Self-Testing in the Compiled Setting via Tilted-CHSH Inequalities

Arthur Mehta
Department of Mathematics and Statistics, University of Ottawa, Canada

Connor Paddock
Department of Mathematics and Statistics, University of Ottawa, Canada

Lewis Wooltorton
Department of Mathematics, University of York, UK
Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory and Department of Electrical & Electronic Engineering, University of Bristol, UK
Inria, ENS de Lyon, LIP, France

Abstract

This work investigates the family of extended tilted-CHSH inequalities in the single-prover cryptographic compiled setting. In particular, we show that a quantum polynomial-time prover can violate these Bell inequalities by at most negligibly more than the violation achieved by two non-communicating quantum provers. To obtain this result, we extend a sum-of-squares technique to monomials with arbitrarily high degree in the Bob operators and degree at most one in the Alice operators. We also introduce a notion of partial self-testing for the compiled setting, which resembles a weaker form of self-testing in the bipartite setting. As opposed to certifying the full model, partial self-testing attempts to certify the reduced states and measurements on separate subsystems. In the compiled setting, this is akin to the states after the first round of interaction and measurements made on that state. Lastly, we show that the extended tilted-CHSH inequalities satisfy this notion of a compiled self-test.

2012 ACM Subject Classification Theory of computation → Computational complexity and cryptography

Keywords and phrases Compiled Bell scenarios, self-testing

Digital Object Identifier 10.4230/LIPIcs.TQC.2025.8

Related Version *Full Version*: https://arxiv.org/abs/2406.04986 [24]

Funding *Arthur Mehta*: NSERC Alliance Consortia Quantum grants, reference number: ALLRP 578455 – 22 and the NSERC Discovery Grants Program.
Connor Paddock: Digital Horizon Europe project FoQaCiA, Foundations of quantum computational advantage, grant no. 101070558, and the Natural Sciences and Engineering Research Council of Canada (NSERC).
Lewis Wooltorton: Engineering and Physical Sciences Research Council (EPSRC Grant No. EP/SO23607/1) and the European Union's Horizon Europe research and innovation programme under the project "Quantum Security Networks Partnership" (QSNP, grant agreement No. 101114043).

Acknowledgements The authors thank Simon Schmidt, Ivan Šupić, Anand Natarajan, and Tina Zhang for helpful discussions. We also thank the anonymous TQC reviewers for valuable feedback.

1 Introduction

In a bipartite Bell scenario, two non-communicating provers receive inputs x and y and reply with outputs a and b to a verifier. The collection of probabilities of observing outcomes (a, b) given (x, y) determines a correlation $\mathsf{p} = \{p(a, b|x, y)\}$. Bell's celebrated theorem implies that if the provers are permitted to share an entangled quantum state and make

local quantum measurements, called a bipartite (quantum) model, then certain correlations have no realization by a classical (or local hidden-variable) model [7]. The distinction between quantum and classical correlations is often explored through Bell inequalities. A Bell inequality is a linear inequality on the set of correlations which is satisfied by all classical correlations. Hence, these inequalities can be violated by certain models using quantum entanglement, realizing correlations that are not classical. The quantum value of a Bell inequality refers to the largest violation achievable by a bipartite (quantum) model. A prominent example is the Clauser-Horne-Shimony-Holt (CHSH) inequality, where the classical bound is 2, but the quantum value is $2\sqrt{2}$ [11].

Due to their ability to witness these non-classical effects, Bell inequality violations play a major role in areas like device-independent cryptography [1, 15, 30, 31, 33], protocols for verifiable delegated quantum computation [32, 17, 14], and in the study of multiprover interactive proofs (MIPs) and the variant MIP* with entangled provers [12], also called nonlocal games. Many of the key applications of Bell inequalities rely on a remarkable property known as *self-testing* [22, 23, 35, 34]. Informally, a Bell inequality is a self-test for an ideal bipartite (quantum) model Q if there exist local isometries which transform any employed bipartite model Q$'$ achieving maximum Bell violation into the ideal model Q. It is well-known that the CHSH inequality is a self-test for the bipartite model employing a maximally entangled state on two qubits, along with the Pauli σ_x and σ_z measurements, among others [22]. Another prominent example is the family of tilted-CHSH inequalities [2, 35, 4], which self-test partially entangled two-qubit states, and were integral in the work of Coladangelo, Goh, and Scarani who employed them as part of a protocol to self-test any pure bipartite entangled state [13].

Despite the enormous success of self-testing, a practical drawback is the requirement of multiple non-communicating quantum provers. Recently, a number of cryptographic approaches have been proposed that replace the non-communication assumption with computational assumptions [19, 26, 18]. This makes the setting more practical by having a single quantum prover, rather than multiple. One new and prominent approach is the Kalai-Lombardi-Vaikuntanathan-Yang (KLVY) compilation procedure introduced in [19], which transforms a 2-prover 1-round Bell scenario into a 1-prover 2-round scenario with a single computationally bounded prover. The core ingredient in the KLVY compilation procedure is quantum homomorphic encryption (QHE), which emulates, to a certain extent, the non-communication between the rounds of interaction. In the compiled game, the inputs to the prover happens sequentially. In the first round, the prover obtains an encryption χ of the input x from the verifier. Without breaking the security, the prover cannot distinguish between encryptions of different inputs. The prover performs a polynomial time quantum circuit on χ, and then returns an output α to the verifier. In the second round, the information about x has already been "hidden" from the prover, so the verifier can send input y in the plain (i.e. unencrypted) to the prover, upon which the prover can perform a measurement and return outcome b to the verifier. The verifier checks for a Bell inequality violation (across many such interactions) using the values of x, the decryption of α, along with (y, b). QHE has two key features that makes this resemble the bipartite setting. Firstly, it allows the first round quantum prover to perform measurements as they would have in the bipartite setting, without knowing the input. Secondly, the encryption ensures that no classical polynomial-time prover can violate a Bell inequality by more than an negligible amount (see Section 3 details). Both of these are non-trivial and were the subject of [19].

In a follow-up work, Natarajan and Zhang showed that the maximal quantum violation of the CHSH inequality in the compiled setting is bounded by the maximal violation in the bipartite setting, up to negligible factors in the security parameter [27]. Subsequent

works have analyzed the quantum soundness of the KLVY compilation procedure for other multiprover scenarious, including all 2-player XOR nonlocal games [16], Bell inequalities tailored to maximally entangled bipartite states [6], delegated quantum computation with a single-device [27, 25], and even in the study of contextuality [3]. Despite these advancements, many results have yet to be reproduced in the compiled setting. Our work takes another step in growing the list of protocols that will function as desired in the compiled setting.

Upper bounding compiled Bell violations

As mentioned, the compiled value of a Bell inequality is always at least the quantum value. This is because any bipartite (quantum) model can be implemented with homomorphic encryption via a *correctness* property of the QHE scheme used in the procedure. On the other hand, establishing upper bounds on the largest violation possible in the compiled setting is challenging, as general techniques for bounding these violations depend on the spatial separation between the two provers. Nonetheless, upper bounds on the violations of a certain Bell inequalities in the compiled setting can be verified using the sum-of-squares (SOS) technique [27, 16, 6]. The SOS approach is a powerful method and has been used extensively to upper bound Bell inequality violations and the values of nonlocal games in the bipartite setting. Informally, this technique relates the maximum compiled value η, of a Bell functional I, to a decomposition of the Bell operator or Bell polynomial S as a sum of Hermitian squares, $\eta\mathbb{I} - S = \sum_i P_i^\dagger P_i$. Before our work, progress was made on realizing this approach in the compiled setting, however, there were some limitations. In particular, it was required that the polynomials P_i involved in the decomposition were at most degree two in both Alice's and Bob's observables, restricting the technique to Bell inequalities with an SOS decomposition of this form; this excludes, for example, the family of tilted-CHSH inequalities.

Our first result extends the SOS technique to a larger family of Bell polynomials. More specifically, we extend the pseudo-expectation techniques in [27, 16] to allow for evaluations on polynomial terms P_i that consist of arbitrary monomials in the algebra generated by Bob's observables. In Theorem 3 we prove that an extended pseudo-expectation will be positive on the corresponding Hermitian square $P_i^\dagger P_i$ for any such term P_i. Consequently, we show that for any Bell inequality with an SOS decomposition in which P_i are of the form $P_i = \sum_j \gamma_j (A_x)^{k_j} w_j(B)$ for some $\gamma_j \in \mathbb{C}$, $k_j \in \{0, 1\}$ and $w_j(B)$ being arbitrary monomials in Bob's observables, η is an upper-bound on the maximum compiled quantum value. Our extension captures a wide class of Bell inequalities including tilted-CHSH, enabling us to bound the compiled value of the tilted-CHSH inequalities, by the quantum value and a negligible function of security parameter, see Theorem 5 for details.

A compiled self-testing result

Our second contribution is a concept of self-testing in the compiled setting. One of the main obstacles to deriving self-testing results in the compiled setting is the lack of techniques for extracting any algebraic relations on the measurement operators acting under the encryption. Nevertheless, it remains possible to derive relations on the observables in the second round. With this in mind, we consider a partial notion of self-testing that applies to the measurements made by the prover in the second round. In particular, our definition only requires the existence of an isometry robustly certifying the ideal post-measurement state after the first round, and the action of the measurements made in the second.

As our final result, we provide an example by showing violations of the compiled tilted-CHSH inequalities satisfy this notion of partial self-testing. This family of inequalities was introduced by Acín, Massar, and Pironio [2], and the Bell functionals take the form $\alpha_\theta\langle A_0\rangle + \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle$, where $\langle A_xB_y\rangle$, $\langle A_x\rangle$ denote the expectation of measurements corresponding to settings $X = x$, $Y = y$, and $\alpha_\theta \in \mathbb{R}$. Notably, they are tailored to robustly self-test the two qubit states $\cos(\theta)|00\rangle + \sin(\theta)|11\rangle$ [35, 4], and were used as part of a more complex protocol to obtain self-testing for all pure bipartite entangled states [13]. The work of Barizien, Sekatski, and Bancal [5] extended this family to include extra degrees of freedom in Bob's measurements, which we will refer to as "extended" tilted-CHSH inequalities.

We apply Theorem 3 to the SOS decomposition for the extended tilted-CHSH inequalities presented in [5]. Specifically, in Theorem 5 we prove that the maximum quantum value achieved for any of the extended tilted-CHSH functionals is preserved by the KLVY compilation procedure. Then in Theorem 12 we use this same decomposition to prove that this family of games is a compiled self-test according to Definition 11.

