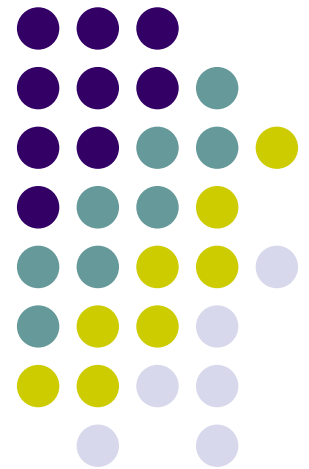


Computação Quântica

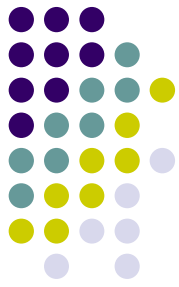
Paulo Mateus

Centro de Lógica e Computação
Instituto Superior Técnico

NEEI-IST



Motivação



- Lei de Moore



Gordon Moore (co-fundador da Intel)

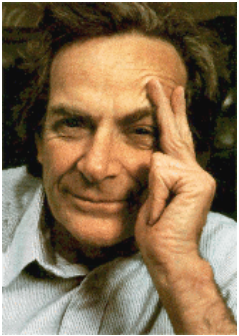
O número de transístores por polegada quadrada deve duplicar por ano (1965).

- A minituarização crescente dos circuitos... relevância dos efeitos quânticos cada vez mais próxima..
- Qual é o limite do computador clássico?

Motivação



- Simulação de sistemas quânticos



Richard Feynman
(Prémio Nobel da Física 1965)

Se os sistemas quânticos parecem necessitar de recursos computacionais exponenciais para serem simulados por computadores, por que não utilizar estes sistemas para fazer computação? (1982)

Motivação

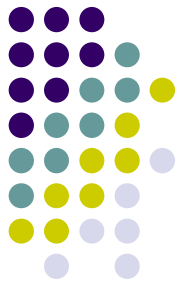


- P=NP? (1 000 000 USD)
 - Multiplicar $\in P$
 - Factorizar $\in NP$
 - RSA12: 8 meses usando 1600 computadores
 - 1000 dígitos: mais do que a vida do universo!!!
- Será possível construir computadores (ou algoritmos) mais eficientes?



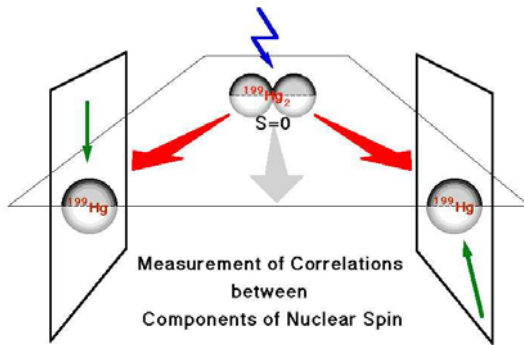
Motivação

- Criptografia – distribuição de chave
 - **Segurança computacional**
A chave distribuída é segura apenas contra ataques de adversários com poder polinomial.
 - **Segurança perfeita**
A chave distribuída é segura contra qualquer adversário.
- Existe algum protocolo de distribuição de chave por canal público perfeitamente seguro?



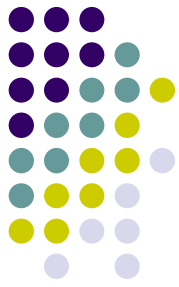
Motivação

- Paradoxo Einstein-Podolsky-Rosen



É a Mecânica Quântica uma teoria completa? (EPR 1935)

- Teorema de Bell (1964)
- Entrelaçamento permite correlação à distância, porque não utilizar este efeito para melhorar a comunicação/sincronização?



Mecânica quântica

- **1º Postulado**

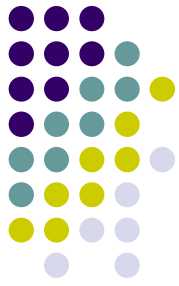
O estado de um sistema quântico fechado é descrito por um vector unitário de um espaço de Hilbert (complexo).

