Supplementary information:
Device-independent quantum key distribution with random key basis

René Schwonnek,[1,*] Koon Tong Goh,[1,*] Ignatius W. Primaatmaja,[2] Ernest Y.-Z. Tan,[3] Ramona Wolf,[4] Valerio Scarani,[2,5] and Charles C.-W. Lim[1,2]

[1] *Department of Electrical & Computer Engineering, National University of Singapore, Singapore*
[2] *Centre for Quantum Technologies, National University of Singapore, Singapore*
[3] *Institute for Theoretical Physics, ETH Zürich, Switzerland*
[4] *Institut für Theoretische Physik, Leibniz Universität Hannover, Germany*
[5] *Department of Physics, National University of Singapore, Singapore*

I. SUPPLEMENTARY NOTE 1 - SECURITY ANALYSIS

This section documents the derivation of our lower bound on the quantity $C^*(S)$, which is introduced in the main text. $C^*(S)$ is defined as the minimum $H(Z|E\Theta)$ (conditional entropy of Z given side-information $E\Theta$) upon observing a CHSH value of S. Recall that

$$H(Z|E\Theta) := \lambda H(A_0|E) + (1-\lambda)H(A_1|E) \tag{1}$$

describes Eve's uncertainty about the measurement outcome Z given Θ and is a keystone for determining the secret key rate of our device-independent quantum key distribution (DIQKD) protocols.

Before diving into the derivation, we will furnish the definitions and notations of the quantum states, operators and functionals that will be used throughout this section. In the main text, we considered a Bell scenario where two parties Alice and Bob input measurement settings $X \in \{0,1\}$ and $Y \in \{0,1,2,3\}$ respectively into their devices and in return, each device outputs a bit. We shall omit the measurement settings $Y = 0, 1$ for the entirety of this section as they do not serve any role in the estimation of $H(Z|E\Theta)$.

Since we are working in a fully device-independent setting, we can assume that all measurements can be written as projectors without any loss of generality (refer to the explanation in [1]). As such, we denote the projectors corresponding to measurements A_0, A_1, B_2, B_3 as

$$A_0 = \{\Pi_0^{A_0}, \Pi_1^{A_0}\}, \quad A_1 = \{\Pi_0^{A_1}, \Pi_1^{A_1}\}, \quad B_2 = \{\Pi_0^{B_2}, \Pi_1^{B_2}\}, \text{ and } B_3 = \{\Pi_0^{B_3}, \Pi_1^{B_3}\}, \tag{2}$$

where the subscript of each projector denotes its corresponding measurement outcome. Therefore, the correlation measurement operators are defined by

$$C^{A_0} := \Pi_0^{A_0} - \Pi_1^{A_0}, \quad C^{A_1} := \Pi_0^{A_1} - \Pi_1^{A_1}, \quad C^{B_2} := \Pi_0^{B_2} - \Pi_1^{B_2}, \text{ and } C^{B_3} := \Pi_0^{B_3} - \Pi_1^{B_3}. \tag{3}$$

The correlation measurement operators and the correlation function $C_{XY} = P(A_X = B_Y|X,Y) - P(A_X \neq B_Y|X,Y)$ defined in the main text is related via $C_{XY} = \operatorname{tr}\left(\rho\, C^{A_X} \otimes C^{B_Y}\right)$ where ρ is the measured quantum state. Hence, the CHSH operator is denoted as

$$CHSH := C^{A_1} \otimes C^{B_2} - C^{A_0} \otimes C^{B_2} - C^{A_0} \otimes C^{B_3} - C^{A_1} \otimes C^{B_3}. \tag{4}$$

Furthermore, we denote the single round quantum state of Alice and Bob by ρ_{AB} and assume that Eve holds the purification of this state. Thus, the joint state describing Alice, Bob, and Eve quantum systems is given by some pure state ψ_{ABE}, whose Hilbert space dimension is unknown. Conventionally, the von Neumann entropy of a quantum state ρ is denoted and defined by $H(\rho) := -\operatorname{tr}(\rho \log \rho)$, we shall adopt the shorthand notation of

$$H(AB) = H(\rho_{AB}), \quad H(B) = H(\rho_B), \quad H(E) = H(\rho_E) \dots \tag{5}$$

to denote the entropy of a specific subsystem, whenever the underlying state is clear from the context. Next, a classical-quantum state after the action of Alice's measurement, A_X, is modelled by

$$\rho_{A_X BE} = \sum_{i\in\{0,1\}} |i\rangle\langle i| \otimes \operatorname{tr}_A \left((\Pi_i^{A_X} \otimes \mathbf{1}_{BE}) \psi_{ABE} (\Pi_i^{A_X} \otimes \mathbf{1}_{BE}) \right), \tag{6}$$

[*] These authors contributed equally to this work.

where $|i\rangle\langle i|$ indexes a classical register that stores the measurement outcomes. Thus, the conditional entropy $H(A_X|E) = H(A_X E) - H(E)$ is well-defined for any given joint quantum state describing Alice, Bob and Eve's systems through the above-mentioned relations.

Finally, we could state the proper mathematical definition of $C^*(S)$ using the furnished definitions:

$$\begin{aligned} C^*(S) = \inf_{A_0,A_1,B_2,B_3}\inf_{\psi_{ABE}} \quad & \lambda H(A_0|E) + (1-\lambda)H(A_1|E) \\ \text{s.th.:} \quad & \langle CHSH\rangle_{\rho_{AB}} = S. \end{aligned} \tag{7}$$

In the following subsections, we will provide the detailed derivation of our lower bound on the quantity $C^*(S)$ and the structure of the proceedings are organised as follows:

I A We start by following a well-known argument [1–3], which allows us to reformulate the estimation of conditional entropy of Eve in a tripartite scenario into the estimation of **entropy production on the Alice-Bob system**.

I B We proceed by following the argument of Pironio et al.[4], which allows us to conclude that the worst case, i.e. the optimal attack of Eve, can always be realised by Alice and Bob performing a convex combination of **projective measurements on a two qubit state**. Even though the problem now may seem straightforward, it still requires the application of a suite of non-trivial numerical and analytical methods. This is due to the fact that the simultaneous optimisation over states and measurements is neither linear nor convex.

I C We then apply a new refined version of Pinsker's inequality (see Thm. 1) that enables the estimation of entropies via certain trace norms. The remaining problem of **optimising over trace norms** can then be bounded using an efficient algorithm, which will be introduced in the follow subsections.

I D We first **formulate the optimisation over the unknown quantum state as a semi-definite program (SDP)**.

I E Although the **optimisation over Bob's measurements** is not convex, we formulated an efficient algorithm that lower bounds this optimisation up to arbitrary precision.

I F At this stage, it only remains to **optimise over Alice's measurements**. Similar to the previous subsection, optimising over Alice's measurements also result in an optimisation problem that is not a SDP. Since this optimisation only involves a single parameter, which is the angle φ between Alice's measurements, we could simply employ an adaptive refining ε-net. This is possible as all operators involved in the previous steps can be explicitly bounded in norm.

I G At this point we are able to compute reliable lower bounds on $C^*(S)$ for any two-qubit strategy. Using I B, we are able to compute the final $C^*(S)$ for a discretised range of different Bell violations S on qubits and taking its convex hull subsequently.

A. Reduction to locally accessible quantities

The defining advantage of quantum over classical cryptography stems from the fact that for a quantum system it is possible to witness the action of Eve, given only access to the Alice-Bob subsystem. In this subsection, we will relate the conditional entropy $H(A_X|E)$, which depends on Eve's system, to quantities that only depends on Alice and Bob's systems. Such effort will allow us to circumvent the obstacle of having to perform optimisation over Eve's quantum system with unbounded Hilbert space dimension.

We begin by viewing any key generating measurement, A_X, of the DIQKD protocol from the perspective of a larger Hilbert space (similarly to the appendix of [2]) by introducing a classical memory $\mathcal{A}_X$ that is used to store the measurement outcome. We denote $\mathcal{A}_X^{init}$ as the abelian algebra describing the initial (empty) state of the memory and ϕ as its associated pure quantum state. As such, the process of measuring A_X on Alice's quantum system (modelled by von Neumann algebra $\mathcal{A}$) and recording the outcome into the memory can be described by a unitary evolution that transforms the pure initial state $\Psi_{ABE}\otimes\phi$ into a final state $\Psi_{A'BEA_X}$. Note that the unitary evolution also involves the transformation of $\mathcal{A}$ into the post measurement state of a system $\mathcal{A}'$. Hence, $H(A_X|E)$ can be understood as entropy production ΔH on the memory-Eve system.

From the dilated perspective (see Fig. 1), the memory-Eve system is only one side of a bipartition, where the Alice-Bob system is the other. Since the local von Neumann entropies on two sides of a bipartite pure state are equal (see Thm.2(c) of [5]), the entropy production on the Alice-Bob system is equal to the entropy production of the memory-Eve system. Consequently, we can conclude that

$$\begin{aligned} H(A_X|E) &= H(A_X E) - H(E) = H(A_X E) - H(A_X^{init} E) & (8)\\ &= H(A'B) - H(AB) := \Delta H & (9) \end{aligned}$$

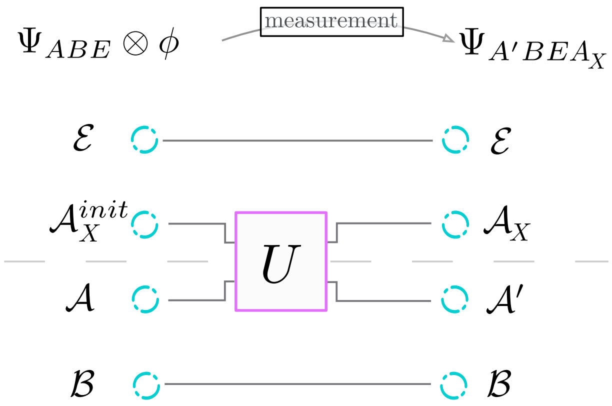

Fig. 1. **The Stinespring dilated perspective:** A key generating measurement A_X is regarded from the perspective of a higher Hilbert space by including the action $\mathcal{A}_X \to \mathcal{A}_X^{init}$ on a classical memory (an abelian algebra). From this perspective the global state before and after the measurement is pure. In this case, due to the Araki-Lieb inequality (see Thm.2(c) of [5]), the entropy production $\Delta H = H(A_X|E)$ on the Eve-Memory partition equals the entropy change on the Alice-Bob partition. This allows us to bound $H(A_X|E)$ by measuring only on the Alice-Bob partition, i.e. without accessing Eve's system.

Therefore, we could restrict the values of $H(A_X|E)$ by only considering the transformation $\mathcal{AB} \to \mathcal{A}'\mathcal{B}$. A short calculation (see [1–3]) shows that this transformation is described by the pinching channels, defined by

$$\begin{aligned} T_0[\rho] &:= (\Pi_0^{A_0} \otimes \mathbf{1})\,\rho\,(\Pi_0^{A_0} \otimes \mathbf{1}) + (\Pi_1^{A_0} \otimes \mathbf{1})\,\rho\,(\Pi_1^{A_0} \otimes \mathbf{1}) \\ T_1[\rho] &:= (\Pi_0^{A_1} \otimes \mathbf{1})\,\rho\,(\Pi_0^{A_1} \otimes \mathbf{1}) + (\Pi_1^{A_1} \otimes \mathbf{1})\,\rho\,(\Pi_1^{A_1} \otimes \mathbf{1}). \end{aligned} \tag{10}$$

Following the definitions of the pinching channels, we have the identities $T[\rho] = T \circ T[\rho] = T^*[\rho]$ and also $f(T[\rho]) = T[f(T[\rho])]$ when used within a functional calculus for a measurable function f. Hence, we can conclude that:

$$\begin{aligned} H(T[\rho]) - H(\rho) &= -\operatorname{tr}(T[\rho]\log(T[\rho])) + \operatorname{tr}(\rho\log(\rho)) \\ &= -\operatorname{tr}(\rho T^*[\log(T[\rho])]) + \operatorname{tr}(\rho\log(\rho)) \\ &= -\operatorname{tr}(\rho\log(T[\rho])) + \operatorname{tr}(\rho\log(\rho)) \\ &= D(\rho\|T[\rho]), \end{aligned} \tag{11}$$

where $D(\rho\|\sigma)$ denotes the relative entropy. Therefore, we can rewrite the convex mixture of conditional entropies as

$$\begin{aligned} &\lambda H(A_0|E) + (1-\lambda)H(A_1|E) \\ &= \lambda H(T_0[\rho_{AB}]) - \lambda H(\rho_{AB}) + (1-\lambda)H(T_1[\rho_{AB}]) - (1-\lambda)H(\rho_{AB}) \\ &= \lambda D(\rho_{AB}\|T_0[\rho_{AB}]) + (1-\lambda)D(\rho_{AB}\|T_1[\rho_{AB}]) \end{aligned} \tag{12}$$

Thus, we are able to bound Eve's conditional uncertainty on the measurement outcomes from any convex mixture of measurement bases by estimating the entropy production on the Alice-Bob system.

