Post-quantum Security of 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 [11]) 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 [5], 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 [9] has sparked the necessity of replacing old cryptography with 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 [5] submission. The security of (unmodified) Optimal Asymmetric Encryption Padding (OAEP) in the quantum random oracle model has been mentioned as an interesting open question in [5]. The existing post-quantum security proof of OAEP [11] requires a modification to OAEP transform. (See details below.)

The random oracle model [1] is a powerful model in which the security of cryptographic scheme is proven assuming the existence of a truly random function that is accessible by all parties including the adversary. But in the 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 [10] showed it is an unjustified belief. Later, Fujisaki et al. [7] proved IND-CCA security of the OAEP-cryptosystem based on a stronger assumption, namely, partial-domain one-wayness of the underlying permutation.

Post-quantum security of OAEP transform has been studied in [11]. 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 [12] 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 [5], affirmatively.

Note that in the IND-qCCA notion, the adversary's challenge queries are restricted to be classical. In [6], the authors define a quantum IND-CCA notion in the real-or-random paradigm that grants the adversary the possibility of submitting quantum challenge queries. We leave verifying the security of OAEP in the sense of the definition in [6] as an open question.

Organization. In Section 2, we present some basics of quantum information and computation, security definitions needed in the paper and a short explanation for the Compressed Standard Oracle that has been introduced in [12] and we use it in the paper. In Section 3, we present OAEP scheme and show that it is IND-qCCA secure in the quantum random oracle model.

2 Preliminaries

Notations. Let $\mathtt{MSP}$ 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 $f(x)$.

2.1 Quantum Computing

We present basics of the quantum computing in this subsection. The interested reader can refer to [8] 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 $\mathcal{H}$. 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

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

where $b \in \{0, 1\}$. 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:

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

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

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* $\perp$ *if ciphertext c is not decryptable.*

In the following, we define IND-qCCA security notion [3] in the quantum random oracle model. 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:

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

where c^* is the challenge ciphertext and $\perp$ 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* $\mathcal{A}$

$$\Big|\Pr\Big[b = 1 : b \leftarrow \mathsf{Exp}^{qCCA,qRO,0}_{\mathcal{A},\mathcal{E}}(n)\Big] - \Pr\Big[b = 1 : b \leftarrow \mathsf{Exp}^{qCCA,qRO,1}_{\mathcal{A},\mathcal{E}}(n)\Big]\Big| \leq \mathsf{negl(n)},$$

where $\mathsf{Exp}^{qCCA,qRO,b}_{\mathcal{A},\mathcal{E}}(n)$ *game is define as:*
$\mathsf{Exp}^{qCCA,qRO,b}_{\mathcal{A},\mathcal{E}}(n)$ *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* $\mathcal{A}$ *is given the public key pk and with* ***quantum*** *oracle access to* $\mathbb{U}_{\mathrm{Dec}}$ *and* ***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 responds with* $c^* \leftarrow Enc_{pk}(m_b)$.

Guess: *The adversary* $\mathcal{A}$ *continues to query the decryption oracle and the random oracles, but may not query the ciphertext* c^* *in a decryption query. Finally, the adversary* $\mathcal{A}$ *produces a bit b.*

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

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

2.3 Compressed Standard Oracle

In this section, we present the high-level ideas of Compressed Standard Oracle (CStO) that has been introduced in [12]. This explanation is informal and the goal is to build the intuition behind CStO oracle. The interested reader can refer to [12] for more details. In the standard quantum random oracle model, a function H is chosen unifromly at random from the set of all functions (lets call it Ω_H) and a quantum algorithm $\mathcal{A}$ has quantum access to a random oracle H if $\mathcal{A}$ can submit queries in superposition and the oracle answers to these queries by applying a unitary transformation $\mathbb{U}_H$ that maps $|x,\ y\rangle$ to $|x,\ y \oplus H(x)\rangle$. The other way to consider this is to put the oracle state in superposition of all functions. Then, a query is implemented as

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

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 this two oracles are perfectly indistinguishable. Now if we apply QFT to the output register before and after applying StO, we will get the Phase oracle that operates as follows:

$$\mathsf{PhO} : |x, y\rangle \sum_H \frac{1}{|\Omega_H|} |H\rangle \to \sum_H \frac{1}{|\Omega_H|} (-1)^{y \cdot H(x)} |x, y\rangle |H\rangle .$$

