ARTICLE   OPEN

Check for updates

Fidelity bounds for device-independent advantage distillation

Thomas A. Hahn [ID][1][✉] and Ernest Y.-Z. Tan [ID][1][✉]

It is known that advantage distillation (that is, information reconciliation using two-way communication) improves noise tolerances for quantum key distribution (QKD) setups. Two-way communication is hence also of interest in the device-independent case, where noise tolerance bounds for one-way error correction are currently too low to be experimentally feasible. Existing security proofs for the device-independent repetition-code protocol (the most prominent form of advantage distillation) rely on fidelity-related security conditions, but previous bounds on the fidelity were not tight. We improve on those results by developing an algorithm that returns arbitrarily tight lower bounds on the fidelity. Our results give insight on how strong the fidelity-related security conditions are, and could also be used to compute some lower bounds on one-way protocol keyrates. Finally, we conjecture a necessary security condition for the protocol studied in this work, that naturally complements the existing sufficient conditions.

INTRODUCTION

The ultimate goal of key distribution protocols is to generate secure keys between two parties, Alice and Bob. To this end, device-independent quantum key distribution (DIQKD) schemes aim to provide information-theoretically secure keys by taking advantage of non-local correlations, which can be verified via Bell inequalities[1–4]. Critically, Bell violations rely only on the measurement statistics, $\Pr(ab|xy)$, where $a(b)$ is Alice's (Bob's) measurement outcome and $x(y)$ is Alice's (Bob's) measurement setting[5]. By basing security on Bell inequalities, DIQKD protocols do not require any knowledge of the bipartite state that Alice and Bob share, nor of the measurements both parties conduct, apart from the assumption that they act on separate Hilbert spaces[1,5]. (To guarantee security, it is still important to ensure that information about the device outputs themselves is not simply leaked to the adversary. Also, if the devices are reused, they must not access any registers retaining memory of 'private data', in order to avoid the memory attack of[6].) We consider all Hilbert spaces to be finite-dimensional.

Although DIQKD allows for the creation of secret keys under very weak assumptions, there is a trade-off when it comes to noise tolerances[1,7]. Standard DIQKD protocols which apply one-way error-correction steps have fairly low noise robustness, and are therefore not currently experimentally feasible[1,3]. To improve noise tolerances, one may implement techniques such as noisy pre-preprocessing[8], basing the protocol on asymmetric CHSH inequalities[9,10], or applying advantage distillation[11]. In this work we focus solely on advantage distillation, which refers to using two-way communication for information reconciliation, in place of one-way error-correction.

In device-dependent QKD[7,12–17], as well as classical key distillation scenarios[18,19], advantage distillation can perform better than standard one-way protocols in terms of noise tolerance. As for DIQKD, it has been shown that advantage distillation leads to an improvement of noise tolerance as well[11], but the results obtained in that work may not be optimal. Specifically, a sufficient condition was derived there for the security of advantage distillation against collective attacks, based on the fidelity between an appropriate pair of conditional states (see Theorem

1 below). However, the approach used in[11] to bound this fidelity is suboptimal, and hence the results were not tight.

Our main contribution in this work is to derive an algorithm based on semidefinite programs (SDPs) that yields arbitrarily tight lower bounds on the relevant fidelity quantity considered in[11]. We apply this algorithm to several DIQKD scenarios studied in that work, and compare the resulting bounds. Surprisingly, while we find improved noise tolerance for some scenarios, we do not have such improvements for the scenario that gave the best noise tolerances in[11], which relied on a more specialized security argument. An important consequence of this finding is that it serves as strong evidence that the general sufficient condition described in[11] is in fact not necessary in the DIQKD setting, in stark contrast to the device-dependent QKD protocols in[14,15], where it is both necessary and sufficient (when focusing on the repetition-code advantage distillation protocol; see below). In light of this fact, we describe an analogous condition that we conjecture to be necessary, and discuss possible directions for further progress.

We consider the following set-up for two parties, Alice and Bob[2,11].

- Measurement Settings: Alice (Bob) has M_A (M_B) possible measurement inputs and chooses $x \in \mathcal{X} = \{0, \dots, M_A - 1\}$ ($y \in \mathcal{Y} = \{0, \dots, M_B - 1\}$). The measurements are denoted as A_x (B_y) for Alice (Bob).
- Measurement Outcomes: Alice (Bob) has 2 possible measurement outcomes and measures $a \in \mathcal{A} = \{0, 1\}$ ($b \in \mathcal{B} = \{0, 1\}$).

The only key-generating measurements are A_0 and B_0. We consider Eve to be restricted to collective attacks[20], where it is assumed that the measurements Alice and Bob may conduct, as well as the single-round tripartite state, ρ_{ABE}, that Alice, Bob, and an adversary, Eve, share are independent and identical for each round. Since we are working in the device-independent setting, we consider Alice and Bob's measurements to be otherwise uncharacterized. For ease of applying the results from[11], we assume that they perform a symmetrization step, in which Alice and Bob publicly communicate a uniformly random bit and XOR it with their raw outputs (see[11] for details on when this step can be omitted). We use ϵ to denote the

quantum bit error rate (QBER), i.e. the probability of obtaining different outcomes from measurements A_0, B_0.

We consider the repetition-code protocol for advantage distillation[13–15,18,19], which proceeds as follows. After gathering the raw output strings from their devices, Alice and Bob split the key-generating rounds into blocks of size n each, and from each block they will attempt to generate a single highly-correlated bit. For each block, Alice generates a secret, uniformly random bit, C, and adds it to her n bits, $\mathbf{A}_0$. She then sends this 'encoded' bitstring, $\mathbf{M} = \mathbf{A}_0 \oplus (C, \dots, C)$, as a message to Bob via an authenticated channel. He then tries to decode the message by adding his own bitstring, $\mathbf{B}_0$, to it. He accepts the block of n bits if and only if $\mathbf{M} \oplus \mathbf{B}_0 = (C', \dots, C')$. If accepted, he indicates this to Alice by sending her a bit $D = 1$ via an authenticated channel. Otherwise, he sends $D = 0$. Considering only the accepted blocks, this process has therefore reduced each block of n bitpairs to a single highly correlated bitpair, (C, C'). Alice and Bob then apply a one-way error correction procedure (from Alice to Bob) on the resulting bitpairs over asymptotically many rounds, followed by privacy amplification to produce a final secret key. This procedure can achieve a positive asymptotic keyrate if the bitpairs in the accepted blocks satisfy some conditions we shall now describe.

The protocol can be used to distill a secret key if[21]

$$r := H(C|\mathbf{EM}; D = 1) - H(C|C'; D = 1) > 0, \tag{1}$$

where $\mathbf{E}$ is Eve's side-information across one block of n rounds and H is the von Neumann entropy[3,21]. The second entropy term, $H(C|C'; D = 1)$, can easily be determined via the QBER[1,11]. In[11], Eve's conditional entropy $H(C|\mathbf{EM}; D = 1)$ was lower-bounded using inequalities that are not necessarily tight, leading to the following result based on the (root-)fidelity $F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1$:

Theorem 1. A secret key can be generated if

$$F(\rho_{E|00}, \rho_{E|11})^2 > \frac{\epsilon}{(1 - \epsilon)}, \tag{2}$$

where $\rho_{E|a_0 b_0}$ denotes Eve's conditional state (in a single round) after Alice and Bob use inputs A_0 and B_0 and obtain outcomes a_0 and b_0.

Our goal will be to find a general method to certify the condition in Theorem 1. For later use, we also note that in the case where both parties have binary inputs and outputs, an alternative condition was derived[11] based on the trace distance $d(\rho, \sigma) := (1/2)\|\rho - \sigma\|_1$:

Theorem 2. If $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ and all measurements have binary outcomes, a secret key can be generated if

$$1 - d(\rho_{E|00}, \rho_{E|11}) > \frac{\epsilon}{(1 - \epsilon)}. \tag{3}$$

RESULTS

To find optimal bounds for Theorem 1, we need to minimize the fidelity for a given observed distribution. We show that this can be written as an SDP in Section "SDP Formulation of Minimum Fidelity Condition", and use this to calculate noise tolerances for a range of repetition-code advantage distillation setups in Section "Results From SDP". We conclude the Results section with a conjecture for a necessary condition that naturally complements the sufficient condition in[11].

SDP formulation of minimum fidelity condition

To see if Eve can minimize the fidelity such that (2) does not hold, we must first solve the following constrained optimization over all

possible ρ_{ABE} and possible measurements by Alice and Bob:

$$\begin{aligned} \inf \quad & F(\rho_{E|00}, \rho_{E|11}) \\ \text{s.t.} \quad & \Pr(ab|xy)_\rho = \mathbf{p}, \end{aligned} \tag{4}$$

where $\Pr(ab|xy)_\rho$ denotes the combined outcome probability distribution that would be obtained from ρ_{ABE} (and some measurements), and $\mathbf{p}$ represents the measurement distribution Alice and Bob actually observe. We observe that after Alice and Bob perform the key-generating measurements, the resulting tripartite state is of the form

$$\sum_{a,b \in \{0,1\}} \Pr(ab)|ab\rangle\langle ab| \otimes \rho_{E|ab}, \tag{5}$$

where for brevity we use $\Pr(ab)$ to denote the probability of getting outcomes (a, b) when the key-generating measurements are performed, i.e. $\Pr(ab|00)_\rho$.

To turn this optimization into an SDP, we first note that for any pair $(\rho_{E|00}, \rho_{E|11})$, there exists a measurement Eve can perform that leaves the fidelity invariant[22]. Also, since this measurement is on Eve's system only, performing it does not change the value $\Pr(ab|xy)_\rho$ in the constraint either. Therefore, given any feasible ρ_{ABE} and measurements in the optimization, we can produce another feasible state and measurements with the same objective value but with Eve having performed the[22] measurement that leaves the fidelity between the original $(\rho_{E|00}, \rho_{E|11})$ states invariant.

