Towards the Impossibility of Quantum Public Key Encryption with Classical Keys from One-Way Functions

Samuel Bouaziz–Ermann[1], Alex B. Grilo[1], Damien Vergnaud[1], and Quoc-Huy Vu[2]

[1] Sorbonne Université, CNRS, LIP6, France
[2] Léonard de Vinci Pôle Universitaire, Research Center, 92 916 Paris La Défense, France

Abstract. There has been a recent interest in proposing quantum protocols whose security relies on weaker computational assumptions than their classical counterparts. Importantly to our work, it has been recently shown that public-key encryption (PKE) from one-way functions (OWF) is possible if we consider quantum public keys. Notice that we do not expect classical PKE from OWF given the impossibility results of Impagliazzo and Rudich (STOC'89).

However, the distribution of quantum public keys is a challenging task. Therefore, the main question that motivates our work is if quantum PKE from OWF is possible if we have classical public keys. Such protocols are impossible if ciphertexts are also classical, given the impossibility result of Austrin *et al.*(CRYPTO'22) of quantum enhanced key-agreement (KA) with classical communication.

In this paper, we focus on black-box separation for PKE with classical public key and quantum ciphertext from OWF under the polynomial compatibility conjecture, first introduced in Austrin *et al.*. More precisely, we show the separation when the decryption algorithm of the PKE does not query the OWF. We prove our result by extending the techniques of Austrin *et al.* and we show an attack for KA in an extended classical communication model where the last message in the protocol can be a quantum state.

1 Introduction

After decades of focusing on the possibility of information-theoretically secure quantum protocols, initiated by the land-marking results on money schemes [Wie83] and key-agreement [BB84], there has been recent progress in understanding how quantum resources can be used to implement cryptographic primitives under weaker computational assumptions.

More concretely, it has been shown in [GLSV21, BCKM21] that Oblivious Transfer (OT) and Multi-party computation (MPC), two central primitives in cryptography can be constructed from one-way functions (OWF), the weakest classical cryptographic assumption. Such a result has been extended to show OT and MPC can be constructed from pseudo-random quantum states [AQY22], which is expected to be a weaker computational assumption than OWF [Kre21, KQST23]. This is in stark contrast with the classical case since we do not expect OT and MPC to be built from one-way functions [IR89].

More recently, it has been asked if quantum protocols are possible for public-key encryption from OWF (or weaker assumptions). While the conditional impossibility result for key-agreement of [ACC$^+$22] implies that public-key encryption (PKE) from OWF with classical communication is impossible even if the honest parties are quantum,[3] it has been recently shown that PKE can be constructed from OWF if we have a quantum public-key [Col23, BGHD$^+$23, KMNY23]. However, having a quantum public key is not ideal, given the issues that appear with public-key distribution, authentication, and reusability. These results leave then as an open question if quantum PKE from OWF is possible with a classical public key and quantum ciphertext.

In this work, we extend the result of [ACC$^+$22] and we show that key agreement is impossible when Alice and Bob exchange classical messages and at the very last round, Bob sends a quantum message to Alice. Our

[3] Such a result is actually conditioned on a conjecture that we state in Conjecture 2.16 and discuss in Section 1.2.

result holds under the same conjecture as [ACC$^+$22] but is limited to the setting where Alice does not query the random oracle in the last round of the protocol. More concretely, we achieve the following result.

Theorem 1.1 (Informal). *Let Π be a key agreement protocol between Alice and Bob, where they first exchange classical messages and at the last round Bob sends a quantum message, and Alice and Bob agree on a key k. Let n be the number of queries that Alice and Bob make to a random oracle $\mathcal{O}$. Then, assuming Alice does not query the oracle after receiving the quantum message from Bob, Eve can find k with $\mathcal{O}(\mathsf{poly}(n))$ classical queries to $\mathcal{O}$ with probability $\frac{1}{\mathsf{poly}(n)}$.*

With this result in hand, we show that quantum PKE is impossible with a classical public key in the Quantum Random Oracle Model (QROM), when the decryption algorithm does not query the random oracle.

Corollary 1.2 (Informal). *Assume $(\mathcal{Gen}, \mathcal{Enc}, \mathcal{Dec})$ is a Public-Key Encryption scheme, where the public key is classical and the ciphertext is a quantum state. Assuming the algorithms $\mathcal{Gen}$ and $\mathcal{Enc}$ makes at most n quantum queries to a random oracle $\mathcal{O}$, then there exists an algorithm* Eve *that can decipher by making $\mathcal{O}(\mathsf{poly}(n))$ classical queries to $\mathcal{O}$.*

Using known techniques from black-box separation, our results can easily be translated to give separations of qPKE from black-box OWF. We also note that our result (Corollary 1.2) marks an initial step towards proving the conjecture of [MY22] on the possibility of black-box constructions of qPKE with classical public keys from quantum symmetric key encryption.

1.1 Technical Overview

To prove Theorem 1.1, we start with a key-agreement protocol with perfect correctness where Alice and Bob have quantum access to a random oracle and exchange polynomially many rounds of classical messages, and then Bob sends a final quantum message $|\psi\rangle$ to Alice. [4]

We show an attack where with inverse polynomial probability:

1. Given the classical transcript and $|\psi\rangle$, Eve guesses the key k that Alice and Bob would share.
2. Eve sends a quantum state ψ^E to Alice such that Alice agrees on the key k at the end of the protocol.

While the first item is sufficient to break the key agreement protocol, the second item allows us to show a much stronger attack: Eve is an active adversary that not only retrieves the key but also does it in a way that Alice and Bob will not detect later since both of them share the same key.

To prove the first item, we use the same technique as [ACC$^+$22, Construction 4.10], which queries all of the "ε-heavy queries" to the random oracle. This approach is similar to the classical approach of [BM09], whose construction queries all of the values that are queried by Alice and Bob with probability *at least* ε. These are called the "ε-heavy queries", and with the right parameter of ε, one can show that it allows Eve to find all of the *intersection queries* with high probability, that is the values queried by both Alice and Bob. A problem that appears in the quantum setting is that the notion of *intersection queries* is unclear, as Alice and Bob are allowed to query the oracle in superposition, it is thus hard to precisely define what information Alice and Bob know about the oracle. This means that a definition for quantum intersection queries must be such that the knowledge of the intersection queries is sufficient to find the key with high probability, which is a strong property.

In the quantum attack of [ACC$^+$22], they start by defining the *quantum* heavy queries. Roughly, these are the queries with high amplitude (see Definition 2.10 for a formal definition), which is the natural quantum equivalent of the classical definition that appears in [BM09]. To replace the notion of intersection queries,

[4] In this overview, we consider for simplicity that the last message sent by Bob is a pure state, denoted as $|\psi\rangle$. In our formal proof, we consider the general case in which the message is a mixed state.

which is problematic in the quantum setting, they propose the Polynomial Compatibility Conjecture (PCC). This conjecture implies that if a pair of quantum states satisfy some conditions, then there exists a random oracle that is consistent with the transcript and with both quantum states. In their attack, Eve learns all of the heavy queries and generates a simulation of the states of Alice and Bob. They show that if Eve is not able to retrieve the key with high probability from these simulated states, then the protocol does not have perfect correctness, leading to a contradiction. This is shown by proving that if Eve does not find the correct key, by the PCC, there exists an oracle h that is consistent with both states, and therefore there exists an execution of the protocol where Alice outputs keys 1 and Bob outputs key 0.

We extend this result to the case where the last message is quantum. Similar to [ACC$^+$22, Construction 4.10], we define the quantum-heavy query learner algorithm, which is formally defined in Construction 2.11 and whose goal is to query all of the ε-heavy queries. In this overview, we consider for simplicity that the last message sent by Bob is a pure state, denoted as $|\psi\rangle$. Eve then run Alice's last step of the protocol (which is publicly defined by the protocol) on the simulated internal state of Alice that Eve generated and the quantum message from Bob. We then need to show that Eve will still be able to guess the good key with high probability. This translates to showing that, for some noticeable parameter ν:

$$\mathrm{Tr}\left(\Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}\left(|\phi_A^E\rangle\langle\phi_A^E|_{W'_A}\otimes|h\rangle\langle h|_H\otimes|\psi\rangle\langle\psi|_M\right)(\mathsf{A}_{\mathsf{fin}})^\dagger\right)\geq 1-\nu, \tag{1}$$

where the register W'_A contains Eve's simulated state of Alice $|\phi_A^E\rangle$, register H contain the superposition of all possible oracles that are consistent with Eve's knowledge of the real oracle, and register M contains the message $|\psi\rangle$ that Bob sent to Alice. The unitary $\mathsf{A}_{\mathsf{fin}}$ corresponds to Alice's operation in the last step of the protocol, after she receives Bob's message, and the projector Π_{k} measures the key. Equation (1) translates to saying that given the *real* message that Bob sends to Alice, Eve can find Bob's key by applying the operations that Alice would have applied on the simulated state of Alice $|\phi_A^E\rangle$ that she obtained by using the quantum-heavy queries learner. This equation is proven in Section 3.2.2.

The proof of Equation (1) comes from the fact that since Alice does not query the oracle when she applies the operator $\mathsf{A}_{\mathsf{fin}}$ after receiving the quantum message ψ from Bob, then the register H is unchanged and thus the resulting state keeps the properties necessary to apply the PCC.

For the second item, we need to define the state ψ^E that Eve sends to Alice. The idea is the following: Eve will pick the post-measurement state of the measurement described in Equation (1), and she applies $\mathsf{A}_{\mathsf{fin}}^\dagger$ to it. Then, Eve traces out the registers W'_A and H and ψ^E is the remaining state in register M.

