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 the 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:

- Two variants of one-way quantum state generator are proposed, called the weak one-way quantum state generator and distributionally one-way quantum state generator. Then the equivalence among these three objects is obtained.
- We construct the distributionally one-way quantum state generator from average-case hardness assumption of a promise problem belongs to QSZK, and hence a construction of one-way quantum state generator is implied.
- We construct quantum bit commitment with statistical binding (sum-binding) and computational hiding directly from the average-case hardness 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 $\mathsf{QMA}^{\mathcal{U}}$.

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 ([20,18,26,44,19,37,23,32]). By Impagliazzo's famous "five worlds" [25], it is called the MiniCrypt that the world OWF exists.

As a quantum analogue to MiniCrypt, the MiniQCrypt represents the world that post-quantum secure one-way function (pqOWF) exists [21]. Many results seem to be consistent with the classical setting [49,10,50]. However, MiniQCrypt may contain some objects that contrast to its classical counterpart. When allowing quantum communication, the celebrated result by Bennett and Brassard showed that the key exchange protocol doesn't need to rely on any cryptographic assumption in quantum world [7] which seems impossible in classical world due to the negative result [27]. Moverover, two independent works concurrently 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]. Whereas, in classical world, no such construction has been found, OT is believed to be a "higher-level" primitive than OWFs due to the black-box barrier [27,33].

It seems that the existence of pqOWFs is probably not necessary for some quantum objects whose classical counterparts are equivalent to (or even "stronger" than) OWFs in classical world. In lieu of outputting a string, Ji, Liu, and Song proposed a quantum analogue of PRGs which is called the pseudorandom states (PRSs) [28]. Taking a random seed as input, PRS outputs a quantum state which masquerades as a real random state (sampled from the Haar measure). 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 $\mathsf{QMA}^{\mathcal{O}} = \mathsf{BQP}^{\mathcal{O}}$ while PRS (and even pseudorandom unitary) still exists, the result by Kretschmer gave negative evidence for ensuring pqOWF from PRS [31]. By exploiting the nature of PRSs, two recently results by Morimae et al. and Ananth et al. devised constructions of quantum commitment from PRSs [36,5], 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 OWSG to one-time secure digital signatures with quantum public keys [36]. Ananth et al. 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 well-known complexity assumptions "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 [36]. Informally, a quantum polynomial-time (QPT) algorithm $\mathtt{f}$ is OWSGs, if it takes a string x as input, and output a state $|\phi_x\rangle$ (it can also be defined as outputting a mixed state by the very recent result [35]) 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. More precisely, PRS is also OWSG.

OWSGs can be treated as the quantum version of OWFs, not only because of the similarity between their definitions, but also due to the potential relations to other cryptographic objects (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 OWSGs [31]. But unfortunately, it remains to be unknown that how to devise a non-trivial construction of OWSGs which can not achieve the requirement of pqOWFs simultaneously.

1.1 Overview of Our Results and Techniques

In a nutshell, this work explores 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 are summarized as 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 QPT algorithm $\mathtt{f}$ which takes a string x as input and outputs a state $|\phi_x\rangle$, the quantum one-wayness of $\mathtt{f}$ is defined by the computational infeasibility of any QPT adversary $\mathcal{A}$ for finding a similar preimage x' [36]. That similarity is characterized by the inner product $|\langle\phi_x|\phi_{x'}\rangle|$ between the fake state $|\phi_{x'}\rangle$ and the real challenge state $|\phi_x\rangle$ which should be negligible when $\mathtt{f}$ 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 generators (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 bounds the success probability to be at most $1 - 1/\mathtt{p}(n)$ for any QPT adversary $\mathcal{A}$ and positive polynomial $\mathtt{p}(\cdot)$. $\mathcal{A}$ succeeds iff it measures $|\phi_x\rangle$ with the basis $\{|\phi_{x'}\rangle\langle\phi_{x'}|, I - |\phi_{x'}\rangle\langle\phi_{x'}|\}$ generated by the forged x' and gets $|\phi_{x'}\rangle$ in result. To define the distributionally OWSGs, note that the distributionally OWF requires the hardness for generating 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. Taking inspiration of that, 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 challenge state. Then the distributionally one-wayness is characterized by the existence of some polynomial n^c such that

$$\mathrm{F}\big(\mathop{\mathrm{E}}_{x}|x\rangle\langle x|\otimes|\phi_x\rangle\langle\phi_x|, \mathop{\mathrm{E}}_{x}\rho_{\mathcal{A},t}^{|\phi_x\rangle}\otimes|\phi_x\rangle\langle\phi_x|\big) \leq 1-\frac{1}{n^c}$$

for any QPT adversary $\mathcal{A}$ when n is sufficiently large. The expected value E_x is taken over some distribution $\mathtt{D}(1^n)$.

By the definitions of these variants of OWSGs, it's obvious that strong OWSG is immediately the weak OWSG, and weak OWSG is distributionally OWSG. As for the other direction, the implication from weak OWSG to strong OWSG follows Yao's construction with only minor modification, Namely, assuming $\mathtt{f}$ is weak OWSG which takes x as input, and outputs $|\phi_x\rangle$, it's not hard to prove

$$\mathtt{f}'(x_1,\ldots,x_m) \to \otimes_{i=1}^m|\phi_{x_i}\rangle^{\otimes\mathtt{poly}(n)}$$

is OWSG by a similar strategy as classical case, where $\mathtt{poly}(n)$ is some polynomial decided by $\mathtt{f}$. That result is consistent with its classical counterpart [17].

Theorem 1. *The existence of weak* OWSG *is equivalent to the existence of strong* OWSG*.*

Then to illustrate the implication from the distributionally OWSG to weak OWSG, let us recall the construction of its classical counterpart by Impagliazzo and Luby [26] which is $f'(x) := (f(x), k, h_k, h_k(x))$ for a distributionally one-way function f. Here $h_k : \{0,1\}^n \to \{0,1\}^k$ is a universal hash function. For ease of notation, h_k also denotes the description of that function, and $k \leq n + O(\log n)$ is the output length. Taking inspiration from that construction, let $\mathtt{f}$ be a distributionally OWSG that takes x as input, and outputs $|\phi_x\rangle$, the candidate of distributionally OWSG is

$$\mathtt{f}'(x, h_k, k) \to |\phi_x, k, h_k, h_k(x)\rangle.$$

The original proof strategy by Impagliazzo and Luby [26] is like that, assuming $\mathcal{A}$ breaks the weak one-wayness of $f'(x) = (f(x), k, h_k, h_k(x))$, then almost all of the outputs $f'(x)$ can be inverted. However, it would contradict the distributionally one-wayness if we find some suitable k (note that k denotes the output length of h_k, there are at most polynomial many of k) such that the following conditions hold with high probability: (1) h_k is injective on the preimage space of the challenge value (i.e. $f^{-1}(f(x))$); (2) The size of the image space of h_k (i.e. 2^k) is at most $|f^{-1}(f(x))| \cdot n^C$ for some polynomial n^C. Conditioned on these two events, for a random guessing $r \in \{0,1\}^k$, 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 x' randomly from $f^{-1}(f(x))$ in that case with high probability. 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 issue appears when we adopt the strategy above. That is, the preimage space $\{x \mid \mathtt{f}(x) \to |\phi_x\rangle\}$ of the challenge state $|\phi_x\rangle$ doesn't necessarily contain all "valid" forgeries. For example, 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. $|\langle\phi_{x'}|\phi_x\rangle| > 1-\mathtt{negl}(n)$), such an x' should also be considered since it's obviously a "valid" forgery. However, 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 arbitrary value in $[0, 1]$ (and that problem doesn't bother its classical counterpart because 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 obstacle can be tackled by a potential nature of the quantum state generator which doesn't satisfy the weak one-wayness. We find that, assuming a quantum state generator $\mathtt{f}$ is not weak one-way, then for almost all x, x', 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, we say $\mathtt{f}$ is $(k, p)-$*polarized* on I, if for any $x, x' \in I$, 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* $\mathtt{f}$ *is not weak OWSG, then for any positive polynomial* $\mathtt{poly}(\cdot)$*, there exists a positive polynomial* $t(\cdot)$ *and subspace* I_n *of the domain, such that* $\mathtt{f}$ *is* $(2t(n), 1/\mathtt{poly}(n)) -$ *polarized on* I_n *and* I_n *takes overwhelming part of the domain.*

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

Theorem 2. *The existence of distributionally* OWSG *is equivalent to the existence of weak* OWSG*.*

Combining these two theorems, we hence show the equivalence among these three primitives, which agrees with its classical counterpart.

Constructing OWSGs from Hard Problem in QSZK. Note that it's possible to construct (distributionally) OWF from any average-case hard problem in statistical zero-knowledge (SZK) [41] [3]. Therefore, to instantiate 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) [46], it's sufficient to investigate the average hardness of the QSD problem.

[3] The existence of OWF can further rely on the non-triviality (i.e. average-case hardness) of the computational zero-knowledge (CZK) [42].

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 from these two circuits is either close enough or pretty far, 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, a complete promise problem for SZK, which is given a pair of classical circuits C_0 and C_1, promised that the output distributions of these two circuits are 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 $\mathtt{S}(r) \to (C_0^r, C_1^r)$ the procedure that the sampler $\mathtt{S}$ 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 OWF [4]. Assuming there is a probabilistic polynomial time (PPT) adversary generates preimages of $f(r,b,x)$ randomly, it's nearly impossible to generates 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 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 hard to handle. Therefore, to get around this obstacle, 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 $(\mathtt{S}_0, \mathtt{S}_1)$, it is promised that these two states $\sum_x p_{0,x} |\phi_x^{U_0}\rangle\langle\phi_x^{U_0}|$ and $\sum_x p_{1,x} |\phi_x^{U_1}\rangle\langle\phi_x^{U_1}|$ are either very close, or far enough, where $U_b|0,x\rangle = |\phi_x^{U_b}, x\rangle$ and $\Pr[\mathtt{S}_b(1^n) \to x] = p_{b,x}$. 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.

For ease of notation, we still use (Q_0^r, Q_1^r) to represent the instance of scQSD problem, but in this case $Q_b^r := (U_0^r, \mathtt{S}_b^r)$ denotes the set of unitary circuit with sampler under the random index r, and $U_b^r|0,x\rangle = |\phi_x^{U_b^r}, x\rangle$. Then assuming the semi-classical QSD problem is hard-on-average for a sampler $\mathtt{S}(r) \to (Q_0^r, Q_1^r)$, we ensure the existence of (distributionally) OWSGs by the following construction

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

That is because, assuming there exists an adversary $\mathcal{A}$ breaks the distributionally one-wayness of $\mathtt{f}$, 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 $\mathtt{E}_x |\phi_x^{U_b^r}\rangle\langle\phi_x^{U_b^r}|^{\otimes t}$ as input state (here the expectation of x is taken over the distribution of $\mathtt{S}_b(1^n)$). Because in that case, the trace distance between $\mathtt{E}_x |\phi_x^{U_b^r}\rangle\langle\phi_x^{U_b^r}|$ and $\mathtt{E}_x |\phi_x^{U_{b\oplus 1}^r}\rangle\langle\phi_x^{U_{b\oplus 1}^r}|$

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

is very far, by the definition of the distributionally OWSG, it's nearly impossible for a successful adversary $\mathcal{A}$ to find another case's preimage. On the other hand, when the mixed states by Q_0^r, Q_1^r are close enough, then the trace distance between $\mathtt{E}_x|\phi_x^{U_b^r}\rangle\langle\phi_x^{U_b^r}|^{\otimes t}$ and $\mathtt{E}_x|\phi_x^{U_{b\oplus 1}^r}\rangle\langle\phi_x^{U_{b\oplus 1}^r}|^{\otimes t}$ is negligibly small. Therefore the output of $\mathcal{A}$ should only change slightly when replacing $\mathtt{E}_x|\phi_x^{U_b^r}\rangle\langle\phi_x^{U_b^r}|^{\otimes t}$ by $\mathtt{E}_x|\phi_x^{U_{b\oplus 1}^r}\rangle\langle\phi_x^{U_{b\oplus 1}^r}|^{\otimes t}$. 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.

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 it is also a promise problem of QSZK. Hence we derive a construction of distributionally OWSG from a hard-on-average promise problem of 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 for handling the purification progress when constructing the distributionally OWSG from the standard QSD problem, but as a by-product and another cryptographic application, we can construct the quantum bit commitment with statistical binding (sum-binding) and computational hiding directly 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^r, Q_1^r are close enough or pretty far. That implies if we send one of the mixed states from Q_0^r, Q_1^r 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. The binding property 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 commiter to convince the receiver with opening 0 and 1 as the message simultaneously. Therefore the implication from the average-case hardness of the QSD problem to the quantum commitment is obtained.

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.*

Note that the average-case QSD problem 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 prove the semi-classical QSD problem is probably not contained in QMA relative to some quantum oracles.

To show that, we adopt Aaronson's technique for separating the SZK and QMA [2], the strategy is like that, we construct the quantum oracle $\mathcal{U}$ which can be treated as the quantum version of the permutation testing problem (PTP) oracle. Then we reduce the hardness for deciding $\mathcal{U}$ 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, let $\mathcal{U}_n := (\mathcal{U}_n^{\mathcal{F}_n(1)}, \ldots, \mathcal{U}_n^{\mathcal{F}_n(2^{n+1})})$ for each $n \in \mathbb{N}$, where $\mathcal{U}_n^{\mathcal{F}_n(i)}$ is chosen from the Haar measure over $\mathbb{U}(2^n)$ independently for all $i \in [2^{n+1}]$. Here $\mathcal{F}_n$ 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 (here the factor $2/3$ can change by other constant, we choose it for aesthetic reasons). Each of these two cases occurs with probability $1/2$. 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 S_b is trivially the uniform distribution on $\{0,1\}^n$. It doesn't belong to $\mathsf{QMA}^{\mathcal{U}}$ due to the quantum lower bound of the permutation testing problem. 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* $\mathsf{scQSD}^{\mathcal{U}} \notin \mathsf{QMA}^{\mathcal{U}}$.

Since OWSGs and quantum bit commitment can be both implemented by the average-case hardness of the scQSD problem, we thus achieve these two quantum cryptographic primitives with complexity assumptions probably beyond QMA.

1.2 Related Works

Concurrent Works. Few days before our paper was published online, a related work by Brakerski, Canetti and Qian appeared. They considered to establish cryptographic primitives from complexity assumption as well [11]. More specifically, they showed the efficiently samplable, statistically far but computationally indistinguishable pairs of distributions (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, where EFI pairs have been shown to be equivalent to the quantum commitment by Yan [48,47]. They also constructed EFI pairs from any non-trivial quantum computationally zero-knowledge (QCZK). That seems to be overlaped with (and also stronger than) our construction of quantum commitment because the equivalence between quantum commitment and non-trivial QCZK by [48,11] and the fact that $\mathsf{QSZK} \subseteq \mathsf{QCZK}$ imply naturally a quantum commitment from non-trivial QSZK. However, we believe our construction of quantum commitment still be of interesting because it achieves quantum commitment directly from non-trivial QSZK. Besides, comparing with [11], the 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 whether the EFI pairs can be used to construct the OWSGs.

Besides, we remark another very recent result by Morimae and Yamakawa also discusses about the properties of OWSGs [35]. They give the generalized definition of OWSGs which allows the output state to be a mixed state and provides an additional verification algorithm for checking the validity. They show the equivalence between OWSGs and weak OWSG by the amplification theorem for weakly verifiable puzzles which is applicable to the secretly verifiable case of OWSGs. However, we note that our proofs of the equivalence among these three variants of OWSG can be lifted to suit the mixed state version of OWSG.

Quantum Primitives below MiniQCrypt. The initiated work by Ji, Liu and Song proposed the notions of PRS and pseudorandom unitary (PRU) [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. concurrently gave constructions of statistically binding and computationally hiding quantum commitment from PRSs in their independent works [36,5], which also indicate the feasibility for constructing 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 [36], and Ananth, Qian and Yuen also gave the notion of PRFSs and obtained several applications [5].

Cryptographic Primitives from Non-Triviality of (Q)SZK. By giving a construction of distributionally OWF, Ostrovsky showed that if SZK contains any hard-on-average problem, then OWFs exist [41]. Subsequently, Ostrovsky and Wigderson further proved the existence of a hard-on-average problem in CZK implies the existence of OWFs in infinitely-often case [42]. Ong and Vadhan studied the equivalence between CZK and instance-dependent commitments [45,40]. A recent work by Komargodski and Yogev 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, Kerenidis and Rosgen devised computationally hiding and statistically binding auxiliary-input quantum commitment schemes by the worst-case complexity assumptions such as $\mathsf{QSZK} \not\subseteq \mathsf{QMA}$ [14] and even much weaker assumption $\mathsf{QIP} \not\subseteq \mathsf{QMA}$ (with quantum advice in the commitment scheme).

