Master's Thesis

# A Security Proof of FO-PKC in the Quantum Random Oracle Model

Naoki Hasegawa

Supervisor : Prof. Eiichiro Fujisaki

Graduate School of Advanced Science and Technology
Japan Advanced Institute of Science and Technology
(Information Science)

March, 2025

**Abstract**

In recent years, expectations for the realization of quantum computers have increased, and the research on post-quantum cryptography (PQC) has become active. Accordingly, the National Institute of Standards and Technology (NIST) has been working on a standardization project for post-quantum cryptography. Cryptographic schemes utilizing hash functions have traditionally been studied and developed with a focus on their security in the Random Oracle Model (ROM), which considers only classical algorithms. However, in the post-quantum cryptography, it is common to use the Quantum Random Oracle Model (QROM), which accounts for quantum algorithms that allow superposition queries to the random oracle. The security evaluation of cryptographic schemes in the QROM is an important topic, as the understanding of security in this model remains incomplete.

The Fujisaki-Okamoto (FO) transformation is a generic method for converting any weak public-key encryption scheme into an IND-CCA secure public-key encryption scheme in the random oracle model. There are two versions of the FO transformation: the PKC version and the CRYPTO version. While the FO transformation has been extensively studied in the classical Random Oracle Model, it is not yet fully understood whether similar results hold in the QROM. In the QROM, the security of the FO transformation has been established through security proofs in the CRYPTO version and its improved version. However, the security proof for the PKC version has not yet been completed.

The reserch in the QROM, properties that could be applied in ROM cannot be used without proof in QROM. Therefore, a key challenge is to prove whether the same theorems and properties as in ROM can be applied or to devise alternative approaches. In the QROM, the challenge was to record queries to the random oracle, which can be done trivially in the classical model. However, Zhandry developed in the compressed oracle technique, which can record queries on the oracle side in the QROM.

Subsequently, Don et al. showed that an upper bound on the computational error when exchanging the order of a unitary operator and a measurement operator within the compressed oracle. This bound, known as the commutator bound, showed that in the QROM, the order of computations in algorithms can be interchanged within a statistical error margin.

From these results, Don et al. constructed a simulator capable of extracting the content of an adversary's queries to the QROM without the adversary

being aware of it and before all queries are completed. Applying this simulator, they provided a security proof for the CRYPTO version of the FO transformation, which converts a PKE with one-way security against CPA attacks (OW-CPA) into a KEM with indistinguishability security against CCA attacks (IND-CCA).

However, to the best of our knowledge, there is no existing security proof for the FO transformation in the PKC version, which converts a PKE with indistinguishability security against CPA attacks (IND-CPA) into a PKE with IND-CCA security.

In this paper, we provide a security proof for the FO-PKC version in the Quantum Random Oracle Model, referencing the proof techniques used by Don et al.

The key point of this proof lies in the differences between proofs in the ROM and QROM. In the QROM proof, the order of the steps differs from that in the ROM proof.

In the ROM, where inputs and outputs are classical bits, it is straightforward to record the access to the random oracle and extract its contents. As a result, after providing the adversary with the challenge ciphertext $c^*$, the decryption oracle can be replaced with one that extracts results by referencing the random oracle access. This operation allows the implementation of a decryption oracle that does not require the secret key. Subsequently, the proof is completed by bounding the differences introduced by this replacement using the OW-Game.

On the other hand, in the QROM, where superposition inputs are allowed, recording and extracting query contents requires the use of a compressed oracle. This necessitates a method for replacing the compressed oracle.

In both classical and quantum proofs, the challenge ciphertext $c^*$ is generated during the initial setup of the game. At this point, the random oracle $H$ is accessed, and its output is used to encrypt $c^*$. In the classical proof, the simulation of the decryption oracle is performed first. To follow the same order in the quantum proof, $H$ must be replaced with a compressed oracle. However, the compressed oracle must be implemented independently of the challenge ciphertext $c^*$. Therefore, it is not possible to conduct the quantum proof in the same order as the classical proof.

To resolve this issue, the quantum proof replaces $H$ with a different random oracle $H'$. The differences introduced by this replacement can be bounded using the O2H lemma. Subsequently, this replaced $H$ is further replaced with a compressed oracle, enabling the challenge ciphertext $c^*$ and the compressed oracle to be treated independently. This replacement allows query recording and extraction, eliminating the need for the secret key, thereby completing the proof.Abstract of this paper

Future work in this study includes improvements to One Way to Hiding Lemma (O2H) and to the commutator bound. In the current proof method, the application of O2H bounds the probability using a square root of the probability. In the classical model, the probability is bounded by the probability without the square root, so if the probability can be bounded by the probability without or close to the square root in the quantum case using some method, better security evaluation results can be obtained.

Additionally, in this proof, the order of the algorithms in the simulator is interchanged, and the error term is generated by the number of such swaps and the commutator bound. Therefore, if the commutator bound can be bounded to a smaller upper bound or the number of exchanging can be reduced to a smaller number, the error term will be smaller, and leading to improved results.

# Contents

**1 Introduction** **1**

**2 Preliminaries** **2**
2.1 Quantum Computation . . . . . 2
2.2 The compressed oracle . . . . . 3
2.2.1 The Fourier basis . . . . . 3
2.2.2 The Compressed Oracle . . . . . 3

**3 Preparation for Proof** **5**
3.1 Measurement Operator . . . . . 5
3.2 A Commutator Bound . . . . . 6
3.3 The Extractable RO-Simulator $S$ . . . . . 6
3.4 One Way to Hiding Lemma . . . . . 8

**4 QROM-Security of Fujisaki-Okamoto Transformation** **9**
4.1 The Fujisaki-Okamoto Transfomation . . . . . 9
4.1.1 A public-key encryption scheme . . . . . 9
4.1.2 The Fujisaki-Okamoto Transfomation . . . . . 9
4.1.3 Security of Public Key Encryption (PKE) . . . . . 11
4.2 Security of FO-PKC in the QROM . . . . . 14
4.2.1 Main Theorem . . . . . 14
4.2.2 Proof of the Theorem . . . . . 14

**5 Summary** **22**

# List of Algorithms


1 GAME IND-CPA-PKE . . . . . 11
2 GAME IND-CCA-PKE . . . . . 11
3 ***Proof.*** of $\gamma$-spread . . . . . 13
4 Game Setup . . . . . 15
5 Main Phase . . . . . 16
6 random oracle . . . . . 16
7 Dec oracle . . . . . 16
8 O2H . . . . . 17

# List of Tables

4.1 A security proof of FO Transformation in the QROM . . . . . 11

# Chapter 1

# Introduction

The Fujisaki-Okamoto (FO) transformation is a generic method for converting any weak public-key encryption scheme into an IND-CCA secure public-key encryption scheme in the random oracle model. It exists in two versions: PKC[FO99a] and CRYPTO[FO99b, FO13]. The original proposed method has its security proven in the classical Random Oracle Model. In Chapter 4, we will explore the Fujisaki-Okamoto (FO) transformation in detail.

