



Instituto de Física

50 ANOS

Universidade Federal do Rio de Janeiro

Criptografia Quântica



Semana da Física UFRJ 2015

Malena Hor-Meyll

Criptografia...

grego: **kryptós**, "escondido", e **gráphein**, "escrita" é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta")

Fonte: Wikipédia

Quântica...

Utiliza na sua implementação um sistema regido pelas leis da Mecânica Quântica:

- Superposição
- Colapso da medida
- Não clonagem

Representação Binária: 0 e 1 (bit)

- Para simplificar, sem perda de generalidade, vamos assumir um alfabeto de apenas 8 caracteres: A, B, C, D, E, F, G, H.
- Para representar univocamente cada letra precisamos de 3 bits.
- Uma possível codificação seria:

A:	000
B:	001
C:	010
D:	011
E:	100
F:	101
G:	110
H:	111

- Pergunta 1: com 4 bits quantos caracteres conseguiríamos representar?
- Pergunta 2: com N bits quantos caracteres conseguiríamos representar?
Resp: 2^N

Criptografia usando a função XOR

- Suponhamos que queremos transmitir secretamente a palavra:

FACE

cuja representação binária é dada por:

A: 000

B: 001

C: 010

D: 011

E: 100

F: 101

G: 110

H: 111

1 0 1 0 0 0 0 1 0 1 0 0
F A C E

- A função XOR (Ou exclusivo) retorna 0 se as entradas forem iguais e 1 se as entradas forem diferentes.
- Para criptografia segura (sem redundância) a chave secreta deve ser uma sequência aleatória do mesmo tamanho da mensagem.

Criptografia usando a função XOR

- Supondo uma moeda não viciada, lançamos neste caso doze vezes:



- Chave Secreta: 0 1 0 0 1 1 0 1 0 0 0 1
- Codificação: 1 0 1 0 0 0 0 1 0 1 0 0

XOR: 1 1 1 0 1 1 0 0 0 1 0 1

H

D

A

F

- Decodificação: 0 1 0 0 1 1 0 1 0 0 0 1

XOR: 1 0 1 0 0 0 0 1 0 1 0 0

F

A

C

E

A: 000, B: 001, C: 010, D: 011, E: 100, F: 101, G: 110, H: 111

Criptografia - Resumo



Criptografia Quântica

Distribuição da chave criptográfica usando um sistema quântico



Protocolo BB84



Charles Bennett

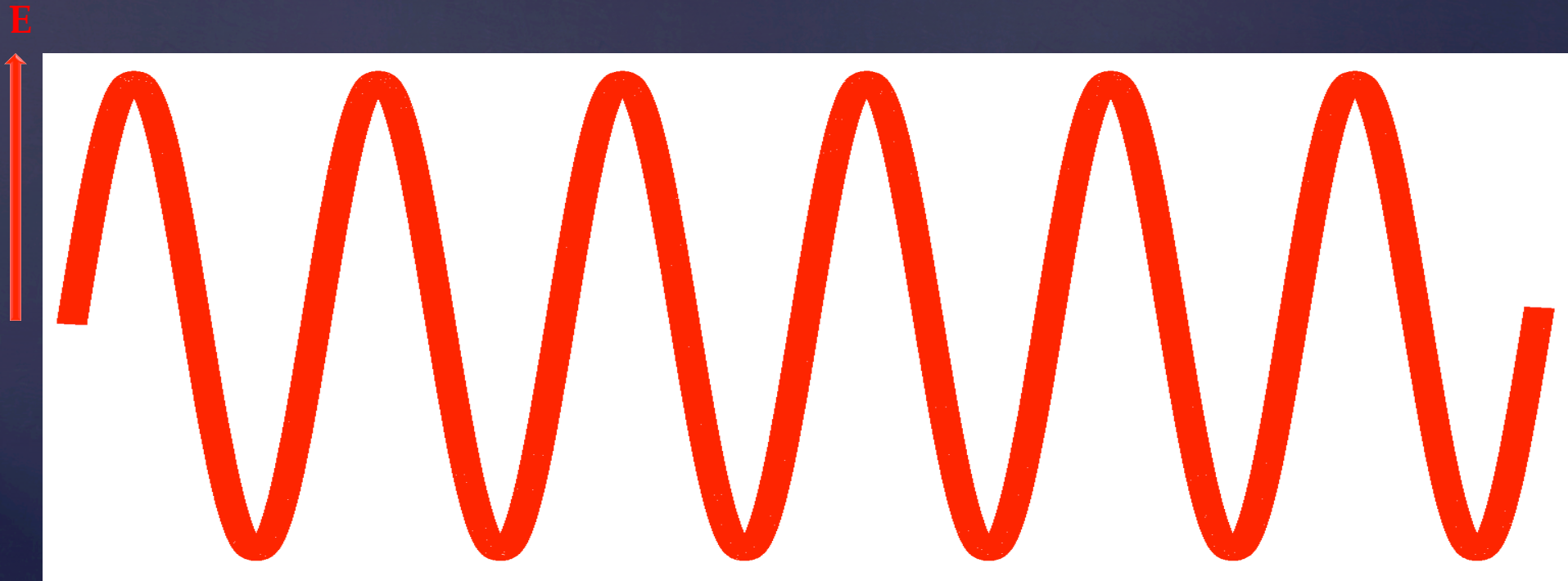


Gilles Brassard

Protocolo BB84: implementação ótica

Representação da informação -> Polarização do fóton (partícula de luz) -> qubit

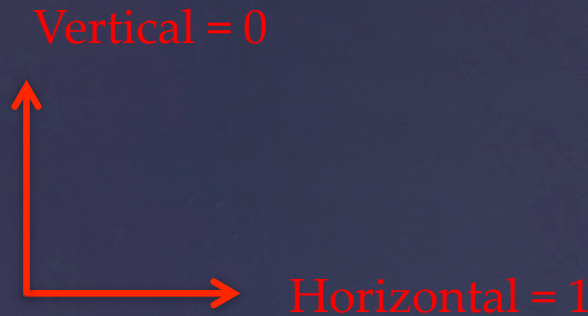
Polarização: Direção de oscilação do vetor campo elétrico



Protocolo BB84: implementação ótica

2 Bases de representação:

- Base Canônica



- Base Rodada a 45°

Antidiagonal = 0

Diagonal = 1



