Upper bounds on device-independent quantum key distribution rates in static and dynamic scenarios

Eneet Kaur,[1] Karol Horodecki,[2,3] and Siddhartha Das[4]

[1]Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
[2]National Quantum Information Centre in Gdańsk, and and Institute of Informatics, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-952 Gdańsk, Poland
[3]International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, 80-308 Gdańsk, Poland
[4]Centre for Quantum Information & Communication (QuIC), Université libre de Bruxelles, Brussels, B-1050, Belgium

Objectives

In this work, we develop upper bounds for key rates for device-independent quantum key distribution (DI-QKD) protocols and devices. We show that the convex hull of the currently known bounds is a tighter upper bound on the device-independent key rates of standard CHSH-based protocol. We further provide a tighter upper bound based on relative entropy based bound for DI-QKD key rates achievable by any protocol applied to the CHSH-based device. Next, we show that the device-independent private capacity for the CHSH based protocols on depolarizing and erasure channels is limited by the secret key capacity of dephasing channels.

Result 1 - Convex bound

We define cc-squashed entanglement as:

$$E^{cc}_{sq}(\rho_{AB}, \mathrm{M}) := \inf_{\Lambda_E} I(A:B|E)_{\mathrm{M}\otimes\Lambda_E(\psi^\rho)},$$

where ρ_{AB} is a quantum state, $\mathrm{M} := M^{\hat{x}}_a \otimes M^{\hat{y}}_a$ corresponding to measurements on Alice's and Bob's system, and Λ_E is a quantum channel on the E system. We define the reduced cc-squashed entanglement as:

$$E^{cc}_{sq,dev}(\rho_{AB}, \mathcal{M}(\hat{x},\hat{y})) := \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})} E^{cc}_{sq}(\sigma_{AB}, \mathcal{M}(\hat{x},\hat{y})),$$

where the infimum is over all quantum strategies $(\sigma, \mathcal{N})$ which yield the same probability distribution $p(a,b|x,y)$. Then from [1],

$$K^{iid,(\hat{x},\hat{y})}_{DI,dev}(\rho,\mathcal{M}) \leq E^{cc}_{sq,dev}(\rho,\mathcal{M}), \tag{1}$$

where $K^{iid,(\hat{x},\hat{y})}_{DI,dev}(\rho,\mathcal{M})$ is the standard device independent key rate of the distribution of quantum strategy $(\rho,\mathcal{M})$. For these protocols, we assume that the key generation rounds involve the measurements $M^{\hat{x}}_a \otimes M^{\hat{y}}_b$. By proving the **convexity of the reduced cc-squashed entanglement**, we conclude that the convex hull of the upper bounds proved in [1, 2], is also an upper bound on device independent key rate.

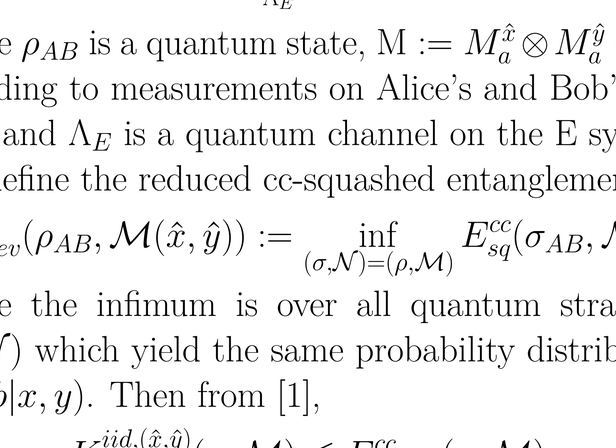

Figure 1: In this figure, we show the plots for standard device-independent CHSH protocol obtained in Refs. [1], [2], and the upper bound obtained in this work, which is the convex hull of the former bounds, depicted in green.

Result 2 - Splitting bound

The maximal DI-QKD rate $K^{iid}_{DI}(\rho, M)$ of a device (ρ, M) is upper bounded as

$$K^{iid}_{DI,dev}(\rho,M) \leq (1-p) \inf_{(\sigma^{\mathrm{NL}},\mathcal{N})=(\rho^{\mathrm{NL}},\mathcal{M})} E_R(\sigma^{NL}) + p \inf_{(\sigma^{\mathrm{L}},\mathcal{N})=(\rho^{\mathrm{L}},\mathcal{M})} E_R(\sigma^{L}), \tag{2}$$

where $E_R(\rho)$ is the relative entropy of entanglement of the bipartite state ρ,

$$\rho = (1-p)\rho^{\mathrm{NL}} + p\rho^{\mathrm{L}} \tag{3}$$

such that $\sigma^{\mathrm{L}}, \rho^{\mathrm{L}} \in$ LHV and $\sigma^{\mathrm{NL}}, \rho^{\mathrm{NL}} \notin$ LHV. Here, LHV denotes the set of states having a local hidden variable model.

