Cryptography in the Common Haar State Model: Feasibility Results and Separations*

Prabhanjan Ananth† UCSB
Aditya Gulati‡ UCSB
Yao-Ting Lin§ UCSB

Abstract

Common random string model is a popular model in classical cryptography. We study a quantum analogue of this model called the common Haar state (CHS) model. In this model, every party participating in the cryptographic system receives many copies of one or more i.i.d Haar random states.

We study feasibility and limitations of cryptographic primitives in this model and its variants:

- We present a construction of pseudorandom function-like states with security against computationally unbounded adversaries, as long as the adversaries only receive (a priori) bounded number of copies. By suitably instantiating the CHS model, we obtain a new approach to construct pseudorandom function-like states in the plain model.
- We present separations between pseudorandom function-like states (with super-logarithmic length) and quantum cryptographic primitives, such as interactive key agreement and bit commitment, with classical communication. To show these separations, we prove new results on the indistinguishability of identical versus independent Haar states against LOCC (local operations, classical communication) adversaries.

*This subsumes [AGL24].

†prabhanjan@cs.ucsb.edu
‡adityagulati@ucsb.edu
§yao-ting_lin@ucsb.edu

Contents

1 Introduction **3**
- 1.1 Our Results . . . 3
  - 1.1.1 Feasibility Results . . . 3
  - 1.1.2 Black-Box Separations . . . 5

2 Technical Overview **6**
- 2.1 Pseudorandomness in the CHS Model . . . 6
- 2.2 Quantum Bit Commitments . . . 9
- 2.3 Black-Box Separations . . . 10

3 Preliminaries **13**
- 3.1 Notation . . . 13
- 3.2 Common Haar State Model . . . 14
  - 3.2.1 Pseudorandom State (PRS) Generators in the CHS model . . . 14
  - 3.2.2 Pseudorandom Function-Like State (PRFS) Generators in the CHS model . . . 15
  - 3.2.3 Quantum Commitments in the CHS model . . . 16
- 3.3 Symmetric Subspaces, Type States, and Haar States . . . 16
- 3.4 Quantum Black-Box Reductions . . . 17

4 Warmup: Statistical Stretch PRS Generators in the CHS model **17**
- 4.1 Useful Lemmas . . . 18
- 4.2 Construction . . . 20
- 4.3 Optimality of Our PRSG Construction . . . 22

5 Statistical Stretch PRFS Generators in the CHS model **23**
- 5.1 Useful Lemmas . . . 24
- 5.2 Construction . . . 25

6 Quantum Commitments in the CHS model **29**
- 6.1 Construction . . . 29
- 6.2 Proving Hiding and Binding . . . 30

7 LOCC Indistinguishability **31**
- 7.1 Definitions . . . 31
- 7.2 LOCC Haar Indistinguishability . . . 32
- 7.3 An Optimal LOCC Haar distinguisher . . . 36

8 Impossibilities of QCCC Primitives in the CHS model **36**

9 Quantum Black-Box Separation in the QCCC Model **40**
- 9.1 The Separating Oracle . . . 40
- 9.2 Separating QCCC Key Agreements from $(\lambda, \omega(\log(\lambda)))$-PRSGs . . . 40
- 9.3 Separating QCCC Interactive Commitments from $(\lambda, \omega(\log(\lambda)))$-PRSGs . . . 45
- 9.4 Extending the Separation Results . . . 53

A Related Work **58**
- A.1 Quantum Pseudorandomness: State of the Art . . . 58
- A.2 Comparison with [CCS24] and [AGL24] . . . 59

B Alternative Proof of Lemma 4.8 **59**

1 Introduction

In classical cryptography, the common random string and the common reference string models were primarily introduced to tackle cryptographic tasks that were impossible to achieve in the plain model. In the common reference string model, there is a trusted setup who produces a string that every party has access to. In the common random string model, the common string available to all the parties is sampled uniformly at random. Due to the lack of structure required from the common random string model, it is in general the more desirable model of the two. There have been many constructions proposed over the years in these two models, including non-interactive zero-knowledge [BFM19], secure computation with universal composition [CF01; CLOS02] and two-round secure computation [GS22; BL18].

It is a worthy pursuit to study similar models for quantum cryptographic protocols. In the quantum world, there is an option to define models that are intrinsically quantum in nature. For instance, we could define a model wherein a trusted setup produces a quantum state and every party participating in the cryptographic system receives one or more copies of this quantum state. Indeed, two works by Morimae, Nehoran and Yamakawa [MNY23] and Qian [Qia23] consider this model, termed as the *common reference quantum state model* (CRQS). They proposed a construction of unconditionally secure commitments in this model. Quantum commitments is a foundational notion in quantum cryptography. In recent years, quantum commitments have been extensively studied [AQY22; MY21; AGQY22; MY23; BCQ23; Bra23] due to its implication to secure computation [BCKM21; GLSV21]. The fact that information-theoretically secure commitments are impossible in the plain model [LC97; May97; CLM23] renders the contributions of [MNY23; Qia23] particularly interesting.

Common Haar State Model. While CRQS is a quantum analogue of the common reference string model, in a similar vein, we can ask if there is a quantum analogue of the common random string model. We consider a novel model called the *common Haar state model* (CHS). In this model, every party in the system (including the adversary) receives many copies of many i.i.d Haar states. We believe that the CHS model is more pragmatic than the CRQS model owing to the fact that we do not require any structure from the common public state. This raises the possibility of avoiding a trusted setup altogether and instead we could rely upon naturally occuring physical processes to obtain the Haar states. This model was also recently introduced in an independent and concurrent recent work[1] by Chen, Coladangelo and Sattath [CCS24] (henceforth, referred to as CCS).

There are three reasons to study this model. Firstly, this model allows us to bypass impossibility results in the plain model. For instance, as we will see later, primitives that require computational assumptions in the plain model, can instead be designed with information-theoretic security in the CHS model. Second, perhaps a less intuitive reason, is that the constructions proposed in this model can, in some cases, be adopted to obtain constructions in the plain model by instantiating the Haar states either using state designs or pseudorandom state generators (PRSGs) [JLS18]. This leads to a modular approach of designing cryptographic primitives from PRS: first design the primitive in the CHS model and then instantiate the common Haar state using PRS. Finally, this model can be leveraged to demonstrate separations between different quantum cryptographic primitives.

1.1 Our Results

We explore both feasibility results and black-box separations in the CHS model.

1.1.1 Feasibility Results

Pseudorandom Function-Like States with Statistical Security. We study the possibility of designing pseudorandom function-like state generators (PRFSGs), introduced by Ananth, Qian and Yuen [AQY22], with statistical security in the CHS model. Roughly speaking, a PRFSG is an efficient keyed quantum circuit

[1] We refer the reader to Appendix A.2 for a comparison with CCS.

that can be used to produce many pseudorandom states. We refer the reader to Appendix A.1 for a detailed discussion on the different notions of pseudorandomness in the quantum world.

We are interested in designing (λ, m, n, t)-PRFSGs in the setting when $n \geq \lambda$ and $m = \Omega(\log(\lambda))$, where λ is the key length, m is the input length, n is the output length (and also the number of the qubits in the common Haar state) and t is the maximum number of queries that can be requested by the adversary. However, in the CHS model, we can in fact achieve statistical security.

We show the following.

Theorem 1.1 (Informal)**.** *There is a statistically secure (λ, m, n, ℓ)-PRFSG in the CHS model, for $m = \lambda^c$, $n \geq \lambda$ and $\ell = O\left(\frac{\lambda^{1-c}}{\log(\lambda)^{1+\varepsilon}}\right)$, for any constant $\varepsilon > 0$ and for all $c \in [0, 1)$.*

CCS is the only other work that has studied pseudorandomness in the CHS model. There are a few advantages of our result over CCS:

- Our theorem subsumes and generalizes the result of CCS who showed (λ, n, t)-PRSGs exists in their model, where the output length is larger than the key length, i.e., $n > \lambda$ and moreover, when $t = 1$ with t being the number of copies of the PRS state given to the adversary.
- Our construction, when restricted to the case of PRSGs, is slightly simpler than CCS: in CCS, on a subset of qubits of the Haar state, a random Pauli operator is applied whereas in our case a random Pauli Z operator is applied. Our construction of PRFSG uses the seminal Goldreich-Goldwasser-Micali approach [GGM86] to go from one-query security to many-query security.
- They propose novel sophisticated tools in their analysis whereas our analysis is arguably more elementary using well known facts about symmetric subspaces.
- Finally, we can achieve arbitrary stretch whereas it is unclear whether this is also achieved by CCS.

As a side contribution, the proof of our PRSG construction also simplifies the proof of the quantum public-key construction of Coladangelo [Col23]; this is due to the fact the core lemma proven in [Col23] is implied by the above theorem.

Interestingly, the above theorem has implications for computationally secure pseudorandomness in the plain model. Specifically, we obtain the following corollary by instantiating the CHS model using stretch PRSGs:

Corollary 1.2. Assuming (λ, n, ℓ)-PRSGs, there exists (λ', m, n, t)-PRFSGs, where $n > \lambda' > \lambda$, $m = \lambda^c$ and $\ell = O\left(\frac{\lambda^{1-c}}{\log(\lambda)^{1+\varepsilon}}\right)$, for any constant $\varepsilon > 0$ and $c \in [0, 1)$.

Prior to our work, stretch PRFSGs for super-logarithmic input length, even in the bounded query setting, was only known from one-way functions [AQY22]. This complements the work of [AQY22] who showed a construction of PRFSGs for logarithmic input length from PRSGs.

Interestingly, the state generators in both works (CCS and ours) only consume one copy of a single Haar state. In this special case, it is interesting to understand whether we can extend our result to the setting when the adversary receives $\frac{\lambda}{\log(\lambda)}$ copies or more. We show this is not possible.

Theorem 1.3 (Informal)**.** *There does not exist a secure (λ, m, n, ℓ)-PRFSG, for any $m \geq 1$, in the CHS model, where $n = \omega(\log(\lambda))$ and $\ell = \Omega\left(\frac{\lambda}{\log(\lambda)}\right)$.*

CCS also proved a lower bound where they showed that unbounded copy pseudorandom states do not exist. Their negative result is stronger in the sense that they rule out PRSGs who use up many copies of the Haar states from the CHRS and thus, their work gives a clean separation between 1-copy stretch PRS and unbounded copy PRS which was not known before. On the other hand, for the special case when the PRFSG takes only one copy of the Haar state, we believe our result yields better parameters.

Commitments. In addition to pseudorandomness, we also study the possibility of constructing other cryptographic primitives in the CHS model. We show the following:

Theorem 1.4 (Informal)**.** *There is an unconditionally secure bit commitment scheme in the CHS model.*

Both our construction and the commitments scheme proposed by CCS are different although they share strong similarities.

1.1.2 Black-Box Separations

LOCC Indistinguishability. We separate pseudorandom function-like states and quantum cryptographic primitives with classical communication using a variant of the CHS model. At the heart of our separations is a novel result that proves indistinguishability of identical versus independent Haar states against LOCC (local operations, classical communication) adversaries. More precisely, (A, B) is an LOCC adversary if A and B are quantum algorithms who can communicate with each other via only classical communication channels. It is important that A and B do not share any entanglement. Moreover, we restrict our attention to LOCC distinguishers which are LOCC adversaries of the form (A, B) where A does not output anything whereas B outputs a single bit. We say that a LOCC distinguisher (A, B) can distinguish two states ρ_{AB} and σ_{AB} with probability at most ε, referred to as ε-LOCC indistinguishability, where A receives the register A and B receives the register B, if $|\Pr[1 \leftarrow (A, B)(\rho_{\mathsf{AB}})] - \Pr[1 \leftarrow (A, B)(\sigma_{\mathsf{AB}})]| = \varepsilon$. Of particular interest is the case when

$$\rho_{\mathsf{AB}} = \mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{H}_n} \left[(|\psi\rangle^{\otimes t})_{\mathsf{A}} \otimes (|\psi\rangle^{\otimes t})_{\mathsf{B}} \right], \ \sigma_{\mathsf{AB}} = \mathop{\mathbb{E}}_{\substack{|\psi\rangle \leftarrow \mathcal{H}_n, \\ |\phi\rangle \leftarrow \mathcal{H}_n}} \left[(|\psi\rangle^{\otimes t})_{\mathsf{A}} \otimes (|\phi\rangle^{\otimes t})_{\mathsf{B}} \right]$$

Here, $\mathcal{H}_n$ denotes the Haar distribution on n-qubit quantum states and t is polynomial in n. A couple of works by Harrow [Har23] and Chen, Cotler, Huang and Li [CCHL22] prove that the LOCC indistinguishability of ρ_{AB} and σ_{AB} is negligible in n in the case when $t = 1$. In this work, we extend to the case when t is arbitrary.

Theorem 1.5. *ρ_{AB} and σ_{AB} (defined above) are ε-LOCC indistinguishable, where $\varepsilon = O\left(\frac{t^2}{2^n}\right)$.*

We also show that the above bound is tight by demonstrating an LOCC distinguisher whose distinguishing probability is $\Theta(\frac{t^2}{2^n})$.

Recently, Ananth, Kaleoglu and Yuen [AKY24] prove the indistinguishability of ρ_{AB} and σ_{AB} in the dual setting, against non-local adversaries that can share entanglement but cannot communicate.

The above theorem can easily be extended to the multi-party setting where either all the parties get (many copies of) the same Haar state or they receive i.i.d Haar states.

Separations. We use Theorem 1.5 to show that some quantum cryptographic primitives with classical communication are impossible in the CHS model. Let us develop some intuition towards proving such a statement. Suppose there are two or more parties participating in a quantum cryptographic protocol with classical communication in the CHS model. By definition, all the parties would receive many, say t, copies of $|\psi\rangle$, where $|\psi\rangle$ is sampled from the Haar distribution. Since the parties can only exchange classical messages, thanks to Theorem 1.5, without affecting correctness or security we can modify the protocol wherein for each party, say P_i, a Haar state $|\psi_i\rangle$ is sampled and t copies of $|\psi_i\rangle$ is given to P_i. From this, we can extract a quantum cryptographic primitive in the plain model since each party can sample a Haar state on its own. In conclusion, quantum cryptographic primitives with classical communication in the CHS model can be turned into their counterparts in the plain model.

This gives a natural recipe for proving impossibility results in the CHS model. We apply this recipe to obtain impossibility results for interactive key agreements and interactive commitments.

Theorem 1.6. *Interactive quantum key agreement and interactive quantum commitment protocols, with classical communication, are impossible in the CHS model.*

We extend the above theorem to separate interactive quantum key agreement and interactive quantum commitments from pseudorandom function-like state generators. The separations are obtained by considering a variant of the CHS model where the adversary does not get access to many copies of one Haar state but instead gets access to infinitely many input-less oracles[2] $\left\{\{G_{k,x}\}_{k,x\in\{0,1\}^\lambda}\right\}_{\lambda\in\mathbb{N}}$ such that each $G_{k,x}$ produces a copy of a Haar state $|\psi_{k,x}\rangle$. In this model, it is easy to construct pseudorandom function-like states. However, an extension of Theorem 1.6 rules out the possibility of interactive quantum key agreement and quantum commitments with classical communication in this variant. Thus, we have the following.

Theorem 1.7. *There does not exist a black-box reduction from interactive quantum key agreement and quantum commitments with classical communication to pseudorandom function-like states.*

Prior work by Chung, Goldin and Gray [CGG24] extensively studies the separations between quantum cryptographic primitives with classical communication and different quantum pseudorandomness notions. However, their framework did not capture the above result.

Prior works by [ACC+22; CLM23; LLLL24] ruled out quantum key agreements and non-interactive commitments with classical communication from post-quantum one-way functions. However, their separation was either based on a conjecture or in a restricted setting whereas our result is unconditional. This makes our result incomparable with the results from [ACC+22; CLM23; LLLL24]. Our work follows a long line of recent works [HY20; ACC+22; AHY23; CLM23; ACH+23; BGVV+23; BM+24; CM24] that make progress in understanding the landscape of black-box separations in quantum cryptography.

2 Technical Overview

2.1 Pseudorandomness in the CHS Model

Warmup: Pseudorandom State Generators (PRSGs). As a warmup, we first study 1-copy PRSG in the CHS model. Consider the following construction: $G_k(|\vartheta\rangle) := (Z^k \otimes I_{n-\lambda})|\vartheta\rangle$, where $Z^k = Z^{k_1}\otimes\cdots\otimes Z^{k_\lambda}$, $k = k_1\cdots k_\lambda \in \{0,1\}^\lambda$ and $I_{n-\lambda}$ is an identity operator on $n-\lambda$ qubits. In other words, G_k applies a random Pauli Z operator only on the first λ qubits and does not touch the rest. Note that this construction already satisfies the stretch property (i.e. the output length is larger than the key length).

Let us consider the case when the adversary receives just one copy of $|\vartheta\rangle$ and is expected to distinguish $G_k(|\vartheta\rangle)$ versus an independent Haar state $|\varphi\rangle$. Formally, we would like to argue that the following states are close.

$$\rho := \mathop{\mathbb{E}}_{\substack{k\leftarrow\{0,1\}^\lambda\\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} [G_k(|\vartheta\rangle)\otimes|\vartheta\rangle\langle\vartheta|] \text{ and } \sigma := \frac{I}{2^n}\otimes\frac{I}{2^n}.$$

By the properties of the symmetric subspace, the following holds:

$$\mathop{\mathbb{E}}_{|\vartheta\rangle\leftarrow\mathcal{H}_n}\left[|\vartheta\rangle\langle\vartheta|^{\otimes 2}\right] \approx_\varepsilon \mathop{\mathbb{E}}_{x,y\leftarrow[2^n],x^1\neq y^1}\left[\frac{1}{2}\left(|xy\rangle\langle xy| + |xy\rangle\langle yx| + |yx\rangle\langle xy| + |yx\rangle\langle yx|\right)\right],$$

where ε is negligible in n and the notation x^1 (respectively, y^1) denotes the first λ bits of x (respectively, y). Now, applying a random Z operator on the first λ qubits tantamounts to measuring the first λ qubits in the computational basis. Given the fact that $x^1 \neq y^1$, this measurement unentangles the last n qubits. Thus, the result is a state of the form $\mathbb{E}_{x,y\leftarrow[2^n],x^1\neq y^1}\left[\frac{1}{2}|x\rangle\langle x|\otimes|y\rangle\langle y| + \frac{1}{2}|y\rangle\langle y|\otimes|x\rangle\langle x|\right]$. This state is in turn close to $\frac{I}{2^n}\otimes\frac{I}{2^n}$.

Generalizing to Many Copies of the CHS. Next, we to generalize the above approach to even when polynomially many copies of the CHS are provided. Formally, we would like to argue that the following two

[2]We note that [Kre21] made similar use of infinitely many oracles to prove a separation between pseudorandom states and one-way functions.

states are close.

$$\rho := \mathop{\mathbb{E}}_{\substack{k\leftarrow\{0,1\}^\lambda \\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[G_k(|\vartheta\rangle)\otimes|\vartheta\rangle\langle\vartheta|^{\otimes t}\right] \text{ and } \sigma := \mathop{\mathbb{E}}_{\substack{|\varphi\rangle\leftarrow\mathcal{H}_n \\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[|\varphi\rangle\langle\varphi|\otimes|\vartheta\rangle\langle\vartheta|^{\otimes t}\right],$$

where t is some polynomial of n. Note that, by the property of the Haar distribution, we can simplify σ to

$$\sigma = \frac{I}{2^n}\otimes \mathop{\mathbb{E}}_{T\leftarrow[0:t]^N}|T\rangle\langle T|,$$

where $|T\rangle$ is a type state[3] and $N = 2^n$. Note that by the properties of the symmetric subspace,

$$\mathop{\mathbb{E}}_{|\vartheta\rangle\leftarrow\mathcal{H}_n}\left[|\vartheta\rangle\langle\vartheta|^{\otimes t+1}\right] \approx_\varepsilon \mathop{\mathbb{E}}_{\substack{T\leftarrow[0:t+1]^N \\ T \text{ is } \lambda\text{-prefix collision-free}}} |T\rangle\langle T|,$$

where ε is negligible in n and T is λ-prefix collision-free if $T\in\{0,1\}^N$ and for any $x,y\in T$[4] with $x\neq y$ implies $x^1\neq y^1$, where the notation x^1 (respectively, y^1) denotes the first λ bits of x (respectively, y). Note that, any λ-prefix collision-free type T,

$$|T\rangle = \frac{1}{\sqrt{\binom{t+1}{t}}}\sum_{x\in T}|x\rangle|T\setminus\{x\}\rangle.$$

Again, applying a random Z operator on the first λ qubits tantamounts to measuring the first λ qubits in the computational basis. Given the fact that T is λ-prefix collision-free, this measurement unentangles the first n qubits. Thus, the result is a state of the form

$$\mathop{\mathbb{E}}_{\substack{T\leftarrow[0:t+1]^N \\ T \text{ is } \lambda\text{-prefix collision-free} \\ x\leftarrow T}} \left[|x\rangle\langle x|\otimes|T\setminus\{x\}\rangle\langle T\setminus\{x\}|\right].$$

This state is in turn close to $\frac{I}{2^n}\otimes\mathbb{E}_{T\leftarrow[0:t]^N}|T\rangle\langle T|$.

Generalizing to ℓ-copy PRSG. Finally, we generalize this ℓ-copy PRSG. Formally, we would like to argue that the following two states are close.

$$\rho := \mathop{\mathbb{E}}_{\substack{k\leftarrow\{0,1\}^\lambda \\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[G_k(|\vartheta\rangle)^{\otimes\ell}\otimes|\vartheta\rangle\langle\vartheta|^{\otimes t}\right] \text{ and } \sigma := \mathop{\mathbb{E}}_{\substack{|\varphi\rangle\leftarrow\mathcal{H}_n \\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[|\varphi\rangle\langle\varphi|^{\otimes\ell}\otimes|\vartheta\rangle\langle\vartheta|^{\otimes t}\right],$$

where ℓ, t is some polynomial of n. Note that, by the property of the Haar distribution, we can simplify σ to

$$\sigma = \mathop{\mathbb{E}}_{T_1\leftarrow[0:\ell]^N}|T_1\rangle\langle T_1|\otimes\mathop{\mathbb{E}}_{T_2\leftarrow[0:t]^N}|T_2\rangle\langle T_2|,$$

where $|T_1\rangle, |T_2\rangle$ are type states and $N = 2^n$. Note that, similar to the last case, we can still write,

$$\mathop{\mathbb{E}}_{|\vartheta\rangle\leftarrow\mathcal{H}_n}\left[|\vartheta\rangle\langle\vartheta|^{\otimes t+\ell}\right] \approx_\varepsilon \mathop{\mathbb{E}}_{\substack{T\leftarrow[0:t+\ell]^N \\ T \text{ is } \lambda\text{-prefix collision-free}}} |T\rangle\langle T|,$$

and any λ-prefix collision-free type T,

$$|T\rangle = \frac{1}{\sqrt{\binom{t+\ell}{\ell}}}\sum_{\substack{T_1\subset T \\ |T_1|=\ell}}|T_1\rangle|T\setminus T_1\rangle.$$

[3] We encourage readers unfamiliar with type states to refer to Definition 3.8.

[4] Since $T\in\{0,1\}^N$, we can treat it as a set, in particular the set associated to T is $\{i : T[i] = 1\}$.

Ideally, we would want the application of $(Z^k \otimes I_{n-\lambda})^{\otimes \ell}$ to unentangle $|T_1\rangle$ from $|T \setminus T_1\rangle$. This is equivalent to measuring the first ℓ registers in the type basis. This is in general not true, not true. Hence, we settle for the next best thing, which is finding a "dense-enough"[5] subset of λ-prefix collision-free type such that $(Z^k \otimes I_{n-\lambda})^{\otimes \ell}$ to unentangle $|T_1\rangle$ from $|T \setminus T_1\rangle$. We find this subset to be "λ-prefix ℓ-fold collision-free" types.

We say that a λ-prefix collision-free type T is "λ-prefix ℓ-fold collision-free" if for all pairs of ℓ sized subsets $T_1, T_2 \subset T$, $\oplus_{x \in T_1} x = \oplus_{x \in T_2} x$ only if $T_1 = T_2$. We start by noting that this subset is only "dense-enough" if $\ell = O\left(\frac{\lambda}{\log(\lambda)^{1+\varepsilon}}\right)$, for any constant $\varepsilon > 0$.[6]

Next, we show that for these λ-prefix ℓ-fold collision-free types states, applying a random $(Z^k \otimes I_{n-\lambda})^{\otimes \ell}$ is equivalent to meauring the first ℓ registers in the type basis. This is because $(Z^k \otimes I_{n-\lambda})^{\otimes \ell}$ on a type state $|T_1\rangle$ is equivalent to adding a phase of $(-1)^{k \cdot (\oplus_{x \in T_1} x)}$. Hence,

$$\mathop{\mathbb{E}}_{k}\left[(Z^k \otimes I_{n-\lambda})^{\otimes \ell} \otimes I_{tn} |T\rangle\langle T| (Z^k \otimes I_{n-\lambda})^{\otimes \ell} \otimes I_{tn}\right] = \mathop{\mathbb{E}}_{k}\left[\frac{1}{\binom{t+\ell}{\ell}} \sum_{\substack{T_1, T_2 \subset T \\ |T_1|=|T_2|=\ell}} (-1)^{k \cdot (\oplus_{x \in T_1} x \oplus \oplus_{y \in T_2} y)} |T_1\rangle|T \setminus T_1\rangle\langle T_2|\langle T \setminus T_2|\right],$$

which for λ-prefix ℓ-fold collision-free types states is non-zero only if $T_1 = T_2$, giving us

$$\mathop{\mathbb{E}}_{k}\left[(Z^k \otimes I_{n-\lambda})^{\otimes \ell} \otimes I_{tn} |T\rangle\langle T| (Z^k \otimes I_{n-\lambda})^{\otimes \ell} \otimes I_{tn}\right] = \mathop{\mathbb{E}}_{\substack{T_1 \subset T \\ |T_1|=\ell}} \left[|T_1\rangle\langle T_1| \otimes |T \setminus T_1\rangle\langle T \setminus T_1|\right].$$

Over expectation over all λ-prefix ℓ-fold collision-free types states, this state is close to $\mathbb{E}_{T_1 \leftarrow [0:\ell]^N} |T_1\rangle\langle T_1| \otimes \mathbb{E}_{T_2 \leftarrow [0:t]^N} |T_2\rangle\langle T_2|$.

Limitations. To complement our result, we show that a t-copy PRSG is impossible in the CHS model, for $\ell = O\left(\frac{\lambda}{\log(\lambda)}\right)$ (for a restricted class of PRSG constructs which only takes one copy of the common Haar state). We show this by showing that the rank of σ grows much faster than the rank of ρ, hence, a simple distinguisher is a projector on the eigenspace of ρ. In particular, let $\tilde{G}_k(\vartheta)$ be the PRSG. Then define

$$\rho := \mathop{\mathbb{E}}_{\substack{k \leftarrow \{0,1\}^\lambda \\ |\vartheta\rangle \leftarrow \mathcal{H}_n}} \left[\tilde{G}_k(|\vartheta\rangle)^{\otimes \ell} \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t}\right] \text{ and } \sigma := \mathop{\mathbb{E}}_{\substack{|\varphi\rangle \leftarrow \mathcal{H}_n \\ |\vartheta\rangle \leftarrow \mathcal{H}_n}} \left[|\varphi\rangle\langle\varphi|^{\otimes \ell} \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t}\right]$$

Now since $\tilde{G}_k(|\vartheta\rangle)$ is a PRSG, its output is negligibly close to a pure state. This means that the rank of $\rho \leq 2^\lambda \binom{2^n+t+\ell-1}{t+\ell}$. In contrast, the rank of $\sigma = \binom{2^n+\ell-1}{\ell}\binom{2^n+t-1}{t}$. Note that, for $t = \lambda^3$ and $\ell = \lambda/\log(\lambda)$, $\operatorname{rank}(\rho)/\operatorname{rank}(\sigma) = \mathsf{negl}$. Hence, we can find a distinguisher. Here the distinguisher just projects onto the eigenspace of ρ, ρ gets accepted with probability 1 but σ gets accepted with probability negl, hence giving a disguisher. Since PRFSs imply PRSs (by setting $c = 0$), achieving an ℓ-query statistical PRFS in the CHS model for $\ell = \Omega(\lambda/\log(\lambda))$ is impossible.

Pseudorandom Function-like State Generators. Next we extend this idea from PRSGs to achieve PRFSGs. We take inspiration from the seminal Goldreich-Goldwasser-Micali approach [GGM86]. In particular, on the key $K = (k_1^0, \ldots, k_m^0, k_1^1, \ldots, k_m^1) \in \{0,1\}^{2\lambda' m}$ and the input $\mathbf{x} = (x_1, \ldots, x_m) \in \{0,1\}^m$, define the PRFSG $G_K(\mathbf{x}, |\vartheta\rangle)$ as follows: $G_K(\mathbf{x}, |\vartheta\rangle) = (Z^{\bigoplus_{i=1}^m k_i^{x_i}} \otimes I_{n-\lambda'})|\vartheta\rangle$. Formally, the following two states are close:

$$\rho := \mathop{\mathbb{E}}_{\substack{K \leftarrow \{0,1\}^{2m\lambda'} \\ |\vartheta\rangle \leftarrow \mathcal{H}_n}} \left[\otimes_{i=1}^q G_K(\mathbf{x}^i, |\vartheta\rangle)^{\otimes \ell_i} \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t}\right],$$

[5] Here, by dense-enough, we mean when picking a random type from λ-prefix collision-free, it lies in this subset with probability $1 - \mathsf{negl}$.

[6] Later, in the impossibility result, we show that this is in fact the best we can hope for as a larger subset would bypass the impossibility result.

and

$$\sigma := \mathop{\mathbb{E}}_{\substack{\forall i\in[q],|\varphi_i\rangle\leftarrow\mathcal{H}_n\\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[\otimes_{i=1}^{q}|\varphi_i\rangle\langle\varphi_i|^{\otimes\ell_i}\otimes|\vartheta\rangle\langle\vartheta|^{\otimes t}\right],$$

for all $\mathbf{x}^1,\ldots,\mathbf{x}^q\in\{0,1\}^m$ and $\ell_1,\ldots,\ell_q$ such that $\sum_{i=1}^q\ell_i=\ell$, for $\ell=O\left(\frac{\lambda^{1-c}}{\log(\lambda)^{1+\varepsilon}}\right)$ and $m=\lambda^c$, for any constant $\varepsilon>0$ and $c\in[0,1)$.

Just as before, we can write σ as follows:

$$\sigma=\bigotimes_{i=1}^{q}\mathop{\mathbb{E}}_{T_i\leftarrow[0:\ell_i]^N}|T_i\rangle\langle T_i|\otimes\mathop{\mathbb{E}}_{\tilde{T}\leftarrow[0:t]^N}|\tilde{T}\rangle\langle\tilde{T}|,$$

where T_i's and $\tilde{T}$ are type states and $N=2^n$. Note that, similar to the last case, we can still write,

$$\mathop{\mathbb{E}}_{|\vartheta\rangle\leftarrow\mathcal{H}_n}\left[|\vartheta\rangle\langle\vartheta|^{\otimes t+\ell}\right]\approx_\varepsilon\mathop{\mathbb{E}}_{\substack{T\leftarrow[0:t+\ell]^N\\ T\text{ is }\lambda\text{-prefix }\ell\text{-fold collision-free}}}|T\rangle\langle T|,$$

and any λ-prefix ℓ-fold collision-free type T,

$$|T\rangle=\frac{1}{\sqrt{\binom{t+\ell}{\ell}}}\sum_{\substack{T_1\subset T\\ |T_1|=\ell}}|T_1\rangle|T\setminus T_1\rangle.$$

Now, after application of one layer of $(Z^k\otimes I_{n-\lambda})^{\otimes\ell}$, we know that $|T_1\rangle$ unentangles from $|T\setminus T_1\rangle$. We extend this idea to show that even for a tensor of type states, applying $(Z^k\otimes I_{n-\lambda})^{\otimes\tilde{\ell}_i}$ on parts of each type state still unentangles each of them as long as all the type states are λ-prefix ℓ-fold collision-free type and their combined set is still λ-prefix ℓ-fold collision-free. Formally, we show the following: Let $\tilde{\ell}_1,\ldots,\tilde{\ell}_q\in\mathbb{N}$, and $t_1,\ldots,t_q\in\mathbb{N}$ such that $\sum_{i=1}^q\tilde{\ell}_i=\tilde{\ell}$ and $\sum_{i=1}^q t_i=t$. Then for any λ-prefix $\tilde{\ell}$-fold collision-free type T and any mutually disjoint sets $T_1,\ldots,T_q$ satisfying $\bigcup_{i=1}^q T_i=T$ and $|T_i|=t_i+\tilde{\ell}_i$ for all $i\in[q]$,

$$\mathop{\mathbb{E}}_{k\leftarrow\{0,1\}^n}\left[\bigotimes_{i=1}^{q}\left(\left(Z^k\otimes I_m\right)^{\otimes\ell_i}\otimes I_{n+m}^{\otimes t_i}\right)|T_i\rangle\langle T_i|\left(\left(Z^k\otimes I_m\right)^{\otimes\tilde{\ell}_i}\otimes I_{n+m}^{\otimes t_i}\right)\right]$$
$$=\bigotimes_{i=1}^{q}\mathop{\mathbb{E}}_{\substack{X_i\subset T_i\\ |X_i|=\tilde{\ell}_i}}\left[|X_i\rangle\langle X_i|\otimes|T_i\setminus X_i\rangle\langle T_i\setminus X_i|\right].$$

Hence, applying each layer $(Z^{k_i^b}\otimes I_{n-\lambda})$ unentangles all type states into two halfs. Hence, by repeated application, we get

$$\rho\approx_\varepsilon\mathop{\mathbb{E}}_{\substack{T\leftarrow[0:t+\ell]^N\\ T\text{ is }\lambda\text{-prefix }\ell\text{-fold collision-free}}}\mathop{\mathbb{E}}_{(T_1,T_2,\ldots,T_q,\hat{T})}\left[\bigotimes_{i=1}^{q}|T_i\rangle\langle T_i|\otimes|\hat{T}\rangle\langle\hat{T}|\right],$$

where $(T_1,T_2,\ldots,T_q,\hat{T})$ are sampled as follows: for $i=1,2,\ldots,q$, sample an ℓ_i-subset from $T\setminus(\bigcup_{j=1}^{i-1}T_j)$ uniformly and let $\hat{T}:=T\setminus(\bigcup_{j=1}^{q}T_j)$. Over expectation over all λ-prefix ℓ-fold collision-free types states, this state is close to σ.

2.2 Quantum Bit Commitments

With t-copy PRSG in hand, we construct a statistically-hiding, statistically-binding commitment scheme in the CHS model. Our scheme draws inspiration from the quantum commitment scheme introduced in [MY21; MNY23] that builds quantum bit commitments from t-copy PRSG.

In particular, to commit to $b = 0$, the committer creates a superposition over all keys of the PRSG in the decommitment register and runs the PRSG in superposition over this register. The committer sets this as the commitment register. To commit to $b = 1$, the committer creates a maximally entangled state over the commitment and the decommitment register. Formally,

$$|\psi_0\rangle_{\mathsf{C}_i\mathsf{R}_i} := \frac{1}{\sqrt{2^\lambda}} \sum_{k\in\{0,1\}^\lambda} G_k(|\vartheta\rangle)_{\mathsf{C}_i}|k||0^{n-\lambda}\rangle_{\mathsf{R}_i}$$

and

$$|\psi_1\rangle_{\mathsf{C}_i\mathsf{R}_i} := \frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} |j\rangle_{\mathsf{C}_i}|j\rangle_{\mathsf{R}_i},$$

where, $(\mathsf{C}_1, \ldots, \mathsf{C}_p)$ is the commitment register and $(\mathsf{R}_1, \ldots, \mathsf{R}_p)$ is the reveal register.

To achieve hiding, our scheme relies on the pseudorandomness property of the PRSG. In particular, the commitment is very close to one where the keys are distinct for all $(\mathsf{C}_i, \mathsf{R}_i)$, in this case, one copy of PRS is indistinguishable from a maximally mixed state.[7]

Unlike the approach in [MY21], our construction is not of the canonical form [Yan22]. To achieve binding, the receiver performs multiple SWAP tests. In particular, we show that since the rank of the commitment registers is exponentially separated, multiple SWAP tests can distinguish between the two.