B. Restriction to qubits

In this subsection, we will show that for the purpose of bounding $C^*(S)$, we could without loss of generality consider Alice-Bob system as a convex combination of two-qubits states.

A fundamental theorem on the algebra generated by a pair of two projections [6–9], which will be in our case $(\Pi_0^{A_0}, \Pi_0^{A_1})$ such as $(\Pi_0^{B_2}, \Pi_0^{B_3})$, states that we can always find a representation of the respective system of Alice and Bob that allows us to decompose the projectors into 2×2 blocks and a commuting rest.

In particular, let K^A, L^A, K^B and L^B be pairwise commuting projectors and let

$$Q(\theta) = \begin{pmatrix} \cos(\theta/2)^2 & \cos(\theta/2)\sin(\theta/2) \\ \cos(\theta/2)\sin(\theta/2) & \sin(\theta/2)^2 \end{pmatrix} \tag{13}$$

be a family of 2×2 projectors. Then, we can decompose

$$\Pi_0^{A_0} = \bigoplus_j \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \oplus K^A \text{ and } \Pi_0^{A_1} = \bigoplus_j Q(\varphi_j) \oplus L^A \tag{14}$$

$$\Pi_0^{B_2} = \bigoplus_l \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \oplus K^B \text{ and } \Pi_0^{B_3} = \bigoplus_l Q(\omega_l) \oplus L^B \tag{15}$$

where $\{\varphi_j\}$ and $\{\omega_l\}$ are families of angles that can be obtained from the spectra of $\sigma(\Pi_0^{A_0} + \Pi_0^{A_1})$ and $\sigma(\Pi_0^{B_2} + \Pi_0^{B_3})$ respectively (see [9] for details). The representations of the remaining projectors $\Pi_1^{A_0}, \Pi_1^{A_1}, \Pi_1^{B_2}$ and $\Pi_1^{B_3}$ follow from the identities

$$\Pi_1^{A_X} = \mathbf{1} - \Pi_0^{A_X} \text{ and } \Pi_1^{B_Y} = \mathbf{1} - \Pi_0^{B_Y}. \tag{16}$$

Furthermore, we can also always find channels T^A_{block}, T^B_{block} and $T^{AB}_{block} := T^A_{block} \otimes T^B_{block}$ that diagonalise the entire systems of Alice and Bob into the corresponding blocks of (14) and (15). Applying these channels on an arbitrary state ρ_{AB} will therefore give us a corresponding decomposition

$$T^{AB}_{block}[\rho_{AB}] = \bigoplus_{jl} \mu_{jl} \rho^{jl} \oplus \mu_{rest} \sigma_{rest}, \tag{17}$$

where σ_{rest} denotes the projection of ρ_{AB} into blocks that are commuting on either Alice's and/or Bob's side while the coefficients μ_{jl} can be obtained by renormalising $T^{AB}_{block}[\rho_{AB}]$ blockwise (see [4]). As the pinching channels T_0 and T_1 commute with T^{AB}_{block} by construction and by using data processing, we can estimate

$$\begin{aligned} &\lambda D(\rho_{AB} \| T_0[\rho_{AB}]) + (1-\lambda) D(\rho_{AB} \| T_1[\rho_{AB}]) \\ &\geq \lambda D(T^{AB}_{block}[\rho_{AB}] \| T_0 \circ T^{AB}_{block}[\rho_{AB}]) + (1-\lambda) D(T^{AB}_{block}[\rho_{AB}] \| T_1 \circ T^{AB}_{block}[\rho_{AB}])) \\ &= \sum_{jl} \mu_{il} \left(\lambda D(\rho^{jl}_{AB} \| T_0[\rho^{jl}_{AB}]) + (1-\lambda) D(\rho^{jl}_{AB} \| T_1[\rho^{jl}_{AB}]) \right) + \mu_{rest} \left(\lambda D(\sigma_{rest} \| T_0[\sigma_{rest}]) + (1-\lambda) D(\sigma_{rest} \| T_1[\sigma_{rest}]) \right). \end{aligned} \tag{18}$$

Relating back to the constraint of optimisation (7), we have $CHSH = T^{AB}_{block}[CHSH]$ which implies

$$\operatorname{tr}(\rho_{AB} CHSH) = S \Leftrightarrow \operatorname{tr}\left(\rho^{jl}_{AB} CHSH\right) = S^{jl} \text{ and } \sum_{jl} \mu_{jl} S^{jl} = S, \tag{19}$$

where we already took into account that σ_{rest} will not play any role in the following optimisation as $|\operatorname{tr}(\sigma_{rest} CHSH)| \leq 2$ since the corresponding blocks commute on at least one side. Using the above relations, we can optimise every ρ^{jl}_{AB} individually and reformulate (7) as

$$C^*(S) = \inf_{A_0,A_1,B_2,B_3} \inf_{\substack{\{\mu_{jl}\} \\ \sum_{jl} \mu_{jl} \leq 1}} \inf_{\substack{\{S^{jl}\} \\ \sum_{jl} \mu_{jl} S^{jl} = S}} \sum_{jl} \mu_{jl} \begin{array}{l} \inf_{\rho^{jl}} \ \lambda D(\rho^{jl}_{AB} \| T_0[\rho^{jl}_{AB}]) + (1-\lambda) D(\rho^{jl}_{AB} \| T_1[\rho^{jl}_{AB}]) \\ \text{s.th.:} \ \ \langle CHSH \rangle_{\rho^{jl}_{AB}} = S^{jl} \end{array} \tag{20}$$

In the above we lower bound $\inf_{\rho^{jl}}[\dots]$ by the function

$$C^*_{\mathbb{C}^{4\times 4}}(S) = \inf_{\varphi,\omega} \begin{array}{l} \inf_{\rho^{jl}} \ \lambda D(\rho^{jl}_{AB} \| T_0[\rho^{jl}_{AB}]) + (1-\lambda) D(\rho^{jl}_{AB} \| T_1[\rho^{jl}_{AB}]) \\ \text{s.th.:} \ \ \langle CHSH \rangle_{\rho^{jl}_{AB}} = S \end{array} \tag{21}$$

Since (21) is by construction independent of the specific angles of the underlying measurements A_0, A_1, B_2, B_3, we can reduce the optimisation over all measurements A_0, A_1, B_2, B_3 to an optimisation over all possible $\{\mu_{jl}\}$. Hence we can conclude the bound

$$\begin{aligned} C^*(S) &\geq \inf_{A_0,A_1,B_2,B_3} \inf_{\substack{\{\mu_{jl}\} \\ \sum_{jl} \mu_{jl} \leq 1}} \inf_{\substack{\{S^{jl}\} \\ \sum_{jl} \mu_{jl} S^{jl} = S}} \sum_{jl} \mu_{jl} \quad C^*_{\mathbb{C}^{4\times 4}}(S^{jl}) \\ &\geq \inf_{\mu} \quad \int_{S'=2}^{2\sqrt{2}} \mu(dS') \, C^*_{\mathbb{C}^{4\times 4}}(S') \\ &\quad \text{s.th.:} \quad \mu([2, 2\sqrt{2}]) \leq 1, \quad \mu \geq 0, \quad \int_{S'=2}^{2\sqrt{2}} \mu(dS') S' = S, \end{aligned} \tag{22}$$

by estimating the optimisation over all $\{\mu_{jl}\}$ of arbitrary length via an integral over a positive sub-normalised measure μ. The boundaries of the above integration originate from the simple observation that S can not be larger than $2\sqrt{2}$ and that $C^*_{\mathbb{C}^{4\times 4}}(S^{jl}) = 0$ for all $S \leq 2$, which in fact also gives us the justification to ignore the σ_{rest} contribution in (18).

At this point, we can write down an explicit matrix representation of the CHSH operator. For reasons that will be clear in the following steps, it is convenient to decompose the CHSH operator with respect to Bob's measurements as

$$CHSH = F_0 + b_x F_x + b_z F_z \tag{23}$$

with

$$\begin{aligned}
&b_x = \sin(\omega) \qquad b_z = \cos(\omega)\\
&F_0 = \begin{pmatrix} \cos(\varphi)-1 & 0 & -\sin(\varphi) & 0\\ 0 & 1-\cos(\varphi) & 0 & \sin(\varphi)\\ -\sin(\varphi) & 0 & 1-\cos(\varphi) & 0\\ 0 & \sin(\varphi) & 0 & \cos(\varphi)-1 \end{pmatrix}\\
&F_x = \begin{pmatrix} 0 & 2\cos^2\left(\frac{\varphi}{2}\right) & 0 & -\sin(\varphi)\\ 2\cos^2\left(\frac{\varphi}{2}\right) & 0 & -\sin(\varphi) & 0\\ 0 & -\sin(\varphi) & 0 & -2\cos^2\left(\frac{\varphi}{2}\right)\\ -\sin(\varphi) & 0 & -2\cos^2\left(\frac{\varphi}{2}\right) & 0 \end{pmatrix}\\
&F_z = \begin{pmatrix} -\cos(\varphi)-1 & 0 & \sin(\varphi) & 0\\ 0 & \cos(\varphi)+1 & 0 & -\sin(\varphi)\\ \sin(\varphi) & 0 & \cos(\varphi)+1 & 0\\ 0 & -\sin(\varphi) & 0 & -\cos(\varphi)-1 \end{pmatrix}
\end{aligned} \tag{24}$$

and reformulate the optimisation over Bob's angle ω as an optimisation over two parameters b_x, b_z fulfilling the constraint $b_x^2 + b_z^2 = 1$. Hence our optimisation problem for a single two-qubit state reads

$$C^*_{\mathbb{C}^{4\times 4}}(S) := \inf_{\varphi\in[0,\pi/2]} \inf_{\substack{(b_x,b_z)\\ b_x^2+b_z^2=1}} \begin{array}{ll} \inf_\rho & \lambda D(\rho\|T_0[\rho]) + (1-\lambda) D(\rho\|T_1[\rho])\\ \text{s.th.:} & \langle F_0\rangle_\rho + b_x\langle F_x\rangle_\rho + b_z\langle F_z\rangle_\rho = S \end{array}, \tag{25}$$

where we will, with a slight abuse of notation, denote the pinching channels for the reduced 2×2 measurements as T_0 and T_1 as well.

C. Estimating the relative entropy via the trace norm (Pinsker++)

In this subsection, we will show that a lower bound of $C^*_{\mathbb{C}^{4\times 4}}(S)$ is related to an optimisation with its objective function given by a combination of trace norms. As such, this optimisation can be efficiently bounded as shown in the following subsections. Here, we employ a refined version of Pinsker's inequality provided in Theorem 1 (also see [10]): for a pinching channel with two-outcomes we can lower bound the relative entropy between its input and output by their trace norm via

$$D(\rho\|T_X[\rho]) \geq \log(2) - h_2\left(\frac{1}{2} - \frac{1}{2}\left\|\rho - T_X[\rho]\right\|_1\right), \tag{26}$$

where $h_2(p) = -p\log p - (1-p)\log(1-p)$ denotes the binary entropy function. Using the above inequality and the concavity of the binary entropy, we could write

$$\begin{aligned}
&\lambda D(\rho\|T_0[\rho]) + (1-\lambda) D(\rho\|T_1[\rho]) \qquad (27)\\
&\geq \log(2) - \lambda h_2\left(\frac{1}{2} - \frac{1}{2}\left\|\rho - T_0[\rho]\right\|_1\right) - (1-\lambda) h_2\left(\frac{1}{2} - \frac{1}{2}\left\|\rho - T_1[\rho]\right\|_1\right)\\
&\geq \log(2) - h_2\left(\frac{1}{2} - \frac{1}{2}\Big(\lambda\left\|\rho - T_0[\rho]\right\|_1 + (1-\lambda)\left\|\rho - T_1[\rho]\right\|_1\Big)\right)
\end{aligned}$$

which is a monotonous function of the sum of the trace norms. Hence, we can employ the inequality

$$C^*_{\mathbb{C}^{4\times 4}}(S) \geq \log(2) - h_2\left(\frac{1}{2} - \frac{1}{2}t\right) \tag{28}$$

for any $t \leq t^*(S)$ that gives a lower bound on the optimisation

$$t^*(S) := \boxed{\inf_{\varphi\in[0,\pi/2]} \quad \boxed{\inf_{\substack{(b_x,b_z)\\ b_x^2+b_z^2=1}} \quad \boxed{\begin{array}{ll} \inf_\rho & \lambda\left\|\rho - T_0[\rho]\right\|_1 + (1-\lambda)\left\|\rho - T_1[\rho]\right\|_1 \\[1ex] \text{s.th.:} & \langle F_0\rangle_\rho + b_x\langle F_x\rangle_\rho + b_z\langle F_z\rangle_\rho = S \end{array}}}} \tag{29}$$

The boxes in (29) highlight different stages in the optimisation that will be addressed individually in the following three subsections.

