Advantage Distillation for Device-Independent Quantum Key Distribution

Ernest Y.-Z. Tan, Charles C.-W. Lim, and Renato Renner

Phys. Rev. Lett. **124**, 020502 — Published 16 January 2020

DOI: 10.1103/PhysRevLett.124.020502

Advantage distillation for device-independent quantum key distribution

Ernest Y.-Z. Tan,[1] Charles C.-W. Lim,[2,3] and Renato Renner[1]

[1] *Institute for Theoretical Physics, ETH Zürich, Switzerland*
[2] *Department of Electrical & Computer Engineering, National University of Singapore, Singapore*
[3] *Centre for Quantum Technologies, National University of Singapore, Singapore*

Device-independent quantum key distribution (DIQKD) offers the prospect of distributing secret keys with only minimal security assumptions, by making use of a Bell violation. However, existing DIQKD security proofs have low noise tolerances, making a proof-of-principle demonstration currently infeasible. We investigate whether the noise tolerance can be improved by using advantage distillation, which refers to using two-way communication instead of the one-way error-correction currently used in DIQKD security proofs. We derive an efficiently verifiable condition to certify that advantage distillation is secure against collective attacks in a variety of DIQKD scenarios, and use this to show that it can indeed allow higher noise tolerances, which could help to pave the way towards an experimental implementation of DIQKD.

Introduction — In quantum key distribution, the goal is to extract a key from correlations obtained by measuring quantum systems. Device-independent quantum key distribution (DIQKD) is based on the observation that when these correlations violate a Bell inequality, a secure key can be extracted even if the users' devices are not fully characterised [1–4]. In a DIQKD security proof, it is merely assumed that the devices do not signal to the adversary or other components except when foreseen by the protocol [1–3]. This differs from traditional QKD protocols [5], which are device-dependent in that they assume the devices are implementing operations within specified tolerances [6]. Implementations of such protocols have been attacked by various methods [7–9], which exploit imperfections that cause the devices to operate outside the prescribed models. By working with fewer assumptions, DIQKD can achieve secure key distribution without detailed device characterisation, which would make the systems more reliable against such attacks.

Unfortunately, there has been substantial difficulty in finding security proofs for DIQKD protocols with sufficient noise tolerance for physical implementation. One approach towards improving the tolerance is to investigate the information-reconciliation step. In QKD, the raw data of the users is not perfectly correlated, and they need to agree on a shared key using public communication. Existing DIQKD security proofs [1, 3] have used one-way error-correction protocols in this step. However, for classical key reconciliation [10, 11] and device-dependent QKD [12–17], the noise tolerance can be improved by using two-way communication, a concept that has been referred to as *advantage distillation*.

It is natural to ask whether this concept could be extended to DIQKD. However, device-dependent security proofs for advantage distillation are often based on detailed state characterisations, given by measurements that are tomographically complete or nearly so [12–17]. This is generally not available in noisy DIQKD scenarios, where there can be many states and measurements compatible with the observed statistics. While recent works [18, 19] have found upper bounds on DIQKD key rates even with two-way communication, there do not appear to be any achievability results resolving the question of whether two-way communication provides an advantage in DIQKD.

In this work, we answer this question in the affirmative, by showing that advantage distillation yields better noise tolerances than one-way error correction in several scenarios. Our key observation is that even with the limited state characterisation available in DIQKD, it is still possible to identify and bound some important parameters that can be used in a security proof. We present our results in the form of several sufficient conditions for advantage distillation to be secure, together with a semidefinite programming (SDP) method to verify when these conditions hold.

Our security proof is valid in the *collective-attacks* regime, where one assumes all states and measurements are independent and identically distributed (IID) across the protocol rounds, but the adversary Eve can store quantum side-information and perform joint measurements on her collected states [6]. Other attack models include *individual attacks*, where Eve has no quantum memory, or the most general *coherent attacks*, where the IID assumption is removed. Collective attacks can be stronger than individual attacks [15, 20], but are often no weaker than coherent attacks [3, 6]; we focus on collective attacks here.

We focus on improving the asymptotic noise-tolerance thresholds, i.e. the maximum noise at which key generation is still possible in the limit of many rounds. This is an important parameter when considering a proof-of-principle realisation of DIQKD. Our approach also yields lower bounds on the asymptotic key rate [21].