2.3 Black-Box Separations

LOCC Indistinguishability. The notion of LOCC indistinguishability is well-studied and is referred to as quantum data hiding by quantum information theorists [BDF+99; DLT02; EW02; Gea02; HLS05; MWW09; CLMO13; PNC14; CH14; CLM+14; HBAB19]. In this setting, there is a challenger, two (possibly entangled and mixed) bipartite quantum states ρ_{AB} and σ_{AB}, and a computationally unbounded, two-party distinguisher (Alice, Bob) who are spatially separated and without pre-shared entanglement. The challenger picks a quantum state from $\{\rho_{\mathsf{AB}}, \sigma_{\mathsf{AB}}\}$ uniformly at random and sends register A to Alice and register B to Bob respectively. The task of Alice and Bob is to distinguish whether they are given ρ_{AB} or σ_{AB} by performing local operations and communicating classically. We call such distinguishers *LOCC adversaries*.

We focus on the case where Alice and Bob each receive $t = \mathrm{poly}(\lambda)$ copies of $|\psi\rangle_{\mathsf{A}}$ and $|\phi\rangle_{\mathsf{B}}$, where $|\psi\rangle$ and $|\phi\rangle$ are either two identical or i.i.d. Haar states of length $n = \omega(\log(\lambda))$. Explicitly, the two input states are

$$\rho_{\mathsf{AB}} = \mathop{\mathbb{E}}_{|\psi\rangle\leftarrow\mathcal{H}_n} \left[|\psi\rangle\langle\psi|_{\mathsf{A}}^{\otimes t} \otimes |\psi\rangle\langle\psi|_{\mathsf{B}}^{\otimes t}\right],$$

$$\sigma_{\mathsf{AB}} = \mathop{\mathbb{E}}_{|\psi\rangle\leftarrow\mathcal{H}_n} \left[|\psi\rangle\langle\psi|_{\mathsf{A}}^{\otimes t}\right] \otimes \mathop{\mathbb{E}}_{|\phi\rangle\leftarrow\mathcal{H}_n} \left[|\phi\rangle\langle\phi|_{\mathsf{B}}^{\otimes t}\right].$$

Note that if global measurements are allowed, performing SWAP tests can easily distinguish them. As one of our main technical contributions, we show that for any LOCC adversary, the advantage of distinguishing ρ_{AB} from σ_{AB} is negligible in λ. Before we explain the proof, we compare our theorem with [Har23, Theorem 8]. In short, the theorems are incomparable. Our setting is stronger in the sense that the LOCC adversary both obtain polynomial copies of the input, while [Har23, Theorem 8] studies the single-copy setting. However, [Har23, Theorem 8] is more general since it holds for a family of input states, whereas the input in our setting is fixed to ρ_{AB} and σ_{AB}, which are belong to the family. We refer the readers to Remark 7.12 for a detailed discussion.

Toward the proof, we start by using the following common technique in proving LOCC indistinguishability: the set of LOCC measurements is a (proper) subset of the set of all positive partial transpose (PPT) measurements [CLM+14]. Hence, it is sufficient to upper bound the maximum distinguishing advantage over two-outcome PPT measurements, i.e., $\{M_{\mathsf{AB}}, I_{\mathsf{AB}} - M_{\mathsf{AB}}\}$ such that $0 \preceq M_{\mathsf{AB}} \preceq I_{\mathsf{AB}}$ and $0 \preceq M_{\mathsf{AB}}^{\Gamma_B} \preceq I_{\mathsf{AB}}$, where $M_{\mathsf{AB}}^{\Gamma_B}$ denote the partial transpose of M_{AB} with respect to B. Next, from the basic properties of partial

[7] Note that this still needs multi-key security which is not trivial in the CHS model, since all the PRS generators share the same Haar state for randomness. But we prove that our construction satisfies multikey security.

transpose and trace norm, we show that the distinguishing advantage is bounded by the trace norm between $\rho_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}$ and $\sigma_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}$.

The most technical part of the proof is to upper bound the quantity $\left\|\rho_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}} - \sigma_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}\right\|_1$. We point out that the partial transpose of a density matrix might *not* be a positive semidefinite matrix. Our first step is to expand ρ_{AB} and σ_{AB} in the *type basis* as follows:

$$\rho_{\mathsf{AB}} = \mathop{\mathbb{E}}_{T \leftarrow [0:2t]^d} \left[|T\rangle\langle T|_{\mathsf{AB}} \right],$$

$$\sigma_{\mathsf{AB}} = \mathop{\mathbb{E}}_{S_A \leftarrow [0:t]^d} \left[|S_A\rangle\langle S_A|_{\mathsf{A}} \right] \otimes \mathop{\mathbb{E}}_{S_B \leftarrow [0:t]^d} \left[|S_B\rangle\langle S_B|_{\mathsf{B}} \right],$$

where $d := 2^n$. Next, we further conditioned on the events that (1) T, S_A and S_B each have no repeated elements (2) S_A and S_B have no identical elements. From the collision bound, doing so only incurs an additional error of $O(t^2/d) = \mathsf{negl}(\lambda)$. Therefore, we can now treat T, S_A and S_B as *sets*. It suffices to prove that $\left\|\tilde{\rho}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}} - \tilde{\sigma}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}\right\|_1$ is negligible in λ, where

$$\tilde{\rho}_{\mathsf{AB}} := \mathop{\mathbb{E}}_{T \leftarrow \binom{[d]}{2t}} \left[|T\rangle\langle T|_{\mathsf{AB}} \right],$$

$$\tilde{\sigma}_{\mathsf{AB}} := \mathop{\mathbb{E}}_{\substack{S_A, S_B \leftarrow \binom{[d]}{t}: \\ S_A \cap S_B = \emptyset}} \left[|S_A\rangle\langle S_A|_{\mathsf{A}} \otimes |S_B\rangle\langle S_B|_{\mathsf{B}} \right].$$

Observe that the $\tilde{\sigma}_{\mathsf{AB}}^{\Gamma_B} = \tilde{\sigma}_{\mathsf{AB}}$. To obtain a simpler expression of $\tilde{\rho}_{\mathsf{AB}}^{\Gamma_B}$, we rely on the following useful identity for bi-partitioning the type states:

$$|T\rangle_{\mathsf{AB}} = \sum_{X \in \binom{T}{t}} \frac{1}{\sqrt{\binom{2t}{t}}} |T \setminus X\rangle_{\mathsf{A}} \otimes |X\rangle_{\mathsf{B}}.$$

Hence, the partial transpose of $\tilde{\rho}_{\mathsf{AB}}$ can be written as

$$\tilde{\rho}_{\mathsf{AB}}^{\Gamma_B} = \mathop{\mathbb{E}}_{T \leftarrow \binom{[d]}{2t}} \left[\frac{1}{\binom{2t}{t}} \sum_{X, Y \in \binom{T}{t}} |T \setminus X\rangle\langle T \setminus Y|_{\mathsf{A}} \otimes |Y\rangle\langle X|_{\mathsf{B}} \right].$$

If $X = Y$, then the term is the tensor product of two *disjoint* sets $|T \setminus X\rangle\langle T \setminus X|_{\mathsf{A}} \otimes |X\rangle\langle X|_{\mathsf{B}}$. Such a term will be canceled out by the corresponding term in $\tilde{\sigma}_{\mathsf{AB}}^{\Gamma_B}$ since they have equal coefficients. Therefore, the difference between them is the following matrix with mismatched X and Y:

$$\tilde{\rho}_{\mathsf{AB}}^{\Gamma_B} - \tilde{\sigma}_{\mathsf{AB}}^{\Gamma_B} = \mathop{\mathbb{E}}_{T \leftarrow \binom{[d]}{2t}} \left[\frac{1}{\binom{2t}{t}} \sum_{X, Y \in \binom{T}{t} : X \neq Y} |T \setminus X\rangle\langle T \setminus Y|_{\mathsf{A}} \otimes |Y\rangle\langle X|_{\mathsf{B}} \right].$$

We continue to simplify it by applying a double-counting argument. Every tuple of sets (T, X, Y) uniquely determines a tuple of mutually disjoint sets (C, I, X', Y') satisfying $C = T \setminus (X \cup Y)$ (C for the complement of $X \cup Y$), $I = X \cap Y$ (I for intersection), $X' = X \setminus I$ and $Y' = Y \setminus I$. Hence, $T \setminus X = C \uplus Y'$, $Y = I \uplus Y'$, $T \setminus Y = C \uplus X'$, and $X = I \uplus X'$ where $\uplus$ denotes the disjoint union. By further classifying the summands according to $s := |C| = |I| \in \{0, 1, \ldots, t-1\}$ (note that then $|X'| = |Y'| = t - s$), we have

$$\left\|\tilde{\rho}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}} - \tilde{\sigma}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}\right\|_1 = \frac{1}{\binom{d}{2t}\binom{2t}{t}} \left\| \sum_{s=0}^{t-1} \sum_{C \in \binom{[d]}{s}} \sum_{I \in \binom{[d] \setminus C}{s}} \sum_{\substack{X', Y' \in \binom{[d] \setminus (C \uplus I)}{t-s}: \\ X' \cap Y' = \emptyset}} |C \uplus Y'\rangle_{\mathsf{A}} |I \uplus Y'\rangle_{\mathsf{B}} \langle C \uplus X'|_{\mathsf{A}} \langle I \uplus X'|_{\mathsf{B}} \right\|_1$$

$$\leq \frac{1}{\binom{d}{2t}\binom{2t}{t}} \sum_{s=0}^{t-1} \sum_{C\in\binom{[d]}{s}} \sum_{I\in\binom{[d]\setminus C}{s}} \Bigg\| \underbrace{\sum_{\substack{X',Y'\in\binom{[d]\setminus(C\uplus I)}{t-s}:\\ X'\cap Y'=\emptyset}} |C\uplus Y'\rangle_{\mathsf{A}}|I\uplus Y'\rangle_{\mathsf{B}}\langle C\uplus X'|_{\mathsf{A}}\langle I\uplus X'|_{\mathsf{B}}}_{=:K_{C,I}} \Bigg\|_1,$$

where the inequality follows from the triangle inequality. We observe that the matrix $K_{C,I}$ has the same structure as the adjacency matrix of *Kneser graphs*. Here, we recall the definition of Kneser graphs. For $v, k \in \mathbb{N}$, the Kneser graph $K(v,k)$ is the graph whose vertices correspond to the k-element subsets of the set $[v]$, and two vertices are adjacent if and only if the two corresponding sets are disjoint. Therefore, for every (C, I), the matrix $K_{C,I}$ is isospectral to the adjacency matrix of the Kneser graph $K(d-|C|-|I|, t-|I|)$. Finally, we employ the well-studied spectral property of Kneser graphs as a black box to obtain an $O(t^2/d) = \mathsf{negl}(\lambda)$ upper bound for $\left\|\tilde{\rho}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}} - \tilde{\sigma}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}\right\|_1$.

Furthermore, we show the tightness of the theorem by constructing an optimal LOCC distinguisher that achieves the same advantage. The strategy is simple: Alice and Bob each individually measure every copy of their input in the computational basis and obtain a total of $2t$ outcomes. Then, they output 1 if there is any collision among these $2t$ outcomes.

Impossibility Results in the CHS model. With the LOCC Haar indistinguishability theorem in hand, we investigate the limits of the CHS model when the communication between the parties is classical. We show that the several impossibility results of information-theoretically secure schemes in the plain model can be generically lifted to the CHS model, even when the adversary does not receive any common Haar state. We emphasize that there is no classical counterpart in the CRS model. If the adversary is not given the CRS, then many information-theoretically secure schemes do exist, such as key agreements.

As common in proving impossibilities, our approach is to convert schemes in the CHS model to those in the plain model. The transform is simple: in the new scheme, the parties each sample polynomially many copies of the Haar state *independently* and run the original scheme. Crucially, despite the inconsistency in their Haar states, the new scheme still satisfies completeness thanks to the LOCC Haar indistinguishability. A caveat is that sampling Haar states is time-inefficient. However, since the impossibilities in the plain model are still valid if the (honest) algorithms in the scheme are time-inefficient, doing so is acceptable for the sake of showing impossibilities.

Separation Results. We separate many important primitives from $(\lambda, \omega(\log(\lambda)))$-PRSG. Since $(\lambda, \omega(\log(\lambda)))$-PRSGs do not exist in the CHS model, we need to "strengthen" the oracle in order to prove separations. For every security parameter $\lambda \in \mathbb{N}$, we define the oracle as $\{G_k\}_{k\in\{0,1\}^\lambda}$ where each G_k is an isometry that takes no input and outputs an i.i.d. Haar state $|\psi_k\rangle$.

Relative to this oracle, the implementation of the PRSG is straightforward: the output on k of any length $\lambda \in \mathbb{N}$ is $|\psi_k\rangle$. The security directly follows from the hardness of unstructured search. To prove the non-existence of QCCC schemes, we employ a two step approach. First, showing that a scheme with respect to this oracle can be transformed to schemes with respect to a much weaker oracle. Second, showing that this much weaker oracle does not give much extra power over the plain model. Formally: First, similar to the previous section, we show that due to the LOCC indistinguishability, the parties can sample all "large" quantum states on their own, and the correctness and security is only "polynomially" affected[8]. This means that any scheme with respect this this oracle can be turned into a scheme with respect to an oracle with only short (constant times logarithmic) Haar states. Second, for short (constant times logarithmic) quantum states, we show that this oracle does not give much extra power since an adversary can learn the oracle completely. This is because for short-enough states, the adversary can run tomography on polynomial queries and learn the state with up to inverse polynomial error. Hence, the adversary can simulate both

[8]Since the Haar indistinguishability has a factor of $O(t^2/d)$, as long as t^2/d is inverse-polynomial, we do not incur a lot of loss.

parties post-selecting on a transcript to learn any secret[9]. This means that any scheme secure in the presence of this oracle can be transformed into another scheme that is secure in the plain model.

Lastly, we observe that by considering a generalized oracle, namely $\{G_{k,x}\}_{k,x\in\{0,1\}^\lambda}$, we can show that (classically accessible) PRFSGs with super-logarithmic input length exist. We can extend the impossibility of QCCC commitments to hold in the presence of the generalized oracle as well. Thus, we can separate PRFS and QCCC commitments.

3 Preliminaries

We denote the security parameter by λ. We assume that the reader is familiar with the fundamentals of quantum computing covered in [NC10].

3.1 Notation

- We use $[n]$ to denote $\{1,\dots,n\}$ and $[0:n]$ to denote $\{0,1,\dots,n\}$.
- For any finite set T and any integer $0\leq k\leq |T|$, we denote by $\binom{T}{k}$ the set of all k-size subsets of T.
- For any finite set T, we use the notation $x\leftarrow T$ to indicate that x is sampled uniformly from T.
- We denote by S_t the symmetric group of degree t.
- For any set A and $t\in\mathbb{N}$, we denote by A^t the t-fold Cartesian product of A.
- For $\sigma\in S_t$ and $\mathbf{v}=(v_1,\dots,v_t)$, we define $\sigma(\mathbf{v}):=(v_{\sigma(1)},\dots,v_{\sigma(t)})$.
- We denote by $\mathcal{D}(H)$ the set of density matrices in the Hilbert space H.
- Let $\rho_{AB}\in\mathcal{D}(H_A\otimes H_B)$, by $\mathrm{Tr}_B(\rho_{AB})\in\mathcal{D}(H_A)$ we denote the reduced density matrix by taking partial trace over B.
- We denote by $\mathsf{TD}(\rho,\rho'):=\frac{1}{2}\|\rho-\rho'\|_1$ the trace distance between quantum states ρ,ρ', where $\|X\|_1=\mathrm{Tr}\left(\sqrt{X^\dagger X}\right)$ denotes the trace norm.
- For any matrices A,B, we write $A\preceq B$ to indicate that $B-A$ is positive semi-definite.
- For any Hermitian matrix O, the trace norm of O has the following variational definition:

$$\|O\|_1=\max_{-I\preceq M\preceq I}\mathrm{Tr}(MO).$$

  Furthermore, if $\mathrm{Tr}(O)=0$ then $\|O\|_1=2\cdot\max_{0\preceq M\preceq I}\mathrm{Tr}(MO)$.
- We denote the Haar measure over n qubits by $\mathcal{H}_n$.
- For any matrix $M_{\mathsf{AB}}=\sum_{i,j,k,\ell}\alpha_{ijk\ell}|i\rangle\langle j|_{\mathsf{A}}\otimes|k\rangle\langle\ell|_{\mathsf{B}}$ on registers (A,B), by $M_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}$ we denote its *partial transpose* with respect to register B, i.e., $M_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}=\sum_{i,j,k,\ell}\alpha_{ijk\ell}|i\rangle\langle j|_{\mathsf{A}}\otimes|\ell\rangle\langle k|_{\mathsf{B}}$.[10]

[9] Note that since the adversary does not need to be efficient, as long as they have the description of this oracle, they can post-select on the transcript.

[10] Note that the (partial) transpose operation needs to be defined with respect to to an orthogonal basis. Throughout this work, it is always defined with respect to to the computational basis.

3.2 Common Haar State Model

The Common Haar State (CHS) model is related to the Common Reference Quantum State (CRQS) model [MNY23]. In this model, all parties receive polynomially many copies of a *single* quantum state sampled from the Haar distribution. Recently, another work of Chen et.al. [CCS24] studied a similar model called the Common Haar Random State (CHRS) model. In the CHRS model, every party receives polynomially many copies of *polynomially many* i.i.d. Haar states.

We define another variant of the CHS model called the *Keyed* Common Haar State Model. In this model, all parties (once the security parameter is set to λ) have access to the oracle (called the *Keyed* Common Haar State Oracle) $G^\lambda := \{G_k\}_{k\in\{0,1\}^\lambda}$ as follows. For every $k \in \{0,1\}^\lambda$, the oracle G_k is a Haar isometry that maps any state $|\psi\rangle$ to $|\psi\rangle|\vartheta_k\rangle$, where $|\vartheta_k\rangle$ is a Haar state of length $n(\lambda) = \omega(\log(\lambda))$.

While the above variant is harder to instantiate (hence not useful for constructions), is a natural candidate for black-box separations as seen is Section 9.

3.2.1 Pseudorandom State (PRS) Generators in the CHS model

Definition 3.1 (Statistically secure (λ, n, ℓ)-pseudorandom state generators in the CHS model)**.** *We say that a QPT algorithm G is a* statistically secure (λ, n, ℓ)-pseudorandom state generator (PRSG) *in the CHS model if the following holds:*

- ***State Generation**: For any $\lambda \in \mathbb{N}$ and $k \in \{0,1\}^\lambda$, the algorithm G_k (where G_k denotes $G(k,\cdot)$) is a quantum channel such that for every $n(\lambda)$-qubit state $|\vartheta\rangle$,*

$$G_k(|\vartheta\rangle\langle\vartheta|) = |\vartheta_k\rangle\langle\vartheta_k|,$$

  for some $n(\lambda)$-qubit state $|\vartheta_k\rangle$. We sometimes write $G_k(|\vartheta\rangle)$ for brevity.[11]

- ***ℓ-copy Pseudorandomness**: For any polynomial $t(\cdot)$ and any non-uniform, unbounded adversary $A = \{A_\lambda\}_{\lambda\in\mathbb{N}}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that:*

$$\left| \Pr_{\substack{k\leftarrow\{0,1\}^\lambda \\ |\vartheta\rangle\leftarrow\mathcal{H}_{n(\lambda)}}} \left[A_\lambda\left(G_k(|\vartheta\rangle)^{\otimes\ell(\lambda)} \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t(\lambda)}\right) = 1\right] - \Pr_{\substack{|\varphi\rangle\leftarrow\mathcal{H}_{n(\lambda)} \\ |\vartheta\rangle\leftarrow\mathcal{H}_{n(\lambda)}}} \left[A_\lambda\left(|\varphi\rangle\langle\varphi|^{\otimes\ell(\lambda)} \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t(\lambda)}\right) = 1\right] \right| \leq \mathsf{negl}(\lambda).$$

If G satisfies ℓ-copy pseudorandomness for every polynomial $\ell(\cdot)$ then we drop ℓ from the notation and simply denote it to be a (λ, n)-PRSG.

We define a stronger definition below called *multi-key ℓ-copy PRS generators*. Looking ahead, our construction of PRS in Section 4.2 satisfies this definition.

Definition 3.2 (Multi-key statistically secure (λ, n, ℓ)-pseudorandom state generators in the CHS model)**.** *We say that a QPT algorithm G is a* multi-key statistically secure (λ, n, ℓ)-pseudorandom state generator *in the CHS model if the following holds:*

[11] More generally, the generation algorithm could take multiple copies of the common Haar state as input or output a state of different size compared to the common Haar state. Here, we focus on a restricted class of generators that only require a single copy of the common Haar state as input, and the output of the generator matches the size of the common Haar states.

- ***State Generation**: For any $\lambda \in \mathbb{N}$ and $k \in \{0,1\}^\lambda$, the algorithm G_k (where G_k denotes $G(k,\cdot)$) is a quantum channel such that for every $n(\lambda)$-qubit state $|\vartheta\rangle$,*

$$G_k(|\vartheta\rangle\langle\vartheta|) = |\vartheta_k\rangle\langle\vartheta_k|,$$

for some $n(\lambda)$-qubit state $|\vartheta_k\rangle$. We sometimes write $G_k(|\vartheta\rangle)$ for brevity.

- ***Multi-key ℓ-copy Pseudorandomness**: For any polynomial $t(\cdot)$, $p(\cdot)$ and any non-uniform, unbounded adversary $A = \{A_\lambda\}_{\lambda\in\mathbb{N}}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that:*

$$\left| \Pr_{\substack{k_1,\ldots,k_{p(\lambda)}\leftarrow\{0,1\}^\lambda \\ |\vartheta\rangle\leftarrow\mathcal{H}_{n(\lambda)}}} \left[A_\lambda \left(\bigotimes_{i=1}^{p(\lambda)} G_{k_i}(|\vartheta\rangle)^{\otimes\ell(\lambda)} \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t(\lambda)} \right) = 1 \right] \right.$$
$$\left. - \Pr_{\substack{|\varphi_1\rangle,\ldots,|\varphi_{p(\lambda)}\rangle\leftarrow\mathcal{H}_{n(\lambda)} \\ |\vartheta\rangle\leftarrow\mathcal{H}_{n(\lambda)}}} \left[A_\lambda \left(\bigotimes_{i=1}^{p(\lambda)} |\varphi_i\rangle\langle\varphi_i|^{\otimes\ell(\lambda)} \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t(\lambda)} \right) = 1 \right] \right| \leq \mathsf{negl}(\lambda).$$

If G satisfies multi-key ℓ-copy pseudorandomness for every polynomial $\ell(\cdot)$ then we drop ℓ from the notation and simply denote it to be a multi-key (λ, n)-PRSG.

Remark 3.3. *Note that in the plain model, PRS implies multi-key PRS because the pseudorandom state generator does not share randomness for different keys. It is not clear whether this holds in the CHS model as the different executions of the pseudorandom state generator share the same common Haar state.*

3.2.2 Pseudorandom Function-Like State (PRFS) Generators in the CHS model

Definition 3.4 (Statistical selectively secure (λ, m, n, ℓ)-PRFS generators)**.** *We say that a QPT algorithm G is a* statistical selectively secure (λ, m, n, ℓ)-PRFS generator *in the CHS model if the following holds:*

- ***State Generation**: For any $\lambda \in \mathbb{N}$, $k \in \{0,1\}^\lambda$ and $x \in \{0,1\}^{m(\lambda)}$, where $m(\lambda)$ is the input length, the algorithm $G_{k,x}$ (where $G_{k,x}$ denotes $G(k,x,\cdot)$) is a quantum channel such that for every $n(\lambda)$-qubit state $|\vartheta\rangle$,*

$$G_{k,x}(|\vartheta\rangle\langle\vartheta|) = |\vartheta_{k,x}\rangle\langle\vartheta_{k,x}|,$$

for some $n(\lambda)$-qubit state $|\vartheta_{k,x}\rangle$. We sometimes write $G_{k,x}(|\vartheta\rangle)$ or $G_k(x,|\vartheta\rangle)$ for brevity.

- ***ℓ-query Selective Security**: For any polynomial $t(\cdot)$, any non-uniform, unbounded adversary $A = \{A_\lambda\}_{\lambda\in\mathbb{N}}$, and any tuple of (possibly repeated) $m(\lambda)$-bit indices $(x_1,\ldots,x_{\ell(\lambda)})$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for all $\lambda \in \mathbb{N}$,*

$$\left| \Pr_{k\leftarrow\{0,1\}^\lambda, |\vartheta\rangle\leftarrow\mathcal{H}_{n(\lambda)}} \left[A_\lambda \left(x_1,\ldots,x_{\ell(\lambda)}, \bigotimes_{i=1}^{\ell(\lambda)} G(k,x_i,|\vartheta\rangle) \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t(\lambda)} \right) = 1 \right] \right.$$
$$\left. - \Pr_{\substack{\forall x\in\{0,1\}^{m(\lambda)},\ |\varphi_x\rangle\leftarrow\mathcal{H}_{n(\lambda)}, \\ |\vartheta\rangle\leftarrow\mathcal{H}_{n(\lambda)}}} \left[A_\lambda \left(x_1,\ldots,x_{\ell(\lambda)}, \bigotimes_{i=1}^{\ell(\lambda)} |\varphi_{x_i}\rangle\langle\varphi_{x_i}| \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t(\lambda)} \right) = 1 \right] \right| \leq \mathsf{negl}(\lambda).$$

If G satisfies ℓ-query selective security for every polynomial $\ell(\cdot)$, we drop ℓ from the notation and say that G is a (λ, m, n)-PRFS generator.

3.2.3 Quantum Commitments in the CHS model

Definition 3.5 (Quantum commitments in the CHS model)**.** *A (non-interactive) quantum commitment scheme in the CHS model is given by a tuple of the committer C and receiver R parameterized by a polynomial $p(\cdot)$, both of which are uniform QPT algorithms. Let $|\vartheta\rangle$ be the $n(\lambda)$-qubit common Haar state. The scheme is divided into two phases: the commit phase, and the reveal phase as follows:*

- *Commit phase: C takes $|\vartheta\rangle^{\otimes p(\lambda)}$ and a bit $b \in \{0,1\}$ to commit as input, generates a quantum state on registers C and R, and sends the register C to R.*
- *Reveal phase: C sends b and the register R to R. R takes $|\vartheta\rangle^{\otimes p(\lambda)}$ and $(b, \mathsf{C}, \mathsf{R})$ given by C as input, and outputs b if it accepts and otherwise outputs $\bot$.*

Definition 3.6 (Poly-copy statistical hiding)**.** *A quantum commitment scheme (C, R) in the CHS model satisfies* poly-copy statistical hiding *if for any non-uniform, unbounded malicious receiver $R^* = \{R^*_\lambda\}_{\lambda\in\mathbb{N}}$, and any polynomial $t(\cdot)$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that*

$$\left|\Pr\left[R^*_\lambda(|\vartheta\rangle^{\otimes t(\lambda)}, \mathrm{Tr}_{\mathsf{R}}(\sigma_{\mathsf{CR}})) = 1 : \substack{|\vartheta\rangle\leftarrow\mathcal{H}_{n(\lambda)},\\ \sigma_{\mathsf{CR}}\leftarrow C_{\mathsf{com}}(|\vartheta\rangle^{\otimes p(\lambda)},0)}\right]\right.$$
$$\left. - \Pr\left[R^*_\lambda(|\vartheta\rangle^{\otimes t(\lambda)}, \mathrm{Tr}_{\mathsf{R}}(\sigma_{\mathsf{CR}})) = 1 : \substack{|\vartheta\rangle\leftarrow\mathcal{H}_{n(\lambda)},\\ \sigma_{\mathsf{CR}}\leftarrow C_{\mathsf{com}}(|\vartheta\rangle^{\otimes p(\lambda)},1)}\right]\right| \le \mathsf{negl}(\lambda),$$

where C_{com} is the commit phase of C.

Definition 3.7 (Statistical sum-binding)**.** *A quantum commitment scheme (C, R) in the CHS model satisfies* statistical sum-binding *if the following holds. For any pair of non-uniform, unbounded malicious senders C^*_0 and C^*_1 that take $|\vartheta\rangle^{\otimes T(\lambda)}$ for arbitrary large $T(\cdot)$ as input and work in the same way in the commit phase, if we let p_b to be the probability that R accepts the revealed bit b in the interaction with C^*_b for $b \in \{0,1\}$, then we have*

$$p_0 + p_1 \le 1 + \mathsf{negl}(\lambda).$$

3.3 Symmetric Subspaces, Type States, and Haar States

The proofs of facts and lemmas stated in this subsection can be found in [Har13]. Let $\mathbf{v} = (v_1, \ldots, v_t) \in A^t$ for some finite set A. Let $|A| = N$. Define $\mathsf{type}(\mathbf{v}) \in [0:t]^N$ to be the *type vector* such that the i^{th} entry of $\mathsf{type}(\mathbf{v})$ equals the number of occurrences of $i \in [N]$ in $\mathbf{v}$.[12] In this work, by $T \in [0:t]^N$ we implicitly assume that $\sum_{i\in[N]} T_i = t$. For $T \in [0:t]^N$, we denote by $\mathsf{mset}(T)$ the *multiset* uniquely determined by T. That is, the multiplicity of $i \in \mathsf{mset}(T)$ equals T_i for all $i \in [N]$. We write $T \leftarrow [0:t]^N$ to mean sampling T uniformly from $[0:t]^N$ conditioned on $\sum_{i\in[N]} T_i = t$. We write $\mathbf{v} \in T$ to mean $\mathbf{v} \in A^t$ satisfies $\mathsf{type}(\mathbf{v}) = T$.

In this work, we will focus on *collision-free* types T which satisfy $T_i \in \{0,1\}$ for all $i \in [N]$. A collision-free type T can be naturally treated as a *set* and we write $\mathbf{v} \leftarrow T$ to mean sampling a uniform $\mathbf{v}$ conditioned on $\mathsf{type}(\mathbf{v}) = T$.

Definition 3.8 (Type states)**.** *Let $T \in [0:t]^N$, we define the* type states*:*

$$|T\rangle := \sqrt{\frac{\prod_{i\in[N]} T_i!}{t!}} \sum_{\mathbf{v}\in T} |\mathbf{v}\rangle.$$

If T is collision-free, then it can be simplified to

$$|T\rangle = \frac{1}{\sqrt{t!}} \sum_{\mathbf{v}\in T} |\mathbf{v}\rangle.$$

[12] We identify $[0:t]^N$ as $[0:t]^A$.

Furthermore, it has the following useful expression

$$|T\rangle\langle T| = \frac{1}{t!}\sum_{\mathbf{v},\mathbf{u}\in T}|\mathbf{v}\rangle\langle\mathbf{u}| = \mathop{\mathbb{E}}_{\mathbf{v}\leftarrow T}\left[\sum_{\sigma\in S_t}|\mathbf{v}\rangle\langle\sigma(\mathbf{v})|\right]. \tag{1}$$

Lemma 3.9 (Average of copies of Haar-random states)**.** *For all $N, t \in \mathbb{N}$, we have*

$$\mathop{\mathbb{E}}_{|\vartheta\rangle\leftarrow\mathcal{H}(\mathbb{C}^N)}|\vartheta\rangle\langle\vartheta|^{\otimes t} = \mathop{\mathbb{E}}_{T\leftarrow[0:t]^N}|T\rangle\langle T|.$$

3.4 Quantum Black-Box Reductions

We recall the definition of fully black-box reductions [RTV04; BBF13] and their quantum analogue. The definitions below are taken verbatim from [HY20].

Definition 3.10 (Quantum primitives)**.** *A quantum primitive $\mathcal{P}$ is a pair $(\mathcal{F}_\mathcal{P}, \mathcal{R}_\mathcal{P})$, where $\mathcal{F}_\mathcal{P}$ is a set of quantum algorithms $\mathcal{I}$, and $\mathcal{R}_\mathcal{P}$ is a relation over pairs $(\mathcal{I}, \mathcal{A})$ of quantum algorithms $\mathcal{I} \in \mathcal{F}_\mathcal{P}$ and $\mathcal{A}$. A quantum algorithm $\mathcal{I}$ implements $\mathcal{P}$ or is an implementation of $\mathcal{P}$ if $\mathcal{I} \in \mathcal{F}_\mathcal{P}$. If $\mathcal{I} \in \mathcal{F}_\mathcal{P}$ is efficient, then $\mathcal{I}$ is an efficient implementation of $\mathcal{P}$. A quantum algorithm $\mathcal{A}$ $\mathcal{P}$-breaks $\mathcal{I} \in \mathcal{F}_\mathcal{P}$ if $(\mathcal{I}, \mathcal{A}) \in \mathcal{R}_\mathcal{P}$. A secure implementation of $\mathcal{P}$ is an implementation $\mathcal{I}$ of $\mathcal{P}$ such that no efficient quantum algorithm $\mathcal{P}$-breaks $\mathcal{I}$. The primitive $\mathcal{P}$ quantumly exists if there exists an efficient and secure implementation of $\mathcal{P}$.*

Definition 3.11 (Quantum primitives relative to oracle)**.** *Let $\mathcal{P} = (\mathcal{F}_\mathcal{P}, \mathcal{R}_\mathcal{P})$ be a quantum primitive, and O be a quantum oracle. An oracle quantum algorithm $\mathcal{I}$ implements $\mathcal{P}$ relative to O or is an implementation of $\mathcal{P}$ relative to O if $\mathcal{I}^O \in \mathcal{F}_\mathcal{P}$. If $\mathcal{I}^O \in \mathcal{F}_\mathcal{P}$ is efficient, then $\mathcal{I}$ is an efficient implementation of $\mathcal{P}$ relative to O. A quantum algorithm $\mathcal{A}$ $\mathcal{P}$-breaks $\mathcal{I} \in \mathcal{F}_\mathcal{P}$ relative to O if $(I^O, \mathcal{A}^O) \in \mathcal{R}_\mathcal{P}$. A secure implementation of $\mathcal{P}$ is an implementation $\mathcal{I}$ of $\mathcal{P}$ relative to O such that no efficient quantum algorithm $\mathcal{P}$-breaks $\mathcal{I}$ relative to O. The primitive $\mathcal{P}$ quantumly exists relative to O if there exists an efficient and secure implementation of $\mathcal{P}$ relative to O.*

Definition 3.12 (Quantum fully black-box reductions)**.** *A pair (C, S) of efficient oracle quantum algorithms is a* quantum fully-black-box reduction *from a quantum primitive $\mathcal{P} = (\mathcal{F}_\mathcal{P}, \mathcal{R}_\mathcal{P})$ to a quantum primitive $\mathcal{Q} = (\mathcal{F}_\mathcal{Q}, \mathcal{R}_\mathcal{Q})$ if the following two conditions are satisfied:*

1. ***(Correctness.)*** *For every implementation $\mathcal{I} \in \mathcal{F}_\mathcal{Q}$, we have $C^\mathcal{I} \in \mathcal{F}_\mathcal{P}$.*
2. ***(Security.)*** *For every implementation $\mathcal{I} \in \mathcal{F}_\mathcal{Q}$ and every quantum algorithm $\mathcal{A}$, if $\mathcal{A}$ $\mathcal{P}$-breaks $C^\mathcal{I}$, then $S^{\mathcal{A},\mathcal{I}}$ $\mathcal{Q}$-breaks $\mathcal{I}$.*

4 Warmup: Statistical Stretch PRS Generators in the CHS model

We present a construction of multi-key PRS generator with statistical security in the CHS model.

Theorem 4.1. *There exists a multi-key (λ, n, ℓ)-statistical PRS generator in the CHS model, where $n \geq \lambda$ and $\ell = O(\lambda/\log(\lambda)^{1+\varepsilon})$ for any constant $\varepsilon > 0$.*

The proof can be found in Section 4.2. Later, we prove the optimality of our construction in Section 4.3. Specifically, we show that any (λ, n, ℓ)-statistical PRS generator cannot simultaneously satisfy $n = \omega(\log(\lambda))$ and $\ell = \Omega(\lambda/\log(\lambda))$.

4.1 Useful Lemmas

At a high level, the proof follows the template of [AGQY22; AGKL23]: we do the analysis in the symmetric subspace. First, we identify a nice property of type vectors such that (1) a randomly sampled type satisfies this property with overwhelming probability and (2) the PRS generation algorithm behaves well on every type state having this property. We identify these type vectors as *ℓ-fold collision-free* types (which are a generalization of distinct types [AGQY22; AGKL23]).

Definition 4.2 (ℓ-fold n-prefix collision-free types)**.** *Let $n, m, t, \ell \in \mathbb{N}$ such that $t \geq \ell$ and $T \in [0:t]^{2^{n+m}}$ is a type vector. We say that T is* ℓ-fold n-prefix collision-free *if for all pairs of ℓ-subsets[13] $\mathcal{S}, \mathcal{T} \subseteq \mathsf{mset}(T)$, the first n bits of $\bigoplus_{x\in\mathcal{S}} x \in \{0,1\}^{n+m}$ is identical to that of $\bigoplus_{y\in\mathcal{T}} y \in \{0,1\}^{n+m}$ if and only if $\mathcal{S} = \mathcal{T}$. We define $\mathcal{I}^{(\ell)}_{n,m}(t) := \{T \in [0:t]^{2^{n+m}} : T$ is ℓ-fold n-prefix collision-free$\}$ as the set of all ℓ-fold n-prefix collision-free type vectors.*

When $t > \ell$, one can easily verify that ℓ-fold n-prefix collision-freeness implies the standard collision-freeness. Also note that when $t > 2\ell$, ℓ-fold n-prefix collision-freeness implies i-fold n-prefix collision-freeness for all $i \leq \ell$.

