Encryption with Quantum Public Keys

Alex B. Grilo[1], Or Sattath[2], and Quoc-Huy Vu[1]

[1]Sorbonne Université, CNRS, LIP6
[2]Computer Science Department, Ben-Gurion University of the Negev

Abstract

It is an important question to find constructions of quantum cryptographic protocols which rely on weaker computational assumptions than classical protocols. Recently, it has been shown that oblivious transfer and multi-party computation can be constructed from one-way functions, whereas this is impossible in the classical setting in a black-box way. In this work, we study the question of building quantum public-key encryption schemes from one-way functions and even weaker assumptions. Firstly, we revisit the definition of IND-CPA security to this setting. Then, we propose three schemes for quantum public-key encryption from one-way functions, pseudorandom function-like states with proof of deletion and pseudorandom function-like states, respectively.

1 Introduction

The use of quantum resources to enable cryptographic tasks under weaker assumptions (or even *unconditionally*) than classically were actually the first concrete proposals of quantum computing, with the seminal quantum money protocol of Wiesner [Wie83] and the key-exchange protocol of Bennet and Brassard [BB84].

Since then, it became a fundamental question in the field of quantum cryptography to find other primitives that can be implemented under weaker computational assumptions. It has recently shown that there exist quantum protocols for Oblivious Transfer (and therefore arbitrary multi-party computation (MPC)) based on the existence of one-way functions (OWF) [BCKM21, GLSV21]. Moreover, the proposed protocols use simple quantum technology that is available currently. The assumption to construct these primitives has been recently improved by showing that the existence of pseudo-random states (PRS) is sufficient for such primitives. Notice that existence of PRS is plausibly a strictly weaker assumption than the existence of OWF, given that PRS families can be constructed from OWF in a black-box way [JLS18], and we have oracle separations between PRS and OWF [Kre21, KQST22].

We notice that classically, OT and MPC are "Cryptomania" objects, meaning that they can be constructed from assumptions that imply public-key encryption (PKE), but there are oracle separations between OWF and PKE (and thus OT and MPC) [IR89]. Therefore, we do not expect that such powerful objects can be built classically from OWF. In this work, we investigate the following natural question:

> Can we have quantum protocols for public-key encryption, the heart of Cryptomania, based on post-quantum one-way functions, or even weaker assumptions?

Recent results imply that it is improbable to achieve PKE schemes from OWF if the public-key and ciphertext are classical even if the encryption or decryption algorithms are quantum [ACC$^+$22]. Therefore, in this work, we will consider schemes where the public-key or ciphertext are quantum states.

We notice that the first problem that we need to address is the syntax of quantum public-key encryption (qPKE) and the corresponding security games. We need to provide a general definition for qPKE where both the public-key and ciphertext might be general quantum states. Furthermore, we note that if the public-key is a quantum state, it might be measured, and the ciphertexts might depend on the measurement outcome. This motivates a stronger definition in which the adversary gets oracle access to the encryption, which we call IND-CPA-EO security.

With our new security definition in hand, we propose three protocols for implementing qPKE from OWF or weaker assumptions, with different advantages and disadvantages. More concretely, we show the following:

1. Assuming the existence of post-quantum OWFs, there exists a qPKE scheme with quantum public-keys and classical ciphertexts that is IND-CPA-EO security.

2. Assuming the existence of pseudo-random function-like states with proof of destruction (PRFSPDs), there is a qPKE scheme with quantum public-key and classical ciphertext that is IND-CPA-EO secure.

3. Assuming the existence of pseudo-random function-like states (PRFSs) with super-logarithmic input-size[1], there is a qPKE scheme with quantum public-key and quantum ciphertext. In this scheme, the quantum public key enables the encryption of a single message.

We would like to stress that for the first two constructions, even if the public-key is a quantum state, the ciphertexts are classical and one quantum public-key can be used to encrypt multiple messages. Our third construction shows how to construct quantum public key encryption from assumptions (the existence of pseudorandom function-like states) which are potentially weaker than post-quantum one-way functions, but the achieved protocol only allows the encryption of one message per public-key.

We would also like to remark that it has been recently shown that OWFs imply PRFSs with super-logarithmic input-size [AQY21] and PRFSPDs [BBSS23]. Therefore, the security of the second and third protocols is based on a potentially weaker cryptographic assumption than the first one. Furthermore, PRFSs with super-logarithmic input-size is *separated* from one-way functions [Kre21]; therefore, our third result shows a black-box separation between a certain form of quantum public key encryption and one-way functions.

However, the first protocol is much simpler to describe and understand since it only uses standard (classical) cryptographic objects. Moreover, it is the only scheme that achieves perfect correctness.

1.1 Technical overview

In this section we provide a technical overview of our results. In Section 1.1.1, we explain the challenges and choices in order to define qPKE and its security definition. In Section 1.1.2, we present our constructions for qPKE.

---

[1]Note that PRS implies PRFS with logarithmic size inputs. No such implication is known for super-logarithmic inputs.

1.1.1 Definitions of qPKE and IND-CPA-EO

In order to consider public-key encryption schemes with quantum public-keys, we need to first revisit the security definition and we define a new security game that we call IND-CPA-EO.

In the classical-key case (even with quantum ciphertexts), the adversary is given a copy the public-key pk and therefore is able to run the encryption algorithm $\mathsf{Enc}(\mathsf{pk}, \cdot)$ as many times they want (where the only constraint is that the adversary is polynomially bounded), and just then choose the messages m_0 and m_1 in the IND-CPA game.

In the quantum public-key case, the first issue is that $\mathsf{Enc}(\rho_{qpk}, \cdot)$ might consume the quantum public-key ρ_{qpk}. Moreover, having more copies of the quantum state could leak information to the adversary (which cannot be the case in the classical-key case, since the adversary *can* copy pk). Therefore, the first modification in IND-CPA towards IND-CPA-EO is that the adversary is given multiple copies of the public-key ρ_{qpk}.

Secondly, it could be the case that $\mathsf{Enc}(\rho_{qpk}, \cdot)$ measures ρ_{qpk} and modifying it to ρ'_{qpk}, which is different from ρ_{qpk} but still a valid key that enables encryption. The second modification that we need is syntactic: $\mathsf{Enc}(\rho_{qpk}, m)$ outputs (ρ'_{qpk}, c), where c is used as the ciphertext and ρ'_{qpk} is used as the key to encrypt the next message.

We notice that in the previous discussion, it could also be the case that Enc measures ρ_{qpk} and the measurement outcome is used to encrypt all the measurements. In this case, even if the adversary is given multiple copies of ρ_{qpk}, they would not be able to post-select on the same measurement outcome and the distribution of ciphertexts that they could generate would be different from the ones in the game. Therefore, we consider a stronger notion of security where the adversary has also access to the encryption oracle that will be used in the IND-CPA-EO game. We notice that this issue does not make sense classically since the public-key used by the challenger and adversary is exactly the same and the distribution of the ciphertexts would be the same.

