Quantum bounds for compiled XOR games and d-outcome CHSH games

Matilde Baroni[1], Quoc-Huy Vu[2], Boris Bourdoncle[3], Eleni Diamanti[1], Damian Markham[1], and Ivan Šupić[1]

[1]Sorbonne Université, CNRS, LIP6, 4 place Jussieu, 75005 Paris, France
[2]De Vinci Higher Education, De Vinci Research Center, Paris, France
[3]Quandela, 7 Rue Léonard de Vinci, 91300 Massy, France

arXiv:2403.05502v4 [quant-ph] 17 Oct 2025

Nonlocal games play a crucial role in quantum information theory and have numerous applications in certification and cryptographic protocols. Kalai et al. (STOC 2023) introduced a procedure to compile a nonlocal game into a single-prover interactive proof, using a quantum homomorphic encryption scheme, and showed that their compilation method preserves the classical bound of the game. Natarajan and Zhang (FOCS 2023) then showed that the quantum bound is preserved for the specific case of the CHSH game. Extending the proof techniques of Natarajan and Zhang, we show that the compilation procedure of Kalai et al. preserves the quantum bound for two classes of games: bipartite XOR games and a higher dimensional generalization of CHSH (the SATWAP inequality), that we refer to as d-outcome CHSH games. We also establish that, for any pair of qubit measurements, there exists a compiled XOR game such that its near-optimal winning probability serves as a robust self-test for that particular pair of measurements. Finally, we derive computational self-testing of three anticommuting qubit observables, based on the compilation of the nonlocal game corresponding to the so-called elegant Bell inequality.

1 Introduction

In quantum information theory, nonlocal games are a class of games that exemplifies the separation between classical and quantum resources. In such games, a referee sends classical inputs to two or more distant parties, and the parties reply with classical outputs. A predicate on the tuples of inputs and outputs defines the winning conditions for the game. In some cases, if the distant parties have access to quantum resources, namely entangled states, they can achieve a score higher than if they only have classical resources. Building on the work of Bell [1], Clauser, Horne, Shimony and Holt introduced the setting for the most famous example of such a game, the CHSH game [2]. While players with classical resources can only reach a maximal value of 0.75, players sharing entanglement can obtain a value of $\cos^2(\pi/8)$.

In addition to its far-reaching foundational interest, Bell nonlocality [3] enjoys a rich array of applications concerned with the certification of quantum resources and cryptographic tasks, such as device-independent quantum key distribution [4, 5, 6], certified randomness [7, 8, 9], self-testing [10, 11] and protocols for verifiable blind delegated quantum computing [12, 13]. All these protocols are characterized by information-theoretic security. Bell nonlocality is also connected to the powerful notion of multiprover interactive proof systems in quantum complexity theory, MIP*, in which two or more non-communicating provers are allowed to share quantum entanglement. In the classical setting, techniques and results from studying MIP (the classical version of MIP*) usually also find applications in the cryptographic setting, where all parties are computationally bounded, such as the celebrated PCP theorem [14] and succinct arguments [15, 16].

The framework of Bell nonlocality however requires at least two non-communicating parties, and the strongest guarantees of information-theoretic security can thus only be achieved if these parties are spatially separated, which is experimentally very challenging. While effective for foundational proofs of quantumness, applying such setups to computing platforms faces challenges due to their incompatibility

Matilde Baroni: matilde.baroni@lip6.fr

with Bell-type scenarios. From a pragmatical point of view, if one wants to certify resources on a quantum computer as it is an integral device, spatial separation and the absence of communication cannot be imposed. Thus, a possibility to translate certification tools requiring two or more spatially separated devices to single device setting would significantly boost their applicability. Interestingly, in the other area where Bell nonlocality finds its application, namely quantum computational complexity that we commented above, there has been a progress in moving from two non-communicating provers to a single one. Crucially, a series of works [17, 18] showed that, using a homomorphic encryption scheme, any MIP sound against non-signalling provers can be compiled into a single-prover protocol in which the single prover is computationally bounded and restrained by cryptographic tools.

Cryptography seems to offer a very promising tool: (quantum) homomorphic encryption, which allows to perform computations on encrypted (quantum) data without decrypting them. This could be used to mimic spatial separation by hiding to the single prover the complete knowledge of the inputs, which would otherwise make the game trivial. Kalai, Lombardi, Vaikuntanathan and Yang formalised in [19] the idea of using quantum homomorphic encryption [20, 21] to emulate spatial separation between the nonlocal parties. They propose a procedure (see Figure 1) to compile every k-players nonlocal game into a single-prover interactive proof of $2k$-rounds, by fixing a sequential structure of the input-output requests and encrypting the first $k-1$ rounds. They then prove: (i) the *completeness* of the procedure, that is, there is an explicit and efficient quantum strategy that achieves the quantum bound of the original nonlocal game; and (ii) its *classical soundness*, that is, no classical prover can outperform the optimal classical bound up to a negligible function in the security parameter, which is the advantage of the classical adversary in the indistinguishability (IND-CPA) security game of the encryption scheme.

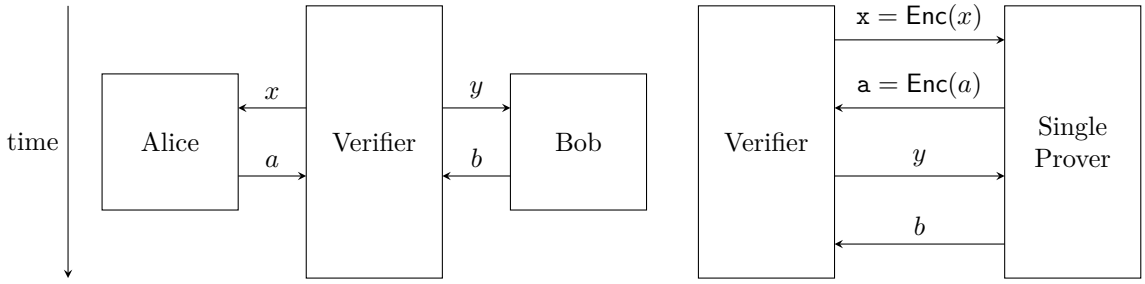


Figure 1: Pictorial representation of the Kalai *et. al.* compilation protocol for 2-player nonlocal games. On the left, a general 2-player nonlocal game; the two parties are spatially separated, and only communicate to a classical verifier which is sampling questions (x, y) and collecting their answers (a, b). On the right, the single prover game resulting from the compilation procedure. In this representation, time flows downwards.

However [19] does not provide an upper bound to the optimal score of a quantum prover. Indeed they use classical rewinding techniques to show the soundness against classical adversaries, which is no longer possible against quantum provers. Follow-up works by Natarajan and Zhang [22] and Brakerski *et al.* [23] prove that the quantum bound is preserved in the specific case of the compiled CHSH game. Their proofs heavily relies on specific properties of CHSH, providing little insight on whether Kalai *et al.* compiler preserves the quantum bound for any other nonlocal games.

1.1 Our Contributions

In this work, we continue this research direction and provide a partial answer for the above open question. In particular, we prove that the quantum bound is preserved for two classes of compiled games: XOR games, where the predicate depends on the logical XOR of the outputs, and d-outcome CHSH games, that generalise the CHSH game to a scenario involving many-output measurements. We also extend our results to self-testing, which relies on the fact that for specific non-local games there is a unique strategy that can achieve the optimal quantum score; then, reaching this bound is a device-independent certification of quantum resources.

The techniques we use are based on the cryptographic SOS decomposition delineated in [22]. The score of a nonlocal game is usually formulated as the expectation value of some function of the observables of the players. This is closely related to the Bell operator $\mathcal{B}$, and its shifted version $\beta\mathbb{1} - \mathcal{B}$, where β is what we call the shift. SOS decomposition - standing for sum of squares - is a method widely used in Bell nonlocality to prove quantum bounds. It consists on mathematically rearranging the terms of the

shifted Bell operator as a sum of polynomials squared, whose expectation value is positive semi-definite by definition.

$$\langle\psi|\beta\mathbb{1}-\mathcal{B}|\psi\rangle=\sum_i\langle\psi|P_i^2|\psi\rangle\geq 0 \implies \langle\psi|\mathcal{B}|\psi\rangle\leq\beta$$

Hence the shifted Bell operator is also positive semi-definite, meaning that the shift β is an upper bound for the optimal quantum score. The bound becomes tight if an explicit quantum strategy achieving β is found. If the polynomials appearing in the decomposition are of degree n, then we say we have a nth-order SOS decomposition.

We consider the the pseudo-expectation value map $\tilde{\mathbb{E}}$ defined in [22], that maps polynomials of nonlocal observables to correlations observed in the compiled nonlocal game. This function allows to translate the SOS decomposition proof from the nonlocal to the compiled game. For polynomials of observables with a physical interpretation, the map corresponds to a simple change of variables, compatible with the structure of the compiled game; therefore it acts trivially on the identity, and when applied to the Bell functional it gives the score of the compiled game. The name pseudo-expectation refers to the fact that it is not a positive semi-definite function by definition. In particular, the pseudo-expectation of the polynomials squared from the SOS decomposition is not positive by definition anymore. Nevertheless, elaborating on the results of [22], we prove that - for specific polynomials - these quantities are still positive up to a negligible function in the security parameter κ of the QHE scheme.

Result (informal) 1. *Consider a Bell inequality $\mathcal{B}$ with a SOS decomposition, whose polynomials can be written as $P_i = A_i - \hat{B}_i$, where $\{A_i\}_i$ are Alice's observables and $\{\hat{B}_i\}_i$ are linear sums of Bob's observables. Then there exists a negligible function negl$(\cdot)$ such that $\tilde{\mathbb{E}}\left[P_i^2\right]\geq -negl(\kappa)$.*

Technically, this is done by extending cryptographic arguments based on the security of the encryption scheme. Then, applying the pseudo-expectation map to the nonlocal SOS decomposition, we prove that the quantum bound of the compiled game is preserved up to a negligible function in the security parameter.

$$\tilde{\mathbb{E}}[\beta\mathbb{1}-\mathcal{B}]=\sum_i\tilde{\mathbb{E}}[P_i^2]\geq -\mathrm{negl}(\kappa) \implies \tilde{\mathbb{E}}[\mathcal{B}]\leq\beta+\mathrm{negl}(\kappa)$$

The pseudo-expectation map is well defined for polynomials of degree 2 in the number of observables, restricting us to work with first-order SOS decompositions. We lack of a meaningful interpretation for polynomials containing two different Alice's observables in the compiled scenario, but we can fix the shape of the SOS polynomials P_i to contain only one observable for Alice for several non-local games of interest.

In particular, in the paper we revise some known results for XOR games, and derive a new result on the decomposition of the shifted game operator. Notably, we prove that it is always possible to have a decomposition with polynomials P_i containing only one Alice's observable. This helps us to prove that the quantum score of all XOR games is preserved by Kalai *et al.* compilation.

Result (informal) 2. *Given a bipartite XOR game with optimal quantum winning probability ω_q, the optimal quantum winning probability of the compiled XOR game is $\omega_q + negl(\kappa)$.*

We also extend the pseudo-expectation map to treat higher dimensional inputs and outputs, hence generalised observables. As an example we apply it to the SATWAP inequality proposed in [24], a generalisation of CHSH for which we know there exists a SOS decomposition in our desired form [25]. We prove that the quantum score of the compiled game is preserved in this case as well. Apart from its mathematical relevance, this could lead to much more efficient certifications.

Result (informal) 3. *Consider the d-dimensional SATWAP Bell inequality $\mathcal{B}_d$ with quantum bound $\omega_q(\mathcal{B}_d)$, and its compiled version. If d is polynomial w.r.t. the security parameter κ, then the quantum bound of the compiled SATWAP inequality is $\omega_q(\mathcal{B}_d) + negl(\kappa)$.*

The SOS decomposition imposes constraints on the strategies achieving the optimal quantum score; sometimes these constraints are enough to uniquely identify these strategies, leading to self-testing protocols. From the cryptographic SOS decomposition we develop computational self-testing techniques for interactive single prover games, built on top of the nonlocal self-testing proofs.

We show that for any pair of single-qubit observables, there is a tailored XOR game whose compiled version forces the prover's device to implement (up to isometry) that specific pair.

Result (informal) 4. *For every pair of qubit observables , there exists an XOR game G such that any polynomial-time prover in the compiled protocol G' who wins with probability at least $\omega_q(G) - \varepsilon$ must implement measurement operators within $O(\sqrt{\varepsilon}, negl(\kappa))$, up to a local isometry.*

Our construction begins with the well-known information-theoretic self-test of two arbitrary qubit measurements via a suitable Bell inequality, then embeds it into the KLVY framework. A careful soundness analysis shows that the usual robust-self-testing error bounds degrade only by a negligible factor in κ. To our knowledge, this is the first computational self-test of arbitrary two qubit measurement observables in a single-prover setting.

Beyond pairs of observables, practical quantum certification often demands a full Bloch-sphere basis. We give the first compiled protocol that self-tests three anti-commuting qubit observables, equivalently, the Pauli set $\sigma_x, \sigma_y, \sigma_z$ through interaction with a single prover.

Result (informal) 5. *There is a single-prover compiled protocol, based on the elegant Bell inequality, such that any efficient prover achieving winning probability within δ of the quantum optimum must implement three anti-commuting Pauli measurements $\sigma_x, \sigma_y, \sigma_z$ up to $O(\delta, negl(\kappa))$ error and local isometry.*

Our analysis combines the elegant inequality's tight self-testing features with the general compilation machinery. The result provides a complete toolkit for certifying an arbitrary single-qubit state or operation under standard cryptographic assumptions.

1.2 Outline of the paper

The paper is structured in the following way. Section 2 is dedicated to preliminary notions. We introduce nonlocal games and Bell inequalities, with a focus on a sub-class: XOR games. For these, in Section 2.2 we revise some known results and derive a new result on the decomposition of the shifted game operator. Then, we introduce quantum homomorphic encryption and Kalai's compilation protocol [19]. We elaborate on the results of [22], in particular on their idea of defining a pseudo-expectation value that maps polynomials of measurement observables to correlations observed in the compiled nonlocal game.

The second part focuses on those cases for which we can prove that such a pseudo-expectation map can be used to upper bound the optimal quantum winning probabilities in compiled nonlocal games. In Section 3 we use the decomposition introduced in the preliminaries to prove the soundness of the quantum bound for any compiled XOR game. Section 4 generalizes our approach to encompass an inequality with a higher number of outputs. Finally, in section 5 we develop computational self-testing techniques for interactive single prover games, built on top of the nonlocal self-testing proofs. In particular, we show that a certain class of compiled XOR games can be used to self-test any pair of qubit measurements. Furthermore we introduce a compiled game which can self-test all three anti-commuting qubit observables.

1.3 Concurrent and independent work

While finishing this manuscript we became aware of a recent work by Cui *et al.* [26] who also show that the compilation procedure of Kalai et al. [19] preserves the quantum bias of all XOR games. Even though both papers use a similar techniques based on [22], [26] and our work also achieve different results. Their work shows a type of self-testing result for all compiled XOR games, while we explore the self-testing properties of carefully designed compiled XOR games, such that any pair of qubit measurements and tomographically complete sets of qubit measurements can be self-tested from the optimal winning probability. The work of Cui *et al.* explores the compilation of parallelly repeated XOR games and the Magic Square game, while we work with the compiled d-CHSH game which cannot be seen as a parallel repetition of XOR games.

1.4 Subsequent works

For completeness, we also highlight subsequent works that advanced our understanding on the quantum soundness of compiled games.

In [27] the authors use similar techniques to show that the quantum bound of the tilted CHSH inequality is preserved under the compilation; this was the first example of an inequality not maximized by a maximally entangled state. Furthermore, they contribute in formalizing which kind of self-testing statements can be potentially derived from compiled games.

In [28], a new algebraic framework is introduced, leading to show that for all bipartite games the compiled quantum value is asymptotically (with respect to the security of the cryptographic scheme)

bounded by the quantum commuting operator value. This elegant general result provides a new point-of-view on compiled games; however it is an asymptotic result, hence it cannot be directly applied to practical scenarios, because it only holds in the case of perfect security. Many interesting questions are still open. How can we make this result more practical, i.e. when is it possible to estimate the value of the compiled game for a finite level of security and the speed of convergence? How to extend the same techniques to games for more than 2 players?

