Device-independent quantum key distribution from generalized CHSH inequalities

Device-independent quantum key distribution from generalized CHSH inequalities

Pavel Sekatski[1], Jean-Daniel Bancal[2], Xavier Valcarce[3], Ernest Y.-Z. Tan[4], Renato Renner[4], and Nicolas Sangouard[1,3]

[1]Department of Physics, University of Basel, Klingelbergstrasse 82, 4056 Basel, Switzerland
[2]Department of Applied Physics, University of Geneva, Chemin de Pinchat 22, 1211 Geneva, Switzerland
[3]Université Paris-Saclay, CEA, CNRS, Institut de physique théorique, 91191, Gif-sur-Yvette, France
[4]Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland
April 12, 2021

Device-independent quantum key distribution aims at providing security guarantees even when using largely uncharacterised devices. In the simplest scenario, these guarantees are derived from the CHSH score, which is a simple linear combination of four correlation functions. We here derive a security proof from a generalisation of the CHSH score, which effectively takes into account the individual values of two correlation functions. We show that this additional information, which is anyway available in practice, allows one to get higher key rates than with the CHSH score. We discuss the potential advantage of this technique for realistic photonic implementations of device-independent quantum key distribution.

1 Introduction

The aim of quantum key distribution (QKD) is to give two parties — Alice & Bob — the possibility to generate a secret key when they share a quantum channel. For instance, in the implementation proposed by Ekert [1], the channel consists of a source producing entangled particles that are distributed to Alice & Bob. At each round, each of Alice & Bob measure one particle by choosing one out of several measurement settings. The claim that Alice's measurement results are secure, i.e. unknown to any third party – Eve – who may control the quantum channel, is guaranteed by inferring (from Alice and Bob's measurement results) that the source emits states close to pure bipartite entangled states. This ensures at the same time that Bob's results are correlated to Alice's ones if he chooses an appropriate measurement setting, i.e. Alice and Bob's measurement results can form a secret key.

Ekert suggested that the information about the key that may be available to an adversary can be quantified by choosing settings allowing Alice & Bob to violate a Bell inequality. This idea was later progressively formalised and led to what is now called device-independent QKD (DIQKD). In its simplest version, DIQKD is implemented by letting Alice choose randomly between two measurement settings at each round, A_x where $x \in \{0,1\}$, while Bob's measurement includes three possible settings, B_y where $y \in \{0,1,2\}$. For settings $x, y \in \{0,1\}$, the results – which can possibly take many values – are post-processed locally and turned into binary values $\mathsf{A}_x, \mathsf{B}_y \in \{-1,+1\}$. After several iterations, Alice and Bob communicate classically to estimate the *CHSH score*

$$S = \langle A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1) \rangle \qquad (1)$$

where $\langle A_x \otimes B_y \rangle = p(\mathsf{A}_x = \mathsf{B}_y | x, y) - p(\mathsf{A}_x \neq \mathsf{B}_y | x, y)$ quantifies the correlation between the outcomes for measurement choices x and y, respectively. The remaining measurement setting $y = 2$ is chosen to generate an outcome B_2 that minimises the uncertainty with respect to A_0. Alice then forms the raw key from the outcomes A_0 of the pairs that Bob measured with respect to $y = 2$.

We consider n such rounds, over which the source produces a tripartite state $|\Psi_{ABE}\rangle$ shared between Alice, Bob and Eve. Ref. [2] showed that Eve's information is the same as in the case where the devices have no memory and behave identically and independently in each communication round of the protocol, up to corrections vanishing with n. In particular, we can write $|\Psi_{ABE}\rangle = |\psi\rangle_{ABE}^{\otimes n}$ where $|\psi\rangle_{ABE}$ is the tripartite state of a single round and consider the case where measurements are done successively on the state $|\psi\rangle_{ABE}$.

In the asymptotic limit of large n, the number of secret bits per round obtained after one-way error correction and privacy amplification (i.e. the key rate) is then given by [3]

$$r = H(\mathsf{A}_0|E) - H(\mathsf{A}_0|\mathsf{B}_2), \qquad (2)$$

where H is the von Neumann entropy. Ref. [4] showed that the conditional entropy $H(\mathsf{A}_0|E)$ optimized over

all states ψ_{ABE} and measurements A_x, B_y compatible with the observed CHSH score S is lower bounded by

$$H(A_0|E) \geq 1 - h\left(\frac{1+\sqrt{(S/2)^2-1}}{2}\right) \qquad (3)$$

where h denotes the binary entropy. This provides a lower bound on the key rate, as the conditional entropy $H(A_0|B_2)$ can be estimated directly from Alice and Bob measurement results associated to setting choices A_0 and B_2. Interestingly, this bound is obtained *device-independently*, i.e. without assumptions on the dimension of quantum states and the calibration of measurements. This is not the case for standard (non-device independent) QKD protocols which are not based on the violation of a Bell inequality and whose security guarantees rely on the assumption that the source and measurements carry out precisely the operations foreseen by the protocol. This assumption is hard to meet in practice and leads to vulnerabilities, as demonstrated by hacking experiments [5, 6, 7, 8]. The robustness of device-independent quantum key distribution against these attacks makes it appealing, and a race between several experimental groups is ongoing to report the first proof-of-principle distribution of a key with a fully device-independent security. Measurement-DIQKD, a precursor of DIQKD where device-independence only applies to the measurement devices, but not to those used for state preparation [9, 10], already admits a number of experimental implementations [11, 12, 13, 14, 15].

Let us note that the proof leading to the bound given in Eq. (3) only uses the knowledge of the CHSH score. This score is computed as a linear combination of the correlation functions $\langle A_x B_y\rangle$, but the additional information provided by considering these correlations individually – which is anyway available in practice – might help to facilitate a realisation of device-independent quantum key distribution. This motivation is at the core of this work.

Concretely, we consider the individual values of two terms appearing in the CHSH score, namely

$$\begin{aligned} \mathrm{X} &= \langle A_0 \otimes (B_0 + B_1)\rangle, \\ \mathrm{Y} &= \langle A_1 \otimes (B_0 - B_1)\rangle. \end{aligned} \qquad (4)$$

The use of values of X and Y proved to be useful for device-independent state certification by improving the certified fidelity from the CHSH score [16]. It is also expected to be useful in DIQKD, as the knowledge of X and Y allows one to differentiate the contributions of the key generating measurement A_0 from the ones associated with A_1, from which no key is generally extracted (see [17] for a noticeable exception). Finally, in implementations of DIQKD with non-unit detection efficiencies where no-detection events are attributed a fixed value ± 1, no-detections on Bob's side can only contribute to one of these two correlation functions (X or Y). The goal of the following sections is to derive a tight bound on Eve's entropy in terms of the expected values X and Y, like the bound in Eq. (3) is a function of the CHSH score S. The main result of this work is to confirm the intuition that the use of individual values of X and Y improves the bounds on Eve's information derived from the CHSH score, and hence the key rate of DIQKD. We also apply the new bound to a concrete setup using a photon pair source based on spontaneous parametric down conversion (SPDC) and photon detections and show that it leads to a subtantial improvement of the key rate, at least for high detection efficiency.

2 Formulation of the problem

Generalization of the CHSH test– We are interested in bounding Eve's conditional entropy $H(A_0|E)$ appearing in Eq. (2) as a direct function of observed quantities X and Y. Formally, this can be accomplished by considering all possible quantum models (ψ_{ABE}, A_x, B_y) that satisfy $\mathrm{X}_{\mathrm{model}} \geq \mathrm{X}$ and $\mathrm{Y}_{\mathrm{model}} \geq \mathrm{Y}$. However, it is clear that the set of points (X,Y) for which Eve's conditional entropy is bounded from below by some constant is convex: two quantum models giving some amount of information to Eve can be joined into a new model on which Eve's conditional entropy is bounded by the weighted sum of entropy bounds associated to the individual models. It is thus equivalent to bound Eve's conditional entropy with linear constraints of the form

$$\frac{\cos(\Omega)}{2}\mathrm{X}_{\mathrm{model}} + \frac{\sin(\Omega)}{2}\mathrm{Y}_{\mathrm{model}} \geq \beta, \qquad (5)$$

where β is deduced from the observed quantities X and Y from the following formula

$$\beta = \frac{1}{2}\left(\cos(\Omega)\,\mathrm{X} + \sin(\Omega)\,\mathrm{Y}\right). \qquad (6)$$

(Further in the text, we will use a compact notation for sine $\mathrm{S}_\Omega = \sin(\Omega)$ and cosine $\mathrm{C}_\Omega = \cos(\Omega)$.) Obviously, $\Omega = \pi/4$ reduces back to the CHSH constraint (up to normalization). Just like the CHSH score can be seen as the result of a test of the CHSH inequality, we can associate β to the test of a Bell inequality – a generalisation of the CHSH inequality – that is characterized in Ref. [18]. This characterization is also done below for the sake of completeness.

Reduction to qubits– The score β given in Eq. (6) is estimated when Alice and Bob choose the measurement A_x, B_y, $x, y = 0, 1$, which are observables with eigenvalues ± 1. Jordan's lemma [19, 20] tells

us that such observables can be jointly block diagonalised with blocks of size 2×2, i.e.

$$A_x = \bigoplus_k A_{x,k} \qquad B_y = \bigoplus_{k'} B_{y,k'} \ , \tag{7}$$

where, without loss of generality, we can assume the restriction to each qubit block to be a real Pauli measurement satisfying $A_{x,k}^2 = \mathbb{1}_k$ and $B_{y,k'}^2 = \mathbb{1}_{k'}$. This means that in each block labelled by k and k' respectively, the measurement is characterized by unit vectors $\mathbf{a}_x^k$, $\mathbf{b}_y^{k'}$ such that

$$A_{x,k} = \mathbf{a}_x^k \cdot \begin{pmatrix} \sigma_z \\ \sigma_x \end{pmatrix} \qquad B_{y,k'} = \mathbf{b}_y^{k'} \cdot \begin{pmatrix} \sigma_z \\ \sigma_x \end{pmatrix} \tag{8}$$

where σ_z and σ_x are Pauli operators.

The state $|\psi\rangle_{ABE}$ can be enforced to take the form

$$|\psi\rangle_{ABE} = \bigoplus_{k,k'} \sqrt{p_{(k,k')}}\, |\psi\rangle_{ABE}^{(k,k')} \ , \tag{9}$$

where $p_{(k,k')}$ is a probability distribution and $|\Psi\rangle_{ABE}^{(k,k')} \in \mathbb{C}_A^2 \otimes \mathbb{C}_B^2 \otimes \mathcal{H}_E^{(4)}$, see Refs [21, 22] for detailed discussions. Given models with such measurements and state, the quantity of interest can be expressed as

$$H(A_0|E) = \sum_{k,k'} p_{(k,k')} H_{(k,k')}(A_0|E) \tag{10}$$

where $H_{(k,k')}(A_0|E)$ is Eve's conditional entropy for four-qubit models (including the two qubits from Eve's purification) involving real Pauli measurements. If the minimization of $H_{(k',k)}(A_0|E)$ over such models satisfying $\frac{\cos(\Omega)}{2}\mathrm{X}_{\text{model, k, k'}} + \frac{\sin(\Omega)}{2}\mathrm{Y}_{\text{model, k, k'}} \geq \beta$ provides a convex function of β, this function can be used directly as a lower bound on the quantity $H(A_0|E)$ through Eq. (10). If it is not convex, it can be convexified so as to apply to all possible mixtures of state and measurement, and thus again apply to Eq. (10). This convexity property allows us to reduce the general problem of finding the minimum of Eve's conditional entropy over all possible models to a minimization over four-qubit models with real Pauli measurements. We will come back to this convexification requirement later.

Noisy preprocessing– We consider a simple post-processing of the raw key, known as *noisy pre-processing* [23, 24, 25], which has been shown to be beneficial to reduce the requirement on the detection efficiency in photonic implementations of device-independent quantum key distribution [22]. Once the raw key is obtained, Alice is instructed to generate a new raw key $\widehat{A}_0$ by flipping each bit of the initial raw key with a probability p. (This can be described using a POVM that is a mixture of the original measurement and a measurement with the outcome labels flipped.) Note that we will often parametrise the amount of noise that Alice adds with a parameter $q = (1-2p)^2$.

Symmetrization– In order to simplify the analysis, it is convenient to consider a symmetrization step in which both parties, Alice and Bob, flip the outcomes of the key generating measurements depending on a public random bit string. This guarantees that bits of the raw key are random, i.e. $H(A_0) = H(\widehat{A}_0) = 1$. Importantly, one can show the equivalence of protocols with and without symmetrization, meaning that the symmetrization does not need to be implemented in practice, see [22] for a complete description of the symmetrization step in the presence of noisy preprocessing.

Reduction to Bell diagonal states– If the constraints appearing in the minimization problem do not depend on the marginal probabilities $p(A_x|x)$ and $p(B_y|y)$ of Alice and Bob respectively, the symmetrization step previously presented reduces the model of the state to a Bell-diagonal structure

$$|\psi\rangle_{ABE} = \sum_{i=1}^{4} \sqrt{L_i}\, |\Phi^i\rangle_{AB} |i\rangle_E \tag{11}$$

where $|\Phi_i\rangle = \{\Phi^+, \Psi^-, \Phi^-, \Psi^+\}_{i=1}^4$, and without loss of generality, a partial ordering of the eigenvalues $L_1 \geq L_2$ and $L_3 \geq L_4$ can be imposed [21]. Note that the superscripts k, k' are omitted in the tripartite state appearing in Eq. (11), i.e. $|\psi\rangle_{ABE} \to |\psi\rangle_{ABE}^{(k,k')}$. Until the end of this section and in the next section which is dedicated to the resolution of the optimization presented in Eq. (19), we remove the index k, k' for making the notation simpler and ask the reader to keep in mind that we consider the restriction to four qubit models with real Pauli measurements in this two sections.

Eve's conditional entropy– Eve's conditional entropy can be expressed as

$$H(\widehat{A}_0|E) = H(\widehat{A}_0) - H(\rho_E) + \sum_{\hat{a}=\pm 1} p(\hat{a}) H(\rho_{E|\hat{a}}) \tag{12}$$

where ρ_E is the reduced state of Eve and $\hat{\rho}_{E|\hat{a}}$ corresponds to Eve's state conditioned on Alice's noisy key bit $\widehat{A}_0$ being equal to $\hat{a}$, which occurs with probability $p(\hat{a})$. The equivalence of the protocol with the symmetrized one allows us to take $H(\widehat{A}_0) = 1$ and $p(\hat{a}) = \frac{1}{2}$.

$H(\rho_E)$ is given by the entropy $H(\mathbf{L})$ of the probability vector $\mathbf{L} = (L_1, \ldots, L_4)$, while for the $H(\rho_{E|\hat{a}})$

terms we have

$$\rho_{E|\hat{a}=+1} = \tag{13}$$
$$\begin{pmatrix} L_1 & 0 & \mathrm{C}_\phi\sqrt{L_1L_3q} & \mathrm{S}_\phi\sqrt{L_1L_4q} \\ 0 & L_2 & \mathrm{S}_\phi\sqrt{L_2L_3q} & -\mathrm{C}_\phi\sqrt{L_2L_4q} \\ \mathrm{C}_\phi\sqrt{L_1L_3q} & \mathrm{S}_\phi\sqrt{L_2L_3q} & L_3 & 0 \\ \mathrm{S}_\phi\sqrt{L_1L_4q} & -\mathrm{C}_\phi\sqrt{L_2L_4q} & 0 & L_4 \end{pmatrix},$$

where ϕ labels Alice measurement $A_0 = \cos(\phi)\sigma_z + \sin(\phi)\sigma_x$ (we use the notation $\mathrm{C}_\phi = \cos(\phi)$ and $\mathrm{S}_\phi = \sin(\phi)$). The two states $\rho_{E|\hat{a}=\pm1}$ are related by a simple unitary transformation and therefore have the same entropy, see App.A.2 for details. The expressions of these entropic quantities provide an explicit way to compute $H(\widehat{A}_0|E)$ as a function of the parameters $\mathbf{L}$ and ϕ. Let us now turn our attention to the constraints.

Quantum correlations in the (X,Y) plane – As mentioned earlier, we are considering quantum models with the values of correlators X and Y given by Eq. (4). Without loss of generality, we can assume $\mathrm{X}, \mathrm{Y} \geq 0$, which can always be attained by relabelling the measurement outcomes of A_1, B_0 and B_1 (i.e. without touching the angle ϕ).