Finally, we would like to mention a few problems with having ρ_{qpk} as a mixed state. Firstly, there is no efficient way of comparing if the two given public-keys are the same, preventing an honest decryptor to "compare" a purported public-key, whereas for pure states, this can be achieved using the swap-test. Secondly, if mixed states are allowed, then the notions of symmetric and public key encryption coincide, both in the classical and quantum setting: Consider a symmetric encryption scheme $(\mathsf{SKE.key\text{-}gen}, \mathsf{SKE.Enc}, \mathsf{SKE.Dec})$. We can transform it into a public-key scheme. To generate the keys, we use the output of $\mathsf{SKE.key\text{-}gen}$ as the secret-key and use it to create the uniform mixture $\frac{1}{2^n} \sum_{\in \{0,1\}^n} |x\rangle\langle x| \otimes |Enc_{sk}(x)\rangle\langle Enc_{sk}(x)|$ as public-key. The ciphertext of a message m is $(\mathsf{Enc}_x(m), \mathsf{Enc}_{sk}(x))$. To decrypt, the decryptor would first recover x by decrypting the second element in the ciphertext using sk, and then recover m by decrypting the first item using x as the secret key. Therefore, we have that the meaningful notion of PKE with quantum public-keys should consider only pure states as quantum public-keys.

1.1.2 Constructions for qPKE

As previously mentioned, we propose in this work three schemes for qPKE, based on different assumptions.

QPKE from OWFs. Our first scheme is based on the existence of post-quantum pseudo-random functions (PRF) and post-quantum IND-CPA secure symmetric-key encryption schemes, and both of these primitives can be constructed from post-quantum OWFs. More concretely, let $\{f_k\}_k$ be a keyed PRF family and $(\mathsf{SE.Enc}, \mathsf{SE.Dec})$ be a symmetric-key encryption scheme. The secret key dk of our scheme is a uniformly random key for the PRF, and for a fixed dk, the

quantum public-key state is

$$|qpk_{\mathsf{dk}}\rangle = \frac{1}{\sqrt{2^\lambda}} \sum_{x \in \{0,1\}^\lambda} |x\rangle |f_{\mathsf{dk}}(x)\rangle.$$

For clarity, we will drop the index of $|qpk\rangle$ when dk is clear from the context.

The encryption algorithm will then measure $|qpk\rangle$ in the computation basis leading to the outcome $(x^*, f_{\mathsf{dk}}(x^*))$. The ciphertext of a message m is $(x^*, \mathsf{SE.Enc}_{f(x^*)}(m))$ and the decryption algorithm receives as input a ciphertext $(\hat{x}, \hat{c})$ and outputs $\mathsf{SE.Dec}_{f(\hat{x})}(\hat{c})$.

Using a hybrid argument, we prove that any adversary that breaks the security of this qPKE scheme can be used to break the security of the PRF family or the security of the symmetric-key encryption scheme. The formal construction and its proof of security is given in Section 4.1.

We notice that such a scheme allows the encryption/decryption of many messages using the same measurement outcome $(x^*, f_{\mathsf{dk}}(x^*))$.

QPKE from PRFSPDs. Our second scheme is based on pseudo-random function-like states with proof of destruction (PRFSPDs), which was recently defined in [BBSS23]. A family of states $\{|\psi_{k,x}\rangle\}_{k,x}$ is pseudo-random function-like [AQY21] if

1. there is a quantum polynomial-time algorithm Gen such that

$$\mathsf{Gen}(k, \sum_x \alpha_x |x\rangle) = \sum_x \alpha_x |x\rangle |\psi_{k,x}\rangle, \text{ and}$$

2. no QPT adversary can distinguish $(|\psi_1\rangle, ..., |\psi_\ell\rangle)$ from $(|\phi_1\rangle, ..., |\phi_\ell\rangle)$, where $|\psi_i\rangle = \sum_x \alpha_x^i |x\rangle |\psi_{k,x}\rangle$, $|\phi_i\rangle = \sum_x \alpha_x^i |x\rangle |\phi_x\rangle$ and $\{|\phi_x\rangle\}_x$ are Haar random states and the states $|\sigma_i\rangle = \sum_x \alpha_x^i |x\rangle$ are chosen by the adversary.

Recently, [BBSS23] extended this notion to pseudo-random function-like states with proof of destruction, where we have two algorithms $\mathcal{Del}$ and $\mathcal{Ver}$, which allows us to verify if a copy of the PRFS was deleted.

We will discuss now how to provide the one-shot security[2] of the encryption of a one-bit message and we discuss later how to use it to achieve general security.

The quantum public-key in this simplified case is

$$\frac{1}{\sqrt{2^\lambda}} \sum_{x \in \{0,1\}^\lambda} |x\rangle |\psi_{\mathsf{dk},x}\rangle.$$

The encryptor will then measure the first register of $|qpk\rangle$ and the post-measurement state is $|x^*\rangle |\psi_{\mathsf{dk},x^*}\rangle$. The encryptor will then generate a proof of deletion $\pi = \mathcal{Del}(|\psi_{\mathsf{dk},x^*}\rangle)$. The encryption chooses $r \in \{0,1\}^\lambda$ uniformly at random and compute the ciphertext $c = (x^*, y)$ where $y = \begin{cases} r, & \text{if } b = 0 \\ \pi, & \text{if } b = 1 \end{cases}$.

The decryptor will receive some value $(\hat{x}, \hat{y})$ and decrypt the message $\hat{b} = \mathcal{Ver}(\mathsf{dk}, \hat{x}, \hat{y})$.

The proof of the security of such a scheme closely follows the proof of our first scheme.

Notice that repeating such a process in parallel trivially gives a one-shot security of the encryption of a string m and moreover, such an encryption is classical. Therefore, in order to achieve IND-CPA-EO secure qPKE scheme, we can actually encrypt a secret key sk that is chosen by the encryptor, and send the message encrypted under sk. We leave the details of such a construction and its proof of security to Section 4.2.

---

[2]Meaning that one can only encrypt once using $|qpk\rangle$.

QPKE from PRFSs. Finally, our third scheme uses the public-key

$$\frac{1}{\sqrt{2^\lambda}} \sum_{x \in \{0,1\}^\lambda} |x\rangle |\psi_{\mathsf{dk},x}\rangle,$$

where $\{|\psi_{k,x}\rangle\}_{k,x}$ is a PRFS family and the size of the input x is super-logarithmic on the security parameter.

The encryptor will then measure the first register of $|qpk\rangle$ and the post-measurement state is $|x^*\rangle |\psi_{\mathsf{dk},x^*}\rangle$. The encryptor will then compute the ciphertext $c = (x^*, \rho)$ where

$$y = \begin{cases} I, & \text{if } b = 0 \\ |\psi_{\mathsf{dk},x^*}\rangle\langle\psi_{\mathsf{dk},x^*}|, & \text{if } b = 1 \end{cases}.$$

The decryptor, on ciphertext $c = (\hat{x}, \hat{\rho})$, sets $\hat{b} \leftarrow \mathsf{Test}(\mathsf{dk}, \hat{x}, \hat{\rho})$, where Test is a tester algorithm checking whether $\hat{\rho}$ is the output of the PRFS generator with key dk and input $\hat{x}$, that is whether $\hat{\rho} = |\psi_{\mathsf{dk},\hat{x}}\rangle\langle\psi_{\mathsf{dk},\hat{x}}|$.

The proof of the security of such a scheme also closely follows the one of our first scheme, and we give the formal construction in Section 4.3.