- **Exemplo:** qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

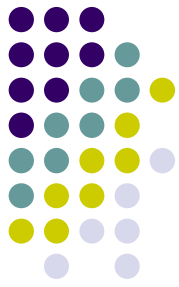
onde $|\alpha|^2 + |\beta|^2 = 1$

Mecânica quântica



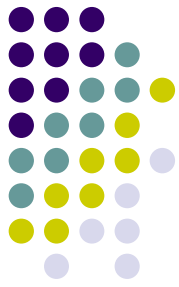
● 2º Postulado

- Uma observação de um sistema quântico é definida por uma decomposição ortogonal em subespaços do espaço de estados.
- Cada componente é observado com probabilidade igual à norma da projecção no subespaço associado.
- O estado evolui para a projecção (normalizada) no subespaço da componente observada.



Mecânica quântica

- **Exemplo:** Observação computacional
A decomposição computacional do espaço de estados de um qubit é $\{ |0\rangle, |1\rangle \}$. Seja $|\psi\rangle$ um qubit no estado $\alpha|0\rangle + \beta|1\rangle$, então
 - 0 é observado com probabilidade $|\alpha|^2$
 - 1 é observado com probabilidade $|\beta|^2$



Mecânica quântica

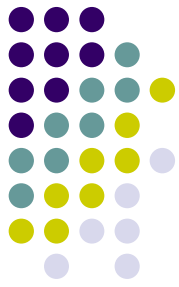
- **Exemplo:** Observação diagonal

A decomposição diagonal do espaço de estados de um qubit é

$$\{ |0\rangle+|1\rangle/2^{1/2}, |0\rangle-|1\rangle/2^{1/2}\}.$$

Seja $|\psi\rangle$ um qubit no estado $\alpha|0\rangle + \beta|1\rangle$, então

- + é observado com probabilidade $|\alpha+\beta|^2/2$
- - é observado com probabilidade $|\alpha-\beta|^2/2$



Mecânica quântica

- **Aplicação:** Geração de números aleatórios

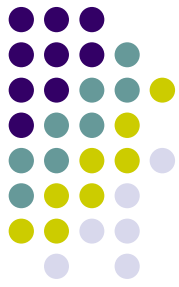


$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Ao aplicar a observação computacional a $|\psi\rangle$

- 0 é obtido com probabilidade $\frac{1}{2}$
- 1 é obtido com probabilidade $\frac{1}{2}$

Id quantique – <http://www.idquantique.com>



Mecânica quântica

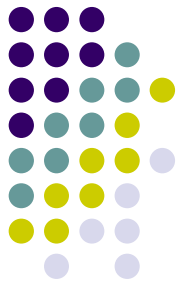
- **3º Postulado**

O espaço de estado de um sistema composto por dois sistemas é descrito pelo produto tensorial dos espaços das componentes.

- **Exemplo:** 2 qubits

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

onde $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$



Criptografia quântica

- Estado EPR de um par de qubits

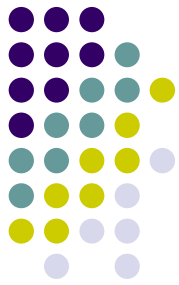
$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- Fazendo uma observação computacional
 - 00 é observado com probabilidade $\frac{1}{2}$
 - 11 é observado com probabilidade $\frac{1}{2}$
- Fazendo uma observação diagonal
 - ++ é observado com probabilidade $\frac{1}{2}$
 - -- é observado com probabilidade $\frac{1}{2}$

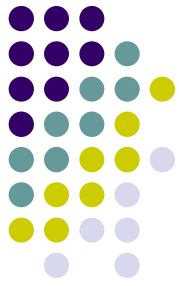
Criptografia quântica

Alice

Bruno



Criptografia quântica



Alice

$$|\Psi_1\rangle_A$$

$$|\Psi_2\rangle_A$$

$$|\Psi_3\rangle_A$$

$$|\Psi_4\rangle_A$$

$$|\Psi_5\rangle_A$$

$$|\Psi_6\rangle_A$$

...

Bruno

$$|\Psi_1\rangle_B$$

$$|\Psi_2\rangle_B$$

$$|\Psi_3\rangle_B$$

$$|\Psi_4\rangle_B$$

$$|\Psi_5\rangle_B$$

$$|\Psi_6\rangle_B$$

...