D. Optimisation of ρ for fixed angles: $\boxed{\textbf{reformulation as SDP}}$

In this subsection, we will formulate the minimisation over ρ (black box in (29)) as a SDP, which can be solved using existing numerical algorithms. To this end, we will use a well-known relation that the trace norm of a quadratic matrix V can be represented by the minimisation (refer to [11])

$$\|V\|_1 = \inf_{K,L} \frac{1}{2}\operatorname{tr}(K+L) \quad \text{s.th.:} \begin{pmatrix} K & V \\ V^\dagger & L \end{pmatrix} \geq 0. \tag{30}$$

over additional matrices K and L. We can explicitly expand the channels T_X in terms of the measurement projectors, which can be written as

$$\rho - T_1(\rho) = \rho Q(\varphi) + Q(\varphi)\rho - 2Q(\varphi)\rho Q(\varphi) \text{ and } \rho - T_0(\rho) = \rho Q(0) + Q(0)\rho - 2Q(0)\rho Q(0). \tag{31}$$

Hence, we can rewrite the minimisation over ρ as the following SDP:

$$\boxed{\begin{array}{ll} \inf_\rho & \lambda\left\|\rho - T_0[\rho]\right\|_1 + (1-\lambda)\left\|\rho - T_1[\rho]\right\|_1 \\[1ex] \text{s.th.:} & \langle F_0\rangle_\rho + b_x\langle F_x\rangle_\rho + b_z\langle F_z\rangle_\rho = S \end{array}} \tag{32}$$

$$\begin{aligned} = \inf_{\substack{\rho\\ K_0,L_0,K_1,L_1}} \quad & \lambda\operatorname{tr}(K_0+L_0) + (1-\lambda)\operatorname{tr}(K_1+L_1) \\ \text{s.th.:} \quad & \begin{pmatrix} K_0 & \rho Q(0) + Q(0)\rho - 2Q(0)\rho Q(0) \\ \rho Q(0) + Q(0)\rho - 2Q(0)\rho Q(0) & L_0 \end{pmatrix} && \geq 0 \\ & \begin{pmatrix} K_1 & \rho Q(\varphi) + Q(\varphi)\rho - 2Q(\varphi)\rho Q(\varphi) \\ \rho Q(\varphi) + Q(\varphi)\rho - 2Q(\varphi)\rho Q(\varphi) & L_1 \end{pmatrix} && \geq 0 \\ & \qquad\qquad\qquad \operatorname{tr}\left(\rho(F_0 + b_xF_x + b_zF_z)\right) && = S. \end{aligned} \tag{33}$$

E. Optimisation of Bob's angle: $\boxed{\textbf{an outer approximation to } b_x, b_z}$

The minimisation over Bob's measurement angle (the magenta box in (29)) was formulated as an optimisation over parameters (b_x, b_z) from a set

$$\mathcal{K} = \{(b_x, b_z) | b_x^2 + b_z^2 = 1\}, \tag{34}$$

which can be interpreted as boundary of a circle with unit radius. Since the objective function of (29) does not explicitly depends on (b_x, b_z), we could move this minimisation directly into the constraints and write

$$\boxed{\inf_{\substack{b_x,b_z\\ b_x^2+b_z^2=1}} \boxed{\begin{array}{ll}\inf_\rho & \lambda \left\|\rho - T_0[\rho]\right\|_1 + (1-\lambda)\left\|\rho - T_1[\rho]\right\|_1 \\[1em] \text{s.th.:} & \langle F_0\rangle_\rho + b_x\langle F_x\rangle_\rho + b_z\langle F_z\rangle_\rho = S\end{array}}} \tag{35}$$

$$= \begin{array}{ll}\inf_\rho & \lambda \left\|\rho - T_0[\rho]\right\|_1 + (1-\lambda)\left\|\rho - T_1[\rho]\right\|_1 \\[1em] \text{s.th.:} & \exists (b_x, b_z) \in \mathcal{K}: \quad \langle F_0\rangle_\rho + b_x\langle F_x\rangle_\rho + b_z\langle F_z\rangle_\rho = S\end{array} \tag{36}$$

$$= \begin{array}{ll}\inf_\rho & \lambda \left\|\rho - T_0[\rho]\right\|_1 + (1-\lambda)\left\|\rho - T_1[\rho]\right\|_1 \\[1em] \text{s.th.:} & \sup\limits_{(b_x,b_z)\in\mathcal{K}} \quad \langle F_0\rangle_\rho + b_x\langle F_x\rangle_\rho + b_z\langle F_z\rangle_\rho \geq S.\end{array} \tag{37}$$

Clearly, the above problem is no longer a convex optimisation problem but there exists a convex relaxation by replacing $\mathcal{K}$ with any convex set $\mathcal{P} \supseteq \mathcal{K}$. We will replace $\mathcal{K}$ by a compact convex polytope $\mathcal{P}$ with finite set of vertices (p_x^l, p_z^l). Since the individual constraints in (35) are linear in b_x, b_z, it suffices to only consider points on these vertices. As such, we can efficiently lower bound (35) via

$$(35) \geq \begin{array}{ll}\inf_\rho & \lambda \left\|\rho - T_0[\rho]\right\|_1 + (1-\lambda)\left\|\rho - T_1[\rho]\right\|_1 \\[1em] \text{s.th.:} & \sup\limits_{(b_x,b_z)\in\mathcal{P}} \quad \langle F_0\rangle_\rho + b_x\langle F_x\rangle_\rho + b_z\langle F_z\rangle_\rho \geq S\end{array} \geq \begin{array}{ll}\inf_l \inf_\rho & \lambda \left\|\rho - T_0[\rho]\right\|_1 + (1-\lambda)\left\|\rho - T_1[\rho]\right\|_1 \\[1em] \text{s.th.:} & \langle F_0\rangle_\rho + p_x^l\langle F_x\rangle_\rho + p_z^l\langle F_z\rangle_\rho \geq S\end{array} \tag{38}$$

The above structure can now be incorporated in a simple algorithm (illustrated in Fig. 2) that computes the optimisation of Bob's measurements via a sequence of lower bounds (also see [12, 13] where a similar method was used for 3-dimensional problems). The algorithm is given by:

(i) Start by initiating $\mathcal{P}$ as a rectangle that contains $\mathcal{K}$.

(ii) Use (32) to compute the value of (38) for every vertices $(p_x^1, p_z^1) \ldots (p_x^n, p_z^n)$ of $\mathcal{P}$.

(iii) Pick the first vertex b_{min} that attains the minimum in (38) and refine $\mathcal{P}$ by introducing a new edge to $\mathcal{P}$ that is tangential to $\mathcal{K}$. This will "cut off" b_{min} and create two new vertices (see Fig.2). Proceed to (ii).

Repeating *(ii)* and *(iii)* will give a progressive refinement of $\mathcal{P}$ that approaches the boundary of $\mathcal{K}$ from the outside at the vicinity of those points (b_x, b_z) that realise the minimum of (29). It turns out that, this algorithm only requires a few iterations to achieve a very high precision for our above-mentioned problem.

F. Optimisation of Alice's angle: an ε-net for φ

For the representation given by equation (14), Alice's measurement on her qubit is fully described by the angle φ, which could take values in the interval $[0, \pi/2]$. Consequently, the minimisation over Alice's measurement angle (cyan box in (29)) is not an SDP.

In this subsection, we will show how one could obtain a bound on the minimisation over Alice's measurement angle by employing an ε-net. The basic idea of the ε-net is as follows: we split the interval $[0, \pi/2]$ into smaller segments of size $2\varepsilon_0$ each centred around a discretised range-point φ_i. We then evaluate (29) (i.e. everything in the magenta box) on each discretised range-point and subtract a pessimistic error $\Delta(\varepsilon_0, \varphi)$, which bounds how much would the value of (29) have changed when evaluated on any other φ within the segment. Taking the minimal value over all segments will then give us a lower bound on the whole optimisation (29)(cyan box).

Refining those segments into even smaller ones will give tighter lower bounds. In order to keep the total computational cost low, we successively refine only the segment that gives the minimum value for a given round of the procedure. By doing so, we arrive in a situation (see Fig.3) where we only have to improve our refinement around a single point corresponding to the global minimum, i.e. the single φ that achieves $C^*_{\mathbb{C}^{4\times4}}(S)$.

In order to bound the error of each segment, we will need to investigate the relation between the entire optimisation and Alice's measurement angle φ. Varying φ (see (14)) will affect the two inner optimisations of (29) in two ways: On

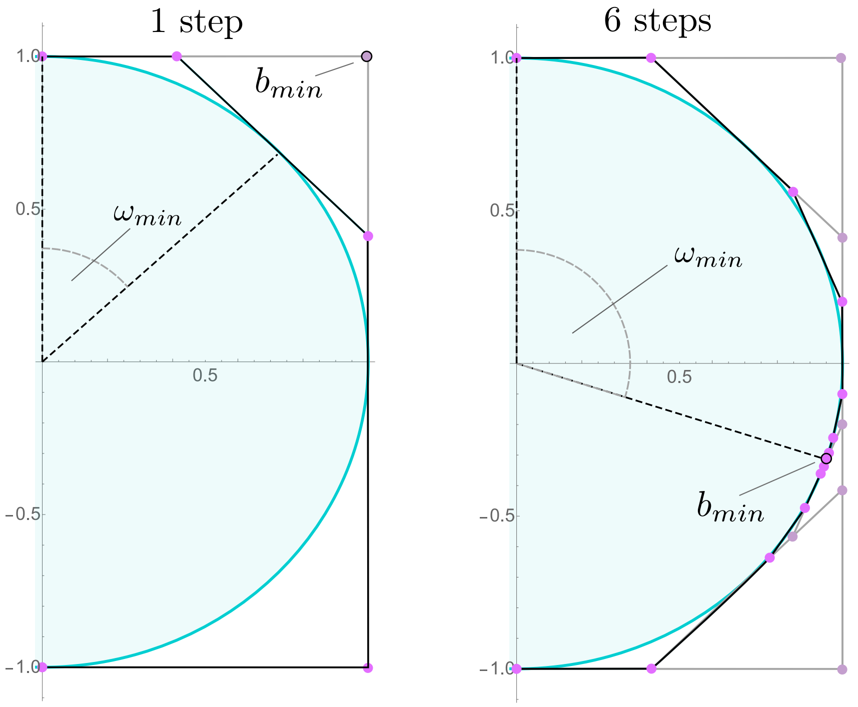

Fig. 2. **Minimising** ω**:** Iterative refinement of $\mathcal{P}$ (magenta vertices, black edges) to identify the optimal ω in $\mathcal{K}$ (cyan semicircle). The parameters considered in the diagram is given by $\lambda = 0.2$, $S = 2.4$ and $\varphi = 1.2$. In every iteration of our algorithm, we identify b_{min} (grey circles), the vertex of $\mathcal{P}$ that gives the minimum value of optimisation (38), and remove it by introducing a new edge. In this example, six iterations are sufficient to achieve a target precision of 10^{-5}.

one hand, since the objective function depends on φ via the $T_1(\rho)$, it will change with varying φ. On the other hand, the feasible set of possible ρ_{AB} will change with varying φ since the CHSH operator, i.e. F_0, F_x and F_z, depends on φ as well.

We will now address the dependence of the CHSH operator on φ. Without loss of generality we could have reformulated (29) by considering all states that could achieve a Bell violation *greater* than or equals the observed CHSH value S as it is a valid relaxation of the optimisation problem. This implies that for fixed φ we could also perform our optimisation over the set

$$\mathcal{S}_{\varphi}^{S} := \{\rho | \langle CHSH|_{\varphi}\rangle_{\rho} \geq S\}\,. \tag{39}$$

When we change φ to $\varphi + \varepsilon$, on a segment specified by $|\varepsilon| \leq \varepsilon_0$, we have to consider a different set of states $\mathcal{S}_{\varphi+\varepsilon}^{s}$. Hence, the optimal solution on the whole segment around φ will be attained on a state from the set

$$\overline{\mathcal{S}}_{\varepsilon_0\varphi}^{S} := \bigcup_{|\varepsilon|\leq\varepsilon_0} \mathcal{S}_{\varphi+\varepsilon}^{S} \tag{40}$$

