Encryption Schemes using Random Oracles: from Classical to Post-Quantum Security

Juliane Krämer and Patrick Struck

Technische Universität Darmstadt, Germany
{jkraemer,pstruck}@cdc.tu-darmstadt.de

Abstract. The security proofs of post-quantum cryptographic schemes often consider only classical adversaries. Therefore, whether such schemes are really post-quantum secure remains unknown until the proofs take quantum adversaries into account. Switching to a quantum adversary might require to adapt the security notion. In particular, post-quantum security proofs for schemes which use random oracles have to be in the quantum random oracle model (QROM), while classical security proofs are in the random oracle model (ROM). We remedy this state of affairs by introducing a framework to obtain post-quantum security of public key encryption schemes which use random oracles. We define a class of encryption schemes, called *oracle-simple*, and identify game hops which are used to prove such schemes secure in the ROM. For these game hops, we state both simple and sufficient conditions to validate that a proof also holds in the QROM. The strength of our framework lies in its simplicity, its generality, and its applicability. We demonstrate this by applying it to the code-based encryption scheme ROLLO-II (Round 2 NIST candidate) and the lattice-based encryption scheme LARA (FC 2019). Thereby we prove that both schemes are post-quantum secure, which had not been shown before.

Keywords: QROM · game-based proofs · code-based cryptography · lattice-based cryptography

1 Introduction

Relying on quantum-hard mathematical assumptions is not sufficient to develop cryptographic schemes that withstand attackers with quantum computing power. To truly provide security against quantum adversaries, their quantum computing power has to be considered in the security proof as well. At least three models regarding the quantum computing power of the adversary and the schemes' users are distinguished [13]: classical security, post-quantum security, and quantum security. In classical security proofs no one has quantum computing power. In post-quantum security proofs, by contrast, the adversary has quantum computing power and can thereby deploy quantum computation in its attacks, e.g., by evaluating hash functions in superposition. The users of the cryptographic scheme, however, remain classical. In a world where every party has quantum computing power, quantum security is needed. In this model, for instance, a quantum adversary is able to query a decryption oracle in superposition.

Post-quantum security of schemes is mandatory to be deployed in a world with large quantum computers. Hence, if only classical proofs exist, it has to be evaluated if these translate to a quantum adversary, i.e., whether the classical security can be lifted to post-quantum security. This is not always the case [9,24]. For cryptographic schemes which are proven secure in the random oracle model (ROM), this entails that they have to be proven secure in the quantum random oracle model (QROM) [9]. In this model, the adversary can query the random oracle in superposition. This requires different proof techniques to cope with the additional power of the adversary.

A popular technique to prove security of a cryptographic scheme is to organise the proof as a sequence of games [7,23]. In a game-based proof, the advantage of an adversary $\mathcal{A}$ in a game G_0 can be bound by its advantage to distinguish the real game G_0 from an ideal game G_k in which the adversary has no advantage. To this end, several intermediate games $\mathsf{G}_1, \dots, \mathsf{G}_{k-1}$ are constructed between G_0 and G_k so that the change between successive games is small. This makes the advantage to distinguish each pair of consecutive games, i.e., each game hop, easier to analyse and allows to upper bound the overall advantage of $\mathcal{A}$ by the sum of these advantages. To lift a classical game-based proof to post-quantum security, an adversary with quantum computing power has to be considered and the classical games have to be replaced by their corresponding post-quantum versions.

In this work, we study under which conditions security proofs of public key encryption (PKE) schemes can be lifted from the ROM in the QROM. The security notion we are considering is *indistinguishability under chosen-plaintext attacks* (IND-CPA), a basic security notion for PKE schemes. Intuitively, an encryption scheme is IND-CPA-secure if an adversary can not distinguish between the encryption of two adversarial chosen messages. More precisely, we study how classical IND-CPA security proofs in the ROM can be lifted to post-quantum IND-CPA (pq-IND-CPA), where the adversary can query the random oracle in superposition (QROM) [13].

1.1 Our Contribution

The contribution of this work is a method to prove IND-CPA-secure encryption schemes pq-IND-CPA-secure. We define a class of public key encryption schemes, called oracle-simple, and develop a framework to lift the security of such schemes from the ROM to the QROM. To this end, we define two different types of game hops and state simple, easily checkable conditions such that the classical proof can be lifted against quantum adversaries. Each PKE scheme which can be proven IND-CPA-secure in this framework thereby is automatically post-quantum secure. Due to its simplicity we expect the framework to be helpful when designing post-quantum secure encryption schemes. Another important aspect is that our framework is generic and not restricted to a certain family of post-quantum cryptography, e.g., lattice-based cryptography.

We demonstrate the value of our framework by applying it to two public key encryption schemes, which until this work were not known to be post-quantum secure: 1) the code-based encryption scheme ROLLO-II [20] and 2) the lattice-based encryption scheme LARA [4].

Two more schemes which can be proven post-quantum secure using our framework are the code-based encryption scheme BigQuake [5] and the lattice-based encryption scheme LIMA [1][1], both Round 1 NIST candidates. Applying our framework to these schemes is very much akin to the application to ROLLO-II and LARA, which is why we omit it. To the best of our knowledge, our framework covers all random-oracle-based encryption schemes submitted to NIST [1,4,5,20] and, in particular, we are not aware of any random-oracle-based encryption scheme which is not covered by it.

To obtain classical security against chosen-ciphertext attacks (CCA), all these schemes rely on generic transformations like the FO-transformation [12]. The pq-IND-CPA security of the schemes is the final requirement for applying the post-quantum variants of this transformation [15,25], i.e., to gain CCA security against quantum adversaries. More recent results of post-quantum secure FO-transformations [17,22] achieve tighter bounds for CCA security at the cost of an additional property called *disjoint simulatability*. Intuitively, this means that there exists a simulator, knowing merely the public key, that can generate fake ciphertexts that are indistinguishable from real ciphertexts of random messages. Showing this property for the concrete schemes ROLLO-II and LARA is beyond the scope of this work.

1.2 Related Work

Song [24] provides a general framework to lift security reductions. However, the main limitation is that the applicability is restricted to the scenario in which the classical security notion holds true even for quantum adversaries, e.g., in the standard model. This restrains the usage of the framework for any proofs in the ROM, since post-quantum security proofs have to be in the QROM. If the security notion changes towards a quantum adversary, applying the framework requires to come up with a quantum proof. That is, one has to transform a quantum adversary in the QROM into a quantum adversary in the ROM.

For signature schemes, there exist results to obtain post-quantum security in the QROM. Along with the introduction of the QROM, Boneh et al. [9] present the concept of history-free reductions for signature schemes proven secure in the ROM. They show that history-free reductions provide post-quantum security for signature schemes in the QROM. Since the known ROM proofs for Fiat-Shamir signatures are not history-free, several works study their post-quantum security and identify specific properties of Fiat-Shamir signatures such that schemes with these properties are post-quantum secure in the QROM, e.g., [10,11,18,19,27].

[1] We note that the IND-CPA security of LIMA can also be proven in the standard model. This makes its pq-IND-CPA security somewhat trivial, as it avoids the main challenge, that is, the switch from the ROM to the QROM.

Others, for instance Alkim et al. [2] for the signature scheme qTESLA, prove post-quantum security directly. Hence, the question whether or not classical security proofs for signature schemes can be lifted to post-quantum security is discussed both with and without random oracles.

