Mittwoch, 27. Januar 2016 08:46

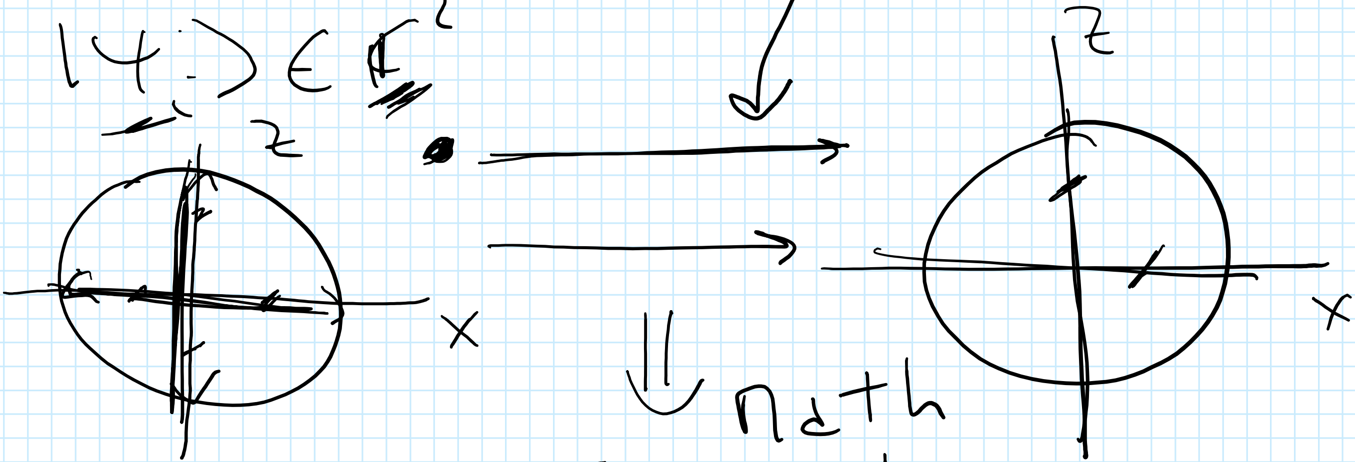
Eve

BB84

Alice

$|\psi\rangle \in \mathbb{C}^2$

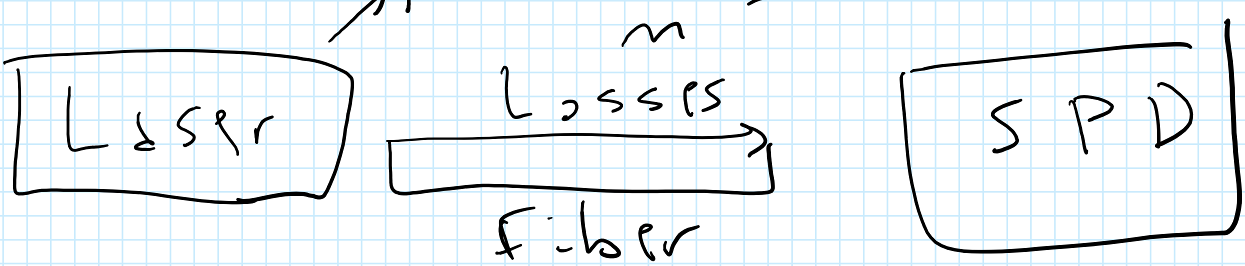
Bob



$\Downarrow$ Math Security Proof

Implementation

Alice $|\alpha\rangle = \sum_n \alpha_n |n\rangle$ Bob



Photon-Number Splitting Attack

$\alpha_0 > \alpha_1 > \alpha_2 > \dots$

