A Note on the Common Haar State Model

Prabhanjan Ananth[*] UCSB

Aditya Gulati[†] UCSB

Yao-Ting Lin[‡] UCSB

Abstract

Common random string model is a popular model in classical cryptography with many constructions proposed in this model. We study a quantum analogue of this model called the common Haar state model, which was also studied in an independent work by Chen, Coladangelo and Sattath (arXiv 2024). In this model, every party in the cryptographic system receives many copies of one or more i.i.d Haar states.

Our main result is the construction of a statistically secure PRSG with: (a) the output length of the PRSG is strictly larger than the key size, (b) the security holds even if the adversary receives $O\left(\frac{\lambda}{(\log(\lambda))^{1.01}}\right)$ copies of the pseudorandom state. We show the optimality of our construction by showing a matching lower bound. Our construction is simple and its analysis uses elementary techniques.

Contents

[*] prabhanjan@cs.ucsb.edu

[†] adityagulati@ucsb.edu

[‡] yao-ting_lin@ucsb.edu

1 Introduction

In classical cryptography, the common random string and the common reference string models were 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, thus avoiding the need for a trusted setup. As a result, the common random string model is 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 secure under 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 this case, there is an option to define models that are inherently quantum. 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 many copies of this quantum state. Indeed, two works by Morimae, Nehoran and Yamakawa [MNY23] and Qian [Qia23] consider this model, termed as the *common quantum reference string model* (CQRS). They proposed 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; BCQ22; 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] makes the contributions of [MNY23; Qia23] quite interesting.

While CQRS is a quantum analogue of common reference string model, we can ask if there is a quantum analogue of the common random string model. An independent and concurrent recent work by Chen, Coladangelo and Sattath [CCS24] (henceforth, referred to as CCS) introduced a model, called the *common Haar random state model* (CHRS). In this model, every party in the system receives many copies of many i.i.d Haar states. They presented constructions of pseudorandomness and commitments in this model. The goal of our work is to study this model further.

Our Work. We consider a simpler version of the common Haar random state model, wherein every party receives many copies of one Haar state. Feasibility results in our model are stronger than the model considered by CCS whereas the negative results would be weaker. We call our model the common Haar state model (CHS).

Similar to CCS, we present constructions of pseudorandom states and commitments in the CHS model.

Statistical Pseudorandom States (i.e., State Designs): 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. Constructions of pseudorandom states are known from one-way functions [JLS18; BS19; AGQY22; JMW23; GB23]. It is known that for a broad range of parameters, we need to impose the restriction that the adversary is computationally bounded [AGQY22]. One such case is when the output length of the state generator is larger than the length of the key; referred to as *stretch* PRSGs. In this case, even if the adversary gets one copy of the state then it can break the pseudorandomness property if it is unbounded.

We consider the possibility of statistically secure stretch PRSGs. We show the following. In the theorem below, we denote λ to be the key length of the PRSG.

Theorem 1.1 (Informal)**.** *There is a statistically secure PRSG in the CHS model satisfying the following: (a) the output length of PRSG is $> \lambda$ and, (b) the security holds as long as the adversary receives $O\left(\frac{\lambda}{(\log(\lambda))^{1+\varepsilon}}\right)$ copies, for some constant $\varepsilon > 0$.*

This improves upon CCS [CCS24] who only showed 1-copy stretch PRSG exists in their model. Moreover, our construction and in particular, our analysis, is arguably simpler and elementary compared to CCS. Another advantage of our work is that 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 a paraphrased version of the above theorem.

Interestingly, both works design PRSGs which 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 $O\left(\frac{\lambda}{\log(\lambda)}\right)$ copies. We show this is not possible.

Theorem 1.2 (Informal)**.** *There does not exist a secure PRSG in the CHS model satisfying the following: (a) the PRSG uses only one copy of the Haar state in the CHS model, (b) the adversary receives $\Omega(\frac{\lambda}{\log(\lambda)})$ copies of the pseudorandom state and, (c) the output length is $\omega(\log(\lambda))$.*

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. On the other hand, for the special case when the PRSG only takes one copy of the Haar state, we believe our result yields better parameters.

