Post-quantum Security of plain OAEP Transform

Ehsan Ebrahimi

FSTM, SnT, University of Luxembourg
ehsan.ebrahimi@uni.lu

Abstract. In this paper, we show that OAEP transform is indistinguishable under chosen ciphertext attack in the quantum random oracle model if the underlying trapdoor permutation is quantum partial-domain one-way. The existing post-quantum security of OAEP (TCC 2016-B [14]) requires a modification to the OAEP transform using an extra hash function. We prove the security of the OAEP transform without any modification and this answers an open question in one of the finalists of NIST competition, NTRU submission [6], affirmatively.

Keywords. Post-quantum Security, OAEP, Quantum Random Oracle Model

1 Introduction

The rapid progress on quantum computing and the existence of quantum algorithms like Shor's algorithm [12] has sparked the necessity of replacing old cryptography with the post-quantum cryptography. Toward this goal, the National Institute of Standards and Technology (NIST) has initiated a competition for post-quantum cryptography. In this paper we address an open question in one of the finalists of NIST competition, NTRU submission [6]. The security of (unmodified) Optimal Asymmetric Encryption Padding (OAEP) in the quantum random oracle model has been mentioned as an interesting open question in [6]. The existing post-quantum security proof of OAEP [14] requires a modification to OAEP transform. (See details below.)

The random oracle model [1] is a powerful model in which the security of a cryptographic scheme is proven assuming the existence of a truly random function that is accessible by all parties including the adversary. But in real world applications, the random oracle will be replaced with a cryptographic hash function and the code of this function is public and known to the adversary. Following [4], we use the quantum random oracle model in which the adversary can make queries to the random oracle in superposition (that is, given a superposition of inputs, he can get a superposition of output values). This is necessary since a quantum adversary attacking a scheme based on a real hash function is necessarily able to evaluate that function in superposition. Hence the random oracle model must reflect that ability if one request post-quantum security.

Bellare and Rogaway [2] proposed OAEP transform, for converting a trapdoor permutation into an encryption scheme using two random oracles. It was believed that the OAEP-cryptosystem is provable secure in the random oracle model based on one-wayness of trapdoor permutation, but Shoup [13] showed it is an unjustified belief. Later, Fujisaki et al. [9] proved IND-CCA security of the OAEP-cryptosystem based on a stronger assumption, namely, partial-domain one-wayness of the underlying permutation.

Is OAEP transform secure in the standard model? The most recent work to study this question [5] shows that a full instantiation of RSA-OAEP is only possible for two variants of RSA-OAEP (called 't-clear' and 's-clear'). Also, we emphasize that the positive results in [5] hold against a classical adversary and one needs to investigate the possibility of such instantiation in the post-quantum setting. For instance, the partial instantiations are based on algebraic properties of RSA assumption that trivially does not hold in the post-quantum setting. Or the full instantiation of t-clear RSA-OAEP is based on non-standard assumptions (called 'XOR-type' assumptions) for which an intuitive justifications has been only given in light of the multiplicative structure of RSA, and etc. Even though the post-quantum instantiation of the random oracles in OAEP is a relevant research question, it is not in the scope of this paper and we leave a further investigation as an open question. Here, we investigate the security of OAEP transform in the quantum random oracle model.

Post-quantum security of OAEP transform has been studied in [14]. The authors modified OAEP transform (called it Q-OAEP) using an extra hash function that is length-preserving and show that Q-OAEP is IND-CCA secure in the quantum random oracle model. The extra hash function in Q-OAEP is used to extract the preimage of a random oracle queries in the security proof. In this work, we show that this extra hash function is unnecessary. We use Zhandry's compressed oracle technique [16] to prove IND-qCCA security of OAEP transform (without any modification) in the quantum random oracle model. IND-qCCA notion introduced in [3] is an adaptation of IND-CCA in which the adversary is allowed to make quantum decryption queries, but, the challenge query is restricted to be classical. Since security in the sense of IND-qCCA implies IND-CCA security, our result answers an open question in one of the finalists of NIST competition, NTRU [6], affirmatively.

Note that in the IND-qCCA notion, the adversary's challenge queries are restricted to be classical. Proposing a quantum IND-CCA notion that grants the adversary the possibility of submitting quantum challenge queries is a challenging task with some partial successes [7, 10]. We postpone verifying the security of OAEP transform in the sense of definitions in [7, 10] until a definite definition is given.

Organization. In Section 2, we present some basics of quantum information and computation, security definitions needed in the paper and an introduction for the Compressed Standard Oracle that has been introduced in [16] which we use it in the paper. In Section 3, we present the OAEP scheme and show that it is IND-qCCA secure in the quantum random oracle model.

2   Preliminaries

Notations. Let MSP stands for the message space. The notation $x \xleftarrow{\$} X$ means that x is chosen uniformly at random from the set X. For a natural number n, $[n]$ means the set $\{1, \cdots, n\}$. $\Pr[P : G]$ is the probability that the predicate P holds true where free variables in P are assigned according to the program in G. The function $\mathsf{negl(n)}$ is any non-negative function that is smaller than the inverse of any non-negative polynomial $p(n)$ for sufficiently large n. That is, $\lim_{n \to \infty} \mathsf{negl(n)} p(n) = 0$ for any polynomial $p(n)$. For a function f, f_x denotes the evaluation of f on the input x, that is $f(x)$. For a bit-string x of size more-than-equal k, $[x]_k$ is the k least significant bits of x and $[x]^k$ is the k most significant bits of x. For two bits b and b', $[b = b']$ is 1 if $b = b'$ and it is 0 otherwise.