In this positive quadrant of the plane, the local strategies are delimited by the CHSH inequality $\mathrm{X} + \mathrm{Y} \leq 2$, i.e. the line connecting the deterministic strategies $(\mathrm{X}, \mathrm{Y}) = (2, 0)$ and $(\mathrm{X}, \mathrm{Y}) = (0, 2)$. This implies the following local bounds for the generalized CHSH tests

$$\frac{1}{2}\mathrm{C}_\Omega \mathrm{X} + \frac{1}{2}\mathrm{S}_\Omega \mathrm{Y} \leq B_\Omega^L = \max(\mathrm{C}_\Omega, \mathrm{S}_\Omega). \tag{14}$$

To identify the upper limit of the quantum set, we consider the expected values of the generalized CHSH operator

$$\mathcal{B}_\Omega = \left\langle \frac{\mathrm{C}_\Omega}{2} A_0 \otimes (B_0 + B_1) + \frac{\mathrm{S}_\Omega}{2} A_1 \otimes (B_0 - B_1) \right\rangle. \tag{15}$$

To find its maximum value, we use the qubit parametrization of measurements A_y, B_y and parametrize the measurement angles on Bob's side as

$$B_0 + B_1 = (\mathbf{b}_0 + \mathbf{b}_1) \cdot \begin{pmatrix} \sigma_z \\ \sigma_x \end{pmatrix} = 2\mathrm{C}_\theta\, \mathbf{c} \cdot \begin{pmatrix} \sigma_z \\ \sigma_x \end{pmatrix} \tag{16}$$

$$B_0 - B_1 = (\mathbf{b}_0 - \mathbf{b}_1) \cdot \begin{pmatrix} \sigma_z \\ \sigma_x \end{pmatrix} = 2\mathrm{S}_\theta\, \mathbf{c}_\perp \cdot \begin{pmatrix} \sigma_z \\ \sigma_x \end{pmatrix} \tag{17}$$

with two arbitrary perpendicular unit vectors $\mathbf{c}$ and $\mathbf{c}_\perp$, and $\cos(2\theta) = \mathbf{b}_0 \cdot \mathbf{b}_1$. From the diagonalization of the operator on the right hand side of Eq. (15), one finds the quantum bound

$$\mathcal{B}_\Omega^Q = 1 \tag{18}$$

attained at $(\mathrm{X}, \mathrm{Y}) = (2\cos(\Omega), 2\sin(\Omega))$ by a maximally entangled two qubit state and measurement settings $\mathbf{a}_0 \cdot \mathbf{a}_1 = 0$ and $\mathbf{b}_0 \cdot \mathbf{b}_1 = \cos(2\Omega)$. It follows that Eve's information is constrained by the part of the quantum set lying between the line $\mathrm{X}+\mathrm{Y} = 2$ and the circle $\mathrm{X}^2 + \mathrm{Y}^2 = 4$. At this point, we can already conclude that any quantum model with (X,Y) lying on the circle satisfies $H(\hat{A}_0|E) = 1$ (except for the two points with X+Y= 2), since the underlying state of Alice and Bob has to be pure. This is a straightforward improvement over the CHSH bound.

Formulation of the problem to solve– The reductions introduced so far invite us to first solve the following optimization

$$\begin{aligned} I(\beta; \Omega, q) = \max_{\mathbf{L}, \phi, \mathbf{a_1}, \mathbf{b_0}, \mathbf{b_1}} & \; H(\mathbf{L}) - H(\rho_{E|\hat{a}=+1}) \\ \text{s.t.} & \; \mathcal{B}_\Omega(\mathbf{L}, \phi, \mathbf{a}_1, \mathbf{b}_0, \mathbf{b}_1) \geq \beta \end{aligned} \tag{19}$$

and then consider directly the solution $I(\beta; \Omega, q)$ if it is concave in β or construct a concave function $\widehat{I}(\beta; \Omega, q) \geq I(\beta; \Omega, q)$ to bound Eve's uncertainty using

$$H(\widehat{A}_0|E) \geq 1 - \min_\Omega \widehat{I}\left(\frac{\mathrm{C}_\Omega \mathrm{X} + \mathrm{S}_\Omega \mathrm{Y}}{2}; \Omega, q\right). \tag{20}$$

Note that from the symmetries of the goal function $H(\mathbf{L}) - H(\rho_{E|\hat{a}=+1})$ and the constraint $\mathcal{B}_\Omega$, we can assume $\phi \in [0, \frac{\pi}{4}]$ for the key generating setting and $L_1 - L_2 \geq L_3 - L_4$ in addition to $L_1 \geq L_2$ and $L_3 \geq L_4$ for the state, see App.A.1 for the details. Further note that we will often use a parametrisation of the tripartite state given by the following 3 component vector

$$\begin{pmatrix} T_z \\ T_x \\ T_p \end{pmatrix} = \begin{pmatrix} L_1 - L_2 + L_3 - L_4 \\ L_1 - L_2 - L_3 + L_4 \\ L_1 + L_2 - L_3 - L_4 \end{pmatrix}, \tag{21}$$

with $0 \leq T_x \leq T_z \leq 1$ and $T_z + T_x - 1 \leq T_p \leq 1 - (T_z - T_x)$.

3 Bounding Eve's information with generalized CHSH tests

We are now ready to compute a bound on Eve's information as a function of the generalized CHSH score given in Eq. (6) by solving the optimisation problem given in Eq. (19). Among the parameters of the model in Eq. (19), the measurement setting $\mathbf{a}_1, \mathbf{b}_0$ and $\mathbf{b}_1$ only influence the constraint but not the goal function. Furthermore, it is shown in Ref. [22] that $H(\rho_{E|\hat{a}=+1})$ is a monotonic function in the key generating setting $\phi \in [0, \frac{\pi}{4}]$. We can thus decompose the maximization problem in two steps. First, for a fixed state $\mathbf{L}$, we find the lowest angle ϕ allowing to satisfy the constraint

$$\begin{aligned} \phi_*(\mathbf{L}, \beta, \Omega) = \min \; & \phi \\ \text{s.t.} \; & \max_{\mathbf{a}_1, \mathbf{b}_0, \mathbf{b}_1} \mathcal{B}_\Omega(\mathbf{L}, \phi, \mathbf{a}_1, \mathbf{b}_0, \mathbf{b}_1) \geq \beta. \end{aligned} \tag{22}$$

Second, we fix $\phi = \phi_*(\mathbf{L}, \beta, \Omega)$ to the optimal value for Eve, and maximize her information with respect to the state, that is, we solve

$$I(\beta;\Omega,q) = \max_{\mathbf{L}} H(\mathbf{L}) - H(\rho_{E|\hat{a}=+1};\phi_*(\mathbf{L},\beta,\Omega)). \quad (23)$$

We solve Eq. (22) in App. A.3. The expression of the optimal angle ϕ_* depends on whether the parameter Ω exceeds $\frac{\pi}{4}$. We treat the two cases $\Omega \leq \frac{\pi}{4}$ and $\Omega > \frac{\pi}{4}$ separately.

3.1 The simple case with $\Omega \leq \frac{\pi}{4}$

For the Bell tests satisfying $\Omega \leq \frac{\pi}{4}$, which include the CHSH test, the observed score β does not constrain the key generating setting ϕ but only the state $\mathbf{L}$, see App. A.3 for details. As a result, there always exists a realization with the optimal angle $\phi_* = 0$ as long as the state is such that the Bell score can be attained, i.e. if

$$\mathrm{C}_\Omega^2 T_z^2 + \mathrm{S}_\Omega^2 T_x^2 \geq \beta_\Omega^2. \quad (24)$$

In other words, the optimization Eq. (22) yields $\phi_* = 0$, and the maximization of the entropy becomes possible: the conditional state $\rho_{E|\hat{a}=+1}$ is then block diagonal and its entropy has a simple closed-form expression. Such a maximization has been done for the CHSH case ($\Omega = \frac{\pi}{4}$) in Ref. [22], but Ref. [26] pointed out that the analytical bounds on conditional entropies given in this reference assume qubit attacks. The same bounds were derived using a different approach in [26], where it is also proved that these bounds are convex. The convexity results of [26], together with Jordan's lemma, imply that the obtained qubit bounds are in fact valid for any dimensions. The same convexity proof applies to the current situation with $\Omega \leq \pi/4$. For the sake of completeness, we provide in App. A.5 an alternative proof of convexity, which directly applies to the present case and to [22]. We show in particular (see App. A.4) that

$$\begin{aligned} I(\beta;\Omega,q) &= h_q(z) = h(z) - h(n_q(z)) \\ \text{with} \quad n_q(z) &= \frac{1+\sqrt{1-4\,(1-q)\,z(1-z)}}{2} \\ \text{and} \qquad z &= \frac{1}{2}\left(\frac{\sqrt{\beta^2-\mathrm{C}_\Omega^2}}{\mathrm{S}_\Omega}+1\right), \end{aligned} \quad (25)$$

where h is the binary entropy. The concavity of $I(\beta;\Omega,q)$ and hence the convexity of Eve's entropy $H(\widehat{A}_0|E)$ follows from (see App. A.5)

$$\frac{d^2}{d\beta^2} h_q\big(z(\beta)\big) = h_q''(z)\big(z'(\beta)\big)^2 + h_q'(z) z''(\beta) \leq 0. \quad (26)$$

Finally, it remains to determine the optimal inequality to use for a given point (X,Y). $h_q(z)$ being a monotonic function of z, we want to maximize its argument

$$\begin{aligned} z &= \frac{1}{2}\left(\frac{\sqrt{(\frac{\mathrm{C}_\Omega \mathrm{X}+\mathrm{S}_\Omega \mathrm{Y}}{2})^2 - \mathrm{C}_\Omega^2}}{\mathrm{S}_\Omega}+1\right) \quad (27)\\ &= \frac{1}{4}\sqrt{\frac{4\,\mathrm{Y}^2}{4-\mathrm{X}^2} - (4-\mathrm{X}^2)\left(\cot(\Omega) - \frac{\mathrm{XY}}{4-\mathrm{X}^2}\right)^2} + \frac{1}{2}, \end{aligned}$$

with respect to Ω in the range where the argument of the square root is positive (which means that the value for the Bell test exceeds the local bound). Manifestly, the expression has a global maximum at

$$\cot(\Omega) = \frac{\mathrm{XY}}{4-\mathrm{X}^2}. \quad (28)$$

Now, we have to verify that the optimal test we found satisfies $\Omega \leq \frac{\pi}{4}$. One finds that this is the case for

$$\frac{4-\mathrm{X}^2}{\mathrm{XY}} \leq 1, \quad (29)$$

providing a bound on Eve's entropy as a direct function of the correlators X and Y:

$$z_{\mathrm{opt}} = \frac{1}{2}\left(\frac{\mathrm{Y}}{\sqrt{4-\mathrm{X}^2}}+1\right). \quad (30)$$

One easily verifies that this bound is indeed better than the CHSH formula [22]

$$z_{\mathrm{CHSH}} = \frac{1}{2}\left(1+\sqrt{\left(\frac{\mathrm{X}+\mathrm{Y}}{2}\right)^2-1}\right) \quad (31)$$

if $\frac{4-\mathrm{X}^2}{\mathrm{XY}} < 1$.

3.2 The complicated case with $\Omega > \frac{\pi}{4}$

3.2.1 Bounding Eve's information from a numerical optimization

For the remaining Bell tests, with $\Omega > \frac{\pi}{4}$, the situation is different. Here, the generalized CHSH score β does not only constraint the state $\mathbf{L}$ but also the setting of the key generating measurement. We therefore adopt a strategy in two steps. First, we develop a method that can efficiently compute a bound on Eve's information, either heuristically or under a set of well-defined ansatz. Second, we provide a numerical method able to certify formally the validity of a given bound.

Considering the parameters when $\Omega > \frac{\pi}{4}$, we find that there are two different regions. First, for the states falling in the range

$$\mathbb{S}(\beta,\Omega) = \{\mathbf{L} | (\mathrm{C}_\Omega^2 T_z^2 + \mathrm{S}_\Omega^2 T_x^2) \leq \beta^2 \leq (\mathrm{C}_\Omega^2 T_x^2 + \mathrm{S}_\Omega^2 T_z^2)\}, \quad (32)$$

the constraint $\mathcal{B}_\Omega \geq \beta$ can be satisfied with the measurement angle $\phi \geq \phi_*(\mathbf{L}, \Omega, \beta)$, where $\cos^2(\phi_*) = c_*^2(\mathbf{L}, \Omega, \beta)$ is given by

$$c_*^2(\mathbf{L}, \Omega, \beta) = \frac{(\beta^2 - \mathrm{S}_\Omega^2 T_x^2)(\mathrm{C}_\Omega^2 T_x^2 + \mathrm{S}_\Omega^2 T_z^2 - \beta^2)}{\mathrm{C}_\Omega^2 (T_z^2 - T_x^2)(\mathrm{S}_\Omega^2 T_z^2 + \mathrm{S}_\Omega^2 T_x^2 - \beta^2)}. \tag{33}$$

The constraint on the angle only becomes trivial, $c_*^2 = 1$, on the boundary of the region $\mathbb{S}$, where $(\mathrm{C}_\Omega^2 T_z^2 + \mathrm{S}_\Omega^2 T_x^2) = \beta^2$.

Second, in the region where $(\mathrm{C}_\Omega^2 T_z^2 + \mathrm{S}_\Omega^2 T_x^2) > \beta^2$ the Bell score β can also be attained with $\phi = 0$. However, there models provide less information to Eve as compared to these on the boundary $(\mathrm{C}_\Omega^2 T_z^2 + \mathrm{S}_\Omega^2 T_x^2) = \beta^2$, see the discussion at the end of App. A.4. So we can safely ignore this region.

To find the best strategy for Eve, it thus remains to solve

$$I(\beta; \Omega, q) = \max_{\mathbf{L} \in \mathbb{S}(\Omega, \beta)} H(\mathbf{L}) - H(E|\hat{a} = +1; c_*^2(\mathbf{L}, \Omega, \beta)). \tag{34}$$

This optimization only involves an analytic function of three parameters on a compact domain. It can be easily and time-efficiently solved heuristically by standard numerical methods, e.g using fmincon on MATLAB, NMaximize on Mathematica, or scipy.optimize on Python. We now give an ansatz on the solution of the optimization given in Eq. (34), which allows one to speed up its numerical resolution even further.

3.2.2 Ansatz

First, we observe that the vector $\mathbf{L}$ saturating Eve's information only has two non-zero coefficients $L_1 = 1 - L_3$ and $L_2 = L_4 = 0$, or $T_z = 1$ and $T_x = T_p$. With this observation, the previous optimization problem becomes a scalar optimization, that is

$$\tilde{I}_{\mathrm{anz}}(\beta; \Omega, q) = \max_{\frac{\beta^2 - \mathrm{S}_\Omega^2}{\mathrm{C}_\Omega^2} \leq T_x^2 \leq \frac{\beta^2 - \mathrm{C}_\Omega^2}{\mathrm{S}_\Omega^2}} h\left(\frac{1 + T_x}{2}\right) - h\left(\frac{1 + \sqrt{T_x^2 + c_*^2 q (1 - T_x^2)}}{2}\right). \tag{35}$$

Second, we see that the bound $\tilde{I}_{\mathrm{anz}}(\beta; \Omega, q)$ is not concave for small β. However, we observe that its concave roof can be obtained by drawing a line which passes through the point

$$\begin{aligned} \beta &= \mathcal{B}_\Omega^L = \sin(\Omega) \\ I_L(q) &= I(\mathcal{B}_\Omega^L; \Omega, q) = 1 - h\left(\frac{1 + \sqrt{q}}{2}\right) \end{aligned} \tag{36}$$

which is tangent to the curve $\tilde{I}_{\mathrm{anz}}(\beta; \Omega, q)$. The value of the generalized CHSH score at the tangent point can be found by solving

$$\beta_* = \operatorname*{argmin}_\beta \frac{I_L(q) - \tilde{I}_{\mathrm{anz}}(\beta; \Omega, q)}{\beta - \sin(\Omega)}. \tag{37}$$

Labeling $I_*(\Omega, q) = \tilde{I}_{\mathrm{anz}}(\beta_*; \Omega, q)$, this leads to the concave roof

$$\widehat{I}_{\mathrm{anz}}(\beta; \Omega, q) = \begin{cases} \frac{I_*(\Omega, q)(\beta - \sin(\Omega)) - I_L(q)(\beta - \beta_*)}{\beta_* - \sin(\Omega)} & \beta < \beta_* \\ \tilde{I}_{\mathrm{anz}}(\beta; \Omega, q) & \beta \geq \beta_*. \end{cases} \tag{38}$$

At this stage, we further observe that the optimal value of T_x^2 for values of $\beta \geq \beta_*$ coincides with its maximum possible value $T_x^2 = \frac{\beta^2 - \mathrm{C}_\Omega^2}{\mathrm{S}_\Omega^2}$ (implying $c_* = 1$). We thus define $I_{\mathrm{anz}}(\beta; \Omega, q)$ accordingly. Interestingly, this expression coincides with the solution given in Eq. (25) for the case $\Omega \leq \frac{\pi}{4}$, meaning in particular that the optimal value of Ω for I_{anz} is given by Eq. (28). In the Eqs. (37) and (38) we can now replace $\tilde{I}_{\mathrm{anz}}(\beta; \Omega, q)$ with $I_{\mathrm{anz}}(\beta; \Omega, q)$, which does not involve any nonlinear optimization.

While we believe this expression to be the true bound, we do not have a formal proof. Anyway, this conjectured expression helps to solve the optimization of interest.

3.2.3 Certified numerical solution

As mentioned before, the optimization in Eq. (34) can be easily solved by standard numerical methods. However, to provide a strict security guarantee to an actual implementation of DIQKD, such a numerical optimization would need to be done in a certified manner, with a formal proof that the obtained numbers lower bound Eve's conditional entropy on the whole domain. Below we present an algorithm which allows one to do such a certified optimisation based on the Lipshitz continuity of the goal function. The algorithm is rather time-costly, but it only has to be used once the optimal experimental parameters are fixed through an ad hoc maximization of Eq. (34), cf. below.