Next, we show that a random type is ℓ-fold n-prefix collision-free with high probability.

Lemma 4.3. $\Pr_{T\leftarrow[0:t]^{2^{n+m}}}[T \in \mathcal{I}^{(\ell)}_{n,m}(t)] = 1 - O(t^{2\ell}/(2^n - 2\ell))$.

Proof. First, sampling $T \leftarrow [0:t]^{2^{n+m}}$ uniformly is $O(t^2/2^{n+m})$-close to sampling a uniform collision-free T from $[0:t]^{2^{n+m}}$ by the collision bound.

Furthermore, sampling a uniform collision-free T from $[0:t]^{2^{n+m}}$ is equivalent to sampling t elements $x_1, x_2, \ldots, x_t$ one by one from $\{0,1\}^{n+m}$ conditioned on them being distinct and setting T such that $\mathsf{mset}(T) = \{x_1, \ldots, x_t\}$. Hence, it suffices to show that sampling t elements $x_1, x_2, \ldots, x_t$ one by one from $\{0,1\}^{n+m}$ conditioned on them being distinct results in an ℓ-fold n-prefix collision-free set with probability $1 - O(t^{2\ell}/2^n)$.

For any two distinct ℓ-subsets of indices $\mathcal{S} \neq \mathcal{T} \subseteq [t]$, let $\mathsf{Bad}_{\mathcal{S},\mathcal{T}}$ denote the event that the first n bits of $\bigoplus_{i\in\mathcal{S}} x_i$ is the same as that of $\bigoplus_{j\in\mathcal{T}} x_j$. Then the following holds:

$$\Pr\left[\mathsf{Bad}_{\mathcal{S},\mathcal{T}} : \substack{x_1,x_2,\ldots,x_t\leftarrow\{0,1\}^{n+m} \\ x_1,x_2,\ldots,x_t \text{ are distinct}}\right] = O(1/(2^n - 2\ell)).$$

This is because we can first sample $|\mathcal{S} \cup \mathcal{T}| - 1$ elements (in $\mathcal{S} \cup \mathcal{T}$) except one with indices in $\mathcal{S} \setminus \mathcal{T}$. Then $\mathsf{Bad}_{\mathcal{S},\mathcal{T}}$ occurs only if the first n bits of the last sample is equal to the first n bits of the bitwise XOR of all other elements in $\mathcal{S}$ with all elements in $\mathcal{T}$, which happens with probability at most $O(1/(2^n - 2\ell))$.

By a union bound, we have $T \in \mathcal{I}^{(\ell)}_{n,m}(t)$ with probability at least $1 - \left(O(t^2/2^{n+m}) + \binom{t}{\ell}^2 \cdot O(1/(2^n - 2\ell))\right) = 1 - O(t^{2\ell}/(2^n - 2\ell))$. □

Finally, the following two lemmas show that applying random Pauli-Z on any ℓ-fold n-prefix collision-free type state is equivalent to a "classical" probabilistic process[14].

Lemma 4.4. *For any $\mathbf{v} \in \{0,1\}^{(n+m)(t+\ell)}$ such that $\mathsf{type}(\mathbf{v}) \in \mathcal{I}^{(\ell)}_{n,m}(t+\ell)$ and $\sigma \in S_{t+\ell}$, define*

$$A_{\mathbf{v},\sigma} := \mathop{\mathbb{E}}_{k\leftarrow\{0,1\}^n}\left[\left(\left(Z^k \otimes I_m\right)^{\otimes\ell} \otimes I_{n+m}^{\otimes t}\right)|\mathbf{v}\rangle\langle\sigma(\mathbf{v})|\left(\left(Z^k \otimes I_m\right)^{\otimes\ell} \otimes I_{n+m}^{\otimes t}\right)\right].$$

Then $A_{\mathbf{v},\sigma} = |\mathbf{v}\rangle\langle\sigma(\mathbf{v})|$ if σ maps $[\ell]$ to $[\ell]$; otherwise, $A_{\mathbf{v},\sigma} = 0$.

[13] Here we allow the subsets to contain duplicate elements.

[14] We say that this is a "classical" probabilistic process because we can write the resulting density matrix as direct sum of matrices with classical descriptions with weights chosen by a completely classical process. This means that we can simualte this process by first doing a completely classical sampling process followed by a state preparation.

Proof. Suppose $\mathbf{v} = (v_1||w_1, \ldots, v_{t+\ell}||w_{t+\ell}) \in \{0,1\}^{(n+m)(t+\ell)}$ with $v_i \in \{0,1\}^n$ and $w_i \in \{0,1\}^m$ for all $i \in [t]$. First, a direct calculation yields:

$$\left(\left(Z^k \otimes I_m\right)^{\otimes \ell} \otimes I_{n+m}^{\otimes t}\right) |\mathbf{v}\rangle\langle\sigma(\mathbf{v})| \left(\left(Z^k \otimes I_m\right)^{\otimes \ell} \otimes I_{n+m}^{\otimes t}\right) = (-1)^{\langle k, \bigoplus_{i=1}^{\ell}(v_i \oplus v_{\sigma(i)})\rangle} |\mathbf{v}\rangle\langle\sigma(\mathbf{v})|.$$

Therefore, after averaging over k,

$$A_{\mathbf{v},\sigma} = \mathop{\mathbb{E}}_{k \leftarrow \{0,1\}^n} \left[(-1)^{\langle k, \bigoplus_{i=1}^{\ell}(v_i \oplus v_{\sigma(i)})\rangle}\right] |\mathbf{v}\rangle\langle\sigma(\mathbf{v})| = \begin{cases} |\mathbf{v}\rangle\langle\sigma(\mathbf{v})| & \text{if } \bigoplus_{i=1}^{\ell}(v_i \oplus v_{\sigma(i)}) = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Since $\mathsf{type}(\mathbf{v}) \in \mathcal{I}_{n,m}^{(\ell)}(t+\ell)$, the condition $\bigoplus_{i=1}^{\ell} v_i = \bigoplus_{i=1}^{\ell} v_{\sigma(i)}$ holds if and only if the two sets $\{1, 2, \ldots, \ell\}$ and $\{\sigma(1), \sigma(2), \ldots, \sigma(\ell)\}$ are identical. □

The following lemma lies at the technical heart of this section. It states that the action of applying random Z^k on ℓ-fold n-prefix collision-free types T[15] has the following "classical" probabilistic interpretation: the output is identically distributed to first uniformly sampling an ℓ-subset X from T and then generating $|X\rangle\langle X| \otimes |T \setminus X\rangle\langle T \setminus X|$.

Lemma 4.5. *For any $T \in \mathcal{I}_{n,m}^{(\ell)}(t+\ell)$,*

$$\mathop{\mathbb{E}}_{k \leftarrow \{0,1\}^n} \left[\left(\left(Z^k \otimes I_m\right)^{\otimes \ell} \otimes I_{n+m}^{\otimes t}\right) |T\rangle\langle T| \left(\left(Z^k \otimes I_m\right)^{\otimes \ell} \otimes I_{n+m}^{\otimes t}\right)\right] = \mathop{\mathbb{E}}_{X \leftarrow \binom{T}{\ell}} \left[|X\rangle\langle X| \otimes |T \setminus X\rangle\langle T \setminus X|\right].$$

Proof. We first use the expression in Equation (1) on the left-hand side:

$$LHS = \mathop{\mathbb{E}}_{\mathbf{v} \leftarrow T} \left[\sum_{\sigma \in S_t} \mathop{\mathbb{E}}_{k \leftarrow \{0,1\}^n} \left[\left(\left(Z^k \otimes I_m\right)^{\otimes \ell} \otimes I_{n+m}^{\otimes t}\right) |\mathbf{v}\rangle\langle\sigma(\mathbf{v})| \left(\left(Z^k \otimes I_m\right)^{\otimes \ell} \otimes I_{n+m}^{\otimes t}\right)\right]\right]. \tag{2}$$

Then from the previous lemma (Lemma 4.4)

$$\begin{aligned}
(2) &= \mathop{\mathbb{E}}_{\mathbf{v} \leftarrow T} \left[\sum_{\sigma_1 \in S_\ell, \sigma_2 \in S_t} |\mathbf{v}\rangle\langle\sigma_1 \circ \sigma_2(\mathbf{v})|\right] \\
&= \mathop{\mathbb{E}}_{\mathbf{v} \leftarrow T} \left[\sum_{\sigma_1 \in S_\ell} |\mathbf{v}_{[1:\ell]}\rangle\langle\sigma_1(\mathbf{v}_{[1:\ell]})| \otimes \sum_{\sigma_2 \in S_t} |\mathbf{v}_{[\ell+1:\ell+t]}\rangle\langle\sigma_2(\mathbf{v}_{[\ell+1:\ell+t]})|\right] \\
&= \mathbb{E}\left[\sum_{\sigma_1 \in S_\ell} |\mathbf{v}_1\rangle\langle\sigma_1(\mathbf{v}_1)| \otimes \sum_{\sigma_2 \in S_t} |\mathbf{v}_2\rangle\langle\sigma_2(\mathbf{v}_2)| : \begin{smallmatrix} X \leftarrow \binom{T}{\ell}, \\ \mathbf{v}_1 \leftarrow X, \\ \mathbf{v}_2 \leftarrow T \setminus X \end{smallmatrix}\right] \\
&= \mathop{\mathbb{E}}_{X \leftarrow \binom{T}{\ell}} \left[|X\rangle\langle X| \otimes |T \setminus X\rangle\langle T \setminus X|\right].
\end{aligned}$$

For the first equality, we use Lemma 4.4 and decompose $\sigma = \sigma_1 \circ \sigma_2$ for some σ_1, σ_2 such that $\sigma_1(x) = x$ for all $x \in \{\ell+1, \ell+2, \cdots, \ell+t\}$ and $\sigma_2(y) = y$ for all $y \in \{1, 2, \cdots, \ell\}$. Since all $\ell+1, \ell+2, \cdots, \ell+t$ are fixed points of σ_1, we can view it as an element in S_ℓ. Similarly, we view $\sigma_2(y)$ as an element in S_t. The second equality follows by denoting the first ℓ part of $\mathbf{v}$ by $\mathbf{v}_{[1:\ell]}$ and the last t part of $\mathbf{v}$ by $\mathbf{v}_{[\ell+1:\ell+t]}$. The third equality holds because sampling a tuple $\mathbf{v}$ from T is equivalent to sampling an ℓ-subset X from T followed by ordering to elements in X and $T \setminus X$. □

[15] Since T is collision-free, we will treat it as a set.

4.2 Construction

In this section, we assume that the length of the common Haar state satisfies $n = n(\lambda) \geq \lambda$ for all $\lambda \in \mathbb{N}$. We define the construction as follows: on input $k \in \{0,1\}^\lambda$ and a single copy of the common Haar state $|\vartheta\rangle$,

$$G_k(|\vartheta\rangle) := (Z^k \otimes I_{n-\lambda})|\vartheta\rangle.$$

Lemma 4.6 (ℓ-copy pseudorandomness)**.** *Let G be as defined above. Let*

$$\rho := \mathop{\mathbb{E}}_{\substack{k\leftarrow\{0,1\}^\lambda \\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[G_k(|\vartheta\rangle)^{\otimes\ell} \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t}\right] \text{ and } \sigma := \mathop{\mathbb{E}}_{\substack{|\varphi\rangle\leftarrow\mathcal{H}_n \\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[|\varphi\rangle\langle\varphi|^{\otimes\ell} \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t}\right].$$

Then $\mathsf{TD}(\rho,\sigma) = O\left(\frac{(\ell+t)^{2\ell}}{2^\lambda}\right)$.

Proof. We prove this via a hybrid argument:

Hybrid 1. Sample $T \leftarrow [0:\ell+t]^{2^n}$. Sample $k \leftarrow \{0,1\}^\lambda$. Output $((Z^k \otimes I_{n-\lambda})^{\otimes\ell} \otimes I_n^{\otimes t})|T\rangle$.

Hybrid 2. Sample $T \leftarrow [0:\ell+t]^{2^n}$ uniformly conditioned on $T \in \mathcal{I}^{(\ell)}_{\lambda,n-\lambda}(\ell+t)$. Sample $k \leftarrow \{0,1\}^\lambda$. Output $((Z^k \otimes I_{n-\lambda})^{\otimes\ell} \otimes I_n^{\otimes t})|T\rangle$.

Hybrid 3: Sample $T \leftarrow [0:\ell+t]^{2^n}$ uniformly conditioned on $T \in \mathcal{I}^{(\ell)}_{\lambda,n-\lambda}(\ell+t)$. Sample a uniform ℓ-subset T_1 from T. Output $|T_1\rangle \otimes |T \setminus T_1\rangle$.

Hybrid 4. Sample $T \leftarrow [0:\ell+t]^{2^n}$. Sample a uniform ℓ-subset T_1 from T.[16] Output $|T_1\rangle \otimes |T \setminus T_1\rangle$.

Hybrid 5. Sample a collision-free T from $[0:\ell+t]^{2^n}$. Sample a uniform ℓ-subset T_1 from T. Output $|T_1\rangle \otimes |T \setminus T_1\rangle$.

Hybrid 6. Sample a uniform collision-free T_1 from $[0:\ell]^{2^n}$. Sample a uniform collision-free T_2 from $[0:t]^{2^n}$ conditioned on T_1 and T_2 have no common elements. Output $|T_1\rangle \otimes |T_2\rangle$.

Hybrid 7. Sample a uniform collision-free T_1 from $[0:\ell]^{2^n}$. Sample a uniform collision-free T_2 from $[0:t]^{2^n}$. Output $|T_1\rangle \otimes |T_2\rangle$.

Hybrid 8. Sample $T_1 \leftarrow [0:\ell]^{2^n}$. Sample $T_2 \leftarrow [0:t]^{2^n}$. Output $|T_1\rangle \otimes |T_2\rangle$.

Indistinuishability of Hybrids.

- By Lemma 4.3, the trace distance between Hybrid 1 and Hybrid 2 is $O((t+\ell)^{2\ell}/2^\lambda)$.
- From Lemma 4.5, the output of Hybrid 2 is

$$\mathop{\mathbb{E}}_{\substack{T\leftarrow[0:\ell+t]^{2^n}: \\ T\in\mathcal{I}^{(\ell)}_{\lambda,n-\lambda}(\ell+t)}} \mathop{\mathbb{E}}_{T_1\leftarrow\binom{T}{\ell}} \left[|T_1\rangle\langle T_1| \otimes |T \setminus T_1\rangle\langle T \setminus T_1|\right].$$

  Hence, Hybrid 2 is equivalent to Hybrid 3.
- Again by Lemma 4.3, the trace distance between Hybrid 3 and Hybrid 4 is $O((t+\ell)^{2\ell}/2^\lambda)$.

[16] Since T might have collisions, T_1 is allowed to contain duplicate elements.

- The trace distance between Hybrid 4 and Hybrid 5 is $O((t+\ell)^2/2^n)$ by the collision bound.
- Hybrid 5 and Hybrid 6 are equivalent.
- The trace distance between Hybrid 6 and Hybrid 7 is $O(t\ell/2^n)$.
- Finally, the trace distance between Hybrid 7 and Hybrid 8 is $O((t^2+\ell^2)/2^n)$ by the collision bound.

This completes the proof. □

In the following, we show that our construction also satisfies multi-key ℓ-copy pseudorandomness using Lemma 4.6.

Lemma 4.7 (Multi-key ℓ-copy pseudorandomness)**.** *Let G be defined as above. Let*

$$\rho := \bigotimes_{i=1}^{p} \mathop{\mathbb{E}}_{|\varphi_i\rangle\leftarrow\mathcal{H}_n} \left[|\varphi_i\rangle\langle\varphi_i|^{\otimes\ell}\right] \otimes \mathop{\mathbb{E}}_{|\vartheta\rangle\leftarrow\mathcal{H}_n} \left[|\vartheta\rangle\langle\vartheta|^{\otimes t}\right] \text{ and } \sigma := \mathop{\mathbb{E}}_{|\vartheta\rangle\leftarrow\mathcal{H}_n} \left[\bigotimes_{i=1}^{p} \mathop{\mathbb{E}}_{k_i\leftarrow\{0,1\}^\lambda} \left[G_{k_i}(|\vartheta\rangle)^{\otimes\ell}\right] \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t}\right].$$

Then $\mathsf{TD}(\rho,\sigma) = O\left(\frac{p\cdot(p\ell+t)^{2\ell}}{2^\lambda}\right)$.

Proof. For $j = 0, 1, \ldots, p$, we define the following (hybrid) density matrices:[17]

$$\xi_j := \bigotimes_{i=1}^{j} \mathop{\mathbb{E}}_{|\varphi_i\rangle\leftarrow\mathcal{H}_n} \left[|\varphi_i\rangle\langle\varphi_i|^{\otimes\ell}\right] \otimes \mathop{\mathbb{E}}_{|\vartheta\rangle\leftarrow\mathcal{H}_n} \left[\bigotimes_{i=j+1}^{p} \mathop{\mathbb{E}}_{k_i\leftarrow\{0,1\}^\lambda} \left[G_{k_i}(|\vartheta\rangle)^{\otimes\ell}\right] \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t}\right].$$

We will complete the poof by showing that $\mathsf{TD}(\xi_j,\xi_{j+1}) = O\left(\frac{((p-j)\cdot\ell+t)^{2\ell}}{2^\lambda}\right)$ for $j = 0, 1, \ldots, p-1$. By the property that $\mathsf{TD}(A\otimes X, A\otimes Y) = \mathsf{TD}(X,Y)$, the trace distance between ξ_j and ξ_{j+1} is identical to that of

$$\xi'_j := \mathop{\mathbb{E}}_{|\vartheta\rangle\leftarrow\mathcal{H}_n} \left[\bigotimes_{i=j+1}^{p} \mathop{\mathbb{E}}_{k_i\leftarrow\{0,1\}^\lambda} [G_{k_i}(|\vartheta\rangle)^{\otimes\ell}] \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t}\right]$$

$$\xi'_{j+1} := \mathop{\mathbb{E}}_{|\varphi_{j+1}\rangle\leftarrow\mathcal{H}_n} \left[|\varphi_{j+1}\rangle\langle\varphi_{j+1}|^{\otimes\ell}\right] \otimes \mathop{\mathbb{E}}_{|\vartheta\rangle\leftarrow\mathcal{H}_n} \left[\bigotimes_{i=j+2}^{p} \mathop{\mathbb{E}}_{k_i\leftarrow\{0,1\}^\lambda} [G_{k_i}(|\vartheta\rangle)^{\otimes\ell}] \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t}\right].$$

By the monotonicity of trace distance (i.e., $\mathsf{TD}(\mathcal{E}(X),\mathcal{E}(Y)) \le \mathsf{TD}(X,Y)$ for any quantum channel $\mathcal{E}$) and setting $\mathcal{E} := \bigotimes_{i=j+2}^{p} \mathbb{E}_{k_i\leftarrow\{0,1\}^\lambda}[G_{k_i}(\cdot)^{\otimes\ell}]$,[18] we have

$$\begin{aligned}
&\mathsf{TD}(\xi'_j,\xi'_{j+1}) \le \\
&\mathsf{TD}\left(\mathop{\mathbb{E}}_{\substack{k_{j+1}\leftarrow\{0,1\}^\lambda,\\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[G_{k_{j+1}}(|\vartheta\rangle)^{\otimes\ell} \otimes |\vartheta\rangle\langle\vartheta|^{\otimes(p-j-1)\ell+t}\right], \mathop{\mathbb{E}}_{\substack{|\varphi_{j+1}\rangle\leftarrow\mathcal{H}_n,\\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[|\varphi_{j+1}\rangle\langle\varphi_{j+1}|^{\otimes\ell} \otimes |\vartheta\rangle\langle\vartheta|^{\otimes(p-j-1)\ell+t}\right]\right) \\
&= O\left(\frac{((p-j)\ell+t)^{2\ell}}{2^\lambda}\right),
\end{aligned}$$

where the last equality follows from Lemma 4.6. Applying the triangle inequality completes the proof. □

Proof of Theorem 4.1. Our construction is a efficiently-implementable unitary channel and thus satisfies the state generation property. Pseudorandomness follows from Lemma 4.7. □

[17] Similar to proving the output of a classical PRG on polynomial i.i.d uniform keys is computationally indistinguishable from polynomial i.i.d uniform strings, we can construct a security reduction to simulate these hybrids. However, since we are in the information-theoretic setting, we instead calculate their trace distances directly.

[18] The channel $\mathcal{E}$ acts as the identity on unspecified registers.

As a remark, Lemma 4.6 gives a simpler proof of the following theorem regarding the one-wayness of an ensemble of quantum states in [Col23]:

Lemma 4.8 ([Col23, Lemma 5])**.** *Consider the ensemble of states:*

$$\{\rho_x\}_{x\in\{0,1\}^n} = \left\{ \mathop{\mathbb{E}}_{|\psi\rangle\leftarrow\mathcal{H}_n} \left[(Z^x\otimes I^{\otimes m})|\psi\rangle\langle\psi|^{\otimes m+1}(Z^x\otimes I^{\otimes m})\right] \right\}_{x\in\{0,1\}^n}.$$

Then, there is a constant $C>0$, such that, for any POVM $\{M_x\}_{x\in\{0,1\}^n}$,

$$\mathop{\mathbb{E}}_{x\leftarrow\{0,1\}^n} \mathrm{Tr}(M_x\rho_x) = C\cdot\left(\frac{m}{2^n}+\frac{m^7}{2^{3n}}\right)^{\frac{1}{2}}.$$

By setting $\ell=1, t=m, \lambda=n$ in Lemma 4.6, the ensemble of states $\{\rho_x\}_{x\in\{0,1\}^n}$ is pseudorandom, which implies its one-wayness.

In Appendix B, we further give another proof by simplifying the calculation in Lemma 4.8, which may be of independent interest. Moreover, we eliminate the $m^7/2^{3n}$ term.

4.3 Optimality of Our PRSG Construction

In this section, if the PRS generation algorithm uses only *one copy* of the common Haar state, we show that ℓ-copy statistical PRS and multi-key ℓ-copy statistical PRS are impossible for $\ell=\Omega(\lambda/\log(\lambda))$ and $n=\omega(\log(\lambda))$.

Theorem 4.9. *Statistically secure (λ,n,ℓ)-PRS is impossible in the CHS model if (a) the generation algorithm uses only one copy of the common Haar state, (b) $n=\omega(\log(\lambda))$, (c) $\ell=\Omega(\lambda/\log(\lambda))$ and, (d) the length of the common Haar state is $n=\omega(\log(\lambda))$.*

Proof. We provve this by contradiction. Let there is a construction of such PRS G. First, from the state generation requirement of PRS generators, G is a quantum channel that on any key and any pure state, outputs a pure state. Hence, G is either an isometry or a replacement channel (i.e., it outputs a fixed pure state for any input state).[19]

We prove Theorem 4.9 by showing that for $t(\lambda):=\lambda^3$ and $\ell(\lambda):=\lambda/\log(\lambda)$, there exists a (computationally unbounded) adversary A such that

$$\left|\Pr_{\substack{k\leftarrow\{0,1\}^\lambda\\|\vartheta\rangle\leftarrow\mathcal{H}_n}}[A(|\vartheta\rangle\langle\vartheta|^{\otimes t}\otimes G(k,|\vartheta\rangle\langle\vartheta|)^{\otimes\ell})=1] - \Pr_{\substack{|\varphi\rangle\leftarrow\mathcal{H}_n\\|\vartheta\rangle\leftarrow\mathcal{H}_n}}[A(|\vartheta\rangle\langle\vartheta|^{\otimes t}\otimes|\varphi\rangle\langle\varphi|^{\otimes\ell})=1]\right|$$

is non-negligible. For short, we use the following notation:

$$\rho_0 := \mathop{\mathbb{E}}_{k\leftarrow\{0,1\}^\lambda,|\vartheta\rangle\leftarrow\mathcal{H}_n}\left[|\vartheta\rangle\langle\vartheta|^{\otimes t}\otimes G(k,|\vartheta\rangle\langle\vartheta|)^{\otimes\ell}\right]$$

$$\rho_1 := \mathop{\mathbb{E}}_{|\varphi\rangle\leftarrow\mathcal{H}_n,|\vartheta\rangle\leftarrow\mathcal{H}_n}\left[|\vartheta\rangle\langle\vartheta|^{\otimes t}\otimes|\varphi\rangle\langle\varphi|^{\otimes\ell}\right].$$

The adversary A is simple: it performs a binary measurement $\{\Pi, I-\Pi\}$ on input ρ_b for $b\in\{0,1\}$, where Π is the projection onto the eigenspace of ρ_0. The rank of ρ_0 and ρ_1 satisfies

$$\mathrm{rank}(\rho_0)\le 2^\lambda\cdot\binom{2^n+\ell+t-1}{\ell+t} \quad\text{and}\quad \mathrm{rank}(\rho_1)=\binom{2^n+\ell-1}{\ell}\cdot\binom{2^n+t-1}{t}.$$

[19] According to the Stinespring representation, the action of any quantum channel is equivalent to appending auxiliary registers, performing a unitary operation on the enlarged system, and (possibly) taking a partial trace over some registers. For a bipartite entangled state, taking the partial trace over one subsystem results in a mixed state. Hence, after applying a unitary operation, either (1) there is no partial trace and the quantum channel is an isometry, or (2) the registers over which the partial trace is taken are not entangled with other registers, and the quantum channel is a replacement channel.

Now, by construction, we have

$$\Pr_{\substack{k\leftarrow\{0,1\}^\lambda\\ |\vartheta\rangle\leftarrow\mathcal{H}_n}}[A(|\vartheta\rangle\langle\vartheta|^{\otimes t}\otimes G(k,|\vartheta\rangle\langle\vartheta|)^{\otimes\ell})=1]=\mathrm{Tr}(\Pi\rho_0)=\mathrm{Tr}(\rho_0)=1.$$

On the other hand, suppose $\Pi=\sum_{i=1}^{\mathrm{rank}(\rho_0)}|u_i\rangle\langle u_i|$, then

$$\begin{aligned}
&\Pr_{\substack{|\varphi\rangle\leftarrow\mathcal{H}_n\\ |\vartheta\rangle\leftarrow\mathcal{H}_n}}[A(|\vartheta\rangle\langle\vartheta|^{\otimes t}\otimes|\varphi\rangle\langle\varphi|^{\otimes\ell})=1]=\mathrm{Tr}(\Pi\rho_1)\\
&\leq\sum_{i=1}^{\mathrm{rank}(\rho_0)}\frac{1}{\binom{2^n+\ell-1}{\ell}\binom{2^n+t-1}{t}}\cdot\sum_{T_1\in[0:\ell]^{2^n},T_2\in[0:t]^{2^n}}|(\langle T_1|\otimes\langle T_2|)|u_i\rangle|^2\\
&\leq\frac{\mathrm{rank}(\rho_0)}{\binom{2^n+\ell-1}{\ell}\binom{2^n+t-1}{t}}=\frac{\mathrm{rank}(\rho_0)}{\mathrm{rank}(\rho_1)}.
\end{aligned}$$

A direct calculation yields:

$$\begin{aligned}
\frac{\mathrm{rank}(\rho_0)}{\mathrm{rank}(\rho_1)}&=\frac{2^\lambda}{\binom{\ell+t}{\ell}}\cdot\prod_{i=0}^{\ell-1}\left(1+\frac{t}{2^n+i}\right)\leq\frac{2^\lambda}{(1+\frac{t}{\ell})^\ell}\cdot\prod_{i=0}^{\ell-1}\left(1+\frac{t}{2^n+i}\right)\\
&=2^\lambda\cdot\prod_{i=0}^{\ell-1}\left(\frac{1+\frac{t}{2^n+i}}{1+\frac{t}{\ell}}\right)\leq 2^\lambda\cdot\left(\frac{1+\frac{t}{2^n}}{1+\frac{t}{\ell}}\right)^\ell,
\end{aligned}$$

where the first inequality follows from $\binom{\ell+t}{\ell}\geq(\frac{\ell+t}{\ell})^\ell$. For $n=\omega(\log(\lambda)), t=\lambda^3$ and $\ell=\lambda/\log(\lambda)$, we have

$$2^\lambda\cdot\left(\frac{1+\frac{t}{2^n}}{1+\frac{t}{\ell}}\right)^\ell=\left(\frac{\lambda\cdot(1+\frac{\lambda^3}{\lambda^{\omega(1)}})}{1+\lambda^2\log(\lambda)}\right)^{\lambda/\log(\lambda)}\leq\left(\frac{\lambda\cdot 2}{\lambda^2\log(\lambda)}\right)^{\lambda/\log(\lambda)}\leq 2^{-\lambda}$$

for sufficiently large λ. Hence, the distinguishing advantage $(1-2^{-\lambda})$ is non-negligible. This completes the proof. □

Since multi-key pseudorandomness is stronger, we have the following immediate corollary.

Corollary 4.10. *Multi-key statistically secure (λ,n,ℓ)-PRS is impossible in the CHS model if (a) the generation algorithm uses only one copy of the common Haar state, (b) $n=\omega(\log(\lambda))$, (c) $\ell=\Omega(\lambda/\log(\lambda))$ and, (d) the length of the common Haar state is $n=\omega(\log(\lambda))$.*

5 Statistical Stretch PRFS Generators in the CHS model

In this section, we extend our techniques from Section 4.2 to construct an (λ,m,n,ℓ)-statistical PRFS in the CHS model, where $m=\lambda^c$, $\ell=\lambda^{1-c}/\log(\lambda)^{1+\varepsilon}$, the length of the common Haar state is $n\geq\lambda^{1-c}$, for any constant $\varepsilon>0$ and $c\in[0,1)$. In the case when $n>\lambda$, the construction satisfies stretch property. We prove the following theorem in Section 5.2.

Theorem 5.1. *There exists an (λ,m,n,ℓ)-statistical selectively secure PRFS generator in the CHS model where the length of the common Haar state is $n(\lambda)$, $m(\lambda)=\lambda^c$, $\ell=O(\lambda^{1-c}/\log(\lambda)^{1+\varepsilon})$ and $n(\lambda)\geq\lambda^{1-c}$, for any constant $\varepsilon>0$ and for any $c\in[0,1)$.*

Note that since a PRS can be used to computationally instantiate CHS in the plain model, the above result also gives us a way to get bounded-query long-input PRFS from PRS in the plain model. In more detail, we

can start with a PRS that has stretch (i.e. $n > \lambda$) and then we can bootstrap into a PRFS for large input length at the cost of a reduction in stretch.[20]

Corollary 5.2. *Assuming the existence of (λ, n, ℓ)-PRS, for $n > \lambda$ and $\ell = O(\lambda^{1-c}/\log(\lambda)^{1+\varepsilon})$, there exists a selectively secure $(2\lambda, m, n, \ell)$-PRFS generator with $m(\lambda) = \lambda^c$, for any constant $\varepsilon > 0$ and for any $c \in [0, 1)$.*

Furthermore, since PRFS imply PRS, achieving an ℓ-query statistical PRFS in the CHS model for $\ell = \Omega(\lambda/\log(\lambda))$ is impossible from Theorem 4.9.

Corollary 5.3. *(λ, m, n, ℓ)-statistical PRFS is impossible in the CHS model if (a) the generation algorithm uses only one copy of the common Haar state, (b) $\ell = \Omega(\lambda/\log(\lambda))$, (c) the length of the common Haar state is n and, (d) $n = \omega(\log(\lambda))$.*

We introduce several lemmas before proving Theorem 5.1.

5.1 Useful Lemmas

The following two lemmas are generalizations of the lemmas in Section 4. In particular, they state that even after splitting an ℓ-fold n-prefix collision-free type vector into q subvectors, the action of a random Pauli-Z still can be seen as a "classical" probabilistic process.

Lemma 5.4 (Generalization of Lemma 4.4)**.** *Let $\ell, n, m, q, t \in \mathbb{N}$, $\ell_1, \dots, \ell_q \in \mathbb{N}$, and $t_1, \dots, t_q \in \mathbb{N}$ such that $\sum_{i=1}^q \ell_i = \ell$ and $\sum_{i=1}^q t_i = t$. For any $\mathbf{v} \in \{0,1\}^{(n+m)(\ell+t)}$ such that $\mathsf{type}(\mathbf{v}) \in \mathcal{I}^{(\ell)}_{n,m}(\ell + t)$, where $\mathbf{v} = (\mathbf{v}^1, \dots, \mathbf{v}^q)$ and $\mathbf{v}^i \in \{0,1\}^{(n+m)(\ell_i+t_i)}$ for $i \in [q]$, and any $\sigma_1 \in S_{\ell_1+t_1}, \sigma_2 \in S_{\ell_2+t_2}, \cdots, \sigma_q \in S_{\ell_q+t_q}$, define the matrix*

$$A_{\mathbf{v},\{\sigma_i\}_{i\in[q]}} := \mathop{\mathbb{E}}_{k\leftarrow\{0,1\}^n} \left[\bigotimes_{i=1}^q \left(\left(Z^k \otimes I_m\right)^{\otimes \ell_i} \otimes I_{n+m}^{\otimes t_i} \right) |\mathbf{v}^i\rangle\langle\sigma_i(\mathbf{v}^i)| \left(\left(Z^k \otimes I_m\right)^{\otimes \ell_i} \otimes I_{n+m}^{\otimes t_i} \right) \right].$$

Then $A_{\mathbf{v},\{\sigma_i\}_{i\in[q]}} = \bigotimes_{i=1}^q |\mathbf{v}^i\rangle\langle\sigma_i(\mathbf{v}^i)|$ if for all $i \in [q]$, σ_i maps $[\ell_i]$ to $[\ell_i]$; otherwise, $A_{\mathbf{v},\{\sigma_i\}_{i\in[q]}} = 0$.

Proof. Suppose for all $i \in [q]$ and $j \in [\ell_i + t_i]$, $\mathbf{v}^i = (v_1^i || w_1^i, \dots, v_{\ell_i+t_i}^i || w_{\ell_i+t_i}^i) \in \{0,1\}^{(n+m)(\ell_i+t_i)}$ with $v_j \in \{0,1\}^n$ and $w_j \in \{0,1\}^m$. A direct calculation yields

$$\left(\left(Z^k \otimes I_m\right)^{\otimes \ell_i} \otimes I_{n+m}^{\otimes t_i} \right) |\mathbf{v}^i\rangle\langle\sigma_i(\mathbf{v}^i)| \left(\left(Z^k \otimes I_m\right)^{\otimes \ell_i} \otimes I_{n+m}^{\otimes t_i} \right) = (-1)^{\langle k, \bigoplus_{j=1}^{\ell_i} (v_j^i \oplus v_{\sigma_i(j)}^i) \rangle} |\mathbf{v}^i\rangle\langle\sigma_i(\mathbf{v}^i)|.$$

After averaging over k,

$$\begin{aligned} A_{\mathbf{v},\{\sigma_i\}_{i\in[q]}} &= \mathop{\mathbb{E}}_{k\leftarrow\{0,1\}^n} \left[(-1)^{\langle k, \bigoplus_{i=1}^q \bigoplus_{j=1}^{\ell_i} (v_j^i \oplus v_{\sigma_i(j)}^i) \rangle} \right] \cdot \bigotimes_{i=1}^q |\mathbf{v}^i\rangle\langle\sigma_i(\mathbf{v}^i)| \\ &= \begin{cases} \bigotimes_{i=1}^q |\mathbf{v}^i\rangle\langle\sigma_i(\mathbf{v}^i)| & \text{if } \bigoplus_{i=1}^q \bigoplus_{j=1}^{\ell_i} (v_j^i \oplus v_{\sigma_i(j)}^i) = 0 \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Since $\mathsf{type}(\mathbf{v}) \in \mathcal{I}^{(\ell)}_{n,m}(t + \ell)$, the condition $\bigoplus_{i=1}^q \bigoplus_{j=1}^{\ell_i} v_j^i = \bigoplus_{i=1}^q \bigoplus_{j=1}^{\ell_i} v_{\sigma_i(j)}^i$ holds if and only if the two sets $\{(i,j) : i \in [q], j \in [\ell_i]\}$ and $\{(i, \sigma_i(j)) : i \in [q], j \in [\ell_i]\}$ are identical. The latter is equivalent to the condition: $\{\sigma_i(j)) : j \in [\ell_i]\} = [\ell_j]$ for every $i \in [q]$. The proof is now complete. □

[20] Formally, let G_{PRS} is a (λ, n, ℓ)-PRS and $G(k, x, |\phi\rangle)$ is (λ, m, n, ℓ)-statistical selectively secure PRFS generator in the CHS model with $n > \lambda$, $\ell = O(\lambda^{1-c}/\log(\lambda)^{1+\varepsilon})$ and $m(\lambda) = \lambda^c$, then for $K = (k_1, k_2) \in \{0,1\}^\lambda \times \{0,1\}^\lambda$ we can define $G_{PRFS}(k, x) := G(k_1, x, G_{PRS}(k_2))$ as the $(2\lambda, m, n, \ell)$-PRFS generator.