1.2 Related works

Gottesman [Got05] has a candidate construction (without formal security analysis) encryption scheme with quantum public keys and quantum ciphers, which consumes the public key for encryption. Ref. [OTU00] defines and constructs a public-key encryption where the keys, plaintexts and ciphers are classical, but the algorithms are quantum. (In their construction, only the key-generation uses Shor's algorithm.)

In [NI09], the authors define and provide impossibility results regarding encryption with quantum public keys. Classically, it is easy to show that a (public) encryption scheme cannot have deterministic ciphers; in other words, encryption must use randomness. They show that this is also true for a quantum encryption scheme with quantum public keys.

In Ref. [MY22a, MY22b], the authors study digital signatures with quantum signatures, and more importantly in the context of this work, quantum public keys.

1.3 Concurrent and independent work

Very recently, two concurrent and independent works have achieved similar tasks. Coladangelo [Col23] shows a qPKE scheme whose construction is very different from ours, and uses a quantum trapdoor function, which is a new notion first introduced in their work. The hardness assumption is the existence of post-quantum OWF. Each quantum public key can be used to encrypt a single message (compared to our construction from OWF, where the public key can be used to encrypt multiple messages). The ciphertexts are quantum (whereas our construction from OWF has classical ciphertexts). Barooti, Malavolta and Walter [BMW23] also construct a qPKE scheme based on OWF. Their construction has quantum public keys and classical ciphertexts, and is very similar to the construction we propose in Section 4.1. They do not discuss the notion of IND-CPA-EO security, but we believe that the hybrid encryption approach we use to achieve IND-CPA-EO can be used in their construction as well. Moreover, their construction also achieves CCA security, which is stronger than CPA security. They leave open the question of constructing qPKE from weaker assumptions than OWF, which we answer affirmatively in our work.

2 Definitions and Preliminaries

2.1 Notation

Throughout this paper, λ denotes the security parameter. The notation $\mathsf{negl}(\lambda)$ denotes any function f such that $f(\lambda) = \lambda^{-\omega(1)}$, and $\mathsf{poly}(\lambda)$ denotes any function f such that $f(\lambda) = \mathcal{O}(\lambda^c)$ for some $c > 0$. When sampling uniformly at random a value a from a set $\mathcal{U}$, we employ the notation $a \leftarrow_\$ \mathcal{U}$. When sampling a value a from a probabilistic algorithm $\mathcal{A}$, we employ the notation $a \leftarrow \mathcal{A}$. Let $|\cdot|$ denote either the length of a string, or the cardinal of a finite set, or the absolute value. By PPT we mean a polynomial-time non-uniform family of probabilistic circuits, and by QPT we mean a polynomial-time family of quantum circuits.

2.2 Pseudorandom Function-Like State (PRFS) Generators

The notion of pseudorandom states were first introduced by Ananth, Qian and Yuen in [AQY21]. A stronger definition where the adversary is allowed to make superposition queries to the challenge oracles was introduced in the follow-up work [AGQY23]. We reproduce their definition here:

Definition 1 (Quantum-accessible PRFS generator). *We say that a QPT algorithm G is a quantum-accessible secure pseudorandom function-like state generator if for all QPT (non-uniform) distinguishers A if there exists a negligible function ϵ, such that for all λ, the following holds:*

$$\left| \Pr_{k \leftarrow \{0,1\}^{1^\lambda}} \left[A_\lambda^{|\mathcal{O}_{\mathsf{PRFS}}(k,\cdot)\rangle}(\rho_\lambda) = 1 \right] - \Pr_{\mathcal{O}_{\mathsf{Haar}}} \left[A_\lambda^{|\mathcal{O}_{\mathsf{Haar}}(\cdot)\rangle}(\rho_\lambda) = 1 \right] \right| \leq \epsilon(\lambda),$$

where:

- $\mathcal{O}_{\mathsf{PRFS}}(k, \cdot)$, *on input a d-qubit register $\mathbf{X}$, does the following: it applies an isometry channel that controlled on the register $\mathbf{X}$ containing x, it creates and stores $G_{1^\lambda}(k, x)$ in a new register $\mathbf{Y}$. It outputs the state on the registers $\mathbf{X}$ and $\mathbf{Y}$.*

- $\mathcal{O}_{\mathsf{Haar}}(\cdot)$, *modeled as a channel, on input a d-qubit register $\mathbf{X}$, does the following: it applies a channel that controlled on the register $\mathbf{X}$ containing x, stores $|\vartheta_x\rangle\langle\vartheta_x|$ in a new register $\mathbf{Y}$, where $|\vartheta_x\rangle$ is sampled from the Haar distribution. It outputs the state on the registers $\mathbf{X}$ and $\mathbf{Y}$.*

Moreover, A_{1^λ} has superposition access to $\mathcal{O}_{\mathsf{PRFS}}(k, \cdot)$ and $\mathcal{O}_{\mathsf{Haar}}(\cdot)$ (denoted using the ket notation).

We say that G is a $(d(\lambda), n(\lambda))$-QAPRFS generator to succinctly indicate that its input length is $d(\lambda)$ and its output length is $n(\lambda)$.

Given a state ρ, it is useful to know whether it is the output of a PRFS generator with key k and input x. The following lemma shows the existence of a tester algorithm to test any PRFS states in a semi-black-box way.

Lemma 1. *[AQY21, Lemma 3.10] Let G be a (d, n)-PRFS generator. There exists a QPT algorithm $\mathsf{Test}(k, x, \cdot)$, called the tester algorithm for $G(k, x)$, such that here exists a negligible function $\nu(\cdot)$ such that for all λ, for all $x \neq y$,*

$$\Pr_k[\mathsf{Test}(k, x, G(k, x)) = 1] \geq 1 - \nu(\lambda),$$

and

$$\Pr_k[\mathsf{Test}(k, x, G(k, y)) = 1] \leq 2^{-n(\lambda)} + \nu(\lambda).$$

2.3 Quantum Pseudorandomness with Proofs of Destruction

The rest of this section is taken verbatim from [BBSS23].

Game 1 Clonning-Exp$_\lambda^{\mathcal{A},\mathsf{PRSPD}}$

1: Given input 1^λ, Challenger samples $k \leftarrow \{0,1\}^{w(\lambda)}$ uniformly at random.
2: $\mathcal{A}$ sends m to the challenger.
3: Challenger runs $\mathsf{Gen}(k)^{\otimes m}$ and sends $|\psi_k\rangle^{\otimes m}$ to $\mathcal{A}$.
4: $\mathcal{A}$ gets classical oracle access to $\mathcal{V}er(k, \cdot)$.
5: $\mathcal{A}$ outputs $c_1, c_2, \ldots, c_{m+1}$ to the challenger.
6: Challenger rejects if c_i's are not distinct.
7: **for** $i \in [m+1]$ **do** Challenger runs $b_i \leftarrow \mathcal{V}er(k, c_i)$
8: **end for**
9: Return $\wedge_{i=1}^{m+1} b_i$.

