




On Constructing One-Way Quantum State Generators, and More

Shujiao Cao^{1,2}  and Rui Xue^{1,2}  

¹ State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

² School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

{caoshujiao, xuerui}@iie.ac.cn

Abstract. As a quantum analogue of one-way function, the notion of one-way quantum state generator is recently proposed by Morimae and Yamakawa (CRYPTO'22), which is proved to be implied by the pseudorandom state, and can be used to devise a construction of one-time secure digital signature. Due to Kretschmer's result (TQC'20), it's believed that pseudorandom state generator requires less than post-quantum secure one-way function. Unfortunately, it remains to be unknown how to achieve the one-way quantum state generator without the existence of post-quantum secure one-way function. In this paper, we mainly study that problem and obtain the following results:

- We propose two variants of one-way quantum state generator, which we call them the weak one-way quantum state generator and distributionally one-way quantum state generator, and show the equivalence among these three primitives.
- The distributionally one-way quantum state generator from average-case hardness assumption of a promise problem belongs to QSZK is obtained, and hence a construction of one-way quantum state generator.
- A direct construction of quantum bit commitment with statistical binding (sum-binding) and computational hiding from the average-case hardness of a complete problem of QSZK.
- To show the non-triviality of the constructions above, a quantum oracle \mathcal{U} is devised relative to which such promise problem in QSZK doesn't belong to $\text{QMA}^{\mathcal{U}}$.

Our results present the first non-trivial construction of one-way quantum state generator from the hardness assumption of complexity class, and give another evidence that one-way quantum state generator probably requires less than post-quantum secure one-way function.

1 Introduction

As the most fundamental primitive, one-way function (OWF) plays a crucial role in cryptography. Plenty of cryptographic primitives have been shown equivalent

to OWF, including the pseudorandom generator (PRG), pseudorandom functions (PRFs), pseudorandom permutations (PRPs), digital signature, symmetric encryption, message authentication code (MAC), bit commitment and more ([20,18,26,43,19,36,23,32]). It is called the MiniCrypt that the world one-way functions exist by Impagliazzo’s famous “five worlds” [25].

As a quantum analogue to MiniCrypt, the MiniQCrypt means the world that post-quantum secure one-way function (pqOWF) exists [21]. Many relations between the pqOWF and other quantum analogues of primitives in Minicrypt have been shown to be consistent with the classical setting, such as the post-quantum pseudorandom generators, quantum pseudorandom functions, quantum pseudorandom permutations, and quantum message authentication codes [47,10,48]. However, the world MiniQCrypt may contain some primitives that contrast to its classical counterpart, when allowing quantum communication, the celebrated result by Bennett and Brassard showed that the security of key exchange protocol doesn’t need to rely on any cryptographic assumption in quantum world [7]. Then, two independent works both showed the feasibility for constructing oblivious transfer (OT) protocol, secure multi-party computation (MPC) protocols from pqOWFs within a non-black box and black-box manner respectively [21,6]. That is because, in classical world, no construction has been found for implementing OT protocol from OWFs, and OT is believed to be a “higher-level” primitive than OWFs due to the existing black-box barrier [27,33].

Therefore, it seems that the existence of pqOWFs is probably not necessary for some quantum primitives whose classical counterparts are equivalent to (or even “stronger” than) OWFs in classical world. When considering a quantum state instead of a string as output, Ji, Liu and Song proposed a quantum analogue of PRGs which is called the pseudorandom states (PRSs) [28]. Its security is characterized by the hardness for distinguishing a real random state (sampled from the Haar measure) from the output state of PRSs with a random seed as input. It is shown that PRSs can be constructed by quantum pseudorandom functions which indicates that PRSs belongs to MiniQCrypt. But the other direction seems to be infeasible, by constructing a quantum oracle \mathcal{O} relative to which $\text{QMA}^{\mathcal{O}} = \text{BQP}^{\mathcal{O}}$ while PRS (and even pseudorandom unitary) still exists, the result by Kretschmer gave negative evidence for constructing pqOWF from PRS [31]. And by exploiting the nature of PRSs, two recently results by Morimae et al. and Ananth et al. devised constructions of quantum commitment from PRSs [35,5], which further showed that quantum bit commitment may be also “weaker” than pqOWFs. Besides, by considering quantum state as output, Morimae et al. defined a new quantum analogue of pqOWF, which they called the one-way quantum state generator (OWSG), and proved the implication from OWS to one-time secure digital signatures with quantum public keys [35]. And Ananth et al. also proposed the notion of pseudorandom function-like quantum states (PRFSs) and obtained several applications such as the pseudo one-time encryption schemes [5]. However, no known construction of these quantum primitives has been found from something “below” pqOWF. That motivates us to study this problem:

Can we achieve these quantum primitives by some computational hardness assumptions which are not sufficient for pqOWF?

One-Way Quantum State Generators Motivated by that problem, we here focus on the notion of OWSGs by Morimae and Yamakawa [35]. Informally, a quantum polynomial-time (QPT) algorithm \mathbf{f} is called OWSGs, if it takes a n -bit string x as input, and output a state $|\phi_x\rangle$ which guarantees the computational infeasibility of finding a “plausible” preimage x' for any QPT adversary even given polynomial many copies of the challenge state $|\phi_x\rangle$. Here “plausible” means the state output by x' is not far from the challenge state $|\phi_x\rangle$, which is characterized by the inner product of these two states. It is obvious that pqOWFs meets the requirement of OWSGs. And it has been further proved that PRS is also OWSG.

We can treat OWSGs as the quantum version of OWFs, not only because of the similarity between these two security definitions, but also due to the potential relations to other primitives (e.g. the implication from PRS to OWSG can be treated as the quantum version of the implication from PRG to OWF, and the construction of one-time secure digital signatures with quantum public keys from OWSG can be regarded as the quantum version of Lamport’s one-time signature scheme from OWF). According to Kretschmer’s result, we know that pqOWFs are probably not necessary to OWFs [31]. But unfortunately, it remains to be unknown that how to devise a non-trivial construction of OWSG which can not achieve the requirement of pqOWFs simultaneously.

1.1 Overview of Our Results and Techniques

In a nutshell, we explore the nature of OWSGs, and study how to construct it with some complexity assumptions which are not known to imply the OWFs. The main results is summarized as the follows.

The Equivalence Among Variants of OWSGs In order to construct OWSG, we consider the weak version of quantum one-wayness. Note that for a PQT algorithm \mathbf{f} which takes a string x as input and outputs a state $|\phi_x\rangle$, the quantum one-wayness of \mathbf{f} is defined by the computational infeasibility of any PQT adversary \mathcal{A} for finding a similar preimage x' [35]. That similarity is characterized by the the inner product $|\langle\phi_x|\phi_{x'}\rangle|$ of the fake state $|\phi_{x'}\rangle$ and the real challenge state $|\phi_x\rangle$ which is a negligible function when \mathbf{f} is OWSG. Note that OWSG (which we call it the strong OWSG sometimes to make it clear) can be regarded as the quantum analogue of (strong) one-way function. We hence accordingly define the notions of weak one-way state generator (weak OWSGs) and distributionally one-way quantum state generators (distributionally OWSGs), which can be regarded as the quantum analogues of the weak one-way functions (weak OWFs) and distributionally one-way functions (distributionally OWFs) [26,17].

These three notions share the same functionality. The only difference is their security definitions. Similar as the weak OWF, the weak OWSG only requires relaxed version of the one-wayness, which only bound the success probability

to be at most $1 - 1/p(n)$ for any QPT adversary \mathcal{A} ³, where $p(\cdot)$ denotes some positive polynomial. Note that the distributionally OWF requires the hardness for generates a nearly random preimage for a challenge value, which is characterized by the statistical distance between the real distribution of the input/output and the forged distribution by the adversary. Hence in quantum case, we describe that property by the trace distance between the real (mixed) state $|input\ string\rangle \otimes |output\ state\rangle$ and the faked (mixed) state generated by a QPT adversary. More specifically, if we denote by $\rho_{\mathcal{A},t}^{|\phi_x\rangle}$ the (mixed) state with the form $\sum p_x |x\rangle\langle x|$ which is output by an adversary \mathcal{A} with $|\phi_x\rangle^{\otimes t}$ as its input state. Then the distributionally one-wayness is characterized by the existence of some polynomial n^c

$$\mathbb{F}\left(\mathbb{E}_x |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_x \rho_{\mathcal{A},t}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|\right) \leq 1 - \frac{1}{n^c}$$

for any QPT adversary \mathcal{A} when n is sufficiently large. The expected value \mathbb{E}_x is taken over the distribution of $\mathcal{D}(1^n)$.

By the definitions of these variants of OWSGs, it's obvious that OWSG is immediately the weak OWSG, and weak OWSG is distributionally OWSG. As for the other direction, assuming \mathbf{f} is weak OWSG which takes x as input, and outputs $|\phi_{x_i}\rangle$ we firstly show that Yao's construction from weak OWF to OWF is also capable in quantum setting with only minor modification. Namely, it's not hard to prove

$$\mathbf{f}'(x_1, \dots, x_m) \rightarrow \otimes_{i=1}^m |\phi_{x_i}\rangle^{\otimes \text{poly}(n)}$$

is OWSG by a similar strategy. Where $\text{poly}(n)$ is some positive polynomial decided by \mathbf{f} . That is consistent with the classical counterpart [17].

Theorem 1. *The existence of weak OWSG and strong OWSG are equivalent.*

Then to illustrate the implication from the distributionally OWSG to weak OWSG, we still consider construction of its classical counterpart by Impagliazzo and Luby [26]. That is, let \mathbf{f} be distributionally OWSG which takes x as input, and outputs $|\phi_{x_i}\rangle$, then we consider

$$\mathbf{f}'(x, h_k, k) \rightarrow |\phi_x, k, h_k, h_k(x)\rangle$$

where $h_k : \{0, 1\}^n \rightarrow \{0, 1\}^k$ is a universal hash function, and $k \leq n + O(\log n)$.

The original proof by Impagliazzo and Luby [26] is like that, assuming \mathcal{A} can break the weak one-wayness of $f'(x) = (f(x), k, h_k, h_k(x))$ for some distributionally one-way function f , then almost all the outputs $f'(x)$ can be inverted. However, when we choose some suitable k (since there are at most polynomial many of k) such that the following conditions hold with non-negligible probability: (1) h_k is injective on the preimage space of the challenge value (i.e.

³ \mathcal{A} succeeds iff it measures $|\phi_x\rangle$ with $\{|\phi_{x'}\rangle\langle\phi_{x'}|, I - |\phi_{x'}\rangle\langle\phi_{x'}|\}$ and gets $|\phi_{x'}\rangle$ in result.

$f^{-1}(f(x))$); (2) The size of the image space of h_k (i.e. 2^k) is at most the size $|f^{-1}(f(x))| \cdot n^C$ for some polynomial n^C . In that case, for some random value $r \in \{0, 1\}^k$, it holds that $r \in h_k(f^{-1}(f(x)))$ with non-negligible probability, and since h_k is a universal hash and injective on $f^{-1}(f(x))$, the adversary \mathcal{A} would return some x' randomly in $f^{-1}(f(x))$. That induces an adversary \mathcal{B} for breaking the distributionally one-wayness by invoking $\mathcal{A}(f(x), k, h_k, r)$ with some random r (and k goes through $n + O(\log n)$ to $O(\log n)$ until a valid output has been found).

However, a subtle problem would appear when we adopt the strategy by Impagliazzo and Luby. That is because the preimage space $\{x \mid \mathbf{f}(x) \rightarrow |\phi_x\rangle\}$ of the challenge state $|\phi_x\rangle$ doesn't contain all valid forgeries. For example, for let x' be a forged preimage such that corresponding output state $|\phi_{x'}\rangle$ is very close to the real challenge state $|\phi_x\rangle$ (i.e. $|\langle\phi_{x'}|\phi_x\rangle| > \text{negl}(n)$), such an x' should also be considered since it's obviously a valid forgery. But it's a little intractable to decide which kinds of x' is "close" to the challenge state and which are not since $|\langle\phi_{x'}|\phi_x\rangle|$ can be any value in $[0, 1]$ (and that problem doesn't bother the result of its classical counterpart, since the output of a one-way function f is a string, either $\langle f(x)|f(x')\rangle = 1$ or $\langle f(x)|f(x')\rangle = 0$).

Fortunately, this problem can be tackled by a potential nature of a quantum state generator which doesn't satisfy the weak one-wayness. We find that, assuming the quantum state generator \mathbf{f} is not weak one-way, there exists a subspace I of the domain which takes in an overwhelming proportion, such that for any $x, x' \in I$, the the output states $|\phi_x\rangle$ and $|\phi_{x'}\rangle$ are either very close, or far enough. We call that property the *polarization* of a quantum state generator. More specifically, \mathbf{f} is (k, p) -*polarized* if for any $x, x' \in \{0, 1\}^n$, either $|\langle\phi_{x'}|\phi_x\rangle|^k \geq 1 - p(n)$ or $|\langle\phi_{x'}|\phi_x\rangle|^k \leq p(n)$.

Lemma 1 (informal). *If \mathbf{f} is not weak OWSG, then for any positive polynomial $\text{poly}(\cdot)$, there exists a positive polynomial $t(\cdot)$ and subspace I_n of the domain, such that I_n takes overwhelming part of the domain, and \mathbf{f} is $(2t(n), 1/\text{poly}(n))$ -polarized on I_n .*

Assuming \mathbf{f} is not weak OWSG, by the lemma above, we can hence divide I_n into several equivalent classes according to their trace distance. Then replacing the collection $f^{-1}(f(x))$ by the the collection of x' whose output state $|\phi_{x'}\rangle$ is close to the challenge state $|\phi_x\rangle$. Then by a similar strategy (but different technique) as the result by Impagliazzo and Luby [26], we hence show the implication from the distributionally OWSG to weak OWSG.

Theorem 2. *The existence of distributionally OWSG and weak OWSG are equivalent.*

Therefore we show the equivalence among these three primitives, which agrees with its classical counterpart.

Constructing OWSGs from Hard Problem in QSZK Since it's possible to construct (distributionally) OWF from an average-case hard problem in sta-

tistical zero-knowledge [40]⁴. Therefore, to construct OWSGs, we consider the average-case hardness of the quantum statistical zero-knowledge (QSZK). Since the quantum state distinguishability (QSD) problem is complete for QSZK (even in average-case) [45], therefore it's sufficient to consider the average hardness of the QSD problem.

Informally, the QSD problem is a promise problem, that given a pair of quantum circuit Q_0 and Q_1 , which is promised the distance of output (mixed) states (which we denote by ρ_0 and ρ_1 respectively) by these two circuits is either close enough or pretty far⁵, the problem is to decide which case it is. The QSD problem can be regarded as the quantum analogue of the statistical difference (SD) problem. The SD problem is a complete promise problem for statistical zero-knowledge which is given a pair of classical circuits C_0 and C_1 , promised that the output distributions of these two circuit is either close or far from each other for a random input.

It's easy to realize the distributionally OWF from the average-case hardness of SD problem. If we denote by $\mathbf{S}(r) \rightarrow (C_0^r, C_1^r)$ the procedure that the sampler \mathbf{S} generates a hard-on-average instance (C_0^r, C_1^r) of the SD problem with r as the internal random number, then $f(r, b, x) := (C_0^r, C_1^r, C_b^r(x))$ is naturally a distributionally OWF⁶. Since if there is a probabilistic polynomial time (PPT) adversary generates preimages of $f(b, x)$ randomly, it's nearly impossible to generate a valid preimage with $b \oplus 1$ when the distributions of C_0^r and C_1^r are far enough whereas a preimage with $b \oplus 1$ would appear more often when these two distributions are close. That hence induces a distinguisher for that SD problem.

However, it's more challenging to construct distributionally OWSG from a hard-on-average QSD problem. The output states by the instance Q_0, Q_1 are mixed with unknown distribution, which makes the purification procedure is hard to handle. Therefore, to settle this problem, we consider a purified version of the QSD problem, which we call it the semi-classical quantum state distinguishability (semi-classical QSD or scQSD) problem. Given a pair of unitary operators (U_0, U_1) along with two samplers $(\mathbf{S}_0, \mathbf{S}_1)$, it is promised that these two states $\sum_x p_{0,x} |\phi_{0,x}\rangle \langle \phi_{0,x}|$ and $\sum_x p_{1,x} |\phi_{1,x}\rangle \langle \phi_{1,x}|$ are either very close, or far enough, where we denote by $U_b |0, x\rangle = |\phi_{b,x}\rangle$ and $\Pr[\mathbf{S}_b(1^n) \rightarrow x] = p_{b,x}$, and the problem is to decide which case it is. It is easy to see that the semi-classical QSD problem is a special case of the QSD problem which specifies the purification progress and the distributions.

Then assuming the semi-classical QSD problem is hard-on-average for a sampler $\mathbf{S}(r) \rightarrow (Q_0^r, Q_1^r)$ here we still adopt the notion (Q_0^r, Q_1^r) to represent the instance of scQSD problem, but in that case $Q_b^r := (U_b^r, \mathbf{S}_b^r)$ represents the set of unitary circuit along sampler under the random index r , and $U_b^r |0, x\rangle = |\phi_{b,x}^{U_b^r}\rangle$.

⁴ Actually, the existence of OWF can further rely on the non-triviality (i.e. average-case hardness) of the computational zero-knowledge (CZK) [41].

⁵ It is usually characterized by whether the trace distance is larger than $2/3$, or smaller than $1/3$, but it's equivalent to replace by $1 - 2^{-n}$ and 2^{-n} respectively.

⁶ Detailed description and other applications of the average-case hardness of the SD problem may refer to [30,9].

We hence can ensure the existence of (distributionally) OWSGs by the following construction

$$\mathbf{f}(r, b, x) := |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle = |Q_0^r, Q_1^r\rangle \otimes |\phi_x^{U_b^r}\rangle.$$

That is because, assuming there exists an adversary \mathcal{A} breaking the distributionally one-wayness of \mathbf{f} , when the mixed states by Q_0^r, Q_1^r are pretty far, it's infeasible for \mathcal{A} to generate a valid preimage $(r^*, b \oplus 1, x^*)$ for $\mathbf{E}_x |\phi_x^{U_b^r}\rangle \langle \phi_x^{U_b^r}|^{\otimes t}$ as input state⁷. Because in that case, the trace distance between $\mathbf{E}_x |\phi_x^{U_b^r}\rangle \langle \phi_x^{U_b^r}|$ and $\mathbf{E}_x |\phi_x^{U_{b \oplus 1}^r}\rangle \langle \phi_x^{U_{b \oplus 1}^r}|$ is also very far, by the definition of the distributionally OWSG, it's impossible for a successful adversary \mathcal{A} for finding another case's preimage. And on the other hand, when the mixed states by Q_0^r, Q_1^r are close enough, then the trace distance between $\mathbf{E}_x |\phi_x^{U_b^r}\rangle \langle \phi_x^{U_b^r}|^{\otimes t}$ and $\mathbf{E}_x |\phi_x^{U_{b \oplus 1}^r}\rangle \langle \phi_x^{U_{b \oplus 1}^r}|^{\otimes t}$ is negligibly small. Therefore the output of \mathcal{A} should only change slightly when replacing $\mathbf{E}_x |\phi_x^{U_b^r}\rangle \langle \phi_x^{U_b^r}|^{\otimes t}$ by $\mathbf{E}_x |\phi_x^{U_{b \oplus 1}^r}\rangle \langle \phi_x^{U_{b \oplus 1}^r}|^{\otimes t}$ as a part of input state. That indicates \mathcal{A} would output another bit $b \oplus 1$ with noticeable probability, and hence we can devise a distinguisher of the semi-classical QSD problem by \mathcal{A} .

Theorem 3. *Assuming the semi-classical QSD problem is hard-on-average in quantum case, then there exists a distributionally one-way state generator.*

Besides, since semi-classical QSD problem is a special case of the QSD problem, we can prove that scQSD problem is also a promise problem of QSZK. And hence we can derive a construction of distributionally OWSG from a hard-on-average problem in QSZK, and therefore achieve the OWSG according to the constructions from weak OWSG to OWSG, and distributionally OWSG to weak OWSG.

Constructing Quantum Commitment from Hardness of QSZK Although we face the problem of handling the progress of purification when constructing the distributionally OWSG from the standard QSD problem, but as a by-product and another cryptographic application of the hardness of QSZK, we can derive a direct construction of quantum bit commitment with statistical binding (sum-binding) and computational hiding from the average-case hardness of the QSD problem.

Informally, note that the hardness of the QSD problem ensures that any QPT adversary can not distinguish whether the mixed states by a given instance of the QSD problem Q_0, Q_1 are close enough or pretty far. That implies if we send one of the mixed state of Q_0, Q_1 as a commitment and reveal it by sending the entangled part of this state. Then the verification can be achieved by checking whether this state is output by the purification circuit of Q_b (here we fix the progress of purification as a deterministic algorithm). The computational hiding holds because of the hardness of the QSD problem, it's infeasible to tell which one it comes from. And the binding is supported by the following fact: when the mixed states by Q_0^r, Q_1^r are far enough, it is impossible for any malicious committer to

⁷ here the expectation of x is taken over the distribution of $\mathbf{S}_b(1^n)$.

convince the receiver with opening 0 and 1 as the message simultaneously. More specifically, we let A, B registers of the following state send in the commit phase, and C, D the send in the opening phase

$$|\Psi_b\rangle_{ABCD} := \sum_r \frac{|Q_0^r, Q_1^r\rangle_A \otimes PQ_b^r|0\rangle_{BC} \otimes |r\rangle_D}{2^{l/2}}$$

where PQ_b^r is the purified circuit of Q_b , and $PQ_b^r|0\rangle_{BC}$ is the purified state such that $\text{Tr}_B PQ_b^r|0\rangle_{BC}$ is the mixed state generated by Q_b . Then we can derive the implication from the average-case hardness of the QSD problem to the quantum commitment.

Theorem 4. *Assuming QSD problem is hard-on-average in quantum case, then there exists a statistical binding (sum-binding) and computational hiding quantum commitment.*

Since it is easy to see that the average-case QSD is also complete for average-case QSZK, our result actually gives a construction of quantum bit commitment from the average-case hardness of QSZK.

Oracle Separation To show the non-triviality of our constructions above, we want to show the the semi-classical QSD problem is probably not contained in QMA relative to some quantum oracle.

