Computing secure key rates for quantum cryptography with untrusted devices

Based on: arXiv:1908.11372

E. Y.-Z. Tan, R. Schwonnek, K. Tong Goh,
I. W. Primaatmaja, and Charles C.-W. Lim

Qlunch 3/9/21
Marco Avesani

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Previously on this show…

Numerical key rates for device-dependent QKD

P. Coles, et al. Numerical approach for unstructured quantum key distribution. Nat Commun 7, 11712 (2016). https://doi.org/10.1038/ncomms11712

Pro:

- Toolbox for calculation of SKR of general (trusted) QKD protocols
- Fast: single SDP

Cons:

- Valid only for device-dependent QKD
- Asymptotic security

Tight finite-key bounds for Device-Independent QKD

R. Arnon-Friedman, et al. Practical device-independent quantum cryptography via entropy accumulation. Nat Commun 9, 459 (2018).

Pro:

- Works for DI-QKD
- Tight finite-size bounds

Cons:

- Needs analytic kung-fu to find the right min-tradeoff function
- Hard for protocols without symmetries

An interesting blend

Numerical key rates for device-dependent QKD

P. Coles, et al. Numerical approach for unstructured quantum key distribution. Nat Commun 7, 11712 (2016). https://doi.org/10.1038/ncomms11712

Tight finite-key bounds for Device-Independent QKD

R. Arnon-Friedman, et al. Practical device-independent quantum cryptography via entropy accumulation. Nat Commun 9, 459 (2018).

Computing secure key rates for quantum cryptography with untrusted devices

arXiv:1908.11372

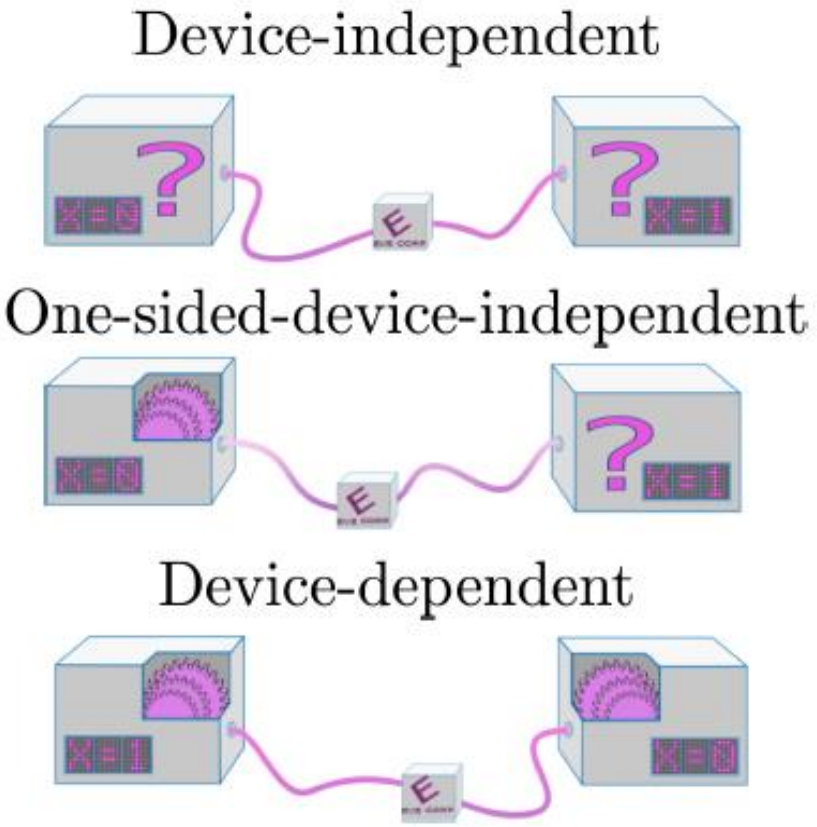
An interesting blend

Computing secure key rates for quantum cryptography with untrusted devices

A single framework to compute QKD SKR with: Device-Independent, 1sDI, Device-Dependent protocols

Key points:

- General structure for tackling all QKD protocols
- More trust on the devices is simply added by adding constraints
- Almost tight bounds (except for Golden-Thompson)
- Reduces to single SDP for DD protocols
- Exploits NPA for DI
- Compatible with EAT framework for tight finite-size analysis



