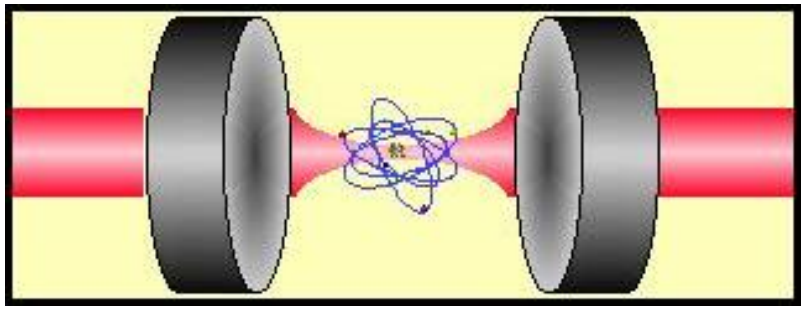
Informação Quântica com Átomos e Fótons

Quebrando Códigos com Computadores Quânticos

Prof. Marcelo Martinelli
Laboratório de Manipulação Coerente de Átomos e Luz



A página:

http://axpfep1.if.usp.br/~mmartine

FAPESP CNPq 50 ANOS CAPES CT BRASIL PADCT

Conteúdo

- 1ª Aula – Princípios de Criptografia.
  Computação "Clássica"
  Computação Quântica.
  Aplicações
  Sistemas experimentais

- 2ª Aula – Princípios de Criptografia Quântica
  Criptografia com um fóton
  Emaranhamento
  Criptografia com feixes intensos

Introdução

•O estado quântico de um sistema representa toda a informação que podemos, *em princípio*, conhecer sobre o sistema.

Mecânica Quântica → *teoria de informação.*

• Vivemos numa "sociedade de informação": a velocidade de progresso do processamento, armazenamento e transmissão de informação é enorme. Há algum limite?

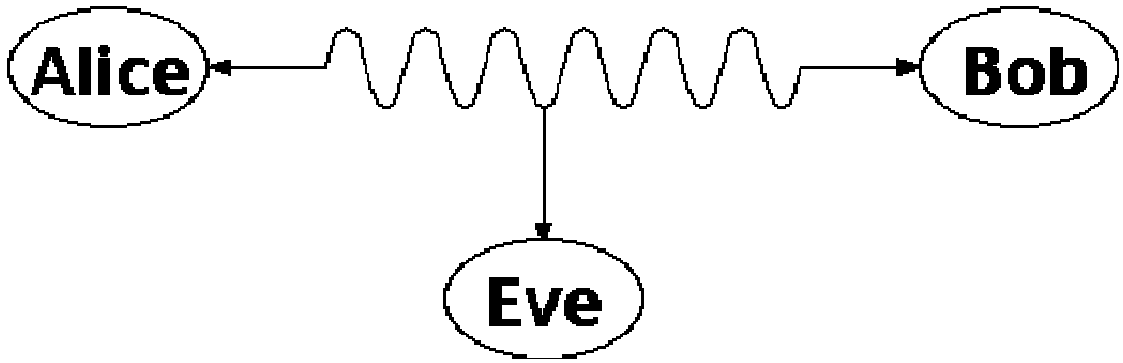
• Toda informação é processada, armazenada e transmitida por algum sistema físico.

miniaturização → sistemas governados pelas leis da MQ.

• As leis da MQ abrem novas possibilidades no processamento e transmissão de informação ⇒ maior eficiência de processamento e maior segurança na transmissão.

Um pouco de criptologia...