Definition 2 (Pseudorandom function-like state generator with proofs of destruction). *A PRFSPD scheme with key-length $w(\lambda)$, input-length $d(\lambda)$, output length $n(\lambda)$ and proof length $c(\lambda)$ is a tuple of QPT algorithms* $\mathsf{Gen}, \mathcal{D}el, \mathcal{V}er$ *with the following syntax:*

1. $|\psi_k^x\rangle \leftarrow \mathsf{Gen}(k, x)$: *takes a key $k \in \{0,1\}^w$, an input string $x \in \{0,1\}^{d(\lambda)}$, and outputs an n-qubit pure state $|\psi_k^x\rangle$.*

2. $p \leftarrow \mathcal{D}el(|\phi\rangle)$: *takes an n-qubit quantum state $|\phi\rangle$ as input, and outputs a c-bit classical string, p.*

3. $b \leftarrow \mathcal{V}er(k, x, q)$: *takes a key $k \in \{0,1\}^w$, a d-bit input string x, a c-bit classical string p and outputs a boolean output b.*

Correctness. *A PRFSPD scheme is said to be correct if for every $x \in \{0,1\}^d$,*

$$\Pr_{k \xleftarrow{u} \{0,1\}^w} [1 \leftarrow \mathcal{V}er(k, x, p) \mid p \leftarrow \mathcal{D}el(|\psi_k^x\rangle); |\psi_k^x\rangle \leftarrow \mathsf{Gen}(k, x)] = 1$$

Security.

1. *Pseudorandomness: A PRFSPD scheme is said to be (adaptively) pseudorandom if for any QPT adversary $\mathcal{A}$, and any polynomial $m(\lambda)$, there exists a negligible function $\mathsf{negl}(\lambda)$, such that*

$$\left| \Pr_{k \leftarrow \{0,1\}^w} [\mathcal{A}^{\mathsf{Gen}(k,\cdot)}(1^\lambda) = 1] - \Pr_{\forall x \in \{0,1\}^d, |\phi^x\rangle \leftarrow \mu_{(\mathbb{C}^2)^{\otimes n}}} [\mathcal{A}^{\mathcal{H}aar^{\{|\phi^x\rangle\}_{x \in \{0,1\}^d}}(\cdot)}(1^\lambda) = 1] \right| = \mathsf{negl}(\lambda),$$

where $\forall x \in \{0,1\}^d$, $\mathcal{H}aar^{\{|\phi^x\rangle\}_{x \in \{0,1\}^d}}(x)$ outputs $|\phi^x\rangle$. Here $\mathcal{A}^{\mathsf{Gen}(k,\cdot)}$ represents that $\mathcal{A}$ gets classical oracle access to $\mathsf{Gen}(k, \cdot)$.

2. Unclonability-of-proofs: *A PRFSPD scheme satisfies* Unclonability-of-proofs *if for any QPT adversary $\mathcal{A}$ in cloning game (see Game 2), there exists a negligible function $\mathsf{negl}(\lambda)$ such that*

$$\Pr[\mathsf{Clonning\text{-}Exp}_\lambda^{\mathcal{A},\mathsf{PRFSPD}} = 1] = \mathsf{negl}(\lambda).$$

Game 2 Clonning-Exp$_\lambda^{\mathcal{A},\text{PRFSPD}}$

1: Given input 1^λ, Challenger samples $k \leftarrow \{0,1\}^{w(\lambda)}$ uniformly at random.
2: Initialize an empty set of variables, S.
3: $\mathcal{A}$ gets oracle access to $\mathsf{Gen}(k,\cdot)$, $\mathcal{V}er(k,\cdot,\cdot)$ as oracle.
4: **for** Gen query x made by $\mathcal{A}$ **do**
5:     **if** $\exists$ variable $t_x \in S$ **then** $t_x = t_x + 1$.
6:     **else** Create a variable t_x in S, initialized to 1.
7:     **end if**
8: **end for**
9: $\mathcal{A}$ outputs $x, c_1, c_2, \ldots, c_{t_x+1}$ to the challenger.
10: Challenger rejects if c_i's are not distinct.
11: **for** $i \in [m+1]$ **do** $b_i \leftarrow \mathcal{V}er(k,x,c_i)$
12: **end for**
13: Return $\wedge_{i=1}^{m+1} b_i$.

3 Security definitions for qPKE

In this section, we introduce the new notion of encryption with quantum public keys (Definition 3) and present our indistinguishability under chosen-plaintext attacks security for quantum public-key encryption.

Definition 3 (Encryption with quantum public keys)**.** *Encryption with quantum public keys (qPKE) consists of 4 algorithms with the following syntax:*

1. $\mathsf{dk} \leftarrow \mathsf{Gen}(1^\lambda)$*: a* PPT *algorithm, which receives the security parameter and outputs a classical decryption key.*

2. $|qpk\rangle \leftarrow \mathcal{QPKGen}(\mathsf{dk})$*: a* QPT *algorithm, which receives a classical decryption key* dk*, and outputs a quantum public key* $|qpk\rangle$*. We require that the output is a pure state, and that* t *calls to* $\mathcal{QPKGen}(\mathsf{dk})$ *should yield the same state, that is,* $|qpk\rangle^{\otimes t}$*.*

3. $(qpk', qc) \leftarrow \mathcal{Enc}(qpk, m)$*: a* QPT *algorithm, which receives a quantum public key* qpk *and a plaintext* m*, and outputs a (possibly classical) ciphertext* qc *and a recycled public-key* qpk'*.*

4. $m \leftarrow \mathcal{Dec}(\mathsf{dk}, qc)$*: a* QPT *algorithm, which uses a decryption key* dk *and a ciphertext* qc*, and outputs a classical plaintext* m*. In the case* qc *is classical, we consider* $\mathcal{Dec}$ *as a* PPT *algorithm.*

We say that a qPKE scheme is complete if for every message $m \in \{0,1\}^*$ and any security parameter $\lambda \in \mathbb{N}$, the following holds:

$$\Pr\left[\mathcal{Dec}(\mathsf{dk}, qc) = m \;\middle|\; \begin{array}{r} \mathsf{dk} \leftarrow \mathsf{Gen}(1^\lambda) \\ |qpk\rangle \leftarrow \mathcal{QPKGen}(\mathsf{dk}) \\ (qpk', qc) \leftarrow \mathcal{Enc}(|qpk\rangle, m) \end{array} \right] \geq 1 - \mathsf{negl}(\lambda),$$

where the probability is taken over the randomness of Gen, $\mathcal{QPKGen}$ and $\mathcal{Enc}$.

Next, we present a quantum analogue of classical indistinguishability under chosen-plaintext attacks security (denoted as IND-CPA) for qPKE.

Definition 4. *A qPKE scheme is IND-CPA secure if for every* QPT *adversary, there exists a negligible function* ϵ *such that the probability of winning the IND-CPA security game (see Game 3) is at most* $\frac{1}{2} + \epsilon(\lambda)$*.*

Game 3 IND-CPA security game for encryption with quantum public key schemes.

1: The challenger generates $\mathsf{dk} \leftarrow \mathsf{Gen}(1^\lambda)$.
2: The adversary gets 1^λ as an input, and oracle access to $\mathit{QPKGen}(\mathsf{dk})$, and sends m_0, m_1 of the same length to the challenger.
3: The challenger samples $b \in_R \{0,1\}$, generates $|\mathit{qpk}\rangle \leftarrow \mathit{QPKGen}(\mathsf{dk})$ and sends $c \leftarrow \mathit{Enc}(|\mathit{qpk}\rangle, m_b)$ to the adversary.
4: The adversary outputs a bit b'.

