arXiv:2209.12828v2 [quant-ph] 12 Apr 2023

Boosting device-independent cryptography with tripartite nonlocality

Federico Grasselli, Gláucia Murta, Hermann Kampermann, and Dagmar Bruß

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany

Device-independent (DI) protocols, such as DI conference key agreement (DICKA) and DI randomness expansion (DIRE), certify private randomness by observing nonlocal correlations when two or more parties test a Bell inequality. While most DI protocols are restricted to bipartite Bell tests, harnessing multipartite nonlocal correlations may lead to better performance. Here, we consider tripartite DICKA and DIRE protocols based on testing multipartite Bell inequalities, specifically: the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequality, and the Holz and the Parity-CHSH inequalities introduced in the context of DICKA protocols. We evaluate the asymptotic performance of the DICKA (DIRE) protocols in terms of their conference key rate (net randomness generation rate), by deriving lower bounds on the conditional von Neumann entropy of one party's outcome and two parties' outcomes. For the Holz inequality, we prove a tight analytical lower bound on the one-outcome entropy and conjecture a tight lower bound on the two-outcome entropy. We additionally re-derive the analytical one-outcome entropy bound for the MABK inequality with a much simpler method and obtain a numerical lower bound on the two-outcome entropy for the Parity-CHSH inequality. Our simulations show that DICKA and DIRE protocols employing tripartite Bell inequalities can significantly outperform their bipartite counterparts. Moreover, we establish that genuine multipartite entanglement is not a precondition for multipartite DIRE while its necessity for DICKA remains an open question.

1 Background

The security of practical quantum cryptographic protocols [1, 2] holds as far as the theoretical model of the quantum devices used in the protocol accurately describes their experimental implementation. Indeed, any small deviation from the ideal functionality of a quantum device can be exploited by an eavesdropper to breach the security of the protocol, as demonstrated by several quantum hacking attacks [2–4].

This leaves the user(s) with only two possibilities to ensure that their quantum cryptographic protocol is actually secure. They can either thoroughly characterize the devices being used, verifying that every assumption on the device is met in practice. However, this procedure might be challenging and beyond the capabilities of an end user. The other possibility is represented by device-independent (DI) cryptography, whose security is guaranteed independently of the inner workings of the employed devices [5–7].

The typical setting of a DI protocol is the Bell scenario [8]. Here, two (or more) parties hold uncharacterized devices, treated as "black boxes". Each party can interact with their device by selecting an input, which prompts the device to return an output. In a quantum realization of the DI protocol, the device corresponds to a quantum system and the party interacts with it by choosing a measurement setting (input) and collecting the measurement outcome (output). By repeating this procedure a sufficient number of times and by revealing a fraction of their input-output pairs, the parties can characterize the probability distribution of the outputs, given the inputs.

To each Bell scenario can be associated a correlation inequality, called Bell inequality [9]. If the distribution of the outputs observed by the parties violates a Bell inequality, the outputs are said to be nonlocally correlated. This occurs, e.g., if the parties perform appropriate measurements on their share of an entangled state in a loophole-free[1] Bell experiment [10, 11].

The intuition behind the security principle of DI protocols is that an eavesdropper cannot have full information on the parties' outputs if they are nonlocally correlated, regardless of the physical implementation of the devices. In fact, if the eavesdropper held a classical variable fully predicting the parties' outputs, that would represent a local explanation of the observed correlations [12]. Therefore, the nonlocality of the outcomes, certified in a device-independent manner by the violation of a Bell inequality, can be used to infer randomness and secrecy with respect to an eavesdropper. In particular, by observing nonlo-

Federico Grasselli: federico.grasselli@hhu.de

[1] Note that, since we assume quantum mechanics to hold, the Bell experiment does not need to close the locality loophole, as far as the parties' devices are isolated.

cality in the outcomes, DI quantum key distribution (DIQKD) [12–16] and its multiparty generalization, DI conference key agreement (DICKA) [17–21], enable a set of parties to share a common secret key, while DI randomness expansion (DIRE) [22–28] expands the initial share of private randomness of one or more parties.

In order to benchmark DI protocols based on different Bell scenarios and Bell inequalities, one needs to quantify the minimum amount of secret randomness in the parties' outcomes, for a given Bell violation. The figure of merit is the conditional von Neumann entropy of the parties' outcomes, given the eavesdropper's quantum side information, up to corrections due to finite-size effects. Indeed, the conditional von Neumann entropy of a set of outcomes determines the rate of secret bits generated by DIRE, DIQKD and DICKA protocols.

Although any lower bound on this quantity is also a valid measure of secret randomness, tighter bounds imply higher secret bit generation rates and hence more efficient and robust DI protocols. This is particularly important since today's quantum technology is mature enough to enable the experimental implementation of DI protocols, as testified by recent DIRE [29, 30] and DIQKD experiments [31–33].

The derivation of tight bounds on the conditional von Neumann entropies relevant for the security of DI protocols has been a major theoretical challenge in the field of DI cryptography. In the bipartite DI scenario, tight analytical bounds on one-outcome entropies [13] were derived for the CHSH inequality [34] and its variants [35–37]. Recently, two-outcome entropy bounds were investigated in [38] for the CHSH inequality. In parallel, reliable numerical lower bounds on the conditional von Neumann entropy can be obtained with the techniques developed in [39–41].

2 Summary of results

In this work we consider a tripartite DI scenario where three unknown quantum systems are individually measured by Alice, Bob and Charlie, respectively. Every party can perform one of two measurements, labelled by inputs 0 and 1, each of which yields a binary outcome, either 0 or 1. The two measurements are: A_0 and A_1 for Alice, B_0 and B_1 for Bob and C_0 and C_1 for Charlie. In this scenario, the parties can either test a tripartite Bell inequality or a bipartite Bell inequality, in which case one of the parties remains idle.

For brevity of notation, we define: $B_\pm := (B_0 \pm B_1)/2$ and $C_\pm := (C_0 \pm C_1)/2$, while $\overset{L}{\leq}$ ($\overset{Q}{\leq}$) indicates the local (quantum) bound. Moreover, $\langle A_x B_y C_z \rangle$ represents the correlation function:

$$\sum_{a,b,c} (-1)^{a+b+c} \Pr[A_x = a, B_y = b, C_z = c], \tag{1}$$

and similarly for the two-party correlators. The Bell inequalities considered in this work are the following:

- The tripartite *Holz inequality* [19],

$$\begin{aligned}\beta_{\mathrm{H}} =& \langle A_1 B_+ C_+ \rangle - \langle A_0 B_- \rangle \\ &- \langle A_0 C_- \rangle - \langle B_- C_- \rangle \overset{L}{\leq} 1 \overset{Q}{\leq} 3/2.\end{aligned} \tag{2}$$

- The tripartite *Parity-CHSH inequality* [20],

$$\beta_{\mathrm{pC}} = \langle A_1 B_- C_0 \rangle + \langle A_0 B_+ \rangle \overset{L}{\leq} 1 \overset{Q}{\leq} \sqrt{2}. \tag{3}$$

- The tripartite *Mermin-Ardehali-Belinskii-Klyshko (MABK) inequality* [42–44],

$$\begin{aligned}\beta_{\mathrm{M}} =& \langle A_0 B_0 C_1 \rangle + \langle A_0 B_1 C_0 \rangle \\ &+ \langle A_1 B_0 C_0 \rangle - \langle A_1 B_1 C_1 \rangle \overset{L}{\leq} 2 \overset{Q}{\leq} 4.\end{aligned} \tag{4}$$

- The bipartite family of *asymmetric Clauser-Horne-Shimony-Holt (CHSH) inequalities* [35, 45], parametrized by $\alpha \in \mathbb{R}$,

$$\begin{aligned}\beta_{\alpha\mathrm{C}} &= 2\alpha \langle A_0 B_+ \rangle + 2 \langle A_1 B_- \rangle \\ &\overset{L}{\leq} \begin{cases} 2|\alpha| & \text{if } |\alpha| > 1 \\ 2 & \text{if } |\alpha| \leq 1 \end{cases} \\ &\overset{Q}{\leq} 2\sqrt{1+\alpha^2}.\end{aligned} \tag{5}$$

The goal of our work is to benchmark the performance of DICKA and DIRE protocols based on the above Bell inequalities and determine which Bell inequality is optimal for each cryptographic task.

The crucial ingredient for our comparison is the derivation of tight analytical and numerical lower bounds on one-outcome conditional entropies, $H(A_0|E)$, and two-outcome conditional entropies, $H(A_0B_0|E)$, as a function of the violation of the considered Bell inequality. Indeed, the entropy $H(A_0|E)$ determines the conference key rate of DICKA protocols, while the two-outcome entropy $H(A_0B_0|E)$ determines the net randomness generation rate of our DIRE protocols.

In order to have a fair comparison, we provide the parties with an equivalent entanglement resource in each Bell scenario, which is chosen to be a noisy version of the entangled state which maximally violates each of the Bell inequalities. The parties then perform the measurements that would lead, in the absence of noise, to maximal Bell violation. In particular, when the parties test the Holz, Parity-CHSH and MABK inequality, they share a locally-depolarized GHZ state:

$$\rho^{(3)} = \mathcal{D}^{\otimes 3}(|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|), \tag{6}$$

where the map $\mathcal{D}$ acts on every qubit as follows:

$$\mathcal{D}(\sigma) = p\sigma + \frac{1-p}{2}\mathbb{1}, \tag{7}$$

and where $|\mathrm{GHZ}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$ is the GHZ state. Conversely, when the parties test the (bipartite) asymmetric CHSH inequalities, they share the bipartite version of the GHZ state, namely the Bell state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, also subjected to local depolarization:

$$\rho^{(2)} = \mathcal{D}^{\otimes 2}(|\Phi^+\rangle\langle\Phi^+|). \tag{8}$$

The noise parameter, p, is linked to the probability that each qubit is depolarized[2], given by $1-p$. We also study the case in which the ideal GHZ and Bell states are globally depolarized:

$$\rho^{(3)} = p|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}| + (1-p)\frac{\mathbb{1}}{8}, \tag{9}$$

for three parties testing a tripartite Bell inequality and

$$\rho^{(2)} = p|\Phi^+\rangle\langle\Phi^+| + (1-p)\frac{\mathbb{1}}{4}, \tag{10}$$

for two parties testing a bipartite Bell inequality. In this case, $1-p$ is the probability that the three-qubit (two-qubit) state is depolarized. Further details on the optimal measurement settings of each inequality are given in Appendix A.

We compare the performance of DICKA protocols based on the inequalities (2), (3) and (5), by computing their asymptotic conference key rates for the two noise models outlined above. Similarly, we compare DIRE protocols based on each of the four Bell inequalities (for the bipartite Bell inequality we set $\alpha = 1$, which recovers the CHSH inequality) in terms of their asymptotic net randomness generation rate, when the randomness is extracted from the outcomes of two parties.

For both DICKA and DIRE protocols, we observe that tripartite Bell inequalities can provide a performance advantage over the family of bipartite Bell inequalities in (5), which are currently regarded as being optimal for DI tasks such as DIQKD [35, 37].

The performance comparisons are enabled by bounds on the conditional von Neumann entropy. The derivation of conditional entropy bounds in the multipartite scenario was first addressed in [46] and then more thoroughly in [47], where one-outcome and two-outcome entropy bounds were derived for the MABK inequality, a full-correlator Bell inequality [42–44].

In this work, we take a significant step further and provide tight analytical entropy bounds as a function of the violation of the Holz inequality. More precisely, we derive a tight analytical bound for the one-outcome entropy $H(A_0|E)$ (see Theorem 1) and provide an analytical conjecture of the tight bound for the two-outcome entropy $H(A_0B_0|E)$ (Conjecture 1), which is robustly confirmed by numerical data. To the best of our knowledge, our bound on $H(A_0|E)$ is the first tight analytical bound derived for a non-full-correlator Bell inequality, like the Holz inequality. And our conjectured bound on $H(A_0B_0|E)$ is the first multi-outcome analytical bound for a non-full-correlator Bell inequality.

The derivation of the analytical bound on $H(A_0|E)$ for the tripartite Holz inequality builds on an entropic uncertainty relation, similarly to the approach used in [35, 36] for the CHSH inequality. However, the increased number of parties and the asymmetry with respect to permutations of parties makes our derivation highly non-trivial. We report the full proof of the bound and of its tightness in Appendix B. By following the same approach, in Appendix C we rederive the analytical bound on $H(A_0|E)$ for the MABK inequality with a proof that is considerably simpler than the derivation in [47]. Besides, in Appendix E we prove that the analytical lower bound on $H(A_0|E)$ for the Parity-CHSH inequality, originally derived in [20], is actually tight.

We additionally compute numerical bounds on the two-outcome entropy $H(A_0B_0|E)$ for the Parity-CHSH and CHSH inequalities, which are used to compute the corresponding DIRE rates. A detailed calculation of the bounds is provided in Appendix D. The numerical bound for the Parity-CHSH inequality is a new result, while the one for the CHSH inequality has been independently derived in [38].

The remainder of the paper is structured as follows. In Sec. 3 we present our analytical and numerical entropy bounds. In Sec. 4 we apply our bounds to DICKA protocols and compare their performance to deduce which Bell inequality is optimal. In Sec. 5 we perform an analogous comparison for DIRE protocols. We discuss our results and conclude in Sec. 6, where Table 3 provides an overview of all the considered entropy bounds. The analytical and numerical calculations of the entropy bounds are presented in Appendices B to E, while in Appendix A we summarize the Bell inequalities and their entropy bounds.

3 One-outcome and two-outcome entropy bounds

In this section, we present our analytical bounds on the conditional von Neumann entropy when the parties test the Holz inequality. Additionally, we compare the analytical and numerical bounds derived in this work with other bounds, when the parties test the inequalities (2)-(5). The bounds are then used to compute DICKA and DIRE rates, respectively, in Sec. 4 and 5.

[2] The effect of photon loss would be modelled similarly to local depolarization (7), as: $\mathcal{L}(\sigma) = p\sigma + (1-p)|vac\rangle\langle vac|$, where $|vac\rangle$ is the vacuum. Since the detection loophole forbids discarding no-detection events, assigning a random measurement outcome when a photon is lost would have the same effect of local depolarization (7). Hence, in our simulations $1-p$ can also be seen as the probability that a photon is lost.

3.1 Single party's outcome

We obtain a tight analytical lower bound on the conditional entropy of Alice's outcome A_0, when Alice, Bob and Charlie test the Holz inequality (2).

Theorem 1. *Let Alice, Bob and Charlie test the Holz inequality [19] and let β_{H} be the expected Bell value. Then, the von Neumann entropy of Alice's outcome A_0 conditioned on Eve's information E satisfies*

$$H(A_0|E) \geq 1 - h\left[\frac{1}{4}\left(\beta_{\mathrm{H}} + 1 + \sqrt{\beta_{\mathrm{H}}^2 + 2\beta_{\mathrm{H}} - 3}\right)\right], \tag{11}$$

where $h(x) = -x\log_2 x + (1-x)\log_2(1-x)$ is the binary entropy. Moreover, the bound is tight. That is, for every Bell value β_{H} there exists a quantum strategy (state and measurements) which attains that Bell value and whose conditional entropy is given by the r.h.s. of (11).

Here we provide a sketch of the proof of Theorem 1, a detailed proof is presented in Appendix B.

Proof sketch. First, we employ Jordan's Lemma [47, 48] to simplify the problem at hand, without loss of generality. In particular, we show that we can focus on deriving a convex lower bound on $H(A_0|E)$ when Alice, Bob and Charlie share a three-qubit state and perform rank-one binary projective measurements on their respective qubits.

We identify the plane induced by the qubit observables of each party to be the (x, z) plane of the Bloch sphere. Then, we choose the local reference frames such that the Bell value (2) is simplified and Alice's measurement A_0 corresponds to the Pauli measurement σ_z: $A_0 = Z$. With these choices, we show that the three-qubit state ρ_{ABC} shared by the parties can be assumed to be block-diagonal in the GHZ basis, without loss of generality. We are thus left to derive a lower bound on $H(Z|E)$.

The next step is to employ the uncertainty relation for von Neumann entropies [49] in combination with other properties of the conditional von Neumann entropy to obtain the lower bound:

$$H(Z|E) \geq 1 - h\left(\frac{1 + |\langle XXX\rangle|}{2}\right), \tag{12}$$

where $\langle XXX\rangle$ is the expectation value of a σ_x measurement performed by all parties. Note that a similar step to the one above is employed in [35] to derive an entropy bound when two parties test the asymmetric CHSH inequality.

The last decisive step of our proof lies in the ability to link the expectation value $\langle XXX\rangle$ to the Bell value β_H. We show that they can be related by the following non-linear inequality:

$$|\langle XXX\rangle| \geq \frac{\beta_{\mathrm{H}}}{2} - \frac{1}{2} + \frac{1}{2}\sqrt{\beta_{\mathrm{H}}^2 + 2\beta_{\mathrm{H}} - 3}. \tag{13}$$

By combining (13) with (12) and with the fact that $h(1/2 + x)$ is monotonically decreasing for $x > 0$, we obtain the result in (11). □

The Holz inequality was introduced in [19] as a multipartite generalization of the CHSH inequality (i.e., all the parties have two inputs and two outputs) and its construction was tailored for DICKA protocols. In Sec. 4, we employ the tight entropy bound we derived in Theorem 1 to show that the Holz inequality indeed leads to DICKA protocols with the currently best-known performance.

Besides, the technique used to derive the entropy bound of Theorem 1 can constitute a simpler alternative to the approach used in [47], as demonstrated by our re-derivation of the single-outcome entropy bound for the MABK inequality from [47]. We provide the details of the derivation in Appendix C.

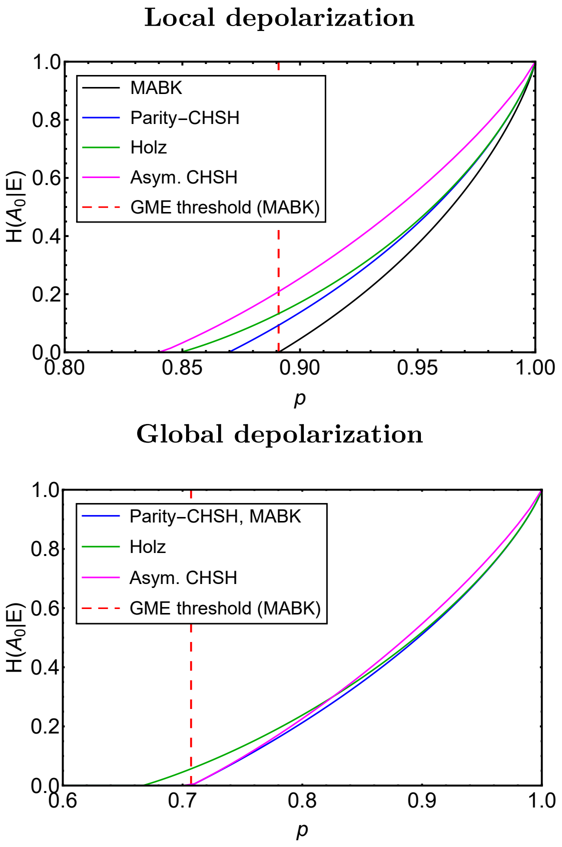

Figure 1: Analytical lower bounds on the conditional entropy $H(A_0|E)$ of Alice's outcome A_0 for various Bell inequalities, when three (two) parties are given a GHZ (Bell) state that has been locally and globally depolarized with probability $1 - p$. The bound for the Holz inequality is derived in Theorem 1, while the bounds for the Parity-CHSH, the asymmetric CHSH, and the MABK inequality are taken from [20], [35], and [47] (and re-derived in Appendix C), respectively. All bounds are reported in Appendix A.

In Fig. 1 we compare the lower bound on $H(A_0|E)$ derived in Theorem 1 for the Holz inequality with analogous bounds for the Parity-CHSH and asymmetric CHSH inequality from Refs. [20, 35], and the bound for the MABK inequality from [47] re-derived in Appendix C. Note that all the bounds are tight (we prove the tightness of the Parity-CHSH bound in Appendix E), except for the case of the MABK inequality, and that we maximize the bound for the asymmetric CHSH inequality (5) over the parameter α. We plot the entropy bounds as a function of the depolarization parameter p, where $1-p$ is the probability of local or global depolarization (see Sec. 2). From the plot with local depolarization we observe that, for a fixed value of p, the largest entropy is certified by the bipartite asymmetric CHSH inequality, while the Holz inequality provides the largest bound among the tripartite inequalities. This is expected, since for local noise the Bell violation is proportional to $\sim p^N$, where N is the number of parties testing the inequality. Hence, the violation decreases for increasing number of parties and fixed noise and so does the entropy bound. This fact does not necessarily hold with other noise models, e.g. global depolarization, where the Holz inequality leads to the largest entropy at high noise levels (low p).

Interestingly, the entropy bounds for the Holz and the Parity-CHSH inequality in Fig. 1 are non-zero below the genuine multipartite entanglement (GME) threshold of the MABK inequality. This suggests that GME might not be necessary to certify the privacy of a single party's outcome when testing multipartite Bell inequalities. Indeed, this is the case for asymmetric Bell inequalities like the Holz and the Parity-CHSH inequality studied here, while a previous study [47] on the permutationally-invariant MABK inequality showed that GME is necessary to extract private randomness from a party's outcome.

