A Note on Separating Classical and Quantum Random Oracles

Takashi Yamakawa*[1] and Mark Zhandry[2,3]

[1]NTT Secure Platform Laboratories
[2]Princeton University
[3]NTT Research

June 24, 2020

Abstract

In this note, we observe that a proof of quantumness in the random oracle model recently proposed by Brakerski et al. can be seen as a *proof of quantum access to a random oracle*. Based on this observation, we give the first examples of natural cryptographic schemes that separate classical and quantum random oracle models. Specifically, we construct digital signature and public key encryption schemes that are secure in the classical random oracle model but insecure in the quantum random oracle model assuming the quantum hardness of learning with error problem.

1 Introduction

The random oracle model (ROM) [BR93] is a widely used heuristic model in cryptography where a hash function is modeled as a random function that is only accessible as an oracle. The ROM was used for constructing practical cryptographic schemes including digital signatures [FS87, PS96, BR96], chosen-ciphertext attack (CCA) secure public key encryption (PKE) [BR95, FOPS01, FO13], identity-based encryption (IBE) [GPV08], etc.

In 2011, Boneh et al. [BDF+11] observed that the ROM may not be sufficient when considering post-quantum security, since a quantum adversary can quantumly evaluate hash functions on superpositions, while the ROM only gives a classically-accessible oracle to an adversary. Considering this observation, they proposed the quantum random oracle model (QROM), which gives an adversary quantum access to an oracle that computes a random function.

Boneh et al. observe that many proof techniques in the ROM cannot be directly translated into one in the QROM, *even if the other building blocks of*

*This work was done in part while the author was visiting Princeton University.

the system are quantum-resistant. Therefore, new proof techniques are needed in order to justify the post-quantum security of random oracle model systems. Fortunately, recent advances of proof techniques have clarified that most important constructions that are originally proven secure in the ROM are also secure in the QROM. These include OAEP [TU16], Fujisaki-Okamoto transform [TU16, JZC+18, Zha19], Fiat-Shamir transform [DFMS19, LZ19], Full-Domain Hash signatures [Zha12] Gentry-Peikert-Vaikuntanathan IBE [Zha12, KYY18] etc.

Given this situation, it is natural to ask if there may be a general theorem lifting *any* classical ROM proof into a proof in the QROM, provided that the other building blocks of the system remain quantum resistant.

Such a general lifting theorem certainly seems like a challenging task. Nevertheless, demonstrating a separation — that is, a scheme using quantum-resistant building blocks that is secure in the ROM but insecure in the QROM — has also been elusive. Intuitively, the reason is that natural problems on random oracles (such as pre-image search, collision finding, etc) only have *polynomial* gaps between classical and quantum query complexity.

We are aware of two works that consider the task of finding a separation. First, Boneh et al. [BDF+11] gave an example of an identification protocol that is secure in the ROM but insecure in the QROM, but is specific to a certain non-standard timing model. Concretely, the protocol leverages the polynomial gap in collision finding to allow an attacker with quantum oracle access to break the system somewhat faster than any classical-access algorithm. The verifier then rejects if the prover cannot respond to its challenges fast enough, thereby blocking classical attacks while allowing the quantum attack to go through. This unfortunately requires a synchronous model where the verifier keeps track of the time between messages; such a model is non-standard.

Second, a recent work of Zhang et al. [ZYF+19] showed that quantum random oracle is *differentiable* from classical random oracle, which roughly means that it is impossible to simulate quantum random oracle using only classical queries to the same function. Their result rules out a natural approach one may take to give a lifting theorem, but it fails to actually give a scheme separating classical from quantum access to a random oracle

In summary, there is no known classical cryptographic scheme (e.g., digital signatures and PKE) that can be proven secure in the ROM but insecure in the QROM.

1.1 Our Result

We observe that a proof of quantumness recently proposed by Brakerski et al. [BKVV20] implicitly gives an example of a cryptographic scheme that is secure in the ROM but insecure in the QROM assuming quantum hardness of the learning with errors (LWE) problem [Reg09]. We formalize this as a *proof of quantum access to random oracle* (PoQRO), and show that the proof of quantumness of Brakerski et al. [BKVV20] can be seen as a PoQRO. Based on this observation, we give the first examples of natural cryptographic schemes that separate the ROM and QROM. Specifically, we construct

1. A digital signature scheme that is EUF-CMA secure in the ROM but not EUF-CMA secure in the QROM, and
2. A PKE scheme that is CCA secure in the ROM but not CCA secure in the QROM

Both these results rely on the assumed quantum hardness of LWE.