The compressed oracle technique, developed in [Zha19], allows queries to be recorded on the oracle side in the QROM. Using this technique, Don et al. showed that a bound on the operator norm of the commutator $[O_{XYD}, M_{DP}]$ (Commutator Bound [Thm3.2]) of the unitary operator $O_{XYD}$, which described the evolution of the compressed oracle, and the (purified) measurement operator $M_{DP}$ in the QROM. This result addressed a key challenge in QROM by showing that the order of computations can be interchanged within a statistical error margin.

In addition, by applying this method, they constructed a simulator that can extract the content of an adversary's queries to the QROM without noticing the adversary, and before all queries are completed. Using this simulator, they provided a security proof for the CRYPTO version of the FO transformation, which converts a PKE with one-way security against CPA attacks (OW-CPA) into a KEM with indistinguishability security against CCA attacks (IND-CCA).

However, to the best of our knowledge, there is no existing security proof for the FO transformation addressed in FO-PKC, which converts a PKE with indistinguishability security against CPA attacks (IND-CPA) into a PKE with IND-CCA security. In this paper, we provide a security proof for the FO-PKC version in the Quantum Random Oracle Model.

# Chapter 2

# Preliminaries

## 2.1 Quantum Computation

In this paper, complex vectors are expressed using Dirac notation. In this notation, $|\psi\rangle$ represents a column vector. $\langle\psi|$ represents the conjugate row vector of $|\psi\rangle$. The symbol $\dagger$ is defined as the conjugate transpose of the original vector, i.e., $\langle\psi| = |\psi\rangle^\dagger$. We define the inner product in this notation. The inner product is defined by combining the $\langle|$ vector and the $|\rangle$ vector and is written as $\langle\psi| \cdot |\phi\rangle = \langle\psi|\phi\rangle$. The norm of the vector $|\psi\rangle$ is defined as $|| \, |\psi\rangle \, || = \sqrt{\langle\psi|\psi\rangle}$.
The computational basis states $|0\rangle$ and $|1\rangle$ are defined as:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.1}$$

A quantum bit (qubit) differs from a classical bit in that its state can be expressed as a superposition of $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{2.2}$$

where $a, b \in \mathbb{C}, |a|^2 + |b|^2 = 1$
A set of projection operators $\{P_i\}_i$ satisfies $\sum_i P_i = I$. When measuring a quantum state $|\psi\rangle$, the probability $p(m)$ of obtaining the measurement result $m$ is given by:

$$p(m) = ||P_m \, |\psi\rangle \, ||^2 \tag{2.3}$$

For example, consider a quantum state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ measured using the projection operators $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$. The probabilities of

obtaining 0 and 1 are:

$$p(0) = ||P_0 |\psi\rangle||^2 = |a|^2, \quad p(1) = ||P_1 |\psi\rangle||^2 = |b|^2. \tag{2.4}$$

This measurement collapses the internal state from a superposition (where the output probabilities are $|a|^2$ or $|b|^2$) to a state where the output is deterministic (0 or 1 with probability 1). As a result, the internal state after measurement differs from the pre-measurement state, potentially altering subsequent outputs depending on whether measurement has occurred. Furthermore, for an operator $A \in \mathcal{L}(\mathcal{H})$, *operatornorm* $||A||$ is defined as:

$$||A|| = \max_{|\phi\rangle} ||A |\phi\rangle|| \tag{2.5}$$

where the max is over all $|\phi\rangle \in \mathcal{H}$ with norm 1.

## 2.2 The compressed oracle

In this papper, we refer to it as $X = \{0,1\}^m$, $|X| = 2^m = M$, $Y = \{0,1\}^n$, $|Y| = 2^n = N$.
The definitions and notations in this section are based on references [NC10], [Zha19] and [CFHL21].

### 2.2.1 The Fourier basis

The computational basis $|j\rangle$ transformed into the basis $|\hat{j}\rangle$ as described below is called the Fourier basis.

**Definition 2.2.1** (The Quantum Fourier Transform (QFT))**.**

$$|j\rangle \to |\hat{j}\rangle := \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \omega_N^{jk} |k\rangle \tag{2.6}$$

where $\omega_N \in \mathbb{C}$ is Nth roots of unity. $\{|\hat{j}\rangle\}$ is the Fourier basis of $\{|j\rangle\}$.

### 2.2.2 The Compressed Oracle

**Definition 2.2.2** (Oracle)**.** $O$ is a unitary operator defined as follows:

$$O : |x\rangle |y\rangle \otimes |H\rangle \to |x\rangle |y + H(x)\rangle \otimes |H\rangle \tag{2.7}$$

**Lemma 2.2.3.** Considering the Quantum Fourier basis under the above definition, the following holds:

$$\begin{aligned} O : |x\rangle |\hat{y}\rangle \otimes |\hat{H}\rangle &\to |x\rangle |\hat{y}\rangle \otimes O_{x\hat{y}} |\hat{H}\rangle \\ &= |x\rangle |\hat{y}\rangle \otimes |\hat{H} - \hat{y} \cdot \delta_x\rangle \end{aligned} \tag{2.8}$$

where $\delta_x : X \to \{0,1\}$ satisfies $\delta_x(x) = 1$ and $\delta_x(x') = 0$ for all $x' \neq x$. And,

$$\begin{aligned} |\hat{H}\rangle &:= \bigotimes_x |\widehat{H(x)}\rangle \\ |\hat{H} - \hat{y} \cdot \delta_x(x)\rangle &:= |\widehat{H(0)}\rangle \otimes \cdots \otimes |\widehat{H(M-1)}\rangle \end{aligned} \tag{2.9}$$

**Definition 2.2.4** ($\mathrm{Comp}_x$)**.** The unitary operator $\mathrm{Comp}_x$, acting on the corresponding part of $x$, is defined as follows:

$$\mathrm{Comp}_x := |\perp\rangle \langle\hat{0}| + |\hat{0}\rangle \langle\perp| + \sum_{\hat{z} \neq \hat{0}} |\hat{z}\rangle \langle\hat{z}| \tag{2.10}$$

**Definition 2.2.5** (Comp)**.** Comp is a unitary operator defined as follows:

$$\mathrm{Comp} |x\rangle |y\rangle |D\rangle := |x\rangle |y\rangle \otimes \mathrm{Comp}_x |D\rangle \tag{2.11}$$

**Definition 2.2.6** (Compressed Oracle)**.** $O_{XYD}$ is a unitary operator defined as follows:

$$O_{XYD} := \mathrm{Comp} \circ O \circ \mathrm{Comp}^\dagger \tag{2.12}$$

# Chapter 3

# Preparation for Proof

## 3.1 Measurement Operator

The definitions and notations in section3.1 to section 3.3 are based on references [DFMS22].

