Quantum Advantage from Any Non-local Game

Quantum Advantage from Any Non-local Game*

Yael Kalai
Microsoft Research and MIT
USA
yael@microsoft.com

Alex Lombardi
Simons Institute and UC Berkeley
USA
alexlombardi@alum.mit.edu

Vinod Vaikuntanathan
MIT
USA
vinodv@mit.edu

Lisa Yang
MIT
USA
lisayang@mit.edu

ABSTRACT

We show a general method of compiling any k-prover non-local game into a single-prover (computationally sound) interactive game maintaining the same quantum completeness and classical soundness guarantees, up to a negligible additive factor in a security parameter. Our compiler uses any quantum homomorphic encryption scheme (Mahadev, FOCS 2018; Brakerski, CRYPTO 2018) satisfying a natural form of correctness with respect to auxiliary quantum input. The homomorphic encryption scheme is used as a cryptographic mechanism to simulate the effect of spatial separation, and is required to evaluate $k-1$ prover strategies out of k on encrypted queries.

In conjunction with the rich literature on (entangled) multi-prover non-local games starting from the celebrated CHSH game (Clauser, Horne, Shimony and Holt, Physical Review Letters 1969), our compiler gives a broad and rich framework for constructing protocols that classically verify quantum advantage.

CCS CONCEPTS

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

KEYWORDS

Quantum computational advantage, cryptographic protocols, non-local games, quantum homomorphic encryption

ACM Reference Format:
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 (STOC '23), June 20–23, 2023, Orlando, FL, USA*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3564246.3585164

*The full version of this paper is available at [25].

STOC '23, June 20–23, 2023, Orlando, FL, USA

ACM ISBN 978-1-4503-9913-5/23/06.
https://doi.org/10.1145/3564246.3585164

1 INTRODUCTION

Quantum computing promises to usher in a new era in computer science. There are several ongoing large-scale efforts by Google, Microsoft, IBM and a number of startups to demonstrate *quantum advantage*, that is, to construct a quantum machine capable of computations that no classical machine can replicate with comparable speed. Central to the demonstration of quantum advantage is the question of verification. That is, can a classical machine *check* that a given device is performing computations that no classical device is capable of? (One could relax this requirement to allow a verifier with *limited* quantum capabilities, for example, preparing and transmitting single-qubit states [3, 18]. In this paper, we deal exclusively with classical verifiers.)

Such verification schemes for quantum advantage are central to the ongoing race to construct non-trivial quantum computers. Several mechanisms have been proposed to classically verify quantum advantage:

(1) **The Algorithmic Method**: Ask the quantum machine to do a computation, such as factor a large number [36], that is believed to be hard for classical machines [28]. This is the most straightforward way to check quantum advantage, yet it is concretely very expensive and requires millions of high-fidelity qubits which is likely infeasible for near-term quantum machines (see [19] for a recent, optimized estimate).
(2) **The Sampling Method:** Ask the quantum machine to (approximately) sample from a distribution, which is presumably hard to accomplish classically [2, 14]. This results in tasks that are feasible for near-term quantum machines [5], yet suffers from two problems. First, checking that the output is correct (at least in the current proposals) is an exponential-time computation that quickly becomes infeasible for a classical machine. Secondly, the question of whether approximate sampling is classically hard is less clear and has come under question [29], despite hardness results for exact sampling [10].
(3) **The Interactive Method:** The most recent example of a way to demonstrate quantum advantage relies on using interactive proofs and the fact that quantum algorithms cannot necessarily be "rewound" which, in turn, is a consequence of the *quantum no-cloning principle*. Starting with the work of Brakerski, Christiano, Mahadev, Vazirani and Vidick [12], there have been a handful of proposals reducing the number

of rounds [13], improving the assumptions [37] and the computational efficiency and near-term feasibility [24], and extending to more powerful guarantees such as self-testing [33] and quantum delegation [31]. The practicality of the quantum machine in these protocols (eg. [38]) seems to fall somewhere between (1) and (2), i.e., the prover is more practical than with the algorithmic method but less than the sampling method. Compared to (2), verification by the classical machine is efficient.

Meanwhile, from more than half a century ago, starting with the celebrated works of John Bell [6] and Clauser, Horne, Shimony and Holt [16] to explain the Einstein-Podolsky-Rosen (EPR) paradox, there is a rich body of work that came up with several methods to test that two or more spatially separated, non-communicating quantum devices can generate (testable) correlations that no pair of classical devices can produce. This immediately gives us a test of quantum advantage of a very different kind, one whose validity relies on the (non-falsifiable) physical assumption that devices do not communicate.

(4) **The Non-Local Method:** Here, quantum advantage comes from *entanglement*. Ask for a pair (or more) of spatially separated, but entangled, quantum devices to perform a computation that no classical machine can replicate without communication. A classical example is the famed CHSH game [16], or other violations of the Bell inequality. A rich class of non-local games have since been constructed and this is an active area of current research with many breakthroughs in the last few years (e.g. [4, 20, 21, 32, 35] up until [23]). While many of these games are attractive and super-efficient (e.g. using only a small constant number of qubits), this suffers from possible "loopholes". That is, *how does one ensure that the provers* do not *subliminally communicate in some way*? Indeed, constructing so-called loophole-free demonstrations of Bell inequality violations is a Nobel prize-winning [1] and still active [22] area of research.

1.1 Our Results

A tantalizing question that comes out of the discussion above is the relation between techniques used to construct *multi-prover* non-local games and the ones used to construct *single-prover* proofs of quantumness. On the one hand, the former relies on entanglement whereas the latter relies on quantum non-rewinding. On the other hand, the intellectual foundations of single-prover protocols for quantum advantage sometimes come from non-local games. Indeed, Kahanamoku-Meyer, Choi, Vazirani and Yao [24], in a recent work, call their interactive single-prover protocol for quantum advantage a "computational Bell test". Yet, there have been no formal connections between multi-prover non-local games and single-prover interactive protocols for quantum advantage.

The central result of this work is the construction of a *simple* and *general* compiler that gives us an interactive protocol demonstrating quantum advantage starting from two building blocks.

Theorem 1.1. *Given:*

- Any *k-prover non-local game with quantum value c and classical value s; and*
- Any *quantum homomorphic encryption scheme satisfying correctness with respect to auxiliary input (Definition 2.3), that can implement homomorphic evaluation of* at least $k-1$ *prover strategies in the non-local game,*

there is a $2k$-message (We refer to a message from the prover to the verifier or the verifier to the prover as a round or a message.) single-prover interactive game with completeness c, realized by a quantum polynomial-time algorithm, and soundness $s + \mathsf{negl}(\lambda)$, against any classical polynomial-time algorithm. Here, λ is a security parameter that governs the security of the quantum homomorphic encryption scheme and negl *denotes a negligible function.*

This gives us a rich class of protocols by mixing and matching any non-local game (CHSH, Magic Square, Odd-Cycle Test, GHZ, and many more) and any powerful enough quantum homomorphic encryption scheme ([11, 30] both satisfy the appropriate correctness property; see the full version for more discussion).

For example, an instantiation of our method using the CHSH game and the quantum FHE scheme of Mahadev [30] gives us a protocol that already improves on the state of the art in several respects:

- **Simplicity of the Assumption.** Compared to [12], the protocols that come out of our framework do not require the adaptive hardcore bit property, and therefore can be instantiated from a variety of assumptions including Ring Learning with Errors (Ring-LWE), (For example, [30] gives a template for building QFHE from any "quantum capable classical homomorphic encryption scheme" ([30] Definition 4.2). [30] instantiates this template from LWE, but there is an analogous construction from Ring-LWE.) resulting in better efficiency.
- **Simpler Usage of Quantum Memory.** Compared to [12, 24], our CHSH-based protocol only requires that the quantum prover retain *a single qubit* of memory in between rounds, while [12, 24] require λ entangled qubits to be retained.
- Compared to [13, 37], our protocols do not require random oracles. [13] uses random oracles in a crucial way to obtain an instantiation from Ring-LWE, bypassing the adaptive hardcore bit property. They simultaneously achieve a two-round protocol in contrast to the 4-round protocol of [12].
- Compared to [24], our protocol requires 4 rounds as opposed to their 6.

Our framework elucidates interactive protocols for quantum advantage by separating them into an information-theoretic component (namely, the non-local game) and a cryptographic component (namely, the QFHE). We believe that the richness and extreme simplicity of our transformation could eventually lead to a protocol that concretely improves on the family of protocols in (3) above in a significant way. Philosophically, a remarkable aspect of our framework is that it uses cryptography as a bridge to connect two apparently different sources of quantumness, namely *entanglement* (used to construct non-local games) and *non-rewinding* (which underlies the reason why single-prover proofs of quantumness as in [12] work).

We proceed to describe a self-contained outline of our transformation below.

1.2 Technical Overview

Our framework is conceptually simple, drawing inspiration from similar compilers in the classical world [8, 9, 26, 27]. For the rest of the introduction, we focus on compiling *two-prover* non-local games and describe how to extend our construction to k provers in Section 3.2. The basic idea is to convert any non-local game into a single prover protocol by sending the prover the queries sent to *both* provers in the non-local game. It is easy to see that if we do this "in the clear", we lose soundness, since by giving both queries to a single prover, we lose the spatial separation condition. This is precisely where the encryption scheme comes into play.

Using cryptography to enforce spatial separation. We enforce spatial separation using an encryption scheme. Specifically, in our protocol the verifier samples two queries q_1, q_2 by emulating the verifier in the non-local game, and the interactive protocol proceeds in rounds, as follows:

(1) The verifier sends $\mathsf{Enc}(q_1)$ to the prover.
(2) The prover sends an encrypted answer $\mathsf{Enc}(a_1)$.
(3) The verifier then sends the second query q_2 (in the clear).
(4) The prover replies with an answer a_2.

The verifier accepts if the decrypted transcript would be accepted in the non-local game.

Comparison with classical compilers. We note that a 2-message version of this protocol was used by Kalai, Raz and Rothblum [26, 27] (and in follow-up works) to obtain 2-message delegation schemes for classical computations. In this 2-message variant, the verifier simply sends all of the queries in the first message each encrypted under independently chosen keys, and the prover computes each answer homomorphically.

However, this transformation *cannot* be used as a protocol that has a gap between classical and quantum winning probabilities. This is the case since the soundness of the resulting 2-message delegation scheme is proven only if the original non-local game has *non-signaling soundness*, namely, assuming the provers cannot cheat via a non-signaling (and therefore, via an entangled) strategy. In other words, classical provers may be able to implement non-signaling strategies, and these strategies can have value which is at least as high as the quantum value. Thus, we cannot argue that in the [27]-like 2-message protocol, a classical cheating prover cannot emulate this non-signaling strategy. Instead, we consider the 4-message protocol described above.