To show that Alice computes the same key as Bob and Eve with high probability, we show that ψ^E is close to $|\psi\rangle$:

$$\langle\psi|\,\psi^E\,|\psi\rangle\geq 1-\nu. \tag{2}$$

Using Equation (2) and the perfect correctness of the protocol, we then show that Alice and Bob will agree on the same key with high probability. This corresponds to proving the following inequality:

$$\mathrm{Tr}\left(\Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}(|\phi_{\mathsf{A}}\rangle\langle\phi_{\mathsf{A}}|_{W_A}\otimes|h\rangle\langle h|_H\otimes\psi^E)\,(\mathsf{A}_{\mathsf{fin}})^\dagger\right)\geq 1-\nu, \tag{3}$$

where $|\phi_{\mathsf{A}}\rangle$ is Alice's real internal state and ψ^E is the message that Eve sends to Alice. Equation (3) translates to saying that given the message of Eve, Alice will find the same key as Eve with high probability when she does her final computation. These equations are proven in Section 3.2.3.

Finally, Corollary 1.2 follows from the fact that if public key encryption with quantum ciphertexts is possible, then we can construct a key agreement protocol: Alice sends the public key and Bob answers with the encryption of a random key k.

1.2 Related Works, Discussion and Open Problems

The Polynomial Compatibility Conjecture. First introduced in [ACC$^+$22], the Polynomial Compatibility Conjecture (PCC) is already known to imply separation results for key agreement [ACC$^+$22] and non-interactive commitments [CLM23]. The conjecture has an alternative expression that uses polynomials and is equivalent to the statement in Conjecture 2.16. The PCC is known to be true with exponential parameters [ACC+22], but it is still open with polynomial parameters. Proving it would be interesting as it would now also establish the separation result for quantum PKE, along with potentially more results as it is a strong statement.

Quantum Public Key Encryption. Classically, public key encryption (PKE) cannot be constructed from black-box one-way functions [IR89]. In the quantum context, various definitions of quantum PKE exist, leading to different feasibility outcomes. With quantum public keys and classical ciphertexts, quantum PKE can be constructed from one-way functions [Col23, BGHD+23, KMNY23]. However, it remains unclear how the distribution of such public keys could be effectively distributed in practice among different parties. Our result focuses on quantum PKE with classical public keys and quantum ciphertexts. In this setting, the distribution of public keys could be implemented using currently available public key infrastructure (PKI). Moreover, compared to having a quantum public key and a classical ciphertext, having a classical public key and a quantum ciphertext is less problematic for implementations, as the message is supposed to be received by only one party and thus the potential destruction of the message after the decryption is inconsequential. With this definition of quantum PKE, we achieve a step towards proving a similar result as the classical case.

Classical Communication One Quantum Message Key Agreement Protocols. In our paper, we introduce a scheme that we call Classical Communication One Quantum Message Key Agreement (CC1QM-KA) protocols. In these types of protocol, Alice and Bob communicate classically, except for the last message that is quantum. We show that key agreement is impossible with this type of protocol in the QROM if Alice does not query the random oracle after receiving the last message. One natural question is what happens if we allow the *first* message to be quantum, while the rest of the communication is classical. Interestingly enough, [BB84] falls into this category of protocol, thus key agreement is possible *unconditionally* in this setting. This asymmetry in terms of feasibility results is quite surprising and a possible explanation is the fact that we cannot postselect on quantum messages, i.e. generate a state that is consistent with an algorithm and one of its output register being a specific quantum state. Indeed, the classical Eve attacks imply a simulation of the internal state of the parties that is consistent with the message, which corresponds to computing an internal state postselected on the classical messages that are communicated. With a quantum message, this would be possible with a classical description of the quantum message since Eve is unbounded, but it is non-trivial with only the quantum state as Eve must learn what the quantum message is in the first place somehow. However, in the CC1QM setting, we do not need to do this postselection, as a simulation of the last part of the protocol is enough to find the right key.

Allowing oracle queries in the decryption algorithm To prove the stronger result that qPKE is impossible even when the decryption algorithms query the oracle, one needs to show an attack on CC1QM-KA protocols where Alice queries the oracle in the last part of the protocol. At first glance, one may think that Equation (1) should be true even if Alice makes queries to the oracle in $\mathsf{A}_{\mathsf{fin}}$, because every new information about the oracle that she learns at this stage of the protocol will not be transmitted to Bob since there is no communication afterward. However, some issues that do not appear in [ACC+22] arise when trying to prove such an inequality.

The first (natural) problem is that since the last message is quantum, Eve cannot compute the heavy queries (which would be sufficient for the attack). Therefore, we need to find another way of simulating Alice's last oracle calls without learning the heavy queries.

A first attempt is to use the operator $\mathsf{A}_{\mathsf{fin}}^{\mathcal{O}}$, that corresponds to Alice's computation in the last step of the protocol with the *real* oracle $\mathcal{O}$. Because this corresponds to the operation that the real Alice would have done and the real outcome is deterministic (since the protocol has perfect correctness), it could allow Eve to find the real key. However, the problem in this approach is that Eve has her simulated state that was constructed using a *simulated* oracle (with correct values for heavy-queries) and Alice's algorithm could use some consistency check that would fail when we decide to change the oracle.

On the other hand, if we want to use the simulated oracle instead of the real oracle, then there is a trivial protocol for which the attack does not work. In this protocol, Bob just picks a random value $x \in \mathcal{X}$, queries it, and sends $|x\rangle$ to Alice. Alice and Bob agree then on the key $H(x)$. By using the simulation oracle, Eve would not be able to find the key with non-negligible probability.

While these two complications are artificial since they do not lead to a secure protocol, they put a barrier to finding a common attack that would make Eve find the keys from Alice and Bob.

2 Preliminaries

2.1 Notation

The following notations will be used throughout the paper,

- By λ we denote the security parameter.
- We use calligraphic letters (e.g., $\mathcal{X}$) to denote sets. We use $\mathcal{Y}^{\mathcal{X}}$ to denote the set of all functions from $\mathcal{X}$ to $\mathcal{Y}$.
- We use bold letters (e.g., $\mathbf{m}$) to denote random variables and distributions. We write $m \leftarrow\!\!\$\ \mathbf{m}$ to denote that m is sampled from the distribution $\mathbf{m}$. We write $m \leftarrow\!\!\$\ \mathcal{M}$ to denote that m is sampled uniformly from the set $\mathcal{M}$.
- We use the Dirac notation for pure states, e.g., $|\psi\rangle$, while mixed states will be denoted by lowercase Greek letters, e.g., ρ.

For the basics of quantum computation, we refer readers to [NC10].

2.2 Quantum Computation

Definition 2.1 (Oracle-aided quantum algorithms). *A quantum algorithm $\mathcal{A}$ is a family of quantum circuits $\mathcal{A} := \{A_\lambda\}_{\lambda\in\mathbb{N}}$ that act on three sets of registers: input registers X, output registers Y, and work registers Z. For convenience, we let $W := (X, Y, Z)$ denote the* internal registers *of $\mathcal{A}$. For each input $x \in \{0,1\}^\lambda$, the output is computed by running the algorithm A_λ on $|x\rangle_X |0\rangle_Y |0\rangle_W$ and at the end the output registers are measured in the computational basis to obtain the output.*

A d-query quantum oracle algorithm $\mathcal{A}^h$ that has access to an oracle h, defined by the unitary $\mathcal{O}_h$ can be specified by a sequence of unitary matrices $(U_d, U_{d-1}, \ldots, U_0)$. The final state of the algorithm is defined as $U_d\mathcal{O}_hU_{d-1}\mathcal{O}_h \ldots \mathcal{O}_hU_0 |x\rangle_X |0\rangle_Y |0\rangle_Z$. When the oracle h implements some classical function $h : \mathcal{X} \to \mathcal{Y}$, the corresponding query operator $\mathcal{O}_h$ is defined as $|x\rangle_X |y\rangle_Y \mapsto |x\rangle_X |y \oplus h(x)\rangle_Y$.

When $\mathcal{A}^h$ is clear from the context, we omit the superscript h and write $\mathcal{A}$.

The following preliminary is borrowed from the formalization of [ACC$^+$22].

Definition 2.2 (The computational and the Fourier basis). *Let $\mathcal{Y}$ be a finite Abelian group with cardinality $|\mathcal{Y}|$. Let $\{|y\rangle\}_{y\in\mathcal{Y}}$ be an orthonormal basis of $\mathbb{C}^{|\mathcal{Y}|}$. We refer to this basis as the computational basis. Let $\hat{\mathcal{Y}}$ be the dual group which is known to be isomorphic to $\mathcal{Y}$. Recall that a member $\hat{y} \in \hat{\mathcal{Y}}$ is a character function (i.e., a function from $\mathcal{Y}$ to the multiplicative group of non-zero complex numbers). The Fourier basis $\{|\hat{y}\rangle\}_{\hat{y}\in\hat{\mathcal{Y}}}$ of $\mathbb{C}^{|\mathcal{Y}|}$ is defined as*

$$|\hat{y}\rangle = \frac{1}{\sqrt{|\mathcal{Y}|}} \sum_{y\in\mathcal{Y}} \hat{y}(y)^\dagger |y\rangle \;\; \text{and} \;\; |y\rangle = \frac{1}{\sqrt{|\mathcal{Y}|}} \sum_{\hat{y}\in\hat{\mathcal{Y}}} \hat{y}(y) |\hat{y}\rangle .$$

Definition 2.3 (Functions and their (quantum) representations). *For any function $h \in \mathcal{Y}^{\mathcal{X}}$, we define its quantum representation to be $|h\rangle_H := \bigotimes_{x \in \mathcal{X}} |h(x)\rangle_{H_x}$ in the computational basis, where the register H_x is associated with $\mathbb{C}^{\mathcal{Y}}$ for all $x \in \mathcal{X}$, and the register H is compounded of all H_x. Similarly, for any $\hat{h} \in \hat{\mathcal{Y}}^{\mathcal{X}}$ we define $|\hat{h}\rangle_H := \bigotimes_{x \in \mathcal{X}} |\hat{h}(x)\rangle_{H_x}$ in the Fourier basis.*

Zhandry [Zha19] shows that the purified random oracle is perfectly indistinguishable from the (standard) quantum random oracle, and thus instead of considering the query operator $\mathcal{O}_h$, we can consider another equivalent query oracle $\mathcal{O}$ acting on three registers X, Y, H as follows.

$$|x\rangle_X |y\rangle_Y |h\rangle_H \mapsto |x\rangle_X |y \oplus h(x)\rangle_Y |h\rangle_H ,$$

where the oracle register H is initialized as $|\Phi_0\rangle_H = \sum_{h \in \mathcal{H}} \frac{1}{\sqrt{|\mathcal{H}|}} |h\rangle_H$.