After performing this measurement, the state (5) becomes

$$\sum_{a,b \in \{0,1\}} \sum_i \Pr(ab|i) \Pr(i)|abi\rangle\langle abi|, \tag{6}$$

where the index i represents the possible outcomes for Eve's measurement (we do not limit the number of such outcomes for now). For these states, the fidelity can be written (assuming the distribution is symmetrized) as

$$F(\rho_{E|00}, \rho_{E|11}) = \sum_i \frac{\sqrt{\Pr(00|i)\Pr(11|i)}}{\Pr(00)} \Pr(i). \tag{7}$$

As for the constraints, we note that this measurement by Eve commutes with Alice and Bob's measurements, hence we can write $\Pr(ab|xy)_\rho = \sum_i \Pr(i)\mathbf{p}^i$, where $\mathbf{p}^i$ denotes the Alice-Bob distribution conditioned on Eve getting outcome i. Note that $\mathbf{p}^i$ is always a distribution realizable by quantum states and measurements, since conditioning on Eve getting outcome i produces a valid quantum state on Alice and Bob's systems.

The solution to (4) is therefore equal to the output of the optimization problem

$$\begin{aligned} \inf_{\Pr(i), \mathbf{p}^i} \quad & \sum_i \frac{\sqrt{\Pr(00|i)\Pr(11|i)}}{\Pr(00)} \Pr(i) \\ \text{s.t.} \quad & \sum_i \Pr(i)\mathbf{p}^i = \mathbf{p} \\ & \mathbf{p}^i \in \mathcal{Q}_{\mathcal{X}, \mathcal{Y}} \\ & \Pr(i) \in \mathcal{P}(\mathcal{I}), \end{aligned} \tag{8}$$

where $\mathcal{Q}_{\mathcal{X}, \mathcal{Y}}$ represents the set of quantum realizable distributions, and $\mathcal{P}(\mathcal{I})$ is the set of probability distributions $\Pr(i)$ on Eve's (now classical) side-information. We note that the constraints can be relaxed to a convergent hierarchy of SDP conditions, following the approach in[23–25], but the objective function is not affine. To address this, we show in Section "Approximating The Fidelity With Polytope Hyperplanes" that since the objective function is a convex sum of bounded concave functions, it can be approximated arbitrarily well using upper envelopes of convex polytopes. This will allow us to lower-bound this optimization using an SDP hierarchy, and do so without any knowledge about the dimension of Eve's system other than the assumption that all Hilbert spaces are finite-dimensional. Critically, SDPs have the important property

that they yield certified lower bounds on the minimum value (via the dual value), so we can be certain that we truly have a lower bound on the optimization (4). Our approach is based on the SDP reduction in[26]; however, we give a more detailed description and convergence analysis for the situation where the optimization involves concave functions of more than one variable (which is required in our work but not necessarily in[26]).

We remark that in this work, we focus on the situation where the constraints in (8) involve the full list of output probabilities. However, our analysis generalizes straightforwardly to situations where the constraints only consist of one or more linear combinations of these probabilities (though it is still necessary to have an estimate of the Pr(00) term in the denominator of the objective function), which can slightly simplify the corresponding DIQKD protocols.

Results from SDP

With the exception of the 2-input scenario for both parties (where Theorem 2 can be applied instead of Theorem 1), previous bounds for the fidelity were calculated via the Fuchs–van de Graaf inequalities[11,27]. To compare this against our method, we consider the depolarizing noise model[28], i.e. where the observed statistics have the form

$$(1 - 2q)\mathrm{Pr}_{target}(ab|xy) + q/2, \tag{9}$$

where Pr_{target} refers to some target distribution in the absence of noise. We consider three possible choices for the target distribution, and show our results for these scenarios in Fig. 1:

(a) Both Alice and Bob have four possible measurement settings. The target distribution is generated by:

$$|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$
$$A_0 = Z, A_1 = (X + Z)/\sqrt{2}, A_2 = X, A_3 = (X - Z)/\sqrt{2}$$
$$B_0 = Z, B_1 = (X + Z)/\sqrt{2}, B_2 = X, B_3 = (X - Z)/\sqrt{2}$$

(b) Alice has two measurement settings, whereas Bob has three. The target distribution is generated by:

$$|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$
$$A_0 = Z, A_1 = X$$
$$B_0 = Z, B_1 = (X + Z)/\sqrt{2}, B_2 = (X - Z)/\sqrt{2}$$

(c) Both Alice and Bob have two possible measurement settings. The target distribution is generated by:

$$|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$
$$A_0 = Z, A_1 = X$$
$$B_0 = (X + Z)/\sqrt{2}, B_1 = (X - Z)/\sqrt{2}$$

Case (a) is meant to include the Mayers-Yao self-test[29] and measurements that maximize the CHSH value. Alternatively, it can be viewed as having both parties perform all four of the measurements from (c). The results of[11] were able to prove security of this advantage distillation protocol up to $q \approx 6.8\%$ in this case. We manage to improve the noise tolerance to $q \approx 8.3\%$, which represents an increase of 1.5%.

As for case (b), the measurements A_0, A_1, B_1, B_2 maximize the CHSH value, and the key-generating measurement B_0 is chosen such that the QBER is zero in Pr_{target}. Again, our approach allows us to improve the noise tolerance threshold from $q \approx 6.0\%$ to $q \approx 7.0\%$.

The final case is a simple CHSH-maximizing setup, where both parties only have two measurements (this is similar to (b), but without the QBER-minimizing measurement for Bob). If we apply Theorem 1 for this case, our approach improves the threshold from $q \approx 3.6\%$ to $q \approx 6.7\%$. Also, if we instead optimize the measurements for robustness against depolarizing noise, this threshold can be increased to $q \approx 7.6\%$ (these optimized measurements correspond to measurements in the x-z plane at

angles $\theta_{A_0} = 0$, $\theta_{A_1} \approx 4.50$, $\theta_{B_0} \approx 3.61$, and $\theta_{B_1} \approx 5.39$ from the z-axis).

However, it is important to note that in case (c), Theorem 2 could be applied instead to yield a noise tolerance bound of $q \approx 7.7\%$, or $q \approx 9.1\%$ with optimized measurements[11]. These values are higher than those obtained above by applying our approach to case (c) with Theorem 1. This gives strong evidence that the sufficient condition in Theorem 1 is not a necessary one, because our approach should yield threshold values close to the optimal ones that could be obtained based only on that sufficient condition. (In principle, there may still be a gap between the true fidelity values and the bounds we computed; however, we consider this somewhat unlikely—see Section "Creating An SDP Algorithm That Minimizes The Fidelity".) Furthermore, we remark that it also suggests that the states $\rho_{E|00}, \rho_{E|11}$ that minimize the fidelity in this scenario cannot be pure. This is because in[11], the critical inequalites used in the proof of Theorem 1 are all saturated (in the large-n limit, at least) if those states are pure, indicating that the resulting sufficient condition should be basically 'tight' (i.e. a necessary condition) in this case. Since our results indicate that the sufficient condition is not a necessary one, this implies that the relevant states $\rho_{E|00}, \rho_{E|11}$ cannot be pure.

Given the above observations, we now conjecture what might be a necessary condition for security of the repetition-code protocol, to serve as a counterpart to Theorem 1.

Conjectured necessary condition for secret key distillation

While our result in this section can be stated in terms of the fidelity, we note that the reasoning holds for any distinguishability measure $g(\rho, \sigma)$ that has the following properties:

$$g(\rho, \sigma) = g(\sigma, \rho), \tag{10}$$

$$g(\rho \otimes \rho', \sigma \otimes \sigma') = g(\rho, \sigma)g(\rho', \sigma'), \tag{11}$$

$$g(\rho, \sigma) + d(\rho, \sigma) \geq 1, \tag{12}$$

$$g(\rho, \sigma)^2 + d(\rho, \sigma)^2 \leq 1. \tag{13}$$

The first line states that it is symmetric, the second that it is multiplicative across tensor products, and the last two lines correspond to the Fuchs–van de Graaf inequality in the case of the fidelity. An example of another distinguishability measure that satisfies these properties is the *pretty-good fidelity*[30–32], defined as $F_{pg}(\rho, \sigma) := \mathrm{Tr}\left[\sqrt{\rho}\sqrt{\sigma}\right]$. To keep our result more general, we shall first present it in terms of any such measure g, and discuss at the end of this section which choices yield better bounds. (In fact, we will only need (10)–(12) for this section. We list (13) as well because it can be used when studying *sufficient* conditions; see Section "Proof of Proposition 3".).