<u>Commitments</u>: We show the following.

Theorem 1.3 (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. Even the proof techniques seem to be similar.

Future Directions. The work by [CCS24] and our work initiates an interesting research direction: to build cryptography in the common Haar state model. It would be interesting to the feasibility of other cryptographic constructions in this model. It would also be interesting to understand other variants of this model. One such variant is the Haar random oracle model, studied by [BFV19; CM21]. We leave open the question of investigating the relationship between these different models and also developing toolkits that will aid us in proving (in)feasibility results in these models.

2 Preliminaries

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

2.1 Notation

- We use $[n]$ to denote $\{1,\ldots,n\}$ and $[0:n]$ to denote $\{0,1,\ldots,n\}$.
- We denote S_t to be the symmetric group of degree t.
- For a set A and $t \in \mathbb{N}$, we define $A^t := \{(a_1,\ldots,a_t) : \ \forall i \in [t],\ a_i \in A\}$.
- For $\sigma \in S_t$ and $\mathbf{v} = (v_1,\ldots,v_t)$, we define $\sigma(\mathbf{v}) := (v_{\sigma(1)},\ldots,v_{\sigma(t)})$.
- We use $\mathcal{D}(H)$ to denote 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 the trace distance between quantum states ρ,ρ' by $\mathsf{TD}(\rho,\rho') := \frac{1}{2}\|\rho-\rho'\|_1$.
- We denote the Haar measure over n qubits by $\mathcal{H}_n$.

2.2 Pseudorandom State Generators

We recall the definition of statistical pseudorandom state generators (PRS).

Definition 2.1. We say that a QPT algorithm G is an ℓ-copy statistical PRS generator if the following holds:

- **State Generation**: For any $\lambda \in \mathbb{N}$ and $k \in \{0,1\}^\lambda$, the algorithm G is a quantum channel that satisfies
$$G(|k\rangle) = |\psi_k\rangle\langle\psi_k|,$$
for some $n(\lambda)$-qubit state $|\psi_k\rangle$.
- **Psuedorandomness**: For any computationally unbounded adversary A, there exists a negligible fuctions $\mathrm{negl}(\cdot)$ such that:
$$\left| \Pr_{k \leftarrow \{0,1\}^\lambda} \left[A_\lambda \left(G(|k\rangle)^{\otimes \ell} \right) = 1 \right] - \Pr_{|\varphi\rangle \leftarrow \mathcal{H}_n} \left[A_\lambda \left(|\varphi\rangle^{\otimes \ell} \right) = 1 \right] \right| \leq \mathrm{negl}(\lambda).$$

If G statisfies the above security definition for every polynomial ℓ, we say that G is an unbounded poly-copy statistical PRS generator.

2.3 Quantum Commitments

We recall the definition of commitment schemes in the CRQS model [MNY23].

Definition 2.2 (Quantum commitments in the Common Reference Quantum State (CRQS) model [MNY23])**.** A (non-interactive) quantum commitment scheme in the CRQS model is given by a tuple of the setup algorithm Setup, committer C, and receiver R, all of which are uniform QPT algorithms. The scheme is divided into three phases, the setup phase, commit phase, and reveal phase as follows:

- Setup phase: Setup takes 1^λ as input, uniformly samples a classical key $k \leftarrow K_\lambda$, generates two copies of the same pure state $|\psi_k\rangle$ and sends one copy each to C and R.
- Commit phase: C takes $|\psi_k\rangle$ given by the setup algorithm 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 $|\psi_k\rangle$ given by the setup algorithm and $(b, \mathsf{C}, \mathsf{R})$ given by C as input, and outputs b if it accepts and otherwise outputs $\perp$.