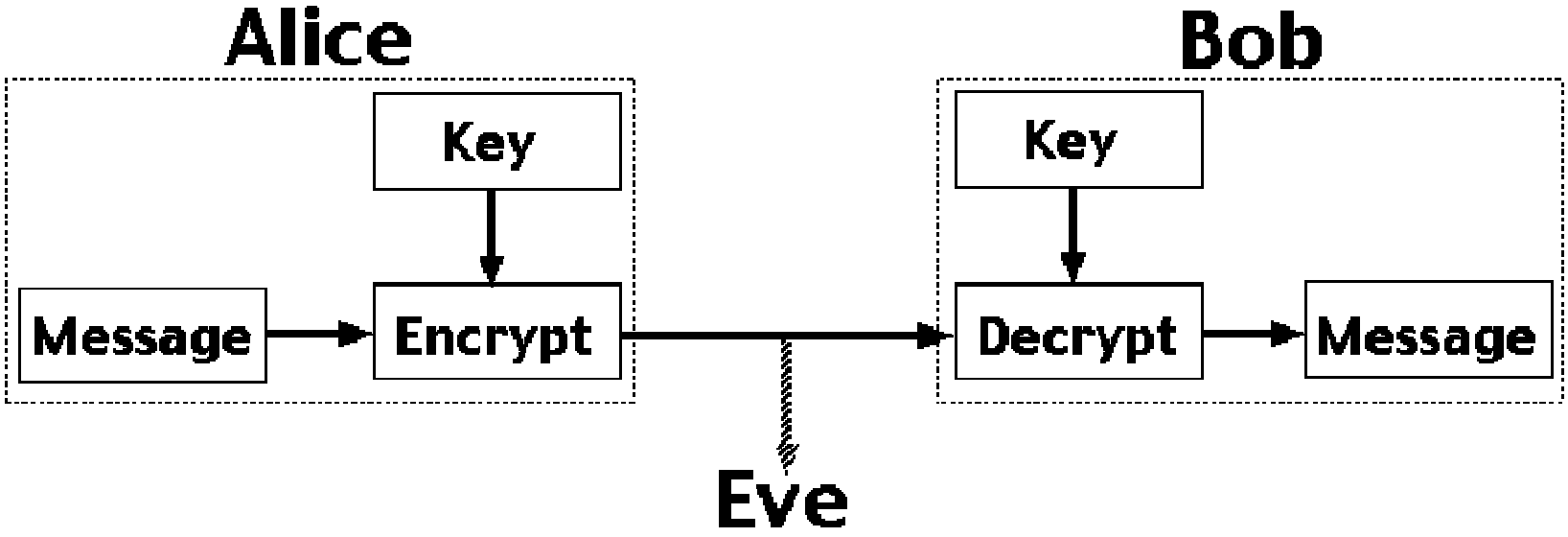
Estações A e B dispõem de um canal de comunicação...



...mas não tem proteção para os dados transmitidos contra um eventual grampo (“eavesdropping”).

Criptografia

Codificação da mensagem enviada



Métodos antigos de criptografia (segredo na codificação)
Descoberta a codificação, a mensagem é aberta.

Criptografia com chave simétrica:
a chave é comum às duas estações

Bloco de cifras de utilização única (1918)

Folha 1	Folha 2	Folha 3
P L M O E	O I W V H	J A B P R
Z Q K J Z	P I Q Z E	M F E C F
L R T E A	T S E B L	L G U X D
V C R C B	C Y R U P	D A G M R
Y N N R B	D U V N M	Z K W Y I

Chave	P L M O E Z Q K J Z L R T E A V C R C B Y
Texto original	a t t a c k t h e v a l l e y a t d a w n
Texto cifrado	P E F O G J J R N U L C E I Y V V U C X L

Fig. 30 Três folhas, cada uma a possível chave para uma cifra de uma única vez. A mensagem é decifrada com o uso da folha 1.

Bloco de cifras de utilização única (1918)

Folha 1	Folha 2	Folha 3
P L M O E	O I W V H	J A B P R
Z Q K J Z	P I Q Z E	M F E C F
L R T E A	T S E B L	L G U X D
V C R C B	C Y R U P	D A G M R
Y N N R B	D U V N M	Z K W Y I

Chave	M A A K T G Q K J N D R T I F D B H K T S
Texto original	d e f e n d t h e h i l l a t s u n s e t
Texto cifrado	P E F O G J J R N U L C E I Y V V U C X L

