Nonlocality under Computational Assumptions

Citation for the original published paper (version of record):
Gluch, G., Barooti, K., Gheorghiu, A. et al (2024). Nonlocality under Computational Assumptions. PROCEEDINGS OF THE 56TH ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING, STOC 2024: 1018-1026. http://dx.doi.org/10.1145/3618260.3649750

Nonlocality under Computational Assumptions

Grzegorz Gluch
EPFL
Lausanne, Switzerland
grzegorz.gluch@epfl.ch

Khashayar Barooti
Aztec Labs
London, United Kingdom
khashayar@aztecprotocol.com

Alexandru Gheorghiu
Chalmers University of Technology
Gothenburg, Sweden
andru@agheorghiu.com

Marc-Olivier Renou
Inria - Université Paris-Saclay - CPHT - École Polytechnique - Institut Polytechnique de Paris
Paris, France
marc-olivier.renou@inria.fr

ABSTRACT

Nonlocality and its connections to entanglement are fundamental features of quantum mechanics that have found numerous applications in quantum information science. A set of correlations is said to be nonlocal if it cannot be reproduced by spacelike-separated parties sharing randomness and performing local operations. An important practical consideration is that the runtime of the parties has to be shorter than the time it takes light to travel between them. One way to model this restriction is to assume that the parties are computationally bounded. We therefore initiate the study of nonlocality under computational assumptions and derive the following results:

(a) We define the set NeL (not-efficiently-local) as consisting of all bipartite states whose correlations arising from local measurements cannot be reproduced with shared randomness and *polynomial-time* local operations.
(b) Under the assumption that the Learning With Errors problem cannot be solved in *quantum* polynomial-time, we show that NeL = ENT, where ENT is the set of *all* bipartite entangled states (pure and mixed). This is in contrast to the standard notion of nonlocality where it is known that some entangled states, e.g. Werner states, are local. In essence, we show that there exist (efficient) local measurements producing correlations that cannot be reproduced through shared randomness and quantum polynomial-time computation.
(c) We prove that if NeL = ENT unconditionally, then BQP ≠ PP. In other words, the ability to certify all bipartite entangled states against computationally bounded adversaries gives a non-trivial separation of complexity classes.
(d) Using (c), we show that a certain natural class of 1-round delegated quantum computation protocols that are sound against PP provers cannot exist.

STOC '24, June 24–28, 2024, Vancouver, BC, Canada

ACM ISBN 979-8-4007-0383-6/24/06
https://doi.org/10.1145/3618260.3649750

CCS CONCEPTS

• **Theory of computation** → **Quantum complexity theory**; **Complexity classes**; *Cryptographic primitives*; Interactive proof systems; *Cryptographic protocols*.

KEYWORDS

Nonlocality, Complexity Theory, Learning With Errors, Delegated Quantum Computation.

ACM Reference Format:
Grzegorz Gluch, Khashayar Barooti, Alexandru Gheorghiu, and Marc-Olivier Renou. 2024. Nonlocality under Computational Assumptions. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC '24), June 24–28, 2024, Vancouver, BC, Canada.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3618260.3649750

1 INTRODUCTION

Quantum advantage refers to a situation in which a quantum machine outperforms classical counterparts. In the context of computation, it is when a quantum computer outperforms classical computers at solving certain problems, such as factoring integers or simulating quantum mechanical systems. *Nonlocality* is a different notion of quantum advantage that dates back to the inception of quantum mechanics itself. This advantage arises in Bell games, where e.g. two non-communicating parties, Alice and Bob, are given inputs x and y and produce outcomes a and b distributed according to a probability distribution $p(a, b|x, y)$. Such distribution is said to be nonlocal if it cannot be expressed as a mixture of deterministic distributions, that is cannot be obtained through local operations on shared randomness. As proven by John Bell [10], to answer questions raised in [22], there exist entangled quantum states that can produce nonlocal correlations through local quantum measurements. The so-called CHSH game [21] fully formalizes this result. There, Alice and Bob are given inputs $x, y \in \{0, 1\}$ and asked to produce outputs $a, b \in \{0, 1\}$ such that $a \oplus b = x \cdot y$. If Alice and Bob's correlations are local, it can be shown that, under uniformly random inputs x, y, their outputs will satisfy $a \oplus b = x \cdot y$ at most 75% of the time. In contrast, if the two share an EPR pair $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ on which they perform local measurements, as a function of their respective inputs, they can succeed with probability $\cos^2(\pi/8) \approx 85\%$. This demonstrates the nonlocal nature of quantum mechanics.

A natural question to ask is whether all entangled states can produce nonlocal correlations. In other words, for a given entangled state, does there exist a *nonlocal game*, like the CHSH game, in which Alice and Bob can achieve a higher success rate by sharing the entangled state and performing local measurements than they could through *any* strategy involving shared randomness and local operations? If we restrict to pure entangled states, then this is indeed the case [25]. However, in 1989, Werner demonstrated the existence of mixed entangled states, for which a local model can always be constructed [42]. That result holds only for projective measurements but it was later generalized to all POVMs in [9]. Hence, there exist entangled states whose correlations (obtained through any local quantum measurements) can be reproduced in a setting where the two parties hold only a separable state, which up to technical details is equivalent to sharing public randomness. It therefore seems that, at least in the standard nonlocal games framework, entanglement and nonlocality are fundamentally distinct notions.

In the hopes of finding a purely operational task that can exactly distinguish between entangled and separable states, other frameworks were considered. Among them is the so-called *semi-quantum games* framework [20]. This differs from a standard nonlocal game by allowing Alice and Bob to receive trusted *quantum inputs*, while still outputting classical bits. All entangled state (both pure and mixed) can produce nonclassical correlations in a semi-quantum game. More precisely, for every entangled state, there exists a semi-quantum game in which Alice and Bob can succeed with higher probability by sharing that state than what they could obtain from any strategy based on any separable state.

While semi-quantum games can distinguish between entangled and separable states, they have the rather unsatisfying feature of requiring quantum inputs. Effectively, the referee of the game must have a trusted device for preparing these quantum input states and then send them to Alice and Bob via quantum channels. But to properly test quantum mechanics, one would aim for a more *device-independent* characterization in which both inputs and outputs are classical and no quantum device is trusted. Subsequent work showed that this is possible at the expense of introducing two additional parties [13], while the bipartite setting remains open.

A common feature of both nonlocal and semi-quantum games is that the "no communication" restriction on participating parties is often assumed to be enforced through *spacelike separation*. In other words, Alice and Bob should send their responses to the referee in less time than it would take light to travel between them. This effectively puts a time limit on how long each party has to compute and send their response. However, do they always have the *time* to compute this response? As we will observe later, [9] simulation algorithm seems computationally costly. Combining this observation with the extended quantum Church-Turing thesis begs the question of whether accounting for the computational efficiency of the parties would change the set of states that can be certified with a nonlocal game.