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 input x and it is zero elsewhere. With this notation we can write the the query above as follows:

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

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

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

Note that $\mathsf{QFT}_{\mathfrak{D}}$ only effects the oracle state and it is undetectable to the adversary. Therefore, the oracle may learn which input/output have been queried when the adversary does make a query. Informally, the oracle can move the entry that is not zero in the database $P_{x,y}$ to the beginning of the oracle register. So, the database after the query is not zero only in the first slot. So the oracle can remove the zero slots to have a compressed database.

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

We only consider single query adversary in the presentation above. For general case, reader can refer to CStO presented in [12]. Note that we do not present the details of CStO here and only import the following lemma:

Lemma 1 (Lemma 4 in [12]). CStO *and* StO *are perfectly indistinguishable.*

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*

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

   where $r \xleftarrow{\$} \{0,1\}^{k_0}$*, and outputs the ciphertext* $c := f(s,t)$[1]*.*
3. Dec*: Given a ciphertext* (c,d)*, the decryption algorithm does the following: Compute* $f^{-1}(c) = (s,t)$ *and then,*
   (a) *query the random oracle* G *on input* r *and compute* $M := s \oplus G(r)$*.*
   (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 when $b = 0$ or this is $\mathsf{Exp}^{qCCA,qRO,0}_{\mathcal{A},\mathcal{OAEP}}(n)$.

Game 0:

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

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

[1] Q-OAEP in [11] outputs the ciphertext $c := \big(f(s,t), H'(s,t)\big)$ for a fresh random oracle H'.

Game 1:

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

Game 2: In this game we change $\mathbb{U}_{\mathrm{Dec}}$ oracle to $\mathbb{U}_{\mathrm{Dec}^{(1)}}$ oracle described below. Let $\mathfrak{D}_G$ denotes the database of CStO_G. Let Test be an unitary such that on input $(c, \mathfrak{D}_G)$ checks if there exists a pair $(r, G_r) \in \mathfrak{D}_G$ such that $[[f^{-1}(c)]^{n+k_1} \oplus G_r]_{k_1} = 0^{k_1}$. If it finds such a pair, it returns 1, otherwise, it returns 0. The output of Test is stored in an ancillary register Q_b. For each decryption query, first, $\mathbb{U}_{\mathrm{Dec}^{(1)}}$ applies the Test operator, then it executes $\mathbb{U}_{\mathrm{Dec}}$ and finally it applies $\mathsf{Test}^\dagger (= \mathsf{Test})$.

Game 2:

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

We show that Test and $\mathbb{U}_{\mathrm{Dec}}$ almost commutes, so Game 1 and Game 2 are indistinguishable. Note that to check if $[[f^{-1}(c)]^{n+k_1} \oplus G_r]_{k_1} = 0^{k_1}$, $\mathbb{U}_{\mathrm{Dec}}$ algorithm queries the random oracle G. So performing this check interfaces with $\mathfrak{D}_G$ and therefore with Test. Let $S \subseteq \{0,1\}^{n+k_1}$ be the set of all values s such that $[[f^{-1}(c)]^{n+k_1} \oplus s]_{k_1} = 0^{k_1}$. It is clear that $|S| = 2^n$. So we can consider $\mathbb{U}_{\mathrm{Dec}}$ (Test) checks if $G_r \in S$ ($G_r \in S$ in the Fourier domain). Now we can invoke Lemma 39 in [12] to show that these two unitaries are $1/2^{(k_1/2)-3}$-almost commute.

Game 3: In this game we change $\mathbb{U}_{\mathrm{Dec}^{(1)}}$ oracle to $\mathbb{U}_{\mathrm{Dec}^{(2)}}$. For each decryption query, $\mathbb{U}_{\mathrm{Dec}^{(2)}}$ first applies the Test operator. Then if the result of the test is 1, it executes $\mathbb{U}_{\mathrm{Dec}}$, otherwise, it XORs $\perp$ to the output register:

$$|c, y\rangle |b\rangle_{Q_b} \rightarrow \begin{cases} |c, y \oplus \perp\rangle |b\rangle & \text{if } c = c^* \\ |c, y \oplus \perp\rangle |b\rangle & \text{if } c \neq c^* \text{ and } b = 0 \\ \left|c, y \oplus \mathrm{Dec}_{f^{-1}}(c)\right\rangle |b\rangle & \text{if } c \neq c^* \text{ and } b = 1 \end{cases}.$$

And finally it applies Test to undo Q_b registers to zero.