A step back: Security of QKD

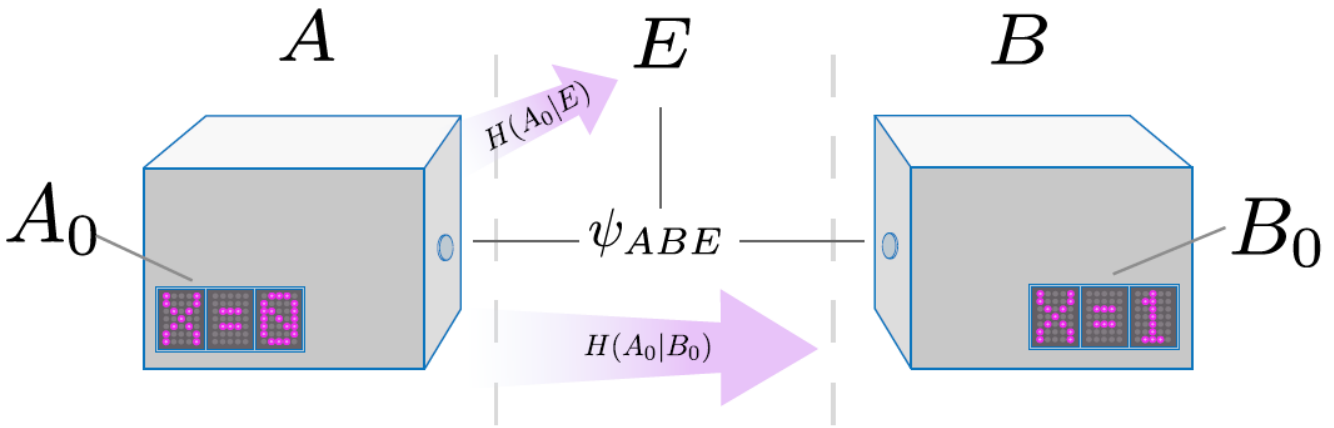
For protocols with one-way error correction the (asymptotic) Secure Key Rate is given by the Devetak-Winter formula:

$$r_\infty = H(A_0|E)_{\psi_{ABE}} - H(A_0|B_0)_{\psi_{ABE}}$$

$$H(\rho) = -Tr[\rho \log_2 \rho]$$

$$H(X|Y) = H(\rho_{XY}) - H(\rho_Y)$$

A_i and B_i are the measurement performed by Alice and Bob



Alice and Bob share an unknown quantum state ρ_{AB}, which is in general correlated with Eve , which is taken as the purifying system of AB, such as $|\psi_{ABE}\rangle$ is pure

The objective is to estimate r_∞ over all the ρ_{AB} compatible with the measurement of Alice and Bob

I. Devetak and A. Winter, P. Roy. Soc. A: Math Phy. 461, 207 (2005).

A step back: Security of QKD

For protocols with one-way error correction the (asymptotic) Secure Key Rate is given by the Devetak-Winter formula:

$$r_\infty = H(A_0|E)_{\psi_{ABE}} - H(A_0|B_0)_{\psi_{ABE}}$$

Eve's uncertainty about Alice's outcome.
Linked to the **Privacy Amplification**.
Hard to calculate because we don't have access to Eve's system

Bob's uncertainty about Alice's outcome.
Linked to **the Error Correction**.
Can be calculated directly from the data

$$r_\infty = \min_{\rho_{AB} \in C} [\, H(A_0|E)_{\psi_{ABE}})] \; - H(A_0|B_0)_{\psi_{ABE}}$$

I. Devetak and A. Winter, P. Roy. Soc. A: Math Phy. 461, 207 (2005).

A step back: Security of QKD

For protocols with one-way error correction the (asymptotic) Secure Key Rate is given by the Devetak-Winter formula:

$$r_\infty = H(A_0|E)_{\psi_{ABE}} - H(A_0|B_0)_{\psi_{ABE}}$$

Eve's uncertainty about Alice's outcome.
Linked to the **Privacy Amplification**.
Hard to calculate because we don't have access to Eve's system

Bob's uncertainty about Alice's outcome.
Linked to **the Error Correction**.
Can be calculated directly from the data

$$r_\infty = \min_{\rho_{AB} \in C} [\, H(A_0|E)_{\psi_{ABE}})] \; - H(A_0|B_0)_{\psi_{ABE}}$$

Hard! Need to optimize over a continuous set of quantum states!

I. Devetak and A. Winter, P. Roy. Soc. A: Math Phy. 461, 207 (2005).

The Waterloo approach

The problem is :

$$\inf H(A_0|E)$$
$$\text{s.th. } \langle L_j \rangle_{\rho_{AB}} = l_j,$$

$$L_j = \sum_{abxy} c^{(j)}_{abxy} P_{a|x} \otimes P_{b|y} \qquad l_j = \sum_{abxy} c^{(j)}_{abxy} \Pr(ab|xy)$$

In [1] the first solution to the problem

$$\max_{\vec{\lambda}} \left(-\left| f\left(\vec{\lambda}, \vec{\mathrm{L}}, A_0\right) \right| - \vec{\lambda} \cdot \vec{l} \right)$$

Unconstrained optimization problem on real parameters $\vec{\lambda}$

[1] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Nat. Commun. 7, 11712 (2016).

