Device-independent Quantum Key distribution

M1 MPR internship

MOHAMED BASSIOUNY

Supervised by

PETER BROWN(ENS-LYON)

Ac. advisors

P.ARRIGI/S. CONCHON

The internship

- Duration: 3 months
- **Research group:** Lyon quantum information group @ Ens-Lyon
- **Topic** : Device independent Quantum Key Distribution (DIQKD)
- **Goal**: Analyze whether or not DIQKD is feasible using current technology.
- **task**: implementation of numerical tools to compute key rates of simple models of experimental setups and developing new protocols to improve the rates.

Preliminaries (1)

- Main concepts we rely on are:
  - Quantum Entanglement
  - CHSH game
  - Entropy (to compute rates)

Refresher on Entanglement :

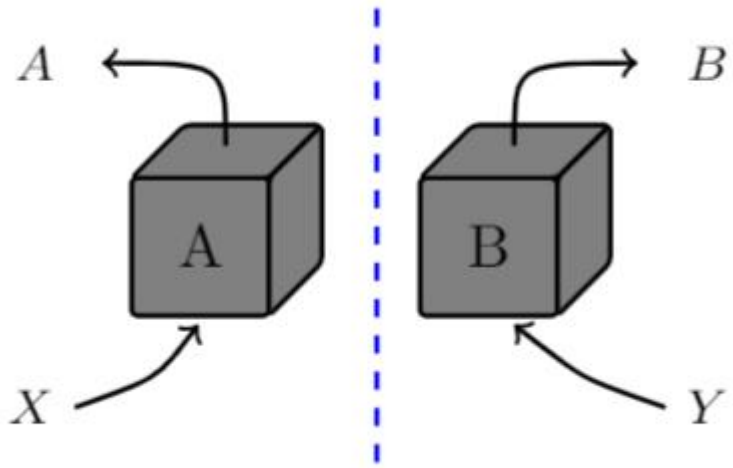
A magnificent property of quantum mechanics that allows non-local correlation.

Used in CHSH game.

Preliminaries (2) - CHSH

CHSH game:

Alice and Bob are given random X and Y in $\{0,1\}^2$ as input



they win the game if:

$$A \oplus B = X \cdot Y$$

Classical winning pr =3/4= 0.75:

X	Y	X.Y
0	0	0
0	1	0
1	0	0
1	1	1

Quantum winning pr

$$p_{win|X=0,Y=0} + p_{win|X=1,Y=0} + p_{win|X=1,Y=0} + p_{win|X=1,Y=1}$$

If we divide this sum by 4 we get 0.85!

DIQKD

Quantum key distribution:

- A process during which two parties attempt to generate a shared random secret at distant locations. This would then allow them to securely send messages using symmetric encryption schemes.

Device-independent Quantum key distribution:

- DIQKD is the process of using untrusted devices to distribute secret keys in an insecure network. The initial state of the device is unknown to us. Devices may be even prepared by an adversary as part of his attack

Computing randomness and rates

Our goal:

- we have devices that obey some set of constraints **C**.
- We want study to the ”quality” of randomness generated by the given devices and asses how good our set of constraints is.

  → we use the concept of **entropy (H_{min})** to evaluate each device.

$$H_{min}(X|E) = -log P_{guess}(X|E)$$

$$P_{guess}(X|E) = max_{\{M_x\}_x} \sum_x \mathcal{P}_x tr[M_x \rho_x^E]$$

We maximize here over all POVMs with ρ_{XE} a state

Formulating the problem

We compute the amount of randomness Alice can generate.

Which is P(0|0) in the CHSH game:

$$r(\omega) = \max \quad P(A=0|X=0)$$
$$\text{s.t.} \quad \text{tr}\{\rho K\}/4 \geq \omega$$

→ The CHSH constraint, We remind that CHSH operators are the given matrices $A_{0|0}, A_{0|1}, B_{0|0}, B_{0|1}$ we define:

$$K = A_{0|0} \otimes B_{0|0} + (I - A_{0|0}) \otimes (I - B_{0|0}) + A_{0|0} \otimes B_{0|1} + (I - A_{0|0}) \otimes (I - B_{0|1}) + A_{0|1} \otimes B_{0|0}$$
$$+ (I - A_{0|1}) \otimes (I - B_{0|0}) + A_{0|1} \otimes (1 - B_{0|1}) + (I - A_{0|1}) \otimes B_{0|1}.$$

$$\text{Where } 0 \leq A_{0|0}, A_{0|1}, B_{0|0}, B_{0|1} \leq I \text{ state.}$$

$$p_{\text{CHSHwin}} = tr\{\rho k\}/4$$

The problem is hard to solve

We are maximizing over all Hilbert spaces, all states and all operators.

