Device Independent Model

→ Previously we've assumed that Eve has no access to Alice and Bob's devices, and their devices are trusted

→ The idea of DI QKD is to build a general model, and use the device means with abstraction (Black box)

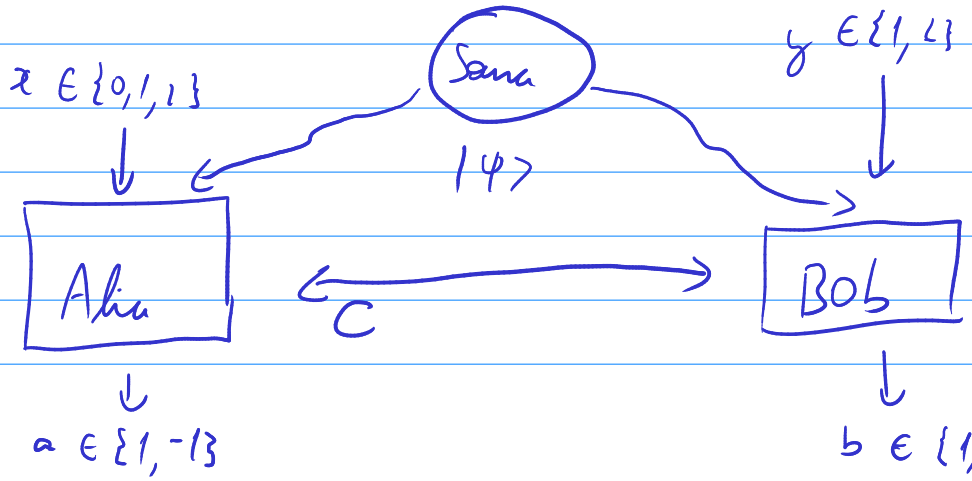
→ Alice and Bob don't communicate to each other

→ In BB84 the dimensions are known, as is DD (also because is trusted that qubits are mutually orthog.)

→ In the DI model:
- → the dimensions are unknown
- → Perhaps Eve has a perfect copy

→ DI phases
1: Quantum transmission
2: Parameter Estimation → CHSH, QBER
3: Post Processing → EC, PA

DI Protocol



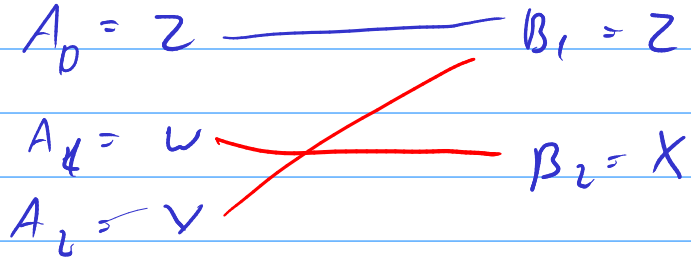
In this protocol, we have a source that sends an entangled pair to Alice and Bob. After that we assume that these qubits have been passed through a depolarizing channel, once Eve could be somewhere, and may have done something to the qubits, losing them. Because of that Alice and Bob are in a mix state:

$$\rho_{AB} = p\,|\Phi^+\rangle\langle\Phi^+|_{AB} + (1-p)\frac{I}{4}$$

($|\Phi^+\rangle\langle\Phi^+|_{AB}$: expected state)

Then Alice select between 3 basis (Z, W, V), in this case we can think like 3 buttons, once the Alice's device is a black Box. Bob also choose between two basis (Z, X).

When the basis match, $(Z_A Z_B)$, we have the key. Otherwise, we do the CHSH

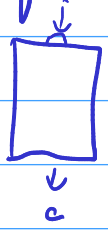


$$S = \langle A_1 B_1\rangle + \langle A_1 B_2\rangle + \langle A_2 B_1\rangle - \langle A_2 B_2\rangle$$

If S is $2\sqrt{2}$, we have a perfect entangled pairs.

