Quantum Indistinguishability
for Public Key Encryption

Tommaso Gagliardoni[1], Juliane Krämer[2], and Patrick Struck[2]

[1] Kudelski Security, Switzerland
`firstname.lastname@kudelskisecurity.com`
[2] Technische Universität Darmstadt, Germany
`{juliane,patrick}@qpc.tu-darmstadt.de`

Abstract. In this work we study the quantum security of public key encryption schemes (PKE). Boneh and Zhandry (CRYPTO'13) initiated this research area for PKE and symmetric key encryption (SKE), albeit restricted to a classical indistinguishability phase. Gagliardoni et al. (CRYPTO'16) advanced the study of quantum security by giving, for SKE, the first definition with a quantum indistinguishability phase. For PKE, on the other hand, no notion of quantum security with a quantum indistinguishability phase exists.

Our main result is a novel quantum security notion (qIND-qCPA) for PKE with a quantum indistinguishability phase, which closes the aforementioned gap. We show a distinguishing attack against code-based schemes and against LWE-based schemes with certain parameters. We also show that the canonical hybrid PKE-SKE encryption construction is secure, even if the underlying PKE scheme by itself is not. Finally, we classify quantum-resistant PKE schemes based on the applicability of our security notion and discuss concurrent and independent work.

Our core idea follows the approach of Gagliardoni et al. by using so-called type-2 operators for encrypting the challenge message. At first glance, type-2 operators appear unnatural for PKE, as the canonical way of building them requires both the secret and the public key. However, we identify a class of PKE schemes - which we call *recoverable* - and show that for this class type-2 operators require merely the public key. Moreover, recoverable schemes allow to realise type-2 operators even if they suffer from decryption failures, which in general thwarts the reversibility mandated by type-2 operators. Our work reveals that many real-world quantum-resistant PKE schemes, including most NIST PQC candidates and the canonical hybrid construction, are indeed recoverable.

1 Introduction

The discovery of Shor's [43] and Grover's [27] quantum algorithms had a significant impact on cryptographic research. Shor's algorithm in particular has the potential to completely break most of the public key cryptosystems used nowadays. This led to the development of quantum-resistant cryptography,[3] that is,

---

[3] This type of cryptography is often called "post-quantum cryptography" [12].

cryptography that can run on non-quantum computers but should withstand attackers equipped with quantum computing power. In recent years the research efforts on quantum-resistant cryptography accelerated significantly due to the standardization process initiated by the NIST [39].

Modern cryptography is based on the paradigm of *provable security*, which is itself given in terms of a security notion, an adversarial model, and a security proof. A widely used framework for defining security notions is the so-called *game-based security*, which is presented as a game between two or more parties.[4] In the case of encryption schemes these parties are: a challenger, representing the user of the scheme, and an adversary, representing an attacker against the scheme. Any meaningful model for quantum-resistant schemes should entail that the adversary has quantum computing power. Based on this, we can differentiate between different models depending on the computing power of the challenger. In the literature there are mainly two of these models that are taken into account. In the first, the challenger remains fully classical, implying that any communication between adversary and challenger is also classical (including oracles provided by the challenger to the adversary), while the adversary retains local quantum computing power. This is the model most often considered in quantum-resistant cryptography, and it is also called QS1 [24] or Q1 [30]. In the second case, the challenger also has quantum computing power, which enables quantum communication between challenger and adversary. This stronger model is sometimes called "superposition-attack security" [22], QS2 [24], or Q2 [30].

Boneh and Zhandry [15] initiated the study of QS2 security for cryptographic primitives. For signature schemes, they give a security definition that allows the adversary to query the signing oracle on a superposition of messages. For public and symmetric key encryption (PKE and SKE) schemes, on the other hand, they prove that simply allowing the adversary to query a superposition of messages as challenge in a "natural" way gives an unachievable security notion (fqIND-CPA). This is due to entanglement between the plaintext register and the ciphertext register. They show how to exploit this entanglement to break this security notion irrespectively of the used encryption scheme. To resolve this, they propose another security notion (IND-qCPA) which allows the adversary superposition queries in the CPA phase while the challenge messages in the IND phase are restricted to be classical. This notion coincides with the traditional QS1 security notion for PKE (as the adversary can simulate the encryption in superposition using his local computing power and the public key), while for SKE, this yields a notion of QS2 security - although the restriction to a classical challenge in this case is clearly a shortcoming.

Gagliardoni et al. [25] overcame this shortcoming in the symmetric key case by showing how to model a quantum challenge query, while keeping the resulting security notion (qIND-qCPA) still achievable, yet stronger than IND-qCPA. At the heart of their idea lies the use of so-called *type-2 operators*[5] rather than so-

---

[4] Other frameworks exist, such as simulation-based, but as a first approximation game-based security notions are very convenient for their intuitivity and simplicity.

[5] Also called *minimal oracles* in [31].

called type-1 operators when encrypting the challenge messages of the adversary. Type-1 operators are the "canonical" way of implementing a classical function $\mathcal{F}$ on a quantum superposition of input, by mapping the state $|x, y\rangle$ to $|x, y \oplus \mathcal{F}(x)\rangle$, thereby ensuring reversibility for any function $\mathcal{F}$ (reversibility being necessary when defining non-measurement quantum operations). An important property of type-1 operators is that they create entanglement between the input and output registers. This is exactly the entanglement which Boneh and Zhandry exploit to show that fqIND-CPA is unachievable. In contrast to these, type-2 operators work directly on the input register, i.e., they map the state $|x\rangle$ to $|\mathcal{F}(x)\rangle$. Only reversible functions, for instance permutations, can be implemented as type-2 operators, while it is impossible to compute, say, an arbitrary one-way function through a type-2 operator. Gagliardoni et al. observe that SKE schemes act as permutations between the plaintext space and the ciphertext space, which allows to implement the encryption algorithm as a type-2 operator. This, in turn, allows to build a solid framework for QS2 security in the case of SKE.

In [25] the authors speculate that their techniques could be extended to the public key case (PKE) as well. However, defining type-2 operators for PKE schemes is much more involved than for SKE schemes. First, to achieve IND-CPA security, PKE schemes are inherently randomised and the randomness is usually erased in the process of decryption. Second, many constructions for quantum-resistant PKE schemes, in particular lattice-based and code-based schemes, suffer from a small probability of decryption failures, i.e., ciphertexts which do not decrypt correctly. Given the above, at first glance it is unclear whether type-2 operators for PKE schemes are possible at all, as these two properties seem to thwart the mandatory reversibility. Hence, QS2 security for the public key case remained an open problem so far.

1.1   Our Contribution

We present a novel QS2 security notion[6] for PKE, provide both achievability results and separation to the QS1 security notion for many real-world schemes, and give a general classification of PKE with respect to our security notion.

Our core focus is to extend the results from [25] to the public key scenario. We first formalize the theory of type-2 encryption operators for PKE. For perfectly correct schemes (i.e., schemes which do not suffer from the possibility of decryption failures) we define the type-2 operator to preserve a randomness register in input and output. Even if such approach might look strange at first glance, we show that this is the most natural way of defining type-2 operators for PKE schemes. As a next step, we identify a class of PKE schemes (which we call *recoverable*) where decryption failures can always be avoided given knowledge of the randomness used during encryption, regardless of the actual failure probability of the decryption algorithm. We observe that most real-world partially correct PKE schemes (including many quantum-resistant NIST candidates) are actually of this type. Then, for schemes that are perfectly correct or recoverable, we show

---
[6] See Appendix C for independent and concurrent work.

how to efficiently construct the type-2 encryption operator. Moreover, we show that for recoverable schemes, this can be done by knowledge of the public key only! This implies, perhaps surprisingly, that the adversary can implement efficiently this type-2 operator already in the QS1 model. Such observation marks a substantial difference from the symmetric key case, where the need for type-2 operators is dictated by necessity in order to cover exotic attack models. Thus, the type-2 operator for these schemes can be realised without the secret key.

Using the theory of type-2 operators developed so far, we give a novel QS2 security notion for PKE, that we call *quantum ciphertext indistinguishability under quantum chosen plaintext attack* (qIND-qCPA). For a new security notion to be meaningful, two properties are required. First, it has to be achievable, and, second, it has to differ from existing security notions.

We analyse several real-world PKE schemes in respect to our new qIND-qCPA security notion. We show that the canonical LWE-based PKE scheme [41] can be attacked, at least for certain parameters. The attack is similar to the "Hadamard distinguisher" given in [25]. Moving on to code-based schemes, we observe that some constructions encrypt the message using a one-time pad operation, which again allows to exploit the distinguishing attack. As an example we show that the code-based scheme ROLLO-II [10] is not qIND-qCPA secure.

However, in practice most real-world PKE schemes (including the NIST submissions) are used as Key Encapsulation Mechanisms (KEM) in combination with a SKE scheme, yielding a hybrid PKE-SKE construction. Looking at such canonical hybrid construction then, we show that its qIND-qCPA security mostly depends on the underlying SKE scheme, while the PKE scheme only needs to be secure in the QS1 sense. Hence, even the code-based PKE scheme ROLLO-II, which as a stand-alone PKE scheme is not qIND-qCPA-secure, can be used to achieve qIND-qCPA security if combined with a qIND-qCPA-secure SKE scheme via the hybrid construction, which is the default way of using it in practice.

Finally, we discuss the difficulty of defining type-2 operators (and the related QS2 security notion) for arbitrary schemes that are neither perfectly correct nor recoverable. We study the problem of their general classification and we identify a class of schemes, that we call *isometric*, that allow to overcome such difficulty, and we provide constructions and separation results.

1.2   The Motivation for QS2 Security

Defining security against quantum adversaries with superposition access to certain oracles requires some motivation. Sometimes, the resulting security notion is already implicitly captured by the corresponding QS1 scenario (for example in the case of *quantum random oracles* [13]). In other cases, for instance those considered in [7, 29, 33], it might look like an artificial extension of the theory.

However, QS2 security extends quantum properties to types of attack scenarios not covered in QS1, and at the same time "bridges" certain security notions from the classical realm to schemes which are meant to run natively on a quantum computer. Some of the reasons why QS2 notions are important to consider are explained in detail in [24]. They basically boil down to five points.

1. To ensure that quantum-resistant classical schemes retain their security even if executed on a quantum computer, possibly in complex environments or protocols where composition should be taken into account.
2. To fix security proofs, where the sole QS1 security of certain underlying building blocks is not enough to ensure that the whole proof goes through. An example is the need of QS2-secure pseudorandom functions (QPRF) in order to simulate a quantum random oracle [46], which is a QS1 concept.
3. To ensure the security of quantum protocols (i.e., meant to run natively on a quantum computer and protect quantum data) when using classical algorithms as building blocks. For example, [24] shows how it is possible to build a secure symmetric quantum encryption scheme (falling into the so-called QS3 domain) by using a qIND-qCPA symmetric classical encryption scheme (QS2), but not necessarily a simple quantum-resistant (QS1) one.
4. To consider cases of *code obfuscation*; for example creating a quantum-resistant PKE scheme by hardcoding a symmetric key into an obfuscated encryption program (a technique known as *whiteboxing* [20]), which is then distributed as a public key.
5. To cover cases of *exotic quantum attacks*. These include, for instance, *quantum fault injection attacks*, where a classical device is subject to controlled and artificial physical conditions that induce full or partial quantum behaviour of its hardware ("tricking" a classical device into being quantum, like in the "frozen smart-card attack" presented in [25]); or cases where a quantum computer is used to run a classical algorithm, but an adversary manages to intercept the intermediate result of the computation *before* the final measurement meant to produce a classical outcome.

In our specific case, our results follow from the core use of type-2 operators. This kind of quantum operations is poorly studied in the quantum computing realm, and might therefore look artificial for cryptographic use. In the present work we make an effort to expand in a detailed way the formalization of such operators which, we stress, are only given for functions that are inherently invertible. It is a well-known fact (see for example [25]) that implementing these operators for encryption schemes usually requires knowledge of the secret key. We do not consider this to be a limitation because in the quantum setting, an honest challenger equipped with the secret key could be allowed to generate particular ciphertext-encoding states which would be hard to compute for an external party: it is therefore necessary to cover this distinction in the preparation of ciphertext states, and type-2 operators do just that. Moreover, as we show in the present work, for many natural PKE schemes, type-2 encryption operators can actually be efficiently implemented by knowledge of the public key only.

1.3 Related Work

The study of quantum security under adversarial queries in superposition can be traced back to works such as [13, 22, 45], which explore different settings where this additional adversarial power has an impact on security. However, for the

case of signatures and encryption schemes, the first framework going beyond the traditional QS1 paradigm was given in [15]. This paradigm was further extended in [25] for symmetric key encryption schemes, and in [6] for MACs/signatures.

Regarding examples of exotic quantum attacks previously mentioned: it is currently not known whether any of these are feasible at all, but as noted in [24]: (1) if they are feasible, in some cases they do not even require a fully fledged quantum computer (for example, in the attack from [25] it would be only necessary to produce and detect a Hadamard superposition of messages); and (2) it is already known in the literature that these attacks can be devastating. For example, *related-key attacks* [42], and superposition attacks against Even-Mansour [33], Feistel networks [28,32], block ciphers [7,9], and HMAC constructions [29].

Qualitatively different, but technically very connected to the QS2 setting is the *fully quantum setting*, or QS3 in short. This security domain encompasses security notions and constructions for schemes which are natively run on quantum hardware. In the case of QS3 encryption, these are schemes which are meant to protect quantum, rather than classical data. It turns out that many of the challenges in this area are shared with the QS2 case. In the computational security setting, the first security notions have been provided in [17] for the CPA case, and in [3] for the CCA1 and semantic security case. These results have been further extended to the CCA2 setting in [5] for the symmetric case, and in [4] for the public key case.

In concurrent and independent work, Chevalier et al. [19] propose alternative QS2 security notions for encryption schemes. Their and our notion are incomparable, as also claimed in a recent work by Carstens et al. [18]. We discuss the differences in more detail in Appendix C.

1.4   Organization of the Paper

Section 2 gives the required background for this work. In Section 3 we study type-2 operators for PKE schemes, define *recoverable* schemes, and give our new quantum security notion for those. Positive and negative results for real-world PKE schemes are presented in Section 4. Finally, we refine the classification of PKE schemes in terms of QS2 security in Section 5 and conclude with open questions in Section 6.