Our goal: maximize Alice's randomness (optimize her winning probability) knowing that the size of our dimension can be infinite.

→we are looking to optimize even if our operators(which are matrices) are of infinite size!

This is non-trivial and can't be easily solved numerically!

we get rid of tensor products and relax the problem to non-commuting polynomials (NCPOP) where the polynomial symbols will simply represent matrices.

Formulating the problem (relaxed)

Optimizing P(0|0) numerically is not an easy task, so…

We formulate the weaker problem as an NCPOP as follows:

$$\begin{aligned} \max \quad & \boxed{\mathrm{tr}\left\{\rho \widehat{K}\right\}/4} \\ \text{s.t.} \quad & 0 \leq A_{0|0}, A_{0|1}, B_{0|0}, B_{0|1} \leq I \\ & [A_{0|x}, B_{0|y}] = 0 \qquad \text{for all } x, y \in \{0,1\} \end{aligned}$$

NEW CHSH Constraint

where $[X, Y] = XY - YX$ and

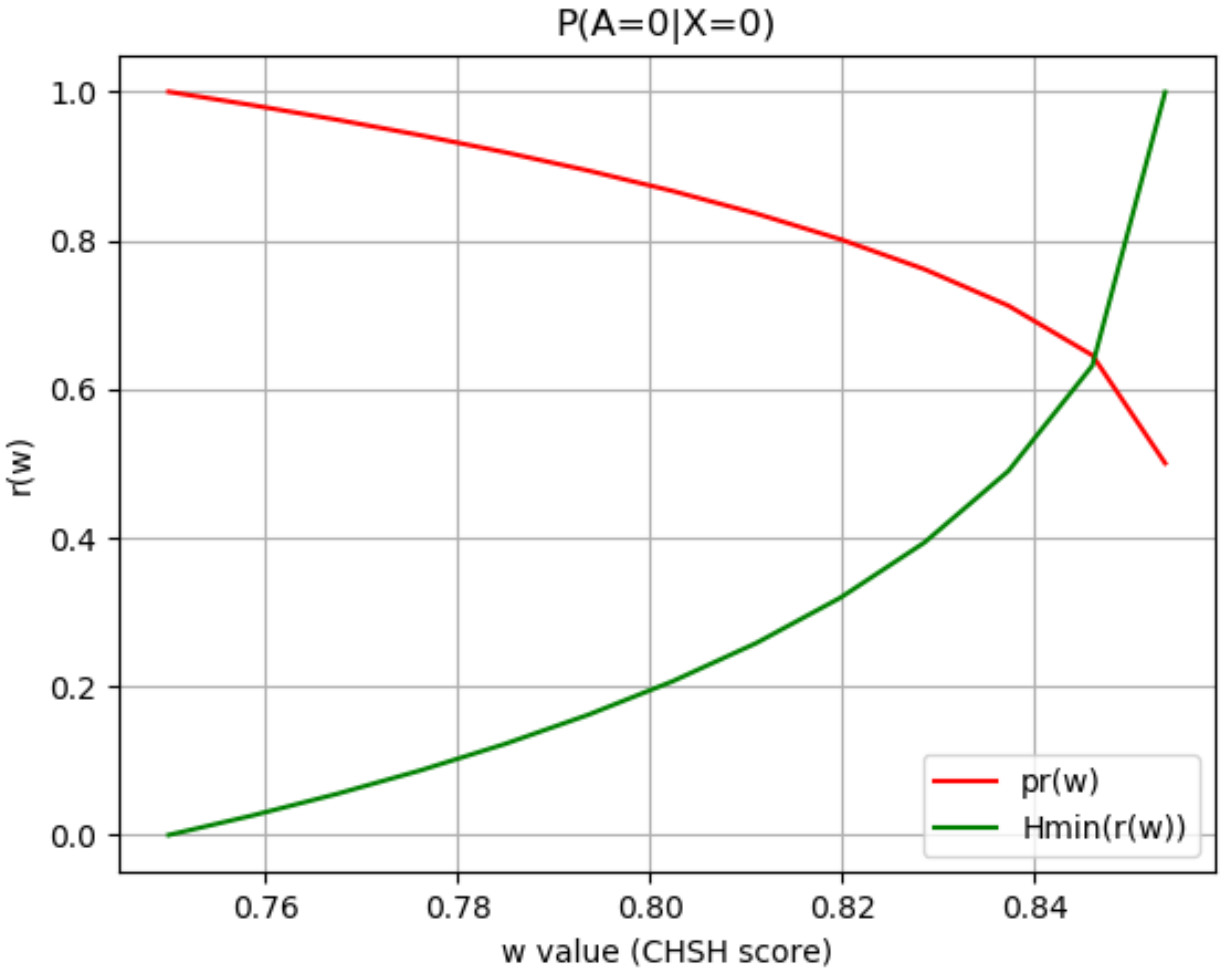
$$\begin{aligned} \widehat{K} = {} & A_{0|0}B_{0|0} + (I - A_{0|0})(I - B_{0|0}) + A_{0|0}B_{0|1} + (I - A_{0|0})(I - B_{0|1}) \\ & + A_{0|1}B_{0|0} + (I - A_{0|1})(I - B_{0|0}) + A_{0|1}(1 - B_{0|1}) + (I - A_{0|1})B_{0|1}. \end{aligned}$$