Oracle Separations. There are lots of works about the oracle separations of (Q)SZK, we only refer to those highly related. Aaronson and Chen defined the oracle $\mathcal{O}$ relative to which $\mathsf{BQP}^{\mathcal{O}} \not\subseteq \mathsf{BPP}^{\mathcal{O}}_{path}$ and $\mathsf{BQP}^{\mathcal{O}} \not\subseteq \mathsf{SZK}^{\mathcal{O}}$ [1,15]. Then Aaronson showed that $\mathsf{SZK}^{\mathcal{O}} \not\subseteq \mathsf{QMA}^{\mathcal{O}}$ by giving a quantum lower bounded for PTP [2]. Chailloux et al. devised computationally hiding and statistically binding auxiliary-input quantum commitment schemes by the worst-case complexity assumptions and also separated the QSZK and QMA by a quantum oracle [14]. Menda and Watrous showed an oracle separation between QSZK and $\mathsf{UP} \cap \mathsf{coUP}$

[34], where 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 [43] and devised an oracle relative to which injective trapdoor functions and one-way permutations exist, while SZK collapses to P [16]. Due to a series of works [42,40,22], 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 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 $\mathsf{QMA}^{\mathcal{O}} = \mathsf{BQP}^{\mathcal{O}}$ while PRS (and even PRU) still exists which gives negative evidence for reducing pqOWF from PRS [31].

2 Preliminaries

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. $[n]$ is the set of integers $\{1, 2 \ldots, n\}$. The mathematical expectation of a random variable X is $\mathrm{E}[X]$. A function $\texttt{negl}(\cdot)$ is negligible if for any $c > 0$, $\texttt{negl}(n) < 1/n^c$ for all sufficiently large n.

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 $U \in \mathbb{U}(N)$, $U^\dagger$ denotes the adjoint of U, and $I_n \in \mathbb{U}(2^n)$ is the identity map. $\mathrm{Tr}(\rho)$ is the trace of ρ, and $\mathrm{Tr}_A(\rho)$ 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 [39].

For two n qubits mixed states (density matrices) ρ_0, ρ_1, we let $\mathrm{TD}(\rho_0, \rho_1)$ and $\mathrm{F}(\rho_0, \rho_1)$ be the trace distance and fidelity respectively, which are defined by $\mathrm{TD}(\rho_0, \rho_1) := \mathrm{Tr}\sqrt{(\rho_0 - \rho_1)^\dagger(\rho_0 - \rho_1)}/2$ and $\mathrm{F}(\rho_0, \rho_1) := \mathrm{Tr}\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$. For pure states $|\phi_0\rangle$, $|\phi_1\rangle$, we denote by $\mathrm{TD}(|\phi_0\rangle, |\phi_1\rangle)$ and $\mathrm{F}(|\phi_0\rangle, |\phi_1\rangle)$ 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 $\mathrm{F}(\cdot)$ between ρ_0 and ρ_1 can be given by*

$$\mathrm{F}(\rho_0, \rho_1) = \max_{|\phi_0\rangle, |\phi_1\rangle} \Big|\langle\phi_0|\phi_1\rangle\Big|. \tag{1}$$

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*

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

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

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

Moreover, we denote by PQ the purification of a general quantum circuit Q which simulates the functionality of Q and satisfies the unitary property simultaneously. The existence of such simulation is justified in [3] by allowing 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 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 QSD problem is defined as follows.

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

Note that the parameters 1/3 and 2/3 are optional, it can be replaced by 2^{-n} and $1 - 2^{-n}$ due to the technique of manipulating the trace distance [46]. Therefore we usually adopt the parameters of the QSD problem as 2^{-n} and $1-2^{-n}$ in the following text. For simplicity, we introduce the following notations

$$\mathsf{QSD}_1 := \{(Q_0, Q_1) \mid \mathrm{TD}(\rho_0, \rho_1) > 1 - 2^{-n}\},$$
$$\mathsf{QSD}_0 := \{(Q_0, Q_1) \mid \mathrm{TD}(\rho_0, \rho_1) < 2^{-n}\}.$$

Then $\mathsf{QSD} := \mathsf{QSD}_1 \cup \mathsf{QSD}_0$.

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* QSD*, it is quantum hard-on-average if there exists an efficient sampler* $\mathtt{S}(1^n)$ *for*

QSD *such that any QPT adversary* $\mathcal{A}$ *can not distinguish an instance generated from* $\mathtt{S}(1^n)$ *with non-negligible advantage, namely it holds that*

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

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

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

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

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

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

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

Moreover, due to the reduction by Watrous [46], it is easy to see that the average-case QSD is also complete for average-case QSZK, which means the construction from the average-case hardness of QSD could be adjusted to suit other hard-on-average languages 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 [36], and define it's variants. To describe the strong (weak) one-way quantum state generator, we firstly give a generalized version of OWSG which we call it $\varepsilon(n)$-OWSG.

Definition 3 **($\varepsilon(n)$-OWSG).** *Let* $\mathtt{f}$ *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 *the ancilla state* [5]*. For any QPT adversary* $\mathcal{A}$*, we consider the following experiment* $\mathtt{Exp}^{owsg}_{\mathtt{f},\mathcal{A}}(n)$:

- *The challenger generates* $x \leftarrow \mathtt{D}(1^n)$ *by some sampleable* $\mathtt{D}(1^n)$*, then runs* $\mathtt{f}(x) \to |\phi_x\rangle \otimes |\eta_x\rangle$ *about* $t(n)$ *times and sends the resulting state* $|\phi_x\rangle^{\otimes t(n)}$ *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 *otherwise* [6].

[5] In this definition, $|\eta_x\rangle$ is the garbage part which is not non-entangled with $|\phi_x\rangle$, the reason for that is explained in [36]. However, the states in Y, Z could be entangled in mixed state version [35] by adding a verification algorithm.

[6] If we consider $\mathtt{f}(x)$ 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 $\mathtt{f}(x)^\dagger$ to $|\phi_{x'}\rangle \otimes |\eta_x\rangle$.

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

$$\Pr_{x \leftarrow \mathtt{D}(1^n)} \left[\mathtt{Exp}^{owsg}_{\mathtt{f},\mathcal{A}}(n) = 1\right] \leq \varepsilon(n) \tag{5}$$

for some function $\varepsilon(\cdot)$*. Sometimes we denote the event as* $\mathtt{Exp}^{owsg}_{\mathcal{A}}(n)$ *for convenience when* $\mathtt{f}$ *is clear from the context.*

When $\varepsilon(\cdot)$ is a negligible function, the definition of $\varepsilon(n)$-OWSG is exactly the OWSG defined in [36], and we call it the *strong one-way quantum state generator* (strong OWSG) sometimes for clarity. When $\varepsilon(n) = 1 - 1/n^c$ for some constant $c > 0$, we call it the *weak one-way quantum state generator* (weak OWSG).

The original notion of strong (weak) OWSG is hard to capture, so here we give an equivalent definition by the trace distance. Let $\rho^{|\phi_x\rangle}_{\mathcal{A},t} = \mathrm{Tr}_N \mathcal{A}(|\phi_x\rangle^{\otimes t})$ be the mixed state after tracing out all the non-output registers by $\mathcal{A}$ with $|\phi_x\rangle^{\otimes t}$ as input. Without loss of generality, we assume $\mathrm{Tr}_N\, \mathcal{A}(|\phi_x\rangle^{\otimes t})$ has the form $\sum p_x |x\rangle\langle x|$ because if not, we can "measure" the output register by performing the CNOT on those x to an additional auxiliary part before tracing out.

In that case, $\mathtt{f}(\rho^{|\phi_x\rangle}_{\mathcal{A},t})$ denotes the unitary process from $\rho^{|\phi_x\rangle}_{\mathcal{A},t} \otimes |0\rangle\langle 0|$ to $\sum p_x |x\rangle\langle x| \otimes |\phi_x, \eta_x\rangle\langle \phi_x, \eta_x|$. Then it holds that

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

On the other hand,

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

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 $\mathrm{Tr}_Z\, \mathtt{f}(\rho^{|\phi_x\rangle}_{\mathcal{A},t})$ is negligible (resp. $1 - 1/n^{c'}$ for some $c' > 0$) that hence derives the equivalent definition of strong (resp. weak) OWSG. We call the strong OWSG the OWSG for convenience when it's clear from the context. Inspired of that, 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* $\mathtt{f}$ *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* $\mathtt{f}$ *is called distributionally one-way quantum state generator (OWSG) on sampleable* $\mathtt{D}(1^n)$, *if for any QPT adversary* $\mathcal{A}$ *in the experiment* $\mathtt{Exp}_{\mathcal{A}}^{owsg}(n)$ *(which is defined in Definition 3) it holds that*

$$\mathrm{TD}\left(\mathop{\mathrm{E}}_{x}|x\rangle\langle x|\otimes|\phi_x\rangle\langle\phi_x|, \mathop{\mathrm{E}}_{x}\rho_{\mathcal{A},t}^{|\phi_x\rangle}\otimes|\phi_x\rangle\langle\phi_x|\right) \geq \frac{1}{n^c}$$

for some constant $c > 0$. *The expectation* E_x *is taken over the distribution* $\mathtt{D}(1^n)$, *and* $\rho_{\mathcal{A},t}^{|\phi_x\rangle} = \mathrm{Tr}_N\mathcal{A}(|\phi_x\rangle^{\otimes t})$ *is the mixed state after tracing out all the non-output registers by* $\mathcal{A}$ *with* $|\phi_x\rangle^{\otimes t}$ *as input.*

Remark 1. Note that the concurrent work by Morimae and Yamakawa generalized OWSGs to the mixed state version [35], our definition of distributionally OWSGs can be also lifted to this general case by just replacing the pure state output in the trace distance by the mixed state Φ_x output by this generator with x as input. Namely, a mixed state generator $\mathtt{f}$ is distributionally OWSGs, if for any QPT adversary $\mathcal{A}$, it holds that $\mathrm{TD}\big(\mathrm{E}_x|x\rangle\langle x|\otimes\Phi_x, \mathrm{E}_x\,\rho_{\mathcal{A},t}^{|\phi_x\rangle}\otimes\Phi_x\big) \geq 1/n^c$.

3 The Equivalence among 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 *is equivalent to the existence of strong* OWSG.

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 with minor modification. Let $\mathtt{f}$ be a weak OWSG on $\mathtt{D}(1^n)$, such that $\mathtt{Exp}_{\mathcal{B}}^{owsg}(n) = 1$ occurs with probability at most $1 - 1/\mathtt{q}(n)$ for some positive polynomial $\mathtt{q}(\cdot)$ and any QPT adversary $\mathcal{B}$. Then for some suitable polynomial $m(n)$ (which is determined by $\mathtt{q}(n)$), the following construction of $\mathtt{f}'$ is strong OWSG:

$$\mathtt{f}'(x_1,\ldots,x_m) = \otimes_{i=1}^m|\phi_{x_i}\rangle_Y^{\otimes n\mathtt{q}(n)} \otimes_{i=1}^m |\eta_{x_i}\rangle_Z^{\otimes n\mathtt{q}(n)} \tag{6}$$

The strategy of proof is very similar to it's classical counterpart [17]. Here we give a sketch to note the different part, and leave the detailed proof in A.1.

Assuming $\mathcal{A}$ breaks the strong one-wayness of $\mathtt{f}'$ with probability $1/\mathtt{p}(n)$, then for a random challenge state $\otimes_{i=1}^m|\phi_{x_i}\rangle^{\otimes n\mathtt{q}(n)}$, the probability that $\mathcal{A}$ outputs $(x_1',\ldots x_m')$ satisfying $\prod_{i=1}^m|\langle\phi_{x_i}|\phi_{x_i'}\rangle|^{2n\mathtt{q}(n)} \geq 1/2m\mathtt{p}(n)$ is noticeble. Therefore, for a challenge state $|\phi_{x^*}\rangle$ of $\mathtt{f}$, we just embed it into $\otimes_{i=1}^m|\phi_{x_i}\rangle^{\otimes n\mathtt{q}(n)}$

for some suitable position $j \in [m]$. Then give this state to $\mathcal{A}$ and repeat it for polynomial many times. We can prove that $\mathcal{A}$ would output x'_j satisfying $|\langle\phi_{x^*}|\phi_{x'_{j_0}}\rangle|^2 \geq (1/2m\mathtt{p}(n))^{1/n\mathtt{q}(n)}$ with high probability. By Chernoff bound, such x'_i can be detected with overwhelming probability by measuring $|\phi_{x^*}\rangle$ with basis $\{|\phi_{x'_j}\rangle\langle\phi_{x'_i}|, I - |\phi_{x'_i}\rangle\langle\phi_{x'_i}|\}$ for polynomial many times.

Remark 2. Note that this result is shown in the pure state version of OWSG, it can be adjusted to fit the mixed state version as well. Assuming the output state of mixed state version of weak OWSG is Φ_x, then $\mathtt{f}'(x_1,\ldots,x_m) = \otimes_{i=1}^m \Phi_{x_i}^{\otimes n\mathtt{q}(n)}$ is a mixed state version of strong OWSG, the proof strategy is almost the same as the pure state one, we just replace the inner product of two states by the fidelity, and consider the verification algorithm instead of measuring the resulting state with basis $\{|\phi_{x'_j}\rangle\langle\phi_{x'_i}|, I - |\phi_{x'_i}\rangle\langle\phi_{x'_i}|\}$.

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

Theorem 7. *The existence of distributionally* OWSG *is equivalent to the existence of weak* OWSG*.*

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

$$\begin{aligned}
&\mathrm{TD}\Big(\mathop{\mathrm{E}}_x |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|, \mathop{\mathrm{E}}_x \rho_{\mathcal{A},t}^{|\phi_x\rangle} \otimes |\phi_x\rangle\langle\phi_x|\Big) \\
&\quad = \mathrm{TD}\Big(\mathop{\mathrm{E}}_x |x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x| \otimes |\phi_x\rangle\langle\phi_x|, \mathop{\mathrm{E}}_x \mathop{\mathrm{Tr}}_Z \mathtt{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}) \otimes |\phi_x\rangle\langle\phi_x|\Big),
\end{aligned}$$

where $\mathtt{f}(|x\rangle\langle x|)$ denotes the unitary process from $|x\rangle\langle x| \otimes |0\rangle\langle 0|$ to $|x\rangle\langle x| \otimes |\phi_x, \eta_x\rangle\langle\phi_x, \eta_x|$. Since $\mathtt{f}$ is weak OWSG such that

$$\mathop{\mathrm{E}}_x\left[\langle\phi_x| \mathop{\mathrm{Tr}}_{X,Z} \mathtt{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle})|\phi_x\rangle\right] = \Pr_x[\mathtt{Exp}_{\mathcal{A}}^{owsg}(n) = 1] \leq 1 - \frac{1}{n^c} \tag{7}$$

for some constant $c > 0$. Without loss of generality, we still assume $\rho_{\mathcal{A},t}^{|\phi_x\rangle}$ has the form $\sum_x p_x |x\rangle\langle x|$. If we denote by $\mathbf{G}$ the collection of x that is "hard-to-find", namely $\mathbf{G} := \{x \mid \langle\phi_x| \mathrm{Tr}_{X,Z}(\mathtt{f}(\rho_{\mathcal{A},t}^{|\phi_x\rangle}))|\phi_x\rangle \leq 1 - 1/2 \cdot n^c\}$. According to (7) we have $\sum_{x\in\mathbf{G}} p_x \geq \frac{1}{2\cdot n^c}$. That hence implies

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

where SWAP is the swap test on the first two parts, and stores the result in the additional qubit $|0\rangle$. That hence justifies the implication from weak OWSGs to distributionally OWSGs [7].

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 $\mathtt{f}(x) \to |\phi_x\rangle \otimes |\eta_x\rangle$ is distributionally OWSG such that for any QPT adversary $\mathcal{A}$, it holds that

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

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

$$\mathtt{f}'(x, h_k, k) \to |\psi_{x,h_k,k}\rangle \otimes |\eta_x\rangle := |\phi_x, h_k(x), h_k, k\rangle \otimes |\eta_x\rangle \tag{8}$$

where $h_k : \{0,1\}^n \to \{0,1\}^k$ is a universal hash function (we assume those keys h_k have the same length), and $k \leq n + O(\log n)$ denotes the output length of h_k.

Before delving into the correctness of this construction, we firstly introduce a notion of *polarization*, we say quantum state generator $\mathtt{f}$ is $(k,p)-$*polarized* on I_n, if for any $x, x' \in I_n$, either $|\langle\phi_{x'}|\phi_x\rangle|^k \geq 1-p(n)$ or $|\langle\phi_{x'}|\phi_x\rangle|^k \leq p(n)$ (alternatively, when considering the mixed state, it is characterized by the fidelity $\mathrm{F}(\Phi_x^{\otimes k}, \Phi_{x'}^{\otimes k})$ between two mixed states $\Phi_x^{\otimes k}, \Phi_{x'}^{\otimes k}$). Then the following lemma shows that the polarization property for any $\mathtt{f}$ which is not weak OWSG.