2   Preliminaries

In the following, we use "classical" as meaning "non-quantum". By *algorithm* or *procedure* (classical or quantum) we mean a uniform family of circuits (classical or quantum) of depth and width polynomial in the index of the family. We call such index a *security parameter*, and we denote it by λ (or 1^λ if written in unary notation). We implicitly assume that all algorithms take 1^λ as a first input, so we will often omit this. If a classical algorithm A is deterministic, we denote its output y on input x as $y := A(x)$, while if it is randomized we use $y \leftarrow A(x)$; when derandomizing an algorithm we look at the deterministic algorithm obtained

when considering explicitly the internal randomness r as an additional auxiliary input, and we write $y := A(x; r)$. We will also use $x \leftarrow \mathcal{D}$ to denote that an element x is sampled from a distribution $\mathcal{D}$; or we will write $x \xleftarrow{\$} X$ if x is sampled uniformly at random from a set X. We will call *negligible* a function that grows more slowly than any inverse polynomial, and *overwhelming* a function which is 1 minus a negligible function. Finally, $a \| b$ denotes concatenation of a and b.

2.1 Quantum Notation

We assume familiarity with the topic of quantum computing, but recall here the basic required notation. For an in-depth discussion we refer to [38].

A quantum system, identified by a letter A, is represented by a complex Hilbert space, which we denote by $\mathfrak{H}_A$. If A is clear from the context, we write $\mathfrak{H}$ rather than $\mathfrak{H}_A$. Pure states in a Hilbert space $\mathfrak{H}$ are representatives of equivalence classes of elements of $\mathfrak{H}$ of norm 1. Mixed states, on the other hand, are a more general representation of quantum states that takes *entanglement* with external systems into account; they are elements of the density matrix operator space over $\mathfrak{H}$, that is, Hermitian positive semi-definite linear operators of trace 1, denoted as $\mathfrak{D}(\mathfrak{H})$. We use the ket notation for pure states, e.g., $|\varphi\rangle$, while mixed states will be denoted by lowercase Greek letter, e.g., ρ. Operations on pure states from A to B are performed by applying a unitary operator $U: \mathfrak{H}_A \to \mathfrak{H}_B$ to the state, while the more general case of operations on mixed states is described by superoperators of the form $U: \mathfrak{D}(\mathfrak{H}_A) \to \mathfrak{D}(\mathfrak{H}_B)$

The canonical way to compute a classical function $\mathcal{F}: \mathcal{X} \to \mathcal{Y}$ on a superposition of possible inputs $\sum_{x \in \mathcal{X}} \alpha_x |x\rangle$ is through the so-called *type-1 operator for $\mathcal{F}$* described by:

$$U_{\mathcal{F}}^{(1)}: \sum_{x,y} \alpha_{x,y} |x, y\rangle \mapsto \sum_{x,y} \alpha_{x,y} |x, y \oplus \mathcal{F}(x)\rangle \ ,$$

This can always be implemented efficiently whenever $\mathcal{F}$ is efficient [38]. By linearity, it is sufficient to specify just the behaviour on the basis elements, i.e.:

$$U_{\mathcal{F}}^{(1)}: |x, y\rangle \mapsto |x, y \oplus \mathcal{F}(x)\rangle \ .$$

If $\mathcal{F}$ is invertible, then there is another non-equivalent possible way to compute $\mathcal{F}$ in superposition. This is done through the so-called *type-2 operators*, which are defined as the unitary:

$$U_{\mathcal{F}}^{(2)}: |x\rangle \mapsto |\mathcal{F}(x)\rangle \ .$$

See Fig. 1 for an illustration of these different operators. Kashefi et al. [31] first introduced type-2 operators using the term *minimal oracles* instead. They show that these operators are strictly stronger by giving a problem which can be solved exponentially faster with type-2 operators than with type-1 operators. They also observe that the adjoint of the type-2 operator corresponds to the type-2 operator of the inverse function $\mathcal{F}^{-1}$, which is (usually) not the case for type-1 operators. Besides that, type-2 operators have been used by Gagliardoni et al. [25] to define quantum security for secret key encryption schemes.
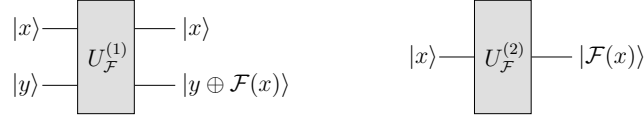
Fig. 1: Type-1 operator (left) and type-2 operator (right) for a function $\mathcal{F}$.

2.2 Public Key Encryption

In this section we give the formal definition for public key encryption schemes and the correctness of such schemes.

Definition 1 *A* public key encryption (PKE) scheme *is a tuple* $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *of three efficient algorithms such that:*

- $\mathsf{KGen} \colon \mathbb{N} \times \mathcal{R} \to \mathcal{P} \times \mathcal{S}$ *is the key generation algorithm which takes a security parameter λ and a randomness r as input, and returns a keypair consisting of a public key pk and a secret key sk. If clear from the context, we will denote it by $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$.*
- $\mathsf{Enc} \colon \mathcal{P} \times \mathcal{M} \times \mathcal{R} \to \mathcal{C}$ *is the encryption algorithm which takes a public key pk, a message m, and a randomness r as input, and returns a ciphertext c. It will be usually denoted by $c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$ or $c \coloneqq \mathsf{Enc}_{\mathsf{pk}}(m; r)$.*
- $\mathsf{Dec} \colon \mathcal{S} \times \mathcal{C} \to \mathcal{M}$ *is the (deterministic) decryption algorithm[7] which takes as input a secret key sk and a ciphertext c, and returns a message m. It will be usually denoted by $m \coloneqq \mathsf{Dec}_{\mathsf{sk}}(c)$.*

By $\mathcal{P}$, $\mathcal{S}$, $\mathcal{M}$, $\mathcal{C}$, and $\mathcal{R}$, we denote the public key space, secret key space, message space, ciphertext space, and randomness space, respectively.

We assume w.l.o.g. that the randomness space for key generation and encryption are identical. Below we define two notions of correctness for PKE schemes.

Definition 2 (Perfectly Correct PKE) *A PKE scheme $\Sigma = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ is* perfectly correct *if for any $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}$, $m \in \mathcal{M}$, and $r \in \mathcal{R}$, it holds that*

$$\mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{pk}}(m; r)) = m \,.$$

Definition 3 ($(1-\alpha)$-Correct PKE [23]) *A $(1-\alpha)$-correct PKE scheme, or PKE with decryption error α, is a PKE scheme $\Sigma = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ such that, for any $m \in \mathcal{M}$:*

$$\Pr_{\substack{(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen} \\ r \leftarrow \mathcal{R}}} \left[\mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{pk}}(m; r)) \neq m \right] \leq \alpha \,.$$

---

[7] For simplicity here we only consider decryption with *implicit rejection*, that is, such the output is a random value whenever the input is not a well-formed ciphertext for the particular sk. The extension to *explicit rejection* decryption can be done for example by adding a *flag bit* that marks the output as $\perp$ whenever decryption fails.

3   Quantum Indistinguishability for PKE Schemes

In this section we extend the QS2 security notion of qIND-qCPA introduced for SKE schemes in [25] to the public key case. This is much more complex than the symmetric case, for the following reasons:

1. PKE schemes are randomized to achieve cipertext indistinguishability;
2. when derandomizing the encryption procedure and considering the randomness as additional input, there might be collisions (different randomnesses leading to the same ciphertext), hence ensuring reversibility of type-2 operators is not straightforward;
3. many existing schemes, such as lattice- or code-based NIST candidates, suffer from a small decryption failure probability.

In particular, as we will see, there are two main consequences: (1) the inverse of type-2 encryption operators is not generally a type-2 decryption operator; and (2), most interestingly, many type-2 encryption operators can be built efficiently by using only knowledge of the public key. The last point is crucial: it shows that in the PKE case, type-2 encryption operators are much more natural than in the SKE case, and for certain schemes they are actually covered in the usual notion of QS1 "post-quantum" security already. We will also show that some of these schemes are very relevant, such as the LWE-based scheme used as a blueprint for many NIST submissions. In this section we will do the following:

1. First, we revisit and define formally type-1 operators for PKE, and we show the difference between type-1 encryption and decryption (cf. Section 3.1).
2. We define type-2 encryption operators for perfectly correct PKE schemes, and we show that they can be efficiently implemented with knowledge of secret and public key (cf. Section 3.2).
3. We define what we call *recoverable* PKE schemes, i.e., schemes that admit an efficient procedure to recover the message given randomness, ciphertext and public key, without the secret key. We show that for such schemes the 'canonical' type-2 encryption operator can be built by only using the public key, *even* if the scheme is not perfectly correct (cf. Section 3.3).
4. We define the qIND-qCPA security notion for any PKE scheme where one can efficiently build the type-2 encryption operator. This includes in particular perfectly correct and recoverable schemes (cf. Section 3.4).
5. Finally, we discuss how to extend these results to the *chosen ciphertext attack* (CCA) scenario (cf. Section 3.5).

3.1   Type-1 Operators for PKE

Recall that, for an arbitrary function $f : \mathcal{X} \to \mathcal{Y}$, the corresponding type-1 operator is the "canonical" way of computing f on a superposition of input through the unitary operator $U_f : \mathfrak{H}_{\mathcal{X}} \otimes \mathfrak{H}_{\mathcal{Y}} \to \mathfrak{H}_{\mathcal{X}} \otimes \mathfrak{H}_{\mathcal{Y}}$ defined by: $U_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$. Realising U_f is always efficient if f is efficiently computable.

Traditionally, when looking at (deterministic) encryption schemes, the type-1 operator for encryption has been defined as:

$$U_{\texttt{Enc}} : |m, y\rangle \mapsto |m, y \oplus \texttt{Enc}(m)\rangle \ .$$

This is the approach used in, e.g., [15] and [25]. However, in our case of PKE schemes (which are generally randomized), we have to consider that encryption can be performed locally by the quantum adversary, who therefore has full control not only on the randomness used for encryption (i.e., it is necessary to explicitly derandomize the encryption procedure[8]), but also on the public key used (i.e., it is theoretically possible to compute encryption for a superposition of different public keys). Therefore, the most general definition of a type-1 encryption operator would look like:

$$U_{\texttt{Enc}} : |\texttt{pk}, r, m, y\rangle \mapsto |\texttt{pk}, r, m, y \oplus \texttt{Enc}_{\texttt{pk}}(m; r)\rangle \ .$$

We argue that this is the most general and correct way to model the local computational power of a quantum adversary, even in the QS1 case. However, for ease of exposition (and also because it would go beyond the traditional meaning of ciphertext indistinguishability), in the present work we do not consider superpositions of public keys, as we assume that the public key to be attacked is given to the adversary at the beginning of the security game. This leads us to the following definition.

Definition 4 (Type-1 Encryption for PKE) *Let $\Sigma = (\texttt{KGen}, \texttt{Enc}, \texttt{Dec})$ be a PKE scheme and let $(\texttt{pk}, \texttt{sk}) \leftarrow \texttt{KGen}$. The* type-1 encryption operator *for* $\texttt{pk}$ *is the unitary defined by:*

$$U^{(1)}_{\texttt{Enc}_{\texttt{pk}}} : |r, m, y\rangle \mapsto |r, m, y \oplus \texttt{Enc}_{\texttt{pk}}(m; r)\rangle \ .$$

Usually the public key is clear from the context, so we will omit that dependency and just write $U^{(1)}_{\texttt{Enc}}$. As usual, when there is no ambiguity, we identify the corresponding superoperator acting on mixed states rather than pure states with the same symbol $U^{(1)}_{\texttt{Enc}} : \mathfrak{D}(\mathfrak{H}_{\mathcal{R}} \otimes \mathfrak{H}_{\mathcal{M}} \otimes \mathfrak{H}_{\mathcal{C}}) \to \mathfrak{D}(\mathfrak{H}_{\mathcal{R}} \otimes \mathfrak{H}_{\mathcal{M}} \otimes \mathfrak{H}_{\mathcal{C}})$. By letting the randomness be an input, Definition 4 allows to encrypt using a superposition of randomnesses, which is fine in the case of the adversary generating ciphertexts himself. Note also that the case of different randomnesses for each message in superposition can be realised by using a single classical randomness and a QS2-secure pseudorandom function [46], as shown by Boneh and Zhandry [15].

The type-1 decryption operator is defined analogously to Definition 4, but with an important difference: the decryption algorithm does not take the randomness used for encryption as input.

Definition 5 (Type-1 Decryption for PKE) *Let $\Sigma = (\texttt{KGen}, \texttt{Enc}, \texttt{Dec})$ be a PKE scheme and let $(\texttt{pk}, \texttt{sk}) \leftarrow \texttt{KGen}$. The* type-1 decryption operator *for* $\texttt{sk}$ *is the unitary defined by:*

$$U^{(1)}_{\texttt{Dec}_{\texttt{sk}}} : |c, z\rangle \mapsto |c, z \oplus \texttt{Dec}_{\texttt{sk}}(c)\rangle \ .$$

---

[8] This is implicitly considered in [15] and [25], but not explicitly formalized.

As usual we denote it by $U_{\texttt{Dec}}^{(1)}$, leaving the secret key understood, and when there is no ambiguity with the same symbol we denote the superoperator acting on mixed states also by $U_{\texttt{Dec}}^{(1)} : \mathfrak{D}(\mathfrak{H}_{\mathcal{C}} \otimes \mathfrak{H}_{\mathcal{M}}) \to \mathfrak{D}(\mathfrak{H}_{\mathcal{C}} \otimes \mathfrak{H}_{\mathcal{M}})$.

Notice the difference in type-1 encryption and decryption acting on different spaces: this is not surprising, as it is already known that the adjoint of a type-1 encryption operator is not, generally, a type-1 decryption operator. Notice also how both operators are efficiently computable, because Enc and Dec are efficient algorithms. The difference is that realising $U_{\texttt{Dec}}^{(1)}$ requires knowledge of the secret key sk, while for realising $U_{\texttt{Enc}}^{(1)}$ it is sufficient to know the public key pk.

3.2   Type-2 Encryption for PKE

When defining type-2 encryption for PKE schemes, we have to remember that defining these operators only makes sense for functions which are reversible. If a PKE scheme is perfectly correct, then encryption is always reversible if seen as a function of the *plaintext*, but not necessarily as a function of the *randomness*. That is because it might be the case that for a given message different randomnesses lead to the same ciphertext. In the context of security games, message and randomness have very different roles anyway, as one is generally chosen by the adversary, while the other is generally chosen by the challenger.

