Post-quantum Plaintext-awareness

Ehsan Ebrahimi[1,2] and Jeroen van Wier[2]

[1] Department of Computer Science, University of Luxembourg
ehsan.ebrahimi@uni.lu
[2] SnT, University of Luxembourg

18 July 2022

Abstract. In this paper, we formalize the plaintext-awareness notion in the superposition access model in which a quantum adversary may implement the encryption oracle in a quantum device and make superposition queries to the decryption oracle. Due to various possible ways an adversary can access the decryption oracles, we present six security definitions to capture the plaintext-awareness notion with respect to each way of access. We study the relationships between these definitions and present various implications and non-implications.
Classically, the strongest plaintext-awareness notion (PA2) accompanied by the indistinguishability under chosen-plaintext attack (IND-CPA) notion yields the indistinguishability under chosen-ciphertext attack (IND-CCA) notion. We show that the PA2 notion is not sufficient to show the above relation when targeting the IND-qCCA notion (Boneh-Zhandry definition, Crypto 2013). However, our proposed post-quantum PA2 notion with superposition decryption queries fulfils this implication.
Keywords. Plaintext-awareness, Post-quantum Security, Public-key Encryption

1 Introduction

Plaintext-awareness is the property of a public-key encryption scheme that guarantees the only way to feasibly create a ciphertext is using the encryption algorithm, similar to the unforgeability notion for symmetric-key schemes. This property guarantees that the creator of a ciphertext knows the corresponding plaintext, even without knowing the secret key. This becomes a powerful tool when constructing proofs of other security properties, as it effectively negates the need to provide the adversary with a decryption oracle. For example, plaintext-awareness allows us to boost security from IND-CPA to IND-CCA since the only difference between these security properties is the availability of a decryption oracle to the adversary. Plaintext-awareness is also a useful property in the setting of deniability, where one would often like a process between two parties to be simulatable by either party. Plaintext-awareness steps in here and guarantees that any ciphertext created in this simulation can be decrypted without the need of a secret key, as the plaintext is known by the ciphertext-creating party and can be extracted from the simulation. Lastly, plaintext-awareness can provide useful insight into why a scheme does or does not achieve a certain level of security. Clearly, it is a property that one would intuitively like to satisfy, as the natural way of creating ciphertexts is to use the encryption algorithm. When another way to craft ciphertext is available, i.e. when a scheme is not plaintext-aware, this might indicate a gap in security.

The plaintext-awareness notion was first introduced in the random oracle model by Bellare and Rogaway [4]. Vaguely speaking, their definition of plaintext-awareness implies the existence of an extractor algorithm which, given access to the random oracle queries, is able to decrypt any ciphertext outputted by the adversary. The main motivation to define this notion was to show the security of Optimal Asymmetric Encryption Padding (OAEP).

The definition in [4] does not take into account the possibility of eavesdropping the communication by the adversary. Subsequently in [2], a stronger definition of plaintext-awareness was introduced in the random oracle model. In [2], the adversary is able to eavesdrop some valid ciphertexts (through an oracle) and the extractor, given access to these ciphertexts and the random oracle queries made by the adversary, should be able to decrypt any ciphertext outputted by the adversary.

The first attempt to define a plaintext-awareness notion in the standard model was in [13], but, it needs to access a trusted third party. Later, Bellare and Palacio defined three levels of plaintext-awareness notions in the standard model (PA0, PA1, PA2) without the use of a third party [3]. In addition, they study the relations between these notions and IND-CCA notions.

The PA+1 notion, which lies between PA1 and PA2, was introduced by Dent [9]. Dent showed that an encryption scheme that is PA+1 and "simulatable" is PA2. Then he showed that the Cramer-Shoup encryption scheme is PA+1 and simulatable and therefore it satisfies the PA2 notion. This result is extended in the journal version [5]. A symmetric-key version of plaintext-awareness was considered in [1].

In this paper, we investigate the plaintext-awareness notion in the quantum setting. This includes adopting the plaintext-awareness notion to the superposition setting in which a quantum adversary is attacking a classical public-key encryption scheme.

1.1 Motivation

The plaintext-awareness notion is a strong security notion for public-key encryption schemes. It guarantees that the adversary is not able to generate a valid ciphertext without knowing the corresponding plaintext (called PA1). If we consider the possibility of eavesdropping the communication for the adversary, a stronger notion is considered. Namely, an adversary with the ability to eavesdrop on the communication is not able to generate a valid ciphertext without knowing the corresponding plaintext unless it obtains this ciphertext through eavesdropping (called PA2).

Since the advent of quantum algorithms that break some classical computational problems [19], there has been extensive research to construct post-quantum secure public-key encryption schemes[3]. This line of works varies from constructing public-key encryption schemes from quantum-hard assumptions [17,18] to considering stronger security notions for public-key encryption schemes [6]. (For instance, the IND-qCCA notion introduced in [6] in which a quantum adversary has superposition access to the decryption oracle.)

Traditionally, the PA2 plaintext-awareness notion, accompanied by the IND-CPA notion, is used to prove IND-CCA security. If we use public-key encryption schemes based on quantum-hard assumptions, we will get the same result in the presence of a quantum adversary as well (PA2 + IND-CPA implies IND-CCA in the presence of a quantum adversary). However, if one wants to achieve a stronger level of security (e.g. IND-qCCA security), the classical PA2 notion is not sufficient. In fact, we show that Classical PA2 + IND-qCPA does not imply IND-qCCA security (see Corollary 3.). Therefore, we need to formalize a stronger plaintext-awareness notion to achieve a security level of type IND-qCCA for public-key encryption schemes.

In addition, a post-quantum plaintext-awareness notion is used in a high-level manner in some existing security proofs in the literature without giving any formal treatment of the notion. For instance in [10], to show IND-qCCA security of plain OAEP transform in the quantum random oracle model, the adversary's inability in producing a valid ciphertext (without executing the encryption oracle or eavesdropping the communication) is crucial in the transition from Game 4 to Game 5 in their security proof. Note that this step will not hold with a classical PA2 notion since the adversary attacking in the sense of the IND-qCCA notion has superposition access to the decryption oracle. However, in the classical PA2 notion the adversary can only make classical decryption queries in order to generate a valid ciphertext. Formalizing a post-quantum plaintext-awareness notion will lead to more formal and accessible IND-qCCA security proofs. And currently, such a notion is not available in the literature.

And last but not least, a quantum adversary on input pk can implement the encryption oracle in his quantum device. So it is natural and necessary to investigate the effect of this stronger access to the encryption oracle on the plaintext-awareness notion. Currently, it is unknown if superposition access to the encryption oracle renders public-key encryption schemes not-plaintext-aware or it does not give a noticeable advantage to the ciphertext-creator adversary.

The overall conclusion is that formalizing and investigating the plaintext-awareness notion in the quantum setting seems a natural and necessary extension given the facts that: 1) a quantum adversary can have quantum access to the encryption oracle and the effect of this access to PA notions is unknown, 2) available plaintext-awareness notions are not sufficient to conclude stronger security notions like the IND-qCCA notion, 3) some post-quantum security proofs rely on post-quantum plaintext-awareness notions in a high-level argument without any formal definition for PA notions in the quantum setting, etc.

[3] Along with NIST competition to standardize the post-quantum public-key encryption schemes.

1.2 Challenges and Our Contribution

Intuitively, we say a scheme is (classically) plaintext-aware if for any (ciphertext-creator) adversary $\mathcal{A}$, there exists a (plaintext-extractor) algorithm $\mathcal{A}^*$ that, when given access to the "view" of $\mathcal{A}$, is able to answer the decryption queries outputted by $\mathcal{A}$.

In the quantum setting, a quantum adversary on input pk can implement the encryption oracle in its quantum device, or equivalently, the adversary can run the encryption oracle in superposition. At a first glance, it seems that the plaintext-awareness notion might not be possible to achieve when the adversary can execute the encryption oracle in superposition. Hypothetically, assume that an adversary $\mathcal{A}$ is able to access the encryption oracle by the "minimal-query model" [15], that is $|m\rangle \rightarrow |\mathrm{Enc}(m;r)\rangle$ (where r is a classical value chosen uniformly at random from the randomness space), without using any ancillary registers. In this model, the adversary is able to generate a valid ciphertext without knowing its corresponding plaintext. Namely, the adversary queries the uniform superposition of all messages, $\sum |m\rangle$, to get the superposition of corresponding ciphertexts, $\sum |\mathrm{Enc}(m;r)\rangle$. Now if the adversary measures the state $\sum |\mathrm{Enc}(m;r)\rangle$, the result is a random valid ciphertext for which the algorithm $\mathcal{A}^*$ might not be able to decrypt.

Even though the minimal query model has been studied in many works [15,11,7,12], it is not a canonical quantum access model. For private-key encryption schemes, the implementation of this query model requires some ancillary quantum registers and a decryption query. In the public-key setting, the query model can be implemented for some public-key encryption schemes without knowledge of the secret key but with access to an ancillary register containing the randomness needed for the encryption [12]. These encryption schemes called "recoverable public-key encryption schemes" in [12]. Note that this implementation of the minimal query model requires an ancillary register to store the randomness, that is, $|r, m\rangle \rightarrow |r, \mathrm{Enc}(m;r)\rangle$. Measuring the quantum state after the query fixes a randomness r and $c := \mathrm{Enc}(m;r)$ and using this randomness r, $\mathcal{A}^*$ is able to recover m from c, that is, the adversary knows the corresponding plaintext of c and the attack sketched above does not work for this implementation.

In this paper, we consider the "standard query model" and not the minimal query model to formulate superposition access to the encryption oracle. For any classical function f, the standard way to implement this function in a quantum computer is $\mathbb{U}_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$. So for an encryption oracle $\mathrm{Enc}_{\mathsf{pk}}$, we consider $\mathbb{U}_{\mathrm{Enc}_{\mathsf{pk}}} : |m, r, c\rangle \rightarrow |m, r, c \oplus \mathrm{Enc}_{\mathsf{pk}}(m;r)\rangle$. Clearly, this transformation is a unitary and an involution. In the above, we briefly discussed that available implementations of the minimal query model require some ancillary registers along with either a decryption query or access to the randomness register. Even though there is no implementation of the minimal query model without using ancillary registers ($|m\rangle \rightarrow |\mathrm{Enc}_{\mathsf{pk}}(m;r)\rangle$) and it might not be possible at all to implement the minimal query model without the use of ancillary registers (since a quantum operation is a unitary but the size of the ciphertext space is usually bigger than the size of the plaintext space and the operation $|m\rangle \to |\mathrm{Enc}_{\mathsf{pk}}(m;r)\rangle$ might not be a unitary), we give an argument below why it is not reasonable to consider the query model $|m\rangle \to |\mathrm{Enc}_{\mathsf{pk}}(m;r)\rangle$ to define plaintext-awareness notions.