[7] When considering the mixed state version of OWSG [35], similar result can be achieved by replacing the operator $\mathtt{f}$ and the swap test by the verification algorithm.

Lemma 4. *If* $\mathtt{f}$ *is not weak* OWSG*, and assuming* $\mathcal{A}$ *is the corresponding adversary with* $t(n)$ *copies. Let* $I_n(\delta)$ *be the collection of* x *such that* $\mathcal{A}$ *wins with probability at least* $1-\delta$

$$I_n(\delta) := \left\{ x' \mid \Pr\left[\mathtt{Exp}^{owsg}_{\mathtt{f},\mathcal{A}}(n) = 1 \mid x = x'\right] \geq 1-\delta \right\}.$$

Then for any positive polynomial $\mathtt{p}(\cdot)$*,* $\mathtt{f}$ *is* $(2t(n), 1/\mathtt{p}(n))-$ *polarized on the collection* $I_n(1/16\mathtt{p}(n)^2 t(n)^2)$*.*

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

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

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

That inspired us to consider a family of pairwise disjointed sets $\{\mathbf{N}^{2t}_x(1/\mathtt{p}(n))\}_{x\in X}$ covering all elements in $I_n(1/16\mathtt{p}(n)^2 t(n)^2)$, namely for $x \in I_n(1/16\mathtt{p}(n)^2 t(n)^2)$, the "$2t$-degree neighbor" of x is

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

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

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

Then it holds that

$$\sqrt{1-(1-\frac{1}{\mathtt{p}(n)})^{\frac{1}{t}}} \leq \mathrm{TD}(|\phi_x\rangle, |\phi_{x'}\rangle) \leq 2\sqrt{1-(1-\frac{1}{\mathtt{p}(n)})^{\frac{1}{t}}} < \sqrt{1-(\frac{1}{\mathtt{p}(n)})^{\frac{1}{t}}}$$

which is contradictory to that lemma 4.

Then we get back to the proof of Theorem 7. We show $\mathtt{f}'$ satisfies the weak one-wayness by making a contradiction. Assuming there is an adversary $\mathcal{A}$ breaks the weak one-wayness of $\mathtt{f}'$, that implies

$$\Pr_{x,h_k,k}[\mathtt{Exp}^{owsg}_{\mathtt{f}',\mathcal{A}}(n) = 1] > 1 - 1/\mathtt{poly}(n) \tag{9}$$

for infinitely many $n \in \mathbb{N}$ and arbitrary polynomial $\mathtt{poly}(\cdot)$. Then we construct an adversary $\mathcal{B}$ breaks the distributionally one-wayness of $\mathtt{f}$ 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 following steps from $k = n + C \cdot \log n$ to $k = C \cdot \log n$ (note that k is the output length of the universal hash $h_k : \{0,1\}^n \to \{0,1\}^k$, $C > 1$ is a constant that will be determined later) [8]:
  - $\mathcal{B}$ generates the key h_k of the universal hash function and 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 gets x' as measurement, then checks if $\mathtt{f}^\dagger(x')|\phi_{x^*}\rangle|\eta_{x'}\rangle$ equals to 0 for $n^2 \cdot t$ times [9], if all the $n^2 \cdot t$ 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 case $k-1$ until $k = C \cdot \log n$.

– 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 parts of $\mathcal{B}$ is described in classical setting, but it's equivalent to analyze it as a unitary operation (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 output (mixed) state by $\mathcal{B}$ after tracing out the non-output part.

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

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

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

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

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 k, h_k and h_x are given as classical string, we can omit it and just consider the quanutm part $|\phi_x\rangle$ when using Lemma 4. In that case, let

$$I_n\left(\frac{1}{16\mathtt{p}(n)^2 t(n)^2}\right) := \left\{x' \mid \bigwedge_k \left(\Pr_{h_k}\left[\mathtt{Exp}_{\mathtt{f}',\mathcal{A}}^{owsg}(n) = 1 \mid x = x'\right] \geq 1 - \frac{1}{16\mathtt{p}(n)^2 t(n)^2}\right)\right\}.$$

Note that $I_n(1/16\mathtt{p}(n)^2 t(n)^2)$ is defined a little differently as the standard description in Lemma 4, here we require $\mathcal{A}$ wins with high probability for all k, and

[8] We call the following steps k-th round when the output length in this iteration is k.

[9] Here $\mathtt{f}(x')$ 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 $\{|\phi_{x'}\rangle\langle\phi_{x'}|, I - |\phi_{x'}\rangle\langle\phi_{x'}|\}$.

there is an randomness from h_k. However, since there are at most polynomial many k (k denotes the output length of hash h_k), $I_n(1/16\mathtt{p}(n)^2t(n)^2)$ is also overwhelming to its domain. Hence we can adopt the polarization lemma in that case and show that $\mathtt{f}$ is $(2t, 1/\mathtt{p}(n))$-polarized on $I_n(1/16\mathtt{p}(n)^2t(n)^2)$ for any positive polynomial $\mathtt{p}(\cdot)$. Then according to the discussion before, we can derive a family of disjointed collections $\{\mathbf{N}_x^{2t}(1/\mathtt{p}(n))\}_x$ that covering $I_n(1/16\mathtt{p}(n)^2t(n)^2)$ (note that $I_n(1/16\mathtt{p}(n)^2t(n)^2)$ and $\mathbf{N}_x^{2t}(1/\mathtt{p}(n))$ only contain those x, the classical parts generated by (k, h_k) are ignored here because either $|\langle h_k(x), h_k, k|h'_{k'}(x'), h'_{k'}, k'\rangle| = 0$ or $|\langle h_k x, h_k, k|h'_{k'}x', h'_{k'}, k'\rangle| = 1$, in other words, we can treat the (k, h_k) as the "evaluation key" of $\mathtt{f}'$).

Then we choose a subset of $\{\mathbf{N}_x^{2t}(1/\mathtt{p}(n)) \cap I_n(1/16\mathtt{p}(n)^2t(n)^2)\}_x$, and denote it by $\{\mathbf{G}_{x_1}^{2t}(1/\mathtt{p}(n)), \ldots, \mathbf{G}_{x_l}^{2t}(1/\mathtt{p}(n))\}$, such that

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

for $i = 1, \ldots, l$. Namely, we choose x_i such that $\mathbf{N}_{x_i}^{2t}(1/\mathtt{p}(n)) \cap I_n(1/16\mathtt{p}(n)^2t(n)^2)$ (i.e. $\mathbf{G}_{x_i}^{2t}(1/\mathtt{p}(n))$) is not much smaller than $\mathbf{N}_{x_i}^{2t}(1/\mathtt{p}(n))$. In the following part, we will drop the parameters and just write $\mathbf{G}_{x_i}$, $\mathbf{N}_{x_i}$, and I_n when they are clear from the context. Besides, it's easy to find that $\{x \mid \mathrm{TD}(|\phi_{x_1}\rangle, |\phi_x\rangle) \leq \sqrt{1 - (1/\mathtt{p}(n))^{t^{-1}}/2}\} \ldots \{x \mid \mathrm{TD}(|\phi_{x_l}\rangle, |\phi_x\rangle) \leq \sqrt{1 - (1/\mathtt{p}(n))^{t^{-1}}/2}\}$ are pairwise disjointed.

Since the weak one-wayness of $\mathtt{f}$ is broken with $t(n)$ copies, we can derive that $|I_n(1/16\mathtt{p}(n)^2t(n)^2)| \geq 2^n \cdot (1 - \mathtt{negl}(n))$ for some negligible function $\mathtt{negl}(\cdot)$. Therefore some suitable $\{\mathbf{G}_{x_1}, \ldots, \mathbf{G}_{x_l}\}$ 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 it holds that $|I'_n| > 2^n \cdot (1 - \mathtt{negl}(n))$ for some negligible function $\mathtt{negl}(\cdot)$ (otherwise, since $\mathtt{p}(\cdot)$ is a positive polynomial, it would also be contradictory to the assumption that $\mathtt{f}$ is not weak OWSG).

According to that classification, we can divide the input space into these disjointed collections $\mathbf{G}_{x_1}, \ldots, \mathbf{G}_{x_l}$. By the convexity of the fidelity, we have [10]

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

[10] 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.

Then it's sufficient to consider the lower bound of each $\mathbf{G}_{x_i}$, we then derive that

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

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

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

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

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

Similar, we have

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

Therefore, the inequality (10) becomes

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

That implies it's sufficient to consider the trace distance between $\mathrm{E}_{x\in\mathbf{G}_{x_i}}|x\rangle\langle x|$ and $\mathrm{E}_{x\in\mathbf{G}_{x_i}}\rho_{\mathcal{B},t'}^{|\phi_x\rangle}$. We now estimate the trace distance above 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 probability that $\mathcal{B}$ accepts and outputs those x only with small probability. We divide these into three 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 [11], then for $k\in[n+C\cdot\log n, \log|\mathbf{G}_{x_i}|+C\cdot\log n]$, it holds that

$$p_k\geq(1-\frac{3n^2}{\mathtt{p}(n)})\cdot\left(\frac{|\mathbf{G}_{x_i}|}{2^k}-\frac{|\mathbf{G}_{x_i}|\cdot(|\mathbf{G}_{x_i}|-1)}{2^{2k+1}}\right). \qquad (12)$$

Hence, when $m\geq 2n^{C+1}$, we have

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

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 Claim 2 analyzes the probability for each output in detail when $\mathcal{B}$ accepts. Before that, for ease of notation, let $\mathbf{B}_{x_i}$ denote the collection of "bad" x which are not "highly invertible" but "close" to x_i, namely

$$\mathbf{B}_{x_i}:=\left\{x\mid\mathrm{TD}(|\phi_{x_i}\rangle,|\phi_x\rangle)\leq\sqrt{1-(\frac{1}{\mathtt{p}(n)})^{\frac{1}{t}}/2}\right\}\setminus\mathbf{G}_{x_i}. \qquad (14)$$

By the definition of $\mathbf{G}_i$, we have $|\mathbf{B}_{x_i}|\leq|\mathbf{G}_{x_i}|\cdot\mathtt{p}(n)^{-1}$.

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 four facts hold.

[11] Note that the probabilities that $\mathcal{B}$ accepts are the same in each of these m repetitions of k-th round, so here we drop the number of repetitions, similar reason for $p_{k,x}$.

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 $p_{k,x} < \mathtt{p}(n)^{-n^2}$.
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

$$\frac{(1 - 2n^{-2C} - 3n^2/\mathtt{p}(n))}{2^k} \leq p_{k,x} \leq 1/2^k.$$

3. For any $x \in \mathbf{B}_{x_i}$, it holds that $p_{k,x} \leq 1/2^k$.
4. For any other x, the probability is at most $p_{k,x} < \exp(-n^2/16)$.

The proofs of Claim 1 and Claim 2 may refer to A.3 and A.4.

Then, based on the two claims above, we can show that the output would follow a "nearly uniform" distribution on $\mathbf{G}_{x_i}$

Claim 3. For a given challenge state $|\phi_{x^*}\rangle$, where $x^* \in \mathbf{G}_{x_i}$, p_x denotes the probability that $\mathcal{B}$ accepts with the measurement x, then we have

1. For $x \in \mathbf{G}_{x_i}$, $|p_x - 1/|\mathbf{G}_{x_i}|| < 5n^2/(\mathtt{p}(n) \cdot |\mathbf{G}_{x_i}|)$.
2. For $x \in \mathbf{B}_{x_i}$, it holds that $p_x \leq 2 \cdot |\mathbf{G}_{x_i}|^{-1} + O(\exp(-n))$.
3. For $x \notin \mathbf{B}_{x_i} \cup \mathbf{G}_{x_i}$, we have $p_x \leq \exp(-n)$.

Due to the limitation of space, we leave the proof of Claim 3 in A.5.

Back to the proof of Theorem 7, according to Claim 2 and 3, we have

$$\begin{aligned}
&\mathrm{TD}\left(\mathop{\mathrm{E}}_{x\in\mathbf{G}_{x_i}} |x\rangle\langle x|, \mathop{\mathrm{E}}_{x\in\mathbf{G}_{x_i}} \rho_{\mathcal{A},t}^{|\phi_x\rangle}\right) \\
&\quad = \max_{0\leq P\leq I} \mathrm{Tr}\left[P\left(\mathop{\mathrm{E}}_{x\in\mathbf{G}_{x_i}} |x\rangle\langle x| - \mathop{\mathrm{E}}_{x\in\mathbf{G}_{x_i}} \rho_{\mathcal{A},t}^{|\phi_x\rangle}\right)\right] < \sum_x \left|p_x - \frac{1}{|\mathbf{G}_{x_i}|}\cdot\delta_x\right| \\
&\quad < \sum_{x\in\mathbf{G}_{x_i}} p_x + \sum_{x\notin\mathbf{B}_{x_i}\cup\mathbf{G}_{x_i}} p_x + \sum_{x\in\mathbf{B}_{x_i}} p_x \overset{*}{<} \frac{5n^2}{\mathtt{p}(n)} + \mathtt{negl}(n) + \frac{2}{\mathtt{p}(n)}
\end{aligned}$$

for some negligible function $\mathtt{negl}(\cdot)$, where $\delta_x = 1$ if $x \in \mathbf{G}_{x_i}$, and $\delta_x = 0$ otherwise. Here $(*)$ follows the Claim 3, and $|\mathbf{B}_{x_i}| \leq |\mathbf{G}_i|/\mathtt{p}(n)$.

Therefore, if we let $\mathtt{p}(n) > 36\mathtt{q}(n)^2 \cdot n^2$, we can derive that

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

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

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

which hence indicates that $\mathtt{f}'$ is a weak one-way state generator. □

Remark 3. For the same reason, this proof can also be adjusted to show the implication from the distributionally OWSGs to the weak OWSGs in the mixed state manner [35] by replacing the inner product by the fidelity of two states, and considering the verification algorithm instead of measuring the resulting state with some basis $\{|\phi_{x'}\rangle\langle\phi_{x'}|, I - |\phi_{x'}\rangle\langle\phi_{x'}|\}$.

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 OWSG 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* $(\mathtt{S}_0, \mathtt{S}_1)$ *such that* $U_b|0,x\rangle = |\phi_x^{U_b}, x\rangle_{AB}$ *and* $\Pr[\mathtt{S}_b(1^n) \to x] = p_{b,x}$ *for* $b \in \{0,1\}$. *It is promised that either*

$$\mathrm{TD}\left(\sum_x p_{0,x}|\phi_x^{U_0}\rangle\langle\phi_x^{U_0}|, \sum_x p_{1,x}|\phi_x^{U_1}\rangle\langle\phi_x^{U_1}|\right) > 1 - 2^{-n},$$

or

$$\mathrm{TD}\left(\sum_x p_{0,x}|\phi_x^{U_0}\rangle\langle\phi_x^{U_0}|, \sum_x p_{1,x}|\phi_x^{U_1}\rangle\langle\phi_x^{U_1}|\right) > 2^{-n}.$$

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 $\mathrm{E}_x\, U_b|0,x\rangle\langle 0,x|U_b^\dagger$, 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 $\mathbf{scQSD}_1$ ($\mathbf{scQSD}_0$ resp.) the collection of (Q_0, Q_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 QSD problem, which is characterized by the hardness for any QPT distinguisher to distinguish $(Q_0, Q_1) \in \mathbf{scQSD}_0$ from $(Q_0, Q_1) \in \mathbf{scQSD}_1$ over a instance sampler $\mathtt{S}(1^n) \to (Q_0, Q_1)$. Then we show the implication of distributionally OWSG from the hard-on-average semi-classical QSD problem 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 $((S_0^r, U_0^r), (S_1^r, U_1^r)) = (Q_0^r, Q_1^r) \leftarrow \mathtt{S}(r)$ such that the semi-classical QSD problem is hard-on-average on distribution of $\mathtt{S}(1^n)$ [12], then the following construction

$$\mathtt{f}(r, b, x) := |\psi_{b,x}^{Q_0^r, Q_1^r}\rangle = |Q_0^r, Q_1^r\rangle \otimes |\phi_x^{U_b^r}\rangle \tag{15}$$

is a distributionally OWSG 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 $((S_0^r, U_0^r), (S_1^r, U_1^r)) = (Q_0^r, Q_1^r) \leftarrow \mathtt{S}(r)$. 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 A.6.

