Certified Randomness implies Secure Classical Position-Verification

Omar Amer*[1], Kaushik Chakraborty†[1], David Cui‡[1,2], Fatih Kaleoglu§[1,3], Charles Lim¶[1], Minzhao Liu‖[1], and Marco Pistoia**[1]

[1] *Global Technology Applied Research, JPMorganChase*
[2] *Massachusetts Institute of Technology*
[3] *UC Santa Barbara*

October 2024

Abstract

Liu et al. (ITCS22) initiated the study of designing a secure position verification protocol based on a specific proof of quantumness protocol and classical communication. In this paper, we study this interesting topic further and answer some of the open questions that are left in that paper. We provide a new generic compiler that can convert any single round proof of quantumness-based certified randomness protocol to a secure classical communication-based position verification scheme. Later, we extend our compiler to different kinds of multi-round proof of quantumness-based certified randomness protocols. Moreover, we instantiate our compiler with a random circuit sampling (RCS)-based certified randomness protocol proposed by Aaronson and Hung (STOC 23). RCS-based techniques are within reach of today's NISQ devices; therefore, our design overcomes the limitation of the Liu et al. protocol that would require a fault-tolerant quantum computer to realize. Moreover, this is one of the first cryptographic applications of RCS-based techniques other than certified randomness.

*omar.amer@jpmchase.com
†kaushik.chakraborty@jpmchase.com
‡dzcui@mit.edu
§ftkaleoglu@gmail.com
¶charles.lim@jpmchase.com
‖minzhao.liu@jpmchase.com
**marco.pistoia@jpmchase.com

Contents

1 Introduction

Secure positioning is a sub-domain of information theory where cryptographic protocols use the geographic location of an entity as the only credential. Although it was formally introduced in [CGMO09], it has been studied before in other domains such as wireless security [BC93, Bus04, CH05, SP05, SSW03, VN06, ZLFW06]. Position verification is one of the simplest and most fundamental position-based cryptographic functionalities, where the goal is to allow multiple parties to verify the geographic location of a prover.

In [CGMO09], Chandran et al. proved the impossibility of a classical position-verification scheme in the standard model. In [Ken11], Kent et al. first proposed the idea of quantum communication-based position verification under quantum tagging. Later, in [BCF+14], Buhrman et al. re-initiated the study of this topic and proved the impossibility of designing an information-theoretically secure quantum communication-based position verification protocol. The authors provide a generic strategy to attack any position verification protocol using the instantaneous non-local computation technique proposed by Vaidman [Vai03]. However, for this attack, the malicious provers need to share a doubly exponential (in the security parameter) number of EPR pairs. Later, in [BK11], the author reduced the entanglement requirement to exponential (in the security parameter) using port-based teleportation. On the other hand, in [BCF+14], Buhrman et al. showed if the adversaries do not have access to EPR pairs, then it is possible to design a secure quantum communication-based position verification scheme. Many protocols in the literature achieve security against non-entangled adversaries, but they become vulnerable to adversaries with an exponential amount of entanglement [CL15, Unr14, JKPPG22, QS15, AEFR+23]. In the standard model, the security of a quantum communication-based position verification scheme against adversaries with a polynomially bounded amount of entanglement remains open. However, in the random oracle model, Unruh [Unr14] proves the security of a quantum communication-based position verification protocol against adversaries with unbounded shared entanglement.

Recently, in [BCS22], Bluhm et al. proposed a noise-robust protocol that uses only a single qubit quantum resources and some classical communication. Interestingly, the adversary's quantum resource for any attack strategy increases with the classical communication resources in the protocol. Later, inspired by this result in [BCS22], Allerfoster et al. propose loss-tolerant and noise-tolerant protocols that are within reach of today's quantum communication technology. However, all these protocols still suffer from the distance limitation of the quantum communication [ABB+23].

In [LLQ22], Liu et al. initiate the study of designing position-verification protocols that are based on proof of quantumness and classical communication. The authors show that the proofs of quantumness is necessary to design a secure classical verifier position-verification protocol. Moreover, the authors prove that if the prover has access to a fault-tolerant quantum computer, then under the LWE hardness assumption, one can design a secure classical communication-based position verification protocol, hence beating the impossibility result proposed by Chandran et al. [CGMO09].

The classical impossibility result and the results of Liu et al. make clear that the existence of proofs of quantum are a necessary condition, and that a specific proof of quantumness can act as a sufficient condition. However, it is unclear whether proofs of quantumness in general are a sufficient condition for designing a classical verifier position verification scheme (CVPV). In this paper, we answer the following question.

What fundamental properties suffice for designing a secure position verification scheme with classical verifiers?

In particular, we show a general class of proofs of quantumness which suffice to enable secure classical position verification. Moreover, the protocol proposed in [LLQ22] requires, along with the hardness of the LWE assumption, a fault-tolerant quantum computer (with quantum memory) and the LWE-hardness assumption. As such, such a protocol is beyond the reach of the current-day available noisy intermediate scale quantum (NISQ) machines. In this paper, we further pose the following question, and answer it in the affirmative.

Is it possible to design a classical position verification protocol that can be implemented using a NISQ device and depends on some other computational hardness assumption?

1.1 Our Results

In this paper, we make progress toward the first question by proving that in the quantum random oracle model, a single-round protocol that achieves certified randomness with classical verifiers is sufficient for the secure position verification scheme with classical verifiers.

Theorem 1 (Single-Round Compiler - Informal)**.** *Suppose there exists a single-round certified randomness protocol with a classical verifier and computationally bounded quantum prover, then there exists a position verification protocol with classical verifiers secure in the quantum random oracle model.*

In the literature, most of the existing certified randomness protocols are multi-round and it is not immediately clear whether we can draw a conclusion similar to Theorem 1 for the multi-round protocols. Moreover, there are many ways to extend our single-round compiler to a multi-round one, each with a different set of advantages and drawbacks. Our first multi-round compiler is a natural generalization of the single-round compiler, where we construct the position verification protocol just by composing the single-round protocols in sequence. However, this compiler works only for the multi-round protocols that achieve a stronger notion of certified randomness, namely those with the so called *Sequential Decomposition* property.

Definition 1 (Sequential Decomposition Property - Informal)**.** *A multi-round PoQ protocol is said to have the sequential decomposition property if the following holds: For an unbounded guesser trying to guess the prover's answer each* *round and is allowed to communicate with the prover after the answer and the guess are sent to the verifiers, the guesser still fails at least one round with high probability.*

Remark 1. *The above definition roughly captures the property that the security of the multi-round protocol reduces to the security of multiple iterations of the smaller single-round protocol. This should not be confused with the requirement that the protocol achieve security under common notions of sequential composition, which is an altogether separate and stronger property than the sequential decomposition property defined above.*

For such multi-round certified randomness protocols, we get the following result.

Theorem 2 (Multi-Round Sequential Compiler - Informal)**.** *Assume there exists a multi-round certified randomness protocol, with a classical verifier and a computationally-bounded quantum prover, that satisfies the sequential decomposition property, then there exists a position verification protocol with classical verifiers secure in the quantum random oracle model.*

Note that most of the existing multi-round certified randomness protocols with a classical verifier and computationally-bounded quantum provers are either based on the post-quantum secure trapdoor claw-free functions with an adaptive hardcore bit property or based on random circuit sampling [BCM+21a, AH23]. It is not clear whether these existing protocols would satisfy the sequential decomposition property that we need for our multi-round compiler. Although these protocols provide a lower bound on the smooth min-entropy conditioned on some side information, our setting allows communication with an guesser that is allowed to receive a copy of the classical outputs, resulting in zero entropy.

Fortunately, to be helpful in assisting the guesses, the side information for the ith round must be present in the ith round, not before or after. Although the conditional entropy cannot be lower bounded due to communication, it should not affect the guessing probability. Here, we show that protocols in Ref [BCM+21a, AH23] indeed satisfy the sequential decomposition property by proving the following theorem.

Theorem 3 (Existence of Multi-Round Certified Randomness Protocol with Sequential Decomposition Property - Informal)**.** *If a multi-round certified randomness protocol, with a classical verifier and a computationally bounded quantum prover, has non-zero single-round von Neumann entropy "on average" when it does not abort (e.g. in [AH23, BCM+21a]), then that certified randomness protocol also satisfy the sequential decomposition property.*

We refer to our second multi-round compiler as a rapid-fire compiler. Here, the verifiers send all the challenges that are related to the multi-round certified randomness protocol sequentially with a small predetermined time gap. The difference with the previous approach is that here, the verifiers do not wait for the answers to arrive from the prover before sending the next challenge. This protocol achieves the desired security in the QROM from the multi-round certified randomness protocols without the sequential decomposition property like in [BCM+21a, AH23]. We get the following result in this direction.

Theorem 4 (Multi-Round Rapid-Fire Compiler - Informal)**.** *Suppose there exists a multi-round certified randomness protocol with a classical verifier and a computationally-bounded quantum prover, then under some restricted communication assumptions, there exists a position verification protocol with classical verifiers secure in the quantum random oracle model.*

Finally, we combine both previous approaches and provide a new compiler called *Sequential Rapid-Fire Compiler* that shows prospects in overcoming the limitations of the previous multi-round compilers.

Theorem 5 (Multi-Round Sequential-Rapid-Fire Compiler - Informal)**.** *Consider the multi-round position verification protocol that exists due to Theorem 4. A sequential compilation of this protocol with communication restrictions within each repetition but not between repetitions is also a position verification protocol with classical verifiers secure in the quantum random oracle model.*

Later, in Appendix B, we instantiate our compilers with a random circuit sampling (RCS)–based multi-round certified randomness protocol proposed by Aaronson and Hung [AH23]. This, along with the recent proposal of [KT24] to use RCS for quantum cryptography, is one of the first cryptographic applications of RCS other than certified randomness. Related recent work [MSY24] explores the minimum complexity assumption needed for protocols such as RCS[1] and characterizes it as *classically-secure one-way puzzles*. Our construction also achieves advantages over the existing protocol in [LLQ22]. For example, compared to the protocol proposed in [LLQ22], our RCS-based protocol doesn't need any fault-tolerant quantum computers to implement. It is within the reach of NISQ devices and, therefore, can be implemented with near-term quantum computers. Moreover, unlike the protocol in [LLQ22], our instantiation doesn't require any quantum memory, which makes our protocol more implementation-friendly. Finally, our construction in this paper also achieves a secure position-verification scheme under the hardness assumption of random circuit sampling, which is entirely different from the LWE-hardness assumption.

1.2 Paper Organization

In Section 1.3 we outline the main technical ideas. We recall some preliminary concepts and definitions useful for relevant to our in Section 2. In Section 3, we provide our compiler for CVPV from single-round certified randomness and prove the security of the construction, our first major result. In Section 4 we provide a number of methods of generalizing this compiler to allow for multi-round certified randomness protocols. Specifically, in Section 4.1 we show that certified

[1]That is to say, proof of quantumness protocols with inefficient classical verification.

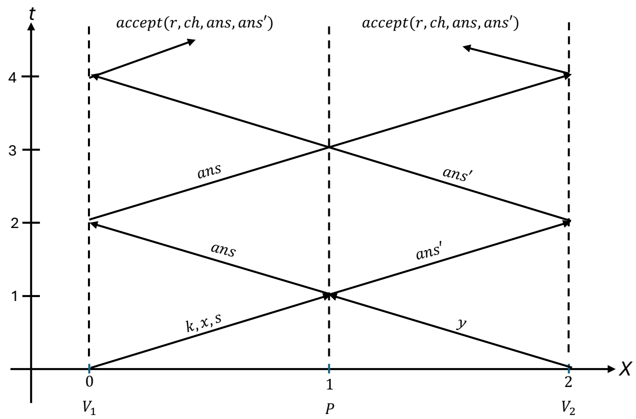

Figure 1: A spacetime diagram describing the honest interaction between two verifiers at locations $X = 0$ and $X = 2$ and an honest prover located at the claimed position (for simplicity, located at $X = 1$ in the diagram). The verifiers pre-share random values x, y, k, r prior to the start of the protocol, and set $s = ch \oplus G_k(x \oplus y)$ for some family of hash functions $\{G_k\}$ and $ch = \mathsf{Gen}(1^n; r)$ for Gen the verifier functionality of some certified randomness verifier and where $accept(\cdot)$ determines a boolean function that determines whether the verifiers accept the provers claim. In all spacetime figures we provide, we implicitly require that the proper timing constraints are observed in order for the verifiers to accept.

randomness protocols with a property we refer to as sequential decomposability suffice to allow for a natural generalization of our compiler for multi-round settings, and in Section 4.2 we prove (with a full proof in Appendix A) that that a class of natural certified randomness protocols satisfy the necessary property. In Section 4.3, and Section 4.4 we prove the security of an alternate compilation method, based on additional timing constraints, which has advantages in the idealized model at the cost of practical robustness. Finally, in Appendix B, we show that the well known near-term proposal for certified randomness due to Aaronson and Hung suffices to instantiate our compiler.

1.3 Technical Overview

Single Round Compiler

We first consider any single-round PoQ-based certified randomness protocol $\mathscr{P} = (P, V)$, which is modeled as a two-message interactive protocol. In the first message, the verifier sends a random challenge ch to the prover. In the second message, it gets back ans as a response. Later, the verifier performs a verification process Ver to accept or reject the response.

Construction: In our compiler, we consider that the two verifiers (say V_1, V_2)

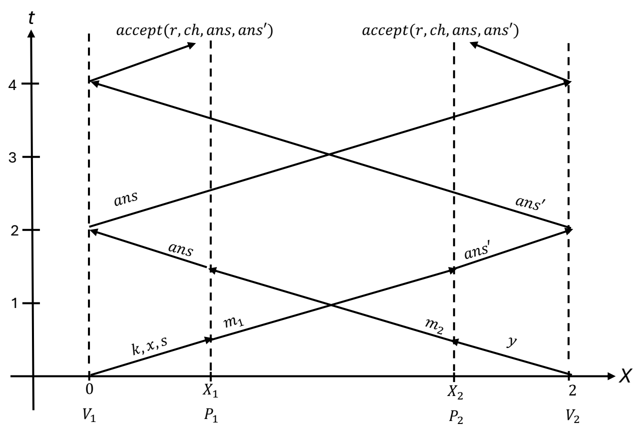

Figure 2: A spacetime diagram describing the honest interaction between two verifiers at locations $X = 0$ and $X = 2$ and two dishonest prover located at arbitrary positions between V_1 and V_2 (for simplicity, located at $X = 0.5$ and $X = 1.5$ in the diagram). The provers are allowed to communicate during the protocol but are non-signaling. Notation and behavior is otherwise analogous to Figure 1. In particular, verifiers expect to recieve messages at times determined by honest prover's position.

in the CVPV protocol have access to a family of cryptographic hash function $\{G_k\}_{k\in\{0,1\}^\lambda} : \{0,1\}^m \to \{0,1\}^n$. In addition, they share a random hash key k and two random inputs $x, y \leftarrow \{0,1\}^m$. At time $t = 0$, V_1 sends $s := G_k(x \oplus y) \oplus \mathsf{ch}$, x, k to the prover P at a claimed location (say $X = 1$ in Figure 1) and V_2 sends y to P. Upon receiving x, s, k, y from the verifiers, the prover can recover ch and send back the response ans to the verifiers. The verifiers verify the position of the prover if the following two conditions are satisfied.

1. **Timing Constraint:** Both verifiers receive at time $t = 2$.
2. **Consistency Constraint:** Both of the received answers are the same.
3. **Certified Randomness Constraint:** The verification process Ver corresponding to the certified randomness protocol accepting the response.

We refer to Figure 1 for the schematic diagram of the compiler. For clarity, we also depict general adversarial behavior in Figure 2.

Soundness Proof Sketch (Proof Sketch of Theorem 1). We reduce the soundness of the CVPV protocol above to the certified randomenss property of $\mathscr{P}$. We first make the connection to certified randomness by imagining an ideal game, where P_1 and P_2 are simultaneously given ch and asked to output the *same* correct answer ans. If no communication is allowed, then beating this game violates certified randomness due to no-signalling. Intuitively, certified randomness dictates that ans cannot be computed deterministically from ch, which forces P_1 and P_2 to perform their own local random computation to output a valid answer.

In the real security game, the provers P_1, P_2 effectively receive secret shares x, y of ch, where $x \oplus y = \mathsf{ch}$, and then get to perform one round of simultaneous communication. If they simply forward their shares, then this would be equivalent to the ideal game. However, we need to argue that this *challenge-forwarding* adversary is optimal. To do so, we rely on the fact that $x \oplus y$ is information-theoretically hidden from the provers before they communicate.

One would hope that this in turn hides any *useful* information about ch during the same timeframe. Nonetheless, it is not clear how to argue this directly. Namely, one needs to rule out *homomorphic* attacks, where P_1 performs a quantum computation on input x, P_2 on input y, and then they can each deterministically recover the same output ans, which could be obtained by running the honest prover of $\mathscr{P}$ on input ch.

To circumvent this issue, we use a cryptographic hash function G and encrypt ch with a one-time-pad using $G(x \oplus y)$. The property we need from G is *query-extractability*, and accordingly we show security in the quantum random oracle model.

Multi-Round Sequential Compiler

For this compiler, we first start with a multi-round (say ℓ-round) certified randomness protocol. Similar to the single-round certified randomness protocol, we can formulate any ℓ-round certified randomness protocol to a 2ℓ-communication round interactive protocol, where at round $i \in [\ell]$, the verifier sends a random challenge ch_i to the prover and gets back ans_i from it. The next round starts after the verifier receives the answer from the prover.

Construction: The compiler corresponding to such an ℓ-round certified randomness protocol is a sequential repetition of the interactive portion of the single-round compiler, followed by the necessary testing of the entire transcript. Before the beginning of the protocol, i.e., at $t = -\infty$ the verifiers (V_1, V_2) share ℓ random hash keys $\{k_i\}_{i\in[\ell]}$, ℓ random input pairs $\{(x_i, y_i)\}_{i\in[\ell]}$, and ℓ random challenges $\{\mathsf{ch}_i\}_{i\in[\ell]}$ corresponding to the challenges of the certified randomness protocol. On the $i \in [\ell]$ round, V_1 sends $s_i := G_{k_i}(x_i \oplus y_i) \oplus \mathsf{ch}_i$ and V_2 sends y_i to the prover P at a claimed location $X = 1$ (see Figure 3 for reference) at time t_{i-1}. Upon receiving k_i, x_i, s_i, y_i, the prover computes ch_i, and sends back the answer ans_i corresponding to the challenge ch_i to the verifiers. Suppose, the verifiers send the challenges at time t_i^{send}, and receive the answers at time t_i^{rec}. At the end of the protocol, the verifiers accepts the claimed location of the prover if the answers satisfy the timing constraint, i.e. $t_i^{\mathrm{rec}} - t_i^{\mathrm{send}} = 2$ for all $i \in [\ell]$, the consistency check, i.e. $\mathsf{ans}_i = \mathsf{ans}'_i$ for all $i \in [\ell]$, and the certified randomness constraint. We refer to Figure 3 for the schematic diagram of the protocol and Figure 4 for the behavior of cheating provers.

