Proofs of Quantum Memory

Minki Hhan[1], Tomoyuki Morimae[2], Yasuaki Okinaka[2], Takashi Yamakawa[3,4,2]

[1]School of Computing, KAIST, Daejeon, Republic of Korea
minkihhan@kaist.ac.kr
[2]Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto, Japan
{tomoyuki.morimae,yasuaki.okinaka}@yukawa.kyoto-u.ac.jp
[3]NTT Social Informatics Laboratories, Tokyo, Japan
takashi.yamakawa@ntt.com
[4]NTT Research Center for Theoretical Quantum Information, Atsugi, Japan

Abstract

With the rapid advances in quantum computer architectures and the emerging prospect of large-scale quantum memory, it is becoming essential to classically verify that remote devices genuinely allocate the promised quantum memory with a specified number of qubits. In this paper, we introduce a new concept, *proofs of quantum memory (PoQM)*. A PoQM is an interactive protocol between a classical probabilistic polynomial-time (PPT) verifier and a quantum polynomial-time (QPT) prover over a classical channel where the verifier can verify that the prover has possessed a quantum memory with a specified number of qubits for a specified period of time. PoQM generalize the well-studied notion of proofs of quantumness (PoQ) [Brakerski, Christiano, Mahadev, Vazirani, and Vidick, JACM 2021] where a classical verifier can verify that the prover is not classical. Our contributions are summarized as follows:

- We introduce a formal definition of PoQM. We also introduce a variant of PoQM, which we call inefficient-verifier PoQM (IV-PoQM), where the verifier's final computation to make the decision is not necessarily efficient. Clearly, PoQM imply IV-PoQM.
- We construct PoQM based on the hardness of LWE. Specifically, we give two constructions of PoQM. The first one is of two-round (i.e., four-message) and has negligible soundness error under the subexponential-hardness of LWE. The second one is of polynomial-round and has inverse-polynomial soundness error under the polynomial-hardness of LWE.
- As a lowerbound of IV-PoQM (and therefore PoQM), we show that IV-PoQM imply one-way puzzles. Moreover, we show that a certain restricted version of PoQM implies quantum computation classical communication (QCCC) key exchange, which suggests the difficulty of black-box constructing PoQM from one-way functions.
- We show that constant-round PoQ imply PoQM or single-round PoQ (with a quantum verifier). Single-round PoQ are "trivial" PoQ in the sense that the verifier asks the prover to solve a classical problem which is quantumly easy but classically hard. The result therefore demonstrates that PoQM capture "genuinely-interactive" PoQ.
- We show that if constant-round IV-PoQ that are black-box constructed from quantumly-secure falsifiable assumptions exist then IV-PoQM exist. This result implies that IV-PoQM can be constructed from quantumly-secure constant-round statistically-hiding commitments (and therefore from quantumly-secure collision-resistant hash functions).

Contents

1 Introduction **1**
- 1.1 Our Results . . . 1
- 1.2 Technical Overview . . . 6
- 1.3 Related Works . . . 11

2 Preliminaries **12**
- 2.1 Basic Notations . . . 12
- 2.2 Lemmata . . . 12
- 2.3 Cryptography . . . 13

3 Proofs of Quantum Memory **16**
- 3.1 Definition . . . 16
- 3.2 Amplification of m_2 . . . 17
- 3.3 Relation to PoQ . . . 18

4 Constructions of PoQM **18**
- 4.1 1-of-2^k Puzzles Imply PoQM . . . 19
- 4.2 RSPs Imply PoQM . . . 20

5 Lowerbounds of (IV-)PoQM **25**
- 5.1 IV-PoQM imply StatePuzzs . . . 25
- 5.2 Predictable PoQM Imply QCCC KE . . . 27

6 Constant-Round PoQ Imply Single-Round QV-PoQ or PoQM **28**

7 Constant-Round IV-PoQ with Black-Box Reduction Imply IV-PoQM **31**
- 7.1 Preliminaries . . . 31
- 7.2 Results . . . 32

A Weak Predictable PoQM **38**

B QCCC KE Security Amplification **40**

1 Introduction

Imagine a quantum computing startup claiming that it has built a quantum processor equipped with a 100-million-qubit quantum memory. How could a classical investor verify such a claim?

Proofs of quantumness (PoQ) [BCM+21] are insufficient for this purpose. A proof of quantumness is an interactive protocol between a classical probabilistic polynomial-time (PPT) verifier and a quantum polynomial-time (QPT) prover over a classical channel. Completeness is that if the prover behaves honestly, the verifier accepts with high probability, and soundness is that the verifier rejects with high probability if the prover is PPT. Using PoQ, a classical investor could confirm that the quantum startup is doing something at least non-classical, but it cannot verify that the startup can manipulate a 100-million-qubit quantum memory.

With the rapid advances in quantum computer architectures and the emerging prospect of large-scale quantum memory, the following question is becoming essential:

Can a classical verifier verify that a remote prover has possessed a quantum memory with a specified number of qubits for a specified period of time?

1.1 Our Results

In this paper, we address this question by introducing a new concept, which we call *proofs of quantum memory* (PoQM). A PoQM is an interactive protocol between a PPT verifier and a QPT prover over a classical channel where the verifier can verify that the prover has kept a specified number of qubits for a specified time period.

Our contributions are summarized as follows:[1]

1. **Definitions.** We give a formal definition of PoQM. We also define a variant of PoQM, which we call inefficient-verifier PoQM (IV-PoQM), where the verifier's final computation to make the decision is not necessarily efficient. Clearly, PoQM imply IV-PoQM.

2. **Constructions.** We provide two constructions of PoQM from the hardness of LWE. The first one is of two-round (i.e., four-message) and has negligible soundness error under the subexponential-hardness of LWE. The second one is of polynomial-round and has inverse-polynomial soundness error under the polynomial-hardness of LWE.

3. **Lowerbounds.** We show a lowerbound of IV-PoQM (and therefore PoQM). We show that IV-PoQM imply one-way puzzles (OWPuzzs), which are a natural quantum analogue of one-way functions (OWFs) introduced by Khurana and Tomer [KT24]. We also show that a certain restricted version of PoQM, which includes one of our constructions, implies quantum key-exchange over a classical channel (QCCC KE), which suggests that black-box constructions of PoQM from OWFs will be difficult.

4. **PoQM capture genuinely-interactive PoQ.** We show that constant-round PoQ imply PoQM or single-round[2] quantum-verifier PoQ (QV-PoQ). Here, QV-PoQ are PoQ with a QPT verifier, while the communication remains classical. Single-round (QV-)PoQ are "trivial" PoQ in the sense that the verifier asks the prover to solve a classical problem which is quantumly easy but classically hard. Therefore, the result demonstrates that PoQM capture "genuinely-interactive" PoQ.

[1] The results in the fourth and fifth items actually hold up to i.o.-soundness, but for simplicity, here we omit it.

[2] In this paper, a single round is a set of two messages, first one being from the verifier to the prover and the second one from the prover to the verifier.

5. **Constant-round IV-PoQ with black-box reduction imply IV-PoQM.** We show that if constant-round IV-PoQ[3] that can be black-box constructed from quantumly-secure falsifiable assumptions[4] exist then IV-PoQM exist. The assumption is natural, because many known constructions of (IV-)PoQ are the black-box ones from quantumly-secure falsifiable assumptions. In particular, [MY24] constructed constant-round IV-PoQ from statistically-hiding commitments in a black-box way. Therefore, the result also implies that IV-PoQM can be constructed from quantumly-secure constant-round statistically-hiding commitments (and therefore from quantumly-secure collision-resistant hash functions).

In the following, we provide more details.

Formal definition of PoQM. We formally define PoQM as follows.[5] (Also see Figure 1.) Let $\alpha, \beta : \mathbb{N} \to [0,1]$ be any functions. Let $m_1, m_2 : \mathbb{N} \to \mathbb{N}$ be any (polynomially-bounded[6]) functions such that $m_1 > m_2$. An $(\alpha, \beta, m_1, m_2)$-PoQM is a tuple $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$ of interactive algorithms over a classical channel. $\mathcal{V}_1$ and $\mathcal{V}_2$ are PPT, and $\mathcal{P}_1$ and $\mathcal{P}_2$ are QPT. The interaction consists of two phases, the initialization phase and the execution phase. In the initialization phase, both $\mathcal{V}_1$ and $\mathcal{P}_1$ take the security parameter 1^λ as input, and interact over a classical channel. $\mathcal{V}_1$ outputs a classical bit string v, and $\mathcal{P}_1$ outputs a classical bit string state and an m_1-qubit quantum state σ_{state}.[7]

In the execution phase, $\mathcal{V}_2$ takes v as input, and $\mathcal{P}_2$ takes $(\mathsf{state}, \sigma_{\mathsf{state}})$ as input. They interact over a classical channel, and $\mathcal{V}_2$ outputs $\top$ or $\bot$. α-completeness requires that $\mathcal{V}_2$ outputs $\top$ with probability at least α, that is, the honest prover with an m_1-qubit memory is accepted with high probability. On the other hand, (β, m_2)-soundness is defined as follows. Let $\mathcal{P}_1^*$ be a QPT algorithm that interacts with $\mathcal{V}_1$, and outputs a classical bit string s and an m_2-qubit state ρ. Let $\mathcal{P}_2^*$ be a QPT algorithm that takes (s, ρ) as input, and interacts with $\mathcal{V}_2$. Then for any such $(\mathcal{P}_1^*, \mathcal{P}_2^*)$, $\mathcal{V}_2$ outputs $\top$ with probability at most β. Note that we do not make any upperbound for the size of the classical bit string s: it can be any polynomial length. Moreover, during the computation, $\mathcal{P}_1^*$ and $\mathcal{P}_2^*$ can use any polynomially-large quantum memory.

This intuitively means that any malicious prover that can preserve at most m_2-qubit quantum memory during the interval between the initialization phase and the execution phase cannot be accepted by the verifier. In other words, if the verifier accepts, the verifier can verify that the prover has possessed at least (m_2+1)-qubit quantum memory during the interval between the initialization phase and the execution phase.

Relation to PoQ. We observe that PoQM generalize the notion of PoQ:

Theorem 1.1. *Let $\alpha, \beta : \mathbb{N} \to [0,1]$ be any functions such that $\alpha(\lambda) > \beta(\lambda)$ for all $\lambda \in \mathbb{N}$. Let $m_1, m_2 : \mathbb{N} \to \mathbb{N}$ be any functions such that $m_1 > m_2$. If $(\alpha, \beta, m_1, m_2)$-PoQM exist, then (α, β)-PoQ exist.*

Constructions of PoQM. We provide two constructions of PoQM based on the hardness of LWE. The first construction is based on the subexponential hardness of LWE.

Theorem 1.2. *Let $m_2 : \mathbb{N} \to \mathbb{N}$ be any polynomially-bounded function. Assuming the subexponential hardness of LWE, two-round $(1 - \mathsf{negl}, \mathsf{negl}, m_1, m_2)$-PoQM exist with some polynomial m_1.*[8]

[3] Inefficient-verifier PoQ (IV-PoQ) [MY24] is a variant of PoQ where the verifier's final computation to make the decision is not necessarily efficient.

[4] In this paper, we define falsifiable assumptions in such a way that the challenger is not necessarily efficient.

[5] Our definition is based on (classical) proofs of space [DFKP15] and quantum proofs of space [MV20]. For details, see Section 1.3.

[6] This means $m_1, m_2 = O(\lambda^c)$ for some constant $c > 0$. This condition is occasionally omitted if it is clear from the context.

[7] During the operation of the initialization phase, the prover can use more than m_1 qubits.

[8] The concrete polynomial for m_1 depends on the choice of parameters of LWE.

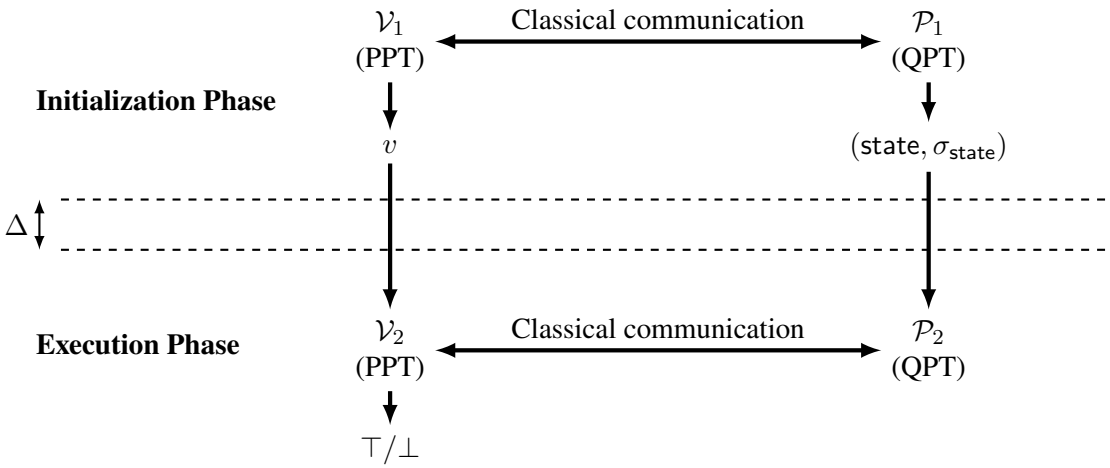

Figure 1: A PoQM consists of two phases: the initialization phase and the execution phase. At the end of the initialization phase, $\mathcal{V}_1$ outputs a classical bit string v, and $\mathcal{P}_1$ outputs a classical bit string state and an m_1-qubit quantum state σ_{state}. The verifier can enforce a time delay Δ between the initialization phase and the execution phase. At the beginning of the execution phase, $\mathcal{V}_2$ takes v as input, and $\mathcal{P}_2$ takes $(\mathsf{state}, \sigma_{\mathsf{state}})$ as input. At the end of the execution phase, $\mathcal{V}_2$ outputs $\top$ or $\bot$.

The second construction is based on the polynomial hardness of LWE.

Theorem 1.3. *Let p be any polynomial. Let $m_2 : \mathbb{N} \to \mathbb{N}$ be any polynomially-bounded function such that $m_2(\lambda) = \omega(\log(\lambda))$. Assuming the polynomial hardness of LWE, r-round $(1 - \mathsf{negl}, 1/p, \lceil 9.1m_2 \rceil, m_2)$-PoQM exist with a certain polynomial r.*

These two results are incomparable. The first construction is of two-round and with negligible soundness, while the assumption, the subexponential hardness of LWE, is stronger. On the other hand, the second construction is based on the polynomial hardness of LWE, but it is of poly-round and soundness is only $1/\mathrm{poly}$.[9]

Lowerbounds of (IV-)PoQM. We show that one-way puzzles (OWPuzzs) [KT24][10] are a lowerbound of IV-PoQM (and therefore PoQM):

Theorem 1.4. *Let $\alpha, \beta : \mathbb{N} \to [0, 1]$ be any functions such that $\alpha(\lambda) - \beta(\lambda) \geq 1/\mathrm{poly}(\lambda)$ for all sufficiently large $\lambda \in \mathbb{N}$. Let $m_1, m_2 : \mathbb{N} \to \mathbb{N}$ be any functions such that $m_1 > m_2$. If $(\alpha, \beta, m_1, m_2)$-IV-PoQM exist, then OWPuzzs exist.*

OWPuzzs are a natural quantum analogue of OWFs. A OWPuzz is a pair $(\mathsf{Samp}, \mathsf{Ver})$ of algorithms. Samp is a QPT algorithm that takes the security parameter 1^λ as input and outputs classical bit strings puzz and ans. Ver is an unbounded algorithm that takes $(\mathsf{puzz}, \mathsf{ans})$ as input and outputs $\top$ or $\bot$. Correctness is

$$\Pr[\top \leftarrow \mathsf{Ver}(\mathsf{puzz}, \mathsf{ans}) : (\mathsf{puzz}, \mathsf{ans}) \leftarrow \mathsf{Samp}(1^\lambda)] \geq 1 - \mathsf{negl}(\lambda) \tag{1}$$

[9] Parallel repetitions are non-trivial in PoQM, and we do not know how to do it.

[10] In this paper, if we just say OWPuzzs, they are quantumly-secure ones. We explicitly add "classically-secure" if they are only classically-secure.

and security is

$$\Pr[\top \leftarrow \mathsf{Ver}(\mathsf{puzz}, \mathsf{ans}') : (\mathsf{puzz}, \mathsf{ans}) \leftarrow \mathsf{Samp}(1^\lambda), \mathsf{ans}' \leftarrow \mathcal{A}(1^\lambda, \mathsf{puzz})] \leq \mathsf{negl}(\lambda) \tag{2}$$

for any QPT adversary $\mathcal{A}$. OWPuzzs are implied by many quantum cryptographic primitives, and imply non-interactive bit commitments and multiparty computations [KT24, MY22, Yan22, AQY22].

[MSY25] showed that PoQ imply classically-secure OWPuzzs. An interesting open question is whether any quantumly-secure quantum cryptographic primitive is implied by PoQ. Theorem 1.4 does not solve the open problem, but gives a "partial answer" in the sense that a generalization (i.e., PoQM) of PoQ implies the quantumly-secure quantum cryptographic primitive, namely, OWPuzzs.

If we consider a restricted version of PoQM (which we call *predictable PoQM*), then we obtain a potentially stronger[11] lowerbound:

Theorem 1.5. *Let $m_1 : \mathbb{N} \to \mathbb{N}$ be any function. Let p be any polynomial. If $(1-\mathsf{negl}, 1-\frac{1}{p}, m_1, 0)$-predictable PoQM exist, then QCCC KE exist.*

Here, an $(\alpha, \beta, m_1, m_2)$-predictable PoQM is an $(\alpha, \beta, m_1, m_2)$-PoQM where the execution phase is of single round, and the final verification algorithm is in the following special form: $\mathcal{V}_2$ computes a bit string by itself and accepts if and only if the bit string is equal to the bit string sent from $\mathcal{P}_2$. Our construction of PoQM based on the polynomial hardness of LWE satisfies this property. A QCCC KE is a key exchange in the quantum computation and classical communication (QCCC) setting, i.e., Alice and Bob are QPT but all communications are classical.

PoQ have been constructed from several assumptions including the hardness of LWE [BCM+21], noisy-trapdoor claw-free functions [BCM+21], trapdoor two-to-one collision resistant hash functions [KMCVY22], full-domain trapdoor permutations [MY23], iO plus OWFs [SZ25], etc. However, these assumptions are relatively stronger, and an important open problem is whether PoQ can be constructed from much weaker assumptions, for example, OWFs.[12] Given the fact that PoQM are a generalization of PoQ, it is also important to ask whether PoQM can be constructed from OWFs. Theorem 1.5 gives a negative evidence: at least the restricted version of PoQM will not be constructed from OWFs in a black-box way, because there is evidence that QCCC KE will not be constructed from OWFs in a black-box way [LLLL25, ACC+22, LLLL24].[13]

PoQM capture genuinely-interactive PoQ. Single-round (QV-)PoQ can be considered as "trivial" ones, because the verifier sends a classical message to the prover, which is a quantumly-easy but classically-hard problem, and asks the prover to solve it. (For example, sending an integer to the prover and asking the prover to return its factor.) On the other hand, there are "genuinely-interactive" PoQ, such as those that use the rewinding [BCM+21]. The formal definition of PoQ just includes these two types of PoQ, and therefore the definition cannot distinguish them. Can we capture only genuinely-interactive PoQ?

We show that PoQM somehow capture such genuinely-interactive PoQ. We show the following theorem, which says that ℓ-round PoQ imply ℓ-round PoQM, $(\ell-1)$-round PoQ, or single-round quantum-verifier PoQ (QV-PoQ).

Theorem 1.6. *Let $\ell : \mathbb{N} \to \mathbb{N}$ be any polynomial. Let $\alpha, \beta : \mathbb{N} \to [0,1]$ be any functions such that $\alpha(\lambda) - \beta(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ for all $\lambda \in \mathbb{N}$. Let $\epsilon, \delta : \mathbb{N} \to [0,1]$ be any functions such that $\epsilon(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$,*

[11] [GMMY24] showed that QCCC KE imply OWPuzzs.

[12] Tomer and Zhandry [TZ26] recently showed that constant-round PoQ will not be constructed from iO plus OWPs in a black-box way.

[13] Note that, however, these impossibility results do not exclude the most general QCCC KE, because the results are only for the perfectly-correct case.

$\delta(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ *and* $(\alpha(\lambda) - \epsilon(\lambda)) - (\beta(\lambda) + \delta(\lambda)) \geq \frac{1}{\mathrm{poly}(\lambda)}$ *for all* $\lambda \in \mathbb{N}$. *If* ℓ*-round* (α, β)*-PoQ exist, then one of the following primitives exists:*

- ℓ*-round* $(\alpha, \alpha - \epsilon, \mathrm{poly}, 0)$*-PoQM (with i.o.-soundness).*
- *single-round* $(\alpha - \epsilon, \beta + \delta)$*-QV-PoQ (with i.o.-soundness).*
- $(\ell - 1)$*-round* $(\beta + \delta, \beta)$*-PoQ.*

By repeating this theorem, we obtain the following corollary.[14]

Corollary 1.7. *If constant-round PoQ exist, then one of the following primitives exists.*

- *constant-round PoQM with* $m_2 = 0$ *(with i.o.-soundness).*
- *single-round QV-PoQ (with i.o.-soundness).*

This corollary demonstrates that PoQM capture "genuinely-interactive" PoQ.

We also note that the proofs of Theorem 1.6 and Corollary 1.7 also work for the inefficient verifier cases, and therefore we obtain similar results for the IV setting.

