SCIS 2018 2018 Symposium on Cryptography and Information Security
Niigata, Japan, Jan. 23 - 26, 2018
The Institute of Electronics, Information and Communication Engineers

Security Notions for the Random Oracle Model in Classical and Quantum Settings

Jeeun Lee* Seunghyun Lee** Kwangjo Kim*

Abstract: The advent of quantum computers and their algorithms has opened the era of post-quantum and fully-quantum cryptography. Accordingly, new security proof tools and notions in a quantum setting need to be settled in order to prove the security of cryptographic primitives appropriately. As the random oracle model is accepted as an efficient security proof tool, it has been suggested to extend it from a classical to quantum setting by allowing the adversary's access to quantum computation. In this paper, we look at the background of the classical, quantum-accessible, and quantum random oracle models for classical, post-quantum, and fully-quantum cryptography, respectively, and how they are defined. Also, suitable security notions for each model are introduced such as IND-ATK, (IND/wqIND/qIND)-qATK, and cqIND-qATK, for ATK $\in \{\mathrm{CPA}, \mathrm{CCA1}, \mathrm{CCA2}\}$. Finally, a brief comparison of different cryptography eras are provided.

Keywords: classical random oracle · quantum-accessible random oracle · quantum random oracle · quantum indistinguishability · quantum attack

1 Introduction

1.1 The Advent of Quantum Computers

As more and more refined classical, *i.e.*, non-quantum, computers are developed, several problems have been encountered such as quantum tunnelling and heat generation. Quantum tunnelling is a phenomenon where a particle tunnels through a barrier that is deemed insurmountable in the classical world. Since the number of transistors in a dense integrated circuit has doubled approximately every 18 months [Moo65], the gaps between transistor terminals would shrink to the classical limits at some point. Then the electrons are able to move between terminals, that is, a transistor in an off state could be unexpectedly switched on even if it is not supposed to be. Also, classical computers use logically irreversible manipulation of information where the output of a device does not uniquely define the inputs, for example, by erasing a bit or merging two computation paths. This necessarily implies physical irreversibility and corresponding heat increase by $nkT \ln 2$ for erasure of n-bit known information, where k is the Boltzmann constant and T is the temperature of the heat sink in kelvins [Lan61].

Quantum computers have been proposed as a natural solution to circumventing the aforementioned problems since 1970s. Quantum computers are based on quantum mechanics, which applies to all systems ranging from micro to macro scales, and use quantum bits, *i.e.*, qubits, to create quantum logic gates for quantum computing. A pure qubit can be represented as a linear superposition of the basis states, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where the complex numbers α and β satisfy $|\alpha|^2 + |\beta|^2 = 1$. We may then use n qubits to represent either 2^n different superposed states, or entangled states. Besides, quantum computers use logically reversible manipulation where the output of a device always uniquely determines its input, by using an injective function for mapping old states to new ones. Such manipulation requires no release of heat in principle [Lan61]. For these reasons, quantum computing has attracted research interest both academically and commercially since its initial proposal.

1.2 Security Proofs in a Quantum Setting

After the publication of Deutsch's groundbreaking paper [Deu85], many quantum algorithms have been introduced, the most famous of which are Simon's algorithm [Sim94], Shor's algorithm [Sho94, Sho97], and Grover's algorithm [Gro96, Gro97]. When large-scale quantum computers are available, Shor's algorithm could break classical asymmetric encryption and digital signature schemes based on integer factorization and discrete logarithm problems in polynomial time. Also, classical symmetric encryption schemes would not be safe due to Grover's algorithm and Simon's algorithm. It has been believed until recently that doubling the key size would provide security against Grover's algorithm [CJL+16, ABB+15], however, widely used modes of operation for authentication and authenticated encryption have proved to be completely broken using Simon's algorithm [KLLNP16, SS16].

In this manner, quantum security of the current cryptosystems has been investigated, and the cryptographic community has developed new security notions and

* School of Computing, KAIST, Daejeon 34141, South Korea. {jeeun.lee,kkj}@kaist.ac.kr
** Department of Mathematical Sciences, KAIST, Daejeon 34141, South Korea. camusian@kaist.ac.kr

proof models accordingly [BDF+11,BJ15,GHS16,Gag17, SLL16]. The most notable security proof models for provable security are the standard and the random oracle models. In the standard model, existence of certain *basic* primitives are assumed, *e.g.*, one-way function, based on which more complex schemes are devised. Hence, cryptographic design in this model proceeds as follows: (a) assume hardness of a computational problem concerning the basic primitive, and (b) prove that an attack necessarily reduces to solving the hard problem. However, in practice, we have access to more *sophisticated* primitives, *e.g.*, hash function, we may readily use. In the random oracle model, these *sophisticated* primitives are idealized as random oracles, which are in turn used for cryptographic design and security proof [BR93]. In this paper, we focus on the random oracle model as it is accepted as a more efficient and feasible proof model than the standard model. Also, the extension of the random oracle model from a classical to quantum setting is explained and suitable security notions for each model are introduced.

1.3 Organization

The rest of this paper is organized as follows. First, the classical and quantum cryptographic primitives and some security notions are briefly recalled in Section 2. The random oracle model in classical, post-quantum, and fully-quantum settings are explained from Sections 3 to 5. Also, suitable security notions for each model are introduced. In Section 6, we conclude the survey by comparing security notions and proof models.

2 Preliminaries

2.1 Classical Cryptographic Primitives

Definition 2.1 (Symmetric Encryption). *A symmetric encryption scheme* Π_{sym} *is a tuple of classical probabilistic polynomial-time algorithms* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *and sets called key space* $\mathcal{K}$*, message space* $\mathcal{M}$*, and ciphertext space* $\mathcal{C}$ *such that*

- $\mathsf{k} \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda)$*: the key generation algorithm* KeyGen *receives a security parameter* λ *and outputs key* $\mathsf{k} \in \mathcal{K}$*.*
- $\mathsf{c} \xleftarrow{\$} \mathsf{Enc}_{\mathsf{k}}(\mathsf{m})$*: the encryption algorithm* Enc *uses the key* k *to encrypt a message* $\mathsf{m} \in \mathcal{M}$ *and outputs a ciphertext* $\mathsf{c} \in \mathcal{C}$*.*
- $\mathsf{m} \leftarrow \mathsf{Dec}_{\mathsf{k}}(\mathsf{c})$*: the decryption algorithm* Dec *uses the key* k *to decrypt a ciphertext* $\mathsf{c} \in \mathcal{C}$ *and outputs a message* m *or* $\perp$ *denoting* c *is invalid.*

