

# Segurança da Informação

Criptografia Quântica e Pós-Quântica

# Criptografia Quântica

# Objetivo

- Conceitos básicos de física quântica (necessário para compreender o processo de computação quântica).
- Impacto da computação quântica sobre a segurança da informação.
- Protocolos quânticos e suas limitações.

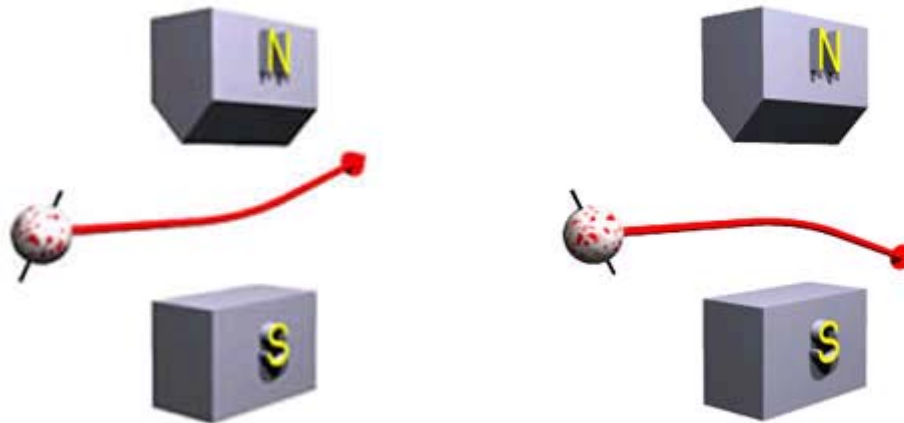
# Advertências

“Anybody who is not shocked by quantum theory has not understood it” (Niels Bohr).

“Nobody really understands quantum theory” (Richard Feynman).

# Experimento de Stern-Gerlach

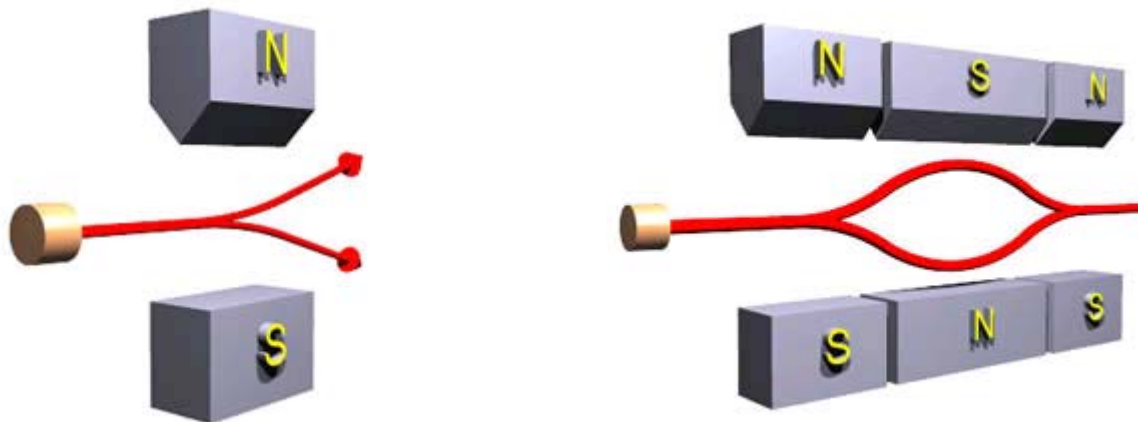
- Deflexão de átomos de hidrogênio neutro num campo magnético:



- Resultado esperado: momento dipolar orientado aleatoriamente  $\Rightarrow$  feixe de átomos de hidrogênio neutro espalhado uniformemente.