Conditions for security — Consider a DIQKD protocol between two parties Alice and Bob, where Alice has $\mathcal{X}$ possible measurements $A_0, A_1, ..., A_{\mathcal{X}-1}$, and similarly Bob has $\mathcal{Y}$ possible measurements $B_0, B_1, ..., B_{\mathcal{Y}-1}$, with A_0, B_0 taken to be binary-outcome measurements that generate a raw key. Eve holds a purification E of Al-

ice and Bob's states, and under the collective-attack assumption the states and measurements are IID, so we can focus on the single-round Alice-Bob-Eve state ρ_{ABE}. We assume that the devices do not eventually broadcast the final key through methods such as device-reuse attacks [22] or covert channels [23]. This assumption could be supported by implementing measures such as those proposed in [22–25].

Given the IID structure, parameter estimation can be performed to arbitrary accuracy, so we shall assume the outcome probabilities $\Pr_{AB|XY}(ab|xy)$ for all measurement pairs (A_x, B_y) are fully characterised in the protocol. (We will suppress subscripts for probability distributions when they are clear from context.) For convenience in the proofs, we assume a *symmetrisation* step is implemented, in which Alice generates a uniform random bit T in each round and sends it to Bob, with both parties flipping their measurement outcome if and only if $T = 1$ [26]. The bit T can be absorbed into Eve's side-information E. (This symmetrisation step can be omitted in practice; see [21] Sec. C.) After this process, the measurements A_0 and B_0 have symmetrised outcomes, in the sense $\Pr(01|00) = \Pr(10|00) = \epsilon/2$ and $\Pr(00|00) = \Pr(11|00) = (1-\epsilon)/2$ for some $\epsilon < 1/2$ [27]. Henceforth, $\Pr_{AB|XY}$ refers to the distribution after symmetrisation.

We focus on the repetition-code protocol [10, 11, 14, 15] for advantage distillation, which is based on a block of n rounds in which A_0 and B_0 were measured (we shall denote the output bitstrings as $\boldsymbol{A}_0$ and $\boldsymbol{B}_0$, and Eve's side-information across all the rounds as $\boldsymbol{E}$). Alice privately generates a uniformly random bit C, and sends the message $\boldsymbol{M} = \boldsymbol{A}_0 \oplus (C, C, ..., C)$ to Bob via a public authenticated channel. Bob replies with a bit D that expresses whether to accept the block, with $D = 1$ (accept) if and only if $\boldsymbol{B}_0 \oplus \boldsymbol{M} = (C', C', ..., C')$ for some $C' \in \mathbb{Z}_2$. If the resulting systems satisfy

$$r \coloneqq H(C|\boldsymbol{E}\boldsymbol{M}; D = 1) - H(C|C'; D = 1) > 0, \quad (1)$$

where H is the von Neumann entropy, then repeating this procedure over many n-round blocks would allow a secret key to be distilled asymptotically from the bits (C, C') in the accepted blocks [3, 28]. Excluding parameter-estimation rounds, the key rate will be $r(\epsilon^n + (1-\epsilon)^n)/n$ [14].

We derive [21] the following theorem (where $F(\rho, \sigma) = \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1$ is the root-fidelity):

Theorem 1. *For a DIQKD protocol as described above, a sufficient condition for Eq.* (1) *to hold for large n is*

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

where $\rho_{E|a_0 b_0}$ is Eve's single-round state conditioned on (A_0, B_0) being measured with outcome (a_0, b_0).

The intuition behind the proof is that if Eve sees the message value $\boldsymbol{M} = \boldsymbol{m}$, then with high probability Alice and Bob's strings have the value $\boldsymbol{A}_0\boldsymbol{B}_0 = \boldsymbol{m}\boldsymbol{m}$ or $\overline{\boldsymbol{m}\boldsymbol{m}}$ (where $\overline{\boldsymbol{m}} \coloneqq \boldsymbol{m} \oplus \boldsymbol{1}$). Hence Eve essentially has to distinguish between these two cases, which can be quantified via the fidelity $F(\rho_{\boldsymbol{E}|\boldsymbol{m}\boldsymbol{m}}, \rho_{\boldsymbol{E}|\overline{\boldsymbol{m}\boldsymbol{m}}}) = F(\rho_{E|00}, \rho_{E|11})^n$.