To show that, we adopt Aaronson's result for separating the SZK and QMA, the strategy is like that, we construct the quantum oracle \mathcal{U} which can be treated as the quantum version of the oracle corresponding to the permutation testing problem (PTP) in [2]. Then we reduce the hardness for deciding that oracle to the quantum lower bounded of the permutation testing problem, which is $q \cdot w = \Omega(2^{n/3})$ for the query number q and the length of witness w .

More specifically, the oracle $\mathcal{U} := \{U_n\}_{n \in \mathbb{N}}$ is defined as follows, we let $\mathcal{U}_n := (\mathcal{U}_n^{\mathcal{F}_n(1)}, \dots, \mathcal{U}_n^{\mathcal{F}_n(2^{n+1})})$ for each $n \in \mathbb{N}$, where each $\mathcal{U}_n^{\mathcal{F}_n(i)}$ is chosen from the Haar measure over $\mathbb{U}(2^n)$ independently for all $i \in [2^{n+1}]$. And \mathcal{F}_n is either (1) a random permutation on $\{0, 1\}^{n+1}$ or (2) a random function that differs from every permutation on at least $2^{n+1} \cdot 2/3$ coordinates with probability 1/2 of each case (here the factor 2/3 can change by other constant). Then the semi-classical QSD relative to \mathcal{U} can be construct as $U_b^{\mathcal{U}}|0, x\rangle := \mathcal{U}_n^{\mathcal{F}_n(b||x)}|0\rangle \otimes |x\rangle$, and the sampler \mathcal{S}_b is trivially the uniform distribution on $\{0, 1\}$. It's not hard to see that we can reduce that problem to the permutation testing problem. And by the property of Haar measure and the randomness of $\mathcal{F}_n(\cdot)$, we can deduce that construction is scQSD with probably 1.

Theorem 5. *There exists a quantum oracle \mathcal{U} such that $\text{scQSD}^{\mathcal{U}} \notin \text{QMA}^{\mathcal{U}}$.*

Since OWGs and quantum bit commitment can both be implemented by the average-case hardness of the scQSD problem, and the existence of pqOWFs at least requires $\text{QMA} \neq \text{BQP}$, we thus achieve these two quantum primitives with complexity assumptions probably below the world MiniQCrypt.

1.2 Related Work

Concurrent Work Few days before our paper was published online, a important work by Brakerski, Canetti and Qian also considered to establish cryptographic primitives from complexity assumption [11]. More specifically, building on the efficiently samplable, statistically far but computationally indistinguishable pairs of distributions (EFI pairs) which has been shown to be equivalent to the quantum commitment by Yan [46]. They showed that EFI pairs are necessary and sufficient for a large class of quantum-cryptographic applications including the quantum commitments schemes, oblivious transfer, and general secure multiparty computation. They also constructed EFI pairs from essentially any non-trivial quantum computationally zero-knowledge (QCZK), which overlaps with (and also stronger than) our construction of quantum commitment because $QSZK \subseteq QCZK$ and the equivalence between EFI pairs and quantum commitments schemes immediately imply the existence of quantum commitment from non-trivial QSZK by their results. However we believe our construction of quantum commitment still be of interesting because it gives a direct construction. Besides, comparing with [11], more different part is that we mainly focus on constructing the OWSGs from some specific non-trivial problem in QCZK. That is not included in [11] because it's unknown that whether EFI pairs can be used to construct the OWSGs.

Quantum Primitives below MiniQCrypt The initiated work by Ji, Liu and Song proposed the notions of PRSs and pseudorandom unitary (PRUs) [28]. They showed the implication of PRSs from the pqOWFs, and gave application on quantum money. Then Brakerski and Shmueli showed that random binary phase suffices for the indistinguishability from a Haar random state [12]. They also gave construction of scalable pseudorandom quantum states from pqOWFs in their following work [13]. Then Morimae et al. and Ananth et al. gave constructions of statistically binding and computationally hiding quantum commitment from PRSs concurrently independently [35,5], which also imply the constructions of OT and MPC according to [21,6]. Besides, Morimae and Yamakawa defined the notion of OWSGs and gave construction of one-time secure signature from it [35], and Ananth, Qian and Yuen also gave the notion of PRFSs and obtained several applications [5].

Cryptographic Primitives from Non-Triviality of (Q)SZK Ostrovsky showed that if SZK contains any hard-on-average problem, then one-way functions exist by giving a construction of distributionally OWF from it [40]. Then, Ostrovsky and Wigderson further proved the existence of a hard-on-average problem in CZK implies the existence of OWFs in infinitely-often case [41]. Ong and Vadhan studied the equivalence between CZK and instance-dependent commitments [44,39]. And a recent work by Komargodski and Yaguev implemented the distributional collision resistant hashes from the average-case hardness of SZK [30]. In quantum case, Kashefi and Kerenidis gave pqOWFs from the circuit quantum sampling (CQS) problem [29]. That induces a construction of pqOWFs from the average-case hardness of SZK because any SZK language can be reduced

to the CQS problem [4]. Then Chailloux and Kerenidis devised computationally hiding and statistically binding auxiliary-input quantum commitment schemes by the worst-case complexity assumptions such as $\text{QSZK} \not\subseteq \text{QMA}$ [14] and even much weaker assumption $\text{QIP} \not\subseteq \text{QMA}$ (with quantum advice in the commitment scheme).

Oracle Separations There are lots of works about the oracle separations related to this work, we only refer those are highly related. Aaronson and Chen defined the oracle \mathcal{O} relative to which $\text{BQP}^{\mathcal{O}} \not\subseteq \text{BPP}_{\text{path}}^{\mathcal{O}}$ and $\text{BQP}^{\mathcal{O}} \not\subseteq \text{SZK}^{\mathcal{O}}$ [1,15]. Then Aaronson showed that $\text{SZK}^{\mathcal{O}} \not\subseteq \text{QMA}^{\mathcal{O}}$ by giving a quantum lower bounded for PTP [2]. And Chailloux and Kerenidis devised computationally hiding and statistically binding auxiliary-input quantum commitment schemes by the worst-case complexity assumptions such as also separates the QSZK and QMA by a quantum oracle [14]. Menda and Watrous showed an oracle separation between QSZK and $\text{UP} \cap \text{coUP}$ [34], which the hardness of the later one yields the existence of one-way permutation in worst case [24]. As the relations between cryptographic primitives, Fischlin extended the Simon’s result [42] and devised an oracle relative to which injective trapdoor functions and one-way permutations exist, while the SZK collapses to P [16]. And due to a series of works [41,39,22], the black-box reduction from hard-on-average problems in SZK to OWPs has also been ruled out. Subsequently, Bitansky et al. showed that even the OWPs along with the indistinguishability obfuscators (and the collision-resistant hash functions) do not imply hard problems in SZK via black-box reductions [8,9]. Recently, by taking advantage of the concentration of Haar measure, Kretschmer gave a quantum oracle \mathcal{O} relative to $\text{QMA}^{\mathcal{O}} = \text{BQP}^{\mathcal{O}}$ while PRS (and even pseudorandom unitary) still exists which gives negative evidence for reducing pqOWF from PRS [31].

2 Preliminary

2.1 Notations

Here are some basic notations used later. \mathbb{N} and \mathbb{R} denote the set of positive integers and real numbers respectively. $[n]$ denotes the set of integers $\{1, 2, \dots, n\}$. Let $|x|$ denote the bit length when x is a string, or denote its size when x is a set. The mathematical expectation of a random variable X is $\mathbb{E}[X]$. A function $\text{negl}(\cdot)$ is negligible if for any $c > 0$, $\text{negl}(n) < 1/n^c$ for all sufficiently large n . We sometimes let $\text{negl}(\cdot)$ be arbitrary negligible function.

We let $\mathbb{S}(N)$ denote the N -dimensional pure quantum states, and $\mathbb{U}(N)$ be the group of $N \times N$ unitary operators. For $U \in \mathbb{U}(N)$, U^\dagger is the adjoint of U , and $I_n \in \mathbb{U}(2^n)$ is the identity map. And we let $\text{Tr}(\rho)$ be the trace of ρ , and $\text{Tr}_A(\rho)$ is the partial trace over A .

2.2 Quantum Computation

This part includes some background information on quantum computation, we assume the familiarity with basic notions, the detail may refer to [38].

For two n qubits mixed states (density matrices) ρ_0, ρ_1 , we let $\text{TD}(\rho_0, \rho_1)$ and $\text{F}(\rho_0, \rho_1)$ be trace distance and the fidelity respectively, which are defined by $\text{TD}(\rho_0, \rho_1) := \text{Tr}\sqrt{(\rho_0 - \rho_1)^\dagger(\rho_0 - \rho_1)}/2$ and $\text{F}(\rho_0, \rho_1) := \text{Tr}\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$. For pure states $|\phi_0\rangle, |\phi_1\rangle$, we denote by $\text{TD}(|\phi_0\rangle, |\phi_1\rangle)$ and $\text{F}(|\phi_0\rangle, |\phi_1\rangle)$ the trace distance and fidelity of $|\phi_0\rangle\langle\phi_0|, |\phi_1\rangle\langle\phi_1|$ for simplicity. Then the following two lemmas are used widely in this paper.

Lemma 2 (Uhlmann's theorem). *For any pair of states ρ_0 and ρ_1 , let $|\phi_0\rangle$ and $|\phi_1\rangle$ denote the purifications of ρ_0 and ρ_1 respectively. The fidelity $\text{F}(\cdot)$ between ρ_0 and ρ_1 can be given by*

$$\text{F}(\rho_0, \rho_1) = \max_{|\phi_0\rangle, |\phi_1\rangle} |\langle\phi_0|\phi_1\rangle|. \quad (1)$$

Where the maximization is taken over all purifications $|\phi_0\rangle, |\phi_1\rangle$.

Lemma 3 (Fuchs-van de Graaf inequalities). *For any pair of states ρ_0 and ρ_1 , we have*

$$1 - \text{F}(\rho_0, \rho_1) \leq \text{TD}(\rho_0, \rho_1) \leq \sqrt{1 - \text{F}(\rho_0, \rho_1)^2}. \quad (2)$$

Where $\text{TD}(\cdot)$ is the trace distance.

A quantum algorithm quantum algorithm \mathcal{A} is a collection of quantum circuits $\{\mathcal{A}_n\}_{n>0}$, and it's quantum polynomial-time (QPT) if it's running time is bounded by some polynomial. And we say \mathcal{A} is uniform QPT algorithm if $\{\mathcal{A}_n\}_{n>0}$ is polynomial-time uniform family of quantum circuits, which means there a polynomial time deterministic Turing machine $M(1^n)$ outputs \mathcal{A}_n for each $n \in \mathbb{N}$. Without specific mention, the situations we considered in this work are all uniform.

Moreover, we denote by PQ a purification of the corresponding general quantum circuit Q which simulates the functionality of Q and satisfies the unitary property simultaneously. The existence of such simulation has been justified in [3], by allowing PQ to add some additional ancillary qubits (which can be initialized as $|0\rangle$) as its input and tracing-out the residual (or garbage) qubits. This simulation of circuit purification can always be done efficiently.

2.3 Average-Case Hardness of QSZK

The hardness of QSZK can be captured by its complete problem, the quantum state distinguishability (QSD) problem. Let ρ_0 and ρ_1 denote the mixed state obtained by running Q_0 and Q_1 on state $|0\rangle$ and discarding (tracing out) the non-output qubits. Then the quantum state distinguishability is defined as follows.

Definition 1 (Quantum State Distinguishability (QSD)). *Given a pair of quantum circuits $Q_0, Q_1 \in \{0, 1\}^n$, and ρ_0, ρ_1 denote the states produced by Q_0, Q_1 respectively, which are promised either $\text{TD}(\rho_0, \rho_1) > 2/3$ or $\text{TD}(\rho_0, \rho_1) < 1/3$, the problem is to decide which is the case.*

Note that the parameters $1/3$ and $2/3$ are optional, we can be replaced by 2^{-n} and $1 - 2^{-n}$ according to the technique for manipulating the trace distance [45]. Therefore we usually adopt the parameters of the QSD problem as 2^{-n} and $1 - 2^{-n}$ in the following text. For the sake of simplicity, we introduce the following notations

$$\text{QSD}_1 := \{(Q_0, Q_1) \mid \text{TD}(\rho_0, \rho_1) > 1 - 2^{-n}\},$$

$$\text{QSD}_0 := \{(Q_0, Q_1) \mid \text{TD}(\rho_0, \rho_1) < 2^{-n}\}.$$

Then let $\text{QSD} := (\text{QSD}_1, \text{QSD}_0)$.

Similar as the notion of average-case hardness of statistical distance problem in [30,9], which is known as a SZK complete promise problem, we formalize the average-case hardness of QSD problem as follows.

Definition 2 (Average-Case Hardness of QSD). *For a promise problem $\text{QSD} := (\text{QSD}_1, \text{QSD}_0)$, it is quantum hard-on-average if there exists an efficient sampler $\mathcal{S}(1^n)$ of QSD such that any QPT adversary \mathcal{A} can not distinguish an instance generated from $\mathcal{S}(1^n)$ with non-negligible advantage, namely it holds that*

$$\Pr[\mathcal{A}(Q_0, Q_1) = b, (Q_0, Q_1) \in \text{QSD}_b : (Q_0, Q_1) \leftarrow \mathcal{S}(1^n)] \leq \frac{1}{2} + \text{negl}(n) \quad (3)$$

for some negligible function $\text{negl}(\cdot)$.

Note that, when we assume the average-case hardness of QSD, it holds that

$$\frac{1}{2} - \text{negl}(n) \leq \Pr[(Q_0, Q_1) \in \text{QSD}_0 : (Q_0, Q_1) \leftarrow \mathcal{S}(1^n)] \leq \frac{1}{2} + \text{negl}(n)$$

for some negligible function $\text{negl}(\cdot)$ (otherwise there is a trivial distinguisher breaks the average-case hardness for infinitely many $n \in \mathbb{N}$). Therefore an equivalent definition of the average-case hardness of QSD can be defined as the non-existence of QPT adversary \mathcal{A} such that

$$\begin{aligned} & |\Pr[\mathcal{A}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathcal{S}(1^n) \mid (Q_0, Q_1) \in \text{QSD}_0] \\ & - \Pr[\mathcal{A}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathcal{S}(1^n) \mid (Q_0, Q_1) \in \text{QSD}_1]| \leq \text{negl}(n) \end{aligned} \quad (4)$$

for some negligible function $\text{negl}(\cdot)$. Sometimes, we denote by $\mathcal{S}(r) = (Q_0^r, Q_1^r)$ the progress of $\mathcal{S}(1^n)$ when we specify the internal random number $r \leftarrow \{0, 1\}^{\ell(n)}$.

Moreover, due to the reduction by Watrous [45], it is easy to see that the average-case QSD is also complete for average-case QSZK, which means any construction from the average-case hardness of QSD could be changed into a construction from any hard-on-average language in QSZK.

2.4 One-Way Quantum State Generator and Its Variants

In this part, we will introduce the notion of one-way quantum state generator (OWSG) by Morimae and Yamakawa [35], and gives its variants. To describe the strong (weak) one-way quantum state generator, we firstly gives a generalized version of OWSG which we call it $\varepsilon(n)$ -OWSG.

Definition 3 ($\varepsilon(n)$ -OWSG). Let \mathbf{f} be a QPT algorithm that takes a string $x \in \{0,1\}^n$ as its input, and outputs a state $|\phi_x\rangle_Y \otimes |\eta_x\rangle_Z$ where the registers Y stores the output state and Z stores the ancilla state⁸. For any QPT adversary \mathcal{A} , we consider the following experiment $\text{Exp}_{\mathcal{A}}^{\text{owsg}}(n)$:

- The challenger generates $x \leftarrow \mathcal{D}(1^n)$ by some sampleable $\mathcal{D}(1^n)$, then runs $\mathbf{f}(x) \rightarrow |\phi_x\rangle \otimes |\eta_x\rangle$ about $t(n)$ times and sends the resulting state to \mathcal{A} , where $t(n)$ is a polynomial of n , and we denote by t for simplicity when there is no confusion.
- \mathcal{A} receives the state $|\phi_x\rangle^{\otimes t}$ and outputs a guess x' .
- The challenger measures the state $|\phi_{x'}\rangle$ by $\{|\phi_x\rangle\langle\phi_x|, I - |\phi_x\rangle\langle\phi_x|\}$ and returns 1 if the measurement is $|\phi_x\rangle$, and returns 0 otherwise⁹.

Let $\text{Exp}_{\mathcal{A}}^{\text{owsg}}(n) = 1$ when the measurement is $|\phi_x\rangle$, and $\text{Exp}_{\mathcal{A}}^{\text{owsg}}(n) = 0$ otherwise. \mathbf{f} is called $\varepsilon(n)$ -one-way state generator ($\varepsilon(n)$ -OWSG) on $\mathcal{D}(1^n)$ if

$$\Pr_{x \leftarrow \mathcal{D}(1^n)} [\text{Exp}_{\mathcal{A}}^{\text{owsg}}(n) = 1] \leq \varepsilon(n) \quad (5)$$

for some function $\varepsilon(\cdot)$. And sometimes we denote the event as $\text{Exp}_{\mathcal{A}}^{\text{owsg}}(n)$ for convenience when there is an explicit \mathbf{f} .

When $\varepsilon(\cdot)$ is a negligible function, the definition of $\varepsilon(n)$ -OWSG is exactly the OWSG defined in [35], and we call it the *strong one-way quantum state generator* (strong OWSG) sometimes for clarity. On the other hand, when $\varepsilon(n) = 1 - 1/n^c$ for some constant $c > 0$, we call it the *weak one-way quantum state generator* (weak OWSG).

Note that the original notion of strong (weak) OWSG is hard to capture, so here we give an equivalent definition by the trace distance. We let $\rho_{\mathcal{A},t}^{|\phi_x\rangle} = \text{Tr}_{N\mathcal{A}}(|\phi_x\rangle^{\otimes t})$ be the mixed state after tracing out all the non-output registers by \mathcal{A} with $|\phi_x\rangle^{\otimes t}$ as input¹⁰. Then it holds that

$$\begin{aligned} \mathbb{E}_x [\text{TD}(|\phi_x\rangle\langle\phi_x|, \text{Tr}_{X,Z} \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}))] &\leq \mathbb{E}_x \left[\sqrt{1 - \text{F}(|\phi_x\rangle\langle\phi_x|, \text{Tr}_{X,Z} \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}))^2} \right] \\ &\leq \sqrt{\mathbb{E}_x [1 - \text{F}(|\phi_x\rangle\langle\phi_x|, \text{Tr}_{X,Z} \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}))^2]} \\ &\leq \sqrt{1 - \mathbb{E}_x [\langle\phi_x| \text{Tr}_{X,Z} \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}) |\phi_x\rangle]} \\ &= \sqrt{1 - \Pr_x [\text{Exp}_{\mathcal{A}}^{\text{owsg}}(n) = 1]}. \end{aligned}$$

⁸ In this general definition, $|\eta_x\rangle$ is the garbage part which is not non-entangled with $|\phi_x\rangle$, the reason for that is explained in [35].

⁹ If we consider $\mathbf{f}(x)$ as a unitary operator that takes $|0\rangle$ as input, and outputs $|\phi_x\rangle \otimes |\eta_x\rangle$, then this process can be achieved by invoking the $\mathbf{f}(x)^\dagger$ to $|\phi_{x'}\rangle$.

¹⁰ Without loss of generality, we can assume $\text{Tr}_z \mathcal{A}(|\phi_x\rangle\langle\phi_x|^{\otimes t})$ has the form $\sum p_z |x\rangle\langle x|$ because we can “measure” these x by performing the CNOT on those x to an additional auxiliary part before tracing out. And $\mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle})$ denotes the unitary process from $\rho_{\mathcal{A},t}^{|\phi_x\rangle} |0\rangle\langle 0|$ to $\sum p_z |x\rangle\langle x| \otimes |\phi_x, \eta_x\rangle\langle\phi_x, \eta_x|$.

On the other hand,

$$\begin{aligned} \mathbb{E}_x [\text{TD}(|\phi_x\rangle\langle\phi_x|, \text{Tr}_{X,Z} \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}) &\geq \mathbb{E}_x [1 - \text{F}(|\phi_x\rangle\langle\phi_x|, \text{Tr}_{X,Z} \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}) & \\ &\geq 1 - \sqrt{\mathbb{E}_x [\langle\phi_x| \text{Tr}_{X,Z} \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}) |\phi_x\rangle]} & \\ &= 1 - \sqrt{\Pr_x[\text{Exp}_{\mathcal{A}}^{\text{owsg}}(n) = 1]}. \end{aligned}$$

Therefore $\varepsilon(\cdot)$ is negligible (or $1 - 1/n^c$ for some $c > 0$), iff the trace distance between $|\phi_x\rangle\langle\phi_x|$ and $\text{Tr}_Z \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle})$ is negligible (or $1 - 1/n^{c'}$ for some $c' > 0$) that hence derive the equivalent definition of strong (weak) OWSG. We call the strong OWSG the OWSG for convenience when there is no confusion. Then we give the definition of distributionally one-way quantum state generator which is also characterized by the trace distance as follows.

Definition 4 (Distributionally OWSG). *Let \mathbf{f} be a QPT algorithm that takes a string $x \in \{0, 1\}^n$ as its input, and outputs a state $|\phi_x\rangle_Y \otimes |\eta_x\rangle_Z$. Then \mathbf{f} is called distributionally one-way quantum state generator (OWSG) on sampleable $\mathcal{D}(1^n)$, if for any QPT adversary \mathcal{A} in the experiment $\text{Exp}_{\mathcal{A}}^{\text{owsg}}(n)$ (which is defined in Definition 3) it holds that*

$$\text{TD}(\mathbb{E}_x |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_x \rho_{\mathcal{A},t}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|) \geq \frac{1}{n^c}$$

for some constant $c > 0$. The expected value \mathbb{E}_x is taken over the distribution of $\mathcal{D}(1^n)$, and $\rho_{\mathcal{A},t}^{|\phi_x\rangle} = \text{Tr}_N \mathcal{A}(|\phi_x\rangle^{\otimes t})$ be the mixed state after tracing out all the non-output registers by \mathcal{A} with $|\phi_x\rangle^{\otimes t}$ as input.

3 The Equivalence between Variants of OWSGs

In this section, we show the equivalence among these three kinds of OWSGs. Firstly, we show the equivalence between weak OWSG and strong OWSG.