Our 4-message protocol also bears some resemblance to (although is significantly simpler than) the classical succinct argument system of [9], which is also concerned with compiling MIPs (with classical soundness) into single-prover protocols.

Completeness. We use the properties of the underlying encryption scheme to argue that any strategy of the (quantum) provers in the non-local game can be emulated in our protocol (partially "under the hood" of the encryption scheme). For this, we need our homomorphic encryption scheme to have the following two properties:

- It needs to support the quantum operations done by the first prover in the non-local game.
- It needs to be *entanglement preserving* in the following sense: if a quantum circuit C is defined using a register $\mathcal{A}$ and is homomorphically evaluated using a state $|\Psi\rangle_{\mathcal{AB}}$ that has entanglement between $\mathcal{A}$ and another register $\mathcal{B}$ (which is not input to C), the decrypted output y should remain correlated with $\mathcal{B}$ (as it would be if C were evaluated using the $\mathcal{A}$ register of $|\Psi\rangle$). This property can be enforced via a natural "aux-input correctness" property (Definition 2.3).

We view correctness with respect to auxiliary input as a natural requirement that one should expect to hold for a "typical" QHE scheme. Indeed, some earlier works on QHE required even stronger forms of entanglement preservation ([15] Definition 3.6), but these correctness variants were not studied for the more recent schemes with classical ciphertexts [11, 30]. In the full version, we show that our correctness definition follows from plain correctness under mild structural assumptions; namely, if decryption is "bit-by-bit" and homomorphic evaluation is "local." In particular, this implies that the seminal homomorphic encryption schemes due to Mahadev and Brakerski [11, 30] satisfy these two properties.

Soundness. We argue that any computationally bounded *classical* cheating prover in the 4-message protocol can be converted into a *local* prover strategy in the 2-player game, with roughly the same acceptance probability (see Theorem 3.2). This allows us to argue quantum advantage: Namely, an honest quantum prover can obtain the quantum value of the 2-player game, whereas any classical prover can obtain only the classical value of the 2-player game.

We prove our desired soundness condition with a security reduction that *rewinds* the classical adversary, something that cannot be done with a general quantum prover.

Special case: the CHSH game. To illustrate how our compiler preserves soundness, we first analyze a simple special case of our transformation where the 2-prover game is the CHSH game [16]. In the CHSH game, the verifier sends i.i.d. random bits x, y to P_1, P_2 (respectively); the provers are then supposed to return bits a, b such that $a \oplus b = xy$. The best local strategy for this game has success probability $3/4$ (e.g., if P_1, P_2 assume that $xy = 0$). This can be proved with a straightforward direct analysis:

- Any (say, deterministic) local strategy can be described by bits a_0, a_1, b_0, b_1 (corresponding to the two provers' responses when the verifier sends 0 or 1).
- The strategy is correct on query pair (x, y) if $a_x \oplus b_y = xy$.
- If the strategy is correct on *both* $(x, 0)$ and $(x, 1)$, then
$$a_x \oplus b_1 = x = x \oplus (a_x \oplus b_0),$$
which can only occur if $x = b_0 \oplus b_1$. Thus, at least one of the four pairs (x, y) must be answered incorrectly.

By making use of *rewinding*, it is possible to give a direct computational analogue of this soundness analysis for our 4-message compiled protocol. In the 4-message protocol, an adversarial prover P^* is given as input a ciphertext $\hat{x}$ encrypting a bit x, and returns a ciphertext $\hat{a}$ (which contains a message $a = a(x)$ that the verifier decrypts). Then, the verifier sends a bit y and the prover replies with a bit b. Unlike the 2-prover setting, this bit b *may* depend on x; however, since x is encrypted, b itself should not reveal *information* about x. However, one must be careful when arguing security because the verifier's *decision* (in the interactive game) makes use of the decryption key sk, which *can* reveal information about x.

Nevertheless, there is a simple argument showing that a classical prover cannot convince V with probability higher than $3/4 + \mathsf{negl}(\lambda)$:

- Let P^* be an adversarial prover (deterministic without loss of generality), and fix:
  - A ciphertext $\hat{x}$ sent by the verifier in the first round (sampled as a random encryption of a random bit), and
  - A ciphertext $\hat{a}$ returned by the prover in the second round.
- Moreover, let b_0 and b_1 denote the prover's responses on challenge $y = 0$ and $y = 1$ respectively (given fixed $\hat{x}, \hat{a}$).
- Then, if the verifier accepts *both* b_0 *and* b_1 (on challenges 0 and 1), we have
$$a \oplus b_1 = x = x \oplus (a \oplus b_0),$$
where $a = \mathrm{Dec}(\hat{a})$. As before, this implies that $b_0 \oplus b_1 = x$!
- Thus, if P^* is more than 3/4-convincing, we will break the security of the encryption scheme by guessing x with non-negligible advantage over 1/2, given only $\hat{x}$ (and the encryption key):
  - Given a ciphertext $\hat{x}$, run P^* on $\hat{x}$ to obtain $\hat{a}$.
  - Run P^* on $y = 0$, obtaining b_0, and then *rewind* P^* and run P^* on $y = 1$, obtaining b_1.
  - Output $b_0 \oplus b_1$.

  A straightforward calculation tells us that our advantage of guessing x in this reduction (compared to random guess) is non-negligible if P^* wins the interactive game with probability non-negligibly higher than 3/4.

This proves the security of our transformation for the special case of the CHSH game.

The General Case. Having illustrated the utility of our transformation in a special case, we now analyze its soundness for *any* 2-prover game.

Fix a classical cheating prover P^* for the 4-message protocol, and assume without loss of generality that it is deterministic (otherwise, fix its random coins to ones that maximize the success probability). The corresponding local provers (P_1^*, P_2^*) for the 2-player game are defined as follows:

- Fix the first 2 messages in the 4-message protocol, by choosing any q_1' (e.g., it can be the all-zero string), computing $\mathrm{ct}_1 = \mathsf{Enc}(q_1')$ and emulating P^* to compute $\mathrm{ct}_2 = P^*(\mathrm{ct}_1)$.
- P_2^* has $(\mathrm{ct}_1, \mathrm{ct}_2)$ hardwired. (We note that it suffices to hardwire ct_1 since $\mathrm{ct}_2 = P^*(\mathrm{ct}_1)$ can be computed from ct_1.) On input a query q_2, it emulates the response of P^*, conditioned on the first two messages being $(\mathrm{ct}_1, \mathrm{ct}_2)$, to obtain $a_2 = P^*(\mathrm{ct}_1, \mathrm{ct}_2, q_2)$. It outputs a_2.
- P_1^* also has $(\mathrm{ct}_1, \mathrm{ct}_2)$ hardwired (and thus can evaluate P_2^* on an arbitrary input). On input q_1 it computes for every possible a_1 the probability (over q_2 sampled conditioned on q_1) that the verifier accepts $(q_1, a_1, q_2, P_2^*(q_2))$ and sends a_1 with the maximal acceptance probability.

To argue that (P_1^*, P_2^*) convinces the verifier to accept with essentially the same probability that P^* does, we rely on the security of the encryption scheme. Namely, we argue (by contradiction) that if the verifier accepts with probability significantly smaller than the acceptance probability of P^* in the 4-message protocol, then there exists an adversary $\mathcal{A}$ that breaks semantic security of the underlying encryption scheme.

Specifically, $\mathcal{A}$ is given a challenge ciphertext ct, which it will use to define P_1^* and P_2^* (as above), and will use P_1^* and P_2^* in his attack. The first barrier is that P_1^* may not be efficient, which results with $\mathcal{A}$ being inefficient. Thus, we first argue that (a good enough approximation of) P_1^* can be emulated in time $2^{|q_1|+|a_1|} \cdot \mathsf{poly}(\lambda)$, which results in $\mathcal{A}$ running in that time as well. Loosely speaking, this is done by estimating for every a_1, the probability of acceptance, and taking a_1 with the maximal acceptance probability. This explains the exponential blowup in a_1. To estimate the probability that (q_1, a_1) is accepted (w.r.t. P_2^*) we do an empirical estimation by choosing many q_2's from the residual query distribution (conditioned on q_1) and compute the fraction of q_2's for which $V(q_1, q_2, a_1, P^*(q_2)) = 1$. We use the Chernoff bound to argue that this empirical estimation is close to the real probability of acceptance. Note that this estimation requires sampling q_2 from the residual query distribution (conditioned on q_1), and it is not clear that this can be done efficiently. Thus, we hardwire into $\mathcal{A}$ many such samples for each and every possible q_1, which results with the exponential blowup in q_1. (However, this blowup can be avoided for many non-local games; for example, if q_1 and q_2 are independent, or if the game is a parallel repetition of a constant-size game.)

Given this $2^{|q_1|+|a_1|}\mathsf{poly}(\lambda)$-time implementation of P_1^*, the hardness reduction proceeds as follows. Loosely speaking, given q_1, q_1', ct where ct is either $\mathsf{Enc}(q_1)$ or $\mathsf{Enc}(q_1')$ with equal probability, we run the 2-prover game with (P_1^*, P_2^*) corresponding to ct and with the first query being q_1, and then run it again with the first query being q_1'. If the verifier accepts exactly one of these executions, then we guess b to be the one corresponding to the winning execution; otherwise, we output a random guess for b.

Note that in our attack we broke the security in time $2^{|q_1|+|a_1|} \cdot \mathsf{poly}(\lambda)$ and thus need to assume that the encryption scheme has that level of security. For constant-size games, this is equivalent to polynomial security; in general, this requires assuming the sub-exponential security of the underlying FHE. However, as discussed in the full version, it is possible to rely on polynomially-secure FHE for certain superconstant-size non-local games such as parallel repetitions of a constant-size game. We refer the reader to Section 3 for the details, and to the proof of Theorem 3.2 for the formal analysis.

2 PRELIMINARIES

We let PT denote deterministic polynomial time, PPT denote probabilistic polynomial time and QPT denote quantum polynomial time. For any random variables A and B (possibly parametrized by a security parameter λ), we use the notation $A \equiv B$ to denote that A and B are identically distributed, and $A \approx_s B$ to denote that A and B have negligible ($\lambda^{-\omega(1)}$) statistical distance. We use $A \approx_c B$ to denote that A and B are computationally indistinguishable, namely for every PPT distinguisher D, $|\Pr[D(A) = 1] - \Pr[D(B) = 1]| = \lambda^{-\omega(1)}$.