For encryption schemes, however, no broad analysis of liftable security proofs in the QROM exists. Zhandry [28] shows that quantum random oracles can be simulated using q-wise independent functions, thereby removing the additional assumption required in the proofs by Boneh et al. [9]. In addition, Zhandry shows how the classical random oracle technique of challenge injection can be restored in the quantum setting using so-called semi-constant distributions. With these results several cryptographic schemes, including identity-based encryption schemes, are proven secure against quantum adversaries. Unruh [26] develops the one-way to hiding (O2H) lemma, another proof technique in the QROM. The O2H lemma is used, for instance, by Targhi and Unruh [25] to prove a slight modification of the FO transformation [12] indistinguishable against chosen-ciphertext attacks in the QROM. Tighter bounds for the O2H lemma have been proposed by Ambainis et al. [3] and Bindel et al. [8] at the cost of a more restricted applicability.

1.3 Organization of the Paper

The rest of this paper is organized as follows. In Section 2, we provide the notation and the necessary background on both the quantum random oracle model and security proofs. In Section 3, we present our framework and show under which conditions a classical security proof in the ROM can be lifted to the QROM. Finally, we apply our framework to the code-based scheme ROLLO-II and the lattice-based scheme LARA in Section 4 and thereby reveal that their IND-CPA security proofs remain valid towards a quantum adversary.

2 Preliminaries

2.1 Notation

For a non-negative integer n we denote the set $\{1, \ldots, n\}$ by $[n]$. The domain and co-domain of a function f are denoted by $\mathsf{Dom}(f)$ and $\mathsf{CoDom}(f)$, respectively. A function f is called negligible if $f(n) < 1/n^c$ for any $c > 0$ and sufficiently large n. For a set $\mathcal{S}$, we write $s \leftarrow_\$ \mathcal{S}$ to denote that a value which is sampled uniformly at random from $\mathcal{S}$ is assigned to s. By $|\mathcal{S}|$ we describe the number of elements in $\mathcal{S}$. We write $\mathcal{A}_z = (\mathcal{M}_z, \mathcal{D}_z)$ to denote an IND-CPA adversary $\mathcal{A}_z$ which consists of two algorithms $\mathcal{M}_z$, the message generator which outputs two messages, and $\mathcal{D}_z$, the distinguisher, which outputs a bit. The subscript z indicates whether the adversary is classical ($z = c$) or quantum ($z = q$). We omit it in the case it is not relevant. It is assumed that $\mathcal{M}_z$ and $\mathcal{D}_z$ share state.

We suppose the reader to be familiar with the fundamental basics of quantum computation, e.g., the ket notation $|\cdot\rangle$ and measurements. For a more thorough discussion of the topic, we refer to [21].

2.2 The Quantum Random Oracle Model

The random oracle model (ROM), formalized by Bellare and Rogaway [6], is a commonly used model to prove cryptographic schemes secure. In the ROM, all parties have access to a random oracle H which, upon being queried on a value x, returns a random value y. Every further query of x, for instance by another party, is answered using the same y as before. When a scheme is proven secure in the ROM, one idealises components like hash functions by a random oracle. Given that the code of a hash function is publicly available, one has to assume that a quantum adversary implements hash functions on its quantum computer, thereby being able to evaluate it in superposition. This assumption gives rise to the quantum random oracle model (QROM), which has been advocated by Boneh et al. [9]. In the QROM, parties which have quantum computing power are allowed to query the random oracle in superposition. In more detail, for a random oracle H, the QROM allows these parties access to the quantum random oracle $|\mathsf{H}\rangle$, where $|\mathsf{H}\rangle : |x, y\rangle \mapsto |x, y \oplus \mathsf{H}(x)\rangle$. To prove a scheme post-quantum secure, the proof should always be in the QROM, as a proof in the ROM would imply the unrealistic expectation that the adversary refrains from implementing a hash function on its quantum computer. We use superscripts to denote oracle access, e.g., $\mathcal{A}^{\mathsf{H}}$ and $\mathcal{A}^{|\mathsf{H}\rangle}$ for the ROM and QROM, respectively.

In our proofs we also consider reprogrammed random oracles. For a random oracle H, we denote the random oracle which is reprogrammed on input x to y by $\mathsf{H}_{x\to y}$, i.e.,

$$\mathsf{H}_{x\to y}(a) = \begin{cases} y & \text{, if } a = x \\ \mathsf{H}(a) & \text{, else} \end{cases} .$$

Below we recall some results we use in our framework. We start with the one-way to hiding (O2H) lemma by Unruh [26], albeit using the reformulation by Ambainis et al. [3] adapted to our case.

Lemma 1 (One-way to hiding (O2H) **[3]).** *Let G, $\mathsf{H} \colon \mathcal{X} \to \mathcal{Y}$ be random functions, let z be a random bitstring, and let $\mathcal{S} \subset \mathcal{X}$ be a random set such that $\forall x \notin \mathcal{S}$, $\mathsf{G}(x) = \mathsf{H}(x)$. $(\mathsf{G}, \mathsf{H}, \mathcal{S}, z)$ may have arbitrary joint distribution. Furthermore, let $\mathcal{A}_q^{|\mathsf{H}\rangle}$ be a quantum oracle algorithm which queries $|\mathsf{H}\rangle$ at most q times. Define an oracle algorithm $\mathcal{B}_q^{|\mathsf{H}\rangle}$ as follows: Pick $i \leftarrow_{\$} [q]$. Run $\mathcal{A}_q^{|\mathsf{H}\rangle}(z)$ until just before its i-th query to $|\mathsf{H}\rangle$. Measure the query in the computational basis, and output the measurement outcome. Let*

$$P_{left} \coloneqq \Pr[\mathcal{A}_q^{|\mathsf{H}\rangle}(z) \Rightarrow 1]$$
$$P_{right} \coloneqq \Pr[\mathcal{A}_q^{|\mathsf{G}\rangle}(z) \Rightarrow 1]$$
$$P_{guess} \coloneqq \Pr[x \in \mathcal{S} \mid \mathcal{B}_q^{|\mathsf{H}\rangle}(z) \Rightarrow x] .$$

Then it holds that

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

The same result holds with $\mathcal{B}_q^{|\mathsf{G}\rangle}(z)$ instead of $\mathcal{B}_q^{|\mathsf{H}\rangle}(z)$ in the definition of P_{guess}.

Bindel et al. [8] developed another variant of the O2H lemma, called double-sided O2H, which is based on the *compressed oracle framework* by Zhandry [29]. It leads to a tighter bound, namely by dropping the factor q. This comes at the cost of requiring two additional properties. First, the simulator $\mathcal{B}_q$ has to be able to simulate both random oracles and, second, the random oracles have to agree on all but one input. To apply the lemma in this work, we only need to show that the two aforementioned properties are satisfied. For a concrete description of the algorithm $\mathcal{B}_q$, we refer to [8].