Eq. (2) is similar to the condition obtained in [15] for device-dependent QKD, but it is derived here without detailed state characterisation. However, it still remains to find bounds on $F(\rho_{E|00}, \rho_{E|11})$ without device-dependent assumptions. We approach this task by combining the Fuchs-van de Graaf inequality [29] with the operational interpretation of trace distance:

$$\begin{aligned} F(\rho_{E|00}, \rho_{E|11}) &\geq 1 - d(\rho_{E|00}, \rho_{E|11}) \\ &= 2(1 - P_g(\rho_{E|00}, \rho_{E|11})), \end{aligned} \quad (3)$$

where $P_g(\rho_{E|00}, \rho_{E|11})$ is Eve's maximum probability of guessing C given the E part of a c-q state $\sigma_{CE} = \sum_c (1/2)\,|c\rangle\langle c| \otimes \rho_{E|cc}$. In a DIQKD protocol as described above, $P_g(\rho_{E|00}, \rho_{E|11})$ can be viewed as Eve's guessing probability for the outcome of A_0B_0, conditioned on the outcome being 00 or 11. A DI method to bound such guessing probabilities based on the distribution $\Pr_{AB|XY}$ was described in [30], using the family of SDPs known as the NPA hierarchy [31]. We can hence apply this method to find whether Eq. (2) holds for various distributions.

However, Eq. (3) is generally not an optimal bound. We observe that if $\rho_{E|00}$ and $\rho_{E|11}$ were both assumed to be pure, then it could be replaced by a better relation,

$$F(\rho_{E|00}, \rho_{E|11})^2 = 1 - d(\rho_{E|00}, \rho_{E|11})^2. \quad (4)$$

While it seems difficult to justify such an assumption in general, we show that for 2-input 2-output protocols, one can almost replace Eq. (3) with Eq. (4) after taking a particular concave envelope [21]:

Theorem 2. *Consider a DIQKD protocol as described above, with $\mathcal{X} = \mathcal{Y} = 2$ and all measurements having binary outcomes. Denoting the set of quantum distributions with $\Pr(00|00) = \Pr(11|00)$ as $\mathcal{S}$, let f be a concave function on $\mathcal{S}$ such that for any $\gamma \in \mathcal{S}$, all states and measurements compatible with γ satisfy $f(\gamma) \geq (1-\epsilon) d(\rho_{E|00}, \rho_{E|11})^2$. Then a sufficient condition for Eq.* (1) *to hold for large n is*

$$1 - \frac{f(\Pr_{AB|XY})}{1-\epsilon} > \frac{\epsilon}{1-\epsilon}. \quad (5)$$

Currently, we do not have a method for finding an optimal concave bound on $(1-\epsilon) d(\rho_{E|00}, \rho_{E|11})^2$. However, we find a condition that is more restrictive than Eq. (5) but more tractable to verify:

Corollary 1. *Consider a DIQKD protocol as described above, with $\mathcal{X} = \mathcal{Y} = 2$ and all measurements having*

TABLE I. Noise thresholds for advantage distillation in various DIQKD scenarios. $\Pr_{\text{target}}$ is the ideal probability distribution that the devices should implement in the absence of noise, and q_t is the maximum depolarising noise such that we can show positive key rate is achievable using Theorem 1 (for rows (i)–(iii)) or Corollary 1 (for rows (iv)–(vi)). Analogously, η_t is the minimum efficiency which can be tolerated when we instead consider a limited-detection-efficiency model. Unless otherwise specified, the state used for $\Pr_{\text{target}}$ is $\left|\Phi^+\right\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

