BELL INEQUALITIES.

The so-called Bell inequalities provide a kind of "certificate" that Alice & Bob can check upon communicating classically (or meeting) to decide if they share entangled states.

There exist today a whole set of such inequalities depending what are the measured observables, the number of parties (A, B, C ...), the shared entanglement ect...

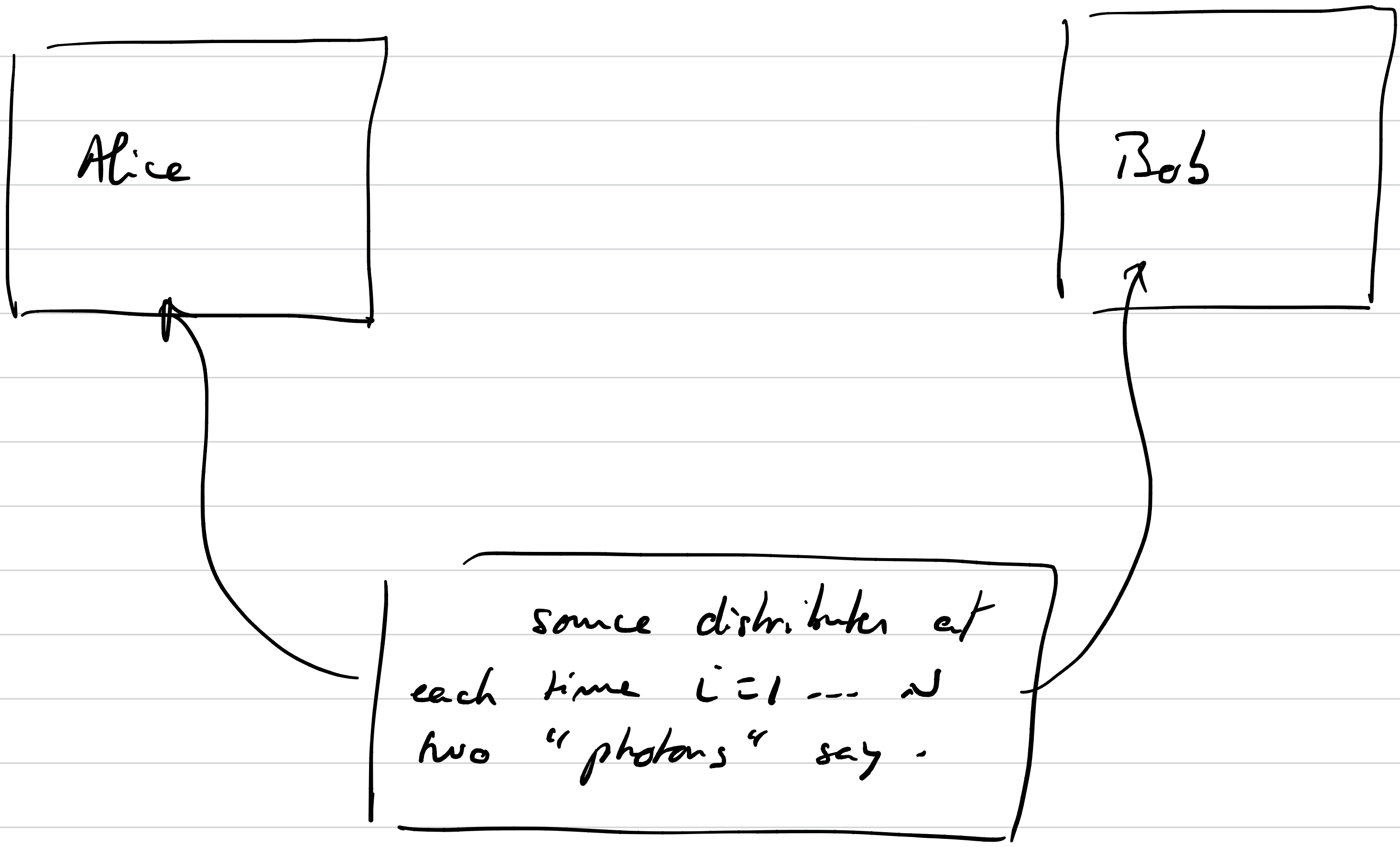
Here we go through the simplest such "Bell inequality" due in fact to Clauser - Horne - Shimony - Holt (CHSH). They have been tested in famous experiments (notably of Aspect - Grangier - Roger).