Na transmissão do qubit para formar a chave, Alice escolhe aleatoriamente uma base e um estado:



base canônica



0



1



base rodada



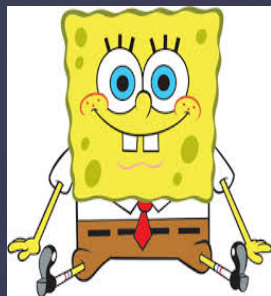
0



1

Protocolo BB84: implementação ótica

Na recepção de cada qubit para formar a chave, Bob escolhe aleatoriamente uma base para efetuar a medida:



base canônica



base rodada

Assim quando termina o processo de envio e recepção de um certo número de qubits temos uma situação do tipo:



BC	BR	BR	BC	BC	BR	BC	BR	BR	BC	BC	BC	BR	BC	BR	BR	BR
0	0	1	0	1	0	1	1	1	0	0	1	0	0	1	0	1
↑		↑	↑			↑	↑	↑			↑	↑	↑	↑		↑
BC	BC	BR	BC	BR	BR	BC	BR	BC	BR	BC	BC	BR	BC	BC	BR	BR



A chave é formada pelos qubits correspondentes a bases iguais. Por que?

Protocolo BB84: Preparação do estado



Fonte de geração de fótons: laser atenuado com polarização bem definida.

