Device-independent lower bounds on the conditional von Neumann entropy

Peter Brown, Hamza Fawzi and Omar Fawzi

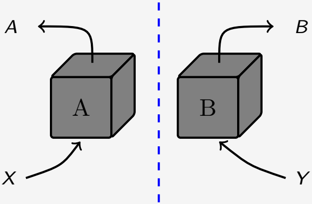
arXiv:2106.13692

Aug 25, 2021

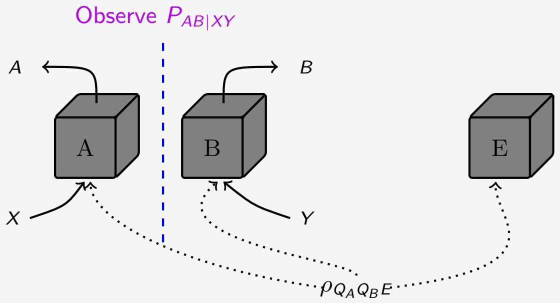
ENS DE LYON

The problem

Observe $P_{AB|XY}$

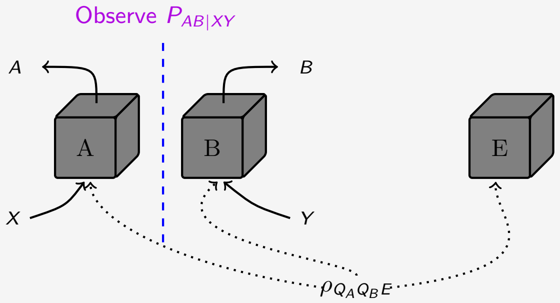


The problem



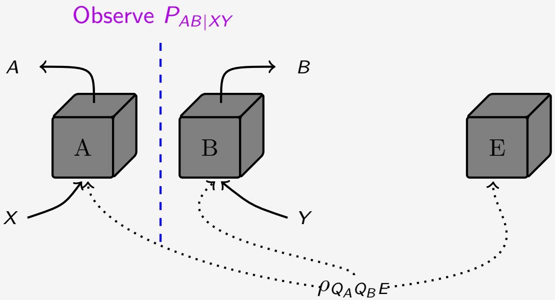
- Foundation for randomness expansion / key-distribution protocols!

The problem



- Foundation for randomness expansion / key-distribution protocols!
- Security and analysis relies on *rate* (bits per interaction).

The problem

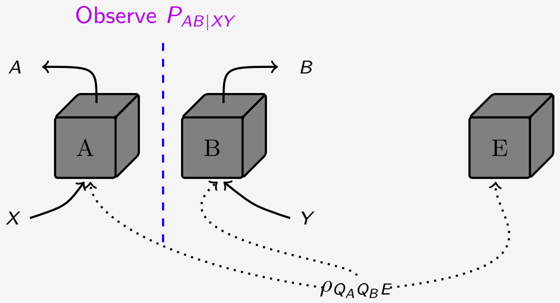


- Foundation for randomness expansion / key-distribution protocols!
- Security and analysis relies on *rate* (bits per interaction).

$$\text{minimize} \quad H(A|E)$$

over **all** devices compatible with statistics.

The problem



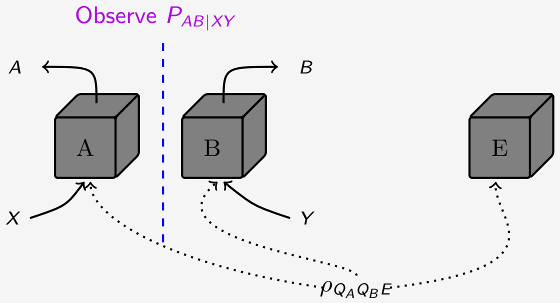
- Foundation for randomness expansion / key-distribution protocols!
- Security and analysis relies on *rate* (bits per interaction).

$$\text{minimize} \quad H(A|E)$$

or $H(AB|E)$
or $H(A|E) - H(A|B)$
or. . .

over **all** devices compatible with statistics.

The problem



- Foundation for randomness expansion / key-distribution protocols!
- Security and analysis relies on *rate* (bits per interaction).

$$\text{minimize} \quad H(A|E)$$

or $H(AB|E)$
or $H(A|E) - H(A|B)$
or...

over **all** devices compatible with statistics.

- Difficult to solve – nonconvex / unbounded dimension

Our approach

- Define a sequence

$$H_m(\rho) = \inf_{Z_1,\ldots,Z_m \in B(H)} \mathrm{Tr}\left[\rho\ q(Z_1,\ldots,Z_m)\right] \tag{1}$$

such that $H_m \leq H$ and $H_m \to H$ as $m \to \infty$.

Our approach

- Define a sequence

$$H_m(\rho) = \inf_{Z_1,\ldots,Z_m \in B(H)} \mathrm{Tr}\left[\rho \; q(Z_1,\ldots,Z_m)\right] \tag{1}$$

such that $H_m \leq H$ and $H_m \to H$ as $m \to \infty$.

