Criptografia quântica

Autores: Gabriel Limeira (5º período), Lívia Paravidino (7º período) , Matheus Reis (7º período)

Universidade Federal do Rio de Janeiro (UFRJ)

Departamento de Engenharia Eletrônica (DEL)

Engenharia de Controle e Automação

Professor : Otto Carlos Muniz Bandeira Duarte

Mecânica Quântica

- Necessidade de se explicar fenômenos quânticos da matéria.
- Max Plank afirma que a radiação eletromagnética é transmitida em “pacotes” de energia.
- Primeiros resultados: Antiga Teoria Quântica – início do século XX.

Mecânica Quântica

- 1927 - princípio da incerteza de Werner Heisenberg.

$$\Delta x \cdot \Delta Q \geq \frac{h}{4\pi}$$

- 1926 - Erwin Schrödinger publica seu trabalho em mecânica ondulatória.
- A equação de Schrödinger descreve a evolução no tempo da função de onda.

Mecânica Quântica

- Conceito de superposição de estados
- Colapso da função de onda
- Postulado da correspondência
- Interpretação de Copenhague

Críticas à mecânica quântica

- A “ação fantasmagórica à distância”, prevista pela teoria quântica, é interpretada por Einstein como um absurdo.
- A mecânica quântica estaria incompleta - teoria de variáveis ocultas seria necessária.
- Teorema de Bell – anos 60
- Violação das desigualdades de Bell por Alan Aspect em 1982 reforça a validade da interpretação de Copenhage.

Criptografia Atual

- Criptografia de Chave Simétrica

One-Time-Pad:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

11(L)	23(X)	01(B)	15(P)	19(T)	07(H)	Chave
+15(P)	+00(A)	+17(R)	+19(T)	+08(I)	+17(R)	Mensagem
26	23	18	34	27	24	Chave+mensagem
00(A)	23(X)	18(S)	08(I)	01(B)	24(Y)	Chave+mensagem (mod26)

00(A)	23(X)	18(S)	08(I)	01(B)	24(Y)	Criptograma
-11(L)	-23(X)	-01(B)	-15(P)	-19(T)	-07(H)	- chave
-11	00	17	19	-18	17	Criptograma-chave
15(P)	00(A)	17(R)	19(T)	08(I)	17(R)	Criptograma-chave (mod26) = mensagem

00(A)	23(X)	18(S)	08(I)	01(B)	24(Y)	Criptograma
-09(J)	-19(T)	-16(Q)	-14(O)	-01(B)	-07(H)	- chave qualquer
-09	04	02	-06	00	17	Criptograma-chave qualquer
17(R)	04(E)	02(C)	20(U)	00(A)	17(R)	Criptograma-chave qualquer (mod26)

00(A)	23(X)	18(S)	08(I)	01(B)	24(Y)	Criptograma
-14(O)	-23(X)	-05(F)	-15(P)	-23(X)	-07(H)	-chave qualquer
-14	00	13	-07	-22	17	Criptograma-chave qualquer
12(M)	00(A)	13(N)	19(T)	04(E)	17(R)	Criptograma-chave qualquer (mod26)

- Criptografia de Chave Assimétrica

Computação Quântica

- Bit Quântico

- Algoritmos Quânticos:

  Algoritmo de Deutsch

  Algoritmo de Grover

  Algoritmo de Shor

Protocolo BB84

- Duas direções de polarização (vertical e diagonal)
- Quatro polarizações espaçadas por π/4
- Escuta gera 25% de erro na mensagem transmitida
- Valor lógico 0 – 0 e π/4
- Valor lógico 1 - π/2 e 3π/4