The Waterloo approach

$$\max_{\vec{\lambda}}\left(-\left|f\left(\vec{\lambda}, \vec{\mathrm{L}}, A_0\right)\right| - \vec{\lambda}\cdot\vec{l}\right)$$

$$L_j = \sum_{abxy} c^{(j)}_{abxy} P_{a|x} \otimes P_{b|y} \qquad l_j = \sum_{abxy} c^{(j)}_{abxy} \Pr(ab|xy)$$

Limitations:

- **The problem depends explicitly from the measurement operators on Alice and Bob side -> cannot generalize to DI-QKD where the measurement are unknown**
- **IID assumption, asymptotic security from identical rounds**
- **Can use AEP + de Finetti / postselection to promote to general attacks (loose bounds)**
- **Still not an SDP (fixed in later works)**

[1] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Nat. Commun. 7, 11712 (2016).

The Singapore way

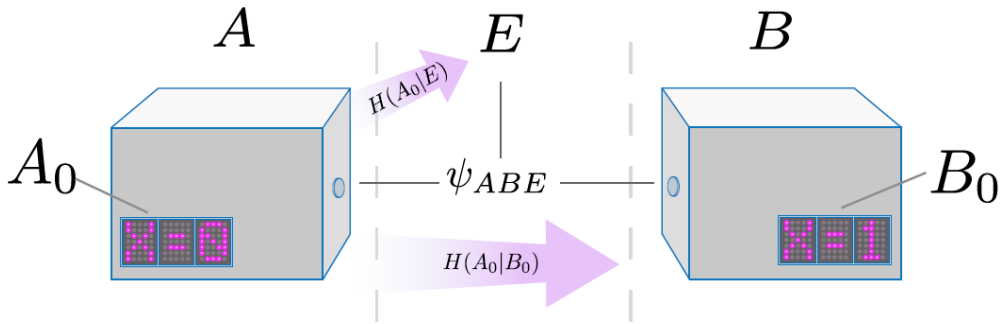
Again the problem we want to solve is

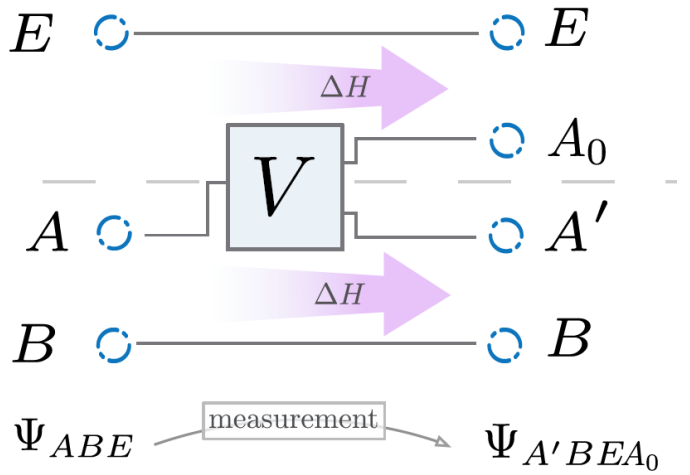
$$\inf H(A_0|E)$$
$$\text{s.th. } \langle L_j \rangle_{\rho_{AB}} = l_j,$$

$$L_j = \sum_{abxy} c^{(j)}_{abxy} P_{a|x} \otimes P_{b|y} \qquad l_j = \sum_{abxy} c^{(j)}_{abxy} \Pr(ab|xy)$$

The idea is to **map** it to a **different but equivalent problem** which is easier to solve

