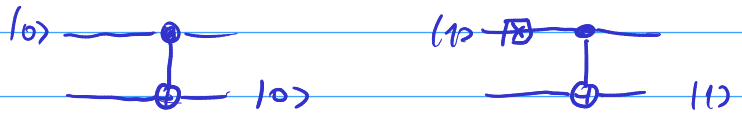
No Cloning Theorem

→ Classical bits can be cloned (like applying a CNOT)



Cloned bit

→ Superposition state (unknown state) are difficult to clone, once we might not know how they were made

Measurements

→ if you measure a value in the same basis it was encoded, you'll get the previous encoded value

→ if you measure in other basis your outcome has some probability to be correct

QKD

1: Alice encode the key in random basis for each qubit

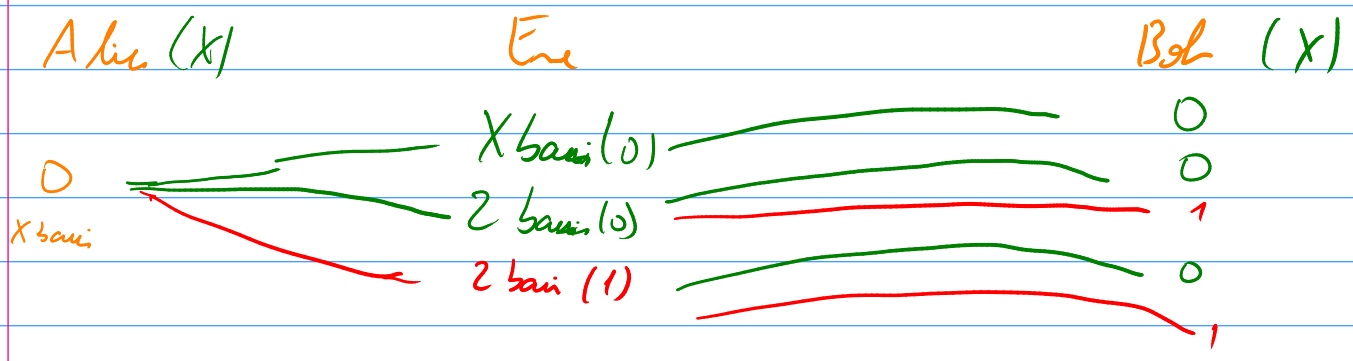
2: Bob receive the qubits and measure each one in a random basis, as well

3: They announce the used basis

4: They discard those values resulted from divergent basis (sifted key)

In reality?

→ Eve can listen to the quantum and classical channel, so she can get everything that's announced



if Alice encode in a basis B, Eve has 2/3 of chance of getting the correct value.

After Eve's attack, Bob recieve the perturbed qubits from Eve, now He has 3/5 of chance of getting the correct values.

So after the MIM attack, errors are introduced in the system. To avoid using a hacked key, the BB84 protocol is used.

BB84 protocol

→ First do the QKD

→ Then do the random permutation in the qubits (to distribute the disturbance equally)

→ Do the QBER estimation (quantum bit error)

QBER estimation

→ Get 50% from the sifted key (randomly) ≈ check bits
→ Announce they mean. from the check bits
→ The fraction of divergent bits is the QBER
→ discard these check bits

high QBER → abort
low QBER → EC e PA

Six state Protocol

→ Protocol with 3 bases (6 ≠ bases in total)
→ different from the BB84, just abt 1/3 of the bases will match (in BB84 it was 1/2), so just 1/3 will probably remain (1/2 in BB84), and Eve's info is 1/3 (so the error introduced is 1/3 as well)

With entanglement

→ using entanglement we can reach a different type of state

$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ → product basis
$\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ → Bell basis
(4 dimensional Hilbert space

→ using entangl. we have randomness by default in relation to one qubit to another
→ if two parts are maximally entangled

So they aren't entangled with a 3d party (monogamy)
→ You can't tell what was the previous state (entangled) just looking at an outcome

CHSH inequality
→ Verify entanglement
→ 4 bases X, Z, W, V

$$W = \frac{1}{\sqrt{2}}(X+Z) \qquad V = \frac{1}{\sqrt{2}}(X-Z)$$

the possible results (eigenvalues) of these bases are ± 1

$$C = Z_1 W_2 + X_1 W_2 + Z_1 V_2 - X_1 V_2 = \pm 2$$
$$(Z_1 + X_1) W_2 + (Z_1 - X_1) V_2$$

$Z \rightarrow$ can be ± 1
$X \rightarrow$ is 1

so

Z_1	X_1	$-X_1$	$Z_1 + X_1$	$Z_1 - X_1$
1	1	-1	2	0
-1	1	-1	0	-2

So if we have a state, $|\Psi^+\rangle$ for instance, we can calculate the expectation value of each operator and find $\langle C \rangle$

$\langle z_1, w_2 \rangle = \langle \phi^+ | z_1 w_2 | \phi^+ \rangle = 1/\sqrt{2}$

$\langle x_1, w_2 \rangle = \langle \phi^+ | x_1 w_2 | \phi^+ \rangle = 1/\sqrt{2}$

$\langle z_1, v_2 \rangle = \langle \phi^+ | z_1 v_2 | \phi^+ \rangle = 1/\sqrt{2}$

$\langle x_1, v_2 \rangle = \langle \phi^+ | x_1 v_2 | \phi^+ \rangle = 1/\sqrt{2}$

$\langle C \rangle = 1/\sqrt{2} + 1/\sqrt{2} + 1/\sqrt{2} - 1/\sqrt{2} = 2/\sqrt{2}$ ↙ Violation of the inequality