For any k *and any* m*, the scheme should satisfy*

$$\Pr\left[\mathsf{Dec}_{\mathsf{k}}(\mathsf{Enc}_{\mathsf{k}}(\mathsf{m})) \neq \mathsf{m}\right] = \mathsf{negl}(\lambda).$$

Definition 2.2 (Asymmetric Encryption). *An asymmetric encryption scheme* Π_{asym} *is a tuple of classical probabilistic polynomial-time algorithms* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *and sets called key space* $\mathcal{K}$*, message space* $\mathcal{M}$*, and ciphertext space* $\mathcal{C}$ *such that*

- $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda)$*: the key generation algorithm* KeyGen *receives a security parameter* λ *and outputs a random pair of corresponding public key* $\mathsf{pk} \in \mathcal{K}$ *and secret key* $\mathsf{sk} \in \mathcal{K}$*.*
- $\mathsf{c} \xleftarrow{\$} \mathsf{Enc}_{\mathsf{pk}}(\mathsf{m})$*: the encryption algorithm* Enc *uses the public key* pk *to encrypt a message* $\mathsf{m} \in \mathcal{M}$ *and outputs a ciphertext* $\mathsf{c} \in \mathcal{C}$*.*
- $\mathsf{m} \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\mathsf{c})$*: the decryption algorithm* Dec *uses the secret key* sk *to decrypt a ciphertext* $\mathsf{c} \in \mathcal{C}$ *and outputs a message* m *or* $\perp$ *denoting* c *is invalid.*

For any $(\mathsf{pk}, \mathsf{sk})$ *and any* m*, the scheme should satisfy*

$$\Pr\left[\mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{pk}}(\mathsf{m})) \neq \mathsf{m}\right] = \mathsf{negl}(\lambda).$$

2.2 Quantum Cryptographic Primitives

Definition 2.3 (Quantum Symmetric Encryption). *A quantum symmetric encryption scheme* Π_{qsym} *is a tuple of quantum probabilistic polynomial-time algorithms* $(\mathsf{KeyGen}, \mathsf{QEnc}, \mathsf{QDec})$ *and sets called key space* $\mathcal{K}$*, message space* $\mathsf{D}(\mathcal{H}_{\mathcal{M}})$*, and ciphertext space* $\mathsf{D}(\mathcal{H}_{\mathcal{C}})$ *such that*

- $\mathsf{k} \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda)$*: the key generation algorithm* KeyGen *receives a security parameter* λ *and outputs key* $\mathsf{k} \in \mathcal{K}$*.*
- $\rho_{\mathsf{c}} \xleftarrow{\$} \mathsf{QEnc}_{\mathsf{k}}(\rho_{\mathsf{m}})$*: the quantum encryption algorithm* QEnc *uses the key* k *to encrypt a message* $\rho_{\mathsf{m}} \in \mathsf{D}(\mathcal{H}_{\mathcal{M}})$ *and outputs a ciphertext* $\rho_{\mathsf{c}} \in \mathsf{D}(\mathcal{H}_{\mathcal{C}})$*.*
- $\rho_{\mathsf{m}} \leftarrow \mathsf{QDec}_{\mathsf{k}}(\rho_{\mathsf{c}})$*: the quantum decryption algorithm* QDec *uses the key* k *to decrypt a ciphertext* $\rho_{\mathsf{c}} \in \mathsf{D}(\mathcal{H}_{\mathcal{C}})$ *and outputs a message* ρ_{m} *or* $\perp$ *denoting* ρ_{c} *is invalid.*

For any k *and any* ρ_{m}*, the scheme should satisfy*

$$\Pr\left[\hat{U}_{\mathsf{QDec}_{\mathsf{k}}}\hat{U}_{\mathsf{QEnc}_{\mathsf{k}}}\rho_{\mathsf{m}}(\hat{U}_{\mathsf{QEnc}_{\mathsf{k}}})^{\dagger}(\hat{U}_{\mathsf{QDec}_{\mathsf{k}}})^{\dagger} \neq \rho_{\mathsf{m}}\right] = \mathsf{negl}(\lambda).$$

Definition 2.4 (Quantum Asymmetric Encryption). *A quantum asymmetric encryption scheme* Π_{qasym} *is a tuple of quantum probabilistic polynomial-time algorithms* $(\mathsf{KeyGen}, \mathsf{QEnc}, \mathsf{QDec})$ *and sets called key space* $\mathcal{K}$*, message space* $\mathsf{D}(\mathcal{H}_{\mathcal{M}})$*, and ciphertext space* $\mathsf{D}(\mathcal{H}_{\mathcal{C}})$ *such that*

- $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda)$*: the key generation algorithm* KeyGen *receives a security parameter* λ *and outputs a random pair of corresponding public key* $\mathsf{pk} \in \mathcal{K}$ *and secret key* $\mathsf{sk} \in \mathcal{K}$*.*
- $\rho_{\mathsf{c}} \xleftarrow{\$} \mathsf{QEnc}_{\mathsf{pk}}(\rho_{\mathsf{m}})$*: the quantum encryption algorithm* QEnc *uses the public key* pk *to encrypt a message* $\rho_{\mathsf{m}} \in \mathsf{D}(\mathcal{H}_{\mathcal{M}})$ *and outputs a ciphertext* $\rho_{\mathsf{c}} \in \mathsf{D}(\mathcal{H}_{\mathcal{C}})$*.*
- $\rho_{\mathsf{m}} \leftarrow \mathsf{QDec}_{\mathsf{sk}}(\rho_{\mathsf{c}})$*: the quantum decryption algorithm* QDec *uses the secret key* sk *to decrypt a ciphertext* $\rho_{\mathsf{c}} \in \mathsf{D}(\mathcal{H}_{\mathcal{C}})$ *and outputs a message* ρ_{m} *or* $\perp$ *denoting* ρ_{c} *is invalid.*

For any $(\mathsf{pk}, \mathsf{sk})$ *and any* ρ_{m}*, the scheme should satisfy*

$$\Pr\left[\hat{U}_{\mathsf{QDec}_{\mathsf{sk}}}\hat{U}_{\mathsf{QEnc}_{\mathsf{pk}}}\rho_{\mathsf{m}}(\hat{U}_{\mathsf{QEnc}_{\mathsf{pk}}})^{\dagger}(\hat{U}_{\mathsf{QDec}_{\mathsf{sk}}})^{\dagger} \neq \rho_{\mathsf{m}}\right] = \mathsf{negl}(\lambda).$$

The concept of quantum encryption was first introduced in [BR00]. Here, the set of all density operators on a Hilbert space $\mathcal{H}_n$ is denoted as $\mathsf{D}(\mathcal{H}_n)$. Note that a quantum encryption scheme uses a classical bit string for a key, and arbitrary quantum states for plaintexts and ciphertexts. The generated key among honest parties must be classical in order to encrypt and decrypt multiple times with the same key. Also, any quantum algorithm must be a set of unitary operations[1] because its output is the time evolution of an input, $|\psi(t)\rangle = \hat{U}(t)|\psi(0)\rangle$, which gives $(\hat{U}(t))^\dagger \hat{U}(t) = \hat{I}$ for all t. As in classical cryptographic primitives, decryption of an encrypted plaintext under the same key must recover the original plaintext with negligible error.