Philosophical reasoning. Note that in the public-key setting, the encryption oracle can be implemented in the standard way, so any effort conducted by the adversary to implement the query model $|m\rangle \to |\mathrm{Enc}_{\mathsf{pk}}(m;r)\rangle$ instead of implementing the encryption oracle as a standard query might be considered an intentional effort to forget the corresponding plaintext that is encrypted. Considering it from a different angle, let us consider this classical scenario in which the classical adversary encrypts a message m to obtain the ciphertext $c := \mathrm{Enc}(m;r)$, then it permanently deletes m from its memory. Now, the adversary possesses a ciphertext c without knowing its corresponding plaintext. We argue that any effort by the adversary to implement the query model $|m\rangle \to |\mathrm{Enc}_{\mathsf{pk}}(m;r)\rangle$ lies in the "encrypt-then-forget" argument sketched above.

In addition, we need to propose a notion that captures the vague intuition that we established above: "a valid ciphertext that is not the output of a superposition execution of the encryption oracle". Note that a superposition query to the encryption oracle can contain an exponential number of ciphertexts and thus we cannot argue that the output of the adversary is not in this superposition of ciphertexts.

1.3 Our Contribution

In the superposition setting (when a classical public-key encryption scheme is attacked by a quantum adversary), we present various definitions. These definitions vary with respect to the following criteria:

- Number of decryption queries: one or many.
- Type of decryption queries: classical or quantum.
- Possibility of eavesdropping some ciphertexts.

Then, we study the relationship between these notions. Table 1 summarizes these notions and their relations with each other. In the abbreviation of notions, pq stands for post-quantum, $\mathsf{C_{dec}}$ stands for classical decryption queries, $\mathsf{Q_{dec}}$ stands for quantum decryption queries, PA0 is a notion with one decryption query and without the possibility of eavesdropping, PA1 is a notion with many decryption queries and without the possibility of eavesdropping and PA2 is a notion with many decryption queries and the possibility of eavesdropping. So for example, pqPA1-$\mathsf{Q_{dec}}$ is a notion in which the adversary is allowed to make many quantum decryption queries but is not allowed to eavesdrop ciphertexts.

Our notions are an adaptation of classical PA0, PA1, and PA2 notions in the standard model [3] to the quantum setting. Vaguely speaking, a public-key encryption scheme is plaintext-aware with respect to a class of adversaries if for any adversary $\mathcal{A}$ in the class, there exists a plaintext-extractor algorithm $\mathcal{A}^*$ that given access to the view of $\mathcal{A}$ is able to simulate the decryption algorithm without

	$\mathsf{pqPA2\text{-}Q_{dec}}$	$\mathsf{pqPA2\text{-}C_{dec}}$	$\mathsf{pqPA1\text{-}Q_{dec}}$	$\mathsf{pqPA1\text{-}C_{dec}}$	$\mathsf{pqPA0\text{-}Q_{dec}}$	$\mathsf{pqPA0\text{-}C_{dec}}$
$\mathsf{pqPA2\text{-}Q_{dec}}$		$\Rightarrow^{Theorem\ 1}$	$\Rightarrow^{Theorem\ 2}$	$\Rightarrow$	$\Rightarrow$	$\Rightarrow$
$\mathsf{pqPA2\text{-}C_{dec}}$	$\not\Rightarrow^{Theorem\ 4}$		$\Rightarrow$	$\Rightarrow^{Theorem\ 1}$	$\not\Rightarrow^{Corollary\ 2}$	$\Rightarrow$
$\mathsf{pqPA1\text{-}Q_{dec}}$	$\not\Rightarrow$	$\not\Rightarrow^{Theorem\ 5}$		$\Rightarrow^{Theorem\ 1}$	$\Rightarrow^{Theorem\ 3}$	$\Rightarrow$
$\mathsf{pqPA1\text{-}C_{dec}}$	$\not\Rightarrow$	$\not\Rightarrow$	$\not\Rightarrow^{Theorem\ 4}$		$\not\Rightarrow$	$\Rightarrow^{Theorem\ 3}$
$\mathsf{pqPA0\text{-}Q_{dec}}$	$\not\Rightarrow$	$\not\Rightarrow$	$\not\Rightarrow$	$\not\Rightarrow^{Theorem\ 6}$		$\Rightarrow^{Theorem\ 1}$
$\mathsf{pqPA0\text{-}C_{dec}}$	$\not\Rightarrow$	$\not\Rightarrow$	$\not\Rightarrow$	$\not\Rightarrow$	$\not\Rightarrow^{Corollary\ 1}$	

Table 1: Implications and separations between definitions. An arrow in row n, column m indicates whether n implies or does not imply m. The superscript number next to an arrow indicates the number of the corresponding theorem. Arrows without a superscript follow by transitivity.

using the secret key. Classically, given access to the view of $\mathcal{A}$ is formalized by given $\mathcal{A}^*$ the access to the coin tosses of $\mathcal{A}$. In our paper, the adversaries are QPT algorithms and are able to generate randomness by doing some quantum operations. For instance, applying Hadamard to $|0\rangle$ and measuring the result in the computational basis gives a random bit. To formalize our notions, we give $\mathcal{A}^*$ the access to the internal quantum registers of $\mathcal{A}$.

For instance, we say a public-key encryption scheme is $\mathsf{pqPA1\text{-}Q_{dec}}$ if for any QPT ciphertext-creator adversary $\mathcal{A}$ that makes quantum queries to the decryption oracle, there exists a QPT plaintext-extractor algorithm $\mathcal{A}^*$ that given access to the internal registers of $\mathcal{A}$ can simulate the decryption queries. In more detail, the execution of $\mathcal{A}$ querying the decryption oracle is indistinguishable from the execution of $\mathcal{A}$ querying $\mathcal{A}^*$ for any QPT distinguisher $\mathcal{D}$.

For PA2 notions, the possibility of eavesdropping the communication is given to $\mathcal{A}$ by classical access to a randomized algorithm $\mathcal{P}$ (called a plaintext-creator) that upon receiving a query from $\mathcal{A}$ generates a message, encrypts it and sends the ciphertext to $\mathcal{A}$. (Since in the post-quantum setting the honest parties use the classical public-key encryption schemes to communicate, we do not consider the possibility of eavesdropping a superposition of ciphertexts in this paper.) Note that $\mathcal{A}^*$ does not have any access to the internal quantum registers of $\mathcal{P}$, so it might not be able to decrypt a ciphertext obtained from $\mathcal{P}$. The list of these ciphertexts is given to both the decryption oracle and $\mathcal{A}^*$ to return $\perp$ when one of these ciphertexts is submitted as a decryption query.

1.4 Organization

We present some preliminaries in Section 2. In Section 3, we define six possible definitions for the plaintext-awareness notion in the post-quantum setting. Section 4 discusses the relationships between notions. Finally, we discuss the achievability of our notions in Section 5.

2 Preliminaries

Any classical function $f : X \to Y$ can be implemented as a unitary operator $\mathbb{U}_f$ in a quantum computer where $\mathbb{U}_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$ and it is clear that

$\mathbb{U}_f^\dagger = \mathbb{U}_f$. A quantum adversary has standard oracle access to a classical function f if it can query the unitary $\mathbb{U}_f$. In the following (Section 2.1), we present a short introduction to quantum computing. We refer to the class of quantum polynomial-time algorithms as QPT.

2.1 Basics of Quantum Computing

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

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

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

For two quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$, the composition of them is defined by the tensor product and it is $\mathcal{H}_1 \otimes \mathcal{H}_2$. For two unitary $\mathbb{U}_1$ and $\mathbb{U}_2$ defined over $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively, $(\mathbb{U}_1 \otimes \mathbb{U}_2)(\mathcal{H}_1 \otimes \mathcal{H}_2) = \mathbb{U}_1(\mathcal{H}_1) \otimes \mathbb{U}_2(\mathcal{H}_2)$.

2.2 Definitions

We define a strong quantum-secure pseudo-random permutation as a permutation that is indistinguishable from a random permutation when the quantum adversary has superposition access to the permutation and its inverse.

Definition 1. *We say a permutation P a strong quantum-secure pseudo-random permutation if for any* QPT *adversary $\mathcal{A}$,*

$$|\Pr[b = 1 : b \leftarrow \mathcal{A}^{\mathbb{U}_P, \mathbb{U}_{P^{-1}}}] - \Pr[b = 1 : b \leftarrow \mathcal{A}^{\mathbb{U}_\pi, \mathbb{U}_{\pi^{-1}}}]| \leq neg(\eta),$$

where π is a truly random permutation and η is the security parameter.

We define a public-key encryption scheme in the following.

Definition 2. *A public-key encryption scheme Π consists of three polynomial time (in the security parameter η) algorithms,* $(\mathrm{KGen}, \mathrm{Enc}, \mathrm{Dec})$*, such that:*

1. KGen*, the key generation algorithm, is a probabilistic algorithm which on input* 1^η *outputs a pair of keys,* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta)$*, called the public key and the secret key for the encryption scheme, respectively.*
2. Enc*, the encryption algorithm, is a probabilistic algorithm which takes as input a public key* pk *and a message m from the message space and outputs a ciphertext* $c \leftarrow \mathrm{Enc}_{\mathsf{pk}}(m)$*. We may specify the randomness r that is used for computing c and write* $c = \mathrm{Enc}_{\mathsf{pk}}(m; r)$*.*
3. Dec*, the decryption algorithm, is a deterministic algorithm that takes as input a secret key* sk *and a ciphertext c and returns the message* $m := \mathrm{Dec}_{\mathsf{sk}}(c)$*. It is required that the decryption algorithm returns the original message, i.e.,* $\mathrm{Dec}_{\mathsf{sk}}(\mathrm{Enc}_{\mathsf{pk}}(m)) = m$*, for every* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta)$ *and every m. The algorithm* Dec *returns $\perp$ if ciphertext c is not decryptable.*

We define a one-way public-key encryption scheme below. This is the minimal security requirement for an encryption scheme. This is needed for separation theorems between PA notions to exclude trivial encryption schemes, for example the identity encryption scheme that is defined as $\mathrm{Enc}_{\mathsf{pk}}(m) = m$, which are plaintext-aware with respect to any reasonable definition.

Definition 3. *We say a public-key encryption scheme* $\Pi = (\mathrm{KGen}, \mathrm{Enc}, \mathrm{Dec})$ *is one-way if for any* QPT *adversary* $\mathcal{A}$

$$\Pr[\mathcal{A}(\mathsf{pk}, c) = m : (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta), m \overset{\$}{\leftarrow} M, c \leftarrow \mathrm{Enc}_{\mathsf{pk}}(m)] \leq neg(\eta),$$

where M is the message space.

IND-qCPA and IND-qCCA. Here, we define a quantum IND-CPA and quantum IND-CCA notion used in this paper. Note that a quantum adversary can implement a public-key encryption algorithm in its quantum device since pk is public. To define IND-qCPA and IND-qCCA notions, we need to determine whether the challenge queries and decryption queries are classical or quantum. There are many quantum IND-CPA notions available in the literature [7] that include definitions with classical challenge queries and quantum challenge queries, on the other hand, there is only one definite quantum IND-CCA notion (called IND-qCCA) available in the literature that only allows classical challenge queries [6][4]. Therefore, we only present the weakest quantum IND-CPA notion which, accompanied by our quantum PA2 notion, implies the IND-qCCA notion. We follow the definitions proposed in [6] by Boneh and Zhandry in this paper.