2 Classical/Quantum Random Oracle Model

In the (classical) random oracle model (ROM) [BR93], a random function H (of a certain domain and range) is chosen at the beginning, and an adversary can classically access to H. The quantum random oracle model (QROM) [BDF+11] is defined similarly except that the access to H can be quantum. More precisely, an adversary (which is quantum) is given an oracle access to a unitary U_H s.t. $U_H |x\rangle |y\rangle = |x\rangle |y \oplus H(x)\rangle$ for any x and y. We often denote $|H\rangle$ to mean the oracle that applies U_H for simplicity. We note that we can implement a unitary U'_H s.t. $U'_H |x\rangle = (-1)^{H(x)} |x\rangle$ by a single call to U_H by a standard technique. We call an oracle that applies U'_H a *phase oracle* of H. We stress that the classical ROM can be considered even when we consider security against quantum adversaries. Namely, when a quantum adversary makes a query to a classical random oracle, then the oracle measures the query register and then apply the unitary U_H as above.

3 Separation between ROM and QROM

In this section, we show examples of cryptographic schemes that are secure in the ROM but insecure in the QROM.

3.1 Proof of Quantum Access to Random Oracle

First, we introduce a notion of proofs of quantum access to random oracle (PoQRO).

Definition 3.1. *A (non-interactive) proof of quantum access to random oracle (PoQRO) consists of algorithms* ($\mathsf{PoQRO.Setup}, \mathsf{PoQRO.Prove}, \mathsf{PoQRO.Verify}$).

$\mathsf{PoQRO.Setup}(1^\lambda)$**:** *This is a classical algorithm that takes the security parameter 1^λ as input and outputs a public key* pk *and a secret key* sk.

$\mathsf{PoQRO.Prove}^{|H\rangle}(\mathsf{pk})$**:** *This is a quantum oracle-aided algorithm that takes a public key* pk *as input and given a quantum access to a random oracle H, and outputs a proof π.*

$\mathsf{PoQRO.Verify}^H(\mathsf{sk}, \pi)$**:** *This is a classical algorithm that takes a secret key* sk *and a proof* π *as input and given a classical access to a random oracle* H*, and outputs* $\top$ *indicating acceptance or* $\bot$ *indicating rejection.*

We require PoQRO to satisfy the following properties.

Correctness. *We have*

$$\Pr\left[\mathsf{PoQRO.Verify}^H(\mathsf{sk}, \pi) = \bot : \begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{PoQRO.Setup}(1^\lambda), \\ \pi \xleftarrow{\$} \mathsf{PoQRO.Prove}^{|H\rangle}(\mathsf{pk}) \end{array}\right] \leq \mathsf{negl}(\lambda).$$

Soundness. *For any quantum polynomial-time adversary* $\mathcal{A}$ *that is given a classical oracle access to* H*, we have*

$$\Pr\left[\mathsf{PoQRO.Verify}^H(\mathsf{sk}, \pi) = \top : \begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{PoQRO.Setup}(1^\lambda), \\ \pi \xleftarrow{\$} \mathcal{A}^H(\mathsf{pk}) \end{array}\right] \leq \mathsf{negl}(\lambda).$$

We observe that proofs of quantumness in the random oracle model recently proposed by Brakerski et al. [BKVV20] can also be seen as a PoQRO. Then we obtain the following lemma. Though the construction and security proof are almost the same as that of [BKVV20], we give a proof sketch for the reader's convenience.

Lemma 3.2 (a variant of [BKVV20])**.** *If the QLWE assumption holds, then there exists a PoQRO.*

Proof. (sketch) As shown in previous works [BCM+18, BKVV20] there exists a quantumly secure family of noisy trapdoor claw-free functions assuming the QLWE assumption. In this proof sketch, we assume that there exists a quantumly-secure family of (non-noisy) trapdoor claw-free functions for simplicity. We note that the proof can be easily extended to the construction from a noisy one as in [BKVV20].