Lemma 2 (Double-sided O2H (adapted from [8])). *Let* $\mathsf{G}, \mathsf{H} \colon \mathcal{X} \to \mathcal{Y}$ *be random functions, let* z *be a random bitstring, and let* $x_0 \in \mathcal{X}$ *be a random value such that* $\forall x \neq x_0$, $\mathsf{G}(x) = \mathsf{H}(x)$. $(\mathsf{G}, \mathsf{H}, x_0, z)$ *may have arbitrary joint distribution. Let* $\mathcal{A}_q^{|\mathsf{H}\rangle}$ *be a quantum oracle algorithm. There exists another quantum oracle algorithm* $\mathcal{B}_q^{|\mathsf{G}\rangle,|\mathsf{H}\rangle}(z)$ *which returns either* x_0 *or a failure symbol* $\perp$. $\mathcal{B}_q$ *runs in about the same amount of time as* $\mathcal{A}_q$*, but when* $\mathcal{A}_q$ *queries* $|\mathsf{H}\rangle$, $\mathcal{B}_q$ *queries both* $|\mathsf{G}\rangle$ *and* $|\mathsf{H}\rangle$*. Let*

$$\begin{aligned} P_{left} &\coloneqq \Pr[\mathcal{A}_q^{|\mathsf{H}\rangle}(z) \Rightarrow 1] \\ P_{right} &\coloneqq \Pr[\mathcal{A}_q^{|\mathsf{G}\rangle}(z) \Rightarrow 1] \\ P_{extract} &\coloneqq \Pr[x = x_0 \mid \mathcal{B}_q^{|\mathsf{H}\rangle,|\mathsf{G}\rangle}(z) \Rightarrow x]\,. \end{aligned}$$

Then it holds that

$$|P_{left} - P_{right}| \leq 2\sqrt{P_{extract}}\,.$$

We will use the O2H lemma in the following way. Suppose we have two games G_0 and G_1 which are identical except for the random oracles that the adversary has access to. Namely, in G_0 it has access to $|\mathsf{H}\rangle$ while in G_1 it has access to $|\mathsf{H}'\rangle$. The advantage of the adversary in distinguishing the games is bound by its advantage in distinguishing the random oracles $|\mathsf{H}\rangle$ and $|\mathsf{H}'\rangle$, which, in turn, can be bound by the O2H lemma.

Next we state a lemma which bounds the probability of a quantum algorithm in finding marked items in a function. On a high level, a quantum adversary is given superposition access to a function $\mathcal{F}$ which maps a randomly chosen input to 1 (the marked item) while all other inputs are mapped to 0. The goal of the adversary is to find the input that is mapped to 1.

Lemma 3 (adapted from [16]). *Let* $x_0 \leftarrow_{\$} \mathcal{X}$ *and* $\mathcal{F} \colon \mathcal{X} \to \{0, 1\}$*, such that*

$$\mathcal{F}(x) = \begin{cases} 1 & , \textit{if } x = x_0 \\ 0 & , \textit{else} \end{cases}\,.$$

Then for any quantum adversary $\mathcal{A}_q$*, making at most* q *(superposition) queries to* $\mathcal{F}$*, it holds that*

$$\Pr[\mathcal{F}(x) = 1 \mid \mathcal{A}_q^{|\mathcal{F}\rangle}() \Rightarrow x] \leq \frac{8(q+1)^2}{|\mathcal{X}|}\,.$$

2.3 Security Proofs

We use game-based proofs following [7, 23], where an adversary plays a game which eventually outputs a bit indicating whether the adversary has won the game or not. Let G_0, G_1 be games and $\mathcal{A}$ be an adversary. We write $\mathsf{G}_0^{\mathcal{A}} \Rightarrow v$ to indicate that the game G_0 outputs v when interacting with $\mathcal{A}$. The *game advantage* between the games G_0 and G_1 is defined as:

$$\mathbf{Adv}\left(\mathsf{G}_0^{\mathcal{A}}, \mathsf{G}_1^{\mathcal{A}}\right) \coloneqq \Pr[\mathsf{G}_0^{\mathcal{A}} \Rightarrow \text{true}] - \Pr[\mathsf{G}_1^{\mathcal{A}} \Rightarrow \text{true}]\,.$$

Whether a game G is in the ROM or the QROM is implicitly defined by the adversary playing the game. That is, $\mathsf{G}^{\mathcal{A}_c}$ is in the ROM while $\mathsf{G}^{\mathcal{A}_q}$ is in the QROM.

A public key encryption (PKE) scheme $\mathrm{E} = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ is a triple of algorithms $\mathtt{KGen}$, $\mathtt{Enc}$, and $\mathtt{Dec}$. $\mathtt{KGen}$ outputs a key pair $(\mathsf{pk}, \mathsf{sk})$. The input to $\mathtt{Enc}$ is a public key pk and a message m, the output is a ciphertext c. The algorithm $\mathtt{Dec}$, on input a secret key sk and a ciphertext c, outputs a message m. We are interested in PKE schemes which use random oracles. Thus we write $\mathtt{Enc}^{\mathsf{H}}$ and $\mathtt{Dec}^{\mathsf{H}}$ to denote that both $\mathtt{Enc}$ and $\mathtt{Dec}$ have oracle access to H.[2]

A basic security notion for encryption schemes is *indistinguishability under chosen plaintext attacks* (IND-CPA) which asks an adversary to distinguish between the encryption of two adversarial chosen messages. Below we formally define the corresponding post-quantum security notion pq-IND-CPA for public key encryption schemes which use random oracles. Note that only the random oracle access changes towards the post-quantum security. Both the inputs and outputs of the adversary (i.e., public key, messages, ciphertexts, and output bit) remain classical in both cases.

Definition 4. *Let* $\mathrm{E} = (\mathtt{KGen}, \mathtt{Enc}^{\mathsf{H}}, \mathtt{Dec}^{\mathsf{H}})$ *be a* PKE *scheme and let the game* $\mathsf{pq\text{-}IND\text{-}CPA}$ *be defined as in Fig. 1. Then for any adversary* $\mathcal{A}$ *its* pq-IND-CPA *advantages is defined as:*

$$\mathbf{Adv}_{\mathrm{E}}^{\mathsf{pq\text{-}IND\text{-}CPA}}(\mathcal{A}) \coloneqq 2\Pr\left[\mathsf{pq\text{-}IND\text{-}CPA}^{\mathcal{A}} \Rightarrow \text{true}\right] - 1\,.$$

We say that $\mathrm{E} = (\mathtt{KGen}, \mathtt{Enc}^{\mathsf{H}}, \mathtt{Dec}^{\mathsf{H}})$ *is* pq-IND-CPA-secure *if* $\mathbf{Adv}_{\mathrm{E}}^{\mathsf{pq\text{-}IND\text{-}CPA}}(\mathcal{A})$ *is negligible. Classical security is defined analogously using game* $\mathsf{IND\text{-}CPA}$*.*

The hardness of a problem P is defined by a game between a challenger and an adversary. In a decisional problem, an adversary obtains a problem instance depending on some secret bit $b \in \{0, 1\}$ chosen by the challenger, and is asked to determine b. In a search problem, an adversary obtains a problem instance depending on some secret s chosen by the challenger, and is asked to find s.

[2] We do not allow the key generation algorithm access to the random oracle as we are not aware of any scheme which requires it. Besides, proving the resulting game hop would be trivial as in case $\mathtt{KGen}$ has access to the random oracle, the adversary gets access to the random oracle only after receiving the public key. Hence, the reduction can trivially reprogram the random oracle unnoticeable for the adversary.

```
IND-CPA
  $b \leftarrow_\$ \{0,1\}$
  $(\mathsf{pk},\mathsf{sk}) \leftarrow_\$ \mathtt{KGen}()$
  $m_0, m_1 \leftarrow_\$ \mathcal{M}_c^{\mathsf{H}}(\mathsf{pk})$
  $c \leftarrow_\$ \mathtt{Enc}^{\mathsf{H}}(\mathsf{pk}, m_b)$
  $b' \leftarrow_\$ \mathcal{D}_c^{\mathsf{H}}(\mathsf{pk}, c)$
  return $(b' = b)$
```

```
pq-IND-CPA
  $b \leftarrow_\$ \{0,1\}$
  $(\mathsf{pk},\mathsf{sk}) \leftarrow_\$ \mathtt{KGen}()$
  $m_0, m_1 \leftarrow_\$ \mathcal{M}_q^{|\mathsf{H}\rangle}(\mathsf{pk})$
  $c \leftarrow_\$ \mathtt{Enc}^{\mathsf{H}}(\mathsf{pk}, m_b)$
  $b' \leftarrow_\$ \mathcal{D}_q^{|\mathsf{H}\rangle}(\mathsf{pk}, c)$
  return $(b' = b)$
```

Fig. 1: Classical (IND-CPA) and post-quantum (pq-IND-CPA) security games for a public key encryption scheme $\mathrm{E} = (\mathtt{KGen}, \mathtt{Enc}^{\mathsf{H}}, \mathtt{Dec}^{\mathsf{H}})$ against a classical adversary $\mathcal{A}_c = (\mathcal{M}_c, \mathcal{D}_c)$ and a quantum adversary $\mathcal{A}_q = (\mathcal{M}_q, \mathcal{D}_q)$, respectively, where $\mathcal{M}$ (*message generator*) and $\mathcal{D}$ (*distinguisher*) implicitly share state.