[4] There are some research works to define a quantum IND-CCA notion with quantum challenge queries (for instance [8,12]), however, a definite definition is not available in the literature so far.

Definition 4. *We say an encryption scheme* Enc *is IND-qCPA secure if the following two games are indistinguishable for any* QPT *adversary* $\mathcal{X}$*.*

Game 0: $G^{qCPA}_{\mathcal{X},0}$

$$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta), \qquad m_0, m_1 \leftarrow \mathcal{X}(\mathsf{pk}),$$
$$\mathrm{Enc}(m_0;r_0) \leftarrow \mathit{Challenger}(m_0,m_1),\ b \leftarrow \mathcal{X}(\mathsf{pk}, \mathrm{Enc}(m_0;r_0))$$

Game 1: $G^{qCPA}_{\mathcal{X},1}$

$$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta), \qquad m_0, m_1 \leftarrow \mathcal{X}(\mathsf{pk}),$$
$$\mathrm{Enc}(m_1;r_1) \leftarrow \mathit{Challenger}(m_0,m_1),\ b \leftarrow \mathcal{X}(\mathsf{pk}, \mathrm{Enc}(m_1;r_1))$$

In other words, $|\Pr[G^{qCPA}_{\mathcal{X},0} = 1] - \Pr[G^{qCPA}_{\mathcal{X},1} = 1]| \leq neg(\eta)$ *for any* QPT *adversary* $\mathcal{X}$*.*

IND-qCCA. Here, a quantum adversary can query the encryption and decryption oracle on superposition of inputs but the challenge queries are classical. Let **List** be the list of ciphertexts obtained during the challenge phase. We say **List** is defined if at least one challenge query has been executed. We define a decryption algorithm $\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}$ as follows:

$$\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}(c) = \begin{cases} \perp & \text{if } \mathbf{List} \text{ is defined and } c \in \mathbf{List} \\ \mathrm{Dec}_{\mathsf{sk}}(c) & \text{otherwise} \end{cases}.$$

Definition 5. *We say an encryption scheme* Enc *is IND-qCCA secure if the following two games are indistinguishable for any* QPT *adversary* $\mathcal{X}$*.*

Game 0: $G^{qCCA}_{\mathcal{X},0}$

$$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta), \qquad m_0, m_1 \leftarrow \mathcal{X}^{\mathbb{U}_{\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}}(\mathsf{pk}),$$
$$\mathrm{Enc}(m_0;r_0) \leftarrow \mathit{Challenger}(m_0,m_1),\ b \leftarrow \mathcal{X}^{\mathbb{U}_{\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}}(\mathsf{pk}, \mathrm{Enc}(m_0;r_0))$$

Game 1: $G^{qCCA}_{\mathcal{X},1}$

$$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta), \qquad m_0, m_1 \leftarrow \mathcal{X}^{\mathbb{U}_{\mathrm{Dec}_{\mathsf{sk}}}}(\mathsf{pk}),$$
$$\mathrm{Enc}(m_1;r_1) \leftarrow \mathit{Challenger}(m_0,m_1),\ b \leftarrow \mathcal{X}^{\mathbb{U}_{\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}}(\mathsf{pk}, \mathrm{Enc}(m_1;r_1))$$

In other words, $|\Pr[G^{qCCA}_{\mathcal{X},0} = 1] - \Pr[G^{qCCA}_{\mathcal{X},1}]| \leq neg(\eta)$ *for any* QPT *adversary* $\mathcal{X}$*.*

Commitment Scheme. In the following, we define a commitment scheme.

Definition 6 (Commitment Scheme). *A commitment scheme consists of three polynomial algorithms* Gen*,* Com *and* Ver *described below.*

- *The key generating algorithm* Gen *that on the input of the security parameter* 1^n *returns a public-key* pk_{com}*.*

- *The commitment algorithm* Com *on the inputs* pk_{com} *and a message* m *chooses a randomness* r *and returns* $c := \mathrm{Com}(\mathsf{pk}_{com}, m; r)$ *and the corresponding opening information* ω*.*
- *The verification algorithm* Ver *on the inputs* pk_{com}*,* c*,* ω *and* m*, either accepts (*$b = 1$*) or rejects (*$b = 0$*).*

The scheme has the correctness property, that is, the verification algorithm returns 1 *with the probability* 1 *if* c, ω *are the output of* Com*:*

$$\Pr[b = 1 : \mathsf{pk}_{com} \leftarrow \mathrm{Gen}(1^n), (c, \omega) \leftarrow \mathrm{Com}(\mathsf{pk}_{com}, m), b \leftarrow \mathrm{Ver}(\mathsf{pk}_{com}, c, \omega, m)] = 1.$$

We define hiding and binding properties of a commitment scheme against a QPT adversary.

Definition 7. *We say a commitment scheme* $(\mathrm{Gen}(1^n), \mathrm{Com}, \mathrm{Ver})$ *is computationally hiding if for any* $\mathsf{pk}_{com} \leftarrow \mathrm{Gen}(1^n)$*, for any two messages* m_1, m_2 *and for any* QPT *distinguisher* $\mathcal{D}$

$$|\Pr[\mathcal{D}(\mathsf{pk}_{com}, c_1) = 1 : (c_1, \omega_1) \leftarrow \mathrm{Com}_{\mathsf{pk}_{com}}(m_1)] - \Pr[\mathcal{D}(\mathsf{pk}_{com}, c_2) = 1 : (c_2, \omega_2) \leftarrow \mathrm{Com}_{\mathsf{pk}_{com}}(m_2)]| \leq \mathtt{neg}(n).$$

Definition 8. *A commitment scheme* $(\mathrm{Gen}(1^n), \mathrm{Com}, \mathrm{Ver})$ *is computationally binding if for any commitment* c*, and any* QPT *adversary* $\mathcal{A}$

$$|\Pr[\mathrm{Ver}(\mathsf{pk}_{com}, c, m_1, \omega_1) = 1 \wedge \mathrm{Ver}(\mathsf{pk}_{com}, c, m_2, \omega_2) = 1 \wedge m_1 \neq m_2 : \mathsf{pk}_{com} \leftarrow \mathrm{Gen}(1^n), (m_1, \omega_1, m_2, \omega_2) \leftarrow \mathcal{A}(c, \mathsf{pk}_{com})]| \leq \mathtt{neg}(n).$$

Note that these properties are achievable, for instance, the commitment scheme in [14] fulfills these properties.

3 Post-quantum Plaintext-awareness

In this section, we define plaintext-awareness for classical encryption schemes in the presence of a quantum adversary. Let Q_{int} indicate the internal registers of the ciphertext-creator adversary $\mathcal{A}$. Note that Q_{int} includes the input, output and some ancillary registers of $\mathcal{A}$.

3.1 Post-quantum PA0, PA1

There are two possible cases to define PA0 and PA1. Namely, either $\mathcal{A}$'s goal is to output a classical ciphertext without knowing its corresponding plaintext or its goal is to output a superposition of ciphertexts where the corresponding quantum plaintext is unknown to $\mathcal{A}$. In the formulation of these two possible cases, the access to the decryption oracle will differ. Namely, either the adversary $\mathcal{A}$ has classical access to the decryption oracle or it has superposition access to the decryption oracle. In other words, to say that $\mathcal{A}$ is not able to output a valid

classical (quantum) ciphertext unless it executes the encryption algorithm, there should be an algorithm $\mathcal{A}^*$ that can respond to classical (quantum) decryption queries given the internal registers of $\mathcal{A}$. That is, any valid ciphertext known to $\mathcal{A}$ can be decrypted if $\mathcal{A}^*$ has access to the internal register of $\mathcal{A}$.
Classical decryption queries We define the definition using two games. In the real game, $\mathcal{A}$ given pk has access to the decryption oracle. In the fake game, the decryption queries will be answered with an algorithm $\mathcal{A}^*$ that has access to the internal register of $\mathcal{A}$. In both games, $\mathcal{A}$ outputs a quantum state in the end. We say a public-key encryption scheme is plaintext-aware if for any QPT adversary $\mathcal{A}$, there exists a QPT algorithm $\mathcal{A}^*$ such that the output of these two games is indistinguishable for any QPT distinguisher $\mathcal{D}$. Without loss of generality, we assume that the output of $\mathcal{D}$ is determined with a computational basis measurement. This computational indistinguishability definition for quantum states is common in the literature, for instance in Definition 1 in [16].

Game $G_{real}^{\mathsf{pqPA1\text{-}C_{dec}}}$. In this game, the ciphertext-creator adversary $\mathcal{A}$ given pk has classical access to the decryption oracle. At the end, $\mathcal{A}$ outputs a quantum state.

Game $G_{real}^{\mathsf{pqPA1\text{-}C_{dec}}}$

$$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta),\ \rho_\eta \leftarrow \mathcal{A}^{\mathrm{Dec}_{\mathsf{sk}}}(\mathsf{pk})$$

Game $G_{fake}^{\mathsf{pqPA1\text{-}C_{dec}}}$. In this game, $\mathcal{A}$'s decryption queries will be responded by a plaintext-extractor algorithm $\mathcal{A}^*$. Here, $\mathcal{A}^*$ has access to pk and the internal register of $\mathcal{A}$. At the end, $\mathcal{A}$ outputs a quantum state.

Game $G_{fake}^{\mathsf{pqPA1\text{-}C_{dec}}}$

$$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta),\ \rho_\eta \leftarrow \mathcal{A}^{\mathcal{A}^*(\mathsf{pk},\mathrm{Q}_{int})}(\mathsf{pk})$$

Definition 9 ($\mathsf{pqPA1\text{-}C_{dec}}$)**.** *We say a public-key encryption scheme* Enc *is* $\mathsf{pqPA1\text{-}C_{dec}}$ *plaintext-aware if for any* QPT *ciphertext-creator* $\mathcal{A}$*, there exists a* QPT *plaintext-extractor* $\mathcal{A}^*$ *such that for all* QPT *distinguishing algorithms* $\mathcal{D}$*, the advantage of* $\mathcal{D}$ *in distinguishing* $G_{real}^{\mathsf{pqPA1\text{-}C_{dec}}}$ *and* $G_{fake}^{\mathsf{pqPA1\text{-}C_{dec}}}$ *is negligible as a function of the security parameter:*

$$\begin{aligned}\mathbf{Adv}_{\mathcal{D},\mathcal{A}} = |\Pr[\mathcal{D}(\rho_\eta) = 1 : \rho_\eta \leftarrow G_{real}^{\mathsf{pqPA1\text{-}C_{dec}}}]-&\\ \Pr[\mathcal{D}(\rho_\eta) = 1 : \rho_\eta \leftarrow G_{fake}^{\mathsf{pqPA1\text{-}C_{dec}}}]| &\leq neg(\eta),\end{aligned}$$

where the output of $\mathcal{D}$ *is determined with the computational basis measurement.*

Definition 10 ($\mathsf{pqPA0\text{-}C_{dec}}$)**.** *This is defined similarly to* $\mathsf{pqPA1\text{-}C_{dec}}$ *except the adversary* $\mathcal{A}$ *is allowed to make only one decryption query.*

Superposition decryption queries. In this subsection, we define plaintext-awareness definition when the adversary $\mathcal{A}$ has superposition access to the decryption oracle. Similar to the above definition, we define this notion using two games.