$\alpha_0 > \alpha_1 > \alpha_2 > \dots$

a) Measures the number the photons

If $n=0$

If $n=1$ she blocks

If $n=2$ → She keeps one

→ She sends the second through an ideal channel

↓

She gets the information

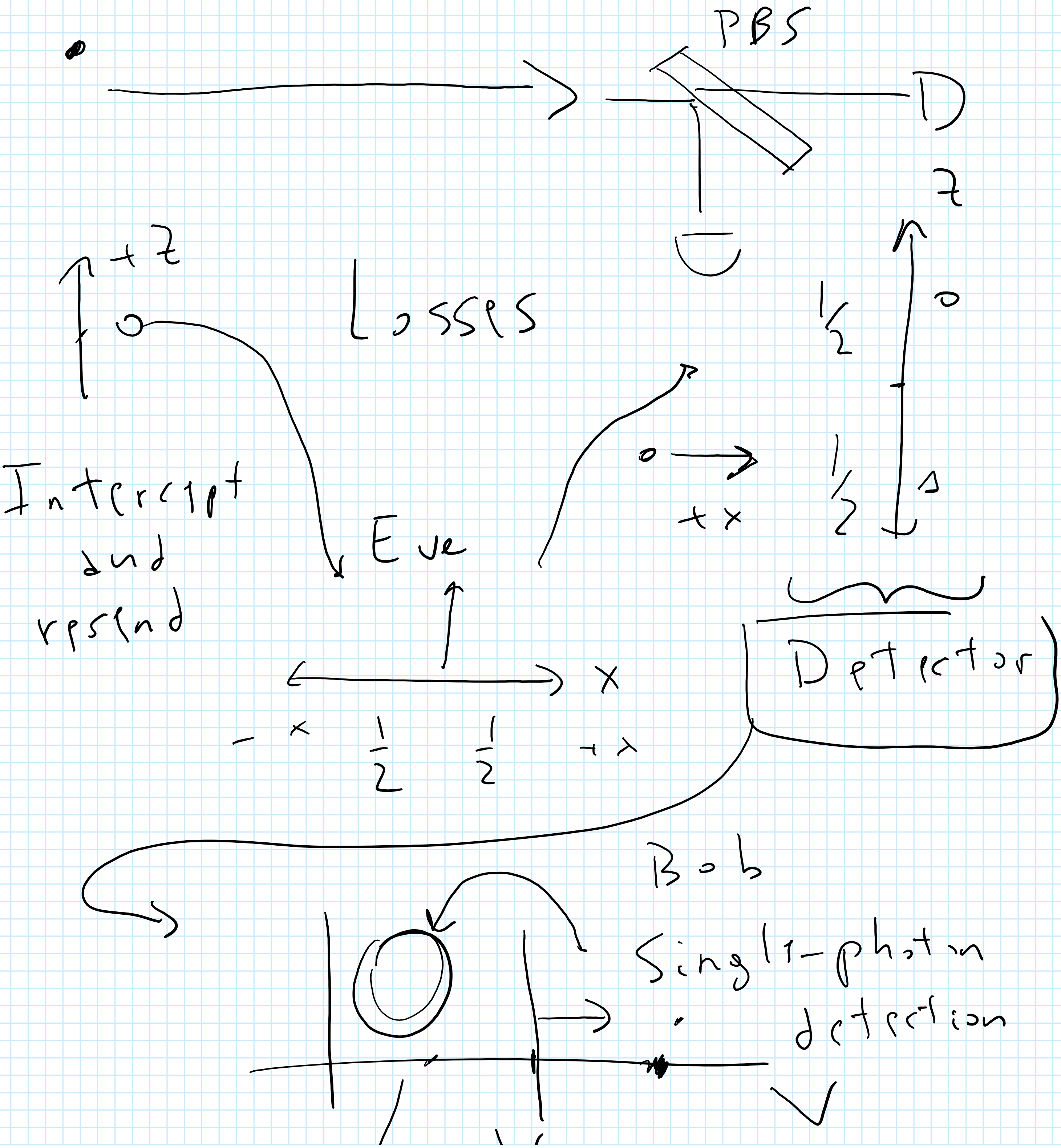
$P_2 \simeq \eta$ = channel losses

Decoy-state solves the

PNS attack.