Partilham n pares EPR

Criptografia quântica



Alice

0 $|\psi_1\rangle_A$

1 $|\psi_2\rangle_A$

0 $|\psi_3\rangle_A$

1 $|\psi_4\rangle_A$

0 $|\psi_5\rangle_A$

1 $|\psi_6\rangle_A$

...

Bruno

0 $|\psi_1\rangle_B$

0 $|\psi_2\rangle_B$

1 $|\psi_3\rangle_B$

1 $|\psi_4\rangle_B$

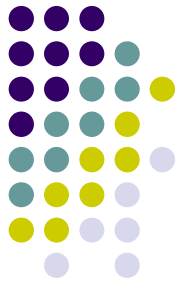
0 $|\psi_5\rangle_B$

1 $|\psi_6\rangle_B$

...

Geram aleatoriamente n bits

Criptografia quântica



Alice

0 $|\psi_1\rangle_A$

1 $|\psi_2\rangle_A$

0 $|\psi_3\rangle_A$

1 $|\psi_4\rangle_A$

0 $|\psi_5\rangle_A$

1 $|\psi_6\rangle_A$

...

Bruno

0 $|\psi_1\rangle_B$

0 $|\psi_2\rangle_B$

1 $|\psi_3\rangle_B$

1 $|\psi_4\rangle_B$

0 $|\psi_5\rangle_B$

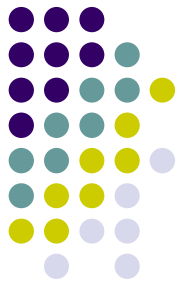
1 $|\psi_6\rangle_B$

...

0 – observa-se o qubit com o observável computacional $\{0,1\}$

1 – observar o qubit com o observável diagonal $\{+,-\}$

Criptografia quântica



Alice

$1 \leftarrow 0 \quad |\psi_1\rangle_A$

$+ \leftarrow 1 \quad |\psi_2\rangle_A$

$0 \leftarrow 0 \quad |\psi_3\rangle_A$

$- \leftarrow 1 \quad |\psi_4\rangle_A$

$1 \leftarrow 0 \quad |\psi_5\rangle_A$

$+ \leftarrow 1 \quad |\psi_6\rangle_A$

...

Bruno

$1 \leftarrow 0 \quad |\psi_1\rangle_B$

$0 \leftarrow 0 \quad |\psi_2\rangle_B$

$+ \leftarrow 1 \quad |\psi_3\rangle_B$

$- \leftarrow 1 \quad |\psi_4\rangle_B$

$1 \leftarrow 0 \quad |\psi_5\rangle_B$

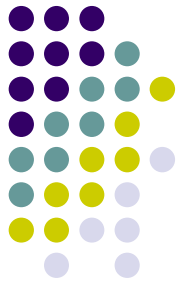
$+ \leftarrow 1 \quad |\psi_6\rangle_B$

...

0 – observa-se o qubit com o observável computacional $\{0,1\}$

1 – observar o qubit com o observável diagonal $\{+,-\}$

Criptografia quântica



Alice

| | |
|-------|--------------------|
| 1 ← 0 | $ \psi_1\rangle_A$ |
| + ← 1 | $ \psi_2\rangle_A$ |
| 0 ← 0 | $ \psi_3\rangle_A$ |
| - ← 1 | $ \psi_4\rangle_A$ |
| 1 ← 0 | $ \psi_5\rangle_A$ |
| + ← 1 | $ \psi_6\rangle_A$ |

...

Bruno

| | |
|-------|--------------------|
| 1 ← 0 | $ \psi_1\rangle_B$ |
| 0 ← 0 | $ \psi_2\rangle_B$ |
| + ← 1 | $ \psi_3\rangle_B$ |
| - ← 1 | $ \psi_4\rangle_B$ |
| 1 ← 0 | $ \psi_5\rangle_B$ |
| + ← 1 | $ \psi_6\rangle_B$ |

...

Publicam a sequência gerada aleatoriamente



Criptografia quântica

Alice

1 ← 0 $|\psi_1\rangle_A$

~~+ ← 1 $|\psi_2\rangle_A$~~

~~0 ← 0 $|\psi_3\rangle_A$~~

- ← 1 $|\psi_4\rangle_A$

1 ← 0 $|\psi_5\rangle_A$

+ ← 1 $|\psi_6\rangle_A$

...

