Protocolos QKD BB84 e B92

Tópicos Especiais em Redes

Maio, 2023

RQ2 – UFPA

Agenda

- Contextualizando
- Comunicação Segura?
- Bases para o Qubit
- Interceptador no QKD
- QKD BB84
- QKD B92
- QuNetSim

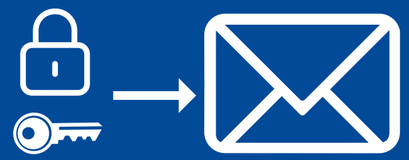
Contextualizando

Protocolos

- Charles H. Bennett e Gilles Brassard, 1984
- Chave pra Criptografia
- Propriedades da Física Quântica
- Aplicação já é uma realidade

Comunicação Segura?

- Criptografia:



- Sem garantia de segurança na comunicação

Bases para o Qubit

Tipos diferentes de base

1. Há diferentes bases;
2. |0⟩ e |1⟩ ou |-⟩ e |+⟩;
3. "Fazer perguntas para o Qubit";
4. Preparar em uma base e medir na mesma: Certeza;
5. Preparar em uma base e medir em outra: Aleatoriedade.

Exemplo:

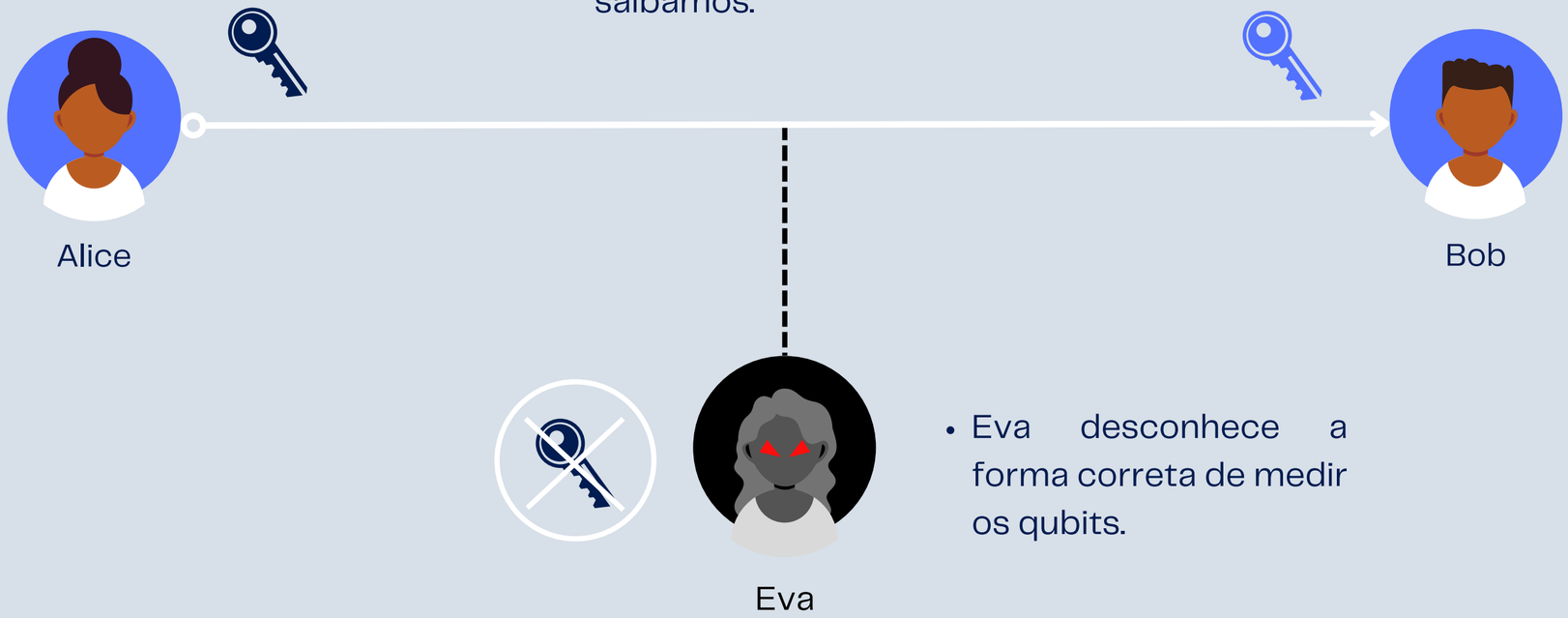
- Base A: |0⟩ para 0 e |1⟩ para 1
- Base B: |-⟩ para 0 e |+⟩ para 1

Qubit no estado |0⟩:

- Medi-lo na base A: |0⟩, ou seja, 0
- Medi-lo na base B: |?⟩, ou seja, 0 ou 1

Interceptador no QKD

- Alice envia uma chave para Bob.
- Seguro por que não pode ser espionando sem que saibamos.
- Com a interceptação, a chave chega diferente



- Eva desconhece a forma correta de medir os qubits.

QKD BB84

Charles H. Bennett e Gilles Brassard, 1984

1. Alice e Bob combinam as bases.
2. Alice prepara os qubits.
3. Alice envia a chave.
4. Bob realiza a medição.
5. Checagem das bases:
   - Logo após o envio;
   - No final do envio das chaves.

Chave: 0 0 1...