Main results. We introduce a model of two-party nonlocal games with *computationally bounded* parties, where Alice and Bob's inputs and outputs are classical bit-strings and the only distinction from standard nonlocal games is the assumption of computational efficiency. In other words, we consider games in which Alice and Bob can achieve a higher success rate by sharing an entangled state and performing *quantum polynomial-time* local operations than they could through *any* quantum polynomial-time strategy involving shared randomness and local operations.

Surprisingly, we show that this brings us closer to the goal of operationally characterizing all entangled states in the bipartite setting.

Our approach follows a recent trend of combining ideas from quantum information theory and computational complexity, which has yielded many new insights such as using cryptographic machinery to solve information-theoretic tasks like generating true randomness ([17]), finding new results in quantum cryptography ([28], [6], [36], [31]), using computational considerations to address paradoxes in quantum gravity ([2], [11]) and others. More recent works have also explored entanglement under computational assumptions, showing that any nonlocal game can lead to a test of quantum computational advantage [30] and that determining how entangled a state is can be computationally intractable (a notion referred to as *pseudoentanglement*) [3, 23], later generalized in [7].

Our contributions are the following:

New model of nonlocality. We define a new notion of nonlocality that incorporates computational efficiency. We say that a state ρ_{AB} is *not-efficiently-local*, and denote the set of all such states as NeL, if there exists a probability distribution arising from local measurements of ρ_{AB} such that no *efficient*, non-communicating parties (sharing a separable state) can reproduce this distribution. "Efficient" in this context is defined as implementable in quantum polynomial time (QPT).

Cryptography implies entanglement certification. We show that in our newly defined model, one can design a distinguishing experiment for *all* entangled states, including mixed states.

More concretely, under *the Quantum Learning With Errors (QLWE) assumption*, we show that for every entangled state, ρ_{AB}, there exists a 3-round (6-message) nonlocal game between a referee (which we will refer to as the *verifier*) and non-communicating parties Alice and Bob such that,

(i) if Alice and Bob share the state ρ_{AB}, there exist efficient quantum operations that they can perform locally so that they win the game with high probability and,
(ii) if Alice and Bob share any separable state, there do not exist any efficient quantum operations that they can perform locally in order to win the game with high probability.

This demonstrates that our notion of not-efficiently-local states, exactly characterizes the set of all bipartite entangled states. Summarizing, under the QLWE assumption, we have that ENT = NeL, where ENT denotes the set of all bipartite entangled states.

As mentioned the protocol relies on the QLWE assumption. The Learning With Errors (LWE) problem introduced in [39] is widely used in cryptography to create secure encryption algorithms. It is based on the idea of representing secret information as a set of equations with errors ([33]). The QLWE assumption is standard in cryptography ([40]) and assumes that LWE is intractable for polynomial-time quantum algorithms. The security of a scheme

under the QLWE assumption is shown via a reduction to this problem. In our case, we show that if the parties win the game when they share some separable state, then this implies that the parties solved the LWE problem. This contradicts the assumptions of our model as the parties were required to be quantum polynomial time.

Entanglement certification implies complexity class separation. Having shown that NeL = ENT under the QLWE assumption, we then focus on what it would take to prove the equality unconditionally. In other words, how hard is it for Alice and Bob to fake entanglement with separable states? To address this question, we consider a particular way of "faking entanglement", namely the Hirsch local model ([26]) for 1-round protocols. We show that this model can be implemented in PP. Concretely, for some entangled state ρ_{AB}, we show how to simulate any QPT strategy of Alice_1 and Bob_1 having access to ρ_{AB}, by a PP strategy of Alice_2 and Bob_2 with access to a *separable state* σ_{AB}. This means that local simulation in the Bell scenario is at most as hard as PP. Summarizing, ENT = NeL $\Rightarrow$ BQP $\neq$ PP.

This shows that separating BQP and PP is a necessary condition for being able to certify entanglement against computationally bounded parties, while the previous result shows that the QLWE assumption is a sufficient condition.[1]

Delegation of quantum computation. The result ENT = NeL $\Rightarrow$ BQP $\neq$ PP has interesting implications for protocols for delegating quantum computations (DQC). These are protocols in which a classical polynomial-time *verifier* delegates a BQP computation to an untrusted quantum *prover* and is able to certify the correctness of the obtained results (a property known as *soundness*). A breakthrough result by Mahadev gave the first such DQC protocol with soundness against BQP provers [35]. This was achieved under the QLWE assumption. A major open problem in the field is whether DQC protocols that are sound against computationally unbounded provers exist.

We give evidence for the difficulty of resolving this question by showing that a version[2] of 1-round DQC protocols sound against PP provers do not exist. We can also rephrase this by saying that if there exists a certain 1-round DQC protocol sound against BQP provers, then BQP $\neq$ PP. This is in the same spirit as the results of [4], showing that blind DQC protocols sound against all provers are unlikely to exist. Our result can be viewed as an improvement over that work, as we show the non-existence of protocols sound against PP provers, which is a weaker requirement.

2 TECHNICAL OVERVIEW

We start by introducing our new model of nonlocality, which we call the not-efficiently-local model. Our definition, in the spirit of the extended quantum Church-Turing thesis, assumes that any computation in the physical world can be modeled by a polynomial time quantum machine. This essentially translates to limiting the power of dishonest parties in a nonlocal game to quantum polynomial time (QPT). An informal version of the definition states

Definition 1 (Not-efficiently-local - Informal). For a quantum state ρ_{AB} we say that ρ_{AB} is not-efficiently-local if there exists a game (or protocol) $\mathcal{G}(\rho_{AB})$ between a probabilistic polynomial-time (PPT) verifier, **V**, and two non-communicating QPT parties **A**, **B**. Specifically, for every $\ell \in \mathbb{N}$, all the parties run in time $\text{poly}(\ell)$ and the verifier exchanges $\text{poly}(\ell)$ bits of communication with **A** and **B**. The game satisfies the following properties:

(1) (**Completeness**) If $\mathcal{G}(\rho_{AB})$ is run with **A**, **B** sharing ρ_{AB}, **V** accepts the interaction with probability at least $c(\ell)$,
(2) (**Soundness**) For **every** QPT $\mathbf{A}', \mathbf{B}'$, if $\mathcal{G}(\rho_{AB})$ is run with $\mathbf{A}', \mathbf{B}'$ sharing a separable state, **V** accepts the interaction with probability at most $s(\ell)$,

with $c(\ell) - s(\ell) > \frac{1}{\text{poly}(\ell)}$. We denote the set of all such states, ρ_{AB}, as NeL.