Constant-round IV-PoQ with black-box reduction imply IV-PoQM. Cryptographic primitives are constructed from assumptions. In particular, we often focus on falsifiable assumptions [Nao03, GW11]. A falsifiable assumption is a pair $(\mathcal{C}, \mathsf{thres})$ of a (potentially-inefficient) challenger $\mathcal{C}$ and a constant $\mathsf{thres} \in [0, 1)$. The challenger interacts with an adversary $\mathcal{A}$ and outputs $\top$ or $\bot$. We say that an adversary $\mathcal{A}$ breaks the assumption if there exists a polynomial p such that $\Pr\left[\top \leftarrow \langle \mathcal{C}(1^\lambda), \mathcal{A}(1^\lambda)\rangle\right] \geq \mathsf{thres} + \frac{1}{p(\lambda)}$ for infinitely many $\lambda \in \mathbb{N}$. Falsifiable assumptions capture a wide class of cryptographic assumptions including OWFs, public-key encryption, oblivious transfers, the hardness of LWE, indistinguishability obfuscation, etc.

We say that an (IV-)PoQ is black-box constructed from a falsifiable assumption if there exists a QPT reduction algorithm $\mathcal{R}$ such that for any (not-necessarily-efficient) classical adversary $\mathcal{P}'$ that breaks soundness of the (IV-)PoQ, $\mathcal{R}^{\mathcal{P}'}$ breaks the assumption.

We show the following result.[15]

Theorem 1.8. *Let* ℓ *be any polynomial. Let* $\alpha, \beta : \mathbb{N} \to [0, 1]$ *be any functions such that* $\alpha(\lambda) - \beta(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ *for all* $\lambda \in \mathbb{N}$. *Let* $\epsilon : \mathbb{N} \to [0, 1]$ *be any function such that* $\epsilon(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ *and* $(\alpha(\lambda) - \epsilon(\lambda)) - \beta(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ *for all* $\lambda \in \mathbb{N}$. *Suppose that there exist* ℓ*-round* (α, β)*-IV-PoQ that are black-box constructed from a falsifiable assumption. Then one of the following exists.*

- ℓ*-round* $(\alpha, \alpha - \epsilon, \mathrm{poly}, 0)$*-IV-PoQM (with i.o.-soundness).*
- $(\ell - 1)$*-round* $(\alpha - \epsilon, \beta)$*-IV-PoQ that are black-box constructed from the falsifiable assumption.*

Repeatedly applying Theorem 1.8, we have the following corollary.[16]

Corollary 1.9. *If there exist constant-round IV-PoQ that are black-box constructed from a falsifiable assumption, then one of the following exists.*

[14] We can repeat the theorem only constant times, because of some technical reasons, and therefore the corollary holds only for the constant-round case. For details, see Remark 6.4.

[15] Showing a similar result for the non IV case is open.

[16] Again, we can show the corollary only for the constant-round case, because we can repeat Theorem 1.8 only constant times.

- *constant-round IV-PoQM (with i.o.-soundness).*
- *single-round IV-PoQ that are black-box constructed from the falsifiable assumption.*

However, [TZ26] showed that single-round IV-PoQ cannot be black-box reduced to a quantumly-secure falsifiable assumption. Therefore, we obtain the following corollary:

Corollary 1.10. *If there exist constant-round IV-PoQ that are black-box constructed from a quantumly-secure falsifiable assumption, then there exist constant-round IV-PoQM (with i.o.-soundness).*

This corollary leads to a new feasibility result of IV-PoQM: [MY24] constructed constant-round IV-PoQ from classically-secure constant-round statistically-hiding commitments in a black-box way, and the proof holds even for quantumly-secure commitments. Therefore Corollary 1.10 implies the following.

Corollary 1.11. *If quantumly-secure constant-round statistically-hiding commitments exist, then there exist constant-round IV-PoQM (with i.o.-soundness).*

Furthermore, constant-round statistically-hiding commitments can be obtained from collision-resistant hash functions [HM96], thus we also obtain the following corollary.

Corollary 1.12. *If quantumly-secure collision-resistant hash functions exist, then there exist constant-round IV-PoQM (with i.o.-soundness).*

1.2 Technical Overview

Here we provide a high-level overview of our proofs.

PoQM based on the polynomial hardness of LWE. (Theorem 1.3) Let us first explain our construction of $(1-\mathsf{negl}, 1/p, \lceil 9.1m_2\rceil, m_2)$-PoQM for any polynomial p and any polynomially-bounded function $m_2 : \mathbb{N} \to \mathbb{N}$ such that $m_2(\lambda) = \omega(\log(\lambda))$ based on the polynomial hardness of LWE. The basic idea of our construction is simple: First, let us consider the following "information-theoretically-secure" $(1-\mathsf{negl}, \mathsf{negl}, n, 0)$-PoQM [MV20]:

- *Initialization phase.* $\mathcal{V}_1$ generates the state $\sigma := \bigotimes_{i=1}^n H^{\theta_i}|x_i\rangle$ with random $(x,\theta) \in \{0,1\}^n \times \{0,1\}^n$ by itself and sends the state to $\mathcal{P}_1$ over a quantum channel. (Here, x_i and θ_i are the ith bit of x and θ, respectively. H is the Hadamard operator.) $\mathcal{V}_1$ outputs (x,θ). $\mathcal{P}_1$ outputs σ.
- *Execution phase.* $\mathcal{V}_2$ takes (x,θ) as input. $\mathcal{P}_2$ takes σ as input. $\mathcal{V}_2$ sends θ to $\mathcal{P}_2$, and $\mathcal{P}_2$ measures ith qubit of σ in the computational (Hadamard) basis if $\theta_i = 0$ ($\theta_i = 1$) for all $i \in [n]$. Let x'_i be the measurement result on the ith qubit. $\mathcal{P}_2$ sends $\{x'_i\}_{i\in[n]}$ to $\mathcal{V}_2$. If $x_i = x'_i$ for all $i \in [n]$, $\mathcal{V}_2$ accepts. Otherwise, $\mathcal{V}_2$ rejects.

This information-theoretically-secure PoQM does not achieve our goal, because of the following two reasons:

1. It is only the case when $m_2 = 0$. We want to construct $(1-\mathsf{negl}, 1/\mathrm{poly}, \lceil 9.1m_2\rceil, m_2)$-PoQM for any polynomial m_2.
2. Both the verifier and the channel are quantum.

The first issue is solved by using a lemma of [BZ13]. The lemma says the following: Let $\mathcal{A}$ be a quantum algorithm that outputs a classical bit string. Let $\mathcal{A}'$ be the algorithm that is the same as $\mathcal{A}$ except that a k-outcome measurement is done at any step. Then, $\Pr[x \leftarrow \mathcal{A}] \leq k \Pr[x \leftarrow \mathcal{A}']$ for any x.[17] Using this lemma, we can show that an $(\alpha, \beta, m_1, 0)$-PoQM is an $(\alpha, 2^{m_2}\beta, m_1, m_2)$-PoQM for any α, β, m_1, m_2 as follows: Let $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$ be an $(\alpha, \beta, m_1, 0)$-PoQM. Assume that it is not an $(\alpha, 2^{m_2}\beta, m_1, m_2)$-PoQM. Then there exists a pair $(\mathcal{P}_1^*, \mathcal{P}_2^*)$ of QPT adversaries such that $\mathcal{P}_1^*$ outputs a classical bit string s and an m_2-qubit state ρ, $\mathcal{P}_2^*$ takes (s, ρ) as input, and the probability that $\mathcal{V}_2$ outputs $\top$ is strictly larger than $2^{m_2}\beta$. Let us define another QPT adversary $\mathcal{P}_1^{**}$ as follows: $\mathcal{P}_1^{**}$ runs $\mathcal{P}_1^*$ but it measures all qubits of the output state ρ of $\mathcal{P}_1^*$ in the computational basis, and outputs the measurement result. Then, by using the lemma of [BZ13], the probability that $(\mathcal{P}_1^{**}, P_2^*)$ is accepted is strictly larger than $2^{-m_2} \times 2^{m_2}\beta = \beta$, which is the contradiction.

Therefore, we want to show that soundness (i.e., β) of the above information-theoretically-secure PoQM is $\beta = 2^{-m_2} \times \mathsf{negl}$.[18] In order to show it, we use the lemma, called *the LOCC leakage property for BB84 states*, which was introduced in [ÇG24] for another purpose, namely, constructions of leakage-resilient encryption and signatures. This lemma shows the following. Let us consider the following security game:

1. A challenger generates a random BB84 state $\sigma := \bigotimes_{i=1}^n H^{\theta_i}|x_i\rangle$ with random $(x, \theta) \in \{0,1\}^n \times \{0,1\}^n$.
2. An adversary sends the challenger a classical description E of a quantum algorithm that takes a quantum state as input and outputs a classical bit string.
3. The challenger runs $\eta \leftarrow E(\sigma)$[19], and sends the classical bit string η to the adversary.
4. The challenger sends θ to the adversary.
5. The adversary returns a bit string $x' \in \{0,1\}^n$ to the challenger.
6. The challenger accepts if $x = x'$, and rejects if $x \neq x'$.

The lemma says that the probability that the challenger accepts is at most $2^{-\frac{\xi}{2}\cdot n + 2^{-n}}$, where $\xi := -\log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) > 0.22$. By considering the above η as the output of $\mathcal{P}_1^*$, and taking $n = \lceil 9.1 m_2 \rceil$, we can show that the probability that the verifier accepts in the information-theoretically-secure PoQM is $2^{-\frac{\xi}{2}\lceil 9.1 m_2 \rceil + 2^{-\lceil 9.1 m_2 \rceil}} \leq 2^{-m_2} \times 2^{-0.001 m_2 + 2^{-9.1 m_2}} = 2^{-m_2} \times \mathsf{negl}$. (Note that $m_2(\lambda) = \omega(\log(\lambda))$ by assumption.)

The second issue that both the verifier and the channel are quantum in the information-theoretically-secure PoQM is solved by using verifiable remote state preparations (RSPs) [GV19, Zha25]. An RSP is a two-party protocol between a PPT sender and a QPT receiver. They interact over a classical channel. The receiver outputs a random BB84 state, and the sender outputs its classical description. By using this, we can replace the quantum verifier and the quantum channel with a PPT verifier and a classical channel. Because the RSP of [Zha25] requires poly round of communication, and it achieves only $1/\mathrm{poly}$-soundness, the final PoQM we obtain is of poly-round, and has only $1/\mathrm{poly}$-soundness.[20]

[17] $\Pr[x \leftarrow \mathcal{A}]$ is the probability that $\mathcal{A}$ outputs x.

[18] At this stage, we can achieve negl-soundness, but as we will see soon, due to the $1/\mathrm{poly}$-soundness of RSPs, what we finally get is only $1/\mathrm{poly}$-soundness.

[19] $\eta \leftarrow E(\sigma)$ means that the algorithm E is run on input σ, and the output is η.

[20] One might hope to avoid the polynomial-round overhead by replacing RSP with Oblivious State Preparation (OSP) [BK25]. However, since our proof crucially relies on verifiability, which OSP does not provide, it is unclear how to construct PoQM from OSP.

PoQM from the subexponential hardness of LWE. (Theorem 1.2) The above construction requires polynomial round of communication and achieves only $1/\mathrm{poly}$-soundness. To complement this, for any polynomially-bounded function $m_2 : \mathbb{N} \to \mathbb{N}$, we next construct two-round $(1-\mathsf{negl}, \mathsf{negl}, m_1, m_2)$-PoQM with some polynomial m_1 from the subexponential hardness of LWE.

The construction is based on 1-of-2^k puzzles [LLQ22]. 1-of-2 puzzles were first introduced in [RS19] to study *semi-quantum money*, which is a variant of quantum money that can be minted and verified classically. [LLQ22] extended 1-of-2 puzzles to 1-of-2^k puzzles to construct classically verifiable position verification. A 1-of-2^k puzzle consists of four algorithms $(\mathsf{KeyGen}, \mathsf{Obligate}, \mathsf{Solve}, \mathsf{Ver})$. KeyGen is a PPT algorithm that takes the security parameter 1^λ as input and outputs a public key pk and a secret key sk. $\mathsf{Obligate}$ is a QPT algorithm that takes pk as input and outputs a bit string y and a quantum state ρ. Solve is a QPT algorithm that takes pk, y, ρ and a randomly chosen k-bit string ch as input and outputs a classical answer ans. Ver is a polynomial-time classical deterministic algorithm that takes $\mathsf{sk}, y, \mathsf{ch}$ and ans as input and outputs $\top$ or $\bot$. Completeness is that Ver outputs $\top$ with probability at least $1-\mathsf{negl}(\lambda)$. In order to define soundness, we consider the following security game between a set $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ of adversaries and a challenger Chal.

1. Chal runs $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$.
2. $\mathcal{A}$ receives the public key pk and outputs a bit string y and a quantum state $\sigma_{\mathbf{BC}}$ over two registers $\mathbf{B}$ and $\mathbf{C}$.
3. $\mathcal{A}$ sends y to Chal. $\mathcal{A}$ sends the register $\mathbf{B}$ to $\mathcal{B}$. $\mathcal{A}$ sends the register $\mathbf{C}$ to $\mathcal{C}$.
4. Chal samples $\mathsf{ch} \leftarrow \{0,1\}^{k(\lambda)}$ and sends ch to both $\mathcal{B}$ and $\mathcal{C}$.
5. $\mathcal{B}$ outputs an answer $\mathsf{ans}_{\mathcal{B}}$, and sends it to Chal. $\mathcal{C}$ outputs an answer $\mathsf{ans}_{\mathcal{C}}$, and sends it to Chal.
6. Chal outputs $\top$ if and only if

$$\mathsf{Ver}(\mathsf{sk}, y, \mathsf{ch}, \mathsf{ans}_{\mathcal{B}}) = \top \wedge \mathsf{Ver}(\mathsf{sk}, y, \mathsf{ch}, \mathsf{ans}_{\mathcal{C}}) = \top. \tag{3}$$

With this security game, we define c-soundness as follows: for any set $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ of non-uniform QPT adversaries,

$$\Pr[\top \leftarrow \mathsf{Chal}] \leq 2^{-k(\lambda)} + \mathsf{negl}(2^{\lambda^c}). \tag{4}$$

We want to construct a two-round $(1-\mathsf{negl}, \mathsf{negl}, m_1, m_2)$-PoQM. Let $c > 0$ be any constant such that $m_2(\lambda) = O(\lambda^c)$. Set $k(\lambda) = \omega(\lambda^c)$. We construct a two-round $(1-\mathsf{negl}, \mathsf{negl}, m_1, m_2)$-PoQM from 1-of-$2^k$ puzzles with c-soundness as follows.

- *Initialization phase.* $\mathcal{V}_1$ runs $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$ and sends pk to $\mathcal{P}_1$. $\mathcal{P}_1$ runs $(y, \rho) \leftarrow \mathsf{Obligate}(\mathsf{pk})$ and sends y to $\mathcal{V}_1$. $\mathcal{V}_1$ outputs (sk, y), and $\mathcal{P}_1$ outputs (pk, y, ρ).
- *Execution phase.* $\mathcal{V}_2$ takes (sk, y) as input, and $\mathcal{P}_2$ takes (pk, y, ρ) as input. $\mathcal{V}_2$ samples random k-bit string ch and sends it to $\mathcal{P}_2$. $\mathcal{P}_2$ runs $\mathsf{ans} \leftarrow \mathsf{Solve}(\mathsf{pk}, y, \rho, \mathsf{ch})$, and sends ans to $\mathcal{V}_2$. $\mathcal{V}_2$ runs $\top/\bot \leftarrow \mathsf{Ver}(\mathsf{sk}, y, \mathsf{ch}, \mathsf{ans})$ and outputs the output.

Thus constructed PoQM is $(1-\mathsf{negl}, \epsilon, m_1, 0)$-PoQM with $\epsilon(\lambda) = (2^{-k(\lambda)} + \mathsf{negl}(2^{\lambda^c}))^{\frac{1}{2}}$, where $m_1(\lambda)$ is the number of qubits of the output quantum state ρ of $\mathsf{Obligate}$. The reason is as follows.

Assume that it is not $(\epsilon, 0)$-sound.[21] Then, there exists a pair $(\mathcal{P}_1^*, \mathcal{P}_2^*)$ of QPT adversaries such that $\mathcal{P}_1^*$ outputs only a classical bit string s, $\mathcal{P}_2^*$ takes only the classical bit string as input, and $\mathcal{V}_2$ outputs $\top$ with probability at least ϵ. From such $(\mathcal{P}_1^*, \mathcal{P}_2^*)$, we can construct a set $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ of adversaries for the 1-of-2^k puzzle whose winning probability is strictly larger than ϵ^2 as follows: Given pk, $\mathcal{A}$ runs $s \leftarrow \mathcal{P}_1^*(\mathsf{pk})$, sends s to both $\mathcal{B}$ and $\mathcal{C}$. $\mathcal{B}$ and $\mathcal{C}$ run $\mathsf{ans} \leftarrow \mathcal{P}_2^*(s, \mathsf{ch})$ and send ans to Chal, respectively. Because $\epsilon^2(\lambda) = ((2^{-k(\lambda)} + \mathsf{negl}(2^{\lambda^c}))^{\frac{1}{2}})^2 = 2^{-k(\lambda)} + \mathsf{negl}(2^{\lambda^c})$, c-soundness is broken.

Assuming the subexponential hardness of LWE, for any constant $c > 0$ and for any polynomial k, there exist 1-of-2^k puzzles with c-soundness [LLQ22]. Therefore, assuming the subexponential hardness of LWE, for any $c > 0$, we obtain $(1 - \mathsf{negl}, \epsilon, m_1, 0)$-PoQM, where $\epsilon(\lambda) = \mathsf{negl}(2^{\lambda^c})$.

Finally, by using the lemma of [BZ13], thus constructed $(1-\mathsf{negl}, \epsilon, m_1, 0)$-PoQM is $(1-\mathsf{negl}, 2^{m_2}\epsilon, m_1, m_2)$-PoQM. Because $2^{m_2(\lambda)}\epsilon(\lambda) = 2^{O(\lambda^c)}\mathsf{negl}(2^{\lambda^c}) = \mathsf{negl}(2^{\lambda^c}) = \mathsf{negl}(\lambda)$, we finally obtain $(1-\mathsf{negl}, \mathsf{negl}, m_1, m_2)$-PoQM.

Remark 1.13. Classical-communication public-key encryption with secure key leasing (PKE-SKL) [CGJL25, PWYZ24] also implies PoQM with $m_2 = 0$. However, the known construction of classical-communication PKE-SKL relies on the LWE assumption, and therefore the resulting PoQM still requires the LWE assumption. Moreover, if we want to amplify m_2 to an arbitrary polynomial, we need the subexponential hardness of LWE to withstand the exponential security loss. Thus, deriving PoQM from classical-communication PKE-SKL does not provide any advantage over the above construction.

IV-PoQM imply OWPuzzs. (Theorem 1.4) As a lowerbound of IV-PoQM, we show that IV-PoQM imply OWPuzzs. Because OWPuzzs are existentially equivalent to state puzzles (StatePuzzs) [KT25], we actually construct StatePuzzs from IV-PoQM. A StatePuzz is a QPT algorithm Samp that takes 1^λ as input and outputs a pair $(s, |\psi_s\rangle)$ of a bit string s and a pure quantum state $|\psi_s\rangle$. The security is that given s, no QPT algorithm can output a quantum state that is close to $|\psi_s\rangle$. Our construction of StatePuzzs from IV-PoQM is as follows: The classical puzzle s of the StatePuzz is the classical output state of $\mathcal{P}_1$ and the transcript τ of the initialization phase. The quantum answer $|\psi_s\rangle$ of the StatePuzz is the (purified) quantum output σ_{state} of $\mathcal{P}_1$. Intuitively, if thus constructed StatePuzz is not secure, there exists a QPT adversary $\mathcal{A}$ that, given $s = (\mathsf{state}, \tau)$, can output a quantum state ρ that is close to σ_{state}. Then, the following adversary $(\mathcal{P}_1^*, \mathcal{P}_2^*)$ can break the soundness of the IV-PoQM: $\mathcal{P}_1^*$ outputs $s = (\mathsf{state}, \tau)$. $\mathcal{P}_2^*$ takes s as input, runs $\rho \leftarrow \mathcal{A}(s)$, and runs $\mathcal{P}_2$ on (state, ρ).

Predictable PoQM imply QCCC KE. (Theorem 1.5) We also show that predictable PoQM imply QCCC KE. Our construction of QCCC KE is as follows: Alice and Bob run the initialization phase of the predictable PoQM: Alice runs $\mathcal{P}_1$ and Bob runs $\mathcal{V}_1$. Alice and Bob next run the execution phase of the predictable PoQM: Alice runs $\mathcal{P}_2$, does not send the output to Bob, and uses the output as her key. Bob runs $\mathcal{V}_2$, computes the output of Alice, and uses the output as his key. Because of the completeness of the predictable PoQM, their keys are equal with high probability, which shows the correctness of the KE. To show the security, assume that there is a QPT adversary Eve who, given the transcript of the interaction between Alice and Bob, can compute Alice's key. By using such Eve, we can construct an adversary $(\mathcal{P}_1^*, \mathcal{P}_2^*)$ that breaks soundness of the predictable PoQM as follows: $\mathcal{P}_1^*$ runs $\mathcal{P}_1$ and outputs the transcript of the initialization phase τ. $\mathcal{P}_2^*$ takes τ as input, runs Eve on input τ and $\mathcal{V}_2$'s message, and outputs the output of Eve.

[21] We remind the reader that $(\epsilon, 0)$-soundness means that the soundness is ϵ and $m_2 = 0$. In other words, any QPT adversary that has at most m_2-qubit quantum memory during the interval between the initialization phase and the execution phase is accepted with probability at most ϵ.

