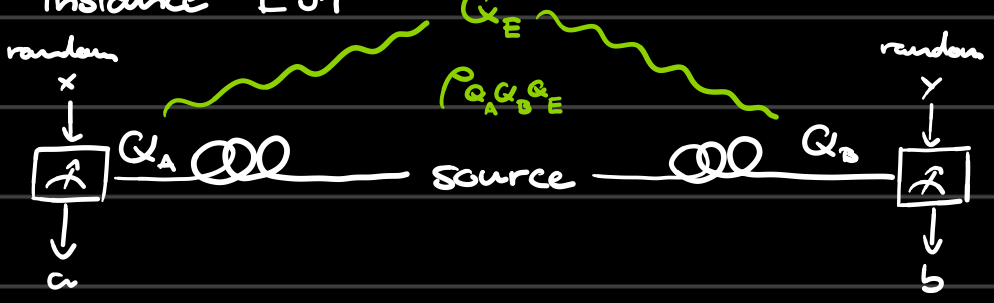
Device-independent QKD

Motivation: Traditional QKD systems require accurate modeling of devices (implementation security)

$\rightsquigarrow$ Relax device assumptions

Take, for instance E91



Alice measures $\{\overbrace{|0\rangle\langle 0|}^{a=0}, \overbrace{|1\rangle\langle 1|}^{a=1}\}$ if $x=0$

and $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ if $x=1$

Same for Bob

Observation: Assume that Alice and Bob observe perfect correlations when picking $x=y$

$\Rightarrow$ They share a state s.t.

$$\mathrm{tr}[\rho(\sigma_x \otimes \sigma_x)] = \mathrm{tr}[\rho(\sigma_z \otimes \sigma_z)] = 1$$

$\Rightarrow$ $\rho_{Q_A Q_B} = |\Psi\rangle\langle\Psi|$, $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

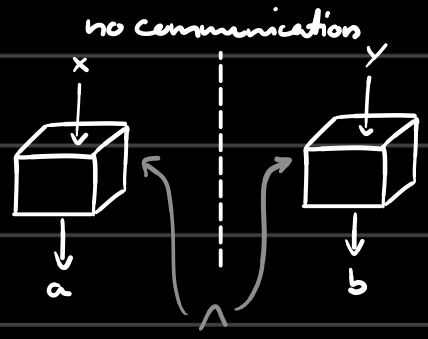
↖ only true if they really measure σ_x and σ_z

Hence $\mathrm{tr}_{Q_E}[\rho_{Q_A Q_B Q_E}] = |\Psi\rangle\langle\Psi|_{Q_A Q_B}$ (pure)

$\Rightarrow$ $\rho_{Q_A Q_B Q_E} = |\Psi\rangle\langle\Psi|_{Q_A Q_B} \otimes \rho_{Q_E}$

Goal: Certify $\mathrm{tr}_{Q_E}[\rho_{Q_A Q_B Q_E}] = |\Psi\rangle\langle\Psi|_{Q_A Q_B}$ using unknown measurements (black-box approach)

Background: Bell inequalities



$p(ab|xy)$

Motivation: Is randomness in QM due to lack of knowledge ?

$$p(ab|xy) = \sum_\lambda p(ab\lambda|xy) = \sum_\lambda \underbrace{p(a|xyb\lambda)}_{p(a|x\lambda)\ \text{locality}} \underbrace{p(b|xy\lambda)}_{p(b|y\lambda)} \overbrace{p(\lambda|xy)}^{\text{free choice}} = \frac{p(xy|\lambda)}{p(xy)} p(\lambda) = p(\lambda)$$

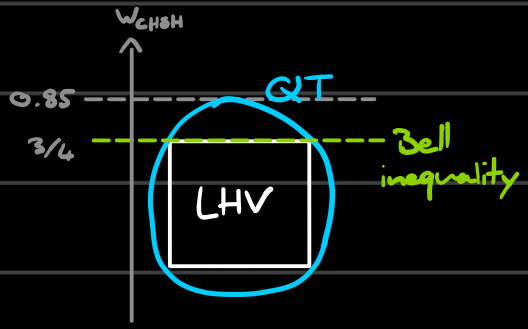
$$= \sum_\lambda \underbrace{p(a|x\lambda)}_{\text{w.l.o.g. deterministic}} p(b|y\lambda)\, p(\lambda) \qquad \text{(LHV)}$$

$$p(ab|xy) = \mathrm{tr}\left[M_{a_A}(a|x) \otimes N_{a_B}(y|b)\, \rho_{a_A a_B}\right] \qquad \text{(QT)}$$

Question: Can we separate (LHV) from (QT) ?

