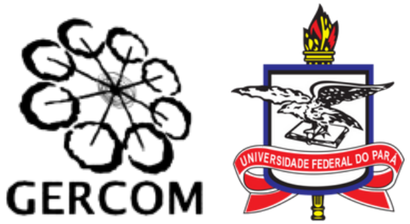


Redes de Distribuição Quântica de Chaves

Workshop GERCOM
Arthur Pimentel
12/04/24

Agenda

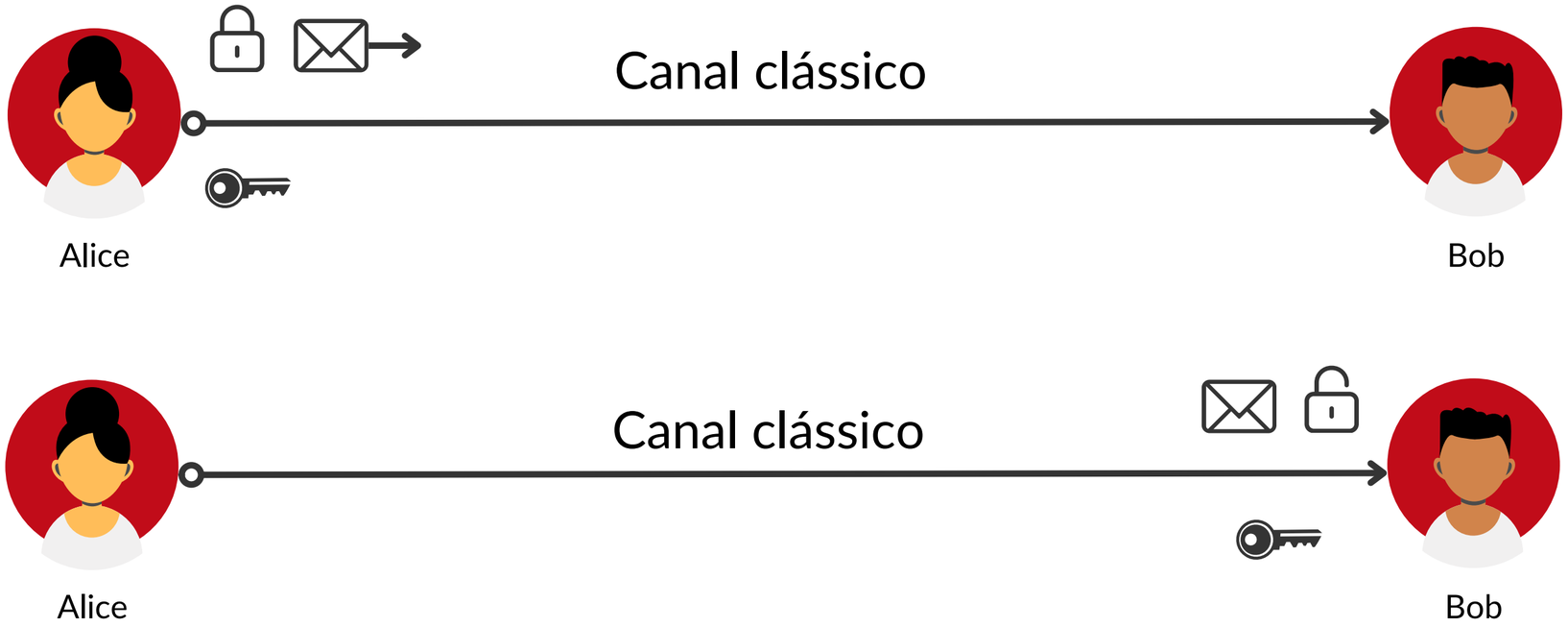
- Distribuição Quântica de Chave
- BB84
- E91
- B92
- Redes QKD
- Alocação de Recursos em Redes QKD

Distribuição Quântica de Chaves (QKD)