Difficulty of the Soundness Proof. The adversarial model of all the existing multi-round certified randomness protocols [AH23, BCM+21a] use entropy

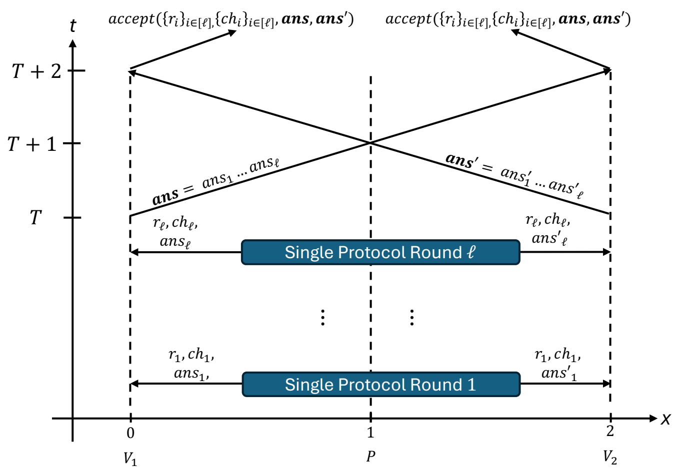

Figure 3: A spacetime diagram describing the honest interaction between two verifiers at locations $X = 0$ and $X = 1$ and an honest prover located at the claimed position (for simplicity, located at $X = 1$ in the diagram). For brevity, we model the execution of the challenge-response portion of each round of the multi-round protocol as a black box that provides the relevant randomness, challenge, and answers from each round, though this abstraction is not used in our proof. Following some ℓ rounds of the protocols, the verifiers engage in a final interaction to accept or reject the protocol. As in Figure 1 and elsewhere, we omit depicting the details of the expected in-round timing constraints, which are detailed in the text.

accumulation theorem (EAT) to calculate a lower bound on the min-entropy of the produced outcomes for all the rounds. More precisely, the multi-round certified randomness protocol in [AH23] models the entire adversary channel as an entropy accumulation channel (EAT) [DFR20]. Although the original security analysis in [BCM+21a] did not directly use EAT, later, Merkulov and Arnon-Friedman show in [MAF23] that the adversarial channel of [BCM+21a] can indeed be modeled as an EAT channel. The EAT channel that is proposed in [DFR20] does not allow the prover to communicate its private registers to the external adversary during the runtime of the protocol. However, in our sequential compiler, after the i-th round the malicious provers can communicate with each other, and exchange their internal registers as well as their answers for the i-th round. We refer to Figure 4 for an example. This stops us from applying the security analysis from [DFR20, BCM+21a, AH23] directly. As a way out, we require that our certified randomness protocols satisfy a stronger notion of security, namely sequential decomposition that we define informally in Definition 1 (formally stated in Definition 5).

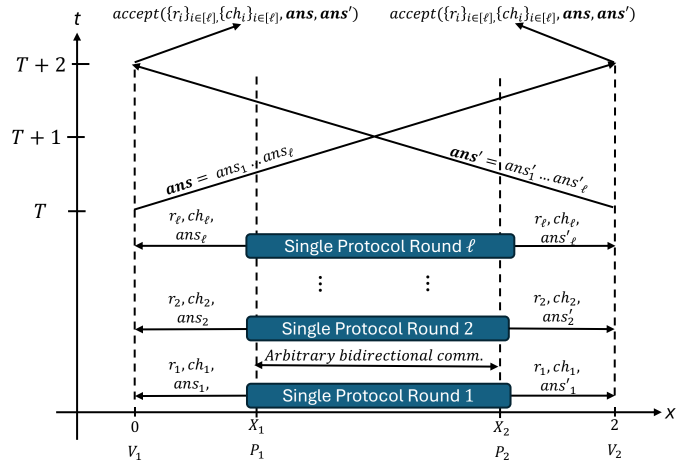

Figure 4: A spacetime diagram describing the interaction between two verifiers at locations $X = 0$ and $X = 1$ and two dishonest prover located at arbitrary positions between V_1 and V_2 (for simplicity, located at $X = .5$ and $X = 1.5$ in the diagram). The provers are allowed arbitrary setup between protocol rounds, as in Definition 5. Notation and behavior is otherwise analogous to Figure 3.

Soundness Proof Sketch (Proof Sketch of Theorem 2). Similar to the soundness proof of the single round protocol, here we also reduce the soundness of the multi-round CVPV protocol to the multi-round certified randomness protocol. Here, the only difference is that due to the multi-round nature of the compiler, we need to consider a multi-round ideal guessing game. In this ideal guessing game on the i-th round P_1 and P_2 are simultaneously given ch_i and asked to output the *same* correct answer ans_i. Note that, the usual definition of the certified randomness do not provide any guarantee on the winning probability of this guessing game. Therefore, we need to add the sequential decomposition property. Indeed, if no communication is allowed then due to the sequential decomposition property of the multi-round certified randomness protocol the winning probability of this guessing game will be negligible. The rest of the reduction to the real security game is similar to the proof sketch of Theorem 1. We refer to Theorem 7 for a more detailed analysis.

Sequential Decomposition from Repetition

We strengthen our result on multi-round compilers by showing the existence of a family of certified randomness protocols that are secure under our notion of sequential decomposition (Definition 1 or Definition 5 for a more formal version). In Theorem 3, we prove that certified randomness protocols based on repetition with single round entropy guarantees, including the well known protocols in [AH23, BCM+21a], satisfy Definition 5.

Proof Sketch of Theorem 3 We prove Theorem 3 by using the key observation that the prover's answers from the previous rounds do not help the guesser after the guess is already committed for each round. First, we consider an optimal adversary (maximum probability of succeeding the proof of quantumness test of the certified randomness protocol and the consistency check of the sequential decomposition property) where the prover may send information about previous answers to the guesser. We then consider a slightly modified adversary that has the same optimal success probability, but only the guesser is allowed to send information to the prover. For this modified adversary, the guesser simply assumes that all guesses are correct thus far. If at least one guess is incorrect, the protocol has already failed and the adversary strategy from then on does not matter. If the all guesses are correct, then pretending the answers are always the same as the guesses results in the correct behavior.

Specifically, we allow the guesser to be unbounded and prepare arbitrary quantum memory for both the guesser and the prover, and the quantum memory state is exactly that of the original optimal adversary (conditioned on classical outcomes on the answers and guesses agreeing with the answers). This adversary must have the same success probability as the original adversary and is therefore optimal. Further, the prover is no longer allowed to communicate with the guesser, and one can lower bound the entropy conditioned on the guesser side information and upper bound the protocol success probability.

Rapid Fire Compiler

In the CVPV protocols that are based on our sequential compiler, the verifiers need to wait for the answer to arrive from the prover before starting the next round. This may introduce some unwanted delay and make the CVPV protocol time consuming. There may also be certified randomness protocols that do not satisfy Definition 1. We show that one can overcome this drawback by sending the challenges without waiting for the responses from the provers. We refer to this compiler as the rapid fire compiler.

Construction: Similar to the sequential compiler here, the verifiers share $\{k_i, x_i, y_i, \mathsf{ch}_i\}_{i\in[\ell]}$. Moreover, the verifiers also share a fixed time interval Δ. During the protocol, verifiers send challenges to the prover in every Δ interval. If the protocol starts around time $t = 0$ then the i-th round starts at time $t = (i-1)\Delta$. On the i-th round, V_1 sends s_i, x_i, k_i, and V_2 sends y_i to P. Similar to the sequential compiler, after collecting all the responses for the ℓ rounds, the verifiers accepts the location of the claimed prover if it passes all the three checks. Note that, here the verifiers send the challenges in every Δ time intervals, then the verifiers should also receive the answers in Δ time interval. Therefore, the total time to run this protocol would be $(\ell-1)\Delta + 2$. For a very small Δ, this is a significant improvement over the sequential protocol that would require $2(\ell-1)$ time to finish. We refer to Figure 5 for the schematic diagram of this protocol. For clarity, we also provide a schematic of the protocol when the verifiers are instead interacting with two malicious provers in Figure 6.

Soundness Proof Sketch. For the rapid-fire compiler, if we assume that

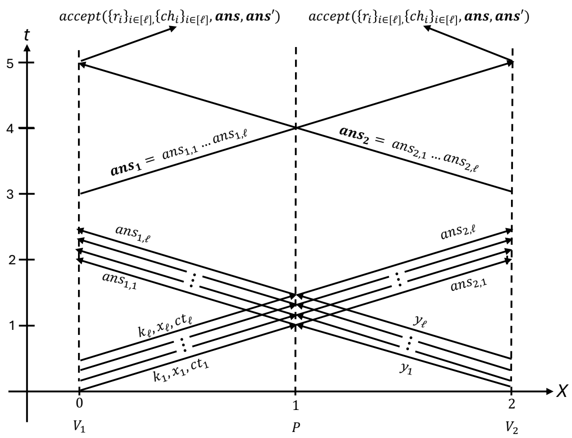

Figure 5: A spacetime diagram describing the interaction between two verifiers at locations $X = 0$ and $X = 2$ and an honest prover located at the claimed position (for simplicity, located at $X = 1$ in the diagram). The verifiers pre-share random values x_i, y_i, k_i, r_i for $i \in [\ell]$ prior to the start of the protocol, and set $s_i = ch_i \oplus G_{k_i}(x_i \oplus y_i)$ for some family of hash functions $\{G_k\}$ and $ch_i = \mathsf{Gen_i}(1^n; r)$ for $\mathsf{Gen_i}$ the verifier functionality of some multi-round certified randomness verifier on round i and where $accept(\cdot)$ determines a boolean function that determines whether the verifiers accept the provers claim based on the transcript received. Verifiers rapidly send each new challenge every Δ seconds.

the malicious provers do not communicate the answers to each other during the runtime of the protocol, then we can directly apply the entropy guarantee to upper bound the guessing probability without the sequential decomposition property. However, to satisfy this requirement we need to assume the condition $\Delta l < 2t_{\text{comm}}$ applies to the protocol, where t_{comm} denotes the communication time between any two malicious provers.

Note that, due to this condition the rapid-fire compiler can only verify whether the prover is within a range of positions, that satisfy the $2t_{\text{comm}}$ requirement. By reducing Δ, and the number of rounds l one can reduce the $2t_{\text{comm}}$ communication time requirement, but that would introduce additional engineering challenges for the implementation. It can make the protocol less-robust to noise as well. One possible way to increase the robustness of the protocol just by sequential or parallel repetition. In this paper, we have studied the impact of sequential repetition of this compiler, called Sequential Rapid Fire. We refer to Section 4.4 for the details of this construction.

Instantiation using Random Circuit Sampling (RCS)

We instantiate the protocol using certified randomness based on random circuit sampling (RCS). Aaronson and Hung [AH23] show that under some models (e.g. a fully general adversary given oracle access to challenge circuits), passing

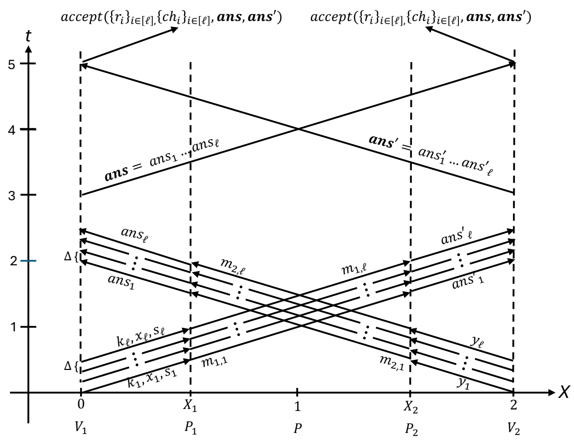

Figure 6: A spacetime diagram describing the interaction between two verifiers at locations $X = 0$ and $X = 2$ and two dishonest prover located at arbitrary positions between V_1 and V_2 (for simplicity, located at $X = .5$ and $X = 1.5$ in the diagram). The provers are allowed to communicate during the protocol but are non-signaling. Notation and behavior is otherwise analogous to Figure 5.

the XHOG test (achieving high average probability $p_C(z)$ over choices of C and output z) implies $\Omega(n)$ von Neumann entropy conditioned on quantum side information, where n is the number of qubits. We formally define the protocols in Appendix B, shown in Figure 9 and Figure 10. The single round entropy guarantees are given by Theorem 12 and Theorem 13.

1.4 Open Problems

In this section, we highlight the remaining problems related to classical verifier position verification.

Security in the Plain Model:

In this paper, we prove the soundness of the compilers in quantum random oracle model. However, it is crucial to have the security analysis in the plain model for a practical implementation of this protocol.

Minimum Sufficient Condition for the CVPV:

This paper requires proof of quantumness-based certified randomness to construct the CVPV protocol. However, it is not clear whether this is the most minimal assumption. We leave the minimum sufficient assumption required to construct a CVPV protocol as an open problem.

2 Preliminaries

We now recall a collection of useful definitions and results froim the literature. Throughout the paper, we denote the security parameter by λ.

2.1 Quantum Information

Random Oracle Model.

Lemma 1 ([BBBV97]). *Let $\mathcal{A}$ be an oracle algorithm which makes at most T oracle queries to a function $H : \{0,1\}^m \to \{0,1\}^n$. Define $|\phi_i\rangle$ as the global state after $\mathcal{A}$ makes i queries, and $W_y(|\phi_i\rangle)$ as the sum of squared amplitudes in $|\phi_i\rangle$ of terms in which $\mathcal{A}$ queries H on input y. Let $\epsilon > 0$ and let $F \subseteq \{0,1,\ldots,T-1\} \times \{0,1\}^m$ be a set of time-input pairs such that $\sum_{(i,y)\in F} W_y(|\phi_i\rangle) \leq \epsilon^2/T$.*

For $i \in \{0,1,\ldots,T-1\}$, let H'_i be an oracle obtained by reprogramming H on inputs in $\{y \in \{0,1\}^m : (i,y) \in F\}$ to arbitrary outputs. Let $|\phi'_T\rangle$ be the global state after $\mathcal{A}$ is run with oracle H'_i on the ith query (instead of H). Then, $\mathsf{TD}\left(|\phi_T\rangle, |\phi'_T\rangle\right) \leq \epsilon/2$.

The following lemma states that it is possible to efficiently simulate a random oracle for a quantum algorithm for which a query-bound is known in advance.

Lemma 2 ([Zha15]). *A random oracle $H : \mathcal{X} \to \mathcal{Y}$ is perfectly indistinguishable from a $2q$-wise hash independent hash function $H' : \mathcal{X} \to \mathcal{Y}$ against a quantum algorithm $\mathcal{A}$ which makes at most q queries.*

2.2 Proof of Quantumness (PoQ)

Definition 2 (PoQ Protocol). *A* proof of quantumness *protocol $\mathscr{P} = (V, P)$ is an interactive protocol between a classical verifier V and an allegedly quantum prover P. Naturally, since V is classical, so is all communication. At the end of the protocol, V either accepts or rejects. $\mathscr{P}$ is parametrized by a security parameter λ and is required to satisfy the following guarantees:*

- **Correctness:** *There exists a QPT prover P such that V accepts with overwhelming probability $(1 - \mathsf{negl}(\lambda))$.*
- **s-Soundness:** *For any PPT prover P, the probability that V accepts is at most $s + \mathsf{negl}(\lambda)$.*

Certified Randomness. A property stronger than soundness is certified randomness. At a high level, certified randomness requires that if a prover P passes the PoQ protocol, then its output cannot be predicted by a guesser E who:

1. Knows the challenge messages sent by V, and
2. Shares entanglement with P.

In the most general case, we require this to hold even if P is fully malicious (a.k.a. a *fully general device*). We give the formal definition below.

Definition 3 (Certified Randomness)**.** *A PoQ protocol $\mathscr{P}$ is said to have* certified randomness *property if for any QPT prover P, conditioned on V accepting, it is true with overwhelming probability that*

$$H_{\min}(Z \mid CE)_\rho \geq \omega(\log \lambda), \quad \textit{where,}$$

- *$\rho = \rho_{ZCDE}$ is the final state of P, with D being the working register.*
- *C is a classical register containing all the messages sent by V.*
- *A is the classical register containing the final message sent by P.*
- *E is arbitrary (possibly entangled) quantum side information of P such that P does not act on E during the protocol.*

2.3 Position Verification with Classical Verifiers

We focus on position verification in one dimension and give the corresponding definition in the idealized model below. We closely follow the vanilla model of [LLQ22]. Nonetheless, we remark that our work could be generalized to higher dimensions and more robust models.

Definition 4 (Position Verification with Classical Verifiers)**.** *A position verification scheme $\mathscr{V} = (V, X)$ with classical verifiers is an interactive relativistic protocol between a set of classical verifiers $V = (V_i, X_i)_{i \in I}$, where each classical verifier V_i is located at position $X_i \in \mathbb{R}$ on the real line, and $X \in \mathbb{R}$ is the purported location of a quantum prover. During the protocol, we assume that all communication happens at the speed of light (1) and all computation is instantaneous. We also assume that V can perform a secure setup before the protocol, and communicate securely during the protocol.*

We say that $\mathscr{V}$ is complete *if there exists an efficient prover P such that if P is located at X, then the probability that the verifiers V accept with overwhelming probability.*

We say that $\mathscr{V}$ is sound *if for any collection of efficient, possibly entangled malicious provers $P = (P_j)_{j \in J}$, the probability that V accepts is negligibly small.*

3 CVPV from Single-Round Certified Randomness

We give a generic construction from a (one-round) PoQ scheme $\mathscr{P} = (P, V)$ with certified randomness. The basic idea is as follows: the verifiers will send two hash inputs x, y from opposing directions such that they reach the alleged location of the prover at the same time. The challenge ch of $\mathscr{P}$ will be computed via evaluating a secure hash function on input $x \oplus y$. This way, the prover needs to receive both x and y before being able to run P. A malicious set of provers in our CVPV protocol, intuitively, will be forced into two options:

1. Try to (at least partially) run P before receiving both x and y, and fail the verification of V.

2. Run P with the knowledge of ch at two locations, and try to get a matching outcome, hence fail due to the certified randomness property.

Without loss of generality, $V = (\mathsf{Gen}, \mathsf{Ver})$ has the following syntax:

1. It samples random coins $r \leftarrow \{0,1\}^{\mathsf{poly}(\lambda)}$.

2. It deterministically generates a challenge $\mathsf{ch} = \mathsf{Gen}(1^\lambda; r) \in \{0,1\}^n$, and sends it to the prover.

3. After receiving an answer ans from the prover, it deterministically verifies by running $\mathsf{Ver}(\mathsf{ch}, \mathsf{ans}; r)$.

Construction 1. Let $\{G_k\}_{k\in\{0,1\}^\lambda} : \{0,1\}^m \to \{0,1\}^n$ be a cryptographic hash function family, with $m = \omega(\log \lambda)$. We describe the CVPV protocol below:

1. At time $t = -\infty$, the verifiers sample random coins $r \leftarrow \{0,1\}^{\mathsf{poly}(\lambda)}$ for V, a hash key $k \leftarrow \{0,1\}^\lambda$, and random inputs $x, y \leftarrow \{0,1\}^m$. They publish the hash key k, and set $s = G_k(x \oplus y) \oplus \mathsf{ch}$.

2. At $t = 0$, V_0 sends (x, s) and V_1 sends y to the prover simultaneously.

3. The honest prover, located at position 1, computes $\mathsf{ch} = G_k(x \oplus y) \oplus s$ and $\mathsf{ans} \leftarrow P(\mathsf{ch})$. He immediately sends ans to both verifiers.

4. V_0 expects ans at time $t = 2$. Similarly, V_1 expects ans' at time $t = 2$.

5. The verifiers accept iff $\mathsf{ans} = \mathsf{ans}'$, and $\mathsf{Ver}(\mathsf{ch}, \mathsf{ans}; r)$ accepts.

Completeness. Completeness follows by completeness of $\mathscr{P}$.

Soundness Proof in QROM.

Theorem 6 (Single-Round)**.** *Let $\mathscr{P} = (V, P)$ be a one-round PoQ scheme that satisfies Definition 3. Then, Construction 1 is a CVPV scheme that is sound in the quantum random oracle model.*

Proof. We will model G_k as a classical random oracle G with superposition access. We will create a sequence of hybrids.

- **Hybrid 0:** This is the original CVPV soundness experiment.
- **Hybrid 1:** In this hybrid, the adversary consists of only two parties: $\mathcal{A}$ at position 0 and $\mathcal{B}$ at position 1.

- **Hybrid 2:** In this hybrid, we replace the oracle at times $t < 1$ with the punctured oracle $G^{\perp}$, defined as

$$G^{\perp}(z) = \begin{cases} G(z), & z \neq x \oplus y \\ u, & z = x \oplus y \end{cases},$$

where $u \in \{0,1\}^n$ is a uniform string.

- **Hybrid 3:** In this hybrid, we also replace the oracles accessed by $\mathcal{A}$ and $\mathcal{B}$ at time $t = 1$ with $G^{\perp}$ defined above. In addition, we give ch as input to both $\mathcal{A}$ and $\mathcal{B}$ at time $t = 1$.