Concretely, we present in this section an algorithm that approximates the set of possible strategies of Eve, delimited by the bound $\widehat{I}(\beta, \Omega, q)$, from the outside. To avoid the issue of concavity posed by Eq. (19), we rewrite the problem in the dual form in which we look for the tangent lines

$$\begin{aligned} f(t; \Omega, q) &= \max_{\mathbf{L}, \phi} H(\rho_E) - H(\rho_E|\hat{A}_0) + t\, \beta_{\max}(\mathbf{L}, \phi; \Omega) \\ \beta_{\max}(\mathbf{L}, \phi; \Omega) &= \max_{\mathbf{a}_1, \mathbf{b}_0, \mathbf{b}_1} \mathcal{B}_\Omega(\mathbf{L}, \phi, \mathbf{a}_1, \mathbf{b}_0, \mathbf{b}_1), \end{aligned} \tag{39}$$

to the curve $\widehat{I}(\beta, \Omega, q)$ with different slopes t. In Eq. (39) we used the fact that it is only the Bell score that depends on the measurement setting

$\mathbf{a}_1, \mathbf{b}_0, \mathbf{b}_1$, so it can be maximized straightforwardly to define $\beta_{\max}(\mathbf{L}, \phi; \Omega)$, see App. A.6 for its closed form expression.

Before giving the details on the way we solve this dual form, let us shortly discuss on how it shall be used. We consider an actual implementation of DIQKD with fixed values of X_*,Y_* and q_* and for which there is an optimal value Ω_* which saturates the minimum in Eq. (20)

$$H(\hat{A}_0|E) \geq 1 - \widehat{I}(\beta_*; \Omega_*, q_*), \tag{40}$$

with $\beta_* = \frac{1}{2}(\mathrm{C}_{\Omega_*}\mathrm{X}_* + \mathrm{S}_{\Omega_*}\mathrm{Y}_*)$. Therefore, an optimal security guarantee for this particular implementation only requires the knowledge of the function $\widehat{I}(\beta_*, \Omega_*, q_*)$ on a single point. The same lower bond on Eve's conditional entropy can be obtained from the value of the dual bound $f(t; \Omega_*, q_*)$ in Eq. (39) on a single point. Indeed, the concavity of $\widehat{I}(\beta; \Omega, q)$ ensures that there exists a value t_* for which the inequality

$$f(t_*; \Omega_*, q_*) \geq \widehat{I}(\beta; \Omega_*, q_*) + t_*\beta \tag{41}$$

is saturated at $\beta = \beta_*$ where $f(t_*; \Omega_*, q_*) = \widehat{I}(\beta; \Omega_*, q_*) + t_*\beta_*$. Using Eq. (39), we deduce that

$$\begin{aligned} H(\hat{A}_0|E) &\geq 1 - f(t_*; \Omega_*, q_*) + t_*\beta_* \\ &= 1 - \widehat{I}(\beta_*; \Omega_*, q_*). \end{aligned} \tag{42}$$

Hence, for a fixed experimental implementation of the protocol, it is sufficient to certify a single value of the function $f(t_*; \Omega_*, q_*)$ in order to provide a strict and optimal security guarantee. Furthermore, the value t_* is straightforward to find from the knowledge of Ω_*, β_*, q_* and the function $\widehat{I}(\beta; \Omega, q)$.

We can now comment on the algorithm to provably upper bound the quantity in Eq. (39). The basic idea is a branch and bound approach relying on the Lipschitz continuity of the goal function. Concretely, we first derive a parametrization of the set $(\mathbf{L}, \phi)$ for which the goal function in Eq. (39) is Lipshitz continuous with a constant that we compute. Then, we obtain an upper bound on its value on the whole domain by computing the value of the function on a grid of points. Finally, the algorithm subsequently refines the grid around the points where the value of the function is large in order to approach, step by step, the global maximum. Additional details are given in the next three sections.

We remark that another algorithm for solving this optimisation was recently developed in a separate work [17], which we believe could be adapted to our situation as well. The basic idea in that work is somewhat different – for fixed measurement angles for Alice and Bob, they find a semidefinite programming (SDP) relaxation for the minimization of Eve's entropy with respect to the state. This SDP is then solved on a grid of angles, and continuity of the goal function with respect to the angles is used to certify that the bound is secure. One advantage of the approach we propose here is that it provably converges to a tight bound, whereas the SDP relaxation in [17] is not known to be tight[1].

Lipshitz continuity of the entropy with respect to the angle – A key ingredient in the practical implementation of the desired certified algorithm is that the von Neumann entropy $H(\rho)$ has a bounded rate of change with respect to the angular distance between the two states ρ and σ (see App. B.1),

$$A(\rho, \sigma) = \arccos(F(\rho, \sigma)), \tag{43}$$

where the fidelity is defined as $F(\rho, \sigma) = \mathrm{tr}|\sqrt{\rho}\sqrt{\sigma}|$. This angle is a metric on the set of states [28]. We show that for n-dimensional quantum states, the entropy satisfies

$$\frac{|H(\rho) - H(\sigma)|}{A(\rho, \sigma)} < \begin{cases} \frac{4\sqrt{r_1(1-r_1)}}{\ln(2)}\sqrt{n-1} & n \leq 4 \\ 2\log(n) & n \geq 5. \end{cases} \tag{44}$$

where $r_1 \approx 0.203$ (see Eq. (157) below for details). This contrasts with the trace distance, another metric on the set of quantum states, for which the entropy has infinite rate of change around non-full-rank states.

Bounding the gradient of the goal function– To apply the continuity bound above to the goal function in Eq. (39), we use the following parametrization of the state

$$\sqrt{\mathbf{L}} = \begin{pmatrix} \cos(\alpha)\cos(\mu) \\ \cos(\alpha)\sin(\mu) \\ \sin(\alpha)\cos(\xi) \\ \sin(\alpha)\sin(\xi) \end{pmatrix}, \tag{45}$$

so that the quantum models are described by four angles

$$\mathbf{x} = (\alpha, \mu, \xi, \phi), \tag{46}$$

with $\mathbf{x} \in [0, \frac{\pi}{4}]^{\times 3} \times [0, \frac{\pi}{2}]$. Here, the condition $\mu, \xi \leq \frac{\pi}{4}$ follow from $L_1 \geq L_2$, $L_3 \geq L_4$. The bound $\alpha \leq \frac{\pi}{4}$ is a consequence of $L_1 + L_2 \geq L_3 + L_4$, which can be imposed on the states as an alternative to $L_1 - L_2 \geq L_3 - L_4$, see App. A.1.

To obtain a bound on the gradient of the goal function

$$G(\mathbf{x}) = H(\mathbf{L}) - H(\rho_E|\hat{a} = +1) + t\,\beta_{\max}(\mathbf{L}, \phi; \Omega) \tag{47}$$

[1] Note that after the publication of this manuscript, some of the authors have shown how to perform an SDP relaxation that converges to a tight bound as well, see [27].

we bound the gradient of each term independently, as described in App. B.2 and B.3. For the entropic terms, we use Eq. (44), while the computation of the maximal gradient is quite straightforward for the CHSH score. Combining the three terms, we obtain a general bound

$$|\nabla_{\mathbf{x}} G| \leq 12.7 + 7\,t \tag{48}$$

on the whole domain of $\mathbf{x}$.

With this global bound on the gradient, a certified maximization of the function $G(\mathbf{x})$ can be obtained with a branch and bound approach. In order to do so, we extended the code developed in Ref. [29] to include global optimization. A detailed description of this code can be found in the App. B.4. A python implementation as well as an example for our case of interest, can be found on Gitlab[2].

4 Results

Improved bound on Eve's conditional entropy– In order to demonstrate the advantage of considering the pair of variables (X, Y) when bounding Eve's conditional entropy, we compute the bound on $H(\widehat{A}_0|E)$ for different values of X, Y and p and compare it to the bound obtained from the CHSH score [22]. Because of the two regimes identified earlier, we compute both the optimal bound assuming $\Omega \leq \pi/4$ and the one assuming $\Omega > \pi/4$ for each value of X and Y, and keep the best one. In the case $\Omega \leq \pi/4$, the optimal choice of Ω is readily given by Eq. (28). In the other case, we optimize the bound over $\Omega \in (\pi/4, \pi/2]$. The difference between this optimal bound on $H(\widehat{A}_0|E)$ given X and Y and Eq. (3) is shown in Fig. 1. It shows that our bound on $H(\widehat{A}_0|E)$ is better than the one derived from the CHSH score, except along the line satisfying $\mathrm{X}(\mathrm{X}+\mathrm{Y}) = 4$. We emphasise that our derivation of the bound is constructive, that is we find the optimal attack that gives $H(\widehat{A}_0|E)$ to Eve. The final bound is thus tight, up to the precision of the numerical algorithms for $\Omega > \frac{\pi}{4}$.

Implication for a practical realization of DIQKD– We now study the potential impact of our bound on practical realizations of DIQKD. In the limit of asymptotically many repetitions, an implementation is uniquely characterized by its key rate r, which is given in Eq. (2). In our case, this key rate is determined from three quantities: X, Y and Bob's uncertainty about Alice's key generating bit as a function of the noisy preprocessing parameter, given

[2] https://gitlab.com/plut0n/bcert

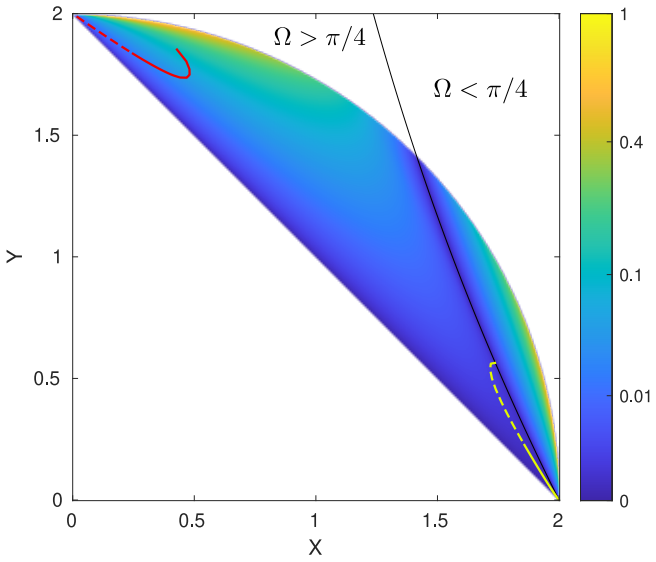

Figure 1: Difference between the bound on Eve's conditional entropy $H(\widehat{A}_0|E)$ computed as a function of X and Y, and as a function of the CHSH quantity $S = \mathrm{X} + \mathrm{Y}$, for $p = 0$. In the presence of noisy preprocessing (i.e. $p > 0$), the advantage follows a similar distribution, but is smaller in magnitude. The CHSH bound is only optimal along the curve $\mathrm{X}(\mathrm{X}+\mathrm{Y}) = 4$. The advantage on the right-hand side of this curve is obtained with $\Omega < \pi/4$, and on the left-hand side with $\Omega > \pi/4$. The yellow (red) curve shows the trajectory in the X-Y plane which optimizes the key rate in an optical implementation of DIQKD for low (high) detection efficiencies. At the efficiency $\eta = 0.923$, it is better to switch from one curve to the other one (at the transition between full and dashed curves). The points with $\Omega > \pi/4$ were computed both with the heuristic method and with the ansatz described in Sec. 3.2.

by $H(\widehat{A}_0|B_2)$. Hence, in order to find the optimal design for an experimental implementation of DIQKD, we express the quantities

$$\text{setup} \simeq \left(\mathrm{X}, \mathrm{Y}, H(\hat{A}_0|B_2)\right) \tag{49}$$

as a function of the model's parameters. Then, we maximize the key rate over these parameters:

$$\begin{aligned} \check{r} &= \max_{\text{setup},\Omega,q} H(\widehat{A}_0|E) - H(\widehat{A}_0|B_2) \\ &= \max_{\text{setup},\Omega,q} 1 - \widehat{I}\left(\frac{\mathrm{C}_\Omega \mathrm{X} + \mathrm{S}_\Omega \mathrm{Y}}{2}; \Omega, q\right) - H(\hat{A}_0|B_2) \end{aligned} \tag{50}$$

Solving this maximization gives a bound on the key rate $\check{r}$, the values $\left(\mathrm{X}_*, \mathrm{Y}_*, H(\widehat{A}_0|B_2)\right)$ expected for a given implementation, as well as the optimal values of the parameters Ω_* and q_* for this implementation.

SPDC-based implementation of DIQKD– Photonic experiments using a source based on spontaneous parametric down conversion (SPDC) are one of the most promising setups for implementing DIQKD, as shown by recent experiments reporting on the violation of a Bell inequality without

the fair sampling assumption [30, 31, 32, 33, 34, 35]. We consider such a setup in which an SPDC source is used to create and distribute polarization entanglement between distant parties who perform measurements as requested here in the proposed protocol. The main limitation in this setup is the overall detection efficiency, i.e. the possibility of losing a photon at any point between its creation at the source and its final detection. To reflect photon losses and non-unit detection efficiency, the transmission channel between the source and the parties is modeled as a lossy channel with an overall transmission η. It is also important to include the statistics of an SPDC source which does not produce a two-qubit state, but a state that contains vacuum and multiple photon components. We invite the reader to look at Ref. [22] to get explicit expressions of the exact statistics created by this source as well as a description of tunable parameters.

When computing the key rate for an SPDC source with a security determined by the CHSH score, any values of X and Y with the same sum impose the same bound on Eve's conditional entropy $H(\widehat{A}_0|E)$. In a Eberhard-like scenario where a significant fraction of the entangled particles can be lost before yielding their measurement result, it is advantageous for Alice to use two measurement settings with different overlap with her Schmidt basis in order to maximize the CHSH quantity [36]. It is then easier for Bob to guess the outcome of one of the two measurements (the one best aligned with the Schmidt basis). When the key rate is extracted from this measurement to minimize the cost of error correction (see Ref. [22] for more details), the value of the X quantity is then larger than Y, as shown in Fig. 1. But in this case, the (X,Y) values are very close to the line $\mathrm{X}(\mathrm{X}+\mathrm{Y}) = 4$, for which there is no advantage. Therefore, we only expect a small improvement in the key rate here.

Given the values shown in Fig. 1, a better bound on Eve's information would be obtained if the same CHSH value was obtained with the contributions from X and Y being inverted, i.e. with $\mathrm{Y} > \mathrm{X}$. However, this requires Alice to define her key-generating measurement as being the one less aligned with the Schmidt basis, hence leading to an increase of the error correction cost. In this case, both conditional entropies $H(\widehat{A}_0|E)$ and $H(\widehat{A}_0|B_2)$ are larger, and we need to check which one increases the most in order to infer a possible gain on the key rate. As it turns out, the tradeoff between these two entropies increase depends on the detection efficiency.

Namely, there are two regimes, as shown in Fig. 2. When the detection efficiency is larger than ~ 0.923, relabelling the measurements in order to enter the region with $\mathrm{Y} > \mathrm{X}$ (where inequalities with $\Omega > \pi/4$ significantly improve the bound on $H(\widehat{A}_0|E)$) is advantageous, because the increase in Bob's uncertainty $H(\widehat{A}_0|B_2)$ is smaller. The red curve in Fig. 1 shows the corresponding trajectory in the X-Y plane. When $\eta < 0.923$, the cost of error correction become prohibitive compared to the potential increase in Eve's uncertainty, and it is better to stay in the region $\mathrm{X} > \mathrm{Y}$, as represented by the yellow curve in Fig. 1. There, a small increase of the key rate is still found because the correlations do not satisfy $\mathrm{X}(\mathrm{X}+\mathrm{Y}) = 4$ exactly. However, this condition is only slightly violated, resulting in an increase in key rate smaller than $\sim 10^{-4}$, which is practically negligible. The critical detection efficiency then also remains at $\sim 83\%$, unchanged compared to a bound based on CHSH alone.

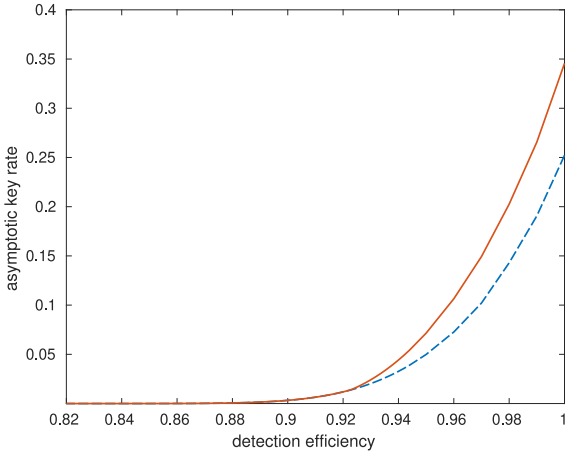

Figure 2: Key rate achievable with a photonic setup as a function of the symmetric detection efficiency η. The dashed blue curve corresponds to the key rate achieved with noisy preprocessing and a security based on the CHSH quantity alone; it is nonzero for efficiencies above $\sim$0.828 [22]. The continuous red curve bases its security on the values of both X and Y (and also includes noisy preprocessing). A significant increase of the key rate is possible for efficiencies above $\eta > 0.923$. At $\eta = 1$, the obtained key rate is 0.346 instead of 0.252.