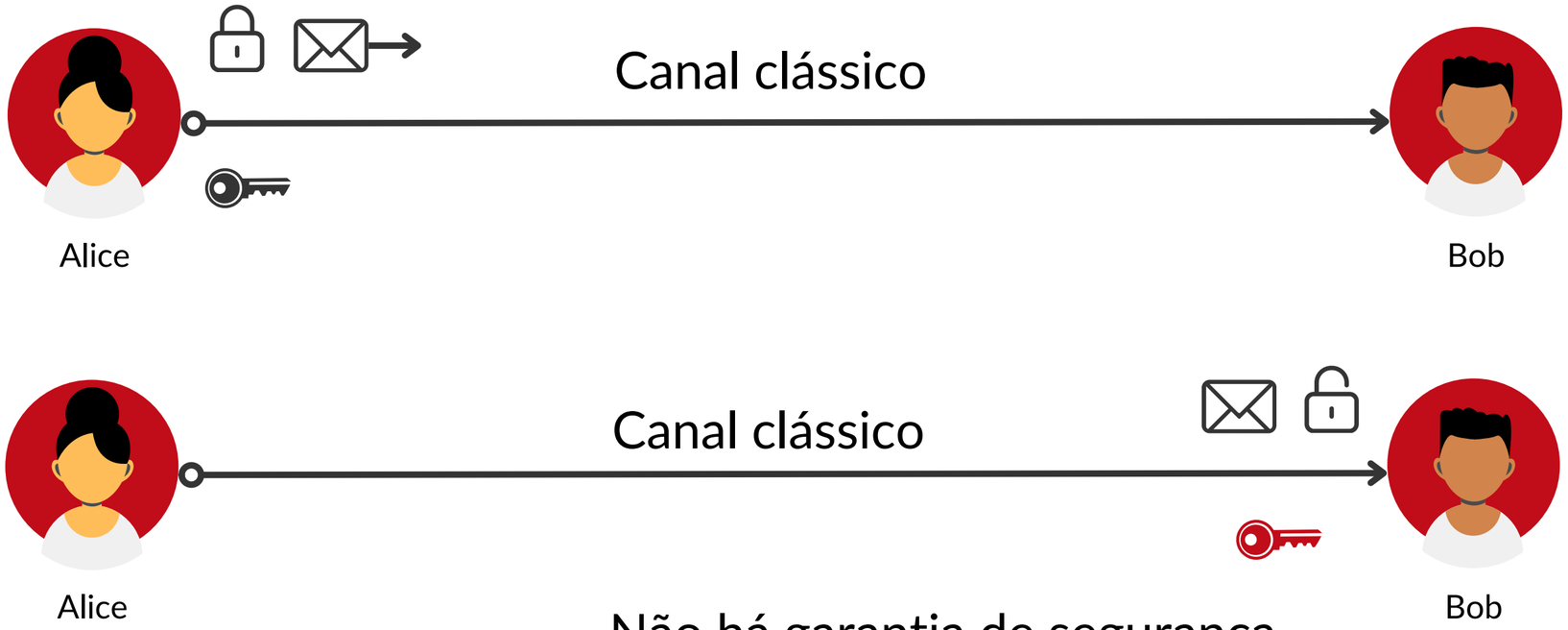
Como realizar comunicação de forma segura?

Criptografia

Distribuição Quântica de Chaves (QKD)

