Certified Randomness from Quantum Supremacy

Scott Aaronson[*]   Shih-Han Hung[†]

Abstract

We propose an application for near-term quantum devices: namely, generating cryptographically certified random bits, to use (for example) in proof-of-stake cryptocurrencies. Our protocol repurposes the existing "quantum supremacy" experiments, based on random circuit sampling, that Google and USTC have successfully carried out starting in 2019. We show that, whenever the outputs of these experiments pass the now-standard Linear Cross-Entropy Benchmark (LXEB), under plausible hardness assumptions they necessarily contain $\Omega(n)$ min-entropy, where n is the number of qubits. To achieve a net gain in randomness, we use a small random seed to produce pseudorandom challenge circuits. In response to the challenge circuits, the quantum computer generates output strings that, after verification, can then be fed into a randomness extractor to produce certified nearly-uniform bits—thereby "bootstrapping" from pseudorandomness to genuine randomness. We prove our protocol sound in two senses: (i) under a hardness assumption called Long List Quantum Supremacy Verification, which we justify in the random oracle model, and (ii) unconditionally in the random oracle model against an eavesdropper who could share arbitrary entanglement with the device. (Note that our protocol's output is unpredictable even to *a computationally unbounded adversary who can see the random oracle.*) Currently, the central drawback of our protocol is the exponential cost of verification, which in practice will limit its implementation to at most $n \sim 60$ qubits, a regime where attacks are expensive but not impossible. Modulo that drawback, our protocol appears to be the *only* practical application of quantum computing that both requires a QC and is physically realizable today.

Contents

1   Introduction

After three decades of quantum computing theory and experiment, the world finally has noisy quantum devices, with $50 - 60$ qubits or ~ 100 photons, that solve special sampling problems in a way that's conjectured to outperform any existing classical computer. The devices include Google's 53-qubit "Sycamore" chip [12], USTC's "Jiuzhang" [65] and "Zu Chongzhi" [62], and most recently Xanadu's "Borealis" [40]. The sampling problems, which include Random Circuit Sampling [7] and BosonSampling [4], grew directly out of work in quantum complexity theory beginning around 2010.

To be clear, it's still debated in which senses current devices have achieved the milestone of "quantum supremacy"—a term coined by Preskill [51] in 2012, to refer to an orders-of-magnitude speedup over all known classical approaches for some well-defined (but not necessarily useful) computational task. On the one hand, since Google's original 2019 announcement [12], the sampling experiments have continued to improve, for example in number of qubits and circuit depth (for RCS) [62], and in number of photons and measurement fidelity (for BosonSampling) [40]. One expects further improvements. On the other hand, classical spoofing attacks against the experiments have *also* improved—with some attacks based on tensor-network contraction (e.g., [49]), and others taking advantage of noise in the devices (e.g., [13]). Notably, however, the attacks that fully replicate the Google device's observed performance, such as that of [49], still have inherently exponential scaling, and still seem to require an ExaFLOPS supercomputer to match or beat the Google device's running time of ~ 3 minutes. As a rough estimate, the Summit supercomputer uses 13 megawatts, while Google [12, Appendix H] estimated that the dilution refrigerator for its 53-qubit QC uses ~ 20 kilowatts. Thus, *despite* the QC's extreme need for refrigeration, it still wins by a factor of hundreds as measured by electricity cost.

For some, the recent quantum supremacy demonstrations were important mostly because they showcased many of the key ingredients of a future *fault-tolerant, scalable* quantum computer—and just as importantly, did not detect any correlated errors of the sort that would render fault-tolerant quantum computing impossible. For others, however, these experiments have done more: namely, they've inaugurated the era of "NISQ" or Noisy Intermediate Scale Quantum computation, another term coined by Preskill [52]. The hope of NISQ is that, even *before* fault-tolerance is achieved, noisy QCs with up to (say) 1000 qubits might already prove useful for certain practical problems, just like various analog computing devices were useful even before the invention of the transistor inaugurated the digital era.

Unfortunately, despite the billions that have by now been invested into NISQ hopes, the lack of any obvious "killer app" for NISQ devices has emerged as a defining fact of the field.

Perhaps NISQ devices will be useful for simulation of condensed-matter physics or even quantum chemistry. Alas, while there are exciting proposals for quantum simulations that would need only a few hundred qubits (e.g., [56]), these proposals invariably have the drawback of requiring thousands or millions of layers of gates. Unless it can be remedied, this would put them completely out of reach for NISQ devices. Or perhaps NISQ devices will yield speedups for optimization problems, via quantum annealing or QAOA [29]. Alas, despite years of intense theoretical and empirical work, researchers have struggled to show any clear advantage for quantum annealing or QAOA over classical computing, for any practical optimization problem—*let alone* an advantage that would be achievable on a NISQ device.

We should add that, in recent years, there have been striking *new* ideas for how to demonstrate quantum supremacy. These include interactive protocols that exploit trapdoor one-way functions [20, 35], as well as the spectacular result of Yamakawa and Zhandry [63], which gave an exponential quantum speedup for an NP search problem relative to a random oracle. Alas, pending some

breakthrough, none of these ideas seem to be implementable on a NISQ device.

1.1 Our Contribution

This paper studies, to our knowledge for the first time, whether current sampling-based supremacy experiments might *themselves* have a useful application outside of physics.[1] We focus on the generation of *cryptographically certified random bits*.

Needless to say, it is easy to use a quantum computer—or for that matter, even a Geiger counter next to some radioactive material—to generate as many random bits as we like: bits that quantum mechanics itself predicts will be fundamentally unpredictable. The problem is, how do we convince a skeptic over the Internet, with no access to our hardware, that the bits were indeed random, and not secretly backdoored? This is not just a theoretical worry: for example, as a byproduct of the Edward Snowden revelations in 2013, the world learned that a NIST pseudorandomness standard known as Dual_EC_DRBG was indeed backdoored by the US National Security Agency.[2]

Certified randomness has become a significant practical problem—particularly with the rise of *proof-of-stake cryptocurrencies*, which notably include Ethereum[3] (market cap at time of writing: $163 billion), following its migration on September 15, 2022. In proof-of-stake systems, lotteries are continually run to decide which currency holder gets to add the next block to the blockchain. There is no trusted authority to manage these lotteries, yet the entire system rests on the assumption that they are conducted honestly and without bias. Other applications of certified randomness include non-interactive zero-knowledge proofs, and financial and electoral audits.

One approach to the certified-randomness problem uses blockchains themselves as a source of random bits—with the argument being that anyone who could predict the bits could exploit their predictability to get rich [19]. Other approaches look to the social or natural worlds for a source of publicly verifiable entropy: for example, perhaps one could use the least significant digits of the Dow Jones Industrial Average, or the patterns of granules that form on the surface of the Sun.

More relevant for us, since 2009, an exciting line of work has shown how to use measurements on entangled particles as a source of physically certified randomness [24, 50, 60, 25, 46, 47]. The idea is that, if the measurement outcomes are observed to violate the Bell/CHSH inequality, then by that very fact, the outcomes *cannot* have been secretly deterministic, unless there was secret communication between the "Alice" and "Bob" detectors. Furthermore, depending on the experimental setup, this communication might need to have occurred faster than light. Thus, the outcomes must contain genuine entropy, which can be fed into a randomness extractor to purify it into nearly-uniform random bits. The technical part is that, in a Bell/CHSH experiment, the measurement bases must *themselves* be unpredictable—and thus, they need to be chosen judiciously if we want an overall net gain in randomness. This is the problem that the line of works [24, 50, 60, 25, 46, 47] has now almost completely solved.

Bell/CHSH-based certified randomness protocols have already been experimentally demonstrated [18], and are even in consideration for practical deployment in the NIST Randomness Beacon [36], which generates 512 random bits per minute.

The central drawback of these protocols is that a user, downloading allegedly random bits from the Internet, has no obvious way to verify that the "Alice" and "Bob" detectors were out of communication—the key assumption needed for security. Indeed, in some Bell/CHSH experiments,

---

[1]Some earlier work explored whether BosonSampling might be useful for (e.g.) calculating molecular vibronic spectra [34] or graph similarity detection [57], but those hopes were killed by efficient classical simulations.

[2]https://en.wikipedia.org/wiki/Dual_EC_DRBG

[3]https://en.wikipedia.org/wiki/Ethereum

"Alice" and "Bob" are mere feet away! But even if they weren't, how would this be proved?

The central insight of this paper is that sampling-based quantum supremacy experiments provide an entirely different route to certified randomness—a route that requires only a single quantum device, while also being practical today. In our protocol, a classical verifier uses a small random seed to generate n-qubit challenge circuits $C_1, C_2, \ldots$ pseudorandomly. The verifier then submits these C_i's one at a time, presumably over the standard Internet, to a quantum computer server. For each C_i, the server needs to respond quickly—say, in less than one second—with independent samples $s_1, \ldots, s_k$ from C_i's output distribution: that is, the distribution over $\{0,1\}^n$ obtained by running C_i on the initial state $|0^n\rangle$ and then measuring in the computational basis.

The verifier, at its leisure, can then calculate the so-called *Linear Cross-Entropy Benchmark*,

$$\text{LXEB} := \sum_{j=1}^{k} |\langle s_j|C_i|0^n\rangle|^2,$$

for at least some of the challenge circuits C_i. *If* the LXEB scores are sufficiently large, our analysis shows that the verifier can then be confident, under plausible computational assumptions, that there must be $\Omega(n)$ bits of genuine min-entropy in the returned samples.

In other words: even a quantum computer should need $\exp(n)$ time to generate samples that pass the LXEB test and yet are secretly deterministic or nearly-deterministic functions of C_i. For a typical circuit C_i, an honest sample from the output distribution will contain $n - O(\log n)$ bits of min-entropy. A dishonest quantum computer could *somewhat* reduce the entropy of the returned samples—for example, by generating many samples and then returning only those that start with 0 bits. But doing better, by finding (e.g.) the lexicographically first samples that pass the LXEB test, or the samples that maximize the LXEB score, should be exponentially hard even quantumly, requiring amplitude amplification or the like (while a subexponential classical algorithm wouldn't stand a chance). The purpose of our security reductions, which we will explain in detail in Section 2, is just to formalize these simple intuitions.

Assuming the returned samples (or enough of them) pass the LXEB test, the last step of our protocol is to feed them into a classical *seeded randomness extractor*, to produce output bits that are exponentially close in total variation distance to uniformly random.

Stepping back, many people have pointed out the close analogy between

1. the Bell/CHSH experiments, which ruled out local hidden-variable theories (and which have now been recognized with the Nobel Prize in Physics), and

2. sampling-based quantum supremacy experiments, which seek to rule out "classical polynomial-time hidden-variable theories."

This paper shows that the analogy goes even further. In both cases, the original purpose of the experiment was just to demonstrate the reality of some quantum phenomenon, and rule out any classical explanation—but we then get certified randomness as a "free byproduct" of the demonstration. In both cases, the entire setup hinges on a numerical inequality—one that any classical explanation must satisfy, that quantum mechanics predicts can be violated by a large amount, and that realistic experiments can violate albeit by less than the maximum that quantum mechanics predicts. In both cases, *any* violation of the inequality turns out to suffice for the certified randomness application.

We note, lastly, that our protocol *inherently requires* the use of a quantum computer. This can be seen as follows: consider any server that's simulable in classical probabilistic polynomial-time. Then by definition, there can be no efficient way to distinguish that server from a simulation

6

whose randomness has been replaced by the output of a pseudorandom generator. Indeed, if the pseudorandom generator has an m-bit seed, then the best distinguishing algorithm would be expected to take $\exp(m)$ time—which means that even given the $\sim 2^n$ time that we allow for verification, the verifier *still* cannot distinguish an honest server from one with only m bits of true entropy, for any $m \gg n$.

How does our actual quantum protocol evade the above impossibility argument? Simply by a fact used again and again in quantum complexity theory: namely, that there is no notion of "pulling the randomness" (or quantumness) out of a quantum algorithm, for example to replace it with pseudorandomness, analogous to what is possible with classical randomized algorithms. One could also say: our protocol's security analysis will depend on a computational assumption, that the problem of "Long List Quantum Supremacy Verification" is hard for the complexity class QCAM, whose classical analogue is simply false. The reasons for this, in turn, are closely related to one of the elemental differences between classical and quantum computation, that PostBPP (BPP with postselected outputs) is contained in the polynomial hierarchy and can be simulated using approximate counting, whereas PostBQP = PP can express #P-complete problems.

1.2 Practical Considerations

Our certified randomness protocol could be demonstrated on existing devices, with $n = 60$ qubits or some other number in the "quantum supremacy regime." However, there are practical and even conceptual issues to be sorted out before deploying the protocol for proof-of-stake cryptocurrency or any other critical application.

Verification cost. The central drawback of our protocol, as it stands, is that to check the server's outputs, the classical verifier needs to calculate a Linear Cross-Entropy score, and this is expected to take $\sim 2^n$ time—similar to the time needed for classical spoofing. This drawback is directly inherited from Random Circuit Sampling and all other current approaches to NISQ quantum supremacy itself.

Because of the verification cost, n, the number of qubits, must be chosen small enough that 2^n is still within range of the most powerful classical supercomputers available. If so, however, the issue is obvious: 2^n would *also* be within range of a sufficiently dedicated classical spoofer, who could then predict and control the allegedly random bits.

Nevertheless, we claim that not all hope is lost. The crucial observation is that spoofing, to be effective, needs to be *continual*: for example, if the challenge circuits are submitted every second, then the spoofer needs to run nearly every second as well. Even if a real quantum computer were used (say) every *other* second, the outputs would contain a lot of genuine min-entropy, which would suffice for a secure protocol. The spoofing also needs to be *fast*—as fast as the QC itself.

One might object that, since most classical algorithms to simulate quantum circuits are highly parallelizable, spoofing our protocol within some exacting time limit is "merely" a matter of spending enough money on classical computing hardware. When (say) $n = 60$, though, we estimate that the expenditure, to do $\exp(60)$ operations per second, would run into billions of dollars, outside the means of all but corporations and nation-states.

Verification, by contrast, only needs to be *occasional*. Using a tiny amount of seed randomness, the verifier can choose $O(1)$ random rounds of the protocol and spot-check only those. Then a malicious server that spoofed even (say) 10% of the rounds would be caught with overwhelming probability. Verification can also be done *at leisure*: so long as the verifier is satisfied to catch the spoofer after the fact, the verifier could spend hours or days where the spoofer needed to take less than a second. Indeed, to keep the server honest, arguably the verification need not even be done:

it's enough to threaten credibly that it *might* be done!

Having said that, of course it would be preferable if the verification could be done in $n^{O(1)}$ time, in some way that retained the protocol's "NISQiness."

In our view, whether it's possible to achieve sampling-based quantum supremacy, *on a NISQ device and with efficient classical verification*, has become one of the most urgent open problems in quantum computing theory, even independently of this work. Our work further underscores the problem's importance, by showing how a solution could turn secure, practical certified randomness into the first real application of quantum computers.

Interactivity. A second practical issue with our protocol is the need for the verifier continually to generate new challenge circuits that are unpredictable to the quantum computing server. One could reasonably ask: if the verifier has that ability, then why does it even *need* the quantum computer to generate random bits?

The short answer is that our protocol offers an "upgrade" in the level of unpredictability: the challenge circuits only need to be *pseudorandom* (for reasons to be explained later, against a QSZK adversary). So in particular, the verifier can generate all the circuits deterministically from a single initial random seed. The protocol's output, by contrast, is guaranteed to be *genuinely* random.

Indeed, our protocol offers an appealing "forward secrecy" property. Namely, even if we imagine that the verifier's pseudorandom generator will be broken in the future, so long as the server can't break the PRG *at the time the protocol is run*, the server is forced to generate truly random bits. Such bits will of course remain unpredictable, conditioned on anything that doesn't depend on themselves, regardless of any future advances in cryptanalysis.

Who verifies the verifier? Still, there remains a difficulty: the verifier checks the QC's outputs, but who checks the verifier? If the verifier just wants random bits for its own private use, then there is no problem: the verifier could use our protocol, for example, to check random bits output by a QC that was bought from an untrusted manufacturer. But consider an application like proof-of-stake cryptocurrency, where the certified random bits need to be shared with the world. Does the world designate some organization to play the role of the verifier? If so, then why couldn't that organization be corrupted or infiltrated, as surely as the organization that owns the quantum computer—bringing us back where we started?

Classical cryptography suggests a variety of potential solutions to this dilemma. For example, perhaps a dozen or more classical verifiers each generate their own pseudorandom sequences, and those sequences are then XORed together to produce a single sequence which is used to generate the challenge circuits to send to the quantum computing server. If even one verifier wants the sequence to be unpredictable to the server, then it will be, provided that no verifier can see any other verifier's sequence before committing to its own.

Again one could ask: if we trust such a XOR protocol, then why not just use its outputs directly, and skip the quantum computer? Again our answer appeals to the "randomness bootstrap": provided we agree that the XOR'ed sequence is unpredictable *in practice, for now*, the quantum computer's output will then be *fundamentally* unpredictable. Our protocol thus provides an upgrade in the level of unpredictability.

1.3 Related Work

We are not the first to propose using a quantum computer to generate certified random bits, which are secure under some computational hardness assumption. Brakerski, Christiano, Mahadev, Vazirani, and Vidick [20] gave an elegant scheme based on the assumed hardness of the Learning With Errors

(LWE) problem. In subsequent work, Mahadev, Vazirani, and Vidick [41] showed that the Brakerski et al. protocol generates $\Omega(n)$ random bits per round, which matches our protocol.

The central advantage of the Brakerski et al. protocol over ours is that its outputs can be verified in classical polynomial time. On the other hand, unlike ours, their protocol seems difficult or impossible to implement on a NISQ device, because it requires evaluating complicated cryptographic functions on superpositions of inputs. In addition, their protocol requires the quantum computer to maintain a coherent superposition state *while it interacts with the verifier*, presumably over the Internet. This is currently feasible only with certain hardware platforms, such as trapped ions, and not for example with superconducting qubits (whose coherence times are measured in microseconds).

More recently, as a byproduct of their breakthrough on an exponential quantum speedup for NP search relative to a random oracle, Yamakawa and Zhandry [63] gave a different interactive protocol to certify $\Omega(\log n)$ random bits, in the random oracle model and also assuming the so-called *Aaronson-Ambainis conjecture* [3]. We do not know whether the Yamakawa-Zhandry protocol remains secure against an entangling adversary, nor whether it accumulates entropy across multiple rounds. In any case, theirs is again a protocol that evaluates complicated functions on superpositions of inputs, meaning there is little or no hope of running it on a NISQ device.

In contrast to these earlier works, here we pursue the "minimalist approach" to generating certified randomness using a quantum computer: we eschew all cryptography done in superposition, and just examine the output distributions of random or pseudorandom quantum circuits. By taking this route, we give up on efficient verification, but we gain feasibility on current hardware, as well as a conceptual unification of certified randomness with sampling-based quantum supremacy itself.

Recently, building on the unpublished announcements by one of us (SA) of the research now reported in this paper, Bassirian, Bouland, Fefferman, Gunn, and Tal [14] took some first steps toward analyzing the use of sampling-based quantum supremacy experiments for certified randomness. Their first result says that, relative to a random oracle, any efficient quantum algorithm for Fourier Sampling must generate $\Omega(n)$ bits of min-entropy as a byproduct of its operation. Their second result says that Long List Quantum Supremacy Verification (LLQSV), the problem that underlies our hardness reduction, is neither in BQP nor in PH relative to a random oracle. To prove non-containment in PH, they build on the breakthrough oracle separation between BQP and PH due to Raz and Tal [55].

These results are of course closely related to ours, but they fall short of a soundness analysis for our certified randomness protocol. We go further than [14] in at least four respects:

1. We prove that a plausible hardness assumption about LLQSV implies the generation of certified random bits. This reduction does not depend on a random oracle.

2. We give black-box evidence for that hardness assumption. (The result of [14], that black-box LLQSV is not in PH, is interesting and new, but neither necessary nor sufficient for us. As we'll explain, we need non-containment in the class QCAM/qpoly.)

3. We prove the accumulation of entropy across multiple rounds.

4. In the black-box setting, we prove security against an entangled adversary.

Our proof techniques are also independent of those in [14].

Lastly, let us mention that Brandão and Peralta [22] have already reported numerical calculations to find appropriate parameter settings for the protocol described in this paper.

1.4 This Paper's History

One of us (SA) conceived the certified randomness protocol, as well as basic elements of its soundness analysis (e.g., the LLQSV $\notin$ QCAM/qpoly hardness assumption), in February 2018. SA then gave various public talks about the proposal (e.g., [2]), albeit only sketching the analysis. Those talks influenced subsequent work on quantum supremacy: for example, the Google group cited them as motivation in its 2019 paper announcing its 53-qubit Sycamore experiment [12].

Alas, the soundness analysis ended up being too involved for SA to complete alone. That and other factors caused a more than four-year delay in writing up this paper. Here, we not only complete the analysis that SA announced in 2018: we also prove security, in the random oracle model, *against an adversary who could be arbitrarily entangled with the QC*. This goes beyond what SA claimed in 2018, and indeed addresses one of the central open problems raised at that time.

1.5 Future Directions

Many important problems remain:

- As mentioned before, perhaps the biggest problem is to design a sampling-based quantum supremacy experiment that both runs on a NISQ device *and* admits efficient classical verification. If such an experiment were developed, then based on our results here, we predict that it could be readily repurposed to get a secure, efficiently-verifiable certified randomness scheme that runs on existing devices.

- Short of that, it would also be interesting to adapt our randomness protocol from Random Circuit Sampling (RCS) to other known quantum supremacy proposals, such as BosonSampling [4] and IQP [23]. With BosonSampling, the problem is that we currently lack a crisp, quantitative conjecture about the best that a polynomial-time classical algorithm can do to spoof tests such as the Linear Cross-Entropy Benchmark (LXEB). From 2013 work of Aaronson and Arkhipov [5], we know that, in contrast to what we conjecture for RCS, efficient classical algorithms can get *some* depth-independent, $\Omega(1)$ LXEB advantage for BosonSampling, but how much? Answering this question seems like a prerequisite to designing a certified randomness protocol, as it would set the lower bound on how well a BosonSampling experiment has to do before it can be used for such a protocol.

- Of course, it would be great to know more about the truth or falsehood of the central hardness conjectures on which we base our protocol's security—e.g., that "Long List Quantum Supremacy Verification" (LLQSV) lacks a QCAM/qpoly protocol. It would be also great to prove our protocol's security under weaker assumptions. Can we at least remove the exponentially long list of circuits, and use a hardness assumption involving a single circuit?

- In the setting with an entangled adversary, we can currently prove security *only* in the random oracle model. Can we state a plausible hardness assumption that suffices for that setting?

- Under some plausible hardness assumption, can we tighten the lower bound on the amount of min-entropy generated per sample—even up to the maximum of $n - O(\log n)$?[4]

- Likewise, can we show that more and more min-entropy continues to be generated, even if we sample with the same circuit C over and over? Clearly there is a limit here: once enough time

---

[4]$n - O(\log n)$ is the maximum because the quantum computer could always (say) generate $n^{O(1)}$ samples from the correct distribution until it finds one whose first $O(\log n)$ bits are all 0's.

has elapsed that a spoofer could have explicitly calculated C's entire output distribution, and perhaps even stored it in a giant lookup table, C is no longer secure and needs to be replaced by a new circuit. But can we at least go up to that limit? To whatever extent we can, our protocol would become much more efficient in practice—especially once we factor in (e.g.) the time needed to calibrate a superconducting QC on a new circuit C.

- We know, both from the Haar-random approximation and from extensive numerical evidence, that an ideal, honest QC *does* succeed at the Linear Cross-Entropy Benchmark with overwhelming probability, given a random quantum circuit C as input. And in some sense, since this fact is never needed in our security analysis, empirical evidence suffices for it! All the same, it is strange that a rigorous proof of the fact is still lacking, at least for "natural" quantum circuit ensembles. In Section 3.4.2, we prove the fact in the random oracle model, but can we prove it outright? Recent advances showing that random quantum circuits yield t-designs [21, 33] take us part of the way, but an additional idea seems needed.

2   Technical Overview

2.1   Our Basic Result (without entangled adversary)

Throughout this paper, we let C be a quantum circuit acting on n qubits, and we let $N = 2^n$ be the Hilbert space dimension. Let P_C be the probability distribution defined by $p_C(z) = |\langle z|C|0^n\rangle|^2$. It is well-known that when $C \sim \mathrm{Haar}(N)$, the Haar measure over $N \times N$ unitary matrices, we have

$$\mathop{\mathbb{E}}_{C} \mathop{\mathbb{E}}_{z \sim P_C} [p_C(z)] = \frac{2}{N+1}. \tag{1}$$

In 2019, Google [12] announced an experiment to show quantum advantage on the following task, called Linear Cross-Entropy Benchmarking (LXEB).

Problem 1 (Linear Cross-Entropy Benchmarking $\mathrm{LXEB}_{b,k}(\mathcal{D})$)**.** *Let $\mathcal{D}$ be a probability distribution over quantum circuits on n qubits. Then the $\mathrm{LXEB}_{b,k}(\mathcal{D})$ problem is as follows: given C drawn from $\mathcal{D}$, output samples $z_1, \ldots, z_k \in \{0,1\}^n$ such that*

$$\frac{1}{k}\sum_{i=1}^{k} p_C(z_i) \geq \frac{b}{N}. \tag{2}$$

We sometimes omit the argument $\mathcal{D}$.

Intuitively, we expect that a polynomial-time classical algorithm should be unable to solve $\mathrm{LXEB}_{b,k}$ for any $b = 1 + \Omega(1)$. By contrast, if an ideal quantum computer simply runs C over and over on the initial state $|0^n\rangle$, measures in the computational basis, and returns the results, then approximating C by a random unitary, by (1) we expect the QC to solve $\mathrm{LXEB}_{b,k}$ with $1 - 1/\exp(k)$ success probability for any constant $b < 2$. Meanwhile, a noisy QC could be expected to solve $\mathrm{LXEB}_{b,k}$ for some b greater than 1 but less than 2—and indeed that's exactly what's observed empirically, with (for example) Google's 2019 experiment achieving $b \sim 1.002$.

In this paper, our aim is to show, not merely a quantum advantage over classical in solving $\mathrm{LXEB}_{b,k}$, but a quantum sampling advantage over *any efficient algorithm—quantum or classical— that returns the same s_i's a large fraction of the time when given the same circuit C.*

To do this, we'll use a new and admittedly nonstandard hardness assumption, but one that strikes us as extremely plausible. Our assumption concerns the following problem:

Problem 2 (Long List Quantum Supremacy Verification LLQSV($\mathcal{U}$)). *We are given oracle access to $M = O(2^{3n})$ quantum circuits $C_1, \ldots, C_M$, each on n qubits, which are promised to be drawn independently from the distribution $\mathcal{U}$. We're also given oracle access to M strings $s_1, \ldots, s_M \in \{0,1\}^n$. Then the task is to distinguish the following two cases:*

1. **No-Case**: *Each s_i is sampled uniformly and uniformly from $\{0,1\}^n$.*

2. **Yes-Case**: *Each s_i is sampled from p_{C_i}, the output distribution of C_i.*

Our hardness assumption, which we call the Long List Hardness Assumption (LLHA$_B(\mathcal{U})$), now says the following, for some parameter $B < n$:

$$\text{LLQSV}(\mathcal{U}) \notin \text{QCAMTIME}(2^B)/\text{q}(2^B n^{O(1)}). \tag{3}$$

Here QCAM, or Quantum Classical Arthur Merlin, is the class of problems that admit an AM protocols with classical communication and a quantum verifier. QCAMTIME(T) is the generalization of QCAM where the verifier can use running time T (the communication is still restricted to be polynomial). QCAMTIME(T)/q(A) is the same, but where the verifier now receives A bits of quantum advice that depend only on n.

Our first main result is then the following.

Theorem 2.1 (Single-round analysis, no side information, informal). *Let $\mathcal{U}$ be a distribution over n-qubit quantum circuits, and suppose LLHA$_B(\mathcal{U})$ holds. Also, let $\mathcal{A}$ be a polynomial-time quantum algorithm that solves LXEB$_{b,k}(\mathcal{U})$ with probability at least q. Then $\mathcal{A}$'s output, $s_1, \ldots, s_k$, satisfies*

$$\Pr_{C' \sim \mathcal{U}} \left[H_{\min}(s_1 \ldots s_k | C = C') \geq B/2 \right] \geq \left(\frac{bq - 1}{b - 1} - o(1) \right), \tag{4}$$

where $H_{\min}(\{p_i\}) := \min_i \log_2 \frac{1}{p_i}$ is the min-entropy.

To illustrate, suppose we set $B := 0.49n$—the best *upper* bound that we know, $B < n/2$, follows from Grover's algorithm. Suppose also that $b = 1.002$, as in Google's experiment [12], and that k is chosen large enough so that $q \geq 0.9990$ by a large deviation inequality. Then Theorem 2.1 is telling us that $\mathcal{A}$'s output must contain at least $(0.12 - o(1))n$ random bits.

Interestingly, while Theorem 2.1 is stated in terms of min-entropy, and while our eventual multi-round result will *also* be stated in terms of min-entropy, as an intermediate step it's convenient to switch to Shannon entropy, as this is what entropy accumulation theorems use. Of course, since $H_{\min}(\mathcal{D}) \leq H(\mathcal{D})$ for every distribution $\mathcal{D}$, Theorem 2.1 immediately implies the same lower bound on Shannon entropy. Indeed, since Shannon entropy behaves linearly with respect to expectation, Theorem 2.1 implies that

$$H(s_1, \ldots, s_k | C) \geq \frac{B}{2} \cdot \left(\frac{bq - 1}{b - 1} - o(1) \right). \tag{5}$$

While LLHA$_B(\mathcal{U})$ is admittedly a strong assumption, our next result justifies it by proving that it holds in the random oracle model:

Theorem 2.2 (Hardness of LLQSV($\mathcal{U}$), informal). *Given a random oracle $\mathcal{O}$, let $\mathcal{U}$ be the uniform distribution over $M = 2^{O(n)}$ quantum circuits $C_1, \ldots, C_M$, which Fourier-sample disjoint Boolean functions $f_1, \ldots, f_M : \{0,1\}^n \to \{-1, +1\}$ respectively defined by A. Then LLHA$_B(\mathcal{U})$ holds relative to $\mathcal{O}$ for $B = \Omega(n)$.*

Here we outline the proof. First we give a reduction for LLQSV from another problem called Boolean Function Bias Detection (BFBD). In the latter problem, the algorithm is given access to M functions sampled from either a distribution $\mathcal{D}$ or the uniform distribution. The distribution $\mathcal{D}$ can be described with the following process: First sample a integer $r \in \{0, 1, \ldots, N\}$ with probability $N(1 - 2r/N)^2 \cdot \binom{N}{r} 2^{-N}$, sample a random subset $R \subseteq \{0,1\}^n$ of size r, and finally set $f(x) = -1$ if and only if $x \in R$. Since both distributions are concentrated around $r = N/2$, a simple hybrid argument leads to a basic lower bound for BQP. We then extend the hardness result to interactive proof systems, specifically, the class QIP[2] of two-message quantum interactive proofs, using a similar argument: Recall that the prover's goal is always to convince the verifier that the given function is sampled from $\mathcal{D}$. From the observation stated above, we can modify a function $f \sim \mathcal{D}$ on a small number of points to yield a random function. Thus a prover which convinces the verifier to accept $f \sim \mathcal{D}$ would also convince the verifier to accept a random function. Then by the inclusion QCAM $\subseteq$ QIP[2], LLQSV is hard for QCAM.

To prove the desired hardness for the non-uniform class QCAM/qpoly (or generalizations of it to use more queries and more advice), we observe that by Aaronson and Drucker's exchange theorem [8], QCAM/qpoly $\subseteq$ QMA/poly, so it suffices to show hardness against the latter class. We then change the oracle model (and not the problem itself) as follows: The oracle $\mathcal{O}$ contains N sections, each indexed by an n-bit string x. The non-uniform protocol given oracle access to $\mathcal{O}$, input x, and all the samples (also indexed by x), is challenged to determine whether the sample s_x is sampled from $\mathcal{O}_x$ or uniform (see Problem 2).

Clearly any solver for LLQSV can determine whether s_x is sampled from $\mathcal{O}_x$ for every $x \in \{0,1\}^n$. By replacing the classical advice with a random guess, we show that any QMA/poly verifier solving the problem would imply a $N n^{O(1)}$-query QMA verifier solving N problems with probability $2^{-\operatorname{poly}(n)}$. Then we appeal to the *strong direct product theorem* by Sherstov [58], who showed that even to achieve success probability $2^{-\Omega(N)}$, computing N independent problems requires $\Omega(Nd)$ queries, where d is the query lower bound of a single problem obtained using the polynomial method. Finally we derive a contradiction by showing that a single problem has an exponential lower bound.

Building upon the above single-round analysis, the next step is to showk *accumulation* of entropy across multiple rounds. We give a simple m-round entropy accumulation process using $\mathrm{LXEB}_{1+\delta,k}$ as the verification for $m = n^{O(1)}$[5] and constant $0 < \delta < 1$. In each round, for $\gamma = O(\log n/m)$, the verifier sends the same circuit as in the previous round with probability $1 - \gamma$, or samples a fresh random circuit with probability γ. We define an *epoch* to be an interval of consecutive rounds where the same circuit is sent.[6] With overwhelming probability, there are at most $O(\log n)$ epochs. The verifier chooses k random samples for each circuit, and checks if the verifier passes $\mathrm{LXEB}_{1+\delta,k}$ for 99% of the given circuits. Applying an Entropy Accumulation Theorem (EAT, explained in Section 2.4), we prove the following statement.

Theorem 2.3 (Entropy accumulation, no side information, informal). *For $\beta \in [0,1]$, if $\mathrm{LLHA}_{\beta n}$ holds, then for integer $k = \Omega(n^2)$ and $m = \Omega(\log n)$, there exists an m-round entropy accumulation protocol taking $k \cdot m$ samples such that conditioned on the event Ω of not aborting,*

$$H_{\min}(Z|C)_{\rho|\Omega} \geq n\left(\left(0.99 - \frac{0.01}{\delta} \right) \frac{\beta}{2} m - O(\sqrt{m}) \right) \tag{6}$$

for every device solving $\mathrm{LXEB}_{1+\delta,k}$, where ρ is the output state, Z is the responses received from the device, and C is the circuit in each round.

---

[5]Potentially m can be exponentially large, but we do not pursue this here.

[6]Brakerski, Christiano, Mahadev, Vazirani and Vidick [20] used the same concept of "epochs" to analyze their certified randomness protocol.

2.2 Entangled Adversary and Ideal Measurements

In the previous section, we assumed that an attacker, Eve, trying to predict the quantum computer's outputs had no preshared entanglement with the quantum computer. Now we relax that assumption.

To build intuition, we start with the special case where the quantum computer performs an ideal measurement—i.e., it "just" applies C to n qubits, followed by a measurement in the standard basis. The "only" problem is that the qubits might not start in the desired initial state $|0^n\rangle$, but rather in some arbitrary state entangled with Eve's qubits.

We define the following idealized score, called b-XHOG($\mathcal{U}$).

Problem 3 (b-XHOG($\mathcal{D}$) [39])**.** *For a distribution $\mathcal{D}$ over quantum circuits on n qubits, an algorithm $\mathcal{A}$ given access to $C \sim \mathcal{D}$ is said to solve b-XHOG if it outputs a sample z such that*

$$\mathbb{E}_{C \sim \mathcal{D}}\left[\mathbb{E}_{z \sim \mathcal{A}^C}[p_C(z)]\right] \geq \frac{b}{N}. \tag{7}$$

For an algorithm $\mathcal{A}$ which is given access to C and outputs z, we define the "XHOG score" of $\mathcal{A}$ to be the value $\mathbb{E}_C[\mathbb{E}_{z \sim \mathcal{A}^C}[p_C(z)]]$. This score was first considered by Kretschmer for showing a Tsirelson bound for random circuit sampling in the oracle model [39]. Recall that with the CHSH game, a violation of the classical bound $3/4$ implies certified randomness. Interestingly, our result may be interpreted as certified randomness from a violation of the classical XHOG score.

We will proceed with our analysis with b-XHOG first, and show a von Neumann entropy lower bound $\Omega(\delta n)$ when the device solves $(1 + \delta)$-XHOG. First, the problem itself is linear in the device's output distribution: that is, for two devices $\mathcal{A}$ with score $s_{\mathcal{A}}$ and $\mathcal{B}$ with score $s_{\mathcal{B}}$, a third device that runs $\mathcal{A}$ with probability p and $\mathcal{B}$ with probability $(1 - p)$ has score $p \cdot s_{\mathcal{A}} + (1 - p) \cdot s_{\mathcal{B}}$. The linearity condition coincides with the score calculation from violation of Bell's inequality.

More concretely, recall that to establish certified randomness from a violation of Bell's inequality, two devices $\mathcal{A}$ and $\mathcal{B}$ are asked to play, say, the CHSH game: the verifier sends two questions x, y to the devices and collecting the responses a, b. The verifier sets the score to 1 if $x \wedge y = a \oplus b$ and 0 otherwise, and the expectation of the score is defined as

$$\omega = \mathbb{E}_{x, y \sim \{0, 1\}}\left[\mathbb{E}_{a, b \sim \mathcal{A}^x \otimes \mathcal{B}^y(\rho)}[\mathbb{1}[x \wedge y = a \oplus b]]\right]. \tag{8}$$

It is well-known that the best achievable expectation is $\omega = \cos^2(\pi/8)$. For certified randomness, it was further shown that when the expectation $\omega \geq \cos^2(\pi/8 + \varepsilon)$, the output of $\mathcal{A}$ has von Neumann entropy lower-bounded by $1 - h(\sin 4\varepsilon) \approx 1 - O(\varepsilon)$, where $h(x) := -x \log x - (1 - x) \log(1 - x)$ is the binary entropy function [11]. Like the XHOG score, here the score ω can be exactly computed only by taking infinitely many samples from the same devices. With a finite number of samples, we can only approximate the score.