Lemma 5.5 (Generalization of Lemma 4.5)**.** *Let $\ell, n, m, q, t \in \mathbb{N}$, $\ell_1, \ldots, \ell_q \in \mathbb{N}$, and $t_1, \ldots, t_q \in \mathbb{N}$ such that $\sum_{i=1}^q \ell_i = \ell$ and $\sum_{i=1}^q t_i = t$. For any $T \in \mathcal{I}^{(\ell)}_{n,m}(t+\ell)$ and any mutually disjoint sets $T_1, \ldots, T_q$ satisfying $\bigcup_{i=1}^q T_i = T$ and $|T_i| = t_i + \ell_i$ for all $i \in [q]$,*

$$\mathop{\mathbb{E}}_{k \leftarrow \{0,1\}^n} \left[\bigotimes_{i=1}^q \left(\left(Z^k \otimes I_m\right)^{\otimes \ell_i} \otimes I_{n+m}^{\otimes t_i} \right) |T_i\rangle\langle T_i| \left(\left(Z^k \otimes I_m\right)^{\otimes \ell_i} \otimes I_{n+m}^{\otimes t_i} \right) \right] = \bigotimes_{i=1}^q \mathop{\mathbb{E}}_{X_i \leftarrow \binom{T_i}{\ell_i}} \left[|X_i\rangle\langle X_i| \otimes |T_i \setminus X_i\rangle\langle T_i \setminus X_i| \right].$$

Proof. By Equation (1), the left-hand side equals

$$\mathop{\mathbb{E}}_{\forall i \in [q], \mathbf{v}^i \leftarrow T_i} \left[\sum_{\forall i \in [q], \sigma_i \in S_{t_i+\ell_i}} \mathop{\mathbb{E}}_{k \leftarrow \{0,1\}^n} \left[\bigotimes_{i=1}^q \left(\left(Z^k \otimes I_m\right)^{\otimes \ell_i} \otimes I_{n+m}^{\otimes t_i} \right) |\mathbf{v}^i\rangle\langle \sigma_i(\mathbf{v}^i)| \left(\left(Z^k \otimes I_m\right)^{\otimes \ell_i} \otimes I_{n+m}^{\otimes t_i} \right) \right] \right]. \tag{3}$$

Then from the previous lemma (Lemma 5.4)

$$\begin{aligned}
(3) &= \mathop{\mathbb{E}}_{\forall i \in [q], \mathbf{v}^i \leftarrow T_i} \left[\sum_{\forall i \in [q], \sigma_i^1 \in S_{\ell_i}, \sigma_i^2 \in S_{t_i}} \bigotimes_{i=1}^q |\mathbf{v}^i\rangle\langle \sigma_i^1 \circ \sigma_i^2(\mathbf{v}^i)| \right] \\
&= \bigotimes_{i=1}^q \mathop{\mathbb{E}}_{\mathbf{v}^i \leftarrow T_i} \left[\sum_{\sigma_i^1 \in S_{\ell_i}, \sigma_i^2 \in S_{t_i}} |\mathbf{v}^i\rangle\langle \sigma_i^1 \circ \sigma_i^2(\mathbf{v}^i)| \right] \\
&= \bigotimes_{i=1}^q \mathop{\mathbb{E}}_{\mathbf{v}^i \leftarrow T_i} \left[\sum_{\sigma_i^1 \in S_{\ell_i}} |\mathbf{v}^i_{[1:\ell]}\rangle\langle \sigma_i^1(\mathbf{v}^i_{[1:\ell_i]})| \otimes \sum_{\sigma_i^2 \in S_{t_i}} |\mathbf{v}^i_{[\ell_i+1:t_i+\ell_i]}\rangle\langle \sigma_i^2(\mathbf{v}^i_{[\ell_i+1:t_i+\ell_i]})| \right] \\
&= \bigotimes_{i=1}^q \mathbb{E} \left[\sum_{\sigma_i^1 \in S_{\ell_i}} |\mathbf{v}_1^i\rangle\langle \sigma_i^1(\mathbf{v}_1^i)| \otimes \sum_{\sigma_i^2 \in S_{t_i}} |\mathbf{v}_2^i\rangle\langle \sigma_i^2(\mathbf{v}_2^i)| : \begin{smallmatrix} X_i \leftarrow \binom{T_i}{\ell_i}, \\ \mathbf{v}_1^i \leftarrow X_i, \\ \mathbf{v}_2^i \leftarrow T_i \setminus X_i \end{smallmatrix} \right] \\
&= \bigotimes_{i=1}^q \mathop{\mathbb{E}}_{X_i \leftarrow \binom{T_i}{\ell_i}} \left[|X_i\rangle\langle X_i| \otimes |T_i \setminus X_i\rangle\langle T_i \setminus X_i| \right].
\end{aligned}$$

For the first equality, we use Lemma 5.4 and decompose for each $i \in [q]$, $\sigma_i = \sigma_i^1 \circ \sigma_i^2$ for some σ_i^1, σ_i^2 such that $\sigma_i^1(x) = x$ for all $x \in \{\ell_i + 1, \ell_i + 2, \cdots, \ell_i + t_i\}$ and $\sigma_i^2(y) = y$ for all $y \in \{1, 2, \cdots, \ell_i\}$. Similar to Lemma 4.5, we can view them as elements in S_{ℓ_i} and S_{t_i}. The second equality follows from linearity of trace. The third equality follows by denoting for each $i \in [q]$, the first ℓ_i part of $\mathbf{v}^i$ by $\mathbf{v}^i_{[1:\ell]}$ and the last t_i part of $\mathbf{v}^i$ by $\mathbf{v}^i_{[\ell_i+1:\ell_i+t_i]}$. The fourth equality holds because for each $i \in [q]$, sampling $\mathbf{v}_i$ from T_i is equivalent to sampling an ℓ_i-subset X_i from T_i followed by ordering the elements in X_i and $T_i \setminus X_i$. □

5.2 Construction

We extend the techniques used in Section 4.2 to construct a statistical PRFS in Figure 1. The construction samples a uniform key for each position of the input being zero or one. Applying this to the common Haar state gives us the output of the PRFS. The details can be seen in Figure 1. Thoughout this section, one should think of $m = \lambda^c$ and $\lambda' = \lambda^{1-c}$ for some constant $c \in [0, 1)$.

The main property of the construction that makes it a PRFS is its ability to *disentangles* any type state in $\mathcal{I}^{(\ell)}_{\lambda', n-\lambda'}(\ell + t)$ into a probabilistic mixture of disjoint subsets of the type. Formally, we show the following lemma:

Given the common Haar state $|\vartheta\rangle$, on the key $K = (k_1^0, \ldots, k_m^0, k_1^1, \ldots, k_m^1) \in \{0,1\}^{2\lambda' m}$ and the input $\mathbf{x} = (x_1, \ldots, x_m) \in \{0,1\}^m$, define $G(K, \mathbf{x}, |\vartheta\rangle)$ as follows:

- $|\psi_{K,\mathbf{x}}\rangle = G(K, \mathbf{x}, |\vartheta\rangle) = (Z^{\bigoplus_{i=1}^m k_i^{x_i}} \otimes I_{n-\lambda'})|\vartheta\rangle$.
- Output $|\psi_{K,\mathbf{x}}\rangle$.

Figure 1: PRFS in the CHS model

Lemma 5.6. *Let G be defined as in Figure 1. Let $q, t \in \mathbb{N}$, $\ell_1, \ldots, \ell_q \in \mathbb{N}$ such that $\sum_{i=1}^q \ell_i = \ell$. Let $\mathbf{x}^1, \ldots, \mathbf{x}^q \in \{0,1\}^m$ with $\mathbf{x}^i \neq \mathbf{x}^j$ for all $i \neq j \in [q]$. For any $T \in \mathcal{I}^{(\ell)}_{\lambda', n-\lambda'}(\ell + t)$, the following density matrices are equal:*

$$\rho := \mathop{\mathbb{E}}_{K \leftarrow \{0,1\}^{2m\lambda'}} \left[\left(\bigotimes_{i=1}^q G_K(\mathbf{x}^i, \cdot)^{\otimes \ell_i} \otimes I^{\otimes t} \right) |T\rangle\langle T| \right]$$

$$\sigma := \mathop{\mathbb{E}}_{(T_1, T_2, \ldots, T_q, \hat{T})} \left[\bigotimes_{i=1}^q |T_i\rangle\langle T_i| \otimes |\hat{T}\rangle\langle \hat{T}| \right]$$

where we omit the Hermitian conjugate of the unitary in ρ and identify it as a quantum channel; $(T_1, T_2, \ldots, T_q, \hat{T})$ in σ are sampled as follows: for $i = 1, 2, \ldots, q$, recursively sample an ℓ_i-subset from $T \setminus (\bigcup_{j=1}^{i-1} T_j)$ uniformly at random and let $\hat{T} := T \setminus (\bigcup_{j=1}^q T_j)$.

Proof. We define the following notation: Let $\ell : \{0,1\}^* \to \mathbb{N}$, such that for all $i \in [m]$, $y \in \{0,1\}^i$, $\ell(y) = \sum_{\substack{j \in [q]: \\ \mathbf{x}^j_{[1:i]} = y}} \ell_j$. Then we start by simplifying ρ:

$$\begin{aligned}
\rho &= \mathop{\mathbb{E}}_{K \leftarrow \{0,1\}^{2m\lambda'}} \left[\left(\bigotimes_{j=1}^q G_K(\mathbf{x}^j, \cdot)^{\otimes \ell_j} \otimes I^{\otimes t} \right) |T\rangle\langle T| \right] \\
&= \mathop{\mathbb{E}}_{K \leftarrow \{0,1\}^{2m\lambda'}} \left[\left(\bigotimes_{j=1}^q \left(Z^{\bigoplus_{i=1}^m k_i^{x_i^j}} \otimes I_{n-\lambda'} \right)^{\otimes \ell_j} \otimes I^{\otimes t} \right) |T\rangle\langle T| \right] \\
&= \mathop{\mathbb{E}}_{K \leftarrow \{0,1\}^{2m\lambda'}} \left[\left(\bigotimes_{j=1}^q \left(Z^{k_m^{x_m^j}} \otimes I_{n-\lambda'} \right)^{\otimes \ell_j} \otimes I^{\otimes t} \right) \cdots \left[\left(\bigotimes_{j=1}^q \left(Z^{k_1^{x_1^j}} \otimes I_{n-\lambda'} \right)^{\otimes \ell_j} \otimes I^{\otimes t} \right) |T\rangle\langle T| \right] \right] \\
&= \mathop{\mathbb{E}}_{k_m^0, k_m^1 \leftarrow \{0,1\}^{\lambda'}} \left[\left(\bigotimes_{j=1}^q \left(Z^{k_m^{x_m^j}} \otimes I_{n-\lambda'} \right)^{\otimes \ell_j} \otimes I^{\otimes t} \right) \cdots \mathop{\mathbb{E}}_{k_1^0, k_1^1 \leftarrow \{0,1\}^{\lambda'}} \left[\left(\bigotimes_{j=1}^q \left(Z^{k_1^{x_1^j}} \otimes I_{n-\lambda'} \right)^{\otimes \ell_j} \otimes I^{\otimes t} \right) |T\rangle\langle T| \right] \right],
\end{aligned}$$

where the first equality is by definition of ρ, second equality is by definition of G, third equality is because $Z^{k_1 \oplus k_2} = Z^{k_1} Z^{k_2}$ and fourth equality is by linearity of expectation. We define for $i \in [q]$, the following channels $\mathcal{C}_i$:

$$\mathcal{C}_i(\cdot) = \mathop{\mathbb{E}}_{k_i^0, k_i^1 \leftarrow \{0,1\}^{\lambda'}} \left[\left(\bigotimes_{j=1}^q \left(Z^{k_i^{x_i^j}} \otimes I_{n-\lambda'} \right)^{\otimes \ell_j} \otimes I^{\otimes t} \right) \cdot \left(\left(\bigotimes_{j=1}^q \left(Z^{k_i^{x_i^j}} \otimes I_{n-\lambda'} \right)^{\otimes \ell_j} \otimes I^{\otimes t} \right) \right)^\dagger \right],$$

then $\rho = \mathcal{C}_m(\mathcal{C}_{m-1}(\ldots \mathcal{C}_1(|T\rangle\langle T|)\ldots))$.

We define $(\{T_x\}_{x\in\{0,1\}^i}, \hat{T}) \leftarrow \mu_i$ as follow: For all $x \in \{0,1\}^i$, sample an $\ell(x)$-subset from $T \setminus (\bigcup_{y=0}^{x} T_y)$ uniformly and let $\hat{T} := T \setminus (\bigcup_{y=0}^{2^i} T_y)$.
We start by computing $\mathcal{C}_1(|T\rangle\langle T|)$, by Lemma 5.5,

$$\mathcal{C}_1(|T\rangle\langle T|) = \mathop{\mathbb{E}}_{(\{T_x\}_{x\in\{0,1\}},\hat{T})\leftarrow\mu_1} \left[\bigotimes_{b\in\{0,1\}} |T_b\rangle\langle T_b| \otimes |\hat{T}\rangle\langle\hat{T}|\right].$$

In fact, for all $i \in [q]$,

$$\mathcal{C}_i(\mathcal{C}_{i-1}(\ldots\mathcal{C}_1(|T\rangle\langle T|)\ldots)) = \mathop{\mathbb{E}}_{(\{T_y\}_{y\in\{0,1\}^i},\hat{T})\leftarrow\mu_i} \left[\bigotimes_{y\in\{0,1\}^i} |T_y\rangle\langle T_y| \otimes |\hat{T}\rangle\langle\hat{T}|\right].$$

We can show the above by induction on i. Assume that for some $i \in [q]$,

$$\mathcal{C}_i(\mathcal{C}_{i-1}(\ldots\mathcal{C}_1(|T\rangle\langle T|)\ldots)) = \mathop{\mathbb{E}}_{(\{T_y\}_{y\in\{0,1\}^i},\hat{T})\leftarrow\mu_i} \left[\bigotimes_{y\in\{0,1\}^i} |T_y\rangle\langle T_y| \otimes |\hat{T}\rangle\langle\hat{T}|\right],$$

then for $i+1 \in [q]$,

$$\begin{aligned}
&\mathcal{C}_{i+1}(\mathcal{C}_i(\ldots\mathcal{C}_1(|T\rangle\langle T|)\ldots)) \\
&= \mathcal{C}_{i+1}\left(\mathop{\mathbb{E}}_{(\{T_y\}_{y\in\{0,1\}^i},\hat{T})\leftarrow\mu_i} \left[\bigotimes_{y\in\{0,1\}^i} |T_y\rangle\langle T_y| \otimes |\hat{T}\rangle\langle\hat{T}|\right]\right) \\
&= \mathop{\mathbb{E}}_{(\{T_y\}_{y\in\{0,1\}^i},\hat{T})\leftarrow\mu_i} \left[\mathop{\mathbb{E}}_{k^0_{i+1},k^1_{i+1}} \left[\bigotimes_{y\in\{0,1\}^i} \left(\left(Z^{k^0_{i+1}} \otimes I_{n-\lambda'}\right)^{\otimes\ell(y0)} \otimes \left(Z^{k^1_{i+1}} \otimes I_{n-\lambda'}\right)^{\otimes\ell(y1)} |T_y\rangle\langle T_y|\right) \otimes |\hat{T}\rangle\langle\hat{T}|\right]\right] \\
&= \mathop{\mathbb{E}}_{(\{T_y\}_{y\in\{0,1\}^{i+1}},\hat{T})\leftarrow\mu_{i+1}} \left[\bigotimes_{y\in\{0,1\}^{i+1}} |T_y\rangle\langle T_y| \otimes |\hat{T}\rangle\langle\hat{T}|\right],
\end{aligned}$$

where the first equality is by the induction hypothesis, the second equality is by the definition of $\mathcal{C}_{i+1}$ and the third equality is by Lemma 5.4.
Hence, we get

$$\rho = \mathcal{C}_m(\mathcal{C}_{m-1}(\ldots\mathcal{C}_1(|T\rangle\langle T|)\ldots)) = \mathop{\mathbb{E}}_{(\{T_x\}_{x\in\{0,1\}^m},\hat{T})\leftarrow\mu_m} \left[\bigotimes_{y\in\{0,1\}^m} |T_y\rangle\langle T_y| \otimes |\hat{T}\rangle\langle\hat{T}|\right].$$

Ignoring the $y \in \{0,1\}^m$ for which $\ell(y) = 0$, we get

$$\rho = \mathop{\mathbb{E}}_{(T_1,T_2,\ldots,T_q,\hat{T})} \left[\bigotimes_{i=1}^{q} |T_i\rangle\langle T_i| \otimes |\hat{T}\rangle\langle\hat{T}|\right],$$

where $(T_1, T_2, \ldots, T_q, \hat{T})$ are sampled as follows: for $i = 1, 2, \ldots, q$, sample an ℓ_i-subset from $T \setminus (\bigcup_{j=1}^{i-1} T_j)$ uniformly and let $\hat{T} := T \setminus (\bigcup_{j=1}^{q} T_j)$. Hence, $\rho = \sigma$. □

Lemma 5.7 (Pseudorandomness)**.** *Let G be as defined above. Let $q, t \in \mathbb{N}$, let $\ell_1, \ldots, \ell_q \in \mathbb{N}$ be such that $\sum_{i=1}^{q} \ell_i = \ell$. Let $\mathbf{x}^1, \ldots, \mathbf{x}^q \in \{0,1\}^m$. Let*

$$\rho := \mathop{\mathbb{E}}_{\substack{K\leftarrow\{0,1\}^{2m\lambda'} \\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[\otimes_{i=1}^{q} G_K(\mathbf{x}^i, |\vartheta\rangle)^{\otimes\ell_i} \otimes |\vartheta\rangle\langle\vartheta|^{\otimes t}\right],$$

and

$$\sigma := \mathop{\mathbb{E}}_{\substack{\forall i\in[q],|\varphi_i\rangle\leftarrow\mathcal{H}_n\\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[\otimes_{i=1}^{q}|\varphi_i\rangle\langle\varphi_i|^{\otimes\ell_i}\otimes|\vartheta\rangle\langle\vartheta|^{\otimes t}\right].$$

Then $\mathsf{TD}(\rho,\sigma) = O\left(\frac{(\ell+t)^{2\ell}}{2^{\lambda'}}\right)$.

Proof. We prove this using hybrid arguments:

Hybrid 1. Sample $T \leftarrow [0:\ell+t]^{2^n}$. Sample $K \leftarrow \{0,1\}^{2m\lambda'}$. Output $(\bigotimes_{j=1}^{q}(Z^{\oplus_{i=1}^{m}k_i^{x_i^j}}\otimes I_{n-\lambda'})^{\otimes\ell_j}\otimes I_n^{\otimes t})|T\rangle$.

Hybrid 2. Sample $T \leftarrow [0:\ell+t]^{2^n}$ uniformly conditioned on $T\in\mathcal{I}^{(\ell)}_{\lambda',n-\lambda'}(\ell+t)$. Sample $K \leftarrow \{0,1\}^{2m\lambda'}$. Output $(\bigotimes_{j=1}^{q}(Z^{\oplus_{i=1}^{m}k_i^{x_i^j}}\otimes I_{n-\lambda'})^{\otimes\ell_j}\otimes I_n^{\otimes t})|T\rangle$.

Hybrid 3: Sample $T \leftarrow [0:\ell+t]^{2^n}$ uniformly conditioned on $T\in\mathcal{I}^{(\ell)}_{\lambda',n-\lambda'}(\ell+t)$. Sample a uniform for all $j\in[q]$, ℓ_j-subsets T_j from T such that for any $j\neq j'\in[q]$, $T_j\cap T_{j'}=\emptyset$. Define $\tilde{T}=\bigcup_{j=1}^{q}T_j$. Output $\bigotimes_{j=1}^{q}|T_j\rangle\otimes|T\setminus\tilde{T}\rangle$.

Hybrid 4. Sample $T \leftarrow [0:\ell+t]^{2^n}$. For all $j\in[q]$, sample a uniform ℓ_j-subset T_j from $T\setminus\bigcup_{i=1}^{j-1}T_j$.[21] Output $\bigotimes_{j=1}^{q}|T_j\rangle\otimes|T\setminus\bigcup_{j=1}^{q}T_i\rangle$.

Hybrid 5. Sample a collision-free T from $[0:\ell+t]^{2^n}$. Sample a uniform for all $j\in[q]$, ℓ_j-subsets T_j from T such that for any $j\neq j'\in[q]$, $T_j\cap T_{j'}=\emptyset$. Define $\tilde{T}=\bigcup_{j=1}^{q}T_j$. Output $\bigotimes_{j=1}^{q}|T_j\rangle\otimes|T\setminus\tilde{T}\rangle$.

Hybrid 6. For all $j\in[q]$, sample uniform collision-free T_j from $[0:\ell_j]^{2^n}$ conditioned on T_j and $\bigcup_{i=1}^{j-1}T_j$ have no common elements. Sample a uniform collision-free $\hat{T}$ from $[0:t]^{2^n}$ conditioned on $\bigcup_{j=1}^{q}T_j$ and $\hat{T}$ have no common elements. Output $\bigotimes_{j=1}^{q}|T_j\rangle\otimes|\hat{T}\rangle$.

Hybrid 7.y, for $y\in[0:q-1]$. For all $j\in[q-y]$, sample uniform collision-free T_j from $[0:\ell_j]^{2^n}$ conditioned on T_j and $\bigcup_{i=1}^{j-1}T_j$ have no common elements. For all $j\in[q-y+1:q]$, sample a uniform collision-free T_j from $[0:\ell_j]^{2^n}$. Sample a uniform collision-free $\hat{T}$ from $[0:t]^{2^n}$. Output $\bigotimes_{j=1}^{q}|T_j\rangle\otimes|\hat{T}\rangle$.

Hybrid 8. For all $j\in[q]$, sample $T_j\leftarrow[0:\ell_j]^{2^n}$. Sample $\hat{T}\leftarrow[0:t]^{2^n}$. Output $\bigotimes_{j=1}^{q}|T_j\rangle\otimes|\hat{T}\rangle$.

Indistinuishability of Hybrids.

- By Lemma 4.3, the trace distance between Hybrid 1 and Hybrid 2 is $O((t+\ell)^{2\ell}/2^{\lambda'})$.
- From Lemma 5.6, the output of Hybrid 2 is equivalent to Hybrid 3.
- By Lemma 4.3, the trace distance between Hybrid 3 and Hybrid 4 is $O((t+\ell)^{2\ell}/2^{\lambda'})$.
- The trace distance between Hybrid 4 and Hybrid 5 is $O((t+\ell)^2/2^n)$ by collision bound.
- Hybrid 5 and Hybrid 6 are equivalent.
- The trace distance between Hybrid 6 and Hybrid 7.0 is $O(t\ell/2^n)$.

[21] Since T might have collisions, T_j is allowed to contain duplicate elements.

- For $y \in [0 : q-2]$, the trace distance between Hybrid 7.y and Hybrid 7.$(y+1)$ is $O(\ell_{q-y}(\sum_{j=1}^{q-y-1} \ell_j)/2^n)$.
- Finally, the trace distance between Hybrid 7 and Hybrid 8 is $O((t^2 + \sum_{j=1}^{q} \ell_j^2)/2^n)$ by collision bound.

This completes the proof. □

Remark 5.8. *Note that the above construction is still secure if we set $k_i^1 = 0$ for all $i \in [2 : m]$. This slightly reduces the key length from $2m\lambda'$ to $(m+1)\lambda'$.*

6 Quantum Commitments in the CHS model

In this section, we construct a commitment scheme that satisfies poly-copy statistical hiding and statistical sum-biding in the CHS model. The scheme is inspired by the quantum commitment scheme proposed in [MY21; MNY23]. In contrast to the scheme in [MY21], our construction is not of the canonical form [Yan22]. To achieve binding, similar to [MNY23], the receiver needs to perform several SWAP tests. To achieve hiding, our scheme relies on the multi-key pseudorandomness property in Lemma 4.7.

6.1 Construction

We assume that $n(\lambda) \geq \lambda+1$ for all $\lambda \in \mathbb{N}$. Our construction, parameterized by the polynomial $p = p(\lambda) := \lambda$, is shown in Figure 2.

Theorem 6.1. *The construction in Figure 2 is a quantum commitment in the CHS model.*

Commit phase: The sender C_λ on input $b \in \{0,1\}$ does the following:

- Use p copies of the common Haar state $|\vartheta\rangle$ to prepare the state $|\Psi_b\rangle_{\mathsf{CR}} := \bigotimes_{i=1}^{p} |\psi_b\rangle_{\mathsf{C}_i\mathsf{R}_i}$, where

$$|\psi_0\rangle_{\mathsf{C}_i\mathsf{R}_i} := \frac{1}{\sqrt{2^\lambda}} \sum_{k\in\{0,1\}^\lambda} (Z^k \otimes I_{n-\lambda})|\vartheta\rangle_{\mathsf{C}_i}|k||0^{n-\lambda}\rangle_{\mathsf{R}_i}$$

  and

$$|\psi_1\rangle_{\mathsf{C}_i\mathsf{R}_i} := \frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} |j\rangle_{\mathsf{C}_i}|j\rangle_{\mathsf{R}_i},$$

  and $\mathsf{C} := (\mathsf{C}_1, \mathsf{C}_2, \ldots, \mathsf{C}_p)$ and $\mathsf{R} := (\mathsf{R}_1, \mathsf{R}_2, \ldots, \mathsf{R}_p)$.
- Send register C to the receiver.

Reveal phase:

- The sender sends b and register R to the receiver.
- The receiver prepares the state $|\Psi_b\rangle_{\mathsf{C}'\mathsf{R}'} = \bigotimes_{i=1}^{p} |\psi_b\rangle_{\mathsf{C}'_i\mathsf{R}'_i}$ by using p copies of the common Haar state $|\vartheta\rangle$, where $\mathsf{C}' := (\mathsf{C}'_1, \mathsf{C}'_2, \ldots, \mathsf{C}'_p)$ and $\mathsf{R}' := (\mathsf{R}'_1, \mathsf{R}'_2, \ldots, \mathsf{R}'_p)$ are receiver's registers.
- For $i \in [p]$, the receiver performs the SWAP test between registers $(\mathsf{C}_i, \mathsf{R}_i)$ and $(\mathsf{C}'_i, \mathsf{R}'_i)$.
- The receiver outputs b if all SWAP tests accept; otherwise, outputs $\perp$.

Figure 2: Quantum commitment scheme in the CHS model

6.2 Proving Hiding and Binding

Now, we prove Theorem 6.1.

Proof of Theorem 6.1. Clearly, the construction has perfect correctness.

Poly-copy statistical hiding. It follows immediately from Lemma 4.7 by setting $\ell = 1$.

Statistical sum binding. For any (fixed) common Haar state $|\vartheta\rangle$ and $i \in [p]$, it holds that

$$\begin{aligned}
&F(\mathrm{Tr}_{\mathsf{R}_i}(|\psi_0\rangle\langle\psi_0|_{\mathsf{C}_i\mathsf{R}_i}), \mathrm{Tr}_{\mathsf{R}_i}(|\psi_1\rangle\langle\psi_1|_{\mathsf{C}_i\mathsf{R}_i}))\\
=&F\left(\underbrace{\frac{1}{2^\lambda}\sum_{k\in\{0,1\}^\lambda}(Z^k\otimes I_{n-\lambda})|\vartheta\rangle\langle\vartheta|_{\mathsf{C}_i}(Z^k\otimes I_{n-\lambda})}_{=:\rho_0}, \frac{I_{\mathsf{C}_i}}{2^n}\right)\\
=&2^{-n}\cdot\mathrm{Tr}(\sqrt{\rho_0})^2\\
\le&2^{-n}\cdot\mathrm{rank}(\sqrt{\rho_0})\cdot\mathrm{Tr}(\rho_0)\\
\le&2^{-n}\cdot 2^\lambda\cdot 1 = 2^{-(n-\lambda)},
\end{aligned} \tag{4}$$

where the second equality is by the definition of fidelity $F(\rho,\sigma) = \left(\mathrm{Tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)\right)^2$; the first inequality follows from $\mathrm{Tr}(\rho)^2 \le \mathrm{rank}(\rho)\cdot\mathrm{Tr}\left(\rho^2\right)$ for $\rho \succeq 0$; the second inequality is because $\mathrm{rank}(\sqrt{\rho}) = \mathrm{rank}(\rho)$ for $\rho \succeq 0$ and $\mathrm{rank}(X+Y) \le \mathrm{rank}(X) + \mathrm{rank}(Y)$.
Let $M^{(b)}_{\mathsf{CR}}$ be the POVM operator corresponding to that the receiver outputs b (i.e., all the SWAP tests accept),

$$M^{(b)}_{\mathsf{CR}} := \bigotimes_{i\in[p]}\left(\frac{I_{\mathsf{C}_i\mathsf{R}_i} + |\psi_b\rangle\langle\psi_b|_{\mathsf{C}_i\mathsf{R}_i})}{2}\right) = \mathop{\mathbb{E}}_{\mathcal{S}\subseteq[p]}\left[\bigotimes_{i\in\mathcal{S}}|\psi_b\rangle\langle\psi_b|_{\mathsf{C}_i\mathsf{R}_i}\otimes\bigotimes_{i\notin\mathcal{S}}I_{\mathsf{C}_i\mathsf{R}_i}\right],$$

where $\mathcal{S}$ is a uniformly random subset of $[p]$. Then the probability that the receiver outputs b is

$$\begin{aligned}
p_b :=& \mathrm{Tr}\left(M^{(b)}_{\mathsf{CR}}\underbrace{\mathrm{Tr}_{\mathsf{E}}(U^{(b)}_{\mathsf{RE}}|\Phi\rangle\langle\Phi|_{\mathsf{CRE}}U^{(b)\dagger}_{\mathsf{RE}})}_{=:\rho^{(b)}_{\mathsf{CR}}}\right)\\
=& \mathop{\mathbb{E}}_{\mathcal{S}\subseteq[p]}\left[\mathrm{Tr}\left(\bigotimes_{i\in\mathcal{S}}|\psi_b\rangle\langle\psi_b|_{\mathsf{C}_i\mathsf{R}_i}\otimes\bigotimes_{i\notin\mathcal{S}}I_{\mathsf{C}_i\mathsf{R}_i}\cdot\rho^{(b)}_{\mathsf{CR}}\right)\right]\\
=& \mathop{\mathbb{E}}_{\mathcal{S}\subseteq[p]}\left[\underbrace{F\left(\bigotimes_{i\in\mathcal{S}}|\psi_b\rangle\langle\psi_b|_{\mathsf{C}_i\mathsf{R}_i}, \mathrm{Tr}_{\mathsf{C}_i\mathsf{R}_i:i\notin\mathcal{S}}(\rho^{(b)}_{\mathsf{CR}})\right)}_{=:p_{b,S}}\right],
\end{aligned}$$

where E is the sender's internal register, $|\Phi\rangle_{\mathsf{CRE}}$ is the malicious sender's initial state that might depend on $|\vartheta\rangle$ (we omit the dependence for simplicity), and $U^{(b)}_{\mathsf{RE}}$ is the malicious sender's attacking unitary for b; we plug in the definition of $M^{(b)}_{\mathsf{CR}}$ and use the short-hand notation $\rho^{(b)}_{\mathsf{CR}}$ to obtain the second equality.
For any fixed $\mathcal{S} \subseteq [p]$, we have

$$p_{0,\mathcal{S}} + p_{1,\mathcal{S}}$$

$$
\begin{aligned}
&= F\left(\bigotimes_{i\in\mathcal{S}} |\psi_0\rangle\langle\psi_0|_{\mathsf{C}_i\mathsf{R}_i}, \mathrm{Tr}_{\mathsf{C}_i\mathsf{R}_i:i\notin\mathcal{S}}(\rho^{(0)}_{\mathsf{CR}})\right) + F\left(\bigotimes_{i\in\mathcal{S}} |\psi_1\rangle\langle\psi_1|_{\mathsf{C}_i\mathsf{R}_i}, \mathrm{Tr}_{\mathsf{C}_i\mathsf{R}_i:i\notin\mathcal{S}}(\rho^{(1)}_{\mathsf{CR}})\right)\\
&\leq F\left(\bigotimes_{i\in\mathcal{S}} \mathrm{Tr}_{\mathsf{R}_i}(|\psi_0\rangle\langle\psi_0|_{\mathsf{C}_i\mathsf{R}_i}), \mathrm{Tr}_{\mathsf{C}_i:i\notin\mathcal{S}}\,\mathrm{Tr}_{\mathsf{R}}(\rho^{(0)}_{\mathsf{CR}})\right) + F\left(\bigotimes_{i\in\mathcal{S}} \mathrm{Tr}_{\mathsf{R}_i}(|\psi_1\rangle\langle\psi_1|_{\mathsf{C}_i\mathsf{R}_i}), \mathrm{Tr}_{\mathsf{C}_i:i\notin\mathcal{S}}\,\mathrm{Tr}_{\mathsf{R}}(\rho^{(1)}_{\mathsf{CR}})\right)\\
&\leq 1 + F\left(\bigotimes_{i\in\mathcal{S}} \mathrm{Tr}_{\mathsf{R}_i}(|\psi_0\rangle\langle\psi_0|_{\mathsf{C}_i\mathsf{R}_i}), \bigotimes_{i\in\mathcal{S}} \mathrm{Tr}_{\mathsf{R}_i}(|\psi_1\rangle\langle\psi_1|_{\mathsf{C}_i\mathsf{R}_i})\right)^{1/2}\\
&= 1 + \bigotimes_{i\in\mathcal{S}} F\left(\mathrm{Tr}_{\mathsf{R}_i}(|\psi_0\rangle\langle\psi_0|_{\mathsf{C}_i\mathsf{R}_i}), \mathrm{Tr}_{\mathsf{R}_i}(|\psi_1\rangle\langle\psi_1|_{\mathsf{C}_i\mathsf{R}_i})\right)^{1/2} \leq 1 + 2^{\frac{-|\mathcal{S}|(n-\lambda)}{2}},
\end{aligned}
$$

where the first inequality follows from the fact that taking a partial trace won't decrease the fidelity; the second inequality is because $\mathrm{Tr}_{\mathsf{R}}(\rho^{(0)}_{\mathsf{CR}}) = \mathrm{Tr}_{\mathsf{R}}(\rho^{(1)}_{\mathsf{CR}})$ and $F(\rho,\xi)+F(\sigma,\xi) \leq 1+\sqrt{F(\rho,\sigma)}$ [NS03]; the last equality follows from the fact that $F(\bigotimes_i \rho_i, \bigotimes_i \sigma_i) = \prod_i F(\rho_i,\sigma_i)$; the last inequality follows from Equation (4). Finally, we bound the probability $p_0 + p_1$ as follows:

$$
\begin{aligned}
p_0 + p_1 = \mathop{\mathbb{E}}_{\mathcal{S}\subseteq[p]}[p_{0,\mathcal{S}} + p_{1,\mathcal{S}}] &\leq 1 + \mathop{\mathbb{E}}_{\mathcal{S}\subseteq[p]}\left[2^{\frac{-|\mathcal{S}|(n-\lambda)}{2}}\right] = 1 + 2^{-p}\cdot\sum_{s=0}^{t}\binom{p}{s}2^{\frac{-s(n-\lambda)}{2}}\\
&= 1 + \left(\frac{1+2^{\frac{-(n-\lambda)}{2}}}{2}\right)^{p} = 1 + \mathsf{negl}(\lambda),
\end{aligned}
$$

since we set $n(\lambda) \geq \lambda + 1$ and $p(\lambda) = \lambda = \omega(\log(\lambda))$. □

7 LOCC Indistinguishability

In this section, we prove our main technical theorem for proving impossibilities and separations in Section 8 and Section 9.

7.1 Definitions

Definition 7.1 (LOCC adversaries)**.** *An* LOCC adversary *is a tuple (A, B), where A and B are spatially separated, non-uniform, and computationally unbounded quantum algorithms without pre-shared entanglement. In addition, A and B can only perform local operations on their registers and communicate classically.*

Definition 7.2 (LOCC Indistinguishability)**.** *We say that two density matrices $(\rho_{\mathsf{AB}}, \sigma_{\mathsf{AB}})$ are* ε-LOCC indistinguishable *if for any LOCC adversary (A, B) with A taking as input register A and B taking as input register B, the probability that B outputs 1 satisfies*[22]

$$
|\Pr[(A,B)(\rho_{\mathsf{AB}}) = 1] - \Pr[(A,B)(\sigma_{\mathsf{AB}}) = 1]| \leq \varepsilon.
$$

If $\varepsilon(\cdot)$ is negligible, then we simply say that $(\rho_{\mathsf{AB}}, \sigma_{\mathsf{AB}})$ are LOCC indistinguishable.