A quantumly secure family of trapdoor claw-free functions enables one to sample a function $f : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$ along with a trapdoor such that

1. $f(0, \cdot)$ and $f(1, \cdot)$ are injective,
2. $f(0, \cdot)$ and $f(1, \cdot)$ are efficiently invertible by using a trapdoor, and
3. it is hard for an efficient quantum adversary that is not given a trapdoor to find x_0 and x_1 such that $f(0, x_0) = f(1, x_1)$.

Let $H : \{0,1\}^n \to \{0,1\}$ be a random oracle. First, we describe a PoQRO with soundness error 1/2.

$\mathsf{PoQRO.Setup}(1^\lambda)$**:** This algorithm generates a trapdoor claw-free function $f : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$ along with a trapdoor td, and outputs $\mathsf{pk} := f$ and $\mathsf{sk} := \mathsf{td}$.

$\mathsf{PoQRO.Prove}^{|H\rangle}(\mathsf{pk} = f)$**:** This algorithm generates a superposition

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle ,$$

computes f into another register to obtain

$$\frac{1}{2^{(n+1)/2}} \left(|0\rangle \sum_{x \in \{0,1\}^n} |x\rangle |f(0,x)\rangle + |1\rangle \sum_{x \in \{0,1\}^n} |x\rangle |f(1,x)\rangle \right),$$

measures the third register to obtain $y \in \{0,1\}^n$ along with a collapsed state

$$\frac{1}{\sqrt{2}}(|0\rangle |x_0\rangle + |1\rangle |x_1\rangle)$$

where $f(0,x_0) = f(1,x_1) = y$, applies the phase oracle of H on the second register to obtain

$$\frac{1}{\sqrt{2}}((-1)^{H(x_0)} |0\rangle |x_0\rangle + (-1)^{H(x_1)} |1\rangle |x_1\rangle),$$

applies the Hadamard transform on both registers to obtain

$$\frac{1}{2^{(n+1)/2}} \sum_{((m,d) \in \{0,1\} \times \{0,1\}^n)} ((-1)^{H(x_0) \oplus d^T x_0} + (-1)^{H(x_1) \oplus m \oplus d^T x_1}) |m\rangle |d\rangle$$
$$= \frac{1}{2^{(n-1)/2}} \sum_{(m,d): m = d^T \cdot (x_0 \oplus x_1) \oplus H(x_0) \oplus H(x_1)} (-1)^{H(x_0) \oplus d^T x_0} |m\rangle |d\rangle ,$$

and measures the both registers in standard basis to obtain (m,d). Then it outputs $\pi := (y,m,d)$.

$\mathsf{PoQRO.Verify}^{H}(\mathsf{sk} = \mathsf{td}, \pi = (y,m,d))$**:** This algorithm computes x_0 and x_1 such that $f(0,x_0) = f(1,x_1) = y$ by using a trapdoor td and outputs $\top$ if

$$m = d^T \cdot (x_0 \oplus x_1) \oplus H(x_0) \oplus H(x_1)$$

holds and $\perp$ otherwise.

The correctness clearly follows from the above description. For proving soundness, we consider an efficient quantum adversary $\mathcal{A}^H$ that is given classical access to H. First, it is easy to see that $\mathcal{A}$ can win with probability $1/2$ if it does not query both x_0 and x_1 to H. Moreover, if $\mathcal{A}$ queries both x_0 and x_1 to H, then we can break the security of the trapdoor claw-free function f by finding a solution from $\mathcal{A}$'s queries. Therefore, such an event happens with negligible probability, and thus $\mathcal{A}$'s winning probability is at most $1/2 + \mathsf{negl}(\lambda)$. Finally, by a parallel repetition, we can exponentially reduce the soundness error to obtain a PoQRO with negligible soundness error. $\square$

3.2 Digital Signatures

In this section, we construct a digital signature scheme that is EUF-CMA secure in the ROM but not EUF-CMA secure in the QROM based on PoQRO.

