at most Q times, then we have*

$$\Pr_{\mathsf{H},\mathcal{A}}[(x,x') \leftarrow \mathcal{A}^{\mathsf{H}(\cdot)} : x \neq x' \wedge \mathsf{H}(x) = \mathsf{H}(x')] \leq C(Q+1)^3/|\mathcal{Y}|,$$

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

Remark 2. We implicitly assume that $|\mathcal{X}| = \Omega(|\mathcal{Y}|)$, because of the birthday bound.

Lemma 4 (QRO is claw-free). *There is a universal constant C such that the following holds: Let $\mathcal{X}_0$ and $\mathcal{X}_1$ and $\mathcal{Y}$ be finite sets. Let $N_0 = |\mathcal{X}_0|$ and $N_1 = |\mathcal{X}_1|$. Without loss of generality, we assume $N_0 \leq N_1$. Let $\mathsf{H}_0\colon \mathcal{X}_0 \to \mathcal{Y}$ and $\mathsf{H}_1\colon \mathcal{X}_1 \to \mathcal{Y}$ be two random oracles. If an unbounded time quantum adversary $\mathcal{A}$ makes a query to H_0 and H_1 at most Q_0 and Q_1 times, then we have*

$$\Pr[(x_0,x_1) \leftarrow \mathcal{A}^{\mathsf{H}_0(\cdot),\mathsf{H}_1(\cdot)} : \mathsf{H}_0(x_0) = \mathsf{H}_1(x_1)] \leq C(Q_0+Q_1+1)^3/|\mathcal{Y}|,$$

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

We omit the security proof, which is due to Hosoyamada [28]. See the full version.

2.1 Public-Key Encryption (PKE)

The model for PKE schemes is summarized as follows:

Definition 1. *A PKE scheme* PKE *consists of the following triple of PPT algorithms* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

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

We review δ-correctness in Hofheinz, Hövelmanns, and Kiltz [26].

Definition 2 (δ-Correctness). *Let $\delta = \delta(\kappa)$. We say* $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is* δ-correct *if*

$$\mathrm{Exp}_{(ek,dk)\leftarrow\mathsf{Gen}(1^\kappa)}\left[\max_{\mu\in\mathcal{M}} \Pr[c \leftarrow \mathsf{Enc}(ek,\mu) : \mathsf{Dec}(dk,c) \neq \mu]\right] \leq \delta.$$

In particular, we say that PKE is perfectly correct *if $\delta = 0$.*

We also define a key pair's accuracy.

Definition 3 (Accuracy [47]). *We say that a key pair (ek, dk) is* accurate *if for any $\mu \in \mathcal{M}$, $\Pr_{c\leftarrow\mathsf{Enc}(ek,\mu)}[\mathsf{Dec}(dk,c) = \mu] = 1$. If a key pair is not accurate, then we call it* inaccurate. *We note that if* PKE *is deterministic, then $\Pr_{(ek,dk)\leftarrow\mathsf{Gen}(1^\kappa)}[(ek,dk)$ is accurate$] \leq \delta$.*

Security Notions: We define pseudorandomness under chosen-ciphertext attacks (PR-CCA) and its strong version (SPR-CCA) with simulator $\mathcal{S}$ as a generalization of IND$-CCA-security in [46, 27]. We also review anonymity (ANON-CCA) [7] and robustness (SROB-CCA) [36]. We additionally define extended collision-freeness (XCFR), in which any efficient adversary cannot find a colliding ciphertext even if the adversary is given two decryption keys. Due to the space limit, we omit the definitions of the standard security notions (OW-CPA, IND-CPA, OW-CCA, and IND-CCA) [38, 8], weak robustness (WROB-CCA) and collision-freeness (WCFR-CCA and SCFR-CCA) [36].

Definition 4 (Security notions for PKE). *Let* $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be a PKE scheme. Let* $\mathcal{D}_{\mathcal{M}}$ *be a distribution over the message space* $\mathcal{M}$*. For any* $\mathcal{A}$ *and* goal-atk $\in \{\text{pr-cca}, \text{anon-cca}\}$*, we define its* goal-atk *advantage against* PKE *as follows:*

$$\mathsf{Adv}^{\text{goal-atk}}_{\mathsf{PKE}[,\mathcal{S}],\mathcal{A}}(\kappa) := \left|2\Pr[\mathsf{Expt}^{\text{goal-atk}}_{\mathsf{PKE}[,\mathcal{S}],\mathcal{A}}(\kappa) = 1] - 1\right|,$$

where $\mathsf{Expt}^{\text{goal-atk}}_{\mathsf{PKE}[,\mathcal{S}],\mathcal{A}}(\kappa)$ *is an experiment described in Figure 1 and* $\mathcal{S}$ *is a PPT simulator.*
For any $\mathcal{A}$ *and* goal-atk $\in \{\text{srob-cca}, \text{xcfr}\}$*, we define its* goal-atk *advantage against* PKE *as follows:*

$$\mathsf{Adv}^{\text{goal-atk}}_{\mathsf{PKE}[,\mathcal{D}_{\mathcal{M}}],\mathcal{A}}(\kappa) := \Pr[\mathsf{Expt}^{\text{goal-atk}}_{\mathsf{PKE}[,\mathcal{D}_{\mathcal{M}}],\mathcal{A}}(\kappa) = 1],$$

where $\mathsf{Expt}^{\text{goal-atk}}_{\mathsf{PKE}[,\mathcal{D}_{\mathcal{M}}],\mathcal{A}}(\kappa)$ *is an experiment described in Figure 1.*
For GOAL-ATK $\in \{\text{PR-CCA}, \text{ANON-CCA}, \text{SROB-CCA}, \text{XCFR}\}$*, we say that* PKE *is* GOAL-ATK*-secure if* $\mathsf{Adv}^{\text{goal-atk}}_{\mathsf{PKE}[,\mathcal{D}_{\mathcal{M}},\mathcal{S}],\mathcal{A}}(\kappa)$ *is negligible for any QPT adversary* $\mathcal{A}$*. We also say that* PKE *is* SPR-CCA*-secure if it is* PR-CCA*-secure, and its simulator ignores* ek*. We also say that* PKE *is* GOAL-CPA*-secure if it is* GOAL-CCA*-secure even without the decryption oracle.*

We observe that strong pseudorandomness of PKE/KEM immediately implies anonymity of PKE/KEM, which may be folklore. We give the proof in the full version for completeness.

Theorem 1. *If* PKE/KEM *is* SPR-CCA*-secure, then it is* ANON-CCA*-secure.*

Disjoint simulatability: We review disjoint simulatability defined in [39].

Definition 5 (Disjoint simulatability [39]). *Let* $\mathcal{D}_{\mathcal{M}}$ *denote an efficiently sampleable distribution on a set* $\mathcal{M}$*. A deterministic PKE scheme* $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *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 followings:*

- *(Statistical disjointness:)*

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

  is negligible.

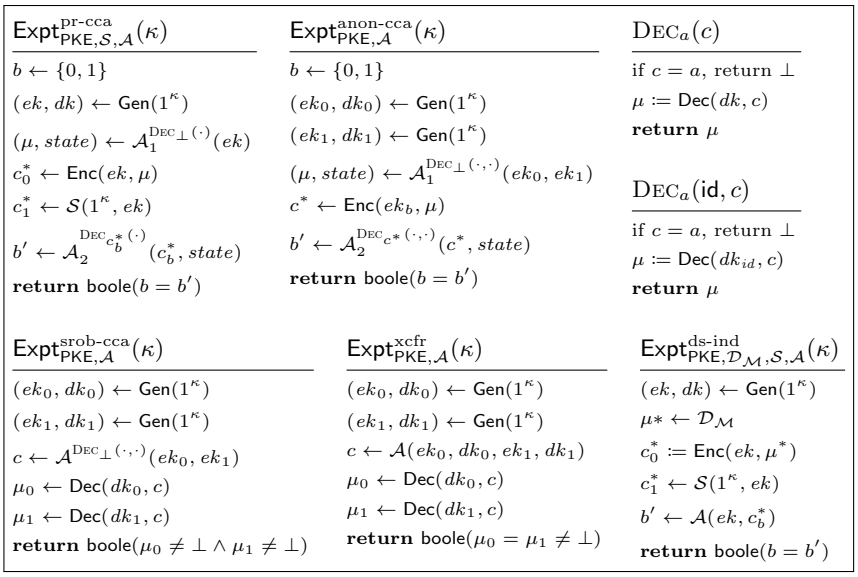

Fig. 1. Games for PKE schemes

– *(Ciphertext-indistinguishability:) For any QPT adversary $\mathcal{A}$, its* ds-ind *advantage* $\mathsf{Adv}^{\text{ds-ind}}_{\mathsf{PKE},\mathcal{D}_\mathcal{M},\mathcal{S},\mathcal{A}}(\kappa)$ *is negligible: The advantage is defined as*

$$\mathsf{Adv}^{\text{ds-ind}}_{\mathsf{PKE},\mathcal{D}_\mathcal{M},\mathcal{S},\mathcal{A}}(\kappa) := \left|2\Pr[\mathsf{Expt}^{\text{ds-ind}}_{\mathsf{PKE},\mathcal{D}_\mathcal{M},\mathcal{S},\mathcal{A}}(\kappa) = 1] - 1\right|,$$

where $\mathsf{Expt}^{\text{ds-ind}}_{\mathsf{PKE},\mathcal{D}_\mathcal{M},\mathcal{S},\mathcal{A}}(\kappa)$ *is an experiment described in Figure 1 and $\mathcal{S}$ is a PPT simulator.*

Liu and Wang gave a slightly modified version of statistical disjointness in [33]. As they noted, their definition below is enough to show the security proof:

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

Definition 6 (strong disjoint-simulatability). *We call* PKE *has* strong disjoint-simulatability *if $\mathcal{S}$ ignores ek.*

Remark 3. We note that a deterministic PKE scheme produced by TPunc [39] or Punc [29] is not *strongly* disjoint-simulatable, because their simulator outputs a random ciphertext $\mathsf{Enc}(ek, \hat{\mu})$ of a special plaintext $\hat{\mu}$.

2.2 Key Encapsulation Mechanism (KEM)

The model for KEM schemes is summarized as follows:

Definition 7. *A KEM scheme* KEM *consists of the following triple of polynomial-time algorithms* $(\overline{\mathsf{Gen}}, \overline{\mathsf{Enc}}, \overline{\mathsf{Dec}})$*:*

– $\overline{\mathsf{Gen}}(1^\kappa) \to (ek, dk)$: *a key-generation algorithm that on input* 1^κ*, where* κ *is the security parameter, outputs a pair of keys* (ek, dk)*. ek and dk are called the encapsulation key and decapsulation key, respectively.*
– $\overline{\mathsf{Enc}}(ek) \to (c, K)$: *an encapsulation algorithm that takes as input encapsulation key ek and outputs ciphertext* $c \in \mathcal{C}$ *and key* $K \in \mathcal{K}$*.*
– $\overline{\mathsf{Dec}}(dk, c) \to K/\perp$: *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 8 (δ-Correctness). *Let* $\delta = \delta(\kappa)$*. We say that* $\mathsf{KEM} = (\overline{\mathsf{Gen}}, \overline{\mathsf{Enc}}, \overline{\mathsf{Dec}})$ *is* δ-correct *if*

$$\Pr[(ek, dk) \leftarrow \overline{\mathsf{Gen}}(1^\kappa), (c, K) \leftarrow \overline{\mathsf{Enc}}(ek) : \overline{\mathsf{Dec}}(dk, c) \neq K] \leq \delta(\kappa).$$

In particular, we say that KEM *is* perfectly correct *if* $\delta = 0$*.*

Security: We define pseudorandomness under chosen-ciphertext attacks (PR-CCA) and its strong version (SPR-CCA) with simulator $\mathcal{S}$ as a generalization of IND$-CCA-security in [46, 27]. We also review anonymity (ANON-CCA), robustness (SROB-CCA), and collision-freeness (SCFR-CCA) [24]. We also define *smoothness* under chosen-ciphertext attacks (denoted by SMT-CCA) by following smoothness of hash proof system [16]. Due to the space limit, we omit the definitions of the standard security notions (OW-CPA, IND-CPA, OW-CCA, and IND-CCA) and weak robustness (WROB-CCA) and weak collision-freeness (WCFR-CCA) [24].