Related work

A recent work of [20] implies that the compiled value of any 2-prover Bell scenario is bounded by the largest violation possible among so-called *commuting operator* models. However, unlike some previous results, such as [6, 16], the upper bound in [20] lacks a dependence on the security parameter λ, making it unclear how the compiled value is related to the quantum value at fixed security parameters. Hence, results such as ours, which obtain a bound on the compiled value that depends negligibly on the security parameter, remain of great importance. Furthermore, [20] also considers a notion of self-testing in the compiled setting, however, due to their methods the results are in terms of commuting operator self-tests (as defined in [29, Proposition 7.8]) and only hold in the limit of the security parameter $\lambda \to \infty$.

Another related work is [26], which presents a protocol for certifying that an unknown computationally bounded device has prepared a maximally entangled pair of qubits, and whether a measurement was performed on each qubit in either the computational or Hadamard basis. The techniques used to prove our compiled self-test have similarities to those of [26], particularly in the choice of isometry (see Definition 11) and proof structure, which in turn resembles self-testing techniques in the bipartite setting [4]. There are however some key differences. Firstly, [26] certifies the preparation of a maximally entangled state by the device before any measurements are made. While our results are tailored to the more general class of partially entangled states, we only make statements about the post-measurement states after each round. It is an interesting open question if our results can be extended in this way (see Section 4.1 for more details), and statements weaker than certifying the prepared state could also be possible. For example, can a compiled self-test be used to show the prepared state must have been entangled? Another significant difference to [26] is that the self-testing protocol in this work strongly resembles the bipartite case, owing to the compilation procedure mapping bipartite nonlocal scenarios to single prover scenarios. Our main result can therefore be interpreted as translating a self-testing statement in the Bell scenario to one in the compiled Bell scenario. On the other hand, the authors of [26] describe their approach as more "custom", guided by the available cryptographic primitives, and pose the open question of finding a general procedure for translating self-testing results from the nonlocal setting. We showed this is possible for the special case of titled-CHSH inequalities.

Future outlook

Moving forward, we consider several natural directions for following up on this work:

1. Tilted-CHSH inequalities were an integral component of the self-testing for all pure bipartite entangled states [13]. Building off of our work on compiled tilted-CHSH inequalities, a natural question is whether similar results can be obtained in the compiled setting.
2. It would be desirable to understand the fundamental limitations of our notion of self-testing and other similar notions such as the computational self-testing given in [26]. Furthermore, is a finer notion of self-testing in the compiled setting that characterizes both Alice's and Bob's operators and the initial state possible without specifying the underlying QHE scheme? Moreover, is every self-test in the standard Bell scenario also a compiled self-test, and vice-versa?
3. Many current techniques for bounding the value of compiled nonlocal games/Bell inequalities can be obtained using some variant of the sum-of-squares decomposition approach. Given our improvements to this approach outlined in Theorem 3, it is possible to search for valid decompositions which include arbitrary words in Bob's operators. Is it possible to use this approach to give a limited variant of the NPA hierarchy [28] in the compiled setting?

2 Background

2.1 Mathematical notation

Throughout the article, Hilbert spaces are denoted by $\mathcal{H}$, and are assumed to be finite-dimensional unless explicitly stated otherwise. Elements of $\mathcal{H}$ are denoted by $|v\rangle \in \mathcal{H}$, where the inner product $\langle u|v\rangle$ for $|v\rangle, |u\rangle \in \mathcal{H}$ is linear in the second argument and defines the vector norm $\||v\rangle\| = \sqrt{\langle v|v\rangle}$. Quantum pure states are the norm 1 elements of $\mathcal{H}$. In this work, $\mathbb{B}(\mathcal{H})$ denotes the unital †-algebra of bounded linear operators on $\mathcal{H}$ with norm $\|M\|_{\text{op}}^2 = \sup_{|v\rangle\in\mathcal{H},|v\rangle\neq 0}\langle v|M^\dagger M|v\rangle/\langle v|v\rangle$. We also write $\|A\|_2 = \sqrt{tr(A^\dagger A)}$ to denote the Schatten 2-norm for $A \in \mathbb{B}(\mathbb{C}^d) \cong M_d(\mathbb{C})$. The unit in $\mathbb{B}(\mathcal{H})$ is denoted by $\mathbb{I}$, and we write $|M| = \sqrt{M^\dagger M}$ for the positive part of $M \in \mathbb{B}(\mathcal{H})$. Given a finite set $\mathcal{A}$, a collection of positive operators $\{M_a \geq 0 : a \in \mathcal{A}\}$ with the property that $\sum_{a\in\mathcal{A}} M_a = \mathbb{I}$, is called a POVM over $\mathcal{A}$. When the operators in a POVM are orthogonal projections, we call it a PVM. Given a random variable X, which takes values $X = x \in \mathcal{X}$ according to a distribution $\mu : \mathcal{X} \to \mathbb{R}_{\geq 0}$ such that $\sum_{x\in X} \mu(x) = 1$, we denote the expectation of X by $\mathbb{E}[X] = \sum_{x\in\mathcal{X}} \mu(x) \cdot x$. For $a, b \in \mathbb{R}$ and $\delta > 0$, $a \approx_\delta b$ is short for $|a - b| \leq \delta$. A function $\text{negl} : \mathbb{N} \to \mathbb{R}$ is called negligible if for all $k \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that for every $n \geq N$ it holds that $\text{negl}(n) \leq \frac{1}{n^k}$.

2.2 Bell scenarios, inequalities, and violations

Before we discuss compiled Bell inequalities, let us recall the bipartite case. Here we let $\mathcal{A}, \mathcal{B}, \mathcal{X}$, and $\mathcal{Y}$ be finite sets, with $|\mathcal{A}| = m_A$, $|\mathcal{B}| = m_B$, $|\mathcal{X}| = n_A$, and $|\mathcal{Y}| = n_B$. A bipartite Bell scenario is described by the tuple $\mathcal{S} = (\mathcal{A}, \mathcal{B}, \mathcal{X}, \mathcal{Y}, \pi)$, where $\pi : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}_{\geq 0}$ is a distribution over the measurement settings. In a scenario, each party receives an input $x \in \mathcal{X}$ (resp. $y \in \mathcal{Y}$) sampled according to π, and returns outputs $a \in \mathcal{A}$ (resp. $b \in \mathcal{B}$). The parties are non-communicating, and therefore cannot coordinate their outputs. The behaviour of the provers is characterized by a correlation, a set of conditional probabilities

$\mathsf{p} = \{p(a,b|x,y) : a \in \mathcal{A}, b \in \mathcal{B}, x \in \mathcal{X}, y \in \mathcal{Y}\}$, which is realized by an underlying physical theory or model. In the quantum setting, we allow the provers to share a bipartite quantum state, and say the correlation p is realized by a **bipartite (quantum) model**

$$\mathrm{Q} = \big(\mathcal{H}_A, \mathcal{H}_B, \{\{M_{a|x}\}_{a\in\mathcal{A}}\}_{x\in\mathcal{X}}, \{\{N_{b|y}\}_{b\in\mathcal{B}}\}_{y\in\mathcal{Y}}, |\Psi\rangle_{AB}\big), \tag{1}$$

where $\mathcal{H}_A$ and $\mathcal{H}_B$ are Hilbert spaces, $\{M_{a|x}\}_{a\in\mathcal{A}}$ and $\{N_{b|y}\}_{b\in\mathcal{B}}$ are POVMs on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, and $|\Psi\rangle_{AB}$ is a vector state in $\mathcal{H}_A \otimes \mathcal{H}_B$. More generally, a correlation p is quantum (or an element of $C_{\mathrm{q}}(n_A, n_B, m_A, m_B)$) if there exists a bipartite model Q for which p can be realized via the Born rule as $p(a,b|x,y) = \langle\Psi|M_{a|x} \otimes N_{b|y}|\Psi\rangle$. We denote the class of bipartite (quantum) models by $\mathcal{Q}(n_A, n_B, m_A, m_B)$. From now on we will refer to such models simply as **bipartite models**.

In contrast to the set of quantum correlations, we have the collection of local correlations $C_{\mathrm{loc}}(n_A, n_B, m_A, m_B)$. These are the correlations $\{p(a,b|x,y)\}$ for which there exists a **classical model**, that is a probability distribution μ_k and a local distributions $p_k^A(a|x)$ and $p_k^B(b|y)$ such that $p(a,b|x,y) = \sum_k \mu_k\, p_k^A(a|x)\, p_k^B(b|y)$. We let $\mathrm{C} = (\mu_k, \{p_k^A\}, \{p_k^B\})$ denote a **classical model** and let $\mathcal{L}(n_A, n_B, m_A, m_B)$ denote the class of all classical models. In what follows we consider Bell scenarios where $n_A = n_B = n$, and $m_A = m_B = m$. With this notation Bell's theorem [7] states that $C_{\mathrm{loc}}(2,2)$ is a strict subset of $C_{\mathrm{q}}(2,2)$.

Given a Bell scenario $\mathcal{S}$, one can consider a linear (or Bell) functional on the set of correlations

$$I = \sum_{a\in\mathcal{A}, b\in\mathcal{B}, x\in\mathcal{X}, y\in\mathcal{Y}} w_{abxy}\, p(a,b|x,y), \tag{2}$$

for coefficients $w_{abxy} \in \mathbb{R}$. A **Bell inequality** is a functional I and a bound $\eta > 0$ such that $I \leq \eta$ for all $\mathsf{p} \in C_{\mathrm{loc}}(n,m)$. Given a functional I, the classical value is the maximal value achieved by the classical correlations $\mathsf{p} \in C_{\mathrm{loc}}(n,m)$. We denote this value by $\eta^{\mathrm{L}} := \sup_{\mathsf{p}\in C_{\mathrm{loc}}(m,n)} I$. The quantum value for I is the maximal value achieved by the set of quantum correlations $\mathsf{p} \in C_{\mathrm{q}}(m,n)$, and we denote the quantum value on I by $\eta^{\mathrm{Q}} := \sup_{\mathsf{p}\in C_{\mathrm{q}}(m,n)} I$. Hence, a Bell violation occurs whenever there is a $\mathsf{p} \in C_{\mathrm{q}}(m,n)$ for which $I > \eta^{\mathrm{L}}$. A violation of a Bell inequality by non-communicating provers employing a quantum model is an indication of entanglement between provers.