Definition 3.3. *A digital signature scheme consists of classical algorithms* $(\mathsf{Sig.KeyGen}, \mathsf{Sig.Sign}, \mathsf{Sig.Verify})$*:*

$\mathsf{Sig.KeyGen}(1^\lambda)$**:** *This algorithm takes the security parameter* 1^λ *as input and outputs a verification key* vk *and a signing key* sigk*.*

$\mathsf{Sig.Sign}(\mathsf{sigk}, m)$**:** *This algorithm takes a signing key* sigk *and a message* m *as input and outputs a signature* σ*.*

$\mathsf{Sig.Verify}(\mathsf{vk}, m, \sigma)$**:** *This algorithm takes a verification key* vk*, a message* m*, and a signature* σ *as input, and outputs* $\top$ *indicating acceptance or* $\bot$ *indicating rejection.*

As correctness, we require that for any m*, we have*

$$\Pr[\mathsf{Sig.Verify}(\mathsf{vk}, x, \sigma) = \top : (\mathsf{vk}, \mathsf{sigk}) \xleftarrow{\$} \mathsf{Sig.KeyGen}(1^\lambda), \sigma \xleftarrow{\$} \mathsf{Sig.Sign}(\mathsf{sigk}, m)] = 1.$$

We say that a digital signature scheme is EUF-CMA secure against quantum adversaries if for any efficient quantum adversary $\mathcal{A}$ *with a classical signing oracle, we have*

$$\Pr\left[\begin{array}{l} \mathsf{Sig.Verify}(\mathsf{vk}, m^*, \sigma^*) = \top \\ \wedge\ \mathcal{A} \text{ never queried } m^* \end{array} : \begin{array}{l} (\mathsf{vk}, \mathsf{sigk}) \xleftarrow{\$} \mathsf{Sig.KeyGen}(1^\lambda), \\ (m^*, \sigma^*) \xleftarrow{\$} \mathcal{A}^{\mathsf{Sig.Sign}(\mathsf{sk}, \cdot)}(\mathsf{vk}) \end{array}\right] \leq \mathsf{negl}(\lambda)$$

where $\mathsf{Sig.Sign}(\mathsf{sk}, \cdot)$ *denotes a classical oracle that computes* $\mathsf{Sig.Sign}(\mathsf{sk}, \cdot)$*.*

Lemma 3.4. *If the QLWE assumption holds, then there exists a digital signature scheme that is secure against quantum adversaries in the ROM but not secure against quantum adversaries in the QROM.*

Proof. Let $(\mathsf{Sig.KeyGen}, \mathsf{Sig.Sign}, \mathsf{Sig.Verify})$ be a digital signature scheme that is EUF-CMA secure against quantum adversaries in the standard model. Such a scheme exists under the QLWE assumption [ABB10, CHKP10]. Let $(\mathsf{PoQRO.Setup}, \mathsf{PoQRO.Prove}, \mathsf{PoQRO.Verify})$ be a PoQRO, which exists under the QLWE assumption as shown in Lemma 3.2. Then we consider a digital signature scheme $(\mathsf{Sig.KeyGen}', \mathsf{Sig.Sign}', \mathsf{Sig.Verify}')$ that uses a random oracle H described below:

$\mathsf{Sig.KeyGen}'^H(1^\lambda)$**:** This algorithm generates $(\mathsf{vk}, \mathsf{sigk}) \xleftarrow{\$} \mathsf{Sig.KeyGen}(1^\lambda)$ and $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{PoQRO.Setup}(1^\lambda)$, and outputs $\mathsf{vk}' := (\mathsf{vk}, \mathsf{pk})$ and $\mathsf{sigk}' := (\mathsf{sigk}, \mathsf{sk})$.

$\mathsf{Sig.Sign}'^H(\mathsf{sigk}' = (\mathsf{sigk}, \mathsf{sk}), m)$**:** If $\mathsf{PoQRO.Verify}^H(\mathsf{sk}, m) = \top$, then it outputs sigk. Otherwise, it outputs $\sigma \xleftarrow{\$} \mathsf{Sig.Sign}(\mathsf{sigk}, m)$.

$\mathsf{Sig.Verify}'^{H}(\mathsf{vk}' = (\mathsf{vk}, \mathsf{pk}), m, \sigma)$**:** This algorithm works in the exactly same way as $\mathsf{Sig.Verify}(\mathsf{vk}, m, \sigma)$.

By the security of PoQRO, any quantum polynomial-time adversary with *classical* access to H cannot find m such that $\mathsf{PoQRO.Verify}^{H}(\mathsf{sk}, m) = \top$ with non-negligible probability. Therefore, we can reduce the EUF-CMA security of the above scheme against quantum adversaries in the ROM to that of the underlying scheme (in the standard model) in a straightforward manner.