Ultimately, what we want is to define a type of unitary which generalizes the case of arbitrary permutations from plaintext to ciphertext spaces (the same approach as considered in [25]). In order to avoid the issue raised by randomness collisions, we will keep the auxiliary randomness register both in input and output of the circuit. This ensures reversibility of the operator, because given a certain ciphertext and a certain randomness, there is only one possible plaintext which was mapped to that ciphertext (otherwise we would have a decryption failure, and for now we are only considering perfectly correct schemes). So, if the sizes of the plaintext space and the ciphertext space coincide, i.e., there is no ciphertext expansion and thus $\dim(\mathfrak{H}_{\mathcal{M}}) = \dim(\mathfrak{H}_{\mathcal{C}})$, then we can define the corresponding type-2 encryption operator as:

$$U_{\texttt{Enc}}^{(2)} : |r, m\rangle \mapsto |r, \texttt{Enc}_{\texttt{pk}}(m; r)\rangle \ ,$$

where, as usual, the public key pk is implicit in the definition of $U_{\texttt{Enc}}^{(2)}$, i.e., it is a parameter of the unitary operator in question.

In the more general case of message expansion, i.e., $\dim(\mathfrak{H}_{\mathcal{M}}) < \dim(\mathfrak{H}_{\mathcal{C}})$, we use the same approach as in [25]: we introduce an auxiliary register in a complementary space $\mathfrak{H}_{\mathcal{C}-\mathcal{M}}$[9] that ensures reversibility of the operation, and

---

[9] We denote by $\mathfrak{H}_{\mathcal{C}-\mathcal{M}}$ a Hilbert space such that $\mathfrak{H}_{\mathcal{M}} \otimes \mathfrak{H}_{\mathcal{C}-\mathcal{M}}$ is isomorphic to $\mathfrak{H}_{\mathcal{C}}$. Notice that the opposite case, i.e., $\dim(\mathfrak{H}_{\mathcal{M}}) > \dim(\mathfrak{H}_{\mathcal{C}})$, cannot happen because it would lead to collisions on the ciphertexts and thus introduce decryption failures. Also notice that, as in [25], the case of adversarially-controlled ancilla qubits is left as an open problem.

which is initialized to $|0\ldots0\rangle$ during an honest execution to yield a correct encryption. So we consider a family of unitary superoperators of the form:

$$U : \mathfrak{D}(\mathfrak{H}_\mathcal{R} \otimes \mathfrak{H}_\mathcal{M} \otimes \mathfrak{H}_{\mathcal{C}-\mathcal{M}}) \to \mathfrak{D}(\mathfrak{H}_\mathcal{R} \otimes \mathfrak{H}_\mathcal{C}), \text{ such that}$$
$$U : |r, m, y\rangle\langle r, m, y| \mapsto \psi,$$

and we define a type-2 encryption operator any arbitrary, efficiently computable (purified) representative of the above family such that:

$$U^{(2)}_{\mathtt{Enc}} : |r, m, 0\ldots0\rangle \mapsto |r, \mathtt{Enc_{pk}}(m; r)\rangle. \tag{1}$$

The choice of the particular representative is irrelevant in our exposition as long as it respects (1) above and it is efficiently computable. However, as already discussed in [25], it might be the case that realising this operator requires knowledge of the secret key, not only of the public key. This finally leads to the following.

Definition 6 (Type-2 Encryption for PKE) *Let $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ be a perfectly correct PKE scheme, and let $(\mathtt{pk}, \mathtt{sk}) \leftarrow \mathtt{KGen}$. A type-2 encryption operator for Σ is an efficiently computable unitary in the family defined by:*

$$U^{(2)}_{(\mathtt{Enc}, \mathtt{pk}, \mathtt{sk})} : |r, m, 0\ldots0\rangle \mapsto |r, \mathtt{Enc_{pk}}(m; r)\rangle.$$

It will be usually denoted by just $U^{(2)}_{\mathtt{Enc}}$ when there is no ambiguity.

It is always possible to find and efficiently sample and implement at least one valid representative for $U^{(2)}_{\mathtt{Enc}}$ given the secret and public keys, by using a conversion circuit of type-1 encryption and decryption operators in a similar way as presented in [25]. We call this the *canonical* type-2 operator.

Theorem 7 (Efficient Realisation of Type-2 Encryption) *Let Σ be a perfectly correct PKE scheme with $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$, and let $(\mathtt{pk}, \mathtt{sk}) \leftarrow \mathtt{KGen}$. Then there exists an efficient procedure which takes $\mathtt{pk}$ and $\mathtt{sk}$ as input, and outputs a polynomial-size quantum circuit realising $U^{(2)}_{\mathtt{Enc}}$.*

Proof. The explicit circuit of the procedure is shown in Fig. 2. It uses type-1 encryption and decryption operators as underlying components, which are both efficient with knowledge of the respective keys. □

Notice that realising this canonical type-2 operator requires knowledge of the secret key, even if it is just an encryption operator, but that is fine because as previously mentioned type-2 operators usually require this additional knowledge. We have to make a distinction between the encryption *unitary* as defined above (a quantum gate modelling local computation of encryption by a party with knowledge of the relevant keys) and the encryption *oracle* (modelling the interaction of the adversary with such party, usually the challenger). By letting the randomness be an input, Definition 6 allows to encrypt using a superposition of randomnesses, which is fine in the case of a party generating ciphertexts himself. In our security notion, however, the (honest) challenger will always produce
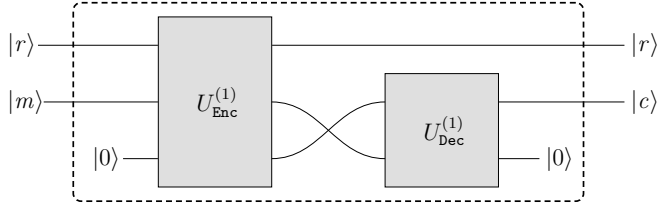
Fig. 2: Canonical type-2 encryption operator for perfectly correct PKE schemes.

ciphertexts using a (secret) classical randomness not controlled by the adversary. In the security game, the challenger cannot send the randomness register back to $\mathcal{A}$, because knowledge of the randomness used would trivially break security, even in a classical scenario. But at the same time if the challenger withholds the randomness register, from $\mathcal{A}$'s perspective this would be equivalent to tracing it out, and if the type-2 encryption operator introduces entanglement between ciphertext and randomness output registers, then tracing out the randomness would disturb the ciphertext state.

Luckily, a simple observation solves this dilemma: as we have already discussed, in our oracle case the randomness is chosen by the (honest) challenger during the challenge query, so we can safely model it as classical.[10] Looking at Definition 6, this means that the output state is always separable as $|r\rangle\langle r| \otimes \psi$. Therefore, in our oracle definition the randomness register can be discarded after applying the type-2 encryption without disturbing the ciphertext state. This leads to the following.

Definition 8 (Type-2 Encryption Oracle) *Let* $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ *be a PKE scheme and let* $(\mathtt{pk}, \mathtt{sk}) \leftarrow \mathtt{KGen}$. *The* type-2 *encryption oracle* $O_{\mathtt{Enc}}^{(2)}$ *for* $\mathtt{pk}$ *is defined by the following procedure:*

Oracle $O_{\mathtt{Enc}}^{(2)}(\varphi)$ *on input* $\varphi \in \mathfrak{D}(\mathfrak{H}_{\mathcal{M}})$

1: $\quad r \xleftarrow{\$} \mathcal{R}$

2: $\quad |r\rangle\langle r| \otimes \psi \coloneqq U_{\mathtt{Enc}}^{(2)} \left(|r\rangle\langle r| \otimes \varphi \otimes |0\ldots0\rangle\langle0\ldots0| \right)$

3: $\quad$ *trace out* $|r\rangle\langle r|$

4: $\quad$ **return** ψ

3.3 Recoverable PKE Schemes

Now we introduce a special case of PKE schemes where it is possible to decrypt a ciphertext *without* knowledge of the secret key, but having access to the randomness used for the encryption instead. These schemes might not be perfectly

---

[10] Even if considering challengers that use superpositions of randomnesses, we show in Appendix B that the difference is irrelevant, and that we can always restrict ourselves to the case of a classical randomness register.

correct, so the decryption procedure might fail on some ciphertext, yet still the recovery procedure will 'decrypt' correctly if the right randomness is provided. We will see in Section 4 that many PKE schemes are actually of this type.

Definition 9 (Recoverable PKE Scheme) *Let* $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ *be a (not necessarily perfectly correct) PKE scheme. We call* Σ *a recoverable PKE scheme if there exists an efficient algorithm* $\mathtt{Rec} : \mathcal{P} \times \mathcal{R} \times \mathcal{C} \to \mathcal{M}$ *such that, for any* $\mathsf{pk} \in \mathcal{P}, r \in \mathcal{R}, m \in \mathcal{M}$, *it holds that*

$$\mathtt{Rec}(\mathsf{pk}, r, \mathtt{Enc}_{\mathsf{pk}}(m; r)) = m \,.$$

Notice how the recovery procedure will always allow to avoid decryption failures even for schemes which do not have full correctness. We will sometimes write a recoverable scheme $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ with recovery algorithm $\mathtt{Rec}$ directly as $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec}, \mathtt{Rec})$. Given pk, it is of course possible to define a type-1 operator for $\mathtt{Rec}$ in the canonical way.

Definition 10 (Type-1 Recovery for PKE) *Let* $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec}, \mathtt{Rec})$ *be a recoverable PKE scheme, and let* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathtt{KGen}$. *The* type-1 recovery operator *for* pk *is the unitary defined by:*

$$U^{(1)}_{\mathtt{Rec}_{\mathsf{pk}}} : |r, c, z\rangle \mapsto |r, c, z \oplus \mathtt{Rec}_{\mathsf{pk}}(r, c)\rangle \,.$$

As usual we will denote this operator by $U^{(1)}_{\mathtt{Rec}}$ when there is no ambiguity in the choice of pk, and with the same symbol we denote the superoperator acting on mixed states, i.e., $U^{(1)}_{\mathtt{Rec}} : \mathfrak{D}(\mathfrak{H}_{\mathcal{R}} \otimes \mathfrak{H}_{\mathcal{C}} \otimes \mathfrak{H}_{\mathcal{M}}) \to (\mathfrak{H}_{\mathcal{R}} \otimes \mathfrak{H}_{\mathcal{C}} \otimes \mathfrak{H}_{\mathcal{M}})$.

Now, the crucial observation is the following: for recoverable PKE schemes, the canonical type-2 encryption operator can be efficiently implemented using only the public key.

Theorem 11 (Type-2 Encryption Operator for Recoverable Schemes) *Let* $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec}, \mathtt{Rec})$ *be a recoverable PKE, and let* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathtt{KGen}$. *Then there exists an efficient procedure which only takes* pk *as input, and outputs a polynomial-size quantum circuit realising the canonical operator* $U^{(2)}_{\mathtt{Enc}}$.

Proof. The explicit circuit of the procedure is shown in Fig. 3. It uses type-1 encryption and recovery operators as underlying components, which are both efficient with knowledge of the public key only. Realisation of both these components is independent of the fact whether the scheme has full correctness or not, as the decryption algorithm itself is never used. □

In particular, for recoverable PKE schemes the type-2 encryption operator can be realised locally by a quantum adversary (or a reduction), without need of additional oracle access. This, together with the fact that most real-world PKE schemes are recoverable (as we will see in Section 4) shows that type-2 encryption operators are very natural, and unlike in the symmetric key case considered in [25] they also appear implicitly in QS1 security notions for such schemes.
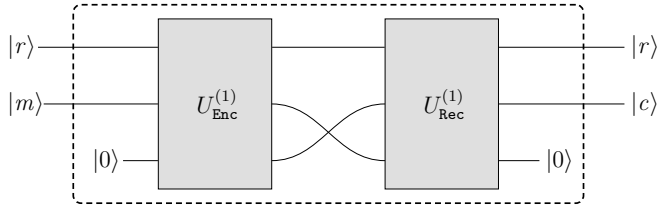
14

Fig. 3: Canonical type-2 encryption operator for recoverable PKE schemes.

3.4 The qIND-qCPA Security Notion

We are now ready to define the notion of *quantum ciphertext indistinguishability under quantum chosen plaintext attack* (qIND-qCPA) for PKE schemes which admit an efficient construction of the canonical type-2 encryption operator $U_{\mathtt{Enc}}^{(2)}$. This includes in particular perfectly correct schemes and recoverable schemes.[11] We follow the approach in [25] and we define a game where a polynomially bounded quantum adversary plays against an external challenger. We have to define the challenge phase and the learning (quantum CPA) phases (pre- and post-challenge), using the theory of type-2 operators we have devised so far.

For the challenge query it is pretty straightforward: as in the original qIND security definition for symmetric key encryption, we assume that the challenger $\mathcal{C}$ generates a keypair and sends the public key pk to the adversary $\mathcal{A}$. Then $\mathcal{A}$ sends two plaintext quantum states (possibly mixed) φ_0, φ_1 to $\mathcal{C}$, who will flip a random bit $b \leftarrow \{0, 1\}$, discard (trace out) φ_{1-b}, and encrypt the other message with the type-2 encryption oracle $\psi \leftarrow O_{\mathtt{Enc}}^{(2)}(\varphi_b)$. Finally, ψ is sent back to $\mathcal{A}$, who will have to guess b in order to win the game.

Justifying the use of a type-2 encryption during the challenge phase requires arguments different from the symmetric key case. In the classical IND-CPA game for PKE, the challenger does not even need to know the secret key, as it is not needed for encryption, and we saw already that the secret key is sometimes necessary to implement the canonical type-2 encryption operator. However, in the QS2 case the challenger can produce ciphertext-encoding quantum states with very different structure depending on whether he knows the secret key or not, thereby leading to different attack models. Type-2 encryption operators in particular are more general in this respect, and allow us to aim for a stronger security notion. Moreover we also saw how certain schemes, like the recoverable ones, allow to build the type-2 operator using only the public key. Thus it makes sense for a QS2 security notion to include the use of type-2 operators during the challenge phase.

