Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols

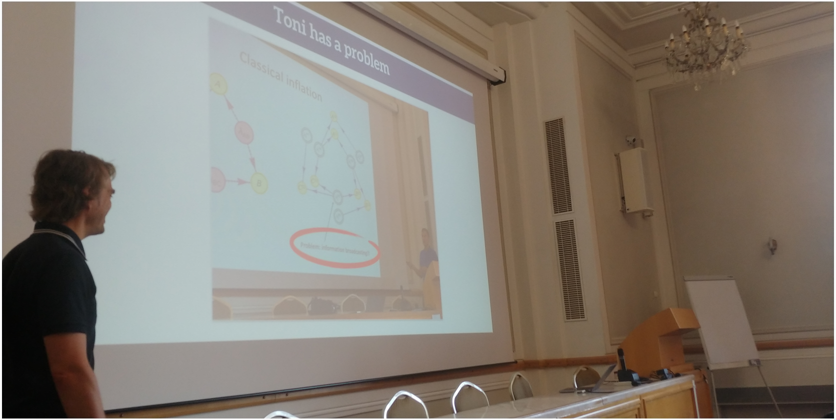
Máté Farkas – ICFO, Barcelona $\longrightarrow$ University of York

6 September, 2023 – 18th CEQIP workshop, Smolenice

joint work with Maria Balanzó-Juandó, Karol Łukanowski, Jan Kołodyński and Antonio Acín

Phys. Rev. Lett. **127**, 050503

Teiko has a problem



Quantum advantage

$$\Downarrow$$

Non-classical phenomenon

Quantum advantage

$\Uparrow$ **?**

Non-classical phenomenon

Quantum advantage

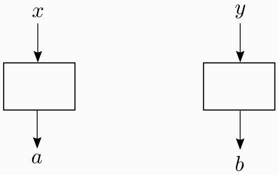
Device-independent quantum key distribution

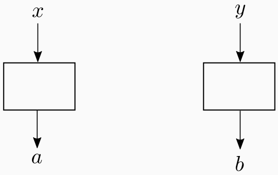
$\Uparrow$ **?**

Non-classical phenomenon

Bell nonlocality

Bell nonlocality

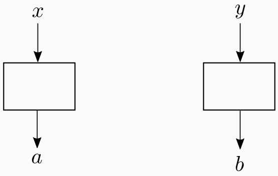

x
y
a
b



- Quantum set:

$$\mathcal{Q} = \{p(a, b|x, y) = \mathrm{tr}[\rho(A_a^x \otimes B_b^y)]\}$$

  - Convex set

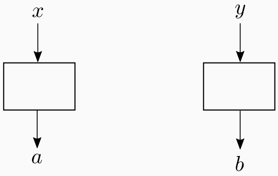


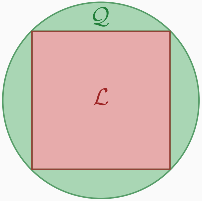
- Quantum set:

$$\mathcal{Q} = \{p(a,b|x,y) = \mathrm{tr}[\rho(A_a^x \otimes B_b^y)]\}$$

  - Convex set
- Local set:

$$\mathcal{L} = \Big\{p(a,b|x,y) = \int_\Lambda p_A(a|x,\lambda)p_B(b|y,\lambda)\mathrm{d}\mu(\lambda)$$
$$= \sum_{\lambda'} p_{\Lambda'}(\lambda')\delta_{a,f_A(x,\lambda')}\delta_{b,f_B(y,\lambda')}\Big\}$$





- Quantum set:

$$\mathcal{Q} = \{p(a,b|x,y) = \mathrm{tr}[\rho(A_a^x \otimes B_b^y)]\}$$

  - Convex set

- Local set:

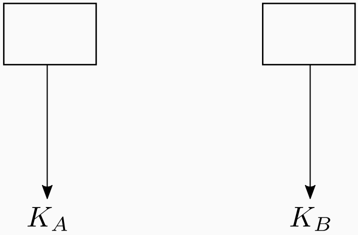
$$\begin{aligned}\mathcal{L} = \Big\{p(a,b|x,y) &= \int_\Lambda p_A(a|x,\lambda)p_B(b|y,\lambda)\mathrm{d}\mu(\lambda) \\ &= \sum_{\lambda'} p_{\Lambda'}(\lambda')\delta_{a,f_A(x,\lambda')}\delta_{b,f_B(y,\lambda')}\Big\}\end{aligned}$$

  - Convex polytope, $\mathcal{L} \subsetneq \mathcal{Q}$

Device-independent quantum key distribution (DIQKD)

DIQKD – idea

Key Distribution



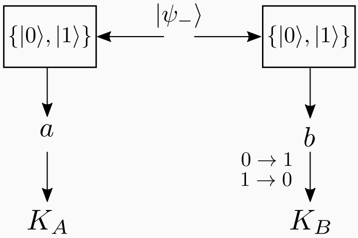
$$K_A = K_B$$

K_A and K_B are random

DIQKD – idea

Quantum

Key Distribution



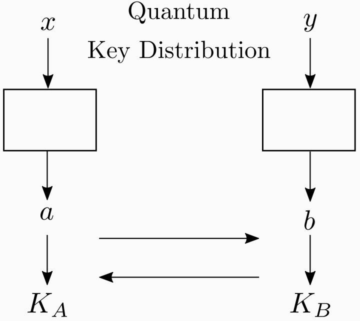
$$K_A = K_B$$

K_A and K_B are random

$$|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

DIQKD – idea

Device-Independent
Quantum
Key Distribution

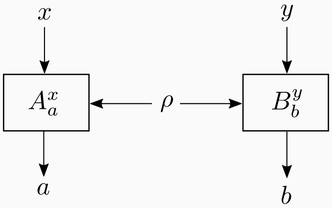


$$K_A = K_B$$

K_A and K_B are random

$$p_{AB}(a,b|x,y) = \mathrm{tr}\big[\rho(A_a^x \otimes B_b^y)\big]$$

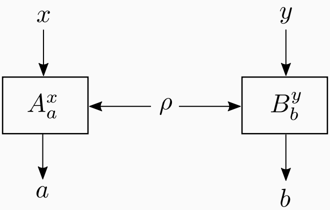
DIQKD based on the CHSH inequality[1]



$$x, a, b \in \{0,1\},\ y \in \{0,1,2\}$$

[1] Acín, Brunner, Gisin, Massar, Pironio, Scarani, *Phys. Rev. Lett.* **98**, 230501

DIQKD based on the CHSH inequality[1]



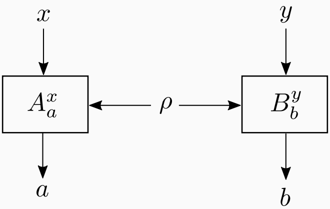
$x, a, b \in \{0, 1\}$, $y \in \{0, 1, 2\}$

Settings 0 and 1: certifying the setup (CHSH)

$$\rho = |\psi_-\rangle\langle\psi_-|, \quad A_0^0 = |0\rangle\langle 0|, \quad A_1^0 = |1\rangle\langle 1|$$

[1] Acín, Brunner, Gisin, Massar, Pironio, Scarani, *Phys. Rev. Lett.* **98**, 230501

DIQKD based on the CHSH inequality[1]



$x, a, b \in \{0, 1\}$, $y \in \{0, 1, 2\}$

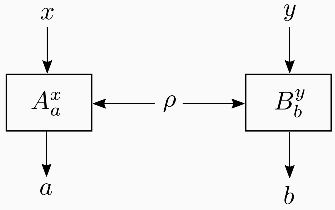
Settings 0 and 1: certifying the setup (CHSH)

$$\rho = |\psi_-\rangle\langle\psi_-|, \quad A_0^0 = |0\rangle\langle 0|, \quad A_1^0 = |1\rangle\langle 1|$$

Setting 2 for Bob: $B_0^2 = |0\rangle\langle 0|, B_1^2 = |1\rangle\langle 1|$

[1] Acín, Brunner, Gisin, Massar, Pironio, Scarani, *Phys. Rev. Lett.* **98**, 230501