On the other hand, a quantum polynomial-time adversary with *quantum* access to H can find m such that $\mathsf{PoQRO.Verify}^{H}(\mathsf{sk}, m) = \top$ with overwhelming probability by correctness of PoQRO. Therfore, the adversary can obtain sigk by querying such an m to the signing oracle to obtain sigk. This enables the adversary to forge a signature on any message, and thus the above scheme is not EUF-CMA secure against quantum polynomial-time adversaries in the QROM. □

3.3 Public Key Encryption

In this section, we construct a PKE scheme scheme that is CCA secure in the ROM but not CCA secure in the QROM based on PoQRO.

Definition 3.5. *A public key encryption (PKE) scheme consists of classical polynomial time algorithms* $(\mathsf{PKE.KeyGen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$*:*

$\mathsf{PKE.KeyGen}(1^{\lambda})$**:** *This algorithm takes the security parameter* 1^{λ} *as input and outputs an encryption key* ek *and a decryption key* dk*.*

$\mathsf{PKE.Enc}(\mathsf{ek}, m)$**:** *This algorithm takes an encryption key* ek *and a message* m *as input and outputs a ciphertext* ct*.*

$\mathsf{PKE.Dec}(\mathsf{dk}, \mathsf{ct})$**:** *This algorithm takes a decryption key* dk *and a ciphertext* ct *as input and outputs a message* m *or* $\bot$*.*

As correctness, we require that for any m*, we have*

$$\Pr[\mathsf{PKE.Dec}(\mathsf{dk}, \mathsf{ct}) = m : (\mathsf{ek}, \mathsf{dk}) \xleftarrow{\$} \mathsf{PKE.KeyGen}(1^{\lambda}), \mathsf{ct} \xleftarrow{\$} \mathsf{PKE.Enc}(\mathsf{ek}, m)] = 1.$$

We say that a PKE scheme is CCA secure against quantum adversaries if for any quantum polynomial-time adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *we have*

$$\left| \Pr\left[\begin{array}{l} \mathcal{A}_2^{\mathsf{PKE.Dec}(\mathsf{dk},\cdot)}(|\mathsf{st}\rangle, \mathsf{ct}^*) = b \\ \wedge\ \mathcal{A}_2 \textit{ never queried } \mathsf{ct}^* \end{array} : \begin{array}{l} (\mathsf{ek}, \mathsf{dk}) \xleftarrow{\$} \mathsf{PKE.KeyGen}(1^{\lambda}), \\ (m_0, m_1, |\mathsf{st}\rangle) \xleftarrow{\$} \mathcal{A}_1^{\mathsf{PKE.Dec}(\mathsf{dk},\cdot)}, \\ b \xleftarrow{\$} \{0,1\}, \\ \mathsf{ct}^* \xleftarrow{\$} \mathsf{PKE.Enc}(\mathsf{ek}, m_b) \end{array} \right] - \frac{1}{2} \right| \leq \mathsf{negl}(\lambda)$$

where $\mathsf{PKE.Dec}(\mathsf{dk}, \cdot)$ *denotes a classical oracle that computes* $\mathsf{PKE.Dec}(\mathsf{dk}, \cdot)$*.*

Lemma 3.6. *If the QLWE assumption holds, then there exists a PKE scheme that is CCA secure against quantum adversaries in the ROM but not CCA secure against quantum adversaries in the QROM.*

Proof. Let $(\mathsf{PKE.KeyGen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ be a PKE scheme that is CCA secure against quantum adversaries in the standard model. Such a scheme exists under the QLWE assumption [PW08]. Let $(\mathsf{PoQRO.Setup}, \mathsf{PoQRO.Prove}, \mathsf{PoQRO.Verify})$ be a PoQRO, which exists under the QLWE assumption as shown in Lemma 3.2. Then we consider a PKE scheme $(\mathsf{PKE.KeyGen}', \mathsf{PKE.Enc}', \mathsf{PKE.Dec}')$ that uses a random oracle H described below:

$\mathsf{PKE.Enc}'^{H}(1^\lambda)$**:** This algorithm generates $(\mathsf{ek}, \mathsf{dk}) \xleftarrow{\$} \mathsf{PKE.KeyGen}(1^\lambda)$ and $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{PoQRO.Setup}(1^\lambda)$, and outputs $\mathsf{ek}' := (\mathsf{ek}, \mathsf{pk})$ and $\mathsf{dk}' := (\mathsf{dk}, \mathsf{sk})$.