2.1   Quantum Computing

We present basics of the quantum computing in this subsection. The interested reader can refer to [11] for more information. For two vectors $|\Psi\rangle = (\psi_1, \psi_2, \cdots, \psi_n)$ and $|\Phi\rangle = (\phi_1, \phi_2, \cdots, \phi_n)$ in $\mathbb{C}^n$, the inner product is defined as $\langle \Psi, \Phi \rangle = \sum_i \psi_i^* \phi_i$ where ψ_i^* is the complex conjugate of ψ_i. Norm of $|\Phi\rangle$ is defined as $\| |\Phi\rangle \| = \sqrt{\langle \Phi, \Phi \rangle}$. The n-dimensional Hilbert space $\mathcal{H}$ is the complex vector space $\mathbb{C}^n$ with the inner product defined above. A quantum system is a Hilbert space $\mathcal{H}$ and a quantum state $|\psi\rangle$ is a vector $|\psi\rangle$ in $\mathcal{H}$ with norm 1. An unitary operation over $\mathcal{H}$ is a transformation $\mathbb{U}$ such that $\mathbb{U}\mathbb{U}^\dagger = \mathbb{U}^\dagger\mathbb{U} = \mathbb{I}$ where $\mathbb{U}^\dagger$ is the Hermitian transpose of $\mathbb{U}$ and $\mathbb{I}$ is the identity operator over $\mathcal{H}$. Norm of an operator $\mathbb{U}$ is $\|\mathbb{U}\| = \max_{|\psi\rangle} \|\mathbb{U}|\psi\rangle\|$. The computational basis for $\mathcal{H}$ consists of $\log n$ vectors $|b_i\rangle$ of length $\log n$ with 1 in the position i and 0 elsewhere. With this basis, the Hadamard unitary is defined as

$$\mathbb{H} : |b\rangle \to \frac{1}{\sqrt{2}}(|\bar{b}\rangle + (-1)^b |b\rangle),$$

for $b \in \{0, 1\}$ where $\bar{b} = 1 - b$. The control-swap unitary is defined as

$$|b\rangle |\psi_0\rangle |\psi_1\rangle \to |b\rangle |\psi_b\rangle |\psi_{\bar{b}}\rangle,$$

for $b \in \{0, 1\}$. The controlled-unitary $\mathbb{U}$ ($c\mathbb{U}$) is define as:

$$c\mathbb{U} |b\rangle |\Psi\rangle \to \begin{cases} |b\rangle \mathbb{U} |\Psi\rangle & \text{if } b = 1 \\ |b\rangle |\Psi\rangle & \text{if } b = 0 \end{cases}.$$

The bit-flip unitary $\mathbb{X}$ maps $|b\rangle$ to $|\bar{b}\rangle$ for $b \in \{0, 1\}$. An orthogonal projection $\mathbb{P}$ over $\mathcal{H}$ is a linear transformation such that $\mathbb{P}^2 = \mathbb{P} = \mathbb{P}^\dagger$. A measurement on a Hilbert space is defined with a family of orthogonal projectors that are pairwise orthogonal. An example of measurement is the computational basis measurement in which any projection is defined by a basis vector. The output of computational measurement on a state $|\Psi\rangle$ is i with probability $\|\langle b_i, \Psi \rangle\|^2$ and

3

the post measurement state is $|b_i\rangle$. For a general measurement $\{\mathbb{P}_i\}_i$, the output of this measurement on a state $|\Psi\rangle$ is i with probability $\|\mathbb{P}_i |\Psi\rangle\|^2$ and the post measurement state is $\frac{\mathbb{P}_i |\Psi\rangle}{\|\mathbb{P}_i |\Psi\rangle\|}$.

For two operators $\mathbb{U}_1$ and $\mathbb{U}_2$, the commutator is $[\mathbb{U}_1, \mathbb{U}_2] = \mathbb{U}_1\mathbb{U}_2 - \mathbb{U}_2\mathbb{U}_1$. For two quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$, the composition of them is defined by the tensor product and it is $\mathcal{H}_1 \otimes \mathcal{H}_2$. For two unitary $\mathbb{U}_1$ and $\mathbb{U}_2$ defined over $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively, $(\mathbb{U}_1 \otimes \mathbb{U}_2)(\mathcal{H}_1 \otimes \mathcal{H}_2) = \mathbb{U}_1(\mathcal{H}_1) \otimes \mathbb{U}_2(\mathcal{H}_2)$. In this paper, QFT over an n-qubits system is $\mathbb{H}^{\otimes n}$. Any classical function $f : X \to Y$ can be implemented as a unitary operator $\mathbb{U}_f$ in a quantum computer where $\mathbb{U}_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$. Note that it is clear that $\mathbb{U}_f^\dagger = \mathbb{U}_f$. A quantum adversary has standard oracle access to a classical function f if it can query the unitary $\mathbb{U}_f$.

2.2 Definitions

Here, we define an asymmetric encryption scheme, the IND-qCCA security notion and the quantum partial one-wayness.

Definition 1. *An asymmetric encryption scheme $\mathcal{E}$ consists of three polynomial time (in the security parameter n) algorithms, $\mathcal{E} = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$, such that:*

1. Gen*, the key generation algorithm, is a probabilistic algorithm which on input 1^n outputs a pair of keys, $(pk, sk) \leftarrow \mathrm{Gen}(1^n)$, called the public key and the secret key for the encryption scheme, respectively.*
2. Enc*, the encryption algorithm, is a probabilistic algorithm which takes as input a public key pk and a message $m \in \mathtt{MSP}$ and outputs a ciphertext $c \leftarrow Enc_{pk}(m)$. The message space, $\mathtt{MSP}$, may depend on pk.*
3. Dec*, the decryption algorithm, is a deterministic algorithm that takes as input a secret key sk and a ciphertext c and returns the message $m := \mathrm{Dec}_{sk}(c)$. It is required that the decryption algorithm returns the original message, i.e., $\mathrm{Dec}_{sk}(Enc_{pk}(m)) = m$, for every $(pk, sk) \leftarrow \mathrm{Gen}(1^n)$ and every $m \in \mathtt{MSP}$. The algorithm Dec returns $\bot$ if ciphertext c is not decryptable.*

In the following, we define the IND-qCCA security notion [3] in the quantum random oracle model. The IND-qCCA security notion for an asymmetric encryption scheme allows the adversary to makes quantum decryption queries but the challenge query is classical. We define $\mathbb{U}_{\mathrm{Dec}}$ as:

$$\mathbb{U}_{\mathrm{Dec}} |c, y\rangle \to \begin{cases} |c, y \oplus \bot\rangle & \text{if } c^* \text{ is defined } \& c = c^*, \\ |c, y \oplus \mathrm{Dec}_{sk}(c)\rangle & \text{otherwise} \end{cases}$$

where c^* is the challenge ciphertext and $\bot$ is a value outside of the output space. We say that the quantum algorithm $\mathcal{A}$ has quantum access to the random oracle H if $\mathcal{A}$ can submit queries in superposition and the oracle H answers to these queries by applying a unitary transformation that maps $|x, y\rangle$ to $|x, y \oplus H(x)\rangle$.