Remark 1. *We emphasize that the polynomial runtime of* **A** *and* **B** *is always with respect to the parameter ℓ which sets the desired gap between completeness and soundness. In particular, the dimension of the shared entangled state that is being tested need not depend on ℓ and can be constant. In a practical run of such a protocol, the value of ℓ would be determined based on the spatial separation between* **A** *and* **B**, *which establishes the maximum amount of time for* **A** *and* **B** *to respond to* **V**, *and cryptographic considerations like whether 2^ℓ operations can be performed in that time.*

Remark 2. *With this definition there is a slight ambiguity in whether we're assuming not just that* **A** *and* **B** *can solve only problems in* BQP, *but that their operations can be modelled using quantum mechanics. That is to say, whether we can represent* **A** *and* **B** *using quantum circuits of polynomial size acting on some input state, as opposed to making no assumptions about their inner workings. This becomes important when one proves computational reductions using the operations of* **A** *and* **B**. *In cryptography, it is the distinction between whitebox and blackbox reductions. We will assume that the former is the case (we model* **A** *and* **B** *as quantum circuits and perform whitebox reductions). As will become clear, this fact is relevant for our second result. The details can be found in the full version of our manuscript and we make additional comments about this distinction in Section 4.*

Essentially by definition, all states that are not-efficiently-local must be entangled. Denoting the set of all entangled bipartite states as ENT, this means that NeL $\subseteq$ ENT. A natural question is whether it is also the case that ENT $\subseteq$ NeL, or in other words, whether ENT = NeL. We phrase this question as a conjecture to which we will refer throughout the paper.

Conjecture 1 (ENT = NeL)**.** *For every finite-dimensional $\mathcal{H}_A, \mathcal{H}_B$ and every entangled state ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$, ρ_{AB} is not-efficiently-local.*

If Conjecture 1 is true then there is an equivalence between the notion of entanglement and our notion of not-efficient-locality. We will also say that if Conjecture 1 is true then we can certify all entangled states.

2.1 Cryptography Implies Entanglement Certification

Our second contribution shows that Conjecture 1 is true (and ENT = NeL), under the assumption that LWE is intractable for

[1] Also note that the QLWE assumption directly implies BQP $\neq$ PP, as LWE $\in$ NP $\subseteq$ PP.
[2] Our version of DQC is related to the quantum fully-homomorphic encryption scheme considered in [30]. See the full version of our paper for details.

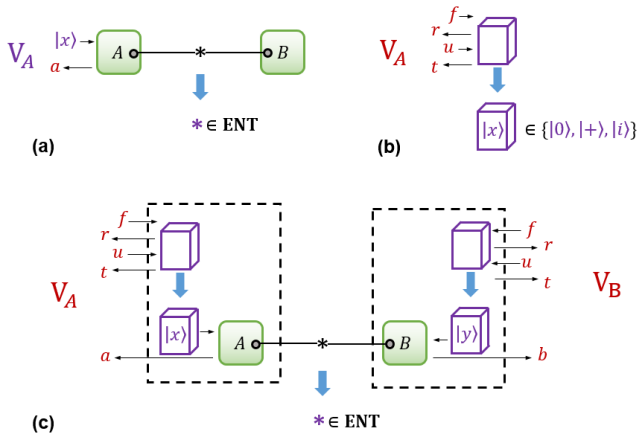

Figure 1: A visualisation of the compilation of the semi-quantum game into a certification test with classic input/outputs.
(a) represents the Semi-Quantum Game (SQG) of [20]. A, B share an entangled state ρ_{AB}. V_A sends an input state $|x\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |i\rangle, |-i\rangle\}$ to A, who performs a Bell state measurement on $|x\rangle$ and its share of ρ_{AB}. V_B, B do the same with input $|y\rangle$. The statistics $p(a, b \mid |x\rangle, |y\rangle)$ certify that ρ_{AB} had to be entangled.
(b) represents the Remote State Preparation (RSP) protocol,The protocol guarantees that under the QLWE assumption, the protocol certifies that A had prepared a quantum state $|x\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |i\rangle, |-i\rangle\}$ blindly, and can be operated on, it. V_A has knowledge of the state A has prepared by the end of the interaction.
(c) visualizes the Entanglement Certification protocol obtained by compiling the SQG using two independent RSP protocols with A and B.

QPT algorithms.[3] The result can be informally summarized as follows:

Theorem 2 (Informal). *Assuming QLWE, for every finite dimensional Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$, every entangled state ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$ and every $\ell \in \mathbb{N}$ there exists a 3-round (6-message[4]) interactive protocol where the PPT(ℓ) verifier, V, exchanges $\mathrm{poly}(\ell)$ bits of communication with QPT(ℓ) A and B such that:*

- *If A and B share ρ_{AB} and follow V's instructions, then their interaction is accepted by V with probability $1 - \mathrm{negl}(\ell)$.*
- *For every $A', B' \in$ QPT(ℓ), if they share a separable state then the interaction is accepted by V with probability $1/\mathrm{poly}(\ell)$.*

Proof techniques. We first develop a *remote state preparation (RSP) protocol* which allows the classical verifier to certify the preparation of certain states by Alice and Bob. Assuming QLWE, the protocol ensures that Alice and Bob will not know which states they have prepared (while the verifier will). The protocol is based on the one from [24]. Next, the verifier will perform the Buscemi *semi-quantum game (SQG)* with Alice and Bob [20]. As mentioned, this game, which requires quantum inputs for Alice and Bob, allows the verifier to certify any bipartite entangled state. Our protocol will then achieve this under computational assumptions. To give more details, let us briefly review both SQG and RSP.

The SQG bipartite protocol. We review the protocol from [20], adopting the formulation of [19]. The protocol is based on *entanglement witnesses*, which are operators W such that $\mathrm{Tr}[W\sigma_{AB}] \leq 0$ for all separable states σ_{AB} but $\mathrm{Tr}[W\rho_{AB}] > 0$ for some entangled state ρ_{AB}. As the set of separable states is convex, any entangled state ρ_{AB} can be associated with an entanglement witness W with $\mathrm{Tr}[W\rho_{AB}] > 0$. Any such W admits a local tomographic decomposition $W = \sum_{s,t} \beta_{s,t}\ \tau_s \otimes \omega_t$ where τ_s, ω_t are the density matrices corresponding to the states in $\mathcal{S} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |i\rangle, |-i\rangle\}$.