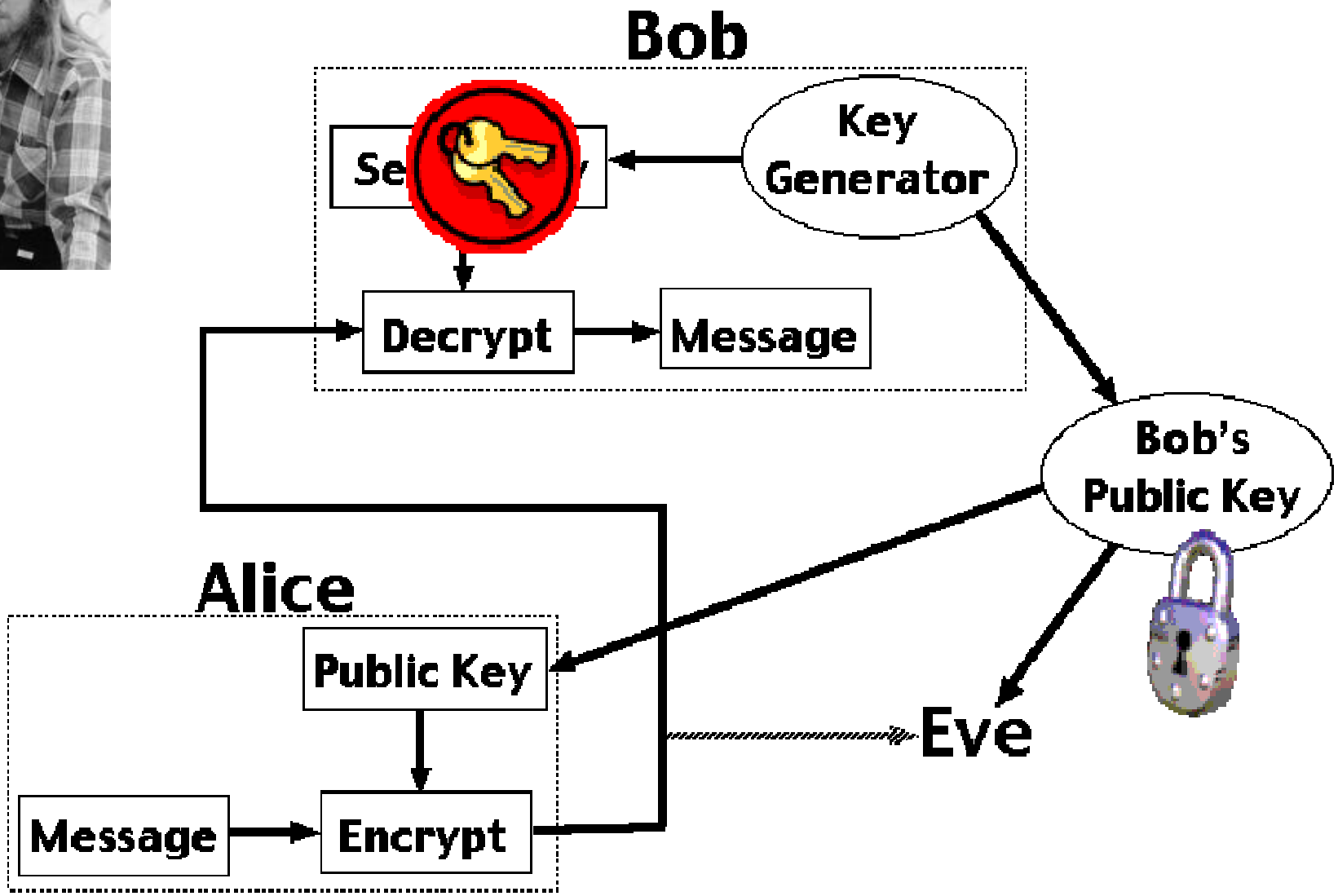
Fig. 30 Três folhas, cada uma a possível chave para uma cifra de uma única vez. A mensagem é decifrada com o uso da folha 1.

Se a chave é aleatória, é usada apenas uma vez e tem o mesmo tamanho da mensagem, oferece segurança absoluta. MAS, como distribuir as chaves? Como gerar chaves aleatórias?

Criptografia com chave assimétrica: encripta com chave pública, decodifica com chave secreta

Diffie, Hellman, Merkle (1976) James Ellis (1969)

Conceito de chave assimétrica ⇒ Distribuição pública



Algoritmo RSA (1977)

Adi Shamir, Ron Rivest and Leonard Adleman

Rivest, Shamir, Adleman (RSA)

Ellis, Cocks, Williamson (1975)