Bruno

1 ← 0 $|\psi_1\rangle_B$

~~0 ← 0 $|\psi_2\rangle_B$~~

~~+ ← 1 $|\psi_3\rangle_B$~~

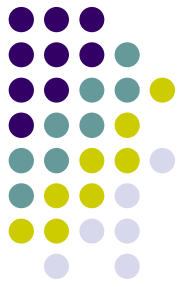
- ← 1 $|\psi_4\rangle_B$

1 ← 0 $|\psi_5\rangle_B$

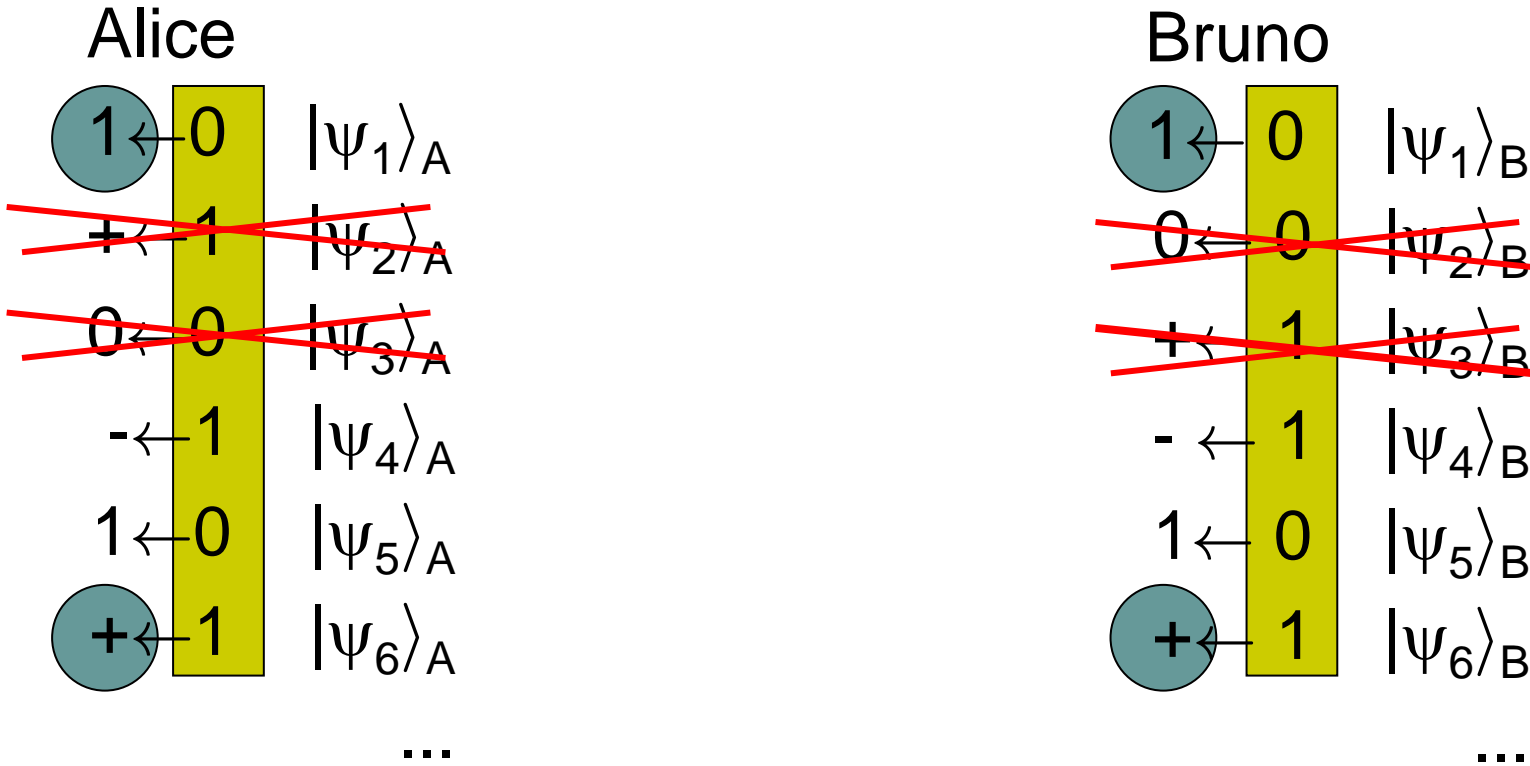
+ ← 1 $|\psi_6\rangle_B$

...