In a second stage we discuss a cryptographic application, the Ekert 91 protocol, for generating a one-time-pad common to Alice & Bob.

We note that the subject has a long history. John Bell was the first to propose in the 60's precise experiment to test the predictions of QM and notably the ones deriving from entanglement. The whole subject was heavily influenced by a famous paper of Einstein - Podolsky - Rosen (1935). For this reason entangled particles in Bell states are also called EPR pairs.

I. CHSH inequality

a) Experimental setting:



- At each time $i = 1 \dots N$ a source distributes a "pair of particles" (say photons). In the quantum experiment it distributes pairs in the state

$$|B_{00}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \right)$$

(but for the moment lets be agnostic about this.).

- Alice does local Measurements. At each time $i = 1 \dots N$ she chooses at random a Measurement basis

$$\{|\alpha\rangle, |\alpha_\perp\rangle\} \quad \text{or} \quad \{|\alpha'\rangle, |\alpha'_\perp\rangle\}$$

(say with analyser-photodetector apparatus).

She registers her Meas Result (click, no click) in a random variable $a = \pm 1$ or $a' = \pm 1$.

- Idem for Bob. with Meas basis

$$\{|\beta\rangle, |\beta_\perp\rangle\}, \quad \text{or} \quad \{|\beta'\rangle, |\beta'_\perp\rangle\}$$

and registers the r.v $b = \pm 1$ or $b' = \pm 1$.

- We denote each Meas basis type of choice by $1 = (\alpha, \beta)$ $\quad 2 = (\alpha, \beta')$ $\quad 3 = (\alpha' \beta)$

$4 = (\alpha' \beta')$.

- Alice and Bob collect their Meas results. These have been performed without communication. After all measurements they meet (or communicate) their results and compute the following "<u>Correlation coefficient</u>":

$$X_{\text{experimental}} = \frac{1}{N_1} \sum_{m_1} a_{m_1} b_{m_1} + \frac{1}{N_2} \sum_{m_2} a_{m_2} b'_{m_2}$$

$$- \frac{1}{N_3} \sum_{m_3} a'_{m_3} b_{m_3} + \frac{1}{N_4} \sum_{m_4} a'_{m_4} b'_{m_4} .$$

b) Theoretical prediction according to "classical physics" (so-called "local hidden variable theories").

We first explain what "classical physics" would predict under "reasonable" and very general assumption about a very wide set of theories often called "local hidden variable theories".

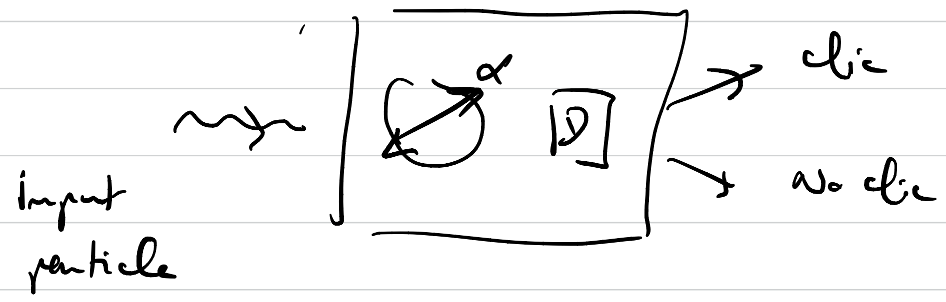
* We assume that the random outcome of Alice is described by a transition probability of the form

$$P_A(a \mid \alpha, \lambda)$$

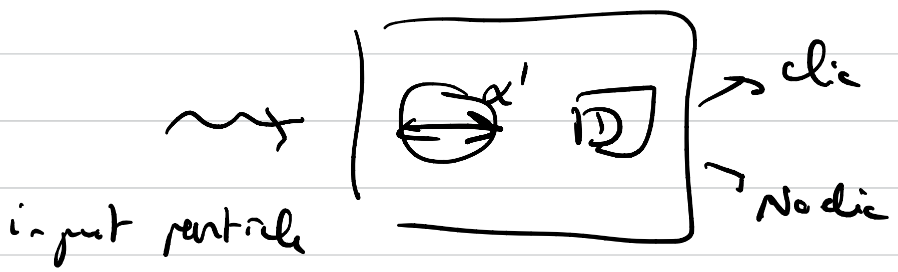
$$\alpha \longrightarrow \boxed{A} \longrightarrow a = \pm 1$$