It is straightforward to find a non-GME state that leads to non-zero entropy in the case of the Parity-CHSH inequality, where Charlie's role is trivial. Indeed, depending on the outcome of Charlie's only measurement C_0, Alice and Bob are effectively testing two distinct CHSH inequalities, one for outcome $C_0 = 0$ and another for outcome $C_0 = 1$. Therefore, one could easily obtain the maximal violation of such inequality by distributing the biseparable state: $|\Phi^+\rangle \otimes |0\rangle$ and selecting the optimal CHSH measurements for Alice and Bob and setting Charlie's measurement to be Z. Because the Parity-CHSH inequality can be seen as a special case of the Holz inequality where Charlie's measurements coincide ($C_0 = C_1$), we can obtain non-zero entropy with non-GME states also for the Holz inequality by choosing the same setup as above, up to some change of sign.

3.2 Two parties' outcomes

In this section we compare lower bounds on the joint conditional entropy $H(A_0B_0|E)$ of Alice's outcome A_0 and Bob's outcome B_0 when the parties test the inequalities (2)-(5) (we set $\alpha = 1$ in the asymmetric CHSH inequality, which reduces it to the standard CHSH inequality), in view of their application for DIRE.

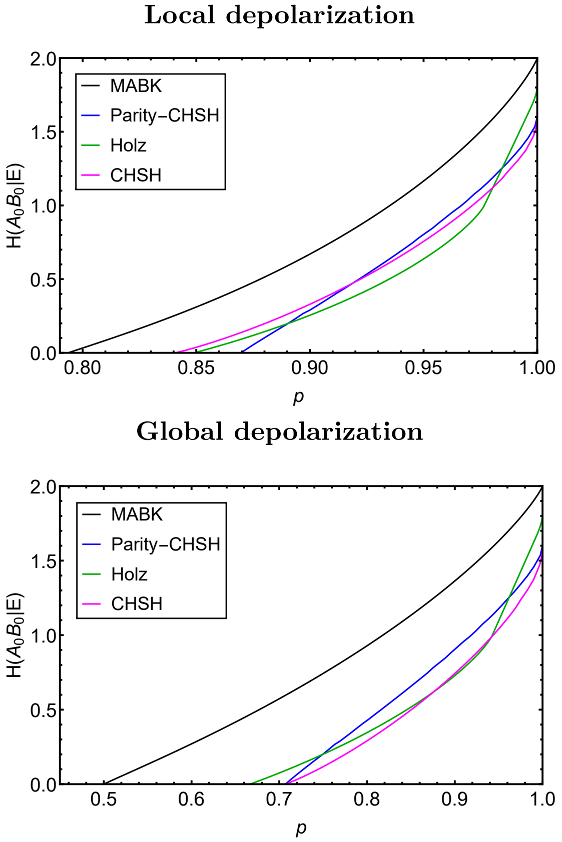

Figure 2: Lower bounds on the conditional entropy $H(A_0B_0|E)$ of Alice's and Bob's outcomes for various Bell inequalities, when three (two) parties are given a GHZ (Bell) state that has been locally and globally depolarized with probability $1-p$. The bound for the MABK inequality is analytical and was obtained in [47], the bound for the Holz inequality is a conjectured tight analytical expression given by (14), while the bounds for the Parity-CHSH and CHSH inequality are numerical (see Appendix D).

The entropy bound when three parties test the MABK inequality (4) is analytical and was derived in [47]; we report it in Appendix A. Conversely, the entropy bounds for the Parity-CHSH, CHSH and Holz inequality are novel numerical bounds obtained by directly minimizing the entropy over all states and measurements yielding a given Bell violation. In order to achieve this, we significantly simplify the optimization problem for each inequality (details in Appendix D) before carrying out the numerical computation.

In particular, the numerical bound on $H(A_0B_0|E)$ for the Holz inequality relies on the intermediate results used to derive Theorem 1, which allow us to simplify the optimization problem by reducing the number of variables. As a result, we optimize over just one measurement direction, i.e. one angle, and over block-diagonal states. This simplification also allowed us to conjecture the form of the corresponding analytical bound (14).

Conjecture 1. *Let Alice, Bob and Charlie test the Holz inequality [19] and let β_{H} be the expected Bell value. Then, the joint von Neumann entropy of Alice's outcome A_0 and Bob's outcome B_0, conditioned on Eve's information E, satisfies*

$$H(A_0B_0|E) \geq \begin{cases} \eta(\beta_{\mathrm{H}}) & \beta_{\mathrm{H}} \in [1,\sqrt{2}] \\ \dfrac{\theta(\beta_{\mathrm{H}}^*, x(\beta_{\mathrm{H}}^*)) - 1}{\beta_{\mathrm{H}}^* - \sqrt{2}}(\beta_{\mathrm{H}} - \sqrt{2}) + 1 & \beta_{\mathrm{H}} \in (\sqrt{2}, \beta_{\mathrm{H}}^*] \\ \theta(\beta_{\mathrm{H}}, x(\beta_{\mathrm{H}})) & \beta_{\mathrm{H}} \in (\beta_{\mathrm{H}}^*, 3/2], \end{cases} \tag{14}$$

where the functions η, θ and x, and the parameter β_{H}^*, are reported in Appendix A. Moreover, the bound is tight.

The bound on $H(A_0B_0|E)$ when three parties test the Parity-CHSH inequality is also obtained by direct numerical optimization, similarly to the bound for the Holz inequality. As a matter of fact, note that the Parity-CHSH inequality (3) is a particular case (upon relabeling the observables) of the Holz inequality (2) when Charlie's two measurements coincide, i.e. $C_0 = C_1$, or equivalently $C_- = 0$.

For the numerical computation of the entropy bound when two parties test the CHSH inequality, we apply the results of [13, 47] to the CHSH scenario and parametrize the state shared by Alice and Bob as a Bell-diagonal state. We remark that the same bound has been independently computed in [38] with numerical techniques. The details on the optimization problem solved for each numerical bound are given in Appendix D.

It is important to remark that the numerical curves obtained by directly minimizing the entropy cannot be treated as reliable lower bounds, as the numerical optimization is non-convex and may return local minima. Nevertheless, we believe that our optimizations are very close to the corresponding tight lower bounds.

In Fig. 2 we plot the bounds on $H(A_0B_0|E)$ as a function of the depolarization parameter p, in the cases of local and global depolarization. We observe that three parties testing the MABK inequality can certify a considerably higher amount of randomness for Alice's and Bob's outcomes, compared to testing the other inequalities, both for locally and globally depolarized states.

In Fig. 3 we plot the analytical conjecture (14) and the corresponding numerical bound on $H(A_0B_0|E)$ for the Holz inequality. We observe that the bound presents a distinct behavior for $\beta_{\mathrm{H}} \leq \sqrt{2}$ and $\beta_{\mathrm{H}} > \sqrt{2}$, represented by two distinct functions $\eta(\beta_{\mathrm{H}})$ and $\theta(\beta_{\mathrm{H}}, x(\beta_{\mathrm{H}}))$ in (14). Interestingly, the boundary of the two regions ($\beta_{\mathrm{H}} = \sqrt{2}$) coincides with the GME threshold [19] above which the Holz inequality certifies genuine multipartite entanglement shared by the three parties. For smaller violations, the inequality cannot certify genuine multipartite entanglement and the entropy is bounded by: $H(A_0B_0|E) \leq \eta(\sqrt{2}) = 1$, while for larger violations the entropy increases rapidly and eventually surpasses the other entropy bounds, except for MABK (see Fig. 2).

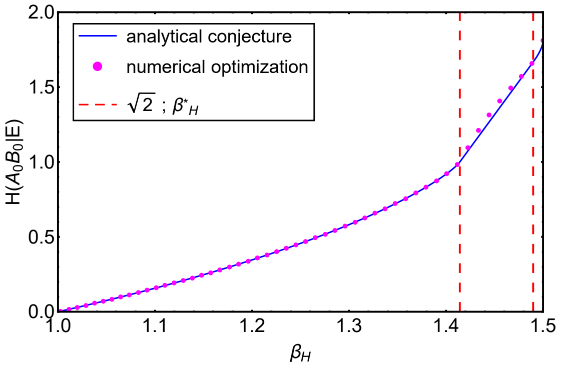

Figure 3: Lower bound on $H(A_0B_0|E)$ as a function of the violation of the tripartite Holz inequality. The plot points are obtained by numerically minimizing the entropy for a fixed Bell value β_{H} (see Appendix D for details), while the blue solid line is our conjectured analytical bound (14). Note that the numerical curve is concave in the interval enclosed by the red dashed lines while our analytical bound is convex in the whole domain, as required for a DI entropy bound.

We remark that the discrepancy between our analytical conjecture and the numerical curve in Fig. 3 is because the latter is not always a convex function of the violation. Indeed, within the interval $(\sqrt{2}, \beta_{\mathrm{H}}^*]$, the numerical curve and its conjectured analytical expression, $\theta(\beta_{\mathrm{H}}, x(\beta_{\mathrm{H}}))$, become concave. However, a DI lower bound on a conditional entropy must be a convex function of the violation. If this is not the case, Eve could distribute a convex combination of states yielding an entropy lower than that certified by the bound, thus spoiling its validity. For this, our conjectured bound (14) is constructed as the convex hull of the numerical curve, which guarantees that the bound is convex in the whole interval $(\sqrt{2}, 3/2]$. In particular, we replace the concave part of the curve by taking the tangent to the function $\theta(\beta_{\mathrm{H}}, x(\beta_{\mathrm{H}}))$ at $\beta_{\mathrm{H}} = \beta_{\mathrm{H}}^*$, such that the point of coordinates $(\sqrt{2}, 1)$ belongs to the tangent line. This explains the definition of β_{H}^* given in Appendix A.

4 Device-independent conference key agreement

The goal of device-independent conference key agreement (DICKA) is to establish a secret conference key among $N > 2$ parties in a DI fashion. For this, it is necessary to certify the secrecy of Alice's outcome used to generate the key, which we choose to be A_0.

This is done by testing a Bell inequality and computing a lower bound on $H(A_0|E)$, which indicates what fraction of Alice's outcome bit is secret with respect to the eavesdropper Eve. At the same time, Alice and the other parties want to obtain correlated outcomes to form the shared conference key. While such outcomes can be obtained from an additional measurement setting for the other parties, Alice's key-generating setting must be the same that is proved to be secret, i.e., A_0 [16, 50]. Due to potential noise affecting the parties' key-generating outcomes, Alice publicly broadcasts some error correction information for the other parties to correct their key bits and match Alice's. Asymptotically, the error-correction information needed by party i to correct their key – affected by a bit error rate Q_i– is given by a fraction $h(Q_i)$ of the whole key. Since the error-correction information is public, it is not secure, and must be subtracted from the fraction of secret key bits. Thus, the asymptotic conference key rate of a DICKA protocol, that is, the asymptotic rate of secret conference key bits produced per distributed state, is given by [46, 51]:

$$r_{\text{DICKA}} = H(A_0|E) - \max_{2\leq i\leq N} h(Q_i), \qquad (15)$$

where we maximize the error-correction information over the error rates Q_i so that even the party with the noisiest raw key can recover Alice's key.

Using the entropy bound on $H(A_0|E)$ derived in Theorem 1 for the Holz inequality, together with the other bounds considered in Subsec. 3.1 (the bound for the asymmetric CHSH inequality is numerically optimized over α), we can compute the asymptotic secret key rate of DICKA protocols based on the Holz, the Parity-CHSH and the asymmetric CHSH inequality, where the latter is implemented as a concatenation of bipartite DIQKD protocols. In contrast, it is conjectured [47, 50] that the MABK inequality cannot be used in a DICKA protocol since Alice's optimal measurements yielding large violations are different from the key-generating measurement she uses to establish a shared conference key with the other parties.

In Fig. 4, we plot the asymptotic conference key rate (15) of the DICKA protocols as a function of the parameter p, in logarithmic scale. The DICKA rates are obtained by using the optimal strategies reported in Appendix A, which require Alice's outcome A_0 to be the result of a Pauli Z measurement. This setting allows the parties to obtain perfectly correlated key bits –in the ideal scenario of no depolarization– if the others also choose Z as their additional key-generating measurement.

From Fig. 4 we observe that the optimal tripartite inequality for DICKA is the Holz inequality, which was expressly designed for this scope in [19]. The plot also shows a clear advantage in establishing a conference key with a DICKA protocol based on multipartite entanglement rather than Bell pairs. This advantage nearly covers the whole range of p in the case of global depolarization, while it vanishes for low values of p and local depolarization. This is due to the starker effect of local depolarization on multipartite entangled states, which reduces their ability to violate a Bell inequality for a given value of local noise. The threshold values for p above which a non-zero conference key can be extracted, in the case of local and global depolarization, are reported in Table 1.

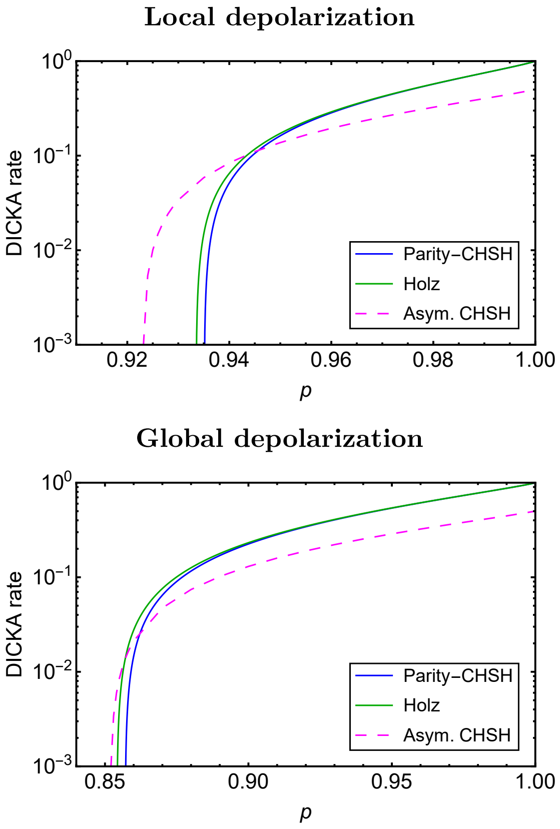

Figure 4: Asymptotic conference key rates, Eq. (15), of tripartite DICKA protocols based on the Holz inequality, Parity-CHSH inequality and a concatenation of bipartite DIQKD based on the asymmetric CHSH inequality, as a function of the parameter p (the probability of local or global depolarization is $1-p$). The DICKA protocol based on the asymmetric CHSH inequality is composed of two consecutive DIQKD protocols that Alice performs with Bob and then with Charlie. Hence its key rate earns a factor of $1/2$. The bit error rate between every pair of parties, for both the GHZ and Bell state, is $Q = (1-p^2)/2$ ($Q = (1-p)/2$) when the state is locally (globally) depolarized.

We remark that, in our comparison, a DICKA protocol based on a bipartite Bell inequality, such as the asymmetric CHSH inequality (5), is obtained as a concatenation of bipartite DIQKD protocols where Alice performs a DIQKD protocol first with Bob and then with Charlie[3]. For this, the total number of states distributed per conference key bit doubles, causing a

[3] Alice then uses the two keys established with Bob and Charlie to distribute the conference key with one-time-pad.

Bell ineq.	local noise	global noise
Holz	0.934	0.855
Parity-CHSH	0.936	0.858
asym. CHSH	0.923	0.852

Table 1: Threshold values for p (with $1-p$ being the probability of local or global depolarization, see Sec 2) such that a non-zero conference key can be extracted, in the asymptotic limit, by DICKA protocols based on different Bell inequalities.

factor 1/2 in the conference key rate (15). In the case of N parties establishing a conference key with concatenated DIQKD protocols, the conference key rate is reduced by a factor of $1/(N-1)$.

Another important drawback of implementing DICKA by a concatenation of DIQKD protocols is that the security of the established conference key is spoiled unless Alice uses a new device for every iteration of the DIQKD protocol [52, 53], making it more resource demanding. We argue on this issue in Sec. 6, where we also discuss about alternative definitions of conference key rates where the advantage provided by multipartite entanglement can still be retained.

5 Device-independent randomness expansion

A DIRE protocol aims to expand the initial share of private randomness of one or more parties in a DI way, by testing a Bell inequality. The amount of randomness in the outcomes of one or more parties is certified by computing a lower bound on a suitable conditional entropy, in terms of the observed Bell violation. Here we can envision a setup where the parties are located in the same lab[4] and wish to explore the randomness of their joint outcomes. The goal is achieved when the amount of randomness produced by the protocol is greater than the input randomness used for testing the Bell inequality.

In this section we investigate the applicability to DIRE of the bounds on $H(A_0B_0|E)$ presented in Sec. 3. Such bounds, as we will see, are particularly suited for spot-checking DIRE protocols [38], where Alice and Bob generate randomness with inputs A_0 and B_0 in most of the rounds and only sporadically test the Bell inequality with random inputs.

In Fig. 2 of Sec. 3 we observed that the two-outcome entropy bound for the MABK inequality is significantly larger than the other bounds. However, this does not necessarily imply that a DIRE protocol based on testing the MABK inequality can generate more *net* randomness than DIRE protocols based on the other inequalities. This is due to the fact that the MABK inequality requires a larger amount of input randomness (two random inputs for Alice, Bob and Charlie compared to the Parity-CHSH and the CHSH inequality where Charlie has a fixed input or remains idle). A definitive answer could come from a thorough finite-key analysis of the DIRE protocols via the entropy accumulation theorem [54]. Here instead, we aim at gaining intuition on the input/output randomness tradeoff by computing lower bounds on the asymptotic net randomness generation rate of DIRE protocols based on the four inequalities (2)-(5), which accounts for the input randomness required by each Bell test.

The net randomness generation rate of a DIRE protocol is the fraction of fresh random bits produced per distributed state, i.e., per round. In a spot-checking DIRE protocol a public source of randomness, shared by all parties, declares whether each round is a testing round ($T=1$ with probability γ) or a randomness-generation round ($T=0$ with probability $1-\gamma$). In a randomness-generation round, Alice and Bob select input 0 and collect the outcomes A_0 and B_0, which generate $H(A_0B_0|E)$ bits of secret randomness (if the protocol involves additional parties, they also select a predefined input). In a testing round, the parties locally choose random inputs for their devices (represented by a joint random variable I) and test the selected Bell inequality. Since this step does not require public communication if the parties operate in the same lab, they consider their outcomes as part of the generated secret randomness. The conditional entropy that quantifies the amount of secret randomness generated in a test round is $H(AB|E)$. This entropy is larger than $H(A_0B_0|E)$, since in this case the inputs that generated the outputs (AB) are random and unknown to Eve. Thus, the output randomness generation rate of the spot-checking DIRE protocol is given by:

$$\begin{aligned} H(AB|TE) &= (1-\gamma)H(A_0B_0|E) + \gamma H(AB|E) \\ &\geq H(A_0B_0|E), \end{aligned} \tag{16}$$

where we used the strong sub-additivity of the von Neumann entropy in the inequality.

The input randomness consumed in a generic round of a spot-checking DIRE protocol is given by:

$$\begin{aligned} H(T,I) &= H(I|T) + H(T) \\ &= \gamma H(I|T=1) + (1-\gamma)H(I|T=0) + h(\gamma) \\ &= r\gamma + h(\gamma), \end{aligned} \tag{17}$$

where r is the total number of random bits required as inputs by the selected Bell inequality. Then, the asymptotic net randomness generation rate of a spot-checking DIRE protocol is obtained by subtracting the input randomness (17) from the output randomness (16), as follows:

$$\begin{aligned} r_{\text{spDIRE}} &= H(AB|TE) - H(T,I) \\ &\geq H(A_0B_0|E) - r\gamma - h(\gamma). \end{aligned} \tag{18}$$

[4] For device-independent randomness certification, it is essential, however, to ensure that the potentially malicious devices do not communicate.

Thus, the net randomness generation rate of a DIRE protocol based on testing the CHSH or Parity-CHSH inequality satisfies:

$$r_{\text{spDIRE}} \geq H(A_0B_0|E) - 2\gamma - h(\gamma), \tag{19}$$

while that of a DIRE protocol based on the MABK or the Holz inequality satisfies:

$$r_{\text{spDIRE}} \geq H(A_0B_0|E) - 3\gamma - h(\gamma), \tag{20}$$

since three random bits are required in each testing round. We can now use the two-outcome entropy bounds presented in Sec. 3 in combination with (19) and (20) to compare the performance of the corresponding DIRE protocols.

We remark that, asymptotically, the optimal value for γ tends to zero, i.e. it is sufficient to test the Bell inequality on a negligible fraction of rounds in order to learn the exact Bell violation. In this case, the net randomness generation rate in (18) is given by $H(A_0B_0|E)$ with an equality sign. However, in order to investigate the effect of test rounds on spot-checking DIRE protocols where more input randomness is required (MABK and Holz inequalities), we set γ to $\gamma = 0.033\%$, which is the value used in the DIRE experiment of [29].

In order to benchmark the DIRE rates (19) and (20), we consider a new type of DIRE protocol without spot-checking and based on the CHSH inequality [38]. In this DIRE protocol there is no distinction between rounds and in each round Alice (Bob) randomly selects her (his) input X (Y) and uses the outputs A and B to test the CHSH inequality. If the outputs are not publicly revealed (e.g. Alice and Bob are in the same lab), they can form part of the randomness generated by the protocol. Moreover, the protocol recycles the input randomness X and Y –which is also secret and unknown to Eve– and appends it to the output randomness before extracting the secret random string. In this case, the asymptotic net randomness generation rate of the protocol is given by:

$$\begin{aligned} r_{\text{DIRE}} &= H(ABXY|E) - H(XY) \\ &= H(AB|XYE), \end{aligned} \tag{21}$$

where, physically, the conditional entropy $H(AB|XYE)$ expresses the uncertainty that Eve has about Alice's and Bob's outcomes, when Alice and Bob use random inputs X and Y and the inputs become known to Eve after the measurement. The authors in [38] conjecture a tight analytical lower bound on $H(AB|XYE)$ as a function of the CHSH value β_C (reported in Appendix A), which we employ to plot the DIRE rate (21).