Game 3:

let $r^* \xleftarrow{\$} \{0,1\}^{k_0}$, $(pk, sk) \leftarrow \mathrm{Gen}(1^n)$
let $m_0, m_1 \leftarrow A^{\mathsf{CStO}_H, \mathsf{CStO}_G, \mathbb{U}_{\mathrm{Dec}^{(2)}}}(pk)$
let $s^* := m_0 || 0^{k_1} \oplus G(r^*)$, $t^* := r^* \oplus H(s^*)$, $c^* := f(s^*, t^*)$
let $b' \leftarrow A^{\mathsf{CStO}_H, \mathsf{CStO}_G, \mathbb{U}_{\mathrm{Dec}^{(2)}}}(c^*)$
return b'

Note that $\mathbb{U}_{\mathrm{Dec}^{(1)}}$ and $\mathbb{U}_{\mathrm{Dec}^{(2)}}$ are exactly the same if $b = 1$. When $b = 0$, the adversary can distinguish these two games by querying a ciphertext c with non-negligible weight such that $\mathrm{Dec}_{f^{-1}}(c) \neq \perp$. Note that $\mathrm{Dec}_{f^{-1}}(c) \neq \perp$ implies $[[f^{-1}(c)]^{n+k_1} \oplus G_r]_{k_1} = 0^{k_1}$. But when $b = 0$, G_r is a uniformly random element from the adversary's point of view. Therefore, the probability that adversary finds a ciphertext c such that $\mathrm{Dec}_{f^{-1}}(c) \neq \perp$ and $b = 0$ is at most $1/2^{k_1}$. So these two games are distinguishable with the probability at most $q_{dec}/2^{k_1}$.

Game 4: Let $\mathfrak{D}_H$ be the databases for CStO_H. In this game, the decryption oracle $\mathbb{U}_{\mathrm{Dec}^{(2)}}$ is changed to a new decryption oracle $\mathbb{U}_{\mathrm{Dec}^{(3)}}$ 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 $\mathbb{U}_{\mathrm{Dec}^{(3)}}$ first applies the unitary $\mathbb{U}_{\mathsf{Search}}$ where its output is stored in $Q_{b'} Q_m$ registers. Then it does as the following:

$$|c, y\rangle |b, m\rangle_{Q_{b'} Q_m} \rightarrow \begin{cases} |c, y \oplus \perp\rangle |b, m\rangle & \text{if } c = c^* \\ |c, y \oplus \perp\rangle |b, m\rangle & \text{if } c \neq c^* \text{ and } b = 0 \\ |c, y \oplus m\rangle |b, m\rangle & \text{if } c \neq c^* \text{ and } b = 1 \end{cases}.$$

And finally it applies $\mathbb{U}_{\mathsf{Search}}$ to undo $Q_{b'} Q_m$ registers to zero.

Game 4:

let $r^* \xleftarrow{\$} \{0,1\}^{k_0}$, $(pk, sk) \leftarrow \mathrm{Gen}(1^n)$
let $m_0, m_1 \leftarrow A^{\mathsf{CStO}_H, \mathsf{CStO}_G, \mathbb{U}_{\mathrm{Dec}^{(3)}}}(pk)$
let $s^* := m_0 || 0^{k_1} \oplus G(r^*)$, $t^* := r^* \oplus H(s^*)$, $c^* := f(s^*, t^*)$
let $b' \leftarrow A^{\mathsf{CStO}_H, \mathsf{CStO}_G, \mathbb{U}_{\mathrm{Dec}^{(3)}}}(c^*)$
return b'