Note

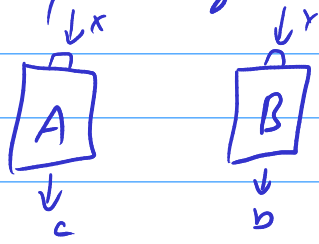
Once we are thinking on black boxes, we could imagine a device that takes an input and returns an output



So $P(a|x) \rightarrow P(0|0) = \frac{1}{2} \Rightarrow P(1|0) = \frac{1}{2}$

this is not the value, but the action of pushing the button 0

So for 2 devices, we could illustrate in the following manner:



$P(ab|xy)$ → now 0 for $\{x,y\}$ is hasn't pushed, and 1 for has pushed

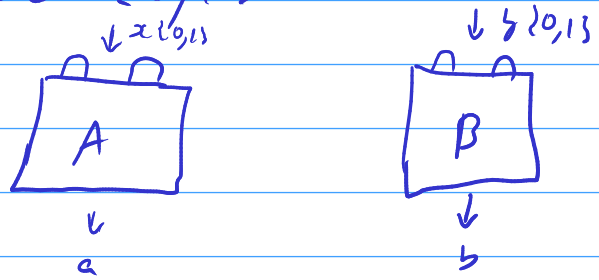
$P(ab|00)$ $P(ab|01)$ $P(ab|10)$ $P(ab|11)$

for equal inputs $\{00, 11\}$, we have $\frac{1}{2}$ of $a=b$, but for different inputs $\{01, 10\}$, we have $\frac{1}{2_a} \cdot \frac{1}{2_b} = \frac{1}{4}$ for every possible outcome

Now, translating to the protocols, if the action triggers a measurement we have:

$P_{AB|xy}(AB|xy) = Tr(M_A^x \otimes M_B^y \rho_{AB})$ ← the state

Lastly, think two devices with 2 buttons each $\{0,1\}$



if $x, y = 0$ measures in the Z and $x, y = 1$ in the X, we have:

$$P = (Z_A \otimes Z_B \; \mathcal{G}_{AB}) = (X_A \otimes X_B \; \mathcal{G}_{AB}) = 1$$

$$(Z_A \otimes X_B \; \mathcal{G}_{AB}) = (X_A \otimes Z_B \; \mathcal{G}_{AB})$$

(these are discarded, once the protocol wants $M_A = M_B$)

$\mathcal{G}_{AB}$ could be think, for instance, as $|\phi^+\rangle\langle\phi^+|$

We can use CHSH in terms of QBER

$$S = 2\sqrt{2}\,P \quad \rightarrow \quad S = 2\sqrt{2}(1 - 2Q)$$

$$Q = \frac{1}{L}(1 - P)$$

the security depends on S and Q (which check if Eve has attacked)

Security Analysis

- → Key rate needs to be > 0
- → EC and PC still needed

$$R = \underbrace{I(A_0 : B_1)}_{\text{mutual info. between A-B (Key)}} - \underbrace{\chi(B_1 : E)}_{\text{how much Bob is correlated to Eve}}$$

$$I(A_0 : B_1) = 1 - H_2(Q) \quad \leftarrow \text{Shannon Entropy}$$

$$H_2(p) = -p \log_2 p - (1-p)\log_2(1-p)$$

$$\chi(B_1 : E) \leq H_2\left(\frac{1 + \sqrt{(s/2)^2 - 1}}{2}\right)$$

$$R \geq 1 - H_2(Q) - H_2\left(\frac{1 + \sqrt{(\frac{s}{2})^2 - 1}}{2}\right)$$

Attack

- → Eve can control the noise.