Against quantum adversaries, the games remain the same, i.e., the challenge and the solution remain classical, but the adversary can use local quantum computing power. Similar to the definition above, we write $\mathbf{Adv}^{\mathrm{P}}(\mathcal{A})$ for the advantage of an adversary $\mathcal{A}$ in solving problem P. For a decisional problem, it is understood to be the advantage in solving the problem over guessing. There are also works which analyse problems in the fully quantum setting, where the challenge is quantum (cf. [14]).

3 The pq-IND-CPA Framework

Within this section we develop our framework to lift classical security proofs in the post-quantum setting. To this end, we first define a class of encryption schemes in Section 3.1 and identify two types of game hops for this class of encryption schemes in Section 3.2. In Section 3.3, we show under which conditions the classical proofs for these game hops hold true against quantum adversaries in the QROM.

3.1 Requirements for PKE Schemes

We start by defining so-called *oracle-simple* public key encryption schemes. These are encryption schemes where the encryption algorithm invokes the random oracle exactly once on an input independent of the message and the public key.[3] Below we formally define such schemes.

Definition 5. *Let* $\mathrm{E} = (\mathtt{KGen}, \mathtt{Enc}^{\mathsf{H}}, \mathtt{Dec}^{\mathsf{H}})$ *be a public key encryption scheme. If there exists an algorithm* Enc-Sub *and a deterministic function* f *which maps*

[3] This property is required to get a meaningful bound from applying the one-way to hiding lemma. Since we are not aware of any PKE scheme which does not satisfy this requirement, we do not consider it a restriction.

from some set $\mathcal{R}$ to $\mathsf{Dom(H)}$ *such that* $\mathtt{Enc}^{\mathsf{H}}$ *can be written as in Fig. 2, i.e., it first invokes the random oracle on* $\mathtt{f}(r)$ *for a random* $r \in \mathcal{R}$ *to obtain* y *and then computes the ciphertext using* $\mathtt{Enc\text{-}Sub}(\mathsf{pk}, m, r, y)$*, then we call* E *an oracle-simple (public key) encryption scheme with function* $\mathtt{f}$*.*

```
$\mathtt{Enc}^{\mathsf{H}}(\mathsf{pk}, m)$
  $r \leftarrow_{\$} \mathcal{R}$
  $x \leftarrow \mathtt{f}(r)$
  $y \leftarrow \mathsf{H}(x)$
  $c \leftarrow_{\$} \mathtt{Enc\text{-}Sub}(\mathsf{pk}, m, r, y)$
  return $c$
```

Fig. 2: Algorithm `Enc` of an oracle-simple encryption scheme using `f` and `Enc-Sub`.

Based on this definition, we can rewrite the IND-CPA and pq-IND-CPA security games for oracle-simple encryption schemes yielding the security games displayed in Fig. 3.

Since our framework is based on oracle-simple encryption schemes, its generality depends on the generality of this class of encryption schemes. Analysing all encryption schemes submitted as Round 1 NIST candidates which use random oracles [1, 4, 5, 20], reveals that all of them are indeed oracle-simple schemes. Note that this analysis is based on the underlying encryption scheme as all candidates use random oracles when applying generic transformations to achieve CCA security. Thus, we see this as a style of notation which greatly simplifies the presentation of our proofs, rather than a restriction of its generality.

3.2 Identification of Game Hops

Within this section we define two different types of game hops which are used to prove security of oracle-simple encryption schemes. Due to the structure of oracle-simple encryption schemes, we can distinguish between game hops for which lifting is rather trivial since they are independent of the random oracle, and game hops which are not independent of the random oracle. We start by defining a Type-I game hop which is independent of the random oracle.

Definition 6. *Let* G_i *and* G_{i+1} *be two* IND-CPA *games (cf. Fig. 3) for an oracle-simple public key encryption scheme* $\mathrm{E} = (\mathtt{KGen}, \mathtt{Enc}^{\mathsf{H}}, \mathtt{Dec}^{\mathsf{H}})$*. We call the game hop between* G_i *and* G_{i+1} *a* Type-I game hop *if the games only differ in using different algorithms* `KGen` *to generate the key pair or different algorithms* `Enc-Sub` *to generate the ciphertext.*

Next, we define a Type-II game hop which affects the usage of the random oracle while encrypting one of the challenge messages by the adversary.

```
IND-CPA
$b \leftarrow\$ \{0,1\}$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow\$ \mathtt{KGen}()$
$m_0, m_1 \leftarrow\$ \mathcal{M}_c^{\mathsf{H}}(\mathsf{pk})$
$c \leftarrow\$$ $\mathtt{Enc}^{\mathsf{H}}(\mathsf{pk}, m_b)$
    $r \leftarrow\$ \mathcal{R}$
    $x \leftarrow \mathtt{f}(r)$
    $y \leftarrow \mathsf{H}(x)$
    $c \leftarrow\$ \mathtt{Enc\text{-}Sub}(\mathsf{pk}, m_b, r, y)$
    return $c$
$b' \leftarrow\$ \mathcal{D}_c^{\mathsf{H}}(\mathsf{pk}, c)$
return $(b' = b)$
```

```
pq-IND-CPA
$b \leftarrow\$ \{0,1\}$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow\$ \mathtt{KGen}()$
$m_0, m_1 \leftarrow\$ \mathcal{M}_q^{|\mathsf{H}\rangle}(\mathsf{pk})$
$c \leftarrow\$$ $\mathtt{Enc}^{\mathsf{H}}(\mathsf{pk}, m_b)$
    $r \leftarrow\$ \mathcal{R}$
    $x \leftarrow \mathtt{f}(r)$
    $y \leftarrow \mathsf{H}(x)$
    $c \leftarrow\$ \mathtt{Enc\text{-}Sub}(\mathsf{pk}, m_b, r, y)$
    return $c$
$b' \leftarrow\$ \mathcal{D}_q^{|\mathsf{H}\rangle}(\mathsf{pk}, c)$
return $(b' = b)$
```

Fig. 3: Security games IND-CPA and pq-IND-CPA for an *oracle-simple* public key encryption scheme $\mathrm{E} = (\mathtt{KGen}, \mathtt{Enc}^{\mathsf{H}}, \mathtt{Dec}^{\mathsf{H}})$ with function $\mathtt{f}$.

Definition 7. *Let G_i and G_{i+1} be two* IND-CPA *games (cf. Fig. 3) for an oracle-simple public key encryption scheme* $\mathrm{E} = (\mathtt{KGen}, \mathtt{Enc}^{\mathsf{H}}, \mathtt{Dec}^{\mathsf{H}})$. *We call the game hop between G_i and G_{i+1} a* Type-II game hop *if their only difference is that game G_i obtains y by invoking H on x while game G_{i+1} samples y uniformly at random from* $\mathsf{CoDom}(\mathsf{H})$.