Note that in the Fourier basis, the unitary $\mathcal{O}$ acts as follows:

$$|x\rangle_X |\hat{y}\rangle_Y |\hat{h}\rangle_H \mapsto |x\rangle_X |\hat{y}\rangle_Y \bigotimes_{x' \in \mathcal{X}} |\hat{h}(x') - \delta_{x,x'} \cdot \hat{y}\rangle_H ,$$

where $\delta_{x,x'}$ is equal to 1 if $x = x'$, and 0 otherwise, and the oracle register H is initialized as $|\Phi_0\rangle_H = \bigotimes_{x \in \mathcal{X}} |\hat{0}\rangle_{H_x}$.

Definition 2.4 (Purified view of two-party protocols in the QROM). *A two-party protocol in the Quantum-Computation Classical-Computation (QCCC) model is a protocol in which two quantum algorithms, Alice and Bob, can query the oracle, apply quantum operation on their internal registers, and send classical strings over the public (authenticated) channel to the other party. The sequence of the strings sent during the protocol is called the* transcript *of the protocol. Let W_A and W_B be Alice's and Bob's internal registers, respectively. Let $\mathcal{H} := \mathcal{Y}^{\mathcal{X}}$. For any two-party protocol, we define its purified version as follows.*

- *If the protocol is inputless, start with $|0\rangle_{W_A} |0\rangle_{W_B} \sum_{h \in \mathcal{H}} \frac{1}{\sqrt{|\mathcal{H}|}} |h\rangle_H$. Otherwise, if Alice takes as input a classical string $a \in \mathcal{X}$ and Bob takes as input a classical string $b \in \mathcal{X}$, start with $|a\rangle_{W_A} |b\rangle_{W_B} \sum_{h \in \mathcal{H}} \frac{1}{\sqrt{|\mathcal{H}|}} |h\rangle_H$.*
- *Alice and Bob run the protocol in superposition, that is, all the measurements (including those used for generating the transcript) are delayed and the query operator $\mathcal{O}_h$ is replaced by $\mathcal{O}$.*
- *Let $|\Psi\rangle_{W_A W_B H}$ denote the state at the end of the protocol, and let $|\Psi_t\rangle_{W_A W_B H}$ denote the post-measurement state of $|\Psi\rangle_{W_A W_B H}$ which is consistent with the transcript t.*

We now define some properties related to this new register for the database $|h\rangle_H$.

Definition 2.5 (Non-zero queries in Fourier basis). *Let $\mathcal{Y}$ be a finite Abelian group and $\hat{\mathcal{Y}}$ be the dual group. For any $\hat{y} \in \hat{\mathcal{Y}}^{\mathcal{X}}$, we define the size of $\hat{h}$ to be*

$$\left|\hat{h}\right| := \left|\{x : x \in \mathcal{X}, \hat{h}(x) \neq \hat{0}\}\right| .$$

Definition 2.6 (Oracle support). *Let $\hat{\mathcal{H}} := \hat{\mathcal{Y}}^{\mathcal{X}}$. For any vector $|\phi\rangle_{WH} = \sum_{w, \hat{h} \in \hat{\mathcal{H}}} \alpha_{w,\hat{h}} |w\rangle_W |\hat{h}\rangle_H$, we define the* oracle support in the Fourier basis *of $|\phi\rangle$ as*

$$\widehat{\operatorname{supp}}^H(|\phi\rangle) := \left\{\hat{h} : \exists w \ s.t. \ \alpha_{w,\hat{h}} \neq 0\right\} .$$

We denote $\hat{h}^H_{max}(|\phi\rangle)$ the function $\hat{h} \in \widehat{\operatorname{supp}}^H(|\phi\rangle)$ that has the largest size $\left|\hat{h}\right|$ (if such function is not unique, by default we pick the lexicographically first one). The definition extends naturally when the register W does not exist.

Similarly, if we write the oracle part in the computational basis $|\phi\rangle_{WH} = \sum_{w,h\in\mathcal{H}} \beta_{w,h} |w\rangle_W |h\rangle_H$, then we define the oracle support in the computational basis of $|\phi\rangle$ as

$$\text{supp}^H(|\phi\rangle) := \{h : \exists w \text{ s.t. } \beta_{w,h} \neq 0\}.$$

Definition 2.7. *A partial oracle L is a partial function from $\mathcal{X}$ to $\mathcal{Y}$. The domain of L is denoted by $Q_L := dom(L)$. Equivalently, we view L as a finite set of pairs $(x, y_x) \in \mathcal{X} \times \mathcal{Y}$ such that for all $(x, y_x), (x', y'_x) \in L, x \neq x'$. We say a partial oracle L is consistent with $h : \mathcal{X} \to \mathcal{Y}$ if and only if $h(x) = y_x$ holds for all $x \in Q_L$.*

For any partial oracle L, we define the associated projector Π_L by

$$\Pi_L := \bigotimes_{x\in Q_L} |y_x\rangle\langle y_x|_{H_x} \bigotimes_{x\notin Q_L} \mathcal{I}_{H_x},$$

where $\mathcal{I}_{H_x}$ is the identity operator acting on H_x. It holds that $\Pi_L |h\rangle_H = |h\rangle_H$ if h is consistent with L, and $\Pi_L |h\rangle_H = 0$ otherwise.

Lemma 2.8. *If A asks at most d queries to the superposition oracle, then for all possible outcomes of A's intermediate measurements, the joint state $|\psi\rangle_{WH}$ conditioned on the outcome satisfies $\left|\hat{h}^H_{max}(|\psi\rangle)\right| \leq d$.*

Lemma 2.9. *Given a state $|\psi\rangle_{WH}$ and a partial oracle L, the state $\Pi_L |\psi\rangle_{WH}$ can be written as*

$$\Pi_L |\psi\rangle_{WH} := \sum_{w\in\mathcal{W},\hat{h}\in\hat{\mathcal{H}}'} \alpha'_{w,\hat{h}} |w\rangle_W \bigotimes_{x\notin Q_L} |\hat{h}(x)\rangle_{H_x} \bigotimes_{x\in Q_L} |y_x\rangle_{H_x},$$

where $\hat{\mathcal{H}}'$ is the set of functions from $\mathcal{X}\backslash Q_L$ to $\hat{\mathcal{Y}}$. Furthermore, if $\left|\hat{h}^H_{max}(|\psi\rangle)\right| \leq d$, then $\left|\hat{h}^{H'}_{max}(\Pi_L|\psi\rangle)\right| \leq d$, where H' is the set of registers corresponding to $\mathcal{X} \setminus Q_L$.

2.3 Quantum-Heavy Queries Learner

We now define the *quantum-heavy queries learner* algorithm. It was first defined in [ACC+22, Construction 4.10], which can be seen as the quantum counterpart of the classical *independence learner* of [BM09], where Eve learns all the *ε-heavy queries* of both Alice and Bob.

Definition 2.10 (Quantum ε-heavy queries [ACC+22, Definition 4.9]). *For $x \in \mathcal{X}$, define the projector*

$$\Pi_x := \sum_{\hat{y}\in\hat{\mathcal{Y}}\backslash\{\hat{0}\}} |\hat{y}\rangle\langle\hat{y}|_{H_x}.$$

Given a quantum state $|\psi\rangle_{W_A W_B H}$, the weight of any $x \in \mathcal{X}$ is defined as

$$w(x) := \|\Pi_x |\psi\rangle\|^2,$$

that is, the quantum heaviness of x is the probability of obtaining a non-$\hat{0}$ outcome while measuring H_x in the Fourier basis. We call $x \in \mathcal{X}$ a quantum ε-heavy *query if $w(x) \geq \varepsilon$.*

Construction 2.11 (Quantum-heavy queries learner [ACC+22]). *Let (A, B) be an inputless two-party QCCC protocol relative to a random oracle h, in which Alice and Bob make at most d quantum queries to the oracle. Given the transcript t, (computationally-unbounded) attacking algorithm* Eve *is parameterized by ε and works as follows.*