Definition 2.3 (t-copy statistical hiding [MNY23])**.** A quantum commitment scheme (Setup, C, R) in the CRQS model satisfies t-copy statistical hiding if for any non-uniform unbounded-time algorithm $\mathcal{A}$,

$$\Bigg| \Pr\Big[\mathcal{A}(1^\lambda, |\psi_k\rangle^{\otimes t}, \mathrm{Tr}_{\mathsf{R}}(\sigma_{\mathsf{CR}})) = 1 : {}_{\sigma_{\mathsf{CR}} \leftarrow C_{\mathsf{com}}(|\psi_k\rangle, 0)}^{k \leftarrow K_\lambda,}\Big] - \Pr\Big[\mathcal{A}(1^\lambda, |\psi_k\rangle^{\otimes t}, \mathrm{Tr}_{\mathsf{R}}(\sigma_{\mathsf{CR}})) = 1 : {}_{\sigma_{\mathsf{CR}} \leftarrow C_{\mathsf{com}}(|\psi_k\rangle, 1)}^{k \leftarrow K_\lambda,}\Big] \Bigg| \leq \mathrm{negl}(\lambda),$$

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

Definition 2.4 (Statistical sum-binding [MNY23])**.** A quantum commitment scheme (Setup, C, R) in the CQRS model satisfies statistical sum-binding if the following holds. For any pair of non-uniform unbounded-time malicious committers C_0^* and C_1^* that take the classical key k, which is sampled by the setup algorithm, 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

$$p_0 + p_1 \leq 1 + \mathrm{negl}(\lambda).$$

2.4 Common Haar State Model

The Common Haar State (CHS) model is a variant of the Common Reference Quantum State (CRQS) model. In this model, all parties receive polynomially many copies of a qubit state sampled from the Haar distribution.

2.4.1 Pseudorandom State Generators in the CHS model

Definition 2.5 (ℓ-copy PRS in CHS model)**.** Let $|\vartheta\rangle$ denote the $n(\lambda)$-qubit common Haar state. We say that a QPT algorithm G is an ℓ-copy statistical PRS generator 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-qubit state $|\vartheta\rangle$,

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

  for some n-qubit state $|\vartheta_k\rangle$. We sometimes write $G_k(|\vartheta\rangle)$ for brevity.[1]

- **Pseudorandomness**: For any polynomial $t(\cdot)$ and computationally unbounded adversary A, there exists a negligible function $\text{negl}(\cdot)$ such that:

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

We define a stronger variant of the above notion called a multi-key ℓ-copy PRS generator. Looking ahead, our construction of PRS in Section 3.1 satisfies this stronger definition. In addition, we show in Section 4 that multi-key 1-copy stretch PRS generator in the CHS model implies statistically hiding, statistically sum-binding commitments in the CHS model.

Definition 2.6 (Multi-key ℓ-copy PRS in CHS model)**.** Let $|\vartheta\rangle$ denote the $n(\lambda)$-qubit common Haar state. We say that a QPT algorithm G is a multi-key ℓ-copy statistical PRS generator 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-qubit state $|\vartheta\rangle$,

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

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

- **Multi-key Pseudorandomness**: For any polynomial $t(\cdot)$, $p(\cdot)$ and computationally unbounded adversary A, there exists a negligible function $\text{negl}(\cdot)$ such that:

$$\left| \Pr_{\substack{k_1,\ldots,k_p\leftarrow\{0,1\}^\lambda \\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[A_\lambda\left(\otimes_{i=1}^p G_{k_i}(|\vartheta\rangle)^{\otimes\ell}, |\vartheta\rangle^{\otimes t}\right) = 1\right] - \Pr_{\substack{|\varphi_1\rangle,\ldots,|\varphi_p\rangle\leftarrow\mathcal{H}_n \\ |\vartheta\rangle\leftarrow\mathcal{H}_n}} \left[A_\lambda\left(\otimes_{i=1}^p |\varphi_i\rangle^{\otimes\ell}, |\vartheta\rangle^{\otimes t}\right) = 1\right] \right| \le \text{negl}(\lambda).$$

Remark 2.7. Note that in the plain model, PRS implies multi-key PRS because the PRS does not share randomness for different keys. This is not trivially true in CHS model as the generator for all keys shares the same common Haar state.