**Definition 3.1.1.** We consider an arbitrary but fixed relation $R \subset X \times \{0,1\}^n$. A crucial parameter of the relation $R$ is the number of $y$'s that fulfill the relation together with $x$, maximized over all possible $x \in X$:

$$\Gamma_R := \max_{x \in X} |\{y \in \{0,1\}^n | (x,y) \in R\}| \tag{3.1}$$

**Definition 3.1.2** (Projectors $\Pi$)**.** Given the relation $R$, $\Pi$ are projectors defined as follows:

$$\begin{aligned} \Pi^x_{D_x} &:= \sum_{y \text{ s.t } (x,y)\in R} |y\rangle \langle y|_{D_x} \\ \Pi^{\emptyset}_D &:= \mathbb{1}_D - \sum_{x \in X} \Pi^x_{D_x} = \bigotimes_{x \in X} \bar{\Pi}^x_{D_x} \end{aligned} \tag{3.2}$$

with $\bar{\Pi}^x_{D_x} := \mathbb{1}_{D_x} - \Pi^x_{D_x}$. Here, $\Pi^x_{D_x}$ checks whether there exists a pair $(x,y) \in R$ for $D_x$.

**Definition 3.1.3** (Measurement Operator $\mathcal{M}$)**.** $\mathcal{M} = \mathcal{M}^R$ to be given by the projectors are the measurement defined as follows:

$$\begin{aligned} \Sigma^x &:= \bigotimes_{x'<x} \bar{\Pi}^{x'}_{D_{x'}} \otimes \Pi^x_{D_x} \\ \Sigma^{\emptyset} &:= \mathbb{1} - \sum_{x'} \Sigma^{x'} = \bigotimes_{x'} \bar{\Pi}^{x'}_{D_{x'}} = \Pi^{\emptyset} \end{aligned} \tag{3.3}$$

where $x$ ranges over all $x \in X$. Here, a measurement outcome $x$ by $\mathcal{M}$ means that register $D_x$ is the first to contain a value $y$ satisfying $(x, y) \in R$ . On the other hand, a outcome $\emptyset$ means that no register contains such a value.

**Definition 3.1.4** ($Purified$ Measurement $M_{DP}$)**.** The $purrified$ measurement $M_{DP} = M_{DP}^R \in \mathcal{L}(\mathcal{H}_D \otimes \mathcal{H}_R)$ is defined as follows by the unitary:

$$\begin{aligned} M_{DP} &:= \sum_{x \in X \cup \{\emptyset\}} \Sigma^x \otimes X^x : \\ |\varphi\rangle_D |\omega\rangle_P &\to \sum_{x \in X \cup \{\emptyset\}} \Sigma^x |\varphi\rangle_D |\omega + x\rangle_P \end{aligned} \tag{3.4}$$

In both $X^x$ and $\omega + x$, $x \in X \cup \{\emptyset\}$ is understood to be encoded as an element of $\mathbb{Z}/(|X|+1)\mathbb{Z}$, $\dim(\mathcal{H}_P) = d := |X| + 1$, and $X \in \mathcal{L}(\mathcal{H}_P)$ is the generalized Pauli operator of order $d$, mapping $|\omega\rangle$ to $|\omega + 1\rangle$.

## 3.2 A Commutator Bound

**Theorem 3.2.1.** (Commutator Bound [DFMS22]) For *any relation* $R \subset X \times \{0,1\}^n$ and $\Gamma_R$ as defined in Eq(3.1), the $purified$ measurement $M_{DP}$ defined in Eq(3.4) almost commutes with the oracle unitary $O_{XYD}$:

$$|||[O_{XYD}, M_{DP}]||| \leq 8\sqrt{2\Gamma_R/2^n} \tag{3.5}$$

where $[A, B] = AB - BA$

## 3.3 The Extractable RO-Simulator $S$

**Definition 3.3.1.** For $f : X \times \{0,1\}^n \to \mathcal{C}$, $\Gamma(f)$ and $\Gamma'(f)$ are defined as follows:

$$\Gamma(f) := \max_{x,c} |\{y | f(x, y) = c\}| \tag{3.6}$$

$$\Gamma'(f) := \max_{x \neq x', y'} |\{y | f(x, y) = f(x', y')\}| \tag{3.7}$$

In encryption, $f$ is replaced by $Enc$

**Definition 3.3.2** (RO-Simulator)**.** The extractable RO-Simulator $S$ is defined as follows:

The extractable RO-Simulator $S$

- Initialization: $S$ prepares its internal register $D$ to be in state $|\perp\rangle_D := \otimes_x |\perp\rangle_{D_x}$
- *S.RO-query*: Upon a (quantum)*RO-query*, with query registers $XY$, $S$ applies $O_{XYD}$ to registers $XYD$.
- *S.E-query*: Upon a classical extraction-query with input $c$, $S$ applies $\mathcal{M}^R$ to $D$ and returns the outcome $\hat{x}$.

**Theorem 3.3.3.** [DFMS22] The extractable RO-simulator $S$ constructed above, with interface $S.RO$ and $S.E$, satisfies the following properties.

1. If $S.E$ is unused, $S$ is perfectly indistinguishable from the random oracle RO.

2.a Any two subsequent independent queries to $S.RO$commute. In particular, two subsequent classical *S.RO-queries* with the same input $x$ give identical responses.

2.b Any two subsequent independent queries to $S.E$ commute. In particular, two subsequent classical *S.E-queries* with the same input $c$ give identical responses.

2.c Any two subsequent independent queries to $S.E$ and $S.RO$ is $8\sqrt{2\Gamma(f)/2^n}$ almost-commute.

3 Any classical query $S.RO(x)$ and any classical query $S.E(c)$ are both idempotent.

4.a If $\hat{x} = S.E(c)$ and $\hat{h} = S.RO(\hat{x})$ are two subsequent classical queries then

$$\Pr[f(\hat{x}, \hat{h}) \neq t \wedge \hat{x} \neq \emptyset] \leq \Pr[f(\hat{x}, \hat{h}) \neq t | \hat{x} \neq \emptyset] \leq 2 \cdot 2^{-n}\Gamma(f) \quad (3.8)$$

4.b If $h = S.RO(x)$ and $\hat{x} = S.E(f(x, h))$ are two subsequent classical queries such that no prior query to $S.E$ has been made, then

$$\Pr[\hat{x} = \emptyset] \leq 2 \cdot 2^{-n} \quad (3.9)$$

**Proposition 3.3.4.** Let $R' \subseteq X \times \mathcal{C}$ be a relation unrelated to $R$. Consider a query algorithm A that makes $q$ queries to the $S.RO$ interface of $S$ but no query to $S.E$, outputting some $\mathbf{c} \in \mathcal{C}^l$. For each $i$, let $\hat{x}_i$ then be obtained by making an additional query to $S.E$ on input $c_i$. Then,

$$\Pr[\exists i; (\hat{x}_i, c_i) \in R'] \leq 128q^2 \cdot \Gamma_R/2^n \tag{3.10}$$

## 3.4 One Way to Hiding Lemma

This lemma is based on reference [AHU19].