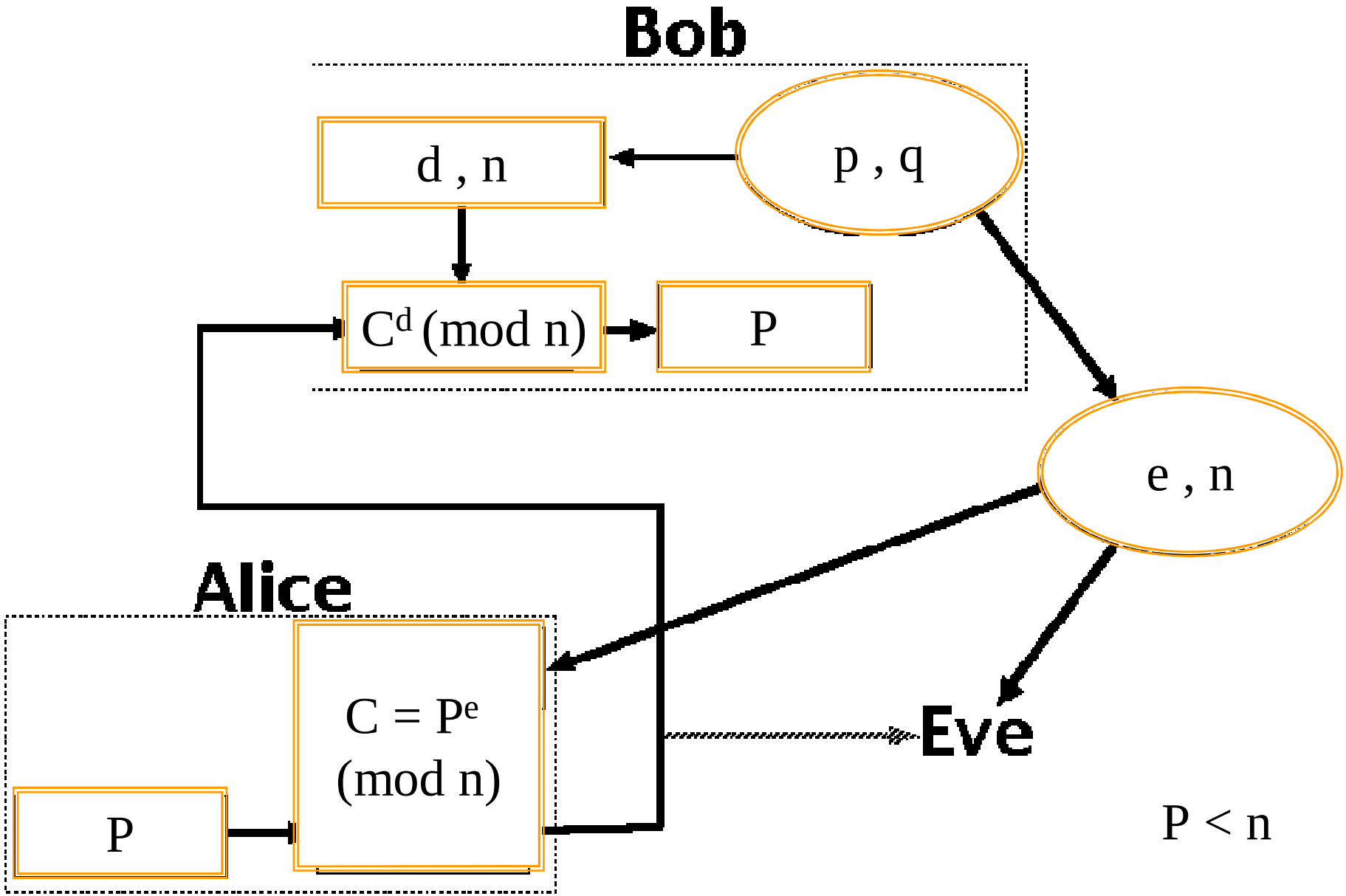
Chave baseada na dificuldade de se decompor números inteiros em seus fatores primos: problema de grande complexidade computacional

- *Escolha* p , q *(primos)*
- *Calcule* n = p q
- *Calcule* m = (p-1) (q-1)
- *Escolha um número* e *(co-primo com* m*)*
- ***Dado* p, q**, *calcule* d, *tal que*

  d e = 1 (mod m)

x = y (mod m) → x + am = y + bm

- *Chave pública:* e, n
- *Chave secreta:* d, n



Número de operações para Eve calcular d: O(exp(n))

Segurança do Algoritmo RSA:

Fatoração de n para obter **p**, **q**, e calcular **d**.