$\mathsf{PKE.Enc}'^{H}(\mathsf{ek}' = (\mathsf{ek}, \mathsf{pk}), m)$**:** This algorithm works in the exactly same way as $\mathsf{PKE.Enc}(\mathsf{ek}, m)$.

$\mathsf{PKE.Dec}'^{H}(\mathsf{dk}' = (\mathsf{dk}, \mathsf{sk}), \mathsf{ct})$**:** If $\mathsf{PoQRO.Verify}^{H}(\mathsf{sk}, \mathsf{ct}) = \top$, then it outputs dk. Otherwise, it outputs $m \xleftarrow{\$} \mathsf{PKE.Dec}(\mathsf{dk}, \mathsf{ct})$.

By the security of PoQRO, any quantum polynomial-time adversary with *classical* access to H cannot find ct such that $\mathsf{PoQRO.Verify}^{H}(\mathsf{sk}, \mathsf{ct}) = \top$ with non-negligible probability. Therefore, we can reduce the CCA security of the above scheme against quantum adversaries in the ROM to that of the underlying scheme (in the standard model) in a straightforward manner.

On the other hand, a quantum polynomial-time adversary with *quantum* access to H can find ct such that $\mathsf{PoQRO.Verify}^{H}(\mathsf{sk}, \mathsf{ct}) = \top$ with overwhelming probability by correctness of PoQRO. Therfore, the adversary can obtain dk by querying such an ct to the decryption oracle to obtain dk. This enables the adversary to decrypt any ciphertext, and thus the above scheme is not CCA secure against quantum polynomial-time adversary in the QROM. □

References

[ABB10] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 553–572. Springer, Heidelberg, May / June 2010.

[BCM+18] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh V. Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In Mikkel Thorup, editor, *59th FOCS*, pages 320–331. IEEE Computer Society Press, October 2018.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Heidelberg, December 2011.

[BKVV20] Zvika Brakerski, Venkata Koppula, Umesh Vazirani, and Thomas Vidick. Simpler proofs of quantumness. *arXiv*, 2005.04826, 2020.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.

[BR95] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. In Alfredo De Santis, editor, *EUROCRYPT'94*, volume 950 of *LNCS*, pages 92–111. Springer, Heidelberg, May 1995.

[BR96] Mihir Bellare and Phillip Rogaway. The exact security of digital signatures: How to sign with RSA and Rabin. In Ueli M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 399–416. Springer, Heidelberg, May 1996.

[CHKP10] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 523–552. Springer, Heidelberg, May / June 2010.

[DFMS19] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the Fiat-Shamir transformation in the quantum random-oracle model. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 356–383. Springer, Heidelberg, August 2019.

[FO13] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *Journal of Cryptology*, 26(1):80–101, January 2013.

[FOPS01] Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern. RSA-OAEP is secure under the RSA assumption. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 260–274. Springer, Heidelberg, August 2001.

[FS87] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, Heidelberg, August 1987.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.

[JZC+18] Haodong Jiang, Zhenfeng Zhang, Long Chen, Hong Wang, and Zhi Ma. IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 96–125. Springer, Heidelberg, August 2018.

[KYY18] Shuichi Katsumata, Shota Yamada, and Takashi Yamakawa. Tighter security proofs for GPV-IBE in the quantum random oracle model. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 253–282. Springer, Heidelberg, December 2018.

[LZ19] Qipeng Liu and Mark Zhandry. Revisiting post-quantum Fiat-Shamir. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 326–355. Springer, Heidelberg, August 2019.

[PS96] David Pointcheval and Jacques Stern. Security proofs for signature schemes. In Ueli M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 387–398. Springer, Heidelberg, May 1996.

[PW08] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 187–196. ACM Press, May 2008.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009.

[TU16] Ehsan Ebrahimi Targhi and Dominique Unruh. Post-quantum security of the Fujisaki-Okamoto and OAEP transforms. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B, Part II*, volume 9986 of *LNCS*, pages 192–216. Springer, Heidelberg, October / November 2016.

[Zha12] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, Heidelberg, August 2012.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 239–268. Springer, Heidelberg, August 2019.

[ZYF+19] Jiang Zhang, Yu Yu, Dengguo Feng, Shuqin Fan, and Zhenfeng Zhang. On the (quantum) random oracle methodology: New separations and more. Cryptology ePrint Archive, Report 2019/1101, 2019. https://eprint.iacr.org/2019/1101.