Definition 9 (Security notions for KEM). *Let* $\mathsf{KEM} = (\overline{\mathsf{Gen}}, \overline{\mathsf{Enc}}, \overline{\mathsf{Dec}})$ *be a KEM scheme.*
For any $\mathcal{A}$ *and* goal-atk $\in \{\text{pr-cca}, \text{anon-cca}, \text{smt-cca}\}$*, we define its* goal-atk *advantage against* KEM *as follows:*

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

where $\mathsf{Expt}^{\text{goal-atk}}_{\mathsf{KEM}[,\mathcal{S}],\mathcal{A}}(\kappa)$ *is an experiment described in Figure 1 and* $\mathcal{S}$ *is a PPT simulator.*
For any $\mathcal{A}$ *and* goal-atk $\in \{\text{srob-cca}, \text{scfr-cca}\}$*, we define its* goal-atk *advantage against* KEM *as follows:*

$$\mathsf{Adv}^{\text{goal-atk}}_{\mathsf{KEM},\mathcal{A}}(\kappa) := \Pr[\mathsf{Expt}^{\text{goal-atk}}_{\mathsf{KEM},\mathcal{A}}(\kappa) = 1],$$

where $\mathsf{Expt}^{\text{goal-atk}}_{\mathsf{KEM},\mathcal{A}}(\kappa)$ *is an experiment described in Figure 1.*
For GOAL-ATK $\in \{$PR-CCA, ANON-CCA, SMT-CCA, SROB-CCA, SCFR-CCA$\}$*, we say that* KEM *is* GOAL-ATK*-secure if* $\mathsf{Adv}^{\text{goal-atk}}_{\mathsf{KEM}[,\mathcal{S}],\mathcal{A}}(\kappa)$ *is negligible for any QPT adversary* $\mathcal{A}$*. We say that* KEM *is* SPR-CCA*-secure or* SSMT-CCA*-secure if it is* PR-CCA*-secure or* SMT-CCA*-secure and its simulator ignores ek, respectively. We say that* KEM *is* wANON-CCA*-secure if it is* ANON-CCA*-secure where the input to the adversary is* (ek_0, ek_1, c^*)*. We also say that* KEM *is* GOAL-CPA*-secure if it is* GOAL-CCA*-secure even without the decapsulation oracle.*

We additionally define ϵ-sparseness for KEM with explicit rejection.

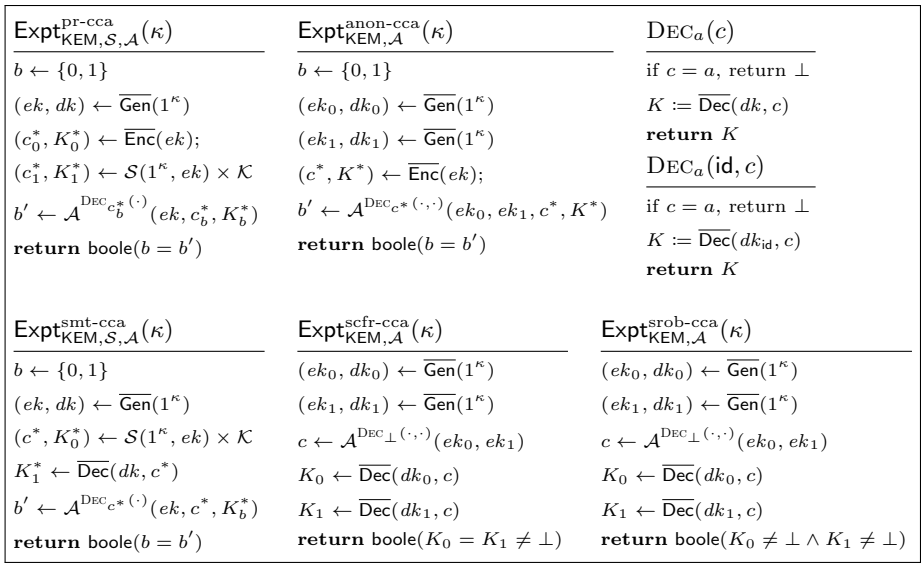

Fig. 2. Games for KEM schemes

Definition 10. *Let $\mathcal{S}$ be a simulator for the* PR-CCA *security. We say that* KEM *is* ϵ-sparse *if*

$$\Pr[(ek, dk) \leftarrow \overline{\mathsf{Gen}}(1^\kappa), c^* \leftarrow \mathcal{S}(1^\kappa, ek) : \overline{\mathsf{Dec}}(dk, c) \neq \perp] \leq \epsilon.$$

2.3 Data Encapsulation Mechanism (DEM)

The model for DEM schemes is summarized as follows:

Definition 11. *A DEM scheme* DEM *consists of the following triple of polynomial-time algorithms* (E, D) *with key space $\mathcal{K}$ and message space $\mathcal{M}$:*

- $\mathsf{E}(K, \mu) \to d$*: an encapsulation algorithm that takes as input key K and data μ and outputs ciphertext d.*
- $\mathsf{D}(K, d) \to m/\perp$*: a decapsulation algorithm that takes as input key K and ciphertext d and outputs data μ or a rejection symbol $\perp \notin \mathcal{M}$.*

Definition 12 (Correctness). *We say* $\mathsf{DEM} = (\mathsf{E}, \mathsf{D})$ *has* perfect correctness *if for any $K \in \mathcal{K}$ and any $\mu \in \mathcal{M}$, we have*

$$\Pr[\mathsf{D}(K, d) = \mu : d \leftarrow \mathsf{E}(K, \mu)] = 1.$$

Security: We review pseudorandomness under chosen-ciphertext attacks (PR-CCA) and pseudorandomness under one-time chosen-ciphertext attacks (PR-otCCA). We also review integrity of ciphertext (INT-CTXT). Robustness of DEM (FROB) are taken from Farshim, Orlandi, and Roşi [19]. Due to the space limit, we omit the definitions of the standard security notion IND-CCA and robustness (XROB) [19].

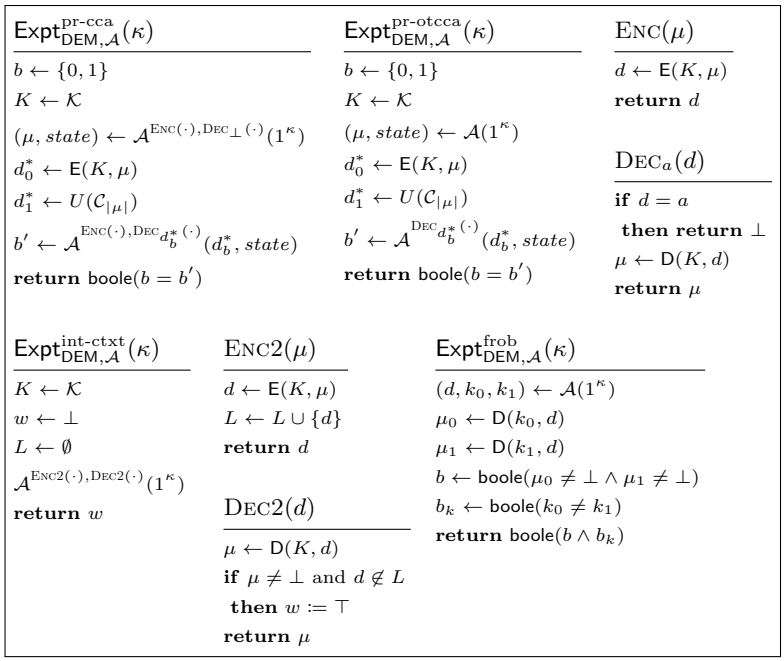

Fig. 3. Games for DEM schemes

Definition 13 (Security notions for DEM). *Let* $\mathsf{DEM} = (\mathsf{E}, \mathsf{D})$ *be a DEM scheme whose key space is* $\mathcal{K}$*. For* $\mu \in \mathcal{M}$*, let* $\mathcal{C}_{|\mu|}$ *be a ciphertext space defined by the length of message* μ*.*
For any $\mathcal{A}$ *and* goal-atk $\in \{\text{pr-cca}, \text{pr-otcca}\}$*, we define its* goal-atk *advantage against* DEM *as follows:*

$$\mathsf{Adv}^{\text{goal-atk}}_{\mathsf{DEM},\mathcal{A}}(\kappa) := \left|2\Pr[\mathsf{Expt}^{\text{goal-atk}}_{\mathsf{DEM},\mathcal{A}}(\kappa) = 1] - 1\right|,$$

where $\mathsf{Expt}^{\text{goal-atk}}_{\mathsf{DEM},\mathcal{A}}(\kappa)$ *is an experiment described in Figure 1.*
For any $\mathcal{A}$ *and* goal-atk $\in \{\text{int-ctxt}, \text{frob}\}$*, we define its* goal-atk *advantage against* DEM *as follows:*

$$\mathsf{Adv}^{\text{goal-atk}}_{\mathsf{DEM},\mathcal{A}}(\kappa) := \Pr[\mathsf{Expt}^{\text{goal-atk}}_{\mathsf{DEM},\mathcal{A}}(\kappa) = 1],$$

where $\mathsf{Expt}^{\text{goal-atk}}_{\mathsf{DEM},\mathcal{A}}(\kappa)$ *is an experiment described in Figure 1.*
For GOAL-ATK $\in \{\text{PR-CCA}, \text{PR-OTCCA}, \text{INT-CTXT}, \text{FROB}\}$*, we say that* DEM *is* GOAL-ATK*-secure if* $\mathsf{Adv}^{\text{goal-atk}}_{\mathsf{DEM},\mathcal{A}}(\kappa)$ *is negligible for any QPT adversary* $\mathcal{A}$*.*

2.4 Review of Grubbs, Maram, and Paterson [24]

Grubbs et al. studied KEM's anonymity and hybrid PKE's anonymity and robustness by extending the results of Mohassel [36]. We use $\mathsf{KEM}^{\perp}$

and $\mathsf{KEM}^{\not\perp}$ to indicate KEM with explicit rejection and implicit rejection, respectively. For KEM with explicit rejection, they showed the following theorem which generalizes Mohassel's theorem [36]:

Theorem 2 ([24, Theorem 1]). *Let* $\mathsf{PKE}_{\mathsf{hy}} = \mathsf{Hyb}[\mathsf{KEM}^{\perp}, \mathsf{DEM}]$*, a hybrid PKE scheme obtained by composing* $\mathsf{KEM}^{\perp}$ *and* DEM*. (See Figure 4.)*

1. *If* $\mathsf{KEM}^{\perp}$ *is* wANON-CPA*-secure,* IND-CCA*-secure,* WROB-CCA*-secure, and* δ*-correct and* DEM *is* INT-CTXT*-secure, then* $\mathsf{PKE}_{\mathsf{hy}}$ *is* ANON-CCA*-secure.*
2. *If* $\mathsf{KEM}^{\perp}$ *is* SROB-CCA*-secure (and* WROB-CCA*-secure), then* $\mathsf{PKE}_{\mathsf{hy}}$ *is* SROB-CCA*-secure (and* WROB-CCA*-secure), respectively.*