→ **Easier to solve thanks to NPA → SDP (see references at the end)**

Computations and results-randomness (1)

Simple protocol with Alice given a CHSH score ω

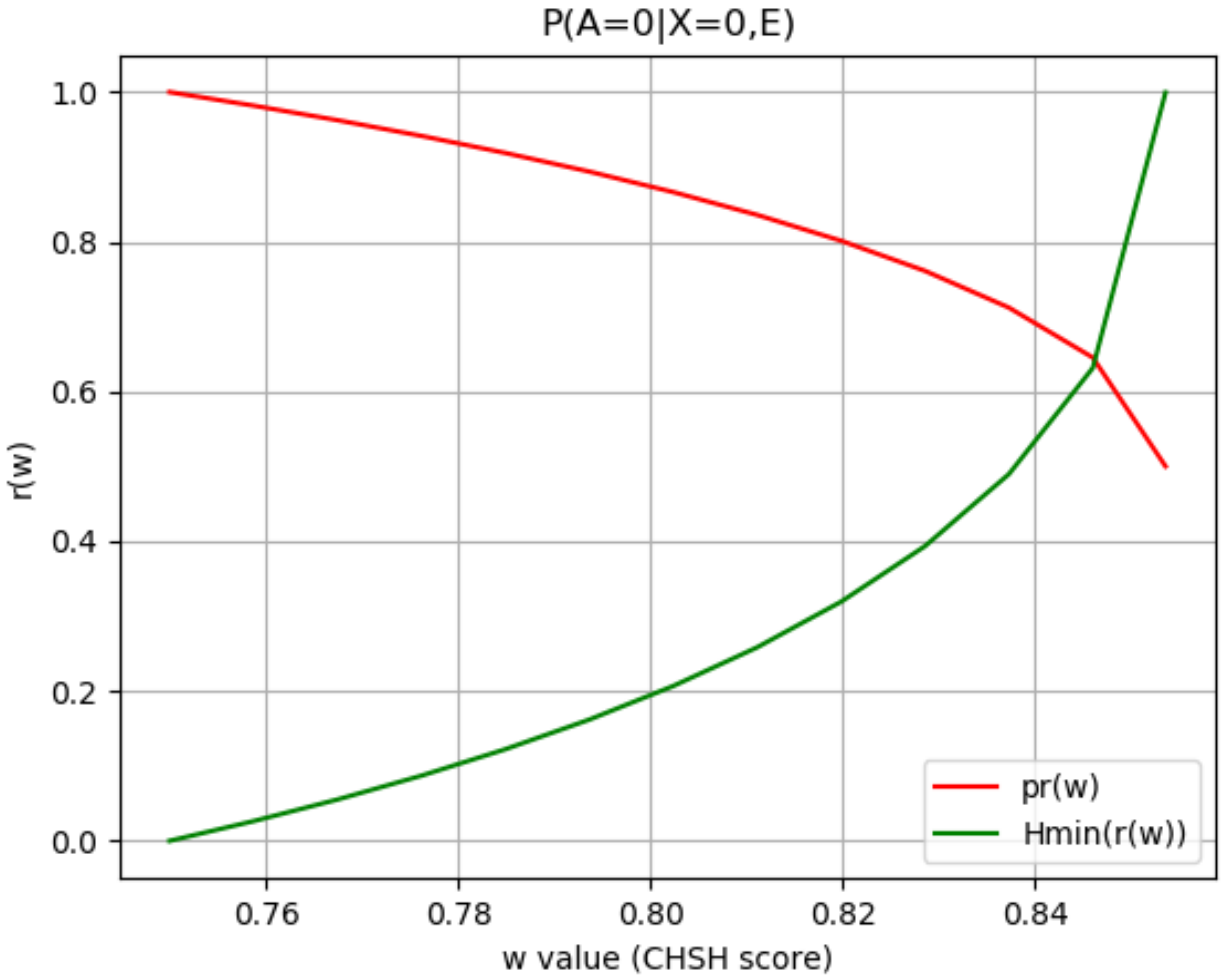
$$r(\omega) = \max \quad P(A=0|X=0)$$
$$\text{s.t.} \quad \mathrm{tr}\left\{\rho \widehat{K}\right\} \geq \omega$$