The other question we have to address, which was left unspecified in [25], is about the learning (qCPA) phase. Shall the adversary be able to perform only

---

[11] As we will see, these cover all the interesting cases in practice, although there might be other classes of schemes which allow an efficient construction of $U_{\mathtt{Enc}}^{(2)}$; we address the general case in Section 5.

type-1 encryption operations, or type-2 as well? In the QS1 case the answer is obvious: it depends on the scheme, e.g., for recoverable schemes both type-1 and type-2 operations are allowed, but in the general case only type-1 operations should. Instead, in the QS2 case that we are considering, the answer is less straightforward. For recoverable schemes again there is no difference, as the adversary can implement both types of operators locally. But for general schemes there might be a difference, and there might exist non-recoverable PKE schemes which become insecure when giving oracle access to a type-2 encryption operator during the learning phase.[12]

In our definition of qIND-qCPA we opt for giving to the adversary as much power as possible, hence explicitly giving access to a type-2 encryption oracle when dealing with non-recoverable schemes, both in the learning and challenge phases. The reason for this choice is twofold. First, this allows us to aim for potentially stronger security notions. Second, remember that, classically, CPA attacks model not only the case where the adversary can compute ciphertexts himself (as in the case of PKE), but also scenarios where the adversary can "trick" an honest encryptor in providing certain ciphertexts (as in the case of IND-CPA security for symmetric key encryption). In the quantum PKE setting, there is a difference whether these ciphertexts are computed locally by the adversary or obtained by the challenger through "trickery" (including scenarios already considered in [25], such as quantum side-channel attacks, quantum obfuscation, etc.), because the challenger has knowledge of the secret key, and is therefore capable of generating type-2 ciphertexts even if the scheme is non-recoverable. So, giving the adversary access to the type-2 encryption oracle seems to be the "safe" choice.

These considerations finally lead to the following.

Experiment 12 *The* qIND-qCPA *experiment* qIND-qCPA$(\Sigma, \mathcal{A}, \lambda)$ *for a PKE scheme* $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ *is defined as follows:*

1: $\mathcal{C}$ *runs* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathtt{KGen}$ *and implements* $O^{(2)}_{\mathtt{Enc}}$
2: $\mathcal{A}^{O^{(2)}_{\mathtt{Enc}}}(\mathsf{pk}) \rightarrow (\varphi_0, \varphi_1, \sigma_{state})$
3: $\mathcal{C}$ *receives* φ_0, φ_1 *and does the following:*
   - *flips* $b \xleftarrow{\$} \{0, 1\}$
   - *traces out* φ_{1-b}
   - *calls* $\psi \leftarrow O^{(2)}_{\mathtt{Enc}}(\varphi_b)$
   - *sends* ψ *to* $\mathcal{A}$
4: $\mathcal{A}^{O^{(2)}_{\mathtt{Enc}}}(\sigma_{state}, \psi) \rightarrow b' \in \{0, 1\}$
5: ***if*** $b = b'$ ***then return*** *win;* ***else return*** *rej.*

Security is defined as negligible advantage over guessing.

---

[12] For example, one could combine a suitable separating SKE scheme with the canonical hybrid construction (cf. Section 4.3), so that the separation property is 'inherited' by the resulting PKE scheme. We are not aware of an explicit example of such SKE scheme and we leave this as an open problem. We stress that such a counterexample is not found in [18], as the authors there "excluded [...] notations that [...] combine quantum learning queries with quantum challenge queries of different query models."

Definition 13 (qIND-qCPA **Security**) *A public key encryption scheme Σ has quantum ciphertext indistinguishability under quantum chosen plaintext attack, or is* qIND-qCPA-*secure, iff for any QPT adversary $\mathcal{A}$ it holds:*

$$\left| \Pr\left[\mathsf{qIND\text{-}qCPA}(\Sigma, \mathcal{A}, \lambda) \to win \right] - \frac{1}{2} \right| \leq \mathrm{negl}(\lambda) .$$

It is easy to show that the above notion is at least as strong as the QS1 notion of IND-qCPA for PKE introduced in [15]. Before we show this, let us first recall some game-based notation [11,44]. Let G be a game (or experiment) instantiated with a cryptographic scheme Σ and $\mathcal{A}$ be an adversary. We write $\mathbf{Adv}_{\Sigma}^{\mathsf{G}}(\mathcal{A})$ to denote the advantage of $\mathcal{A}$ in game G instantiated with Σ, e.g., $\mathbf{Adv}_{\Sigma}^{\mathrm{qIND\text{-}qCPA}}(\mathcal{A})$ for the qIND-qCPA advantage against Σ. If the scheme is clear from the context, we simply write $\mathbf{Adv}^{\mathsf{G}}(\mathcal{A})$. For games G_1 and G_2, we write $\mathbf{Adv}\left(\mathsf{G}_1^{\mathcal{A}}, \mathsf{G}_2^{\mathcal{A}} \right)$ for the advantage of adversary $\mathcal{A}$ in distinguishing the games.

Theorem 14 (qIND-qCPA $\Rightarrow$ IND-qCPA) *Let $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ be a PKE scheme. For any adversary $\mathcal{A}$, it holds that*

$$\mathbf{Adv}^{\mathrm{IND\text{-}qCPA}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{qIND\text{-}qCPA}}(\mathcal{A}) .$$

Proof. We show that any adversary $\mathcal{A}$ wins the qIND-qCPA game with at least the same probability of winning the IND-qCPA game; the latter (Experiment 27) is described in Appendix A. The differences with Experiment 12 are:

1. In the IND-qCPA game $\mathcal{A}$ does not get oracle access to $O_{\mathtt{Enc}}^{(2)}$. Hence, when switching to qIND-qCPA, the winning probability cannot decrease, because the power of the adversary is augmented by the type-2 oracle.
2. In the IND-qCPA game $\mathcal{A}$ is restricted to classical challenge messages m_0, m_1. When switching to qIND-qCPA, the adversary will simply use quantum states $|m_0\rangle, |m_1\rangle$ as challenge plaintexts instead, and will measure the quantum ciphertext received by the challenger.

Notice in fact that, since the randomness r in the qIND-qCPA challenge query is classical, the type-2 operator $U_{\mathtt{Enc}}^{(2)}$ will produce a ciphertext state which is just a classical ciphertext encoded as a basis state $|c = \mathtt{Enc}_{\mathsf{pk}}(m; r)\rangle$. In other words, quantum plaintexts are *more generic* than classical plaintexts (or, to put it differently, classical plaintexts are a very special case of quantum plaintexts), and hence again the power of the adversary is not diminished when switching to the qIND-qCPA game. $\qquad\square$

3.5   The CCA Case

We leave the case of extending our exposition to the quantum chosen ciphertext attack case (with the relevant notions of qIND-qCCA1 and qIND-qCCA2) as future work, but we want anyway to sketch here the general strategy.

The first task is to formalize a type-2 operator for decryption. Unlike in the symmetric key setting considered in [25], this is not necessarily going to be the

adjoint of the type-2 encryption operator, and in particular it might not require a randomness register as input; this has to be expected given that there is already an asymmetry in the definition of type-1 encryption and decryption operators in the public key setting. Then, in the qIND-qCCA1 case, we just extend the qIND-qCPA experiment by also providing the adversary with oracle access to the type-1 and type-2 decryption operators.

Extending the framework to the qIND-qCCA2 case is not straightforward, mainly due to no-cloning and the destructive nature of quantum measurement. In fact, this case was left as an open problem already in [25] for the symmetric key setting. Fortunately, the technique presented in [5] shows how to overcome this difficulty, by using a real-VS-ideal approach which makes it possible to differentiate the behaviour of the adversary when replaying the challenge ciphertext to the decryption oracle, hence effectively detecting a challenge replay attack. The approach in [5] (and its extension to the public key case presented in [4]) is given in the context of *quantum encryption schemes* (a scenario which falls under the QS3 domain in [24]), but it is easy to generalize to the QS2 notions we are considering here.

4 Security Analysis for Real-World PKE Schemes

We analyse the qIND-qCPA security of several real-world public key encryption schemes. We start with the canonical LWE-based PKE scheme in Section 4.1, followed by the code-based PKE scheme ROLLO-II in Section 4.2. The hybrid encryption scheme is analysed in Section 4.3 while Section 4.4 concludes with a discussion of these results.

4.1 Results for LWE-Based PKE

In this section we analyse the canonical LWE-based public key encryption scheme due to Regev [41] with respect to our qIND-qCPA security notion.

LWE-Based Public Key Encryption Schemes. The canonical LWE-based encryption scheme has been proposed by Regev [41]. It underpins most lattice-based PKE schemes such as Kyber [16], LIMA [8], the LP scheme [34], and the schemes underlying NewHope [40] and LAC [35]. The pseudocode (that we give for simplicity in a generic form, i.e., not specifying concrete domains and distributions for the parameters) is given in Fig. 4. Its security is based on the computational hardness of the *Learning With Errors (LWE)* lattice problem. The canonical LWE-based scheme works on n-dimensional vectors of elements of $\mathbb{Z}_q$ for $q \geq 2$. The functions Encode and Decode are used for encoding and decoding bit strings to and from elements of $(\mathbb{Z}_q)^n$. The Decode function has a certain error tolerance which, upon being exceeded, results in a decryption failure.

The Encode function maps the bits of the message into the high-order bit representation of group elements, which are then represented as a vector. For

our purpose, it is not important here to have a precise definition of this encoding function, nor to have a detailed discussion on the the sampling distribution of the LWE vectors – which is generally crucial for proving the security of the scheme. We leave these details to an appropriate reference, for example [37]. In this section, we will only consider the following, simplified characterization of the encoding function.

Lemma 15 (Canonical LWE-Based Message Encoding Representation)
Let $\mathsf{Encode} : m \mapsto \mathsf{v}$ *as from Figure 4, and let* $\mathsf{Bit}(\mathsf{v})$ *the canonical bit string representation in use for a vector element* v *over a finite group* $\mathbb{Z}_q$. *Then there exists a public efficient invertible permutation* π *and an integer* $\tau \geq 0$ *such that*

$$\mathsf{Bit}(\mathsf{Encode}(m)) = \pi \left(m \| \overbrace{0 \ldots 0}^{\tau} \right).$$

In particular, for $q = 2$, *it holds* $\tau = 0$ *and* $\mathsf{Bit}(\mathsf{Encode}(m)) = \pi(m)$.

Notice that in practice the parameter τ denotes the expansion factor between m and c_1 in Fig. 4 and is upper bounded by $n \cdot \lceil \log_2(q) \rceil$ minus the bit size of the message. The larger τ, the less efficient the scheme is in terms of ciphertext size but the lower the decryption failure rate.

$\mathtt{KGen}(\lambda; r)$	$\mathtt{Enc}(\mathsf{pk}, m; r)$
$\mathsf{a}, \mathsf{s}, \mathsf{e} \coloneqq r$	**parse** pk **as** (a, b)
$\mathsf{b} \coloneqq \mathsf{as} + \mathsf{e}$	$\mathsf{e}_1, \mathsf{e}_2, \mathsf{d} \coloneqq r$
$\mathsf{pk} \coloneqq (\mathsf{a}, \mathsf{b})$	$c_1 \coloneqq \mathsf{bd} + \mathsf{e}_1 + \mathsf{Encode}(m)$
$\mathsf{sk} \coloneqq \mathsf{s}$	$c_2 \coloneqq \mathsf{ad} + \mathsf{e}_2$
return $(\mathsf{sk}, \mathsf{pk})$	**return** $c \coloneqq (c_1, c_2)$

Fig. 4: Pseudocode of the canonical LWE-based public key encryption scheme $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$. For the randomness r used by $\mathtt{KGen}$ and $\mathtt{Enc}$, let $x \coloneqq r$ denote that x is deterministically derived from r. The decryption algorithm is omitted, as it is irrelevant for this work.

Recall that qIND-qCPA security can only be defined for schemes which admit an efficient realisation of a type-2 encryption operator. Showing this for the canonical LWE scheme is hence our first goal.

Lemma 16 *The canonical LWE-based PKE scheme* $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$, *shown in Fig. 4, is recoverable as from Definition 9.*

Proof. To prove the statement, we have to specify the algorithm $\mathtt{Rec}$ that is introduced in Definition 9. Its input is a public key $\mathsf{pk} = (\mathsf{a}, \mathsf{b})$, a randomness r, and a ciphertext $c = (c_1, c_2)$ such that c corresponds to the encryption of a message m, using the public key pk and randomness r. The algorithm $\mathtt{Rec}$

proceeds as follows. Given the randomness r, it obtains the same values e_1, e_2, and d that have been derived from r during encryption and outputs

$$\mathsf{Decode}(c_1 - \mathsf{bd} - \mathsf{e}_1) = \mathsf{Decode}(\mathsf{bd} + \mathsf{e}_1 + \mathsf{Encode}(m) - \mathsf{bd} - \mathsf{e}_1)$$
$$= \mathsf{Decode}(\mathsf{Encode}(m)) = m\,.$$

This concludes the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\Box$

QS2 Attack For LWE-Based PKE Schemes. Here we give an attack against the canonical LWE-based scheme for the case $q = 2$. We leave the case of arbitrary q as an open problem, albeit we conjecture that the distinguishing attack can be adapted to the general case.

Theorem 17 (Attack Against Canonical LWE Scheme for $q = 2$). *Let Σ be the canonical LWE-based PKE scheme shown in Fig. 4 defined over $\mathbb{Z}_q$ with $q = 2$. Then there exists an efficient distinguishing adversary $\mathcal{A}$ that wins the experiment* qIND-qCPA$(\Sigma, \mathcal{A})$ *with probability* 1.

Proof. First of all recall that, because $q = 2$, group elements are just represented as bits. This means that $\tau = 0$ (there is no padding nor message expansion) and $\mathsf{Bit}(\mathsf{Encode}(m)) = \pi(m)$. Moreover, addition is performed by XORing elements bitwise. The distinguishing adversary $\mathcal{A}$ performs a single quantum challenge query using the Hadamard basis state $H\,|0\dots0\rangle$ (an uniform superposition of all messages) as a first quantum plaintext φ_0, and the state $H\,|1\dots1\rangle$ as a second quantum plaintext.

$$\varphi_0 = H\,|0\dots0\rangle = \sum_m \frac{1}{\sqrt{2^{|m|}}}\,|m\rangle\,,\;\; \varphi_1 = H\,|1\dots1\rangle = \sum_m \frac{1}{\sqrt{2^{|m|}}}(-1)^{\mathsf{parity}(m)}\,|m\rangle\,.$$

Upon receiving back the ciphertext ψ, $\mathcal{A}$ does the following:

1. traces out the second part of the ciphertext, corresponding to c_2 in Fig. 4;
2. applies to the resulting state (a type-2 operator of) π^{-1} (cf. Lemma 15);
3. measures the resulting state in the Hadamard basis;
4. if the outcome is $0\dots0$ then output 0, otherwise output 1.