For any such g, we shall show that under a particular assumption, the condition

$$g(\rho_{E|00}, \rho_{E|11}) > \frac{\epsilon}{(1 - \epsilon)} \tag{14}$$

is necessary for (1) to hold. Specifically, the assumption is that given some state and measurements compatible with the observed statistics, Eve can produce some other state and measurements (with the same measurement-outcome probability distribution) that have the same value of $g(\rho_{E|00}, \rho_{E|11})$, but with $\rho_{E|01} = \rho_{E|10}$. This assumption seems reasonable because $\rho_{E|01} = \rho_{E|10}$ describes a situation where Eve is unable to distinguish the cases where Alice and Bob's outcomes are 01 versus 10, i.e. in some sense this appears to be a 'suboptimal' attack by Eve. (It might seem that this could be trivially satisfied by having Eve erase her side-information conditioned on Alice and Bob obtaining different outcomes. However, for Eve to do so, she would need to know when Alice and Bob obtain different
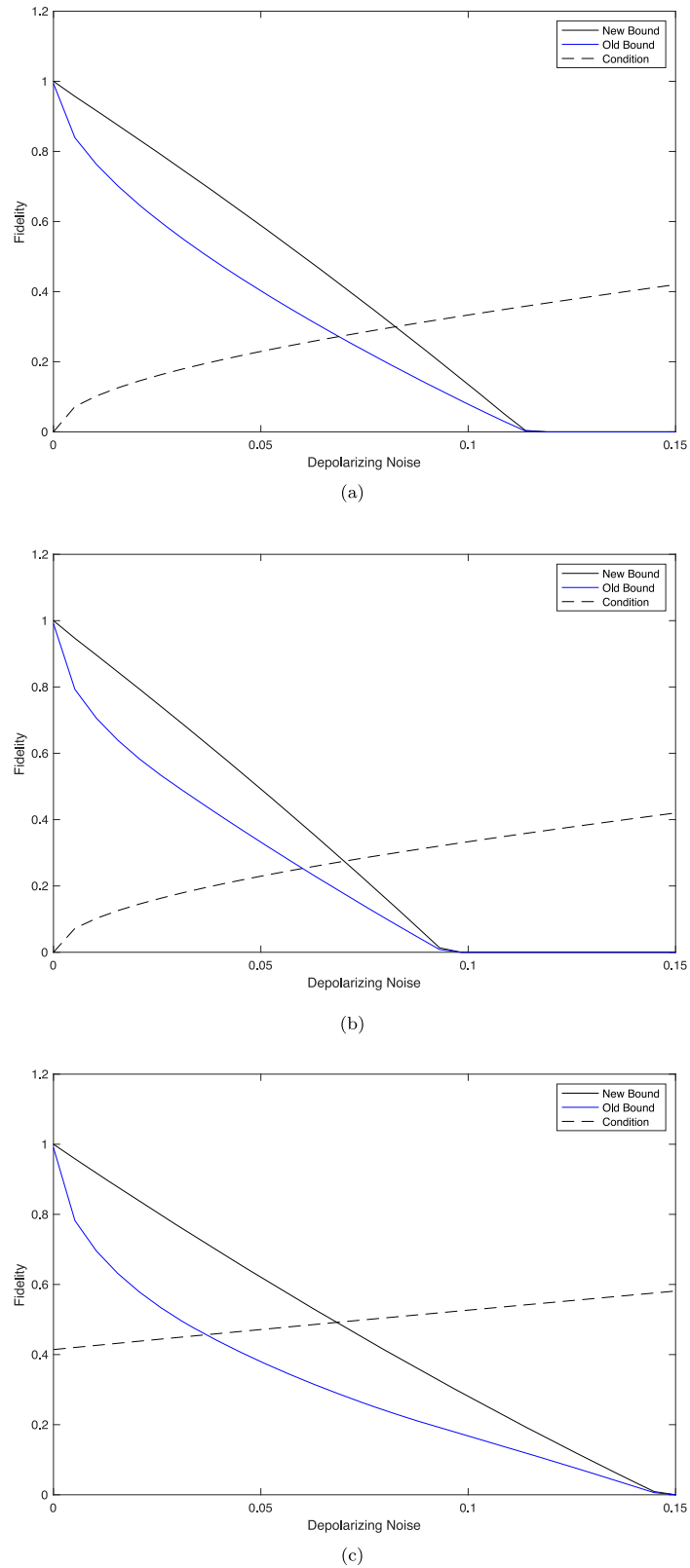
(a)

(b)

(c)

Fig. 1 Fidelity Bounds for depolarizing noise. Fidelity bounds as a function of depolarizing noise in several scenarios (described in main text), regarding the repetition-code protocol defined in our Introduction. The blue and black solid lines respectively represent the fidelity bounds derived via the previous approach (based on the Fuchs–van de Graaf inequality) and our new algorithm. It can be seen that the latter yields substantially better bounds. The dashed lines show the value of $\sqrt{\epsilon/(1-\epsilon)}$, so the points where they intersect the solid lines give the threshold values for which advantage distillation is possible according to the condition $F(\rho_{E|00}, \rho_{E|11})^2 > \frac{\epsilon}{(1-\epsilon)}$. For our approach, these thresholds are $q \approx 8.3\%, q \approx 7.0\%$, and $q \approx 6.7\%$ (from top to bottom in the scenarios shown here).

outcomes, and it is not clear that this is always possible for the states in Eve's optimal attacks in DIQKD scenarios. This property does hold for the QKD protocols studied in[14,15], and they use it as part of the proof that their condition is also necessary).

To prove that (14) is in fact necessary (given the stated assumption), we show that if it is not satisfied, then regardless of the choice of block size in the repetition-code protocol, in each block Eve can always produce a classical bit C'' such that

$$H(C|C''; D = 1) - H(C|C'; D = 1) \leq 0, \qquad (15)$$

which in turn implies (as noted in 14, using the results for binary symmetric channels in 18) that the repetition-code protocol as described above (i.e. with only one-way error correction from Alice to Bob after the initial blockwise 'distillation' procedure) cannot achieve positive asymptotic keyrate. To prove that Eve can indeed do this, we first derive an 'intermediate' implication (we give the proof in Section. "Proof of Proposition 3", based on the arguments in[11,14,15]):

Proposition 1. Let g be a function satisfying (10)–(12). If Eve's side-information satisfies $\rho_{E|01} = \rho_{E|10}$ and

$$g(\rho_{E|00}, \rho_{E|11}) \leq \frac{\epsilon}{(1-\epsilon)}, \qquad (16)$$

then for all n, Eve can use the information available to her (i.e. **E**, **M**, and $D = 1$) to construct a classical binary-valued guess C'' for the bit C that satisfies

$$\Pr(C \neq C''|D = 1) \leq \Pr(C \neq C'|D = 1). \qquad (17)$$

We now observe that the following relations hold (the first by Fano's inequality, the second by a straightforward calculation using the fact that the bits C, C' have uniform marginal distributions in the accepted blocks):

$$\begin{aligned} H(C|C''; D = 1) &\leq h_2(\Pr(C \neq C''|D = 1)), \\ H(C|C'; D = 1) &= h_2(\Pr(C \neq C'|D = 1)), \end{aligned} \qquad (18)$$

where h_2 is the binary entropy function. With this we find that Eve can indeed produce a bit C'' such that (15) holds, thereby concluding the proof.

If it could be shown that $\rho_{E|01} = \rho_{E|10}$ is in fact always possible to achieve for Eve without compromising $g(\rho_{E|00}, \rho_{E|11})$ or the post-measurement probability distribution, then (14) would genuinely be a necessary condition for security. It could then be used to find upper bounds for noise tolerance of the repetition-code protocol.

Regarding specific choices of the measure g, note that the pretty-good fidelity and the fidelity are related by $F(\rho, \sigma) \geq F_{pg}(\rho, \sigma) \geq F(\rho, \sigma)^2$ [31], with the first inequality being saturated for commuting states and the second inequality for pure states. In particular, the $F(\rho, \sigma) \geq F_{pg}(\rho, \sigma)$ side of the inequality implies that when aiming to find upper bounds on noise tolerance of this protocol using the condition (14), it is always better to consider pretty-good fidelity rather than fidelity (since all states satisfying the condition (14) with $g = F_{pg}$ also must satisfy it with $g = F$, but not vice versa). We leave for future work the question of whether there are other more useful choices for the measure g.

DISCUSSION
We discuss several consequences of our findings in this section. With regards to noise tolerances, our results show that by calculating bounds directly via the fidelity, a significant improvement can be achieved over the results based on Theorem 1 in[11]. This is especially important for the 3-input-scenario for Bob, as the previous advantage distillation bound falls well short of the bound for standard one-way error correction (even when only accounting

for the QBER and CHSH value)[1,9,10]. As advantage distillation improves the key rate for device-dependent QKD[7,12–17], it is expected to behave analogously for the device-independent setting. Our bound of $q \approx 7.0\%$ lies within 0.15% of the noise threshold for one-way protocols using the CHSH inequality[1] and within 0.40% of those using asymmetric CHSH inequalities[9,10], thereby substantially reducing this gap; however, it still does not yield an overall improvement. Again, this suggests that the sufficient condition (2) is in fact not necessary.

This brings us to the question of finding a condition that is both necessary and sufficient for security (of the repetition-code protocol) in the DIQKD setting. Note that while one could view the results of[14,15] as stating that condition (2) is both necessary and sufficient in the device-dependent QKD scenarios studied there, there are some subtleties to consider. Namely, that condition could be rewritten in several ways that are equivalent in those QKD scenarios, but not necessarily in DIQKD. For instance, in those QKD scenarios the states $\rho_{E|ab}$ are all pure, which means that $F(\rho_{E|00}, \rho_{E|11})^2$ could be rewritten as $1 - d(\rho_{E|00}, \rho_{E|11})^2$; however, this equivalence may not hold in the DIQKD setting, where those states might not be pure in general. Hence if we think in terms of trying to extend the necessary and sufficient condition in[14,15] to DIQKD, we would first need to address the question of finding the 'right' way to formulate that condition.

Indeed, our findings raise the question of whether attempting to determine security via $F(\rho_{E|00}, \rho_{E|11})$ is the right approach at all, because of the following informal argument. First, assuming that the fidelity bounds we obtained were essentially tight, our results indicate that there are scenarios where condition (2) is violated but the repetition-code protocol is still secure (via Theorem 2 instead), implying that it is not a necessary condition. However, if it is not necessary, it is not immediately clear how one might improve upon it. In particular, it seems unlikely that our conjectured necessary condition (14) could also be sufficient—after all, for the device-dependent QKD protocols studied in[14,15], it is condition (2) rather than (14) that is both sufficient and necessary. Since a Fuchs–van de Graaf inequality was used to incorporate the fidelity into the security condition and this inequality is most likely the reason that (2) is not necessary, finding a new, completely device-independent approach might necessitate using different inequalities.

A speculative, but interesting, alternative approach could be to instead consider the (non-logarithmic) quantum Chernoff bound[33,34],

$$Q(\rho, \sigma) := \inf_{0 \leq s \leq 1} \text{Tr}\left[\rho^s \sigma^{1-s}\right]. \qquad (19)$$

This is because this measure yields asymptotically tight bounds on the distinguishability of the states $\rho^{\otimes n}$ and $\sigma^{\otimes n}$[34], which we might be able to use. However, there is still some work that needs to be done before noise tolerances can be calculated via this method. For example, in contrast to the fidelity, it still not known whether there exists a measurement that preserves this distinguishability measure (this is the main reason we could construct an SDP for bounding the fidelity). Moreover, a security condition for the repetition-code protocol will in all likelihood require a measure of distinguishability between states that are not of the form $\rho^{\otimes n}$ and $\sigma^{\otimes n}$, albeit with some similarities (see Section "Proof of Proposition 3"). Hence one would need to investigate which aspects of the proof in[34] could be generalized to such states as well. We discuss this further in Section "Proof of Proposition 3".