Game $G_{real}^{\mathsf{pqPA1\text{-}Q_{dec}}}$. In this game, the ciphertext-creator adversary $\mathcal{A}$ given pk has quantum access to the decryption oracle. At the end, $\mathcal{A}$ outputs a quantum state.

```
Game $G_{real}^{\mathsf{pqPA1\text{-}Q_{dec}}}$
    $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{KGen}(1^{\eta}),\ \rho_{\eta} \leftarrow \mathcal{A}^{\mathbb{U}_{\mathrm{Dec}_{\mathsf{sk}}}}(\mathsf{pk})$
```

Game $G_{fake}^{\mathsf{pqPA1\text{-}Q_{dec}}}$. In this game, $\mathcal{A}$'s quantum decryption queries will be responded by a plaintext-extractor algorithm $\mathcal{A}^*$. Here, $\mathcal{A}^*$ has access to pk and the internal register of $\mathcal{A}$. At the end, $\mathcal{A}$ outputs a quantum state.

```
Game $G_{fake}^{\mathsf{pqPA1\text{-}Q_{dec}}}$
    $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{KGen}(1^{\eta}),\ \rho_{\eta} \leftarrow \mathcal{A}^{\mathcal{A}^*(\mathsf{pk}, \mathsf{Q}_{int})}(\mathsf{pk})$
```

Definition 11 ($\mathsf{pqPA1\text{-}Q_{dec}}$)**.** *We say a public-key encryption scheme* Enc *is* $\mathsf{pqPA1\text{-}Q_{dec}}$ *plaintext-aware if for any* QPT *ciphertext-creator* $\mathcal{A}$*, there exists a* QPT *plaintext-extractor* $\mathcal{A}^*$ *such that for all* QPT *distinguishing algorithms* $\mathcal{D}$*, the advantage of* $\mathcal{D}$ *in distinguishing* $G_{real}^{\mathsf{pqPA1\text{-}Q_{dec}}}$ *and* $G_{fake}^{\mathsf{pqPA1\text{-}Q_{dec}}}$ *is negligible as a function of the security parameter:*

$$\begin{aligned}\mathbf{Adv}_{\mathcal{D},\mathcal{A}} = |\Pr[\mathcal{D}(\rho_{\eta}) = 1 : \rho_{\eta} \leftarrow G_{real}^{\mathsf{pqPA1\text{-}Q_{dec}}}] - \\ \Pr[\mathcal{D}(\rho_{\eta}) = 1 : \rho_{\eta} \leftarrow G_{fake}^{\mathsf{pqPA1\text{-}Q_{dec}}}]| \le neg(\eta),\end{aligned}$$

where the output of $\mathcal{D}$ *is determined with the computational basis measurement.*

Definition 12 ($\mathsf{pqPA0\text{-}Q_{dec}}$)**.** *This is defined similarly to* $\mathsf{pqPA1\text{-}Q_{dec}}$ *except the adversary* $\mathcal{A}$ *is allowed to make only one decryption query.*

3.2 Post-quantum PA2

In $\mathsf{pqPA0}$ and $\mathsf{pqPA1}$ definitions, it has not been considered that the adversary may be able to eavesdrop some ciphertexts and use them to generate new ciphertexts without knowing their corresponding plaintexts. There are two scenarios for the eavesdropping:

- The adversary may eavesdrop some classical ciphertexts.
- The adversary may obtain some superposition of ciphertexts.

Note that in the post-quantum setting, the honest parties are using their classical devices to communicate. So the assumption that the adversary may be able to eavesdrop some superposition of ciphertexts seems too exotic and we do not analyse it in this paper. We provide a short discussion on the main obstacle in defining a plaintext-awareness definition with the superposition eavesdropping in Appendix A.

The possibility for eavesdropping is granted to the adversary by a randomized algorithm $\mathcal{P}$ (called the plaintext-creator). Here, $\mathcal{P}$ upon receiving a query from $\mathcal{A}$ outputs the encryption of a message of its choosing to $\mathcal{A}$. Additionally, $\mathcal{P}$ adds m and its corresponding ciphertext to a **List**.

Similar to $\mathsf{pqPA0}$ and $\mathsf{pqPA1}$, we consider two possible goals for the adversary $\mathcal{A}$: outputting a classical ciphertext without knowing its corresponding plaintext or a superposition of ciphertexts without knowing its corresponding superposition of plaintexts.

Recall that $\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}$ is defined as:

$$\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}(c) = \begin{cases} \bot & \text{if } \mathbf{List} \text{ is defined and } c \in \mathbf{List} \\ \mathrm{Dec}_{\mathsf{sk}}(c) & \text{otherwise} \end{cases}.$$

Classical decryption queries. In this subsection, we define plaintext-awareness when the adversary $\mathcal{A}$ has classical access to a plaintext creator algorithm $\mathcal{P}$ and the decryption oracle $\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}$. Similarly, we define the notion using two games.

Game $G_{real}^{\mathsf{pqPA2\text{-}C_{dec}}}$. In this game, the ciphertext-creator adversary $\mathcal{A}$ given pk has oracle access to $\mathcal{P}$. It has classical access to the decryption oracle $\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}$. At the end, $\mathcal{A}$ outputs a quantum state.

Game $G_{real}^{\mathsf{pqPA2\text{-}C_{dec}}}$

$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta)$, $\rho_\eta \leftarrow \mathcal{A}^{\mathcal{P},\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}(\mathsf{pk})$

Game $G_{fake}^{\mathsf{pqPA2\text{-}C_{dec}}}$. In this game, $\mathcal{A}$'s decryption queries will be responded by a plaintext-extractor algorithm $\mathcal{A}^*$. Here, $\mathcal{A}^*$ given pk has access to **List** and the internal register of $\mathcal{A}$. At the end, $\mathcal{A}$ outputs a quantum state.

Game $G_{fake}^{\mathsf{pqPA2\text{-}C_{dec}}}$

$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta)$, $\rho_\eta \leftarrow \mathcal{A}^{\mathcal{P},\mathcal{A}^*(\mathsf{pk},\mathbf{List},\mathrm{Q}_{int})}(\mathsf{pk})$

Definition 13 ($\mathsf{pqPA2\text{-}C_{dec}}$). *We say a public-key encryption scheme* Enc *is* $\mathsf{pqPA2\text{-}C_{dec}}$ *plaintext-aware if for any* QPT *ciphertext-creator* $\mathcal{A}$*, there exists a* QPT *plaintext-extractor* $\mathcal{A}^*$ *such that for any* QPT *plaintext-creator* $\mathcal{P}$ *and any* QPT *distinguishing algorithms* $\mathcal{D}$*, the advantage of* $\mathcal{D}$ *in distinguishing* $G_{real}^{\mathsf{pqPA2\text{-}C_{dec}}}$ *and* $G_{fake}^{\mathsf{pqPA2\text{-}C_{dec}}}$ *is negligible as a function of the security parameter:*

$$\mathbf{Adv}_{\mathcal{D},\mathcal{A}} = |\Pr[\mathcal{D}(\rho_\eta) = 1 : \rho_\eta \leftarrow G_{real}^{\mathsf{pqPA2\text{-}C_{dec}}}] - \Pr[\mathcal{D}(\rho_\eta) = 1 : \rho_\eta \leftarrow G_{fake}^{\mathsf{pqPA2\text{-}C_{dec}}}]| \leq neg(\eta),$$

where the output of $\mathcal{D}$ *is determined with the computational basis measurement.*

Superposition decryption queries. In this subsection, we define plaintext-awareness when the adversary $\mathcal{A}$ has classical access to a plaintext creator algorithm $\mathcal{P}$ and superposition access to the decryption oracle $\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}$. Similarly, we define the notion using two games.

Game $G_{real}^{\mathsf{pqPA2\text{-}Q_{dec}}}$. In this game, the ciphertext-creator adversary $\mathcal{A}$ given pk has oracle access to $\mathcal{P}$ and superposition access to the decryption oracle. At the end, $\mathcal{A}$ outputs a quantum state.

```
Game $G_{real}^{\mathsf{pqPA2\text{-}Q_{dec}}}$
    $(\mathsf{pk},\mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta)$, $\rho_\eta \leftarrow \mathcal{A}^{\mathcal{P},\mathbb{U}_{\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}}(\mathsf{pk})$
```

Game $G_{fake}^{\mathsf{pqPA2\text{-}Q_{dec}}}$. In this game, $\mathcal{A}$'s decryption queries will be responded by a plaintext-extractor algorithm $\mathcal{A}^*$. Here, $\mathcal{A}^*$ given pk has access to **List** and the internal register of $\mathcal{A}$. At the end, $\mathcal{A}$ outputs a quantum state.

```
Game $G_{fake}^{\mathsf{pqPA2\text{-}Q_{dec}}}$
    $(\mathsf{pk},\mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta)$, $\rho_\eta \leftarrow \mathcal{A}^{\mathcal{P},\mathcal{A}^*(\mathsf{pk},\mathbf{List},\mathrm{Q}_{int})}(\mathsf{pk})$
```

Definition 14 ($\mathsf{pqPA2\text{-}Q_{dec}}$). *We say a public-key encryption scheme* Enc *is* $\mathsf{pqPA2\text{-}Q_{dec}}$ *plaintext-aware if for any* QPT *ciphertext-creator* $\mathcal{A}$*, there exists a* QPT *plaintext-extractor* $\mathcal{A}^*$ *such that that for any* QPT *plaintext-extractor* $\mathcal{P}$ *and any* QPT *distinguishing algorithms* $\mathcal{D}$*, the advantage of* $\mathcal{D}$ *in distinguishing* $G_{real}^{\mathsf{pqPA2\text{-}Q_{dec}}}$ *and* $G_{fake}^{\mathsf{pqPA2\text{-}Q_{dec}}}$ *is negligible as a function of the security parameter:*

$$\mathbf{Adv}_{\mathcal{D},\mathcal{A}} = |\Pr[\mathcal{D}(\rho_\eta) = 1 : \rho_\eta \leftarrow G_{real}^{\mathsf{pqPA2\text{-}Q_{dec}}}] - \Pr[\mathcal{D}(\rho_\eta) = 1 : \rho_\eta \leftarrow G_{fake}^{\mathsf{pqPA2\text{-}Q_{dec}}}]| \leq neg(\eta),$$

where the output of $\mathcal{D}$ *is determined with the computational basis measurement.*

4 Relationships Between Notions

In this section, we study the relations between different PA notions defined in this paper. In addition, we show that the $\mathsf{pqPA2\text{-}Q_{dec}}$ plaintext-awareness notion defined in this paper along with IND-qCPA security implies IND-qCCA security.

4.1 Relationships between PA notions

Implications. First we show implications between the notions. Clearly, $\mathsf{pqPA}i\text{-}\mathsf{Q_{dec}}$ plaintext-awareness implies $\mathsf{pqPA}i\text{-}\mathsf{C_{dec}}$ plaintext-awareness for $i = 0, 1, 2$. The reason is the existence of a plaintext-extractor algorithm $\mathcal{A}^*$ for an adversary $\mathcal{A}$ that makes superposition queries to the decryption oracle is enough to prove $\mathsf{pqPA}i\text{-}\mathsf{C_{dec}}$ plaintext-awareness. In other words, the algorithm $\mathcal{A}^*$ is a plaintext extractor for an adversary attacking in the sense of $\mathsf{pqPA}i\text{-}\mathsf{C_{dec}}$.