We now analyse the attack. If the challenge bit is 0, then the state $\varphi_0 = H\,|0\dots0\rangle$ is encrypted. The resulting ψ is:

$$O_{\mathsf{Enc}}^{(2)}\left(\sum_m \frac{1}{\sqrt{2^{|m|}}}\,|m\rangle\right) = \sum_m \frac{1}{\sqrt{2^{|m|}}}\,|\mathsf{Enc}(m)\rangle = \sum_m \frac{1}{\sqrt{2^{|m|}}}\,|c_1^{(m)}\rangle \otimes |c_2\rangle\,;$$

where $c_1^{(m)}$ is the c_1 part of the ciphertext (cf. Fig. 4) related to superposition element m, while the second part c_2 is independent of the underlying plaintext. The two corresponding registers are hence unentangled, and after tracing out the second, $\mathcal{A}$ has the state

$$\sum_m \frac{1}{\sqrt{2^{|m|}}}\,|c_1^{(m)}\rangle = \sum_m \frac{1}{\sqrt{2^{|m|}}}\,|\mathsf{u} + \mathsf{Encode}(m)\rangle = \sum_m \frac{1}{\sqrt{2^{|m|}}}\,|\mathsf{u} + \pi(m)\rangle\,;$$

for an unknown element u. Looking at the bit representation of u and writing $\pi^{-1}(u) = w$, from Lemma 15 the state above can be written as

$$\sum_m \frac{1}{\sqrt{2^{|m|}}} |u \oplus \pi(m)\rangle = \sum_m \frac{1}{\sqrt{2^{|m|}}} |\pi(w \oplus m)\rangle \ .$$

Undoing π finally yields:

$$\sum_m \frac{1}{\sqrt{2^{|m|}}} |w \oplus m\rangle = H |0 \ldots 0\rangle \ ;$$

which will give outcome $0 \ldots 0$ on a Hadamard measurement with probability 1.

On the other hand, if the challenge bit is 1, then the state $\varphi_1 = |1 \ldots 1\rangle$ is encrypted. A similar computation as before shows that the outcome of the encryption is another Hadamard state orthogonal to $H |0 \ldots 0\rangle$, so the outcome of $\mathcal{A}$'s final measurement will be different from $0 \ldots 0$ with probability 1. $\qquad \square$

4.2 Results for Code-based PKE

In this section we analyse the code-based PKE scheme ROLLO-II [10] with respect to our qIND-qCPA security notion. It turns out that, due to the one-time pad encryption, ROLLO-II is not qIND-qCPA-secure.

Code-Based Public Key Encryption ROLLO-II. The encryption scheme ROLLO-II [10] is a code-based public key encryption scheme based on rank metric codes. The scheme in a generic, simplified form is displayed in Fig. 5, where O is a random oracle, Supp describes the support of vectors, and P is a polynomial from the underlying code problem.

$\mathtt{KGen}(\lambda; r)$	$\mathtt{Enc}(\mathsf{pk}, m; r)$
$\mathbf{x}, \mathbf{y} \coloneqq r$	$\mathbf{e}_1, \mathbf{e}_1 \coloneqq r$
$\mathbf{h} \coloneqq \mathbf{x}^{-1}\mathbf{y} \bmod \mathsf{P}$	$\mathsf{E} \coloneqq \mathsf{Supp}(\mathbf{e}_1, \mathbf{e}_2)$
$\mathsf{sk} \coloneqq (\mathbf{x}, \mathbf{y})$	$c_1 \coloneqq m \oplus \mathsf{O}(\mathsf{E})$
$\mathsf{pk} \coloneqq \mathbf{h}$	$c_2 \coloneqq \mathbf{e}_1 + \mathbf{e}_2\mathbf{h} \bmod \mathsf{P}$
$\mathbf{return}\ (\mathsf{pk}, \mathsf{sk})$	$\mathbf{return}\ c \coloneqq (c_1, c_2)$

Fig. 5: Pseudocode of the code-based public key encryption scheme ROLLO-II. For the randomness r used by $\mathtt{KGen}$ and $\mathtt{Enc}$, let $x \coloneqq r$ denote that x is deterministically derived from r. The decryption algorithm is omitted since it is irrelevant for our work.

We first show that ROLLO-II is recoverable, and hence admits a qIND-qCPA security definition.

Lemma 18 *The code-based PKE scheme ROLLO-II, shown in Fig. 5, is recoverable as from Definition 9.*

Proof. To prove the statement, we have to specify the algorithm Rec that is introduced in Definition 9. Its input is a public key $\mathsf{pk} = \mathbf{h}$, a randomness r, and a ciphertext $c = (c_1, c_2)$, such that c corresponds to the encryption of a message m, using the public key pk and randomness r. The algorithm Rec proceeds as follows. Given the randomness r, it obtains the same values $\mathbf{e}_1$ and $\mathbf{e}_1$ that have been derived from r during encryption. It then computes $\mathsf{O}(\mathsf{Supp}(\mathbf{e}_1, \mathbf{e}_1))$ and outputs $c_1 \oplus \mathsf{O}(\mathsf{Supp}(\mathbf{e}_1, \mathbf{e}_1))$. □

At this point, we would like to point out that the code-based PKE schemes which underlie the NIST proposals BigQuake [21], HQC [1], and RQC [2] are recoverable as well.

QS2 Attack against ROLLO-II. We give an explicit attack against the qIND-qCPA security of ROLLO-II. It is an Hadamard distinguisher that exploits the fact that the message is essentially encrypted using a one-time pad (ciphertext part c_1 in Fig. 5).

Theorem 19 *Let Σ be the code-base PKE scheme ROLLO-II shown in Fig. 5. Then there exists an efficient distinguishing adversary $\mathcal{A}$ that wins the experiment* qIND-qCPA$(\Sigma, \mathcal{A})$ *with probability* $\frac{3}{4}$.

Proof. In the challenge phase, the adversary $\mathcal{A}$ prepares the two states $\varphi_0 = |0 \dots 0\rangle$ and $\varphi_1 = \sum_m \frac{1}{\sqrt{2^{|m|}}} |m\rangle$ and sends them to the challenger. Upon receiving the challenge ciphertext ψ, $\mathcal{A}$ traces out the register $|c_2\rangle$ and measures the resulting state in the Hadamard basis. If the measurement outcome is 0, $\mathcal{A}$ outputs 1, otherwise, it outputs 0.

If the secret bit b is 1, the state φ_1 is encrypted. Then the state ψ is

$$O_{\mathsf{Enc}}^{(2)} \left(\sum_m \frac{1}{\sqrt{2^{|m|}}} |m\rangle \right) = \sum_m \frac{1}{\sqrt{2^{|m|}}} |\mathsf{Enc}(m)\rangle = \sum_m \frac{1}{\sqrt{2^{|m|}}} |c_1^{(m)}\rangle \otimes |c_2\rangle \ ;$$

where $c_1^{(m)}$ is the c_1 part of the ciphertext (cf. Fig. 5) related to superposition element m, while the second part c_2 is independent of the underlying plaintext. Hence, the two corresponding registers are unentangled, and after tracing out the second, $\mathcal{A}$ gets the state

$$\sum_m \frac{1}{\sqrt{2^{|m|}}} |c_1^{(m)}\rangle = \sum_m \frac{1}{\sqrt{2^{|m|}}} |m \oplus \mathsf{O}(\mathsf{E})\rangle = \sum_m \frac{1}{\sqrt{2^{|m|}}} |m\rangle = |+\rangle \ ;$$

hence measuring in the Hadamard basis yields 0 with probability 1.

If the secret bit b is 0, the state φ_0 is encrypted and the outcome of the final Hadamard measurement will be a 0 or 1, each with probability 50%, which concludes the proof. □

We note that the attack also works against the code-based scheme BigQuake [21] which uses the same one-time pad approach to encrypt the message.

4.3 Results for Hybrid Encryption

In this section we analyse the canonical hybrid encryption scheme with respect to our qIND-qCPA security notion. We show that its security mainly depends on the underlying symmetric key encryption scheme.

Hybrid Encryption Scheme. The canonical hybrid PKE-SKE encryption scheme combines a public key encryption and a symmetric key encryption scheme into a public key encryption scheme. That is, a message is encrypted using a fresh one-time key of the symmetric encryption scheme. The one-time key is then encrypted using the public key encryption scheme, whereupon the encrypted one-time key is attached to the ciphertext. To decrypt, one first recovers the symmetric one-time key, and then uses it to decrypt the ciphertext containing the message. The canonical hybrid encryption scheme is shown in Fig. 6. For additional background on symmetric key encryption schemes and the security notion used in this section, see Appendix A.

$\texttt{KGen}(\lambda)$	$\texttt{Enc}_{\mathsf{pk}}(m; r)$	$\texttt{Dec}_{\mathsf{sk}}(c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \texttt{KGen}^P(\lambda)$	**parse** r **as** (r_1, r_2, r_3)	**parse** c **as** (c_1, c_2)
return $(\mathsf{pk}, \mathsf{sk})$	$\mathsf{k} := \texttt{KGen}^S(\lambda; r_1)$	$\mathsf{k} := \texttt{Dec}^P_{\mathsf{sk}}(c_2)$
	$c_1 := \texttt{Enc}^S_{\mathsf{k}}(m; r_2)$	$m := \texttt{Dec}^S_{\mathsf{k}}(c_1)$
	$c_2 := \texttt{Enc}^P_{\mathsf{pk}}(\mathsf{k}; r_3)$	**return** m
	return (c_1, c_2)	

Fig. 6: Hybrid encryption scheme $\Sigma = (\texttt{KGen}, \texttt{Enc}, \texttt{Dec})$ built from a PKE scheme $\Sigma^P = (\texttt{KGen}^P, \texttt{Enc}^P, \texttt{Dec}^P)$ and an SKE scheme $\Sigma^S = (\texttt{KGen}^S, \texttt{Enc}^S, \texttt{Dec}^S)$.

Below we show that the canonical hybrid encryption scheme is recoverable. Given the randomness, the used one-time key can be obtained, which allows to decrypt the ciphertext part that contains the message. We emphasise that the hybrid encryption scheme is recoverable even if the underlying PKE scheme is not recoverable.

Lemma 20 *The canonical hybrid encryption scheme* $\Sigma = (\texttt{KGen}, \texttt{Enc}, \texttt{Dec})$, *shown in Fig. 6, is recoverable as from Definition 9.*

Proof. To prove the statement, we have to specify the algorithm $\texttt{Rec}$ that is introduced in Definition 9. Its input is a public key pk, a randomness r, and a ciphertext $c = (c_1, c_2)$, such that c corresponds to the encryption of a message m, using the public key pk and randomness r. The algorithm $\texttt{Rec}$ proceeds as follows. Given the randomness r, it obtains r_1, r_2, and r_3, which have been derived from r during encryption. It then computes $\mathsf{k} := \texttt{KGen}^S(\lambda; r_1)$ and outputs $\texttt{Dec}^S_{\mathsf{k}}(c_1)$. This concludes the proof. □

qIND-qCPA Security of Hybrid Encryption. We now turn our attention towards the QS2 security of the hybrid encryption scheme. It turns out that the QS2 security depends on the underlying SKE scheme, while the underlying PKE scheme merely requires QS1 security. This is formalised in the theorem below.

Theorem 21 (QS2 Security of Hybrid Encryption) *Let $\Sigma = (\mathtt{KGen}, \mathtt{Enc},$ $\mathtt{Dec})$ be the hybrid encryption scheme built from an SKE scheme $\Sigma^S = (\mathtt{KGen}^S,$ $\mathtt{Enc}^S, \mathtt{Dec}^S)$ and a PKE scheme $\Sigma^P = (\mathtt{KGen}^P, \mathtt{Enc}^P, \mathtt{Dec}^P)$, as shown in Fig. 6. For any adversary $\mathcal{A}$ against Σ, there exist adversaries $\mathcal{B}$ and $\mathcal{C}$ against Σ^P and Σ^S, respectively, such that*

$$\mathbf{Adv}_{\Sigma}^{\mathrm{qIND\text{-}qCPA}}(\mathcal{A}) \leq \mathbf{Adv}_{\Sigma^P}^{\mathrm{IND\text{-}qCPA}}(\mathcal{B}) + \mathbf{Adv}_{\Sigma^S}^{\mathrm{qIND}}(\mathcal{C})\,.$$

Proof. The proof uses two games G_0 and G_1, where G_0 is the qIND-qCPA security game instantiated with Σ, and G_1 is the same except that the ciphertext part c_2 is replaced by encrypting a random key k' rather than k. It holds that

$$\mathbf{Adv}_{\Sigma}^{\mathrm{qIND\text{-}qCPA}}(\mathcal{A}) = \mathbf{Adv}\left(\mathsf{G}_0^{\mathcal{A}}, \mathsf{G}_1^{\mathcal{A}}\right) + \mathbf{Adv}^{\mathsf{G}_1}(\mathcal{A})\,.$$

We construct the following adversary $\mathcal{B}$ which receives a public key pk as input. It flips a bit b at random and runs $\mathcal{A}$ on the same public key pk. It answers every learning query φ by $\mathcal{A}$ by generating a one-time key k, asking its own challenger for an encryption of this key to obtain the ciphertext $|c_2\rangle$, locally computes $|c_1\rangle$ by applying the type-2 encryption operator $U_{\mathtt{Enc}^S}^{(2)}$ to φ, and sends the ciphertext back to $\mathcal{A}$. For the challenge query φ_0, φ_1 by $\mathcal{A}$, $\mathcal{B}$ picks two (classical) keys k and k', applies the type-2 encryption operator $U_{\mathtt{Enc}_{\mathsf{k}}^S}^{(2)}$, using key k, to φ_b to obtain $|c_1\rangle$, obtains $|c_2\rangle$ by sending k and k' to its own challenger, and sends the ciphertext back to $\mathcal{A}$. When $\mathcal{A}$ guesses the bit b correctly, $\mathcal{B}$ outputs 0, otherwise, it outputs 1. It holds that $\mathcal{B}$ perfectly simulates G_0 and G_1, depending on its own challenge, hence

$$\mathbf{Adv}\left(\mathsf{G}_0^{\mathcal{A}}, \mathsf{G}_1^{\mathcal{A}}\right) \leq \mathbf{Adv}_{\Sigma^P}^{\mathrm{IND\text{-}qCPA}}(\mathcal{B})\,.$$

Next we transform an adversary $\mathcal{A}$, playing G_1, into an qIND adversary $\mathcal{C}$ against Σ^S. The adversary $\mathcal{C}$ generates a key pair $(\mathsf{pk},\mathsf{sk})$ for the underlying PKE, which allows to perform all operations related to the PKE scheme. It runs $\mathcal{A}$ on the public key pk and answers any learning query by generating a key k which it uses to encrypt the query by $\mathcal{A}$ and then encrypts this key using the PKE scheme. The challenge query φ_0, φ_1 by $\mathcal{A}$ is forwarded by $\mathcal{C}$ as its own challenge to obtain the ciphertext $|c_2\rangle$, while the ciphertext $|c_1\rangle$ is computed locally by encrypting a randomly generated key k using the PKE scheme. When $\mathcal{A}$ outputs its guess, $\mathcal{C}$ forwards it as its own output. It holds that $\mathcal{C}$ perfectly simulated game G_1 for $\mathcal{A}$, with the same secret bit as its qIND security game, thus it holds that

$$\mathbf{Adv}^{\mathsf{G}_1}(\mathcal{A}) \leq \mathbf{Adv}_{\Sigma^S}^{\mathrm{qIND}}(\mathcal{C})\,.$$

Collecting the bounds above proves the statement. □

Theorem 21 reveals that to achieve our qIND-qCPA security notion, we can instantiate the hybrid encryption scheme with a PKE that merely achieves QS1 security. This allows the usage of ROLLO-II, which, used as a stand-alone PKE scheme, is not qIND-qCPA-secure.