Entropy Production

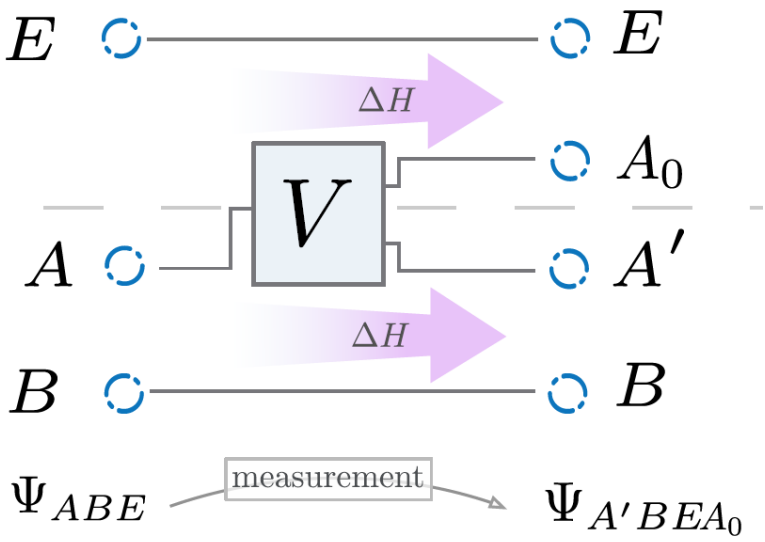




arXiv:1908.11372

Entropy Production

We consider the problem as thermodynamic system



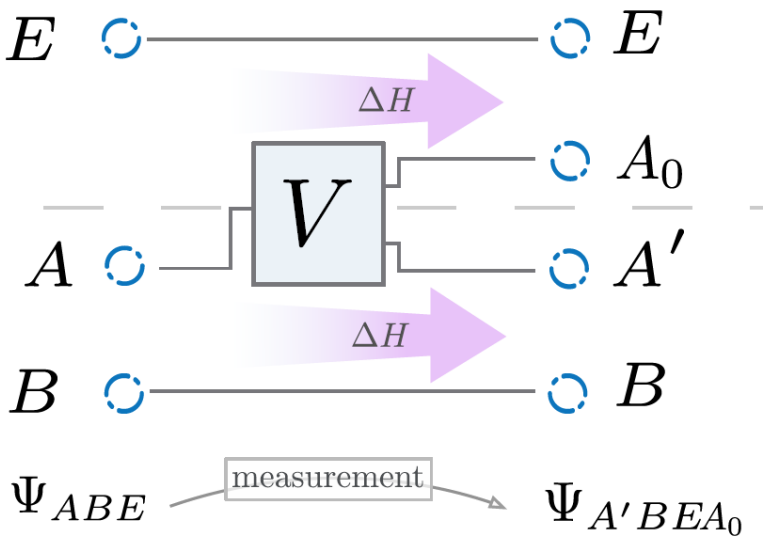
On the left the system before Alice measurement, on the right after

The measurement is a **quantum to classical channel** to a classical register A_0

This channel can be described as an **isometry V to an extended** system A_0A' that maps **the pure state ψ_{ABE} to the pure $\psi_{A'BEA_0}$**

Entropy Production

We consider the problem as thermodynamic system



On the left the system before Alice measurement, on the right after

The measurement is a **quantum to classical channel** to a classical register A_0

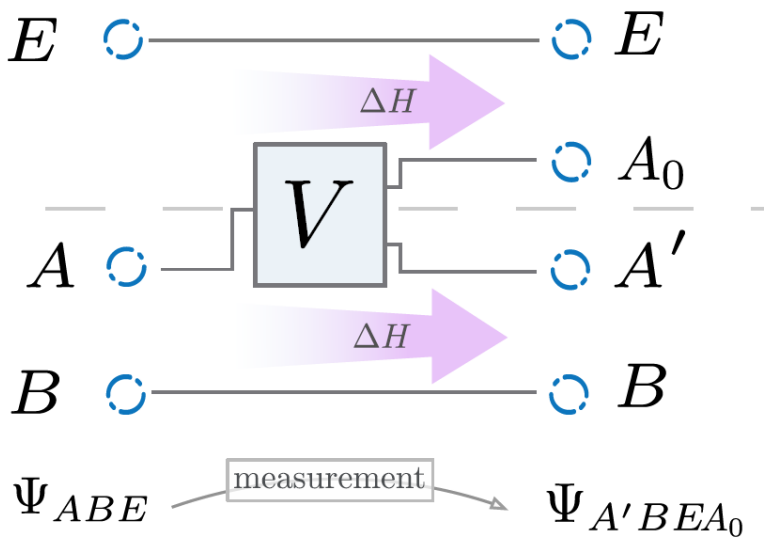
This channel can be described as an **isometry V to an extended** system A_0A' that maps **the pure state ψ_{ABE} to the pure $\psi_{A'BEA_0}$**

Initial and final states are pure, and thus the entropy change ΔH on the memory-Eve subsystem equals the entropy change on the Alice-Bob subsystem.

$$T[\rho_{AB}] = \mathrm{tr}_{A_0}((V \otimes \mathbb{I}_B)\rho_{AB}(V \otimes \mathbb{I}_B)^\dagger)$$

$$\begin{aligned} H(A_0|E) &= H(A_0E) - H(E) \\ &= H(A'B) - H(AB) \\ &= H(T[\rho_{AB}]) - H(\rho_{AB}) =: \Delta H \end{aligned}$$

Entropy Production



$$H(A_0|E) = H(A_0E) - H(E)$$
$$= H(A'B) - H(AB)$$
$$= H(T[\rho_{AB}]) - H(\rho_{AB}) =: \Delta H$$

The nice thing is that $H(A_0|E)$ which **requires the knowledge of the system E is computed only from information in the system A and B**

Need to fix the isometry: the pinching channel

$$T[\rho_{AB}] = \mathrm{tr}_{A_0}((V \otimes \mathbb{I}_B)\rho_{AB}(V \otimes \mathbb{I}_B)^\dagger) \longrightarrow T[\rho_{AB}] = \sum_a (P_{a|0} \otimes \mathbb{I}_B)\rho_{AB}(P_{a|0} \otimes \mathbb{I}_B).$$

arXiv:1908.11372

The tricks

$$H(A_0|E) = H(A_0E) - H(E)$$
$$= H(A'B) - H(AB)$$
$$= H(T[\rho_{AB}]) - H(\rho_{AB}) =: \Delta H$$

$$T[\rho_{AB}] = \sum_a (P_{a|0} \otimes \mathbb{I}_B)\rho_{AB}(P_{a|0} \otimes \mathbb{I}_B).$$