1. *Let L denote the set of oracle query-answer pairs obtained by* Eve *from the oracle, and $\mathcal{Q}_L$ is defined similarly while only containing the queries. Initially prepare $L = \emptyset$ and the classical description of the state*
$$|\psi\rangle_{W'_{\mathsf{A}}W'_{\mathsf{B}}H'} = |0\rangle_{W'_{\mathsf{A}}} |0\rangle_{W'_{\mathsf{B}}} |\Phi_0\rangle_{H'} ,$$
where $|\Phi_0\rangle$ is a uniform superposition over all $h \in \mathcal{H}$, W'_{A} , W'_{B} and H' are the simulated registers for Alice, Bob, and the oracle prepared by Eve.
2. *Simulate the state evolution during the protocol. Concretely,* Eve *calculates the state in $W'_{\mathsf{A}}W'_{\mathsf{B}}H'$ after each round in the protocol. Whenever* Eve *encounters the moments in which Alice (Bob) sends their message,* Eve *calculates the post-measurement state that is consistent with t.*
3. *While there is any query $x \notin \mathcal{Q}_L$ that is quantum ε-heavy conditioned on (t, L), do the following:*
   (a) Ask the lexicographically first quantum ε-heavy query x from the real oracle h.
   (b) Update the state in $W'_{\mathsf{A}}W'_{\mathsf{B}}H'$ to the post-measurement state that is consistent with $(x, h(x))$.
   (c) Update L by adding $(x, h(x))$ to L.
4. *When there is no quantum ε-heavy query left to ask,* Eve *outputs the simulated quantum state $|\psi_t\rangle_{W'_{\mathsf{A}}W'_{\mathsf{B}}H'}$ and her list L, conditioned on the transcript t.*

Remark 2.12. We note that Construction 2.11 described above is almost identical to [ACC+22, Construction 4.10]. The only difference is that Eve outputs the simulated state, which can be constructed from the classical description that Eve has computed, along with the list of queries she made to the oracle.

The technical properties of the quantum-heavy queries learner in Construction 2.11 are stated in the following lemma.

Lemma 2.13 ([ACC+22]). *For any $0 < \varepsilon < 1$, the quantum-heavy queries learner described in Construction 2.11 satisfies the following properties:*

- ***Efficiency:*** *$\mathbb{E}[|L|] \leq \frac{d}{\varepsilon}$, where the expectation is over the randomness of the oracle and the algorithm* Eve.
- ***Security:*** *When the learner stops and learns a list L, there is no $x \in \mathcal{Q}_L$ that is ε-quantum heavy in the purified view of* Eve *conditioned on knowing L and the transcript t.*

2.4 Polynomial Compatibility Conjecture

In this section, we recall the Polynomial Compatibility Conjecture (PCC) of [ACC+22]. The formulation we use here is based on quantum states.

Definition 2.14 ($(\mathcal{Y}, \delta, d, N)$-state [ACC+22, Definition 4.1]). *Let H be a register over the Hilbert space $\mathcal{Y}^N$. A quantum state $|\psi\rangle$ over registers W and H is a $(\mathcal{Y}, \delta, d, N)$*-state *if it satisfies the following two conditions:*

- *d-**sparsity**: $\left|\hat{h}^H_{max}(|\psi\rangle)\right| \leq d$. This means that for any measurement of registers H in the Fourier basis, and W in any basis, the oracle support in the Fourier basis is at most d.*
- *δ-**lightness**: For every $x \in \mathcal{X}$, if we measure the H_x register of $|\psi\rangle$ in the Fourier basis, the probability of getting $\hat{0}$ is at least $1 - \delta$. This mean that $|\psi\rangle$ has no δ-heavy queries.*

Definition 2.15 (Compatible states [ACC+22, Definition 4.2]). *Two quantum states $|\phi\rangle$ and $|\psi\rangle$ over registers W and H are* compatible *if their oracle supports in the computational basis (as defined in Definition 2.6) have non-empty intersection, i.e., if $\mathrm{supp}^H(|\phi\rangle) \cap \mathrm{supp}^H(|\psi\rangle) \neq \emptyset$.*

We now state the conjecture.

Conjecture 2.16 (Polynomial compatibility conjecture [ACC+22, Conjecture 4.3]). *There exists a finite Abelian group $\mathcal{Y}$ and $\delta = 1/\mathsf{poly}(d)$ such that for any $d, N \in \mathbb{N}$, it holds that any two $(\mathcal{Y}, \delta(d), d, N)$-states $|\phi\rangle$ and $|\psi\rangle$ are compatible.*

2.5 Useful Lemmas

We will use the following lemma frequently in our proofs in subsequent sections.

Lemma 2.17 (Independence [ACC$^+$22, Lemma 3.2]). *Suppose two quantum algorithms* A *and* B *interact classically in the quantum random oracle model. Let* W_{A} *and* W_{B} *denote their internal registers respectively. Then, at any time during the protocol, conditioned on the (classical) transcript* t *and the fixed oracle* $h \in \mathcal{H}$*, the joint state of the registers* W_{A} *and* W_{B} *conditioned on* t *and* h *is a product state.*

3 Attack on the Key Agreement Protocols

In this section, we consider key agreement protocols in an extended setting where both parties are quantum algorithms but they can only send classical strings over the public authenticated channel to the other party, except that the last message in the protocol can be a quantum state (in this case, the last message is not authenticated). We call this the Classical Communication One Quantum Message (CC1QM) model. In this extended setting, we show a conditional result based on the polynomial compatibility conjecture, that any protocol in the CC1QM model with perfect completeness where Alice does not query the oracle after receiving the last message can be broken with an expected polynomial number of queries. We present the formal definition of key agreement protocols in the CC1QM model in Section 3.1. In Section 3.2, we state the main result and its proof.

3.1 Definitions

We start by defining the model of Classical Communication One Quantum Message, where two quantum parties (Alice and Bob) communicate using the public authenticated classical channel, except for the last message that can be quantum. We assume the first message is from Alice to Bob, while the last message is from Bob to Alice, and the last quantum message is non-authenticated. This can be assumed without loss of generality since if the first message is from Bob to Alice, we can always transform it into the other case, by letting Alice sends a dummy message to Bob for the first message. Furthermore, we consider the case where the key that Alice and Bob agree on is one bit and the protocol succeeds with probability 1 (i.e., perfect correctness). Also, as for Quantum Key Distribution (QKD), we allow the parties to abort the protocol at any time, if they detect suspicious activity in the quantum communication. Formally, this is done by making Alice output the character $\perp$ instead of a key when the protocol is aborted. More formally, we define:

Definition 3.1 (Key agreement protocols in the CC1QM model). *We say that* (A, B) *is a key agreement protocol between two parties Alice and Bob in the CC1QM model (CC1QM-KA) if the following holds:*

1. *At the beginning of the protocol, Alice and Bob share no common information. Their corresponding algorithms,* A *and* B*, are stateful oracle-aided quantum algorithms which make at most* d *oracle queries.*
2. ***CC1QM.*** *All of the messages are classical messages, except for the last message (from Bob to Alice) that can be a (mixed) quantum state, denoted as* ψ*. The transcript of the protocol is denoted as* $T := (m_1, \cdots, m_\ell, \psi)$*.*
3. ***Perfect completeness.*** *At the end of the protocol, Alice and Bob agree on a key* $\mathsf{k} \in \{0, 1\}$ *with probability* 1 *when the protocol succeeds (i.e. when neither Alice or Bob outputs* $k = \perp$*).*
4. ***Security.*** *Let* $\mathsf{A}'_{\mathsf{fin}}$ *be Alice's last computation in the protocol after she receives the final message from Bob. By deferred measurement principle, we can modify* $\mathsf{A}'_{\mathsf{fin}}$ *so that it applies a unitary transformation* $\mathsf{A}_{\mathsf{fin}}$ *followed by a measurement in the computational basis* $\{\Pi_{\mathsf{k}}\}_{\mathsf{k} \in \{0,1\}}$ *and outputting*

a key k, *and we write* $\mathsf{A}'_{\mathsf{fin}} := \Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}$. *Similarly, let* $\mathsf{B}'_{\mathsf{fin}} := \Pi_{\mathsf{k}}\mathsf{B}_{\mathsf{fin}}$ *be Bob's last computation in the protocol after he sends the final message to Alice. We note that* $\mathsf{A}_{\mathsf{fin}}$ *and* $\mathsf{B}_{\mathsf{fin}}$ *can make quantum queries to the oracle, and the output of* $\mathsf{A}_{\mathsf{fin}}$ *(resp.* $\mathsf{B}'_{\mathsf{fin}}$*) is the output key of Alice (resp. Bob) at the end of the protocol execution. Let* $(T, \phi_{\mathsf{A}}, \phi_{\mathsf{B}}) \leftarrow \langle \mathsf{A} \models \mathsf{B} \rangle$ *be the output of an execution of the protocol right before Alice receives the last quantum message from Bob, where* $T := (m_1, \cdots, m_\ell, \psi)$ *is the transcript of the execution,* ϕ_{A} *and* ϕ_{B} *are the internal state of* A *and* B*, respectively.* (A, B) *is secure if for any polynomially-bounded query adversary* $\mathcal{E}$*:*

$$\Pr\left[\begin{array}{c} \mathsf{k} = \mathsf{k}_{\mathsf{A}} = \mathsf{k}_{\mathsf{B}} \\ \mathsf{k}_{\mathsf{A}} \neq \bot \\ \mathsf{k}_{\mathsf{B}} \neq \bot \end{array} \middle| \begin{array}{r} (T, \phi_{\mathsf{A}}, \phi_{\mathsf{B}}) \leftarrow \langle \mathsf{A} \models \mathsf{B} \rangle \\ (\mathsf{k}, \psi') \leftarrow \mathcal{E}(1^\lambda, T) \\ \mathsf{k}_{\mathsf{A}} \leftarrow \mathsf{A}'_{\mathsf{fin}}(\phi_{\mathsf{A}}, \psi') \\ \mathsf{k}_{\mathsf{B}} \leftarrow \mathsf{B}'_{\mathsf{fin}}(\phi_{\mathsf{B}}) \end{array}\right] \leq \mathsf{negl}(\lambda).$$

We say that a CC1QM-KA protocol (A, B) *is* (ε, s)*-broken if there exists an attacker Eve that finds the key of* (A, B) *with probability at least* ε*,* (A, B) *succeeds with probability at least* $\mathsf{poly}(\varepsilon)$*, and Eve makes an expected number of queries at most* s*.*

3.2 The Attack on Key Agreements Protocols

The goal of the section is to prove the following theorem that states that are no CC1QM-KA protocol in the QROM.