We say that the adversary wins the game (or alternatively, that the outcome of the game is 1) iff $b = b'$.

Note that this is the standard CPA-security game of a public-key encryption scheme, with the exception that the adversary can receive polynomially many copies of $|\mathit{qpk}\rangle$, by making several calls to the $\mathit{QPKGen}(\mathsf{dk})$ oracle.

In the classical setting, there is no need to provide access to an encryption oracle since the adversary can use the public key to apply the encryption herself. In the quantum setting, this is not the case: as we will see, the quantum public key might be measured, and the ciphertexts might depend on the measurement outcome. This motivates a stronger definition in which the adversary gets oracle access to the encryption, denoted as IND-CPA-EO security.

Definition 5. *A qPKE scheme is (single-challenge) IND-CPA-EO secure if for every* QPT *adversary, there exists a negligible function ϵ such that the probability of winning the IND-CPA-EO security game (see Game 4) is at most $\frac{1}{2} + \epsilon(\lambda)$.*

Game 4 (Single-challenge) Chosen plaintext attack with an encryption oracle (IND-CPA-EO) security game for encryption with quantum public key schemes.

1: The challenger generates $\mathsf{dk} \leftarrow \mathsf{Gen}(1^\lambda)$.
2: The adversary gets 1^λ as an input, and oracle access to $\mathit{QPKGen}(\mathsf{dk})$.
3: The challenger generates $|\mathit{qpk}\rangle \leftarrow \mathit{QPKGen}(\mathsf{dk})$. Let $\mathit{qpk}_1 := |\mathit{qpk}\rangle$.
4: For $i = 1, \ldots, \ell$, the adversary creates a classical message m_i and send it to the challenger.
5: The challenger computes $(qc_i, \mathit{qpk}_{i+1}) \leftarrow \mathit{Enc}(\mathit{qpk}_i, m_i)$ and send qc_i to the adversary.
6: The adversary sends two messages m'_0, m'_1 of the same length to the challenger.
7: The challenger samples $b \in_R \{0,1\}$, computes $(qc^*, \mathit{qpk}_{l+2}) \leftarrow \mathit{Enc}(\mathit{qpk}_{\ell+1}, m'_b)$ and sends qc^* to the adversary.
8: For $i = \ell+2, \ldots, \ell'$, the adversary creates a classical message m_i and send it to the challenger.
9: The challenger computes $(qc_i, \mathit{qpk}_{i+1}) \leftarrow \mathit{Enc}(\mathit{qpk}_i, m_i)$ and send qc_i to the adversary.
10: The adversary outputs a bit b'.

We say that the adversary wins the game (or alternatively, that the outcome of the game is 1) iff $b = b'$.

Definition 6. *A qPKE scheme is (multi-challenge) IND-CPA-EO secure if for every* QPT *adversary, there exists a negligible function ϵ such that the probability of winning the IND-CPA-EO security game (see Game 5) is at most $\frac{1}{2} + \epsilon(\lambda)$.*

Theorem 1. *Single-challenge security (Definition 5) implies multi-challenge security (Definition 6).*

Proof. Recall that classically, single-challenge IND-CPA implies multi-challenge IND-CPA, see, e.g., [KL14, Theorem 3.24]. Following the exact same argument works in our case as well: single-challenge IND-CPA-EO implies multi-challenge IND-CPA-EO. $\square$

Game 5 (Multi-challenge) Chosen plaintext attack with an encryption oracle (IND-CPA-EO) security game for encryption with quantum public key schemes.

1: The challenger generates $\mathsf{dk} \leftarrow \mathsf{Gen}(1^\lambda)$.
2: The adversary gets 1^λ as an input, and oracle access to $\mathcal{QPKGen}(\mathsf{dk})$.
3: The challenger generates $|qpk\rangle \leftarrow \mathcal{QPKGen}(\mathsf{dk})$. Let $qpk_1 := |qpk\rangle$.
4: For $i = 1, \ldots, \ell$, the adversary creates a classical message m_i and send it to the challenger.
5: The challenger computes $(qc_i, qpk_{i+1}) \leftarrow \mathcal{Enc}(qpk_i, m_i)$ and send qc_i to the adversary.
6: The adversary sends two messages m'_0, m'_1 of the same length to the challenger.
7: The challenger samples $b \in_R \{0,1\}$, computes $(qc^*, qpk_{l+2}) \leftarrow \mathcal{Enc}(qpk_{\ell+1}, m'_b)$ and sends qc^* to the adversary.
8: For $i = \ell+2, \ldots, \ell'$, the adversary creates a classical message m_i and send it to the challenger.
9: The challenger computes $(qc_i, qpk_{i+1}) \leftarrow \mathcal{Enc}(qpk_i, m_i)$ and send qc_i to the adversary.
10: The challenger and the adversary can repeat step 3 - 9 polynomially many times. For the i-th repetition, let $qpk_{1,i}$ be $qpk_{l'+1,i-1}$.
11: The challenger and the adversary can repeat step 3 - 10 polynomially many times.
12: The adversary outputs a bit b'.

We say that the adversary wins the game (or alternatively, that the outcome of the game is 1) iff $b = b'$.

4 Constructions

4.1 QPKE with Classical ciphertext from OWFs

We show a construction based on the existence of post-quantum one-way functions. Recalls that post-quantum one-way functions imply a qPRF [Zha12], and IND-CPA[3] symmetric encryption [BZ13].

Assumes: A PRF family $\{f_k\}_k$, and a symmetric encryption scheme $\{\mathsf{Enc}, \mathsf{Dec}\}$.
$\mathsf{Gen}(1^\lambda)$
    1. $\mathsf{dk} \leftarrow_R \{0,1\}^\lambda$.
$\mathcal{QPKGen}(\mathsf{dk})$
    1. Output $|qpk\rangle = \frac{1}{\sqrt{2^\lambda}} \sum_{x \in \{0,1\}^\lambda} |x\rangle |f_{\mathsf{dk}}(x)\rangle$.
$\mathcal{Enc}(|qpk\rangle, m)$
    1. Measure both registers of $|qpk\rangle$ in the standard basis. Denote the result as x and y.
    2. Output $c = (x, \mathsf{Enc}(y, m))$.
$\mathsf{Dec}_{\mathsf{dk}}(c)$
    1. Interpret c as (x, z)
    2. Set $y := f_{\mathsf{dk}}(x)$.
    3. Output $m = \mathsf{Dec}(y, z)$.

Figure 1: An encryption scheme with quantum public keys.

Theorem 2. *Assuming the existence of quantum-secure PRF family $\{f_k\}_k$ and post-quantum IND-CPA symmetric-key encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$, any QPT adversary $\mathcal{A}$ wins the IND-CPA-EO game for the scheme presented in Figure 1 with advantage at most $\mathsf{negl}(\lambda)$.*

Proof. In order to prove our results, we define the following Hybrids.
Hybrid H_0. The original security game as defined in Algorithm 4.

---

[3]In fact, this can be strengthened to IND-qCCA security, but this is unnecessary for our application.