2 Preliminaries

2.1 Nonlocal games and Bell inequalities

In a two-party nonlocal game, a referee randomly selects questions, also called inputs, according to a predetermined distribution and sends them to the non-communicating parties, usually called Alice and Bob. Upon receiving the answers, also called outputs, from Alice and Bob, the referee determines whether they won or lost based on the game rule, which is public. Winning is nontrivial because the players can't communicate during the game: they must generate their output solely based on their respective inputs and potentially a shared resource. $x \in \mathsf{X}$ and $y \in \mathsf{Y}$ denote the questions sent to Alice and Bob, respectively, $a \in \mathsf{A}$ and $b \in \mathsf{B}$ denote their respective answers. $|\cdot|$ denotes the cardinality of a set. The referee samples the questions from a distribution $q(x, y)$, and the game rule is a predicate $V : (a, b, x, y) \mapsto \{0, 1\}$. Alice and Bob define a strategy to answer the questions, based on the resources that they have, and the conditional probabilities of obtaining outputs a and b when inputting x and y, is denoted by $p(a, b|x, y)$. The winning probability of the game is then given by:

$$\omega = \sum_{x,y} q(x, y)V(a, b, x, y)p(a, b|x, y). \tag{1}$$

If Alice and Bob use classical resources, in the most general case they can share a random variable t sampled from a distribution $p(t)$, and they can determine their respective output based on the value of t and the received input. In the context of Bell nonlocality, such strategy corresponds to a local hidden variable model (LHV). In that case, the maximal winning probability is called the classical score of the game. Alice and Bob can always reach the maximal winning probability with deterministic response functions $f(x, t)$, $g(y, t)$ to choose their outputs [29], and the maximal classical score is then equal to:

$$\omega_c = \max_{f,g} \sum_{x,y,t} p(t)q(x, y)V(f(x, t), g(y, t), x, y). \tag{2}$$

If Alice and Bob have access to quantum resources, they can share a quantum state $|\psi\rangle$ and perform quantum measurements on it. For each output, they can perform a different measurement, meaning that Alice has $|\mathsf{X}|$ different measurements, one for each for each x, characterized by $|\mathsf{A}|$ operators $\{M_{a|x}\}_a$, such that:

$$M_{a|x} \succeq 0 \qquad \forall x \in \mathsf{X}, \forall a \in \mathsf{A} \tag{3}$$

$$\sum_{a \in \mathsf{A}} M_{a|x} = \mathbb{1} \qquad \forall x \in \mathsf{X}. \tag{4}$$

Bob's measurements are defined similarly and denoted by $\{N_{b|y}\}_b$. The probability that Alice and Bob get outputs a and b, given inputs x and y is determined by the Born rule $p(a, b|x, y) = \langle\psi|M_{a|x} \otimes N_{b|y}|\psi\rangle$. In that case, the winning probability is equal to:

$$\omega = \sum_{x,y} q(x, y)V(a, b|x, y)\langle\psi|M_{a|x} \otimes N_{b|y}|\psi\rangle. \tag{5}$$

and the maximal quantum score is given by:

$$\omega_q = \max_{\{M_{a|x}\}_x, \{N_{b|y}\}_y, |\psi\rangle} \omega. \tag{6}$$

Note that, more generally, Alice and Bob could have access to a mixed state ρ, but since we don't impose any restriction on the dimension of the underlying Hilbert space, any score reachable with a mixed state can also be reached with a pure state by increasing the dimension of the Hilbert space.

If players output bits, i.e. $\mathsf{A} = \mathsf{B} = \{0, 1\}$, the game is said to be binary, and the quantum strategies can be characterised in a simpler way: their measurements are defined by the Hermitian measurement observables

$$A_x = \sum_a (-1)^a M_{a|x}, \qquad B_y = \sum_b (-1)^b N_{b|y}. \tag{7}$$

In the rest of the paper, we use the following notations:

$$|A_x\rangle = A_x|\psi\rangle, \qquad |A\rangle = \sum_x |A_x\rangle \otimes |x\rangle, \tag{8}$$

$$|B_y\rangle = B_y|\psi\rangle, \qquad |B\rangle = \sum_y |B_y\rangle \otimes |y\rangle, \tag{9}$$

which allows us to express the players' correlations through a correlation matrix as:

$$C = \sum_{x,y} c_{xy}|x\rangle\langle y| \qquad \text{with } c_{xy} = \langle A_x|B_y\rangle. \tag{10}$$

Nonlocal games are closely related to Bell inequalities [30, 31]. A Bell inequality can be defined via a linear form on the space of the conditional distributions $p(a, b|x, y) \in \mathbb{R}^{|A||B||X||Y|}$:

$$\sum_{a,b,x,y} \gamma_{a,b,x,y} p(a, b|x, y) \leq \beta_c, \tag{11}$$

where $\{\gamma_{a,b,x,y}\}_{a,b,x,y}$ is a fixed set of complex coefficients; different coefficients identifies different inequalities.

Importantly, the quantum Bell score can be written as $\beta = \langle\psi|\mathcal{B}|\psi\rangle$ where $\mathcal{B}$ is the Bell operator

$$\mathcal{B} = \sum_{a,b,x,y} \gamma_{a,b,x,y} M_{a|x} \otimes N_{b|y}. \tag{12}$$

When there is a gap between the maximal classical and quantum scores, the quantum strategies that achieve a score higher than the classical value also violate a Bell inequality. For instance, the quantum state and measurements yielding the maximal value for the CHSH game also yield the maximal quantum value, known as Tsirelson's bound, for the CHSH inequality. In the remainder of this paper, we sometimes switch between the nonlocal game and the Bell inequality formulations. The local bound of a Bell inequality will be denoted with β_c, while the maximal value considering quantum strategy will be denoted as β_q. For a Bell inequality with quantum bound β_q we will often use the shifted Bell operator

$$\beta_q \mathbb{1} - \mathcal{B}, \tag{13}$$

which is by construction positive semi-definite.

2.2 XOR games

XOR games are a subclass of nonlocal games with binary outputs, in which the winning conditions for each pair of inputs depend only on the parity of the two output bits, i.e. there is a function f such that $V(a, b, x, y) = 1$ if and only if $f(x, y) = a \oplus b$. Hence, the winning probability takes the form

$$\omega = \sum_{a,b,x,y} q(x, y)\delta_{a\oplus b=f(x,y)} p(a, b|x, y).^{1} \tag{14}$$

The winning probability of an XOR game is connected to its bias

$$\xi = \sum_{x,y} q(x, y)(-1)^{f(x,y)} c_{x,y}, \tag{15}$$

[1] Here δ denotes the Kronecker function.

through the relation $\omega = (1+\xi)/2$. The term "bias" comes from the fact that in XOR games, the score 1/2 can be achieved by players that do not use any resources, but randomly output their bits, independently of the inputs. An XOR game can be characterized by its so-called game matrix Φ:

$$\Phi = \sum_{x,y} q(x,y)(-1)^{f(x,y)}|x\rangle\langle y|. \tag{16}$$

The bias can then be compactly written as $\xi = \mathrm{Tr}\left[C^T\Phi\right]$. We can also define the operator associated to an XOR game as

$$\mathcal{B}_g = \sum_{x,y} q(x,y)(-1)^{f(x,y)} A_x \otimes B_y, \tag{17}$$

and the bias can then be computed as the expectation value of the corresponding game operator $\xi = \langle\psi|\mathcal{B}_g|\psi\rangle$. From this game operator, one obtains a valid Bell operator by simply multiplying the r.h.s. of eq. (17) with $|\mathsf{X}|\cdot|\mathsf{Y}|$.

Lemma 1 ([32])**.** *Alice's optimal quantum strategy in an XOR game, encoded in the vector $|A_q\rangle$, is fully determined by Bob's optimal strategy $|B_q\rangle$ through a linear transformation:*

$$|A_q\rangle = \mathbb{1}\otimes F|B_q\rangle. \tag{18}$$

Proof. This lemma was proven by Tsirelson in [32], but we reproduce here the proof of [33]. The optimal quantum bias of an XOR game can be obtained as the solution to a semidefinite program (SDP) [34]. For that purpose let us define the Gram matrix $\tilde{Q}$

$$\tilde{Q} = \left[\begin{array}{c|c} R & C \\ \hline C^T & S \end{array}\right], \text{ with } R = \sum_{x,x'}\langle A_x|A_{x'}\rangle|x\rangle\langle x'|, \text{ and } S = \sum_{y,y'}\langle B_y|B_{y'}\rangle|y\rangle\langle y'|. \tag{19}$$

Every Gram matrix is positive semidefinite and has 1-s on the diagonal. Thus, the SDP yielding the optimal quantum bias for an XOR game takes the form

$$\begin{aligned} \xi_q = &\max_{\tilde{Q}} \mathrm{Tr}\left[\tilde{Q}\tilde{\Phi}\right], \\ \text{s.t.} \quad &\tilde{Q}_{ii} = 1, \quad \text{for} \quad i = 1,\cdots,|\mathsf{X}|+|\mathsf{Y}|, \\ &\tilde{Q} \succeq 0, \end{aligned} \tag{20}$$

where $\tilde{\Phi} = \frac{1}{2}\begin{pmatrix} 0 & \Phi \\ \Phi^T & 0 \end{pmatrix}$. From this primal form of the SDP, we can obtain the dual formulation by introducing the Lagrangian $\mathcal{L} = \mathrm{Tr}[\tilde{Q}\tilde{\Phi}] - \frac{1}{2}\sum_i \lambda_i(\mathrm{Tr}\left[|i\rangle\langle i|\tilde{Q}\right] - 1)$, where λ_i are nonnegative Lagrangian multipliers. Let us define the diagonal matrix $\Lambda = \mathrm{diag}(\lambda_1,\cdots,\lambda_{|\mathsf{X}|+|\mathsf{Y}|})$. The minimal value of the Lagrangian upper bounds the solution to the primal SDP if $\frac{1}{2}\Lambda - \tilde{\Phi} \succeq 0$, so the dual SDP takes the form

$$\min \mathrm{Tr}\left[\frac{\Lambda}{2}\right], \qquad \text{s.t.} \quad \frac{\Lambda}{2} - \tilde{\Phi} \succeq 0. \tag{21}$$

As a consequence of the aforementioned construction, it can be deduced that any given pair of primal and dual feasible solutions satisfy $\mathrm{Tr}[\tilde{Q}\tilde{\Phi}] \leq \xi_q \leq \mathrm{Tr}[\Lambda]/2$. The optimal values of the primal and of the dual coincide if strong duality holds. A sufficient condition for strong duality to hold, when the primal and dual are finite, is the existence of a strictly feasible solution to the dual problem, which is satisfied here. Hence, the optimal value can be obtained if the complementary slackness condition is satisfied

$$\mathrm{Tr}\left[\tilde{Q}\left(\frac{1}{2}\Lambda - \tilde{\Phi}\right)\right] = 0. \tag{22}$$

Let us now introduce the notations $\Lambda = \Lambda_A \oplus \Lambda_B$, where Λ_A (Λ_B) is a diagonal $|\mathsf{X}|\times|\mathsf{X}|$ ($|\mathsf{Y}|\times|\mathsf{Y}|$) matrix, and $|Q\rangle = |A\rangle \oplus |B\rangle$. We can write the quantum bias as $\xi = \langle Q|\mathbb{1}\otimes\tilde{\Phi}|Q\rangle$. The slackness condition (22) gives $\mathrm{Tr}\left[\mathbb{1}\otimes\left(\frac{1}{2}\Lambda - \tilde{\Phi}\right)|Q\rangle\langle Q|\right] = 0$, or equivalently $\mathbb{1}\otimes(\frac{1}{2}\Lambda - \tilde{\Phi})|Q\rangle = 0$, since $\frac{1}{2}\Lambda - \tilde{\Phi}$ is positive semidefinite. The form of Λ and $\tilde{\Phi}$ implies the following conditions for the optimal strategies of Alice and Bob:

$$\mathbb{1}\otimes\Lambda_A|A_q\rangle = \mathbb{1}\otimes\Phi|B_q\rangle, \quad \text{and} \quad \mathbb{1}\otimes\Lambda_B|B_q\rangle = \mathbb{1}\otimes\Phi^T|A_q\rangle. \tag{23}$$

Taking $F = \Lambda_A^{-1}\Phi$ gives the desired result. □

Another convenient way to write the relations obtained above is

$$|A_x\rangle = \lambda_x^{-1} \sum_{y=1}^{m_B} \Phi_{xy} |B_y\rangle, \qquad \text{for } x = 1, \cdots, |\mathsf{X}|\,. \tag{24}$$

The matrix $\tilde{Q}$ can be seen as a moment matrix corresponding to the first level of Navascues-Pironio-Acín hierarchy (NPA) [35]. The n-th level NPA moment matrix is obtained by defining all degree-n monomials S_i of the operators from the set $\{A_1, \cdots, A_{|\mathsf{X}|}, B_1, \cdots, B_{|\mathsf{Y}|}\}$ and taking $\tilde{Q}^{(n)} = \langle\psi|S_i^\dagger S_j|\psi\rangle |i\rangle\langle j|$. Upper bounds on the maximal quantum score of an arbitrary nonlocal game can be obtained as solutions to an SDP analogous to (20), but taking $\tilde{Q}^n$ instead of $\tilde{Q}$ and the appropriate game matrix $\tilde{\Phi}$. The larger n is, the tighter the upper bound is. In the case of XOR games, the moment matrix of the first level of the NPA hierarchy actually suffices to find the exact optimal value, as it was proven in [36]. The dual formulation can be seen as an optimization over sum-of-squares (SOS) polynomials, given the duality theory between positive semidefinite moment matrices and SOS polynomials [37]. In the case of the NPA hierarchy the difference between the solutions of the dual and primal problems can be seen as the expectation value of an SOS polynomial $\sum_i S_i^\dagger S_i$, where S_i belongs to the monomials used to create the corresponding moment matrix [38]. For XOR games, this implies that for every Gram matrix $\tilde{Q}$ obtained by measuring the state $|\psi\rangle$, the following holds:

$$\xi_q - \mathrm{Tr}[\tilde{Q}\tilde{\Phi}] = \langle\psi| \sum_i P_i^\dagger P_i |\psi\rangle, \tag{25}$$

where the P_i-s are first degree polynomials over $\{A_1, \cdots, A_{|\mathsf{X}|}, B_1, \cdots, B_{|\mathsf{Y}|}\}$, i.e. $P_i = \sum_{x,y}(\alpha_x^i A_x + \beta_y^i B_y)$. As Eq. (25) holds for all quantum realizations, it can be written as

$$\xi_q \mathbb{1} - \mathcal{B}_g = \sum_i P_i^\dagger P_i, \tag{26}$$

where $\xi_q \mathbb{1} - \mathcal{B}_g$ is usually called the shifted game operator. The following theorem stipulates that for XOR games, the shifted game operator can be written as a sum of squares, with each term containing a single Alice operator, plus a positive polynomial depending only of Bob's operators.

Theorem 1. *Let $\mathcal{B}_g$ be the game operator of an XOR game with optimal quantum bias ξ_q. Then the following holds:*

$$\xi_q \mathbb{1} - \mathcal{B}_g = \sum_x \frac{\lambda_x}{2} \left(A_x - \sum_y F_{xy} B_y \right)^2 + P\left(\{B_y\}_y\right), \tag{27}$$

where F is the matrix of Lemma 1 and $P(\{B_y\}_y)$ is a positive polynomial over Bob's measurement operators.

To prove this theorem, we first use the following lemma proven by Ostrev.