**Lemma 3.4.1.** (One way to hiding, O2H [AHU19]) Let $S \subseteq X$ be random. Let $G, H : X \to Y$ be a random functions satisfying $\forall x \notin S$, $G(x) = H(x)$. Let $z$ be a random bit string ($S, G, H, z$ may have arbitrary joint distribution ).
Let $A$ be quantum oracle algorithm with query depth $q$ (not necessarily unitary). Let $B^H$ be an oracle algorithm that on input $z$ does the following: pick $i \xleftarrow{\$} \{1...q\}$, run $A^H(z)$ until (just before) the $i$-$th$ query, measure all query input registers in the computational basis, output the set $T$ of measurement outcomes. Let

$$\begin{aligned} P_{left} :=& \Pr[b = 1 : b \leftarrow A^H(z)] \\ P_{right} :=& \Pr[b = 1 : b \leftarrow A^G(z)] \\ P_{guess} :=& \Pr[S \cap T \neq \emptyset : T \leftarrow B^H(z)] \end{aligned} \tag{3.11}$$

Then

$$|P_{left} - P_{right}| \leq 2q\sqrt{P_{guess}} \tag{3.12}$$

# Chapter 4

# QROM-Security of Fujisaki-Okamoto Transformation

## 4.1 The Fujisaki-Okamoto Transfomation

### 4.1.1 A public-key encryption scheme

A public-key encryption scheme PKE is defined as follows:

$$\text{PKE} = (\text{KG}, Enc, Dec) \tag{4.1}$$

KG is key generation scheme, generating public key and secret key. *Enc* is encryption scheme, using public key. *Dec* is decryption scheme, using secret key.

### 4.1.2 The Fujisaki-Okamoto Transfomation

There are two versions of the FO transformation: the PKC version [FO99a] and the CRYPTO version [FO99b, FO13]. We will refer to these as FO-PKC and FO-CRYPTO, respectively. (Strictly speaking, the CRYPTO version [FO99b] and the journal version [FO13] differ slightly, but we will treat them as equivalent here.)

The FO-CRYPTO transformation was modified into a KEM (Key Encapsulation Mechanism) by Victor Shoup, who was an ISO editor at the

time [Sho01]. We will refer to this modified FO-CRYPTO transformation as FO-KEM. In ISO18033-2, FO-KEM is named PSEC-KEM.

Subsequently, Hofheinz, Hövelmanns, and Kiltz [HHK17] decomposed FO-KEM into a combination of the T-transformation and the U-transformation. Furthermore, they proposed four variations of the U-transformation: $\mathrm{U}^{\not\perp}$, $\mathrm{U}^{\not\perp}_m$, $\mathrm{U}^{\perp}$, and $\mathrm{U}^{\perp}_m$. In this classification, FO-KEM corresponds to the transformation $\mathrm{U}^{\perp}_m \circ \mathrm{T}$.

For example, let PKE be a (probabilistic) public-key encryption scheme. Applying the T-transformation to PKE yields a deterministic public-key encryption scheme dPKE = T(PKE). Applying one of the U-transformations to dPKE results in a KEM, FO(PKE) = U(dPKE) = U $\circ$ T(PKE). Based on the variations of the U-transformation, we can denote the transformations as $\mathrm{FO} = \mathrm{U}^{\not\perp} \circ \mathrm{T}$, $\mathrm{FO}^{\not\perp}_m = \mathrm{U}^{\not\perp}_m \circ \mathrm{T}$,$\mathrm{FO}^{\perp} = \mathrm{U}^{\perp} \circ \mathrm{T}$, and $\mathrm{FO}^{\perp}_m = \mathrm{U}^{\perp}_m \circ \mathrm{T}$. The above-mentioned FO-KEM corresponds to $\mathrm{FO}^{\perp}_m$. All four transformations guarantee that if the underlying public-key encryption scheme is OW-CPA secure, the resulting KEM is IND-CCA secure in the (classical) random oracle model.

In the quantum random oracle model, it initially appeared that results valid in the classical random oracle model would not hold. However, recent research has shown that similar results can also be achieved in the quantum random oracle model. For generic transformations like FO Transformation for public-key encryption (or KEMs), two key elements in the proofs are the One Way to Hiding (O2H) lemma introduced by Unruh [Unr15] and the Compressed Oracle technique introduced by Zhandry [Zha19]. The O2H lemma has been refined since [Unr15], as seen in works like [AHU19, BHH$^+$19, KSS$^+$20]. Meanwhile, the Compressed Oracle technique was enhanced by Don et al. [DFMS22] with improved extraction methods.

Regarding the quantum random oracle security of the four FO-KEM transformations: [BHH$^+$19, KSS$^+$20] proved the security of $\mathrm{FO}^{\not\perp}$ and $\mathrm{FO}^{\not\perp}_m$. [DFMS22, HHM22] proved the security of $\mathrm{FO}^{\perp}_m$.

To prove the security of $\mathrm{FO}^{\not\perp}$ and $\mathrm{FO}^{\not\perp}_m$, the Compressed Oracle technique is not strictly necessary. In fact, [BHH$^+$19, KSS$^+$20] use the O2H lemma but do not employ the compressed-oracle technique. On the other hand, proving the security of $\mathrm{FO}^{\perp}_m$ seems to require both the Compressed Oracle technique and the improved extraction methods. Zhandry [Zha19] proved the security of FO-CRYPTO for public-key encryption schemes (not KEMs). According to [DFMS22], there is a bug in this proof, but the authors claim that it can be resolved using their improved extraction techniques. As for the quantum random oracle security of $\mathrm{FO}^{\perp}$, no references were found in the literature. However, it is likely that the methods described in [DFMS22, HHM22] can be used to prove it.

Table 4.1: A security proof of FO Transformation in the QROM

| Transform | Type | Reference | Techniques |
|---|---|---|---|
| FO-CRYPTO | PKE | [Zha19, DFMS22] | O2H, cO tech. |
| $FO^{\not\perp}$ | KEM | [BHH+19, KSS+20] | O2H |
| $FO^{\not\perp}_m$ | KEM | [BHH+19, KSS+20] | O2H |
| $FO^{\perp}$ | KEM | ? | ? |
| $FO^{\perp}_m$ | KEM | [DFMS22, HHM22] | O2H, cO tech. |
| FO-PKC | PKE | This work | O2H, cO tech. |

### 4.1.3 Security of Public Key Encryption (PKE)

As shown below, the algorithms for the respective games of IND-CPA (Algorithm 1) and IND-CCA (Algorithm 2). The adversary outputs plain texts $(m_0, m_1) : (m_0 \neq m_1)$. Finally, the adversary takes ciphertext $c^*$ and guess whether it is $c^*$ of $m_0$ or $m_1$. The specific difference lies in whether the adversary can access the Dec.oracle when producing the output $b'$ in line 6 of the both of algorithms.