Theorem 6. *The existence of weak OWSG and strong OWSG are equivalent.*

Proof. Note that the strong OWSG implies the weak OWSG trivially. Therefore the rest of this proof aims to show the other direction. Here we adopt Yao's original construction. Let \mathbf{f} be a weak OWSG on distribution $\mathcal{D}(1^n)$, satisfying the event $\text{Exp}_{\mathcal{B}}^{\text{owsg}}(n) = 1$ occurs with probability at most $1 - 1/q(n)$ for some positive polynomial $q(\cdot)$ and any QPT adversary \mathcal{B} . Then for some suitable polynomial $m(n)$ (which is determined by $q(n)$), the following construction of \mathbf{f}' is strong OWSG:

$$\mathbf{f}'(x_1, \dots, x_m) = \otimes_{i=1}^m |\phi_{x_i}\rangle_Y^{\otimes nq(n)} \otimes_{i=1}^m |\eta_{x_i}\rangle_Z^{\otimes nq(n)} \quad (6)$$

The strategy of proof is very similar to its classical counterpart [17]. So here we only give a sketch to note the different part, and leave the detailed proof in

supplementary materials A.1. Assuming \mathcal{A} breaks the strong one-wayness of \mathbf{f}' then for a random challenge state $\otimes_{i=1}^m |\phi_{x_i}\rangle^{\otimes nq(n)}$, the probability that \mathcal{A} would output (x'_1, \dots, x'_m) satisfying $\prod_{i=1}^m |\langle \phi_{x_i} | \phi_{x'_i} \rangle|^{2nq(n)} \geq 1/2mp(n)$ is noticeable. Therefore, for a challenge state $|\phi_{x^*}\rangle$ of \mathbf{f} , we just embed it into $\otimes_{i=1}^m |\phi_{x_i}\rangle^{\otimes nq(n)}$ for some random position $j \in [m]$. Then give this state to \mathcal{A} and repeat it for polynomial many times. We can hence prove that \mathcal{A} would output x'_j satisfying $|\langle \phi_{x^*} | \phi_{x'_{j_0}} \rangle|^2 \geq (1/2mp(n))^{1/nq(n)}$ with overwhelming probability. By Chernoff bound, such x'_j can be detected with overwhelming probability by measuring $|\phi_x\rangle$ with $\{|\phi_{x'_j}\rangle\langle \phi_{x'_j}|, I - |\phi_{x'_j}\rangle\langle \phi_{x'_j}|\}$ for polynomial many times.

Then we give the equivalence between distributionally OWSG and weak OWSG by the following theorem.

Theorem 7. *The existence of distributionally OWSG and weak OWSG are equivalent.*

Proof. It is easy to derive the distributionally one-wayness from the weak one-wayness, since the distance is invariant under unitary operator, it holds that

$$\begin{aligned}
 & \text{TD}\left(\mathbb{E}_x |x\rangle\langle x| \otimes |\phi_x\rangle\langle \phi_x|, \mathbb{E}_x \rho_{\mathcal{A},t}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle \phi_x|\right) \\
 &= \text{TD}\left(\mathbb{E}_x |x\rangle\langle x| \otimes |\phi_x\rangle\langle \phi_x| \otimes |\phi_x\rangle\langle \phi_x|, \mathbb{E}_x \text{Tr}_Z \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}) \otimes |\phi_x\rangle\langle \phi_x|\right)
 \end{aligned}$$

Where $\mathbf{f}(|x\rangle)$ denotes the operator that outputs $|x\rangle \otimes |\phi_x\rangle$. Since \mathbf{f} is weak OWSG such that

$$\mathbb{E}_x \left[\langle \phi_x | \text{Tr}_{X,Z}(\mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle})) | \phi_x \rangle \right] = \Pr_x[\text{Exp}_{\mathcal{A}}^{owsq}(n) = 1] \leq 1 - \frac{1}{n^c} \quad (7)$$

for some constant $c > 0$. Note that without loss of generality, we can assume $\rho_{\mathcal{A},t}^{|\phi_x\rangle}$ has the form $\sum_x p_x |x\rangle\langle x|$ (because we can “measure” these x by performing the CNOT on those x then tracing out it). Then if we denote by \mathbf{G} the collection of “good” x such that $\mathbf{G} := \{x \mid \langle \phi_x | \text{Tr}_{X,Z}(\mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle})) | \phi_x \rangle \leq 1 - 1/2 \cdot n^c\}$. According

to (7) we have $\sum_x^{x \in \mathbf{G}} p_x \geq \frac{1}{2 \cdot n^c}$. That hence implies

$$\begin{aligned}
& \text{TD} \left(\mathbb{E}_x |x\rangle\langle x| \otimes |\phi_x\rangle\langle \phi_x| \otimes |\phi_x\rangle\langle \phi_x|, \mathbb{E}_x \text{Tr}_Z \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}) \otimes |\phi_x\rangle\langle \phi_x| \right) \\
& \geq \text{TD} \left(\mathbb{E}_x |\phi_x\rangle\langle \phi_x| \otimes |\phi_x\rangle\langle \phi_x|, \mathbb{E}_x \text{Tr}_{X,Z} \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}) \otimes |\phi_x\rangle\langle \phi_x| \right) \\
& = \text{TD} \left(\mathbb{E}_x \text{SWAP}(|\phi_x\rangle\langle \phi_x| \otimes |\phi_x\rangle\langle \phi_x| \otimes |0\rangle\langle 0|) \right. \\
& \quad \left. , \mathbb{E}_x \text{SWAP}(\text{Tr}_{X,Z} \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}) \otimes |\phi_x\rangle\langle \phi_x| \otimes |0\rangle\langle 0|) \right) \\
& \geq \text{Tr} \left(\mathbb{E}_x \left(\frac{1 - \langle \phi_x | \text{Tr}_{X,Z} \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}) | \phi_x \rangle}{2} \right) \right) \\
& \geq \text{Tr} \left(\sum_x^{x \in \mathbf{G}} p_x \left(\frac{1 - \langle \phi_x | \text{Tr}_{X,Z} \mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}) | \phi_x \rangle}{2} \right) \right) \\
& \geq \frac{1}{2 \cdot n^c} \cdot \left(\frac{1}{4 \cdot n^c} \right) = \frac{1}{8 \cdot n^{2c}}.
\end{aligned}$$

Where SWAP is the swap test for the first two parts, and stores the result in the additional qubit $|0\rangle$. That hence justify the implication from weak OWSGs to distributionally OWSGs.

Therefore the remaining part of this proof is to construct weak OWSG from distributionally OWSG. Here we adopt the construction by Impagliazzo and Luby. Assuming $\mathbf{f}(x) \rightarrow |\phi_x\rangle \otimes |\eta_x\rangle$ is distributionally OWSG such that for any efficient quantum adversary \mathcal{A} , it holds that

$$\mathbb{E}_x [\mathbf{F}(\rho_x \otimes |\phi_x\rangle\langle \phi_x|, \rho_{\mathcal{A},t}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle \phi_x|)] \leq 1 - \frac{1}{\mathbf{p}(n)}$$

for some positive polynomial $\mathbf{p}(\cdot)$ when $n \in \mathbb{N}$ is sufficiently large. Then we construct \mathbf{f}' as follows:

$$\mathbf{f}'(x, h_k, k) \rightarrow |\psi_{x, h_k, k}\rangle \otimes |\eta_x\rangle := |\phi_x, h_k(x), h_k, k\rangle \otimes |\eta_x\rangle \quad (8)$$

where $h_k : \{0, 1\}^n \rightarrow \{0, 1\}^k$ is a universal hash function, and $k \leq n + O(\log n)$.

Before we give the proof, we firstly introduce a notion of *polarization*, we say \mathbf{f} is (k, p) -polarized if for any $x, x' \in \{0, 1\}^n$, either $|\langle \phi_{x'} | \phi_x \rangle|^k \geq 1 - p(n)$ or $|\langle \phi_{x'} | \phi_x \rangle|^k \leq p(n)$. Then we the following lemma shows that the polarization property for any \mathbf{f} which is not weak OWSG.

Lemma 4. *If \mathbf{f} is not a weak one-way state generator, and assuming \mathcal{A} is the corresponding adversary using $t(n)$ copies (denoted as t in brief sometimes). Let $I_n(\delta)$ be the collection of x such that \mathcal{A} accept with probability at least $1 - \delta$*

$$I_n(\delta) := \{x' \mid \Pr_x [\text{Exp}_{\mathbf{f}, \mathcal{A}}^{owsq}(n) = 1 \mid x = x'] > 1 - \delta\}.$$

Then for any positive polynomial $\text{poly}(\cdot)$, \mathbf{f} is $(2t, 1/\text{poly}(n))$ -polarized on $I_n(1/(4\text{poly}(n)t(n))^2)$.

Due to the limitation of space, we remove the proof of Lemma 4 to the supplementary materials A.2.

Note that Lemma 4 indicates that for any polynomial $\text{poly}(\cdot)$, and $x_0, x_1 \in I_n(1/16\text{poly}(n)^{2t}(n)^2)$, either

$$\text{TD}(|\phi_{x_0}\rangle, |\phi_{x_1}\rangle) \leq \sqrt{1 - \left(1 - \frac{1}{\text{poly}(n)}\right)^{\frac{1}{t}}}, \text{ or } \text{TD}(|\phi_{x_0}\rangle, |\phi_{x_1}\rangle) \geq \sqrt{1 - \left(\frac{1}{\text{poly}(n)}\right)^{\frac{1}{t}}}.$$

Hence we can construct a family of pairwise disjointed collections $\{\mathbf{N}_x^{2t}(1/\mathfrak{p}(n))\}_{x \in X}$ covering all elements in $I_n(1/16\text{poly}(n)^{2t}(n)^2)$, where

$$\mathbf{N}_x^{2t}(1/\mathfrak{p}(n)) := \{x' \mid |\langle \phi_{x'} | \phi_x \rangle|^{2t} \geq 1 - 1/\mathfrak{p}(n)\}.$$

The strategy for generating that collection is simple, we just find an x which are not contained in the former union $\cup_{x \in X} \mathbf{N}_x^{2t}(1/\mathfrak{p}(n))$ and add those x in X recursively, until any element of $I_n(1/16\text{poly}(n)^{2t}(n)^2)$ has been included. Therefore the collections in $\{\mathbf{N}_x^{2t}(1/\mathfrak{p}(n))\}_{x \in X}$ cover all elements in $I_n(1/16\text{poly}(n)^{2t}(n)^2)$. To prove it's pairwise disjointed, assuming there exist $x, x' \in X$ such that

$$\mathbf{N}_x^{2t}(1/\text{poly}(n)) \cap \mathbf{N}_{x'}^{2t}(1/\text{poly}(n)) \neq \emptyset$$

Then it holds that

$$\begin{aligned} \sqrt{1 - \left(1 - \frac{1}{\text{poly}(n)}\right)^{\frac{1}{t}}} &\leq \text{TD}(|\phi_{x_j}\rangle, |\phi_{x_j}\rangle) \leq 2\sqrt{1 - \left(1 - \frac{1}{\text{poly}(n)}\right)^{\frac{1}{t}}} \\ &< \sqrt{1 - \left(\frac{1}{\text{poly}(n)}\right)^{\frac{1}{t}}} \end{aligned}$$

which is contradictory to that lemma 4.

Then we back to the proof of Theorem 7. We show \mathbf{f}' satisfies the weak one-wayness by making a contradiction. Assuming there is an adversary \mathcal{A} breaks the weak one-wayness of \mathbf{f}' (with t copies input states), namely

$$\Pr_{x, h_k, k} [\text{Exp}_{\mathbf{f}', \mathcal{A}}^{owsq}(n) = 1] > 1 - \text{negl}(n) \quad (9)$$

for infinitely many $n \in \mathbb{N}$ with some negligible function $\text{negl}(\cdot)$. Then we construct an adversary \mathcal{B} breaks the distributionally one-wayness of \mathbf{f} as follows:

- \mathcal{B} takes as input a challenge state $|\phi_{x^*}\rangle^{\otimes t'}$ where $t' = (n^3 + n) \cdot m \cdot t$, it then repeats the follow steps from $k = n + C \cdot \log n$ to $k = C \cdot \log n$ (here $C > 1$ is a constant that will be determined later):
 - \mathcal{B} generates h_k and then chooses $r_k \leftarrow \{0, 1\}^k$ uniformly at random.
 - \mathcal{B} invokes \mathcal{A} with input $|\phi_x, r_k, h_k, k\rangle^{\otimes t}$ and get x' as measurement, then checks if $\mathbf{f}^\dagger(x')|\phi_{x^*}\rangle|\eta_{x'}\rangle$ equals to 0 for $n^2 \cdot t$ times ¹¹, if all the $n^2 \cdot t$

¹¹ Here $\mathbf{f}(x')$ denotes the unitary operator that takes $|0\rangle$ as input state and outputs $|\phi_{x'}, \eta_{x'}\rangle$, it is equivalent to measure it with $\{|\phi_{x'}\rangle\langle\phi_{x'}|, I - |\phi_{x'}\rangle\langle\phi_{x'}|\}$.

measurements are 0, \mathcal{B} would accept that output x' and stop. Otherwise, it repeats that step with a new generated random h_k, r_k about m times until finds some x' , if it still fails to find such x' , it would continue to the round $k - 1$.

- If \mathcal{B} doesn't find an acceptable output in the iterations above until $k = C \cdot \log n$, it would output \perp .

Note that some part of \mathcal{B} is described in classical setting, but it's equivalent to analyze it as a unitary one (such as replacing $|\phi_x, r_k, h_k, k\rangle$ for a random r_k by the state $\sum_{r_k} |r_k\rangle \otimes |\phi_x, r_k, h_k, k\rangle / 2^{-l/2}$). So here we still use $\rho_{\mathcal{B}, t'}^{|\phi_x\rangle}$ to denote the corresponding output (mixed) state by \mathcal{B} after tracing out the non-output part.

Then the strategy for proving this part is as follows. Since \mathbf{f} is distributional one-way, there should exist a positive polynomial $q(\cdot)$ such that

$$F\left(\mathbb{E}_x |x\rangle\langle x| \otimes |\phi_x\rangle\langle \phi_x|, \mathbb{E}_x \rho_{\mathcal{B}, t'}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle \phi_x|\right) \leq 1 - \frac{1}{q(n)}$$

for any QPT adversary \mathcal{B} . Then, we are going to show that, if \mathbf{f}' is not weak one-way, then the adversary \mathcal{B} constructed above should satisfy

$$1 - \frac{1}{q(n)} < F\left(\mathbb{E}_x |x\rangle\langle x| \otimes |\phi_x\rangle\langle \phi_x|, \mathbb{E}_x \rho_{\mathcal{B}, t'}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle \phi_x|\right),$$

which will lead a contradiction.

For that purpose, before estimating the output distribution for each challenge state each challenge state $|\phi_x\rangle$, we firstly introduce a classification of the input space according to the polarization.

Since \mathcal{A} breaks the weak one-wayness of \mathbf{f}' , it's not hard to see that \mathcal{A} also breaks the weak one-wayness of \mathbf{f} , which indicates \mathbf{f} is $(2t, 1/p(n))$ -polarized on $I_n(1/16p(n)^2 t(n)^2)$ for any positive polynomial $p(\cdot)$. Then according to the discussion before, we can derive a family of disjointed collections $\{\mathbf{N}_x^{2t}(1/p(n))\}_x$ that covering the $I_n(1/16p(n)^2 t(n)^2)$.

Then we choose a subset of those $\{\mathbf{N}_x^{2t}(1/p(n))\}_x$ (and to denote it by $\{\mathbf{G}_{x_1}, \dots, \mathbf{G}_{x_l}\}$ for convenience), such that

$$(1 + 1/p(n))|\mathbf{G}_{x_i}| > |\{x \mid \text{TD}(|\phi_{x_i}\rangle, |\phi_x\rangle) \leq \sqrt{1 - (\frac{1}{p(n)})^{\frac{1}{t}}/2}\}|,$$

for each $i = 1, \dots, l$. It's easy to see that those sets $\{x \mid \text{TD}(|\phi_{x_i}\rangle, |\phi_x\rangle) \leq \sqrt{1 - (1/p(n))^{\frac{1}{t}}/2}\}, \dots, \{x \mid \text{TD}(|\phi_{x_l}\rangle, |\phi_x\rangle) \leq \sqrt{1 - (1/p(n))^{\frac{1}{t}}/2}\}$ are pairwise disjointed.

Moreover, since we assume \mathcal{A} breaks the weak one-wayness of \mathbf{f} , it's easy to see that $|I_n(1/16p(n)^2 t(n)^2)| \geq 2^n \cdot (1 - \text{negl}(n))$ for some negligible function $\text{negl}(\cdot)$. Therefore some suitable $\{\mathbf{G}_{x_1}, \dots, \mathbf{G}_{x_l}\}$ can be chosen such that the union of those \mathbf{G}_{x_i} are also overwhelming to the domain, namely, if we let

$$I'_n := \bigcup_i \mathbf{G}_{x_i},$$

then $|I'_n| > 2^n \cdot (1 - \text{negl}'(n))$ for some negligible function $\text{negl}'(\cdot)$ (otherwise, since $p(\cdot)$ is a positive polynomial, it would also be contradictory to the assumption that \mathbf{f} is not weak OWSG).

According to that classification, we divide the input space into these disjointed collections $\mathbf{G}_{x_1}, \dots, \mathbf{G}_{x_l}$. By the convexity of the fidelity, we have ¹²

$$\begin{aligned} & \mathbb{F}\left(\mathbb{E}_x |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_x \rho_{\mathcal{B},t'}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|\right) \\ & \geq (1 - \text{negl}(n)) \cdot \mathbb{F}\left(\mathbb{E}_{x \in I'_n} |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_{x \in I'_n} \rho_{\mathcal{B},t'}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|\right) \\ & \geq (1 - \text{negl}(n)) \cdot \sum_{i=1}^l \frac{|\mathbf{G}_{x_i}|}{2^n} \cdot \mathbb{F}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B},t'}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|\right). \end{aligned}$$

Then it's sufficient to consider the lower bound for each \mathbf{G}_{x_i} . For each \mathbf{G}_{x_i} , we can further derive that.

$$\begin{aligned} & \mathbb{F}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B},t'}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|\right) \\ & \geq 1 - \text{TD}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B},t'}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|\right). \end{aligned}$$

Due to the Triangle inequality of the trace distance, it holds that

$$\begin{aligned} & \text{TD}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B},t'}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|\right) \\ & \leq \text{TD}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_{x_i}\rangle\langle\phi_{x_i}|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B},t'}^{|\phi_x\rangle} \otimes |\phi_{x_i}\rangle\langle\phi_{x_i}|\right) \quad (10) \\ & \quad + \text{TD}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B},t'}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B},t'}^{|\phi_x\rangle} \otimes |\phi_{x_i}\rangle\langle\phi_{x_i}|\right) \\ & \quad + \text{TD}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_{x_i}\rangle\langle\phi_{x_i}|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|\right). \end{aligned}$$

Then we can estimate the unwanted two parts of (10) as follows

$$\begin{aligned} & \text{TD}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B},t'}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B},t'}^{|\phi_x\rangle} \otimes |\phi_{x_i}\rangle\langle\phi_{x_i}|\right) \\ & \leq \sqrt{1 - \mathbb{F}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_{x_i}\rangle\langle\phi_{x_i}|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|\right)^2} \\ & \leq \sqrt{1 - \left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} \mathbb{F}(|x\rangle\langle x| \otimes |\phi_{x_i}\rangle\langle\phi_{x_i}|, |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|)\right)^2} \\ & \leq \sqrt{1 - \left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} \mathbb{F}(|\phi_{x_i}\rangle\langle\phi_{x_i}|, |\phi_x\rangle\langle\phi_x|)\right)^2} \leq \sqrt{1 - \left(1 - \frac{1}{p(n)}\right)^{\frac{1}{t}}} \leq \sqrt{\frac{1}{p(n)}}. \end{aligned}$$

¹² Here for simplicity, we assume the distribution of x is the uniform distribution on $\{0, 1\}^n$, it's easy to extend that result to a general distribution.

Similar, we have

$$\text{TD}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_{x_i}\rangle\langle\phi_{x_i}|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|\right) \leq \sqrt{\frac{1}{\mathbf{p}(n)}}.$$

Therefore, the inequality (10) becomes

$$\begin{aligned} & \mathbb{F}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B}, t'}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|\right) \quad (11) \\ & \geq 1 - \text{TD}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_{x_i}\rangle\langle\phi_{x_i}|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B}, t'}^{|\phi_x\rangle} \otimes |\phi_{x_i}\rangle\langle\phi_{x_i}|\right) - 2 \cdot \sqrt{\frac{1}{\mathbf{p}(n)}} \\ & \geq 1 - \text{TD}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B}, t'}^{|\phi_x\rangle}\right) - 2 \cdot \sqrt{\frac{1}{\mathbf{p}(n)}}. \end{aligned}$$

That implies it's sufficient to consider the trace distance between $\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x|$ and $\mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{B}, t'}^{|\phi_x\rangle}$. We now estimate the trace distance above that by showing the probability that \mathcal{B} outputs x is not far from $1/|\mathbf{G}_{x_i}|$ for any $x \in \mathbf{G}_{x_i}$, and for other $x \notin \mathbf{G}_{x_i}$ the that \mathcal{B} accepts and outputs those x only with small probability. We divide these into two claims. The first one gives a lower bound of the success probability of \mathcal{B} in each repetition, and says that \mathcal{B} would succeed with overwhelming probability.

Claim 1. For a given challenge state $|\phi_{x^*}\rangle$, where $x^* \in \mathbf{G}_{x_i}$, let p_k be the probability that \mathcal{B} accepts at one repetition of k -th round, then for $k \in [n + C \cdot \log n, \log |\mathbf{G}_{x_i}| + C \cdot \log n]$, it holds that

$$p_k \geq \left(1 - \frac{n^2 \cdot t(n)}{\mathbf{p}(n)} - \frac{5}{4 \cdot \mathbf{p}(n)}\right) \cdot \frac{|\mathbf{G}_{x_i}|}{2^k} \quad (12)$$

We have

$$\Pr[\mathcal{B} \text{ accepts} \wedge k \geq \log |\mathbf{G}_{x_i}| + C \cdot \log n] \geq 1 - \exp(-n), \quad (13)$$

namely, the probability that \mathcal{B} accepts for some $k \geq \log |\mathbf{G}_{x_i}| + C \cdot \log n$ is at least $1 - \exp(-n)$ when $m \geq 2n^{C+1}$.