Proving a conditional min-entropy lower bound from sample statistics, in an m-round sequential process, amounts to the problem of entropy accumulation. An Entropy Accumulation Theorem (EAT) for certified randomness is usually stated as follows: In an m-round sequential process, the verifier randomly selects $O(\log m)$ rounds to get an approximation of the score. If the approximation is sufficiently close to $\cos^2(\pi/8)$, the number of extractable random bits is at least $\Omega(m)$ times the von Neumann entropy lower bound established in a single-round analysis.

Without loss of generality, let the entanglement shared between the device and Eve be a pure state $|\psi\rangle$. For every state ρ_{ZE} classical on Z, we show that the conditional von Neumann entropy $H(Z|CE)_\rho \geq H(Z|C)_\rho - \chi(Z : CE)_\rho$, where χ is the Holevo quantity. To see why they they

must use weak entanglement, we can write $|\psi\rangle := \sum_x \alpha_x |\psi_x\rangle |\phi_x\rangle$ for orthonormal bases $\{|\psi_x\rangle\}$ and $\{|\phi_x\rangle\}$ in the Schmidt decomposition. We show that the device solving b-XHOG for $b \geq 1 + \delta$, the amplitude α_x must concentrate at a single compoment, say x^*, such that $|\alpha_{x^*}|^2 \geq \delta$. By the observation that the Holevo quantity equals the entanglement entropy, we establish an upper bound $O((1-\delta)n)$ on the Holevo quantity.

In this simplified setting, we have already seen that if the device has a large XHOG score, then they must use weak entanglement to pass the verification. However, the entire analysis relies on the assumption that the device must perform the ideal measurement.

2.3 A Fully General Device

Next, we consider the setting in which the adversary may share arbitrary entanglement with Eve. We give an unconditional proof for certified randomness in the random oracle model.

Instead of setting a binary-valued score for each question-answer pair as in Section 2.1, for question C and response z, the score is set to $p_C(z)$. Then, in a single round analysis, we first show that if the device passes $(1+\delta)$-XHOG score, then the von Neumann entropy of the joint state is at least $\Omega(n)$.

Theorem 2.4 (Single-round analysis, informal)**.** *Every device $\mathcal{A}$ that on input the first system of a bipartite state ρ_{DE} and given oracle access to a Haar random C, makes $T \leq 2^{n/7}$ queries and solves $(1+\delta)$-XHOG must output a state $2^{-\Omega(n)}$-close to a state ψ_{ZE} classical on system Z such that*

$$H(Z|CE)_\psi \geq 0.99\delta n - O(\log T). \tag{9}$$

Furthermore, there is a single-query device that solves $(2 - 2^{-n})$-XHOG.

To prove Theorem 2.4, the key observation is that one can approximate, to diamond distance $2^{-\Omega(n)}$, any device $\mathcal{A}$ making T queries to a Haar random C by another device $\mathcal{F}$ which does not make any queries, but is given k samples $z_1, \ldots, z_k \sim P_C$ for $k = T^2 \cdot 2^{O(n)}$. For each $\mathcal{A}$, we call the associated device $\mathcal{F}$ the simplified device. With probability $1 - O(k^2/N)$, these samples does not contain any collision. In this event (no collision occurring), $\mathcal{F}$ solves $(1+\delta)$-XHOG implies that $\mathcal{F}$ outputs $z \in S = \{z_1, \ldots, z_k\}$ with probability at least $\delta - o(1)$. Intuitively, this robustly certifies that $\mathcal{A}$'s output must be ε-close to a strategy where the output is prepared by sampling from C for k times and choosing one of the samples.

From this point of view, a simplified device solving $(1+\delta)$-XHOG is equivalent to winning the following game with probability at least $\delta - o(1)$: Given k independent samples S from P_C, outputs a string $z \in S$. Though the game looks quite trivial, it yields a sharp lower bound of the von Neumann min-entropy. By the no-communication theorem, Eve, even if she learns P_C, has no information about the samples given to $\mathcal{F}$, but Eve can potentially control the output distribution when the device sees a particular set of samples. Since with high probability over C, P_C has min-entropy $n - O(\log n)$, we show that averaging over any distribution supported on these samples, the resulting distribution has von Neumann entropy at least $0.99\delta n - O(\log T)$.

Our lower bound in Theorem 2.4 is close to optimal. Consider a device which samples from P_C with probability δ and outputs a uniform string obtained by performing a standard basis measurement on EPR pairs shared with Eve with probability $1 - \delta$. In the former event, the device solves b-XHOG for $b \approx 2$, whereas in the latter, the output is a uniformly random string, which solves 1-XHOG. Thus, by linearity, the device solves $(1 + \delta)$-XHOG. The output joint classical-quantum state from the device is a probabilistic mixture of the two states. Moreover, with overwhelming probability over

15

choices of C, the Shannon entropy of P_C is $n - O(\log n)$. Then by the concavity of von Neumann entropy, the output has conditional von Neumann entropy $\delta n - o(n)$.

To accumulate the entropy, we give a sequential process which is very similar to the one introduced in Section 2.1: The verifier samples $t = O(\log n)$ different circuits, and asks for at least k samples for each circuit. Upon receiving the samples, the verifier chooses k random samples for each circuit, and checks if the device passes $\text{LXEB}_{1+\delta,k}$ for a constant δ for 99% of the circuits. We show that the accumulation process certifies $\Omega(\delta mn)$ bits.

Theorem 2.5 (Entropy accumulation from a general device, informal). *For integer $k = \Omega(n^2)$, $m = \Omega(k \log n)$, there exists an entropy accumulation protocol taking m samples such that conditioned on the event Ω of non-aborting,*

$$H_{\min}(Z|CE)_{\rho|\Omega} \geq n\big(0.99\delta m - O(\sqrt{m})\big) \tag{10}$$

for devices solving $\text{LXEB}_{1+\delta,k}$, where ρ is the output state, Z is the samples from the device, C is the circuits and E is the information held by Eve.

More concretely, taking $\delta = 0.1$, this bound is $n \cdot (0.099m - O(\sqrt{m}))$ by taking m samples from the device. We note that this bound is seemingly weaker than the bound in Theorem 2.3, but the number of samples is m (instead of km as in Theorem 2.3). The minimal sample complexities in the protocols are no different—both are $\Omega(n^2 \log n)$—for a perfect device to pass the verification with overwhelming probability. For technical reasons, in the latter protocol, k samples for each verification are randomly chosen (from all samples sent by the device corresponding to the same challenge circuit) and received sequentially. In contrast, in the former protocol, in each round the device is asked to send k samples, and the verifier checks one round for each circuit.

We also note that Theorem 2.3 and Theorem 2.5 are incomparable results. In particular, the security analysis for Theorem 2.5 heavily relies on the model in which the device is given access to the circuit and the distribution (the Haar measure) over circuits. In contrast, the security analysis based on LLHA may still hold when the device is given access to a description of circuits sampled from other distributions. We leave it as an open question whether there exists a hardness assumption under which linear cross-entropy benchmarking certifies min-entropy against an entangling adversary in the plain model.

2.4 Entropy Accumulation

The proof of Theorem 2.5 is based on the entropy accumulation theorem (EAT) by Dupuis, Fawzi and Renner [28], with modifications explained as follows. Let f be an affine function, called the min-tradeoff function, such that in a single-round analysis, one can show that $H(Z|E)_\rho \geq f(q)$ for distribution $q = (p, 1-p)$ and any state ρ whose acceptance probability is p. In an m-round sequential process, the verifier checks γm rounds (called test rounds) by computing the decision bits from the samples, and computes an approximate distribution $\tilde{q} = (\tilde{p}, 1-\tilde{p})$. The min-entropy round across the m rounds is then $m \cdot f(\tilde{q}) - O(\sqrt{m})$. Thus an EAT reduces a multi-round analysis to a lower bound on the single-round von Neumann entropy.

Since we adopt the b-XHOG score for a bound of the von Neumann entropy in a single round analysis, the score obtained from the test rounds is no longer computed from binary random variables. Thus we define a new min-tradeoff function f' which maps the *score* to a lower bound of the von Neumann entropy. Then we show that if an approximation of the score, defined as the average of $p_{C_i}(z_i)$ is more than s, then the accumulated entropy is at least $m \cdot f'(s) - O(\sqrt{m})$.

The entropy accumulation procedure allows for *spot checking*, that is, in the m-round process, instead of computing $p_{C_i}(z_i)$ for every round $i \in [m]$, the verifier only computes $p_{C_i}(z_i)$ for a subset of indices i of size $O(n^2 \log n)$. In more details, the verifier changes the circuits for $O(\log n)$ times, and in each epoch the verifier computes the average of $k = O(n^2)$ samples. The number of test rounds is set for the device that takes i.i.d. samples from p_C on each circuit C to pass the verification with overwhelming probability. By Hoeffding's inequality, a device that samples from p_C outputs k samples whose average score is concentrated above $2 - O(1)$ for a typical C with overwhelming probability. If the verifier passes $\text{LXEB}_{b,k}$ for the epoches of a sufficiently large fraction $\Omega(1)$, the average is above $1 + \Omega(1)$ with overwhelming probability, and by the entropy accumulation theorem, the conditional min-entropy is $\Omega(nm)$.

2.5 Pseudorandomness and Statistical Zero Knowledge

The protocols for certified randomness rely on perfect randomness for generating the challenge circuit. However, by a counting argument, the challenge space is doubly exponentially large, and it requires exponentially many random bits to compute a truly random circuit. To produce a net gain in randomness, we must rely an efficiently computable function which uses polynomially many random bits and generates pseudorandomness with security level sufficient for our purpose.

However, the standard notion of pseudorandom functions (PRFs) against quantum polynomial-time adversaries does not seem to be sufficient, since it only guarantees the output of the device is *pseudorandom*! Thus for certified randomness, we require a stronger pseudorandom function, when a truly random function is replaced with which, the output remains *statistically indistinguishable* from the uniform distribution.

To provide such a security guarantee, we construct a pseudorandom function indistinguishable from a truly random function for any QSZK protocols. To see why such a security level is sufficient, we recall facts about the class QSZK which consists of promise problems that admit a quantum statistical zero-knowledge protocol. A QSZK protocol is one that consists of a proof system, i.e., a quantum polynomial-time verifier and an unbounded prover, and an efficient quantum simulator which simulates the interaction of the proof system without access to a witness.

Watrous showed that QSZK has a natural complete problem called the *quantum state distinguishability problem* (QSD) [61]. In this problem, the instance is a tuple of two efficiently computable quantum circuits Q_0, Q_1. For $\alpha \in (0, 1]$, the verifier is challenged to determine the trace distance $\|\rho_0 - \rho_1\|_{\text{tr}}$ is at least α, or at most α^2, where ρ_b is a marginal state obtained by computing Q_b for $b \in \{0, 1\}$. It is known for this class, there is an amplification procedure, and therefore the gap can be made exponentially close to 1 [61]. More recently, Menda and Watrous showed that relative to a random oracle, $\text{UP} \not\subset \text{QSZK}$ [44]. Ben-David and Kothari defined a query measure on statistical zero-knowledge proof, and showed that the positive-weighted adversary method can only prove suboptimal lower bounds for certain problems [16].

For certified randomness, we define the QSZK-distinguishability between two distributions over functions, and a similar definition can be extended to distributions over unitaries.

Definition 2.6 (QSZK-distinguishability, informal)**.** *Two distributions $\mathcal{D}_0, \mathcal{D}_1$ over functions are said to be* QSZK-*distinguishable if there exist a pair of algorithms $\mathcal{A}, \mathcal{B}$ such that the averaged trace distance between $\mathcal{A}^F$ and $\mathcal{B}^F$'s output states has non-neglgigible difference between $F \sim \mathcal{D}_0$ and $F \sim \mathcal{D}_1$. The distributions are said to be* QSZK-*indistinguishable if no such algorithms exist.*

A QSZK-secure pseudorandom function is defined as one QSZK-indistinguishable from a random function. We propose an assumption, called pseudorandom function assumption (PRFA), that there

exists a QSZK-secure pseudorandom function. We justify the assumptions are valid by giving a construction for algorithms given oracle access to the function.

Theorem 2.7 (Pseudorandom functions, informal). *There exists a QSZK-secure pseudorandom function with key length $O(n)$ relative to a random oracle.*

Similarly, we say a pseudorandom unitary is QSZK-secure if it is QSZK-indistinguishable from a random unitary. We propose a similar assumption, called pseudorandom unitary assumption (PRUA), that there exists a QSZK-secure pseudorandom unitary, and prove the existence relative to an oracle with key length $O(n)$.

Under these assumptions, when replacing a random circuit with a pseudorandom one, the output remains statistical indistinguishable from a uniform distribution, conditioned on Eve's side information. To see why, recall that De, Portmann, Vidick, and Renner [26] showed that Trivesan's randomness extractor [59] is quantum-proof. That is, the output from the randomness extractor together with Eve's side information is a quantum state ρ statistically indistinguishable from $\sigma \otimes \rho_E$, where σ is a maximally mixed state and ρ_E is the marginal state held by Eve. If the device given a pseudorandom circuit outputs a quantum state that changes the distance by a non-negligible amount from $\sigma \otimes \rho_E$, then such a device implies a QSZK protocol that distinguishes a pseudorandom circuit from a random one.

To see there is a net gain in randomness, the protocol samples $O(\log n)$ pseudorandom circuits, each of which takes $O(n)$ random bits for the keys of the pseudorandom function, and finally it produces $\Omega(mn)$ random bits. For $m = \text{poly}(n)$, we have a polynomial expansion.

While we do not know whether a weaker assumption can work for certified randomness, the security level seems necessary against an entangling adversary. Indeed, if there is no quantum side information, then all we need is to use a pseudorandom circuit against adversaries solving the *statistical difference from uniform* problem. In the purely classical setting, the problem is known to be complete for NISZK, a subclass of SZK consisting of problems that admits a non-interactive statistical zero-knowledge protocol [31]. However, in the presence of quantum side information, an unbounded Eve can prepare any ρ_E, and security against QSZK seems necessary.

3 Preliminaries

As we said, a circuit C acts on n qubits, and $N = 2^n$. The binary entropy function $h : [0,1] \to \mathbb{R}$ is defined as $h(x) := -x \log x - (1-x) \log(1-x)$ and $h(0) = h(1) = 0$. For matrix A, we denote by $\|A\|_p := \text{tr}(|A|^p)^{1/p}$ the Schatten p-norm of A. Furthermore, we denote $\|A\|_{\text{op}}$ the operator norm and $\|A\|_F := \left(\sum_{i=1}^n \sum_{j=1}^n |A_{ij}|^2\right)^{1/2}$ the Frobenius norm of an $n \times n$ matrix A. The trace distance between two quantum states ρ, σ is defined as $\|\rho - \sigma\|_{\text{tr}} := \frac{1}{2}\|\rho - \sigma\|_1$. The fidelity $F(\rho, \sigma)$ between two quantum states ρ, σ is defined as $\|\rho^{1/2}\sigma^{1/2}\|_1$. The function F is symmetric, i.e., $F(\rho, \sigma) = F(\sigma, \rho)$. If ρ is a pure state $|\psi\rangle$, then the fidelity $F(\rho, \sigma) = \langle\psi|\sigma|\psi\rangle$.

A quantum processes is completely positive trace preserving (CPTP) map. For integer $n, m > 0$, let $\Phi : M_n(\mathbb{C}) \to M_m(\mathbb{C})$ denote a linear transformation from complex-valued $n \times n$ matrices $M_n(\mathbb{C})$ to $M_m(\mathbb{C})$. The diamond norm of Φ is defined as $\|\Phi\|_\diamond := \max_{X \in M_n(\mathbb{C}):\|X\|_1 \leq 1} \|\Phi \otimes \mathbb{1}_n(X)\|$. The diamond distance between two quantum processes Φ and Ψ is defined as $\|\Phi - \Psi\|_\diamond$.

For Hilbert space A, we denote $\mathbb{S}(A)$ the set of normalized quantum state in A. For Hilbert spaces A, B, we denote $\text{CPTP}(A, B)$ the set of CPTP maps from linear operators on A to linear operators on B. The set of unitary operators on A be $\mathbb{U}(A)$.

3.1 Complexity Classes

We assume the readers to have the familiarity with standard classical complexity classes and the class BQP. Here we briefly introduce quantum complexity classes related to our work. The class QMA (which stands for "Quantum Merlin-Arthur") is a quantum analogue of MA, defined as follows.

Definition 3.1 (QMA). *The complexity class* QMA *consists of languages L for which there exists a quantum polynomial-time algorithm V such that the following conditions hold.*

- *If $x \in L$, there exists a quantum state ρ on $\mathrm{poly}(|x|)$ qubits such that $\Pr[V(x, \rho)\ accepts] \geq 2/3$.*

- *If $x \notin L$, for every quantum state ρ on $\mathrm{poly}(|x|)$ qubits, $\Pr[V(x, \rho)\ accepts] \leq 1/3$.*

The quantum polynomial-time algorithm V is also called the QMA verifier, and the state ρ can be thought of as a state sent by a QMA "prover" of unbounded power. The class QCMA is also a quantum analogue of MA and can be defined similarly as QMA, except that the witness state ρ is restricted to a classical string. To be specific about the running time or the query complexity of a QMA verifier, we denote QMA(T) to be a QMA verifier running in time T or making T queries in a relativized world. The same notation also applies to other classes.

The class QCAM (which stands for "Quantum-Classical Arthur Merlin") is a quantum analogue of AM, and can be defined in terms of a two-message protocol. In the first message, the quantum polynomial-time verifier sends a random string r of size polynomial in the size of the instance to the prover Merlin. Merlin then sends a response w (also called the witness) which is also of size polynomial in the size of the instance. Note that the witness w can arbitrarily depend on the instance and the random string r. A language is in QCAM if there exists an Arthur which outputs the correct answer for every instance with probability at least 2/3.

Definition 3.2 (QCAM). *The complexity class* QCAM *consists of languages L for which there exists a quantum polynomial-time algorithm V (also called Arthur) and a polynomial p such that the following conditions hold.*

- *If $x \in L$, then there exist a polynomial q and a classical string $w \in \{0,1\}^{q(|x|)}$ such that*

$$\Pr_{r \in \{0,1\}^{p(|x|)}}[V(x, r, w)\ accepts] \geq 2/3. \tag{11}$$

- *If $x \notin L$, then for every polynomial q and every string $w \in \{0,1\}^{q(|x|)}$,*

$$\Pr_{r \in \{0,1\}^{p(|x|)}}[V(x, r, w)\ accepts] \leq 1/3. \tag{12}$$

A k-message interactive proof system consists of two algorithms, the computationally unbounded prover P and a polynomial-time verifier V, and there are k message exchanges between V and P. We will also say such a protocol is a verifier of length k. The class QIP is an interactive proof system in which the verifier runs in quantum polynomial time, and each message can be a quantum state. Such a protocol is also called a quantum interactive proof system.

Definition 3.3 (QIP[k]). *The complexity class* QIP[k] *consists of languages L for which there exists a quantum polynomial-time algorithm V (also called the verifier) of length k such that the following conditions hold.*

- If $x \in L$, then there exists a prover P which makes the verifier accepts with probability $2/3$.

- If $x \notin L$, then for every prover P, the verifier V accepts with probability at most $1/3$.

The complexity class QSZK (which stands for "Quantum Statistical Zero-Knowledge) consists of languages that admit a quantum statistical zero-knowledge protocol, defined by Watrous [61].

Definition 3.4 (QSZK). *A quantum statistical zero-knowledge proof system for a language L consists of an unbounded P (called the honest prover), a quantum polynomial-time verifier V such that the following holds.*

- *Completeness and soundness: (V, P) is a proof system for L.*

- *Zero-knowledge: there exist a negligible function η and a set of preparable states $\{\sigma_{x,i}\}$ such that if $x \in L_1$, $\|\sigma_{x,i} - \mathrm{view}_{V,P}(x,i)\|_{\mathrm{tr}} \leq \eta(|x|)$. Here $\mathrm{view}_{V,P}(x,i)$ is the verifier's view after the i-th round, i.e., the mixed state of the verifier and the message qubits after i-th message have been sent during an execution of the proof system on input x.*

Watrous showed that QSZK has a natural complete problem called Quantum State Distinguishability (QSD) [61], defined as follows.

Definition 3.5 $((\alpha, \beta)$-QSD). *The promise problem (α, β)-QSD $= (\mathrm{QSD}_1, \mathrm{QSD}_0)$ for $0 \leq \alpha < \beta^2 \leq 1$ consists of a pair of quantum circuits (Q_0, Q_1) such that*

- *if $(Q_0, Q_1) \in \mathrm{QSD}_1$, then $\|\rho_0 - \rho_1\|_{\mathrm{tr}} \geq \beta$, and*

- *if $(Q_0, Q_1) \in \mathrm{QSD}_0$, then $\|\rho_0 - \rho_1\|_{\mathrm{tr}} \leq \alpha$,*

where ρ_b is obtained by applying Q_b on the zero state followed by partial tracing on some of the qubits.

Watrous showed that the complete and soundness parameters (α, β) can be amplified to $(2^{-n}, 1 - 2^{-n})$ by giving a transformation from Q_b to a circuit that has size polynomial in n and $|Q_b|$ for $b \in \{0, 1\}$ [61]. Since the parameters do not matter for this problem, we will denote QSD the same problem with a constant gap.

The problem has a very simple QSZK protocol: The verifier tosses a random coin b, and sends ρ_b to the prover. The prover performs the optimal measurement that saturates the trace distance and outputs a bit b'. The verifier accepts if $b = b'$. The completeness follows from the fact that the states's trace distance is negligibly close to one, and this implies there exists a measurement that perfectly distinguishes the states. For the soundness, since the states are negligibly close in trace distance, the prover does not succeed with non-negligibly advantage over random guessing. To show the protocol is zero-knowledge, the quantum simulator applies the verifier's quantum operation first. After receiving the reponse b' from the prover, it sets $b' = b$.

The QSZK-completeness of QSD relativizes. In particular, Menda and Watrous [44] showed that for oracle A, a problem L_A in QSZK^A if there exists a reduction from L_A to QSD^A.

Theorem 3.6 ([44, Theorem 1]). *For alphabet Σ, Γ, let $L \subseteq \Gamma^*$ be a language and $A \subseteq \Sigma^*$ be an oracle. The language L_A is contained in QSZK^A if and only if there exists a polynomial-time uniform family of pairs of relativized quantum circuits (Q_0^A, Q_1^A) with the following properties:*

- *If $x \in L_A$, then $(Q_0^A, Q_1^A) \in \mathrm{QSD}_1^A$.*

- *If $x \notin L_A$, then $(Q_0^A, Q_1^A) \in \mathrm{QSD}_0^A$.*

Ben-David and Kothari [16] studied independently the so-called QSZK complexity of function f, denoted QSZK(f), which is defined as the minimum number k made by a pair of query algorithms $\mathcal{A}, \mathcal{B}$ given oracle access to x such that for every x such that (i) if $f(x) = 1$, then $\|\mathcal{A}^x - \mathcal{B}^x\|_{\mathrm{tr}} \geq 2/3$, and (ii) if $f(x) = 0$, then $\|\mathcal{A}^x - \mathcal{B}^x\|_{\mathrm{tr}} \leq 1/3$.

3.2 The Polynomial Method

The quantum polynomial method by Beals, Buhrman, Cleve, Mosca, and de Wolf is a standard technique for proving quantum lower bound of query problems [15]. Specifically, we will use the degree lower bound by Markov and the strong direct product theorem by Sherstov [58].

Lemma 3.7. *Let* $p : \mathbb{R} \to \mathbb{R}$ *be a polynomial. For real numbers* a, b, *if*

$$\max_{a \leq x \leq b} |p(x) - p(y)| \leq H, \tag{13}$$

then

$$|p'(x)| \leq \frac{H}{b - a} \deg(p)^2, \tag{14}$$

where p' *is the first derivative of* p *and* $\deg(p)$ *is the degree of* p.

Theorem 3.8 (Strong direct product theorem [58, Theorem 1.5]). *Fix functions* $f_1, \ldots, f_k : \{-1, +1\}^m \to \{-1, +1\}$. *Then solving* $(f_1, \ldots, f_k)$ *with worst-case probability* $2^{-\Omega(k)}$ *requires*

$$\Omega \left(\min_{S \subseteq [k]:|S|=0.99k} \left(\sum_{i \in S} \deg_{1/5}(f_i) \right) \right), \tag{15}$$

where $\deg_\varepsilon(f)$ *stands for the least degree of a real polynomial that approximates* f *within* ε *pointwise.*

3.3 Quantum Information Theory

The amount of extractable randomness is the conditional min-entropy $H_{\min}(Z|E)$ which describe the amount of randomness system Z has conditioned on Eve's information E. The smooth min-entropy is formally defined as

$$H_{\min}(Z|E)_\rho = \sup_{\sigma_E} \left\{ -\inf_\lambda \left\{ \lambda : \rho_{ZE} \leq 2^{-\lambda} \mathbb{1}_Z \otimes \sigma_E \right\} \right\}. \tag{16}$$

In the case where both Z and E are classical, they are formally defined as random variables, and both ρ_{ZE} and σ_E are diagonal in the same basis.

We will also consider a smooth version of conditional min-entropy, which relaxes the above notion by considering an ε-close pair of random variables, in total variation distance:

$$H_{\min}^\varepsilon(Z|E)_\rho = \sup_{\tilde{\rho}:\|\tilde{\rho}_{ZE} - \rho_{ZE}\|_{\mathrm{tr}} \leq \varepsilon} H_{\min}(Z|E)_\rho. \tag{17}$$

Another useful quantity in the family of quantum Rényi entropies is the von Neumann entropy. The von Neumann entropy of a quantum state ρ_A is defined as $H(A)_\rho := -\mathrm{tr}(\rho \log \rho)$. The conditional von Nemann entropy of a bipartite state ρ_{AB} is defined as $H(A|B)_\rho = H(AB)_\rho - H(B)_\rho$.

For classical random variable X distributed according to a distribution P, we denote $H(X)$ or $H(P)$ the von Neumann entropy of X, and $H_{\min}(X)$ or $H_{\min}(P)$ the min-entropy of X.

The following inequalities for von Neumann entropy will be useful.

Lemma 3.9. *For finite-dimensional Hilbert spaces A, B, C and a tripartite state ρ_{ABC} on $A \otimes B \otimes C$, it holds that*

$$H(A|B)_\rho + H(B|C)_\rho \geq H(A|C)_\rho. \tag{18}$$

Proof. By strong sub-additivity, $H(A|BC)_\rho \leq H(A|B)_\rho$ and thus

$$\begin{aligned} H(B|C)_\rho &= H(AB|C)_\rho - H(A|BC)_\rho \\ &\geq H(A|C)_\rho - H(A|B)_\rho. \end{aligned} \tag{19}$$

$\square$

Lemma 3.10. *For finite-dimensional Hilbert space A, let ρ, σ be two normalized quantum states on A. For $\lambda \in [0, 1]$,*

$$H(A)_{(1-\lambda)\rho+\lambda\sigma} \leq (1-\lambda)H(A)_\rho + \lambda H(A)_\sigma + h(\lambda) \tag{20}$$

where h is the binary entropy function.

Proof. Define the quantum state

$$\psi_{BA} = (1-\lambda)|0\rangle\langle0|_B \otimes \rho_A + \lambda|1\rangle\langle1|_B \otimes \sigma_A. \tag{21}$$

By definition, the von Neumann entropy of ψ is

$$\begin{aligned} H(BA)_\psi &= -\mathrm{tr}((1-\lambda)\rho\log(1-\lambda)\rho)) - \mathrm{tr}(\lambda\sigma\log\lambda\sigma)) \\ &= -(1-\lambda)\log(1-\lambda) - (1-\lambda)\mathrm{tr}(\rho\log\rho) - \lambda\log\lambda - \lambda\mathrm{tr}(\sigma\log\sigma) \\ &= H(A)_\rho + H(A)_\sigma + h(\lambda). \end{aligned} \tag{22}$$

Moreover, since $\mathrm{tr}_B(\psi) = (1-\lambda)\rho + \lambda\sigma$, $H(A)_\psi = H(A)_{(1-\lambda)\rho+\lambda\sigma}$. Since conditional von Neumann entropy is always non-negative, $H(BA)_\psi \geq H(A)_\psi$, and we conclude the proof. $\square$

Lemma 3.11 ([48, Theorem 11.9]). *For Hilbert space A, let ρ be a quantum state on A and $\{P_i\}$ be a complete set of projective measurements on A. Then the entropy of the post-measurement state $\sigma = \sum_i P_i \rho P_i$ is at least as great as the original entropy, i.e., $H(A)_\sigma \geq H(A)_\rho$.*

By Lemma 3.10 and concavity of von Neumann entropy, we can lower bound the mutual information of a probabilistic mixture of states by a convex combination of the mutual information of each component. Recall that by definition, for Hilbert space A, B and bipartite state ρ_{AB}, $I(A : B)_\rho = H(A) + H(B) - H(AB)$.

Lemma 3.12. *For finite-dimensional Hilbert space A and B, let ρ_{AB}, σ_{AB} be a bipatite state. For $\lambda \in [0, 1]$,*

$$I(A : B)_{(1-\lambda)\rho+\lambda\sigma} \geq (1-\lambda)I(A : B)_\rho + \lambda I(A : B)_\sigma - h(\lambda).$$

Proof. By convexity of von Neumann entropy, for $X \in \{A, B\}$,

$$H(X)_{(1-\lambda)\rho+\lambda\sigma} \geq (1-\lambda)H(X)_\rho + \lambda H(X)_\sigma. \tag{23}$$

Then by Lemma 3.10,

$$\begin{aligned} I(A : B)_{(1-\lambda)\rho+\lambda\sigma} &= H(A)_{(1-\lambda)\rho+\lambda\sigma} + H(B)_{(1-\lambda)\rho+\lambda\sigma} - H(AB)_{(1-\lambda)\rho+\lambda\sigma} \\ &\geq (1-\lambda)I(A : B)_\rho + \lambda I(A : B)_\sigma - h(\lambda). \end{aligned} \tag{24}$$

$\square$

3.4 Haar Random Unitaries

We will rely one the following facts. For a Haar random unitary $C \in \mathbb{C}^{N \times N}$, for every $i \in \{0, 1\}^n$, it holds that the distribution P of density $P_z = p_C(z) := |\langle z|C|0\rangle|^2$ is distributed according to the Dirichlet distribution $\mathrm{Dir}(1^N)$ on the probability simplex [27, 39].

3.4.1 The Dirichlet Distributions

Let $\mathrm{Dir}(\alpha)$ denote the Dirichlet distribution for concentration hyperparameter α. The moments for $(X_1, \ldots, X_N) \sim \mathrm{Dir}(\alpha)$ for $\alpha = (\alpha_1, \ldots, \alpha_N)$ is well-studied. First, the mean of each random variable $\mathbb{E}[X_i] = \frac{\alpha_i}{\alpha_0}$, where $\alpha_0 = \sum_{i=1}^N \alpha_i$. Moreover,

$$\mathbb{E}\left[\prod_{i=1}^N X_i^{\beta_i}\right] = \frac{B(\alpha + \beta)}{B(\alpha)}, \tag{25}$$

where $B(\alpha) := \frac{1}{\Gamma(\alpha_0)} \prod_{i=1}^N \Gamma(\alpha_i)$.

The Dirichlet distribution is the conjugate prior distribution of the categorical distribution and the multinomial distribution [30]. If the prior distribution is sampled according to the Dirichlet distribution, the posterior is also a Dirichlet distribution with a different hyperparameter. In particular, let the data points be $z_1, \ldots, z_k \sim P$ where $P \sim \mathrm{Dir}(\alpha)$. Then the posterior distribution $P|(z_1, \ldots, z_k) \sim \mathrm{Dir}(\alpha + m)$, where m is the vector of the number of occurrences for the data points in each category.

We can sample a probability distribution from the Dirichlet distribution $\mathrm{Dir}(\alpha)$ using the following process: First sample $Q_i \sim \Gamma(\alpha_i, 1)$ independently for $i \in [N]$, where $\Gamma(\alpha_i, 1)$ is the Gamma distribution with parameters $\alpha_i, 1$. Then compute $\bar{Q} = \sum_{i=1}^N Q_i$ and set $P_i = Q_i/\bar{Q}$ for each $i \in [N]$. Thus it would be useful to briefly introduce facts about the Gamma function. Recall that the Gamma distribution $\Gamma(\alpha, \beta)$ has pdf

$$f(x; \alpha, \beta) = \frac{\beta^\alpha e^{-\beta x} x^{\alpha-1}}{\Gamma(\alpha)}. \tag{26}$$

In particular, for $\alpha = \beta = 1$, the pdf is $f(x; 1, 1) = e^{-x}$. This implies that the CDF of $\Gamma(1, 1)$ is

$$F(x; 1, 1) = 1 - e^{-x}. \tag{27}$$

Using these facts, we prove a few lemmas which will be useful later. First, the maximum value of $P \sim \mathrm{Dir}(1^N)$ is $O(n)/N$ in expectation.

Lemma 3.13. *Let $P \sim \mathrm{Dir}(1^N)$. Then*

$$\mathop{\mathbb{E}}_{P \sim \mathrm{Dir}(1^N)}\left[\max_z P_z\right] \leq \frac{2\ln N + 7}{N}. \tag{28}$$

and

$$\mathop{\mathbb{E}}_{P \sim \mathrm{Dir}(1^N)}[H_{\min}(P)] \geq n - \log n - O(1). \tag{29}$$

Proof. Let $F(x) = 1 - e^{-x}$ be the CDF of $\Gamma(1, 1)$ and $Q_1, \ldots, Q_N \sim \Gamma(1, 1)$. Also let $Q = (Q_1, \ldots, Q_N)$. The CDF of $\max_z Q_z$ is

$$G(x) = \Pr[\forall z, Q_z \leq x] = (1 - e^{-x})^N. \tag{30}$$

Thus the expectation

$$\mathop{\mathbb{E}}_{Q\sim\Gamma(1,1)^N}\left[\max_z Q_z\right] = \int_0^\infty dx(1-(1-e^{-x})^N)$$

$$= \int_0^1 dy\frac{1-y^N}{1-y}$$

$$= \int_0^1 dy(1+y+y^2+\ldots y^{N-1})$$

$$= 1+\frac{1}{2}+\ldots+\frac{1}{N}$$

$$\leq \ln N+1. \tag{31}$$

As shown in the proof of Lemma 3.14, $\bar{Q}=\sum_z Q_z$ is concentrated:

$$\Pr_Q[|\bar{Q}-N|\leq N/2]\geq 1-\frac{4}{N}. \tag{32}$$

Let $\Omega := \{Q : \bar{Q}\geq N/2\}$. From (32), $\Pr_{Q\sim\Gamma(1,1)^N}[Q\in\Omega]\geq 1-4/N$. This means that

$$\mathop{\mathbb{E}}_{Q\sim\Gamma(1,1)^N}\left[\frac{\max_z Q_z}{\bar{Q}}\right] \leq \mathop{\mathbb{E}}_Q\left[\frac{\max_z Q_z}{\bar{Q}}\middle|Q\in\Omega\right]+\Pr[Q\notin\Omega]$$

$$\leq \frac{2}{N}\mathop{\mathbb{E}}_Q\left[\max_z Q_z\middle|Q\in\Omega\right]+\frac{4}{N}$$

$$\leq \frac{2}{N}\frac{1}{\Pr[Q\in\Omega]}\mathop{\mathbb{E}}_Q\left[\max_z Q_z\right]+\frac{4}{N}$$

$$\leq \frac{2\ln N+7}{N}. \tag{33}$$

This show that (28) is correct. For (29), by Jensen's inequality,

$$\mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N)}[H_{\min}(P)] \geq -\log\mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N)}\left[\max_z P_z\right]\geq n-\log n-O(1). \tag{34}$$

$$\square$$

In fact, the maximum of $P\sim\mathrm{Dir}(1^N)$ is concentrated around $O(n)/N$.

Lemma 3.14. *It holds that*

$$\Pr_{P\sim\mathrm{Dir}(1^N)}\left[\max_z P_z\leq\frac{4\ln N}{N}\right]\geq 1-\frac{6}{N}. \tag{35}$$

Proof. Let $F(x)=(1-e^{-x})$ be the CDF of $\Gamma(1,1)$. Thus instead consider

$$\Pr_{Q\sim\Gamma(1,1)^N}\left[\max_z Q_z\leq 2\ln N\right] = \Pr_{Q\sim\Gamma(1,1)^N}[\forall z,Q_z\leq 2\ln N]$$

$$= F(2(\ln 2)n)^N$$

$$= (1-N^{-2})^N$$

$$\geq 1-2/N. \tag{36}$$

Also $\bar{Q} = \sum_z Q_z$ is concentrated since the mean $\mathbb{E}[\bar{Q}] = N$ and the variance $\sigma^2 = \mathbb{E}[\bar{Q}^2] - \mathbb{E}[\bar{Q}]^2 = N(\mathbb{E}[\bar{Q}_0^2] - \mathbb{E}[\bar{Q}_0]^2) = N$. By Chebyshev inequality,

$$\Pr_Q[|\bar{Q} - N| \leq N/2] \geq 1 - \frac{4}{N}. \tag{37}$$

Combining (36) and (37),

$$\Pr_Q\left[\frac{\max_z Q_z}{\bar{Q}} \leq \frac{4\ln N}{N}\right] \geq 1 - \frac{6}{N}. \tag{38}$$

$\square$

3.4.2 The Performance of a Perfect Device

In this paper, we define a perfect device to be one that is given C, outputs a sample $z \sim p_C$, where p_C is the distribution defined by $p_C(z) := |\langle z|C|0^n\rangle|^2$. The first result is well-known and has been proven using different mathematical tools: a perfect device solves b-XHOG for $b \approx 2$. Here we prove the result using properties of the Dirichlet distribution.