In Fig. 5 we plot the asymptotic net randomness generation rates of spot-checking DIRE protocols based on the CHSH and Parity-CHSH inequalities (19) and on the MABK and Holz inequalities (20), as well as the net randomness generation rate of the DIRE protocol without spot-checking based on the CHSH inequality (21). The threshold values for p above which we have a positive randomness generation rate, assuming $\gamma = 0$, can be calculated analytically since each of the analyzed two-outcome entropy bounds yields non-zero randomness as soon as the corresponding classical bound is violated. The numerical values we obtain are reported in Table 2.

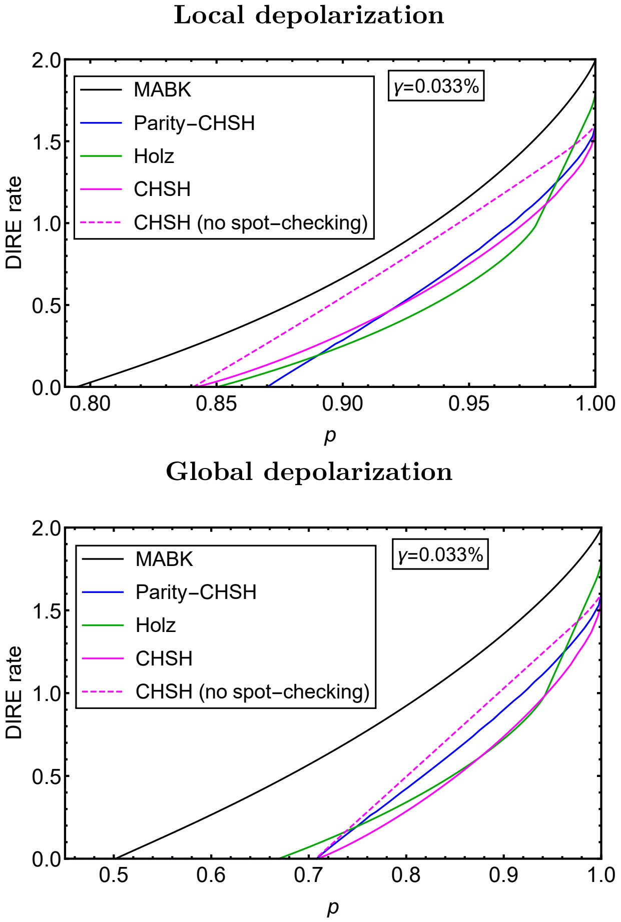

Figure 5: Asymptotic net randomness generation rates for DIRE protocols that extract secret randomness from the outcomes of two parties, as a function of p, where $1 - p$ is the probability of local or global depolarization. The solid lines correspond to spot-checking DIRE protocols where a test round is performed on a fraction γ of the total set of rounds, while the dashed line represents a DIRE protocol where the CHSH inequality is tested in every round and the random inputs are recycled [38]. A spot-checking DIRE protocol based on the MABK inequality still generates the largest amount of net randomness. The value of γ is set to the experimental value of [29].

From Fig. 5 we observe that the optimal Bell inequality for DIRE is the MABK inequality, both in terms of randomness generation rate and noise tolerance. However, DIRE protocols based on the Holz inequality can also outperform protocols based on the CHSH inequality in the low-noise regime (high values of p), even when compared to CHSH-based DIRE protocols which recycle the input randomness. More-

Bell ineq.	local noise	global noise
MABK	0.794	0.500
Parity-CHSH	0.870	0.707
Holz	0.849	0.667
CHSH	0.841	0.707
CHSH (no spot-ch.)	0.841	0.707

Table 2: Threshold values for p (with $1-p$ being the probability of local or global depolarization, see Sec 2) such that, asymptotically, DIRE protocols based on the analyzed Bell inequalities yield a positive net-randomness generation rate.

over, for the chosen realistic value of γ, the effect of test rounds on the DIRE rates is negligible as they approximately coincide with the entropy curves in Fig. 2.

Nevertheless, for a fixed Bell inequality, a DIRE protocol without spot-checking and with recycled input randomness may yield more net randomness than the corresponding protocol with spot-checking. This holds for any DIRE protocol based on a Bell inequality which is symmetric with respect to permutations of the parties' observables, like the CHSH inequality. Indeed, the asymptotic net randomness generation rate of, say, a bipartite spot-checking protocol is given by a lower bound $F(\beta)$ on $H(A_0B_0|E)$ (recall that $\gamma \to 0$ in the asymptotic regime), while the rate of the protocol without spot-checking and with recycled input randomness is given by a lower bound on $H(AB|XYE)$. Due to the permutation symmetry of the inequality, the lower bound on $H(A_0B_0|E)$ is actually valid for any combination of inputs of Alice and Bob: $F(\beta) \leq H(A_kB_l|E) \equiv H(AB|X=k, Y=l, E)$ for all $k, l \in \{0,1\}$, hence it is also a lower bound on $H(AB|XYE) = \sum_{k,l} p_{kl} H(AB|X=k, Y=l, E)$. However, it is likely that a direct calculation of $H(AB|XYE)$ would lead to a tighter lower bound and hence to a higher rate for the DIRE protocol without spot-checking. This is confirmed in the CHSH case by Fig. 5, where the dashed magenta line (DIRE protocol without spot-checking) lies significantly above the solid magenta line (DIRE protocol with spot-checking).

6 Discussion and conclusion

In this work we consider a two-input/two-output tripartite device-independent (DI) scenario with different tripartite Bell inequalities, namely: the Holz inequality [19], the MABK inequality [42–44], and the Parity-CHSH inequality [20], as well as the family of (bipartite) asymmetric CHSH inequalities [35, 45]. We investigate the asymptotic performance of DI conference key agreement (DICKA) and DI randomness expansion (DIRE) protocols when the different Bell inequalities are tested to certify private randomness in the parties' outcomes. To this aim, we present analytical and numerical lower bounds on the conditional von Neumann entropy of a single party's outcome and of two parties' outcomes, as a function of the Bell inequality violation. We provide a concise overview of the bounds in Table 3.

Specifically, for the Holz inequality [19] we derive a tight analytical bound on the one-outcome entropy, $H(A_0|E)$, and conjecture a tight analytical bound on the two-outcome entropy, $H(A_0B_0|E)$, that is strongly supported by numerical results. These are the first tight analytical bounds on the conditional von Neumann entropy for a non-full-correlator Bell inequality –apart from the one-outcome entropy bound derived in [20] for the Parity-CHSH inequality, whose tightness is only proved in this work in Appendix E. For the Parity-CHSH and CHSH inequality we instead compute numerical bounds on the two-outcome entropy $H(A_0B_0|E)$.

By using the derived bounds together with bounds obtained in previous literature [20, 35, 47], we compute the asymptotic conference key rate (net randomness generation rate) of DICKA (DIRE) protocols based on the above-mentioned Bell inequalities. We remark, however, that the analytical bounds presented in this work could be applied to finite-key analyses of DICKA and DIRE protocols through the entropy accumulation theorem [16, 54], although we leave this as a matter for future work.

Importantly, our results show that DI protocols based on multipartite Bell inequalities can outperform implementations based on bipartite Bell inequalities under different noise models (local and global depolarizing noise) and for a broad range of noise levels.

For the task of DICKA, the Holz inequality turns out to be the one that yields the largest key rate and, in general, DICKA is better performed with multipartite Bell inequalities. In Sec. 4 we remark that a DICKA protocol based on a bipartite Bell inequality must be obtained as a concatenation of DIQKD protocols subsequently run, e.g., between Alice and each of the other parties. Hence, its conference key rate, defined as the fraction of secret conference key bits per distributed state, is overly penalized compared to the key rate of a DICKA protocol based on a multipartite Bell inequality. In this regard, one could argue that a more practical definition of conference key rate is given by the fraction of secret conference key bits generated per unit of time. In this case, the relationship between the key rates in Fig. 4 might change significantly due to, e.g., a faster distribution of Bell pairs compared to multipartite entangled states. However, future quantum networks might generate highly non-trivial resource states in order to suit the different needs of its nodes [55], or could present peculiar topologies (e.g. bottle-necks [56]) such that the distillation of a multipartite entangled state and of a Bell pair require the same amount of resources and time. In these cases, the advantage of performing DICKA with multipartite entangled states rather

Bell inequality	$\mathbf{H(A_0\|E)}$		$\mathbf{H(A_0B_0\|E)}$	
	lower bound	tight	lower bound	tight
Holz	Theorem 1 [This work]	YES [This work]	Conjecture 1 [This work]	YES [This work]
Parity-CHSH	(A.11) [20]	YES [This work]	numerical [This work]	YES* [This work]
MABK	Appendix C [This work] & [46, 47]	NO [47]	(A.15) [47]	NO [47]
asymmetric CHSH (CHSH for $\alpha = 1$)	(A.19) [35]	YES [35]	numerical ($\alpha = 1$) [This work] & [38]	YES* [This work] & [38]

Table 3: Summary of the one-outcome and two-outcome entropy bounds used to investigate DIRE and DICKA protocols based on different Bell inequalities. The expressions of all the analytical bounds are reported in Appendix A. We additionally employ the tight analytical bound (A.20) on $H(AB|XYE)$, conjectured in [38], to study a CHSH-based DIRE protocol without spot-checking and with recycled input randomness. *Note that the numerical lower bounds obtained in this work are not reliable as they are the result of a non-convex minimization of the entropy over the set of states compatible with the Bell violation. Hence, their tightness is understood as the existence of an implementation which attains the plotted curve.

than a concatenation of DIQKD protocols would be retained even with more practical definitions of conference key rate.

Another important drawback of implementing DICKA by a concatenation of DIQKD protocols is that the security of the established conference key is spoiled unless Alice uses a new device for every iteration of the DIQKD protocol. Indeed, reusing the same quantum device in independent runs of a DIQKD protocol could lead to security loopholes [52, 53]. Thus, in such a case, Alice would need to possess $N-1$ quantum measurement devices in order to establish a conference key with $N-1$ other parties. For the tripartite DICKA protocol based on the asymmetric CHSH inequality, she would need two distinct quantum devices. Conversely, Alice can establish a conference key with an arbitrary number of parties with only one device, by a single run of a DICKA protocol based on multipartite Bell inequalities, such as the Holz inequality.

Concerning DIRE, we observe that a spot-checking DIRE protocol based on the MABK inequality is the one that yields the largest amount of net randomness in the outcomes of two parties, even when compared with a recent CHSH-based DIRE protocol without spot-checking, where the input randomness is recycled [38]. The advantage of the MABK inequality over the other inequalities could lie in its permutational symmetry, which does not privilege one party at the expense of the other parties (as in the Holz and the Parity-CHSH inequality). However, the CHSH inequality is also permutationally-invariant but its bound on $H(A_0B_0|E)$ lies well below the bound for the MABK inequality. This could be explained by the fact that, for any full-correlator Bell inequality such as the MABK and the CHSH inequality, one can assume all the marginal distributions of the outcomes to be symmetric, without loss of generality [47]. Therefore, for the tripartite MABK inequality we have that the unconditional entropy of Alice's and Bob's outcomes is maximal: $H(A_0B_0) = 2$. While in general this is not true for the bipartite CHSH inequality: $H(A_0B_0) < 2$, where the conditions on the marginals ($\langle A_0\rangle = \langle B_0\rangle = 0$) cannot fix the joint distribution of A_0B_0.

Our work suggests many possible lines of future research. To start with, we emphasize that the techniques employed in the derivation of the one-outcome entropy bounds for the Holz and the MABK inequality (Theorem 1 and Appendix C) are applicable to general Bell inequalities with two inputs and two outputs per party. For instance, one could generalize Theorem 1 to the multipartite scenario where the N-party Holz inequality is tested [19], although the way to achieve this might be highly non-trivial. This result, nevertheless, could lead to the best DICKA rate achievable by N parties, since the Holz inequality was introduced in [19] exactly for the purpose of DICKA. On a similar note, one could derive a one-outcome entropy bound that accounts for noisy pre-processing and bias of Alice's raw output, similarly to what has been done in the bipartite case for the CHSH inequality [35, 36].

In the case of DIRE, it is important to remark that the net randomness generated by testing tripartite Bell inequalities can be significantly increased compared to the results presented in Sec. 5, making multipartite nonlocality even more beneficial for DI cryptography. One obvious way to increase the DI randomness is to combine the outputs of all three parties in the randomness-generation rounds, instead of only using Alice's and Bob's outputs. However, this requires the derivation of bounds on three-outcome entropies of the form $H(A_iB_jC_k|E)$, for which no analytical nor numerical result is yet available. Another way to generate more randomness from multipartite nonlocality is to extend the idea of DIRE protocols without spot-checking and with recycled input randomness to the multiparty scenario. Indeed, such protocols can outperform the corresponding spot-checking protocol that tests the same Bell inequality, especially when the latter is permutationally invariant. Therefore, an important avenue to improve the randomness generated by the MABK-based DIRE protocol, and any multipartite DIRE protocol based on permutationally-invariant Bell inequalities, is the derivation of entropy bounds on quantities like $H(AB|XYZE)$ and $H(ABC|XYZE)$.

Besides deriving new entropy bounds and improving the performance of DI protocols, our work leaves an interesting question open. In Sec. 3 we show that genuine multipartite entanglement (GME) is not always necessary to certify non-zero entropy in a single party's outcome when testing a multipartite Bell inequality, especially when the latter presents asymmetries. This means that GME is not a precondition for DIRE protocols with multipartite Bell inequalities. Conversely, DICKA schemes, apart from certifying private randomness, also require the parties to obtain correlated outcomes that can form a shared conference key. It remains an open question whether non-GME states can be used to perform DICKA, while their usefulness has been established in the case of device-dependent CKA [57].

Acknowledgements

We acknowledge support by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1 -390534769. D.B. and H.K. acknowledge support by the QuantERA project QuICHE, via the German Ministry for Education and Research (BMBF Grant No. 16KIS1119K). F.G. and D.B. acknowledge support by the DFG Individual Research Grant BR2159/6-1.

References

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. "Advances in quantum cryptography". Adv. Opt. Photon. **12**, 1012–1236 (2020).

[2] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. "Secure quantum key distribution with realistic devices". Rev. Mod. Phys. **92**, 025002 (2020).

[3] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. "Hacking commercial quantum cryptography systems by tailored bright illumination". Nature Photonics **4**, 686–689 (2010).

[4] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. "Full-field implementation of a perfect eavesdropper on a quantum cryptography system". Nature Communications **2**, 349 (2011).

[5] A. Yao and D. Mayers. "Quantum cryptography with imperfect apparatus". In IEEE 54th Annual Symposium on Foundations of Computer Science. Page 503. Los Alamitos, CA, USA (1998). IEEE Computer Society.

[6] Antonio Acín, Nicolas Gisin, and Lluis Masanes. "From bell's theorem to secure quantum key distribution". Phys. Rev. Lett. **97**, 120405 (2006).

[7] Jonathan Barrett, Adrian Kent, and Stefano Pironio. "Maximally nonlocal and monogamous quantum correlations". Phys. Rev. Lett. **97**, 170409 (2006).

[8] J. S. Bell and Alain Aspect. "Speakable and unspeakable in quantum mechanics: Collected papers on quantum philosophy". Cambridge University Press. (2004). 2 edition.

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

[10] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. "Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres". Nature **526**, 682–686 (2015).

[11] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. "Significant-loophole-free test of bell's theorem with entangled photons". Phys. Rev. Lett. **115**, 250401 (2015).

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

[13] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. "Device-independent quantum key distribution secure against collective attacks". New Journal of Physics **11**, 045021 (2009).

[14] Lluís Masanes, Stefano Pironio, and Antonio Acín. "Secure device-independent quantum key distribution with causally independent measurement devices". Nature Communications **2**, 238 (2011).

[15] Umesh Vazirani and Thomas Vidick. "Fully device-independent quantum key distribution". Phys. Rev. Lett. **113**, 140501 (2014).

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

[17] Valerio Scarani and Nicolas Gisin. "Quantum communication between n partners and bell's inequalities". Phys. Rev. Lett. **87**, 117901 (2001).

[18] Valerio Scarani and Nicolas Gisin. "Quantum key distribution between n partners: Optimal eavesdropping and bell's inequalities". Phys. Rev. A **65**, 012311 (2001).

[19] Timo Holz, Hermann Kampermann, and Dagmar Bruß. "Genuine multipartite bell inequality for device-independent conference key agreement". Phys. Rev. Research **2**, 023251 (2020).

[20] Jérémy Ribeiro, Gláucia Murta, and Stephanie Wehner. "Reply to "comment on fully device-independent conference key agreement"". Phys. Rev. A **100**, 026302 (2019).

[21] Gláucia Murta, Federico Grasselli, Hermann Kampermann, and Dagmar Bruß. "Quantum conference key agreement: A review". Advanced Quantum Technologies **3**, 2000025 (2020).

[22] Roger Colbeck. "Quantum and relativistic protocols for secure multi-party computation" (2011). arXiv:0911.3814.

[23] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, et al. "Random numbers certified by bell's theorem". Nature **464**, 1021–1024 (2010).

[24] Roger Colbeck and Adrian Kent. "Private randomness expansion with untrusted devices". Journal of Physics A: Mathematical and Theoretical **44**, 095305 (2011).

[25] Carl A. Miller and Yaoyun Shi. "Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices". J. ACM**63** (2016).

[26] Stefano Pironio and Serge Massar. "Security of practical private randomness generation". Phys. Rev. A **87**, 012336 (2013).

[27] Serge Fehr, Ran Gelles, and Christian Schaffner. "Security and composability of randomness expansion from bell inequalities". Phys. Rev. A **87**, 012335 (2013).

[28] Erik Woodhead, Boris Bourdoncle, and Antonio Acín. "Randomness versus nonlocality in the Mermin-Bell experiment with three parties". Quantum **2**, 82 (2018).

[29] Wen-Zhao Liu, Ming-Han Li, Sammy Ragy, Si-Ran Zhao, Bing Bai, Yang Liu, Peter J. Brown, Jun Zhang, Roger Colbeck, Jingyun Fan, Qiang Zhang, and Jian-Wei Pan. "Device-independent randomness expansion against quantum side information". Nature Physics **17**, 448–451 (2021).

[30] Lynden K. Shalm, Yanbao Zhang, Joshua C. Bienfang, Collin Schlager, Martin J. Stevens, Michael D. Mazurek, Carlos Abellán, Waldimar Amaya, Morgan W. Mitchell, Mohammad A. Alhejji, Honghao Fu, Joel Ornstein, Richard P. Mirin, Sae Woo Nam, and Emanuel Knill. "Device-independent randomness expansion with entangled photons". Nature Physics **17**, 452–456 (2021).

[31] Wei Zhang, Tim van Leent, Kai Redeker, Robert Garthoff, René Schwonnek, Florian Fertig, Sebastian Eppelt, Wenjamin Rosenfeld, Valerio Scarani, Charles C.-W. Lim, and Harald Weinfurter. "A device-independent quantum key distribution system for distant users". Nature **607**, 687–691 (2022).

[32] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal. "Experimental quantum key distribution certified by bell's theorem". Nature **607**, 682–686 (2022).

[33] Wen-Zhao Liu, Yu-Zhe Zhang, Yi-Zheng Zhen, Ming-Han Li, Yang Liu, Jingyun Fan, Feihu Xu, Qiang Zhang, and Jian-Wei Pan. "Toward a photonic demonstration of device-independent quantum key distribution". Phys. Rev. Lett. **129**, 050502 (2022).

[34] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. "Proposed experiment to test local hidden-variable theories". Phys. Rev. Lett. **23**, 880–884 (1969).

[35] Erik Woodhead, Antonio Acín, and Stefano Pironio. "Device-independent quantum key distribution with asymmetric CHSH inequalities". Quantum **5**, 443 (2021).

[36] Michele Masini, Stefano Pironio, and Erik Woodhead. "Simple and practical DIQKD security analysis via BB84-type uncertainty relations and pauli correlation constraints". Quantum **6**, 843 (2022).

[37] Pavel Sekatski, Jean-Daniel Bancal, Xavier Valcarce, Ernest Y.-Z. Tan, Renato Renner, and Nicolas Sangouard. "Device-independent quantum key distribution from generalized CHSH inequalities". Quantum **5**, 444 (2021).

[38] Rutvij Bhavsar, Sammy Ragy, and Roger Colbeck. "Improved device-independent random-

ness expansion rates using two sided randomness" (2023). arXiv:2103.07504.

[39] Peter Brown, Hamza Fawzi, and Omar Fawzi. "Computing conditional entropies for quantum correlations". Nature Communications **12**, 575 (2021).

[40] Ernest Y.-Z. Tan, René Schwonnek, Koon Tong Goh, Ignatius William Primaatmaja, and Charles C.-W. Lim. "Computing secure key rates for quantum cryptography with untrusted devices". npj Quantum Information **7**, 158 (2021).

[41] Ernest Y.-Z. Tan, Pavel Sekatski, Jean-Daniel Bancal, René Schwonnek, Renato Renner, Nicolas Sangouard, and Charles C.-W. Lim. "Improved DIQKD protocols with finite-size analysis". Quantum **6**, 880 (2022).

[42] N. David Mermin. "Extreme quantum entanglement in a superposition of macroscopically distinct states". Phys. Rev. Lett. **65**, 1838–1840 (1990).

[43] M. Ardehali. "Bell inequalities with a magnitude of violation that grows exponentially with the number of particles". Phys. Rev. A **46**, 5375–5378 (1992).

[44] A. V. Belinskiĭ and D. N. Klyshko. "Interference of light and bell's theorem". Phys. Rev. A **36**, 653–693 (1993).