Grubbs et al. [24] then treat KEM with implicit rejection, which is used in all NIST PQC Round 3 KEM candidates except HQC. Their results are related to the FO transform with implicit rejection, which is decomposed into two transforms, T and $\mathsf{U}^{\not\perp}$: T transforms a probabilistic PKE scheme PKE into a deterministic PKE scheme PKE_1 with a random oracle G; $\mathsf{U}^{\not\perp}$ transforms a deterministic PKE scheme PKE_1 into a probabilistic KEM KEM with a random oracle H. Roughly speaking, they showed the following two theorems on robustness and anonymity of hybrid PKE from KEM with implicit rejection:

Theorem 3 (Robustness of $\mathsf{PKE}_{\mathsf{hy}}$ [24, Theorem 2]). *Let* $\mathsf{PKE}_{\mathsf{hy}} = \mathsf{Hyb}[\mathsf{KEM}^{\not\perp}, \mathsf{DEM}]$*. If* $\mathsf{KEM}^{\not\perp}$ *is* SCFR-CCA*-secure (and* WCFR-CCA*-secure) and* DEM *is* FROB*-secure (and* XROB*-secure), then* $\mathsf{PKE}_{\mathsf{hy}}$ *is* SROB-CCA*-secure (and* WROB-CCA*-secure), respectively.*

Theorem 4 (Anonymity of $\mathsf{PKE}_{\mathsf{hy}}$ using $\mathsf{FO}^{\not\perp}$ [24, Theorem 7]). *Let* $\mathsf{PKE}_{\mathsf{hy}} = \mathsf{Hyb}[\mathsf{KEM}^{\not\perp}, \mathsf{DEM}]$*. If* PKE *is* δ*-correct, and* γ*-spreading,* $\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ *is* WCFR-CPA*-secure,* $\mathsf{KEM}^{\not\perp} = \mathsf{FO}^{\not\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}]$ *is* ANON-CCA*-secure and* IND-CCA*-secure,* DEM *is* INT-CTXT*-secure, then* $\mathsf{PKE}_{\mathsf{hy}}$ *is* ANON-CCA*-secure.*

They also showed that the following theorem:

Theorem 5 (Anonymity of $\mathsf{KEM}^{\not\perp}$ using $\mathsf{FO}^{\not\perp}$ [24, Theorem 5]). *If* PKE *is* wANON-CPA*-secure,* OW-CPA*-secure, and* δ*-correct, and* $\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ *is* SCFR-CPA*-secure, then a KEM scheme* $\mathsf{KEM} = \mathsf{FO}^{\not\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}]$ *is* ANON-CCA*-secure.*

Grubbs et al. reduced from the wANON-CPA-security of PKE to the ANON-CCA-security of KEM. We note that there are two decapsulation oracles in the security game of the ANON-CCA-security of KEM. Thus, they need to simulate *both* decapsulation oracles without secrets. Jiang et al. [31] used the simulation trick that replaces $\mathsf{H}(\mu, c)$ with $\mathsf{H}_q(\mathsf{Enc}(ek, \mu))$ if $c = \mathsf{Enc}(ek, \mu)$ and $\mathsf{H}'_q(\mu, c)$ else, which helps the simulation of the decapsulation oracle without secrets in the QROM. Grubbs et al. extended this trick to simulate *two* decapsulation oracles by replacing $\mathsf{H}(\mu, c)$ with $\mathsf{H}_{q,i}(\mathsf{Enc}(ek_i, \mu))$ if $c = \mathsf{Enc}(ek_i, \mu)$ and $\mathsf{H}'_q(\mu, c)$ else. Notice that this extended simulation heavily depends on the fact that H takes μ and c and the SCFR-CCA-security of PKE_1. If the random oracle takes μ only, their trick fails the simulation.

3 Strong Pseudorandomness of Hybrid PKE

The hybrid PKE $\mathsf{PKE}_{\mathsf{hy}} = (\mathsf{Gen}_{\mathsf{hy}}, \mathsf{Enc}_{\mathsf{hy}}, \mathsf{Dec}_{\mathsf{hy}})$ constructed from $\mathsf{KEM} = (\overline{\mathsf{Gen}}, \overline{\mathsf{Enc}}, \overline{\mathsf{Dec}})$ and $\mathsf{DEM} = (\mathsf{E}, \mathsf{D})$ is summarized as in Figure 4

$\mathsf{Gen}_{\mathsf{hy}}(1^\kappa)$	$\mathsf{Enc}_{\mathsf{hy}}(ek, \mu)$	$\mathsf{Dec}_{\mathsf{hy}}(dk, ct = (c, d))$
$(ek, dk) \leftarrow \overline{\mathsf{Gen}}(1^\kappa)$	$(c, K) \leftarrow \overline{\mathsf{Enc}}(ek)$	$K' \leftarrow \overline{\mathsf{Dec}}(dk, c)$
return (ek, dk)	$d \leftarrow \mathsf{E}(K, \mu)$	**if** $K' = \perp$ **then return** $\perp$
	return $ct := (c, d)$	$\mu' \leftarrow \mathsf{D}(K', d)$
		if $\mu' = \perp$ **then return** $\perp$
		return μ'

Fig. 4. $\mathsf{PKE}_{\mathsf{hy}} = \mathsf{Hyb}[\mathsf{KEM}, \mathsf{DEM}]$

We show the following two theorems on strong pseudorandomness and anonymity of a hybrid PKE:

Theorem 6 (Case for KEM with Explicit Rejection). *Let* $\mathsf{PKE}_{\mathsf{hy}} = (\mathsf{Gen}_{\mathsf{hy}}, \mathsf{Enc}_{\mathsf{hy}}, \mathsf{Dec}_{\mathsf{hy}})$ *be a hybrid encryption scheme obtained by composing a KEM scheme* $\mathsf{KEM}^{\perp} = (\overline{\mathsf{Gen}}, \overline{\mathsf{Enc}}, \overline{\mathsf{Dec}})$ *and a DEM scheme* $\mathsf{DEM} = (\mathsf{E}, \mathsf{D})$ *that share key space* $\mathcal{K}$*. If* $\mathsf{KEM}^{\perp}$ *is* SPR-CCA*-secure,* δ*-correct with negligible* δ*, and* ϵ*-sparse and* DEM *is* PR-OTCCA*-secure and* INT-CTXT*-secure, then* $\mathsf{PKE}_{\mathsf{hy}}$ *is* SPR-CCA*-secure (and* ANON-CCA*-secure).*

Theorem 7 (Case for KEM with Implicit Rejection). *Let* $\mathsf{PKE}_{\mathsf{hy}} = (\mathsf{Gen}_{\mathsf{hy}}, \mathsf{Enc}_{\mathsf{hy}}, \mathsf{Dec}_{\mathsf{hy}})$ *be a hybrid encryption scheme obtained by composing a KEM scheme* $\mathsf{KEM}^{\not\perp} = (\overline{\mathsf{Gen}}, \overline{\mathsf{Enc}}, \overline{\mathsf{Dec}})$ *and a DEM scheme* $\mathsf{DEM} = (\mathsf{E}, \mathsf{D})$ *that share key space* $\mathcal{K}$*. If* $\mathsf{KEM}^{\not\perp}$ *is* SPR-CCA*-secure,* SSMT-CCA*-secure, and* δ*-correct with negligible* δ *and* DEM *is* PR-OTCCA*-secure, then* $\mathsf{PKE}_{\mathsf{hy}}$ *is* SPR-CCA*-secure (and* ANON-CCA*-secure).*

We here prove Theorem 7 and give the proof of Theorem 6 in the full version.

3.1 Proof of Theorem 7

Let us consider Game_i for $i = 0, \ldots, 6$. We summarize the games in Table 2. Let S_i denote the event that the adversary outputs $b' = 1$ in Game_i.
Let $\mathcal{S}$ be the simulator for the SPR-CCA security of $\mathsf{KEM}^{\not\perp}$. We define $\mathcal{S}_{\mathsf{hy}}(1^\kappa, |\mu^*|) := \mathcal{S}(1^\kappa) \times U(\mathcal{C}_{|\mu^*|})$ be the simulator for the SPR-CCA security of $\mathsf{PKE}_{\mathsf{hy}}$.
The security proof is similar to the security proof of the IND-CCA security of KEM/DEM [17] for $\mathsf{Game}_0, \ldots, \mathsf{Game}_4$. We need to take care of pseudorandom ciphertexts when moving from Game_4 to Game_5 and require the SSMT-CCA security of $\mathsf{KEM}^{\not\perp}$.

Table 2. Summary of Games for the Proof of Theorem 7

Game	c^* and K^*	d^*	Decryption	Justification
Game_0	$\overline{\mathsf{Enc}}(ek)$	$\mathsf{E}(K^*, \mu^*)$		
Game_1	$\overline{\mathsf{Enc}}(ek)$ at first	$\mathsf{E}(K^*, \mu^*)$		conceptual change
Game_2	$\overline{\mathsf{Enc}}(ek)$ at first	$\mathsf{E}(K^*, \mu^*)$	use K^* if $c = c^*$	δ-correctness of $\mathsf{KEM}^{\not\perp}$
Game_3	$\mathcal{S}(1^\kappa) \times U(\mathcal{K})$ at first	$\mathsf{E}(K^*, \mu^*)$	use K^* if $c = c^*$	SPR-CCA security of $\mathsf{KEM}^{\not\perp}$
Game_4	$\mathcal{S}(1^\kappa) \times U(\mathcal{K})$ at first	$U(\mathcal{C}_{\lvert\mu^*\rvert})$	use K^* if $c = c^*$	SPR-OTCCA security of DEM
Game_5	$\mathcal{S}(1^\kappa) \times U(\mathcal{K})$ at first	$U(\mathcal{C}_{\lvert\mu^*\rvert})$		SSMT-CCA security of $\mathsf{KEM}^{\not\perp}$
Game_6	$\mathcal{S}(1^\kappa) \times U(\mathcal{K})$	$U(\mathcal{C}_{\lvert\mu^*\rvert})$		conceptual change

Game_0: This is the original game $\mathsf{Expt}^{\text{spr-cca}}_{\mathsf{PKE}_{\mathsf{hy}},\mathcal{S}_{\mathsf{hy}},\mathcal{A}}(\kappa)$ with $b = 0$. Given μ^*, the challenge ciphertext is computed as follows:

$$(c^*, K^*) \leftarrow \overline{\mathsf{Enc}}(ek); d^* \leftarrow \mathsf{E}(K^*, \mu^*);\ \text{return}\ ct^* = (c^*, d^*).$$

We have

$$\Pr[S_0] = 1 - \Pr[\mathsf{Expt}^{\text{spr-cca}}_{\mathsf{PKE}_{\mathsf{hy}},\mathcal{S}_{\mathsf{hy}},\mathcal{A}}(\kappa) = 1 \mid b = 0].$$

Game_1: In this game, c^*_0 and K^*_0 are generated before invoking $\mathcal{A}$ with ek. This change is just conceptual, and we have

$$\Pr[S_0] = \Pr[S_1].$$

Game_2: In this game, the decryption oracle uses K^* if $c = c^*$ instead of $K = \overline{\mathsf{Dec}}(dk, c^*)$. Game_1 and Game_2 differ if correctly generated ciphertext c^* with K^* is decapsulated into different $K \neq K^*$ or $\perp$, which violates the correctness and occurs with probability at most δ. Hence, the difference of Game_1 and Game_2 is bounded by δ, and we have

$$|\Pr[S_1] - \Pr[S_2]| \leq \delta.$$

We note that this corresponds to the event $\mathsf{BadKeyPair}$ in [17].