Computations and results-randomness (2)

Simple protocol with Alice and Eve given a CHSH score ω

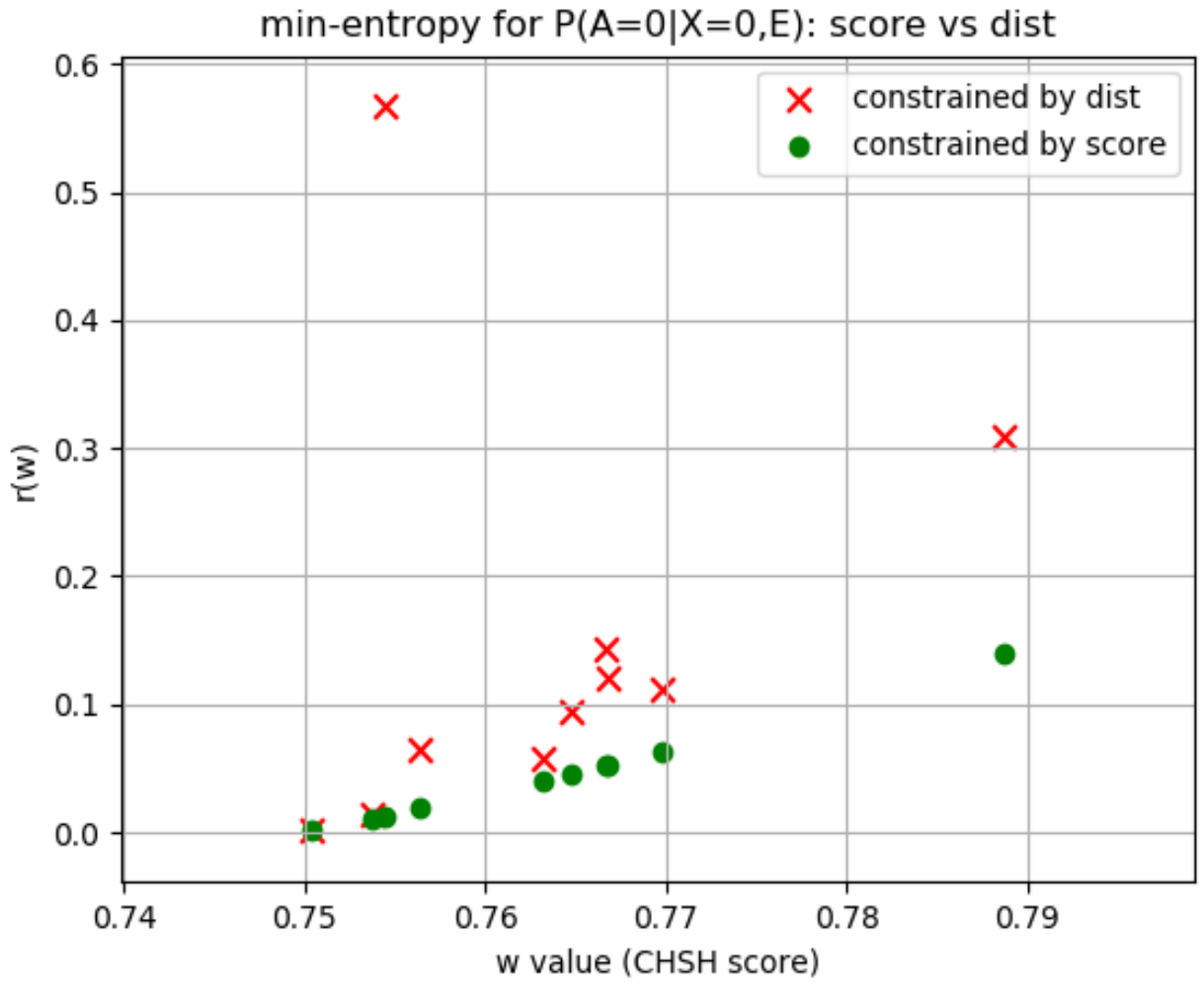
$$r(\omega) = \max \quad P(A=0|X=0,E)$$
$$\text{s.t.} \quad \mathrm{tr}\left\{\rho\widehat{K}\right\} \geq \omega$$



Computations and results-randomness (3)

Comparing set of constraints:

CHSH score vs Full distribution



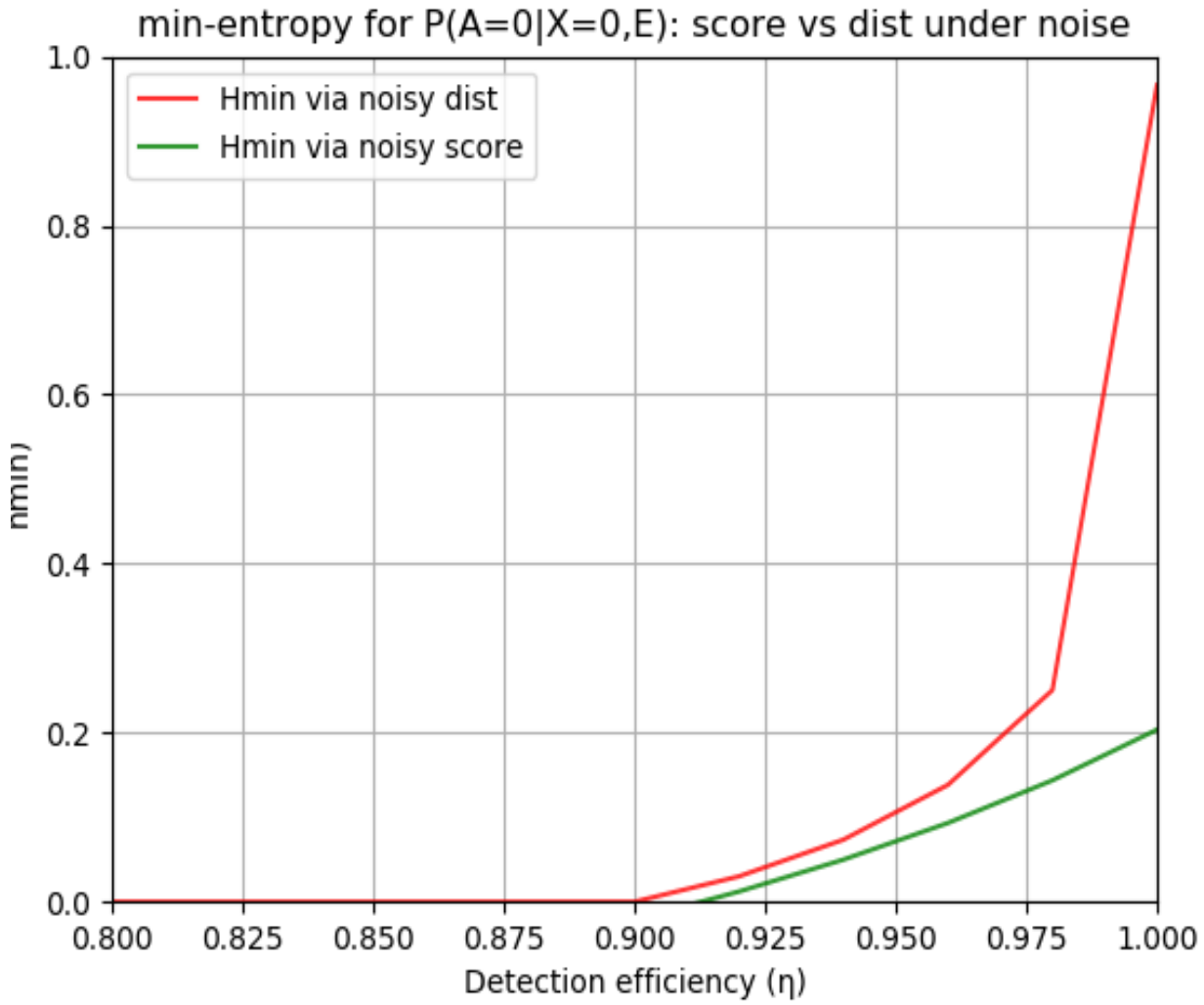
Computations and results-randomness (4a)

Comparing set of constraints:

CHSH score vs Full distribution

Taking into account **possibility of device failures (detection efficiency) η**

With a random device



Computations and results-randomness (4b)