[45] Antonio Acín, Serge Massar, and Stefano Pironio. "Randomness versus nonlocality and entanglement". Phys. Rev. Lett. **108**, 100402 (2012).

[46] Jérémy Ribeiro, Gláucia Murta, and Stephanie Wehner. "Fully device-independent conference key agreement". Phys. Rev. A **97**, 022307 (2018).

[47] Federico Grasselli, Gláucia Murta, Hermann Kampermann, and Dagmar Bruß. "Entropy bounds for multiparty device-independent cryptography". PRX Quantum **2**, 010308 (2021).

[48] Lluís Masanes. "Asymptotic violation of bell inequalities and distillability". Phys. Rev. Lett. **97**, 050503 (2006).

[49] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner. "The uncertainty principle in the presence of quantum memory". Nature Physics **6**, 659–662 (2010).

[50] Timo Holz, Daniel Miller, Hermann Kampermann, and Dagmar Bruß. "Comment on "fully device-independent conference key agreement"". Phys. Rev. A **100**, 026301 (2019).

[51] Federico Grasselli. "Quantum cryptography". Springer International Publishing. (2021).

[52] G Murta, S B van Dam, J Ribeiro, R Hanson, and S Wehner. "Towards a realization of device-independent quantum key distribution". Quantum Science and Technology **4**, 035011 (2019).

[53] Jonathan Barrett, Roger Colbeck, and Adrian Kent. "Memory attacks on device-independent quantum cryptography". Phys. Rev. Lett. **110**, 010503 (2013).

[54] F. Dupuis and O. Fawzi. "Entropy accumulation with improved second-order term". IEEE Transactions on Information Theory **65**, 7596–7612 (2019).

[55] Alexander Pickston, Joseph Ho, Andrés Ulibarrena, Federico Grasselli, Massimiliano Proietti, Christopher L. Morrison, Peter Barrow, Francesco Graffitti, and Alessandro Fedrizzi. "Experimental network advantage for quantum conference key agreement" (2022). arXiv:2207.01643.

[56] Michael Epping, Hermann Kampermann, Chiara Macchiavello, and Dagmar Bruß. "Multi-partite entanglement can speed up quantum key distribution in networks". New Journal of Physics **19**, 093012 (2017).

[57] Giacomo Carrara, Hermann Kampermann, Dagmar Bruß, and Glá ucia Murta. "Genuine multipartite entanglement is not a precondition for secure conference key agreement". Physical Review Research**3** (2021).

[58] Michael A. Nielsen and Isaac L. Chuang. "Quantum computation and quantum information: 10th anniversary edition". Cambridge University Press. (2010).

[59] Lucas Tendick, Hermann Kampermann, and Dagmar Bruß. "Quantifying necessary quantum resources for nonlocality". Physical Review Research**4** (2022).

[60] Wolfram Research, Inc. "Mathematica, Version 10.3" (2016).

A Summary of optimal strategies and entropy bounds

In this appendix we report the quantum strategies that lead to maximal violation of the Bell inequalities considered in the manuscript, as well as a summary of the one-outcome and two-outcome entropy bounds used to benchmark DICKA and DIRE protocols.

Holz inequality [19] For three parties, the inequality reads:

$$\beta_{\mathrm{H}} := \langle A_1 B_+ C_+\rangle - \langle A_0 B_-\rangle - \langle A_0 C_-\rangle - \langle B_- C_-\rangle \leq 1, \tag{A.1}$$

and has quantum bound $\beta_{\mathrm{H}}^Q = 3/2$. The quantum bound is attained when the parties share a GHZ state and choose the following optimal measurements:

$$\begin{aligned} A_0 = \sigma_z \quad &; \quad A_1 = \sigma_x \\ B_+ = C_+ = \frac{\sqrt{3}}{2}\sigma_x \quad &; \quad B_- = C_- = -\frac{1}{2}\sigma_z . \end{aligned} \tag{A.2}$$

The tight lower bound on the conditional entropy of Alice's outcome A_0, certified by a violation of the Holz inequality, reads (Theorem 1):

$$H(A_0|E) \geq 1 - h\left[\frac{1}{4}\left(\beta_{\mathrm{H}} + 1 + \sqrt{\beta_{\mathrm{H}}^2 + 2\beta_{\mathrm{H}} - 3}\right)\right]. \tag{A.3}$$

The tight lower bound on the conditional entropy of Alice's and Bob's outcomes A_0 and B_0 is conjectured to be (Conjecture 1):

$$H(A_0 B_0|E) \geq \begin{cases} \eta(\beta_{\mathrm{H}}) & \beta_{\mathrm{H}} \in [1, \sqrt{2}] \\ \dfrac{\theta(\beta_{\mathrm{H}}^*, x(\beta_{\mathrm{H}}^*)) - 1}{\beta_{\mathrm{H}}^* - \sqrt{2}}(\beta_{\mathrm{H}} - \sqrt{2}) + 1 & \beta_{\mathrm{H}} \in (\sqrt{2}, \beta_{\mathrm{H}}^*] \\ \theta(\beta_{\mathrm{H}}, x(\beta_{\mathrm{H}})) & \beta_{\mathrm{H}} \in (\beta_{\mathrm{H}}^*, 3/2] \end{cases} \tag{A.4}$$

where the functions η and θ are defined as:

$$\eta(\beta_{\mathrm{H}}) = 2 - H\left(\left\{\frac{1}{4}\left(1 + \sqrt{\beta_{\mathrm{H}}^2 - 1}\right), \frac{1}{4}\left(1 + \sqrt{\beta_{\mathrm{H}}^2 - 1}\right), \frac{1}{4}\left(1 - \sqrt{\beta_{\mathrm{H}}^2 - 1}\right), \frac{1}{4}\left(1 - \sqrt{\beta_{\mathrm{H}}^2 - 1}\right)\right\}\right) \tag{A.5}$$

and

$$\begin{aligned} \theta(\beta_{\mathrm{H}}, x) = H&\left(\left\{\frac{\beta_{\mathrm{H}}(2-\beta_{\mathrm{H}}) - x^2}{8(\beta_{\mathrm{H}} - 1)}, \frac{\beta_{\mathrm{H}}(2-\beta_{\mathrm{H}}) - x^2}{8(\beta_{\mathrm{H}} - 1)}, \frac{(\beta_{\mathrm{H}} - 1)(\beta_{\mathrm{H}} + 3) + x^2 - 1}{8(\beta_{\mathrm{H}} - 1)}, \frac{(\beta_{\mathrm{H}} - 1)(\beta_{\mathrm{H}} + 3) + x^2 - 1}{8(\beta_{\mathrm{H}} - 1)}\right\}\right) \\ &- h\left(\frac{2(1-x) - (\beta_{\mathrm{H}} - x)^2}{4x(\beta_{\mathrm{H}} - 1)}\right). \end{aligned} \tag{A.6}$$

The function $x(\beta_{\mathrm{H}})$ returns the real solution of the following transcendental equation in x:

$$\begin{aligned} &\left(\beta_{\mathrm{H}}^2 - x^2 - 2\right)\log\left(-\beta_{\mathrm{H}}^2 - 2\beta_{\mathrm{H}}x - x^2 + 2x + 2\right) + \left(x^2 + 2\right)\log\left(\beta_{\mathrm{H}}^2 - 2\beta_{\mathrm{H}}x + x^2 + 2x - 2\right) \\ &+ 2x^3\log\left(\beta_{\mathrm{H}}^2 + 2\beta_{\mathrm{H}} + x^2 - 4\right) - \beta_{\mathrm{H}}^2\log\left(\beta_{\mathrm{H}}^2 - 2\beta_{\mathrm{H}}x + x^2 + 2x - 2\right) - 2x^3\log\left(-\beta_{\mathrm{H}}^2 + 2\beta_{\mathrm{H}} - x^2\right) = 0, \end{aligned} \tag{A.7}$$

which is obtained by setting $\partial\theta(\beta_{\mathrm{H}}, x)/\partial x = 0$. Finally, the violation β_{H}^* is approximately given by $\beta_{\mathrm{H}}^* \approx 1.49$ and is implicitly defined by the following equation:

$$\frac{d\theta(\beta_{\mathrm{H}}^*, x(\beta_{\mathrm{H}}^*))}{d\beta_{\mathrm{H}}^*}(\beta_{\mathrm{H}}^* - \sqrt{2}) = \theta(\beta_{\mathrm{H}}^*, x(\beta_{\mathrm{H}}^*)) - 1. \tag{A.8}$$

Parity-CHSH inequality [20] The inequality reads, after renormalization, as follows:

$$\beta_{\mathrm{pC}} = \langle A_1 B_- C\rangle + \langle A_0 B_+\rangle \leq 1 \tag{A.9}$$

where $B_{\pm};= (B_0 \pm B_1)/2$ and $\beta^Q_{\mathrm{pC}} = \sqrt{2}$ is the quantum bound, which is attained when the parties share a GHZ state and choose the following optimal measurements:

$$\begin{aligned} A_0 = \sigma_z \quad &; \quad A_1 = \sigma_x \quad ; \quad C = \sigma_x \\ B_+ = \frac{1}{\sqrt{2}}\sigma_z \quad &; \quad B_- = \frac{1}{\sqrt{2}}\sigma_x. \end{aligned} \tag{A.10}$$

A lower bound on the entropy of Alice's outcome A_0 certified by the Parity-CHSH inequality is given by:

$$H(A_0|E) \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\left(\beta_{\mathrm{pC}}\right)^2 - 1}\right). \tag{A.11}$$

The above bound is derived in [20], however it was not proved to be tight. We show its tightness in Appendix E.

A numerical lower bound on the two-outcome entropy $H(A_0B_0|E)$ is obtained in this work. For details, see Appendix D.

MABK inequality [42–44] In the case of three parties the inequality reads:

$$\beta_{\mathrm{M}} = \langle A_0B_0C_1\rangle + \langle A_0B_1C_0\rangle + \langle A_1B_0C_0\rangle - \langle A_1B_1C_1\rangle \leq 2. \tag{A.12}$$

The quantum bound $\beta^Q_{\mathrm{M}} = 4$ is achieved by the following optimal measurements on the GHZ state:

$$\begin{aligned} A_0 = B_0 = \sigma_y \quad &; \quad A_1 = B_1 = \sigma_x \\ C_0 = -\sigma_y \quad &; \quad C_1 = -\sigma_x. \end{aligned} \tag{A.13}$$

A lower bound on the entropy of Alice's outcome is given by [46, 47]:

$$H(A_0|E) \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{\beta_{\mathrm{M}}^2}{8} - 1}\right). \tag{A.14}$$

We provide an alternative proof of this bound in Appendix C.

For the two-party entropy $H(A_0B_0|E)$, a lower bound is given by [47]:

$$H(A_0B_0|E) \geq 2 - H\left(\{1 - 3f(\beta_{\mathrm{M}}), f(\beta_{\mathrm{M}}), f(\beta_{\mathrm{M}}), f(\beta_{\mathrm{M}})\}\right), \tag{A.15}$$

where $H(\{p_1, p_2, \dots\})$ is the Shannon entropy of the probability distribution $\{p_1, p_2, \dots\}$ and the function f is defined as:

$$f(\beta_{\mathrm{M}}) = \frac{1}{4} - \frac{\sqrt{3}}{24}\sqrt{\beta_{\mathrm{M}}^2 - 4}. \tag{A.16}$$

We remark that, according to the numerical calculations in [47], the bounds in (A.14) and (A.15) are not tight but are close to the corresponding tight lower bound.

Asymmetric CHSH inequalities [35, 45] The family of inequalities is parametrized by $\alpha \in \mathbb{R}$ and reads:

$$\beta_{\alpha\mathrm{C}} = \alpha\langle A_0B_0\rangle + \alpha\langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \leq \begin{cases} 2|\alpha| & \text{if } |\alpha| > 1 \\ 2 & \text{if } |\alpha| \leq 1 \end{cases} \tag{A.17}$$

The CHSH inequality is maximally violated and reaches its quantum bound $\beta^Q_{\alpha\mathrm{C}} = 2\sqrt{1+\alpha^2}$ when Alice and Bob share $|\Phi^+\rangle$ and perform the optimal measurements [35]:

$$\begin{aligned} A_0 = \sigma_z \quad &; \quad A_1 = \sigma_x \\ B_0 = \frac{\alpha}{\sqrt{1+\alpha^2}}\sigma_z + \frac{1}{\sqrt{1+\alpha^2}}\sigma_x \quad &; \quad B_1 = \frac{\alpha}{\sqrt{1+\alpha^2}}\sigma_z - \frac{1}{\sqrt{1+\alpha^2}}\sigma_x. \end{aligned} \tag{A.18}$$

A tight lower bound on the entropy of Alice's outcome was derived in [35], and reads:

$$H(A_0|E) \geq \begin{cases} g'(\beta^*_{\alpha\mathrm{C}})(\beta_{\alpha\mathrm{C}} - 2) & \text{if } |\alpha| < 1 \text{ and } 2 \leq \beta_{\alpha\mathrm{C}} < \beta^*_{\alpha\mathrm{C}} \\ g(\beta_{\alpha\mathrm{C}}) & \text{if } |\alpha| \geq 1 \text{ or } \beta_{\alpha\mathrm{C}} \geq \beta^*_{\alpha\mathrm{C}} \end{cases}, \tag{A.19}$$

where the function $g(x)$ is defined as: $g(x) := 1 - h(1/2 + (1/2)\sqrt{x^2/4 - \alpha^2})$, $g'(x)$ is its first derivative and $\beta^*_{\alpha\mathrm{C}}$ is the solution of the following equation: $g'(x)(x-2) = g(x)$.

For the two-party entropy $H(A_0B_0|E)$, a numerical bound for the case of $\alpha = 1$ (which reduces to the standard CHSH inequality) is obtained in this work (see Appendix D) and agrees with the numerical bound independently derived in [38]. Moreover, for the CHSH inequality a tight analytical lower bound on $H(AB|XYE)$ (where X and Y are Alice's and Bob's inputs) as a function of the CHSH value β_C is conjectured in [38] and reported here:

$$H(AB|XYE) \geq \begin{cases} g_1'(\beta_{\mathrm{C}}^*)(\beta_{\mathrm{C}} - 2) & \text{if } 2 \leq \beta_{\mathrm{C}} \leq \beta_{\mathrm{C}}^* \\ g_1(\beta_{\mathrm{C}}) & \text{if } \beta_{\mathrm{C}}^* < \beta_{\mathrm{C}} \leq 2\sqrt{2} \end{cases}, \tag{A.20}$$

where $g_1(x)$ is defined as $g_1(x) = 1 + h(1/2 + x/8) - 2\,h(1/2 + \sqrt{2}x/8)$, $g_1'(x)$ is its first derivative and β_C^* is the solution of $g_1'(x)(x-2) = g_1(x)$ and is approximately given by $\beta_C^* \approx 2.75$.

B Proof of one-outcome entropy bound for the Holz inequality

In this appendix we prove Theorem 1, i.e., we prove the following lower bound on the von Neumann entropy of Alice's outcome A_0, conditioned on the eavesdropper's total side information E_{tot}, when three parties test the Holz inequality:

$$H(A_0|E_{\mathrm{tot}}) \geq 1 - h\left[\frac{1}{4}\left(\beta_{\mathrm{H}} + 1 + \sqrt{\beta_{\mathrm{H}}^2 + 2\beta_{\mathrm{H}} - 3}\right)\right], \tag{B.1}$$

where $h(x) = -x\log_2 x + (1-x)\log_2(1-x)$ is the binary entropy. Additionally, we prove that the bound above is tight.

Directly performing an analytical minimization of the conditional entropy over every quantum state (of any dimension) and measurement would be prohibitive. Therefore, the first step to prove (B.1) is to simplify the problem at hand.

B.1 Simplification of the problem

Here we simplify the generic quantum state shared by the parties and the form of the Holz inequality, without losing generality.

Holz's Bell inequality [19], for $N = 3$ parties, is given by:

$$\beta_{\mathrm{H}} := \langle A_1B_+C_+\rangle - \langle A_0B_-\rangle - \langle A_0C_-\rangle - \langle B_-C_-\rangle \leq 1, \tag{B.2}$$

where A_i, B_i and C_i (for $i = 0, 1$) are Alice's, Bob's and Charlie's binary observables, respectively, and where we define the unnormalized observables: $B_\pm = (B_0 \pm B_1)/2$ and $C_\pm = (C_0 \pm C_1)/2$.

To start with, we observe that each party holds two observables with binary outcomes. By following the proof of Theorem 1 in [47], it is not restrictive to assume that (in every protocol round) Alice, Bob and Charlie share a mixture of three-qubit states and perform rank-one binary projective measurements on their respective qubits. In particular, due to the DI setting, we allow Eve to be in control of the state preparation and to determine the projective measurements performed by the parties on each state of the mixture. We formalize this by saying that, in each round, Eve distributes the following three-qubit mixture:

$$\rho_{ABC\Xi E'} = \sum_\alpha p_\alpha \rho_\alpha \otimes |\alpha\rangle\langle\alpha|_{\xi_A} \otimes |\alpha\rangle\langle\alpha|_{\xi_B} \otimes |\alpha\rangle\langle\alpha|_{\xi_C} \otimes |\alpha\rangle\langle\alpha|_{E'} \tag{B.3}$$

together with a set of ancillae $\Xi = \{\xi_A, \xi_B, \xi_C\}$ that instruct the parties' devices on the projective measurements to implement on each state ρ_α of the mixture. Recall that Eve knows which state in the mixture gets distributed; this is represented by the classical register $|\alpha\rangle_{E'}$.

The conditional entropy of Alice's outcome A_0 given Eve's total information $E_{\mathrm{tot}} = EE'$ can then be expressed as follows[5]:

$$\begin{aligned} H(A_0|E_{\mathrm{tot}}) &= \sum_\alpha p_\alpha H(A_0|EE' = \alpha) \\ &= \sum_\alpha p_\alpha H(A_0|E)_{\rho_\alpha}, \end{aligned} \tag{B.4}$$

[5] Note that the same result can also be derived from a generic pure state distributed by Eve [35]. In this case, the classical mixture in (B.3) is the result of the block-diagonal measurement of each party (due to Jordan's lemma [48]). Thanks to the concavity of the conditional von Neumann entropy one recovers (B.4).

and we aim at deriving a lower bound on $H(A_0|E_{\text{tot}})$ as a function of the Bell value β_{H} yielded by (B.3). The latter can be expressed in terms of the Bell values $\beta_{\text{H}}^{\alpha}$ yielded by each state ρ_α of the mixture:

$$\beta_{\text{H}} = \sum_\alpha p_\alpha \beta_{\text{H}}^{\alpha}. \tag{B.5}$$

Equations (B.4) and (B.5) allow us to focus on a specific state ρ_α and derive a convex lower bound F on its conditional entropy $H(A_0|E)_{\rho_\alpha}$ in terms of the Bell value $\beta_{\text{H}}^{\alpha}$:

$$H(A_0|E)_{\rho_\alpha} \geq F(\beta_{\text{H}}^{\alpha}). \tag{B.6}$$

Indeed, by combining the above expression with (B.4) and (B.5) and by exploiting the convexity of F, we obtain the desired lower bound:

$$H(A_0|E_{\text{tot}}) \geq F(\beta_{\text{H}}). \tag{B.7}$$

For the above argument, we now focus on a specific three-qubit state ρ_α and derive the convex lower bound (B.6). For ease of notation, in the following we omit the symbol α.

B.1.1 Reduction of the inequality

Lemma 1. *The Bell value of the Holz inequality* (2) *can be reduced without loss of generality to the following form, for some angles a_1, b_-, and c_-,*

$$\beta_{\text{H}} = (\cos a_1 \langle ZXX\rangle + \sin a_1 \langle XXX\rangle)\cos b_- \cos c_- + \sin b_- \langle ZZ\mathbb{1}\rangle + \sin c_- \langle Z\mathbb{1}Z\rangle - \sin b_- \sin c_- \langle \mathbb{1}ZZ\rangle\,, \tag{B.8}$$

where $\mathbb{1}$ is the identity operator.

Proof. We identify the plane induced by the two qubit observables of each party to be the (x, z) plane of the Bloch sphere. Then the parties' observables can be parametrized as follows:

$$A_i = Z\cos a_i + X \sin a_i \tag{B.9}$$
$$B_i = Z\cos b_i + X \sin b_i \tag{B.10}$$
$$C_i = Z\cos c_i + X \sin c_i \tag{B.11}$$

where $a_i, b_i, c_i \in [0, 2\pi]$ and where X, Y and Z are the Pauli operators. By defining the parameters $b_\pm = (b_0 \pm b_1)/2$ and $c_\pm = (c_0 \pm c_1)/2$, we can recast the observables $B_\pm$ and $C_\pm$ as follows:

$$B_+ = \cos b_-(Z\cos b_+ + X\sin b_+) \tag{B.12}$$
$$B_- = -\sin b_-(Z\sin b_+ - X\cos b_+) \tag{B.13}$$
$$C_+ = \cos c_-(Z\cos c_+ + X\sin c_+) \tag{B.14}$$
$$C_- = -\sin c_-(Z\sin c_+ - X\cos c_+). \tag{B.15}$$

By employing the rotational degree of freedom of the local reference frame of each party (rotations around the y axis), we can partially fix the observables (without loss of generality) by rotating Alice's, Bob's and Charlie's reference frames such that:

$$a_0 = 0 \tag{B.16}$$
$$b_+ = c_+ = \frac{\pi}{2}. \tag{B.17}$$

In particular, we have fixed Alice's key generation measurement A_0 to be Z. With the above non-restrictive conditions, we reduce the Bell value of the Holz inequality to the form given in (B.8). □

B.1.2 Reduction of the quantum state

After having reduced the generic quantum state shared by Alice, Bob and Charlie in each round to a mixture of three-qubit states (B.3), here we prove that each state of the mixture, without loss of generality, is diagonal in the GHZ basis except for some real off-diagonal coefficients. The GHZ basis is an orthonormal basis for the Hilbert space of three qubits and is given by $\{|\psi_{i,j,k}\rangle\}_{i,j,k=0}^{1}$, with:

$$|\psi_{i,j,k}\rangle = \frac{1}{\sqrt{2}}\left(|0, j, k\rangle + (-1)^i |1, \bar{j}, \bar{k}\rangle\right), \tag{B.18}$$

where the bar over a bit indicates its negation.