Assuming a QPT adversary $\mathcal{A}$ breaks the distributionally one-wayness of $\mathtt{f}$, 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 captured by the trace distance). Then for a given hard instance Q_0^r, Q_1^r, we generate $\mathrm{E}_x\, |\phi_x^{U_b^r}, x\rangle\langle\phi_x^{U_b^r}, x|$, let $\mathrm{E}_x\, |Q_0^r, Q_1^r, \phi_x^{U_b^r}\rangle\langle Q_0^r, Q_1^r, \phi_x^{U_b^r}|$ be the challenge state of $\mathcal{A}$ for a random coin $b \in \{0, 1\}$. Then in the case that $(Q_0^r, Q_1^r) \in \mathbf{scQSD}_0$, the state $\mathrm{E}_x\, |Q_0^r, Q_1^r, \phi_x^{U_0^r}\rangle\langle Q_0^r, Q_1^r, \phi_x^{U_0^r}|$ is very close to $\mathrm{E}_x\, |Q_0^r, Q_1^r, \phi_x^{U_1^r}\rangle\langle Q_0^r, Q_1^r, \phi_x^{U_1^r}|$, 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 $(Q_0^r, Q_1^r) \in \mathbf{scQSD}_1$, 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 Constructing Quantum Bit Commitment Directly 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. *Assuming* QSD *problem is hard-on-average in quantum case, then there exists a statistical binding (sum-binding) and computational hiding quantum commitment.*

The construction of quantum bit commitment: Assuming there exists a efficient sampler $(Q_0^r, Q_1^r) \leftarrow \mathtt{S}(r)$ such that the QSD problem is hard-on-average under distribution of $\mathtt{S}(1^n)$, then the quantum bit commitment scheme is as follows:

[12] Here $r \in \{0, 1\}^{l(n)}$ is the internal randomness of $\mathtt{S}$ which is a polynomial of n, and we denote $l(n)$ by l for short when there is no confusion

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

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

Let $b \leftarrow \{0,1\}$ be the message the commiter intends to commit, it generates

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

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 fix the purification procedure). 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 $(H^{\otimes l} \otimes I_{ABC}) \circ (\mathtt{S}^\dagger \otimes I_{BC}) \circ U_b^\dagger)^{\otimes n}$ 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 give a sketch here and leave the detailed version to A.7.

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 commitments 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 these two commitment states are far from each other, therefore no (computational unbounded) cheating commiter can both open 0 and 1 for one commitment with non-negligible probability which ensures the sum-binding of this construction.

Remark 4. Note that, the hard-core predicate of OWSGs can be realized by the same way as OWFs. Therefore for a one-way state generator $\mathtt{f}$, when there exist some positive polynomial $\mathtt{p}(\cdot)$ such that $|\langle\phi_{x'}|\phi_x\rangle| \leq 1 - 1/\mathtt{p}(n)$ for any $x \neq x'$, we can just send the $\mathtt{p}(n) \cdot n$ 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 show an evidence of the non-triviality for our constructions above. Note that, the existence of pqOWF at least requires $\mathsf{QMA} \neq \mathsf{BQP}$, and by Kretschmer's result [31], there is a quantum oracle relative to which $\mathsf{QMA}^{\mathcal{O}} = \mathsf{BQP}^{\mathcal{O}}$ 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 $\mathsf{scQSD}^{\mathcal{U}} \notin QMA^{\mathcal{U}}$.*

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

The description of $\mathcal{U}$: Let $\mathcal{U} := \{\mathcal{U}_n\}_{n\in\mathbb{N}}$ and $\mathcal{U}_n := (\mathcal{U}_n^{\mathcal{F}_n(1)}, \ldots, \mathcal{U}_n^{\mathcal{F}_n(2^{n+1})})$ for each $n \in \mathbb{N}$, here $\mathcal{U}_n^{\mathcal{F}_n(i)}$ is chosen from the Haar measure over $\mathbb{U}(2^n)$ independently for all $i \in [2^{n+1}]$. In this case, $\mathcal{F}_n$ 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, each case occurs with probability 1/2 respectively. Let $\mathbf{U}_{n,0}$ and $\mathbf{U}_{n,1}$ be the ensembles of thers two types of $\mathcal{U}_n$ respectively.

The construction of the hard instance $(Q_0, Q_1) = ((U_0^{\mathcal{U}}, \mathsf{S}_U^{\mathcal{U}}), (U_1^{\mathcal{U}}, \mathsf{S}_1^{\mathcal{U}}))$ of the semi-classical QSD problem 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 S_b is the uniform distribution on $\{0,1\}^n$. It's easy to see the correctness of this construction. Because when $\mathcal{F}_n$ is a random permutation, we have

$$\begin{aligned}
&\mathop{\mathrm{E}}_{\mathcal{U}}\left[\mathrm{F}\left(\mathop{\mathrm{E}}_{x}\left(\mathcal{U}_n^{\mathcal{F}_n(0\|x)}|0\rangle\langle 0|\big(\mathcal{U}_n^{\mathcal{F}_n(0\|x)}\big)^\dagger\right), \mathop{\mathrm{E}}_{x}\left(\mathcal{U}_n^{\mathcal{F}_n(1\|x)}|0\rangle\langle 0|\big(\mathcal{U}_n^{\mathcal{F}_n(1\|x)}\big)^\dagger\right)\right)\right] \\
&\quad \overset{*}{\leq} \mathop{\mathrm{E}}_{\mathcal{U}} \max_{V} \left|\Big(\sum_x \langle 0|(\mathcal{U}_n^{\mathcal{F}_n(0\|x)})^\dagger \otimes \langle x|\Big)\Big(\sum_x \mathcal{U}_n^{\mathcal{F}_n(1\|x)}|0\rangle \otimes V|x\rangle\Big)\right| / 2^n \overset{**}{\leq} O(1/2^{n/2})
\end{aligned}$$

for any such $\mathcal{F}_n$, where $(*)$ holds due to the Uhlmann's theorem (Lemma 2), and $(**)$ follows the fact that $\mathcal{U}_n^{\mathcal{F}_n(i)}$ is chosen from the Haar measure independently.

In the case that $\mathcal{F}_n$ differs from every permutation on at least $2^{n+2}/3$ coordinates, there is at least $2^{n+2}/9$ disjointed pairs [13]. Let $\mathbf{X} := \{(x_0^1, x_1^1), (x_0^2, x_1^2), \ldots\}$ be the collections of the pairwise disjointed pairs such that $\mathcal{F}_n(0\|x_0^i) = \mathcal{F}_n(1\|x_1^i)$ and $x_b^i \neq x_b^j$ for all $i \neq j$ and $b = 0, 1$ which achieves the maximum cardinality. Since $\mathcal{F}_n$ is chosen randomly (it's equivalent to the distribution of $\mathcal{F}_n \circ p_n^{-1}$ with random permutation p_n), each disjointed pair contained separately in $0\|\cdot$ and $1\|\cdot$ with probability nearly 1/2, one may hence deduce that $|X|$ is smaller than its expected value ($c \cdot 2^n$ for some constant $c > 0$) with negligible probability, which means that

$$\begin{aligned}
&\mathop{\mathrm{E}}_{\mathcal{U}}\left[\mathrm{TD}\left(\mathop{\mathrm{E}}_{x}\left(\mathcal{U}_n^{\mathcal{F}_n(0\|x)}|0\rangle\langle 0|\big(\mathcal{U}_n^{\mathcal{F}_n(0\|x)}\big)^\dagger\right), \mathop{\mathrm{E}}_{x}\left(\mathcal{U}_n^{\mathcal{F}_n(1\|x)}|0\rangle\langle 0|\big(\mathcal{U}_n^{\mathcal{F}_n(1\|x)}\big)^\dagger\right)\right)\right] \\
&\quad \overset{*}{\leq} \sum_{x_0 \notin \mathbf{X}} \max_{P} \mathrm{Tr}\left[P\mathcal{U}_n^{\mathcal{F}_n(0\|x_0)}|0\rangle\langle 0|(\mathcal{U}_n^{\mathcal{F}_n(0\|x_0)})^\dagger\right] \leq 1 - c.
\end{aligned}$$

[13] Here we call $\{(y_0^1, y_1^1), (y_0^2, y_1^2), \ldots\}$ collection of disjointed pairs if $\mathcal{F}_n(y_0^i) = \mathcal{F}_n(y_1^i)$ and $y_b^i \neq y_{b'}^j$ for all $i \neq j \vee b \neq b'$.

occurs with overwhelming probability. It's obvious that $(1-c) < (1-O(1/2^{n/2}))^2$ for all sufficiently large n which meets the requirement for amplifying the gap [46], 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 $\mathtt{V}$ with w qubits witness that decides the $\mathsf{scQSD}^{\mathcal{U}}$ problem, it holds that $q \cdot w = \Omega(2^{n/3})$.*

Proof (of Proposition 1). Let $\mathtt{V}$ be the quantum verifier of scQSD problem relative to $\mathcal{U}$, Note that the choice of $\mathcal{U}_m$ is irrelevant for distinguishing $\mathbf{U}_{n,1}$ from $\mathbf{U}_{n,0}$ when $m \neq n$, therefore

$$\begin{aligned} &\left| \Pr_{\mathcal{U}}[\mathtt{V}^{\mathcal{U}}(1^n) = 1 \mid \mathcal{U}_n \in \mathbf{U}_{n,0}] - \Pr_{\mathcal{U}}[\mathtt{V}^{\mathcal{U}}(1^n) = 1 \mid \mathcal{U}_n \in \mathbf{U}_{n,1}] \right| \\ &\quad = \left| \Pr_{\mathcal{U}_n}[\mathtt{V}^{\mathcal{U}_n}(1^n) = 1 \mid \mathcal{U}_n \in \mathbf{U}_{n,0}] - \Pr_{\mathcal{U}_n}[\mathtt{V}^{\mathcal{U}_n}(1^n) = 1 \mid \mathcal{U}_n \in \mathbf{U}_{n,1}] \right|. \end{aligned} \tag{16}$$

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 quanutm 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 $\mathtt{V}$ with $\bar{\mathcal{U}}_n$, then outputs $\mathtt{V}$'s decision as result.

We then have

$$\Pr[\mathcal{B}^{\mathcal{F}_n}(1^n) = 1 \mid \mathcal{F}_n \text{ is case}(b)] = \Pr[\mathcal{A}_0^{\mathcal{U}_n}(1^n) = 1 \mid \mathcal{U}_n \in \mathbf{U}_{n,b}] \tag{17}$$

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. □

Therefore, by Proposition 1, any verifier $\mathtt{V}$ 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. □

References

1. Scott Aaronson. BQP and the polynomial hierarchy. In Leonard J. Schulman, editor, *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010*, pages 141–150. ACM, 2010.
2. Scott Aaronson. Impossibility of succinct quantum proofs for collision-freeness. *Quantum Inf. Comput.*, 12(1-2):21–28, 2012.

3. Dorit Aharonov, Alexei Y. Kitaev, and Noam Nisan. Quantum circuits with mixed states. In Jeffrey Scott Vitter, editor, *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*, pages 20–30. ACM, 1998.
4. Dorit Aharonov and Amnon Ta-Shma. Adiabatic quantum state generation and statistical zero knowledge. In Lawrence L. Larmore and Michel X. Goemans, editors, *Proceedings of the 35th Annual ACM Symposium on Theory of Computing, June 9-11, 2003, San Diego, CA, USA*, pages 20–29. ACM, 2003.
5. Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part I*, pages 208–236. Springer, 2022.
6. James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I 41*, pages 467–496. Springer, 2021.
7. Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.*, 560:7–11, 2014.
8. Nir Bitansky and Akshay Degwekar. On the complexity of collision resistant hash functions: New and old black-box separations. In *Theory of Cryptography: 17th International Conference, TCC 2019, Nuremberg, Germany, December 1–5, 2019, Proceedings, Part I 17*, pages 422–450. Springer, 2019.
9. Nir Bitansky, Akshay Degwekar, and Vinod Vaikuntanathan. Structure versus hardness through the obfuscation lens. *SIAM J. Comput.*, 50(1):98–144, 2021.
10. Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In *Advances in Cryptology–EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings 32*, pages 592–608. Springer, 2013.
11. Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. In Yael Tauman Kalai, editor, *14th Innovations in Theoretical Computer Science Conference, ITCS 2023, January 10-13, 2023, MIT, Cambridge, Massachusetts, USA*, volume 251 of *LIPIcs*, pages 24:1–24:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023.
12. Zvika Brakerski and Omri Shmueli. (pseudo) random quantum states with binary phase. In *Theory of Cryptography: 17th International Conference, TCC 2019, Nuremberg, Germany, December 1–5, 2019, Proceedings, Part I*, pages 229–250. Springer, 2019.
13. Zvika Brakerski and Omri Shmueli. Scalable pseudorandom quantum states. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II*, volume 12171 of *Lecture Notes in Computer Science*, pages 417–440. Springer, 2020.
14. André Chailloux, Iordanis Kerenidis, and Bill Rosgen. Quantum commitments from complexity assumptions. In *Automata, Languages and Programming: 38th International Colloquium, ICALP 2011, Zurich, Switzerland, July 4-8, 2011, Proceedings, Part I 38*, pages 73–85. Springer, 2011.
15. Lijie Chen. A note on oracle separations for BQP. *CoRR*, abs/1605.00619, 2016.
16. Marc Fischlin. On the impossibility of constructing non-interactive statistically-secret protocols from any trapdoor one-way function. In *Topics in Cryptology—CT-*

RSA 2002: The Cryptographers' Track at the RSA Conference 2002 San Jose, CA, USA, February 18–22, 2002 Proceedings, pages 79–95. Springer, 2002.
17. Oded Goldreich. *Foundations of cryptography.* Cambridge university press, 2009.
18. Oded Goldreich, Shafi Goldwasser, and Silvio Micali. On the cryptographic applications of random functions. In *Advances in Cryptology: Proceedings of CRYPTO 84 4*, pages 276–288. Springer, 1985.
19. Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the Acm*, 33(4):792–807, 1986.
20. Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *J. Comput. Syst. Sci.*, 28(2):270–299, 1984.
21. Alex B Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. In *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*, pages 531–561. Springer, 2021.
22. Iftach Haitner, Jonathan J. Hoch, Omer Reingold, and Gil Segev. 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.
23. Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.
24. Christopher M. Homan and Mayur Thakur. One-way permutations and self-witnessing languages. *J. Comput. Syst. Sci.*, 67(3):608–622, 2003.
25. Russell Impagliazzo. 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*, pages 134–147. IEEE Computer Society, 1995.
26. Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography. In *30th Annual Symposium on Foundations of Computer Science*, pages 230–235. IEEE, 1989.
27. Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 44–61, 1989.
28. Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*, volume 10993 of *Lecture Notes in Computer Science*, pages 126–152. Springer, 2018.
29. Elham Kashefi and Iordanis Kerenidis. Statistical zero knowledge and quantum one-way functions. *Theor. Comput. Sci.*, 378(1):101–116, 2007.
30. Ilan Komargodski and Eylon Yogev. On distributional collision resistant hashing. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 303–327. Springer, 2018.
31. William Kretschmer. Quantum pseudorandomness and classical complexity. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography*, 2021.
32. Michael Luby and Charles Rackoff. How to construct pseudo-random permutations from pseudo-random functions. *Siam Journal on Computing*, 17(2):373–386, 2006.

33. Mohammad Mahmoody, Hemanta K Maji, and Manoj Prabhakaran. On the power of public-key encryption in secure computation. In *Theory of Cryptography: 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings 11*, pages 240–264. Springer, 2014.
34. Sanketh Menda and John Watrous. Oracle separations for quantum statistical zero-knowledge. *CoRR*, abs/1801.08967, 2018.
35. Tomoyuki Morimae and Takashi Yamakawa. One-wayness in quantum cryptography. *IACR Cryptol. ePrint Arch.*, page 1336, 2022.
36. Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In *Advances in Cryptology–CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part I*, pages 269–295. Springer, 2022.
37. Moni Naor. Bit commitment using pseudorandomness. *J. Cryptol.*, 4(2):151–158, 1991.
38. Ashwin Nayak and Peter Shor. Bit-commitment-based quantum coin flipping. *Physical Review A*, 67(1), jan 2003.
39. Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.
40. Shien Jin Ong and Salil Vadhan. An equivalence between zero knowledge and commitments. In *Theory of Cryptography: Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008. Proceedings 5*, pages 482–500. Springer, 2008.
41. Rafail Ostrovsky. One-way functions, hard on average problems, and statistical zero-knowledge proofs. In *Computational Complexity Conference*, pages 133–138. Citeseer, 1991.
42. Rafail Ostrovsky and Avi Wigderson. One-way functions are essential for non-trivial zero-knowledge. In *The 2nd Israel Symposium on Theory and Computing Systems*, pages 3–17. IEEE, 1993.
43. Daniel R Simon. Finding collisions on a one-way street: Can secure hash functions be based on general assumptions? In *Eurocrypt*, volume 98, pages 334–345, 1998.
44. Johan Stad, Russell Impagliazzo, Leonid A Levin, and Michael Luby. A pseudorandom generator from any one-way function. *Siam Journal on Computing*, 28(4):1364–1396, 1999.
45. Salil P. Vadhan. An unconditional study of computational zero knowledge. *SIAM J. Comput.*, 36(4):1160–1214, 2006.
46. John Watrous. Limits on the power of quantum statistical zero-knowledge. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, pages 459–468. IEEE, 2002.
47. Jun Yan. General properties of quantum bit commitments. In *Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part IV*, pages 628–657. Springer, 2023.
48. Jun Yan, Jian Weng, Dongdai Lin, and Yujuan Quan. Quantum bit commitment with application in quantum zero-knowledge proof. In *Algorithms and Computation: 26th International Symposium, ISAAC 2015, Nagoya, Japan, December 9-11, 2015, Proceedings 26*, pages 555–565. Springer, 2015.
49. Mark Zhandry. How to construct quantum random functions. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, pages 679–687. IEEE Computer Society, 2012.
50. Mark Zhandry. A note on quantum-secure prps. *IACR Cryptology ePrint Archive*, 2016:1076, 2016.