Alice | **Bob**

ok | Detector



Ver

linear regime

$I > I_{th}$

$\Downarrow$

click

Alice

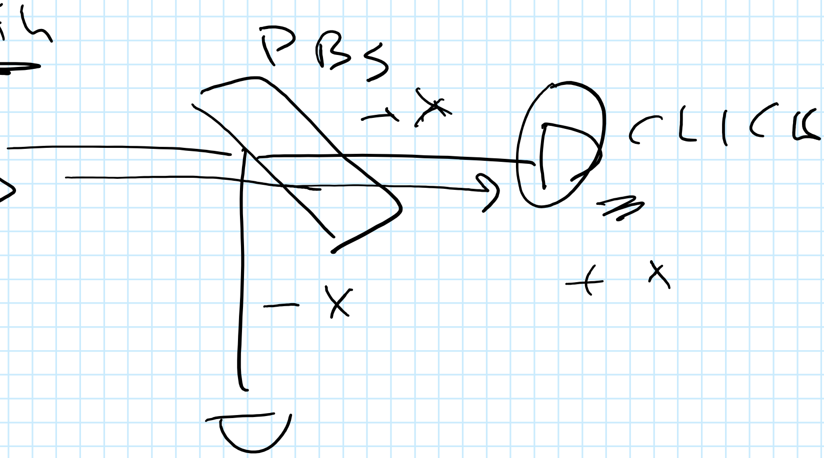
Eve

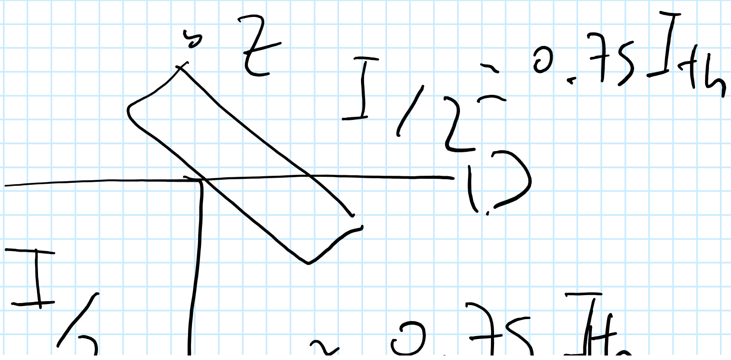
x

+x

$1.5\, I_{th}$

Bob



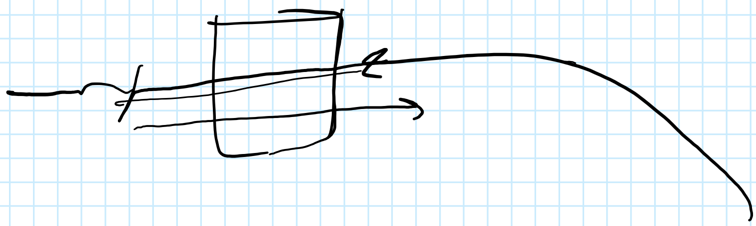


$\frac{1}{2}$ ... ≈ 0.75 Ith

Trojan horse attack

Alice

Encode information

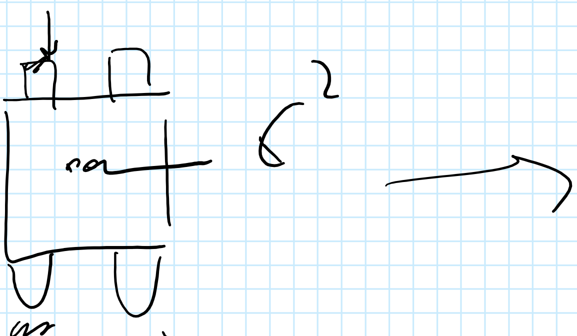


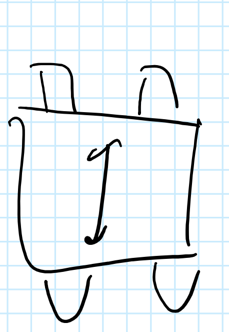
$|\psi\rangle \in \mathbb{C}^2$

Theory Requirements $\overset{?}{\Longleftrightarrow}$ Implementation

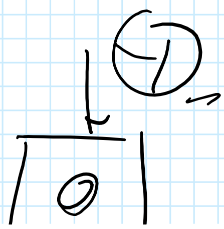
Alice

Bob





$p(ab|xy)$



$x = 1, 2$ $\qquad$ $y = 1, 2$

$a = \pm 1$ $\qquad$ $b = \pm 1$

$p(+1, +1 \mid 11)$ $\quad$ $p(+-)$ $\quad$ $p(-+)$ $\quad$ $p(--)$

$12 \quad 12 \quad 12$

$n = 16$

$$p(ab \mid xy) \in \mathbb{R}^{n}$$

Secure

$p(ab \mid xy) \longrightarrow$ Key

$x \qquad y$

$a \qquad b$

$$p(ab \mid xy) = \langle \psi \mid \Pi_{a|x} \otimes \Pi_{b|y} \mid \psi \rangle$$

?