We still need to optimize over the unknown quantum states ρ_{AB}**, while we usually only know the expectation values**

$$l_j = \sum_{abxy} c^{(j)}_{abxy} \Pr(ab|xy)$$

Gibb's variational principle: we choose an ansatz

$$H\left(T[\rho]\right) - H(\rho) \geq \langle L \rangle_\rho - \ln\langle K \rangle_\rho,$$

$$L = \sum_j \lambda_j L_j$$

For some λ_j **real to optimize and an operator K**

arXiv:1908.11372

The tricks

$$H\left(T[\rho]\right) - H(\rho) \geq \langle L \rangle_\rho - \ln \langle K \rangle_\rho,$$

The shape of K can be chosen wisely (from the lagrangian dual of the problem) + Generalized Golden-Thompson.. **FINALLY**

$$\sup_{\vec{\lambda}} \left(\sum_j \lambda_j l_j - \ln \left(\sup_{\substack{\rho_{AB}, P_{a|x}, P_{b|y} \\ s.th.\ \langle L_j \rangle_{\rho_{AB}} = l_j}} \langle K \rangle_{\rho_{AB}} \right) \right)$$

$$L = \sum_j \tilde{L}_j,$$

$$K = T^* T \left[\int_{\mathbb{R}} dt\ \beta(t) \left| \prod_j e^{\frac{1+it}{2} \tilde{L}_j} \right|^2 \right],$$

$$with\ \beta(t) = \frac{\pi/2}{\cosh(\pi t) + 1},$$

arXiv:1908.11372

Device-Dependent case

This single formulation covers all the 3 QKD cases: Device-Dependent, One-Side Device-Independent, Device-Independent

For the Device-Dependent the measurement are known and K is fixed

$$\sup_{\vec{\lambda}} \left(\sum_j \lambda_j l_j - \ln \left(\sup_{\substack{\rho_{AB}, P_{a|x}, P_{b|y} \\ s.th.\ \langle L_j \rangle_{\rho_{AB}} = l_j}} \langle K \rangle_{\rho_{AB}} \right) \right)$$

The problem reduces at a single SDP: fast

$$\begin{aligned} \max \quad & \mathrm{tr}(\rho K) \\ \text{s.th.:} \quad & \mathrm{tr}(\rho \tilde{L}_j) = l_j \qquad \forall j \in \mathcal{J} \\ & \mathrm{tr}(\rho) = 1 \\ & \rho \geq 0 \end{aligned}$$

$$L = \sum_j \tilde{L}_j,$$

$$K = T^* T \left[\int_{\mathbb{R}} dt\ \beta(t) \left| \prod_j e^{\frac{1+it}{2} \tilde{L}_j} \right|^2 \right],$$

$$with\ \beta(t) = \frac{\pi/2}{\cosh(\pi t) + 1},$$

Device-Independent case

The measurement are not known, but the problem can be expressed as a non-commutative polynomial optimization

$$\sup_{\vec{\lambda}} \left(\sum_j \lambda_j l_j - \ln \left(\sup_{\substack{\rho_{AB}, P_{a|x}, P_{b|y} \\ s.th.\ \langle L_j \rangle_{\rho_{AB}} = l_j}} \langle K \rangle_{\rho_{AB}} \right) \right)$$

Can be solved with NPA hierarchy of SDP

$$L = \sum_j \tilde{L}_j,$$

Bonus: this formulation allows for the optimization of the min-tradeoff function of EAT, so can be generalized to non-IID scenarios with finite-size effects

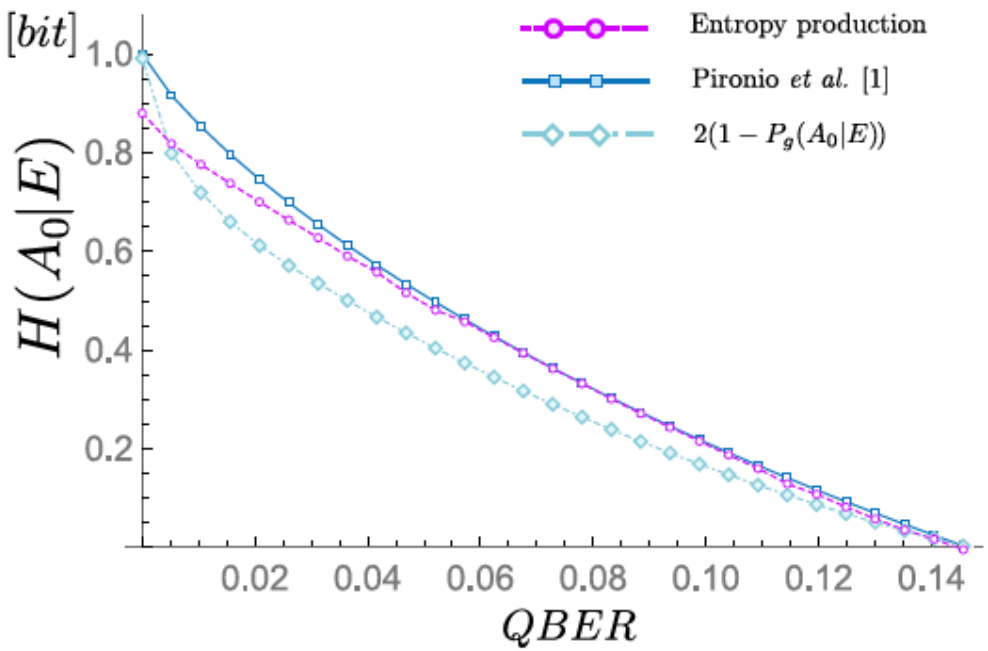
$$K = T^* T \left[\int_{\mathbb{R}} dt\ \beta(t) \left| \prod_j e^{\frac{1+it}{2} \tilde{L}_j} \right|^2 \right],$$