**Algorithm 1** GAME IND-CPA-PKE

1: $(pk, sk) \leftarrow KG$
2: $(b, r^*) \xleftarrow{\$} \{0,1\} \times \mathbf{R}$
3: $(m_0, m_1) \leftarrow A$
4: $H^* = H(r^*||m_b)$
5: $c^* = Enc_{pk}(r^*||m_b, H^*)$
6: $b' \leftarrow A(pk, c^*)$
7: $b' == b$

**Algorithm 2** GAME IND-CCA-PKE

1: $(pk, sk) \leftarrow KG$
2: $(b, r^*) \xleftarrow{\$} \{0,1\} \times \mathbf{R}$
3: $(m_0, m_1) \leftarrow A$
4: $H^* = H(r^*||m_b)$
5: $c^* = Enc_{pk}(r^*||m_b, H^*)$
6: $b' \leftarrow A^{Dec}(pk, c^*)$
7: $b' == b$

Additionally, the definitions of two conditions required for the IND-CCA game used at the start of the proof, namely $\delta$-correctness and $\gamma$-spreadness, are also provided. $\delta$-correctness refers to the requirement that the decryption of a ciphertext, which was generated by encrypting a plaintext, accurately recovers the original plaintext. The $\gamma$-spreadness requires that the ciphertext has high minimum entropy relative to the average key generation, ensuring robust randomness.

The definitions and notations in this section are based on references [DFMS22].

**Definition 4.1.1** ($\delta$-*correctness*)**.** A public-key encryption scheme is $\delta$-*correct* if

$$\mathop{\mathbb{E}}_{(sk,pk)\leftarrow \mathrm{KG}}[\max_{m\in M}\Pr[Dec_{sk}(c)\neq m : c\leftarrow Enc_{pk}(m))]] \leq \delta \tag{4.2}$$

where the probability is over the randomness of the encryption.

**Definition 4.1.2** ($\gamma$-*spreadness*)**.** A public-key encryption scheme is $\gamma$-spread if

$$\min_{\substack{m\in M\\(sk,pk)}}(-\log \max_{c\in\mathcal{C}} \Pr[c\leftarrow Enc_{pk}(m)]) \geq \gamma \tag{4.3}$$

where the probability is over the randomness of the encryption, and the minimum is over all key pairs that have positive probability of being produced by KG.

**Theorem 4.1.3.** An IND-CPA secure PKE is $\gamma$-spread where $\gamma \geq -\log \epsilon^{ind-cpa} + \log(\mathrm{poly}(k))$.

***Proof.*** For an IND-CPA secure, the advantage of adversary is bounded by a negligible value $\epsilon^{ind-cpa}$.

$$\mathrm{ADV}[B]^{\text{IND-CPA}}_{\text{PKE}} = \Pr[b=b^*] - \frac{1}{2} \leq \epsilon^{\text{IND-CPA}} \tag{4.4}$$

And, we consider the adversary with $b' \leftarrow A(pk, c^*)$(Algorithm 3) against IND-CPA Game.

**Algorithm 3** ***Proof.*** of $\gamma$-spread

**Input:** $pk, c^*$
**Output:** $b'$

**while** $i \leq k$ **do**
  $r_i \xleftarrow{\$} \mathbf{R}$
  **if** $Enc_{pk}(r_i; m_0) = c^*$ or $Enc_{pk}(r_i; m_1) = c^*$ **then**
    return $b'$ $(Enc_{pk}(r_i; m_{b'}) = c^*)$
  **else**
    $i = i + 1$
  **end if**
**end while**
return $b' \xleftarrow{\$} \{0, 1\}$

where **while** is a polynomial number of iteration. Here

$$\begin{aligned} \Pr[b = b^*] =& 2^{-\gamma} \cdot 2 \text{ poly}(k) + (1 - 2^{-\gamma} \cdot 2 \text{ poly}(k)) \cdot \frac{1}{2} \\ =& 2^{-\gamma} \cdot \text{poly}(k) + \frac{1}{2} \end{aligned} \tag{4.5}$$

Therefore

$$\begin{aligned} 2^{-\gamma} \cdot \text{poly}(k) \leq& \epsilon^{\text{IND-CPA}} \\ -\log \epsilon^{ind-cpa} + \log(\text{poly}(k)) \leq& \gamma \end{aligned} \tag{4.6}$$

□

Next, the theorem regarding the relationship between OW secure and IND secure is provided below.

**Proposition 4.1.4.** Let ATK $\in \{\text{CPA}, \text{CCA1}, \text{CCA2}\}$ be the context. If there exists an adversary B against a public-key encryption scheme PKE, then there necessarily exists an adversary A with the following relationship between success probabilities:

$$\text{ADV}[B]^{\text{OW-ATK}}_{\text{PKE}}(\kappa) \leq \text{ADV}[A]^{\text{IND-ATK}}_{\text{PKE}}(\kappa) + \frac{1}{|X|} \tag{4.7}$$

In other words, if PKE is IND secure, then it is OW secure.

## 4.2 Security of FO-PKC in the QROM

### 4.2.1 Main Theorem

**Theorem 4.2.1.** Let PKE be a $\delta$-correct public-key encryption scheme. Let A be any IND-CCA adversary against FO[PKE, $H$], making $q_D \geq 1$ queries to the decryption oracle and $q_A$ queries to $H : X \to Y$, where $H$ is modeled as random oracles. Then, there exists an IND-CPA adversary B against PKE with

$$\begin{aligned} &\mathrm{ADV}[A]^{\text{IND-CCA}}_{\text{FO}} \\ \leq &(1 + \frac{q_D}{q_A + q_D})(\mathrm{ADV}[B]^{\text{IND-CPA}}_{\text{PKE}} + \epsilon') + \frac{q_D}{q_A + q_D} \cdot \frac{1}{|X|} \\ + &\frac{2{q_A}^2}{q_A + q_D} \sqrt{\mathrm{ADV}[B]^{\text{IND-CPA}}_{\text{PKE}} + \frac{1}{|X|} + \epsilon'} \\ \text{with } \epsilon' = &\, 8q_D(2q_A + q_D)\sqrt{2 \cdot 2^{-\gamma}} + 128{q_A}^2 \cdot \delta + 2q_D \cdot 2^{-n} \end{aligned} \tag{4.8}$$

### 4.2.2 Proof of the Theorem

In the following, we provide a proof of Thm 4.2.1. In performing this proof, we use a different procedure than the FO transformation of the classical random oracle model. The following Steps are used in the proof. In quantum, the order is changed because it is necessary to apply O2H before deleting the secret key by extraction.

***Classical.***

1. Replace decryption oracle with the extraction result. This change would allow decryption oracle to be executed without secret key. Therefore, the Game turned from IND-CCA to IND-CPA.

2. Bound the probability of a successful attack on Game original and replacement in Step1 with Game that outputs plain text. It is classical, so O2H is not necessary.