Game_3: In this game, the challenger uses random (c^*, K^*) and uses K^* in DEM. The challenge ciphertext is generated as follows:

$$(c^*, K^*) \leftarrow \mathcal{S}(1^\kappa) \times U(\mathcal{K}); d^+ \leftarrow \mathsf{E}(K^*, \mu^*);\ \text{return}\ ct^* = (c^*, d^+).$$

The difference is bounded by SPR-CCA security of $\mathsf{KEM}^{\not\perp}$: There is an adversary $\mathcal{A}_{23}$ whose running time is approximately the same as that of $\mathcal{A}$ satisfying

$$|\Pr[S_2] - \Pr[S_3]| \leq \mathsf{Adv}^{\text{spr-cca}}_{\mathsf{KEM}^{\not\perp},\mathcal{S},\mathcal{A}_{23}}(\kappa).$$

We omit the detail of $\mathcal{A}_{23}$ since it is straightforward.

Game_4: In this game, the challenger uses random d^*. The challenge ciphertext is generated as follows:

$$(c^*, K^*) \leftarrow \mathcal{S}(1^\kappa) \times \mathcal{K}; d^* \leftarrow U(\mathcal{C}_{\lvert\mu^*\rvert});\ \text{return}\ ct^* = (c^*, d^*).$$

The difference is bounded by SPR-OTCCA security of DEM: There is an adversary $\mathcal{A}_{34}$ whose running time is approximately the same as that of $\mathcal{A}$ satisfying

$$|\Pr[S_3] - \Pr[S_4]| \leq \mathsf{Adv}^{\text{spr-otcca}}_{\mathsf{DEM},\mathcal{A}_{34}}(\kappa).$$

We omit the detail of $\mathcal{A}_{34}$ since it is straightforward.

Game_5: We replace the decryption oracle defined as follows: If given $ct = (c^*, d)$, the decryption oracle uses $K = \overline{\mathsf{Dec}}(dk, c^*)$ instead of K^*. The difference is bounded by SSMT-CCA security of $\mathsf{KEM}^{\not\perp}$: There is an adversary $\mathcal{A}_{45}$ whose running time is approximately the same as that of $\mathcal{A}$ satisfying

$$|\Pr[S_4] - \Pr[S_5]| \leq \mathsf{Adv}^{\text{ssmt-cca}}_{\mathsf{KEM}^{\not\perp},\mathcal{S},\mathcal{A}_{45}}(\kappa).$$

We omit the detail of $\mathcal{A}_{45}$ since it is straightforward.

Game_6: We finally change the timing of the generation of (c^*, K^*). This change is just conceptual, and we have

$$\Pr[S_5] = \Pr[S_6].$$

Notice that this is the original game $\mathsf{Expt}^{\text{spr-cca}}_{\mathsf{PKE}_{\mathsf{hy}},\mathcal{S}_{\mathsf{hy}},\mathcal{A}}(\kappa)$ with $b = 1$, thus, we have

$$\Pr[S_6] = \Pr[\mathsf{Expt}^{\text{spr-cca}}_{\mathsf{PKE}_{\mathsf{hy}},\mathcal{S}_{\mathsf{hy}},\mathcal{A}}(\kappa) = 1 \mid b = 1].$$

Summing the (in)equalities, we obtain the bound in the statement as follows:

$$\begin{aligned}\mathsf{Adv}^{\text{spr-cca}}_{\mathsf{PKE}_{\mathsf{hy}},\mathcal{S}_{\mathsf{hy}}\mathcal{A}}(\kappa) &= |\Pr[S_0] - \Pr[S_6]| \leq \sum_i |\Pr[S_i] - \Pr[S_{i+1}]| \\ &\leq \delta + \mathsf{Adv}^{\text{spr-cca}}_{\mathsf{KEM}^{\not\perp},\mathcal{S},\mathcal{A}_{23}}(\kappa) + \mathsf{Adv}^{\text{spr-otcca}}_{\mathsf{DEM},\mathcal{A}_{34}}(\kappa) + \mathsf{Adv}^{\text{ssmt-cca}}_{\mathsf{KEM}^{\not\perp},\mathcal{S},\mathcal{A}_{45}}(\kappa).\end{aligned}$$

□

4 Properties of SXY

Let us review SXY [39] as known as $\mathsf{U}^{\not\perp}_m$ with explicit re-encryption check [26].

Let $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a deterministic PKE scheme. Let $\mathcal{M}$, $\mathcal{C}$, and $\mathcal{K}$ be a plaintext, ciphertext, and key space of PKE, respectively. Let $\mathsf{H}\colon \mathcal{M} \to \mathcal{K}$ and $\mathsf{H}_{\mathsf{prf}}\colon \{0,1\}^\ell \times \mathcal{C} \to \mathcal{K}$ be hash functions modeled by random oracles. $\mathsf{KEM} = (\overline{\mathsf{Gen}}, \overline{\mathsf{Enc}}, \overline{\mathsf{Dec}}) = \mathsf{SXY}[\mathsf{PKE}, \mathsf{H}, \mathsf{H}_{\mathsf{prf}}]$ is defined as in Figure 5.

$\overline{\mathsf{Gen}}(1^\kappa)$	$\overline{\mathsf{Enc}}(ek)$	$\overline{\mathsf{Dec}}(\overline{dk}, c)$, where $\overline{dk} = (dk, ek, s)$
$(ek, dk) \leftarrow \mathsf{Gen}(1^\kappa)$	$\mu \leftarrow \mathcal{D}_{\mathcal{M}}$	$\mu' \leftarrow \mathsf{Dec}(dk, c)$
$s \leftarrow \{0,1\}^\ell$	$c := \mathsf{Enc}(ek, \mu)$	**if** $\mu' = \perp$ or $c \neq \mathsf{Enc}(ek, \mu')$
$\overline{dk} := (dk, ek, s)$	$K := \mathsf{H}(\mu)$	**then return** $K := \mathsf{H}_{\mathsf{prf}}(s, c)$
return $(ek, \overline{dk})$	**return** (c, K)	**else return** $K := \mathsf{H}(\mu')$

Fig. 5. $\mathsf{KEM} = \mathsf{SXY}[\mathsf{PKE}, \mathsf{H}, \mathsf{H}_{\mathsf{prf}}]$

Table 3. Summary of games for the proof of Theorem 8

Game	H	c^*	K^*	Decapsulation: valid c	Decapsulation: invalid c	Justification
Game_0	$\mathsf{H}(\cdot)$	$\mathsf{Enc}(ek, \mu^*)$	$\mathsf{H}(\mu^*)$	$\mathsf{H}(\mu)$	$\mathsf{H}_{\mathsf{prf}}(s, c)$	
Game_1	$\mathsf{H}(\cdot)$	$\mathsf{Enc}(ek, \mu^*)$	$\mathsf{H}(\mu^*)$	$\mathsf{H}(\mu)$	$\mathsf{H}_q(c)$	Lemma 2
$\mathsf{Game}_{1.5}$	$\mathsf{H}'_q(\mathsf{Enc}(ek, \cdot))$	$\mathsf{Enc}(ek, \mu^*)$	$\mathsf{H}(\mu^*)$	$\mathsf{H}(\mu)$	$\mathsf{H}_q(c)$	key's accuracy
Game_2	$\mathsf{H}_q(\mathsf{Enc}(ek, \cdot))$	$\mathsf{Enc}(ek, \mu^*)$	$\mathsf{H}(\mu^*)$	$\mathsf{H}(\mu)$	$\mathsf{H}_q(c)$	key's accuracy
Game_3	$\mathsf{H}_q(\mathsf{Enc}(ek, \cdot))$	$\mathsf{Enc}(ek, \mu^*)$	$\mathsf{H}_q(c^*)$	$\mathsf{H}_q(c)$	$\mathsf{H}_q(c)$	key's accuracy
Game_4	$\mathsf{H}_q(\mathsf{Enc}(ek, \cdot))$	$\mathcal{S}(1^\kappa)$	$\mathsf{H}_q(c^*)$	$\mathsf{H}_q(c)$	$\mathsf{H}_q(c)$	ciphertext indistinguishability
Game_5	$\mathsf{H}_q(\mathsf{Enc}(ek, \cdot))$	$\mathcal{S}(1^\kappa)$	$U(\mathcal{K})$	$\mathsf{H}_q(c)$	$\mathsf{H}_q(c)$	statistical disjointness
Game_6	$\mathsf{H}_q(\mathsf{Enc}(ek, \cdot))$	$\mathcal{S}(1^\kappa)$	$U(\mathcal{K})$	$\mathsf{H}(\mu)$	$\mathsf{H}_q(c)$	key's accuracy
$\mathsf{Game}_{6.5}$	$\mathsf{H}'_q(\mathsf{Enc}(ek, \cdot))$	$\mathcal{S}(1^\kappa)$	$U(\mathcal{K})$	$\mathsf{H}(\mu)$	$\mathsf{H}_q(c)$	key's accuracy
Game_7	$\mathsf{H}(\cdot)$	$\mathcal{S}(1^\kappa)$	$U(\mathcal{K})$	$\mathsf{H}(\mu)$	$\mathsf{H}_q(c)$	key's accuracy
Game_8	$\mathsf{H}(\cdot)$	$\mathcal{S}(1^\kappa)$	$U(\mathcal{K})$	$\mathsf{H}(\mu)$	$\mathsf{H}_{\mathsf{prf}}(s, c)$	Lemma 2

4.1 SPR-CCA Security

We first show that KEM is strongly pseudorandom if the underlying PKE is strongly disjoint-simulatable.

Theorem 8. *Suppose that a ciphertext space $\mathcal{C}$ of PKE depends on the public parameter only. If PKE is strongly disjoint-simulatable and δ-correct with negligible δ, then $\mathsf{KEM} = \mathsf{SXY}[\mathsf{PKE}, \mathsf{H}, \mathsf{H}_{\mathsf{prf}}]$ is* SPR-CCA*-secure.*

Correctly speaking, the bound of the advantage differ if PKE is derandomized by T. See the full version for the detail.

Proof of Theorem 8: We use the game-hopping proof. We consider Game_i for $i = 0, \ldots, 8$. We summarize the games in Table 3. Let S_i denote the event that the adversary outputs $b' = 1$ in game Game_i. Let Acc be an event that a key pair (ek, dk) is accurate. Let $\overline{\mathsf{Acc}}$ denote the event that a key pair (ek, dk) is inaccurate. We note that we have $\Pr[\mathsf{Acc}] \leq \delta$ since PKE is deterministic. We extend the security proof for IND-CCA security of SXY in [39, 47, 33].