Loophole

- → Alice's noise must be unknown by Bob
- → They have to be far from each other
- → Detection loophole → Bob may not click, so Eve can manipulate the result

① all result = 1

$$S = 1 + 1 + 1 - 1 = 2$$

② $B_1 = -1$ otherwise $= 1$

$$S = 1 - 1 + 1 + 1 = 2$$

③ combine ① and ②, when ① alice's device detect only A_1, and for ② only A_2

$$S = \underset{1}{\langle A_1 B_1 \rangle} + \underset{1}{\langle A_1 B_2 \rangle} + \underset{0}{\langle A_2 B_1 \rangle} - \underset{-1}{\langle A_2 B_2 \rangle} = 4$$

$4 > 2\sqrt{2}$

↳ Alice and Bob get suspicious

otherwise Alice and Bob can be fooled

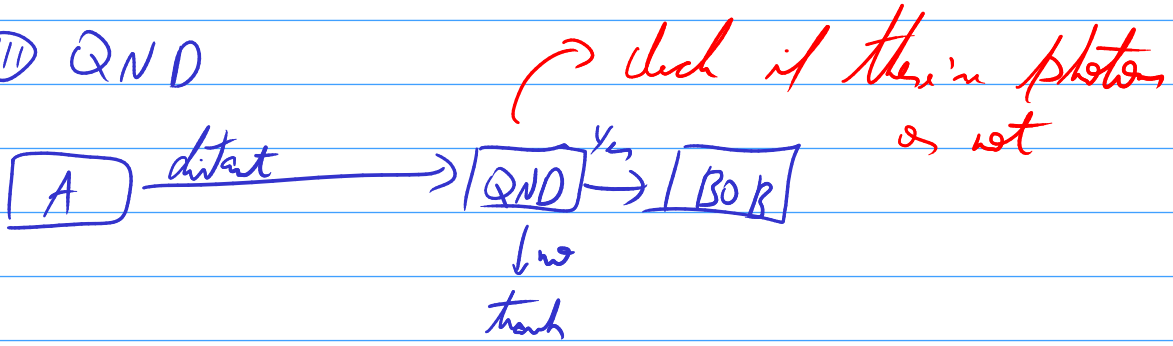
$$2 \leq S \leq 2\sqrt{2}$$

→ Ways to bypass this attack:

① add a "no click" result, she should answer when it happens. But, because of the long distance, error might be introduced in the way.

② Use qubits instead of photons. But decoherence is a problem

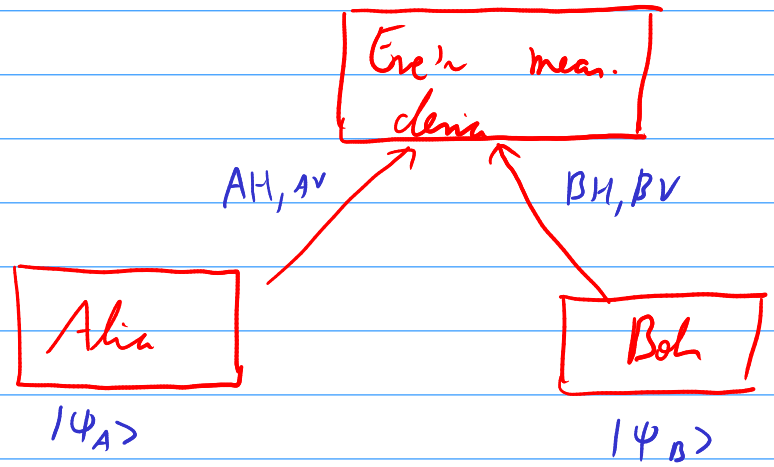
(III) QND



with QND we can use the ④

Meas. Device Indep. QKD

→ Eve has the meas. device now



$$|\psi_A\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A |\rangle_{AH} + |V\rangle_A |\rangle_{AV}\right)$$

$$|\psi_B\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_B |\rangle_{BH} + |V\rangle_B |\rangle_{BV}\right)$$

$$|\psi_A\rangle|\psi_B\rangle = \frac{1}{2}\left(|\phi^+\rangle_{AB}|\phi^+\rangle_E + |\phi^-\rangle_{AB}|\phi^-\rangle_E + |\psi^+\rangle_{AB}|\psi^+\rangle_E + |\psi^-\rangle_{AB}|\psi^-\rangle_E\right)$$

Eve has the stick, but after A and B mean the stick, and now Eve doesn't have the key