Quantum States. Let $\mathcal{H}$ be a Hilbert space of finite dimension 2^n (thus, $\mathcal{H} \simeq \mathbb{C}^{2^n}$). A (pure, n-qubit) quantum state $|\Psi\rangle \in \mathcal{H}$ is an element of the form

$$|\Psi\rangle = \sum_{b_1,\ldots,b_n \in \{0,1\}} \alpha_{b_1,\ldots,b_n} |b_1,\ldots,b_n\rangle$$

where $\{|b_1,\ldots,b_n\rangle\}_{b_1,\ldots,b_n \in \{0,1\}}$ forms an orthonormal basis of $\mathcal{H}$, $\alpha_{b_1,\ldots,b_n} \in \mathbb{C}$ and

$$\sum_{b_1,\ldots,b_n \in \{0,1\}} |\alpha_{b_1,\ldots,b_n}|^2 = 1.$$

We refer to n as the number of registers of $|\Psi\rangle$.

We denote by $M(|\Psi\rangle)$ the outcome of measuring $|\Psi\rangle$ in the standard basis (throughout this work we are only concerned with standard basis measurements). For any set of registers $\mathcal{I} \subseteq [n]$, we denote by $M_{\mathcal{I}}(|\Psi\rangle)$ the outcome of measuring only the $\mathcal{I}$ registers of $|\Psi\rangle$ in the standard basis.

A *mixed state* $\boldsymbol{\rho}$ over $\mathcal{H}$ is a density operator (we use $\mathsf{S}(\mathcal{H})$ to denote the space of density operators on $\mathcal{H}$) normalized so that $\mathrm{Tr}(\boldsymbol{\rho}) = 1$. Every pure state $|\Psi\rangle$ has a corresponding rank 1 mixed state $|\Psi\rangle\langle\Psi|$ such that for any PSD projection Π, we have $||\Pi|\Psi\rangle||^2 = \mathrm{Tr}(\Pi|\Psi\rangle\langle\Psi|)$.

We sometimes divide the registers of $\mathcal{H}$ into named registers, denoted by calligraphic upper-case letters, such as $\mathcal{A}$ and $\mathcal{B}$, in which case we also decompose the Hilbert space into $\mathcal{H} = \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, so that each pure quantum state $|\Psi\rangle$ is a linear combination of quantum states $|\Psi_{\mathcal{A}}\rangle \otimes |\Psi_{\mathcal{B}}\rangle \in \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$.

For any mixed state $\boldsymbol{\rho}$, we denote by $\boldsymbol{\rho}_{\mathcal{A}}$ the reduced density operator

$$\boldsymbol{\rho}_{\mathcal{A}} = \mathrm{Tr}_{\mathcal{B}}(\boldsymbol{\rho}) \in \mathsf{S}(\mathcal{H}_{\mathcal{A}}),$$

where $\mathrm{Tr}_{\mathcal{B}}$ is the "partial trace" linear operator defined by

$$\mathrm{Tr}_{\mathcal{B}}(|\Psi_{\mathcal{A}}\rangle\langle\Psi_{\mathcal{A}}| \otimes |\Psi_{\mathcal{B}}\rangle\langle\Psi_{\mathcal{B}}|) = |\Psi_{\mathcal{A}}\rangle\langle\Psi_{\mathcal{A}}| \cdot \mathrm{Tr}(|\Psi_{\mathcal{B}}\rangle\langle\Psi_{\mathcal{B}}|).$$

Quantum Ciruits and Locality. A quantum circuit is a sequence of elementary quantum gates (taken from some complete basis) and measurement operations. These operations are applied to an initial state $|\psi\rangle$ and result in some final state $|\psi'\rangle$. For further definitions related to quantum circuits and gate types, we refer the reader to [34].

One direct consequence of this model is a form of **locality**: if $|\psi\rangle = |\psi\rangle_{\mathcal{AB}}$ is shared between two registers ($\mathcal{A}$ and $\mathcal{B}$), operations of the form $C \otimes \mathsf{Id}_{\mathcal{B}}$ (where C is a quantum circuit acting only on $\mathcal{A}$) can be performed *without possession of the register* $\mathcal{B}$.

2.1 Non-local Games

Definition 2.1 (k-Player Non-local Game). *A k-player non-local game $\mathcal{G}$ consists of a* PPT *sampleable query distribution Q over $(q_1,\ldots,q_k) \in (\{0,1\}^n)^k$ and a polynomial time verification predicate $\mathcal{V}(q_1,q_2,\ldots,q_k,a_1,a_2,\ldots,a_k) \in \{0,1\}$, where each $a_i \in \{0,1\}^m$. The classical value and the quantum value of $\mathcal{G}$ are defined below.*

- ***Classical (local) value:*** *The classical (or local) value v of $\mathcal{G}$ is defined as:*

$$\max_{\substack{P_1,\ldots,P_k:\\ \{0,1\}^n \to \{0,1\}^m}} \Pr_{(q_1,\ldots,q_k)\leftarrow Q} [\mathcal{V}(q_1,\ldots,q_k,P_1(q_1),\ldots,P_k(q_k)) = 1]$$

- ***Quantum (entangled) value:*** *The quantum (or entangled) value v^* of $\mathcal{G}$ is defined as:*

$$\sup_{\substack{|\Psi\rangle \in \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_k\\ U_i \in U(\mathcal{H}_i \otimes \mathbb{C}^n), 1 \le i \le k}} \Pr_{(q_1,\ldots,q_k)\leftarrow Q} [\mathcal{V}(q_1,\ldots,q_k,a_1,\ldots,a_k) = 1]$$

where the maximum is over all k-partite states $|\Psi\rangle \in \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_k$ (each $\mathcal{H}_i$ is an arbitrary finite-dimensional Hilbert space), unitaries U_i acting on $\log \dim_{\mathbb{C}} \mathcal{H}_i + n$ qubits respectively, and answers a_i computed by applying $U_1 \otimes \ldots \otimes U_k$ to $|\Psi\rangle \otimes |q_1 \ldots q_k\rangle$, and measuring the first m qubits in each $\mathcal{H}_i$; that is,

$$(a_1,a_2,\ldots,a_k) \leftarrow M_{\mathcal{I}}(U_1 \otimes \ldots \otimes U_k (|\Psi\rangle \otimes |q_1,\ldots,q_k\rangle))$$

for $\mathcal{I} = \{1,\ldots,m\} \times [k]$. We remark that without loss of generality, $|\Psi\rangle$ can be (and is above) taken to be a pure state.

We are interested in non-local games where quantum strategies can win with probability strictly more than any classical strategy, that is ones for which $v^* > v$.

Remark 2.2. In this work, it is crucial to consider the complexity of the honest provers in a non-local game, which is often not a parameter of interest in the literature but instead hidden in the description of the provers as a tuple of unitaries $(U_1,\ldots,U_k)$ and state $|\Psi\rangle$.

We explicitly consider non-local games where the each prover's unitary U_i can be implemented as a quantum circuit C_i of size polynomial in a security parameter λ. When $\mathcal{G}$ has constant size (such as the CHSH or Magic square games) this holds automatically, but this is a non-trivial requirement when the size of $\mathcal{G}$ grows with λ.

2.2 Quantum Homomorphic Encryption

We define the notion of quantum homomorphic encryption [11, 30] that is central to our framework. Unlike in [11], our definition requires a form of *correctness with respect to auxiliary input*. However, we show that this definition holds for QHE schemes satisfying mild additional requirements, and in particular holds for the [11, 30] schemes.

Definition 2.3 (Quantum Homomorphic Encryption (QHE)). *A quantum homomorphic encryption scheme* $\mathsf{QHE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{Dec})$ *for a class of quantum circuits C is a tuple of algorithms with the following syntax:*

- Gen *is a* PPT *algorithm that takes as input the security parameter 1^λ and outputs a (classical) secret key* sk *of* $\mathrm{poly}(\lambda)$ *bits;*
- Enc *is a* PPT *algorithm that takes as input a secret key* sk *and a classical input x, and outputs a ciphertext* ct*;*
- Eval *is a* QPT *algorithm that takes as input a tuple $(C, |\Psi\rangle, \mathsf{ct}_{\mathrm{in}})$, where $C : \mathcal{H} \times (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes m}$ is a quantum circuit, $|\Psi\rangle \in \mathcal{H}$ is a quantum state, and $\mathsf{ct}_{\mathrm{in}}$ is a ciphertext corresponding to an n-bit plaintext.* Eval *computes a quantum circuit $\mathsf{Eval}_C(|\Psi\rangle \otimes |0\rangle^{\mathrm{poly}(\lambda,n)}, \mathsf{ct}_{\mathrm{in}})$ which outputs a ciphertext $\mathsf{ct}_{\mathrm{out}}$. If C has classical output, we require that Eval_C also has classical output.*

- Dec *is a* PT *algorithm that takes as input a secret key* sk *and ciphertext* ct*, and outputs a state* $|\phi\rangle$*. Additionally, if* ct *is a classical ciphertext, the decryption algorithm outputs a classical string* y.

The above syntax is more general than the form required in [11]; we elaborate on this difference below. We require the following two properties from (Gen, Enc, Eval, Dec)*:*

- ***Correctness with Auxiliary Input:*** *For every security parameter* $\lambda \in \mathbb{N}$*, any quantum circuit* $C : \mathcal{H}_{\mathcal{A}} \times (\mathbb{C}^2)^{\otimes n} \to \{0,1\}^*$ *(with classical output), any quantum state* $|\Psi\rangle_{\mathcal{AB}} \in \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$*, any message* $x \in \{0,1\}^n$*, any secret key* $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$ *and any ciphertext* $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{sk}, x)$*, the following states have negligible trace distance:*
  Game 1*. Start with* $(x, |\Psi\rangle_{\mathcal{AB}})$*. Evaluate* C *on* x *and register* $\mathcal{A}$*, obtaining classical string* y*. Output* y *and the contents of register* $\mathcal{B}$*.*
  Game 2*. Start with* $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{sk}, x)$ *and* $|\Psi\rangle_{\mathcal{AB}}$*. Compute* $\mathsf{ct}' \leftarrow \mathsf{Eval}_C(\cdot \otimes |0\rangle^{\mathrm{poly}(\lambda,n)}, \mathsf{ct})$ *on register* $\mathcal{A}$*. Compute* $y' = \mathsf{Dec}(\mathsf{sk}, \mathsf{ct}')$*. Output* y' *and the contents of register* $\mathcal{B}$*.*
- T***-Classical Security:*** *For any two messages* x_0, x_1 *and any* $\mathrm{poly}(T(\lambda))$*-size classical circuit ensemble* $\mathcal{A}$*:*

$$\left| \Pr\left[\mathcal{A}(\mathsf{ct}_0) = 1 \;\middle|\; \begin{array}{l} \mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda) \\ \mathsf{ct}_0 \leftarrow \mathsf{Enc}(\mathsf{sk}, x_0) \end{array} \right] - \Pr\left[\mathcal{A}(\mathsf{ct}_1) = 1 \;\middle|\; \begin{array}{l} \mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda) \\ \mathsf{ct}_1 \leftarrow \mathsf{Enc}(\mathsf{sk}, x_1) \end{array} \right] \right| \le \mathsf{negl}(T(\lambda)) \;.$$

In words, "correctness with auxiliary input" requires that if QHE evaluation is applied to a register $\mathcal{A}$ that is a part of a joint (entangled) state in $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, the entanglement between the QHE evaluated output and $\mathcal{B}$ is preserved.