Then the Claim 2 indicates that when \mathcal{B} accept, the output would follow a “nearly uniform” distribution on \mathbf{G}_{x_i} .

Claim 2. For a given challenge state $|\phi_{x^*}\rangle$, where $x^* \in \mathbf{G}_{x_i}$, $p_{k,x}$ denotes the probability that \mathcal{B} accepts with the measurement x from \mathcal{A} at one repetition, then the following three facts hold.

1. For any $x \in I_n \setminus \mathbf{G}_{x_i}$, the probability that \mathcal{B} accepts with the measurement x it is at most $p_{k,x} < \mathbf{p}(n)^{-n^2}$.

2. For any $x \in \mathbf{G}_{x_i}$, and $k \geq \log |\mathbf{G}_{x_i}| + C \cdot \log n$ for some suitable $C > 0$, it holds that

$$\frac{(1 - n^{-2C} - (2 + t(n) \cdot n^2)/\mathbf{p}(n))}{2^k} \leq p_{k,x} \leq 1/2^k$$

3. For any $x \in \{x \mid \text{TD}(|\phi_{x_i}\rangle, |\phi_x\rangle) > \sqrt{1 - (1/\mathbf{p}(n))^{1/t(n)}/2}\} \setminus I_n$, the probability that \mathcal{A} output it is at most $p_{k,x} < \exp(-n^2/16)$

The proof of Claim 1 and Claim 2 may refer to the supplementary materials A.3 and A.4.

Let \mathbf{B}_{x_i} denote the collection of “bad” x which are not “highly invertible” but “close” to x_i , namely

$$\mathbf{B}_{x_i} := \left\{ x \mid \text{TD}(|\phi_{x_i}\rangle, |\phi_x\rangle) \leq \sqrt{1 - \left(\frac{1}{\mathbf{p}(n)}\right)^{\frac{1}{t(n)}/2}} \right\} \setminus \mathbf{G}_{x_i}.$$

Then by the definition of \mathbf{G}_i , we have $|\mathbf{B}_{x_i}| \leq |\mathbf{G}_{x_i}| \mathbf{p}(n)^{-1}$ the probability that \mathcal{B} accepts conditioned on the measurement by \mathcal{A} belongs to \mathbf{B}_{x_i} at one repetition is at most $|\mathbf{G}_{x_i}| \mathbf{p}(n)^{-1} \cdot 2^{-k}$.

Combine the three facts in Claim 2, we can get an upper bounded of p_k , which is

$$\begin{aligned} p_k &\leq \sum_x \Pr_{r_k, h_k} [\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}\rangle, r_k, h_k, k)^{\otimes t} \rightarrow x] = \sum_x p_{k,x} \quad (14) \\ &< \mathbf{p}(n)^{-n} \cdot 2^n + |\mathbf{G}_{x_i}| \mathbf{p}(n)^{-1} \cdot 2^{-k} + |\mathbf{G}_{x_i}| \cdot 2^{-k} + \exp(-n^2/16) \cdot 2^n \\ &< 2^{-2n} + |\mathbf{G}_{x_i}| (\mathbf{p}(n)^{-1} + 1) \cdot 2^{-k} \end{aligned}$$

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

Therefore, for a challenge state $|\phi_{x^*}\rangle$ if we denote by p_x the probability that \mathcal{B} accepts with a measurement x , then it holds that

$$p_x = \sum_{k=n+C \log n}^{C \log n} q_k p_{k,x}, \quad (15)$$

where $q_{k-1} := \prod_{j=n+C \log n}^{k+1} (1 - p_j)$.

Then by (14) and Claim 1 and Claim 2, for any $x \in \mathbf{G}_{x_i}$, and $k \geq \log |\mathbf{G}_{x_i}| + C \cdot \log n$ for some suitable $C > 0$, we have

$$\left(1 - \frac{n^2}{\mathbf{p}(n)} - \frac{5}{4 \cdot \mathbf{p}(n)} - \frac{1}{(2 \cdot n^{2C})}\right) \cdot |\mathbf{G}_{x_i}| < \frac{p_k}{p_{k,x}} < \frac{2^{k-2n} + |\mathbf{G}_{x_i}| (\mathbf{p}(n)^{-1} + 1)}{(1 - 2n^{-2C} - 5/4 \cdot \mathbf{p}(n) - n^2/\mathbf{p}(n))}$$

Namely, if we let $C = (\deg \mathbf{p}(n))/2$, then

$$\frac{\mathbf{p}(n)^2}{(1 + \mathbf{p}(n))(\mathbf{p}(n) - 3n^2) \cdot |\mathbf{G}_{x_i}|} < \frac{p_{k,x}}{p_k} < \frac{\mathbf{p}(n)}{(\mathbf{p}(n) - 3n^2) \cdot |\mathbf{G}_{x_i}|} \quad (16)$$

for any $k \geq \log |\mathbf{G}_{x_i}| + C \log n$.

Then still by Claim 1 (inequality (13)), we have

$$\sum_{k < \log |\mathbf{G}_{x_i}| + C \cdot \log n} q_k p_k \leq \exp(-n)$$

Combining it with (16), we get

$$\sum_{k=n+C \log n}^{\log |\mathbf{G}_{x_i}| + C \cdot \log n} q_k p_k \frac{\mathbf{p}(n)^2}{(1 + \mathbf{p}(n))(\mathbf{p}(n) - 3n^2) \cdot |\mathbf{G}_{x_i}|} - \exp(-n) < p_x,$$

and

$$p_x < \sum_{k=n+C \log n}^{\log |\mathbf{G}_{x_i}| + C \cdot \log n} q_k p_k \frac{\mathbf{p}(n)}{(\mathbf{p}(n) - 3n^2) \cdot |\mathbf{G}_{x_i}|} + \exp(-n)$$

hence implies

$$\frac{\mathbf{p}(n)^2}{(1 + \mathbf{p}(n))(\mathbf{p}(n) - 3n^2) \cdot |\mathbf{G}_{x_i}|} - \exp(-n) < p_x < \frac{\mathbf{p}(n)}{(\mathbf{p}(n) - 3n^2) \cdot |\mathbf{G}_{x_i}|} + \exp(-n)$$

for any $x \in \mathbf{G}_{x_i}$. Then for any $x \in \mathbf{G}_{x_i}$, we have

$$\begin{aligned} & |p_x - 1/|\mathbf{G}_{x_i}|| \\ & < \max\left\{ \frac{3n^2}{(\mathbf{p}(n) - 3n^2) \cdot |\mathbf{G}_{x_i}|} + \exp(-n), \frac{3n^2 + 3n^2 \mathbf{p}(n) - \mathbf{p}(n)}{(1 + \mathbf{p}(n))(\mathbf{p}(n) - 3n^2) \cdot |\mathbf{G}_{x_i}|} - \exp(-n) \right\} \\ & = \frac{3n^2}{(\mathbf{p}(n) - 3n^2) \cdot |\mathbf{G}_{x_i}|} + \exp(-n) \end{aligned}$$

Therefore

$$\begin{aligned} & \text{TD}\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{A},t}^{|\phi_x\rangle}\right) \\ & = \max_{0 \leq P \leq I} \text{Tr}\left[P\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| - \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{A},t}^{|\phi_x\rangle}\right)\right] \\ & < \sum_x \left|p_x - \frac{1}{|\mathbf{G}_{x_i}|} \cdot \delta_x\right| \\ & < \frac{3n^2}{(\mathbf{p}(n) - 3n^2)} + 2 \exp(-n) \cdot |\mathbf{G}_{x_i}| + 2^{-2n} \cdot 2^n + \sum_{x \in \mathbf{B}_{x_i}} p_x \\ & \stackrel{*}{<} \frac{3n^2}{(\mathbf{p}(n) - 3n^2)} + \frac{1}{\mathbf{p}(n)} + \text{negl}(n) \end{aligned}$$

for some negligible function $\text{negl}(\cdot)$, where $\delta_x = 1$ if $x \in \mathbf{G}_{x_i}$, and $\delta_x = 0$ otherwise. Here (*) holds due to the fact that $p_{k,x} \leq 2^{-k}$ and $|\mathbf{B}_{x_i}| \leq |\mathbf{G}_i|/\mathbf{p}(n)$.

Therefore, if we let $p(n) > 16q(n)^2 \cdot n^3 + 3n^2$, we can derive that

$$\begin{aligned}
 & F\left(\mathbb{E}_x |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_x \rho_{\mathcal{A},t}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|\right) \\
 & \geq (1 - \text{negl}(n)) \cdot \sum_{i=1}^l \frac{|\mathbf{G}_{x_i}|}{2^n} \cdot F\left(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{A},t}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|\right) \\
 & \geq (1 - \text{negl}(n)) \cdot \sum_{i=1}^l \frac{|\mathbf{G}_{x_i}|}{2^n} \cdot (1 - \text{TD}(\mathbb{E}_{x \in \mathbf{G}_{x_i}} |x\rangle\langle x|, \mathbb{E}_{x \in \mathbf{G}_{x_i}} \rho_{\mathcal{A},t}^{|\phi_x\rangle}) - 2 \cdot \sqrt{\frac{1}{p(n)}}) \\
 & \geq (1 - \text{negl}(n)) \cdot (1 - \frac{1}{2 \cdot q(n)}).
 \end{aligned}$$

for infinitely many $n \in \mathbb{N}$. It is contradictory to the fact that

$$F\left(\mathbb{E}_x |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathbb{E}_x \rho_{\mathcal{A},t}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|\right) < (1 - \frac{1}{q(n)}),$$

which hence means that f' is a weak one-way state generator. \square

4 The Cryptographic Applications of Average-Case Hardness of QSZK

4.1 OWSG from Variant QSD Problem

In this part, we show how to construct distributionally one-way state generator from the average-case hardness of a variant QSD problem which we call the semi-classical quantum state distinguishability problem.

Definition 5 (Semi-Classical QSD). *Given a pair of quantum unitary circuits (U_0, U_1) along with two samplers $(\mathcal{S}_0, \mathcal{S}_1)$ such that $U_b|0, x\rangle = |\phi_{b,x}, x\rangle_{AB}$ and $\Pr[\mathcal{S}_b(1^n) \rightarrow x] = p_{b,x}$ for $b \in \{0, 1\}$. It is promised that either*

$$\text{TD}(\sum_x p_{0,x} |\phi_{0,x}\rangle\langle\phi_{0,x}|, \sum_x p_{1,x} |\phi_{1,x}\rangle\langle\phi_{1,x}|) > 1 - 2^{-n},$$

or

$$\text{TD}(\sum_x p_{0,x} |\phi_{0,x}\rangle\langle\phi_{0,x}|, \sum_x p_{1,x} |\phi_{1,x}\rangle\langle\phi_{1,x}|) > 2^{-n}.$$

The semi-classical quantum state distinguishability problem (semi-classical QSD or scQSD for short) is to decide which is the case.

It is easy to see that scQSD is also a promise problem for QSZK because when we let Q_b be the quantum circuit that outputs $\mathbb{E}_x U_b|0, x\rangle\langle 0, x| U_b^\dagger$, the scQSD problem can be treated as a special case of QSD. So in this part, we denote by Q_b the pair (S_b, U_b) for convenience, and scQSD_1 (scQSD_0 resp.) the collection of (U_0, U_1) such that the trace distance is at least $1 - 2^{-n}$ (at most 2^{-n} resp.).

The average-case hardness of semi-classical QSD problem is defined similarly as the original QSD problem which characterized the hardness for any QPT distinguisher to distinguish $(Q_0, Q_1) \in \text{scQSD}_0$ from $(Q_0, Q_1) \in \text{scQSD}_1$ for a hard instance sampler $\mathbf{S}(1^n) \rightarrow (Q_0, Q_1)$. Then the distributionally OWSG can be ensured by the average-case hardness semi-classical QSD problem which is demonstrated as follows.

Theorem 8. *Assuming semi-classical QSD problem is hard-on-average in quantum case, then there exists a distributionally OWSG.*

We justify this theorem by giving the construction as follows:

The construction of distributionally OWSG: Assuming there exists a efficient sampler $((S_0^r, U_0^r), (S_1^r, U_1^r)) = (Q_0^r, Q_1^r) \leftarrow \mathbf{S}(r)$ such that the semi-classical QSD problem is hard on average on distribution of $\mathbf{S}(1^n)$ ¹³, then the following construction

$$\mathbf{f}(r, b, x) := |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle = |Q_0^r, Q_1^r\rangle \otimes |\phi_x^{U_b^r}\rangle \quad (17)$$

is a distributionally one-way state generator on the distribution over (r, b, x) . Where $|\phi_x^{U_b^r}\rangle$ is the state for $U_b^r|0, x\rangle = |\phi_x^{U_b^r}, x\rangle$, and $((S_0^r, U_0^r), (S_1^r, U_1^r)) = (Q_0^r, Q_1^r) \leftarrow \mathbf{S}(r)$. It is apparently a correct implementation of distributionally OWSG. Therefore we aim to show it meets the distributionally one-wayness. Due to the limitation of space, here we give a sketch of it and remove the detailed proof to the supplementary materials A.5.

Assuming a QPT adversary \mathcal{A} breaks the distributionally one-wayness of \mathbf{f} , that implies for a random hard instance Q_0^r, Q_1^r along with a random challenge state $|\phi_x^{U_b^r}\rangle$, \mathcal{A} would return the preimage with almost the same distribution as the real case (which is characterized by the trace distance). Then for a given hard instance Q_0^r, Q_1^r , we generate $\mathbb{E}_x |\phi_x^{U_b^r}, x\rangle \langle \phi_x^{U_b^r}, x|$, let $\mathbb{E}_x |Q_0^r, Q_1^r, \phi_x^{U_b^r}\rangle \langle Q_0^r, Q_1^r, \phi_x^{U_b^r}|$ be the challenge state of \mathcal{A} for a random coin $b \in \{0, 1\}$. Then in the case that $(Q_0^r, Q_1^r) \in \text{scQSD}_0$, the state $\mathbb{E}_x |Q_0^r, Q_1^r, \phi_x^{U_0^r}\rangle \langle Q_0^r, Q_1^r, \phi_x^{U_0^r}|$ is very close to $\mathbb{E}_x |Q_0^r, Q_1^r, \phi_x^{U_1^r}\rangle \langle Q_0^r, Q_1^r, \phi_x^{U_1^r}|$, so by the definition of distributionally OWSG, \mathcal{A} would output $b \oplus 1$ with probability nearly equals to 1/2. On the other side, when $(Q_0^r, Q_1^r) \in \text{scQSD}_1$, these two states are pretty far, which indicates that \mathcal{A} returns b with overwhelming probability, that hence induces a distinguisher for the scQSD problem.

4.2 A Direct Construction of Quantum Bit Commitment from QSD

To show the application of the average-case hardness of QSZK, we construct a quantum commitment scheme directly from the average-case hardness of the QSD problem.

Theorem 9. *The construction above is a computational hiding, sum-binding quantum commitment assuming the QSD problem is quantum hard-on-average.*

¹³ Here $r \in \{0, 1\}^{l(n)}$ denote the internal randomness of \mathbf{S} where we assume the length of the random number of \mathbf{S} is same as \mathbf{S}_b^r since we can choose the longest $l(n)$ and it is also a polynomial of n .

The construction of quantum bit commitment: Assuming there exists a efficient sampler $(Q_0^r, Q_1^r) \leftarrow \mathcal{S}(r)$ such that the QSD problem is hard on average on distribution of $\mathcal{S}(1^n)$ (here $r \in \{0, 1\}^{l(n)}$ denotes the internal randomness of \mathcal{S} , and we denote $l(n)$ by l for short when there is no confusion), then the quantum bit commitment scheme is as follows:

- **Commit phase:** The commiter generates $|0\rangle \xrightarrow{H^{\otimes l \cdot n}} \bigotimes_{i=1}^n \sum_{r_i} |r_i\rangle / 2^{l/2}$, then gets n copies of the superposition state of these circuits from \mathcal{S}

$$\bigotimes_{i=1}^n \sum_{r_i} \frac{|r_i, 0\rangle}{2^{l/2}} \xrightarrow{\mathcal{S}^{\otimes n}} \bigotimes_{i=1}^n \sum_{r_i} \frac{|r_i, Q_0^{r_i}, Q_1^{r_i}\rangle}{2^{l/2}}.$$

Then let $b \leftarrow \{0, 1\}$ be the message that the commiter intents to commit, it then generates

$$\bigotimes_{i=1}^n \sum_{r_i} \frac{|r_i, Q_0^{r_i}, Q_1^{r_i}, 0\rangle}{2^{l/2}} \xrightarrow{U^{\otimes n}} |\Psi_b\rangle_{ABCD}^{\otimes n}.$$

Where

$$|\Psi_b\rangle_{ABCD} := \sum_r \frac{|Q_0^r, Q_1^r\rangle_A \otimes PQ_b^r|0\rangle_{BC} \otimes |r\rangle_D}{2^{l/2}}$$

PQ_b^r denotes a purified circuit of Q_b^r (here we choose a deterministic procedure of the purification in this commit algorithm). Then the commiter sends the registers A, B of $|\Psi_b\rangle_{ABCD}^{\otimes n}$ to the receiver as the commitment, where A stores the Q_0^r, Q_1^r , the registers B, C store the output/ancilla parts of $PQ_b^r|0\rangle$, and D stores the random number r .

- **Reveal phase:** The commiter sends the register C, D and the message b to the receiver. The receiver invokes the operator $(H^{\otimes l} \otimes \mathcal{S}^\dagger \otimes I \circ U^\dagger)^{\otimes n}$ to the whole system, then measures the resulting state in the computational basis. The receiver accepts iff the measurement is 0.

It is not hard to derive the correctness of this construction. The remaining aims to discuss the hiding and binding properties, and we give a sketch here and leave the detailed version to the supplementary materials [A.6](#).

Firstly, we show the computationally hiding property by making a contradiction, assuming there exist a QPT adversary \mathcal{A} breaks it. That implies \mathcal{A} can distinguish one state from another of these commitment with non-negligible advantage. However when $(Q_0, Q_1) \in \mathbf{QSD}_0$, no adversary can distinguish one from another with advantage larger than $O(2^{-n})$, that hence indicates a QPT distinguisher of these QSD problem. On the other hand, the sum-binding property is guaranteed by the fact that the trace distance between these two states returned by $(Q_0, Q_1) \in \mathbf{QSD}_1$ is pretty far. That indicates the trace distance of these two commit states is pretty far, therefore no (computational unbounded) cheating commiter can both open 0 and 1 with one commit state with non-negligible probability which ensures the sum-binding of this construction.

Remark 1. Note that, the hard-core predicate of OWSGs can be realized by the same way as OWFs. Therefore for a one-way state generator \mathbf{f} , when there exist some positive polynomial $p(\cdot)$ such that $|\langle \phi_{x'} | \phi_x \rangle| \leq 1 - 1/p(n)$ for any $x \neq x'$, we can just send the $p(n) \cdot n$ copies of $|\phi_x\rangle$ along with its hard-core predicate (or a random bit) as the commitment, which can also achieve the sum-binding and computationally hiding quantum commitment. Since the proof is very similar to the classical counterpart from OWPs to the commitment via the hard-core predicate, so we omit the proof here.

5 Oracle Separation

In this section, we want to show an evidence for the non-triviality of our constructions in the last section. Note that, the existence of pqOWF at least requires that $\text{QMA} \neq \text{BQP}$, and by Kretschmer's result [31], there is a quantum oracle relative to which $\text{QMA}^{\mathcal{O}} = \text{BQP}^{\mathcal{O}}$ while PRS exists. Therefore, to give evidence indicating our result is meaningful, we show scQSD doesn't belong to QMA relative to a quantum oracle.

Theorem 10. *There exists a quantum oracle \mathcal{U} such that $\text{scQSD}^{\mathcal{O}} \notin \text{QMA}^{\mathcal{U}}$.*

Proof. We Firstly construct the oracle \mathcal{U} as follows:

The description of \mathcal{U} : The oracle $\mathcal{U} := \{\mathcal{U}_n\}_{n \in \mathbb{N}}$, where we let $\mathcal{U}_n := (\mathcal{U}_n^{\mathcal{F}_n(1)}, \dots, \mathcal{U}_n^{\mathcal{F}_n(2^{n+1})})$ for each $n \in \mathbb{N}$, and $\mathcal{U}_n^{\mathcal{F}_n(i)}$ is chosen from the Haar measure over $\mathbb{U}(2^n)$ independently for all $i \in [2^{n+1}]$. And \mathcal{F}_n is either (1) a random permutation on $\{0, 1\}^{n+1}$ or (2) a random function that differs from every permutation on at least $2^{n+2}/3$ coordinates with probability $1/2$ respectively.

For convenience, we denote by $\mathbf{U}_{n,0}$ and $\mathbf{U}_{n,1}$ the collections of these two types of \mathcal{U}_n respectively.

The construction of the hard instance $(Q_0, Q_1) = ((U_0^{\mathcal{U}}, \mathbf{S}_U^{\mathcal{U}}), (U_1^{\mathcal{U}}, \mathbf{S}_1^{\mathcal{U}}))$ of the semi-classical QSD is given directly by

$$U_b^{\mathcal{U}}|0, x\rangle := \mathcal{U}_n^{\mathcal{F}_n(b\|x)}|0\rangle \otimes |x\rangle,$$

and the \mathbf{S}_b is simply the uniform distribution of $\{0, 1\}^n$. It's easy to see the correctness of this construction, because when \mathcal{F}_n is a random permutation. Since $\mathcal{U}_n^{\mathcal{F}_n(i)}$ is chosen from the Haar measure over $\mathbb{U}(2^n)$ independently, then

$$\begin{aligned} & \mathbb{E}_{\mathcal{U}} \mathbb{F}_x (\mathbb{E}_x \mathcal{U}_n^{\mathcal{F}_n(0\|x)}|0\rangle \langle 0| (\mathcal{U}_n^{\mathcal{F}_n(0\|x)})^\dagger, \mathbb{E}_x \mathcal{U}_n^{\mathcal{F}_n(1\|x)}|0\rangle \langle 0| (\mathcal{U}_n^{\mathcal{F}_n(1\|x)})^\dagger) \\ & \leq \mathbb{E}_{\mathcal{U}} \max_V \frac{|(\sum_x \langle 0| (\mathcal{U}_n^{\mathcal{F}_n(0\|x)})^\dagger \otimes \langle x|) (\mathcal{U}_n^{\mathcal{F}_n(1\|x)}|0\rangle \otimes V|x\rangle)|}{2^n} \stackrel{**}{\leq} O(1/2^n) \end{aligned}$$

for any such \mathcal{F}_n . Where (*) holds due to the Uhlmann's theorem, and (**) follows the property of Haar measure.