Having discussed the generality of the class of encryption schemes, the next natural question asks for the generality of the defined game hops. A Type-II game hop is a standard game hop to make the challenge independent of the random oracle, thereby rendering it obsolete for the adversary. As for Type-I game hops, we observe the following. To bound the game advantage, one transforms an adversary that distinguishes the games into an adversary (the reduction) that solves some problem. To achieve this, the game hop has to be connected with the problem instance. Thus the reduction has to feed the problem instance to the adversary. Considering IND-CPA security, its options are fairly limited. Either it feeds it via the inputs to the adversary, that is the public key pk or the ciphertext c, or as a response from the random oracle. The former case is the one we cover with a Type-I game hop. The latter case is not covered, as none of the schemes, that we are aware of, requires such a game hop. Nevertheless, we emphasise that our framework can be easily extended by another type of game hop, if needed. The post-quantum analogue of such a challenge injection in a random oracle response can be achieved using Zhandry's semi-constant distributions [28], where a challenge is injected in a subset of inputs which gives a significant chance that the adversary uses the injected challenge while the probability of detecting the challenge injection remains small enough.

3.3 Lifting Security

Within this section we state the conditions under which a classical security proof holds true in the post-quantum setting. We present one lemma to lift Type-I game hops and two lemmas for lifting Type-II game hops, one being a special case of the other.

The lemma below states that classical reductions from a decisional problem to the game advantage of a Type-I game hop hold true in the post-quantum setting.

Lemma 8. *Let G_i and G_{i+1} be games such that the game hop between these is a* Type-I *game hop. Suppose there exists a decisional problem* P *which is reduced to the game advantage between the games. Then, for any quantum adversary $\mathcal{A}_q$, there exists a quantum adversary $\mathcal{B}_q$ against* P *such that*

$$\mathbf{Adv}\left(\mathsf{G}_i^{\mathcal{A}_q}, \mathsf{G}_{i+1}^{\mathcal{A}_q}\right) \leq \mathbf{Adv}^{\mathrm{P}}(\mathcal{B}_q)\,.$$

Proof. The difference between the games is independent from the random oracle. Hence the same proof holds against quantum adversaries, albeit the adversary $\mathcal{B}_q$ has to simulate a quantum random oracle for the adversary $\mathcal{A}_q$. This can be done using a $2q_{\mathsf{H}}$-wise independent function, where q_{H} is the number of random oracle queries by $\mathcal{A}_q$ [28]. □

Alternatively, Lemma 8 can be formally proven using the framework by Song [24]. Due to the complex notation used in [24], however, this leads to a rather long and tedious proof.

The following lemma states conditions under which the classical proof for a Type-II game hop holds true against quantum adversaries. Recall that we consider oracle-simple encryption schemes with function `f`. For an arbitrary function `f`, we can not argue about the distribution of the value that is queried to the random oracle. This prevents us to use known results like finding marked items in a function, as we do when proving a special case of the lemma.

Lemma 9. *Let G_i and G_{i+1} be games such that the game hop between these is a* Type-II *game hop. Suppose there exists a search problem* P *which is reduced to the probability that an adversary queries the random oracle on x. Then, for any quantum adversary $\mathcal{A}_q$, making q_{H} queries to $|\mathsf{H}\rangle$, there exists a quantum adversary $\mathcal{C}_q$ against* P *such that*

$$\mathbf{Adv}\left(\mathsf{G}_i^{\mathcal{A}_q}, \mathsf{G}_{i+1}^{\mathcal{A}_q}\right) \leq 2q_{\mathsf{H}}\sqrt{\mathbf{Adv}^{\mathrm{P}}(\mathcal{C}_q)}\,.$$

Proof. We observe that the games G_i and G_{i+1} are perfectly indistinguishable given that $\mathcal{A}$ has no knowledge about the random oracle output on x, that is, $\mathsf{H}(x)$. Hence the game advantage can be bound by the knowledge of $\mathcal{A}$ about $\mathsf{H}(x)$. For the classical proof in the ROM, this is fairly easy as the only way for the adversary to obtain knowledge about $\mathsf{H}(x)$ is to query x. For the post-quantum proof in the QROM, the issue is that, for example, superposition access allows the adversary to trivially get (some) knowledge about $\mathsf{H}(x)$ by making an equal superposition query over all possible inputs. If the distribution of x is uniform, this issue can be tackled using existing results on finding marked items in a random function. For oracle-simple encryption schemes, however, the distribution of x depends on the function `f`. Hence, for an arbitrary function `f`, we can not argue using the distribution of x.

We tackle this issue as follows. First, we show that the game advantage is bound by the distinguishing advantage between two random oracles, see Equation (1). This enables us to apply the O2H lemma as the second step, see Equation (2). In the final step, we bound the resulting term from the O2H lemma using the hardness of P, see Equation (3).

Recall that the games differ in how the value y (input to `Enc-Sub`) is generated. In G_i it is the output of the random oracle on input x while it is sampled uniformly at random from $\mathsf{CoDom}(\mathsf{H})$ in G_{i+1}. By the random oracle paradigm, the value y is distributed identically in both games, as is the ciphertext c. Based on this, we conclude that the only inconsistency lies in the random oracle. Namely, querying the random oracle on x yields the same y which is fed as input to `Enc-Sub` in G_i, while it yields a random value independent of the inputs to `Enc-Sub` in G_{i+1}. This allows us to see G_{i+1} as G_i, that is $y \leftarrow \mathsf{H}(x)$, with the exception that the random oracle H, which $\mathcal{A}$ has access to, is replaced with $\mathsf{H}_{x\to\$}$. Based on this thought, it is easy to see that the game advantage is bound by the chance that $\mathcal{A}$ can distinguish between the two random oracles H and $\mathsf{H}_{x\to\$}$. The same argument holds for a quantum adversary $\mathcal{A}_q$ except that access to the corresponding quantum random oracles $|\mathsf{H}\rangle$ and $|\mathsf{H}_{x\to\$}\rangle$ is granted. For ease of notation, we henceforth assume that the random oracle is reprogrammed to $\perp$ instead of a random value. Then it holds that

$$\mathbf{Adv}\left(\mathsf{G}_i^{\mathcal{A}_q}, \mathsf{G}_{i+1}^{\mathcal{A}_q}\right) \le \left|\Pr[\mathcal{A}_q^{|\mathsf{H}\rangle} \Rightarrow 1] - \Pr[\mathcal{A}_q^{|\mathsf{H}_{x\to\perp}\rangle} \Rightarrow 1]\right| . \tag{1}$$

Applying the O2H lemma (cf. Lemma 1) yields that there exists a quantum algorithm $\mathcal{B}_q$ such that

$$\left|\Pr[\mathcal{A}_q^{|\mathsf{H}\rangle} \Rightarrow 1] - \Pr[\mathcal{A}_q^{|\mathsf{H}_{x\to\perp}\rangle} \Rightarrow 1]\right| \le 2q_{\mathsf{H}}\sqrt{\Pr[\mathcal{B}_q^{|\mathsf{H}\rangle} \Rightarrow x]}\,. \tag{2}$$

It remains to bound the probability that $\mathcal{B}_q$ outputs x. At this point we use the classical security proof, that is, the problem P is reduced to the probability of querying x. It holds that the solution for P is x or can be derived from it, thus $\mathcal{B}_q$ can be transformed into an adversary $\mathcal{C}_q$ against P. The mere difference is that this adversary $\mathcal{C}_q$ is quantum, as $\mathcal{B}_q$ is quantum. Hence, we conclude with

$$2q\sqrt{\Pr[\mathcal{B}_q^{|\mathsf{H}\rangle} \Rightarrow x]} \le 2q_{\mathsf{H}}\sqrt{\mathbf{Adv}^{\mathrm{P}}(\mathcal{C}_q)}\,. \tag{3}$$

This proves the claim. □

Finally we prove a special case for Type-II game hops. Here the function `f`, induced by the oracle-simple encryption scheme, is the identity function.[4] In

[4] In fact, we could relax the requirement to `f` being bijective, however, we are not aware of a scheme where `f` is bijective and not the identity.

this case we can bound the game advantage using well known results about finding marked items in a function given superposition access to the function. This works because the random oracle is invoked on an input chosen uniformly at random while generating the challenge ciphertext.