Remark 2.4. A *quantum fully homomorphic encryption (*QFHE*)* is a QHE for the class of all poly-size quantum circuits. While [11, 30] construct QFHE (with security against quantum distinguishers), weaker forms of QHE may yield more efficient quantum advantage protocols (see Section 4.2 for discussion).

Remark 2.5. In our definition of security, we only consider classical attacks. Classical security is sufficient for the purposes of this work as protocols for quantum advantage are required to have quantum completeness and classical soundness.

For the purposes of this paper, it suffices to know the following claim about the instantiability of Definition 2.3.

Claim 2.6. *The [11, 30] QFHE schemes satisfy Definition 2.3 with correctness holding for the class of all poly-size quantum circuits.*

Claim 2.6 can be verified by inspecting the constructions given in [11, 30]. In the full version, we show mild generic conditions under which a QFHE scheme satisfies correctness with respect to auxiliary input, and sketch a proof of Claim 2.6.

3 OUR COMPILER: FROM NON-LOCAL GAMES TO INTERACTIVE PROTOCOLS

In this section, we show how to use a quantum homomorphic encryption scheme satisfying aux-input correctness (Definition 2.3) to convert a 2-prover non-local game into a *single-prover* interactive protocol with *computational soundness.*

Definition 3.1 (Single-Prover Computationally Sound Interactive Game). *A single-prover computationally sound* (CS) *interactive game* $\mathcal{G}$ *consists of an interactive* PPT *verifier* $\mathcal{V}$ *that takes as input a security parameter* 1^λ *and interacts with an interactive prover. The classical (computationally sound) value and the quantum (computationally sound) value of* $\mathcal{G}$ *are defined below.*

- ***Classical*** CS ***value:*** $\mathcal{G}$ *has classical* CS *value* $\ge v$ *if and only if there exists an interactive polynomial-size Turing machine* $\mathcal{P}$ *such that for every* $\lambda \in \mathbb{N}$*,*

$$\Pr\Big[(\mathcal{P}, \mathcal{V})(1^\lambda) = 1\Big] \ge v$$

  where the probability is over the random coin tosses of $\mathcal{V}$*, and where* $(\mathcal{P}, \mathcal{V})(1^\lambda) \in \{0,1\}$ *denotes the output bit of* $\mathcal{V}(1^\lambda)$ *after interacting with* $\mathcal{P}$*.*
- ***Quantum*** CS ***value:*** $\mathcal{G}$ *has quantum* CS *value* $\ge v^*$ *if and only if there exists a Hilbert space* $\mathcal{H}$ *and a quantum state* $|\Psi\rangle \in \mathcal{H}$ *and an interactive* QPT *prover* $\mathcal{P}$ *such that for every* $\lambda \in \mathbb{N}$*,*

$$\Pr\Big[(\mathcal{P}(|\Psi\rangle), \mathcal{V})(1^\lambda) = 1\Big] \ge v^*$$

  where the probability is over the randomness of $\mathcal{P}$ *and* $\mathcal{V}$*.*

3.1 Our Transformation, $k = 2$ case.

Fix a quantum homomorphic encryption scheme QHE = (Gen, Enc, Eval, Dec) for a class of quantum circuits C (e.g. [11, 30], see Claim 2.6). We present a PPT transformation $\mathcal{T}$ that converts any 2-prover non-local game $\mathcal{G} = (\mathcal{Q}, \mathcal{V})$ into a single-prover computationally sound interactive game $\mathcal{T}^{\mathcal{G}}$ (asociated with security parameter λ), defined as follows.

(1) The verifier samples $(q_1, q_2) \leftarrow \mathcal{Q}$, $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$, and $\hat{q}_1 \leftarrow \mathsf{Enc}(\mathsf{sk}, q_1)$. In the first round the verifier sends $\hat{q}_1$ and in the third round he sends q_2.
(2) The verifier, upon receiving $\hat{a}_1$ from the prover in the first round, and a_2 in the second round, accepts if and only if $\mathcal{V}(q_1, q_2, \mathsf{Dec}(\mathsf{sk}, \hat{a}_1), a_2) = 1$.

Theorem 3.2. *Fix any* QHE *scheme for a circuit class* C*, and any 2-player non-local game* $\mathcal{G} = (\mathcal{Q}, \mathcal{V})$ *with classical value* v *and quantum value* v^**, such that the value* v^* *is obtained by a prover strategy* (C_1^*, C_2^*) *with a quantum state* $|\Psi\rangle \in \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ *where* $C_1^*(|\Psi\rangle_{\mathcal{A}}, \cdot) \in C$*. Denote by* $|q_1|$ *and* $|a_1|$ *the lengths of the query and answer of the first prover, respectively. If the underlying* QHE *encryption scheme is* T*-secure, for* $T(\lambda) = 2^{|q_1|+|a_1|} \cdot \mathrm{poly}(\lambda)$*, then the following holds:*

(1) *The quantum* CS *value of* $\mathcal{T}^{\mathcal{G}}$ *is at least* $v^* - \mathsf{negl}(\lambda)$*.*
(2) *The classical* CS *value of* $\mathcal{T}^{\mathcal{G}}$ *is at most* $v + \mathsf{negl}(\lambda)$*.*

Proof. Fix any 2-player non-local game $\mathcal{G} = (\mathcal{Q}, \mathcal{V})$ with classical value v and quantum value v^*, such that the value v^* is obtained by a prover strategy (C_1^*, C_2^*) with the (joint) quantum state $|\Psi\rangle \in \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, where $C_1^* \in C$.

The quantum CS *value of* $\mathcal{T}^{\mathcal{G}}$ *is at least* v^*. Consider the following QPT prover $\mathcal{P}^*$:

(1) In the first round, upon receiving $\hat{q}_1$, $\mathcal{P}^*$ computes $\mathsf{ct}' \leftarrow \mathsf{Eval}(\cdot_{\mathcal{A}}, C_1^*, \hat{q}_1)$ on the register $\mathcal{A}$ of $|\Psi\rangle_{\mathcal{A}\mathcal{B}}$, and sends ct. As internal state, $\mathcal{P}^*$ retains the contents of register $\mathcal{B}$.
(2) In the second round, upon receiving q_2, $\mathcal{P}^*$ uses its internal state $\boldsymbol{\rho}_{\mathcal{B}}$ to compute and send $a_2' \leftarrow C_2^*(\cdot_{\mathcal{B}}, q_2)$.

We argue that

$$\Pr\left[\mathcal{V}(q_1, q_2, a_1', a_2') = 1\right] = v^* - \mathsf{negl}(\lambda),$$

in the probability space where:

- $(q_1, q_2) \leftarrow Q$
- $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$ and $\hat{q}_1 \leftarrow \mathsf{Enc}(q_1, \mathsf{sk})$
- $\mathsf{ct}' \leftarrow \mathsf{Eval}(\cdot_{\mathcal{A}}, C_1^*, \hat{q}_1)$ applied to $|\Psi\rangle_{\mathcal{A}\mathcal{B}}$ and $\boldsymbol{\rho}$ set to the contents of $\mathcal{B}$.
- $a_1' = \mathsf{Dec}(\mathsf{sk}, \mathsf{ct}')$, and
- $a_2' \leftarrow C_2^*(\boldsymbol{\rho}, q_2)$

By the aux-input correctness of QHE (Definition 2.3) and the fact that $C_1^* \in C$, we see that for every q_1, the mixed state consisting of the distribution over $(a_1', \boldsymbol{\rho})$ above is the same (up to negligible trace distance) as what would have been obtained by applying $C_1 \otimes \mathsf{Id}_{\mathcal{B}}$ to $(|\Psi\rangle_{\mathcal{A}\mathcal{B}}, q_1)$. By the contractivity of trace distance (with respect to the map defined by $C_2^*(\cdot_{\mathcal{B}}, q_2)$ and $\mathcal{V}$), we conclude that

$$\begin{aligned}\Pr\left[\mathcal{V}(q_1, q_2, a_1', a_2') = 1\right] &= \Pr[\mathcal{V}(q_1, q_2, a_1, a_2) = 1] \pm \mathsf{negl}(\lambda) \\ &= v^* \pm \mathsf{negl}(\lambda),\end{aligned}$$

as desired.

The classical CS *value of* $\mathcal{T}^{\mathcal{G}}$ *is at most* $v + \mathsf{negl}(\lambda)$. Suppose for the sake of contradiction that the classical value of $\mathcal{T}^{\mathcal{G}}$ is $v' = v + \delta$ for a non-negligible $\delta = \delta(\lambda)$. This implies that there exists a (deterministic) poly-size classical prover $\tilde{\mathcal{P}}$ such that for every $\lambda \in \mathbb{N}$,

$$\Pr\left[(\tilde{\mathcal{P}}, \mathcal{V}(\mathcal{T}^{\mathcal{G}}))(1^\lambda) = 1\right] = v',$$

where $\mathcal{V}(\mathcal{T}^{\mathcal{G}})$ denotes the verifier in the protocol $\mathcal{T}^{\mathcal{G}}$. Next, for every $\lambda \in \mathbb{N}$ we convert $\tilde{\mathcal{P}}$ into (local) classical provers $(\mathcal{P}_1, \mathcal{P}_2) = (\mathcal{P}_1(\lambda), \mathcal{P}_2(\lambda))$ such that there exists a negligible function μ such that for every $\lambda \in \mathbb{N}$,

$$\Pr[(\mathcal{P}_1, \mathcal{P}_2, \mathcal{V}) = 1] \geq v' - \mu(\lambda).$$

Since $v' - \mu(\lambda) > v$ for sufficiently large λ, this contradicts the fact that the classical value of $\mathcal{G}$ is at most v.