[1] More generally, the generation algorithm could take multiple copies of the common Haar state as input or output a state of size different from the CHS but we focus on generation algorithms taking only one copy of the Haar state and the output of the generator is the same size as the CHS.

2.4.2 Quantum Commitments in the CHS model

Definition 2.8 (Quantum commitments in the Common Haar State (CHS) model)**.** A (non-interactive) quantum commitment scheme in the CHS model is given by a tuple of the committer C and receiver R, all of which are uniform QPT algorithms. Let $|\vartheta\rangle$ be the $n(\lambda)$-qubit common Haar state. The scheme is divided into two phases, commit phase, and reveal phase as follows:

- Commit phase: C takes $|\vartheta\rangle^{\otimes p}$ for some polynomial $p(\cdot)$ 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 $|\vartheta\rangle^{\otimes p}$ and $(b, \mathsf{C}, \mathsf{R})$ given by C as input, and outputs b if it accepts and otherwise outputs $\perp$.

Definition 2.9 (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-time algorithm $\mathcal{A}$, and any polynomial $t(\cdot)$, there exists a negligible function $\mathrm{negl}(\cdot)$ such that

$$\Bigg| \Pr\Big[\mathcal{A}(1^\lambda, |\vartheta\rangle^{\otimes t}, \mathrm{Tr}_{\mathsf{R}}(\sigma_{\mathsf{CR}})) = 1 : {}^{|\vartheta\rangle \leftarrow \mathcal{H}_n,}_{\sigma_{\mathsf{CR}} \leftarrow C_{\mathsf{com}}(|\vartheta\rangle^{\otimes p}, 0)}\Big] - \Pr\Big[\mathcal{A}(1^\lambda, |\vartheta\rangle^{\otimes t}, \mathrm{Tr}_{\mathsf{R}}(\sigma_{\mathsf{CR}})) = 1 : {}^{|\vartheta\rangle \leftarrow \mathcal{H}_n,}_{\sigma_{\mathsf{CR}} \leftarrow C_{\mathsf{com}}(|\vartheta\rangle^{\otimes p}, 1)}\Big] \Bigg| \leq \mathrm{negl}(\lambda),$$

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

Definition 2.10 (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-time malicious committers C_0^* and C_1^* that take $|\vartheta\rangle^{\otimes T}$ 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

$$p_0 + p_1 \leq 1 + \mathrm{negl}(\lambda).$$

2.5 Symmetric Subspaces, Type States, and Haar States

The proof of facts and lemmas 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 $\mathbf{v}$.[2] 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 2.11 (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

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

[2] 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 2.12 (Average of copies of Haar-random states)**.** For all $N, t \in \mathbb{N}$, we have

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

Definition 2.13 (ℓ-fold n-prefix collision-free types)**.** Let $n, m, t, \ell \in \mathbb{N}$ such that $t \geq \ell$ and $T \in [0:t]^{2^{n+m}}$. We say T is *ℓ-fold n-prefix collision-free* if for all pairs of ℓ-subsets $\mathcal{S}, \mathcal{T} \subseteq \mathsf{mset}(T)$, 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 $\mathcal{I}_{n,m}^{(\ell)}(t) := \{T \in [0:t]^{2^{n+m}} : T \text{ is } \ell\text{-fold } n\text{-prefix collision-free}\}$.

For a fixed t, one can easily verify that ℓ-fold n-prefix collision-freeness implies ℓ'-fold n-prefix collision-freeness for $\ell > \ell'$, and 1-fold n-prefix collision-freeness is equivalent to the standard collision-freeness.

Lemma 2.14. If $\ell = o(2^n)$, then $\Pr_{T\leftarrow[0:t]^{2^{n+m}}}[T \in \mathcal{I}_{n,m}^{(\ell)}(t)] = 1 - O(t^{2\ell}/2^n)$.