Lemma 2. *[39]*

1. *Let $\lambda_1, \cdots, \lambda_{|\mathsf{X}|+|\mathsf{Y}|}$ be an optimal solution to the dual semidefinite program (21). Then there exist vectors $\{|u_i\rangle = \sum_{j=1}^{|\mathsf{X}|} u_{ij}|j\rangle\}_{i=1}^r$ and $\{|v_i\rangle = \sum_{j=1}^{|\mathsf{Y}|} v_{ij}|j\rangle\}_{i=1}^r$ such that*

$$\sum_{i=1}^r |u_i\rangle\langle u_i| = \frac{1}{2}\Lambda_A, \qquad \sum_{i=1}^r |v_i\rangle\langle v_i| = \frac{1}{2}\Lambda_B, \qquad \sum_{i=1}^r |u_i\rangle\langle v_i| = \frac{1}{2}\Phi. \tag{28}$$

2. *Let $|A\rangle$ and $|B\rangle$ be a quantum strategy for an XOR game. Let $\{|u_i\rangle = \sum_{j=1}^{|\mathsf{X}|} u_{ij}|j\rangle\}_{i=1}^r$ and $\{|v_i\rangle = \sum_{j=1}^{|\mathsf{Y}|} v_{ij}|j\rangle\}_{i=1}^r$ satisfy (28). Then the following identity holds:*

$$\sum_{i=1}^r \left\| \sum_{j=1}^{|\mathsf{X}|} u_{ij}|A_j\rangle - \sum_{j=1}^{|\mathsf{Y}|} v_{ij}|B_j\rangle \right\|^2 = \frac{1}{2}\mathrm{Tr}[\Lambda] - \sum_{ij} \langle A_i|\Phi_{ij}|B_j\rangle. \tag{29}$$

Proof. The interested reader can find the proof of the first part in [39] (Lemma 4 therein), we reproduce here the proof of the second part (Lemma 5 in [39]). The l.h.s. of (29) reads

$$\begin{aligned}
&\sum_{i=1}^{r}\left\|\sum_{j=1}^{|\mathsf{X}|}u_{ij}|A_j\rangle-\sum_{j=1}^{|\mathsf{Y}|}v_{ij}|B_j\rangle\right\|^2 = \\
&=\langle A|\mathbb{1}\otimes\left(\sum_{i=1}^{r}|u_i\rangle\langle u_i|\right)|A\rangle+\langle B|\mathbb{1}\otimes\left(\sum_{i=1}^{r}|v_i\rangle\langle v_i|\right)|B\rangle-2\langle A|\mathbb{1}\otimes\left(\sum_{i=1}^{r}|u_i\rangle\langle v_i|\right)|B\rangle = \\
&=\frac{1}{2}\langle A|\mathbb{1}\otimes\Lambda_A|A\rangle+\frac{1}{2}\langle B|\mathbb{1}\otimes\Lambda_B|B\rangle-\langle A|\left(\mathbb{1}\otimes\Phi\right)|B\rangle = \\
&=\frac{1}{2}\mathrm{Tr}[\Lambda_A]+\frac{1}{2}\mathrm{Tr}[\Lambda_B]-\langle A|\mathbb{1}\otimes\Phi|B\rangle,
\end{aligned}$$

which is exactly the second statement of the lemma, given that $\Lambda=\Lambda_A+\Lambda_B$. □

We now define a robust version of Ostrev's lemma.

Lemma 3. *1. Let $\lambda_1,\cdots,\lambda_{|\mathsf{X}|+|\mathsf{Y}|}$ be an optimal solution to the dual semidefinite program (21). Then there exist vectors $\{|u_i\rangle=\sum_{j=1}^{|\mathsf{X}|}u_{ij}|j\rangle\}_{i=1}^{r}$ and $\{|v_i\rangle=\sum_{j=1}^{|\mathsf{Y}|}v_{ij}|j\rangle\}_{i=1}^{r}$ such that*

$$\sum_{i=1}^{r}|u_i\rangle\langle u_i|=\frac{1}{2}\Lambda_A,\qquad\sum_{i=1}^{r}|v_i\rangle\langle v_i|\preceq\frac{1}{2}\Lambda_B,\qquad\sum_{i=1}^{r}|u_i\rangle\langle v_i|=\frac{1}{2}\Phi \tag{30}$$

2. Let $|A\rangle$ and $|B\rangle$ be a quantum strategy for an XOR game. Let $\{|u_i\rangle=\sum_{j=1}^{|\mathsf{X}|}u_{ij}|j\rangle\}_{i=1}^{r}$ and $\{|v_i\rangle=\sum_{j=1}^{|\mathsf{Y}|}v_{ij}|j\rangle\}_{i=1}^{r}$ satisfy (30). Then the following inequality holds:

$$\sum_{i=1}^{r}\left\|\sum_{j=1}^{|\mathsf{X}|}u_{ij}|A_j\rangle-\sum_{j=1}^{|\mathsf{Y}|}v_{ij}|B_j\rangle\right\|^2\leq\frac{1}{2}\mathrm{Tr}[\Lambda]-\sum_{ij}\langle A_i|\Phi_{ij}|B_j\rangle. \tag{31}$$

Proof. For the proof of the first part, we give an explicit construction of the vectors $|u_i\rangle$ and $|v_i\rangle$. We choose $u_{ij}=\sqrt{\frac{\lambda_i}{2}}\delta_{ij}$, where δ_{ij} is the Kronecker delta, and we take $|v_i\rangle=\frac{1}{\lambda_i}\sum_j\Phi_{ij}|u_j\rangle$. The first and third relations in (30) are satisfied, as $\sum_i|u_i\rangle\langle u_i|=\frac{1}{2}\mathrm{diag}(\lambda_1,\cdots,\lambda_{|\mathsf{X}|})$, and $\sum_i|u_i\rangle\langle v_i|=\frac{1}{2}\Phi$. Concerning the second relation, we get $\sum_i|v_i\rangle\langle v_i|=\frac{1}{2}\Phi^T\Lambda_A^{-1}\Phi$. To analyze it, we use the complementary slackness condition, which implies that $\Lambda-\tilde{\Phi}\succeq 0$. By Schur's complement lemma , this matrix is positive if and only if $\Lambda_B-\Phi^T\Lambda_A^{-1}\Phi\succeq 0$. This completes the proof of the first part of the lemma. The second part follows analogously to the second part of Lemma 2. □

We can now prove Theorem 1.

Proof. Taking the $|u_i\rangle$-s and $|v_i\rangle$-s used to prove the first part of Lemma 3 in (31), we get

$$\xi_q-\langle\psi|\mathcal{B}_g|\psi\rangle-\sum_{x=1}^{m_A}\frac{\lambda_x}{2}\left\|A_x|\psi\rangle-\lambda_x^{-1}\sum_y\Phi_{x,y}B_y|\psi\rangle\right\|^2\geq 0. \tag{32}$$

When opening the sum of squares, we get

$$\xi_q-\sum_{x=1}^{m_A}\frac{1}{\lambda_x}\langle\psi|\sum_{y,y'}B_y\Phi_{y,x}\Phi_{x,y'}B_{y'}|\psi\rangle\geq 0, \tag{33}$$

which holds for every valid quantum state $|\psi\rangle$, implying

$$2P\left(\{B_y\}_y\right)\equiv\xi_q\mathbb{1}-\sum_{x=1}^{m_A}\frac{1}{\lambda_x}\sum_{y,y'}B_y\Phi_{y,x}\Phi_{x,y'}B_{y'}\succeq 0. \tag{34}$$

The simple expansion of all the squares shows that

$$\xi_q\mathbb{1}-\mathcal{B}_g=\frac{\lambda_x}{2}\left(A_x-\lambda_x^{-1}\sum_y\Phi_{x,y}B_y\right)^2+P\left(\{B_y\}_y\right), \tag{35}$$

which together with (34) proves the theorem. □

2.3 Self-testing

Self-testing is a powerful technique that allows one to identify quantum states and measurements leading to the optimal winning probability in a nonlocal game. To be more precise, the score ω_q is said to self-test the state and measurements $|\psi'\rangle, \{M'_{a|x}\}, \{N'_{b|y}\}$ if for all states and measurements $\varrho_{\mathrm{AB}}, \{M_{a|x}\}, \{N_{b|y}\}$ allowed to reach ω_q there exists

(i) local Hilbert spaces $\mathcal{H}_{\mathrm{A}}$, $\mathcal{H}_{\mathrm{B}}$ such that $\varrho_{\mathrm{AB}} \in \mathcal{L}[\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}]$, $M_{a|x} \in \mathcal{L}[\mathcal{H}_{\mathrm{A}}]$, $N_{b|y} \in \mathcal{L}[\mathcal{H}_{\mathrm{B}}]$

(ii) a local isometry $\Phi = \Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}}$

such that for any purification $|\psi\rangle^{\mathrm{ABP}}$ of ϱ^{AB} it holds

$$\Phi \otimes \mathbb{I}_{\mathrm{P}} \left[M_{a|x} \otimes N_{b|y} \otimes \mathbb{I}_{\mathrm{P}} |\psi\rangle^{\mathrm{ABP}} \right] = \left(M'_{a|x} \otimes N'_{b|y} |\psi'\rangle^{\mathrm{A'B'}} \right) \otimes |\xi\rangle^{\mathrm{ABP}}$$

for all a, x, b, y and for some state $|\xi\rangle^{\mathrm{ABP}}$. In this paper, we are especially interested in self-testing of measurements. A compact way of writing the self-testing statement for Bob's measurements from the description given above is that there exists an isometry Φ_B that maps each $M_{b|y}$ to $M'_{b|y} \otimes \mathbb{1}$.

2.4 Quantum homomorphic encryption

Homomorphic encryption is a cryptographic technique that enables to execute computations directly on encrypted data, without prior decryption. The results of these computations remain in an encrypted form and, upon decryption, yield outputs identical to those obtained through operations on the unencrypted data. The term "homomorphic" draws from algebraic homomorphism, wherein encryption and decryption functions are likened to homomorphisms between plaintext and ciphertext spaces. A cryptosystem supporting arbitrary computation on ciphertexts is termed fully homomorphic encryption (FHE), representing the most robust form of homomorphic encryption. Originally conceptualized as a privacy homomorphism by Rivest, Adleman, and Dertouzous [40] shortly after the invention of the RSA cryptosystem [41], the first plausible construction for FHE using lattice-based cryptography was presented by Gentry [42]. Leveraging the hardness of the (Ring) Learning With Errors (RLWE) problem, more efficient schemes for fully homomorphic encryption have been devised [43, 44]. The possibility of quantum homomorphic encryption (QHE), allowing for quantum computations on encrypted data, was introduced by Mahadev [20], with Brakerski [21] subsequently enhancing it to achieve improved noise tolerance.

Before reminding the formalism of QHE, we first recall the definition of quantum polynomial time algorithms. Throughout the paper, κ denotes the security parameter.

Definition 1 (Quantum polynomial time algorithm)**.** *A quantum algorithm is quantum polynomial time (QPT) it can be implemented by a family of quantum circuits with size polynomial in the security parameter κ.*

We now reproduce the definition of QHE as it appears in [19].

Definition 2 (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 consists of the following four quantum algorithms which run in quantum polynomial time in terms of the security parameter:*

- Gen *takes as input the security parameter 1^κ and outputs a (classical) secret key* sk *of size* $\mathrm{poly}(\kappa)$ *bits;*
- Enc *takes as input a secret key* sk *and a classical input x, and outputs a ciphertext* ct*;*
- Eval *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* $\mathsf{Eval}_C(|\Psi\rangle \otimes |0\rangle^{\otimes \mathrm{poly}(\kappa,n)}, \mathsf{ct}_{\mathrm{in}})$ *which outputs a ciphertext* $\mathsf{ct}_{\mathrm{out}}$*. If C has classical output, we require that* Eval_C *also has classical output.*
- Dec *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.*

As in [19] the following property is required from QHE, in order for it to behave "nicely" with entanglement:

Definition 3 (Correctness with auxiliary input)**.** *For every security parameter $\kappa \in \mathbb{N}$, any quantum circuit $C : \mathcal{H}_A \times (\mathbb{C}^2)^{\otimes n} \to \{0,1\}^*$ (with classical output), any quantum state $|\Psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, any message $x \in \{0,1\}^n$, any secret key $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\kappa)$ and any ciphertext $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{sk}, x)$, the following states have negligible trace distance:*

Game 1 *Start with $(x, |\Psi\rangle_{AB})$. Evaluate C on x and register A, obtaining classical string y. Output y and the contents of register B.*

Game 2 *Start with $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{sk}, x)$ and $|\Psi\rangle_{AB}$. Compute $\mathsf{ct}' \leftarrow \mathsf{Eval}_C(|\Psi\rangle_{AB} \otimes |0\rangle^{\mathrm{poly}(\kappa,n)}, \mathsf{ct})$ on register A. Compute $y' = \mathsf{Dec}(\mathsf{sk}, \mathsf{ct}')$. Output y' and the contents of register B.*

In simple terms, "correctness with auxiliary input" stipulates that when QHE evaluation is employed on a register A within a joint (entangled) state in $\mathcal{H}_A \otimes \mathcal{H}_B$, the entanglement between the QHE-evaluated output and B must be maintained.

Finally, the following definition characterizes another property expected from QHE, and it is in cryptography well-known indistinguishability under chosen plaintext attack (IND-CPA).

Definition 4. *An QHE scheme is IND-CPA secure if for every quantum-polynomial time (QPT) adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, there exists a negligible function negl such that the following holds for all $\kappa \in \mathbb{N}$:*

$$\Pr\left[\tilde{b} = b \;\middle|\; \begin{array}{l} \mathsf{sk} \leftarrow \mathsf{Gen}(1^\kappa) \\ (x_0, x_1) \leftarrow \mathcal{A}_1^{\mathsf{Enc}(\mathsf{sk},\cdot)}(1^\kappa) \\ b \xleftarrow{\$} \{0,1\} \\ \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{sk}, x_b) \\ \tilde{b} \leftarrow \mathcal{A}_2^{\mathsf{Enc}(\mathsf{sk},\cdot)}(\mathsf{ct}^*) \end{array}\right] \leq \frac{1}{2} + \mathsf{negl}(\kappa).$$

2.5 Compiled nonlocal games

In [19], Kalai *et al.* introduced a compilation technique that can be used to construct single-prover proofs of quantumness. Their procedure transforms any k-player nonlocal game into a single-prover interactive game, employing post-quantum cryptography to emulate spatial separation among the parties. The proposed protocol maintains classical soundness, ensuring that no classical polynomially-bounded prover can surpass the maximal classical score of the original game. Additionally, leveraging quantum homomorphic encryption (QHE), the authors devise an explicit and efficient quantum strategy that achieves the quantum bound of the original nonlocal game. This enables the translation of proofs of quantumness into the single-prover interactive proof framework.

In this context, we refer to a single-prover interactive game that is generated through the KLVY compilation of a nonlocal game as a compiled nonlocal game. We recall the definition of compiled nonlocal games introduced in [19]. Using the interactive proof terminology, the entity called "referee" in the nonlocal game will be referred to as the "verifier".

Definition 5 (Compiled nonlocal game)**.** *In a compiled nonlocal game, a verifier, equipped with access to a Quantum Homomorphic Encryption (QHE) scheme as defined in Def. 2, engages with a prover. According to a probability distribution $q(x, y)$, the verifier samples x and y. In the first round, the verifier transmits $\mathsf{x} = \mathsf{Enc}(x)$ to the prover, who responds with an encrypted output $\mathsf{a} = \mathsf{Enc}(a)$. In the second round, the verifier sends the input y to the prover in the clear, and the prover replies with the answer b. The verifier assesses the outcome using the game predicate $V(\mathsf{Dec}(\mathsf{a}), b|\mathsf{Dec}(\mathsf{x}), y) \in \{0,1\}$ to determine whether the prover has passed or failed in the game.*

The following theorem (Theorem 1.1 in [19]) relates the classical and quantum score of a nonlocal game to the scores of the corresponding compiled game.

Theorem 2 ([19])**.** *Given any 2-player nonlocal game with quantum bound ξ_q and classical bound ξ_c and any QHE scheme (with security parameter κ) that satisfies correctness with auxiliary inputs and IND-CPA security against quantum distinguishers then, there is a 4-round single prover interactive game with completeness ξ_q realized by a quantum polynomial-time algorithm and soundness $\xi_c + negl(\kappa)$ against any classical polynomial-time algorithm.*

The classical soundness statement in this theorem guarantees that the maximal winning probability that a classical polynomial-time prover can achieve in a compiled nonlocal game is nearly identical to the optimal classical winning probability in the corresponding nonlocal game, with a negligible deviation dependent on the security parameter. The main insight in [19] is that the success of the classical prover is primarily hindered by the sequential nature of the game. This sequential structure forces the prover to commit to an answer a before receiving the input y. The combination of this sequential setup with secure QHE effectively replicates the locality requirement of a nonlocal game that is ensured by the spatial separation of the players. The quantum completeness statement ensures that a QPT prover can win the compiled nonlocal game with a probability that is at least as large as the optimal quantum winning probability in the corresponding nonlocal game.