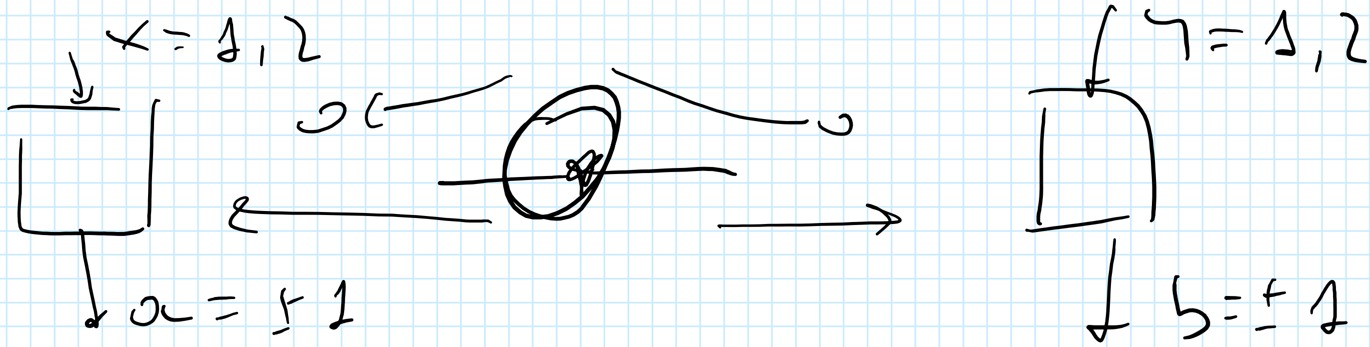
C

$\Downarrow$

Physical principles $\Longrightarrow$ Structure to correlations

$p(ab|xy)$

Bell inequality



$p(ab|xy)$

If $x = 1$ $\quad a = +1$

$x = 2$ $\quad a = -1$

If $y = 1$ $\quad b = +1$

$y = 2$ $\quad b = +1$

$A_1 = +1$, $A_2 = -1$ $\quad$ LHV

CHSH

LHV $\quad B_1 = +1$, $B_2 = +1$

$$S = A_1 B_1 + \underline{A_1 B_2} + A_2 B_1 - A_2 B_2 = +2$$

$+1 \quad +1 \quad -1 \quad -1$

$= \pm 2$

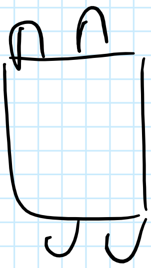
—

$E(S) \leq 2$

Bell inequalities are violated

$S = 2\sqrt{2}$!! z

DIQKD



problem

$\downarrow$

Bell inequality

$\downarrow$ Secure key

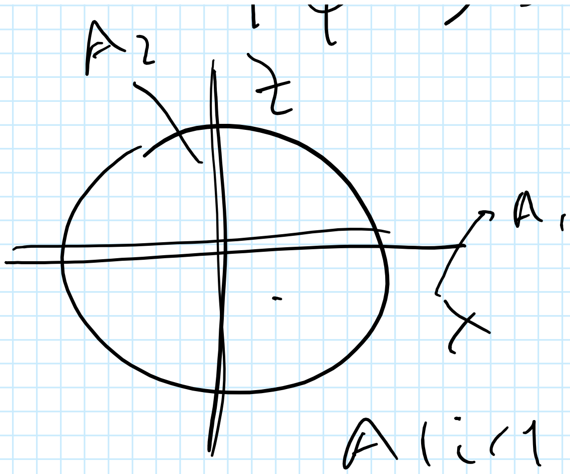
$S \leq 2$ $\qquad$ $\underline{S_Q = 2\sqrt{2}}$