Typically when η^{L} is known for a given I, the main challenge is finding an upper bound on η^{Q}. In this case, one often considers the **Bell operator**[1] $S = \sum_{abxy} w_{abxy}\, M_{a|x} \otimes N_{b|y}$, and $\langle S\rangle = \langle\Psi|S|\Psi\rangle$ its quantum expectation with respect to $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. Since bipartite models with separable quantum states generate the classical correlations $C_{\mathrm{q}}(m,n)$, $\langle\Psi|S|\Psi\rangle \leq \eta^{\mathrm{L}}$ whenever $|\Psi\rangle$ is separable (unentangled). However, it's possible that there could be entangled states for which $\langle\Psi'|S|\Psi'\rangle > \eta^{\mathrm{L}}$. Hence, given a Bell operator S, we can recover the maximum classical and quantum values $\eta^{\mathrm{L}} = \sup_{\mathrm{C}\in\mathcal{L}(n,m)}\langle S\rangle$ and $\eta^{\mathrm{Q}} = \sup_{\mathrm{Q}\in\mathcal{Q}(n,m)}\langle S\rangle$ respectively. Technically, we have not fixed the dimensions of the Bell operator as we want to consider any finite-dimensional model. Hence, the supremum is implicitly over all finite-dimensional Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$.

An approach to establishing upper bounds on $\langle S\rangle$ is using sum-of-squares techniques. Let S be a Bell operator and $\eta' > 0$. The shifted Bell operator $\eta'\mathbb{I} - S$ admits a **sum-of-squares** (SOS) decomposition if there exists a set of polynomials $\{P_i\}_{i\in\mathcal{I}}$ in the elements $\{M_{a|x}, N_{b|y} : a \in \mathcal{A}, b \in \mathcal{B}, x \in \mathcal{X}, y \in \mathcal{Y}\}$ satisfying $\eta'\mathbb{I} - S = \sum_{i\in\mathcal{I}} P_i^\dagger P_i$. The existence of

[1] For a more mathematically rigorous treatment of Bell operators and the SOS approach consult [16].

an SOS decomposition for the operator $\eta'\mathbb{I} - S$ implies that $\eta'\mathbb{I} - S$ is positive, and therefore η' is an upper bound on the maximum quantum value of $\langle S \rangle$. Additionally, if η' is achievable by a bipartite model, then we write $\eta' = \eta^{\mathrm{Q}}$. In this case, the *shifted* Bell operator is $\bar{S} = \eta^{\mathrm{Q}}\mathbb{I} - S$, and observing $\langle \Psi | \bar{S} | \Psi \rangle = 0$ implies the constraints $P_i|\Psi\rangle = 0$ for all $i \in \mathcal{I}$; these constraints can often be used to infer the algebraic structure (rigidity) of the measurements $\{M_{a|x}\}_{a\in\mathcal{A},x\in\mathcal{X}}, \{N_{b|y}\}_{b\in\mathcal{B},y\in\mathcal{Y}}$ which achieve $\langle S \rangle = \eta^{\mathrm{Q}}$.

3 Compiled Bell scenarios

The compilation procedure of a Bell scenario is essentially the same as the procedure for compiling nonlocal games outlined in [19]. Let $\mathcal{S} = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \pi)$ be a 2-prover Bell scenario and fix a quantum homomorphic encryption scheme with *security against quantum distinguishers* and *correctness with respect to auxiliary input*. Readers unfamiliar with QHE schemes and these properties can refer to Definition 14 found in the appendix.

A **compiled Bell scenario** is the following 2-round single-prover scenario. To setup, the verifier samples a secret key $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$. Then, the verifier samples a pair of inputs $(x, y) \in \mathcal{X} \times \mathcal{Y}$ according to the distribution $\pi : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}_{\geq 0}$, and encrypts the first input as the ciphertext $\chi \leftarrow \mathsf{Enc}(\mathsf{sk}, x)$.

1. The verifier sends the ciphertext χ to the prover. The prover replies with a ciphertext α encoding their output. The verifier decrypts obtaining outcome $a \leftarrow \mathsf{Dec}(\mathsf{sk}, \alpha)$ from $\mathcal{A}$.
2. The verifier sends the sampled (plaintext) input $y \in \mathcal{Y}$ to the prover, who replies with another outcome $b \in \mathcal{B}$.

In the compiled scenario, for a chosen security parameter λ, the prover prepares an initial quantum polynomial time (QPT) preparable state $|\Psi^{(\lambda)}\rangle \in \widetilde{\mathcal{H}}^{(\lambda)}$ where $\widetilde{\mathcal{H}}^{(\lambda)}$ is a single Hilbert space (see Definition 13 for details on efficient quantum procedures). Then, the first round of the protocol is characterized by a family of POVMs $\{\{\widetilde{M}^{(\lambda)}_{\alpha|\chi}\}_{\alpha\in\bar{\mathcal{A}}}\}_{\chi\in\bar{\mathcal{X}}}$ and unitaries $\{U^{(\lambda)}_{\alpha,\chi}\}_{\alpha\in\bar{\mathcal{A}},\chi\in\bar{\mathcal{X}}}$, where $\bar{\mathcal{X}}$ and $\bar{\mathcal{A}}$ are the set of all valid ciphertexts of the first round input and output, respectively. Unlike in the bipartite setting, we must account for unitary operations applied to the post-measurement state in the first round. With this in mind, we denote the sub-normalized post-measurement state given the measurement over ciphertext χ and encrypted outcome α by

$$U^{(\lambda)}_{\alpha,\chi}\widetilde{M}^{(\lambda)}_{\alpha|\chi}|\Psi^{(\lambda)}\rangle =: |\Psi^{(\lambda)}_{\alpha|\chi}\rangle. \tag{3}$$

Note that these vectors are sub-normalized. In particular, the probability of obtaining $\alpha \in \bar{\mathcal{A}}$ given $\chi \in \bar{\mathcal{X}}$ is given by $\langle \Psi^{(\lambda)}_{\alpha|\chi} | \Psi^{(\lambda)}_{\alpha|\chi} \rangle$. In the second round, the device makes a POVM measurement $\{\{N^{(\lambda)}_{b|y}\}_{b\in\mathcal{B}}\}_{y\in\mathcal{Y}}$, where the resulting conditional probability is given by

$$\langle \Psi^{(\lambda)} | \widetilde{M}^{(\lambda)\dagger}_{\alpha|\chi} U^{(\lambda)\dagger}_{\alpha,\chi} N^{(\lambda)}_{b|y} U^{(\lambda)}_{\alpha,\chi} \widetilde{M}^{(\lambda)}_{\alpha|\chi} | \Psi^{(\lambda)} \rangle = \langle \Psi^{(\lambda)}_{\alpha|\chi} | N^{(\lambda)}_{b|y} | \Psi^{(\lambda)}_{\alpha|\chi} \rangle, \tag{4}$$

for a fixed, $\lambda \in \mathbb{N}$, $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$, ciphertexts $\chi \in \bar{\mathcal{X}}$, $\alpha \in \bar{\mathcal{A}}$, and plaintexts $y \in \mathcal{Y}$, $b \in \mathcal{B}$.

To summarize, for a fixed QHE scheme, $\lambda \in \mathbb{N}$, a **compiled (quantum) model** is given by a tuple

$$\widetilde{\mathrm{Q}}^{(\lambda)} = (\widetilde{\mathcal{H}}^{(\lambda)}, \{|\Psi^{(\lambda)}_{\alpha|\chi}\rangle\}_{\alpha\in\bar{\mathcal{A}},\chi\in\bar{\mathcal{X}}}, \{\{N^{(\lambda)}_{b|y}\}_{b\in\mathcal{B}}\}_{y\in\mathcal{Y}}), \tag{5}$$

where all the relevant measurements and states are obtained by some QPT procedure. We remark that one can consider a description of the model which includes the initial state $|\Psi^{(\lambda)}\rangle$ and the operators $\{U^{(\lambda)}_{\alpha,\chi}\widetilde{M}^{(\lambda)}_{\alpha|\chi}\}_{\alpha\in\bar{\mathcal{A}},\chi\in\bar{\mathcal{X}}}$, rather than the post-measurement states $|\Psi^{(\lambda)}_{\alpha|\chi}\rangle$.

Hence, $\widetilde{\mathrm{Q}}^{(\lambda)}$ is really a coarse description of a quantum model in the compiled setting. The joint distribution of the outcomes after both rounds is given by

$$p^{(\lambda)}(a,b|x,y) = \mathop{\mathbb{E}}_{\mathsf{sk}\leftarrow\mathsf{Gen}(1^\lambda)} \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha:\mathsf{Dec}(\alpha)=a} \langle \Psi^{(\lambda)}_{\alpha|\chi} | N^{(\lambda)}_{b|y} | \Psi^{(\lambda)}_{\alpha|\chi} \rangle. \tag{6}$$

Note that the marginal distribution $p^{(\lambda)}(a|x)$ obtained from Equation (6) will be independent of the second input y due to the sequential nature of the protocol. However, the marginal $p^{(\lambda)}(b|y,x)$ currently depends on x. The aim of what follows is to establish a computational independence between this distribution and the inputs x. To do so we will need to consider the distributions of the decrypted outputs and appeal to the security promise of the QHE scheme. Specifically, we require a key lemma which has appeared in several works [27, 16, 6]. We borrow a version from [20] and we refer the reader to the reference for the proof.

▶ **Lemma 1** ([20], Proposition 4.6)**.** *Let $\widetilde{\mathrm{Q}}^{(\lambda)}$ be a compiled quantum model, and $\mathcal{N}^{(\lambda)} = w(\{N^{(\lambda)}_{b|y}\}_{b\in\mathcal{B},y\in\mathcal{Y}})$ be a monomial in the measurement operators $\{N^{(\lambda)}_{b|y}\}_{b\in\mathcal{B},y\in\mathcal{Y}}$, where $\lambda\in\mathbb{N}$ is the security parameter for a fixed QHE scheme. Then, for any two QPT sampleable distributions $\mathcal{D}_1,\mathcal{D}_2$ over plaintext inputs $x\in\mathcal{X}$ there exists a negligible function* $\mathrm{negl}(\lambda)$ *of the security parameter λ such that the following holds*

$$\left| \mathop{\mathbb{E}}_{\mathsf{sk}\leftarrow\mathsf{Gen}(1^\lambda)} \mathop{\mathbb{E}}_{x\leftarrow\mathcal{D}_1} \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha\in\bar{\mathcal{A}}} \langle \Psi^{(\lambda)}_{\alpha|\chi} | \mathcal{N}^{(\lambda)} | \Psi^{(\lambda)}_{\alpha|\chi} \rangle - \mathop{\mathbb{E}}_{\mathsf{sk}\leftarrow\mathsf{Gen}(1^\lambda)} \mathop{\mathbb{E}}_{x\leftarrow\mathcal{D}_2} \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha\in\bar{\mathcal{A}}} \langle \Psi^{(\lambda)}_{\alpha|\chi} | \mathcal{N}^{(\lambda)} | \Psi^{(\lambda)}_{\alpha|\chi} \rangle \right| \leq \mathrm{negl}(\lambda).$$

The approximate no-signalling conditions from Alice to Bob can then be seen by applying Lemma 1 to the monomials of degree 1 in the QPT measurement operators $\{N^{(\lambda)}_{b|y}\}_{b\in\mathcal{B},y\in\mathcal{Y}}$, since

$$\left| \mathop{\mathbb{E}}_{\mathsf{sk}\leftarrow\mathsf{Gen}(1^\lambda)} \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha\in\bar{\mathcal{A}}} \langle \Psi^{(\lambda)}_{\alpha|\chi} | N^{(\lambda)}_{b|y} | \Psi^{(\lambda)}_{\alpha|\chi} \rangle - \mathop{\mathbb{E}}_{\mathsf{sk}\leftarrow\mathsf{Gen}(1^\lambda)} \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x')=\chi} \sum_{\alpha\in\bar{\mathcal{A}}} \langle \Psi^{(\lambda)}_{\alpha|\chi} | N^{(\lambda)}_{b|y} | \Psi^{(\lambda)}_{\alpha|\chi} \rangle \right| \leq \mathrm{negl}(\lambda) \tag{7}$$

holds for all $b\in\mathcal{B}, y\in\mathcal{Y}$ and $x,x'\in\mathcal{X}$ with $x\neq x'$.