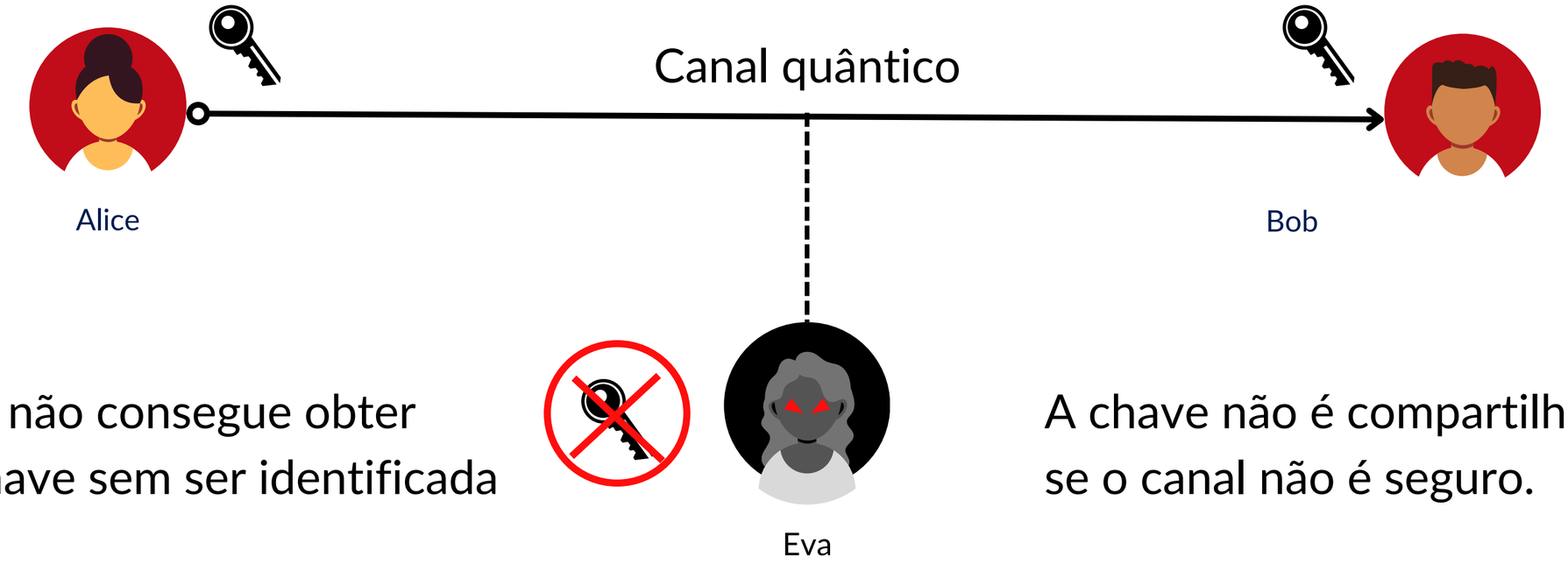


Distribuição Quântica de Chaves (QKD)



Não há garantia de segurança na transmissão da chave

Distribuição Quântica de Chaves (QKD)



Eve não consegue obter
a chave sem ser identificada

A chave não é compartilhada
se o canal não é seguro.

Distribuição Quântica de Chaves (QKD)

Bases

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⟩:

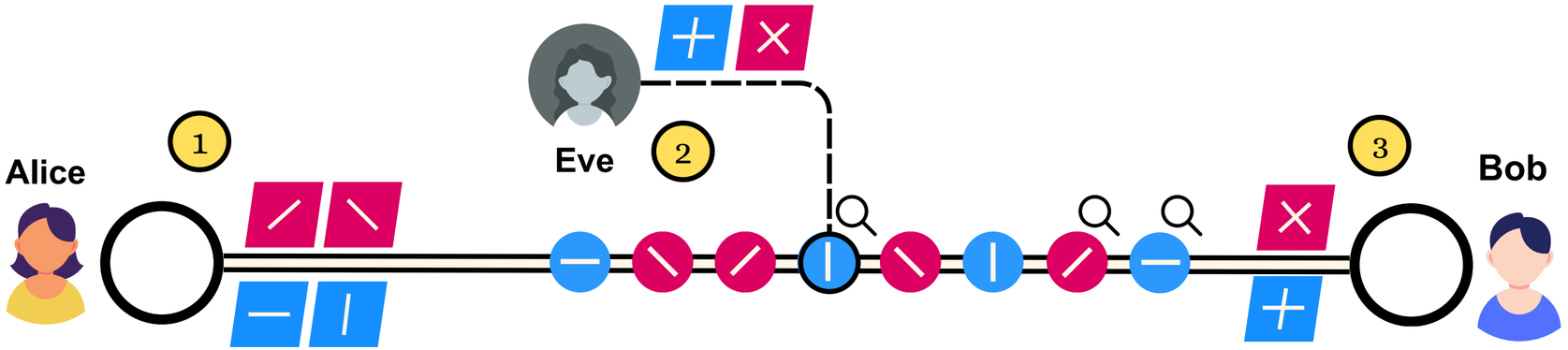
- Medi-lo na base A: |0⟩, ou seja, 0
- Medi-lo na base B: |?⟩, ou seja, 0 ou 1

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. Comparam as bases.
6. Utilizam a chave.

BB84



Estados quânticos:

0	—	/
1	|	\

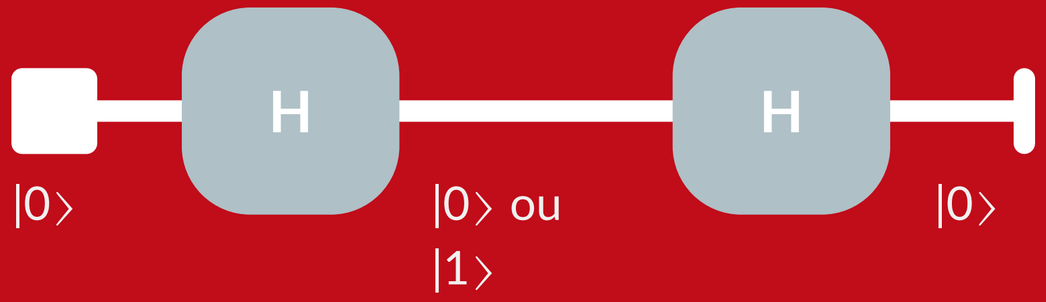
Alice	Bits:	0	1	0	1	1	1	0	1
	Bases:	+	×	×	+	×	+	+	×
	Qubits enviados:	—	\	/	|	\	|	—	\
Eve	Espião:	☐	☐	☐	X	☐	☐	X	X
Bob	Bases:	+	+	×	+	+	×	+	×
	Qubits recebidos:	—	—	/	—	|	/	|	\
4	Chave gerada:	0	-	0	0	-	-	1	1