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

Lemma 2.15. For any $\mathbf{v} \in \{0,1\}^{(n+m)t}$ such that $\mathsf{type}(\mathbf{v}) \in \mathcal{I}_{n,m}^{(\ell)}(t)$ and $\sigma \in S_t$, define

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

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

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

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

Therefore, after averaging over k,

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

Since $\mathsf{type}(\mathbf{v}) \in \mathcal{I}_{n,m}^{(\ell)}(t)$, the condition $\oplus_{i=1}^{\ell} v_i = \oplus_{i=1}^{\ell} v_{\sigma(i)}$ 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 in the technical heart of this work. It says that the action of applying random Z^k on ℓ-fold n-prefix collision-free types T has the following "classical" probabilistic interpretation: the output is identically distributed to first uniformly sampling an ℓ-subset $X \subset T$ and then outputting $|X\rangle\langle X| \otimes |T \setminus X\rangle\langle T \setminus X|$.

Lemma 2.16. For any $T \in \mathcal{I}_{n,m}^{(\ell)}(t)$,

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

where X is a uniform ℓ-subset of T.[3]

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

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

Then from the previous lemma (Lemma 2.15)

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

For the first equality, we use Lemma 2.15 and decompose $\sigma = \sigma_1 \circ \sigma_2$ for some σ_1, σ_2 such that $\sigma_1(x) = x$ for all $x \in \{\ell+1, \ell+2, \cdots, t\}$ and $\sigma_2(y) = y$ for all $y \in \{1, 2, \cdots, \ell\}$, which uniquely correspond to elements in S_ℓ and $S_{t-\ell}$. The second equality follows by denoting the first ℓ part of $\mathbf{v}$ by $\mathbf{v}_{[1:\ell]}$ and the last $t-\ell$ part of $\mathbf{v}$ by $\mathbf{v}_{[\ell+1:t]}$. The third equality holds because sampling $\mathbf{v}$ from T is equivalent to sampling $X \subset T$ followed by assigning order to elements in X and $T \setminus X$. ☐

3 ℓ-copy statistical PRS in the CHS model

In this section, we discuss the construction of ℓ-copy statistical PRS in the CHS model for $\ell = O(\lambda/\log(\lambda)^{1+\epsilon})$ (for any constant $\epsilon > 0$) and length of the common Haar state $n \geq \lambda$. We also show that the construction satisfies multikey security for the same parameters. Further, we complement our result by showing that for $n = \omega(\log(\lambda))$, achieving an ℓ-copy statistical PRS in the CHS model for $\ell = \Omega(\lambda/\log(\lambda))$ is impossible (similarly for the multikey case), this shows that our construction is optimal (best one can hope for) for $n \geq \lambda$.

Theorem 3.1. *For all constants $\epsilon > 0$, there exists multi-key $O(\lambda/\log(\lambda)^{1+\epsilon})$-copy statistical stretch PRS in the CHS model.*

[3] Since T is collision-free, we can interpret it as a set.

3.1 Construction

In this section, we assume that $n(\lambda) \geq \lambda$. We define the construction as follows: on input $k \in \{0,1\}^\lambda$ of the n-qubit common Haar state $|\vartheta\rangle$,

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

Note that when $n(\lambda) > \lambda$, our construction is a *stretch* PRS.

Lemma 3.2 (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 using hybrid arguments:

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.[4] 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 $|T_1\rangle \otimes |T_2\rangle$.
By Lemma 2.14, the trace distance between Hybrid 1 and Hybrid 2 is $O((t + \ell)^{2\ell}/2^\lambda)$. From Lemma 2.16, the output of Hybrid 2 is

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

Hence, Hybrid 2 is equivalent to Hybrid 3. From now on, we will prove the closeness of the remaining hybrids by classical arguments. Again by Lemma 2.14, 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 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 collision bound. Collecting the probabilities completes the proof.