Hybrid H_1. Same as Hybrid H_0, except that the challenger, instead of measuring $|qpk\rangle$ when the adversary queries the encryption oracle for the first time, the challenger measures this state before providing the copies of $|qpk\rangle$ to the adversary. Note that by measuring $|qpk\rangle$ in the computational basis, the challenger would obtain a uniformly random string x^* (and the corresponding $f_{\mathsf{dk}}(x^*)$).

Hybrid H_2. Same as Hybrid H_1, except that the challenger samples x^* as in the previous hybrid, and instead of providing $|qpk\rangle$ to the adversary, she provides

$$|qpk'\rangle = \frac{1}{\sqrt{2^\lambda - 1}} \sum_{x \in \{0,1\}^*, x \neq x^*} |x\rangle|f_{\mathsf{dk}}(x)\rangle.$$

Moreover, the challenger provides ciphertexts $(x^*, \mathsf{Enc}(f_{\mathsf{dk}}(x^*), m))$ for the chosen messages m. We note that this state $|qpk'\rangle$ can be efficiently prepared by computing the functions δ_{x,x^*} over the state $\sum_x |x\rangle$ in superposition and measuring the output register. With overwhelming probability, the post-measurement state is $\sum_{x \neq x^*} |x\rangle$.

Hybrid H_3. Same as Hybrid H_2, except the challenger uses a random function H in place of f_{dk}, and provides $|qpk'\rangle = \frac{1}{\sqrt{2^\lambda - 1}} \sum_{x \in \{0,1\}^*, x \neq x^*} |x\rangle|H(x)\rangle$. Moreover, for each encryption query, the challenger uses $H(x^*)$ as qpk_i, and answers the query with $(x^*, \mathsf{Enc}(H(x^*), m))$ for the chosen message m.

Hybrid H_4. Same as Hybrid H_3, except the challenger samples uniformly at random a string z, and uses z as qpk_i. The answer to each encryption query is now $(x^*, \mathsf{Enc}(z, m))$ for the chosen message m.

We will now show that, given our assumptions, Hybrids H_i and H_{i+1} are indistinguishable except with probability at most $\mathsf{negl}(\lambda)$ and that every polynomial-time adversary wins H_4 with advantage at most $\mathsf{negl}(\lambda)$. We can then use triangle inequality to prove the security of Theorem 2.

Lemma 2. *No adversary can distinguish Hybrid H_0 and Hybrid H_1 with non-zero advantage.*

Proof. Notice that the operations corresponding to the challenger's measurement of $|qpk\rangle$ and the creation of the copies of $|qpk\rangle$ given to the adversary commute. In this case, we can swap the order of these operations and the outcome is exactly the same. $\square$

Lemma 3. *No adversary can distinguish Hybrid H_1 and Hybrid H_2 with non-negligible advantage.*

Proof. Notice that distinguishing the two adversaries imply that we can distinguish the following quantum states $|qpk\rangle^{\otimes p} \otimes |x^*\rangle$ and $|qpk'\rangle^{\otimes p} \otimes |x^*\rangle$, but these two quantum states have $1 - \mathsf{negl}(\lambda)$ trace-distance for any polynomial p. Therefore, this task can be performed with success at most $\mathsf{negl}(\lambda)$. $\square$

Lemma 4. *No QPT adversary can distinguish Hybrid H_2 and Hybrid H_3 with non-negligible advantage.*

Proof. Suppose that there exists an adversary $\mathcal{A}$ such that $\Pr[F_1] - \Pr[F_2] \geq \frac{1}{p(\lambda)}$ for some polynomial p, where F_1 is the event where $\mathcal{A}$ outputs 1 on H_2 and F_2 is the event where $\mathcal{A}$ outputs 1 on H_3. Then, we show that we can construct an adversary $\mathcal{A}'$ that can distinguish the PRF family from random.

$\mathcal{A}'$ will behave as the challenger in the CPA-EO game and instead of computing f_{dk} to create $|qpk'\rangle$ and answer the encryption queries, she queries the oracle O (that is either a PRF or a random function). $\mathcal{A}'$ then outputs 1 iff $\mathcal{A}$ outputs 1.

Notice that if O is a PRF, then the experiment is the same as Hybrid H_2. On the other hand, if O is a random oracle, the experiment is the same as Hybrid H_3.

In this case, we have that

$$\Pr_{O\sim\mathcal{F}}[\mathcal{A}'^{O}() = 1] - \Pr_{\mathsf{dk}}[\mathcal{A}'^{f_{\mathsf{dk}}}() = 1]$$
$$= \Pr[F_1] - \Pr[F_2]$$
$$\geq \frac{1}{p(\lambda)}.$$

$\square$

Lemma 5. *No adversary can distinguish Hybrid H_3 and Hybrid H_4 with non-zero advantage.*

Proof. Since the adversary never gets the evaluation of $H(x^*)$ (as x^* was punctured from all $|qpk\rangle$), the distributions of the two hybrid are identical. $\square$

Lemma 6. *Any polynomially-bounded adversary wins the game in Hybrid H_4 with an advantage at most $\mathsf{negl}(\lambda)$.*

Proof. Suppose that there exists an adversary $\mathcal{A}$ such that wins the game in Hybrid H_4 with advantage $\frac{1}{p(\lambda)}$ for some polynomial p. Then, we show that we can construct an adversary $\mathcal{A}'$ that can break IND-CPA security of the symmetric-key encryption scheme with the same probability.

$\mathcal{A}'$ will simulate $\mathcal{A}$ and for that, she picks x^* and z, creates $|qpk'\rangle = \frac{1}{\sqrt{2^\lambda - 1}} \sum_{x\in\{0,1\}^*, x\neq x^*} |x\rangle|H(x)\rangle$ using the compressed oracle technique [Zha19] and uses oracle provided by the IND-CPA game of the symmetric-key encryption scheme for answering the encryption oracles. $\mathcal{A}'$ will output 1 iff $\mathcal{A}$ outputs 1. We note that the encryption key z is sampled uniformly at random independently of all other variables. We have that the winning probability of $\mathcal{A}'$ in the IND-CPA game is the same of $\mathcal{A}$ in the IND-CPA-EO game. $\square$

$\square$

4.2 QPKE with Classical Ciphertexts from PRFSPDs

In this section, we propose a construction for qPKE from pseudo-random function-like states with proof of destruction.

In this section, we construct a qPKE scheme based on PRFSPD. For that, we need the following result that builds *symmetric*-key encryption from such an assumption.

Proposition 1 ([BBSS23]). *If quantum-secure PRFSPD exists, then there exists a quantum CPA symmetric encryption with classical ciphertexts.*

Theorem 3. *If quantum-secure PRFSPD with super-logarithmic input size exists, then there exists a public-key encryption with classical ciphertexts which is IND-CPA-EO secure.*

Proof. Our construction is given in Fig. 2. It uses a PRFSPD, as well as a quantum CPA *symmetric* encryption with classical ciphertexts. Such symmetric encryption is known to exist, based on PRFSPD:

In order to prove our results, we define the following Hybrids.

Hybrid H_0. This is the original security game.