Ignoram as observações para os quais o bit aleatório não coincide

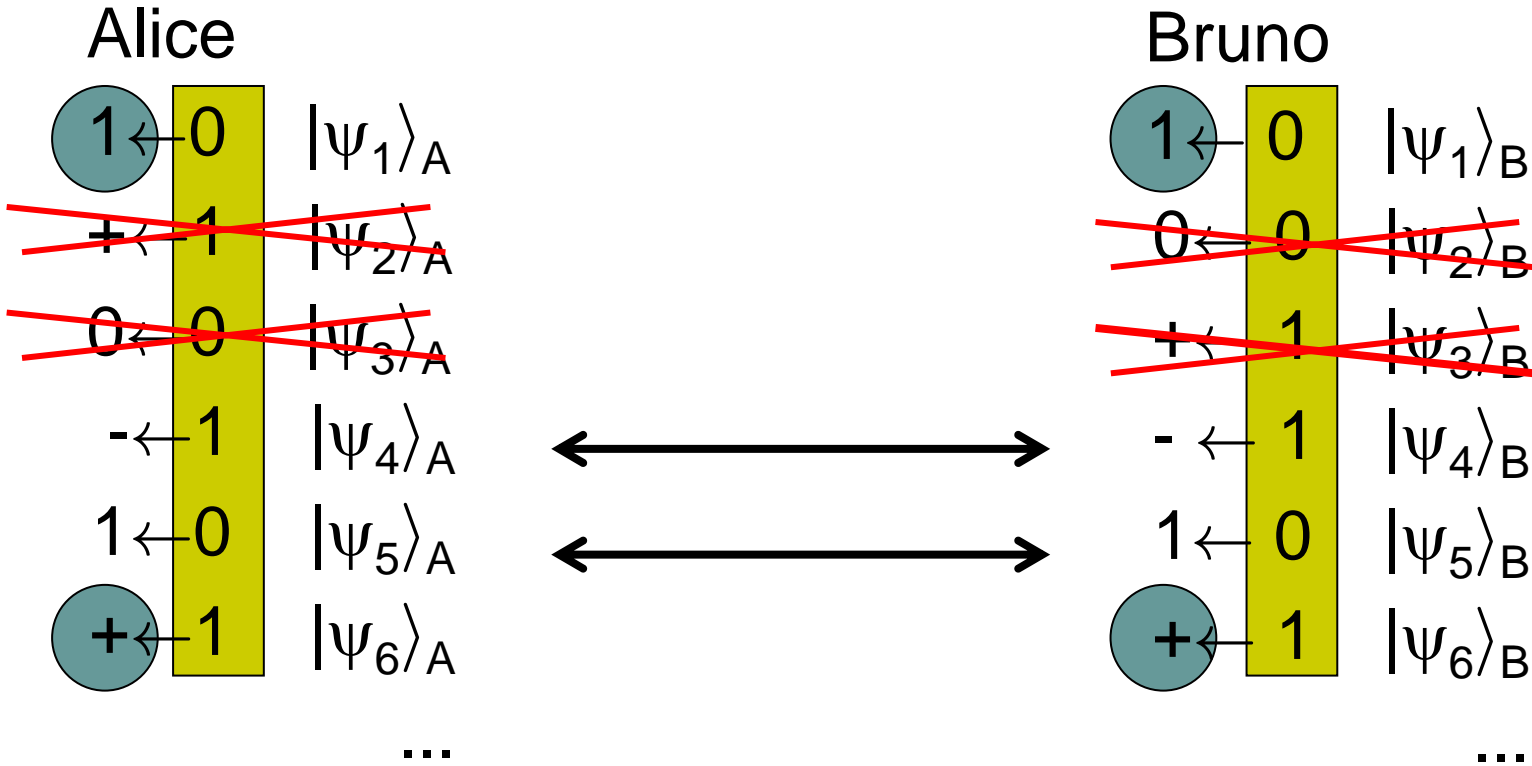
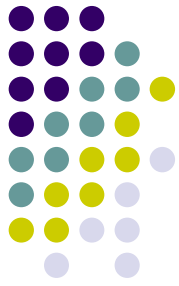