□

[4] Since T might have collision, T_1 is a multiset of size ℓ.

Remark 3.3. From Lemma 3.2, we conclude that the construction given above is an ℓ-copy statistical PRS in the CRHS model for $\ell = O(\lambda/\log(\lambda)^{1+\epsilon})$ (for any constant $\epsilon > 0$).

By the following lemma, we can also show that the above construction is a multi-key ℓ-copy statistical PRS in the CRHS model for $\ell = O(\lambda/\log(\lambda)^{1+\epsilon})$ (for any constant $\epsilon > 0$):

Lemma 3.4 (Multi-key pseudorandomness)**.** Let G be as defined 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 $\mathsf{TD}\left(\rho, \sigma\right) = O\left(\frac{p\cdot(p\ell+t)^{2\ell}}{2^\lambda}\right)$.

Proof. For $j = 0, 1, \ldots, p$, we define the following (hybrid) density matrices:[5]

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

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

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

and

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

By the monotonicity of trace distance (i.e., $\mathsf{TD}(\mathcal{E}(X), \mathcal{E}(Y)) \leq \mathsf{TD}(X, Y)$ for any quantum channel $\mathcal{E}$) and setting $\mathcal{E} := \bigotimes_{i=j+2}^{p} \mathbb{E}_{k_i \leftarrow \{0,1\}^\lambda}[G_{k_i}(\cdot)^{\otimes \ell}]$,[6] we have

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

where the last equality follows from Lemma 3.2. Applying the triangle inequality completes the proof. $\square$

As a remark, note that Lemma 3.2 gives a simpler proof of the following theorem in [Col23]:

Lemma 3.5 ([Col23, Lemma 5])**.** Consider the ensemble of states:

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

[5] 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.

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

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 $\ell = 1, t = m, n = \lambda$ in Lemma 3.2 and a hybrid, the success probability is at most $O(m^2/2^n)$ plus the probability of inverting x when the input is σ, which is at most $1/2^n$ since σ is independent of x.

In Appendix A, we further give another proof by simplifying the calculation in Lemma 3.5, which may be of independent interest. Moreover, we eliminate the $m^7/2^{3n}$ term.

3.2 Impossibility of a special class of PRS in CHS model

In this subsection, 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 3.6. *ℓ-copy statistical PRS is impossible in the CHS model if (a) the generation algorithm uses only one copy of the common Haar state, (b) $\ell = \Omega(\lambda/\log(\lambda))$ and (c) the length of the common Haar state is $\omega(\log(\lambda))$.*

Proof. We prove this by showing that for $t(\lambda) := \lambda^3$ and $\ell(\lambda) := \lambda/\log(\lambda)$, there exists a (computationally unbounded) adversary $\mathcal{A}$ such that

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

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

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

and

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

The adversary $\mathcal{A}$ 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

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

Now, by construction, we have

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

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

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

$$\leq \frac{\mathrm{rank}(\rho_0)}{\binom{2^n+\ell-1}{\ell}\binom{2^n+t-1}{t}} = \frac{\mathrm{rank}(\rho_0)}{\mathrm{rank}(\rho_1)}.$$

A direct calculation yields:

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

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. □

Note that since ℓ-copy statistical PRS in the CHS model implies multi-key ℓ-copy statistical PRS in the CHS model, we also have the following:

Theorem 3.7. *Multi-key ℓ-copy statistical PRS is impossible in the CHS model if (a) the generation algorithm uses only one copy of the common Haar state, (b) $\ell = \Omega(\lambda/\log(\lambda))$ and (c) the length of the common Haar state is $\omega(\log(\lambda))$.*

Proof. Since ℓ-copy statistical PRS in the CHS model implies multi-key ℓ-copy statistical PRS in the CHS model, by Theorem 3.6, multi-key ℓ-copy statistical PRS is impossible in CHS model for $\ell = \Omega(\lambda/\log(\lambda))$. □

4 Quantum commitments in 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], adapting it to the CHS model and providing a formal proof of its security. In contrast to the scheme in [MY21], our construction is not in the canonical form [Yan22]. Hence, we need SWAP tests to verify rather than uncomputing, this makes the proof of binding more involved. Our scheme relies on the multi-key pseudorandomness property of the construction giving in Section 3.1 for hiding.