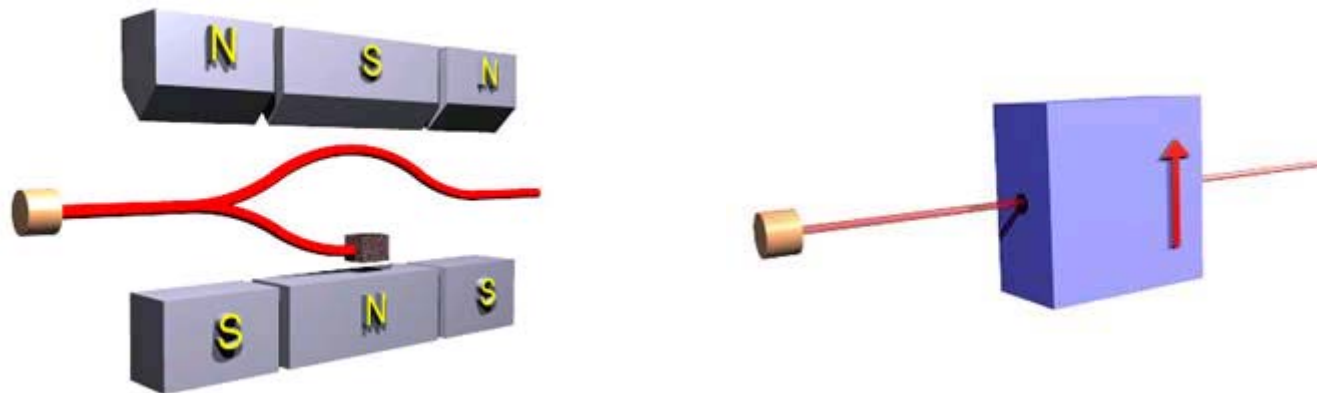
# Experimento de Stern-Gerlach

- Resultado efetivo: divisão do feixe em dois subfeixes iguais na direção  $z$ ! (deflexão com exatamente a *mesma* magnitude para cima ou para baixo, virtualmente sem dispersão na direção  $z$ ):



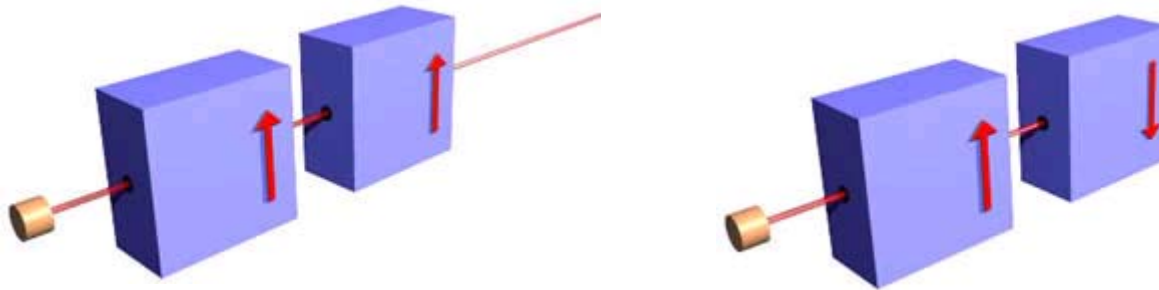
# Experimento de Stern-Gerlach

- Interpretação superficial: cada elétron tem a *mesma* carga total, a *mesma* distribuição espacial de carga, e um movimento intrínseco de rotação (spin) com a *mesma* velocidade angular (nos dois sentidos).
- Consequência dessa interpretação: filtro de sp

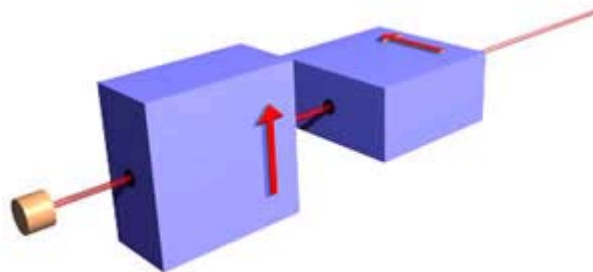


# Experimento de Stern-Gerlach

- Efeitos esperados do filtro de spin:



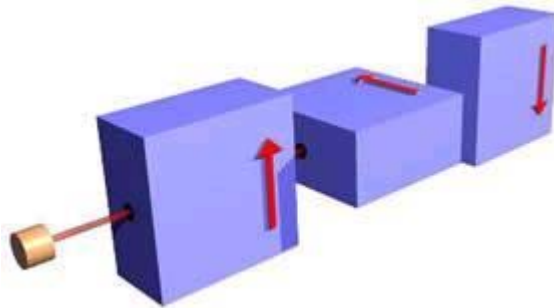
- Medições ortogonais deveriam ser independentes:



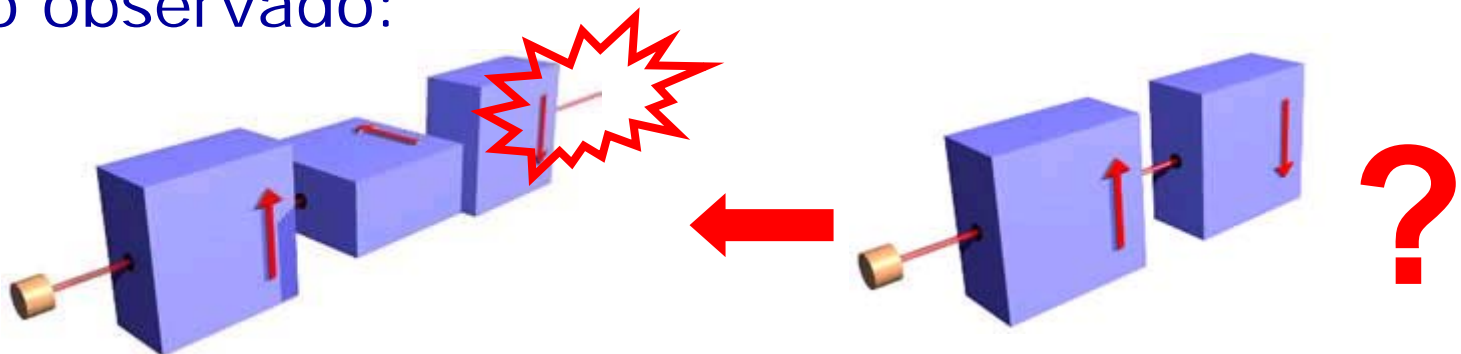


# Experimento de Stern-Gerlach

- Efeito esperado de medições ortogonais sucessivas:



- Efeito observado:



# Experimento de Stern-Gerlach

- Conclusões:
  - O elétron possui momento angular intrínseco (spin) quantizado em dois estados discretos  $|\pm z\rangle$ , originando um momento magnético igualmente quantizado.
  - Os componentes do spin em direções ortogonais *não* são independentes.

$$|\pm z\rangle = \frac{|+x\rangle \pm |-x\rangle}{\sqrt{2}}, \quad |\pm x\rangle = \frac{|+z\rangle \pm |-z\rangle}{\sqrt{2}}$$

# Qubit

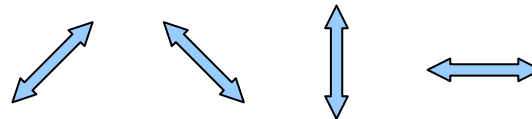
- Assim como o spin, outras propriedades físicas são descritas por combinações (superposições) de dois estados clássicos denotados  $|0\rangle$  e  $|1\rangle$ , e.g. polarização de um fóton em  $0^\circ$  ou  $90^\circ$ .
- Um estado desses chama-se *qubit*, e escreve-se  $a|0\rangle + b|1\rangle$ , onde  $a$  e  $b$  são coeficientes complexos com  $|a|^2 + |b|^2 = 1$ .

# Protocolo Bennett-Brassard

- Idéia: codificar as informações usando propriedades físicas não simultaneamente mensuráveis.
- Exemplo:
  - somente polarizações *ortogonais* de fótons podem ser simultaneamente medidas;
  - um feixe de fótons com quatro polarizações ( $0^\circ$ ,  $45^\circ$ ,  $90^\circ$ ,  $135^\circ$ ) permite distinguir *somente* entre  $0^\circ$  vs.  $90^\circ$  (polarizações retas) *ou* entre  $45^\circ$  vs.  $135^\circ$  (polarizações oblíquas).

# Protocolo Bennett-Brassard

- Alice envia para Beto um feixe de fótons, escolhendo aleatoriamente a polarização de cada fóton dentre as quatro possibilidades:



- Beto escolhe aleatoriamente que tipo de medição (reta ou oblíqua) vai realizar com cada fóton recebido, e registra a polarização medida, mantendo o resultado em segredo.