Note that when both $\mathbb{U}_{\mathsf{search}}$ and Test return $b = 0$, $\mathbb{U}_{\mathrm{Dec}^{(2)}}$ and $\mathbb{U}_{\mathrm{Dec}^{(3)}}$ XOR $\perp$ to the output register. Also, it is clear that if $\mathbb{U}_{\mathsf{search}}$ sets $Q_{b'}$ to 1, the unitary Test sets $Q_{b'}$ to 1 as well and therefore $\mathbb{U}_{\mathrm{Dec}^{(2)}}$ and $\mathbb{U}_{\mathrm{Dec}^{(3)}}$ return the same output. (Both XOR $[G_r \oplus s]^n$ to the output register.) So the adversary can distinguish these two games if he submits a query $c := f(s, t := r \oplus H_s)$ with non-negligible weight such that $\mathbb{U}_{\mathsf{search}}$ returns $b = 0$ and Test returns $b = 1$. But this means

that (s, H_s) is not in $\mathfrak{D}_H$. So from the adversary's point of view, H_s is an uniformly random value. Consequently, $t = r \oplus H_s$ is uniformly at random. Since f is a permutation, the probability of producing such a ciphertext c is at most $1/2^{k_0}$. so these two games are distinguishable with the probability at most $q_{dec}/2^{k_0}$

Game 5: In this game, the oracle measures the input register of all queries to CStO_G conducted before the challenge phase with the projective measurements $\mathcal{M}_{r^*} = \{\mathbb{P}_0, \mathbb{P}_1\}$ where $\mathbb{P}_1 = |r^*\rangle\langle r^*|$ and $\mathbb{P}_0 = \mathbb{I} - \mathbb{P}_1$. If the result of the measurement on one of the queries is 0, it returns a random bit and it aborts. Otherwise, it sends the query to CStO_G oracle.

Game 5:

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

The adversary $\mathcal{A}$ can distinguish Game 4 and Game 5 by submitting a query to CStO_G that has a non-negligible weight on the state $|r^*\rangle$. Assume that the adversary makes q_{G1} queries to the CStO_G before the challenge phase. Since r^* is an uniformly random value that has not been used in the challenge phase yet, the probability that the adversary can distinguish these two games is at most $q_{H1}/2^{k_0}$.

Game 6: In this game, the oracle measures the input register of all queries to CStO_H conducted before the challenge phase with the projective measurements $\mathcal{M}_{s^*} = \{\mathbb{P}_0, \mathbb{P}_1\}$ where $\mathbb{P}_1 = |s^*\rangle\langle s^*|$ and $\mathbb{P}_0 = \mathbb{I} - \mathbb{P}_1$. If the result of the measurement on one of the queries is 0, it returns a random bit and it aborts. Otherwise, it sends the query to CStO_H oracle.

Game 6:

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

The adversary $\mathcal{A}$ can distinguish Game 5 and Game 6 by submitting a query to CStO_H that has a non-negligible weight on the state $|s^*\rangle$. Assume that the adversary makes q_{H1} queries to the CStO_H before the challenge phase. Since r^* has not been queried to CStO_G, $G(r^*)$ is an uniformly random value from the adversary's point of view. So $s^* := m_0||0^{k_1} \oplus G(r^*)$ is an uniformly random value. This means that the probability that the adversary can distinguish these two games is at most $q_{H1}/2^{n+k_1}$.

Game 7: This is identical to Game 6, except the oracle measures all the queries to CStO_H and CStO_G with the projective measurements $\mathcal{M}_{s^*}$ and $\mathcal{M}_{r^*}$, respectively. If there is an 1-output measurement, the oracle aborts and returns a random bit. Let q_{H2} and q_{G2} be the number of queries to CStO_H and CStO_H after the challenge phase, respectively.

Game 7:

let $r^* \xleftarrow{\$} \{0,1\}^{k_0}$, $(pk, sk) \leftarrow \mathrm{Gen}(1^n)$,
$\mathcal{M}_{r^*} = \{\mathbb{P}_1 = |r^*\rangle\langle r^*|, \mathbb{P}_0 = \mathbb{I} - \mathbb{P}_1\}$,
$\mathcal{M}_{s^*} = \{\mathbb{P}_1 = |s^*\rangle\langle s^*|, \mathbb{P}_0 = \mathbb{I} - \mathbb{P}_1\}$
run until *there is an 1-output measurement with* $\mathcal{M}_{r^*}$ *or* $\mathcal{M}_{s^*}$
  $A^{\mathsf{CStO}_H, \mathsf{CStO}_G, \mathbb{U}_{\mathrm{Dec}^{(3)}}}(pk)$
return a random bit if there is an 1-output measurement and abort
run until *there is an 1-output measurement with* $\mathcal{M}_{r^*}$ *or* $\mathcal{M}_{s^*}$
  let $m_0, m_1 \leftarrow A^{\mathbb{U}_{\mathrm{Dec}^{(3)}}}(pk)$
  let $s^* := m_0||0^{k_1} \oplus G(r^*)$, $t^* := r^* \oplus H(s^*)$, $c^* := f(s^*, t^*)$
  let $b' \leftarrow A^{\mathsf{CStO}_H, \mathsf{CStO}_G, \mathbb{U}_{\mathrm{Dec}^{(3)}}}(c^*)$
return a random bit if there is an 1-output measurement and abort.
Otherwise, return b'

The adversary $\mathcal{A}$ can distinguish Game 6 and Game 7 by submitting a query to CStO_H that has a non-negligible weight on the state $|s^*\rangle$, after the challenge phase. Or $\mathcal{A}$ can distinguish Game 6 and Game 7 by submitting a query to CStO_G that has a non-negligible weight on the state $|r^*\rangle$, after the challenge phase. Let ϵ be the probability that $\mathcal{A}$ submits such a query. From $\mathcal{A}$ that distinguishes Game 6 and Game 7, 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 $[q_{H2+q_G2}]$, runs the adversary $\mathcal{A}$ using two compressed oracles CStO_H, CStO_G and private compressed oracle $\mathsf{CStO}_{G'}$. The random oracle G is define as follows:

$$|r, y\rangle\,|\mathfrak{D}_H\rangle \to \begin{cases} |r, y \oplus G'(r)\rangle & \text{if } \mathsf{Find}(\mathsf{r}, \mathsf{c}^*, \mathfrak{D}_\mathsf{H}) = (0, 0) \\ |r, y \oplus (m_0||0^{k_1} \oplus s^*)\rangle & \text{if } \mathsf{Find}(\mathsf{r}, \mathsf{c}^*, \mathfrak{D}_\mathsf{H}) = (1, \mathsf{s}^*) \end{cases},$$

where 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 $(0, 0^{n+k_1})$. We can implement the oracle G as follows.

1. First we initiate an ancillary register Q_bQ_s of $(1+n+k_1)$ qubits with zero. These registers store the output of Find. Then we apply $\mathbb{U}_{\mathsf{Find}}$ to the input register (r-register), $\mathfrak{D}_H$ and Q_bQ_s registers.

2. We apply controlled-unitary $\mathbb{U}_{m_0||0^{k_1}\oplus s^*}$ on registers Q_bQ_s and y-register. Basically, if Q_b is set to 1, it XORs y-register with $m_0||0^{k_1}\oplus s^*$. Otherwise, it is identity.

3. Next, we apply bit-flip unitary $\mathbb{X}$ to Q_b.

4. Then, we apply controlled-unitary $\mathbb{U}_{G'}$ on registers Q_b, r-register and y-register where the control register is Q_b.

5. Finally, we apply $\mathbb{U}_{\mathsf{Find}}$ to the input register (r register), $\mathfrak{D}_H$ and Q_bQ_s register. This uncomputes Q_bQ_s register to zero.

Since the message m_0 is not known to $\mathcal{B}$ before the challenge query, it seems that CStO_G defined above can not be sued to answer queries before the challenge phase. However, before the challenge query, the adversary $\mathcal{B}$ forwards queries to CStO_G only if Find returns 0. Here, for each query on input $|r,y\rangle$, $\mathcal{B}$ invokes Find on inputs $r, \mathfrak{D}_H, c^*$ and stores the result of check in Q_bQ_s. Then it measures Q_b. If the measurement outcome is 1, it aborts and returns a random bit. Otherwise, it forwards the query to CStO_G. Note that since f is a permutation and only one r satisfies $c^* = f(s^*, r\oplus H_{s^*})$, this is the same as we measure the input register with $\{|r\rangle\langle r|, \mathbb{I}-|r\rangle\langle r|\}$ where $c^* = f(s^*, r\oplus H_{s^*})$. In addition, the measurement in Q_b is equivalent to measuring the database $\mathfrak{D}_H$ with $\mathcal{M}_{s^*}$ and this is equivalent to measuring the input of queries to CStO_H with $\mathcal{M}_{s^*}$. Therefore, the adversary simulates the queries in Game 3 and Game 4, before the challenge query.