Definition 2 (IND-qCCA in the quantum random oracle model). *An asymmetric encryption scheme $\mathcal{E} = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is IND-qCCA secure if for*

*any **quantum** polynomial time adversary $\mathcal{A}$*

$$\Pr\left[b = 1 : b \leftarrow \mathsf{Exp}^{qCCA,qRO}_{\mathcal{A},\mathcal{E}}(n)\right] \leq 1/2 + \mathsf{negl(n)},$$

where $\mathsf{Exp}^{qCCA,qRO}_{\mathcal{A},\mathcal{E}}(n)$ *game is define as:*

$\underline{\mathsf{Exp}^{qCCA,qRO}_{\mathcal{A},\mathcal{E}}(n) \text{ game:}}$

Key Gen: *The challenger runs* $\mathrm{Gen}(1^n)$ *to obtain a pair of keys* (pk, sk) *and chooses random oracles.*

Query: *The adversary $\mathcal{A}$ given the public key pk, the **quantum** oracle access to $\mathbb{U}_{\mathrm{Dec}}$ and the **quantum** access to the random oracles, chooses two **classical** messages m_0, m_1 of the same length and sends them to the challenger. The challenger chooses a random bit b and responds with $c^* \leftarrow Enc_{pk}(m_b)$.*

Guess: *The adversary $\mathcal{A}$ continues to query the decryption oracle and the random oracles. Finally, the adversary $\mathcal{A}$ produces a bit b'. The output of the game is $[b = b']$.*

Definition 3 (Quantum partial-domain one-way function). *We say a permutation $f : \{0,1\}^{n+k_1} \times \{0,1\}^{k_0} \to \{0,1\}^m$ is quantum partial-domain one-way if for any polynomial time quantum adversary A,*

$$\Pr\left[\tilde{s} = s : s \xleftarrow{\$} \{0,1\}^{n+k_1}, \ t \xleftarrow{\$} \{0,1\}^{k_0}, \ \tilde{s} \leftarrow A(f(s,t))\right] \leq \mathsf{negl(n)}.$$

2.3 Compressed Standard Oracle

In this section, we briefly present the Compressed Standard Oracle (CStO) that have been introduced in [16]. The interested reader can refer to [8, 16] for more details.

In the standard quantum random oracle model, a function $H : \{0,1\}^m \to \{0,1\}^n$ is chosen uniformly at random from the set of all functions (lets call it Ω_H) and superposition queries will be answered by the unitary $\mathbb{U}_H$ that maps $|x, \ y\rangle$ to $|x, \ y \oplus H(x)\rangle$. Another perspective to consider this is that the oracle puts the superposition of all functions on his private register[1] and a query is implemented as

$$\mathsf{StO} : |x, \ y\rangle \sum_H \frac{1}{\sqrt{|\Omega_H|}} |H\rangle \to \sum_H \frac{1}{\sqrt{|\Omega_H|}} |x, \ y \oplus H(x)\rangle |H\rangle.$$

Note that if the oracle measures its internal state in the computational basis, this corresponds to choosing H uniformly at random from Ω_H and answer with $\mathbb{U}_H$. So these two oracles are perfectly indistinguishable. Now if we apply QFT to

---

[1]This requires exponential number of registers that is not efficient.

the output register before and after applying StO, we will get the Phase oracle that operates as follows:

$$\text{PhO} : |x, y\rangle \sum_{H} \frac{1}{\sqrt{|\Omega_H|}} |H\rangle \rightarrow \sum_{H} \frac{1}{\sqrt{|\Omega_H|}} (-1)^{y \cdot H(x)} |x, y\rangle |H\rangle .$$

Let $\mathfrak{D}$ represents the truth table of the function H and $P_{x,y}$ represents the truth table of the point function that is y on the input x and it is zero elsewhere. With this notation we can write the query above as follows:

$$\text{PhO} : |x, \ y\rangle \sum_{\mathfrak{D}} \frac{1}{\sqrt{|\Omega_H|}} |\mathfrak{D}\rangle \rightarrow \sum_{\mathfrak{D}} \frac{1}{\sqrt{|\Omega_H|}} (-1)^{P_{x,y} \cdot \mathfrak{D}} |x, y\rangle |\mathfrak{D}\rangle .$$

Now if the oracle applies QFT to the oracle register after applying PhO, it will get:

$$\text{QFT}_{\mathfrak{D}} \text{PhO} : |x, \ y\rangle \sum_{\mathfrak{D}} \frac{1}{\sqrt{|\Omega_H|}} |\mathfrak{D}\rangle \rightarrow |x, y\rangle |P_{x,y}\rangle .$$

Note that $\text{QFT}_{\mathfrak{D}}$ only effects the oracle state and it is undetectable to the adversary. At this stage, the oracle will symmetrically store the inputs/outputs of the the adversary's queries in its private register. Informally, if the oracle is able to move the entry that is not zero in the database $P_{x,y}$ to the beginning of its private register and remove all the zero slots (without the adversary's detection), the private register of the oracle can contain polynomial number of registers.

$$\text{RmoV}_{\mathfrak{D}} \text{MoV}_{\mathfrak{D}} \text{QFT}_{\mathfrak{D}} \text{PhO} : \sum_{x,y} \alpha_{x,y} |x, y\rangle \sum_{\mathfrak{D}} \frac{1}{\sqrt{|\Omega_H|}} |\mathfrak{D}\rangle \rightarrow \sum_{x,y} \alpha_{x,y} |x, y\rangle |x, y\rangle .$$

Following the perspective above, Zhandry [16] developed the CStO oracle that its private register can be implemented efficiently, symmetrically stores the inputs/outputs of the adversary's queries in its private register and it is perfectly indistinguishable from the standard oracle (StO).