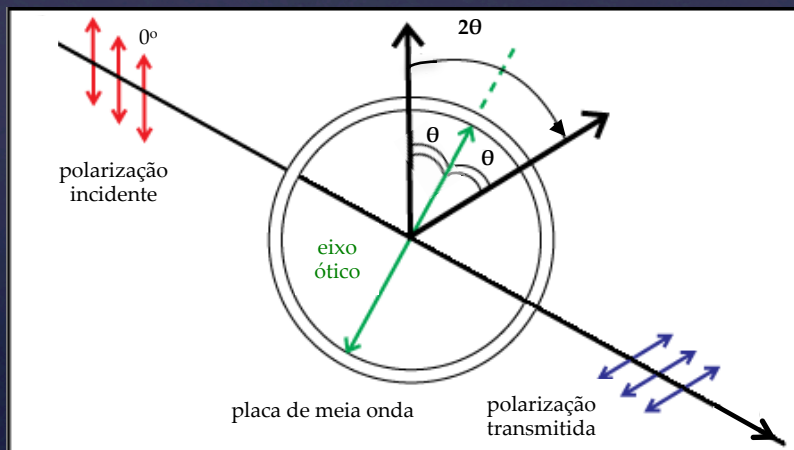
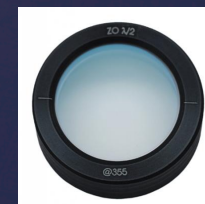


Exemplo: polarização vertical



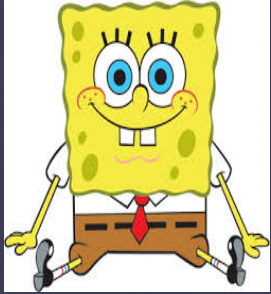
Preparação do estado:

- Utiliza-se um dispositivo ótico denominado placa de meia onda (HWP), capaz de mudar a polarização de acordo com o ângulo formado pela a orientação de seu *eixo ótico* e a a orientação da polarização incidente:

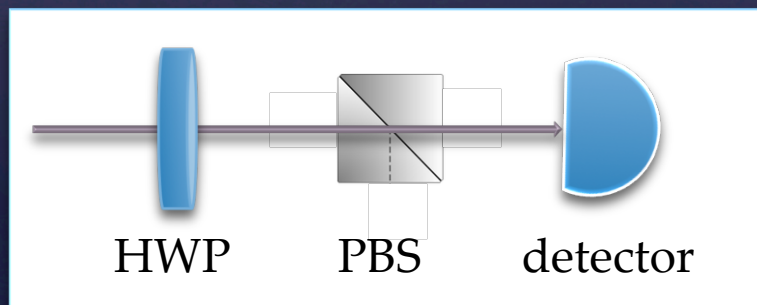
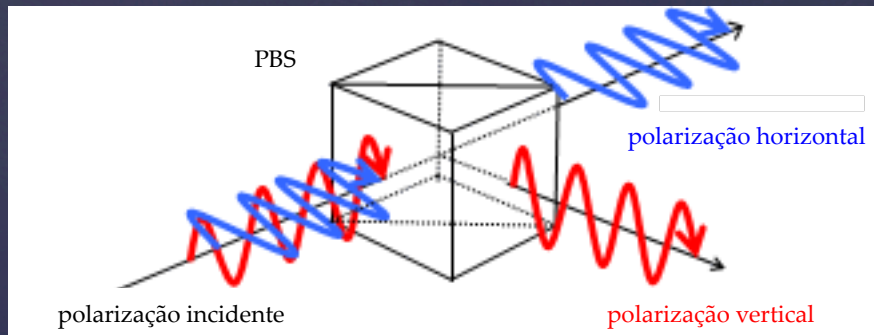


Estado	Ângulo da Placa
Vertical	0°
Horizontal	45°
Diagonal	$22,5^\circ$
Antidiagonal	$-22,5^\circ$