DIQKD based on the CHSH inequality[1]



$x, a, b \in \{0, 1\}$, $y \in \{0, 1, 2\}$

Settings 0 and 1: certifying the setup (CHSH)

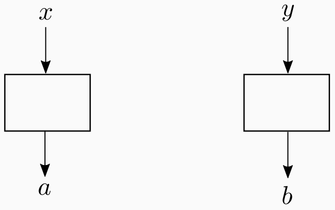
$$\rho = |\psi_-\rangle\langle\psi_-|, \quad A_0^0 = |0\rangle\langle 0|, \quad A_1^0 = |1\rangle\langle 1|$$

Setting 2 for Bob: $B_0^2 = |0\rangle\langle 0|, B_1^2 = |1\rangle\langle 1|$

$x = 0$ and $y = 2$: perfect randomness, perfect correlation

[1] Acín, Brunner, Gisin, Massar, Pironio, Scarani, *Phys. Rev. Lett.* **98**, 230501

Standard DIQKD protocol



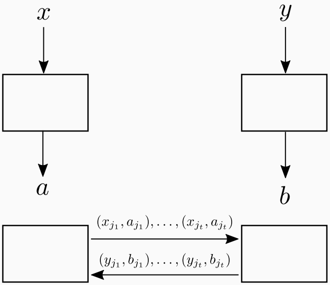
n rounds

$a_1, a_2, \ldots, a_n$

$b_1, b_2, \ldots, b_n$

$n \to \infty$

Standard DIQKD protocol



n rounds

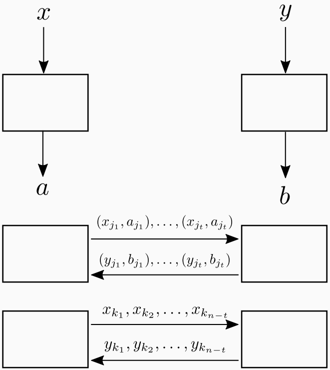
$$a_1, a_2, \dots, a_n$$

$$b_1, b_2, \dots, b_n$$

$$n \to \infty$$

$$p_{AB}(a, b|x, y)$$

Standard DIQKD protocol



n rounds

$a_1, a_2, \ldots, a_n$

$b_1, b_2, \ldots, b_n$

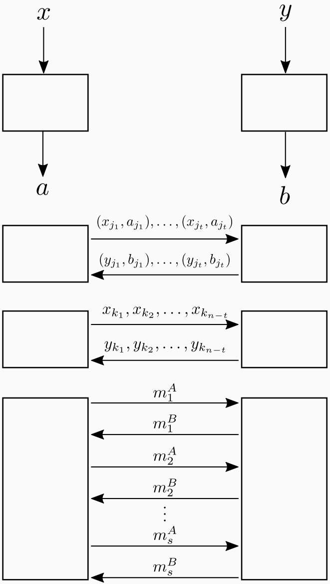
$n \to \infty$

$p_{AB}(a, b|x, y)$

input announcement

standard protocol

Standard DIQKD protocol



n rounds

$a_1, a_2, \ldots, a_n$

$b_1, b_2, \ldots, b_n$

$n \to \infty$

$p_{AB}(a, b|x, y)$

input announcement

standard protocol