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.

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

$$\Pr_{x\leftarrow \mathtt{D}(1^n)}\left[\mathtt{Exp}^{owsg}_{\mathtt{f},\mathcal{B}}(n)=1\right]\leq 1-\frac{1}{\mathtt{q}(n)} \tag{18}$$

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

$$\mathtt{f}'(x_1,\dots,x_m)=\otimes_{i=1}^m|\phi_{x_i}\rangle_Y^{\otimes n\mathtt{q}(n)}\otimes_{i=1}^m|\eta_{x_i}\rangle_Z^{\otimes n\mathtt{q}(n)} \tag{19}$$

is a strong OWSGs on distribution $\mathtt{D}(1^n)^m$. We prove it by making a contradiction. Assuming $\mathcal{A}$ breaks the strong one-wayness of $\mathtt{f}'$ with t copies, namely there is a positive polynomial $\mathtt{p}(\cdot)$ such that

$$\Pr_{(x_1,\dots,x_m)\leftarrow \mathtt{D}(1^n)^m}\left[\mathtt{Exp}^{owsg}_{\mathtt{f}',\mathcal{A}}(n)=1\right]\geq \frac{1}{\mathtt{p}(n)} \tag{20}$$

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

- $\mathcal{B}$ takes as input the state $|\phi_{x^*}\rangle^{\otimes 2n^2\cdot m^2\cdot \mathtt{p}(n)\cdot\mathtt{q}(n)\cdot(t+\mathtt{q}(n))}$, it runs the following steps from $j=1$ to m.
- $\mathcal{B}$ sets $|\phi_{x_j}\rangle=|\phi_{x^*}\rangle$ and generates $|\phi_{x_i}\rangle$ by $x_i\leftarrow \mathtt{D}(1^n)$ for all $i\in[m]/\{j\}$.
- $\mathcal{B}$ invokes $\mathcal{A}$ with input state $|\Phi\rangle^{\otimes t}:=\otimes_{i=1}^m|\phi_{x_i}\rangle^{\otimes n\mathtt{q}(n)\cdot t}$, 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 $2n\cdot m\cdot\mathtt{p}(n)$ times.
- $\mathcal{B}$ checks all the $2nm^2\mathtt{p}(n)$ 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 $n\cdot\mathtt{q}(n)^2$ times for each x_j' and returns the most possible answer (that is, one of those x_j' that gets $|\phi_{x_j'}\rangle$ as measurement with at least $n\cdot\mathtt{q}(n)^2-n\cdot\mathtt{q}(n)/3$ 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

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

where the probability is taken over the randomness of $\mathcal{A}(|\Phi\rangle^{\otimes t})\to(x_1',\dots,x_m')$ and $x_i\leftarrow\mathtt{D}(1^n)$ for $i\in[m]/\{j\}$. Namely, $\mathbf{BadX}_j$ is the collection of "bad"

x_j such that $\mathcal{A}$ outputs those "good" $(x'_1, \ldots, x'_m)$ satisfying $|\langle\phi_{x_i}|\phi_{x'_i}\rangle|^{2n\mathtt{q}(n)} \geq 1/2m\mathtt{p}(n)$ with probability at most $1/2m\mathtt{p}(n)$ when taking $\otimes_{i=1}^m|\phi_{x_i}\rangle^{\otimes n\mathtt{q}(n)\cdot t}$ as input (note that x_j is fixed, and others are chosen randomly from $x_i \leftarrow \mathtt{D}(1^n)$ for $i \in [m]/\{j\}$). Then there is at least one $j \in [m]$ satisfies that

$$\Pr_x[x \in \mathbf{BadX}_j] \leq \frac{1}{2\cdot\mathtt{q}(n)} \tag{21}$$

for those n satisfying (20). Since if not, when let $m = 2\cdot\mathtt{q}(n)\cdot n$, it holds that

$$\begin{aligned}
\frac{1}{\mathtt{p}(n)} &\leq \Pr_{(x_1,\ldots,x_m)\leftarrow\mathtt{D}(1^n)^m}\left[\mathtt{Exp}^{owsg}_{\mathtt{f}',\mathcal{A}}(n)=1\right] \\
&= \Pr_{(x_1,\ldots,x_m)\leftarrow\mathtt{D}(1^n)^m}\left[\mathtt{Exp}^{owsg}_{\mathtt{f}',\mathcal{A}}(n)=1 \wedge_{i=1}^m x_i \notin \mathbf{BadX}_i\right] \\
&\quad + \Pr_{(x_1,\ldots,x_m)\leftarrow\mathtt{D}(1^n)^m}\left[\mathtt{Exp}^{owsg}_{\mathtt{f}',\mathcal{A}}(n)=1 \wedge (\vee_{i=1}^m x_i \in \mathbf{BadX}_i)\right] \\
&\leq \Pr_{(x_1,\ldots,x_m)\leftarrow\mathtt{D}(1^n)^m}\left[\wedge_{i=1}^m x_i \notin \mathbf{BadX}_i\right] \\
&\qquad + m\cdot\max_j \Pr_{(x_1,\ldots,x_m)\leftarrow\mathtt{D}(1^n)^m}\left[\mathtt{Exp}^{owsg}_{\mathtt{f}',\mathcal{A}}(n)=1 \wedge x_j \in \mathbf{BadX}_j\right] \\
&\leq \left(1-\frac{1}{2\cdot\mathtt{q}(n)}\right)^m + m\cdot\max_j \Pr_{(x_1,\ldots,x_m)\leftarrow\mathtt{D}(1^n)^m}\left[\mathtt{Exp}^{owsg}_{\mathtt{f}',\mathcal{A}}(n)=1 \mid x_j \in \mathbf{BadX}_j\right] \\
&\overset{*}{\leq} \left(1-\frac{1}{2\cdot\mathtt{q}(n)}\right)^m + m\cdot\frac{1}{2\cdot m\cdot\mathtt{p}(n)} < \frac{1}{\mathtt{p}(n)}
\end{aligned}$$

which is a contradiction. Here $(*)$ follows the definition of $\mathbf{BadX}_j$. We denote by j_0 the index that $\mathbf{BadX}_{j_0}$ satisfies (21). Since we run all possible j (i.e. from 1 to m), we could get that $j = j_0$ with probability 1.

Conditioned on $x^* \notin \mathbf{BadX}_{j_0}$, and $\mathcal{B}$ chooses $j = j_0$ ($|\phi_{j_0}\rangle = |\phi_{x^*}\rangle$), the probability $\mathcal{A}$ outputs some $(x'_1, \ldots, x'_m)$ satisfying $\prod_{i=1}^m |\langle\phi_{x_i}|\phi_{x'_i}\rangle|^{2n\mathtt{q}(n)} \geq 1/2m\mathtt{p}(n)$ is at least $1/2m\mathtt{p}(n)$. Since $\mathcal{B}$ repeats each round j for $2nm\mathtt{p}(n)$ times, it has output some $(x'_1, \ldots, x'_m)$ satisfying $\prod_{i=1}^m |\langle\phi_{x_i}|\phi_{x'_i}\rangle|^{2n\mathtt{q}(n)} \geq 1/2m\mathtt{p}(n)$ with probability at least $1-(1-1/2m\mathtt{p}(n))^{2nm\mathtt{p}(n)} \geq 1-O(\exp(-n))$.

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

$$\left|\langle\phi_{x^*}|\phi_{x'_{j_0}}\rangle\right|^2 = \left|\langle\phi_{x_{j_0}}|\phi_{x'_{j_0}}\rangle\right|^2 \geq (1/2m\mathtt{p}(n))^{1/n\mathtt{q}(n)} > 1-\frac{1}{4\mathtt{q}(n)}.$$

That implies $\mathcal{B}$ finds some returns such that $|\langle\phi_{x^*}|\phi_{x'_{j_0}}\rangle|^2 > 1-1/4\mathtt{q}(n)$ with probability at least $1-O(\exp(-n))$ when $x^* \notin \mathbf{BadX}_{j_0}$. The remaining problem is how to find it among the polynomial many (i.e. $2nm^2\mathtt{p}(n)$) candidates x'_j. That can be settled by measuring $|\phi_{x^*}\rangle$ with $\{|\phi_{x'_j}\rangle\langle\phi_{x'_j}|, I-|\phi_{x'_j}\rangle\langle\phi_{x'_j}|\}$ polynomial times (i.e. $n\cdot\mathtt{q}(n)^2$) for each output x'_j. To show that, for any output x'_j, we let X'_j be the number that $\mathcal{B}$ measures $|\phi_{x^*}\rangle$ with $\{|\phi_{x'_j}\rangle\langle\phi_{x'_j}|, I-|\phi_{x'_j}\rangle\langle\phi_{x'_j}|\}$ and gets $|\phi_{x'_j}\rangle$ in result among this $n\cdot\mathtt{q}(n)^2$ measurements. Since each measurement is independent, by Chernoff bound, the result is close to its expected value (for some polynomial amount) with probability

$$\begin{aligned}\Pr\left[\left|X'_j - \left|\langle\phi_{x^*}|\phi_{x'_j}\rangle\right|^2 \cdot n \cdot \mathtt{q}(n)^2\right| \leq \left|\langle\phi_{x^*}|\phi_{x'_j}\rangle\right|^2 \cdot n \cdot \mathtt{q}(n)^2 \cdot \delta\right] \\ \geq 1 - 2 \cdot \exp\left(-\delta^2 \cdot \left|\langle\phi_{x^*}|\phi_{x'_j}\rangle\right|^2 \cdot n \cdot \mathtt{q}(n)^2/3\right).\end{aligned} \tag{22}$$

Therefore, in the case that $\left|\langle\phi_{x^*}|\phi_{x'_j}\rangle\right|^2 > 1 - 1/4\mathtt{q}(n)$, X'_j should be at least $n \cdot \mathtt{q}(n)^2 - n \cdot \mathtt{q}(n)/3$ with overwhelming probability, namely

$$\begin{aligned}&\Pr[X'_j > n \cdot \mathtt{q}(n)^2 - n \cdot \mathtt{q}(n)/3] \\ &\quad\geq 1 - 2 \cdot \exp\left(-\left(\frac{1}{12\mathtt{q}(n) - 3}\right)^2 \cdot |\langle\phi_{x^*}|\phi_{x'_j}\rangle|^2 \cdot n \cdot \mathtt{q}(n)^2/3\right) \\ &\quad> 1 - 2 \cdot \exp(-n/432).\end{aligned}$$

On the other hand, in the case that $\left|\langle\phi_{x^*}|\phi_{x'_j}\rangle\right|^2 \leq 1 - 1/2\mathtt{q}(n)$, it holds that

$$\begin{aligned}&\Pr[X'_j \leq n \cdot \mathtt{q}(n)^2 - n \cdot \mathtt{q}(n)/3] \\ &\quad\geq 1 - 2\exp\left(-\left(\frac{n \cdot \mathtt{q}(n)^2 - n \cdot \mathtt{q}(n)/3}{|\langle\phi_{x^*}|\phi_{x'_j}\rangle|^2 \cdot n \cdot \mathtt{q}(n)^2} - 1\right)^2 \cdot |\langle\phi_{x^*}|\phi_{x'_j}\rangle|^2 \cdot n \cdot \mathtt{q}(n)^2/3\right) \\ &\quad\geq 1 - 2\exp\left(-\left(\frac{1}{6\mathtt{q}(n) - 3}\right)^2 \cdot (1 - \frac{1}{2\mathtt{q}(n)}) \cdot n \cdot \mathtt{q}(n)^2/3\right) \\ &\quad> 1 - 2 \cdot \exp(-n/108).\end{aligned}$$

Since there are at most polynomial many outputs, all results would follow that rules with probability $1 - \mathtt{negl}(n)$. Namely, if we denote by $\mathtt{Good}$ the event that all the outputs x'_j by $\mathcal{A}$ meet the following conditions:

- If $\left|\langle\phi_{x^*}|\phi_{x'_j}\rangle\right|^2 \leq 1 - 1/2\mathtt{q}(n)$, then $X'_j < n \cdot \mathtt{q}(n)^2 - n \cdot \mathtt{q}(n)/3$.
- If $\left|\langle\phi_{x^*}|\phi_{x'_j}\rangle\right|^2 \geq 1 - 1/4\mathtt{q}(n)$, then $X'_j > n \cdot \mathtt{q}(n)^2 - n \cdot \mathtt{q}(n)/3$.

Then by the argument above, we can conclude that

$$\begin{aligned}\Pr[\mathtt{Good}] &> (1 - \exp(-C \cdot n))^{2nm^2\mathtt{p}(n)} \\ &> 1 - 2nm^2\mathtt{p}(n) \cdot \exp(-C \cdot n) > 1 - \mathtt{negl}(n).\end{aligned}$$

In that case, $\mathcal{B}$ would find some satisfactory x'_{j_0} only if $|\langle\phi_{x^*}|\phi_{x'_{j_0}}\rangle|^2 > 1 - 1/2\mathtt{q}(n)$, because all these "bad" outputs can be distinguished with overwhelming probability.

Overall, $\mathcal{B}$ would output some x'_{j_0} such that $|\langle\phi_{x^*}|\phi_{x'_{j_0}}\rangle|^2 > 1 - 1/2\mathtt{q}(n)$ with probability at least $1 - \mathtt{negl}(n) - O(\exp(-n))$. Namely

$$\begin{aligned}
&\Pr_{x^*\leftarrow \mathtt{D}(1^n)}\left[\mathtt{Exp}^{owsg}_{\mathtt{f},\mathcal{B}}(n) = 1\right] \\
&\geq \Pr_{x^*\leftarrow \mathtt{D}(1^n)}\left[\mathtt{Exp}^{owsg}_{\mathtt{f},\mathcal{B}}(n) = 1 \wedge x^* \notin \mathbf{BadX}_{j_0}\right] \\
&\geq \Pr_{x^*\leftarrow \mathtt{D}(1^n)}\left[\mathtt{Exp}^{owsg}_{\mathtt{f},\mathcal{B}}(n) = 1 \mid x^* \notin \mathbf{BadX}_{j_0}\right] \cdot \left(1 - \frac{1}{2\mathtt{q}(n)}\right) \\
&\geq \left(1 - \frac{1}{2\mathtt{q}(n)}\right) \cdot \left|\langle\phi_{x^*}|\phi_{x'_{j_0}}\rangle\right|^2 \cdot \Pr_{x^*\leftarrow \mathtt{D}(1^n)}[\mathcal{B} \text{ finds a such } x'_{j_0} \wedge \\
&\qquad \mathcal{A} \text{ has output a satisfactory output } (x'_1, \ldots, x'_m) \mid x^* \notin \mathbf{BadX}_{j_0}] \\
&\geq \left(1 - \frac{1}{2\mathtt{q}(n)}\right)^2 \cdot (1 - \mathtt{negl}(n) - O(\exp(-n))) > 1 - \frac{1}{\mathtt{q}(n)}.
\end{aligned}$$

That is contradictory to the weak one-wayness of $\mathtt{f}$ (namely the inequality (18)) which hence completes the proof of Theorem 6. □

A.2 Proof of Lemma 4

We firstly recall Lemma 4 as follows:

Lemma 4. If $\mathtt{f}$ is not weak OWSG,, and assuming $\mathcal{A}$ is the corresponding adversary with $t(n)$ copies. Let $I_n(\delta)$ be the collection of x such that $\mathcal{A}$ wins with probability at least $1 - \delta$

$$I_n(\delta) := \left\{x' \mid \Pr\left[\mathtt{Exp}^{owsg}_{\mathtt{f},\mathcal{A}}(n) = 1 \mid x = x'\right] \geq 1 - \delta\right\}.$$

Then for any positive polynomial $\mathtt{p}(\cdot)$, $\mathtt{f}$ is $(2t(n), 1/\mathtt{p}(n)) -$ *polarized* on the collection $I_n(1/16\mathtt{p}(n)^2 t(n)^2)$.