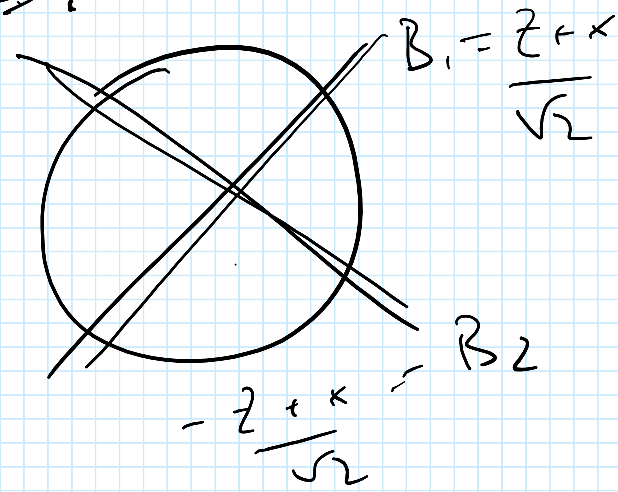
Tsirelson

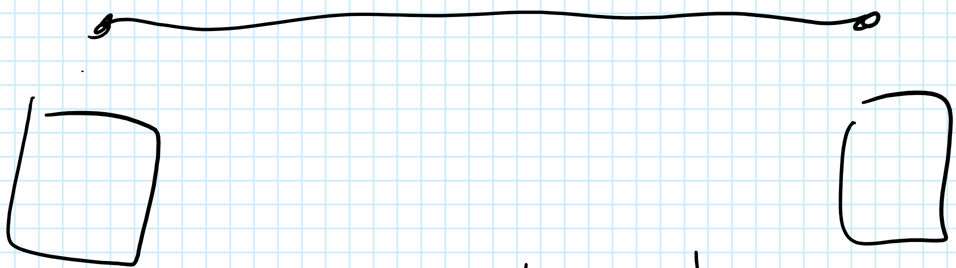
$\underline{S_Q = 2\sqrt{2}}$ $\qquad$ self-testing

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{AB}$$

A_1^2 ... $B_1 = Z + X$



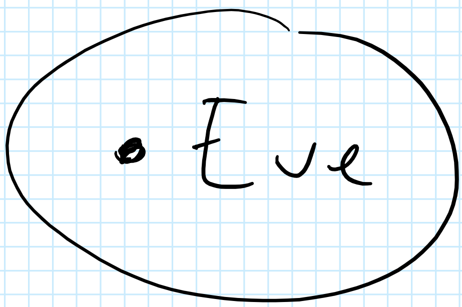




$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Alice Bob

$\otimes$



$$\rho_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

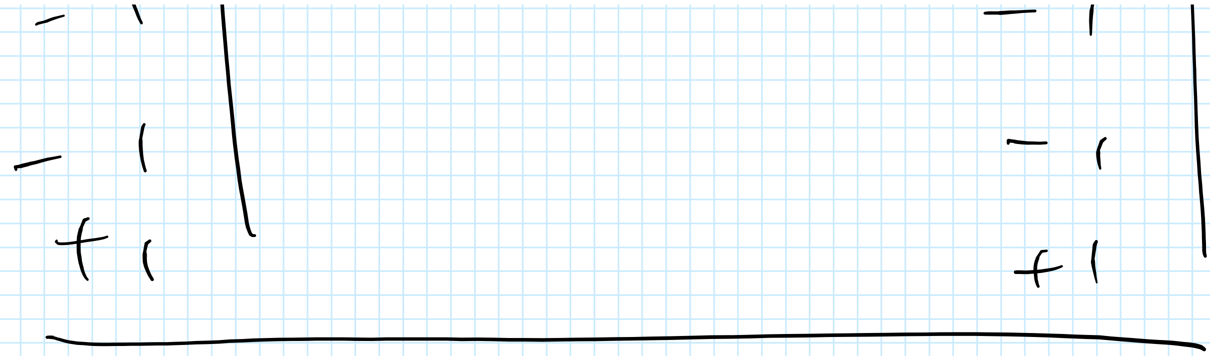
$P(+1) = \frac{1}{2}$ $\quad P(-1) = \frac{1}{2}$