Description of $\Pr_{\text{target}}$	State and measurements for $\Pr_{\text{target}}$	q_t	η_t
(i) Achieves maximal CHSH value with the measurements A_0, A_1, B_1, B_2.	$A_0 = B_0 = Z,\ \ A_1 = X,$ $B_1 = (X+Z)/\sqrt{2},\ \ B_2 = (X-Z)/\sqrt{2}.$	6.0%	93.7%
(i) Modification of a distribution exhibiting the Hardy paradox [32, 33] for improved robustness against limited detection efficiency.	$\|\psi\rangle = \sqrt{\kappa}(\|01\rangle + \|10\rangle) + \sqrt{1-2\kappa}\,\|11\rangle$ with $\kappa = (3-\sqrt{5})/2$; the 0 outcomes correspond to projectors onto $\|a_0\rangle = \|b_0\rangle \propto \left(\sqrt{1+2\kappa} - \sqrt{1-2\kappa}\right)\|0\rangle + 2\sqrt{\kappa}\,\|1\rangle,$ $\|a_1\rangle = \|b_1\rangle \approx 0.37972\,\|0\rangle + 0.92510\,\|1\rangle,$ $\|a_2\rangle = \|b_2\rangle \approx 0.90821\,\|0\rangle + 0.41851\,\|1\rangle.$	3.2%	92.0%
(ii) Includes the Mayers-Yao self-test [34] and the CHSH measurements.	$A_0 = B_0 = Z,\ \ A_1 = B_1 = (X+Z)/\sqrt{2},$ $A_2 = B_2 = X,\ \ A_3 = B_3 = (X-Z)/\sqrt{2}.$	6.8%	92.7%
(i) Achieves maximal CHSH value with the measurements A_0, A_1, B_0, B_1.	$A_0 = Z,\ \ A_1 = X,$ $B_0 = (X+Z)/\sqrt{2},\ \ B_1 = (X-Z)/\sqrt{2}.$	7.7%	91.7%
(i) Similar to (iv), but with measurements optimised for robustness against depolarising noise.	Measurements are in the x-z plane at angles $\theta_{A_0} = 0.4187,\ \ \theta_{A_1} = 1.7900,\ \ \theta_{B_0} = 0.8636,\ \ \theta_{B_1} = 2.6340.$	9.1%	90.0%
(ii) Similar to (iv), but with states and measurements maximising CHSH violation for each value of detection efficiency η [35].	$\|\psi\rangle = \cos\Omega\,\|00\rangle + \sin\Omega\,\|11\rangle$ with $\Omega = 0.6224$; the 0 outcomes correspond to projectors onto states of the form $\cos(\theta/2)\,\|0\rangle + \sin(\theta/2)\,\|1\rangle$ with $\theta_{A_0} = -\theta_{B_0} = -0.35923,\ \ \theta_{A_1} = -\theta_{B_1} = 1.1538.$	7.3%	89.1%

binary outcomes. Then a sufficient condition for Eq. (1) *to hold for large n is*

$$1 - d(\rho_{E|00}, \rho_{E|11}) > \frac{\epsilon}{1-\epsilon}. \tag{6}$$

As before, we can bound $d(\rho_{E|00}, \rho_{E|11})$ by using the NPA hierarchy. Effectively, Corollary 1 improves over the combination of Theorem 1 and Eq. (3) by replacing $\left(1 - d(\rho_{E|00}, \rho_{E|11})\right)^2$ with $1 - d(\rho_{E|00}, \rho_{E|11})$.

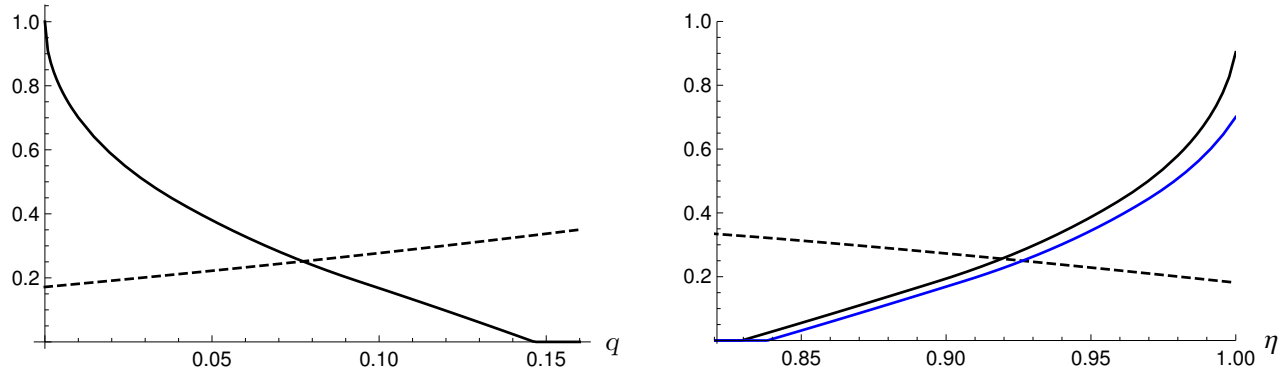
Noise thresholds — Using this method, we study the effects of two possible noise models for binary-outcome distributions. The first is depolarising noise parametrised by $q \in [0, 1/2]$:

$$\Pr(ab|xy) = (1-2q)\Pr_{\text{target}}(ab|xy) + q/2, \tag{7}$$

where $\Pr_{\text{target}}$ is some ideal target distribution [36]. The second noise model is limited detection efficiency parametrised by $\eta \in [0, 1]$, where all outcomes are subjected to independent Z-channels that flip 1 to 0 with probability $1 - \eta$. This is a standard model for photonic setups where photon loss or non-detection occurs with probability $1 - \eta$, with such events assigned to outcome 0 [1]. (η is an effective parameter describing all such losses. Given more detailed noise models [37], our method can be applied to the resulting distributions for more precise results.)

In Table I, we present a selection of our results (see [21] for the full list). Additionally, in Fig. 1 we plot both sides of Eq. (6) for row (iv) of the table. From the table, we see that appropriate choices of $\Pr_{\text{target}}$ can tolerate depolarising noise of $q_t \approx 9.1\%$ or detection efficiencies of $\eta_t \approx 89.1\%$. This indeed outperforms the DIQKD protocol in [1] based on one-way error correction, which can tolerate $q_t \approx 7.1\%$ or $\eta_t \approx 92.4\%$ (or $\eta_t \approx 90.7\%$ for a modified version where the state and measurements A_0, A_1, B_1, B_2 are optimised to maximise the CHSH value for each value of η [35], and B_0 is then separately optimised to be maximally correlated to A_0).

We observe that the DIQKD protocol in [1] uses essentially the same $\Pr_{\text{target}}$ as row (i) in Table I. This is not a 2-input 2-output scenario, and so the noise thresholds we can prove for that specific setup are somewhat worse. However, row (iv) is in fact the same scenario with one measurement *omitted*, making it a 2-input 2-output scenario, thus we could use Corollary 1 to show that advantage distillation in this scenario can surpass the thresholds in [1]. Hence we have shown that for the scenario in [1], advantage distillation achieves a higher noise tol-



(a) Depolarising noise

(b) Limited detection efficiency

FIG. 1. (Colour online) Left- and right-hand sides of Eq. (6), shown as solid and dashed curves respectively, for a DIQKD scenario where the target distribution attains maximum CHSH violation in the absence of noise. Plot (a) shows the effect of depolarising noise q, while in plot (b) a small amount of depolarising noise is applied ($q = 0.1\%$ for the black curve, $q = 1\%$ for the blue curve) followed by a limited-detection-efficiency noise model with efficiency η. In plots (a) and (b), the solid and dashed curves intersect at $q_t \approx 7.7\%$ and $\eta_t \approx 91.7\%$ (black), 92.6% (blue) respectively, which yield the threshold values such that we can show positive key rate is achievable via Corollary 1. The solid curves reach zero at the same noise values as where the CHSH violation becomes zero.

erance even while ignoring one measurement. This is particularly surprising since the key-generating measurements in row (iv) are not perfectly correlated. In fact, if the proof in [1] were applied to this scenario [38], it would only tolerate noise up to $q_t \approx 3.1\%$.

In Table I, the noise thresholds for scenarios with more than 2 inputs are generally worse, because for such scenarios we cannot apply Corollary 1. The best results we have for such cases are listed in rows (ii) and (iii). It would be of interest to find a way to overcome this issue, perhaps by finding more direct bounds on $F(\rho_{E|00}, \rho_{E|11})$, or further study of when the analysis can be reduced to states satisfying Eq. (4) (see [21] Sec. F for an example where the states are not pure).

Conclusion and outlook — In summary, we have found that by using advantage distillation, the noise thresholds for DIQKD with one-way error correction can be surpassed. Specifically, advantage distillation is secure against collective attacks up to depolarising-noise values of $q \approx 9.1\%$ or detection efficiencies of $\eta \approx 89.1\%$, which exceeds the best-known noise thresholds of $q \approx 7.1\%$ and $\eta \approx 90.7\%$ respectively for DIQKD with one-way error correction.

Currently, we require large block sizes n to certify positive key rates. However, small block sizes are sufficient for reasonable asymptotic key rates in the device-dependent case [14]. Tighter bounds on $F(\rho_{E|00}, \rho_{E|11})$ should give similar results in DIQKD, hence this would be an important next step. Alternatively, one could analyse the finite-key security [3, 39, 40]. Since our approach yields explicit bounds [21] on the entropies in Eq. (1), it could in principle be extended to a finite-size security proof against collective attacks by using the quantum asymptotic equipartition property [41], following the approach in [40]. However, this approach is likely to require a large number of rounds to achieve positive key rates, which would pose a challenge for practical implementation.