Criptografia quântica



Confirmam que não há interferência da Eva

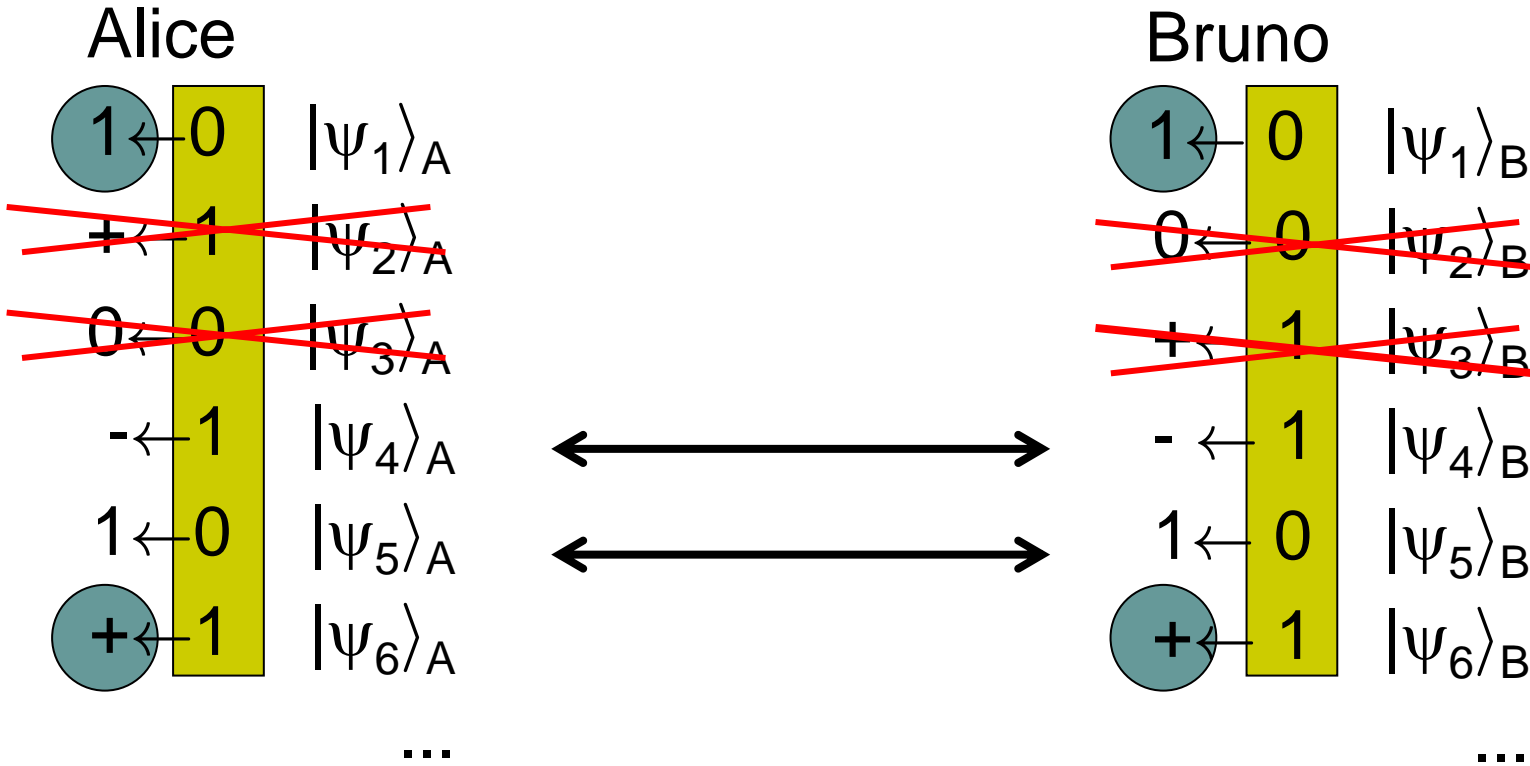
Criptografia quântica



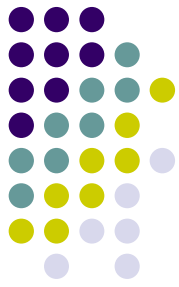
A chave partilhada é obtida pelas restantes observações



Criptografia quântica



Teorema (Shor e Preskill 01): O protocolo Ekert 91 tem segurança perfeita.