Assumes: A PRFSPD family $\{|\psi_{\mathsf{dk},x}\rangle\}_{\mathsf{dk},x}$ and a quantum symmetric encryption scheme with classical ciphers $\{\mathsf{Enc}, \mathsf{Dec}\}$.

$\mathsf{Gen}(1^\lambda)$

    1. $\mathsf{dk} \leftarrow_R \{0,1\}^\lambda$.

$\mathcal{QPKG}en(\mathsf{dk})$

    1. Output $|qp\mathcal{k}\rangle = \bigotimes_{i \in [\lambda]} \frac{1}{\sqrt{2^\lambda}} \sum_{x^{(i)} \in \{0,1\}^\lambda} |x^{(i)}\rangle |\psi_{\mathsf{dk},x^{(i)}}\rangle$.

$\mathcal{E}nc(|qp\mathcal{k}\rangle, m)$ for $m \in \{0,1\}$

    1. Let $|qp\mathcal{k}_i\rangle := \frac{1}{\sqrt{2^\lambda}} \sum_{x^{(i)} \in \{0,1\}^\lambda} |x^{(i)}\rangle |\psi_{\mathsf{dk},x^{(i)}}\rangle$, and write $|qp\mathcal{k}\rangle$ as $|qp\mathcal{k}\rangle = \bigotimes_{i \in [\lambda]} |qp\mathcal{k}_i\rangle$.

    2. Measure the left registers of $|qp\mathcal{k}_i\rangle$ to obtain classical strings $x^{(i)}$. Denote the post-measurement states as $|\psi'_i\rangle$.

    3. Set $y^{(i)} \leftarrow \mathcal{D}el(|\psi'\rangle)$.

    4. Pick $k = \{0,1\}^\lambda$ and $r^{(i)} = \{0,1\}^{|y^{(i)}|}$ uniformly at random.

    5. Set $\tilde{y}^{(i)} = \begin{cases} r^{(i)} & \text{, if } k_i = 0 \\ y^{(i)} & \text{, if } k_i = 1 \end{cases}$.

    6. Output $\left(\mathsf{Enc}(k, m), \left((x^{(i)}, \tilde{y}^{(i)}) \right)_i \right)$

$\mathsf{Dec}_{\mathsf{dk}}(c)$

    1. Interpret c as $\left(c', \left((x^{(i)}, \tilde{y}^{(i)}) \right)_i \right)$

    2. Let $k'_i = \mathcal{V}er(x^{(i)}, \tilde{y}^{(i)})$.

    3. Output $\mathsf{Dec}(k', c')$

Figure 2: An encryption scheme with quantum public keys.

Hybrid H_1. Same as Hybrid H_0, except that the challenger picks $x^{(i)*}$ uniformly at random, instead of providing $|qp\mathcal{k}\rangle$ to the adversary, she provides

$$|qp\mathcal{k}'\rangle = \bigotimes_{i \in [\lambda]} \frac{1}{\sqrt{2^\lambda - 1}} \sum_{x^{(i)} \in \{0,1\}^\lambda, x^{(i)} \neq x^{(i)*}} |x^{(i)}\rangle |\psi_{\mathsf{dk},x^{(i)}}\rangle.$$

The challenger uses the states $|x^{(i)*}\rangle |\psi_{\mathsf{dk},x^{(i)*}}\rangle$ to encrypt the challenge.

Hybrid H_2. Same as Hybrid H_1, but to answer the encryption queries, the challenger picks each $\tilde{y}^{(i)}$ uniformly at random and answers the encryption queries with $\left(\mathsf{Enc}(k, m), \left((x^{(i)}, \tilde{y}^{(i)}) \right)_i \right)$

We will now show that, given our assumptions, Hybrids H_i and H_{i+1} are indistinguishable except with probability at most $\mathsf{negl}(\lambda)$ and that every polynomial-time adversary wins H_3 with advantage at most $\mathsf{negl}(\lambda)$. We can then use triangle inequality to prove the security of Theorem 3.

Lemma 7. *No adversary can distinguish Hybrid H_0 and Hybrid H_1 with non-zero advantage.*

Proof. The proof follows analogously to Lemmas 2 and 3 and the triangle inequality. $\qquad\square$

Lemma 8. *No adversary can distinguish Hybrid H_2 and Hybrid H_3 with non-negligible advantage.*

Proof. Suppose that there exists an adversary $\mathcal{A}$ such that $\Pr[F_1] - \Pr[F_2] \geq \frac{1}{p(\lambda)}$ for some polynomial p, where F_1 is the event where $\mathcal{A}$ outputs 1 on H_2 and F_2 is the event where $\mathcal{A}$ outputs 1 on H_3. Then, we show that we can construct an adversary $\mathcal{A}'$ that can break the PRFSPD family scheme.

$\mathcal{A}'$ will behave as the challenger in the CPA-EO game and instead of computing $|qp\mathcal{k}'\rangle$ by herself, she queries the oracle O (that on input $|x\rangle|0\rangle$ answers either a PRFSPD $|x\rangle|\psi_{\mathsf{dk},x}\rangle$ or a Haar random state $|x\rangle|\vartheta_x\rangle$). Then, $\mathcal{A}'$ picks a random bit b and performs as follows:

- if $b = 0$, $\mathcal{A}'$ answers the encryption queries as Hybrid H_2

- if $b = 1$, $\mathcal{A}'$ picks each $\tilde{y}^{(i)}$ uniformly at random and answers the encryption queries with $\left(Enc_k(m), \left((x^{(i)}, \tilde{y}^{(i)})\right)_i\right)$

$\mathcal{A}'$ then outputs 1 iff $\mathcal{A}$ outputs 1.

Notice that if $b = 0$ and O answers a PRFSPD, then the experiment is the same as Hybrid H_2. On the other hand, if $b = 0$ and O is a random oracle or if $b = 1$, the experiment is the same as Hybrid H_3. Let us define the event E_1 be the event where $\mathcal{A}'$ outputs 1 if O is a PRFSPD, and E_2 be the event where $\mathcal{A}'$ outputs 1 if O answers with Haar random states.

In this case, we have that $\mathcal{A}'$ distinguishes the PRFS family from Haar random states with probability

$$\Pr[E_1] - \Pr[E_2]$$
$$= \frac{1}{2}\left(\Pr[E_1 \wedge b = 0] + \Pr[E_1 \wedge b = 1] - \Pr[E_2 \wedge b = 0] - \Pr[E_2 \wedge b = 1]\right)$$
$$= \frac{1}{2}\left(\Pr[F_1] + \Pr[F_2] - \Pr[F_2] - \Pr[F_2]\right)$$
$$\geq \frac{1}{2p(\lambda)}.$$

$\square$

Lemma 9. *Any polynomially-bounded adversary wins the game in Hybrid H_3 with an advantage at most $\mathsf{negl}(\lambda)$.*

Proof. Suppose that there exists an adversary $\mathcal{A}$ such that wins the game in Hybrid H_3 with advantage $\frac{1}{p(\lambda)}$ for some polynomial p. Then, we show that we can construct an adversary $\mathcal{A}'$ that can break IND-CPA security of the symmetric-key encryption scheme.