A consequence of the above theorem is the following result: The maximal DI-QKD rate $K^{iid}_{DI,dev}(\rho,M)$ of a device (ρ,M) under CHSH protocol $\mathcal{P}_{CHSH}$, is upper bounded as

$$K^{iid}_{DI,dev}(\rho,M) \leq (1-p) \inf_{(\sigma^{\mathrm{bl}},\mathcal{N})=(\rho^{\mathrm{bnl}},\mathcal{M})} E_R(\sigma^{\mathrm{bnl}}), \tag{4}$$

where $\rho = (1-p)\rho^{\mathrm{bnl}} + p\rho^{\mathrm{bl}}$ and ρ^{bl} denotes state satisfying CHSH inequality and ρ^{bnl} denotes state violating CHSH inequality.

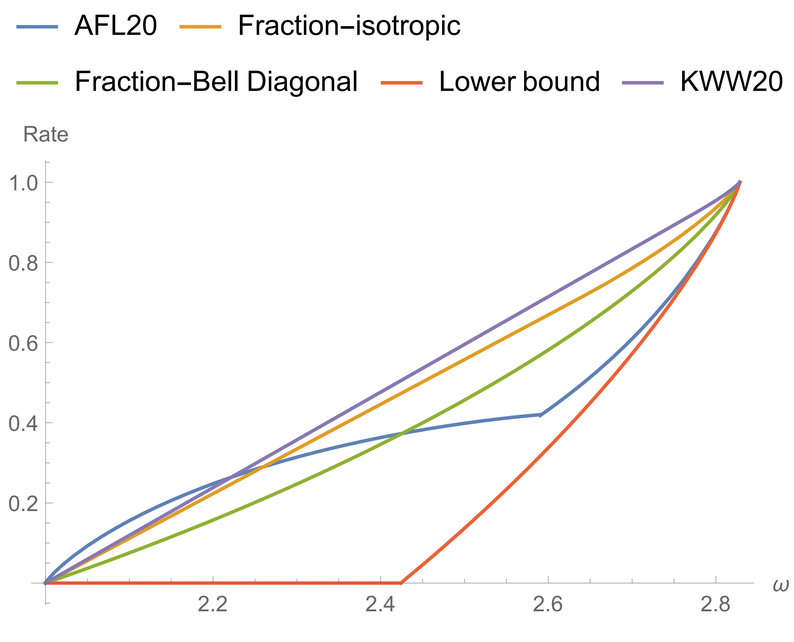

Figure 2: In this plot, we depict the bounds on the amount of DI key that can be obtained from a CHSH-based device. The yellow line and green line corresponds to two upper bounds obtained from (4). The blue line corresponds to the bound obtained in Appendix B of [1]. The purple line corresponds to the bound obtained in [3]. The red line corresponds to the lower bound.

Result 3 - DI-QKD capacity bound

The DI-QKD capacity of the device $(\mathrm{id}\otimes\Lambda, \rho, M)$ under the assumption of its iid uses assisted with i-way communication between allies outside the device and j-way communication between the input-output rounds within the device, is given by [4]

$$P_i^{IDI_j}(\mathrm{id}\otimes\Lambda,\rho,M) := \inf_{\varepsilon>0} \limsup_{n\to\infty} \mu_{i,n}^{IDI_j,\varepsilon}(\mathrm{id}\otimes\Lambda,\rho,M), \tag{5}$$

where $\mu_{i,n}^{IDI_j,\varepsilon}(\mathrm{id}\otimes\Lambda,\rho,M)$ is the maximum key rate optimized over all viable privacy protocols $\hat{\mathcal{P}}$ over the *iid* uses of device, and also includes a minimization over the possible *iid* devices IDI_j that are compatible with the honest device. For the class of channels Λ that are simulable via LOCC and the respective Choi states as resource, the following upper bounds hold:

$$P_i^{IDI_j}(\mathrm{id}\otimes\Lambda,\rho,M) \leq \inf_{\substack{(\mathrm{id}\otimes\Lambda',\sigma,N)\in IDI_j \\ (\mathrm{id}\otimes\Lambda',\sigma,N)=(\mathrm{id}\otimes\Lambda,\rho,M)}} E_R(\Phi^{\Lambda'}), \tag{6}$$

where $\Phi^{\Lambda'} := \Lambda'(\Phi^+)$ is the Choi state of the channel Λ, with $\Phi^+_{A'B} := \frac{1}{d}\sum_{i,j=0}^{d-1} |i,i\rangle\langle j,j|_{A'B}$ denoting a maximally entangled state of Schmidt rank $d = \min\{|A'|, |B|\}$. For some well known channels, we plot the upper bounds in Fig 3.

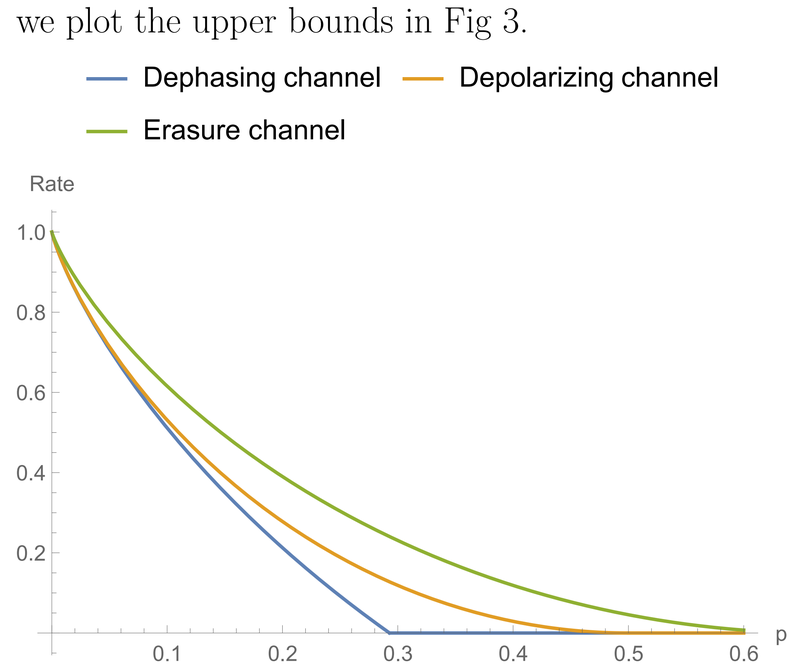

Figure 3: In the above figure, we plot upper bounds on the device-dependent QKD capacities of depolarizing channel (yellow line), dephasing channel (blue line) and erasure channel (green line). We notice that the upper bounds for erasure and dephasing channels are achievable device-dependent QKD rates (capacities). We then notice that for the CHSH protocols, the upper bounds on the DI-QKD capacities of channels is limited by the device-dependent QKD capacity of dephasing channels.

Acknowledgments

Part of this work is performed at the Institute for Quantum Computing (IQC), University of Waterloo, which is supported by Innovation, Science and Economic Development Canada. EK acknowledges support by NSERC under the Discovery Grants Program, Grant No. 341495.
This work is part of the ICTQT IRAP project of FNP. The"International Centre for Theory of Quantum Technologies' project (contract no. 2018/MAB/5) is carried out within the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union from the funds of the Smart Growth Operational Programme, axis IV: Increasing the research potential (Measure 4.3). KH thanks Anubhav Chaturvedi for discussion and Tamoghna Das for valuable insight in the topic of upper bounds on device-independent quantum key distribution rates.
SD acknowledges Individual Fellowships at Université libre de Bruxelles; this project receives funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 801505.

References

[1] Arnon-Friedman, Rotem and Leditzky, Felix. Upper bounds on device-independent quantum key distribution rates and a revised peres conjecture. arXiv:1810.05627 (2020)

[2] Farkas, Máté and Balanzó-Juandó, Maria and Łukanowski, Karol and Kołodyński, Jan and Acín, Antonio. Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols. arXiv:2103.02639.

[3] Kaur, Eneet and Wilde, Mark M. and Winter, Andreas. Fundamental limits on key rates in device-independent quantum key distribution. New Journal of Physics, vol. 22, page 023039, February 2020.

[4] Matthias Christandl, Roberto Ferrara, Karol Horodecki. Upper bounds on device-independent quantum key distribution. Phys. Rev. Lett. 126, 160501 (2021).