Base vertical e diagonal

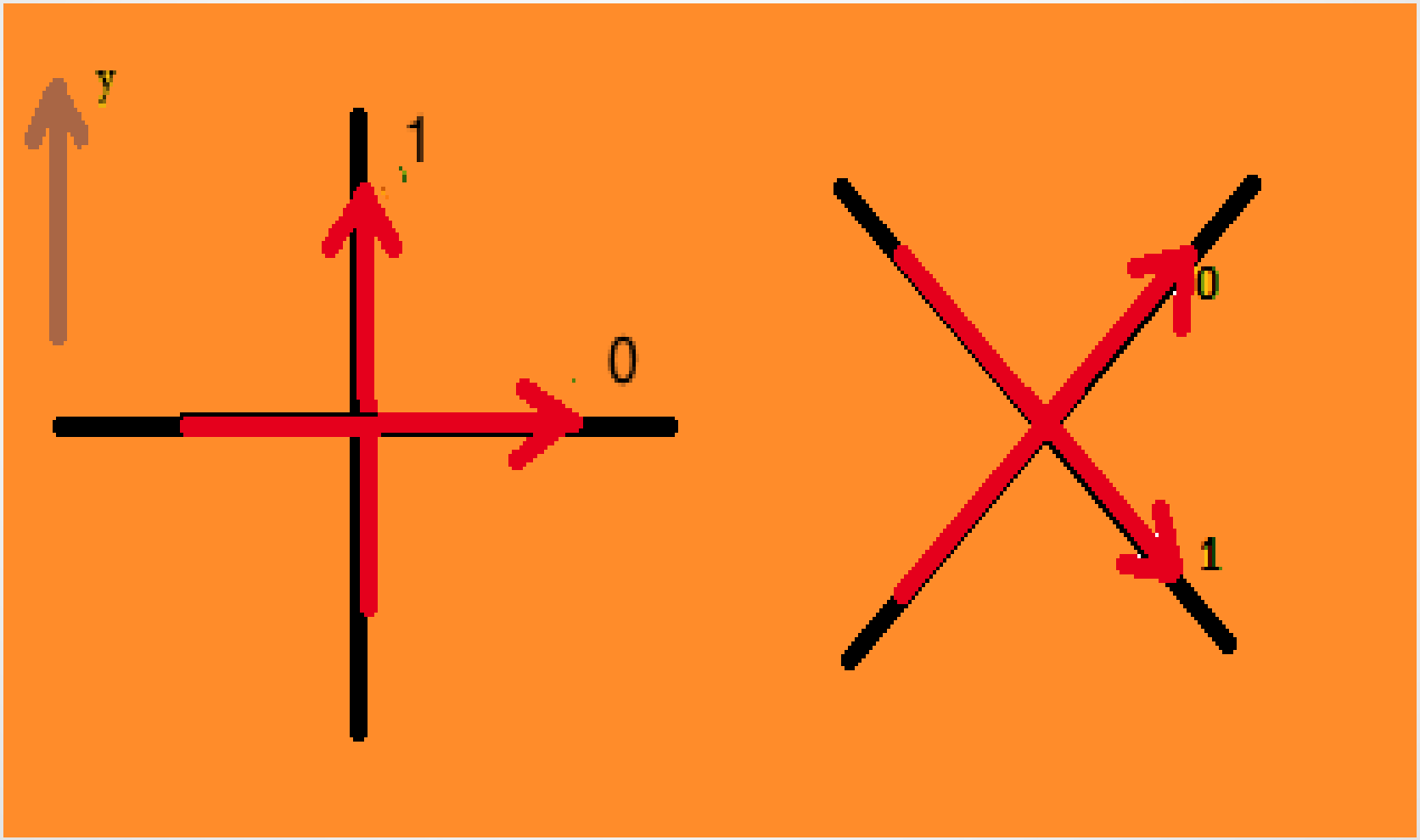


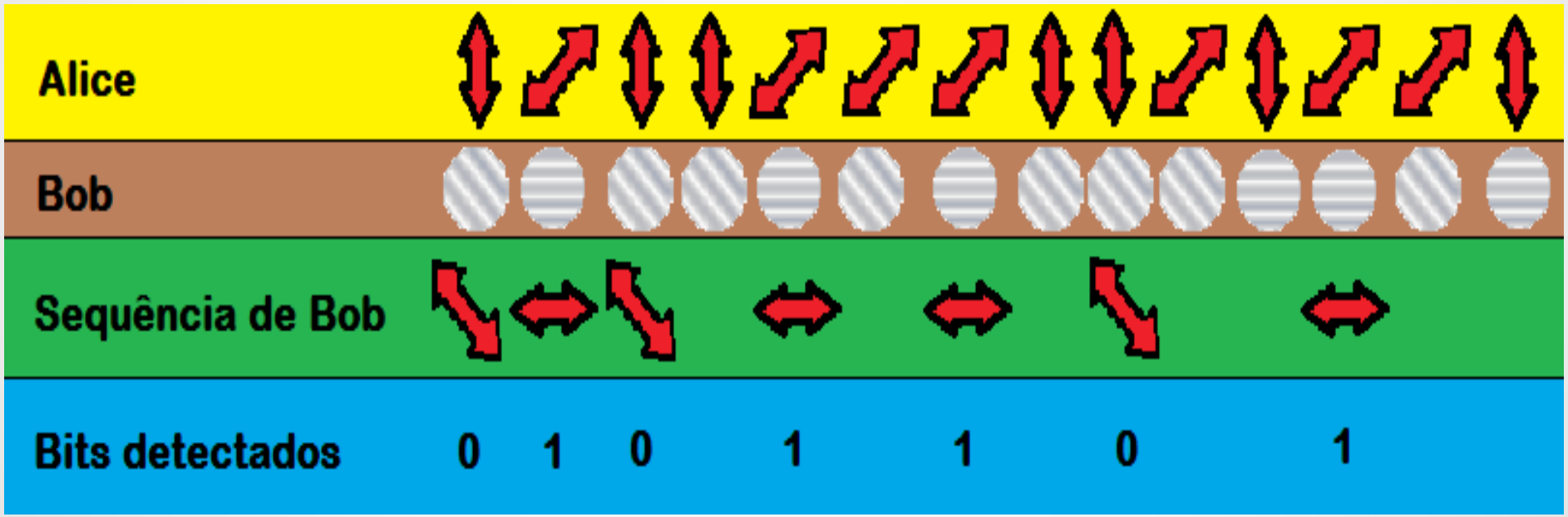
Tabela protocolo BB84

Bits Alice	0	1	0	1	1	0	0	0	1	1	0	1
Bases Alice	+	×	×	+	×	+	×	+	+	×	+	+
Bases Bob	+	+	×	×	×	+	+	×	+	+	+	×
Bits Bob	0	1*	0	0*	1	0	1*	0*	1	1*	0	0*
Chave secreta	0		0		1	0			1		0	

Protocolo B92

- Duas polarizações não- ortogonais
- Filtro polarizador que permite passar parte de uma direção bloqueia totalmente a outra
- Parte da mensagem é perdida de modo que escutar e reenviar é muito difícil