3. Proof is complete as it was bounded with IND-CPA Game and OW-CPA Game.

***Quantum.***

1. Replace the original random oracle with another random oracle that has a different output than the original. Apply O2H to compose Game to bound the difference between two Games.

2. The random oracle is replaced with compressed oracle. This replacement makes the extraction possible, so the information of the secret key erases.

3. Proof is complete as it was bounded with IND-CPA Game and OW-CPA Game.

***Proof.*** Algorithms 4 to 8 are shown below. These algorithms are divided by roles into, Game Setup, Main Phase, Random Oracle(RO), Decryption Oracle(Dec.oracle), and One Way to Hiding(O2H). The corresponding game number is noted next to each line, and lines without number are common across all games. These algorithms describe the transformations from Game0 to Game5, starting with the CCA adversary A in Game0 and ending with the CPA adversary B in Game5.

In this proof, we first fix the generated key pair $(sk, pk) \leftarrow \mathrm{KG}$ and denote the CCA adversary's advantage for this pair as $\mathrm{ADV}[A]^{\text{IND-CPA}}_{\text{FO}}$. Additionally, since $\delta$-correctness is assumed for the game in this key pair $(sk, pk)$, let $\delta_{sk}$ be the maximum probability of a decryption error, and $g_{sk}$ be the maximum probability of any ciphertext, so that $\mathbb{E}[\delta_{sk}] \leq \delta$ and $g_{sk} \leq 2^{-\gamma}$, with the expectation over $(sk, pk)$.

**Algorithm 4** Game Setup

$(pk, sk) \leftarrow KG$
$(b, r^*) \xleftarrow{\$} \{0,1\} \times \mathbf{R}$
$H^* = H(r^* || m_b)$
$c^* = Enc_{pk}(r^* || m_b, H^*)$

**Algorithm 5** Main Phase

**Input:** $c^*$

$A^{Dec,H}(m_0, m_1, c^*) \rightarrow b'$ /G0

$A^{Dec,H'}(m_0, m_1, c^*) \rightarrow b'$ /G1

$A^{Dec,S.RO}(m_0, m_1, c^*) \rightarrow b'$ /G2-G5

**while** $i \in I$ **do**

  $\hat{r}_i||\hat{m}_i \leftarrow S.E(c_i)$ /G2

**end while**

$b' == b$

**Algorithm 6** random oracle

**Input:** $(r||m)$

**Output:** $H$

$H(r||m) = H$ /G0

$H'(r||m) = H$ /G1

$S.RO(r||m) = H$ /G2-5

return $H$

**Algorithm 7** Dec oracle

**Input:** $c_i (c_i \neq c^*)$

**Output:** $m_i$

$r_i||m_i \leftarrow Dec_{sk}(c_i)$ /G0-G4

$S.E(c_i) = \hat{r_i}||\hat{m_i}$ /G4-G5

$H = H(r_i||m_i)$ /G0

$H = H'(r_i||m_i)$ /G1

$H = S.RO(r_i||m_i)$ /G2-G3

$H = S.RO(\hat{r_i}||\hat{m_i})$ /G4-G5

**if** $Enc_{pk}(r_i||m_i, H) = c_i$ **then**

  return $m_i$ /G0-G3

**else**

  return $\perp$ /G0-G3

**end if**

**if** $Enc_{pk}(\hat{r}_i||\hat{m}_i, H) = c_i$ **then**

  return $\hat{m}_i$ /G4-G5

**else**

  return $\perp$ /G4-G5

**end if**

$\hat{r}_i||\hat{m}_i \leftarrow S.E(c_i)$ /G3

In Game1 using Lem 3.4.1, a new game is defined. In this game, $j$ random queries are selected from the adversary's quantum queries $q_A \in J_A$ and the classical queries $q_D \in J_D$ made by the Dec.oracle to the random oracle. These selected queries are measured, and an algorithm $MA$ is considered, which submits the plaintext $r'||m'$ derived from the measurement results.

In the middle of the game, the role of outputting the plaintext in $MA$ changes to $EA$. It submits the plaintext when referencing Dec.oracle queries, uses the extracted plaintext $\hat{r}||\hat{m}$ from a simulator $S$ instead of directly using the Dec.oracle.

**Algorithm 8** O2H

**Input:** $c^*$

1: $j \xleftarrow{\$} J_A \cup J_D$
2: $r'||m' \leftarrow MA_j^{Dec,H'}(c^*)$ /G1
3: $r'||m' \leftarrow MA_j^{Dec,S.RO}(c^*)$ /G2-G3
4: $r'||m' \leftarrow EA_j^{Dec,S.RO}(c^*)$ /G4-G5
5: return $r'||m' == r^*||m_b$

**Game0** Consider the standard IND-CCA game.

$$\Pr[b = b' \text{ in Game0}] = \frac{1}{2} + \mathrm{ADV}[A]^{\text{IND-CCA}}_{\text{FO}} \tag{4.9}$$

**Game1** The random oracle $H$ is replaced with a new random oracle $H'$. The oracle $H'$ has the output corresponding to input $r^*||m_b$ that differ from $H$, while the outputs corresponding to inputs other than $r^*||m_b$ remain the same. Then, the change introduced by the transformation from Game0 to Game1 is evaluated using O2H, which applicable to quantum queries.

In this case, the random oracle $H'$ accepts two of queries, $q_A$ quantum queries made by the adversary A and $q_D$ classical queries made by the Dec.oracle. O2H is applied only to the $q_A$ quantum queries.

From the above, let $P_A$ denote the probability that plaintext $r'||m'$ is output from the quantum queries made by adversary A such that $r'||m' = r^*||m_b$, and $P_D$ denote the probability that plaintext $r'||m'$ is output from the classical queries made by the Dec oracle to the random oracle. However, $P_A$ and $P_D$ are equal because there is one output obtained by measuring each query. So, we replace both $P_A$ and $P_D$ with $P_\epsilon$

For the evaluation of quantum queries, a new game is prepared in Algorithm 6. Through these operations, the difference in the success probabilities of attacks in Game0 and Game1 can be bounded by the sum of two proba-

bilities. Therefore, the following equation is obtained:

$$\begin{aligned} &|\Pr[b = b' \text{ in Game0}] - \Pr[b = b' \text{ in Game1}]| \\ \leq &\frac{2{q_A}^2}{q_A + q_D}\sqrt{P_A} + \frac{q_D}{q_A + q_D}P_D \\ = &\frac{2{q_A}^2}{q_A + q_D}\sqrt{P_\epsilon} + \frac{q_D}{q_A + q_D}P_\epsilon \\ P_\epsilon = &\Pr[r'||m' = r^*||m_b \text{ in Game1}] \end{aligned} \tag{4.10}$$