B92

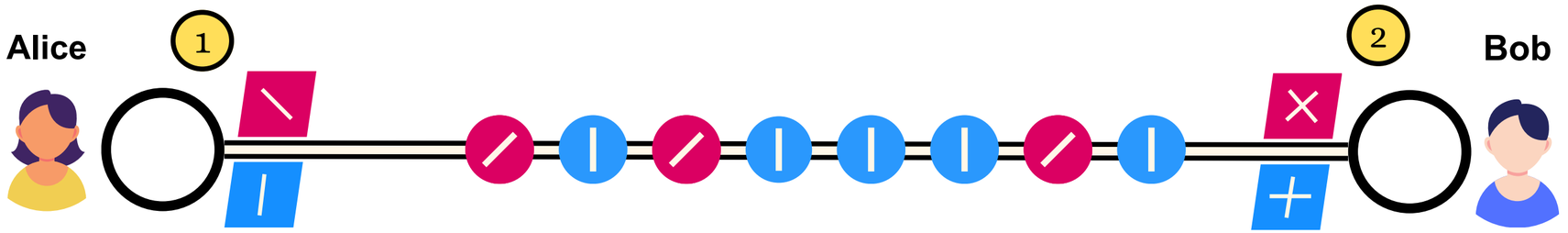
Charles H. Bennett, 1992

- Dois estados não ortogonais.
- Alice e Bob escolhem qual base representa qual bit.
- |0⟩ para 0 e |+⟩ para 1
- Existem estados com ambiguidade.
- Restante do processo.

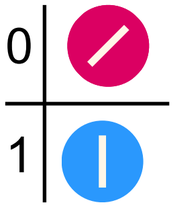
Estado |+⟩ é um estado de Bell
Qubit |0⟩ aplicado Hadamard



B92



Estados quânticos:



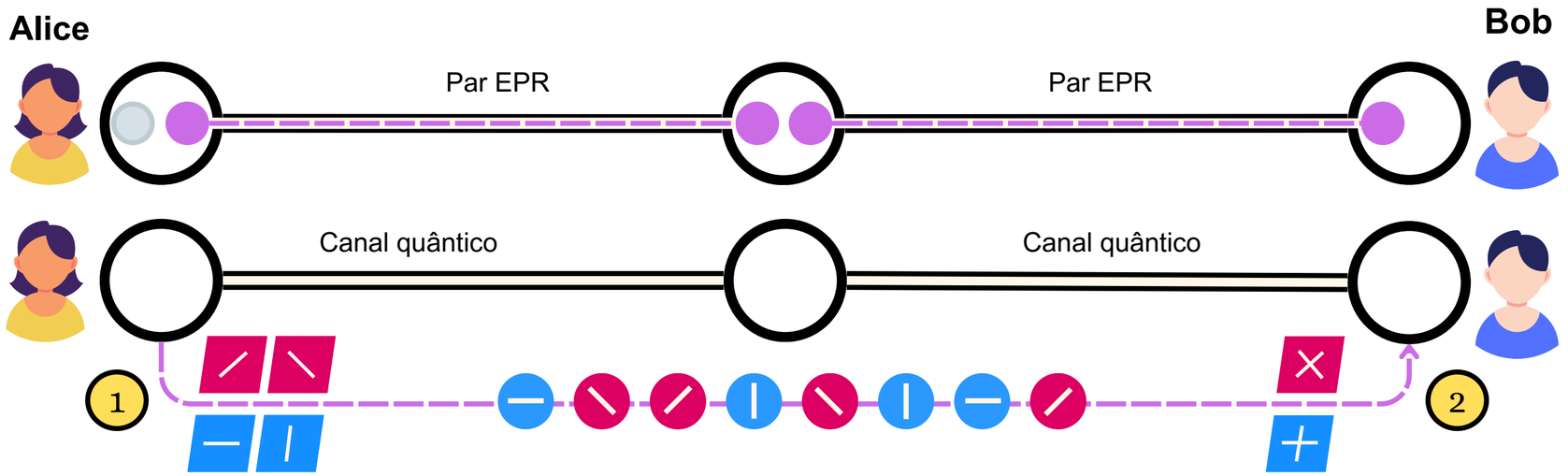
Alice	Bits:	0	1	0	1	1	1	0	1
	Qubits enviados:	⊘	|	⊘	|	|	|	⊘	|
Bob	Bases:	+	+	×	+	+	×	+	×
	Qubits recebidos:	|	|	⊘	|	|	⊘	|	⟍
	Medição:	1	0	0	0	0	0	1	1
3	Chave gerada:	0	-	-	-	-	-	1	1