α = choice of basis analyser

binary output click/no click in photo detector



$P_A(a \mid \alpha, \lambda)$



$P_A(a' \mid \alpha' \lambda)$

Here λ denote a collection of so-called "hidden variables" describing or characterising the "state" of the source of the pairs. These are modelled as random variables (that could change values at each $i = 1 \dots N$ but independently of basis choices of A & B). We suppose that λ are distributed according to some pdf $h(\lambda)$ st $h(\lambda) \geq 0$ and $\int h(\lambda) d\lambda = 1$.

* We assume the same for the outcomes of Bob. They are described by a transition probability

$$P_B(b \mid \beta, \lambda).$$

* The important & crucial point is that the description of A & B is <u>local</u>. This means that a (or a') depends only on α & λ (or α' & λ) and not on β & β'. Idem on the side of Bob.

Locality assumption can be expressed more formally as follows:

$$\text{prob}(a, b \mid \alpha, \beta, \lambda) = P_A(a \mid \alpha, \lambda)\, P_B(b \mid \beta, \lambda)$$

Of course this equation apply to all four settings $1 = (\alpha, \beta)$, $2 = (\alpha, \beta')$, $3 = (\alpha', \beta)$, $4 = (\alpha', \beta')$.

The theoretical prediction for $X_{experimental}$ can be calculated as

$$X^{classical}_{theory} = \mathbb{E}_1(ab) + \mathbb{E}_2(ab') - \mathbb{E}_3(a'b) + \mathbb{E}_4(a'b')$$

where

$$\mathbb{E}_1(ab) = \sum_{a,b=\pm 1} \int d\lambda\, h(\lambda)\, p(a,b/\alpha\,\beta,\lambda)\, ab\,.$$

$$\mathbb{E}_2(ab') = \sum_{a,b'} \int d\lambda\, h(\lambda)\, p(a,b'/\alpha\,\beta'\lambda)\, ab'$$

$$\mathbb{E}_3(a'b) = \sum_{a',b} \int d\lambda\, h(\lambda)\, p(a',b/\alpha'\,\beta\,\lambda)\, a'b$$

$$\mathbb{E}_4(a'b') = \sum_{a',b'} \int d\lambda\, h(\lambda)\, p(a',b'/\alpha'\,\beta'\lambda)\, a'b'$$

Lemma $-2 \leq X^{\text{classical}}_{\text{theory}} \leq 2$

This is the CHSH inequality.

Proof

Note:

$$\mathbb{E}_1(ab) = \sum_{a,b} \int d\lambda\, h(\lambda)\, p(ab|\alpha\beta\lambda)\, ab$$

$$= \sum_{a,b} \int d\lambda\, h(\lambda)\, p_A(a|\alpha\lambda)\, p_B(b|\beta\lambda)\, ab.$$

$$= \sum_{a,b,a',b'} \int d\lambda\, h(\lambda)\, p_A(a|\alpha\lambda)\, p_A(a'|\alpha'\lambda)\, p_B(b|\beta\lambda)\, p_B(b'|\beta'\lambda)\, ab$$

where we used:

$$\sum_{a'=\pm 1} p_A(a'|\alpha'\lambda) = \sum_{b'=\pm 1} p_B(b'|\beta'\lambda) = 1.$$

continued from previous page

$\downarrow$

$$= \sum_{a,b,a',b'} Q(a, a', b, b' \,|\, \alpha \alpha' \beta \beta') \; a b$$

where

$$Q(a, a', b, b' \,|\, \alpha\alpha'\beta\beta') =$$

$$\int d\lambda \, h(\lambda) \, p_A(a|\alpha\lambda) \, p_A(a'|\alpha'\lambda) \, p_B(b|\beta\lambda) \cdot p_B(b'|\beta'\lambda).$$

can be thought as a "joint" prob distr over a, a', b, b'. given $\alpha\alpha'\beta\beta'$ (but note this is a theoretical construct not realized in the experiment).