Chaves de 1024 a 2048 bits.

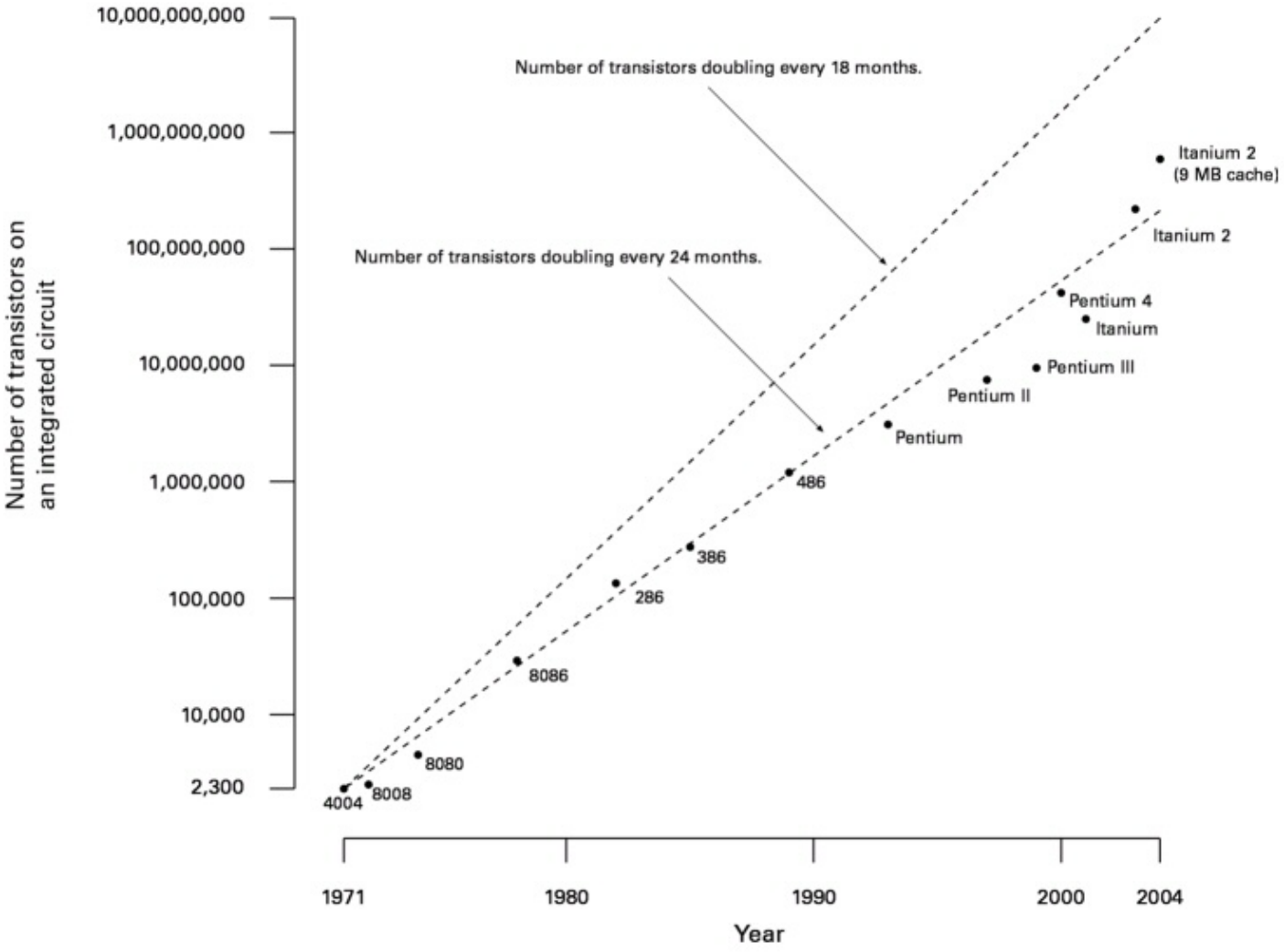
Fatoração de chave.