E91

Artur Ekert, 1991

- Mesma lógica de BB84.
- Baseado em entrelaçamento.
- Fonte confiável envia os qubits emaranhados.
- Também pode ser realizada ponto a ponto.

E91



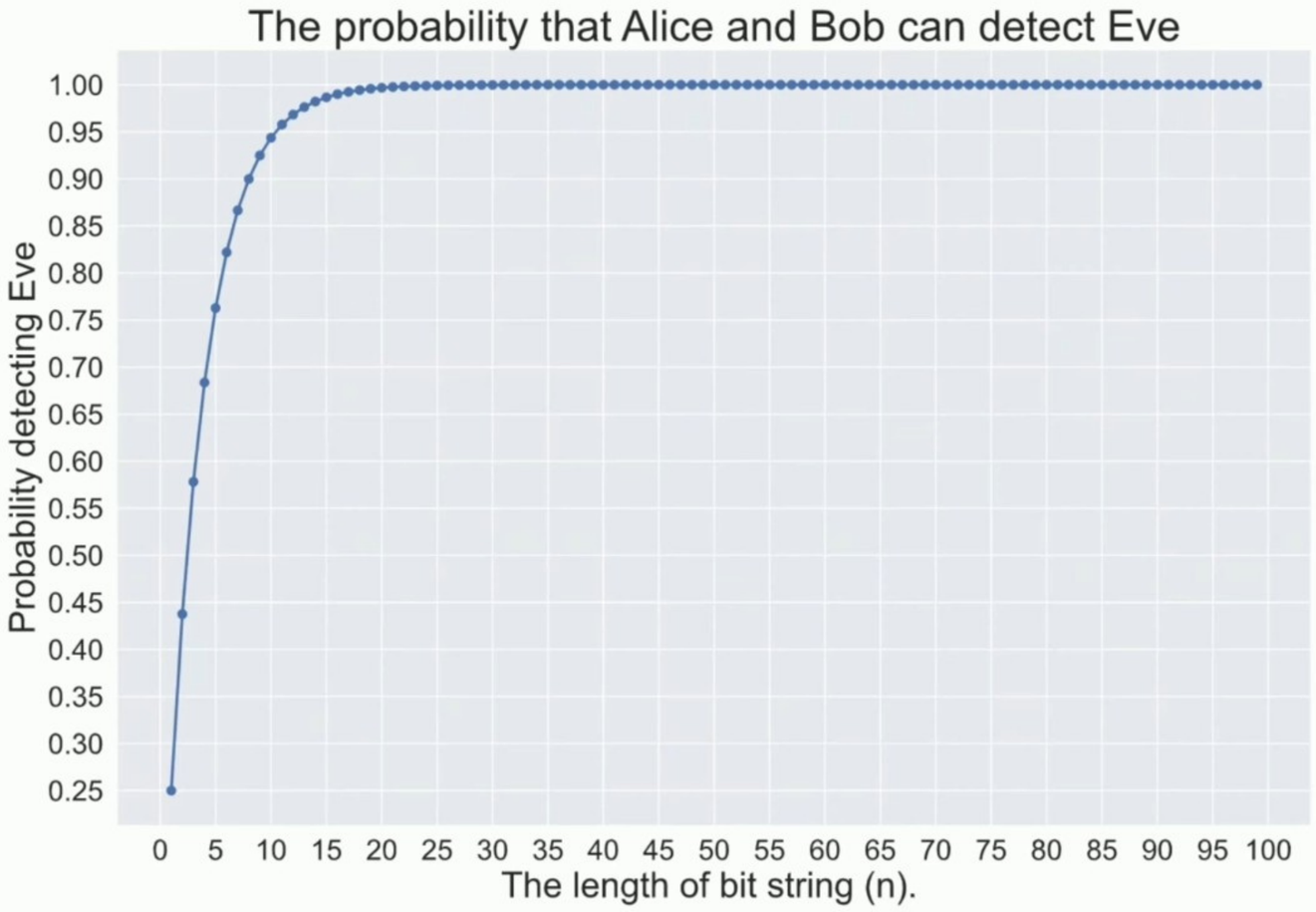
Estados quânticos:

0	—	/
1	|	\

Alice	Bits:	0	1	0	1	1	1	0	1
	Bases:	+	×	×	+	×	+	+	×
	Qubits:	—	\	/	|	\	|	—	\
Bob	Bases:	+	+	×	+	+	×	+	×
	Qubits:	—	—	/	|	|	/	—	\
3	Chave:	0	-	0	1	-	-	0	1

Probabilidade de detecção de Eve

$$P(n) = 1 - \left(\frac{3}{4}\right)^n$$



Redes QKD

- Redes que compartilham dados de forma totalmente segura;
- Nós com dispositivos QKD;
- Fibra ótica, satélite;
- Aplicações que utilizam criptografia;

Redes QKD

DARPA QKD network

- 2004
- 10 nós
- Massachusetts, EUA
- Diferentes tipos de links
- Ponto a ponto

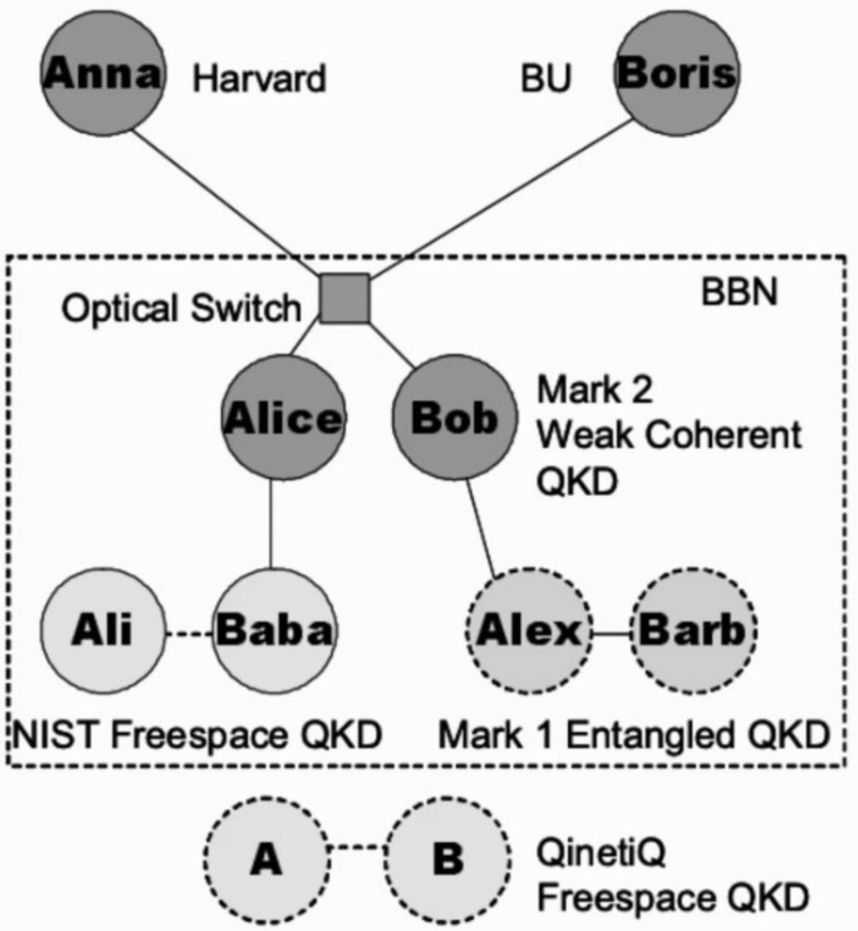


Figure 13: Current Topology of the DARPA Quantum Network.