- **Hybrid 4:** In this hybrid, $\mathcal{A}$ and $\mathcal{B}$ each get (only) ch as input at time $t = 0$, but they are not allowed to communicate. Also, they do not get access to the oracle $G^{\perp}$.

Let p_i be the optimal success probability of an efficient adversary in **Hybrid** i. Let $q = \mathsf{poly}(\lambda)$ be an upper-bound on the total number of oracle queries made by $(\mathcal{A}, \mathcal{B})$. We will show a sequence of claims which suffice for the proof:

Claim 1. $p_1 \geq p_0$.

Proof. This step is standard.[2] One can easily perform a reduction where $\mathcal{A}$ of **Hybrid 1** can simulate all adversaries in $[0, 0.5)$ in **Hybrid 0** and $\mathcal{B}$ of **Hybrid 1** can simulate all adversaries in $(0.5, 1]$ in **Hybrid 0**. □

Claim 2. $|p_2 - p_1| \leq \mathsf{negl}(\lambda)$.

Proof. Suppose the inequality is false for $(\mathcal{A}, \mathcal{B})$, i.e. $|p_2 - p_1| < \varepsilon$ for a non-negligible function $\varepsilon(\lambda)$. Then, by Lemma 1, in **Hybrid 2** the query weight on $G(x, y)$ by $\mathcal{A}$ (the case of $\mathcal{B}$ being similar) at time $t < 1$ is lower-bounded by $2\varepsilon^2/q$. Consider the following extractor $\mathcal{A}'(\mathcal{A})$:

- $\mathcal{A}'$ receives (x, s) from the challenger and the A register of the initial state $|\psi\rangle_{AB}$ for $(\mathcal{A}, \mathcal{B})$. Then $\mathcal{A}'$ samples $i \leftarrow [q]$ and runs $\mathcal{A}$ on input (x, s, A), measuring the input register of the i-th query made by $\mathcal{A}$ to G as z^*. She outputs $y^* = z^* \oplus x$.

Now, the probability that $\mathcal{A}'$ outputs y is at least $2\varepsilon^2/q^2$ due to no-signalling, which is a contradiction since $\mathcal{A}'$ has no information about y and $2\varepsilon^2/q^2 > 2^{-m}$. □

Claim 3. $p_3 \geq p_2$.

Proof. Follows by a simple reduction $(\mathcal{A}', \mathcal{B}')$, which simulates $(\mathcal{A}, \mathcal{B})$ in **Hybrid 2**. $\mathcal{A}'$ forwards (x, s) and $\mathcal{B}'$ forwards y. Furthermore, they use (ch, x, y, s) to reprogram the oracle $G^{\perp}$ in order to simulate the oracle G. □

[2] For instance, see [LLQ22].

Claim 4. $p_4 \geq p_3$.

Proof. We give a reduction $(\mathcal{A}', \mathcal{B}')$ from **Hybrid 3** to **Hybrid 4**:

- Let $(\mathcal{A}, \mathcal{B})$ be an adversary for **Hybrid 3** that succeeds with probability p_3.
- At time $t = -\infty$, $\mathcal{A}'$ and $\mathcal{B}'$ prepare the bipartite state $|\psi\rangle_{AB}$ shared between $\mathcal{A}$ and $\mathcal{B}$. In addition, they sample a $2q$-wise independent hash function G' as well as $(x, y, s) \leftarrow \{0,1\}^m \times \{0,1\}^m \times \{0,1\}^n$.
- At time $t = 0$, $\mathcal{A}'(t = 0)$ runs $\mathcal{A}$ on input (x, s, A), using G' as the oracle. At time $t = 1$, $\mathcal{A}'$ receives ch from the verifier and runs $\mathcal{A}(t = 1)$ with ch as additional input.
- At time $t = 0$, $\mathcal{B}'(t = 0)$ runs $\mathcal{B}$ on input (y, B), using G' as the oracle. At time $t = 1$, $\mathcal{B}'$ receives ch from the verifier and runs $\mathcal{B}(t = 1)$ with ch as additional input.

Observe that since the oracle $G^{\perp}$ in **Hybrid 3** is independent of (x, y, s, ch), and by Lemma 2, the view of $(\mathcal{A}, \mathcal{B})$ is perfectly simulated by the reduction. □

Claim 5. $p_4 \leq \mathsf{negl}(\lambda)$.

Proof. Suppose p_4 is not negligible for some $(\mathcal{A}, \mathcal{B})$. We will break the certified randomness (Definition 3) of $\mathscr{P}$:

- P holds the A register of $|\psi\rangle_{AB}$ prepared by $(\mathcal{A}, \mathcal{B})$ at time $t < 0$. After receiving ch from the verifier, P runs $\mathcal{A}(t \geq 0)$ and outputs ans which is sent to the verifier.
- The guesser Q holds register $E = B$. She eavesdrops ch and runs $\mathcal{B}(t \geq 0)$ to output ans'.

With probability p_4, $\mathsf{ans} = \mathsf{ans}'$ and ans is accepted by the verifier (denoted by event ACC). Thus, we have

$$p_4 \leq \Pr[\mathsf{ans} = \mathsf{ans}' \mid ACC] \leq 2^{-H_{\min}(\mathsf{ans} \mid \mathsf{ch}, E)}$$
$$\implies H_{\min}(\mathsf{ans} \mid \mathsf{ch}, E) \leq \log_2(1/p_4) \leq O(\log \lambda),$$

which violates certified randomness (Definition 3). □

□

Remark 2. *Note that soundness still holds if the adversary $(\mathcal{A}, \mathcal{B})$ get access to G at time $t = -\infty$. This means we can heuristically instantiate G using an unkeyed public hash function such as SHA-512.*

4 CVPV from Multi-Round Certified Randomness

If the underlying PoQ-based certified randomness protocol uses more than round, we can naturally generalize our compiler just by composing our single-round compiler sequentially. We first give a natural way to do this in Section 4.1. This requires a protocol satisfying the stronger Definition 5 of certified randomness with sequential decomposition, but we show that any protocol satisfying the definition of certified randomness with single round entropy must satisfy the sequential decomposition property in Appendix A, lending its applicability to a wide range of possible instantiations. We then give a more clever way in Section 4.3 and Section 4.4 which is superior in the idealized model at the cost of practical robustness.

Definition 5 (Multi-round Certified Randomness Protocol with Sequential Decomposition Property)**.** *An ℓ-round PoQ protocol $\mathscr{P}$ is said to have* sequential decomposition *property if no pair of a QPT prover P and an unbounded guesser Q can succeed in the following security game with non-negligible probability:*

- *For $i \in [\ell]$, the following steps occur in order:*
  1. *The verifier V of $\mathscr{P}$ sends a challenge ch_i to both P and Q.*
  2. *P sends back an answer ans_i.*
  3. *Q outputs a guess ans'_i.*
  4. *P and Q can communicate freely and setup again.*
- *(P, Q) win the game if V accepts and $\mathsf{ans}_i = \mathsf{ans}'_i$ for all $i \in [\ell]$.*

We also consider a weaker variant of Definition 5 by restricting the communication round between P and Q, with the difference being highlighted:

Definition 6 (Multi-round Sequential Certified Randomness with Sequential Decomposition and Restricted Communication)**.** *An ℓ-round PoQ protocol $\mathscr{P}$ is said to have* sequential certified randomness with restricted communication *if no pair of a QPT prover P and an unbounded guesser Q can succeed in the following security game with non-negligible probability:*

- *For $i \in [\ell]$, the following steps occur in order:*
  1. *The verifier V of $\mathscr{P}$ sends a challenge ch_i to both P and Q.*
  2. *P sends back an answer ans_i.*
  3. *Q outputs a guess ans'_i.*
  4. *P and Q can perform simultaneous single-round communication.*
- *(P, Q) win the game if V accepts and $\mathsf{ans}_i = \mathsf{ans}'_i$ for all $i \in [\ell]$.*

Remark 3. *For single-round $\mathscr{P}$, Definitions 3 and 5 to 7 all coincide.*

We say that two spatially separated parties $(\mathcal{A}, \mathcal{B})$ perform *one round of simultaneous communication* at time t if $\mathcal{A}$ sends one (classical or quantum) message to $\mathcal{B}$ at time t and vice versa.

4.1 Sequential Compiler

As before, we give a generic construction from a (multi-round) PoQ scheme $\mathscr{P} = (V, P)$ which has certified randomness with sequential decomposition (Definition 6).

Construction 2. Let $\ell = \mathsf{poly}(\lambda)$ be the number of rounds in $\mathscr{P}$. Without loss of generality, $V = (\mathsf{Gen}_1, \dots, \mathsf{Gen}_\ell, \mathsf{Ver})$ has the following syntax:

1. It samples random coins $r \leftarrow \{0,1\}^{\mathsf{poly}(\lambda)}$.
2. For $i = 1, \dots, \ell$:
   - It deterministically generates a challenge $\mathsf{ch}_i = \mathsf{Gen}_i(1^\lambda, \mathsf{ans}_1, \dots, \mathsf{ans}_{i-1}; r) \in \{0,1\}^n$.
   - It receives an answer ans_i from P.
3. It deterministically verifies by running $\mathsf{Ver}(\mathsf{ch}_1, \mathsf{ans}_1, \dots, \mathsf{ch}_\ell, \mathsf{ans}_\ell; r)$.

Similarly, $P = (P_1, \dots, P_\ell)$ has the following syntax: For $i = 1, \dots, \ell$, after receiving the i-th challenge ch_i, P computes

$$\mathsf{ans}_i \leftarrow P_i(\mathsf{ch}_1, \mathsf{ans}_1, \dots, \mathsf{ch}_{i-1}, \mathsf{ans}_{i-1}, \mathsf{ch}_i)$$

and responds with ans_i.

Let $\{G_k\}_{k \in \{0,1\}^\lambda} : \{0,1\}^m \to \{0,1\}^n$ be a cryptographic hash function family, with $m = \omega(\log \lambda)$. We describe the (multi-round) CVPV protocol below:

1. At time $t = -\infty$, the verifiers sample random coins $r \leftarrow \{0,1\}^{\mathsf{poly}(\lambda)}$ for V and a hash key $k \leftarrow \{0,1\}^\lambda$. For $i = 1, \dots, \ell$, they sample random inputs $x_i, y_i \leftarrow \{0,1\}^m$. They publish the hash key k.
2. For $i = 1, \dots, \ell$:
   - At time $t = i-1$, V_0 computes $\mathsf{ch}_i = \mathsf{Gen}_i(1^\lambda, \mathsf{ans}_1, \dots, \mathsf{ans}_{i-1}; r)$ and $s_i = G_k(x_i \oplus y_i) \oplus \mathsf{ch}_i$. It sends (x_i, s_i) and expects an answer ans_i at time $t = i$.
   - Similarly, at time $t = i - 1$, V_1. It sends y_i and expects an answer ans'_i at time $t = i$.
   - At time $t = i - 1/2$, the honest prover, located at position 0.5, computes $\mathsf{ch}_i = G_k(x_i \oplus y_i) \oplus s_i$ and $\mathsf{ans}_i \leftarrow P_i(\mathsf{ch}_1, \dots, \mathsf{ch}_i, \mathsf{ans}_1, \dots, \mathsf{ans}_{i-1})$. It immediately sends ans_i to both verifiers.
3. The verifiers accept iff $\mathsf{ans}_i = \mathsf{ans}'_i$ for all i, and $\mathsf{Ver}(\mathsf{ch}_1, \mathsf{ans}_1, \dots, \mathsf{ch}_\ell, \mathsf{ans}_\ell; r)$ accepts.

Security Proof in QROM.

Theorem 7 (Sequential Compiler). *Let $\mathscr{P} = (V, P)$ be a PoQ scheme that satisfies Definition 6. Then, Construction 2 is a secure CVPV scheme.*

Proof. We will model G_k, where $k \leftarrow \{0,1\}^\lambda$, as a random oracle G. We give a sequence of hybrid experiments below:

- **Hybrid 0:** This is the original CVPV soundness experiment.
- **Hybrid 1:** In this hybrid, the adversary consists of only two parties: $\mathcal{A}$ at position 0 and $\mathcal{B}$ at position 1. W.l.o.g., $(\mathcal{A}, \mathcal{B})$ perform a round of simultaneous communication at times $t = 0, 1, \dots, \ell - 1$.
- **Hybrid 2:** In this hybrid, we additionally give $\mathcal{A}$ and $\mathcal{B}$ ch_i at time $t = i$ for $i = 1, \dots, \ell$.
- **Hybrid 2.1-ℓ:** We set **Hybrid 2.0** to be **Hybrid 2** and $G_0 := G$. For $i \in [\ell]$, we define **Hybrid 2.i** to be the same as **Hybrid 2.$(i-1)$**, except the oracle G_{i-1} is replaced by the reprogrammed oracle G_i, where

$$G_i(z) = \begin{cases} G_{i-1}(z), & z \neq x_i \oplus y_i \\ u_i, & z = x_i \oplus y_i \end{cases},$$

  with $u_i \leftarrow \{0,1\}^n$ being a fresh random string.
- **Hybrid 3:** In this hybrid, $\mathcal{A}$ and $\mathcal{B}$ only receive ch_i at time $t = i$, for $i \in [\ell]$, and no other input. They do not get access to the oracle G_ℓ either.

Let p_i be the optimal success probability of an efficient adversary in **Hybrid** i. Let $q = \mathsf{poly}(\lambda)$ be an upper-bound on the total number of oracle queries made by $(\mathcal{A}, \mathcal{B})$. We will show a sequence of claims which suffice for the proof:

Claim 6. $p_1 \geq p_0$.

Proof. Follows by a simple generalization of the corresponding claim in the proof of Theorem 6. ☐

Claim 7. $p_2 \geq p_1$.

Proof. Since we give extra information to the adversary, the success probability cannot decrease. ☐

Claim 8. *Setting $p_{2.0} := p_2$, $p_{2.i} \geq p_{2.(i-1)} - \mathsf{negl}(\lambda)$ for $i \in [\ell]$.*

Proof. Let $i \in [\ell]$ and $(\mathcal{A}, \mathcal{B})$ be an adversary that succeeds in **Hybrid 2.**$(i-1)$ with probability $p_{2.(i-1)}$. We will give a reduction $(\mathcal{A}', \mathcal{B}')$ for **Hybrid 2.**i:

- At times $t < i$, $\mathcal{A}'$ (resp. $\mathcal{B}'$) runs $\mathcal{A}$ (resp. $\mathcal{B}$) using G_i as the oracle.
- At time $t = i - 1$, $\mathcal{A}'$ sends (x_i, s_i) and $\mathcal{B}'$ sends y_i to each other, so that the messages are received at $t = i$.

- At times $t \geq i$, $\mathcal{A}'$ and $\mathcal{B}'$ can simulate G_{i-1} using $(x_i, y_i, s_i, \mathsf{ch}_i, G_i)$ by reprogramming G_i to output $\mathsf{ch}_i \oplus s_i$ on input $x_i \oplus y_i$.

- $\mathcal{A}'$ (resp. $\mathcal{B}'$) outputs what $\mathcal{A}$ (resp. $\mathcal{B}$) outputs.

Note that the view of $(\mathcal{A}, \mathcal{B})$ as simulated by $(\mathcal{A}', \mathcal{B}')$ differs from **Hybrid 2.**$(i-1)$ at times $t < i$, and only on input $x_i \oplus y_i$ to the oracle. Therefore, if the probability that $(\mathcal{A}', \mathcal{B}')$ succeeds is upper-bounded by $p_{2.(i-1)} - \varepsilon$ for some non-negligible function ε, then by Lemma 1 the total query weight by $(\mathcal{A}, \mathcal{B})$ on input $x_i \oplus y_i$ at times $t < i$ must be at least $2\varepsilon^2/q$. Suppose the query weight by $\mathcal{A}$ is at least ε^2/q, for the other case is similar. We give an extractor $(\widetilde{\mathcal{A}}, \widetilde{\mathcal{B}})$ in **Hybrid 2.**$(i-1)$:

- $\widetilde{\mathcal{A}}$ samples $j \leftarrow [q]$ and simulates $\mathcal{A}$, stopping the execution at the j-th query made by $\mathcal{A}$ to the oracle G_{i-1}, measuring the query as z^*. She outputs $y^* = z^* \oplus x_i$, where x_i is received at time $t = i - 1$ from V_0.

- $\widetilde{\mathcal{B}}$ simulates $\mathcal{B}$.

By assumption, $y^* = y_i$ with probability $\varepsilon^2/q^2 > 2^{-m}$, which is a contradiction since y_i is information theoretically hidden from $\widetilde{\mathcal{A}}$ at times $t < i$. □

Claim 9. $p_3 \geq p_{2.\ell}$.

Proof. Let $(\mathcal{A}, \mathcal{B})$ be an adversary for **Hybrid 2.**ℓ that succeeds with probability $p_{2.\ell}$. We give a reduction $(\mathcal{A}', \mathcal{B}')$ that succeeds in **Hybrid 3** with the same probability:

- At time $t = -\infty$, $\mathcal{A}'$ and $\mathcal{B}'$ sample a $2q$-wise independent hash function G'. In addition, they sample $(x_i, y_i, s_i) \leftarrow \{0,1\}^m \times \{0,1\}^m \times \{0,1\}^n$ for $i \in [\ell]$.

- $\mathcal{A}'$ simulates $\mathcal{A}$ using G' as the oracle, the sampled values (x_i, y_i), as well as the values ch_i received from V_0.

- $\mathcal{B}'$ similarly simulates $\mathcal{B}$ using G' as the oracle, the sampled values y_i, as well as the values ch_i received from V_1.

The view of $(\mathcal{A}, \mathcal{B})$ is perfectly simulated since the oracle G_ℓ in **Hybrid 2.**ℓ is independent of the values (x_i, y_i, s_i) for all $i \in [\ell]$. This is because the oracle has been reprogrammed on all inputs $x_i \oplus y_i$ to remove any such dependence. Thus, by Lemma 2, G' simulates an independent random oracle and the proof is complete. □

Claim 10. $p_3 \leq \mathsf{negl}(\lambda)$.

Proof. Follows directly from Definition 6. $\mathcal{A}$ plays the role of the prover and $\mathcal{B}$ that of the eavesdropper. □

□

4.2 Sequential Decomposition from Repetition

This section uses the same notation as Appendix A. Although other multi-round approaches are possible, the most general sequential compilation approach is desirable due to practical robustness considerations. Section 4.1 proves that one can construct CVPV protocols from certified randomness protocols with the sequential decomposition property. However, the usual notion of certified randomness (Definition 3) is defined in terms of entropy lower bounds, but we cannot lower bound the CVPV protocol entropy conditioned on the guesser's side information since she can communication with the prover. Therefore, it is not immediately obvious whether a certified randomness protocol defined with entropy is a sequential certified randomness protocol (Definition 5) defined by the guessing probability. We show that for a large class of multi-round certified randomness protocols, namely those that rely on repetition of single rounds with entropy bounds 'on average', all have the sequential decomposition property.

Definition 7 (Certified Randomness from Repetition)**.** *A PoQ protocol $\mathscr{P}$ is said to be* certified randomness from repetition *if*

- *The verifier V of $\mathscr{P}$ samples ℓ challenges $\{\mathsf{ch}_1, \ldots, \mathsf{ch}_\ell\}$ in an i.i.d. manner.*
- *For $i \in [\ell]$, the following steps occur in order:*
  1. *The verifier V of $\mathscr{P}$ sends the challenge ch_i to P.*
  2. *P sends back an answer ans_i.*
  3. *V computes a classical output X_i from ch_i and ans_i.*
- *V accepts if $X_1^n \equiv X_1 \cdots X_n = x_1^n \in \omega'$, where x_1^n is the classical value of register X_1^n and ω' is a set of acceptable values of x_1^n that satisfy the certified randomness test condition.*
- *For any QPT prover P and verifier V described by the quantum channel $\mathcal{P}_i : R_{i-1} \to X_i A_i C_i R_i, \mathcal{P}_n \circ \cdots \circ \mathcal{P}_1$, we have*

$$\inf_{\nu \in \Sigma_i(q)} H(A_i|C_iE)_\nu \geq f(q), \quad \textit{where} \tag{1}$$

$$\Sigma_i(q) = \left\{ \nu_{X_iA_iC_iR_iE} = \mathcal{P}_i(\rho) \middle| \rho \in S(R_{i-1}E) \wedge \nu_{X_i} = q \right\}, \tag{2}$$

  R is the quantum memory, A is the output register for ans, C is the challenge register for ch, E is the quantum side information register, $S(R_{i-1}E)$ is the set of all quantum states on $R_{i-1}E$, $q \in \mathbb{P}$, $\mathbb{P}$ is the set of density operators corresponding to classical probability distributions on the alphabet $\mathcal{X}$ of X_i, and f is an affine function.