4.1 Construction

We assume that $n(\lambda) \geq \lambda + 1$ for all $\lambda \in \mathbb{N}$. Our construction is shown in Figure 1.

4.2 Proof of Correctness, Hiding, and Binding

Clearly, the construction given in Figure 1 has perfect correctness.

Theorem 4.1. *The construction given in Figure 1 satisfies poly-copy statistical hiding and statistical sum binding.*

Proof of Theorem 4.1.

Poly-copy statistical hiding. It follows immediately from Lemma 3.4 by setting $\ell = 1$.

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

- Use $p(\lambda) = \lambda$ 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 the register C to the receiver.

Reveal phase:

- The committer sends b and the 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 1: Commitment scheme in the CHS model

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

$$\begin{aligned}
&F(\mathrm{Tr}_{\mathsf{R}_i}(|\psi_0\rangle\langle\psi_0|_{\mathsf{C}_i\mathsf{R}_i}), \mathrm{Tr}_{\mathsf{R}_i}(|\psi_1\rangle\langle\psi_1|_{\mathsf{C}_i\mathsf{R}_i})) \\
=&F\left(\underbrace{\frac{1}{2^\lambda} \sum_{k\in\{0,1\}^\lambda} (Z^k \otimes I_{n-\lambda})|\vartheta\rangle\langle\vartheta|_{\mathsf{C}_i} (Z^k \otimes I_{n-\lambda})}_{\rho_0}, \frac{I_{\mathsf{C}_i}}{2^n}\right) \\
=&2^{-n} \cdot \mathrm{Tr}(\sqrt{\rho_0})^2 \\
\leq&2^{-n} \cdot \mathrm{rank}(\sqrt{\rho_0}) \cdot \mathrm{Tr}(\rho_0) \\
\leq&2^{-n} \cdot 2^\lambda \cdot 1 = 2^{-(n-\lambda)},
\end{aligned} \tag{3}$$

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 $\mathrm{Tr}(\rho)^2 \leq \mathrm{rank}(\rho) \cdot \mathrm{Tr}(\rho^2)$ for $\rho \succeq 0$; the second inequality is because $\mathrm{rank}(\sqrt{\rho}) = \mathrm{rank}(\rho)$ for $\rho \succeq 0$ and $\mathrm{rank}(X+Y) \leq \mathrm{rank}(X) + \mathrm{rank}(Y)$.

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

$$p_b := \mathrm{Tr}\left(M_{\mathsf{CR}}^{(b)} \underbrace{\mathrm{Tr}_{\mathsf{E}}(U_{\mathsf{RE}}^{(b)} |\Phi\rangle\langle\Phi|_{\mathsf{CRE}} U_{\mathsf{RE}}^{(b)\dagger})}_{\rho_{\mathsf{CR}}^{(b)}} \right)$$

$$= \mathop{\mathbb{E}}_{\mathcal{S}\subseteq[p]} \left[\mathrm{Tr}\left(\bigotimes_{i\in\mathcal{S}} |\psi_b\rangle\langle\psi_b|_{\mathsf{C}_i\mathsf{R}_i} \otimes \bigotimes_{i\notin\mathcal{S}} I_{\mathsf{C}_i\mathsf{R}_i} \cdot \rho_{\mathsf{CR}}^{(b)} \right) \right]$$

$$= \mathop{\mathbb{E}}_{\mathcal{S}\subseteq[p]} \left[\underbrace{F\left(\bigotimes_{i\in\mathcal{S}} |\psi_b\rangle\langle\psi_b|_{\mathsf{C}_i\mathsf{R}_i}, \mathrm{Tr}_{\mathsf{C}_i\mathsf{R}_i : i\notin\mathcal{S}}(\rho_{\mathsf{CR}}^{(b)}) \right)}_{p_{b,\mathcal{S}}} \right],$$