Criptografia quântica

- Vectis – Sistema comercial de QCrypto



www.idquantique.com

- Muito investimento e investigação:
 - Sistemas de de QCrypto por satélite
 - Routers para qubits
 - Massificação do uso da informação quântica

Computação quântica



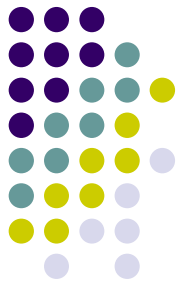
- **4º Postulado**

A evolução de um sistema quântico fechado é descrito por uma transformação unitária sobre o espaço de Hilbert associado.

- **Corolários**

- Teorema da não clonagem
- Computação quântica é reversível

Computação quântica



- Computador quântico
 - Memória – sistema de qubits + sistema de bits
 - Controlo - comandos imperativos usuais enriquecidos com:
 - Aplicação de uma transformação unitária a um conjunto de qubits;
 - Observação de qubits, guardando o resultado da observação num conjunto de bits
- Um computador quântico é probabilístico!!!

Computação quântica

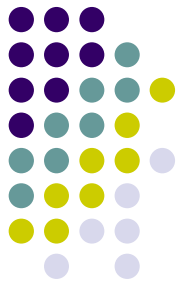


- Algoritmo de factorização de Shor



Peter Shor
(Prémio Nevanlinna 1998
Prémio Gödel 1999)

- O algoritmo de Shor permite atacar eficientemente todos os sistemas criptográficos de chave pública de uso comercial com um computador quântico!!!

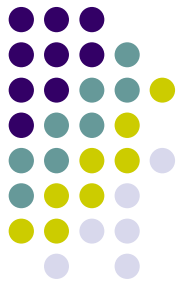


Computação quântica

- Transformada de Fourier quântica
 - Espaço de Hilbert H de dimensão n ($\log(n)$ qubits, e a base é $\{|0\rangle, |1\rangle, \dots, |n-1\rangle\}$)

QFT: $H \rightarrow H$

$$|j\rangle \mapsto \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} e^{2\pi i k j / n} |k\rangle$$



Computação quântica

- Factorizar reduz-se a encontrar a fase de um vector próprio de um operador unitário

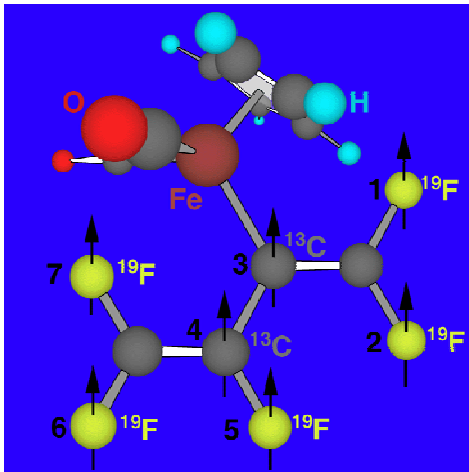
$$U|\psi\rangle = e^{i\theta} |\psi\rangle$$

- Encontrar esta fase reduz-se a aplicar a inversa da transformada de Fourier quântica a um estado alcançável a partir de $|\psi\rangle$
- A transformada de Fourier quântica pode ser calculada em tempo polinomial por um computador quântico



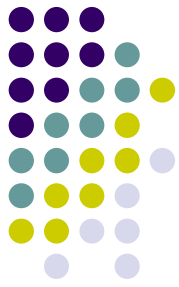
Computação quântica

- Computador quântico da IBM



Computador com 7 qubits, que em 2005 foi estendido para 1 qubyte

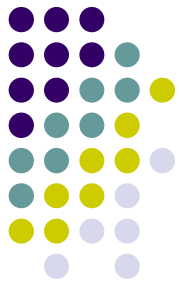
- Nature 2006 – Breakthrough in Quantum computing