We consider the norm of the difference of the two CHSH operators and we have:

$$\begin{aligned}
&\|CHSH|_{\varphi} - CHSH|_{\varphi-\varepsilon}\|_{\infty} \\
&= \|(F_0 + b_xF_x + b_zF_z)|_{\varphi} - (F_0 + b_xF_x + b_zF_z)|_{\varphi-\varepsilon}\|_{\infty} \\
&= 2\|(Q(\varphi) - Q(\varphi-\varepsilon)) \otimes (C^{B_2} + C^{B_3})\|_{\infty} \\
&\leq 4\|Q(\varphi) - Q(\varphi-\varepsilon)\|_{\infty} \\
&\leq 4 \max_{\varphi,|\varepsilon|\leq\varepsilon_0} \|Q(\varphi) - Q(\varphi-\varepsilon)\|_{\infty} && (41)\\
&= 4 \max_{\varphi,|\varepsilon|\leq\varepsilon_0} \left\| \begin{pmatrix} \cos(\frac{\varphi}{2})^2 - \cos(\frac{\varphi-\varepsilon}{2})^2 & \cos(\frac{\varphi}{2})\sin(\frac{\varphi}{2}) - \cos(\frac{\varphi-\varepsilon}{2})\sin(\frac{\varphi-\varepsilon}{2}) \\ \cos(\frac{\varphi}{2})\sin(\frac{\varphi}{2}) - \cos(\frac{\varphi-\varepsilon}{2})\sin(\frac{\varphi-\varepsilon}{2}) & \sin(\frac{\varphi}{2})^2 - \sin(\frac{\varphi-\varepsilon}{2})^2 \end{pmatrix} \right\|_{\infty} && (42)\\
&= 4 \max_{|\varepsilon|\leq\varepsilon_0} \sqrt{\frac{1}{2} - \frac{1}{2}\cos(\varepsilon)} && (43)\\
&\leq 2\varepsilon_0, && (44)
\end{aligned}$$

where we assumed that $b_x^2 + b_z^2 = 1$ holds up to a negligible deviation as sufficient iterations are taken in the outer approximation shown in Fig. 2 (otherwise, adding a further factor $\approx 1 + \epsilon$ will be required). From the above relation, we conclude that every state ρ that could attain a CHSH value S for measurements with the measurement angle $\varphi + \varepsilon$ will attain a CHSH value of at least $S - 2\varepsilon_0$ with the measurements angle φ. Hence, we have the inclusion relation:

$$\overline{\mathcal{S}}_{\varepsilon_0\varphi}^{S} \subseteq \mathcal{S}_{\varphi}^{S-2\varepsilon_0}. \tag{45}$$

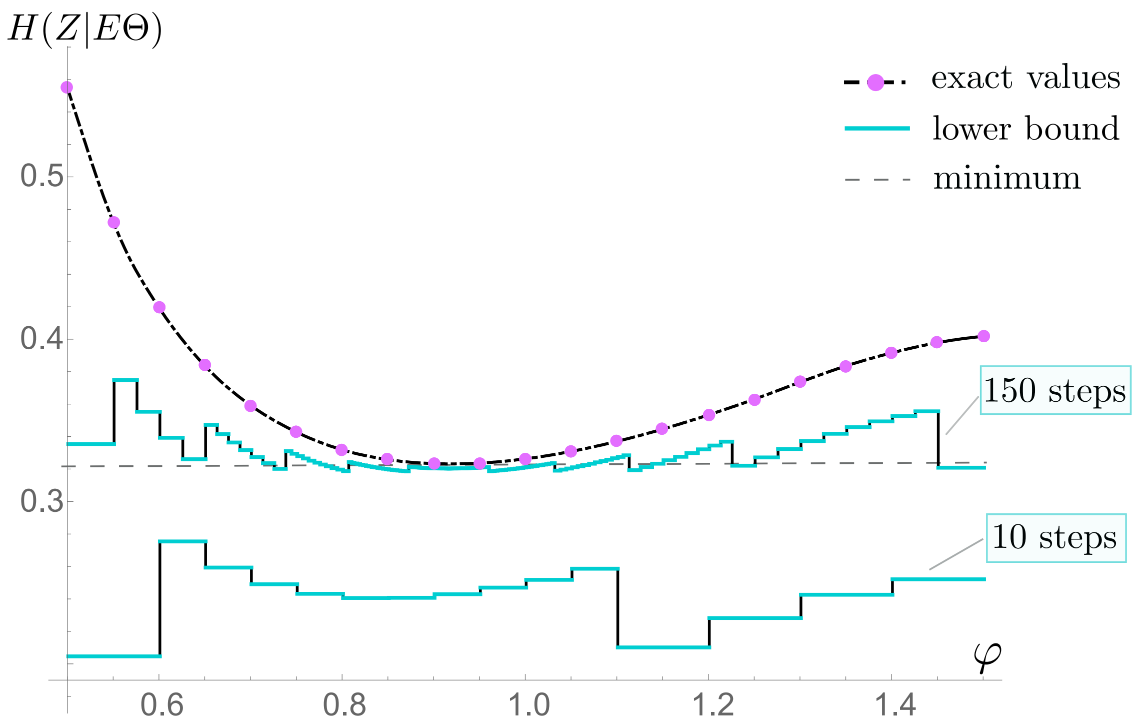

Fig. 3. **Adaptive refinement of the ε-net** Lower bounds on $H(Z|E\theta)$, by evaluating (28) on segments. (For comparison) The magenta coloured points give the exact value of (29) for a discretised range of different φ. (The actual bound) The cyan coloured line gives a pessimistic lower bound (not assuming continuity) valid for a segment of length ε_0 centred around a specific φ. Fixing the width of a segment, ε_0, to be fine enough will give a tighter lower bound. In order to perform the computation efficiently, we start with a rough discretised range with a large segment size. We then identify and refine the segment with the lowest estimate on the target function $H(Z|E\theta)$ and we repeat this procedure.

which means that we can perform optimisation (29) by replacing S with $S - 2\varepsilon_0$ on each segment of size $2\varepsilon_0$ (see Fig. 4) to obtain a reliable lower bound.

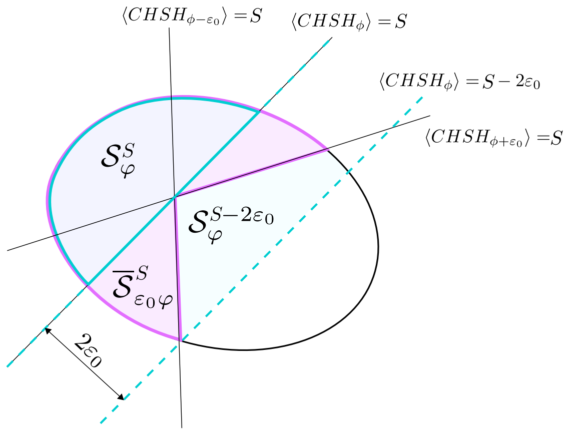
$\langle CHSH_{\phi-\varepsilon_0}\rangle = S$
$\langle CHSH_{\phi}\rangle = S$
$\langle CHSH_{\phi}\rangle = S - 2\varepsilon_0$
$\langle CHSH_{\phi+\varepsilon_0}\rangle = S$
$\mathcal{S}_\varphi^S$
$\mathcal{S}_\varphi^{S-2\varepsilon_0}$
$\overline{\mathcal{S}}_{\varepsilon_0\varphi}^S$
$2\varepsilon_0$

Fig. 4. **Feasible sets:** The optimisation for a fixed φ runs over a set $\mathcal{S}_\varphi^S$, i.e. all states with CHSH values larger than or equals to S. Varying φ by not more than ε_0 will not change the CHSH value by more than $2\varepsilon_0$. Therefore, the set $\mathcal{S}_\varphi^{S-2\varepsilon_0}$ includes all states that can attain CHSH value larger than or equals to S for some angle in the interval $(\varphi - \varepsilon_0, \varphi + \varepsilon_0)$.

We are now left with assessing the change in the objective of (29) introduced by varying φ, i.e. the error of the functional. Using Hölder's inequality, we can dualise the trace norm of an operator X as

$$\|X\|_1 = \sup_{Y:\|Y\|_\infty = 1} \mathrm{tr}(YX) \tag{46}$$

and for suitably chosen M,N with $\|M\|_\infty = \|N\|_\infty = 1$, we can rewrite the objective of (29) as

$$f_{M,N}(\varphi,\rho) := \langle \lambda\{M, Q(0)\} - \lambda Q(0)MQ(0) + (1-\lambda)\{N, Q(\varphi)\} - (1-\lambda)Q(\varphi)NQ(\varphi)\rangle_\rho \tag{47}$$

Here, we could bound the following expression by:

$$\begin{aligned}&|f_{M,N}(\varphi,\rho)-f_{M,N}(\varphi+\varepsilon,\rho)|\\&\leq(1-\lambda)\sup_{N,\varphi,\varepsilon}\Big\|\{N,Q(\varphi)\}-Q(\varphi)NQ(\varphi)-\{N,Q(\varphi+\varepsilon)\}+Q(\varphi+\varepsilon)NQ(\varphi+\varepsilon)\Big\|_\infty\\&\leq(1-\lambda)4\varepsilon_0\end{aligned}\tag{48}$$

which follows after a short computation from the central estimate $\|(Q(\varphi)-Q(\varphi+\varepsilon))\|_\infty\leq\varepsilon_0/2$, which was already computed in (44).

Thus, by combining (44) and (48), we can estimate the maximal error on a segment around some fixed φ. Applying this estimate and the technique described above to (29), finally gives

$$\begin{aligned}t^*(S)=&\boxed{\inf_{\varphi\in[0,\pi/2]}\;\boxed{\inf_{\substack{(b_x,b_z)\\b_x^2+b_z^2=1}}\;\boxed{\begin{array}{ll}\inf_\rho & \lambda\left\|\rho-T_0[\rho]\right\|_1+(1-\lambda)\left\|\rho-T_1[\rho]\right\|_1\\ \text{s.th.:} & \langle F_0\rangle_\rho+b_x\langle F_x\rangle_\rho+b_z\langle F_z\rangle_\rho=S\end{array}}}}\\&\geq\inf_{\varphi_k\in\mathcal{I}}\inf_l\begin{array}{ll}\inf_\rho & \lambda\left\|\rho-T_0[\rho]\right\|_1+(1-\lambda)\left\|\rho-T_1[\rho]\right\|_1-2(1-\lambda)\varepsilon_0^k\\ \text{s.th.:} & \langle F_0\rangle_\rho+b_x\langle F_x\rangle_\rho+b_z\langle F_z\rangle_\rho=S-2\varepsilon_0^k\end{array}\end{aligned}\tag{49}$$

where ε_0^k denotes the according segment width and $\varphi_k\in\mathcal{I}$ denote the angles which form the discretised range as described above and in Fig. 3.

G. Worst case convex hull over two-qubit strategies:

By employing the techniques described in the previous subsections, we are able to compute the two-qubit function $C^*_{\mathbb{C}^{4\times4}}(S)$ point-wise up to arbitrary precision. The only remaining step for computing the desired bound $C^*(S)$ is to estimate (22). We will tackle this problem by defining a convex function $\overline{C}(S)$ that is smaller or equals to $C^*_{\mathbb{C}^{4\times4}}(S)$ for all $S\in(2,2\sqrt{2})$, (see Fig. 5). Given such a function $\overline{C}(S)$, we can conclude that

$$\begin{aligned}C^*(S)&=\inf_{\mu:\langle S'\rangle_\mu=S}\int_{S'=2}^{2\sqrt{2}}\mu(dS')\,C^*_{\mathbb{C}^{4\times4}}(S')\\&\geq\inf_{\mu:\langle S'\rangle_\mu=S}\int_{S'=2}^{2\sqrt{2}}\mu(dS')\,\overline{C}(S')\\&=\inf_{\mu:\langle S'\rangle_\mu=S}\overline{C}\left(\int_{S'=2}^{2\sqrt{2}}\mu(dS')\,S'\right)=\overline{C}(S).\end{aligned}\tag{50}$$

At this point, we note that the analytical result of [4], which is a special case of our computation for $\lambda=1$, shows that $C^*_{\mathbb{C}^{4\times4}}(S)$ is convex. This means that we can set $\overline{C}(S)=C^*_{\mathbb{C}^{4\times4}}(S)$ in the case of $\lambda=1$. The numerical evaluation of $C^*_{\mathbb{C}^{4\times4}}(S)$ suggest the same conclusion might actually hold for all $\lambda\in(0,1)$. However, we could not prove this analytically and therefore, the following steps is necessary.

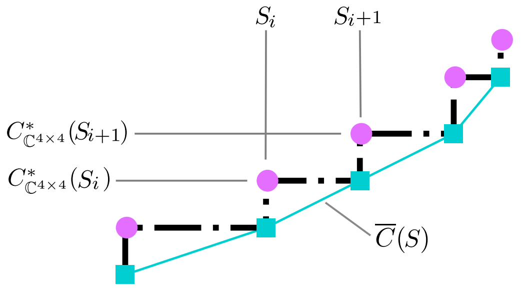
S_i
S_i+1
$C^*_{\mathbb{C}^{4\times4}}(S_i+1)$
$C^*_{\mathbb{C}^{4\times4}}(S_i)$
$\overline{C}(S)$

Fig. 5. **Convex bound:** given the value of $C^*_{\mathbb{C}^{4\times4}}(S)$ for a discretised range of values $\cdots\leq S_i\leq S_{i+1}\leq\ldots$ (magenta points) allows us to estimate $C^*_{\mathbb{C}^{4\times4}}(S)$ from below by taking the floor on every interval (dot-dashed black line). The extreme points of this graph are a subset of the points marked by cyan squares. From this we can easily compute the lower convex estimate $\overline{C}(S)$ (cyan line).