Proof. Here we prove the Lemma 4 only in the pure state version of OWSGs for clarity. We remark that the proof of Lemma 4 holds for the mixed state version of OWSGs as well by just replacing the inner product $|\langle\phi_{x'}|\phi_x\rangle|^k$ by the fidelity of $\mathrm{F}(\Phi_x^{\otimes k}, \Phi_{x'}^{\otimes k})$.

To prove that lemma, we let $\mathbf{N}^k_x(\varepsilon)$ be the set of the "k-degree neighbor" of x such that

$$\mathbf{N}^k_x(\varepsilon) := \left\{x' \mid |\langle\phi_{x'}|\phi_x\rangle|^k \geq 1 - \varepsilon\right\}. \tag{23}$$

Then we show that, for any positive polynomial $\mathtt{p}(n)$, the collection $\mathbf{N}^{2t}_x(1/\mathtt{p}(n))$ defines an equivalent classification of $I_n(\delta)$ for some polynomial $1/\delta$ (which will be given later). More specifically, we can prove that, for any pair $x, x' \in I_n(\delta)$, either x_0, x_1 belong to a same neighbor $\mathbf{N}^{2t}_x(1/\mathtt{p}(n))$ or they are a little "far" from each other (i.e. $|\langle\phi_{x_1}|\phi_{x_0}\rangle|^{2t} \leq 1/\mathtt{p}(n)$).

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

$$\frac{1}{\mathtt{p}(n)} < |\langle \phi_{x_0} | \phi_{x_1} \rangle|^{2t} < 1 - \frac{1}{\mathtt{p}(n)}. \tag{24}$$

Since $x_0, x_1 \in I_n(\delta)$, by the definition of $I_n(\delta)$, we have

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

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 the coefficient of those x satisfying $|\langle \phi_{x'} | \phi_x \rangle|^2 \geq 1 - \sqrt{\delta}$ should not be small, namely

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

where $\mathbf{N}_{x_b}^2(\sqrt{\delta})$ is just $\{x' \mid |\langle \phi_{x'} | \phi_x \rangle|^k \geq 1 - \varepsilon\}$ due to its definition.

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

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

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

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

That means $\mathbf{N}_{x_0}^2(\sqrt{\delta}) \cap \mathbf{N}_{x_1}^2(\sqrt{\delta}) = \emptyset$ when $\sqrt{\delta} \leq 1/(4\mathtt{p}(n)t(n))$. Therefore if we denote by $\Pi_{\mathbf{N}_{x_b}^2(\sqrt{\delta})}$ the projection map of the space generated by $\{|x\rangle \mid x \in$

$\mathbf{N}^2_{x_b}(\sqrt{\delta})\}$, the trace distance between this two cases can be estimated as follows

$$\begin{aligned}
&\mathrm{TD}\left(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle}, \rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle}\right) \qquad (26)\\
&= \mathrm{TD}\left(\mathop{\mathit{\Pi}}_{\mathbf{N}^2_{x_0}(\sqrt{\delta})}\left(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle}\right) + g_{x_0}, \mathop{\mathit{\Pi}}_{\mathbf{N}^2_{x_1}(\sqrt{\delta})}\left(\rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle}\right) + g_{x_1}\right)\\
&\overset{*}{\geq} \mathrm{TD}\left(\mathop{\mathit{\Pi}}_{\mathbf{N}^2_{x_0}(\sqrt{\delta})}\left(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle}\right)/\mathrm{Tr}\left(\mathop{\mathit{\Pi}}_{\mathbf{N}^2_{x_0}(\sqrt{\delta})}\left(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle}\right)\right), \mathop{\mathit{\Pi}}_{\mathbf{N}^2_{x_1}(\sqrt{\delta})}\left(\rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle}\right)/\mathrm{Tr}\left(\mathop{\mathit{\Pi}}_{\mathbf{N}^2_{x_1}(\sqrt{\delta})}\left(\rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle}\right)\right)\right)\\
&\quad - \mathrm{TD}\left(\mathop{\mathit{\Pi}}_{\mathbf{N}^2_{x_1}(\sqrt{\delta})}\left(\rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle}\right) + g_{x_1}, \mathop{\mathit{\Pi}}_{\mathbf{N}^2_{x_1}(\sqrt{\delta})}\left(\rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle}\right)/\mathrm{Tr}\left(\mathop{\mathit{\Pi}}_{\mathbf{N}^2_{x_1}(\sqrt{\delta})}\left(\rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle}\right)\right)\right)\\
&\quad - \mathrm{TD}\left(\mathop{\mathit{\Pi}}_{\mathbf{N}^2_{x_0}(\sqrt{\delta})}\left(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle}\right) + g_{x_0}, \mathop{\mathit{\Pi}}_{\mathbf{N}^2_{x_0}(\sqrt{\delta})}\left(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle}\right)/\mathrm{Tr}\left(\mathop{\mathit{\Pi}}_{\mathbf{N}^2_{x_0}(\sqrt{\delta})}\left(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle}\right)\right)\right)\\
&\overset{**}{\geq} 1 - 2\cdot\sqrt{\delta} \geq 1 - \frac{1}{2\cdot \mathtt{p}(n)\cdot t(n)}
\end{aligned}$$

where g_{x_b} is the "garbage" part such that $\rho_{\mathcal{A},t}^{|\phi_{x_b}\rangle} = \mathit{\Pi}_{\mathbf{N}^2_{x_b}(\sqrt{\delta})}(\rho_{\mathcal{A},t}^{|\phi_{x_b}\rangle}) + g_{x_b}$. $(*)$ follows the triangle inequality, and $(*)$ holds due to the convexity of the trace distance and the fact that $\mathrm{Tr}(g_{x_b}) \leq \sqrt{\delta}$ (by the inequality (25)).

However, since we assume $1/\mathtt{p}(n) < |\langle\phi_{x_0}|\phi_{x_1}\rangle|^{2t}$ in (24), we can also derive an upper bound of that trace distance

$$\begin{aligned}
&\mathrm{TD}\left(\rho_{\mathcal{A},t}^{|\phi_{x_0}\rangle}, \rho_{\mathcal{A},t}^{|\phi_{x_1}\rangle}\right) \qquad (27)\\
&= \mathrm{TD}\left(\mathrm{Tr}_Z\mathcal{A}\left(|\phi_{x_0}\rangle^{\otimes t}\otimes|0\rangle\right), \mathrm{Tr}_Z\mathcal{A}\left(|\phi_{x_1}\rangle^{\otimes t}\otimes|0\rangle\right)\right)\\
&\leq \mathrm{TD}\left(\mathcal{A}\left(|\phi_{x_0}\rangle^{\otimes t}\otimes|0\rangle\right), \mathcal{A}\left(|\phi_{x_1}\rangle^{\otimes t}\otimes|0\rangle\right)\right)\\
&= \mathrm{TD}\left(|\phi_{x_0}\rangle^{\otimes t}, |\phi_{x_1}\rangle^{\otimes t}\right)\\
&\leq \sqrt{1 - 1/\mathtt{p}(n)}.
\end{aligned}$$

Combining the inequalities (26) and (27) would lead to a contradiction, which completes the proof of Lemma 4. □

This lemma seems already sufficient for our result. Besides, we note that, for those quantum state generators $\mathtt{f}$ which are not $\varepsilon(n)$-OWSGs, it can be extended to a generalized version of this polarization property. We hope that could be of independent interest and illuminate some important natures of these kinds of quantum primitives.

A.3 Proof of Claim 1

We recall Claim 1 as follows:

Claim 1. For a given challenge state $|\phi_{x^*}\rangle$, where $x^* \in \mathbf{G}_{x_i}$, 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

$$p_k \geq (1 - \frac{3n^2}{\mathtt{p}(n)}) \cdot \left(\frac{|\mathbf{G}_{x_i}|}{2^k} - \frac{|\mathbf{G}_{x_i}| \cdot (|\mathbf{G}_{x_i}| - 1)}{2^{2k+1}}\right). \tag{28}$$

Hence, when $m \geq 2n^{C+1}$, we have

$$\Pr\left[\mathcal{B} \text{ accepts} \wedge k \geq \log|\mathbf{G}_{x_i}| + C \cdot \log n\right] \geq 1 - \exp(-n). \tag{29}$$

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. Before delving into the proof, we firstly recall that $\mathbf{N}_x^k(\varepsilon)$ is the set of the "k-degree neighbor" of x such that

$$\mathbf{N}_x^k(\varepsilon) := \left\{x' \mid |\langle\phi_{x'}|\phi_x\rangle|^k \geq 1 - \varepsilon\right\}, \tag{30}$$

and $\mathbf{G}_x^{2t}(1/\mathtt{p}(n)) := \mathbf{N}_x^{2t}(1/\mathtt{p}(n)) \cap I_n(1/16\mathtt{p}(n)^2 t(n)^2)$ for

$$I_n(\frac{1}{16\mathtt{p}(n)^2 t(n)^2}) := \left\{x' \mid \bigwedge_k \left(\Pr_{h_k}\left[\mathtt{Exp}_{\mathtt{f}',\mathcal{A}}^{owsg}(n) = 1 \mid x = x'\right] \geq 1 - \frac{1}{16\mathtt{p}(n)^2 t(n)^2}\right)\right\},$$

which are simplified as $\mathbf{G}_x$ and $\mathbf{N}_x$.

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 $\mathbf{N}_{x_i}$, namely

$$\begin{aligned} p_k &\geq \Pr_{r_k,h_k}[\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}, r_k, h_k, k\rangle^{\otimes t}) \in \mathbf{N}_{x_i})] \\ &\overset{*}{\geq} \Pr_{r_k,h_k}[\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}, r_k, h_k, k\rangle^{\otimes t}) \in \mathbf{N}_{x_i}) \wedge r_k \in h_k(\mathbf{G}_{x_i}))]. \end{aligned} \tag{31}$$

Here $(*)$ holds because any measurement $x \in \mathbf{N}_{x_i}$ 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. By the Bonferroni's inequality, conditioned on the fact that $h_k : \{0,1\}^n \to \{0,1\}^k$ is a universal hash function, it holds that

$$\begin{aligned} &\Pr_{r_k,h_k}[r_k \in h_k(\mathbf{G}_{x_i}))] \\ &\quad\geq \sum_{x\in\mathbf{N}_{x_i}} \Pr_{r_k,h_k}[r_k = h_k(x)] - \sum_{x,x'\in\mathbf{N}_{x_i}} \Pr_{r_k,h_k}[r_k = h_k(x) = h_k(x')] \\ &\quad\geq \frac{|\mathbf{G}_{x_i}|}{2^k} - \frac{|\mathbf{G}_{x_i}| \cdot (|\mathbf{G}_{x_i}| - 1)}{2^{2k+1}}. \end{aligned} \tag{32}$$

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

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

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

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

Since

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

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 $O(1/\mathtt{p}(n))$ probability. More specifically

$$\Pr_{h_k}\left[\mathcal{A}\left(|\phi_{x^*}, h_k(x), h_k, k\rangle^{\otimes t}\right) \in \mathbf{N}_{x_i}\right] \geq 1 - \frac{5}{4 \cdot \mathtt{p}(n)}. \tag{33}$$

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

$$\begin{aligned}&\Pr_{h_k}\left[\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}, h_k(x), h_k, k\rangle^{\otimes t}) \in \mathbf{N}_{x_i}\right] \\ &\quad\geq \left(1 - \frac{n^2}{\mathtt{p}(n)}\right) \cdot \left(1 - \frac{5}{4 \cdot \mathtt{p}(n)}\right).\end{aligned} \tag{34}$$

Then we get back to estimate the inequality (31) 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 (32) and (34), it holds that

$$\begin{aligned}&\Pr_{r_k,h_k}\left[\mathcal{B} \text{ accepts} \wedge \mathcal{A}\left(|\phi_{x^*}, r_k, h_k, k\rangle^{\otimes t}\right) \in \mathbf{N}_{x_i} \wedge r_k \in h_k(\mathbf{G}_{x_i})\right] \\ &\quad\geq \Pr_{r_k,h_k}\left[\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}, r_k, h_k, k\rangle^{\otimes t}) \in \mathbf{N}_{x_i} \mid r_k \in h_k(\mathbf{G}_{x_i})\right] \\ &\qquad\quad \cdot \Pr_{r_k,h_k}\left[r_k \in h_k(\mathbf{G}_{x_i}))\right] \\ &\quad\geq \left(1 - \frac{n^2}{\mathtt{p}(n)}\right)\left(1 - \frac{5}{4 \cdot \mathtt{p}(n)}\right) \cdot \left(\frac{|\mathbf{G}_{x_i}|}{2^k} - \frac{|\mathbf{G}_{x_i}| \cdot (|\mathbf{G}_{x_i}| - 1)}{2^{2k+1}}\right) \\ &\quad> (1 - \frac{3n^2}{\mathtt{p}(n)}) \cdot \left(\frac{|\mathbf{G}_{x_i}|}{2^k} - \frac{|\mathbf{G}_{x_i}| \cdot (|\mathbf{G}_{x_i}| - 1)}{2^{2k+1}}\right).\end{aligned}$$

That hence finish the first part of this claim. To show the other part, we let $a(n) := 1 - 3n^2/\mathtt{p}(n)$, and g be the integer such that $2^g \leq |\mathbf{G}_{x_i})| < 2^{g+1}$. Then $p_k \geq a(n) \cdot \left(\frac{1}{2^{k-g}} - \frac{1}{2^{2k-2g+1}}\right)$, 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

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

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

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

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 $n^2/\mathtt{p}(n) = o(1)$, then m can be $2 \cdot n^{C+1}$ for all sufficiently large $n \in \mathbb{N}$. That completes the proof of Claim 1. □

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 the following four 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 $p_{k,x} < \mathtt{p}(n)^{-n^2}$.
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

$$\frac{(1 - 2n^{-2C} - 3n^2/\mathtt{p}(n))}{2^k} \leq p_{k,x} \leq 1/2^k.$$

3. For any $x \in \mathbf{B}_{x_i}$, it holds that $p_{k,x} \leq 1/2^k$.
4. For any other x, the probability is at most $p_{k,x} < \exp(-n^2/16)$.

Proof. It's easy to derive the Fact 1, since $\mathtt{f}'$ is "polarized" when it's not weak one-way, Lemma 4 implies that $|\langle \phi_x|\phi_{x^*}\rangle|^{2t} \leq 1/\mathtt{p}(n)$ 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 by $t \cdot n^2$ times of measuring with probability at most $|\langle \phi_x|\phi_{x^*}\rangle|^{2t\cdot n^2} \leq 1/\mathtt{p}(n)^{n^2}$. 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 $\mathcal{A}(|\phi_{x^*}, h_k(x), h_k, k\rangle^{\otimes t})$ outputs $x \in \mathbf{G}_{x_i}$ is at least $1 - 5/(4 \cdot \mathtt{p}(n)) - n^{-2C}$. That is because, by inequality (33), for a random h_k, $\mathcal{A}(|\phi_{x^*}, h_k(x), h_k, k\rangle^{\otimes t})$ outputs $x \in \mathbf{G}_{x_i}$ with probability at least $1 - 5/(4 \cdot \mathtt{p}(n))$, and there are at most $1/n^{2C}$ of h_k is not injective. Hence we have

$$\begin{aligned} p_{k,x} &= \Pr_{r_k,h_k}[\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}, r_k, h_k, k\rangle^{\otimes t}) \to x \wedge r_k = h_k(x)] \qquad (35) \\ &\geq \Pr_{r_k,h_k}[\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}, r_k, h_k, k\rangle^{\otimes t}) \to x \wedge r_k = h_k(x) \wedge h_k \text{ is injective on } \mathbf{G}_{x_i}] \\ &\geq \frac{(1 - n^2/\mathtt{p}(n))(1 - 5/4 \cdot \mathtt{p}(n) - n^{-2C})(1 - n^{-2C})}{2^k} \\ &> \frac{(1 - 2n^{-2C} - 5/(4 \cdot \mathtt{p}(n)) - n^2/\mathtt{p}(n))}{2^k}. \end{aligned}$$

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

$$p_{k,x} \leq \Pr_{r_k,h_k}[r_k = h_k(x)] = 1/2^k \qquad (36)$$

Combining the (36) with (36), we thus have

$$\frac{(1-2n^{-2C}-3n^2/\mathtt{p}(n))}{2^k} \leq p_{k,x} \leq 1/2^k.$$

which completes the proof of the Fact 2.

The Fact 3 also follows directly from (36), namely

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

for any $x \in \mathbf{B}_{x_i}$.