Lemma 2. *Without loss of generality, the three-qubit state shared by Alice, Bob and Charlie can be parametrized as follows:*

$$\rho = \sum_{i,j,k=0}^{1} \lambda_{ijk} |\psi_{i,j,k}\rangle\langle\psi_{i,j,k}| + \sum_{j,k=0}^{1} r_{jk} \left(|\psi_{0,j,k}\rangle\langle\psi_{1,\bar{j},\bar{k}}| + \text{h.c.} \right), \tag{B.19}$$

where λ_{ijk} are the diagonal terms and r_{jk} are real off-diagonal coefficients.

In view of later calculations, we provide the eigenvalues and eigenvectors of the state in (B.19). The eigenvalues $\{\rho_{ijk}\}$ of ρ are given by:

$$\rho_{ijk} = \frac{1}{2} \left(\lambda_{0jk} + \lambda_{1\bar{j}\bar{k}} + (-1)^i \sqrt{(\lambda_{0jk} - \lambda_{1\bar{j}\bar{k}})^2 + 4r_{jk}^2} \right), \tag{B.20}$$

and the corresponding eigenvectors $\{|\rho_{ijk}\rangle\}$ read as follows:

$$\begin{aligned} |\rho_{0jk}\rangle &= \cos(t_{jk}) |\psi_{0,j,k}\rangle + \sin(t_{jk}) |\psi_{1,\bar{j},\bar{k}}\rangle \\ |\rho_{1jk}\rangle &= -\sin(t_{jk}) |\psi_{0,j,k}\rangle + \cos(t_{jk}) |\psi_{1,\bar{j},\bar{k}}\rangle, \end{aligned} \tag{B.21}$$

where t_{jk} is defined as:

$$t_{jk} = \arctan \frac{2r_{jk}}{\lambda_{0jk} - \lambda_{1\bar{j}\bar{k}} + \sqrt{(\lambda_{0jk} - \lambda_{1\bar{j}\bar{k}})^2 + 4r_{jk}^2}}. \tag{B.22}$$

We remark that the two sets of parameters $\{\lambda_{ijk}, r_{jk}\}$ and $\{\rho_{ijk}, t_{jk}\}$ can be used interchangeably to completely describe the state ρ. The inverse relations of (B.20) and (B.22) read as follows:

$$\begin{align} r_{jk} &= \sin(2t_{jk})(\rho_{0jk} - \rho_{1jk}) \tag{B.23} \\ \lambda_{0jk} &= \cos^2(t_{jk})\rho_{0jk} + \sin^2(t_{jk})\rho_{1jk} \tag{B.24} \\ \lambda_{1\bar{j}\bar{k}} &= \cos^2(t_{jk})\rho_{1jk} + \sin^2(t_{jk})\rho_{0jk}. \tag{B.25} \end{align}$$

Proof. We start by noticing that the elements of the GHZ basis are eigenstates of the operators whose expectation value appear in the Holz inequality (B.8), except for ZXX. More specifically, the action of every operator in (B.8) on the GHZ basis reads:

$$\begin{align} XXX |\psi_{i,j,k}\rangle &= (-1)^i |\psi_{i,j,k}\rangle \tag{B.26} \\ ZZ\mathbb{1} |\psi_{i,j,k}\rangle &= (-1)^j |\psi_{i,j,k}\rangle \tag{B.27} \\ Z\mathbb{1}Z |\psi_{i,j,k}\rangle &= (-1)^k |\psi_{i,j,k}\rangle \tag{B.28} \\ \mathbb{1}ZZ |\psi_{i,j,k}\rangle &= (-1)^{j+k} |\psi_{i,j,k}\rangle \tag{B.29} \\ ZXX |\psi_{i,j,k}\rangle &= |\psi_{\bar{i},\bar{j},\bar{k}}\rangle. \tag{B.30} \\ & \tag{B.31} \end{align}$$

Let us now consider the most generic three-qubit state and express it in the GHZ basis:

$$\rho = \sum_{\substack{i,j,k=0 \\ i',j',k'=0}}^{1} \rho_{(ijk),(i'j'k')} |\psi_{i,j,k}\rangle\langle\psi_{i',j',k'}|. \tag{B.32}$$

For the observation above, the only terms in (B.32) that matter in the calculation of the Bell value β_{H} are the diagonal elements $\rho_{(ijk),(ijk)}$ and the coherences $\rho_{(ijk),(\bar{i}\bar{j}\bar{k})}$. Any other term would provide no contribution to the Bell value β_{H}.

Let us denote by ρ' the state with the same matrix elements $\rho_{(ijk),(ijk)}$ and $\rho_{(ijk),(\bar{i}\bar{j}\bar{k})}$ of ρ in the GHZ basis and null elements otherwise. Recall that in the DI scenario Eve is in total control of the quantum channel and can distribute any arbitrary three-qubit state to Alice, Bob and Charlie.

Reduction to block-diagonal state

Here we show that we can assume, without loss of generality, that Eve distributes the state ρ' in place of the generic state ρ. This is so because, by construction, the Bell value observed by the parties would not change if they are given ρ' instead of ρ. Moreover, Eve's uncertainty about Alice's outcome when she measures Z would not increase. More formally we show that:

$$H(Z|E)_\rho \geq H(Z|E)_{\rho'}. \tag{B.33}$$

In order to show (B.33), we first derive the quantum map $\mathcal{D}$ that brings any generic state ρ to ρ', i.e., that sets to zero every coherence of ρ in the GHZ basis except for $\rho_{(ijk),(\bar{i}\bar{j}\bar{k})}$, while leaving the diagonal elements untouched. The map $\mathcal{D}$ can be better understood as a composition of two consecutive maps. The first map acts as follows on the generic state ρ:

$$\rho \mapsto \frac{1}{2}\rho + \frac{1}{2}\mathbb{1}ZZ\rho\mathbb{1}ZZ, \tag{B.34}$$

so that any off-diagonal term in (B.32) with $j+k \neq j'+k'$ is set to zero, while the other terms are not affected. The second map is given by:

$$\rho \mapsto \frac{1}{2}\rho + \frac{1}{2}YYX\rho YYX, \tag{B.35}$$

so that every coherence with $i+j \neq i'+j'$ is set to zero[6]. The combined effect of (B.34) and (B.35) is exactly the desired map $\mathcal{D}$. We can express the action of $\mathcal{D}$ in a more compact form as follows:

$$\begin{aligned}\mathcal{D}(\rho) &= \frac{1}{4}\left(\rho + \mathbb{1}ZZ\rho\mathbb{1}ZZ + YYX\rho YYX + YXY\rho YXY\right) && \text{(B.36)}\\ &= \sum_{i,j,k=0}^{1} \rho_{(ijk),(ijk)}|\psi_{i,j,k}\rangle\langle\psi_{i,j,k}| + \rho_{(ijk),(\bar{i}\bar{j}\bar{k})}|\psi_{i,j,k}\rangle\langle\psi_{\bar{i},\bar{j},\bar{k}}|, && \text{(B.37)}\end{aligned}$$

and we have that $\rho' = \mathcal{D}(\rho)$. We can now prove (B.33).

To start with, we interpret the state $\mathcal{D}(\rho)$ in (B.36) as Eve preparing one of the four states (ρ, $\mathbb{1}ZZ\rho\mathbb{1}ZZ$, $YYX\rho YYX$ and $YXY\rho YXY$) in the mixture according to the value t of a random variable T known to her. We generically indicate each of the four states as ρ^t, for different values of t. Since we provide Eve with maximum power, we assume that she holds the purification $|\phi^t_{ABCE}\rangle$ of each ρ^t. Therefore, the global quantum state Eve produces reads:

$$\rho_{ABCET} = \frac{1}{4}\sum_t |\phi^t_{ABCE}\rangle\langle\phi^t_{ABCE}| \otimes |t\rangle\langle t|_T, \tag{B.38}$$

where the classical register T storing the value t is held by Eve. Finally, Eve also holds the purifying system T' of (B.38), such that the global state reads:

$$\rho_{ABCETT'} = \frac{1}{2}\sum_t |\phi^t_{ABCE}\rangle \otimes |t\rangle_T \otimes |t\rangle_{T'}, \tag{B.39}$$

where the total information available to Eve is $E_{\text{tot}} = ETT'$. Then, by the strong subadditivity property, we can upper bound the conditional entropy computed on $\rho' = \mathcal{D}(\rho)$ as follows:

$$H(Z|E_{\text{tot}})_{\mathcal{D}(\rho)} \leq H(Z|ET)_{\mathcal{D}(\rho)}, \tag{B.40}$$

where the entropy on the rhs is computed on the state:

$$\begin{aligned}\rho_{ZET} &= \frac{1}{4}\sum_t \mathrm{Tr}_{BC}\left[(\mathcal{E}_Z \otimes \mathbb{1}_{BCE})|\phi^t_{ABCE}\rangle\langle\phi^t_{ABCE}|\right] \otimes |t\rangle\langle t|_T \\ &=: \frac{1}{4}\sum_t \rho^t_{ZE} \otimes |t\rangle\langle t|_T, && \text{(B.41)}\end{aligned}$$

where $\mathcal{E}_Z$ is the quantum map describing Alice's Z measurement and where we implicitly defined the state ρ^t_{ZE}.

Since Alice's Z measurement is a projection on the computational basis states of subsystem A, we can recast ρ^t_{ZE} as follows:

$$\rho^t_{ZE} = \sum_{z=0,1} |z\rangle\langle z|_Z \otimes \mathrm{Tr}_{BC}[\langle z|\phi^t_{ABCE}\rangle\,\langle\phi^t_{ABCE}|z\rangle]. \tag{B.42}$$

[6] Note that $YYX\,|\psi_{i,j,k}\rangle = -(-1)^{i+j}\,|\psi_{i,j,k}\rangle$.

Let us now fix for concreteness the value of t such that $|\phi^t_{ABCE}\rangle$ is the purification of the state $YYX\rho YYX$. Nevertheless, our conclusions hold for any other state of the mixture (B.36). Then we have that:

$$|\phi^t_{ABCE}\rangle = \sum_\lambda \sqrt{\lambda}\, YYX \,|\lambda\rangle_{ABC} \otimes |e_\lambda\rangle_E \tag{B.43}$$

when the spectral decomposition of ρ reads $\rho = \sum_\lambda \lambda|\lambda\rangle\langle\lambda|$ and with $\{|e_\lambda\rangle\}$ an orthonormal basis for E. By substituting (B.43) into (B.42) we obtain:

$$\rho^t_{ZE} = \sum_{z=0,1} |z\rangle\langle z|_Z \otimes \sum_{\lambda,\sigma} \sqrt{\lambda\sigma}\, \mathrm{Tr}_{BC}[\langle z|\, YYX|\lambda\rangle\langle\sigma|YYX\,|z\rangle] \otimes |e_\lambda\rangle\langle e_\sigma|_E. \tag{B.44}$$

By using the cyclic property of the trace on BC and the fact that $Y\,|z\rangle = \mathbb{i}(-1)^z\,|\bar{z}\rangle$ (we indicate the imaginary unit with $\mathbb{i}$), we can simplify the previous expression as follows:

$$\begin{aligned}\rho^t_{ZE} &= \sum_{z=0,1} |z\rangle\langle z|_Z \otimes \sum_{\lambda,\sigma} \sqrt{\lambda\sigma}\, \mathrm{Tr}_{BC}[\langle\bar{z}|\lambda\rangle\,\langle\sigma|\bar{z}\rangle] \otimes |e_\lambda\rangle\langle e_\sigma|_E \\ &= \sum_{z=0,1} |\bar{z}\rangle\langle \bar{z}|_Z \otimes \sum_{\lambda,\sigma} \sqrt{\lambda\sigma}\, \mathrm{Tr}_{BC}[\langle z|\lambda\rangle\,\langle\sigma|z\rangle] \otimes |e_\lambda\rangle\langle e_\sigma|_E\end{aligned} \tag{B.45}$$

Being ρ_{ZET} classical on subsystem T (B.41), we can compute its conditional entropy as follows:

$$H(Z|ET)_{\mathcal{D}(\rho)} = \frac{1}{4}\sum_t H(Z|E)_{\rho^t}, \tag{B.46}$$

i.e., as the average over t of the entropies of (B.45). However, from (B.45) we deduce that the states ρ^t_{ZE} are all the same up to a relabeling of the classical register Z. Therefore, they lead to the same conditional entropy $H(Z|E)_{\rho^t} = H(Z|E)_\rho$ which is just the conditional entropy of the original state ρ. By employing this observation in (B.46) we can write:

$$H(Z|ET)_{\mathcal{D}(\rho)} = H(Z|E)_\rho. \tag{B.47}$$

Finally, by combining the last expression with (B.40), we obtain (B.33). We thus proved that it is not restrictive to assume that the parties are given a block-diagonal state of the form (B.37). In order to continue with the proof, we relabel the non-null matrix elements of the distributed state in terms of real numbers:

$$\rho' = \sum_{i,j,k=0}^{1} \lambda_{ijk}|\psi_{i,j,k}\rangle\langle\psi_{i,j,k}| + \sum_{j,k=0}^{1} (r_{jk} + \mathbb{i}s_{jk})|\psi_{0,j,k}\rangle\langle\psi_{1,\bar{j},\bar{k}}| + \text{h.c.} \tag{B.48}$$

where λ_{ijk}, r_{jk} and s_{jk} are real numbers and h.c. indicates the Hermitian conjugate of the preceding addend.

Reduction to purely-real coherences

Here we show that, without loss of generality, we can assume that $s_{jk} = 0$ for every j and k in (B.48). That is, the state shared by the parties only displays real off-diagonal elements.

We start by computing the Bell value (B.8) on the state ρ'. One obtains:

$$\begin{aligned}(\beta_{\mathrm{H}})_{\rho'} = \sum_{i,j,k=0}^{1} \lambda_{ijk}\left[(-1)^i \sin a_1 \cos b_- \cos c_- + (-1)^j \sin b_- + (-1)^k \sin c_- - (-1)^{j+k} \sin b_- \sin c_-\right] \\ + 2r_{jk} \cos a_1 \cos b_- \cos c_-.\end{aligned} \tag{B.49}$$

We observe that $(\beta_{\mathrm{H}})_{\rho'}$ is independent of the imaginary component of the coherences of ρ', therefore it would read the same when computed for the complex conjugate of ρ' with respect to the GHZ basis, namely

$$(\rho')^* = \sum_{i,j,k=0}^{1} \lambda_{ijk}|\psi_{i,j,k}\rangle\langle\psi_{i,j,k}| + \sum_{j,k=0}^{1} (r_{jk} - \mathbb{i}s_{jk})|\psi_{0,j,k}\rangle\langle\psi_{1,\bar{j},\bar{k}}| + \text{h.c.} \tag{B.50}$$

Moreover, note that the states ρ'_{ZE} and $(\rho'_{ZE})^*$ –obtained from (B.48) and (B.50) after purification, Alice's Z measurement and partial trace over BC– are still the complex conjugate of each other with respect to the orthonormal basis of E used for the purification. Given that ρ'_{ZE} is Hermitian, this implies that $(\rho'_{ZE})^*$ is also the transposed of ρ'_{ZE} with respect to the same basis. Since a matrix and its transpose have the same eigenvalues, their von Neumann entropies must coincide:

$$H(Z|E)_{\rho'} = H(Z|E)_{(\rho')^*}. \tag{B.51}$$

We conclude that ρ' and $(\rho')^*$ lead to the same Bell value $(\beta_\mathrm{H})_{\rho'}$ and provide Eve with the same amount of information about Alice's Z outcome. This means that Eve has no preference in preparing ρ' rather than $(\rho')^*$. As a matter of fact, we can assume without loss of generality that Eve prepares a balanced mixture of the two states:

$$\bar{\rho} := \frac{\rho' + (\rho')^*}{2}. \tag{B.52}$$

Indeed, the Bell value $(\beta_\mathrm{H})_{\bar{\rho}}$ would be unchanged ($(\beta_\mathrm{H})_{\bar{\rho}} = (\beta_\mathrm{H})_{\rho'}$) and Eve's uncertainty would not increase:

$$H(Z|E)_{\rho'} \geq H(Z|E_\mathrm{tot})_{\bar{\rho}}. \tag{B.53}$$

In order to verify the above inequality, we interpret $\bar{\rho}$ as Eve preparing the purifications $|\varphi_{ABCE}\rangle$ and $|\varphi^*_{ABCE}\rangle$ of ρ' and $(\rho')^*$, respectively, according to the value of a classical random variable T known to her:

$$\frac{1}{2}|\varphi_{ABCE}\rangle\langle\varphi_{ABCE}|\otimes|0\rangle\langle 0|_T + \frac{1}{2}|\varphi^*_{ABCE}\rangle\langle\varphi^*_{ABCE}|\otimes|1\rangle\langle 1|_T. \tag{B.54}$$

Moreover, we provide Eve with the purifying system T' of the above quantum state. Thus, similarly to (B.39), the global quantum state prepared by Eve reads:

$$\frac{1}{\sqrt{2}}\,|\varphi_{ABCE}\rangle \otimes |0\rangle_T \otimes |0\rangle_{T'} + \frac{1}{\sqrt{2}}\,|\varphi^*_{ABCE}\rangle \otimes |1\rangle_T \otimes |1\rangle_{T'} \tag{B.55}$$

and she holds systems $E_\mathrm{tot} = ETT'$. By the strong subadditivity property and the fact that the states are classical on T, we can upper bound the rhs of (B.53) by:

$$\begin{aligned} H(Z|E_\mathrm{tot})_{\bar{\rho}} \leq H(Z|ET)_{\bar{\rho}} &= \frac{1}{2}H(Z|E)_{\rho'} + \frac{1}{2}H(Z|E)_{(\rho')^*} \\ &= H(Z|E)_{\rho'}, \end{aligned} \tag{B.56}$$

where we used (B.51) in the last equality. This proves (B.53). Hence, without loss of generality the three-qubit state shared by Alice, Bob and Charlie is given by (B.52), which is exactly the state given in (B.19). □

B.2 Derivation of the bound

Having simplified the inequality (Lemma 1) and the form of a generic three-qubit state (Lemma 2) shared by Alice, Bob and Charlie, we are now ready to prove Theorem 1.

The bound derivation is based on a recent technique presented in [35]. The main idea is to lower bound the conditional entropy in terms of a certain expectation value appearing in the Holz inequality, via the uncertainty relation for von Neumann entropies [49]. The proof is then completed by relating the chosen expectation value to the whole Bell value of the Holz inequality.

Proof of Theorem 1. In Subsec. B.1 we show that it is not restrictive to assume that the state shared by Alice, Bob and Charlie is a mixture of three-qubit states. We now focus on a single element of the mixture, ρ_{ABC}, and on its extension ρ_{ABCE} that accounts for Eve's quantum side information.

Since we fixed $A_0 = Z$ as Alice's key generation measurement, we are interested in finding a lower bound on the conditional von Neumann entropy of Alice's key generation outcome given Eve's quantum side information, $H(Z|E)$. The uncertainty relation in the presence of quantum memories [49] states that:

$$H(Z|E) \geq 1 - H(X|BC), \tag{B.57}$$

where $H(X|BC)$ is the entropy of Alice's outcome if she measures X on her qubit, given the quantum side information of Bob and Charlie. By the fact that quantum operations can only increase the conditional entropy when applied to the conditioning system (see e.g. Theorem 11.15 in [58]), we have that:

$$H(X|BC) \leq H(X|X_B X_C) \leq H(X|X_{BC}), \tag{B.58}$$

where X_B (X_C) represents Bob's (Charlie's) outcome upon measuring in the X basis and X_{BC} is a classical random variable defined as the multiplication of X_B and X_C, $X_{BC} = X_B X_C$. Then, thanks to Fano's inequality, the Shannon entropy on the rhs of (B.58) can be bounded by the binary entropy of the probability that X differs from X_{BC}, namely:

$$H(X|X_{BC}) \leq h(Q_X), \tag{B.59}$$

with $Q_X = \Pr[XX_BX_C = -1] = (1-\langle XXX\rangle)/2$ (where XXX is intended as the product of the X outcomes of Alice, Bob and Charlie). By combining (B.58) and (B.59), we obtain the following upper bound on $H(X|BC)$:

$$\begin{aligned} H(X|BC) &\leq h\left(\frac{1-\langle XXX\rangle}{2}\right) \\ &= h\left(\frac{1-|\langle XXX\rangle|}{2}\right) \\ &= h\left(\frac{1+|\langle XXX\rangle|}{2}\right), \end{aligned} \tag{B.60}$$

where we used the fact that $h(1/2-p/2)$ is symmetric in p in the first equality and that $h(p)=h(1-p)$ in the second equality.