In the following we show that Theorem 21 is strict. If the underlying SKE is not qIND-secure, then the resulting hybrid scheme is not qIND-qCPA-secure, irrespectively of the underlying PKE scheme. This is shown in the theorem below. Examples for SKE schemes which are not qIND-secure are given in [25].

Theorem 22 *Let* $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ *be the hybrid encryption scheme built from an SKE scheme* $\Sigma^S = (\mathtt{KGen}^S, \mathtt{Enc}^S, \mathtt{Dec}^S)$ *and a PKE scheme* $\Sigma^P = (\mathtt{KGen}^P, \mathtt{Enc}^P, \mathtt{Dec}^P)$, *as shown in Fig. 6. Assume that there exists an adversary* $\mathcal{A}$ *which has some non-negligible advantage* ε *against the* qIND *security of* Σ^S. *Then there exists an adversary* $\mathcal{B}$ *against* Σ *such that*

$$\mathbf{Adv}_{\Sigma}^{\mathrm{qIND\text{-}qCPA}}(\mathcal{B}) \geq \varepsilon\,.$$

Proof. We construct the adversary $\mathcal{B}$, which uses adversary $\mathcal{A}$ as subroutine, as follows. When $\mathcal{A}$ outputs its challenge messages φ_0 and φ_1, $\mathcal{B}$ forwards these to its own challenger. Upon receiving the challenge ciphertext $\psi = |c_1\rangle \otimes |c_2\rangle$, $\mathcal{B}$ sends $|c_1\rangle$ to $\mathcal{A}$. When $\mathcal{A}$ outputs its guess b', $\mathcal{B}$ outputs b' as its own guess. It holds that $\mathcal{B}$ perfectly simulates the qIND security experiment, with the same challenge bit b, for $\mathcal{A}$. By outputting the same bit as $\mathcal{A}$, we have

$$\mathbf{Adv}_{\Sigma}^{\mathrm{qIND\text{-}qCPA}}(\mathcal{B}) \geq \mathbf{Adv}_{\Sigma^S}^{\mathrm{qIND}}(\mathcal{A}) = \varepsilon\,,$$

which proves the claim. □

4.4 Discussion

In this section, we gave both positive and negative examples regarding the QS2 security of real-world public key encryption schemes. We gave a concrete attack against the canonical LWE-based scheme for the case $q = 2$ and an attack against the code-based scheme ROLLO-II showing that these schemes are qIND-qCPA insecure. These results, however, considered that the scheme are used as public key encryption schemes to encrypt the actual message. On the other hand, Theorem 21 reveals that both ROLLO-II and the canonical LWE-based scheme are sufficient to achieve qIND-qCPA secure when used as a key encapsulation mechanism, together with a QS2-secure SKE scheme.

The standardization effort by NIST focuses on the latter scenario, hence our results show that for these standardized schemes it is sufficient to achieve QS1 security in order for the resulting KEM to achieve our stronger, more conservative security notion. At the same time, our results also show that extra cautiousness is necessary when these standardized schemes are deployed directly as PKE schemes in protocols that require security in the QS2 sense.

5 Classifying Other Public Key Encryption Schemes

So far we have built a framework for QS2 security of PKE schemes which are perfectly correct or recoverable (or both). But what about schemes which do not fall in either of these two categories? Are there such examples at all? And what can we learn from this? In this section, we initiate the classification of PKE schemes in general, extend our results to other classes of PKE schemes where possible, and point out the obstacles in other cases.

5.1 Dealing with Decryption Failures: The General Case

First, we discuss why arbitrary non-correct PKE schemes do not allow, in general, to define a type-2 encryption operator and, consequently, we cannot always define the qIND-qCPA game as from Experiment 12. However, we also discuss a possible workaround.

First of all, recall that defining a type-2 operator is only possible for functions that are inherently invertible. Then observe that a $(1 - \alpha)$-correct PKE scheme (cf. Definition 3) could have arbitrary, even overwhelming decryption error α. In the most extreme case, the scheme can be almost identical to a constant function (for example, consider an artificial scheme where every public key pk always encrypts to 0, except for one particular randomness $\bar{r}$ where it produces a correctly decryptable ciphertext instead). In the presence of decryption failures, it is therefore impossible to find a general way to define type-2 operators for encryption, and hence, to define a suitable qIND-qCPA security notion.[13]

We call *non-isometric* such schemes, where it is simply not possible to define a unitary operator that behaves *exactly* as from Definition 6 for any keypair, even if we drop the requirement of efficiency.

Definition 23 (Non-Isometric Schemes) *Let $\Sigma = (\texttt{KGen}, \texttt{Enc}, \texttt{Dec})$ be a PKE scheme. We say that Σ is* non-isometric *if, for any $(\texttt{pk}, \texttt{sk}) \leftarrow \texttt{KGen}$, there exists at least a randomness r_{pk} such that the function $m \mapsto \texttt{Enc}_{\mathsf{pk}}(m; r_{\mathsf{pk}})$ is non-injective. In particular, for any unitary U acting on the appropriate Hilbert spaces, there exists at least a pair $(m_{\mathsf{pk}}, r_{\mathsf{pk}})$ such that:*

$$\Pr\left[M(U \ket{r_{\mathsf{pk}}, m_{\mathsf{pk}}, 0, \ldots, 0}) \to (r_{\mathsf{pk}}, \texttt{Enc}_{\mathsf{pk}}(m_{\mathsf{pk}}; r_{\mathsf{pk}}))\right] < 1 \,,$$

where M denotes measurement in the canonical computational base.

A possible workaround for these non-isometric schemes is to 'enforce' the reversibility of the encryption, obtaining a new type of encryption unitary. Consider what happens if we want to use the type-1 encryption operator (cf. Definition 4) during the challenge query:

$$U_{\texttt{Enc}_{\mathsf{pk}}}^{(1)} : \ket{r, m, y} \mapsto \ket{r, m, y \oplus \texttt{Enc}_{\mathsf{pk}}(m; r)} \,.$$

---

[13] Recoverable schemes are a special case: they might not be always reversible in the message space only, but they are always reversible in the union of message space and randomness space.

As already observed, the randomness r can be understood as classical and discarded by the challenger. However, the other two registers are generally going to be entangled, and both would have to be sent to the adversary for a meaningful quantum notion; but this would clearly break security because the message would remain in clear.[14] We could try to 'fix' this issue by (reversibly) masking the message register sent to the adversary, for example by using a permutation π on the message space drawn uniformly at random. The following unitary:

$$U_{\mathtt{Enc_{pk}}}^{(\pi)} : |r, m, y\rangle \mapsto |r, \pi(m), y \oplus \mathtt{Enc_{pk}}(m; r)\rangle$$

allows hence to define a new type of quantum challenge query, where the challenger still discards the randomness register after encryption, but sends back the other two registers to the adversary. Notice how, from the adversary's point of view, $\pi(m)$ is a completely random element, and therefore the presence of this additional register does not offer any distinguishing advantage. Moreover, in actual security reductions, the uniformly drawn π can be replaced by a quantum-secure pseudorandom permutation [25], or QPRP in short.

We can hence use these *type-π operators* to define (for *any* PKE scheme, including the non-isometric ones) a new indistinguishability game and a related security notion with quantum challenge query. Motivating the use of such operators when modelling security is arguably non-trivial. In certain cases, one could see $\pi(m)$ as some sort of side-channel information given to the adversary, but in general it looks like just an artificial way to enforce reversibility on schemes which are not. We will therefore not study the resulting security notion in this work, but we want nevertheless to make a few observations on it.

First of all, notice that such a new security notion cannot be stronger than qIND-qCPA, at least when considering correct or recoverable schemes. As a separating example, consider the distinguishing attack from Theorem 22: this will not work any more because of the presence of the entangled $\pi(m)$ register, so that the hybrid scheme might be secure according to the new notion but still qIND-qCPA insecure.

Second, notice how the challenge query resulting from the use of type-π operators reminds of the one given in an alternative quantum indistinguishability notion for secret key encryption schemes proposed by Mossayebi and Schack [36] - the difference is basically producing $|m, \mathtt{Enc_{pk}}(\pi(m))\rangle$ instead of $|\pi(m), \mathtt{Enc_{pk}}(m)\rangle$ - which is itself not comparable to qIND-qCPA. This security notion has been recently investigated and expanded by Chevalier et al. [19].

5.2 Refining the Classification

Now we know how to define qIND-qCPA security of PKE schemes which are perfectly correct or recoverable (or both), and at the same time we know that it is not possible for schemes that are non-isometric. But it turns out we can say more. First of all we make a distinction for those schemes which *are* isometric:

---

[14] This explanation appears in detail in [25].

it means that it is possible to define a unitary operator that behaves exactly as a type-2 encryption operator, but we distinguish whether finding and building such operator is efficient or not.

Definition 24 ((Efficiently) Isometric Schemes) *Let Σ be a PKE scheme with $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$. We say that Σ is* isometric *if, for any $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathtt{KGen}$ and for any randomness r the function $m \mapsto \mathtt{Enc}_{\mathsf{pk}}(m; r)$ is injective. In particular, there exists a unitary U acting on the appropriate Hilbert spaces, such that for any (m, r):*

$$\Pr\left[M(U \left|r, m, 0, \ldots, 0\rangle\right) \to (r, \mathtt{Enc}_{\mathsf{pk}}(m; r))\right] = 1\,,$$

where M denotes measurement in the canonical computational base. Furthermore, we say that Σ is efficiently isometric *if U can be efficiently realised.*

Notice how, in general, an isometric scheme is not necessarily efficiently isometric. This is because, unlike for type-1 operators, the efficiency of the $\mathtt{Enc}$ procedure is only enough to guarantee the existence of a unitary U with the above property, but not its *efficiency*. Then, notice how a type-2 encryption operator (as from Definition 6) satisfies the above definition of U, both by construction and by efficiency. In other words, efficiently isometric schemes are exactly all and only those schemes which, by definition, admit an efficient construction of the type-2 encryption operator. Clearly, in particular this includes perfectly correct schemes (by Theorem 7) and recoverable schemes (by Theorem 11).

Corollary 25 *Let Σ be a PKE scheme. If Σ is perfectly correct or recoverable, then it is efficiently isometric.*

The situation is depicted in Fig. 7. This means that, as from Definition 13, we can extend the qIND-qCPA security notion not only to recoverable or perfectly correct schemes, but to all the efficiently isometric ones. For the non-efficient case (arbitrary isometric schemes) the qIND-qCPA notion can still be defined, but its usefulness would be less clear, as it might require unbounded challengers in the security game (and therefore, difficulty in simulating them by efficient reductions when proving the security of a particular scheme). Still, it would be useful for *impossibility results*, i.e., proving that a particular isometric scheme is not qIND-qCPA-secure.

Finally, can we find representative examples of schemes which fall in the categories that we have just defined? We have already mentioned an example of a non-isometric scheme at the beginning of Section 5.1 (the almost-constant one). Here we show a construction of an efficiently isometric scheme that is neither perfectly correct nor recoverable. The construction is given in Fig. 8: it transforms a recoverable, not perfectly correct encryption scheme by pre-processing the message with a quantum-secure trapdoor permutation [24] before encrypting it, and inverts again the permutation after decryption (the public and secret keys of the trapdoor permutation are embedded in the public and secret key, respectively, of the resulting scheme). It works because the permutation 'scrambles' the resulting ciphertexts but not the randomness, thereby hindering an
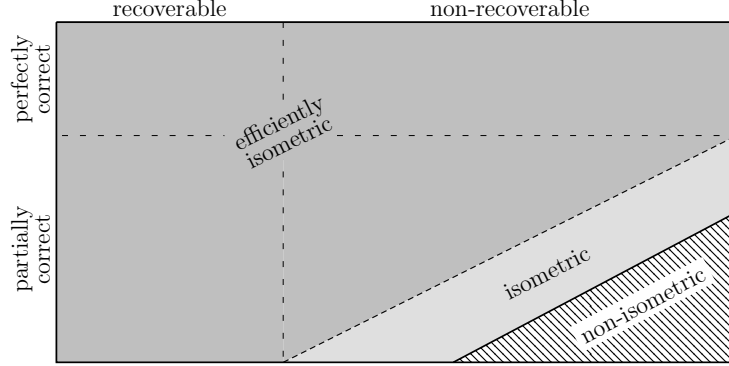
Fig. 7: Classification of PKE schemes. The qIND-qCPA security notion can be defined for all schemes except those in the shaded area (non-isometric). For efficiently isometric schemes (dark gray area) the type-2 operator can be realised efficiently and we provide concrete circuits for the schemes that are perfectly correct or recoverable. For isometric schemes (light gray area) the type-2 operator can be realised but not efficiently.

adversary (or a challenger) who tries to build an efficient recovery algorithm $\mathtt{Rec}$ for the transformed scheme. At the same time, we show how such construction is efficiently isometric, by showing an efficient circuit for the canonical type-2 encryption operator $U_{\mathtt{Enc}}^{(2)}$. This is formalised in the theorem below.