ℓ-round PoQ imply $(\ell-1)$-round PoQ, single-round QV-PoQ or ℓ-round PoQM. (Theorem 1.6) Assume that an ℓ-round PoQ $\langle \mathcal{V}, \mathcal{P} \rangle$ exists. We consider the following two cases:

- There exists a QPT prover $\mathcal{P}^*$ that is accepted by $\mathcal{V}$ with high probability and its internal state after the end of the $(\ell-1)$th round is classical.
- There is no such prover.

The second case immediately means the existence of PoQM by considering the first $(\ell-1)$ rounds as the initialization phase and the last round as the execution phase.

Therefore, let us assume that the first case happens. Then, by using $\mathcal{P}^*$, we construct the following single-round QV-PoQ $\langle \mathcal{V}', \mathcal{P}' \rangle$:

1. $\mathcal{V}'$ simulates the interaction between $\mathcal{V}$ and $\mathcal{P}^*$ by itself until $\mathcal{V}$ outputs its ℓth message.
2. $\mathcal{V}'$ sends the transcript and $\mathcal{P}^*$'s classical internal state to $\mathcal{P}'$.
3. $\mathcal{P}'$ computes $\mathcal{P}^*$'s ℓth message and sends it to $\mathcal{V}'$.
4. $\mathcal{V}'$ runs the last step of $\mathcal{V}$ to make the decision, and outputs the decision.

By the assumption, it is complete, i.e., $\mathcal{P}'$ is accepted by $\mathcal{V}'$ with high probability. If it is sound, i.e., no PPT prover can be accepted by $\mathcal{V}'$ with high probability, we obtain single-round QV-PoQ.

Therefore, let us assume that it is not sound. That is, there exists a PPT prover $\mathcal{A}$ that is accepted by $\mathcal{V}'$ with high probability. By using $\mathcal{A}$, we construct the following $(\ell-1)$-round PoQ $\langle \mathcal{V}'', \mathcal{P}'' \rangle$:

1. $\mathcal{V}''$ and $\mathcal{P}''$ run $\mathcal{V}$ and $\mathcal{P}^*$, respectively, until the end of the $(\ell-1)$th round. When $\mathcal{P}''$ sends the $(\ell-1)$th message to $\mathcal{V}''$, it also sends its classical internal state.
2. $\mathcal{V}''$ computes ℓth message of $\mathcal{V}$ and, by using it, runs $\mathcal{A}$.
3. By using the output of $\mathcal{A}$, $\mathcal{V}''$ runs the final step of $\mathcal{V}$ to compute the decision.
4. Output the decision.

By the assumption, it is complete, i.e., $\mathcal{P}''$ is accepted by $\mathcal{V}''$ with high probability. We can also show that it is sound. To show it, assume that there is a PPT adversary $\mathcal{B}$ that is accepted by $\mathcal{V}''$ with high probability. Then, $\mathcal{B}$ plus $\mathcal{A}$ break soundness of the original ℓ-round PoQ $\langle \mathcal{V}, \mathcal{P} \rangle$: first $\mathcal{B}$ is run by the $(\ell-1)$th round, and then $\mathcal{A}$ is run in the ℓth round. However, it is the contradiction.

ℓ-round IV-PoQ with black-box reduction imply ℓ-round IV-PoQM or $(\ell-1)$-round IV-PoQ with black-box reduction. (Theorem 1.8) Let $(\mathcal{V}, \mathcal{P})$ be an ℓ-round IV-PoQ that are black-box constructed from a falsifiable assumption. This means that there exists a QPT reduction algorithm $\mathcal{R}$ that satisfies the following: for any (not-necessarily-efficient) classical prover $\mathcal{P}'$ that is accepted by $\mathcal{V}$ with high probability, $\mathcal{R}^{\mathcal{P}'}$ breaks the falsifiable assumption.

Let us consider the following two cases.

- There exists a QPT algorithm $\mathcal{P}^*$ whose internal state after sending its $(\ell-1)$th message is classical and it is accepted by $\mathcal{V}$ with high probability.
- There is no such $\mathcal{P}^*$.

In the second case, we immediately obtain IV-PoQM by considering the first $(\ell-1)$ rounds of the IV-PoQ as the initialization phase and the ℓth round as the execution phase.

Therefore let us consider the first case. By using $\mathcal{P}^*$, we construct an $(\ell-1)$-round IV-PoQ $(\widetilde{\mathcal{V}}, \widetilde{\mathcal{P}})$ as follows:

1. $\widetilde{\mathcal{V}}$ and $\widetilde{\mathcal{P}}$ run $\mathcal{V}$ and $\mathcal{P}^*$, respectively, until the end of the $(\ell-1)$th round.
2. When $\widetilde{\mathcal{P}}$ sends its $(\ell-1)$th message, it also sends its classical internal state s.
3. $\widetilde{\mathcal{V}}$ simulates the ℓth round between $\mathcal{V}$ and $\mathcal{P}^*$ by itself, and outputs the output of $\mathcal{V}$.

Its completeness clearly follows from the assumption that $\mathcal{P}^*$ is accepted by $\mathcal{V}$ with high probability.

The remaining task is to show the existence of a QPT reduction algorithm $\mathcal{Q}$ that satisfies the following: for any (not-necessarily-efficient) classical algorithm $\widetilde{\mathcal{P}}^*$ that is accepted by $\widetilde{\mathcal{V}}$ with high probability, $\mathcal{Q}^{\widetilde{\mathcal{P}}^*}$ breaks the falsifiable assumption.

To show it, we define a classical (inefficient) adversary $\mathcal{A}$ interacting with $\mathcal{V}$ as follows: Run $\widetilde{\mathcal{P}}^*$ until the $(\ell-1)$th round. In the ℓth round, simulate the ℓth round of $\mathcal{P}^*$.

Clearly, $\mathcal{A}$ is accepted by $\mathcal{V}$ with high probability. Therefore, $\mathcal{R}^{\mathcal{A}}$ breaks the falsifiable assumption.

Let us define the QPT reduction algorithm $\mathcal{Q}^{\widetilde{\mathcal{P}}^*}$ as follows: It is identical to $\mathcal{R}^{\mathcal{A}}$ except for the following: when $\mathcal{R}$ queries $\mathcal{A}$'s inefficient part (namely, simulating the ℓth round of $\mathcal{P}^*$), the query is replaced with the efficient simulation of it.

Here, the last efficient simulation is always possible as is shown in [TZ26].[22] Therefore, the probability that $\mathcal{Q}^{\widetilde{\mathcal{P}}^*}$ wins the security game of the falsifiable assumption is close to that of $\mathcal{R}^{\mathcal{A}}$, which is large. Hence $\mathcal{Q}^{\widetilde{\mathcal{P}}^*}$ breaks the falsifiable assumption.

1.3 Related Works

[MM25] constructed information-theoretically-sound PoQ that are sound against *classical*-memory-bounded classical provers. They also constructed information-theoretically-secure claw generation that are secure against quantum-memory-bounded quantum provers. [CH22] introduced classical verification of quantum depth. Although these results share similar motivations, they would not be able to classically verify that a prover has possessed a certain amount of quantum memory for a specified period of time.

[CR20] constructed information-theoretically-sound quantum dimension tests. [FWZ23] constructed computationally-sound quantum dimension tests with a classical verifier. Dimension tests certify the amount of quantum memory available during the computation, but cannot certify the amount of quantum memory retained for a specified period of time.

[BGKM+23] constructed a test of qubits protocol. More recently, [BS26] introduced tests of non-commutation (ToNC), a weaker variant of qubit tests. As observed in [BS26], ToNC imply PoQM. Therefore, PoQM are weaker than qubit tests.

[MV20] introduced quantum proofs of space, which are a quantum variant of proofs of space [DFKP15]. Our definition of PoQM is based on them. However, the verifier and the channel of [MV20] are quantum.

[TZ26] showed that ℓ-round PoQ imply $(\ell-1)$-round PoQ, OWFs, or signature tokens. This result is similar to our Theorem 1.6 capturing "genuinely-interactive" PoQ. However, their result is incomparable with our result. (In particular, we do not know any relation between PoQM and signature tokens.)

[22] [TZ26] showed that any quantum query to a classical oracle can be efficiently simulated in QPT if the classical oracle's truth table is sampled from a distribution that can be QPT samplable. See Lemma 7.3.

[TZ26] showed that IV-PoQ (even of poly round) that are black-box constructed from a quantumly-secure falsifiable assumption imply OWPuzzs. Corollary 1.10 is stronger than their result in the sense that IV-PoQM are obtained, while it is weaker because it holds only for constant-round IV-PoQ.

2 Preliminaries

2.1 Basic Notations

We use standard notations of quantum computing and cryptography. All polynomials in this paper have coefficients in $\mathbb{N}$. We use λ as the security parameter. For a bit string x, x_i denotes the ith bit of x. For two bit strings x and y, $x\|y$ means the concatenation of them. $[n]$ means the set $\{1, 2, \dots, n\}$. $\lceil x \rceil$ means the minimum integer greater than or equal to x. negl is a negligible function, and poly is a polynomial. PPT stands for (classical) probabilistic polynomial-time and QPT stands for quantum polynomial-time. We refer to a non-uniform QPT algorithm as a QPT algorithm with polynomial-size quantum advice. For a set S, $x \leftarrow S$ means that an element x is chosen from S uniformly at random. For an algorithm $\mathcal{A}$, $y \leftarrow \mathcal{A}(x)$ means that the algorithm $\mathcal{A}$ outputs y on input x. For an algorithm $\mathcal{A}$ that takes a quantum state as input and outputs a quantum state, $\mathcal{A}(\rho)$ often means the output state of $\mathcal{A}$ on input ρ. For two density matrices ρ and σ, $\mathsf{TD}(\rho, \sigma)$ is their trace distance.

For two interactive algorithms $\mathcal{A}$ and $\mathcal{B}$ over a classical channel, $\rho_{\mathbf{A},\mathbf{B}} \leftarrow \langle \mathcal{A}(x), \mathcal{B}(y) \rangle$ means that $\mathcal{A}$ and $\mathcal{B}$ are executed on input x and y, respectively, and the final output state is a quantum state $\rho_{\mathbf{A},\mathbf{B}}$ over two registers $\mathbf{A}$ and $\mathbf{B}$, where $\mathcal{A}$'s output register is $\mathbf{A}$ and $\mathcal{B}$'s output register is $\mathbf{B}$.

2.2 Lemmata

Here we explain two lemmata that we will use later.

Lemma 2.1 ([BZ13], Lemma 1). *Let $\mathcal{A}$ be a quantum algorithm that outputs a classical bit string. Let $\mathcal{A}'$ be another quantum algorithm obtained from $\mathcal{A}$ by pausing $\mathcal{A}$ at an arbitrary stage of the execution, performing a measurement that obtains one of k outcomes, and then resuming $\mathcal{A}$. Then $\Pr[x \leftarrow \mathcal{A}'] \geq \Pr[x \leftarrow \mathcal{A}]/k$ for any bit string x.*

Lemma 2.2 (LOCC Leakage Property for BB84 States [ÇG24], Theorem 10). *Let us consider the following game between a (not-necessarily-polynomial-time) adversary $\mathcal{A}$ and a challenger $\mathcal{C}$:*

1. *$\mathcal{C}$ samples $x, \theta \leftarrow \{0,1\}^\lambda$ and outputs $|R_0\rangle := \bigotimes_{i=1}^{\lambda} H^{\theta_i} |x_i\rangle$. Here, H is the Hadamard operator.*
2. *Let $N : \mathbb{N} \to \mathbb{N}$ be a function. For $i = 1, 2, ..., N(\lambda)$, $\mathcal{A}$ and $\mathcal{C}$ do the following.*
   (a) *$\mathcal{A}$ sends $\mathcal{C}$ a classical description E_i of a (not-necessarily-polynomial-time) quantum algorithm which takes a quantum state as input and outputs a classical bit string and a pure quantum state.*
   (b) *$\mathcal{C}$ runs the algorithm E_i on input $|R_{i-1}\rangle$. Let $(L_i, |R_i\rangle)$ be the output, where L_i is a classical bit string.*
   (c) *$\mathcal{C}$ sends L_i to $\mathcal{A}$.*
3. *$\mathcal{C}$ sends θ to $\mathcal{A}$.*
4. *$\mathcal{A}$ outputs x' and sends it to $\mathcal{C}$.*

5. *$\mathcal{C}$ outputs $\top$ if $x' = x$, and otherwise it outputs $\bot$.*

Then, for all sufficiently large $\lambda \in \mathbb{N}$ and for any (not-necessarily-polynomial-time) adversary $\mathcal{A}$, $\Pr[\top \leftarrow \mathcal{C}] \leq 2^{-\frac{\xi}{2}\cdot\lambda+2^{-\lambda}}$, where $\xi := -\log\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right) > 0.22$.

2.3 Cryptography

In this subsection, we explain several cryptographic primitives that we will use.

First, we recall the definition of proofs of quantumness (PoQ) introduced by [BCM+21].

Definition 2.3 (Proofs of Quantumness (PoQ) [BCM+21]). *An (α, β)-proof of quantumness (PoQ) is a set $(\mathcal{V}, \mathcal{P})$ of interactive algorithms over a classical channel. $\mathcal{V}$ (verifier) is a PPT algorithm that takes 1^λ as input and outputs $\top$ or $\bot$. $\mathcal{P}$ (prover) is a QPT algorithm that takes 1^λ as input and outputs nothing. We require the following two properties.*

α-completeness: *For all sufficiently large $\lambda \in \mathbb{N}$, $\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}(1^\lambda)\rangle\right] \geq \alpha(\lambda)$.*

β-soundness: *For any non-uniform PPT adversary $\mathcal{P}^*$ and for all sufficiently large $\lambda \in \mathbb{N}$, $\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}^*(1^\lambda)\rangle\right] \leq \beta(\lambda)$.*

We say that i.o.-β-soundness is satisfied if the above inequality is satisfied for infinitely many $\lambda \in \mathbb{N}$.

[MY24] introduced the following variant of PoQ, called inefficient-verifier proofs of quantumness (IV-PoQ).

Definition 2.4 (Inefficient-Verifier Proofs of Quantumness (IV-PoQ) [MY24]). *An (α, β)-inefficient-verifier proof of quantumness (IV-PoQ) is an (α, β)-PoQ in which the verifier's final computation to make the decision can be unbounded.*

We also consider another variant of PoQ where the verifier is QPT:

Definition 2.5 (Quantum-Verifier Proofs of Quantumness (QV-PoQ)). *An (α, β)-quantum-verifier proof of quantumness (QV-PoQ) is an (α, β)-PoQ with a QPT verifier. (Note that the communication between the verifier and the prover is still classical.)*

Next, we give the definition of state puzzles (StatePuzzs).

Definition 2.6 (State Puzzles [KT25]). *Let $\epsilon : \mathbb{N} \to [0, 1]$ be a function. An ϵ-StatePuzz is a QPT algorithm Samp that takes 1^λ as input and outputs a pair $(s, |\psi_s\rangle)$ of a bit string s and a pure quantum state $|\psi_s\rangle$ satisfying the following property.*

Security: *For any non-uniform QPT adversary $\mathcal{A}$ that takes s as input and outputs a quantum state, and for all sufficiently large $\lambda \in \mathbb{N}$, $\mathop{\mathbb{E}}_{(s,|\psi_s\rangle)\leftarrow\mathsf{Samp}(1^\lambda)} \langle\psi_s|\mathcal{A}(s)|\psi_s\rangle \leq 1 - \epsilon(\lambda)$. If $\epsilon(\lambda) = 1 - \mathsf{negl}(\lambda)$, we just call it a state puzzle.*

The following lemma is implicitly shown in [KT25].

Lemma 2.7. *Let p be any polynomial. If $1/p$-StatePuzzs exist, then StatePuzzs exist.*

We also define 1-of-2^k puzzles [LLQ22].

Definition 2.8 (1-of-2^k puzzles [LLQ22]). *Let k be a polynomial. A 1-of-2^k puzzle is a set* $(\mathsf{KeyGen}, \mathsf{Obligate}, \mathsf{Solve}, \mathsf{Ver})$ *of algorithms with the following syntax.*

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$: *A PPT algorithm that takes 1^λ as input and outputs a public key* pk *and a secret key* sk.
- $\mathsf{Obligate}(\mathsf{pk}) \to (y, \rho)$: *A QPT algorithm that takes* pk *as input and outputs a bit string y and a quantum state ρ.*
- $\mathsf{Solve}(\mathsf{pk}, y, \rho, \mathsf{ch}) \to \mathsf{ans}$: *A QPT algorithm that takes* pk, y, ρ *and a challenge k-bit string* ch *as input and outputs a classical answer* ans.
- $\mathsf{Ver}(\mathsf{sk}, y, \mathsf{ch}, \mathsf{ans}) \to \top/\bot$: *A polynomial-time classical deterministic algorithm that takes* $\mathsf{sk}, y, \mathsf{ch}$ *and* ans *as input and outputs $\top$ or $\bot$.*

We require the following properties.

Completeness:

$$\Pr\left[\top \leftarrow \mathsf{Ver}(\mathsf{sk}, y, \mathsf{ch}, \mathsf{ans}) : \begin{array}{l}(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)\\ (y, \rho) \leftarrow \mathsf{Obligate}(\mathsf{pk})\\ \mathsf{ch} \leftarrow \{0,1\}^{k(\lambda)}\\ \mathsf{ans} \leftarrow \mathsf{Solve}(\mathsf{pk}, y, \rho, \mathsf{ch})\end{array}\right] \geq 1 - \mathsf{negl}(\lambda). \tag{5}$$

c-soundness: *Let us consider the following game between a set $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ of adversaries and a challenger* Chal*:*

1. Chal *runs* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$.
2. *$\mathcal{A}$ receives the public key* pk*, and outputs a bit string y and a quantum state $\sigma_{\mathbf{BC}}$ over two registers $\mathbf{B}$ and $\mathbf{C}$.*
3. *$\mathcal{A}$ sends y to* Chal*. $\mathcal{A}$ sends $\mathcal{B}$ the register $\mathbf{B}$. $\mathcal{A}$ sends $\mathcal{C}$ the register $\mathbf{C}$.*
4. Chal *samples* $\mathsf{ch} \leftarrow \{0,1\}^{k(\lambda)}$ *and sends* ch *to both $\mathcal{B}$ and $\mathcal{C}$.*
5. *$\mathcal{B}$ outputs an answer* $\mathsf{ans}_\mathcal{B}$ *and sends it to* Chal*. $\mathcal{C}$ outputs an answer* $\mathsf{ans}_\mathcal{C}$ *and sends it to* Chal.
6. Chal *outputs $\top$ if* $\mathsf{Ver}(\mathsf{sk}, y, \mathsf{ch}, \mathsf{ans}_\mathcal{B}) = \top \wedge \mathsf{Ver}(\mathsf{sk}, y, \mathsf{ch}, \mathsf{ans}_\mathcal{C}) = \top$*. Otherwise,* Chal *outputs $\bot$.*

For any set $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ of non-uniform QPT adversaries,

$$\Pr[\top \leftarrow \mathsf{Chal}] \leq 2^{-k(\lambda)} + \mathsf{negl}(2^{\lambda^c}). \tag{6}$$

The following lemma is implicitly shown in [LLQ22].[23]

[23] [LLQ22] implicitly showed that, for any $c > 0$, assuming c-subexponential hardness of LWE, 1-of-2^k puzzles with c-soundness exist. c-subexponential hardness of LWE roughly means that any quantum algorithm running in time $O(2^{\lambda^c})$ can distinguish two distributions with probability at most $\mathsf{negl}(2^{\lambda^c})$. Let $c' > 0$ be any constant. By replacing the security parameter λ with $\lambda' := \lambda^{\frac{c}{c'}}$, c'-subexponential hardness of LWE can be converted to c-subexponential hardness of LWE. Thus, for any $c, c' > 0$, assuming c'-subexponential hardness of LWE, 1-of-2^k puzzles with c-soundness exist.

Lemma 2.9. *Assuming the subexponential hardness of LWE, for any $c > 0$ and for any polynomial k, 1-of-2^k puzzles with c-soundness exist.*

We also use verifiable remote state preparations [GV19, Zha25]. In this paper, we use the formalism of [Zha25].