When \mathcal{F}_n is a differs from every permutation on at least $2^{n+2}/3$ coordinates, then $|\mathbf{X}| := |\{0\|x_0 \mid \exists \mathcal{F}_n(0\|x_0) = \mathcal{F}_n(1\|x_1)\}| > c \cdot 2^n$ with probability nearly

$1 - \text{negl}(n)$ over the randomness of \mathcal{F}_n , where $0 < c < 1$ is a constant. Then for those \mathcal{F}_n satisfying that condition, we have

$$\begin{aligned} & \mathbb{E}_{\mathcal{U}} \text{TD}(\mathbb{E}_x \mathcal{U}_n^{\mathcal{F}_n(0\|x)} |0\rangle\langle 0| (\mathcal{U}_n^{\mathcal{F}_n(0\|x)})^\dagger, \mathbb{E}_x \mathcal{U}_n^{\mathcal{F}_n(1\|x)} |0\rangle\langle 0| (\mathcal{U}_n^{\mathcal{F}_n(1\|x)})^\dagger) \\ & \leq \sum_{x_0 \notin \mathbf{X}}^* \max_P \text{Tr} P \mathcal{U}_n^{\mathcal{F}_n(0\|x_0)} |0\rangle\langle 0| (\mathcal{U}_n^{\mathcal{F}_n(0\|x_0)})^\dagger \leq 1 - c. \end{aligned}$$

It's obvious that $(1 - c)^2 > O(1/2^n)$ for all sufficiently large n , and by Borel-Cantelli lemma we can see that it's a correct implementation of scQSD for all but finite $n \in \mathbb{N}$ with probability 1 under the randomness of \mathcal{U} .

Then we show that the semi-classical QSD problem doesn't belong to QMA^U by Aaronson's result [2].

Proposition 1. *For any q -query oracle-aided QMA verifier V with w qubits witness that decides the scQSD U problem, it holds that $q \cdot w = \Omega(2^{n/3})$.*

Proof (of Proposition 1). We let V be the quantum verifier of scQSD problem relative to \mathcal{U} , Note that the choice of \mathcal{U}_m is irrelevant for distinguishing $\mathbf{U}_{1,n}$ from $\mathbf{U}_{2,n}$ when $m \neq n$, therefore

$$\begin{aligned} & \left| \Pr_{\mathcal{U}}[V^{\mathcal{U}}(1^n) = 1 \mid \mathcal{U}_n \in \mathbf{U}_{n,0}] - \Pr_{\mathcal{U}}[V^{\mathcal{U}}(1^n) = 1 \mid \mathcal{U}_n \in \mathbf{U}_{n,1}] \right| \quad (18) \\ & = \left| \Pr_{\mathcal{U}_n}[V^{\mathcal{U}_n}(1^n) = 1 \mid \mathcal{U}_n \in \mathbf{U}_{n,0}] - \Pr_{\mathcal{U}_n}[V^{\mathcal{U}_n}(1^n) = 1 \mid \mathcal{U}_n \in \mathbf{U}_{n,1}] \right|. \end{aligned}$$

However, that induces a quantum distinguisher \mathcal{B} for the permutation testing problem (PTP) in [2]. That is, for a give oracle \mathcal{F}_n , which is either (1) a random permutation on $\{0, 1\}^{n+1}$, or (2) a random function that differs from every permutation on at least $2^{n+2}/3$ coordinates. We can then establish \mathcal{B} as follows:

- \mathcal{B} is quantum accessible to oracle \mathcal{F}_n , it then simulates $\bar{\mathcal{U}}_n^{(\mathcal{F}_n(i))} \leftarrow \mathbb{U}(2^n)$ locally for all $i \in [2^{n+1}]$.
- \mathcal{B} simulates $U_b^{\mathcal{U}}$ by taking $|b, x\rangle$ as input and outputs $\bar{\mathcal{U}}_n^{(\mathcal{F}_n(b\|x))} |0\rangle \otimes |x\rangle$.
- \mathcal{B} invokes V with $\bar{\mathcal{U}}_n$, then outputs V 's decision as result.

We then have

$$\Pr[\mathcal{B}^{\mathcal{F}_n}(1^n) = 1 \mid \mathcal{F}_n \text{ is case}(b)] = \Pr[\mathcal{A}_0^{\mathcal{U}_n}(1^n) = 1 \mid \mathcal{U}_n \in \mathbf{U}_{n,b}] \quad (19)$$

However, according to the quantum query lower bound of permutation testing problem (Theorem 8 in [2]), the number of queries for such \mathcal{B} is bounded by $q \cdot w = \Omega(2^{n/3})$, which hence justifies the Proposition 1. \square

Therefore, by Proposition 1, any verifier V can not distinguish $\mathbf{U}_{n,0}$ from $\mathbf{U}_{n,1}$ with at most polynomial many queries and witness, which hence completes the proof of Theorem 10. \square

References

1. Aaronson, S.: BQP and the polynomial hierarchy. In: Schulman, L.J. (ed.) Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010. pp. 141–150. ACM (2010), <https://doi.org/10.1145/1806689.1806711>
2. Aaronson, S.: Impossibility of succinct quantum proofs for collision-freeness. *Quantum Inf. Comput.* **12**(1-2), 21–28 (2012), <https://doi.org/10.26421/QIC12.1-2-3>
3. Aharonov, D., Kitaev, A.Y., Nisan, N.: Quantum circuits with mixed states. In: Vitter, J.S. (ed.) Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998. pp. 20–30. ACM (1998), <https://doi.org/10.1145/276698.276708>
4. Aharonov, D., Ta-Shma, A.: Adiabatic quantum state generation and statistical zero knowledge. In: Larmore, L.L., Goemans, M.X. (eds.) Proceedings of the 35th Annual ACM Symposium on Theory of Computing, June 9-11, 2003, San Diego, CA, USA. pp. 20–29. ACM (2003), <https://doi.org/10.1145/780542.780546>
5. Ananth, P., Qian, L., Yuen, H.: Cryptography from pseudorandom quantum states. *IACR Cryptol. ePrint Arch.* To appear in CRYPTO 2022 p. 1663 (2021), <https://eprint.iacr.org/2021/1663>
6. Bartusek, J., Coladangelo, A., Khurana, D., Ma, F.: One-way functions imply secure computation in a quantum world. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12825, pp. 467–496. Springer (2021), https://doi.org/10.1007/978-3-030-84242-0_17
7. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014), <https://doi.org/10.1016/j.tcs.2014.05.025>
8. Bitansky, N., Degwekar, A.: On the complexity of collision resistant hash functions: New and old black-box separations. In: Hofheinz, D., Rosen, A. (eds.) Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part I. Lecture Notes in Computer Science, vol. 11891, pp. 422–450. Springer (2019), https://doi.org/10.1007/978-3-030-36030-6_17
9. Bitansky, N., Degwekar, A., Vaikuntanathan, V.: Structure versus hardness through the obfuscation lens. *SIAM J. Comput.* **50**(1), 98–144 (2021), <https://doi.org/10.1137/17M1136559>
10. Boneh, D., Zhandry, M.: Quantum-secure message authentication codes. In: Johansson, T., Nguyen, P.Q. (eds.) Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings. Lecture Notes in Computer Science, vol. 7881, pp. 592–608. Springer (2013), https://doi.org/10.1007/978-3-642-38348-9_35
11. Brakerski, Z., Canetti, R., Qian, L.: On the computational hardness needed for quantum cryptography. *Cryptology ePrint Archive* (2022)
12. Brakerski, Z., Shmueli, O.: (pseudo) random quantum states with binary phase. In: Hofheinz, D., Rosen, A. (eds.) Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part I. Lecture Notes in Computer Science, vol. 11891, pp. 229–250. Springer (2019), https://doi.org/10.1007/978-3-030-36030-6_10

13. Brakerski, Z., Shmueli, O.: Scalable pseudorandom quantum states. In: Micciancio, D., Ristenpart, T. (eds.) *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II. Lecture Notes in Computer Science*, vol. 12171, pp. 417–440. Springer (2020), https://doi.org/10.1007/978-3-030-56880-1_15
14. Chailloux, A., Kerenidis, I., Rosgen, B.: Quantum commitments from complexity assumptions. In: Aceto, L., Henzinger, M., Sgall, J. (eds.) *Automata, Languages and Programming - 38th International Colloquium, ICALP 2011, Zurich, Switzerland, July 4-8, 2011, Proceedings, Part I. Lecture Notes in Computer Science*, vol. 6755, pp. 73–85. Springer (2011), https://doi.org/10.1007/978-3-642-22006-7_7
15. Chen, L.: A note on oracle separations for BQP. *CoRR* **abs/1605.00619** (2016), <http://arxiv.org/abs/1605.00619>
16. Fischlin, M.: On the impossibility of constructing non-interactive statistically-secret protocols from any trapdoor one-way function. In: Preneel, B. (ed.) *Topics in Cryptology - CT-RSA 2002, The Cryptographer's Track at the RSA Conference, 2002, San Jose, CA, USA, February 18-22, 2002, Proceedings. Lecture Notes in Computer Science*, vol. 2271, pp. 79–95. Springer (2002), https://doi.org/10.1007/3-540-45760-7_7
17. Goldreich, O.: *Foundations of cryptography*. Cambridge university press (2009)
18. Goldreich, O., Goldwasser, S., Micali, S.: On the cryptographic applications of random functions. In: Blakley, G.R., Chaum, D. (eds.) *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings. Lecture Notes in Computer Science*, vol. 196, pp. 276–288. Springer (1984), https://doi.org/10.1007/3-540-39568-7_22
19. Goldreich, O., Goldwasser, S., Micali, S.: How to construct random functions. *Journal of the Acm* **33**(4), 792–807 (1986)
20. Goldwasser, S., Micali, S.: Probabilistic encryption. *J. Comput. Syst. Sci.* **28**(2), 270–299 (1984), [https://doi.org/10.1016/0022-0000\(84\)90070-9](https://doi.org/10.1016/0022-0000(84)90070-9)
21. Grilo, A.B., Lin, H., Song, F., Vaikuntanathan, V.: Oblivious transfer is in minicrypt. In: Canteaut, A., Standaert, F. (eds.) *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II. Lecture Notes in Computer Science*, vol. 12697, pp. 531–561. Springer (2021), https://doi.org/10.1007/978-3-030-77886-6_18
22. Haitner, I., Hoch, J.J., Reingold, O., Segev, G.: Finding collisions in interactive protocols - tight lower bounds on the round and communication complexities of statistically hiding commitments. *SIAM J. Comput.* **44**(1), 193–242 (2015), <https://doi.org/10.1137/130938438>
23. Hästad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. *SIAM J. Comput.* **28**(4), 1364–1396 (1999), <https://doi.org/10.1137/S0097539793244708>
24. Homan, C.M., Thakur, M.: One-way permutations and self-witnessing languages. *J. Comput. Syst. Sci.* **67**(3), 608–622 (2003), [https://doi.org/10.1016/S0022-0000\(03\)00068-0](https://doi.org/10.1016/S0022-0000(03)00068-0)
25. Impagliazzo, R.: A personal view of average-case complexity. In: *Proceedings of the Tenth Annual Structure in Complexity Theory Conference, Minneapolis, Minnesota, USA, June 19-22, 1995*. pp. 134–147. IEEE Computer Society (1995), <https://doi.org/10.1109/SCT.1995.514853>

26. Impagliazzo, R., Luby, M.: One-way functions are essential for complexity based cryptography. In: 30th Annual Symposium on Foundations of Computer Science. pp. 230–235. IEEE (1989)
27. Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: Johnson, D.S. (ed.) Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14–17, 1989, Seattle, Washington, USA. pp. 44–61. ACM (1989), <https://doi.org/10.1145/73007.73012>
28. Ji, Z., Liu, Y., Song, F.: Pseudorandom quantum states. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III. Lecture Notes in Computer Science, vol. 10993, pp. 126–152. Springer (2018), https://doi.org/10.1007/978-3-319-96878-0_5
29. Kashefi, E., Kerenidis, I.: Statistical zero knowledge and quantum one-way functions. *Theor. Comput. Sci.* **378**(1), 101–116 (2007), <https://doi.org/10.1016/j.tcs.2007.03.013>
30. Komargodski, I., Yogev, E.: On distributional collision resistant hashing. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part II. Lecture Notes in Computer Science, vol. 10992, pp. 303–327. Springer (2018), https://doi.org/10.1007/978-3-319-96881-0_11
31. Kretschmer, W.: Quantum pseudorandomness and classical complexity. In: Hsieh, M. (ed.) 16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5–8, 2021, Virtual Conference. LIPIcs, vol. 197, pp. 2:1–2:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2021), <https://doi.org/10.4230/LIPIcs.TQC.2021.2>
32. Luby, M., Rackoff, C.: How to construct pseudo-random permutations from pseudo-random functions. *Siam Journal on Computing* **17**(2), 373–386 (2006)
33. Mahmoody, M., Maji, H.K., Prabhakaran, M.: On the power of public-key encryption in secure computation. In: Lindell, Y. (ed.) Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24–26, 2014. Proceedings. Lecture Notes in Computer Science, vol. 8349, pp. 240–264. Springer (2014), https://doi.org/10.1007/978-3-642-54242-8_11
34. Menda, S., Watrous, J.: Oracle separations for quantum statistical zero-knowledge. *CoRR* **abs/1801.08967** (2018), <http://arxiv.org/abs/1801.08967>
35. Morimae, T., Yamakawa, T.: Quantum commitments and signatures without one-way functions. *IACR Cryptol. ePrint Arch.* To appear in CRPTPO 2022 p. 1691 (2021), <https://eprint.iacr.org/2021/1691>
36. Naor, M.: Bit commitment using pseudorandomness. *J. Cryptol.* **4**(2), 151–158 (1991), <https://doi.org/10.1007/BF00196774>
37. Nayak, A., Shor, P.: Bit-commitment-based quantum coin flipping. *Physical Review A* **67**(1) (jan 2003). <https://doi.org/10.1103/physreva.67.012304>, <https://doi.org/10.1103%2Fphysreva.67.012304>
38. Nielsen, M.A., Chuang, I.: Quantum computation and quantum information (2002)
39. Ong, S.J., Vadhan, S.P.: An equivalence between zero knowledge and commitments. In: Canetti, R. (ed.) Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19–21, 2008. Lecture Notes in Computer Science, vol. 4948, pp. 482–500. Springer (2008), https://doi.org/10.1007/978-3-540-78524-8_27
40. Ostrovsky, R.: One-way functions, hard on average problems, and statistical zero-knowledge proofs. In: Proceedings of the Sixth Annual Structure in Complexity

- Theory Conference, Chicago, Illinois, USA, June 30 - July 3, 1991. pp. 133–138. IEEE Computer Society (1991), <https://doi.org/10.1109/SCT.1991.160253>
41. Ostrovsky, R., Wigderson, A.: One-way functions are essential for non-trivial zero-knowledge. In: Second Israel Symposium on Theory of Computing Systems, ISTCS 1993, Natanya, Israel, June 7-9, 1993, Proceedings. pp. 3–17. IEEE Computer Society (1993), <https://doi.org/10.1109/ISTCS.1993.253489>
 42. Simon, D.R.: Finding collisions on a one-way street: Can secure hash functions be based on general assumptions? In: Nyberg, K. (ed.) Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding. Lecture Notes in Computer Science, vol. 1403, pp. 334–345. Springer (1998), <https://doi.org/10.1007/BFb0054137>
 43. Stad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. *Siam Journal on Computing* **28**(4), 1364–1396 (1999)
 44. Vadhan, S.P.: An unconditional study of computational zero knowledge. *SIAM J. Comput.* **36**(4), 1160–1214 (2006), <https://doi.org/10.1137/S0097539705447207>
 45. Watrous, J.: Limits on the power of quantum statistical zero-knowledge. In: 43rd Symposium on Foundations of Computer Science (FOCS 2002), 16-19 November 2002, Vancouver, BC, Canada, Proceedings. p. 459. IEEE Computer Society (2002), <https://doi.org/10.1109/SFCS.2002.1181970>
 46. Yan, J.: General properties of quantum bit commitment. *IACR Cryptol. ePrint Arch.* To Appear in ASIACRYPT 2022 p. 1488 (2022), <https://eprint.iacr.org/2020/1488>
 47. Zhandry, M.: How to construct quantum random functions. In: 53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012. pp. 679–687. IEEE Computer Society (2012), <https://doi.org/10.1109/FOCS.2012.37>
 48. Zhandry, M.: A note on quantum-secure prps. *IACR Cryptology ePrint Archive* **2016**, 1076 (2016), <http://eprint.iacr.org/2016/1076>

A Supplementary Materials

A.1 Proof of Theorem 6

We firstly recall Theorem 6 as follows:

Theorem 6. The existence of weak OWSG and strong OWSG are equivalent.

In this part, let \mathbf{f} be a weak one-way state generator on distribution $D(1^n)$, satisfying

$$\Pr_{x \leftarrow D(1^n)} [\text{Exp}_{\mathbf{f}, \mathcal{B}}^{owsq}(n) = 1] \leq 1 - \frac{1}{q(n)} \quad (20)$$

for some positive polynomial $q(\cdot)$. For some suitable polynomial $m(n)$ (which is determined by $q(n)$), the construction \mathbf{f}'

$$\mathbf{f}'(x_1, \dots, x_m) = \otimes_{i=1}^m |\phi_{x_i}\rangle_Y^{\otimes nq(n)} \otimes_{i=1}^m |\eta_{x_i}\rangle_Z^{\otimes nq(n)} \quad (21)$$

is a strong OWSGs. Then we prove that \mathbf{f}' is strong one-way state generator on distribution $\mathbb{D}(1^n)^m$ by making a contradiction. Assuming \mathcal{A} breaks the strong one-wayness of \mathbf{f}' with t copies, namely

$$\Pr_{(x_1, \dots, x_m) \leftarrow \mathbb{D}(1^n)^m} [\text{Exp}_{\mathcal{A}}^{\text{owsg}}(n) = 1] \geq \frac{1}{\mathbf{p}(n)} \quad (22)$$

for infinitely many $n \in \mathbb{N}$. Then we construct \mathcal{B} breaks the weak one-wayness as follows:

- \mathcal{B} takes as input the state $|\phi_{x^*}\rangle^{\otimes 4n^3 \cdot m \cdot \mathbf{p}(n) \mathbf{q}^2(n) \cdot (t+1)}$, it sets $|\phi_{x_j}\rangle = |\phi_{x^*}\rangle$ for a random $j \in [m]$.
- For $i \in [m]/\{j\}$, \mathcal{B} generates $x_i \leftarrow \mathbb{D}(1^n)$, and gets $|\phi_{x_i}\rangle$.
- \mathcal{B} invokes \mathcal{A} with input state $|\Phi\rangle^{\otimes t} := \otimes_{i=1}^m |\phi_{x_i}\rangle^{\otimes n \mathbf{q}(n) \cdot t}$, and gets outputs (x'_1, \dots, x'_m) . Then it repeats that step for a new generated $|\phi_{x_i}\rangle$ as input for $i \in [m]/\{j\}$ about $2n \cdot m \cdot \mathbf{p}(n)$ times.
- \mathcal{B} generates a new random j and sets $|\phi_{x_j}\rangle = |\phi_{x^*}\rangle$, repeats the steps above for $2n \mathbf{q}(n)$ times.
- \mathcal{B} checks all these $4n^2 m \mathbf{p}(n) \mathbf{q}(n)$ outputs by measuring $|\phi_{x^*}\rangle$ with $\{|\phi_{x'_j}\rangle\langle\phi_{x'_j}|, I - |\phi_{x'_j}\rangle\langle\phi_{x'_j}|\}$ about $n \cdot \mathbf{q}(n)$ times for each x'_j and returns the most possible answer (one of the x'_j that gets $|\phi_{x'_j}\rangle$ as measurement with at least $(n-1) \cdot \mathbf{q}(n)$ times).

To estimate the probability that \mathcal{B} wins, for each $j \in [m]$, let \mathbf{BadX}_j be the collection of x^* such that

$$\mathbf{BadX}_j := \{x^* \mid \Pr\left[\prod_{i=1}^m |\langle\phi_{x_i}|\phi_{x'_i}\rangle|^{2n \mathbf{q}(n)} \geq \frac{1}{2m \mathbf{p}(n)}, |\phi_{x^*}\rangle = |\phi_{x_j}\rangle\right] \leq \frac{1}{2m \mathbf{p}(n)}\}$$

Where the probability inside is taken over of the randomness of \mathcal{A} and $x_i \leftarrow \mathbb{D}(1^n)$ for $i \in [m]/\{j\}$. Then there is at least one $j \in [m]$ satisfies that

$$\Pr_x[x \in \mathbf{BadX}_j] \leq \frac{1}{2 \cdot \mathbf{q}(n)} \quad (23)$$

for those n satisfying (22). If not, since \mathcal{A} wins with probability at least $1/\mathfrak{p}(n)$ for those n , Therefore when we let $m = 2 \cdot \mathfrak{q}(n) \cdot n$

$$\begin{aligned}
 \frac{1}{\mathfrak{p}(n)} &\leq \Pr_{(x_1, \dots, x_m) \leftarrow \mathcal{D}(1^n)^m} [\text{Exp}_{\mathfrak{f}, \mathcal{A}}^{\text{owsg}}(n) = 1] \\
 &= \Pr_{(x_1, \dots, x_m) \leftarrow \mathcal{D}(1^n)^m} [\text{Exp}_{\mathfrak{f}, \mathcal{A}}^{\text{owsg}}(n) = 1 \wedge \bigwedge_{i=1}^m x_i \notin \mathbf{BadX}_i] \\
 &\quad + \Pr_{(x_1, \dots, x_m) \leftarrow \mathcal{D}(1^n)^m} [\text{Exp}_{\mathfrak{f}, \mathcal{A}}^{\text{owsg}}(n) = 1 \wedge (\bigvee_{i=1}^m x_i \in \mathbf{BadX}_i)] \\
 &\leq \Pr_{(x_1, \dots, x_m) \leftarrow \mathcal{D}(1^n)^m} [\bigwedge_{i=1}^m x_i \notin \mathbf{BadX}_i] \\
 &\quad + m \cdot \max_i \Pr_{(x_1, \dots, x_m) \leftarrow \mathcal{D}(1^n)^m} [\text{Exp}_{\mathfrak{f}, \mathcal{A}}^{\text{owsg}}(n) = 1 \wedge x_i \in \mathbf{BadX}_i] \\
 &\leq \left(1 - \frac{1}{2 \cdot \mathfrak{q}(n)}\right)^m \\
 &\quad + m \cdot \max_i \Pr_{(x_1, \dots, x_m) \leftarrow \mathcal{D}(1^n)^m} [\text{Exp}_{\mathfrak{f}, \mathcal{A}}^{\text{owsg}}(n) = 1 \mid x_i \in \mathbf{BadX}_i] \\
 &\leq \left(1 - \frac{1}{2 \cdot \mathfrak{q}(n)}\right)^m + m \cdot \frac{1}{2 \cdot m \cdot \mathfrak{p}(n)} < \frac{1}{\mathfrak{p}(n)}
 \end{aligned}$$

which is a contradiction. Then we denote by j_0 one set that \mathbf{BadX}_{j_0} satisfies the (23). Then there are at least $1 - 1/2\mathfrak{q}(n)$ of x^* such that, when \mathcal{B} chooses $j = j_0$, the probability that \mathcal{A} outputs some (x'_1, \dots, x'_m) satisfying the probability that $\prod_{i=1}^m |\langle \phi_{x_i} | \phi_{x'_i} \rangle|^{2n\mathfrak{q}(n)} \geq 1/2m\mathfrak{p}(n)$ is at least $1/2m\mathfrak{p}(n)$.