It is well-known that the class of operations having positive partial transpose (PPT) is a strict superset of the class of LOCC operations (see, e.g., [DLT02; EW02; CLM+14; Har23]). Hence, it suffices to consider the maximum distinguishing advantage over PPT measurements.

Lemma 7.3. *For any two density matrices $\rho_{\mathsf{AB}}, \sigma_{\mathsf{AB}}$ and $\varepsilon \geq 0$, $(\rho_{\mathsf{AB}}, \sigma_{\mathsf{AB}})$ are ε-LOCC indistinguishable if*

$$
\sup_{\substack{M_{\mathsf{AB}}:0\preceq M_{\mathsf{AB}}\preceq I\\ \wedge 0\preceq M_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}\preceq I}} |\mathrm{Tr}(M_{\mathsf{AB}}(\rho_{\mathsf{AB}} - \sigma_{\mathsf{AB}}))| \leq \varepsilon.
$$

[22] Since (A, B) are allowed to communicate and we do not care about communication complexity, it is without loss of generality to assume that B outputs the bit.

We can extend the LOCC indistinguishability into the multi-party setting.

Definition 7.4 (m-party LOCC adversaries)**.** *An m-party* LOCC adversary *is an m-tuple $(\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_m)$, where each P_i is a non-uniform, computationally unbounded quantum algorithms and every distinct pair $(\mathsf{P}_i, \mathsf{P}_j)$ is spatially separated and without pre-shared entanglement. In addition, every party can only perform local operations on their registers and communicate classically.*

Definition 7.5 (m-party LOCC Indistinguishability)**.** *We say that two density matrices $(\rho_{\mathsf{P}}, \sigma_{\mathsf{P}})$ on register $\mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_m)$ are* (m, ε)-LOCC indistinguishable *if for any m-party LOCC adversary $(\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_m)$ with each P_i taking as input register P_i, the probability that P_m outputs 1 satisfies*

$$|\Pr[(\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_m)(\rho_{\mathsf{P}}) = 1] - \Pr[(\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_m)(\sigma_{\mathsf{P}}) = 1]| \leq \varepsilon.$$

7.2 LOCC Haar Indistinguishability

We first introduce several useful lemmas.

Lemma 7.6. *For any $d \in \mathbb{N}$, any set $T \subseteq [d]$ and any integer $0 \leq x \leq |T|$, the type state $|T\rangle$ can be written as*

$$|T\rangle_{\mathsf{AB}} = \sum_{X \in \binom{T}{x}} \frac{1}{\sqrt{\binom{|T|}{x}}} |X\rangle_{\mathsf{A}} \otimes |T \setminus X\rangle_{\mathsf{B}},$$

where register A contains the first x qudits and register B contains the last $|T| - x$ qudits.

Proof. For every $X \in \binom{T}{x}$, the inner product of $|X\rangle_{\mathsf{A}} \otimes |T \setminus X\rangle_{\mathsf{B}}$ and $|T\rangle_{\mathsf{AB}}$ is

$$\left(\frac{1}{\sqrt{x!(|T|-x)!}} \sum_{\mathbf{x} \in X, \mathbf{y} \in T \setminus X} \langle \mathbf{x}|_{\mathsf{A}} \otimes \langle \mathbf{y}|_{\mathsf{B}}\right) \left(\frac{1}{\sqrt{T!}} \sum_{\mathbf{v} \in T} |\mathbf{v}\rangle_{\mathsf{AB}}\right) = \sqrt{\frac{x!(|T|-x)!}{T!}} = \frac{1}{\sqrt{\binom{|T|}{x}}}.$$

Moreover, $|X\rangle_{\mathsf{A}} \otimes |T \setminus X\rangle_{\mathsf{B}}$ and $|X'\rangle_{\mathsf{A}} \otimes |T \setminus X'\rangle_{\mathsf{B}}$ are orthogonal for every pair $X \neq X' \in \binom{T}{x}$. Since $|T\rangle$ is normalized, the equality holds. □

Kneser graphs. For any $v, k \in \mathbb{N}$, the *Kneser graph* $K(v, k)$ is the graph whose vertices correspond to the k-element subsets of the set $[v]$, and two vertices are adjacent if and only if the two corresponding sets are disjoint.

Lemma 7.7 ([LW12, Theorem 1])**.** *For any $v, k \in \mathbb{N}$ such that $v \geq 2k + 1$, the sum of absolute eigenvalues of the adjacency matrix of $K(v, k)$ (which is equal to its 1-norm) is*

$$\frac{2^k (v-1)(v-3)\ldots(v-2k+1)}{k!}.$$

The following lemma is the crux for proving Theorem 7.9.

Lemma 7.8. *Let $\tilde{\rho}_{\mathsf{AB}} := \mathbb{E}_{T \leftarrow \binom{[d]}{2t}} [|T\rangle\langle T|_{\mathsf{AB}}]$ and $\tilde{\sigma}_{\mathsf{AB}} := \mathbb{E}_{S_A, S_B \leftarrow \binom{[d]}{t} : S_A \cap S_B = \emptyset} [|S_A\rangle\langle S_A|_{\mathsf{A}} \otimes |S_B\rangle\langle S_B|_{\mathsf{B}}]$. Then we have $\left\| \tilde{\rho}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}} - \tilde{\sigma}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}} \right\|_1 \leq O(t^2/d)$.*

Proof. By Lemma 7.6, we can expand $\tilde{\rho}$ as follows:

$$\tilde{\rho}_{\mathsf{AB}} = \frac{1}{\binom{d}{2t}\binom{2t}{t}} \sum_{T \in \binom{[d]}{2t}} \sum_{X, Y \in \binom{T}{t}} |T \setminus X\rangle\langle T \setminus Y|_{\mathsf{A}} \otimes |X\rangle\langle Y|_{\mathsf{B}}.$$

On the other hand, we have

$$\tilde{\sigma}_{\mathsf{AB}} = \frac{1}{\binom{d}{t}\binom{d-t}{t}} \sum_{\substack{S_A,S_B\in\binom{[d]}{t}:\\ S_A\cap S_B=\emptyset}} |S_A\rangle\langle S_A|_{\mathsf{A}} \otimes |S_B\rangle\langle S_B|_{\mathsf{B}} = \frac{1}{\binom{d}{2t}\binom{2t}{t}} \sum_{\substack{S_A,S_B\in\binom{[d]}{t}:\\ S_A\cap S_B=\emptyset}} |S_A\rangle\langle S_A|_{\mathsf{A}} \otimes |S_B\rangle\langle S_B|_{\mathsf{B}}.$$

Taking partial transpose with respect to B, we have $\tilde{\sigma}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}} = \tilde{\sigma}_{\mathsf{AB}}$ and

$$\begin{aligned}\tilde{\rho}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}} &= \frac{1}{\binom{d}{2t}\binom{2t}{t}} \sum_{T\in\binom{[d]}{2t}} \sum_{X,Y\in\binom{T}{t}} |T\setminus X\rangle\langle T\setminus Y|_{\mathsf{A}} \otimes |Y\rangle\langle X|_{\mathsf{B}} \\ &= \tilde{\sigma}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}} + \frac{1}{\binom{d}{2t}\binom{2t}{t}} \sum_{T\in\binom{[d]}{2t}} \sum_{\substack{X,Y\in\binom{T}{t}:\\ X\neq Y}} |T\setminus X\rangle\langle T\setminus Y|_{\mathsf{A}} \otimes |Y\rangle\langle X|_{\mathsf{B}}.\end{aligned}$$

where the second equality is because when $X = Y$,

$$\sum_{T\in\binom{[d]}{2t}} \sum_{X\in\binom{T}{t}} |T\setminus X\rangle\langle T\setminus X|_{\mathsf{A}} \otimes |X\rangle\langle X|_{\mathsf{B}} = \sum_{S_A,S_B\in\binom{[d]}{t}:S_A\cap S_B=\emptyset} |S_A\rangle\langle S_A|_{\mathsf{A}} \otimes |S_B\rangle\langle S_B|_{\mathsf{B}}.$$

Hence, we have

$$\left\|\tilde{\rho}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}} - \tilde{\sigma}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}\right\|_1 = \frac{1}{\binom{d}{2t}\binom{2t}{t}} \left\| \sum_{T\in\binom{[d]}{2t}} \sum_{\substack{X,Y\in\binom{T}{t}:\\ X\neq Y}} |T\setminus X\rangle\langle T\setminus Y|_{\mathsf{A}} \otimes |Y\rangle\langle X|_{\mathsf{B}} \right\|_1.$$

Now, we will apply a double-counting argument. Each (T, X, Y) can uniquely correspond to a tuple of mutually disjoint sets (C, I, X', Y') satisfying $C = T\setminus(X\cup Y)$ (C denotes complement of $X\cup Y$), $I = X\cap Y$ (I denotes intersection), $X' = X\setminus I$ and $Y' = Y\setminus I$. Hence, $T\setminus X = C\uplus Y'$, $Y = I\uplus Y'$, $T\setminus Y = C\uplus X'$, and $X = I\uplus X'$ where $\uplus$ denotes the disjoint union. By further classifying the summands according to $s := |C| = |I| \in \{0, 1, \ldots, t-1\}$ (note that then $|X'| = |Y'| = t - s$), we have

$$\begin{aligned}\left\|\tilde{\rho}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}} - \tilde{\sigma}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}\right\|_1 &= \frac{1}{\binom{d}{2t}\binom{2t}{t}} \left\| \sum_{s=0}^{t-1} \sum_{C\in\binom{[d]}{s}} \sum_{I\in\binom{[d]\setminus C}{s}} \sum_{\substack{X',Y'\in\binom{[d]\setminus(C\uplus I)}{t-s}:\\ X'\cap Y'=\emptyset}} |C\uplus Y'\rangle_{\mathsf{A}}|I\uplus Y'\rangle_{\mathsf{B}}\langle C\uplus X'|_{\mathsf{A}}\langle I\uplus X'|_{\mathsf{B}} \right\|_1 \\ &\le \frac{1}{\binom{d}{2t}\binom{2t}{t}} \sum_{s=0}^{t-1} \sum_{C\in\binom{[d]}{s}} \sum_{I\in\binom{[d]\setminus C}{s}} \underbrace{\left\| \sum_{\substack{X',Y'\in\binom{[d]\setminus(C\uplus I)}{t-s}:\\ X'\cap Y'=\emptyset}} |C\uplus Y'\rangle_{\mathsf{A}}|I\uplus Y'\rangle_{\mathsf{B}}\langle C\uplus X'|_{\mathsf{A}}\langle I\uplus X'|_{\mathsf{B}} \right\|_1}_{=:K_{C,I}}, \qquad (*)\end{aligned}$$

where the inequality follows from the triangle inequality. Observe that for every (C, I), the matrix $K_{C,I}$ is isospectral[23] to the adjacency matrix of the Kneser graph $K(d-2s, t-s)$. By Lemma 7.7, we continue bounding the above inequality:

$$(*) = \frac{1}{\binom{d}{2t}\binom{2t}{t}} \sum_{s=0}^{t-1} \binom{d}{s}\binom{d-s}{s} \frac{2^{t-s}(d-2s-1)(d-2s-3)\ldots(d-2t+1)}{(t-s)!}$$

[23] Two matrices are isospectral to one another if they have the same set of non-zero eigenvalues, including multiplicities.

$$= \sum_{s=0}^{t-1} \frac{2^{t-s}\left(\frac{t!}{s!}\right)^2}{(t-s)!(d-2s)(d-2s-2)\dots(d-2t+2)}$$
$$\leq \sum_{s=0}^{t-1} \frac{2^{t-s}\cdot t^{2(t-s)}}{(t-s)!(d-2t+2)^{t-s}}. \qquad (**)$$

By letting $k := t-s$, we finally have

$$(**) = \sum_{k=1}^{t} \frac{(\frac{2t^2}{d-2t+2})^k}{k!} \leq \exp\left(\frac{2t^2}{d-2t+2}\right) - 1 = O\left(\frac{t^2}{d}\right). \qquad \square$$

Theorem 7.9 (LOCC Haar Indistinguishability)**.** *Let* $\rho_{\mathsf{AB}} := \mathbb{E}_{|\psi\rangle\leftarrow\mathcal{H}_n}\left[|\psi\rangle\langle\psi|_{\mathsf{A}}^{\otimes t}\otimes|\psi\rangle\langle\psi|_{\mathsf{B}}^{\otimes t}\right]$ *and* $\sigma_{\mathsf{AB}} := \mathbb{E}_{|\psi\rangle\leftarrow\mathcal{H}_n}\left[|\psi\rangle\langle\psi|_{\mathsf{A}}^{\otimes t}\right]\otimes\mathbb{E}_{|\phi\rangle\leftarrow\mathcal{H}_n}\left[|\phi\rangle\langle\phi|_{\mathsf{B}}^{\otimes t}\right]$*. Then* ρ_{AB} *and* σ_{AB} *are* $O(t^2/2^n)$*-LOCC indistinguishable.*

Proof. Let $\tilde{\rho}_{\mathsf{AB}}$ and $\tilde{\sigma}_{\mathsf{AB}}$ be defined as in Lemma 7.8. By the collision bound, both $(\rho_{\mathsf{AB}}, \tilde{\rho}_{\mathsf{AB}})$, and $(\sigma_{\mathsf{AB}}, \tilde{\sigma}_{\mathsf{AB}})$ are $O(t^2/d)$-close in trace distance, which trivially implies their $O(t^2/d)$-LOCC indistinguishability. Thus, if suffices to show that $\tilde{\rho}_{\mathsf{AB}}$ and $\tilde{\sigma}_{\mathsf{AB}}$ are $O(t^2/d)$-LOCC indistinguishable. From Lemma 7.3, the LOCC distinguishing advantage of $\tilde{\rho}_{\mathsf{AB}}$ and $\tilde{\sigma}_{\mathsf{AB}}$ can be upper bounded by

$$\begin{aligned}
&\sup_{\substack{M_{\mathsf{AB}}:0\preceq M_{\mathsf{AB}}\preceq I\\ \wedge 0\preceq M_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}\preceq I}} |\operatorname{Tr}(M_{\mathsf{AB}}(\tilde{\rho}_{\mathsf{AB}}-\tilde{\sigma}_{\mathsf{AB}}))| \\
&\leq \sup_{M_{\mathsf{AB}}:0\preceq M_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}\preceq I} |\operatorname{Tr}(M_{\mathsf{AB}}(\tilde{\rho}_{\mathsf{AB}}-\tilde{\sigma}_{\mathsf{AB}}))| \\
&= \sup_{M_{\mathsf{AB}}:0\preceq M_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}\preceq I} |\operatorname{Tr}\left(M_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}(\tilde{\rho}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}-\tilde{\sigma}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}})\right)| \\
&= \sup_{M_{\mathsf{AB}}:0\preceq M_{\mathsf{AB}}\preceq I} |\operatorname{Tr}\left(M_{\mathsf{AB}}(\tilde{\rho}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}-\tilde{\sigma}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}})\right)| \\
&= \frac{1}{2}\left\|\tilde{\rho}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}-\tilde{\sigma}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}\right\|_1.
\end{aligned}$$

The first inequality holds because we omit the constraint $0 \preceq M_{\mathsf{AB}} \preceq I$. The first equality follows from the fact that $\operatorname{Tr}(P_{\mathsf{AB}}Q_{\mathsf{AB}}) = \operatorname{Tr}\left(P_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}Q_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}\right)$ for all matrices $P_{\mathsf{AB}}, Q_{\mathsf{AB}}$. Since $\tilde{\rho}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}} - \tilde{\sigma}_{\mathsf{AB}}^{\Gamma_{\mathsf{B}}}$ is Hermitian and has trace zero, the last equality follows from the variational definition of trace norm. Applying Lemma 7.8 completes the proof. $\square$

To prove the separations in Section 9, we rely on the following generalization of Theorem 7.9 which states the LOCC indistinguishability when (A, B) are further given many i.i.d. input instances with different lengths.

Corollary 7.10. *For positive integers* $s, t, n_1, n_2, \dots, n_s$*, define*

$$\rho_{\mathsf{AB}} := \bigotimes_{i=1}^{s} \mathbb{E}_{|\psi_i\rangle\leftarrow\mathcal{H}_{n_i}}\left[\left(|\psi_i\rangle\langle\psi_i|^{\otimes t}\right)_{\mathsf{A}_i}\otimes\left(|\psi_i\rangle\langle\psi_i|^{\otimes t}\right)_{\mathsf{B}_i}\right]$$

$$\sigma_{\mathsf{AB}} := \bigotimes_{i=1}^{s} \mathbb{E}_{|\psi_i\rangle\leftarrow\mathcal{H}_{n_i}}\left[\left(|\psi_i\rangle\langle\psi_i|^{\otimes t}\right)_{\mathsf{A}_i}\right]\otimes\bigotimes_{i=1}^{s} \mathbb{E}_{|\phi_i\rangle\leftarrow\mathcal{H}_{n_i}}\left[\left(|\phi_i\rangle\langle\phi_i|^{\otimes t}\right)_{\mathsf{B}_i}\right],$$

where $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2, \dots, \mathsf{A}_s)$ *and* $\mathsf{B} = (\mathsf{B}_1, \mathsf{B}_2, \dots, \mathsf{B}_s)$*. Then* ρ_{AB} *and* σ_{AB} *are* $O\left(\sum_{i=1}^{s} t^2/2^{n_i}\right)$*-LOCC indistinguishable.*

Proof. For $0 \le k \le s$, we define the (hybrid) state

$$\xi_k := \bigotimes_{i=1}^{k} \mathop{\mathbb{E}}_{|\psi_i\rangle \leftarrow \mathcal{H}_{n_i}} \left[\left(|\psi_i\rangle\langle\psi_i|^{\otimes t}\right)_{\mathsf{A}_i} \otimes \left(|\psi_i\rangle\langle\psi_i|^{\otimes t}\right)_{\mathsf{B}_i} \right] \otimes \bigotimes_{j=k+1}^{s} \left(\mathop{\mathbb{E}}_{|\psi_j\rangle \leftarrow \mathcal{H}_{n_j}} \left[|\psi_j\rangle\langle\psi_j|_{\mathsf{A}_j}^{\otimes t} \right] \otimes \mathop{\mathbb{E}}_{|\phi_j\rangle \leftarrow \mathcal{H}_{n_j}} \left[|\phi_j\rangle\langle\phi_j|_{\mathsf{B}_j}^{\otimes t} \right] \right).$$

Note that $\xi_0 = \rho$ and $\xi_s = \sigma$. By the triangle inequality, we have

$$\sup_{(A,B)} \left| \Pr[(A,B)(\rho) = 1] - \Pr[(A,B)(\sigma) = 1] \right| \le \sum_{k=0}^{s-1} \sup_{(A,B)} \left| \Pr[(A,B)(\xi_k) = 1] - \Pr[(A,B)(\xi_{k+1}) = 1] \right|,$$

where the supremum is over all LOCC adversary. We will show that for each k,

$$\begin{aligned} \sup_{(A,B)} \left| \Pr[(A,B)(\xi_k) = 1] - \Pr[(A,B)(\xi_{k+1}) = 1] \right| = \sup_{(A,B)} \Bigg| & \Pr\left[(A,B) \left(\mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{H}_{n_{k+1}}} \left[|\psi\rangle\langle\psi|_{\mathsf{A}}^{\otimes t} \otimes |\psi\rangle\langle\psi|_{\mathsf{B}}^{\otimes t} \right] \right) = 1 \right] \\ & - \Pr\left[(A,B) \left(\mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{H}_{n_{k+1}}} \left[|\psi\rangle\langle\psi|_{\mathsf{A}}^{\otimes t} \right] \otimes \mathop{\mathbb{E}}_{|\phi\rangle \leftarrow \mathcal{H}_{n_{k+1}}} \left[|\phi\rangle\langle\phi|_{\mathsf{B}}^{\otimes t} \right] \right) = 1 \right] \Bigg|, \end{aligned}$$

which then completes the proof by Theorem 7.9. It is easy to see that the LHS is at least as large as the RHS since (A, B) on the LHS can simply discard all input registers except for $(\mathsf{A}_{k+1}, \mathsf{B}_{k+1})$. To see that the RHS is at least as large as the LHS, for every (A, B) on the LHS, we define (A', B') on the RHS based on (A, B) as follows. For $0 \le i \le k$, A' samples the classical description of i.i.d. n_i-qubit Haar states $|\psi_i\rangle$ and sends them to B'.[24] They then prepare t copies of the quantum state $|\psi_i\rangle$ according to the description on registers A_i and B_i respectively. For $k + 2 \le j \le s$, A' and B' each locally sample t copies of i.i.d. n_j-qubit Haar state $|\psi_j\rangle$ and $|\phi_j\rangle$ on registers A_j and B_j respectively. They then embed their input on registers A_{k+1} and B_{k+1}, and run (A, B) respectively. Since the input of (A, B) is exactly ξ_k or ξ_{k+1}, (A', B') have the same advantage as that of (A, B). □

Moreover, we have the following corollary regarding the multi-party LOCC indistinguishability.

Corollary 7.11. *Let* $\rho_{\mathsf{P}} := \mathbb{E}_{|\psi\rangle \leftarrow \mathcal{H}_n} \left[\bigotimes_{i=1}^{m} |\psi\rangle\langle\psi|_{\mathsf{P}_i}^{\otimes t} \right]$ *and* $\sigma_{\mathsf{P}} := \bigotimes_{i=1}^{m} \mathbb{E}_{|\psi_i\rangle \leftarrow \mathcal{H}_n} \left[|\psi_i\rangle\langle\psi_i|_{\mathsf{P}_i}^{\otimes t} \right]$ *where register* $\mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_m)$. *Then* ρ_{P} *and* σ_{P} *are* $(m, O(m^2 t^2 / 2^n))$*-LOCC indistinguishable.*

Proof. Similar to the proof of Corollary 7.10, we prove it via a hybrid argument. Without loss of generality, we can assume that m is a power of 2, i.e., $m = 2^r$. Otherwise, by the monotonicity of LOCC indistinguishability, we can instead consider the smallest power of 2 that is greater than or equal to m, which only increases the advantage by a constant factor. Define the following states for $k \in \{0, 1, \ldots, r\}$:

$$\xi_k := \bigotimes_{i=0}^{2^{r-k}-1} \mathop{\mathbb{E}}_{|\psi_i\rangle \leftarrow \mathcal{H}_n} \left[\bigotimes_{j=1}^{2^k} |\psi_i\rangle\langle\psi_i|_{\mathsf{P}_{i2^k+j}}^{\otimes t} \right].$$

For each ξ_k, there are 2^{r-k} blocks, each corresponding to a Haar state. Within the i-th block, there are 2^k parties holding t-copies of the same state $|\psi_i\rangle$. By construction, $\xi_r = \rho$ and $\xi_0 = \sigma$. We will show that the LOCC distinguishing advantage between ξ_k and ξ_{k+1} is $O\left(\frac{m 2^k t^2}{2^n}\right)$. This would then implies that the LOCC distinguishing advantage between ρ and σ is $\sum_{k=0}^{r-1} O\left(\frac{m 2^k t^2}{2^n}\right) = O\left(\frac{m^2 t^2}{2^n}\right)$.

To prove the closeness between ξ_k and ξ_{k+1}, we introduce sub-hybrids $\xi_{k,\ell}$ for $\ell \in \{0, 1, \ldots, 2^{r-k}\}$. In $\xi_{k,\ell}$, the first ℓ blocks are all "split in half". That is, for any $i \in \{1, 2, \ldots, \ell\}$, in the i-th block, the first 2^{k-1} parties are holding t-copies of $|\psi_{i,0}\rangle$ and the other 2^{k-1} parties are holding t-copies of $|\psi_{i,1}\rangle$. For any

[24] Note that (A', B') are information-theoretic and thus the description can approximate the Haar state with arbitrarily small error.

$i \in \{\ell+1, \ell+2, \ldots, 2^{r-k}\}$, in the i-th block, all 2^k parties are holding t-copies of the same $|\psi_i\rangle$. Hence, the only difference between $\xi_{k,\ell}$ and $\xi_{k,\ell+1}$ is in the $(\ell+1)$-th block — in the former all 2^k parties are holding t-copies of the same $|\psi_{\ell+1}\rangle$, whereas in the latter the first 2^{k-1} parties are holding t-copies of $|\psi_{\ell+1,0}\rangle$ and the other 2^{k-1} parties are holding t-copies of $|\psi_{\ell+1,1}\rangle$. Now, we can view the first 2^{k-1} parties and the other 2^{k-1} parties as two entities. By Theorem 7.9 and setting the number of copies each party receives as $2^{k-1}t$, the LOCC distinguishing advantage between $\xi_{k,\ell}$ and $\xi_{k,\ell+1}$ is $O\left(\frac{(2^{k-1}t)^2}{2^n}\right)$. This implies that the LOCC distinguishing advantage between ξ_k and ξ_{k+1} is $O\left(\frac{2^{r-k}(2^{k-1}t)^2}{2^n}\right) = O\left(\frac{2^{r+k}t^2}{2^n}\right) = O\left(\frac{m2^kt^2}{2^n}\right)$ as desired. □

Remark 7.12. *We compare Corollary 7.11 with [Har23, Theorem 8]. Although both theorems address multi-party LOCC indistinguishability, they are incomparable for the following reasons. Corollary 7.11 is stronger in the sense that each party receives t copies of the states, as opposed to the single-copy setting in [Har23, Theorem 8]. Moreover, when $t = 1$, Corollary 7.11 implies an $O(m^2/2^n)$ bound which is better than the $O(m^2/\sqrt{2^n})$ bound given by [Har23, Theorem 8]. On the other hand, the statement of [Har23, Theorem 8] is more general since their bound holds for a large family of input states. While the input states in Corollary 7.11 are fixed to ρ and σ.*

7.3 An Optimal LOCC Haar distinguisher

We present an (optimal) LOCC Haar distinguisher with advantage $\Omega(t^2/2^n)$. Hence, the upper bound in Theorem 7.9 is tight.

Theorem 7.13. *There exists an LOCC adversary that distinguishes $\rho_{\mathsf{AB}} := \mathbb{E}_{|\psi\rangle\leftarrow\mathcal{H}_n}\left[\bigotimes_{i=1}^t |\psi\rangle\langle\psi|_{\mathsf{A}_i} \otimes \bigotimes_{i=1}^t |\psi\rangle\langle\psi|_{\mathsf{B}_i}\right]$ from $\sigma_{\mathsf{AB}} := \mathbb{E}_{|\psi\rangle\leftarrow\mathcal{H}_n}\left[\bigotimes_{i=1}^t |\psi\rangle\langle\psi|_{\mathsf{A}_i}\right] \otimes \mathbb{E}_{|\phi\rangle\leftarrow\mathcal{H}_n}\left[\bigotimes_{i=1}^t |\phi\rangle\langle\phi|_{\mathsf{B}_i}\right]$ with advantage $\Omega(t^2/2^n)$, where $\mathsf{A} = (\mathsf{A}_1, \ldots, \mathsf{A}_t)$ and $\mathsf{B} = (\mathsf{B}_1, \ldots, \mathsf{B}_t)$. Moreover, the running time is polynomial in t and n.*

Proof. The LOCC adversary (A, B) is defined as follows. For $1 \le i \le t$, A measures register A_i in the computational basis and obtains the outcome $a_i \in \{0,1\}^n$. Similarly, B measures every B_i in the computational basis and obtains b_i. Then B sends $b_1, b_2, \ldots, b_t$ to A, and A outputs 1 if there is no collision among $a_1, a_2, \ldots, a_t, b_1, b_2, \ldots, b_t$. Let $d := 2^n$. The distinguishing advantage can be lower bounded as follows:

$$
\begin{aligned}
&\Pr[(A,B)(\sigma_{\mathsf{AB}}) = 1] - \Pr[(A,B_{\mathsf{AB}})(\rho) = 1] \\
&= \Pr_{T_1,T_2\leftarrow[0:t]^d}[T_1, T_2 \text{ are collision-free } \wedge T_1, T_2 \text{ are disjoint}] - \Pr_{T\leftarrow[0:2t]^d}[T \text{ is collision-free}] \\
&= \frac{\binom{d}{t}\binom{d-t}{t}}{\binom{d+t-1}{t}^2} - \frac{\binom{d}{2t}}{\binom{d+2t-1}{2t}} \\
&= \frac{\binom{d}{2t}}{\binom{d+2t-1}{2t}} \cdot \left(\frac{\binom{d}{t}\binom{d-t}{t}\binom{d+2t-1}{2t}}{\binom{d+t-1}{t}^2\binom{d}{2t}} - 1\right) \\
&= \prod_{i=0}^{2t-1}\left(1 - \frac{2t-1}{d+i}\right) \cdot \left(\prod_{i=0}^{t-1}\left(1 + \frac{t}{d+i}\right) - 1\right) \\
&= \left(1 - O\left(\frac{t^2}{d}\right)\right) \cdot \left(1 + \Omega\left(\frac{t^2}{d}\right) - 1\right) = \Omega\left(\frac{t^2}{d}\right),
\end{aligned}
$$

where the first equality follows from the fact that $\sigma_{\mathsf{AB}} = \mathbb{E}_{T_1,T_2\leftarrow[0:t]^d}[|T_1\rangle\langle T_1|_{\mathsf{A}} \otimes |T_2\rangle\langle T_2|_{\mathsf{B}}]$ and $\rho_{\mathsf{AB}} = \mathbb{E}_{T\leftarrow[0:2t]^d}[|T\rangle\langle T|_{\mathsf{AB}}]$. □

8 Impossibilities of QCCC Primitives in the CHS model

In this section, we investigate the impossibility of *statistically* secure quantum-computation classical-communication (QCCC) primitives in the CHS model. A recent work by Khurana and Tomer [KT24]

proposed the notion of *one-way puzzles*, which involves a QPT sampler that outputs a classical puzzle-solution pair $(\mathsf{Puz}, \mathsf{Sol})$ satisfying a relation, which may not be efficiently computable. In addition, they show that many QCCC primitives imply one-way puzzles. In a very recent work by Chung, Goldin and Gray [CGG24], the authors observed that certain QCCC primitives possess an efficient verification algorithm, and they defined a special class of one-way puzzles called *efficiently verifiable one-way puzzles*. In particular, since we are considering impossibility results, we will focus on the following (fairly weak) form of one-way puzzles in the CHS model.

Definition 8.1 (One-way puzzles in the CHS model)**.** *A one-way puzzle is a pair of sampling and verification algorithms* $(\mathsf{Samp}, \mathsf{Ver})$ *with the following syntax. Let* $q = q(\lambda)$ *be an arbitrary polynomial and* $n = n(\lambda) = \omega(\log(\lambda))$.

- $\mathsf{Samp}(1^\lambda, \rho) \to (\mathsf{Puz}, \mathsf{Sol})$*, is a (possibly time-inefficient) quantum algorithm that on input the security parameter and a* 2^{nq}*-dimensional quantum state* ρ *(ideally,* ρ *will be* q *copies of an* n*-qubit Haar state), outputs a pair of* classical *strings* $(\mathsf{Puz}, \mathsf{Sol})$*. We refer to* Puz *as the* puzzle *and* Sol *as its* solution*.*
- $\mathsf{Ver}(\mathsf{Puz}, \mathsf{Sol}, \rho) \to \top$ *or* $\bot$*, is a (possibly time-inefficient) quantum algorithm that on input any pair of classical strings* $(\mathsf{Puz}, \mathsf{Sol})$ *and a* 2^{nq}*-dimensional quantum state* ρ *(ideally,* ρ *is the same state used to generate the puzzle), outputs either* $\top$ *(indicating accept) or* $\bot$ *(indicating reject).*

These satisfy the following properties.

- ***Completeness.*** *The correctness guarantee states that as long as* Samp *and* Ver *get the same copy of* ρ*, which in turn is* q *copies of an* n*-qubit Haar state, the output of the sampler will pass the verification with overwhelming probability. That is,*

$$\Pr\left[\mathsf{Ver}(\mathsf{Puz}, \mathsf{Sol}, |\psi\rangle^{\otimes q}) = \top : \substack{|\psi\rangle \leftarrow \mathcal{H}_n, \\ (\mathsf{Puz},\mathsf{Sol}) \leftarrow \mathsf{Samp}(1^\lambda, |\psi\rangle^{\otimes q})}\right] = 1 - \mathsf{negl}(\lambda).$$

- ***Security.*** *Given* Puz*, it is statistically infeasible to find* Sol *satisfying* $\mathsf{Ver}(\mathsf{Puz}, \mathsf{Sol}) = \top$*, i.e., for every unbounded adversary* A*,*[25]

$$\Pr\left[\mathsf{Ver}(\mathsf{Puz}, \mathsf{Sol}', |\psi\rangle^{\otimes q}) = \top : \substack{|\psi\rangle \leftarrow \mathcal{H}_n, \\ (\mathsf{Puz},\mathsf{Sol}) \leftarrow \mathsf{Samp}(1^\lambda, |\psi\rangle^{\otimes q}), \\ \mathsf{Sol}' \leftarrow A(\mathsf{Puz})}\right] = \mathsf{negl}(\lambda).$$

Definition 8.2 (QCCC key agreements in the CHS model)**.** *A QCCC key agreement in the CHS model is a two-party interactive protocol consisting of a pair of QPT algorithms* (A, B) *with their communication being classical. Let* $q = q(\lambda)$ *be an arbitrary polynomial and* $n = n(\lambda) = \omega(\log(\lambda))$*.* A, B *each take as input the security parameter* 1^λ *and a* 2^{nq}*-dimensional quantum state (ideally,* A *and* B *each obtain* q *copies of an* n*-qubit Haar state), and outputs classical keys* $k_A \in \{0,1\}$ *and* $k_B \in \{0,1\}$ *respectively.*[26]

- ***Completeness.*** *There exists a negligible function* negl *such that for all* $\lambda \in \mathbb{N}$*,*

$$\Pr\left[k_A = k_B : \substack{|\psi\rangle \leftarrow \mathcal{H}_n, \\ (k_A,k_B,\tau) \leftarrow \langle A(1^\lambda, |\psi\rangle^{\otimes q}), B(1^\lambda, |\psi\rangle^{\otimes q})\rangle}\right] \geq 1 - \mathsf{negl}(\lambda),$$

  where $\langle A, B\rangle$ *denote the execution of the protocol and* τ *is the transcript of the protocol.*

- ***Statistical Security.*** *For every computationally unbounded eavesdropper* E*, there exists a negligible function* negl *such that for all* $\lambda \in \mathbb{N}$*,*[27]

$$\Pr\left[k_E = k_B : \substack{|\psi\rangle \leftarrow \mathcal{H}_n, \\ (k_A,k_B,\tau) \leftarrow \langle A(1^\lambda, |\psi\rangle^{\otimes q}), B(1^\lambda, |\psi\rangle^{\otimes q})\rangle, \\ k_E \leftarrow E(1^\lambda, \tau)}\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

[25] Note that the security definition is weak in the sense that the adversary is *not* given any copy of the common Haar state.
[26] Since we are proving negative results, we assume that the key space of the key agreement is $\{0,1\}$, i.e., a bit agreement.
[27] Similarly, we consider a weak security definition in which the eavesdropper is not given any common Haar state.

There are various definitions of binding for quantum commitments in literature. Since we are showing impossibility, we focus on sum-binding, which is implied by binding for classical commitments. Similarly, we assume that the input space is $\{0,1\}$, i.e., a bit commitment.

Definition 8.3 (QCCC interactive commitments in the CHS model)**.** *A QCCC commitment in the CHS model is a two-party interactive protocol consisting of a pair of QPT algorithms (C,R), where C is the committer and R is the receiver, with their communication being classical. Let $q=q(\lambda)$ be an arbitrary polynomial and $n=n(\lambda)=\omega(\log(\lambda))$.*

- ***Commit Phase:*** *In the (possibly interactive) commit phase, C takes as input the security parameter 1^λ, a bit $b\in\{0,1\}$ and a 2^{nq}-dimensional quantum state ρ_C, and R takes as input the security parameter 1^λ and a 2^{nq}-dimensional quantum state ρ_R (ideally, C and R each obtain q copies of an n-qubit Haar state). We denote the execution of the commit phase by $(\sigma_{CR},\tau)\leftarrow\mathsf{Commit}\langle C(1^\lambda,b,\rho_C),R(1^\lambda,\rho_R)\rangle$, where σ_{CR} is the joint state of C and R after the commit phase, and τ denotes the transcript in the commit phase.*
- ***Reveal Phase:*** *In the (possibly interactive) reveal phase, the output is $\mu\in\{0,1,\bot\}$ indicating the receiver's output bit or abort. We denote the execution of the reveal phase by $\mu\leftarrow\mathsf{Reveal}\langle C,R,\sigma_{CR},\tau\rangle$.*

The scheme satisfies the following conditions.