Lemma 1 (Lemma 4 in [16]). CStO *and* StO *are perfectly indistinguishable.*

For the rest, we import the representation of CStO from [8]. Let $\mathfrak{D} = \otimes_{x \in X} \mathfrak{D}_x$ be the oracle register. The state space of $\mathfrak{D}_x$ is generated with vectors $|y\rangle$ for $y \in Y \cup \{\perp\}$. Let $F_{\mathfrak{D}_x}$ is an unitary acting on $\mathfrak{D}_x$ that maps $|\perp\rangle$ to $\text{QFT} |0\rangle$ and vice versa. And for any vector orthogonal to $|\perp\rangle$ and $\text{QFT} |0\rangle$, F is identity. We define CStO to be the following unitary acting on the input register, the output register and the $\mathfrak{D}$ register.

$$\text{CStO} = \sum_{x} |x\rangle\langle x| \otimes F_{\mathfrak{D}_x} CNOT_{Y\mathfrak{D}_x} F_{\mathfrak{D}_x},$$

where $CNOT_{Y\mathfrak{D}_x} |y, y_x\rangle = |y \oplus y_x, y_x\rangle$ for $y, y_x \in Y$ and it is identity on $|y, \perp\rangle$. The initial state of $\mathfrak{D}$ register is $\otimes_{x \in X} |\perp\rangle$.

We call a query to CStO 'dummy' if its output register is set to the uniform superposition. Note that for such a query $CNOT_{Y\mathfrak{D}_x}$ is identity and therefore CStO is identity.

In the following, we present preliminaries for Theorem 3.1 in [8] that will be used in the security proof in Section 3. For a fixed relation $R \subset X \times Y$, Γ_R is the maximum number of y's that fulfill the relation R where the maximum is taken over all $x \in X$:

$$\Gamma_R = \max_{x \in X} |\{y \in Y | (x, y) \in R\}|.$$

We define a projector $\Pi^x_{\mathfrak{D}_x}$ that checks if the register $\mathfrak{D}_x$ contains a value $y \neq \perp$ such that $(x, y) \in R$:

$$\Pi^x_{\mathfrak{D}_x} := \sum_{y \ s.t. \ (x,y) \in R} |y\rangle\langle y|_{\mathfrak{D}_x}.$$

Let $\bar{\Pi}^x_{\mathfrak{D}_x} = \mathbb{I}_{\mathfrak{D}_x} - \Pi^x_{\mathfrak{D}_x}$. We define the measurement $\mathbb{M}$ to be the set of projectors $\{\Sigma^x\}_{x \in X \cup \{\emptyset\}}$ where

$$\Sigma^x := \bigotimes_{x' < x} \bar{\Pi}^{x'}_{\mathfrak{D}_{x'}} \otimes \Pi^x_{\mathfrak{D}_x} \text{ for } x \in X \text{ and } \Sigma^\emptyset := \mathbb{I} - \sum_x \Sigma^x. \tag{1}$$

Informally, the measurement $\mathbb{M}$ checks for the smallest x for which $\mathfrak{D}_x$ contains a value $y \neq \perp$ such that $(x, y) \in R$. If no register $\mathfrak{D}_x$ contains a value $y \neq \perp$ such that $(x, y) \in R$, the outcome of $\mathbb{M}$ is $\emptyset$. We define a purified measurement $\mathbb{M}_{\mathfrak{D}P}$ corresponding to $\mathbb{M}$ that XORs the outcome of the measurement to an ancillary register:

$$\mathbb{M}_{\mathfrak{D}P} |\phi, z\rangle_{\mathfrak{D}P} \to \sum_{x \in X \cup \{\emptyset\}} \Sigma^x |\phi\rangle_{\mathfrak{D}} |z \oplus x\rangle_P.$$

The following lemma states that CStO and $\mathbb{M}_{\mathfrak{D}P}$ almost commute if Γ_R is small proportional to the size of Y.

Lemma 2 (Theorem 3.1 in [8]). *For any relation R and Γ_R defined above, the commutator $[\mathsf{CStO}, \mathbb{M}_{\mathfrak{D}P}]$ is bounded as follows:*

$$\|[\mathsf{CStO}, \mathbb{M}_{\mathfrak{D}P}]\| \leq 8 \cdot 2^{-n/2} \sqrt{2\Gamma_R}.$$

In addition to lemmas above, we use 'gentle-measurement lemma' [15] in the proof. Informally, it states that if an output of a measurement is almost certain for a quantum state, the measurement does not disturb the state much.

Lemma 3 (gentle-measurement lemma). *Let $\mathbb{M} = \{\mathbb{P}_i\}_i$ is a measurement. For any state $|\Psi\rangle$, if there exists an i such that $\|\mathbb{P}_i |\Psi\rangle\|^2 \geq 1 - \epsilon$, then $\mathrm{tr}(|\Psi\rangle, \mathbb{M} |\Psi\rangle) \leq \sqrt{\epsilon} + \epsilon$.*

3 Security of OAEP

Definition 4. *Let $G : \{0,1\}^{k_0} \to \{0,1\}^{k-k_0}$, $H : \{0,1\}^{k-k_0} \to \{0,1\}^{k_0}$ be random oracles. The encryption scheme $\mathcal{OAEP} = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is defined as:*

1. Gen*: Specifies an instance of the injective function f and its inverse f^{-1}. Therefore, the public key and secret key are f and f^{-1} respectively.*
2. Enc*: Given a message $m \in \{0,1\}^n$, the encryption algorithm computes*

$$s := m\|0^{k_1} \oplus G(r) \quad and \quad t := r \oplus H(s),$$

where $r \xleftarrow{\$} \{0,1\}^{k_0}$, and outputs the ciphertext $c := f(s,t)^2$.
3. Dec*: Given a ciphertext c, the decryption algorithm does the following: Compute $f^{-1}(c) = (s,t)$ and then,*
   (a) *query the random oracle G on input $t \oplus H(s)$ and compute $M := s \oplus G(t \oplus H(s))$.*
   (b) *if the k_1 least significant bits of M are zero then return the n most significant bits of M, otherwise return $\perp$.*

Note that k_0 and k depend on the security parameter n.

Theorem 1. *If the underlying permutation is quantum partial-domain one-way, then the OAEP scheme is IND-qCCA secure in the quantum random oracle model.*

Proof. Let Ω_H and Ω_G be the set of all function $H : \{0,1\}^{k-k_0} \to \{0,1\}^{k_0}$ and $G : \{0,1\}^{k_0} \to \{0,1\}^{k-k_0}$, respectively. Let A be a polynomial time quantum adversary that attacks the OAEP-cryptosystem in the sense of IND-qCCA in the quantum random oracle model and makes at most q_H and q_G queries to the random oracles H and G respectively and q_{dec} decryption queries.