Another significant goal would be extending our results to non-IID scenarios. We conjecture that allowing coherent attacks will not change the asymptotic key rates, as was the case for various device-dependent QKD and DIQKD protocols [3, 6]. To support this, we observe that if the measurements have an IID tensor-product structure, then the analysis of any permutation-symmetric protocol can be asymptotically reduced to the IID case using de Finetti theorems [14], assuming the system dimensions are bounded. Hence any attack that can be modelled by simply using non-IID states (with IID measurements) cannot yield an asymptotic advantage over collective attacks (see [21] Sec. E). To find a security proof for non-IID measurements, the entropy accumulation theorem [3, 42] or a new type of de Finetti theorem may be required.

Finally, an open question in information theory is the existence of *bound information*, referring to correlations which require secret bits to be produced but from which no secret key can be extracted [17, 43]. There is a simple analogue to this in the context of DIQKD, namely whether there exist correlations which violate Bell inequalities but cannot be distilled into a secret key in a DI setting. Our results have a gap between the noise thresholds at which we can no longer prove the protocol's security and the thresholds at which the Bell violation becomes zero (see also [21] Sec. E, where we outline a potential attack for $q \gtrsim 12.8\%$ if the users only

measure ϵ and the CHSH value). It would be of interest to find whether this gap can be closed.

We thank Jean-Daniel Bancal, Srijita Kundu, Joseph Renes, Valerio Scarani, Le Phuc Thinh and Marco Tomamichel for helpful discussions. E. Y.-Z. Tan and R. Renner were funded by the Swiss National Science Foundation via the National Center for Competence in Research for Quantum Science and Technology (QSIT), and by the Air Force Office of Scientific Research (AFOSR) via grant FA9550-19-1-0202. C. C.-W. Lim acknowledges support from the National Research Foundation (Singapore), the Ministry of Education (Singapore), the National University of Singapore, and the Asian Office of Aerospace Research and Development. Computations were performed with the NPAHierarchy function in QETLAB [44], using the CVX package [45, 46] with solver SDPT3.