Redes QKD

SECOQC QKD network

- 2008
- 6 nós, 8 links
- Viena
- Já envolvia arquitetura em camadas

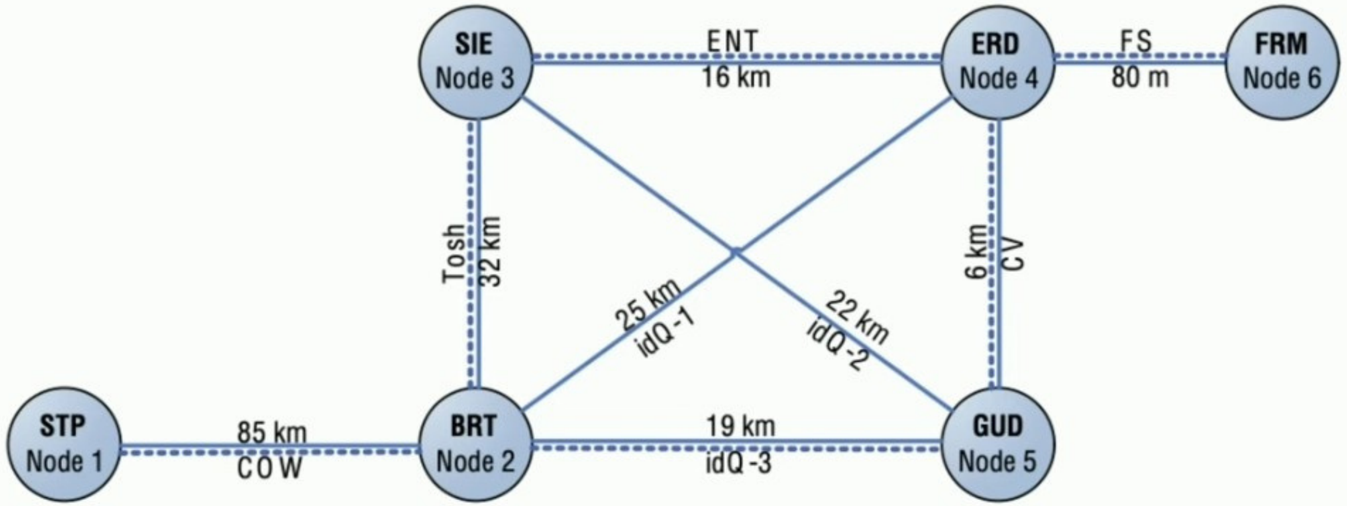


Figure 2. Network topology of the SECOQC QKD network prototype. Solid lines represent quantum communication channels, dotted lines denote classical communication channels.

Redes QKD

Tokyo QKD network

- 2010
- 6 nós
- Viena
- Também envolvia arquitetura em camadas
- Utilizada para videoconferências