Game 0: This is IND-qCCA game in qROM, $\mathsf{Exp}^{qCCA,qRO}_{A,\mathcal{OAEP}}(n)$.

Game 0:

---

   let $(pk, sk) \leftarrow \text{Gen}(1^n)$, $r^* \xleftarrow{\$} \{0,1\}^{k_0}$, $b \xleftarrow{\$} \{0,1\}$, $H \xleftarrow{\$} \Omega_H, G \xleftarrow{\$} \Omega_G$
   let $m_0, m_1 \leftarrow A^{H,G,\mathbb{U}_{\text{Dec}}}(pk)$
   let $s^* := m_b\|0^{k_1} \oplus G(r^*)$, $t^* := r^* \oplus H(s^*)$, $c^* := f(s^*, t^*)$
   let $b' \leftarrow A^{H,G,\mathbb{U}_{\text{Dec}}}(c^*)$
   return $[b = b']$

Game 1: In this game, we consider H, G are being implemented as the compressed standard oracles CStO_H and CStO_G. Since these oracles are equivalent to the standard oracles StO_H and StO_G, respectively, by Lemma 1, this change does not effect the adversary's success probability.

Game 1:

---

   let $(pk, sk) \leftarrow \text{Gen}(1^n)$, $r^* \xleftarrow{\$} \{0,1\}^{k_0}$, $b \xleftarrow{\$} \{0,1\}$
   let $m_0, m_1 \leftarrow A^{\mathsf{CStO}_H,\mathsf{CStO}_G,\mathbb{U}_{\text{Dec}}}(pk)$
   let $s^* := m_b\|0^{k_1} \oplus G(r^*)$, $t^* := r^* \oplus H(s^*)$, $c^* := f(s^*, t^*)$
   let $b' \leftarrow A^{\mathsf{CStO}_H,\mathsf{CStO}_G,\mathbb{U}_{\text{Dec}}}(c^*)$
   return $[b = b']$

---

[2]Q-OAEP in [14] outputs the ciphertext $c := (f(s,t), H'(s,t))$ for a fresh random oracle H'.

Game 2: In this game we change $\mathbb{U}_{\mathrm{Dec}}$ oracle to $\mathbb{U}_{\mathrm{Dec}^{(1)}}$ described below. Let $\mathfrak{D}_G$ denotes the database of CStO_G. We define the relation R_c^G to be the set of all (r, G_r) such that $[[f^{-1}(c)]^{n+k_1} \oplus G_r]_{k_1} = 0^{k_1}$. Given the relation R_c^G, the projectors Σ_c^r for $r \in \{0,1\}^{k_0}$ and $\Sigma_c^\emptyset$ are defined similar to Equation (1). Now the measurement $\mathbb{M} = \{\Sigma_c^r\}_{r \in \{0,1\}^{k_0} \cup \{\emptyset\}}$ checks if there exists a pair in $\mathfrak{D}_G$ satisfying the relation R_c^G or not. If there are more than one pair satisfying the relation R_c^G, the smallest r will be the output of $\mathbb{M}$. If there is no such a pair the output of $\mathbb{M}$ is $\emptyset$. Let $\mathbb{M}_{\mathfrak{D}_G, P}^c$ be the following purified measurement corresponding to $\mathbb{M}$:

$$\mathbb{M}_{\mathfrak{D}_G P}^c |\phi, z\rangle_{\mathfrak{D}_G P} \to \sum_{r \in \{0,1\}^{k_0} \cup \{\emptyset\}} \Sigma_c^r |\phi\rangle_{\mathfrak{D}_G} |z \oplus x\rangle_P .$$

We define the unitary $\mathbb{M}_{\mathfrak{D}_G, P}$ that operates on the ciphertext, $\mathfrak{D}_G$ and P registers as:

$$\mathbb{M}_{\mathfrak{D}_G, P} |c\rangle |\phi, z\rangle_{\mathfrak{D}_G P} \to |c\rangle \otimes \mathbb{M}_{\mathfrak{D}_G P}^c |\phi, z\rangle_{\mathfrak{D}_G P} .$$

For each decryption query, $\mathbb{U}_{\mathrm{Dec}^{(1)}}$ first applies the $\mathbb{M}_{\mathfrak{D}_G, P}$ unitary with the P register initiated with 0. Then, if c^* is defined and $c = c^*$ it XORs $\perp$ to the output register. Otherwise, if the P register contains $\emptyset$ it XORs $\perp$ to the output register and make two dummy queries to the random oracles G, H [3]. If the P register does not contain $\emptyset$, it executes $\mathbb{U}_{\mathrm{Dec}}$:

$$|c, y\rangle |z\rangle_P \to \begin{cases} |c, y \oplus \perp\rangle |z\rangle & \text{if } c^* \text{ is defined } \& c = c^* \\ |c, y \oplus \perp\rangle |z\rangle & \text{if } z = \emptyset \\ |c, y \oplus \mathrm{Dec}_{f^{-1}}(c)\rangle |z\rangle & \text{if } z \neq \emptyset \end{cases} .$$

Finally, it applies the unitary $\mathbb{M}_{\mathfrak{D}_G, P}$.

Game 2:

$\quad$ **let** $(pk, sk) \leftarrow \mathrm{Gen}(1^n)$, $r^* \xleftarrow{\$} \{0,1\}^{k_0}$, $b \xleftarrow{\$} \{0,1\}$

$\quad$ **let** $m_0, m_1 \leftarrow A^{\mathsf{CStO}_H, \mathsf{CStO}_G, \mathbb{U}_{\mathrm{Dec}^{(1)}}}(pk)$

$\quad$ **let** $s^* := m_b || 0^{k_1} \oplus G(r^*)$, $t^* := r^* \oplus H(s^*)$, $c^* := f(s^*, t^*)$

$\quad$ **let** $b' \leftarrow A^{\mathsf{CStO}_H, \mathsf{CStO}_G, \mathbb{U}_{\mathrm{Dec}^{(1)}}}(c^*)$

$\quad$ **return** $[b = b']$

In the following, we show that $\mathbb{U}_{\mathrm{Dec}}$ and $\mathbb{U}_{\mathrm{Dec}^{(1)}}$ algorithms are indistinguishable and therefore Game 1 and Game 2 are indistinguishable.