Note $Q \geq 0$ and $\sum_{a,a',b,b'} Q(a a' b b' | \alpha\alpha'\beta\beta') = 1.$

Similarly ;

$$\mathbb{E}_2(ab') = \sum_{a,a',b,b'} \varphi(aa'bb'/\alpha\alpha'\beta\beta')\, ab'$$

$$\mathbb{E}_3(a'b) = \sum_{aa'bb'} \varphi(aa'bb'/\alpha\alpha'\beta\beta')\, a'b$$

$$\mathbb{E}_4(a'b') = \sum_{aa'bb'} \varphi(aa'bb'/\alpha\alpha'\beta\beta')\, a'b'$$

Thus

$$X^{\text{classical}}_{\text{theory}} = \sum_{aa'bb'} \varphi(aa'bb'/\alpha\alpha'\beta\beta') \cdot \{ab + ab' - a'b + a'b'\}$$

Now $\quad ab + ab' - a'b + a'b'$

$$= a(b+b') + a'(b'-b)$$

As all variables <u>are binary note that</u> :

$$\underbrace{a}_{\pm 1}\underbrace{(b+b')}_{\substack{\pm 2\\ 0}} + \underbrace{a'}_{\pm 1}\underbrace{(b'-b)}_{\substack{0\\ \pm 2}} = \begin{cases} +2 \\ -2 \end{cases}.$$

Thus the average under any distr, in particular $Q(a a' b b' | \alpha \alpha' \beta \beta')$ is

$$\boxed{-2 \leq X^{\text{class}}_{\text{theory}} \leq +2}$$

This inequality above is the content of the CHSH (Bell) inequality. It turns out that experimentally, if the source distributes Bell or EPR pairs (entangled pairs), it is violated. Moreover the experimental results are in agreement with the prediction of Quantum Theory. In the next paragraph we compute the quantum predictions.

c) Quantum Prediction for correlation coefficient.

Let us apply the postulates of QM ;

* Alice mesures observable (polarization)

$$A = (+1)\, |\alpha\rangle\langle\alpha| + (-1)\, |\alpha_\perp\rangle\langle\alpha_\perp|$$

or

$$A' = (+1)\, |\alpha'\rangle\langle\alpha'| + (-1)\, |\alpha'_\perp\rangle\langle\alpha'_\perp| .$$

* Bob mesures observable (polarization)

$$B = (+1)\, |\beta\rangle\langle\beta| + (-1)\, |\beta_\perp\rangle\langle\beta_\perp|$$

or

$$B' = (-1)\, |\beta'\rangle\langle\beta'| + (-1)\, |\beta'_\perp\rangle\langle\beta'_\perp|$$

* The state of the distributed pair $|\psi\rangle$.
(pour le moment gardons $|\psi\rangle$ général).

The global observable measured in the four settings is:

$1 = (\alpha, \beta)$ $\quad$ $2 = (\alpha, \beta')$ $\quad$ $3 = (\alpha' \beta)$

$A \otimes B$ $\quad$ $A \otimes B'$ $\quad$ $A' \otimes B$

et $4 = (\alpha' \beta')$

$A' \otimes B'$

The correlation coefficient is

$$X^{QM}_{\text{theory}} = \langle \psi | \mathcal{B} | \psi \rangle$$

for the matrix (observable)

$$\mathcal{B} = A \otimes B + A \otimes B' - A' \otimes B + A' \otimes B'$$

(also called a "Bell operator" often).

Now we calculate $X^{QM}_{theory}(\alpha, \alpha', \beta, \beta')$

for $|\psi\rangle = |B_{00}\rangle = \frac{1}{\sqrt{2}}\left(|0_A\rangle\otimes|0_B\rangle + |1_A\rangle\otimes|1_B\rangle\right)$.

First average:

$$\langle B_{00}| A\otimes B | B_{00}\rangle =$$

$$= \frac{1}{2}\langle\alpha\alpha| A\otimes B|\alpha\alpha\rangle + \frac{1}{2}\langle\alpha_\perp\alpha_\perp| A\otimes B|\alpha_\perp\alpha_\perp\rangle$$
$$+ \frac{1}{2}\langle\alpha\alpha| A\otimes B|\alpha_\perp\alpha_\perp\rangle + \frac{1}{2}\langle\alpha_\perp\alpha_\perp| A\otimes B|\alpha\alpha\rangle$$