2.3 Security Notions

As one of possible security goals, *indistinguishability* formalizes an adversary's advantage to distinguish the encryptions of two plaintexts of the same length [GM84]. As possible attack models, three different attacks are considered: *chosen-plaintext attack* (CPA), *non-adaptive chosen-ciphertext attack* (CCA1), and *adaptive chosen-ciphertext attack* (CCA2). Under CPA, the adversary has an encryption oracle access and obtains ciphertexts for plaintexts of their choice [GM84]. Under CCA1, the adversary has an additional decryption oracle access before the challenge phase [NY90], whereas under CCA2, the adversary has an additional decryption oracle access before and after the challenge phase [RS91]. The CCA2 adversary, however, is not allowed to query the challenge ciphertext itself to the decryption oracle. Hence, the decryption oracle after the challenge phase is modified as follows:

$$\mathsf{Dec}_{\mathsf{k}}^{\mathsf{c_b}}(\mathsf{c}) = \begin{cases} \perp & \text{if } \mathsf{c} = \mathsf{c_b} \\ \mathsf{Dec_k}(\mathsf{c}) & \text{otherwise.} \end{cases}$$

Also, the term *adaptive* is in respect of the challenge phase, not oracle's answers. Note that the adversary under any attack is able to choose queries adaptively to the oracle's answers.

3 Classical Cryptography

3.1 Classical Random Oracle Model

The *classical random oracle* (CRO) model is an efficient security proof tool introduced in [BR93] in order to bridge the gap between theory and practice. For implementation of an ideal system in the real world, the following two steps are performed. First, one designs an ideal system where all parties have an oracle access to a truly random function f and proves the security of this system. Then one replaces the random oracle with a *good* hash function. In the random oracle model, the random oracle makes an independent random choice for each query, but returns the same answer for the same query by recording all previous responses. In a classical query algorithm,

$$\mathsf{state}_i := \mathcal{O}_f(x_i, \mathsf{state}_{i-1}),$$

where x_i and state_i are the i-th query and the state for an oracle $\mathcal{O}_f$, respectively. Although there have been controversies concerning too strong assumptions for a hash function to be modelled as a random oracle [CGH04], the CRO model became a good replacement of the standard model where security proofs are extremely difficult to achieve. Furthermore, no real-world protocol based on the random oracle model has failed in practice for the past twenty years [KM15].

The security proof procedure to devise a good protocol P for a given protocol problem Π is summarized as follows:

(a) Find a formal definition for Π in the model where all parties share a random oracle.
(b) Devise an efficient protocol P for Π.
(c) Prove that P satisfies the definition for Π.
(d) Replace oracle accesses to the random oracle with hash function computation.

The protocol problem Π and protocol P should be independent of the hash function we use.

3.2 Classical Security Notions

For the CRO model, the *indistinguishability under ATK* (IND-ATK) is defined as follows:

Definition 3.1 (IND-ATK for Π_{sym}). *For* $\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{CCA1}, \mathsf{CCA2}\}$*, a symmetric encryption scheme* Π_{sym} *is said to be IND-ATK secure if the advantage of any classical probabilistic polynomial-time adversary* $\mathcal{A} = (\mathcal{A}_\mathsf{M}, \mathcal{A}_\mathsf{D})$*, where* $\mathcal{A}_\mathsf{M}$ *and* $\mathcal{A}_\mathsf{D}$ *are a message generator and a distinguisher, respectively, winning the game is negligible.*

$$\mathsf{Adv}_{\mathcal{A},\Pi_{\mathsf{sym}}}^{\mathsf{IND-ATK}}(\lambda) := 2 \cdot \mathsf{Succ}_{\mathcal{A},\Pi_{\mathsf{sym}}}^{\mathsf{IND-ATK}} - 1 = \mathsf{negl}(\lambda),$$

where $\mathsf{Succ}_{\mathcal{A},\Pi_{\mathsf{sym}}}^{\mathsf{IND-ATK}}$ *is as follows:*

$$\Pr\Big[\mathsf{k} \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda); (\mathsf{m}_0, \mathsf{m}_1, \mathsf{state}) \xleftarrow{\$} \mathcal{A}_\mathsf{M}^{\mathcal{O}_1}; \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{c_b} \xleftarrow{\$} \mathcal{O}_{\mathsf{Enc_k}}(\mathsf{m_b}); \mathsf{b}' \leftarrow \mathcal{A}_\mathsf{D}^{\mathcal{O}_2}(\mathsf{c_b}, \mathsf{state}) : \mathsf{b}' = \mathsf{b}\Big] \quad \textit{for}$$

$$(\mathsf{ATK}, \mathcal{O}_1, \mathcal{O}_2) = \begin{cases} (\mathsf{CPA}, \mathcal{O}_{\mathsf{Enc_k}}, \mathcal{O}_{\mathsf{Enc_k}}) \\ (\mathsf{CCA1}, \{\mathcal{O}_{\mathsf{Enc_k}}, \mathcal{O}_{\mathsf{Dec_k}}\}, \mathcal{O}_{\mathsf{Enc_k}}) \\ (\mathsf{CCA2}, \{\mathcal{O}_{\mathsf{Enc_k}}, \mathcal{O}_{\mathsf{Dec_k}}\}, \{\mathcal{O}_{\mathsf{Enc_k}}, \mathcal{O}_{\mathsf{Dec_k^{c_b}}}\}). \end{cases}$$