- N.B.: As escolhas de Alice e de Beto são independentes, podendo coincidir ou não.

# Protocolo Bennett-Brassard

- O resultado de uma medição será *sinal* ou *ruído* conforme a escolha de Beto coincidir ou não com a escolha de Alice.
- Beto ainda não tem como saber se qualquer medida particular é sinal ou ruído, isto é, se a sua escolha entre medida reta ou oblíqua coincidiu ou não com a escolha de Alice.

# Protocolo Bennett-Brassard

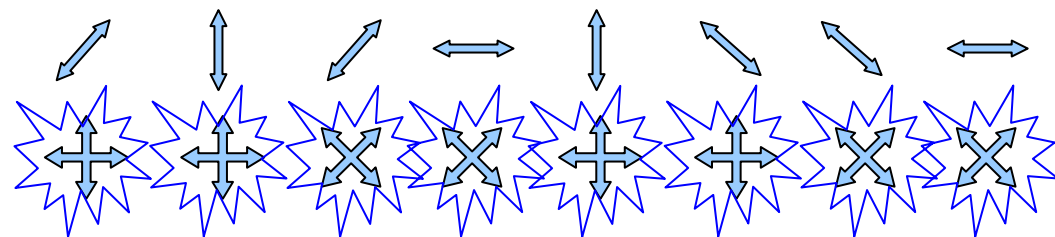
- Ao final da transmissão de Alice, Beto anuncia publicamente o *tipo* de medição (reta ou oblíqua) efetuada para cada fóton, mas não o *resultado*.
- Alice responde indicando quais escolhas de Beto coincidiram com as suas próprias.
- As polarizações dos fótons onde as escolhas coincidiram soletram os bits da chave negociada, e.g. segundo a convenção  $0^\circ = 45^\circ = \mathbf{0}$ ,  $90^\circ = 135^\circ = \mathbf{1}$ .

# Protocolo Bennett-Brassard

## Parte Quântica:

Alice (sinais aleatórios):

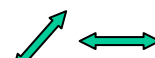

Beto (medições aleatórias):



## Parte Clássica:

Discussão pública  
sobre canal confiável



Convenção: {  
0:   
1: 



# Protocolo Bennett-Brassard





























- Que resistência este protocolo oferece contra escuta não autorizada ("grampo")?
- Se a linha estiver sendo grampeada, as polarizações dos fótons será afetada: *qualquer* medição (incluindo o "grampo") de um estado físico *altera* esse estado.

# Protocolo Bennett-Brassard

- Alice e Beto revelam e comparam publicamente o valor gerado e o valor medido de  $n$  bits aleatoriamente selecionados da chave. Esses bits são depois descartados.
- A probabilidade de um grampo ser bem sucedido com  $n$  bits coincidentes é  $2^{-n}$ .

# Protocolo Bennett-Brassard

## Parte Quântica:

Te Quântica:	1	0	1	1				
Alice (sinais aleatórios):								
Geraldo (grampo):								
								
Beto (medições aleatórias):								

## Parte Clássica:

Discussão pública  
sobre canal confiável

Convenção:  $\left\{ \begin{array}{l} 0: \\ 1: \end{array} \right. \left\{ \begin{array}{l} \text{diagonal up-right} \\ \text{horizontal right} \end{array} \right.$

# Limitações

- Os protocolos quânticos de acordo de chave têm uma falha estrutural: a *autenticidade* da chave negociada depende de um canal *clássico* confiável.
- Exemplo: no protocolo Bennett-Brassard, Beto precisa anunciar publicamente os tipos das medições efetuadas, e Alice precisa indicar quais escolhas foram corretas.

# Limitações

- Aparentemente (salvo pesquisas muito recentes, ainda incompletas), a segurança do sistema como um todo *não* pode ser garantida exclusivamente pelas leis da física quântica.
- Dilema: que vantagem pode ter um sistema quântico cuja segurança depende de uma informação clássica?