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 in 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.

The adversary $\mathcal{B}$ measures the (i)-th random oracle query after the challenge phase. If the (i)-th random oracle query is submitted to CStO_H, $\mathcal{B}$ measures with $\mathcal{M}_{s^*}$, otherwise, it measures with $\mathcal{M}_{r^*}$. It returns the post-measurement state and aborts. Since there exists a query with non-negligible weight on $|s^*\rangle$ or $|r^*\rangle$, the adversary $\mathcal{B}$ can break the quantum partial-domain one-wayness of f with probability $\frac{\epsilon}{q_{H2}+q_{G2}}$. (Note that when the post-measurement state is $|r^*\rangle$, the adversary computes $s^* = m_0||0^{k_1}\oplus G(r^*)$ and returns s^* as the partial inverse of f on the input c^*.)

Game 8: In this game, we replace m_0 with m_1 in the definition of s^*.

Game 8:

Let $r^* \xleftarrow{\$} \{0,1\}^{k_0}$, $(pk, sk) \leftarrow \mathrm{Gen}(1^n)$,
$\mathcal{M}_{r^*} = \{\mathbb{P}_1 = |r^*\rangle\langle r^*|, \mathbb{P}_0 = \mathbb{I} - \mathbb{P}_1\}$,
$\mathcal{M}_{s^*} = \{\mathbb{P}_1 = |s^*\rangle\langle s^*|, \mathbb{P}_0 = \mathbb{I} - \mathbb{P}_1\}$
run until *there is an 1-output measurement with* $\mathcal{M}_{r^*}$ *and* $\mathcal{M}_{s^*}$
  $A^{\mathsf{CStO}_H, \mathsf{CStO}_G, \mathbb{U}_{\mathrm{Dec}^{(3)}}}(pk)$
return a random bit if there is an 1-output measurement and abort
run until *there is an 1-output measurement with* $\mathcal{M}_{r^*}$ *and* $\mathcal{M}_{s^*}$
  let $m_0, m_1 \leftarrow A^{\mathbb{U}_{\mathrm{Dec}^{(3)}}}(pk)$
  let $s^* := m_1 || 0^{k_1} \oplus G(r^*)$, $t^* := r^* \oplus H(s^*)$, $c^* := f(s^*, t^*)$
  let $b' \leftarrow A^{\mathsf{CStO}_H, \mathsf{CStO}_G, \mathbb{U}_{\mathrm{Dec}^{(3)}}}(c^*)$
return a random bit if there is an 1-output measurement and abort.
Otherwise, return b'

Note that Game 6 and Game 7 are indistinguishable since r^* has not been queried to CStO_G and therefore we can replace $G(r^*)$ with a random value. So the distribution of $m_0||0^{k_1} \oplus G(r^*)$ and $m_1||0^{k_1} \oplus G(r^*)$ are the same.

Games 9-15: We can switch to $\mathsf{Exp}^{qCCA,qRO,1}_{\mathcal{A},\mathcal{OAEP}}(n)$ game similar to what we have done above to reach Game 5.

Since each two consecutive games are indistinguishable, we have shown that

$$\left|\Pr\left[b = 1 : b \leftarrow \mathsf{Exp}^{qCCA,qRO,0}_{\mathcal{A},\mathcal{OAEP}}(n)\right] - \Pr\left[b = 1 : b \leftarrow \mathsf{Exp}^{qCCA,qRO,1}_{\mathcal{A},\mathcal{OAEP}}(n)\right]\right| \leq \mathsf{negl(n)}.$$

□

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. 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.
6. 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.
7. E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. RSA-OAEP is secure under the RSA assumption. *J. Cryptology*, 17(2):81–104, 2004.
8. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information (10th Anniversary edition)*. Cambridge University Press, 2016.
9. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.
10. 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.
11. 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.
12. 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.