Based on this decomposition, [19] proposes a two player game, which certifies that ρ_{AB} is entangled. Two players, sharing ρ_{AB}, independently receive random quantum input states τ_s and ω_t, respectively, from two verifiers.[5] Each player is asked to perform a joint Bell state measurement on the received quantum input state and their share of ρ_{AB} and output the result of the measurement. One can introduce a Bell-like score based on the decomposition of W such that if the players act honestly then the score is exactly $\mathrm{Tr}[W\rho_{AB}]$, and if the players cheat by employing any strategy based on some separable shared state σ_{AB}, then the score is upper bounded by $\mathrm{Tr}[W\sigma_{AB}] \leq 0$. Hence, if the score is strictly positive, the protocol certifies that the players shared some entangled state. The possible quantum inputs for Alice and Bob are the states in $\mathcal{S}$ and so, for our protocol, these are the states the verifier(s) would have to instruct them to prepare.

The RSP protocol. Remote state preparation is a protocol between a classical verifier and a quantum prover, allowing the verifier to certify the preparation of a quantum state in the prover's system. It will allow the verifier to check (under the QLWE assumption)

[3] Strictly speaking, we are assuming that LWE is intractable for *non-uniform* QPT algorithms, i.e. LWE $\notin$ BQP/qpoly. This is a standard assumption in post-quantum cryptography (see for instance Definition 2.5 in [18]).
[4] We assume 1 round is always equal to 2 messages.

[5] This can also be just one verifier, as before. We mention two verifiers to be consistent with the presentation from [19] and to be closer to how such an experiment would be realized in practice. Indeed, since our resulting protocol is 3-round, the only way to ensure spacelike separation would be to have a local verifier for Alice and one for Bob that are giving them their questions and recording their responses. The two verifiers would then communicate with each other to decide whether Alice and Bob win the game or not.

that the prover has prepared a random state from the set $\mathcal{S}$. We show that our protocol is (i) complete, meaning that an honest QPT prover succeeds with high probability in preparing a state from $\mathcal{S}$, known only to the verifier, and (ii) sound, meaning that any dishonest QPT prover attempting to deceive the verifier will fail with high probability. The formal statement of soundness is delicate but informally speaking it guarantees that if the QPT prover is accepted, then its behavior is equivalent to it having received a random quantum state from $\mathcal{S}$.

Our protocol is simpler than the one from [24]. In that protocol the prover prepares eigenstates of all of the five bases $\left\{X, \frac{X-Y}{\sqrt{2}}, Y, \frac{X+Y}{\sqrt{2}}, Z\right\}$. We require the prover to prepare eigenstates only of $\{X, Y, Z\}$. It is because these eigenstates are exactly the members of $\mathcal{S}$ which we require to perform the SQG. Our protocol performs fewer checks and therefore the soundness does not follow directly from that of [24]. As such, we require a careful analysis to derive the soundness of our protocol.

The Entanglement Certification protocol. Our resulting entanglement certification protocol is a combination of RSP and SQG. The verifier performs two independent runs of RSP, one with Alice and one with Bob. If either one fails, the verifier will count this as a loss. Otherwise, the verifier will then perform the Buscemi SQG with Alice and Bob. Combining the two protocols involves several nontrivial steps stemming from the fact that we operate in the computationally-bounded model. Fig 1 provides a high-level visualization of the compilation.

2.2 Entanglement Certification Implies Separation of Complexity Classes

The previous result gives a *sufficient* condition for proving Conjecture 1, namely the QLWE assumption. Here, we derive a *necessary* condition by showing that if the conjecture is true we obtain a non-trivial separation of complexity classes. Specifically:

Theorem 3. ENT = NeL ⇒ BQP ≠ PP.

We note that PP is a relatively large class, e.g. PH ⊆ P^{PP} by Toda's theorem ([41]), but nevertheless PP ⊆ PSPACE. A consequence of our result is therefore that proving Conjecture 1 is at least as hard as proving that BQP ≠ PSPACE.

Proof techniques. Our starting point is a result of [26] showing that for a certain entangled state, ρ_{AB}, there is a local model for *all* POVM measurements. In other words, by sharing only a separable state (or random bits), Alice and Bob would be able to reproduce the statistics produced through local measurements of ρ_{AB}. In effect, this implies that the state ρ_{AB} cannot be certified through a nonlocal game. The question then becomes: how hard is it for Alice and Bob to implement the strategy from [26]? We show that their strategies, given as Algorithms 1 and 2, can be implemented in PP. This then proves the contrapositive of Theorem 3, i.e. that if BQP = PP then ENT ≠ NeL. For ease of explanation, we will describe Alice and Bob's strategies as implementable by QPT machines with postselection, making use of the seminal result of Aaronson that PP = PostBQP [1]. PostBQP is the set of problems solvable in quantum polynomial-time with *postselection*.

The input in Algorithm 1 (a similar situation happens for Algorithm 2) is a POVM $\{\mathcal{A}_a\}_a$. Up to "fine-graining" we can, without a loss of generality, assume that $\mathcal{A}_a = \eta_a P_a$ with $\eta_a \in (0, 1]$ and P_a being a rank one projector. In our computational setting, this POVM is implicitly defined by a question x, which **A** received from **V**, and a circuit $C^{\mathbf{A}}_{\mathsf{poly}(\ell)}$ that an honest **A** would have applied to her share of ρ_{AB}. The main challenge in implementing the simulation is to realize the operations in Algorithm 1 (and 2), which are expressed in terms of $\{\mathcal{A}_a\}_a$, efficiently while having access to the description of $C^{\mathbf{A}}_{\mathsf{poly}(\ell)}$ only. Intuitively, the local model works as follows. **A** and **B** will share many copies of Haar random single-qubit states, denoted $|\lambda\rangle$.[6] Their answers to **V** are then computed based on dot products of the form $\langle\lambda| P_a |\lambda\rangle$. The key step in the proof is to estimate these dot products up to enough precision in PostBQP. For instance, to implement $\mathbb{1}_{\{\langle\lambda|P_a|\lambda\rangle < \langle\lambda|(\mathbb{I}-P_a)|\lambda\rangle\}}$ from Algorithm 1, we show that there exists a QPT algorithm with postselection that, given a, creates a 1-qubit state which is equal to the eigenvector of P_a. Next, we prove that given a description of $|\lambda\rangle$ it is possible to compute an approximation to $\langle\lambda| P_a |\lambda\rangle$ while having access to polynomially many copies of the eigenvector state of P_a. To do that