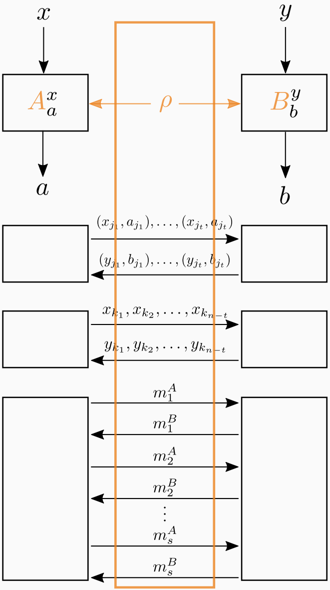
K_A, K_B

key rate: r

$$\frac{1}{n} I(K_A : K_B) > r - \epsilon$$

$$\frac{1}{n} I(\{m_j^A\}_j, \{m_k^B\}_k, E : K_A) < \epsilon$$

Eavesdropping – individual attacks



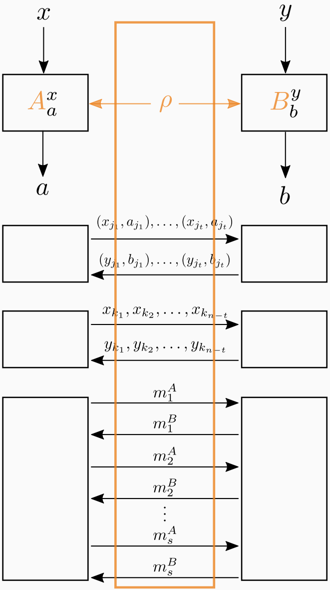
n rounds

$$\rho_1, \rho_2, \dots, \rho_n$$

$$\rho = \frac{1}{n} \sum_j \rho_j$$

$$p_{AB}(a, b|x, y) = \mathrm{tr}[\rho(A_a^x \otimes B_b^y)]$$

Eavesdropping – individual attacks



n rounds

$$\rho_1, \rho_2, \ldots, \rho_n$$

$$\rho = \frac{1}{n} \sum_j \rho_j$$

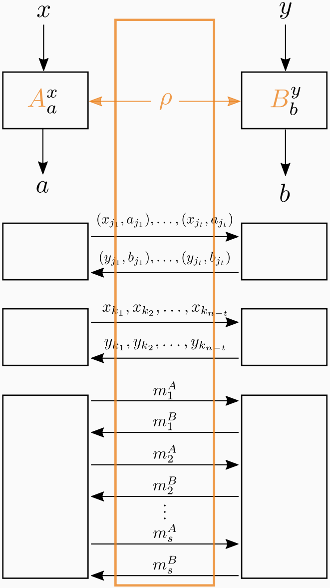
$$p_{AB}(a, b|x, y) = \mathrm{tr}[\rho(A_a^x \otimes B_b^y)]$$

Eavesdropper's information:

$$\left.\begin{matrix} \rho_j, A_a^x, B_b^y \\ x_{k_j}, y_{k_j} \end{matrix}\right\} e_{k_j}$$

$$p_{ABE}(a, b, e|x, y)$$

Eavesdropping – individual attacks



n rounds

$$\rho_1, \rho_2, \ldots, \rho_n$$

$$\rho = \frac{1}{n} \sum_j \rho_j$$

$$p_{AB}(a, b|x, y) = \mathrm{tr}[\rho(A_a^x \otimes B_b^y)]$$

Eavesdropper's information:

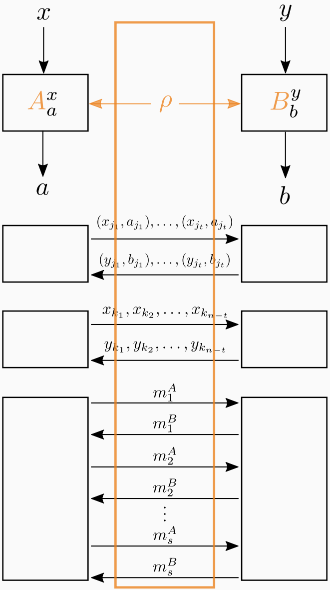
$$\left.\begin{array}{l} \rho_j, A_a^x, B_b^y \\ x_{k_j}, y_{k_j} \end{array}\right\} e_{k_j}$$

$$p_{ABE}(a, b, e|x, y)$$

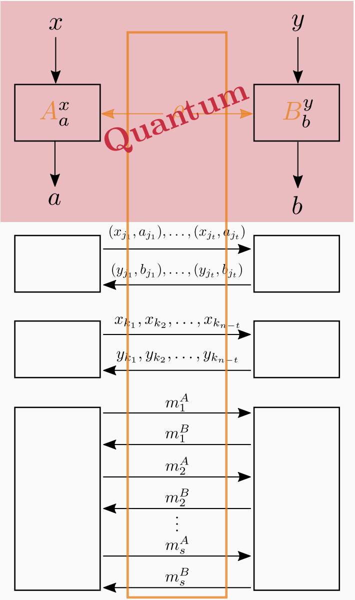
Key extraction:

$$m_1^A, \ldots, m_s^A, m_1^B, \ldots, m_s^B$$

Upper bounds



Upper bounds

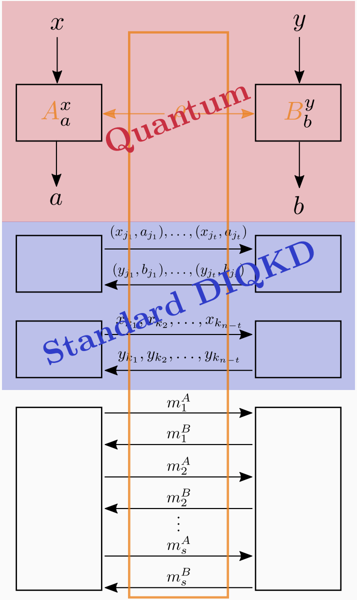


Quantum correlations

$p_{AB}(a, b|x, y)$

Which ones are useful?

Upper bounds



Quantum correlations

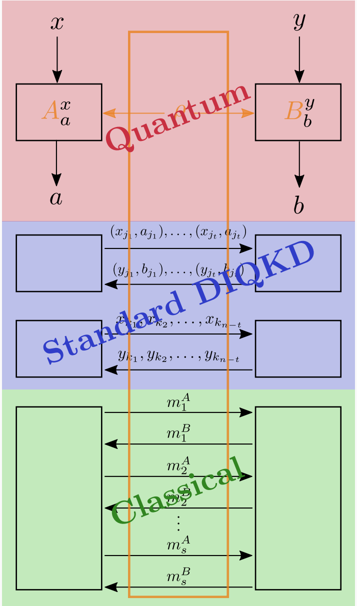
$p_{AB}(a, b|x, y)$

Which ones are useful?

Standard DIQKD

$\implies p_{ABE}(a, b, e|x, y)$

Upper bounds



Quantum correlations

$p_{AB}(a, b|x, y)$

Which ones are useful?

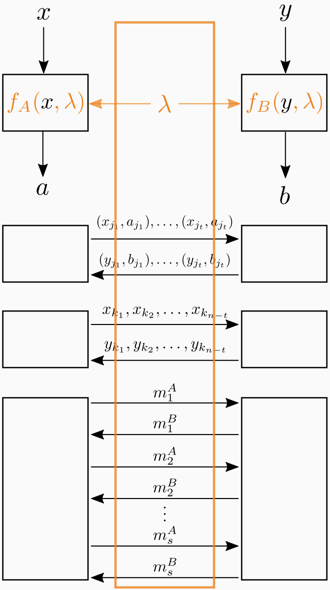
Standard DIQKD

$\implies \; p_{ABE}(a, b, e|x, y)$

Classical KD results

$r \leq I(A : B \downarrow E)$

Bell nonlocality is necessary



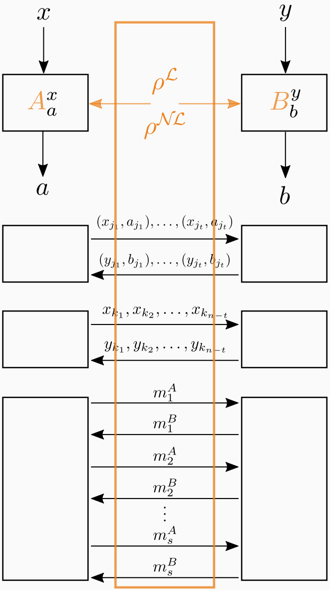
$$p_{AB}^{\mathcal{L}}(a,b|x,y) = \sum_\lambda p_\Lambda(\lambda)\delta_{a,f_A(x,\lambda)}\delta_{b,f_B(y,\lambda)}$$