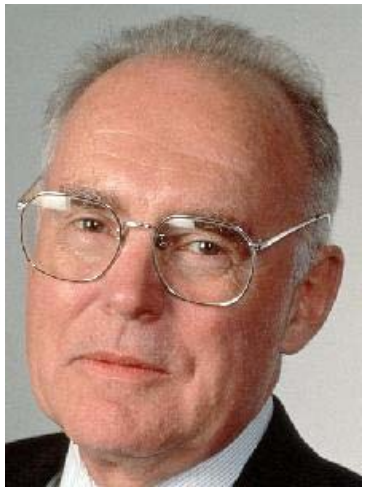
- 256 bits: PC
- 512 bits: conjunto de máquinas em alguns meses
- 1024 bits: seguras até 2010
- 2048 bits: seguras até 2030

Unidirecional: útil como canal seguro para partilhar um “one-time pad”

Problema: geração aleatória de chave simétrica

Moore's Law


Number of transistors on an integrated circuit
10,000,000,000
1,000,000,000
100,000,000
10,000,000
1,000,000
100,000
10,000
2,300
Number of transistors doubling every 18 months.
Number of transistors doubling every 24 months.
Itanium 2 (9 MB cache)
Itanium 2
Pentium 4
Itanium
Pentium III
Pentium II
Pentium
486
386
286
8086
8080
8008
4004
1971
1980
1990
2000
2004
Year



Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

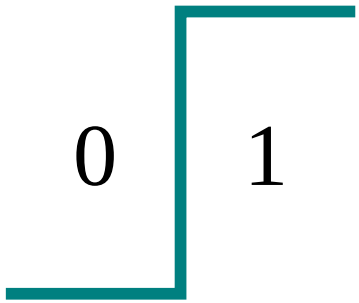
0272-5428/94 $04.00 © 1994 IEEE

Peter Shor (1994): algoritmo quântico eficiente para decomposição em fatores primos

Computador clássico:

BIT

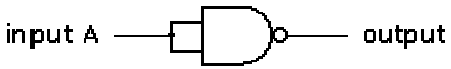
Dois estados possíveis



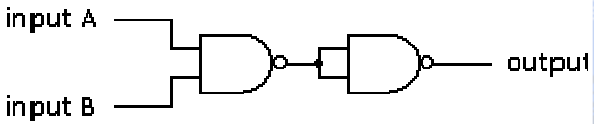
Portas lógicas

Name	Graphic Symbol	Algebraic Function	Truth Table
AND		$F = A \cdot B$ or $F = AB$	A B | F 0 0 | 0 0 1 | 0 1 0 | 0 1 1 | 1
OR		$F = A + B$	A B | F 0 0 | 0 0 1 | 1 1 0 | 1 1 1 | 1
NOT		$F = \overline{A}$ or $F = A'$	A | F 0 | 1 1 | 0
NAND		$F = (\overline{AB})$	A B | F 0 0 | 1 0 1 | 1 1 0 | 1 1 1 | 0
NOR		$F = (\overline{A + B})$	A B | F 0 0 | 1 0 1 | 0 1 0 | 0 1 1 | 0

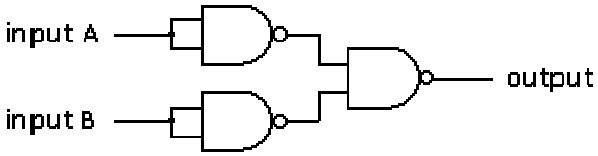
NOT gate (inputs joined together)



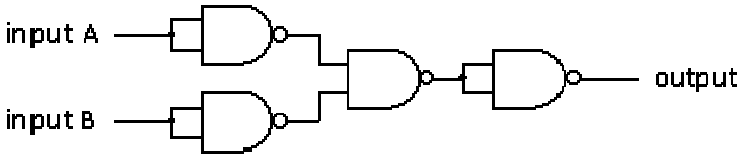
AND gate (NAND followed by NOT)



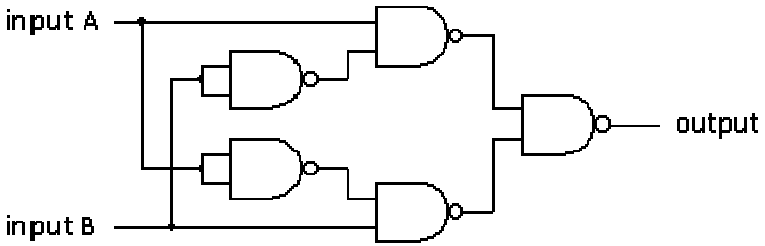
OR gate (NOT of each input followed by NAND)