By combining (B.57) and (B.60) we derive the following lower bound on $H(Z|E)$:

$$H(Z|E) \geq 1 - h\left(\frac{1+|\langle XXX\rangle|}{2}\right). \tag{B.61}$$

The rest of the proof focuses on proving the following inequality between the expectation value $\langle XXX\rangle$ and the Bell value β_{H} of the Holz inequality:

$$|\langle XXX\rangle| \geq \frac{\beta_{\mathrm{H}}}{2} - \frac{1}{2} + \frac{1}{2}\sqrt{\beta_{\mathrm{H}}^2 + 2\beta_{\mathrm{H}} - 3}. \tag{B.62}$$

Indeed, by employing (B.62) in (B.61) we obtain the desired lower bound on the conditional entropy (B.1).

We implicitly assume throughout the proof that $\beta_{\mathrm{H}} > 1$, otherwise without Bell violation the conditional entropy is trivially bounded by zero. Moreover we assume that every inequality is to be proven for every value of its parameters, unless otherwise stated.

To start with, we recast the inequality to be proven (B.62) as follows:

$$2\,|\langle XXX\rangle| + 1 - \beta_{\mathrm{H}} \geq \sqrt{\beta_{\mathrm{H}}^2 + 2\beta_{\mathrm{H}} - 3}, \tag{B.63}$$

which is true if and only if the following system of inequalities is true:

$$\begin{cases} (2\,|\langle XXX\rangle| + 1 - \beta_{\mathrm{H}})^2 \geq \beta_{\mathrm{H}}^2 + 2\beta_{\mathrm{H}} - 3 & \text{(B.64a)} \\ 2\,|\langle XXX\rangle| + 1 - \beta_{\mathrm{H}} \geq 0 & \text{(B.64b)} \end{cases}$$

First we focus on proving (B.64b). A sufficient condition for proving (B.64b) is given by:

$$|\langle XXX\rangle| + \langle XXX\rangle \sin a_1 \cos b_- \cos c_- + 1 - \beta_{\mathrm{H}} \geq 0, \tag{B.65}$$

which reads as follows after employing (B.8):

$$1 + |\langle XXX\rangle| \geq \cos a_1 \cos b_- \cos c_- \langle ZXX\rangle + \sin b_- \langle ZZ\mathbb{1}\rangle + \sin c_- \langle Z\mathbb{1}Z\rangle - \sin b_- \sin c_- \langle \mathbb{1}ZZ\rangle. \tag{B.66}$$

The inequality in (B.66) is implied by another inequality, namely:

$$1 \geq |\cos b_- \cos c_- \langle ZXX\rangle| + \sin b_- \langle ZZ\mathbb{1}\rangle + \sin c_- \langle Z\mathbb{1}Z\rangle - \sin b_- \sin c_- \langle \mathbb{1}ZZ\rangle. \tag{B.67}$$

Thus, it is sufficient that we prove the following inequality:

$$C := \cos b_- \cos c_- \langle ZXX\rangle + \sin b_- \langle ZZ\mathbb{1}\rangle + \sin c_- \langle Z\mathbb{1}Z\rangle - \sin b_- \sin c_- \langle \mathbb{1}ZZ\rangle \leq 1 \tag{B.68}$$

for *every* value of b_- and c_- in order to show that (B.67), and hence (B.66), holds. Indeed, the first term in (B.68) can always be made equal to $|\cos b_- \cos c_- \langle ZXX\rangle|$ by replacing b_- with $\pi - b_-$ if the term is negative. Note that this replacement does not affect the other terms.

To show that (B.68) holds, we start by exploiting the inverse relations (B.23), (B.24) and (B.25), we compute the expectation values in (B.68) in terms of the parameters $\{\rho_{ijk}, t_{jk}\}$ describing the shared state ρ. We obtain:

$$\langle ZXX\rangle = \sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) \sin(2t_{jk}) \tag{B.69}$$

$$\langle ZZ\mathbb{1}\rangle = \sum_{j,k=0}^{1} (-1)^j (\rho_{0jk} - \rho_{1jk}) \cos(2t_{jk}) \tag{B.70}$$

$$\langle Z\mathbb{1}Z\rangle = \sum_{j,k=0}^{1} (-1)^k (\rho_{0jk} - \rho_{1jk}) \cos(2t_{jk}) \tag{B.71}$$

$$\langle \mathbb{1}ZZ\rangle = \sum_{j,k=0}^{1} (-1)^{j+k} (\rho_{0jk} + \rho_{1jk}). \tag{B.72}$$

By inserting the expectation values in the lhs of (B.68) we get:

$$\begin{aligned} C = &\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) \left[\sin(2t_{jk}) \cos b_- \cos c_- + (-1)^j \cos(2t_{jk}) \sin b_- + (-1)^k \cos(2t_{jk}) \sin c_-\right] \\ &- \sum_{j,k=0}^{1} (-1)^{j+k} (\rho_{0jk} + \rho_{1jk}) \sin b_- \sin c_-. \end{aligned} \tag{B.73}$$

We upper bound C by maximizing it over t_{jk}. In doing so we use the fact that $\rho_{0jk} \geq \rho_{1jk}$ and that $A\cos\theta + B\sin\theta \leq \sqrt{A^2 + B^2}$. We thus obtain:

$$\begin{aligned} C \leq &\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) \sqrt{\cos^2 b_- \cos^2 c_- + \sin^2 b_- + \sin^2 c_- + 2(-1)^{j+k} \sin b_- \sin c_-} \\ &- \sum_{j,k=0}^{1} (-1)^{j+k} (\rho_{0jk} + \rho_{1jk}) \sin b_- \sin c_- \\ = &\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) \sqrt{\cos^2 c_- + \sin^2 b_- (1 - \cos^2 c_-) + \sin^2 c_- + 2(-1)^{j+k} \sin b_- \sin c_-} \\ &- \sum_{j,k=0}^{1} (-1)^{j+k} (\rho_{0jk} + \rho_{1jk}) \sin b_- \sin c_- \\ = &\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) \sqrt{1 + \sin^2 b_- \sin^2 c_- + 2(-1)^{j+k} \sin b_- \sin c_-} - \sum_{j,k=0}^{1} (-1)^{j+k} (\rho_{0jk} + \rho_{1jk}) \sin b_- \sin c_- \\ = &\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) \left[1 + (-1)^{j+k} \sin b_- \sin c_-\right] - \sum_{j,k=0}^{1} (-1)^{j+k} (\rho_{0jk} + \rho_{1jk}) \sin b_- \sin c_- \\ = &\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) + \sum_{j,k=0}^{1} (-1)^{j+k} \sin b_- \sin c_- (\rho_{0jk} - \rho_{1jk} - \rho_{0jk} - \rho_{1jk}) \\ \leq &\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) + 2 \left| \sum_{j,k=0}^{1} (-1)^{j+k} \rho_{1jk} \right| \\ \leq &\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) + 2 \sum_{j,k=0}^{1} \rho_{1jk} \\ = &\sum_{i,j,k=0}^{1} \rho_{ijk} = 1, \end{aligned} \tag{B.74}$$

where we maximized over b_- and c_- in the second inequality, used the fact that $\rho_{ijk} \geq 0$ in the third inequality and that the eigenvalues ρ_{ijk} of ρ sum to one in the last equality. We proved (B.68) and thus proved (B.64b).

We now focus on proving (B.64a). By computing the square in the lhs of (B.64a), we can recast the inequality as follows:

$$(1+|\langle XXX\rangle|)\,\beta_{\mathrm{H}} \le 1+|\langle XXX\rangle|+\langle XXX\rangle^2\,. \tag{B.75}$$

We now insert (B.8) into the above expression and obtain:

$$\begin{aligned}
&(1+|\langle XXX\rangle|)\\
&(\cos a_1\cos b_-\cos c_-\,\langle ZXX\rangle+\sin a_1\cos b_-\cos c_-\,\langle XXX\rangle+\sin b_-\,\langle ZZ\mathbb{1}\rangle+\sin c_-\,\langle Z\mathbb{1}Z\rangle-\sin b_-\sin c_-\,\langle \mathbb{1}ZZ\rangle)\\
&\le 1+|\langle XXX\rangle|+\langle XXX\rangle^2
\end{aligned} \tag{B.76}$$

Now consider that the above inequality must be proven true for every value of a_1. In particular it must hold true for a_1 and $2\pi-a_1$, which is equivalent to having an arbitrary sign for the second term in the second bracket. Then, we can equivalently express the fact that (B.76) must hold for every a_1 as the requirement that the following inequality holds for every a_1:

$$\begin{aligned}
&(1+|\langle XXX\rangle|)\\
&(\cos a_1\cos b_-\cos c_-\,\langle ZXX\rangle+\sin a_1\cos b_-\cos c_-\,|\langle XXX\rangle|+\sin b_-\,\langle ZZ\mathbb{1}\rangle+\sin c_-\,\langle Z\mathbb{1}Z\rangle-\sin b_-\sin c_-\,\langle \mathbb{1}ZZ\rangle)\\
&\le 1+|\langle XXX\rangle|+\langle XXX\rangle^2\,,
\end{aligned} \tag{B.77}$$

where we replaced $\langle XXX\rangle$ with $|\langle XXX\rangle|$ in the second term of the second bracket. By rearranging the terms in (B.77) we obtain:

$$\begin{aligned}
&|\langle XXX\rangle|^2\,(1-\sin a_1\cos b_-\cos c_-)+|\langle XXX\rangle|\\
&(1-\sin a_1\cos b_-\cos c_- -\cos a_1\cos b_-\cos c_-\,\langle ZXX\rangle-\sin b_-\,\langle ZZ\mathbb{1}\rangle-\sin c_-\,\langle Z\mathbb{1}Z\rangle+\sin b_-\sin c_-\,\langle \mathbb{1}ZZ\rangle)\\
&+1-\cos a_1\cos b_-\cos c_-\,\langle ZXX\rangle-\sin b_-\,\langle ZZ\mathbb{1}\rangle-\sin c_-\,\langle Z\mathbb{1}Z\rangle+\sin b_-\sin c_-\,\langle \mathbb{1}ZZ\rangle\ge 0.
\end{aligned} \tag{B.78}$$

A sufficient condition for (B.78) to be true is when the second degree equation, obtained by replacing $|\langle XXX\rangle|$ with a generic variable x and taking the equals sign in (B.78), has no solution or only one solution in $\mathbb{R}$. Indeed, in that case the parabola defined by the lhs of (B.78) never intersects the x axis and always sits above zero (except at most in one point), thus proving the inequality[7]. Therefore, a sufficient condition for (B.78) to be true is having the discriminant of the second degree equation smaller or equal to zero:

$$\begin{aligned}
&(1-\sin a_1\cos b_-\cos c_- -\cos a_1\cos b_-\cos c_-\,\langle ZXX\rangle-\sin b_-\,\langle ZZ\mathbb{1}\rangle-\sin c_-\,\langle Z\mathbb{1}Z\rangle+\sin b_-\sin c_-\,\langle \mathbb{1}ZZ\rangle)^2\\
&-4(1-\sin a_1\cos b_-\cos c_-)(1-\cos a_1\cos b_-\cos c_-\,\langle ZXX\rangle-\sin b_-\,\langle ZZ\mathbb{1}\rangle-\sin c_-\,\langle Z\mathbb{1}Z\rangle+\sin b_-\sin c_-\,\langle \mathbb{1}ZZ\rangle)\le 0,
\end{aligned} \tag{B.79}$$

which can be rewritten as

$$\begin{aligned}
&(1-\sin a_1\cos b_-\cos c_- +\cos a_1\cos b_-\cos c_-\,\langle ZXX\rangle+\sin b_-\,\langle ZZ\mathbb{1}\rangle+\sin c_-\,\langle Z\mathbb{1}Z\rangle-\sin b_-\sin c_-\,\langle \mathbb{1}ZZ\rangle)^2\\
&\le 4(1-\sin a_1\cos b_-\cos c_-),
\end{aligned} \tag{B.80}$$

and hence as

$$\begin{aligned}
&|1-\sin a_1\cos b_-\cos c_- +\cos a_1\cos b_-\cos c_-\,\langle ZXX\rangle+\sin b_-\,\langle ZZ\mathbb{1}\rangle+\sin c_-\,\langle Z\mathbb{1}Z\rangle-\sin b_-\sin c_-\,\langle \mathbb{1}ZZ\rangle|\\
&\le 2\sqrt{1-\sin a_1\cos b_-\cos c_-}.
\end{aligned} \tag{B.81}$$

We now remove the absolute value by splitting the previous inequality into an equivalent system of inequalities:

$$\begin{cases}
1-\sin a_1\cos b_-\cos c_- +\cos a_1\cos b_-\cos c_-\,\langle ZXX\rangle+\sin b_-\,\langle ZZ\mathbb{1}\rangle+\sin c_-\,\langle Z\mathbb{1}Z\rangle-\sin b_-\sin c_-\,\langle \mathbb{1}ZZ\rangle\\
\le 2\sqrt{1-\sin a_1\cos b_-\cos c_-} & \text{(B.82a)}\\
-(1-\sin a_1\cos b_-\cos c_- +\cos a_1\cos b_-\cos c_-\,\langle ZXX\rangle+\sin b_-\,\langle ZZ\mathbb{1}\rangle+\sin c_-\,\langle Z\mathbb{1}Z\rangle-\sin b_-\sin c_-\,\langle \mathbb{1}ZZ\rangle)\\
\le 2\sqrt{1-\sin a_1\cos b_-\cos c_-} & \text{(B.82b)}
\end{cases}$$

which can be rearranged as follows:

$$\begin{cases}
\cos a_1\cos b_-\cos c_-\,\langle ZXX\rangle+\sin b_-\,\langle ZZ\mathbb{1}\rangle+\sin c_-\,\langle Z\mathbb{1}Z\rangle-\sin b_-\sin c_-\,\langle \mathbb{1}ZZ\rangle\\
\le \sqrt{1-\sin a_1\cos b_-\cos c_-}(2-\sqrt{1-\sin a_1\cos b_-\cos c_-}) & \text{(B.83a)}\\
-\cos a_1\cos b_-\cos c_-\,\langle ZXX\rangle-\sin b_-\,\langle ZZ\mathbb{1}\rangle-\sin c_-\,\langle Z\mathbb{1}Z\rangle+\sin b_-\sin c_-\,\langle \mathbb{1}ZZ\rangle\\
\le \sqrt{1-\sin a_1\cos b_-\cos c_-}(2+\sqrt{1-\sin a_1\cos b_-\cos c_-}). & \text{(B.83b)}
\end{cases}$$

[7] We can conclude this since the parabola described by the lhs of (B.78) is concave upward, which we deduce from the positivity of the coefficient of $\langle XXX\rangle^2$. In the special case where $\sin a_1\cos b_-\cos c_-=1$, the inequality (B.78) is trivially satisfied.

We emphasize that once we prove (B.83a) and (B.83b) we are done, since this is a sufficient condition for the validity of (B.64a).

We first observe that (B.83a), together with a simple inequality to be proved, implies (B.83b). In order to see this, let us label the lhs and rhs of (B.83a) as l and r, respectively, so that (B.83a) can be written as $l \leq r$. Now notice that since (B.83b) must be proved for every angle a_1, b_- and c_-, we can obtain an equivalent inequality by replacing $a_1 \to \pi - a_1$, $b_- \to -b_-$ and $c_- \to -c_-$ and requiring that the new inequality is satisfied for every a_1, b_- and c_-. The resulting inequality reads:

$$\begin{aligned}\cos a_1 \cos b_- \cos c_- \langle ZXX\rangle + \sin b_- \langle ZZ\mathbb{1}\rangle + \sin c_- \langle Z\mathbb{1}Z\rangle + \sin b_- \sin c_- \langle \mathbb{1}ZZ\rangle \\ \leq \sqrt{1 - \sin a_1 \cos b_- \cos c_-}(2 + \sqrt{1 - \sin a_1 \cos b_- \cos c_-}),\end{aligned} \tag{B.84}$$

and can be recast in terms of l and r as follows:

$$l + 2 \sin b_- \sin c_- \langle \mathbb{1}ZZ\rangle \leq r + 2(1 - \sin a_1 \cos b_- \cos c_-). \tag{B.85}$$

Now assuming that (B.83a) holds, (B.84) –and hence (B.83b)– follows upon proving that the following inequality is true:

$$\sin b_- \sin c_- \langle \mathbb{1}ZZ\rangle \leq 1 - \sin a_1 \cos b_- \cos c_-. \tag{B.86}$$

The proof of (B.86) is easily obtained from the following sufficient condition for its validity:

$$|\sin b_- \sin c_-| + |\cos b_- \cos c_-| \leq 1, \tag{B.87}$$

which is trivially true for $b_-, c_- \in [0, \pi/2]$ since

$$1 \geq \cos(b_- - c_-) = \sin b_- \sin c_- + \cos b_- \cos c_- = |\sin b_- \sin c_-| + |\cos b_- \cos c_-|\,. \tag{B.88}$$

Note that for angles outside the interval $[0, \pi/2]$ similar arguments can be made.

We are thus left to prove that (B.83a) holds. In order to do so, we again express the expectation values in (B.83a) in terms of the parameters describing the shared state ρ:

$$\begin{aligned}&\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) \left[\cos a_1 \cos b_- \cos c_- \sin(2t_{jk}) + (-1)^j \sin b_- \cos(2t_{jk}) + (-1)^k \sin c_- \cos(2t_{jk})\right] \\ &- \sum_{j,k=0}^{1} (-1)^{j+k} (\rho_{0jk} + \rho_{1jk}) \sin b_- \sin c_- \leq \sqrt{1 - \sin a_1 \cos b_- \cos c_-}(2 - \sqrt{1 - \sin a_1 \cos b_- \cos c_-})\end{aligned} \tag{B.89}$$

We find a sufficient condition for (B.89) by maximizing the lhs over t_{jk}. In doing so, we use the fact that $\rho_{0jk} \geq \rho_{1jk}$ and that $A \cos\theta + B \sin\theta \leq \sqrt{A^2 + B^2}$. We obtain:

$$\begin{aligned}&\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) \sqrt{\cos^2 a_1 \cos^2 b_- \cos^2 c_- + \sin^2 b_- + \sin^2 c_- + 2(-1)^{j+k} \sin b_- \sin c_-} \\ &- \sum_{j,k=0}^{1} (-1)^{j+k} (\rho_{0jk} + \rho_{1jk}) \sin b_- \sin c_- \leq \sqrt{1 - \sin a_1 \cos b_- \cos c_-}(2 - \sqrt{1 - \sin a_1 \cos b_- \cos c_-}).\end{aligned} \tag{B.90}$$

In turn, a sufficient condition for (B.90) is given by:

$$\begin{aligned}&\sum_{j,k=0}^{1} \tau_{jk} \left[\sqrt{\cos^2 a_1 \cos^2 b_- \cos^2 c_- + \sin^2 b_- + \sin^2 c_- + 2(-1)^{j+k} \sin b_- \sin c_-} - (-1)^{j+k} \sin b_- \sin c_-\right] \\ &\leq \sqrt{1 - \sin a_1 \cos b_- \cos c_-}(2 - \sqrt{1 - \sin a_1 \cos b_- \cos c_-}),\end{aligned} \tag{B.91}$$

where we defined $\tau_{jk} := \rho_{0jk} + \rho_{1jk}$. We recast (B.91) in the following chain of equivalent inequalities:

$$\begin{aligned}
&\sum_{j,k=0}^{1} \tau_{jk} \Big[\sqrt{(1-\sin^2 b_-)\cos^2 c_- + \sin^2 b_- + \sin^2 c_- + 2(-1)^{j+k}\sin b_- \sin c_- - \sin^2 a_1 \cos^2 b_- \cos^2 c_-} \\
&-(-1)^{j+k}\sin b_- \sin c_-\Big] \leq \sqrt{1-\sin a_1 \cos b_- \cos c_-}\,(2-\sqrt{1-\sin a_1 \cos b_- \cos c_-}) \\
\Leftrightarrow\ &\sum_{j,k=0}^{1} \tau_{jk} \left[\sqrt{1+\sin^2 b_- \sin^2 c_- + 2(-1)^{j+k}\sin b_- \sin c_- - \sin^2 a_1 \cos^2 b_- \cos^2 c_-} - (-1)^{j+k}\sin b_- \sin c_-\right] \\
&\leq \sqrt{1-\sin a_1 \cos b_- \cos c_-}\,(2-\sqrt{1-\sin a_1 \cos b_- \cos c_-}) \\
\Leftrightarrow\ &\sum_{j,k=0}^{1} \tau_{jk} \left[\sqrt{(1+(-1)^{j+k}\sin b_- \sin c_-)^2 - \sin^2 a_1 \cos^2 b_- \cos^2 c_-} - (-1)^{j+k}\sin b_- \sin c_-\right] \\
&\leq \sqrt{1-\sin a_1 \cos b_- \cos c_-}\,(2-\sqrt{1-\sin a_1 \cos b_- \cos c_-}) \\
\Leftrightarrow\ &(\tau_{00}+\tau_{11})A + (\tau_{01}+\tau_{10})B \leq \sqrt{1-\sin a_1 \cos b_- \cos c_-}\,(2-\sqrt{1-\sin a_1 \cos b_- \cos c_-}) \qquad \text{(B.92)}
\end{aligned}$$

where in the last inequality we defined:

$$A := \sqrt{(1+\sin b_- \sin c_-)^2 - \sin^2 a_1 \cos^2 b_- \cos^2 c_-} - \sin b_- \sin c_- \qquad \text{(B.93)}$$

$$B := \sqrt{(1-\sin b_- \sin c_-)^2 - \sin^2 a_1 \cos^2 b_- \cos^2 c_-} + \sin b_- \sin c_-. \qquad \text{(B.94)}$$

Now, a sufficient condition for (B.92) is obtained by replacing A and B by $\max\{A, B\}$. However, since A and B can be mapped to each other under $b_- \leftrightarrow -b_-$ and since (B.92) must hold for every b_-, we can always assume that $A \geq B$. Thus we replace B with A in (B.92) and use the fact that $\sum_{j,k}\tau_{jk} = 1$ to obtain the following sufficient condition for (B.83a):

$$\sqrt{(1+\sin b_- \sin c_-)^2 - \sin^2 a_1 \cos^2 b_- \cos^2 c_-} - \sin b_- \sin c_- \leq \sqrt{1-\sin a_1 \cos b_- \cos c_-}\,(2-\sqrt{1-\sin a_1 \cos b_- \cos c_-}), \qquad \text{(B.95)}$$

which is equivalent to:

$$\sqrt{(1+\sin b_- \sin c_-)^2 - (\sin a_1 \cos b_- \cos c_-)^2} \leq \sin b_- \sin c_- + 2\sqrt{1-\sin a_1 \cos b_- \cos c_-} - (1-\sin a_1 \cos b_- \cos c_-). \qquad \text{(B.96)}$$

By taking the square of both sides in the last inequality, we obtain the equivalent system of inequalities:

$$\begin{cases} (1+\sin b_- \sin c_-)^2 - (\sin a_1 \cos b_- \cos c_-)^2 \\ \leq \left[\sin b_- \sin c_- + 2\sqrt{1-\sin a_1 \cos b_- \cos c_-} - (1-\sin a_1 \cos b_- \cos c_-)\right]^2 & \text{(B.97a)} \\ \sin b_- \sin c_- + 2\sqrt{1-\sin a_1 \cos b_- \cos c_-} - (1-\sin a_1 \cos b_- \cos c_-) \geq 0. & \text{(B.97b)} \end{cases}$$

We first focus on proving (B.97b). If $\sin a_1 \cos b_- \cos c_- = 1$, then the inequality (B.97b) is trivially true. If $\sin a_1 \cos b_- \cos c_- \neq 1$, we can recast (B.97b) as follows:

$$2 \geq \sqrt{1-\sin a_1 \cos b_- \cos c_-} - \frac{\sin b_- \sin c_-}{\sqrt{1-\sin a_1 \cos b_- \cos c_-}}, \qquad \text{(B.98)}$$

and deduce the following sufficient condition:

$$\frac{|\sin b_- \sin c_-|}{\sqrt{1-\sin a_1 \cos b_- \cos c_-}} \leq 1 \quad \Leftrightarrow \quad |\sin b_- \sin c_-| \leq \sqrt{1-\sin a_1 \cos b_- \cos c_-}. \qquad \text{(B.99)}$$

The validity of the last inequality can be easily proved from (B.87) and from the fact that $1-\sin a_1 \cos b_- \cos c_- \leq \sqrt{1-\sin a_1 \cos b_- \cos c_-}$. This completes the proof of (B.97b).