Theorem 3.2. *Let* (A, B) *be a CC1QM-KA protocol, where Alice and Bob make at most* d *queries to a random oracle* $h : \mathcal{X} \to \mathcal{Y}$*, and Alice does not query the oracle in the last part of the protocol (after receiving the quantum message from Bob). Assuming Conjecture 2.16 is true, then there exists an attacker Eve that makes at most* $\mathsf{poly}(d, |\mathcal{Y}|)$ *many* classical *queries to* h *and breaks the security (according to Definition 3.1) with probability at least* 0.8*.*

The proof consists of two parts, the first one shows that Eve manages to find the same key as the one computed as Bob, and this is proven in Section 3.2.2. The second part consists of showing that Alice agrees on the same key as Eve and Bob and this corresponds to Section 3.2.3. First, in the next section, we prove that the attack does not depend on the group of the domain of the function.

3.2.1 Group Equivalence of the Attack

We first show that if there is an attack for an Abelian group $\mathcal{Y}$, then there is an attack for any other Abelian group $\mathcal{Y}'$, up to some error terms. This allows us to relax the conjecture to be true for *any* Abelian group, as in [ACC$^+$22]. The proof follows closely [ACC$^+$22]'s proof as they are almost identical, and we include it here for completeness.

Lemma 3.3. *Suppose there exists a finite Abelian group* $\mathcal{Y}$*, a constant* $\tau > 0$ *and a function* $s(\cdot)$ *such that for all* $d \in \mathbb{N}$ *and any CC1QM-KA protocol* $\left(\mathsf{A}_1^h, \mathsf{B}_1^h\right)$ *where Alice and Bob asks* d *queries to a random oracle* h *whose range is* $\mathcal{Y}$*, and Alice does not query the oracle after receiving the last message, it holds that* $\left(\mathsf{A}_1^h, \mathsf{B}_1^h\right)$ *is* $(\tau, s(d))$*-broken. Then, for any finite Abelian group* $\mathcal{Y}'$*, any* $d' \in \mathbb{N}$*,* $\delta > 0$ *and any CC1QM-KA protocol* $\left(\mathsf{A}_2^{h'}, \mathsf{B}_2^{h'}\right)$ *where Alice and Bob asks* d' *queries to another random oracle* h' *whose range is* $\mathcal{Y}'$*,* $\left(\mathsf{A}_2^{h'}, \mathsf{B}_2^{h'}\right)$*, and Alice does not query the oracle after receiving the last message, can be* $(\tau - \delta, 4s(md'))$*-broken, where*

$$m = \left\lceil \log_{|\mathcal{Y}|}(d'^3 \left|\mathcal{Y}'\right| / 4\delta^2) \right\rceil.$$

Proof. The proof follows from the proof of Lemma 4.8 from [ACC+22]. The only difference is that we must also show that with probability at least $\tau - \delta$, Alice and Bob agree on the same key as Eve. However, their proof relies on the fact that we can simulate a random oracle with another random oracle, even when their ranges are different, up to some errors. Thus, their proof follows through in our setting as well, and with the same parameters. □

Lemma 3.4 (Attacking CC1QM-KA protocols). *Assume Conjecture 2.16 is true for some Abelian group $\mathcal{Y}$ and parameters d and $\delta = \nu/\varepsilon$. Let (A, B) be a CC1QM-KA protocol where Alice and Bob make at most d queries to a random oracle $h : \mathcal{X} \to \mathcal{Y}$, and Alice does not query the oracle after receiving the last message. Then, there exists an active attacker Eve who finds the secret key k with probability $1 - \nu$ according to Definition 3.1. Moreover, Eve is expected to make at most d/ε queries to h.*

The proof of Lemma 3.4 is given in subsequent Sections 3.2.2 and 3.2.3.

We can now prove Theorem 3.2:

Proof of Theorem 3.2. The proof follows immediately from Lemma 3.4, Lemma 3.3 and the proof of [ACC+22, Theorem 4.5]. □

3.2.2 Part 1: Finding Bob's Key

In this subsection, we show that the attack algorithm described in Construction 2.11 can efficiently find Bob's key with high probability, assuming that Conjecture 2.16 is true. We first state and show a useful lemma that allows us to assume that when Bob sends the last message, he has already computed the key k on his side.

Lemma 3.5. *Let (A, B) be a CC1QM-KA protocol. Let ϕ_{B} be the internal state of B after he computed the message ψ. Then, we can assume w.l.o.g. that Bob has computed the key k_{B} from ϕ_{B} before he sends the last message ψ to Alice.*

Proof. Since the last message of the protocol is sent to Alice by Bob, by the no-signaling principle, Alice's computation after receiving ψ must commute with Bob's computation after sending ψ. Thus, Bob can compute the key on his side before sending the last message ψ.

□

Lemma 3.6 (Simulation). *Let (A, B) be a CC1QM-KA protocol where Alice and Bob make at most d queries to an oracle $h : \mathcal{X} \to \mathcal{Y}$, and Alice does not query the oracle after receiving the last message. Assuming Conjecture 2.16 is true, for $0 < \nu < 1$, there exists an active attacker Eve that finds Bob's key k_{B} with probability at least $1 - \nu$ and Eve is expected to make at most $\mathsf{poly}\left(d, \frac{1}{\nu}\right)$ queries to h.*

Proof of Lemma 3.6. Let Bob's last message be $\psi_M = \sum_i q_i |\psi_i\rangle\langle\psi_i|_M$, and let $\mathsf{A}'_{\mathsf{fin}} := \Pi_{\mathsf{k}} \mathsf{A}_{\mathsf{fin}}$ be Alice's computation in the last step of the protocol. Let k_{B} be the key computed by Bob at the end of the protocol. By Lemma 3.5, we can assume that Bob already computes his key k_{B} before sending the last message to Alice.

Our attacking algorithm Eve_1 is described below.

Construction 3.7. Eve_1 *runs the quantum-heavy queries learner* Eve *in Construction 2.11 with parameter $\varepsilon := \frac{1}{\mathsf{poly}\left(d, \frac{1}{\nu}\right)}$ conditioned on the classical transcript t until before Bob sends his last message, except that it aborts if* Eve *asks more than $\frac{d}{\varepsilon}$ queries. In the case* Eve_1 *does not abort, let $|\Psi_t^{\mathsf{Eve}}\rangle_{W'_{\mathsf{A}} W'_{\mathsf{B}} H'}$ be the state that* Eve *outputs, conditioned on the classical transcript t.* Eve_1 *then outputs the measurement outcome of*

$$\mathsf{A}'_{\mathsf{fin}} \left(|\Psi_t^{\mathsf{Eve}}\rangle_{W'_{\mathsf{A}} W'_{\mathsf{B}} H'} \otimes \psi_M \right),$$

where $\mathsf{A}'_{\mathsf{fin}}$ makes no oracle query to h and acts on two registers W'_{A} and M only.

By Lemma 2.13, the number of queries asked by Eve satisfies $\mathbb{E}\left[|L|\right] \le \frac{d}{\varepsilon}$. By Markov's inequality, we have

$$\Pr\left[|L| \ge \frac{d}{\nu \cdot \varepsilon}\right] \le \nu.$$

Thus, we can conclude that with probability at least $1-\nu$, all of the following events hold:

- Eve_1 is efficient: Eve_1 does not abort and asks at most $\frac{d}{\nu\cdot\varepsilon} = \mathsf{poly}(d, 1/\nu)$ queries.
- Up until before Bob sends his last message, no quantum ε-heavy query is left: for all $x \notin \mathcal{Q}_L, w(x) < \varepsilon$, where $w(\cdot)$ is defined in Definition 2.10.

Suppose that all the above events occur for the rest of the proof ($\star$). For simplicity, denote $|\Psi_t^{\mathsf{Eve}}\rangle_{W'_{\mathsf{A}}W'_{\mathsf{B}}H'}$ as $|\Psi_t^{\mathsf{Eve}}\rangle_{W'_{\mathsf{A}}E}$.

We will consider the purified version of the protocol. Let $|\phi_t\rangle_{WH}$ be the joint state of the real protocol before Bob sends his last message to Alice, conditioned on the classical transcript t. After Eve_1 learns the heavy queries, the resulting state becomes $|\phi_{t,L}\rangle$ conditioned on t and Eve's list of query-answer L. Since the oracle registers corresponding to Q_L are now measured, we can consider the "truncated" version of $|\phi_{t,L}\rangle_{WH}$ by discarding those registers. Let $\widetilde{H} := \{H_x\}_{x\in\mathcal{X}\setminus Q_L}$ be the set of remaining registers. By $|\phi_{t,L}\rangle_{W\widetilde{H}}$ we denote the truncated $|\phi_{t,L}\rangle_{WH}$.