It is straight forward to see from the definition of (25) that $C^*_{\mathbb{C}^{4\times4}}(S)$ is a monotonous non-decreasing function, i.e. we have $C^*_{\mathbb{C}^{4\times4}}(S_1)\leq C^*_{\mathbb{C}^{4\times4}}(S_2)$ for $S_1\leq S_2$, since increasing S will impose more restrictions on Eve leaving her with a smaller set of possible attacks. The evaluation of $C^*_{\mathbb{C}^{4\times4}}(S)$ for a discretised range of values $S_0 = 2 \leq S_1 \leq S_2 \leq \cdots \leq S_N = 2\sqrt{2}$ will therefore enable us to estimate $C^*_{\mathbb{C}^{4\times4}}(S)$ from below for all values of S by taking the floor

$$\lfloor C^*_{\mathbb{C}^{4\times4}}(S) \rfloor := C^*_{\mathbb{C}^{4\times4}}(S_i) \qquad \forall S \in [S_i, S_{i+1}) \tag{51}$$

on every interval $[S_i, S_{i+1})$. Since this function is now defined on every S and is never larger than $C^*_{\mathbb{C}^{4\times4}}(S)$ itself, computing its lower convex hull by applying a Legendre transformation twice will give us a valid convex estimate $\overline{C}(S)$ (see Fig. 5).

H. A conjectured alternative proof

We observed from some numerical exploration that the states saturating optimisation (7) for $\lambda = 1/2$ appear to have the following two properties:

1. The reduced state on $\mathcal{AB}$ is Bell-diagonal with only two nonzero eigenvalues.
2. The states satisfy $P_g(A_0|E) = P_g(A_1|E)$, where $P_g(A_X|E)$ is Eve's maximum probability of guessing the outcome of measurement A_X.

Letting $\rho_{E|A_X}$ denote Eve's state conditioned on the outcome A_X, the first property would imply $F(\rho_{E|A_X=0}, \rho_{E|A_X=1})^2 = 1 - d(\rho_{E|A_X=0}, \rho_{E|A_X=1})^2$, where F is the root-fidelity and d is the trace distance. (This is because Eve's states would then be supported on a common qubit subspace, and this equality holds for qubit states when the states have the same eigenvalues [14], which is indeed the case here [4].) Using the fact that we can assume A_X to be uniform without loss of generality, it would then follow from the bound in [15] and the relation $d(\rho_{E|A_X=0}, \rho_{E|A_X=1}) = 2P_g(A_X|E) - 1$ that

$$H(A_X|E) \geq \log(2) - h_2\left(\frac{1 - F(\rho_{E|A_X=0}, \rho_{E|A_X=1})}{2}\right) = \log(2) - h_2\left(\frac{1 - \sqrt{4P_g(A_X|E)(1 - P_g(A_X|E))}}{2}\right). \tag{52}$$

Applying the second property would then imply[1]

$$\begin{aligned}\frac{1}{2}H(A_0|E) + \frac{1}{2}H(A_1|E) &\geq \log(2) - h_2\left(\frac{1 - \sqrt{4P_g(A_X|E)(1 - P_g(A_X|E))}}{2}\right) \text{ for either } X \\ &= \log(2) - h_2\left(\frac{1 - \sqrt{4P_g^{\text{avg}}(1 - P_g^{\text{avg}})}}{2}\right), \text{ where } P_g^{\text{avg}} = \frac{1}{2}P_g(A_0|E) + \frac{1}{2}P_g(A_1|E).\end{aligned} \tag{53}$$

The key point of this reduction is that the maximum value of P_g^{avg} (subject to a constraint on the CHSH value) can be bounded by SDP methods [16–18]. We computed the corresponding bounds, and found that they matched closely with the results obtained above. Hence if it could be proven that the two properties listed above indeed hold for the states saturating the optimisation in (7), this would provide an alternative approach to deriving our results. The benefit of such an approach is that it would be substantially faster, as it does not rely on computing an ε-net of points.

We remark that for the case $\lambda = 1$ (i.e. simply bounding the $H(A_0|E)$ term alone), we can prove that the first property holds, and thus Eq. (52) must hold in that scenario. In that case, we find that substituting the known closed-form bound on $P_g(A_0|E)$ in terms of the CHSH value [19] yields exactly the closed-form bound on $H(A_0|E)$ derived in Ref. [4]. This can be viewed as an alternative method to derive the latter bound, and it may be of interest to study how this approach could be generalised.

I. Approaches without the qubit reduction

Our analysis thus far relied on reducing the analysis to a qubit scenario. In principle, however, there are some approaches which could be used to tackle the optimisation (7) without this reduction, and we shall now briefly outline these possibilities. These approaches could potentially allow for more general applicability of our methods.

[1] If the bound (52) were convex with respect to $P_g(A_X|E)$, the second property would not be required; unfortunately, the bound is instead concave, so instead this approach only yields the desired final result *if and only if* the second property holds.

The first approach consists of noting that the trace norm terms in the optimisation (29) can be rewritten using

$$\|\rho - T[\rho]\|_1 = \sup_{-\mathbf{1} \leq M \leq \mathbf{1}} \operatorname{tr}(M(\rho - T[\rho])) = \sup_P \frac{1}{\|P\|_\infty} \operatorname{tr}(P(\rho - T[\rho])) = \sup_P \frac{1}{\|P\|_\infty} \operatorname{tr}((P - T[P])\rho), \tag{54}$$

where $\sup_P$ is taken over all Hermitian P, and for the last equality we used the fact that pinching channels are self-adjoint. Therefore, any choice of P yields a valid lower bound. In particular, if we choose P to be a (noncommutative) polynomial function of the measurement operators, then lower-bounding $\operatorname{tr}((P - T[P])\rho)$ is precisely a noncommutative polynomial optimisation of the type studied in [18], which can be solved by SDP methods *without* reducing the analysis to qubits. An advantage of this approach is that we can impose the full output statistics as constraints (similar to [1, 16, 17]) instead of just the CHSH value alone. As for the $\|P\|_\infty$ term, it can be upper-bounded separately by noting that $\|P\|_\infty = \sup_\sigma |\operatorname{tr}(P\sigma)| = \max\{\sup_\sigma \operatorname{tr}(P\sigma), \sup_\sigma \operatorname{tr}(-P\sigma)\}$, where $\sup_\sigma$ is taken over all normalised density operators σ. This is also of the right form to be bounded using the SDP method described in [18]. If P is chosen to be a polynomial of low degree, the corresponding SDPs are quite tractable and can be solved quickly (in particular, they are substantially simpler than the ones described in [1]).

Unfortunately, when we applied this method to the CHSH scenario, we were unable to find a choice of P that was sufficiently robust to noise for practical purposes. While we did find that it can yield a tight bound at maximum CHSH value, the bound quickly drops to zero once noise is added. It is not currently clear whether this is an inherent limitation of this approach, or whether some better choice of P might overcome this difficulty. (A possible cause of this suboptimality could be the fact that since the optimisations for $\operatorname{tr}((P - T[P])\rho)$ and $\|P\|_\infty$ were solved separately, this "decouples" them from each other, resulting in worse bounds than would be obtained from tackling (54) directly. The choice of P that certifies a tight bound at maximum CHSH violation was obtained by exploiting the fact that the states and measurements which attain maximum CHSH value are essentially unique, up to trivial local operations. Therefore, we were able to find an explicit operator P that saturates the variational characterisation in Eq. (54) and write it as a polynomial of those measurement operators. However, some care was still needed to choose the polynomial in such a way that the bound on $\|P\|_\infty$ is tight.)

A second approach is based on the method developed in [1]. To briefly summarise, the method described in that work essentially yields some possible choices of vector $\vec{\mu}$ and operator polynomials K_0, K_1 such that

$$H(A_X|E) \geq \vec{\mu} \cdot \vec{\gamma} - \log\langle K_X \rangle, \tag{55}$$

where $\vec{\gamma}$ is the list of all statistics estimated in the experiment (which could be, for instance, just the CHSH value alone but could also be all output statistics instead). We now note that for any $\alpha > 0$, we have $\log x \leq x/\alpha + \log\alpha - 1$ (this is simply the tangent line to $\log x$ at the point $x = \alpha$). Therefore, for any α_0, α_1 we would have

$$\lambda H(A_0|E) + (1-\lambda)H(A_1|E) \geq \lambda(\vec{\mu} \cdot \vec{\gamma} - \log\langle K_0 \rangle) + (1-\lambda)(\vec{\mu} \cdot \vec{\gamma} - \log\langle K_1 \rangle) \tag{56}$$

$$\geq \vec{\mu} \cdot \vec{\gamma} - \left\langle \frac{\lambda}{\alpha_0} K_0 + \frac{1-\lambda}{\alpha_1} K_1 \right\rangle - \lambda \log\alpha_0 - (1-\lambda)\log\alpha_1 + 1. \tag{57}$$

In this final expression, $\langle (\lambda/\alpha_0)K_0 + ((1-\lambda)/\alpha_1)K_1 \rangle$ is again an operator polynomial of a form which can be bounded using the SDPs in [18] without requiring the qubit reduction. By optimising over choices of the two tangent points α_X (as well as the vector $\vec{\mu}$ and operator polynomials K_X), we were able to compute some bounds on the main optimisation (7), imposing constraints based on the full output statistics. However, we found that while the resulting bounds are indeed better than the bounds on $H(A_0|E)$ alone, the improvement was fairly small (in particular, the resulting curves were worse than those shown in the main text). Hence we were also unable to use this approach to obtain tight bounds in this situation, though in contrast to the first approach above, it performs well at moderate noise values rather than low noise values. Again, it is not currently clear whether it might be possible to improve on this finding with a better choice of the variational parameters $\alpha_X, \vec{\mu}, K_X$. (In fact, the parameter $\vec{\mu}$ could also be optimised separately for each term $H(A_X|E)$, but this is computationally expensive.)

J. States saturating the bounds

As discussed in the main part, it is sufficient to only consider the cases $\lambda = 1$(fixed bases) and $\lambda = 1/2$(uniform basis choice) within our protocol. For $\lambda = 1$ the (lower) bound $C^*(S)$ resembles the one from Acìn et. al. [4], which was proven to be optimal in the sense that it can be achieved by an explicit choice of states and measurements.

For $\lambda = 1/2$, we found heuristically that the bound $C^*_{\mathbb{C}^{4\times4}}(S)$ appears to be saturated by states of the form

$$\rho_a = a\psi^+ + (1-a)\psi^- \tag{58}$$

and measurements given by projectors

$$\Pi_0^{A_0} = \frac{1}{2}\begin{pmatrix} 1+\sin(\tau) & \cos(\tau) \\ \cos(\tau) & 1-\sin(\tau) \end{pmatrix} \qquad \Pi_0^{A_1} = \begin{pmatrix} 1+\sin(\tau) & -\cos(\tau) \\ -\cos(\tau) & 1-\sin(\tau) \end{pmatrix}$$
$$\Pi_0^{B_0} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \qquad \Pi_0^{B_1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{59}$$

with parameters (a, τ) given as optimisers of the program

$$\begin{aligned} k^* := \min_{a,\tau} \quad & 4 - 16(1-a)a\sin(\tau)^2 \\ s.th.: \quad & (4a-2)\cos(\tau) + 2\sin(\tau) = S \quad \frac{1}{2} \le a \le 1 \quad 0 \le \tau \le \pi/2. \end{aligned} \tag{60}$$

Furthermore, we find numerically that the final lower bound on $C(S)$ we obtained appears to be related to k^* via

$$C(S) \ge \log(2) - h_2\left(\frac{1}{2} - \frac{\sqrt{k^*}}{4}\right). \tag{61}$$

However, our heuristic computations of the bound $C^*_{\mathbb{C}^{4\times 4}}(S)$ indicate that it is in fact nonconvex over a large range of values of S, and hence the true $C(S)$ bound (for systems of arbitrary dimension) cannot be saturated simply by qubit-qubit systems, but rather only by "block-diagonal combinations" of such systems. In particular, this means that the states described above cannot saturate either the $C(S)$ bound or our final lower bound on it (for all S), though it may be possible to do so using "block-diagonal combinations" of them.

II. SUPPLEMENTARY NOTE 2 - SIMULATION WITH ALL-PHOTONIC SETUP

In this section, we present the simulated asymptotic key rate that one could achieve in an all-photonic experiment. For all-photonic implementations the noise model presented in Ref. [20] gives a more realistic description than the white noise considered in the main text. In this model, the source is modelled by a pair of two-mode squeeze vacua (TMSV) over polarisation modes with mean photon number λ_1 and λ_2. Alice and Bob will then set the measurement angles to be θ_{A_X} and θ_{B_Y} where $X \in \{0,1\}$ and $Y \in \{0,1,2,3\}$ are their corresponding inputs. Both Alice and Bob will have a pair of single-photon detectors, each with some imperfect quantum efficiency. We let the effective detection efficiency (the total transmittivity between the source and each detector) be η. Furthermore, we assume that Alice and Bob will give deterministic outputs whenever they observe no detection events. Finally, we also assume that the detectors have negligible dark count rates.