Lemma 3.15. *Sampling from $z \sim P_C$ for Haar random C, it holds that*

$$\mathbb{E}_{C\sim\mathrm{Haar}(N),z\sim P_C}[p_C(z)] = \frac{2}{N+1}. \tag{39}$$

Proof. The algorithm $\mathcal{A}$ outputs the given sample z. For $z \in \{0,1\}^n$, let $P_z = |\langle z|C|0\rangle|^2$ be a random variable for Haar random C, and $P = (P_0, \ldots, P_{N-1})$ be a vector of random variables distributed on the probability simplex. Since $P \sim \mathrm{Dir}(1^N)$, $P|z \sim \mathrm{Dir}(m + 1^N)$, where $m = (0, \ldots, 0, m_z = 1, 0, \ldots, 0)$. The score can be calculated as follows:

$$\mathbb{E}_{P\sim\mathrm{Dir}(1^N)}[P_z|m] = \mathbb{E}_{P\sim\mathrm{Dir}(m+1^N)}[P_z] = \frac{m_z + 1}{N+1}. \tag{40}$$

Thus for z such that $m_z = 1$, and the expectation is $\frac{2}{N+1}$. $\square$

In fact, the score for $C \sim \mathrm{Haar}(N)$ is concentrated around $\frac{2}{N+1}$. Thus sampling from $C \sim \mathrm{Haar}(N)$, with overwhelming probability, a perfect device answers with a sample that has score close to $\frac{2}{N+1}$.

Lemma 3.16 (Concentration of collision probability). *Let $S_C := \mathbb{E}_{z\sim p_C}[p_C(z)]$. Then S_C is concentrated in the sense that*

$$\Pr_C\left[\left|S_C - \frac{2}{N+1}\right| \leq \frac{\varepsilon}{N+1}\right] \geq 1 - O\left(\frac{1}{\varepsilon^2 N}\right). \tag{41}$$

Proof. We consider the moments of the random variable $S_C = \sum_z p_C(z)^2$ for Haar random C. By

25

Lemma 3.15, $\mu = \mathbb{E}_C[S_C] = \frac{2}{N+1}$.

$$
\begin{aligned}
\mathbb{E}_C[S_C^2] &= \mathbb{E}_C\left[\sum_{z,z'} p_C(z)^2 p_C(z')^2\right] \\
&= N\,\mathbb{E}_C[p_C(0)^4] + N(N-1)\,\mathbb{E}_C[p_C(0)^2 p_C(1)^2] \\
&= \frac{N!4!}{(N+3)!} + N(N-1)\frac{(N-1)!2!2!}{(N+3)!} \\
&= \frac{20+4N}{(N+1)(N+2)(N+3)}
\end{aligned}
\tag{42}
$$

Therefore, the variance is

$$
\begin{aligned}
\mathbb{E}_C[S_C^2] - \mathbb{E}_C[S_C]^2 &= \frac{(4N+20)(N+1) - 4(N+2)(N+3)}{(N+1)^2(N+2)(N+3)} \\
&= \frac{4(N-1)}{(N+1)^2(N+2)(N+3)} = O\left(\frac{1}{N^3}\right).
\end{aligned}
\tag{43}
$$

By Chebyshev inequality,

$$
\begin{aligned}
\Pr_C\left[\frac{2+\varepsilon}{N+1} \geq S_C \geq \frac{2-\varepsilon}{N+1}\right] &= \Pr_C\left[|S_C - \mu| \leq \frac{\varepsilon}{N+1}\right] \\
&\geq 1 - \frac{4(N-1)}{\varepsilon^2(N+2)(N+3)} = 1 - O\left(\frac{1}{\varepsilon^2 N}\right).
\end{aligned}
\tag{44}
$$

This implies that with probability $1 - O(\frac{1}{\varepsilon^2 N})$ over C, when $S_C \geq (2-\varepsilon)/N$. $\qquad\square$

This lemma shows that the collision probability of P_C is sharply concentrated around its mean. That is, for almost every C, if the device samples from P_C, the expectation of $p_C(z)$ is very close to $\frac{2}{N+1}$. This implies that a device sampling from P_C solves $\mathrm{LXEB}_{b,k}$ with constant probability for $k = \Omega(n^2)$ and $b \geq 1.98$.

Lemma 3.17. *For integer k, with probability $1 - O(1/N)$ over $C \sim \mathrm{Haar}(N)$, sampling $z_1, \ldots, z_k \sim P_C$,*

$$
\Pr_{z_1,\ldots,z_k \sim P_C}\left[\frac{1}{k}\sum_{i=1}^k p_C(z_i) \geq \frac{1.98}{N+1}\right] \geq 1 - 2^{-\Omega(k/n^2)}.
\tag{45}
$$

Proof. By Lemma 3.16 with $\varepsilon = 0.01$,

$$
\Pr_{C \sim \mathrm{Haar}(N)}\left[S_C \geq \frac{1.99}{N+1}\right] \geq 1 - O(1/N).
\tag{46}
$$

Furthermore, by Lemma 3.14, with probability $1 - O(1/N)$, $\max_z p_C(z) \leq 4n/N$. For C satisfying $S_C \geq 1.99/(N+1)$ and $\max_z p_C(z) \leq 4n/N$, by Hoeffding's inequality,

$$
\begin{aligned}
\Pr_{z_1,\ldots,z_k \sim P_C}\left[\frac{1}{k}\sum_{i=1}^k p_C(z_i) \leq \frac{1.98}{N+1}\right] &\leq \Pr_{z_1,\ldots,z_k \sim P_C}\left[\left|\frac{1}{k}\sum_{i=1}^k p_C(z_i) - S_C\right| \geq \frac{0.01}{N+1}\right] \\
&\leq 2e^{-0.01k/(16n^2)} = 2e^{-k/(1600n^2)}.
\end{aligned}
\tag{47}
$$

$\qquad\square$

Therefore, it suffices to take $O(n^2)$ independent samples from $O(\log n)$ different circuits.

Lemma 3.18. *For integer k, circuit C and a tuple d of k strings in $\{0,1\}^n$, let $V_k(C,d)$ be defined as*

$$V_k(C,d) := \mathbb{1}\left[\frac{1}{k}\sum_{i=1}^{k} p_C(z_i) \geq \frac{1.98}{N+1}\right] \tag{48}$$

for $d = (z_1, \ldots, z_k)$. Then for $k = O(n^2)$ and $m = \Omega(\log n)$, sampling a perfect device $\mathcal{A}$ mk times yields $d_1, \ldots, d_m$ satisfying

$$\Pr_{C_1,\ldots,C_m \sim \mathrm{Haar}(N), \{d_i \sim \mathcal{A}(C_i)\}_{i=1}^{m}}\left[\sum_{i=1}^{m} V_k(C_i, d_i) \geq 0.99m\right] \geq 1 - 1/n. \tag{49}$$

Proof. By Lemma 3.17, for $k = cn^2$ for sufficiently large constant c,

$$\mu := \Pr_{C \sim \mathrm{Haar}(N), d \sim \mathcal{A}(C)}[V(C,d) = 1] \geq 0.995. \tag{50}$$

Then by Hoeffding's inequality,

$$\Pr_{C_1,\ldots,C_m \sim \mathrm{Haar}(N), \{d_i \sim \mathcal{A}(C_i)\}_{i=1}^{m}}\left[\sum_{i=1}^{m} V_k(C_i, d_i) \leq 0.99m\right]$$

$$\leq \Pr_{C_1,\ldots,C_m \sim \mathrm{Haar}(N), \{d_i \sim \mathcal{A}(C_i)\}_{i=1}^{m}}\left[\left|\frac{1}{m}\sum_{i=1}^{m} V_k(C_i, d_i) - \mu\right| \geq 0.005\right]$$

$$\leq 2^{-2 \cdot 0.005^2 m}$$

$$\leq 1/n \tag{51}$$

for $m = c' \log n$ for sufficiently large c'. $\qquad\square$

This implies that sampling from a perfect device mk times to yield an approximation of the XHOG score close to $1.94/(N+1)$. The bound can be improved to $2 - c$ for an arbitrarily small constant $c > 0$.

Corollary 3.19. *For $k = O(n^2)$ and $m = \Omega(\log n)$, sampling a perfect device $\mathcal{A}$ for k times on m independent circuits sampled from the Haar measure, with probability $1 - 1/n$,*

$$\frac{1}{mk}\sum_{i=1}^{m}\sum_{j=1}^{k} p_{C_i}(z_{ij}) \geq \frac{1.94}{N+1}, \tag{52}$$

where z_{ij} denotes the j-th sample from C_i.

Proof. The corollary holds from Lemma 3.18 and the implication that

$$\frac{1}{m}\sum_{i=1}^{m} V_k(C_i, d_i) \geq 0.98 \implies \frac{1}{mk}\sum_{i=1}^{m}\sum_{j=1}^{k} p_{C_i}(z_{ij}) \geq \frac{1.94}{N+1}, \tag{53}$$

for $d_i = (z_{i1}, \ldots, z_{ik})$. $\qquad\square$

4   An Entropy Accumulation Theorem

In this section, we modify the entropy accumulation theorem (EAT) from the one given by Dupuis, Fawzi, and Renner [28]. Our proof follows closely from that of [28] except with the following minor changes: In [28], the min-tradeoff function $f : \mathbb{P} \to \mathbb{R}$ is defined over the set of probability distributions $\mathbb{P}$. Here our min-tradeoff function $f : \mathbb{R}^{\geq 0} \to \mathbb{R}$, where the input corresponds to the score of the device. To see the modification does lead to an useful tool that reduces the analysis of a multi-round entropy accumulation process to single-round analysis of von Neumann entropy, we formally prove the theorem from scratch.

Recall that for von Neumann entropy, by definition, the chain rule holds:

$$H(A_1 A_2 | B)_\rho = H(A_1 | B)_\rho + H(A_2 | A_1 B)_\rho \tag{54}$$

for every tripartite state $\rho_{A_1 A_2 B}$. However, the same equality does not hold for other Rényi entropies. Instead, Dupuis, Fawzi, and Renner [28] show the following statement.

Theorem 4.1 ([28, Theorem 3.2]). *Let $\rho_{A_1 A_2 B}$ be a density operator and $\alpha \in (0, \infty)$. Then*

$$H_\alpha(A_1 A_2 | B)_\rho = H_\alpha(A_1 | B)_\rho + H_\alpha(A_2 | A_1 B)_\nu, \tag{55}$$

where

$$\nu_{A_1 A_2 B} = \nu_{A_1 B}^{1/2} \rho_{A_2 | A_1 B} \nu_{A_1 B}^{1/2} \qquad with \qquad \nu_{A_1 B} = \frac{\left(\rho_{A_1 B}^{1/2} \rho_B^{\frac{1-\alpha}{\alpha}} \rho_{A_1 B}^{1/2} \right)^\alpha}{\mathrm{tr} \left(\rho_{A_1 B}^{1/2} \rho_B^{\frac{1-\alpha}{\alpha}} \rho_{A_1 B}^{1/2} \right)^\alpha}. \tag{56}$$

Note that $\nu_{A_1 A_2 B}$ is normalized and $\nu_{A_1 B}$ is the marginal of $\nu_{A_1 A_2 B}$ obtained by tracing out the system A_2. Though there is a state ν such that the equality in (55) holds, for our purpose, we only care about some family of states for which an inequality can be derived. In particular, the following inequality will be useful.

Theorem 4.2 ([28, Theorem 3.3]). *Let $\rho_{A_1 B_1 A_2 B_2}$ be a density operator and $\alpha \in (0, \infty)$ such that the Markov chain condition holds. Then*

$$\inf_\nu H_\alpha(A_2 | B_2 A_1 B_1)_\nu \leq H_\alpha(A_1 A_2 | B_1 B_2)_\rho - H_\alpha(A_1 | B_1)_\rho \leq \inf_\nu H_\alpha(A_2 | B_2 A_1 B_1)_\nu \tag{57}$$

Theorem 4.2 can be obtained by showing that the Markov chain condition implies that $H_\alpha(A_1 | B_1 B_2)_\rho = H_\alpha(A_1 | B_1)_\rho$ and by Theorem 4.1. We can further represent Theorem 4.2 in terms of quantum channels.

Theorem 4.3 ([28, Corollary 3.5]). *Let $\rho_{R A_1 B_1}$ be a density operator on $R \otimes A_1 \otimes B_1$, $\mathcal{M} \in \mathrm{CPTP}(R, A_2 B_2)$ and $\alpha \in (0, \infty)$. If $\mathcal{M}(\rho_{R A_1 B_1})$ satisfies the Markov chain condition $A_1 \leftrightarrow B_1 \leftrightarrow B_2$, then*

$$\inf_\omega H_\alpha(A_2 | B_2 A_1 B_1)_{\mathcal{M}(\omega)} \leq H_\alpha(A_1 A_2 | B_1 B_2)_{\mathcal{M}(\rho)} - H_\alpha(A_1 | B_1)_\rho \leq \sup_\omega H_\alpha(A_2 | B_2 A_1 B_1)_{\mathcal{M}(\omega)}, \tag{58}$$

where the supremum and infimum range over density operator on $R \otimes A_1 \otimes A_2$. Moreover, if $\rho_{R A_1 B_1}$ is pure, then it suffices to optimize over pure states $\omega_{R A_1 B_1}$.

Theorem 4.3 can be obtained by applying Theorem 4.2 and presenting a state ω that saturates the inequalities. In our case, the Markov chain condition trivially holds since the system B_i is empty.

Let $\tilde{E}_{i-1}$ be a system isomorphic to $R_{i-1}E$ and $\mathbb{P}$ denote the set of distributions. Adding a system $\tilde{R}_{i-1}$ is meant to purify the state on $R_{i-1}E$ so the state $\omega_{R_{i-1}E\tilde{R}_{i-1}}$ is pure and its marginal is any state on R_{i-1} input to $\mathcal{M}_i$.

We modify the definition of min-tradeoff function from [28], formally stated as follows.

Definition 4.4. *A real-valued function on $f : \mathbb{R}^{\geq 0} \to \mathbb{R}$ is called a min-tradeoff function for $\mathcal{M}_i$ if it satisfies*

$$f(s) \leq \inf_{\nu \in \Sigma_i(G,s)} H(A_i|E\tilde{E}_{i-1})_\nu \tag{59}$$

where $\Sigma_i(G,s) := \{\rho_{A_i R_i E \tilde{E}_{i-1}} = (\mathcal{M}_i \otimes \mathbb{1}_{E\tilde{R}_{i-1}})(\omega_{R_{i-1}E\tilde{R}_{i-1}}) : \operatorname{tr}(G\rho_{A_i}) = s\}$, i.e., the set of states whose marginal on A_i has score s evaluated using a diagonal, positive semi-definite matrix G.

While the domain of f is the set of non-negative real numbers, we restrict our attention to the properties of f in the interval $[0,2]$ for normalization purposes. Let $\|\nabla f\|_\infty$ be the infinity norm of ∇f restricted to $[0,2]$, and $g_{\max}, g_{\min}$ be the maximum and the minimum of f over $[0,2]$, i.e.,

$$g_{\max} := \max_{s\in[0,2]} f(s), \qquad g_{\min} = \min_{s\in[0,2]} f(s) \tag{60}$$

In particular, it holds that $\frac{1}{2}|g_{\max} - g_{\min}| \leq \|\nabla f\|_\infty$, where $\|\nabla f\|_\infty$ is the infinite norm of f, by setting the domain in $[0,2]$. Note that the restriction is without loss of generality: given a game with score in $[0,a]$ with some diagonal G', we can set $G = 2G'/a$.

To determine the infimum, it suffices to consider only pure states $\omega_{R_{i-1}\tilde{R}_{i-1}}$ since by strong subadditivity, adding a purification system cannot increase $H(A_i|E\tilde{R}_{i-1})$. For an event $\Omega \subseteq \mathcal{A}^m$, we denote

$$\Pr_\rho[\Omega] := \sum_{(a_1,\ldots,a_m)\in\Omega} \operatorname{tr}(\rho_{E,a_1,\ldots,a_m}) \tag{61}$$

for classical-quantum state ρ classical on A^m the trace of the state projected onto the subspace spanned by $|w_1,\ldots,w_m\rangle$ for $(w_1,\ldots,w_m) \in \Omega$. For any state $\rho_{A_1^m B_1^m E}$ classical on $A_1^m B_1^m$, we denote the conditional state

$$\rho_{A^m E|\Omega} := \frac{1}{\Pr_\rho[\Omega]} \sum_{(a_1,\ldots,a_m)\in\Omega} |a_1,\ldots,a_m\rangle\langle a_1,\ldots,a_m| \otimes \rho_{E,a_1,\ldots,a_m}. \tag{62}$$

Clearly, the state is normalized.

The following theorem states it suffices to bound $H_\alpha^\uparrow(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega}$ from below.

Proposition 4.5 ([28, Lemma B.10]). *For any density operator ρ, and non-negative operator σ any $\alpha \in (1,2]$, and any $\varepsilon \in (0,1)$,*

$$H_{\min}^\varepsilon(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} \geq H_\alpha^\uparrow(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} - \frac{\log(2/\varepsilon^2)}{\alpha - 1}. \tag{63}$$

To account for the event Ω, we follow the ideas from [28]: First, we introduce systems $D_1,\ldots,D_m$ and normalized states $\{\tau(z) : z \in \mathcal{Z}\}$ such that

$$H(D_i)_{\tau(z)} = \bar{g} - f(G_z), \tag{64}$$

29

where $G_z := \langle z|G|z \rangle$ and CPTP maps $\mathcal{D}_i : \text{CPTP}(Z_i, Z_i D_i)$, where

$$\mathcal{D}_i(|z\rangle\langle z|) := |z\rangle\langle z| \otimes \tau(z)_{D_i}. \tag{65}$$

Also we define $\bar{\mathcal{M}}_i := \mathcal{D}_i \circ \mathcal{M}_i$. This allows us to apply the following proposition due to Metger, Fawzi, Sutter, and Renner [45].

Proposition 4.6 ([45, Lemma 4.5]). *For $\alpha > 1$ and normalized state ρ,*

$$H_\alpha^\uparrow(Z^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)|\Omega} \geq H_\alpha^\uparrow(Z^m D^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)|\Omega} - \max_{z \in \Omega} H_\alpha(D^m)_{\bar{\mathcal{M}}_m \circ \ldots \circ \bar{\mathcal{M}}_1(\rho)_z}. \tag{66}$$

Let $g_{\min}$ and $g_{\max}$ denote the maximum and minimum of the range of f. Furthermore, let $\bar{g} := \frac{1}{2}(g_{\min} + g_{\max})$. We say a distribution q is induced by samples $z_1, \ldots, z_m$ if

$$q(z) = \frac{1}{m}|\{i : z_i = z\}|. \tag{67}$$

For affine f and distribution q induced by the samples $z_1, \ldots, z_m$,

$$\left| \bar{g} - f\left(\mathop{\mathbb{E}}_{z \sim q} G_z \right) \right| \leq \frac{1}{2}|g_{\max} - g_{\min}| \leq \|\nabla f\|_\infty. \tag{68}$$

We next bound each term on the rhs of (66) individually.

Proposition 4.7. *For $\alpha > 1$ and every $z = (z_1, \ldots, z_m) \in \mathcal{Z}^m$,*

$$H_\alpha(D^m)_{\bar{\mathcal{M}}_m \circ \ldots \circ \bar{\mathcal{M}}_1(\rho)_{D,z}} \leq m\|\nabla f\|_\infty, \tag{69}$$

Proof. Since each $\tau(z_i)_{D_i}$ is determined from z_i, the marginal state is product, i.e.,

$$\bar{\mathcal{M}}_m \circ \ldots \circ \bar{\mathcal{M}}_1(\rho)_{D_1 \ldots D_m} = \tau(z_1)_{D_1} \otimes \ldots \otimes \tau(z_m)_{D_m}. \tag{70}$$

Thus

$$\begin{aligned}
\frac{1}{m} H_\alpha(D^m)_{\bar{\mathcal{M}}_m \circ \ldots \circ \bar{\mathcal{M}}_1(\rho)} &= \frac{1}{m} \sum_{i=1}^m H_\alpha(D_i)_{\tau(z_i)} \\
&\leq \frac{1}{m} \sum_{i=1}^m H(D_i)_{\tau(z_i)} \\
&= \frac{1}{m} \sum_{i=1}^m \bar{g} - f(G_{z_i}) \\
&= \bar{g} - f\left(\mathop{\mathbb{E}}_{z \sim q} G_z \right) \\
&\leq \|\nabla f\|_\infty.
\end{aligned} \tag{71}$$

The first equality holds from (70). The first inequality holds by the monotonicity of Rényi entropyies in α. The second equality holds from (64). The third equality holds because f is an affine function. The last inequality holds from (68). $\qquad\square$

The first term of (66) can be further simplified using the chain rule Theorem 4.3. Note that the Markov chain trivially holds since in this paper, we only consider the case where each system B_i in Theorem 4.3 is empty for $i \in [m]$.

Proposition 4.8. *For $\alpha \in (1, \infty)$,*

$$H_\alpha^\uparrow(Z^m D^m|E)_{\sigma|\Omega}$$
$$\geq \sum_{i=1}^m \inf_{\omega_{i-1}\in\mathrm{S}(R_{i-1}E\tilde{E}_{i-1})} H_\alpha(Z_i D_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} - \frac{\alpha}{\alpha - 1}\log\left(\frac{1}{\Pr_\sigma[\Omega]}\right), \qquad (72)$$

where $\sigma := \mathcal{M}_m \circ \cdots \circ \mathcal{M}_1(\rho)$ and $\tilde{E}_{i-1}$ is a system isomorphic to $R_{i-1}E$ (see Definition 4.4).

Proof. By direct calculation,

$$H_\alpha^\uparrow(Z^m D^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)|\Omega} \geq H_\alpha(Z^m D^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)|\Omega}$$
$$\geq H_\alpha(Z^m D^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)} - \frac{\alpha}{\alpha - 1}\log\left(\frac{1}{\Pr_\sigma[\Omega]}\right). \qquad (73)$$

The first inequality holds $H_\alpha^\uparrow(A|B)_\rho \geq H_\alpha(A|B)_\rho$ for any finite-dimensional Hilbert spaces A, B and bipartite state ρ. The second inequality holds from [28, Lemma B.5].

Next, we apply the chain rule Theorem 4.3 on the first term and have

$$H_\alpha(Z^m D^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)} \geq \sum_{i=1}^m \inf_{\omega_{i-1}\in\mathrm{S}(R_{i-1}E\tilde{E}_{i-1})} H_\alpha(Z_i D_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})}, \qquad (74)$$

where we introduce an purifying system $\tilde{E}_i$ for each i such that $\omega_{i-1} \in \mathrm{S}(R_{i-1}E\tilde{E}_{i-1})$ is a pure state. $\qquad \square$

Now we bound each term in (72). In fact, the bound will be depend on the dimension of D_i. Recall that each D_i is introduce for analysis purposes, and we can choose a sufficient large dimension $d_{D_i} = d_D := \lceil 2^{\|\nabla f\|_\infty}\rceil$ such that (64) can be satisfied for every $i \in [m]$. This implies the following proposition.

Proposition 4.9. *For $\alpha \in (1, 1 + \log(2d_Z d_D + 1))$,*

$$H_\alpha(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} \geq H(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} - (\alpha - 1)(\|\nabla f\|_\infty + \log(2d_Z + 1))^2. \qquad (75)$$

Proof. By [28, Lemma B.9],

$$H_\alpha(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} \geq H(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} - (\alpha - 1)\log^2(2d_Z d_D + 1)$$
$$\geq H(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} - (\alpha - 1)(\|\nabla f\|_\infty + \log(2d_Z + 1))^2. \qquad (76)$$

$\qquad \square$

Combining Proposition 4.8 and Proposition 4.9, we have the following corollary.

Corollary 4.10. *For $\alpha \in (1, 1 + 2/V)$,*

$$H_\alpha^\uparrow(Z^m D^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)|\Omega}$$
$$\geq \sum_{i=1}^m \inf_{\omega_{i-1}\in\mathrm{S}(R_{i-1}E\tilde{E}_{i-1})} H(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} - m\left(\frac{\alpha - 1}{4}\right)V^2 - \frac{\alpha}{\alpha - 1}\log\left(\frac{1}{\Pr_\sigma[\Omega]}\right), \quad (77)$$

where $V = 2(\log(2d_Z + 1) + \|\nabla f\|_\infty)$.

Proof. By direct calculation,

$$H_\alpha^\uparrow(Z^m D^m|E)_{\sigma|\Omega}$$

$$\geq \sum_{i=1}^m \inf_{\omega_{i-1}\in S(R_{i-1}E\tilde{E}_{i-1})} H_\alpha(Z_i D_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\mathrm{Pr}_\sigma[\Omega]}\right)$$

$$\geq \sum_{i=1}^m \inf_{\omega_{i-1}\in S(R_{i-1}E\tilde{E}_{i-1})} H(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} - m\left(\frac{\alpha-1}{4}\right)V^2 - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\mathrm{Pr}_\sigma[\Omega]}\right). \quad (78)$$

The first inequality holds from Proposition 4.8. The second inequality holds from Proposition 4.9. $\square$

Next we simplify the first term in Corollary 4.10.

Proposition 4.11.

$$H(Z_i D_i|E\tilde{E}_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} \geq \bar{g}. \quad (79)$$

Proof. By direct calculation,

$$\begin{aligned}
H(Z_i D_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} &= H(Z_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} + H(D_i|Z_i E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} \\
&= H(Z_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} + H(D_i|Z_i)_{\bar{\mathcal{M}}_i(\omega_{i-1})} \\
&= H(Z_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} + \mathop{\mathbb{E}}_{z\sim r} H(D_i)_{\tau(z)} \\
&= H(Z_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} + \bar{g} - \mathop{\mathbb{E}}_{z\sim r} f(G_z) \\
&= H(Z_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} + \bar{g} - f\left(\mathop{\mathbb{E}}_{z\sim r} G_z\right) \\
&\geq \bar{g}, \quad (80)
\end{aligned}$$

where r is the distribution obtained by taking the marginal of $\bar{\mathcal{M}}_i(\omega_{i-1})$ on Z_i. The first equality holds by the chain rule of von Neumann entropy. The second holds because the marginal state $\bar{\mathcal{M}}_i(\omega_{i-1})_{D_i Z_i} = \sum_z \tau_i(z)_{D_i} \otimes r(z)|z\rangle\langle z|_{Z_i}$. The third holds by the definition of conditional von Neumann entropy and that of r. The fourth holds from (64). The fifth equality holds since f is affine. The inequality holds since by definition, $H(Z_i|E\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} \geq f(\mathbb{E}_{z\sim r} G_z)$, where $r = \bar{\mathcal{M}}_i(\omega_{i-1})_{Z_i}$. $\square$

Combining Proposition 4.6, Proposition 4.7, Corollary 4.10, and Proposition 4.11, we have the following corollary.

Corollary 4.12. *For $\alpha \in (1, 1+2/V)$,*

$$H_\alpha^\uparrow(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} \geq mf(s) - m\left(\frac{\alpha-1}{4}\right)V^2 - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\mathrm{Pr}_\sigma[\Omega]}\right), \quad (81)$$

where $\sigma := \mathcal{M}_m \circ \cdots \circ \mathcal{M}_1(\rho)$, and $s := \frac{1}{m}\sum_{i=1}^m G_{z_i}$ is the score evaluated by taking the average of G_{z_i} from each round $i \in [m]$.

Proof. By direct calculation,

$$\begin{aligned}
H_\alpha^\uparrow(Z^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} &\geq H_\alpha^\uparrow(Z^m D^m|E)_{\mathcal{M}_m\circ\ldots\circ\mathcal{M}_1(\rho)|\Omega} - m\|\nabla f\|_\infty \\
&\geq m\bar{g} - m\left(\frac{\alpha-1}{4}\right)V^2 - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\mathrm{Pr}_\sigma[\Omega]}\right) - m\|\nabla f\|_\infty \\
&\geq mf(s) - m\left(\frac{\alpha-1}{4}\right)V^2 - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\mathrm{Pr}_\sigma[\Omega]}\right). \quad (82)
\end{aligned}$$

The first inequality holds from Proposition 4.6 and Proposition 4.7. The second holds from Corollary 4.10. The third holds because $f(s) \leq \bar{g} - \|\nabla f\|_\infty$. $\square$

Finally, by Proposition 4.5 and Corollary 4.12, we have the following corollary.

Corollary 4.13. *For $\alpha \in (1, 1 + 2/V)$,*

$$H_{\min}^\varepsilon(Z^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)|\Omega} \geq mf(s) - m\left(\frac{\alpha - 1}{4}\right)V^2 - \frac{1}{\alpha - 1}\log\left(\frac{2}{\varepsilon^2 \Pr_\sigma(\Omega)^2}\right). \qquad (83)$$

Note that Corollary 4.13 holds for any $\alpha \in (1, 1 + 2/V)$. Thus we optimize the bound by finding a good α.

Corollary 4.14. *For $V = 2(\log(2d_Z + 1) + \|\nabla f\|_\infty)$,*

$$H_{\min}^\varepsilon(Z^m|E)_{\mathcal{M}_m \circ \ldots \circ \mathcal{M}_1(\rho)|\Omega} \geq mf(s) - \sqrt{m}V\sqrt{\log\frac{2}{\Pr_\sigma[\Omega]^2\varepsilon^2}} \qquad (84)$$

Proof. To optimize the parameter α, we set

$$m\left(\frac{\alpha - 1}{4}\right)V^2 = \frac{1}{\alpha - 1}\log\left(\frac{2}{\varepsilon^2 \Pr_\sigma[\Omega]^2}\right), \qquad (85)$$

which gives

$$\alpha = 1 + \left(\frac{4}{mV^2}\log\left(\frac{2}{\varepsilon^2 \Pr_\sigma[\Omega]^2}\right)\right)^{1/2}. \qquad (86)$$

This implies that

$$m\left(\frac{\alpha - 1}{4}\right)V^2 = \frac{\sqrt{m}V}{2}\sqrt{\log\left(\frac{2}{\varepsilon^2 \Pr_\sigma[\Omega]^2}\right)}. \qquad (87)$$

$\square$

In a spot-checking protocol, the verifier in each round tosses a biased coin $T_i \sim \mathsf{Bernoulli}(\gamma)$ for probability $\gamma \in [0, 1]$. If $T_i = 1$, then the protocol enters a test round, in which case the verifier counts the score. Otherwise, if $T_i = 0$, then the protocol enters a generation round, in which case the verifier does not calculate the score. Effectively, this sets the score to zero.

To see how spot-checking works with our modification, we follow the idea from [28]. In particular, we multiply G by the factor γ, i.e., we consider a new linear operator $G' = \gamma G$. Furthermore, we choose a new min-tradeoff function $f' = \frac{1}{\gamma}f$. With the new choices G' and f', the above analysis establishes the same lower bound on the smooth conditional min-entropy.

The change for spot-checking does seem to allow us to choose an arbitrarily small γ. However, an arbitrarily small γ should not work since taking $\gamma \to 0$ would imply the entropy accumulation protocol does not require any verification. Instead, we want to choose γ sufficiently large such that a *good* device can satisfy Ω with probability asymptotically close to one. For example, in an entropy accumulation protocol from a violation of Bell's inequality, the score is a value in $[\omega_c, \omega_q]$, where ω_c and ω_q are constants describing the best score achievable from a classical and a quantum device respectively. By Hoeffding's inequality, it suffices to take $\gamma = O((\log m)/m)$ for a perfect device to succeed with probability $1 - O(1/m)$.

In the following sections of this paper, we are aiming to prove a lower bound on the conditional min-entropy in an LXEB-based accumulation protocol. In Section 3.4.2, we have shown that the concentration of the collision probability over choices of C allows us to conclude that it suffices to verify samples from $O(\log n)$ circuits for a perfect device to succeed with probability $1 - O(1/n)$ by the same reasoning.

5 A General Device with No Side Information

In this section, we consider the following situation where the device does not share an entanglement with the adversary, but the circuit can be learned. In this setting, we give a protocol in which conditioned on the event Ω of passing $\text{LXEB}_{1+\delta,k}$, the entropy is accumulated, for sufficiently large $\delta = \Omega(1)$. More formally, we aim to show $H_{\min}^\varepsilon(Z_1 \ldots Z_m | C_1 \ldots C_m)_{\rho|\Omega}$ has a lower bound $\Omega(nm)$.

In Section 5.1, we define a problem, called the Long List Quantum Supremacy Verification (LLQSV) problem, which is to determine whether a string s is sampled from a random circuit C, or it is independently sampled according to the uniform distribution. Our hardness assumption, called the Long List Hardness Assumption (LLHA), states that LLQSV is hard for QCAM protocols with access to a quantum advice state. In Section 5.2, we show that if LLHA holds, then any device must generate min-entropy $\Omega(n)$ with probability $\Omega(1)$ over choices of C. Since conditional von Neumann entropy is calculated by taking the expectation, this implies that every device passing $\text{LXEB}_{1+\delta,k}$ must establish a conditional von Neumann entropy lower bound $\Omega(n)$ on the input circuit.

We state our protocol in Figure 1. In particular, the verifier randomly selects $\Omega(\log n)$ test rounds by chossing to verifier each round with probability $\gamma = \Omega((\log n)/m)$, in which the verifier determines whether the device passes $\text{LXEB}_{1+\delta,k}$. By the conditional von Neumann entropy lower bound established in Section 5.1 and the entropy accumulation theorem shown in Section 4, in Section 5.3, we establish an $\Omega(nm)$ lower bound of the smooth conditional min-entropy.

Since LLHA is a seemingly strong assumption, we must justify it. In Section 5.4, we prove that ralative to a random oracle, the assumption that LLQSV is hard for QCAM protocols with quantum advice. This implies that there exists a circuit distribution with which $\text{LXEB}_{1+\delta,k}$ can be used to certify randomness in a sequential process, if the device is given oracle access to the random circuit.

5.1 The Long List Quantum Supremacy Verification Problem

In this section, we formally define the problem LLQSV, as follows.

Problem 4 (Long List Quantum Supremacy Verification (LLQSV)). *Given a list of $M = O(N^3)$ circuit-string tuples $\{(C_i, s_i) : i \in [M]\}$, distinguish the following cases:*

- ***Yes-case:*** *for each $i \in [M]$, $C_i \sim \mathcal{D}$ and s_i is sampled from C_i, i.e., $s_i \sim p_{C_i}$.*

- ***No-case:*** *for each $i \in [M]$, $C_i \sim \mathcal{D}$ and s_i is sampled uniformly (hence independent of C_i).*

We will show that if

$$\text{LLQSV}(\mathcal{D}) \notin \text{QCAMTIME}(2^B n^{O(1)})/\text{q}(2^B n^{O(1)}), \tag{88}$$

then any quantum algorithm that runs in $n^{O(1)}$ time solving $\text{LXEB}_{b,k}$ with probability q, must output $s_1, \ldots, s_k$ of min-entropy at least B with probability $\frac{bq-1}{b-1}$ over choices of C. Thus the parameter B determines the min-entropy lower bound. We prove this assuming what we call the Long List Hardness Assumption (LLHA).

Assumption 5.1 (LLHA$_B(\mathcal{D})$). *There exists no* QCAM *protocol in which the quantum Arthur solves* LLQSV$(\mathcal{D}, V)$ *in time* $2^B n^{O(1)}$ *given access to a quantum advice of length* $2^B n^{O(1)}$. *In other words,* LLQSV$(\mathcal{D}) \notin$ QCAMTIME$(2^B n^{O(1)})/\mathsf{q}(2^B n^{O(1)})$.

5.2 LLHA implies Certified Randomness

In this section, we show that LLHA$_B(\mathcal{D})$ implies that any device passing LXEB$_{b,k}$ must output samples of min-entropy $\Omega(n)$ given $C \sim \mathcal{D}$. Our reduction relies on the Goldwasser-Sipser protocol for approximate counting [32], explained as follows. Recall that the instance consists of M tuples (C_i, s_i) for $i \in [M]$, where $C_i \sim \mathcal{D}$ and s_i is either sampled from p_{C_i} or from the uniform distribution $\mathcal{U}$. Let V be a quantum-classical Merlin-Arthur protocol running in time $2^B n^{O(1)}$ such that V accepts at least κ tuples for a yes instance and accepts at most $(1 - \Omega(\varepsilon))\kappa$ tuples, both with probability $1 - 2^{-\Omega(n)}$. Then this immediately yields a quantum-classical Arthur-Merlin protocol:

Input: Both Arthur and Merlin receives an instance $(C_1, s_1), \ldots, (C_M, s_M)$.

1. Arthur samples a random hash function $h : [M] \to [R]$ for R determined later.

2. Merlin sends $i \in [M]$ and a proof π.

3. Arthur accepts if V accepts (C_i, s_i) with witness π and $h(i) = y$.

The gap of the protocol is $\Omega(\varepsilon^2/\alpha)$, proved as follows.

Lemma 5.2. *For real number $\alpha > 1$ and integer κ, there exists an Arthur-Merlin protocol which on input the description of a set S, determines $\alpha\kappa \geq |S| \geq \kappa$ or $|S| \leq (1 - \varepsilon)\kappa$ with gap at least $\frac{\varepsilon^2}{4\alpha}$ using a hash function of range size $R = 2\alpha\kappa/\varepsilon$.*

Proof. It suffices to get an tight upper bound and a lower bound of the probability

$$\Pr_{h,y}[\exists x \in S, h(x) = y] \tag{89}$$

for a random hash function h of range size R. By union bound, an upper bound is $\sum_{x \in S} \Pr_{h,y}[h(x) = y] = \frac{|S|}{R}$. For a lower bound, by the inclusion-exclusion principle[7]

$$\begin{aligned}
\Pr_{h,y}[\exists x \in S, h(x) = y] &\geq \frac{|S|}{R} - \sum_{x \leq x', x, x' \in S} \Pr_{h,y}[h(x) = h(x') = y] \\
&= \frac{|S|}{R} - \binom{|S|}{2} \frac{1}{R^2} \\
&= \frac{|S|}{R}\left(1 - \frac{|S| - 1}{2R}\right) > \frac{|S|}{R}\left(1 - \frac{|S|}{R}\right)
\end{aligned} \tag{90}$$

In the yes case, $\alpha\kappa \geq |S| \geq \kappa$ and $R = 2\alpha\kappa/\varepsilon$, and

$$\begin{aligned}
\Pr_{h,y}[\exists x \in S, h(x) = y] &\geq \frac{|S|}{R}\left(1 - \frac{|S|}{R}\right) \\
&\geq \frac{\kappa}{R}\left(1 - \frac{\alpha\kappa}{R}\right) \\
&\geq \frac{\kappa}{R}\left(1 - \frac{\varepsilon}{2}\right),
\end{aligned} \tag{91}$$

---

[7]The principle states that $\Pr[\bigvee_i E_i] \geq \sum_i \Pr[E_i] - \sum_{i<j} \Pr[E_i \wedge E_j]$.

whereas in the no case, $|S| \leq (1 - \varepsilon)\kappa$, and

$$\Pr_{h,y}[\exists x \in S, h(x) = y] \leq \frac{|S|}{R} \leq \frac{\kappa}{R}(1 - \varepsilon). \tag{92}$$

The gap is at least $\frac{\kappa\varepsilon}{2R} = \frac{\varepsilon^2}{4\alpha}$. $\qquad\square$

Assume that there is a quantum device $\mathcal{A}$ which solves $\text{LXEB}_{b,k}$ with probability q over choices of C, and outputs k tuples $(s_1, \ldots, s_k)$ of min-entropy at most $B/2$ with probability p such that p and q satisfy

$$p > \frac{b}{b-1}(1 - q) + \varepsilon. \tag{93}$$

For breaking $\text{LLHA}_B(\mathcal{D})$, we consider the following random variable $Y_\tau(C, s)$ for $\tau \in [0, 1]$:

$$Y_\tau(C, s) := \begin{cases} 1 & \text{if } \exists d = (z_1, \ldots, z_k), \Pr[\mathcal{A}(C) = d] \geq \frac{\tau}{2^{B/2}} \text{ and } s \in \mathcal{A}(C) \\ 0 & \text{otherwise.} \end{cases} \tag{94}$$

Here $s \in \mathcal{A}(C)$ means that the samples $s \in \{z_1, \ldots, z_k\}$ for samples $(z_1, \ldots, z_k) \sim \mathcal{A}(C)$. Define

$$\mu_1(\tau) = \mathbb{E}_{C \sim \mathcal{D}, s \sim p_C}[Y_\tau(C, s)], \qquad \mu_0(\tau) = \mathbb{E}_{C \sim \mathcal{D}, s \sim \mathcal{U}}[Y_\tau(C, s)], \tag{95}$$

where $\mathcal{U}$ is the uniform distribution over $\{0, 1\}^n$.