We now focus on proving (B.97a). For ease of notation, we define the variables s and c as follows:

$$s := \sin b_- \sin c_- \qquad \text{(B.100)}$$

$$c := \sin a_1 \cos b_- \cos c_-. \qquad \text{(B.101)}$$

Then (B.97a) can be recast as follows:

$$\begin{aligned}
&(1+s)^2 - c^2 \leq \left[s + 2\sqrt{1-c} - (1-c)\right]^2 \\
\Leftrightarrow\ & 1 + s^2 + 2s - c^2 \leq 4(1-c) + (s+c-1)^2 + 4\sqrt{1-c}(s+c-1) \\
\Leftrightarrow\ & 2s - c^2 \leq 4(1-c) - 2s + c^2 - 2c(1-s) + 4\sqrt{1-c}(s+c-1) \\
\Leftrightarrow\ & 2c^2 + 4 - 4c - 4s - 2c(1-s) + 4\sqrt{1-c}(s+c-1) \geq 0 \\
\Leftrightarrow\ & 1 + (1-c)^2 - 2s - c + cs + 2\sqrt{1-c}(s+c-1) \geq 0 \\
\Leftrightarrow\ & (1-c)^2 + (1-c) - s(1-c) + 2s\sqrt{1-c} - 2\sqrt{1-c}(1-c) - s \geq 0 \\
\Leftrightarrow\ & (1-c)^2 - 2\sqrt{1-c}(1-c) + (1-c)(1-s) + 2s\sqrt{1-c} - s \geq 0. \qquad \text{(B.102)}
\end{aligned}$$

We now view (B.102) as a fourth degree inequality in the variable $x := \sqrt{1-c}$, i.e. we rewrite it as follows:

$$f(x) := x^4 - 2x^3 + (1-s)x^2 + 2sx - s \geq 0. \qquad \text{(B.103)}$$

Then a sufficient condition for the validity of (B.102) is that $f(x) \geq 0$ for every $x \in [0, \sqrt{2}]$, which is the domain induced by the definition of x. Nevertheless, if there are intervals in the domain where $f(x) < 0$, inequality (B.102) can still hold true as far as such intervals are not compatible with the underlying definitions of s and c given in (B.100) and (B.101). We will see that this is indeed the case.

In order to study the plot of $f(x)$, we first find its zeroes[8] for different parametric regions of s:

- If $-1 \leq s < 0$, then $f(x)$ has only one zero in $x_0 = 1$. Since $f(1/2) = 1/16 - s/4 > 0$ and $f(x)$ is a C^∞ function, we conclude that $f(x) \geq 0$ for $x \in [0,1]$. Similarly, $f(5/4) = 241/256 - s/16 > 0$ which implies that $f(x) \geq 0$ for $x \in [1, \sqrt{2}]$. Thus we conclude that $f(x) \geq 0$ in all its domain.
- If $s = 0$ then $f(x) = x^2(1-x^2) \geq 0$ for every x.
- If $s = 1$ then it follows from (B.101) that $c = 0$ and thus $x = 1$. We have that $f(1)|_{s=1} = 0$.
- If $0 < s < 1$, then $f(x)$ has three zeroes in $x_0 = -\sqrt{s}$, $x_0' = \sqrt{s}$ and $x_0'' = 1$. Since $f(\sqrt{s}/2) = -3s(1-\sqrt{s})/4 - 3s^2/16 < 0$, we conclude that $f(x) \leq 0$ for $x \in [0, \sqrt{s}]$.

  Moreover, by studying the first derivative of $f(x)$ we find the following critical points (where $f'(x) = 0$):

$$\begin{aligned}
x_1 &= \frac{1}{4}\left(1 - \sqrt{1+8s}\right) && \text{(B.104)}\\
x_1' &= \frac{1}{4}\left(1 + \sqrt{1+8s}\right) && \text{(B.105)}\\
x_1'' &= 1. && \text{(B.106)}
\end{aligned}$$

  We can easily deduce that $x_1 < 0$ and that $\sqrt{s} < x_1' < 1$. By combining this with the fact that $f''(1) = 2(1-s) > 0$, we conclude that $f(x) \geq 0$ for $x \in [\sqrt{s}, \sqrt{2}]$ and that it presents a local minimum in $x = 1$.

From the above analysis, we deduce that $f(x) < 0$ for $x \in [0, \sqrt{s})$ when $0 < s < 1$. However, as anticipated, the condition $0 \leq x < \sqrt{s}$ is not compatible with the definitions of s and c. Indeed, by using the definitions (B.100) and (B.101) we show that $x \geq \sqrt{s}$ holds:

$$\begin{aligned}
x \geq \sqrt{s} \ &\Leftrightarrow\ \sqrt{1 - \sin a_1 \cos b_- \cos c_-} \geq \sqrt{\sin b_- \sin c_-} \\
&\Leftrightarrow\ 1 - \sin a_1 \cos b_- \cos c_- \geq \sin b_- \sin c_- \qquad \text{(B.107)}
\end{aligned}$$

which can be proved via the sufficient condition (B.87). This implies that $f(\sqrt{1 - \sin a_1 \cos b_- \cos c_-}) \geq 0$ for every a_1, b_- and c_-, which proves (B.102).

We thus proved (B.97a), which completes the proof of (B.83a), which in turn completes the proof of the validity of (B.64a). This proves the lower bound (B.62), which employed in (B.61) provides us with the bound (B.6) on the conditional entropy of a fixed state ρ_α in the mixture:

$$H(A_0|E)_{\rho_\alpha} \geq 1 - h\left[\frac{1}{4}\left(\beta_{\mathrm{H}}^\alpha + 1 + \sqrt{(\beta_{\mathrm{H}}^\alpha)^2 + 2\beta_{\mathrm{H}}^\alpha - 3}\right)\right] \qquad \text{(B.108)}$$

Finally, by the convexity of (B.108), we extend the derived bound to the whole mixed state (B.3) as shown in (B.7), thus obtaining the entropy bound (B.1). This concludes the proof of Theorem 1. □

[8] We used Mathematica's "Reduce" function to easily find the zeroes of $f(x)$.

B.3 Tightness of the bound

In order to demonstrate that the entropy bound (B.1) is tight we need to show that, for every Bell value $\beta_{\rm H}$, there exists a quantum state and a set of measurements performed by the parties such that the Bell value is exactly given by $\beta_{\rm H}$ and such that the conditional entropy of Alice's outcome A_0 is equal to the rhs of (B.1).

The states that satisfy the above conditions (for every $\beta_{\rm H}$) belong to the following family of states diagonal in the GHZ basis:

$$\tau(\nu) = \nu|\psi_{0,0,0}\rangle\langle\psi_{0,0,0}|+(1-\nu)|\psi_{1,0,0}\rangle\langle\psi_{1,0,0}|, \tag{B.109}$$

where $\nu \in [1/2, 1]$. In order to see this, we first assign to Eve maximum knowledge by letting her hold the purifying system E of $\tau(\nu)$:

$$|\Psi_{ABCE}\rangle = \sqrt{\nu}\,|\psi_{0,0,0}\rangle \otimes |e_0\rangle_E + \sqrt{1-\nu}\,|\psi_{1,0,0}\rangle \otimes |e_1\rangle_E\,. \tag{B.110}$$

We now fix Alice's observable A_0 to be Z and compute the classical-quantum state of Alice's Z outcome and Eve's quantum system:

$$\begin{aligned}\tau_{ZE}(\tau) &= \sum_{z=0}^{1} |z\rangle\langle z|_Z \otimes \mathrm{Tr}_{BC}[\langle z|\Psi_{ABCE}\rangle\,\langle\Psi_{ABCE}|z\rangle] \\ &= \sum_{z=0}^{1} \frac{1}{2}|z\rangle\langle z|_Z \otimes \rho_E^z. \end{aligned}\tag{B.111}$$

In the above expression, ρ_E^z is the conditional state of Eve given that Alice obtained outcome $Z = z$ and can be easily computed as:

$$\rho_E^z = \nu|e_0\rangle\langle e_0|+(-1)^z\sqrt{\nu(1-\nu)}(|e_0\rangle\langle e_1|+\text{h.c.}) + (1-\nu)|e_1\rangle\langle e_1|, \tag{B.112}$$

with eigenvalues $\{0, 1\}$. Then, the conditional entropy of $\tau(\nu)$ can be computed in terms of the parameter ν as follows:

$$\begin{aligned}H(Z|E)_{\tau(\nu)} &= H(E|Z)_{\tau(\nu)} + H(Z)_{\tau(\nu)} - H(E)_{\tau(\nu)} \\ &= 1 - h(\nu)\end{aligned}\tag{B.113}$$

where $h(x)$ is the binary entropy.

The second step is to derive the maximal Bell value achievable by the state $\tau(\nu)$. We parametrize the parties' observables and partially fix the measurement angles[9] a_0, b_+ and c_+ as in Subsec. B.1.1. Then, by computing the Bell value (B.8) for the state $\tau(\nu)$, we get:

$$\beta_{\rm H}^{\tau(\nu)} = (2\nu-1)\sin a_1 \cos b_- \cos c_- + \sin b_- + \sin c_- - \sin b_- \sin c_- \tag{B.114}$$

The above expression can be maximized over the remaining measurement directions a_1, b_- and c_- thus yielding the following maximal Bell value:

$$\beta_{\rm H}^{\tau(\nu)} = 2\nu + \frac{1}{2\nu} - 1, \tag{B.115}$$

with corresponding optimal angles:

$$a_1 = \frac{\pi}{2} \quad , \quad b_- = \arctan\frac{1}{\sqrt{4\nu^2-1}} \quad , \quad c_- = \arcsin\frac{1}{2\nu}. \tag{B.116}$$

By reverting (B.115) and by inserting the result in (B.113), we express the conditional entropy of $\tau(\nu)$ in terms of its achievable Bell value $\beta_{\rm H}^{\tau(\nu)}$:

$$H(Z|E)_{\tau(\nu)} = 1 - h\left[\frac{1}{4}\left(\beta_{\rm H}^{\tau(\nu)} + 1 + \sqrt{(\beta_{\rm H}^{\tau(\nu)})^2 + 2\beta_{\rm H}^{\tau(\nu)} - 3}\right)\right], \tag{B.117}$$

which coincides with the lower bound (B.1) on the conditional entropy of Alice's A_0 outcome. This proves that the entropy bound in (B.1) is tight, since there exists an honest implementation that attains it.

Interestingly, we notice that the optimal measurement angles (B.116) of Bob and Charlie for the state (B.109) are given by $b_- = c_- = \pi/2$ when $\nu \to 1/2$. In other words, the optimal observables of Bob and Charlie that maximize the Bell value tend to be compatible ($B_0 = -B_1$ and $C_0 = -C_1$) when $\tau(\nu)$ tends to a separable state. This fact has been recently observed in [59] for the CHSH inequality [34], where less incompatible observables yield higher Bell values while demanding less entanglement from the state.

[9] The measurement angle a_0 of Alice's observable A_0 is already fixed by the fact that we chose to study the conditional entropy of Alice's Z outcome when the parties share the state $\tau(\nu)$.

C Proof of one-outcome entropy bound for MABK inequality

The proof technique based on the uncertainty relation, used to derive the entropy bound of Theorem 1, can be easily adapted to obtain further entropy bounds.

In this Appendix we rederive the conditional entropy bound on Alice's outcome A_0 when Alice, Bob and Charlie test the MABK inequality [42–44]. This bound was first obtained in [46] via a correspondence between the MABK inequality and its bipartite counterpart, the CHSH inequality [34]. The bound is also obtained in [47] by direct minimization of the conditional entropy for a fixed violation β_{M}. We report the bound for clarity.

Theorem 2. *Let Alice, Bob and Charlie test the MABK inequality [42–44] and obtain a Bell value of β_{M}. Then, the von Neumann entropy of Alice's outcome A_0 conditioned on Eve's information E satisfies*

$$H(A_0|E) \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{\beta_{\mathrm{M}}^2}{8} - 1}\right), \tag{C.1}$$

where $h(x) = -x\log_2 x + (1-x)\log_2(1-x)$ is the binary entropy.

We point out that the bound in (C.1) also holds for Alice's observable A_1 due to the symmetry of the MABK inequality.

Proof. From [47], we know that we can reduce the state shared by the parties to a three-qubit state and their measurements to rank-one projective measurements on their respective qubits.

We start by deriving an upper bound on the three-party MABK value. In order to do so, we consider its expression as obtained from the recursive definition [47]:

$$\beta_M = \frac{1}{2}\left\langle [A_0(B_0+B_1) + A_1(B_0-B_1)]\,(C_0+C_1) + [A_1(B_0+B_1) - A_0(B_0-B_1)]\,(C_0-C_1)\right\rangle, \tag{C.2}$$

and we exploit the degrees of freedom in the choice of the local reference frames to impose that every party's observable lies in the (x, y) plane of the Bloch sphere:

$$A_i = X\cos a_i + Y\sin a_i \tag{C.3}$$
$$B_i = X\cos b_i + Y\sin b_i \tag{C.4}$$
$$C_i = X\cos c_i + Y\sin c_i. \tag{C.5}$$

Moreover, we rotate Alice's reference frame along the z axis such that:

$$A_0 = X \tag{C.6}$$
$$A_1 = X\cos a + Y\sin a. \tag{C.7}$$

We define new operators $B_\pm := (B_0 \pm B_1)/2$ and $C_\pm := (C_0 \pm C_1)/2$ for Bob and Charlie, such that they can be recast as follows:

$$B_+ = \cos b_-(X\cos b_+ + Y\sin b_+) \tag{C.8}$$
$$B_- = -\sin b_-(X\sin b_+ - Y\cos b_+) \tag{C.9}$$
$$C_+ = \cos c_-(X\cos c_+ + Y\sin c_+) \tag{C.10}$$
$$C_- = -\sin c_-(X\sin c_+ - Y\cos c_+), \tag{C.11}$$

where $b_\pm := (b_0 \pm b_1)/2$ and $c_\pm := (c_0 \pm c_1)/2$. We rotate Bob's and Charlie's reference frames such that $b_+ = c_+ = 0$. By inserting everything in (C.2) we obtain the following simplified MABK value:

$$\begin{aligned}\beta_M &= 2\cos b_-\cos c_-\langle XXX\rangle - 2\sin b_-\sin c_-\langle XYY\rangle \\ &\quad + 2\left\langle (X\cos a + Y\sin a)(\sin b_-\cos c_- YX + \cos b_-\sin c_- XY)\right\rangle \\ &\quad =: 2\vec{V}\cdot\vec{W},\end{aligned} \tag{C.12}$$

where in the last line we defined the vectors:

$$\vec{V} = \left(\langle XXX\rangle, \langle XYY\rangle, \langle XYX\rangle, \langle XXY\rangle, \langle YYX\rangle, \langle YXY\rangle\right) \tag{C.13}$$

$$\begin{aligned}\vec{W} = (&\cos b_-\cos c_-, -\sin b_-\sin c_-, \cos a\sin b_-\cos c_-, \cos a\cos b_-\sin c_-, \sin a\sin b_-\cos c_-, \\ &\sin a\cos b_-\sin c_-).\end{aligned} \tag{C.14}$$

By the Cauchy-Schwarz inequality and by observing that $\|W\| = 1$, we obtain:

$$\beta_M \leq 2\sqrt{\langle YXY\rangle^2 + \langle YYX\rangle^2 + (\langle XXX\rangle^2 + \langle XXY\rangle^2) + (\langle XYY\rangle^2 + \langle XYX\rangle^2)}. \tag{C.15}$$

We now prove that for a generic three-qubit state the following inequalities hold:

$$\langle XXX\rangle^2 + \langle XXY\rangle^2 \leq 1 \tag{C.16}$$

$$\langle XYY\rangle^2 + \langle XYX\rangle^2 \leq 1. \tag{C.17}$$

To show this, we write the generic three-qubit state in the GHZ basis:

$$\rho = \sum_{i,j,k=0}^{1} \lambda_{ijk} |\psi_{i,j,k}\rangle\langle\psi_{i,j,k}| + \sum_{j,k=0}^{1} (c_{jk}|\psi_{0,j,k}\rangle\langle\psi_{1,j,k}| + \text{h.c.}) + \ldots, \tag{C.18}$$

where λ_{ijk} are the real diagonal elements, c_{jk} are the complex coherences between the states $|\psi_{0,j,k}\rangle$ and $|\psi_{1,j,k}\rangle$ and h.c. stands for the Hermitian conjugate of the term preceding it. In the dots "$\ldots$" we include every other coherence of the state ρ, since they do not play a role in the expectation values appearing in (C.16) and (C.17). This can be readily seen by considering the action of the operators of (C.16) and (C.17) on the states of the GHZ basis:

$$XXX\,|\psi_{i,j,k}\rangle = (-1)^i\,|\psi_{i,j,k}\rangle \tag{C.19}$$

$$XXY\,|\psi_{i,j,k}\rangle = -\mathbb{i}(-1)^{i+k}\,|\psi_{\bar{i},j,k}\rangle \tag{C.20}$$

$$XYY\,|\psi_{i,j,k}\rangle = (-1)^{i+j+k+1}\,|\psi_{i,j,k}\rangle \tag{C.21}$$

$$XYX\,|\psi_{i,j,k}\rangle = -\mathbb{i}(-1)^{i+j}\,|\psi_{\bar{i},j,k}\rangle\,, \tag{C.22}$$

which yield the following expectation values on ρ:

$$\langle XXX\rangle = \sum_{j,k=0}^{1} \lambda_{0jk} - \lambda_{1jk} \tag{C.23}$$

$$\langle XXY\rangle = \sum_{j,k=0}^{1} (-1)^k 2\mathrm{Im}(c_{jk}) \tag{C.24}$$

$$\langle XYY\rangle = -\sum_{j,k=0}^{1} (-1)^{j+k}(\lambda_{0jk} - \lambda_{1jk}) \tag{C.25}$$

$$\langle XYX\rangle = \sum_{j,k=0}^{1} (-1)^j 2\mathrm{Im}(c_{jk}). \tag{C.26}$$

Before proving (C.16) and (C.17), we need to derive a couple of conditions satisfied by the parameters describing the state ρ. Since $\rho \geq 0$, then also its restriction to every 2-dimensional subspace spanned by $\{|\psi_{0,j,k}\rangle, |\psi_{1,j,k}\rangle\}$ (for $j,k \in \{0,1\}$) must be positive-semidefinite. Indeed, let $P_{jk} := |\psi_{0,j,k}\rangle\langle\psi_{0,j,k}| + |\psi_{1,j,k}\rangle\langle\psi_{1,j,k}|$ be the projector on such a subspace. Then,

$$P_{jk}\rho P_{jk} \geq 0 \quad \iff \quad \lambda_{0jk}|\psi_{0,j,k}\rangle\langle\psi_{0,j,k}| + \lambda_{1jk}|\psi_{1,j,k}\rangle\langle\psi_{1,j,k}| + c_{jk}|\psi_{0,j,k}\rangle\langle\psi_{1,j,k}| + \text{h.c.} \geq 0, \tag{C.27}$$

for all j and k. A necessary condition for (C.27) is that its determinant is non-negative (the eigenvalues of positive-semidefinite operators are all non-negative):

$$\lambda_{0jk}\lambda_{1jk} \geq |c_{jk}|^2 \geq \mathrm{Im}^2(c_{jk}). \tag{C.28}$$