Then we turn to the final part, since $x \notin I_n \cup \mathbf{B}_{x_i}$, that implies

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

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

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

where $(*)$ holds because $1/\mathtt{p}(n) < (1-1/t(n))^{t(n)}$ for all sufficiently large $n \in \mathbb{N}$. That hence completes the proof of Fact 4. That finishes the proof of Claim 2.□

A.5 Proof of Claim 3

We recall Claim 3 as follows:

Claim 3. For a given challenge state $|\phi_{x^*}\rangle$, where $x^* \in \mathbf{G}_{x_i}$, p_x denotes the probability that $\mathcal{B}$ accepts with the measurement x, then we have

1. For $x \in \mathbf{G}_{x_i}$, $|p_x - 1/|\mathbf{G}_{x_i}|| < 5n^2/(\mathtt{p}(n)\cdot|\mathbf{G}_{x_i}|)$.
2. For $x \in \mathbf{B}_{x_i}$, it holds that it holds that $p_x \leq 2\cdot|\mathbf{G}_{x_i}|^{-1} + O(\exp(-n))$.
3. For $x \notin \mathbf{B}_{x_i} \cup \mathbf{G}_{x_i}$, we have $p_x \leq \exp(-n)$.

Proof. Combining the facts in Claim 2, we can get an upper bounded of p_k as follows

$$\begin{aligned} p_k &\leq \sum_x \Pr_{r_k,h_k}[\mathcal{B} \text{ accepts} \wedge \mathcal{A}(|\phi_{x^*}, r_k, h_k, k\rangle^{\otimes t}) \to x] = \sum_x p_{k,x} \qquad (37)\\ &< \mathtt{p}(n)^{-n} \cdot 2^n + |\mathbf{G}_{x_i}| \cdot \mathtt{p}(n)^{-1} \cdot 2^{-k} + |\mathbf{G}_{x_i}| \cdot 2^{-k} + \exp(-n^2/16) \cdot 2^n \\ &< 2^{-2n} + |\mathbf{G}_{x_i}| \cdot (\mathtt{p}(n)^{-1} + 1) \cdot 2^{-k}. \end{aligned}$$

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

$$p_x = \sum_{k=n+C\log n}^{C\log n} \sum_{m'=0}^{m-1} q_{k,m'} p_{k,x}, \qquad (38)$$

where $q_{k,m'} := \prod_{j=n+C\log n}^{k+1}(1-p_j)^m \cdot (1-p_k)^{m'}$ is the probability that $\mathcal{B}$ doesn't accept from $n+C\log n$ to $k+1$ and the first m' repetitions of the k-th round. Then by (37) 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

$$(1 - \frac{3n^2}{\mathtt{p}(n)}) \cdot \left(|\mathbf{G}_{x_i}| - \frac{|\mathbf{G}_{x_i}| \cdot (|\mathbf{G}_{x_i}| - 1)}{2^{k+1}}\right) < \frac{p_k}{p_{k,x}} < \frac{2^{k-2n} + |\mathbf{G}_{x_i}|(\mathtt{p}(n)^{-1} + 1)}{(1 - 2n^{-2C} - 3n^2/\mathtt{p}(n))}$$

Namely, if we let $C > (\deg \mathtt{p}(n))/2$, it holds that

$$\frac{(\mathtt{p}(n) - 4n^2)}{(2 + \mathtt{p}(n)) \cdot |\mathbf{G}_{x_i}|} < \frac{p_{k,x}}{p_k} < \frac{\mathtt{p}(n)}{(\mathtt{p}(n) - 4n^2) \cdot |\mathbf{G}_{x_i}|} \qquad (39)$$

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

Then still by Claim 1, $\mathcal{B}$ would succeed for some $k \geq \log|\mathbf{G}_{x_i}| + C \cdot \log n$ with overwhelming probability, which means

$$\sum_{k=n+C\log n}^{\log|\mathbf{G}_{x_i}|+C\cdot\log n} \sum_{m'=0}^{m-1} q_{k,m'} p_k \geq 1 - O(\exp(-n))$$

and

$$\sum_{k<\log|\mathbf{G}_{x_i}|+C\cdot\log n} \sum_{m'=0}^{m-1} q_{k,m'} p_k \leq O(\exp(-n)).$$

Combining them with (39), we get

$$\sum_{k=n+C\log n}^{\log|\mathbf{G}_{x_i}|+C\cdot\log n} \sum_{m'=0}^{m-1} q_{k,m'} p_k \cdot \frac{(\mathtt{p}(n) - 4n^2)}{(2 + \mathtt{p}(n)) \cdot |\mathbf{G}_{x_i}|} < p_x,$$

and

$$p_x < \sum_{k=n+C\log n}^{\log|\mathbf{G}_{x_i}|+C\cdot\log n} \sum_{m'=0}^{m-1} q_{k,m'} p_k \cdot \frac{\mathtt{p}(n)}{(\mathtt{p}(n)-4n^2)\cdot|\mathbf{G}_{x_i}|} + O(\exp(-n)).$$

That hence implies

$$\frac{(\mathtt{p}(n)-4n^2)}{(2+\mathtt{p}(n))\cdot|\mathbf{G}_{x_i}|} - O(\exp(-n)) < p_x < \frac{\mathtt{p}(n)}{(\mathtt{p}(n)-4n^2)\cdot|\mathbf{G}_{x_i}|} + O(\exp(-n))$$

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

$$\begin{aligned} &|p_x - 1/|\mathbf{G}_{x_i}|| \\ &< \max\{\frac{4n^2}{(\mathtt{p}(n)-4n^2)\cdot|\mathbf{G}_{x_i}|} + O(\exp(-n)), \frac{(4n^2+2)}{(2+\mathtt{p}(n))\cdot|\mathbf{G}_{x_i}|} + O(\exp(-n))\} \\ &< \frac{5n^2}{\mathtt{p}(n)\cdot|\mathbf{G}_{x_i}|}, \end{aligned}$$

when the degree of $\mathtt{p}(n)$ is larger than 2, that completes the proof of Fact 1.

Similarly, for $x \in \mathbf{B}_{x_i}$, we have

$$\frac{p_{k,x}}{p_k} < \frac{\mathtt{p}(n)}{(\mathtt{p}(n)-4n^2)\cdot|\mathbf{G}_{x_i}|}, \tag{40}$$

therefore the Fact 2 follows

$$p_x < \frac{\mathtt{p}(n)}{(\mathtt{p}(n)-4n^2)\cdot|\mathbf{G}_{x_i}|} + O(\exp(-n)) \le 2\cdot|\mathbf{G}_{x_i}|^{-1} + O(\exp(-n)),$$

when the degree of polynomial $\mathtt{p}(n)$ is larger than 2.

In the case $x \notin \mathbf{B}_{x_i} \cup \mathbf{G}_{x_i}$, by Claim 2, we have

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

Therefore

$$p_x < \exp(-n^2/16) < \exp(-n).$$

That completes the proof of that claim. □

A.6 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 $((S_0^r, U_0^r), (S_1^r, U_1^r)) = (Q_0^r, Q_1^r) \leftarrow \mathtt{S}(r)$ such that the semi-classical QSD problem is hard-on-average on distribution of $\mathtt{S}(1^n)$, then the following construction

$$\mathtt{f}(r,b,x) := |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle = |Q_0^r, Q_1^r\rangle \otimes |\phi_x^{U_b^r}\rangle \tag{41}$$

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

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

$$\mathrm{TD}\left(\mathop{\mathrm{E}}_{r,b,x} |r,b,x\rangle\langle r,b,x| \otimes |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r,Q_1^r}| \right. \\ \left. , \mathop{\mathrm{E}}_{r,b,x} \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r,Q_1^r}\rangle} \otimes |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r,Q_1^r}| \right) \leq \mathtt{negl}(n), \tag{42}$$

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. Similarly, we assume it is the state after tracing out all irrelevant part except the input register of $\mathtt{f}$ (which only contains r, b, x).

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

- $\mathcal{B}$ is given $(Q_0^r, Q_1^r) \leftarrow \mathtt{S}(1^n)$ as its input, it firstly generates the state $\mathrm{E}_x |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle^{\otimes t}$ 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 quantum operation. To estimate the success probability of $\mathcal{B}$, we further derive the following relation by inequality (42) and Lemma 3

$$\begin{aligned} \mathtt{negl}(n) \geq \mathrm{TD}&\left(\mathop{\mathrm{E}}_{r,b,x} |r,b,x\rangle\langle r,b,x| \otimes |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r,Q_1^r}| \right. \\ &\left. , \mathop{\mathrm{E}}_{r,b,x} \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r,Q_1^r}\rangle} \otimes |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r,Q_1^r}| \right) \\ = \max_P \mathrm{Tr}&\left[P\left(\mathop{\mathrm{E}}_{r,b,x}\left(|r,b,x\rangle\langle r,b,x| - \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r,Q_1^r}\rangle}\right) \otimes |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r,Q_1^r}|\right)\right] \end{aligned} \tag{43}$$

Then we let P_0 and P_1 be some projections on the space spaned by $Q_0^r, Q_1^r \in \mathsf{scQSD}_0$ and $Q_0^r, Q_1^r \in \mathsf{scQSD}_1$ respectively [14], then by average-case hardness of **scQSD**, we have

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

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

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

$$\mathrm{TD}\left(\mathop{\mathrm{E}}_{r,b,x}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_d} |r,b,x\rangle\langle r,b,x| \otimes |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r,Q_1^r}| \right. \\ \left. , \mathop{\mathrm{E}}_{r,b,x}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_d} \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r,Q_1^r}\rangle} \otimes |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r,Q_1^r}| \right) \leq \mathtt{negl}'(n) \tag{44}$$

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

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

$$\mathrm{TD}(|\psi_{0,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{0,x}^{Q_0^r,Q_1^r}|^{\otimes t+1}, |\psi_{1,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{1,x}^{Q_0^r,Q_1^r}|^{\otimes t+1}) \leq (t+1)/2^{-n} \tag{45}$$

for any $Q_0^r, Q_1^r \in \mathsf{scQSD}_0$, hence when we replace the challenge state $|\psi_{1,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{1,x}^{Q_0^r,Q_1^r}|^{\otimes t}$ by the $|\psi_{0,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{0,x}^{Q_0^r,Q_1^r}|^{\otimes t}$, the output of $\mathcal{A}$ would only change slightly, more specifically, according to (44) and (45), it holds that

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

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

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

for some negligible $\mathtt{negl}_1(\cdot)$.

Therefore, when $\mathcal{A}$ takes $\mathrm{E}_{x,r}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_0} |\psi_{0,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{0,x}^{Q_0^r,Q_1^r}|^{\otimes t}$ as input state, it would output $b^* = 1$ with probability nearly equals to $1/2$. By a similar argument, we can get the same conclusion for the case that $\mathcal{A}$ takes the state $\mathrm{E}_x^{Q_0^r,Q_1^r\in\mathsf{scQSD}_0} |\psi_{1,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{1,x}^{Q_0^r,Q_1^r}|^{\otimes t}$ as input. Therefore we have

$$\Pr_{(Q_0,Q_1)\leftarrow\mathsf{S}(1^n)}[\mathcal{B}(Q_0,Q_1) = 1 \mid (Q_0,Q_1) \in \mathsf{scQSD}_0] \leq \frac{1}{2} + \mathtt{negl}_1(n) \tag{46}$$

On the other hand, when $Q_0^r, Q_1^r \in \mathsf{scQSD}_1$, by the definition of scQSD_1, it holds that

$$\mathrm{TD}\left(\mathop{\mathrm{E}}_x |\psi_{0,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{0,x}^{Q_0^r,Q_1^r}|, \mathop{\mathrm{E}}_x |\psi_{1,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{1,x}^{Q_0^r,Q_1^r}|\right) \geq 1 - 2^{-n/2}$$

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

$$\begin{aligned}&\mathrm{Tr}\left[P_{Q_0^r,Q_1^r}\left(\mathop{\mathrm{E}}_{x}\left(|\phi_x^{U_0^r}\rangle\langle\phi_x^{U_0^r}| - |\phi_x^{U_1^r}\rangle\langle\phi_x^{U_1^r}|\right)\right)\right]\\ &\quad = \mathrm{TD}\left(\mathop{\mathrm{E}}_{x}|\phi_x^{U_0^r}\rangle\langle\phi_x^{U_0^r}|, \mathop{\mathrm{E}}_{x}|\phi_x^{U_1^r}\rangle\langle\phi_x^{U_1^r}|\right) \geq 1 - 2^{-n}.\end{aligned}$$

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

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

After tracing out the registers W_0 (which contains all the registers except the decision bit b), the trace distance can be further estimated as

$$\begin{aligned}&\mathrm{TD}\Bigg(\mathop{\mathrm{E}}_{r,b,x}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_1} |r,b,x\rangle\langle r,b,x| \otimes |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r,Q_1^r}| \\ &\qquad, \mathop{\mathrm{E}}_{r,b,x}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_1} \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r,Q_1^r}\rangle} \otimes |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r,Q_1^r}|\Bigg) \\ &\geq \mathrm{TD}\Bigg(\mathop{\mathrm{Tr}}_{W_0} \mathop{\mathrm{E}}_{r,b,x}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_1} |r,b,x\rangle\langle r,b,x| \otimes |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r,Q_1^r}| \\ &\qquad, \mathop{\mathrm{Tr}}_{W_0} \mathop{\mathrm{E}}_{r,b,x}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_1} \rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r,Q_1^r}\rangle} \otimes |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r,Q_1^r}|\Bigg) \\ &\geq \mathrm{Tr}\left[P'\Big(\mathop{\mathrm{E}}_{r,b,x}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_1}(|b\rangle\langle b| - \mathop{\mathrm{Tr}}_{W_0}\rho_{\mathcal{A},t}^{|\psi_{b,x}^{Q_0^r,Q_1^r}\rangle}) \otimes |\psi_{b,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{b,x}^{Q_0^r,Q_1^r}|\Big)\right] \\ &\geq \frac{1}{2}\cdot\mathrm{Tr}\left[P\Big(\mathop{\mathrm{E}}_{r,x}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_1}(|0\rangle\langle 0| - \mathop{\mathrm{Tr}}_{W_0}\rho_{\mathcal{A},t}^{|\psi_{0,x}^{Q_0^r,Q_1^r}\rangle}) \otimes |\psi_{0,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{0,x}^{Q_0^r,Q_1^r}|\Big)\right] - 2^{-n} \\ &\geq \frac{1}{2}\cdot(1-2^{-n})\cdot\left(1 - \mathop{\mathrm{E}}_{r,x}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_1}\langle 0|\mathop{\mathrm{Tr}}_{W_0}\rho_{\mathcal{A},t}^{|\psi_{0,x}^{Q_0^r,Q_1^r}\rangle}|0\rangle\right).\end{aligned} \tag{47}$$

According to (43) and (47), we have

$$\mathop{\mathrm{E}}_{r,x}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_1}\langle 0|\mathop{\mathrm{Tr}}_{W_0}\rho_{\mathcal{A},t}^{|\psi_{0,x}^{Q_0^r,Q_1^r}\rangle}|0\rangle \geq 1 - \mathtt{negl}_2(n) \tag{48}$$

for some negligible function $\mathtt{negl}_2(\cdot)$.