Let $p(\tau)$ be the probability that $\mathcal{A}(C)$'s maximum probability is at least $\tau/2^{B/2}$ for $C \sim \mathcal{D}$, i.e.,

$$p(\tau) := \Pr_{C \sim \mathcal{D}}\left[\max_d \Pr[\mathcal{A}(C) = d] \geq \frac{\tau}{2^{B/2}}\right]. \tag{96}$$

The following lemma shows that the ratio $\mu_1(\tau)/\mu_0(\tau)$ is bounded by $b \cdot (p(\tau) + q - 1)/p(\tau)$.

Lemma 5.3. *For $\tau \in [0, 1]$, let Y_τ be defined as in (94), $\mu_1(\tau), \mu_0(\tau)$ as in (95) and $p(\tau)$ as in (96). Then*

$$\frac{\mu_1(\tau)}{\mu_0(\tau)} \geq b \cdot \frac{p(\tau) + q - 1}{p(\tau)}. \tag{97}$$

Proof. Note that in each case, we are bounding

$$\mathbb{E}_{C \sim \mathcal{D}, s}[Y_\tau(C, s)] = \Pr_{C \sim \mathcal{D}, (z_1, \ldots, z_k) \sim \mathcal{A}(C), s}\left[\exists d, \Pr[\mathcal{A}(C) = d] \geq \frac{\tau}{2^{B/2}} \wedge s \in \{z_1, \ldots, z_k\}\right], \tag{98}$$

where $s \sim p_C$ in the yes case, or $s \sim \mathcal{U}$ in the no case. Define

$$G_\tau(C) := \mathbb{1}\left[\max_d \Pr[\mathcal{A}(C) = d] \geq \frac{\tau}{2^{B/2}}\right]. \tag{99}$$

By (96), $p(\tau) = \mathbb{E}_{C \sim \mathcal{D}}[G_\tau(C)]$.

- For the yes case,

$$\begin{aligned} \mu_1(\tau) &= \mathbb{E}_{C \sim \mathcal{D}, s \sim p_C}[Y_\tau(C, s)] \\ &= \Pr_{C \sim \mathcal{D}, O \sim \mathcal{A}(C), s \sim p_C}[G_\tau(C) \wedge s \in O] \\ &\geq \Pr_{C \sim \mathcal{D}, O \sim \mathcal{A}(C), s \sim p_C}[G_\tau(C) \wedge s \in O \wedge V(C, O)], \end{aligned} \tag{100}$$

where $V(C,O) = 1$ if $\text{LXEB}_{b,k}$ accepts $O = (z_1, \ldots, z_k)$, i.e.,

$$\sum_{i=1}^{k} p_C(z_i) \geq \frac{bk}{N} \tag{101}$$

and 0 otherwise. By union bound,

$$\Pr_{C \sim \mathcal{D}, O \sim \mathcal{A}(C), s \sim p_C}[G_\tau(C) \wedge V(C,O) = 1] \geq \Pr_{C \sim \mathcal{D}}[G_\tau(C)] + \Pr_{C \sim \mathcal{D}, O \sim \mathcal{A}(C)}[V(C,O)] - 1$$

$$= p(\tau) + q - 1. \tag{102}$$

Furthermore, the conditional probability

$$\Pr_{C \sim \mathcal{D}, O \sim \mathcal{A}(C), s \sim p_C}[s \in O | G_\tau(C) \wedge V(C,O)] \geq \frac{bk}{N} \tag{103}$$

since if $V(C,O) = 1$, the probability that $\Pr_{s \sim p_C}[s \in O] = \sum_{z \in O} p_C(z) \geq bk/N$ by (101). Combining (102) and (103),

$$\mu_1(\tau) = \frac{bk}{N}(p(\tau) + q - 1). \tag{104}$$

- For the no case, since s is independently sampled,

$$\mu_0(\tau) = \Pr_{C \sim \mathcal{D}, O \sim \mathcal{A}(C), s \sim \mathcal{U}}[G_\tau(C) \wedge s \in O]$$

$$= \frac{k}{N} \Pr_{C \sim \mathcal{D}}[G_\tau(C)] = \frac{k}{N} \cdot p(\tau). \tag{105}$$

By (104) and (105), we conclude the proof. □

Furthermore, we show that the lower bound is monotonically non-increasing.

Lemma 5.4. *The ratio $(p(\tau) + q - 1)/p(\tau)$ is monotonically non-increasing for $\tau \in [0,1]$.*

Proof. For $1 \geq \alpha \geq \beta \geq 0$, $p(\alpha) \leq p(\beta)$, and

$$\frac{p(\beta) + q - 1}{p(\alpha) + q - 1} \geq \frac{p(\beta)}{p(\alpha)} \tag{106}$$

This implies that $\frac{p(\tau) + q - 1}{p(\tau)}$ is monotonically non-increasing for $\tau \in [0,1]$. □

Lemma 5.3 and Lemma 5.4 imply that

$$\frac{\mu_1(\tau)}{\mu_0(\tau)} \geq \frac{\mu_1(1)}{\mu_0(1)} \geq b \cdot \frac{p + q - 1}{p} \geq 1 + \varepsilon. \tag{107}$$

While this seems to give us a sufficient condition for applying the Goldwasser-Sipser protocol, a caveat is that we do not know how to verify if Y_τ accepts (C, s) (in particular, Y_1) in time $2^B n^{O(1)}$. The reason is that the condition that $\mathcal{A}(C)$ outputs a string d with probability greater than $\tau/2^B$ cannot be efficiently verified, even when a witness d is given. The next step is to show that for sufficiently large T, there exists $j \in [T]$ such that for $\tau = 1/2 + j/T$, $\mu_1(\tau) \geq (1 + \varepsilon/2)\mu_0(\tau - 1/T)$.

Lemma 5.5. *Let μ_1 and μ_0 be defined as in (95). Assume that (93) holds. Then for $T \geq \frac{8}{\varepsilon}\log(\frac{N}{\varepsilon})$, there exists $j \in [T]$ such that*

$$\mu_1(1/2 + j/T) \geq (1 + \varepsilon/2)\mu_0(1/2 + (j-1)/T). \tag{108}$$

Proof. We prove the lemma by contrapositive. Suppose that for every $j \in [T]$,

$$\mu_1(1/2 + j/T) < (1 + \varepsilon/2)\mu_0(1/2 + (j-1)/T). \tag{109}$$

Then expanding the ratio into a telescoping product,

$$\frac{\mu_1(1/2)}{\mu_1(1)} = \prod_{j=1}^{T} \frac{\mu_1(1/2 + j/T)}{\mu_1(1/2 + (j+1)/T)}$$

$$\geq (1 + \varepsilon/2)^{-T} \prod_{j=1}^{T} \frac{\mu_1(1/2 + j/T)}{\mu_0(1/2 + j/T)}$$

$$\geq \left(\frac{1 + \varepsilon}{1 + \varepsilon/2}\right)^{T}$$

$$\geq (1 + \varepsilon/4)^{T}. \tag{110}$$

The first inequality holds by (109). The second holds by (107). The third holds by the inequality $1 + \varepsilon - (1 + \varepsilon/2)(1 + \varepsilon/4) = \varepsilon/4 \cdot (1 - \varepsilon/2) \geq 0$ for $\varepsilon \leq 2$. Taking $T \geq \frac{8}{\varepsilon}\log(n/\varepsilon)$,

$$\mu_1(1/2) > (1 + \varepsilon/4)^{T} \cdot \mu_1(1)$$

$$\geq \frac{k}{N} \cdot \varepsilon(1 + \varepsilon/4)^{T}$$

$$\geq \frac{k}{N} \cdot \varepsilon e^{\varepsilon T/8}$$

$$\geq k. \tag{111}$$

This contradicts the fact that $\mu_1(1/2) \leq 1$. $\qquad\square$

With the gap, we can consider the following Merlin-Arthur protocol which verifies that $s \sim p_C$ in time $2^B \cdot T^2 \cdot n^{O(1)}$:

Both Arthur and Merlin are given access to a circuit C and a string $s \in \{0, 1\}^n$.

1. Merlin sends $d = (z_1, \ldots, z_k)$.

2. Arthur gets $K + 1$ samples $d_1, \ldots, d_K, O \sim \mathcal{A}(C)$ for integer K determined later. Arthur accepts if

$$\frac{1}{K}|\{\ell : d_\ell = d\}| \geq \left(\tau - \frac{1}{2T}\right)2^{-B/2}, \tag{112}$$

and $s \in O$, and rejects otherwise.

This quantum-classical Merlin-Arthur protocol solves the problem that either (C, s) is accepted by Y_τ, or rejected by $Y_{\tau - 1/T}$.

38

Lemma 5.6. *For $\tau \in [1/2, 1]$, $\eta = O(1/N^2)$ and $K \geq 4T^2 2^B n$, the above process satisfies the following conditions:*

1. *If Y_τ accepts (C, s), then Arthur accepts with probability $1 - \eta$, and*

2. *if $Y_{\tau - 1/T}$ rejects (C, s), then Arthur rejects with probability $1 - \eta$.*

Proof. If Y_τ accepts (C, s), then there exists $d = (z_1, \ldots, z_k)$ such that $\Pr[\mathcal{A}(C) = d] \geq \tau/2^B$ and $s \in \{z_1, \ldots, z_k\}$. By Hoeffding's inequality, the fraction $\tilde{\nu}$ in (112) no more than $(\tau - \frac{1}{2T})2^{-B/2}$ occurs with probability at most

$$\Pr\left[|\tilde{\nu} - \Pr[\mathcal{A}(C) = d]| > \frac{1}{2T}2^{-B/2}\right] \leq 2e^{-2\frac{K}{4T^2 2^B}} \leq 2e^{-2n}. \tag{113}$$

If $Y_{\tau - 1/T}$ rejects (C, s), then for every d such that s is contained in d, $\Pr[\mathcal{A}(C) = d] < (\tau - 1/T)/2^{B/2}$. Again, by Hoeffding's inequality, (112) occurs with probability at most $2e^{-2n}$. $\qquad \square$

For $M \geq N^3$, the quantum-classical Merlin-Arthur protocol accepts more tuples in an yes instance than a no instance, with overwhelming probability.

Lemma 5.7. *For $M \geq N^3$ and $\eta' = 2^{-\Omega(N)}$, there exists an integer $\kappa \in [M]$ such that with probability at least $1 - \eta'$, Arthur accepts at least κ tuples in an yes instance and accept at most $\kappa' = (1 - \varepsilon/5 + O(\varepsilon^2))\kappa$ tuples in a no instance.*

Proof. Recall that $\mu_1(\tau) = \mathbb{E}_{C \sim \mathcal{D}, s \sim p_C}[Y_\tau(C, s)]$. Since each tuple is independently sampled both in the yes instance and in the no instance, by Lemma 5.6, Authur accepts each sample with probability at most $\mu_0(\tau) + \eta$. Thus by Hoeffding's inequality, for $\kappa' = (\mu_0(\tau) + \eta)(1 + \varepsilon/8)M$,

$$\Pr_{C_1, \ldots, C_M \sim \mathcal{D}, s_1, \ldots, s_M \sim \mathcal{U}}[\text{Arthur accepts more than } \kappa' \text{ tuples}] \leq 2e^{-M\varepsilon^2(\mu_0(\tau) + \eta)^2/32}$$

$$= 2e^{-\Omega(M\varepsilon^2 k^2 p^2/N^2)}$$

$$\leq 2e^{-\Omega(M\varepsilon^4 k^2/N^2)}, \tag{114}$$

since by (93), $\mu_0(\tau) = p(\tau)k/N \geq pk/N \geq \varepsilon k/N$. Taking $M \geq N^3$, the upper bound is $2e^{-\Omega(N)}$.

Similarly, for $\kappa = (\mu_1(\tau) - \eta)(1 - \varepsilon/8)M$,

$$\Pr_{C_1, \ldots, C_M \sim \mathcal{D}, s_i \sim p_{C_i}}[\text{Arthur accepts fewer than } \kappa \text{ tuples}] \leq 2e^{-M\varepsilon^2(\mu_1(\tau) - \eta)^2/32}$$

$$\leq 2e^{-\Omega(M\varepsilon^2 p^2 k^2/N^2)}, \tag{115}$$

since $\eta = O(1/N^2)$ and $\mu_1(\tau) - \eta = \Omega(\mu_1(\tau)) = \Omega(\mu_0(\tau)) = \Omega(pk/N)$.

It remains to give an upper bound of the ratio: Since $\eta = o(\varepsilon)$,

$$\frac{\kappa'}{\kappa} \leq \frac{\mu_0(\tau) + \eta}{\mu_1(\tau) - \eta} \frac{1 + \varepsilon/8}{1 - \varepsilon/8}$$

$$\leq \frac{\mu_0(\tau) + \eta}{\mu_1(\tau) - \eta} \frac{1}{1 - \varepsilon/4}$$

$$\leq \frac{1}{1 + \varepsilon/4 - O(\eta)}$$

$$\leq \frac{1}{1 + \varepsilon/5}$$

$$\leq 1 - \varepsilon/5 + O(\varepsilon^2). \tag{116}$$

$\square$

We have proved all the statements needed for proving our main theorem in this section. Now we describe the quantum-classical Arthur-Merlin protocol.

Both Merlin and Arthur are given access to $(C_1, s_1), \ldots, (C_M, s_M)$ and advice strings including integers T, $j \in [T]$ and R.

1. Arthur chooses a random hash function $h : [M] \to [R]$ and y uniformly from $[R]$.

2. Merlin sends i and $d = (z_1, \ldots, z_k)$.

3. For $K \geq 4T^2 2^B n$, Arthur takes $K + 1$ samples $d_1, \ldots, d_K, O \sim \mathcal{A}(C_i)$. He accepts if

   (a) $\frac{1}{K}|\{\ell : d_\ell = d\}| \geq \left(\tau - \frac{1}{2T}\right)2^{-B/2}$, where $\tau = 1/2 + j/T$,

   (b) $s_i \in O$, and

   (c) $h(i) = y$.

We prove the main theorem in this section.

Theorem 5.8. *If there exists a device $\mathcal{A}$ which runs in quantum polynomial time and satisfies (93), then there is a quantum-classical Arthur-Merlin protocol which on input an $O(n)$-bit advice string, solves $\mathrm{LLQSV}_B(\mathcal{D})$. In other words, $\mathrm{LLQSV}_B(\mathcal{D}) \in \mathsf{QCAMTIME}(2^B n^{O(1)})/O(n)$.*

Proof. We show that the above protocol solves $\mathrm{LLQSV}_B(\mathcal{D})$ with a constant gap. By Lemma 5.7, $\kappa' \leq (1-\varepsilon/6)\kappa$ with probability $1-2^{-\Omega(N)}$. Then by Lemma 5.2, for $R = 12\alpha\kappa/\varepsilon$, since $\alpha = 1+O(\varepsilon)$, the gap is $\Omega(\varepsilon)$. Thus running an $(1/\varepsilon)^{O(1)}$-fold parallel repetition of the above protocol yields a constant gap. For the length of the advice string, since $1/\varepsilon = n^{O(1)}$, $T = n^{O(1)}$ and $R \leq M$ and it suffices to choose $M = N^3$, the total length is $O(n)$. $\square$

As a corollary, if $\mathrm{LLHA}_B(\mathcal{D})$ is true, then

$$p \leq \frac{b}{b-1}(1-q) + n^{-\omega(1)}. \tag{117}$$

Corollary 5.9. *For integer n, assume that $\mathrm{LLHA}_B(\mathcal{D})$ holds for distribution $\mathcal{D}$ over circuit acting on n qubits. Then for every device $\mathcal{A}$ passes $\mathrm{LXEB}_{b,k}$ with probability q over choices of $C \sim \mathcal{D}$,*

$$\Pr_{C\sim\mathcal{D}}[H_{\min}(\mathcal{A}(C)) \geq B/2] \geq \frac{bq-1}{b-1} - n^{-\omega(1)}. \tag{118}$$

Since min-entropy is the smallest quantity in the family of Rényi entropies, we establish a lower bound on the von Neumann entropy.

Theorem 5.10. *For integer n, assume that $\mathrm{LLHA}_B(\mathcal{D})$ holds for distribution $\mathcal{D}$ over circuits acting on n qubits. Then for any device which on input a circuit C, outputs a classical state ψ over $\{0,1\}^{nk}$ solving $\mathrm{LXEB}_{b,k}$ with probability q, it holds that*

$$H(Z|C)_\psi \geq \frac{B}{2}\left(\frac{bq-1}{b-1} - n^{-\omega(1)}\right). \tag{119}$$

40

Proof. By Corollary 5.9, since min-entropy is the smallest quantity in the family of Rényi entropies,

$$\Pr_{C \sim \mathcal{D}} \left[H(Z)_{\psi^C} \geq B/2 \right] \geq \frac{bq-1}{b-1} - n^{-\omega(1)}$$

where ψ^C is the distribution output by the device conditioned on C. Since for every C, the von Neumann entropy is non-negative, by definition of conditional von Neumann entropy, we conclude the proof. □

5.3 Entropy Accumulation

To apply the EAT we showed in Section 4, we must give a min-tradeoff function f such that for devices outputting a classical state ψ and solving $\text{LXEB}_{b,k}$ with probability q, $H(Z|C)_\psi \geq f(q)$. From Theorem 5.10, the affine function can be defined as

$$f(q) := \frac{bq-1}{b-1} \frac{B}{2} - c, \tag{120}$$

for $c = n^{-\omega(1)}$ independent of q.

For spot checking, by Lemma 3.18, we change the circuit $\Omega(\log n)$ times so that a perfect device can pass the verification with overwhelming probability. With the parameters, we are ready to give our protocol in Figure 1.

We prove that the entropy accumulates. In the following theorem, let $D = D_1 \dots D_m$ denote the responses received from the device, $C = C_1 \dots C_m$ denote the circuit sent from the device, and $T = T_1 \dots T_m$ the flags indicating whether a test round is executed (see Figure 1).

Theorem 5.11. *Assume that $\text{LLHA}_B(\mathcal{D})$ holds for distribution $\mathcal{D}$. Conditioned on the event Ω that the verifier does not abort in the protocol in Figure 1,*

$$H_{\min}^{\varepsilon}(D|CT)_{\rho|\Omega} \geq n\left((0.99 - 0.01/\delta)\beta m - O(\sqrt{m}) \cdot \sqrt{\log \frac{2}{p^2 \varepsilon^2}} \right), \tag{123}$$

where $\beta = \frac{B}{2n}$, ρ is the output state, and p is the probability of non-aborting. Furthermore, there exists a device which solves $\text{LXEB}_{2,k}$ for $k = O(n^2)$ with probability $1 - o(1)$.

Proof. Let f be as defined in (120). To apply Corollary 4.14, we set $d_Z = N$ and $\|\nabla f\|_\infty = \frac{b}{b-1}\frac{B}{2}$, and therefore $V \leq (n+1) + \frac{b}{b-1}\frac{B}{2}$. For $b = 1 + \delta$ and $q \geq 0.99$,

$$\frac{bq}{b-1} \geq \frac{(1+\delta)0.99 - 1}{\delta} \geq 0.99 - 0.01/\delta. \tag{124}$$

This implies a lower bound

$$(0.99 - 0.01/\delta)Bm/2 - \sqrt{m}((n+1) + (1/\delta + 1)B/2)\sqrt{\frac{2}{p^2 \varepsilon^2}}$$

$$= n\left((0.99 - 0.01/\delta)\beta m - \sqrt{m} \cdot (1 + 1/n + (1/\delta + 1)\beta)\sqrt{\frac{2}{p^2 \varepsilon^2}} \right)$$

$$\geq n\left((0.99 - 0.01/\delta)\beta m - O(\sqrt{m}) \cdot \sqrt{\frac{2}{p^2 \varepsilon^2}} \right), \tag{125}$$

where $\beta = \frac{B}{2n}$. □

Input: security parameter n, a distribution $\mathcal{D}$ over circuits on n qubits, the threshold constant $b \in [1, 2]$, the number of samples $k = O(n^2)$ per iteration, the number of rounds m, and the fraction $\gamma = O((\log n)/m)$ of circuit updates.

The protocol:

1. For $i = 1, \ldots, m$, run the following steps:

   (a) The verifier samples $T_i \sim \mathsf{Bernoulli}(\gamma)$. If $T_{i-1} = 1$ (when $i > 1$) or $i = 1$, the device samples $C_i \sim \mathcal{D}$. Otherwise, the device sets $C_i = C_{i-1}$. The verifier sends C_i to the device (and keeps T_i secret).

   (b) The device returns k samples $d_i = (z_1, \ldots, z_k)$.

   (c) If $T_i = 1$, the verifier sets

   $$W_i = \mathbb{1}\left[\frac{1}{k}\sum_{i=1}^{k} p_C(z_i) \geq \frac{b}{N} \wedge E_i\right]. \tag{121}$$

   where $E_i = 0$ if there exist distinct $\ell, \ell' \in \{j : C_j = C_i\}$ such that the samples $d_\ell = (z_{\ell 1}, \ldots, z_{\ell k})$ and $d_{\ell'} = (z_{\ell' 1}, \ldots, z_{\ell' k})$ are not all distinct. (This check is used to prevent the device repeats responses for any two rounds using the same challenge circuit.) If $T_i = 0$, the verifier sets $W_i = \perp$.

2. Let $t = |\{i : T_i = 1\}|$ be the number of test rounds. The verifier computes

$$W = \sum_{i:T_i=1} W_i. \tag{122}$$

If $W \geq 0.99t$, then the verifier accepts and outputs $(d_1, \ldots, d_m)$ to the quantum-proof randomness extractor.

Figure 1: The entropy accumulation protocol based on LLHA.

5.4 LLHA Relative to a Random Oracle

Now, we turn our attention to justifying Assumption 5.1 relative to a random oracle. Given access to a random function $f : \{0,1\}^n \to \{+1, -1\}$, there is a simple algorithm which samples from the Fourier spectrum:

$$|0^n\rangle \xrightarrow{H^{\otimes n}} \sum_{x \in \{0,1\}^n} |x\rangle \xrightarrow{O_f} \sum_{x \in \{0,1\}^n} f(x)|x\rangle \xrightarrow{H^{\otimes n}} \sum_{y \in \{0,1\}^n} \hat{f}(x)|x\rangle, \tag{126}$$

where $\hat{f}(x) := \frac{1}{N} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} f(y)$ is the Fourier coefficient of f. Given oracle access to M random Boolean functions and the samples, we defined a black-box version of the LLQSV problem. For concreteness, the algorithm is given access to a unitary $\mathcal{O} : |i, x\rangle \mapsto f_i(x)|i, x\rangle$, where i ranges from 1 to M and $f_1, \ldots, f_M$ are random functions sampled from the uniform distribution $\mathcal{F}_n$ over n-bit Boolean functions. The black-box version of LLQSV is formally defined as follows.

Problem 5 (Black-box LLQSV). *For $M = 2^{O(n)}$, given access to strings $s_1, \ldots, s_M \in \{0,1\}^n$ and to functions $f_1, \ldots, f_M \sim \mathcal{F}_n$ through the unitary $\mathcal{O} : |i, x\rangle \mapsto f_i(x)|i, x\rangle$, determine whether, in the yes case, $s_i \sim |\hat{f}_i|^2$, or, in the no case, each s_i is sampled from the uniform distribution (hence independent of f_i).*

The proof is organized in the following steps. We prove LLQSV is not in QIP[2], the class of problems which admits a two-message quantum interactive proof system, relative to a random oracle. The proof is closely related to the black-box LLQSV lower bound for BQP by Bassirian, Bouland, Fefferman, Gunn, and Tal [14], which also uses a hybrid argument [17], but here we strengthen the hardness to QIP[2]. Thus the problem is not in QCAM.

However, the hybrid argument does not immediately lead to hardness for QCAM/qpoly. By Aaronson and Drucker's exchange theorem, QCAM/qpoly $\subseteq$ QMA/poly, and thus it suffices to show hardness for the latter. We then give a query lower bound using the polynomial method, and appeal to the strong direct product theorem by Sherstov [58].

5.4.1 Two-message quantum interactive proofs

To show LLHA holds relative to $\mathcal{O}$, we first provide intuition. If the algorithm is not given access to $\mathcal{O}$, then for both cases, $s_1, \ldots, s_M$ are uniform. Thus, alternatively, we can view $\mathcal{O}$ as a distribution which may or may not depend on uniform $s_1, \ldots, s_M$. This fact is stated in the following lemma.

Lemma 5.12. *Let $\mathcal{F}_n$ be the uniform distribution over n-bit Boolean functions $\{0,1\}^n \to \{+1, -1\}$ and $\mathcal{U}_n$ be the uniform distribution over n-bit strings. The following two sampling processes are equivalent, i.e. their output distributions are identical:*

- *Sample $f \sim \mathcal{F}_n$ and then $s \sim |\hat{f}|^2$. Output (f, s).*

- *Sample $s \sim \mathcal{U}_n$ and then $f \sim \mathcal{G}_{n,s}$, where $\mathcal{G}_{n,s}(f) = \mathcal{F}_n(f) \cdot |\hat{f}(s)|^2 \cdot N$. Output (f, s).*

Proof. Let the probability density of the first distribution be $\mu(f, s) = \mathcal{F}_n(f) \cdot |\hat{f}(s)|^2$. The marginal

$$\mu(s) = \sum_f \mathcal{F}_n(f) \cdot |\hat{f}(s)|^2$$

$$= \mathbb{E}_f[|\hat{f}(s)|^2]$$

$$= \frac{1}{N}. \tag{127}$$

It remains to calculate $\mu(f|s)$:

$$\mu(f|s) = \frac{\mu(f, s)}{\mu(s)}$$
$$= \mathcal{F}_n(f) \cdot |\hat{f}(s)|^2 \cdot N. \tag{128}$$

$\square$

We then define the following promise problem, called Boolean Function Bias Detection (BFBD).

Definition 5.13 (Boolean Function Bias Detection (BFBD)). *The Boolean Function Bias Detection problem is to distinguish between the follow cases:*

- **Yes-case**: *For each $i \in [M]$, sample $f \sim \mathcal{G}_n$, where $\mathcal{G}_n$ is the probability distribution of density $\mathcal{G}_n(f) := N(1 - 2\Delta(f))^2 \mathcal{F}_n(f)$, where $\Delta(f)$ is the fraction of elements that evaluates to -1, i.e., $\Delta(f) := \frac{1}{N}|\{x : f(x) = -1\}|$.*

- **No-case**: *For each $i \in [M]$, sample the distribution $f \sim \mathcal{F}_n$.*

For function f, we will also call $\Delta(f)$ the distance of f. We now prove that BFBD reduces to LLQSV, and thus it suffices to establish a lower bound for BFBD.

Lemma 5.14. BFBD *reduces to* LLQSV.

Proof. The reduction works as follows: Sample $s_1, \ldots, s_M$ uniformly and simulate the oracle $\mathcal{Q} : |i, x\rangle \mapsto (-1)^{s_i \cdot x}|i, x\rangle$. Run the protocol for LLQSV using the oracle $\mathcal{QO}$, and effectively the protocol is given oracle access to the function $g_i = \chi_{s_i} \cdot f$, where $\chi_{s_i}(x) := (-1)^{s_i \cdot x}$ for each $i \in [M]$. To see why the reduction works, it suffices to show that each oracle distributed identically as the associated case for LLQSV. In the no case, the distribution of $\chi_s \cdot f$ for uniform s and f is distribubed uniformly and independently of s. In the yes case, let $g = \chi_s \cdot f$: the density μ of g can be calculated as follows:

$$\mu(g|s) = N(1 - 2\Delta(g \cdot \chi_s))^2 \cdot \mathcal{F}_n(g \cdot \chi_s)$$
$$= N(1 - 2\Delta(g \cdot \chi_s))^2 \cdot \mathcal{F}_n(g). \tag{129}$$

The second equality holds since $\mathcal{F}_n$ is uniform. It remains to show that $\hat{g}(s) = 1 - 2\Delta(g \cdot \chi_s)$:

$$\hat{g}(s) = \frac{1}{N} \sum_x \chi_s(x) f(x)$$
$$= \frac{1}{N} \sum_{x : \chi_s(x) f(x) = 1} \chi_s(x) f(x) - \frac{1}{N} \sum_{x : \chi_s(x) f(x) = -1} \chi_s(x) f(x)$$
$$= 1 - 2\Delta(g \cdot \chi_s). \tag{130}$$

$\square$

Though our purpose is to show LLQSV, or equivalently BFBD, is not in QCAM, here we prove a stronger result: BFBD is not in QIP[2]. First, we observe that each distribution can be sampled by choosing the distance Δ first, and then sampling a function f according to the uniform distribution among all functions of distance Δ. More formally, BFBD is equivalent to the following problem:

- **No-case**: For each $i \in [M]$, sample $D_i \sim \mathsf{Binomial}(N, 1/2)$, the binomial distribution with N trials and bias $1/2$, and set $\Delta_i = D_i/N$, i.e., the density is

$$p_0(\Delta_i) = \binom{N}{N\Delta_i} 2^{-N}. \tag{131}$$

Then sample $f_i \sim \mathcal{H}_{\Delta_i}$, the uniform distribution over all functions g of distance $\Delta(g) = \Delta_i$.

- **Yes-case**: For each $i \in [M]$, sample Δ_i according to the distribution p_1 of density

$$p_1(\Delta_i) := p_0(\Delta_i) \cdot N(1 - 2\Delta_i)^2. \tag{132}$$

Then sample $f_i \sim \mathcal{H}_{\Delta_i}$.

Then we show that for each distribution, Δ is concentrated around $1/2$, this allows us to only consider the event that Δ is sufficiently close to $1/2$.

Lemma 5.15. *For $b \in \{0, 1\}$ and $\alpha > 0$,*

$$\Pr_{\Delta_1,\dots,\Delta_M \sim p_b}\left[\exists i, |\Delta_i - 1/2| \geq \frac{\alpha}{\sqrt{N}}\right] \leq 2MN e^{-2\alpha^2}. \tag{133}$$

Proof. In the no case, since each element of f is a fair coin, by Hoeffding's inequality and union bound,

$$\Pr_{\Delta_1,\dots,\Delta_M \sim p_0}\left[\exists i, |\Delta_i - 1/2| \geq \frac{\alpha}{\sqrt{N}}\right] \leq 2M e^{-2\alpha^2}. \tag{134}$$

In the yes case,

$$\Pr_{\Delta_1,\dots,\Delta_M \sim p_1}\left[\exists i, |\Delta_i - 1/2| \geq \frac{\alpha}{\sqrt{N}}\right] \leq M \Pr_{\Delta \sim p_1}\left[|\Delta - 1/2| \geq \frac{\alpha}{\sqrt{N}}\right]$$

$$\leq 2MN e^{-2\alpha^2}. \tag{135}$$

The second inequality holds since for $p_1(\Delta) \leq N \cdot p_0(\Delta)$ and by Hoeffding's inequality. $\qquad \square$

For each distribution, consider the event Ω that $|\Delta - 1/2| \leq t$, where $t = ((\ln MN^2)/N)^{1/2} = O((n/N)^{1/2})$. By Lemma 5.15, conditioned on Ω, the gap decreases by at most $O(1/N)$. Then for $(\Delta_1, \dots, \Delta_M) \in \Omega$, we are dealing with the function distributed from H_{Δ_i} for each i. Since $\mathcal{H}_\Delta$ can be obtained by flipping $|\Delta - 1/2|N$ bits of $f \sim \mathcal{H}_{1/2}$, we can use BBBV to give a query lower bound.

Before we give the proof, let us characterize the behavior of a two-message quantum interactive proof system for distinguishing two distributions $\mathcal{D}_1$ and $\mathcal{D}_0$. In a two-message protocol, the verifier first makes T_1 queries to f either sampled from $\mathcal{D}_1$ or $\mathcal{D}_0$ and computes a bipartite quantum state σ_{AB}. The verifier sends the first system A to the (unbounded) prover, which performs an arbitrary quantum process $\mathcal{P} \in \mathrm{CPTP}(A, A')$ and returns a second quantum message $\tau_{A'}$. Let the resulting state be $\tau_{A'B} := \mathcal{P} \otimes \mathbb{1}_B(\sigma_{AB})$. Then the verifier continues making T_2 queries on input $\tau_{A'B}$ and outputs a decision bit. A T-query protocol is defined to be one making $T = T_1 + T_2$ queries. The protocol is said to solve the problem if the verifier outputs b given $\mathcal{D}_b$ with probability at least $2/3$.

Our goal is to determine b, given access to M samples $\Delta_1, \dots, \Delta_M \sim p_b$, encoded as the oracle $\mathcal{O}$. To show that no protocol can solve the problem, we start with any verifier which outputs 1 with probability at least $2/3$ for an yes instance. We prove that when given a no instance, there is a prover who convinces the verifier with probability at least $2/3 - \eta$ for negligible η. More concretely, we make random modifications from an yes instance to a no instance, in the following steps:

1. Given $f_1, \ldots, f_M$, for $i \in [M]$, compute $\Delta_i = \Delta(f_i)$ and $S_i = \{x : f_i(x) = -1\}$. Also let $\bar{S}_i = \{0, 1\}^n \backslash S_i$.

2. Sample $\Delta'_1, \ldots, \Delta'_M \sim p_0$. For $i \in [M]$, if $\Delta'_i \geq \Delta_i$, choose a random subset R of S_i such that $|R| = \Delta'_i - \Delta_i$. Set $g_i(x) = f_i(x) \cdot (-1)^{\mathbb{1}_R(x)}$, where $\mathbb{1}_R$ is the indicator function for set $R \subseteq \{0, 1\}^n$; otherwise, choose a random subset R of $\bar{S}_i$ such that $|R| = \Delta_i - \Delta'_i$. Set $g_i(x) = f_i(x) \cdot (-1)^{\mathbb{1}_R(x)}$.

3. Output $g_1, \ldots, g_M$.

We then prove that the modification yields a no instance.

Lemma 5.16. *The following two processes are equivalent, i.e., their output distributions are identical:*

1. *Output $g_1, \ldots, g_M \sim \mathcal{F}_n$.*

2. *Sample $f_1, \ldots, f_M \sim \mathcal{G}_n$ and perform the modification in the above. Output $g_1, \ldots, g_M$.*

Proof. It suffices to show that for every $\Delta_1, \ldots, \Delta_M$, performing the modification on the product distribution $\mathcal{H}_{\Delta_1} \times \ldots \times \mathcal{H}_{\Delta_M}$ yields the distribution $\mathcal{F}_n$ since $\mathcal{G}_n$ is a probabilistic mixture of $\mathcal{H}_{\Delta_1} \times \ldots \times \mathcal{H}_{\Delta_M}$ for $\Delta_1, \ldots, \Delta_M \sim p_0$. For each $i \in [M]$, recall that $f_i \sim \mathcal{H}_{\Delta_i}$ is a random subset of size $\Delta_i N$. If $\Delta'_i \geq \Delta_i$, removing $\Delta'_i - \Delta_i$ elements from S_i yields a random subset of size Δ'_i. The other case follows similarly. $\square$

We provide intuition on why there exists a cheating prover for every $o((N/n)^{1/4})$-query $\mathsf{QIP}[2]$ protocol. By Lemma 5.15, with probability $O(1/N)$ over choices of functions sampled from $\mathcal{G}_n$, $|\Delta_i - 1/2| \leq O((n/N)^{1/2})$ for every $i \in [M]$. Again by Lemma 5.15, with probability $O(1/N^{1/2})$, sampling $\Delta'_1, \ldots, \Delta'_M \sim p_0$, $|\Delta'_i - 1/2| \leq O((n/N)^{1/2})$. This implies that randomly flipping $\sum_{i=1}^M |\Delta'_i - \Delta_i| N = O(\sqrt{nN}M)$ elements from a set of at least $NM(1/2 - o(1))$ elements yields a no instance. By BBBV's hybrid argument [17], solving BFBD must make $O((N/n)^{1/4})$ queries.

Theorem 5.17. *Every $\mathsf{QIP}[2]$ protocol solving BFBD must make $\Omega((N/n)^{1/4})$ queries.*

Proof. Let $\mathcal{V}$ be any verifier which outputs 1 for an yes instance with proabability $p \geq 2/3$. Starting from an yes instance $f_1, \ldots, f_M \sim \mathcal{G}_n$, by Lemma 5.16, we perform the random modification to yield a function $g_1, \ldots, g_M$. Let $\Delta_i = \Delta(f_i)$ and $\Delta'_i = \Delta(g_i)$. By Lemma 5.15, with probability $O(1/N)$, $|\Delta_i - 1/2|$ and $|\Delta'_i - 1/2|$ are bounded by $O((n/N)^{1/2})$. Conditioned on this event happening, $|\Delta_i - \Delta'_i| \leq O((n/N)^{1/2})$.