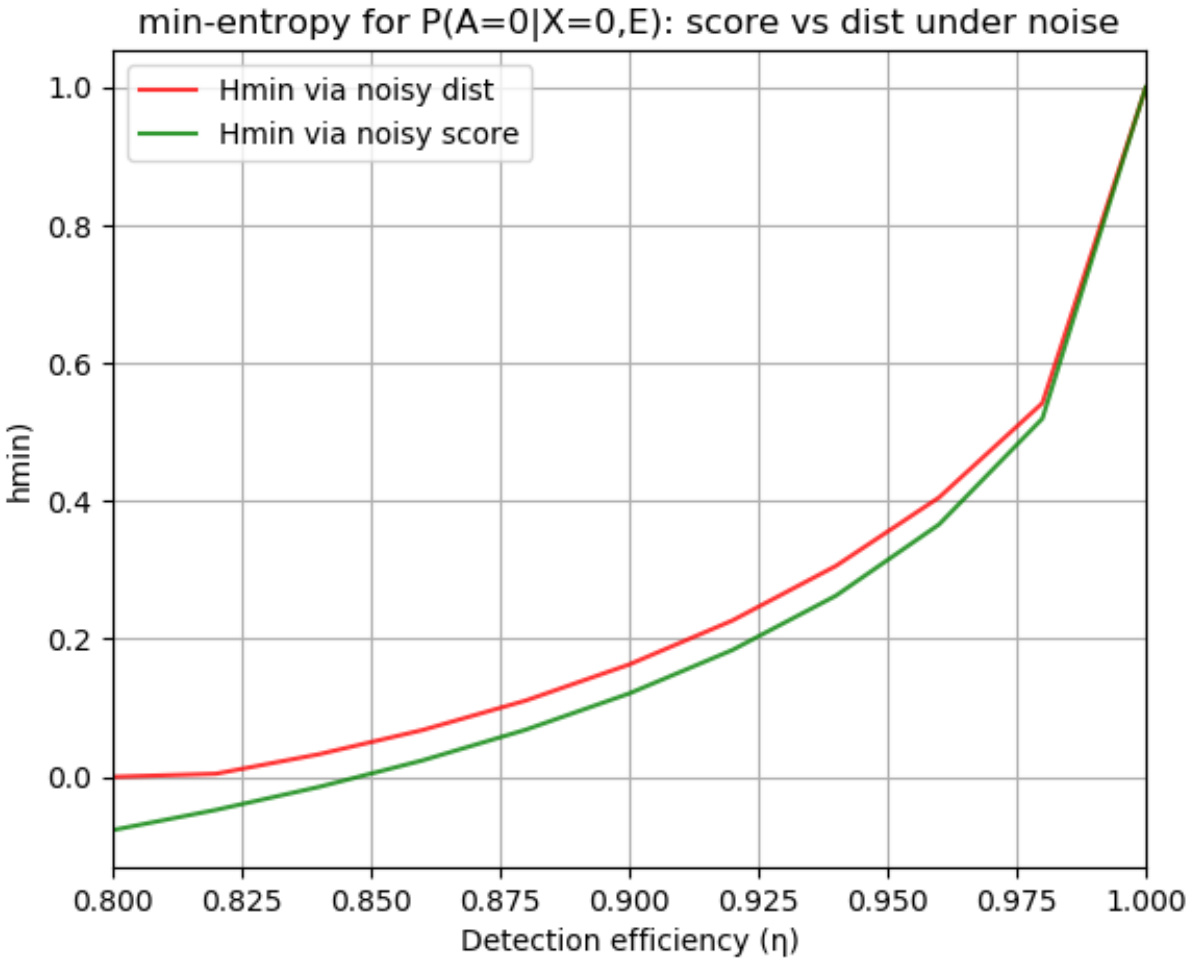
Comparing set of constraints:

CHSH score vs Full distribution

Adding Detection efficiency **η**

With Another (better) device

(using a maximally entangled state)