Let $|\widehat{\Psi}_{t,L}\rangle_{W'_{\mathsf{A}}EW\widetilde{H}} := |\Psi_t^{\mathsf{Eve}}\rangle_{W'_{\mathsf{A}}E}\,|\phi_{t,L}\rangle_{W\widetilde{H}}$ be the joint state of Eve_1 and the real protocol right before Bob sends his last message to Alice. By Lemma 2.8, it holds that $\left|\hat{h}^{H}_{max}\left(|\widehat{\Psi}_{t,L}\rangle\right)\right| \le \mathsf{poly}(d, 1/\nu)$, and by Lemma 2.9, it holds that $\left|\hat{h}^{\widetilde{H}}_{max}\left(|\widehat{\Psi}_{t,L}\rangle\right)\right| \le \mathsf{poly}(d, 1/\nu)$.

By the assumption ($\star$) above, we have that $|\widehat{\Psi}_{t,L}\rangle$ is a $(\mathcal{Y}, \varepsilon, \mathsf{poly}(d,\nu), |\mathcal{X}|)$-state (with the register H in Definition 2.14 being $\widehat{H}$). Next, let $\psi_M = \sum_i q_i |\psi_i\rangle\langle\psi_i|_M$, we need to show that

$$\forall i, \left\|\Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}\,|\widehat{\Psi}_{t,L}\rangle_{W'_{\mathsf{A}}EW\widetilde{H}}\,|\psi_i\rangle_M\right\|^2 \ge 1 - \frac{1}{\nu},$$

where $\mathsf{A}_{\mathsf{fin}}$ cannot make queries to h and only acts on W'_{A} and M.

Fix i and write $|\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle_{W'_{\mathsf{A}}EW\widetilde{H}M} := \mathsf{A}_{\mathsf{fin}}\left(|\widehat{\Psi}_{t,L}\rangle_{W'_{\mathsf{A}}EW\widetilde{H}} \otimes |\psi_i\rangle_M\right)$.

Claim 3.8. *If $|\widehat{\Psi}_{t,L}\rangle$ is a $(\mathcal{Y}, \varepsilon, \mathsf{poly}(d,\nu), |\mathcal{X}|)$-state, it follows that $|\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle$ is a $(\mathcal{Y}, \varepsilon, \mathsf{poly}(d,\nu), |\mathcal{X}|)$-state as well.*

Proof. Assume that $|\widehat{\Psi}_{t,L}\rangle_{RH}$ is a $(\mathcal{Y}, \varepsilon, \mathsf{poly}(d,\nu), |\mathcal{X}|)$-state. Then, $|\widehat{\Psi}_{t,L}\rangle_{RH} \otimes |\psi_i\rangle_M$ is also a $(\mathcal{Y}, \varepsilon, \mathsf{poly}(d,\nu), |\mathcal{X}|)$-state, because this property only depends on the H register, who is unchanged there. Then, since $\mathsf{A}_{\mathsf{fin}}$ makes no query to the random oracle, the oracle register H is not modified and thus $|\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle$ is a $(\mathcal{Y}, \varepsilon, \mathsf{poly}(d,\nu), |\mathcal{X}|)$-state. □

We are going to show that there exists a key $\mathsf{k}' = b \in \{0,1\}$ such that the probability of the key b in the key distribution of $|\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle$ is larger than $1-\nu$. By contradiction, assume that for both $b=0$ and $b=1$, we have that the probability of this key is smaller than $1-\nu$. By considering the complementary events, we have that:

$$\left\|\Pi_0\,|\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle\right\|^2 \ge \nu, \text{ and}$$
$$\left\|\Pi_1\,|\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle\right\|^2 \ge \nu.$$

Let $|\widehat{\Psi}^{(\mathrm{i})}_{t,L,\mathsf{k}'=b}\rangle$ be the residual state conditioned on the key equal to b. Then, it follows that $|\widehat{\Psi}^{(\mathrm{i})}_{t,L,\mathsf{k}'=b}\rangle$ is a $(\mathcal{Y}, \varepsilon/\nu, \mathsf{poly}(d, 1/\nu), |\mathcal{X}|)$-state for both $b=0$ and $b=1$ because

1. $|\widehat{\Psi}^{(\mathrm{i})}_{t,L,\mathsf{k}'=b}\rangle$ is $\mathsf{poly}\big(d,\frac{1}{\nu}\big)$-sparse since $|\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle$ is $\mathsf{poly}\big(d,\frac{1}{\nu}\big)$-sparse and $\mathrm{supp}^{\widetilde{H}}(|\widehat{\Psi}^{(\mathrm{i})}_{t,L,\mathsf{k}'=b}\rangle) \subseteq \mathrm{supp}^{\widetilde{H}}(|\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle)$.
2. $|\widehat{\Psi}^{(\mathrm{i})}_{t,L,\mathsf{k}'=b}\rangle$ is ε/ν-light because:

$$\begin{aligned}
\Pr[\text{Not measuring } \hat{0} \text{ in } |\widehat{\Psi}^{(\mathrm{i})}_{t,L,\mathsf{k}'=b}\rangle] &= \Pr\left[\text{Not measuring } \hat{0} \text{ in } |\widehat{\Psi}^{(\mathrm{i})}_{t,L,\mathsf{k}'=b}\rangle \mid \mathsf{k}' = b\right] \\
&= \frac{\Pr\left[\text{Not measuring } \hat{0} \text{ in } |\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle \text{ and } \mathsf{k}' = b\right]}{\Pr[\mathsf{k}' = b]} \\
&\leq \frac{\Pr\left[\text{Not measuring } \hat{0} \text{ in } |\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle\right]}{\Pr[\mathsf{k}' = b]} \\
&\leq \varepsilon/\nu,
\end{aligned}$$

where the last inequality comes from the fact that $|\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle$ is ε-light and $\Pr[\mathsf{k}' = b] = \left\|\Pi_b\, |\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle\right\|^2 \geq \nu$.

Then Conjecture 2.16 implies that the states $|\widehat{\Psi}^{(\mathrm{i})}_{t,L,\mathsf{k}'=0}\rangle$ and $|\widehat{\Psi}^{(\mathrm{i})}_{t,L,\mathsf{k}'=1}\rangle$ are compatible, which means that there exists two different states $w^0, w^1 \in W'_{\mathsf{A}}EW$ and an oracle $\hat{h}$ such that $\hat{h}$ is consistent with w^0 and w^1. And for this specific oracle, w^0 outputs the key 0 and w^1 outputs the key 1, both with non-zero probability. However, Bob's key has already been computed by Lemma 3.5, and is fixed to some $\mathsf{k}_{\mathsf{B}} \in \{0,1\}$. Thus, there is an oracle such that Bob outputs k_{B}. Plus, for this specific oracle, Alice outputs key 0 with non-zero probability, and outputs key 1 with non-zero probability as well. Hence there is an execution of the protocol such that Bob outputs k_{B} and Alice outputs $\mathsf{k}_{\mathsf{A}} = 1 - \mathsf{k}_{\mathsf{B}}$, which breaks the perfect completeness of the protocol.

We now show that the key computed by Eve is the same as hypothetical Alice's key, defined by $\mathsf{k}_{\mathsf{A}'} = \mathsf{A}'_{\mathsf{fin}}\left(|\phi_{\mathsf{A}}\rangle_{AH} \otimes |\psi_i\rangle_M\right)$, that is the key that Alice would have computed if the protocol had continued normally. Since the protocol is perfect, we have that $\mathsf{k}_{\mathsf{A}'} = \mathsf{k}_{\mathsf{B}}$. Recall that Eve's key is computed from the state $|\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle = \mathsf{A}_{\mathsf{fin}}\left(|\widehat{\Psi}_{t,L}\rangle_{W'_{\mathsf{A}}EW\widetilde{H}} \otimes |\psi_i\rangle_M\right)$, and the state $|\widehat{\Psi}_{t,L}\rangle_{W'_{\mathsf{A}}EW\widetilde{H}}$ is a superposition of all of Alice's internal states that are consistent with Eve's view so far. The state $|\psi_i\rangle_M$ corresponds to the real message that Bob sent to Alice. First note that Alice will never output $\mathsf{k}_{\mathsf{A}} = \perp$, because the state of Eve consists of a superposition of Alice's states that are consistent with the transcript. Indeed, if the message $|\psi_i\rangle_M$ from Bob is inconsistent with the oracle, Alice is not able to detect it as she does not query the oracle in $\mathsf{A}_{\mathsf{fin}}$. Note that the real oracle used in the protocol is one of the oracles in the superposition of oracles that are consistent with Eve's view. Also, for a fixed oracle, the key is computed deterministically by the perfectness of the protocol, and thus Eve's key is equal to Bob's hypothetical key with probability $\left\|\Pi_{\mathsf{k}}\, |\widehat{\Psi}^{(\mathrm{i})}_{t,L}\rangle\right\|^2$ over the random oracles. This shows that Eve succeeds with probability at least $1 - \nu$.

□

3.2.3 Part 2: Making Alice Agrees on the Same Key as Bob

Using Lemma 3.6, we can now prove Lemma 3.4.