$\mathtt{KGen}(\lambda)$	$\mathtt{Enc}_{\mathsf{pk}}(m; r)$	$\mathtt{Dec}_{\mathsf{sk}}(c)$
$(\mathsf{pk}_e, \mathsf{sk}_e) \leftarrow \mathtt{KGen}^{\Sigma}(\lambda)$	**parse** pk **as** $(\mathsf{pk}_e, \mathsf{pk}_f)$	**parse** sk **as** $(\mathsf{sk}_e, \mathsf{sk}_f)$
$(\mathsf{pk}_f, \mathsf{sk}_f) \leftarrow \mathtt{KGen}^{F}(\lambda)$	$y := \mathtt{F}(\mathsf{pk}_f, m)$	$y := \mathtt{Dec}^{\Sigma}(\mathsf{sk}_e, c)$
$\mathsf{pk} := (\mathsf{pk}_e, \mathsf{pk}_f)$	$c := \mathtt{Enc}^{\Sigma}(\mathsf{pk}_e, y; r)$	$m := \mathtt{F}^{-1}(\mathsf{sk}_f, y)$
$\mathsf{sk} := (\mathsf{sk}_e, \mathsf{sk}_f)$	**return** c	**return** m
return $(\mathsf{pk}, \mathsf{sk})$		

Fig. 8: Transformed scheme Γ, where $\Sigma = (\mathtt{KGen}^{\Sigma}, \mathtt{Enc}^{\Sigma}, \mathtt{Dec}^{\Sigma})$ is a PKE scheme and $\Pi = (\mathtt{KGen}^{F}, \mathtt{F}, \mathtt{F}^{-1})$ is a deterministic trapdoor permutation.

Theorem 26 *Let $\Pi = (\mathtt{KGen}^{F}, \mathtt{F}, \mathtt{F}^{-1})$ be a deterministic trapdoor permutation and $\Sigma = (\mathtt{KGen}^{\Sigma}, \mathtt{Enc}^{\Sigma}, \mathtt{Dec}^{\Sigma})$ be a PKE scheme. If Π is quantum-secure and Σ is recoverable and $(1-\alpha)$-correct, then the scheme $\Gamma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ depicted in Fig. 8 is $(1 - \alpha)$-correct, non-recoverable, and efficiently isometric PKE.*

Proof. Partial correctness of the encryption scheme Γ follows immediately from the partial correctness of Σ, as permuting the messages does not change the overall decryption failure probability.

Assume, for sake of contradiction, that Γ is recoverable. Then there exists an efficient algorithm Rec that, on input pk, r, and $\mathrm{Enc}_{\mathsf{pk}}(m; r)$, outputs m. We construct the following adversary $\mathcal{B}$ against the trapdoor permutation Π. He receives a public key pk_f for the trapdoor permutation F along with $y := \mathsf{F}_{\mathsf{pk}_f}(x)$ for a random x, and is asked to find x. $\mathcal{B}$ computes $(\mathsf{pk}_e, \mathsf{sk}_e) \leftarrow \mathtt{KGen}^{\Sigma}(\lambda)$, chooses $r \leftarrow \mathcal{R}$, computes $c := \mathrm{Enc}^{\Sigma}_{\mathsf{pk}_e}(y; r)$, and uses $\mathsf{pk} = (\mathsf{pk}_e, \mathsf{pk}_f), r, c$ as an input to Rec. By construction, we have $c = \mathrm{Enc}^{\Sigma}_{\mathsf{pk}_e}(\mathsf{F}_{\mathsf{pk}_f}(x); r) = \mathrm{Enc}_{\mathsf{pk}}(x; r)$, hence Rec outputs x. So $\mathcal{B}$ can find the correct preimage with probability 1, hence breaking the security of the trapdoor permutation. This contradicts the recoverability of Γ.

Finally, in Fig. 9 we show an efficient circuit for the realisation of $U^{(2)}_{\mathrm{Enc}}$. This uses subcircuits for computing the type-1 operator for the trapdoor permutation and its inverse (given the trapdoor permutation's public key and secret key), and type-1 encryption and recovery for the underlying PKE scheme. □
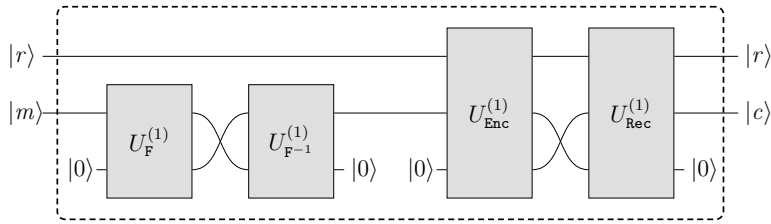

Fig. 9: Efficient realisation of the canonical type-2 encryption operator for the construction shown in Fig. 8.

Remark 1. Note that, albeit the above construction works at a theoretical level, there are currently no known candidates for quantum-secure trapdoor permutations. Alternatively, a quantum-secure *injective trapdoor function* could be used instead, for which candidates exist. In this case, because of the inherent expansion factor, the message space for the transformed scheme will be smaller than the one in the original PKE scheme.

6 Future Directions

In this work we have filled the existing gap between the symmetric key and the public key case when defining security in the QS2 setting. We showed how the existence of this gap was not due to a mere lack of interest, but because of non-trivial definitional issues that we solved. We believe that our results provide useful guidelines in the security analysis of quantum-resistant PKE, but many research directions remain open to exploration.

In Section 3.5 we sketch a general strategy for extending our results to the chosen ciphertext case. Although we believe that such a strategy works, we leave it as an open problem to formalize it correctly. We also leave it as an open problem to improve our game-based definitions to different provable security paradigms such as simulation-based.

We notice how our notions of qIND-qCPA for PKE can be also used to study the security of cryptographic primitives that 'extend' PKE with extra functionalities. Such primitives include, for example, fully homomorphic encryption [17,26], identity-based encryption [47], and functional encryption [14].

We did not found any natural example of a scheme that is isometric, yet not efficiently so. A simple idea would be to modify the construction from Fig. 8 in such a way that the circuit provided in Fig. 9 becomes non-efficient (for example by using a hard to invert permutation instead of a trapdoor permutation). This idea does not work for two reasons. First, it would only show that *this* particular construction of the type-2 operator is inefficient, while we would need to show that *any* construction is. Second, and more importantly, switching to a hard to invert permutation would make the decryption algorithm inefficient. Hence the resulting scheme would no longer be a PKE scheme according to Definition 1.

Also, notice the following: given that qIND-qCPA is a stronger notion than IND-qCPA, having a PKE scheme where it is not even possible to define a type-2 encryption operator can actually be *desirable*. For such a scheme in fact, one should not worry about proving the (stricter) qIND-qCPA security notion, because the related attack scenario is simply not enforceable, and hence the scheme cannot be broken in a qIND-qCPA sense. So it would be interesting to find schemes which are IND-qCPA secure but non-isometric. We conjecture that a generic transformation to obtain such schemes is possible assuming the existence of quantum-secure *indistinguishability obfuscation*, but leave the problem open to further study.

We have also left unstudied the possibility of extending QS2 security notions to the use of type-π operators, and to models where the adversary can query oracles on superpositions of public keys.

Acknowledgements

References

1. C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, E. Persichetti, and G. Zémor. HQC. Technical report, National In-

stitute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

2. C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, G. Zémor, A. Couvreur, and A. Hauteville. RQC. Technical report, National Institute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

3. G. Alagic, A. Broadbent, B. Fefferman, T. Gagliardoni, C. Schaffner, and M. S. Jules. Computational security of quantum encryption. In A. C. A. Nascimento and P. Barreto, editors, *ICITS 16*, volume 10015 of *LNCS*, pages 47–71. Springer, Heidelberg, Aug. 2016.

4. G. Alagic, T. Gagliardoni, and C. Majenz. Can you sign a quantum state. *IACR Cryptology ePrint Archive*, 2018:1164, 2018.

5. G. Alagic, T. Gagliardoni, and C. Majenz. Unforgeable quantum encryption. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 489–519. Springer, Heidelberg, Apr. / May 2018.

6. G. Alagic, C. Majenz, A. Russell, and F. Song. Quantum-access-secure message authentication via blind-unforgeability. In A. Canteaut and Y. Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 788–817. Springer, Heidelberg, May 2020.

7. G. Alagic and A. Russell. Quantum-secure symmetric-key cryptography based on hidden shifts. In J.-S. Coron and J. B. Nielsen, editors, *EUROCRYPT 2017, Part III*, volume 10212 of *LNCS*, pages 65–93. Springer, Heidelberg, Apr. / May 2017.

8. M. R. Albrecht, E. Orsini, K. G. Paterson, G. Peer, and N. P. Smart. Tightly secure ring-LWE based key encapsulation with short ciphertexts. In S. N. Foley, D. Gollmann, and E. Snekkenes, editors, *ESORICS 2017, Part I*, volume 10492 of *LNCS*, pages 29–46. Springer, Heidelberg, Sept. 2017.

9. M. V. Anand, E. E. Targhi, G. N. Tabia, and D. Unruh. Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation. In T. Takagi, editor, *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016*, pages 44–63. Springer, Heidelberg, 2016.

10. N. Aragon, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, O. Ruatta, J.-P. Tillich, G. Zémor, C. Aguilar Melchor, S. Bettaieb, L. Bidoux, M. Bardet, and A. Otmani. ROLLO. Technical report, National Institute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

11. M. Bellare and P. Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In S. Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 409–426. Springer, Heidelberg, May / June 2006.

12. D. J. Bernstein, J. Buchmann, and E. Dahmen. Post-quantum cryptography, 2009.

13. D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In D. H. Lee and X. Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Heidelberg, Dec. 2011.

14. D. Boneh, A. Sahai, and B. Waters. Functional encryption: Definitions and challenges. In Y. Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 253–273. Springer, Heidelberg, Mar. 2011.

15. D. Boneh and M. Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 361–379. Springer, Heidelberg, Aug. 2013.

16. J. W. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé. CRYSTALS - kyber: A cca-secure module-lattice-based KEM. In *2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018*, pages 353–367, 2018.

17. A. Broadbent and S. Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 609–629. Springer, Heidelberg, Aug. 2015.

18. T. V. Carstens, E. Ebrahimi, G. Tabia, , and D. Unruh. On quantum indistinguishability under chosen plaintext attack. Cryptology ePrint Archive, Report 2020/596, 2020. https://eprint.iacr.org/2020/596.

19. 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.

20. S. Chow, P. A. Eisen, H. Johnson, and P. C. van Oorschot. White-box cryptography and an AES implementation. In K. Nyberg and H. M. Heys, editors, *SAC 2002*, volume 2595 of *LNCS*, pages 250–270. Springer, Heidelberg, Aug. 2003.

21. A. Couvreur, M. Bardet, E. Barelli, O. Blazy, R. Canto-Torres, P. Gaborit, A. Otmani, N. Sendrier, and J.-P. Tillich. BIG QUAKE. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

22. I. Damgård, J. Funder, J. B. Nielsen, and L. Salvail. Superposition attacks on cryptographic protocols. In C. Padró, editor, *ICITS 13*, volume 8317 of *LNCS*, pages 142–161. Springer, Heidelberg, 2014.

23. C. Dwork, M. Naor, and O. Reingold. Immunizing encryption schemes from decryption errors. In C. Cachin and J. Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 342–360. Springer, Heidelberg, May 2004.

24. T. Gagliardoni. *Quantum Security of Cryptographic Primitives*. PhD thesis, Darmstadt University of Technology, Germany, 2017.

25. T. Gagliardoni, A. Hülsing, and C. Schaffner. Semantic security and indistinguishability in the quantum world. In M. Robshaw and J. Katz, editors, *CRYPTO 2016, Part III*, volume 9816 of *LNCS*, pages 60–89. Springer, Heidelberg, Aug. 2016.

26. C. Gentry. Fully homomorphic encryption using ideal lattices. In M. Mitzenmacher, editor, *41st ACM STOC*, pages 169–178. ACM Press, May / June 2009.

27. L. K. Grover. A fast quantum mechanical algorithm for database search. In *28th ACM STOC*, pages 212–219. ACM Press, May 1996.

28. G. Ito, A. Hosoyamada, R. Matsumoto, Y. Sasaki, and T. Iwata. Quantum chosen-ciphertext attacks against Feistel ciphers. In M. Matsui, editor, *CT-RSA 2019*, volume 11405 of *LNCS*, pages 391–411. Springer, Heidelberg, Mar. 2019.

29. M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In M. Robshaw and J. Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 207–237. Springer, Heidelberg, Aug. 2016.

30. M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Quantum differential and linear cryptanalysis. *IACR Trans. Symm. Cryptol.*, 2016(1):71–94, 2016. http://tosc.iacr.org/index.php/ToSC/article/view/536.

31. E. Kashefi, A. Kent, V. Vedral, and K. Banaszek. Comparison of quantum oracles. *Physical Review A*, 65(5):050304, 2002.

32. H. Kuwakado and M. Morii. Quantum distinguisher between the 3-round feistel cipher and the random permutation. In *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, pages 2682–2685, 2010.

33. H. Kuwakado and M. Morii. Security on the quantum-type even-mansour cipher. In *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, pages 312–316, 2012.

34. R. Lindner and C. Peikert. Better key sizes (and attacks) for LWE-based encryption. In A. Kiayias, editor, *CT-RSA 2011*, volume 6558 of *LNCS*, pages 319–339. Springer, Heidelberg, Feb. 2011.

