Fidelity Bounds for Device-Independent Advantage Distillation

Thomas A. Hahn, Ernest Y.-Z. Tan
thomas.hahn@weizmann.ac.il, ernestt@itp.phys.ethz.ch

ETH zürich

Summary of Key Results

- We develop an SDP hierarchy to verify a sufficient security condition for DIQKD with advantage distillation. (Specifically, it is known that a secret key can be generated for the repetition code protocol if

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

  Our approach yields tight bounds on this fidelity quantity, in contrast to previous approaches which were not optimal.)

- We apply our approach to several DIQKD scenarios, and compare the resulting noise tolerances to previous results.

- In light of our findings, we conjecture a necessary condition for key distillation, to complement the sufficient condition.

Scenarios

- We focus on the depolarizing noise model, i.e. the observed distribution is given by

$$(1-2q)\,\mathrm{Pr}_{\mathrm{target}}(ab|xy) + q/2, q \in [0, 1/2] \ .$$

- We considered the following 3 set-ups

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

Conclusion and Outlook

- Significantly tighter fidelity bounds than previous results.
- Results from (c) strongly suggest sufficient condition is not necessary.
- Alternative approach would be to consider the Quantum Chernoff Bound:

$$Q(\rho,\sigma) \coloneqq \min_{0<s<1} \mathrm{Tr}\left[\rho^s \sigma^{1-s}\right] \ .$$

- Algorithm can also be used to compute one-way DIQKD keyrates.

Results: Lower Bounds on the Fidelity

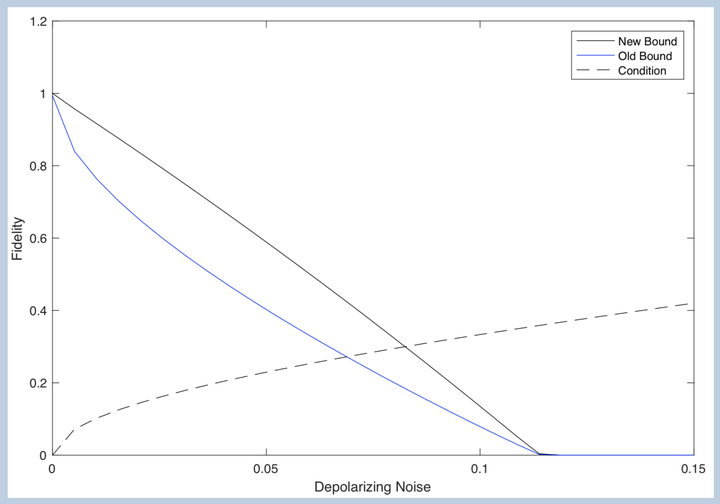
To find optimal bounds for the sufficient condition, we need to minimize the fidelity for a given observed distribution, i.e.

$$\begin{aligned} \inf \quad & \mathrm{F}(\rho_{E|00}, \rho_{E|11}) \\ \text{s.t.} \quad & \mathrm{Pr}(ab|xy)_\rho = \mathbf{p} \ . \end{aligned} \tag{1}$$

Since there exists a fidelity-invariant measurement that Eve can conduct, this minimization can be written as

$$\begin{aligned} \inf_{\mathrm{Pr}(i),\mathbf{p^i}} \quad & \sum_i \frac{\sqrt{\mathrm{Pr}(00|00i)\,\mathrm{Pr}(11|00i)}}{\mathrm{Pr}(00|00)}\,\mathrm{Pr}(i) \\ \text{s.t.} \quad & \sum_i \mathrm{Pr}(i)\mathbf{p^i} = \mathbf{p} \\ & \mathbf{p}^i \in \mathcal{Q}_{\mathcal{X},\mathcal{Y}} \\ & \mathrm{Pr}(i) \in \mathcal{P}(\mathcal{I}) \ , \end{aligned} \tag{2}$$

We develop an algorithm to solve this, via a generalization of the SDP reduction used in [arXiv:1905.09117].