Definition 2.10 (Remote State Preparations (RSPs) [Zha25]). *Let $n : \mathbb{N} \to \mathbb{N}$ be any polynomially bounded function. Let p be polynomial. An $(n, \frac{1}{p})$-remote state preparation (RSP) is a set $(\mathcal{V}, \mathcal{P})$ of interactive algorithms over a classical channel. $\mathcal{V}$ is a PPT algorithm that takes 1^λ as input and outputs classical bit strings $(x, \theta) \in \{0,1\}^n \times \{0,1\}^n$ and $\mathsf{flag} \in \{\mathsf{pass}, \mathsf{fail}\}$. $\mathcal{P}$ is a QPT algorithm that takes 1^λ as input and outputs a quantum state on the register $\mathbf{Q}$. We require the following two properties.*

Completeness:

$$\mathsf{TD}(\phi_{\mathbf{F},\mathbf{D},\mathbf{Q}}, |\mathsf{pass}\rangle\langle\mathsf{pass}|_{\mathbf{F}} \otimes \eta_{\mathbf{D},\mathbf{Q}}) \leq \mathsf{negl}(\lambda). \tag{7}$$

Here, for the notational simplicity, we consider that $\mathcal{V}$'s classical outputs are encoded in a quantum state in the computational basis. $\mathcal{V}$'s classical output flag *is written in the register $\mathbf{F}$, and (x, θ) is written in the register $\mathbf{D}$. $\phi_{\mathbf{F},\mathbf{D},\mathbf{Q}} \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}(1^\lambda)\rangle$ and $\eta_{\mathbf{D},\mathbf{Q}} := \frac{1}{4^n}\sum_{(x,\theta)\in\{0,1\}^n\times\{0,1\}^n} |x,\theta\rangle\langle x,\theta|_{\mathbf{D}} \otimes (\bigotimes_{i=1}^n H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i})_{\mathbf{Q}}$.*

$\frac{1}{p}$-soundness: *For any non-uniform QPT adversary $\mathcal{P}^*$ that outputs a quantum state on a register $\mathbf{Q}'$, there exists a non-uniform QPT algorithm* Sim *that maps a quantum state on the register $\mathbf{Q}$ to a quantum state on the registers $\mathbf{F}$ and $\mathbf{Q}'$ such that for any non-uniform QPT algorithm $\mathcal{D}$,*

$$\left|\mathrm{Tr}\left[\Pi^{\mathsf{pass}}_{\mathbf{F}}\sigma_{\mathbf{F},\mathbf{D},\mathbf{Q}'}\right]\Pr\left[\top \leftarrow \mathcal{D}\left(\frac{\Pi^{\mathsf{pass}}_{\mathbf{F}}\sigma_{\mathbf{F},\mathbf{D},\mathbf{Q}'}\Pi^{\mathsf{pass}}_{\mathbf{F}}}{\mathrm{Tr}\left[\Pi^{\mathsf{pass}}_{\mathbf{F}}\sigma_{\mathbf{F},\mathbf{D},\mathbf{Q}'}\right]}\right)\right]\right. \tag{8}$$

$$\left. - \mathrm{Tr}\left[\Pi^{\mathsf{pass}}_{\mathbf{F}}\mathsf{Sim}(\eta_{\mathbf{D},\mathbf{Q}})\right]\Pr\left[\top \leftarrow \mathcal{D}\left(\frac{\Pi^{\mathsf{pass}}_{\mathbf{F}}\mathsf{Sim}(\eta_{\mathbf{D},\mathbf{Q}})\Pi^{\mathsf{pass}}_{\mathbf{F}}}{\mathrm{Tr}\left[\Pi^{\mathsf{pass}}_{\mathbf{F}}\mathsf{Sim}(\eta_{\mathbf{D},\mathbf{Q}})\right]}\right)\right]\right| \leq \frac{1}{p(\lambda)}. \tag{9}$$

Here, $\Pi^{\mathsf{pass}}_{\mathbf{F}} := |\mathsf{pass}\rangle\langle\mathsf{pass}|_{\mathbf{F}}$ and $\sigma_{\mathbf{F},\mathbf{D},\mathbf{Q}'} \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}^*(1^\lambda)\rangle$.

The following lemma is shown in [Zha25]:

Lemma 2.11. *Assuming the polynomial hardness of LWE, for any polynomially bounded function $n : \mathbb{N} \to \mathbb{N}$ and polynomial p, r-round $(n, \frac{1}{p})$-RSPs exist with a certain polynomial r.*

Finally, we explain quantum computation and classical communication key exchange (QCCC KE).

Definition 2.12 (QCCC Key Exchange (QCCC KE) [GMMY24]). *An (α, β)-QCCC key exchange (KE) is a set $(\mathcal{A}, \mathcal{B})$ of interactive algorithms over a classical channel. $\mathcal{A}$ ($\mathcal{B}$) is a QPT algorithm that takes 1^λ as input and outputs a bit string a (b). We require the following properties.*

α-correctness: *For all sufficiently large $\lambda \in \mathbb{N}$,*

$$\Pr\left[a = b : (a, b) \leftarrow \langle \mathcal{A}(1^\lambda), \mathcal{B}(1^\lambda)\rangle\right] \geq \alpha(\lambda). \tag{10}$$

Here, $(a, b) \leftarrow \langle \mathcal{A}(1^\lambda), \mathcal{B}(1^\lambda)\rangle$ means that $\mathcal{A}$'s output is a and $\mathcal{B}$'s output is b.

β-security: *For any non-uniform QPT adversary $\mathcal{E}$ and for all sufficiently large $\lambda \in \mathbb{N}$,*

$$\Pr\Big[a = e : (a, b; \tau) \leftarrow \langle \mathcal{A}(1^\lambda), \mathcal{B}(1^\lambda)\rangle, e \leftarrow \mathcal{E}(\tau)\Big] \leq \beta(\lambda). \tag{11}$$

Here, $(a, b; \tau) \leftarrow \langle \mathcal{A}(1^\lambda), \mathcal{B}(1^\lambda)\rangle$ means that $\mathcal{A}$'s output is a, $\mathcal{B}$'s output is b, and τ is the transcript.
If $(\mathcal{A}, \mathcal{B})$ is a $(1 - \mathsf{negl}, \mathsf{negl})$-QCCC KE, then we simply say that $(\mathcal{A}, \mathcal{B})$ is a QCCC KE.

We use the following security amplification lemma.

Lemma 2.13. *Let p be any polynomial. If $(1 - \mathsf{negl}, 1 - \frac{1}{p})$-QCCC KE exist, then QCCC KE exist.*

The proof is given in Appendix B.

3 Proofs of Quantum Memory

In this section, we define proofs of quantum memory (PoQM). We also observe that PoQM generalize the notion of PoQ.

3.1 Definition

We first define PoQM as follows.

Definition 3.1 (Proofs of Quantum Memory (PoQM)). *Let $\alpha, \beta : \mathbb{N} \to [0, 1]$ be any functions. Let $m_1, m_2 : \mathbb{N} \to \mathbb{N}$ be any functions such that $m_1 > m_2$. An $(\alpha, \beta, m_1, m_2)$-proof of quantum memory ($(\alpha, \beta, m_1, m_2)$-PoQM) is a set $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$ of interactive algorithms over a classical channel with the following syntax.*

Initialization Phase: *In the initialization phase, $\mathcal{V}_1$ and $\mathcal{P}_1$ interact over a classical channel. $\mathcal{V}_1$ is a PPT algorithm that takes 1^λ as input and outputs a bit string v. $\mathcal{P}_1$ is a QPT algorithm that takes 1^λ as input and outputs a bit string state and an m_1-qubit quantum state σ_{state}. In other words,*

$$(v, (\mathsf{state}, \sigma_{\mathsf{state}})) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle. \tag{12}$$

Execution Phase: *In the execution phase, $\mathcal{V}_2$ and $\mathcal{P}_2$ interact over a classical channel. $\mathcal{V}_2$ is a PPT algorithm that takes v as input and outputs $\top$ or $\bot$. $\mathcal{P}_2$ is a QPT algorithm that takes state and σ_{state} as input and outputs nothing. In other words,*

$$\top/\bot \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}_2(\mathsf{state}, \sigma_{\mathsf{state}})\rangle. \tag{13}$$

We require the following two properties.

α-completeness: *For all sufficiently large $\lambda \in \mathbb{N}$,*

$$\Pr\Big[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}_2(\mathsf{state}, \sigma_{\mathsf{state}})\rangle : (v, (\mathsf{state}, \sigma_{\mathsf{state}})) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle\Big] \geq \alpha(\lambda). \tag{14}$$

(β, m_2)**-soundness:** *For any non-uniform QPT adversary $\mathcal{P}_1^*$ that outputs a bit string s and an m_2-qubit quantum state ρ, for any non-uniform [24] QPT adversary $\mathcal{P}_2^*$ that takes s and ρ as input, and for all sufficiently large $\lambda \in \mathbb{N}$,*

$$\Pr\left[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}_2^*(s,\rho)\rangle : (v,(s,\rho)) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1^*(1^\lambda)\rangle\right] \leq \beta(\lambda). \tag{15}$$

We say that i.o.-(β, m_2)-soundness is satisfied if the above inequality is satisfied for infinitely-many $\lambda \in \mathbb{N}$.

We also introduce inefficient-verifier proofs of quantum memory (IV-PoQM), which is a variant of PoQM.

Definition 3.2 (Inefficient-Verifier Proofs of Quantum Memory (IV-PoQM)). *An $(\alpha, \beta, m_1, m_2)$-inefficient-verifier proof of quantum memory (IV-PoQM) is an $(\alpha, \beta, m_1, m_2)$-PoQM in which the verifier's final computation to make the decision can be unbounded.*

3.2 Amplification of m_2

We show that m_2 can be increased by increasing β.

Lemma 3.3. *Let $\alpha, \beta : \mathbb{N} \to [0,1]$ be any functions. Let $m_1, m_2 : \mathbb{N} \to \mathbb{N}$ be any functions such that $m_1 > m_2$. An $(\alpha, \beta, m_1, 0)$-PoQM is an $(\alpha, 2^{m_2}\beta, m_1, m_2)$-PoQM.*

Proof of Lemma 3.3. Let $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$ be an $(\alpha, \beta, m_1, 0)$-PoQM. We show that this is also an $(\alpha, 2^{m_2}\beta, m_1, m_2)$-PoQM. α-completeness is straightforward. For the sake of contradiction, we assume that the PoQM is not $(2^{m_2}\beta, m_2)$-sound. This means that there exists an adversary $\mathcal{P}_1^{*(m_2)}$ that outputs an m_2-qubit quantum state ρ and a bit string s, and an adversary $\mathcal{P}_2^{*(m_2)}$ that takes ρ and s as input such that

$$\Pr\left[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}_2^{*(m_2)}(s,\rho)\rangle : (v,(s,\rho)) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1^{*(m_2)}(1^\lambda)\rangle\right] > 2^{m_2(\lambda)}\beta(\lambda) \tag{16}$$

for infinitely many $\lambda \in \mathbb{N}$.

From this $(\mathcal{P}_1^{*(m_2)}, \mathcal{P}_2^{*(m_2)})$, we can construct a pair $(\mathcal{P}_1^{*(0)}, \mathcal{P}_2^{*(0)})$ of adversaries that breaks $(\beta, 0)$-soundness as follows.

- $\mathcal{P}_1^{*(0)}$: Run $(s,\rho) \leftarrow \mathcal{P}_1^{*(m_2)}(1^\lambda)$. Measure ρ in the computational basis to get a measurement result $p \in \{0,1\}^{m_2(\lambda)}$. Output $s' \coloneqq (s,p)$.
- $\mathcal{P}_2^{*(0)}$: Get $s' = (s,p)$ as input. Run $\mathcal{P}_2^{*(m_2)}(s, |p\rangle\langle p|)$.

By Lemma 2.1 and Equation (16),

$$\begin{aligned}
&\Pr\left[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}_2^{*(0)}(s')\rangle : (v,s') \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1^{*(0)}(1^\lambda)\rangle\right] &(17)\\
&\geq 2^{-m_2(\lambda)} \Pr\left[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}_2^{*(m_2)}(s,\rho)\rangle : (v,(s,\rho)) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1^{*(m_2)}(1^\lambda)\rangle\right] &(18)\\
&> \beta(\lambda) &(19)
\end{aligned}$$

for infinitely many $\lambda \in \mathbb{N}$. This contradicts $(\beta, 0)$-soundness of the PoQM. □

[24] In our setting, it is more natural that the non-uniform QPT adversary $\mathcal{P}_2^*$ takes only classical advice since we are interested in how much quantum memory the adversary can possess. However, we can construct PoQM with such stronger security, and therefore this only makes our results stronger.

3.3 Relation to PoQ

We can show that PoQ is a special case of PoQM.

Lemma 3.4. *Let $\alpha, \beta : \mathbb{N} \to [0,1]$ be any functions. Let $m_1, m_2 : \mathbb{N} \to \mathbb{N}$ be any functions such that $m_1 > m_2$. If $(\alpha, \beta, m_1, m_2)$-PoQM exist, then (α, β)-PoQ exist.*

Lemma 3.4 is obtained from the following lemma, because an $(\alpha, \beta, m_1, m_2)$-PoQM is trivially an $(\alpha, \beta, m_1, m_2 - 1)$-PoQM for any $m_2 \geq 1$.

Lemma 3.5. *Let $\alpha, \beta : \mathbb{N} \to [0,1]$ be any functions. Let $m_1 : \mathbb{N} \to \mathbb{N}$ be any function. If $(\alpha, \beta, m_1, 0)$-PoQM exist, then (α, β)-PoQ exist.*

Proof of Lemma 3.5. Assume that $(\alpha, \beta, m_1, 0)$-PoQM exist. Let $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$ be an $(\alpha, \beta, m_1, 0)$-PoQM. From it, we construct an (α, β)-PoQ $(\mathcal{V}, \mathcal{P})$ as follows:

1. $\mathcal{V}$ and $\mathcal{P}$ get 1^λ as input.
2. $\mathcal{V}$ and $\mathcal{P}$ interact over a classical channel. $\mathcal{V}$ runs $v \leftarrow \mathcal{V}_1(1^\lambda)$, and $\mathcal{P}$ runs $(\mathsf{state}, \sigma_{\mathsf{state}}) \leftarrow \mathcal{P}_1(1^\lambda)$.
3. $\mathcal{V}$ and $\mathcal{P}$ interact over a classical channel. $\mathcal{V}$ runs $\top/\bot \leftarrow \mathcal{V}_2(v)$, and $\mathcal{P}$ runs $\mathcal{P}_2(\mathsf{state}, \sigma_{\mathsf{state}})$. $\mathcal{V}$ outputs the output of $\mathcal{V}_2(v)$.

α-completeness of thus constructed PoQ is clear. Next we show β-soundness. For the sake of contradiction, we assume that the constructed PoQ is not β-sound. This means that there exists a non-uniform PPT prover $\mathcal{P}^*$ such that

$$\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}^*(1^\lambda)\rangle\right] > \beta(\lambda) \tag{20}$$

for infinitely many $\lambda \in \mathbb{N}$. We divide $\mathcal{P}^*$ into two algorithms $\mathcal{P}_1^*$ and $\mathcal{P}_2^*$ such that $\mathcal{P}_1^*$ interacts with $\mathcal{V}_1$ and $\mathcal{P}_2^*$ interacts with $\mathcal{V}_2$. Because $\mathcal{P}^*$ is a PPT algorithm, $\mathcal{P}_1^*$ outputs only a classical bit string, which we call s, and $\mathcal{P}_2^*$ takes only s as input. We can show that thus constructed $(\mathcal{P}_1^*, \mathcal{P}_2^*)$ breaks $(\beta, 0)$-soundness of the PoQM, because

$$\Pr\left[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}_2^*(s)\rangle : (v,s) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1^*(1^\lambda)\rangle\right] \tag{21}$$

$$= \Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}^*(1^\lambda)\rangle\right] > \beta(\lambda) \tag{22}$$

for infinitely many $\lambda \in \mathbb{N}$. Hence the constructed PoQ is β-sound. □

4 Constructions of PoQM

In this section, we provide two constructions of PoQM. The first construction is from 1-of-2^k puzzles. The second one is from RSPs.

4.1 1-of-2^k Puzzles Imply PoQM

Theorem 4.1. *Let $m_2 : \mathbb{N} \to \mathbb{N}$ be any polynomially-bounded function. Let $c > 0$ be any constant such that $m_2(\lambda) = O(\lambda^c)$. Let k be any polynomial such that $k(\lambda) = \omega(\lambda^c)$. If 1-of-$2^k$ puzzles with c-soundness exist, then, two-round*[25] *$(1 - \mathsf{negl}, \mathsf{negl}, m_1, m_2)$-PoQM exist with some polynomial m_1.*

By combining this theorem with Lemma 2.9, we obtain the following corollary.

Corollary 4.2. *Let $m_2 : \mathbb{N} \to \mathbb{N}$ be any polynomially-bounded function. Assuming the subexponential hardness of LWE, two-round $(1 - \mathsf{negl}, \mathsf{negl}, m_1, m_2)$-PoQM exist with some polynomial m_1.*

Proof of Theorem 4.1. Assume that 1-of-2^k puzzles with c-soundness exist. Let $(\mathsf{KeyGen}, \mathsf{Obligate}, \mathsf{Solve}, \mathsf{Ver})$ be a 1-of-2^k puzzle with c-soundness. We construct a PoQM $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$ as follows:

Initialization Phase:

1. $\mathcal{V}_1$ and $\mathcal{P}_1$ get 1^λ as input.
2. $\mathcal{V}_1$ runs $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$ and sends pk to $\mathcal{P}_1$.
3. $\mathcal{P}_1$ runs $(y, \rho) \leftarrow \mathsf{Obligate}(\mathsf{pk})$ and sends y to $\mathcal{V}_1$. The number of qubits of ρ is $m_1(\lambda)$.
4. $\mathcal{V}_1$ outputs $v := (\mathsf{sk}, y)$. $\mathcal{P}_1$ outputs $(\mathsf{state}, \sigma_{\mathsf{state}}) := ((\mathsf{pk}, y), \rho)$.

Execution Phase:

1. $\mathcal{V}_2$ takes v as input. $\mathcal{P}_2$ takes $(\mathsf{state}, \sigma_{\mathsf{state}})$ as input.
2. $\mathcal{V}_2$ samples $\mathsf{ch} \leftarrow \{0,1\}^{k(\lambda)}$ and sends it to $\mathcal{P}_2$.
3. $\mathcal{P}_2$ runs $\mathsf{ans} \leftarrow \mathsf{Solve}(\mathsf{pk}, y, \rho, \mathsf{ch})$ and sends ans to $\mathcal{V}_2$.
4. $\mathcal{V}_2$ runs $\top/\bot \leftarrow \mathsf{Ver}(\mathsf{sk}, y, \mathsf{ch}, \mathsf{ans})$ and outputs its output.

Our goal is to show that the constructed $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$ is a $(1 - \mathsf{negl}, \mathsf{negl}, m_1, m_2)$-PoQM. We achieve this goal with the following three steps:

1. We show that $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$ is a $(1 - \mathsf{negl}, \epsilon, m_1, 0)$-PoQM, where $\epsilon(\lambda) := (2^{-k(\lambda)} + \mathsf{negl}(2^{\lambda^c}))^{\frac{1}{2}}$.
2. Using Lemma 3.3, a $(1 - \mathsf{negl}, \epsilon, m_1, 0)$-PoQM is a $(1 - \mathsf{negl}, 2^{m_2}\epsilon, m_1, m_2)$-PoQM.
3. We show that $2^{m_2(\lambda)}\epsilon(\lambda) = \mathsf{negl}(\lambda)$.

The second step is straightforward. In the following, we will explain the first and third steps.

[25] In this paper, a single round is a pair of two messages first one is from the verifier to the prover and the second one is from the prover to the verifier.

First step. $(1-\mathsf{negl})$-completeness is straightforward. Let us show $(\epsilon,0)$-soundness. For the sake of contradiction, assume that it is not $(\epsilon,0)$-sound. Then there exists a pair $(\mathcal{P}_1^*,\mathcal{P}_2^*)$ of adversaries such that

$$\epsilon(\lambda) < \Pr\left[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}_2^*(s)\rangle : (v,s) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1^*(1^\lambda)\rangle\right] \tag{23}$$

$$= \Pr\left[\top \leftarrow \mathsf{Ver}(\mathsf{sk}, y, \mathsf{ch}, \mathsf{ans}) : \begin{array}{l}(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)\\ (y,s') \leftarrow \mathcal{P}_1^*(\mathsf{pk})\\ \mathsf{ch} \leftarrow \{0,1\}^{k(\lambda)}\\ \mathsf{ans} \leftarrow \mathcal{P}_2^*(\mathsf{ch}, s')\end{array}\right] \tag{24}$$

for infinitely many $\lambda \in \mathbb{N}$. From this $(\mathcal{P}_1^*,\mathcal{P}_2^*)$, we can construct a set $(\mathcal{A},\mathcal{B},\mathcal{C})$ of adversaries that breaks c-soundness of the 1-of-2^k puzzle as follows:

- $\mathcal{A}$: Run $(y,s') \leftarrow \mathcal{P}_1^*(\mathsf{pk})$. Send y to Chal and send s' to $\mathcal{B}$ and $\mathcal{C}$.
- $\mathcal{B}$: Run $\mathsf{ans}_\mathcal{B} \leftarrow \mathcal{P}_2^*(\mathsf{ch}, s')$ and send $\mathsf{ans}_\mathcal{B}$ to Chal.
- $\mathcal{C}$: Run $\mathsf{ans}_\mathcal{C} \leftarrow \mathcal{P}_2^*(\mathsf{ch}, s')$ and send $\mathsf{ans}_\mathcal{C}$ to Chal.

$(\mathcal{A},\mathcal{B},\mathcal{C})$ can break c-soundness as follows:

$$\Pr[\top \leftarrow \mathsf{Chal}] \tag{25}$$

$$= \Pr\left[\top \leftarrow \mathsf{Ver}(\mathsf{sk}, y, \mathsf{ch}, \mathsf{ans}_\mathcal{B}) \wedge \top \leftarrow \mathsf{Ver}(\mathsf{sk}, y, \mathsf{ch}, \mathsf{ans}_\mathcal{C}) : \begin{array}{l}(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)\\ (y,s') \leftarrow \mathcal{P}_1^*(\mathsf{pk})\\ \mathsf{ch} \leftarrow \{0,1\}^{k(\lambda)}\\ \mathsf{ans}_\mathcal{B} \leftarrow \mathcal{P}_2^*(\mathsf{ch}, s')\\ \mathsf{ans}_\mathcal{C} \leftarrow \mathcal{P}_2^*(\mathsf{ch}, s')\end{array}\right] \tag{26}$$

$$\geq \Pr\left[\top \leftarrow \mathsf{Ver}(\mathsf{sk}, y, \mathsf{ch}, \mathsf{ans}) : \begin{array}{l}(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)\\ (y,s') \leftarrow \mathcal{P}_1^*(\mathsf{pk})\\ \mathsf{ch} \leftarrow \{0,1\}^{k(\lambda)}\\ \mathsf{ans} \leftarrow \mathcal{P}_2^*(\mathsf{ch}, s')\end{array}\right]^2 \tag{27}$$

$$> \epsilon(\lambda)^2 = 2^{-k(\lambda)} + \mathsf{negl}(2^{\lambda^c}) \tag{28}$$

for infinitely many $\lambda \in \mathbb{N}$. The first inequality follows from the Jensen's inequality. Hence, $(\mathcal{A},\mathcal{B},\mathcal{C})$ break c-soundness of the 1-of-2^k puzzle, contradicting the assumption.