To that end, for every $i \in \{1, 2\}$ we denote by Q_i the residual distribution of Q corresponding to player $\mathcal{P}_i$. Namely, Q_i samples $(q_1, q_2) \leftarrow Q$ and outputs q_i. Similarly, we denote by $Q|q_1$ to be the distribution that samples $(q_1', q_2') \leftarrow Q$ conditioned on $q_1' = q_1$, and outputs q_2'.

We next define $(\mathcal{P}_1, \mathcal{P}_2)$:

(1) Choose $q_1' \leftarrow Q_1$ and generate $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$. Let $\mathsf{ct}_1 \leftarrow \mathsf{Enc}(\mathsf{sk}, q_1')$ and $\mathsf{ct}_2 = \tilde{\mathcal{P}}(\mathsf{ct}_1)$ (i.e., ct_2 is the first message sent by $\tilde{\mathcal{P}}$ upon receiving ct_1 from the verifier).
(2) $\mathcal{P}_2$ has the ciphertexts $(\mathsf{ct}_1, \mathsf{ct}_2)$ hardwired into it. On input q_2, it simply emulates the response of $\tilde{\mathcal{P}}$ given the first three messages $(\mathsf{ct}_1, \mathsf{ct}_2, q_2)$ to obtain a_2. It outputs a_2.
(3) $\mathcal{P}_1$ also has $(\mathsf{ct}_1, \mathsf{ct}_2)$ hardwired into it. On input q_1, it computes and outputs a_1 that maximizes the probability of the verifier accepting (w.r.t. $\mathcal{P}_2$ defined above). Namely, it outputs

$$a_1 = \arg\max_{a_1} \Pr_{q_2 \leftarrow Q|q_1}[\mathcal{V}(q_1, q_2, a_1, \mathcal{P}_2(q_2)) = 1].$$

We next argue that there exists a negligible function $\mu = \mu(\lambda)$ such that for every $\lambda \in \mathbb{N}$,

$$\Pr[(\mathcal{P}_1(\lambda), \mathcal{P}_2(\lambda), \mathcal{V}) = 1] \geq v' - \mu(\lambda),$$

as desired. To this end, suppose for the sake of contradiction that there exists a non-negligible $\epsilon = \epsilon(\lambda)$ such that for every $\lambda \in \mathbb{N}$,

$$\Pr[(\mathcal{P}_1(\lambda), \mathcal{P}_2(\lambda), \mathcal{V}) = 1] \leq v' - \epsilon(\lambda). \tag{1}$$

We construct an adversary $\mathcal{A}$ of size $2^{|q_1|+|a_1|} \cdot \mathsf{poly}(\lambda/\epsilon)$ that breaks the semantic security of the underlying encryption scheme with advantage $\frac{\epsilon}{4}$.

The adversary $\mathcal{A}$ will use his challenge ciphertext ct to define $\mathcal{P}_1$ and $\mathcal{P}_2$, and will use $\mathcal{P}_1$ and $\mathcal{P}_2$ in his attack. Note that $\mathcal{P}_2$ can be efficiently emulated in time $\mathsf{poly}(\lambda)$ (assuming λ is larger than the communication complexity of $\mathcal{G}$). However, $\mathcal{P}_1$ may not be efficient. In what follows we show that the maximization problem implicit in $\mathcal{P}_1$ can be *approximated* in (non-uniform) time $2^{|q_1|+|a_1|} \cdot \mathsf{poly}(\lambda/\epsilon)$. More specifically, we show that there exists a function F, that takes as input a ciphertext ct and a query $q_1 \in \mathsf{Support}(Q_1)$, it runs in time $2^{|a_1|+|q_1|} \cdot \mathsf{poly}(\frac{\lambda}{\epsilon})$, and for every $q_1 \in \mathsf{Support}(Q_1)$,

$$\begin{aligned}&\Pr_{q_2 \leftarrow Q|q_1}[\mathcal{V}(q_1, q_2, \mathcal{P}_1(q_1), \mathcal{P}_2(q_2)) = 1] \\ &- \Pr_{q_2 \leftarrow Q|q_1}[\mathcal{V}(q_1, q_2, F(\mathsf{ct}, q_1), \mathcal{P}_2(q_2)) = 1] \leq \frac{\epsilon}{2},\end{aligned} \tag{2}$$

where $\mathcal{P}_1, \mathcal{P}_2$ are defined w.r.t. the ciphertext ct.

In what follows, we describe F as having randomized advice, but we will later set its advice to be "the best possible", and thus obtain a deterministic function. For every possible $q_1 \in \mathsf{Support}(Q_1)$, we hardwire $N = \frac{9(\lambda+|a_1|)}{\epsilon^2}$ queries $q_{2,1}, \ldots, q_{2,N}$ sampled independently from the distribution $Q|q_1$.

$F(\mathsf{ct}, q_1)$ is computed by approximating for every a_1 the probability

$$p_{q_1,a_1} = \Pr_{q_2 \leftarrow Q|q_1}[\mathcal{V}(q_1, q_2, a_1, \mathcal{P}_2(q_2)) = 1]$$

by its empirical value

$$p'_{q_1,a_1} = \frac{1}{N}|\{i : \mathcal{V}(q_1, q_{2,i}, a_1, \mathcal{P}_2(q_{2,i}) = 1\}|.$$

It outputs a_1 with the maximal value of p'_{q_1,a_1}.

Note that (as a circuit) F is of size $2^{|q_1|+|a_1|} \cdot \mathsf{poly}(\lambda)$, since it has hardwired into it $N \cdot 2^{|q_1|}$ queries hardwired (N for each possible q_1), and on input (ct, q_1) it runs in time $2^{|a_1|} \cdot N \cdot \mathsf{poly}(\lambda)$. Thus, its total size is as desired.

By a Chernoff bound, (The form of Chernoff bound that we use here is that for $X_1, \ldots, X_N$ identically and independently distributed in $\{0, 1\}$ with expectation μ, it holds that $\Pr\left[|\frac{1}{N}\sum_{i=1}^N X_i - \mu| > \delta\right] \leq 2^{-2N\delta^2}$.)

$$\Pr\left[|p'_{q_1,a_1} - p_{q_1,a_1}| > \frac{\epsilon}{3}\right] \leq 2^{-2N(\epsilon/3)^2} = 2^{-\lambda} \cdot 2^{-|a_1|}$$

From the equation above (and applying a union bound over all a_1) indeed the difference between the two probabilities in Equation (2) is at most $\frac{\epsilon}{3} + 2^{-\lambda} \le \frac{\epsilon}{2}$, as desired.

We are now ready to define our adversary $\mathcal{A}$ that will use (F, P_2) to break semantic security. Specifically, $\mathcal{A}$ takes as input a tuple $(q_{1,0}, q_{2,0}, q_{1,1}, q_{2,1}, \mathrm{ct})$, where $(q_{1,0}, q_{2,0}), (q_{1,1}, q_{2,1}) \leftarrow \mathcal{Q}$, and ct is distributed by choosing $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$ and $b^* \leftarrow \{0,1\}$, and sampling $\mathrm{ct} \leftarrow \mathsf{Enc}(\mathsf{sk}, q_{1,b^*})$. It guesses b^* as follows:

(1) For every $b \in \{0,1\}$, run $F(\mathrm{ct}, q_{1,b})$ in time $2^{|q_1|+|a_1|} \cdot \mathrm{poly}(\lambda/\epsilon)$ and compute $a_{1,b} = F(\mathrm{ct}, q_{1,b})$.
(2) If there exists $b \in \{0,1\}$ such that $\mathcal{V}(q_{1,b}, q_{2,b}, a_{1,b}, \mathcal{P}_2(q_{2,b})) = 1$ and $\mathcal{V}(q_{1,1-b}, q_{2,1-b}, a_{1,1-b}, \mathcal{P}_2(q_{2,1-b})) = 0$, then output b. Else output a random $b \leftarrow \{0,1\}$.

Note that by definition of $\tilde{\mathcal{P}}$ and $(\mathcal{P}_1, \mathcal{P}_2)$, it holds that for $b = b^*$,

$$\Pr_{(q_{1,b}, q_{2,b}) \leftarrow \mathcal{Q}}[\mathcal{V}(q_{1,b}, q_{2,b}, \mathcal{P}_1(q_{1,b}), \mathcal{P}_2(q_{2,b})) = 1] \ge v'.$$

Thus, by Equation (2), it holds that for $b = b^*$,

$$\Pr_{(q_{1,b}, q_{2,b}) \leftarrow \mathcal{Q}}[\mathcal{V}(q_{1,b}, q_{2,b}, F(\mathrm{ct}, q_{1,b}), \mathcal{P}_2(q_{2,b})) = 1] \ge v' - \frac{\epsilon}{2}. \quad (3)$$

On the other hand, by our contradiction assumption (Equation (1)), again making use of Equation (2), it holds that for $b = 1 - b^*$,

$$\Pr_{(q_{1,b}, q_{2,b}) \leftarrow \mathcal{Q}}[\mathcal{V}(q_{1,b}, q_{2,b}, F(\mathrm{ct}, q_{1,b}), \mathcal{P}_2(q_{2,b})) = 1] \le v' - \frac{3\epsilon}{4}. \quad (4)$$

Denote by E_{Good} the event that both

$$\mathcal{V}(q_{1,b}, q_{2,b}, F(\mathrm{ct}, q_{1,b}), \mathcal{P}_2(q_{2,b})) = 1 \text{ for } b = b^*$$
$$\mathcal{V}(q_{1,b}, q_{2,b}, F(\mathrm{ct}, q_{1,b}), \mathcal{P}_2(q_{2,b})) = 0 \text{ for } b = 1 - b^*$$

Similarly, denote by E_{Bad} the event that both

$$\mathcal{V}(q_{1,b}, q_{2,b}, F(\mathrm{ct}, q_{1,b}), \mathcal{P}_2(q_{2,b})) = 0 \text{ for } b = b^*$$
$$\mathcal{V}(q_{1,b}, q_{2,b}, F(\mathrm{ct}, q_{1,b}), \mathcal{P}_2(q_{2,b})) = 1 \text{ for } b = 1 - b^*$$