- ***Completeness.*** *There exists a negligible function negl such that for all $\lambda\in\mathbb{N}$,*

$$\Pr\left[\mu=b:\begin{array}{c}|\psi\rangle\leftarrow\mathcal{H}_n,\\ b\leftarrow\{0,1\},\\ (\sigma_{CR},\tau)\leftarrow\mathsf{Commit}\langle C(1^\lambda,b,|\psi\rangle^{\otimes q}),R(1^\lambda,|\psi\rangle^{\otimes q})\rangle,\\ \mu\leftarrow\mathsf{Reveal}\langle C,R,\sigma_{CR},\tau\rangle,\\ \mu\in\{0,1,\bot\}\end{array}\right]\geq 1-\mathsf{negl}(\lambda).$$

- ***Statistical Hiding.*** *For every computationally unbounded malicious receiver R^*, there exists a negligible function negl such that for all $\lambda\in\mathbb{N}$,*

$$\Pr\left[b'=b:\begin{array}{c}|\psi\rangle\leftarrow\mathcal{H}_n,\\ b\leftarrow\{0,1\},\\ (\sigma_{CR^*},\tau)\leftarrow\mathsf{Commit}\langle C(1^\lambda,b,|\psi\rangle^{\otimes q}),R^*(1^\lambda,|\psi\rangle^{\otimes q})\rangle,\\ b'\leftarrow R^*(\sigma_{R^*},\tau)\end{array}\right]\leq\frac{1}{2}+\mathsf{negl}(\lambda),$$

  where σ_{R^*} denotes the state obtained by tracing out the committer's part of the state σ_{CR^*}.

- ***Statistical Binding.*** *For every computationally unbounded malicious committer C^*, there exists a negligible function negl such that for all $\lambda\in\mathbb{N}$,*

$$\Pr\left[\mu=b:\begin{array}{c}|\psi\rangle\leftarrow\mathcal{H}_n,\\ (\sigma_{C^*R},\tau)\leftarrow\mathsf{Commit}\langle C^*(1^\lambda,|\psi\rangle^{\otimes q}),R(1^\lambda,|\psi\rangle^{\otimes q})\rangle,\\ b\leftarrow\{0,1\},\\ \mu\leftarrow\mathsf{Reveal}\langle C^*(b),R,\sigma_{C^*R},\tau\rangle\end{array}\right]\leq\frac{1}{2}+\mathsf{negl}(\lambda).$$

Theorem 8.4. *There does not exist primitive $\mathcal{P}$ in the CHS model where $\mathcal{P}\in\{$one-way puzzles, statistically secure QCCC key agreements, statistically hiding and statistically binding QCCC interactive commitments$\}$.*

Proof intuition. The high-level idea is to convert the scheme in the CHS model to a scheme in the *plain* model. In the CHS model, given a pair of algorithms, we define the new pair of (time-inefficient) algorithms to be identical except for their input, which consists of copies of two i.i.d Haar states. Thanks to the LOCC Haar indistinguishability (Theorem 7.9), the expense of doing so is to only increase the completeness error and security loss by a negligible amount. Therefore, if there were to exist a complete and secure scheme in the CHS model, it would imply the existence of such a scheme in the plain model, contradicting the trivial impossibility.[28]

[28] The impossibilities in the plain model still hold even when the algorithms of the primitives are time-inefficient.

Proof of Theorem 8.4.

One-way puzzles. Suppose there exists a one-way puzzle $(\mathsf{Samp}, \mathsf{Ver})$ in the CHS model. We define $(\widetilde{\mathsf{Samp}}, \widetilde{\mathsf{Ver}})$ as follows. $\widetilde{\mathsf{Samp}}(1^\lambda)$ simply samples q copies of a Haar state $|\psi\rangle$ and runs $\mathsf{Samp}(1^\lambda, |\psi\rangle^{\otimes q})$. $\widetilde{\mathsf{Ver}}(\mathsf{Puz}, \mathsf{Sol})$ is defined similarly; it samples q copies of a Haar state $|\phi\rangle$ and then runs $\mathsf{Ver}(\mathsf{Puz}, \mathsf{Sol}, |\phi\rangle^{\otimes q})$. It is important to note that $\widetilde{\mathsf{Samp}}$ and $\widetilde{\mathsf{Ver}}$ sample the Haar states independently.

First, we claim that $(\widetilde{\mathsf{Samp}}, \widetilde{\mathsf{Ver}})$ has negligible completeness error. Otherwise, we construct an LOCC distinguisher (A, B) with a non-negligible advantage for the task in Theorem 7.9. A runs Samp on the security parameter and her input, obtains $(\mathsf{Puz}, \mathsf{Sol})$, and sends $(\mathsf{Puz}, \mathsf{Sol})$ to B. Then B runs Ver on $(\mathsf{Puz}, \mathsf{Sol})$ and his input, and outputs 1 if the verification passes. If the input of (A, B) is ρ (defined in Theorem 7.9, i.e., each is given q copies of the same Haar state), then the probability of B outputting 1 is equal to the completeness of $(\mathsf{Samp}, \mathsf{Ver})$. Similarly, if the input is σ (i.e., each is given q copies of two i.i.d Haar states), then the probability of B outputting 1 is equal to the completeness of $(\widetilde{\mathsf{Samp}}, \widetilde{\mathsf{Ver}})$. Hence, (A, B) has a non-negligible advantage by the premise. However, this contradicts Theorem 7.9.

Next, we claim that $(\widetilde{\mathsf{Samp}}, \widetilde{\mathsf{Ver}})$ satisfies security. Suppose there is an adversary $\widetilde{E}$ that breaks the security of $(\widetilde{\mathsf{Samp}}, \widetilde{\mathsf{Ver}})$ with a non-negligible advantage of $\widetilde{\varepsilon} = \widetilde{\varepsilon}(\lambda)$. We claim that $\widetilde{E}$ breaks the security of $(\mathsf{Samp}, \mathsf{Ver})$ with an advantage of $\varepsilon = \varepsilon(\lambda)$ satisfying $|\varepsilon - \widetilde{\varepsilon}| = \mathsf{negl}(\lambda)$, which means that $\widetilde{\varepsilon}$ is non-negligible as well. Otherwise, suppose $|\varepsilon - \widetilde{\varepsilon}|$ is non-negligible, we can construct an LOCC distinguisher (A, B) as follows.

- A runs Samp on the security parameter and her input to obtain $(\mathsf{Puz}, \mathsf{Sol})$. It then runs $\widetilde{E}$ on Puz to obtain Sol'. Finally, it sends $(\mathsf{Puz}, \mathsf{Sol}')$ to B.
- B runs Ver on $(\mathsf{Puz}, \mathsf{Sol}')$. If the output is $\bot$, it outputs 1. Otherwise, it outputs 0.

If the input of (A, B) is ρ (defined in Theorem 7.9, i.e., each is given q copies of the same Haar state), then the probability of B outputting 1 is equal to ε. Similarly, if the input is σ (i.e., each is given q copies of two i.i.d Haar states), then the probability of B outputting 1 is $\widetilde{\varepsilon}$. Again, this contradicts Theorem 7.9.

So far, we have shown that $(\widetilde{\mathsf{Samp}}, \widetilde{\mathsf{Ver}})$ satisfies completeness and security in the plain model. However, such a scheme cannot exist. This is because an unbounded adversary, given a puzzle, can find the solution with the highest probability of passing the verification to break the security. Hence, we conclude that $(\mathsf{Samp}, \mathsf{Ver})$ is not a one-way puzzle in the CHS model.

The structure of proving the impossibility of key agreements and interactive commitments is very similar. We only describe the LOCC distinguishers and omit the full details.

Key agreements. Suppose $\mathsf{KA} = (P_1, P_2)$ is a statistically secure QCCC key agreement in the CHS model. Define $\widetilde{\mathsf{KA}} = (\widetilde{P_1}, \widetilde{P_2})$ such that $\widetilde{P_1}$ (resp., $\widetilde{P_2}$) samples q copies of a Haar state and they run P_1 (resp., P_2). We argue that $\widetilde{\mathsf{KA}}$ satisfies both completeness and security.

Suppose completeness error of $\widetilde{\mathsf{KA}}$ is inverse polynomial (in λ), we define an LOCC adversary (A, B) as follows. Upon receiving a bipartite state on registers A and B, A (resp., B) runs P_1 (resp., P_2) on input 1^λ and the register A (resp., B). Then, A obtains the key k_{P_1} and B obtains the key k_{P_2}. They perform an extra round of communication to check if $k_{P_1} = k_{P_2}$. Similar to the argument for one-way puzzles, it can be shown that (A, B) can distinguish ρ and σ (defined in Theorem 7.9) with inverse polynomial probability, which is a contradiction.

Suppose $\widetilde{\mathsf{KA}}$ is not statistically secure. That is, there exists an eavesdropper $\widetilde{E}$ that can break the security of $\widetilde{\mathsf{KA}}$ with inverse polynomial (in λ) probability. Using $\widetilde{E}$, we define an LOCC adversary (A, B), who upon receiving a bipartite state on two registers A and B do the following.

- A runs P_1 on 1^λ and the register A. Similarly, B runs P_2 on 1^λ and the register B. Denote τ be the transcript of the protocol.
- B runs $\widetilde{E}(\tau)$ to obtain k_E. It then checks if $k_E = k_{P_2}$. If so, it outputs 1. Otherwise, it outputs 0.

Similarly, as before, we can show that (A, B) succeeds in distinguishing ρ and σ with inverse polynomial probability, a contradiction.

So far, we have shown that $\widetilde{\mathsf{KA}}$ is a key agreement protocol in the plain model that satisfies both completeness and statistical security. However, such a scheme cannot exist which further means that KA either does not satisfy completeness or security.

Interactive Commitments. Suppose $\mathsf{Com} = (C, R)$ is a statistically hiding and statistically binding QCCC interactive commitment in the CHS model. We define $\widetilde{\mathsf{Com}} = (\widetilde{C}, \widetilde{R})$ as follows. Upon receiving the input bit $b \in \{0,1\}$, $\widetilde{C}$ simply samples q copies of a Haar state $|\psi\rangle$ and runs C on input 1^λ, b and $|\psi\rangle^{\otimes q}$. Similarly, $\widetilde{R}$ samples q copies of a Haar state $|\phi\rangle$ and runs R on input 1^λ and $|\phi\rangle^{\otimes q}$.

Intuitively, $\widetilde{\mathsf{Com}}$ is at least as secure as Com since the malicious party in $\widetilde{\mathsf{Com}}$ has no information about the other party's Haar state as opposed to Com. Suppose $\widetilde{\mathsf{Com}}$ is not statistically hiding. That is, there exists a malicious receiver $\widetilde{R}^*$ that can break the statistical hiding of $\widetilde{\mathsf{Com}}$ with inverse polynomial (in λ) probability. Using $\widetilde{R}^*$, we define a malicious receiver R^* that breaks the statistical hiding of Com. R^* simply discards its common Haar states and runs $\widetilde{R}^*$. Then the distinguishing advantage of R^* is identical to that of $\widetilde{R}^*$, which is a contradiction. Suppose $\widetilde{\mathsf{Com}}$ is not statistically binding. That is, there exists a malicious receiver $\widetilde{C}^*$ that can break the statistical binding of $\widetilde{\mathsf{Com}}$ with inverse polynomial (in λ) probability. Similarly, discarding the common Haar states and using $\widetilde{C}^*$ breaks the statistical binding of Com, which is a contradiction.

Suppose completeness error of $\widetilde{\mathsf{Com}}$ is inverse polynomial (in λ), we define an LOCC adversary (A, B) as follows. Upon receiving a bipartite state on registers A and B, A (resp., B) runs C (resp., R) on input 1^λ, a uniform bit $b \in \{0,1\}$, and the register A (resp., B). Then, B obtains μ. They perform an extra round of communication to check if $b = \mu$. Similar to the argument for one-way puzzles, it can be shown that (A, B) can distinguish ρ and σ (defined in Theorem 7.9) with inverse polynomial probability, which is a contradiction. □

9 Quantum Black-Box Separation in the QCCC Model

9.1 The Separating Oracle

As is common in black-box impossibility results, we will define oracles relative to which $\omega(\log(\lambda))$-PRSGs exist while QCCC key agreements and interactive commitments do not. We define the oracle $G := \{\{G_k\}_{k\in\{0,1\}^\lambda}\}_{\lambda\in\mathbb{N}}$ as follows. For every $\lambda \in \mathbb{N}$ and $k \in \{0,1\}^\lambda$, the oracle G_k is a Haar isometry that maps any state $|\psi\rangle$ to $|\psi\rangle|\vartheta_k\rangle$, where $|\vartheta_k\rangle$ is a Haar state of length $n(\lambda) = \omega(\log(\lambda))$. The existence of $\omega(\log(\lambda))$-PRSGs relative to G can be proven easily.

Lemma 9.1 ($(\lambda, \omega(\log(\lambda)))$-PRSGs exist relative to G)**.** *There exists a $(\lambda, \omega(\log(\lambda)))$-PRSG relative to G. In particular, for any polynomial $q(\cdot)$ and any computationally unbounded adversary A^G that takes as input 1^λ and asks $q(\lambda)$ quantum queries to G, the distinguishing advantage is negligible in λ.*

Proof sketch. The proof is similar to the proof of [Kre21, Lemma 30]. The implementation of the PRSG is simply the oracle G: on input k, outputs the state $|\vartheta_k\rangle$ generated by G_k. The security follows from the hardness of the unstructed search problem [BBBV97]. □

9.2 Separating QCCC Key Agreements from $(\lambda, \omega(\log(\lambda)))$-PRSGs

Definition 9.2 (QCCC key agreements relative to oracle)**.** *A* QCCC key agreement relative to an oracle $\mathcal{O}$ *is a two-party interactive protocol consisting of a pair of uniform quantum (possibly time-inefficient) oracle algorithms (A, B) such that A, B each take as input the security parameter 1^λ, ask $q(\lambda)$ queries to the oracle $\mathcal{O}$ for some polynomial q, communicate classically, and output the classical keys $k_A \in \{0,1\}$ and $k_B \in \{0,1\}$ respectively. An* (ε, p, δ)-QCCC key agreement relative to $\mathcal{O}$ *satisfies the following:*

- ***ε-completeness.*** *We say that a QCCC key agreement is* ε-complete *if the following holds for all* $\lambda \in \mathbb{N}$*,*

$$\Pr\left[k_A = k_B : \substack{O\leftarrow\mathcal{O},\\ (k_A,k_B,\tau)\leftarrow\langle A^O(1^\lambda),B^O(1^\lambda)\rangle}\right] \geq 1-\varepsilon(\lambda),$$

where $\langle A, B\rangle$ *denote the execution of the protocol and* τ *is the transcript of the protocol. We anticipate that* ε *is negligible.*

- (p,δ)***-security.*** *We say that a QCCC key agreement is* (p,δ)-secure *if for any computationally unbounded eavesdropper* E *that on input* 1^λ *and transcript* τ *and asks at most* $p(\lambda)$ *classical queries to* $\mathcal{O}$*, the following holds for all* $\lambda \in \mathbb{N}$*,*

$$\Pr\left[k_E = k_B : \substack{O\leftarrow\mathcal{O},\\ (k_A,k_B,\tau)\leftarrow\langle A^O(1^\lambda),B^O(1^\lambda)\rangle,\\ k_E\leftarrow E^O(1^\lambda,\tau)}\right] \leq \frac{1}{2}+\delta(\lambda).$$

We anticipate that for any polynomial p*, there exists a negligible* δ *such that the key agreement is* (p,δ)*-secure.*

In the plain model, completeness and security are defined similarly in the absence of an oracle. In particular, a QCCC key agreement is an (ε,δ)-*QCCC key agreement* if it satisfies ε-completeness and δ-security.

Lemma 9.3 (Conditional independence)**.** *For any two-party interactive QCCC protocol* (A,B) *where the party's initial state is a product state, the joint state at the end of each round* i *can be written as*

$$\sum_{t^i} p_{t^i}|t^i\rangle\langle t^i|_{\mathsf{T}} \otimes \rho^{t^i}_{\mathsf{AB}},$$

for some partial transcripts $t^i := (t_1, t_2, \ldots, t_i)$ *until round* i *and product states* $\rho^{t^i}_{\mathsf{AB}}$*, where register* T *is for storing the transcript.*

Proof. We prove it by induction on rounds. Initially, the joint state is $|\bot\rangle\langle\bot|_{\mathsf{T}}\otimes\rho^{\bot}_{\mathsf{A}}\otimes\rho^{\bot}_{\mathsf{B}}$ by the premise, where $\bot$ denotes the empty transcript. Suppose after the j-th round, the joint state is $\sum_{t^j} p_{t^j}|t^j\rangle\langle t^j|_{\mathsf{T}}\otimes\rho^{t^j}_{\mathsf{A}}\otimes\rho^{t_j}_{\mathsf{B}}$. In the $(j+1)$-th round (suppose it is A's round), A will first apply a unitary controlled by t^j of the form $\sum_{t^j}|t^j\rangle\langle t^j|_{\mathsf{T}}\otimes U^{(t^j)}_{\mathsf{A}}$ and then perform the measurement to generate the message t_{j+1} of this round. Then the state $\rho^{t^j}_{\mathsf{A}}$ becomes $\sum_{t_{j+1}}|t_{j+1}\rangle\langle t_{j+1}|_{\mathsf{T}_{j+1}}\otimes\left((\langle t_{j+1}|\otimes I)U^{(t^j)}_{\mathsf{A}}\rho^{t^j}_{\mathsf{A}}\left(U^{(t^j)}_{\mathsf{A}}\right)^\dagger(|t_{j+1}\rangle\otimes I)\right)$, where register T_{j+1} is appended to the transcript register. We can write $\left((\langle t_{j+1}|\otimes I)U^{(t^j)}_{\mathsf{A}}\rho^{t^j}_{\mathsf{A}}\left(U^{(t^j)}_{\mathsf{A}}\right)^\dagger(|t_{j+1}\rangle\otimes I)\right)$ as $p(t_{j+1}|t^j)\cdot\rho^{t^j||t_{j+1}}_{\mathsf{A}}$, where $p(t_{j+1}|t^j)$ is the probability of getting the outcome t_{j+1} by measuring $U^{(t^j)}_{\mathsf{A}}\rho^{t^j}_{\mathsf{A}}\left(U^{(t^j)}_{\mathsf{A}}\right)^\dagger$ in the computational basis. Hence we get that the final state is

$$\sum_{t^j}\sum_{t_{j+1}} p_{t^j}p(t_{j+1}|t^j)\cdot|t^j||t_{j+1}\rangle\langle t^j||t_{j+1}|_{\mathsf{T}}\otimes\rho^{t^j||t_{j+1}}_{\mathsf{A}}\otimes\rho^{t_j}_{\mathsf{B}},$$

which is still a product state for any $t^{j+1} = t^j||t_{j+1}$. □

Lemma 9.4 (Impossibility of key agreements in the plain model)**.** *For any* $\varepsilon,\delta:\mathbb{N}\to[0,1]$ *and* (ε,δ)*-QCCC key agreement in the plain model, it holds that* $\varepsilon(\lambda)+\delta(\lambda)\geq 1/2$ *for any* $\lambda\in\mathbb{N}$*.*

Proof. Let KA be an (ε,δ)-QCCC key agreement in the plain model that outputs (τ,k_A,k_B). Fix λ for the rest of the proof. In execution of KA, equivalently, we can first sample τ, then sample k_B conditioned on τ, and finally sample k_A conditioned on (τ,B). For any fixed τ in the support, by Lemma 9.3, the joint state of A and B is a product state. Thus, further fixing k_B won't change the marginal distribution of k_A. In the rest of the proof, we fix τ and k_B.

Consider the following eavesdropper E. Upon receiving the transcript τ, E runs the protocol coherently and computes the post-measurement state conditioned on τ. Then E sets k_E to k_A computed from the final joint state. Hence, the distribution of k_E is identically distributed to the marginal distribution of k_A in KA conditioned on τ. That is, the probability of $k_E = k_B$ is equal to that of $k_A = k_B$. Finally, averaging over (τ, k_B), we have the probability of $k_E = k_B$ is $\geq 1 - \varepsilon(\lambda) = 1/2 + (1/2 - \varepsilon(\lambda))$ from the ε-completeness of KA. In other words, $\delta(\lambda)$ must be $\geq 1/2 - \varepsilon(\lambda)$. Hence, we have $\delta(\lambda) + \varepsilon(\lambda) \geq 1/2$ for any $\lambda \in \mathbb{N}$. □

Theorem 9.5 (Quantum state tomography [OW16])**.** *There exists an algorithm* $\mathsf{Tomography}$ *and a polynomial* $p_{\mathsf{Tomography}}$ *satisfy the following. For any* $d \in \mathbb{N}, \Delta, \gamma \in (0,1]$ *and* d*-dimensional pure quantum state* $|\psi\rangle\langle\psi|$*, given* $p_{\mathsf{Tomography}}(d, \Delta^{-1}, \log(\gamma^{-1}))$ *copies of* $|\psi\rangle\langle\psi|$*,* $\mathsf{Tomography}$ *outputs the classical description of* $|\widehat{\psi}\rangle\langle\widehat{\psi}|$ *satisfying* $\mathsf{TD}(|\psi\rangle\langle\psi|, |\widehat{\psi}\rangle\langle\widehat{\psi}|) \leq \Delta$ *with probability at least* $1 - \gamma$*.*

Lemma 9.6 (Compling out G from KA^G)**.** *If QCCC key agreements relative to* G *(the keyed common Haar state oracle defined in Section 9.1) exist, then there exists an* (ε, δ)*-QCCC key agreement in the plain model such that* $\varepsilon(\lambda)$ *is an inverse polynomial and* $\delta(\lambda) \leq 0.2$ *for sufficiently large* $\lambda \in \mathbb{N}$*.*

Proof. Let $\mathsf{KA}^G = (A^G, B^G)$ be a QCCC key agreement relative to $G = \{\{G_k\}_{k\in\{0,1\}^\lambda}\}_{\lambda\in\mathbb{N}}$ in which A and B each ask $q(\lambda) = \mathsf{poly}(\lambda)$ queries with the maximum input length of the queries being $L(\lambda) = \mathsf{poly}(\lambda)$. Define $\Lambda(\lambda) := \lceil \log(q^{10} + L^{10} + \lambda^{10}) \rceil = O(\log(\lambda))$ and the "truncated" oracle $G_\Lambda = \{\{G_k\}_{k\in\{0,1\}^i}\}_{i=1}^{\Lambda}$. We define the following hybrid protocol $\widetilde{\mathsf{KA}}^{G_\Lambda} = (\widetilde{A}^{G_\Lambda}, \widetilde{B}^{G_\Lambda})$:

$\widetilde{\mathsf{KA}}^{G_\Lambda}(1^\lambda, \widetilde{A}^{G_\Lambda}, \widetilde{B}^{G_\Lambda})$:

1. For every $k \in \bigcup_{i=\Lambda+1}^{L}\{0,1\}^i$, $\widetilde{A}$ and $\widetilde{B}$ samples $|\phi_k^A\rangle, |\phi_k^B\rangle \leftarrow \mathcal{H}_{|k|}$ respectively.
2. $(\widetilde{A}^{G_\Lambda}, \widetilde{B}^{G_\Lambda})$ runs (A^G, B^G) on 1^λ by answering the queries as follows: Suppose A asks a query $k \in \bigcup_{i=1}^{L}\{0,1\}^i$. If $|k| \leq \Lambda$, then $\widetilde{A}$ asks k to oracle G_Λ and forwards the response. Otherwise, $\widetilde{A}$ sends $|\phi_k^A\rangle$ to A. $\widetilde{B}$ answers the queries of B similarly by replacing $|\phi_k^A\rangle$ with $|\phi_k^B\rangle$.
3. $\widetilde{A}$ outputs the key k_A generated by A and $\widetilde{B}$ outputs key k_B generated by B.

$\widetilde{\mathsf{KA}}^{G_\Lambda}$ is query-efficient. Since $(\widetilde{A}^{G_\Lambda}, \widetilde{B}^{G_\Lambda})$ needs to sample Haar states in Step 1, $\widetilde{\mathsf{KA}}^{G_\Lambda}$ is not time-efficient. However, each of $\widetilde{A}^{G_\Lambda}, \widetilde{B}^{G_\Lambda}$ makes at most q queries in Step 2 in $\widetilde{\mathsf{KA}}^{G_\Lambda}$.

$\widetilde{\mathsf{KA}}^{G_\Lambda}$ is $1/\mathsf{poly}$-complete. First, we prove that $\widetilde{\mathsf{KA}}^{G_\Lambda}$ satisfies completeness. The idea is similar to the proof of Theorem 8.4. Define LOCC distinguisher $(A_{\mathsf{LOCC}}, B_{\mathsf{LOCC}})$ for the task in Corollary 7.10 with the following parameters: $t = 2q$, $n_{2qi+j} = \Lambda + i + 1$ for $i = 0, 1, \ldots, L - \Lambda - 1$ and $j = 1, 2, \ldots, 2q$, and thus $s = (L - \Lambda) \cdot 2q$:[29]

1. A_{LOCC} and B_{LOCC} receive input register.
2. A_{LOCC} samples oracle G_Λ and sends its description to B_{LOCC}.
3. A_{LOCC} and B_{LOCC} initialize lists $\mathcal{L}_\ell = \{(1, \bot), (2, \bot), \ldots, (2q, \bot)\}$ for answering queries of different lengths $\ell = \Lambda + 1, \Lambda + 2, \ldots, \lambda$ (let $\mathcal{L} := \{\mathcal{L}_\ell\}_{\ell\in[\Lambda+1:L]}$), and runs $\mathsf{KA}^{(\cdot)} = (A^{(\cdot)}, B^{(\cdot)})$ on 1^λ by lazy evaluation and jointly maintaining the list $\mathcal{L}$ as follows:

   In the r-th round (suppose it's A_{LOCC}'s round), upon received the message t_{r-1} and list $\mathcal{L}$ from B_{LOCC} in the $(r-1)$-th round, A_{LOCC} feeds t_{r-1} to A.[30] Upon receiving A's query $x \in \bigcup_{i=1}^{L}\{0,1\}^i$, if $|x| \leq \Lambda$,

[29] For $k \in [s]$, we represent the k-th state by $|\psi_{i+\Lambda+1}^j\rangle$ ($|\phi_{i+\Lambda+1}^j\rangle$ resp.) where i, j are determined by uniquely writing $k = 2qi + j$ for $i = 0, 1, \ldots, L - \Lambda - 1$ and $j = 1, 2, \ldots, 2q$.

[30] In the first round (suppose it's A_{LOCC}'s round), A_{LOCC} simply runs A on input the security parameter and $t_0 := \bot$.

then A_{LOCC} uses G_Λ to answer the query. Otherwise, A_{LOCC} checks if (i,x) is in $\mathcal{L}_{|x|}$ for some $i \in [2q]$ (i.e., whether x has already been queried by A or B). If $(i,x) \in \mathcal{L}_{|x|}$, then A_{LOCC} answers the query using a copy of $|\psi^i_{|x|}\rangle$. Otherwise, A_{LOCC} finds the first index $i \in [2q]$ such that $(i,\bot) \in \mathcal{L}_{|x|}$, updates it into (i,x), and answers the query using a copy of $|\psi^i_{|x|}\rangle$. At the end of the round, A outputs a classical message t_r. Then A_{LOCC} sends $\mathcal{L}$ and t_r to B_{LOCC}.[31]

4. At the end of the protocol, A, B outputs the keys k_A, k_B respectively.
5. A_{LOCC} sends k_A to B_{LOCC}, and B_{LOCC} outputs 1 if $k_A = k_B$.

Hence, (A,B) asks at most $2q$ queries in total, $(A_{\mathsf{LOCC}}, B_{\mathsf{LOCC}})$ perfectly simulates either KA^G or $\widetilde{\mathsf{KA}}^{G_\Lambda}$ depending on if they obtained the same states or i.i.d. states. Hence, by Corollary 7.10 we have

$$\left|\Pr_{\mathsf{KA}^G}[k_A = k_B] - \Pr_{\widetilde{\mathsf{KA}}^{G_\Lambda}}[k_A = k_B]\right| \le O\left(\sum_{n=\Lambda+1}^{L} 2q \cdot \frac{(2q)^2}{2^n}\right) \le O\left(L \cdot \frac{q^3}{2^\Lambda}\right),$$

which implies $\Pr_{\widetilde{\mathsf{KA}}^{G_\Lambda}}[k_A = k_B] \ge \Pr_{\mathsf{KA}^G}[k_A = k_B] - O\left(Lq^3/2^\Lambda\right) = 1 - 1/\mathsf{poly}(\lambda)$ for some polynomial poly.

$\widetilde{\mathsf{KA}}^{G_\Lambda}$ is 0.1-secure. Next, we claim that for any polynomial p and eavesdropper that asks $p(\lambda)$ classical queries to G_Λ, her advantage of finding k_B in $\widetilde{\mathsf{KA}}^{G_\Lambda}$ is at most 0.1 for sufficiently large λ. For contradiction, suppose there exist a polynomial p and an eavesdropper $\widetilde{E}$ that asks $p(\lambda)$ classical queries to G_Λ and finds k_B with advantage at least 0.1 for infinitely many λ in $\widetilde{\mathsf{KA}}^{G_\Lambda}$. Then we construct following the LOCC distinguisher: $(A_{\mathsf{LOCC}}, B_{\mathsf{LOCC}})$ first run KA^G as the previous paragraph and obtains k_A, k_B and the transcript τ. Then B_{LOCC} runs $\widetilde{E}$ on input the transcript τ, answers the queries by G_Λ defined by themselves (without using any input state), and obtains a key k_E. B_{LOCC} outputs 1 if $k_B = k_E$. By the same argument, $(A_{\mathsf{LOCC}}, B_{\mathsf{LOCC}})$ perfectly simulates either $\widetilde{E}^G$ in KA^G or $\widetilde{E}^{G_\Lambda}$ in $\widetilde{\mathsf{KA}}^{G_\Lambda}$ depending on if they got the same states or i.i.d. states. Hence, by Corollary 7.10 we have

$$\left|\Pr_{\mathsf{KA}^G}[k_B = k_E] - \Pr_{\widetilde{\mathsf{KA}}^{G_\Lambda}}[k_B = k_E]\right| \le O\left(\sum_{n=\Lambda+1}^{L} 2q \cdot \frac{(2q)^2}{2^n}\right) \le O\left(L \cdot \frac{q^3}{2^\Lambda}\right),$$

which implies $\Pr_{\widetilde{\mathsf{KA}}^{G_\Lambda}}[k_B = k_E] \ge \Pr_{\mathsf{KA}^G}[k_B = k_E] - O\left(Lq^3/2^\Lambda\right) \ge 0.1 - O\left(Lq^3/2^\Lambda\right)$ for infinitely many λ. However, this contradicts the security of KA^G.

Getting to plain model: Finally, define the following protocol $\mathsf{KA}_{\mathsf{plain}}(A_{\mathsf{plain}}, B_{\mathsf{plain}})$ in the plain model:

$\mathsf{KA}_{\mathsf{plain}}(1^\lambda, A_{\mathsf{plain}}, B_{\mathsf{plain}})$:

1. For every $k \in \bigcup_{i=1}^{\Lambda}\{0,1\}^i$, A_{plain} samples $|\psi_k\rangle \leftarrow \mathcal{H}_{|k|}$.
2. For every $k \in \bigcup_{i=1}^{\Lambda}\{0,1\}^i$, A_{plain} run $\mathsf{Tomography}$ (defined in Theorem 9.5) on $|\psi_k\rangle$ with parameters $\Delta = 2^{-2\Lambda}$ and $\gamma = 2^{-\lambda}$ to obtain the classical description of $|\widehat{\psi}_k\rangle$.[a]
3. For every $k \in \bigcup_{i=1}^{\Lambda}\{0,1\}^i$, A_{plain} sends the description of $|\widehat{\psi}_k\rangle$ to B_{plain}.
4. $(A_{\mathsf{plain}}, B_{\mathsf{plain}})$ define the output of the oracle $\widehat{G}_\Lambda$ to be $\{\{|\widehat{\psi}_k\rangle\}_{k\in\{0,1\}^i}\}_{i\in\{1,\ldots,\Lambda\}}$.
5. $(A_{\mathsf{plain}}, B_{\mathsf{plain}})$ runs $\widetilde{\mathsf{KA}}^{\widehat{G}_\Lambda}$ on 1^λ to obtain (k_A, k_B).

[31] In B_{LOCC}'s round, B acts similarly as defined above.

6. A_{plain} outputs key k_A and B_{plain} outputs key k_B respectively.

[a]Note that A_{plain} samples $|\psi_k\rangle$ and thus has its classical description. Performing tomography is merely for the simplicity of proof.

$\mathsf{KA}_{\mathsf{plain}}$ is $1/\mathsf{poly}$-complete. Define the event Good in $\mathsf{KA}_{\mathsf{plain}}$ as:

$$\mathsf{Good} \equiv \bigwedge_{k\in\bigcup_{i=1}^{\Lambda}\{0,1\}^i} \left[\mathsf{TD}(|\psi_k\rangle\langle\psi_k|, |\widehat{\psi}_k\rangle\langle\widehat{\psi}_k|) \leq \Delta\right].$$

From the guarantee of tomography (Theorem 9.5) and a union bound, the probability of Good happening is at least $1-\sum_{i=1}^{\Lambda} 2^i\cdot\gamma = 1-\mathsf{negl}(\lambda)$. Since $\widetilde{A}^{(\cdot)}$ and $\widetilde{B}^{(\cdot)}$ in $\widetilde{\mathsf{KA}}^{G_\Lambda}$ (resp., $\widetilde{\mathsf{KA}}^{\widehat{G}_\Lambda}$) ask a total of $2q$ queries, one can use $\{\{|\psi_k\rangle^{\otimes 2q}\}_{k\in\{0,1\}^i}\}_{i=1}^{\Lambda}$ (resp., $\{\{|\widehat{\psi}_k\rangle^{\otimes 2q}\}_{k\in\{0,1\}^i}\}_{i=1}^{\Lambda}$) to perfectly answer A's and B's queries. Hence, from the operational definition of trace distance, we have

$$\begin{aligned}
&\left|\Pr_{\mathsf{KA}_{\mathsf{plain}}}[k_A=k_B] - \Pr_{\widetilde{\mathsf{KA}}^{G_\Lambda}}[k_A=k_B]\right| \\
&\leq \Pr[\neg\mathsf{Good}] + \mathbb{E}\left[\mathsf{TD}\left(\bigotimes_{i=1}^{\Lambda}\bigotimes_{k\in\{0,1\}^i}|\psi_k\rangle\langle\psi_k|^{\otimes 2q}, \bigotimes_{i=1}^{\Lambda}\bigotimes_{k\in\{0,1\}^i}|\widehat{\psi}_k\rangle\langle\widehat{\psi}_k|^{\otimes 2q}\right) \mid \mathsf{Good}\right] \\
&\leq \Pr[\neg\mathsf{Good}] + \sum_{i=1}^{\Lambda}\sum_{k\in\{0,1\}^i} 2q\cdot\mathbb{E}\left[\mathsf{TD}(|\psi_k\rangle\langle\psi_k|, |\widehat{\psi}_k\rangle\langle\widehat{\psi}_k|) \mid \mathsf{Good}\right] \\
&\leq \mathsf{negl}(\lambda) + 2q\cdot\sum_{i=1}^{\Lambda} 2^i\cdot\Delta \leq \frac{1}{\mathsf{poly}'(\lambda)}
\end{aligned}$$

for some polynomial poly'. Hence, the completeness of $\mathsf{KA}_{\mathsf{plain}}$ is at least

$$\Pr_{\mathsf{KA}_{\mathsf{plain}}}[k_A=k_B] \geq \Pr_{\widetilde{\mathsf{KA}}^{G_\Lambda}}[k_A=k_B] - \frac{1}{\mathsf{poly}'(\lambda)} = 1-\frac{1}{\mathsf{poly}(\lambda)} - \frac{1}{\mathsf{poly}'(\lambda)} = 1-\varepsilon(\lambda)$$

for some inverse polynomial ε, where the first equality is because $\widetilde{\mathsf{KA}}^{G_\Lambda}$ is $1/\mathsf{poly}(\lambda)$-complete for some polynomial poly.

$\mathsf{KA}_{\mathsf{plain}}$ is 0.2-secure. For contradiction, suppose there exists an eavesdropper E_{plain} that finds k_B in $\mathsf{KA}_{\mathsf{plain}}$ with advantage 0.2 for infinitely many λ. We construct the following eavesdropper $\widetilde{E}^{G_\Lambda}$ for $\widetilde{\mathsf{KA}}^{G_\Lambda}$ by using E_{plain} as follows.