- *For*

$$h = \min_{x_1^n \in \omega'} f\left(\mathsf{freq}(x_1^n)\right) \tag{3}$$

$$\mathsf{freq}(x_1^n)(x) = \frac{|\{i \in \{1, \ldots, n\} : x_i = x\}|}{n}, \tag{4}$$

  we have $h > 0$.

Indeed, in the situation where we only care about the side information in the challenges or the initial quantum register E that does not evolve, the Markov chain condition is trivially satisfied since the challenges are generated in an i.i.d. manner. In such a case, the quantum channel of the protocol is illustrated in Fig. 8(a). Therefore, we can apply the entropy accumulation theorem [DFR20] to a certified randomness from repetition protocol to lower bound the smooth min-entropy. Conversely, any protocol that can be proven sound using the entropy accumulation theorem must satisfy Definition 7. Similarly, for protocols that are secure under a more general adversary model where the environment may be updated each round and use the generalized entropy accumulation theorem of [MFSR22] to prove soundness, they must be secure under the more restricted model where the environment cannot be updated. They must satisfy Definition 7 since generalized entropy accumulation has a stronger single-round entropy requirement.

We note that many existing protocols reuse challenges due to the need for randomness expansion. However, randomness expansion does not concern CVPV, and generating challenges for every round makes the analysis simpler.

To show that protocols satisfying Definition 7 can be used to construct CVPV protocols (illustrated in Fig. 8(b)) with the sequential decomposition property, we first consider an optimal adversary with the largest overall acceptance probability $\Pr[\Omega]$, where Ω denotes the event where the answers pass the protocol statistical test and all the guesses are correct. We denote the quantum channel of the n-round optimal adversary as $\mathcal{M}_n^{'*} \circ \cdots \circ \mathcal{M}_1^{'*}$. We then construct a modified adversary $\bar{\mathcal{M}}_n' \circ \cdots \circ \bar{\mathcal{M}}_1'$ from this optimal adversary, and show that the modified adversary has the same $\Pr[\Omega]$. Then, we show the modified adversary also satisfies the non-signalling condition required by the generalized entropy accumulation theorem [MFSR22]. This allows us to lower bound the smooth min-entropy conditioned on the guesses and other side information of the modified adversary using the generalized entropy accumulation theorem. Finally, we derive an upper bound on $\Pr[\Omega]$ by using the fact that either the test fails with high probability, or the prover output has high entropy relative to the guesses and the guesser must fail. A rigorous proof is given in Supplement Section Appendix A.

Consider an intermediate quantum-classical state for the optimal adversary:

$$\sum_{a_1^i c_1^i g_1^i} p^*(a_1^i c_1^i g_1^i) |a_1^i c_1^i g_1^i\rangle\langle a_1^i c_1^i g_1^i|_{A_1^i C_1^i G_1^i} \otimes \rho^{*a_1^i c_1^i g_1^i}_{R_i R_i'},$$

where R_i, R_i' are prover and guesser quantum memory registers after the ith round, $A_1^i C_1^i G_1^i$ are classical registers of the answers, challenges, and guessers for the first i rounds, lowercase variables are classical values of the respective registers, p^* is the probability of the classical outcome, and ρ^* is the quantum state on the quantum memory corresponding to the classical outcome. We define the modified adversary quantum channel $\bar{\mathcal{M}}_n' \circ \cdots \circ \bar{\mathcal{M}}_1'$ as

$$\bar{\mathcal{M}}_{i+1}' = \Gamma_{i+1} \circ \mathrm{tr}_{R_{i+1} R_{i+1}'} \circ \mathcal{M}_{i+1}^{'*} \circ \Gamma_i \circ \mathrm{tr}_{R_i R_i'}, \tag{5}$$

where $\Gamma_i : C_1^i G_1^i \to R_i R_i' C_1^i G_1^i$ is a quantum channel give by

$$\Gamma_i(\rho) = \sum_{c_1^i g_1^i} \Pi_{C_1^i G_1^i}^{c_1^i g_1^i} \; \rho \; \Pi_{C_1^i G_1^i}^{c_1^i g_1^i} \otimes |c_1^i g_1^i\rangle\langle c_1^i g_1^i| \otimes \rho_{R_i R_i'}^{*g_1^i c_1^i g_1^i}, \tag{6}$$

where Π is the projector onto classical values.

Intuitively, the modified quantum channel first throws the quantum memory away with $\mathrm{tr}_{R_i R_i'}$, and then replaces the memory with another memory state. An optimal adversary may use the quantum memory depends on the classical history $a_1^i c_1^i g_1^i$. Fortunately, this is not an issue. If the guess is incorrect ($g_1^i \neq a_1^i$), then the protocol has already aborted and it does not matter what quantum memory is supplied to the next round. If the guess is correct ($g_1^i = a_1^i$), then the supplied quantum memory supplied by the modified adversary is the same as that of an optimal adversary ($\rho_{R_i R_i'}^{*g_1^i c_1^i g_1^i} = \rho_{R_i R_i'}^{*a_1^i c_1^i g_1^i}$). This concludes the proof that the modified adversary defined in E.q. 5 has the maximum success probability.

Further, since the prover output a_i is discarded (here, single round classical output register is denoted as A_i and the value is denoted as a_i, and the single round challenges and guesses are similarly denoted as $C_i G_i$ and $c_i g_i$), the output side information must be independent on a_i. The quantum channel defined in E.q. 5 satisfies the non-signalling condition. Namely, for all i, there exists $\mathcal{R}_{i+1} : E_i \to E_{i+1}$ such that

$$\mathrm{tr}_{A_{i+1} R_{i+1}} \circ \bar{\mathcal{M}}_{i+1}' = \mathcal{R}_{i+1} \circ \mathrm{tr}_{R_i}, \tag{7}$$

where $E_i = C_1^i G_1^i R_i'$. This is apparent from Fig. 7(c).

However, we only have single round entropy for certified randomness shown in Fig. 7(a). Namely, $H(A_i|C_i E) \geq f(q)$ for arbitrary input quantum states over $R_{i-1}E$, where $f(q)$ is a function on some test outcome. Instead, in order to use entropy accumulation for the CVPV protocol, for the channel illustrated in Fig. 7(c), we need $H(A_i|E_i \tilde{E}) \geq f(q)$ for arbitrary input quantum states over $R_{i-1} E_{i-1} \tilde{E}$.

Since processing with $\mathcal{G}_i$ cannot decrease entropy, $H(A_i|C_i E) \geq f(q)$ for arbitrary states over $R_{i-1}E$ and arbitrary register E implies $H(A_i|C_1^{i-1} G_1^{i-1} R_{i-1}') \geq f(q)$ and similarly $H(A_i|E_i) \geq f(q)$ before $\mathcal{N}_i$ is applied. Further, since $\mathcal{N}_i$ does not change $C_1^i G_1^i$, the entropy $H(A_i|C_1^i G_1^i)$ does not change before or after $\mathcal{N}_i$ and $H(A_i|C_1^i G_1^i) \geq H(A_i|E_i) \geq f(q)$ at the end of channel $\mathcal{M}_i'^*$.

For channel $\bar{\mathcal{M}}_i'$, since $\Gamma_i \circ \mathrm{tr}_{R_i R_i'}$ outputs a state that only depends on $C_1^i G_1^i$, we must have $H(A_i|E_i) = H(A_i|C_1^i G_1^i) \geq f(q)$. Finally, for conditioning on the arbitrarily entangled register $\tilde{E}$, we recognize that the input state to $\mathcal{M}_i'^*$ after $\Gamma_{i-1} \circ \mathrm{tr}_{R_{i-1} R_{i-1}'}$ is of the form

$$\sum_{c_1^{i-1} g_1^{i-1}} p(c_1^{i-1} g_1^{i-1}) |c_1^{i-1} g_1^{i-1}\rangle\langle c_1^{i-1} g_1^{i-1}| \otimes \rho_{R_{i-1} R_{i-1}'}^{c_1^{i-1} g_1^{i-1}} \otimes \sigma_{\tilde{E}}^{c_1^{i-1} g_1^{i-1}}, \tag{8}$$

where $\rho_{R_{i-1} R_{i-1}'}^{c_1^{i-1} g_1^{i-1}}, \sigma_{\tilde{E}}^{c_1^{i-1} g_1^{i-1}}$ are some density operators over $R_{i-1} R_{i-1}'$ and $\tilde{E}$ that depend on $c_1^{i-1} g_1^{i-1}$. This is to say that the input state to $\mathcal{M}_i'^*$, and

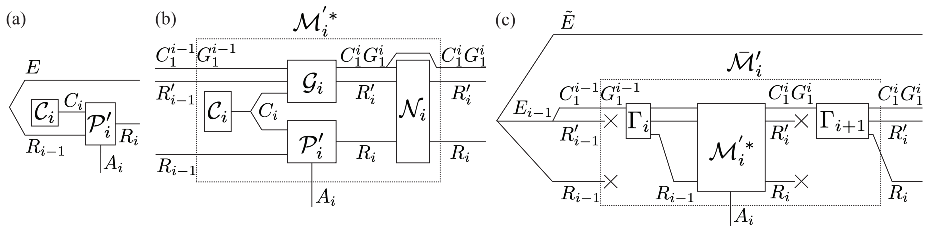

Figure 7: (a) Original certified randomness protocol quantum channel with one prover. (b) CVPV protocol quantum channel with one prover and one guesser. (c) Modified CVPV protocol quantum channel, where crosses represent tracing over the register. For all subpanels, $\mathcal{P}'$ is the prover channel, $\mathcal{G}$ is the guesser channel, $\mathcal{N}$ is the communication channel, and $\mathcal{C}$ is the challenge generation channel. We also use the notation $E_i = C_1^i G_1^i R_i'$.

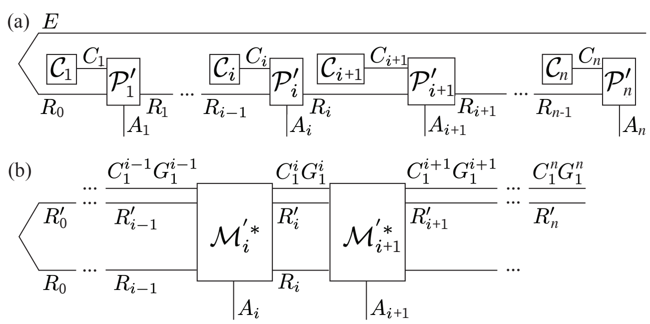

Figure 8: (a) Quantum channel of a certified randomness from repetition protocol. (b) Quantum channel of a CVPV protocol built from (a). Notations are the same as Fig. 7.

therefore the output A_i, is only correlated with $\tilde{E}$ through classical variables $c_1^{i-1}g_1^{i-1}$. This means conditioning on $\tilde{E}$ cannot reduce entropy when we are already conditioning on $C_1^i G_1^i$. Hence $H(A_i|E_i\tilde{E}) \geq f(q)$.

For an n-round protocol, entropy accumulation implies $H_{\min}^{\varepsilon} = O(n)$, and we can similarly choose the smoothing parameter $\varepsilon = O(2^{-n})$. Combined, we show that $\Pr[\Omega] = O(2^{-n})$, which proves the soundness of the CVPV protocol. The completeness of CVPV follows from the certified randomness protocol.

4.3 Rapid-Firing

Another way to construct CVPV from multi-round PoQ with CR is *rapid-firing*. The idea is to send messages back-to-back in intervals much smaller than the round-trip communication time. Note that this construction only works if the challenges are chosen non-adaptively in the PoQ scheme because the verifiers need to *fire* the challenges before receiving the answers for previous rounds.

We now describe the construction formally.

Construction 3. In this construction, we assume the same syntax for $\mathscr{P} = (V, P)$ as in Construction 2. In addition, we assume that V samples challenges non-adaptively. That is, if $V = (\mathsf{Gen}_1, \ldots, \mathsf{Gen}_\ell, \mathsf{Ver})$, then Gen_i ignores the inputs $\mathsf{ans}_1, \ldots, \mathsf{ans}_{i-1}$, that is, there exists $\widetilde{\mathsf{Gen}}_i$ such that

$$\mathsf{Gen}_i(1^\lambda, \mathsf{ans}_1, \ldots, \mathsf{ans}_{i-1}; r) =: \widetilde{\mathsf{Gen}}_i(1^\lambda; r). \tag{9}$$

Let $\{G_k\}_{k \in \{0,1\}^\lambda} : \{0,1\}^m \to \{0,1\}^n$ be a cryptographic hash function family, with $m = \omega(\log \lambda)$. Set[3] $\Delta \in (0, 1/(\ell - 1))$. We describe the (multi-round) CVPV protocol below:

1. At time $t = -\infty$, the verifiers sample random coins $r \leftarrow \{0,1\}^{\mathsf{poly}(\lambda)}$ for V and a hash key $k \leftarrow \{0,1\}^\lambda$. For $i = 1, \ldots, \ell$, they sample random inputs $x_i, y_i \leftarrow \{0,1\}^m$. They publish the hash key k.
2. For $i = 1, \ldots, \ell$:
   - At time $t = (i-1)\Delta$, V_0 computes $\mathsf{ch}_i = \widetilde{\mathsf{Gen}}_i(1^\lambda; r)$ and $s_i = G_k(x_i \oplus y_i) \oplus \mathsf{ch}_i$. It sends (x_i, s_i) and expects an answer ans_i at time $t = (i-1)\Delta + 1$.
   - Similarly, at time $t = (i-1)\Delta$, V_1 sends y_i and expects an answer ans'_i at time $t = (i-1)\Delta + 1$.
   - At time $t = (i-1)\Delta + 1/2$, the honest prover, located at position 0.5, computes $\mathsf{ch}_i = G_k(x_i \oplus y_i) \oplus s_i$ and $\mathsf{ans}_i \leftarrow P_i(\mathsf{ch}_1, \ldots, \mathsf{ch}_i, \mathsf{ans}_1, \ldots, \mathsf{ans}_{i-1})$. It immediately sends ans_i to both verifiers.
3. The verifiers accept iff $\mathsf{ans}_i = \mathsf{ans}'_i$ for all i, and $\mathsf{Ver}(\mathsf{ch}_1, \mathsf{ans}_1, \ldots, \mathsf{ch}_\ell, \mathsf{ans}_\ell; r)$ accepts.

Security Proof in QROM.

Theorem 8 (Rapid-Firing)**.** *Let $\mathscr{P} = (V, P)$ be a PoQ scheme that satisfies Definition 3, such that V non-adaptively samples challenges. Then, Construction 3 is a sound CVPV scheme in the quantum random oracle model.*

The proof of Theorem 8 is nearly identical to the proof of Theorem 7. The major difference is that in the final hybrid we reach, the adversary has no time to communicate anymore due to the rapid-fire design, hence Definition 3 suffices. For the sake of completeness, we provide the full proof in Appendix C.1.

Remark 4 (Comparison to Sequential Compilation)**.** *Rapid-firing is theoretically more advantageous than sequential composition, as the latter requires a stronger notion of certified randomness. Nonetheless, this is in the idealized (vanilla) model of CVPV, and in practice the robustness of rapid-firing will be worse; it will require shorter network delays and shorter computation time.*

[3] While this condition is all we need in the idealized model, in practice the optimal value of Δ is not necessarily the smallest possible value, for a small Δ will make a faster quantum computer necessary for the prover.

4.4 Sequential Rapid-Firing

One shortcoming of the rapid-firing CVPV construction is that the number of messages which can be sent depends on the distance between the provers and the time it takes the honest prover to respond. Instead, we consider m sequential rounds of the ℓ-round rapid-firing protocol. Now, although there may be a practical bound on how large ℓ can be, there is no such bound on m. In this protocol, we require all rounds pass the consistency check, but only some fraction α of rounds need to pass the certified randomness test.

In the following discussion of sequential compilation of the rapid-firing protocol, we denote each rapid-firing round combined quantum channel of the verifier, prover, and guesser as $\mathcal{M}_i : R_{i-1}E_{i-1} \to \Omega_i$, where $i \in [m]$, R_{i-1}, E_{i-1} are the prover and guesser input quantum memory, and Ω_i is the event that the ith rapid-firing round succeeds (both pass the certified randomness test and the consistency check). We only keep the abort status register Ω_i for each round and traced out any output registers for the answers, guessers, and any other registers used for certified randomness check. This is because the traced out registers are only intermediate results used to determine Ω_i, and only Ω_i ultimately determines if the overall sequentially compiled protocol aborts.

To show asymptotic soundness in m while there is no restriction in communication and setup between rapid-fire rounds, we first show the following lemma.

Lemma 3. *There exists independent states $\rho_{R_0E_0}, \rho_{R_1E_1}, \ldots, \rho_{R_{m-1}E_{m-1}}$ such that*

$$\Pr\left[\Omega_i = 1 \ \forall i \in S\right]_\nu \leq \prod_{i\in S} \Pr\left[\Omega_i = 1\right]_{\mathcal{M}_i\left(\rho_{R_{i-1}E_{i-1}}\right)}$$

for any $S \subset [m]$ and $\nu = \mathcal{M}_m \circ \cdots \circ \mathcal{M}_1\left(\sigma_{R_0E_0}\right)$.

Proof. We one-by-one choose the $\rho_{R_{i-1}E_{i-1}}$ to be optimal in maximizing $\Pr\left[\Omega_i = 1\right]$. Fix $S \subset [m]$. Then,

$$\begin{aligned}
&\Pr\left[\Omega_i = 1 \ \forall i \in S\right]_\nu \leq \sup_{\rho_{R_0E_0}} \Pr\left[\Omega_i = 1 \ \forall i \in S\right]_{\mathcal{M}_m\circ\cdots\circ\mathcal{M}_1\left(\rho_{R_0E_0}\right)} \\
&= \sup_{\rho_{R_0E_0}} \prod_{i\in S} \Pr\left[\Omega_i = 1 | \Omega_j = 1 \forall j < i \in S\right]_{\mathcal{M}_i\circ\cdots\circ\mathcal{M}_1\left(\rho_{R_0E_0}\right)} \\
&= \sup_{\rho_{R_0E_0}} \prod_{i\in S} \Pr\left[\Omega_i = 1\right]_{\nu_i(\rho_{R_0E_0})\big|\Omega_j=1\forall j<i\in S} \\
&\leq \prod_{i\in S} \sup_{\rho'_{R_{i-1}E_{i-1}}} \Pr\left[\Omega_i = 1\right]_{\mathcal{M}_i(\rho'_{R_{i-1}E_{i-1}})} = \sup_{\rho_{R_0E_0}} \prod_{i\in S} \Pr\left[\Omega_i = 1\right]_{\nu_i(\rho_{R_0E_0})\big|\Omega_j=1\forall j<i\in S} \\
&\leq \prod_{i\in S} \Pr\left[\Omega_i = 1\right]_{\mathcal{M}_i(\rho_{R_{i-1}E_{i-1}})},
\end{aligned}$$

where $\nu_i(\rho_{R_0E_0}) \equiv \mathcal{M}_i \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0E_0}\right)$, $\nu_i(\rho_{R_0E_0})\big|\Omega_j = 1\forall j < i \in S$ is the normalized state of $\nu_i(\rho_{R_0E_0})$ projected to satisfy the condition $\Omega_j = 1\forall j < i \in S$, and $\rho_{R_{i-1}E_{i-1}} = \underset{\rho'_{R_{i-1}E_{i-1}}}{\arg\max} \Pr\left[\Omega_i = 1\right]_{\mathcal{M}_i}\left(\rho'_{R_{i-1}E_{i-1}}\right)$. □

This allows us to provide an upper bound on the overall protocol success probability.