Denote by E the event that

$$\mathcal{V}(q_{1,b}, q_{2,b}, F(\mathrm{ct}, q_{1,b}), \mathcal{P}_2(q_{2,b})) = 1 \; \forall b \in \{0,1\}$$

Then by Equation (3),

$$\Pr[E_{\mathrm{Good}}] + \Pr[E] \ge v' - \frac{\epsilon}{2},$$

and by Equation (4),

$$\Pr[E_{\mathrm{Bad}}] + \Pr[E] \le v' - \frac{3\epsilon}{4},$$

which together imply that

$$\Pr[E_{\mathrm{Good}}] - \Pr[E_{\mathrm{Bad}}] \ge \frac{\epsilon}{4}. \quad (5)$$

Thus we have

$$\begin{aligned}\Pr\left[b = b^*\right] &\ge \frac{1}{2} \cdot (1 - \Pr[E_{\mathrm{Good}} \cup E_{\mathrm{Bad}}]) + \Pr[E_{\mathrm{Good}}] \\ &\ge \frac{1}{2} + \frac{1}{2}(\Pr[E_{\mathrm{Good}}] - \Pr[E_{\mathrm{Bad}}]) \\ &= \frac{1}{2} + \frac{\epsilon}{8},\end{aligned}$$

as desired, where the first equation follows from the definition of E_{Good} and E_{Bad} and the definition of $\mathcal{A}$, the second equation follows from the union bound, the third equation follows from Equation (5). This contradicts the security of QHE; thus, we conclude the desired bound on the classical CS value of $\mathcal{T}^{\mathcal{G}}$. □

3.2 Extension to k-Player Games

In this section, we generalize Theorem 3.2 to k-player games for $k > 2$. We begin with a construction that is a $2k$-round analogue of the transformation $\mathcal{T}$ from Theorem 3.2: given any k-player non-local game $\mathcal{G}$, we define the following interactive game $\mathcal{T}^{\mathcal{G}}$:

(1) The verifier samples $(q_1, \ldots, q_k) \leftarrow \mathcal{Q}$, $\mathsf{sk}_1, \ldots, \mathsf{sk}_{k-1} \leftarrow \mathsf{Gen}(1^\lambda)$, and $\hat{q}_i \leftarrow \mathsf{Enc}(\mathsf{sk}_i, q_i)$ for each $1 \le i \le k-1$.
(2) For each $1 \le i \le k-1$, in round $2i - 1$ the verifier sends $\hat{q}_i$. In round $2i$ the prover responds with a ciphertext $\hat{a}_i$.
(3) In round $2k - 1$ the verifier sends q_k; in round $2k$ the prover responds with some string a_k.
(4) The verifier decrypts each $\hat{a}_i$ with sk_i and accepts if and only if the transcript $(q_1, a_1, \ldots, q_k, a_k)$ is accepting according to $\mathcal{G}$.

We prove the following theorem.

Theorem 3.3. *Fix any* QHE *scheme (satisfying correctness with respect to auxiliary inputs) for a circuit class C, and any k-player non-local game $\mathcal{G} = (\mathcal{Q}, \mathcal{V})$ with classical value v and quantum value v^*, such that the value v^* is obtained by a prover strategy $(C_1^*, \ldots, C_k^*)$ with a quantum state $|\Psi\rangle \in \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_k$ with each $C_i^* \in C$ (except possibly C_k^*). Denote by $|q_i|$ and $|a_i|$ the lengths of the query and answer of P_i, respectively. If the underlying* QHE *encryption scheme is T-secure, for $T(\lambda) = 2^{\sum_{i=1}^{k-1}(|q_i|+|a_i|)} \cdot \mathrm{poly}(\lambda)$, then the following holds:*

(1) *The quantum* CS *value of $\mathcal{T}^{\mathcal{G}}$ is at least v^*.*
(2) *The classical* CS *value of $\mathcal{T}^{\mathcal{G}}$ is at most $v + \mathsf{negl}(\lambda)$.*

Proof. We briefly sketch the quantum CS value of $\mathcal{T}^{\mathcal{G}}$. Given a k-tuple of entangled provers $\mathcal{P}_1, \ldots \mathcal{P}_k$ (with shared state $|\Psi\rangle$), we define the following prover $\mathcal{P}$ for the interactive game:

- $\mathcal{P}$ initially has internal state $|\Psi\rangle_{\mathcal{A}_1, \ldots, \mathcal{A}_k}$.
- Given $\hat{q}_i$ (for each $1 \le i \le k-1$), $\mathcal{P}$ homomorphically evaluates the circuit defining $\mathcal{P}_i$ on register $\mathcal{A}_i$ and $\hat{q}_i$ (tracing out any ancilla registers). $\mathcal{P}$ sends the encrypted answer $\hat{a}_i$ to the verifier.
- Given q_k, $\mathcal{P}$ evaluates the circuit defining $\mathcal{P}_k$ on $\mathcal{A}_k$ (and q_k), and sends the answer a_k to the verifier.

Analogously to Theorem 3.2, the aux-input correctness of QHE implies that the verifier will accept with probability $v^*(\mathcal{P}_1, \ldots, \mathcal{P}_k) \pm \mathsf{negl}(\lambda)$, where $v^*(\mathcal{P}_1, \ldots, \mathcal{P}_k, |\Psi\rangle)$ denotes the value of strategy $(\mathcal{P}_1, \ldots, \mathcal{P}_k, |\Psi\rangle)$. In more detail, we invoke aux-input correctness and the contractivity of trace distance $k-1$ times sequentially (starting with auxiliary registers $(\mathcal{A}_2, \ldots, \mathcal{A}_k)$ and removing one $\mathcal{A}_i$ each time).

We now bound the classical value of $\mathcal{T}^{\mathcal{G}}$ via the following argument. Suppose that a (computationally bounded) classical interactive prover $\widetilde{\mathcal{P}}$ (deterministic without loss of generality) has value v' in $\mathcal{T}^{\mathcal{G}}$. We will construct local provers $(P_1^*, \ldots, P_k^*)$ winning $\mathcal{G}$ with probability at least $v' - \mathsf{negl}(\lambda)$.

To this end, we sample $(q_1', \ldots, q_k') \leftarrow \mathcal{Q}$, secret keys $\mathsf{sk}_1', \ldots, \mathsf{sk}_{k-1}' \leftarrow \mathsf{Gen}(1^\lambda)$ and $\mathrm{ct}_i' \leftarrow \mathsf{Enc}(\mathsf{sk}_i', q_i')$ for $1 \le i \le k-1$. Each prover P_i^* has $\mathrm{ct}_1', \ldots, \mathrm{ct}_i'$ hardwired into its description. The prover

P_k^* simply emulates the last message function of $\widetilde{P}$; namely, upon receiving q_k it emulates $\widetilde{P}$ assuming that the first $k-1$ messages from the verifier were $\mathsf{ct}'_1, \dots, \mathsf{ct}'_{k-1}$. We next define $P_1^*, \dots, P_{k-1}^*$ recursively starting with P_1^*.

Assuming we have already defined $P_1^*, \dots, P_{\ell-1}^*$ (this includes the base case $\ell = 1$), we define P_ℓ^* and an *interactive* prover $\widetilde{P}_{\ell+1,\dots,k}$ that has $\mathsf{ct}'_1, \dots, \mathsf{ct}'_\ell$ hardwired to its description, and is sequentially given $\hat{q}_{\ell+1}, \dots, \hat{q}_{k-1}, q_k$ as inputs and returns $\hat{a}_{\ell+1}, \dots, \hat{a}_{k-1}, a_k$ as outputs.

- $\widetilde{P}_{\ell+1,\dots,k}$ simply emulates $\widetilde{P}$ using hard-coded $\mathsf{ct}'_1, \dots, \mathsf{ct}'_\ell$.
- P_ℓ^* is given as input q_ℓ and outputs an optimum of the following maximization problem:

$$a_\ell^* = \arg\max_{a_\ell} \Pr_{\{q_j\}_{j\neq\ell} \leftarrow Q|q_\ell} [\mathcal{V}(q_1, a_1, \dots q_k, a_k) = 1],$$

  where $a_j = P_j^*(q_j)$ for all $j < \ell$, and for all $j > \ell$, a_j is obtained by running $\widetilde{P}_{\ell+1,\dots,k}$ on encryptions (under fresh secret keys) of $q_{\ell+1}, \dots, q_k$ and then (unless $j = k$) decrypting the resulting answers.

Note that by construction, $P_k^* = \widetilde{P}_k$, and $P_1^*, \dots, P_k^*$ are indeed local. Moreover, just as in the proof of Theorem 3.2, we can *approximately* solve the maximization problems defined in $P_1^*, \dots P_{k-1}^*$ with functions $F_1, \dots, F_{k-1}$ that can be implemented in time $2^{\sum_{i=1}^{k-1} |q_i| + |a_i|} \cdot \mathsf{poly}(\lambda)$. This is done, given an inverse polynomial error ϵ, by hard-coding for each q_i, $N = \frac{18k^2(\lambda + |a_i|)}{\epsilon^2}$ samples $\{q_j^{(\ell)}\}_{j\neq k}$ (for $1 \le \ell \le N$) from $Q|_{q_i}$, and will result in provers $F_1, \dots, F_{k-1}, P_k^*$ that attain value matching $P_1^*, \dots, P_k^*$ up to error $\epsilon/4$.

Thus, to complete the proof of Theorem 3.3 it remains to prove the following claim.

Claim 3.4. *The tuple $(P_1^*, \dots, P_k^*)$ has success probability at least $v' - \mathsf{negl}(\lambda)$.*

Proof. Assume that $(P_1^*, \dots, P_k^*)$ has success probability at most $v' - \epsilon$ for some non-negligible ϵ. We first replace P_i^* by F_i defined above, and obtain that $(F_1, \dots, F_k)$ has success probability at most $v' - 3\epsilon/4$. We now derive a contradiction by a hybrid argument. Specifically, for every j, we define the quantity

$$\mathsf{Hyb}_j = \Pr_{\substack{q_1,\dots,q_k \leftarrow Q \\ \text{for } i \le j:\ a_i = F_i(q_i) \\ \text{for } i > j:\ a_i = \mathrm{Dec}(\hat{a}_i), \\ \hat{a}_i \text{ output by } \widetilde{P}_{j+1,\dots,k}}} [\mathcal{V}(q_1, a_1, \dots, q_k, a_k) = 1]$$

Note that Hyb_0 is equal to the success probaiblity of $\widetilde{P}$, which is equal to v' by assumption, while Hyb_{k-1} is equal to the value of $(F_1, \dots, F_k)$.