$\widetilde{E}^{G_\Lambda}(1^\lambda,\tau)$:

1. For every $k\in\bigcup_{i=1}^{\Lambda}\{0,1\}^i$, ask $p_{\mathsf{Tomography}}(2^{|k|},\Delta^{-1},\log(\gamma^{-1}))$ queries to G_k with parameters $\Delta=2^{-2\Lambda}$ and $\gamma=2^{-\lambda}$ to get $\{|\psi_k\rangle^{\otimes p_{\mathsf{Tomography}}(2^{|k|},\Delta^{-1},\log(\gamma^{-1}))}\}_{k\in\bigcup_{i=1}^{\Lambda}\{0,1\}^i}$.
2. Perform $\mathsf{Tomography}$ (defined in Theorem 9.5) on every state obtained in the previous step to obtain the description of $\{|\widehat{\psi}_k\rangle\}_{k\in\bigcup_{i=1}^{\Lambda}\{0,1\}^i}$.
3. Run E_{plain} on input τ and all the descriptions obtained by tomography, and set k_E to the output of E_{plain}.

4. Output k_E.

First, $\widetilde{E}^{G_\Lambda}$ makes at most $\sum_{i=1}^{\Lambda} 2^i \cdot p_{\mathsf{Tomography}}(2^i, \Delta^{-1}, \log(\gamma^{-1})) = p(\lambda)$ queries for some polynomial p. Next, in $\widetilde{\mathsf{KA}}^{G_\Lambda}$, the joint distribution of G_Λ and the description $\{|\widehat{\psi}_k\rangle\}_{k\in\bigcup_{i=1}^{\Lambda}\{0,1\}^i}$ obtained from tomography in Step 2 of $\widetilde{E}^{G_\Lambda}$ is identically distributed as Steps 1 to 3 in $\mathsf{KA}_{\mathsf{plain}}$. Now, from the correctness guarantee of $\mathsf{Tomography}$, there is a $1-\mathsf{negl}(\lambda)$ fraction of $\{|\psi_k\rangle\}_{k\in\bigcup_{i=1}^{\Lambda}\{0,1\}^i}$ and $\{|\widehat{\psi}_k\rangle\}_{k\in\bigcup_{i=1}^{\Lambda}\{0,1\}^i}$ such that event Good occurs. By the same argument in the previous paragraph, the distributions of (τ, k_A, k_B) generated by $(\widetilde{A}^{G_\Lambda}, \widetilde{B}^{G_\Lambda})$ and $(\widetilde{A}^{\widehat{G}_\Lambda}, \widetilde{B}^{\widehat{G}_\Lambda})$ are $1/\mathsf{poly}'(\lambda)$-close in statistical distance. Since E_{plain} takes as input τ and $\{|\widehat{\psi}_k\rangle\}_{k\in\bigcup_{i=1}^{\Lambda}\{0,1\}^i}$, $\widetilde{E}^{G_\Lambda}$ breaks the security of $\widetilde{\mathsf{KA}}^{G_\Lambda}$ with advantage at least $0.2 - 1/\mathsf{poly}'(\lambda) > 0.1$ for infinitely many λ, which contradicts the security of $\widetilde{\mathsf{KA}}^{G_\Lambda}$. □

Lemma 9.7. *There does not exist a secure QCCC key agreement relative to G.*

Proof. It immediately follows from Lemmas 9.4 and 9.6. □

Theorem 9.8. *There does not exist a quantum fully black-box reduction (C, S) from QCCC key agreements to $(\lambda, \omega(\log(\lambda)))$-PRSGs such that C only asks classical queries to the PRSG.*

Proof. For the sake of contradiction, suppose (C, S) is a fully black-box reduction satisfying the conditions. Let $\mathcal{I}$ be the implementation of $(\lambda, \omega(\log(\lambda)))$-PRSGs as stated in the proof of Lemma 9.1. Then $C^{\mathcal{I}}$ is a key agreement that satisfies completeness. From Lemma 9.7, there exists a poly-query adversary $\widetilde{E}$ that breaks the security of the QCCC key agreement $C^{\mathcal{I}}$. Then $S^{\widetilde{E},\mathcal{I}}$ by definition breaks the security of the $(\lambda, \omega(\log(\lambda)))$-PRSG $\mathcal{I}$ by asking polynomially many queries to $\widetilde{E}$ and $\mathcal{I}$, thus in total polynomial queries to G. However, this contradicts Lemma 9.1. □

9.3 Separating QCCC Interactive Commitments from $(\lambda, \omega(\log(\lambda)))$-PRSGs

Definition 9.9 (QCCC interactive commitments relative to oracle)**.** *A QCCC commitment relative to an oracle $\mathcal{O}$ is a two-party interactive protocol consisting of a pair of uniform QPT oracle algorithms (C, R), where C is the committer and R is the receiver. Let $q = q(\lambda)$ be an arbitrary polynomial. Each of C and R can ask q queries to the oracle $\mathcal{O}$ and are allowed to communicate classically.*

- ***Commit phase:*** *In the (possibly interactive) commit phase, C takes as input the security parameter 1^λ and a bit $b \in \{0,1\}$, and R takes as input the security parameter 1^λ. We denote the execution of the commit phase by $(\sigma_{CR}, \tau) \leftarrow \mathsf{Commit}\langle C^{\mathcal{O}}(1^\lambda, b), R^{\mathcal{O}}(1^\lambda)\rangle$, where σ_{CR} is the joint state of C and R after the commit phase, and τ denotes the transcript in the commit phase.*
- ***Reveal phase:*** *In the (possibly interactive) reveal phase, the output is $\mu \in \{0, 1, \bot\}$ indicating the receiver's output bit or abort. We denote the execution of the reveal phase by $\mu \leftarrow \mathsf{Reveal}\langle C^{\mathcal{O}}(1^\lambda, b), R^{\mathcal{O}}(1^\lambda), \sigma_{CR}, \tau\rangle$.*

The scheme satisfies the following conditions.

- ***ε-completeness.*** *For all $\lambda \in \mathbb{N}$,*

$$\Pr\left[\mu = b : \begin{array}{c} O\leftarrow\mathcal{O}, \\ b\leftarrow\{0,1\}, \\ (\sigma_{CR},\tau)\leftarrow\mathsf{Commit}\langle C^O(1^\lambda,b), R^O(1^\lambda)\rangle, \\ \mu\leftarrow\mathsf{Reveal}\langle C^O(1^\lambda,b), R^O(1^\lambda), \sigma_{CR}, \tau\rangle, \\ \mu\in\{0,1,\bot\} \end{array}\right] \geq 1-\varepsilon(\lambda).$$

  If ε is negligible, then we simply say that it is complete.

- ***Statistical hiding.*** *For any polynomial p and any computationally unbounded malicious receiver R^* who asks at most $p(\lambda)$ classical queries, there exists a negligible function* negl *such that for all $\lambda \in \mathbb{N}$,*

$$\Pr\left[b' = b : \begin{array}{c} O \leftarrow \mathcal{O}, \\ b \leftarrow \{0,1\}, \\ (\sigma_{CR^*}, \tau) \leftarrow \mathsf{Commit}\langle C^O(1^\lambda, b), R^{*O}(1^\lambda)\rangle, \\ b' \leftarrow R^{*O}(\sigma_{R^*}, \tau) \end{array}\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda),$$

where σ_{R^*} denotes the state obtained by tracing out the committer's part of the state σ_{CR^*}.

- ***Statistical binding.*** *For any polynomial p and any computationally unbounded malicious committer C^* who asks $p(\lambda)$ classical queries, there exists a negligible function* negl *such that for all $\lambda \in \mathbb{N}$,*

$$\Pr\left[\mu = \mathbf{ch} : \begin{array}{c} O \leftarrow \mathcal{O}, \\ (\sigma_{C^*R}, \tau) \leftarrow \mathsf{Commit}\langle C^{*O}(1^\lambda), R^O(1^\lambda)\rangle, \\ \mathbf{ch} \leftarrow \{0,1\}, \\ \mu \leftarrow \mathsf{Reveal}\langle C^{*O}(\mathbf{ch}), R^O, \sigma_{C^*R}, \tau\rangle \end{array}\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

We need the following lemma regarding total variation distance.

Lemma 9.10. *Let $\mathbf{P}_{BT}, \mathbf{Q}_{BT}$ be two discrete distributions over $\{0,1\} \times \mathcal{T}$. Consider the following experiment:*

Exp.0 :

1. *Sample $(b, \tau) \leftarrow \mathbf{P}_{BT}$.*
2. *If $\mathbf{Q}_T(\tau) = 0$,[a] then set b' to a uniform bit. Otherwise, set b' to the more likely bit according to $\mathbf{Q}_{B|T=\tau}$.*
3. *Output (b, b', τ).*

[a] $\mathbf{Q}_T$ denotes the marginal distribution of $\mathbf{Q}_{BT}$ on T.

Exp.1 :

1. *Sample $(b, \tau) \leftarrow \mathbf{P}_{BT}$.*
2. *Set b' to the more likely bit according to $\mathbf{P}_{B|T=\tau}$.*
3. *Output (b, b', τ).*

Then it holds that

$$\Pr_{\mathbf{Exp.0}}[b = b'] \geq \Pr_{\mathbf{Exp.1}}[b = b'] - 3\mathsf{d}_{\mathsf{TV}}(\mathbf{P}_{BT}, \mathbf{Q}_{BT}).$$

Proof. Consider the following hybrid:

Hyb :

1. Sample $(b, \tau) \leftarrow \mathbf{Q}_{BT}$.
2. If $\mathbf{Q}_T(\tau) = 0$,[a] then set b' to a uniform bit. Otherwise, set b' to the more likely bit according to $\mathbf{Q}_{B|T=\tau}$.
3. Output (b, b', τ).

[a] Since (b, τ) is sampled from $\mathbf{Q}_{BT}$, $\mathbf{Q}_T(\tau)$ is always > 0. We write it merely for the clarity of the proof.

Since a randomized function (Step 2 in **Exp.0** and **Hyb**) cannot increase the total variation distance, we have

$$\left|\Pr_{\mathbf{Exp.0}}[b = b'] - \Pr_{\mathbf{Hyb}}[b = b']\right| \leq \mathsf{d}_{\mathsf{TV}}(\mathbf{P}_{BT}, \mathbf{Q}_{BT}),$$

which implies

$$\Pr_{\mathbf{Exp.0}}[b = b'] \geq \Pr_{\mathbf{Hyb}}[b = b'] - \mathsf{d}_{\mathsf{TV}}(\mathbf{P}_{BT}, \mathbf{Q}_{BT}). \tag{5}$$

In **Hyb**, we have

$$\begin{aligned}\Pr_{\mathbf{Hyb}}[b=b'] &= \mathop{\mathbb{E}}_{\tau\leftarrow\mathbf{Q}_T}\left[\frac{1}{2}+\mathsf{d_{TV}}(\mathbf{Q}_{B|T=\tau},\mathbf{U}_1)\right]\\ &= \frac{1}{2}+\sum_{\tau}\mathbf{Q}_T(\tau)\cdot\frac{1}{2}\sum_{b\in\{0,1\}}\left|\mathbf{Q}(b)_{B|T=\tau}-\frac{1}{2}\right|\\ &= \frac{1}{2}+\frac{1}{2}\sum_{\tau,b\in\{0,1\}}\left|\mathbf{Q}(b,\tau)_{BT}-\frac{1}{2}\cdot\mathbf{Q}_T(\tau)\right|\\ &= \frac{1}{2}+\mathsf{d_{TV}}(\mathbf{Q}_{BT},\mathbf{U}_1\otimes\mathbf{Q}_T), \end{aligned} \tag{6}$$

where $\mathbf{U}_1$ denotes the uniform distribution on $\{0,1\}$. Similarly, in **Exp.1**, we have

$$\begin{aligned}\Pr_{\mathbf{Exp.1}}[b=b'] &= \mathop{\mathbb{E}}_{\tau\leftarrow\mathbf{P}_T}\left[\frac{1}{2}+\mathsf{d_{TV}}(\mathbf{P}_{B|T=\tau},\mathbf{U}_1)\right]\\ &= \frac{1}{2}+\mathsf{d_{TV}}(\mathbf{P}_{BT},\mathbf{U}_1\otimes\mathbf{P}_T)\\ &\le \frac{1}{2}+\mathsf{d_{TV}}(\mathbf{P}_{BT},\mathbf{Q}_{BT})+\mathsf{d_{TV}}(\mathbf{Q}_{BT},\mathbf{U}_1\otimes\mathbf{Q}_T)+\mathsf{d_{TV}}(\mathbf{U}_1\otimes\mathbf{Q}_T,\mathbf{U}_1\otimes\mathbf{P}_T)\\ &= \frac{1}{2}+\mathsf{d_{TV}}(\mathbf{P}_{BT},\mathbf{Q}_{BT})+\mathsf{d_{TV}}(\mathbf{Q}_{BT},\mathbf{U}_1\otimes\mathbf{Q}_T)+\mathsf{d_{TV}}(\mathbf{Q}_T,\mathbf{P}_T)\\ &\le \frac{1}{2}+\mathsf{d_{TV}}(\mathbf{P}_{BT},\mathbf{Q}_{BT})+\mathsf{d_{TV}}(\mathbf{Q}_{BT},\mathbf{U}_1\otimes\mathbf{Q}_T)+\mathsf{d_{TV}}(\mathbf{Q}_{BT},\mathbf{P}_{BT}), \end{aligned} \tag{7}$$

where the first inequality follows from the triangle inequality. From Equations (6) and (7), we have

$$\Pr_{\mathbf{Hyb}}[b=b'] \ge \Pr_{\mathbf{Exp.1}}[b=b'] - 2\mathsf{d_{TV}}(\mathbf{P}_{BT},\mathbf{Q}_{BT}). \tag{8}$$

Hence, combining Equations (5) and (8), we have

$$\Pr_{\mathbf{Exp.0}}[b=b'] \ge \Pr_{\mathbf{Exp.1}}[b=b'] - 3\mathsf{d_{TV}}(\mathbf{P}_{BT},\mathbf{Q}_{BT}). \qquad \square$$

Lemma 9.11. *There does not exist a QCCC interactive commitment relative to G.*

Proof. For the sake of contradiction, suppose $\mathsf{Com}^G = (C^G, R^G)$ is a QCCC interactive commitment relative to G, where $q(\lambda) = \mathsf{poly}(\lambda)$ is the number of queries asked by C and R respectively and $L(\lambda) = \mathsf{poly}(\lambda)$ is the maximum input length of the queries. Define the function $\Lambda(\lambda) := \lceil \log\left(q^{10} + L^{10} + \lambda^{10}\right)\rceil = O(\log(\lambda))$ and the truncated oracle $G_\Lambda = \{\{G_k\}_{k\in\{0,1\}^i}\}_{i=1}^{\Lambda}$. The proof consists of two major parts. First, we will show that Com^G can be converted to a QCCC interactive commitment $\widetilde{\mathsf{Com}}^{G_\Lambda}$ relative to G_Λ. Next, we will show that any QCCC interactive commitment relative to G_Λ cannot satisfy completeness, statistical hiding, and statistical binding simultaneously.

Converting Com^G to $\widetilde{\mathsf{Com}}^{G_\Lambda}$. We define the following scheme $\widetilde{\mathsf{Com}}^{G_\Lambda} = (\widetilde{C}^{G_\Lambda}, \widetilde{R}^{G_\Lambda})$ relative to G_Λ:

$\widetilde{\mathsf{Com}}^{G_\Lambda}(1^\lambda, \widetilde{C}^{G_\Lambda}, \widetilde{R}^{G_\Lambda})$:

1. For every $k \in \bigcup_{i=\Lambda+1}^{L}\{0,1\}^i$, $\widetilde{C}$ and $\widetilde{R}$ samples $|\phi_k^C\rangle, |\phi_k^R\rangle \leftarrow \mathcal{H}_{|k|}$ respectively.
2. On input 1^λ and b, $\widetilde{C}^{G_\Lambda}$ runs $C^{(\cdot)}(1^\lambda, b)$ by answering the queries as follows. Suppose C asks a query $k \in \bigcup_{i=1}^{L}\{0,1\}^i$. If $|k| \le \Lambda$, then $\widetilde{C}$ ask k to oracle G_Λ and forward the response. Otherwise,

$\widetilde{C}$ sends $|\phi_k^C\rangle$ to C. On input 1^λ, $\widetilde{R}^{G_\Lambda}$ runs $R^{(\cdot)}(1^\lambda)$ by answering R's queries similarly, except that it replaces $|\phi_k^C\rangle$ with $|\phi_k^R\rangle$.

$\widetilde{\mathsf{Com}}^{G_\Lambda}$ is 1/poly-complete. This is similar to proving the completeness of $\widetilde{\mathsf{KA}}^{G_\Lambda}$ in the proof of Lemma 9.6.

$\widetilde{\mathsf{Com}}^{G_\Lambda}$ is statistically hiding and statistically binding. Intuitively, $\widetilde{\mathsf{Com}}^{G_\Lambda}$ is at least as secure as Com^G because the malicious party cannot obtain any information about the Haar states of length greater than Λ held by the other party via asking queries. To prove statistical hiding, suppose there exists a malicious receiver $(\widetilde{R}^*)^{G_\Lambda}$ that breaks the statistical hiding of $\widetilde{\mathsf{Com}}^{G_\Lambda}$ by asking polynomially many queries to G_Λ, then we construct a malicious receiver $(R^*)^G$ that breaks the statistical hiding of Com^G by using $(\widetilde{R}^*)^{(\cdot)}$. $(R^*)^G$ simply runs $\widetilde{R}^*$ by answering its queries with G. Since the distributions of the (honest) committer C in Com^G and $\widetilde{C}$ in $\widetilde{\mathsf{Com}}^{G_\Lambda}$ are identical, the advantage of $(R^*)^G$ is equal to that of $(\widetilde{R}^*)^{G_\Lambda}$. This contradicts the premise that Com^G is statistically hiding.

Similarly, to prove statistical binding, suppose there exists a malicious committer $(\widetilde{C}^*)^{G_\Lambda}$ that breaks the statistical binding of $\widetilde{\mathsf{Com}}^{G_\Lambda}$ by asking polynomially many queries to G_Λ, then we construct a malicious committer $(C^*)^G$ that breaks the statistical binding of Com^G by using $(\widetilde{C}^*)^{(\cdot)}$. $(C^*)^G$ simply runs $\widetilde{C}^*$ by answering its queries with G. Since the distributions of the (honest) receiver R in Com^G and $\widetilde{R}$ in $\widetilde{\mathsf{Com}}^{G_\Lambda}$ are identical, the advantage of $(C^*)^G$ is equal to that of $(\widetilde{C}^*)^{G_\Lambda}$. This contradicts the premise that Com^G is statistically binding.

In the rest of the proof, we will show that a commitment scheme relative to G_Λ cannot satisfy completeness, statistical hiding, and statistical binding at the same time. Intuitively, this is because the output length of G_Λ is short, so each party can approximate the whole oracle by performing tomography using polynomially many queries. Hence, the scheme can be reduced to the plain model, modulo the error introduced by tomography.

QCCC commitments do not exist relative to G_Λ. We will show that there does not exist a complete, statistically hiding, and statistically binding QCCC interactive commitment relative to G_Λ. Toward contradiction, suppose $\widetilde{\mathsf{Com}}^{G_\Lambda} = (\widetilde{C}^{G_\Lambda}, \widetilde{R}^{G_\Lambda})$ is such a scheme. Consider the following malicious receiver R^* (for brevity, we omit the tilde $\widetilde{\cdot}$ in the rest of the proof) with classical oracle access to G_Λ:

R^* **in Hiding Experiment**:

1. R^* runs the commit phase honestly with C who commits to $\mathbf{b}$ (where b was sampled uniformly at random by C) and obtains the transcript τ.
2. R^* performs $\mathsf{Tomography}$ (defined in Theorem 9.5) with parameters $\Delta = 2^{-2\Lambda}$ and $\gamma = 2^{-\lambda}$ on every output state of G_Λ to obtain the description, denoted by $\widehat{G}_\Lambda$.
3. If τ and $\widehat{G}_\Lambda$ are not consistent, then R^* output a uniform bit $\mathbf{b}'$. Otherwise, R^* outputs the more likely bit $\mathbf{b}'$ from the distribution conditioned on $(\tau, \widehat{G}_\Lambda)$.

For efficiency, R^* asks polynomially many queries in Step 2. For every fixed $(G_\Lambda, \widehat{G}_\Lambda)$, we denote by $p^{R^*}_{G_\Lambda, \widehat{G}_\Lambda}$ the probability that R^* guess the committed bit correctly.

Analyze R^*. The structure of the proof is similar to proving the completeness of $\mathsf{KA}_{\mathsf{plain}}$ in Lemma 9.6. Define the event Good in the hiding experiment as

$$\mathsf{Good} \equiv \bigwedge_{k \in \bigcup_{i=1}^{\Lambda} \{0,1\}^i} \left[\mathsf{TD}(|\psi_k\rangle\langle\psi_k|, |\widehat{\psi}_k\rangle\langle\widehat{\psi}_k|) \leq \Delta \right].$$

We now consider any pair $G_\Lambda = \{\{|\psi_k\rangle\}_{k\in\{0,1\}^i}\}_{i=1}^\Lambda$ and $\widehat{G}_\Lambda = \{\{|\widehat{\psi}_k\rangle\}_{k\in\{0,1\}^i}\}_{i=1}^\Lambda$ such that event Good occurs. Let $\mathbf{D}_{BT|G_\Lambda}$ (resp., $\mathbf{D}_{BT|\widehat{G}_\Lambda}$) denote the distribution of (b,τ) in the honest commit phase of $\widetilde{\mathsf{Com}}$ conditioned on oracle being G_Λ (resp., $\widehat{G}_\Lambda$). Since $\widetilde{C}^{(\cdot)}$ and $\widetilde{R}^{(\cdot)}$ in $\widetilde{\mathsf{Com}}^{G_\Lambda}$ (resp., $\widetilde{\mathsf{Com}}^{\widehat{G}_\Lambda}$) ask a total of $2q$ queries, one can use $\{\{|\psi_k\rangle^{\otimes 2q}\}_{k\in\{0,1\}^i}\}_{i=1}^\Lambda$ (resp., $\{\{|\widehat{\psi}_k\rangle^{\otimes 2q}\}_{k\in\{0,1\}^i}\}_{i=1}^\Lambda$) to perfectly answer $\widetilde{C}$'s and $\widetilde{R}$'s queries. From the operational definition of trace distance, we have

$$\mathsf{d_{TV}}(\mathbf{D}_{BT|G_\Lambda}, \mathbf{D}_{BT|\widehat{G}_\Lambda}) \le 2q \cdot \sum_{i=1}^{\Lambda} 2^i \cdot \Delta = \frac{1}{\mathsf{poly}(\lambda)}$$

for some polynomial poly.

Define the quantity $p^{R^*}_{G_\Lambda}$ which is equal to the success probability of R^* conditioned on G_Λ without tomography error, i.e.,

$$\begin{aligned} p^{R^*}_{G_\Lambda} &:= \frac{1}{2} + \mathop{\mathbb{E}}_{\tau\leftarrow\mathbf{D}_{\tau|G_\Lambda}} \left[\mathsf{d_{TV}}(\mathbf{D}_{B|G_\Lambda,T=\tau}, \mathbf{U}_1)\right] \\ &= \frac{1}{2} + \sum_\tau \Pr_{\mathsf{Commit}}[\tau \mid G_\Lambda] \cdot \mathsf{d_{TV}}(\mathbf{D}_{B|G_\Lambda,T=\tau}, \mathbf{U}_1), \end{aligned} \tag{9}$$

where Commit denotes the honest commit phase of $\widetilde{\mathsf{Com}}$. By Lemma 9.10 (setting $\mathbf{P} \equiv \mathbf{D}_{BT|G_\Lambda}$ and $\mathbf{Q} \equiv \mathbf{D}_{BT|\widehat{G}_\Lambda}$), we have

$$p^{R^*}_{G_\Lambda,\widehat{G}_\Lambda} \ge p^{R^*}_{G_\Lambda} - 3\mathsf{d_{TV}}(\mathbf{D}_{BT|G_\Lambda}, \mathbf{D}_{BT|\widehat{G}_\Lambda}) = p^{R^*}_{G_\Lambda} - \frac{3}{\mathsf{poly}(\lambda)}. \tag{10}$$

Finally, after averaging over $(G_\Lambda, \widehat{G}_\Lambda)$, the probability $p_{R^*\mathrm{win}}$ that R^* guess the committed bit correctly satisfies

$$\begin{aligned} p_{R^*\mathrm{win}} &:= \mathop{\mathbb{E}}_{G_\Lambda,\widehat{G}_\Lambda}[p^{R^*}_{G_\Lambda,\widehat{G}_\Lambda}] \\ &= \mathop{\mathbb{E}}_{G_\Lambda}\left[\mathop{\mathbb{E}}_{\widehat{G}_\Lambda}\left[p^{R^*}_{G_\Lambda,\widehat{G}_\Lambda} \mid G_\Lambda\right]\right] \\ &\ge \mathop{\mathbb{E}}_{G_\Lambda}\left[\Pr_{\widehat{G}_\Lambda}[\mathsf{Good} \mid G_\Lambda] \cdot \mathop{\mathbb{E}}_{\widehat{G}_\Lambda}\left[p^{R^*}_{G_\Lambda,\widehat{G}_\Lambda} \mid G_\Lambda \wedge \mathsf{Good}\right]\right] \\ &\ge \mathop{\mathbb{E}}_{G_\Lambda}\left[(1-\mathsf{negl}(\lambda)) \cdot \left(p^{R^*}_{G_\Lambda} - \frac{3}{\mathsf{poly}(\lambda)}\right)\right] \\ &= (1-\mathsf{negl}(\lambda)) \cdot \left(\mathop{\mathbb{E}}_{G_\Lambda}\left[p^{R^*}_{G_\Lambda}\right] - \frac{3}{\mathsf{poly}(\lambda)}\right). \end{aligned} \tag{11}$$

The second inequality follows from Equation (10) and the following reason: by the correctness guarantee of $\mathsf{Tomography}$ (Theorem 9.5) and a union bound, the probability of Good happening conditioned on any G_Λ is at least $1 - \sum_{i=1}^{\Lambda} 2^i \cdot \gamma = 1 - \mathsf{negl}(\lambda)$.

Next, consider the following malicious committer C^*:

C^* **in Binding Experiment**:

1. C^* commits to a uniform bit $\mathbf{b}$, runs the commit phase with R honestly, and generates the transcript τ. The joint state of C^* and R after the commit phase is $\rho^{\mathsf{C}}_{\mathbf{b},G_\Lambda,\tau} \otimes \sigma^{\mathsf{R}}_{G_\Lambda,\tau}$.[a]
2. C^* performs $\mathsf{Tomography}$ (defined in Theorem 9.5) with parameters $\Delta = 2^{-2\Lambda}$ and $\gamma = 2^{-\lambda}$ on every output state of G_Λ to obtain the description, denoted by $\widehat{G}_\Lambda$.

3. Upon receiving the challenge bit $\mathbf{ch}$, C^* computes the description of the joint state conditioned on $(\mathbf{ch}, \tau, \widehat{G}_\Lambda)$, denoted by $\rho^{\mathsf{CR}}_{\mathbf{ch},\widehat{G}_\Lambda,\tau}$. If $(\mathbf{ch}, \widehat{G}_\Lambda, \tau)$ is inconsistent, then C^* aborts.[b]

4. C^* runs the reveal phase honestly on input $\mathbf{ch}$ and state $\rho^{\mathsf{C}}_{\mathbf{ch},\widehat{G}_\Lambda,\tau}$.

[a] From Lemma 9.3, the joint state is a product state. Moreover, fixing (G_Λ, τ) already determines the state of R. So it is independent of $\mathbf{b}$ after conditioned on (G_Λ, τ).

[b] Note that it is equivalently to setting $\rho^{\mathsf{CR}}_{\mathbf{ch},\widehat{G}_\Lambda,\tau}$ to the zero matrix in terms of calculating C^*'s success probability.

For efficiency, C^* asks polynomially many queries in Step 2. For every fixed $(G_\Lambda, \widehat{G}_\Lambda)$, the probability that C^* successfully opens to $\mathbf{ch}$ is

$$\begin{aligned}
&p^{C^*}_{G_\Lambda,\widetilde{G}_\Lambda} := \sum_{\tau} \sum_{b,ch\in\{0,1\}} \Pr_{\mathsf{Commit}}[\tau \mid G_\Lambda] \cdot \Pr_{\mathsf{Commit}}[\mathbf{b} = b \mid \tau, G_\Lambda] \cdot \Pr_{\mathsf{Commit}}[\mathbf{ch} = ch \mid \mathbf{b} = b, \tau, G_\Lambda] \\
&\cdot \Pr\left[\mathsf{Reveal}\langle C^{G_\Lambda}(ch), R^{G_\Lambda}, \rho^{\mathsf{C}}_{ch,\widehat{G}_\Lambda,\tau} \otimes \sigma^{\mathsf{R}}_{G_\Lambda,\tau}, \tau\rangle = ch\right] \\
&= \sum_{\tau} \sum_{b,ch\in\{0,1\}} \Pr_{\mathsf{Commit}}[\tau \mid G_\Lambda] \cdot \Pr_{\mathsf{Commit}}[\mathbf{b} = b \mid \tau, G_\Lambda] \cdot \frac{1}{2} \cdot \Pr\left[\mathsf{Reveal}\langle C^{G_\Lambda}(ch), R^{G_\Lambda}, \rho^{\mathsf{C}}_{ch,\widehat{G}_\Lambda,\tau} \otimes \sigma^{\mathsf{R}}_{G_\Lambda,\tau}, \tau\rangle = ch\right]
\end{aligned}$$

since $\mathbf{ch}$ is sampled uniformly and independently.

Analyze C^*. Define the event Good in the same way as in the hiding experiment. For every fixed $(G_\Lambda, \widehat{G}_\Lambda)$ such that Good happens, consider the following two classical-quantum states corresponding to the joint state of C and R right after the honest commit phase of $\widetilde{\mathsf{Com}}$ conditioned on the oracle being G_Λ and $\widehat{G}_\Lambda$ respectively:

$$\Psi_{G_\Lambda} := \sum_{b\in\{0,1\}} \sum_{\tau} \frac{1}{2} \cdot \Pr_{\mathsf{Commit}}[\tau \mid \mathbf{b} = b, G_\Lambda] \cdot |b\rangle\langle b|_{\mathsf{B}} \otimes \rho^{\mathsf{C}}_{b,G_\Lambda,\tau} \otimes \sigma^{\mathsf{R}}_{G_\Lambda,\tau} \otimes |\tau\rangle\langle\tau|_{\mathsf{T}},$$

$$\Psi_{\widehat{G}_\Lambda} := \sum_{b\in\{0,1\}} \sum_{\tau} \frac{1}{2} \cdot \Pr_{\mathsf{Commit}}[\tau \mid \mathbf{b} = b, \widehat{G}_\Lambda] \cdot |b\rangle\langle b|_{\mathsf{B}} \otimes \rho^{\mathsf{C}}_{b,\widehat{G}_\Lambda,\tau} \otimes \sigma^{\mathsf{R}}_{\widehat{G}_\Lambda,\tau} \otimes |\tau\rangle\langle\tau|_{\mathsf{T}},$$

where register B is the committer's private register for storing the input and register T is the public register for storing the transcript. Similar to the previous section, since $\widetilde{C}^{(\cdot)}$ and $\widetilde{R}^{(\cdot)}$ in $\widetilde{\mathsf{Com}}^{G_\Lambda}$ (resp., $\widetilde{\mathsf{Com}}^{\widehat{G}_\Lambda}$) ask a total of $2q$ queries, one can use $\{\{|\psi_k\rangle^{\otimes 2q}\}_{k\in\{0,1\}^i}\}_{i=1}^{\Lambda}$ (resp., $\{\{|\widehat{\psi}_k\rangle^{\otimes 2q}\}_{k\in\{0,1\}^i}\}_{i=1}^{\Lambda}$) to perfectly answer $\widetilde{C}$'s and $\widetilde{R}$'s queries. From the correctness guarantee of $\mathsf{Tomography}$, we have

$$\mathsf{TD}(\Psi_{G_\Lambda}, \Psi_{\widehat{G}_\Lambda}) \leq 2q \cdot \sum_{i=1}^{\Lambda} 2^i \cdot \Delta = \frac{1}{\mathsf{poly}(\lambda)}. \tag{12}$$

In order to analyze the success probability of C^* conditioned on $(G_\Lambda, \widehat{G}_\Lambda)$, we define the following state

$$\Psi_{G_\Lambda,\widehat{G}_\Lambda} := \sum_{b\in\{0,1\}} \sum_{\tau} \frac{1}{2} \cdot \Pr_{\mathsf{Commit}}[\tau \mid \mathbf{b} = b, G_\Lambda] \cdot |b\rangle\langle b|_{\mathsf{B}} \otimes \rho^{\mathsf{C}}_{b,\widehat{G}_\Lambda,\tau} \otimes \sigma^{\mathsf{R}}_{G_\Lambda,\tau} \otimes |\tau\rangle\langle\tau|_{\mathsf{T}}.$$

We claim that

$$\mathsf{TD}(\Psi_{G_\Lambda}, \Psi_{G_\Lambda,\widetilde{G}_\Lambda}) \leq \frac{2}{\mathsf{poly}(\lambda)}. \tag{13}$$

To prove Equation (13), we introduce the following hybrid state:

$$\Psi_{\mathsf{Hyb}} := \sum_{b\in\{0,1\}} \sum_{\tau} \frac{1}{2} \cdot \Pr_{\mathsf{Commit}}[\tau \mid \mathbf{b} = b, \widehat{G}_\Lambda] \cdot |b\rangle\langle b|_{\mathsf{B}} \otimes \rho^{\mathsf{C}}_{b,\widehat{G}_\Lambda,\tau} \otimes \sigma^{\mathsf{R}}_{G_\Lambda,\tau} \otimes |\tau\rangle\langle\tau|_{\mathsf{T}}.$$

By the triangle inequality, we can bound Equation (13) as

$$\mathsf{TD}(\Psi_{G_\Lambda}, \Psi_{G_\Lambda,\widehat{G}_\Lambda}) \leq \mathsf{TD}(\Psi_{G_\Lambda}, \Psi_{\mathsf{Hyb}}) + \mathsf{TD}(\Psi_{\mathsf{Hyb}}, \Psi_{G_\Lambda,\widehat{G}_\Lambda}). \tag{14}$$

For the first term in Equation (14), we have

$$\begin{aligned}
\mathsf{TD}(\Psi_{G_\Lambda}, \Psi_{\mathsf{Hyb}}) &= \sum_{b\in\{0,1\}} \sum_{\tau} \frac{1}{2} \cdot \mathsf{TD}\left(\Pr_{\mathsf{Commit}}[\tau \mid \mathbf{b}=b, G_\Lambda] \cdot \rho^{\mathsf{C}}_{b,G_\Lambda,\tau}, \Pr_{\mathsf{Commit}}[\tau \mid \mathbf{b}=b, \widehat{G}_\Lambda] \cdot \rho^{\mathsf{C}}_{b,\widehat{G}_\Lambda,\tau} \right) \\
&= \mathsf{TD}(\mathrm{Tr}_{\mathsf{R}}(\Psi_{G_\Lambda}), \mathrm{Tr}_{\mathsf{R}}(\Psi_{\widehat{G}_\Lambda})) \\
&\leq \mathsf{TD}(\Psi_{G_\Lambda}, \Psi_{\widehat{G}_\Lambda}) \\
&= \frac{1}{\mathsf{poly}(\lambda)},
\end{aligned}$$

where the first two equalities are because $\mathsf{TD}(\bigoplus_i A_i, \bigoplus_i B_i) = \sum_i \mathsf{TD}(A_i, B_i)$ and the inequality is because the trace distance won't increase under partial trace; the inequality follows from Equation (12). Similarly, For the first term in Equation (14), we have

$$\begin{aligned}
\mathsf{TD}(\Psi_{\mathsf{Hyb}}, \Psi_{G_\Lambda,\widehat{G}_\Lambda}) &= \sum_{b\in\{0,1\}} \sum_{\tau} \frac{1}{2} \cdot \mathsf{TD}\left(\Pr_{\mathsf{Commit}}[\tau \mid \mathbf{b}=b, G_\Lambda], \Pr_{\mathsf{Commit}}[\tau \mid \mathbf{b}=b, \widehat{G}_\Lambda] \right) \\
&= \mathsf{TD}(\mathrm{Tr}_{\mathsf{CR}}(\Psi_{G_\Lambda}), \mathrm{Tr}_{\mathsf{CR}}(\Psi_{\widehat{G}_\Lambda})) \\
&\leq \mathsf{TD}(\Psi_{G_\Lambda}, \Psi_{\widehat{G}_\Lambda}) \\
&= \frac{1}{\mathsf{poly}(\lambda)}.
\end{aligned}$$

Thus, the proof of Equation (13) is complete.