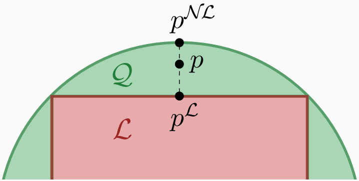
Bell nonlocality is not sufficient

Specific eavesdropping attack

Specific (large) family of nonlocal correlations

The convex combination attack

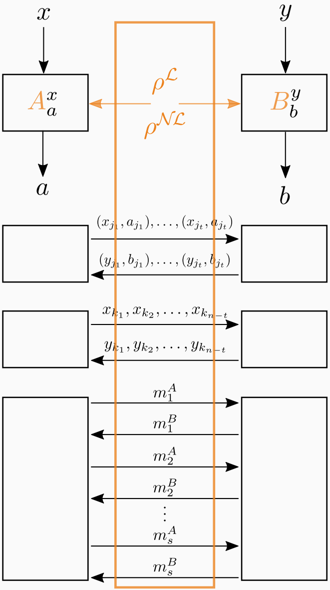


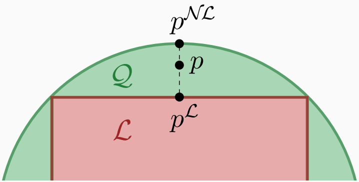


Observed correlation:

$$p = q_{\mathcal{L}} p^{\mathcal{L}} + (1 - q_{\mathcal{L}}) p^{\mathcal{NL}}$$

The convex combination attack



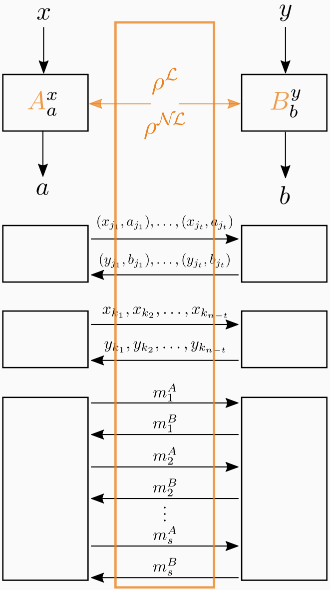


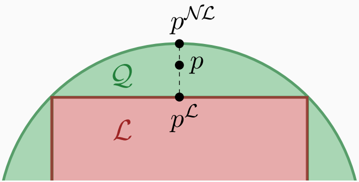
Observed correlation:

$$p = q_{\mathcal{L}} p^{\mathcal{L}} + (1 - q_{\mathcal{L}}) p^{\mathcal{NL}}$$

$$\rho = q_{\mathcal{L}} \rho^{\mathcal{L}} + (1 - q_{\mathcal{L}}) \rho^{\mathcal{NL}}$$

The convex combination attack





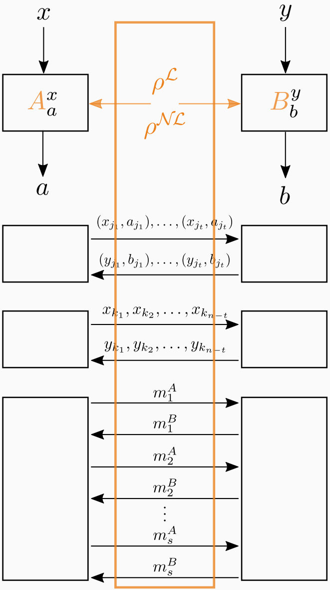
Observed correlation:

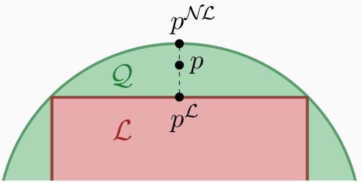
$$p = q_{\mathcal{L}} p^{\mathcal{L}} + (1 - q_{\mathcal{L}}) p^{\mathcal{NL}}$$

$$\rho = q_{\mathcal{L}} \rho^{\mathcal{L}} + (1 - q_{\mathcal{L}}) \rho^{\mathcal{NL}}$$

$$\implies p_{ABE}(a, b, e|x, y)$$

The convex combination attack





Observed correlation:

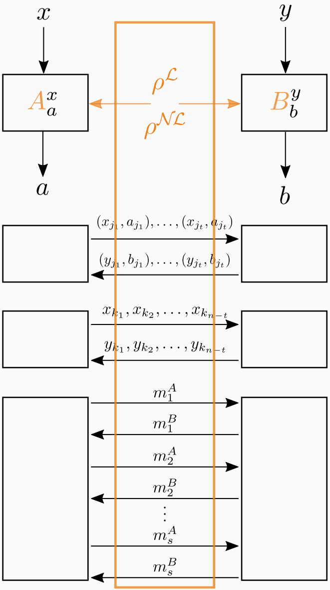
$$p = q_{\mathcal{L}} p^{\mathcal{L}} + (1 - q_{\mathcal{L}}) p^{\mathcal{NL}}$$

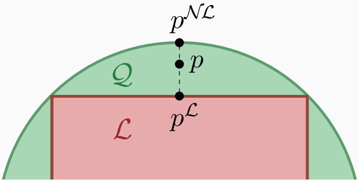
$$\rho = q_{\mathcal{L}} \rho^{\mathcal{L}} + (1 - q_{\mathcal{L}}) \rho^{\mathcal{NL}}$$

$$\Longrightarrow \; p_{ABE}(a, b, e | x, y)$$

Maximising $q_{\mathcal{L}}$: linear program

The convex combination attack





Observed correlation:

$$p = q_{\mathcal{L}} p^{\mathcal{L}} + (1 - q_{\mathcal{L}}) p^{\mathcal{NL}}$$

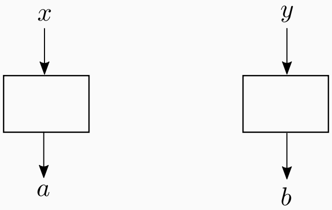
$$\rho = q_{\mathcal{L}} \rho^{\mathcal{L}} + (1 - q_{\mathcal{L}}) \rho^{\mathcal{NL}}$$

$$\implies p_{ABE}(a, b, e|x, y)$$

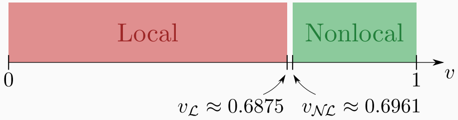
Maximising $q_{\mathcal{L}}$: linear program

$$r \leq I(A : B \downarrow E)$$

Protocols with Werner states and projective measurements

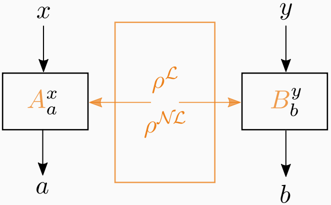


$$p_{AB}(a,b|x,y) = \mathrm{tr}[(v|\psi_-\rangle\langle\psi_-| + (1-v)\tfrac{\mathbb{I}}{4})(A_a^x \otimes B_b^y)]$$



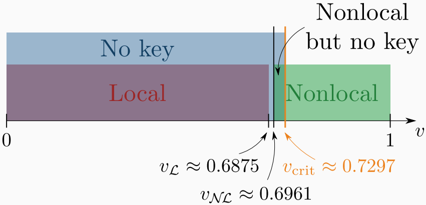
Designolle, Iommazzo, Besançon, Knebel, Gelß, Pokutta, arXiv:2302.04721
(see poster no. 5, Sébastien Designolle)