A second condition on the state's parameters can be found starting from the following chain of equivalences (note that $\lambda_{ijk} \geq 0$ follows from $\rho \geq 0$):

$$\begin{aligned}
&2\left(\sqrt{\lambda_{0jk}\lambda_{1j'k'}} - \sqrt{\lambda_{1jk}\lambda_{0j'k'}}\right)^2 \geq 0 \\
&\iff \; 2\left(\lambda_{0jk}\lambda_{1j'k'} + \lambda_{1jk}\lambda_{0j'k'} - 2\sqrt{\lambda_{0jk}\lambda_{1jk}\lambda_{0j'k'}\lambda_{1j'k'}}\right) \geq 0 \\
&\iff \; \lambda_{0jk}\lambda_{1j'k'} + \lambda_{1jk}\lambda_{0j'k'} \geq 4\sqrt{\lambda_{0jk}\lambda_{1jk}\lambda_{0j'k'}\lambda_{1j'k'}} - \lambda_{0jk}\lambda_{1j'k'} - \lambda_{1jk}\lambda_{0j'k'}.
\end{aligned} \tag{C.29}$$

By using (C.28) twice we can lower bound the square-root on the rhs as follows:

$$4\sqrt{\lambda_{0jk}\lambda_{1jk}\lambda_{0j'k'}\lambda_{1j'k'}} \geq 4\,|\mathrm{Im}(c_{jk})\mathrm{Im}(c_{j'k'})| \geq 4(-1)^{k+k'}\mathrm{Im}(c_{jk})\mathrm{Im}(c_{j'k'}). \tag{C.30}$$

By employing the last expression in (C.29), we obtain the second condition needed to prove inequalities (C.16) and (C.17):

$$\lambda_{0jk}\lambda_{1j'k'} + \lambda_{1jk}\lambda_{0j'k'} \geq 4(-1)^{k+k'}\mathrm{Im}(c_{jk})\mathrm{Im}(c_{j'k'}) - \lambda_{0jk}\lambda_{1j'k'} - \lambda_{1jk}\lambda_{0j'k'}. \tag{C.31}$$

We now proceed on proving (C.16). The lhs of (C.16) can be expressed using (C.23) and (C.24) as follows:

$$\begin{aligned}
\langle XXX\rangle^2 + \langle XXY\rangle^2 &= \left[\sum_{j,k=0}^{1}(\lambda_{0jk}-\lambda_{1jk})\right]^2 + 4\left[\sum_{j,k=0}^{1}(-1)^k\mathrm{Im}(c_{jk})\right]^2 \\
&= \sum_{j,k=0}^{1}\left[(\lambda_{0jk}-\lambda_{1jk})^2 + 4\mathrm{Im}^2(c_{jk})\right] \\
&\quad + 2\sum_{(j,k)\neq(j',k')}\left[(\lambda_{0jk}-\lambda_{1jk})(\lambda_{0j'k'}-\lambda_{1j'k'}) + 4(-1)^{k+k'}\mathrm{Im}(c_{jk})\mathrm{Im}(c_{j'k'})\right] \\
&= \sum_{j,k=0}^{1}\left[(\lambda_{0jk}-\lambda_{1jk})^2 + 4\mathrm{Im}^2(c_{jk})\right] \\
&\quad + 2\sum_{(j,k)\neq(j',k')}\left[\lambda_{0jk}\lambda_{0j'k'} + \lambda_{1jk}\lambda_{1j'k'} + 4(-1)^{k+k'}\mathrm{Im}(c_{jk})\mathrm{Im}(c_{j'k'}) - \lambda_{0jk}\lambda_{1j'k'} - \lambda_{1jk}\lambda_{0j'k'}\right].
\end{aligned} \tag{C.32}$$

We now upper bound the above expression by using (C.28) in the first sum and (C.31) in the second sum. We obtain:

$$\begin{aligned}
\langle XXX\rangle^2 + \langle XXY\rangle^2 &\leq \sum_{j,k=0}^{1}(\lambda_{0jk}+\lambda_{1jk})^2 + 2\sum_{(j,k)\neq(j',k')}(\lambda_{0jk}+\lambda_{1jk})(\lambda_{0j'k'}+\lambda_{1j'k'}) \\
&= \left[\sum_{j,k=0}^{1}\lambda_{0jk}+\lambda_{1jk}\right]^2 = 1,
\end{aligned} \tag{C.33}$$

where in the last equality we used the fact that $\mathrm{Tr}\,\rho = 1$. This proves (C.16).

Similarly, the lhs of (C.17) can be expressed through (C.25) and (C.26) and upper bounded using (C.28) and (C.31) as follows:

$$\begin{aligned}
\langle XYY\rangle^2 + \langle XYX\rangle^2 &= \sum_{j,k=0}^{1}\left[(\lambda_{0jk}-\lambda_{1jk})^2 + 4\mathrm{Im}^2(c_{jk})\right] \\
&\quad + 2\sum_{(j,k)\neq(j',k')}(-1)^{j+j'+k+k'}\left[(\lambda_{0jk}-\lambda_{1jk})(\lambda_{0j'k'}-\lambda_{1j'k'}) + 4(-1)^{k+k'}\mathrm{Im}(c_{jk})\mathrm{Im}(c_{j'k'})\right] \\
&\leq \sum_{j,k=0}^{1}(\lambda_{0jk}+\lambda_{1jk})^2 + 2\sum_{(j,k)\neq(j',k')}(-1)^{j+j'+k+k'}(\lambda_{0jk}+\lambda_{1jk})(\lambda_{0j'k'}+\lambda_{1j'k'}) \\
&= \left[\sum_{j,k=0}^{1}(-1)^{j+k}(\lambda_{0jk}+\lambda_{1jk})\right]^2 \leq 1,
\end{aligned} \tag{C.34}$$

which proves (C.17).

Finally, by employing (C.16) and (C.17) in (C.15) we derive the following upper bound on the MABK value:

$$\beta_M \leq 2\sqrt{2 + 2\max\{|\langle YXY\rangle|\,, |\langle YYX\rangle|\}^2}. \tag{C.35}$$

Now, we can turn to the conditional entropy of Alice's outcome when she measures $A_0 = X$ and lower bound it with the uncertainty relation [49]:

$$H(X|E) \geq 1 - H(Y|BC) \geq 1 - h(Q_{Y,O_BO_C}), \tag{C.36}$$

where in the second inequality we followed the same steps that lead to (B.58) and (B.59), and where Q_{Y,O_BO_C} is defined as the probability that the Y outcome of Alice differs from the product of the outcomes of Bob (O_B) and Charlie (O_C), that is:

$$Q_{Y,O_BO_C} := \Pr[YO_BO_C = -1] = \frac{1 - \langle YO_BO_C\rangle}{2}. \tag{C.37}$$

Moreover, by using the properties of the binary entropy $h(x)$ as in (B.60), we obtain:

$$H(X|E) \geq 1 - h\left(\frac{1 + |\langle YO_BO_C\rangle|}{2}\right). \tag{C.38}$$

We emphasize that we can employ the uncertainty relation and derive a bound like the one in (C.38) independently of the measurement settings A_i, B_i and C_i of the parties in the DI scenario. Of course, in order to make the derived inequality useful in our case, we set one of Alice's measurements to X –which is also one of Alice's settings in the DI scenario, see (C.6)– so that we obtain an inequality for the conditional entropy $H(X|E)$. For this argument, we can arbitrarily choose Bob's and Charlie's measurements in (C.38) to be either $O_B = X$ and $O_C = Y$ or $O_B = Y$ and $O_C = X$. Both cases lead to valid lower bounds on the conditional entropy of Alice's X outcome. We can then lower bound the conditional entropy $H(X|E)$ by:

$$H(X|E) \geq 1 - h\left(\frac{1 + \max\{|\langle YXY\rangle|, |\langle YYX\rangle|\}}{2}\right). \tag{C.39}$$

By reverting the upper bound on the MABK value (C.35), we obtain:

$$\max\{|\langle YXY\rangle|, |\langle YYX\rangle|\} \geq \sqrt{\frac{\beta_{\mathrm{M}}^2}{8} - 1}. \tag{C.40}$$

Finally, by employing (C.40) in (C.39) we recover the entropy bound (C.1).

We point out that, although the proof derives a lower bound on the conditional entropy of Alice's X-basis outcome, the derived bound is general and holds for any measurement Alice implements. This is because at the beginning of the proof, we purposely set Alice's local reference frame such that her qubit observable A_0 coincides with the Pauli operator X. This has no effect on the description of the state (C.18) shared by Alice, Bob and Charlie since it is a completely generic three-qubit state for any choice of local reference frames. □

D Numerical computation of two-outcome entropy bounds

In this Appendix we describe the steps that allow us to numerically compute lower bounds on the two-outcome entropy $H(A_0B_0|E)$ for the Holz inequality, the Parity-CHSH inequality and the CHSH inequality. The bounds are plotted in Fig. 2 and are used in Sec. 5 to compare the performance of DIRE protocols based on different Bell inequalities.

Holz inequality We compute a numerical lower bound on $H(A_0B_0|E)$ as a function of the violation β_{H} of the Holz inequality for three parties. The bound is obtained by direct optimization of the entropy once the violation is fixed. Based on the numerical bound, we also conjecture the correspondent analytical expression (Conjecture 1).

In order to make the optimization numerically feasible, we arbitrarily fix the local reference frames of Alice, Bob and Charlie and parametrize the state they share as shown in Subsec. B.1. Then, the measurement angle b_1 is fixed by b_0 through (B.17) as follows: $b_1 = \pi - b_0$, which implies that $b_- = b_0 - \pi/2$. By substituting in the Bell value (B.8) of the Holz inequality, we obtain:

$$v_{\mathrm{H}} = (\cos a_1 \langle ZXX\rangle + \sin a_1 \langle XXX\rangle) \sin b_0 \cos c_- - \cos b_0 \langle ZZ\mathbb{1}\rangle + \sin c_- \langle Z\mathbb{1}Z\rangle + \cos b_0 \sin c_- \langle \mathbb{1}ZZ\rangle, \tag{D.1}$$

which is now written in terms of the free measurement angles a_1 and c_- and the angle b_0 that instead appears in the conditional entropy expression. Note that, thanks to the parametrization of the state in Subsec. B.1.2, the expectation values in (D.1) are easily written in terms of the state parameters $\{\rho_{ijk}, t_{jk}\}$ as follows:

$$\langle XXX \rangle = \sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) \cos(2t_{jk}) \tag{D.2}$$

$$\langle ZXX \rangle = \sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk}) \sin(2t_{jk}) \tag{D.3}$$

$$\langle ZZ\mathbb{1} \rangle = \sum_{j,k=0}^{1} (-1)^{j} (\rho_{0jk} - \rho_{1jk}) \cos(2t_{jk}) \tag{D.4}$$

$$\langle Z\mathbb{1}Z \rangle = \sum_{j,k=0}^{1} (-1)^{k} (\rho_{0jk} - \rho_{1jk}) \cos(2t_{jk}) \tag{D.5}$$

$$\langle \mathbb{1}ZZ \rangle = \sum_{j,k=0}^{1} (-1)^{j+k} (\rho_{0jk} + \rho_{1jk}). \tag{D.6}$$

By also expressing the entropy $H(A_0B_0|E)$ in terms of the state parameters $\{\rho_{ijk}, t_{jk}\}$ and the angle b_0 (recall that Alice's reference frame is chosen such that $a_0 = 0$), we numerically solve the following optimization problem:

$$\begin{aligned} \min_{\{\rho_{ijk}, t_{jk}, b_0, a_1, c_-\}} \quad & H(A_0B_0|E)(\rho_{ijk}, t_{jk}, b_0) \\ \text{sub. to} \quad & v_{\mathrm{H}}(\rho_{ijk}, t_{jk}, b_0, a_1, c_-) = \beta_{\mathrm{H}}\,;\ \textstyle\sum_{ijk} \rho_{ijk} = 1\,;\ \rho_{ijk} \geq 0, \end{aligned} \tag{D.7}$$

when varying β_{H} in the interval $(1, 3/2]$. In reality, we solve the equivalent –in the sense that leads to the same entropy for every β_{H}– but simpler optimization problem:

$$\begin{aligned} \min_{\{\rho_{ijk}, t_{jk}, b_0\}} \quad & H(A_0B_0|E)(\rho_{ijk}, t_{jk}, b_0) \\ \text{sub. to} \quad & \bar{v}_{\mathrm{H}}(\rho_{ijk}, t_{jk}, b_0) \geq \beta_{\mathrm{H}}\,;\ \textstyle\sum_{ijk} \rho_{ijk} = 1\,;\ \rho_{ijk} \geq 0, \end{aligned} \tag{D.8}$$

where $\bar{v}_{\mathrm{H}}$ is the maximum of (D.1) over the free angles a_1 and c_-:

$$\bar{v}_{\mathrm{H}} = \sqrt{\sin^2 b_0 (\langle ZXX \rangle^2 + \langle XXX \rangle^2) + (\langle Z\mathbb{1}Z \rangle + \cos b_0 \langle \mathbb{1}ZZ \rangle)^2} - \cos b_0 \langle ZZ\mathbb{1} \rangle\,. \tag{D.9}$$

The numerical plot points obtained by solving (D.8) with the built-in functions of Wolfram Mathematica [60] are reported in Fig. 3, together with our conjectured bound on $H(A_0B_0|E)$. Our conjecture on the analytical expression of the entropy bound is given in Conjecture 1.

Parity-CHSH inequality The bound on $H(A_0B_0|E)$ when three parties test the Parity-CHSH inequality is also obtained by direct numerical optimization, similarly to the bound for the Holz inequality.

As a matter of fact, note that the Parity-CHSH inequality (3) is a particular case (upon relabeling the observables) of the Holz inequality (2) for $c_0 = c_1$, i.e., when Charlie's two measurements coincide. Thus, the optimization problem yielding the entropy bound for the Parity-CHSH inequality is equal to (D.7), where we set $c_- = 0$.

CHSH inequality The bound on $H(A_0B_0|E)$ when two parties test the CHSH inequality is again obtained by direct numerical optimization. In order to simplify the optimization, we apply the results of [47] to the CHSH scenario and parametrize the state shared by Alice and Bob as a Bell-diagonal state:

$$\rho = \sum_{i,j=0}^{1} \lambda_{ij} |\psi_{i,j}\rangle\langle\psi_{i,j}|, \tag{D.10}$$

where $|\psi_{i,j}\rangle = (|0j\rangle + (-1)^i |1\bar{j}\rangle)/\sqrt{2}$ are the states of the Bell basis. We also assume without loss of generality that the parties' observables are rank-one projective measurements in the (x, y)-plane, defined by the eigenstates:

$$|a\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^a e^{\mathrm{i}\varphi_{A_k}} |1\rangle \right) \tag{D.11}$$

$$|b\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^b e^{\mathrm{i}\varphi_{B_k}} |1\rangle \right) \tag{D.12}$$

where $a, b \in \{0, 1\}$ are the outcomes of Alice's and Bob's observables A_k and B_k and $\varphi_{A_k}, \varphi_{B_k}$ are the corresponding measurement directions, respectively. Then, one can compute the joint probability of obtaining outcomes a and b when Alice and Bob measured A_k and B_l. We obtain:

$$p(a, b|k, l) = \frac{1}{4}\left[1 + (-1)^{a+b}\cos(\varphi_{A_k} + \varphi_{B_l})(\lambda_{00} - \lambda_{10}) + (-1)^{a+b}\cos(\varphi_{A_k} - \varphi_{B_l})(\lambda_{01} - \lambda_{11})\right], \tag{D.13}$$

and observe that $p(0, 0|k, l) = p(1, 1|k, l)$ and $p(0, 1|k, l) = p(1, 0|k, l) = 1/2 - p(0, 0|k, l)$. We can thus express all the probabilities appearing in the conditional entropy $H(A_0B_0|E)$ in terms of $p := p(0, 0|0, 0)$.

We can now derive a simple expression for the conditional entropy of interest:

$$\begin{aligned} H(A_0B_0|E) &= H(A_0B_0) + H(E|A_0B_0) - H(E) \\ &= -2p\log_2 p - 2(1/2 - p)\log_2(1/2 - p) - H(\{\lambda_{ij}\}) \\ &= 1 + h(2p) - H(\{\lambda_{ij}\}), \end{aligned} \tag{D.14}$$

where in the second equality we used the fact that the state shared by Alice, Bob and Eve is pure (hence $H(E) = H(\rho)$) and the conditional state $\rho_E^{a,b}$ of Eve, given that Alice and Bob obtained outcomes a and b, is still pure (thus $H(E|A_0B_0) = 0$).

The CHSH Bell value, for the parametrization described above, reduces to:

$$\begin{aligned} v_{\mathrm{C}} &= \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \\ &= (\lambda_{00} - \lambda_{10})(\cos(\varphi_{A_0} + \varphi_{B_0}) + \cos(\varphi_{A_0} + \varphi_{B_1}) + \cos(\varphi_{A_1} + \varphi_{B_0}) - \cos(\varphi_{A_1} + \varphi_{B_1})) \\ &\quad + (\lambda_{01} - \lambda_{11})(\cos(\varphi_{A_0} - \varphi_{B_0}) + \cos(\varphi_{A_0} - \varphi_{B_1}) + \cos(\varphi_{A_1} - \varphi_{B_0}) - \cos(\varphi_{A_1} - \varphi_{B_1})). \end{aligned} \tag{D.15}$$

We then numerically solved the following optimization problem with the built-in functions of Wolfram Mathematica [60]:

$$\begin{aligned} &\min_{\{\lambda_{ij}, \varphi_{A_0}, \varphi_{B_0}, \varphi_{A_1}, \varphi_{B_1}\}} \quad 1 + h(2p) - H(\{\lambda_{ij}\}) \\ &\text{sub. to} \quad v_{\mathrm{C}}(\lambda_{ij}, \varphi_{A_0}, \varphi_{B_0}, \varphi_{A_1}, \varphi_{B_1}) = \beta_{\mathrm{C}}\,;\ \textstyle\sum_{ij}\lambda_{ij} = 1\,;\ \lambda_{ij} \geq 0, \end{aligned} \tag{D.16}$$

where p is given by:

$$p = \frac{1}{4}\left[1 + \cos(\varphi_{A_0} + \varphi_{B_0})(\lambda_{00} - \lambda_{10}) + \cos(\varphi_{A_0} - \varphi_{B_0})(\lambda_{01} - \lambda_{11})\right]. \tag{D.17}$$

The numerical solution of (D.16) is the entropy bound reported in Fig. 2. We remark that the same bound has been independently computed in [38] by combining an analytical simplification similar to the one reported here with numerical techniques.

E Tightness of one-outcome entropy bound for Parity-CHSH inequality

In this Appendix we demonstrate that the lower bound on the entropy of Alice's outcome A_0 when three parties test the Parity-CHSH inequality, reported in (A.11), is tight.

Lemma 3. *Let Alice, Bob and Charlie test the Parity-CHSH inequality [20] and obtain a Bell value of β_{pC}. Then, the following lower bound on the von Neumann entropy of Alice's outcome A_0, conditioned on Eve's information E,*

$$H(A_0|E) \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{(\beta_{\mathrm{pC}})^2 - 1}\right), \tag{E.1}$$

is tight. Namely, that there exists a quantum state and a set of measurements yielding a Bell value of β_{pC} with conditional entropy of Alice's outcome A_0 given by the rhs of (E.1).

Proof. Consider the same family of states used to prove the tightness of the bound in (11), that is:

$$\tau(\nu) = \nu|\psi_{0,0,0}\rangle\langle\psi_{0,0,0}| + (1 - \nu)|\psi_{1,0,0}\rangle\langle\psi_{1,0,0}|, \tag{E.2}$$

where $\nu \in [1/2, 1]$. Then, the conditional entropy of Alice's outcome $A_0 = Z$ can be computed in terms of the parameter ν and reads:

$$H(A_0|E)_{\tau(\nu)} = 1 - h(\nu). \tag{E.3}$$

Now, we compute the maximal violation of the Parity-CHSH inequality (3) achieved by the state $\tau(\nu)$. To do this, we first parametrize the parties' observables as in Subsec. B.1.1 and orient the reference frames such that $C = X$, $A_0 = Z$ and $b_+ = 0$ (thus $B_+ = \cos b_0 Z$ and $B_- = \sin b_0 X$). Then, the Bell value of the Parity-CHSH inequality reads:

$$\beta_{\mathrm{pC}} = \sin b_0(\cos a_1 \langle ZXX\rangle + \sin a_1 \langle XXX\rangle) + \cos b_0 \langle ZZ\mathbb{1}\rangle\,. \tag{E.4}$$

By computing the expectation values on the state $\tau(\nu)$, we obtain:

$$\beta_{\mathrm{pC}}^{\tau(\nu)} = \sin b_0 \sin a_1(2\nu - 1) + \cos b_0. \tag{E.5}$$

The above expression can be maximized over the remaining measurement directions a_1 and b_0 yielding the following maximal Bell value:

$$\beta_{\mathrm{pC}}^{\tau(\nu)} = \sqrt{(2\nu - 1)^2 + 1}. \tag{E.6}$$

By reverting the last expression we obtain:

$$\nu = \frac{1}{2} + \frac{1}{2}\sqrt{(\beta_{\mathrm{pC}}^{\tau(\nu)})^2 - 1} \tag{E.7}$$

which substituted in (E.3) returns exactly the lower bound in (E.1). Hence we proved that the bound is tight. □