Similar to[1], one could conduct a qubit analysis in the hopes that this approach produces fidelity bounds that are 'strong enough'. We show in[35], however, that this is not the case. Moreover, we prove for maximal CHSH violation, i.e. $S = 2\sqrt{2}$, that $F(\rho_{E|00}, \rho_{E|11}) = 1$ must hold for qubit strategies. As can be seen in[35], this will no longer generally be the case in higher dimensions.

In principle, by combining the bounds we computed here with the security proof in[11], one could compute lower bounds on the keyrates under the I.I.D. assumption (both in the asymptotic limit and for finite sample sizes, by using the finite version of the quantum asymptotic equipartition property). However, some numerical estimates we performed indicate that the resulting values are very low, even in the asymptotic case. Informally, this is likely because the proof in[11] bounds the von Neumann entropy in terms of fidelity with an inequality that is suboptimal in this context, as previously discussed. However, in the case of device-dependent QKD, the keyrates of this protocol are more reasonable, so it is possible that with better proof techniques, the same may hold for DIQKD.

We conclude by mentioning that it should be possible to use our algorithm to obtain keyrate lower bounds for one-way communication protocols as well. This is because the keyrate in such protocols is given by[21]

$$H(A_0|E) - H(A_0|B_0), \tag{20}$$

and the main challenge in computing this value is finding lower bounds on $H(A_0|E)$ (again, the $H(A_0|B_0)$ term is straightforward to handle, e.g. by estimating the QBER). Taking A_0 to be symmetrized as previously mentioned, we can apply the following inequality[36]:

$$H(A_0|E) \geq 1 - h_2\left(\frac{1 - F(\rho_{E|0}, \rho_{E|1})}{2}\right), \tag{21}$$

where the states $\rho_{E|a_0}$ refer to conditioning on the outcome A_0 only. Hence $H(A_0|E)$ can be bounded in terms of $F(\rho_{E|0}, \rho_{E|1})$. It should be straightforward to adapt our algorithm to bound such a fidelity expression as well, in which case our approach would also be useful to compute keyrates for non-advantage distillation setups. We aim to investigate this in future work.

METHODS
Fidelity for post-measurement tripartite states

Proposition 2. The fidelity, $F(\rho_{E|00}, \rho_{E|11})$, of a state of the form (6) is given by

$$F(\rho_{E|00}, \rho_{E|11}) = \sum_i \frac{\sqrt{Pr(00|i)\,Pr(11|i)}}{Pr(00)} Pr(i). \tag{22}$$

Proof. It is easily verified that:

$$\rho_{E|00} = \sum_i \frac{Pr(00|i)\,Pr(i)}{Pr(00)} |i\rangle\langle i| \tag{23}$$

$$\rho_{E|11} = \sum_i \frac{Pr(11|i)\,Pr(i)}{Pr(11)} |i\rangle\langle i|. \tag{24}$$

We note that $Pr(00) = Pr(11)$ due to the symmetrization step. Since these states are diagonal in the same basis, we can directly compute the fidelity:

$$F(\rho_{E|00}, \rho_{E|11}) \tag{25}$$

$$= Tr\left(\sqrt{\rho_{E|11}^{\frac{1}{2}} \rho_{E|00} \rho_{E|11}^{\frac{1}{2}}}\right) \tag{26}$$

$$= Tr\left(\sqrt{\sum_i \frac{Pr(11|i)\,Pr(00|i)\,Pr(i)^2}{Pr(00)^2} |i\rangle\langle i|}\right) \tag{27}$$

$$= \sum_i \frac{\sqrt{Pr(00|i)\,Pr(11|i)}}{Pr(00)} Pr(i), \tag{28}$$

as claimed.

Approximating the fidelity with polytope hyperplanes

Our goal in this section will be to find a lower bound on $\sqrt{Pr(00|i)\,Pr(11|i)}$ that can be written as a pointwise minimum of affine functions (of $\mathbf{p}^i$). Note that this function depends only on $Pr(00|i)$ and $Pr(11|i)$. (We need to consider both $Pr(00|i)$ and $Pr(11|i)$ without assuming they are equal, as we cannot assume the distributions conditioned on i are still symmetrized. This is because Eve's measurement takes place after the symmetrization step, and does not have to respect the symmetry.) Hence for the purposes of this section, we shall focus on 2-dimensional vectors $\mathbf{x}$, with the implicit understanding that

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} Pr(00|i) \\ Pr(11|i) \end{pmatrix}. \tag{29}$$

An affine function of such a vector $\mathbf{x}$ straightforwardly defines a corresponding affine function of $\mathbf{p}^i$, by considering the latter to depend only on the terms $Pr(00|i)$ and $Pr(11|i)$.

We begin the construction by defining an appropriate lattice of points:

Definition 1. For each $n \in \mathbb{N}$, let $\mathcal{L}_n$ denote a uniformly spaced grid of $2^n + 1 \cdot 2^n + 1$ points in $[0,1]^2$, i.e.

$$\mathcal{L}_n := \left\{0, \frac{1}{2^n}, \frac{2}{2^n}, \dots, 1\right\}^2. \tag{30}$$

For a concave function $f : [0,1]^2 \to \mathbb{R}$, we define the nth *order lattice of* f to be the set of $2^n + 1 \cdot 2^n + 1$ ordered triples $(x_1, x_2, f(\mathbf{x}))$ such that $(x_1, x_2) \in \mathcal{L}_n$.

(The above definition naturally generalizes to higher-dimensional arrays.)

Proposition 3. Let $\mathscr{P}_n$ denote the convex hull of the union of the nth order lattice of $f(\mathbf{x}) := \sqrt{x_1 x_2}$ and the nth order lattice of $g(\mathbf{x}) := 0$. Then $\mathscr{P}_n$ is a convex polytope that lies on or beneath the graph of the function $f(\mathbf{x}) = \sqrt{x_1 x_2}$.

Proof. <u>Step 1</u>: Show that the $2 \cdot (2^n + 1)^2$ lattice points lie on or beneath the graph of $f(\mathbf{x})$.

The lattice points of $f(\mathbf{x})$ automatically lie on the function graph as desired. Also, since $f(\mathbf{x})$ is always non-negative, the lattice points of $g(\mathbf{x})$ also lie on or beneath the function graph.

<u>Step 2</u>: Show that the convex hull of the union of both lattices lies on or beneath the graph of $f(\mathbf{x})$.

All points in the convex hull are a convex sum of the lattice points. As $f(\mathbf{x})$ is a concave function, such convex sums must lie on or beneath the graph of $f(\mathbf{x})$ as well.

We can use $\mathscr{P}_n$ to construct the desired lower bound on $f(\mathbf{x})$, as follows. As we shall formally prove in Proposition 7, this process is basically constructing the upper envelope of $\mathscr{P}_n$ (i.e. the function whose graph is the 'upper surface' of $\mathscr{P}_n$; this is formally defined by (37) below).

We first transform $\mathscr{P}_n$ to its facet representation[37], i.e. the description of the polytope by its facet-defining half-spaces. This gives us a set of inequalities described by parameters $\{(a_j, b_j, c_j, d_j)\}_j$, such that $(x_1, x_2, x_3) \in \mathscr{P}_n$ if and only if

$$a_j x_1 + b_j x_2 + c_j x_3 \leq d_j \quad \forall j. \tag{31}$$

To only retrieve the facets that will be used to approximate $f(\mathbf{x})$, i.e. the facets that describe the upper envelope of the polytope we constructed, keep only the facets for which $c_j > 0$. Geometrically, this corresponds to facets such that the normal vector (directed outwards from the polytope) has a vertical component that points upwards.

In our case, this means we remove the facets

$$-x_3 \leq 0 \tag{32}$$

$$x_1 \leq 1 \tag{33}$$

$$x_2 \leq 1, \tag{34}$$

which correspond to a lower horizontal facet and two vertical facets, respectively. (For more general concave f, there would be more vertical facets to remove, but the subsequent analysis still holds as it is based only on the fact that we keep exactly the facets with $c_j > 0$.) Let $\mathcal{S}$ denote the set of indices of the remaining facets. For each $j \in \mathcal{S}$, we define a corresponding affine function,

$$h_j(\mathbf{x}) := \frac{1}{c_j}(d_j - a_j x_1 - b_j x_2), \tag{35}$$

and use these to define a function (denoted f_n) that is meant to bound $f(\mathbf{x})$:

$$f_n(\mathbf{x}) := \min_{j \in \mathcal{S}} h_j(\mathbf{x}). \tag{36}$$

We verify that the above procedure indeed produces the upper envelope of $\mathscr{P}_n$:

Proposition 4. For all $n \in \mathbb{N}$ and $\mathbf{x} \in [0,1]^2$, f_n as defined above satisfies

$$f_n(\mathbf{x}) = \max\{x_3 | (\mathbf{x}, x_3) \in \mathscr{P}_n\}. \tag{37}$$

Proof. We first remark that it is indeed valid to write the expression (37) as a maximum rather than a supremum, because by construction of $\mathscr{P}_n$, the feasible set in (37) is non-empty (for $\mathbf{x} \in [0,1]^2$) and compact.