- inf H_m efficiently approximated by semidefinite programming [NPA].

Our approach

- Define a sequence

$$H_m(\rho) = \inf_{Z_1,\dots,Z_m \in B(H)} \mathrm{Tr}\left[\rho\, q(Z_1,\dots,Z_m)\right] \tag{1}$$

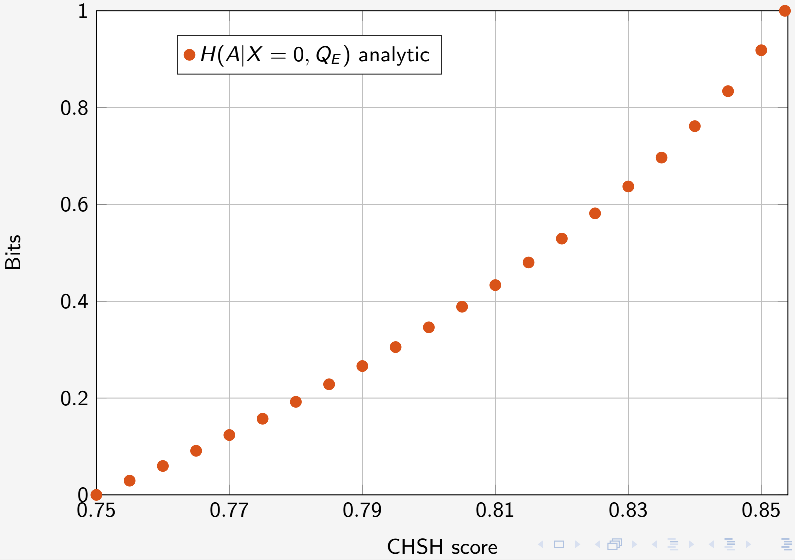
such that $H_m \leq H$ and $H_m \to H$ as $m \to \infty$.

- $\inf H_m$ efficiently approximated by semidefinite programming [NPA].

- close to optimal / more efficient / wider scope

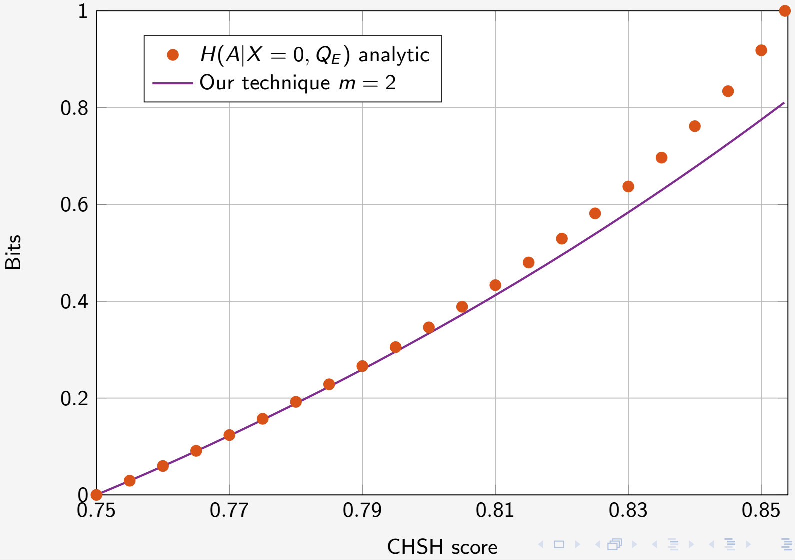
Results I – Recovering tight bounds for the CHSH game

Bounding $\inf H(A|X=0, Q_E)$



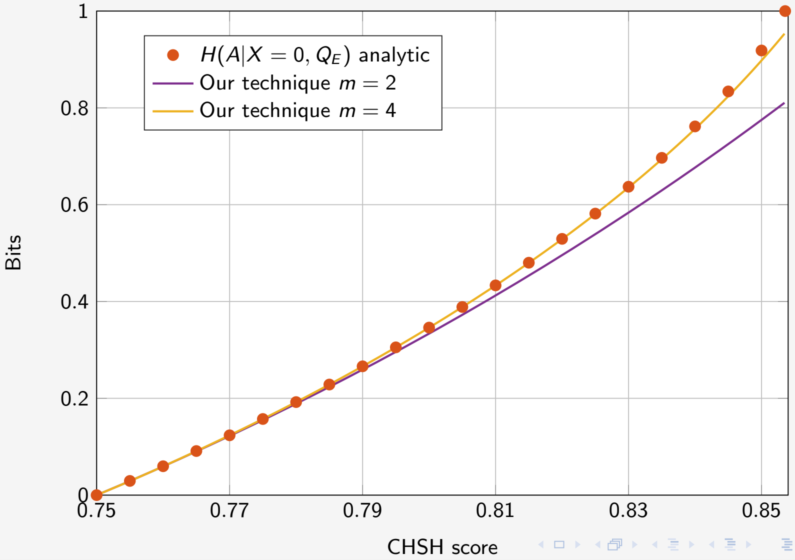
Results I – Recovering tight bounds for the CHSH game