In the above statements, the measurements are completely general, and the states are sub-normalized vectors. The following lemma shows that when considering the compiled value, we can assume that the states and measurement operators in the compiled strategy are pure and projective.

▶ **Lemma 2.** *Let $\mathcal{H}'^{(\lambda)}$ be the Hilbert space of the device, and $\{\{\rho^{(\lambda)}_{\alpha|\chi}\}_{\alpha\in\bar{\mathcal{A}}}\}_{\chi\in\bar{\mathcal{X}}}$ be a family of QPT-preparable sub-normalized states on $\mathcal{H}'^{(\lambda)}$ after the first round. Let $\{\{N'^{(\lambda)}_{b|y}\}_{b\in\mathcal{B}}\}_{y\in\mathcal{Y}}$ be a family of QPT-implementable POVMs on $\mathcal{H}'^{(\lambda)}$, which induce the behaviour $p^{(\lambda)}(\alpha,b|\chi,y) = \mathrm{tr}[N'^{(\lambda)}_{b|y}\rho^{(\lambda)}_{\alpha|\chi}]$. Then there exists a Hilbert space $\mathcal{H}^{(\lambda)}$, a family of QPT-preparable sub-normalized states $\{\{|\Psi^{(\lambda)}_{\alpha|\chi}\rangle\}_{\alpha\in\bar{\mathcal{A}}}\}_{\chi\in\bar{\mathcal{X}}}$ in $\mathcal{H}^{(\lambda)}$, and a family of QPT-implementable PVMs $\{\{N^{(\lambda)}_{b|y}\}_{b\in\mathcal{B}}\}_{y\in\mathcal{Y}}$ on $\mathcal{H}^{(\lambda)}$ which satisfy*

$$\langle \Psi^{(\lambda)}_{\alpha|\chi} | N^{(\lambda)}_{b|y} | \Psi^{(\lambda)}_{\alpha|\chi} \rangle = p^{(\lambda)}(\alpha,b|\chi,y), \quad \forall \alpha\in\bar{\mathcal{A}},\ \chi\in\bar{\mathcal{X}},\ b\in\mathcal{B},\ y\in\mathcal{Y}. \tag{8}$$

See Section A.2 for the proof of Lemma 2.

We say a compiled model $\widetilde{\mathrm{Q}}^{(\lambda)} = (\widetilde{\mathcal{H}}^{(\lambda)}, \{|\Psi^{(\lambda)}_{\alpha|\chi}\rangle\}_{\alpha\in\bar{\mathcal{A}},\chi\in\bar{\mathcal{X}}}, \{\{N^{(\lambda)}_{b|y}\}_{b\in\mathcal{B}}\}_{y\in\mathcal{Y}})$ is pure and projective whenever the states $|\Psi^{(\lambda)}_{\alpha|\chi}\rangle$ are all pure and the measurements $N^{(\lambda)}_{b|y}$ are all projective (i.e. PVMS).

3.1 Quantum bounds for compiled inequalities

A compiled (quantum) model $\widetilde{\mathrm{Q}}^{(\lambda)}$ describes the correlations $\mathsf{p}^{(\lambda)} = \{p^{(\lambda)}(a,b|x,y)\}_{a\in\mathcal{A},b\in\mathcal{B},x\in\mathcal{X},y\in\mathcal{Y}}$ observed in a compiled Bell scenario. A **compiled Bell functional** is a linear functional $I^{(\lambda)}$ evaluated on correlations realized by compiled models. That is

$$I^{(\lambda)} = \sum_{abxy} w_{abxy} \mathop{\mathbb{E}}_{\substack{\mathsf{sk}\leftarrow\mathsf{Gen}(1^\lambda)\\ \chi:\mathsf{Enc}(x)=\chi}} \sum_{\alpha:\mathsf{Dec}(\alpha)=a} \langle\Psi^{(\lambda)}_{\alpha|\chi}|N^{(\lambda)}_{b|y}|\Psi^{(\lambda)}_{\alpha|\chi}\rangle. \tag{9}$$

By the properties of the compilation procedure [19, Theorem 3.2], Bell inequalities are preserved under compilation (up to negligible error). In particular, for large security parameter, efficient classical provers cannot violate a Bell inequality by much more than they could in the (bipartite) scenario. From now on, we will suppress the security parameter $\lambda \in \mathbb{N}$ along with the expectation over secret keys $\mathbb{E}_{\mathsf{sk}\leftarrow\mathsf{Gen}(1^\lambda)}$ and simply write the expectation for a fixed key. In particular, we express the compiled model as $\widetilde{\mathrm{Q}}$ and Equation (9) as

$$I = \sum_{abxy} w_{abxy} \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha:\mathsf{Dec}(\alpha)=a} \langle\Psi_{\alpha|\chi}|N_{b|y}|\Psi_{\alpha|\chi}\rangle.$$

We now turn our attention to the maximum value I can take in the compiled setting with an efficient quantum prover. The results of [19] imply that an efficient quantum prover can achieve the same violation in the bipartite setting. However, the existence of a quantum compiled behavior which exceeds the maximal quantum Bell violation in the bipartite case (by more than negligible factors) has not been ruled out. Nonetheless, in several cases (like the CHSH inequality and more generally all XOR games [16]) we know that the quantum compiled behavior cannot exceed the value η^{Q} by more than negligible amounts. One technique for establishing such bounds was introduced in [27] and uses SOS techniques to bound the quantum violation of the compiled Bell functional.

3.2 Extending the pseudo-expectations

Our approach builds off the methods used in [27] and [16]. To explain this approach we recall that a pseudo-expectation is a unital, linear map from a subspace $\mathcal{T}$ of the algebra generated by $\{M_{a|x}, N_{b|y}\}_{a\in\mathcal{A},x\in\mathcal{X},b\in\mathcal{B},y\in\mathcal{Y}}$ to the complex numbers, $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}} : \mathcal{T} \to \mathbb{C}$, which is determined by a compiled quantum model $\widetilde{\mathrm{Q}}$. In the case $n = m = 2$, it suffices to define the pseudo-expectation $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}$ on the observables $A_x = \sum_{a\in\{0,1\}}(-1)^a M_{a|x}$, $B_y = \sum_{b\in\{0,1\}}(-1)^b N_{b|y}$ and require that they are mapped to their expectations in the compiled scenario[2]. We further assume that all measurements are projective (cf. Lemma 2). In previous works, the definition of the pseudo-expectation had been restricted to monomials consisting of at most one Alice and one Bob observable as outlined below:

[2] Though in the following we define $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}$ for $n = m = 2$, this can be directly extended to arbitrary Bell scenarios by defining $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}$ on the POVM elements $M_{a|x}, N_{b|y}$ in an analogous way.

$$
\begin{aligned}
\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[A_x B_y] &:= \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha} (-1)^{\mathsf{Dec}(\alpha)} \langle \Psi_{\alpha|\chi} | B_y | \Psi_{\alpha|\chi} \rangle, \\
\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[A_x A_{x'}] &:= \delta_{x,x'}, \\
\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[B_y B_{y'}] &:= \mathop{\mathbb{E}}_{x\in\mathcal{X}} \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha} \langle \Psi_{\alpha|\chi} | B_y B_{y'} | \Psi_{\alpha|\chi} \rangle, \\
\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[A_x] &:= \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha} (-1)^{\mathsf{Dec}(\alpha)} \langle \Psi_{\alpha|\chi} | \Psi_{\alpha|\chi} \rangle, \\
\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[B_y] &:= \mathop{\mathbb{E}}_{x\in\mathcal{X}} \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha} \langle \Psi_{\alpha|\chi} | B_y | \Psi_{\alpha|\chi} \rangle, \\
\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[\mathbb{I}] &:= 1,
\end{aligned}
\tag{10}
$$

where $\mathbb{E}_{x\in\mathcal{X}}$ denotes the expectation according to an arbitrary fixed distribution over $\mathcal{X}$. This is already sufficient to handle known SOS decompositions for a variety of well-studied Bell inequalities whenever the polynomials are expressed in the basis $\{\mathbb{I}, A_x, B_y\}_{x\in\mathcal{X},y\in\mathcal{Y}}$. However, there are Bell inequalities, such as the tilted-CHSH inequality [4, 5], for which no known SOS decomposition exists in the basis $\{\mathbb{I}, A_x, B_y\}_{x\in\mathcal{X},y\in\mathcal{Y}}$.