Convex combination attack



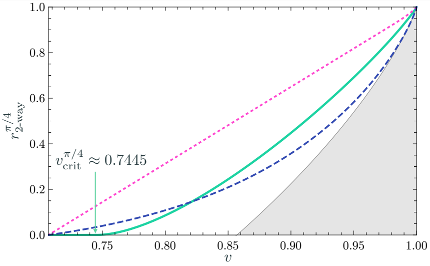
$$\rho^{\mathcal{L}} = v_{\mathcal{L}}|\psi_-\rangle\langle\psi_-| + (1 - v_{\mathcal{L}})\frac{\mathbb{I}}{4},\ \rho^{\mathcal{NL}} = |\psi_-\rangle\langle\psi_-|$$

$$q_{\mathcal{L}} = (1 - v)/(1 - v_{\mathcal{L}})$$



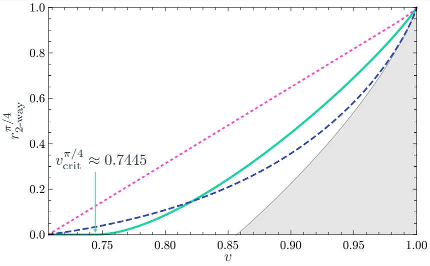
Implications and limitations

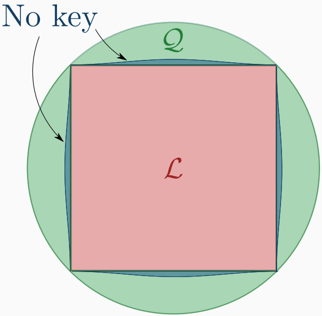
All the commonly used protocols become insecure while still exhibiting nonlocality



Implications and limitations

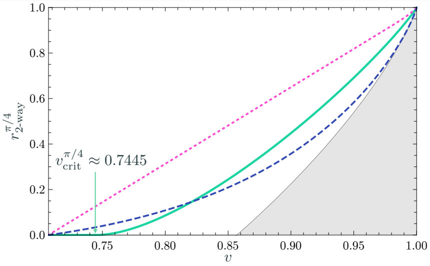
All the commonly used protocols become insecure while still exhibiting nonlocality

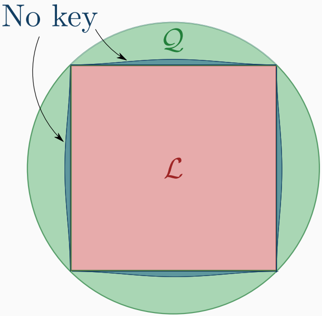




Implications and limitations

All the commonly used protocols become insecure while still exhibiting nonlocality

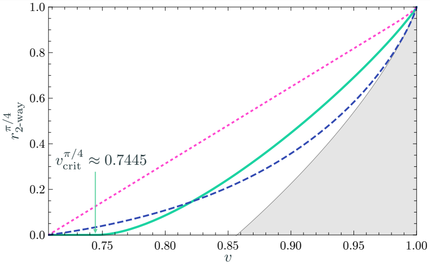


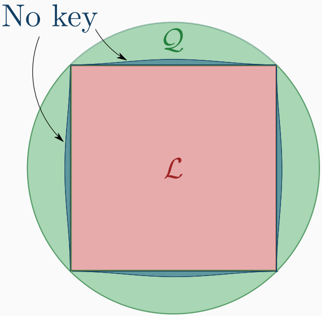


What if only one party announces their settings?

Implications and limitations

All the commonly used protocols become insecure while still exhibiting nonlocality



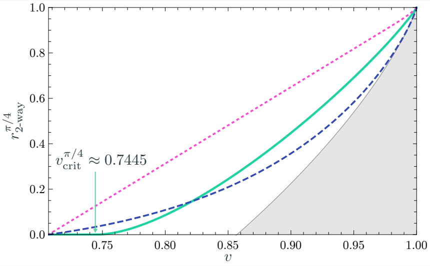


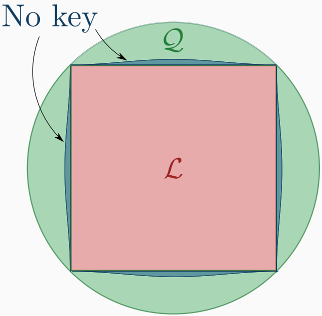
What if only one party announces their settings?

Multiple parties? (see poster no. 22, Jan Nöller)

Implications and limitations

All the commonly used protocols become insecure while still exhibiting nonlocality





What if only one party announces their settings?

Multiple parties? (see poster no. 22, Jan Nöller)

Thank you!