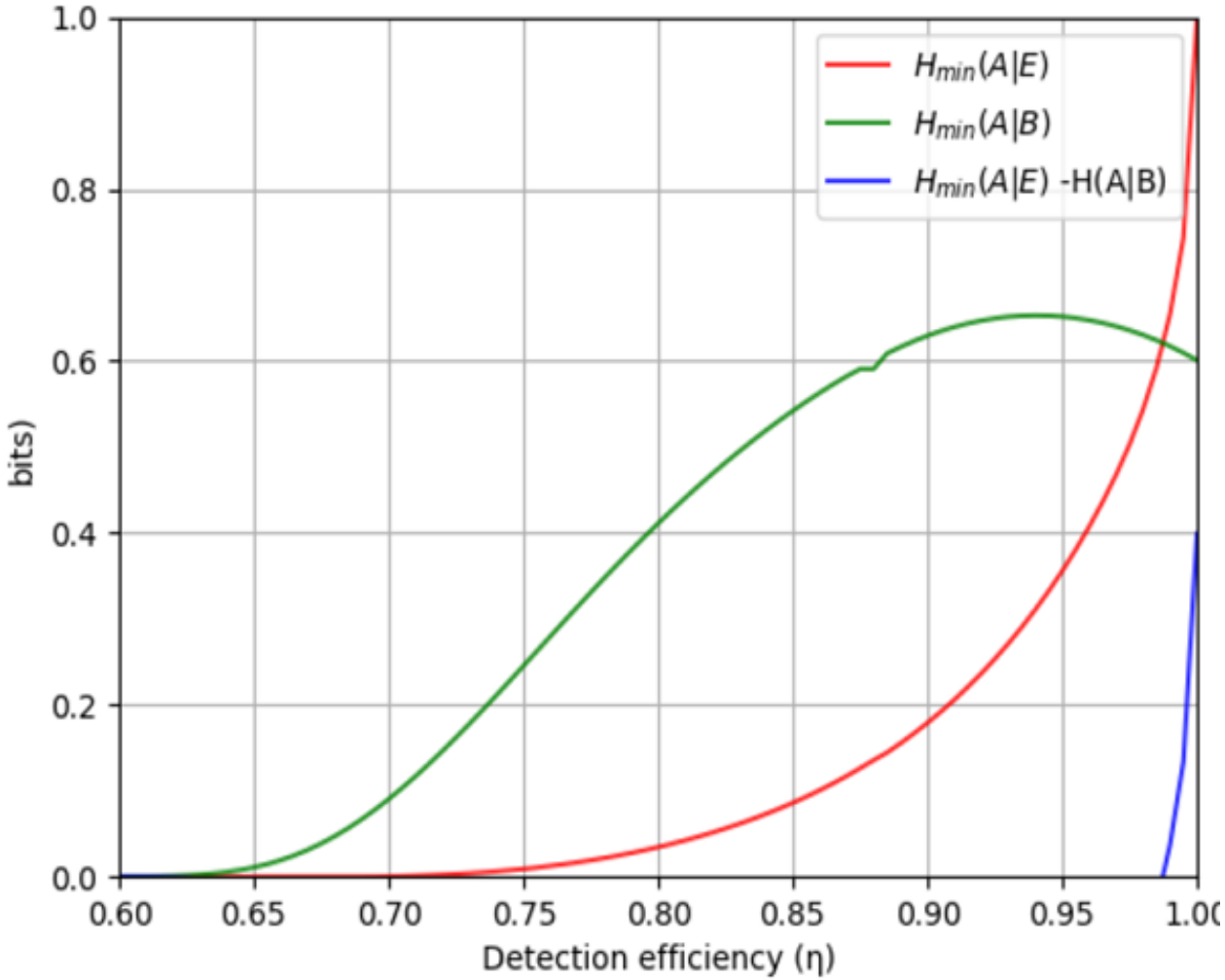


Computations and results-rates (1)

Rate for DIQKD :

$$inf\ H(A|X = x^*,E) - H(A|\ B, X=x^*, Y=y^*)$$

- $inf\ H(A|X = x^*,E)$: previous slides
- $H(A|\ B, X=x^*, Y=y^*)$: computed from the probability distribution



Computations and results-rates (2)