Definition 3.2 (IND-ATK for Π_{asym}). *For* $\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{CCA1}, \mathsf{CCA2}\}$*, an asymmetric encryption scheme* Π_{asym} *is said to be IND-ATK secure if the advantage of any classical probabilistic polynomial-time adversary* $\mathcal{A} = (\mathcal{A}_\mathsf{M}, \mathcal{A}_\mathsf{D})$*, where* $\mathcal{A}_\mathsf{M}$ *and* $\mathcal{A}_\mathsf{D}$ *are a message generator and a distinguisher, respectively, winning the game is negligible.*

$$\mathsf{Adv}_{\mathcal{A},\Pi_{\mathsf{asym}}}^{\mathsf{IND-ATK}}(\lambda) := 2 \cdot \mathsf{Succ}_{\mathcal{A},\Pi_{\mathsf{asym}}}^{\mathsf{IND-ATK}} - 1 = \mathsf{negl}(\lambda),$$

[1] A unitary operation, any transformation that preserves the inner product, is used to make the norm of the physical state stay fixed.

where $\mathsf{Succ}^{\mathsf{IND-ATK}}_{\mathcal{A},\Pi_{\mathsf{asym}}}$ *is as follows:*

$$\Pr\Big[(\mathsf{pk},\mathsf{sk}) \overset{\$}{\leftarrow} \mathsf{KeyGen}(1^\lambda); (\mathsf{m}_0,\mathsf{m}_1,\mathsf{state}) \overset{\$}{\leftarrow} \mathcal{A}^{\mathcal{O}_1}_{\mathsf{M}};$$
$$\mathsf{b} \overset{\$}{\leftarrow} \{0,1\}; \mathsf{c_b} \overset{\$}{\leftarrow} \mathcal{O}_{\mathsf{Enc_{pk}}}(\mathsf{m_b});$$
$$\mathsf{b}' \leftarrow \mathcal{A}^{\mathcal{O}_2}_{\mathsf{D}}(\mathsf{c_b},\mathsf{state}) : \mathsf{b}' = \mathsf{b}\Big] \quad \textit{for}$$

$$(\mathsf{ATK},\mathcal{O}_1,\mathcal{O}_2) = \begin{cases} (\mathsf{CPA},\epsilon,\epsilon) \\ (\mathsf{CCA1},\mathcal{O}_{\mathsf{Dec_{sk}}},\epsilon) \\ (\mathsf{CCA2},\mathcal{O}_{\mathsf{Dec_{sk}}},\mathcal{O}_{\mathsf{Dec^{c_b}_{sk}}}). \end{cases} \quad {}^2$$

The definition of IND-ATK for Π_{asym} was formalized in [BDPR98, Definition 2.1].

4 Post-quantum Cryptography

4.1 Quantum-accessible Random Oracle Model

A classical query algorithm that computes a Boolean function $f : \{0,1\}^n \to \{0,1\}$ by using oracle queries is called a *decision tree*. A decision tree can be represented as a binary tree where each node represents a query, and its two children represent the two possible outcomes of the query. A leaf node represents the final answer 0 or 1. The depth of the tree, *i.e.*, the number of queries needed to compute f, is the cost of an algorithm. This query model is useful in security proof since the number of queries an adversary needs to break a scheme corresponds to the time the attack takes.

Following [BBC+98], a quantum query algorithm with q queries is a quantum analogue of a classical decision tree with q queries, where we use the power of quantum parallelism by making queries and operations in quantum superposition. This can be represented as a sequence of unitary transformations:

$$\hat{\mathsf{Alg}}_{\mathsf{Qa}} := \hat{U}_q\hat{\mathcal{O}}_f \cdots \hat{U}_1\hat{\mathcal{O}}_f\hat{U}_0.$$

Here, $\hat{U}_j$'s are fixed unitary transformations that do not depend on inputs, and the (possibly) identical $\hat{\mathcal{O}}_f$'s are unitary transformations that correspond to an oracle.

Consider a quantum system consisting of m qubits, with each qubit having basis states $|0\rangle$ and $|1\rangle$, so that there are 2^m possible basis states. Then the oracle transformation $\hat{\mathcal{O}}_f$, called *quantum-accessible random oracle* (QaRO), maps basis state $|x,y,z\rangle$ to $|x, y \oplus f(x), z\rangle$, where the length of query register x is $\lceil \log n \rceil$ qubits, answer register y is one qubit, ancilla register z is an arbitrary string of $m - \lceil \log n \rceil - 1$ qubits, and $\oplus$ is exclusive or. Besides the standard transformation which maps basis state $|x,y\rangle$ to $|x, y \oplus g(x)\rangle$ for a general function $g : \{0,1\}^n \to \{0,1\}^m$, there can be different transformations to implement an oracle such as *Fourier phase* oracle $|x,y\rangle \to e^{2\pi i g(x)y/2^m}|x,y\rangle$ and *minimal* oracle $|x\rangle \to |g(x)\rangle$ [KKVB02]. Using standard and minimal oracles, the following quantum encryption oracles are used for constructing security notions in Section 4.2: $\hat{\mathcal{O}}_{\mathsf{Enc_k}}$ mapping basis state $|\mathsf{m},\mathsf{c}\rangle$ to $|\mathsf{m},\mathsf{c} \oplus \mathsf{Enc_k}(\mathsf{m})\rangle$ and $\hat{\mathcal{O}}'_{\mathsf{Enc_k}}$ mapping basis state $|\mathsf{m}\rangle$ to $|\mathsf{Enc_k}(\mathsf{m})\rangle$.

Finally, the $\hat{\mathsf{Alg}}_{\mathsf{Qa}}$ is applied to an oracle-independent initial state, which gives an oracle-dependent final state. The computation ends with some measurement or observation of the final state.

4.2 Post-quantum Security Notions

The QaRO model replaces all classical communication with quantum communication by allowing an adversary to have both quantum encryption oracle access and quantum challenge queries. In this case, the adversary and the challenger are modelled as quantum circuits sharing a certain number of qubits. For this model, one of the first attempts at defining a security notion was to extend IND-CPA to *fully-quantum indistinguishability under quantum chosen-plaintext attack* (fqIND-qCPA), which renames [BZ13, Definition 4.1] for consistency. This security notion is the most naturally emerging concept for an entirely quantum game, however, no symmetric encryption scheme satisfies it due to the entanglement between quantum registers:

Theorem 4.1 (BZ Attack [BZ13, Theorem 4.2]). *No symmetric encryption scheme achieves fqIND-qCPA security.*

Proof. The proof [GHS16, Proof 2.7] can be interpreted as follows: as shown in Figure 1, the generic adversary $\mathcal{A}$ prepares three quantum registers, two message registers and an ancilla register for storing ciphertext.