Third step. Since $k(\lambda) = \omega(\lambda^c)$, we have $2^{-k(\lambda)} = \mathsf{negl}(2^{\lambda^c})$, and thus $\epsilon(\lambda) = (2^{-k(\lambda)} + \mathsf{negl}(2^{\lambda^c}))^{\frac{1}{2}} = \mathsf{negl}(2^{\lambda^c})$. From $m_2(\lambda) = O(\lambda^c)$, there exists a polynomial p such that $2^{m_2(\lambda)} \leq p(2^{\lambda^c})$ for all sufficiently large $\lambda \in \mathbb{N}$. Hence, we obtain $2^{m_2(\lambda)}\epsilon(\lambda) \leq p(2^{\lambda^c})\mathsf{negl}(2^{\lambda^c}) = \mathsf{negl}(2^{\lambda^c}) = \mathsf{negl}(\lambda)$. □

4.2 RSPs Imply PoQM

Theorem 4.3. *Let p be any polynomial. Let $m_2 : \mathbb{N} \to \mathbb{N}$ be any polynomially-bounded function such that $m_2(\lambda) = \omega(\log(\lambda))$. If $(\lceil 9.1m_2\rceil, \frac{1}{2p})$-RSPs exist, then $(1-\mathsf{negl}, 1/p, \lceil 9.1m_2\rceil, m_2)$-PoQM exist.*

By combining this theorem with Lemma 2.11, we obtain the following corollary.

Corollary 4.4. *Let p be any polynomial. Let $m_2 : \mathbb{N} \to \mathbb{N}$ be any polynomially-bounded function such that $m_2(\lambda) = \omega(\log(\lambda))$. Assuming the polynomial hardness of LWE, r-round $(1 - \mathsf{negl}, 1/p, \lceil 9.1m_2 \rceil, m_2)$-PoQM exist with a certain polynomial r.*

Proof of Theorem 4.3. Assume that $(\lceil 9.1m_2 \rceil, \frac{1}{2p})$-RSPs exist. Let $(\mathcal{V}, \mathcal{P})$ be a $(\lceil 9.1m_2 \rceil, \frac{1}{2p})$-RSP. We construct a $(1 - \mathsf{negl}, 1/p, \lceil 9.1m_2 \rceil, m_2)$-PoQM $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$ as follows:

Initialization Phase:

1. $\mathcal{V}_1$ and $\mathcal{P}_1$ take 1^λ as input.
2. $\mathcal{V}_1$ runs $v \leftarrow \mathcal{V}(1^\lambda)$ where $v \in \{(\mathsf{pass}, x, \theta), \mathsf{fail}\}$ and $\mathcal{P}_1$ runs $\phi \leftarrow \mathcal{P}(1^\lambda)$. Here, x and θ are $\lceil 9.1m_2 \rceil$-bit strings, and ϕ is a $\lceil 9.1m_2 \rceil$-qubit state.
3. $\mathcal{V}_1$'s output is v. $\mathcal{P}_1$'s output is $(\mathsf{state}, \sigma_{\mathsf{state}}) := (1^\lambda, \phi)$.

Execution Phase:

1. $\mathcal{V}_2$ takes $v \in \{(\mathsf{pass}, x, \theta), \mathsf{fail}\}$ as input. $\mathcal{P}_2$ takes $(\mathsf{state}, \sigma_{\mathsf{state}}) = (1^\lambda, \phi)$ as input.
2. If $v = \mathsf{fail}$, then $\mathcal{V}_2$ samples $\theta \leftarrow \{0,1\}^{\lceil 9.1m_2 \rceil}$ and sends it to $\mathcal{P}_2$. If $v = (\mathsf{pass}, x, \theta)$, $\mathcal{V}_2$ sends θ to $\mathcal{P}_2$.
3. For each $i \in [\lceil 9.1m_2 \rceil]$, $\mathcal{P}_2$ measures ith qubit of ϕ in the computational basis if $\theta_i = 0$ or in the Hadamard basis if $\theta_i = 1$. Let x'_i be the measurement result on the ith qubit. $\mathcal{P}_2$ sets $x' := x'_1 \| ... \| x'_{\lceil 9.1m_2 \rceil}$.
4. $\mathcal{P}_2$ sends x' to $\mathcal{V}_2$.
5. If $v = \mathsf{fail}$ or $x \neq x'$, $\mathcal{V}_2$ outputs $\bot$. Otherwise, $\mathcal{V}_2$ outputs $\top$.

Now we show that the constructed $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$ is a $(1 - \mathsf{negl}, 1/p, \lceil 9.1m_2 \rceil, m_2)$-PoQM.

$(1 - \mathsf{negl})$-completeness is straightforward. Let us next show $(1/p, m_2)$-soundness. We define $\mathbf{Hybrid}_0$ as follows, which is the original security game for $(1/p, m_2)$-soundness.

$\mathbf{Hybrid}_0$:

1. $\mathcal{V}_1$ and $\mathcal{P}_1^*$ take 1^λ as input.
2. They run the RSP. $\mathcal{V}_1$ outputs $v \in \{(\mathsf{pass}, x, \theta), \mathsf{fail}\}$. $\mathcal{P}_1^*$ outputs a quantum state $\sigma_{\mathbf{Q}'}$ on the register $\mathbf{Q}'$.
3. $\mathcal{P}_1^*$ runs a certain QPT algorithm E on $\sigma_{\mathbf{Q}'}$ to get (s, ρ), where s is a classical bit string and ρ is an m_2-qubit quantum state: $(s, \rho) \leftarrow E(\sigma_{\mathbf{Q}'})$. $\mathcal{P}_1^*$ outputs (s, ρ).
4. $\mathcal{V}_2$ takes v as input. $\mathcal{P}_2^*$ takes (s, ρ) as input.
5. If $v = \mathsf{fail}$, then $\mathcal{V}_2$ samples $\theta \leftarrow \{0,1\}^{\lceil 9.1m_2 \rceil}$ and sends it to $\mathcal{P}_2^*$. If $v = (\mathsf{pass}, x, \theta)$, $\mathcal{V}_2$ sends θ to $\mathcal{P}_2^*$.
6. $\mathcal{P}_2^*$ sends x' to $\mathcal{V}_2$.
7. If $v = \mathsf{fail}$ or $x \neq x'$, $\mathcal{V}_2$ outputs $\bot$. Otherwise, $\mathcal{V}_2$ outputs $\top$.

Because of $\frac{1}{2p}$-soundness of the RSP (Equation (9)), there exists a non-uniform QPT algorithm Sim. By using it, we define $\mathbf{Hybrid}_1$, which is the same as $\mathbf{Hybrid}_0$ except for the step 2:

$\mathbf{Hybrid}_1$:

2. $\mathcal{V}_1$ samples $(x,\theta) \leftarrow \{0,1\}^{\lceil 9.1m_2\rceil} \times \{0,1\}^{\lceil 9.1m_2\rceil}$ and generates $\mathsf{Sim}(\bigotimes_{i=1}^{\lceil 9.1m_2\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i})$, which consists of two registers $\mathbf{F}$ and $\mathbf{Q}'$. $\mathcal{V}_1$ gets $\mathsf{flag} \in \{\mathsf{pass},\mathsf{fail}\}$ by measuring the register $\mathbf{F}$ and sends the register $\mathbf{Q}'$ of the post-measurement state to $\mathcal{P}_1^*$. $\mathcal{V}_1$ sets $v := \mathsf{fail}$ if $\mathsf{flag} = \mathsf{fail}$. Otherwise, $\mathcal{V}_1$ sets $v := (\mathsf{pass}, x, \theta)$.

Lemma 4.5.

$$|\Pr[\top \leftarrow \mathbf{Hybrid}_0(\lambda)] - \Pr[\top \leftarrow \mathbf{Hybrid}_1(\lambda)]| \leq \frac{1}{2p(\lambda)} \tag{29}$$

for all sufficiently large $\lambda \in \mathbb{N}$.

Proof of Lemma 4.5. For the sake of contradiction, we assume that

$$|\Pr[\top \leftarrow \mathbf{Hybrid}_0(\lambda)] - \Pr[\top \leftarrow \mathbf{Hybrid}_1(\lambda)]| > \frac{1}{2p(\lambda)} \tag{30}$$

for infinitely many $\lambda \in \mathbb{N}$. Then, we can construct a non-uniform QPT algorithm $\mathcal{D}$ that breaks $\frac{1}{2p}$-soundness of $(\lceil 9.1m_2\rceil, \frac{1}{2p})$-RSP as follows:

1. Get a quantum state over registers $\mathbf{F}, \mathbf{D}, \mathbf{Q}'$, where registers are defined as in Definition 2.10.
2. Get $(x,\theta) \in \{0,1\}^{\lceil 9.1m_2\rceil} \times \{0,1\}^{\lceil 9.1m_2\rceil}$ by measuring register $\mathbf{D}$. Set $v = (\mathsf{pass}, x, \theta)$.
3. Run $(s,\rho) \leftarrow E(\xi_{\mathbf{Q}'})$, where E is the algorithm of step 3 of $\mathbf{Hybrid}_0$ and $\xi_{\mathbf{Q}'}$ is the reduced state on the register $\mathbf{Q}'$ of the post-measurement state.
4. Simulate the interaction between $\mathcal{V}_2$ and $\mathcal{P}_2^*$ from the step 4 of $\mathbf{Hybrid}_0$ to the last step.
5. Output $\top$ if $\mathcal{V}_2$ outputs $\top$. Otherwise, output $\bot$.

It is clear that

$$\Pr[\top \leftarrow \mathbf{Hybrid}_0(\lambda)] \tag{31}$$

$$= \mathrm{Tr}\left[\Pi_{\mathbf{F}}^{\mathsf{pass}}\sigma_{\mathbf{F},\mathbf{D},\mathbf{Q}'}\right] \Pr\left[\top \leftarrow \mathcal{D}\left(\frac{\Pi_{\mathbf{F}}^{\mathsf{pass}}\sigma_{\mathbf{F},\mathbf{D},\mathbf{Q}'}\Pi_{\mathbf{F}}^{\mathsf{pass}}}{\mathrm{Tr}\left[\Pi_{\mathbf{F}}^{\mathsf{pass}}\sigma_{\mathbf{F},\mathbf{D},\mathbf{Q}'}\right]}\right)\right], \tag{32}$$

where $\sigma_{\mathbf{F},\mathbf{D},\mathbf{Q}'}$ is the output of $\mathcal{V}_1$ and $\mathcal{P}_1^*$ at step 2 of $\mathbf{Hybrid}_0$, and

$$\Pr[\top \leftarrow \mathbf{Hybrid}_1(\lambda)] \tag{33}$$

$$= \mathrm{Tr}\left[\Pi_{\mathbf{F}}^{\mathsf{pass}}\mathsf{Sim}(\eta_{\mathbf{D},\mathbf{Q}})\right] \Pr\left[\top \leftarrow \mathcal{D}\left(\frac{\Pi_{\mathbf{F}}^{\mathsf{pass}}\mathsf{Sim}(\eta_{\mathbf{D},\mathbf{Q}})\Pi_{\mathbf{F}}^{\mathsf{pass}}}{\mathrm{Tr}\left[\Pi_{\mathbf{F}}^{\mathsf{pass}}\mathsf{Sim}(\eta_{\mathbf{D},\mathbf{Q}})\right]}\right)\right]. \tag{34}$$

By Equation (30),

$$\left|\mathrm{Tr}\left[\Pi_{\mathbf{F}}^{\mathsf{pass}}\sigma_{\mathbf{F},\mathbf{D},\mathbf{Q}'}\right] \Pr\left[\top \leftarrow \mathcal{D}\left(\frac{\Pi_{\mathbf{F}}^{\mathsf{pass}}\sigma_{\mathbf{F},\mathbf{D},\mathbf{Q}'}\Pi_{\mathbf{F}}^{\mathsf{pass}}}{\mathrm{Tr}\left[\Pi_{\mathbf{F}}^{\mathsf{pass}}\sigma_{\mathbf{F},\mathbf{D},\mathbf{Q}'}\right]}\right)\right]\right. \tag{35}$$

$$\left. - \mathrm{Tr}\left[\Pi_{\mathbf{F}}^{\mathsf{pass}}\mathsf{Sim}(\eta_{\mathbf{D},\mathbf{Q}})\right] \Pr\left[\top \leftarrow \mathcal{D}\left(\frac{\Pi_{\mathbf{F}}^{\mathsf{pass}}\mathsf{Sim}(\eta_{\mathbf{D},\mathbf{Q}})\Pi_{\mathbf{F}}^{\mathsf{pass}}}{\mathrm{Tr}\left[\Pi_{\mathbf{F}}^{\mathsf{pass}}\mathsf{Sim}(\eta_{\mathbf{D},\mathbf{Q}})\right]}\right)\right]\right| \tag{36}$$

$$= |\Pr[\top \leftarrow \mathbf{Hybrid}_0(\lambda)] - \Pr[\top \leftarrow \mathbf{Hybrid}_1(\lambda)]| \tag{37}$$

$$> \frac{1}{2p(\lambda)} \tag{38}$$

for infinitely many $\lambda \in \mathbb{N}$. This contradicts $\frac{1}{2p}$-soundness of the RSP. □

Let us define $\mathbf{Hybrid}_2$, which is the same as $\mathbf{Hybrid}_1$ except for the step 2:

$\mathbf{Hybrid}_2$:

2. $\mathcal{V}_1$ samples $(x,\theta) \leftarrow \{0,1\}^{\lceil 9.1m_2\rceil} \times \{0,1\}^{\lceil 9.1m_2\rceil}$, generates $\bigotimes_{i=1}^{\lceil 9.1m_2\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i}$ and sends it to $\mathcal{P}_1^*$. $\mathcal{V}_1$ sets $v := (\mathsf{pass}, x, \theta)$.

As shown below, the acceptance probability of $\mathbf{Hybrid}_2$ is at least that of $\mathbf{Hybrid}_1$.

Lemma 4.6.

$$\Pr[\top \leftarrow \mathbf{Hybrid}_1(\lambda)] \leq \Pr[\top \leftarrow \mathbf{Hybrid}_2(\lambda)] \tag{39}$$

for all $\lambda \in \mathbb{N}$.

Proof of Lemma 4.6. We start by expanding the acceptance probability of $\mathbf{Hybrid}_1$.

$$\Pr[\top \leftarrow \mathbf{Hybrid}_1(\lambda)] \tag{40}$$
$$= \Pr[\mathsf{pass}] \tag{41}$$
$$\times \Pr\left[\top \leftarrow \langle \mathcal{V}_2(\mathsf{pass}, x, \theta), \mathcal{P}_2^*(s,\rho)\rangle : \begin{array}{l}(x,\theta) \leftarrow \{0,1\}^{\lceil 9.1m_2\rceil} \times \{0,1\}^{\lceil 9.1m_2\rceil} \\ (s,\rho) \leftarrow E(\zeta_{\mathbf{Q}'}^{x,\theta})\end{array}\right]. \tag{42}$$

Here, $\zeta_{\mathbf{Q}'}^{x,\theta}$ is the reduced state on register $\mathbf{Q}'$ of

$$\frac{\Pi_{\mathbf{F}}^{\mathsf{pass}}\mathsf{Sim}(\bigotimes_{i=1}^{\lceil 9.1m_2\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i})\Pi_{\mathbf{F}}^{\mathsf{pass}}}{\mathrm{Tr}\left[\Pi_{\mathbf{F}}^{\mathsf{pass}}\mathsf{Sim}(\bigotimes_{i=1}^{\lceil 9.1m_2\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i})\right]}, \tag{43}$$

and

$$\Pr[\mathsf{pass}] = \mathrm{Tr}\left[\Pi_{\mathbf{F}}^{\mathsf{pass}}\mathsf{Sim}(\bigotimes_{i=1}^{\lceil 9.1m_2\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i})\right]. \tag{44}$$

Next, we write down explicitly the acceptance probability of $\mathbf{Hybrid}_2$. Then we bound this probability by considering the special case where $\mathcal{P}_1^*$, as its first step after applying Sim, measures register $\mathbf{F}$, and conditions on the measurement outcome being pass. We further restrict by replacing the state with its reduced version. Since these restrictions can only reduce the acceptance probability, the resulting experiment provides

a lowerbound for $\mathbf{Hybrid}_2$, which coincides exactly with the acceptance probability of $\mathbf{Hybrid}_1$.

$$\Pr[\top \leftarrow \mathbf{Hybrid}_2(\lambda)] \tag{45}$$

$$= \Pr\left[\top \leftarrow \langle \mathcal{V}_2(\mathsf{pass}, x, \theta), \mathcal{P}_2^*(s,\rho)\rangle : \begin{array}{l}(x,\theta) \leftarrow \{0,1\}^{\lceil 9.1m_2\rceil} \times \{0,1\}^{\lceil 9.1m_2\rceil} \\ (s,\rho) \leftarrow E\left(\bigotimes_{i=1}^{\lceil 9.1m_2\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i}\right)\end{array}\right] \tag{46}$$

$$\geq \Pr[\mathsf{pass}] \tag{47}$$

$$\times \Pr\left[\top \leftarrow \langle \mathcal{V}_2(\mathsf{pass}, x, \theta), \mathcal{P}_2^*(s,\rho)\rangle : \begin{array}{l}(x,\theta) \leftarrow \{0,1\}^{\lceil 9.1m_2\rceil} \times \{0,1\}^{\lceil 9.1m_2\rceil} \\ (s,\rho) \leftarrow E\left(\frac{\Pi_{\mathbf{F}}^{\mathsf{pass}}\mathsf{Sim}(\bigotimes_{i=1}^{\lceil 9.1m_2\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i})\Pi_{\mathbf{F}}^{\mathsf{pass}}}{\mathrm{Tr}\left[\Pi_{\mathbf{F}}^{\mathsf{pass}}\mathsf{Sim}(\bigotimes_{i=1}^{\lceil 9.1m_2\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i})\right]}\right)\end{array}\right] \tag{48}$$

$$\geq \Pr[\mathsf{pass}] \tag{49}$$

$$\times \Pr\left[\top \leftarrow \langle \mathcal{V}_2(\mathsf{pass}, x, \theta), \mathcal{P}_2^*(s,\rho)\rangle : \begin{array}{l}(x,\theta) \leftarrow \{0,1\}^{\lceil 9.1m_2\rceil} \times \{0,1\}^{\lceil 9.1m_2\rceil} \\ (s,\rho) \leftarrow E(\zeta_{\mathbf{Q}'}^{x,\theta})\end{array}\right] \tag{50}$$

$$= \Pr[\top \leftarrow \mathbf{Hybrid}_1(\lambda)]. \tag{51}$$

□

We define $\mathbf{Hybrid}_3$, which is the same as $\mathbf{Hybrid}_2$ except for steps 3 and 4:

$\mathbf{Hybrid}_3$:

3. $\mathcal{P}_1^*$ runs a certain QPT algorithm E on $\bigotimes_{i=1}^{\lceil 9.1m_2\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i}$ to get (s,ρ), where s is a classical bit string and ρ is an m_2-qubit quantum state: $(s,\rho) \leftarrow E(\bigotimes_{i=1}^{\lceil 9.1m_2\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i})$. Get a bit string $p \in \{0,1\}^{m_2}$ by measuring ρ in the computational basis. Set $s' := (s,p)$. $\mathcal{P}_1^*$ outputs s'.
4. $\mathcal{V}_2$ takes v as input. $\mathcal{P}_2^*$ takes $s' = (s,p)$ as input, and uses it as $(s, |p\rangle\langle p|)$.

By Lemma 2.1, we can obtain the following lemma.

Lemma 4.7.

$$\Pr[\top \leftarrow \mathbf{Hybrid}_2(\lambda)] \leq 2^{m_2(\lambda)} \Pr[\top \leftarrow \mathbf{Hybrid}_3(\lambda)] \tag{52}$$

for all $\lambda \in \mathbb{N}$.

To conclude the theorem, we show the following lemma.

Lemma 4.8. *For all sufficiently large* $\lambda \in \mathbb{N}$,

$$\Pr[\top \leftarrow \mathbf{Hybrid}_3(\lambda)] \leq 2^{-\frac{\xi}{2}\cdot\lceil 9.1m_2(\lambda)\rceil + 2^{-\lceil 9.1m_2(\lambda)\rceil}}. \tag{53}$$

Here, $\xi = -\log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) > 0.22$.

Proof of Lemma 4.8. For the sake of contradiction, we assume that there exists a pair $(\mathcal{P}_1^*, \mathcal{P}_2^*)$ of adversaries such that

$$2^{-\frac{\xi}{2}\cdot\lceil 9.1m_2(\lambda)\rceil + 2^{-\lceil 9.1m_2(\lambda)\rceil}} < \Pr[\top \leftarrow \mathbf{Hybrid}_3(\lambda)] \tag{54}$$

$$= \Pr\left[x = x' : \begin{array}{l}(x,\theta) \leftarrow \{0,1\}^{\lceil 9.1m_2(\lambda)\rceil} \times \{0,1\}^{\lceil 9.1m_2(\lambda)\rceil} \\ (s,p) \leftarrow \mathcal{P}_1^*(\bigotimes_{i=1}^{\lceil 9.1m_2(\lambda)\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i}) \\ x' \leftarrow \mathcal{P}_2^*(\theta, s, |p\rangle\langle p|)\end{array}\right] \tag{55}$$

for infinitely many $\lambda \in \mathbb{N}$. From this $(\mathcal{P}_1^*, \mathcal{P}_2^*)$, we can construct a non-uniform QPT adversary $\mathcal{A}$ that breaks Lemma 2.2 as follows:

1. Send the classical description of $\mathcal{P}_1^*$ to $\mathcal{C}$.
2. $\mathcal{C}$ runs $(s,p) \leftarrow \mathcal{P}_1^*(\bigotimes_{i=1}^{\lceil 9.1m_2(\lambda)\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i})$ and returns (s,p) to $\mathcal{A}$.
3. Receive θ from $\mathcal{C}$, run $x' \leftarrow \mathcal{P}_2^*(\theta, s, |p\rangle\langle p|)$ and send x' to $\mathcal{C}$.