2.5.1 Modelling the quantum prover

Let us now model the behavior of the single quantum prover, in the same way as it was done in [22]. In a compiled game, denoted as per Def. 5, the prover, initially in state $|\psi\rangle$, undergoes a process involving encrypted questions and answers. Specifically, in the first round, the prover receives an encrypted question x, performs a POVM measurement, and computes an encrypted answer a. Using Naimark dilation theorem, the prover's POVM measurement is simulated by a projective measurement, denoted here with $M_{\mathsf{a}|\mathsf{x}}$. The prover's action could potentially involve a unitary operation $U_{\mathsf{x},\mathsf{a}}$ following the measurement, crucial in the sequential setting. The projectors and unitaries can be unified into a set of potentially non-Hermitian operators $\mathsf{M}_{\mathsf{a}|\mathsf{x}}$, satisfying $\mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger \mathsf{M}_{\mathsf{a}|\mathsf{x}} = M_{\mathsf{a}|\mathsf{x}}$ and hence $\sum_{\mathsf{a}} \mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger \mathsf{M}_{\mathsf{a}|\mathsf{x}} = \mathbb{1}$. The prover's state after the first round of the game corresponds to the post-measurement state

$$|\psi_{\mathsf{a}|\mathsf{x}}\rangle = \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle, \tag{36}$$

and the probability to get output a for input x is

$$p(\mathsf{a}|\mathsf{x}) = \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle = \left\||\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2. \tag{37}$$

In the second round, the prover's behavior is characterized by a set of projective operators $\{\{N_{b|y}\}_b\}_y$. If the second-round answers are bits, the measurements can be characterized by specifying a Hermitian observable $B_y = \sum_b (-1)^b N_{b|y}$. Similarly, if Alice's outputs in the corresponding nonlocal game are bits, we can define a "decrypted" observable

$$\mathrm{A}_x = \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} (-1)^{\mathsf{Dec}(\mathsf{a})} \mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger \mathsf{M}_{\mathsf{a}|\mathsf{x}} \tag{38}$$

$$= \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} A_{\mathsf{x}}, \tag{39}$$

where A_{x} are binary observables, while A_x in general is not. If both a and b are bits, we can define the correlators allowing to characterize the winning probability of a quantum prover in a computational single-prover game:

$$\langle \mathrm{A}_x, B_y \rangle = \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} (-1)^{\mathsf{Dec}(\mathsf{a})} \langle \psi_{\mathsf{a}|\mathsf{x}}|B_y|\psi_{\mathsf{a}|\mathsf{x}}\rangle \tag{40}$$

The correlators have the same operational meaning as in nonlocal games: when the verifier samples a question pair (x, y) in the compiled game and receives (decrypted) answers (a, b), $\langle \mathrm{A}_x, B_y\rangle$ is precisely the expected value of $(-1)^{a+b}$.

The marginals of the second-round observables in principle depends on the encrypted x of the first round and have form:

$$\langle B_y \rangle_x = \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \langle \psi_{\mathsf{a}|\mathsf{x}}|B_y|\psi_{\mathsf{a}|\mathsf{x}}\rangle. \tag{41}$$

2.6 Technical tools for estimating quantum bounds of compiled nonlocal games

2.6.1 Block encodings

We now examine certain outcomes related to the block encoding of quantum processes. Block encoding is a method for the efficient implementation of a quantum operation. Our motivation for exploring this process stems from the contextual constraint imposed in the subsequent sections of this paper, where we address computational limitations among participants. Consequently, we aim to identify operations that can be efficiently executed by leveraging available quantum resources.

Definition 6 (Block encoding)**.** *Given a matrix $A \in \mathbb{C}^{c\times c}$, we say that $U \in \mathbb{C}^{d\times d}$ is a Q-block encoding of A if*

- *U is a unitary matrix whose quantum circuit can be implementable with $O(Q)$ gates,*
- *U has the following form $U = \begin{pmatrix} \tau A & \cdot \\ \cdot & \cdot \end{pmatrix}$, where we call τ the scale factor of the block encoding.*

We say U is QPT-implementable if Q is polynomially bounded in the size of the input.

If U is a block encoding of A, then A can be implemented by performing the following operation

$$A = \frac{1}{\tau}\left(\langle 0| \otimes \mathbb{1}\right) U \left(|0\rangle \otimes \mathbb{1}\right)$$

where $\mathbb{1}$ is the identity matrix of the size of A.

Through the linear combination and multiplication of matrices possessing a block encoding, our anticipation is the persistence of this property in the resulting matrix. Although the explicit construction in complete generality is not immediately apparent, [45, Lemmas 52 and 53] provides a technical framework for the block encoding of linear combinations and products of matrices with block encoding. Here, we present a streamlined version of their results, tailored to our specific requirements.

First, we present a lemma about the block encoding of a linear combination of matrices that have block encoding, whose proof can be found in [45, Lemma 52].

Lemma 4 (Linear combination of block encoded matrices)**.** *Let $A = \sum_{j=1}^{m} y_j A_j$, where $y \in \mathbb{C}^m$ is a complex bounded vector $\|y\|_1 \leq \beta$ and A_j are matrices for which we know a Q_j-block encoding U_j. Then we can implement a $\left(m + \sum_{j=1}^{m} Q_j\right)$-block encoding of A.*

Corollary 1. *Let $A = \sum_{j=1}^{m} y_j A_j$, where $y \in \mathbb{C}^m$ is a complex bounded vector $\|y\|_1 \leq \beta$. If $m = \mathrm{poly}(\kappa)$ and each A_j is an operator with QPT-implementable block encodings with scale factor $O(1)$ for all j, A also has a QPT-implementable block encoding with scale factor $O(1)$.*

The subsequent lemma guarantees the presence of a block encoding for the product of matrices, each possessing its own block encoding, whose proof can be found in [45, Lemma 53].

Lemma 5 (Product of block encoded matrices)**.** *Let U and V be the Q_U and Q_V-block encodings of A and B respectively. Then we can implement a $(Q_U + Q_V)$-block encoding of AB.*

Corollary 2. *Let U and V be the Q_U and Q_V-block encodings of A and B respectively. If U and V are QPT-implementable, each with scale factor $O(1)$, AB also has a QPT-implementable block encoding with scale factor $O(1)$.*

For operators with a QPT-implementable block-encoding, the following technical lemma from [22] applies.

Lemma 6 ([22, Lemma 14])**.** *Let $\mathscr{B}$ be an operator with a QPT-implementable block encoding with $O(1)$ scale factor and $\|\mathscr{B}\| \leq O(1)$. Then there exists a QPT-measurable POVM $\{M_\beta\}_\beta$ such that for any state ρ, the following holds:*

$$\left| \sum_{\beta} \beta \cdot \mathrm{Tr}\left[M_\beta \rho\right] - \mathrm{Tr}\left[\mathscr{B}\rho\right] \right| \leq \varepsilon, \tag{42}$$

for any $\varepsilon = 1/\mathrm{poly}(\kappa)$.

These results, together with the definition of the IND-CPA security, allow us to state the following:

Lemma 7 (adapted from [22, Lemmas 15-17])**.** *Let $\mathscr{B}$ be an operator with a QPT-implementable block encoding with $O(1)$ scale factor and $\|\mathscr{B}\| \leq O(1)$. Let $\mathrm{QHE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{Dec})$ be a secure quantum homomorphic encryption scheme (see Definition 2), let D_0, D_1 be any two QPT sampleable distributions over plaintext questions x, and let $|\psi\rangle$ be any efficiently preparable state of the prover. Then, for any security parameter $\kappa \in \mathbb{N}$, there exists a negligible function $\delta_{\mathrm{QHE}}(\kappa)$ such that*

$$\left| \mathop{\mathbb{E}}_{x\leftarrow D_0} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} \mathscr{B} \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle - \mathop{\mathbb{E}}_{x\leftarrow D_1} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} \mathscr{B} \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \right| \leq \delta_{\mathrm{QHE}}(\kappa). \tag{43}$$

The proof of this Lemma encompasses Lemmas 15, 16 and 17 in [22]. Importantly, $\mathscr{B}$ does not have to be a binary observable, it just has to be efficiently implementable by quantum circuits. This lemma establishes a link between QPT-implementable block encodings and IND-CPA security. Looking ahead, using the fact that XOR games and SATWAP Bell inequalities have a nice form of SOS decomposition into linear combination and product of block encodings as presented in previous sections, this lemma will allow us to relate the quantum bound of the compiled nonlocal games to those of the original nonlocal games, at the expense of a negligible security loss.

2.6.2 Crypto-correlation matrix and pseudo-expectation map

In this section, we revisit and further expound upon the concepts delineated in Section 4.4 of [22]. In that section, the authors introduced a compelling argument to establish the optimal quantum winning probability for the compiled CHSH game through the introduction of a cryptographic SOS decomposition. Our objective is to broaden their findings to encompass a more extensive array of games, namely XOR games and d-outcome CHSH games.

Consider an XOR game with an optimal quantum bias ξ_q. Its game operator (17) is

$$\mathcal{B}_g = \sum_{x,y} \gamma_{x,y}^{AB} A_x B_y, \tag{44}$$

and the corresponding shifted game operator has an SOS decomposition

$$\xi_q \mathbb{1} - \mathcal{B}_g = \sum_i b_i P_i^\dagger P_i + \sum_i d_i [A_{x_i}, B_{y_i}] + \sum_i e_i (\mathbb{1} - A_{x_i}^2) + \sum_i f_i (\mathbb{1} - B_{y_i}^2), \tag{45}$$

where $b_j \in \mathbb{R}^+$ are real positive coefficients for the terms of the SOS decomposition, d_i-s could be complex numbers referring to the constraint that Alice's and Bob's operators commute, e_i-s and f_i-s multiply terms that vanish if the measurements of Alice and Bob are projective. All terms on the r.h.s. of (45) except the first one are general constraints that are usually implicitly assumed. Here, the aim is to develop an analogous procedure for bounding the optimal quantum bias of compiled games, so one has to be careful as some of the constraints satisfied in the case of nonlocal games might not be satisfied in the case of compiled games. For example, operations in two rounds of the compiled game do not necessarily commute.

Analogously to matrix $\tilde{Q}$ from Section 2.2, expounding on the ideas from [22], we define a $(|\mathsf{X}|+|\mathsf{Y}|)\times(|\mathsf{X}|+|\mathsf{Y}|)$ matrix $\tilde{\mathcal{Q}}$ as follows

$$\tilde{\mathcal{Q}} = \left[\begin{array}{c|c} \mathbb{1}_{|\mathsf{X}|} & C \\ \hline C^T & S \end{array}\right], \tag{46}$$

where $\mathbb{1}_{|\mathsf{X}|}$ is the $|\mathsf{X}| \times |\mathsf{X}|$ identity matrix, where

$$C = \sum_{x,y} \langle \mathrm{A}_x, B_y \rangle |x\rangle\langle y|, \tag{47}$$

$$S = \sum_{y,y'} \mathop{\mathbb{E}}_{x\in\mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \langle \psi_{\mathsf{a}|\mathsf{x}} | B_y B_{y'} | \psi_{\mathsf{a}|\mathsf{x}} \rangle |y\rangle\langle y'|, \tag{48}$$

and where $\langle \mathrm{A}_x, B_y \rangle$ correspond to Eq. (40). The matrix $\tilde{\mathcal{Q}}$, unlike $\tilde{Q}$, is not necessarily positive semidefinite, as there is no real consistency in assigning values to its entries. Similarly to $\tilde{Q}$, $\tilde{\mathcal{Q}}$ has ones on the diagonal, in the first block by construction and in the second because

$$\begin{aligned} S_{y,y} &= \mathop{\mathbb{E}}_{x\in\mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \langle \psi_{\mathsf{a}|\mathsf{x}} | \mathbb{1} | \psi_{\mathsf{a}|\mathsf{x}} \rangle \\ &= \mathop{\mathbb{E}}_{x\in\mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \langle \psi | \mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger \mathsf{M}_{\mathsf{a}|\mathsf{x}} | \psi \rangle \\ &= \mathop{\mathbb{E}}_{x\in\mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \langle \psi | \psi \rangle \\ &= 1. \end{aligned}$$

Then, as in [22], we define a linear operator $\tilde{\mathbb{E}}$ that maps every homogeneous degree-2 polynomial in the variables A_x, B_y to linear combinations of elements of the matrix $\tilde{\mathcal{Q}}$ in the following way:

$$\tilde{\mathbb{E}}[A_x B_y] = C_{x,y}, \qquad \tilde{\mathbb{E}}[B_y \mathrm{A}_x] = C_{y,x}^T, \tag{49}$$

$$\tilde{\mathbb{E}}[A_x A_{x'}] = \delta_{x,x'}, \qquad \tilde{\mathbb{E}}[B_y B_{y'}] = S_{y,y'}. \tag{50}$$

For $y = y'$ or $x = x'$ in Eq. (50), we get a consistent mapping of identity

$$\tilde{\mathbb{E}}[A_x A_x] = \tilde{\mathbb{E}}[\mathbb{1}] = 1, \qquad \tilde{\mathbb{E}}[B_y B_y] = \tilde{\mathbb{E}}[\mathbb{1}] = S_{y,y} = 1. \tag{51}$$

As in [22], we call the map $\tilde{\mathbb{E}}$ a pseudo-expectation. Such defined pseudo-expectation maps the game operator $\mathcal{B}_g$ introduced in Eq. (44)) to a bias in the compiled nonlocal game:

$$\tilde{\mathbb{E}}[\mathcal{B}_g] = \sum_{x,y} \gamma_{x,y} \tilde{\mathbb{E}}[A_x B_y] = \sum_{x,y} \gamma_{x,y} \langle \mathrm{A}_x, B_y \rangle = \bar{\xi}. \tag{52}$$

The optimal quantum bias can be upper bounded using the SOS decomposition of the shifted game operator(eq. (45)):

$$\tilde{\mathbb{E}}\left[\xi_q \mathbb{1} - \mathcal{B}_g\right] = \tilde{\mathbb{E}}\left[\sum_i b_i P_i^\dagger P_i + \sum_i d_i [A_{x_i}, B_{y_i}] + \sum_i e_i (\mathbb{1} - A_{x_i}^2) + \sum_i f_i (\mathbb{1} - B_{y_i}^2)\right] \tag{53}$$

Given (49), the terms multiplied by d_i vanish because, under the pseudo-expectation map, the operators A_x and B_y commute. The terms multiplied by e_i and f_i also vanish because of Eq. (51); hence

$$\tilde{\mathbb{E}}\left[\xi_q \mathbb{1} - \mathcal{B}_g\right] = \sum_i b_i \tilde{\mathbb{E}}\left[P_i^\dagger P_i\right]. \tag{54}$$

Thus, if $\tilde{\mathbb{E}}\left[P_i^\dagger P_i\right]$ is non-negative, the bias in a compiled game cannot be larger than the optimal quantum bias of the corresponding nonlocal game.

3 Quantum bound of compiled biparite XOR games

In Section 2.2, we established key insights into XOR games. Here, building upon the methodology outlined in [22] and revisited in 2.6.2, we present our first important result: compiled XOR games exhibit a quantum bias that closely aligns with the quantum bias of the corresponding nonlocal game, fluctuating only slightly with the security parameter. The power of the quantum prover to win a compiled XOR game with a probability larger than the optimal quantum winning probability for the corresponding XOR game crucially depends on their ability to transmit from the first round information about the received plaintext input. However, inputs are encrypted in such a way that the encryption satisfies IND-CPA security, meaning that even the quantum prover cannot do better than randomly guessing its question x knowing the encryption $\mathtt{x}$ of x. This inability of a QPT prover to break the encryption is articulated in Lemma 7. In essence, this lemma conveys that regardless of the measurement employed by a QPT prover in the second round of the game, they are unable to differentiate between states resulting from distinct samples of plaintext questions taken in the first round.

Before stating our main result let us state two lemmas about the behavior of the XOR game operator under the pseudo-expectation map defined in Sec. 2.6.2. The first lemma is a generalization of Claims 31 and 33 from [22].