That implies, when taking $\mathrm{E}_{r,x}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_1}|\psi_{0,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{0,x}^{Q_0^r,Q_1^r}|^{\otimes t}$ as input state, the output decision b^* by $\mathcal{A}$ would equal to the real b with overwhelming probability. By a similar argument, we can get the same conclusion for the case that $\mathcal{A}$ takes $\mathrm{E}_{r,x}^{Q_0^r,Q_1^r\in\mathsf{scQSD}_0}|\psi_{1,x}^{Q_0^r,Q_1^r}\rangle\langle\psi_{1,x}^{Q_0^r,Q_1^r}|$ as input. Therefore we have

$$\Pr_{(Q_0,Q_1)\leftarrow\mathtt{S}(1^n)}[\mathcal{B}(Q_0,Q_1)=1 \mid (Q_0,Q_1)\in\mathsf{scQSD}_1] \geq 1 - \mathtt{negl}_2(n) \tag{49}$$

Combining the inequalities (46) and (49), we have

$$\begin{aligned}&\Pr_{(Q_0,Q_1)\leftarrow \mathtt{S}(1^n)}[\mathcal{B}(Q_0,Q_1)=1 \mid (Q_0,Q_1)\in \mathsf{scQSD}_0] \\ &\quad - \Pr_{(Q_0,Q_1)\leftarrow \mathtt{S}(1^n)}[\mathcal{B}(Q_0,Q_1)=1 \mid (Q_0,Q_1)\in \mathsf{scQSD}_0] \\ &\geq \frac{1}{2} - \mathtt{negl}_3(n)\end{aligned} \tag{50}$$

for some negligible function $\mathtt{negl}_3(\cdot)$. That hence contradicts the average-case hardness of the **scQSD** problem, which justifies our result. □

A.7 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 $(Q_0^r, Q_1^r) \leftarrow \mathtt{S}(r)$ such that the QSD problem is hard-on-average under distribution of $\mathtt{S}(1^n)$, then the quantum bit commitment scheme is as follows:

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

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

  Let $b \leftarrow \{0,1\}$ be the message the commiter intends to commit, it generates

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

  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 fix the purification procedure). 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 $(H^{\otimes l} \otimes I_{ABC}) \circ (\mathtt{S}^{\dagger} \otimes I_{BC}) \circ U_b^{\dagger})^{\otimes n}$ 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 $\mathrm{Tr}_{C,D}|\Psi_0\rangle\langle\Psi_0|^{\otimes n}$ 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 $\mathcal{A}(\rho) \to b$, we denote the event that $\mathcal{A}$ gets a measurement b with ρ as its input. It then holds that

$$\begin{aligned}&\left|\Pr\left[\mathtt{Exp}_{\mathcal{A}}^{hiding}(0)=1\right]-\Pr\left[\mathtt{Exp}_{\mathcal{A}}^{hiding}(1)=1\right]\right|\\&\quad\le \mathrm{TD}\left(\mathcal{A}\left(\mathrm{Tr}_{C,D}|\Psi_0\rangle\langle\Psi_0|^{\otimes n}\right),\mathcal{A}\left(\mathrm{Tr}_{C,D}|\Psi_1\rangle\langle\Psi_1|^{\otimes n}\right)\right)\\&\quad\le\sqrt{1-\mathrm{F}\left(\mathcal{A}\left(\mathrm{Tr}_{C,D}|\Psi_0\rangle\langle\Psi_0|^{\otimes n}\right),\mathcal{A}\left(\mathrm{Tr}_{C,D}|\Psi_1\rangle\langle\Psi_1|^{\otimes n}\right)\right)^2}.\end{aligned}$$

If we denote by $P^{\mathcal{A}}_{b,b'}$ the probability that $\mathcal{A}$ takes $\mathrm{Tr}_{C,D}|\Psi_b\rangle\langle\Psi_b|^{\otimes n}$ as input, and outputs b'. Then it holds that

$$\begin{aligned}&1-\mathrm{F}\left(\mathcal{A}\left(\mathrm{Tr}_{C,D}|\Psi_0\rangle\langle\Psi_0|^{\otimes n}\right),\mathcal{A}\left(\mathrm{Tr}_{C,D}|\Psi_1\rangle\langle\Psi_1|^{\otimes n}\right)\right)\\&\quad\le 1-\left(\sqrt{P^{\mathcal{A}}_{0,0}\cdot P^{\mathcal{A}}_{1,0}}+\sqrt{P^{\mathcal{A}}_{0,1}\cdot P^{\mathcal{A}}_{1,1}}\right)^2\\&\quad=1-P^{\mathcal{A}}_{0,0}+P^{\mathcal{A}}_{0,0}\cdot P^{\mathcal{A}}_{1,1}-P^{\mathcal{A}}_{0,1}+P^{\mathcal{A}}_{0,1}\cdot P^{\mathcal{A}}_{1,0}-2\sqrt{P^{\mathcal{A}}_{0,0}\cdot P^{\mathcal{A}}_{1,0}\cdot P^{\mathcal{A}}_{0,1}\cdot P^{\mathcal{A}}_{1,1}}\\&\quad=\left(\sqrt{P^{\mathcal{A}}_{0,0}\cdot P^{\mathcal{A}}_{1,1}}-\sqrt{P^{\mathcal{A}}_{0,1}\cdot P^{\mathcal{A}}_{1,0}}\right)^2\overset{*}{\le}\left(\sqrt{P^{\mathcal{A}}_{1,1}}-\sqrt{P^{\mathcal{A}}_{0,1}}\right)^2\overset{**}{\le}2\cdot\left|P^{\mathcal{A}}_{1,1}-P^{\mathcal{A}}_{0,1}\right|.\end{aligned}$$

Here $(*)$ and $(**)$ holds because $P^{\mathcal{A}}_{b,b'}\le 1$ and $P^{\mathcal{A}}_{b,b'}=1-P^{\mathcal{A}}_{b,b'\oplus 1}$ for any $b,b'\in\{0,1\}$. Note that if we let ρ^r_b be the (mixed) state produced by the quantum circuit Q^r_b, it holds that

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

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

$$\left|P^{\mathcal{A}}_{1,1}-P^{\mathcal{A}}_{0,1}\right|\ge\frac{1}{n^c}\tag{51}$$

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

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

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

Note that the $\mathtt{Hyb}_0$ and $\mathtt{Hyb}_n$ represent the two cases of in the inequality (51), therefore

$$\begin{aligned}
&\mathop{\mathrm{E}}_{j}\left|\Pr\left[\mathtt{Hyb}_j = 1\right] - \Pr\left[\mathtt{Hyb}_{j+1} = 1\right]\right| \\
&\geq \left|\sum_{j=0}^{n-1}\left(\Pr\left[\mathtt{Hyb}_j = 1\right] - \Pr\left[\mathtt{Hyb}_{j+1} = 1\right]\right)\right|/n \qquad (52)\\
&= \left|P^{\mathcal{A}}_{1,1} - P^{\mathcal{A}}_{0,1}\right| \geq \frac{1}{n^{c+1}}
\end{aligned}$$

Let j_{max} be the index that maximizes $|\Pr[\mathtt{Hyb}_{j_{max}} = 1] - \Pr[\mathtt{Hyb}_{j_{max}+1} = 1]|$, and without loss of generality, we assume $\Pr[\mathtt{Hyb}_{j_{max}+1} = 1] > \Pr[\mathtt{Hyb}_{j_{max}} = 1]$. Based the inequality above, we construct an adversary $\mathcal{B}$ for the QSD as follows:

– $\mathcal{B}$ receives a pair of circuits (Q_0, Q_1) as its input, its task is to determine whether $(Q_0, Q_1) \in \mathsf{QSD}_1$ or not.
– $\mathcal{B}$ chooses $j \leftarrow \{1, \ldots, n\}$ randomly, and generates $r_1, \ldots, r_{j-1}, r_{j+1}, \ldots, r_n$ uniformly at random. Then it invokes $\mathtt{S}(r_i) = (Q_0^{r_i}, Q_1^{r_i})$ for those $i \neq j$, and sets $(Q_0^{r_j}, Q_1^{r_j}) = (Q_0, Q_1)$.
– $\mathcal{B}$ tosses $t \leftarrow \{0, 1\}$ randomly, 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

$$\begin{aligned}
&\left|\Pr\left[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathtt{S}(1^n)\right] - \frac{1}{2}\right| \\
&= \frac{1}{2} \cdot \left|\mathop{\mathrm{E}}_{j}\left(\Pr[\mathtt{Hyb}_j = 0 \mid t = 0] + \Pr[\mathtt{Hyb}_{j+1} = 1 \mid t = 1]\right) - 1\right| \qquad (53)\\
&= \frac{1}{2} \cdot \left|\mathop{\mathrm{E}}_{j}\left(\Pr[\mathtt{Hyb}_j = 1] - \Pr[\mathtt{Hyb}_{j+1} = 1]\right)\right| \geq \frac{1}{n^{c+1}}
\end{aligned}$$

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

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

$$\begin{aligned}
&\Pr\left[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathtt{S}(1^n) \mid (Q_0, Q_1) \in \mathsf{QSD}_0\right] \\
&\quad = \frac{1}{2} \cdot \mathop{\mathrm{E}}_{j} \big(\Pr\left[\mathtt{Hyb}_j = 0 \mid (Q_0, Q_1) \in \mathsf{QSD}_0 \wedge t = 0\right] \\
&\qquad\qquad + \Pr\left[\mathtt{Hyb}_{j+1} = 1 \mid (Q_0, Q_1) \in \mathsf{QSD}_0 \wedge t = 1\right]\big) \\
&\quad \leq \frac{1}{2} \cdot \mathop{\mathrm{E}}_{j} \big(\Pr\left[\mathtt{Hyb}_j = 0 \mid (Q_0, Q_1) \in \mathsf{QSD}_0 \wedge t = 0\right] \\
&\qquad\qquad + \Pr\left[\mathtt{Hyb}_j = 1 \mid (Q_0, Q_1) \in \mathsf{QSD}_0 \wedge t = 0\right] + \mathtt{negl}_1(n)\big) \\
&\quad \leq \frac{1}{2} \cdot (1 + \mathtt{negl}_1(n))
\end{aligned} \tag{54}$$

for some negligible function $\mathtt{negl}_1(\cdot)$. Note that $(Q_0, Q_1) \in \mathsf{QSD}_0$ with probability nearly equals to $1/2$, namely

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

for $b \in \{0, 1\}$. Therefore, we have

$$\begin{aligned}
&\Pr\left[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathtt{S}(1^n) \mid (Q_0, Q_1) \in \mathsf{QSD}_1\right] \cdot \left(\frac{1}{2} + \mathtt{negl}_0(0)\right) \\
&\quad \geq \Pr\left[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathtt{S}(1^n) \mid (Q_0, Q_1) \in \mathsf{QSD}_1\right] \cdot \Pr\left[(Q_0, Q_1) \in \mathsf{QSD}_1\right] \\
&\quad \geq \Pr\left[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathtt{S}(1^n)\right] \\
&\qquad - \left(\frac{1}{2} + \mathtt{negl}_0(n)\right) \cdot \Pr\left[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathtt{S}(1^n) \mid (Q_0, Q_1) \in \mathsf{QSD}_0\right] \\
&\quad \overset{*}{\geq} \Pr\left[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathtt{S}(1^n)\right] - \frac{1}{2} \cdot (1 + \mathtt{negl}_1(n)) \cdot \left(\frac{1}{2} + \mathtt{negl}_0(n)\right) \\
&\quad \overset{**}{\geq} \frac{1}{4} + \frac{1}{n^{c+1}} - \mathtt{negl}_2(n)
\end{aligned}$$

for infinitely many n, where $(*)$ comes from the inequality (54), and $(**)$ holds because we assume the case $\Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathtt{S}(1^n)] \geq 1/2 + 1/n^{c+1}$ of the inequality (53)[15]. That inequality indicates there is a negligible function $\mathtt{negl}(\cdot)$ such that

$$\begin{aligned}
&\Pr\left[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathtt{S}(1^n) \mid (Q_0, Q_1) \in \mathsf{QSD}_1\right] \\
&\quad \geq \frac{1}{2} + \frac{2}{n^{c+1}} - \mathtt{negl}(n)
\end{aligned} \tag{55}$$

[15] In the other case that $\Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathtt{S}(1^n)] \leq 1/2 - 1/n^{c+1}$, we can estimate the lower bound of that probability in the inequality (53), which is $1/2 - \mathtt{negl}_1(n)$, and the upper bound of $\Pr[\mathcal{B}(Q_0, Q_1) = 1 : (Q_0, Q_1) \leftarrow \mathtt{S}(1^n) \mid (Q_0, Q_1) \in \mathsf{QSD}_1]$ is $1/2 - 2/n^{c+1} + \mathtt{negl}(n)$ accordingly.

for infinitely many n.

Therefore, combining the inequality (54) with (55), we thus have

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

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

Then we discuss the sum-binding property, we denote by p_b the probability that the receiver accepts with message b. Let $\mathrm{Tr}_{C,D,E}|\Psi\rangle\langle\Psi|$ be the commitment sent by a cheating commiter, where $|\Psi\rangle\langle\Psi|$ is the whole "fake" state, and E stores the auxiliary qubits of the cheating commiter. Then the cheating commiter invokes the operator U^b_{CDE} when it intends to open that with b. Since the monotonicity of the fidelity under trace-preserving CP maps, it holds that

$$\begin{aligned}p_0+p_1&=\sum_b\langle\Psi_b|^{\otimes n}\operatorname*{Tr}_E\left[I\otimes U^b_{CDE}|\Psi\rangle\langle\Psi|I\otimes\left(U^b_{CDE}\right)^\dagger\right]|\Psi_b\rangle^{\otimes n} \qquad (56)\\&=\sum_b \mathrm{F}\left(|\Psi_b\rangle\langle\Psi_b|^{\otimes n},\operatorname*{Tr}_E\left[I\otimes U^b_{CDE}|\Psi\rangle\langle\Psi|I\otimes\left(U^b_{CDE}\right)^\dagger\right]\right)^2\\&\leq\sum_b \mathrm{F}\left(\operatorname*{Tr}_{C,D}|\Psi_b\rangle\langle\Psi_b|^{\otimes n},\operatorname*{Tr}_{C,D,E}\left[I\otimes U^b_{CDE}|\Psi\rangle\langle\Psi|I\otimes\left(U^b_{CDE}\right)^\dagger\right]\right)^2\\&\leq\sum_b \mathrm{F}\left(\operatorname*{Tr}_{C,D}|\Psi_b\rangle\langle\Psi_b|^{\otimes n},\operatorname*{Tr}_{C,D,E}|\Psi\rangle\langle\Psi|\right)^2\\&\overset{*}{\leq}1+\mathrm{F}\left(\operatorname*{Tr}_{C,D}|\Psi_0\rangle\langle\Psi_0|^{\otimes n},\operatorname*{Tr}_{C,D}|\Psi_1\rangle\langle\Psi_1|^{\otimes n}\right)\\&\leq 1+\left(1-\mathrm{TD}\left(\operatorname*{E}_{r_1,\ldots,r_n}\bigotimes_{i=1}^n|Q_0^{r_i},Q_1^{r_i}\rangle\langle Q_0^{r_i},Q_1^{r_i}|\otimes\rho_0^{r_i}\right.\right.\\&\qquad\qquad\left.\left.,\operatorname*{E}_{r_1,\ldots,r_n}\bigotimes_{i=1}^n|Q_0^{r_i},Q_1^{r_i}\rangle\langle Q_0^{r_i},Q_1^{r_i}|\otimes\rho_1^{r_i}\right)^2\right)^{\frac{1}{2}},\end{aligned}$$

where $(*)$ holds because $\mathrm{F}(\eta_0,\eta_1)^2+\mathrm{F}(\eta_0,\eta_2)^2\leq 1+\mathrm{F}(\eta_1,\eta_2)$ for any state η_0,η_1,η_2 (refer to [38,36]).

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

$$\begin{aligned}\mathrm{TD}&\left(\mathop{\mathrm{E}}_{r_1,\ldots,r_n}\bigotimes_{i=1}^{n}|Q_0^{r_i},Q_1^{r_i}\rangle\langle Q_0^{r_i},Q_1^{r_i}|\otimes\rho_0^{r_i},\mathop{\mathrm{E}}_{r_1,\ldots,r_n}\bigotimes_{i=1}^{n}|Q_0^{r_i},Q_1^{r_i}\rangle\langle Q_0^{r_i},Q_1^{r_i}|\otimes\rho_1^{r_i}\right)\\&\geq\mathrm{Tr}\left[P\mathop{\mathrm{E}}_{r_1,\ldots,r_n}\bigotimes_{i=1}^{n}|Q_0^{r_i},Q_1^{r_i}\rangle\langle Q_0^{r_i},Q_1^{r_i}|\otimes\left(\bigotimes_{i=1}^{n}\rho_0^{r_i}-\bigotimes_{i=1}^{n}\rho_1^{r_i}\right)\right]\end{aligned}$$

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

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

where $P_{r_1,\ldots,r_n}$ 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

$$\mathrm{TD}\left(\bigotimes_{i=1}^{n}\rho_0^{r_i},\bigotimes_{i=1}^{n}\rho_1^{r_i}\right)=P_{r_1,\ldots,r_n}\left(\bigotimes_{i=1}^{n}\rho_0^{r_i}-\bigotimes_{i=1}^{n}\rho_1^{r_i}\right).$$

In the case that there exists i satisfying $(Q_0^{r_i},Q_1^{r_i})\in\mathsf{QSD}_1$, we have

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

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

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

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

$$\begin{aligned}\mathrm{Tr}&\left[P\left(\mathop{\mathrm{E}}_{r_1,\ldots,r_n}\bigotimes_{i=1}^{n}|Q_0^{r_i},Q_1^{r_i}\rangle\langle Q_0^{r_i},Q_1^{r_i}|\otimes\left(\bigotimes_{i=1}^{n}\rho_0^{r_i}-\bigotimes_{i=1}^{n}\rho_1^{r_i}\right)\right)\right] &(57)\\&\geq\mathrm{Tr}\left[\sum_{r_1,\ldots,r_n}^{\exists\, i:Q_0^{r_i},Q_1^{r_i}\in\mathsf{QSD}_1}\bigotimes_{i=1}^{n}|Q_0^{r_i},Q_1^{r_i}\rangle\langle Q_0^{r_i},Q_1^{r_i}|\otimes P_{r_1,\ldots,r_n}\left(\bigotimes_{i=1}^{n}\rho_0^{r_i}-\bigotimes_{i=1}^{n}\rho_1^{r_i}\right)/2^l\right]\\&\geq\left(1-\left(\frac{2}{3}\right)^n\right)\cdot\left(1-2^{-n}\right).\end{aligned}$$

Combining the inequality (57) with (56), we thus have

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

for some negligible $\mathtt{negl}(\cdot)$, that hence completes the proof of the sum-binding property. □