Proof of Lemma 3.4. Let (A, B) be a CC1QM-KA protocol where Alice and Bob make at most d queries to an oracle $h : \mathcal{X} \to \mathcal{Y}$, and Alice does not query the oracle after receiving the last message. Consider the following construction for Eve:

Construction 3.9. *Input:* ε, ν

1. Eve *applies the quantum* ε*-heavy query learner of Construction 2.11 to compute a state* $|\phi^E_A\rangle_{W'_A} |\phi^E_B\rangle_{W'_B} |h\rangle_H$ *which corresponds to a simulation of the internal state of Alice and Bob after the classical communication part of the protocol.*

2. *Let* $\mathsf{A}_{\mathsf{fin}}$ *be the operations that Alice applies at the end of the protocol after receiving the message* ψ *from Bob. Then,* Eve *outputs the resulting key* k_E *of* $\Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}|\phi_A^E\rangle\langle\phi_A^E||h\rangle\langle h|\psi(\mathsf{A}_{\mathsf{fin}})^\dagger$*, where* ψ *is the quantum message Bob sends to Alice.*
3. *Writing* $\tau_{EM} = \frac{\widetilde{\tau}}{\|\widetilde{\tau}\|}$*, where* $\widetilde{\tau} = (\mathsf{A}_{\mathsf{fin}})^\dagger\Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}|\phi_A^E\rangle\langle\phi_A^E||h\rangle\langle h|\psi$*,* Eve *sends the resulting state* $\mathrm{Tr}_E\left(\tau_{EM}\right)$ *to Alice, where she traces out everything but the register that contains the message.*

In the last part of the construction, Eve applies the operator $(\mathsf{A}_{\mathsf{fin}})^\dagger$ to uncompute Alice's operation before sending her state to Alice. Note that in step 2, we use the fact that Alice and Bob's states are unentangled, as shown by Lemma 2.17

Now, we prove that Construction 3.9 succeeds with probability at least $1-\nu$. Using Lemma 3.6, we have that Eve finds the right key k in Step 2 with probability at least $1-\nu$. Writing $\psi = \sum_i q_i \left|\psi_i\right\rangle$, this means that

$$\forall i, \left\|\Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}\left|\phi_A^E\right\rangle\left|h\right\rangle\left|\psi_i\right\rangle\right\|^2 \geq 1-\lambda. \tag{4}$$

We write $\psi^E = \mathrm{Tr}_E\left(\tau_{EM}\right)$ the message that Eve sends to Alice. The first thing that we want to show is that the message ψ^E from Eve is "close" to the real message ψ from Bob. More precisely, we will show that:

$$\forall i, \left\langle\psi_i\right|\psi^E\left|\psi_i\right\rangle \geq 1-\lambda. \tag{5}$$

For every i, we have that:

$$\begin{aligned}
\left\langle\psi_i\right|\psi^E\left|\psi_i\right\rangle &= \left\langle\psi_i\right|\mathrm{Tr}_E\left(\tau_{EM}\right)\left|\psi_i\right\rangle \\
&= \left\langle\psi_i\right|\mathrm{Tr}_E\left(\frac{\widetilde{\tau}}{\|\widetilde{\tau}\|}\right)\left|\psi_i\right\rangle \\
&\geq \left\langle\psi_i\right|\mathrm{Tr}_E\left(\widetilde{\tau}\right)\left|\psi_i\right\rangle \\
&= \mathrm{Tr}\left(|\psi_i\rangle\langle\psi_i|\,\mathrm{Tr}_E\left(\widetilde{\tau}\right)\right) \\
&= \mathrm{Tr}\left(I_E\otimes\left\langle\psi_i\right|_M\widetilde{\tau}\cdot I_E\otimes\left|\psi_i\right\rangle_M\right) \\
&\geq \mathrm{Tr}\left(\left\langle\phi_A^E\right|\left\langle h\right|\otimes\left\langle\psi_i\right|_M\widetilde{\tau}\cdot\left|\phi_A^E\right\rangle\left|h\right\rangle\otimes\left|\psi_i\right\rangle_M\right),
\end{aligned}$$

where we used elementary properties of the trace operator. Next, we have that

$$\mathrm{Tr}\left(\left\langle\phi_A^E\right|\left\langle h\right|\otimes\left\langle\psi_i\right|_M\widetilde{\tau}\cdot\left|\phi_A^E\right\rangle\otimes\left|\psi_i\right\rangle_M\right) = \left\langle\phi_A^E\right|\otimes\left\langle\psi_i\right|_M\widetilde{\tau}\cdot\left|\phi_A^E\right\rangle\left|h\right\rangle\otimes\left|\psi_i\right\rangle_M,$$

since the right term is a pure state. Replacing $\widetilde{\tau}$ with its value, we have:

$$\begin{aligned}
\left\langle\psi_i\right|\psi^E\left|\psi_i\right\rangle &\geq \left\langle\phi_A^E\right|\left\langle h\right|\left\langle\psi_i\right|\left((\mathsf{A}_{\mathsf{fin}})^\dagger\Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}|\phi_A^E\rangle\langle\phi_A^E||h\rangle\langle h|\psi\right)\left|\phi_A^E\right\rangle\left|h\right\rangle\left|\psi_i\right\rangle \\
&= \sum_j q_j\left\langle\phi_A^E\right|\left\langle h\right|\left\langle\psi_i\right|\left((\mathsf{A}_{\mathsf{fin}})^\dagger\Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}|\phi_A^E\rangle\langle\phi_A^E||H\rangle\langle H||\psi_j\rangle\langle\psi_j|\right)\left|\phi_A^E\right\rangle\left|h\right\rangle\left|\psi_i\right\rangle \\
&= \left\langle\phi_A^E\right|\left\langle h\right|\left\langle\psi_i\right|\left((\mathsf{A}_{\mathsf{fin}})^\dagger\Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}\left|\phi_A^E\right\rangle\left|h\right\rangle\left|\psi_i\right\rangle\right) \\
&= \left\|(\mathsf{A}_{\mathsf{fin}})^\dagger\Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}\left|\phi_A^E\right\rangle\left|h\right\rangle\left|\psi_i\right\rangle\right\|^2 \\
&= \left\|\Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}\left|\phi_A^E\right\rangle\left|h\right\rangle\left|\psi_i\right\rangle\right\|^2 \\
&\geq 1-\lambda,
\end{aligned}$$

where the last inequality comes from Equation (4).

Now fix i. We write $\left|\varPhi_A\right\rangle = \mathsf{A}_{\mathsf{fin}}\left|\phi_{\mathsf{A}}\right\rangle\otimes\left|h\right\rangle\otimes\left|\psi_i\right\rangle$ where $\left|\phi_{\mathsf{A}}\right\rangle$ corresponds to Alice's *real* register before receiving the message ψ. Since Π_{k} is a projector and $\Pi_{\mathsf{k}}\left|\varPhi_A\right\rangle = \left|\varPhi_A\right\rangle$ from perfect correctness, we can write it:

$$\Pi_{\mathsf{k}} = |\varPhi_A\rangle\langle\varPhi_A| + \sum_i |\sigma_i\rangle\langle\sigma_i|,$$

where the σ_i are such that $\langle\sigma_i|\Phi_A\rangle = 0$.

We write:

$$\psi^E = \alpha|\psi_i\rangle\langle\psi_i| + \beta\rho,$$

where $\rho = \sum_j p_j|\Psi_j\rangle\langle\Psi_j|$ is a mixed state such that $\langle\psi_i|\,\rho\,|\psi_i\rangle = 0$.

For every $|\psi_i\rangle$, we have that:

$$\begin{aligned}
&\mathrm{Tr}\left(\Pi_{\mathsf{k}}\mathsf{A}_{\mathsf{fin}}(|\phi_{\mathsf{A}}\rangle\langle\phi_{\mathsf{A}}| \otimes |h\rangle\langle h| \otimes \psi^E)\,(\mathsf{A}_{\mathsf{fin}})^\dagger\right)\\
&= \mathrm{Tr}\left(\left(|\Phi_A\rangle\langle\Phi_A| + \sum_i |\sigma_i\rangle\,\langle\sigma_i|\right)\left(\mathsf{A}_{\mathsf{fin}}|\phi_{\mathsf{A}}\rangle\langle\phi_{\mathsf{A}}| \otimes |h\rangle\langle h| \otimes (\alpha|\psi_i\rangle\langle\psi_i| + \beta\rho)\,(\mathsf{A}_{\mathsf{fin}})^\dagger\right)\right)\\
&= \mathrm{Tr}\left(\left(|\Phi_A\rangle\langle\Phi_A| + \sum_i |\sigma_i\rangle\,\langle\sigma_i|\right)\left(\alpha|\Phi_A\rangle\langle\Phi_A| + \beta\mathsf{A}_{\mathsf{fin}}|\phi_{\mathsf{A}}\rangle\langle\phi_{\mathsf{A}}| \otimes |h\rangle\langle h| \otimes \rho\,(\mathsf{A}_{\mathsf{fin}})^\dagger\right)\right)\\
&= \alpha\,\langle\Phi_A|\Phi_A\rangle^2 + \beta\,\langle\Phi_A|\,\mathsf{A}_{\mathsf{fin}}|\phi_A\rangle\langle\phi_A| \otimes |h\rangle\langle h| \otimes \rho(\mathsf{A}_{\mathsf{fin}})^\dagger\,|\Phi_A\rangle\\
&\quad + \alpha\sum_i |\,\langle\Phi_A|\sigma_i\rangle\,|^2 + \beta\sum_i \langle\sigma_i|\,\mathsf{A}_{\mathsf{fin}}|\phi_{\mathsf{A}}\rangle\langle\phi_{\mathsf{A}}| \otimes |h\rangle\langle h| \otimes \rho(\mathsf{A}_{\mathsf{fin}})^\dagger\,|\sigma_i\rangle\\
&= \alpha + \beta\sum_i \langle\sigma_i|\,\mathsf{A}_{\mathsf{fin}}|\phi_{\mathsf{A}}\rangle\langle\phi_{\mathsf{A}}| \otimes |h\rangle\langle h| \otimes \rho(\mathsf{A}_{\mathsf{fin}})^\dagger\,|\sigma_i\rangle\\
&\geq \alpha\\
&\geq 1 - \lambda,
\end{aligned}$$

where the fourth equality comes from the fact that

$$\langle\Phi_A|\,\mathsf{A}_{\mathsf{fin}}|\phi_{\mathsf{A}}\rangle\langle\phi_{\mathsf{A}}| \otimes \rho(\mathsf{A}_{\mathsf{fin}})^\dagger\,|\Phi_A\rangle = \langle\phi_{\mathsf{A}}|\,\langle\psi_i|\,(\mathsf{A}_{\mathsf{fin}})^\dagger\mathsf{A}_{\mathsf{fin}}|\phi_{\mathsf{A}}\rangle\langle\phi_{\mathsf{A}}| \otimes \rho(\mathsf{A}_{\mathsf{fin}})^\dagger\mathsf{A}_{\mathsf{fin}}\,|\phi_{\mathsf{A}}\rangle\,|\psi_i\rangle = \langle\psi_i|\,\rho\,|\psi_i\rangle = 0,$$

and that $\langle\sigma_i|\Phi_A\rangle = 0$. The first inequality comes from the fact that the terms in the sum are positive, because they correspond to the probability of measuring the state $|\phi_{\mathsf{A}}\rangle\langle\phi_{\mathsf{A}}| \otimes |h\rangle\langle h| \otimes \rho$ using the projection $\mathsf{A}_{\mathsf{fin}}\,\langle\sigma_i\rangle\,\mathsf{A}_{\mathsf{fin}}{}^\dagger$, and the last inequality comes from Equation (5).