1. When c^* is defined and $c = c^*$, both algorithms return $\perp$ without any random oracle queries. Since $\mathbb{U}_{\mathrm{Dec}^{(1)}}$ does not make any query to the random oracle G for decryption the second application of $\mathbb{M}_{\mathfrak{D}_G, P}$ undo the first application of $\mathbb{M}_{\mathfrak{D}_G, P}$. In other words, the database $\mathfrak{D}_G$ remains unaffected.

---

[3] Note that these dummy queries are required to make the number of queries submitted to G, H equal in both games.

2. When $z = \emptyset$, $\mathbb{U}_{\text{Dec}^{(1)}}$ returns $\perp$. We show that a ciphertext c for which $z = \emptyset$ and $\text{Dec}_{f^{-1}} \neq \perp$ can be generated only with a negligible probability. Let c is a ciphertext for which $z = \emptyset$ and $[s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1}$ where $(s', t') = f^{-1}(c)$. Note that since $z = \emptyset$, there is no pair (r, G_r) in $\mathfrak{D}_G$ that satisfies $[[f^{-1}(c)]^{n+k_1} \oplus G_r]_{k_1} = 0^{k_1}$. This means that the adversary has not queried the input $t' \oplus H(s')$ to G and since G is a random oracle, the probability of producing c is at most $1/2^{k_1}$. So $\mathbb{U}_{\text{Dec}}$ returns $\perp$ with the probability at least $1 - 1/2^{k_1}$. In addition, both algorithm make a query to the random oracles G, H to do the decryption. Note that the output register in a dummy query contain the uniform superposition and therefore it does not have any effect in the databases. Similar to the above, the second application of M_{DP}^G cancel out the first application of M_{DP}^G. So the database $\mathfrak{D}_G$ remains unaffected.

3. When $z \neq \emptyset$, both algorithms execute $\text{Dec}_{f^{-1}}$. We only need to show that the purified measurement $\mathbb{M}_{\mathfrak{D}_G, P}$ will not have any noticeable effect on $\mathfrak{D}_G$. To do that, we show $\mathbb{M}_{\mathfrak{D}_G, P}$ and $\text{Dec}_{f^{-1}}$ almost commute. Note that $\mathbb{M}_{\mathfrak{D}_G, P}$ interfaces with $\text{Dec}_{f^{-1}}$ when $\text{Dec}_{f^{-1}}$ makes a query to the random oracle G. By Lemma 2, if we commute $\mathbb{M}_{\mathfrak{D}_G, P}^c$ and $\text{Dec}_{f^{-1}}$, this will be distinguishable to the adversary with a probability at most $8 \cdot 2^{-\frac{n+k_1}{2}} \sqrt{2 \Gamma_{R_G^c}}$. Since $\Gamma_{R_G^c} = 2^n$, the distinguishing advantage of the adversary is at most $2^{-\frac{k_1}{2} - \frac{7}{2}}$.

Game 3: Let $\mathfrak{D}_H$ be the databases for CStO_H. In this game, the decryption oracle. $\mathbb{U}_{\text{Dec}^{(1)}}$ is changed to a new decryption oracle $\mathbb{U}_{\text{Dec}^{(2)}}$ that uses the databases $\mathfrak{D}_H$ and $\mathfrak{D}_G$ to decrypt. Let Search be a function that on input $(c, \mathfrak{D}_H, \mathfrak{D}_G)$ searches for the pairs (s, H_s) in $\mathfrak{D}_H$ and (r, G_r) in $\mathfrak{D}_G$ such that $c = f(s, r \oplus H_s)$ and $[G_r \oplus s]_{k_1} = 0^{k_1}$. If it finds such pairs, it returns $(1, [G_r \oplus s]^n)$, otherwise it returns $(0, \perp)$.

Let $Q_b Q_m$ be quantum registers of size $(n+1)$ that are initiated with zero. The unitary $\mathbb{U}_{\text{Dec}^{(2)}}$ first applies the unitary $\mathbb{U}_{\text{Search}}$ where its output is stored in $Q_b Q_m$ registers. Then it does as the following:

$$|c, y\rangle |b, m\rangle_{Q_b Q_m} \to \begin{cases} |c, y \oplus \perp\rangle |b, m\rangle & \text{if } c^* \text{ is defined } \& c = c^* \\ |c, y \oplus \perp\rangle |b, m\rangle & \text{if } b = 0 \\ |c, y \oplus m\rangle |b, m\rangle & \text{if } b = 1 \end{cases},$$

and in addition it submits dummy queries to the random oracles G, H when c^* is not defined or $c \neq c^*$ (in the last two lines when $b = 0, 1$). Finally, it applies $\mathbb{U}_{\text{Search}}$ to undo $Q_{b'} Q_m$ registers to zero.

Game 3:

---

   let $(pk, sk) \leftarrow \text{Gen}(1^n)$, $r^* \overset{\$}{\leftarrow} \{0,1\}^{k_0}$, $b \overset{\$}{\leftarrow} \{0,1\}$

   let $m_0, m_1 \leftarrow A^{\text{CStO}_H, \text{CStO}_G, \mathbb{U}_{\text{Dec}^{(2)}}}(pk)$

   let $s^* := m_b || 0^{k_1} \oplus G(r^*)$, $t^* := r^* \oplus H(s^*)$, $c^* := f(s^*, t^*)$

   let $b' \leftarrow A^{\text{CStO}_H, \text{CStO}_G, \mathbb{U}_{\text{Dec}^{(2)}}}(c^*)$

   return $[b = b']$

In the following, we show that $\mathbb{U}_{\mathrm{Dec}^{(1)}}$ and $\mathbb{U}_{\mathrm{Dec}^{(2)}}$ are indistinguishable:

1. When c^* is defined and $c = c^*$, both algorithms XOR $\perp$ to the output register without any random oracle queries.
2. When $b = 1$, it is clear that $z \neq \emptyset$ after invoking $M_{\mathfrak{D}_G P}^G$ in $\mathbb{U}_{\mathrm{Dec}^{(1)}}$. So both algorithms XOR $[G_r \oplus s]^n$ to the output register and make random oracle queries to G, H.
3. When $b = 0$ and $z = \emptyset$, both algorithms XOR $\perp$ to the output register and make random oracle queries to G, H.
4. When $b = 0$ and $z \neq \emptyset$. Both algorithms make queries to G, H. The algorithm $\mathbb{U}_{\mathrm{Dec}^{(1)}}$ invokes $\mathrm{Dec}_{f^{-1}}$ but $\mathbb{U}_{\mathrm{Dec}^{(2)}}$ returns $\perp$. We show that $\mathrm{Dec}_{f^{-1}}$ returns $\perp$ with a high probability. Let $c := f(s', t')$ for which $b = 0$. Recall that $b = 0$ means there are no pairs (s, H_s) in $\mathfrak{D}_H$ and (r, G_r) in $\mathfrak{D}_G$ such that $c = f(s, r \oplus H_s)$ and $[G_r \oplus s]_{k_1} = 0^{k_1}$. So if $(s', H_{s'})$ is in $\mathfrak{D}_H$ and $(t' \oplus H_{s'}, G_{t' \oplus H_{s'}})$ is in $\mathfrak{D}_G$, then $[s' \oplus G(t' \oplus H_{s'})]_{k_1} \neq 0^{k_1}$ and $\mathrm{Dec}_{f^{-1}}$ returns $\perp$. If $(s', H_{s'})$ is in $\mathfrak{D}_H$ and $(t' \oplus H_{s'}, G_{t' \oplus H_{s'}})$ is not in $\mathfrak{D}_G$, then $[s' \oplus G(t' \oplus H_{s'})]_{k_1} = 0^{k_1}$ with probability at most $1/2^{k_1}$ and $\mathrm{Dec}_{f^{-1}}$ returns $\perp$ with probability at least $1 - \frac{1}{2^{k_1}}$. If $(s', H_{s'})$ is not in $\mathfrak{D}_H$, from the adversary's point of view, $H_{s'}$ is an uniformly random value. Consequently, $t' \oplus H_{s'}$ is uniformly at random. Then $[s' \oplus G(t' \oplus H_{s'})]_{k_1} = 0^{k_1}$ with probability at most $1/2^{k_1}$ and $\mathrm{Dec}_{f^{-1}}$ returns $\perp$ with probability at least $1 - \frac{1}{2^{k_1}}$.

Game 4: This is identical to Game 3, except it measures all the queries to CStO_G with the projective measurements $\mathbb{M}_{r^*}$. If there is an 1-output measurement, it aborts and returns a random bit.

Game 4:

$\quad$ **let** $(pk, sk) \leftarrow \mathrm{Gen}(1^n)$, $r^* \xleftarrow{\$} \{0,1\}^{k_0}$, $b \xleftarrow{\$} \{0,1\}$
$\quad$ $\mathbb{M}_{r^*} = \{\mathbb{P}_1 = |r^*\rangle\langle r^*|, \mathbb{P}_0 = \mathbb{I} - \mathbb{P}_1\}$,
$\quad$ **run until** $\boxed{\textit{there is an 1-output measurement} \;\; \textit{with } \mathbb{M}_{r^*}}$
$\quad\quad$ **let** $m_0, m_1 \leftarrow A^{\mathsf{CStO}_H, \mathsf{CStO}_G, \mathbb{U}_{\mathrm{Dec}^{(3)}}}(pk)$
$\quad\quad$ **let** $s^* := m_b \| 0^{k_1} \oplus G(r^*)$, $t^* := r^* \oplus H(s^*)$, $c^* := f(s^*, t^*)$
$\quad\quad$ **let** $b' \leftarrow A^{\mathsf{CStO}_H, \mathsf{CStO}_G, \mathbb{U}_{\mathrm{Dec}^{(3)}}}(c^*)$
$\quad$ **return** $[b = b']$

If there is no query to CStO_G with non-negligible weight on the state $|r^*\rangle$, we can use Lemma 3 (gentle-measurement lemma) to show that these two games are indistinguishable. In more details, let ρ_i is the state of the i-th query (for $i \in [q_G]$) and let $\mathbb{M}_{r^*}(\rho_i)$ returns 1 with the probability ϵ_i. By the gentle-measurement lemma, the trace distance between $\mathbb{M}_{r^*}(\rho_i)$ and ρ_i is at most $\sqrt{\epsilon_i} + \epsilon_i$. So in overall, these two games are distinguishable with the advantage of at most $2q_G\sqrt{\max_i\{\epsilon_i\}}$. Therefore, if $\max_i\{\epsilon_i\}$ is negligible, two games are indistinguishable.

Proof by contrary, let assume $\mathcal{A}$ makes a query to CStO_G with a non-negligible weight on $|r^*\rangle$. From $\mathcal{A}$, we can construct an adversary $\mathcal{B}$ that breaks the quantum partial-domain one-wayness of f. In more details, $\mathcal{B}$ on input $c^*\big(:= f(s^*, t^*)$ for uniformly random $s^*, t^*\big)$, chooses a random element i from

$[q_G]$ and a random bit b, runs the adversary $\mathcal{A}$, answers random oracle queries and decryption queries using two compressed oracles CStO_H, CStO_G and finally it measures the input register of the i-th query to CStO_G and the database $\mathfrak{D}_H$ with the computational basis measurement, returns an output and aborts. In the following we describe $\mathcal{B}$ in more details.