Theorem 9. *Suppose we have a single-round or rapid-firing protocol such that the probability of success is upper bounded by p over all possible input quantum states. An m-round sequential compilation of these protocols must have*

$$\Pr\left[\sum_i \Omega_i \geq \alpha m\right]_\nu \leq \left(\frac{ep}{\alpha}\right)^{\lfloor \alpha m \rfloor}. \tag{10}$$

Proof. We first notice that by a union-bound together with Lemma 3,

$$\begin{aligned}
&\Pr\left[\sum_i \Omega_i \geq \alpha m\right]_\nu \leq \Pr\left[\exists S, |S| = \lfloor \alpha m \rfloor,\ \Omega_i = 1\ \forall i \in S\right]_\nu \\
&\leq \sum_S \Pr\left[\Omega_i = 1\ \forall i \in S\right]_\nu \leq \sum_S \prod_{i\in S} \Pr\left[\Omega_i = 1\right]_{\mathcal{M}_i\left(\rho_{R_{i-1}E_{i-1}}\right)} \\
&\leq \sum_S p^{\lfloor \alpha m \rfloor} = \binom{m}{\lfloor \alpha m \rfloor} p^{\lfloor \alpha m \rfloor} \leq \left(\frac{e}{\alpha}\right)^{\lfloor \alpha m \rfloor} p^{\lfloor \alpha m \rfloor}.
\end{aligned}$$

This concludes the proof. □

Disclaimer

This paper was prepared for informational purposes by the Global Technology Applied Research center of JPMorgan Chase & Co. This paper is not a product of the Research Department of JPMorgan Chase & Co. or its affiliates. Neither JPMorgan Chase & Co. nor any of its affiliates makes any explicit or implied representation or warranty and none of them accept any liability in connection with this paper, including, without limitation, with respect to the completeness, accuracy, or reliability of the information contained herein and the potential legal, compliance, tax, or accounting effects thereof. This document is not intended as investment research or investment advice, or as a recommendation, offer, or solicitation for the purchase or sale of any security, financial instrument, financial product or service, or to be used in any way for evaluating the merits of participating in any transaction.

Acknowledgments

We thank Dakshita Khurana and Kabir Tomer for pointing out an inaccuracy in our citation of recent work.

References

[ABB+23] Rene Allerstorfer, Andreas Bluhm, Harry Buhrman, Matthias Christandl, Llorenç Escolà-Farràs, Florian Speelman, and

Philip Verduyn Lunel. Making existing quantum position verification protocols secure against arbitrary transmission loss. *arXiv preprint arXiv:2312.12614*, 2023.

[AEFR+23] Rene Allerstorfer, Llorenç Escolà-Farràs, Arpan Akash Ray, Boris Škorić, Florian Speelman, and Philip Verduyn Lunel. Security of a continuous-variable based quantum position verification protocol. *arXiv preprint arXiv:2308.04166*, 2023.

[AH23] Scott Aaronson and Shih-Han Hung. Certified randomness from quantum supremacy. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, page 933–944, New York, NY, USA, 2023. Association for Computing Machinery.

[BBBV97] 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.

[BC93] Stefan Brands and David Chaum. Distance-bounding protocols. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 344–359. Springer, 1993.

[BCF+14] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, 2014.

[BCM+21a] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *Journal of the ACM (JACM)*, 68(5):1–47, 2021.

[BCM+21b] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device, 2021.

[BCS22] Andreas Bluhm, Matthias Christandl, and Florian Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nature Physics*, 18(6):623–626, 2022.

[BK11] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011.

[Bus04] Laurent Bussard. *Trust establishment protocols for communicating devices*. PhD thesis, PhD thesis, Eurecom-ENST, 2004.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *Annual International Cryptology Conference*, pages 391–407. Springer, 2009.

[CH05] Srdjan Capkun and J-P Hubaux. Secure positioning of wireless devices with application to sensor networks. In *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, volume 3, pages 1917–1928. IEEE, 2005.

[CL15] Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. *Physical Review A*, 92(5):052304, 2015.

[DFR20] F Dupuis, O. Fawzi, and R. Renner. Entropy accumulation. *Commun. Math. Phys.*, 379:867–913, 2020.

[JKPPG22] Marius Junge, Aleksander M Kubicki, Carlos Palazuelos, and David Pérez-García. Geometry of banach spaces: a new route towards position based cryptography. *Communications in Mathematical Physics*, 394(2):625–678, 2022.

[Ken11] Adrian Kent. Quantum tagging for tags containing secret classical data. *Physical Review A—Atomic, Molecular, and Optical Physics*, 84(2):022335, 2011.

[KT24] Dakshita Khurana and Kabir Tomer. Founding quantum cryptography on quantum advantage, or, towards cryptography from #p-hardness. *arXiv preprint arXiv:2409.15248*, 2024.

[LLQ22] Jiahui Liu, Qipeng Liu, and Luowen Qian. Beating classical impossibility of position verification. Cryptology ePrint Archive, Paper 2022/008, 2022. https://eprint.iacr.org/2022/008.

[MAF23] Ilya Merkulov and Rotem Arnon-Friedman. Entropy accumulation under post-quantum cryptographic assumptions. *arXiv preprint arXiv:2307.00559*, 2023.

[MFSR22] Tony Metger, Omar Fawzi, David Sutter, and Renato Renner. Generalised entropy accumulation. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 844–850, 2022.

[MSY24] Tomoyuki Morimae, Yuki Shirakawa, and Takashi Yamakawa. Cryptographic characterization of quantum advantage, 2024.

[QS15] Bing Qi and George Siopsis. Loss-tolerant position-based quantum cryptography. *Physical Review A*, 91(4):042337, 2015.

[SP05] Dave Singelee and Bart Preneel. Location verification using secure distance bounding protocols. In *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.*, pages 7–pp. IEEE, 2005.

[SSW03] Naveen Sastry, Umesh Shankar, and David Wagner. Secure verification of location claims. In *Proceedings of the 2nd ACM workshop on Wireless security*, pages 1–10, 2003.

[Tom15] Marco Tomamichel. *Quantum information processing with finite resources: mathematical foundations*, volume 5. Springer, 2015.

[Unr14] Dominique Unruh. Quantum position verification in the random oracle model. In *Advances in Cryptology–CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II 34*, pages 1–18. Springer, 2014.

[Vai03] Lev Vaidman. Instantaneous measurement of nonlocal variables. *Physical review letters*, 90(1):010402, 2003.

[VN06] Adnan Vora and Mikhail Nesterenko. Secure location verification using radio broadcast. *IEEE Transactions on Dependable and Secure Computing*, 3(4):377–385, 2006.

[Zha15] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. *International Journal of Quantum Information*, 13(04):1550014, 2015.

[ZLFW06] Yanchao Zhang, Wei Liu, Yuguang Fang, and Dapeng Wu. Secure localization and authentication in ultra-wideband sensor networks. *IEEE Journal on Selected areas in communications*, 24(4):829–835, 2006.

A CVPV from Certified Randomness through Repetition

A summary of notations used in this appendix is presented in Table 1. In this appendix, we prove that certified randomness protocols that repeat single rounds with an average von Neumann entropy lower bound, or more formally those that satisfy Definition 7, satisfy the sequential decomposition property of Definition 5 and can be used to construct a CVPV protocol secure under the quantum random oracle model by Theorem 7.

To proceed, we first provide a formal model of the sequential protocol quantum channels in Appendix A.1. We then consider an optimal adversary with the largest acceptance probability $\Pr[\Omega]$ in Appendix A.2. We also construct a modified adversary from this optimal adversary, and show that the modified adversary has the same $\Pr[\Omega]$. Then, we show the modified adversary also satisfies the non-signaling condition required by the generalized entropy accumulation theorem in Appendix A.3, which allows us to apply entropy accumulation to lower bound the entropy of the prover output conditioned on the guesser side information. Finally, we derive an upper bound on $\Pr[\Omega]$ by using the fact that either the certified randomness protocol test condition ω' fails with high probability, or the prover output A_1^n has high entropy relative to the guesser side information E_n in Appendix A.4. This concludes the proof of the sequential decomposition property.

A.1 Protocol Quantum Channels

We first provide a model of the sequential protocol. We model the action of the verifier V, the prover P, and the guesser Q in the i-th round as a single map $\mathcal{M}_i$. We denote the register of the classical challenge as C_i, the register of the classical prover output from P as A_i, the classical guess of the guesser as G_i. Furthermore, P and Q may share an arbitrary entangled quantum state on R_{i-1} and R'_{i-1} on input. They then engage in arbitrary communication to produce an output state on R_i and R'_i for the next round. We also use the notation $E_i = C_1^i G_1^i R'_i$, where we use the notation $Y_i^j = Y_i \cdots Y_j$ to denote the values of a given set of registers Y between rounds i and j.

The verifier V also computes some test result based on the values in C_iA_i each round. Namely, X_i are classical systems with common alphabet $\mathcal{X}$, and the test can be modeled by the map $\mathcal{T}_i : A_iC_i \to X_iA_iC_i$,

where

$$\mathcal{T}_i\left(\rho_{A_iC_i}\right) = \sum_{a_i,c_i} \left(\Pi_{A_i}^{a_i} \otimes \Pi_{C_i}^{c_i}\right) \rho_{A_iC_i} \left(\Pi_{A_i}^{a_i} \otimes \Pi_{C_i}^{c_i}\right) \otimes |x_i\rangle\langle x_i|_{X_i}, \tag{11}$$

where $\{\Pi_Y^y\}$ is the family of projectors on Y to classical values y and $x_i = x(a_i, c_i)$ for some deterministic function x. Overall, each round can be modeled by the map

$$\mathcal{M}_i : R_{i-1}E_{i-1} \to X_iA_iR_iE_i = \mathcal{T}_i \circ \mathcal{M}'_i, \tag{12}$$

V, P, Q	Verifier, prover, guesser
$\mathcal{T}_i$	Quantum channel of the ith round prover test result computation. Explanation for the subscript i will be omitted below
$\mathcal{C}_i$	Quantum channel for challenge generation, part of the verifier V
$\mathcal{P}_i$	Quantum channel of the certified randomness protocol of V, P including the test
$\mathcal{P}'_i$	Quantum channel of the certified randomness protocol of V, P excluding the test
$\mathcal{G}_i$	Quantum channel of the guesser G
$\mathcal{N}_i$	Quantum communication channel between P and G
$\mathcal{M}_i$	Quantum channel of the CVPV protocol of V, P, Q including test
$\mathcal{M}'_i$	Quantum channel of the CVPV protocol of V, P, Q excluding test
$\mathcal{M}^*_i$	Original optimal quantum channel of the CVPV protocol of V, P, Q including the test
$\mathcal{M}'^*_i$	Original optimal quantum channel of the CVPV protocol of V, P, Q excluding the test
$\bar{\mathcal{M}}_i$	Modified optimal quantum channel of the CVPV protocol of V, P, Q including the test
$\bar{\mathcal{M}}'_i$	Modified optimal quantum channel of the CVPV protocol of V, P, Q excluding the test, defined by Equation (28)
C_i	Register of the challenge of the ith round
A_i	Register of the prover's answer for the ith round
G_i	Register of the guesser's guess for the ith round
Y_i^j	Collection of $Y_i \dots Y_j$ for any register Y
R_{i-1}	Quantum memory input of the prover in the ith round
R'_{i-1}	Quantum memory input of the guesser in the ith round
E_i	All side information after the ith round, i.e. $E_i = C_1^i G_1^i R'_i$
X_i	Test result register for the ith round
Ω'	Channel to determine if the protocol passes 1. the certified randomness test from X_i, and 2. the consistency check
Ω	Channel to determine if the protocol passes from $C_1^n A_1^n G_1^n$, i.e. $\Omega = \Omega' \circ \mathcal{T}_n \circ \cdots \circ \mathcal{T}_1$. Also denotes the event of the success
ω'	Function taking the single-round test results X_1^n and determine if the certified randomness protocol accepts
W	Binary Register determining if the protocol succeeds
$\Sigma_i(q)$	Set of all input states such that after passing through $\mathcal{P}_i$, the probability distribution on test output X_i is q
$\Sigma'_i(q)$	Same as $\Sigma_i(q)$ except for the original optimal channel $\bar{\mathcal{M}}'^*_i$
$\bar{\Sigma}_i(q)$	Same as $\Sigma_i(q)$ except for the modified optimal channel $\bar{\mathcal{M}}'_i$
$\tilde{E}$	Purification register of $R_{i-1}E_{i-1}$

Table 1: Table of variables for this Appendix A.

where $\mathcal{M}'_i : R_{i-1}E_{i-1} \to A_i R_i E_i = \mathrm{tr}_{X_i}\mathcal{M}_i$ is the quantum channel without the test computation.

The n-round protocol output state is of the form

$$\rho_{X_1^n A_1^n R_n E_n} = (\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1)\, \rho_{R_0 E_0}, \tag{13}$$

where $\rho_{R_0E_0}$ is a density operator on R_0E_0. Similarly,

$$\rho_{A_1^n R_n E_n} = \mathrm{tr}_{X_1^n} \rho_{X_1^n A_1^n R_n E_n} = (\mathcal{M}'_n \circ \cdots \circ \mathcal{M}'_1)\, \rho_{R_0 E_0} \tag{14}$$

for the state without the test result registers.

The verifier finally determines whether to accept the transcript by checking that the outputs pass some test condition Ω. Specifically, define $\Omega' : X_1^n A_1^n G_1^n \to W X_1^n A_1^n G_1^n$ with action

$$\Omega'(\rho) = \sum_{x_1^n, a_1^n, g_1^n} \Pi_{X_1^n A_1^n G_1^n}^{x_1^n a_1^n g_1^n}\ \rho\ \Pi_{X_1^n A_1^n G_1^n}^{x_1^n a_1^n g_1^n} \otimes |\omega\rangle\langle\omega|_W, \tag{15}$$

where

$$\omega = \omega(x_1^n a_1^n g_1^n) = \begin{cases} \omega'(x_1^n) & \text{if } A_1^n = G_1^n \\ 0 & \text{otherwise,} \end{cases} \tag{16}$$

and ω' is a deterministic function with target $\{0, 1\}$. We can define the full test operator Ω as

$$\Omega = \Omega' \circ \mathcal{T}_n \circ \cdots \circ \mathcal{T}_1. \tag{17}$$

All of this is to say that the verifier only accepts if 1. some test condition ω' on the prover outputs A_1^n and the challenges C_1^n is satisfied, and 2. the consistency check passes (i.e. $A_1^n = G_1^n$). The probability of accepting is

$$\Pr[\Omega]_{\rho_{A_1^n R_n E_n}} = \Pi_W^1 \left[\mathrm{tr}_{X_1^n A_1^n R_n E_n} \circ \Omega\left(\rho_{A_1^n R_n E_n}\right)\right] \Pi_W^1, \tag{18}$$

where Π_W^1 is a projector on W to the 1 state.

The state in eq. (14) is built from a sequence of quantum channels, similar to those considered in entropy accumulation. In the context of randomness expansion, the guesser's information about the prover's output can be bounded given certain restrictions on this sequence of channels using entropy accumulation theorems, namely the Markov chain or non-signaling condition. However, in our context of CVPV, we do not have such restrictions on the channels since P and Q can perform arbitrary communication after A_i, G_i are output each round.

In fact, if arbitrary communication is allowed, the adversary can simply copy all A_i to the guesser's final side information E_n, which results in zero entropy. However, to be usefully helpful in assisting the guesses, the side information for the ith round must be present in the ith round, not before or after. This exactly what the Markov chain condition and the non-signaling condition in the entropy accumulation and the generalized entropy accumulation theorem aim to enforce.

A.2 Proof of Equal Abort Probability

We first show that modifying any quantum channel by ignoring the prover output does not change the protocol success probability.

Lemma 4. *Given a quantum channel $\Omega \circ \mathcal{M}_n'^* \circ \cdots \circ \mathcal{M}_1'^*$ with classical registers $A_1^n C_1^n G_1^n$ and intermediate states*

$$\begin{aligned}\rho^*_{A_1^i R_i E_i} &= \left(\mathcal{M}_i'^* \circ \cdots \circ \mathcal{M}_1'^*\right)(\rho_{R_0 E_0}) \\ &= \sum_{a_1^i c_1^i g_1^i} p^*(a_1^i c_1^i g_1^i) |a_1^i c_1^i g_1^i\rangle\langle a_1^i c_1^i g_1^i| \otimes \rho^{*a_1^i c_1^i g_1^i}_{R_i R_i'},\end{aligned} \tag{19}$$

a related quantum channel $\Omega \circ \bar{\mathcal{M}}_n' \circ \cdots \circ \bar{\mathcal{M}}_1'$ defined by

$$\bar{\mathcal{M}}_{i+1}' = \Gamma_{i+1} \circ \mathrm{tr}_{R_{i+1} R_{i+1}'} \circ \mathcal{M}_{i+1}'^* \circ \Gamma_i \circ \mathrm{tr}_{R_i R_i'}, \tag{20}$$

where $\Gamma_i : C_1^i G_1^i \to R_i E_i$ is a quantum channel give by

$$\Gamma_i(\rho) = \sum_{c_1^i g_1^i} \Pi^{c_1^i g_1^i}_{C_1^i G_1^i} \; \rho \; \Pi^{c_1^i g_1^i}_{C_1^i G_1^i} \otimes |c_1^i g_1^i\rangle\langle c_1^i g_1^i| \otimes \rho^{*g_1^i c_1^i g_1^i}_{R_i R_i'}, \tag{21}$$

has the same probability of accept as the original quantum channel. Formally,

$$\Pr[\Omega]_{\rho^*_{A_1^n R_n E_n}} = \Pr[\Omega]_{\rho_{A_1^n R_n E_n}} \tag{22}$$

for $\rho_{A_1^n R_n E_n} = \left(\bar{\mathcal{M}}_n' \circ \cdots \circ \bar{\mathcal{M}}_1'\right)(\rho_{R_0 E_0})$.

Proof. In general, the quantum memory state $\rho^{*a_1^i c_1^i g_1^i}_{R_i R_i'}$ conditioned on any particular outcome depends on $a_1^i c_1^i g_1^i$, and therefore the side information E_{i+1} of the next round might depend on a_1^i, violating the no-signaling condition. Applying the second half of the optimal adversary yields

$$\begin{aligned}\rho^*_{A_1^n R_n E_n} &= \left(\mathcal{M}_n'^* \circ \cdots \circ \mathcal{M}_{i+1}'^*\right) \rho^*_{A_1^i R_i E_i} \\ &= \sum_{a_1^i c_1^i g_1^i} p^*(a_1^i c_1^i g_1^i) |a_1^i c_1^i g_1^i\rangle\langle a_1^i c_1^i g_1^i| \left(\mathcal{M}_n'^* \circ \cdots \circ \mathcal{M}_{i+1}'^*\right) \rho^{*a_1^i c_1^i g_1^i}_{R_i R_i'}.\end{aligned} \tag{23}$$

Therefore, we can express the non-abort probability as

$$\begin{aligned}\Pr[\Omega] &= \sum_{a_1^i c_1^i g_1^i} p^*(a_1^i c_1^i g_1^i) \; \Pr[\Omega]_{|a_1^i c_1^i g_1^i\rangle\langle a_1^i c_1^i g_1^i| \left(\mathcal{M}_n'^* \circ \cdots \circ \mathcal{M}_{i+1}'^*\right) \rho^{*a_1^i c_1^i g_1^i}_{R_i R_i'}} \\ &= \sum_{c_1^i g_1^i} p^*(g_1^i c_1^i g_1^i) \; \Pr[\Omega]_{|g_1^i c_1^i g_1^i\rangle\langle g_1^i c_1^i g_1^i| \left(\mathcal{M}_n'^* \circ \cdots \circ \mathcal{M}_{i+1}'^*\right) \rho^{*g_1^i c_1^i g_1^i}_{R_i R_i'}},\end{aligned} \tag{24}$$

where the second equality holds because applying Ω to states where $a_1^i \neq g_1^i$ gives $|\omega = 0\rangle_W$. Now, let us consider the effect of inserting $\Gamma_i \circ \mathrm{tr}_{R_i R_i'}$, which leads to an intermediate quantum state

$$\left(\Gamma_i \circ \mathrm{tr}_{R_i R_i'} \mathcal{M}_i'^* \circ \cdots \circ \mathcal{M}_1'^*\right) \rho_{R_0 E_0} = \sum_{a_1^i c_1^i g_1^i} p^*(a_1^i c_1^i g_1^i) |a_1^i c_1^i g_1^i\rangle\langle a_1^i c_1^i g_1^i| \rho_{R_i R_i'}^{*g_1^i c_1^i g_1^i}. \tag{25}$$

Applying the rest of the quantum channel $\left(\mathcal{M}_n'^* \circ \cdots \circ \mathcal{M}_{i+1}'^*\right)$ yields

$$\rho_{X_1^n A_1^n R_n E_n} = \sum_{a_1^i c_1^i g_1^i} p^*(a_1^i c_1^i g_1^i) |a_1^i c_1^i g_1^i\rangle\langle a_1^i c_1^i g_1^i| \left(\mathcal{M}_n'^* \circ \cdots \circ \mathcal{M}_{i+1}'^*\right) \rho_{R_i R_i'}^{*g_1^i c_1^i g_1^i}. \tag{26}$$

Therefore,

$$\begin{aligned} \Pr[\Omega] &= \sum_{a_1^i c_1^i g_1^i} p^*(a_1^i c_1^i g_1^i) \ \Pr[\Omega]_{|a_1^i c_1^i g_1^i\rangle\langle a_1^i c_1^i g_1^i| \left(\mathcal{M}_n'^* \circ \cdots \circ \mathcal{M}_{i+1}'^*\right) \rho_{R_i R_i'}^{*g_1^i c_1^i g_1^i}} \\ &= \sum_{c_1^i g_1^i} p^*(g_1^i c_1^i g_1^i) \ \Pr[\Omega]_{|a_1^i c_1^i g_1^i\rangle\langle a_1^i c_1^i g_1^i| \left(\mathcal{M}_n'^* \circ \cdots \circ \mathcal{M}_{i+1}'^*\right) \rho_{R_i R_i'}^{*g_1^i c_1^i g_1^i}}, \end{aligned} \tag{27}$$

which is identical to the probability of the original optimal adversary. The only difference between the derivation is that we replace $\rho_{R_i R_i'}^{*a_1^i c_1^i g_1^i}$ with $\rho_{R_i R_i'}^{*g_1^i c_1^i g_1^i}$ everywhere instead of just the final result.