Game_0*:* This game is the original game $\mathsf{Expt}^{\text{spr-cca}}_{\mathsf{KEM},\mathcal{A}}(\kappa)$ with $b = 0$. Thus, we have

$$\Pr[S_0] = 1 - \Pr[\mathsf{Expt}^{\text{spr-cca}}_{\mathsf{KEM},\mathcal{A}}(\kappa) = 1 \mid b = 0].$$

Game_1*:* This game is the same as Game_0 except that $\mathsf{H}_{\mathsf{prf}}(s, c)$ in the decapsulation oracle is replace with $\mathsf{H}_q(c)$ where $\mathsf{H}_q \colon \mathcal{C} \to \mathcal{K}$ is another random oracle. We remark that $\mathcal{A}$ cannot access H_q directly.
As in [47, Lemmas 4.1], from Lemma 2 we have the bound

$$|\Pr[S_0] - \Pr[S_1]| \leq 2(q_{\mathsf{H}_{\mathsf{prf}}} + q_{\textsc{Dec}}) \cdot 2^{-\ell/2},$$

where $q_{\mathsf{H}_{\mathsf{prf}}}$ and $q_{\textsc{Dec}}$ denote the number of queries to $\mathsf{H}_{\mathsf{prf}}$ and $\textsc{Dec}$ the adversary makes, respectively.
In addition, according to Lemma 8, for any $p \geq 0$, we have

$$|\Pr[S_1] - p| \leq |\Pr[S_1 \wedge \mathsf{Acc}] - p| + \delta.$$

$\mathsf{Game}_{1.5}$*:* This game is the same as Game_1 except that the random oracle $\mathsf{H}(\cdot)$ is simulated by $\mathsf{H}'_q(\mathsf{Enc}(ek,\cdot))$ where $\mathsf{H}'_q\colon \mathcal{C} \to \mathcal{K}$ is yet another random oracle. We remark that the decapsulation oracle and the generation of K^* also use $\mathsf{H}'_q(\mathsf{Enc}(ek,\cdot))$ as $\mathsf{H}(\cdot)$.
If the key pair (ek, dk) is accurate, then $g(\mu) \coloneqq \mathsf{Enc}(ek,\mu)$ is *injective*. Thus, if the key pair is accurate, then $\mathsf{H}'_q \circ g\colon \mathcal{M} \to \mathcal{K}$ is a random function and the two games Game_1 and $\mathsf{Game}_{1.5}$ are equivalent Thus, we have

$$\Pr[S_1 \wedge \mathsf{Acc}] = \Pr[S_{1.5} \wedge \mathsf{Acc}].$$

Game_2*:* This game is the same as $\mathsf{Game}_{1.5}$ except that the random oracle H is simulated by $\mathsf{H}_q \circ g$ instead of $\mathsf{H}'_q \circ g$.
A ciphertext c is said to be *valid* if we have $\mathsf{Enc}(ek, \mathsf{Dec}(dk, c)) = c$ and *invalid* otherwise.
Notice that, in $\mathsf{Game}_{1.5}$, H_q is used for *invalid* ciphertext, and an adversary cannot access a value of H_q for a valid ciphertext. In addition, in $\mathsf{Game}_{1.5}$, an adversary can access a value of H'_q on input a valid ciphertext and cannot access a value of H'_q on input an invalid ciphertext if the key pair is accurate. Thus, there is no difference between $\mathsf{Game}_{1.5}$ and Game_2 if the key pair is accurate and we have

$$\Pr[S_{1.5} \wedge \mathsf{Acc}] = \Pr[S_2 \wedge \mathsf{Acc}].$$

Game_3*:* This game is the same as Game_2 except that K^* is set as $\mathsf{H}_q(c^*)$ and the decapsulation oracle always returns $\mathsf{H}'_q(c)$ as long as $c \neq c^*$. This decapsulation oracle will denoted by $\textsc{Dec}'$.
If the key pair is accurate, for a valid ciphertext c and its decrypted result μ, we have $\mathsf{H}(\mu) = \mathsf{H}_q(\mathsf{Enc}(ek,\mu)) = \mathsf{H}_q(c)$. Thus, the two games Game_2 and Game_3 are equivalent and we have

$$\Pr[S_2 \wedge \mathsf{Acc}] = \Pr[S_3 \wedge \mathsf{Acc}].$$

According to Lemma 8, for any $p \geq 0$, we have

$$|\Pr[S_3 \wedge \mathsf{Acc}] - p| \leq |\Pr[S_3] - p| + \delta.$$

Game_4*:* This game is the same as Game_3 except that c^* is generated by $\mathcal{S}(1^\kappa)$.
The difference between two games Game_3 and Game_4 is bounded by the advantage of ciphertext indistinguishability in disjoint simulatability as in [47, Lemma 4.7]. The reduction algorithm is obtained straightforwardly, and we omit it. We have

$$|\Pr[S_3] - \Pr[S_4]| \leq \mathsf{Adv}^{\text{ds-ind}}_{\mathsf{PKE},\mathcal{D}_\mathcal{M},\mathcal{S},\mathcal{A}_{34}}(\kappa).$$

Game_5*:* This game is the same as Game_4 except that $K^* \leftarrow \mathcal{K}$ instead of $K^* \leftarrow \mathsf{H}_q(c^*)$.
In Game_4, if $c^* \leftarrow \mathcal{S}(1^\kappa)$ is not in $\mathsf{Enc}(ek, \mathcal{M})$, then the adversary has no information about $K^* = \mathsf{H}_q(c^*)$ and thus, K^* looks uniformly at random. Hence, the difference between two games Game_4 and Game_5 is

bounded by the statistical disjointness in disjoint simulatability as in [47, Lemma 4.8]. We have

$$|\Pr[S_4] - \Pr[S_5]| \leq \mathsf{Disj}_{\mathsf{PKE},\mathcal{S}}(\kappa).$$

According to Lemma 8, for any $p \geq 0$, we have

$$|\Pr[S_5] - p| \leq |\Pr[S_5 \wedge \mathsf{Acc}] - p| + \delta.$$

Game_6: This game is the same as Game_5 except that the decapsulation oracle is reset as DEC. Similar to the case for Game_2 and Game_3, if a key pair is accurate, the two games Game_5 and Game_6 are equivalent as in the proof of [47, Lemma 4.5]. We have

$$\Pr[S_5 \wedge \mathsf{Acc}] = \Pr[S_6 \wedge \mathsf{Acc}].$$

$\mathsf{Game}_{6.5}$: This game is the same as Game_6 except that the random oracle H is simulated by $\mathsf{H}'_q \circ g$ where $\mathsf{H}'_q : \mathcal{C} \to \mathcal{K}$ is yet another random oracle as in $\mathsf{Game}_{1.2}$ instead of $\mathsf{H}_q \circ g$. If a key pair is accurate, then two games Game_6 and $\mathsf{Game}_{6.5}$ are equal to each other as the two games $\mathsf{Game}_{1.5}$ and Game_2 are equal to each other. We have

$$\Pr[S_6 \wedge \mathsf{Acc}] = \Pr[S_{6.5} \wedge \mathsf{Acc}].$$

Game_7: This game is the same as $\mathsf{Game}_{6.5}$ except that the random oracle $\mathsf{H}(\cdot)$ is set as the original. If a key pair is accurate, then the two games $\mathsf{Game}_{6.5}$ and Game_7 are equal to each other as the two games $\mathsf{Game}_{1.5}$ and Game_1 are equal to each other. We have

$$\Pr[S_{6.5} \wedge \mathsf{Acc}] = \Pr[S_7 \wedge \mathsf{Acc}].$$

According to Lemma 8, for any $p \geq 0$, we have

$$|\Pr[S_7 \wedge \mathsf{Acc}] - p| \leq |\Pr[S_7] - p| + \delta.$$

Game_8: This game is the same as Game_7 except that $\mathsf{H}_q(c)$ in the decapsulation oracle is replaced by $\mathsf{H}_{\mathsf{prf}}(s, c)$.
As we discussed the difference between the two games Game_0 and Game_1, from Lemma 2 we have the bound

$$|\Pr[S_7] - \Pr[S_8]| \leq 2(q_{\mathsf{H}_{\mathsf{prf}}} + q_{\mathrm{DEC}}) \cdot 2^{-\ell/2}.$$

We note that this game is the original game $\mathsf{Expt}^{\text{spr-cca}}_{\mathsf{KEM},\mathcal{A}}(\kappa)$ with $b = 1$. Thus, we have

$$\Pr[S_8] = \Pr[\mathsf{Expt}^{\text{spr-cca}}_{\mathsf{KEM},\mathcal{A}}(\kappa) = 1 \mid b = 1].$$

Summing those (in)equalities, we obtain the following bound:

$$\begin{aligned}\mathsf{Adv}^{\text{spr-cca}}_{\mathsf{KEM},\mathcal{A}}(\kappa) = |\Pr[S_0] - \Pr[S_8]| &\leq \sum_{i=0}^{7} |\Pr[S_i] - \Pr[S_{i+1}]| \\ &\leq \mathsf{Adv}^{\text{ds-ind}}_{\mathsf{PKE},\mathcal{D}_{\mathcal{M}},\mathcal{S},\mathcal{A}_{34}}(\kappa) + \mathsf{Disj}_{\mathsf{PKE},\mathcal{S}}(\kappa) \\ &\quad + 4(q_{\mathsf{H}_{\mathsf{prf}}} + q_{\mathrm{DEC}}) \cdot 2^{-\ell/2} + 4\delta.\end{aligned}$$

Table 4. Summary of games for the proof of Theorem 9: '$\mathcal{S}(1^\kappa) \setminus \mathsf{Enc}(ek, \mathcal{M})$' implies that the challenger generates $c^* \leftarrow \mathcal{S}(1^\kappa)$ and returns $\perp$ if $c^* \in \mathsf{Enc}(ek, \mathcal{M})$.

Game	c^*	K^*	Decapsulation: valid c	Decapsulation: invalid c	Justification
Game_0	$\mathcal{S}(1^\kappa)$	random	$\mathsf{H}(\mu)$	$\mathsf{H}_{\mathsf{prf}}(s, c)$	
Game_1	$\mathcal{S}(1^\kappa) \setminus \mathsf{Enc}(ek, \mathcal{M})$	random	$\mathsf{H}(\mu)$	$\mathsf{H}_{\mathsf{prf}}(s, c)$	statistical disjointness
Game_2	$\mathcal{S}(1^\kappa) \setminus \mathsf{Enc}(ek, \mathcal{M})$	random	$\mathsf{H}(\mu)$	$\mathsf{H}_q(c)$	Lemma 2
Game_3	$\mathcal{S}(1^\kappa) \setminus \mathsf{Enc}(ek, \mathcal{M})$	$\mathsf{H}_q(c^*)$	$\mathsf{H}(\mu)$	$\mathsf{H}_q(c)$	$\mathsf{H}_q(c^*)$ is hidden
Game_4	$\mathcal{S}(1^\kappa) \setminus \mathsf{Enc}(ek, \mathcal{M})$	$\mathsf{H}_{\mathsf{prf}}(s, c^*)$	$\mathsf{H}(\mu)$	$\mathsf{H}_{\mathsf{prf}}(s, c)$	Lemma 2
Game_5	$\mathcal{S}(1^\kappa) \setminus \mathsf{Enc}(ek, \mathcal{M})$	$\overline{\mathsf{Dec}}(dk, c^*)$	$\mathsf{H}(\mu)$	$\mathsf{H}_{\mathsf{prf}}(s, c)$	re-encryption check
Game_6	$\mathcal{S}(1^\kappa)$	$\overline{\mathsf{Dec}}(dk, c^*)$	$\mathsf{H}(\mu)$	$\mathsf{H}_{\mathsf{prf}}(s, c)$	statistical disjointness

4.2 SSMT-CCA Security

Theorem 9. *Suppose that a ciphertext space $\mathcal{C}$ of* PKE *depends on the public parameter only. If* PKE *is strongly disjoint-simulatable, then* $\mathsf{KEM} = \mathsf{SXY}[\mathsf{PKE}, \mathsf{H}, \mathsf{H}_{\mathsf{prf}}]$ *is* SSMT-CCA*-secure.*
Formally speaking, for any adversary $\mathcal{A}$ against SSMT-CCA *security of* KEM *issuing at most $q_{\mathsf{H}_{\mathsf{prf}}}$ and q_{DEC} queries to $\mathsf{H}_{\mathsf{prf}}$ and* DEC*, we have*

$$\mathsf{Adv}^{\text{ssmt-cca}}_{\mathsf{KEM},\mathcal{S},\mathcal{A}}(\kappa) \leq 2\mathsf{Disj}_{\mathsf{PKE},\mathcal{S}}(\kappa) + 4(q_{\mathsf{H}_{\mathsf{prf}}} + q_{\mathrm{DEC}}) \cdot 2^{-\ell/2}.$$

We note that this security proof is unrelated to PKE is deterministic PKE or one derandomized by T.