For every functions $F = (f_1, \ldots, f_M)$, let the prover be a quantum channel $\mathcal{P}_F \in \mathrm{CPTP}(A, A')$. Given access to $\mathcal{O} = \mathcal{O}(F)$ which encodes F, let $\mathcal{V}_{\mathcal{O}}^{(1)}$ and $\mathcal{V}_{\mathcal{O}}^{(2)}$ be the unitary channels performed by the verifier in the first step and the second step of the protocol respectively. For $c \in \{1, 2\}$, we can without loss of generality write

$$V_{\mathcal{O}}^{(c)} = U_{T_c}^{(c)} \mathcal{O} \ldots U_1^{(c)} \mathcal{O} U_0^{(c)}, \tag{136}$$

and $\mathcal{V}_{\mathcal{O}}(\rho) = V_{\mathcal{O}} \rho V_{\mathcal{O}}^\dagger$. The cheating prover proves to the verifier that it is given oracle access to $f_1, \ldots, f_M \sim \mathcal{G}_n$, but the verifier is given access to $\mathcal{O}(G)$ encoding $G = (g_1, \ldots, g_M)$ obtained from the above modification. The overall quantum channel $\mathcal{T}_F$ is defined $\mathcal{V}_{\mathcal{O}(G)}^{(2)} \circ \mathcal{P}_F \circ \mathcal{V}_{\mathcal{O}(G)}^{(1)}$ under a random modification. Without loss of generality, by introducing a purifying system E inaccessible to the verifier, we can assume that $\mathcal{P}_F \in \mathrm{CPTP}(AE, A'E')$ is a unitary channel for some system E' also inaccessible to the verifier.

Our goal is to show $\mathcal{V}^{(2)}_{\mathcal{O}(F)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(F)}$ is close to $\mathcal{T}_F$. By triangle inequality,

$$
\begin{aligned}
\eta &:= \left\| \mathop{\mathbb{E}}_G \mathcal{V}^{(2)}_{\mathcal{O}(G)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(G)}(|0\rangle\langle 0|) - \mathcal{V}^{(2)}_{\mathcal{O}(F)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(F)}(|0\rangle\langle 0|) \right\|_{\mathrm{tr}} \\
&\leq \mathop{\mathbb{E}}_G \left\| \mathcal{V}^{(2)}_{\mathcal{O}(G)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(G)}(|0\rangle\langle 0|) - \mathcal{V}^{(2)}_{\mathcal{O}(G)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(F)}(|0\rangle\langle 0|) \right\|_{\mathrm{tr}} \\
&\quad + \mathop{\mathbb{E}}_G \left\| \mathcal{V}^{(2)}_{\mathcal{O}(G)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(F)}(|0\rangle\langle 0|) - \mathcal{V}^{(2)}_{\mathcal{O}(F)} \circ \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(F)}(|0\rangle\langle 0|) \right\|_{\mathrm{tr}} \\
&\leq \mathop{\mathbb{E}}_G \left\| \mathcal{V}^{(1)}_{\mathcal{O}(G)}(|0\rangle\langle 0|) - \mathcal{V}^{(1)}_{\mathcal{O}(F)}(|0\rangle\langle 0|) \right\|_{\mathrm{tr}} + \mathop{\mathbb{E}}_G \left\| \mathcal{V}^{(2)}_{\mathcal{O}(G)}(\rho_F) - \mathcal{V}^{(2)}_{\mathcal{O}(F)}(\rho_F) \right\|_{\mathrm{tr}}, \quad (137)
\end{aligned}
$$

where $\rho_F := \mathcal{P}_F \circ \mathcal{V}^{(1)}_{\mathcal{O}(F)}(|0\rangle\langle 0|)$ is a quantum state independent of the random modification. Thus it suffices to give an upper bound on the second term, and an upper bound for the first follows using a similar argument since the zero state is also a state independent of the random modification.

Let $|\psi_F\rangle$ be a purification of any quantum state ρ_F independent of the random modification. For $c \in \{1, 2\}$, consider the sequence of states:

$$
\begin{aligned}
|\phi^G_{T_c}\rangle &= U^{(c)}_{T_2} \mathcal{O}(F) U^{(c)}_{T_2-1} \mathcal{O}(F) \dots U^{(c)}_1 \mathcal{O}(F) U^{(c)}_0 |\psi_F\rangle, \\
|\phi^G_{T_c-1}\rangle &= U^{(c)}_{T_2} \mathcal{O}(G) U^{(c)}_{T_2-1} \mathcal{O}(F) \dots \mathcal{O}(F) U^{(c)}_1 \mathcal{O}(F) U^{(c)}_0 |\psi_F\rangle, \\
&\;\;\vdots \\
|\phi^G_1\rangle &= U^{(c)}_{T_2} \mathcal{O}(G) U^{(c)}_{T_2-1} \mathcal{O}(G) \dots \mathcal{O}(G) U^{(c)}_1 \mathcal{O}(F) U^{(c)}_0 |\psi_F\rangle, \\
|\phi^G_0\rangle &= U^{(c)}_{T_2} \mathcal{O}(G) U^{(c)}_{T_2-1} \mathcal{O}(G) \dots \mathcal{O}(G) U^{(c)}_1 \mathcal{O}(G) U^{(c)}_0 |\psi_F\rangle. \quad (138)
\end{aligned}
$$

The Euclidean distance between the first and the last hybrids can be bounded by bounding the distance between two adjacent hybrids:

$$
\| |\phi^G_{T_1}\rangle - |\phi^G_0\rangle \| \leq 2 \sum_{i=0}^{T-1} \| \mathbb{1}_W |\psi_t\rangle \|, \quad (139)
$$

where $|\psi_t\rangle := U_t \mathcal{O}(F) U_{t-1} \dots U_1 \mathcal{O}(F) U_0 |\psi_F\rangle$ is the intermediate state after t queries and the set $W := \{(i, x) : g_i(x) \neq f_i(x)\}$. Note that $|\psi^t\rangle$ is independent of W. Recall that we fix F and produce G by flipping random elements, by (139), taking the expectation over W yields

$$
\begin{aligned}
\mathop{\mathbb{E}}_W \| \mathcal{V}^{(2)}_{\mathcal{O}(G)}(\rho_F) - \mathcal{V}^{(1)}_{\mathcal{O}(F)}(\rho_F) \|_{\mathrm{tr}} &\leq 2 \mathop{\mathbb{E}}_W \| |\phi^G_{T_1}\rangle - |\phi^G_0\rangle \| \\
&\leq 4 T_1 \|Q\|^{1/2}_{\mathrm{op}}, \quad (140)
\end{aligned}
$$

where $Q := \mathbb{E}_W \mathbb{1}_W$. Since the modification picks a random subset of size $|W| = \sum_{i=1}^M |\Delta_i - \Delta'_i| N = O(M(nN)^{1/2})$ on a set of size at least $M(N/2 - O((nN)^{1/2}))$, $\|Q\| \leq O((n/N)^{1/2})$. Thus $\eta \leq O(T(n/N)^{1/4})$. Thus the verifier accepts the no case with probability at least $p - \eta - O(1/N) > 1/3$. $\qquad \square$

The statement in Theorem 5.17 can be further strengthened to $\mathsf{QIP} = \mathsf{QIP}[3]$ using a similar hybrid argument, but since we will not need this result, we do not pursue this further. By the equivalence of BFBD and LLQSV shown in Lemma 5.14 and Theorem 5.17, we immediately have the following corollary.

Corollary 5.18. *There exists a constant $c > 0$ such that $\mathsf{LLQSV} \notin \mathsf{QIP}[2](c(N/n)^{1/4})$ relative to a random oracle.*

47

5.4.2 Strengthen the hardness

The final step is to "lift" from a lower bound against a uniform complexity class like QIP[2] or its subclass QMA, to a lower bound against the nonuniform complexity class QCAM/qpoly (or its generalization to use more time and more advice).

As a first observation, QCAM = BP · QCMA, and the BP· operator can be simulated by polynomial-size classical advice using Adleman's trick. Thus QCAM/poly = QCMA/poly and QCAM/qpoly = QCMA/qpoly. As a second observation, Aaronson and Drucker [8] proved that QCMA/qpoly ⊆ QMA/poly. Furthermore, all of these results relativize.

We apply the strong direct product theorem (SDPT) by Sherstov [58] to lift the hardness to QMA/poly. Recall that Sherstov showed that the query complexity obeys SDPT when the query lower bound of a single instance is proved using the *polynomial method* [15].

In the first step, we give an oracle separation coNP ⊄ QMA/poly, and the proof for LLQSV ∉ QMA/poly will basically follow the same ideas with minor modifications.

Warmup: coNP ⊄ QMA/poly. To give an oracle separation, the oracle F encodes $N = 2^n$ instances of the problem. The oracle F contains N sections, and each section $F_x \in \{0,1\}^N$ is indexed by an n-bit string x. Let an yes instance be the all-one function, i.e., $f_0(x) = 1$ for every $x \in \{0,1\}^n$. The no instance is obtained by flipping εN points for $\varepsilon \geq \eta$ and $\eta = 100/N$. Each section F_x is either the yes case or the no case, with probability $1/2$. The task is on input x, determine in which case F_x is. The problem is clearly in coNP, and therefore the proof of the following theorem is devoted to showing that the problem is not in QMA/poly.

Theorem 5.19. *There exists an oracle relative to which* coNP ⊄ QMA/poly.

Proof. Let $\mathcal{D}_x$ denote equal mixture of the yes case and the no case for each $x \in \{0,1\}^n$. For $x \in \{0,1\}^n$, let F_{-x} denote all the sections but F_x and similarly for $\mathcal{D}_{-x}$. Let $f_0 = 1^N$ denote the yes instance and $\rho_{F,x}$ be the witness states given oracle access to F and input x. For a sufficiently small constant c, $\eta = 100/N$, $T = o((1/\eta)^{1/2}/n)$ and $S = cN$, our idea is to show that a set of witness states $\{\rho_x : x \in \{0,1\}^n\}$ that convince any QMA(T)/S verifier V with probability at least $2/3$ when $F_x = f_0$ can be used to convince the same verifier to accept a no instance for some $x \in \{0,1\}^n$ with probability more than $1/3$. Thus the V does not solve the problem.

Suppose toward contradiction that it is not the case. Then V accepts when $F_x = f_0$ with probability at least $2/3$, i.e.,

$$\Pr_{F_x=f_0, F_{-x}\sim\mathcal{D}_{-x}}\left[V^F(w_F, x, \rho_x) = 1\right] \geq 2/3, \tag{141}$$

where $w_F \in \{0,1\}^S$ is a classical advice that depends on F. Furthermore, when the modification is applied to F_x, the verifier can detect the change with the aid of the advice. More concretely, for $y \in \{0,1\}^n$, let M_y denote a probabilistic algorithm applied F to change $F_y = f_0$ to a no instance, i.e., $M_y(F)_x$ is a no case if $x = y$ and $M_y(F)_x = F_x$ otherwise. By the assumption we make, with the modification, for every $x \in \{0,1\}^n$,

$$\Pr_{F_x=f_0, F_{-x}\sim\mathcal{D}_{-x}, M_x(F)=G}\left[V^G(w_G, x, \rho_x) = 0\right] \geq 2/3. \tag{142}$$

Note that the advice can be sensitive to the change. Since the witness state does not depend on the modification, we effectively remove the witness out of picture.

Let $\mathcal{D}_1$ denote the distribution of the yes case and $\mathcal{D}_0$ denote the distribution of the no case. Applying a witness-preserving amplification [42], let V' be the $\mathsf{QMA}(c'Tn)/S$ protocol which solves the problem with probability at least $1 - 1/N^2$ for a sufficient large constant c'. Then we can construct an $\mathsf{QMA}(c'TnN)/S$ verifier $\tilde{V}$ which solves N problems: The prover sends the witness state $\rho := \bigotimes_{x \in \{0,1\}^n} \rho_x$ in one message, and the verifier runs V' on every $x \in \{0,1\}^n$, ρ_x and the given advice w_F, i.e., $\tilde{V}^F(w_F, \rho) := \bigotimes_{x \in \{0,1\}^n}(V')^F(w_F, x, \rho_x)$. By a union bound, with probability at least $1 - 1/N$, $\tilde{V}$ outputs the correct N-bit string, i.e.,

$$\Pr_{b \sim \mathcal{U}_N, F \sim \mathcal{D}_b}\left[\tilde{V}^F(w_F, \rho) = b\right] \geq 1 - 1/N, \tag{143}$$

where $\mathcal{U}_N$ denote the uniform distribution over N-bit strings and $\mathcal{D}_b$ denote the distribution $\times_{x \in \{0,1\}^n} \mathcal{D}_{b_x}$.

Now we replace the advice w_F with a random string (independent of F), and by (143), this yields

$$\Pr_{b \sim \mathcal{U}_n, F \sim \mathcal{D}_b, r \sim \mathcal{U}_S}\left[\tilde{V}^F(r, \rho) = b\right] \geq \frac{1 - 1/N}{2^S} \geq \frac{1}{2^{S+1}}. \tag{144}$$

This effectively yields a $c'TnN$-query algorithm solving N problems with probability at least 2^{-S-1}. For each problem, let p denote the real polynomial that approximates the AND function to error $1/3$. Thus the constraints we have are (i) $p(0) \geq 2/3$, and (ii) $p(\varepsilon) \leq 1/3$ for every $1 \geq \varepsilon \geq \eta$ and εN is an integer. By Lemma 3.7, $\deg(p) \geq \Omega(\sqrt{1/\eta})$. Now by Theorem 3.8, for a sufficiently small constant c and $S = cN$, solving N independent problems with probability 2^{-S-1} requires $2cN\sqrt{1/\eta}$ queries. Thus it must hold that $c'TnN \geq 2cN\sqrt{1/\eta}$ queries and $T = \Omega(\sqrt{1/\eta}/n)$. $\square$

LLQSV $\notin$ QMA/poly. The proof for LLQSV $\notin$ QMA/poly basically follows the idea for coNP $\not\subset$ QMA/poly, with the following modifications. First, the distribution $\mathcal{D}_1$ does not describe a fixed function; instead, we replace it with the yes case in BFBD (Definition 5.13). For this, we basically apply an averaging argument. Second, by Lemma 5.15, the no case of BFBD is obtained by modifying the yes case on a random subset of size $O(\sqrt{n/N})$ with probability at least $1 - 1/N$. The QMA/poly verifier is no longer required to solve the problem for *every* $\varepsilon \geq \eta$, which is essential for a lower bound using the polynomial method. We show that via a reduction, we can get sufficiently many constraints to get a tight lower bound.

Here we describe the problem LLQSV relative to the following oracle: The oracle F contains N sections, each indexed by an n-bit string x. Each section F_x is sampled uniformly from n-bit Boolean functions, and the sample s_x is either sampled from $|\hat{F}_x|^2$, or a uniform n-bit string (independent of F_x). On input x, the protocol is challenged to determine s_x is sampled from $|\hat{F}_x|^2$ in the yes case or the uniform distribution in the no case.

Theorem 5.20. *There exists a constant $c > 0$ such that* LLQSV $\notin$ QMA$(c(N/n)^{1/4}/n)/(cN)$ *relative to a random oracle.*

Proof. The proof basically follows that of Theorem 5.19. First by Lemma 5.14, let $\mathcal{D}_1$ and $\mathcal{D}_0$ denote the distributions in the yes and the no cases of BFBD (Definition 5.13) respectively. In this picture, each section of the oracle is either sampled from $\mathcal{D}_1$ or from $\mathcal{D}_0$. Let $\mathcal{D}$ denote the equal mixture of $\mathcal{D}_1$ and $\mathcal{D}_0$.

The idea is to show that for $T = o((N/n)^{1/4}/n)$, any set of witness states $\{\rho_{F,x} : F \in \{0,1\}^{N \times N}, x \in \{0,1\}^n\}$ that convince any QMA$(T)/S$ verifier V with probability $2/3$ when $F_x \sim \mathcal{D}_1$ can be used to convince the verifier that $F_x \sim \mathcal{D}_0$ for some $x \in \{0,1\}^n$ with probability more than

49

1/3. Suppose toward contradiction that for every x, when $F_x \sim \mathcal{D}_0$, V accepts with probability at most $1/3$. Let the modification denote M_x to change any F_x such that $M_x(F_x)$ is distributed according to $\mathcal{D}_0$, and other sections are unchanged. By an averaging argument, for every $x \in \{0,1\}^n$, there exists a function F_x and a random modification of size $r_x = O(\sqrt{nN})$ such that the verifier detects if the modification has been applied with probability at least $2/3 - o(1)$. Then by random self-reducibility, there exists a verifier which outputs the correct answer on every modification of size r_x with probability at least $2/3 - o(1)$ as well.

By a witness-preserving amplification, there is a $\mathsf{QMA}(O(Tn))/S$ verifier which detects if there is a random modification of size r_x with probability at least $1 - 1/N^2$ on every x. The assumption implies that there is a $\mathsf{QMA}(O(TNn))/S$ verifier $\tilde{V}$ which solves N problems (i.e., $\tilde{V}$ determines if there is a modification of size r_x for every $x \in \{0,1\}^n$) with probability at least $1 - O(1/N)$ on the witness state $\rho_F := \bigotimes_{x \in \{0,1\}^n} \rho_{F,x}$ independent of the modifications. Now we replace the advice string with a random string, and yield a $O(TNn)$-query QMA verifier which is given the witness state ρ_F and solves N problems with probability at least 2^{-S-1} on the witness ρ_F. Then we apply Theorem 3.8 to get $\deg(p) = O(Tn)$ for any real polynomial p that approximate the function to compute to error $1/5$ for $S = cN$ for a sufficiently small constant c.

It remains to show that every T'-query algorithm detecting modifications on a random subset R of size $r \le O(\sqrt{nN})$ in a set Q of size $q = \Omega(N)$ implies that a T'-query algorithm which detects a random modification $R' \subseteq Q'$ for $|R'| \in \{1, 2, \ldots, |Q'|\}$ and $|Q'| = \Omega(q/r)$. Thus we can use the polynomial method to conclude that every T'-query algorithm solving the problem must satisfy $2T' = \deg(p)$, for any polynomial p satisfying the following constraints: (i) $p(0) \ge 2/3$ and (ii) $p(i) \le 1/3$ for $i \in \{1, 2, \ldots, |Q'|\}$. By Lemma 3.7, $\deg(p) = \Omega(\sqrt{|Q'|}) = \Omega((N/n)^{1/4})$ and thus $T = \Omega(T'/n) = \Omega((N/n)^{1/4}/n)$.

Without loss of generality, let $Q = [q]$ and R be a random subset of size r. For every function $f_0 : [q] \to \{0,1\}$, we define the problem $\mathcal{P}_{q,r}$ as follows: In the yes case, the algorithm is given access to $f = f_0$, and in the no case, the algorithm is given access to $f(x) := f_0(x) \oplus \mathbb{1}[x \in R]$ for a random subset R of size r. Thus from the previous paragraph, our goal is to show that an algorithm solving $\mathcal{P}_{q,r}$ implies an algorithm solving $\mathcal{P}_{\eta,\ell}$ for $\eta = \lfloor q/r \rfloor$ and every $\ell \in \{1, 2, \ldots, \eta\}$ using the same number of queries. First we can stretch the parameters η, ℓ by a factor $\alpha \ge 1$ to yield an instance g in $\mathcal{P}_{\alpha\eta,\alpha\ell}$: Define $\tilde{g} : [\alpha\eta] \to \{0,1\}$, $\tilde{g}(x) := f(((x-1) \bmod \eta) + 1)$, and the function $g(x) := \tilde{g} \circ \pi(x)$ for a random permutation π on $[\alpha\eta]$. Second, we can pad a function with β elements to yield a reduction from $\mathcal{P}_{\eta,\ell}$ to $\mathcal{P}_{\eta+\beta,\ell}$: Let $\tilde{g} : [\eta+\beta] \to \{0,1\}$, $\tilde{g}(x) = f(x)$ for $x \in [q]$ and $\tilde{g}(x) = 0$ for $x > \eta$, and the function $g := \tilde{g} \circ \pi$ for a random permutation π on $[\eta+\beta]$. For problem $\mathcal{P}_{\eta,\ell}$, first we apply a stretch to yield $\mathcal{P}_{\eta r/\ell, r}$, followed by a padding with $q - \eta r/\ell$ elements to yield $\mathcal{P}_{q,r}$. $\qquad\square$

When combining powerful quantum complexity classes with *quantum* advice, one needs to be even more careful. For example, Raz [53] showed that $\mathsf{QIP}/\mathsf{qpoly} = \mathsf{ALL}$ (ALL being the class of all languages), and Aaronson [2] likewise showed that $\mathsf{PDQP}/\mathsf{qpoly} = \mathsf{ALL}$, where PDQP is the generalization of BQP to allow multiple non-disturbing measurements [6]. Our proof based on a strong direct product theorem can be used to further strengthen our result to $\mathsf{LLQSV} \notin \mathsf{QMA}/\mathsf{qpoly}$, thereby giving a new proof for $\mathsf{QMA}/\mathsf{qpoly} \ne \mathsf{ALL}$ relative to a random oracle. Previously, Aaronson proved that $\mathsf{QMA}/\mathsf{qpoly} \subseteq \mathsf{PSPACE}/\mathsf{poly}$ [1].

We note that the proof technique does not allow us to prove the problem is not in $\mathsf{QIP}[2]/\mathsf{qpoly} = \mathsf{ALL}$, because there is no generic rewinding procedure to restore the quantum advice for another use.

In any case, the above suffices to establish the following.

Theorem 5.21. *Relative to a random oracle, LLQSV $\notin$ QCAM(c^n)/q(c^n), for some constant $1 < c < 2$.*

6 A Device Performing the Ideal Measurement

In this section, we consider a device which does the following: the device may share an arbitrary entanglement ψ_{DE} with Eve before receiving a Haar-random circuit. After receiving $C \sim \text{Haar}(N)$, the device $\mathcal{A}$ performs the ideal measurement, i.e., it runs the circuit C on system D of ρ_{DE}, and performs a standard basis measurement to output strings. On the other hand, the eavesdropper Eve may learn information about the device's output by applying an arbitrary quantum operation on the second system E, but it has no direct access to $\mathcal{A}$'s system and output. In the following discussion, we will also call such a device $\mathcal{A}$ a semi-honest device.

6.1 A single-round analysis

In general, the first system is a Hilbert space $D \cong \mathbb{C}^{2^d}$ for $d \geq n$. Without loss of generality, we can only consider the case where $D \cong \mathbb{C}^N$, i.e., $d = n$. The reason is that for $d \geq n$, we can decompose $D = D' \otimes D''$ such that $\mathcal{H}_{D'} \cong \mathbb{C}^N$ is the system the circuit C acts on, and let $E' = D'' \otimes E$. In this case, it suffices to find a lower bound of $H(D'|E')_\rho$ since $H(D|E)_\rho \geq H(D'|E')_\rho$ and $H_{\min}(D|E)_\rho \geq H_{\min}(D'|E')_\rho$, where $\rho = \mathcal{A}_D^C \otimes \mathbb{1}_E(\psi)$ is the classical-quantum state after the ideal measurement is performed when C is chosen by the verifier. Thus in the following analysis, we assume $D \cong \mathbb{C}^N$ and $\mathcal{A}^C$ is the unitary channel of C on D.

6.1.1 The Holevo Information

By linearity of quantum operations, without loss of generality, we can consider the special case where the device and the eavesdropper share a pure state in Schmidt decomposition

$$|\psi\rangle = \sum_{i \in \{0,1\}^n} \sqrt{\lambda_i} |\phi_i\rangle_D |\psi_i\rangle_E, \tag{145}$$

where each $\lambda_i \geq 0$ is real for every i and $\{|\phi_i\rangle\}$ and $\{|\psi_i\rangle\}$ are twe sets of orthonormal vectors. We also denote $\psi := |\psi\rangle\langle\psi|$.

Lemma 6.1. *For any algorithm $\mathcal{A}$, let $\sigma = \mathcal{A}^C(\psi)$ be the classical-quantum state obtained by performing a projective measurement depending on C on the first system D. Then the Holevo information of σ, denoted $\chi(D : E)_\sigma = H(\lambda)$, where $H(\lambda)$ is the Shannon entropy of the distribution λ.*

Proof. We consider the unitary $U := \sum_i |\phi_i\rangle\langle i|$ and let $U_{ij} = \langle i|U|j\rangle$ be the element of matrix U. Also let $\bar{U} = \sum_{ji} U_{ji}|\psi_i\rangle\langle\psi_j|$, $\rho = \sum_i \lambda|i\rangle\langle i|$ and $\bar{\rho} = \sum_i \lambda_i|\psi_i\rangle\langle\psi_i|$. Since $\{|\psi_i\rangle\}$ is a set of orthonormal vectors, $\bar{U}$ is also a unitary acts on the space span$\{|\psi_i\rangle\}$. The entanglement $|\psi\rangle$ can

be written in the standard basis:

$$
\begin{aligned}
|\psi\rangle &= \sum_i \sqrt{\lambda_i} U |i\rangle |\psi_i\rangle \\
&= \sum_{ij} \sqrt{\lambda_i} U_{ji} |j\rangle |\psi_i\rangle \\
&= \sum_{ij} \sqrt{\lambda_i} |j\rangle |\psi_i\rangle \langle \psi_i| \bar{U} |\psi_j\rangle \\
&= \sum_j |j\rangle_D \bar{\rho}^{1/2} \bar{U} |\psi_j\rangle_E.
\end{aligned}
\tag{146}
$$

We define the subnormalized pure state

$$
\sigma_i := \bar{\rho}^{1/2} \bar{U} |\psi_i\rangle \langle \psi_i| \bar{U}^\dagger \bar{\rho}^{1/2},
\tag{147}
$$

and compute the Holevo information:

$$
\begin{aligned}
\chi(D:E)_{\mathcal{A}^C(\psi)} &= H(E)_{\sum_i \sigma_i} - \sum_i \alpha_i H(E)_{\sigma_i/\alpha_i} \\
&= H(\lambda).
\end{aligned}
\tag{148}
$$

where $H(\lambda)$ is the Shannon entropy of λ and $\alpha_i := \operatorname{tr}(\sigma_i)$. The second equality in (148) holds since

$$
\sum_i \sigma_i = \bar{\rho},
\tag{149}
$$

and $H(E)_{\bar{\rho}} = H(\lambda)$. Moreover, since $\frac{1}{\alpha_i}\sigma_i$ is a normalized pure state, $H(E)_{\sigma_i/\alpha_i} = 0$. Note that $\sum_i \sigma_i$ is independent of $\bar{U}$, so the Holevo information does not change if a different measurement is performed on the first system D. Therefore for every C, the Holevo information is $H(\lambda)$. $\qquad\square$

Next, we show that if the device solves $\frac{(2-\varepsilon)N}{N+1}$-XHOG, then the Holevo information is at most $\varepsilon n + 1$. This observation can be used to estabilish a lower bound of the conditional von Neumann entropy.

6.1.2 High XHOG Score Implies Small Holevo Information

Previously, we have shown the Holevo information can be explicitly computed if the Schmidt decomposition is known. In this section, we establish the connection between the Holevo information and the score of any semi-honest device.

First, we introduce a useful technical lemma.

Lemma 6.2. *Let p be a distribution p over finite set $\mathcal{X}$ of N elements such that there exists $x \in \mathcal{X}$, $p(x) \geq 1 - \varepsilon$. Then the Shannon entropy $H(p) \leq \varepsilon n + 1$.*

Proof. Let $p(x) = 1 - \gamma$ for $\gamma \leq \varepsilon$ and q be the conditional distribution on the event that $y \neq x$ i.e.,

$q(y) = p(x)/\gamma$ for $y \neq x$. By definition,

$$H(p) = -p(x)\log p(x) - \sum_{y \neq x} p(y)\log p(y)$$

$$= -(1-\gamma)\log(1-\gamma) - \gamma \sum_{y \neq x} q(y)(\log q(y) + \log \gamma)$$

$$= -(1-\gamma)\log(1-\gamma) - \gamma \log \gamma - \gamma \sum_{y \neq x} q(y)\log q(y)$$

$$= h(\gamma) + \gamma H(q), \tag{150}$$

where h is the binary entropy function satisfying $h(\gamma) \leq 1$ for $\gamma \in [0,1]$. Since q is a distribution over $N-1$ elements, it Shannon entropy is upper bounded by $\log(N-1) \leq n$. $\qquad\square$

By Lemma 6.2, to prove the Holevo information is small, it suffices to show that when the XHOG score is high, the distribution λ must be concentrated on a single point.

Lemma 6.3. *The Holevo information of the classical-quantum state obtained from any semi-honest device solves $\frac{(2-\varepsilon)N}{N+1}$-XHOG is at most $\varepsilon n + 1$.*

Proof. We analyze the XHOG score of a device on input a standard basis vector $|i\rangle$:

$$S_i := \mathop{\mathbb{E}}_{C \sim \text{Haar}(N)}\left[\sum_z q_{C,i}(z)p_C(z)\right]. \tag{151}$$

where $q_{C,i}(z) = |\langle z|C|i\rangle|^2$. For $i = 0$, $q_{C,0} = p_C$ the score is $\frac{2}{N+1}$. For $i \neq 0$, the distribution of $p_C(z)$ and $q_{C,i}(z)$ can be seen as two distinct elements of $P \sim \text{Dir}(1^N)$. These facts imply

$$S_i = N \cdot \mathop{\mathbb{E}}_{P \sim \text{Dir}(1^N)}[P_0 P_i]$$

$$= \frac{1 + \delta_{i0}}{N+1}. \tag{152}$$

By definition, the XHOG score using $|\psi\rangle$ is

$$S = \mathop{\mathbb{E}}_{C}\left[\sum_z p_C(z)\langle\psi|(C^\dagger|z\rangle\langle z|C) \otimes \mathbb{1}|\psi\rangle\right]$$

$$= \sum_i S_i \cdot \langle\psi_i|\bar{U}^\dagger\bar{\rho}\bar{U}|\psi_i\rangle. \tag{153}$$

Let $\bar{\tau} := \bar{U}^\dagger\bar{\rho}\bar{U}$ and $\bar{\tau}'$ be the state obtained by measuring $\bar{\tau}$ in basis $\{|\psi_i\rangle\}$. If $S \geq \frac{2-\varepsilon}{N+1}$,

$$\frac{2-\varepsilon}{N+1} \leq \sum_i S_i \bar{\tau}'_{ii}$$

$$= \frac{1 + \bar{\tau}'_{00}}{N+1}. \tag{154}$$

This implies that $\bar{\tau}'_{00} \geq 1 - \varepsilon$. By Lemma 6.1, the Holevo information can be upper bounded:

$$\chi(D:E)_{\mathcal{A}^C(\rho)} = H(E)_{\bar{\tau}} \leq H(E)_{\bar{\tau}'} \leq \varepsilon n + 1. \tag{155}$$

Since $\bar{\tau}'$ is obtained by performing a projective measurement $\{|\psi_i\rangle\}$ on τ, by Lemma 3.11, $H(E)_{\bar{\tau}} \leq H(E)_{\bar{\tau}'}$. The second inequality holds by Lemma 6.2. Moreover, the inequality saturates when $\bar{U}$ is the identity matrix, i.e., $\{|\psi_i\rangle\}$ is the standard basis. $\qquad\square$

We note that the bound in Lemma 6.3 is nearly optimal: Consider the case where the entanglement shared by the device and Eve be the quantum state

$$|\psi\rangle_{DE} = (1-\varepsilon)^{1/2}|0,0\rangle + \left(\frac{\varepsilon}{N-1}\right)^{1/2}\sum_{x\neq 0}|x,x\rangle. \tag{156}$$

The the Holevo information by Lemma 6.1 is $\varepsilon\log(N-1) + h(\varepsilon)$.

6.1.3 A Single-Round Analysis

Now we show small Holevo information implies large conditional von Neumann entropy. We apply the idea from [11] and [10]. Let D and E denote the device's output random variable and Eve's quantum register, repectively. By definition, the Holevo information

$$\chi(D:E)_{\mathcal{A}^C(\rho)} = H(E)_{\mathcal{A}^C(\rho)} - H(E|D)_{\mathcal{A}^C(\rho)}, \tag{157}$$

where H denotes the von Neumann entropy. The following theorem shows a linear lower bound of the von Neumann entropy when the device solves b-XHOG for $b \approx (2-\varepsilon)$.

Theorem 6.4. *For any device $\mathcal{A}^C$ that given access to C and performs the ideal measurement on the first system D of any bipartite quantum state ρ_{DE} and solves b-XHOG for $b \geq \frac{(2-\varepsilon)N}{N+1}$,*

$$\Pr_{C\sim\text{Haar}(N)}\left[H(D|E)_{\mathcal{A}^C(\rho)} \geq (0.99-\varepsilon)n\right] \geq 1 - O\left(\frac{1}{N^{0.02}}\right). \tag{158}$$

Proof. Let $\mathcal{A}^C$ be any device that performs an ideal measurement to yield $\psi_{DE}^C := \mathcal{A}^C(\rho)$ and outputs a random variable D. We observe that

$$\begin{aligned}
H(D|E)_{\psi^C} &= H(DE)_{\psi^C} - H(E)_{\psi^C} \\
&= H(D)_{\psi^C} + H(E|D)_{\psi^C} - H(E)_{\psi^C} \\
&= H(D)_{\psi^C} - \chi(D:E)_{\psi^C}.
\end{aligned} \tag{159}$$

The first term in the third line of (159), i.e., $H(D)_{\psi^C}$, denotes the von Neumann entropy of the device's output, when Eve's system E is empty. To lower bound the first term in (159), recall that $q_{C,i}(z) = |\langle z|C|i\rangle|^2 = p_{CX^i}(z)$. From (44) and right translational invariance of the Haar measure, for every i,

$$\begin{aligned}
\Pr_{C\sim\text{Haar}(N)}[H(p_{CX^i}) \geq 0.99n + 1] &\geq \Pr_C\left[S_C \leq N^{-0.99}/2\right] \\
&\geq 1 - O\left(\frac{1}{N^{1.02}}\right).
\end{aligned} \tag{160}$$

By the union bound,

$$\Pr_{C\sim\text{Haar}(N)}\left[\min_{i\in\{0,1\}^n} H(p_{CX^i}) \geq 0.99n + 1\right] \geq 1 - O\left(\frac{1}{N^{0.02}}\right). \tag{161}$$

Now by the convexity of Shannon entropy and the definition that $q_C(z) = \mathbb{E}_{i\sim\bar{\tau}'}[q_{C,i}(z)]$,

$$\begin{aligned}
\Pr_{C\sim\text{Haar}(N)}[H(q_C) \geq 0.99n + 1] &\geq \Pr_{C\sim\text{Haar}(N)}\left[\mathbb{E}_{i\sim\bar{\tau}'}[H(p_{CX^i})] \geq 0.99n + 1\right] \\
&\geq \Pr_{C\sim\text{Haar}(N)}\left[\min_i H(p_{CX^i}) \geq 0.99n + 1\right] \\
&\geq 1 - O\left(\frac{1}{N^{0.02}}\right).
\end{aligned} \tag{162}$$

Input: security parameter n, the number of rounds m, the score parameter $\delta \in [0,1]$ and the fraction of test rounds γ.

The protocol:

1. The verifier samples $C \sim \mathrm{Haar}(N)$. For $i = 1, \ldots, m$, run the following steps:

   (a) The verifier sends C to the device. (This step may be omitted.)

   (b) The device returns a sample z_i.

2. Let $t = |\{i : T_i = 1\}|$ be the number of test rounds. The verifier computes

$$s = \frac{1}{t} \sum_{i:T_i=1} p_C(z_i). \tag{166}$$

   If $s \geq (1 + \delta)/N$, then the verifier accepts and outputs $(z_1, \ldots, z_m)$ to the quantum-proof randomness extractor.

Figure 2: The entropy accumulation protocol for a device performing the ideal measurement.

Thus since $H(D)_{\psi^C} = H(q_C)$,

$$\Pr_{C \sim \mathrm{Haar}(N)} \big[H(D)_{\psi^C} \geq 0.99n + 1 \big] \geq 1 - O\left(\frac{1}{N^{0.02}} \right). \tag{163}$$

In Lemma 6.3, we have shown that for every C, $\chi(D : E)_{\psi^C} \leq \varepsilon n + 1$. Then by (163),

$$\Pr_{C \sim \mathrm{Haar}(N)} \big[H(D|E)_{\psi^C} \geq (0.99 - \varepsilon)n \big] \geq 1 - O\left(\frac{1}{N^{0.02}} \right). \tag{164}$$

$\square$

We denote the output state $\psi = \mathbb{E}_{C \sim \mathrm{Haar}(N)} \big[|C\rangle\langle C| \otimes \psi^C \big]$, and

$$H(D|CE)_\psi := \mathbb{E}_{C \sim \mathrm{Haar}(N)} \big[H(D|E)_{\psi^C} \big]. \tag{165}$$

The following corollary concludes our single-round analysis for this ideal setting.

Corollary 6.5. *Let $\mathcal{A}$ be any device performing an ideal measurement solving $(1+\delta)$-XHOG and ψ be its output. Then $H(D|CE)_\psi \geq (\delta - 0.01)n - o(1)$.*

Proof. By definition and Theorem 6.4, $H(D|CE)_\psi \geq (\delta - 0.01)n - O(N^{-0.02})$. $\square$

6.2 Entropy Accumulation

We present our entropy accumulation protocol for any device which performs the ideal measurement in Figure 2. Note that since the von Neumann entropy lower bound holds for almost every C, the verifier may reuse the circuit in every round.