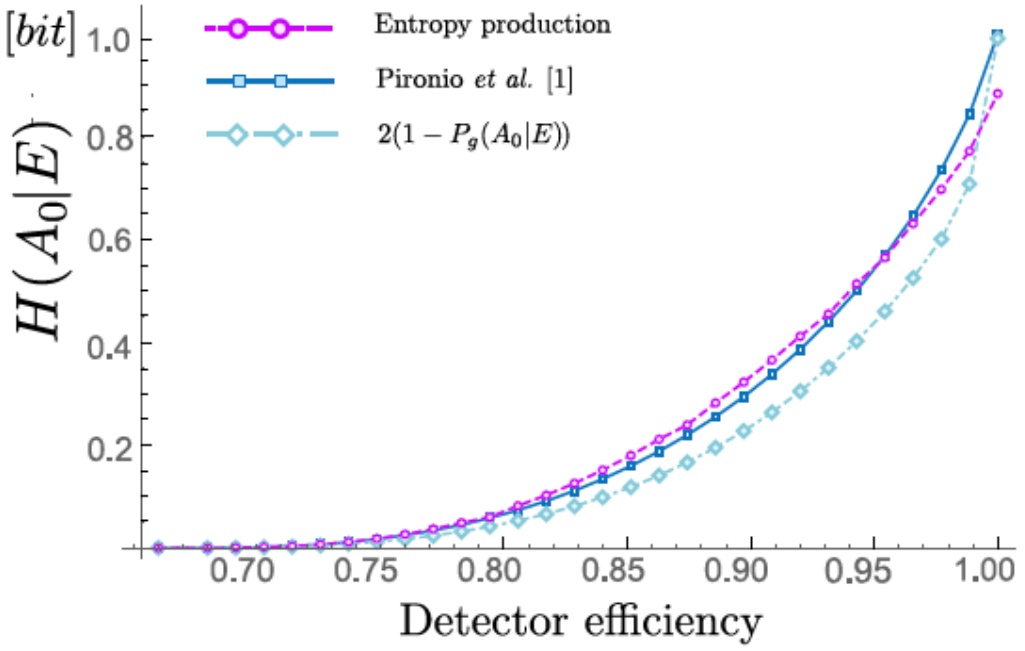
$$with\ \beta(t) = \frac{\pi/2}{\cosh(\pi t) + 1},$$

Results: is it any better?