Lemma 10. *Let G_i and G_{i+1} be games such that the game hop between these is a* Type-II *game hop. Suppose the function* `f`*, specified by the oracle-simple encryption scheme, is the identity function. Then, for any quantum adversary $\mathcal{A}_q$, making q_{H} queries to $|\mathsf{H}\rangle$, it holds that*

$$\mathbf{Adv}\left(\mathsf{G}_i^{\mathcal{A}_q}, \mathsf{G}_{i+1}^{\mathcal{A}_q}\right) \leq \frac{6(q_{\mathsf{H}}+1)}{\sqrt{|\mathsf{Dom}(\mathsf{H})|}} .$$

Proof. Given that `f` is the identity function, it holds that x is sampled uniformly at random from $\mathsf{Dom}(\mathsf{H})$. This allows us to bound the game advantage by the advantage of an adversary in finding marked items, for which bounds are known. Instead of the plain O2H lemma (cf. Lemma 1), we make use of the double-sided O2H lemma (cf. Lemma 2) to obtain a tighter bound.

Using the same argument from the proof of Lemma 9, we bound the game advantage by bounding the probability of detecting reprogramming of the random oracle, again, for ease of notation, assuming that the random oracle is reprogrammed to $\perp$. Thus it holds that

$$\mathbf{Adv}\left(\mathsf{G}_i^{\mathcal{A}_q}, \mathsf{G}_{i+1}^{\mathcal{A}_q}\right) \leq \left|\Pr[\mathcal{A}_q^{|\mathsf{H}\rangle} \Rightarrow 1] - \Pr[\mathcal{A}_q^{|\mathsf{H}_{x\to\perp}\rangle} \Rightarrow 1]\right| .$$

In order to apply the double-sided O2H lemma, two conditions have to be fulfilled. First, the random oracles must agree on all but one input and, second, the simulator $\mathcal{B}_q$ has to be able to simulate both random oracles. The former is fulfilled as the random oracles only differ on input x. The latter is a bit more subtle. The reason is that $\mathcal{B}_q$ has to simulate $|\mathsf{H}_{x\to\perp}\rangle$ for an x unknown to $\mathcal{B}_q$, as knowledge of x would trivially allow to find the marked item. We show that this does not pose a hindrance. Let $\mathcal{B}_q$ be an algorithm that has access to a function $\mathcal{F} : \mathsf{Dom}(\mathsf{H}) \to \{0,1\}$, such that $\mathcal{F}(x) = 1$ and $\mathcal{F}(a) = 0$ for all $a \neq x$. Consider the mapping $\mathcal{G} : \mathsf{Dom}(\mathsf{H}) \times \{0,1\} \to \mathsf{CoDom}(\mathsf{H}) \cup \{\perp\}$ such that

$$\mathcal{G}(x,b) = \begin{cases} \perp & \text{, if } b = 1 \\ \mathsf{H}(x) & \text{, else} \end{cases} .$$

To simulate the quantum random oracle $|\mathsf{H}\rangle$, $\mathcal{B}_q$ simply fixes the last input bit of $\mathcal{G}$ to be 0. To simulate the quantum random oracle $|\mathsf{H}_{x\to\perp}\rangle$, $\mathcal{B}_q$ first invokes the function $\mathcal{F}$ on the input and sets the last input bit of $\mathcal{G}$ to the output of $\mathcal{F}$. For the marked item of $\mathcal{F}$, $\mathcal{G}$ will return $\perp$ as the last input bit is 1, while $\mathcal{G}$ returns the output of the random oracle for all non-marked items. This is illustrated in Fig. 4, where we assume that the domain and co-domain of the random oracle can be represented using n and k qubits, respectively.

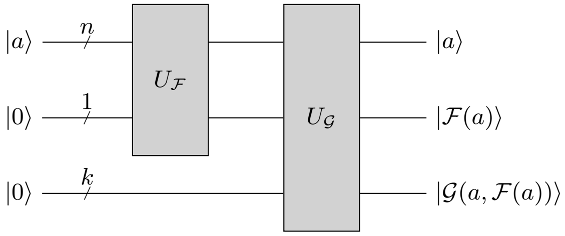

Fig. 4: Simulation of $|\mathsf{H}_{x\to\perp}\rangle$ using $\mathcal{F}$ and $\mathcal{G}$.

If the adversary $\mathcal{A}_q$ can detect the reprogramming, then the simulator $\mathcal{B}_q$ can find the marked item in the function $\mathcal{F}$. Hence we conclude with

$$\begin{aligned}\mathbf{Adv}\left(\mathsf{G}_i^{\mathcal{A}_q},\mathsf{G}_{i+1}^{\mathcal{A}_q}\right) &\leq \left|\Pr[\mathcal{A}_q^{|\mathsf{H}\rangle}\Rightarrow 1]-\Pr[\mathcal{A}_q^{|\mathsf{H}_{x\to\perp}\rangle}\Rightarrow 1]\right|\\ &\overset{\text{(Lemma 2)}}{\leq} 2\sqrt{\Pr[\mathcal{B}_q^{|\mathsf{H}\rangle,|\mathsf{H}_{x\to\perp}\rangle}\Rightarrow x]}\\ &\overset{\text{(Lemma 3)}}{\leq} 2\sqrt{\frac{8(q_{\mathsf{H}}+1)^2}{|\mathsf{Dom}(\mathsf{H})|}}\\ &\leq \frac{6(q_{\mathsf{H}}+1)}{\sqrt{|\mathsf{Dom}(\mathsf{H})|}}\end{aligned}$$

which proves the claim. □

Now we are ready to state our main result, namely the conditions under which our framework lifts the classical security proof of an oracle-simple public key encryption scheme in the post-quantum setting.

Theorem 11. *Let* E $=(\mathtt{KGen},\mathtt{Enc}^{\mathsf{H}},\mathtt{Dec}^{\mathsf{H}})$ *be an oracle-simple* PKE *scheme with function* $\mathtt{f}$ *according to Definition 5. Suppose there exists a classical security proof using a sequence of games* $\mathsf{G}_0,\ldots,\mathsf{G}_k$*, where* G_0 *is the* IND-CPA *game instantiated with* E *and* G_k *is constructed such that* $\mathbf{Adv}^{\mathsf{G}_k}(\mathcal{A}_c)=0$*. Let* i *be such that the game hop between* G_{i-1} *and* G_i *is a* Type-II *game hop. If*

1. *for any* $j\in[k]\backslash\{i\}$*, the game hop between* G_{j-1} *and* G_j *is a* Type-I *game hop such that a quantum hard (decisional) problem* P_j *is reduced to the game advantage between* G_{j-1} *and* G_j *and*
2. *either some quantum hard (search) problem* P_i *is reduced to the probability of querying* x *or the function* $\mathtt{f}$ *is the identity function,*

then E *is* pq-IND-CPA*-secure.*

Proof. The proof follows pretty much from the previous lemmas. For the Type-I game hops, i.e., between G_{j-1} and G_j for $j\in[k]\backslash\{i\}$, we can apply Lemma 8 and conclude that the game advantage is bound by the post-quantum hardness of P_j. Since P_j is a quantum hard problem, this is negligible. For the Type-II game hop, i.e., between G_{i-1} and G_i, we can apply either Lemma 9, using again that P_i is hard for quantum adversaries, or using Lemma 10 if the function $\mathtt{f}$ is the identity function. As the game advantage of all game hops is negligible, we conclude that the advantage of any quantum adversary $\mathcal{A}_q$ in game $\mathsf{pq\text{-}IND\text{-}CPA}$ against $\mathrm{E} = (\mathtt{KGen}, \mathtt{Enc}^{\mathsf{H}}, \mathtt{Dec}^{\mathsf{H}})$ is also negligible. Hence, the oracle-simple public key encryption scheme E is pq-IND-CPA-secure. □

4 Post-Quantum Security of PKE Schemes

We use our framework to lift the classical security of two public key encryption schemes to post-quantum security. In Section 4.1 we lift the security for the code-based public key encryption scheme ROLLO-II [20]. The post-quantum security of the lattice-based public key encryption scheme LARA [4] is proven in Section 4.2.