To prove the desired equality, we start by considering a fixed $\mathbf{x} \in [0,1]^2$, and arguing that the expression (37) is in fact equal to

$$\max\{x_3 | a_j x_1 + b_j x_2 + c_j x_3 \leq d_j \quad \forall j \in \mathcal{S}\}, \tag{38}$$

where the values a_j, b_j, c_j, d_j are from the facet inequalities (31). This is because $\mathscr{P}_n$ is exactly the set of points which satisfy the facet inequalities (31) for all j, so the only difference between (37) and (38) is that the latter maximization has omitted the facet inequalities such that $c_j \leq 0$. Removing these inequalities does not change the maximum value, by the following argument. The inequalities with $c_j = 0$ are independent of x_3, so either they are satisfied for all x_3 or for no x_3; however, as previously noted the feasible set of (37) is non-empty (for $\mathbf{x} \in [0,1]^2$), so the former must be the case. This implies that removing them does not change the maximum value. As for the inequalities with $c_j < 0$, notice that they are *lower* bounds on x_3, which means that removing them also does not change the maximum value (as long as the original maximization (37) is feasible, which it indeed is as noted previously). Thus the expressions (37) and (38) are equal for any $\mathbf{x} \in [0,1]^2$.

It remains to show that the original definition (36) of f_n is equal to (38) (when treating the latter as a function of $\mathbf{x}$ on the same domain). To do so, we show that they have the same subgraph. The subgraph of (36) is

$$\{(\mathbf{x}, x_3) | x_3 \leq h_j(\mathbf{x}) \quad \forall j \in \mathcal{S}\} \tag{39}$$

$$= \left\{(\mathbf{x}, x_3) \middle| x_3 \leq \frac{1}{c_j}(d_j - a_j x_1 - b_j x_2) \quad \forall j \in \mathcal{S}\right\} \tag{40}$$

$$= \{(\mathbf{x}, x_3) | a_j x_1 + b_j x_2 + c_j x_3 \leq d_j \quad \forall j \in \mathcal{S}\}, \tag{41}$$

using the fact that $c_j > 0$ for all $j \in \mathcal{S}$. (To be precise, in those expressions $\mathbf{x}$ should be restricted to the function domain, but the argument at this step holds regardless of whether we take the

domain to be $[0,1]^2$ or $\mathbb{R}^2$.) The last line is the subgraph of (38), so indeed the functions are equal. $\square$

With the formula (37), we can prove some intuitive properties of f_n, which will be useful in subsequent arguments:

Proposition 5. ...

$$f_n(\mathbf{x}) \leq f(\mathbf{x}) \quad \forall n \in \mathbb{N} \quad \forall \mathbf{x} \in [0,1]^2, \tag{42}$$

with $f_n(\mathbf{x}) = f(\mathbf{x})$ whenever $\mathbf{x} \in \mathcal{L}_n$.

Proof. We showed in Proposition 6 that $\mathscr{P}_n$ lies on or below the graph of f. Hence (42) follows immediately from the formula (37).

As for the equality condition, we note that for all $\mathbf{x} \in \mathcal{L}_n$ we have that $(\mathbf{x}, f(\mathbf{x}))$ lies in $\mathscr{P}_n$ (by construction). Hence (37) implies $f_n(\mathbf{x}) \geq f(\mathbf{x})$, which implies they must be equal since the reverse inequality (42) holds in general. $\square$

Proposition 6.

$$f_n(\mathbf{x}) \leq f_{n+1}(\mathbf{x}) \quad \forall n \in \mathbb{N} \quad \forall \mathbf{x} \in [0,1]^2. \tag{43}$$

Proof. By increasing n by one, we don't remove any lattice points, but rather just add additional points by halving the intervals in both directions. Thus we have $\mathscr{P}_n \subseteq \mathscr{P}_{n+1}$, which yields the desired inequality via (37). $\square$

We now show the sequence f_n indeed converges uniformly to f, so it yields arbitrarily tight bounds. The main intuition is that f_n forms a monotone sequence of uniformly continuous functions that have the same value as f on an increasingly fine grid.

Proposition 7. As $n \to \infty$, f_n converges uniformly to f.

Proof. We note that three conditions must hold:

$$\forall \delta > 0 \quad \exists n \in \mathbb{N} : \quad \forall \mathbf{x} \in [0,1]^2 \quad \exists \mathbf{y} \in \mathcal{L}_n \quad \text{s.t.} \quad |\mathbf{x} - \mathbf{y}| < \delta \tag{44}$$

$$\forall \epsilon_1 > 0 \quad \exists \delta_1 > 0 : \quad \forall \mathbf{x}, \mathbf{y}, \in [0,1]^2 \quad \text{if} \quad |\mathbf{x} - \mathbf{y}| < \delta_1 \quad \text{then} \quad |f(\mathbf{x}) - f(\mathbf{y})| < \epsilon_1 \tag{45}$$

$$\forall \epsilon_2 > 0 \quad \exists \delta_2 > 0 : \quad \forall \mathbf{x}, \mathbf{y}, \in [0,1]^2 \quad \text{if} \quad |\mathbf{x} - \mathbf{y}| < \delta_2 \quad \text{then} \quad |f_n(\mathbf{x}) - f_n(\mathbf{y})| < \epsilon_2 \tag{46}$$

The first statement just says that one can create an arbitrarily fine grid $\mathcal{L}_n$. The other two statements follow from the fact that continuous functions on compact sets are automatically uniformly continuous.

To show uniform convergence, we would need to prove that

$$\forall \epsilon > 0 \quad \exists n \in \mathbb{N} : \quad \forall n' \geq n \quad \forall \mathbf{x} \in [0,1]^2, \quad |f_{n'}(\mathbf{x}) - f(\mathbf{x})| < \epsilon. \tag{47}$$

To prove this, consider any $\epsilon > 0$, and choose n by the following procedure: set $\epsilon_1 < \epsilon/2$ and $\epsilon_2 < \epsilon/2$, and take some corresponding δ_1, δ_2 according to (45)–(46). Then set $\delta < \min(\delta_1, \delta_2)$, and take a corresponding $n \in \mathbb{N}$ according to (44). This choice of n has the desired property: for all $n' \geq n$ and for all $\mathbf{x} \in [0,1]^2$, (44) ensures that there exists some $\mathbf{y} \in \mathcal{L}_n$ satisfying $|\mathbf{x} - \mathbf{y}| < \delta$, hence

$$|f_{n'}(\mathbf{x}) - f(\mathbf{x})| \leq |f_n(\mathbf{x}) - f(\mathbf{x})| \tag{48}$$

$$\leq |f_n(\mathbf{x}) - f(\mathbf{y})| + |f(\mathbf{y}) - f(\mathbf{x})| \tag{49}$$

$$= |f_n(\mathbf{x}) - f_n(\mathbf{y})| + |f(\mathbf{y}) - f(\mathbf{x})| \tag{50}$$

$$< \epsilon_2 + \epsilon_1 < \epsilon, \tag{51}$$

where the first line follows from Propositions 8 and 9, while the third line follows from Proposition 8.

Creating an SDP algorithm that minimizes the fidelity

Without loss of generality, we ignore the factor $1/\text{Pr}(00)$ in the fidelity expression, as it is a positive constant (for a given distribution $\text{Pr}(ab|xy)$). We consider the functions f and f_n defined in the previous section, but as previously discussed, we now view them as functions of $\mathbf{p}^i$ (though with dependence only on the $\text{Pr}(00|i), \text{Pr}(11|i)$ terms), i.e. so we have $f(\mathbf{p}^i) = \sqrt{\text{Pr}(00|i)\,\text{Pr}(11|i)}$ and analogously for f_n. Since f_n is a lower bound on f, our optimization problem (after dropping the $1/\text{Pr}(00)$ factor) is clearly lower bounded by the following:

$$
\begin{aligned}
\inf_{\text{Pr}(i),\mathbf{p}^i} \quad & \sum_i f_n(\mathbf{p}^i)\,\text{Pr}(i) \\
\text{s.t.} \quad & \sum_i \text{Pr}(i)\mathbf{p}^i = \mathbf{p} \\
& \mathbf{p}^i \in \mathcal{Q}_{\mathcal{X,Y}} \\
& \text{Pr}(i) \in \mathcal{P}(\mathcal{I})
\end{aligned}
\tag{52}
$$

we can show that this lower bound converges uniformly to the original problem (8) as $n \to \infty$, using our previous results about convergence of f_n:

Proposition 8. As $n \to \infty$, the optimal value of (52) converges uniformly to that of (8) (rescaled by the constant factor of $1/\text{Pr}(00)$).

Proof. We denote the solutions to the original and approximate optimization problems by $f^\star(\mathbf{p})$ and $f_n^\star(\mathbf{p})$, respectively. For all $\mathbf{p} \in \mathcal{Q}_{\mathcal{X,Y}}$, for all $n \in \mathbb{N}$, and for all $\epsilon_1 > 0$, there exists a probability distribution $\text{Pr}(i)$ and a set of quantum realizable probability distributions $\mathbf{p}^i$ that satisfy the optimization constraints, such that

$$
\left| \sum_i f_n(\mathbf{p}^i)\,\text{Pr}(i) - f_n^\star(\mathbf{p}) \right| < \epsilon_1.
\tag{53}
$$

As $f_n(\mathbf{p}^i)$ converges uniformly to $f(\mathbf{p}^i)$, for all $\epsilon_2 > 0$, there exists an n such that for all $n' \geq n$ and all $\mathbf{p}^i \in \mathcal{Q}_{\mathcal{X,Y}}$,

$$
\left| \sum_i f(\mathbf{p}^i)\,\text{Pr}(i) - \sum_i f_{n'}(\mathbf{p}^i)\,\text{Pr}(i) \right| < \epsilon_2
\tag{54}
$$

if one chooses $\epsilon_1 + \epsilon_2 < \epsilon$, then

$$
\begin{aligned}
\forall \epsilon > 0 \quad & \exists n \in \mathbb{N}: \quad \forall n' \geq n \quad \forall \mathbf{p} \in \mathcal{Q}_{\mathcal{X,Y}}, \\
& \left| f^\star(\mathbf{p}) - f_{n'}^\star(\mathbf{p}) \right|
\end{aligned}
\tag{55}
$$

$$
\leq \left| \sum_i f(\mathbf{p}^i)\,\text{Pr}(i) - f_{n'}^\star(\mathbf{p}) \right|
\tag{56}
$$

$$
\begin{aligned}
\leq & \left| \sum_i f(\mathbf{p}^i)\,\text{Pr}(i) - \sum_i f_{n'}(\mathbf{p}^i)\,\text{Pr}(i) \right| \\
& + \left| \sum_i f_{n'}(\mathbf{p}^i)\,\text{Pr}(i) - f_{n'}^\star(\mathbf{p}) \right|
\end{aligned}
\tag{57}
$$

$$
< \epsilon_2 + \epsilon_1 < \epsilon,
\tag{58}
$$

as desired.