Theorem 1. *For any* $i = 0, 1, 2$*, a public-key encryption scheme* Enc *that is* $\mathsf{pqPA}i\text{-}\mathsf{Q_{dec}}$ *plaintext-aware, it is* $\mathsf{pqPA}i\text{-}\mathsf{C_{dec}}$ *plaintext-aware.*

Below, we investigate the relations between PAi notions for different i.

Theorem 2. *If an encryption scheme is* $\mathsf{pqPA2}$-Qu *aware then it is* $\mathsf{pqPA1}$-Qu *aware when* $Qu \in \{\mathsf{C_{dec}}, \mathsf{Q_{dec}}\}$.

Proof. The proof is straightforward because an adversary $\mathcal{A}$ that breaks $\mathsf{pqPA1}$-Qu awareness can be run to break $\mathsf{pqPA2}$-Qu awareness. In more detail, the reduction adversary $\mathcal{B}$ runs $\mathcal{A}$ and simulates $\mathcal{A}$'s decryption queries using its decryption oracle. (Note that the reduction adversary $\mathcal{B}$ does not use the possibility of querying the plaintext-creator and breaks the $\mathsf{pqPA2}$-Qu awareness notion.) □

Theorem 3. *If an encryption scheme is* $\mathsf{pqPA1}$-Qu *aware then it is* $\mathsf{pqPA0}$-Qu *aware when* $Qu \in \{\mathsf{C_{dec}}, \mathsf{Q_{dec}}\}$.

Proof. The proof is obvious since the only difference between $PA1$ and $PA0$ notions are the number of decryption queries, which is polynomially many queries and one query, respectively. □

Non-implications. The rest of this subsection shows non-implications (i.e. separations) between notions. Note that in order to exclude the trivial encryption schemes that are plaintext-aware with respect to all definitions (for instance, the identity encryption), we add a security requirement (one-wayness or IND-qCPA security) for encryption in the separation theorems.

Below, we show that $\mathsf{pqPA}i$-$\mathsf{Q_{dec}}$ is strictly stronger than $\mathsf{pqPA}i$-$\mathsf{C_{dec}}$ for $i = 1, 2$. The high-level idea is to take an encryption scheme that is $\mathsf{pqPA}i$-$\mathsf{C_{dec}}$ plaintext-aware and modifies its decryption algorithm in a way that remains $\mathsf{pqPA}i$-$\mathsf{C_{dec}}$ plaintext-aware but it leaks a valid ciphertext to the $\mathsf{pqPA}i$-$\mathsf{Q_{dec}}$ adversary.

Theorem 4. *A one-way* $\mathsf{pqPA}i$-$\mathsf{C_{dec}}$ *plaintext-aware public-key encryption scheme is not necessarily* $\mathsf{pqPA}i$-$\mathsf{Q_{dec}}$ *plaintext-aware for* $i = 1, 2$.

Proof. Let $\mathit{\Pi} = (\mathrm{KGen}, \mathrm{Enc}, \mathrm{Dec})$ be a public-key encryption scheme that is $\mathsf{pqPA}i$-$\mathsf{C_{dec}}$ plaintext-aware. Let $\{0,1\}^n$ be the ciphertext space of $\mathit{\Pi}$. Let the ciphertext c_v be generated by choosing a random message m and a randomness r and computing $\mathrm{Enc}(m;r)$. We modify $\mathit{\Pi}$ to a new encryption scheme $\mathit{\Pi}' = (\mathrm{KGen}', \mathrm{Enc}', \mathrm{Dec}')$. The algorithm KGen' runs KGen to get $(\mathsf{pk}, \mathsf{sk})$, it outputs a key pk_{com} for a computationally hiding and binding commitment scheme $(\mathrm{Com}, \mathrm{Ver})$, and it chooses a random periodic function f on c_v. (That is for any $x \in \{0,1\}^n$, $f(x \oplus c_v) = f(x)$.) It returns the pair $(\mathsf{pk}', \mathsf{sk}') = ((\mathsf{pk}, \mathsf{pk}_{com}), (\mathsf{sk}, f))$ and the commitment value $c_{com} = \mathrm{Com}(\mathsf{pk}_{com}, c_v)$ with the corresponding opening ω. For any message m in the message-space of $\mathit{\Pi}$, $\mathrm{Enc}'_{\mathsf{pk}'}(m) = \mathrm{Enc}_{\mathsf{pk}}(m) || \perp$. The new decryption algorithm $\mathrm{Dec}'_{(\mathsf{sk},f)}$ takes as input a ciphertext from $(\{0,1\}^n \cup \perp) \times (\{0,1\}^n \cup \perp)$ and operates as the following:

$$\mathrm{Dec}'_{(\mathsf{sk},f,r)}(c_1, c_2) = \begin{cases} \mathrm{Dec}_{\mathsf{sk}}(c_1) & \text{if } c_1 \neq \perp \text{ and } c_2 = \perp \\ \mathrm{Dec}_{\mathsf{sk}}(c_v) \| r \| \omega & \text{if } c_1 = \perp \text{ and } c_2 = c_v \\ \perp & \text{if } c_1 = \perp \text{ and } c_2 \neq c_v \\ f(c_2) & \text{otherwise} \end{cases}.$$

Since $\mathrm{Dec}'_{\mathsf{sk}'}(\mathrm{Enc}'_{\mathsf{pk}'}(m)) = \mathrm{Dec}_{\mathsf{sk}}(\mathrm{Enc}_{\mathsf{pk}}(m))$, $\mathit{\Pi}'$ satisfies the correctness property. It is clear that $\mathit{\Pi}'$ is one-way since $\mathit{\Pi}$ is one-way. We show that $\mathit{\Pi}'$ is $\mathsf{pqPA1\text{-}C_{dec}}$ plaintext-aware. Let $\mathcal{A}^*$ be the QPT plaintext-extractor algorithm for $\mathit{\Pi}$. We construct a QPT plaintext-extractor algorithm $\mathcal{A}'^*$ for $\mathit{\Pi}'$. Namely, $\mathcal{A}'^*$ chooses a random function f' with the same domain and co-domain as f and for any (c_1, c_2) operates as follows:

$$\mathcal{A}'^*(c_1, c_2) = \begin{cases} \mathcal{A}^*(c_1) & \text{if } c_1 \neq \perp \text{ and } c_2 = \perp \\ \perp & \text{if } c_1 = \perp \\ f'(c_2) & \text{otherwise} \end{cases} .$$

Note that an adversary with classical access to the decryption oracle is not able to get c_v. In addition, the commitment scheme is computationally hiding and c_{com} reveals c_v only with a negligible probability. Therefore, the decryption query $(\perp, c_v)$ will be submitted with a negligible probability. Since for a polynomial-time adversary with classical access to f and f', these two functions are indistinguishable, $\mathcal{A}'^*$ is a successful polynomial-time plaintext-extractor algorithm for $\mathit{\Pi}'$.

However, an adversary $\mathcal{A}$ with superposition access to Dec', can choose a random ciphertext c' from $\{0,1\}^n$ and queries $|c'\rangle \otimes \sum_{c \in \{0,1\}^n} \frac{1}{\sqrt{n}} |c\rangle$ to Dec'. Therefore, the adversary can employ the Simon's quantum algorithm [20]to obtain c_v and break $\mathsf{pqPA}i\text{-}\mathsf{Q_{dec}}$ plaintext-awareness. In more detail, $\mathcal{A}$ submits $(\perp, c_v)$ as a decryption query. After getting a response $m' \| r' \| \omega'$, it checks if $c_v = \mathrm{Enc}(m'; r')$ and $\mathrm{Ver}(\mathsf{pk}_{com}, c_{com}, c_v, \omega') = 1$. If both equalities hold, it returns 1, otherwise, it returns 0.

In the real case, the Dec' returns $\mathrm{Dec}_{\mathsf{sk}}(c_v) \| r$ and $\mathcal{A}$ outputs 1 with a high probability, namely the probability of Simon's algorithm succeeding. However, in the fake game, since Enc is one-way and the commitment scheme is computationally binding, there is no QPT algorithm $\mathcal{A}^*$ that can simulate an answer to the decryption query $(\perp, c_v)$ such that both equalities above hold with a non-negligible probability. So $\mathcal{A}$ returns 1 with a negligible probability in this case. Consequently, a distinguisher that returns the output of $\mathcal{A}$ can distinguish between the real game and the fake game with a non-negligible probability. □

We can use a similar trick to show that $\mathsf{pqPA0\text{-}Q_{dec}}$ is strictly stronger than $\mathsf{pqPA0\text{-}C_{dec}}$. Since Simon's algorithm needs a polynomial number of queries to extract c_v but in the $\mathsf{pqPA0\text{-}C_{dec}}$ notion the adversary is only allowed to make a single query, we need to modify Dec' a bit further. Namely, we expand the ciphertext space and define Dec'' as the following:

$$\mathrm{Dec}''(c_1, c_2, \cdots, c_m) = \begin{cases} \mathrm{Dec}(c_1) & \text{if } c_1 \neq \perp \text{ and } c_2 = \cdots = c_m = \perp \\ \mathrm{Dec}_{\mathsf{sk}}(c_v) \| r \| \omega & \text{if } c_1 = c_3 = \cdots = c_m = \perp \text{ and } c_2 = c_v \\ \perp & \text{if } c_1 = \perp \text{ and } c_2 \neq c_v \\ f(c_2) || \cdots || f(c_m) & \text{otherwise} \end{cases} .$$

The adversary queries

$$|c\rangle \otimes \sum_{c\in\{0,1\}^n} \frac{1}{\sqrt{n}} |c\rangle \otimes \cdots \otimes \sum_{c\in\{0,1\}^n} \frac{1}{\sqrt{n}} |c\rangle$$

to Dec$''$ to extract c_v. (Note that m is big enough that Simon's algorithm returns c_v with a high probability.)

Corollary 1. *A one-way* $\mathsf{pqPA0\text{-}C_{dec}}$ *plaintext-aware public-key encryption scheme* Enc *is not necessarily* $\mathsf{pqPA0\text{-}Q_{dec}}$ *plaintext-aware.*

Therefore, we can conclude that even the strongest plaintext-awareness notion with classical decryption queries will not imply the weakest plaintext-awareness notion with quantum decryption queries.