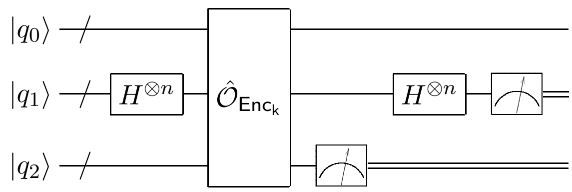

Fig. 1. Quantum circuit for BZ attack

- They are initialized as $|0^n\rangle$ and the initial quantum state is $|\varphi_0\rangle = |0^n\rangle|0^n\rangle|0^n\rangle$.
- To put superposition of all possible messages in the second register, the Hadamard gate acts on $|q_1\rangle$ and the state becomes $|\varphi_1\rangle = |0^n\rangle \sum_{x\in\{0,1\}^n} 2^{-n/2}|x\rangle|0^n\rangle$.
- When $\mathcal{A}$ challenges fqIND game and gets a quantum encryption oracle access mapping basis state $|q_0,q_1,q_2\rangle$ to $|q_0,q_1,q_2 \oplus \mathsf{Enc_k}(q_b)\rangle$, then we have two cases as below:

$$|\varphi_2\rangle = \begin{cases} |0^n\rangle \sum_{x\in\{0,1\}^n} 2^{-n/2}|x\rangle|\mathsf{Enc_k}(0^n)\rangle & \text{if } b=0 \\ |0^n\rangle \sum_{x\in\{0,1\}^n} 2^{-n/2}|x\rangle|\mathsf{Enc_k}(x)\rangle & \text{if } b=1. \end{cases}$$

- Measurement on $|q_2\rangle$ gives

$$|\varphi_3\rangle = \begin{cases} |0^n\rangle \sum_{x\in\{0,1\}^n} 2^{-n/2}|x\rangle|\mathsf{Enc_k}(0^n)\rangle & \text{if } b=0 \\ |0^n\rangle|x\rangle|\mathsf{Enc_k}(x)\rangle \text{ with prob. } 2^{-n} & \text{if } b=1. \end{cases}$$

[2] $\mathcal{O}_i = \epsilon$ is the function returning the empty string ϵ on any input.

- Acting the Hadamard on $|q_1\rangle$ again gives

$$|\varphi_4\rangle = \begin{cases} |0^n\rangle|0^n\rangle|\mathsf{Enc_k}(0^n)\rangle & \text{if } b=0 \\ |0^n\rangle(|+\rangle^{n_0}|-\rangle^{n-n_0})|\mathsf{Enc_k}(x)\rangle & \text{if } b=1. \end{cases}$$

- Finally, the measurement on $|q_1\rangle$ gives

$$|\varphi_5\rangle = \begin{cases} |0^n\rangle|0^n\rangle|\mathsf{Enc_k}(0^n)\rangle & \text{if } b=0 \\ |0^n\rangle|i\rangle|\mathsf{Enc_k}(x)\rangle \text{ for } i \in \{0,1\}^n & \\ \qquad\qquad \text{with prob. } 2^{-n} & \text{if } b=1. \end{cases}$$

For $b = 0$, the measurement on $|q_1\rangle$ yields $|0^n\rangle$ with probability 1. For $b = 1$, the measurement on $|q_1\rangle$ yields $|0^n\rangle$ with probability 2^{-n}. The $\mathcal{A}$ outputs $b' = 0$ iff the last outcome is $|0^n\rangle$, otherwise $b' = 1$. □

In order to find weaker but achievable security notions, [GHS16] analyses 16 possible candidates by spanning a binary tree. [GHS16] considers the challenger model instead of the random oracle model, in order to rule out far too powerful adversaries. In this model, the adversary and the challenger do not share the same quantum circuits. The adversary now has an access to the quantum encryption oracle provided by an external challenger, whereas in the random oracle model, the adversary has a direct access to the quantum encryption oracle. Excluding unreasonable or unachievable notions, the following definitions are left: *indistinguishability under quantum ATK* (IND-qATK), *weak-quantum indistinguishability under quantum ATK* (wqIND-qATK), and *quantum indistinguishability under quantum ATK* (qIND-qATK).

Definition 4.1 (IND-qATK for Π_{sym}). *For* $\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{CCA1}, \mathsf{CCA2}\}$*, a symmetric encryption scheme* Π_{sym} *is said to be IND-qATK secure if the advantage of any quantum probabilistic polynomial-time adversary* $\mathcal{A} = (\mathcal{A}_{\mathsf{M}}, \mathcal{A}_{\mathsf{D}})$*, where* $\mathcal{A}_{\mathsf{M}}$ *and* $\mathcal{A}_{\mathsf{D}}$ *are a message generator and a distinguisher, respectively, winning the game is negligible.*

$$\mathsf{Adv}^{\mathsf{IND-qATK}}_{\mathcal{A},\Pi_{\mathsf{sym}}}(\lambda) := 2 \cdot \mathsf{Succ}^{\mathsf{IND-qATK}}_{\mathcal{A},\Pi_{\mathsf{sym}}} - 1 = \mathsf{negl}(\lambda),$$

where $\mathsf{Succ}^{\mathsf{IND-qATK}}_{\mathcal{A},\Pi_{\mathsf{sym}}}$ *is as follows:*

$$\Pr\Big[\mathsf{k} \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda); (\mathsf{m}_0, \mathsf{m}_1, |\mathsf{state}\rangle) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_1}_{\mathsf{M}}; \\ \mathsf{b} \xleftarrow{\$} \{0,1\}; \mathsf{c_b} \xleftarrow{\$} \mathcal{O}_{\mathsf{Enc_k}}(\mathsf{m_b}); \\ \mathsf{b}' \leftarrow \mathcal{A}^{\mathcal{O}_2}_{\mathsf{D}}(\mathsf{c_b}, |\mathsf{state}\rangle) : \mathsf{b}' = \mathsf{b}\Big] \quad \textit{for}$$

$$(\mathsf{ATK}, \mathcal{O}_1, \mathcal{O}_2) = \begin{cases} (\mathsf{CPA}, \hat{\mathcal{O}}_{\mathsf{Enc_k}}, \hat{\mathcal{O}}_{\mathsf{Enc_k}}) \\ (\mathsf{CCA1}, \{\hat{\mathcal{O}}_{\mathsf{Enc_k}}, \hat{\mathcal{O}}_{\mathsf{Dec_k}}\}, \hat{\mathcal{O}}_{\mathsf{Enc_k}}) \\ (\mathsf{CCA2}, \{\hat{\mathcal{O}}_{\mathsf{Enc_k}}, \hat{\mathcal{O}}_{\mathsf{Dec_k}}\}, \{\hat{\mathcal{O}}_{\mathsf{Enc_k}}, \hat{\mathcal{O}}_{\mathsf{Dec_k^{c_b}}}\}). \end{cases}$$

The definitions of IND-qCPA and IND-qCCA were discussed in [BZ13, Definition 4.5] and [BZ13, Definition 4.6], respectively.