We now describe how to bound (52) using SDPs.

Proposition 9. (52) can be solved via an SDP hierarchy.

Proof. To reduce the sum to a bounded number of terms, we adopt the approach from[24,25]. Specifically, consider any feasible

point of the optimization (52), i.e. some feasible values for $\mathbf{p}^i$ and $\text{Pr}(i)$. Following the previous section, let $\mathcal{S}$ denote the indices of the affine functions used to define f_n.

Partition the summation domain of i into subsets $\{\mathcal{R}_j\}_{j \in \mathcal{S}}$, such that $i \in \mathcal{R}_j$ implies the minimum in the definition (36) of $f_n(\mathbf{p}^i)$ is attained by the index j. In other words, $i \in \mathcal{R}_j$ implies $f_n(\mathbf{p}^i) = h_j(\mathbf{p}^i)$. (Geometrically speaking, we are partitioning the terms based on which facet of $\mathscr{P}_n$ they lie on.) Let us define

$$
\tilde{\text{P}}_j = \sum_{i \in \mathcal{R}_j} \text{Pr}(i), \quad \tilde{\mathbf{p}}^j = \sum_{i \in \mathcal{R}_j} \mathbf{p}^i \frac{\text{Pr}(i)}{\tilde{\text{P}}_j}.
\tag{59}
$$

Note that the choice of partition may not be unique, e.g. if the feasible point being considered has a $\mathbf{p}^i$ term where the minimum in the definition (36) is attained by more than one $j \in \mathcal{S}$. However, this nonuniqueness is not a problem; any partition with the specified property suffices. Also, some $\mathcal{R}_j$ may be empty, but this is not a problem either; one should simply select an arbitrary distribution $\tilde{\mathbf{p}}^j \in \mathcal{Q}_{\mathcal{X,Y}}$ instead of using (59) (since the denominator is zero if $\mathcal{R}_j$ is empty).

Then we can rewrite

$$
\sum_{i \in \mathcal{R}_j} f_n(\mathbf{p}^i)\,\text{Pr}(i) = \sum_{i \in \mathcal{R}_j} h_j(\mathbf{p}^i)\,\text{Pr}(i)
\tag{60}
$$

$$
= \left(\sum_{i \in \mathcal{R}_j} h_j(\mathbf{p}^i)\frac{\text{Pr}(i)}{\tilde{\text{P}}_j} \right) \tilde{\text{P}}_j
\tag{61}
$$

$$
= h_j(\tilde{\mathbf{p}}^j)\tilde{\text{P}}_j,
\tag{62}
$$

where in the third line we used the fact that h_j is affine and $\{\text{Pr}(i)/\tilde{\text{P}}_j\}_i$ forms a normalized probability distribution over $i \in \mathcal{R}_j$.

Observe that $\tilde{\mathbf{p}}^j \in \mathcal{Q}_{\mathcal{X,Y}}$ (by convexity of $\mathcal{Q}_{\mathcal{X,Y}}$), and that $\tilde{\text{P}}_j$ is a valid probability distribution (over $j \in \mathcal{S}$) since the sets $\mathcal{R}_j$ partition the sum over i. Together with the expression (62), this implies that if we replace the original objective function with

$$
\sum_{i \in \mathcal{S}} h_i(\mathbf{p}^i)\,\text{Pr}(i),
\tag{63}
$$

the value of the optimization will not increase, since every feasible point of the original optimization yields another feasible point with the same objective value but in the form (63). In other words, by rewriting the objective function in the form (63), we have essentially taken $\mathbf{p}^i$ and $\text{Pr}(i)$ to be the $\tilde{\mathbf{p}}^j$ and $\tilde{\text{P}}_j$ we constructed above. Furthermore, since we constructed f_n via (36),

$$
h_i(\mathbf{p}^i) \geq f_n(\mathbf{p}^i)
\tag{64}
$$

holds for all $\mathbf{p}^i \in \mathcal{Q}_{\mathcal{X,Y}}$. Thus (63) is a natural upper bound on our previous objective function in (52), so replacing the latter with the former will not decrease the optimal value either. In summary, we can replace the objective function with (63) without changing the optimal value, which is useful because it is the sum of a (known) finite number of terms; also, we no longer need to address the minimization in the definition of f_n.

However, since $h_i(\mathbf{p}^i)\text{Pr}(i)$ is a product of affine functions of the optimization variables, (63) is still not an affine function. To deal with this, we consider subnormalized probability distributions, i.e. the terms in the distribution sum up to a value in $[0, 1]$ instead of having to sum to 1 (here we mean summing over (a, b) for each choice of (x, y); also, we impose that all (x, y) have the same normalization factor). In our case, we scale the probability distributions $\mathbf{p}^i$ by the scaling factor $\text{Pr}(i)$, i.e. we define new variables $\breve{\mathbf{p}}^i = \text{Pr}(i)\mathbf{p}^i$. To verify that the objective function is affine in these new variables, we show that each term in the summation is affine. Writing $h_i(\mathbf{p}^i)$ in the form $a_i + \mathbf{a}_i \cdot \mathbf{p}^i$ for some scalar a_i and

vector $\mathbf{a}_i$, we have

$$h_i(\mathbf{p}^i)\Pr(i) \tag{65}$$

$$= a_i\Pr(i) + (\mathbf{a}_i \cdot \mathbf{p}^i)\Pr(i) \tag{66}$$

$$= a_i\left(\sum_{ab}\Pr(ab|00i)\Pr(i)\right) + \mathbf{a}_i \cdot \check{\mathbf{p}}^i \tag{67}$$

$$= a_i\mathbf{z} \cdot \check{\mathbf{p}}^i + \mathbf{a}_i \cdot \check{\mathbf{p}}^i, \tag{68}$$

where $\mathbf{z}$ is a vector, which contains only zeroes and ones, that specifies the terms summed over in (67) (this is possible since each $\Pr(ab|00i)\Pr(i)$ term is equal to an element of $\check{\mathbf{p}}^i$; also, note that the choice to use the input pair $xy = 00$ at that step is arbitrary and any other pair would suffice). This is indeed affine (in fact linear) in $\check{\mathbf{p}}^i$. As for the constraints, observe that the first constraint is linear in $\check{\mathbf{p}}^i$. Also, as long as $\mathbf{p}$ is normalized, we can replace the second and third constraints by a single constraint $\check{\mathbf{p}}^i \in \check{\mathcal{Q}}_{\mathcal{X},\mathcal{Y}}$, where $\check{\mathcal{Q}}_{\mathcal{X},\mathcal{Y}}$ denotes subnormalized distributions compatible with quantum theory (and with a common normalization factor for all input pairs (x, y)). This is because when $\mathbf{p}$ is normalized, the first constraint implicitly imposes a normalization condition on the variables $\check{\mathbf{p}}^i$ that subsumes the original third constraint.

In summary, the optimal value of (52) is the same as

$$\inf_{\check{\mathbf{p}}^i} \quad \sum_{i \in \mathcal{S}} a_i\mathbf{z} \cdot \check{\mathbf{p}}^i + \mathbf{a}_i \cdot \check{\mathbf{p}}^i$$
$$\text{s.t.} \quad \sum_i \check{\mathbf{p}}^i = \mathbf{p} \tag{69}$$
$$\check{\mathbf{p}}^i \in \check{\mathcal{Q}}_{\mathcal{X},\mathcal{Y}}$$

where $a_i, \mathbf{a}_i, \mathbf{z}$ are the values described above regarding (68). Finally, we use the fact that there exists a SDP hierarchy for the verification of subnormalized quantum probability distributions $\check{\mathcal{Q}}_{\mathcal{X},\mathcal{Y}}$[23–25]. Hence the entire constrained optimization can be lower-bounded by using this hierarchy of SDP relaxations to impose the $\check{\mathcal{Q}}_{\mathcal{X},\mathcal{Y}}$ constraint, yielding a sequence of increasingly tight lower bounds on the optimization. Note that each level of the hierarchy yields a certified *lower* bound, i.e. our results are never an over-estimate of the true minimum of the optimization.

We close this section with some implementation remarks. For Fig. 1a, we used a 4×4 lattice to construct the bound f_n, and NPA level 2. For Fig. 1b, c, we used an 8×8 lattice and NPA level 3 (for the latter case, we found that NPA levels 2 and 4 also gave basically the same results). The SDP runtime was not too long in all cases, ranging from a few seconds to under 15 minutes (for each data point on the graphs), depending on the size of the scenarios.

In principle, there are two ways in which our bounds might not be tight: first, we have replaced f with f_n; second, the SDP hierarchy of[23] may not have converged to a sufficiently tight bound. We consider the latter to be less of an issue, because this hierarchy typically performs well in situations with few inputs and outputs (for instance in Fig. 1c, which was the main example supporting our reasoning that Theorem 1 may not be a necessary condition). As for the former, we performed some checks by noting that every feasible point of the optimization we solve (namely, (69) with the constraint $\check{\mathbf{p}}^i \in \check{\mathcal{Q}}_{\mathcal{X},\mathcal{Y}}$ relaxed to the SDP hierarchy) gives us a feasible point of the original optimization (8) (albeit with the constraint $\mathbf{p}^i \in \mathcal{Q}_{\mathcal{X},\mathcal{Y}}$ relaxed to the SDP hierarchy). We found that for points near the thresholds shown in Fig. 1b, c, the corresponding feasible values in that original optimization were within 0.0003 of the lower bounds we obtained, indicating that the bounds are almost tight. (For Fig. 1a we found a bigger gap of about 0.03 using a 6×6 lattice to find feasible points, but this is also not too large).