Corollary 2. *A one-way* $\mathsf{pqPA2\text{-}C_{dec}}$ *plaintext-aware public-key encryption scheme* Enc *is not necessarily* $\mathsf{pqPA0\text{-}Q_{dec}}$ *plaintext-aware.*

Proof. The proof is similar to the proof of Corollary 1. □

In the theorem below, we show that an adversary with the ability to eavesdrop some ciphertexts is strictly stronger than an adversary without this ability. Namely, we show that an encryption scheme that is $\mathsf{pqPA1\text{-}Q_{dec}}$ plaintext-aware, it is not necessarily $\mathsf{pqPA2\text{-}C_{dec}}$ plaintext-aware. The high-level idea to show this claim is to design an encryption scheme that is malleable on the last bit, however, this malleability does not change the corresponding plaintext. In other words, if we flip the last bit of any ciphertext, we will get a valid ciphertext, but, without any change on the corresponding plaintext. A PA1 adversary is not able to use this malleability since this does not change the plaintext inside of the ciphertext. However, an PA2 adversary can obtain a valid ciphertext (c, b) by eavesdropping and change it to a new ciphertext $(c, b \oplus 1)$ where its corresponding plaintext is unknown to the adversary.

Theorem 5. *A public-key encryption scheme that is* $\mathsf{pqPA1\text{-}Q_{dec}}$ *plaintext-aware and IND-qCPA secure, it is not necessarily* $\mathsf{pqPA2\text{-}C_{dec}}$ *plaintext-aware.*

Proof. Let $\Pi = (\mathrm{Enc}, \mathrm{Dec}, \mathrm{KGen})$ be a $\mathsf{pqPA1\text{-}Q_{dec}}$ plaintext-aware. We construct the following encryption scheme Π':

- $\mathrm{KGen}' = \mathrm{KGen}$
- $\mathrm{Enc}'(m) = \mathrm{Enc}(m)\|0$
- $\mathrm{Dec}'(c\|b) = \mathrm{Dec}(c)$, where $b \in \{0, 1\}$

The IND-qCPA security of Π' is obtained easily by the IND-qCPA security of Π. We show that Π' is also $\mathsf{pqPA1\text{-}Q_{dec}}$ plaintext-aware. Let $\mathcal{A}$ be an adversary that attacks Π' in the sense of $\mathsf{pqPA1\text{-}Q_{dec}}$. We construct an adversary $\mathcal{B}$ that attacks Π. The adversary $\mathcal{B}$ runs $\mathcal{A}$ and answers its decryption queries as follows. Let Q_c, Q_b be the input quantum registers for c, b respectively. Let Q_{out} be the output quantum register. The adversary $\mathcal{B}$ upon receiving Q_c, Q_b, Q_{out} registers from $\mathcal{A}$, it forwards Q_c, Q_{out} registers to its decryption oracle. After getting back $\mathbb{U}_{\mathrm{Dec}}(Q_c Q_{out})$ from its decryption oracle, it sends all three registers to $\mathcal{A}$. It is clear that the decryption queries are simulated perfectly for $\mathcal{A}$. Since Π is $\mathsf{pqPA1\text{-}Q_{dec}}$ plaintext-aware, there exists a plaintext-extractor algorithm $\mathcal{B}^*$ for $\mathcal{B}$. Now from $\mathcal{B}^*$, one can construct an extractor $\mathcal{A}^*$ for $\mathcal{A}$. Namely, $\mathcal{A}^*(c\|b) := \mathcal{B}^*(c)$.

However, Π' is not $\mathsf{pqPA2\text{-}C_{dec}}$ plaintext-aware. Let $\mathcal{A}$ be an adversary that sends two messages $m_0 := 0^n$ and $m_1 := 1^n$ as a query to its plaintext-creator $\mathcal{P}$. Upon receiving a ciphertext $(c\|0)$ from $\mathcal{P}$, it sends $(c\|1)$ as a decryption query. If the answer is 0^n, it returns 0, otherwise it returns 1. Consider a plaintext-creator algorithm $\mathcal{P}_b$ that upon receiving a query m_0, m_1, it sends m_b to Enc. Then, it forwards $(c_b\|0) := \mathrm{Enc}(m_b)$ to the adversary. Let $\mathcal{D}$ be a distinguisher that returns the output of $\mathcal{A}$. Proof by contrary, let assume that Π' is $\mathsf{pqPA2\text{-}C_{dec}}$ plaintext-aware. Then, there exists a plaintext-extractor algorithm $\mathcal{A}^*$ that works for $(\mathcal{A}, \mathcal{P}_0, \mathcal{D})$ and $(\mathcal{A}, \mathcal{P}_1, \mathcal{D})$. That is,

$$G_{real}^{\mathsf{pqPA2\text{-}C_{dec}}}(\mathcal{A}, \mathbb{U}_{\mathrm{Dec}'}, \mathcal{P}_0, \mathcal{D}) \cong G_{fake}^{\mathsf{pqPA2\text{-}C_{dec}}}(\mathcal{A}, \mathcal{A}^*, \mathcal{P}_0, \mathcal{D})$$

and

$$G_{real}^{\mathsf{pqPA2\text{-}C_{dec}}}(\mathcal{A}, \mathbb{U}_{\mathrm{Dec}'}, \mathcal{P}_1, \mathcal{D}) \cong G_{fake}^{\mathsf{pqPA2\text{-}C_{dec}}}(\mathcal{A}, \mathcal{A}^*, \mathcal{P}_1, \mathcal{D})$$

It is clear that in the real case, $\mathcal{D}$ returns 0 with the probability 1 when $\mathcal{A}$ interacts with $\mathcal{P}_0$ and it returns 1 with the probability 1 when $\mathcal{A}$ interacts with $\mathcal{P}_1$. So these two games are distinguishable. Consequently, in the fake game, $\mathcal{A}$'s interaction with $\mathcal{P}_0$ is distinguishable from its interaction with $\mathcal{P}_1$. And this is a contradiction to the IND-qCPA security of Π'. Namely, an adversary $\mathcal{B}$ that runs $\mathcal{A}$ and answers its decryption queries with $\mathcal{A}^*$ and its queries to a plaintext creator with Π''s challenger can break IND-qCPA security of Π'. □

In the following theorem, we show that a one-way public-key encryption scheme that is plaintext-aware against adversaries that make a single quantum decryption query is not necessarily plaintext-aware against adversaries that make many classical decryption queries. The high-level idea is that the decryption oracle partially reveals a valid ciphertext in each query. In more details, we write a valid ciphertext c_v as XOR of two random values $c_v^{(1)}$ and $c_v^{(2)}$, that is $c_v = c_v^{(1)} \oplus c_v^{(2)}$. Then the decryption oracle reveals one of $c_v^{(1)}$ or $c_v^{(2)}$ randomly in each query. Obviously, the adversary with a single query is able to get one of $c_v^{(1)}$ or $c_v^{(2)}$ and that does not give any useful information. On other hand, the adversary with many decryption queries is able to obtain c_v.

Theorem 6. *A one-way* $\mathsf{pqPA0\text{-}Q_{dec}}$ *plaintext-aware public-key encryption scheme is not necessarily* $\mathsf{pqPA1\text{-}C_{dec}}$ *plaintext-aware.*

Proof. Let $\Pi = (\mathrm{KGen}, \mathrm{Enc}, \mathrm{Dec})$ be a $\mathsf{pqPA0\text{-}Q_{dec}}$ plaintext-aware encryption scheme. Let c_v be a ciphertext that is generated by choosing a random message m and a randomness r and computing $\mathrm{Enc}(m; r)$. Let $c_v^{(1)}$ and $c_v^{(2)}$ be two random elements such that $c_v = c_v^{(1)} \oplus c_v^{(2)}$. We construct an encryption scheme

$\Pi' = (\mathrm{KGen}', \mathrm{Enc}', \mathrm{Dec}')$. The algorithm KGen' runs KGen to get $(\mathsf{pk}, \mathsf{sk})$ and it outputs a key pk_{com} for a computationally hiding and binding commitment scheme (Com, Ver). That is, the outputs of KGen' are $((\mathsf{pk}, \mathsf{pk}_{com}), \mathsf{sk})$ and the commitment value $c_{com} = \mathrm{Com}(\mathsf{pk}_{com}, c_v)$ with the corresponding opening ω. Note that a QPT adversary is not able to compute c_v from c_{com} with a non-negligible probability since the commitment scheme is computationally hiding. Let $\omega = \omega^{(1)} \oplus \omega^{(2)}$ for random values $\omega^{(1)}$ and $\omega^{(2)}$. For any message m, $\mathrm{Enc}'(m) = \mathrm{Enc}(m)\|0$. Dec' is a probabilistic algorithm and is defined as:

$$\mathrm{Dec}'(c\|b) = \begin{cases} \mathrm{Dec}(c) & \text{if } \mathrm{Dec}(c) \neq \perp \text{ or } b = 0 \\ c_v^{(i)}\|r\|\omega^{(i)} \text{ for a random i} \in \{0,1\} & \text{if } b = 1 \text{ and } \mathrm{Dec}(c) = \perp \end{cases}.$$

It is clear that $\mathrm{Dec}'(\mathrm{Enc}'(m)) = m$ with the probability 1. We make a convention that for any bit string x, $x \oplus \perp = x$. We show that Π' is $\mathsf{pqPA0\text{-}Q_{dec}}$ plaintext-aware. Let $\mathcal{A}$ be an adversary that attacks Π' in the sense of $\mathsf{pqPA0\text{-}Q_{dec}}$. From $\mathcal{A}$, we construct an adversary $\mathcal{B}$ that attacks Π in the sense of $\mathsf{pqPA0\text{-}Q_{dec}}$. The adversary $\mathcal{B}$ runs $\mathcal{A}$ and answers to its decryption query as follows. Let Q_c, Q_b be the quantum input registers to store the c-part and the b-part of the ciphertext, respectively. Let Q_{out} be a register to store the output. The adversary $\mathcal{B}$ upon receiving these three registers Q_c, Q_b, Q_{out}, it forwards Q_c, Q_{out} to its decryption oracle. After getting $\mathbb{U}_{\mathrm{Dec}}(Q_c Q_{out})$ back from its decryption oracle, it applies a control operator $\mathbb{U}_{cnt}$ on Q_c, Q_b, Q_{out}. The unitary $\mathbb{U}_{cnt}$ XORs a classical random value $c'\|r'\|\omega'$ to the Q_{out} register if $b = 1$ and $\mathrm{Dec}(c) = \perp$. Otherwise, $\mathbb{U}_{cnt}$ is identity. It is clear that the decryption query is simulated perfectly. Since Π is $\mathsf{pqPA0\text{-}Q_{dec}}$, there exists a successful plaintext-extractor $\mathcal{B}^*$ for $\mathcal{B}$. Now we construct a successful plaintext-extractor for $\mathcal{A}$. Namely,

$$\mathcal{A}^*(c\|b) = \begin{cases} \mathcal{B}^*(c) & \text{if } \mathcal{B}^*(c) \neq \perp \text{ or } b = 0 \\ c'\|r'\|\omega' & \text{if } b = 1 \text{ and } \mathcal{B}^*(c) = \perp \end{cases},$$

where c', r' and ω' are random values.

The encryption scheme Π' is not $\mathsf{pqPA1\text{-}C_{dec}}$ aware since an adversary $\mathcal{A}$ is able to obtain c_v, ω, and the corresponding randomness r. It then sends c_v as a decryption query to get m'. Then it outputs 1 if $c_v = \mathrm{Enc}(m'; r)$ and $\mathrm{Ver}(\mathsf{pk}_{com}, c_{com}, c_v, \omega) = 1$. Otherwise, it returns 0. It is clear that in the real case, $\mathcal{A}$ outputs 1 with the probability 1. However, in the fake game, $\mathcal{A}$ outputs 0 with a non-negligible probability since Π is one-way and the commitment scheme is computationally binding. □

4.2 Relation with IND-qCCA

First we show that IND-qCPA security and $\mathsf{pqPA2\text{-}C_{dec}}$ plaintext-awareness notions are not enough to conclude IND-qCCA security. The proof technique is similar to the proof of Theorem 4.