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

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

where the first inequality follows from the fact that taking a partial trace won't decrease the fidelity; the second inequality is because $\mathrm{Tr}_{\mathsf{R}}(\rho_{\mathsf{CR}}^{(0)}) = \mathrm{Tr}_{\mathsf{R}}(\rho_{\mathsf{CR}}^{(1)})$ and $F(\rho,\xi) + F(\sigma,\xi) \le 1 + \sqrt{F(\rho,\sigma)}$ [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 (3).
Finally, we bound the probability $p_0 + p_1$ as follows:

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

□

Acknowledgements

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

References

[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 p. 2).

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. "Cryptography from Pseudorandom Quantum States." In: *CRYPTO*. 2022 (cit. on p. 2).

[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. 2).

[BCQ22] Zvika Brakerski, Ran Canetti, and Luowen Qian. "On the computational hardness needed for quantum cryptography". In: *arXiv preprint arXiv:2209.04101* (2022) (cit. on p. 2).

[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. 2).

[BFV19] Adam Bouland, Bill Fefferman, and Umesh Vazirani. "Computational pseudorandomness, the wormhole growth paradox, and constraints on the AdS/CFT duality". In: *arXiv preprint arXiv:1910.14646* (2019) (cit. on p. 3).

[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. 2).

[Bra23] Zvika Brakerski. "Black-Hole Radiation Decoding Is Quantum Cryptography". In: *Annual International Cryptology Conference*. Springer. 2023, pp. 37–65 (cit. on p. 2).

[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 p. 2).

[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. 2, 3).

[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. 2).

[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 p. 2).

[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. 2).

[CM21] Lijie Chen and Ramis Movassagh. "Quantum merkle trees". In: *arXiv preprint arXiv:2112.14317* (2021) (cit. on p. 3).

[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. 3, 10, 17).

[GB23] Tudor Giurgica-Tiron and Adam Bouland. "Pseudorandomness from subset states". In: *arXiv preprint arXiv:2312.09206* (2023) (cit. on p. 2).

[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. 2).

[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. 2).

[Har13] Aram W Harrow. "The church of the symmetric subspace". In: *arXiv preprint arXiv:1308.6595* (2013) (cit. on p. 6).

[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 p. 2).

[JMW23] Fernando Granha Jeronimo, Nir Magrafta, and Pei Wu. "Subset States and Pseudorandom States". In: *arXiv preprint arXiv:2312.15285* (2023) (cit. on p. 2).

[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. 2).

[May97] Dominic Mayers. "Unconditionally secure quantum bit commitment is impossible". In: *Physical review letters* 78.17 (1997), p. 3414 (cit. on p. 2).

[MNY23] Tomoyuki Morimae, Barak Nehoran, and Takashi Yamakawa. *Unconditionally Secure Commitments with Quantum Auxiliary Inputs*. 2023. arXiv: 2311.18566 [quant-ph] (cit. on pp. 2, 4).

[MY21] Tomoyuki Morimae and Takashi Yamakawa. *Quantum commitments and signatures without one-way functions*. 2021. DOI: 10.48550/ARXIV.2112.06369 (cit. on pp. 2, 12).

[MY23] Tomoyuki Morimae and Takashi Yamakawa. *One-Wayness in Quantum Cryptography*. 2023. arXiv: 2210.03394 [quant-ph] (cit. on p. 2).

[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. 3).

[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. 14).

[Qia23] Luowen Qian. "Unconditionally secure quantum commitments with preprocessing". In: *Cryptology ePrint Archive* (2023) (cit. on p. 2).

[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 p. 12).

A Alternative proof of Lemma 3.5

Proof sketch of Lemma 3.5. 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

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

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):

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

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

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

Then we use the submultiplicativity of the operator norm to obtain

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

Hence, it holds that

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

□