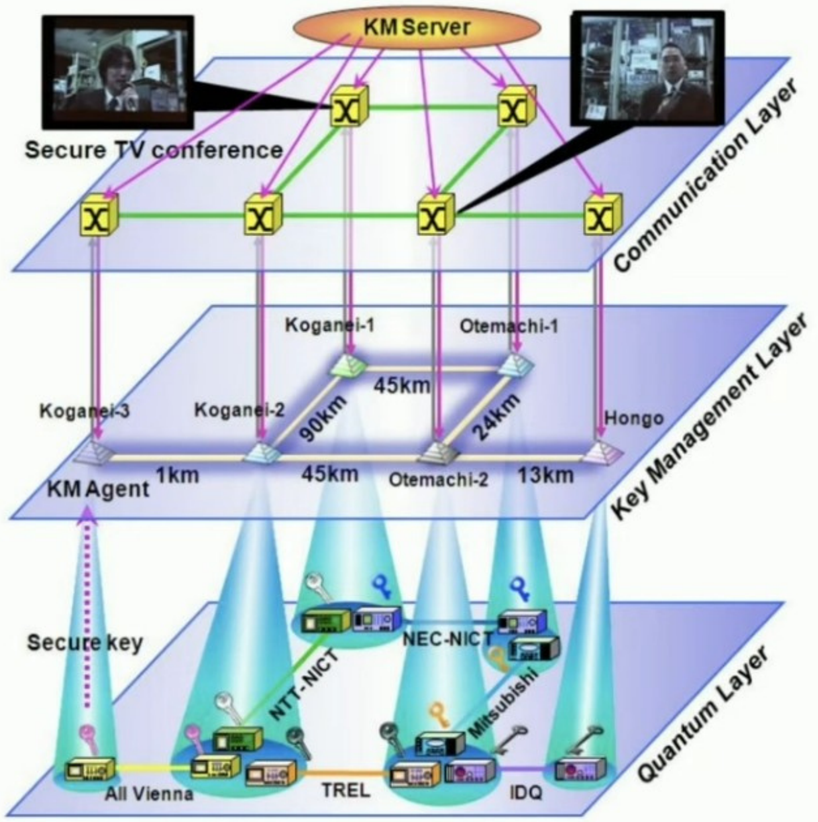
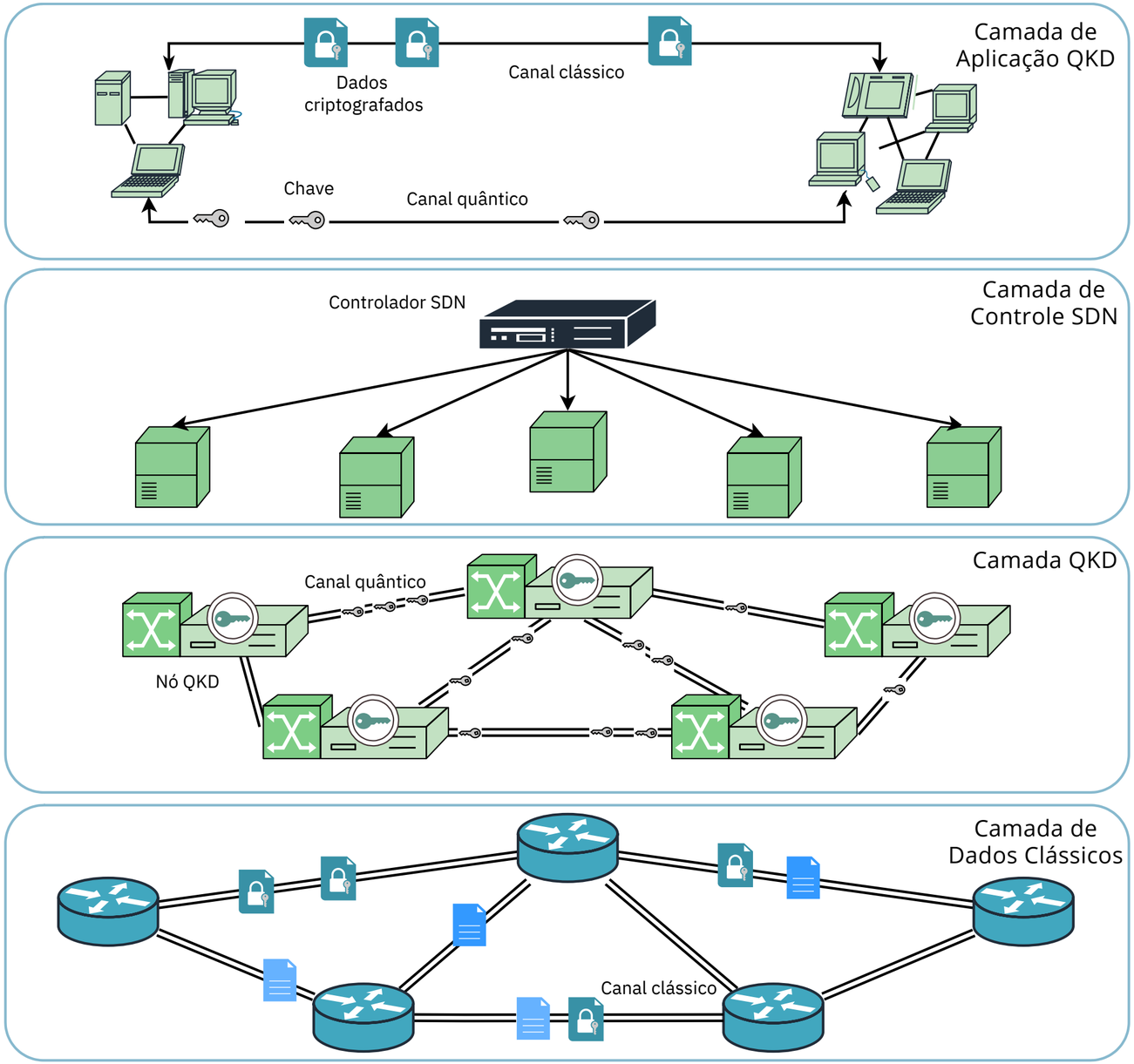


Fig. 2. Three-layer architecture of the Tokyo QKD Network. It consists of the quantum, the key management, and the communication layer.

Alocação de recursos em Redes QKD

- Diferentes dispositivos
- Comutação de circuitos
- Prioridades
- Controle da rede
- Garantir bom funcionamento da rede
- Simulações em Python



Obrigado!