4.1 Code-based Public Key Encryption Scheme ROLLO-II

We start by introducing the notation used in the public key encryption scheme ROLLO-II [20]. The scheme can be written as an oracle-simple encryption scheme with function $\mathtt{f}$, where $\mathtt{f}$ maps vectors to their support. The pseudocode is given in Fig. 5.

Throughout, p is a prime and q is some power of p. For an integer k, the finite field that contains q^k elements is $\mathbb{F}_{q^k}$ and the corresponding vector space of dimension n is given by $\mathbb{F}_{q^k}^n$. The set of vectors of length n with rank weight w over the set $\mathbb{F}_{q^k}$ is denoted by $\mathcal{S}_w^n(\mathbb{F}_{q^k})$, where the rank weight of a vector is the rank of a specific matrix associated with that vector (see [20] for more details). Below we define the support of a word.

Definition 12. *Let* $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^k}^n$*. The support* E *of* $\mathbf{x}$*, denoted* $\mathsf{Supp}(\mathbf{x})$*, is the* $\mathbb{F}_q$*-subspace of* $\mathbb{F}_{q^k}$ *generated by the* $\mathbf{x}$*, i.e.,* $\mathsf{E} = \langle x_1, \ldots, x_n \rangle_{\mathbb{F}_q}$*.*

Multiplications are considered to be polynomial multiplications, where vectors and polynomials are transformed into one another by taking the vector entries as coefficients and vice versa. In the scheme, d and r are integers while P is an irreducible polynomial over $\mathbb{F}_{q^k}$.

The Ideal-LRPC codes indistinguishability problem, where LRPC stands for *low rank parity check*, asks to distinguish whether a vector $\mathbf{h}$ is sampled uniformly at random or computed as $\mathbf{x}^{-1}\mathbf{y} \bmod \mathsf{P}$, for vectors $\mathbf{x}$, $\mathbf{y}$ of small dimension. In the ideal *rank support recovery* (Ideal-RSR) problem, one is given a vector $\mathbf{h}$, a polynomial P, and a syndrome σ, and asked to find a support E containing vectors $\mathbf{e}_1$, $\mathbf{e}_2$ such that $\mathbf{e}_1 + \mathbf{e}_2\mathbf{h} = \sigma \bmod \mathsf{P}$.

The theorem below shows that the code-based encryption scheme ROLLO-II is pq-IND-CPA-secure.

Theorem 13. *Assuming the post-quantum hardness of the* Ideal-LRPC *problem and the* Ideal-RSR *problem, the code-based encryption scheme* ROLLO-II*, described in Fig. 5, is* pq-IND-CPA*-secure.*

```
ROLLO-II-KGen()
    $\mathbf{x}, \mathbf{y} \leftarrow_{\$} \mathcal{S}_d^{2n}(\mathbb{F}_{q^k})$
    $\mathbf{h} \leftarrow \mathbf{x}^{-1}\mathbf{y} \bmod \mathsf{P}$
    $\mathsf{sk} \leftarrow (\mathbf{x}, \mathbf{y})$
    $\mathsf{pk} \leftarrow \mathbf{h}$
    return $(\mathsf{pk}, \mathsf{sk})$

ROLLO-II-Enc$^{\mathsf{H}}(\mathsf{pk}, m)$
    $\mathbf{e}_1, \mathbf{e}_1 \leftarrow_{\$} \mathcal{S}_r^{2n}(\mathbb{F}_{q^k})$
    $\mathsf{E} \leftarrow \mathsf{Supp}(\mathbf{e}_1, \mathbf{e}_2)$
    $y \leftarrow \mathsf{H}(\mathsf{E})$
    $c \leftarrow_{\$}$ Enc-Sub$(\mathsf{pk}, m, r = (\mathbf{e}_1, \mathbf{e}_2), y)$
        $c_1 \leftarrow \mathbf{e}_1 + \mathbf{e}_2\mathbf{h} \bmod \mathsf{P}$
        $c_2 \leftarrow m \oplus y$
        return $c \leftarrow (c_1, c_2)$
    return $c$
```

Fig. 5: Encryption scheme ROLLO-II written as oracle-simple encryption scheme. Decryption is omitted as it is irrelevant for the IND-CPA security of the scheme.

Proof. The classical IND-CPA security proof of ROLLO-II, given in [20], uses games $\mathsf{G}_0, \ldots, \mathsf{G}_3$. Except for the first game G_0, we only state the change to its predecessor.

Game G_0: This is the IND-CPA game instantiated with ROLLO-II.
Game G_1: In this game the vector $\mathbf{h}$ is sampled randomly.
Game G_2: The value y is sampled randomly, independent of H.
Game G_3: The value c_2 is sampled randomly.

The game hop between G_1 and G_2 is a Type-II game hop, while all other game hops are Type-I game hops. The classical proof reduces the Ideal-LRPC problem to the game advantage between G_0 and G_1 (Type-I) and the Ideal-RSR problem to the probability of querying the random oracle on $\mathsf{E} = \mathsf{Supp}(\mathbf{e}_1, \mathbf{e}_2)$ and thereby also to the game advantage between G_1 and G_2 (Type-II). The game hop between G_2 and G_3 (Type-I) is bound by the problem of distinguishing between a one-time pad encryption and a random ciphertext. Since all these problems are assumed to be hard even for quantum adversaries, Theorem 11 proves the claim. □

4.2 Lattice-based Public Key Encryption Scheme LARA

We start by introducing the notation used in the public key encryption scheme LARA [4]. The scheme, written as an oracle-simple encryption scheme, is given in Fig. 6. Throughout this section, q is an integer and n is a power of 2. The polynomial ring $\mathbb{Z}_q[X]/\langle X^n + 1\rangle$ is denoted by $\mathcal{R}_q$. The decisional learning with errors (DLWE) problem asks to distinguish whether a polynomial z is sampled uniformly at random or generated as $\mathsf{z} \leftarrow \mathsf{as} + \mathsf{e}$, where a is given and s and e are small polynomials which are kept secret.