Therefore when we repeat to choose j randomly for more than $2n\mathfrak{q}(n)$ times, we could get that $j = j_0$ with probability at least $1 - O(\exp(-n))$.

Conditioned on $x^* \in \mathbf{BadX}$ and $j = j_0$, \mathcal{A} would output some (x'_1, \dots, x'_m) satisfying the probability that $\prod_{i=1}^m |\langle \phi_{x_i} | \phi_{x'_i} \rangle|^{2n\mathfrak{q}(n)} \geq 1/2m\mathfrak{p}(n)$ is at least $1/2m\mathfrak{p}(n)$ where $|\phi_{x^*}\rangle$ is embedded as $|\phi_{x_{j_0}}\rangle$. Since \mathcal{B} repeats each round j for $2nmp(n)$ times, the probability that $\prod_{i=1}^m |\langle \phi_{x_i} | \phi_{x'_i} \rangle|^{2n\mathfrak{q}(n)} \geq 1/2m\mathfrak{p}(n)$ occurs is at least $1 - O(\exp(-n))$.

That implies \mathcal{B} would outputs some (x'_1, \dots, x'_m) satisfying $\prod_{i=1}^m |\langle \phi_{x_i} | \phi_{x'_i} \rangle|^{2n} \geq 1/2m\mathfrak{p}(n)$ with probability at least $1 - O(\exp(-n))$. And in that case, it holds that

$$|\langle \phi_{x^*} | \phi_{x'_{j_0}} \rangle|^2 = |\langle \phi_{x_{j_0}} | \phi_{x'_{j_0}} \rangle|^2 \geq (1/2m\mathfrak{p}(n))^{1/n\mathfrak{q}(n)} > 1 - \frac{1}{2\mathfrak{q}(n)}.$$

That implies \mathcal{B} finds some returns such that $|\langle \phi_{x^*} | \phi_{x'_{j_0}} \rangle|^2 > 1 - 1/2\mathfrak{q}(n)$ with probability at least $1 - O(\exp(-n))$. Therefore the remaining problem is to find it among the polynomial many $(4n^2m\mathfrak{p}(n)\mathfrak{q}(n))$ outputs. That can be settled by measuring $|\phi_{x^*}\rangle$ with $\{|\phi_{x'_{j_0}}\rangle\langle \phi_{x'_{j_0}}|, I - |\phi_{x'_{j_0}}\rangle\langle \phi_{x'_{j_0}}|\}$ polynomial times for each output x'_{j_0} . Since each measurement is independent, by Chernoff bound, the result is close to the expected value (for some polynomial amount) with probability at least $1 - O(\exp(-n))$, since there are at most polynomial many outputs, all results would follows that rules with probability $1 - \text{negl}(n)$, which implies that \mathcal{B} would output x' such that $|\langle \phi_{x^*} | \phi_{x'} \rangle|^2 > 1 - 1/2\mathfrak{q}(n)$ with

probability at least $1 - \mathbf{negl}(n) - O(\exp(-n)) - 1/2\mathbf{q}(n)$. Namely

$$\Pr_{x \leftarrow \mathbb{D}(1^n)} [\mathbf{Exp}_{\mathbf{f}, \mathcal{B}}^{ows\mathbf{g}}(n) = 1] \geq 1 - \mathbf{negl}(n) - O(\exp(-n)) - 1/2\mathbf{q}(n)$$

That is contradictory to the weak one-wayness of \mathbf{f} (namely the inequality (20)) which hence completes the proof of Theorem 6. \square

A.2 Proof of Lemma 4

We firstly recall Lemma 4 as follows:

Lemma 4. If \mathbf{f} is not a weak one-way state generator, and assuming \mathcal{A} is the corresponding adversary using $t(n)$ copies (denoted as t in brief sometimes). Let $I_n(\delta)$ be the collection of x such that \mathcal{A} accept with probability at least $1 - \delta$

$$I_n(\delta) := \{x' \mid \Pr_x[\mathbf{Exp}_{\mathbf{f}, \mathcal{A}}^{ows\mathbf{g}}(n) = 1 \mid x = x'] > 1 - \delta\}.$$

Then for any positive polynomial $\mathbf{poly}(\cdot)$, \mathbf{f} is $(2t, 1/\mathbf{poly}(n))$ -polarized on $I_n(1/(4\mathbf{poly}(n)t(n))^2)$.

Proof (of Lemma 4). Apparently, when $1/\delta$ is some positive polynomial, it holds that $|I_n(\delta)| = (1 - \mathbf{negl}(n)) \cdot 2^n$ for some negligible function $\mathbf{negl}(\cdot)$ (assuming the domain is $\{0, 1\}^n$).

We let $\mathbf{N}_x^k(\varepsilon)$ be the set of the “ k -degree neighbor” of x such that

$$\mathbf{N}_x^k(\varepsilon) := \{x' \mid |\langle \phi_{x'} | \phi_x \rangle|^k \geq 1 - \varepsilon\}. \quad (24)$$

Then we show that, for any positive polynomial $\mathbf{poly}(n)$, the collection $\mathbf{N}_x^{2t}(1/\mathbf{poly}(n))$ defines an equivalent classification of $I_n(\delta)$ for some polynomial $1/\delta$ (which will be defined later). More specifically, we can prove that, for any pair $x, x' \in I_n(\delta)$, either x, x' belong to a same neighbor $\mathbf{N}_x^{2t}(1/\mathbf{poly}(n))$ or they are a little “far” from each other (i.e. $|\langle \phi_{x'} | \phi_x \rangle|^{2t} \leq 1/\mathbf{poly}(n)$).

We show that by making a contraction, assuming there are $x_0, x_1 \in I_n(\delta)$, such that

$$\frac{1}{\mathbf{poly}(n)} < |\langle \phi_{x_0} | \phi_{x_1} \rangle|^{2t} < 1 - \frac{1}{\mathbf{poly}(n)}.$$

On the other hand, since $x_0, x_1 \in I_n(\delta)$, by the definition of $I_n(\delta)$, it holds that

$$\langle \phi_{x_b} | \mathbf{Tr}_{X,Z}(\mathbf{f}(\rho_{\mathcal{A},t}^{|\phi_{x_b}\rangle})) | \phi_{x_b} \rangle \geq 1 - \delta,$$

for $b = 0, 1$. If we denote by $\sum \alpha_{x,z}^b |x, z\rangle$ the purification of $\rho_{\mathcal{A},t}^{|\phi_{x_b}\rangle}$ for $b = 0, 1$, that hence implies that

$$\sum_{x \in \mathbf{N}_{x_b}^2(\sqrt{\delta})} |\alpha_{x,z}^b|^2 \geq 1 - \sqrt{\delta} \quad (25)$$

On the other hand, for any x' , it holds that

$$\begin{aligned} \sum_b \sqrt{1 - |\langle \phi_{x'} | \phi_{x_b} \rangle|^2} &= \sum_b \text{TD}(|\phi_{x'}\rangle \langle \phi_{x'}|, |\phi_{x_b}\rangle \langle \phi_{x_b}|) \\ &\geq \text{TD}(|\phi_{x_0}\rangle \langle \phi_{x_0}|, |\phi_{x_1}\rangle \langle \phi_{x_1}|) \\ &\geq \sqrt{1 - \left(1 - \frac{1}{\text{poly}(n)}\right)^{\frac{1}{t}}} > \sqrt{\frac{1}{\text{poly}(n) \cdot t(n)}}. \end{aligned}$$

Therefore, if $x' \in \mathbf{N}_{x_0}^2(\sqrt{\delta}) \cap \mathbf{N}_{x_1}^2(\sqrt{\delta})$, we should have

$$2 \cdot \delta^{1/4} \geq \sum_b \sqrt{1 - |\langle \phi_{x'} | \phi_{x_b} \rangle|^2} > \sqrt{\frac{1}{\text{poly}(n) \cdot t(n)}}.$$

That means $\mathbf{N}_{x_0}^2(\sqrt{\delta}) \cap \mathbf{N}_{x_1}^2(\sqrt{\delta}) = \emptyset$ when $\sqrt{\delta} \leq 1/(4\text{poly}(n)t(n))$. Therefore if we denote by $\Pi_{\mathbf{N}_{x_b}^2(\sqrt{\delta})}$ the projection map of the space generated by the $\{ |x\rangle \mid x \in \mathbf{N}_{x_b}^2(\sqrt{\delta}) \}$, the trace distance between this two cases can be estimated as follows

$$\begin{aligned} &\text{TD}(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle}, \rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle}) \\ &= \text{TD}\left(\Pi_{\mathbf{N}_{x_0}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle}) + g_{x_0}, \Pi_{\mathbf{N}_{x_1}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle}) + g_{x_1}\right) \\ &\geq \text{TD}\left(\Pi_{\mathbf{N}_{x_0}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle})/\text{Tr}\left(\Pi_{\mathbf{N}_{x_0}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle})\right), \Pi_{\mathbf{N}_{x_0}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle})/\text{Tr}\left(\Pi_{\mathbf{N}_{x_0}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle})\right)\right) \\ &\quad - \text{TD}\left(\Pi_{\mathbf{N}_{x_1}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle}) + g_{x_1}, \Pi_{\mathbf{N}_{x_1}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle})/\text{Tr}\left(\Pi_{\mathbf{N}_{x_1}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle})\right)\right) \\ &\quad - \text{TD}\left(\Pi_{\mathbf{N}_{x_0}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle}) + g_{x_0}, \Pi_{\mathbf{N}_{x_0}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle})/\text{Tr}\left(\Pi_{\mathbf{N}_{x_0}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle})\right)\right) \\ &\stackrel{*}{\geq} 1 - 2 \cdot \sqrt{\delta} \geq 1 - \frac{1}{2 \cdot \text{poly}(n) \cdot t(n)} \end{aligned}$$

where g_{x_b} is the ‘‘garbage’’ part such that $\rho_{\mathcal{A},t}^{|\phi_{x_b}\rangle} = \Pi_{\mathbf{N}_{x_b}^2(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_b}\rangle}) + g_{x_b}$ (here we denote by $\Pi(\rho) := \Pi\rho\Pi^\dagger$ for convenience). And (*) hold due to the fact that $\text{Tr}(g_{x_b}) \leq \sqrt{\delta}$ (the inequality (25)).

However, since we assume $1/\text{poly}(n) < |\langle \phi_{x_0} | \phi_{x_1} \rangle|^{2t}$, we can also derive an upper bound of that trace distance

$$\begin{aligned} &\text{TD}(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle}, \rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle}) \\ &= \text{TD}(\text{Tr}_Z \mathcal{A}(|\phi_{x_0}\rangle^{\otimes t} \otimes |0\rangle), \text{Tr}_Z \mathcal{A}(|\phi_{x_1}\rangle^{\otimes t} \otimes |0\rangle)) \\ &\leq \text{TD}(\mathcal{A}(|\phi_{x_0}\rangle^{\otimes t} \otimes |0\rangle), \mathcal{A}(|\phi_{x_1}\rangle^{\otimes t} \otimes |0\rangle)) \\ &= \text{TD}(|\phi_{x_0}\rangle^{\otimes t}, |\phi_{x_1}\rangle^{\otimes t}) \\ &\leq \sqrt{1 - 1/\text{poly}(n)} \end{aligned}$$

which leads to a contradiction. That completes the proof of Lemma 4. \square

A.3 Proof of Claim 1

We recall Claim 1 as follows:

Claim 1. For a given challenge state $|\phi_{x^*}\rangle$, where $x^* \in \mathbf{G}_{x_i}$, we denote by p_k the probability that \mathcal{B} accepts at one repetition of k -th round, then for $k \in [n + C \cdot \log n, \log |\mathbf{G}_{x_i}| + C \cdot \log n]$, it holds that

$$p_k \geq \left(1 - \frac{n^2 \cdot t(n)}{\mathbf{p}(n)} - \frac{5}{4 \cdot \mathbf{p}(n)}\right) \cdot \frac{|\mathbf{G}_{x_i}|}{2^k} \quad (26)$$

Then it holds that

$$\Pr[\mathcal{B} \text{ accepts} \wedge k \geq \log |\mathbf{G}_{x_i}| + C \cdot \log n] \geq 1 - \exp(-n), \quad (27)$$

namely, the probability that \mathcal{B} accepts for some $k \geq \log |\mathbf{G}_{x_i}| + C \cdot \log n$ is at least $1 - \exp(-n)$ when $m \geq 2n^{C+1}$.

Proof (of Claim 1). For each $k \in [n + C \cdot \log n, \log |\mathbf{G}_{x_i}| + C \cdot \log n]$, the probability that \mathcal{B} accepts in one repetition at the k -th round is at least the probability that \mathcal{B} accepts with some measurement in \mathbf{G}_{x_i} , namely

$$\begin{aligned} p_k &\geq \Pr_{r_k, h_k} [\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}, r_k, h_k, k\rangle^{\otimes t}) \in \mathbf{G}_{x_i}] \\ &\stackrel{*}{\geq} \Pr_{r_k, h_k} [\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}, r_k, h_k, k\rangle^{\otimes t}) \in \mathbf{G}_{x_i} \wedge r_k \in h_k(\mathbf{G}_{x_i})]. \end{aligned} \quad (28)$$

Here (*) holds because any measurement $x \in \mathbf{G}_{x_i}$ returned by \mathcal{A} accepted by \mathcal{B} only if $r_k = h_k(x)$, otherwise, it would reject by \mathcal{B} with probability 1.

We now estimate the probabilities above. Since $h_k : \{0, 1\}^n \rightarrow \{0, 1\}^k$ is a universal hash, and $r_k \leftarrow \{0, 1\}^k$ is chosen uniformly at random, we thus have

$$\Pr_{r_k, h_k} [r_k \in h_k(\mathbf{G}_{x_i})] \leq \sum_{x \in \mathbf{G}_{x_i}} \Pr_{r_k, h_k} [r_k = h_k(x)] = \frac{|\mathbf{G}_{x_i}|}{2^k}.$$

On the other hand, by the Bonferroni's inequality, conditioned on the fact that $h_k : \{0, 1\}^n \rightarrow \{0, 1\}^k$ is a universal hash, it holds that

$$\begin{aligned} &\Pr_{r_k, h_k} [r_k \in h_k(\mathbf{G}_{x_i})] \\ &\geq \sum_{x \in \mathbf{G}_{x_i}} \Pr_{r_k, h_k} [r_k = h_k(x)] - \sum_{x, x' \in \mathbf{G}_{x_i}} \Pr_{r_k, h_k} [r_k = h_k(x) = h_k(x')] \\ &\geq \frac{|\mathbf{G}_{x_i}|}{2^k} - \frac{|\mathbf{G}_{x_i}| \cdot (|\mathbf{G}_{x_i}| - 1)}{2^{2k+1}}. \end{aligned} \quad (29)$$

Consider any $x \in I'_n \cap \mathbf{G}_{x_i}$, due to the definition of I'_n , it holds that

$$\Pr_{h_k} [\mathcal{A}(|\phi_x, h_k(x), h_k, k\rangle^{\otimes t}) \in \mathbf{N}_{x_i}^2(1/4\mathbf{p}(n)t(n))] \geq 1 - 1/4\mathbf{p}(n)t(n).$$

Since $\mathbf{N}_{x_i}^2(1/4\mathfrak{p}(n)t(n)) \subseteq \mathbf{G}_{x_i}$, we further have

$$\Pr_{h_k}[\mathcal{A}(|\phi_x, h_k(x), h_k, k\rangle^{\otimes t}) \in \mathbf{G}_{x_i}] \geq 1 - 1/4\mathfrak{p}(n)t(n).$$

Next, for those $x \in I'_n$ as input, \mathcal{A} would return a preimage in \mathbf{G}_{x_i} . Since

$$|(\mathcal{A}(|\phi_x, r_k, h_k, k\rangle^{\otimes t}))^\dagger \mathcal{A}(|\phi_{x^*}, r_k, h_k, k\rangle^{\otimes t})|^2 = |\langle \phi_x | \phi_{x^*} \rangle|^{2t} \geq 1 - 1/\mathfrak{p}(n),$$

for any $x \in \mathbf{G}_{x_i}$, therefore if we change the input state $|\phi_{x^*}\rangle$ by some state $|\phi_x\rangle$ satisfying $h_k(x) = r_k$ the output is similar as the former one except with $O(1/\mathfrak{p}(n))$ probability. More specifically

$$\Pr_{h_k}[\mathcal{A}(|\phi_{x^*}, h_k(x), h_k, k\rangle^{\otimes t}) \in \mathbf{G}_{x_i}] \geq 1 - \frac{5}{4 \cdot \mathfrak{p}(n)}.$$

And note that for any measurement $x \in \mathbf{G}_{x_i}$, \mathcal{B} accepts with probability at least $(1 - n^2/\mathfrak{p}(n))$, therefore

$$\begin{aligned} \Pr_{h_k}[\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}, h_k(x), h_k, k\rangle^{\otimes t}) \in \mathbf{G}_{x_i}] & \quad (30) \\ & \geq (1 - \frac{n^2}{\mathfrak{p}(n)})(1 - \frac{5}{4 \cdot \mathfrak{p}(n)}). \end{aligned}$$

Then we back to estimate the inequality (28) as follows. Since conditioned on $r_k \in h_k(x)$ for some $x \in \mathbf{G}_{x_i}$, the distribution of (r_k, h_k) is identical to the real distribution $(h_k(x), h_k)$, therefore according to inequalities (29) and (30), it holds that

$$\begin{aligned} & \Pr_{r_k, h_k}[\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}, r_k, h_k, k\rangle^{\otimes t}) \in \mathbf{G}_{x_i} \wedge r_k \in h_k(\mathbf{G}_{x_i})] \\ & \geq \Pr_{r_k, h_k}[\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}, r_k, h_k, k\rangle^{\otimes t}) \in \mathbf{G}_{x_i} \mid r_k \in h_k(\mathbf{G}_{x_i})] \\ & \quad \cdot \Pr_{r_k, h_k}[r_k \in h_k(\mathbf{G}_{x_i})] \\ & \geq (1 - \frac{n^2 \cdot t(n)}{\mathfrak{p}(n)})(1 - \frac{5}{4 \cdot \mathfrak{p}(n)}) \cdot \frac{|\mathbf{G}_{x_i}|}{2^k} - \frac{|\mathbf{G}_{x_i}| \cdot (|\mathbf{G}_{x_i}| - 1)}{2^{2k+1}} \\ & > (1 - \frac{n^2 \cdot t(n)}{\mathfrak{p}(n)} - \frac{5}{4 \cdot \mathfrak{p}(n)}) \cdot \frac{|\mathbf{G}_{x_i}|}{2^k} - \frac{|\mathbf{G}_{x_i}| \cdot (|\mathbf{G}_{x_i}| - 1)}{2^{2k+1}} \end{aligned}$$

That hence finish the first part of this claim. To show the other part, we let $a(n) := 1 - n^2 \cdot t(n)/\mathfrak{p}(n) - 5/(4 \cdot \mathfrak{p}(n))$, and g be the integer such that $2^g \leq |\mathbf{G}_{x_i}| < 2^{g+1}$. Then $p_k \geq a(n) \cdot (\frac{1}{2^{k-g}} - \frac{1}{2^{2k-2g+1}})$, therefore the probability that \mathcal{B} rejects for all the $k \in [\log |\mathbf{G}_{x_i}| + C \cdot \log n, n + C \cdot \log n]$ is at least

$$\begin{aligned} \prod_{k=n+C \cdot \log n}^{\log |\mathbf{G}_{x_i}| + C \cdot \log n} (1 - p_k)^m & \leq \prod_{k=n+C \cdot \log n}^{g+1+C \cdot \log n} (1 - a(n) \cdot (\frac{1}{2^{k-g}} - \frac{1}{2^{2k-2g+1}}))^m \\ & \leq \prod_{k=n+C \cdot \log n}^{g+1+C \cdot \log n} (1 - b(n) \cdot (\frac{1}{2^{k-g}}))^m \end{aligned}$$

where $b(n) := a(n) \cdot (1 - 1/(2 \cdot n^{2C}))$. Since the fact that

$$(1 - b(n) \cdot (\frac{1}{2^{k-g}}))^2 > 1 - b(n) \cdot (\frac{1}{2^{k-g-1}}),$$

we can further estimate the inequality as

$$\begin{aligned} & \prod_{k=n+C \cdot \log n}^{g+1+C \cdot \log n} (1 - b(n) \cdot (\frac{1}{2^{k-g}}))^m \\ & \leq \prod_{i=0}^{n-g-1} (1 - b(n) \cdot (\frac{1}{2^{n-i+C \log n-g}}))^m \\ & \leq \prod_{i=0}^{n-g-1} (1 - b(n) \cdot (\frac{1}{2^{n+C \log n-g}}))^{2^i \cdot m} \\ & = (1 - b(n) \cdot (\frac{1}{2^{n+C \log n-g}}))^{\sum_{i=0}^{n-g-1} 2^i \cdot m} \\ & < (1 - b(n) \cdot (\frac{1}{2^{n+C \log n-g}}))^{2^{n-g} \cdot m} \\ & < (1 - b(n) \cdot (\frac{1}{2^{n+C \log n-g}}))^{\frac{2^{n-g+C \log n}}{b(n)} \cdot m \cdot 2^{-C \log n} \cdot b(n)} \\ & < \frac{1}{e} \cdot 2^{C \log n \cdot b(n)} = \frac{1}{e} \cdot m \cdot n^{-C \cdot b(n)} \end{aligned}$$

That shows, if \mathcal{B} repeats $m > n^{C+1}/b(n)$ times for each $k \in [\log |\mathbf{G}_{x_i}| + C \cdot \log n, n + C \cdot \log n]$, it would accept with probability at least $1 - \exp(-n)$ for those given state $|\phi_{x^*}\rangle$ (which satisfies $x^* \in \mathbf{G}_{x_i}$). It's easy to see that when $n^2 t(n)/\mathbf{p}(n) = o(1)$, then m can be $2 \cdot n^{C+1}$ for all sufficiently large $n \in \mathbb{N}$. That completes the proof of Claim 1. \square

A.4 Proof of Claim 2

We firstly recall Claim 2 as follows:

Claim 2. For a given challenge state $|\phi_{x^*}\rangle$, where $x^* \in \mathbf{G}_{x_i}$, $p_{k,x}$ denotes the probability that \mathcal{B} accepts with the measurement x from \mathcal{A} at one repetition, then we can prove the following three facts.