The contribution of this section is to expand the definition of the pseudo-expectation to the basis encompassing all monomials in A_x, B_0, B_1, for a fixed $x \in \mathcal{X}$, in a way that is approximately non-negative on Hermitian squares. This allows us to handle more general SOS decompositions, and in particular, the tilted-CHSH inequalities. Let $w(A_x, B_0, B_1)$ be a monomial in the elements $\{A_x, B_0, B_1\}$. Importantly, x is fixed, and we do not consider monomials of the form $A_0 A_1 B_y$ for example. Let $\bar{w}$ be the canonical form of w under the relations $[A_x, B_y] = 0$, $(B_y)^2 = (A_x)^2 = \mathbb{I}$, where all A_x terms are commuted to the left. Since we only consider one value of x, these will all be of the form $(A_x)^i \bar{w}(B_0, B_1)$ for some $i \in \{0, 1\}$, where the monomial $\bar{w}(B_0, B_1)$ cannot be reduced further. We then define the pseudo-expectation

$$
\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}\big[w(A_x, B_0, B_1)\big] := \tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}\big[(A_x)^i \bar{w}(B_0, B_1)\big]. \tag{11}
$$

For the case $i = 0$, we define

$$
\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}\big[\bar{w}(B_0, B_1)\big] := \mathop{\mathbb{E}}_{x\in\mathcal{X}} \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha} \langle \Psi_{\alpha|\chi} | \bar{w}(B_0, B_1) | \Psi_{\alpha|\chi} \rangle, \tag{12}
$$

and for the case $i = 1$,

$$
\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}\big[A_x \bar{w}(B_0, B_1)\big] := \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha} (-1)^{\mathsf{Dec}(\alpha)} \langle \Psi_{\alpha|\chi} | \bar{w}(B_0, B_1) | \Psi_{\alpha|\chi} \rangle. \tag{13}
$$

From the above definitions, we next state the main result of this section, which can be applied generally to any polynomial expressible in the basis $\{A_x, B_0, B_1\}$.

▶ **Theorem 3.** *Let $\{A_x\}_{x\in\mathcal{X}}$ and $\{B_y\}_{y\in\mathcal{Y}}$ be binary observables, and let*

$$
P = \sum_i \gamma_i (A_x)^{k_i} w_i(B_0, B_1), \tag{14}
$$

where $\gamma_i \in \mathbb{C}$, $k_i \in \{0, 1\}$ and each $w_i(B_0, B_1)$ is any monomial in the algebra of $\{B_0, B_1\}$. Then there exists a negligible function $\mathrm{negl}(\lambda)$ of the security parameter $\lambda \in \mathbb{N}$ such that

$$
\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[P^\dagger P] \geq -\mathrm{negl}(\lambda). \tag{15}
$$

Furthermore, for a given Bell functional I, and a compiled model $\widetilde{\mathrm{Q}}$, $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}(I)$ is the expected value of the compiled model $\widetilde{\mathrm{Q}}$ on I.

The proof can be found in Section A.2.

3.3 Quantum bounds for compiled tilted-CHSH expressions

We now present the family of extended tilted-CHSH type expressions and their SOS decompositions discovered in [5]. Let $\theta \in (0, \pi/4]$, $\phi \in \big(\max\{-2\theta, -\pi+2\theta\}, \min\{2\theta, \pi-2\theta\}\big) \setminus \{0\}$, and $t_{\theta,\phi} \in \mathbb{R}$ such that

$$\frac{1}{t_{\theta,\phi}^2} = \frac{\sin^2(2\theta)}{\tan^2(\phi)} - \cos^2(2\theta). \tag{16}$$

From here, we define the following expressions:

$$\begin{aligned} S_{\theta,\phi} &:= A_0 \otimes \frac{B_0+B_1}{\cos(\phi)} + t_{\theta,\phi}^2\Big[\sin(2\theta)\, A_1 \otimes \frac{B_0-B_1}{\sin(\phi)} + \cos(2\theta)\, \mathbb{I} \otimes \frac{B_0+B_1}{\cos(\phi)}\Big], \\ \eta^{\mathrm{Q}}_{\theta,\phi} &:= 2(1+t_{\theta,\phi}^2). \end{aligned} \tag{17}$$

We also let $I_{\theta,\phi}$ denote the corresponding Bell functional, and recall the following result.

▶ **Lemma 4** ([5], Section 3.2.1). *Let $\theta \in (0, \pi/4]$, $\phi \in \big(\max\{-2\theta, -\pi+2\theta\}, \min\{2\theta, \pi-2\theta\}\big) \setminus \{0\}$, $t_{\theta,\phi}$ be given by Equation (16) and $S_{\theta,\phi}, \eta^{\mathrm{Q}}_{\theta,\phi}$ be defined in Equation (17). Define the following polynomials:*

$$\begin{aligned} N_0 &:= A_0 \otimes \mathbb{I} - \mathbb{I} \otimes \frac{B_0+B_1}{2\cos(\phi)}, \\ N_1 &:= A_1 \otimes \mathbb{I} - \sin(2\theta)\, \mathbb{I} \otimes \frac{B_0-B_1}{2\sin(\phi)} - \cos(2\theta)\, A_1 \otimes \frac{B_0+B_1}{2\cos(\phi)}. \end{aligned} \tag{18}$$

Then the shifted Bell operator $\bar{S}_{\theta,\phi} = \eta^{\mathrm{Q}}_{\theta,\phi}\mathbb{I} - S_{\theta,\phi}$ admits the SOS decomposition

$$\bar{S}_{\theta,\phi} = N_0^\dagger N_0 + t_{\theta,\phi}^2 N_1^\dagger N_1. \tag{19}$$

Using the decomposition in Lemma 4, it was shown in [5] that the inequality $\langle S_{\theta,\phi}\rangle \leq \eta^{\mathrm{Q}}_{\theta,\phi}$ self-tests the partially entangled state $|\psi_\theta\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle$ and the measurements

$$\begin{aligned} &A_0 = \sigma_Z,\ A_1 = \sigma_X, \\ &B_y = \cos(\phi)\,\sigma_Z + (-1)^y \sin(\phi)\,\sigma_X,\ y \in \{0,1\}, \end{aligned} \tag{20}$$

where σ_Z, σ_X are the Pauli operators. Notably, by setting $\phi = \mu_\theta$ where $\tan(\mu_\theta) = \sin(2\theta)$, this family encompasses what are most commonly referred to as "tilted-CHSH inequalities" given by the Bell operator

$$T_\theta = \alpha_\theta A_0 \otimes \mathbb{I} + A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1), \tag{21}$$

where $\alpha_\theta = 2/\sqrt{1+2\tan^2(2\theta)}$ [2, 35, 4]. Compared to the SOS decompositions for T_θ from [4], the decomposition of [5] is expressed in the basis for which our extended pseudo-expectation is well defined (cf. Theorem 3), allowing us to provide bounds on the compiled value of T_θ, and more generally the family $S_{\theta,\phi}$.

▶ **Theorem 5.** *Let $\theta \in (0, \pi/4]$, $\phi \in \big(\max\{-2\theta, -\pi+2\theta\}, \min\{2\theta, \pi-2\theta\}\big) \setminus \{0\}$, and let $S_{\theta,\phi}$ be the extended tilted-CHSH expression with quantum bound $\eta^{\mathrm{Q}}_{\theta,\phi}$, given by Equation (17). Then the maximum quantum value of the corresponding compiled Bell inequality is given by $\eta^{\mathrm{Q}}_{\theta,\phi} + \mathrm{negl}(\lambda)'$, where $\mathrm{negl}(\lambda)'$ is a negligible function of the security parameter.*

Proof. We evaluate the pseudo-expectation on the shifted Bell expression $\bar{S}_{\theta,\phi}$:

$$\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[\bar{S}_{\theta,\phi}] = \tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[N_0^\dagger N_0] + \lambda_{\theta,\phi}^2 \tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[N_1^\dagger N_1], \tag{22}$$

where we used the decomposition in Lemma 4. The polynomial N_0 is expressed in the basis $\{A_0, B_0, B_1\}$, and we find by Theorem 3 that

$$\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[N_0^\dagger N_0] \geq -\mathrm{negl}(\lambda). \tag{23}$$

Similarly, N_1 is expressed in the basis $\{A_1, B_0, B_1\}$, and we see by Theorem 3 that $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[N_1^\dagger N_1] \geq -\mathrm{negl}(\lambda)$. Putting these together, we obtain

$$\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[\bar{S}_{\theta,\phi}] \geq -\mathrm{negl}(\lambda)(1 + \lambda_{\theta,\phi}^2) =: -\mathrm{negl}(\lambda)', \tag{24}$$

which implies $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[S_{\theta,\phi}] \leq \eta_{\theta,\phi}^{\mathrm{Q}} + \mathrm{negl}(\lambda)'$ as desired, where $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[S_{\theta,\phi}]$ is the expected value of the compiled Bell inequality. ◀

▶ Remark 6. The extension of the $S_{\theta,\phi}$ family presented in [5, Section 3.2.3] self-tests the state $|\psi_\theta\rangle$ along with the more general measurements

$$\begin{aligned} A_0 &= \sigma_Z, \;\; A_1 = \sigma_X, \\ B_0 &= \cos(\phi)\,\sigma_Z + \sin(\phi)\,\sigma_X, \\ B_1 &= \cos(\omega)\,\sigma_Z + \sin(\omega)\,\sigma_X, \end{aligned} \tag{25}$$

for $\phi \in (-2\theta, 0)$ and $\omega \in (0, 2\theta)$. This family of Bell inequalities can also be compiled under our definition of the pseudo-expectation. This is because each SOS polynomial is given in the basis $\{A_x, B_0, B_1\}$ for a fixed x, and we can apply Theorem 3 directly as was done in Theorem 5. We omit the explicit proof of this for brevity.

4 Self-testing in the compiled setting

Recall that a bipartite (quantum) model Q, consists of a shared state $|\Psi\rangle$, along with local POVM measurements $\{M_{a|x}\}$ and $\{N_{b|y}\}$ for Alice and Bob, respectively. Given a Bell expression I, the inequality $I \leq \eta^Q$ self-tests an ideal bipartite model Q^* if any optimal bipartite model is essentially the same as Q^*, modulo some physically irrelevant degrees of freedom. This is more formally stated in terms or the existence of local isometries which maps the employed model to the ideal one. When small errors are permitted, one considers the following definition of robust self-testing.

▶ **Definition 7** (Bipartite self-test). *The inequality $I \leq \eta^{\mathrm{Q}}$ is a self-test for a bipartite model $\mathrm{Q}^* = \big(\{P_{a|x}\}, \{Q_{b|y}\}, |\phi\rangle\big)$ if there exist a non-negative function $f(\epsilon)$ such that $f(\epsilon) \to 0$ as $\epsilon \to 0$, such that for any bipartite model $\mathrm{Q} = \big(\{M_{a|x}\}, \{N_{b|y}\}, |\Psi\rangle\big)$ achieving $I \geq \eta^{\mathrm{Q}} - \epsilon$ for $\epsilon \geq 0$, there exists a Hilbert space $\mathcal{H}_{\mathrm{aux}}$, an auxiliary state $|\zeta\rangle \in \mathcal{H}_{\mathrm{aux}}$ and local isometries V_A and V_B, such that defining $V : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathcal{H}_{\mathrm{aux}}$, $V = V_A \otimes V_B$, the following is satisfied for all x, y, a, b:*

$$\big\| V_A \otimes V_B (M_{a|x} \otimes N_{b|y})|\Psi\rangle - (P_{a|x} \otimes Q_{b|y})|\phi\rangle \otimes |\zeta\rangle \big\| \leq f(\epsilon).$$

In the bipartite setting, one could consider the situation where Alice measures first using a POVM $\{P_{a|x}\}$, collapsing the state to a post-measurement state $\rho_{a|x}$ on Bob's subsystem $\mathcal{H}_B$, upon which Bob performs his measurement, resulting in the application of the POVM element $Q_{b|y}$. With this in mind, we consider the setting where the only relevant features of the model are those from Bob's (resp. Alice's) perspective. In particular, subsystem A is traced out following the recorded measurement of outcome of a given x.