Tabela protocolo B92

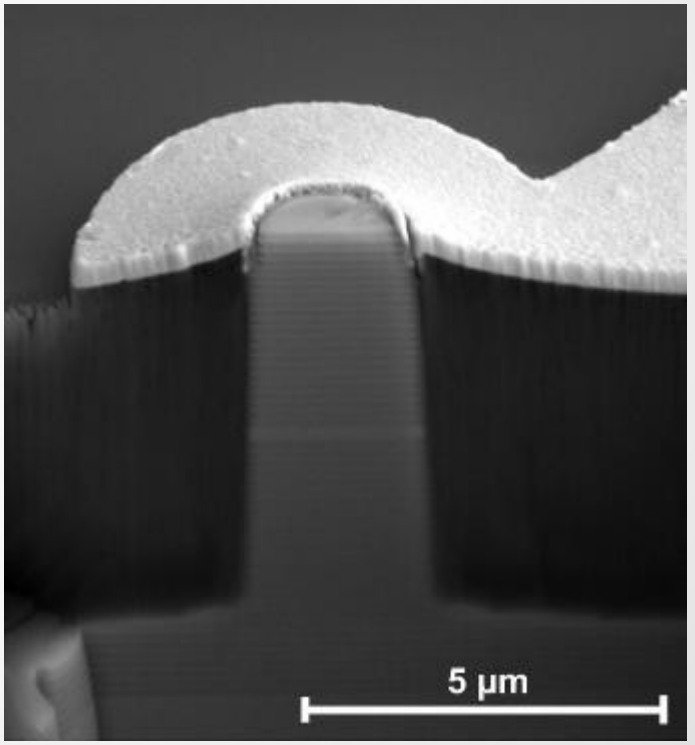


Protocolo E91 ou EPR

- EPR- Paradoxo de Einstein-Podolsky-Rosen.
- Entrelaçamento quântico – previsto pela física quântica, mas ainda não foi totalmente compreendido.
- Dois fótons ficam com a mesma polarização independente da distância que os separa.
- Polarização só pode ser determinada no momento da medida. A tentativa de escuta prévia altera parte das polarizações.

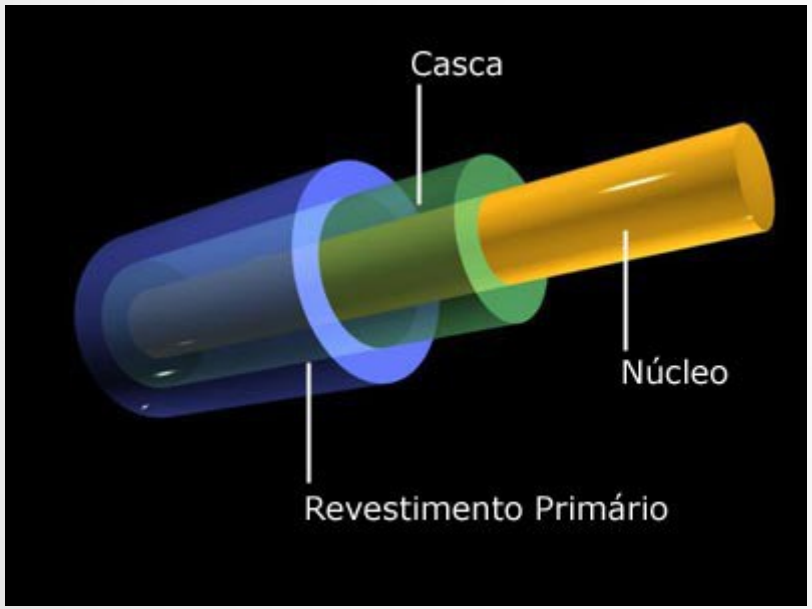
Tecnologias

- Geração de fótons individuais



Tecnologias

- Fibras Óticas



Tecnologias

- Detectores quânticos

Perguntas

1) Quais são os principais princípios físicos nos quais o desenvolvimento da criptografia quântica se baseia?
R: O princípio da incerteza e o fenômeno de entrelaçamento quântico.

2) Como o desenvolvimento da computação quântica afeta a criptografia quântica?
R: Com o desenvolvimento da computação quântica, os sistemas atuais mais seguros de criptografia tornam-se relativamente frágeis devido ao aumento exponencial no poder e velocidade de processamento de sistemas computacionais quânticos. Por isso, sistemas de criptografia quântica podem oferecer uma solução mais segura em comunicação no futuro.

3) Apenas o uso da criptografia quântica é capaz de garantir a confidencialidade na comunicação?
R: Não, porque o espião ainda pode se infiltrar como “homem-do-meio”, conseguir separar e capturar apenas parte de um pulso do feixe ou obter as polarizações usadas pelo emissor
através do envio de pulsos fortes para o seu polarizador, que se refletiriam no seu transmissor de volta ao espião caso esse transmissor tenha uma superfície reflexiva.

Perguntas

4) Como o monitoramento de uma transmissão quântica pode ser detectado?
R: A monitoração de uma transmissão de fótons gera mudanças na chave transmitida, que pode ser detectada comparando parte da chave, que é anunciada publicamente.

5) Quais são as principais limitações para o uso de sistemas de criptografia quântica hoje?
R: Alto custo, dificuldade de implementação, distâncias limitadas entre emissor e receptor, e dificuldade de integração entre uma rede quântica e a infra-estrutura das redes atuais.