We refer to [4] for the parameters s, w, p, and r_{sec}, as applying our framework is independent of those. LARA uses the discrete Gaussian distribution which is denoted by $\mathcal{D}_{x,\sigma}$, where x and σ are the support and standard deviation, respectively. Multiplications are considered to be polynomial multiplications. Vectors and polynomials are transformed into one another by setting the coefficients to the vector entries and vice versa. The scheme uses an encoding function Encode which maps messages to polynomials.

```
LARA-KGen()
    $\mathsf{a}_1, \mathsf{a}_2 \leftarrow_{\$} \mathcal{R}_q$
    $\mathsf{r}_1, \mathsf{r}_2 \leftarrow \mathcal{D}_{\mathbb{Z}^n, r_{sec}}$
    $\mathsf{a}_3 \leftarrow p^{k-1} - (\mathsf{a}_1\mathsf{r}_1 + \mathsf{a}_2\mathsf{r}_2)$
    $\mathsf{sk} \leftarrow (\mathsf{r}_1, \mathsf{r}_2)$
    $\mathsf{pk} \leftarrow (\mathsf{a}_1, \mathsf{a}_2, \mathsf{a}_3)$
    return $(\mathsf{pk}, \mathsf{sk})$

LARA-Enc$^{\mathsf{H}}(\mathsf{pk}, m = (m_1, m_2, m_3))$
    $\mathbf{c} \leftarrow_{\$} \mathbb{Z}_p^n$
    $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{d} \leftarrow \mathsf{H}(\mathbf{c})$
    $c \leftarrow_{\$}$ Enc-Sub$(\mathsf{pk}, m, r = \mathbf{c}, y = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{d}))$
        $\mathbf{s} \leftarrow \mathbf{c} + p\mathbf{d}$
        $\mathbf{t}_i \leftarrow \mathsf{Encode}(m_i) + \mathbf{v}_i \bmod w$ for $i \in [3]$
        $\mathbf{e}_i \leftarrow \mathcal{D}_{\mathbf{t}_i + w\mathbb{Z}^n, s}$ for $i \in [3]$
        $\mathsf{b}_i \leftarrow \mathsf{a}_i\mathbf{s} + \mathbf{e}_i$ for $i \in [3]$
        return $c \leftarrow (\mathsf{b}_1, \mathsf{b}_2, \mathsf{b}_3)$
    return $c$
```

Fig. 6: Encryption scheme LARA written as an oracle-simple encryption scheme. Decryption is omitted as it is irrelevant for the IND-CPA security of the scheme.

The following theorem states that the lattice-based encryption scheme LARA is pq-IND-CPA-secure.

Theorem 14. *Assuming the post-quantum hardness of the* DLWE *problem, the lattice-based encryption scheme* LARA*, described in Fig. 6, is* pq-IND-CPA-*secure.*

Proof. The classical IND-CPA security proof of LARA, given in [4], uses games $\mathsf{G}_0, \ldots, \mathsf{G}_4$. Except for game G_0, we only state the change to its predecessor.

Game G_0: This is the $\mathsf{IND\text{-}CPA}$ game instantiated with LARA.
Game G_1: In this game the polynomial a_3 is sampled randomly.
Game G_2: The vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{d}$ are sampled randomly, independent of H.
Game G_3: The polynomials e_i are sampled according to the distribution $\mathcal{D}_{\mathbb{Z}^n,s}$.
Game G_4: The polynomials b_i are sampled randomly.

The game hop between G_1 and G_2 is a Type-II game hop, while all other game hops are Type-I game hops. The classical proof reduces the DLWE problem (with a different number of samples) to the game advantage between the Type-I game hops. We further observe that the function `f` is the identity function for LARA. Thus, we can apply Theorem 11 which proves the claim. □

Acknowledgements

We thank Nina Bindel and Lucas Schabhüser for insightful discussions. We also thank an anonymous reviewer for valuable feedback on an earlier version of this paper. This work was funded by the Deutsche Forschungsgemeinschaft (DFG) – SFB 1119 – 236615297 and by the German Ministry of Education, Research and Technology in the context of the project Aquorypt (grant number 16KIS1022).

References

1. Martin R. Albrecht, Emmanuela Orsini, Kenneth G. Paterson, Guy Peer, and Nigel P. Smart. Tightly secure ring-LWE based key encapsulation with short ciphertexts. In Simon N. Foley, Dieter Gollmann, and Einar Snekkenes, editors, *ESORICS 2017, Part I*, volume 10492 of *LNCS*, pages 29–46. Springer, Heidelberg, September 2017.
2. Erdem Alkim, Nina Bindel, Johannes A. Buchmann, Özgür Dagdelen, Edward Eaton, Gus Gutoski, Juliane Krämer, and Filip Pawlega. Revisiting TESLA in the quantum random oracle model. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017*, pages 143–162. Springer, Heidelberg, 2017.
3. Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 269–295. Springer, Heidelberg, August 2019.
4. Rachid El Bansarkhani. LARA: A design concept for lattice-based encryption. In Ian Goldberg and Tyler Moore, editors, *FC 2019*, volume 11598 of *LNCS*, pages 377–395. Springer, Heidelberg, February 2019.
5. Magali Bardet, Élise Barelli, Olivier Blazy, Rodolfo Canto Torres, Alain Couvreur, Philippe Gaborit, Ayoub Otmani, Nicolas Sendrier, and Jean-Pierre Tillich. Big quake, 2019. NIST Round 1 Candidate.
6. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.
7. Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 409–426. Springer, Heidelberg, May / June 2006.
8. Nina Bindel, Mike Hamburg, Kathrin Hövelmanns, Andreas Hülsing, and Edoardo Persichetti. Tighter proofs of CCA security in the quantum random oracle model. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part II*, volume 11892 of *LNCS*, pages 61–90. Springer, Heidelberg, December 2019.
9. Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Heidelberg, December 2011.
10. Özgür Dagdelen, Marc Fischlin, and Tommaso Gagliardoni. The Fiat-Shamir transformation in a quantum world. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part II*, volume 8270 of *LNCS*, pages 62–81. Springer, Heidelberg, December 2013.

11. Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the Fiat-Shamir transformation in the quantum random-oracle model. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 356–383. Springer, Heidelberg, August 2019.
12. Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 537–554. Springer, Heidelberg, August 1999.
13. Tommaso Gagliardoni. *Quantum Security of Cryptographic Primitives*. PhD thesis, Darmstadt University of Technology, Germany, 2017.
14. Alex B Grilo, Iordanis Kerenidis, and Timo Zijlstra. Learning-with-errors problem is easy with quantum samples. *Physical Review A*, 99(3):032314, 2019.
15. Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A modular analysis of the Fujisaki-Okamoto transformation. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017, Part I*, volume 10677 of *LNCS*, pages 341–371. Springer, Heidelberg, November 2017.
16. Andreas Hülsing, Joost Rijneveld, and Fang Song. Mitigating multi-target attacks in hash-based signatures. In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *PKC 2016, Part I*, volume 9614 of *LNCS*, pages 387–416. Springer, Heidelberg, March 2016.
17. Haodong Jiang, Zhenfeng Zhang, Long Chen, Hong Wang, and Zhi Ma. IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 96–125. Springer, Heidelberg, August 2018.
18. Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 552–586. Springer, Heidelberg, April / May 2018.
19. Qipeng Liu and Mark Zhandry. Revisiting post-quantum Fiat-Shamir. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 326–355. Springer, Heidelberg, August 2019.
20. Carlos Aguilar Melchor, Nicolas Aragon, Magali Bardet, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Ayoub Otmani, Olivier Ruatta, Jean-Pierre Tillich, and Gilles Zémor. Rollo, 2019. NIST Round 2 Candidate.
21. Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.
22. Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 520–551. Springer, Heidelberg, April / May 2018.
23. Victor 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.
24. Fang Song. A note on quantum security for post-quantum cryptography. In Michele Mosca, editor, *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014*, pages 246–265. Springer, Heidelberg, October 2014.
25. Ehsan Ebrahimi Targhi and Dominique Unruh. Post-quantum security of the Fujisaki-Okamoto and OAEP transforms. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B, Part II*, volume 9986 of *LNCS*, pages 192–216. Springer, Heidelberg, October / November 2016.

26. Dominique Unruh. Revocable quantum timed-release encryption. *J. ACM*, 62(6):49:1–49:76, 2015.
27. Dominique Unruh. Post-quantum security of Fiat-Shamir. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 65–95. Springer, Heidelberg, December 2017.
28. Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, Heidelberg, August 2012.
29. Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 239–268. Springer, Heidelberg, August 2019.