Then, for infinitely many $\lambda \in \mathbb{N}$,

$$\begin{aligned}\Pr[\top \leftarrow \mathcal{C}] &= \Pr\left[x = x' : \begin{array}{l}(x,\theta) \leftarrow \{0,1\}^{\lceil 9.1m_2(\lambda)\rceil} \times \{0,1\}^{\lceil 9.1m_2(\lambda)\rceil} \\ (s,p) \leftarrow \mathcal{P}_1^*(\bigotimes_{i=1}^{\lceil 9.1m_2(\lambda)\rceil} H^{\theta_i}|x_i\rangle\langle x_i|H^{\theta_i}) \\ x' \leftarrow \mathcal{P}_2^*(\theta, s, |p\rangle\langle p|)\end{array}\right] && (56)\\ &= \Pr[\top \leftarrow \mathbf{Hybrid}_3(\lambda)] && (57)\\ &> 2^{-\frac{\xi}{2}\cdot\lceil 9.1m_2(\lambda)\rceil + 2^{-\lceil 9.1m_2(\lambda)\rceil}}. && (58)\end{aligned}$$

This contradicts Lemma 2.2. □

By combining Lemmata 4.5 to 4.8, we have

$$\Pr[\top \leftarrow \mathbf{Hybrid}_0(\lambda)] < \frac{1}{2p(\lambda)} + \mathsf{negl}(\lambda) < \frac{1}{p(\lambda)} \tag{59}$$

for all sufficiently large $\lambda \in \mathbb{N}$. □

5 Lowerbounds of (IV-)PoQM

In this section, we show that IV-PoQM imply StatePuzzs (and therefore OWPuzzs). We also show that predictable PoQM imply QCCC KE.

5.1 IV-PoQM imply StatePuzzs

We first show that IV-PoQM imply StatePuzzs.

Theorem 5.1. *Let $\alpha, \beta : \mathbb{N} \to [0,1]$ be any functions such that $\alpha(\lambda) - \beta(\lambda) \geq 1/\mathrm{poly}(\lambda)$ for all sufficiently large $\lambda \in \mathbb{N}$. Let $m_1 : \mathbb{N} \to \mathbb{N}$ be any function. If $(\alpha, \beta, m_1, 0)$-IV-PoQM exist, then StatePuzzs exist.*

Proof of Theorem 5.1. Let $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$ be an $(\alpha, \beta, m_1, 0)$-IV-PoQM. The final state before the measurement of $\mathcal{P}_1$ is written as $\sum_{\mathsf{state}} c_{\mathsf{state}}|\phi_{\mathsf{state}}\rangle|\mathsf{state}\rangle$ with some complex coefficients $\{c_{\mathsf{state}}\}$, where $|\phi_{\mathsf{state}}\rangle$ is a pure m_1'-qubit state. $\mathcal{P}_1$ measures the second register to get the result state. $\mathcal{P}_1$ outputs $(\mathsf{state}, \sigma_{\mathsf{state}})$, where σ_{state} is the first m_1 qubits of $|\phi_{\mathsf{state}}\rangle$.

From $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$, we construct an $(\alpha, \beta, m_1', 0)$-IV-PoQM $(\mathcal{V}_1, \mathcal{P}_1', \mathcal{V}_2, \mathcal{P}_2')$ as follows:

1. $\mathcal{P}_1'$ runs $\mathcal{P}_1$ to generate $\sum_{\mathsf{state}} c_{\mathsf{state}}|\phi_{\mathsf{state}}\rangle|\mathsf{state}\rangle$, measures the second register, and outputs $(\mathsf{state}, |\phi_{\mathsf{state}}\rangle)$.
2. $\mathcal{P}_2'$ takes $(\mathsf{state}, |\phi_{\mathsf{state}}\rangle)$ as input, and runs $\mathcal{P}_2(\mathsf{state}, \sigma_{\mathsf{state}})$, where σ_{state} is the first m_1 qubits of $|\phi_{\mathsf{state}}\rangle$.

From $(\mathcal{V}_1, \mathcal{P}'_1, \mathcal{V}_2, \mathcal{P}'_2)$, we construct a StatePuzz, Samp, as follows:

1. Take 1^λ as input.
2. Run $(v, (\mathsf{state}, |\phi_{\mathsf{state}}\rangle)) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}'_1(1^\lambda)\rangle$. Let τ be the transcript.
3. Output $s := (\mathsf{state}, \tau)$ and $|\psi_s\rangle := |\phi_{\mathsf{state}}\rangle$.

Now we show that thus constructed Samp is a $1/p$-StatePuzz with a certain polynomial p. From Lemma 2.7, such a $1/p$-StatePuzz can be amplified to obtain a StatePuzz.

Let p be a polynomial such that $p(\lambda) > (\alpha(\lambda) - \beta(\lambda))^{-2}$ for all sufficiently large $\lambda \in \mathbb{N}$. For the sake of contradiction, we assume that Samp is not a $1/p$-StatePuzz. Then there exists a non-uniform QPT algorithm $\mathcal{A}$ such that for infinitely many $\lambda \in \mathbb{N}$,

$$\mathop{\mathbb{E}}_{(s,|\psi_s\rangle)\leftarrow\mathsf{Samp}(1^\lambda)} \langle\psi_s|\mathcal{A}(s)|\psi_s\rangle > 1 - \frac{1}{p(\lambda)}. \tag{60}$$

From this $\mathcal{A}$, we construct a pair $(\mathcal{P}^*_1, \mathcal{P}^*_2)$ of adversaries that breaks $(\beta, 0)$-soundness of the IV-PoQM as follows:

- $\mathcal{P}^*_1$: Run $(\mathsf{state}, |\phi_{\mathsf{state}}\rangle) \leftarrow \mathcal{P}'_1(1^\lambda)$. Let τ be the transcript. Output (state, τ).
- $\mathcal{P}^*_2$: Run $\mathcal{A}(\mathsf{state}, \tau)$. Run $\mathcal{P}'_2(\mathsf{state}, \mathcal{A}(\mathsf{state}, \tau))$.

$(\mathcal{P}^*_1, \mathcal{P}^*_2)$ can break $(\beta, 0)$-soundness of the IV-PoQM as follows.

$$\Pr\left[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}^*_2(\mathsf{state}, \tau)\rangle : (v, (\mathsf{state}, \tau)) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}^*_1(1^\lambda)\rangle\right] \tag{61}$$

$$= \Pr\left[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}'_2(\mathsf{state}, \mathcal{A}(\mathsf{state}, \tau))\rangle : (v, (\mathsf{state}, |\phi_{\mathsf{state}}\rangle)) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}'_1(1^\lambda)\rangle\right] \tag{62}$$

$$\geq \Pr\left[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}'_2(\mathsf{state}, |\phi_{\mathsf{state}}\rangle)\rangle : (v, (\mathsf{state}, |\phi_{\mathsf{state}}\rangle)) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}'_1(1^\lambda)\rangle\right] \tag{63}$$

$$- \mathop{\mathbb{E}}_{((\mathsf{state},\tau),|\phi_{\mathsf{state}}\rangle)\leftarrow\mathsf{Samp}(1^\lambda)} \mathsf{TD}(|\phi_{\mathsf{state}}\rangle, \mathcal{A}(\mathsf{state}, \tau)) \tag{64}$$

$$\geq \alpha(\lambda) - \mathop{\mathbb{E}}_{((\mathsf{state},\tau),|\phi_{\mathsf{state}}\rangle)\leftarrow\mathsf{Samp}(1^\lambda)} \sqrt{1 - \langle\phi_{\mathsf{state}}|\mathcal{A}(\mathsf{state}, \tau)|\phi_{\mathsf{state}}\rangle} \tag{65}$$

for all sufficiently large $\lambda \in \mathbb{N}$. By Jensen's inequality and Equation (60),

$$\mathop{\mathbb{E}}_{((\mathsf{state},\tau),|\phi_{\mathsf{state}}\rangle)\leftarrow\mathsf{Samp}(1^\lambda)} \sqrt{1 - \langle\phi_{\mathsf{state}}|\mathcal{A}(\mathsf{state}, \tau)|\phi_{\mathsf{state}}\rangle} \tag{66}$$

$$\leq \sqrt{1 - \mathop{\mathbb{E}}_{((\mathsf{state},\tau),|\phi_{\mathsf{state}}\rangle)\leftarrow\mathsf{Samp}(1^\lambda)} \langle\phi_{\mathsf{state}}|\mathcal{A}(\mathsf{state}, \tau)|\phi_{\mathsf{state}}\rangle} \tag{67}$$

$$< \frac{1}{p(\lambda)^{\frac{1}{2}}} \tag{68}$$

for infinitely many $\lambda \in \mathbb{N}$. Therefore,

$$\Pr\left[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}^*_2(\mathsf{state}, \tau)\rangle : (v, (\mathsf{state}, \tau)) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}^*_1(1^\lambda)\rangle\right] \tag{69}$$

$$> \alpha(\lambda) - \frac{1}{p(\lambda)^{\frac{1}{2}}} \tag{70}$$

$$> \beta(\lambda) \tag{71}$$

for infinitely many $\lambda \in \mathbb{N}$. This contradicts $(\beta, 0)$-soundness of the IV-PoQM. □

5.2 Predictable PoQM Imply QCCC KE

We next show that a restricted version of PoQM, which we call predictable PoQM, implies QCCC KE.

Predictable PoQM are defined as follows.

Definition 5.2 (Predictable PoQM). *We call an $(\alpha, \beta, m_1, m_2)$-PoQM an $(\alpha, \beta, m_1, m_2)$-predictable PoQM if the execution phase is of a single round, and has the following specific form:*

1. *$\mathcal{V}_2$ takes v as input, where v is the output of $\mathcal{V}_1$.*
2. *$\mathcal{P}_2$ takes $(\mathsf{state}, \sigma_{\mathsf{state}})$ as input, where $(\mathsf{state}, \sigma_{\mathsf{state}})$ is the output of $\mathcal{P}_1$.*
3. *$\mathcal{V}_2$ sends a bit string x to $\mathcal{P}_2$.*
4. *$\mathcal{P}_2$ sends a bit string y to $\mathcal{V}_2$.*
5. *$\mathcal{V}_2$ computes y' from v and x. If $y = y'$, $\mathcal{V}_2$ outputs $\top$. If $y \neq y'$, $\mathcal{V}_2$ outputs $\bot$.*

The construction of PoQM from RSPs in Section 4.2 realizes the predictable PoQM. Thus, we obtain the following lemma.

Lemma 5.3. *Let p be any polynomial. Let m_2 be any polynomially bounded function such that $m_2(\lambda) = \omega(\log(\lambda))$. Assuming the polynomial hardness of LWE, r-round $(1 - \mathsf{negl}, 1/p, \lceil 9.1 m_2 \rceil, m_2)$-predictable PoQM exist with a certain polynomial r.*

We show that predictable PoQM imply QCCC KE.

Theorem 5.4. *Let $m_1 : \mathbb{N} \to \mathbb{N}$ be any function. Let p be any polynomial. If $(1-\mathsf{negl}, 1-\frac{1}{p}, m_1, 0)$-predictable PoQM exist, then QCCC KE exist.*

Proof of Theorem 5.4. Let $(\mathcal{V}_1, \mathcal{P}_1, \mathcal{V}_2, \mathcal{P}_2)$ be an $(1 - \mathsf{negl}, 1 - \frac{1}{p}, m_1, 0)$-predictable PoQM. From it, we construct a QCCC KE $(\mathcal{A}, \mathcal{B})$ as follows:

1. $\mathcal{A}$ and $\mathcal{B}$ take 1^λ as input.
2. $\mathcal{A}$ runs $\mathcal{P}_1(1^\lambda)$, and $\mathcal{B}$ runs $\mathcal{V}_1(1^\lambda)$. Let $(\mathsf{state}, \sigma_{\mathsf{state}})$ be $\mathcal{P}_1$'s output. Let v be $\mathcal{V}_1$'s output.
3. $\mathcal{B}$ runs $x \leftarrow \mathcal{V}_2(v)$ and sends x to $\mathcal{A}$.
4. $\mathcal{A}$ runs $y \leftarrow \mathcal{P}_2(\mathsf{state}, \sigma_{\mathsf{state}}, x)$, but does not send y to $\mathcal{B}$.
5. $\mathcal{B}$ runs $y' \leftarrow \mathcal{V}_2(v, x)$.
6. $\mathcal{A}$ outputs $a := y$, and $\mathcal{B}$ outputs $b := y'$.

Now we show that thus constructed $(\mathcal{A}, \mathcal{B})$ is a $(1 - \mathsf{negl}, 1 - \frac{1}{2p})$-QCCC KE. From Lemma 2.13, such a $(1 - \mathsf{negl}, 1 - \frac{1}{2p})$-QCCC KE can be amplified to obtain a QCCC KE.

$(1 - \mathsf{negl})$-correctness is clear from $(1 - \mathsf{negl})$-completeness of predictable PoQM. Next, we show $(1 - \frac{1}{2p})$-security. For the sake of contradiction, we assume that $(\mathcal{A}, \mathcal{B})$ is not $(1 - \frac{1}{2p})$-secure. This means that there exists a non-uniform QPT adversary $\mathcal{E}$ such that

$$\Pr\left[y \leftarrow \mathcal{E}(\tau, x) : \begin{array}{l}(v, (\mathsf{state}, \sigma_{\mathsf{state}}); \tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle \\ x \leftarrow \mathcal{V}_2(v) \\ y \leftarrow \mathcal{P}_2(\mathsf{state}, \sigma_{\mathsf{state}}, x)\end{array}\right] > 1 - \frac{1}{2p(\lambda)} \tag{72}$$

for infinitely many $\lambda \in \mathbb{N}$. Here, $(v, (\mathsf{state}, \sigma_{\mathsf{state}}); \tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle$ means that $\mathcal{V}_1$'s output is v, $\mathcal{P}_1$'s output is $(\mathsf{state}, \sigma_{\mathsf{state}})$, and τ is the transcript. From this $\mathcal{E}$, we can construct a pair $(\mathcal{P}_1^*, \mathcal{P}_2^*)$ of adversaries that breaks $(1 - \frac{1}{p}, 0)$-soundness of the predictable PoQM as follows:

- $\mathcal{P}_1^*$: Run $(\mathsf{state}, \sigma_{\mathsf{state}}) \leftarrow \mathcal{P}_1(1^\lambda)$. Let τ be the transcript. Output τ.
- $\mathcal{P}_2^*$: Take τ and x as input, and run $e \leftarrow \mathcal{E}(\tau, x)$. Send e to $\mathcal{V}_2$.

$(\mathcal{P}_1^*, \mathcal{P}_2^*)$ breaks $(1 - \frac{1}{p}, 0)$-soundness as follows:

$$\Pr\left[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}_2^*(\tau)\rangle : (v, \tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1^*(1^\lambda)\rangle\right] \tag{73}$$

$$= \Pr\left[\top \leftarrow \mathcal{V}_2(v, x, e) : \begin{array}{l}(v, (\mathsf{state}, \sigma_{\mathsf{state}}); \tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle \\ x \leftarrow \mathcal{V}_2(v) \\ e \leftarrow \mathcal{E}(\tau, x)\end{array}\right] \tag{74}$$

$$= \Pr\left[\top \leftarrow \mathcal{V}_2(v, x, e) : \begin{array}{l}(v, (\mathsf{state}, \sigma_{\mathsf{state}}); \tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle \\ x \leftarrow \mathcal{V}_2(v) \\ e \leftarrow \mathcal{E}(\tau, x) \\ y \leftarrow \mathcal{P}_2(\mathsf{state}, \sigma_{\mathsf{state}}, x)\end{array}\right] \tag{75}$$

$$\geq \Pr\left[\top \leftarrow \mathcal{V}_2(v, x, e) \wedge e = y : \begin{array}{l}(v, (\mathsf{state}, \sigma_{\mathsf{state}}); \tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle \\ x \leftarrow \mathcal{V}_2(v) \\ e \leftarrow \mathcal{E}(\tau, x) \\ y \leftarrow \mathcal{P}_2(\mathsf{state}, \sigma_{\mathsf{state}}, x)\end{array}\right] \tag{76}$$

$$= \Pr\left[\top \leftarrow \mathcal{V}_2(v, x, y) \wedge y \leftarrow \mathcal{E}(\tau, x) : \begin{array}{l}(v, (\mathsf{state}, \sigma_{\mathsf{state}}); \tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle \\ x \leftarrow \mathcal{V}_2(v) \\ y \leftarrow \mathcal{P}_2(\mathsf{state}, \sigma_{\mathsf{state}}, x)\end{array}\right] \tag{77}$$

$$> 1 - \frac{1}{2p(\lambda)} - \mathsf{negl}(\lambda) \tag{78}$$

$$> 1 - \frac{1}{p(\lambda)} \tag{79}$$

for infinitely many $\lambda \in \mathbb{N}$. Here, in Equation (78), we have used the union bound. This contradicts $(1 - \frac{1}{p}, 0)$-soundness of the predictable PoQM. □

Remark 5.5. We can actually define a weaker notion of predictable PoQM, and can show that they also imply QCCC KE. See Appendix A.

6 Constant-Round PoQ Imply Single-Round QV-PoQ or PoQM

In this section, we show the following result.[26]

Theorem 6.1. *Let $\ell : \mathbb{N} \to \mathbb{N}$ be any polynomial. Let $\alpha, \beta : \mathbb{N} \to [0, 1]$ be any functions such that $\alpha(\lambda) - \beta(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ for all $\lambda \in \mathbb{N}$. Let $\epsilon, \delta : \mathbb{N} \to [0, 1]$ be any functions such that $\epsilon(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$, $\delta(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ and $(\alpha(\lambda) - \epsilon(\lambda)) - (\beta(\lambda) + \delta(\lambda)) \geq \frac{1}{\mathrm{poly}(\lambda)}$ for all $\lambda \in \mathbb{N}$. If ℓ-round (α, β)-PoQ exist, then one of the following primitives exists:*

[26] Note that in this theorem we consider only uniform PPT (QPT) adversaries, because as we can see in the proof, we can show only the uniform setting.

- *ℓ-round $(\alpha, \alpha-\epsilon, \mathrm{poly}, 0)$-PoQM (with i.o.-soundness).*
- *single-round $(\alpha-\epsilon, \beta+\delta)$-QV-PoQ (with i.o.-soundness).*
- *$(\ell-1)$-round $(\beta+\delta, \beta)$-PoQ.*

Note that the above single-round QV-PoQ is a special one where the verifier's second computation (i.e., the computation to make the decision) is PPT.

Remark 6.2. With a similar proof, we also obtain the same theorem except that the single-round QV-PoQ is a special one where the verifier's first computation (i.e., the computation that generates the challenge) is PPT.

Proof of Theorem 6.1. Let $(\mathcal{V}, \mathcal{P})$ be an ℓ-round (α, β)-PoQ. We consider the following two cases.

Case 1. For any QPT algorithm $\mathcal{P}^*$ whose internal state after sending its $(\ell-1)$th message is classical,

$$\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}^*(1^\lambda)\rangle\right] \leq \alpha(\lambda) - \epsilon(\lambda) \tag{80}$$

for infinitely many $\lambda \in \mathbb{N}$. Then we can construct an $(\alpha, \alpha-\epsilon, \mathrm{poly}, 0)$-PoQM with i.o.-soundness as follows:

- *Initialization phase:* The verifier and the prover run $\mathcal{V}$ and $\mathcal{P}$, respectively, until the end of the $(\ell-1)$th round.
- *Execution phase:* The verifier and the prover run the ℓth round of $\mathcal{V}$ and $\mathcal{P}$. Finally, the verifier outputs the output of $\mathcal{V}$.

Its α-completeness immediately follows from that of the original PoQ. Its i.o.-$(\alpha-\epsilon, 0)$-soundness is also clear from Equation (80).

Case 2. Case 1 does not hold. In other words, there exists a QPT algorithm $\mathcal{P}^*$ whose internal state after sending its $(\ell-1)$th message is classical such that

$$\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}^*(1^\lambda)\rangle\right] > \alpha(\lambda) - \epsilon(\lambda) \tag{81}$$

for all sufficiently large $\lambda \in \mathbb{N}$.

Let us construct a single-round $(\alpha-\epsilon, \beta+\delta)$-QV-PoQ with i.o.-soundness as follows:

1. The verifier simulates the interaction between $\mathcal{V}$ and $\mathcal{P}^*$ until the end of the $\mathcal{V}$'s ℓth computation (i.e., by the step when $\mathcal{V}$ outputs its ℓth message).
2. The verifier sends the transcript and $\mathcal{P}^*$'s classical internal state to the prover.
3. The prover runs the ℓth computation of $\mathcal{P}^*$ (i.e., the prover computes $\mathcal{P}^*$'s ℓth message), and sends the ℓth message to the verifier.
4. The verifier makes the decision.

Its $(\alpha-\epsilon)$-completeness follows from Equation (81). If it is i.o.-$(\beta+\delta)$-sound, we obtain single-round $(\alpha-\epsilon, \beta+\delta)$-QV-PoQ with i.o.-soundness.