Base A: $|0\rangle$ e $|1\rangle$

Base B: $|-\rangle$ e $|+\rangle$

Base aleatória

1º Q: Base A

2º Q: Base A

Base aleatória

1º Q: Base A ✓

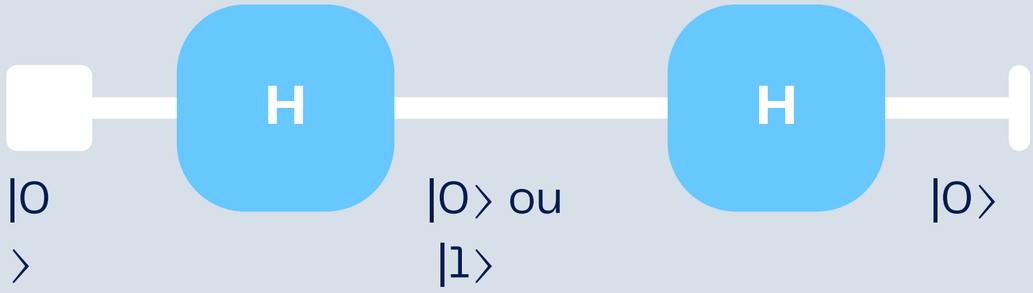
2º Q: Base B ✗

QKD B92

Charles H. Bennett, 1984

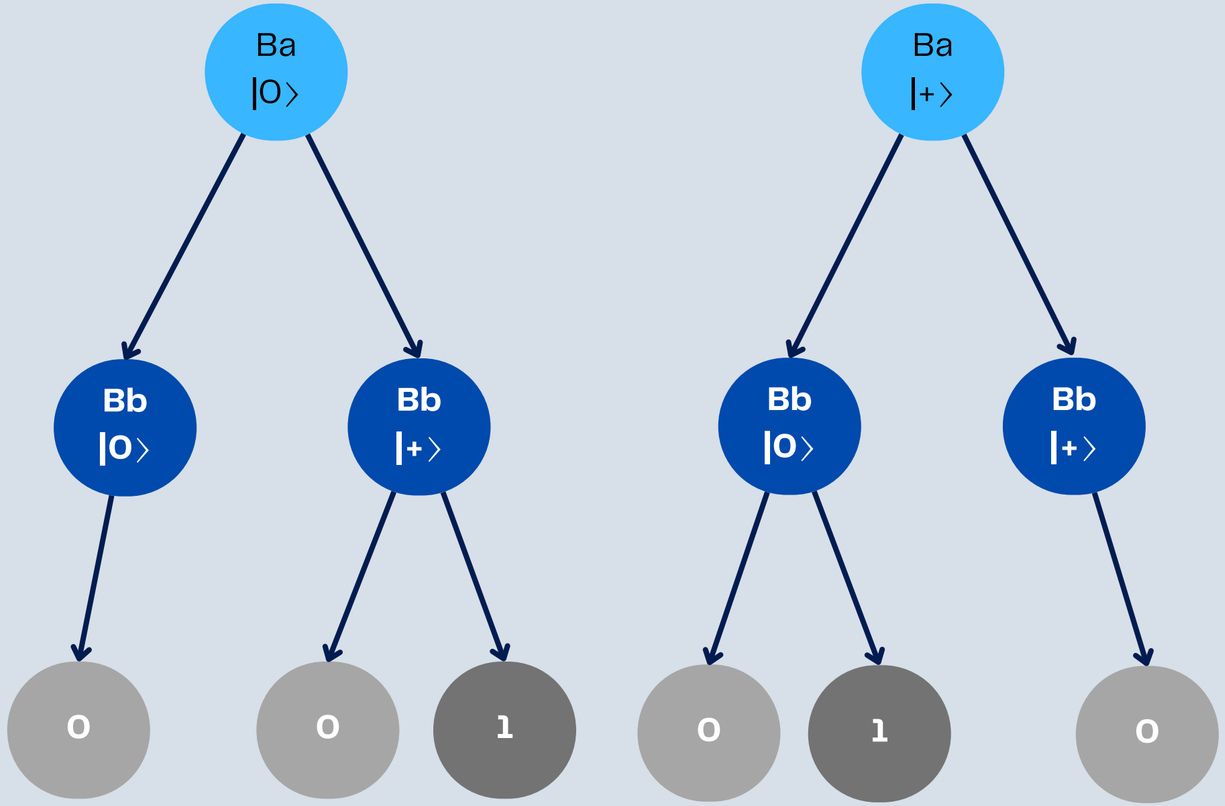
- Dois estados não ortogonais.
- Alice e Bob escolhem qual base representa qual bit.
- $|0\rangle$ para 0 e $|+\rangle$ para 1
- Existem estados com ambiguidade.
- Semelhante ao BB84.

Estado $|+\rangle$ é um estado de Bell
Qubit $|0\rangle$ aplicado Hadamard



QKD B92

Charles H. Bennett, 1984



- Descarta quando resultado em 0

Chave: 0 100010...

- Base escolhida por Alice: Ba
- Base escolhida por Bob: Bb

1. Alice envia $|0\rangle$
2. Bob mede com $|0\rangle$
3. Resultado com certeza é 0
4. Ambiguidade. Próximo!
5. Alice envia $|+\rangle$
6. Bob escolhe $|0\rangle$
7. Resultado 0 ou 1