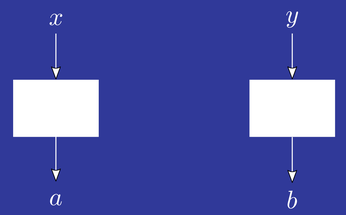
Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols

Máté Farkas, Maria Balanzó-Juandó, Karol Łukanowski, Jan Kołodyński and Antonio Acín

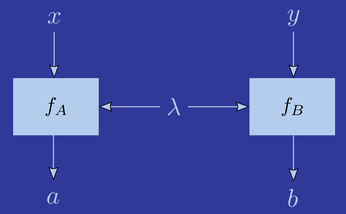
ICFO, UNIVERSITY OF WARSAW

Nonlocal scenario



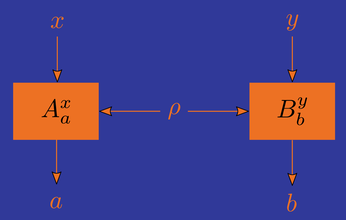
$$p_{AB}(a,b|x,y)$$

Local model $\mathcal{L}$

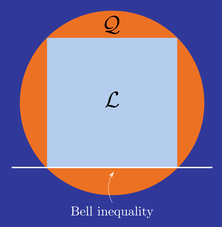


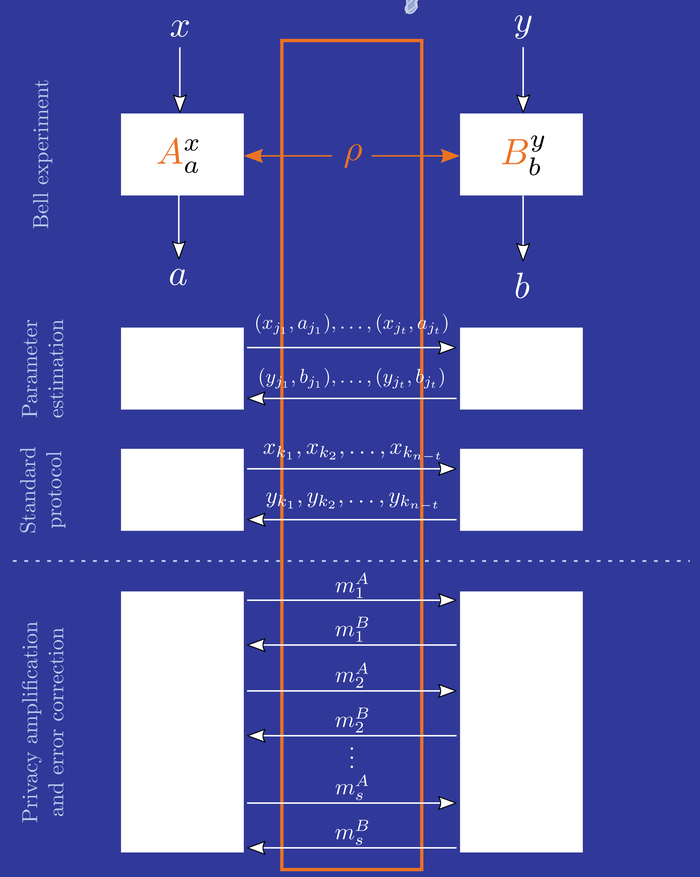
$$p_{AB}(a,b|x,y) = \sum_\lambda p_\Lambda(\lambda)\delta_{a,f_A(x,\lambda)}\delta_{b,f_B(y,\lambda)}$$

Quantum model $\mathcal{Q}$



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



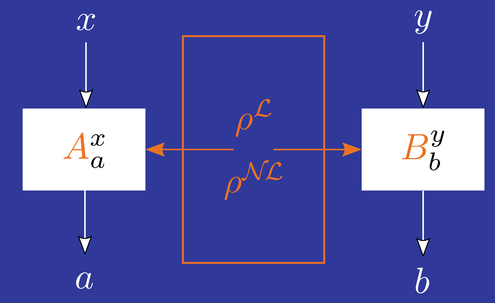


Eavesdropper's information: $\rho,\ A_a^x,\ B_b^y \implies e$

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

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

Convex combination attack



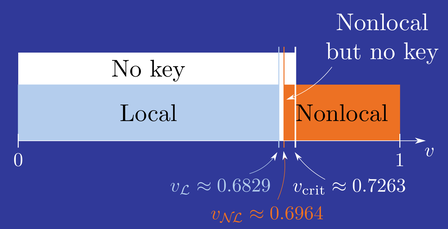
$$p_{ABE}(a,b,e|x,y) = q_{\mathcal{L}} \cdot p^{\mathcal{L}}_{AB}(a,b|x,y)\cdot\delta_{e,(a,b)} + (1-q_{\mathcal{L}})\cdot p^{\mathcal{NL}}_{AB}(a,b|x,y)\cdot\delta_{e,?}$$

Werner state protocols

$$\rho = v|\psi_-\rangle\langle\psi_-| + (1-v)\frac{\mathbb{I}}{4}$$

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

A_a^x and B_b^y are projective



Hirsch et al., *Quantum* **1**, 3 (2017)

Diviánszky, Bene, Vértesi, *Phys. Rev. A* **96**, 012113 (2017)

CHSH-based protocols