Comparison of qubit vs SPDC bounds– To illustrate the impact of the photon statistics of SPDC sources on DIQKD, we now consider a simpler model in which the state shared between Alice and Bob is a two-qubit state:

$$|\psi\rangle = \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle\,. \tag{51}$$

We are not aware of physical setups allowing one to produce a state with $\theta = \pi/4$ but not allowing for a different value of θ. Still, for the sake of the discussion, we distinguish between the cases where the state can be either constrained to be maximally

Keyrate formula	Singlet	Qubit	SPDC
$1 - I(\beta; \frac{\pi}{4}, 0) - h(Q)$	0.923	0.893	0.927
$1 - I(\beta; \frac{\pi}{4}, 0) - H(A_0\|B_2)$	0.908	0.865	0.909
$1 - I(\beta; \frac{\pi}{4}, q) - H(A_0\|B_2)$	0.903	0.826	0.826
$1 - I(\beta; \Omega, q) - H(A_0\|B_2)$	0.900	0.826	0.826

Table 1: Critical detection efficiencies for various states and protocols. Here, Q is the quantum bit error rate (QBER). These thresholds are compared in Fig. 3.

entangled, i.e. $\theta = \pi/4$, or can have an arbitrary parameter $\theta \in [0, \pi/4]$.

In Tab. 1, see also Fig. 3, we report the critical detection efficiencies corresponding to various security analyses applied on these implementations. Like for the SPDC model, no advantage on the critical detection efficiency is found when using arbitrary two-qubit systems. A small advantage is however present when restricting to measurements on the singlet state. Still, this model is not optimal and it remains of course better to use partially entangled states. In fact, even partially entangled states produced by an SPDC source perform better.

In this respect, it is worth noticing here that the performance of an SPDC source is essentially comparable to that of an arbitrary two-qubit state once noisy preprocessing is taken into consideration, i.e. the requirement on the detection efficiency is very similar. In the case without noisy preprocessing, the state produced by these physical sources do not have a better tolerance to losses than measurements on a maximally entangled state. This suggests that noisy preprocessing is a key ingredient for a first proof of principle implementation with an SPDC source [22].

5 Discussion

In this paper, we introduced a refinement of the usual CHSH-based analysis of DIQKD experiments: Instead of projecting the measurement statistics onto a single line giving the CHSH score X + Y, we kept the information about the individual values of X and Y throughout the whole security analysis. We found that this refined analysis gives a more restrictive bound on the information available to the eavesdropper for almost all values X and Y in the quantum set.

When applying our results to photonic implementations of DIQKD with a SPDC source, we found that the key rate is improved by a factor going up to 37% for unit detection efficiency. On the other hand, we could not find any improvement for the critical detection efficiency as compared to the CHSH protocol with noisy processing presented in Ref. [22].

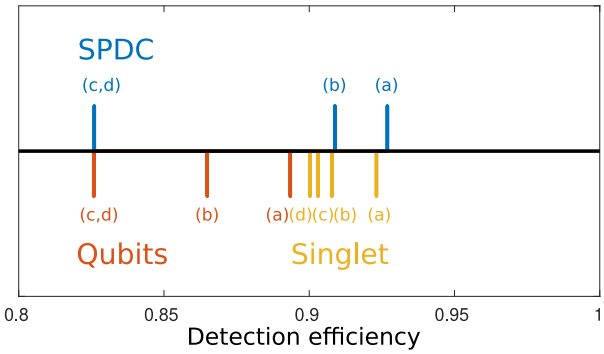

Figure 3: Comparison of the critical detection efficiencies for several setup models. Blue markers are for SPDC statistics, yellow ones for measurement on a maximally entangled two-qubit state, and red ones for measurement on an arbitrary two-qubit state. The four protocols of Tab. 1 are considered here: the security of (a) is based on the CHSH value following Eq. (3) and error correction based on the QBER [21], (b) Eq. (3) with error correction based on conditional entropy $H(A|B)$ [37], (c) security from CHSH with noisy preprocessing and error correction based on $H(A|B)$ following [22], (d) security from X and Y with noisy preprocessing and error correction based on $H(A|B)$.

However, we focused on a given photonic implementation, and the question of the most favorable optical setup combining squeezing operations, displacement operations, linear optical elements and photon counting techniques is still open. Advanced techniques using automated design of quantum experiments based on reinforcement learning which already proved to be useful to optimize the CHSH score [38] are inspiring. Applying them to the proposed protocol in order to reduce the required detection efficiency for implementing DIQKD appears to be promising for future work.

Finally, we would like to remark that the certified numerical techniques we proposed also open up the possibility of bounding Eve's information reliably when more correlators, or even the full measurement statistics, are taken into account.

6 Note added

While writing this manuscript, we became aware of another manuscript [26] reporting on similar results.

7 Acknowledgments

We thank Stefano Pironio for pointing out that the convexity argument provided in [22] was not complete, see the discussion in Sec. 3.1 and App. A.5. We acknowledge funding by the Swiss National Science Foundation (SNSF), through the Grants PP00P2-179109 as well as via the National Center for Compe-

tence in Research for Quantum Science and Technology (QSIT).

References

[1] Artur K. Ekert. "Quantum cryptography based on Bell's theorem". In: *Phys. Rev. Lett.* 67 (6 1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661.

[2] Rotem Arnon-Friedman et al. "Practical device-independent quantum cryptography via entropy accumulation". In: *Nature Communications* 9.1 (2018), p. 459. DOI: 10.1038/s41467-017-02307-4.

[3] Igor Devetak and Andreas Winter. "Distillation of secret key and entanglement from quantum states". In: *Proc. R. Soc. Lond. A* 461 (2005), pp. 207–235. DOI: 10.1098/rspa.2004.1372.

[4] Antonio Acín, Nicolas Gisin, and Lluis Masanes. "From Bell's Theorem to Secure Quantum Key Distribution". In: *Phys. Rev. Lett.* 97 (12 2006), p. 120405. DOI: 10.1103/PhysRevLett.97.120405.

[5] Yi Zhao et al. "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems". In: *Phys. Rev. A* 78 (4 2008), p. 042333. DOI: 10.1103/PhysRevA.78.042333.

[6] Lars Lydersen et al. "Hacking commercial quantum cryptography systems by tailored bright illumination". In: *Nature Photonics* 4 (2010), pp. 686–689. DOI: 10.1038/nphoton.2010.214.

[7] Henning Weier et al. "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors". In: *New Journal of Physics* 13.7 (2011), p. 073024. DOI: 10.1088/1367-2630/13/7/073024.

[8] Juan Carlos Garcia-Escartin, Shihan Sajeed, and Vadim Makarov. "Attacking quantum key distribution by light injection via ventilation openings". In: *preprint arXiv:1910.08152* (2019).

[9] Samuel L. Braunstein and Stefano Pirandola. "Side-Channel-Free Quantum Key Distribution". In: *Phys. Rev. Lett.* 108 (13 2012), p. 130502. DOI: 10.1103/PhysRevLett.108.130502.

[10] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. "Measurement-Device-Independent Quantum Key Distribution". In: *Phys. Rev. Lett.* 108 (13 2012), p. 130503. DOI: 10.1103/PhysRevLett.108.130503.

[11] A. Rubenok et al. "Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks". In: *Phys. Rev. Lett.* 111 (13 2013), p. 130501. DOI: 10.1103/PhysRevLett.111.130501.

[12] T. Ferreira da Silva et al. "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits". In: *Phys. Rev. A* 88 (5 2013), p. 052303. DOI: 10.1103/PhysRevA.88.052303.

[13] Yang Liu et al. "Experimental Measurement-Device-Independent Quantum Key Distribution". In: *Phys. Rev. Lett.* 111 (13 2013), p. 130502. DOI: 10.1103/PhysRevLett.111.130502.

[14] Zhiyuan Tang et al. "Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution". In: *Phys. Rev. Lett.* 112 (19 2014), p. 190503. DOI: 10.1103/PhysRevLett.112.190503.

[15] L. Comandar, M. Lucamarini, and B. et al. Fröhlich. "Quantum key distribution without detector vulnerabilities using optically seeded lasers". In: *Nature Photon* 10 (2016), pp. 312–315. DOI: 10.1038/nphoton.2016.50.

[16] Xavier Valcarce et al. "Self-testing two-qubit maximally entangled states from generalized CHSH tests". In: *preprint arXiv:2011.03047* (2020).

[17] Rene Schwonnek et al. "Robust Device-Independent Quantum Key Distribution". In: *preprint arXiv:2005.02691* (2020).

[18] Antonio Acín, Serge Massar, and Stefano Pironio. "Randomness versus Nonlocality and Entanglement". In: *Phys. Rev. Lett.* 108 (10 2012), p. 100402. DOI: 10.1103/PhysRevLett.108.100402.

[19] Camille Jordan. "Essai sur la géométrie à n dimensions". In: *Bulletin de la Société mathématique de France* 3 (1875), pp. 103–174.

[20] Ivan Šupić and Joseph Bowles. "Self-testing of quantum systems: a review". In: *Quantum* 4 (Sept. 2020), p. 337. DOI: 10.22331/q-2020-09-30-337.

[21] Stefano Pironio et al. "Device-independent quantum key distribution secure against collective attacks". In: *New Journal of Physics* 11.4 (2009), p. 045021. DOI: 10.1088/1367-2630/11/4/045021.

[22] M. Ho et al. “Noisy Preprocessing Facilitates a Photonic Realization of Device-Independent Quantum Key Distribution”. In: *Phys. Rev. Lett.* 124 (23 2020), p. 230502. DOI: 10.1103/PhysRevLett.124.230502.

[23] Renato Renner, Nicolas Gisin, and Barbara Kraus. “Information-theoretic security proof for quantum-key-distribution protocols”. In: *Physical Review A* 72.1 (2005), p. 012332. DOI: 10.1103/PhysRevA.72.012332.

[24] B. Kraus, N. Gisin, and R. Renner. “Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication”. In: *Phys. Rev. Lett.* 95 (8 2005), p. 080501. DOI: 10.1103/PhysRevLett.95.080501.

[25] Joseph M. Renes and Graeme Smith. “Noisy Processing and Distillation of Private Quantum States”. In: *Phys. Rev. Lett.* 98 (2 2007), p. 020502. DOI: 10.1103/PhysRevLett.98.020502.

[26] Erik Woodhead, Antonio Acín, and Stefano Pironio. “Device-independent quantum key distribution based on asymmetric CHSH inequalities”. In: *preprint arXiv:2007.16146* (2020).

[27] Ernest Y-Z Tan et al. “Improved DIQKD protocols with finite-size analysis”. In: *arXiv preprint arXiv:2012.08714* (2020).

[28] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 10th. USA: Cambridge University Press, 2011. ISBN: 1107002176.

[29] Xavier Valcarce et al. “What is the minimum CHSH score certifying that a state resembles the singlet?” In: *Quantum* 4 (Mar. 2020), p. 246. ISSN: 2521-327X. DOI: 10.22331/q-2020-03-23-246.

[30] Marissa Giustina et al. “Bell violation using entangled photons without the fair-sampling assumption”. In: *Nature* 497.7448 (2013), p. 227. DOI: 10.1038/nature12012.

[31] BG Christensen et al. “Detection-loophole-free test of quantum nonlocality, and applications”. In: *Physical review letters* 111.13 (2013), p. 130406. DOI: 10.1103/PhysRevLett.111.130406.

[32] Lynden K Shalm et al. “Strong loophole-free test of local realism”. In: *Physical review letters* 115.25 (2015), p. 250402. DOI: 10.1103/PhysRevLett.115.250402.

[33] Marissa Giustina et al. “Significant-loophole-free test of Bell’s theorem with entangled photons”. In: *Physical review letters* 115.25 (2015), p. 250401. DOI: 10.1103/PhysRevLett.115.250401.

[34] Lijiong Shen et al. “Randomness extraction from bell violation with continuous parametric down-conversion”. In: *Physical review letters* 121.15 (2018), p. 150402. DOI: 10.1103/PhysRevLett.121.150402.

[35] Yang Liu et al. “Device-independent quantum random-number generation”. In: *Nature* 562.7728 (2018), p. 548. DOI: 10.1038/s41586-018-0559-3.

[36] Philippe H. Eberhard. “Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment”. In: *Phys. Rev. A* 47 (2 1993), R747–R750. DOI: 10.1103/PhysRevA.47.R747.

[37] Xiongfeng Ma and Norbert Lütkenhaus. “Improved Data Post-Processing in Quantum Key Distribution and Application to Loss Thresholds in device independent QKD”. In: *Quantum Inf. Comput.* 12 (2012), pp. 203–214. DOI: https://doi.org/10.26421/QIC12.3-4.

[38] Alexey A. Melnikov, Pavel Sekatski, and Nicolas Sangouard. “Setting Up Experimental Bell Tests with Reinforcement Learning”. In: *Phys. Rev. Lett.* 125 (16 2020), p. 160401. DOI: 10.1103/PhysRevLett.125.160401.

[39] Erik Woodhead. “Tight asymptotic key rate for the Bennett-Brassard 1984 protocol with local randomization and device imprecisions”. In: *Phys. Rev. A* 90 (2 2014), p. 022306. DOI: 10.1103/PhysRevA.90.022306.

[40] L. Mirsky. “A trace inequality of John von Neumann”. In: *Monatshefte für Mathematik* 79.4 (Dec. 1975), pp. 303–306. DOI: 10.1007/bf01647331.

A Analytical results

A.1 Parametrization of two-qubit models

Following the logic of [21], we assume, without loss of generality that after the qubit reduction, the state shared by Alice, Bob and Eve is of the form

$$|\Psi\rangle_{ABE} = \sum_{i=1}^{4} \sqrt{L_i} \left|\Phi^i\right\rangle_{AB} |i\rangle_E \tag{52}$$

where we $|\Phi_i\rangle = \{\Phi^+, \Psi^-, \Phi^-, \Psi^+\}_{i=1}^4$, with nonnegative $L_1 \geq L_2$ and $L_3 \geq L_4$, and the measurements A_x, B_y appearing in the constraint are in the x-z plane

$$A_x = \mathbf{a}_x^T \begin{pmatrix} \sigma_z \\ \sigma_x \end{pmatrix} \qquad B_y = \mathbf{b}_y^T \begin{pmatrix} \sigma_z \\ \sigma_x \end{pmatrix}. \tag{53}$$

The key generating setting is explicitly parametrized by an angle ϕ

$$\mathbf{a}_0 = \begin{pmatrix} \mathrm{C}_\phi \\ \mathrm{S}_\phi \end{pmatrix}. \tag{54}$$

(As mentioned in the main text we use a compact notation $\mathrm{C}_\phi = \cos(\phi)$ and $\mathrm{S}_\phi = \sin(\phi)$ throughout the paper.) One notes that the application of a unitary transformation σ_Z on Alice's system is equivalent to changing the state and the measurements as

$$\begin{aligned} (L_1, L_2, L_3, L_4) &\to (L_3, L_4, L_1, L_2) \\ \mathbf{a}_x &\to \sigma_z \mathbf{a}_x \\ \mathbf{b}_y &\to \mathbf{b}_y. \end{aligned} \tag{55}$$

The two situations are completely equivalent for our purpose, so our parametrization of quantum models is actually redundant. To avoid this, we can introduce an order relation between the pairs of coefficients (L_1, L_2) and (L_3, L_4) (permuted by a basis transformation). In particular, we will impose

$$L_1 - L_2 \geq L_3 - L_4 \tag{56}$$

below, but will also use $L_1 + L_2 \geq L_3 + L_4$ for the certified numerical algorithm.