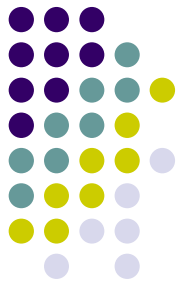
Marcos da CIQ

- Proposta de Benioff (1980): máquina de Turing quântica;
- Proposta de Feynman (1982): computação quântica;
- **Protocolo de Bennett e Brassard** (1984): partilha de chaves privadas; Protocolo de Ekert (1991).
- Proposta de Deutsch (1985): computador quântico universal;
- Protocolo de Bennett e Wiesner (1992): codificação densa;
- Protocolo de Bennett et al (1993): teleportação quântica;
- **Algoritmo de Shor** (1994): decomposição em factores primos;
- Algoritmo de Grover (1995): pesquisa em bases de dados;
- Teorema de DiVincenzo (1995): portas quânticas universais;

Marcos da CIQ

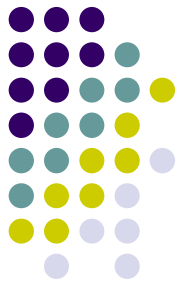


- Teorema de Schumacher (1993/1995): 1o. teorema de Shannon para canais quânticos;
- Shor (1995) and Steane (1996): códigos de correção de erros para viabilização da computação quântica na presença de ruído;
- Teorema de Holevo-Schumacher-Westmoreland (1997/98): minorante da capacidade de canal quântico na presença de ruído;
- Teorema de Lloyd-Shor-Devetak (2005): 2o. teorema de Shannon para canais quânticos.
- Algoritmo de Childs *et al* (2003): pesquisa em grafo;
- **Modelos alternativos de computação quântica (XXI):** equivalência entre circuitos, processos adiabáticos e processos irreversíveis.



Desafios

- Computação quântica
 - Resolução mais eficiente de problemas
 - Ganho exponencial: pesquisa em grafos
 - Factorização em primos polinomial: ganho exponencial?
 - $NP \subseteq BQP$ $SAT \in BQP$
 - Realização de computador quântico:
 - Memória: até 8 qubits em laboratório...
 - Memórias maiores? Utilizáveis na prática?
- Informação quântica
 - Distribuição de chave: 122km
 - Distâncias maiores? Via satélite? Routers?



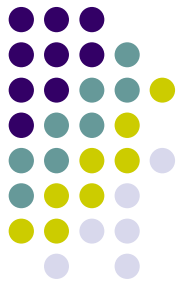
Investigação no CLC-IST

- **Projecto** FEDER POCI/MAT/55796/2004 QUANTLOG
Janeiro 1, 2005 - Dezembro 31, 2007
<http://clc.math.ist.utl.pt/quantlog.html>
- **Seminário** (quase) semanal
QCI: sextas-feiras 15h00 IST PG04.35
(desde 26/09/2003)
<http://sem.math.ist.utl.pt/qci/>
- **Workshop** Lisbon Quantum Computation, Information and Logic (LQCIL'07) IST, 18-20 de Julho de 2007
<http://wslc.math.ist.utl.pt/lqcil07/>

Investigação no CLC-IST



- **Física da CIQ** (com U College)
 - Entrelaçamento em sistemas de estado sólido.
- **Algoritmos quânticos** (com U Waterloo)
 - Pesquisa quântica de padrões genómicos (*NATO ASI*);
 - Comparação entre passeios aleatórios e passeios quânticos;
 - Solução quântica para *SAT* (gap problem).
- **Autómatos quânticos** (com Tsinghua U)
 - Minimização do número de qubits;
 - Composição e interconexão.



Investigação no CLC-IST

- **Lógica quântica exógena** (Kings College et al)
 - Valoração quântica = sobreposição de valorações clássicas;
 - Axiomatização completa (*Information and Computation*);
 - Lógica de Hoare para programas quânticos.
- **Aplicações em segurança** (U Berkeley e U Penn)
 - Composicionalidade de protocolos quânticos (*ENTCS*);
 - Ataques quânticos a protocolo clássico de sistema de prova sem transferência de conhecimento;
 - Protocolos quânticos para realização de contratos.



Conclusões

- Impacto na Informática
 - Eminente – na área de redes e sistemas distribuídos.
 - Eventual – em algoritmia, bases de dados.
- Software bottleneck
 - Existem essencialmente 2 algoritmos quânticos!
- Hardware bottleneck
 - Não é fácil manter um sistema quântico isolado.