Algorithm 1 AliceSim-Ideal$(q, \rho^*_{AB}, \mathcal{A}, |\lambda\rangle)$

Input: parameter q, description of $\rho^*_{AB} = \frac{1}{4}[\rho_0(q) + \rho_A \otimes \sigma_B + \sigma_A \otimes \rho_B + \sigma_A \otimes \sigma_B] \in \mathcal{S}(\mathbb{C}^2)$, POVM $\mathcal{A} = \{\mathcal{A}_a\}_a = \{\eta_a P_a\}_a$, state $|\lambda\rangle \sim \omega(\mathbb{C}^2)$.
Sample a according to $\eta_a/2$
Set $c_1 = \mathbb{1}_{\{\langle\lambda|P_a|\lambda\rangle < \langle\lambda|(\mathbb{I}-P_a)|\lambda\rangle\}}$
Sample $c_2 \sim \mathrm{Ber}(\langle 0| P_a |0\rangle)$
Sample $c_3 \sim \mathrm{Ber}(\langle -| P_a |-\rangle)$
Pick c from $\{c_1, c_2, c_3\}$ with corresponding probabilities $2q, 1-3q, q$
if $c = 1$ **then**
  Return a
else
  Sample a' according to $\mathrm{Tr}[\mathcal{A}_{a'}\sigma_A]$
  Return a'
end if

Algorithm 2 BobSim-Ideal$(q, \rho^*_{AB}, \mathcal{B}, |\lambda\rangle)$

Input: parameter q, description of $\rho^*_{AB} = \frac{1}{4}[\rho_0(q) + \rho_A \otimes \sigma_B + \sigma_A \otimes \rho_B + \sigma_A \otimes \sigma_B] \in \mathcal{S}(\mathbb{C}^2)$, POVM $\mathcal{B} = \{\mathcal{B}_b\}_b = \{\xi_b Q_b\}_b$, state $|\lambda\rangle \sim \omega(\mathbb{C}^2)$.
Sample c according to $\xi_b/2$
Sample $c_1 \sim \mathrm{Ber}(\langle\lambda| Q_b |\lambda\rangle)$
Sample $c_2 \sim \mathrm{Ber}(\frac{1}{2})$
Pick c from $\{c_1, c_2\}$ with corresponding probabilities $2q$ and $1-2q$
if $c = 1$ **then**
  Return b
else
  Sample b' according to $\mathrm{Tr}[\mathcal{B}_{b'}\sigma_B]$
  Return b'
end if

[6] We note that the proof works even if the two share classical descriptions of these states that can represent them to a sufficiently high precision.

we build on the ideas from [1] to show that using the power of postselection one can compute exponentially accurate dot products between 1-qubit states in polynomial time.

The final step is to argue that if PostBQP = BQP then we can implement our simulation in QPT. This is not immediate, as the assumption PostBQP = BQP allows us to replace QPT machines with postselection with QPT machines without postselection *only for decision problems*. However, the QPT algorithm with postselection designed for our local simulation, samples an answer according to a distribution—it is thus an instance of a sampling problem. As such, we need to also prove a sampling-to-decision reduction for this problem. We do this through a careful binary-search-like procedure.

Remark 3. *It's important to clarify how postselection is used in our setting. Indeed, one thing that* ***we do not do*** *is to allow Alice and Bob to postselect on their shared randomness, as that would permit them to signal instantaneously. As mentioned, we use* PostBQP *merely for ease of explanation. We can equivalently view Alice and Bob as being efficient agents with access to a* PP *oracle which they use in order to obtain very precise estimates of inner products. From this perspective, postselection is used to provide a "boost" in computational power, not to communicate instantaneously.*

2.3 Implications for Delegation of Quantum Computation (DQC)

We consider a version of a 1-round DQC protocol, which we refer to as Extended Delegation of Quantum Computation (EDQC). We then show that EDQC protocols sound against PP provers do not exist. Equivalently, we prove that the existence of a BQP-sound, EDQC implies BQP ≠ PP. This can be summarized in the following informal theorem:

Theorem 4 (Informal). PP-*sound EDQC protocols do not exist.*

Proof techniques. The high-level idea of the proof is to construct a PP prover that is always able to cheat successfully in an EDQC protocol. Let us first informally describe what an EDQC protocol is. For a circuit C that accepts as input a classical s and an auxiliary 1-qubit[7] state ρ_Q, EDQC guarantees the following.

- **(Completeness)** There exists a PPT verifier and a QPT prover such that for every state ρ_{QE} on $\mathbb{C}^2 \otimes \mathcal{H}_E$ chosen by the prover the interaction will be accepted and will satisfy the following. For every s the following two states are equal: (i) the output bit collected by the verifier and the contents of the E register, (ii) the result of measuring the output qubit of $U_C \otimes \mathbb{I}_E |s\rangle \rho_{QE}$ and the contents of the E register (where U_C is the unitary corresponding to C). In words, the protocol preserves the entanglement between the output of C and the E register.
- **(Soundness)** For every QPT prover accepted with high probability there exists a state ρ_Q on $\mathbb{C}^2$ such that the output bit collected by the verifier is, *for every classical* x, close to the distribution of measuring the output qubit of $U_C |s\rangle \rho_Q$.

[7]We could have considered a more general definition, where the auxiliary register holds a state on many qubits. Our definition generalizes naturally. We chose this version for simplicity and because our result implies that the more general protocol is not possible either.

Note that if the output qubit of C doesn't depend on ρ_Q then our definition reduces to the standard verification definition for 1-round DQC. This means that the only additional requirement of EDQC is consistency with the auxiliary input. A recent work ([30], Definition 2.3) considered a very similar requirement in the context of quantum fully-homomorphic-encryption (qFHE). The authors demonstrate that the auxiliary input requirement is satisfied by preexisting qFHE protocols of [34] and [14]. Recently, this was used by [37] to show that the existence of qFHE with auxillary input implies the existence of DQC. The main difference between our notion of EDQC and qFHE with auxillary input is that the soundness of qFHE is expressed as indistinguishability of the prover's views, whereas our definition requires a type of verifiability. We note that although the EDQC definition is nonstandard, protocols satisfying its requirements most likely exist under the QLWE assumption in the quantum random-oracle model (QROM). We refer the reader to the full manuscript for a more in-depth discussion about the details of EDQC and a comparison to other variants of DQC.

To prove Theorem 4 we make use of Theorem 3, i.e. ENT = NeL ⇒ BQP ≠ PP. Specifically, we assume towards contradiction that a BQP-sound, EDQC protocol exists and that BQP = PP. Next, we build a nonlocal game certifying ENT = NeL by using two independent instances of EDQC to control the behavior of the two players. This is very much in the same spirit as how we used RSP and SQG to prove ENT = NeL under the QLWE assumption in Theorem 2. We then obtain a contradiction with Theorem 3 which concludes the proof.

Our approach yields a stronger result about the limits of DQC compared to previous works. We summarize those results, together with our contribution, in Table 1. Note that showing the impossibility of a PP-sound protocol is a harder requirement than showing the impossibility of an ALL-sound protocol. Finding a local hidden variable model implementable in a lower complexity class (i.e. a subset of PP), or with more rounds of interaction, would imply even stronger lower bounds. We also expect our technique to be useful for showing impossibility results about other cryptographic primitives, such as (quantum) FHE.