Applying the modified adversary defined in E.q. 20 for all i is simply inserting $\Gamma_i \circ \mathrm{tr}_{R_i R_i'}$ between all $\mathcal{M}_i'^*$ ($\Gamma_i \circ \mathrm{tr}_{R_i R_i'} \circ \Gamma_i \circ \mathrm{tr}_{R_i R_i'} = \Gamma_i \circ \mathrm{tr}_{R_i R_i'}$). Since the final $\Gamma_n \circ \mathrm{tr}_{R_n R_n'}$ does not change $A_1^n C_1^n G_1^n$, the final probability $\Pr[\Omega]$ does not change. □

This allows to construct a modified optimal adversary channel that ignores prover outputs.

Lemma 5. *For quantum channel $\bar{\mathcal{M}}_n' \circ \cdots \circ \bar{\mathcal{M}}_1'$ such that*

$$\bar{\mathcal{M}}_{i+1}' = \Gamma_{i+1} \circ \mathrm{tr}_{R_{i+1} R_{i+1}'} \circ \mathcal{M}_{i+1}'^* \circ \Gamma_i \circ \mathrm{tr}_{R_i R_i'}, \tag{28}$$

where

$$\mathcal{M}_n'^* \circ \cdots \circ \mathcal{M}_1'^*, \rho_{R_0 E_0}^* = \underset{\mathcal{N}_n' \circ \cdots \circ \mathcal{N}_1' \in \mathsf{poly}, \rho_{R_0 E_0} \in S(R_0 E_0)}{\arg\max} \Pr[\Omega]_{\left(\mathcal{N}_n' \circ \cdots \circ \mathcal{N}_1'\right) \rho_{R_0 E_0}}, \tag{29}$$

and $S(R_0 E_0)$ is the space of all density operators on $R_0 E_0$, we have

$$\sup_{\mathcal{N}_n' \circ \cdots \circ \mathcal{N}_1' \in \mathsf{poly}, \rho_{R_0 E_0} \in S(R_0 E_0)} \Pr[\Omega]_{\left(\mathcal{N}_n' \circ \cdots \circ \mathcal{N}_1'\right) \rho_{R_0 E_0}} = \Pr[\Omega]_{\left(\bar{\mathcal{M}}_n' \circ \cdots \circ \bar{\mathcal{M}}_1'\right) \rho_{R_0 E_0}^*}. \tag{30}$$

Proof. By Lemma 4,

$$\Pr[\Omega]_{\left(\bar{\mathcal{M}}_n' \circ \cdots \circ \bar{\mathcal{M}}_1'\right) \rho_{R_0 E_0}^*} = \Pr[\Omega]_{\left(\mathcal{M}_n'^* \circ \cdots \circ \mathcal{M}_1'^*\right) \rho_{R_0 E_0}^*}. \tag{31}$$

By definition of $\mathcal{M}_n'^* \circ \cdots \circ \mathcal{M}_1'^*, \rho_{R_0 E_0}^*$ and the supremum, this completes the proof. □

A.3 Proof of Entropy

Lemma 6. *The quantum channel defined in E.q. 28 satisfies the non-signalling condition. Namely, for all i, there exists $\mathcal{R}_{i+1} : E_i \to E_{i+1}$ such that*

$$\mathrm{tr}_{A_{i+1}R_{i+1}}\bar{\mathcal{M}}'_{i+1} = \mathcal{R}_{i+1} \circ \mathrm{tr}_{R_i}. \tag{32}$$

Proof. This is satisfied by setting

$$\mathcal{R}_{i+1} = \mathrm{tr}_{A_{i+1}R_{i+1}}\Gamma_{i+1} \circ \mathrm{tr}_{R_{i+1}R'_{i+1}} \circ \mathcal{M}'^{*}_{i+1} \circ \Gamma_i \circ \mathrm{tr}_{R'_i}. \tag{33}$$

□

Since the modified adversary satisfies the non-signalling condition, we can apply entropy accumulation theorem to bound the unpredictability of z_i from the perspective of the guesser, which is bounded by $H_{\min}(A_1^n|E_n)$. To do this, we need a lower bound on the single-round von Neumann entropy. Namely, for $q \in \mathbb{P}$ and $\mathbb{P}$ a set of probability distributions on the alphabet $\mathcal{X}$ of X_i, we need

$$\inf_{\nu \in \Sigma_i(q)} H(A_i|E_i\tilde{E})_\nu \geq f(q), \tag{34}$$

where $\tilde{E}$ is isomorphic to $R_{i-1}E_{i-1}$, and

$$\bar{\Sigma}_i(q) = \left\{ \nu_{X_iA_iR_iE_i\tilde{E}} = \mathcal{T}_i \circ \bar{\mathcal{M}}_i'(\rho) \middle| \rho \in S(R_{i-1}E_{i-1}\tilde{E}) \wedge \nu_{X_i} = q \right\}. \tag{35}$$

Here, $f(q)$ is called the min-tradeoff function, and it is an affine function.

However, $\bar{\mathcal{M}}'_i$ are modified quantum channels and we do not have an entropy lower bound for them. Given some entropy lower bound on the original quantum channels $\mathcal{M}'^{*}_i$, we wish to establish a lower bound for $\bar{\mathcal{M}}'_i$. We proceed with this task by first showing some useful lemmas about conditional entropy.

Lemma 7. *For state ρ on quantum system ABC where C is classical and $\rho = \sum_c p(c)|c\rangle\langle c|_C \otimes \sigma_A^c \otimes \eta_B^c$,*

$$H(ABC) = H(C) + H(A|C) + H(B|C). \tag{36}$$

Proof. First, we note that ρ is block diagonal. Further, each sub-block of $C = c$ is in a product form $\sigma_A^c \otimes \eta_B^c$. Say σ_A^c has eigenvalues λ_a^c and η_B^c has eigenvalues λ_b^c. Note that the eigenvectors are not the same for different c in general. Still, $\sigma_A^c \otimes \eta_B^c$ has eigenvalues $\lambda_a^c\lambda_b^c$ for all possible a, b. Overall, ρ has eigenvalues $p(c)\lambda_a^c\lambda_b^c$ for all a, b, c. The entropy of the system is identical to a classical system with probability distribution $p(abc) = p(c)p(a|c)p(b|c)$, and the entropy is $H(ABC) = H(C) + H(A|C) + H(B|C)$. □

Lemma 8. *For state ρ on quantum system ABC where C is classical and $\rho = \sum_c p(c)|c\rangle\langle c|_C \otimes \sigma_A^c \otimes \eta_B^c$, we have $H(A|BC) = H(A|C)$.*

Proof. Using Lemma 7,

$$\begin{aligned} H(A|BC) =& H(ABC) - H(BC) \\ =& (H(C) + H(A|C) + H(B|C)) - (H(C) + H(B|C)) = H(A|C). \end{aligned}$$

□

This now allows us to reduce the entropy of the modified adversary conditioned on quantum registers (which we need to apply generalized entropy accumulation theorem) to entropy conditioned on classical registers only.

Lemma 9. *For input quantum state* $\sigma \in S(R_{i-1}E_{i-1}\tilde{E})$ *and*

$$\nu_{X_iA_iR_iE_i\tilde{E}} = \left(\Gamma_i \circ \mathrm{tr}_{R_iR_i'} \circ \mathcal{T}_i \circ \mathcal{M}_i'^{*} \circ \Gamma_{i-1} \circ \mathrm{tr}_{R_{i-1}R_{i-1}'}\right)\sigma, \tag{37}$$

we have $H(A_i|E_i\tilde{E})_{\nu_{A_iE_i\tilde{E}}} = H(A_i|C_1^iG_1^i)_{\nu_{A_iC_1^iG_1^i}}$.

Proof. We know that $\mathrm{tr}_{R_iR_i'}\sigma \in S(C_{i-1}G_{i-1}\tilde{E})$. Further,

$$\begin{aligned} \nu_{A_iE_i\tilde{E}_i} =& \mathrm{tr}_{X_iR_i}\nu_{X_iA_iR_iE_i\tilde{E}} \\ =& \mathrm{tr}_{X_iR_i} \circ \Gamma_i \circ \mathrm{tr}_{R_iR_i'} \circ \mathcal{T}_i \circ \mathcal{M}_i'^{*} \circ \Gamma_{i-1} \circ \mathrm{tr}_{R_{i-1}R_{i-1}'}\sigma \\ =& \mathrm{tr}_{R_i} \circ \Gamma_i \circ \mathrm{tr}_{X_iR_iR_i'} \circ \mathcal{M}_i'^{*} \\ & \sum_{c_1^{i-1}g_1^{i-1}} p(c_1^{i-1}g_1^{i-1})|c_1^{i-1}g_1^{i-1}\rangle\langle c_1^{i-1}g_1^{i-1}| \otimes \rho^{*g_1^{i-1}c_1^{i-1}g_1^{i-1}}_{R_{i-1}R_{i-1}'} \otimes \sigma^{c_1^{i-1}g_1^{i-1}}_{\tilde{E}} \\ =& \mathrm{tr}_{R_i} \circ \Gamma_i \circ \sum_{c_1^{i-1}g_1^{i-1}} p(c_1^{i-1}g_1^{i-1})|c_1^{i-1}g_1^{i-1}\rangle\langle c_1^{i-1}g_1^{i-1}| \otimes \eta^{c_1^{i-1}g_1^{i-1}}_{A_iC_iG_i} \otimes \sigma^{c_1^{i-1}g_1^{i-1}}_{\tilde{E}} \\ =& \mathrm{tr}_{R_i}\sum_{c_1^ig_1^i} p(c_1^ig_1^i)|c_1^ig_1^i\rangle\langle c_1^ig_1^i| \otimes \rho^{*g_1^ic_1^ig_1^i}_{R_iR_i'} \otimes \zeta^{c_1^ig_1^i}_{A_i} \otimes \sigma^{c_1^{i-1}g_1^{i-1}}_{\tilde{E}} \\ =& \sum_{c_1^ig_1^i} p(c_1^ig_1^i)|c_1^ig_1^i\rangle\langle c_1^ig_1^i| \otimes \left(\rho^{c_1^ig_1^i}_{R_i'} \otimes \sigma^{c_1^{i-1}g_1^{i-1}}_{\tilde{E}}\right) \otimes \zeta^{c_1^ig_1^i}_{A_i}, \end{aligned} \tag{38}$$

where

$$p(c_1^{i-1}g_1^{i-1})\sigma^{c_1^{i-1}g_1^{i-1}}_{\tilde{E}} = \langle c_1^{i-1}g_1^{i-1}|\mathrm{tr}_{R_{i-1}R_{i-1}'}\sigma|c_1^{i-1}g_1^{i-1}\rangle \in S(\tilde{E}), \tag{39}$$

$$\mathrm{tr}_{\tilde{E}}\sigma^{c_1^{i-1}g_1^{i-1}}_{\tilde{E}} = 1, \tag{40}$$

$$\mathrm{tr}_{X_iR_iR_i'} \circ \mathcal{M}_i'^{*}|c_1^{i-1}g_1^{i-1}\rangle\langle c_1^{i-1}g_1^{i-1}|\rho^{*g_1^{i-1}c_1^{i-1}g_1^{i-1}}_{R_{i-1}R_{i-1}'} = |c_1^{i-1}g_1^{i-1}\rangle\langle c_1^{i-1}g_1^{i-1}|\eta^{c_1^{i-1}g_1^{i-1}}_{A_iC_iG_i}, \tag{41}$$

since $\mathrm{tr}_{X_iR_iR_i'} \circ \mathcal{M}_i'^{*}$ cannot change $C_1^iG_1^i$ (this is because $C_1^iG_1^i$ are committed classical variables that cannot be changed), and

$$p(c_1^ig_1^i)\zeta^{c_1^ig_1^i}_{A_i} = p(c_1^{i-1}g_1^{i-1})\langle c_ig_i|\eta^{c_1^{i-1}g_1^{i-1}}_{A_iC_iG_i}|c_ig_i\rangle, \tag{42}$$

$$\mathrm{tr}_{A_i}\zeta^{c_1^ig_1^i}_{A_i} = 1. \tag{43}$$

Finally, by Lemma 8, we have

$$H(A_i|E_i\tilde{E})_{\nu_{A_iE_i\tilde{E}}} = H(A_i|C_1^iG_1^i)_{\nu_{A_iC_1^iG_1^i}}. \tag{44}$$

□

Lemma 10. *For Γ_i defined in E.q. 21 and $\nu' = \left(\Gamma_i \circ \operatorname{tr}_{R_iR_i'}\right)\nu$, we have*

$$H(A_i|C_1^iG_1^i)_\nu = H(A_i|C_1^iG_1^i)_{\nu'}. \tag{45}$$

Proof. Since $\Gamma_i \circ \operatorname{tr}_{R_iR_i'}$ does not modify $A_iC_1^iG_1^i$, we have

$$\nu_{A_iC_1^iG_1^i} = \operatorname{tr}_{X_iR_iR_i'}\nu = \operatorname{tr}_{X_iR_iR_i'}\left(\Gamma_i \circ \operatorname{tr}_{R_iR_i'}\right)\nu = \nu'_{A_iC_1^iG_1^i}, \tag{46}$$

which means the two entropy quantities must be equal. □

We now show that if we have a lower bound on the entropy conditioned on $C_1^iG_1^i$ for the original optimal adversary, then we also have a lower bound on the entropy conditioned on quantum side information for the modified adversary.

Lemma 11. *For the quantum channel defined in E.q. 28, if*

$$\inf_{\nu'\in\Sigma_i'(q)} H(A_i|C_1^iG_1^i)_{\nu'} \geq f(q), \tag{47}$$

where

$$\Sigma_i'(q) = \left\{\nu_{X_iA_iR_iE_i} = \mathcal{T}_i \circ \mathcal{M}_i^{'*}(\rho)\middle|\rho \in S(R_{i-1}E_{i-1}) \wedge \nu_{X_i} = q\right\}, \tag{48}$$

$q \in \mathbb{P}$, and $\mathbb{P}$ is the set of probability distributions on the alphabet $\mathcal{X}$ of X_i, then

$$\inf_{\nu\in\bar{\Sigma}_i(q)} H(A_i|E_i\tilde{E})_\nu \geq f(q), \tag{49}$$

where $\tilde{E}$ is isomorphic to $R_{i-1}E_{i-1}$, and

$$\bar{\Sigma}_i(q) = \left\{\nu_{X_iA_iR_iE_i\tilde{E}} = \mathcal{T}_i \circ \bar{\mathcal{M}}_i^{'}(\rho)\middle|\rho \in S(R_{i-1}E_{i-1}\tilde{E}) \wedge \nu_{X_i} = q\right\}. \tag{50}$$

Proof. By Lemma 9,

$$\inf_{\nu\in\bar{\Sigma}_i(q)} H(A_i|E_i\tilde{E})_\nu = \inf_{\nu\in\bar{\Sigma}_i(q)} H(A_i|C_1^iG_1^i)_\nu. \tag{51}$$

Define $\rho^* \in S(R_{i-1}E_{i-1}\tilde{E})$ and $\nu^*_{X_iA_iR_iE_i\tilde{E}} = \mathcal{T}_i \circ \bar{\mathcal{M}}_i^{'}(\rho^*)$ as anything that satisfies the following conditions. First, $\nu^*_{X_i} = q$, which implies $\nu^* \in \bar{\Sigma}_i(q)$. Second, for all $\rho \in S(R_{i-1}E_{i-1}\tilde{E})$ and $\nu_{X_iA_iR_iE_i\tilde{E}} = \mathcal{T}_i \circ \bar{\mathcal{M}}_i^{'}(\rho)$ such that $\nu_{X_i} = q$, we have $H(A_i|C_1^iG_1^i)_{\nu^*} \leq H(A_i|C_1^iG_1^i)_\nu$. By definition, we have

$$\inf_{\nu\in\bar{\Sigma}_i(q)} H(A_i|C_1^iG_1^i)_\nu = H(A_i|C_1^iG_1^i)_{\nu^*}, \tag{52}$$

Further,

$$
\begin{aligned}
\nu^*_{X_iA_iR_iE_i} &= \mathrm{tr}_{\tilde{E}}\nu^*_{X_iA_iR_iE_i\tilde{E}} \\
&= \left(\mathrm{tr}_{\tilde{E}} \circ \Gamma_i \circ \mathrm{tr}_{R_iR_i'} \circ \mathcal{T}_i \circ \mathcal{M}_i'^* \circ \Gamma_{i-1} \circ \mathrm{tr}_{R_{i-1}R_{i-1}'}\right)\rho^* \\
&= \left(\Gamma_i \circ \mathrm{tr}_{R_iR_i'}\right)\left(\mathcal{T}_i \circ \mathcal{M}_i'^*\right)\left[\left(\Gamma_{i-1} \circ \mathrm{tr}_{R_{i-1}R_{i-1}'\tilde{E}}\right)\rho^*\right] \\
&= \left(\Gamma_i \circ \mathrm{tr}_{R_iR_i'}\right)\left(\mathcal{T}_i \circ \mathcal{M}_i'^*\right)\left(\rho'_{R_{i-1}E_{i-1}}\right) &(53)\\
&= \left(\Gamma_i \circ \mathrm{tr}_{R_iR_i'}\right)\mu^*_{X_iA_iR_iE_i}. &(54)
\end{aligned}
$$

Therefore, by Lemma 10,

$$
H(A_i|C_1^iG_1^i)_{\nu^*} = H(A_i|C_1^iG_1^i)_{\left(\Gamma_i\circ\mathrm{tr}_{R_iR_i'}\right)\mu^*_{X_iA_iR_iE_i}} = H(A_i|C_1^iG_1^i)_{\mu^*} \quad (55)
$$

Since the quantum channel $\Gamma_i \circ \mathrm{tr}_{R_iR_i'}$ does not act on X_i and $\nu^* \in \bar{\Sigma}_i(q)$, we must have $\mu^*_{X_i} = \nu^*_{X_i} = 1$. Further, $\mu^*_{X_iA_iR_iE_i} = \left(\mathcal{T}_i \circ \mathcal{M}_i'^*\right)\left(\rho'_{R_{i-1}E_{i-1}}\right)$ for some $\rho' \in S(R_{i-1}E_{i-1})$. Together, these two conditions means that $\mu^*_{X_iA_iR_iE_i} \in \Sigma_i'(q)$ by the definition of $\Sigma_i'(q)$. As a result,

$$
H(A_i|C_1^iG_1^i)_{\mu^*} \geq \inf_{\nu\in\Sigma_i'(q)} H(A_i|C_1^iG_1^i)_{\nu'}. \quad (56)
$$

Combining E.q. 51, 52, 55, 56, and 47 yields

$$
\begin{aligned}
\inf_{\nu\in\bar{\Sigma}_i(q)} H(A_i|E_i\tilde{E})_\nu &= \inf_{\nu\in\bar{\Sigma}_i(q)} H(A_i|C_1^iG_1^i)_\nu = H(A_i|C_1^iG_1^i)_{\nu^*} \\
&= H(A_i|C_1^iG_1^i)_{\mu^*} \geq \inf_{\nu\in\Sigma_i'(q)} H(A_i|C_1^iG_1^i)_{\nu'} \geq f(q). \quad (57)
\end{aligned}
$$

□

Now that we derived the bound on the required single round von Neumann entropy of the modified adversary, we can apply entropy accumulation to it.