$$= \frac{1}{2}\langle\alpha|A|\alpha\rangle\langle\alpha|B|\alpha\rangle + \frac{1}{2}\langle\alpha_\perp|A|\alpha_\perp\rangle\langle\alpha_\perp|B|\alpha_\perp\rangle$$
$$= \frac{1}{2}(+1)\left(|\langle\alpha|\beta\rangle|^2 - |\langle\alpha|\beta_\perp\rangle|^2\right)$$
$$+ \frac{1}{2}(-1)\left(|\langle\alpha_\perp|\beta\rangle|^2 - |\langle\alpha_\perp|\beta_\perp\rangle|^2\right)$$

$$= \frac{1}{2}\left(\cos^2(\alpha-\beta) - \sin^2(\alpha-\beta)\right) - \frac{1}{2}\left(\sin^2(\alpha-\beta) - \cos^2(\alpha-\beta)\right)$$

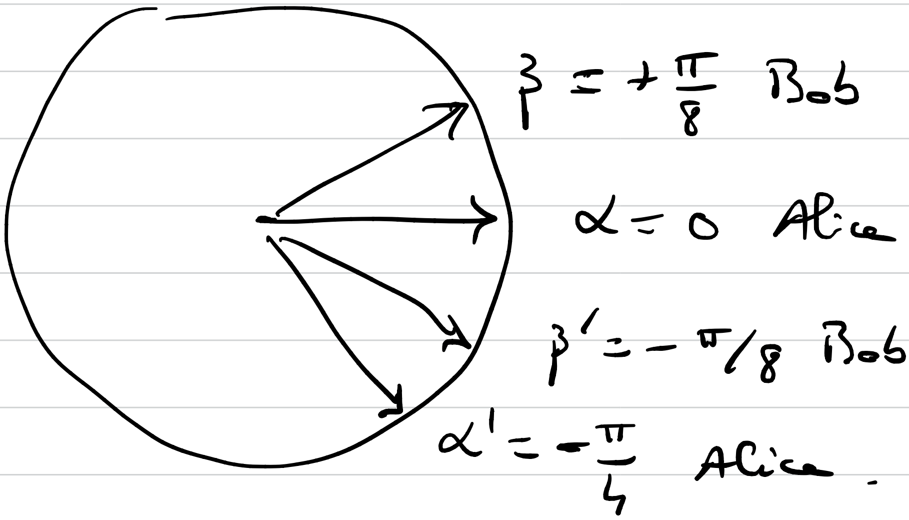
$$= \cos^2(\alpha-\beta) - \sin^2(\alpha-\beta)$$

$$= \cos(2(\alpha-\beta)).$$

Thus we obtain

$$\boxed{X^{QM}_{theory} = \cos 2(\alpha-\beta) + \cos 2(\alpha-\beta') - \cos 2(\alpha'-\beta) + \cos 2(\alpha'-\beta')}$$

The following choice of analyser angles maximizes the correlation (NOT unique choice of course)



$$\Rightarrow \quad X^{QM, max}_{theory} = \underbrace{2\sqrt{2}}_{\text{Max quantum value.}} > \underbrace{2}_{\text{Classical bound.}}$$

Remarks.

1) One can check that for $|\psi\rangle = |B_{00}\rangle$ the joint distribution

$$p_{\text{quantum}}(a, b \mid \alpha, \beta) = \frac{1}{4}\left(1 + ab \cos 2(\alpha - \beta)\right)$$

$$\neq P_A(a|\alpha)\, P_B(b|\beta).$$

2) For $|\psi\rangle = |\varphi_A\rangle \otimes |\varphi_B\rangle$ a product state instead:

$$p(a, b \mid \alpha, \beta) =$$

$$= \left(\frac{1-a}{2}|\langle\alpha_\perp|\varphi_A\rangle|^2 + \frac{1+a}{2}|\langle\alpha|\varphi_A\rangle|^2\right)$$

$$\cdot\left(\frac{1-b}{2}|\langle\beta_\perp|\varphi_B\rangle|^2 + \frac{1+b}{2}|\langle\beta|\varphi_B\rangle|^2\right)$$

$$= p_A(a|\alpha)\, p_B(b|\beta).$$

3) We say that in the above sense Bell states are "non local" (and more generally QM displays non-locality).

Product states on the other hand are "local".

II. Application to the Ekert 91 protocol.

Generation of the one-time-pad.