3 RELATED WORKS

Computational entanglement. There are a number of recent works that study entanglement through the computational lens. In [3] the authors give a construction of states computationally indistinguishable from maximally entangled states with entanglement entropy arbitrarily close to $\log n$ across every cut. This gives an exponential separation between computational and information-theoretic quantum pseudorandomness (in the form of t-designs). Extending upon [3] in [7] a rigorous study of computational entanglement is initiated. More concretely, they define the computational versions of one-shot entanglement cost and distillable entanglement. Informally speaking, the operational measure of entanglement in both of these works relates to the number of maximally entangled states to which a state in question is equivalent. In contrast, our operational measure is whether a state displays any nonlocality.

Recently, [30] demonstrated how to compile any nonlocal game to a single-prover interactive game maintaining the same completeness and soundness guarantees, where the soundness holds

Table 1: Summary of known results about the possibility or impossibility of DQC protocols. The rows denote the number of rounds in a protocol and the columns denote the required soundness. We implicitly assume BQP completeness. Additionally, next to each entry we list the corresponding work and the assumptions needed. We note that our result doesn't require any assumptions.

	BQP-sound	PP-sound	ALL-sound
1-round	**YES** – [5] QLWE, in QROM	**NO** – Theorem 4	**NO** – By def. BQP⊈AM
2-round	**YES** – [35] QLWE	?	**NO** – [8] BQP⊈AM
poly-round	**YES** – [35] QLWE	?	**NO** – [4] BQP⊈NP/poly

against BPP adversaries. The compilation uses a version of quantum fully-homomorphic-encryption (qFHE). This means that under computational assumptions any non-local game leads to a single-prover quantum computational advantage protocol. Building upon [30] in [37] a DQC protocol is constructed by compiling the CHSH game using a qFHE scheme (sound against BQP adversaries). These works are in some sense dual to Theorem 2. They show how to use nonlocal games to construct more efficient protocols for quantum advantage and DQC while Theorem 2 shows how to use RSP to construct nonlocal games.

Generalizations of nonlocality and local simulations. Compared to the Bell scenario, a larger set of entangled states can be certified in a scenario where many copies of the state are given [38], or where more rounds of communication are allowed [26], or in the broadcasting scenario [12]. However, it is still an open question whether one of these scenarios (or a combination of them) can reconcile the concepts of entanglement and nonlocality.

The local simulation of Barrett ([9]) was generalized in [27], where it was shown that there exist entangled states with local models for all protocols in a special case of a sequential scenario called local filtering. These are 3-message protocols, where the parties first send one bit each to the verifier, then receive a challenge, and finally reply to the challenge.

Assumptions needed for BQP*-sound DQC..* It is believed that BQP is not in AM, where AM is a class of languages recognizable by 1-round protocols sound against ALL provers. A classical result shows that for every constant $k > 2$ we have $\mathsf{AM}[k] = \mathsf{AM}$, where $\mathsf{AM}[k]$ is the same as AM but with k-messages (each round consists of 2 messages) [8]. These two results imply that ALL-sound, constant-round DQC protocols don't exist under the likely assumption that BQP $\not\subseteq$ AM. In [4] a generalization to more rounds was considered. It was observed that ALL-sound blind DQC with polynomially-many rounds of interaction does not exist provided BQP $\not\subseteq$ NP/poly. It was also shown that blind DQC protocols exchanging $O(n^d)$ bits of communication, which is ALL-sound imply that BQP $\subseteq \mathsf{MA}/O(n^d)$—containment which does not hold relative to an oracle.

Note, that [5] showed that a sufficient assumption for BQP-sound 1-round DQC protocol in the QROM is the QLWE assumption. Our result shows that BQP $\neq$ PP is a necessary condition. Similarly, the assumption of BQP $\neq$ PP was recently shown necessary for the existence of pseudorandom states, which shows that it is a non-trivial requirement [32]. Pseudorandom states, introduced in [29], are efficiently computable quantum states that are computationally indistinguishable from Haar-random states.

4 DISCUSSION AND OPEN PROBLEMS

We have introduced the concept of nonlocality under computational assumptions by considering nonlocal games in which participating parties are computationally bounded. In this model, we showed that all entangled states can be distinguished from separable states, under the QLWE assumption. This is in contrast to the standard notion of nonlocality in which states like certain Werner states cannot be distinguished from separable states. This can be seen in analogy to the notions of *proof systems* and *argument systems*. The former are interactive protocols that should be sound against unbounded adversaries, whereas the latter have to be sound merely against computationally bounded adversaries. It is known that in many situations argument systems are more expressive than proof systems. For instance, in the case of zero-knowledge protocols, SZK, the set of problems that admit statistical zero-knowledge proofs is believed to be strictly smaller than CZK, the set of problems admitting computational zero-knowledge arguments. Similarly, we showed that the set of entangled states that can be distinguished from separable states is strictly larger when the parties are computationally bounded. While the QLWE assumption is sufficient for our results, we also showed that BQP $\neq$ PP is a necessary requirement. From this, we derived the non-existence of certain PP-sound protocols for delegating quantum computations. Our work opens up several interesting directions for further exploration.

Operational characterization of ENT *and blackbox reductions.* As mentioned in the introduction, one of the main goals of research into nonlocality is to give an operational characterization of the set of all entangled states. Importantly, this characterization should not assume the correctness of quantum mechanics a priori. For this reason, while we showed that all entangled states can be distinguished from separable ones under the QLWE assumption, we also assumed the correctness of quantum mechanics because we described the inner workings of Alice and Bob using quantum circuits. In the cryptographic terminology, we proved a *whitebox* reduction from LWE to the soundness of the NeL protocol. This is inherited from the soundness proof of the RSP protocol, which uses the prover's quantum operations explicitly in order to construct an efficient adversary that solves LWE. As such, an interesting open problem is

whether there exists a *blackbox* reduction. If so, this would indeed provide the desired operational characterization of ENT under the QLWE assumption.

It would also be desirable to have a NeL protocol involving only one round of communication, as opposed to our protocol which uses 3 rounds.

Further applications of computational entanglement. As we've noted, several recent works have investigated computational notions of entanglement, primarily pseudoentanglement. Much like how pseudoentanglement provides a separation between computational and information-theoretic pseudorandomness, we expect computational nonlocality to provide further interesting separations with respect to standard, information-theoretic nonlocality. For instance, one could consider nonlocal games in which both parties receive the same question from the referee. In standard nonlocality, this would not allow for the certification of any state, as both Alice and Bob would know each other's input. However, in the semi-quantum games framework, while both parties receive the same quantum state, due to the uncertainty principle they would still not know which state they received. This could then be extended to the NeL setting, showing that nonlocal games with both parties having the same question can still certify entangled states, provided the parties are computationally bounded. In essence, in this computational setting, one is trading the uncertainty principle for non-rewindability. A similar connection between these two distinct notions of non-classicality was also observed by [30].