Note that by applying Carathéodory's theorem for convex hulls, we can argue the minimum value in the optimization (52) can always be attained by a distribution $\Pr(i)$ with at most $d + 2$ nonzero terms, where d is the dimension of $\mathbf{p}$. This eventually implies that the minimum value in our final optimization (69) can be attained with at most $d + 2$ of the subnormalized distributions $\check{\mathbf{p}}^i$ being nonzero. In practice, $d + 2$ is often smaller than the number of affine bounds h_i (i.e. $|\mathcal{S}|$). Hence if the optimization (69) is too large to solve directly, an alternative approach in principle is to run it for every subset of $\mathcal{S}$ with size $d + 2$, then take the smallest of the resulting values. This reduces the size of each individual optimization, but comes at the cost of having to run many more of them.

As another point regarding efficiency, note that our construction of f_n involves a transformation to the facet representation of $\mathscr{P}_n$. While this can be quickly implemented when $\mathbf{x}$ is 2-dimensional, the transformation may be computationally demanding in high dimensions[37]. It would be interesting to know whether there are more efficiently computable alternatives.

A natural attempt would be to partition the domain of f into triangles (more generally, simplices) and construct an affine lower bound in each triangle, yielding a piecewise affine lower bound on f. One benefit of this approach is that it may be usable (though not necessarily straightforward) in some cases when f is not concave, whereas our current construction of f_n relies heavily on concavity of f. However, it runs into the subtle issue that having f_n be a pointwise minimum of affine functions is a stronger condition than simply requiring it to be piecewise affine; in particular, our analysis used the structure in the former. (Note that it is not useful to simply take the pointwise minimum of the affine bounds constructed this way — there can be very large gaps between f and the resulting bound).

Still, it may be possible to adapt our analysis to this case. To sketch a rough outline, we would again aim to partition the sum in (52) into finitely many subsets, but this time by which of the triangles each $\mathbf{p}^i$ lies in. Transforming to a new feasible point as in (59) (here we would need to use the convexity of the triangles to argue that each $\tilde{\mathbf{p}}^j$ still lies within its defining triangle), we should be able to perform a similar analysis to reduce the objective to the form (63), but with the summation index ranging over the triangles in the domain instead. However, to proceed further we would need to constrain each $\tilde{\mathbf{p}}^j$ to remain within the corresponding triangle, appearing as additional constraints in (52). Since these constraints can be imposed as affine constraints, the final result should still be solvable using the SDP hierarchy.

Finally, we note that in[26], the authors do not convert their optimization to the form (69), but rather to a dual form via a somewhat different argument. A similar argument is possible in principle here (see[35]), but we choose to present our result in the form (69) since it seems most straightforward for implementation. We thank the authors of[26] for clarifications on these different approaches.

Proof of Proposition 3

Proof. After Alice and Bob conduct n key-generating measurements, the resulting classical-classical-quantum tripartite state is of the form

$$\sum_{\mathbf{a},\mathbf{b}\in\{0,1\}^n}\Pr(\mathbf{ab})|\mathbf{ab}\rangle\langle\mathbf{ab}| \otimes \rho_{\mathbf{E}|\mathbf{ab}}. \tag{70}$$

Considering that Alice and Bob only take accepted blocks into account, i.e. $D = 1$, and Alice sends the message $\mathbf{M} = \mathbf{m}$, it is simple to construct the bipartite state $\rho_{C\mathbf{E}|\mathbf{M}=\mathbf{m}\wedge D=1}$, which denotes the state that describes both the value of the bit C and Eve's corresponding side-information. As $D = 1$ implies that Alice's and Bob's measurement devices either output $\mathbf{m}$ or $\overline{\mathbf{m}} = \mathbf{m} \oplus \mathbf{1}$,

the resulting state is given by

$$\rho_{C\mathbf{E}|\mathbf{M}=\mathbf{m}\wedge D=1} = \sum_{c\in\{0,1\}} \frac{1}{2}|c\rangle\langle c|\otimes\omega_c, \tag{71}$$

where

$$\omega_0 = \frac{\Pr(\mathbf{mm})\rho_{\mathbf{E}|\mathbf{mm}} + \Pr(\mathbf{m\overline{m}})\rho_{\mathbf{E}|\mathbf{m\overline{m}}}}{\Pr(\mathbf{mm}) + \Pr(\mathbf{m\overline{m}})} \tag{72}$$

$$\omega_1 = \frac{\Pr(\overline{\mathbf{m}}\mathbf{m})\rho_{\mathbf{E}|\overline{\mathbf{m}}\mathbf{m}} + \Pr(\overline{\mathbf{mm}})\rho_{\mathbf{E}|\overline{\mathbf{mm}}}}{\Pr(\overline{\mathbf{m}}\mathbf{m}) + \Pr(\overline{\mathbf{mm}})} \tag{73}$$

denotes Eve's conditioned side-information[11]. Moreover, after symmetrization, we get $\Pr(\mathbf{mm}) = \Pr(\overline{\mathbf{mm}}) = \frac{(1-\epsilon)^n}{2^n}$ and $\Pr(\mathbf{m\overline{m}}) = \Pr(\overline{\mathbf{m}}\mathbf{m}) = \frac{\epsilon^n}{2^n}$, which further simplifies (72) and (73).

Eve's ability to correctly guess C therefore depends on the distinguishability of ω_0 and ω_1. As C, and consequently ω_i, is distributed uniformly, we may use the operational interpretation of the trace distance to derive Eve's optimal guessing probability. The optimal probability of guessing it incorrectly is thus given by

$$\Pr(C\neq C''|D=1) = \frac{1}{2}(1-d(\omega_0,\omega_1)). \tag{74}$$

We first consider Bob's guess. As $C\neq C'$ only if Alice measures $\mathbf{m}$ and Bob measures $\overline{\mathbf{m}}$ or vice versa,

$$\Pr(C\neq C'|D=1) = \frac{\Pr(\mathbf{m\overline{m}}) + \Pr(\overline{\mathbf{m}}\mathbf{m})}{\Pr(\mathbf{mm}) + \Pr(\overline{\mathbf{mm}}) + \Pr(\mathbf{m\overline{m}}) + \Pr(\overline{\mathbf{m}}\mathbf{m})} = \frac{\epsilon^n}{\epsilon^n + (1-\epsilon)^n} =: \delta_n. \tag{75}$$

We now consider Eve's guess. By using the reverse triangle inequality of the 1-norm, we can get a lower bound on $d(\omega_0,\omega_1)$ in terms of δ_n:

$$d(\omega_0,\omega_1) \geq (1-\delta_n)\cdot d(\rho_{\mathbf{E}|\mathbf{mm}},\rho_{\mathbf{E}|\overline{\mathbf{mm}}}) - \delta_n\cdot d(\rho_{\mathbf{E}|\mathbf{m\overline{m}}},\rho_{\mathbf{E}|\overline{\mathbf{m}}\mathbf{m}}), \tag{76}$$

and substituting this into (74) yields

$$\begin{aligned}\Pr(C\neq C''|D=1) &\leq \tfrac{1}{2}(1-(1-\delta_n)\cdot d(\rho_{\mathbf{E}|\mathbf{mm}},\rho_{\mathbf{E}|\overline{\mathbf{mm}}}) + \delta_n\cdot d(\rho_{\mathbf{E}|\mathbf{m\overline{m}}},\rho_{\mathbf{E}|\overline{\mathbf{m}}\mathbf{m}}))\\ &= \tfrac{1}{2}(1-(1-\delta_n)\cdot d(\rho_{\mathbf{E}|\mathbf{mm}},\rho_{\mathbf{E}|\overline{\mathbf{mm}}})),\end{aligned} \tag{77}$$

where to get the second line we used the hypothesis $\rho_{E|01}=\rho_{E|10}$ (which implies $\rho_{\mathbf{E}|\mathbf{m\overline{m}}}=\rho_{\mathbf{E}|\overline{\mathbf{m}}\mathbf{m}}$). The 'Fuchs–van de Graaf-type' inequality (12) then implies that

$$\Pr(C\neq C''|D=1) \leq \frac{1}{2}(1-(1-\delta_n)\cdot(1-g(\rho_{\mathbf{E}|\mathbf{mm}},\rho_{\mathbf{E}|\overline{\mathbf{mm}}}))). \tag{78}$$

Moreover, note that we have $g(\rho_{\mathbf{E}|\mathbf{mm}},\rho_{\mathbf{E}|\overline{\mathbf{mm}}}) = g(\rho_{E|00},\rho_{E|11})^n$ (by applying the I.I.D. assumption together with the multiplicative property (11), followed by the symmetry property (10)). Therefore a sufficient condition for (17) to hold is

$$\frac{1}{2}(1-(1-\delta_n)\cdot(1-g(\rho_{E|00},\rho_{E|11})^n)) \leq \delta_n. \tag{79}$$

We conclude the proof by showing that for all $n\in\mathbb{N}$, (16) is equivalent to (79). Note that the inequality (12) (together with the fact that $d(\rho,\sigma)\leq 1$) implies that $g(\rho,\sigma)$ is always non-negative. Hence for all $n\in\mathbb{N}$ the inequality (16) is equivalent to

$$g(\rho_{E|00},\rho_{E|11})^n \leq \frac{\epsilon^n}{(1-\epsilon)^n} = \frac{(1-\epsilon)^n-(1-\epsilon)^n+\epsilon^n}{(1-\epsilon)^n} = 1-\frac{(1-\epsilon)^n-\epsilon^n}{(1-\epsilon)^n} \tag{80}$$

This inequality can be rewritten as

$$1-g(\rho_{E|00},\rho_{E|11})^n \geq \frac{(1-\epsilon)^n-\epsilon^n}{(1-\epsilon)^n} = \frac{1-2\delta_n}{1-\delta_n}. \tag{81}$$

The previous inequality is equivalent to

$$1-(1-\delta_n)\cdot\left(1-g\left(\rho_{E|00},\rho_{E|11}\right)^n\right) \leq 2\delta_n \tag{82}$$

and dividing both sides by 2 gives (79).