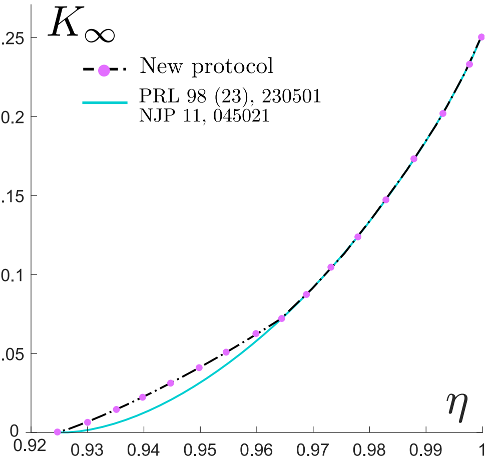

Fig. 6. **Asymptotic key rate for all-photonic experiments.** For this simulation, we use the model presented in Ref. [20] and set the dark count rate of the detectors to zero. We also assumed that Alice and Bob assign deterministic outputs whenever their detectors do not click. We plot the lower bound on the key rate as a function of detection efficiency η. From the plot, we can see that randomised key basis can improve the achievable key rate in the lower detection efficiency regime.

The corresponding key rate is presented in Fig. 6. To obtain these curves, we optimise the achievable key rates by varying the mean photon number of the TMSV λ_1 and λ_2 as well as the measurement angles of Alice and Bob θ_{A_X} θ_{B_Y} for each value of η. Unfortunately, the improvement from employing the randomised key basis protocol is rather limited for the all-photonic experiments. Remarkably, the required detection efficiency to achieve non-zero key rate remains extremely demanding.

III. SUPPLEMENTARY NOTE 3 - ADDITIONAL LEMMAS AND THEOREMS

Theorem 1 DI-Binary Pinsker++: (The following Thm. is a special case of Thm.1 in [10]) Let Q be a (not necessarily rank one) projector on a finite dimensional Hilbert space of dimension d and let T be the pinching channel constructed from Q via

$$T[\rho] = Q\rho Q + (\mathbf{1} - Q)\rho(\mathbf{1} - Q) = \rho + 2Q\rho Q - \{Q, \rho\}. \tag{62}$$

For any state ρ, the following inequality holds:

$$D(\rho \| T[\rho]) \geq \log(2) - h_2\left(\frac{1 - \|\rho - T[\rho]\|_1}{2}\right). \tag{63}$$

For the proof of Thm. 1, we will require the following Lemmas:

Lemma 1 Gibbs variational principle for operators: Let L be a self-adjoint operator. For any quantum state ρ, the following holds:

$$-\operatorname{tr}(\rho L) \geq H(\rho) - \log \operatorname{tr}\left(e^L\right). \tag{64}$$

Proof. Consider the thermal state $\sigma = \frac{e^L}{\operatorname{tr}(e^L)}$.

$$\begin{aligned} -\operatorname{tr}(\rho L) &= -\operatorname{tr}\left(\rho \log e^L\right) & (65)\\ &= -\operatorname{tr}\left(\rho\left(\log \frac{e^L}{\operatorname{tr}\left(e^L\right)} + \log \operatorname{tr}\left(e^L\right)\right)\right) & (66)\\ &= -\operatorname{tr}\left(\rho \log \frac{e^L}{\operatorname{tr}\left(e^L\right)}\right) - \operatorname{tr}\left(\rho \log \operatorname{tr}\left(e^L\right)\right) & (67)\\ &= -\operatorname{tr}\left(\rho \log \sigma\right) - \log \operatorname{tr}\left(e^L\right) & (68)\\ &\geq -\operatorname{tr}\left(\rho \log \rho\right) - \log \operatorname{tr}\left(e^L\right) & (69)\\ &= H(\rho) - \log \operatorname{tr}\left(e^L\right), & (70) \end{aligned}$$

where we have used the positivity of the quantum relative entropy $D(\rho||\sigma) = \operatorname{tr}(\rho \log \rho - \rho \log \sigma)$. □

Lemma 2 : For a quantum state χ and an operator A with spectral radius $r_{\text{spec}}(A) \leq s$, the following relation holds:

$$\operatorname{tr}\left(\chi e^A\right) \leq \cosh(s) + \frac{1}{s}\sinh(s)\operatorname{tr}(\chi A). \tag{71}$$

Proof. Firstly, we will find an upper bound to the exponential function in a fixed interval $[-s, s]$. The simplest ansatz is to upper bound it with a linear function, which can be parameterise with α and β such that $e^x \leq \alpha + \beta x$. Such an upper bound can be determined by demanding that the points of the exponential function at the boundaries of the interval intersects with the linear function, i.e.

$$\alpha \pm \beta s = e^{\pm s}, \tag{72}$$

which yields $\alpha = \cosh(s)$, $\beta = \frac{1}{s}\sinh(s)$. Hence, we obtain

$$\begin{aligned} \operatorname{tr}\left(\chi e^A\right) &\leq \operatorname{tr}\left(\chi\left[\cosh(s) + \frac{1}{s}\sinh(s)A\right]\right) & (73)\\ &= \cosh(s) + \frac{1}{s}\sinh(s)\operatorname{tr}\left(\chi A\right). & (74) \end{aligned}$$

□

Lemma 3 : For any projector Q and quantum state ρ, we have

$$\|\rho - T[\rho]\|_1 \leq 1 \tag{75}$$

Proof. We use equation (46) and projectors P and $M = 2P - \mathbf{1}$ to rewrite

$$\begin{aligned}\sup_{\rho Q} \|\rho - T[\rho]\|_1 &= 2 \sup_{\rho\, P\, Q} \operatorname{tr}\left(P(\rho - T[\rho])\right)\\ &= 2 \sup_{\rho\, P\, Q} \langle \{P, Q\} - 2QPQ\rangle_\rho\\ &= 2 \sup_{P\, Q} \|\{P, Q\} - 2QPQ\|_\infty \end{aligned} \tag{76}$$

Using the usual block decomposition of the algebra generated by two projectors (P and Q) we can conclude that the optimal solution of the above will be attained on 2×2 matrices. We can assume without loss of generality that

$$P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } Q = \begin{pmatrix} \cos(\phi)^2 & \cos(\phi)\sin(\phi) \\ \cos(\phi)\sin(\phi) & \sin(\phi)^2 \end{pmatrix}. \tag{77}$$

Thus, we have

$$\begin{aligned}&\sup_\phi \left\| \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \cos(\phi)^2 & \cos(\phi)\sin(\phi) \\ \cos(\phi)\sin(\phi) & \sin(\phi)^2 \end{pmatrix} \right\} \right.\\ &\qquad \left. - 2 \begin{pmatrix} \cos(\phi)^2 & \cos(\phi)\sin(\phi) \\ \cos(\phi)\sin(\phi) & \sin(\phi)^2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \cos(\phi)^2 & \cos(\phi)\sin(\phi) \\ \cos(\phi)\sin(\phi) & \sin(\phi)^2 \end{pmatrix} \right\|_\infty\\ &= \frac{1}{2}. \end{aligned} \tag{78}$$

□

Proof of Pinsker++. The basic idea of this proof is to find a lower bound on $D(\rho\|T[\rho])$ in terms of $\|\rho - T[\rho]\|_1$ by bounding the expression

$$\inf_\rho D(\rho\|T[\rho]) - \lambda\|\rho - T[\rho]\|_1 \geq c_\lambda \tag{79}$$

from below by some c_λ that only depends on a variational parameter $\lambda \in \mathbb{R}^+$ but not on ρ. Given such a c_λ for all λ will then allow us to obtain a bound on D via an inverse Legendre transformation

$$\forall\rho: \quad D(\rho\|T[\rho]) \geq \sup_{\lambda\in\mathbb{R}^+} c_\lambda + \lambda\|\rho - T[\rho]\|_1 := f(\|\rho - T[\rho]\|_1) \tag{80}$$

Rewriting (79) with equation (46), $M = 2P - \mathbf{1}$ and Lem. 1 for $L = \log(T[\rho]) + 2\lambda(P - T[P])$ yields the following inequality:

$$\begin{aligned} &D(\rho\|T[\rho]) - \lambda\|\rho - T[\rho]\|_1\\ &\geq \inf_\rho \inf_{0\leq P\leq \mathbb{I}} - \operatorname{tr}\left(\rho(\log(T[\rho]) \; + 2\lambda(P - T[P]))\right) - H(\rho)\\ &\geq \inf_\rho \inf_{0\leq P\leq \mathbb{I}} - \log\operatorname{tr}\left(e^{\log(T[\rho]) + 2\lambda(P - T[P])}\right)\\ &\geq -\log\sup_\rho \sup_{0\leq P\leq \mathbb{I}} \operatorname{tr}\left(e^{\log(T[\rho]) + 2\lambda(P - T[P])}\right)\\ &\geq -\log\sup_\rho \sup_{0\leq P\leq \mathbb{I}} \operatorname{tr}\left(e^{\log(T[\rho])} e^{2\lambda(P - T[P])}\right)\\ &= -\log\sup_\rho \sup_{0\leq P\leq \mathbb{I}} \operatorname{tr}\left(T[\rho] \;\; e^{2\lambda(P - T[P])}\right), \end{aligned} \tag{81}$$

where we have applied the Golden-Thompson inequality $\operatorname{tr}(e^{A+B}) \leq \operatorname{tr}(e^A e^B)$. Next, we use Lem. 2 with $\chi = T[\rho]$, $A = 2\lambda(P - T[P])$, which implies $s = \lambda$ (see Lem. 3). This yields

$$\begin{aligned} \text{Eq. (81)} &\geq -\log\left(\cosh(s) + \sup_\rho \sup_{0\leq P\leq \mathbb{I}} \frac{2\lambda}{s} \sinh(s)\operatorname{tr}\left(T[\rho]\,(P - T[P])\right)\right)\\ &= -\log\left(\cosh(\lambda)\right) \end{aligned} \tag{82}$$

Hence, we know that

$$D\left(\rho||T\left[\rho\right]\right) \geq -\log\left(\cosh(\lambda)\right) + \lambda\|\rho - T[\rho]\|_1. \tag{83}$$

Since this is true for all $\lambda \geq 0$, the optimal bound can be found by maximizing the right hand side over $\lambda \geq 0$, which gives

$$\lambda_{\max} = \operatorname{arccoth}\left(\frac{1}{\|\rho - T[\rho]\|_1}\right). \tag{84}$$

Inserting it back into (83), where we use the notation $x = \|\rho - T[\rho]\|_1$, yields

$$\begin{aligned}
D\left(\rho||T\left[\rho\right]\right) &\geq -\log\left(\cosh\left(\operatorname{arccoth}\left(\frac{1}{x}\right)\right)\right) + x\ \operatorname{arccoth}\left(\frac{1}{x}\right) &(85)\\
&= \frac{1}{2}\left(\log\left(1-x^2\right) + x\log\left(\frac{1+x}{1-x}\right)\right) &(86)\\
&= \frac{1}{2}\left(\log(1+x) + \log(1-x) + x\log(1+x) - x\log(1-x)\right) &(87)\\
&= \frac{1+x}{2}\log(1+x) + \frac{1-x}{2}\log(1-x) &(88)\\
&= \log(2) + \frac{1+x}{2}\log\left(\frac{1+x}{2}\right) + \frac{1-x}{2}\log\left(\frac{1-x}{2}\right) &(89)\\
&= \log(2) - h_2\left(\frac{1-x}{2}\right), &(90)
\end{aligned}$$

which concludes the proof. □

IV. SUPPLEMENTARY NOTE 4 - FINITE-SIZE ANALYSIS

In this section, we give a condensed summary of the finite-size security proof based on the entropy accumulation theorem [21, 22], with the details in an extended writeup [23]. As compared to previous results, the technical contributions from this analysis are as follows. Firstly, it uses tighter finite-size bounds in several points as compared to [24, 25]. Additionally, we perform a different analysis regarding the effects of conditioning on success in the various protocol steps, in order to accommodate practical error-correction protocols that may not have the appropriate form of correctness guarantee required for the analysis in [24]. Furthermore, to apply the entropy accumulation theorem it is necessary to define the protocol steps in such a way that the theorem can be applied to the channels in the protocol — in particular, this requires finding appropriate choices for how to perform the sifting and parameter estimation steps (see below).

A. Security definitions

Before beginning the proof, we first need to formalize the security definitions that we aim to achieve. Following [24], we choose the definitions stated below:

Definition 1. Consider a DIQKD protocol such that at the end, the honest parties either *accept* (producing keys K_A and K_B of length ℓ_{key} for Alice and Bob respectively) or *abort* (producing an abort symbol $\perp$ for all parties). It is said to be ϵ^{com}-complete and ϵ^{sou}-sound if the following properties hold:

- (Completeness) The honest protocol implementation aborts with probability at most ϵ^{com}.
- (Soundness) For any implementation of the protocol, we have

$$\Pr[\text{accept}]\,\frac{1}{2}\left\|\sigma_{K_A K_B E'} - \left(\frac{1}{2^{\ell_{\text{key}}}}\sum_k |kk\rangle\langle kk|_{K_A K_B}\right)\otimes\sigma_{E'}\right\|_1 \leq \epsilon^{\text{sou}}, \tag{91}$$

  where σ denotes the normalized state conditioned on the protocol accepting, and E' denotes all side-information registers available to the adversary at the end of the protocol.