Assume that it is not i.o.-$(\beta+\delta)$-sound. Then, there exists a PPT algorithm $\mathcal{A}$ that breaks the QV-PoQ. Let us define the following QPT algorithm $\mathcal{P}^{**}$:

1. Run $\mathcal{P}^*$ until the end of the $(\ell-1)$th round.
2. Run the PPT algorithm $\mathcal{A}$ for its ℓth computation.

Note that $\mathcal{P}^{**}$'s internal state after sending $(\ell-1)$th message is classical. $\mathcal{P}^{**}$ satisfies

$$\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}^{**}(1^\lambda)\rangle\right] > \beta(\lambda)+\delta(\lambda) \tag{82}$$

for all sufficiently large $\lambda \in \mathbb{N}$. Then, we can construct $(\ell-1)$-round $(\beta+\delta,\beta)$-PoQ as follows.

1. The verifier and the prover run $\mathcal{V}$ and $\mathcal{P}^{**}$, respectively, until the end of the $(\ell-1)$th round.
2. When prover sends its $(\ell-1)$th message, it also sends its classical internal state.
3. The verifier simulates the ℓth round between $\mathcal{V}$ and $\mathcal{P}^{**}$ by itself.
4. The verifier outputs the output of $\mathcal{V}$.

Its $(\beta+\delta)$-completeness follows from Equation (82) and β-soundness follows from that of the original PoQ. □

By repeating Theorem 6.1, we obtain the following corollary.

Corollary 6.3. *If constant-round PoQ exist, then one of the following primitives exists.*

- *constant-round PoQM with $m_2=0$ (with i.o.-soundness).*
- *single-round QV-PoQ (with i.o.-soundness).*

Proof of Corollary 6.3. Let $\ell \geq 2$. Assume that ℓ-round (α_0,β_0)-PoQ exist with some α_0,β_0 such that $\alpha_0(\lambda)-\beta_0(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ for all $\lambda \in \mathbb{N}$.

1. Define $\epsilon_1 := \frac{(\alpha_0-\beta_0)}{n}$ and $\delta_1 := \frac{(\alpha_0-\beta_0)(n-2)}{n}$, where $n := 2\ell(\ell-1)$. Then from Theorem 6.1, we obtain $(\ell-1)$-round (α_1,β_1)-PoQ with $\alpha_1 := \beta_0+\delta_1$ and $\beta_1 := \beta_0$, or other primitives (i.e., PoQM or single-round QV-PoQ) with $\frac{1}{\mathrm{poly}}$ completeness-soundness gap.
2. If we obtain $(\ell-1)$-round (α_1,β_1)-PoQ, define $\epsilon_2 := \frac{(\alpha_1-\beta_1)}{n}$ and $\delta_2 := \frac{(\alpha_1-\beta_1)(n-2)}{n} = \delta_1\frac{n-2}{n} = (\alpha_0-\beta_0)\left(\frac{n-2}{n}\right)^2$. Then from Theorem 6.1, we obtain $(\ell-2)$-round (α_2,β_2)-PoQ with $\alpha_2 := \beta_1+\delta_2 = \beta_0+\delta_2$ and $\beta_2 := \beta_1 = \beta_0$, or other primitives with $\frac{1}{\mathrm{poly}}$ completeness-soundness gap.
3. If we obtain $(\ell-2)$-round (α_2,β_2)-PoQ, define $\epsilon_3 := \frac{(\alpha_2-\beta_2)}{n}$ and $\delta_3 := \frac{(\alpha_2-\beta_2)(n-2)}{n} = \delta_2\frac{n-2}{n} = (\alpha_0-\beta_0)\left(\frac{n-2}{n}\right)^3$. Then from Theorem 6.1, we obtain $(\ell-3)$-round (α_3,β_3)-PoQ with $\alpha_3 := \beta_2+\delta_3 = \beta_0+\delta_3$ and $\beta_3 := \beta_2 = \beta_0$, or other primitives with $\frac{1}{\mathrm{poly}}$ completeness-soundness gap.

If we repeat this, we finally obtain single-round $(\alpha_{\ell-1},\beta_{\ell-1})$-PoQ with $\alpha_{\ell-1} = \beta_0+\delta_{\ell-1}$ and $\beta_{\ell-1}=\beta_0$, or other primitives with $\frac{1}{\mathrm{poly}}$ completeness-soundness gap. Because

$$\delta_{\ell-1} = (\alpha_0-\beta_0)\left(\frac{n-2}{n}\right)^{\ell-1} = (\alpha_0-\beta_0)\left(1-\frac{2}{n}\right)^{\ell-1} \tag{83}$$

$$= (\alpha_0-\beta_0)\left(1-\frac{1}{\ell(\ell-1)}\right)^{\ell-1} \geq (\alpha_0-\beta_0)\left(1-\frac{1}{\ell}\right) \geq \frac{1}{\mathrm{poly}}, \tag{84}$$

we have $\alpha_{\ell-1}(\lambda)-\beta_{\ell-1}(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ for all $\lambda \in \mathbb{N}$.

□

Remark 6.4. In the above proof, we can see that the new verifier of the $(\ell-1)$-round PoQ runs $\mathcal{A}$. If $\mathcal{A}$'s run-time is proportional to the square of the run-time of the verifier of the ℓ-round PoQ, for example, the run-time of the new verifier is proportional to the square of the run-time of the old verifier. Hence, if we apply Theorem 6.1 polynomially-many times, the verifier's run-time can blowup exponentially. This is why Corollary 6.3 holds only for constant ℓ.[27]

7 Constant-Round IV-PoQ with Black-Box Reduction Imply IV-PoQM

7.1 Preliminaries

Before showing the main result of this section, we give definitions of several concepts.

First, we recall falsifiable assumptions [Nao03, GW11]. While [GW11] considers efficient challengers, we also allow inefficient challengers.

Definition 7.1 (Falsifiable Assumptions [Nao03, GW11, TZ26]). *A falsifiable assumption $(\mathcal{C}, \mathsf{thres})$ consists of a (potentially-inefficient) challenger $\mathcal{C}$ and a constant $\mathsf{thres} \in [0,1)$. The challenger interacts with an adversary $\mathcal{A}$ and outputs $\top$ or $\bot$. We say that an adversary $\mathcal{A}$ breaks the assumption if there exists a polynomial p such that for infinitely many $\lambda \in \mathbb{N}$,*

$$\Pr\left[\top \leftarrow \langle \mathcal{C}(1^\lambda), \mathcal{A}(1^\lambda)\rangle\right] \geq \mathsf{thres} + \frac{1}{p(\lambda)}. \tag{85}$$

[TZ26] introduced the notion of *IV-PoQ with black-box reduction*, which is defined as follows.

Definition 7.2 (IV-PoQ with Black-Box Reduction [TZ26]). *An (α,β)-IV-PoQ with black-box reduction to a falsifiable assumption $(\mathcal{C}, \mathsf{thres})$ is a set $(\mathcal{V}, \mathcal{P}, \mathcal{R})$ of algorithms. $\mathcal{V}$ and $\mathcal{P}$ interact over a classical channel. $\mathcal{V}$ is an algorithm that takes 1^λ as input and outputs $\top$ or $\bot$. It is PPT during the interaction, and the final computation to make the decision can be unbounded. $\mathcal{P}$ is a QPT algorithm that takes 1^λ as input and outputs nothing. $\mathcal{R}$ is a QPT reduction algorithm. We require the following properties:*

α-completeness: *For all sufficiently large $\lambda \in \mathbb{N}$,*

$$\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}(1^\lambda)\rangle\right] \geq \alpha(\lambda). \tag{86}$$

β-soundness by reduction. *For any polynomial p', there exists a polynomial p such that for any (not-necessarily-efficient) classical prover $\mathcal{A}$ that satisfies*

$$\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{A}(1^\lambda)\rangle\right] \geq \beta(\lambda) + \frac{1}{p'(\lambda)} \tag{87}$$

for infinitely many $\lambda \in \mathbb{N}$, it holds that

$$\Pr\left[\top \leftarrow \langle \mathcal{C}(1^\lambda), \mathcal{R}^{\mathcal{A}}(1^\lambda)\rangle\right] \geq \mathsf{thres} + \frac{1}{p(\lambda)} \tag{88}$$

for infinitely many $\lambda \in \mathbb{N}$. Here, $\mathcal{R}^{\mathcal{A}}$ is defined as follows. Let $x := (i, \tau, st, k)$, where $i \in [\ell]$, τ and st are bit strings, and $k \in \mathbb{N}$. $\mathcal{D}_x$ is the distribution of the output of $\mathcal{A}$ when we run the ith computation of $\mathcal{A}$ on input a transcript τ and a state st.[28] Sample a classical oracle $\mathcal{O}$ in such a way that the xth row of its truth table is sampled from $\mathcal{D}_x$. Once one $\mathcal{O}$ is sampled, we fix $\mathcal{O}$, and $\mathcal{R}$ can quantumly query $\mathcal{O}$.

[27] We thank Kabir Tomer for pointing out this fact.

[28] The index k is included so that we can sample the output of $\mathcal{A}$ many times on the same input.

We use the following lemma that is shown in [TZ26].[29]

Lemma 7.3 ([TZ26]). *Let $\{U_x\}_{x\in\{0,1\}^*}$ be a set of efficient unitaries. For each $x \in \{0,1\}^*$, let $\mathcal{D}_x$ be the distribution of the computational-basis measurement results on $U_x|0...0\rangle$. Let $\mathcal{D} := \bigotimes_{x\in\{0,1\}^*} \mathcal{D}_x$. Let $\mathcal{O}$ be a classical oracle. We say an oracle $\mathcal{O}$ is sampled from $\mathcal{D}$, and denote by $\mathcal{O} \leftarrow \mathcal{D}$, when the xth row of its truth table is sampled from $\mathcal{D}_x$ for each $x \in \{0,1\}^*$. Then for any polynomial q and for any QPT algorithm $\mathcal{A}$, there exists a QPT simulator Sim such that*

$$\left|\Pr_{\mathcal{O}\leftarrow\mathcal{D}}[\top \leftarrow \mathcal{A}^{\mathcal{O}}(1^\lambda)] - \Pr\left[\top \leftarrow \mathsf{Sim}(1^\lambda)\right]\right| \leq \frac{1}{q(\lambda)} \tag{89}$$

for all $\lambda \in \mathbb{N}$.

7.2 Results

Now we show our main result of this section.[30]

Theorem 7.4. *Let ℓ be any polynomial. Let $\alpha, \beta : \mathbb{N} \to [0,1]$ be any functions such that $\alpha(\lambda)-\beta(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ for all $\lambda \in \mathbb{N}$. Let $\epsilon : \mathbb{N} \to [0,1]$ be any function such that $\epsilon(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ and $(\alpha(\lambda) - \epsilon(\lambda))-\beta(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ for all $\lambda \in \mathbb{N}$. Suppose that there exist ℓ-round (α,β)-IV-PoQ with black-box reduction to a falsifiable assumption $(\mathcal{C}, \mathsf{thres})$. Then one of the following primitives exists.*

- *ℓ-round $(\alpha, \alpha-\epsilon, \mathrm{poly}, 0)$-IV-PoQM (with i.o.-soundness).*
- *$(\ell-1)$-round $(\alpha-\epsilon,\beta)$-IV-PoQ with black-box reduction to a falsifiable assumption $(\mathcal{C}, \mathsf{thres})$.*

Proof of Theorem 7.4. Let $(\mathcal{V},\mathcal{P},\mathcal{R})$ be an ℓ-round (α,β)-IV-PoQ with black-box reduction to a falsifiable assumption $(\mathcal{C},\mathsf{thres})$. This means that for all sufficiently large $\lambda \in \mathbb{N}$,

$$\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}(1^\lambda)\rangle\right] \geq \alpha(\lambda), \tag{90}$$

and for any polynomial p', there exists a polynomial p such that for any classical prover $\mathcal{A}$ that satisfies

$$\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{A}(1^\lambda)\rangle\right] \geq \beta(\lambda) + \frac{1}{p'(\lambda)} \tag{91}$$

for infinitely many $\lambda \in \mathbb{N}$, it holds that

$$\Pr\left[\top \leftarrow \langle \mathcal{C}(1^\lambda), \mathcal{R}^{\mathcal{A}}(1^\lambda)\rangle\right] \geq \mathsf{thres} + \frac{1}{p(\lambda)} \tag{92}$$

for infinitely many $\lambda \in \mathbb{N}$.

We consider the following two cases.

[29] [TZ26] formulates the lemma in the non-uniform setting, but here we state its uniform version, because our results hold only for the uniform setting.

[30] Note that in this theorem we consider only uniform PPT (QPT) adversaries, because as we can see in the proof, we can show only the uniform setting.

Case 1. For any QPT algorithm $\mathcal{P}^*$ whose internal state after sending its $(\ell-1)$th message is classical,

$$\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}^*(1^\lambda)\rangle\right] \leq \alpha(\lambda) - \epsilon(\lambda) \tag{93}$$

for infinitely many $\lambda \in \mathbb{N}$. Then we can construct an $(\alpha, \alpha-\epsilon, \mathrm{poly}, 0)$-IV-PoQM as follows:

- *Initialization phase:* The verifier and the prover run $\mathcal{V}$ and $\mathcal{P}$, respectively, until the end of the $(\ell-1)$th round.
- *Execution phase:* The verifier and the prover run the ℓth round of $\mathcal{V}$ and $\mathcal{P}$. Finally, the verifier outputs the output of $\mathcal{V}$.

Its α-completeness immediately follows from Equation (90). Its i.o.-$(\alpha-\epsilon, 0)$-soundness is also clear from Equation (93).

Case 2. Case 1 does not hold. In other words, there exists a QPT algorithm $\mathcal{P}^*$ whose internal state after sending its $(\ell-1)$th message is classical such that

$$\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{P}^*(1^\lambda)\rangle\right] > \alpha(\lambda) - \epsilon(\lambda) \tag{94}$$

for all sufficiently large $\lambda \in \mathbb{N}$.

By using $\mathcal{P}^*$, we construct an $(\ell-1)$-round $(\alpha-\epsilon, \beta)$-IV-PoQ $(\widetilde{\mathcal{V}}, \widetilde{\mathcal{P}})$ as follows:

1. $\widetilde{\mathcal{V}}$ and $\widetilde{\mathcal{P}}$ run $\mathcal{V}$ and $\mathcal{P}^*$, respectively, until the end of the $(\ell-1)$th round.
2. When $\widetilde{\mathcal{P}}$ sends its $(\ell-1)$th message, it also sends its classical internal state s.
3. $\widetilde{\mathcal{V}}$ simulates the ℓth round between $\mathcal{V}$ and $\mathcal{P}^*$ by itself, and outputs the output of $\mathcal{V}$.

Its $(\alpha-\epsilon)$-completeness follows from Equation (94).

Let us next show β-soundness by reduction. Our goal is to show the existence of a QPT reduction algorithm $\mathcal{Q}$ such that for any polynomial p' there exists a polynomial p such that for any classical algorithm $\widetilde{\mathcal{P}}^*$ that satisfies

$$\Pr\left[\top \leftarrow \langle \widetilde{\mathcal{V}}(1^\lambda), \widetilde{\mathcal{P}}^*(1^\lambda)\rangle\right] \geq \beta(\lambda) + \frac{1}{p'(\lambda)} \tag{95}$$

for infinitely many $\lambda \in \mathbb{N}$, it holds that

$$\Pr\left[\top \leftarrow \langle \mathcal{C}(1^\lambda), \mathcal{Q}^{\widetilde{\mathcal{P}}^*}(1^\lambda)\rangle\right] \geq \mathsf{thres} + \frac{1}{p(\lambda)} \tag{96}$$

for infinitely many $\lambda \in \mathbb{N}$.

For that goal, let us define a classical (inefficient) algorithm $\mathcal{A}$ as follows.

$\mathcal{A}$**:** Run $\widetilde{\mathcal{P}}^*$ until the $(\ell-1)$th round. In the ℓth round, simulate the ℓth round of $\mathcal{P}^*$.
By Equation (95),

$$\Pr\left[\top \leftarrow \langle \mathcal{V}(1^\lambda), \mathcal{A}(1^\lambda)\rangle\right] \geq \beta(\lambda) + \frac{1}{p'(\lambda)} \tag{97}$$

for infinitely many $\lambda \in \mathbb{N}$. By Equation (92), there exists a polynomial p such that

$$\Pr\left[\top \leftarrow \langle \mathcal{C}(1^\lambda), \mathcal{R}^{\mathcal{A}}(1^\lambda)\rangle\right] \geq \mathsf{thres} + \frac{1}{p(\lambda)} \tag{98}$$

for infinitely many $\lambda \in \mathbb{N}$.

Let us define the QPT reduction algorithm $\mathcal{Q}^{\widetilde{\mathcal{P}}^*}$ as follows:

$\mathcal{Q}^{\widetilde{\mathcal{P}}^*}$: It is identical to $\mathcal{R}^{\mathcal{A}}$ except for the following: when $\mathcal{R}$ queries $\mathcal{A}$'s inefficient part (namely, simulating the ℓth round of $\mathcal{P}^*$), the query is replaced with the efficient simulation of it that is guaranteed by Lemma 7.3.

By Lemma 7.3, we have

$$\Pr\left[\top \leftarrow \langle \mathcal{C}(1^\lambda), \mathcal{Q}^{\widetilde{\mathcal{P}}^*}(1^\lambda)\rangle\right] \geq \Pr\left[\top \leftarrow \langle \mathcal{C}(1^\lambda), \mathcal{R}^{\mathcal{A}}(1^\lambda)\rangle\right] - \frac{1}{2p(\lambda)} \tag{99}$$

$$\geq \mathsf{thres} + \frac{1}{2p(\lambda)} \tag{100}$$

for infinitely many $\lambda \in \mathbb{N}$.

□

Repeatedly applying Theorem 7.4, we have the following corollary.

Corollary 7.5. *If there exist constant-round IV-PoQ with black-box reduction to a falsifiable assumption, then one of the following exists.*

- *constant-round IV-PoQM (with i.o.-soundness).*
- *single-round IV-PoQ with black-box reduction to a falsifiable assumption.*

Proof of Corollary 7.5. Let $\ell \geq 2$. Assume that ℓ-round (α_0, β_0)-IV-PoQ with black box reduction to a falsifiable assumption exist with some α_0, β_0 such that $\alpha_0(\lambda) - \beta_0(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$ for all $\lambda \in \mathbb{N}$.

1. Define $\epsilon := \frac{\alpha_0 - \beta_0}{\ell} \left(\geq \frac{1}{\mathrm{poly}}\right)$. Then from Theorem 7.4, we obtain $(\ell-1)$-round (α_1, β_1)-IV-PoQ with black-box reduction to a falsifiable assumption with $\alpha_1 := \alpha_0 - \epsilon$ and $\beta_1 := \beta_0$ or IV-PoQM with $\frac{1}{\mathrm{poly}}$ completeness-soundness gap.
2. If we obtain $(\ell-1)$-round IV-PoQ with black-box reduction to a falsifiable assumption, then from Theorem 7.4, we obtain $(\ell-2)$-round (α_2, β_2)-IV-PoQ with black-box reduction to a falsifiable assumption with $\alpha_2 := \alpha_1 - \epsilon = \alpha_0 - 2\epsilon$ and $\beta_2 := \beta_1 = \beta_0$ or IV-PoQM with $\frac{1}{\mathrm{poly}}$ completeness-soundness gap.

3. If we obtain $(\ell-2)$-round IV-PoQ with black-box reduction to a falsifiable assumption, then from Theorem 7.4, we obtain $(\ell-3)$-round (α_3,β_3)-IV-PoQ with black-box reduction to a falsifiable assumption with $\alpha_3 := \alpha_2 - \epsilon = \alpha_0 - 3\epsilon$ and $\beta_3 := \beta_2 = \beta_0$ or IV-PoQM with $\frac{1}{\mathrm{poly}}$ completeness-soundness gap.

If we repeat this, we finally obtain single-round $(\alpha_{\ell-1},\beta_{\ell-1})$-IV-PoQ with black-box reduction to a falsifiable assumption with $\alpha_{\ell-1} = \alpha_0 - (\ell-1)\epsilon$ and $\beta_{\ell-1} = \beta_0$ or IV-PoQM with $\frac{1}{\mathrm{poly}}$ completeness-soundness gap. Because

$$\alpha_{\ell-1}(\lambda) - \beta_{\ell-1}(\lambda) = \alpha_0 - (\ell-1)\epsilon - \beta_0 = \frac{\alpha_0(\lambda)-\beta_0(\lambda)}{\ell} \geq \frac{1}{\mathrm{poly}(\lambda)} \tag{101}$$

for all $\lambda \in \mathbb{N}$, the single-round IV-PoQ with black-box reduction to a falsifiable assumption have $\frac{1}{\mathrm{poly}}$ completeness-soundness gap. □

On the other hand, Tomer and Zhandry [TZ26] showed that single-round IV-PoQ cannot have a quantum black-box reduction to a falsifiable assumption, otherwise the falsifiable assumption is quantumly broken. Combining Corollary 7.5 and the result, we obtain the following corollary:

Corollary 7.6. *If there exist constant-round IV-PoQ with black-box reduction to a falsifiable assumption, then there exist constant-round IV-PoQM (with i.o.-soundness) or the falsifiable assumption is quantumly broken.*

In particular, [MY24] constructed constant-round IV-PoQ from (classically-secure) constant-round statistically-hiding commitments in a black-box way, and therefore we obtain the following corollary.

Corollary 7.7. *If quantumly-secure constant-round statistically-hiding commitments exist, then there exist constant-round IV-PoQM (with i.o.-soundness).*

Furthermore, constant-round statistically-hiding commitments can be obtained from collision-resistant hash functions [HM96], thus we also obtain the following corollary.