▶ **Definition 8** (Partial model). *Given a bipartite model* $\mathrm{Q} = \big(\{M_{a|x}\}, \{N_{b|y}\}, |\Psi\rangle\big)$*, we define the partial model of* Q *by* $\mathrm{Q}' = (\{N_{b|y}\}, \{\rho_{a|x}\})$ *where*

$$\rho_{a|x} = \mathrm{tr}_A[(M_{a|x} \otimes \mathbb{I}_B)|\Psi\rangle\langle\Psi|]. \tag{26}$$

We note that $\rho_{a|x}$ *will generally be mixed. When each* $\rho_{a|x}$ *is pure, we say that* Q *has a pure partial model, denoted by* $\mathrm{Q}' = (\{N_{b|y}\}, \{|\phi_{a|x}\rangle\})$*.*

Symmetrically, given a bipartite model one can consider a (pure) partial model on $\mathcal{H}_A$ by tracing out subsystem B. However, because our motivation is the compiled setting, we will focus on the partial models on $\mathcal{H}_B$. Furthermore, we remark that the notion of pure partial models is not vacuous. In particular, the optimal bipartite model for the CHSH inequality has a pure partial model on $\mathcal{H}_B$ [10]. With the notion of a partial quantum model, we define the notion of a partial (or one-sided) self-test for a bipartite model.

▶ **Definition 9** (Partial self-test). *The inequality* $I \leq \eta^{\mathrm{Q}}$ *is a partial self-test for a bipartite model* $\mathrm{Q}^* = \big(\{P_{a|x}\}, \{Q_{b|y}\}, |\phi\rangle\big)$ *with a pure partial model* $\big(\{Q_{b|y}\}, \{|\phi_{a|x}\rangle\}\big)$ *if there exists a non-negative function* $f(\epsilon)$ *such that* $f(\epsilon) \to 0$ *as* $\epsilon \to 0$*, such that for any partial quantum model* $\mathrm{Q} = \big(\{N_{b|y}\}, \{\rho_{a|x}\}\big)$ *achieving* $I \geq \eta^{\mathrm{Q}} - \epsilon$ *for* $\epsilon \geq 0$*, there exist a Hilbert space* $\mathcal{H}_{\mathrm{aux}}$*, a collection of auxiliary states* $\{\sigma_{a|x}\}$ *and an isometry* $V : \mathcal{H}_B \to \mathbb{C}^d \otimes \mathcal{H}_{\mathrm{aux}}$ *such that the following is satisfied for all* x, y, a, b*:*

$$\big\|V N_{b|y} \rho_{a|x} N_{b|y} V^\dagger - Q_{b|y}|\phi_{a|x}\rangle\langle\phi_{a|x}|Q_{b|y} \otimes \sigma_{a|x}\big\|_2 \leq f(\epsilon)$$
$$\text{and} \quad \big\|V \rho_{a|x} V^\dagger - |\phi_{a|x}\rangle\langle\phi_{a|x}| \otimes \sigma_{a|x}\big\|_2 \leq f(\epsilon),$$

Give the symmetry of $\mathcal{H}_A$ and $\mathcal{H}_B$ in the bipartite case, one can define a notion of partial self-test for either subsystem. Given a bipartite self-test, one can check that tracing out either subsystem results in a partial self-test. We leave it as an open question as to whether a partial self-test (say over $\mathcal{H}_A$ and over $\mathcal{H}_B$) implies that the correlation is a bipartite self-test.

4.1 Compiled self-tests from partial models

There are two main difficulties with self-testing in the compiled setting. Firstly, the *correctness with respect to auxiliary systems* property of the compiler (see *Property (1)* in Definition 14) only guarantees that a QPT prover can prepare states (possibly mixed) $\rho_{a|x}$ over $\mathcal{H}_B$ that are negligible in trace distance from the post measurement states $P_{a|x}|\Psi\rangle\langle\Psi|P_{a|x}/p(a|x)$ of the ideal bipartite model Q. This puts a fundamental constraint on our ability to exactly describe the set of ideal models in the compiled setting. Secondly, unlike in the nonlocal setting, it is not clear how to extract information about the measurements and states in the first round due to the homomorphic evaluation of the measurements and preparation of the states. To address these challenges we introduce the compiled counter-part of a partial quantum model.

Recall that a compiled (quantum) model $\widetilde{\mathrm{Q}}$ consists of a family of post-measurement states for "Alice" $|\widetilde{\phi}_{\alpha|\chi}\rangle$, which correspond to the state of the device following the encrypted question χ, and encrypted answer α, and a POVM $\{N_{b|y}\}$ employed by "Bob". One could also consider a more general compiled quantum model, which includes a description of the initial state and Alice's operators. The point of taking the coarser model is that it allows us to introduce the notion of the *compiled-counterpart* of a bipartite model Q, which relates the post-measurement information in the bipartite setting with another bipartite model that resembles a compiled model.

▶ **Definition 10** (Compiled-counterpart model). *Given a pure partial model* Q'*, the compiled-counterpart model of* Q' *is the pure partial model* $\widetilde{\mathrm{Q}}^{(\lambda)} = (\{|\widetilde{\phi}^{(\lambda)}_{\alpha|\chi}\rangle\}, \{Q^{(\lambda)}_{b|y}\})$ *satisfying the following conditions for all* $\lambda \in \mathbb{N}$*:*

$$|\widetilde{\phi}^{(\lambda)}_{\alpha|\chi}\rangle = |\phi_{a|x}\rangle, \quad \textit{for all} \;\; \mathsf{sk} : \mathsf{Gen}(1^\lambda) = \mathsf{sk}, \;\; \chi : \mathsf{Enc}(x, \mathsf{sk}) = \chi, \;\; \alpha : \mathsf{Dec}(\alpha, \mathsf{sk}) = a.$$
$$N^{(\lambda)}_{b|y} = Q_{b|y}, \quad \textit{for all } b, y.$$

We remark that the compiled counterpart need not be an actual compiled model. For example, it is not required to satisfy the QPT conditions needed of a compiled model. Instead it is a model that resembles an idealized version of an honest implementation of a partial model under homomorphic encryption. We proceed with a definition of self-testing in the compiled setting that resembles partial self-testing in the bipartite setting in the context of these compiled-counterparts.

▶ **Definition 11** (Compiled self-test). *Let* I *denote a Bell expression with an optimal pure partial model* Q^**. The inequality* $I \leq \eta^{\mathrm{Q}}$ *is a compiled self-test for the corresponding compiled-counterpart* $\widetilde{\mathrm{Q}}^* = (\{|\widetilde{\phi}_{\alpha|\chi}\rangle\}, \{Q_{b|y}\})$*, if there exists a non-negative function* $f(\epsilon)$ *such that* $f(\epsilon) \to 0$ *as* $\epsilon \to 0$*, such that for every pure and projective compiled model* $\widetilde{\mathrm{Q}} = \big(\{|\Psi_{\alpha|\chi}\rangle\}, \{N_{b|y}\}\big)$ *that achieves* $I \geq \eta^{\mathrm{Q}} - \epsilon$ *for some* $\epsilon \geq 0$*, there exists a negligible function* $\mathrm{negl}(\lambda)$*, an isometry* $V : \widetilde{\mathcal{H}} \to \mathbb{C}^d \otimes \mathcal{H}_{\mathrm{aux}}$*, and auxiliary states* $|\mathsf{aux}_{\alpha|\chi}\rangle \in \mathcal{H}_{\mathrm{aux}}$*, which satisfy the following for all* x, b, y*:*

$$\mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha} \left\| V|\Psi_{\alpha|\chi}\rangle - |\widetilde{\phi}_{\alpha|\chi}\rangle \otimes |\mathsf{aux}_{\alpha|\chi}\rangle \right\|^2 \leq \mathrm{negl}(\lambda) + f(\epsilon), \quad \textit{and} \tag{27a}$$

$$\mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_{\alpha} \left\| V N_{b|y}|\Psi_{\alpha|\chi}\rangle - Q_{b|y}|\widetilde{\phi}_{\alpha|\chi}\rangle \otimes |\mathsf{aux}_{\alpha|\chi}\rangle \right\|^2 \leq \mathrm{negl}(\lambda) + f(\epsilon). \tag{27b}$$

Equation (27a) is a statement about the provers state after the first round. It asserts that, given a question x and answer a, the post-measurement state is negligibly close to that of an ideal prover implementing the honest bipartite model. To see this concretely, suppose the right hand side was exactly equal to zero. Then we have the equality $V|\Psi_{\alpha|\chi}\rangle = |\widetilde{\phi}_{\alpha|\chi}\rangle \otimes |\mathsf{aux}_{\alpha|\chi}\rangle$ for all χ such that $\mathsf{Enc}(x) = \chi$ and all α. Substituting $|\widetilde{\phi}_{\alpha|\chi}\rangle$ for the states $|\phi_{a|x}\rangle$ from Definition 10, we obtain

$$V|\Psi_{\alpha|\chi}\rangle = |\phi_{a|x}\rangle \otimes |\mathsf{aux}_{\alpha|\chi}\rangle \tag{28}$$

whenever $\mathsf{Enc}(x) = \chi$ and $\mathsf{Dec}(\alpha) = a$. That is, the post-measurement states are equal to the target states up an isometry. Therefore, we interpret (27a) as an approximate version of Equation (28), which accounts for a finite size security parameter λ and small errors in the Bell violation ϵ. Equation (27b) is the analogous statement including the measurements in the second round. We remark that if V could depend on the question x and answer a, (27a) would trivially hold regardless of the compiled Bell violation, since the states $|\phi_{a|x}\rangle$ could be prepared directly. It is therefore essential to enforce the same isometry is applied for all a and x. Furthermore, (27b) captures several existing self-testing results in the compiled setting. For example those presented in [27, Lemma 34], [16, Theorem 3.6] and [16, Eqs. 98 and 103]. Our proposed definition then goes further by also certifying the states after the first round but before Bob's measurements, as captured by (27a).