This means that Alice measures the key k with probability at least $1-\lambda$ when receiving the message ψ^E from Eve and for pure message $|\psi_i\rangle$, and if this is the case the meet-in-the-middle attack is a success. Since this is true for all of the $|\psi_i\rangle$, it also follows for ψ by convexity. This concludes the proof.

□

3.3 Impossibility of quantum public-key encryption with classical keys

In this section, we show that the (conditional) impossibility of CC1QM-KA protocols proven above also implies a (conditional) impossibility for quantum public key encryption (qPKE) with classical public keys, but ciphertexts can be quantum states.

We first define the notion of qPKE with classical keys which is modified from the notion of qPKE with quantum keys given in [BGHD+23], then prove our impossibility.

Definition 3.10 (Public-key encryption with classical public keys). *Public-key encryption with classical public keys (qPKE) consists of three algorithms with the following syntax:*

- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{Gen}(1^\lambda)$: *a quantum algorithm, which takes as input the security parameter and outputs a classical key pair* $(\mathsf{pk}, \mathsf{sk})$.
- $qc \leftarrow \mathcal{Enc}(\mathsf{pk}, m)$: *a quantum algorithm, which takes as input a classical public key* pk, *a plaintext* m, *and outputs a possibly quantum ciphertext* qc.

- $m/\bot \leftarrow \mathcal{Dec}(\mathsf{sk}, qc)$*: a quantum algorithm, which takes as input a decryption key* sk*, a ciphertext* qc*, and outputs a classical plaintext* m *or a distinguished symbol* $\bot$ *indicating decryption failure.*

Furthermore, in the quantum random oracle model, we allow these algorithms to make quantum queries to a random function H*. We also allow these algorithms to be inefficient, but can only make at most polynomially (in the security parameter) many queries to the random oracle.*

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

$$\Pr\left[\mathcal{Dec}(\mathsf{sk}, qc) = m \;\middle|\; \begin{array}{c}(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{Gen}(1^\lambda) \\ qc \leftarrow \mathcal{Enc}(\mathsf{pk}, m)\end{array}\right] = 1,$$

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

We next define indistinguishability security of one-bit qPKE in Definition 3.11. When considering one-bit encryption this notion coincides with the one-way security notion, which is considered the weakest security notion of encryption. Thus, using this notion makes our negative result stronger.

Definition 3.11. *A one-bit qPKE scheme with classical public keys is IND-CPA secure if for every* QPT *adversary* $\mathcal{A}$*, for any* $\lambda \in \mathbb{N}$*, there exists a negligible function* $\mathsf{negl}(\lambda)$ *such that*

$$\Pr\left[\mathtt{IND-CPA}(\lambda, \mathcal{A}) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda),$$

where $\mathtt{IND-CPA}(\lambda, \mathcal{A})$ *is the following experiment:*

1. *The challenger chooses a random key pair* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{Gen}(1^\lambda)$*, and sends* pk *to the adversary* $\mathcal{A}$*.*
2. $\mathcal{A}$*, upon receiving the public key* pk*, sends two bits* $m_0, m_1 \in \{0,1\}$ *to the challenger.*
3. *The challenger samples a random bit* $b \leftarrow\$ \{0,1\}$*, and sends* $qc \leftarrow \mathcal{Enc}(\mathsf{pk}, m_b)$ *to* $\mathcal{A}$*.*
4. $\mathcal{A}$ *responds with a guess* b' *for* b*.*
5. *The challenger outputs* 1 *if* $b' = b$*, and* 0 *otherwise.*

Since the existence of an IND-CPA secure qPKE scheme with classical public keys in the QROM implies the existence of a CC1QM-KA protocol in the QROM, we also obtain the following result.

Corollary 3.12. *Assuming Conjecture 2.16 is true, there is no IND-CPA secure qPKE scheme with classical public keys in the QROM, where the decryption algorithm does not query the random oracle.*

Proof. By contradiction, let $\mathit{\Pi} = (\mathcal{Gen}, \mathcal{Enc}, \mathcal{Dec})$ be a qPKE scheme with classical public keys and assume it is IND-CPA secure. We construct a two-message one-bit CC1QM-KA protocol $\tilde{\mathit{\Pi}}$, where the first message from Alice to Bob is classical and the second message from Bob to Alice is quantum, as follows.

1. Alice generates $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$, and sends pk to Bob.
2. Bob generates uniformly at random a secret key $\mathsf{k} \in \{0,1\}$ and computes $qc \leftarrow \mathcal{Enc}(\mathsf{pk}, \mathsf{k})$, and sends qc to Alice.
3. Alice recovers the common key by computing $\mathsf{k} \leftarrow \mathcal{Dec}(\mathsf{sk}, qc)$.

It is easy to see that $\tilde{\mathit{\Pi}}$ is a secure CC1QC-KM protocol in the QROM if $\mathit{\Pi}$ is IND-CPA secure. Furthermore, if $\mathit{\Pi}$ is perfectly correct, $\tilde{\mathit{\Pi}}$ is also perfectly correct. Finally, if $\mathcal{Dec}(\cdot,\cdot)$ does not query the oracle, then Alice in the last step of $\tilde{\mathit{\Pi}}$ does not query the oracle as well. This contradicts Theorem 3.2 and concludes our proof. □

Remark 3.13. We note that our impossibility of CC1QM-KA is the strongest possible impossibility (conditioned on the assumption that Conjecture 2.16 is true), in the sense that the adversary can find the shared key and maintain the correctness of the protocol (that is, Alice and Bob can still find the shared key), while the usual security definition only asks the adversary to find the key of one of two parties. This strong impossibility allows us to rule out the possibility of qPKE in the QROM with stronger requirements, for example, qPKE with decryption error detectability as defined in [KMNY23].

Acknowledgments

This work is part of HQI initiative (www.hqi.fr) and is supported by France 2030 under the French National Research Agency award number ANR-22-PNCQ-0002.

ABG is supported by ANR JCJC TCS-NISQ ANR-22-CE47-0004 and QHV was also partially supported by the same grant.

References

ACC$^+$22. Per Austrin, Hao Chung, Kai-Min Chung, Shiuan Fu, Yao-Ting Lin, and Mohammad Mahmoody. On the impossibility of key agreements from quantum random oracles. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part II*, volume 13508 of *LNCS*, pages 165–194. Springer, Heidelberg, August 2022.

AQY22. Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 208–236. Springer, Heidelberg, August 2022.

BB84. Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *EEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8, 1984.

BCKM21. James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. On the round complexity of secure quantum computation. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 406–435, Virtual Event, August 2021. Springer, Heidelberg.

BGHD$^+$23. Khashayar Barooti, Alex B. Grilo, Loïs Huguenin-Dumittan, Giulio Malavolta, Or Sattath, Quoc-Huy Vu, and Michael Walter. Public-key encryption with quantum keys. Cryptology ePrint Archive, Paper 2023/877, 2023. https://eprint.iacr.org/2023/877.

BM09. Boaz Barak and Mohammad Mahmoody-Ghidary. Merkle puzzles are optimal - an $O(n^2)$-query attack on any key exchange from a random oracle. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 374–390. Springer, Heidelberg, August 2009.

CLM23. Kai-Min Chung, Yao-Ting Lin, and Mohammad Mahmoody. Black-box separations for non-interactive classical commitments in a quantum world. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part I*, volume 14004 of *LNCS*, pages 144–172. Springer, Heidelberg, April 2023.

Col23. Andrea Coladangelo. Quantum trapdoor functions from classical one-way functions. *CoRR*, abs/2302.12821, 2023.

GLSV21. Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in MiniQCrypt. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 531–561. Springer, Heidelberg, October 2021.

IR89. Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In *21st ACM STOC*, pages 44–61. ACM Press, May 1989.

KMNY23. Fuyuki Kitagawa, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Quantum public-key encryption with tamper-resilient public keys from one-way functions. Cryptology ePrint Archive, Paper 2023/490, 2023. https://eprint.iacr.org/2023/490.

KQST23. William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. In Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023*, pages 1589–1602. ACM, 2023.

Kre21. William Kretschmer. Quantum pseudorandomness and classical complexity. In Min-Hsiu 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.

MY22. Tomoyuki Morimae and Takashi Yamakawa. One-wayness in quantum cryptography. Cryptology ePrint Archive, Report 2022/1336, 2022. https://eprint.iacr.org/2022/1336.

NC10. Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information.* Cambridge university press, 2010.

Wie83. Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

Zha19. 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.