[1] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).
[2] V. Scarani, Acta Physica Slovaca **62**, 347 (2012).
[3] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nat. Commun. **9**, 459 (2018).
[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] C. H. Bennett and G. Brassard, in *Proceedings of International Conference on Computers, Systems and Signal Processing* (1984) p. 175.
[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[7] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).
[8] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).
[9] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, IEEE Journal of Selected Topics in Quantum Electronics **21**, 168 (2015).
[10] U. M. Maurer, IEEE T. Inform. Theory **39**, 733 (1993).
[11] S. Wolf, *Information-Theoretically and Computationally Secure Key Agreement in Cryptography*, Ph.D. thesis, ETH Zürich (1999).
[12] D. Gottesman and Hoi-Kwong Lo, IEEE T. Inform. Theory **49**, 457 (2003).
[13] H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002).
[14] R. Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, ETH Zürich (2005).
[15] J. Bae and A. Acín, Phys. Rev. A **75**, 012334 (2007).
[16] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, Phys. Rev. A **76**, 032312 (2007).
[17] S. Khatri and N. Lütkenhaus, Phys. Rev. A **95**, 042320 (2017).
[18] E. Kaur, M. M. Wilde, and A. Winter, arXiv:1810.05627 [quant-ph] (2018), arXiv: 1810.05627.
[19] M. Winczewski, T. Das, and K. Horodecki, arXiv:1903.12154 [quant-ph] (2019), arXiv: 1903.12154.
[20] N. Gisin and S. Wolf, Phys. Rev. Lett. **83**, 4200 (1999).
[21] See Supplemental Material, which includes Refs. [47–57].
[22] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. Lett. **110**, 010503 (2013).
[23] M. Curty and H.-K. Lo, npj Quantum Inf. **5**, 1 (2019).
[24] M. McKague and L. Sheridan, in *Information Theoretic Security*, Lecture Notes in Computer Science, edited by C. Padró (Springer International Publishing, 2014) pp. 122–141.
[25] F. G. Lacerda, J. M. Renes, and R. Renner, J. Cryptol. **32**, 1071 (2019).
[26] In this work, we take the symmetrisation step to be applied to all measurements, which is possible because we focus on scenarios where all measurements have binary outcomes. In principle, one could instead symmetrise the key-generating measurements only.
[27] If $\epsilon > 1/2$, simply swap Bob's outcome labels.
[28] I. Devetak and A. Winter, P. Roy. Soc. A: Math Phy. **461**, 207 (2005).
[29] C. A. Fuchs and J. van de Graaf, IEEE T. Inform. Theory **45**, 1216 (1999).
[30] L. P. Thinh, G. de la Torre, J.-D. Bancal, S. Pironio, and V. Scarani, New Journal of Physics **18**, 035007 (2016).
[31] M. Navascués, S. Pironio, and A. Acín, New J. Phys. **10**, 073013 (2008).
[32] L. Hardy, Phys. Rev. Lett. **71**, 1665 (1993).
[33] R. Rabelo, Y. Z. Law, and V. Scarani, Phys. Rev. Lett. **109**, 180401 (2012).
[34] D. Mayers and A. Yao, Quantum Inf. Comput. **4**, 273 (2004).
[35] P. H. Eberhard, Phys. Rev. A **47**, R747 (1993).
[36] Here $\Pr(ab|xy)$ refers to the probabilities before symmetrisation, though if $\Pr_{\text{target}}$ already has symmetrised outcomes then symmetrising $\Pr(ab|xy)$ has no further effect.
[37] V. Caprara Vivoli, P. Sekatski, J.-D. Bancal, C. C. W. Lim, B. G. Christensen, A. Martin, R. T. Thew, H. Zbinden, N. Gisin, and N. Sangouard, Phys. Rev. A **91**, 012107 (2015).
[38] By replacing the error-correction term $H(A_0|B_0) = h_2(q)$ with $H(A_0|B_0) = h_2(\epsilon)$.
[39] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 1 (2012).
[40] G. Murta, S. B. van Dam, J. Ribeiro, R. Hanson, and S. Wehner, Quantum Science and Technology **4**, 035011 (2019).
[41] M. Tomamichel, R. Colbeck, and R. Renner, IEEE T. Inform. Theory **55**, 5840 (2009).
[42] F. Dupuis, O. Fawzi, and R. Renner, arXiv:1607.01796 (2016).
[43] N. Gisin and S. Wolf, in *Advances in Cryptology — CRYPTO 2000*, edited by M. Bellare (Springer Berlin Heidelberg, Berlin, Heidelberg, 2000) pp. 482–500.
[44] N. Johnston, "QETLAB: A MATLAB toolbox for quantum entanglement, version 0.9," `http://qetlab.com` (2016).
[45] M. Grant and S. Boyd, "CVX: Matlab Software for Disciplined Convex Programming, version 2.1," `http://cvxr.com/cvx` (2014).
[46] M. Grant and S. Boyd, in *Recent Advances in Learning and Control*, Lecture Notes in Control and Information Sciences, edited by V. Blondel, S. Boyd, and H. Kimura (Springer-Verlag Limited, 2008) pp. 95–110, `http://stanford.edu/~boyd/graph_dcp.html`.
[47] A. Winter, Commun. Math. Phys. **347**, 291 (2016).
[48] W. Roga, M. Fannes, and K. Życzkowski, Phys. Rev.

Lett. **105**, 040505 (2010).
[49] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).
[50] M. Tomamichel and A. Leverrier, Quantum **1**, 14 (2017).
[51] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, Phys. Rev. Lett. **113**, 040401 (2014).
[52] C. A. Fuchs and C. M. Caves, Open Syst. Inf. Dyn. **3**, 345 (1995).
[53] N. Gisin, arXiv:quant-ph/0702021v2 (2007).
[54] O. Andersson, P. Badziąg, I. Bengtsson, I. Dumitru, and A. Cabello, Phys. Rev. A **96**, 032119 (2017).
[55] V. Scarani and R. Renner, in *Theory of Quantum Computation, Communication, and Cryptography*, edited by Y. Kawano and M. Mosca (Springer Berlin Heidelberg, Berlin, Heidelberg, 2008) pp. 83–95.
[56] M. Hübner, Phys. Lett. A **163**, 239 (1992).
[57] J. Briët and P. Harremoës, Phys. Rev. A **79**, 052311 (2009).