**Game2** Next, replace the random oracle $H'$ with the random oracle component $S.RO$ of the simulator $S$. The component $S.E$ operates only after all queries from the adversary have been completed. Therefore, there is no change due to $S.E$. Additionally, from the theorem, the adversary cannot detect the replacement with the simulator $S$. Hence,

$$\Pr[b = b' \text{ in Game1}] = \Pr[b = b' \text{ in Game2}] \tag{4.11}$$

Similarly, in Game1 and Game2, the random oracle was replaced from $H'$ to $S.RO$, but since there is no change in the output, applying O2H to compare Game0 and Game2 yields the following:

$$\begin{aligned} &|\Pr[b = b' \text{ in Game0}] - \Pr[b = b' \text{ in Game2}]| \\ = &|\Pr[b = b' \text{ in Game0}] - \Pr[b = b' \text{ in Game1}]| \\ \leq &\frac{2{q_A}^2}{q_A + q_D}\sqrt{\Pr[r'||m' = r^*||m_b \text{ in Game1}]} \\ + &\frac{q_D}{q_A + q_D}\Pr[r'||m' = r^*||m_b \text{ in Game1}] \\ = &\frac{2{q_A}^2}{q_A + q_D}\sqrt{\Pr[r'||m' = r^*||m_b \text{ in Game2}]} \\ + &\frac{q_D}{q_A + q_D}\Pr[r'||m' = r^*||m_b \text{ in Game2}] \end{aligned} \tag{4.12}$$

**Game3** The $S.E$ prepared after the adversary's queries is moved to the final operation of the Dec.oracle. Since this relocation occurs at most $q_D(q_A + q_D)$ times, and the error for a single relocation is $8\sqrt{2\Gamma(f)/2^n}$, and $\Gamma(f)/2^n = g_{sk}$. i.e., $8q_D(q_A+q_D)\sqrt{2\Gamma(f)/2^n} = 8q_D(q_A+q_D)\sqrt{2 \cdot g_{sk}} \leq 8q_D(q_A+q_D)\sqrt{2 \cdot 2^{-\gamma}}$. Hence,

$$\Pr[b = b' \text{ in Game3}] \geq \Pr[b = b' \text{ in Game2}] - \epsilon_1 \tag{4.13}$$

where, $\epsilon_1 = 8q_D(q_A + q_D)\sqrt{2 \cdot 2^{-\gamma}}$.
Furthermore, applying Prop 3.3.4 for $R' := \{(r||m, c) : Dec_{sk}(c) \neq r||m\}$, we get that the event

$$P^\dagger = [\forall i; \hat{m}_i = m_i \vee \hat{m}_i = \emptyset] \tag{4.14}$$

holds except with probability $128{q_A}^2 \cdot \Gamma_R/2^n \leq 128{q_A}^2 \cdot \delta =: \epsilon_2$, where $\Gamma_R/2^n = \delta_{sk}$. Thus,

$$\Pr[b = b' \wedge P^{\dagger} \text{ in Game3}] \geq \Pr[b = b' \text{ in Game3}] - \epsilon_2 \tag{4.15}$$

Additionally, if we defined a new event $P$, $P$ represents the event where $S.E$ performs a correct extraction.

$$P = [\forall i; \hat{m}_i = m_i \vee (\hat{m}_i = \emptyset \wedge Enc_{pk}(\hat{r}_i||\hat{m}_i; S.RO) \neq c_i)] \tag{4.16}$$

The difference in probabilities between $P$ and $P^{\dagger}$ is bounded by Thm 3.3.3 4.b with each individual difference limited to $2 \cdot 2^{-n}$. Since this event does not occur even once in $q_D$ trials, and considering the first term of the Taylor expansion, the difference is ultimately bounded by $2q_D \cdot 2^{-n}$. Therefore, the following inequality is obtained:

$$\Pr[b = b' \wedge P \text{ in Game3} \geq \Pr[b = b' \wedge P^{\dagger} \text{ in Game3}] - \epsilon_3 \tag{4.17}$$

where, $\epsilon_3 = 2q_D \cdot 2^{-n}$.
From (4.13), (4.15) and (4.17), the following equation holds:

$$\begin{aligned} &\Pr[b = b' \wedge P \text{ in Game3}] \geq \\ &\Pr[b = b' \wedge P^{\dagger} \text{ in Game3}] - \epsilon_3 \geq \\ &\Pr[b = b' \text{ in Game3}] - \epsilon_2 - \epsilon_3 \geq \\ &\Pr[b = b' \text{ in Game2}] - \epsilon_1 - \epsilon_2 - \epsilon_3 \end{aligned} \tag{4.18}$$

And, regarding the O2H, the probability that $[r'||m' = r^*||m_b$ in Game2] and $[r'||m' = r^*||m_b \wedge P$ in Game3] exhibit different behaviors is, as in the previous discussion, bounded by $\epsilon = \epsilon_1 + \epsilon_2 + \epsilon_3$.

$$\begin{aligned} &\Pr[r'||m' = r^*||m_b \text{ in Game2}] \\ \leq &\Pr[r'||m' = r^*||m_b \text{ in Game3}] + \epsilon_1 \\ \leq &\Pr[r'||m' = r^*||m_b \wedge P \text{ in Game3}] + \epsilon \end{aligned} \tag{4.19}$$

**Game4** The responses in the Dec.oracle are handled using $S.E$ instead of the Dec function. Considering event $P$ in Game3, the output of $S.E$ corresponding to the input $c_i$ is indistinguishable from the Dec function from the adversary. Therefore,

$$\Pr[b = b' \wedge P \text{ in Game4}] = \Pr[b = b' \wedge P \text{ in Game3}] \tag{4.20}$$

Similarly, based on the same reason, O2H can be expressed as follows:

$$\begin{aligned} &\Pr[r'||m' = r^*||m_b \wedge P \text{ in Game4}] \\ = &\Pr[r'||m' = r^*||m_b \wedge P \text{ in Game3}] \end{aligned} \tag{4.21}$$

**Game5** The Dec.oracle has been completely replaced by the simulator $S$, and the adversary can no longer obtain any information about $sk$ from the Dec.oracle. Thus, the Dec.oracle can be completely removed. As a result, Game5 can be regarded as an IND-CPA game. The discrepancy between Game4 and Game5 is $\epsilon_4$, which accounts for the removal of all queries from the Dec function to the random oracle. This can be understood as moving all queries from Dec to the random oracle to the end of the operations. Since the maximum number of such queries is $q_A \cdot q_D$, the discrepancy is bounded by $8q_A \cdot q_D\sqrt{2\Gamma(f)/2^n} \leq 8q_A \cdot q_D\sqrt{2 \cdot 2^{-\gamma}} =: \epsilon_4$.

$$\begin{aligned} &\Pr[b = b' \wedge P \text{ in Game4}] \\ \leq &\Pr[b = b' \wedge P \text{ in Game5}] + \epsilon_4 \\ \leq &\frac{1}{2} + \mathrm{ADV}[B]^{\text{IND-CPA}}_{\text{PKE}} + \epsilon_4 \end{aligned} \tag{4.22}$$