Proof: We use the game-hopping proof. We consider Game_i for $i = 0, \ldots, 6$. We summarize those games in Table 4. Let S_i denote the event that the adversary outputs $b' = 1$ in game Game_i.

Game_0*:* This game is the original game $\mathsf{Expt}^{\text{ssmt-cca}}_{\mathsf{KEM},\mathcal{S},\mathcal{A}}(\kappa)$ with $b = 0$. The challenge is generated as $c^* \leftarrow \mathcal{S}(1^\kappa)$ and $K^*_0 \leftarrow \mathcal{K}$. We have

$$\Pr[S_0] = 1 - \Pr[\mathsf{Expt}^{\text{ssmt-cca}}_{\mathsf{KEM},\mathcal{S},\mathcal{A}}(\kappa) = 1 \mid b = 0].$$

Game_1*:* In this game, the challenge ciphertext is set as $\perp$ if c^* is in $\mathsf{Enc}(ek, \mathcal{M})$. Since the difference between two games Game_0 and Game_1 is bounded by statistical disjointness, we have

$$|\Pr[S_0] - \Pr[S_1]| \leq \mathsf{Disj}_{\mathsf{PKE},\mathcal{S}}(\kappa).$$

Game_2*:* This game is the same as Game_1 except that $\mathsf{H}_{\mathsf{prf}}(s, c)$ in the decapsulation oracle is replace with $\mathsf{H}_q(c)$ where $\mathsf{H}_q \colon \mathcal{C} \to \mathcal{K}$ is another random oracle.
As in [47, Lemmas 4.1], from Lemma 2 we have the bound

$$|\Pr[S_1] - \Pr[S_2]| \leq 2(q_{\mathsf{H}_{\mathsf{prf}}} + q_{\mathrm{DEC}}) \cdot 2^{-\ell/2}.$$

Game_3*:* This game is the same as Game_2 except that K^* is set as $\mathsf{H}_q(c^*)$ instead of chosen randomly. Since c^* is always outside of $\mathsf{Enc}(ek, \mathcal{M})$, $\mathcal{A}$ cannot obtain any information about $\mathsf{H}_q(c^*)$. Hence, the two games Game_2 and Game_3 are equivalent and we have

$$\Pr[S_2] = \Pr[S_3].$$

Game_4: This game is the same as Game_3 except that $\mathsf{H}_q(\cdot)$ is replaced by $\mathsf{H}_{\mathsf{prf}}(s,\cdot)$. As in [47, Lemmas 4.1], from Lemma 2 we have the bound

$$|\Pr[S_3] - \Pr[S_4]| \leq 2(q_{\mathsf{H}_{\mathsf{prf}}} + q_{\mathrm{DEC}}) \cdot 2^{-\ell/2}.$$

Game_5: This game is the same as Game_4 except that K^* is set as $\overline{\mathsf{Dec}}(dk, c^*)$ instead of $\mathsf{H}_{\mathsf{prf}}(s, c^*)$. Recall that c^* is always in *outside* of $\mathsf{Enc}(ek, \mathcal{M})$. Thus, we always have $\mathsf{Dec}(c^*) = \bot$ or $\mathsf{Enc}(ek, \mathsf{Dec}(c^*)) \neq c^*$ and, thus, $K^* = \mathsf{H}_{\mathsf{prf}}(s, c^*)$ in Game_5. Hence, the two games are equivalent and we have

$$\Pr[S_4] = \Pr[S_5].$$

Game_6: We finally replace the way to compute c^*: In this game, the ciphertext is chosen by $\mathcal{S}(1^\kappa)$ as in Game_0. Again, since the difference between two games Game_5 and Game_6 is bounded by statistical disjointness, we have

$$|\Pr[S_5] - \Pr[S_6]| \leq \mathsf{Disj}_{\mathsf{PKE},\mathcal{S}}(\kappa).$$

Moreover, this game Game_6 is the original game $\mathsf{Expt}^{\text{ssmt-cca}}_{\mathsf{KEM},\mathcal{S},\mathcal{A}}(\kappa)$ with $b = 1$ and we have

$$\Pr[S_6] = \Pr[\mathsf{Expt}^{\text{ssmt-cca}}_{\mathsf{KEM},\mathcal{S},\mathcal{A}}(\kappa) = 1 \mid b = 1].$$

Summing those (in)equalities, we obtain Theorem 9:

$$\begin{aligned}\mathsf{Adv}^{\text{ssmt-cca}}_{\mathsf{KEM},\mathcal{S},\mathcal{A}}(\kappa) &= |\Pr[S_0] - \Pr[S_6]| \\ &\leq 2\mathsf{Disj}_{\mathsf{PKE},\mathcal{S}}(\kappa) + 4(q_{\mathsf{H}_{\mathsf{prf}}} + q_{\mathrm{DEC}}) \cdot 2^{-\ell/2}.\end{aligned}$$

4.3 SCFR-CCA Security

Theorem 10. *If* PKE *is* XCFR*-secure or* SCFR-CCA*-secure, then* $\mathsf{KEM} = \mathsf{SXY}[\mathsf{PKE}, \mathsf{H}, \mathsf{H}_{\mathsf{prf}}]$ *is* SCFR-CCA*-secure in the QROM.*

Proof. Suppose that an adversary against KEM's SCFR-CCA security outputs a ciphertext c which is decapsulated into $K \neq \bot$ by both $\overline{dk}_0$ and $\overline{dk}_1$, that is, $K = \overline{\mathsf{Dec}}(\overline{dk}_0, c) = \overline{\mathsf{Dec}}(\overline{dk}_1, c) \neq \bot$. For $i \in \{0,1\}$, we define μ'_i as an internal decryption result under dk_i, that is, $\mu'_i = \mathsf{Dec}(dk_i, c)$. For $i \in \{0,1\}$, we also define $\mu_i := \mu'_i$ if $c = \mathsf{Enc}(ek_i, \mu'_i)$ and $\mu_i := \bot$ otherwise.

We have five cases classified as follows:

- Case 1 ($\mu_0 = \mu_1 \neq \bot$): This $\mu_0 = \mu_1 \neq \bot$ violates the XCFR security (or the SCFR-CCA security) of the underlying PKE and it is easy to make a reduction.
- Case 2 ($\bot \neq \mu_0 \neq \mu_1 \neq \bot$): In this case, the decapsulation algorithm outputs $K = \mathsf{H}(\mu_0) = \mathsf{H}(\mu_1)$. Thus, we succeed to find a collision for H, which is negligible for any QPT adversary (Lemma 3).
- Case 3 ($\mu_0 = \bot$ and $\mu_1 \neq \bot$): In this case, the decapsulation algorithm outputs $K = \mathsf{H}_{\mathsf{prf}}(s_0, c) = \mathsf{H}(\mu_1)$ and we find a claw $((s_0, c), \mu_1)$ of $\mathsf{H}_{\mathsf{prf}}$ and H. The probability that we find such claw is negligible for any QPT adversary (Lemma 4).

– Case 4 ($\mu_0 \neq \bot$ and $\mu_1 = \bot$): In this case, the decapsulation algorithm outputs $K = \mathsf{H}(\mu_0) = \mathsf{H}_{\mathsf{prf}}(s_1, c)$ and we find a claw $(\mu_0, (s_1, c))$ of H and $\mathsf{H}_{\mathsf{prf}}$. The probability that we find such claw is negligible for any QPT adversary (Lemma 4).
– Case 5 (The other cases): In this case, we find a collision $((s_0, c), (s_1, c))$ of $\mathsf{H}_{\mathsf{prf}}$, which is indeed collision if $s_0 \neq s_1$ which occurs with probability at lease $1 - 1/2^\ell$. The probability that we find such collision is negligible for any QPT adversary (Lemma 3).

We conclude that the advantage of the adversary is negligible in any case. □

5 NTRU

We briefly review NTRU [14] in subsection 5.1, discuss the security properties of the underlying PKE, NTRU-DPKE, in subsection 5.2, and discuss the security properties of NTRU in subsection 5.3. We want to show that, under appropriate assumptions, NTRU is ANON-CCA-secure in the QROM, and NTRU leads to ANON-CCA-secure and SROB-CCA-secure hybrid PKE in the QROM. In order to do so, we show that the underlying NTRU-DPKE of NTRU is strongly disjoint-simulatable under the modified DSPR and PLWE assumptions and XCFR-secure in subsection 5.2. Since NTRU is obtained by applying SXY to NTRU-DPKE, the former implies that NTRU is SPR-CCA-secure and SSMT-CCA-secure in the QROM under those assumptions and the latter implies that NTRU is SCFR-CCA-secure in the QROM. Those three properties lead to the anonymity of NTRU and hybrid PKE in the QROM as we wanted.

5.1 Review of NTRU

Preliminaries: Φ_1 denotes the polynomial $x - 1$ and Φ_n denotes $(x^n - 1)/(x - 1) = x^{n-1} + x^{n-2} + \cdots + 1$. We have $x^n - 1 = \Phi_1\Phi_n$. R, $R/3$, and R/q denotes $\mathbb{Z}[x]/(\Phi_1\Phi_n)$, $\mathbb{Z}[x]/(3, \Phi_1\Phi_n)$, and $\mathbb{Z}[x]/(q, \Phi_1\Phi_n)$, respectively. S, $S/3$, and S/q denotes $\mathbb{Z}[x]/(\Phi_n)$, $\mathbb{Z}[x]/(3, \Phi_n)$, and $\mathbb{Z}[x]/(q, \Phi_n)$, respectively.

We say a polynomial *ternary* if its coefficients are in $\{-1, 0, +1\}$. $\underline{\mathsf{S3}}(a)$ returns a canonical $S/3$-representative of $z \in \mathbb{Z}[x]$, that is, $b \in \mathbb{Z}[x]$ of degree at most $n - 2$ with ternary coefficients in $\{-1, 0, +1\}$ such that $a \equiv b \pmod{3, \Phi_n}$. Let $\mathcal{T}$ be a set of non-zero ternary polynomials of degree at most $n - 2$, that is, $\mathcal{T} = \{a = \sum_{i=0}^{n-2} a_i x^i : a \neq 0 \wedge a_i \in \{-1, 0, +1\}\}$. We say a ternary polynomial $v = \sum_i v_i x^i$ has the *non-negative correlation* property if $\sum_i v_i v_{i+1} \geq 0$. $\mathcal{T}_+$ is a set of non-zero ternary polynomials of degree at most $n-2$ with *non-negative correlation* property. $\mathcal{T}(d)$ is a set of non-zero balanced ternary polynomials of degree at most $n-2$ with Hamming weight d, that is, $\{a \in \mathcal{T} : |\{a_i : a_i = 1\}| = |\{a_i : a_i = -1\}| = d/2\}$.

The following lemma is due to Schanck [41]. (See, e.g., [14] for this design choice.)