Answer: Yes ! (Bell 1964)

Consider $w_{CHSH} = \sum_{x,y \atop a,b} \underbrace{\delta_{a\oplus b = x\cdot y}}_{\text{win if } a\oplus b = x\cdot y} p(ab|xy)\, \frac{1}{4}$



For (LHV): $w_{CHSH}^{(LHV)} \leq \frac{3}{4}$

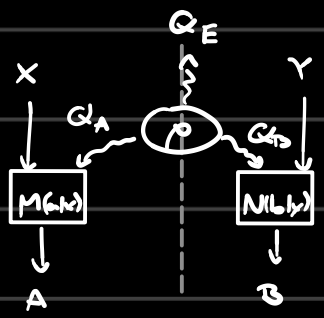
(QT): $w_{CHSH}^{(QT)} \leq \frac{2+\sqrt{2}}{4} \simeq 0.85$

What's more, to achieve the value $\frac{2+\sqrt{2}}{4}$, one requires

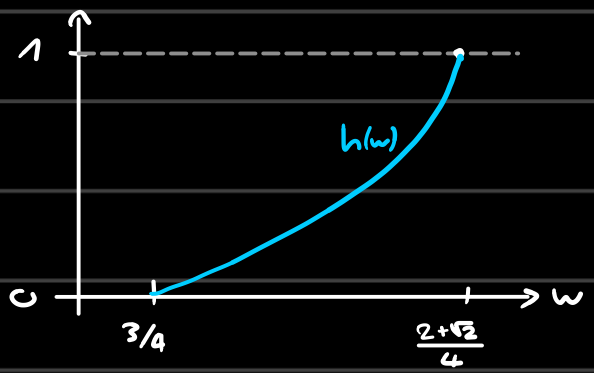
$$\rho_{Q_A Q_B} = |\Psi\rangle\langle\Psi|_{Q_A Q_B} \qquad |\Psi\rangle_{Q_A Q_B} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

But even for $w_{CHSH}^{(LHV)} < w_{CHSH} \leq w_{CHSH}^{(QT)}$ there cannot be a LHV model to predict A perfectly.

~> Make this quantitative



$$h(w) = \min_{\rho,M,N} H(A|X=0, Q_E) \quad \text{s.t. } w(\rho,M,N) \geq w$$



Pironio et al. 2009

Loopholes

1.) Locality loophole

2.) Free choice loophole

3.) Detection loophole

4.) Isolation loophole

DIQKD protocols

1. Quantum phase
   - For $i = 1, \dots, n$ Alice & Bob pick random inputs x_i & y_i and obtain outputs
2. Classical phase
   - Announce a random subset of x_i, y_i, a_i, b_i
   - Check that the fraction of won CHSH games is above w^th
   - Use remaining a_i as raw key (for privacy amplification)
   - Perform error-correction and privacy amplification

Proof sketch

1. By leftover hashing lemma it remains to bound $H_{\min}^{\varepsilon}(A^n|X^nE)$
2. Apply the EAT to get

$$H_{\min}^{\varepsilon}(A^n|X^nE) \geq \sum_i \inf_{A^{i-1}E} H(A_i|A^{i-1}X^iE) - O(\sqrt{n})$$

3. The entropy of a single round is bounded

$$\inf_{A^{i-1}E} H(A_i|A^{i-1}X^iE) \geq h(w^{th})$$

In total: $\ell \approx n h(w^{th}) - n H(A|B)$

error correction cost

Device-independence beyond QKD

Bell-tests are useful for more than just QKD

Examples

1. DI randomness expansion:

   Few uniform bits $\Rightarrow$ Many uniform bits

2. DI randomness amplification:

   Many non-uniform bits $\Rightarrow$ Fewer uniform bits

3. DI with computational assumptions

   Replace non-signalling with computational assumptions