We also introduce a different parametrization of the probability simplex $\mathbf{L}$ with a vector $\mathbf{T} = (T_z, T_x, T_p)$ given by

$$\begin{cases} T_z = (L_1 - L_2) + (L_3 - L_4) \\ T_x = (L_1 - L_2) - (L_3 - L_4) \\ T_p = L_1 + L_2 - L_3 - L_4. \end{cases} \tag{57}$$

The conditions $L_1 \geq L_2, L_3 \geq L_4$ and $L_1 - L_2 \geq L_3 - L_4$ enforce

$$\begin{aligned} 0 \leq T_x \leq T_z \leq 1 \\ T_z + T_x - 1 \leq T_p \leq 1 - (T_z - T_x). \end{aligned} \tag{58}$$

A.2 Entropies of $\rho_{E|\hat{a}=\pm 1}$

Having introduced a parametrization of quantum models, we now express the quantities of interest $H(\rho_E), H(\rho_E|\hat{A}_0)$ and B_Ω as functions of the distribution $\mathbf{L}$ describing the state $|\Psi\rangle_{ABE}$ and the measurement settings $\mathbf{a}_x, \mathbf{b}_y$. The marginal state of Eve is straightforward to write down:

$$\rho_E = \begin{pmatrix} L_1 & & & \\ & L_2 & & \\ & & L_3 & \\ & & & L_4 \end{pmatrix}. \tag{59}$$

For the conditional states, we have

$$\rho_{E|\hat{a}=+1} = 2\,\mathrm{tr}_{AB}\frac{1+\hat{A}_0}{2}\otimes \mathbb{1}_{BE}\,|\Psi\rangle\langle\Psi|_{ABE} = \begin{pmatrix} L_1 & 0 & \mathrm{C}_\phi\sqrt{L_1L_3q} & \mathrm{S}_\phi\sqrt{L_1L_4q} \\ 0 & L_2 & \mathrm{S}_\phi\sqrt{L_2L_3q} & -\mathrm{C}_\phi\sqrt{L_2L_4q} \\ \mathrm{C}_\phi\sqrt{L_1L_3q} & \mathrm{S}_\phi\sqrt{L_2L_3q} & L_3 & 0 \\ \mathrm{S}_\phi\sqrt{L_1L_4q} & -\mathrm{C}_\phi\sqrt{L_2L_4q} & 0 & L_4 \end{pmatrix}, \tag{60}$$

where the factor of two arises because the probability to observe the outcome $\hat{A}_0 = 1$ is simply $\frac{1}{2}$. The conditional state for the other outcome $\hat{A}_0 = -1$ can be easily obtained by noticing that the two outcomes are interchanged by a mapping $\hat{A}_0 \to -\hat{A}_0$, i.e. with the inversion of the vector $\binom{\mathrm{C}_\phi}{\mathrm{S}_\phi} \to -\binom{\mathrm{C}_\phi}{\mathrm{S}_\phi}$. Consequently, we have

$$\rho_{E|\hat{a}=-1} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{pmatrix} \rho_{E|\hat{a}=1} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{pmatrix}. \tag{61}$$

It follows that the entropies of both conditional states are equal and

$$H(\rho_E|\hat{A}_0) = \frac{1}{2}H(\rho_{E|\hat{a}=+1}) + \frac{1}{2}H(\rho_{E|\hat{a}=-1}) = H(\rho_{E|\hat{a}=+1}). \tag{62}$$

Analogously to Eq. (61), there are unitary transformations (with different positions of 1 and -1 on the diagonal) that correspond to the transformations $\binom{\mathrm{C}_\phi}{\mathrm{S}_\phi} \to \binom{-\mathrm{C}_\phi}{\mathrm{S}_\phi}$ and $\binom{\mathrm{C}_\phi}{\mathrm{S}_\phi} \to \binom{\mathrm{C}_\phi}{-\mathrm{S}_\phi}$. This implies that $H(\rho_E|\hat{A}_0)$ and $H(\hat{A}_0|E)$ do not depend on these sign changes, i.e. they are only functions of C_ϕ^2 and S_ϕ^2.

A.3 Optimal key generating setting $\mathbf{a}_0$

In this section, we give the minimal angle ϕ for which constraint $\mathcal{B}_\Omega \geq \beta$ can be fulfilled for a given $\mathbf{L}$. We first focus on the possible values of ϕ. The expected Bell score is straightforward to compute:

$$\begin{aligned} \mathcal{B}_\Omega &= \frac{1}{2}\mathrm{tr}\left(\left(\left(\mathrm{C}_\Omega A_0 \otimes (B_0+B_1) + \mathrm{S}_\Omega A_1 \otimes (B_0-B_1)\right)\otimes \mathbb{1}_E\right)|\Psi\rangle\langle\Psi|_{ABE}\right) \\ &= \frac{1}{2}\mathrm{C}_\Omega\,\mathbf{a}_0^T \begin{pmatrix} T_z & \\ & T_x \end{pmatrix}(\mathbf{b}_0+\mathbf{b}_1) + \frac{1}{2}\mathrm{S}_\Omega\,\mathbf{a}_1^T \begin{pmatrix} T_z & \\ & T_x \end{pmatrix}(\mathbf{b}_0-\mathbf{b}_1) \end{aligned} \tag{63}$$

From this expression we notice that any of the following transformations of the key generating setting:

$$\mathbf{a}_0 \to \begin{pmatrix} (-1)^{s_1} & \\ & (-1)^{s_2} \end{pmatrix}\mathbf{a}_0, \tag{64}$$

with $s_1, s_2 \in \{0,1\}$ can be compensated by applying the same transformation to the remaining settings $\mathbf{a}_1$, $\mathbf{b}_y$ to give the same Bell score $\mathcal{B}_\Omega$. Furthermore, we have seen that this transformation does not change Eve's conditional entropy $H(\hat{A}_0|E)$. Therefore we can always restrict $\mathbf{a}_0$ to the positive quadrant of the circle

$$\phi \in [0, \frac{\pi}{2}] \tag{65}$$

without loss of generality. We now express the Bell score with Bob's settings parametrized as in Eq. (16):

$$\mathcal{B}_\Omega = \left\langle \mathrm{C}_\Omega\mathrm{C}_\theta\,\mathbf{a}_0\cdot\begin{pmatrix}Z\\X\end{pmatrix}\otimes\mathbf{c}\cdot\begin{pmatrix}Z\\X\end{pmatrix} + \mathrm{S}_\Omega\mathrm{S}_\theta\,\mathbf{a}_1\cdot\begin{pmatrix}Z\\X\end{pmatrix}\otimes\mathbf{c}_\perp\cdot\begin{pmatrix}Z\\X\end{pmatrix}\right\rangle. \tag{66}$$

Computing the expected value of the operators on our Bell diagonal state gives

$$\mathcal{B}_\Omega = \mathrm{C}_\Omega\mathrm{C}_\theta\,\mathbf{a}_0^T \begin{pmatrix} T_z & \\ & T_x \end{pmatrix}\mathbf{c} + \mathrm{S}_\Omega\mathrm{S}_\theta\,\mathbf{a}_1^T \begin{pmatrix} T_z & \\ & T_x \end{pmatrix}\mathbf{c}_\perp. \tag{67}$$

We introduce an angle γ to parametrize the vectors $\mathbf{c}$ and $\mathbf{c}_\perp$:

$$\mathbf{c} = \begin{pmatrix}\mathrm{C}_\gamma\\ \mathrm{S}_\gamma\end{pmatrix}, \quad \mathbf{c}_\perp = \begin{pmatrix}-\mathrm{S}_\gamma\\ \mathrm{C}_\gamma\end{pmatrix}. \tag{68}$$

The maximization with the second setting of Alice is straightforward, that is

$$\max_{\mathbf{a}_1} \mathrm{S}_\theta \mathbf{a}_1^T \begin{pmatrix} T_z & \\ & T_x \end{pmatrix} \mathbf{c}_\perp = \|\mathrm{S}_\theta \begin{pmatrix} T_z & \\ & T_x \end{pmatrix} \mathbf{c}_\perp\| = |\mathrm{S}_\theta| \sqrt{T_z^2 \mathrm{S}_\gamma^2 + T_x^2 \mathrm{C}_\gamma^2}. \tag{69}$$

The Bell score (optimized with respect to $\mathbf{a}_1$) becomes

$$\mathcal{B}_\Omega = \mathrm{C}_\Omega \mathrm{C}_\theta \begin{pmatrix} \mathrm{C}_\phi \\ \mathrm{S}_\phi \end{pmatrix}^T \begin{pmatrix} T_z & \\ & T_x \end{pmatrix} \begin{pmatrix} \mathrm{C}_\gamma \\ \mathrm{S}_\gamma \end{pmatrix} + \mathrm{S}_\Omega |\mathrm{S}_\theta| \sqrt{T_z^2 \mathrm{S}_\gamma^2 + T_x^2 \mathrm{C}_\gamma^2}. \tag{70}$$

Since $T_z, T_x \geq 0$ and $\phi, \Omega \in [0, \frac{\pi}{2}]$, we can also restrict the angle θ and γ to the interval $[0, \frac{\pi}{2}]$ without loss of generality, and drop the absolute value: $|\mathrm{S}_\theta| = \mathrm{S}_\theta$. The constraint $\mathcal{B}_\Omega \geq \beta$ takes the form

$$\mathrm{C}_\Omega \begin{pmatrix} \mathrm{C}_\phi \\ \mathrm{S}_\phi \end{pmatrix}^T \begin{pmatrix} T_z & \\ & T_x \end{pmatrix} \begin{pmatrix} \mathrm{C}_\gamma \\ \mathrm{S}_\gamma \end{pmatrix} \geq \frac{\beta - \mathrm{S}_\Omega \mathrm{S}_\theta \sqrt{T_z^2 \mathrm{S}_\gamma^2 + T_x^2 \mathrm{C}_\gamma^2}}{\mathrm{C}_\theta}. \tag{71}$$

Recall that we wish to find the minimal ϕ for which this inequality can be fulfilled for at least one value of the free parameters θ and γ. We observe that if the right hand side (RHS) can become zero or negative by some choice of θ and γ, the constraint becomes trivial. Since $T_z \geq T_x$, this is possible for

$$\beta^2 \leq \mathrm{S}_\Omega^2 T_z^2 \implies \phi_* = 0. \tag{72}$$

In the following we assume that this is not the case, i.e. $\beta^2 > \mathrm{S}_\Omega^2 T_z^2$. The angle θ only appears on the right of the inequality, so to satisfy the inequality our best choice is to minimize the RHS with respect to θ. The expression

$$\frac{\beta - \mathrm{S}_\Omega \mathrm{S}_\theta \sqrt{T_z^2 \mathrm{S}_\gamma^2 + T_x^2 \mathrm{C}_\gamma^2}}{\mathrm{C}_\theta} \tag{73}$$

either has a local minimum that can be found by setting its derivative to zero, or there is no local minimum and the expression is minimal at the boundary $\theta = 0$ since it diverges for $\theta \to \frac{\pi}{2}$. Differentiating the expression with respect to theta, we find that a local minumum does exist at

$$\mathrm{S}_\theta = \frac{\mathrm{S}_\Omega \sqrt{T_z^2 \mathrm{S}_\gamma^2 + T_x^2 \mathrm{C}_\gamma^2}}{\beta}, \tag{74}$$

(recall the assumption above). Plugging this value into Eq. (71) allows us to rewrite the constraint as

$$\mathrm{C}_\Omega \begin{pmatrix} \mathrm{C}_\phi \\ \mathrm{S}_\phi \end{pmatrix}^T \begin{pmatrix} T_z & \\ & T_x \end{pmatrix} \begin{pmatrix} \mathrm{C}_\gamma \\ \mathrm{S}_\gamma \end{pmatrix} \geq \sqrt{\beta^2 - \mathrm{S}_\Omega^2 (T_z^2 \mathrm{S}_\gamma^2 + T_x^2 \mathrm{C}_\gamma^2)}, \tag{75}$$

which we rewrite as

$$\begin{pmatrix} \mathrm{C}_\phi \\ \mathrm{S}_\phi \end{pmatrix}^T \mathbf{v}_\gamma \geq 1, \qquad \text{with} \qquad \mathbf{v}_\gamma = \frac{\mathrm{C}_\Omega}{\sqrt{\beta^2 - \mathrm{S}_\Omega^2 (T_z^2 \mathrm{S}_\gamma^2 + T_x^2 \mathrm{C}_\gamma^2)}} \begin{pmatrix} T_z \mathrm{C}_\gamma \\ T_x \mathrm{S}_\gamma \end{pmatrix}. \tag{76}$$

Now it becomes simple to check if the constraint can be satisfied at all. The vector $\mathbf{v}_\gamma$ belongs to the positive quadrant of the plane with $\mathbf{v}_0 \parallel \binom{1}{0}$ and $\mathbf{v}_{\pi/2} \parallel \binom{0}{1}$, hence the inequality $\mathbf{a}_0 \cdot \mathbf{v}_\gamma \geq 1$ can be satisfied if and only if the length of the vector $\mathbf{v}_\gamma$ reaches 1, i.e.

$$|\mathbf{v}_\gamma|^2 = \frac{\mathrm{C}_\Omega^2 (T_z^2 \mathrm{C}_\gamma^2 + T_x^2 \mathrm{S}_\gamma^2)}{\beta^2 - \mathrm{S}_\Omega^2 (T_z^2 \mathrm{S}_\gamma^2 + T_x^2 \mathrm{C}_\gamma^2)} \geq 1 \tag{77}$$

for some γ. We rewrite this inequality as

$$\frac{1}{2} \left(T_z^2 + T_x^2 + (T_z^2 - T_x^2) \mathrm{C}_{2\gamma} \mathrm{C}_{2\Omega} - 2\beta^2 \right) \geq 0. \tag{78}$$

Given that $T_z^2 \geq T_x^2$, the left hand side (LHS) is maximal for $\gamma = 0$ if $\Omega \leq \frac{\pi}{4}$ and for $\gamma = \frac{\pi}{2}$ if $\Omega > \frac{\pi}{4}$. Hence, $\mathcal{B}_\Omega \geq \beta$ can be fulfilled if and only if

$$\boxed{\begin{array}{ll} \text{for } \Omega \leq \dfrac{\pi}{4}, & \mathrm{C}_\Omega^2 T_z^2 + \mathrm{S}_\Omega^2 T_x^2 \geq \beta^2 \\ \text{for } \Omega > \dfrac{\pi}{4}, & \mathrm{S}_\Omega^2 T_z^2 + \mathrm{C}_\Omega^2 T_x^2 \geq \beta^2. \end{array}} \tag{79}$$

Consider the first case $\boxed{\Omega \leq \frac{\pi}{4}}$. Setting $\gamma = 0$ one verifies that if the constraint can be fulfilled, then it can be fulfilled with $\phi = 0$:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}^T \mathbf{v}_0 = \frac{\mathrm{C}_\Omega T_z}{\sqrt{\beta^2 - \mathrm{S}_\Omega^2 T_x^2}} \geq 1 \quad \Longleftrightarrow \quad \mathrm{C}_\Omega^2 T_z^2 + \mathrm{S}_\Omega^2 T_x^2 \geq \beta^2. \tag{80}$$

Hence, in this case the minimal possible angle is $\phi_* = 0$ as long as the Bell score can be attained as formalized by Eq. (79).

The other case $\boxed{\Omega > \frac{\pi}{4}}$ is less trivial. Assume that the constraint can be satisfied, $\mathrm{S}_\Omega^2 T_z^2 + \mathrm{C}_\Omega^2 T_x^2 \geq \beta^2$. We first check if $\phi = 0$ is a solution

$$\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}^T \mathbf{v}_\gamma\right)^2 = \frac{\mathrm{C}_\Omega^2 \mathrm{C}_\gamma^2 T_z^2}{\beta^2 - \mathrm{S}_\Omega^2 (T_z^2 \mathrm{S}_\gamma^2 + T_x^2 \mathrm{C}_\gamma^2)} \geq 1 \quad \Longleftrightarrow \quad \mathrm{C}_\gamma^2 (\mathrm{C}_\Omega^2 T_z^2 + \mathrm{S}_\Omega^2 T_x^2 - \mathrm{S}_\Omega^2 T_z^2) + \mathrm{S}_\Omega^2 T_z^2 \geq \beta^2. \tag{81}$$

As $\mathrm{S}_\Omega^2 T_z^2 + \mathrm{C}_\Omega^2 T_x^2 \geq \beta^2 \geq \mathrm{S}_\Omega^2 T_z^2$, the LHS is maximal for $\gamma = 0$. Therefore $\phi_* = 0$ iff

$$\mathrm{C}_\Omega^2 T_z^2 + \mathrm{S}_\Omega^2 T_x^2 \geq \beta^2. \tag{82}$$

We now assume

$$\mathrm{S}_\Omega^2 T_z^2 + \mathrm{C}_\Omega^2 T_x^2 \geq \beta^2 > \mathrm{C}_\Omega^2 T_z^2 + \mathrm{S}_\Omega^2 T_x^2, \tag{83}$$

such that the constraint can be fulfilled but not with $\phi = 0$. To find the minimal ϕ that allows to do so we look on the dependence of the length of the vector $\mathbf{v}_\gamma$ on γ. We compute

$$\frac{d}{d\gamma} |\mathbf{v}_\gamma|^2 = \frac{(T_z^2 - T_x^2) \mathrm{C}_\Omega^2 \mathrm{S}_{2\gamma}}{(\beta^2 - (T_z^2 \mathrm{S}_\gamma^2 + T_x^2 \mathrm{C}_\gamma^2) \mathrm{S}_\Omega^2)^2} ((T_z^2 + T_x^2) \mathrm{S}_\Omega^2 - \beta^2), \tag{84}$$

here $(T_z^2 + T_x^2)\mathrm{S}_\Omega^2 \geq \mathrm{S}_\Omega^2 T_z^2 + \mathrm{C}_\Omega^2 T_x^2 \geq \beta^2$. Thus the derivative is positive and the length of $\mathbf{v}_\gamma$ is increasing with γ.