Corollary 7.8. *If quantumly-secure collision-resistant hash functions exist, then there exist constant-round IV-PoQM (with i.o.-soundness).*

Acknowledgements. TM is supported by JST CREST JPMJCR23I3, JST Moonshot R&D JPMJMS2061-5-1-1, JST FOREST, MEXT QLEAP, the Grant-in Aid for Transformative Research Areas (A) 21H05183, and the Grant-in-Aid for Scientific Research (A) No.22H00522.

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, Cham, August 2022. (Cited on page 4.)

[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, Cham, August 2022. (Cited on page 4.)

[BCM+21] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *Journal of the ACM*, 68(5):31:1–31:47, 2021. (Cited on page 1, 4, 13.)

[BGKM+23] Zvika Brakerski, Alexandru Gheorghiu, Gregory D. Kahanamoku-Meyer, Eitan Porat, and Thomas Vidick. Simple tests of quantumness also certify qubits. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part V*, volume 14085 of *LNCS*, pages 162–191. Springer, Cham, August 2023. (Cited on page 11.)

[BK25] James Bartusek and Dakshita Khurana. On the power of oblivious state preparation. In *CRYPTO 2025, Part II*, LNCS, pages 575–607. Springer, Cham, August 2025. (Cited on page 7.)

[BQSY24] John Bostanci, Luowen Qian, Nicholas Spooner, and Henry Yuen. An efficient quantum parallel repetition theorem and applications. In Bojan Mohar, Igor Shinkar, and Ryan O'Donnell, editors, *56th ACM STOC*, pages 1478–1487. ACM Press, June 2024. (Cited on page 40.)

[BS26] James Bartusek and Itay Shalit. On the cryptographic structure required for verifying qubits. Cryptology ePrint Archive, Paper 2026/1215, 2026. (Cited on page 11.)

[BZ13] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 361–379. Springer, Berlin, Heidelberg, August 2013. (Cited on page 7, 9, 12.)

[ÇG24] Alper Çakan and Vipul Goyal. Unbounded leakage-resilient encryption and signatures. Cryptology ePrint Archive, Paper 2024/1876, 2024. (Cited on page 7, 12.)

[CGJL25] Orestis Chardouvelis, Vipul Goyal, Aayush Jain, and Jiahui Liu. Quantum key leasing for PKE and FHE with a classical lessor. In *EUROCRYPT 2025, Part III*, LNCS, pages 248–277. Springer, Cham, June 2025. (Cited on page 9.)

[CH22] Nai-Hui Chia and Shih-Han Hung. Classical verification of quantum depth. *arXiv preprint arXiv:2205.04656*, 2022. (Cited on page 11.)

[CR20] Rui Chao and Ben W Reichardt. Quantum dimension test using the uncertainty principle. *arXiv preprint arXiv:2002.12432*, 2020. (Cited on page 11.)

[DFKP15] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. Proofs of space. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 585–605. Springer, Berlin, Heidelberg, August 2015. (Cited on page 2, 11.)

[FWZ23] Honghao Fu, Daochen Wang, and Qi Zhao. Parallel self-testing of EPR pairs under computational assumptions. In Kousha Etessami, Uriel Feige, and Gabriele Puppis, editors, *ICALP 2023*, volume 261 of *LIPIcs*, pages 64:1–64:19. Schloss Dagstuhl, July 2023. (Cited on page 11.)

[GMMY24] Eli Goldin, Tomoyuki Morimae, Saachi Mutreja, and Takashi Yamakawa. CountCrypt: Quantum cryptography between QCMA and PP. Cryptology ePrint Archive, Paper 2024/1707, 2024. (Cited on page 4, 15.)

[GV19] Alexandru Gheorghiu and Thomas Vidick. Computationally-secure and composable remote state preparation. In David Zuckerman, editor, *60th FOCS*, pages 1024–1033. IEEE Computer Society Press, November 2019. (Cited on page 7, 15.)

[GW11] Craig Gentry and Daniel Wichs. Separating succinct non-interactive arguments from all falsifiable assumptions. In Lance Fortnow and Salil P. Vadhan, editors, *43rd ACM STOC*, pages 99–108. ACM Press, June 2011. (Cited on page 5, 31.)

[HM96] Shai Halevi and Silvio Micali. Practical and provably-secure commitment schemes from collision-free hashing. In Neal Koblitz, editor, *CRYPTO'96*, volume 1109 of *LNCS*, pages 201–215. Springer, Berlin, Heidelberg, August 1996. (Cited on page 6, 35.)

[KMCVY22] Gregory D. Kahanamoku-Meyer, Soonwon Choi, Umesh V. Vazirani, and Norman Y. Yao. Classically verifiable quantum advantage from a computational bell test. *Nature Physics*, 2022. (Cited on page 4.)

[KT24] Dakshita Khurana and Kabir Tomer. Commitments from quantum one-wayness. In Bojan Mohar, Igor Shinkar, and Ryan O'Donnell, editors, *56th ACM STOC*, pages 968–978. ACM Press, June 2024. (Cited on page 1, 3, 4.)

[KT25] Dakshita Khurana and Kabir Tomer. Founding quantum cryptography on quantum advantage, or, towards cryptography from #p hardness. In *57th ACM STOC*, pages 178–188. ACM Press, June 2025. (Cited on page 9, 13.)

[LLLL24] Longcheng Li, Qian Li, Xingjian Li, and Qipeng Liu. How (not) to build quantum PKE in minicrypt. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part VII*, volume 14926 of *LNCS*, pages 152–183. Springer, Cham, August 2024. (Cited on page 4.)

[LLLL25] Longcheng Li, Qian Li, Xingjian Li, and Qipeng Liu. Toward the impossibility of perfect complete quantum PKE from OWFs. In *ITCS 2025*, pages 71:1–71:16. LIPIcs, January 2025. (Cited on page 4.)

[LLQ22] Jiahui Liu, Qipeng Liu, and Luowen Qian. Beating classical impossibility of position verification. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPIcs*, pages 100:1–100:11. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. (Cited on page 8, 9, 14.)

[MM25] Giulio Malavolta and Tamer Mour. How to verify that a small device is quantum, unconditionally. In *TCC 2025, Part III*, LNCS, pages 377–408. Springer, Cham, November 2025. (Cited on page 11.)

[MSY25] Tomoyuki Morimae, Yuki Shirakawa, and Takashi Yamakawa. Cryptographic characterization of quantum advantage. In Michal Koucký and Nikhil Bansal, editors, *57th ACM STOC*, pages 1863–1874. ACM Press, June 2025. (Cited on page 4.)

[MV20] Jack Maxfield and Thomas Vidick. Quantum proofs of space, 2020. (Cited on page 2, 6, 11.)

[MY22] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 269–295. Springer, Cham, August 2022. (Cited on page 4.)

[MY23] Tomoyuki Morimae and Takashi Yamakawa. Proofs of quantumness from trapdoor permutations. In Yael Tauman Kalai, editor, *ITCS 2023*, volume 251, pages 87:1–87:14. LIPIcs, January 2023. (Cited on page 4.)

[MY24] Tomoyuki Morimae and Takashi Yamakawa. Quantum advantage from one-way functions. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part V*, volume 14924 of *LNCS*, pages 359–392. Springer, Cham, August 2024. (Cited on page 2, 6, 13, 35.)

[Nao03] Moni Naor. On cryptographic assumptions and challenges (invited talk). In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 96–109. Springer, Berlin, Heidelberg, August 2003. (Cited on page 5, 31.)

[PWYZ24] Duong Hieu Phan, Weiqiang Wen, Xingyu Yan, and Jinwei Zheng. Adaptive hardcore bit and quantum key leasing over classical channel from LWE with polynomial modulus. In *Advances in Cryptology – ASIACRYPT 2024, Part IX*, volume 15492 of *LNCS*, pages 185–214. Springer, Singapore, December 2024. (Cited on page 9.)

[RS19] Roy Radian and Or Sattath. Semi-quantum money. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT 2019, Zurich, Switzerland, October 21-23, 2019*, pages 132–146. ACM, 2019. (Cited on page 8.)

[SZ25] Omri Shmueli and Mark Zhandry. On one-shot signatures, quantum vs. classical binding, and obfuscating permutations. In *CRYPTO 2025, Part II*, LNCS, pages 350–383. Springer, Cham, August 2025. (Cited on page 4.)

[TZ26] Kabir Tomer and Mark Zhandry. On the cryptographic foundations of interactive quantum advantage. In Aditya Bhaskara and Artur Czumaj, editors, *58th ACM STOC*, pages 455–466. ACM Press, 2026. (Cited on page 4, 6, 11, 12, 31, 32, 35.)

[Yan22] Jun Yan. General properties of quantum bit commitments (extended abstract). In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part IV*, volume 13794 of *LNCS*, pages 628–657. Springer, Cham, December 2022. (Cited on page 4.)

[Zha25] Jiayu Zhang. Formulations and constructions of remote state preparation with verifiability, with applications. In *ITCS 2025*, pages 96:1–96:19. LIPIcs, January 2025. (Cited on page 7, 15.)

A Weak Predictable PoQM

We define the following weaker version of predictable PoQM.

Definition A.1 (Weak Predictable PoQM). *A weak predictable* $(\alpha, \beta, m_1, m_2)$*-PoQM is an* $(\alpha, \beta, m_1, m_2)$*-PoQM with the following single-round execution phase.*

1. $\mathcal{V}_2$ *takes* v *as input, where* v *is the output of* $\mathcal{V}_1$.
2. $\mathcal{P}_2$ *takes* $(\mathsf{state}, \sigma_{\mathsf{state}})$ *as input, where* $(\mathsf{state}, \sigma_{\mathsf{state}})$ *is the output of* $\mathcal{P}_1$.
3. $\mathcal{V}_2$ *sends a bit string* x *to* $\mathcal{P}_2$.

4. *$\mathcal{P}_2$ sends a bit string y to $\mathcal{V}_2$.*

5. *$\mathcal{V}_2$ outputs $\top$ or $\bot$.*

Moreover, we require the existence of a QPT algorithm Ext *such that*

$$\Pr\left[y \leftarrow \mathsf{Ext}(v,\tau,x) : \begin{array}{l}(v,(\mathsf{state},\sigma_{\mathsf{state}});\tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle \\ x \leftarrow \mathcal{V}_2(v) \\ y \leftarrow \mathcal{P}_2(\mathsf{state},\sigma_{\mathsf{state}},x)\end{array}\right] \geq \alpha(\lambda). \tag{102}$$

Here, $(v,(\mathsf{state},\sigma_{\mathsf{state}});\tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle$ means that $\mathcal{V}_1$'s output is v, $\mathcal{P}_1$'s output is $(\mathsf{state},\sigma_{\mathsf{state}})$, and τ is the transcript.

Predictable PoQM (Definition 5.2) satisfy the above definition, since we can construct a QPT algorithm Ext that satisfies Equation (102) as follows: On input (v,τ,x), run $y' \leftarrow \mathcal{V}_2(v,x)$ and output its output. Thus, we have the following lemma.

Lemma A.2. *Let $\alpha,\beta : \mathbb{N} \to [0,1]$ be any functions. Let m_1, m_2 be any polynomials. If (α,β,m_1,m_2)-predictable PoQM exist, then (α,β,m_1,m_2)-weak predictable PoQM exist.*

We show that weak predictable PoQM also imply QCCC KE.

Theorem A.3. *Let $m_1 : \mathbb{N} \to \mathbb{N}$ be any function. Let p be any polynomial. If $(1-\mathsf{negl}, 1-\frac{1}{p}, m_1, 0)$-weak predictable PoQM exist, then QCCC KE exist.*

Proof of Theorem A.3. Let $(\mathcal{V}_1,\mathcal{P}_1,\mathcal{V}_2,\mathcal{P}_2)$ be an $(1-\mathsf{negl}, 1-\frac{1}{p}, m_1, 0)$-weak predictable PoQM. From it, we construct a QCCC KE $(\mathcal{A},\mathcal{B})$ as follows:

1. $\mathcal{A}$ and $\mathcal{B}$ take 1^λ as input.
2. $\mathcal{A}$ runs $\mathcal{P}_1(1^\lambda)$, and $\mathcal{B}$ runs $\mathcal{V}_1(1^\lambda)$. Let $(\mathsf{state},\sigma_{\mathsf{state}})$ be $\mathcal{P}_1$'s output. Let v be $\mathcal{V}_1$'s output.
3. $\mathcal{B}$ runs $x \leftarrow \mathcal{V}_2(v)$ and sends x to $\mathcal{A}$.
4. $\mathcal{A}$ runs $y \leftarrow \mathcal{P}_2(\mathsf{state},\sigma_{\mathsf{state}},x)$, but does not send y to $\mathcal{B}$.
5. $\mathcal{B}$ runs $y' \leftarrow \mathsf{Ext}(v,\tau,x)$.
6. $\mathcal{A}$ outputs $a := y$, and $\mathcal{B}$ outputs $b := y'$.

Now we show that thus constructed $(\mathcal{A},\mathcal{B})$ is a $(1-\mathsf{negl}, 1-\frac{1}{2p})$-QCCC KE. From Lemma 2.13, such a $(1-\mathsf{negl}, 1-\frac{1}{2p})$-QCCC KE can be amplified to obtain a QCCC KE.

$(1-\mathsf{negl})$-correctness is clear from Equation (102). Next, we show $(1-\frac{1}{2p})$-security. For the sake of contradiction, we assume that $(\mathcal{A},\mathcal{B})$ is not $(1-\frac{1}{2p})$-secure. This means that there exists a non-uniform QPT adversary $\mathcal{E}$ such that

$$\Pr\left[y \leftarrow \mathcal{E}(\tau,x) : \begin{array}{l}(v,(\mathsf{state},\sigma_{\mathsf{state}});\tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle \\ x \leftarrow \mathcal{V}_2(v) \\ y \leftarrow \mathcal{P}_2(\mathsf{state},\sigma_{\mathsf{state}},x)\end{array}\right] > 1 - \frac{1}{2p(\lambda)} \tag{103}$$

for infinitely many $\lambda \in \mathbb{N}$. Here, $(v,(\mathsf{state},\sigma_{\mathsf{state}});\tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle$ means that $\mathcal{V}_1$'s output is v, $\mathcal{P}_1$'s output is $(\mathsf{state},\sigma_{\mathsf{state}})$, and τ is the transcript. From this $\mathcal{E}$, we can construct a pair $(\mathcal{P}_1^*,\mathcal{P}_2^*)$ of adversaries that breaks $(1-\frac{1}{p},0)$-soundness of the PoQM as follows:

- $\mathcal{P}_1^*$: Run $(\mathsf{state}, \sigma_{\mathsf{state}}) \leftarrow \mathcal{P}_1(1^\lambda)$. Let τ be the transcript. Output τ.
- $\mathcal{P}_2^*$: Take τ and x as input, and run $e \leftarrow \mathcal{E}(\tau, x)$. Send e to $\mathcal{V}_2$.

$(\mathcal{P}_1^*, \mathcal{P}_2^*)$ breaks $(1 - \frac{1}{p}, 0)$-soundness as follows:

$$\Pr\left[\top \leftarrow \langle \mathcal{V}_2(v), \mathcal{P}_2^*(\tau)\rangle : (v, \tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1^*(1^\lambda)\rangle\right] \tag{104}$$

$$= \Pr\left[\top \leftarrow \mathcal{V}_2(v, x, e) : \begin{array}{l}(v, (\mathsf{state}, \sigma_{\mathsf{state}}); \tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle \\ x \leftarrow \mathcal{V}_2(v) \\ e \leftarrow \mathcal{E}(\tau, x)\end{array}\right] \tag{105}$$

$$= \Pr\left[\top \leftarrow \mathcal{V}_2(v, x, e) : \begin{array}{l}(v, (\mathsf{state}, \sigma_{\mathsf{state}}); \tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle \\ x \leftarrow \mathcal{V}_2(v) \\ e \leftarrow \mathcal{E}(\tau, x) \\ y \leftarrow \mathcal{P}_2(\mathsf{state}, \sigma_{\mathsf{state}}, x)\end{array}\right] \tag{106}$$

$$\geq \Pr\left[\top \leftarrow \mathcal{V}_2(v, x, e) \wedge e = y : \begin{array}{l}(v, (\mathsf{state}, \sigma_{\mathsf{state}}); \tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle \\ x \leftarrow \mathcal{V}_2(v) \\ e \leftarrow \mathcal{E}(\tau, x) \\ y \leftarrow \mathcal{P}_2(\mathsf{state}, \sigma_{\mathsf{state}}, x)\end{array}\right] \tag{107}$$

$$= \Pr\left[\top \leftarrow \mathcal{V}_2(v, x, y) \wedge y \leftarrow \mathcal{E}(\tau, x) : \begin{array}{l}(v, (\mathsf{state}, \sigma_{\mathsf{state}}); \tau) \leftarrow \langle \mathcal{V}_1(1^\lambda), \mathcal{P}_1(1^\lambda)\rangle \\ x \leftarrow \mathcal{V}_2(v) \\ y \leftarrow \mathcal{P}_2(\mathsf{state}, \sigma_{\mathsf{state}}, x)\end{array}\right] \tag{108}$$

$$> 1 - \frac{1}{2p(\lambda)} - \mathsf{negl}(\lambda) \tag{109}$$

$$> 1 - \frac{1}{p(\lambda)} \tag{110}$$

for infinitely many $\lambda \in \mathbb{N}$. Here, in Equation (109), we have used the union bound. This contradicts $(1 - \frac{1}{p}, 0)$-soundness of the weak predictable PoQM. □

B QCCC KE Security Amplification

In this section, we give a proof of Lemma 2.13. We use the following lemma.

Lemma B.1 ([BQSY24], Theorem 1). *Let k be a polynomial. Let $s : \mathbb{N} \to [0, 1]$ be any function. Let π be a 3-message quantum interactive protocol with soundness error $s(\lambda)$ against any non-uniform QPT adversary. Then, the k-fold parallel repetition $\pi^{\otimes k}$ has soundness error at most $s(\lambda)^{k(\lambda)} + \mathsf{negl}(\lambda)$ against any non-uniform QPT adversary.*

We now show Lemma 2.13.

Proof of Lemma 2.13. Let $k(\lambda) := \lambda p(\lambda)$. Let $(\mathcal{A}, \mathcal{B})$ be a $(1 - \mathsf{negl}, 1 - \frac{1}{p})$-QCCC KE. We construct a QCCC KE as follows:

- $\mathcal{A}'$: On input 1^λ, run $\mathcal{A}^{\otimes k}(1^\lambda)$. For each $i \in [k]$, let a_i denote the output of i-th copy of $\mathcal{A}$. Output $a := a_1 \| ... \| a_k$.

- $\mathcal{B}'$: On input 1^λ, run $\mathcal{B}^{\otimes k}(1^\lambda)$. For each $i \in [k]$, let b_i denote the output of i-th copy of $\mathcal{B}$. Output $b := b_1 \| ... \| b_k$.

First, we show correctness. By the correctness of $(1-\mathsf{negl}, 1-\frac{1}{p})$-QCCC KE,

$$\Pr\Big[a = b : (a, b; \tau) \leftarrow \langle \mathcal{A}'(1^\lambda), \mathcal{B}'(1^\lambda)\rangle\Big] \geq 1 - \sum_{i=1}^{k} \Pr\Big[a_i \neq b_i : (a_i, b_i, \tau_i) \leftarrow \langle \mathcal{A}(1^\lambda), \mathcal{B}(1^\lambda)\rangle\Big] \tag{111}$$

$$\geq 1 - \mathsf{negl}(\lambda), \tag{112}$$

where Equation (111) follows from the union bound. Thus, $(\mathcal{A}', \mathcal{B}')$ satisfies correctness.

We next show security. Consider the following 3-message quantum interactive protocol π.

1. The adversary $\mathcal{E}$ sends 1^λ to the challenger $\mathcal{C}$.
2. $\mathcal{C}$ runs $(a, b; \tau) \leftarrow \langle \mathcal{A}(1^\lambda), \mathcal{B}(1^\lambda)\rangle$ and sends τ to $\mathcal{E}$.
3. $\mathcal{E}$ outputs a bit string e and sends it to $\mathcal{C}$.
4. If $a = e$, $\mathcal{C}$ outputs $\top$. If $a \neq e$, $\mathcal{C}$ outputs $\bot$.

By the security of $(1-\mathsf{negl}, 1-\frac{1}{p})$-QCCC KE, for any non-uniform QPT adversary $\mathcal{E}$,

$$\Pr\Big[\top \leftarrow \langle \mathcal{C}(1^\lambda), \mathcal{E}(1^\lambda)\rangle\Big] = \Pr\Big[a = e : (a, b; \tau) \leftarrow \langle \mathcal{A}(1^\lambda), \mathcal{B}(1^\lambda)\rangle, e \leftarrow \mathcal{E}(\tau)\Big] \leq 1 - \frac{1}{p(\lambda)}, \tag{113}$$

for all sufficiently large $\lambda \in \mathbb{N}$. The security game for $(\mathcal{A}', \mathcal{B}')$ is the $k(\lambda)$-fold parallel repetition of π. Therefore, by Lemma B.1, for any non-uniform QPT adversary $\mathcal{E}$,

$$\Pr\Big[a = e : (a, b; \tau) \leftarrow \langle \mathcal{A}'(1^\lambda), \mathcal{B}'(1^\lambda)\rangle, e \leftarrow \mathcal{E}(\tau)\Big] \leq \left(1 - \frac{1}{p(\lambda)}\right)^{k(\lambda)} + \mathsf{negl}(\lambda) \tag{114}$$

$$\leq \exp\left(-\frac{k(\lambda)}{p(\lambda)}\right) + \mathsf{negl}(\lambda) \tag{115}$$

$$\leq \mathsf{negl}(\lambda) \tag{116}$$

where Equation (115) follows from $1 + x \leq \exp(x)$ and Equation (116) follows from $k(\lambda) = \lambda p(\lambda)$. This completes the proof. □