Definition 4.2 (wqIND-qATK for Π_{sym}). *For* $\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{CCA1}\}$*, a symmetric encryption scheme* Π_{sym} *is said to be wqIND-qATK secure if the advantage of any quantum probabilistic polynomial-time adversary* $\mathcal{A} = (\mathcal{A}_{\mathsf{M}}, \mathcal{A}_{\mathsf{D}})$*, where* $\mathcal{A}_{\mathsf{M}}$ *and* $\mathcal{A}_{\mathsf{D}}$ *are a message generator and a distinguisher, respectively, winning the game is negligible.*

$$\mathsf{Adv}^{\mathsf{wqIND-qATK}}_{\mathcal{A},\Pi_{\mathsf{sym}}}(\lambda) := 2 \cdot \mathsf{Succ}^{\mathsf{wqIND-qATK}}_{\mathcal{A},\Pi_{\mathsf{sym}}} - 1 = \mathsf{negl}(\lambda),$$

where $\mathsf{Succ}^{\mathsf{wqIND-qATK}}_{\mathcal{A},\Pi_{\mathsf{sym}}}$ *is as follows:*

$$\Pr\Big[\mathsf{k} \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda); (\mathsf{Dsc}(\rho_{\mathsf{m}_0}), \mathsf{Dsc}(\rho_{\mathsf{m}_1}), \rho_{\mathsf{state}}) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_1}_{\mathsf{M}}; \\ \mathsf{b} \xleftarrow{\$} \{0,1\}; \rho_{\mathsf{m_b}} \xleftarrow{\$} \mathsf{Qbd}(\mathsf{Dsc}(\rho_{\mathsf{m_b}})); \rho_{\mathsf{c_b}} \xleftarrow{\$} \hat{\mathcal{O}}'_{\mathsf{Enc_k}}(\rho_{\mathsf{m_b}}); \\ \mathsf{b}' \leftarrow \mathcal{A}^{\mathcal{O}_2}_{\mathsf{D}}(\rho_{\mathsf{c_b}}, \rho_{\mathsf{state}}) : \mathsf{b}' = \mathsf{b}\Big] \quad \textit{for}$$

$$(\mathsf{ATK}, \mathcal{O}_1, \mathcal{O}_2) = \begin{cases} (\mathsf{CPA}, \hat{\mathcal{O}}'_{\mathsf{Enc_k}}, \hat{\mathcal{O}}'_{\mathsf{Enc_k}}) \\ (\mathsf{CCA1}, \{\hat{\mathcal{O}}'_{\mathsf{Enc_k}}, \hat{\mathcal{O}}'_{\mathsf{Dec_k}}\}, \hat{\mathcal{O}}'_{\mathsf{Enc_k}}). \end{cases}$$

The definition of wqIND-qCPA was discussed in [GHS16, Definition 3.1] and [Gag17, Definition 5.26]. Here, the classical description of a quantum state ρ, $\mathsf{Dsc}(\rho)$, is a bit string describing a quantum circuit which outputs ρ. The quantum probabilistic polynomial-time algorithm Qbd receives a classical description of a quantum state and outputs the quantum state ρ, *i.e.*, $\rho \xleftarrow{\$} \mathsf{Qbd}(\mathsf{Dsc}(\rho))$. This procedure models the situation where the adversary is familiar with the message that is encrypted but the message is not generated by the adversary himself. By doing so, it prevents the adversary from generating entanglement of the plaintext with other registers.

Definition 4.3 (qIND-qATK for Π_{sym}). *For* $\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{CCA1}\}$*, a symmetric encryption scheme* Π_{sym} *is said to be qIND-qATK secure if the advantage of any quantum probabilistic polynomial-time adversary* $\mathcal{A} = (\mathcal{A}_{\mathsf{M}}, \mathcal{A}_{\mathsf{D}})$*, where* $\mathcal{A}_{\mathsf{M}}$ *and* $\mathcal{A}_{\mathsf{D}}$ *are a message generator and a distinguisher, respectively, winning the game is negligible.*

$$\mathsf{Adv}^{\mathsf{qIND-qATK}}_{\mathcal{A},\Pi_{\mathsf{sym}}}(\lambda) := 2 \cdot \mathsf{Succ}^{\mathsf{qIND-qATK}}_{\mathcal{A},\Pi_{\mathsf{sym}}} - 1 = \mathsf{negl}(\lambda),$$

where $\mathsf{Succ}^{\mathsf{qIND-qATK}}_{\mathcal{A},\Pi_{\mathsf{sym}}}$ *is as follows:*

$$\Pr\Big[\mathsf{k} \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda); (\rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1}, \rho_{\mathsf{state}}) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_1}_{\mathsf{M}}; \\ \mathsf{b} \xleftarrow{\$} \{0,1\}; \rho_{\mathsf{c_b}} \xleftarrow{\$} \hat{\mathcal{O}}'_{\mathsf{Enc_k}}(\rho_{\mathsf{m_b}}); \textit{trace out } \rho_{\mathsf{m_{1-b}}}; \\ \mathsf{b}' \leftarrow \mathcal{A}^{\mathcal{O}_2}_{\mathsf{D}}(\rho_{\mathsf{c_b}}, \rho_{\mathsf{state}}) : \mathsf{b}' = \mathsf{b}\Big] \quad \textit{for}$$

$$(\mathsf{ATK}, \mathcal{O}_1, \mathcal{O}_2) = \begin{cases} (\mathsf{CPA}, \hat{\mathcal{O}}'_{\mathsf{Enc_k}}, \hat{\mathcal{O}}'_{\mathsf{Enc_k}}) \\ (\mathsf{CCA1}, \{\hat{\mathcal{O}}'_{\mathsf{Enc_k}}, \hat{\mathcal{O}}'_{\mathsf{Dec_k}}\}, \hat{\mathcal{O}}'_{\mathsf{Enc_k}}). \end{cases}$$

The definition of qIND-qCPA was discussed in [BJ15, Definition B.1], [GHS16, Definition 3.2], and [Gag17, Definition 5.26]. Here, tracing out is used to discard the knowledge about non-selected state since we would like

Table 1. Comparison of the random oracle model in classical, post-quantum, and fully-quantum settings

	Classical cryptography	Post-quantum cryptography	Fully-quantum cryptography
Cryptosystem	classical	classical but resistant to quantum attacks	quantum
Adversary	classical	quantum	quantum
Oracle model	CRO with a hash function f	QaRO with a hash function f	QRO with a quantum one-way function h
Quantum query	no	yes	yes
Security notion*	IND-ATK	(IND/wqIND/qIND)-qATK	cqIND-qATK
Implication	IND-CPA $\Leftarrow$ IND-qCPA $\Leftarrow$ wqIND-qCPA $\Leftarrow$ qIND-qCPA [GHS16, Figure 2]		

* The security notions are defined for ATK $\in$ {CPA, CCA1, CCA2}, except (wqIND/qIND/cqIND)-qCCA2.

to describe a particular subsystem without having to know the overall system.