# Apêndice

## Criptografia Pós-Quântica

# Sistemas compostos

- Dois qubits independentes  $|\psi\rangle = a|0\rangle + b|1\rangle$  e  $|\phi\rangle = c|0\rangle + d|1\rangle$  constituem um estado composto  $|\psi\rangle|\phi\rangle = (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$ .
- Certos sistemas de dois qubits *não* podem ser escritos de forma separada, embora sejam uma superposição de estados observáveis  $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ .

# Emaranhamento

- Esses estados são ditos *emaranhados*.  
Exemplo:

$$|s\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

- Estados emaranhados de  $n$  qubits podem representar  $2^n$  valores *simultaneamente*.
- N.B.:  $n$  bits clássicos podem representar  $2^n$  valores, mas só um de cada vez.



# Paralelismo Quântico

- Se uma função clássica  $f(x)$  com argumento de  $n$  bits puder ser implementada como um operador linear unitário, poderá ser aplicada sobre um registrador de  $n$  qubits.
- Se esses  $n$  qubits estiverem emaranhados, a função será calculada *simultaneamente* sobre todos os  $2^n$  valores possíveis do seu argumento.

# Impacto sobre Complexidade

- Classes de problemas:
  - P: problemas solúveis em tempo polinomial determinístico.
  - NP: problemas solúveis em tempo polinomial não determinístico.
  - PSPACE: problemas solúveis em espaço polinomial.
- Obviamente  $P \subseteq NP \subseteq PSPACE$ , mas não se sabe se  $P = PSPACE$ .