We can now give a simple geometrical interpretation to our problem of finding the minimal ϕ: for each value ϕ such that

$$\begin{pmatrix} \mathrm{C}_\phi \\ \mathrm{S}_\phi \end{pmatrix}^T \mathbf{v}_\gamma \geq 1 \tag{85}$$

a line tangent to the unit circle at $\binom{\mathrm{C}_\phi}{\mathrm{S}_\phi}$ is also crossing the curve $\mathbf{v}_\gamma$. So for the minimal value ϕ_* there is a line tangent to both $\mathbf{v}_\gamma$ and the unit circle at $\binom{\mathrm{C}_{\phi_*}}{\mathrm{S}_{\phi_*}}$. The equation of the line tangent to $\mathbf{v}_\gamma$ reads $\boldsymbol{\ell}(\lambda) = \mathbf{v}_\gamma + \lambda \mathbf{v}'_\gamma$. This line is tangent to the unit circle if and only if the equation

$$|\mathbf{v}_\gamma + \lambda \mathbf{v}'_\gamma|^2 = 1 \tag{86}$$

has only one solution, where the derivative is with respect to γ. This is a quadratic equation

$$\lambda^2 |\mathbf{v}'_\gamma|^2 + 2\lambda \mathbf{v}'_\gamma \cdot \mathbf{v}_\gamma + |\mathbf{v}_\gamma|^2 - 1 = 0, \tag{87}$$

which has a unique solution iff its determinant is zero

$$\left(\mathbf{v}'_\gamma \cdot \mathbf{v}_\gamma\right)^2 = |\mathbf{v}'_\gamma|^2 \left(|\mathbf{v}_\gamma|^2 - 1\right). \tag{88}$$

With

$$\mathbf{v}'_\gamma = \frac{\mathrm{C}_\Omega}{(\beta^2 - \mathrm{S}_\Omega^2(T_x^2\mathrm{C}_\gamma^2 + T_z^2\mathrm{S}_\gamma^2))^{3/2}} \begin{pmatrix} T_z\mathrm{S}_\gamma(T_z^2\mathrm{S}_\Omega^2 - \beta^2) \\ -T_x\mathrm{C}_\gamma(T_x^2\mathrm{S}_\Omega^2 - \beta^2) \end{pmatrix} \tag{89}$$

lengthy but straightforward algebra gives

$$\mathrm{S}_\gamma^2 = -\frac{T_x^2(\beta^2 - T_x^2\mathrm{S}_\Omega^2)(\beta^2 - (T_z^2 + T_x^2)\mathrm{S}_\Omega^2)}{(T_z^2 - T_x^2)\left(\beta^4 + \mathrm{S}_\Omega^2(T_x^2T_z^2 - 2\beta^2(T_x^2 + T_z^2)) + \mathrm{S}_\Omega^4(T_x^4 + T_z^4)\right)}. \tag{90}$$

To find that the minimal angle ϕ_* note that for the tangent line $\binom{\mathrm{C}_{\phi_*}}{\mathrm{S}_{\phi_*}} \cdot \mathbf{v}'_\gamma = 0$, and therefore $\binom{-\mathrm{S}_{\phi_*}}{\mathrm{C}_{\phi_*}} = \frac{\mathbf{v}'_\gamma}{|\mathbf{v}'_\gamma|}$. Plugging in the above equations we find

$$c_*^2(\mathbf{L}, \Omega, \beta) = \cos^2\left(\phi_*(\mathbf{L}, \Omega, \beta)\right) = \frac{(\beta^2 - \mathrm{S}_\Omega^2T_x^2)(\mathrm{C}_\Omega^2T_x^2 + \mathrm{S}_\Omega^2T_z^2 - \beta^2)}{\mathrm{C}_\Omega^2(T_z^2 - T_x^2)(\mathrm{S}_\Omega^2T_z^2 + \mathrm{S}_\Omega^2T_x^2 - \beta^2)}. \tag{91}$$

A.4 Eve's maximum information for $\Omega \leq \frac{\pi}{4}$

We here give details on the derivation of the formula (25) in the main text which corresponds to Eve's maximum information in the case $\Omega \leq \frac{\pi}{4}$. For these inequalities we have seen that the constraint $\mathrm{C}_\Omega^2\, T_z^2 + \mathrm{S}_\Omega\, T_x^2 \geq \beta^2$ can be fulfilled with $c_*^2(\mathbf{L}, \beta) = 1$. It has been shown in Ref. [22] that $H(\rho_{E|\hat{a}=+1})$ is a monotonic function in the key generating setting $\phi \in [0, \frac{\pi}{4}]$. The wost case (optimal attack for Eve) thus consists in setting the measurement angle $\mathrm{C}_\phi = 1$, which implies a simple form for the state

$$\rho_{E|\hat{a}=+1} = \begin{pmatrix} L_1 & 0 & \sqrt{L_1L_3q} & 0 \\ 0 & L_2 & 0 & -\sqrt{L_2L_4q} \\ \sqrt{L_1L_3q} & 0 & L_3 & 0 \\ 0 & -\sqrt{L_2L_4q} & 0 & L_4 \end{pmatrix}, \tag{92}$$

with a closed form expression for its eigenvalues implying

$$H(\rho_{E|\hat{a}=1}) = H\Big(\mathbf{p} = \begin{pmatrix} \frac{1}{2}\left(L_1 + L_3 + \sqrt{4L_1L_3q + (L_1 - L_3)^2}\right) \\ \frac{1}{2}\left(L_1 + L_3 - \sqrt{4L_1L_3q + (L_1 - L_3)^2}\right) \\ \frac{1}{2}\left(L_2 + L_4 + \sqrt{4L_2L_4q + (L_2 - L_4)^2}\right) \\ \frac{1}{2}\left(L_2 + L_4 - \sqrt{4L_2L_4q + (L_2 - L_4)^2}\right) \end{pmatrix}\Big). \tag{93}$$

The constraint on the generalized CHSH score leads to the following constraint on the vector $\mathbf{L}$

$$\begin{pmatrix} T_Z^2 \\ T_X^2 \end{pmatrix} \cdot \begin{pmatrix} \mathrm{C}_\Omega^2 \\ \mathrm{S}_\Omega^2 \end{pmatrix} = 2\,(L_3 - L_4)\,(L_1 - L_2)\,\mathrm{C}_{2\Omega} + (L_1 - L_2)^2 + (L_3 - L_4)^2 \geq \beta^2. \tag{94}$$

Our goal is thus to find the components of the vector $\mathbf{L}$ maximizing $H(\mathbf{L}) - \mathbf{H}(\mathbf{p})$ and satisfying the previous constraint. Inspired by Ref. [22], we first introduce the following parametrization

$$\begin{aligned} L_1 &= Px \\ L_3 &= P(1 - x) \\ L_2 &= (1 - P)y \\ L_4 &= (1 - P)(1 - y). \end{aligned} \tag{95}$$

The partial ordering of the $\mathbf{L}$ coefficients implies

$$(1 - P)y \leq Px \leq (1 - P)y + 2P - 1 \tag{96}$$

which requires $P \geq \frac{1}{2}$. The advantage of this parametrization comes from the fact that our figure of merit can be nicely rewritten as

$$\begin{aligned} H(\mathbf{L}) - H(\mathbf{p}) &= Ph_q(x) + (1 - P)h_q(y) \\ h_q(z) &= h(z) - h(n_q(z)) \\ n_q(z) &= \frac{1 + \sqrt{1 - 4\,(1 - q)\,z(1 - z)}}{2} \end{aligned} \tag{97}$$

where $h(z) = -z\log(z) - (1-z)\log(1-z)$ is the binary entropy function with the logarithm in base 2, while the constraint on the expected value of the generalized CHSH operator is given by

$$\mathrm{S}_\Omega\,(2P(x+y-1)-2y+1)^2 + \mathrm{C}_\Omega\,(1-2P)^2 \geq \beta^2 \tag{98}$$

For a fixed P, the curve in the (x,y)-plan that corresponds to a constant value β satisfies $P\,dx = (1-P)\,dy$. This remark allows one to maximize $H(\mathbf{L}) - H(\mathbf{p})$ along this curve and find that it is optimal for Eve to set $x+y=1$, see appendix C2 in Ref. [22] for the detailed argument. The symmetry of the function $h_q(x) = h_q(1-x)$ allows us to write the problem as

$$\begin{aligned} &\max_{x,P}\ H(\mathbf{L}) - H(\mathbf{p}) = h_q(x) \\ &\text{s.t. } (2P-1)^2\mathrm{C}_\Omega^2 + (1-2x)^2\mathrm{S}_\Omega^2 \geq \beta^2. \end{aligned} \tag{99}$$

As the goal function $h_q(x)$ does not depend on P, we can set its value to $P=1$ because this is the value maximizing the LHS of the constraint inequality and allowing the largest possible interval for the remaining variable x. We thus get

$$\begin{aligned} &\max_{x,P}\ H(\mathbf{L}) - H(\mathbf{p}) = h_q(x) \\ &\text{s.t. } (1-2x)^2 \geq \frac{\beta^2 - \mathrm{C}_\Omega^2}{\mathrm{S}_\Omega^2}. \end{aligned} \tag{100}$$

Finally, as $h_q(x)$ is a monotonically decreasing function of x (see Ref. [22]), it is optimal to set x to the least possible value compatible with the constraint. This implies

$$\boxed{\begin{aligned} &I(\beta;\Omega,q) = h_q(z) \\ &\quad\text{with } z = \frac{1}{2}\left(\frac{\sqrt{\beta^2-\mathrm{C}_\Omega^2}}{\mathrm{S}_\Omega}+1\right). \end{aligned}} \tag{101}$$

Let us now recall that the situation with $c_*^2(\mathbf{L},\beta) = 1$ and $\mathrm{C}_\Omega^2\,T_z^2 + \mathrm{S}_\Omega\,T_x^2 \geq \beta^2$ also occurs in the case $\Omega > \frac{\pi}{4}$. The above proof guarantees that it is optimal for Eve to use strategies where the inequality is saturated $\mathrm{C}_\Omega^2\,T_z^2 + \mathrm{S}_\Omega\,T_x^2 = \beta^2$. Hence in the optimization problem for $\Omega > \frac{\pi}{4}$ we can ignore all the strategies with $\mathrm{C}_\Omega^2\,T_z^2 + \mathrm{S}_\Omega\,T_x^2 > \beta^2$.

A.5 Concavity of $h_q \circ z(\beta)$

Recall that in order to use the bound $I(\beta;\Omega,q)$ derived for two-qubit strategies in the previous section as a universal bound (valid for strategies in any dimension), we have to show that this function is concave. In this case, for any mixture of qubit strategies (enforced by the Jordan's lemma) with an average score $\bar{\beta} = \sum_i p_i\beta_i$, Eve's information satisfies

$$\bar{I}(\beta;\Omega,q) = \sum_i p_i I(\beta_i;\Omega,q) \leq I(\bar{\beta};\Omega,q). \tag{102}$$

The concavity of $I(\beta;\Omega,q) = h_q(z(\beta))$ follows from the fact that its second derivative is negative

$$\frac{d^2}{d\beta^2}h_q\big(z(\beta)\big) = h_q''(z)\big(z'(\beta)\big)^2 + h_q'(z)z''(\beta) \leq 0, \tag{103}$$

which we are going to show below. In this section we will use the natural algorithm instead of logarithm in base 2. The function $h_q(z)$ takes a positive real factor upon changing the base of the algorithm, so it is irrelevant for its concavity. Note first that $z(\beta) \in [\frac{1}{2},1]$ and

$$\sqrt{\beta^2-\mathrm{C}_\Omega^2} = \mathrm{S}_\Omega(2z-1). \tag{104}$$

Then consider the following identities

$$\begin{aligned} (z'(\beta))^2 &= \frac{\beta^2}{4\mathrm{S}_\Omega^2(\beta^2-\mathrm{C}_\Omega^2)} = \frac{\mathrm{S}_\Omega^2(2z-1)^2+\mathrm{C}_\Omega^2}{4\mathrm{S}_\Omega^4(2z-1)^2} \\ z''(\beta) &= \frac{-\mathrm{C}_\Omega^2}{2\mathrm{S}_\Omega(\beta^2-\mathrm{C}_\Omega^2)^{3/2}} = \frac{-\mathrm{C}_\Omega^2}{2\mathrm{S}_\Omega^4(2z-1)^3}. \end{aligned} \tag{105}$$

The identity (26) that we want to prove thus becomes

$$\frac{h_q''(z)(2z-1)(\mathrm{S}_\Omega^2(2z-1)^2+\mathrm{C}_\Omega^2)-2h_q'(z)\mathrm{C}_\Omega^2}{4\mathrm{S}_\Omega^4(2z-1)^3}\leq 0. \tag{106}$$

Multiplying by a positive fraction $\frac{4\mathrm{S}_\Omega^4(2z-1)^3}{\mathrm{C}_\Omega^2}$ it can be straightforwardly simplified to the form

$$h_q''(z)(2z-1)(\mathrm{T}_\Omega^2(2z-1)^2+1)-2\,h_q'(z)\leq 0. \tag{107}$$

As $h_q''(z)\leq 0$ was proven in [22, 39], we have the inequality

$$h_q''(z)(2z-1)^2\,\mathrm{T}_\Omega^2\leq 0. \tag{108}$$

We use it to relax the inequality in Eq. (107) to

$$h_q''(z)(z-\frac{1}{2})-h_q'(z)\leq 0. \tag{109}$$

At the point $z=\frac{1}{2}$ the left hand side becomes zero, since $h_q'(\frac{1}{2})=0$ and $|h_q''(\frac{1}{2})|<\infty$, see below. From now on, we thus exclude the point $z=\frac{1}{2}$ and consider $z\in(\frac{1}{2},1]$. Now we can divide the whole expression by a strictly positive factor $(z-\frac{1}{2})^2$. We obtain

$$\frac{1}{2}\frac{h_q''(z)(z-\frac{1}{2})-h_q'(z)(z-\frac{1}{2})'}{(z-\frac{1}{2})^2}\leq 0, \tag{110}$$

or

$$\frac{1}{2}\left(\frac{h_q'(z)}{z-\frac{1}{2}}\right)'=\left(\frac{h_q'(z)}{2z-1}\right)'\leq 0. \tag{111}$$

In other words we want to show that the function

$$(*)\ \frac{d}{dz}\left(\frac{h_q'(z)}{2z-1}\right)\leq 0 \tag{112}$$

on the interval $z\in(\frac{1}{2},1]$. Let us now compute this function:

$$\frac{h_q'(z)}{2z-1}=\frac{h'(z)}{2z-1}-h'(n_q(z))\frac{n_q'(z)}{2z-1}. \tag{113}$$

The last fraction can be simplified to

$$\frac{n_q'(z)}{2z-1}=\frac{(2z-1)(1-q)}{(2z-1)\sqrt{1-4\,(1-q)\,z(1-z)}}=\frac{1-q}{2n_q(z)-1}. \tag{114}$$

Therefore

$$\frac{h_q'(z)}{2z-1}=\frac{h'(z)}{2z-1}-(1-q)\frac{h'(n_q(z))}{2n_q(z)-1}=g(z)-(1-q)g\big(n_q(z)\big), \tag{115}$$

where

$$g(z)=\frac{h'(z)}{2z-1}=-\frac{\log(\frac{z}{1-z})}{2z-1}. \tag{116}$$

To complete the proof we thus need to show that

$$(*)\quad g'(z)-(1-q)g'\big(n_q(z)\big)n_q'(z)\leq 0. \tag{117}$$

From Eq. (114), we have

$$n_q'(z)=(1-q)\frac{2z-1}{2n_q(z)-1}, \tag{118}$$

so the inequality to be shown can be rewritten as

$$\frac{g'(z)}{2z-1}-(1-q)^2\frac{g'(n_q(z))}{2n_q(z)-1}\leq 0. \tag{119}$$

For $q = 0$ we have $(1-q) = 1$ and $n_q(z) = z$ so the two terms are equal. The identity to be shown can then be expressed as

$$\begin{aligned} (*) \qquad & f(z,0) - f(z,q) \leq 0 \\ \text{with} \quad & f(z,q) = (1-q)^2 u(n_q(z)) \\ & u(z) = \frac{g'(z)}{2z-1} = \frac{\frac{1}{z-1} + \frac{1}{z} + 2\log\left(\frac{z}{1-z}\right)}{(2z-1)^3}, \end{aligned} \tag{120}$$

which holds for $q = 0$ trivially. To show that it holds for all q it is sufficient to demonstrate that the function $f(z,q)$ is increasing with q, i.e.

$$(*) \qquad \frac{d}{dq} f(z,q) \geq 0, \tag{121}$$

which we are going to show now.
Using

$$\frac{d}{dq} n_q(z) = \frac{(1-z)z}{\sqrt{1-4(1-q)(1-z)z}} = \frac{n_q(z)(1-n_q(z))}{(1-q)(2n_q(z)-1)} \tag{122}$$

we obtain

$$\begin{aligned} \frac{d}{dq} f(z,q) &= -2(1-q)u\big(n_q(z)\big) + (1-q)^2 u'\big(n_q(z)\big) \frac{d}{dq} n_q(z) \\ &= -2(1-q)u(n) + (1-q)u'(n)\frac{n(1-n)}{2n-1} \end{aligned} \tag{123}$$

for $n > \frac{1}{2}$, which is positive iff $q = 1$ or

$$(*) \qquad u'(n)n(1-n) - 2u(n)(2n-1) \geq 0. \tag{124}$$

In the case $q < 1$, straightforward algebra allows to find a simple expression of the left hand side and rewrite the condition as

$$\begin{aligned} & \frac{6n^2 - 4n^3 - 1 + 4(n^4 - 2n^3 + 2n^2 - n)\log\left(\frac{n}{1-n}\right)}{(2n-1)^4 n(1-n)} \geq 0 \\ \iff \quad & 6n^2 - 4n^3 - 1 + 4(n^4 - 2n^3 + 2n^2 - n)\log\left(\frac{n}{1-n}\right) \geq 0 \end{aligned} \tag{125}$$

Changing the variable to $x + 1 = \frac{n}{1-n}$ with $x \geq 0$ we express the above inequality as

$$\begin{aligned} & \frac{x(x^2+6x+6)}{(x+2)^3} - 4\frac{(x+1)(x^2+3x+3)}{(x+2)^4}\log(x+1) \geq 0 \\ \iff \quad & \log(1+x) \leq \frac{x(x+2)(x^2+6x+6)}{4(x+1)(x^2+3x+3)}. \end{aligned} \tag{126}$$

To prove this relation note that there is equality for $x = 0$, but the LHS increases slower than the RHS

$$\begin{aligned} & \log'(1+x) \leq \left(\frac{x(x+2)(x^2+6x+6)}{4(x+1)(x^2+3x+3)}\right)' \\ \iff \quad & \frac{1}{1+x} \leq \frac{1}{4}\left(\frac{9(x+1)}{(x(x+3)+3)^2} + \frac{1}{(x+1)^2} + \frac{3}{x(x+3)+3} + 1\right) \\ \iff \quad & \frac{x^4(x+2)^2}{4(x+1)^2(x(x+3)+3)^2} \geq 0, \end{aligned} \tag{127}$$

which concludes the proof.