We now claim that $\mathsf{Hyb}_j > \mathsf{Hyb}_{j-1} - \frac{\epsilon}{4k} - \mathsf{negl}(\lambda)$ for every j. To prove this, we will reduce from the security of QHE with respect to ciphertext ct'_j; note that $F_1, \dots, F_{j-1}$ do not depend on ct'_j. Ciphertexts $\mathsf{ct}'_1, \dots, \mathsf{ct}'_{j-1}$ will remain fixed for this entire argument, while $\mathsf{ct}'_{j+1}, \dots, \mathsf{ct}'_{k-1}$ are not used by any algorithms in Hyb_{j-1} or Hyb_j.

Define the auxiliary quantity Hyb'_j to be the same as Hyb_j, except that ct'_j is sampled as $\mathsf{Enc}(\mathsf{sk}'_j, q_j)$, where q_j is the input sent to F_j in the experiment. Note that $\mathsf{Hyb}'_j > \mathsf{Hyb}_{j-1} - \frac{\epsilon}{4k}$, because the particular choice of $a_j^* = \mathsf{Dec}(\widetilde{P}_{j,\dots,k}(\mathsf{ct}'_j))$ in the maximization problem defining P_j^* would have value Hyb_{j-1} (as this strategy matches the value of $(F_1, \dots, F_{j-1}, \widetilde{P}_{j,\dots,k})$), and F_j approximates the P_j^* maximization problem up to error $\frac{\epsilon}{4k}$.

Moreover, it holds that $\mathsf{Hyb}'_j - \mathsf{Hyb}_{j-1} = \mathsf{negl}(\lambda)$, or this would result in an efficient test distinguishing encryptions of q_j vs. encryptions of q'_j (by an analogous reduction as in the proof of Theorem 3.2).

Thus, by a hybrid argument, (As discussed in [17] (although context differs slightly here), a hybrid argument can be applied because the collection of indistinguishability claims $\mathsf{Hyb}'_j \approx \mathsf{Hyb}_{j-1}$ are proved via a universal reduction R from the security of QHE.) we conclude that $\mathsf{Hyb}_{k-1} > \mathsf{Hyb}_0 - \frac{\epsilon}{4} - \mathsf{negl}(\lambda) = v' - \frac{\epsilon}{4} - \mathsf{negl}(\lambda)$, contradicting our initial assumption. This completes the proof of the claim. □

This completes the proof of Theorem 3.3. □

4 PROTOCOLS FOR VERIFYING QUANTUM ADVANTAGE

In this section, we give a concrete instantiation of our framework and outline directions for future work, focusing on obtaining protocols with simple(r) quantum provers. We proceed to describe a concrete instantiation of our blueprint, using the CHSH game and the Mahadev QFHE scheme.

4.1 Compiling the CHSH Game

We first recall the CHSH game.

Definition 4.1 (The CHSH Game). *The CHSH game $\mathcal{G}_{\mathsf{CHSH}}$ consists of the uniform query distribution Q_{CHSH} over $(q_1, q_2) \in (\{0,1\})^2$ and verification predicate $\mathcal{V}_{\mathsf{CHSH}}(q_1, q_2, a_1, a_2)$ which is 1 if and only if*

$$a_1 \oplus a_2 = q_1 q_2 \pmod 2.$$

The classical value of this game is $v_{\mathsf{CHSH}} = 0.75$ and the quantum value is $v^*_{\mathsf{CHSH}} = \cos^2(\pi/8) \approx 0.85$. The optimal quantum strategy is as follows: The two players $\mathcal{A}, \mathcal{B}$ share an EPR pair

$$\frac{1}{\sqrt{2}}(|0\rangle_{\mathcal{A}} |0\rangle_{\mathcal{B}} + |1\rangle_{\mathcal{A}} |1\rangle_{\mathcal{B}})$$

where players $\mathcal{A}, \mathcal{B}$ have the $\mathcal{A}, \mathcal{B}$ registers respectively. Upon receiving q_1, player $\mathcal{A}$ measures her register $\mathcal{A}$ in the Hadamard $(\pi/4)$ basis if $q_1 = 0$, and in the standard basis if $q_1 = 1$, and reports the outcome $a_1 \in \{0,1\}$. Player $\mathcal{B}$ measures her register $\mathcal{B}$ in the $\pi/8$-basis if $q_2 = 0$ and in the $3\pi/8$-basis if $q_2 = 1$, and reports the outcome $a_2 \in \{0,1\}$.

By Theorem 3.2 and Claim 2.6, we have the following corollary:

Corollary 4.2. *Consider the [30] QHE scheme for poly-size circuits in the Toffoli and Clifford basis. Consider the CHSH game $\mathcal{G}_{\mathsf{CHSH}} = (Q_{\mathsf{CHSH}}, \mathcal{V}_{\mathsf{CHSH}})$ and quantum strategy in Definition 4.1 where*

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{\mathcal{A}} |0\rangle_{\mathcal{B}} + |1\rangle_{\mathcal{A}} |1\rangle_{\mathcal{B}})$$

and $C_1^*(|\Psi\rangle_{\mathcal{A}}, \cdot) \in C$.

The single-player computationally sound interactive game $\mathcal{T}^{\mathcal{G}}$ has:

- *quantum* CS *value* $\ge v^*_{\mathsf{CHSH}} - \mathsf{negl}(\lambda) \ge 0.85 - \mathsf{negl}(\lambda)$

- *classical* CS *value* $\leq v_{\mathrm{CHSH}} + \mathsf{negl}(\lambda) = 0.75 + \mathsf{negl}(\lambda)$.

Amplifying this gap can be done by sequential repetition. Alternatively, one can compile a parallel-repeated version of the CHSH game to get a protocol with a large gap between the quantum and classical CS values.

Prover Efficiency. The compilation of the CHSH game with Mahadev's QFHE (Corollary 4.2) results in a conceptually simple 4-round protocol with a relatively simple quantum prover. Here, we analyze the quantum prover's algorithm.

Returning to the quantum strategy for the CHSH game (Definition 4.1), player $\mathcal{A}$ applies a controlled Hadamard gate to $|\hat{q_1}\rangle\,|\Psi\rangle_{\mathcal{A}}$, and then measures the $\mathcal{A}$ register. This can be implemented by a circuit C_1^* containing Clifford gates and a single Toffoli gate [7]. Recall that in Mahadev's scheme ([30]), evaluating Clifford gates only requires applying the intended Clifford gate to a (Pauli one-time-padded) encryption of the underlying state. To evaluate a Toffoli gate, the Toffoli gate is applied to the encrypted qubit, followed by 3 "encrypted CNOT" operations and 2 Hadamard gates. The bulk of the computational cost of the prover is in the encrypted CNOT operations. Using the trapdoor claw-free functions (TCF) for the classical ciphertexts in the Mahadev QHE scheme, an encrypted CNOT operation consists of creating a uniform superposition over the TCF domain, evaluating the function in superposition, measurements and Clifford gates. That is, this requires $p(\lambda) := \log|\mathcal{D}| + \log|\mathcal{R}|$ ancilla qubits corresponding to the TCF domain $\mathcal{D}$ and range $\mathcal{R}$. Concretely, the prover's quantum operations in our compilation of CHSH are as follows.

- The prover creates an EPR pair which involves applying a Hadamard and a CNOT gate.
- The prover receives a classical ciphertext $\hat{q_1}$ from the verifier in round 1.
- The prover homomorphically evaluates $C_1^*(|\Psi\rangle_{\mathcal{A}}, q_1)$ (where C_1^* implements player $\mathcal{A}$'s strategy in CHSH). This uses the constant number of qubits in C_1^* and $3p(\lambda)$ ancilla qubits for TCF evaluations. All of its operations are Clifford gates except a single Toffoli gate and 3 invocations of the TCF evaluation algorithm run in superposition.
- The prover sends back a classical ciphertext, and receives a bit $q_2 \in \{0,1\}$ in round 2. It measures $|\Psi\rangle_{\mathcal{B}}$ in the $\pi/8$ or $3\pi/8$ basis (depending on q_2, as per player $\mathcal{B}$'s strategy in CHSH). It sends back the result as $a_2 \in \{0,1\}$. In particular, the prover can discard the remaining qubits right after it computes and sends its message in round 1.

Overall, the prover uses $3p(\lambda) + O(1)$ qubits, and the complexity of its operations is dominated by the 3 TCF evaluations. We note that designing a more efficient QHE scheme supporting the controlled-Hadamard gate, potentially based on simpler assumptions, is an attractive route to improving the prover efficiency.

4.2 Future Directions

Our work suggests several intriguing directions for future research.

Analyzing quantum soundness. In this work, we prove that (1) the classical value of our cryptographically compiled game is at most the classical value of the original non-local game, and (2) the quantum value of the compiled game is at least the entangled value of the non-local game, which is sufficient to establish quantum advantage. However, we do not *upper bound* the quantum value of the compiled game. Is the quantum value always *at most* the entangled value of the non-local game (up to negligible factors)? Such a general result would have powerful implications: for example, [35] gives an efficient-prover entangled MIP for deciding all BQP (and QMA) languages, which would immediately be compiled into a single-prover delegation scheme.

Protocols for quantum advantage with very simple quantum provers? The honest quantum prover in our protocol has a simple and natural structure: for a fixed non-local game, first homomorphically evaluate the P_1 strategy on an encrypted question $\mathsf{Enc}(q_1)$, and then (in the clear) evaluate the P_2 strategy on a question q_2. In particular, the second prover message can be computed using only a constant-size quantum state and prover unitary (for a constant-size game). Can we build a protocol where the *entire* honest prover strategy is extremely efficient?

Simpler homomorphic encryption schemes. Can we design better somewhat homomorphic encryption schemes for the compilation in Theorem 3.2? We note that the scheme only needs to support the evaluation of *one* of the two provers' strategies in the non-local game, which can often be implemented by a simple circuit. For example, designing a scheme that simply supports the controlled-Hadamard gate would suffice for compiling the CHSH game. This may give a quantum advantage protocol with a simpler prover strategy.

Protocols based on different assumptions. We note that for quantum advantage, we only need soundness against classical adversaries. Namely, the homomorphic encryption should have completeness for some quantum gates, but *only needs security against classical polynomial-time adversaries*. This opens the door to designing QHEs based on e.g. discrete log-style assumptions, or the hardness of factoring, rather than learning with errors. (Indeed, quantum advantage protocols have been constructed using factoring-based TCFs; see [24]).