Theorem 6.6. *Let $\mathcal{A}_1, \ldots, \mathcal{A}_m$ be $n^{O(1)}$-query sequential processes given access to the first system of a bipartite state ρ_{DE} and outputting $z_1, \ldots, z_m$ solving $\mathrm{LXEB}_{1+\delta,m}$ with probability p. Then with probability $1 - 2^{-\Omega(n)}$ over the choices of C,*

$$H_{\min}^{\varepsilon}(Z^m|E)_{\mathcal{A}_m \circ \ldots \mathcal{A}_1(\rho)|\Omega} \geq n\big((\delta - 0.01)m - c\sqrt{m} - o(1)\big) \tag{167}$$

where Ω denotes the event that the output $z_1, \ldots, z_m$ solves $\mathrm{LXEB}_{1+\delta,m}$, i.e.,

$$\Omega := \left\{ (z_1, \ldots, z_m) : \frac{1}{m}\sum_{i=1}^{m} P(z) \geq \frac{1+\delta}{N} \right\}. \tag{168}$$

The parameter $c := 4.01(1 + \log(\frac{1}{p\varepsilon}))^{1/2}$.

Proof. We apply the EAT shown in Section 4. In particular, we choose $G := N\sum_z |z\rangle\langle z|P(z)$. By Corollary 6.5, we choose $f(\delta) = (\delta - 0.01)n - o(1)$. This gives $\|\nabla f\|_\infty = n$. Then we have $V = 2(\log(2d_Z + 1) + \|\nabla f\|_\infty) = 2(\log(2N + 1) + n) = 4n + O(1/N) \leq 4.01n$. Now we have

$$H_{\min}^{\varepsilon}(Z^m|E)_{\mathcal{A}_m \circ \ldots \circ \mathcal{A}_1(\rho)|\Omega} \geq n\left((\delta - 0.01)m - o(1/n) - 4.01\sqrt{m}\sqrt{\log\frac{2}{\Pr_\sigma[\Omega]^2 \varepsilon^2}} \right). \tag{169}$$

$\square$

As a side note, the same analysis in Section 6.1 and Section 6.2 also applies to a Fourier sampling circuit, i.e., C describes the unitary transformations in (126) under a random n-bit Boolean functions f. In this case, an ideal devices solves b-XHOG for $b \approx 3$ [39], and any device solving $(1 + 2\delta)$-XHOG has a lower bound $\Omega(\delta n)$ on the conditional von Neumann entropy. Applying the entropy accumulation theorem, an m-round protocol also accumulates $\Omega(\delta mn)$ conditional min-entropy.

The analysis in Section 6 is meant to provide an intuition on why LXEB can be used to generate randomness in a simplified setting. In particular, for entropy accumulation, the channels $\mathcal{A}_1, \ldots, \mathcal{A}_m$ are the ideal unitary channel of C, so this setting is far from full device-independence. In the next section, we provide an analysis for a fully general device where the channels $\mathcal{A}_1, \ldots, \mathcal{A}_m$ are not necessarily ideal.

7 A Fully General Device

In this section, we give an analysis for a general device. Before we prove our main result, first we provide some intuition. Let ρ_{DE} be an entangled state shared between the device and Eve, and $\mathcal{A}^C(\rho_{DE})$ be the quantum algorithm that the device performs given access to the first subsystem D and the circuit C. Without loss of generality, $\mathcal{A}^C(\rho_{DE})$ outputs a classical-quantum state in the form $\sum_z p(z)|z\rangle\langle z|_{D'} \otimes \xi_E(z)$ (this also implies that $\mathcal{A}^C$ is a quantum channel of type $D \to D'$ for Hilbert spaces D and D') for normalized quantum states $\xi_E(z)$. The classical part, i.e., the random variable z is sent to the verifier, and the quantum information $\xi_E(z)$ can be used as the input to the next round of interaction. In an m-round protocol, the device and the verifier repeat the message exchanges m times, and the verifier outputs a decision bit indicating accept or abort. If the verifier accepts, then the output of the device is fed into a quantum-proof randomness extractor.

We consider any device given oracle access to C, and show that if the device passes $\mathrm{LXEB}_{b,k}$, the output must has a min-entropy lower bound. First, applying the rotational invariance of a Haar random unitary, we formally define an input model in which the device is given access to:

the verifier samples a circuit $C \sim \mathrm{Haar}(N)$ and two unitaries V, W. The first unitary V is a random phase unitary of the form $\sum_z e^{i\theta_z} |z\rangle\langle z|$, where each θ_z is independently sampled from the uniform distribution over $[0, 2\pi)$. The second unitary W is a Haar random unitary on the subspace $\{|x\rangle : x \in \{0,1\}^n \setminus \{0^n\}\}$. The device is then given oracle access to $C' = VCW$, and by definition, it is clear that $p_C = p_{C'}$, where $p_C(z) := |\langle z|C|0\rangle|^2$ is the density of p_C. Also, C and C' are identically distributed (according to the Haar measure). We will say an efficient device is given oracle access to C if it can apply C' on any subset of its system D of the same size.

The symmetrization allows us to analyze a von Neumann entropy lower bound. In particular, we show that the conditional von Neumann entropy on C is equal to the von Neumann entropy on p_C in this query model. Since C is distributed over an infinite set, we define the von Neumann entropy $H(Z|CE)_\psi := \mathbb{E}_C [H(Z|E)_{\psi^C}]$, where ψ^C is the classical-quantum state output by the device $\mathcal{A}$ when $\mathcal{A}$ is given access to C. In the following discussion, we use capitalized P_C to emphasize that the distribution is a vector of complex-valued random variables over the probability simplex. In particular, for $C \sim \mathrm{Haar}(N)$, P_C is distributed according the the Dirichlet distribution $\mathrm{Dir}(1^N)$ (see Section 3.4 for details).

Theorem 7.1. *For Haar random C and every device $\mathcal{A}$ which on input the first system of a bipartite state ρ_{DE} and outputs a classical-quantum state ψ given oracle access to C. Then $H(Z|CE)_\psi = H(Z|P_C E)_\psi$, where $P_C(z) := |\langle z|C|0^n\rangle|^2$ is distributed according to the Dirichlet distribution $\mathrm{Dir}(1^N)$.*

Proof. For every distribution P, we let S_P be the set of unitaries such that $P_C = P$. For each P, let C_P denote a representative in the set S_P. Then for $C \in S_P$, there exists a diagonal unitary V' and a unitary W' on the subspace $\mathrm{span}\{|x\rangle : x \neq 0^n\}$ such that $C = V'C_P W'$. This implies that one can simulate a query to $C \in S_P$ using one query to C_P. More precisely, for $C \in S_P$, we denote $\sigma^P = \psi^C = \psi^{C_P}$. This implies that $H(Z|E)_{\psi^C} = H(Z|E)_{\sigma^P}$. By the definition of conditional von Neumann entropy and the fact that p_C is distributed according the distribution $\mathrm{Dir}(1^N)$, $H(Z|CE)_\psi = \mathbb{E}_{P \sim \mathrm{Dir}(1^N)}[H(Z|E)_{\sigma^p}] = H(Z|PE)_\psi$. $\qquad\square$

Our analysis proceeds in the following steps. First, we show that for every T-query $\mathcal{A}$ and ρ_{DE}, there is another quantum algorithm $\mathcal{B}$ which on input the first system D of ρ_{DE} and k i.i.d. random variables $z_1, \ldots, z_k$ sampled according to P_C for Haar-random C such that

$$\left\| \mathbb{E}_C \mathcal{A}^C(\rho_{DE}) - \mathbb{E}_{C, z_1, \ldots, z_k \sim P_C} \mathcal{B}(\rho_{DE}, z_1, \ldots, z_k) \right\|_{\mathrm{tr}} \leq 2^{-\Omega(n)}, \tag{170}$$

for $k = T^2 \cdot 2^{-\Omega(n)}$. Thus without loss of generality, we may consider the behavior of $\mathcal{B}$.

Next, we show that $\mathcal{B}$'s score can be easily calculated using the probability that the output $z \in \{z_1, \ldots, z_k\}$. More specifically, we show that $\mathcal{B}$'s score is negligibly close to $\frac{1}{N+k} \cdot (1 + \Pr[z \in \{z_1, \ldots, z_k\}])$. Thus, when $\mathcal{B}$'s score is $\frac{1+\delta}{N+k}$, potentially the device and the eavesdropper can coordinate in a way such that the conditional von Neumann entropy using ρ_{DE} with probability negligibly close to δ; otherwise, since the eavesdropper has no information about $z_1, \ldots, z_k$, and each z_i is sampled from P_C, the conditional von Neumann entropy can be bounded by the min-entropy of P_C. Then since with overwhelming probability over C, P_C's min-entropy is $n - \log n - O(1)$, $\mathcal{A}$'s output must have high conditional von Neumann entropy when it wins the protocol for a "typical" C.

7.1 Simulation of a Haar Random Unitary Given Sample Access

In this section, we show that any T-query algorithm for $T = 2^{O(n)}$ outputs a classical-quantum state whose conditional von Neumann entropy is $\delta n - o(n)$, provided it solves the $(1+\delta)$-XHOG problem.

We show that one can simulate an oracle-access algorithm using a sample-access one. For this, we rely on the ideas from Ambainis, Rosmanis and Unruh [9] and from Kretschmer [39].

7.1.1 From a Circuit Oracle to a State-Preparation Oracle

For state $|\psi\rangle$, let C^ψ be a random unitary such that $C^\psi|0\rangle = |\psi\rangle$ and C^ψ is Haar random for the subspace orthogonal to $|0\rangle$, and $\mathcal{O}^\psi$ be a reflection about $|\psi_\perp\rangle = \frac{|\psi\rangle - |\perp\rangle}{\sqrt{2}}$, i.e., it sends $|\psi\rangle \mapsto |\perp\rangle$ and $|\perp\rangle \mapsto |\psi\rangle$ and acts trivially for states orthogonal to states in $\mathrm{span}\{|\psi\rangle, |\perp\rangle\}$.

The first step is to show one can approximate every T-query algorithm given access to C^ψ using an $O(T)$-query algorithm given access to $\mathcal{O}^\psi$ for every $|\psi\rangle$. We prove the following theorem, improving the constant factor of [39, Theorem 19].

Theorem 7.2 (cf. [39, Theorem 19]). *For every quantum state $|\psi\rangle$, every T-query algorithm $\mathcal{A}^{C^\psi}$ can be approximated by a $(2T)$-query quantum algorithm $\mathcal{B}^{\mathcal{O}^\psi}$ such that*

$$\left\| \mathcal{B}^{\mathcal{O}^\psi} - \mathop{\mathbb{E}}_{C^\psi}[\mathcal{A}^{C^\psi}] \right\|_\diamond \leq \frac{4T}{2^{n/2}}. \tag{171}$$

Proof. It suffices to give a simulation of C^ψ using oracle access to $\mathcal{O}^\psi$. The crucial idea from Kretschmer [39] is that if we have access to $\mathcal{O}^{\psi^\perp}$ for any state $|\psi^\perp\rangle$ orthogonal to $|\psi\rangle$, and can prepare $|\psi^\perp\rangle$ with any unitary $V^{\psi^\perp}|0\rangle = |\psi^\perp\rangle$, then

$$|0^n\rangle \xrightarrow{V^{\psi^\perp}} |\psi^\perp\rangle \xrightarrow{\mathcal{O}^\psi} |\psi^\perp\rangle \xrightarrow{\mathcal{O}^{\psi^\perp}} |\perp\rangle \xrightarrow{\mathcal{O}^\psi} |\psi\rangle. \tag{172}$$

Then we consider another unitary $W = |0\rangle\langle 0| \oplus C'$ where C' is a Haar random unitary on the Hilbert space $\mathrm{span}\{|x\rangle : x \neq 0\}$. The sequence of unitaries

$$|0^n\rangle \xrightarrow{W} |0\rangle \xrightarrow{V^{\psi^\perp}} |\psi^\perp\rangle \xrightarrow{\mathcal{O}^\psi} |\psi^\perp\rangle \xrightarrow{\mathcal{O}^{\psi^\perp}} |\perp\rangle \xrightarrow{\mathcal{O}^\psi} |\psi\rangle, \tag{173}$$

$$|x\rangle \xrightarrow{\mathcal{O}^\psi \mathcal{O}^{\psi^\perp} \mathcal{O}^\psi V^{\psi^\perp} W} |\psi_x\rangle, \qquad x \neq 0, \tag{174}$$

satisfying $|\psi_x\rangle$ is a Haar random unitary over spaces spanned by states orthogonal to $|\psi\rangle$ (and of course $|\perp\rangle$). Setting $C^\psi := \mathcal{O}^\psi \mathcal{O}^{\psi^\perp} \mathcal{O}^\psi V^{\psi^\perp} W$ satisfies all the requirements as desired.

However, since we do not know $|\psi\rangle$, we have no access to $|\psi^\perp\rangle$, $V^{\psi^\perp}$ and $\mathcal{O}^{\psi^\perp}$, thus the above maps may not be implemented (without using a large number of queries to $\mathcal{O}^\psi$). Instead, if we sample a Haar random state $|\varphi\rangle$, $\Pr_{|\varphi\rangle}[|\langle\varphi|\psi\rangle| \geq \gamma] \leq e^{-n\gamma^2}$; thus with high probability they are nearly orthogonal. Given the observation, we can sample a haar random state $|\varphi\rangle$, and use $|\varphi\rangle$ in place of $|\psi^\perp\rangle$ for our simulation of C^ψ. Since the state $|\varphi\rangle$ is sampled uniformly instead of a fixed quantum state, we must consider the quantum channel

$$\Phi^\psi(\rho) := \mathop{\mathbb{E}}_{|\varphi\rangle}\left[\mathcal{O}^\psi \mathcal{O}^\varphi \mathcal{O}^\psi V^\varphi \rho (\mathcal{O}^\psi \mathcal{O}^\varphi \mathcal{O}^\psi V^\varphi)^\dagger\right]. \tag{175}$$

and show that Φ^ψ is close to $\mathcal{C}^\psi(\rho) := C^\psi \rho (C^\psi)^\dagger$ in diamond norm.

Let $\mathcal{V}^\varphi$ be the unitary channel of V^φ. To show they are close, by triangle inequality,

$$\|\Phi^\psi - \mathcal{C}^\psi\|_\diamond \leq \left\| \mathop{\mathbb{E}}_{|\varphi\rangle} \mathcal{V}^\varphi - \mathcal{V}^{\psi^\perp} \right\|_\diamond + \left\| \mathop{\mathbb{E}}_{|\varphi\rangle} \mathcal{O}^\varphi - \mathcal{O}^{\psi^\perp} \right\|_\diamond. \tag{176}$$

Since all state $|\psi^\perp\rangle$ behaves equally well for the simulation purpose (i.e., every $|\psi^\perp\rangle$ orthogonal to $|\psi\rangle$ can be used simulates C^ψ exactly), in (176) our choice of $|\psi^\perp\rangle$ can be made to actually depend on $|\varphi\rangle$. More explicitly, we define $|\psi^\perp\rangle \in \mathrm{span}\{|\psi\rangle, |\varphi\rangle\}$ to be the unique orthogonal state to $|\psi\rangle$ (up to a phase). In this case, the diamond norm $\|\mathcal{V}^\varphi - \mathcal{V}^{\psi^\perp}\|_\diamond \le 2|\langle\psi|\varphi\rangle|$. Since $\mathcal{O}^\varphi \mathcal{O}^{\psi^\perp}$ is a rotation by angle 2α for $\alpha = \arccos(\cos^2(\theta/2))$, the eigenvalues are $e^{i2\alpha}, e^{-i2\alpha}, 1$, and

$$
\begin{aligned}
\|\mathcal{O}^\varphi - \mathcal{O}^{\psi^\perp}\|_\diamond &\le 2\sin\alpha \\
&= 2\sqrt{1 - \cos^4(\theta/2)} \\
&= 2\sqrt{1 - \left(\frac{1 + \sqrt{1 - |\varepsilon|^2}}{2}\right)^2} \\
&\le 2|\varepsilon|,
\end{aligned}
\tag{177}
$$

where $\varepsilon = \langle\varphi|\psi\rangle$. The last equality in (177) holds since $\sqrt{1 - x^2} \le 1$ for $x \in [0, 1]$. By (176) and a hybrid argument,

$$
\begin{aligned}
\|\Phi^\psi - \mathcal{C}^\psi\|_\diamond &\le 4 \mathop{\mathbb{E}}_{|\varphi\rangle}[|\langle\psi|\varphi\rangle|] \\
&\le 4 \mathop{\mathbb{E}}_{|\varphi\rangle}[|\langle\varphi|\psi\rangle|^2]^{1/2} \\
&= \frac{4}{2^{n/2}}.
\end{aligned}
\tag{178}
$$

Now let $\mathcal{A}^{C^\psi}$ be a quantum algorithm given access to C^ψ and $\mathcal{B}^{\mathcal{O}^\psi} = \mathcal{A}^{\Phi^\psi}$. By triangle inequality and (178), $\|\mathcal{A}^{C^\psi} - \mathcal{B}^{\mathcal{O}^\psi}\|_\diamond \le \frac{4T}{2^{n/2}}$. Also from (175), $\mathcal{B}^{\mathcal{O}^\psi}$ makes $2T$ queries to $\mathcal{O}^\psi$. $\qquad\square$

In the above analysis, note that the definition of $|\perp\rangle$ is not unique: every state $|\perp\rangle$ orthogonal to $\mathrm{span}\{|z\rangle : z \in \{0,1\}^n\}$ can be used. In particular, we can replace $|\perp\rangle$ with $e^{i\theta}|\perp\rangle$, and the analysis will still go through. Let $\mathcal{O}_\theta^\psi$ be a map $e^{i\theta}|\perp\rangle \mapsto |\psi\rangle, |\psi\rangle \mapsto e^{i\theta}|\perp\rangle$ and acts as the identity for states orthogonal to $|\psi\rangle$ and $|\perp\rangle$. The observation leads to the following corollary.

Corollary 7.3. *Let $|\perp\rangle$ be a fixed state orthogonal to $\mathrm{span}\{|z\rangle : z \in \{0,1\}^n\}$. For $\theta \in [0, 2\pi)$, every quantum state $|\psi\rangle$ and every T-query algorithm $\mathcal{A}^{C^\psi}$, there exists a $(2T)$-query algorithm $\mathcal{B}$ such that*

$$
\left\|\mathcal{B}^{\mathcal{O}_\theta^\psi} - \mathop{\mathbb{E}}_{C^\psi}[\mathcal{A}^{C^\psi}]\right\|_\diamond \le \frac{4T}{2^{n/2}}.
\tag{179}
$$

7.1.2 From Canonical State Preparation Oracles to Resource States

In this section, we apply the idea from Ambainis, Rosmanis and Unruh [9] to show that given resource states that depend on the Haar random state, one can approximate any algorithm given access to the canonical state preparation oracle.

Theorem 7.4 ([9, Theorem 3], paraphrased). *Let $|\psi\rangle$ be a quantum state and $\mathcal{O}^\psi$ be a reflection about $\frac{1}{\sqrt{2}}(|\psi\rangle - |\perp\rangle)$. Let $\mathcal{O}$ be an oracle and ρ be a quantum state. Let $|R^\psi\rangle = |\psi^\ell\rangle \otimes |\alpha_1^\psi\rangle \otimes \ldots \otimes |\alpha_m^\psi\rangle$, where $|\alpha_i^\psi\rangle = \cos(\frac{i\pi}{2k})|\psi\rangle + \sin(\frac{i\pi}{2m})|\perp\rangle$. For every quantum state ρ and algorithm $\mathcal{B}$ that on input ρ and makes T-query to $\mathcal{O}^\psi$, there exists an algorithm $\mathcal{G}$ that on input $\rho, |R\rangle$ makes the same number of queries to $\mathcal{O}$ as $\mathcal{B}$ such that*

$$
\|\mathcal{B}^{\mathcal{O}^\psi, \mathcal{O}}(\rho) - \mathcal{G}^{\mathcal{O}}(\rho, |R^\psi\rangle)\|_{\mathrm{tr}} \le O\left(T\left(\frac{1}{\sqrt{m}} + \frac{1}{\sqrt{\ell}}\right)\right).
\tag{180}
$$

Moreover, (180) holds when $|\psi\rangle$, $\mathcal{O}$ and ρ are not independent.

For a detailed proof, see [9]. Here we provide some intuition. Let S be the left cyclic shift operator and $|\tilde{R}^\psi\rangle = |\alpha_1^\psi\rangle \otimes \ldots \otimes |\alpha_m^\psi\rangle$. One application of S on $|\perp\rangle|\tilde{R}^\psi\rangle$ yields $S|\perp\rangle|\tilde{R}^\psi\rangle = |\tilde{R}^\psi\rangle|\perp\rangle \approx |\psi\rangle|\tilde{R}^\psi\rangle$ since the fidelity

$$|\langle\psi, \tilde{R}^\psi|S|\perp, \tilde{R}^\psi\rangle|^2 = \cos\left(\frac{\pi}{2k}\right)^k \geq \left(1 - \frac{\pi^2}{4k^2}\right)^k \geq 1 - \frac{\pi^2}{4k} \tag{181}$$

implies that the trace distance is $O(k^{-1/2})$. Furthermore, with an ideal resource state where $k \to \infty$, one can give rise to a reflection about $\frac{1}{\sqrt{2}}(|\psi\rangle - |\perp\rangle)$ using control-S, if the reflection R about $|\psi\rangle$ can be implemented. Since $|\psi\rangle$ is unknown, it is not known how to implement R exactly. However, with ℓ copies of $|\psi\rangle$, we can approximate R to diamond distance $O(\ell^{-1/2})$: Let V be the space of $(\ell+1)$-partite states invariant under permutations and M be the projection onto V. For $|\Phi\rangle = |\phi\rangle|T\rangle$ where $|T\rangle = |\psi\rangle^{\otimes\ell}$, if $|\phi\rangle = |\psi\rangle$, $\langle\Phi|M|\Phi\rangle = 1$; for $|\phi\rangle$ orthogonal to $|\psi\rangle$, $\langle\Phi|M|\Phi\rangle \leq O(1/\ell)$. Thus a reflection $\mathbb{1} - 2M$ approximates R to diamond distance $O(1/\sqrt{\ell})$, and after the measurement, the state is disturbed to trace distance $O(\ell^{-1/2})$. Finally, since there are T queries, by a hybrid argument, the overall diamond distance is $O(T(m^{-1/2} + \ell^{-1/2}))$.

For every state $|\psi\rangle$, let the state $|R_\theta^\psi\rangle$ be the same as $|R^\psi\rangle$ except that $|\perp\rangle$ is replaced with $e^{i\theta}|\perp\rangle$, i.e.,

$$|R_\theta^\psi\rangle := |\psi^\ell\rangle \otimes \bigotimes_{i=1}^{k}\left(\cos\left(\frac{i\pi}{2m}\right)|\psi\rangle + \sin\left(\frac{i\pi}{2m}\right)e^{i\theta}|\perp\rangle\right) \tag{182}$$

Since Theorem 7.4 holds if every occurrence of $|\perp\rangle$ is replaced by $e^{i\theta}|\perp\rangle$, we have the following corollary:

Corollary 7.5. *Let $|\psi\rangle$ be a quantum state and $\mathcal{O}_\theta^\psi$ be a reflection about $\frac{1}{\sqrt{2}}(|\psi\rangle - e^{i\theta}|\perp\rangle)$. Let $\mathcal{O}$ be an oracle and ρ be a quantum state. Let $|R_\theta^\psi\rangle$ be defined as in (182). For $\theta \in [0, 2\pi)$, quantum state ρ and every algorithm $\mathcal{B}$ that on input ρ and makes T-query to $\mathcal{O}_\theta^\psi$, there exists an algorithm $\mathcal{G}$ that on input $\rho, |R_\theta^\psi\rangle$ makes the same number of queries to $\mathcal{O}$ as $\mathcal{B}$ such that*

$$\|\mathcal{B}^{\mathcal{O}_\theta^\psi, \mathcal{O}}(\rho) - \mathcal{G}^{\mathcal{O}}(\rho, |R_\theta^\psi\rangle)\|_{\mathrm{tr}} \leq O\left(T\left(\frac{1}{\sqrt{m}} + \frac{1}{\sqrt{\ell}}\right)\right). \tag{183}$$

Moreover, (183) holds when $|\psi\rangle$, $\mathcal{O}$ and ρ are not independent.

Combining Corollary 7.3 and Corollary 7.5, the following corollary holds.

Corollary 7.6. *For quantum state $|\psi\rangle$ and every quantum algorithm $\mathcal{A}$ making T queries to C^ψ, there exists a quantum algorithm $\mathcal{G}$ given access to $|R_\theta^\psi\rangle$ for uniform $\theta \in [0, 2\pi)$ such that*

$$\left\|\mathop{\mathbb{E}}_{C^\psi}\left[\mathcal{A}^{C^\psi}\right] - \mathcal{G}\left(\mathop{\mathbb{E}}_\theta[|R_\theta^\psi\rangle\langle R_\theta^\psi|]\right)\right\|_\diamond \leq O(Tk^{-1/2}) + \frac{4T}{N^{1/2}}. \tag{184}$$

Proof. By Corollary 7.3, for every $\theta \in [0, 2\pi)$ and T-query algorithm $\mathcal{A}^{C^\psi}$, there exists $\mathcal{B}^{\mathcal{O}_\theta^\psi}$ such that their diamond distance is at most $4TN^{-1/2}$. By Corollary 7.5, for every $\theta \in [0, 2\pi)$ and T-query algorithm $\mathcal{B}^{\mathcal{O}_\theta^\psi}$, there exists $\mathcal{G}(|R_\theta^\psi\rangle)$ such that their diamond distance is at most $O(Tm^{-1/2})$ (we set $m = \ell = k/2$ to simplify the expression).

By triangle inequality,

$$\left\| \underset{C^\psi}{\mathbb{E}}\left[\mathcal{A}^{C^\psi}\right] - \mathbb{E}_\theta[\mathcal{G}(|R_\theta^\psi\rangle\langle R_\theta^\psi|)]\right\|_\diamond \leq \underset{\theta}{\mathbb{E}}\left\|\underset{C^\psi}{\mathbb{E}}\left[\mathcal{A}^{C^\psi}\right] - \mathcal{B}^{\mathcal{O}_\theta^\psi}\right\|_\diamond + \underset{\theta}{\mathbb{E}}\left\|\mathcal{B}^{\mathcal{O}_\theta^\psi} - \mathcal{G}(|R^\theta\rangle\langle R^\theta|)\right\|_\diamond$$

$$\leq O(Tk^{-1/2}) + \frac{4T}{N^{1/2}}. \tag{185}$$

By linearity of quantum operations, $\mathbb{E}_\theta\left[\mathcal{G}\left(|R_\theta^\psi\rangle\langle R_\theta^\psi|\right)\right] = \mathcal{G}\left(\mathbb{E}_\theta\left[|R_\theta^\psi\rangle\langle R_\theta^\psi|\right]\right).$ $\qquad\square$

7.1.3 From Resource States to Samples

Now we go from resource states to samples. For random $|\psi\rangle$, we write the state

$$|\psi\rangle = (\sqrt{P_0}e^{i\Theta_0}, \ldots, \sqrt{P_{N-1}}e^{i\Theta_{N-1}}), \tag{186}$$

where $P = (P_0, \ldots, P_{N-1}) \sim \mathrm{Dir}(1^N)$ and each component Θ_i of $\Theta = (\Theta_0, \ldots, \Theta_{N-1})$ are independent random phases, i.e., each Θ_i is sampled according to the uniform distribution over $[0, 2\pi)$. For every distribution P, we denote $|P\rangle := (\sqrt{P_0}, \ldots, \sqrt{P_{N-1}})$ and $|\psi^P\rangle = W|P\rangle$ for a random diagonal phase matrix $W = \mathrm{diag}(W_0, \ldots, W_{N-1}) := e^{i\mathrm{diag}(\Theta)}$. For every $|\psi\rangle$, let $|R_\theta^{P,W}\rangle$ be the associated resource state. In matrix form,

$$|R_\theta^{P,W}\rangle = |\psi^{P,W}\rangle^{\otimes\ell} \otimes \bigotimes_{j=1}^m |\alpha_{i,\theta}^{P,W}\rangle, \tag{187}$$

where $|\alpha_{i,\theta}^{P,W}\rangle := \cos(\frac{\pi i}{2k})|\psi^{P,W}\rangle + \sin(\frac{\pi i}{2k})e^{i\theta}|\bot\rangle$.

Let $\tilde{W} = W + e^{i\theta}|\bot\rangle\langle\bot|$. The state $|R_\theta^{P,W}\rangle$ can be written as

$$|R^{P,\tilde{W}}\rangle := |R_\theta^{P,W}\rangle = (\tilde{W}|P\rangle)^{\otimes\ell} \otimes \bigotimes_{j=1}^k (\tilde{W}|P_i\rangle) \tag{188}$$

We will use the following lemma from [39].

Lemma 7.7 ([39, Lemma 15], paraphrased)**.** *There is an algorithm which prepares*

$$\sigma^P := \underset{\tilde{W}}{\mathbb{E}}\left[|R^{P,W}\rangle\langle R^{P,W}|\right] \tag{189}$$

by measuring $(k + \ell)$ copies of $|\psi\rangle$ in the standard basis.

Let C^P be the following random circuit: Let $V|0\rangle = (\sqrt{P_0}, \ldots, \sqrt{P_{N-1}})$, C' be a Haar random matrix on $\mathrm{span}\{|z\rangle : z \in \{1, \ldots, N-1\}\}$ and $C^P = WVC'$ for random diagonal phase matrix W. We then prove the following theorem.

Theorem 7.8. *For every distribution P, let C^P be a random circuit sampled from the above process. For every algorithm $\mathcal{A}$ making T queries to C^P, there exists a quantum algorithm $\mathcal{F}$ given access to k samples drawn from P such that*

$$\left\|\bar{\mathcal{A}}^P - \bar{\mathcal{F}}^P\right\|_\diamond \leq O(Tk^{-1/2}) + \frac{4T}{N^{1/2}}, \tag{190}$$

where $\bar{\mathcal{A}}^P := \mathbb{E}_{C^P}[\mathcal{A}^{C^P}]$ and $\bar{\mathcal{F}}^P := \mathbb{E}_{z_1,\ldots,z_k \sim P}\mathcal{F}(z_1, \ldots, z_k)$.

Proof. Let $|\psi^P\rangle = \tilde{W}|P\rangle$ for random phase matrix $\tilde{W}$ on $\mathrm{span}\{|0\rangle, \ldots, |N-1\rangle, |\perp\rangle\}$. The channel

$$\underset{C^P}{\mathbb{E}}\left[\mathcal{A}^{C^P}\right] = \underset{\tilde{W}, C^\psi}{\mathbb{E}}\left[\mathcal{A}^{C^\psi}\right]. \tag{191}$$

Let the quantum process in Lemma 7.7 be Φ, the process

$$\begin{aligned}
\underset{\tilde{W}}{\mathbb{E}}\left[\mathcal{G}(|R^{P,\tilde{W}}\rangle\langle R^{P,\tilde{W}}|)\right] &= \mathcal{G}\left(\underset{\tilde{W}}{\mathbb{E}}|R^{P,\tilde{W}}\rangle\langle R^{P,\tilde{W}}|\right) \\
&= \mathcal{G}(\sigma^P) = \underset{z_1,\ldots,z_k \sim P}{\mathbb{E}} \mathcal{G} \circ \Phi(z_1, \ldots, z_k).
\end{aligned} \tag{192}$$

Now let $\mathcal{F} = \mathcal{G} \circ \Phi$. By triangle inequality and Corollary 7.6,

$$\begin{aligned}
\left\|\underset{C^P}{\mathbb{E}}\left[\mathcal{A}^{C^P}\right] - \underset{z_1,\ldots,z_m \sim P}{\mathbb{E}} \mathcal{F}(z_1, \ldots, z_k)\right\|_\diamond &\leq \underset{W}{\mathbb{E}}\left\|\underset{C^\psi}{\mathbb{E}}\left[\mathcal{A}^{C^\psi}\right] - \mathcal{G}\left(\underset{\theta}{\mathbb{E}}|R_\theta^\psi\rangle\langle R_\theta^\psi|]\right)\right\|_\diamond \\
&\leq O(Tk^{-1/2}) + \frac{4T}{N^{1/2}}.
\end{aligned} \tag{193}$$

$\square$

7.2   A Single-Round Analysis

In this section, we prove our main result in Section 7. We show that with probability $1 - N^{-\Omega(1)}$ over the choice of P_C for Haar random C, the conditional von Neumann entropy of any T-query device's output on Eve's information is at least $\Omega(\delta n)$, provided that $T = 2^{O(n)}$ and the device solves b-XHOG for $b \approx 1 + \delta$.

First, we consider a simplified device $\mathcal{F}$ which is only given sample access to P_C and solves b-XHOG. We show this game is equivalent to the following protocol: The verifier samples a distribution $P \sim \mathrm{Dir}(1^N)$, $z_1, \ldots, z_k \sim P$. The verifier sends $z_1, \ldots, z_k$ to the device. Without loss of generality, we may assume that P is revealed to Eve but not all the samples. The device is challenged to return a string z and the verifier accepts if $z \in \{z_1, \ldots, z_k\}$. Recall that if C is Haar random, P_C is distributed according to $\mathrm{Dir}(1^N)$. A detailed description of the protocol is given in Figure 3.

The simplified protocol is equivalent to solving XHOG in the following sense: If the device solves $(2 - \varepsilon')$-XHOG, then the device is accepted in the protocol described in Figure 3 with probability at least $1 - \varepsilon'$ for $\varepsilon' = \varepsilon + O(k^3/N)$. Then, we show that for every device in Figure 3 wins the protocol with probability $1 - \varepsilon'$, the conditional von Neumann entropy is at least $(1 - \varepsilon')n - o(n)$. This implies that the protocol in Figure 3 also certifies the conditional von Neumann entropy.

By Theorem 7.8, any T-query algorithm $\mathcal{A}$ can be well approximated by an algorithm $\mathcal{F}$ that is given only sample access to P_C to diamond distance $\delta = O(Tk^{-1/2})$. Furthermore, we will also show that if $\mathcal{A}$ solves $(2 - \varepsilon)$-XHOG, then $\mathcal{F}$ solves b'-XHOG for $b' = 2 - \varepsilon - \delta$. Combining these results completes our single-round analysis.

7.2.1   A Simplified Device

In this section, we show that for any algorithm $\mathcal{F}$ given k samples drawn from P, the only way that $\mathcal{F}$ has high score is to output one of the given samples. Thus the proof system in Figure 3 is equivalent to solving XHOG.

First, we prove a technical lemma which will be useful later.

Input: security parameter n and number of samples k.

The protocol:

1. Eve and the device $\mathcal{F}$ share an arbitrary entangled state ρ_{DE}.

2. The verifier samples a distribution $P \sim \mathrm{Dir}(1^N)$ (where $N = 2^n$) and samples $z_1, \ldots, z_k \sim P$ which is sent to the device $\mathcal{F}$ (but not to Eve). Moreover, P may be revealed to Eve (but not to the device).

3. The device sends a string z.

4. The verifier accepts if $z \in \{z_1, \ldots, z_k\}$.

Figure 3: A simplified protocol.

Lemma 7.9. *For $P \sim \mathrm{Dir}(1^N)$ and $z_1, \ldots, z_k \sim P$, let $m = (m_0, \ldots, m_{N-1})$ be the frequency vector with $m_z = |\{i \in [k] : z_i = z\}|$. Then m is distributed according to $\Phi(N, k)$, the uniform distribution over frequency vectors that has N elements summing to k.*

Proof. Recall that the probability density function (pdf) of $\mathrm{Dir}(1^N)$ is $f(p) = \Gamma(N)$, where $p = (p_0, \ldots, p_{N-1})$ is any element in the probability simplex. Given a probability distribution p, the probability density that k samples form a frequency vector m is

$$f(m|p) = p_0^{m_0} \ldots p_{N-1}^{m_{N-1}} \frac{\Gamma(k+1)}{\Gamma(m_0+1) \ldots \Gamma(m_{N-1}+1)}. \tag{194}$$

Since the posterior disrbitution is $\mathrm{Dir}(1^N + m)$, the probability density

$$f(p|m) = p_0^{m_0} \ldots p_{N-1}^{m_{N-1}} \frac{\Gamma(N+k)}{\Gamma(m_0+1) \ldots \Gamma(m_{N-1}+1)}. \tag{195}$$

Thus the probability density of m is

$$f(m) = \frac{f(m|p)f(p)}{f(p|m)} = \frac{\Gamma(k+1)\Gamma(N)}{\Gamma(N+k)} = \binom{N+k-1}{k}^{-1}. \tag{196}$$

This means that m is distributed according to the uniform distribution over frequency vectors that has N elements summing to k. $\qquad \square$

The following theorem says that any algorithm $\mathcal{F}$ given k independent samples drawn according to P and solves $\frac{(2-\varepsilon)N}{N+k}$-XHOG, $\mathcal{F}$ must output a given sample with probability at least $1 - \varepsilon - O(k^3/N)$.

Theorem 7.10. *For every quantum channel $\mathcal{F}$, let $\bar{\mathcal{F}}^P(\rho) := \mathbb{E}_{z_1, \ldots, z_k \sim P}[\mathcal{F}(\rho, z_1, \ldots, z_k)]$. If*

$$\mathbb{E}_{P \sim \mathrm{Dir}(1^N)} \mathbb{E}_{z \sim \bar{\mathcal{F}}^P(\rho)} [P_z] \geq \frac{2-\varepsilon}{N+k}, \tag{197}$$

then

$$\Pr_{P \sim \mathrm{Dir}(1^N), z_1, \ldots, z_k \sim P} [\mathcal{F}(\rho, z_1, \ldots, z_k) \in \{z_1, \ldots, z_k\}] \geq 1 - \varepsilon - O\left(\frac{k^3}{N}\right). \tag{198}$$

63

Proof. For each tuple of samples $(z_1, \ldots, z_k)$, let $m = (m_0, \ldots, m_{N-1})$ be the frequency vector. Since there are k samples, $\|m\|_1 = k$. Let $\Phi(N, k)$ be the uniform distribution over possible frequency vectors.

Sampling $m \sim \Phi(N, k)$ can be done with the following process: sample $P \sim \text{Dir}(1^N)$ and $z_1, \ldots, z_k \sim P$; output the frequency vector m. By Lemma 7.9, the frequency vector has infinity norm 1, i.e., $\max_z m_z = 1$, with probability

$$
\begin{aligned}
\Pr_{m \sim \Phi(N,k)}[\|m\|_\infty = 1] &= \frac{\binom{N}{k}}{\binom{N+k-1}{k}} \\
&= \frac{N!(N-1)!}{(N-k)!(N+k-1)!} \\
&= \frac{(N-1)\ldots(N-k+1)}{(N+k-1)\ldots(N+1)} \\
&\geq \left(1 - \frac{k}{N}\right)^{k-1} \\
&= 1 - \frac{O(k^2)}{N}.
\end{aligned}
\tag{199}
$$

The first equality holds by Lemma 7.9 and the fact that the number of frequency vector that has norm 1 is $\binom{N}{k}$. The rest follows by direct calculation.