Protocolo BB84: Medida do estado

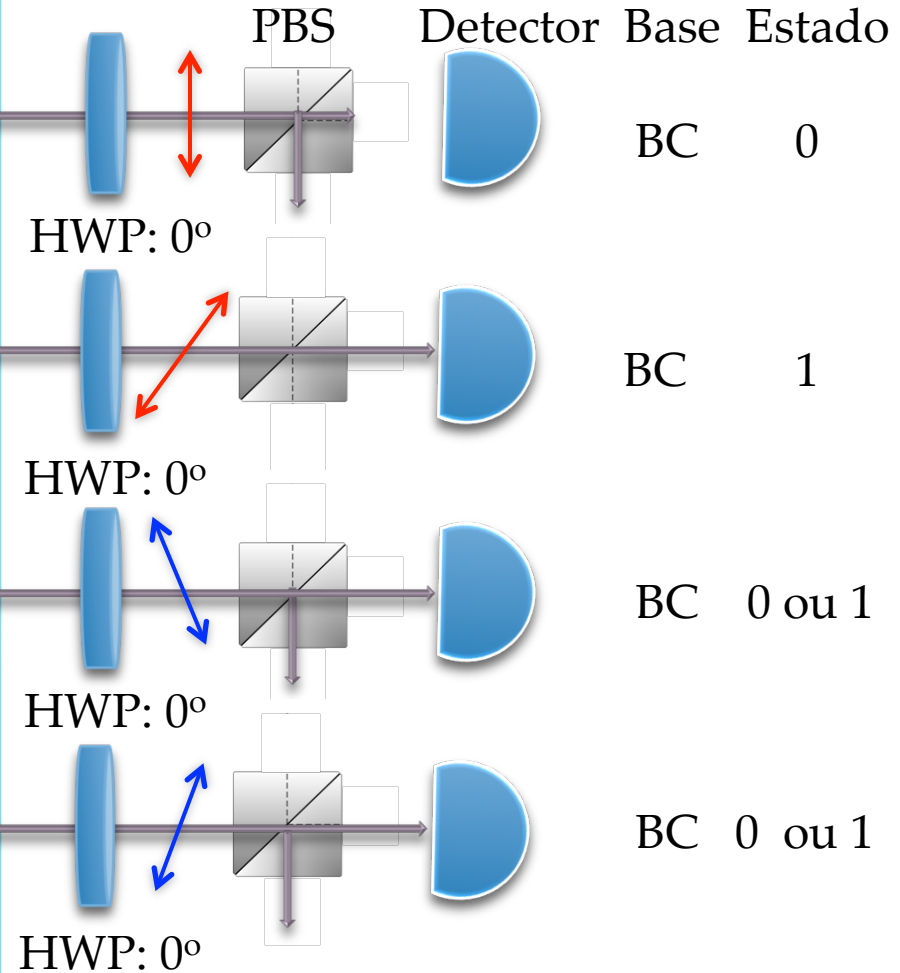
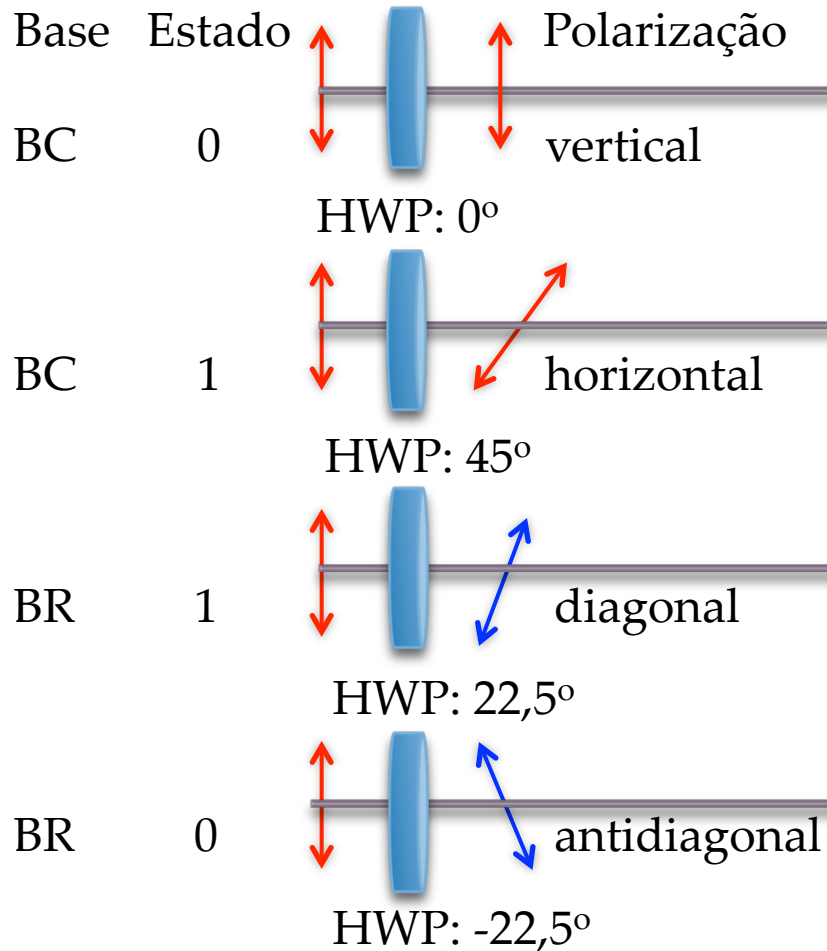