For these three definitions, the security notions for Π_{asym} are defined similarly as in Definition 3.2. For quantum encryption oracles, IND-qATK game uses standard transformation $\hat{\mathcal{O}}_{\mathsf{Enc_k}}$, where $(\hat{\mathcal{O}}_{\mathsf{Enc_k}})^\dagger \neq \hat{\mathcal{O}}_{\mathsf{Dec_k}}$, and (wqIND/qIND)-qATK game uses minimal transformation $\hat{\mathcal{O}}'_{\mathsf{Enc_k}}$, where $(\hat{\mathcal{O}}'_{\mathsf{Enc_k}})^\dagger = \hat{\mathcal{O}}'_{\mathsf{Dec_k}}$. That is, whether an encryption device, *i.e.*, challenger, performs standard or minimal transformations depends on its specific architecture. For devices using standard transformation, it would be sufficient to be IND-qATK secure [GHS16].

It is worth mentioning that definition of (wqIND/qIND)-qCCA2 is not as straightforward as that of IND-(CCA2/qCCA2). In the definition of IND-(CCA2/qCCA2), there was a restriction that the adversary is not allowed to query the challenge ciphertext to the decryption oracle. Otherwise, the adversary would simply decrypt the challenge ciphertext and trivially win the game. Therefore, IND-(CCA2/qCCA2) was defined by modifying the decryption oracle, in Section 2.3: the classical IND game copies the challenge ciphertext $\mathsf{c_b}$ and stores it in order to reject forbidden queries, *i.e.*, when $\mathsf{c} = \mathsf{c_b}$. For (wqIND/qIND)-qCCA2, however, generalization of no-cloning theorem [WZ82, Die82] restricts copying the challenge ciphertext $\rho_{\mathsf{c_b}}$. Also, it is unclear whether the challenger can check if $\rho_{\mathsf{c}} = \rho_{\mathsf{c_b}}$ or not without disturbing the challenge ciphertext or the query state, due to the collapse of states after measurement [GHS16].

5 Fully-quantum Cryptography

5.1 Quantum Random Oracle Model

While a classical one-way function is based on classical infeasible mathematical problems, a quantum one-way function is provably secure by a fundamental theorem of quantum information theory [GC01]. It takes a classical bit string k as an input and outputs a quantum state $|h_k\rangle$. The mapping $k \mapsto |h_k\rangle$ is easy to compute and verify but impossible to invert without knowing k, no matter how powerful the adversary's computers are. More explicitly, [Hol73] showed that n qubits can give at most n bits of classical information although qubits can carry a larger amount of classical information. In other words, the amount of classical information that can be extracted from a quantum state is limited. It should be also noted that different classical inputs may lead to the same quantum outputs due to measurement. Therefore, in order to give effective security proofs of quantum cryptographic primitives based on quantum one-way functions, *quantum random oracle* (QRO) is introduced in [SLL16]. It is used to realize the collision-free property, so the quantum states generated by QRO are assumed to be distinguishable by its measurement. For this model, a quantum query algorithm with q queries can be represented as follows:

$$\hat{\mathsf{Alg}}_{\mathsf{Q}} := \hat{U}'_q \hat{\mathcal{O}}_h \cdots \hat{U}'_1 \hat{\mathcal{O}}_h \hat{U}'_0.$$

Here, $\hat{U}'_j$'s are fixed unitary transformations that do not depend on inputs, and the (possibly) identical $\hat{\mathcal{O}}_h$'s are unitary transformations that correspond to an oracle. As in QaRO model, the $\hat{\mathsf{Alg}}_{\mathsf{Q}}$ is applied to an oracle-independent initial state, which gives an oracle-dependent final state. The computation ends with some measurement or observation of the final state.

5.2 Fully-quantum Security Notions

For the QRO model, the *computational-quantum indistinguishability under quantum ATK* (cqIND-qATK) is defined as follows:

Definition 5.1 (cqIND-qATK for Π_{qsym}). *For* $\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{CCA1}\}$*, a quantum symmetric encryption scheme* Π_{qsym} *is said to be cqIND-qATK secure if the advantage of any quantum probabilistic polynomial-time adversary* $\mathcal{A} = (\mathcal{A}_{\mathsf{M}}, \mathcal{A}_{\mathsf{D}})$*, where* $\mathcal{A}_{\mathsf{M}}$ *and* $\mathcal{A}_{\mathsf{D}}$ *are a message generator and a distinguisher, respectively, winning the game is negligible.*

$$\mathsf{Adv}^{\mathsf{cqIND-qATK}}_{\mathcal{A},\Pi_{\mathsf{qsym}}}(\lambda) := 2 \cdot \mathsf{Succ}^{\mathsf{cqIND-qATK}}_{\mathcal{A},\Pi_{\mathsf{qsym}}} - 1 = \mathsf{negl}(\lambda),$$

where $\mathsf{Succ}^{\mathsf{cqIND-qATK}}_{\mathcal{A},\Pi_{\mathsf{qsym}}}$ *is as follows:*

$$\Pr\Big[\mathsf{k} \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda); (\rho_{\mathsf{m}_0}, \rho_{\mathsf{m}_1}, \rho_{\mathsf{state}}) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_1}_{\mathsf{M}};$$
$$\mathsf{b} \xleftarrow{\$} \{0,1\}; \rho_{\mathsf{c}_\mathsf{b}} \xleftarrow{\$} \hat{\mathcal{O}}_{\mathsf{QEnc}_\mathsf{k}}(\rho_{\mathsf{m}_\mathsf{b}}); \textit{trace out } \rho_{\mathsf{m}_{1-\mathsf{b}}};$$
$$\mathsf{b}' \leftarrow \mathcal{A}^{\mathcal{O}_2}_{\mathsf{D}}(\rho_{\mathsf{c}_\mathsf{b}}, \rho_{\mathsf{state}}) : \mathsf{b}' = \mathsf{b}\Big] \quad \textit{for}$$