35. X. Lu, Y. Liu, D. Jia, H. Xue, J. He, Z. Zhang, Z. Liu, H. Yang, B. Li, and K. Wang. LAC. Technical report, National Institute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

36. S. Mossayebi and R. Schack. Concrete security against adversaries with quantum superposition access to encryption and decryption oracles. *CoRR*, abs/1609.03780, 2016.

37. M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila. FrodoKEM. Technical report, National Institute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

38. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, New York, NY, USA, 10th edition, 2011.

39. N. I. of Standards and Technology. Post-quantum cryptography standardization process, 2017.

40. T. Poppelmann, E. Alkim, R. Avanzi, J. Bos, L. Ducas, A. de la Piedra, P. Schwabe, D. Stebila, M. R. Albrecht, E. Orsini, V. Osheter, K. G. Paterson, G. Peer, and N. P. Smart. NewHope. Technical report, National Institute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

41. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In H. N. Gabow and R. Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.

42. M. Rötteler and R. Steinwandt. A note on quantum related-key attacks. *Inf. Process. Lett.*, 115(1):40–44, 2015.

43. P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, Nov. 1994.

44. V. Shoup. Sequences of games: a tool for taming complexity in security proofs. Cryptology ePrint Archive, Report 2004/332, 2004. http://eprint.iacr.org/2004/332.

45. J. Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009.

46. M. Zhandry. How to construct quantum random functions. In *53rd FOCS*, pages 679–687. IEEE Computer Society Press, Oct. 2012.

47. M. Zhandry. Secure identity-based encryption in the quantum random oracle model. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, Heidelberg, Aug. 2012.

48. M. Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In A. Boldyreva and D. Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 239–268. Springer, Heidelberg, Aug. 2019.

A   Additional Preliminaries

A.1   IND-qCPA Security of Public Key Encryption Schemes

The security game for IND-qCPA security [15] of public key encryption schemes is defined as follows. We note that this notion is equivalent to the standard QS1 security notion for public key encryption schemes.

Experiment 27 *The* IND-qCPA *experiment* $\mathsf{IND\text{-}qCPA}(\Sigma, \mathcal{A}, \lambda)$ *for a PKE scheme* $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ *is defined as follows:*

1: $\mathcal{C}$ *runs* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathtt{KGen}$
2: $\mathcal{A}(\mathsf{pk}) \rightarrow (m_0, m_1, \sigma_{state})$
3: $\mathcal{C}$ *receives* m_0, m_1 *and does the following:*
    - *flips* $b \xleftarrow{\$} \{0, 1\}$
    - *samples* $r \xleftarrow{\$} \mathcal{R}$
    - *computes* $\mathtt{Enc}_{\mathsf{pk}}(m_b; r) \rightarrow c$
    - *sends* c *to* $\mathcal{A}$
4: $\mathcal{A}(\sigma_{state}, c) \rightarrow b' \in \{0, 1\}$
5: **if** $b = b'$ **then return** *win;* **else return** *rej.*

Security is defined as negligible advantage over guessing in winning the security game.

Definition 28 (IND-qCPA**, PKE**) *A PKE scheme* Σ *has* ciphertext indistinguishability under quantum chosen plaintext attack*, or it is* IND-qCPA*-secure, iff for any QPT adversary* $\mathcal{A}$ *it holds:*

$$\left| \Pr\left[\mathsf{IND\text{-}qCPA}(\Sigma, \mathcal{A}, \lambda) \rightarrow win \right] - \frac{1}{2} \right| \leq \mathrm{negl}(\lambda).$$

A.2   Symmetric Key Encryption

Below we define symmetric key encryption (SKE) schemes.

Definition 29 *A symmetric key encryption* (SKE) *scheme* Σ *is a tuple of three efficient algorithms* $(\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ *such that:*

- $\mathtt{KGen} \colon \mathbb{N} \rightarrow \mathcal{K}$ *is the (randomized) encryption algorithm which takes a security parameter* λ *as input, and returns a key* k.
- $\mathtt{Enc} \colon \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$ *is the (randomized) encryption algorithm which takes a key* k *and a message* m *as input, and returns a ciphertext* c.
- $\mathtt{Dec} \colon \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$ *is the decryption algorithm which takes as input a key* k *and a ciphertext* c, *and returns a message* m.

By $\mathcal{K}$, $\mathcal{M}$, *and* $\mathcal{C}$, *we denote the key space, message space, and ciphertext space, respectively.*

Next, we define the security game for qIND security, following [25].

Experiment 30 *The* qIND *experiment* $\mathsf{qIND}(\Sigma, \mathcal{A}, \lambda)$ *for a SKE scheme* $\Sigma = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ *is defined as follows:*

1: $\mathcal{C}$ *runs* $\mathsf{k} \leftarrow \mathtt{KGen}(\lambda)$ *and implements* $O_{\mathtt{Enc}}^{(2)}$
2: $\mathcal{A}() \rightarrow (\varphi_0, \varphi_1, \sigma_{state})$
3: $\mathcal{C}$ *receives* φ_0, φ_1 *and does the following:*
     - *flips* $b \xleftarrow{\$} \{0, 1\}$
     - *traces out* φ_{1-b}
     - *calls* $\psi \leftarrow O_{\mathtt{Enc}}^{(2)}(\varphi_b)$
     - *sends* ψ *to* $\mathcal{A}$
4: $\mathcal{A}(\sigma_{state}, \psi) \rightarrow b' \in \{0, 1\}$
5: **if** $b = b'$ **then return** *win;* **else return** *rej.*

Just as for our new security notion, security is defined as negligible advantage over guessing in winning the game.

Definition 31 (qIND, **SKE**) *A SKE scheme* Σ *has* quantum ciphertext indistinguishability, *or it is* qIND-*secure, iff for any QPT adversary* $\mathcal{A}$ *it holds:*

$$\left| \Pr\left[\mathsf{qIND}(\Sigma, \mathcal{A}, \lambda) \rightarrow win \right] - \frac{1}{2} \right| \leq \mathrm{negl}(\lambda) \,.$$

B   The Role of Randomness Superposition

In this section we discuss the possibility of having superposition of randomness in the type-2 challenge query. So far, we have only considered the case of classical randomness, as this is chosen by the (honest) challenger. But one could consider scenarios where the adversary can somehow trick the challenger into using a superposition of randomness in the challenge query. Here we discuss two possible ways to deal with this issue, one of which turns out to be unachievable while the other yields a notion equivalent to the one we propose in Section 3.

Assume that the challenger chooses a superposition of randomness to encrypt one of the messages chosen by the adversary. Following our security experiment, the challenger would keep the randomness register and merely send the ciphertext register to the adversary. The crucial observation is that the registers containing the randomness and the ciphertext are now entangled. As observed in [25], withholding the randomness register is equivalent to measuring it from the point of view of the adversary. This means that this approach would in fact be equivalent to our security notion using a classical randomness.

Alternatively, to prevent the aforementioned issue of entanglement between the challenger and the adversary, we might let the challenger send the randomness register to the adversary. However, the resulting security notion is unachievable as it would allow the adversary to always distinguish encryptions. We illustrate this with the following attack. First, the adversary chooses two distinct classical messages m_0, m_1, and executes the qIND challenge query with these two. Upon receiving the ciphertext register and the randomness register, the adversary evaluates (locally) the type-1 encryption operator initialising the

input register with $|m_0\rangle$, the randomness register with the randomness state received from the challenger, and the ancilla register with the received ciphertext. Finally, the adversary measures the ciphertext register output of the type-1 encryption operator: if he measures 0, then he outputs $b = 0$, otherwise outputs $b = 1$. The circuit is depicted in Fig. 10. The attack works because, if $b = 0$, then the adversary will compute the same ciphertext as the challenger, hence the output register of the type-1 encryption will be $|0\rangle$; on the other hand, if $b = 1$, a random value will be observed instead. Clearly, this results in output states that the adversary can distinguish with overwhelming probability.
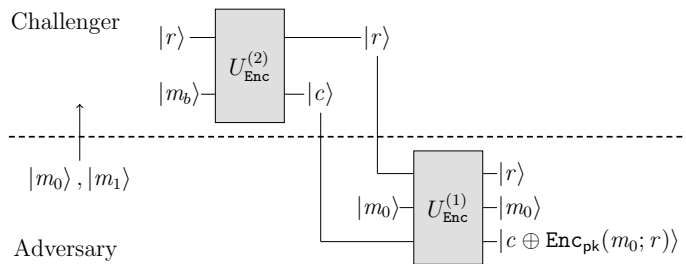

Fig. 10: Generic attack against superposition of randomness.

C   Concurrent Work

In concurrent and independent work, Chevalier et al. [19] and Carstens et al. [18] propose alternative QS2 security notions for public and symmetric key encryption schemes. There are important, conceptual differences between these works and ours which we illustrate in this section.

Chevalier et al. start by resuming a game-based quantum indistinguishability notion previously introduced by Mossayebi and Schack [36] which, we conjecture, is not comparable to ours. This notion is based on a real-or-permuted approach: in the security game, the adversary sends a *single* quantum plaintext of the form $\sum_x \alpha_x |x\rangle$ and (depending on the value of the secret challenge bit b) receives back either $\sum_x \alpha_x |x, \text{Enc}(x)\rangle$, or $\sum_x \alpha_x |x, \text{Enc}(\pi(x))\rangle$, where π is a random permutation implemented by the challenger. To avoid confusion with our notion (qIND-qCPA), we refer to their notion as π-qIND-qCPA. Consider the canonical IND-CPA symmetric key encryption scheme that works by XOR-ing the message with $\text{F}_k(r)$, where F is a keyed pseudorandom function and r is a freshly sampled randomness which is then attached to the resulting ciphertext. This scheme was previously known to be secure according to Boneh and Zhandry's IND-qCPA notion; however, in [36], Mossayebi and Schack show that such scheme is not π-qIND-qCPA secure,[15] thereby yielding a separation result.

---

[15] The proof of the attack is only sketched, whereas it is formally given by Chevalier et al. in [19].

Starting from this consideration, the authors of [19] develop a framework of new QS2 security notions (both for the symmetric and public key case) where the challenge query is quantum but implemented as a single message in the real-or-permuted setting. This approach has advantages and disadvantages compared with the one in [25] (for the symmetric key case) and the one we adopt in this work (for the public key case):

- The notion of π-qIND-qCPA (and the related CCA and non-malleability notions) only require the use of type-1 oracles, therefore greatly simplifying the modelling of the security game. Another advantage is that it can be defined for any encryption scheme, while we require *isometric schemes* (cf. Section 5).
- On the other hand, the notion of Chevalier et al. (unlike ours) deviates from the established framework for the classical case. In the traditional setting of symmetric and public key security notions, in fact, it is well-known that many different characterizations of IND-CPA (with two or more messages chosen by the adversary, with one chosen and one random or fixed, etc.) are all equivalent to an intuitive (but more cumbersome) notion of semantic security. For π-qIND-qCPA, however, it is *crucial* that the adversary can only send *one single challenge message* to the challenger.[16] This is not the case for our qIND-qCPA (and related) notions: although we do not write them down explicitly here (we leave them for a future update in the appendix of this manuscript), all these good 'sanity checks' can be easily inferred by:
  - The lifting from a two-message qIND (QS2) challenge query to a two-message QIND (QS3) challenge query as shown in [24];
  - The equivalence between different types of QIND challenge query (two messages, many messages, real-or-random, etc.) as shown in [17];
  - The equivalence of such QIND notion to a sound notion of *quantum semantic security* as from [3].

  This means that our notions (in the public key case) and the ones in [25] (for the symmetric key case) closely mirror the well-established framework in the classical setting.
- Analogously, because of the presence of entanglement between plaintext and ciphertext registers, the notions by Chevalier et al. do not mirror the existing solid framework for *fully quantum notions* (QS3 setting) in the literature. This is not a flaw by itself, but it has the drawback that many useful tools cannot be straightforwardly 'imported' from the QS3 setting. An example mentioned above is the difficulty of formalizing the equivalence of π-qIND-qCPA to a natural notion of quantum semantic security, or the possibility of easily lifting the QS2 security of a classical scheme Σ to the QS3 security of a quantum scheme Π that uses Σ as a building block. Another example is the difficulty of defining quantum CCA2 security, which

---

[16] Chevalier et al. prove the *composability* of their notions, but this refers to the fact that one can formulate their security game using multiple challenge queries, where each query is still restricted to a *single* message.

can be done in a relatively easy way in the QS3 setting with the real-vs-ideal approach by Alagic et al. from [5], while requiring the more involved compressed oracle technique by Zhandry [48] for the results in [19].[17]

– Chevalier et al. expand substantially Mossayebi and Schack's results, answering many questions left previously open (some of which also mentioned in an early version of the present work) such as the security of the encrypt-then-MAC construction. Moreover they introduce a technique (based on Zhandry's compressed oracles) to record queries and simulate answers to inverse oracles which is of independent interest.

– It is important to notice that the separation result by Chevalier et al. and Mossayeby and Schack rely on entanglement between message and ciphertext register and not on a particular weakness in the scheme. In contrast, our separation (and the one in [25]) relies solely on a property of the encryption scheme in question. One has to consider how the ability of a quantum adversary of receiving back an entangled pair of message and ciphertext really mirrors the classical intuition, where an adversary would only receive a ciphertext instead.

– Finally, and most importantly, in the present work we show that for many real-world PKE schemes (including most of the NIST candidates) type-2 encryption operators can be implemented *without knowledge of the secret key*. This invalidates Chevalier et al.'s argument that type-2 operators are unreasonable in the public key setting, and actually makes the need for our qIND-qCPA notion in the public key case stronger than ever.

Ultimately, we think that the contribution of Chevalier et al. is of great importance and their results are undoubtedly interesting. It is important to notice that the canonical IND-CPA scheme used by Chevalier et al. and Mossayebi and Schack as a separation from Boneh and Zhandry's IND-qCPA is also shown to be insecure according to the qIND-qCPA security notion in [25]. We can hence see π-qIND-qCPA as a QS2 security notion which is incomparable to the qIND-qCPA notion we present in this work, with advantages and disadvantages as explained above.

In a recent work, Carstens et al. [18] study in detail the relationships between existing security notions for QS2 encryption. Their work is mainly focused on SKE, and they prove certain separations based on (reasonable) conjectures. In particular their work supports our conjecture that qIND-qCPA and π-qIND-qCPA are incomparable also in the PKE case.

---

[17] The authors of [19] also explain in their work why Alagic et al.'s approach would not work in their case.