BB84: An entanglement-based attack and why it does not work

Elías F. Combarro
combarro@gmail.com

CERN openlab (Geneva, Switzerland) - University of Oviedo (Oviedo, Spain)

CERN - November 27, 2020

Universidad de Oviedo

Eve tries to use entanglement to break BB84 by using entanglement

- Imagine that Eve intercepts the qubit $|\psi\rangle$ sent by Alice to Bob
- Then, instead of measuring it:
  - She entangles it with a qubit of her own (that initially was in state $|0\rangle$) by using a CNOT gate
  - She then sends the original qubit $|\psi\rangle$ to Bob
  - She waits until Alice and Bob reveal the basis of measurement
  - She then measures her qubit in that basis
- This seems to work fine if $|\psi\rangle$ is either $|0\rangle$ or $|1\rangle$
- But...

The problem with this attack

- If $|\psi\rangle = |+\rangle$, after Eve uses the CNOT gate the joint state of the two qubits is

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

- Bob receives the first qubit of that state
- If he measures in the $\{|0\rangle, |1\rangle\}$ basis, the bit is discarded (wrong basis)
- If he measures in the $\{|+\rangle, |-\rangle\}$ basis, we applies *H* and the joint state becomes

$$\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right)$$

- Then, Bob has 0.5 probability of measuring 1, which is incorrect
- Alice and Bob can detect Eve's action by sharing (and discarding) some of the bits of the key