Simulation of random oracle queries. For H-queries, the adversary $\mathcal{B}$ uses CStO_H. For G-queries, $\mathcal{B}$ does as follows. Let Find is an operator that on inputs $r, c^*, \mathfrak{D}_H$, checks if there exists a pair (s^*, H_{s^*}) in $\mathfrak{D}_H$ such that $c^* = f(s^*, r \oplus H_{s^*})$. If there exists such a pair it returns $(1, s^*)$. Otherwise, it returns $(0, 0^{n+k_1})$. For each query, $\mathcal{B}$ first applies Find operator with an ancillary register $Q_b Q_s$ of $(1 + n + k_1)$ qubits initiated with zero. Then, if the query is conducted before the challenge query or the Q_b is set to 0, it forwards the query to CStO_G, otherwise, it XORs $m_b || 0^{k_1} \oplus s^*$ to the output register:

$$
G' : |r, y\rangle\, |\mathfrak{D}_H\rangle \to \begin{cases} |r, y \oplus G(r)\rangle & \text{if } m_b \text{ is not defined} \\ |r, y \oplus G(r)\rangle & \text{if } \mathsf{Find}(\mathsf{r}, \mathsf{c}^*, \mathfrak{D}_\mathsf{H}) = (0, 0) \\ |r, y \oplus (m_b || 0^{k_1} \oplus s^*)\rangle & \text{if } \mathsf{Find}(\mathsf{r}, \mathsf{c}^*, \mathfrak{D}_\mathsf{H}) = (1, \mathsf{s}^*) \end{cases} .
$$

And finally it applies Find operator. Note that if there is no G-query with a non-negligible weight on $|r^*\rangle$ for which $\mathsf{Find}(\mathsf{r}^*, \mathsf{c}^*, \mathfrak{D}_\mathsf{H}) = (1, \mathsf{s}^*)$, CStO_G and G' are the same. Also, in this case, Find will cancel out with its second application. So the simulation of random oracle queries will be indistinguishable unless the adversary submits a post-challenge query with a non-negligible weight on the state $|r^*\rangle$ such that $\mathsf{Find}(\mathsf{r}^*, \mathsf{c}^*, \mathfrak{D}_\mathsf{H}) = (1, \mathsf{s}^*)$. (And if this happens, it breaks the quantum partial-domain one-wayness of f explained below.)

The challenge query. Upon receiving m_0 and m_1 from $\mathcal{A}$, the adversary $\mathcal{B}$ returns c^* as the challenge ciphertext.

Simulation of decryption queries. $\mathcal{B}$ uses the oracle $\mathbb{U}_{\mathrm{Dec}^{(3)}}$ on inputs $\mathfrak{D}_H$ and $\mathfrak{D}_G$ for the decryption queries. Note that G and G' only differ on the input r^* for which $c^* = f(s^*, r^* \oplus H_{s^*})$. Since $\mathbb{U}_{\mathrm{Dec}^{(3)}}$ on input c^* does not use its database and returns $\perp$, the simulation of the decryption queries is perfect.

Output of $\mathcal{B}$. The adversary $\mathcal{B}$ measures the (i)-th random oracle query to CStO_G with $\mathbb{M}_{r^*}$ and it measures the database $\mathfrak{D}_H$. Since there exists a query with a non-negligible weight on the state $|r^*\rangle$ for which $\mathsf{Find}(\mathsf{r}^*, \mathsf{c}^*, \mathfrak{D}_\mathsf{H}) = (1, \mathsf{s}^*)$, the adversary $\mathcal{B}$ can obtain r^* with a non-negligible probability. Then, the adversary searches over $\mathfrak{D}_H$ to find the s^* in which $c^* = f(s^*, r^* \oplus H_{s^*})$. Finally it returns s^* as the partial inverse of f on the input c^*. Since f is quantum partial-domain one-way, Games 4 and 3 are indistinguishable.

Now, it is clear that Game 4 returns 1 with the probability $1/2$ because if one of the measurements returns 1, the output of the game is a random bit. If non of measurements return 1, $G(r^*)$ remains an uniformly random value for $\mathcal{A}$ and consequently $m_b || 0^{k_1} \oplus G(r^*)$ is an uniformly random value for $\mathcal{A}$. So the probability that $\mathcal{A}$ guesses b is $1/2$. Finally, since each two consecutive games

12

are indistinguishable, the probability that $\mathcal{A}$ guesses b in Game 0 is $1/2 + \mathsf{neg}(\mathsf{n})$ and this finishes the proof of theorem. □

References

1. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In D. E. Denning, R. Pyle, R. Ganesan, R. S. Sandhu, and V. Ashby, editors, *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993.*, pages 62–73. ACM, 1993.

2. M. Bellare and P. Rogaway. Optimal asymmetric encryption. In A. D. Santis, editor, *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 92–111. Springer, 1994.

3. Boneh and M. Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In R. Canetti and J. A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 361–379. Springer, 2013.

4. D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In D. H. Lee and X. Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.

5. N. Cao, A. O'Neill, and M. Zaheri. Toward RSA-OAEP without random oracles. In A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, editors, *Public-Key Cryptography - PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7, 2020, Proceedings, Part I*, volume 12110 of *Lecture Notes in Computer Science*, pages 279–308. Springer, 2020.

6. C. Chen, O. Danba, J. Hoffstein, A. Hulsing, J. Rijneveld, J. M. Schanck, P. Schwabe, W. Whyte, Z. Zhang, T. Saito, T. Yamakawa, and K. Xagawa. Ntru, 2020. `https://ntru.org`.

7. C. Chevalier, E. Ebrahimi, and Q. H. Vu. On the security notions for encryption in a quantum world. *IACR Cryptol. ePrint Arch.*, 2020:237, 2020.

8. J. Don, S. Fehr, C. Majenz, and C. Schaffner. Online-extractability in the quantum random-oracle model. Cryptology ePrint Archive, Report 2021/280, 2021. `https://eprint.iacr.org/2021/280`.

9. E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. RSA-OAEP is secure under the RSA assumption. *J. Cryptology*, 17(2):81–104, 2004.

10. T. Gagliardoni, J. Krämer, and P. Struck. Quantum indistinguishability for public key encryption. *IACR Cryptol. ePrint Arch.*, 2020:266, 2020.

11. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information (10th Anniversary edition)*. Cambridge University Press, 2016.

12. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

13. V. Shoup. OAEP reconsidered. In J. Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 239–259. Springer, 2001.

14. E. E. Targhi and D. Unruh. Post-quantum security of the fujisaki-okamoto and OAEP transforms. In M. Hirt and A. D. Smith, editors, *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II*, volume 9986 of *Lecture Notes in Computer Science*, pages 192–216, 2016.

15. A. J. Winter. Coding theorem and strong converse for quantum channels. *IEEE Trans. Inf. Theory*, 45(7):2481–2485, 1999.

16. M. Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In A. Boldyreva and D. Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 239–268. Springer, 2019.