Properties of $h'_q(\frac{1}{2})$ and $h''_q(\frac{1}{2})$ We start with the first derivative and want to show that $h'_q(\frac{1}{2}) = 1/2$. We have

$$h'_q(z) = \Big(h(z) - h(n_q(z))\Big)' = h'(z) - h'(n_q(z))n'_q(z) \tag{128}$$

The binary entropy hits a maximum at $z = 1/2$ so $h'(\frac{1}{2}) = 0$. For the second term, we use (118) to get

$$h'(n_q(z))n'_q(z) = -(1-q)\frac{2z-1}{2n_q(z)-1}\log\left(\frac{n_q(z)}{1-n_q(z)}\right), \tag{129}$$

$(2z-1) = 0$ at $z = \frac{1}{2}$, while

$$\left|\frac{1-q}{2n_q(z)-1}\log\left(\frac{n_q(z)}{1-n_q(z)}\right)\Big|_{z=1/2}\right| = \left|\frac{(1-q)\log\left(\frac{1+\sqrt{q}}{1-\sqrt{q}}\right)}{\sqrt{q}}\right|. \tag{130}$$

Changing the variable to $x+1 = \frac{1+\sqrt{q}}{1-\sqrt{q}}$ with $x \geq 0$ yields for the last expression

$$\left|\frac{4(x+1)\log(x+1)}{x(x+2)}\right| < \infty. \tag{131}$$

It is obviously bounded for $x > \epsilon$ with any ϵ, and the fact that the limit $x \to 0$ exists can be seen by straightforward application of l'Hôpital's rule. Hence,

$$h'_q\left(\frac{1}{2}\right) = 0. \tag{132}$$

We also wish to show that the second derivative $h''_q(\frac{1}{2})$ is bounded. To do so we compute

$$h''_q\left(\frac{1}{2}\right) = \frac{2(1-q)\log\left(\frac{1+\sqrt{q}}{1-\sqrt{q}}\right)}{\sqrt{q}} - 4. \tag{133}$$

But as we have just shown that

$$\left|\frac{(1-q)\log\left(\frac{1+\sqrt{q}}{1-\sqrt{q}}\right)}{\sqrt{q}}\right| < \infty, \tag{134}$$

the desired result

$$\left|h''_q\left(\frac{1}{2}\right)\right| < \infty \tag{135}$$

follows.

A.6 Maximization of the generalized CHSH score with respect to auxiliary settings

In the goal function

$$H(\rho_E) - H(\rho_E|\hat{a}_0(q)) + t\,\mathcal{B}_\Omega(\mathbf{L}, \phi, \boldsymbol{a}_1, \boldsymbol{b}_0, \boldsymbol{b}_1) \tag{136}$$

that *a priori* appears in Eq. (39), it is only the Bell score which depends on the auxiliaty measuremnt settigns $\boldsymbol{a}_1, \boldsymbol{b}_0$ and $\boldsymbol{b}_1$. As t is always positive we can straigtforwardly maximise the score with respect to these settings. We thus define

$$\beta_{\max}(\boldsymbol{L}, \phi) = \max_{\boldsymbol{a}_1, \boldsymbol{b}_0, \boldsymbol{b}_1} \mathcal{B}_\Omega(\mathbf{L}, \phi, \boldsymbol{a}_1, \boldsymbol{b}_0, \boldsymbol{b}_1), \tag{137}$$

which actually appears in Eq. (39).

Let us now compute this expression starting from Eq. (67), that we put in the form

$$\mathcal{B}_\Omega = \begin{pmatrix} \mathrm{C}_\theta \\ \mathrm{S}_\theta \end{pmatrix} \cdot \begin{pmatrix} \mathrm{C}_\Omega\, \mathbf{a}_0^T \begin{pmatrix} T_z \mathrm{C}_\gamma \\ T_x \mathrm{S}_\gamma \end{pmatrix} \\ \mathrm{S}_\Omega\, \mathbf{a}_1^T \begin{pmatrix} -T_z \mathrm{S}_\gamma \\ T_x \mathrm{C}_\gamma \end{pmatrix} \end{pmatrix}. \tag{138}$$

This form makes the maximization with respect to θ and $\mathbf{a}_1$ straightforward

$$\begin{aligned}\max_{\theta,\mathbf{a_1}} \mathcal{B}_\Omega &= \max_{\mathbf{a}_1} \sqrt{\left(\mathrm{C}_\Omega\, \mathbf{a}_0^T \begin{pmatrix} T_z \mathrm{C}_\gamma \\ T_x \mathrm{S}_\gamma \end{pmatrix}\right)^2 + \left(\mathrm{S}_\Omega\, \mathbf{a}_1^T \begin{pmatrix} -T_z \mathrm{S}_\gamma \\ T_x \mathrm{C}_\gamma \end{pmatrix}\right)^2} \\ &= \sqrt{\mathrm{C}_\Omega^2 \left(\mathrm{C}_\phi T_z \mathrm{C}_\gamma + \mathrm{S}_\phi T_x \mathrm{S}_\gamma\right)^2 + \mathrm{S}_\Omega^2 \left(T_z^2 \mathrm{S}_\gamma^2 + T_x^2 \mathrm{C}_\gamma^2\right)}.\end{aligned} \tag{139}$$

To find the maximum with respect to γ or $\mathbf{c} = \binom{\mathrm{C}_\gamma}{\mathrm{S}_\gamma}$ it is convenient to write the expression inside the square root as

$$\left(\max_{\theta,\mathbf{a_1}} \mathcal{B}_\Omega\right)^2 = \mathbf{c}^T \begin{pmatrix} \mathrm{C}_\Omega^2 \mathrm{C}_\phi^2 T_z^2 + \mathrm{S}_\Omega^2 T_x^2 & \mathrm{C}_\Omega^2 \mathrm{C}_\phi \mathrm{S}_\phi T_z T_x \\ \mathrm{C}_\Omega^2 \mathrm{C}_\phi \mathrm{S}_\phi T_z T_x & \mathrm{C}_\Omega^2 \mathrm{S}_\phi^2 T_x^2 + \mathrm{S}_\Omega^2 T_z^2 \end{pmatrix} \mathbf{c}. \tag{140}$$

It is now obvious that the value is maximal if $\mathbf{c}$ is aligned with the eigenvector of the matrix which corresponds to the maximal eigenvalue. Therefore

$$\begin{aligned}\beta_{\max}(\boldsymbol{L}, \phi) &= \max_{\theta,\gamma,\mathbf{a_1}} \mathcal{B}_\Omega(\mathbf{L}, \phi, \boldsymbol{a}_1, \boldsymbol{b}_0, \boldsymbol{b}_1), \\ &= \sqrt{\mathrm{Eig}_+ \begin{pmatrix} \mathrm{C}_\Omega^2 \mathrm{C}_\phi^2 T_Z^2 + \mathrm{S}_\Omega^2 T_x^2 & \mathrm{C}_\Omega^2 \mathrm{C}_\phi \mathrm{S}_\phi T_z T_x \\ \mathrm{C}_\Omega^2 \mathrm{C}_\phi \mathrm{S}_\phi T_z T_x & \mathrm{C}_\Omega^2 \mathrm{S}_\phi^2 T_x^2 + \mathrm{S}_\Omega^2 T_z^2 \end{pmatrix}} \\ &= \frac{1}{\sqrt{2}} \left(\mathrm{C}_\Omega^2 (\mathrm{C}_\phi^2 T_z^2 + \mathrm{S}_\phi^2 T_x^2) + \mathrm{S}_\Omega^2 (T_z^2 + T_x^2) + \sqrt{(\mathrm{C}_\Omega^2 (\mathrm{C}_\phi^2 T_z^2 - \mathrm{S}_\phi^2 T_x^2) - \mathrm{S}_\Omega^2 (T_z^2 - T_x^2))^2 + 4 (\mathrm{C}_\Omega^2 \mathrm{C}_\phi \mathrm{S}_\phi T_z T_x)^2} \right)^{1/2}.\end{aligned} \tag{141}$$

B Numerical tool

B.1 Lipshitz continuity of von Neumann entropy

Consider two states ρ and σ on an n-dimensional Hilbert space, that are close in fidelity:

$$F(\rho, \sigma) = \mathrm{tr} \left| \sqrt{\rho} \sqrt{\sigma} \right| = f. \tag{142}$$

Given the monotonicity of arccos in the range $[0, 1]$, this condition can be equivalently written in terms of the angle $A(\rho, \sigma) = \arccos(F(\rho, \sigma))$

$$A(\rho, \sigma) = a = \arccos(f). \tag{143}$$

The angle is a metric on the space of density operators [28], in particular it satisfies the triangle inequality.

Next, note that the angle between two states is lower bounded by the angle between the ordered vectors made of their ordered eigenvalues

$$a = A(\rho, \sigma) \geq A(\mathbf{p}, \mathbf{q}) = \arccos\left(\sqrt{\mathbf{p}} \cdot \sqrt{\mathbf{q}}\right), \tag{144}$$

with $\mathbf{p} = \mathrm{Eig}^{\downarrow}(\rho)$, $\mathbf{q} = \mathrm{Eig}^{\downarrow}(\sigma)$ such that $p_1 \geq p_2 \geq \ldots$ This inequality follows from

$$F(\rho, \sigma) = \mathrm{tr} |\sqrt{\rho} \sqrt{\sigma}| = \max_U \mathrm{tr} \sqrt{\rho}\, (\sqrt{\sigma} U) \leq \sqrt{\mathbf{p}} \cdot \sqrt{\mathbf{q}}, \tag{145}$$

where in second line we used the so-called von Neumann trace inequality [40]. This bound is useful because the entropies of the states match the entropies of the probability distributions

$$H(\rho) = H(\mathbf{p}) \,, \qquad H(\sigma) = H(\mathbf{q}). \tag{146}$$

Let us now bound their difference

$$\Delta H = |H(\rho) - H(\sigma)| = |H(\mathbf{p}) - H(\mathbf{q})| \,. \tag{147}$$

To do so, note that for any two unit vectors $\sqrt{\mathbf{p}}$ and $\sqrt{\mathbf{q}}$ on the n-sphere there exist a path $\boldsymbol{\gamma}$ connecting the two and such that the integral along the path satisfies

$$\int_{\sqrt{\mathbf{p}}}^{\sqrt{\mathbf{q}}} dA = A(\mathbf{p}, \mathbf{q}) \leq a. \tag{148}$$

Let us bound the variation of the entropy along the path. To this end, we associate a probability distribution $\mathbf{r}$ to each vector $\mathbf{v}$ on the path $\boldsymbol{\gamma}$, with $r_i = (v^{(i)})^2$ (note that the vectors along the curve remain in the positive part of the n-sphere $v^{(i)} \geq 0$). A step dA from $\mathbf{v}$ along the path corresponds to some deformation of the vector given by

$$\mathbf{v}_{dA} \to \mathbf{v} + \mathbf{v}_\perp dA, \tag{149}$$

with $\mathbf{v} \cdot \mathbf{v}_\perp = 0$. To simplify the following computations we introduce the "natural" entropy

$$H_e(\rho) = -\mathrm{tr}\rho \ln(\rho) = \ln(2)\, H(\rho), \tag{150}$$

as the von Neumann entropy computed with the natural logarithm (recall that the log in $H(\rho)$ was taken in base 2). From

$$H_e(\mathbf{r}) = -\sum_i (v^{(i)})^2 \ln((v^{(i)})^2) \tag{151}$$

we compute the entropy variation for an infinitesimal increment of the angle

$$\begin{aligned} \left|\frac{dH_e}{dA}\right| &= 2|\sum_i v^{(i)} v_\perp^{(i)} (\ln((v^{(i)})^2) + 1)| \\ &= 2|\sum_i v_\perp^{(i)}\, v^{(i)} \ln((v^{(i)})^2)| \\ &= 2\,|\mathbf{v}_\perp \cdot \mathbf{w}| \leq 2||\mathbf{w}|| \end{aligned} \tag{152}$$

where we defined a vector $\mathbf{w}$ as $w_i = v^{(i)} \ln((v^{(i)})^2) = \sqrt{r_i} \ln(r_i)$. Hence we obtain

$$\left|\frac{dH_e}{dA}\right| \leq 2\sqrt{\sum_i r_i \ln^2(r_i)}, \tag{153}$$

and it remains to bound the expression on the RHS. To do so, we will construct a concave upper bound on the function

$$c(r) = r \ln^2(r) \tag{154}$$

defined on $[0, 1]$. By computing the second derivative

$$c''(r) = 2\frac{1 + \ln(r)}{r} \tag{155}$$

we see that the function is concave $c'' \leq 0$ on the interval $r \in [0, \frac{1}{e}]$, and convex $c'' \geq 0$ on the complement. To get a concave upper-bound we thus look for a line passing by $r = 1$ and $c(1) = 0$ and tangent to $c(r)$. In the (r, c)-plane the equation of a line tangent to $c(r)$ at r is given by

$$\boldsymbol{\ell}_r(\lambda) = \begin{pmatrix} r \\ c(r) \end{pmatrix} + \begin{pmatrix} 1 \\ c'(r) \end{pmatrix} \lambda. \tag{156}$$

It passes through the point $\boldsymbol{\ell}_r(\lambda) = (1, 0)$ iff

$$\begin{aligned} &\begin{cases} r + \lambda = 1 \\ c(r) + \lambda c'(r) = 0 \end{cases} \\ \implies & c(r) + (1 - r)c'(r) = 0 \\ \implies & \ln(r)(2 - 2r + \ln(r)) = 0 \\ \implies & \begin{cases} r_1 = -\frac{1}{2} W_0(-\frac{2}{e^2}) \approx 0.203 \\ r_2 = 1 \end{cases} \end{aligned}, \tag{157}$$

where W_0 is the principal branch of the Lambert W-function, and the trivial solution $r_2 = 1$ is irrelevant. Knowing r_1 we can construct a concave upper bound

$$c(r) \leq \hat{c}(r) = \begin{cases} c(r) & r \leq r_1 \\ c(r_1)\frac{1-r}{1-r_1} & r > r_1. \end{cases} \tag{158}$$

Note that $r_1 < \frac{1}{e}$. Furthermore, r_1 is the solution of the equation $2 - 2r_1 + \ln(r_1) = 0$. This allows us to simplify

$$c(r_1) = r_1 \ln^2(r_1) = 4\, r_1 (1 - r_1)^2, \tag{159}$$

and

$$\hat{c}(r) = \begin{cases} r \ln^2(r) & r \leq r_1 \\ 4\, r_1 (1 - r_1)(1 - r) & r > r_1. \end{cases} \tag{160}$$

Finally with the concave bound $\hat{c}$ it is easy to obtain

$$\begin{aligned} \sum_i r_i \ln^2(r_i) &= \sum_i c(r_i) \\ &\leq \sum_i \hat{c}(r_i) = n \sum_i \frac{1}{n} \hat{c}(r_i) \\ &\leq n\, \hat{c} \left(\sum_i \frac{r_i}{n} \right) = n\, \hat{c} \left(\frac{1}{n} \right). \end{aligned} \tag{161}$$

So for entropy susceptibility we get

$$\left| \frac{dH_e}{dA} \right| \leq 2 \sqrt{n\, \hat{c} \left(\frac{1}{n} \right)} \tag{162}$$

For $n \leq 4$, we have $r_1 < \frac{1}{n}$, so from Eq. (160) we get

$$n \leq 4 : \qquad n\, \hat{c} \left(\frac{1}{n} \right) = 4\, r_1 (1 - r_1)(n - 1). \tag{163}$$

For $n \geq 5$, we instead have $r_1 > \frac{1}{n}$, so we are in the other "part" of the function in Eq. (160) and get a simpler expression:

$$n \geq 5 : \qquad n\, \hat{c} \left(\frac{1}{n} \right) = \ln^2(n). \tag{164}$$

Finally, combining the two and recalling that $H(\rho) = \frac{H_e(\rho)}{\ln(2)}$ we get the expression

$$\boxed{\left| \frac{dH}{dA} \right| \leq \begin{cases} \frac{4\sqrt{r_1(1-r_1)}}{\ln(2)} \sqrt{n-1} & n \leq 4 \\ 2 \log(n) & n \geq 5 \end{cases}}. \tag{165}$$