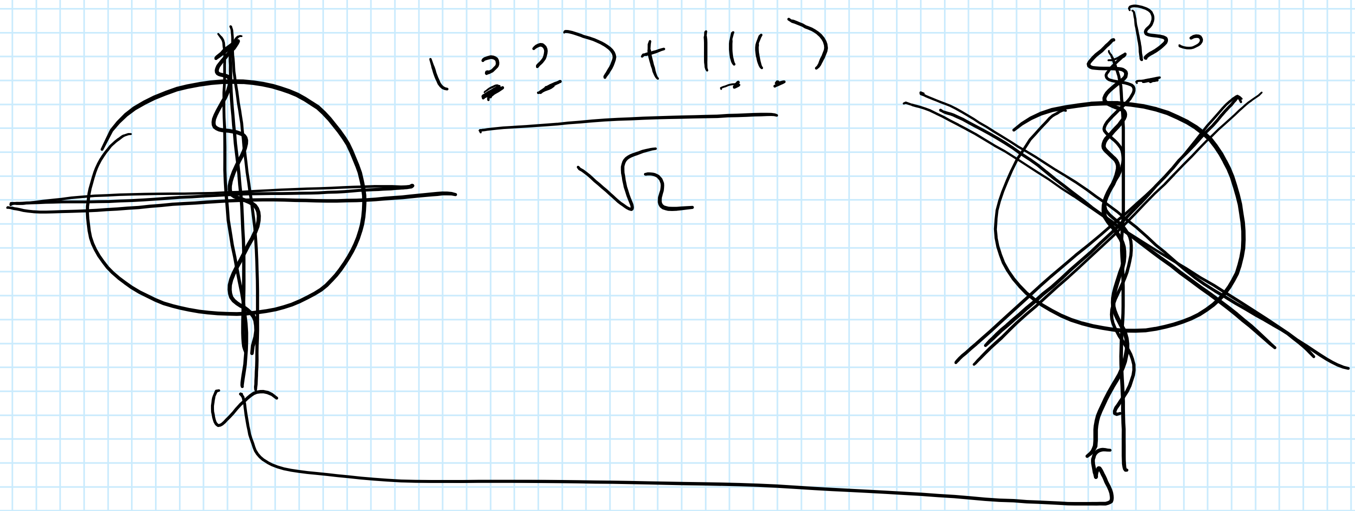
$+1$ $\quad$ $+1$

-1 $\quad$ -1

$2\sqrt{2}$

-1 $\quad$ -1



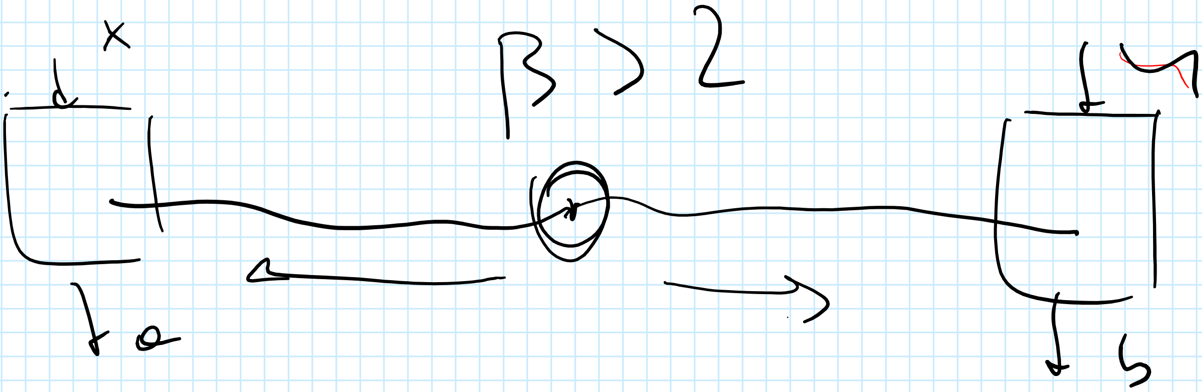


$$S_a = 2\sqrt{2}$$

$$2 < \beta < S_a = 2\sqrt{2} - \varepsilon$$

Miller & Shi

$$\beta > 2$$



$\longleftarrow L \approx 10\,km \longrightarrow$