It is natural to ask if Definition 11 is the strongest form of self-testing possible in this scenario, or if one can also certify the initial state $|\Psi\rangle$ before Alice's measurements. An initial guess would be to show there exists an isometry V satisfying

$$V|\Psi\rangle \approx_{\mathrm{negl}(\lambda)} |\phi\rangle \otimes |\mathsf{aux}\rangle, \tag{29}$$

where $|\phi\rangle$ is the ideal bipartite entangled state. However, on its own this statement is not very useful: such an isometry always exists, namely, one which ignores $|\Psi\rangle$ and prepares $|\phi\rangle$ directly. A possible way around is to demand the same V also satisfies (27). At a glance, this suggests certifying the initial state alone is not meaningful in the single prover setting; one always needs to also consider the measurements. This contrasts the two prover setting, where self-testing statements made only about the state are known [34] and non-trivial due to the space-like separation of the provers. Another question worth asking is if the assumption of having a pure projective models $\widetilde{\mathrm{Q}}$ can be relaxed in the definition Definition 11.

4.2 Compiled self-test for tilted-CHSH inequalities

Our final result is that the extended tilted-CHSH Bell inequalities are compiled self-tests according to Definition 11. In particular, we have the following result.

▶ **Theorem 12.** *Let $\theta \in (0, \pi/4]$, $\phi \in \big(\max\{-2\theta, -\pi + 2\theta\}, \min\{2\theta, \pi - 2\theta\}\big) \setminus \{0\}$, and let $I_{\theta,\phi}$ be the generalized tilted-CHSH functional with quantum bound $\eta^{\mathrm{Q}}_{\theta,\phi}$ according to Equation* (17)*. Then the inequality $I_{\theta,\phi} \leq \eta^{\mathrm{Q}}_{\theta,\phi}$ is a compiled self-test for the compiled-counter part of* (20) *according to Definition 11.*

The proof is reminiscent of the approach in [4], and includes similar calculations to those used in [27, 6] which establish rigidity statements in the compiled setting. Given the length of the proof, we refer the reader to the longer version of this work [24] for all the details.

References

1 Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98:230501, 2007. doi:10.1103/PhysRevLett.98.230501.

2 Antonio Acín, Serge Massar, and Stefano Pironio. Randomness versus nonlocality and entanglement. *Physical Review Letters*, 108:100402, March 2012. doi:10.1103/PhysRevLett.108.100402.

3 Atul Singh Arora, Kishor Bharti, Alexandru Cojocaru, and Andrea Coladangelo. A computational test of contextuality and, even simpler proofs of quantumness. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1106–1125. IEEE, October 2024. doi:10.1109/focs61266.2024.00073.

4 Cédric Bamps and Stefano Pironio. Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing. *Physical Review A*, 91:052111, May 2015. doi:10.1103/PhysRevA.91.052111.

5 Victor Barizien, Pavel Sekatski, and Jean-Daniel Bancal. Custom Bell inequalities from formal sums of squares. *Quantum*, 8:1333, May 2024. doi:10.22331/q-2024-05-02-1333.

6 Matilde Baroni, Quoc-Huy Vu, Boris Bourdoncle, Eleni Diamanti, Damian Markham, and Ivan Šupić. Quantum bounds for compiled XOR games and d-outcome CHSH games. *arXiv:2403.05502*, 2024.

7 John S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

8 Zvika Brakerski. Quantum FHE (almost) as secure as classical. In *Annual International Cryptology Conference*, pages 67–95. Springer, 2018.

9 Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In *Annual Cryptology Conference*, pages 609–629. Springer, 2015.

10 J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969. doi:10.1103/PhysRevLett.23.880.

11 John Clauser, Michael Horne, Abner Shimony, and Richard Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.

12 Richard Cleve, Peter Hoyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.*, pages 236–249. IEEE, 2004.

13 Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. All pure bipartite entangled states can be self-tested. *Nature Communications*, 8(1), May 2017. doi:10.1038/ncomms15485.

14 Andrea Coladangelo, Alex B Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-leash: New schemes for verifiable delegated quantum computation, with quasilinear resources. *Theory of Computing*, 20(1):1–87, 2024.

15 Roger Colbeck. *Quantum and Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2007. Also available as *arXiv:0911.3814*.

16 David Cui, Giulio Malavolta, Arthur Mehta, Anand Natarajan, Connor Paddock, Simon Schmidt, Michael Walter, and Tina Zhang. A computational Tsirelson's theorem for the value of compiled XOR games. *arXiv preprint arXiv:2402.17301*, 2024.

17 Alex Grilo. A simple protocol for verifiable delegation of quantum computation in one round. In *icalp2019*, pages 28:1–28:13, 2019. doi:10.4230/LIPIcs.ICALP.2019.28.

18 Gregory D. Kahanamoku-Meyer, Soonwon Choi, Umesh V. Vazirani, and Norman Y. Yao. Classically verifiable quantum advantage from a computational Bell test. *Nature Physics*, 18(8):918–924, August 2022. doi:10.1038/s41567-022-01643-7.

19 Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum advantage from any non-local game. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1617–1628, 2023.

20 Alexander Kulpe, Giulio Malavolta, Connor Paddock, Simon Schmidt, and Michael Walter. A bound on the quantum value of all compiled nonlocal games. *arXiv:2408.06711*, 2024.

21 Urmila Mahadev. Classical homomorphic encryption for quantum circuits. *SIAM Journal on Computing*, 52(6):FOCS18–189, 2020.

22 Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Information and Computation*, 4:273–286, 2004. doi:10.26421/QIC4.4-3.

23 Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012.

24 Arthur Mehta, Connor Paddock, and Lewis Wooltorton. Self-testing in the compiled setting via tilted-CHSH inequalities. *arXiv preprint arXiv:2406.04986*, 2024.

25 Tony Metger, Anand Natarajan, and Tina Zhang. Succinct arguments for QMA from standard assumptions via compiled nonlocal games. *arXiv:2404.19754*, 2024.

26 Tony Metger and Thomas Vidick. Self-testing of a single quantum device under computational assumptions. *Quantum*, 5:544, 2021.

27 Anand Natarajan and Tina Zhang. Bounding the quantum value of compiled nonlocal games: from CHSH to BQP verification. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1342–1348. IEEE, 2023.

28 Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008. doi:10.1088/1367-2630/10/7/073013.

29 Connor Paddock, William Slofstra, Yuming Zhao, and Yangchen Zhou. An operator-algebraic formulation of self-testing. *Annales Henri Poincaré*, 25(10):4283–4319, October 2023. doi:10.1007/s00023-023-01378-y.

30 S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464:1021–1024, 2010. doi:10.1038/nature09008.

31 Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009. doi:10.1088/1367-2630/11/4/045021.

32 Ben Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013.

33 Valerio Scarani. The device-independent outlook on quantum physics. *Acta Physica Slovaca*, 62(4):347–409, 2012.

34 Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, September 2020. doi:10.22331/q-2020-09-30-337.

35 Tzyh Haur Yang and Miguel Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Physical Review A*, 87:050102, May 2013. doi:10.1103/PhysRevA.87.050102.

A Appendix

A.1 Efficient quantum circuits and homomorphic encryption

To define a quantum homomorphic encryption scheme we require the following concepts from quantum cryptography.

▶ **Definition 13.** *A procedure $\mathcal{P}$ is quantum polynomial time (QPT) if:*

1. *there exists a uniform logspace family of quantum circuits that implement $\mathcal{P}$, and*
2. *the runtime of the circuit is polynomial in the number of qubits and the security parameter $\lambda \in \mathbb{N}$.*

A family of quantum states $\mathcal{F}$ is QPT (preparable) if there is a QPT $\mathcal{P}$ for preparing $\mathcal{F}$.

We now define a quantum homomorphic encryption (QHE) scheme. A formal definition of QHE first appeared in [9]. We follow the description of QHE outlined in [19, 8]:

▶ **Definition 14.** *A quantum homomorphic encryption scheme* Q *for a family of circuits $\mathcal{C}$ consists of a security parameter $\lambda \in \mathbb{N}$ and the following algorithms:*

(i) *A PPT algorithm* Gen *which takes as input a unary encoding 1^λ of the security parameter $\lambda \in \mathbb{N}$ and outputs a secret key* sk.

(ii) *A PPT algorithm* Enc *which takes as input the secret key* sk *and a plaintext $x \in \{0,1\}^n$ and produces a ciphertext $\chi \in \{0,1\}^k$.*

(iii) *A QPT algorithm* Eval *which takes as input a classical description of a quantum circuit $\mathsf{C} : \mathcal{H} \otimes (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes m}$ from $\mathcal{C}$, a quantum plaintext $|\Psi\rangle \in \mathcal{H}$ on a Hilbert space, a ciphertext χ, and evaluates a quantum circuit $\mathsf{Eval}_{\mathsf{C}}(|\Psi\rangle \otimes |0\rangle^{\mathrm{poly}(\lambda,n)}, \chi)$ producing a ciphertext $\alpha \in \{0,1\}^\ell$.*

(iv) *A QPT algorithm* Dec *which takes as input ciphertext α, and secret key* sk*, and produces a quantum state $|\Psi'\rangle$.*

Although the existence of algorithms (i)-(iv) defines a QHE scheme, we consider several additional important properties a scheme may or may not possess:

1. (Correctness with auxiliary input). For every security parameter $\lambda \in \mathbb{N}$, secret key $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$, classical circuit $\mathsf{C} : \mathcal{H}_A \otimes (\mathbb{C}^2)^{\otimes n} \to \{0,1\}^m$, quantum state $|\Psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, plaintext $x \in \{0,1\}^n$ ciphertext $\chi \leftarrow \mathsf{Enc}(x, \mathsf{sk})$, the following procedures produce states with negligible trace distance with respect to λ:
   a. Starting from the pair $(x, |\Psi\rangle_{AB})$, run the quantum circuit C on register A, outputting the classical string $a \in \{0,1\}^m$ along with the contents of register B.
   b. Starting from $(\chi, |\Psi\rangle_{AB})$, run the circuit $\mathsf{Eval}_C(\cdot)$ on register A, obtaining ciphertext $\alpha \in \{0,1\}^\ell$, output $a' = \mathsf{Dec}(\alpha, \mathsf{sk})$ along with the contents of register B.