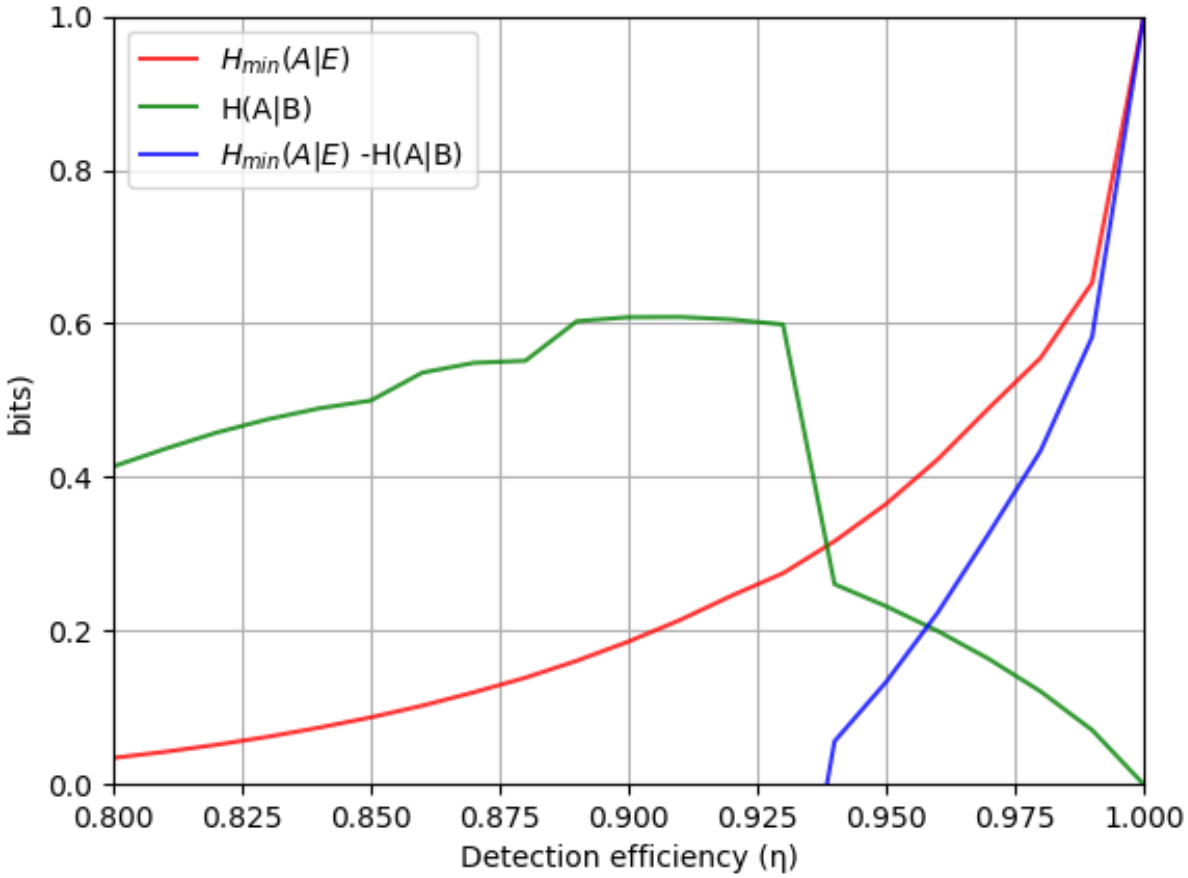
Rate for DIQKD, minimizing H(A|B) **:**

We give Bob a third input that acts as his key-generation input

→ x,a,b ∈ {0,1} and y ∈{0,1,2}

The rate becomes:

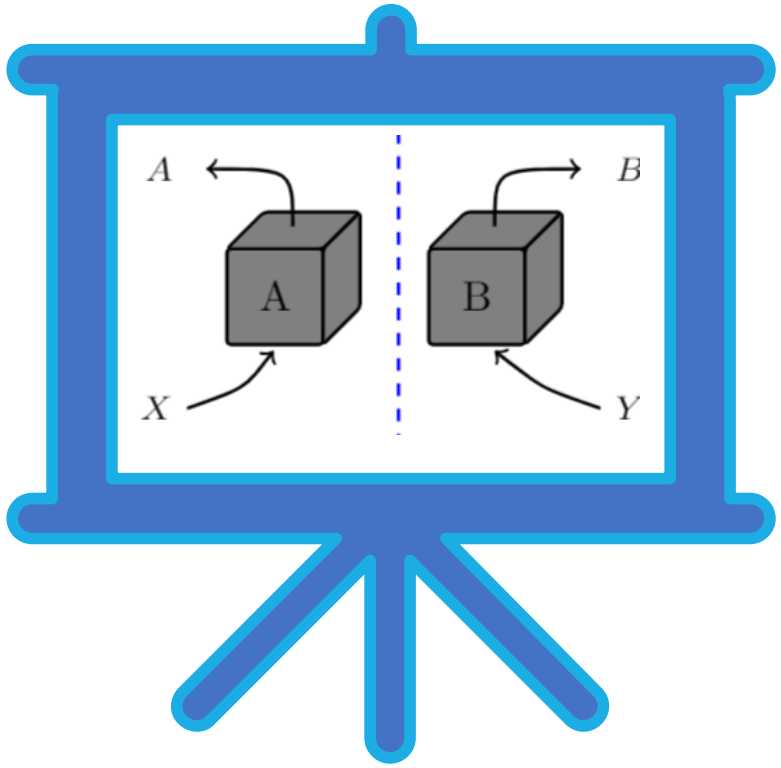
inf H(A|X = x*,E) - H(A|B,X= 0,Y= 2).



Conclusion

- DIQKD is powerful, gives security guarantees but requires a good system.
- Noise in experiments is a major challenge.
- We hope to improve our rates in order to achieve a reliable/feasible DIQKD protocol with our current devices.

Thank you



References

The illustration in slide 4 is borrowed from another presentation made by my mentor, Peter Brown, so thanks a lot for allowing me to re-use it.

Also, most of the formulas presented in slides 7 and 8 are borrowed from his notes that he shared with me during this internship to teach me more on the topic.

NPA and SDP: Miguel Navascus, Stefano Pironio, and Antonio Acn. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. New Journal of Physics, 10(7):073013, Aug 2008.

Internship based on the following publications:

Peter Brown, Hamza Fawzi, and Omar Fawzi. Computing conditional entropies for quantum correlations. Nature communications , 12(1):1–12, 2021

Stefano Pironio, Antonio Ać ın, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. New Journal of Physics , 11(4):045021, 2009.

Peter Brown, Hamza Fawzi, and Omar Fawzi. Device-independent lower bounds on the conditional von Neumann entropy - arXiv preprint arXiv:2106.13692, 2021