$\mathsf{Gen}(1^\kappa)$	$\mathsf{Enc}(h, (r, m) \in \mathcal{L}_r \times \mathcal{L}_m)$	$\mathsf{Dec}((f, f_p, h_q), c)$
$(f, g) \leftarrow \mathsf{Sample\_fg}()$	$\mu' \coloneqq \mathsf{Lift}(m)$	**if** $c \not\equiv 0 \bmod (q, \Phi_1)$
$f_q \coloneqq (1/f) \in S/q$	$c \coloneqq (h \cdot r + \mu') \in R/q$	**then return** $(0, 0, 1)$
$h \coloneqq (3 \cdot g \cdot f_q) \in R/q$	**return** c	$a \coloneqq (c \cdot f) \in R/q$
$h_q \coloneqq (1/h) \in S/q$		$m \coloneqq (a \cdot f_p) \in S/3$
$f_p \coloneqq (1/f) \in S/3$		$\mu' \coloneqq \mathsf{Lift}(m)$
$ek \coloneqq h, dk \coloneqq (f, f_p, h_q)$		$r \coloneqq ((c - \mu') \cdot h_q) \in S/q$
return (ek, dk)		**if** $(r, m) \in \mathcal{L}_r \times \mathcal{L}_m$
		then return $(r, m, 0)$
		else return $(0, 0, 1)$

Fig. 6. NTRU-DPKE

Lemma 5. *Suppose that* $(n, q) = (509, 2048)$, $(677, 2048)$, $(821, 4096)$, *or* $(701, 8192)$, *which are the parameter sets in NTRU. If* $r \in \mathcal{T}$, *then* r *has an inverse in* S/q.

Proof. Φ_n is irreducible over $\mathbb{F}_2$ if and only if n is prime and 2 is primitive element in $\mathbb{F}_n^\times$ (See e.g., Cohen et al. [15]). The conditions are satisfied for all $n = 509$, 677, 701, and 821. Hence, $\mathbb{Z}[x]/(2, \Phi_n)$ is a finite field and every polynomial r in $\mathcal{T}$ has an inverse in $\mathbb{Z}[x]/(2, \Phi_n)$. Such r is also invertible in $S/q = \mathbb{Z}[x]/(q, \Phi_n)$ with $q = 2^k$ for some k and, indeed, one can find it using the Newton method or the Hensel lifting. □

NTRU: NTRU involves four subsets $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_r$, $\mathcal{L}_m$ of R. It uses $\mathsf{Lift}(m)\colon \mathcal{L}_m \to R$. NTRU has two types of parameter sets, NTRU-HPS and NTRU-HRSS, specified as later.

- NTRU-HPS: The parameters are defined as follows: $\mathcal{L}_f = \mathcal{T}, \mathcal{L}_g = \mathcal{T}(q/8 - 2), \mathcal{L}_r = \mathcal{T}, \mathcal{L}_m = \mathcal{T}(q/8 - 2)$, and $\mathsf{Lift}(m) = m$.
- NTRU-HRSS: The parameters are defined as follows: $\mathcal{L}_f = \mathcal{T}_+, \mathcal{L}_g = \{\Phi_1 \cdot v \mid v \in \mathcal{T}_+\}, \mathcal{L}_r = \mathcal{T}, \mathcal{L}_m = \mathcal{T}$, and $\mathsf{Lift}(m) = \Phi_1 \cdot \underline{\mathsf{S3}}(m/\Phi_1)$.

It uses $\mathsf{Sample\_fg}()$ to sample f and g from $\mathcal{L}_f$ and $\mathcal{L}_g$. NTRU also uses $\mathsf{Sample\_rm}()$ to sample r and m from $\mathcal{L}_r$ and $\mathcal{L}_m$.

The underlying DPKE of NTRU, which we call NTRU-DPKE, is defined as Figure 6. We note that, for an encryption key h, we have $h \equiv 0 \pmod{(q, \Phi_1)}$, h is invertible in S/q, and $hr + m \equiv 0 \pmod{(q, \Phi_1)}$. (See [14, Section2.3].)

NTRU then apply SXY to NTRU-DPKE in order to obtain IND-CCA-secure KEM as in Figure 7, where $\mathsf{H} = \mathsf{SHA3\text{-}256}$ and $\mathsf{H}_{\mathsf{prf}} = \mathsf{SHA3\text{-}256}$. Since the lengths of their input space differ, we can treat them as different random oracles.

Rigidity: NTRU uses SXY, while its KEM version (Figure 7) seems to lack the re-encryption check. We note that NTRU implicitly checks $hr + \mathsf{Lift}(m) = c$ by checking if $(r, m) \in \mathcal{L}_r \times \mathcal{L}_m$ in NTRU-DPKE (Figure 6). See [14] for the details.

$\overline{\mathsf{Gen}}(1^\kappa)$	$\overline{\mathsf{Enc}}(ek = h)$	$\overline{\mathsf{Dec}}(\overline{dk} = (dk, s), c)$
$(ek, dk) \leftarrow \mathsf{Gen}(1^\kappa)$	$\mathsf{coins} \leftarrow \{0,1\}^{256}$	$(r, m, \mathsf{fail}) := \mathsf{Dec}(dk, c)$
$s \leftarrow \{0,1\}^{256}$	$(r, m) \leftarrow \mathsf{Sample\_rm}(\mathsf{coins})$	$k_1 := \mathsf{H}(r, m)$
$\overline{dk} := (dk, s)$	$c := \mathsf{Enc}(h, (r, m))$	$k_2 := \mathsf{H}_{\mathsf{prf}}(s, c)$
return $(ek, \overline{dk})$	$K := \mathsf{H}(r, m)$	**if** $\mathsf{fail} = 0$ **then return** k_1
	return (c, K)	**else return** k_2

Fig. 7. NTRU

5.2 Properties of NTRU-DPKE

We show that NTRU-DPKE is strongly disjoint-simulatable and XCFR-secure.

We have known that the generalized NTRU PKE is pseudorandom [44] and disjointly simulatable [39] if the decisional small polynomial ratio (DSPR) assumption [34] and the polynomial learning with errors (PLWE) assumption [45, 35] hold. See [39, Section 3.3 of the ePrint version.].

Let us adapt their arguments to NTRU-DPKE. We modify the DSPR and the PLWE assumptions as follows:

Definition 14. *Fix the parameter set. Define* $R' := \{c \in R/q : c \equiv 0 \pmod{(q, \Phi_1)}\}$*, which is efficiently sampleable.*

- *The modified DSPR assumption: It is computationally hard to distinguish* $h := 3 \cdot g \cdot f_q \pmod{q, \Phi_1\Phi_n}$ *from* h'*, where* $(f, g) \leftarrow \mathsf{Sample\_fg}()$*,* $f_q \leftarrow (1/f) \bmod (q, \Phi_n)$*, and* $h' \leftarrow R'$*.*
- *The modified PLWE assumption: It is computationally hard to distinguish* $(h, hr + \mathsf{Lift}(m) \pmod{q, \Phi_1\Phi_n})$ *from* (h, c') *with* $h, c' \leftarrow R'$ *and* $(r, m) \leftarrow \mathsf{Sample\_rm}()$*.*

We can show NTRU-DPKE is strongly disjoint-simulatable under those two assumptions:

Lemma 6. *Suppose that the modified DSPR and PLWE assumptions hold. Then, NTRU-DPKE is strongly disjoint-simulatable with a simulator* $\mathcal{S}$ *that outputs a random polynomial chosen from* R'*.*

Proof. The proof for ciphertext-indistinguishability is obtained by modifying the proof in [39]. We want to show that $(h, c = hr + \mathsf{Lift}(m) \bmod (q, \Phi_1\Phi_n)) \approx_c (h, c')$, where $h = 3gf_q \bmod (q, \Phi_1\Phi_n)$ and $f_q = (1/f) \bmod (q, \Phi_n)$ with $(f, g) \leftarrow \mathsf{Sample\_fg}()$, $(r, m) \leftarrow \mathsf{Sample\_rm}()$, and $c' \leftarrow R'$.

- We first replace h with $h' \leftarrow R'$, which is justified by the modified DSPR assumption.
- We next replace $c = h'r + \mathsf{Lift}(m) \bmod (q, \Phi_1\Phi_n)$ with $c' \leftarrow R'$, which is justified by the modified PLWE assumption.
- We then go backward by replacing random h' with h, which is is justified by the modified DSPR assumption again.

Statistical disjointness follows from the fact that $|R'| = q^{n-1} \gg 3^{2n} = |\mathcal{T} \times \mathcal{T}| \geq |\mathcal{L}_m \times \mathcal{L}_r| \geq |\mathsf{Enc}(h, \mathcal{L}_m \times \mathcal{L}_r)|$. Since R' is independent of an encryption key h, NTRU-DPKE is strong disjoint-simulatability. □

We next show the XCFR security of NTRU-DPKE.

Lemma 7. *NTRU-DPKE is* XCFR*-secure.*

Proof. Suppose that the adversary wins with its output c on input ek_0, dk_0, ek_1, and dk_1, where $ek_i = h_i$ for $i \in \{0,1\}$. Let us define $\mu_0 = \mathsf{Dec}(dk_0, c)$ and $\mu_1 = \mathsf{Dec}(dk_1, c)$.
If the adversary wins, we can assume $\mu_0 = \mu_1 = (r, m, 0) \in \mathcal{L}_r \times \mathcal{L}_m \times \{0,1\}$. Otherwise, that is, if $\mu_0 = \mu_1 = (0,0,1)$, then the output is treated as $\perp$ and the adversary loses.
Moreover, because of the check in the decryption, we have $c \equiv h_0 \cdot r + \mathsf{Lift}(m) \equiv h_1 \cdot r + \mathsf{Lift}(m) \pmod{q, \Phi_1\Phi_n}$, which implies $r(h_0 - h_1) \equiv 0 \pmod{(q, \Phi_n)}$. On the other hand, according to Lemma 5, for any $r \in \mathcal{L}_r = \mathcal{T}$, we have $r \not\equiv 0 \in S/q$ In addition, we have $h_0 \equiv h_1 \in S/q$ with negligible probability. Thus, all but negligible choices of h_0 and h_1, any $r \in \mathcal{L}_r = \mathcal{T}$ results in $r(h_0 - h_1) \not\equiv 0 \pmod{(q, \Phi_n)}$ and $h_0 \cdot r + \mathsf{Lift}(m) \not\equiv h_1 \cdot r + \mathsf{Lift}(m) \pmod{q, \Phi_1\Phi_n}$. Hence, the probability that the adversary wins is negligible, concluding the proof. □

5.3 Properties of NTRU

Combining NTRU-DPKE's strong disjoint-simulatability and XCFR security with previous theorems on SXY, we obtain the following theorems.