A medida é realizada conjuntamente com uma placa de onda, outro dispositivo óptico denominado divisor de feixes polarizado (PBS), que transmite polarização horizontal e reflete polarização vertical e um detector de fótons.

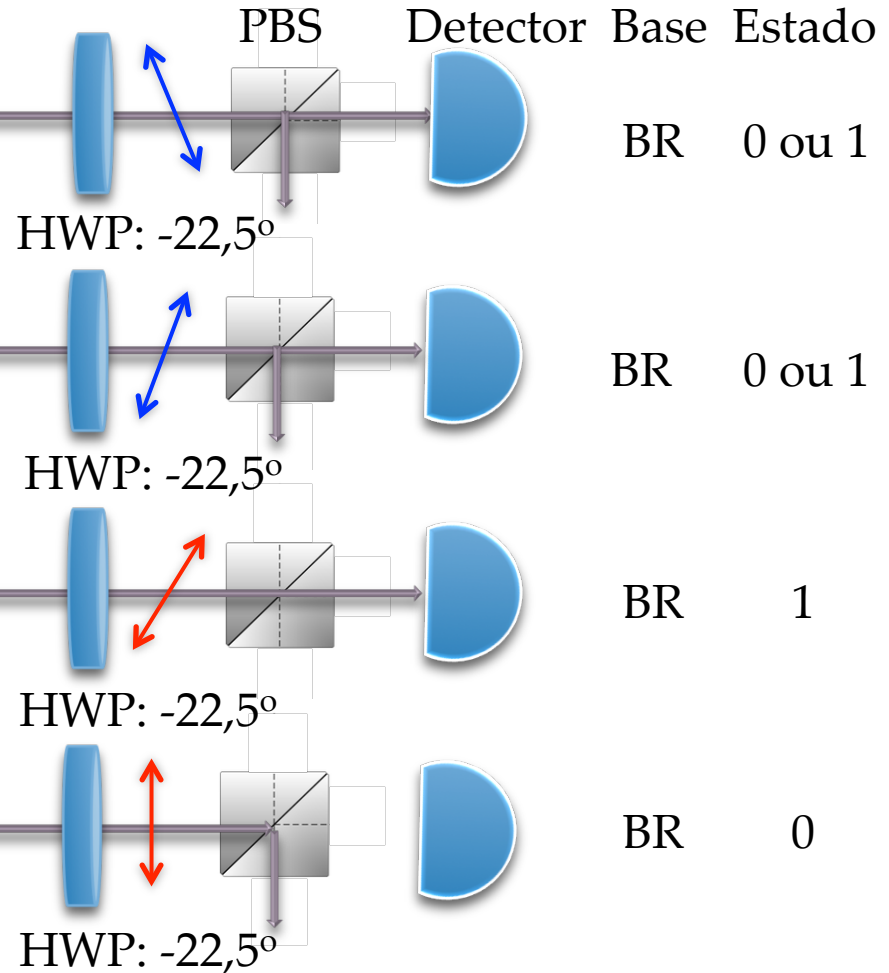
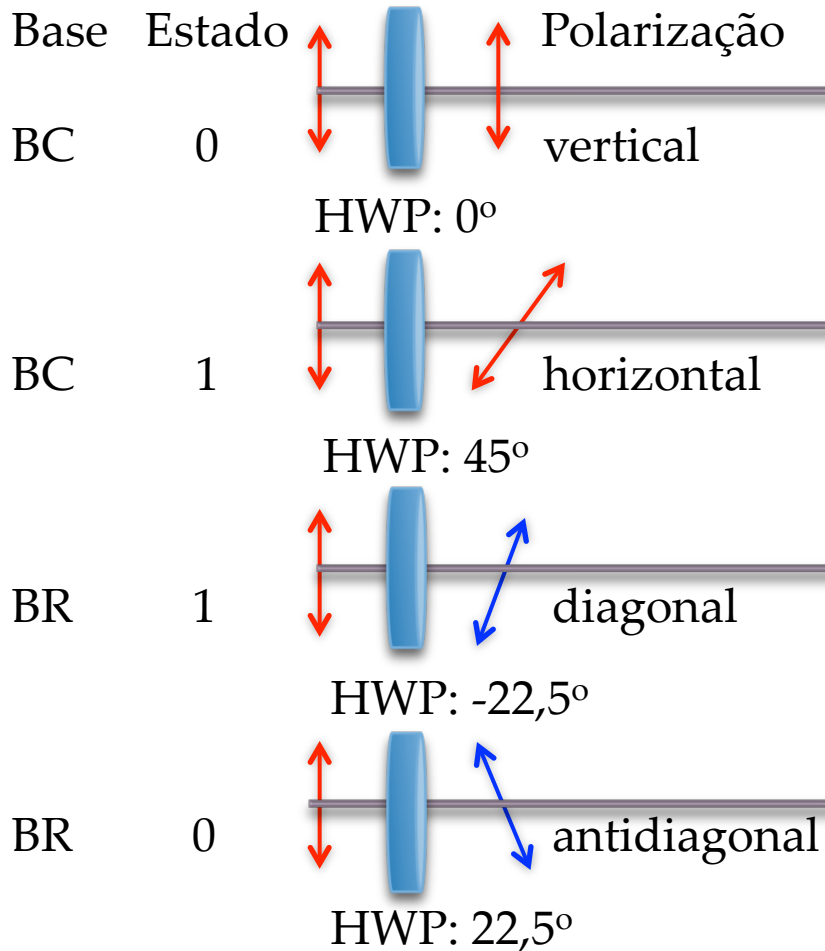