For DD is equivalent to other state of the art approaches

For DI: **2-input 2-output DI protocols**



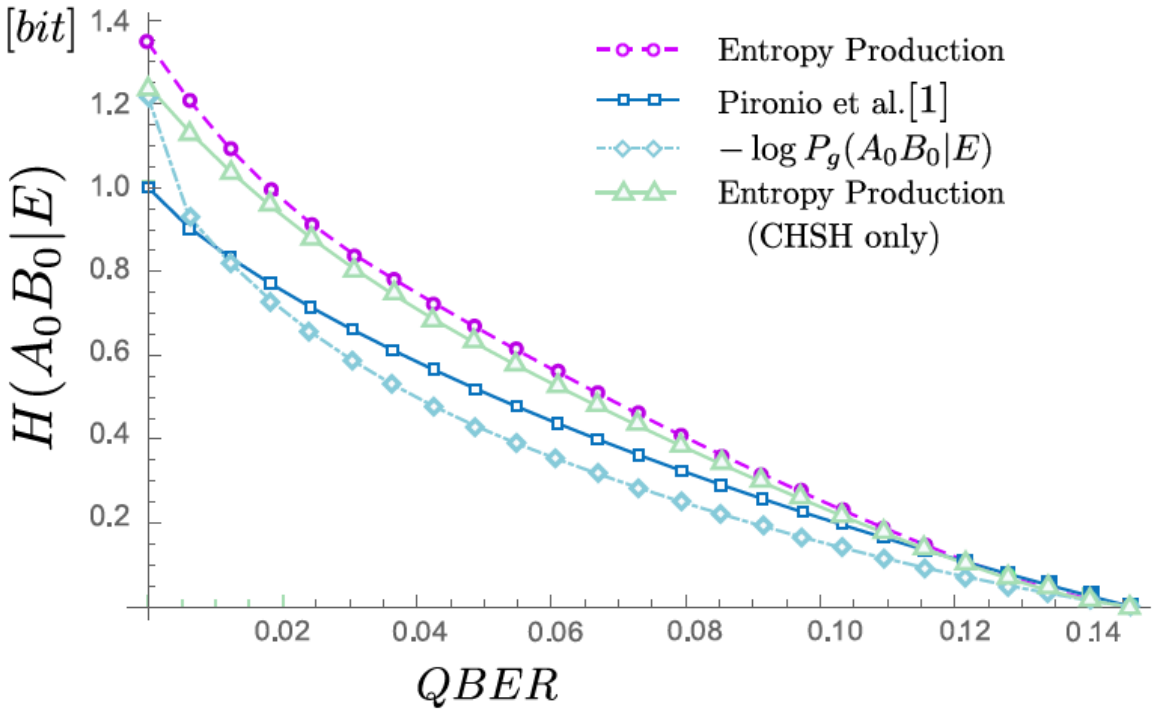


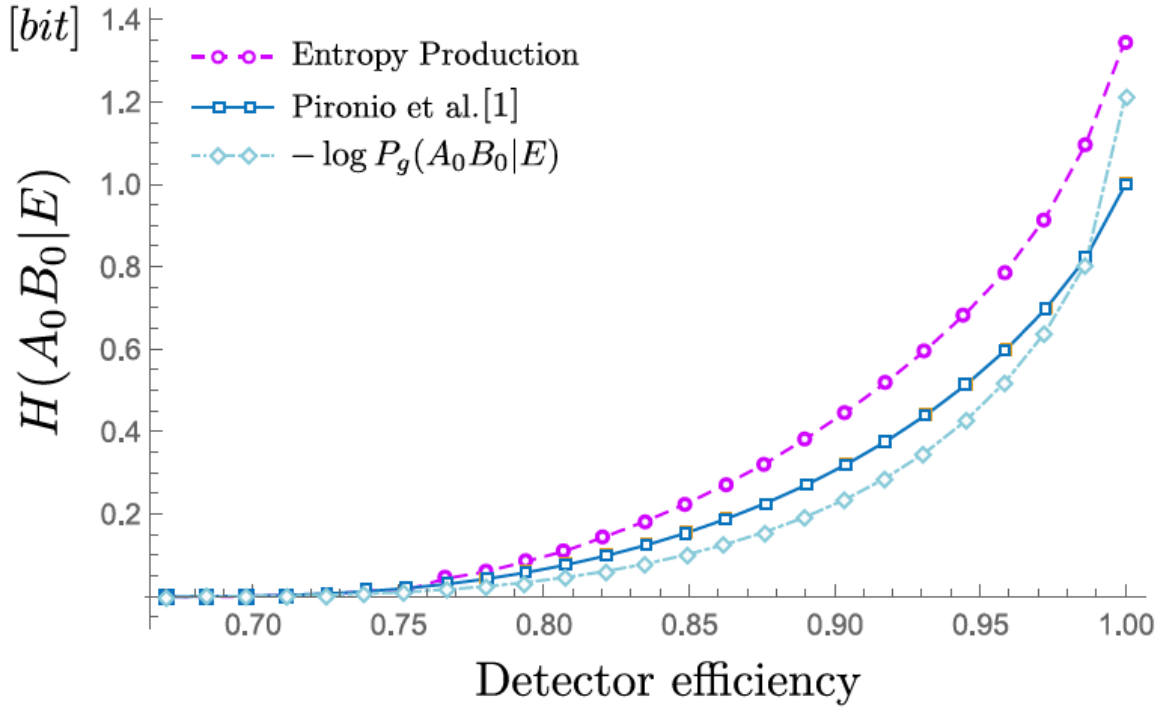
Results: is it any better?

For DD is equivalent to other state of the art approaches

For DI:

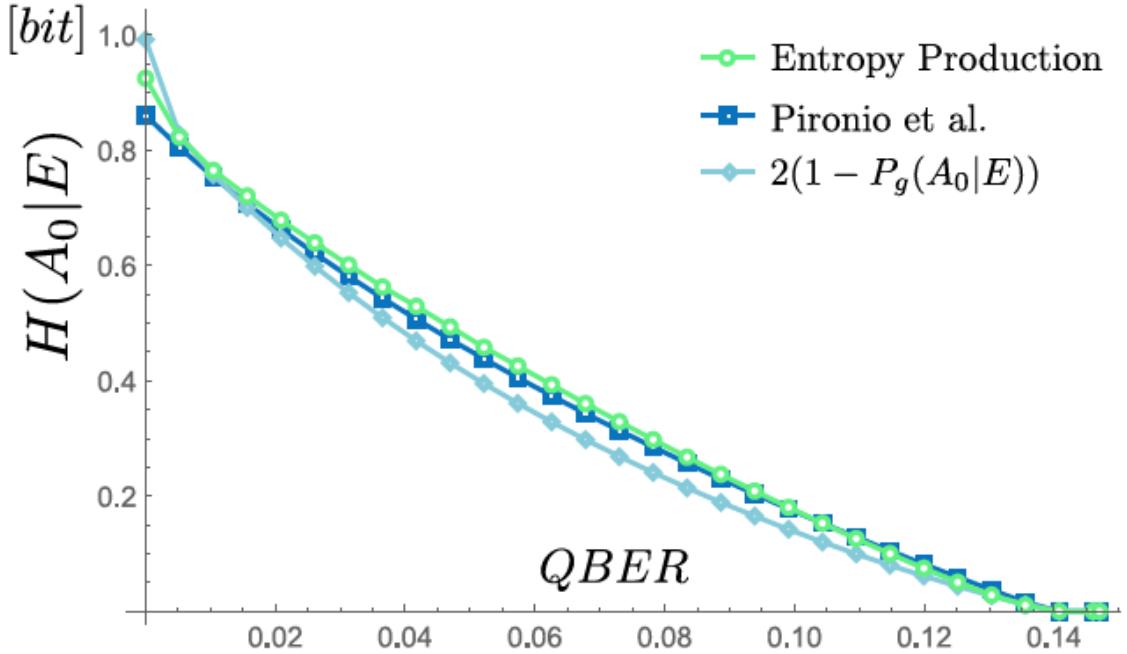
2-input 2-output DI global randomness



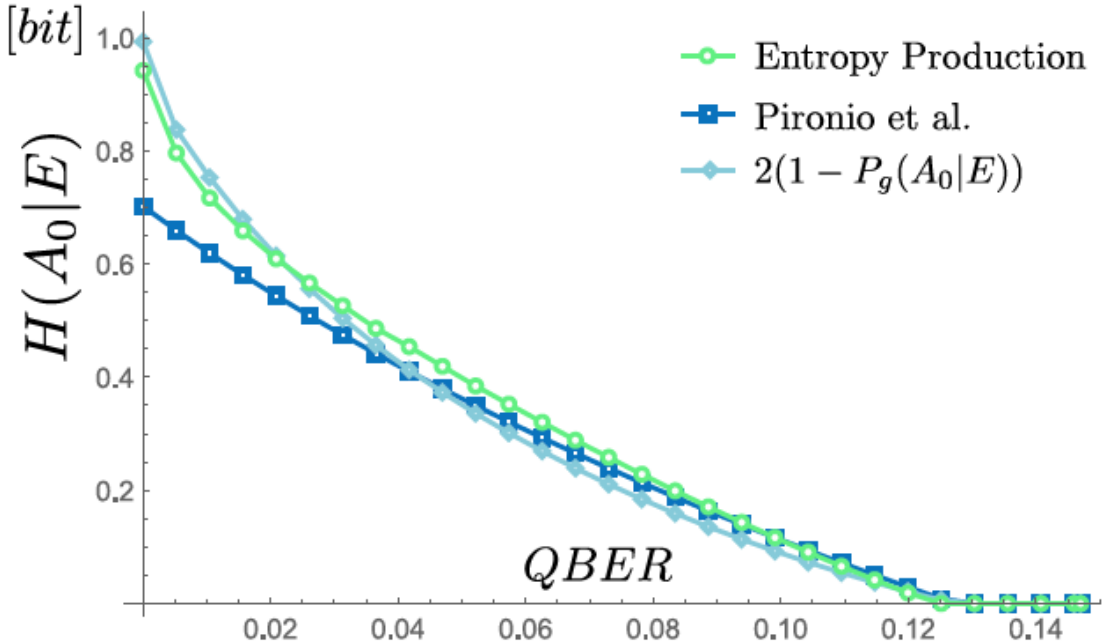


A general idea of why it's working

Tilted CHSH: $\alpha\left(\langle A_0B_0\rangle + \langle A_0B_1\rangle\right) + \langle A_1B_0\rangle - \langle A_1B_1\rangle.$



$\alpha = 1{,}5$



$\alpha = 2$

Conclusions

Key points:

- General structure for tackling all QKD protocols
- More trust on the devices is simply added by adding constraints
- Almost tight bounds (except for Golden-Thompson)
- Reduces to single SDP for DD protocols
- Exploits NPA for DI
- Compatible with EAT framework for tight finite-size analysis

Main drawbacks:

- Computation power in DI-QKD: already for the class of 2-input 2-output DI-QKD it requires an NPA at level 6
- Intractable at 4-input 4-output
- Still bounds the von-Neumann entropy… New approaches to directly bound the Smooth-conditional min-entropy