Lemma 8. *Let $P_x = A_x - \sum_y F_{xy} B_y$ with$\{A_x\}_{x \in \mathsf{X}}$ and $\{B_y\}_{y \in \mathsf{Y}}$ binary observables. Then there exists a negligible function $\delta_{\mathrm{QHE}}(\cdot)$ such that we have $\tilde{\mathbb{E}}\left[P_x^\dagger P_x\right] \geq -\delta_{\mathrm{QHE}}(\kappa)$, where $\tilde{\mathbb{E}}[\cdot]$ is the pseudo-expectation map defined in Sec. 2.6.2.*

Proof. Let us introduce the shortened notation $\hat{B}_x = \sum_y F_{xy} B_y$.

$$
\begin{aligned}
\tilde{\mathbb{E}}\left[P_x^\dagger P_x\right] &= \tilde{\mathbb{E}}\left[A_x^\dagger A_x\right] - \tilde{\mathbb{E}}\left[A_x^\dagger \hat{B}_x\right] - \tilde{\mathbb{E}}\left[\hat{B}_x^\dagger A_x\right] + \tilde{\mathbb{E}}\left[\hat{B}_x^\dagger \hat{B}_x\right] \\
&= 1 - 2\sum_y F_{xy} C_{xy} + \sum_{y,y'} F_{yx} F_{xy'} S_{yy'} \\
&= 1 - 2\sum_y F_{xy} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} (-1)^{\mathsf{Dec}(\mathsf{a})} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger B_y \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&\quad + \sum_{y,y'} F_{yx} F_{xy'} \mathop{\mathbb{E}}_{z\in\mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(z)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger B_y B_{y'} \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&= 1 - 2 \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} (-1)^{\mathsf{Dec}(\mathsf{a})} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger \hat{B}_x \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle + \mathop{\mathbb{E}}_{z\in\mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(z)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger \hat{B}_x^\dagger \hat{B}_x \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&\approx_{\delta_{\mathrm{QHE}}(\kappa)} 1 - 2 \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} (-1)^{\mathsf{Dec}(\mathsf{a})} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger \hat{B}_x \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle + \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger \hat{B}_x^\dagger \hat{B}_x \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&= \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger \left(\mathbb{1} - 2(-1)^{\mathsf{Dec}(\mathsf{a})} \hat{B}_x + \hat{B}_x^2\right) \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&= \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger \left((-1)^{\mathsf{Dec}(\mathsf{a})}\mathbb{1} - \hat{B}_x\right)^2 \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle
\end{aligned}
$$

In the first two lines, we used the linearity and the definition of the pseudo-expectation map. In the third line, we used the definition of matrices C (eq. (49)) and S (eq. (50)). In the fourth line, we just used the definition of $\hat{B}_x$. To get the fifth line we used the fact that $\hat{B}_x^\dagger \hat{B}_x$ has a QPT-implementable block encoding (Corrolaries 1 and 2) and thus we can apply Lemma 7 given above to fix the input $z \in \mathsf{X}$ to be exactly x, paying the price of a $\delta_{\mathrm{QHE}}(\kappa)$. To get the sixth line we used linearity and we grouped all terms inside of one average over $\mathsf{x} = \mathsf{Enc}(x)$; in particular we noticed that we could write the first term 1 as $\mathbb{1}$ inside this average. Finally, in the seventh line we recognised that the expression within round brackets can be expressed as the square of an operator. This is necessarely positive, implying that up to a negligible factor $\tilde{\mathbb{E}}\left[P_x^\dagger P_x\right]$ must also be positive. □

Remark 1. *This lemma is the key-point that allows to generalize the framework introduced in [22] to all games for which we have a SOS decomposition whose polynomials can be written as $P_x = A_x - \sum_y F_{xy} B_y$. This specific shape might seem restricting, but we showed in the previous section that it is expressive enough to describe all XOR games. Extending the statement to more general forms of the polynomials might be challenging, because we lack of a clear intuition on how to interpret product of Alice's observables in the compiled scenario. The pseudo-expectation map is designed to mimic a true expectation map, assigning non-negative values to positive operators. Its small deviation from positivity, allowed only by a negligible function of the security parameter, is justified by the IND-CPA security of the encryption scheme. However, this justification relies on the SOS decomposition having the specific form described above. More general SOS forms lead to pseudo-expectation values that, with current techniques, cannot be meaningfully estimated.*

Lemma 9. *Let P be a positive semi-definite homogeneous degree-2 polynomial over binary observables $\{B_y\}_y$. Then $\tilde{\mathbb{E}}[P] \geq 0$, where $\tilde{\mathbb{E}}[\cdot]$ is the pseudo-expectation map defined in Sec. 2.6.2.*

Proof. The pseudo-expectation of P reads

$$
\tilde{\mathbb{E}}[P] = \mathop{\mathbb{E}}_{x\in\mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger P \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \geq 0. \tag{55}
$$

Since all of the elements in the sum are positive, because P is positive semi-definite, the relation trivially holds. □

We can now state the main theorem, providing the quantum optimal bias of compiled XOR games.

Theorem 3. *Given an XOR game with optimal quantum bias ξ_q, the optimal quantum bias of the compiled XOR game is $\xi_q + \delta_{\mathrm{QHE}}(\kappa)$, where $\delta_{\mathrm{QHE}}(\cdot)$ is a negligible function.*

Proof. Let us recall Theorem 1 which states that for every XOR game we have

$$
\xi_q \mathbb{1} - \mathcal{B}_g = \sum_x \frac{\lambda_x}{2} \left(A_x - \sum_y F_{xy} B_y\right)^2 + P\left(\{B_y\}_y\right),
$$

By applying the pseudo-expectation map we get

$$\tilde{\mathbb{E}}\left[\xi_q \mathbb{1} - \mathcal{B}_g\right] = \tilde{\mathbb{E}}\left[\sum_x \frac{\lambda_x}{2}\left(A_x - \sum_y F_{xy} B_y\right)^2 + P\left(\{B_y\}_y\right)\right] \tag{56}$$

$$= \sum_x \frac{\lambda_x}{2}\tilde{\mathbb{E}}\left[\left(A_x - \sum_y F_{xy} B_y\right)^2\right] + \tilde{\mathbb{E}}\left[P\left(\{B_y\}_y\right)\right]. \tag{57}$$

To get the second line we used the linearity of the pseudo-expectation map. Based on Lemmas 8 implies that the first term on the r.h.s is up to a negligible function nonnegative, while Lemma 9 implies that the second term on the r.h.s. must be nonnegative. The pseudo-expectation map on the l.h.s. gives $\xi_q - \bar{\xi}_q$, implying that in the worst case the compiled game optimal bias can be only negligibly larger than the optimal quantum bias of the corresponding XOR game:

$$\bar{\xi}_q \leq \xi_q + \delta_{\mathrm{QHE}}(\kappa), \tag{58}$$

which completes the proof. □

4 Quantum bound of compiled nonlocal games with many outputs and conditions for self-testing of qudit measurements from a single prover

We now introduce a family of nonlocal games in which the players respond with more than two outputs. In this case, the quantum strategy involves d-outcome measurements, $\{M_{a|x}\}_{a=0}^{d-1}$ for Alice and $\{N_{b|y}\}_{b=0}^{d-1}$ for Bob. These measurements can be represented through generalized observables

$$A_x^{(k)} = \sum_{a=0}^{d-1} \omega^{ak} M_{a|x}, \qquad B_y^{(l)} = \sum_{b=0}^{d-1} \omega^{bl} N_{b|y}, \quad \forall k, l = 0, \cdots, d-1, \tag{59}$$

where $\omega = \exp\left(\frac{2\pi i}{d}\right)$. Clearly, the eigenvalues of the generalized unitary observables $A_x^{(k)}$ and $B_y^{(l)}$ are roots of unity. We will refer to the indices k and l as the orders of the generalised measurement; notice that the orders $k = 0 \mod d$ are the identity. For $d > 2$, generalized observables are not Hermitian, but still satisfy the following regular property:

$$(A^{(k)})^\dagger = A^{(-k)} \qquad (B^{(l)})^\dagger = B^{(-l)}$$

and hence $\left[A^{(k)}\right]^\dagger A^{(k)} = \mathbb{1}$ for every k. Considering only projective measurements, it is easy to check that $A^{(k)} = \left[A^{(1)}\right]^k$ and $B^{(l)} = \left[B^{(1)}\right]$; we will use these two notations interchangeably.

In this section, we adopt the perspective of Bell inequalities. The CHSH inequality is the simplest Bell inequality whose maximal violation self-tests the maximally entangled pair of qubits. Several propositions have been formulated to capture different features of the CHSH inequality, some focusing on self-testing maximally entangled shared states [24], some on self-testing mutually unbiased bases measurements for both parties [46]. We concentrate on the Salavrakos-Augusiak-Tura-Wittek-Acin-Pironio (SATWAP) Bell inequality introduced in [24], for which a self-test of arbitrary local dimension with minimal number of measurements (2 per part) has been proposed in [25]. We refer to this inequality as d-CHSH, because it shares many similarities with the CHSH inequality, generalising it to outputs that are d-dimensional. However, this is not related to the class of Bell inequalities introduced by Buhrman and Massar in [47], and later developed in [48], [49] and [50], which are also known as d-CHSH inequalities.

The SATWAP inequality is defined for two spatially separated players, each receiving a bit as input, $\mathsf{X} = \mathsf{Y} = \{1, 2\}$, and subsequently producing an output that can take one of d different values, $\mathsf{A} = \mathsf{B} = \{0, \ldots, d-1\}$. Many Bell inequalities can be expressed by conveniently defining some regular combination of probabilities given fixed inputs, called correlators. The definition of the generalised correlator is:

$$\langle A_x^{(k)} B_y^{(l)} \rangle = \sum_{a=0}^{d-1}\sum_{b=0}^{d-1} \omega^{ak+bl} p(ab|xy). \tag{60}$$

The SATWAP inequality is given in terms of these generalised correlators:

$$\beta_d^{\mathrm{SATWAP}} = \sum_{k=1}^{d-1} \left(a_k \langle A_1^k B_1^{d-k} \rangle + a_k^* \omega^k \langle A_1^k B_2^{d-k} \rangle + a_k^* \langle A_2^k B_1^{d-k} \rangle + a_k \langle A_2^k B_2^{d-k} \rangle \right), \tag{61}$$

with the following definition of the phases $a_k = \frac{\omega^{\frac{2k-d}{8}}}{\sqrt{2}} = \frac{1-i}{2}\omega^{k/4}$ such that $a_k^* = a_{d-k}$ and $a_{\pm d} = \pm\frac{1+i}{2}$. To simplify the notation it is convenient to group Bob's observables in the following sums:

$$C_1^{(k)} = a_k B_1^{-k} + a_k^* \omega^k B_2^{-k}, \qquad C_2^{(k)} = a_k^* B_1^{-k} + a_k B_2^{-k}. \tag{62}$$

Using these definitions, the corresponding Bell operator is thus

$$\mathcal{B}_d^{\mathrm{SATWAP}} = \sum_{k=1}^{d-1} \left(A_1^k \otimes C_1^{(k)} + A_2^k \otimes C_2^{(k)} \right). \tag{63}$$

Bell value is thus given as $\beta_d^{\mathrm{SATWAP}} = \langle\psi|\mathcal{B}_d^{\mathrm{SATWAP}}|\psi\rangle$. The classical and the quantum bounds of this inequality are

$$\left(\beta_d^{\mathrm{SATWAP}}\right)_l = \frac{1}{2}\left(3\cot\left(\frac{\pi}{4}d\right) - \cot\left(\frac{3\pi}{4}d\right)\right) - 2, \qquad \left(\beta_d^{\mathrm{SATWAP}}\right)_q = 2(d-1).$$

The quantum bound can be found by explicitly building the SOS decomposition of the shifted Bell operator, as shown in [24]. The terms of the SOS decomposition are labeled by $x \in \{1,2\}$ and $k \in \{0,\ldots,d-1\}$:

$$P_{x,k} = (A_x^k)^\dagger - C_x^{(k)}.$$

A quick calculation allows us to check the correctness of the SOS decomposition :

$$\begin{aligned} \beta_q \mathbb{1} - \mathcal{B}_d^{\mathrm{SATWAP}} &= \frac{1}{2}\sum_{k=1}^{d-1}\left(P_{1,k}^\dagger P_{1,k} + P_{2,k}^\dagger P_{2,k}\right) \\ &= -\mathcal{B}_d^{\mathrm{SATWAP}} + (d-1)\mathbb{1} + \frac{1}{2}\sum_{k=1}^{d-1}\left(C_1^{(d-k)}C_1^{(k)} + C_2^{(d-k)}C_2^{(k)}\right) \\ &= -\mathcal{B}_d^{\mathrm{SATWAP}} + 2(d-1). \end{aligned} \tag{64}$$

The maximal quantum violation of this inequality is a self-test of a maximally entangled pair of qudits, together with measurements that are unitarily equivalent to the measurements used to maximally violate well-known Collins-Gisin-Linden-Massar-Popescu (CGLMP) Bell inequalities [51]. We summarise this technical result in the following lemma, proven in [25].

Lemma 10 ([25])**.** *The maximal violation of the SATWAP Bell inequality certifies the following:*

- *The dimension of Alice's and Bob's Hilbert spaces is a multiple of d, and we can write their Hilbert space as the tensor products $\mathcal{H}_A = \mathbb{C}^d \otimes \mathcal{H}_{A'}$, $\mathcal{H}_B = \mathbb{C}^d \otimes \mathcal{H}_{B'}$, where $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$ are auxiliary Hilbert spaces of finite dimension;*
- *There exist local unitary transformations $U_A : \mathcal{H}_A \to \mathcal{H}_A$ and $U_B : \mathcal{H}_B \to \mathcal{H}_B$ such that*

$$U_B B_1 U_B^\dagger = Z_d \otimes \mathbb{1}_{B'}, \qquad U_B B_2 U_B^\dagger = T_d \otimes \mathbb{1}_{B'}, \tag{65}$$

$$U_A A_1 U_A^\dagger = (a_1^* Z_d + 2(a_1^*)^3 T_d) \otimes \mathbb{1}_{A'}, \qquad U_A A_2 U_A^\dagger = (a_1 Z_d - a_1^* T_d) \otimes \mathbb{1}_{B'}. \tag{66}$$

  where $Z_d = diag[1,\omega,\ldots,\omega^{d-1}]$ and $T_d = \sum_{i=0}^{d-1}\omega^{i+1/2}|i\rangle\langle i| - \frac{2}{d}\sum_{j,i=0}^{d-1}(-1)^{\delta_{i,0}+\delta_{j,0}}\omega^{(i+j+1)/2}|i\rangle\langle j|$.
- *Alice and Bob share a state $|\psi_{AB}\rangle$ which is unitarily equivalent to the maximally entangled pair of qudits*

$$U_A \otimes U_B|\psi_{AB}\rangle = |\phi_d^+\rangle \otimes |\tau_{A'B'}\rangle.$$

Note that Eqs. (65) fully characterize Bob's measurements, given that they are projective and $B_y^{(k)} = B_y^k$.

For the compiled SATWAP Bell inequality, a modification in the modeling of the quantum prover is necessary. Our focus, thus far, has primarily been on compiled games with binary outputs. The prover is initiated in some quantum state $|\psi\rangle$ and its action in the first round is described in the same way, with eqs. (36) and (37) still holding. However, a generalized k-th order decrypted observable now reads:

$$\mathrm{A}_x^{(k)} = \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \omega^{k\mathsf{Dec}(\mathsf{a})} \mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger \mathsf{M}_{\mathsf{a}|\mathsf{x}} \tag{67}$$

$$= \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} A_{\mathsf{x}}^{(k)} \tag{68}$$

and the generalized decrypted correlator takes the form

$$\langle \mathrm{A}_x^{(k)}, B_y^{(l)} \rangle = \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \omega^{k\mathsf{Dec}(\mathsf{a})} \langle \psi_{\mathsf{a}|\mathsf{x}} | B_y^{(l)} | \psi_{\mathsf{a}|\mathsf{x}} \rangle, \tag{69}$$

with this value operationally giving the expectation value of ω^{ak+bl}, which will be directly used to asses the performance of the prover in the SATWAP game.

We generalize the modified moment matrix $\tilde{\mathcal{Q}}$ to include the expectation values of generalized observables. Recall that generalized observables are labeled not only by the input $x \in \mathsf{X}$ (or $y \in \mathsf{Y}$) but also by the degree $k \in \{1, \ldots, d-1\}$ (or l). Every entry of the modified covariance matrix $\tilde{\mathcal{Q}}$ is labeled by two generalized observables, hence is a square matrix of dimension $(|\mathsf{X}| + |\mathsf{Y}|)(d-1)$. Hence, we define a generalization of the matrix $\tilde{\mathcal{Q}}$ as follows

$$\tilde{\mathcal{Q}} = \left[\begin{array}{c|c} \mathbb{1}_{(d-1)|\mathsf{X}|} & C \\ \hline C^T & S \end{array}\right] \tag{70}$$

where $\mathbb{1}_{(d-1)|\mathsf{X}|}$ is $(d-1)|\mathsf{X}| \times (d-1)|\mathsf{X}|$ identity matrix and

$$C = \sum_{x,y,k,l} \langle \mathrm{A}_x^{(d-k)}, B_y^{(l)} \rangle |(k-1)d + x\rangle\langle (l-1)d + y| \tag{71}$$

$$S = \mathop{\mathbb{E}}_{x \in \mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \langle \psi_{\mathsf{a}|\mathsf{x}} | B_y^{(d-l)} B_{y'}^{(l')} | \psi_{\mathsf{a}|\mathsf{x}} \rangle |(l-1)d + y\rangle\langle (l'-1)d + y'| \tag{72}$$

with $\langle \mathrm{A}_x^{(k)}, B_y^{(l)} \rangle$ being introduced in eq. (69).