$\longleftarrow \quad L \approx 10\,\text{km} \quad \longrightarrow$

20

$a = +1, -1, \emptyset$ $\qquad$ $b = +1, -1, \emptyset$

$p(ab|xy) \quad 2 \sqrt{2}$

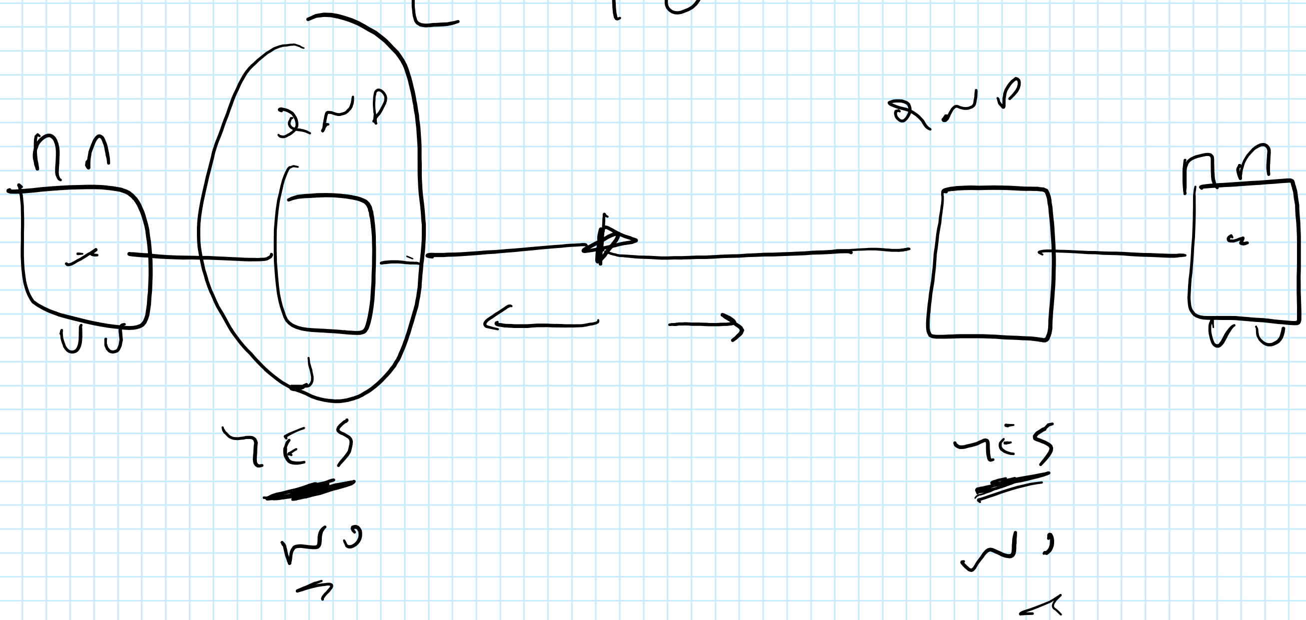
η losses are moderate

$\downarrow$

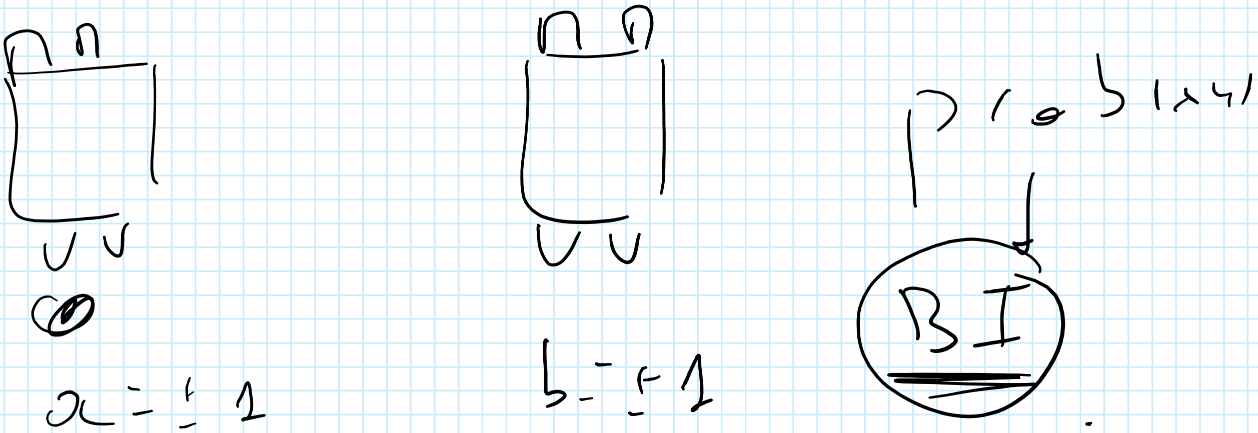
$p(ab|xy)$ don't violate any Bell inequality