In the security proof, it is convenient to use the fact that the soundness property is implied by a pair of slightly simpler conditions, as shown in [26]. Specifically, to prove a DIQKD protocol is ϵ^{sou}-sound, it suffices to find $\epsilon^{\text{cor}}_{\text{QKD}}, \epsilon^{\text{sec}}_{\text{QKD}}$ such that $\epsilon^{\text{sou}} \geq \epsilon^{\text{cor}}_{\text{QKD}} + \epsilon^{\text{sec}}_{\text{QKD}}$ and the protocol is both $\epsilon^{\text{cor}}_{\text{QKD}}$-correct and $\epsilon^{\text{sec}}_{\text{QKD}}$-secret, defined as follows:

Definition 2. A DIQKD protocol as described above is said to be $\epsilon^{\text{cor}}_{\text{QKD}}$-correct and $\epsilon^{\text{sec}}_{\text{QKD}}$-secret if the following properties hold:

- (Correctness) For any implementation of the protocol, we have

$$\Pr[K_A \neq K_B \wedge \text{accept}] \leq \epsilon^{\text{cor}}_{\text{QKD}}. \tag{92}$$

- (Secrecy) For any implementation of the protocol, we have

$$\Pr[\text{accept}]\,\frac{1}{2}\left\|\sigma_{K_A E'} - \mathbb{U}_{K_A}\otimes\sigma_{E'}\right\|_1 \leq \epsilon^{\text{sec}}_{\text{QKD}}, \tag{93}$$

  where σ is as described in Definition 1, and $\mathbb{U}_{K_A}$ denotes the maximally mixed state (i.e. a uniformly random key for Alice).

The parameters in these security definitions are not merely abstract values, but rather they have important operational interpretations. The completeness parameter ϵ^{com} is straightforward — it is simply the probability that the honest devices abort. As for the soundness parameter ϵ^{sou}, an important consequence of the definition is regarding the notion of *composability*, as follows [26][2]: suppose one designs a larger protocol (for instance, the one-time-pad protocol) which makes use of an ideal resource that generates a perfectly secret key whenever it does not abort. Furthermore, suppose one proves that when that larger protocol is indeed using the ideal secret-key resource, the probability of some "failure" event

[2] Strictly speaking, this interpretation was obtained for the standard QKD setting rather than the DIQKD setting — there are technical issues in formalizing composable security for the latter, because of device-reuse attacks. However, these issues only affect the operational *interpretation* of Definition 1; there are no issues in proving that the protocol satisfies this definition by itself.

(no restrictions need to be imposed on what constitutes a failure, except that it be a well-defined event) is upper-bounded by some value p_{fail}. In that case, it can be shown [26] that if one replaces the ideal secret-key resource with a protocol that is ϵ^{sou}-sound as defined above, then the probability of the failure event is still upper-bounded by $p_{\text{fail}} + \epsilon^{\text{sou}}$. In other words, the soundness definition allows us to use an ϵ^{sou}-sound protocol in place of the ideal secret-key resource in a larger protocol, with only an increase of at most ϵ^{sou} to the maximum probability of *any* failure event. Further details on this topic can be found in [26].

B. Security proof sketch

Let n be the total number of rounds in the protocol. Let $\mathbf{A}$ and $\mathbf{B}$ denote the output strings that Alice and Bob respectively obtain from the protocol; similarly, let $\mathbf{X}$ and $\mathbf{Y}$ denote their input strings. Let $\mathbf{L}$ denote the syndrome that Alice sends to Bob, and let E denote all the other (quantum) side-information that Eve collects over the course of the protocol (note that it may not have a tensor-product structure since we consider general attacks).

First, we need to describe the error-correction step in a bit more detail. We focus on the case where this step takes the following form: the string $\mathbf{L}$ consists of two substrings $\mathbf{L}_{\text{EC}}, \mathbf{L}_{\text{h}}$, such that $\mathbf{L}_{\text{EC}}$ is what Bob uses to produce a guess $\tilde{\mathbf{A}}$ for $\mathbf{A}$, and $\mathbf{L}_{\text{h}}$ is a 2-universal hash of $\mathbf{A}$ which Bob uses to check whether his guess is correct (if the hash of his guess $\tilde{\mathbf{A}}$ does not match $\mathbf{L}_{\text{h}}$, Bob announces an abort of the protocol). Furthermore, we shall suppose that before the protocol begins, a constant $\text{EC}_{\max}$ is chosen such that the length of $\mathbf{L}_{\text{EC}}$ is at most $\text{EC}_{\max}$ (we allow the option of using an error-correction procedure that sends a shorter $\mathbf{L}_{\text{EC}}$ if the noise level encountered during execution of the protocol is lower than expected). By using an error-correction step of this form, we shall argue below that the completeness and correctness conditions can be satisfied if we choose suitable values for $\text{EC}_{\max}$ and the length of $\mathbf{L}_{\text{h}}$.

Also, for the parameter-estimation analysis, instead of using the CHSH value in terms of correlators, it is easier to consider the winning probability of the *CHSH game*. Specifically, view Alice and Bob's outputs as taking values in $\{0, 1\}$ rather than $\{+1, -1\}$, and for outputs $a, b \in \{0, 1\}$ from inputs $x \in \{0, 1\}$, $y \in \{2, 3\}$ (in a test round), we say that Alice and Bob win the CHSH game if $a \oplus b = x \cdot (y - 2)$. The probability w of winning the CHSH game (given uniformly random inputs) is related to the correlator-based CHSH value S by the simple conversion $S = 8w - 4$. We shall suppose that the honest devices are IID and achieve some CHSH winning probability w_{exp} in each individual round.

For simplicity, we shall focus on the case where the protocol is performed with $p = 1/2$, since our results indicate that this is optimal at higher noise levels. In that case, the inputs in the test rounds are uniformly random, so Alice and Bob can indeed be considered to be playing the CHSH game in those rounds. Given this, it is easier to instead consider a slightly different version of the parameter-estimation step, which differs somewhat from more commonly studied QKD protocols, but facilitates a technical application of the entropy accumulation theorem to prove security against general attacks [23]. Specifically, parameter estimation is performed as follows: introducing a tolerance value δ_{tol}, Bob will check that the number of test rounds that won the CHSH game is at least $(w_{\text{exp}} - \delta_{\text{tol}})qn$, and also that the number of test rounds that lost the CHSH game is at most $(1 - w_{\text{exp}} + \delta_{\text{tol}})qn$. (Performing both of these checks allows for a technical optimization in the finite-size security analysis; see [23]. Also, note that we do not "normalize" by dividing by the number of test rounds that actually occurred — the qn factor is computed directly from the protocol parameters. Our results indicate [23] that this form of parameter estimation incurs certain losses compared to the more standard form, but it remains an open question whether the latter can be formalised in a manner compatible with the entropy accumulation theorem.) If either of these conditions is not satisfied, Bob aborts the protocol at that step.

In the previous sections, we have derived a lower bound on $\lambda H(A_0|E) + (1 - \lambda)H(A_1|E)$ as a function of the CHSH value S (for the choice $p = 1/2$ we have $\lambda = 1 - \lambda = 1/2$). Now, let $r(w)$ denote such a lower bound, but in terms of the CHSH winning probability w instead, and with the additional condition that it be an affine function (this could be obtained in principle as part of the Legendre-transform process we described in Sec. I G, though in practice we found it more efficient to use the approach described in [23]). With this in mind, we now define a function

$$g(w) = \frac{1 + q}{2} r(w), \tag{94}$$

which can be informally interpreted as a lower bound on the entropy "accumulated" in one round of the protocol. (The prefactor is to account for the fact that Alice and Bob sift out generation rounds which they have chosen different inputs[3]. To maintain compatibility with entropy accumulation, we interpret the sifting step as Alice and Bob setting their outcomes to some deterministic values whenever their inputs differ, rather than truly "discarding" those rounds.)

With this in mind, we can state the security guarantees of the protocol [23]:

[3] To optimize the keyrates, we include the test rounds in the contribution to the entropy; see [23].

Theorem 2 : Take any $\epsilon_{\mathrm{EC}}^{\mathrm{com}}, \epsilon_{\mathrm{PE}}^{\mathrm{com}}, \epsilon_{\mathrm{EA}}, \epsilon_{\mathrm{PA}}, \epsilon_{\mathrm{h}}, \epsilon_s, \epsilon_s', \epsilon_s'' \in (0,1]$ such that $\epsilon_s > \epsilon_s' + 2\epsilon_s''$, and any $\alpha \in (1,2)$, $\alpha' \in (1, 1+2/V')$, $\beta \in [g(0), g(1)]$, $q \in (0,1)$, where $V' = 2\log 7$. For $p = 1/2$, the described protocol is $(\epsilon_{\mathrm{EC}}^{\mathrm{com}} + \epsilon_{\mathrm{PE}}^{\mathrm{com}})$-complete and $(\max\{\epsilon_{\mathrm{EA}}, \epsilon_{\mathrm{PA}} + 2\epsilon_s\} + 2\epsilon_{\mathrm{h}})$-sound when performed with $\mathrm{EC}_{\max}$ satisfying Eq. (99), and $\delta_{\mathrm{tol}}, \ell_{\mathrm{key}}$ satisfying

$$\epsilon_{\mathrm{PE}}^{\mathrm{com}} \geq B_{n,qw_{\exp}}(\lfloor(w_{\exp} - \delta_{\mathrm{tol}})qn\rfloor) + B_{n,1-q+qw_{\exp}}(\lfloor(1-q+w_{\exp}q - \delta_{\mathrm{tol}}q)n\rfloor), \tag{95}$$

$$\begin{aligned}\ell_{\mathrm{key}} \leq ng(w_{\exp} - \delta_{\mathrm{tol}}) - n\frac{(\alpha-1)\ln 2}{2}V^2 - n(\alpha-1)^2K_\alpha^2 - nq - n\left(\frac{\alpha'-1}{4}\right)V'^2 \\ - \frac{\vartheta_{\epsilon_s'}}{\alpha-1} - \frac{\vartheta_{\epsilon_s''}}{\alpha'-1} - \left(\frac{\alpha}{\alpha-1} + \frac{\alpha'}{\alpha'-1} - 2\right)\log\frac{1}{\epsilon_{\mathrm{EA}}} - 3\vartheta_{\epsilon_s - \epsilon_s' - 2\epsilon_s''} \\ - \mathrm{EC}_{\max} - \left\lceil \log\left(\frac{1}{\epsilon_{\mathrm{h}}}\right)\right\rceil - 2\log\frac{1}{\epsilon_{\mathrm{PA}}} + 2,\end{aligned} \tag{96}$$

where V and K_α are constants (depending on q, g, β and α) that can be explicitly computed [22, 23], ϑ_ϵ is defined as

$$\vartheta_\epsilon = \log\frac{1}{1-\sqrt{1-\epsilon^2}}, \tag{97}$$

and $B_{n,p}(k)$ denotes the cumulative distribution function of a binomial distribution with parameters (n, p):

$$B_{n,p}(k) = \Pr_{X\sim\mathrm{Binom}(n,p)}[X \leq k]. \tag{98}$$

The variables listed at the start of Theorem 2 can be considered to be variational parameters that should be chosen to optimize the keyrate as much as possible. To get a sense of the asymptotic scaling, it can be shown [21–23] that as $n \to \infty$, we can choose these parameters in such a manner that $\delta_{\mathrm{tol}}, q \to 0$ and the key-length expression (96) is dominated by the terms $ng(w_{\exp} - \delta_{\mathrm{tol}})$ and $\mathrm{EC}_{\max}$. By taking Eq. (99) for the latter, this yields an asymptotic keyrate of essentially[4] $(1/2)\left(\sum_x H(A_x|E) - \sum_x H(A_x|B_x)\right)$ as expected.

We now sketch the proof of the above theorem, by considering those variational parameters to take some fixed values, and then showing that indeed the desired security claims (as functions of these values) hold.