Additionally, by modifying the O2H game in accordance with the changes in Game 5, the removal of the decryption oracle transforms Game 5 into an IND-CPA game. Since $P$ can be regarded as equivalent to an OW-CPA game where it predicts a specific output with differing values, $P$ can be bounded by the OW-CPA advantage.

$$\begin{aligned} &\Pr[r'||m' = r^*||m_b \wedge P \text{ in Game4}] \\ \leq &\Pr[r'||m' = r^*||m_b \wedge P \text{ in Game5}] + \epsilon_4 \\ \leq &\mathrm{ADV}[B]^{\text{OW-CPA}}_{\text{PKE}} + \epsilon_4 \end{aligned} \tag{4.23}$$

Combining Game0 through Game5, the following inequality is obtained:

$$
\begin{aligned}
&\frac{1}{2} + \mathrm{ADV}[A]^{\text{IND-CCA}}_{\text{FO}} = \Pr[b = b' \text{ in Game0}] \\
\leq &\Pr[b = b' \wedge P \text{ in Game5}] + \epsilon' + \frac{2{q_A}^2}{q_A + q_D}\sqrt{P_\epsilon} + \frac{q_D}{q_A + q_D}P_\epsilon \\
\leq &\frac{1}{2} + \mathrm{ADV}[B]^{\text{IND-CPA}}_{\text{PKE}} + \epsilon' + \frac{2{q_A}^2}{q_A + q_D}\sqrt{\mathrm{ADV}[B]^{\text{OW-CPA}}_{\text{PKE}} + \epsilon'} \\
&+ \frac{q_D}{q_A + q_D}(\mathrm{ADV}[B]^{\text{OW-CPA}}_{\text{PKE}} + \epsilon') \\
\leq &\frac{1}{2} + \mathrm{ADV}[B]^{\text{IND-CPA}}_{\text{PKE}} + \epsilon' + \frac{2{q_A}^2}{q_A + q_D}\sqrt{\mathrm{ADV}[B]^{\text{IND-CPA}}_{\text{PKE}} + \frac{1}{|X|} + \epsilon'} \\
&+ \frac{q_D}{q_A + q_D}(\mathrm{ADV}[B]^{\text{IND-CPA}}_{\text{PKE}} + \frac{1}{|X|} + \epsilon') \\
= &\frac{1}{2} + (1 + \frac{q_D}{q_A + q_D})(\mathrm{ADV}[B]^{\text{IND-CPA}}_{\text{PKE}} + \epsilon') + \frac{q_D}{q_A + q_D} \cdot \frac{1}{|X|} \\
&+ \frac{2{q_A}^2}{q_A + q_D}\sqrt{\mathrm{ADV}[B]^{\text{IND-CPA}}_{\text{PKE}} + \frac{1}{|X|} + \epsilon'}
\end{aligned}
\tag{4.24}
$$

where $\epsilon' = \epsilon + \epsilon_4$. Therefore,

$$
\begin{aligned}
&\mathrm{ADV}[A]^{\text{IND-CCA}}_{\text{FO}} \\
\leq &(1 + \frac{q_D}{q_A + q_D})(\mathrm{ADV}[B]^{\text{IND-CPA}}_{\text{PKE}} + \epsilon') + \frac{q_D}{q_A + q_D} \cdot \frac{1}{|X|} \\
&+ \frac{2{q_A}^2}{q_A + q_D}\sqrt{\mathrm{ADV}[B]^{\text{IND-CPA}}_{\text{PKE}} + \frac{1}{|X|} + \epsilon'}
\end{aligned}
\tag{4.25}
$$

And $\epsilon'$ is as follows:

$$
\begin{aligned}
\epsilon' = &8q_D(q_A + q_D)\sqrt{2 \cdot 2^{-\gamma}} + 128{q_A}^2 \cdot \delta \\
&+ 2q_D \cdot 2^{-n} + 8q_A \cdot q_D\sqrt{2 \cdot 2^{-\gamma}} \\
= &8q_D(2q_A + q_D)\sqrt{2 \cdot 2^{-\gamma}} + 128{q_A}^2 \cdot \delta + 2q_D \cdot 2^{-n}
\end{aligned}
\tag{4.26}
$$

□

# Chapter 5

# Summary

In this paper, we provided a security proof for the FO transformation in PKC, which converts a PKE with IND-CPA security into a PKE with IND-CCA security, based on Don et al.'s proof. From this result, it was showed that the FO transformation, previously considered applicable only in the classical Random Oracle Model, can also be applied to the Quantum Random Oracle Model (QROM) using compressed oracle.

Future work in this study includes improvements to One Way to Hiding Lemma (O2H) and to the commutator bound. In the current proof method, the application of O2H bounds the probability using a square root of the probability. In the classical model, the probability is bounded by the probability without the square root, so if the probability can be bounded by the probability without or close to the square root in the quantum case using some method, better security evaluation results can be obtained.

Additionally, in this proof, the order of the algorithms in the simulator is swapped, and the error term is generated by the number of such swaps and the commutator bound. Therefore, if the commutator bound can be bounded to a smaller upper bound or the number of swapping can be reduced to a smaller number, the error term will be smaller, and leading to improved results.

# Bibliography


[AHU19] Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39*, pages 269–295. Springer, 2019.

[BHH+19] Nina Bindel, Mike Hamburg, Kathrin Hövelmanns, Andreas Hülsing, and Edoardo Persichetti. Tighter proofs of cca security in the quantum random oracle model. In *Theory of Cryptography Conference*, pages 61–90. Springer, 2019.

[CFHL21] Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao. On the compressed-oracle technique, and post-quantum security of proofs of sequential work. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 598–629. Springer, 2021.

[DFMS22] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Online-extractability in the quantum random-oracle model. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 677–706. Springer, 2022.

[FO99a] Eiichiro Fujisaki and Tatsuaki Okamoto. How to enhance the security of public-key encryption at minimum cost. In *International workshop on public key cryptography*, pages 53–68. Springer, 1999.

[FO99b] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Annual international cryptology conference*, pages 537–554. Springer, 1999.

[FO13] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *Journal of cryptology*, 26:80–101, 2013.

[HHK17] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A modular analysis of the fujisaki-okamoto transformation. In *Theory of Cryptography Conference*, pages 341–371. Springer, 2017.

[HHM22] Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Failing gracefully: decryption failures and the fujisaki-okamoto transform. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 414–443. Springer, 2022.

[KSS+20] Veronika Kuchta, Amin Sakzad, Damien Stehlé, Ron Steinfeld, and Shi-Feng Sun. Measure-rewind-measure: tighter quantum random oracle model proofs for one-way to hiding and cca security. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 703–728. Springer, 2020.

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[Sho01] Victor Shoup. A proposal for an iso standard for public key encryption. *Cryptology ePrint Archive*, 2001.

[Unr15] Dominique Unruh. Revocable quantum timed-release encryption. *Journal of the ACM (JACM)*, 62(6):1–76, 2015.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39*, pages 239–268. Springer, 2019.