Another avenue would be to explore scaled-down versions of standard multi-prover complexity classes. For instance, one could consider instances of MIP or QMA(2) with BQP honest provers. It's known that $\mathsf{MIP}^*[\mathsf{BQP}] = \mathsf{BQP}$, where $\mathsf{MIP}^*[\mathsf{BQP}]$ denotes the set of problems that can be verified efficiently by interacting with two BQP provers sharing entanglement (and in which soundness is against unbounded provers). Less is known in the setting where the provers are only allowed to share a separable state (such as MIP or QMA(2)) or an entangled state that is local. Connections to local simulation, along the lines of the proof of Theorem 4, might yield a separation between $\mathsf{MIP}[\mathsf{BQP}]$ and $\mathsf{MIP}^*[\mathsf{BQP}]$.

Cryptography and ENT = NeL. It is natural to conjecture that Theorems 2 and 3 could be strengthened so that an equivalence between the existence of a cryptographic primitive and ENT = NeL is achieved. One avenue for strengthening Theorem 2 could be to base the result on qFHE with auxiliary input [30]. Indeed, this was shown in [37] to allow for DQC. Likely, their results would also lead to an RSP protocol, in which case one would indeed derive ENT = NeL from BQP-sound qFHE, following our approach. This would also have the intriguing feature of compiling a standard nonlocal game (in the case of [37], the CHSH game) into a nonlocal game with computationally bounded parties.

To improve Theorem 3 one could try to use the fact that ENT = NeL gives us an *average-case hardness* and not just the worst-case hardness that we used. Additionally, since the main element in our proof was the estimation of certain inner products to within inverse exponential precision, any approach for doing this in a class that's lower than PP (i.e. a subset of PP), would directly improve our result. It would be worth seeing, for instance, whether Stockmeyer's approximate counting could help, in which case one would obtain that ENT = NeL implies BPP ≠ NP.

It is worth mentioning that connections of a similar flavor have recently been found in other contexts, e.g. in [15] an equivalence between a phenomenon in high-energy physics (the hardness of black-hole radiation decoding) and the existence of standard cryptographic primitives (EFI pairs from [16]) was shown.

Local simulation and DQC.. Further exploration of connections with local simulations can be fruitful. As we mentioned, [27] gives a local simulation for 3-message protocols. If one can implement it in PP also then that would likely imply that PP-sound 3-message protocols for DQC don't exist. Moreover, there is a strong connection between many-round local simulations and the major open problem of whether information-theoretic sound DQC protocols exist. For instance, if one could show that there exists a local simulation for some entangled state, for any number of rounds, then that should rule out information-theoretic sound EDQC protocols.

ACKNOWLEDGEMENTS

We thank Thomas Vidick for the helpful discussions. AG is supported by the Knut and Alice Wallenberg Foundation through the Wallenberg Centre for Quantum Technology (WACQT). At the time this research was conducted, KB was affiliated with EPFL.

REFERENCES

[1] Scott Aaronson. 2005. Quantum Computing, Postselection, and Probabilistic Polynomial-Time. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 461 (01 2005). https://doi.org/10.1098/rspa.2005.1546

[2] Scott Aaronson. 2016. The Complexity of Quantum States and Transformations: From Quantum Money to Black Holes. *Electron. Colloquium Comput. Complex.* TR16 (2016). https://api.semanticscholar.org/CorpusID:1869239

[3] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. 2022. Quantum pseudoentanglement. *arXiv preprint arXiv:2211.00747* (2022).

[4] Scott Aaronson, Alexandru Cojocaru, Alexandru Gheorghiu, and Elham Kashefi. 2019. Complexity-Theoretic Limitations on Blind Delegated Quantum Computation. In *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 132)*, Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi (Eds.). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 6:1–6:13. https://doi.org/10.4230/LIPIcs.ICALP.2019.6

[5] Gorjan Alagic, Andrew M. Childs, Alex Bredariol Grilo, and Shih-Han Hung. 2020. Non-interactive classical verification of quantum computation. *IACR Cryptol. ePrint Arch.* 2020 (2020), 1422.

[6] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. 2022. Cryptography From Pseudorandom Quantum States. In *Advances in Cryptology – CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part I* (Santa Barbara, CA, USA). Springer-Verlag, Berlin, Heidelberg, 208–236. https://doi.org/10.1007/978-3-031-15802-5_8

[7] Rotem Arnon-Friedman, Zvika Brakerski, and Thomas Vidick. 2023. Computational Entanglement Theory. (10 2023). arXiv:2310.02783 [quant-ph]

[8] László Babai and Shlomo Moran. 1988. Arthur-Merlin games: A randomized proof system, and a hierarchy of complexity classes. *J. Comput. System Sci.* 36, 2 (1988), 254–276. https://doi.org/10.1016/0022-0000(88)90028-1

[9] Jonathan Barrett. 2002. Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality. *Phys. Rev. A* 65 (Mar 2002), 042302. Issue 4. https://doi.org/10.1103/PhysRevA.65.042302

[10] J. S. Bell. 1964. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika* 1 (Nov 1964), 195–200. Issue 3. https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195

[11] Adam Bouland, Bill Fefferman, and Umesh Vazirani. 2020. Computational Pseudorandomness, the Wormhole Growth Paradox, and Constraints on the AdS/CFT Duality. In *11th Innovations in Theoretical Computer Science Conference (ITCS 2020) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 151)*, Thomas Vidick (Ed.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 63:1–63:2. https://doi.org/10.4230/LIPIcs.ITCS.2020.63

[12] Joseph Bowles, Flavien Hirsch, and Daniel Cavalcanti. 2020. Single-copy activation of Bell nonlocality via broadcasting of quantum states. *Quantum* 5 (2020),