For every $\mathcal{F}$ that learns $(z_1, \ldots, z_k)$, the posterior distribution $P|m \sim \text{Dir}(1^N + m)$. That is, seeing these samples, the distribution of P to $\mathcal{F}$ is distributed according to $\text{Dir}(1^N + m)$. Thus the expectation

$$
\begin{aligned}
\mathbb{E}_{P \sim \text{Dir}(1^N)}[P_z|m] &= \mathbb{E}_{P \sim \text{Dir}(m+1^N)}[P_z] \\
&= \frac{m_z + 1}{N + k}.
\end{aligned}
\tag{200}
$$

Without loss of generality, the output of any algorithm $\mathcal{F}(z_1, \ldots, z_k, \rho)$ can be described with a distribution $Q(m)$ that only depends on the frequency vector m. For each m, the score of the algorithm is

$$
\mathbb{E}_{z \sim Q(m)} \mathbb{E}_{P \sim \text{Dir}(1^N + m)}[P_z] = \mathbb{E}_{z \sim Q(m)}\left[\frac{m_z + 1}{N + k}\right].
\tag{201}
$$

For each m such that $\|m\|_\infty = 1$,

$$
\mathbb{E}_{z \sim Q(m)} \mathbb{E}_{P \sim \text{Dir}(1^N + m)}[P_z] = \frac{1}{N + k}\left(1 + \Pr_{z \sim Q(m)}[m_z > 0]\right).
\tag{202}
$$

Let γ be the probability that $\|m\|_\infty > 1$ for $m \sim \Phi(N, k)$. From (199), $\gamma = O(k^2/N)$. The score of $\mathcal{F}$ can be calculated with the expectation

$$
\begin{aligned}
&\mathbb{E}_{m \sim \Phi(N,k)} \mathbb{E}_{z \sim Q(m)} \mathbb{E}_{P \sim \text{Dir}(1^N + m)}[P_z] \\
&\leq (1 - \gamma)\frac{1}{N + k}\left(1 + \Pr_{m \sim \Phi(N,k), z \sim Q(m)}[m_z > 0]\right) + \gamma\frac{k + 1}{N + k} \\
&\leq \frac{1}{N + k} + \frac{1}{N + k}\Pr_{m \sim \Phi(N,k), z \sim Q(m)}[m_z > 0] + \frac{O(k^3)}{N(N + k)}.
\end{aligned}
\tag{203}
$$

Thus if the score is at least $\frac{2-\varepsilon}{N+k}$,

$$\Pr_{m\sim\Phi(N,k),z\sim Q(m)}[m_z > 0] \geq 1 - \varepsilon - \frac{O(k^3)}{N}. \tag{204}$$

$\square$

For every P, if $\mathcal{F}$ outputs one of the given samples in the protocol in Figure 3, then it is not difficult to see the von Neumann entropy of $\mathcal{F}$'s output conditioned on Eve's side information is at least $H_{\min}(P)$ up to an $O(\log k)$ additive loss. We show that the entropy lower bound scales linearly in the probability that $\mathcal{F}$ outputs one of the given samples.

Theorem 7.11. *For distribution P over $\{0,1\}^n$, let $\mathcal{F}$ be any algorithm given access to $z_1, \ldots, z_k \sim P$ and the first subsystem of any bipartite state ρ_{DE} and $\bar{\mathcal{F}}(\rho) = \mathbb{E}_{z_1,\ldots,z_k\sim P}[\mathcal{F}(\rho, z_1, \ldots, z_k)]$. If*

$$\Pr_{z_1,\ldots,z_k\sim P}[\mathcal{F}(\rho, z_1, \ldots, z_k) \in \{z_1, \ldots, z_k\}] = 1 - \delta, \tag{205}$$

then

$$H(Z|E)_{\bar{\mathcal{F}}(\rho)} \geq (1-\delta)(H_{\min}(P) - 2\log k) - 2. \tag{206}$$

Proof. We give a lower bound on the von Neumann entropy $H(Z|E)_{\bar{\mathcal{F}}^P(\rho)}$ for random variable $Z \in \{Z_1, \ldots, Z_k\}$ and $Z_1, \ldots, Z_k \sim P$. Here we use uppercase $Z_1, \ldots, Z_k$ to denote the registers or the random variables describing these samples, and lowercase $z_1, \ldots, z_k$ to denote a particular event. We define the classical-quantum state

$$\psi_{Z_1\ldots Z_k ZE} = \sum_{z_1,\ldots z_k} P(z_1)\ldots P(z_k)|z_1, \ldots, z_k\rangle\langle z_1, \ldots, z_k|_{Z_1\ldots Z_k} \otimes \mathcal{F}(\rho, z_1, \ldots, z_k)_{ZE}. \tag{207}$$

By definition, $\bar{\mathcal{F}}^P(\rho) = \mathrm{tr}_{Z_1\ldots Z_k}(\psi)$, and thus $H(Z|E)_{\bar{\mathcal{F}}^P(\rho)} = H(Z|E)_\psi$.

Applying Lemma 3.9 with $A = Z_1 \ldots Z_k$, $B = Z$ and $C = E$,

$$H(Z|E)_\psi \geq H(Z_1\ldots Z_k|E)_\psi - H(Z_1\ldots Z_k|Z)_\psi. \tag{208}$$

Since the register Z is disjoint from $Z_1 \ldots Z_k E$,

$$\mathrm{tr}_Z(\psi) = \sum_{z_1,\ldots,z_k} P(z_1)\ldots P(z_k)|z_1, \ldots, z_k\rangle\langle z_1, \ldots, z_k|_{Z_1\ldots Z_k} \otimes \rho_E, \tag{209}$$

which is product state. Thus we have $H(Z_1\ldots Z_k|E)_\psi = H(Z_1\ldots Z_k)_\psi$, and therefore

$$\begin{aligned} H(Z|E)_\psi &\geq H(Z_1\ldots Z_k)_\psi - H(Z_1\ldots Z_k|Z)_\psi \\ &= I(Z : Z_1, \ldots, Z_k)_\psi. \end{aligned} \tag{210}$$

This means that it suffices to bound the mutual information between Z and $Z_1, \ldots, Z_k$. Now we give a lower bound on $H(Z)_\psi$: Recall that ψ is a quantum state of the form

$$\psi = \sum_{z_1,\ldots,z_k} P(z_1)\ldots P(z_k)|z_1, \ldots, z_k\rangle\langle z_1, \ldots, z_k| \otimes \sum_z Q(z|z_1, \ldots, z_k)|z\rangle\langle z|, \tag{211}$$

for some conditional distribution $Q(\cdot|z_1, \ldots, z_k)$ which may depend on P. We decompose each distribution

$$Q(z|z_1, \ldots, z_k) = Q_1(z|z_1, \ldots, z_k) + Q_0(z|z_1, \ldots, z_k) \tag{212}$$

into two subnormalized distributions $Q_1(\cdot|z_1, \ldots, z_k)$ and $Q_0(|z_1, \ldots, z_k)$ such that the support $\operatorname{supp}(Q_1(\cdot|z_1, \ldots, z_k) \subseteq \{z_1, \ldots, z_k\}$ and $\operatorname{supp}(Q_0(\cdot|z_1, \ldots, z_k)) \cap \{z_1, \ldots, z_k\} = \emptyset$. Let $\delta_{z_1, \ldots, z_k} = \sum_z Q_0(z|z_1, \ldots, z_k)$. By definition, $\mathbb{E}_{z_1, \ldots, z_k \sim P}[\delta_{z_1, \ldots, z_k}] = \delta$. Furthermore, for $b \in \{0, 1\}$, let the normalized distribution

$$\bar{Q}_b(z|z_1, \ldots, z_k) = \frac{1}{p_{b, z_1, \ldots, z_k}} Q_b(z|z_1, \ldots, z_k), \tag{213}$$

where $p_{1, z_1, \ldots, z_k} = 1 - \delta_{z_1, \ldots, z_k}$ and $p_{0, z_1, \ldots, z_k} = \delta_{z_1, \ldots, z_k}$. Now let $(p_0, p_1) = (\delta, 1 - \delta)$. For $b \in \{0, 1\}$, define

$$\psi_b := \frac{1}{p_b} \sum_{z_1, \ldots, z_k} p_{b, z_1, \ldots, z_k} P(z_1) \ldots P(z_k)|z_1, \ldots, z_k\rangle\langle z_1, \ldots, z_k| \otimes \sum_z \bar{Q}_b(z|z_1, \ldots, z_k)|z\rangle\langle z|. \tag{214}$$

We have $\psi = p_0 \psi_0 + p_1 \psi_1$. By Lemma 3.12 and non-negativity of quantum mutual information,

$$I(Z : Z_1 \ldots Z_k)_\psi \geq p_0 I(Z : Z_1 \ldots Z_k)_{\psi_0} + p_1 I(Z : Z_1 \ldots Z_k)_{\psi_1} - h(\delta)$$
$$\geq (1 - \delta) I(Z : Z_1 \ldots Z_k)_{\psi_1} - 1. \tag{215}$$

It suffices to give a lower bound on $I(Z : Z_1 \ldots Z_k)_{\psi_1}$.

Let $\sigma_1 := \operatorname{tr}_{Z_1 \ldots Z_k}(\psi_1)$. By definition,

$$\sigma_1 = \frac{1}{1 - \delta} \sum_{z_1, \ldots, z_k} (1 - \delta_{z_1, \ldots, z_k}) P(z_1) \ldots P(z_k) \sum_z \bar{Q}_1(z|z_1, \ldots, z_k)|z\rangle\langle z|$$

$$\leq \frac{1}{1 - \delta} \sum_{z_1, \ldots, z_k} (1 - \delta_{z_1, \ldots, z_k}) P(z_1) \ldots P(z_k) \sum_z \mathbb{1}[z \in \{z_1, \ldots, z_k\}]|z\rangle\langle z|$$

$$\leq \frac{1}{1 - \delta} \sum_{z_1, \ldots, z_k} (1 - \delta_{z_1, \ldots, z_k}) P(z_1) \ldots P(z_k) \sum_z \sum_{i=1}^k \mathbb{1}[z = z_i]|z\rangle\langle z|. \tag{216}$$

Thus for every $z \in \{0, 1\}^n$,

$$\langle z|\sigma_1|z\rangle \leq \sum_i \frac{1 - \delta_z^{(i)}}{1 - \delta} P(z), \tag{217}$$

where $\delta_z^{(i)} := \mathbb{E}_{z_1, \ldots, z_{i-1}, z_{i+1} \ldots, z_k \sim P}[\delta_{z_1, \ldots, z_k}]$. By definition, $\delta_z^{(i)} \in [0, 1]$, and thus $\langle z|\sigma_1|z\rangle \leq \frac{k}{1-\delta} \max_z P(z)$. This implies that

$$H(Z)_{\psi_1} \geq H_{\min}(Z)_{\sigma_1} \geq H_{\min}(P) - \log k + \log(1 - \delta). \tag{218}$$

Next we consider the quantity $H(Z|Z_1 \ldots Z_k)_{\psi_1}$: By definition,

$$H(Z|Z_1 \ldots Z_k)_{\psi_1} = \frac{1}{1 - \delta} \sum_{z_1, \ldots, z_k} (1 - \delta_{1, z_1, \ldots, z_k}) P(z_1) \ldots P(z_k) H(\bar{Q}_1(\cdot|z_1, \ldots, z_k)) \tag{219}$$

66

Since $\bar{Q}_1(\cdot|z_1,\ldots,z_k)$ has support in $\{z_1,\ldots,z_k\}$, for every $z_1,\ldots,z_k$,

$$S(\bar{Q}_1(\cdot|z_1,\ldots,z_k)) \leq \log k. \tag{220}$$

This gives

$$H(Z|Z_1\ldots Z_k)_{\psi_1} \leq \log k. \tag{221}$$

Combining (210), (215), (218) and (221),

$$\begin{aligned}
H(Z|E)_\psi &\geq (1-\delta)I(Z:Z_1\ldots Z_k)_{\psi_1} - 1 \\
&\geq (1-\delta)(H_{\min}(P) - 2\log k) + (1-\delta)\log(1-\delta) - 1 \\
&\geq (1-\delta)(H_{\min}(P) - 2\log k) - 2.
\end{aligned} \tag{222}$$

The last inequality holds since $-(1-\delta)\log(1-\delta) \leq h(\delta) \leq 1$. $\qquad\square$

Theorem 7.11 says that the von Neumann entropy depends on the probability that the device's output $z \in \{z_1,\ldots,z_k\}$. For $P \sim \mathrm{Dir}(1^N)$, by Lemma 3.14, with overwhelming probability, $S_{\min}(P) \geq n - \log n - O(1)$. We now use the notation

$$H(Z|PE)_\psi := \mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N)}\Big[H(Z|E)_{\bar{\mathcal{F}}^P(\rho)}\Big], \tag{223}$$

where ψ is the joint output classical-quantum state, defined by

$$\psi = \mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N)}\big[|P\rangle\langle P| \otimes \bar{\mathcal{F}}^P(\rho)\big], \tag{224}$$

even though P is not sampled from a finite set. We then show the following theorem.

Corollary 7.12. *For $P \sim \mathrm{Dir}(1^N)$, let $\mathcal{F}$ be any algorithm given access to $z_1,\ldots,z_k \sim P$ and the first subsystem of any bipartite state ρ_{DE}, and $\bar{\mathcal{F}}^P(\rho) = \mathbb{E}_{z_1,\ldots,z_k\sim P}[\mathcal{F}(\rho,z_1,\ldots,z_k)]$. If*

$$\mathop{\mathrm{Pr}}_{P\sim\mathrm{Dir}(1^N),z_1,\ldots,z_k\sim P}[\mathcal{F}(\rho,z_1,\ldots,z_k) \in \{z_1,\ldots,z_k\}] \geq 1-\varepsilon, \tag{225}$$

then

$$H(Z|PE)_\psi \geq (1-\varepsilon)n - \log n - 2\log k - O(1), \tag{226}$$

where ψ is the state defined in (224).

Proof. The corollary is a direct consequence of Theorem 7.11. Let the error probability for P be ε_P. By Theorem 7.11,

$$\begin{aligned}
H(Z|E)_{\bar{\mathcal{F}}^P(\rho)} &\geq (1-\varepsilon_P)H_{\min}(P) - 2\log k \\
&\geq H_{\min}(P) - \varepsilon_P n - 2\log k.
\end{aligned} \tag{227}$$

By Lemma 3.13,

$$\begin{aligned}
H(Z|PE)_\psi &\geq \mathop{\mathbb{E}}_{P\sim\mathrm{Dir}(1^N)}[H_{\min}(P)] - \mathop{\mathbb{E}}_{P}[\varepsilon_P]n - 2\log k \\
&\geq (1-\varepsilon)n - \log n - 2\log k - O(1).
\end{aligned} \tag{228}$$

$\qquad\square$

Combining Theorem 7.10 and Corollary 7.12, we conclude that any $\bar{\mathcal{F}}$ solving $(1+\delta)$-XHOG has conditional von Neumann entropy $n - o(n)$.

Corollary 7.13. *Let $\mathcal{F}$ be any device given access to k samples from $P = P_C$ for $C \sim \mathrm{Haar}(N)$. If $\mathcal{F}$ solves $(1+\delta)$-XHOG, then*

$$H(Z|PE)_\psi \geq \big(\delta - O(k^3/N)\big)n - \log n - 2\log k - O(1). \tag{229}$$

7.2.2 The Analysis of a General Device

Given the analysis of the protocol in Figure 3 and the closeness of a general device and the simplified device, we show that any device must exhibit a von Neumann entropy lower bound if it solves XHOG.

Theorem 7.14. *For every T-query device $\mathcal{A}$ that solves b-XHOG, there exists a device $\mathcal{F}$ given access to k samples such that $\mathcal{F}$ solves b'-XHOG for $b' \geq b - O(nTk^{-1/2})$.*

Proof. For every $\mathcal{A}^P$, by Theorem 7.8, there exists $\mathcal{F}^P$ such that

$$\left| \mathop{\mathbb{E}}_{z \sim \bar{\mathcal{A}}^P(\rho)}[P_z] - \mathop{\mathbb{E}}_{z \sim \bar{\mathcal{F}}^P(\rho)}[P_z] \right| = \left| \sum_z P_z(p_\mathcal{A}(z) - p_\mathcal{F}(z)) \right|$$

$$\leq \max_z P_z \sum_z |p_A(z) - p_F(z)|$$

$$\leq \max_z P_z \cdot \|\bar{\mathcal{A}}^P(\rho) - \bar{\mathcal{F}}^P(\rho)\|_{\mathrm{tr}}$$

$$\leq \max_z P_z \cdot (O(Tk^{-1/2}) + O(TN^{-1/2})). \tag{230}$$

Taking the expectation over $P \sim \mathrm{Dir}(1^N)$, the upper bound is at most $O(nT(k^{-1/2} + N^{-1/2})/N)$ by Lemma 3.13. This implies that if $\mathcal{A}$ solves b-XHOG, then $\mathcal{F}$ solves $(b - O(nTk^{-1/2} + nTN^{-1/2}))$-XHOG. $\qquad\square$

Theorem 7.14 shows that the score of any device $\mathcal{A}$ and its simplified version $\mathcal{F}$ must be close if $\mathcal{F}$ is given sufficiently many samples. Given this fact, we prove the following theorem.

Theorem 7.15. *Let $\mathcal{A}$ be any algorithm making T queries to a Haar random unitary C. If $\mathcal{A}$ solves $(1+\delta)$-XHOG, then there exists a state ψ which is $O(Tk^{-1/2})$-close to $\mathcal{A}$'s output classical-quantum state such that*

$$H(Z|CE)_\psi \geq \Big(\delta - O(k^3/N) - O(nTk^{-1/2} + nTN^{-1/2})\Big)n - \log n - 2\log k - O(1). \tag{231}$$

Proof. By Theorem 7.8, for every T-query $\mathcal{A}$, there exists $\mathcal{F}$ given access to k samples (drawn according to $P \sim \mathrm{Dir}(1^N)$) such that $\|\bar{\mathcal{A}}^P - \bar{\mathcal{F}}^P\|_\diamond \leq O(Tk^{-1/2})$. Also by Theorem 7.14, $\mathcal{F}$ solves b-XHOG for $b = 1 + \delta - O(nTk^{-1/2})$. By Corollary 7.13,

$$H(Z|PE)_\psi \geq \Big(\delta - O(k^3/N) - O(nTk^{-1/2} + nTN^{-1/2})\Big)n - \log n - 2\log k - O(1), \tag{232}$$

where ψ_{ZPE} is $\mathcal{F}$'s output state defined in (224) and is $O(Tk^{-1/2})$-close to $\mathcal{A}$'s output. Finally, by Theorem 7.1, we conclude the proof. $\qquad\square$

Input: security parameter n, the number of rounds m, the score parameter $\delta \in [0,1]$, the fraction of circuit updates $\gamma = O((\log n)/m)$, and the fraction of test rounds $\eta = O((n^2 \log n)/m)$.

The protocol:

1. For $i = 1, \ldots, m$, run the following steps:

    (a) The verifier samples $T_i \sim \mathsf{Bernoulli}(\gamma)$, and $F_i \sim \mathsf{Bernoulli}(\eta)$. If $T_{i-1} = 1$ or $i = 1$, the device chooses a fresh circuit $C_i \sim \mathrm{Haar}(N)$. Otherwise, if $T_{i-1} = 0$ and $i > 1$, then the device sets $C_i = C_{i-1}$ to be the circuit used in the previous round. The verifier sends C_i to the device.

    (b) The prover returns a sample z_i.

2. Let the number of epoches, i.e., the set of consecutive rounds i such that the same circuit $C_i = C$ is used, be t. For each epoch E_j, let $t_j = |\{i \in E_j : F_i = 1\}|$ denote the number of test rounds in this epoch. The verifier computes

$$s_j = \frac{1}{t_j} \sum_{i \in E_j : T_i = 1} p_{C_i}(z_i). \tag{234}$$

If $\frac{1}{t} \sum_{j=1}^{t} \delta[s_j \geq (1+\delta)/N] \geq 0.99$, then the verifier accepts and outputs $(z_1, \ldots, z_m)$ to the quantum-proof randomness extractor.

Figure 4: The entropy accumulation protocol.

By Theorem 7.15, for constant δ, every algorithm solving $(1+\delta)$-XHOG outputs a sample of conditional von Neumann entropy $o(n)$ must make $N^{\Omega(\delta)}$ queries. For devices making $\mathrm{poly}(n)$ queries, Theorem 7.15 implies the following corollary.

Corollary 7.16. *For $T = \mathrm{poly}(n)$, $\delta = \Omega(1)$, and $\eta \in (0,1]$, every algorithm T-query algorithm which solves $(1+\delta)$-XHOG must output a sample Z satisfying*

$$H(Z|CE)_\psi \geq (1-\eta)\delta n - O(\log n), \tag{233}$$

where ψ is a quantum state $N^{-\Omega(\delta\eta)}$-close to $\mathcal{A}$'s output state.

Proof. By Theorem 7.15, choosing $k = T^2 N^{\delta\eta}$, $Tk^{-1/2} = N^{-\delta\eta/2}$ and $k^3/N = n^{O(1)} \cdot N^{-1+3\delta\eta}$. This implies the von Neumann entropy has lower bound $(1-\eta)\delta n - O(\log n)$. □

7.3 Entropy Accumulation

We present our entropy accumulation protocol in Figure 4. By the entropy accumulation theorem shown in Section 4, we prove the following lower bound on the conditional min-entropy.

Theorem 7.17. *Let $\mathcal{A}_1, \ldots, \mathcal{A}_m$ be $n^{O(1)}$-query sequential processes given access to the first system of a bipartite state ρ_{DE} and outputting $z_1, \ldots, z_m$ solving $\mathrm{LXEB}_{1+\delta,k}$ with probability p. Then*

$$H_{\min}^{\varepsilon + m\varepsilon'}(Z^m | C^m T^m E)_{\mathcal{A}_m \circ \ldots \mathcal{A}_1(\rho)|\Omega} \geq n\left(0.99\delta m - c\sqrt{m} - o(1)\right) \tag{235}$$

where $\varepsilon' = 2^{-\Omega(n)}$ and Ω denotes the event of non-aborting. The parameter $c := 3.99(1 + \log(\frac{1}{p\varepsilon}))^{1/2}$.

Proof. We apply the entropy accumulation theorem shown in Section 4. In particular, we choose $G := N \sum_z |z\rangle\langle z| P(z)$. By Corollary 7.16, we choose $f(\delta) = (1 - \eta)\delta n - O(\log n)$ for $\eta = 0.01$ for concreteness. This gives $\|\nabla f\|_\infty = 0.99n$. Then we have

$$\begin{aligned} V &= 2(\log(2d_Z + 1) + \|\nabla f\|_\infty) \\ &= 2(\log(2N + 1) + 0.99n) \\ &= 3.98n + O(1) \\ &\leq 3.99n. \end{aligned} \tag{236}$$

Now we have

$$H_{\min}^{\varepsilon + m\varepsilon'}(Z^m | C^m T^m E)_{\mathcal{A}_m \circ \dots \circ \mathcal{A}_1(\rho)|\Omega} \geq n\left(0.99\delta m - O\left(\frac{\log n}{n}\right) - 3.99\sqrt{m}\sqrt{\log \frac{2}{\Pr_\sigma[\Omega]^2 \varepsilon^2}}\right). \tag{237}$$

$\square$

8 Pseudorandomness and Statistical Zero-Knowledge

To produce a net gain in randomness, we must derandomize the challenge circuits in our protocols Figure 1 and Figure 4. However, existing quantum-secure pseudorandom function was not known to be secure for certified randomness since the security only holds against quantum polynomial-time adversaries. In Section 8.1, we define a stronger security notion for pseudorandom functions sufficient for certified randomness, and show there exists a construction relative to a random oracle. Then in Section 8.3, with the pseudorandom function, polynomial expansion can be achieved.

In this section, we show that a pseudorandom function against quantum statistical zero-knowledge protocols is sufficient for certified randomness. The same argument also applies to pseudorandom unitaries.

By Theorem 3.6 with an extension to oracle distributions, two oracle distributions $\mathcal{D}_0, \mathcal{D}_1$ are said to be QSZK-distinguishable if there exists a pair of algorithms $\mathcal{A}, \mathcal{B}$ such that if $\mathbb{E}_{F \sim \mathcal{D}_0} \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}}$ and $\mathbb{E}_{F \sim \mathcal{D}_1} \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}}$ are far apart.

Definition 8.1 (QSZK-distinguishability)**.** *Two oracle distributions are said to be* QSZK-*distinguishable if there exist a pair of algorithms $\mathcal{A}, \mathcal{B}$ and a polynomial p such that*

$$\left| \mathop{\mathbb{E}}_{F \sim \mathcal{D}_0} \|\mathcal{A}^{\mathcal{F}} - \mathcal{B}^F\|_{\mathrm{tr}} - \mathop{\mathbb{E}}_{F \sim \mathcal{D}_0} \|\mathcal{A}^{\mathcal{F}} - \mathcal{B}^F\|_{\mathrm{tr}} \right| > \frac{1}{p(n)}. \tag{238}$$

If no such algorithms exist, then the distributions are said to be QSZK-*indistinguishable.*

Definition 8.1 strengthens the definition against BQP adversaries by Zhandry [64]: Two oracle distributions $\mathcal{D}_0, \mathcal{D}_1$ are said to be distinguishable if there exists an algorithm $\mathcal{A}$ which outputs one with probability far apart, i.e.,

$$\left| \mathop{\Pr}_{F \sim \mathcal{D}_0} [\mathcal{A}^F = 1] - \mathop{\Pr}_{F \sim \mathcal{D}_1} [\mathcal{A}^F = 1] \right| > \frac{1}{\mathrm{poly}(n)}. \tag{239}$$

For clarity, in this paper, we will say $\mathcal{D}_0, \mathcal{D}_1$ are standard-distinguishable if there exists $\mathcal{A}$ such that (239) holds. To see why Definition 8.1 is a stronger definition, we prove the following theorem.

Theorem 8.2. *If two oracle distributions $\mathcal{D}_0, \mathcal{D}_1$ are standard-distinguishable, then they are* QSZK-*distinguishable.*

Proof. Since $\mathcal{D}_0, \mathcal{D}_1$ are standard-distinguishable, there exists $\mathcal{A}$ which outputs a single bit such that (239) holds. Then consider a trivial algorithm $\mathcal{B}$ which outputs 0 with probability 1. This implies that

$$\underset{F \sim \mathcal{D}_b}{\mathbb{E}} \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} = \underset{F \sim \mathcal{D}_b}{\Pr} [\mathcal{A}^F = 1], \tag{240}$$

and (238) holds. $\qquad\square$

8.1   Pseudorandom Functions

It is known that there is a construction of a pseudorandom function standard-indistinguishable from a random function. As we do not know if the converse of Theorem 8.2 holds, we propose the following assumption.

Assumption 8.3 (Pseudorandom function assumption). *Let $\kappa \in \mathbb{N}$ be the security parameter and ℓ, m be polynomially bounded functions. There exists a keyed function $F : \{0,1\}^{\ell(\kappa)} \times \{0,1\}^{m(\kappa)} \to \{0,1\}$ such that the following conditions hold.*

- *$F(k, x)$ can be computed in polynomial time for every $k \in \{0,1\}^{\ell(\kappa)}$ and $x \in \{0,1\}^{m(\kappa)}$.*

- *For every pair of quantum algorithms $\mathcal{A}, \mathcal{B}$, it holds that*

$$\left| \underset{k \sim \mathcal{K}_{\ell(\kappa)}}{\mathbb{E}} \|\mathcal{A}^{F_k} - \mathcal{B}^{F_k}\|_{\mathrm{tr}} - \underset{F \sim \mathcal{F}_{m(\kappa)}}{\mathbb{E}} \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} \right| \leq \mathrm{negl}(\kappa) \tag{241}$$

for sufficiently large κ, where $\mathcal{F}_m$ is the uniform distribution over m-bit Boolean functions and $\mathcal{K}_\ell$ is the uniform distribution over $\{0,1\}^\ell$.

In this section, we prove that Assumption 8.3 holds relative to a random oracle: For $\kappa = n$, $m(n) = n$, let $\mathcal{O} : \{0,1\}^{\ell+n} \to \{0,1\}$ be a random function and $\mathcal{O}_k(x) := \mathcal{O}(k, x)$ for $k \in \{0,1\}^\ell$ and $x \in \{0,1\}^n$. The key length ℓ is to be determined later. We show that for every pair of $\mathrm{poly}(n)$-query algorithms $\mathcal{A}$ and $\mathcal{B}$, $\mathcal{O}, \mathcal{O}_k$ for uniform $k \in \{0,1\}^\ell$ is indistinguishable from $\mathcal{O}, H$ for random $H : \{0,1\}^n \to \{0,1\}$.

Recall that for a random function $H : \{0,1\}^n \to \{0,1\}$ and $x \in \{0,1\}^n$, $H(x)$ is a fair coin independent from $H(x')$ for every $x' \neq x$. We will also say a distribution $\mathcal{D}$ over n-bit Boolean functions is a ε-biased random function if for $F \sim \mathcal{D}$, the random variables in $\{F(x) : x \in \{0,1\}^n\}$ are independent, and for each $x \in \{0,1\}^n$, the marginal distribution of F on x satisfies $|\Pr_{F \sim \mathcal{D}}[F(x) = 1] - 1/2| \leq \varepsilon$. First we prove the following lemma which states that for the uniform distribution $\mathcal{U}_\ell$ over $\{0,1\}^\ell$ and every $x \in \{0,1\}^n$, $\mathbb{E}_{k \sim \mathcal{U}_\ell} \mathcal{O}_k(x)$ is weakly biased under uniform k.

Lemma 8.4. *For integer m, let $\mathcal{F}_m$ be the uniform distribution over functions $\{0,1\}^m \to \{0,1\}$. Then*

$$\underset{\mathcal{O} \sim \mathcal{F}_{\ell+n}}{\Pr} \left[\forall x \in \{0,1\}^n, \left| \underset{k \sim \mathcal{U}_\ell}{\mathbb{E}} \mathcal{O}_k(x) - 1/2 \right| \leq \varepsilon \right] \geq 1 - 2 \cdot 2^N e^{-L\varepsilon^2}. \tag{242}$$

Proof. By Hoeffding's inequality, for every x,

$$\Pr_{\mathcal{O}\sim\mathcal{F}_{\ell+n}}\left[\left|\underset{k\sim\mathcal{U}_\ell}{\mathbb{E}}\,\mathcal{O}_k(x) - 1/2\right| \le \varepsilon\right] \ge 1 - 2e^{-L\varepsilon^2}. \tag{243}$$

By a union bound, we conclude the proof. $\qquad\square$

Fix a function $\mathcal{O}$ that satisfies this likely event. Since for each $k \in \{0,1\}^\ell$, $\{\mathcal{O}_k(x) : x \in \{0,1\}^n\}$ are independent, $\mathcal{O}_k$ under uniform k is an ε-biased random function. The following lemma shows that no pair of T-query algorithms can distinguish a slightly biased random function from a random function with advantage $O(T\sqrt{\varepsilon})$ for the difference in biases ε.

Lemma 8.5. *Let $\mathcal{A}$ and $\mathcal{B}$ be two T-query algorithms given access to an oralce sampled from either $\mathcal{D}_0$ or $\mathcal{D}_1$ such that for every $x \in \{0,1\}^\ell$, $|\Pr_{F\sim\mathcal{D}_0}[F(x)=1] - \Pr_{F\sim\mathcal{D}_1}[F(x)=1]| \le \varepsilon$. Then*

$$\left|\underset{F\sim\mathcal{D}_0}{\mathbb{E}}\,\|\mathcal{A}^F - B^F\|_{\mathrm{tr}} - \underset{F\sim\mathcal{D}_1}{\mathbb{E}}\,\|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}}\right| \le 16T\sqrt{\varepsilon}. \tag{244}$$

Proof. For $b \in \{0,1\}$ and $x \in \{0,1\}^n$, let $p_b(x) := \Pr_{F\sim\mathcal{D}_b}[F(x)=1]$. By definition, $\varepsilon(x) := p_0(x) - p_1(x)$ satisfies $|\varepsilon(x)| \le \varepsilon$. Then we consider the following hybrid distribution $\mathcal{R}$ defined as follows: For each x, let

$$\Pr_{F\sim\mathcal{R}}[F(x)=1] = \frac{\min\{p_0(x), p_1(x)\}}{1 - |\varepsilon(x)|}. \tag{245}$$

Also for $b \in \{0,1\}$, define the following difference distributions $\mathcal{T}_b$

$$\Pr_{F\sim\mathcal{T}_b}[F(x)=1] = \begin{cases} 1 & \text{if } p_b(x) > p_{1-b}(x) \\ 0 & \text{if } p_b(x) < p_{1-b}(x) \\ 1/2 & \text{otherwise.} \end{cases} \tag{246}$$

For every $x \in \{0,1\}^n$,

$$\Pr_{F\sim\mathcal{D}_b}[F(x)=1] = (1 - |\varepsilon(x)|)\Pr_{F\sim\mathcal{R}}[F(x)=1] + |\varepsilon(x)|\Pr_{F\sim\mathcal{T}_b}[F(x)=1]. \tag{247}$$

That is, sampling $F \sim \mathcal{D}_b$ can be done using the following process: For each $x \in \{0,1\}^n$, first sample $X \in \{0,1\}$ according to the distribution $\Pr[X=1] = \Pr_{F\sim\mathcal{R}}[F(x)=1]$. Then with probability $1 - |\varepsilon(x)|$, outputs X; with probability $|\varepsilon(x)|$, output 1 with probability $\Pr_{F\sim\mathcal{T}_b}[F(x)=1]$. Thus $\mathcal{D}_b$ can be viewed as the distribution $\mathcal{R}$ with modification on each x with probability at most $|\varepsilon(x)|$.

Thus the rest of the proof is devoted to showing that for $b \in \{0,1\}$,

$$\left|\underset{F\sim\mathcal{D}_b}{\mathbb{E}}\,\|\mathcal{A}^F - B^F\|_{\mathrm{tr}} - \underset{F\sim\mathcal{R}}{\mathbb{E}}\,\|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}}\right| \le 8T\sqrt{\varepsilon}. \tag{248}$$

For every T-query algorithm $\mathcal{A}$ given oracle access to $F \sim \mathcal{D}_b$ described by unitaries $U_0, \ldots, U_T$, we use the above sampling process to get $F = F_0 \oplus \Delta$ where $F_0 \sim \mathcal{R}$ and Δ is a biased random function where for each $x \in \{0,1\}^n$, $\Delta(x) = 1$ with probability at most $|\varepsilon(x)|$. For $b \in \{0,1\}$, let the distribution of Δ be $\mathcal{P}_b$. For every $F_0, \Delta : \{0,1\}^n \to \{0,1\}$, consider the following hybrids:

$$|\phi_T^\Delta\rangle = U_T\mathcal{O}(F_0)U_{T-1}\mathcal{O}(F_0)\ldots\mathcal{O}(F_0)U_1\mathcal{O}(F_0)U_0|0\rangle,$$
$$|\phi_{T-1}^\Delta\rangle = U_T\mathcal{O}(F)U_{T-1}\mathcal{O}(F_0)\ldots\mathcal{O}(F_0)U_1\mathcal{O}(F_0)U_0|0\rangle,$$
$$\vdots$$
$$|\phi_0^\Delta\rangle = U_T\mathcal{O}(F)U_{T-1}\mathcal{O}(F)\ldots\mathcal{O}(F)U_1\mathcal{O}(F_0)U_0|0\rangle,$$
$$|\phi_0^\Delta\rangle = U_T\mathcal{O}(F)U_{T-1}\mathcal{O}(F)\ldots\mathcal{O}(F)U_1\mathcal{O}(F)U_0|0\rangle. \tag{249}$$

72

That is, the state $|\phi_t^x\rangle$ is obtained by making t queries to F_0 followed by $T - t$ queries to F. Also let $|\psi_t^0\rangle = U_t \mathcal{O}(F_0) \dots U_1 \mathcal{O}(F_0) U_0 |0\rangle$, which is independent of Δ.

For every function $\Delta : \{0, 1\}^n \to \{0, 1\}$, let P_Δ denote the projector onto the subspace $\{x : \Delta(x) = 1\}$. By triangle inequality,

$$\||\phi_0^\Delta\rangle - |\phi_T^\Delta\rangle\| \leq \sum_{t=0}^{T-1} \|\mathcal{O}(F)|\psi_t^0\rangle - \mathcal{O}(F_0)|\psi_t^0\rangle\|$$

$$= 2 \sum_{t=0}^{T-1} \|P_\Delta|\psi_t^0\rangle\|. \tag{250}$$

Since $\Delta(x) = 1$ with probability at most ε, $\mathbb{E}_\Delta P_\Delta \leq \varepsilon \mathbb{1}$, and

$$\underset{\Delta \sim \mathcal{P}_b, F_0 \sim \mathcal{R}}{\mathbb{E}} \|\mathcal{A}^{F_0 \oplus \Delta} - \mathcal{A}^{F_0}\|_{\mathrm{tr}} \leq 2 \underset{\Delta \sim \mathcal{P}_b, F_0 \sim \mathcal{R}}{\mathbb{E}} \||\phi_0^\Delta\rangle - |\phi_T^\Delta\rangle\|$$

$$\leq 4T \underset{F_0 \sim \mathcal{R}}{\mathbb{E}} \|Q\|_{\mathrm{op}}^{1/2}$$

$$\leq 4T\sqrt{\varepsilon}. \tag{251}$$

where $Q = \mathbb{E}_\Delta P_\Delta$. Since the same bound holds for $\mathcal{B}$,

$$\left| \underset{F \sim \mathcal{D}_b}{\mathbb{E}} \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} - \underset{F \sim \mathcal{R}}{\mathbb{E}} \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} \right|$$

$$= \left| \underset{F \sim \mathcal{R}}{\mathbb{E}} \left(\underset{\Delta \sim \mathcal{P}_b}{\mathbb{E}} \|\mathcal{A}^{F \oplus \Delta} - \mathcal{B}^{F \oplus \Delta}\|_{\mathrm{tr}} - \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} \right) \right|$$

$$\leq \underset{F \sim \mathcal{R}}{\mathbb{E}} \left(\underset{\Delta \sim \mathcal{P}_b}{\mathbb{E}} \|\mathcal{A}^{F \oplus \Delta} - \mathcal{A}^F\|_{\mathrm{tr}} + \underset{\Delta \sim \mathcal{P}_b}{\mathbb{E}} \|\mathcal{B}^{F \oplus \Delta} - \mathcal{B}^F\|_{\mathrm{tr}} \right)$$

$$\leq 8T\sqrt{\varepsilon}. \tag{252}$$

The first inequality holds by triangle inequality, and the second holds from (251). $\qquad \square$

Combining Lemma 8.4 and Lemma 8.5, we prove the following theorem.