As in 2.6.2, we define a linear operator $\tilde{\mathrm{E}}$ that maps every homogeneous degree-2 polynomial in the variables $\{A_x^{(k)}, B_y^{(l)}\}_{x,y,k,l}$ to linear combinations of elements of matrix $\tilde{\mathcal{Q}}$ in the following way

$$\tilde{\mathrm{E}}[A_x^{(d-k)} B_y^{(l)}] = C_{(k-1)d+x,(l-1)d+y}, \qquad \tilde{\mathrm{E}}[B_y^{(l)} \mathrm{A}_x^{(d-k)}] = C^T_{(l-1)d+y,(k-1)d+x} \tag{73}$$

$$\tilde{\mathrm{E}}[A_x^{(k)} A_{x'}^{(k')}] = \delta_{x,x'}\delta_{k,k'}, \qquad \tilde{\mathrm{E}}[B_y^{(l)} B_{y'}^{(l')}] = S_{(l-1)d+y,(l'-1)d+y'} \tag{74}$$

For $y = y'$, $l = l'$ or $x = x'$, $k = k'$ in eq. (50) we get a consistent mapping of identity

$$\tilde{\mathrm{E}}[A_x^{(d-k)} A_x^{(k)}] = \tilde{\mathrm{E}}[\mathbb{1}] = 1, \qquad \tilde{\mathrm{E}}[B_y^{(d-l)} B_y^{(l)}] = \tilde{\mathrm{E}}[\mathbb{1}] = S_{(l-1)d+y,(l-1)d+y} = 1. \tag{75}$$

With this formalism, we can prove a result equivalent to Theorem (3) for the quantum bound of the compiled SATWAP inequality. Let us first introduce the following lemma.

Lemma 11. *Let $P_{x,k} = (A_x^k)^\dagger - C_x^{(k)}$, where A_x^k is a generalised observable, and $C_x^{(k)}$ are linear sums of generalised observables defined in eq. (62). Then there exists a negligible function $\delta_{\mathrm{QHE}}(\cdot)$ such that we have $\tilde{\mathrm{E}}\left[(P_x^k)^\dagger P_x^k\right] \geq -\delta_{\mathrm{QHE}}(\kappa)$, where $\tilde{\mathrm{E}}[\cdot]$ is the pseudo-expectation map generalised above.*

Proof. The proof follows closely the arguments presented in the proof of Lemma 8, with the difference

that generalised observables are not hermitian, and phases are also complex.

$$\begin{aligned}
\tilde{\mathbb{E}}\left[P_{x,k}^{\dagger}P_{x,k}\right] &= \tilde{\mathbb{E}}\left[(A_x^{(k)})^{\dagger}A_x^{(k)}\right] - \tilde{\mathbb{E}}\left[(A_x^{(k)})^{\dagger}C_x^{(k)}\right] - \tilde{\mathbb{E}}\left[(C_x^{(k)})^{\dagger}A_x^{k}\right] + \tilde{\mathbb{E}}\left[(C_x^{(k)})^{\dagger}C_x^{(k)}\right] \\
&= \tilde{\mathbb{E}}\left[A_x^{(d-k)}A_x^{(k)}\right] - \tilde{\mathbb{E}}\left[A_x^{(d-k)}C_x^{(k)}\right] - \tilde{\mathbb{E}}\left[C_x^{(d-k)}A_x^{(k)}\right] + \tilde{\mathbb{E}}\left[C_x^{(d-k)}C_x^{(k)}\right] \\
&= 1 - \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \omega^{(d-k)\mathsf{Dec}(\mathsf{a})} \langle\psi_{\mathsf{a}|\mathsf{x}}|C_x^{(k)}|\psi_{\mathsf{a}|\mathsf{x}}\rangle - \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \omega^{k\mathsf{Dec}(\mathsf{a})} \langle\psi_{\mathsf{a}|\mathsf{x}}|C_x^{(d-k)}|\psi_{\mathsf{a}|\mathsf{x}}\rangle \\
&+ \mathop{\mathbb{E}}_{i\in\mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(i)} \sum_{\mathsf{a}} \langle\psi_{\mathsf{a}|\mathsf{x}}|C_x^{(d-k)}C_x^{(k)}|\psi_{\mathsf{a}|\mathsf{x}}\rangle \\
&\approx_{\delta_{\mathrm{QHE}}(\kappa)} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi_{\mathsf{a}|\mathsf{x}}| \left(\mathbb{1} - \omega^{-k\mathsf{Dec}(\mathsf{a})}C_x^{(k)} - \omega^{k\mathsf{Dec}(\mathsf{a})}C_x^{(d-k)} + C_x^{(d-k)}C_x^{(k)}\right) |\psi_{\mathsf{a}|\mathsf{x}}\rangle \\
&\approx_{\delta_{\mathrm{QHE}}(\kappa)} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi_{\mathsf{a}|\mathsf{x}}| \left(\omega^{k\mathsf{Dec}(\mathsf{a})}\mathbb{1} - C_x^{(k)}\right)^2 |\psi_{\mathsf{a}|\mathsf{x}}\rangle \geq 0
\end{aligned}$$

In the second and in the third line we used the linearity of the pseudo-expectation map over sums of generalised observables and the definitions stated above. In the fourth step we apply Lemma 7 to the last addend and we fix the index $i = x$, at the price of a negligible function $\delta_{\mathrm{QHF}}(\kappa)$. We can apply this lemma because $C_x^{(d-k)}C_x^{(k)}$ has a QPT-implementable block encoding, since is composed by linear sums and multiplications of QPT-implementable generalised observables (Corollaries 1 and 2). Finally, using linearity we can group all the terms inside of one average over $\mathsf{x} = \mathsf{Enc}(x)$; we rephrase this sum as an operator square, which is non-negative by definition. □

Theorem 4. *Let's consider the d-dimensional SATWAP Bell inequality, with quantum bound $(\beta_d^{SATWAP})_q$, and its compiled version through Kalai protocol. If d is polynomial w.r.t. the security parameter κ, then the quantum bound of the compiled SATWAP inequality is $(\beta_d^{SATWAP})_q + \theta(\kappa)$, where $\theta(\cdot)$ is a negligible function.*

Proof. Applying the map $\tilde{\mathbb{E}}$ to the shifted SATWAP operator given in eq. (64) gives :

$$\tilde{\mathbb{E}}\left[\beta_q\mathbb{1} - \mathcal{B}_d^{\mathrm{SATWAP}}\right] = \frac{1}{2}\sum_{k=1}^{d-1}\left(\tilde{\mathbb{E}}\left[P_{1,k}^{\dagger}P_{1,k}\right] + \tilde{\mathbb{E}}\left[P_{2,k}^{\dagger}P_{2,k}\right]\right), \tag{76}$$

In Lemma 11 we proved that all elements in the sum on the r.h.s. are non-negative up to a negligible function, *i.e.*

$$\tilde{\mathbb{E}}\left[P_{x,k}^{\dagger}P_{x,k}\right] \approx_{\delta} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^{\dagger}\left(\omega^{k\mathsf{Dec}(\mathsf{a})}\mathbb{1} - C_x^{(k)}\right)^2 \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \tag{77}$$

This implies that there exists a negligible function of the security parameter $\theta(\kappa)$ such that the maximal quantum score $\bar{\beta}_q$ in the compiled SATWAP inequality becomes

$$\bar{\beta}_q \leq 2(d-1) + \theta(\kappa). \tag{78}$$

□

Let us now explore self-testing properties, and assume that a QPT prover achieved the score $\bar{\beta}_q$ in the compiled SATWAP inequality. Given eq. (76), reaching the optimal quantum score implies

$$0 = \frac{1}{2}\sum_{k=1}^{d-1}\left(\tilde{\mathbb{E}}\left[P_{1,k}^{\dagger}P_{1,k}\right] + \tilde{\mathbb{E}}\left[P_{2,k}^{\dagger}P_{2,k}\right]\right). \tag{79}$$

By using eqs. (77) and (79) we get

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^{\dagger}\left(\omega^{k\mathsf{Dec}(\mathsf{a})}\mathbb{1} - C_x^{(k)}\right)^2 \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \approx_{\delta} 0, \tag{80}$$

where we write δ as shorthand for δ_{QHE}. This further gives us

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \left\| C_x^{(k)}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle - \omega^{k\mathsf{Dec}(\mathsf{a})}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \right\|^2 \approx_{\delta} 0, \tag{81}$$

further implying that for every k, every $\mathtt{x}$ decrypting to x, and every $\mathtt{a}$

$$C_x^{(k)}\mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle \approx_\delta \omega^{k\mathsf{Dec}(\mathtt{a})}\mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle. \tag{82}$$

If we fix k' the previous relation implies

$$\begin{aligned}\left[C_x^{(1)}\right]^{k'}\mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle &\approx_\delta \left[C_x^{(1)}\right]^{k'-1}C_x^{(1)}\mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle\\ &\approx_{2\cdot\delta} \omega^{\mathsf{Dec}(\mathtt{a})}\left[C_x^{(1)}\right]^{k'-1}\mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle\\ &\approx_{3\cdot\delta} \omega^{2\mathsf{Dec}(\mathtt{a})}\left[C_x^{(1)}\right]^{k'-2}\mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle\\ &\dots\\ &\approx_{k'\cdot\delta} \omega^{k'\mathsf{Dec}(\mathtt{a})}\mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle\\ &\approx_{(k'+1)\cdot\delta} C_x^{(k')}\mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle,\end{aligned}$$

where in the second line we used eq. (82) for $k=1$, which we used successively until the last line where we used again eq. (82) for $k=k'$. By summing over $\mathtt{a}$, and noting that $k'<d$ which is polynomially bounded in the security parameter κ we get:

$$\left[C_x^{(1)}\right]^{k}|\psi\rangle \approx_{O(\delta)} C_x^{(k)}|\psi\rangle. \tag{83}$$

Now we develop the following expression for an arbitrary k

$$\begin{aligned}C_x^{(d-k)}C_x^{(k)}\mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle &\approx_\delta \omega^{k\mathsf{Dec}(\mathtt{a})}C_x^{(d-k)}\mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle\\ &\approx_{2\delta} \omega^{k\mathsf{Dec}(\mathtt{a})}\omega^{(d-k)\mathsf{Dec}(\mathtt{a})}\mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle\\ &= \omega^{d\mathsf{Dec}(\mathtt{a})}\mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle\\ &= \mathsf{M}_{\mathtt{a}|\mathtt{x}}|\psi\rangle,\end{aligned}$$

where for the first line we used eq. (82), for the second line we used the same equation by changing k to $d-k$, and the last line follows from $\omega^d=1$. Again by summing over $\mathtt{a}$ we obtain

$$C_x^{(d-k)}C_x^{(k)}|\psi\rangle \approx_{O(\delta)} |\psi\rangle, \tag{84}$$

Thus, on the support of $|\psi\rangle$ the observables $C_x^{(k)}$ satisfy condition

$$\left[C_x^{(1)}\right]^{k} \approx_{O(\delta)} C_x^{(k)}, \qquad C_x^{(d-k)}C_x^{(k)} \approx_{O(\delta)} \mathbb{1}. \tag{85}$$

In [25] it is proven that these two equations for $O(\delta)=0$ imply though Lemmas 1, 2, and 3 in the supplementary material therein that there exists a unitary U such that

$$U_B B_1^{(1)} U_B^\dagger = Z_d \otimes \mathbb{1}_{B'}, \qquad U_B B_2^{(1)} U_B^\dagger = T_d \otimes \mathbb{1}_{B'}, \tag{86}$$

with Z_d and T_d being given in Lemma 10. Since $B_1^{(1)}$ and $B_2^{(1)}$ are unitary we get $B_1^{(k)} = \left[B_1^{(1)}\right]^k$ and $B_2^{(k)} = \left[B_2^{(1)}\right]^k$. We conjecture that the derivation procedure is robust to noise, implying that in the case of reaching the optimal quantum violation of the compiled SATWAP inequality relations (86) hold up to a negligible function of the security parameter.

5 Computational self-test of any two binary measurements from a single prover

In the previous sections we showed that the KLVY compiler preserves the quantum bound for some classes of games; the natural follow-up question is to investigate whether the self-testing properties can also be translated. This opens up the possibility of defining single-prover self-testing protocols, based on computational assumptions.

Let us start by focusing on the self-test of any pair of binary observable. We identify in the non-locality literature an inequality that self tests such configuration; furthermore this is a specific XOR game, for which our result apply. We explicitly carry out the calculations for the robust case as well, showing the feasibility of a single-prover self-test of any pair of qubit observables, with computational assumptions.

More precisely, consider the class of correlation Bell inequalities as introduced in [52] and further discussed in [53]. This family of Bell inequalities is characterized by three parameters, namely, μ, ν, and χ. The Bell operator within this framework is defined as

$$\begin{aligned}\mathcal{B}_{\mu\nu\chi} = &\cos(\mu+\nu)\cos(\mu+\chi)(\cos(\chi)A_0 - \cos(\nu)A_1)\otimes B_0 \\ &+ \cos(\nu)\cos(\chi)(-\cos(\mu+\chi)A_0 + \cos(\mu+\nu)A_1)\otimes B_1.\end{aligned} \tag{87}$$

This formulation encompasses the CHSH inequality for $\mu = \chi = 0$ and $\nu = \pi$. A Bell inequality belonging to this class exhibits quantum violations when $\cos(\mu+\chi)\cos(\mu+\nu)\cos(\nu)\cos(\chi) < 0$. In instances where this condition is met, achieving the quantum limit,

$$\beta_q = \pm\sin(\mu)\sin(\chi-\nu)\sin(\mu+\nu+\chi) \tag{88}$$

self-tests the maximally entangled pair of qubits [54]. This characteristic renders it a viable candidate for our compilation procedure. The sum-of-squares (SOS) decomposition of the shifted Bell operator is

$$\beta_q \mathbb{1} - \mathcal{B}_{\mu\nu\chi} = c_0 P_0^\dagger P_0 + c_1 P_1^\dagger P_1, \tag{89}$$

where

$$c_0 = -\frac{\cos(\chi)\cos(\mu+\chi)}{2\sin(\mu)}, \quad c_1 = -\frac{\cos(\nu)\cos(\mu+\nu)}{2\sin(\mu)}$$

and

$$\begin{aligned}P_0 &= \sin(\mu)A_0 + \cos(\mu+\nu)B_0 - \cos(\nu)B_1 \\ P_1 &= \sin(\mu)A_1 + \cos(\mu+\chi)B_0 - \cos(\chi)B_1.\end{aligned}$$

Given the form of the SOS decomposition (89), the optimal value of the compiled inequality $\bar{\beta}_q$ is the same as the quantum bound β_q given in (88) up to a negligible function. Taking the pseudo-expectation value of Eq. (89) we get

$$\beta_q - \bar{\beta} = c_0\tilde{\mathbb{E}}\left[P_0^\dagger P_0\right] + c_1\tilde{\mathbb{E}}\left[P_1^\dagger P_1\right], \tag{90}$$

where $\bar{\beta}$ is the violation of the compiled inequality. As usual, we denote $\hat{B}_0 = (-\cos(\mu+\nu)B_0 + \cos(\nu)B_1)/\sin(\mu)$ and $\hat{B}_1 = -(\cos(\mu+\chi)B_0 + \cos(\chi)B_1)/\sin(\mu)$. If $\bar{\beta} = \beta_q - \varepsilon$, the equation above simplifies to

$$\varepsilon = c_0\tilde{\mathbb{E}}\left[P_0^\dagger P_0\right] + c_1\tilde{\mathbb{E}}\left[P_1^\dagger P_1\right] \tag{91}$$

where, as outlined in Lemma 8, the two terms on the right-hand side differ from a nonnegative function only by a negligible function contingent upon the quantum homomorphic encryption scheme:

$$\tilde{\mathbb{E}}\left[P_x^\dagger P_x\right] \geq \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \left\| \hat{B}_x|\psi_{\mathsf{a}|\mathsf{x}}\rangle - (-1)^{\mathsf{Dec}(\mathsf{a})}|\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 - \delta_{\mathrm{QHE}}(\kappa).$$

Employing this bound in eq. (91) yields:

$$\begin{aligned}\varepsilon + (c_0+c_1)\delta_{\mathrm{QHE}}(\kappa) \geq &c_0 \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}} \left\| \hat{B}_0|\psi_{\mathsf{a}|\mathsf{x}}\rangle - (-1)^{\mathsf{Dec}(\mathsf{a})}|\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \\ &+ c_1 \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(1)} \sum_{\mathsf{a}} \left\| \hat{B}_1|\psi_{\mathsf{a}|\mathsf{x}}\rangle - (-1)^{\mathsf{Dec}(\mathsf{a})}|\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2\end{aligned}$$

where now the right-hand side comprises solely positive quantities

Hence, for all values of x we obtain:

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \left\| \hat{B}_x|\psi_{\mathsf{a}|\mathsf{x}}\rangle - (-1)^{\mathsf{Dec}(\mathsf{a})}|\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \leq \frac{\varepsilon}{c_x} + \frac{c_0+c_1}{c_x}\delta_{\mathrm{QHE}}(\kappa) \qquad \forall x \in \{0,1\}. \tag{92}$$

We initially consider the noiseless and infinite security case *i.e.* $\varepsilon = 0$ and $\delta_{\text{QHE}} = 0$ for pedagogical purposes, acknowledging that the actual scenario does not conform to our simplified model. The equation above would imply that every addend is equal to zero, implying

$$\hat{B}_x|\psi_{\mathsf{a}|\mathsf{x}}\rangle = (-1)^{\mathsf{Dec}(\mathsf{a})}|\psi_{\mathsf{a}|\mathsf{x}}\rangle, \qquad \forall \mathsf{x} : \mathsf{Dec}(\mathsf{x}) = x, \forall \mathsf{a}.$$

When the quantum bound is saturated, the square of the hat operator $\hat{B}_x$ acts like identity on $|\psi_{\mathsf{a}|\mathsf{x}}\rangle$:

$$(\hat{B}_x)^2|\psi_{\mathsf{a}|\mathsf{x}}\rangle = (-1)^{\mathsf{Dec}(\mathsf{a})}\hat{B}_x|\psi_{\mathsf{a}|\mathsf{x}}\rangle = |\psi_{\mathsf{a}|\mathsf{x}}\rangle \qquad \forall \mathsf{x} : \mathsf{Dec}(\mathsf{x}) = x, \forall \mathsf{a}. \tag{93}$$

By the definition of $\hat{B}_0$, and assuming $B_0^2 = B_1^2 = \mathbb{1}$, the following is always true for every state:

$$\begin{aligned}(\hat{B}_0)^2|\psi_{\mathsf{a}|\mathsf{x}}\rangle &= \left(\frac{\cos^2(\nu) + \cos^2(\nu+\mu)}{\sin^2(\mu)}\mathbb{1} - \frac{\cos(\nu)\cos(\nu+\mu)}{\sin^2(\mu)}\{B_0, B_1\}\right)|\psi_{\mathsf{a}|\mathsf{x}}\rangle \\ &= k_{\mathbb{1}}|\psi_{\mathsf{a}|\mathsf{x}}\rangle - k_{\{\}}\{B_0, B_1\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle \end{aligned} \tag{94}$$

where in the second line we simply fixed a notation for the coefficients of the operators. Equations (93) and (94) together fix the value of the anti-commutator of Bob's observables when the maximal quantum violation is achieved:

$$\{B_0, B_1\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle = \frac{k_{\mathbb{1}} - 1}{k_{\{\}}}|\psi_{\mathsf{a}|\mathsf{x}}\rangle = 2\cos(\mu)|\psi_{\mathsf{a}|\mathsf{x}}\rangle \qquad \forall \mathsf{x} : \mathsf{Dec}(\mathsf{x}) = x, \forall \mathsf{a}$$

where the second inequality is a simple trigonometric identity

$$\frac{k_{\mathbb{1}} - 1}{k_{\{\}}} = \frac{\cos^2(\nu) + \cos^2(\nu+\mu) - \sin^2(\mu)}{\sin^2(\mu)} \frac{\sin^2(\mu)}{\cos(\nu)\cos(\nu+\mu)} = 2\cos(\mu).$$

Since all observables are binary, this is a self-test. Indeed, Jordan's lemma ensures that B_0 and B_1 can be simultaneously block-diagonalised such that all blocks are either of size 2×2 or 1×1. In the same way like in [55], we embed every 1×1 into a Hilbert space of larger dimension. This operation does not affect the correlation probabilities, and it simplifies our analysis, as we work with a Jordan decomposition in which all blocks are of the size 2×2. Without loss of generalisation, we can apply a local unitary to the observable B_0 and bring it to Pauli's σ_x in every 2×2 block:

$$UB_0U^\dagger = \sigma_x \otimes \sum_i |i\rangle\langle i|. \tag{95}$$

We can also safely bring all the 2×2 blocks of B_1 to the XZ plane of the Bloch sphere; by fixing the value of the anti-commutator, we get that B_1 has $\cos(\mu)\sigma_x + \sin(\mu)\sigma_z$ in every block. For every $\mu \neq 0$ we can find ν and χ such that the condition $\cos(\mu+\chi)\cos(\mu+\nu)\cos(\nu)\cos(\chi) < 0$ is satisfied, implying that the quantum bound is larger than the classical. This implies that in the noiseless and infinite QHE security case we can perform a single-prover self-test of any two observables applied by Bob, *i.e.* for every μ there is a compiled XOR game whose maximal violation self-tests Bob's measurements implying:

$$UB_0U^\dagger = \sigma_x \otimes \mathbb{1}, \qquad UB_1U^\dagger = (\cos(\mu)\sigma_x + \sin(\mu)\sigma_z) \otimes \mathbb{1} \tag{96}$$

The assumptions made in our simplified case are unrealistic, both from a cryptographic and experimental point of view. Assuming a finite security parameter κ and small experimental deviations ε, we can still prove that the anti-commutator of Bob's observables is close to the noiseless value, obtaining a robust self-test for Bob's binary observables. Let's start considering Eq. (92) with $\mathsf{x} = \mathsf{Enc}(0)$, and open the sum over a:

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \left[\sum_{\mathsf{a}=\mathsf{Enc}(0)} \left\| (\hat{B}_0 - \mathbb{1})|\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 + \sum_{\mathsf{a}=\mathsf{Enc}(1)} \left\| (\hat{B}_0 + \mathbb{1})|\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \right] \leq \frac{\varepsilon}{c_0} + \frac{c_0 + c_1}{c_0}\delta_{\text{QHE}}(\kappa)$$

We call the vectors inside the norms as $|\Delta^{\pm}_{\mathsf{a}|\mathsf{x}}\rangle = (\hat{B}_0 \pm \mathbb{1})|\psi_{\mathsf{a}|\mathsf{x}}\rangle$, hence we can write:

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \left[\sum_{\mathsf{a}=\mathsf{Enc}(0)} \left\| |\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 + \sum_{\mathsf{a}=\mathsf{Enc}(1)} \left\| |\Delta^{+}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \right] \leq \frac{\varepsilon}{c_0} + \frac{c_0 + c_1}{c_0}\delta_{\text{QHE}}(\kappa) \tag{97}$$

The square of $\hat{B}_0$ is

$$\begin{aligned}(\hat{B}_0)^2 &= \mathbb{1} + (\hat{B}_0 - \mathbb{1}) + \hat{B}_0(\hat{B}_0 - \mathbb{1}) = \mathbb{1} - (\hat{B}_0 + \mathbb{1}) + \hat{B}_0(\hat{B}_0 + \mathbb{1}) \\ &= k_{\mathbb{1}}\mathbb{1} - k_{\{\}}\{B_0, B_1\}\end{aligned}$$

where the first lines are trivial identities, and in the second line we rewrote Eq. (94). Rearranging the terms, and applying the observables on $|\psi_{\mathsf{a}|\mathsf{x}}\rangle$, we obtain the following formula for the anti-commutator of Bob's observables:

$$\left[2\cos(\mu)\mathbb{1} - \{B_0, B_1\}\right]|\psi_{\mathsf{a}|\mathsf{x}}\rangle = \pm\frac{1}{k_{\{\}}}|\Delta^{\mp}_{\mathsf{a}|\mathsf{x}}\rangle + \frac{1}{k_{\{\}}}\hat{B}_0|\Delta^{\mp}_{\mathsf{a}|\mathsf{x}}\rangle$$

where to find $2\cos(\mu)$ we used again the trigonometric identity above. Let us first focus on the equation with $|\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle$. We compute its norm squared, averaging over $\mathsf{x} = \mathsf{Enc}(0)$ and summing over $\mathsf{a} = \mathsf{Enc}(0)$

$$\begin{aligned}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)}\sum_{\mathsf{a}=\mathsf{Enc}(0)}\left\|\left[2\cos(\mu)\mathbb{1} - \{B_0, B_1\}\right]|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 &= \frac{1}{k_{\{\}}^2}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)}\sum_{\mathsf{a}=\mathsf{Enc}(0)}\left\||\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle + \hat{B}_0|\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 \\ &\leq \frac{1}{k_{\{\}}^2}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)}\sum_{\mathsf{a}=\mathsf{Enc}(0)}\left(\left\||\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 + \left\|\hat{B}_0|\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2\right) \\ &\leq \frac{1}{k_{\{\}}^2}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)}\sum_{\mathsf{a}=\mathsf{Enc}(0)}\left(\left\||\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 + \|\hat{B}_0\|^2\left\||\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2\right) \\ &= \frac{1 + \|\hat{B}_0\|^2}{k_{\{\}}^2}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)}\sum_{\mathsf{a}=\mathsf{Enc}(0)}\left\||\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2\end{aligned}$$

where we used Cauchy-Schwarz and the triangle inequality. Similarly, we can find a similar bound summing over $\mathsf{a} = \mathsf{Enc}(1)$ and using the decomposition of the anti-commutator with the vectors $|\Delta^{+}_{\mathsf{a}|\mathsf{x}}\rangle$:

$$\begin{aligned}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)}\sum_{\mathsf{a}=\mathsf{Enc}(1)}\left\|\left[2\cos(\mu)\mathbb{1} - \{B_0, B_1\}\right]|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 &= \frac{1}{k_{\{\}}^2}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)}\sum_{\mathsf{a}=\mathsf{Enc}(1)}\left\|-|\Delta^{+}_{\mathsf{a}|\mathsf{x}}\rangle + \hat{B}_0|\Delta^{+}_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 \\ &\leq \frac{1 + \|\hat{B}_0\|^2}{k_{\{\}}^2}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)}\sum_{\mathsf{a}=\mathsf{Enc}(1)}\left\||\Delta^{+}_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2\end{aligned}$$

Now, putting together these two result we can bound the sum over a

$$\begin{aligned}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)}\sum_{\mathsf{a}}\left\|\left[2\cos(\mu)\mathbb{1} - \{B_0, B_1\}\right]|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 &\leq \frac{1 + \|\hat{B}_0\|^2}{k_{\{\}}^2}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)}\left[\sum_{\mathsf{a}=\mathsf{Enc}(0)}\left\||\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 + \sum_{\mathsf{a}=\mathsf{Enc}(1)}\left\||\Delta^{+}_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2\right] \\ &\leq \frac{1 + \|\hat{B}_0\|^2}{k_{\{\}}^2}\left(\frac{\varepsilon}{c_0} + \frac{c_0 + c_1}{c_0}\delta_{\mathrm{QHE}}(\kappa)\right) \\ &\leq \sin^2(\mu)\left[2\cos(\mu) + \frac{1}{\cos(\nu)\cos(\nu + \mu)}\right]\left(\frac{\varepsilon}{c_0} + \frac{c_0 + c_1}{c_0}\delta_{\mathrm{QHE}}(\kappa)\right)\end{aligned}$$

where in the second line we used the bound found in Eq. (97). The angles are fixed from the inequality, therefore in the last line we have some negligible functions in ϵ and κ multiplied by some constant factors depending on the angles. Therefore we proved that, on the support of the states used in the compiled game, the anti-commutator of Bob's observable is $2\cos(\mu)\mathbb{1}$ up to a function $\eta_{anticomm}$:

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)}\sum_{\mathsf{a}}\left\|\left[2\cos(\mu)\mathbb{1} - \{B_0, B_1\}\right]|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 \leq \eta_{anticomm}(\epsilon, \kappa, \nu, \mu) \tag{98}$$

We can adapt the procedure for $x = 1$. We start by reformulating Eq. (94) for the observable $\hat{B}_1$:

$$(\hat{B}_1)^2|\psi_{\mathsf{a}|\mathsf{x}}\rangle = \left(\frac{\cos^2(\chi) + \cos^2(\chi + \mu)}{\sin^2(\mu)}\mathbb{1} + \frac{\cos(\chi)\cos(\chi + \mu)}{\sin^2(\mu)}\{B_0, B_1\}\right)|\psi_{\mathsf{a}|\mathsf{x}}\rangle$$

Following the same steps, we get an equivalent statement for the anticommutator averaged over $\mathsf{x} = \mathsf{Enc}(1)$:

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(1)} \sum_{\mathsf{a}} \left\| [2\cos(\mu)\mathbb{1} + \{B_0, B_1\}] \, |\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \leq \sin^2(\mu) \left[2\cos(\mu) + \frac{1}{\cos(\chi)\cos(\chi+\mu)} \right] \left(\frac{\varepsilon}{c_1} + \frac{c_0+c_1}{c_1} \delta_{\mathrm{QHE}}(\kappa) \right)$$
$$\leq \eta'_{anticomm}(\epsilon, \kappa, \chi, \mu).$$

These equations imply that the anticommutator of B_0 and B_1 is approximately equal to $2\cos(\mu)\mathbb{1}$. For binary observables, this is enough to prove robust self-testing of Bob's observables. The proof of this statement can be found in [56].

6 Computational self-test of three Pauli observables

In this section, we present a single-prover self-testing protocol for the triplet of Pauli observables. As in previous cases, we rely on a known inequality—the Elegant Bell inequality—whose quantum bound is preserved and for which a cryptographic sum-of-squares (SOS) decomposition is well-defined. The SOS decomposition then serves as the key tool for establishing the robust self-testing result. The result provides a complete toolkit for certifying an arbitrary single-qubit state or operation under standard cryptographic assumptions.

The Elegant Bell inequality, first introduced in [57], is defined for two parties and binary observables, with input sets $\mathsf{X} \in [4]$ and $\mathsf{Y} \in [3]$. The Bell operator has the form

$$\mathcal{B}^{el} = (A_0 + A_1 - A_2 - A_3) \otimes B_0 + (A_0 - A_1 + A_2 - A_3) \otimes B_1 + (A_0 - A_1 - A_2 + A_3) \otimes B_2$$

The quantum bound $\beta_q = 4\sqrt{3}$ self-tests a maximally entangled pair of qubits and all three Pauli observables measured by Bob [58].

The nonlocal game corresponding to the elegant Bell inequality is an XOR game, therefore Theorem 3 applies and the quantum bound of the compiled game is preserved. In the following section we prove that the self-testing properties of this game are also preserved by Kalai compilation.

The standard SOS decomposition for the shifted elegant Bell operator is

$$\beta_q \mathbb{1} - \mathcal{B}^{el} = \frac{\sqrt{3}}{2} \sum_{i=0}^{3} P_i^2 \tag{99}$$

with the following definition for the polynomials P_i:

$$P_0 = A_0 - \frac{B_0 + B_1 + B_2}{\sqrt{3}}, \qquad P_1 = A_1 - \frac{B_0 - B_1 - B_2}{\sqrt{3}},$$
$$P_2 = A_2 - \frac{-B_0 + B_1 - B_2}{\sqrt{3}}, \qquad P_3 = A_3 - \frac{-B_0 - B_1 + B_2}{\sqrt{3}}.$$

We use the standard notation $P_i = A_i - \hat{B}_i$ and repeat the procedure of taking the pseudo-expectation value of the shifted Bell operator to get the bound on the sum-of-square elements. When the compiled game reaches the score $\bar{\beta} = \beta_q - \epsilon$, the following is true

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \left\| \hat{B}_x |\psi_{\mathsf{a}|\mathsf{x}}\rangle - (-1)^{\mathsf{Dec}(\mathsf{a})} |\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \leq \frac{2}{\sqrt{3}} \varepsilon + 4\delta_{\mathrm{QHE}}(\kappa) \qquad \forall x. \tag{100}$$

For simplicity we study first the noiseless case, with $\delta_{\mathrm{QHE}}(\kappa) = 0$ and $\varepsilon = 0$, implying that

$$\hat{B}_x |\psi_{\mathsf{a}|\mathsf{x}}\rangle - (-1)^{\mathsf{Dec}(\mathsf{a})} |\psi_{\mathsf{a}|\mathsf{x}}\rangle = 0, \qquad \forall \mathsf{x} : \mathsf{Dec}(\mathsf{x}) = x, \forall x.$$

Once again, this proves that the square of the hat operator acts like identity on $|\psi_{\mathsf{a}|\mathsf{x}}\rangle$:

$$(\hat{B}_x)^2 |\psi_{\mathsf{a}|\mathsf{x}}\rangle = (-1)^{\mathsf{Dec}(\mathsf{a})} \hat{B}_x |\psi_{\mathsf{a}|\mathsf{x}}\rangle = |\psi_{\mathsf{a}|\mathsf{x}}\rangle. \tag{101}$$

The square of the hat operator can be completely characterized in terms of the anti-commutators of the observables, assuming their projectivity $B_1^2 = B_2^2 = B_3^2 = \mathbb{1}$. Let's consider $x = 1$, then

$$(\hat{B}_1)^2 = \mathbb{1} + \frac{1}{3}\big(\{B_1, B_2\} + \{B_2, B_3\} + \{B_1, B_3\}\big).$$

Considering all possible x and Eq. (101), we obtain the following system of equations :

$$\begin{aligned}
\big(+ \{B_1, B_2\} + \{B_2, B_3\} + \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle = 0,\\
\big(- \{B_1, B_2\} + \{B_2, B_3\} - \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle = 0,\\
\big(- \{B_1, B_2\} - \{B_2, B_3\} + \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle = 0,\\
\big(+ \{B_1, B_2\} - \{B_2, B_3\} - \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle = 0
\end{aligned}$$

whose only solution is

$$\{B_1, B_2\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle = \{B_2, B_3\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle = \{B_1, B_3\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle = 0. \tag{102}$$

This completely fixes the three observales: they must be unitarely equivalent to the three Pauli's. See Appendix C of [56] for a formal proof of this statement.