Bounding $\inf H(A|X=0, Q_E)$



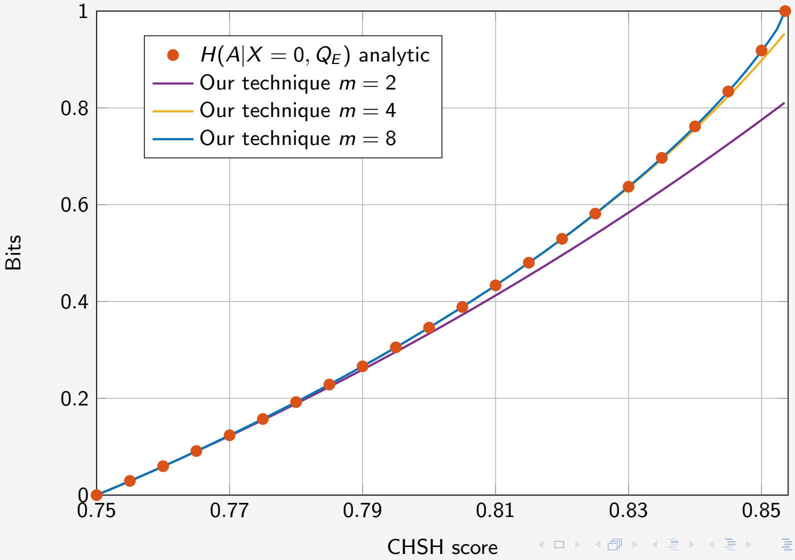
Results I – Recovering tight bounds for the CHSH game

Bounding $\inf H(A|X=0,Q_E)$



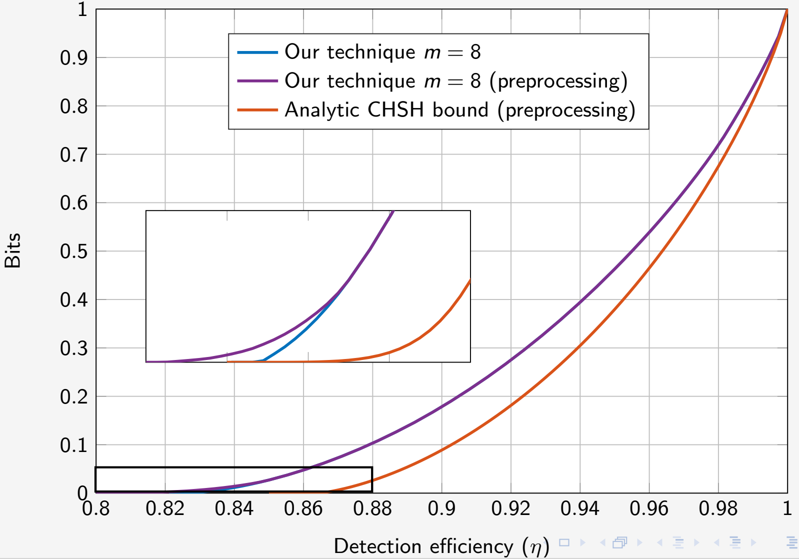
Results I – Recovering tight bounds for the CHSH game

Bounding $\inf H(A|X=0, Q_E)$



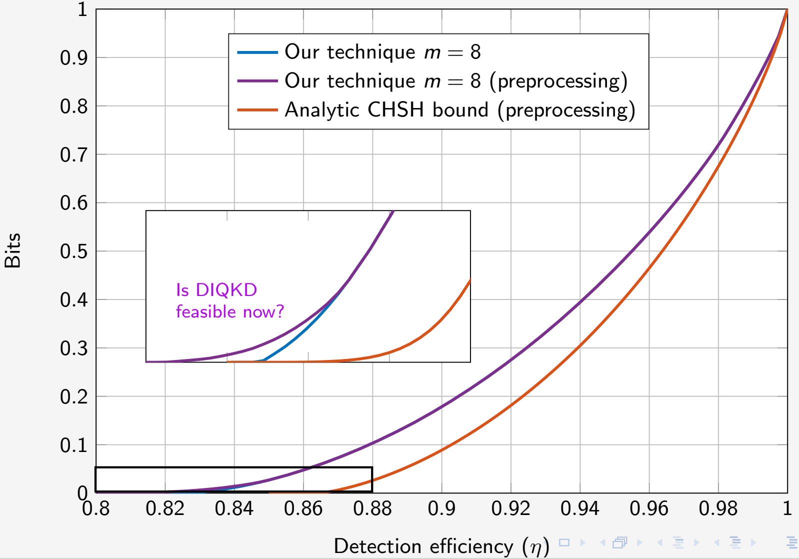
Results III – Improved DIQKD rates

Bounding $\inf H(A|X=0, Q_E) - H(A|X=0, Y=2, B)$



Results III – Improved DIQKD rates

Bounding $\inf H(A|X=0,Q_E) - H(A|X=0,Y=2,B)$



Thanks for listening!