$\mathcal{A}'$ will simulate $\mathcal{A}$ and for that, she picks dk and creates $|qpk'\rangle$ and in order to answer the encryption queries, they use the encryption oracle provided by the IND-CPA game. $\mathcal{A}'$ will output 1 iff $\mathcal{A}$ outputs 1. We have that the winning probability of $\mathcal{A}'$ in its IND-CPA game is the same of $\mathcal{A}$ in its IND-CPA-EO game. $\square$

$\square$

4.3 QPKE with Quantum Ciphertexts from PRFSs

We finally present our third scheme for qPKE, whose security is based on the existence of PRFS with super-logarithmic input size.

Theorem 4. *The construction in Fig. 3 is IND-CPA secure (see Definition 4), assuming $\{|\psi_{k,x}\rangle\}_{k,x}$ is a PRFS with super-logarithmic input-size.*

The proof of this theorem uses the same proof strategy of Theorem 2 and Theorem 3, the only difference is that here the scheme is only IND-CPA secure, while the previous ones are IND-CPA-EO secure.

Acknowledgments

Assumes: A PRFS family $\{|\psi_{\mathsf{dk},x}\rangle\}_{\mathsf{dk},x}$ with super-logarithmic input-size.

$\mathsf{Gen}(1^\lambda)$
    1. $\mathsf{dk} \leftarrow_R \{0,1\}^\lambda$.

$\mathcal{QPKGen}(\mathsf{dk})$
    1. Output $|qpk\rangle = \frac{1}{\sqrt{2^\lambda}} \sum_{x \in \{0,1\}^\lambda} |x\rangle|\psi_{\mathsf{dk},x}\rangle$.

$\mathcal{Enc}(|qpk\rangle, m)$ for $m \in \{0,1\}$
    1. Measure left register, denoted by x. Let $|\phi\rangle = |\psi_{\mathsf{dk},x}\rangle$ if $m = 0$, and a maximally mixed state otherwise.
    2. Output $c = (x, |\phi\rangle)$.

$\mathsf{Dec}_{\mathsf{dk}}(c)$
    1. Interpret c as $(x, |\phi\rangle)$
    2. Output 0 if $|\phi\rangle = |\psi_{\mathsf{dk},x}\rangle$, otherwise output 1.

Figure 3: An encryption scheme with quantum public keys based on a PRFS.

References

[ACC⁺22] P. Austrin, H. Chung, K. Chung, S. Fu, Y. Lin, and M. Mahmoody. On the Impossibility of Key Agreements from Quantum Random Oracles. In Y. Dodis and T. Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II*, volume 13508 of *Lecture Notes in Computer Science*, pages 165–194. Springer, 2022, Cryptology ePrint Archive: `Report 2022/218`.

[AGQY23] P. Ananth, A. Gulati, L. Qian, and H. Yuen. Pseudorandom (Function-Like) Quantum State Generators: New Definitions and Applications. In *Theory of Cryptography: 20th International Conference, TCC 2022, Chicago, IL, USA, November 7–10, 2022, Proceedings, Part I*, pages 237–265. Springer, 2023.

[AQY21] P. Ananth, L. Qian, and H. Yuen. Cryptography from Pseudorandom Quantum States, 2021, arXiv: `2112.10020`.

[BB84] C. H. Bennett and G. Brassard. An Update on Quantum Cryptography. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, volume 196 of *Lecture Notes in Computer Science*, pages 475–480. Springer, 1984.

[BBSS23] A. Behera, Z. Brakerski, O. Sattath, and O. Shmueli. Quantum pseudorandomness with proof of destruction. Private communication, 2023.

[BCKM21] J. Bartusek, A. Coladangelo, D. Khurana, and F. Ma. One-Way Functions Imply Secure Computation in a Quantum World. In T. Malkin and C. Peikert, editors, *Advances in Cryptology - CRYPTO 2021*, volume 12825, pages 467–496. Springer, 2021, Cryptology ePrint Archive: `Report 2020/1487`.

[BMW23] K. Barooti, G. Malavolta, and M. Walter. A Simple Construction of Quantum Public-Key Encryption from Quantum-Secure One-Way Functions. Cryptology ePrint Archive, Paper 2023/306, 2023. `https://eprint.iacr.org/2023/306`.

[BZ13] D. Boneh and M. Zhandry. Quantum-Secure Message Authentication Codes. In T. Johansson and P. Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT*, volume 7881 of *Lecture Notes in Computer Science*, pages 592–608. Springer, 2013, Cryptology ePrint Archive: `Report 2012/606`.

[Col23] A. Coladangelo. Quantum trapdoor functions from classical one-way functions. Cryptology ePrint Archive, Paper 2023/282, 2023. `https://eprint.iacr.org/2023/282`.

[GLSV21] A. B. Grilo, H. Lin, F. Song, and V. Vaikuntanathan. Oblivious Transfer Is in MiniQCrypt. In *EUROCRYPT (2)*, volume 12697 of *Lecture Notes in Computer Science*, pages 531–561. Springer, 2021, arXiv: `2011.14980`.

[Got05]   D. Gottesman. Quantum Public Key Cryptography with Information-Theoretic Security. *https://www2.perimeterinstitute.ca/personal/dgottesman/Public-key.ppt*, 2005.

[IR89]   R. Impagliazzo and S. Rudich. Limits on the Provable Consequences of One-Way Permutations. In D. S. Johnson, editor, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washigton, USA*, pages 44–61. ACM, 1989.

[JLS18]   Z. Ji, Y. Liu, and F. Song. Pseudorandom Quantum States. In H. Shacham and A. Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*, volume 10993 of *Lecture Notes in Computer Science*, pages 126–152. Springer, 2018, arXiv: `1711.00385`.

[KL14]   J. Katz and Y. Lindell. *Introduction to Modern Cryptography, Second Edition*. CRC Press, 2014.

[KQST22]   W. Kretschmer, L. Qian, M. Sinha, and A. Tal. Quantum Cryptography in Algorithmica, 2022, arXiv: `2212.00879`.

[Kre21]   W. Kretschmer. Quantum Pseudorandomness and Classical Complexity. In M. Hsieh, editor, *16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference*, volume 197 of *LIPIcs*, pages 2:1–2:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

[MY22a]   T. Morimae and T. Yamakawa. Quantum Commitments and Signatures Without One-Way Functions. In Y. Dodis and T. Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I*, volume 13507 of *Lecture Notes in Computer Science*, pages 269–295. Springer, August 2022, arXiv: `2112.06369`.

[MY22b]   T. Morimae and Y. Yamakawa. One-Wayness in Quantum Cryptography, October 2022, arXiv: `2210.03394`.

[NI09]   G. M. Nikolopoulos and L. M. Ioannou. Deterministic quantum-public-key encryption: Forward search attack and randomization. *Phys. Rev. A*, 79:042327, Apr 2009.

[OTU00]   T. Okamoto, K. Tanaka, and S. Uchiyama. Quantum Public-Key Cryptosystems. In M. Bellare, editor, *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, volume 1880 of *Lecture Notes in Computer Science*, pages 147–165. Springer, 2000.

[Wie83]   S. Wiesner. Conjugate Coding. *SIGACT News*, 15(1):78–88, jan 1983.

[Zha12]   M. Zhandry. How to Construct Quantum Random Functions. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, pages 679–687. IEEE Computer Society, 2012.

[Zha19]   M. Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39*, pages 239–268. Springer, 2019.