Theorem 7. *A public-key encryption scheme* Enc *that is* $\mathsf{pqPA2\text{-}C_{dec}}$ *plaintext-aware and IND-qCPA secure is not necessarily IND-qCCA secure.*

Proof. Let Enc with the decryption algorithm Dec be a public-key encryption scheme that is $\mathsf{pqPA2\text{-}C_{dec}}$ plaintext-aware and IND-qCPA. Let $\{0,1\}^n$ is the ciphertext space of Enc. We modify Dec to a new decryption algorithm Dec$'$ in which it takes as input a ciphertext from $\{0,1\}^n \times \{0,1\}^n$ and operates as the following:

$$\mathrm{Dec}'(c_1, c_2) = \begin{cases} \mathrm{Dec}(c_1) || \perp & \text{if } \mathrm{Dec}(c_1) \neq \perp \\ \perp || f(c_2) & \text{otherwise} \end{cases},$$

where f is a periodic function on the secret key sk. (That is for any $x \in \{0,1\}^n$, $f(x \oplus \mathsf{sk}) = f(x)$.) It is clear that Enc remains $\mathsf{pqPA1\text{-}C_{dec}}$ plaintext-aware and IND-qCPA secure with this modification to Dec since exponential classical decryption queries are needed to recover sk. However, an adversary with superposition access to Dec$'$, can choose a random ciphertext c' from $\{0,1\}^n$ and queries $|c'\rangle \otimes \sum_{c \in \{0,1\}^n} \frac{1}{\sqrt{n}} |c\rangle$ to Dec$'$. Since Enc is $\mathsf{pqPA}i\mathsf{\text{-}C_{dec}}$ plaintext-aware, with overwhelming probability $\mathrm{Dec}(c') = \perp$. Therefore, the adversary can employ the Simon's quantum algorithm [20] to obtain sk and breaks IND-qCCA security. □

Since $\mathsf{pqPA2\text{-}C_{dec}}$ plaintext-awareness notion implies classical PA2 notion, we can conclude that PA2 + IND-qCPA notion does not imply IND-qCCA security.

Corollary 3. *A public-key encryption scheme* Enc *that is PA2 plaintext-aware and IND-qCPA secure is not necessarily IND-qCCA secure.*

In the theorem below, we show that a plaintext-awareness notion that allows quantum decryption queries, namely the $\mathsf{pqPA2\text{-}Q_{dec}}$ notion, along with the IND-qCPA notion is enough to imply IND-qCCA security.

Theorem 8. *Any public-key encryption scheme* Enc *that is* $\mathsf{pqPA2\text{-}Q_{dec}}$ *plaintext-aware and IND-qCPA secure is IND-qCCA secure.*

Proof. On a high level, we start with the IND-qCCA game when $b = 0$. Since Enc is plaintext-aware there is a ciphertext-extractor algorithm $\mathcal{A}^*$ that can simulate the decryption queries. We replace the decryption oracle with $\mathcal{A}^*$. Then, we switch to the IND-qCCA game with $b = 1$ by IND-qCPA security of Enc. And finally, we replace $\mathcal{A}^*$ with the actual decryption oracle.

Let $\mathcal{X}$ be a QPT adversary that attacks the encryption scheme Enc in the sense of IND-qCCA. We start with IND-qCCA game with the challenge bit $b = 0$ (G_0^{qCCA}) and reach the IND-qCCA game with the challenge bit 1 (G_1^{qCCA}) by introducing intermediate games that are in a negligible distance.

Game 0: G_0^{qCCA}

$$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta), \qquad m_0, m_1 \leftarrow \mathcal{X}^{\mathbb{U}_{\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}}(\mathsf{pk}),$$

$$\mathrm{Enc}(m_0; r_0) \leftarrow \mathrm{Challenger}(m_0, m_1), \; b \leftarrow \mathcal{X}^{\mathbb{U}_{\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}}(\mathsf{pk}, \mathrm{Enc}(m_0; r_0))$$

Let $\mathcal{P}_0$ be a plaintext-creator that upon receiving a query of type m_0, m_1 chooses a randomness r_0 and returns $\mathrm{Enc}(m_0, r_0)$. We replace the challenger in $G_{b=0}^{qCCA}$ with $\mathcal{P}_0$ to reach Game 1.

Game 1: $G_{real}^{\mathsf{pqPA2\text{-}Q_{dec}}}$ *with* $\mathcal{P}_0$

$$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta), \qquad m_0, m_1 \leftarrow \mathcal{X}^{\mathbb{U}_{\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}}(\mathsf{pk}),$$
$$\mathrm{Enc}(m_0; r_0) \leftarrow \mathcal{P}_0(m_0, m_1),\ b \leftarrow \mathcal{X}^{\mathbb{U}_{\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}}(\mathsf{pk}, \mathrm{Enc}(m_0; r_0))$$

It is obvious that Game 0 and Game 1 are indistinguishable.

Since Enc is $\mathsf{pqPA2\text{-}Q_{dec}}$ aware there exists a successful ciphertext extractor $\mathcal{A}^*$ for $\mathcal{X}$. Let Q_{int} be the internal register of $\mathcal{X}$. In Game 2, we replace the decryption oracle with $\mathcal{A}^*$.

Game 2: $G_{fake}^{\mathsf{pqPA2\text{-}Q_{dec}}}$ *with* $\mathcal{P}_0$

$$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta), \qquad m_0, m_1 \leftarrow \mathcal{X}^{\mathcal{A}^*(\mathsf{pk}, \mathrm{Q}_{int})},$$
$$\mathrm{Enc}(m_0; r_0) \leftarrow \mathcal{P}_0, \quad b \leftarrow \mathcal{X}^{\mathcal{A}^*(\mathsf{pk}, \mathbf{List}, \mathrm{Q}_{int})}(\mathsf{pk}, \mathrm{Enc}(m_0; r_0))$$

Since $\mathcal{A}^*$ is a successful ciphertext extractor for $\mathcal{X}$, Game 1 and Game 2 are indistinguishable.

Let $\mathcal{P}_1$ be a plaintext-creator algorithm that upon receiving a query of type m_0, m_1 chooses randomness r_1 and returns $\mathrm{Enc}(m_1; r_1)$. We replace $\mathcal{P}_0$ with $\mathcal{P}_1$ in Game 2 to reach Game 3.

Game 3: $G_{fake}^{\mathsf{pqPA2\text{-}Q_{dec}}}$ *with* $\mathcal{P}_1$

$$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta), \qquad m_0, m_1 \leftarrow \mathcal{X}^{\mathcal{A}^*(\mathsf{pk}, \mathrm{Q}_{int})},$$
$$\mathrm{Enc}(m_1; r_1) \leftarrow \mathcal{P}_1, \quad b \leftarrow \mathcal{X}^{\mathcal{A}^*(\mathsf{pk}, \mathbf{List}, \mathrm{Q}_{int})}(\mathsf{pk}, \mathrm{Enc}(m_1; r_1))$$

Since Enc is IND-qCPA secure, Game 2 and Game 3 are indistinguishable. In more detail, let us assume there is a distinguisher $\mathcal{D}$ with a non-negligible advantage for these two games. Now $\mathcal{Y} = (\mathcal{X}, \mathcal{A}^*, \mathcal{D})$ is an adversary to break IND-qCPA security of Enc that is a contradiction.

In Game 4, we replace $\mathcal{A}^*$ with the decryption oracle.

Game 4

$$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta), \qquad m_0, m_1 \leftarrow \mathcal{X}^{\mathbb{U}_{\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}}(\mathsf{pk}),$$
$$\mathrm{Enc}(m_1; r_1) \leftarrow \mathcal{P}_1(m_0, m_1),\ b \leftarrow \mathcal{X}^{\mathbb{U}_{\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}}(\mathsf{pk}, \mathrm{Enc}(m_1; r_1))$$

Since $\mathcal{A}^*$ is a successful plaintext-extractor for $\mathcal{X}$, these two games are indistinguishable.

Finally, we replace $\mathcal{P}_1$ with the challenger in Game 5 to reach G_1^{qCCA}.

Game 5: G_1^{qCCA}

$$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathrm{KGen}(1^\eta), \qquad m_0, m_1 \leftarrow \mathcal{X}^{\mathbb{U}_{\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}}(\mathsf{pk}),$$
$$\mathrm{Enc}(m_1; r_1) \leftarrow \mathrm{Challenger}(m_0, m_1),\ b \leftarrow \mathcal{X}^{\mathbb{U}_{\mathrm{Dec}'_{(\mathsf{sk},\mathbf{List})}}}(\mathsf{pk}, \mathrm{Enc}(m_1; r_1))$$

It is clear that Game 4 and Game 5 are indistinguishable. And this finishes the proof. □

5 Achievability

In this section, we lift a public-key encryption scheme that is PA2 plaintext-aware against a quantum adversary (PA2 notion with classical decryption) to an encryption scheme that is $\mathsf{pqPA2\text{-}Q_{dec}}$.

Let $\Pi^{asy} = (\mathrm{KGen}^{asy}, \mathrm{Enc}^{asy}, \mathrm{Dec}^{asy})$ be a public-key encryption scheme that is PA2 plaintext-aware. We construct a public-key encryption scheme $\Pi^{hyb} = (\mathrm{KGen}^{hyb}, \mathrm{Enc}^{hyb}, \mathrm{Dec}^{hyb})$ and shows that it is $\mathsf{pqPA2\text{-}Q_{dec}}$. The encryption scheme Π^{hyb} is defined as :

- The algorithm KGen^{hyb} on input of the security parameter η runs $\mathrm{KGen}^{asy}(\eta)$ and returns its output $(\mathsf{pk}, \mathsf{sk})$.
- For any message $m \in \{0,1\}^n$, the algorithm Enc^{hyb} chooses a randomness r and returns $\mathrm{Enc}^{asy}_{\mathsf{pk}}(r) || qPRP_r(m||0^k)$ where $qPRP$ is a strong quantum-secure pseudo-random permutation and k depends on the security parameter η.
- For any ciphertext (c_1, c_2), Dec^{hyb} first decrypts c_1 using sk, if the output is $\perp$, it returns $\perp$. Otherwise, it uses the output as the key for $qPRP$ to decrypt c_2. If the k_1 least significant bits of the outcome is not 0, it returns $\perp$, otherwise it returns the n most significant bits of the outcome.

$$\mathrm{Dec}^{hyb}(c_1, c_2) = \begin{cases} \perp & \text{if } \mathrm{Dec}^{asy}_{\mathsf{sk}}(c_1) = \perp \\ \perp & \text{if } [qPRP^{-1}_{\mathrm{Dec}^{asy}_{\mathsf{sk}}(c_1)}(c_2)]_k \neq 0^k \\ [qPRP^{-1}_{\mathrm{Dec}^{asy}_{\mathsf{sk}}(c_1)}(c_2)]^n & \text{otherwise} \end{cases}.$$

Theorem 9. *Under the assumption of the existence of a quantum one-way function, the public-key encryption scheme* $\Pi^{hyb} = (\mathrm{KGen}^{hyb}, \mathrm{Enc}^{hyb}, \mathrm{Dec}^{hyb})$ *described above is* $\mathsf{pqPA2\text{-}Q_{dec}}$.