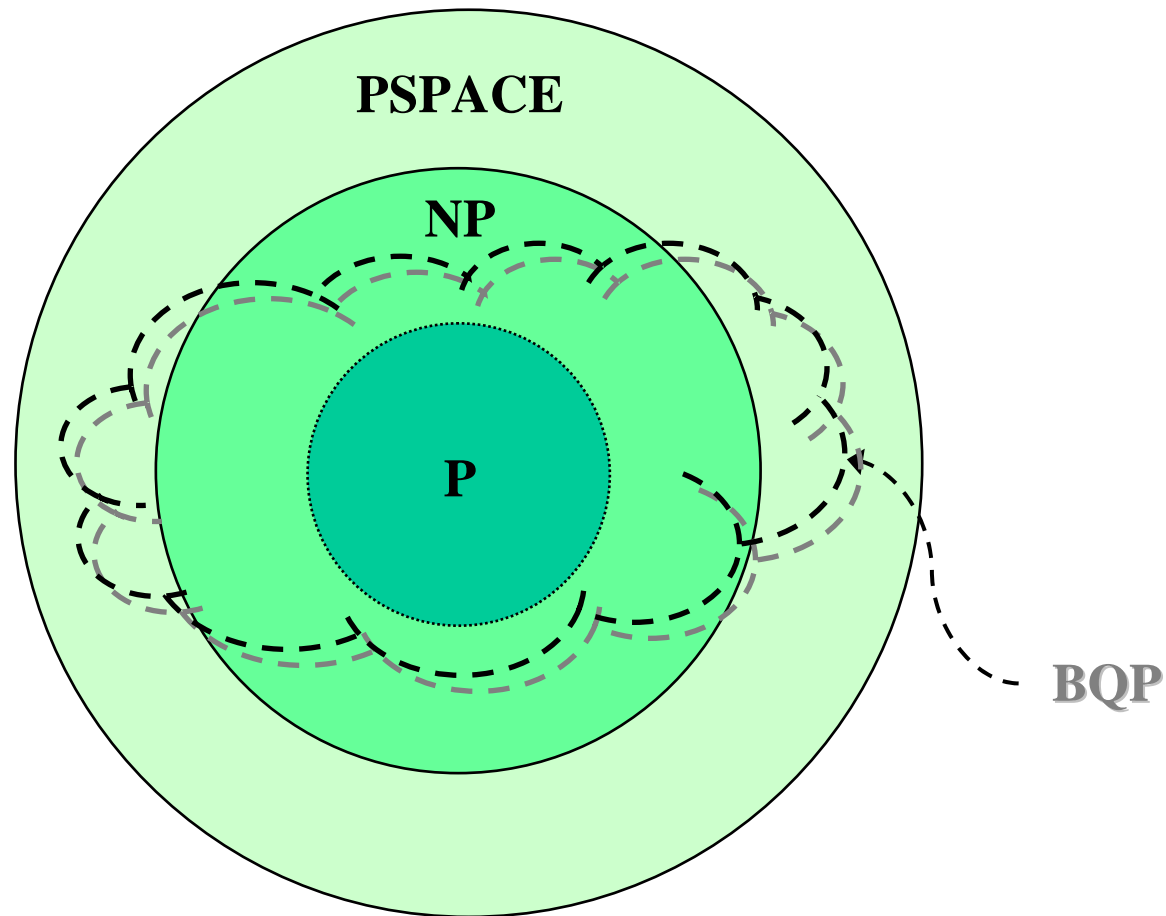
# Impacto sobre Complexidade

- Computadores quânticos podem resolver eficientemente qualquer problema em  $P$  (basta emular um computador clássico).
- Computadores quânticos *não* podem resolver eficientemente problemas fora de  $PSPACE$ , pois exigiriam um número superpolinomial de portas quânticas.

# Impacto sobre Complexidade

- A classe dos problemas solúveis eficiente-mente por computadores quânticos é chamada BQP.
- $P \subseteq BQP \subseteq PSPACE$ .
- Não se conhece a relação exata entre BQP e as demais classes de problemas.

# Impacto sobre Complexidade



# Impacto sobre Segurança

- Algoritmos quânticos podem resolver **IFP** e **DLP** em tempo polinomial.



# Impacto sobre Segurança

- Se  $P \neq NP$ , pode acontecer que  $P \subset BQP \subset NP$ , e alguns problemas NP-difíceis ainda poderiam servir de base para definir primitivas criptográficas (“pós-quânticas”).
- Se um computador quântico puder resolver eficientemente um problema NP-completo, então  $P = NP \subseteq BQP$ , e alguma abordagem completamente nova para a criptografia terá que ser elaborada e adotada.

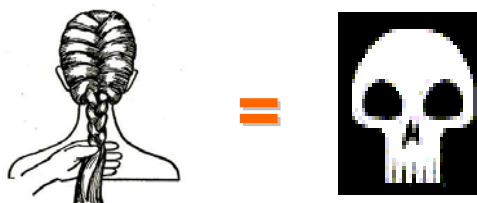
# Sistemas Pós-Quânticos

- Grupos Não-Abelianos
  - Análogos de esquemas baseados no DLP sobre grupos de tranças, grupos hiperbólicos e outros grupos não-abelianos.
- Redução de Reticulados
  - Ajtai-Dwork, GGH, Regev, NTRU, LWE, Peikert...
- Decodificação de Síndromes
  - McEliece, Niederreiter, CFS, ...
- Outros sistemas
  - Núcleos e percéptrons permutados, sistemas quadráticos multivariados, equações lineares vinculadas, posto mínimo, assinaturas de Merkle, ...



# Sistemas Pós-Quânticos

- Sistemas baseados em grupos de tranças são conceitualmente simples devido à herança da criptografia convencional (e.g. acordo de chaves no estilo DH).
- Contudo – a exemplo dos sistemas baseados no problema da mochila – todos os protocolos propostos até agora sobre grupos de tranças foram quebrados.



# Sistemas Pós-Quânticos

- A capacidade de resolver o DHSP é suficiente para quebrar as hipóteses de segurança comuns de sistemas baseados em reticulados (Regev 2002).
- $\exists$  algoritmos quânticos para resolver o DHSP com complexidade subexponencial (mas superpolinomial):
  - Tempo  $2^{O(\sqrt{n})}$ , espaço  $2^{O(\sqrt{n})}$  (Kuperberg 2003).
  - Tempo  $2^{O(\sqrt{n \log n})}$ , espaço  $O(n)$  (Regev 2006).

# Sistemas Pós-Quânticos

- Decodificação de síndromes e redução de reticulados parecem bastante promissores (nenhum resultado negativo de segurança).
- Eficiência:
  - alto desempenho (complexidade quadrática, vs. cúbica em sistemas baseados em IFP e DLP);
  - assinaturas compactas (comprimento “entrópico”).
- Restrição: chaves grandes (obter sistemas com chaves compactas é um interessante problema de pesquisa).