Lemma 12. *For $\Sigma_i'(q)$ defined in Lemma 11, $\bar{\mathcal{M}}_i'$ defined in E.q. 28, $\bar{\mathcal{M}}_i = \mathcal{T}_i \circ \bar{\mathcal{M}}_i'$, ω' a set of possible outputs on X_1^n, if*

$$
\inf_{\nu'\in\Sigma_i'(q)} H(A_i|C_1^iG_1^i)_{\nu'} \geq f(q), \quad (58)
$$

then,

$$
H^\varepsilon_{\min}(A_1^n|E_n)_{\bar{\mathcal{M}}_n\circ\cdots\circ\bar{\mathcal{M}}_1(\rho_{R_0E_0})_{|\omega'}} \geq nh - c_1\sqrt{n} - c_0, \quad (59)
$$

where

$$
h = \min_{x_1^n\in\omega'} f\left(\mathsf{freq}(x_1^n)\right) \quad (60)
$$

$$
\mathsf{freq}(x_1^n)(x) = \frac{|\{i \in \{1,\ldots,n\} : x_i = x\}|}{n}, \quad (61)
$$

and c_0, c_1 are as defined in Corollary 4.6 in [MFSR22], correcting the typo where $g(\varepsilon)$ should be

$$g(\varepsilon) = -\log_2(1 - \sqrt{1-\varepsilon^2}) \tag{62}$$

and replacing $\Pr[\Omega]$ *with* $\Pr[\omega']$.

Proof. By Lemma 11, for $\bar{\Sigma}_i(q)$ defined in Lemma 11,

$$\inf_{\nu \in \bar{\Sigma}_i(q)} H(A_i|E_i\tilde{E})_\nu \geq f(q). \tag{63}$$

Applying Corollary 4.6 of [MFSR22] completes the proof, which is valid because of Lemma 6. □

A.4 Proof of the Sequential Decomposition Property

Although EAT bounds the ε-min-entropy instead of the min-entropy, we can use the following relation.

Lemma 13. *For a classical probability distribution ρ over random variable X,*

$$H_{\min}(X) \geq -\log_2\left(\varepsilon + 2^{-H^{\varepsilon}_{\min}}\right). \tag{64}$$

Proof. Consider $x^*_\rho = \operatorname{argmax}_x \Pr[X = x]_\rho$ and $p_{\max,\rho} = \Pr[X = x^*_\rho]_\rho$. By definition of the min-entropy, $p_{\max,\rho} = 2^{-H_{\min}(X)_\rho}$. Consider a classical distribution ρ' in the ε-ball of ρ. Maximization of the min-entropy over such a classical state gives the smooth min-entropy due to the definition of the smooth min-entropy in Definition 6.9 and Lemma 6.13 of of [Tom15]. For classical distributions, the TVD distance between ρ and ρ' must be less than ε. Define $x^*_{\rho'} = \operatorname{argmax}_x \Pr[X = x]_{\rho'}$ and $p_{\max,\rho'} = \Pr[X = x^*_{\rho'}]_{\rho'}$.

Either $x^*_\rho = x^*_{\rho'}$ or $x^*_\rho \neq x^*_{\rho'}$. If $x^*_\rho = x^*_{\rho'}$, we must have $\varepsilon \geq \mathrm{TVD}[\rho, \rho'] \geq |p_{\max,\rho} - p_{\max,\rho'}|$, and therefore $p_{\max,\rho} \leq p_{\max,\rho'} + \varepsilon$.

If $x^*_\rho \neq x^*_{\rho'}$, we must have $\varepsilon \geq \mathrm{TVD}[\rho, \rho'] \geq |p_{\max,\rho} - \Pr[X = x^*_\rho]_{\rho'}|$, and therefore $p_{\max,\rho} \leq \Pr[X = x^*_\rho]_{\rho'} + \varepsilon$. Note that $\Pr[X = x^*_\rho]_{\rho'}$ is the probability of measuring from ρ' the maximum probability string of ρ. Since $x^*_\rho \neq x^*_{\rho'}$, we have $\Pr[X = x^*_\rho]_{\rho'} \leq p_{\max,\rho'}$ by definition of $p_{\max,\rho'}$, and $p_{\max,\rho} \leq p_{\max,\rho'} + \varepsilon$.

Since in both cases, $p_{\max,\rho} \leq p_{\max,\rho'} + \varepsilon$, we have

$$H_{\min}(X)_\rho = -\log_2 p_{\max,\rho} \geq -\log_2 \left(p_{\max,\rho'} + \varepsilon\right). \tag{65}$$

Finally, since by definition of the smooth min-entropy in Definition 6.9 of [Tom15], $H^{\varepsilon}_{\min}(X)_\rho \geq H_{\min}(X)_{\rho'} = -\log_2 p_{\max,\rho'}$,

$$H_{\min}(X)_\rho \geq -\log_2\left(2^{-H^{\varepsilon}_{\min}(X)_\rho} + \varepsilon\right). \tag{66}$$

□

However, this lemma is only for unconditional min-entropy, which does not directly apply. We now use similar arguments to show this for conditional min-entropy.

Lemma 14. *For a classical probability distribution ρ over random variables X, Y,*

$$H_{\min}(X|Y)_\rho \geq -\log_2\left(2^{-H^{\varepsilon}_{\min}(X|Y)_\rho} + \epsilon\right). \tag{67}$$

Proof. We closely follow the same arguments presented in the proof of Lemma 13. Consider $x^*_{\rho_{X|Y=y}} = \text{argmax}_x \Pr[X = x]_{\rho_{X|Y=y}}$, where $\rho_{X|Y=y} = \langle y|\rho|y\rangle$. Define $p_{\max,\rho_{X|Y=y}} = \Pr\left[X = x^*_{\rho_{X|Y=y}}\right]_{\rho_{X|Y=y}}$. Consider a distribution ρ' in the ε-ball of ρ. Maximization of the min-entropy over such a classical state gives the smooth min-entropy due to the definition of the smooth min-entropy in Definition 6.9 and Lemma 6.13 of of [Tom15]. Similarly, we define $x^*_{\rho'_{X|Y=y}}$ and $p_{\max,\rho'_{X|Y=y}}$.

We must have

$$\begin{aligned}
\varepsilon \geq& \text{TVD}[\rho, \rho'] && (68)\\
\geq& \sum_y \Bigg| \Pr[Y = y]_\rho \cdot p_{\max,\rho_{X|Y=y}} && (69)\\
&- \Pr[Y = y]_{\rho'} \cdot \Pr\left[X = x^*_{\rho_{X|Y=y}}\right]_{\rho'_{X|Y=y}} \Bigg| && (70)\\
\geq& \Bigg| \sum_y \Pr[Y = y]_\rho \cdot p_{\max,\rho_{X|Y=y}} && (71)\\
&- \sum_y \Pr[Y = y]_{\rho'} \cdot \Pr\left[X = x^*_{\rho_{X|Y=y}}\right]_{\rho'_{X|Y=y}} \Bigg|. && (72)
\end{aligned}$$

Since $\Pr\left[X = x^*_{\rho_{X|Y=y}}\right]_{\rho'_{X|Y=y}} \leq p_{\max,\rho'_{X|Y=y}}$ by definition of $p_{\max,\rho'_{X|Y=y}}$, we have

$$\sum_y \Pr[Y = y]_\rho \cdot p_{\max,\rho_{X|Y=y}} \leq \sum_y \Pr[Y = y]_{\rho'} \cdot p_{\max,\rho'_{X|Y=y}} + \epsilon. \tag{73}$$

Therefore, we have

$$\begin{aligned}
H_{\min}(X|Y)_\rho &= -\log_2\left(\sum_y \Pr[Y = y]_\rho \cdot p_{\max,\rho_{X|Y=y}}\right) && (74)\\
&\geq -\log_2\left(\sum_y \Pr[Y = y]_{\rho'} \cdot p_{\max,\rho'_{X|Y=y}} + \epsilon\right), && (75)
\end{aligned}$$

where the definition of conditional min-entropy for classical distributions follow E.q. 6.26 of [Tom15]. Finally, since by definition of the smooth min-entropy in Definition 6.9 of [Tom15],

$$H^{\varepsilon}_{\min}(X|Y)_\rho \geq H_{\min}(X|Y)_{\rho'} = -\log_2\left(\sum_y \Pr[Y = y]_{\rho'} \cdot p_{\max,\rho'_{X|Y=y}}\right), \tag{76}$$

we have

$$H_{\min}(X|Y)_\rho \geq -\log_2\left(2^{-H^{\varepsilon}_{\min}(X|Y)_\rho} + \epsilon\right). \tag{77}$$

□

Further, for a CVPV protocol based on certified randomness with acceptance probability p, the CVPV acceptance probability is

$$\Pr[\Omega] \leq \min\left(p, 2^{-H_{\min}}\right). \tag{78}$$

This is because the guessing probability is given by the exponential of the conditional min-entropy for classical variables as shown in E.q. 6.27 of [Tom15].

To more explicitly show asymptotic soundness, we prove the following theorem.

Lemma 15. *For the modified quantum channel defined in E.q. 28 and h defined in E.q. 60, if $h > 0$, then the n-round protocol has $\Pr[\Omega] \leq O(2^{-n})$.*

Proof. Lemma 12 shows that to achieve $H^{\varepsilon}_{\min} = O(n)$, we can tolerate $c_0 = O(n)$ and $c_1 = O(\sqrt{n})$. To achieve this, we can tolerate $g(\varepsilon) = O(n)$ and $\Pr[\omega'] = O(n)$ with suitably chosen constants such that c_0 and c_1 are sufficiently small and $H^{\varepsilon}_{\min} > 0$. To achieve this, we can have $\Pr[\omega'] = O(2^{-n})$ and $\varepsilon = O(2^{-n})$. In this case,

$$H_{\min} \geq -\log_2\left(\varepsilon + 2^{-H^{\varepsilon}_{\min}}\right) = O(n) \tag{79}$$

$$\Pr[\Omega] \leq \min\left(\Pr[\omega'], 2^{-H_{\min}}\right) = \min(O(2^{-n}), O(2^{-n})) = O(2^{-n}). \tag{80}$$

□

Finally, we have a bound on the probability of the protocol not aborting in the adversarial setting for soundness. According to Definition 5, P and Q can communicate and setup arbitrarily only after $\mathsf{ans}_i, \mathsf{ans}'_i$ are provided. Therefore, we can model the ith round CVPV protocol quantum channel as

$$\mathcal{M}^*_i = \mathcal{T}_i \circ \mathcal{N}_i \circ (\mathcal{P}'_i \circ \mathcal{G}_i) \circ (\mathcal{C}_i \otimes \mathcal{I}), \tag{81}$$

where $\mathcal{I}$ is identity over $R_{i-1}E_{i-1}$, $\mathcal{C}_i : \mathbb{C} \to C_i$ is a channel from complex number to the challenge, $\mathcal{G}_i : C_iE_{i-1} \to E_i$ where $E_i = C^i_1 G^i_1 R'_i$, $\mathcal{P}'_i : C_iR_{i-1} \to A_iR_i$, $\mathcal{N}_i : R_iE_i \to R_iE_i$ is the arbitrary communication and setup channel, and $\mathcal{T}_i : A_iC_i \to X_i$ is the test channel.

Theorem 10. *Given a PoQ protocol for h defined in 60, if $h > 0$ for all single-round QPT channels $\mathcal{M}^*_i$ of the form of E.q. 81, then the protocol is a sequential certified randomness protocol.*

Proof. For the modified quantum channel, if $h > 0$ is satisfied, then the n-round protocol has $\Pr[\Omega] \leq O(2^{-n})$ due to Lemma 15. Finally, by Lemma 4, for the original channel, the acceptance probability is identical. □

Additionally, to show that any certified randomness from repetition satisfying Definition 7 is a sequential certified randomness protocol, we need to show $h > 0$ for channel $\mathcal{M}_i^*$ is implied by $h > 0$ channel $\mathcal{P}_i$.

Theorem 11. *An ℓ-round PoQ protocol $\mathscr{P}$ is a sequential certified randomness protocol if it is a certified randomness from repetition, and performs the consistency check and timing check of CVPV.*

Proof. Consider $\mathcal{M}_i^*$ defined in E.q. 81. Since $\mathcal{N}_i$ does not change $A_i C_1^i G_1^i$, it does not affect $H(A_i|C_1^i G_1^i)$. Therefore, we have

$$H(A_i|C_1^i G_1^i)_{\mathcal{M}_i^*(\rho_{R_{i-1}E_{i-1}})} = H(A_i|C_1^i G_1^i)_{\mathcal{T}_i \circ \left(\mathcal{P}_i' \otimes \mathcal{G}_i\right) \circ (\mathcal{C}_i \otimes \mathcal{I})(\rho_{R_{i-1}E_{i-1}})} \tag{82}$$

$$\geq H(A_i|E_i)_{\mathcal{T}_i \circ \left(\mathcal{P}_i' \otimes \mathcal{G}_i\right) \circ (\mathcal{C}_i \otimes \mathcal{I})(\rho_{R_{i-1}E_{i-1}})}. \tag{83}$$

Further, since $\mathcal{G}_i$ does not act on A_i,

$$H(A_i|E_i)_{\mathcal{T}_i \circ \left(\mathcal{P}_i' \otimes \mathcal{G}_i\right) \circ (\mathcal{C}_i \otimes \mathcal{I})(\rho_{R_{i-1}E_{i-1}})} \geq H(A_i|C_i E_{i-1})_{\mathcal{T}_i \circ \mathcal{P}_i' \circ (\mathcal{C}_i \otimes \mathcal{I})(\rho_{R_{i-1}E_{i-1}})}. \tag{84}$$

Moreover, $\mathcal{T}_i \circ \mathcal{P}_i' \circ (\mathcal{C}_i \otimes \mathcal{I})$ is exactly the ith round certified randomness from repetition quantum channel $\mathcal{P}_i$. This is because for the challenges to be generated by the verifier independent of any other information, which is required by Definition 7, the channel must have this form. Therefore,

$$H(A_i|C_1^i G_1^i)_{\mathcal{M}_i^*(\rho_{R_{i-1}E_{i-1}})} = H(A_i|C_i E_{i-1})_{\mathcal{P}_i(\rho_{R_{i-1}E_{i-1}})}, \tag{85}$$

and therefore

$$\inf_{\nu' \in \Sigma_i'(q)} H(A_i|C_1^i G_1^i)_{\nu'} \geq \inf_{\nu \in \Sigma_i(q)} H(A_i|C_i E_{i-1})_\nu \geq f(q), \tag{86}$$

where $\Sigma_i'(q)$ is defined in Lemma 11 and $\Sigma_i(q), f(q)$ are as in Definition 7. □

Corollary 1. *All results in Section 4.1 hold for PoQ scheme $\mathscr{P} = (V, P)$ that is certified randomness from repetition.*

B Instantiation

For a specific instantiation of a CVPV protocol, we consider certified randomness from random circuit sampling (RCS) [AH23]. In particular, it is appealing for near-term implementation due to the fact that RCS is already demonstrated experimentally and classical simulation is believed to be hard. Crucially, the protocol is based on solving the heavy output generation problem.

Definition 8 (Heavy Output Generation)**.** *A quantum algorithm $\mathcal{A}$ given $C \sim \mathcal{D}$ is said to solve b-XHOG if it outputs a bitstring z such that*

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

[AH23] showed that any quantum algorithm given oracle access to C and passes b-XHOG must output samples with conditional von Neumann entropy at least $\Omega(n)$ (Theorem 13).

Specifically, for the single round analysis, RCS-based certified randomness yields different bounds on the von Neumann entropy under different models. Denote the single round output as A, the challenge as C, and any side information as E.

One model that is considered is the semi-honest adversary, where the prover may be entangled with an guesser but performs ideal quantum measurement.

Theorem 12 (Theorem 6.4 of [AH23])**.** *Consider a semi-honest adversary performing ideal measurement on a state sharing some entanglement with register E while solving b-XHOG for $b \geq \frac{(1-\varepsilon)N}{N+1}$, A is a length-n bitstring, and C is an n-qubit quantum circuit from the Haar measure. We have*

$$\Pr_{C \sim \mathrm{Haar}(N)} [H(A|E)_\psi \geq (0.99 - \varepsilon)n] \geq 1 - O(N^{-0.02}). \tag{87}$$

where ψ is the output state.

Finally, a fully general device given oracle access to C is considered.

Theorem 13 (Corollary 7.16 of [AH23])**.** *Consider a T-query adversary solving $(1+\delta)$-XHOG, A is a length-n bitstring, and C is an n-qubit quantum circuit from the Haar measure. For $T = \mathsf{poly}(n), \delta = \Omega(1)$, and $\eta \in (0, 1]$, we have*

$$H(A|CE)_\psi \geq (1-\eta)\delta n - O(\log n), \tag{88}$$

where ψ is a quantum state $N^{-\Omega(\delta\eta)}$-close to the output of the adversary.

B.1 Protocols

The above single round results allow them to use the entropy accumulation theorem to define a multi-round protocols that outputs certified smooth min-entropy for each case. Moreover, for randomness expansion, fresh randomness is only consumed on logarithmically many rounds to generate fresh challenge circuits.

We see that the semi-honest adversary model and the random oracle model allows one to obtain a bound on the von Neumann entropy with quantum side information, and the respective RCS-based certified randomness protocols are certified randomness from entropy accumulation protocols satisfying Definition 7. We have omitted discussions of a general device in Section 5 of [AH23] since does not consider quantum side information, and Definition 7 is not satisfied.

We describe below a protocol in Fig. 9 that instantiates CVPV based on Theorem 12, which is closely related to Fig. 2 of [AH23]. The completeness of the protocol follows from the completeness of the original protocol in [AH23], and the soundness follows from the application of the entropy accumulation theorem.

We note that [AH23] claims to prove entropy accumulation of the protocol in Theorem 6.6 from Corollary 6.5, which is incorrect. Since the theorem states entropy is $\Omega(mn)$ with overwhelming probability over choices of C, where m is the number of rounds, the proof should be built on Theorem 6.4 (or Theorem 12 in reproduced here). It is straightforward to apply Corollary 6.5 for entropy accumulation, however, but the resulting theorem should no longer contain the clause 'with probability $1 - 2^{-\Omega(n)}$ over the choices of C' and the entropy needs to be conditioned on the challenge circuits as well.

Input: the qubit count n, the number of rounds ℓ, the score parameter $\delta \in [0, 1]$ and the fraction of test rounds $\gamma = O((\log n)/\ell)$.
Protocol:
V sample $C \sim \text{Haar}(N)$ and sends C to P.
For $i \in [\ell]$:

1. V_1 receives $A_i \in \{0, 1\}^n$ and V_2 receives $A'_i \in \{0, 1\}^n$
2. V aborts if the timing requirement fails
3. V aborts if $A_i \neq A'_i$

V samples $T_i \sim \mathsf{Bernoulli}(\gamma)$ for all $i \in [\ell]$.
Let $t = |\{i : T_i = 1\}|$. V aborts if $\frac{1}{t} \sum_{i:T_i=1} p_C(A_i) < (1 + \delta)/N$.