Completeness: To show that this condition holds, we impose the requirement that $\mathrm{EC}_{\max}$ is long enough such that for the honest devices, Bob can use $\mathbf{L}_{\mathrm{EC}}$ and $\mathbf{B}$ to produce a guess for $\mathbf{A}$ that is correct with probability at least $1 - \epsilon_{\mathrm{EC}}^{\mathrm{com}}$. From the results of [21, 27], this is possible as long as $\mathrm{EC}_{\max}$ is chosen such that[5]

$$\mathrm{EC}_{\max} \geq nh_{\mathrm{hon}} + \sqrt{n}\,(2\log 5)\sqrt{\log\frac{2}{\tilde{\epsilon}_s^2}} + 2\log\frac{1}{\epsilon_{\mathrm{EC}}^{\mathrm{com}} - \tilde{\epsilon}_s} + 4, \tag{99}$$

where $\tilde{\epsilon}_s \in [0, \epsilon_{\mathrm{EC}}^{\mathrm{com}})$ is another parameter that can be optimized over, and

$$h_{\mathrm{hon}} = \frac{1-q}{4}\left(H(A_0|B_0)_{\mathrm{hon}} + H(A_1|B_1)_{\mathrm{hon}}\right) + qh_2(w_{\exp}), \tag{100}$$

where the subscript $_{\mathrm{hon}}$ denotes that the terms should be computed with respect to the honest behaviour, and for simplicity we have assumed that the honest devices win the CHSH game with the same probability $w_{\exp}$ for all input pairs. Having imposed this requirement (that Bob's guess is correct with probability at least $1 - \epsilon_{\mathrm{EC}}^{\mathrm{com}}$) on the honest protocol, we see that the probability that it aborts during the error-correction step (because the hashes of $\tilde{\mathbf{A}}$ and $\mathbf{A}$ do not match) is at most $\epsilon_{\mathrm{EC}}^{\mathrm{com}}$. Furthermore, since the honest devices win the CHSH game with probability $w_{\exp}$, and the parameter-estimation step accepts when the number of test rounds that won (resp. lost) the CHSH game is at least $(w_{\exp} - \delta_{\mathrm{tol}})qn$ (resp. at most $(1 - w_{\exp} + \delta_{\mathrm{tol}})qn$), it is not hard to show that the probability that the honest protocol aborts during the parameter-estimation step is at most $\epsilon_{\mathrm{PE}}^{\mathrm{com}}$ as defined in Eq. (95) (because in the honest protocol, the number of test rounds that win/lose the CHSH game follows a binomial distribution). Applying the union bound to these different ways the protocol could abort, we see the protocol is $(\epsilon_{\mathrm{EC}}^{\mathrm{com}} + \epsilon_{\mathrm{PE}}^{\mathrm{com}})$-complete as claimed.

[4] Technically, $H(A_x|E)$ and $H(A_x|B_x)$ refer to single-round quantities and are hence only well-defined when the rounds are IID, i.e. the values of these quantities are the same in all rounds. However, the asymptotic rate we have described for Theorem 2 is essentially analogous in the sense that $(1/2)\sum_x H(A_x|E)$ is replaced by a lower bound $g(w_{\exp} - \delta_{\mathrm{tol}})$ that, informally speaking, holds for all rounds. (As for the $H(A_x|B_x)$ terms, they are computed with respect to the honest behaviour, which is indeed IID.)

[5] Other error-correction procedures are possible in principle; see [23] for further discussion.

Soundness: To prove the claim of $(\max\{\epsilon_{\mathrm{EA}}, \epsilon_{\mathrm{PA}} + 2\epsilon_s\} + 2\epsilon_{\mathrm{h}})$-soundness, we argue the protocol is ϵ_{h}-correct and $(\max\{\epsilon_{\mathrm{EA}}, \epsilon_{\mathrm{PA}} + 2\epsilon_s\} + \epsilon_{\mathrm{h}})$-secret, as follows:

Correctness: To satisfy this condition, we shall set the length of $\mathbf{L}_{\mathrm{h}}$ to be $\lceil \log(1/\epsilon_{\mathrm{h}}) \rceil$. By the defining property of 2-universal hashing, for a hash of this length, the probability that two different strings hash to the same value is at most ϵ_{h}. Since K_A and K_B are produced from $\mathbf{A}$ and $\tilde{\mathbf{A}}$ respectively, a straightforward calculation shows that this implies $\Pr[K_A \neq K_B \wedge \text{accept}] \leq \epsilon_{\mathrm{h}}$ as well, and hence we have that the protocol is ϵ_{h}-correct.

Secrecy: The main challenge is in proving this condition holds. To slightly improve the keyrates, in proving Theorem 2 we impose (see [23, 24]) that Alice's test-round outputs are not sent in plaintext to Bob, but rather they are compressed into an error-correction syndrome as well. In that case, strictly speaking Bob is performing parameter estimation using his guess $\tilde{\mathbf{A}}$ rather than $\mathbf{A}$ itself, but it can be shown [23] that roughly speaking, the fact that we have ϵ_{h}-correctness as shown above implies that we can perform the analysis conditioned on $\tilde{\mathbf{A}} = \mathbf{A}$, at the cost of increasing the secrecy parameter by ϵ_{h}. We will not further discuss this point here, except to remember to add ϵ_{h} to the secrecy parameter at the end.

At the end of the protocol Eve holds the registers $\mathbf{XYL}E$, and the final privacy amplification step in the protocol was performed by Alice on the register $\mathbf{A}$ (and by Bob on $\tilde{\mathbf{A}}$). The fundamental property of privacy amplification is basically that it produces a final key satisfying the secrecy definition, with length related to the smoothed min-entropy of $\mathbf{A}$ conditioned on $\mathbf{XYL}E$. More specifically [23, 28], as long as we set the length of the privacy-amplification output (i.e. the final key) to satisfy

$$\ell_{\mathrm{key}} \leq H^{\epsilon_s}_{\min}(\mathbf{A}|\mathbf{XYL}E) + 2 - 2\log\frac{1}{\epsilon_{\mathrm{PA}}}, \tag{101}$$

we will get an $(\epsilon_{\mathrm{PA}} + 2\epsilon_s)$-secret key (putting aside several technicalities about conditioning on the various steps accepting). Hence to find a bound on the final achievable key length, it suffices to give a lower bound on $H^{\epsilon_s}_{\min}(\mathbf{A}|\mathbf{XYL}E)$. To do so, we first apply a chain rule [29] to get

$$\begin{aligned} H^{\epsilon_s}_{\min}(\mathbf{A}|\mathbf{XYL}E) &\geq H^{\epsilon_s}_{\min}(\mathbf{A}|\mathbf{XY}E) - \mathrm{len}(\mathbf{L}) \\ &\geq H^{\epsilon_s}_{\min}(\mathbf{A}|\mathbf{XY}E) - \mathrm{EC}_{\max} - \left\lceil \log\left(\frac{1}{\epsilon_{\mathrm{h}}}\right) \right\rceil, \end{aligned} \tag{102}$$

reducing our task to bounding $H^{\epsilon_s}_{\min}(\mathbf{A}|\mathbf{XY}E)$. This is achieved by using the entropy accumulation theorem, which yields a lower bound on the smoothed min-entropy of a state produced by a sequence of channels (which in this case we basically take to correspond to the rounds of the protocol). Specifically, the entropy accumulation theorem can be used to show that one of the following must be true: (1) the probability of the parameter-estimation step accepting is at most ϵ_{EA}, or (2) conditioned on accepting, we have the lower bound

$$\begin{aligned} H^{\epsilon_s}_{\min}(\mathbf{A}|\mathbf{XY}E) > ng(w_{\exp} - \delta_{\mathrm{tol}}) - n\frac{(\alpha-1)\ln 2}{2}V^2 - n(\alpha-1)^2 K_\alpha^2 - nq - n\left(\frac{\alpha'-1}{4}\right)V'^2 \\ - \frac{\vartheta_{\epsilon_s'}}{\alpha-1} - \frac{\vartheta_{\epsilon_s''}}{\alpha'-1} - \left(\frac{\alpha}{\alpha-1} + \frac{\alpha'}{\alpha'-1}\right)\log\frac{1}{\epsilon_{\mathrm{EA}}} - 3\vartheta_{\epsilon_s - \epsilon_s' - 2\epsilon_s''}. \end{aligned} \tag{103}$$

In case (1), the secrecy condition immediately holds with secrecy parameter ϵ_{EA}. In case (2), the sequence of equations (101)–(103) tells us that we can get an $(\epsilon_{\mathrm{PA}} + 2\epsilon_s)$-secret key with length given by (96)[6]. Recalling to add the ϵ_{h} correction because parameter estimation is performed with $\tilde{\mathbf{A}}$ rather than $\mathbf{A}$, we conclude the protocol is $(\max\{\epsilon_{\mathrm{EA}}, \epsilon_{\mathrm{PA}} + 2\epsilon_s\} + \epsilon_{\mathrm{h}})$-secret.

In the above, we have described the key rates for general attacks. If we make the assumption of collective attacks, then the completeness and correctness proofs proceed in exactly the same way — only the secrecy proof needs to be modified. The main modification (ignoring some technical details) is that the bound (103) is replaced with one based on the *asymptotic equipartition property* (we use the version presented in [21]), which holds for IID states. The resulting rates are higher than those resulting from (103), since the asymptotic equipartition property exploits the assumption of

[6] To be precise, the expression (96) has a slightly improved dependence on ϵ_{EA} by keeping track of the event conditioning in a more precise statement of privacy amplification (Eq. (101)), but we defer the details to [23].

an IID structure for the states.

[1] Tan, E. Y.-Z., Schwonnek, R., Goh, K. T., Primaatmaja, I. W. & Lim, C. C.-W. Computing secure key rates for quantum key distribution with untrusted devices. *arXiv preprint arXiv:1908.11372v1* (2019).

[2] Coles, P. J. Unification of different views of decoherence and discord. *Physical Review A* **85**, 042103 (2012).

[3] Coles, P. J., Metodiev, E. M. & Lütkenhaus, N. Numerical approach for unstructured quantum key distribution. *Nature Communications* **7**, 11712 (2016).

[4] Pironio, S. *et al.* Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics* **11**, 045021 (2009).

[5] Araki, H. & Lieb, E. H. Entropy inequalities. *Communications in Mathematical Physics* **18**, 160–170 (1970).

[6] Jordan, C. Essai sur la géométrie à n dimensions. *Bulletin de la Société mathématique de France* **3**, 103–174 (1875).

[7] Halmos, P. R. Two subspaces. *Transactions of the American Mathematical Society* **144**, 381–389 (1969).

[8] Masanes, L. Asymptotic violation of bell inequalities and distillability. *Physical Review Letters* **97**, 050503 (2006).

[9] Böttcher, A. & Spitkovsky, I. A gentle guide to the basics of two projections theory. *Linear Algebra and its Applications* **432**, 1412 – 1459 (2010).

[10] Schwonnek, R. & Wolf, R. Pinsker's inequality for a quantum channel. In preparation.

[11] Boyd, S. & Vandenberghe, L. *Convex Optimization* (Cambridge University Press, 2004).

[12] Schwonnek, R., Dammeier, L. & Werner, R. F. State-independent uncertainty relations and entanglement detection in noisy systems. *Physical Review Letters* **119**, 170404 (2017).

[13] Zhao, Y.-Y. *et al.* Entanglement detection by violations of noisy uncertainty relations: A proof of principle. *Physical Review Letters* **122**, 220401 (2019).

[14] Tan, E. Y.-Z., Lim, C. C.-W. & Renner, R. Advantage Distillation for Device-Independent Quantum Key Distribution. *Physical Review Letters* **124**, 020502 (2020).

[15] Roga, W., Fannes, M. & Życzkowski, K. Universal Bounds for the Holevo Quantity, Coherent Information, and the Jensen-Shannon Divergence. *Physical Review Letters* **105**, 040505 (2010).

[16] Bancal, J.-D., Sheridan, L. & Scarani, V. More randomness from the same data. *New Journal of Physics* **16**, 033011 (2014).

[17] Nieto-Silleras, O., Pironio, S. & Silman, J. Using complete measurement statistics for optimal device-independent randomness evaluation. *New Journal of Physics* **16**, 013035 (2014).

[18] Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics* **10**, 073013 (2008).

[19] Masanes, L., Pironio, S. & Acín, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications* **2**, 238 (2011).

[20] Tsujimoto, Y. *et al.* Optimal conditions for the Bell test using spontaneous parametric down-conversion sources. *Physical Review A* **98**, 063842 (2018).

[21] Dupuis, F., Fawzi, O. & Renner, R. Entropy accumulation. *arXiv preprint arXiv:1607.01796* (2016).

[22] Dupuis, F. & Fawzi, O. Entropy accumulation with improved second-order term. *IEEE T. Inform. Theory* 1–1 (2019).

[23] Tan, E. Y. Z. *et al.* Improved DIQKD protocols with finite-size analysis. *arXiv:2012.08714v1 [quant-ph]* (2020).

[24] Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R. & Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commun.* **9**, 459 (2018).

[25] Brown, P. J., Ragy, S. & Colbeck, R. An adaptive framework for quantum-secure device-independent randomness expansion. *arXiv preprint arXiv:1810.13346* (2018).

[26] Portmann, C. & Renner, R. Cryptographic security of quantum key distribution. *arXiv:1409.3525v1 [quant-ph]* (2014).

[27] Renes, J. M. & Renner, R. One-Shot Classical Data Compression With Quantum Side Information and the Distillation of Common Randomness or Secret Keys. *IEEE Transactions on Information Theory* **58**, 1985–1991 (2012).

[28] Tomamichel, M. & Leverrier, A. A largely self-contained and complete security proof for quantum key distribution. *Quantum* **1**, 14 (2017).

[29] Vitanov, A., Dupuis, F., Tomamichel, M. & Renner, R. Chain Rules for Smooth Min- and Max-Entropies. *IEEE Transactions on Information Theory* **59**, 2603–2612 (2013).