We note that the current gap between the sufficient and necessary conditions can be viewed as arising from the 'Fuchs–van de Graaf-type' inequalities (12) and (13). This is because the sufficient condition (Theorem 1) proof requires lower bounds on $H(C|\mathbf{EM};D=1)$, whereas the conjectured necessary condition needs upper bounds. As noted in the supplemental material for[11], the analysis we performed above also serves an alternative approach for proving Theorem 1 (the main proof in[11] instead used the inequality from[36] to lower-bound $H(C|\mathbf{EM};D=1)$). The main idea is that $H(C|\mathbf{EM};D=1)$ can be lower bounded by the min-entropy, which simply equals $-\log((1-d(\omega_0,\omega_1))/2)$. By performing an analysis similar to the above but using the inequality (13) instead of (12), we end up (after some asymptotic analysis) with a sufficient condition for (1) to hold, which turns out to be exactly the same as Theorem 1 (except that since the only properties of g required for this argument are (10)–(13), it would hold with any g satisfying those properties in place of the fidelity F). Note that no assumption is needed on $d(\rho_{E|01},\rho_{E|10})$ for this direction of the proof. From this perspective, it appears that the main contribution to the gap is the difference between the bounds (12) and (13), since other steps of the proof have comparatively small effects asymptotically.

However, regarding possible choices of distinguishability measure g in this generalized version of Theorem 1, note that replacing the fidelity in the theorem statement with the pretty-good fidelity yields a worse result, due to the inequality $F(\rho,\sigma)\geq F_{pg}(\rho,\sigma)$. (The opposite was true for the necessary condition, Proposition 3). The question remains of whether there are choices for the measure g that yield better bounds for the sufficient condition.

Finally, we remark that the above analysis essentially centers around distinguishing $\rho_{\mathbf{E}|\mathbf{mm}}$ and $\rho_{\mathbf{E}|\overline{\mathbf{mm}}}$. Returning to our discussion of the quantum Chernoff bound, we observe that unless $\mathbf{M}=\mathbf{0}$ or $\mathbf{M}=\mathbf{1}$, these states are not of the form $\rho^{\otimes n}$ and $\sigma^{\otimes n}$ studied in the quantum Chernoff bound, though there are some structural similarities. (If $\mathbf{M}$ were restrained to $\mathbf{M}=\mathbf{0}$ or $\mathbf{M}=\mathbf{1}$, one may consider only $\mathbf{M}=\mathbf{0}$, as $\mathbf{M}=\mathbf{1}$ can be thought of as a relabeling of measurement outcomes). Since $\mathbf{M}$ is not restricted to these cases in general, we would need to study whether these other structurally similar states could still be analyzed using the proof techniques for the quantum Chernoff bound.

As another perspective, note that the quantum Chernoff bound in fact satisfies almost all the properties (10)–(13)[31]. However, instead of the equality (11), it only satisfies the inequality $g(\rho\otimes\rho',\sigma\otimes\sigma')\geq g(\rho,\sigma)g(\rho',\sigma')$. Looking through the proofs described above for the necessary versus sufficient conditions, this means that only the proof of the latter generalizes directly if we choose $g=Q$. Unfortunately, Theorem 1 with the fidelity simply replaced by the quantum Chernoff bound is a worse result, because the quantities are related by $F(\rho,\sigma)\geq Q(\rho,\sigma)$[33] (similar to the previous situation for pretty-good fidelity). Hence an argument that simply follows the proof structure sketched above with $g=Q$ would not yield a better result than the the original Theorem 1 statement based on fidelity — to get better results using the quantum Chernoff bound, one would need a different proof structure.

DATA AVAILABILITY

The datasets produced in this work are available from the authors upon reasonable request.

CODE AVAILABILITY

The MATLAB code for this paper can be found at the following URL: https://github.com/Thomas0501/Fidelity-Optimization

REFERENCES

1. Pironio, S. et al. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11**, 045021 (2009).
2. Scarani V. The device-independent outlook on quantum physics (lecture notes on the power of Bell's theorem). Preprint at https://arxiv.org/abs/1303.3081 (2013).
3. Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R. & Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commun.* **9**, 459 (2018).
4. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
5. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–478 (2014).
6. Barrett, J., Colbeck, R. & Kent, A. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.* **110**, 010503 (2013).
7. Gottesman, D. & Lo, H.-K. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theory* **49**, 457–475 (2003).
8. Ho, M. et al. Noisy preprocessing facilitates a photonic realization of device-independent quantum key distribution. *Phys. Rev. Lett.* **124**, 230502 (2020).
9. Woodhead E., Acín A., & Pironio S. Device-independent quantum key distribution based on asymmetric CHSH inequalities. *Quantum.* vol 5, 443 (Verein zur Forderung des Open Access Publizierens in den Quantenwissenschaften, 2021).
10. Sekatski P. et al. Device-independent quantum key distribution from generalized CHSH inequalities. *Quantum.* vol 5, 444 (Verein zur Forderung des Open Access Publizierens in den Quantenwissenschaften, 2021).
11. Tan, E. Y.-Z., Lim, C. C.-W. & Renner, R. Advantage distillation for device-independent quantum key distribution. *Phys. Rev. Lett.* **124**, 020502 (2020).
12. Chau, H. F. Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate. *Phys. Rev. A* **66**, 060302 (2002).
13. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **06**, 1–127 (2008).
14. Bae J. & Acín A. Key distillation from quantum channels using two-way communication protocols. *Phys. Rev. A*, **75**, 012334 (American Physical Society, 2007).
15. Acín, A. et al. Secrecy properties of quantum channels. *Phys. Rev. A* **73**, 012327 (2006).
16. Watanabe, S., Matsumoto, R., Uyematsu, T. & Kawano, Y. Key rate of quantum key distribution with hashed two-way classical communication. *Phys. Rev. A* **76**, 032312 (2007).
17. Khatri, S. & Lütkenhaus, N. Numerical evidence for bound secrecy from two-way postprocessing in quantum key distribution. *Phys. Rev. A* **95**, 042320 (2017).
18. Maurer, U. M. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **39**, 733–742 (1993).
19. Wolf, S., *Information-Theoretically and Computationally Secure Key Agreement in Cryptography*. PhD thesis, ETH Zurich, 1999.
20. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
21. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. Math. Phys. Eng. Sci.* **461**, 207–235 (2005).
22. Fuchs, C. A. & Caves, C. M. Mathematical techniques for quantum communication theory. *Open Syst. Inf. Dyn.* **3**, 345–356 (1995).
23. Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.* **10**, 073013 (2008).
24. Bancal, J.-D., Sheridan, L. & Scarani, V. More randomness from the same data. *New J. Phys.* **16**, 033011 (2014).
25. Nieto-Silleras, O., Pironio, S. & Silman, J. Using complete measurement statistics for optimal device-independent randomness evaluation. *New J. Phys.* **16**, 013035 (2014).
26. Himbeeck T. V., & Pironio S. Correlations and randomness generation based on energy constraints. Preprint at https://arxiv.org/abs/1905.09117 (2019).
27. Fuchs, C. & van de Graaf, J. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inf. Theory* **45**, 1216–1227 (1999).
28. Nielsen M. A. & Chuang I. L. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.
29. Mayers, D. & Yao, A. Self testing quantum apparatus. *Quantum Info. Comput.* **4**, 273–286 (2004).
30. Luo, S. & Zhang, Q. Informational distance on quantum-state space. *Phys. Rev. A* **69**, 032106 (2004).
31. Audenaert, K. M. R. Comparisons between quantum state distinguishability measures. *Quantum Info. Comput.* **14**, 31–38 (2014).
32. Iten, R., Renes, J. M. & Sutter, D. Pretty good measures in quantum information theory. *IEEE Trans. Inf. Theory* **63**, 1270–1279 (2017).
33. Audenaert, K. M. R. et al. Discriminating states: the quantum chernoff bound. *Phys. Rev. Lett.* **98**, 160501 (2007).
34. Nussbaum, M. & Szkoła, A. The Chernoff lower bound for symmetric quantum hypothesis testing. *Ann. Stat.* **37**, 1040–1057 (2009).
35. Hahn T. Fidelity Bounds for Device-Independent Advantage Distillation, Master's thesis, ETH Zurich, 2021.
36. Roga, W., Fannes, M. & Życzkowski, K. Universal Bounds for the Holevo Quantity, Coherent Information, and the Jensen-Shannon Divergence. *Phys. Rev. Lett.* **105**, 040505 (2010).
37. Toth, C. D., O'Rourke, J., & Goodman, J. E (Eds.). Handbook of Discrete and Computational Geometry (3rd ed.). Chapman and Hall/CRC, 2017, ch. 15, pp. 383–414. https://doi.org/10.1201/9781315119601.
38. Johnston, N. QETLAB: A MATLAB toolbox for quantum entanglement, version 0.9. http://qetlab.com, (2016).
39. Grant, M. & Boyd, S. CVX: Matlab Software for Disciplined Convex Programming, version 2.1. http://cvxr.com/cvx, (2014).
40. Grant, M., & Boyd, S. Graph implementations for nonsmooth convex programs, in *Recent Advances in Learning and Control* (V. Blondel, S. Boyd, and H. Kimura, eds.), Lecture Notes in Control and Information Sciences, pp. 95–110, Springer-Verlag Berlin Heidelberg, 2008. https://web.stanford.edu/~boyd/papers/graph_dcp.html.

ACKNOWLEDGEMENTS

AUTHOR CONTRIBUTIONS

Both authors contributed to the theoretical analysis and algorithm development. T. H. implemented the algorithm and generated the corresponding data.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to Thomas A. Hahn or Ernest Y.-Z. Tan.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.