1. For any $x \in I_n \setminus \mathbf{G}_{x_i}$, the probability that \mathcal{B} accepts with the measurement x it is at most $p_{k,x} < \mathbf{p}(n)^{-n^2}$.
2. For any $x \in \mathbf{G}_{x_i}$, and $k \geq \log |\mathbf{G}_{x_i}| + C \cdot \log n$ for some suitable $C > 0$, it holds that

$$\frac{(1 - n^{-2C} - (2 + t(n) \cdot n^2)/\mathbf{p}(n))}{2^k} \leq p_{k,x} \leq 1/2^k$$

3. For any $x \in \{x \mid \text{TD}(|\phi_{x_i}\rangle, |\phi_x\rangle) > \sqrt{1 - (1/\mathbf{p}(n))^{1/t(n)}/2}\} \setminus I_n$, the probability that \mathcal{A} output it is at most $p_{k,x} < \exp(-n^2/16)$

Proof (of Claim 2). It's easy to derive the Fact 1, since \mathbf{f} is “polarized” when it's not weak one-way, Lemma 4 implies that $|\langle \phi_x | \phi_{x^*} \rangle|^{2t} \leq 1/\mathbf{p}(n)$ for any $x \in I_n \setminus \mathbf{G}_{x_i}$. That implies if \mathcal{B} gets an $x \in I_n \setminus \mathbf{G}_{x_i}$ as a measurement returned by \mathcal{A} , it would accept with probability at most $|\langle \phi_x | \phi_{x^*} \rangle|^{2t \cdot n^2} \leq 1/\mathbf{p}(n)^{n^2}$. That immediately justifies the Fact 1.

The Fact 2 is the most important part, to prove that, we first show that h_k is injective on \mathbf{G}_{x_i} with high probability when $k \geq \log |\mathbf{G}_{x_i}| + C \cdot \log n$ for some suitable $C > 0$. Since h_k is universal hash, it holds that

$$\begin{aligned} & \Pr_{r_k, h_k} [|h_k^{-1}(r_k) \cap \mathbf{G}_{x_i}| \geq 2] \\ & \leq \sum_{x_0, x_1 \in \mathbf{G}_{x_i}} \Pr_{r_k, h_k} [h_k(x_0) = h_k(x_1) = r_k] \\ & \leq \frac{|\mathbf{G}_{x_i}| \cdot (|\mathbf{G}_{x_i}| - 1)}{2^{2k+1}} \leq n^{-2C} \end{aligned}$$

Therefore h_k is injective on \mathbf{G}_{x_i} with probability at least $1 - n^{-2C}$. Note that conditioned on h_k is injective on \mathbf{G}_{x_i} , the probability that $\mathcal{A}(|\phi_{x^*}\rangle, h_k(x), h_k, k)^{\otimes t}$ outputs $x \in \mathbf{G}_{x_i}$ is at least $1 - 5/(4 \cdot \mathbf{p}(n)) - n^{-2C}$ (since for a random h_k , $\mathcal{A}(|\phi_{x^*}\rangle, h_k(x), h_k, k)^{\otimes t}$ outputs $x \in \mathbf{G}_{x_i}$ with probability at least $1 - 5/(4 \cdot \mathbf{p}(n))$), and there are at most $1/n^{2C}$ of h_k is not injective). That hence implies

$$\begin{aligned} p_{k,x} &= \Pr_{r_k, h_k} [\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}\rangle, r_k, h_k, k)^{\otimes t} \rightarrow x \wedge r_k = h_k(x)] \quad (31) \\ &\geq \Pr_{r_k, h_k} [\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}\rangle, r_k, h_k, k)^{\otimes t} \rightarrow x \wedge r_k = h_k(x) \wedge h_k \text{ is injective on } \mathbf{G}_{x_i}] \\ &\geq \frac{(1 - n^2/\mathbf{p}(n))(1 - 5/4 \cdot \mathbf{p}(n) - n^{-2C})(1 - n^{-2C})}{2^k} \\ &> \frac{(1 - 2n^{-2C} - 5/4 \cdot \mathbf{p}(n) - n^2/\mathbf{p}(n))}{2^k}. \end{aligned}$$

On the other hand, since when \mathcal{A} returns x as a measurement, it's necessary to have $r_k \in h_k(x)$ for \mathcal{B} to accept, that implies

$$p_{k,x} \leq \Pr_{r_k, h_k} [r_k = h_k(x)] = 1/2^k \quad (32)$$

Combining the (32) with (32), we thus have

$$\frac{(1 - n^{-2C} - 2/\mathbf{p}(n) - t(n)n/\mathbf{p}(n))}{2^k} \leq p_{k,x} \leq 1/2^k,$$

which completes the proof of the Fact 2.

Then we turn to the final part, since

$$x \in \{x \mid \text{TD}(|\phi_{x_i}\rangle, |\phi_x\rangle) > \sqrt{1 - \left(\frac{1}{\mathbf{p}(n)}\right)^{1/t(n)}/2}\} \setminus I_n,$$

then in the case that \mathcal{B} gets such an x as a measurement, the probability that \mathcal{B} accepts it is at most

$$\begin{aligned}
|\langle \phi_x | \phi_{x^*} \rangle|^{2t(n) \cdot n^2} &\leq (1 - (\text{TD}(|\phi_{x_i}\rangle, |\phi_x\rangle) - \text{TD}(|\phi_{x^*}\rangle, |\phi_x\rangle))^2)^{t(n) \cdot n^2} \\
&\leq \left(1 - \left(\frac{\sqrt{1 - (1/\mathbf{p}(n))^{\frac{1}{t(n)}}} - \sqrt{1 - (1 - 1/\mathbf{p}(n))^{\frac{1}{t(n)}}}}{2}\right)^2\right)^{t(n) \cdot n^2} \\
&\leq \left(1 - \left(\frac{\sqrt{1 - (1/\mathbf{p}(n))^{\frac{1}{t(n)}}}}{4}\right)^2\right)^{t(n) \cdot n^2} \\
&\leq \left(1 - \frac{1 - (1/\mathbf{p}(n))^{\frac{1}{t(n)}}}{16}\right)^{t(n) \cdot n^2} \\
&\leq \left(\frac{15}{16} + \frac{(1/\mathbf{p}(n))^{\frac{1}{t(n)}}}{16}\right)^{t(n) \cdot n^2} \stackrel{*}{\leq} \left(1 - \frac{1}{16 \cdot t(n)}\right)^{t(n) \cdot n^2} \\
&\leq \exp(-n^2/16)
\end{aligned}$$

where (*) holds because $1/\mathbf{p}(n) < (1 - 1/t(n))^{t(n)}$ for all sufficiently large $n \in \mathbb{N}$. That hence completes the proof of Fact 3. That finishes the proof of Claim 2 \square

A.5 Proof of Theorem 8

We firstly recall the construction of Theorem 8 as follows:

The construction of distributionally OWSG: Assuming there exists a efficient sampler $((S_0^r, U_0^r), (S_1^r, U_1^r)) = (Q_0^r, Q_1^r) \leftarrow \mathbf{S}(r)$ such that the semi-classical QSD problem is hard on average on distribution of $\mathbf{S}(1^n)$ ¹⁴, then the following construction

$$\mathbf{f}(r, b, x) := |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle = |Q_0^r, Q_1^r\rangle \otimes |\phi_x^{U_b^r}\rangle \quad (33)$$

is a distributionally one-way state generator on the distribution over (r, b, x) .

We justify the quantum distributionally one-wayness of that construction by making a contradiction. Assuming there exist an adversary \mathcal{A} that takes $t(n)$ copies of a challenge state as input, and breaks the distributional one-wayness of $\mathbf{f}(r, b, x)$ efficiently. Namely, there exists a negligible function $\text{negl}(\cdot)$ such that

$$\begin{aligned}
&\mathbb{F}\left(\mathbb{E}_{r,b,x} |r, b, x\rangle\langle r, b, x| \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle \psi_{b,x}^{Q_0^r, Q_1^r}| \right. \\
&\quad \left. , \mathbb{E}_{r,b,x} \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle} \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle \psi_{b,x}^{Q_0^r, Q_1^r}| \right) \geq 1 - \text{negl}(n).
\end{aligned} \quad (34)$$

Where $\rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle}$ is the (mixed) state output by \mathcal{A} with $|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle^{\otimes t}$ as input, after tracing out all irrelevant part except the input register of \mathbf{f} (which contains only r, b, x).

¹⁴ Here $r \in \{0, 1\}^{l(n)}$ denote the internal randomness of \mathbf{S} where we assume the length of the random number of \mathbf{S} is same as \mathbf{S}_b^r since we can choose the longest $l(n)$ and it is also a polynomial of n .

We now give a QPT algorithm \mathcal{B} decides the instance $(Q_0^r, Q_1^r) = \mathcal{S}(r)$ as follows:

- \mathcal{B} is given $(Q_0^r, Q_1^r) \leftarrow \mathcal{S}(1^n)$ as its input, it firstly generates the state $\mathbb{E}_x |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle^{\otimes t+1}$ for a random $b \in \{0, 1\}$ and $x \in \{0, 1\}^k$.
- \mathcal{B} invokes \mathcal{A} with the input state $|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle^{\otimes t}$ and gets output (r^*, b^*, x^*) in result.
- \mathcal{B} returns 1 if $b \neq b^*$, otherwise, \mathcal{B} outputs a random decision $d \in \{0, 1\}$.

Note that some part of \mathcal{B} is described in classical setting, but it's equivalent to consider it as a mixed state of x . Then in order to estimate the success probability of \mathcal{B} , we firstly consider the inequality (34) by Lemma 3 and the definition of trace distance

$$\begin{aligned} 2 \cdot \mathbf{negl}(n) &\geq \text{TD} \left(\mathbb{E}_{r,b,x} |r, b, x\rangle\langle r, b, x| \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle \psi_{b,x}^{Q_0^r, Q_1^r}| \right. \\ &\quad \left. , \mathbb{E}_{r,b,x} \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle} \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle \psi_{b,x}^{Q_0^r, Q_1^r}| \right) \\ &= \max_P \text{Tr} P \left(\mathbb{E}_{r,b,x} (|r, b, x\rangle\langle r, b, x| - \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle}) \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle \psi_{b,x}^{Q_0^r, Q_1^r}| \right) \end{aligned} \quad (35)$$

Then we let P_0 and P_1 be some projections on the space spanned by $Q_0^r, Q_1^r \in \text{scQSD}_0$ and $Q_0^r, Q_1^r \in \text{scQSD}_1$ respectively¹⁵, then by average-case hardness of scQSD , we have

$$\begin{aligned} 2 \cdot \mathbf{negl}(n) &\geq |\text{Tr} P_d \left(\mathbb{E}_{r,b,x} (|r, b, x\rangle\langle r, b, x| - \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle}) \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle \psi_{b,x}^{Q_0^r, Q_1^r}| \right)| \\ &\geq \left(\frac{1}{2} - \mathbf{negl}_0(n) \right) |\text{Tr} P_d \left(\mathbb{E}_{r,b,x}^{Q_0^r, Q_1^r \in \text{scQSD}_d} (|r, b, x\rangle\langle r, b, x| - \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle}) \right. \\ &\quad \left. \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle \psi_{b,x}^{Q_0^r, Q_1^r}| \right)| \end{aligned}$$

for any possible projections space spanned by $Q_0^r, Q_1^r \in \text{scQSD}_d$. That hence implies

$$\begin{aligned} \text{TD} \left(\mathbb{E}_{r,b,x}^{Q_0^r, Q_1^r \in \text{scQSD}_d} |r, b, x\rangle\langle r, b, x| \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle \psi_{b,x}^{Q_0^r, Q_1^r}| \right. \\ \left. , \mathbb{E}_{r,b,x}^{Q_0^r, Q_1^r \in \text{scQSD}_d} \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle} \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle \psi_{b,x}^{Q_0^r, Q_1^r}| \right) \leq \mathbf{negl}'(n) \end{aligned} \quad (36)$$

for both $d = 0, 1$, and some negligible function $\mathbf{negl}'(\cdot)$.

Then we consider the $Q_0^r, Q_1^r \in \text{scQSD}_0$ and $Q_0^r, Q_1^r \in \text{scQSD}_1$ separately. When $Q_0^r, Q_1^r \in \text{scQSD}_0$, since it holds that

$$\text{TD}(|\psi_{0,x}^{Q_0^r, Q_1^r}\rangle\langle \psi_{0,x}^{Q_0^r, Q_1^r}|^{\otimes t+1}, |\psi_{1,x}^{Q_0^r, Q_1^r}\rangle\langle \psi_{1,x}^{Q_0^r, Q_1^r}|^{\otimes t+1}) \leq (t+1)/2^{-n} \quad (37)$$

¹⁵ Namely, P_d is the projection on the space that generated by $\{|r, b, x, Q_0, Q_1, \phi\rangle \mid (Q_0, Q_1) \in \text{scQSD}_0, r \in \{0, 1\}^l, b \in \{0, 1\}, x \in \{0, 1\}^k, \phi \in \{0, 1\}^m\}$

for any $Q_0^r, Q_1^r \in \text{scQSD}_0$, hence when we replace the challenge state $|\psi_{1,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{1,x}^{Q_0^r, Q_1^r}|^{\otimes t+1}$ by the $|\psi_{0,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{0,x}^{Q_0^r, Q_1^r}|^{\otimes t+1}$ the output of \mathcal{A} would only change slightly, more specifically, according to (35) and (37), it holds that

$$\text{TD}\left(\mathbb{E}_{r,b,x}^{Q_0^r, Q_1^r \in \text{scQSD}_0} |r, b, x\rangle\langle r, b, x| \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r, Q_1^r}| \right. \\ \left. , \mathbb{E}_{r,x}^{Q_0^r, Q_1^r \in \text{scQSD}_0} \rho_{\mathcal{A},t}^{|\psi_{0,x}^{Q_0^r, Q_1^r}\rangle} \otimes |\psi_{0,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{0,x}^{Q_0^r, Q_1^r}| \right) \leq \text{negl}'(n) + (t+1)/2^{-n}.$$

That implies, when tracing out the all the register except the b (we denote by these register the W_0) output by $\rho_{\mathcal{A},t}^{|\psi_{0,x}^{Q_0^r, Q_1^r}\rangle}$, we can get

$$\left| \langle 1 | \text{Tr}_{W_0} \mathbb{E}_{r,x}^{Q_0^r, Q_1^r \in \text{scQSD}_0} \rho_{\mathcal{A},t}^{|\psi_{0,x}^{Q_0^r, Q_1^r}\rangle} | 1 \rangle - \frac{1}{2} \right| \leq \text{negl}_1(n)$$

for some negligible function. That implies when \mathcal{A} takes $\mathbb{E}_x^{Q_0^r, Q_1^r \in \text{scQSD}_0} |\psi_{0,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{0,x}^{Q_0^r, Q_1^r}|$ as input state, it would output $b^* = 1$ with probability nearly equals to $1/2$ over the randomness of r and the internal randomness of \mathcal{A} . By a similar argument, we can get the same conclusion for the case that \mathcal{A} takes $\mathbb{E}_{r,x}^{Q_0^r, Q_1^r \in \text{scQSD}_0} |\psi_{1,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{1,x}^{Q_0^r, Q_1^r}|$ as input. Therefore we have

$$\Pr_{(Q_0, Q_1) \leftarrow \mathbf{s}(1^n)} [\mathcal{B}(Q_0, Q_1) = 1 \mid (Q_0, Q_1) \in \text{scQSD}_0] \leq \frac{1}{2} + \text{negl}_1(n) \quad (38)$$

On the other hand, when $Q_0^r, Q_1^r \in \text{scQSD}_1$, since

$$\text{TD}\left(\mathbb{E}_{r,b,x}^{Q_0^r, Q_1^r \in \text{scQSD}_1} |r, b, x\rangle\langle r, b, x| \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r, Q_1^r}| \right. \\ \left. , \mathbb{E}_{r,b,x}^{Q_0^r, Q_1^r \in \text{scQSD}_1} \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle} \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r, Q_1^r}| \right) \leq \text{negl}'(n).$$

By the definition of scQSD_1 , it holds that

$$\text{TD}(\mathbb{E}_x |\psi_{0,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{0,x}^{Q_0^r, Q_1^r}|^{\otimes t+1}, \mathbb{E}_x |\psi_{1,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{1,x}^{Q_0^r, Q_1^r}|^{\otimes t+1}) \geq 1 - 2^{-(n+1)t/2}$$

We then denote by $P_{Q_0^r, Q_1^r}$ the projection that maximizes the trace distance between $\mathbb{E}_x |\phi_x^{U_0^r}\rangle\langle\phi_x^{U_0^r}|$ and $\mathbb{E}_x |\phi_x^{U_1^r}\rangle\langle\phi_x^{U_1^r}|$, namely

$$\text{Tr} P_{Q_0^r, Q_1^r} \mathbb{E}_x (|\phi_x^{U_0^r}\rangle\langle\phi_x^{U_0^r}| - |\phi_x^{U_1^r}\rangle\langle\phi_x^{U_1^r}|) \\ = \text{TD}(\mathbb{E}_x |\phi_x^{U_0^r}\rangle\langle\phi_x^{U_0^r}|, \mathbb{E}_x |\phi_x^{U_1^r}\rangle\langle\phi_x^{U_1^r}|) \geq 1 - 2^{-n}.$$

That indicates $\text{Tr} P_{Q_0^r, Q_1^r} \mathbb{E}_x (|\phi_x^{U_1^r}\rangle\langle\phi_x^{U_1^r}|) \leq 2^{-n}$ and $\text{Tr} P_{Q_0^r, Q_1^r} \mathbb{E}_x (|\phi_x^{U_0^r}\rangle\langle\phi_x^{U_0^r}|) \geq 1 - 2^{-n}$. Then we denote by P the projection as follows

$$P := \sum_{Q_0^r, Q_1^r \in \text{scQSD}_1} |0\rangle\langle 0| \otimes |Q_0^r, Q_1^r\rangle\langle Q_0^r, Q_1^r| \otimes P_{Q_0^r, Q_1^r}.$$

After tracing out the register that contains the r and x (we denote by the registers R, X), the trace distance can be further estimated as

$$\begin{aligned}
 \text{TD} & \left(\mathbb{E}_{r,b,x}^{Q_0^r, Q_1^r \in \text{scQSD}_1} |r, b, x\rangle\langle r, b, x| \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r, Q_1^r}| \right. \\
 & \left. , \mathbb{E}_{r,b,x}^{Q_0^r, Q_1^r \in \text{scQSD}_1} \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle} \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r, Q_1^r}| \right) \\
 & \geq \text{TD} \left(\text{Tr}_{R,X} \mathbb{E}_{r,b,x}^{Q_0^r, Q_1^r \in \text{scQSD}_1} |r, b, x\rangle\langle r, b, x| \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r, Q_1^r}| \right. \\
 & \left. , \text{Tr}_{R,X} \mathbb{E}_{r,b,x}^{Q_0^r, Q_1^r \in \text{scQSD}_1} \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle} \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r, Q_1^r}| \right) \\
 & \geq \text{Tr}P \left(\mathbb{E}_{r,b,x}^{Q_0^r, Q_1^r \in \text{scQSD}_1} (|b\rangle\langle b| - \text{Tr}_{R,X} \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r, Q_1^r}\rangle}) \otimes |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r, Q_1^r}| \right) \\
 & \geq \frac{1}{2} \cdot \text{Tr}P \left(\mathbb{E}_{r,x}^{Q_0^r, Q_1^r \in \text{scQSD}_1} (|0\rangle\langle 0| - \text{Tr}_{R,X} \rho_{\mathcal{A},t}^{|\psi_{0,x}^{Q_0^r, Q_1^r}\rangle}) \otimes |\psi_{0,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{0,x}^{Q_0^r, Q_1^r}| \right) - 2^{-n} \\
 & \geq \frac{1}{2} (1 - 2^{-n}) (1 - \mathbb{E}_{r,x}^{Q_0^r, Q_1^r \in \text{scQSD}_1} \langle 0 | \text{Tr}_{R,X} \rho_{\mathcal{A},t}^{|\psi_{0,x}^{Q_0^r, Q_1^r}\rangle} | 0 \rangle).
 \end{aligned} \tag{39}$$