For later use, we evaluate the constant for the $n = 4$ case in particular:

$$\left| \frac{dH}{dA} \right| \leq \frac{4\sqrt{r_1(1-r_1)}}{\ln(2)} \sqrt{3} < 4.023. \tag{166}$$

To bound the entropy difference for non-infinitesimal distances, we simply integrate along the curve $\boldsymbol{\gamma}$; e.g. for $n = 4$ this yields

$$\Delta H \leq \int_{\sqrt{\mathbf{p}}}^{\sqrt{\mathbf{q}}} \left| \frac{dH}{dA} \right| dA \leq 4.023\, A(\rho, \sigma). \tag{167}$$

B.2 Continuity of the goal function

The entropy term – To apply the continuity bound previously described to our situation, let ρ, ρ' be the states on $\hat{A}_0 E$ produced by measurements along angles ϕ, ϕ' on the states $|\Psi\rangle_{ABE}$ with the weight $\mathbf{L}, \mathbf{L}'$ respectively. Our aim is to bound $\left| H(\hat{A}_0|E)_\rho - H(\hat{A}_0|E)_{\rho'} \right|$. We use

$$\begin{aligned} \left| H(\hat{A}_0|E)_\rho - H(\hat{A}_0|E)_{\rho'} \right| &= \left| H(\rho_E) - H(E|\hat{A}_0)_\rho - H(\rho'_E) + H(E|\hat{A}_0)_{\rho'} \right| \\ &\leq |H(\rho_E) - H(\rho'_E)| + \left| H(E|\hat{A}_0)_\rho - H(E|\hat{A}_0)_{\rho'} \right| \end{aligned} \tag{168}$$

and bound the two last terms independently. For the first term involving $H(\rho_E)_\rho$, things are straightforward. The states of Eve $\rho_E = \mathrm{diag}(\mathbf{L})$ are 4-dimensional and independent of ϕ, so

$$|H(\rho_E)_{\mathbf{L}} + H(\rho_E)_{\mathbf{L}'}| \leq 4.023 \arccos(\sqrt{\mathbf{L}} \cdot \sqrt{\mathbf{L}'}). \tag{169}$$

For the other term, we note

$$\begin{aligned} \left| H(E|\hat{A}_0)_\rho - H(E|\hat{A}_0)_{\rho'} \right| &= \left| H(\hat{A}_0 E)_\rho - H(\hat{A}_0 E)_{\rho'} \right| \\ &= |H(\rho) - H(\rho')| \end{aligned} \tag{170}$$

as $H(\hat{A}_0) = 1$. Since $\hat{A}_0 E$ is 8-dimensional we get

$$\left| H(E|\hat{A}_0)_\rho - H(E|\hat{A}_0)_{\rho'} \right| \leq 2\log(8)\, A(\rho, \rho') = 6\, A(\rho, \rho'). \tag{171}$$

Given that $\rho = \rho(\mathbf{L}, \phi)$ and $\rho' = \rho(\mathbf{L}', \phi')$, we can use the triangle inequality to write

$$A(\rho, \rho') \leq A(\rho(\mathbf{L}, \phi), \rho(\mathbf{L}', \phi)) + A(\rho(\mathbf{L}', \phi), \rho(\mathbf{L}', \phi')). \tag{172}$$

For $A(\rho(\mathbf{L}, \phi), \rho(\mathbf{L}', \phi))$ we note that both states result from the action of the same CPTP map on two initial state $|\Psi(\mathbf{L})\rangle_{ABE}$ and $|\Psi(\mathbf{L}')\rangle_{ABE}$. By the data-processing inequality (inherited by the angle from the fidelity F) we have

$$\begin{aligned} A(\rho(\mathbf{L}, \phi), \rho(\mathbf{L}', \phi)) &\leq A(|\Psi(\mathbf{L})\rangle_{ABE}, |\Psi(\mathbf{L}')\rangle_{ABE}) \\ &= A(\mathbf{L}, \mathbf{L}') \\ &= \arccos(\sqrt{\mathbf{L}} \cdot \sqrt{\mathbf{L}'}). \end{aligned} \tag{173}$$

To bound the other term $A(\rho(\mathbf{L}', \phi), \rho(\mathbf{L}', \phi'))$ we note that if we apply a channel that performs a Z measurement followed by noisy preprocessing to the state $\left(e^{i\phi Y_A/2} \otimes \mathbb{1}_{BE}\right) |\Psi\rangle_{ABE}$, this produces exactly the state ρ on $\hat{A}_0 E$; analogously, applying the same channel to the state $\left(e^{i\phi' Y_A/2} \otimes \mathbb{1}_{BE}\right) |\Psi\rangle_{ABE}$ produces the state ρ'. Therefore the data-processing inequality implies $F(\rho, \rho')$ is lower-bounded by

$$\begin{aligned} F\left(\left(e^{i\phi Y_A/2} \otimes \mathbb{1}_{BE}\right) |\Psi\rangle, \left(e^{i\phi' Y_A/2} \otimes \mathbb{1}_{BE}\right) |\Psi\rangle\right) &= \left| \langle\Psi| \left(e^{i(\phi'-\phi) Y_A/2} \otimes \mathbb{1}_{BE}\right) |\Psi\rangle \right| \\ &= \left| \cos\frac{\phi' - \phi}{2} + i \sin\frac{\phi' - \phi}{2} \langle\Psi| (Y_A \otimes \mathbb{1}_{BE}) |\Psi\rangle \right| \\ &\geq \left| \cos\frac{\phi' - \phi}{2} \right|, \quad \text{since } \langle\Psi| (Y_A \otimes \mathbb{1}_{BE}) |\Psi\rangle \in \mathbb{R}. \end{aligned} \tag{174}$$

Putting these together, we conclude that (for $|\phi' - \phi| < \pi$)

$$A(\rho(\mathbf{L}', \phi), \rho(\mathbf{L}', \phi')) \leq \frac{|\phi' - \phi|}{2}. \tag{175}$$

Combining everything together, we get

$$\left| H(\hat{A}_0|E)_\rho - H(\hat{A}_0|E)_{\rho'} \right| \leq 10.023 \arccos(\sqrt{\mathbf{L}} \cdot \sqrt{\mathbf{L}'}) + 3\,|\phi - \phi'| \tag{176}$$

The Bell score – Next we wish to bound the increment $|d\beta_{\max}(\mathbf{L}, \mathbf{a_0}, \Omega)|$ for infinitesimal changes of the parameters $(d\mathbf{L}, d\phi)$. It is actually straightforward to bound the gradient of the Bell score before the maximization with respect to $\mathbf{a}_0, \mathbf{b}_0, \mathbf{b}_1$, so we just need to be careful to apply this bound on $\beta_{\max}$.

First, note that $\mathcal{B}_\Omega(\mathbf{L}, \phi, \mathbf{a}_1, \mathbf{b}_0, \mathbf{b}_1)$ is a positive smooth infinitely differential function of all its parameters. For a fixed Ω, let us group these parameters in two vectors $\mathbf{x} = (\mathbf{a_1}, \mathbf{b_0}, \mathbf{b_1})$ and $\mathbf{y} = (T_z, T_x, \mathbf{a_0})$. We then formally define

$$\begin{aligned} f(\mathbf{x}, \mathbf{y}) &= \mathcal{B}_\Omega(\mathbf{L}, \phi, \mathbf{a}_1, \mathbf{b}_0, \mathbf{b}_1) \\ g(\mathbf{y}) &= \max_{\mathbf{x}} f(\mathbf{x}, \mathbf{y}) = \beta_{\max}(\mathbf{L}, \mathbf{a_0}, \Omega). \end{aligned} \tag{177}$$

We are interested in bounding $|dg(\mathbf{y})|$ as a function of $d\mathbf{y}$. Consider two values of the parameter, $\mathbf{y}_1$ and $\mathbf{y_2}$, and define

$$\begin{aligned} \bar{\mathbf{x}}_1 &= \text{argmax}_{\mathbf{x}} f(\mathbf{x}, \mathbf{y}_1) \\ \bar{\mathbf{x}}_2 &= \text{argmax}_{\mathbf{x}} f(\mathbf{x}, \mathbf{y}_2), \end{aligned} \tag{178}$$

such that $g(\mathbf{y}_1) = f(\bar{\mathbf{x}}_1, \mathbf{y}_1)$ and $g(\mathbf{y}_2) = f(\bar{\mathbf{x}}_2, \mathbf{y}_2)$. Without loss of generality we assume $g(\mathbf{y}_1) \geq g(\mathbf{y}_2)$ and consider the difference

$$\begin{aligned} |g(\mathbf{y_1}) - g(\mathbf{y_2})| &= |f(\bar{\mathbf{x}}_1, \mathbf{y_1}) - f(\bar{\mathbf{x}}_2, \mathbf{y_2})| \\ &\leq |f(\bar{\mathbf{x}}_1, \mathbf{y_1}) - f(\bar{\mathbf{x}}_1, \mathbf{y_2})| \\ &\leq \max_{\mathbf{x}} |f(\mathbf{x}, \mathbf{y_1}) - f(\mathbf{x}, \mathbf{y_2})| \end{aligned} \tag{179}$$

Taking the limit $\mathbf{y_2} \to \mathbf{y}_1$ we get

$$|dg(\mathbf{y})| \leq \max_{\mathbf{x}} |\nabla_{\mathbf{y}} \mathbf{f}(\mathbf{x}, \mathbf{y}) \cdot \mathbf{dy}|. \tag{180}$$

Using the expression (67) for $\mathcal{B}_\Omega(\mathbf{L}, \phi, \mathbf{a}_1, \mathbf{b}_0, \mathbf{b}_1)$ we then get

$$|d\beta_{\max}(\mathbf{L}, \phi)| \leq \begin{pmatrix} 1 \\ 1 \\ \mathrm{C}_\Omega \end{pmatrix} \cdot \begin{pmatrix} |dT_z| \\ |dT_x| \\ |d\phi| \end{pmatrix}. \tag{181}$$

B.3 Gradient of the goal function

We will now combine all the elements to upper bound the gradient of the goal function

$$G(\mathbf{L}, \phi; \Omega, q) = H(\rho_E) - H(E|\hat{a}_0(q)) + t\beta_{\max}(\mathbf{L}, \phi). \tag{182}$$

We parametrize the vector $\mathbf{L}$ with the help of the angles as in Eq. (45), such that the "model" is described by four angles

$$(\mathbf{L}, \phi) \simeq \boldsymbol{\omega} = (\alpha, \mu, \xi, \phi). \tag{183}$$

We will bound the gradient of the goal function with respect to this parametrization.

We start with the gradient of the angle. It satisfies

$$dA = |A(\mathbf{L}(\boldsymbol{\omega}), \mathbf{L}(\boldsymbol{\omega} + \mathbf{n}d\omega))| \leq |\nabla A(\boldsymbol{\omega})| d\omega, \tag{184}$$

with a unit vector $\mathbf{n} = (n_\alpha, n_\mu, n_\xi, 0)$. For the fidelity one finds

$$\begin{aligned} F(\mathbf{L}(\boldsymbol{\omega}), \mathbf{L}(\boldsymbol{\omega} + \mathbf{n}d\omega)) &= \sqrt{\mathbf{L}(\boldsymbol{\omega})} \cdot \sqrt{\mathbf{L}(\boldsymbol{\omega} + \mathbf{d\omega_i})} \\ &\geq 1 - \frac{3}{4} d\omega^2 + O(d\omega^3) \end{aligned} \tag{185}$$

for $d\omega_i = d\alpha, d\mu$ or $d\xi$, one easily finds

$$|\nabla A(\boldsymbol{\omega})| \leq \sqrt{\frac{3}{2}}. \tag{186}$$

We thus get from Eq. (176)

$$|d(H(\rho_E) - H(E|\hat{a}_0(q)))| \leq 10.023 \sqrt{\frac{3}{2}} \sqrt{d\alpha^2 + d\mu^2 + d\xi^2} + 3d\phi \tag{187}$$

and

$$|\nabla(H(\rho_E) - H(E|\hat{a}_0(q))| \leq \sqrt{10.023^2 \frac{3}{2} + 9} < 12.7 \tag{188}$$

For the gradient of the Bell score contribution $|\nabla \beta_{\max}(\mathbf{L}, \phi)|$ we note that

$$|dT_z|, |dT_x| \leq 2\Big(|d\alpha| + |d\mu| + |d\xi|\Big), \tag{189}$$

which implies form (181) that

$$|\nabla \beta_{\max}(\mathbf{L}, \phi)| \leq t\sqrt{3 \times 4^2 + \mathrm{C}_\Omega^2} \leq 7t \tag{190}$$

Finally, for the goal function

$$\boxed{|\nabla G| \leq 12.7 + 7\,t}. \tag{191}$$

B.4 Lipschitz function certified maximization on a compact space

General approach – In this section section we explain how we obtain a certified maximum of a Lipschitz function $f : \mathbb{R}^n \to \mathbb{R}$ with a Lipschitz constant Λ, i.e. a bounded gradient $|\nabla f| \leq \Lambda$, on a closed domain

$$\mathcal{D} = \{x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n \mid x_i \in [\tau_i, \mu_i],\ \forall\, i\}. \tag{192}$$

We start by meshing $\mathcal{D}$ into an hypercube grid graph $G(s)$ with element of size s. If possible, we take s so that s evenly divides $\mu_i - \tau_i$ for all i. We label the center of each hypercube $\vec{c}$ so that each first neighbor in a given direction is separated by s, e.g. for $\vec{c}$ and its neighbor $\vec{c'}$ in the direction $+\vec{e_1}$

$$\vec{c'} = \begin{pmatrix} c'_1 \\ c'_2 \\ \vdots \\ c'_n \end{pmatrix} = \vec{c} + s.\vec{e_1} = \begin{pmatrix} c_1 + s \\ c'_2 \\ \vdots \\ c'_n \end{pmatrix}. \tag{193}$$

A hypercube of center $\vec{c}$, $h(\vec{c})$, element of G, is thus defined as

$$h(\vec{c}) = \{x \in \mathbb{R}^n | c_i - \frac{s}{2} \leq x_i \leq c_i + \frac{s}{2},\ \forall i \in \{1, \ldots, n\}\}. \tag{194}$$

Given the Lipschitz constant Λ, the function f in a given hypercube $h(\vec{c})$ is upper bounded by

$$f(x) \leq f(\vec{c}) + \frac{\sqrt{n}\Lambda}{2} s, \quad \forall x \in h(\vec{c}). \tag{195}$$

Trivially, an upper bound on the maximum of f over $\mathcal{D}$ is given by,

$$\max_{x \in \mathcal{D}} f(x) \leq \max_{\vec{c} \in G(s)} f(\vec{c}) + \frac{\sqrt{n}\Lambda}{2} s. \tag{196}$$

The maximum of f over $\mathcal{D}$ can thus be obtained by taking the smallest possible step, i.e.

$$\max_{x \in \mathcal{D}} f(x) = \lim_{s \to 0} \left(\max_{\vec{c} \in G(s)} \left(f(\vec{c}) + \frac{\sqrt{n}\Lambda}{2} s \right) \right). \tag{197}$$

Numerical realisation – While Eq. (197) gives the optimal maximum on f, it is however impracticable using numerical resources, due to the obvious need of discretization. A first naive approach is to relax the problem by setting a lower bound on s. This is, with the lower bound $s \geq \varepsilon$,

$$\max_{x \in \mathcal{D}} f(x) \leq \lim_{s \to \varepsilon} \left(\max_{\vec{c} \in G(s)} \left(f(\vec{c}) + \frac{\sqrt{n}\Lambda}{2} s \right) \right). \tag{198}$$

Resource wise, this method is cumbersome. Indeed, setting ε to a small value compared to the domain space, i.e. $\varepsilon \ll \min_i(\tau_i - \mu_i)$, will result in a high number of hypercubes to explore. Furthermore, for a given step s, the number of hypercubes scales exponentially with the dimension n.

Speed-up using a guess on the maximum – Providing a guess on the maximum of f may significantly speed up the previous method. Such a maximum can be found using an optimization algorithm without guarantees of optimality (BFGS, CMA, and others...). Denote such a maximum as ν.
We start by setting a not-too-small step, s_0, so that the number of hypercubes composing the grid graph, $G_0(s_0)$, is reasonnable. For each hypercube $h_0(\vec{c})$ we start by computing the potential maximum,

$$\xi^0(\vec{c}) = f(\vec{c}) + \frac{\sqrt{n}\Lambda}{2} s_0. \tag{199}$$

We then compare this value to ν. In the case where $\nu > \xi^0(\vec{c})$, we pass to the next hypercube since the guessed maximum is higher than the potential maximum value of f in $h_0(\vec{c})$. Otherwise, we mesh $h_0(\vec{c})$ into a new hypercube grid graph $G_1(s_1)$ of element of size $s_1 = s_0/2$. For all of the new generated hypercubes, $h_1(\vec{c}) \in G_1(s_1)$, we compute the potential maximum $\xi^1(\vec{c})$ using Eq. (199). This method is applied recursively until either all new hypercubes of graph G_m^k satisfy $\nu > h_m(\vec{c})$, or we reach the minimum step $s_m \leq \varepsilon$. An upper bound of f is thus given by the maximum $\xi^m(\vec{c})$

$$\max(\xi^m(\vec{c})) = f(\vec{c}) + \frac{\sqrt{n}\Lambda}{2} s_m \tag{200}$$

where $s_m = s_0/2^m$.