Proof. Let $\mathcal{A}$ be an adversary that attacks Π^{hyb} in the sense of $\mathsf{pqPA2\text{-}Q_{dec}}$. We construct an adversary $\mathcal{B}$ that attacks Π^{asy} in the sense of PA2. Let $\mathcal{P}_B$ be a plaintext-creator adversary that upon receiving a query, chooses a randomness r and sends it to the encryption oracle Π^{asy} to receive $\mathrm{Enc}^{asy}_{\mathsf{pk}}(r)$. Then it sends $\mathrm{Enc}^{asy}_{\mathsf{pk}}(r)$ to the ciphertex-creator adversary. The adversary $\mathcal{B}$ runs $\mathcal{A}$ and answers to the decryption queries as follows. When $\mathcal{A}$ makes a decryption query $\sum_{c_2} \alpha_{c_2} |c_1\rangle |c_2\rangle$, the adversary $\mathcal{B}$ forwards only the first part of the ciphertext (c_1) to its oracle. (Note that c_1 is a classical value and it is not entangled with the rest of the query. So forwarding the c_1-part does not disturb the decryption query.) If its oracle on input c_1 returns $\perp$, $\mathcal{B}$ returns $\perp$. Otherwise, if its oracle on input c_1 returns r ($\neq\perp$), $\mathcal{B}$ uses r as the key for $qPRP$ to decrypt the c_2-part. Note that if the k_1 least significant bits of $qPRP_r^{-1}(c_2)$ is not zero, the output of $\mathcal{B}$ will be $\perp$. Otherwise, the output will be the n most significant bits of $qPRP_r^{-1}(c_2)$. When $\mathcal{A}$ makes a query m to its plaintext-creator $\mathcal{P}_A$, $\mathcal{B}$ makes a query to $\mathcal{P}_B$ to receive the ciphertext c_1. Then it sends $(c_1, \pi(m||0^k))$ to $\mathcal{A}$ where π is a random permutation. Since Π^{asy} is PA2, there exists a ciphertex extractor $\mathcal{B}^*$ for $\mathcal{B}$.

Now we consider the ciphertex extractor $\mathbb{U}_{\mathcal{A}_1^*}$ where for any (c_1, c_2),

$$\mathcal{A}_1^*(c_1, c_2) = \begin{cases} \perp & \text{if } \mathcal{B}^*(c_1) = \perp \\ \perp & \text{if } [qPRP^{-1}_{\mathcal{B}^*(c_1)}(c_2)]_k \neq 0^k \\ [qPRP^{-1}_{\mathcal{B}^*(c_1)}(c_2)]^n & \text{otherwise} \end{cases} .$$

We show that $\mathbb{U}_{\mathcal{A}_1^*}$ is a successful plaintext-extractor for $\mathcal{A}$ in the following.

Game 0: We start with $G_{real}^{\mathsf{pqPA2\text{-}Q_{dec}}}$ that is run by a plaintext-creator $\mathcal{P}_A$ and a distinguisher $\mathcal{D}$.
Game 1: We change the plaintex creator $\mathcal{P}_A$ to a new plaintext-creator $\mathcal{P}'_B$ that upon receiving a query m runs $\mathcal{P}_B$ to obtain c_1, then it chooses a random permutation π and returns $(c_1, \pi(m||0^k))$. We show that these two games are indistinguishable. An observation is that the first part of the $\mathcal{P}_A$'s output (c_1) is independent of $\mathcal{P}_A$ since it is the encryption of a random string that is chosen by the encryption algorithm. In other words, the c_1-part is generated exactly the same by $\mathcal{P}_A$ and $\mathcal{P}'_B$. The indistinguishability of the c_2-part holds as well since a quantum-secure pseudo-random permutation is indistinguishable from a random permutation.
Game 2: In this game, the decryption queries will be answered by $\mathbb{U}_{\mathcal{A}_1^*}$. An observation is that $\mathcal{A}_1^*$ is indistinguishable from Dec^{hyb} because $\mathcal{B}^*$ is indistinguishable from $\mathrm{Dec}^{asy}_{\mathsf{sk}}$ (the rest of $\mathcal{A}_1^*$ and Dec^{hyb} are the same). Therefore, these two games remain indistinguishable. In other words, these two games are indistinguishable because $\mathcal{B}^*$ is a successful plaintext-extractor for $\mathcal{B}$.
Game 3: In the last game, we replace the plaintext-creator $\mathcal{P}'_B$ with $\mathcal{P}_A$. The same reasoning as Game 0,1 shows that Game 2 and Game 3 are indistinguishable and this finishes the proof. □

5.1 OAEP transform

The main motivation to present the first definition for plaintext-awareness notion [4] was to show the security of Optimal Asymmetric Encryption Padding (OAEP). Even though our definitions for PA notions are in the standard model, we argue that these definitions apply to the random oracle model as well because queries to the random oracles is a part of the internal register of the adversary. We briefly explain why we think OAEP is $\mathsf{pqPA1\text{-}Q_{dec}}$ plaintext-aware.

We take this from a recent work on the IND-qCCA security of OAEP transform [10]. There, Ebrahimi started with the actual decryption algorithm $\mathbb{U}_{\mathrm{Dec}}$ and introduced a sequence of indistinguishable decryption algorithms to construct a decryption algorithm $\mathbb{U}_{\mathrm{Dec}^{(4)}}$ that does not use the secret key. (Since the queries to the random oracles are quantum, Zhandry's compressed oracle technique [21] has been used in [10].) This decryption algorithm $\mathbb{U}_{\mathrm{Dec}^{(4)}}$ can be invoked by a plaintext-extractor adversary $\mathcal{A}^*$ in the fake game. The indistinguishably of $\mathbb{U}_{\mathrm{Dec}}$ and $\mathbb{U}_{\mathrm{Dec}^{(4)}}$ gives us the $\mathsf{pqPA1\text{-}Q_{dec}}$ plaintext-awareness. However, whether OAEP is $\mathsf{pqPA2\text{-}Q_{dec}}$ plaintext-aware or not is an open question. The reason is the random oracle queries that are submitted by a plaintext-creator $\mathcal{P}$ are not accessible by $\mathcal{A}^*$. So $\mathbb{U}_{\mathrm{Dec}^{(4)}}$ sketched above is not able to decrypt a ciphertext that is obtained by indirect (for instance by a malleability of a ciphertext obtained from $\mathcal{P}$) use of these random oracle queries.

Acknowledgment. We would like to thank Peter Ryan, Peter Browne Rønne and Dimiter Ostrev for discussions about this work. Jeroen van Wier is supported by the Luxembourg National Research Fund (FNR), under the joint CORE project Q-CoDe (CORE17/IS/11689058/Q-CoDe/Ryan).

References

1. E. Andreeva, A. Bogdanov, A. Luykx, B. Mennink, N. Mouha, and K. Yasuda. How to securely release unverified plaintext in authenticated encryption. In *ASIACRYPT 2014*, volume 8873, pages 105–125. Springer, 2014.
2. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *CRYPTO 1998*, volume 1462, pages 26–45. Springer, 1998.
3. M. Bellare and A. Palacio. Towards plaintext-aware public-key encryption without random oracles. In *ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, pages 48–62. Springer, 2004.
4. M. Bellare and P. Rogaway. Optimal asymmetric encryption. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 92–111. Springer, 1994.
5. J. Birkett and A. W. Dent. Security models and proof strategies for plaintext-aware encryption. *J. Cryptol.*, 27(1):139–180, 2014.
6. D. Boneh and M. Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *CRYPTO 2013*, volume 8043, pages 361–379. Springer, 2013.
7. T. V. Carstens, E. Ebrahimi, G. N. Tabia, and D. Unruh. Relationships between quantum IND-CPA notions. In *TCC 2021,*, volume 13042, pages 240–272. Springer, 2021.
8. C. Chevalier, E. Ebrahimi, and Q. H. Vu. On the security notions for encryption in a quantum world. *IACR Cryptology ePrint Archive*, 2020:237, 2020.
9. A. W. Dent. The cramer-shoup encryption scheme is plaintext aware in the standard model. In *EUROCRYPT 2006*, volume 4004, pages 289–307. Springer, 2006.
10. E. Ebrahimi. Post-quantum security of plain OAEP transform. In *PKC 2022*, volume 13177, pages 34–51. Springer, 2022.

11. T. Gagliardoni, A. Hülsing, and C. Schaffner. Semantic security and indistinguishability in the quantum world. In *CRYPTO 2016*, volume 9816, pages 60–89. Springer, 2016.
12. T. Gagliardoni, J. Krämer, and P. Struck. Quantum indistinguishability for public key encryption. In *PQCrypto 2021*, volume 12841, pages 463–482. Springer, 2021.
13. J. Herzog, M. D. Liskov, and S. Micali. Plaintext awareness via key registration. In D. Boneh, editor, *CRYPTO 2003*, volume 2729, pages 548–564. Springer, 2003.
14. A. Jain, S. Krenn, K. Pietrzak, and A. Tentes. Commitments and efficient zero-knowledge proofs from learning parity with noise. In *ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 663–680. Springer, 2012.
15. E. Kashefi, A. Kent, V. Vedral, and K. Banaszek. Comparison of quantum oracles. *Phys. Rev. A*, 65:050304, May 2002.
16. A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami. Computational indistinguishability between quantum states and its cryptographic application. In *EUROCRYPT 2005*, volume 3494, pages 268–284. Springer, 2005.
17. R. J. McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.
18. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *ACM Symposium on Theory of Computing, 2005*, pages 84–93. ACM, 2005.
19. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.
20. D. R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474–1483, 1997.
21. M. Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In *CRYPTO 2019*, volume 11693, pages 239–268. Springer, 2019.

A Discussion on Quantum Eavesdropping

A possible plaintext-awareness definition that considers superposition eavesdropping may be difficult to define due to the no-cloning theorem. For instance, if we follow the above formalism, the plaintext-creator adversary $\mathcal{P}$ upon receiving the input and output registers Q_{inp} and Q_{out} from $\mathcal{A}$, can apply a random unitary to Q_{inp}, then applies the encryption unitary and sends both registers back to the adversary. But now it is not clear how one can handle decryption queries. More specifically, the superposition ciphertexts that have been created by calling $\mathcal{P}$ can not be recorded in general and if one of them is submitted as a decryption query, in the real game, the decryption oracle will return the corresponding superposition of messages but in the fake game, but $\mathcal{A}^*$ is not able to return the corresponding superposition of messages without access to the internal register of $\mathcal{P}$. Note that if $\mathcal{A}^*$ is able to decrypt those queries without access to the internal register of $\mathcal{P}$ and the secret key, it renders the encryption scheme insecure.