Define the quantity $p^{C^*}_{G_\Lambda}$ which is equal to the success probability of C^* conditioned on G_Λ without tomography error:

$$p^{C^*}_{G_\Lambda} := \sum_{\tau} \sum_{ch\in\{0,1\}} \Pr_{\mathsf{Commit}}[\tau \mid G_\Lambda] \cdot \frac{1}{2} \cdot \Pr\left[\mathsf{Reveal}\langle C^{G_\Lambda}(ch), R^{G_\Lambda}, \rho^{\mathsf{C}}_{ch,G_\Lambda,\tau} \otimes \sigma^{\mathsf{R}}_{G_\Lambda,\tau}, \tau\rangle = ch\right].$$

Thus, from the operational definition of trace distance and Equation (13), we have

$$|p^{C^*}_{G_\Lambda,\widehat{G}_\Lambda} - p^{C^*}_{G_\Lambda}| \leq \mathsf{TD}(\Psi_{G_\Lambda}, \Psi_{G_\Lambda,\widehat{G}_\Lambda}) \leq \frac{2}{\mathsf{poly}(\lambda)},$$

which implies

$$p^{C^*}_{G_\Lambda,\widehat{G}_\Lambda} \geq p^{C^*}_{G_\Lambda} - \frac{2}{\mathsf{poly}(\lambda)}. \tag{15}$$

By a similar argument to that of Equation (11), the probability $p_{C^*\mathrm{win}}$ that C^* successfully opens to **ch** satisfies

$$p_{C^*\mathrm{win}} := \mathop{\mathbb{E}}_{G_\Lambda,\widehat{G}_\Lambda}[p^{C^*}_{G_\Lambda,\widehat{G}_\Lambda}] \geq (1 - \mathsf{negl}(\lambda)) \cdot \left(\mathop{\mathbb{E}}_{G_\Lambda}\left[p^{C^*}_{G_\Lambda}\right] - \frac{2}{\mathsf{poly}(\lambda)} \right). \tag{16}$$

Trade-off between completeness, hiding, and binding of commitments. Suppose $\widetilde{\mathsf{Com}}^{G_\Lambda}$ satisfies ε-completeness. In other words,

$p_{\mathsf{Complete}} :=$

$$\mathop{\mathbb{E}}_{G_\Lambda}\left[\sum_{\tau}\sum_{b\in\{0,1\}}\Pr_{\mathsf{Commit}}[\tau \mid G_\Lambda]\cdot\Pr_{\mathsf{Commit}}[\mathbf{b}=b \mid \tau, G_\Lambda]\cdot\Pr\left[\mathsf{Reveal}\langle C^{G_\Lambda}(b), R^{G_\Lambda}, \rho^{\mathsf{C}}_{b,G_\Lambda,\tau}\otimes\sigma^{\mathsf{R}}_{G_\Lambda,\tau},\tau\rangle = b\right]\right]$$
$$\geq 1-\varepsilon. \tag{17}$$

Now, for any fixed (G_Λ,τ) in the support of the honest commit phase of $\widetilde{\mathsf{Com}}^{G_\Lambda}$, define the success probabilities of R^* and C^* conditioned on (G_Λ,τ):

$$p^{R^*}_{G_\Lambda,\tau} := \frac{1}{2}+\mathsf{d}_{\mathsf{TV}}(\mathbf{D}_{B|G_\Lambda,\tau},\mathbf{U}_1) = \frac{1}{2}+\frac{1}{2}\sum_{b\in\{0,1\}}\left|\Pr_{\mathsf{Commit}}[\mathbf{b}=b \mid \tau,G_\Lambda]-\frac{1}{2}\right|,$$

$$p^{C^*}_{G_\Lambda,\tau} := \sum_{ch\in\{0,1\}}\frac{1}{2}\cdot\Pr\left[\mathsf{Reveal}\langle C^{G_\Lambda}(ch), R^{G_\Lambda}, \rho^{\mathsf{C}}_{ch,G_\Lambda,\tau}\otimes\sigma^{\mathsf{R}}_{G_\Lambda,\tau},\tau\rangle = ch\right].$$

W.L.O.G, suppose $\Pr_{\mathsf{Commit}}[\mathbf{b}=0 \mid \tau,G_\Lambda]=\frac{1}{2}+\eta$ and $\Pr_{\mathsf{Commit}}[\mathbf{b}=1 \mid \tau,G_\Lambda]=\frac{1}{2}-\eta$ for some $\eta\in[0,0.5]$ (the opposite case can be proven symmetrically). Thus, it holds that

$$p^{R^*}_{G_\Lambda,\tau} = \frac{1}{2}+\eta.$$

A straightforward calculation yields

$$\begin{aligned}
&p^{R^*}_{G_\Lambda,\tau}+p^{C^*}_{G_\Lambda,\tau}\\
&=\frac{1}{2}+\eta+\sum_{ch\in\{0,1\}}\frac{1}{2}\cdot\Pr\left[\mathsf{Reveal}\langle C^{G_\Lambda}(ch), R^{G_\Lambda}, \rho^{\mathsf{C}}_{ch,G_\Lambda,\tau}\otimes\sigma^{\mathsf{R}}_{G_\Lambda,\tau},\tau\rangle = ch\right]\\
&\geq\frac{1}{2}+\eta\cdot\left(\Pr\left[\mathsf{Reveal}\langle C^{G_\Lambda}(0), R^{G_\Lambda}, \rho^{\mathsf{C}}_{0,G_\Lambda,\tau}\otimes\sigma^{\mathsf{R}}_{G_\Lambda,\tau},\tau\rangle = 0\right]-\Pr\left[\mathsf{Reveal}\langle C^{G_\Lambda}(1), R^{G_\Lambda}, \rho^{\mathsf{C}}_{1,G_\Lambda,\tau}\otimes\sigma^{\mathsf{R}}_{G_\Lambda,\tau},\tau\rangle = 1\right]\right)\\
&+\sum_{ch\in\{0,1\}}\frac{1}{2}\cdot\Pr\left[\mathsf{Reveal}\langle C^{G_\Lambda}(ch), R^{G_\Lambda}, \rho^{C}_{ch,G_\Lambda,\tau}\otimes\rho^{R}_{G_\Lambda,\tau},\tau\rangle = ch\right]\\
&=\frac{1}{2}+\left(\frac{1}{2}+\eta\right)\Pr\left[\mathsf{Reveal}\langle C^{G_\Lambda}(0), R^{G_\Lambda}, \rho^{\mathsf{C}}_{0,G_\Lambda,\tau}\otimes\sigma^{\mathsf{R}}_{G_\Lambda,\tau},\tau\rangle = 0\right]\\
&+\left(\frac{1}{2}-\eta\right)\Pr\left[\mathsf{Reveal}\langle C^{G_\Lambda}(1), R^{G_\Lambda}, \rho^{\mathsf{C}}_{1,G_\Lambda,\tau}\otimes\sigma^{\mathsf{R}}_{G_\Lambda,\tau},\tau\rangle = 1\right]\\
&=\frac{1}{2}+\sum_{b\in\{0,1\}}\Pr_{\mathsf{Commit}}[\mathbf{b}=b \mid \tau,G_\Lambda]\cdot\Pr\left[\mathsf{Reveal}\langle C^{G_\Lambda}(b), R^{G_\Lambda}, \rho^{\mathsf{C}}_{b,G_\Lambda,\tau}\otimes\rho^{\mathsf{R}}_{G_\Lambda,\tau},\tau\rangle = b\right].
\end{aligned}\tag{18}$$

By averaging over (G_Λ,τ) in Equation (18) and recalling the definition of p_{Complete} in Equation (17), we have

$$\mathop{\mathbb{E}}_{G_\Lambda}[p^{R^*}_{G_\Lambda}]+\mathop{\mathbb{E}}_{G_\Lambda}[p^{C^*}_{G_\Lambda}] = \mathop{\mathbb{E}}_{G_\Lambda,\tau}[p^{R^*}_{G_\Lambda,\tau}+p^{C^*}_{G_\Lambda,\tau}] \geq \frac{1}{2}+p_{\mathsf{Complete}} \geq \frac{3}{2}-\varepsilon. \tag{19}$$

Finally, combining Equations (11), (16) and (19), $p_{R^*\mathrm{win}}$, $p_{C^*\mathrm{win}}$, and ε satisfy

$$\frac{p_{R^*\mathrm{win}}+p_{C^*\mathrm{win}}}{1-\mathsf{negl}(\lambda)}+\frac{5}{\mathsf{poly}(\lambda)} \geq \frac{3}{2}-\varepsilon.$$

After rearranging, we have

$$\left(p_{R^*\mathrm{win}}-\frac{1}{2}\right)+\left(p_{C^*\mathrm{win}}-\frac{1}{2}\right)+(1-\mathsf{negl}(\lambda))\cdot\varepsilon \geq \frac{1}{2}-\frac{3}{2}\mathsf{negl}(\lambda)-\frac{5(1-\mathsf{negl}(\lambda))}{\mathsf{poly}(\lambda)}.$$

Therefore, at least one of $\{p_{R^*\mathrm{win}}-1/2, p_{C^*\mathrm{win}}-1/2, \varepsilon\}$ is non-negligible. That is, $\widetilde{\mathsf{Com}}^{G_\Lambda}$ cannot satisfy completeness, statistical hiding, and statistical binding simultaneously. □

Theorem 9.12. *There does not exist a quantum fully black-box reduction (C, S) from QCCC interactive commitments to $(\lambda, \omega(\log(\lambda)))$-PRSGs such that C only asks classical queries to the PRSG.*

Proof. It is essentially the same as the proof of Theorem 9.8. □

Remark 9.13. *We compare our results with existing results. Note that our impossibility results only rule out implementations that ask classical queries to the PRSG. There exist applications that need to query a PRSG/PRFSG in superposition, e.g., quantum bit commitments [MY21], quantum PKEs [BGH+23], etc. However, all of them require quantum communication. It is less obvious how this would be helpful in the QCCC setting. We leave the generalization of the impossibility results as an open problem.*

Next, since PRS generators can be constructed from one-way functions in a black-box way [JLS18], one might wonder whether Theorem 9.8 is already implied by the classical separation result between key agreements and one-way functions [IR89; BM09]. In other words, can we prove Theorem 9.8 by using a (classical) random oracle? We pointed out that all currently known constructions of PRS generators from one-way functions [JLS18; BS19; BS20; GB23; JMW23] require quantum *oracle access. The impossibility of QCCC key agreements in the quantum random oracle model was studied in [ACC+22], where they ruled out* perfectly-complete *key agreements based on a conjecture. However, Theorem 9.8 separates imperfectly-complete key agreements from $\omega(\log(\lambda))$-PRSGs without relying on any conjecture. Hence, the two results are incomparable.*

9.4 Extending the Separation Results

We observe that our technique can also separate QCCC key agreements and commitments from *classically accessible (λ, m, n)-PRFSGs with $n = \omega(\log(\lambda))$* and m being arbitrary. Recall that currently there is no construction of long-input PRFSGs (i.e., $m = \omega(\log(\lambda))$) from PRSGs. Hence, the separation might be strictly stronger. To prove it, we strengthen the separating oracle by increasing the number of oracles as $G = \{\{G_{k,x}\}_{k,x\in\{0,1\}^\lambda}\}_{\lambda\in\mathbb{N}}$. In this way, G can support answering the classical query on key k and input x. The rest of the proof is identical to the case of $(\lambda, \omega(\log(\lambda)))$-PRSGs.

Acknowledgements

This work is supported by the National Science Foundation under Grant No. 2329938 and Grant No. 2341004.

References

[ACC+22] Per Austrin, Hao Chung, Kai-Min Chung, Shiuan Fu, Yao-Ting Lin, and Mohammad Mahmoody. "On the impossibility of key agreements from quantum random oracles". In: *Annual International Cryptology Conference*. Springer. 2022, pp. 165–194 (cit. on pp. 6, 53).

[ACH+23] Abtin Afshar, Kai-Min Chung, Yao-Ching Hsieh, Yao-Ting Lin, and Mohammad Mahmoody. "On the (Im) possibility of Time-Lock Puzzles in the Quantum Random Oracle Model". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2023, pp. 339–368 (cit. on p. 6).

[AGKL23] Prabhanjan Ananth, Aditya Gulati, Fatih Kaleoglu, and Yao-Ting Lin. *Pseudorandom Isometries*. 2023. arXiv: 2311.02901 [quant-ph] (cit. on p. 18).

[AGL24] Prabhanjan Ananth, Aditya Gulati, and Yao-Ting Lin. "A Note on the Common Haar State Model". In: *arXiv preprint arXiv:2404.05227* (2024) (cit. on pp. 1, 59).

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. "Pseudorandom (Function-Like) Quantum State Generators: New Definitions and Applications". In: *Theory of Cryptography Conference*. Springer. 2022, pp. 237–265 (cit. on pp. 3, 18, 59).

[AHY23] Prabhanjan Ananth, Zihan Hu, and Henry Yuen. "On the (im) plausibility of public-key quantum money from collision-resistant hash functions". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2023, pp. 39–72 (cit. on p. 6).

[AKY24] Prabhanjan Ananth, Fatih Kaleoglu, and Henry Yuen. "Simultaneous Haar Indistinguishability with Applications to Unclonable Cryptography". In: *arXiv preprint arXiv:2405.10274* (2024) (cit. on p. 5).

[ALY23] Prabhanjan Ananth, Yao-Ting Lin, and Henry Yuen. "Pseudorandom strings from pseudorandom quantum states". In: *arXiv preprint arXiv:2306.05613* (2023) (cit. on p. 59).

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. "Cryptography from Pseudorandom Quantum States." In: *CRYPTO*. 2022 (cit. on pp. 3, 4, 58, 59).

[BBBV97] Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. "Strengths and weaknesses of quantum computing". In: *SIAM journal on Computing* 26.5 (1997), pp. 1510–1523 (cit. on p. 40).

[BBF13] Paul Baecher, Christina Brzuska, and Marc Fischlin. "Notions of black-box reductions, revisited". In: *Advances in Cryptology-ASIACRYPT 2013: 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I 19*. Springer. 2013, pp. 296–315 (cit. on p. 17).

[BCKM21] 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*. Ed. by Tal Malkin and Chris Peikert. Vol. 12825. Lecture Notes in Computer Science. Springer, 2021, pp. 467–496. DOI: 10.1007/978-3-030-84242-0_17 (cit. on p. 3).

[BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. "On the Computational Hardness Needed for Quantum Cryptography". In: *14th Innovations in Theoretical Computer Science Conference, ITCS 2023*. Schloss Dagstuhl-Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing. 2023, p. 24 (cit. on p. 3).

[BDF+99] Charles H Bennett, David P DiVincenzo, Christopher A Fuchs, Tal Mor, Eric Rains, Peter W Shor, John A Smolin, and William K Wootters. "Quantum nonlocality without entanglement". In: *Physical Review A* 59.2 (1999), p. 1070 (cit. on p. 10).

[BFM19] Manuel Blum, Paul Feldman, and Silvio Micali. "Non-interactive zero-knowledge and its applications". In: *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*. 2019, pp. 329–349 (cit. on p. 3).

[BGH+23] Khashayar Barooti, Alex B. Grilo, Lois Huguenin-Dumittan, Giulio Malavolta, Or Sattath, Quoc-Huy Vu, and Michael Walter. "Public-Key Encryption with Quantum Keys". In: *Theory of Cryptography - 21st International Conference, TCC 2023, Taipei, Taiwan, November 29 - December 2, 2023, Proceedings, Part IV*. Ed. by Guy N. Rothblum and Hoeteck Wee. Vol. 14372. Lecture Notes in Computer Science. Springer, 2023, pp. 198–227. DOI: 10.1007/978-3-031-48624-1_8. URL: https://doi.org/10.1007/978-3-031-48624-1%5C_8 (cit. on p. 53).

[BGVV+23] Samuel Bouaziz, Alex B Grilo, Damien Vergnaud, Quoc-Huy Vu, et al. "Towards the Impossibility of Quantum Public Key Encryption with Classical Keys from One-Way Functions". In: *Cryptology ePrint Archive* (2023) (cit. on p. 6).

[BL18] Fabrice Benhamouda and Huijia Lin. "k-round multiparty computation from k-round oblivious transfer via garbled interactive circuits". In: *Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part II 37*. Springer. 2018, pp. 500–532 (cit. on p. 3).

[BM+24] Samuel Bouaziz, Garazi Muguruza, et al. "Quantum Pseudorandomness Cannot Be Shrunk In a Black-Box Way". In: *Cryptology ePrint Archive* (2024) (cit. on pp. 6, 59).

[BM09] Boaz Barak and Mohammad Mahmoody-Ghidary. "Merkle puzzles are optimal—an O (n 2)-query attack on any key exchange from a random oracle". In: *Annual International Cryptology Conference*. Springer. 2009, pp. 374–390 (cit. on p. 53).

[Bra23] Zvika Brakerski. "Black-Hole Radiation Decoding Is Quantum Cryptography". In: *Annual International Cryptology Conference*. Springer. 2023, pp. 37–65 (cit. on p. 3).

[BS19] 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*. Ed. by Dennis Hofheinz and Alon Rosen. Vol. 11891. Lecture Notes in Computer Science. Springer, 2019, pp. 229–250. DOI: 10.1007/978-3-030-36030-6_10 (cit. on pp. 53, 58, 59).

[BS20] Zvika Brakerski and Omri Shmueli. "Scalable Pseudorandom Quantum States". In: *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Springer, 2020, pp. 417–440. DOI: 10.1007/978-3-030-56880-1_15 (cit. on pp. 53, 58, 59).

[CBB+24] Chi-Fang Chen, Adam Bouland, Fernando GSL Brandão, Jordan Docter, Patrick Hayden, and Michelle Xu. "Efficient unitary designs and pseudorandom unitaries from permutations". In: *arXiv preprint arXiv:2404.16751* (2024) (cit. on p. 58).

[CCHL22] Sitan Chen, Jordan Cotler, Hsin-Yuan Huang, and Jerry Li. "Exponential separations between learning with and without quantum memory". In: *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2022, pp. 574–585 (cit. on p. 5).

[CCS24] Boyang Chen, Andrea Coladangelo, and Or Sattath. "The power of a single Haar random state: constructing and separating quantum pseudorandomness". In: *arXiv preprint arXiv:2404.03295* (2024) (cit. on pp. 3, 14, 59).

[CF01] Ran Canetti and Marc Fischlin. "Universally composable commitments". In: *Advances in Cryptology—CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001 Proceedings 21*. Springer. 2001, pp. 19–40 (cit. on p. 3).

[CGG24] Kai-Min Chung, Eli Goldin, and Matthew Gray. *On Central Primitives for Quantum Cryptography with Classical Communication*. 2024. arXiv: 2402.17715 [cs.CR] (cit. on pp. 6, 37).

[CH14] Eric Chitambar and Min-Hsiu Hsieh. "Asymptotic state discrimination and a strict hierarchy in distinguishability norms". In: *Journal of Mathematical Physics* 55.11 (2014) (cit. on p. 10).

[CLM+14] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. "Everything you always wanted to know about LOCC (but were afraid to ask)". In: *Communications in Mathematical Physics* 328 (2014), pp. 303–326 (cit. on pp. 10, 31).

[CLM23] Kai-Min Chung, Yao-Ting Lin, and Mohammad Mahmoody. "Black-box separations for non-interactive classical commitments in a quantum world". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 144–172 (cit. on pp. 3, 6).

[CLMO13] Andrew M Childs, Debbie Leung, Laura Mančinska, and Maris Ozols. "A framework for bounding nonlocality of state discrimination". In: *Communications in Mathematical Physics* 323 (2013), pp. 1121–1153 (cit. on p. 10).

[CLOS02] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai. "Universally composable two-party and multi-party secure computation". In: *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*. 2002, pp. 494–503 (cit. on p. 3).

[CM24] Andrea Coladangelo and Saachi Mutreja. "On black-box separations of quantum digital signatures from pseudorandom states". In: *arXiv preprint arXiv:2402.08194* (2024) (cit. on pp. 6, 59).

[Col23] Andrea Coladangelo. *Quantum trapdoor functions from classical one-way functions*. Cryptology ePrint Archive, Paper 2023/282. https://eprint.iacr.org/2023/282. 2023. URL: https://eprint.iacr.org/2023/282 (cit. on pp. 4, 22, 59, 60).

[DLT02] David P DiVincenzo, Debbie W Leung, and Barbara M Terhal. "Quantum data hiding". In: *IEEE Transactions on Information Theory* 48.3 (2002), pp. 580–598 (cit. on pp. 10, 31).

[EW02] Tilo Eggeling and Reinhard F Werner. "Hiding classical data in multipartite quantum states". In: *Physical Review Letters* 89.9 (2002), p. 097905 (cit. on pp. 10, 31).

[GB23] Tudor Giurgica-Tiron and Adam Bouland. *Pseudorandomness from Subset States*. 2023. arXiv: 2312.09206 [quant-ph] (cit. on p. 53).

[Gea02] Julio Gea-Banacloche. "Hiding messages in quantum data". In: *Journal of Mathematical Physics* 43.9 (2002), pp. 4531–4536 (cit. on p. 10).

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. "How to construct random functions". In: *Journal of the ACM (JACM)* 33.4 (1986), pp. 792–807 (cit. on pp. 4, 8).

[GJMZ23] Sam Gunn, Nathan Ju, Fermi Ma, and Mark Zhandry. "Commitments to quantum states". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 2023, pp. 1579–1588 (cit. on p. 58).

[GLSV21] 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*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12697. Lecture Notes in Computer Science. Springer, 2021, pp. 531–561. DOI: 10.1007/978-3-030-77886-6_18 (cit. on p. 3).

[GS22] Sanjam Garg and Akshayaram Srinivasan. "Two-round multiparty secure computation from minimal assumptions". In: *Journal of the ACM* 69.5 (2022), pp. 1–30 (cit. on p. 3).

[Har13] Aram W Harrow. "The church of the symmetric subspace". In: *arXiv preprint arXiv:1308.6595* (2013) (cit. on p. 16).

[Har23] Aram W Harrow. "Approximate orthogonality of permutation operators, with application to quantum information". In: *Letters in Mathematical Physics* 114.1 (2023), p. 1 (cit. on pp. 5, 10, 31, 36).

[HBAB19] Saronath Halder, Manik Banik, Sristy Agrawal, and Somshubhro Bandyopadhyay. "Strong quantum nonlocality without entanglement". In: *Physical review letters* 122.4 (2019), p. 040403 (cit. on p. 10).

[HLS05] Patrick Hayden, Debbie Leung, and Graeme Smith. "Multiparty data hiding of quantum information". In: *Physical Review A* 71.6 (2005), p. 062339 (cit. on p. 10).

[HY20] Akinori Hosoyamada and Takashi Yamakawa. "Finding collisions in a quantum world: quantum black-box separation of collision-resistance and one-wayness". In: *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part I 26*. Springer. 2020, pp. 3–32 (cit. on pp. 6, 17).

[IR89] Russell Impagliazzo and Steven Rudich. "Limits on the Provable Consequences of One-Way Permutations". In: *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washington, USA*. Ed. by David S. Johnson. ACM, 1989, pp. 44–61. DOI: 10.1145/73007.73012 (cit. on p. 53).

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. "Pseudorandom Quantum States". In: *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10993. Lecture Notes in Computer Science. Springer, 2018, pp. 126–152. DOI: 10.1007/978-3-319-96878-0_5 (cit. on pp. 3, 53, 58, 59).

[JMW23] Fernando Granha Jeronimo, Nir Magrafta, and Pei Wu. "Subset States and Pseudorandom States". In: *arXiv preprint arXiv:2312.15285* (2023) (cit. on p. 53).

[Kre21] William Kretschmer. "Quantum Pseudorandomness and Classical Complexity". In: *16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference*. Ed. by Min-Hsiu Hsieh. Vol. 197. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 2:1–2:20. DOI: 10.4230/LIPIcs.TQC.2021.2 (cit. on pp. 6, 40, 58).

[KT24] Dakshita Khurana and Kabir Tomer. "Commitments from Quantum One-Wayness". In: *STOC'24 (to appear)* (2024). URL: https://arxiv.org/abs/2310.11526 (cit. on p. 36).

[LC97] Hoi-Kwong Lo and Hoi Fung Chau. "Is quantum bit commitment really possible?" In: *Physical Review Letters* 78.17 (1997), p. 3410 (cit. on p. 3).

[LLLL24] Longcheng Li, Qian Li, Xingjian Li, and Qipeng Liu. "How (not) to Build Quantum PKE in Minicrypt". In: *arXiv preprint arXiv:2405.20295* (2024) (cit. on p. 6).

[LMW23] Alex Lombardi, Fermi Ma, and John Wright. "A one-query lower bound for unitary synthesis and breaking quantum cryptography". In: *arXiv preprint arXiv:2310.08870* (2023) (cit. on p. 58).

[LW12] Benjian Lv and Kaishun Wang. "The energy of Kneser graphs". In: *MATCH Commun. Math. Comput. Chem* 68 (2012), pp. 763–765 (cit. on p. 32).

[May97] Dominic Mayers. "Unconditionally secure quantum bit commitment is impossible". In: *Physical review letters* 78.17 (1997), p. 3414 (cit. on p. 3).

[MNY23] Tomoyuki Morimae, Barak Nehoran, and Takashi Yamakawa. *Unconditionally Secure Commitments with Quantum Auxiliary Inputs*. 2023. arXiv: 2311.18566 [quant-ph] (cit. on pp. 3, 9, 14, 29).

[MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. "Pseudorandom unitaries with non-adaptive security". In: *arXiv preprint arXiv:2402.14803* (2024) (cit. on pp. 58, 59).

[MWW09] William Matthews, Stephanie Wehner, and Andreas Winter. "Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding". In: *Communications in Mathematical Physics* 291 (2009), pp. 813–843 (cit. on p. 10).

[MY21] Tomoyuki Morimae and Takashi Yamakawa. *Quantum commitments and signatures without one-way functions*. 2021. DOI: 10.48550/ARXIV.2112.06369 (cit. on pp. 3, 9, 10, 29, 53).

[MY23] Tomoyuki Morimae and Takashi Yamakawa. *One-Wayness in Quantum Cryptography*. 2023. arXiv: 2210.03394 [quant-ph] (cit. on p. 3).

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667 (cit. on p. 13).

[NS03] Ashwin Nayak and Peter Shor. "Bit-commitment-based quantum coin flipping". In: *Phys. Rev. A* 67 (1 Jan. 2003), p. 012304. DOI: 10.1103/PhysRevA.67.012304. URL: https://link.aps.org/doi/10.1103/PhysRevA.67.012304 (cit. on p. 31).

[OW16] Ryan O'Donnell and John Wright. "Efficient quantum tomography". In: *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*. 2016, pp. 899–912 (cit. on p. 42).

[PNC14] Marco Piani, Varun Narasimhachar, and John Calsamiglia. "Quantumness of correlations, quantumness of ensembles and quantum data hiding". In: *New Journal of Physics* 16.11 (2014), p. 113001 (cit. on p. 10).

[Qia23] Luowen Qian. "Unconditionally secure quantum commitments with preprocessing". In: *Cryptology ePrint Archive* (2023) (cit. on p. 3).

[RTV04] Omer Reingold, Luca Trevisan, and Salil Vadhan. "Notions of reducibility between cryptographic primitives". In: *Theory of Cryptography Conference*. Springer. 2004, pp. 1–20 (cit. on p. 17).

[Yan22] Jun Yan. "General properties of quantum bit commitments". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2022, pp. 628–657 (cit. on pp. 10, 29).

A Related Work

A.1 Quantum Pseudorandomness: State of the Art

We present the state of the art of the pseudorandomness notions in the quantum world. We will only restrict our attention to two notions relevant to this work. The open problems will be *italicized*.

Pseudorandomnes State Generators (PRSGs). The concept of pseudorandom state generators (PRSGs) was introduced in a seminal work by Ji, Liu and Song [JLS18]. Roughly speaking, it states that any computationally bounded adversary cannot distinguish whether it receives many copies of a state produced using a pseudorandom state generator on a uniform key versus many copies of a single Haar state. We summarise the state of the art of PRSGs below. We use the notation (λ, n)-PRSG to denote a PRSG with λ being the key length and n being the output length. The number of copies of the state given to the adversary is denoted to be t. Unless otherwise stated, t will be an arbitrary polynomial in λ that is not fixed ahead of time. If t is indeed fixed ahead of time then we denote such a notion by (λ, n, t)-PRSGs.

- $n > \lambda$ (stretch): It is known that (λ, n)-PRSGs exist assuming one-way functions [JLS18; BS19; BS20] or even pseudorandom unitaries[32] [JLS18; MPSY24; CBB+24]. Even to design $(\lambda, n, 1)$-PRSG, we need computational assumptions and in fact, $(\lambda, n, 1)$-PRSG is implied by multi-copy PRSGs with output length $\Omega(\log(\lambda))$ [GJMZ23]. *However, it is not known if stretch (n, λ)-PRSGs exist under weaker assumptions*, although we do have some candidates inspired from random circuits [AQY22]. There is some evidence to believe that stretch PRSGs might be weaker than any existing classical cryptographic assumption [Kre21; LMW23].
- $n \leq \lambda$: This can be broken down into three parameter regimes:
  - $n < c \cdot \log(\lambda)$, for some $c \in \mathbb{R}$: (n, λ)-PRSGs exists unconditionally [BS20].

[32] An efficiently computable keyed circuit is a pseudorandom unitary if any adversary cannot distinguish whether it has oracle access to the keyed circuit or a Haar unitary.

– $n \in \Omega(\log(\lambda))$: for $n \geq \log(\lambda)$, it was shown [AGQY22] that (λ, n)-PRSGs cannot be unconditionally secure. However, assuming one-way functions, (n, λ)-PRSGs was shown to exist [JLS18; BS19; BS20] or even pseudorandom unitaries [JLS18; MPSY24]. *Designing (λ, n)-PRSGs from weaker assumptions is an interesting direction.* There seems to be a separation between $n = \Theta(\log(\lambda))$ and $n = \Omega(\log(\lambda))$ as shown in [ALY23; BM+24; CM24]. On the other hand, when t is known ahead of time, (λ, n, t)-PRSGs with statistical security, where λ could be much larger than n, are implied by state designs.

Pseudorandom Function-Like State Generators (PRFSGs). The notion of pseudorandom function-like state generators (PRFSGs) was introduced in the work of [AQY22] as a quantum analogue of pseudorandom functions. Unlike pseudorandom state generators, in the case of PRFSG, we can use the same key to generate many pseudorandom states, indexed by classical strings. We summarise the state of the art of PRFSGs below. We use the notation (λ, m, n)-PRFSG to denote a PRFSG with λ being the key length, m being the input length and n being the output length. The number of copies of the state given to the adversary is denoted to be t. Unless otherwise stated, t will be an arbitrary polynomial in λ and not fixed ahead of time. If t is indeed fixed ahead of time then we denote such a notion by (λ, m, n, t)-PRFSGs.

- $m = O(\log(\lambda))$: It is known that (λ, m, n)-PRFSGs, for some n, exist based on PRSGs.
- $m = \omega(\log(\lambda))$: While we know how to construct (λ, m, n)-PRFSGs from one-way functions [AGQY22], *it is not yet known that stretch (λ, m, n)-PRFSGs exist assuming PRSGs.*

In the case when t is known ahead of time, unitary designs can be used to achieve statistically secure PRFSGs.

A.2 Comparison with [CCS24] and [AGL24]

The common Haar state model was concurrently introduced by [CCS24] and an earlier version of this work [AGL24]. Even though the main theme – studying feasibility and separations in the CHS model – was common among both the works, there were two main differences. Firstly, [CCS24] showed the feasibility of 1-copy PRSGs whereas [AGL24] showed the feasibility of bounded-copy PRSGs with simplified construction and its analysis. Secondly, [CCS24] showed a separation between 1-copy PRS and unbounded-copy PRS which is unique to their work.

Subsequent to both [CCS24] and [AGL24], we improved upon [AGL24] to show that even bounded-query PRFSGs exist in the CHS model. We also demonstrate optimality, in terms of the query bound, of our construction. We also added separation results in the revised version (Section 7, Section 8 and Section 9).

B Alternative Proof of Lemma 4.8

Proof sketch of Lemma 4.8. The first part of the proof is the same as in [Col23]. Here we introduce the required notations and omit the details. Let $d := 2^n$ and

$$\begin{aligned}
\sigma := \sum_{x\in\{0,1\}^n} \rho_x &= \sum_{x\in\{0,1\}^n} \mathop{\mathbb{E}}_{|\psi\rangle\leftarrow\mathcal{H}(2^n)} \left[(Z^x \otimes I^{\otimes m})|\psi\rangle\langle\psi|^{\otimes m+1}(Z^x \otimes I^{\otimes m})\right] \\
&= \mathop{\mathbb{E}}_{\vec{t}\in\mathcal{I}_{d,m+1}} \sum_{x\in\{0,1\}^n} \left[(Z^x \otimes I^{\otimes m})|s(\vec{t})\rangle\langle s(\vec{t})|(Z^x \otimes I^{\otimes m})\right] \\
&= \frac{d}{\binom{d+m}{m+1}} \cdot \sum_{\vec{t}\in\mathcal{I}_{d,m+1}} \sum_{j\in\{0,1\}^n} (|j\rangle\langle j| \otimes I^{\otimes m})|s(\vec{t})\rangle\langle s(\vec{t})|(|j\rangle\langle j| \otimes I^{\otimes m}) \\
&= \frac{d}{\binom{d+m}{m+1}} \cdot \sum_{j\in\{0,1\}^n} \sum_{0\leq r\leq m} \sum_{\vec{t}\in T^m_{j,r}} \frac{r+1}{m+1} |j\rangle\langle j| \otimes |s(\vec{t})\rangle\langle s(\vec{t})|.
\end{aligned}$$

So we have

$$\sigma^{-1/2} = \sqrt{\frac{\binom{d+m}{m+1}}{d}} \cdot \sum_{j\in\{0,1\}^n} \sum_{0\le r\le m} \sum_{\vec{t}\in T^m_{j,r}} \sqrt{\frac{m+1}{r+1}} |j\rangle\langle j| \otimes |s(\vec{t})\rangle\langle s(\vec{t})|.$$

Note that $\sigma^{-1/2}$ is PSD with the largest eigenvalue $\left\|\sigma^{-1/2}\right\| = \sqrt{\binom{d+m}{m+1}(m+1)/d}$ (when $r=0$). In [Col23], the main technicality is to show Equation (28):

$$\mathop{\mathbb{E}}_{x\leftarrow\{0,1\}^n} \mathrm{Tr}\Big(\rho_x \sigma^{-1/2} \rho_x \sigma^{-1/2}\Big) \le C' \cdot \left(\frac{m}{d} + \frac{m^7}{d^3}\right),$$

where $C' > 0$ is some constant. Here, we provide an alternative and simpler proof. Since $\sigma^{-1/2}$ and ρ_x are both PSD, the matrix $\sigma^{-1/2}\rho_x\sigma^{-1/2}$ is PSD as well. As ρ_x is a density matrix, we have

$$\mathrm{Tr}\Big(\rho_x \cdot \sigma^{-1/2}\rho_x\sigma^{-1/2}\Big) \le \left\|\sigma^{-1/2}\rho_x\sigma^{-1/2}\right\|.$$

Then we use the submultiplicativity of the operator norm to obtain

$$\begin{aligned}
&\left\|\sigma^{-1/2}\rho_x\sigma^{-1/2}\right\| \\
&\le \left\|\sigma^{-1/2}\right\| \cdot \left\|Z^x \otimes I^{\otimes m}\right\| \cdot \left\|\mathop{\mathbb{E}}_{\vec{t}\in\mathcal{I}_{d,m+1}} |s(\vec{t})\rangle\langle s(\vec{t})|\right\| \cdot \left\|Z^x \otimes I^{\otimes m}\right\| \cdot \left\|\sigma^{-1/2}\right\| \\
&= \left\|\sigma^{-1/2}\right\|^2 \cdot \left\|\mathop{\mathbb{E}}_{\vec{t}\in\mathcal{I}_{d,m+1}} |s(\vec{t})\rangle\langle s(\vec{t})|\right\| \qquad \text{(unitaries have a unit operator norm)} \\
&= \frac{\binom{d+m}{m+1}\cdot(m+1)}{d} \cdot \frac{1}{\binom{d+m}{m+1}} = \frac{m+1}{d}.
\end{aligned}$$

Hence, it holds that

$$\mathop{\mathbb{E}}_{x\leftarrow\{0,1\}^n} \mathrm{Tr}\Big(\rho_x \sigma^{-1/2} \rho_x \sigma^{-1/2}\Big) \le \frac{m+1}{d}. \qquad \square$$