To make the self-testing cryptographically and experimentally meaningful it needs to be robust to noise, *i.e.* we need to consider a non-zero ε and $\delta_{\mathrm{QHE}}(\kappa)$. We want to prove that all the anti-commutators are a negligible function depending on the noise ε and the security parameter κ:

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}} \big\|\{B_{y_1}, B_{y_2}\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2 \leq \eta(\epsilon, \kappa) \qquad \forall y_1 \neq y_2.$$

Using similar tricks as in the previous section we get the following system of equations:

$$\begin{aligned}
\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}} \big\|\big(+ \{B_1, B_2\} + \{B_2, B_3\} + \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2 &\leq 9(1+\sqrt{3})\left(\frac{2}{\sqrt{3}}\varepsilon + 4\delta_{\mathrm{QHE}}(\kappa)\right),\\
\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(1)} \sum_{\mathsf{a}} \big\|\big(- \{B_1, B_2\} + \{B_2, B_3\} - \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2 &\leq 9(1+\sqrt{3})\left(\frac{2}{\sqrt{3}}\varepsilon + 4\delta_{\mathrm{QHE}}(\kappa)\right),\\
\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(2)} \sum_{\mathsf{a}} \big\|\big(- \{B_1, B_2\} - \{B_2, B_3\} + \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2 &\leq 9(1+\sqrt{3})\left(\frac{2}{\sqrt{3}}\varepsilon + 4\delta_{\mathrm{QHE}}(\kappa)\right),\\
\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(3)} \sum_{\mathsf{a}} \big\|\big(+ \{B_1, B_2\} - \{B_2, B_3\} - \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2 &\leq 9(1+\sqrt{3})\left(\frac{2}{\sqrt{3}}\varepsilon + 4\delta_{\mathrm{QHE}}(\kappa)\right).
\end{aligned}$$

In equations above the averages are computed across various values of x, but from them we can obtain the averages over the same value $\bar{x}$, albeit incurring an additional cost represented by $\delta_{\mathrm{QHE}}(\kappa)$ on the right-hand side. We proceed by expanding the constituent terms within the norms. Subsequently, for each equation within the system, an analogous treatment is employed, yielding expressions akin to:

$$\begin{aligned}
&\big\|\big(\{B_1, B_2\} + \{B_2, B_3\} + \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2 =\\
&= \big\|\{B_1, B_2\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2 + \big\|\{B_2, B_3\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2 + \big\|\{B_3, B_1\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2 +\\
&+ \langle\psi_{\mathsf{a}|\mathsf{x}}|\{\{B_1, B_2\}, \{B_2, B_3\}\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle + \langle\psi_{\mathsf{a}|\mathsf{x}}|\{\{B_1, B_2\}, \{B_1, B_3\}\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle + \langle\psi_{\mathsf{a}|\mathsf{x}}|\{\{B_1, B_3\}, \{B_2, B_3\}\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle
\end{aligned}$$

with possibly different signs in the last line. When we sum all of the inequalities; only the terms with the norm of the anti-commutators are going to survive, hence

$$4 \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(\bar{x})} \sum_{\mathsf{a}} \left(\big\|\{B_1, B_2\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2 + \big\|\{B_2, B_3\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2 + \big\|\{B_3, B_1\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2\right) \leq 4(9(1+\sqrt{3}))\left(\frac{2}{\sqrt{3}}\varepsilon + 4\delta_{\mathrm{QHE}}(\kappa)\right).$$

All the terms in the sum are positive, hence we obtain the desired bound for all the pairs of anti-correlators:

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(\bar{x})} \sum_{\mathsf{a}} \big\|\{B_{y_1}, B_{y_2}\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\big\|^2 \leq 6(3+\sqrt{3})\varepsilon + 36(1+\sqrt{3})\delta_{\mathrm{QHE}}(\kappa) \qquad \forall y_1 \neq y_2 \tag{103}$$

which is indeed the robust version of equation (102).

7 Open problems

Our findings reveal that the compilation procedure introduced in [19] effectively preserves the quantum bound of XOR games. However, it remains uncertain whether this preservation extends to generic nonlocal games. As demonstrated, the compilation of Bell inequalities is feasible, yet determining whether the quantum bound preservation holds for Bell inequalities not expressible as nonlocal games poses a challenge. In both scenarios, the complexity arises from the inability to find the quantum bound using a simple correlation matrix and the duality of semi-definite programming. Resolving this likely requires using the NPA hierarchy and employing moment matrices with numerous nonobservable elements. An additional open problem pertains to the quantum behavior of compiled games involving more than two players. Modeling a single quantum prover in such instances necessitates a rigorous characterization of sequential encrypted operations. Lastly, understanding the relationship between self-testing in standard nonlocal games and their compiled counterparts proves to be an instructive avenue for future exploration.

Acknowledgements

We thank Paul Hermouet, Dominik Leichtle, Mirjam Weilenmann, Jef Pauwels and Borivoje Dakić for insightful discussions. MB acknowledges funding from QuantEdu France, a state aid managed by the French National Research Agency for France 2030 with the reference ANR-22-CMAS-0001. BB acknowledges support from the European Commission Horizon-CL4 program under grant agreement 101135288 for the EPIQUE project. IŠ and DM acknowledge funding from PEPR integrated project EPiQ ANR-22-PETQ-0007 part of Plan France 2030. ED acknowledges funding from the European Union's Horizon Europe research and innovation program under the grant agreement No 101114043 (QSNP).

References

[1] J. S. Bell. "On the Einstein Podolsky Rosen paradox". Physics Physique Fizika **1**, 195–200 (1964).

[2] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. "Proposed experiment to test local hidden-variable theories". Phys. Rev. Lett. **23**, 880 (1969).

[3] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. "Bell nonlocality". Rev. Mod. Phys. **86**, 419–478 (2014).

[4] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. "Device-independent security of quantum cryptography against collective attacks". Phys. Rev. Lett. **98**, 230501 (2007).

[5] Umesh Vazirani and Thomas Vidick. "Fully Device-Independent Quantum Key Distribution". Phys. Rev. Lett. **113**, 140501 (2014).

[6] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. "Practical device-independent quantum cryptography via entropy accumulation". Nature Communications **9**, 459 (2018).

[7] Roger Colbeck. "Quantum and relativistic protocols for secure multi-party computation". PhD thesis. University of Cambridge. (2007).

[8] S. Pironio, A. Acín, 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).

[9] Antonio Acín and Lluis Masanes. "Certified randomness in quantum physics". Nature **540**, 213–219 (2016).

[10] Dominic Mayers and Andrew Yao. "Self testing quantum apparatus". Quantum Info. Comput. **4**, 273–286 (2004).

[11] Ivan Šupić and Joseph Bowles. "Self-testing of quantum systems: a review". Quantum **4**, 337 (2020).

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

[13] Andrea Coladangelo, Alex B Grilo, Stacey Jeffery, and Thomas Vidick. "Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources". In Annual international conference on the theory and applications of cryptographic techniques. Pages 247–277. Springer (2019). arXiv:1708.07359.

[14] László Babai, Lance Fortnow, and Carsten Lund. "Non-deterministic exponential time has two-prover interactive protocols". Computational complexity **1**, 3–40 (1991).

[15] Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. "Delegation for bounded space". In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, 45th Annual ACM Symposium on Theory of Computing. Pages 565–574. ACM Press (2013).

[16] Tony Metger, Anand Natarajan, and Tina Zhang. "Succinct arguments for QMA from standard assumptions via compiled nonlocal games". In 65th Annual Symposium on Foundations of Computer Science. Pages 1193–1201. IEEE Computer Society Press (2024).

[17] William Aiello, Sandeep Bhatt, Rafail Ostrovsky, and S Raj Rajagopalan. "Fast verification of any remote procedure call: Short witness-indistinguishable one-round proofs for NP". In International Colloquium on Automata, Languages, and Programming. Pages 463–474. Springer (2000).

[18] Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. "How to delegate computations: the power of no-signaling proofs". In David B. Shmoys, editor, 46th Annual ACM Symposium on Theory of Computing. Pages 485–494. ACM Press (2014).

[19] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. "Quantum advantage from any non-local game". In Barna Saha and Rocco A. Servedio, editors, 55th Annual ACM Symposium on Theory of Computing. Pages 1617–1628. ACM Press (2023).

[20] Urmila Mahadev. "Classical homomorphic encryption for quantum circuits". In Mikkel Thorup, editor, 59th Annual Symposium on Foundations of Computer Science. Pages 332–338. IEEE Computer Society Press (2018).

[21] Zvika Brakerski. "Quantum FHE (almost) as secure as classical". In Hovav Shacham and Alexandra Boldyreva, editors, Advances in Cryptology – CRYPTO 2018, Part III. Volume 10993 of Lecture Notes in Computer Science, pages 67–95. Springer, Cham (2018).

[22] Anand Natarajan and Tina Zhang. "Bounding the quantum value of compiled nonlocal games: From CHSH to BQP verification". In 64th Annual Symposium on Foundations of Computer Science. Pages 1342–1348. IEEE Computer Society Press (2023).

[23] Zvika Brakerski, Alexandru Gheorghiu, Gregory D. Kahanamoku-Meyer, Eitan Porat, and Thomas Vidick. "Simple tests of quantumness also certify qubits". In Helena Handschuh and Anna Lysyanskaya, editors, Advances in Cryptology – CRYPTO 2023, Part V. Volume 14085 of Lecture Notes in Computer Science, pages 162–191. Springer, Cham (2023).

[24] Alexia Salavrakos, Remigiusz Augusiak, Jordi Tura, Peter Wittek, Antonio Acín, and Stefano Pironio. "Bell inequalities tailored to maximally entangled states". Phys. Rev. Lett. **119**, 040402 (2017).

[25] Shubhayan Sarkar, Debashis Saha, Jędrzej Kaniewski, and Remigiusz Augusiak. "Self-testing quantum systems of arbitrary local dimension with minimal number of measurements". npj Quantum Information**7** (2021).

[26] 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" (2024). arXiv:2402.17301.

[27] Arthur Mehta, Connor Paddock, and Lewis Wooltorton. "Self-testing in the compiled setting via tilted-chsh inequalities" (2025). arXiv:2406.04986.

[28] Alexander Kulpe, Giulio Malavolta, Connor Paddock, Simon Schmidt, and Michael Walter. "A bound on the quantum value of all compiled nonlocal games" (2024). arXiv:2408.06711.

[29] Arthur Fine. "Hidden variables, joint probability, and the Bell inequalities". Phys. Rev. Lett. **48**, 291–295 (1982).

[30] J. Silman, S. Machnes, and N. Aharon. "On the relation between Bell's inequalities and nonlocal games". Physics Letters A **372**, 3796–3800 (2008).

[31] Samson Abramsky and Lucien Hardy. "Logical Bell inequalities". Phys. Rev. A **85**, 062114 (2012).

[32] Boris Tsirelson. "Quantum analogues of the Bell inequalities. the case of two spatially separated domains". Journal of Soviet Mathematics **36**, 557–570 (1987).

[33] Llorenç Escolà, John Calsamiglia, and Andreas Winter. "All tight correlation Bell inequalities have quantum violations". Phys. Rev. Res. **2**, 012044 (2020).

[34] Stephanie Wehner. "Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities". Phys. Rev. A **73**, 022110 (2006).

[35] Miguel Navascués, Stefano Pironio, and Antonio Acín. "Bounding the set of quantum correlations". Phys. Rev. Lett. **98**, 010401 (2007).

[36] Miguel Navascués and Harald Wunderlich. "A glance beyond the quantum model". Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **466**, 881–890 (2010).

[37] Monique Laurent. "Sums of squares, moment matrices and optimization over polynomials". Emerging applications of algebraic geometryPages 157–270 (2009).

[38] Armin Tavakoli, Alejandro Pozas-Kerstjens, Peter Brown, and Mateus Araújo. "Semidefinite programming relaxations for quantum correlations". Reviews of Modern Physics**96** (2024).

[39] Dimiter Ostrev. "The structure of nearly-optimal quantum strategies for the non-local xor games". Quantum Information & Computation **16**, 1191–1211 (2016).

[40] Ronald L Rivest, Len Adleman, and Michael L Dertouzos. "On data banks and privacy homomorphisms". Foundations of secure computation **4**, 169–180 (1978). url: `https://api.semanticscholar.org/CorpusID:6905087`.

[41] Ronald L Rivest, Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems". Communications of the ACM **21**, 120–126 (1978).

[42] Craig Gentry. "Fully homomorphic encryption using ideal lattices". In Michael Mitzenmacher, editor, 41st Annual ACM Symposium on Theory of Computing. Pages 169–178. ACM Press (2009).

[43] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. "(Leveled) fully homomorphic encryption without bootstrapping". In Shafi Goldwasser, editor, ITCS 2012: 3rd Innovations in Theoretical Computer Science. Pages 309–325. Association for Computing Machinery (2012).

[44] Zvika Brakerski and Vinod Vaikuntanathan. "Efficient fully homomorphic encryption from (standard) LWE". SIAM Journal on computing **43**, 831–871 (2014).

[45] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. "Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics". In Moses Charikar and Edith Cohen, editors, 51st Annual ACM Symposium on Theory of Computing. Pages 193–204. ACM Press (2019).

[46] Jędrzej Kaniewski, Ivan Šupić, Jordi Tura, Flavio Baccari, Alexia Salavrakos, and Remigiusz Augusiak. "Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems". Quantum **3**, 198 (2019).

[47] H. Buhrman and S. Massar. "Causality and tsirelson's bounds". Phys. Rev. A **72**, 052103 (2005).

[48] Mohammad Bavarian and Peter W. Shor. "Information causality, szemerédi-trotter and algebraic variants of chsh" (2014). arXiv:1311.5186.

[49] Yeong-Cherng Liang, Chu-Wee Lim, and Dong-Ling Deng. "Reexamination of a multisetting bell inequality for qudits". Phys. Rev. A **80**, 052116 (2009).

[50] Ravishankar Ramanathan, Remigiusz Augusiak, and Gláucia Murta. "Generalized xor games with d outcomes and the task of nonlocal computation". Phys. Rev. A **93**, 022333 (2016).

[51] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu. "Bell inequalities for arbitrarily high-dimensional systems". Physical review letters **88**, 040404 (2002).

[52] Thinh P. Le, Chiara Meroni, Bernd Sturmfels, Reinhard F. Werner, and Timo Ziegler. "Quantum correlations in the minimal scenario". Quantum **7**, 947 (2023).

[53] Victor Barizien, Pavel Sekatski, and Jean-Daniel Bancal. "Custom bell inequalities from formal sums of squares". Quantum **8**, 1333 (2024).

[54] Lewis Wooltorton, Peter Brown, and Roger Colbeck. "Device-independent quantum key distribution with arbitrarily small nonlocality". Phys. Rev. Lett. **132**, 210802 (2024).

[55] Ivan Šupić, Jean-Daniel Bancal, Yu Cai, and Nicolas Brunner. "Genuine network quantum nonlocality and self-testing". Physical Review A**105** (2022).

[56] Jędrzej Kaniewski. "Self-testing of binary observables based on commutation". Phys. Rev. A **95**, 062323 (2017).

[57] Nicolas Gisin. "Bell inequalities: Many questions, a few answers". Pages 125–138. Springer Netherlands. Dordrecht (2009).

[58] Antonio Acín, Stefano Pironio, Tamás Vértesi, and Peter Wittek. "Optimal randomness certification from one entangled bit". Physical Review A**93** (2016).