Understanding existing protocols. The existing interactive protocols for quantum advantage (to our knowledge, [12, 13, 24]) are presented as an all-in-one package. Intuitively, a protocol testing quantumness should have a component testing for quantum resources, e.g. a test of entanglement, and a component that tests computational power, i.e. the cryptography. Can existing protocols be disentangled to two such components? A starting point is [24] which has some resemblance to our CHSH compilation in Section 4.1, although it does incur two more rounds.

More ambitiously, could we understand any single-prover quantum advantage protocol as compiling a (perhaps contrived) k-player non-local game via a somewhat homomorphic encryption scheme? We leave it open to understand the reach and the universality of our framework for constructing protocols for quantum advantage.

ACKNOWLEDGEMENTS

We thank the anonymous STOC reviewers for their helpful feedback. We thank Fermi Ma for comments on earlier drafts of this paper, and Dorit Aharonov for a helpful discussion regarding the prover complexity in non-local games.

This research was conducted while AL was at MIT, where he was supported by a Charles M. Vest Grand Challenges Fellowship, an NDSEG Fellowship, and grants of VV. VV is supported in part by DARPA under Agreement No.
HR00112020023, a grant from the MIT-IBM Watson AI, a grant from Analog Devices and a Microsoft Trustworthy AI grant. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Government or DARPA. LY is supported by an NSF Graduate Research Fellowship and grants of VV.

REFERENCES

[1] 2022. Press release: The Nobel Prize in Physics 2022. https://www.nobelprize.org/prizes/physics/2022/press-release/ 2
[2] Scott Aaronson and Alex Arkhipov. 2010. The Computational Complexity of Linear Optics. arXiv:1011.3245 [quant-ph] 1
[3] Dorit Aharonov, Michael Ben-Or, and Elad Eban. 2008. Interactive Proofs For Quantum Computations. arXiv:0810.5375 [quant-ph] 1
[4] P.K. Aravind. 2001. Bell's theorem without inequalities and only two distant observers, In Optical Fiber Communication Conference and International Conference on Quantum Information. *Optical Fiber Communication Conference and International Conference on Quantum Information*, EAPA7. https://doi.org/10.1364/ICQI.2001.EAPA7 2
[5] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando Brandao, David Buell, Brian Burkett, Yu Chen, Jimmy Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fowler, Craig Michael Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew Harrigan, Michael Hartmann, Alan Ho, Markus Rudolf Hoffmann, Trent Huang, Travis Humble, Sergei Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, Dave Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandrà, Jarrod Ryan McClean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Ostby, Andre Petukhov, John Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin Jeffery Sung, Matt Trevithick, Amit Vainsencher, Benjamin Villalonga, Ted White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, and John Martinis. 2019. Quantum Supremacy using a Programmable Superconducting Processor. *Nature* 574 (2019), 505–510. https://www.nature.com/articles/s41586-019-1666-5 1
[6] 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 2
[7] Debajyoti Bera, Stephen Fenner, Frederic Green, and Steve Homer. 2008. Universal Quantum Circuits. arXiv:0804.2429 [cs.CC] 10
[8] Ingrid Biehl, Bernd Meyer, and Susanne Wetzel. 1998. Ensuring the integrity of agent - based computations by short proofs. In *Mobile Agents - Second International Workshop, MA'98, Proceedings (Lecture Notes in Computer Science)*. Springer, 183–194. 2nd International Workshop on Mobile Agents, MA'98 ; Conference date: 09-09-1998 Through 11-09-1998. 3
[9] Nir Bitansky and Alessandro Chiesa. 2012. Succinct Arguments from Multi-prover Interactive Proofs and Their Efficiency Benefits. In *CRYPTO 2012 (LNCS, Vol. 7417)*, Reihaneh Safavi-Naini and Ran Canetti (Eds.). Springer, Heidelberg, 255–272. https://doi.org/10.1007/978-3-642-32009-5_16 3
[10] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. 2018. On the complexity and verification of quantum random circuit sampling. *Nature Physics* 15, 2 (Oct 2018), 159–163. https://doi.org/10.1038/s41567-018-0318-2 1
[11] 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 (Lecture Notes in Computer Science, Vol. 10993)*, Hovav Shacham and Alexandra Boldyreva (Eds.). Springer, 67–95. https://doi.org/10.1007/978-3-319-96878-0_3 2, 3, 5, 6
[12] Zvika Brakerski, Paul F. Christiano, Urmila Mahadev, Umesh V. Vazirani, and Thomas Vidick. 2018. A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device. In *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, Mikkel Thorup (Ed.). IEEE Computer Society, 320–331. https://doi.org/10.1109/FOCS.2018.00038 1, 2, 10
[13] Zvika Brakerski, Venkata Koppula, Umesh V. Vazirani, and Thomas Vidick. 2020. Simpler Proofs of Quantumness. In *15th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2020, June 9-12, 2020, Riga, Latvia (LIPIcs, Vol. 158)*, Steven T. Flammia (Ed.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 8:1–8:14. https://doi.org/10.4230/LIPIcs.TQC.2020.8 2, 10
[14] Michael J. Bremner, Richard Jozsa, and Dan J. Shepherd. 2010. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 467, 2126 (Aug 2010), 459–472. https://doi.org/10.1098/rspa.2010.0301 1
[15] Anne Broadbent and Stacey Jeffery. 2015. Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity. In *CRYPTO 2015, Part II (LNCS, Vol. 9216)*, Rosario Gennaro and Matthew J. B. Robshaw (Eds.). Springer, Heidelberg, 609–629. https://doi.org/10.1007/978-3-662-48000-7_30 3
[16] 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 2, 3
[17] Marc Fischlin and Arno Mittelbach. 2021. An Overview of the Hybrid Argument. Cryptology ePrint Archive, Report 2021/088. https://eprint.iacr.org/2021/088. 9
[18] Joseph F. Fitzsimons and Elham Kashefi. 2017. Unconditionally verifiable blind quantum computation. *Physical Review A* 96, 1 (Jul 2017). https://doi.org/10.1103/physreva.96.012303 1
[19] Craig Gidney and Martin Ekerå. 2021. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum* 5 (Apr 2021), 433. https://doi.org/10.22331/q-2021-04-15-433 1
[20] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. 2007. Going Beyond Bell's Theorem. arXiv:0712.0921 [quant-ph] 2
[21] Lucien Hardy. 1993. Nonlocality for two particles without inequalities for almost all entangled states. *Phys. Rev. Lett.* 71 (Sep 1993), 1665–1668. Issue 11. https://doi.org/10.1103/PhysRevLett.71.1665 2
[22] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. 2015. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* 526, 7575 (2015), 682–686. https://doi.org/10.1038/nature15759 2
[23] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. 2020. MIP*=RE. arXiv:2001.04383 [quant-ph] 2
[24] Gregory D. Kahanamoku-Meyer, Soonwon Choi, Umesh V. Vazirani, and Norman Y. Yao. 2021. Classically-Verifiable Quantum Advantage from a Computational Bell Test. *CoRR* abs/2104.00687 (2021). arXiv:2104.00687 https://arxiv.org/abs/2104.00687 2, 10
[25] Yael Tauman Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. 2022. Quantum Advantage from Any Non-Local Game. Cryptology ePrint Archive, Report 2022/400. https://eprint.iacr.org/2022/400. 1
[26] Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. 2013. Delegation for bounded space. In *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, Dan Boneh, Tim Roughgarden, and Joan Feigenbaum (Eds.). ACM, 565–574. https://doi.org/10.1145/2488608.2488679 3
[27] Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. 2014. How to delegate computations: the power of no-signaling proofs. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, David B. Shmoys (Ed.). ACM, 485–494. https://doi.org/10.1145/2591796.2591809 3
[28] Arjen K. Lenstra, Hendrik W. Lenstra Jr., Mark S. Manasse, and John M. Pollard. 1990. The Number Field Sieve. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*, Harriet Ortiz (Ed.). ACM, 564–572. https://doi.org/10.1145/100216.100295 1
[29] Yong (Alexander) Liu, Xin (Lucy) Liu, Fang (Nancy) Li, Haohuan Fu, Yuling Yang, Jiawei Song, Pengpeng Zhao, Zhen Wang, Dajia Peng, Huarong Chen, Chu Guo, Heliang Huang, Wenzhao Wu, and Dexun Chen. 2021. Closing the "quantum supremacy" gap. *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis* (Nov 2021). https://doi.org/10.1145/3458817.3487399 1
[30] Urmila Mahadev. 2018. Classical Homomorphic Encryption for Quantum Circuits. In *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, Mikkel Thorup (Ed.). IEEE Computer Society, 332–338. https://doi.org/10.1109/FOCS.2018.00039 2, 3, 5, 6, 9, 10
[31] Urmila Mahadev. 2018. Classical Verification of Quantum Computations. In *59th FOCS*, Mikkel Thorup (Ed.). IEEE Computer Society Press, 259–267. https://doi.org/10.1109/FOCS.2018.00033 2
[32] N. David Mermin. 1990. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.* 65 (Dec 1990), 3373–3376. Issue 27. https://doi.org/10.1103/PhysRevLett.65.3373 2
[33] Tony Metger and Thomas Vidick. 2021. Self-testing of a single quantum device under computational assumptions. *Quantum* 5 (Sep 2021), 544. https://doi.org/10.22331/q-2021-09-16-544 2
[34] Michael A. Nielsen and Isaac L. Chuang. 2000. *Quantum Computation and Quantum Information*. Cambridge University Press. 5

[35] Ben W Reichardt, Falk Unger, and Umesh Vazirani. 2013. Classical command of quantum systems. *Nature* 496, 7446 (2013), 456–460. 2, 10

[36] Peter W. Shor. 1997. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* 26, 5 (1997), 1484–1509. https://doi.org/10.1137/S0097539795293172 1

[37] Takashi Yamakawa and Mark Zhandry. 2022. Verifiable Quantum Advantage without Structure. *IACR Cryptol. ePrint Arch.* (2022), 434. https://eprint.iacr.org/2022/434 2

[38] Daiwei Zhu, Gregory D. Kahanamoku-Meyer, Laura Lewis, Crystal Noel, Or Katz, Bahaa Harraz, Qingfeng Wang, Andrew Risinger, Lei Feng, Debopriyo Biswas, Laird Egan, Alexandru Gheorghiu, Yunseong Nam, Thomas Vidick, Umesh Vazirani, Norman Y. Yao, Marko Cetina, and Christopher Monroe. 2021. Interactive Protocols for Classically-Verifiable Quantum Advantage. arXiv:2112.05156 [quant-ph] 2

Received 2022-11-07; accepted 2023-02-06