According to (35) and (39), we have

$$\mathbb{E}_{r,x}^{Q_0^r, Q_1^r \in \text{scQSD}_1} \langle 0 | \text{Tr}_{R,X} \rho_{\mathcal{A},t}^{|\psi_{0,x}^{Q_0^r, Q_1^r}\rangle} | 0 \rangle \geq 1 - \text{negl}_2(n) \tag{40}$$

for some negligible function $\text{negl}_2(\cdot)$. That implies, when taking $\mathbb{E}_x |\psi_{0,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{0,x}^{Q_0^r, Q_1^r}|^{\otimes t}$ as input for some $Q_0^r, Q_1^r \in \text{scQSD}_1$, the output b^* by \mathcal{A} would equal to the real b with overwhelming probability over the randomness of r and the internal randomness of \mathcal{A} . By a similar argument, we can get the same conclusion for the case that \mathcal{A} takes $\mathbb{E}_{r,x}^{Q_0^r, Q_1^r \in \text{scQSD}_0} |\psi_{1,x}^{Q_0^r, Q_1^r}\rangle\langle\psi_{1,x}^{Q_0^r, Q_1^r}|$ as input. Therefore we have

$$\Pr_{(Q_0, Q_1) \leftarrow \mathcal{S}(1^n)} [\mathcal{B}(Q_0, Q_1) = 1 \mid (Q_0, Q_1) \in \text{scQSD}_1] \geq 1 - \text{negl}_2(n) \tag{41}$$

Combining the inequalities (38) and (41), we have

$$\begin{aligned}
 & \Pr_{(Q_0, Q_1) \leftarrow \mathcal{S}(1^n)} [\mathcal{B}(Q_0, Q_1) = 1 \mid (Q_0, Q_1) \in \text{scQSD}_0] \\
 & \quad - \Pr_{(Q_0, Q_1) \leftarrow \mathcal{S}(1^n)} [\mathcal{B}(Q_0, Q_1) = 1 \mid (Q_0, Q_1) \in \text{scQSD}_1] \\
 & \geq \frac{1}{2} - \text{negl}_3(n)
 \end{aligned} \tag{42}$$

for some negligible function $\text{negl}_3(\cdot)$. That hence contradict the average-case hardness of the **scQSD** problem, which justify our result. \square

A.6 Proof of Theorem 9

We firstly recall the construction of Theorem 9 as follows:

The construction of quantum bit commitment: Assuming there exists a efficient sampler $(Q_0^r, Q_1^r) \leftarrow \mathbf{S}(r)$ such that the QSD problem is hard on average on distribution of $\mathbf{S}(1^n)$ (here $r \in \{0, 1\}^{l(n)}$ denote the internal randomness of \mathbf{S} , and we denote it by l for short when there is no confusion), then we give a quantum bit commitment scheme as follows:

- **Commit phase:** The commiter generates $|0\rangle \xrightarrow{H^{\otimes l \cdot n}} \bigotimes_{i=1}^n \sum_{r_i} |r_i\rangle / 2^{l/2}$, then gets n copies of the superposition state of these circuits from \mathbf{S}

$$\bigotimes_{i=1}^n \sum_{r_i} \frac{|r_i, 0\rangle}{2^{l/2}} \xrightarrow{\mathbf{S}^{\otimes n}} \bigotimes_{i=1}^n \sum_{r_i} \frac{|r_i, Q_0^{r_i}, Q_1^{r_i}\rangle}{2^{l/2}}.$$

Then the commiter randomly chooses $b \leftarrow \{0, 1\}$ and generates

$$\bigotimes_{i=1}^n \sum_{r_i} \frac{|r_i, Q_0^{r_i}, Q_1^{r_i}, 0\rangle}{2^{l/2}} \xrightarrow{U^{\otimes n}} |\Psi_b\rangle_{ABCD}^{\otimes n}.$$

Where

$$|\Psi_b\rangle_{ABCD} := \sum_r \frac{|Q_0^r, Q_1^r\rangle_A \otimes |PQ_b^r|0\rangle_{BC} \otimes |r\rangle_D}{2^{l/2}}$$

PQ_b^r denotes a purified circuit of Q_b^r (here we choose a deterministic procedure of the purification in this commit algorithm). Then the commiter sends the registers A, B of $|\Psi_b\rangle_{ABCD}^{\otimes n}$ to the receiver, where A stores the Q_0^r, Q_1^r , the registers B, C store the output/ancilla part of $PQ_b^r|0\rangle$, and D stores the copied Q_0^r, Q_1^r and the random number r .

- **Reveal phase:** The commiter sends the register C, D and the message b to the receiver. The receiver invokes the operator $(H^{\otimes l} \otimes \mathbf{S}^\dagger \otimes I \circ U^\dagger)^{\otimes n}$ to the whole system, then measures the resulting state in the computational basis. The receiver accepts iff the measurement is 0.

It is not hard to derive the correctness of this construction. The remaining aims to discuss the hiding and binding properties. We firstly show that any efficient adversary can't break the computational hiding property unless it breaks the average-case hardness of the QSD problem. We prove it by making a contradiction, let \mathcal{A} be the adversary that breaks the computational hiding, instead of considering it as a unitary operator, without loss of generality, we assume \mathcal{A} is a linear trace-preserving CP maps which takes $\text{Tr}_{C,D} |\Psi_0\rangle \langle \Psi_0|^{\otimes n}$ as input, outputs one qubit (mixed) state $u_0|0\rangle \langle 0| + u_1|1\rangle \langle 1|$ as its decision, and when refer to $\mathcal{A}(\rho) \rightarrow b$, we denote the event that \mathcal{A} gets a measurement b with ρ as

its input. It then holds that

$$\begin{aligned}
 & |\Pr[\text{Exp}_{\mathcal{A}}^{\text{hiding}}(0) = 1] - \Pr[\text{Exp}_{\mathcal{A}}^{\text{hiding}}(1) = 1]| \\
 & \leq \text{TD}(\mathcal{A}(\text{Tr}_{C,D}|\Psi_0\rangle\langle\Psi_0|^{\otimes n}), \mathcal{A}(\text{Tr}_{C,D}|\Psi_1\rangle\langle\Psi_1|^{\otimes n})) \\
 & \leq \left(1 - \left(\mathbb{F}\left[\mathcal{A}\left(\mathbb{E}_{r_1, \dots, r_n} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_1^{r_i}\right)\right.\right.\right. \\
 & \quad \left.\left.\left.\mathcal{A}\left(\mathbb{E}_{r_1, \dots, r_n} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_0^{r_i}\right)\right]\right)\right)^{\frac{1}{2}}
 \end{aligned}$$

Where ρ_b^r denotes the (mixed) state produced by the quantum circuit Q_b^r . And if we denote by $P_{b,b'}^A$ the probability that \mathcal{A} takes $\mathbb{E}_{r_1, \dots, r_n} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_b^{r_i}$ as input, and outputs b' . Then it holds that

$$\begin{aligned}
 & 1 - \left(\mathbb{F}\left[\mathcal{A}\left(\mathbb{E}_{r_1, \dots, r_n} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_1^{r_i}\right)\right.\right. \\
 & \quad \left.\left.\mathcal{A}\left(\mathbb{E}_{r_1, \dots, r_n} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_0^{r_i}\right)\right]\right)^2 \\
 & \leq 1 - \left(\sqrt{P_{0,0}^A \cdot P_{1,0}^A} + \sqrt{P_{0,1}^A \cdot P_{1,1}^A}\right)^2 \\
 & = 1 - P_{0,0}^A + P_{0,0}^A \cdot P_{1,1}^A - P_{0,1}^A + P_{0,1}^A \cdot P_{1,0}^A - 2\sqrt{P_{0,0}^A \cdot P_{1,0}^A \cdot P_{0,1}^A \cdot P_{1,1}^A} \\
 & = \left(\sqrt{P_{0,0}^A \cdot P_{1,1}^A} - \sqrt{P_{0,1}^A \cdot P_{1,0}^A}\right)^2 \stackrel{*}{\leq} \left(\sqrt{P_{1,1}^A} - \sqrt{P_{0,1}^A}\right)^2 \stackrel{**}{\leq} 2 \cdot |P_{1,1}^A - P_{0,1}^A|.
 \end{aligned}$$

Here (*) and (**) holds because $P_{b,b'}^A \leq 1$ and $P_{b,b'}^A = 1 - P_{b,b' \oplus 1}^A$ for any $b, b' \in \{0, 1\}$. Note that

$$P_{b,b'}^A = \Pr_{r_1, \dots, r_n} [\mathcal{A}\left(\bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_b^{r_i}\right) = b'].$$

Therefore, if \mathcal{A} breaks the computational hiding property with non-negligible advantage, we can derive that there exist $c > 0$ such that

$$|P_{1,1}^A - P_{0,1}^A| \geq \frac{1}{n^c} \quad (43)$$

for infinitely $n \in \mathbb{N}$.

Then for $j \in \{0, \dots, n\}$, we denote by $\text{Hyb}_j = b$ the following event:

- Choose r_1, \dots, r_n uniformly at random and generate $\mathfrak{S}(r_i) = (Q_0^{r_i}, Q_1^{r_i})$.
- \mathcal{A} is given $\bigotimes_{i=1}^{n-j} |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_0^{r_i} \otimes_{i=n-j+1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_1^{r_i}$ as input state, and output b as the measurement.

Note that the Hyb_0 and Hyb_n represent the two cases of in the inequality (43), therefore

$$\begin{aligned} & \mathbb{E}_j |\Pr[\text{Hyb}_j = 1] - \Pr[\text{Hyb}_{j+1} = 1]| \\ & \geq \left| \sum_{j=0}^{n-1} (\Pr[\text{Hyb}_j = 1] - \Pr[\text{Hyb}_{j+1} = 1]) \right| / n \\ & = |P_{1,1}^{\mathcal{A}} - P_{0,1}^{\mathcal{A}}| \geq \frac{1}{n^{c+1}} \end{aligned} \quad (44)$$

We denote j_{max} that maximizes the $|\Pr[\text{Hyb}_j = 1] - \Pr[\text{Hyb}_{j+1} = 1]|$. And without loss of generality, we assume $\Pr[\text{Hyb}_{j_{max}+1} = 1] > \Pr[\text{Hyb}_{j_{max}} = 1]$. Based the inequality above, we construct an adversary \mathcal{B} for the QSD as follows:

- \mathcal{B} receives a Q_0, Q_1 as its input, its task is to determine whether $(Q_0, Q_1) \in \text{QSD}_1$ or not.
- \mathcal{B} choose $j \leftarrow \{1, \dots, n\}$ randomly, then generates $r_1, \dots, r_{j-1}, r_{j+1}, \dots, r_n$ uniformly at random and invokes $\mathbf{S}(1^n, r_i) = (Q_0^{r_i}, Q_1^{r_i})$ for those r_i , and sets $(Q_0^{r_j}, Q_1^{r_j}) = (Q_0, Q_1)$.
- \mathcal{B} tosses $t \leftarrow \{0, 1\}$, if $t = 0$, it runs \mathcal{A} with input state

$$\bigotimes_{i=1}^{n-j} |Q_0^{r_i}, Q_1^{r_i}\rangle \langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_0^{r_i} \bigotimes_{i=n-j+1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle \langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_1^{r_i}$$

if $t = 1$, it runs \mathcal{A} with input state

$$\bigotimes_{i=1}^{n-j-1} |Q_0^{r_i}, Q_1^{r_i}\rangle \langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_0^{r_i} \bigotimes_{i=n-j}^n |Q_0^{r_i}, Q_1^{r_i}\rangle \langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_1^{r_i}.$$

- \mathcal{B} returns 1 if \mathcal{A} outputs t , otherwise, it returns 0.

Therefore, we can deduce that

$$\begin{aligned} & |\Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n)] - \frac{1}{2}| \\ & = \frac{1}{2} \cdot \left| \mathbb{E}_j (\Pr[\text{Hyb}_j = 0 \mid t = 0] + \Pr[\text{Hyb}_{j+1} = 1 \mid t = 1]) - 1 \right| \\ & = \frac{1}{2} \cdot \left| \mathbb{E}_j (\Pr[\text{Hyb}_j = 1] - \Pr[\text{Hyb}_{j+1} = 1]) \right| \geq \frac{1}{n^{c+1}} \end{aligned} \quad (45)$$

Therefore, either $\Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n)] \geq 1/2 + 1/n^{c+1}$, or $\Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n)] \leq 1/2 - 1/n^{c+1}$, and here we assume the first case, the conclusion of other case can be derived accordingly.

Since $\text{TD}(\rho_0^{r_j}, \rho_1^{r_j}) \leq 2^{-n}$ when $(Q_0, Q_1) \in \text{QSD}_0$, that hence implies the difference is negligible if we replace the $\rho_1^{r_j}$ by $\rho_0^{r_j}$, namely

$$\begin{aligned}
 & \Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n) \mid (Q_0, Q_1) \in \text{QSD}_0] \\
 &= \frac{1}{2} \cdot \mathbb{E}_j (\Pr[\text{Hyb}_j = 0 \mid (Q_0, Q_1) \in \text{QSD}_0 \wedge t = 0] \\
 &\quad + \Pr[\text{Hyb}_{j+1} = 1 \mid (Q_0, Q_1) \in \text{QSD}_0 \wedge t = 1]) \tag{46} \\
 &\leq \frac{1}{2} \cdot \mathbb{E}_j (\Pr[\text{Hyb}_j = 0 \mid (Q_0, Q_1) \in \text{QSD}_0 \wedge t = 0]) \\
 &\quad + \Pr[\text{Hyb}_j = 1 \mid (Q_0, Q_1) \in \text{QSD}_0 \wedge t = 1] + \text{negl}_1(n) \\
 &\leq \frac{1}{2} \cdot (1 + \text{negl}_1(n))
 \end{aligned}$$

for some negligible function $\text{negl}_1(\cdot)$. Since it probability that $(Q_0, Q_1) \in \text{QSD}_0$ from $(Q_0, Q_1) \leftarrow \mathbf{S}(1^n)$ is nearly equal to $1/2$, namely

$$\frac{1}{2} - \text{negl}_0(n) \leq \Pr[(Q_0, Q_1) \in \text{QSD}_0 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n)] \leq \frac{1}{2} + \text{negl}_0(n)$$

Therefore, we have

$$\begin{aligned}
 & \Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n) \mid (Q_0, Q_1) \in \text{QSD}_1] \cdot \left(\frac{1}{2} + \text{negl}_0(n)\right) \\
 &\geq \Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n) \mid (Q_0, Q_1) \in \text{QSD}_1] \cdot \Pr[(Q_0, Q_1) \in \text{QSD}_1] \\
 &\geq \Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n)] \\
 &\quad - \left(\frac{1}{2} + \text{negl}_0(n)\right) \cdot \Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n) \mid (Q_0, Q_1) \in \text{QSD}_0] \\
 &\stackrel{*}{\geq} \Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n)] - \frac{1}{2} \cdot (1 + \text{negl}_1(n)) \cdot \left(\frac{1}{2} + \text{negl}_0(n)\right) \\
 &\stackrel{**}{\geq} \frac{1}{4} + \frac{1}{n^{c+1}} - \text{negl}_2(n)
 \end{aligned}$$

for infinitely many n , where $(*)$ comes from the inequality (46), and $(**)$ holds because the we assume the case that $\Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n)] \geq 1/2 + 1/n^{c+1}$ of the inequality (45)¹⁶. That inequality indicates there is a negligible function $\text{negl}(\cdot)$ such that

$$\begin{aligned}
 & \Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n) \mid (Q_0, Q_1) \in \text{QSD}_1] \tag{47} \\
 &\geq \frac{1}{2} + \frac{2}{n^{c+1}} - \text{negl}(n).
 \end{aligned}$$

for infinitely many n .

¹⁶ In the other case that $\Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n)] \leq 1/2 - 1/n^{c+1}$, we can estimate the lower bound of that probability, which is $1/2 - \text{negl}_1(n)$, and the upper bound of $\Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathbf{S}(1^n) \mid (Q_0, Q_1) \in \text{QSD}_1]$ is $1/2 - 2/n^{c+1} + \text{negl}(n)$.

Therefore, combine the inequality (46) with (47), we thus have

$$\begin{aligned} & |\Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathcal{S}(1^n) \mid (Q_0, Q_1) \in \text{QSD}_1] \\ & \quad - \Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathcal{S}(1^n) \mid (Q_0, Q_1) \in \text{QSD}_0]| \\ & \geq \frac{2}{n^{c+1}} - \text{negl}'(n) \end{aligned}$$

for some negligible function $\text{negl}'(\cdot)$, which breaks the average-case hardness of QSD problem. That hence prove the computational hiding of this construction.

Then we discuss the sum-binding, we denote by p_b the probability that the receiver accepts with the message b , and we let a cheating commiter sends $\text{Tr}_{C,D,E}|\Psi\rangle\langle\Psi|$ as the commitment where $|\Psi\rangle\langle\Psi|$ is some “fake” state generated by a cheating commiter. Then the cheating commiter invokes the operator U_{CDE}^b when he want to open with b where E stores the auxiliary qubits of a cheating commiter. Since the monotonicity of the fidelity under trace-preserving CP maps, it holds that

$$\begin{aligned} p_0 + p_1 &= \sum_b \langle \Psi_b |^{\otimes n} I \otimes \text{Tr}_E(U_{CDE}^b |\Psi\rangle\langle\Psi| I \otimes U_{CDE}^b) | \Psi_b \rangle^{\otimes n} \quad (48) \\ &= \sum_b F(|\Psi_b\rangle\langle\Psi_b|^{\otimes n}, I \otimes \text{Tr}_E(U_{CDE}^b |\Psi\rangle\langle\Psi| I \otimes U_{CDE}^b))^2 \\ &\leq \sum_b F(\text{Tr}_{C,D} |\Psi_b\rangle\langle\Psi_b|^{\otimes n}, I \otimes \text{Tr}_{C,D,E}(U_{CDE}^b |\Psi\rangle\langle\Psi| I \otimes U_{CDE}^b))^2 \\ &\leq \sum_b F(\text{Tr}_{C,D} |\Psi_b\rangle\langle\Psi_b|^{\otimes n}, \text{Tr}_{C,D,E}(|\Psi\rangle\langle\Psi|))^2 \\ &\stackrel{*}{\leq} 1 + F(\text{Tr}_{C,D} |\Psi_0\rangle\langle\Psi_0|^{\otimes n}, \text{Tr}_{C,D} |\Psi_1\rangle\langle\Psi_1|^{\otimes n}) \\ &\leq 1 + (1 - \text{TD}(\text{E}_{r_1, \dots, r_n} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_0^{r_i} \\ & \quad , \text{E}_{r_1, \dots, r_n} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_1^{r_i}))^{\frac{1}{2}}. \end{aligned}$$

Where (*) holds because $F(\eta_0, \eta_1)^2 + F(\eta_0, \eta_2)^2 \leq 1 + F(\eta_1, \eta_2)$ for any state η_0, η_1, η_2 [37,35].

Then we further estimate the trace distance above. Since it holds that

$$\begin{aligned} & \text{TD}(\text{E}_{r_1, \dots, r_n} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_0^{r_i}, \text{E}_{r_1, \dots, r_n} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes \rho_1^{r_i}) \\ & \geq \text{Tr}(P_{r_1, \dots, r_n} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle\langle Q_0^{r_i}, Q_1^{r_i}| \otimes (\bigotimes_{i=1}^n \rho_0^{r_i} - \bigotimes_{i=1}^n \rho_1^{r_i})) \end{aligned}$$

for any $0 \leq P \leq I$. We hence let

$$P := \sum_{r_1, \dots, r_n}^{\exists i: Q_0^{r_i}, Q_1^{r_i} \in \text{QSD}_1} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle \langle Q_0^{r_i}, Q_1^{r_i}| \otimes P_{r_1, \dots, r_n},$$

where P_{r_1, \dots, r_n} is the projection that maximizes the trace of $(\bigotimes_{i=1}^n \rho_0^{r_i} - \bigotimes_{i=1}^n \rho_1^{r_i})$, namely

$$\text{TD}(\bigotimes_{i=1}^n \rho_0^{r_i}, \bigotimes_{i=1}^n \rho_1^{r_i}) = P_{r_1, \dots, r_n} (\bigotimes_{i=1}^n \rho_0^{r_i} - \bigotimes_{i=1}^n \rho_1^{r_i}).$$

And in the case that there exists i such that $Q_0^{r_i}, Q_1^{r_i} \in \text{QSD}_1$, we have

$$P_{r_1, \dots, r_n} (\bigotimes_{i=1}^n \rho_0^{r_i} - \bigotimes_{i=1}^n \rho_1^{r_i}) = \text{TD}(\bigotimes_{i=1}^n \rho_0^{r_i}, \bigotimes_{i=1}^n \rho_1^{r_i}) \geq 1 - 2^{-n}.$$

Since the event that $\exists i : Q_0^{r_i}, Q_1^{r_i} \in \text{QSD}_1$ occurs with overwhelming probability

$$\Pr_{r_1, \dots, r_n} [\exists i : Q_0^{r_i}, Q_1^{r_i} \in \text{QSD}_1] \geq 1 - \left(\frac{1}{2} + \text{negl}_0(n)\right)^n > 1 - \left(\frac{2}{3}\right)^n$$

for all sufficiently large $n \in \mathbb{N}$. We further have

$$\begin{aligned} & \text{Tr}(P \mathbb{E}_{r_1, \dots, r_n} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle \langle Q_0^{r_i}, Q_1^{r_i}| \otimes (\bigotimes_{i=1}^n \rho_0^{r_i} - \bigotimes_{i=1}^n \rho_1^{r_i})) \quad (49) \\ & \geq \text{Tr} \left(\sum_{r_1, \dots, r_n}^{\exists i: Q_0^{r_i}, Q_1^{r_i} \in \text{QSD}_1} \bigotimes_{i=1}^n |Q_0^{r_i}, Q_1^{r_i}\rangle \langle Q_0^{r_i}, Q_1^{r_i}| \otimes P_{r_1, \dots, r_n} (\bigotimes_{i=1}^n \rho_0^{r_i} - \bigotimes_{i=1}^n \rho_1^{r_i}) / 2^l \right) \\ & \geq \left(1 - \left(\frac{2}{3}\right)^n\right) \cdot (1 - 2^{-n}). \end{aligned}$$

Combining the inequality (49) with (48), we thus have

$$\begin{aligned} p_0 + p_1 &= 1 - \left(1 - \left[1 - \left(\frac{2}{3}\right)^n \cdot (1 - 2^{-n})\right]^2\right)^{\frac{1}{2}} \\ &\leq 1 + \text{negl}(n) \end{aligned}$$

for some negligible function, that hence completes the proof of the sum-binding property. \square