Figure 9: CVPV protocol against a semi-honest adversary.

For an instantiation based on Theorem 13, we use following protocol in Fig. 10. However, the protocol in Fig. 10 is very different from the protocol in Fig. 4 of [AH23]. Specifically, we do not reuse the circuit and therefore do not perform the test by summing the scores over epochs. The main reason for this choice is that we do not believe the application of entropy accumulation in [AH23] is correct, which we discuss in the supplement Section B.2.

In both cases, the original entropy accumulation theorem does not apply since Theorem 12 and 13 give entropy lower bounds for some scores, and the score is averaged over all rounds. This is in contract to bounding the entropy given some probability distribution. We discuss how to address this issue in the supplement Section B.3.

B.2 Issues with the Protocol in [AH23]

For the protocol in Fig. 4 of [AH23], the ith round quantum channel $\mathcal{M}_i$ is the joint system of V and P. Moreover, V takes the previous round circuit C_{i-1} as one of the inputs and set $C_i = C_{i-1}$ if $T_i = 0$ or $C_i \sim \text{Haar}(N)$ otherwise. Similarly, P also takes C_{i-1} as one of the inputs along with a quantum memory R_{i-1}. For this channel, the single round entropy $H(A_i|C_iE)$ where P takes on input a quantum state over $R_{i-1}E$ is not given by Theorem 13, since $C_i \sim$

Input: the qubit count n, the number of rounds ℓ, the score parameter $\delta \in [0,1]$ and the fraction of test rounds $\gamma = O((\log n)/\ell)$.
Protocol:
For $i \in [\ell]$:

1. V sample $C_i \sim \mathrm{Haar}(N)$ and sends C_i to P.
2. V_1 receives $A_i \in \{0,1\}^n$ and V_2 receives $A'_i \in \{0,1\}^n$
3. V aborts if the timing requirement fails
4. V aborts if $A_i \neq A'_i$

V samples $T_i \sim \mathsf{Bernoulli}(\gamma)$ for all $i \in [\ell]$.
Let $t = |\{i : T_i = 1\}|$. V aborts if $\frac{1}{\ell}\sum_{i:T_i=1} p_{C_i}(A_i) < (1+\delta)/N$.

Figure 10: CVPV protocol against a T-query adversary.

$\mathrm{Haar}(N)$ is required for Theorem 13.

$$H(A_i|C_iE) = (1-\gamma)H(A_i|C_iET_i = 0) + \gamma H(A_i|C_iET_i = 1) \tag{89}$$

To see this more explicitly, consider the case where P takes a classical state as input in memory R_{i-1}. Let the classical state be an output of an honest prover with input C_{i-1}. For a T-query P, P is allowed to simply output this classical state if $C_i = C_{i-1}$. The conditional entropy $H(A_i|R_{i-1})$ in this case is zero. Therefore, there should not be entropy accumulation over any rounds with $T_i = 0$.

We now describe mathematically where this breaks:

$$\begin{aligned}
H(A_i|C_iT_iE)_\nu &= \sum_C \Pr_{T_i}[C_i = C]\, H(A_i|T_iE, C_i = C)_\nu \\
&= \sum_C \Pr_{T_i}[C_i = C]\, H(A_i|E, C_i = C)_\nu \\
&= \gamma \sum_C h(C) H(A_i|E, C_i = C)_\nu + (1-\gamma)H(A_i|E, C_i = C_{i-1})_\nu \\
&= \gamma H(A_i|C_iE)_\nu + (1-\gamma)H(A_i|E, C_i = C_{i-1})_\nu,
\end{aligned}$$

where $h(C)$ is the probability of sampling C for a random challenge, and the second equality follows from the fact that once C is fixed, A_i and T_i are independent. To bound the entropy independent of a γ scaling factor, we need to be able to bound single-round entropy (with side information) for other distributions. In our case, we need to bound single-round entropy for point distributions which is clearly impossible.

One may argue that this type of argument could be used against certified randomness based on post-quantum secure trapdoor claw-free functions

[BCM$^+$21b]. Indeed, [BCM$^+$21b] explicitly discusses this issue that entropy accumulation theorem requires that single-round entropy bound for *all* possible input states, including those that are computationally inefficient strings. As a result, [BCM$^+$21b] presents significant additional analysis to show that entropy accumulates in the protocol, and nontrivial work was presented in [MAF23] to use the entropy accumulation theorem.

It is plausible that similar techniques may be applied to the analysis of [AH23] to the randomness expansion protocol, but we do not consider it here. In our setting, we do not require randomness expansion, and C_i can be sampled each round. This avoids the complications due to circuit reuse, and the entropy accumulation theorem can be directly applied to Theorem 13.

B.3 Issues with Entropy Accumulation

The single-round entropy lower bounds are in Theorem 12 and 13 are conditioned on the output achieving some score (e.g. b in b-XHOG), and the min-tradeoff functions used in [AH23] are defined for continuous scores. As a result, [AH23] developed a modified entropy accumulation theorem, which requires the Markov chain condition. However, for the arguments in Section A, we prove that the modified adversary satisfies the non-signalling condition which allows us to apply generalized entropy accumulation. To apply the entropy accumulation theorem in [AH23] to the modified adversary, we have to show that the modified adversary also satisfies the Markov chain condition.

Consider the modified adversary defined in E.q. 28. For the ith round channel output, we relabel $C_1^i G_1^i$ as I_i, and we have $\mathcal{M}'_{i+1} : R_i E_i \to A_{i+1} R_{i+1} R'_{i+1} I_{i+1}$. Further, copy the classical values of I_i into another register I'_i and send $E_i = I'_i R'_i$ as input to the guesser next round. Formally, the new quantum channel becomes

$$\mathcal{M}''_{i+1} : R_i E_i \to A_{i+1} R_{i+1} E_{i+1} I_{i+1} = \Lambda_{i+1} \mathcal{M}'_{i+1}, \tag{90}$$

where $\Lambda_i : I_i \to I_i I'_i$ is the classical channel that copies I_i into I'_i.

It should be noted that I_1^n has $n - i$ copies of $C_i G_i$. Nevertheless, we have $H_{\min}^{\varepsilon}(A_1^n | C_1^n G_1^n) = H_{\min}^{\varepsilon}(A_1^n | I_1^n)$, and therefore bounding $H_{\min}^{\varepsilon}(A_1^n | I_1^n)$ is sufficient for the protocol soundness.

Lemma 16. *For the quantum channel defined in E.q. 90, for some $\mathcal{R}'$, the Markov chain condition $A_i \leftrightarrow I_i \leftrightarrow I_{i+1}$ is satisfied:*

$$\rho_{A_i I_i I_{i+1}} = \mathcal{I}_{A_i} \otimes \mathcal{R}'_{I_i I_{i+1} \leftarrow I_i}(\rho_{A_i I_i}). \tag{91}$$

Proof.

$$\begin{aligned}
\rho_{A_i I_i I_{i+1}} &= \left(\operatorname{tr}_{A_{i+1} R_{i+1} E_{i+1}}\right) \rho_{A_{i+1} A_i R_{i+1} E_{i+1} I_{i+1} I_i} && (92)\\
&= \left(\operatorname{tr}_{A_{i+1} R_{i+1} R'_{i+1} I'_{i+1}} \Lambda_{i+1} \circ \mathcal{M}'_{i+1} \circ \Lambda_i\right) \rho_{A_i R_i R'_i I_i} && (93)\\
&= \left(\operatorname{tr}_{R'_{i+1}} \left(\operatorname{tr}_{A_{i+1} R_{i+1}} \mathcal{M}'_{i+1}\right) \circ \Lambda_i\right) \rho_{A_i R_i R'_i I_i} && (94)\\
&= \left(\operatorname{tr}_{R'_i - 1} \mathcal{R}_{E_{i+1} \leftarrow E_i} \circ \operatorname{tr}_{R_i} \circ \Lambda_i\right) \rho_{A_i R_i R'_i I_i} && (95)\\
&= \left(\operatorname{tr}_{R'_{i+1}} \mathcal{R}_{E_{i+1} \leftarrow I'_i} \circ \operatorname{tr}_{R'_i} \circ \Lambda_i\right) \rho_{A_i R'_i I_i} && (96)\\
&= \left(\operatorname{tr}_{R'_{i+1}} \mathcal{R}_{E_{i+1} \leftarrow I'_i} \circ \Lambda_i\right) \rho_{A_i I_i}, && (97)
\end{aligned}$$

where the third equality holds because $\operatorname{tr}_{I'_{i+1}} \Lambda_{i+1} = \mathcal{I}_{I_{i+1}}$, the forth equality holds due to Lemma 6, and the fifth equality holds for suitably defined $\mathcal{R}_{E_{i+1} \leftarrow I'_i}$ due to E.q. 32. □

As a result, we can bound $H^{\varepsilon}_{\min}(A_1^n | C_1^n G_1^n)$ by bounding $H^{\varepsilon}_{\min}(A_1^n | I_1^n)$ instead with the entropy accumulation theorem of [AH23]. We can expand the definition of certified randomness from entropy accumulation to the case where the min-tradeoff function is for a score. To do this, we simply need to change q for $\Sigma_i(q)$ into a score s, and define h as $h = \min_s f(s)$. With this expanded definition, the protocols in Fig. 9 and 10 are certified randomness from repetition due to Theorem 12 and 13, and they are therefore CVPV protocols.

Finally, we note that the choices of the min-tradeoff function in the application of entropy accumulation theorem of [AH23] are incorrect. Specifically, when using the entropy accumulation theorem in Section 4 of [AH23], $f(\delta) \to f(\delta/\gamma)$ and $\delta \to \gamma\delta$ should be applied for the general adversary without side information due to the fact that the test channel performs the test with probability γ only. The analysis of our CVPV protocols are immune from this issue as we effectively have $\gamma = 1$ since every round is tested. As for the semi-honest and general T-query adversary, similar changes should be adopted, but we leave rigorous analysis regarding this to future work.

The change $f(\delta) \to f(\delta/\gamma)$ and $\delta \to \gamma\delta$ has no effect on the linear term of the accumulated entropy, but it makes the correction term more significant due to the change in $\|\nabla f\|_\infty$. Otherwise, the current theorems in [AH23] of accumulated entropy gives entropy completely independent of the test probability γ. This is implausible since higher γ should lead to lower acceptance probability at fixed entropy (fixed adversary), which should increase the entropy if the acceptance probability should be fixed.

We show this more formally and illustrate this for the general adversary without side-information case of Section 5 of [AH23], and leave the other two cases for future work. The test score state for each round i is given by

$$\mathcal{M}_i(\sigma_{R_{i-1}})_{W_i} = (1-\gamma)\left|\perp\right\rangle\left\langle\perp\right| + \gamma \Pr_{C,\vec{z}\sim\mathcal{A}(C)}\left[\sum_i p_C(z_i) < \frac{bk}{N}\right]\left|0\right\rangle\left\langle 0\right| + \gamma \Pr_{C,\vec{z}\sim\mathcal{A}(C)}\left[\sum_i p_C(z_i) \geq \frac{bk}{N}\right]\left|1\right\rangle\left\langle 1\right|,$$

where $|\perp\rangle$ denotes the state on the test outcome register W_i that the round is not a test round, $|0\rangle$ is the test failed to pass the XEB test, and $|1\rangle$ is the test succeeded. From this, we know that we have an entropy bound of

$$H(A_i|C_i)_{\nu_{A_iC_i}} \geq \frac{B}{2}\frac{b\Pr_{C,\vec{z}\sim\mathcal{A}(C)}\left[\sum_i p_C(z_i) \geq \frac{bk}{N}\right] - \epsilon - 1}{b-1} = \frac{B}{2}\frac{b\frac{\langle 1|\nu_{W_i}|1\rangle}{\gamma} - \epsilon - 1}{b-1}.$$

Notice that what this means is that we have a min-tradeoff function $f_{\min}$ given by

$$f_{\min}(p) = \frac{B}{2}\frac{b\frac{p(1)}{\gamma} - \epsilon - 1}{b-1},$$

where p is a probability distribution over register W_i and $p(1) \equiv \Pr[W_i = 1]$. Note that this is the usual notion of min-tradeoff function with probability distributions as the argument, not the version with scores as the argument as required by [AH23]. One can in principle carry out the analysis using the second type as well, but the two types coincide in the analysis for general adversary without side information since the score for each round is a probability.

Now, applying the usual entropy accumulation theorem [DFR20], we have that

$$H_{\min}^{\epsilon_s}(Z_1^m|C_1^mT_1^mE)_{\rho_{ZCTE|\Omega}} \geq m\frac{B}{2}\frac{bq - \frac{b\delta}{\gamma} - \epsilon - 1}{b-1} - V\sqrt{m}\sqrt{\log\frac{2}{\Pr[\Omega]^2\epsilon_s^2}}$$

where $V = \log(1+2^{kn}) + \lceil \frac{Bb}{2\gamma(b-1)} \rceil$.

C Missing Proofs

In this section, we provide the additional proofs missing from the main body for brevity and due to similarity with already provided proofs.

C.1 Proof of Theorem 8

Proof. As in the proof of Theorem 7, we will consider hybrid experiments:

- **Hybrid 0:** This is the original CVPV soundness experiment.
- **Hybrid 1:** In this hybrid, the adversary consists of only two parties: $\mathcal{A}$ at position 0 and $\mathcal{B}$ at position 1. W.l.o.g., $(\mathcal{A},\mathcal{B})$ perform a round of simultaneous communication at times $t = 0, \Delta, \ldots, (\ell-1)\Delta$.

- **Hybrid 2:** In this hybrid, we additionally give $\mathcal{A}$ and $\mathcal{B}$ ch_i at time $t = (i-1)\Delta + 1$ for $i = 1, \ldots, \ell$.
- **Hybrid 2.1-ℓ:** We set **Hybrid 2.0** to be **Hybrid 2** and $G_0 := G$. For $i \in [\ell]$, we define **Hybrid 2.i** to be the same as **Hybrid 2.**$(i-1)$, except the oracle G_{i-1} is replaced by the reprogrammed oracle G_i, where

$$G_i(z) = \begin{cases} G_{i-1}(z), & z \neq x_i \oplus y_i \\ u_i, & z = x_i \oplus y_i \end{cases},$$

  with $u_i \leftarrow \{0,1\}^n$ being a fresh random string.
- **Hybrid 3:** In this hybrid, $\mathcal{A}$ and $\mathcal{B}$ only receive ch_i at time $t = (i-1)\Delta+1$, for $i \in [\ell]$, and no other input. They do not get access to the oracle G_ℓ either.

Let p_i be the optimal success probability of an efficient adversary in **Hybrid** i. Let $q = \mathsf{poly}(\lambda)$ be an upper-bound on the total number of oracle queries made by $(\mathcal{A}, \mathcal{B})$. We will show a sequence of claims which suffice for the proof:

Claim 11. $p_1 \geq p_0$.

Proof. Follows by a simple generalization of the corresponding claim in the proof of Theorem 6. □

Claim 12. $p_2 \geq p_1$.

Proof. Since we give extra information to the adversary, the success probability cannot decrease. □

Claim 13. *Setting* $p_{2.0} := p_2$, $p_{2.i} \geq p_{2.(i-1)} - \mathsf{negl}(\lambda)$ *for* $i \in [\ell]$.

Proof. Let $i \in [\ell]$ and $(\mathcal{A}, \mathcal{B})$ be an adversary that succeeds in **Hybrid 2.**$(i-1)$ with probability $p_{2.(i-1)}$. We will give a reduction $(\mathcal{A}', \mathcal{B}')$ for **Hybrid 2.i**:

- At times $t < (i-1)\Delta + 1$, $\mathcal{A}'$ (resp. $\mathcal{B}'$) runs $\mathcal{A}$ (resp. $\mathcal{B}$) using G_i as the oracle.
- At time $t = (i-1)\Delta$, $\mathcal{A}'$ sends (x_i, s_i) and $\mathcal{B}'$ sends y_i to each other, so that the messages are received at $t = (i-1)\Delta + 1$.
- At times $t \geq (i-1)\Delta+1$, $\mathcal{A}'$ and $\mathcal{B}'$ can simulate G_{i-1} using $(x_i, y_i, s_i, \mathsf{ch}_i, G_i)$ by reprogramming G_i to output $\mathsf{ch}_i \oplus s_i$ on input $x_i \oplus y_i$.
- $\mathcal{A}'$ (resp. $\mathcal{B}'$) outputs what $\mathcal{A}$ (resp. $\mathcal{B}$) outputs.

Note that the view of $(\mathcal{A}, \mathcal{B})$ as simulated by $(\mathcal{A}', \mathcal{B}')$ differs from **Hybrid 2.**$(i-1)$ at times $t < (i-1)\Delta+1$, and only on input $x_i \oplus y_i$ to the oracle. Therefore, if the probability that $(\mathcal{A}', \mathcal{B}')$ succeeds is upper-bounded by $p_{2.(i-1)} - \varepsilon$ for some non-negligible function ε, then by Lemma 1 the total query weight by $(\mathcal{A}, \mathcal{B})$ on input $x_i \oplus y_i$ at times $t < (i-1)\Delta + 1$ must be at least $2\varepsilon^2/q$. Suppose the query weight by $\mathcal{A}$ is at least ε^2/q, for the other case is similar. We give an extractor $(\widetilde{\mathcal{A}}, \widetilde{\mathcal{B}})$ in **Hybrid 2.**$(i-1)$:

- $\widetilde{\mathcal{A}}$ samples $j \leftarrow [q]$ and simulates $\mathcal{A}$, stopping the execution at the j-th query made by $\mathcal{A}$ to the oracle G_{i-1}, measuring the query as z^*. She outputs $y^* = z^* \oplus x_i$, where x_i is received at time $t = (i-1)\Delta$ from V_0.

- $\widetilde{\mathcal{B}}$ simulates $\mathcal{B}$.

By assumption, $y^* = y_i$ with probability $\varepsilon^2/q^2 > 2^{-m}$, which is a contradiction since y_i is information theoretically hidden from $\widetilde{\mathcal{A}}$ at times $t < (i-1)\Delta$. □

Claim 14. $p_3 \geq p_{2.\ell}$.

Proof. Let $(\mathcal{A}, \mathcal{B})$ be an adversary for **Hybrid 2.**ℓ that succeeds with probability $p_{2.\ell}$. We give a reduction $(\mathcal{A}', \mathcal{B}')$ that succeeds in **Hybrid 3** with the same probability:

- At time $t = -\infty$, $\mathcal{A}'$ and $\mathcal{B}'$ sample a $2q$-wise independent hash function G'. In addition, they sample $(x_i, y_i, s_i) \leftarrow \{0,1\}^m \times \{0,1\}^m \times \{0,1\}^n$ for $i \in [\ell]$.

- $\mathcal{A}'$ simulates $\mathcal{A}$ using G' as the oracle, the sampled values (x_i, y_i), as well as the values ch_i received from V_0.

- $\mathcal{B}'$ similarly simulates $\mathcal{B}$ using G' as the oracle, the sampled values y_i, as well as the values ch_i received from V_1.

The view of $(\mathcal{A}, \mathcal{B})$ is perfectly simulated since the oracle G_ℓ in **Hybrid 2.**ℓ is independent of the values (x_i, y_i, s_i) for all $i \in [\ell]$. This is because the oracle has been reprogrammed on all inputs $x_i \oplus y_i$ to remove any such dependence. Thus, by Lemma 2, G' simulates an independent random oracle and the proof is complete. □

Claim 15. $p_3 \leq \mathsf{negl}(\lambda)$.

Proof. Follows from the certified randomness property (Definition 3). $\mathcal{A}$ plays the role of the prover and $\mathcal{B}$ that of the eavesdropper. Note that the no-signalling condition is satisfied because $(\ell-1)\Delta < 1$, which means no message can be sent between $\mathcal{A}$ and $\mathcal{B}$ in time from the first challenge until the last. □

□