Base de Medida	Ângulo da Placa
Canônica	0°
Rodada a 45°	$-22,5^\circ$

Protocolo BB84: situações possíveis

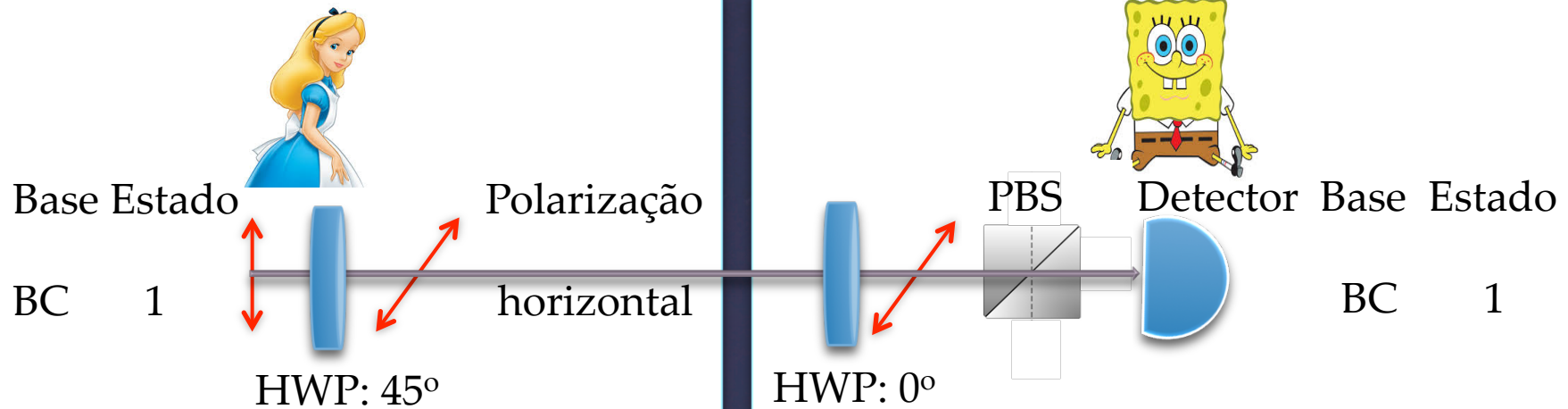


Protocolo BB84: situações possíveis

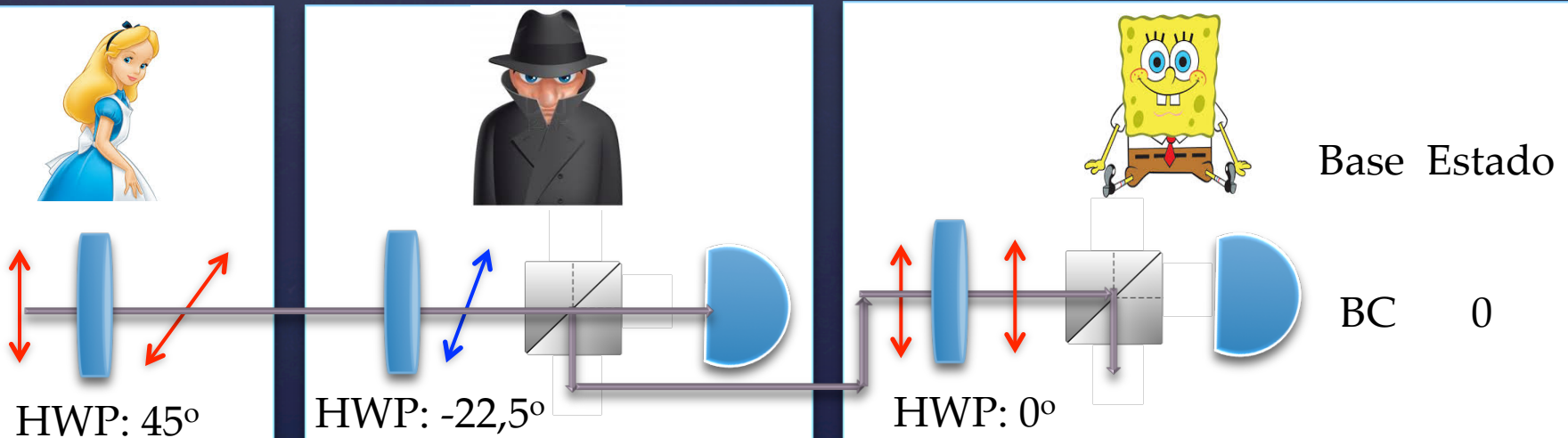


Protocolo BB84: Detecção do espião

- Sem espião: bases de Alice e Bob coincidem, estado coincide



- Com espião: bases de Alice e Bob coincidem, estado pode coincidir ou não



Protocolo BB84: Mecânica Quântica

- Superposição:

Utilização de bases diferentes, onde os vetores de uma base são superposições dos vetores da outra base.

- Colapso da medida:

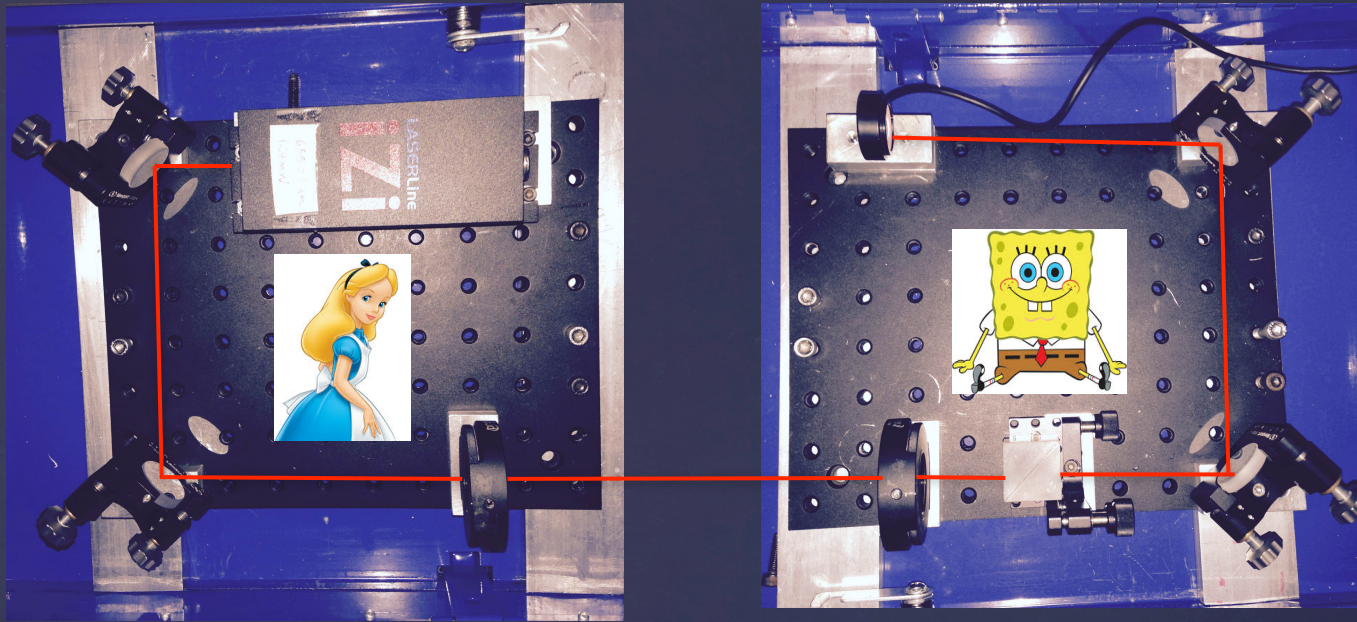
Qualquer tentativa de interceptar a mensagem (processo de medida) interfere na mensagem.

- Teorema da não-clonagem:

É impossível copiar um estado quântico sem destruí-lo.

Espião não pode, pelas leis da mecânica quântica, copiar o estado para mandá-lo para Bob e fazer sua medida no estado original de tal modo que quando usasse a informação das bases de medida e preparação pudesse reproduzir a chave.

Experimento do LOQ-UFRJ



Obs: Usando um feixe clássico, no caso de base trocada metade do feixe é transmitida pelo PBS, metade é refletida.

Espera-se na medida metade do valor. A simulação do caso quântico, fóton transmitido OU refletido, se dará considerando a potência medida:

$P_m > P_{max}/2 \rightarrow 1$ (fóton transmitido) $P_m < P_{max}/2 \rightarrow 1$ (fóton refletido)

que tem tal comportamento devido às flutuações.

Sistemas Comerciais de Criptografia



T +41 22 301 83 71 | E info@idquantique.com

[SUPPORT](#)

[RANDOM NUMBER
GENERATION](#) ▾

[QUANTUM-SAFE
CRYPTO](#) ▾

[PHOTON
COUNTING](#) ▾

[NEWS & EVENTS](#) ▾

[RESOURCE CENTRE](#) ▾

[ABOUT IDQ](#) ▾

ID Quantique

Redefining the fields of Random Numbers, Quantum-Safe
Crypto & Photon Counting



SWISS
QUANTUM

ID Quantique

QUANTUM-SAFE CRYPTO – PHOTON COUNTING – RANDOMNESS

ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services to the financial industry, enterprises and government organisations globally.

IDQ also commercializes a quantum random number generator, which is the reference in the gaming and lottery industries.

Additionally, IDQ is a leading provider of optical instrumentation products; most notably photon counters and related electronics. The company's innovative photonic solutions are used in both commercial and research applications.

News & Press

KPN's CISO calls for Post-Quantum
Cryptography within 5 years

[> Read More](#)

Gemalto launch SafeNet CN8000 Multi-
Link Encryptor

[> Read More](#)

Meet us at QIP 2015, Leeds



Quantum Optics and Information
Universidade Federal do Rio de Janeiro

O@brig%ad*a!!1

Alices:



Nina
Pompeu



Amanda
Nicotina

Espião:



????

Bobs:



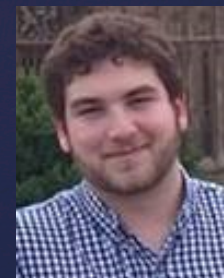
Paulo
Sahium



Otávio
Cals



Yohan
Vianna



Matheus
Esteves

EIQ: Encontros de Informação Quântica