$$(\mathsf{ATK}, \mathcal{O}_1, \mathcal{O}_2) = \begin{cases} (\mathsf{CPA}, \hat{\mathcal{O}}_{\mathsf{QEnc}_\mathsf{k}}, \hat{\mathcal{O}}_{\mathsf{QEnc}_\mathsf{k}}) \\ (\mathsf{CCA1}, \{\hat{\mathcal{O}}_{\mathsf{QEnc}_\mathsf{k}}, \hat{\mathcal{O}}_{\mathsf{QDec}_\mathsf{k}}\}, \hat{\mathcal{O}}_{\mathsf{QEnc}_\mathsf{k}}). \end{cases}$$

The definitions of cqIND-qCPA and cqIND-qCCA1 were initially introduced in [Gag17, Definition 6.6] and [Gag17, Definition 6.10], respectively. The security notions for Π_{qasym} are defined similarly as in Definition 3.2. As already discussed in Section 4.2, cqIND-qCCA2 is not yet defined.

6 Concluding Remarks

The advent of quantum computers and algorithms has threatened the current cryptographic protocols. The cryptographic community has been motivated to establish new security notions and proof models against quantum adversaries ever since. In particular, we have reviewed previous approaches to extend the classical random oracle model to a quantum setting. Accordingly, we have introduced various indistinguishability notions under different attack models and the implication among them, as shown in Table 1. Defining (wqIND/qIND/cqIND)-qCCA2 that aptly captures the CCA2 scenario remains an open problem, and we leave it as future work.

Acknowledgements

This work was partly supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2017-0-00555, Towards Provable-secure Multi-party Authenticated Key Exchange Protocol based on Lattices in a Quantum World) and National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2015R1A2A2A01006812, Design and Security Analysis of Novel Lattice-based Fully Homomorphic Signatures Robust to Quantum Computing Attack).

References

[ABB+15] D. Augot, L. Batina, D. J. Bernstein, J. W. Bos, J. Buchmann, W. Castryck, O. Dunkelman, T. Güneysu, S. Gueron, A. Hülsing, T. Lange, M. S. E. Mohamed, C. Rechberger, P. Schwabe, N. Sendrier, F. Vercauteren, and B.-Y. Yang. Initial recommendations of long-term secure post-quantum systems. PQCRYPTO Post-Quantum Cryptography for Long-Term Security, September 2015. https://pqcrypto.eu.org/docs/initial-recommendations.pdf.

[BBC+98] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS 1998)*, Palo Alto, CA, USA, November 1998.

[BDF+11] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In *Proceedings of the 17th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2011)*, pages 41–69, Seoul, South Korea, December 2011.

[BDPR98] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *Proceedings of the 18th Annual International Cryptology Conference (Crypto 1998)*, pages 26–45, Santa Barbara, CA, USA, August 1998.

[BJ15] A. Broadbent and S. Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity, June 2015. https://arxiv.org/abs/1412.8766.

[BR93] M. Bellare and P. Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security (CCS 1993)*, pages 62–73, Fairfax, VA, USA, November 1993.

[BR00] P. O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits, March 2000. https://arxiv.org/abs/quant-ph/0003059.

[BZ13] D. Boneh and M. Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. Cryptology ePrint Archive, Report 2013/088, 2013. https://eprint.iacr.org/2013/088.

[CGH04] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. *Journal of the ACM*, 51(4):557–594, July 2004.

[CJL+16] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone. Report on post-quantum cryptography. National Institute of Standards and Technology Internal Report 8105, April 2016. http://dx.doi.org/10.6028/NIST.IR.8105.

[Deu85] D. E. Deutsch. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 400(1818):97–117, July 1985.

[Die82] D. Dieks. Communication by EPR devices. *Physics Letters A*, 92A(6):271–272, November 1982.

[Gag17] T. Gagliardoni. *Quantum security of cryptographic primitives.* PhD thesis, Technische Universität Darmstadt, February 2017.

[GC01] D. Gottesman and I. L. Chuang. Quantum digital signatures, May 2001. `https://arxiv.org/abs/quant-ph/0105032`.

[GHS16] T. Gagliardoni, A. Hülsing, and C. Schaffner. Semantic security and indistinguishability in the quantum world. In *Proceedings of the 36th Annual International Cryptology Conference (Crypto 2016)*, pages 60–89, Santa Barbara, CA, USA, August 2016.

[GM84] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC 1996)*, pages 212–219, Philadelphia, PA, USA, May 1996.

[Gro97] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79:325–328, July 1997.

[Hol73] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission*, 9(3):177–183, 1973.

[KKVB02] E. Kashefi, A. Kent, V. Vedral, and K. Banaszek. Comparison of quantum oracles. *Physical Review A*, 65:050304, May 2002.

[KLLNP16] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In *Proceedings of the 36th Annual International Cryptology Conference (Crypto 2016)*, pages 207–237, Santa Barbara, CA, USA, August 2016.

[KM15] N. Koblitz and A. J. Menezes. The random oracle model: a twenty-year retrospective. *Designs, Codes and Cryptography*, 77(2):587–610, December 2015.

[Lan61] R. W. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5(3):183–191, July 1961.

[Moo65] G. E. Moore. Cramming more components onto integrated circuits. *Electronics*, 38(8):114–117, April 1965.

[NY90] M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (STOC 1990)*, pages 427–437, Seattle, WA, USA, May 1990.

[RS91] C. Rackoff and D. R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Proceedings of the 11th Annual International Cryptology Conference (Crypto 1991)*, pages 433–444, Santa Barbara, CA, USA, August 1991.

[Sho94] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS 1994)*, pages 124–134, Santa Fe, NM, USA, November 1994.

[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[Sim94] D. R. Simon. On the power of quantum computation. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS 1994)*, pages 116–123, Santa Fe, NM, USA, November 1994.

[SLL16] T. Shang, Q. Lei, and J. Liu. Quantum random oracle model for quantum digital signature. *Physical Review A*, 94:042314, October 2016.

[SS16] T. Santoli and C. Schaffner. Using Simon's algorithm to attack symmetric-key cryptographic primitives, March 2016. `https://arxiv.org/abs/1603.07856`.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, October 1982.