Theorem 8.6. *For $\ell \geq 2n$, $L = 2^\ell$, and every pair of T-query algorithms $\mathcal{A}, \mathcal{B}$,*

$$\underset{\mathcal{O} \sim \mathcal{F}_{\ell+n}}{\mathrm{Pr}} \left[\left| \underset{k \sim \mathcal{U}_\ell}{\mathbb{E}} \|\mathcal{A}^{\mathcal{O}, \mathcal{O}_k} - \mathcal{B}^{\mathcal{O}, \mathcal{O}_k}\|_{\mathrm{tr}} - \underset{H \sim \mathcal{F}_n}{\mathbb{E}} \|\mathcal{A}^{\mathcal{O}, H} - \mathcal{B}^{\mathcal{O}, H}\|_{\mathrm{tr}} \right| > 16TN^{-1/4} \right] \leq 2^{-\Omega(N)}, \tag{253}$$

where $\mathcal{U}_\ell$ is the uniform distribution over $\{0, 1\}^\ell$ and $\mathcal{F}_m$ is the uniform distribution over $\{0, 1\}^m \to \{0, 1\}$.

Proof. For $\ell \geq 2n$, $L = 2^\ell$, and $\varepsilon = N^{-1/2}$, $L \geq N^2$ and $2 \cdot 2^N e^{-L\varepsilon^2} = 2 \cdot 2^N e^{-L/N} \leq 2^{-\Omega(N)}$. By Lemma 8.5,

$$\underset{\mathcal{O} \sim \mathcal{F}_{\ell+n}}{\mathrm{Pr}} \left[\left| \underset{k \sim \mathcal{U}_\ell}{\mathbb{E}} \|\mathcal{A}^{\mathcal{O}, \mathcal{O}_k} - \mathcal{B}^{\mathcal{O}, \mathcal{O}_k}\|_{\mathrm{tr}} - \underset{H \sim \mathcal{F}_n}{\mathbb{E}} \|\mathcal{A}^{\mathcal{O}, H} - \mathcal{B}^{\mathcal{O}, H}\|_{\mathrm{tr}} \right| \leq 16TN^{-1/4} \right]$$

$$\geq \underset{\mathcal{O} \sim \mathcal{F}_{\ell+n}}{\mathrm{Pr}} \left[\forall x \in \{0, 1\}^n, \left| \underset{k}{\mathbb{E}} \mathcal{O}_k(x) - 1/2 \right| \leq N^{-1/2} \right]$$

$$\geq 1 - 2 \cdot 2^N e^{-L/N}$$

$$\geq 1 - 2^{-\Omega(N)}. \tag{254}$$

$\qquad \square$

By the Borel-Cantelli Lemma, every pair of poly(n)-query algorithms breaks the conditions in Assumption 8.3 infintely often with probability 0.

Corollary 8.7. *Assumption 8.3 holds relative to a random oracle with probability 1.*

8.2 Pseudorandom Unitaries

Similarly, we assume that there exists a pseudorandom unitary and give a construction relative to an oracle. The construction is the same as the one given by Kretschmer [38], and we strengthen the hardness to QSZK.

Assumption 8.8 (Pseudorandom unitary assumption). *Let $\kappa \in \mathbb{N}$ be the security parameter, ℓ, m be polynomially bounded functions. There exists a family of keyed unitaries $\{U_k \in \mathbb{U}(2^{m(\kappa)}) : k \in \{0,1\}^{\ell(\kappa)}\}$ such that the following conditions hold.*

- *There exists a polynomial-time quantum algorithm G that implements U_k on input $k \in \{0,1\}^{\ell(\kappa)}$, i.e., on input k and quantum state $|\psi\rangle \in \mathbb{S}(2^{m(\kappa)})$, $G(k, |\psi\rangle) = U_k|\psi\rangle$.*

- *For every pair of quantum algorithms $\mathcal{A}, \mathcal{B}$ that makes poly(κ) queries, it holds that*

$$\left| \mathop{\mathbb{E}}_{k \sim \mathcal{K}_{\ell(\kappa)}} \|\mathcal{A}^{U_k} - \mathcal{B}^{U_k}\|_{\mathrm{tr}} - \mathop{\mathbb{E}}_{U \sim \mathrm{Haar}(2^{m(\kappa)})} \|\mathcal{A}^U - \mathcal{B}^U\|_{\mathrm{tr}} \right| \leq \mathrm{negl}(\kappa). \tag{255}$$

We give a construction relative to the following oracle: Let $\kappa = n$, $N = 2^n$, $L = 2^\ell$, and $\mathcal{O} = \sum_{k \in \{0,1\}^\ell} |k\rangle\langle k| \otimes \mathcal{O}_k$ where $\mathcal{O}_k \in \mathbb{U}(N)$ is a Haar random unitary for every $k \in \{0,1\}^\ell$. Also let $\mu = \mathrm{Haar}(N)^L$ denote the measure of $\mathcal{O}$. We show that every pair of algorithms $\mathcal{A}, \mathcal{B}$ distinguishes $\mathcal{O}, \mathcal{O}_k$ under uniform k from $\mathcal{O}, U$ for Haar random U must make exponentially many queries in ℓ. This implies that for $\ell = \Omega(n)$, the construction satisfies the conditions in Assumption 8.8.

Let $(P_1 = P, P_0 = \mathbb{1} - P)$ be any binary measurement and $f(U) := \mathrm{tr}(\mathcal{A}^U P)$ denote the probability that measuring $\mathcal{A}^U$'s output state yields an outcome 1. We apply the following lemma by Kretschmer [38].

Lemma 8.9 ([38, Lemma 18], paraphrased). *Let $\mathcal{A}^U$ be any T-query algorithm and $f(U) = \mathrm{tr}(\mathcal{A}^U P)$ for $0 \leq P \leq \mathbb{1}$. Then $f(U)$ is a $2T$-Lipschitz function in the Frobenius norm.*

We skip the proof of Lemma 8.9 and only sketch the ideas. For a detailed proof, see [38, Lemma 18]. For unitaries U, V satisfying $\|U - V\|_F = d$, their unitary channels have diamond distance at most $2d$. Thus by triangle inequality, $\|\mathcal{A}^U - \mathcal{A}^V\|_\diamond \leq 2Td = 2T\|U - V\|_F$ and thus $f(U)$ is $2T$-Lipschitz.

For our purpose, we show that that for every k and U and pairs of T-query algorithms $\mathcal{A}$ and $\mathcal{B}$, the function

$$f(\mathcal{O}, k, U) := \|\mathcal{A}^{\mathcal{O}, \mathcal{O}_k} - \mathcal{B}^{\mathcal{O}, \mathcal{O}_k}\|_{\mathrm{tr}} - \|\mathcal{A}^{\mathcal{O}, U} - \mathcal{B}^{\mathcal{O}, U}\|_{\mathrm{tr}} \tag{256}$$

is a $2T$-Lipschitz function of $\mathcal{O}$.

Lemma 8.10. *For every pair of T-query algorithms $\mathcal{A}, \mathcal{B}$, $k \in [L]$, and $U \in \mathbb{U}(N)$, $f(\mathcal{O}, k, U)$ as defined in (256) is $8T$-Lipschitz.*

74

Proof. It suffices to show that for each k, $\|\mathcal{A}^{\mathcal{O},\mathcal{O}_k} - \mathcal{B}^{\mathcal{O},\mathcal{O}_k}\|_{\mathrm{tr}}$ is a Lipschitz function of $\mathcal{O}$, and a similar argument applies to the second term in (256). To see why, we observe that

$$\|\mathcal{A}^{\mathcal{O},\mathcal{O}_k} - \mathcal{B}^{\mathcal{O},\mathcal{O}_k}\|_{\mathrm{tr}} = \max_{0 \leq P \leq \mathbb{1}} \left(\mathrm{tr}(\mathcal{A}^{\mathcal{O},\mathcal{O}_k} P) - \mathrm{tr}(\mathcal{B}^{\mathcal{O},\mathcal{O}_k} P) \right). \tag{257}$$

By Lemma 8.9, for every P, $\mathrm{tr}(\mathcal{A}^{\mathcal{O},\mathcal{O}_k} P) - \mathrm{tr}(\mathcal{B}^{\mathcal{O},\mathcal{O}_k} P)$ is $4T$-Lipschitz, and so is the left side of (257). Since for every $k \in \{0,1\}^\ell$ and $U \in \mathbb{U}(N)$, $f(\mathcal{O}, k, U)$ is a summation of two $4T$-Lipschitz functions, it is $8T$-Lipschitz. $\square$

Lemma 8.10 implies that the advantage we aim to upper bound, i.e.,

$$\begin{aligned} \mathrm{adv}(\mathcal{O}) &:= \mathop{\mathbb{E}}_{k \sim \mathcal{U}_\ell, U \sim \mathrm{Haar}(N)} f(\mathcal{O}, k, U) \\ &= \mathop{\mathbb{E}}_{k \sim \mathcal{U}_\ell} \|\mathcal{A}^{\mathcal{O},\mathcal{O}_k} - \mathcal{B}^{\mathcal{O},\mathcal{O}_k}\|_{\mathrm{tr}} - \mathop{\mathbb{E}}_{U \sim \mathrm{Haar}(N)} \|\mathcal{A}^{\mathcal{O},U} - \mathcal{B}^{\mathcal{O},U}\|_{\mathrm{tr}} \end{aligned} \tag{258}$$

is $8T$-Lipschitz.

Next, we prove a search lower bound, formally stated in Lemma 8.12, for showing that the average $\mathbb{E}_{\mathcal{O}} \, \mathrm{adv}(\mathcal{O})$ is bounded with overwhelming probability over choices of $\mathcal{O}$. We denote F_0 the all-zero ℓ-bit Boolean function and F_x denote the function whose only 1-preimage is x, i.e., $F_x(y) = \mathbb{1}[x = y]$. The following lemma will be useful later.

Lemma 8.11. *Let $\mathcal{A}$ be a T-query algorithm, $\mathcal{D}$ be the uniform distribution over $\{F_x : x \in \{0,1\}^\ell\}$, and F_0 be the zero function. Then*

$$\mathop{\mathbb{E}}_{F \sim \mathcal{D}} \|\mathcal{A}^F - \mathcal{A}^{F_0}\|_{\mathrm{tr}} \leq 4T L^{-1/2}. \tag{259}$$

Proof. Let the query algorithm be described with $T + 1$ unitaries $U_T, \ldots, U_0$, i.e.,

$$\mathcal{A}^F |0\rangle = U_T \mathcal{O}(F) \ldots U_1 \mathcal{O}(F) U_0 |0\rangle. \tag{260}$$

where $\mathcal{O}(F) := \sum_z (-1)^{F(z)} |z\rangle\langle z|$ is the oracle. Let F_x denote the function whose only one-preimage is x.

Consider the sequence of states

$$\begin{aligned} |\phi_T^x\rangle &= U_T \mathcal{O}(F_0) U_{T-1} \mathcal{O}(F_0) \ldots \mathcal{O}(F_0) U_1 \mathcal{O}(F_0) U_0 |0\rangle, \\ |\phi_{T-1}^x\rangle &= U_T \mathcal{O}(F_x) U_{T-1} \mathcal{O}(F_0) \ldots \mathcal{O}(F_0) U_1 \mathcal{O}(F_0) U_0 |0\rangle, \\ &\vdots \\ |\phi_0^x\rangle &= U_T \mathcal{O}(F_x) U_{T-1} \mathcal{O}(F_x) \ldots \mathcal{O}(F_x) U_1 \mathcal{O}(F_0) U_0 |0\rangle, \\ |\phi_0^x\rangle &= U_T \mathcal{O}(F_x) U_{T-1} \mathcal{O}(F_x) \ldots \mathcal{O}(F_x) U_1 \mathcal{O}(F_0) U_0 |0\rangle. \end{aligned} \tag{261}$$

That is, the state $|\phi_t^x\rangle$ is obtained by making t queries to F_0 followed by $T - t$ queries to F_x. Also let $|\psi_t^0\rangle = U_t \mathcal{O}(F_0) \ldots U_1 \mathcal{O}(F_0) U_0 |0\rangle$, which is independent of x.

Let $P_x = |x\rangle\langle x|$ denote the projection onto $|x\rangle$. By triangle inequality,

$$\begin{aligned} \| |\phi_T^x\rangle - |\phi_0^x\rangle \| &\leq \sum_{t=0}^{T-1} \|\mathcal{O}(F_x)|\psi_t^0\rangle - \mathcal{O}(F_0)|\psi_t^0\rangle \| \\ &\leq 2 \sum_{t=0}^{T-1} \|P_x |\psi_t^0\rangle \|. \end{aligned} \tag{262}$$

Note that

$$\mathop{\mathbb{E}}_{F \sim \mathcal{D}} \|\mathcal{A}^F - \mathcal{A}^{F_0}\|_{\mathrm{tr}} \le 4 \sum_{t=0}^{T-1} \mathop{\mathbb{E}}_{x \sim \mathcal{U}_n} \|P_x |\psi_t^0\rangle\|$$
$$\le 4 \sum_{t=0}^{T-1} \left(\mathop{\mathbb{E}}_x \langle \psi_t^0 | P_x | \psi_t^0 \rangle \right)^{1/2}$$
$$\le 4T \cdot L^{-1/2}. \tag{263}$$

The first inequality holds by the fact that $\||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\|_{\mathrm{tr}} \le 2\||\psi\rangle - |\phi\rangle\|$ for two normalized states $|\psi\rangle$ and $|\phi\rangle$. The second inequality holds by Cauchy-Schwarz inequality, and the third holds since $\mathbb{E}_x P_x = \mathbb{1}/L$. $\qquad \square$

Next, we use Lemma 8.11 to prove the following search lower bound.

Lemma 8.12. *Let $\mathcal{A}, \mathcal{B}$ be two T-query algorithms, $\mathcal{D}$ be the uniform distribution over $\{F_x : x \in \{0,1\}^\ell\}$, and F_0 be the zero function. Then*

$$\left| \mathop{\mathbb{E}}_{F \sim \mathcal{D}} \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} - \|\mathcal{A}^{F_0} - \mathcal{B}^{F_0}\|_{\mathrm{tr}} \right| \le 8TL^{-1/2}. \tag{264}$$

Proof. By Lemma 8.11,

$$\mathop{\mathbb{E}}_{F \sim \mathcal{D}} \|\mathcal{A}^F - \mathcal{A}^{F_0}\|_{\mathrm{tr}} \le 4TL^{-1/2}, \tag{265}$$

and a similar statement holds for $\mathcal{B}$. Then for each $F = F_x$ for $x \in \{0,1\}^\ell$,

$$\|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} - \|\mathcal{A}^{F_0} - \mathcal{B}^{F_0}\|_{\mathrm{tr}} \le \|\mathcal{A}^F - \mathcal{B}^F - \mathcal{A}^{F_0} + \mathcal{B}^{F_0}\|_{\mathrm{tr}}$$
$$\le \|\mathcal{A}^F - \mathcal{A}^{F_0}\|_{\mathrm{tr}} + \|\mathcal{B}^F - \mathcal{B}^{F_0}\|_{\mathrm{tr}}. \tag{266}$$

Since the above inequality is symmetric with repect to the exchange of F and F_0, we also have

$$\|\mathcal{A}^{F_0} - \mathcal{B}^{F_0}\|_{\mathrm{tr}} - \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} \le \|\mathcal{A}^F - \mathcal{A}^{F_0}\|_{\mathrm{tr}} + \|\mathcal{B}^F - \mathcal{B}^{F_0}\|_{\mathrm{tr}}. \tag{267}$$

Thus we have

$$\mathop{\mathbb{E}}_{F \sim \mathcal{D}} \left[\left| \|\mathcal{A}^F - \mathcal{B}^F\|_{\mathrm{tr}} - \|\mathcal{A}^{F_0} - \mathcal{B}^{F_0}\|_{\mathrm{tr}} \right| \right] \le 8TL^{-1/2}. \tag{268}$$

The rest of the proof follows from the triangle inequality. $\qquad \square$

With Lemma 8.12, we are ready to prove that the average of $\mathrm{adv}(\mathcal{O})$ is exponentially small in ℓ. Then we apply a concentration inequality to show $|\mathrm{adv}(\mathcal{O})|$ is sharply concentrated around $|\mathbb{E}_{\mathcal{O} \sim \mu} \mathrm{adv}(\mathcal{O})|$.

Lemma 8.13. *For every pair of T-query algorithms $\mathcal{A}, \mathcal{B}$, $|\mathbb{E}_{\mathcal{O} \sim \mu} \mathrm{adv}(\mathcal{O})| \le 8TL^{-1/2}$.*

Proof. We prove the lemma by contrapositive. Assume that there exist two algorithms $\mathcal{A}, \mathcal{B}$

$$\mathop{\mathbb{E}}_{\mathcal{O} \sim \mu} \mathrm{adv}(\mathcal{O}) = \mathop{\mathbb{E}}_{\mathcal{O} \sim \mu, k \sim \mathcal{U}_\ell} \|\mathcal{A}^{\mathcal{O}, \mathcal{O}_k} - \mathcal{B}^{\mathcal{O}, \mathcal{O}_k}\|_{\mathrm{tr}} - \mathop{\mathbb{E}}_{\mathcal{O} \sim \mu, U \sim \mathrm{Haar}(N)} \|\mathcal{A}^{\mathcal{O}, U} - \mathcal{B}^{\mathcal{O}, U}\|_{\mathrm{tr}} > 8TL^{-1/2}. \tag{269}$$

Then we construct another pair of algorithms $\tilde{\mathcal{A}}, \tilde{\mathcal{B}}$ which break the bound in Lemma 8.12. Given access to F which is either the zero function or F_x for uniform $x \in \{0,1\}^\ell$, $\tilde{\mathcal{A}}$ samples $U_0, \ldots, U_L \sim$ Haar(N), and sets $V = U_0$ and $\mathcal{O} = \sum_{k \in [L]} |k\rangle\langle k| \otimes V_k$, where $V_k = U_k$ if $F(k) = 0$ and $V_k = U_0$ if $F(k) = 1$. The algorithm $\tilde{\mathcal{A}}$ runs $\mathcal{A}^{\mathcal{O},V}$, and each query to $\mathcal{O}$ takes one query to F. If $F = 0$, then $\tilde{\mathcal{A}}^F$ outputs $\mathbb{E}_{\mathcal{O} \sim \mu, U \sim \text{Haar}(N)} |\mathcal{O}, U\rangle\langle\mathcal{O}, U| \otimes \mathcal{A}^{\mathcal{O},U}$ for independent $\mathcal{O}, U$; if $F = F_k$, then $\tilde{\mathcal{A}}^F$ outputs $\mathbb{E}_{\mathcal{O} \sim \mu, k \sim \mathcal{U}_\ell} |\mathcal{O}, k\rangle\langle\mathcal{O}, k| \otimes \mathcal{A}^{\mathcal{O}, \mathcal{O}_k}$. The algorithm $\tilde{\mathcal{B}}$ runs exactly the same algorithm except that $\mathcal{A}$ is replaced with $\mathcal{B}$. With $\tilde{\mathcal{A}}, \tilde{\mathcal{B}}$, we get a bound that violates Lemma 8.12.

Now we have shown that $\mathbb{E}_{\mathcal{O} \sim \mu} \text{adv}(\mathcal{O}) \leq 8TL^{-1/2}$. The same argument can be used to prove $-\mathbb{E}_{\mathcal{O} \sim \mu} \text{adv}(\mathcal{O}) \leq 8TL^{-1/2}$, and thus we conclude the proof. $\qquad\square$

We have shown that $\text{adv}(\mathcal{O})$ is a $8T$-Lipschitz function and the absolute value of the average $|\mathbb{E}_{\mathcal{O} \sim \mu} \text{adv}(\mathcal{O})|$ is $O(TL^{-1/2})$. Now we apply the following concentration inequality to show that with overwhelming probability over choices of $\mathcal{O}$, $|\text{adv}(\mathcal{O})| \leq O(TL^{-1/2})$.

Theorem 8.14 ([38, Theorem 11] and [43, Theorem 5.17]). *For $N_1, \ldots, N_k \in \mathbb{N}$, let $X = \mathbb{U}(N_1) \oplus \ldots \oplus \mathbb{U}(N_k)$. Let $\mu = \text{Haar}(N_1) \times \ldots \text{Haar}(N_k)$ be the product of the Haar measure on X. Suppose that $f : X \to \mathbb{R}$ is K-Lipschitz in the Frobenius norm. Then for every $t > 0$,*

$$\Pr_{\mathcal{O} \sim \mu} \left[f(\mathcal{O}) \geq \mathbb{E}_{\mathcal{P} \sim \mu} f(\mathcal{P}) + t \right] \leq \exp\left(-\frac{(N-2)t^2}{24K^2} \right), \tag{270}$$

where $N = \min\{N_1, \ldots, N_k\}$.

Since $\mathcal{O} = \sum_{k \in \{0,1\}^\ell} |k\rangle\langle k| \otimes \mathcal{O}_k$ where $\mathcal{O}_k \sim \text{Haar}(N)$ for each $k \in \{0,1\}^\ell$, $\text{adv}(\mathcal{O})$ is a function of $\{\mathcal{O}_k\}_{k \in \{0,1\}^\ell}$, and thus the concentration inequality can be applied.

Theorem 8.15. *For $\ell = \lceil n - \log n \rceil$ and $L = 2^\ell$, $\Pr_{\mathcal{O} \sim \mu}[|\text{adv}(\mathcal{O})| \geq 16TL^{-1/2}] \leq 2^{-\Omega(n)}$.*

Proof. By Theorem 8.14,

$$\Pr_{\mathcal{O} \sim \mu} [\text{adv}(\mathcal{O}) \geq 16TL^{-1/2}] \leq \exp\left(-\frac{(N-2)}{1536L} \right). \tag{271}$$

For $\ell = \lceil n - \log n \rceil$, the upper bound is $2^{-\Omega(n)}$. The same argument can be used to show the event $-\text{adv}(\mathcal{O}) \geq 16TL^{-1/2}$ occurs with probability $2^{-\Omega(n)}$. Applying a union bound, we conclude the proof. $\qquad\square$

Applying the Borel-Cantelli Lemma, for $\ell = \lceil n - \log n \rceil$, the event that every pair of poly(n)-query algorithms breaks the conditions in Assumption 8.8 occurs infinitely often with probability 0.

Corollary 8.16. *There exists an oracle relative to which Assumption 8.8 holds with probability 1.*

8.3 Randomness Expansion

Under the assumptions introduced in Section 8.1, we can reduce the input entropy to the device for any certified randomness protocol, and meanwhile, the output remains close to uniform. To see why, we recall the definition of quantum-proof randomness extractor [37, 26].

Definition 8.17 (Quantum-proof strong extractor [26, Definition 3.2]). *A function* $\text{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is a quantum-proof* (k, ε)-*stronger extractor with uniform seed if for all state* ρ_{XE} *classical on* X *with* $H_{\min}(X|E) \geq k$, *and for uniform* Y,

$$\|\rho_{\text{Ext}(X,Y)YE} - \rho_{U_m} \otimes \rho_Y \otimes \rho_E\|_{\text{tr}} \leq \varepsilon, \tag{272}$$

where ρ_{U_m} *is the uniform distribution over* $\{0,1\}^m$.

If alternatively we only have the guarantee that $H_{\min}^\delta(X|E) \geq k$, for sufficiently small but nonzero δ, the extractor still outputs a distribution close enough to the uniform distribution conditioned on the side information E by triangle inequality.

Lemma 8.18 ([26, Lemma 3.5]). *If* $\text{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is a quantum-proof* (k, ε)-*strong extractor, then for any* ρ_{XE} *and* $\delta > 0$ *with* $H_{\min}^\delta(X|E)_\rho \geq k$,

$$\|\rho_{\text{Ext}(X,Y)YE} - \rho_{U_m} \otimes \rho_Y \otimes \rho_E\|_{\text{tr}} \leq \varepsilon + 2\delta. \tag{273}$$

If E is restricted to a classical state, then we say an extractor that satisfies Definition 8.17 a classical-proof (k, ε)-strong extractor. Furthermore, if Definition 8.17 holds in the special case that E is empty, we call such an extractior a (k, ε)-stronger extractor.

In the same paper, De, Portmann, Vidick, and Renner [26] showed that Trevisan's extractor [59] is a quantum-proof strong extractor. We take relevant definitions from [26].

Definition 8.19 (Weak design [26, Definition 4.1]). *For integer* d, *the family of sets* $S_1, \ldots, S_m \subset [d]$ *is a weak* (t, r)-*design if*

1. *For every* $i \in [m]$, $|S_i| = t$.

2. *For every* $i \in [m]$, $\sum_{j=1}^{i-1} 2^{|S_i \cap S_j|} \leq rm$.

Definition 8.20 (Trevisan's extractor [26, Definition 4.2][59]). *For a one-bit extractor* $C : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}$, *which uses a (not necessarily uniform) seed of length* t, *and for a weak* (t, r)-*design,* $S_1, \ldots, S_m \subset [d]$, *an* m-*bit extractor* $\text{Ext}_C : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is defined as*

$$\text{Ext}_C(x, y) := C(x, y_{S_1}) \ldots C(x, y_{S_m}). \tag{274}$$

The integer d in Definition 8.19 is the length of the seed of the extractor Ext_C and depends on t, the size of the seed of the 1-bit extractor C. The size of the seed will always be $d = \text{poly}(\log n)$ if the error $\varepsilon = \text{poly}(1/n)$ [26]. In the same paper, it is also proved that that a single-bit strong extractor is also a quantum-proof strong extractor.

Theorem 8.21 ([26, Theorem 4.7]). *Let* $C : \{0,1\}^n \to \{0,1\}^t \to \{0,1\}$ *be a* (k, ε)-*strong extractor with an* s-*bit seed—i.e., the seed needs at least* s *bits of min-entropy—and* $S_1, \ldots, S_m \subset [d]$ *a weak* (t, r)-*design. Then the extractor defined in Definition 8.20 is a quantum proof* $(k + rm + \log(1/\varepsilon), 6m\sqrt{\varepsilon})$-*strong extractor for any seed with min-entropy* $d - (t - s - \log \frac{1}{3\sqrt{\varepsilon}})$.

Furthermore, there exists a (k, ε)-strong extractor by Raz, Reingold and Vadhan [54], and the input seed has length $\text{poly} \log(n)$.

Theorem 8.22 ([26, Proposition 5.2]). *For any* $\varepsilon > 0$ *and* $n \in \mathbb{N}$, *there exists a* (k, ε)-*strong extractor with uniform seed* $\text{Ext}_{n,\varepsilon} : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}$ *with* $t = O(\log(n/\varepsilon))$ *and* $k = 3 \log(1/\varepsilon)$.

Combining the fact that there exists a quantum-proof strong extractor and Assumption 8.3, we prove the following theorem.

Theorem 8.23. *Assume that Assumption 5.1 and Assumption 8.3 holds. There exists a randomness expansion protocol for a device which solve* $\mathrm{LXEB}_{b,k}$ *for* 99% *of the given circuits and achieves polynomial expansion for* $b = 1.02$ *and* $k = O(n^2)$, *where* n *is the number of qubits each circuit acts on.*

Proof. In our m-round randomness expansion protocol in Figure 1 using a random circuit, we change the circuits at least $\gamma m = O(\log n)$ times, and each can be replaced with pseudorandom circuits that can be computed using $\ell = \mathrm{poly}(n)$ bits as input (used for generating the key of the pseudorandom function). The protocol generates a distribution $(\varepsilon + 2\varepsilon' + \mathrm{negl}(n))$-close to an $\Omega(m)$-bit uniform distribution for devices solving $\mathrm{LXEB}_{1+\delta,k}$ for constant δ and $k = O(n^2)$, using an input of $O(\ell \log n)$ uniformly random bits. Setting $m = \ell^c$ for $c \geq 2$, the protocol accumulates net entropy. $\square$

Applying the same reasoning as in the proof of Theorem 8.23, we conclude that Assumption 8.8 implies that there exists a randomness expansion protocol.

Theorem 8.24. *Assume that Assumption 8.8 holds. There exists a randomness expansion protocol for a device that is given oracle access to a pseudorandom unitary and solves* $\mathrm{LXEB}_{b,k}$ *for* 99% *of the given circuits and achieves polynomial expansion for* $b = 1.02$ *and* $k = O(n^2)$, *where* n *is the number of qubits each circuit acts on.*

Acknowledgements

References

[1] Scott Aaronson. QMA/qpoly ⊆ PSPACE/poly: de-merlinizing quantum protocols. In *21st Annual IEEE Conference on Computational Complexity (CCC'06)*, pages 13–pp. IEEE, 2006.

[2] Scott Aaronson. Certified randomness from quantum supremacy. *Talk at Google Quantum Symposium, Venice Beach, CA, May 16, 2018*, 2018. https://www.scottaaronson.com/talks/certrand-huji.ppt.

[3] Scott Aaronson and Andris Ambainis. The need for structure in quantum speedups. *Theory of Computing*, 10(1):133–166, 2014.

[4] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342, 2011.

[5] Scott Aaronson and Alex Arkhipov. Bosonsampling is far from uniform. *Quantum Information & Computation*, 14(15-16):1383–1423, 2014.

[6] Scott Aaronson, Adam Bouland, Joseph Fitzsimons, and Mitchell Lee. The space "just above" BQP. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, pages 271–280, 2016.

[7] Scott Aaronson and Lijie Chen. Complexity-theoretic foundations of quantum supremacy experiments. *arXiv preprint arXiv:1612.05903*, 2016.

[8] Scott Aaronson and Andrew Drucker. A full characterization of quantum advice. In *Proceedings of the forty-second ACM symposium on Theory of computing*, pages 131–140, 2010.

[9] Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *2014 IEEE 55th Annual Symposium on Foundations of Computer Science*, pages 474–483. IEEE, 2014.

[10] Rotem Arnon-Friedman. *Reductions to IID in Device-independent Quantum Information Processing*. PhD thesis, ETH Zurich, 2018.

[11] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature communications*, 9(1):1–11, 2018.

[12] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandão, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[13] Boaz Barak, Chi-Ning Chou, and Xun Gao. Spoofing linear cross-entropy benchmarking in shallow quantum circuits. In *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2021.

[14] Roozbeh Bassirian, Adam Bouland, Bill Fefferman, Sam Gunn, and Avishay Tal. On certified randomness from quantum advantage experiments. *arXiv preprint arXiv:2111.14846*, 2021.

[15] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM (JACM)*, 48(4):778–797, 2001.

[16] Shalev Ben-David and Robin Kothari. Quantum distinguishing complexity, zero-error algorithms, and statistical zero knowledge. In *14th Conference on the Theory of Quantum Computation, Communication and Cryptography*, volume 21, page 24, 2019.

[17] Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523, 1997.

[18] Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature*, 556(7700):223–226, 2018.

[19] Joseph Bonneau, Jeremy Clark, and Steven Goldfeder. On bitcoin as a public randomness source. Cryptology ePrint Archive, Paper 2015/1015, 2015. https://eprint.iacr.org/2015/1015.

[20] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 320–331. IEEE, 2018.

[21] Fernando GSL Brandão, Aram W. Harrow, and Michał Horodecki. Local random quantum circuits are approximate polynomial-designs. *Communications in Mathematical Physics*, 346(2):397–434, 2016.

[22] Luís TAN Brandão and René Peralta. Notes on interrogating random quantum circuits. NIST White Paper, 2020.

[23] Michael J Bremner, Richard Jozsa, and Dan J Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 467(2126):459–472, 2011.

[24] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation. *Ph. D. Thesis*, 2009.

[25] Matthew Coudron and Henry Yuen. Infinite randomness expansion with a constant number of devices. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 427–436, 2014.

[26] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan's extractor in the presence of quantum side information. *SIAM Journal on Computing*, 41(4):915–940, 2012.

[27] Catherine Donati-Martin and Alain Rouault. Random truncations of haar distributed matrices and bridges. *arXiv preprint arXiv:1302.6539*, 2013.

[28] Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation. *Communications in Mathematical Physics*, 379(3):867–913, 2020.

[29] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum approximate optimization algorithm. *arXiv preprint arXiv:1411.4028*, 2014.

[30] Bela A. Frigyik, Amol Kapila, and Maya R. Gupta. Introduction to the dirichlet distribution and related processes. *Department of Electrical Engineering, University of Washignton, UWEETR-2010-0006*, 6:1–27, 2010.

[31] Oded Goldreich, Amit Sahai, and Salil Vadhan. Can statistical zero knowledge be made non-interactive? or on the relationship of szk and niszk. In *Annual International Cryptology Conference*, pages 467–484. Springer, 1999.

[32] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 59–68, 1986.

[33] Jonas Haferkamp. Random quantum circuits are approximate unitary t-designs in depth $O\left(nt^{5+o(1)}\right)$. *arXiv preprint arXiv:2203.16571*, 2022.

[34] Joonsuk Huh, Gian Giacomo Guerreschi, Borja Peropadre, Jarrod R McClean, and Alán Aspuru-Guzik. Boson sampling for molecular vibronic spectra. *Nature Photonics*, 9(9):615–620, 2015.

[35] Gregory D Kahanamoku-Meyer, Soonwon Choi, Umesh V Vazirani, and Norman Y Yao. Classically verifiable quantum advantage from a computational bell test. *Nature Physics*, 18(8):918–924, 2022.

[36] John Kelsey, Luís TAN Brandão, Rene Peralta, and Harold Booth. A reference for randomness beacons: Format and protocol version 2. Technical report, National Institute of Standards and Technology, 2019.

[37] Robert Konig and Renato Renner. Sampling of min-entropy relative to quantum knowledge. *IEEE Transactions on Information Theory*, 57(7):4760–4787, 2011.

[38] William Kretschmer. Quantum pseudorandomness and classical complexity. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2021.

[39] William Kretschmer. The quantum supremacy tsirelson inequality. *Quantum*, 5:560, 2021.

[40] Lars S Madsen, Fabian Laudenbach, Mohsen Falamarzi Askarani, Fabien Rortais, Trevor Vincent, Jacob FF Bulmer, Filippo M Miatto, Leonhard Neuhaus, Lukas G Helt, Matthew J Collins, et al. Quantum computational advantage with a programmable photonic processor. *Nature*, 606(7912):75–81, 2022.

[41] Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. Efficient certifiable randomness from a single quantum device. *arXiv preprint arXiv:2204.11353*, 2022.

[42] Chris Marriott and John Watrous. Quantum arthur-merlin games. In *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.*, pages 275–285. IEEE, 2004.

[43] Elizabeth S Meckes. *The random matrix theory of the classical compact groups*, volume 218. Cambridge University Press, 2019.

[44] Sanketh Menda and John Watrous. Oracle separations for quantum statistical zero-knowledge. *arXiv preprint arXiv:1801.08967*, 2018.

[45] Tony Metger, Omar Fawzi, David Sutter, and Renato Renner. Generalised entropy accumulation. *ArXiv*, abs/2203.04989, 2022.

[46] Carl A Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *Journal of the ACM (JACM)*, 63(4):1–63, 2016.

[47] Carl A Miller and Yaoyun Shi. Universal security for randomness expansion from the spot-checking protocol. *SIAM Journal on Computing*, 46(4):1304–1335, 2017.

[48] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[49] Feng Pan, Keyang Chen, and Pan Zhang. Solving the sampling problem of the sycamore quantum supremacy circuits. *arXiv preprint arXiv:2111.03011*, 2021.

[50] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by bell's theorem. *Nature*, 464(7291):1021–1024, 2010.

[51] John Preskill. Quantum computing and the entanglement frontier. *arXiv preprint arXiv:1203.5813*, 2012.

[52] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[53] Ran Raz. Quantum information and the pcp theorem. *Algorithmica*, 55(3):462–489, 2009.

[54] Ran Raz, Omer Reingold, and Salil Vadhan. Extracting all the randomness and reducing the error in trevisan's extractors. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 149–158, 1999.

[55] Ran Raz and Avishay Tal. Oracle separation of BQP and PH. *ACM Journal of the ACM (JACM)*, 69(4):1–21, 2022.

[56] Markus Reiher, Nathan Wiebe, Krysta M Svore, Dave Wecker, and Matthias Troyer. Elucidating reaction mechanisms on quantum computers. *Proceedings of the national academy of sciences*, 114(29):7555–7560, 2017.

[57] Maria Schuld, Kamil Brádler, Robert Israel, Daiqin Su, and Brajesh Gupt. Measuring the similarity of graphs with a gaussian boson sampler. *Physical Review A*, 101(3):032314, 2020.

[58] Alexander A Sherstov. Strong direct product theorems for quantum communication and query complexity. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 41–50, 2011.

[59] Luca Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, 48(4):860–879, 2001.

[60] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 61–76, 2012.

[61] John Watrous. Limits on the power of quantum statistical zero-knowledge. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, pages 459–468. IEEE, 2002.

[62] Yulin Wu, Wan-Su Bao, Sirui Cao, Fusheng Chen, Ming-Cheng Chen, Xiawei Chen, Tung-Hsun Chung, Hui Deng, Yajie Du, Daojin Fan, et al. Strong quantum computational advantage using a superconducting quantum processor. *Physical review letters*, 127(18):180501, 2021.

[63] Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. *arXiv preprint arXiv:2204.02063*, 2022.

[64] Mark Zhandry. How to construct quantum random functions. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 679–687. IEEE, 2012.

[65] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, 2020.