1) A & B have access at each time instant to a Bell pair in state $|B_{00}\rangle$. For $i = 1 \ldots N$:

→ Alice Measure her qubit by chosing at random a basis with $\alpha_1 = -\frac{\pi}{4}$, $\alpha_2 = -\frac{\pi}{8}$, $\alpha_3 = 0$

→ Bob Measure his qubit by chosing at random a basis with $\beta_1 = -\frac{\pi}{8}$, $\beta_2 = 0$, $\beta_3 = \frac{\pi}{8}$.

Alice records $x_i = \pm 1$ according to outcome α or $\alpha_\perp$ (for each basis) $i = 1 \ldots N$.

Bob records $y_i = \pm 1$ according to outcome β or $\beta_\perp$ (for each basis) $i = 1 \ldots N$.

All this is done without ever communicating.

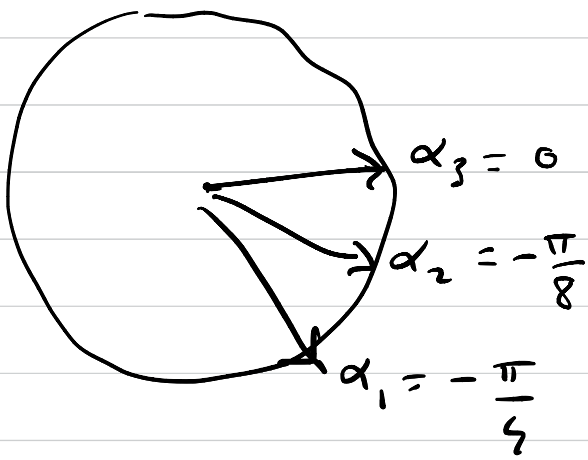
2) <u>Public communication phase</u>:

A & B exchange publicly their basis choices for each $i = 1 \dots N$. They then select time instants such that they choose the settings

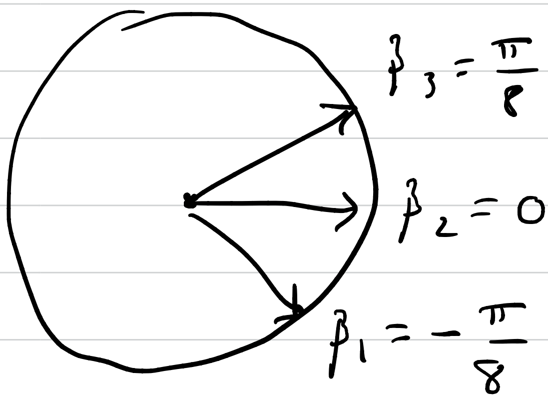
$$(\alpha_3, \beta_3), \ (\alpha_3, \beta_1), \ (\alpha_1, \beta_1), \ (\alpha_1, \beta_3)$$

Note that these are the "CHSH angles" that give max violation of the Bell inequality.

Alice basis choices:



Bob choices:



A & B compute the $\underbrace{\text{the}}_{}$ correlation coefficient for the above basis choices. If there is no eavesdropper they will find $2\sqrt{2}$ (at this point they have to exchange x_i & y_i for these specific basis choices).

(empirical)

3) Secret key generation.

A & B now select the time instants such that they choose the settings:

$$\underbrace{(\alpha_3, \beta_2)}_{(0,0)} \quad \text{or} \quad \underbrace{(\alpha_2, \beta_1)}_{(-\frac{\pi}{8}, -\frac{\pi}{8})}$$

Since their basis choices are identical, their meas outcomes are equal $x_i = y_i$. Note that they have not revealed x_i & y_i for these basis choices so it is unknown (publicly) if $x_i = y_i = \pm 1$

$\boxed{\text{This subsequence constitutes the one time pad}}$

Analysis. (heuristic)

We just make a few remarks here. What can an eavesdropper do? Suppose it prepares two photons in some "very special" product state and distributes them to A & B. Then the correlation coeff will be in $[-2, +2]$ since the state is product (see previous remark page 18).

If on the other hand the eavesdropper just produces new states $|B_{00}\rangle$ for itself and makes measurements like A & B in settings $(\alpha_3, \beta_2) = (0, 0)$ or $(\alpha_2, \beta_1) = (-\frac{\pi}{8}, -\frac{\pi}{8})$ the resulting r.v in $Z_i^{\text{eavesdropper}} = \pm 1$ but Bernoulli random and independent of $x_i^{\text{Alice}} = y_i^{\text{Bob}}$.

Thus the eavesdropper extracts no information.

∎