Theorem 11. *Suppose that the modified DSPR and PLWE assumptions hold. Then, NTRU is* SPR-CCA*-secure and* SSMT-CCA*-secure in the QROM.*

Proof. Under the modified DSPR and PLWE assumptions, NTRU-DPKE is strongly disjoint-simulatable (Lemma 6). In addition, NTRU-DPKE is perfectly correct. Applying Theorem 8 and Theorem 9, we obtain the theorem. □

Theorem 12. *NTRU is* SCFR-CCA*-secure in the QROM.*

Proof. NTRU-DPKE is XCFR-secure (Lemma 7). Applying Theorem 10, we have that NTRU is SCFR-CCA-secure in the QROM. □

Theorem 13. *Under the modified DSPR and PLWE assumptions, NTRU is* ANON-CCA*-secure in the QROM.*

Proof. Due to Theorem 11, under the modified DSPR and PLWE assumptions, NTRU is SPR-CCA-secure in the QROM. Thus, applying Theorem 1, we have that, under those assumptions, NTRU is ANON-CCA-secure in the QROM. □

Theorem 14. *Under the modified DSPR and PLWE assumptions, NTRU leads to* ANON-CCA*-secure and* SROB-CCA*-secure hybrid PKE in the QROM, combined with* SPR-OTCCA*-secure and* FROB*-secure DEM.*

Proof. Due to Theorem 11, under the modified DSPR and PLWE assumptions, NTRU is SPR-CCA-secure and SSMT-CCA-secure in the QROM. Moreover, NTRU is perfectly correct. Thus, combining NTRU with SPR-OTCCA-secure DEM, we obtain a SPR-CCA-secure hybrid PKE in the QROM (Theorem 7). Moreover, NTRU is SCFR-CCA-secure in the QROM (Theorem 12). Thus, if DEM is FROB-secure, then the hybrid PKE is SROB-CCA-secure (Theorem 3). □

Acknowledgement

The author is grateful to John Schanck for insightful comments and suggestions on NTRU, Akinori Hosoyamada and Takashi Yamakawa for insightful comments and discussion on quantum random oracles. The author would like to thank Daniel J. Bernstein for insightful comments and discussion on the indifferentiability of the quantum random oracles. The author would like to thank anonymous reviewers for their valuable comments and suggestions on this paper.

References

1. Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205–222. Springer, Heidelberg (Aug 2005).
2. Abdalla, M., Bellare, M., Neven, G.: Robust encryption. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 480–497. Springer, Heidelberg (Feb 2010).
3. Abe, M. (ed.): ASIACRYPT 2010, LNCS, vol. 6477. Springer, Heidelberg (Dec 2010)
4. Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Persichetti, E., Zémor, G., Bos, J.: HQC. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
5. Albrecht, M.R., Bernstein, D.J., Chou, T., Cid, C., Gilcher, J., Lange, T., Maram, V., von Maurich, I., Misoczki, R., Niederhagen, R., Paterson, K.G., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., Szefer, J., Tjhai, C.J., Tomlinson, M., Wang, W.: Classic McEliece. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
6. Aragon, N., Barreto, P., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Gueron, S., Guneysu, T., Aguilar Melchor, C., Misoczki, R., Persichetti, E., Sendrier, N., Tillich, J.P., Zémor, G., Vasseur, V., Ghosh, S.: BIKE. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
7. Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-privacy in public-key encryption. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 566–582. Springer, Heidelberg (Dec 2001).
8. Bellare, M., Desai, A., Pointcheval, D., Rogaway, P.: Relations among notions of security for public-key encryption schemes. In: Krawczyk, H. (ed.) CRYPTO'98. LNCS, vol. 1462, pp. 26–45. Springer, Heidelberg (Aug 1998).
9. Bernstein, D.J.: personal communication (Oct 2021)

10. Bernstein, D.J., Brumley, B.B., Chen, M.S., Chuengsatiansup, C., Lange, T., Marotzke, A., Peng, B.Y., Tuveri, N., van Vredendaal, C., Yang, B.Y.: NTRU Prime. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
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 (Dec 2011).
12. Boyd, C., Cliff, Y., González Nieto, J.M., Paterson, K.G.: One-round key exchange in the standard model. Int. J. Appl. Cryptogr. **1**(3), 181–199 (2009). , https://doi.org/10.1504/IJACT.2009.023466
13. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (May 2001).
14. Chen, C., Danba, O., Hoffstein, J., Hulsing, A., Rijneveld, J., Schanck, J.M., Schwabe, P., Whyte, W., Zhang, Z., Saito, T., Yamakawa, T., Xagawa, K.: NTRU. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
15. Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., Vercauteren, F.: Handbook of Elliptic and Hyperelliptic Curve Cryptography (2005)
16. Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45–64. Springer, Heidelberg (Apr / May 2002).
17. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing **33**(1), 167–226 (2003)
18. D'Anvers, J.P., Karmakar, A., Roy, S.S., Vercauteren, F., Mera, J.M.B., Beirendonck, M.V., Basso, A.: SABER. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
19. Farshim, P., Orlandi, C., Roşie, R.: Security of symmetric primitives under incorrect usage of keys. IACR Trans. Symm. Cryptol. **2017**(1), 449–473 (2017).
20. Fujioka, A., Suzuki, K., Xagawa, K., Yoneyama, K.: Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism. In: Chen, K., Xie, Q., Qiu, W., Li, N., Tzeng, W.G. (eds.) ASIACCS 13. pp. 83–94. ACM Press (May 2013)
21. Fujioka, A., Suzuki, K., Xagawa, K., Yoneyama, K.: Strongly secure authenticated key exchange from factoring, codes, and lattices. Des. Codes Cryptogr. **76**(3), 469–504 (2015). , https://doi.org/10.1007/s10623-014-9972-2
22. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M.J. (ed.) CRYPTO'99. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg (Aug 1999).

23. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. Journal of Cryptology **26**(1), 80–101 (Jan 2013).
24. Grubbs, P., Maram, V., Paterson, K.G.: Anonymous, robust post-quantum public key encryption. Cryptology ePrint Archive, Report 2021/708 (2021), https://eprint.iacr.org/2021/708. To appear in EUROCRYPT 2022
25. Grubbs, P., Maram, V., Paterson, K.G.: Anonymous, robust post-quantum public key encryption (presentation slides). The third NIST PQC Standardization Conference (2021), https://csrc.nist.gov/Presentations/2021/anonymous-robust-post-quantum-public-key-encryptio
26. 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, Heidelberg (Nov 2017).
27. Hopper, N.: On steganographic chosen covertext security. In: Caires, L., Italiano, G.F., Monteiro, L., Palamidessi, C., Yung, M. (eds.) ICALP 2005. LNCS, vol. 3580, pp. 311–323. Springer, Heidelberg (Jul 2005).
28. Hosoyamada, A.: personal communication (Jun 2021)
29. Hövelmanns, K., Kiltz, E., Schäge, S., Unruh, D.: Generic authenticated key exchange in the quantum random oracle model. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020, Part II. LNCS, vol. 12111, pp. 389–422. Springer, Heidelberg (May 2020).
30. Jao, D., Azarderakhsh, R., Campagna, M., Costello, C., De Feo, L., Hess, B., Jalali, A., Koziel, B., LaMacchia, B., Longa, P., Naehrig, M., Renes, J., Soukharev, V., Urbanik, D., Pereira, G., Karabina, K., Hutchinson, A.: SIKE. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
31. Jiang, H., Zhang, Z., Chen, L., Wang, H., Ma, Z.: IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part III. LNCS, vol. 10993, pp. 96–125. Springer, Heidelberg (Aug 2018).
32. Jiang, H., Zhang, Z., Ma, Z.: Key encapsulation mechanism with explicit rejection in the quantum random oracle model. In: Lin, D., Sako, K. (eds.) PKC 2019, Part II. LNCS, vol. 11443, pp. 618–645. Springer, Heidelberg (Apr 2019).
33. Liu, X., Wang, M.: QCCA-secure generic key encapsulation mechanism with tighter security in the quantum random oracle model. In: Garay, J. (ed.) PKC 2021, Part I. LNCS, vol. 12710, pp. 3–26. Springer, Heidelberg (May 2021).
34. 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.) 44th ACM STOC. pp. 1219–1234. ACM Press (May 2012).

35. 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 (May / Jun 2010).
36. Mohassel, P.: A closer look at anonymity and robustness in encryption schemes. In: Abe [3], pp. 501–518.
37. Naehrig, M., Alkim, E., Bos, J., Ducas, L., Easterbrook, K., LaMacchia, B., Longa, P., Mironov, I., Nikolaenko, V., Peikert, C., Raghunathan, A., Stebila, D.: FrodoKEM. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
38. Rackoff, C., Simon, D.R.: Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Feigenbaum, J. (ed.) CRYPTO'91. LNCS, vol. 576, pp. 433–444. Springer, Heidelberg (Aug 1992).
39. Saito, T., Xagawa, K., Yamakawa, T.: Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part III. LNCS, vol. 10822, pp. 520–551. Springer, Heidelberg (Apr / May 2018).
40. Sako, K.: An auction protocol which hides bids of losers. In: Imai, H., Zheng, Y. (eds.) PKC 2000. LNCS, vol. 1751, pp. 422–432. Springer, Heidelberg (Jan 2000).
41. Schanck, J.: personal communication (Jun 2021)
42. Schwabe, P., Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Seiler, G., Stehlé, D.: CRYSTALS-KYBER. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
43. Schwabe, P., Stebila, D., Wiggers, T.: Post-quantum TLS without handshake signatures. In: Ligatti, J., Ou, X., Katz, J., Vigna, G. (eds.) ACM CCS 2020. pp. 1461–1480. ACM Press (Nov 2020).
44. Stehlé, D., Steinfeld, R.: Faster fully homomorphic encryption. In: Abe [3], pp. 377–394.
45. Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient public key encryption based on ideal lattices. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 617–635. Springer, Heidelberg (Dec 2009).
46. von Ahn, L., Hopper, N.J.: Public-key steganography. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 323–341. Springer, Heidelberg (May 2004).
47. Xagawa, K., Yamakawa, T.: (Tightly) QCCA-secure key-encapsulation mechanism in the quantum random oracle model. In: Ding, J., Steinwandt, R. (eds.) Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019. pp. 249–268. Springer, Heidelberg (2019).
48. Zhandry, M.: A note on the quantum collision and set equality problems. Quantum Info. Comput. **15**(7–8), 557–567 (May 2015)
49. Zhandry, M.: How to record quantum queries, and applications to quantum indifferentiability. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 239–268. Springer, Heidelberg (Aug 2019).

A Missing Lemma

Lemma 8. *Let* A *and* B *denote events. Suppose that we have* $\Pr[\mathsf{A}] \leq \delta$. *For any* $p \geq 0$, *we have*

$$|\Pr[\mathsf{B}] - p| \leq |\Pr[\mathsf{B} \wedge \neg\mathsf{A}] - p| + \delta \quad \textit{and} \quad |\Pr[\mathsf{B} \wedge \neg\mathsf{A}] - p| \leq |\Pr[\mathsf{B}] - p| + \delta.$$

Proof. Those bounds are obtained by using the triangle inequality. We have

$$\begin{aligned} |\Pr[\mathsf{B}] - p| &= |\Pr[\mathsf{B} \wedge \mathsf{A}] + \Pr[\mathsf{B} \wedge \neg\mathsf{A}] - p| \leq \Pr[\mathsf{B} \wedge \mathsf{A}] + |\Pr[\mathsf{B} \wedge \neg\mathsf{A}] - p| \\ &\leq \Pr[\mathsf{A}] + |\Pr[\mathsf{B} \wedge \neg\mathsf{A}] - p| \leq |\Pr[\mathsf{B} \wedge \neg\mathsf{A}] - p| + \delta \end{aligned}$$

and

$$\begin{aligned} |\Pr[\mathsf{B} \wedge \neg\mathsf{A}] - p| &= |\Pr[\mathsf{B} \wedge \neg\mathsf{A}] + \Pr[\mathsf{B} \wedge \mathsf{A}] - \Pr[\mathsf{B} \wedge \mathsf{A}] - p| \\ &= |\Pr[\mathsf{B}] - p - \Pr[\mathsf{B} \wedge \mathsf{A}]| \leq |\Pr[\mathsf{B}] - p| + \Pr[\mathsf{B} \wedge \mathsf{A}] \\ &\leq |\Pr[\mathsf{B}] - p| + \Pr[\mathsf{A}] \leq |\Pr[\mathsf{B}] - p| + \delta \end{aligned}$$

as we wanted. □