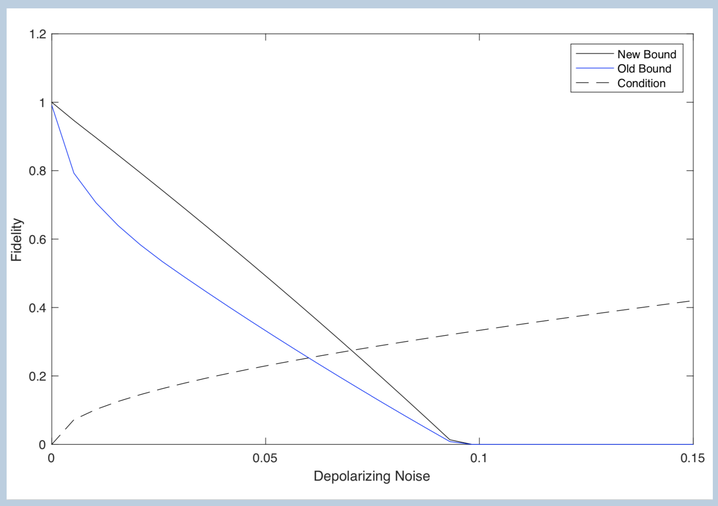


Figure 1: Fidelity bounds as a function of depolarizing noise for the first two scenarios (described in Scenarios). The blue and black solid lines respectively represent the fidelity bounds derived via the previous approach (based on the Fuchs-van de Graaf inequality) and our new algorithm. It can be 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 sufficient condition. The thresholds given by our approach (i.e. the black solid lines) in these scenarios are $q \approx 8.3\%$ and $q \approx 7.0\%$ (from left to right).

For case (c), there exists an alternative condition that does not rely on the fidelity and gives better noise tolerances. This, however, strongly implies that the sufficient condition is in fact not necessary.

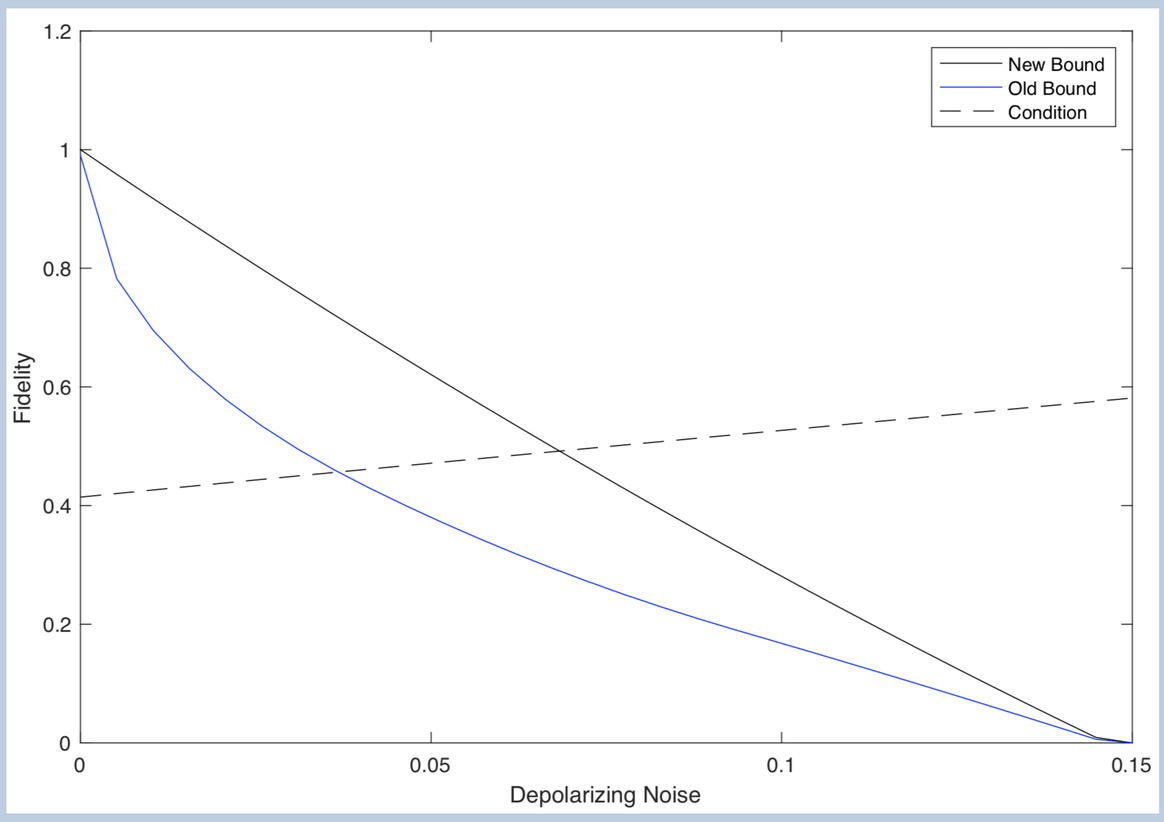


Figure 2: Fidelity bounds as a function of depolarizing noise for the last scenario (described in Scenarios). The thresholds given by our approach (i.e. the black solid lines) is $q \approx 6.7\%$.

Results: Conjectured Necessary Condition

- Assumption: $\mathrm{F}(\rho_{E|01}, \rho_{E|10}) = 0$
- Necessary Condition: $\mathrm{F}(\rho_{E|00}, \rho_{E|11}) > \frac{\epsilon}{(1-\epsilon)}$ must hold.