2. (Security against efficient quantum distinguishers). Fix a secret key $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$. Any quantum polynomial time adversary $\mathfrak{A}$ with access to $\mathsf{Enc}(\cdot, \mathsf{sk})$ (but does not know sk) cannot distinguish between ciphertexts $\chi \leftarrow \mathsf{Enc}(x_0, \mathsf{sk})$ and $\chi' \leftarrow \mathsf{Enc}(x_1, \mathsf{sk})$ with non-negligible probability in λ, where x_0 and x_1 are any plaintexts chosen by the adversary. That is

$$|\Pr[\mathfrak{A}^{\mathsf{Enc}(x_0,\mathsf{sk})}(x_0) = 1] - \Pr[\mathfrak{A}^{\mathsf{Enc}(x_0,\mathsf{sk})}(x_1) = 1]| \leq \mathrm{negl}(\lambda),$$

for all pairs (x_0, x_1).

The KLVY compilation procedure requires schemes that satisfy (1) and (2). QHE schemes satisfying (1) and (2) have been described in [21, 8].

A.2 Proofs

Proof of Lemma 2. Let $V_y^{(\lambda)} : \mathcal{H}'^{(\lambda)} \to \mathbb{C}^{|\mathcal{B}|} \otimes \mathcal{H}'^{(\lambda)}$ be the isometry defined by

$$V_y^{(\lambda)}|\phi\rangle = \sum_{b\in\mathcal{B}} |b\rangle \otimes \sqrt{N_{b|y}'^{(\lambda)}}|\phi\rangle, \ \forall|\phi\rangle \in \mathcal{H}'^{(\lambda)}. \tag{30}$$

Furthermore, let $U_y^{(\lambda)}$ be the unitary which satisfies $U_y^{(\lambda)}(|0\rangle \otimes |\phi\rangle) = V_y^{(\lambda)}|\phi\rangle$ for all $|\phi\rangle \in \mathcal{H}'^{(\lambda)}$. Define the projectors,

$$\tilde{N}_{b|y}^{(\lambda)} := U_y^{(\lambda)\dagger}(|b\rangle\langle b| \otimes \mathbb{I})U_y^{(\lambda)}. \tag{31}$$

Since $|\mathcal{B}|$ is constant with respect to λ and each $N_{b|y}'^{(\lambda)}$ is QPT, the resulting PVMs $\{\tilde{N}_{b|y}^{(\lambda)}\}_{b\in\mathcal{B}}$ are QPT for every $y \in \mathcal{Y}$. For the sub-normalized states, let $|\tilde{\Psi}_{\alpha|\chi}\rangle \in \mathcal{H}'^{(\lambda)} \otimes \tilde{\mathcal{H}}^{(\lambda)}$ be any purification[3] of $\rho_{\alpha|\chi}^{(\lambda)}$ with $\mathcal{H}'^{(\lambda)} \cong \tilde{\mathcal{H}}^{(\lambda)}$, and define

$$|\Psi_{\alpha|\chi}^{(\lambda)}\rangle := |0\rangle \otimes |\tilde{\Psi}_{\alpha|\chi}^{(\lambda)}\rangle \in \mathbb{C}^{|\mathcal{X}|} \otimes \mathcal{H}'^{(\lambda)} \otimes \tilde{\mathcal{H}}^{(\lambda)} =: \mathcal{H}^{(\lambda)}. \tag{32}$$

Again, since $|\mathcal{X}|$ is constant with respect to λ the (sub-normalized) states $|\Psi_{\alpha|\chi}^{(\lambda)}\rangle$ are QPT-preparable. Now, extend each $\tilde{N}_{b|y}^{(\lambda)}$ to act trivially on the purifying system $\tilde{\mathcal{H}}^{(\lambda)}$ by defining $N_{b|y}^{(\lambda)} := \tilde{N}_{b|y}^{(\lambda)} \otimes \mathbb{I}$. We observe

$$\begin{aligned} \mathrm{tr}\big[N_{b|y}^{(\lambda)}|\Psi_{\alpha|\chi}^{(\lambda)}\rangle\langle\Psi_{\alpha|\chi}^{(\lambda)}|\big] &= \mathrm{tr}\Big[\tilde{N}_{b|y}^{(\lambda)}\mathrm{tr}_{\tilde{Q}}[|\Psi_{\alpha|\chi}^{(\lambda)}\rangle\langle\psi_{\alpha|\chi}^{(\lambda)}|]\Big] \\ &= \mathrm{tr}[\tilde{N}_{b|y}^{(\lambda)}(|0\rangle\langle 0| \otimes \rho_{\alpha|\chi}^{(\lambda)})] \\ &= \mathrm{tr}\big[\big(|b\rangle\langle b| \otimes \mathbb{I}\big)U_y^{(\lambda)}\big(|0\rangle\langle 0| \otimes \rho_{\alpha|\chi}\big)U_y^{(\lambda)\dagger}\big] \\ &= \mathrm{tr}\Big[\sqrt{N_{b|y}'^{(\lambda)}}\rho_{\alpha|\chi}^{(\lambda)}\sqrt{N_{b|y}'^{(\lambda)}}\Big] = p^{(\lambda)}(\alpha, b|\chi, x), \end{aligned} \tag{33}$$

where $\tilde{Q}$ denotes the purifying system $\tilde{\mathcal{H}}^{(\lambda)}$. Since $\tilde{\mathcal{H}}^{(\lambda)}$ has the same dimensions as $\mathcal{H}^{(\lambda)}$, the PVMs $N_{b|y}^{(\lambda)}$ are indeed QPT. ◀

[3] Strictly speaking, since $\rho_{\alpha|\chi}^{(\lambda)}$ is sub-normalized, $|\tilde{\Psi}_{\alpha|\chi}^{(\lambda)}\rangle$ is equal to the purification of $\rho_{\alpha|\chi}^{(\lambda)}/tr[\rho_{\alpha|\chi}^{(\lambda)}]$ weighted by $\mathrm{tr}[\rho_{\alpha|\chi}^{(\lambda)}]$, whenever $\mathrm{tr}[\rho_{\alpha|\chi}^{(\lambda)}] > 0$.

Proof of Theorem 3. To begin, we write

$$\begin{aligned}\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[P^\dagger P] &= \sum_{ij} \gamma_i^* \gamma_j \tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[(A_x)^{k_i} w_i(B_0,B_1)(A_x)^{k_j} w_j(B_0,B_1)] \\ &= \sum_{ij} \gamma_i^* \gamma_j \tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[(A_x)^{k_i+k_j} \bar{w}_{ij}(B_0,B_1)],\end{aligned} \tag{34}$$

where we used the linearity of $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[\cdot]$ in the first line, and in the second line we used the fact that $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[w] = \tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[\bar{w}]$ (where $\bar{w}$ is the canonical form of the monomial w), and defined $\bar{w}_{ij}$ to be the canonical form of $w_i w_j$. We now need to consider two types of terms. First, when $k_i \oplus k_j = 0$, we apply the definition in Equation (12) in conjunction with Lemma 1 to write

$$\begin{aligned}&\sum_{ij:k_i\oplus k_j=0} \gamma_i^* \gamma_j \tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[\bar{w}_{ij}(B_0,B_1)] \\ &= \mathop{\mathbb{E}}_{x'\in\mathcal{X}} \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x')=\chi} \sum_\alpha \langle\Psi_{\alpha|\chi}| \left(\sum_{ij:k_i\oplus k_j=0} \gamma_i^*\gamma_j \bar{w}_{ij}(B_0,B_1) \right) |\Psi_{\alpha|\chi}\rangle \\ &\approx_{\mathrm{negl}(\lambda)} \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_\alpha \langle\Psi_{\alpha|\chi}| \left(\sum_{ij:k_i\oplus k_j=0} \gamma_i^*\gamma_j \bar{w}_{ij}(B_0,B_1) \right) |\Psi_{\alpha|\chi}\rangle \\ &= \sum_{ij:k_i\oplus k_j=0} \gamma_i^*\gamma_j \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_\alpha \langle\Psi_{\alpha|\chi}|\bar{w}_{ij}(B_0,B_1)|\Psi_{\alpha|\chi}\rangle.\end{aligned} \tag{35}$$

When $k_i \oplus k_j = 1$, we can apply Equation (13) directly. Putting these two together, we observe

$$\begin{aligned}&\sum_{ij} \gamma_i^*\gamma_j \tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[(A_x)^{k_i+k_j}\bar{w}_{ij}(B_0,B_1)] \\ &= \sum_{ij:k_i\oplus k_j=0} \gamma_i^*\gamma_j \tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[\bar{w}_{ij}] + \sum_{ij:k_i\oplus k_j=1} \gamma_i^*\gamma_j \tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[A_x\bar{w}_{ij}] \\ &\approx_{\mathrm{negl}(\lambda)} \sum_{ij:k_i\oplus k_j=0} \gamma_i^*\gamma_j \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_\alpha \langle\Psi_{\alpha|\chi}|\bar{w}_{ij}(B_0,B_1)|\Psi_{\alpha|\chi}\rangle \\ &+ \sum_{ij:k_i\oplus k_j=1} \gamma_i^*\gamma_j \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_\alpha (-1)^{\mathsf{Dec}(\alpha)} \langle\Psi_{\alpha|\chi}|\bar{w}_{ij}(B_0,B_1)|\Psi_{\alpha|\chi}\rangle \\ &= \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_\alpha \langle\Psi_{\alpha|\chi}| \sum_{ij} (-1)^{\mathsf{Dec}(\alpha)\cdot(k_i+k_j)} \gamma_i^*\gamma_j w_i(B_0,B_1) w_j(B_0,B_1) |\Psi_{\alpha|\chi}\rangle \\ &= \mathop{\mathbb{E}}_{\chi:\mathsf{Enc}(x)=\chi} \sum_\alpha \langle\Psi_{\alpha|\chi}| \Big| \sum_i (-1)^{\mathsf{Dec}(\alpha)\cdot k_i} \gamma_i w_i(B_0,B_1) \Big|^2 |\Psi_{\alpha|\chi}\rangle \geq 0.\end{aligned} \tag{36}$$

Where in the fifth line, we used the fact that Bob's observables satisfy the canonical relations, so we can always replace the canonical monomial $\bar{w}_{ij}$ with $w_i w_j$. The final line is obtained by noting the square inside the expectation. We therefore conclude $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[P^\dagger P] \approx_{\mathrm{negl}(\lambda)} h$ for some $h \geq 0$, which implies $|\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[P^\dagger P] - h| \leq \mathrm{negl}(\lambda)$, and $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}[P^\dagger P] \geq h - \mathrm{negl}(\lambda) \geq -\mathrm{negl}(\lambda)$ as required. Lastly, it is straightforward to verify from the definition that for any Bell functional I we have $\tilde{\mathbb{E}}_{\widetilde{\mathrm{Q}}}(I)$ recovers the expected value under $\widetilde{\mathrm{Q}}$. ◀