499. https://api.semanticscholar.org/CorpusID:220919966
[13] Joseph Bowles, Ivan Šupić, Daniel Cavalcanti, and Antonio Acín. 2018. Device-Independent Entanglement Certification of All Entangled States. *Phys. Rev. Lett.* 121 (Oct 2018), 180503. Issue 18. https://doi.org/10.1103/PhysRevLett.121.180503
[14] Zvika Brakerski. 2018. Quantum FHE (Almost) As Secure As Classical. In *Advances in Cryptology – CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III* (Santa Barbara, CA, USA). Springer-Verlag, Berlin, Heidelberg, 67–95. https://doi.org/10.1007/978-3-319-96878-0_3
[15] Zvika Brakerski. 2023. Black-Hole Radiation Decoding is Quantum Cryptography. arXiv:2211.05491 [quant-ph]
[16] Zvika Brakerski, Ran Canetti, and Luowen Qian. 2023. On the Computational Hardness Needed for Quantum Cryptography. In *14th Innovations in Theoretical Computer Science Conference, ITCS 2023 (Leibniz International Proceedings in Informatics, LIPIcs)*, Yael Tauman Kalai (Ed.). Schloss Dagstuhl- Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing. https://doi.org/10.4230/LIPIcs.ITCS.2023.24 Publisher Copyright: © Zvika Brakerski, Ran Canetti, and Luowen Qian; licensed under Creative Commons License CC-BY 4.0.; 14th Innovations in Theoretical Computer Science Conference, ITCS 2023 ; Conference date: 10-01-2023 Through 13-01-2023.
[17] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. 2021. A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device. *J. ACM* 68, 5, Article 31 (aug 2021), 47 pages. https://doi.org/10.1145/3441309
[18] Zvika Brakerski, Paul F. Christiano, Urmila Mahadev, Umesh V. Vazirani, and Thomas Vidick. 2018. Certifiable Randomness from a Single Quantum Device. *CoRR* abs/1804.00640 (2018). arXiv:1804.00640 http://arxiv.org/abs/1804.00640
[19] Cyril Branciard, Denis Rosset, Yeong-Cherng Liang, and Nicolas Gisin. 2013. Measurement-Device-Independent Entanglement Witnesses for All Entangled Quantum States. *Phys. Rev. Lett.* 110 (Feb 2013), 060405. Issue 6. https://doi.org/10.1103/PhysRevLett.110.060405
[20] Francesco Buscemi. 2012. All Entangled Quantum States Are Nonlocal. *Phys. Rev. Lett.* 108 (May 2012), 200401. Issue 20. https://doi.org/10.1103/PhysRevLett.108.200401
[21] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. 1969. Proposed Experiment to Test Local Hidden-Variable Theories. *Phys. Rev. Lett.* 23 (Oct 1969), 880–884. Issue 15. https://doi.org/10.1103/PhysRevLett.23.880
[22] A. Einstein, B. Podolsky, and N. Rosen. 1935. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* 47 (May 1935), 777–780. Issue 10. https://doi.org/10.1103/PhysRev.47.777
[23] Alexandru Gheorghiu and Matty J Hoban. 2020. Estimating the entropy of shallow circuit outputs is hard. *arXiv preprint arXiv:2002.12814* (2020).
[24] Alexandru Gheorghiu and Thomas Vidick. 2019. Computationally-Secure and Composable Remote State Preparation. https://doi.org/10.1109/FOCS.2019.00066
[25] N. Gisin. 1991. Bell's inequality holds for all non-product states. *Physics Letters A* 154, 5 (1991), 201–202. https://doi.org/10.1016/0375-9601(91)90805-I
[26] Flavien Hirsch, Marco Túlio Quintino, Joseph Bowles, and Nicolas Brunner. 2013. Genuine hidden quantum nonlocality. *Physical review letters* 111 16 (2013), 160402.
[27] Flavien Hirsch, Marco Túlio Quintino, Joseph Bowles, Tamás Vértesi, and Nicolas Brunner. 2016. Entanglement without hidden nonlocality. *New Journal of Physics* 18, 11 (nov 2016), 113019. https://doi.org/10.1088/1367-2630/18/11/113019
[28] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. 2018. Pseudorandom Quantum States. Cryptology ePrint Archive, Paper 2018/544. https://eprint.iacr.org/2018/544 https://eprint.iacr.org/2018/544.
[29] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. 2018. Pseudorandom Quantum States. Cryptology ePrint Archive, Paper 2018/544. https://eprint.iacr.org/2018/544 https://eprint.iacr.org/2018/544.
[30] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. 2023. Quantum Advantage from Any Non-Local Game. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing* (Orlando, FL, USA) *(STOC 2023)*. Association for Computing Machinery, New York, NY, USA, 1617–1628. https://doi.org/10.1145/3564246.3585164
[31] William Kretschmer. 2021. Quantum Pseudorandomness and Classical Complexity. *ArXiv* abs/2103.09320 (2021). https://api.semanticscholar.org/CorpusID:232257841
[32] William Kretschmer. 2021. Quantum Pseudorandomness and Classical Complexity. Schloss Dagstuhl - Leibniz-Zentrum für Informatik. https://doi.org/10.4230/LIPICS.TQC.2021.2
[33] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. 2013. On Ideal Lattices and Learning with Errors over Rings. *J. ACM* 60, 6, Article 43 (nov 2013), 35 pages. https://doi.org/10.1145/2535925
[34] Urmila Mahadev. 2017. Classical Homomorphic Encryption for Quantum Circuits. *CoRR* abs/1708.02130 (2017). arXiv:1708.02130 http://arxiv.org/abs/1708.02130
[35] Urmila Mahadev. 2018. Classical Verification of Quantum Computations. *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (2018), 259–267.
[36] Tomoyuki Morimae and Takashi Yamakawa. 2022. Quantum Commitments And Signatures Without One-Way Functions. In *Advances in Cryptology – CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part I* (Santa Barbara, CA, USA). Springer-Verlag, Berlin, Heidelberg, 269–295. https://doi.org/10.1007/978-3-031-15802-5_10
[37] Anand Natarajan and Tina Zhang. 2023. Bounding the quantum value of compiled nonlocal games: from CHSH to BQP verification. https://api.semanticscholar.org/CorpusID:257353407
[38] Carlos Palazuelos. 2012. Superactivation of Quantum Nonlocality. *Phys. Rev. Lett.* 109 (Nov 2012), 190401. Issue 19. https://doi.org/10.1103/PhysRevLett.109.190401
[39] Oded Regev. 2005. On lattices, learning with errors, random linear codes, and cryptography.. In *STOC*, Harold N. Gabow and Ronald Fagin (Eds.). ACM, 84–93. http://dblp.uni-trier.de/db/conf/stoc/stoc2005.html#Regev05
[40] Oded Regev. 2009. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *J. ACM* 56, 6, Article 34 (sep 2009), 40 pages. https://doi.org/10.1145/1568318.1568324
[41] Seinosuke Toda. 1989. On the computational power of PP and (+)P. *30th Annual Symposium on Foundations of Computer Science* (1989), 514–519. https://api.semanticscholar.org/CorpusID:30272970
[42] Reinhard F. Werner. 1989. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A* 40 (Oct 1989), 4277–4281. Issue 8. https://doi.org/10.1103/PhysRevA.40.4277

Received 13-NOV-2023; accepted 2024-02-11