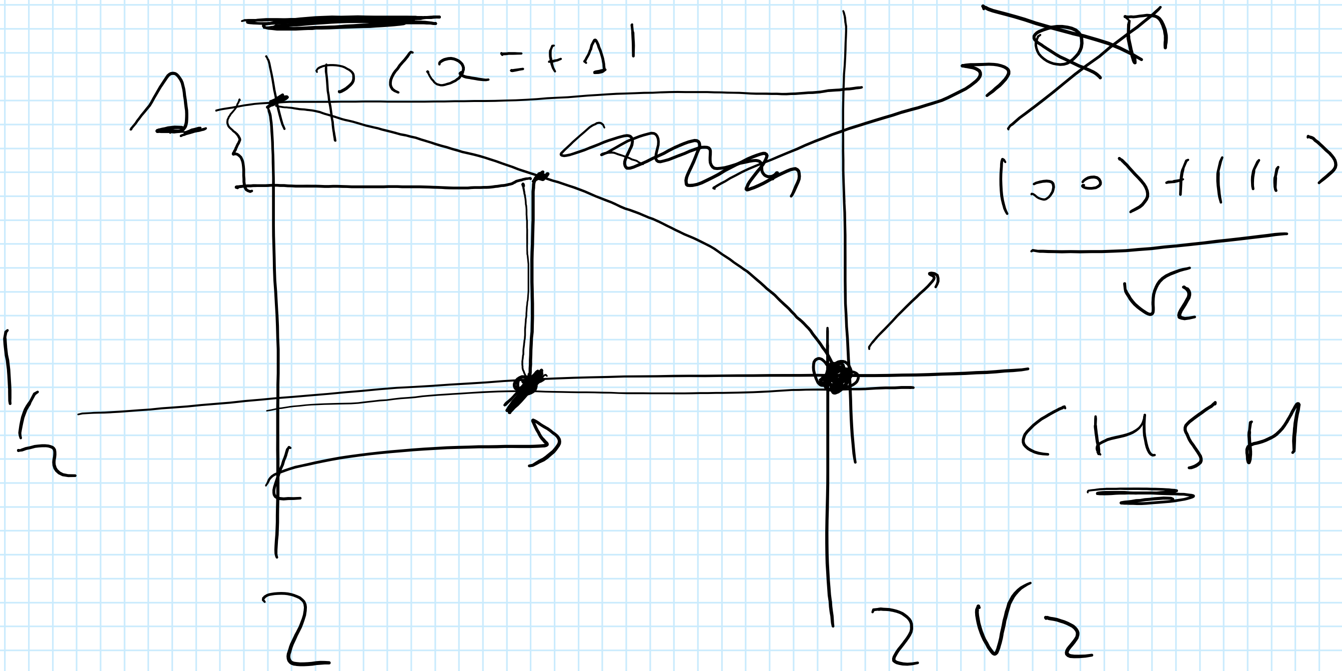
CHSH $\qquad \eta = \frac{2}{3} = 0.66\ldots$

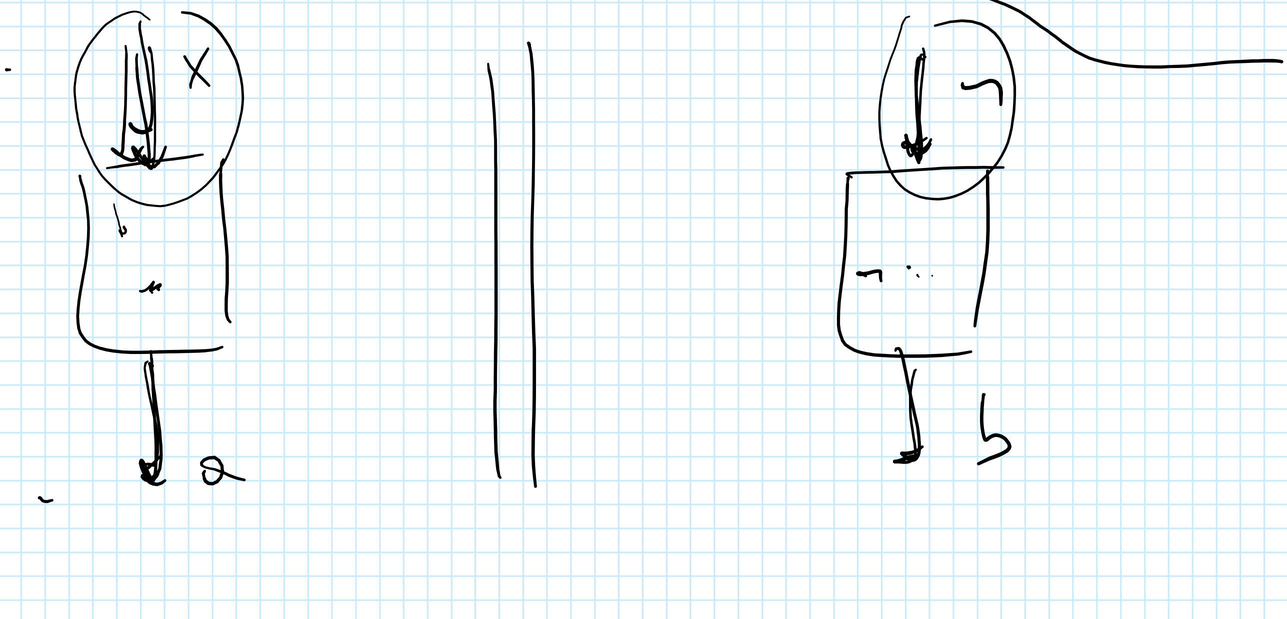
$L = 10^{-\frac{\alpha L}{10}}$ 13 km



Randomness generation







$a_1 \quad a_2 \quad \ldots \quad a_N$

$\boxed{H|_{min} \geq K = g(B7)} \quad \overline{\|Sccd\|}$

$\bar{a} \quad \ldots \quad \bar{a}_K$