NOR gate (OR followed by NOT)

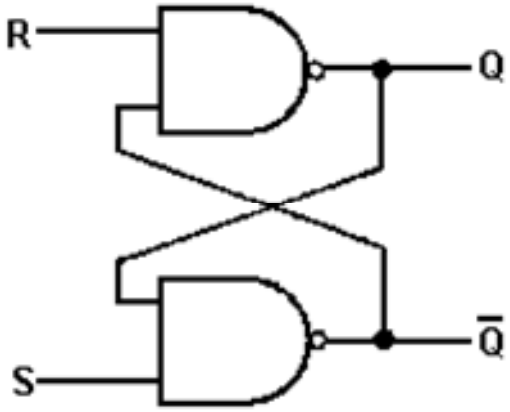


EXOR gate



Registradores (memórias)

Estáticas



R	S	Q	$\overline{Q}$
0	0	1*	1*
0	1	1	0
1	1	1	0
1	0	0	1
1	1	0	1

The R=0, S=0 state must be avoided, since it causes Q = - Q

The R-S flip.flop

Dinâmicas

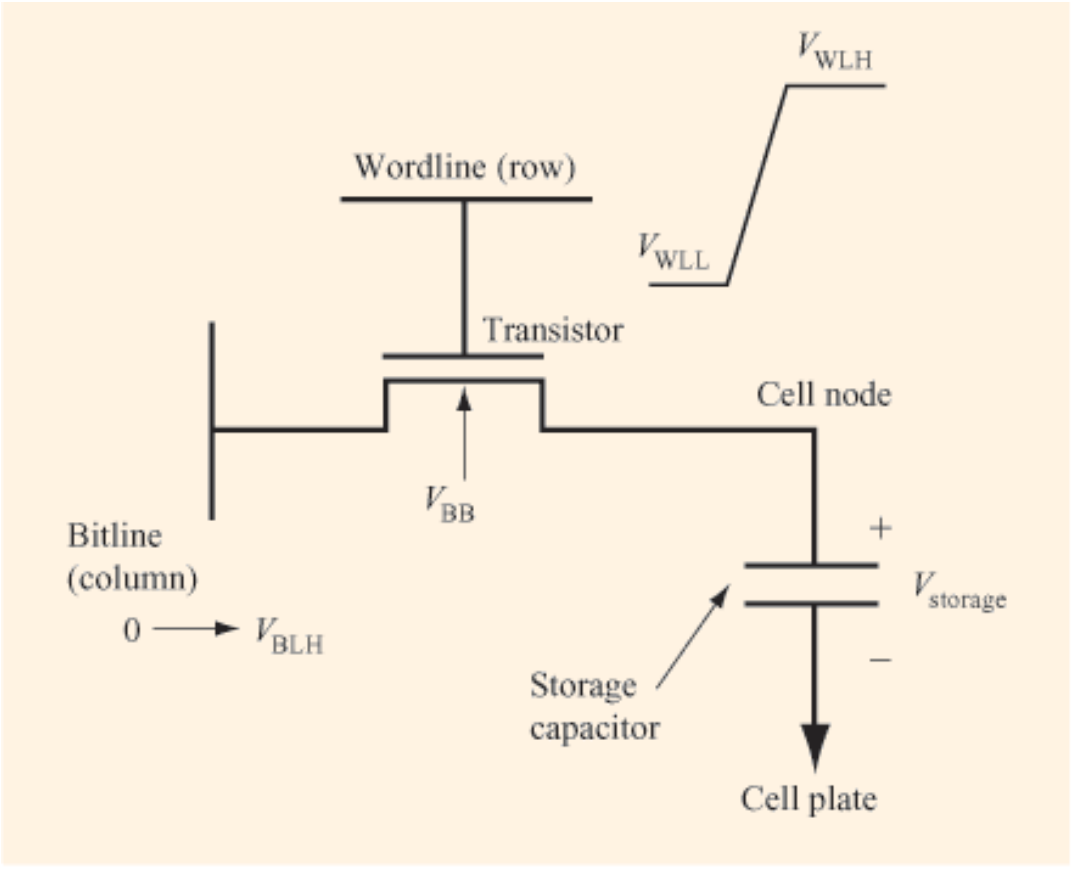
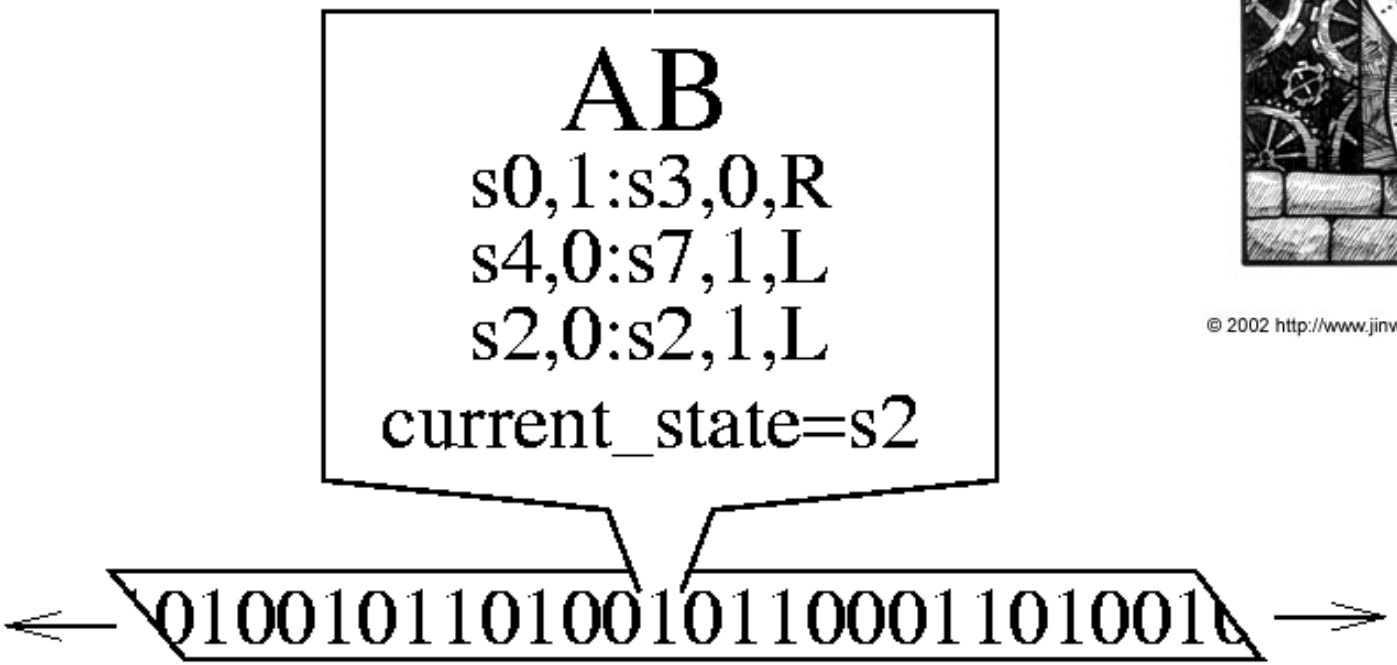


Figure 1

Schematic of a one-transistor DRAM cell [1]. The array device (transistor) is addressed by switching the wordline voltage from V_{WLL} (wordline-low) to V_{WLH} (wordline-high), enabling the bitline and the capacitor to exchange charge. In this example, a data state of either a "0" (0 V) or a "1" (V_{BLH}) is written from the bitline to the storage capacitor. V_{BB} is the electrical bias applied to the p-well.

Máquina de Turing

Modelo geral de computador



Limites da computação

- Capacidade de processamento limitada à densidade de transistores no chip (limite da lei de Moore em 2050)

- Espaço de problemas solúveis:
  crescimento polinomial do número de passos com número de bits.

- Problemas insolúveis
  crescimento exponencial do número de passos com número de bits.

  - Fatoração
  - Transformada de Fourier
  - Busca em uma lista

- Simulação quântica — Feynman

Quebrando o limite clássico

Os computadores obedecem as leis da Física...

...e portanto à Mecânica Quântica (David Deustch – 1985).

O que acontece quando o transistor fica “muito pequeno”?

Podemos usar a “estranheza”da Mecânica Quântica
a nosso favor?

Computação Quântica

Qubit

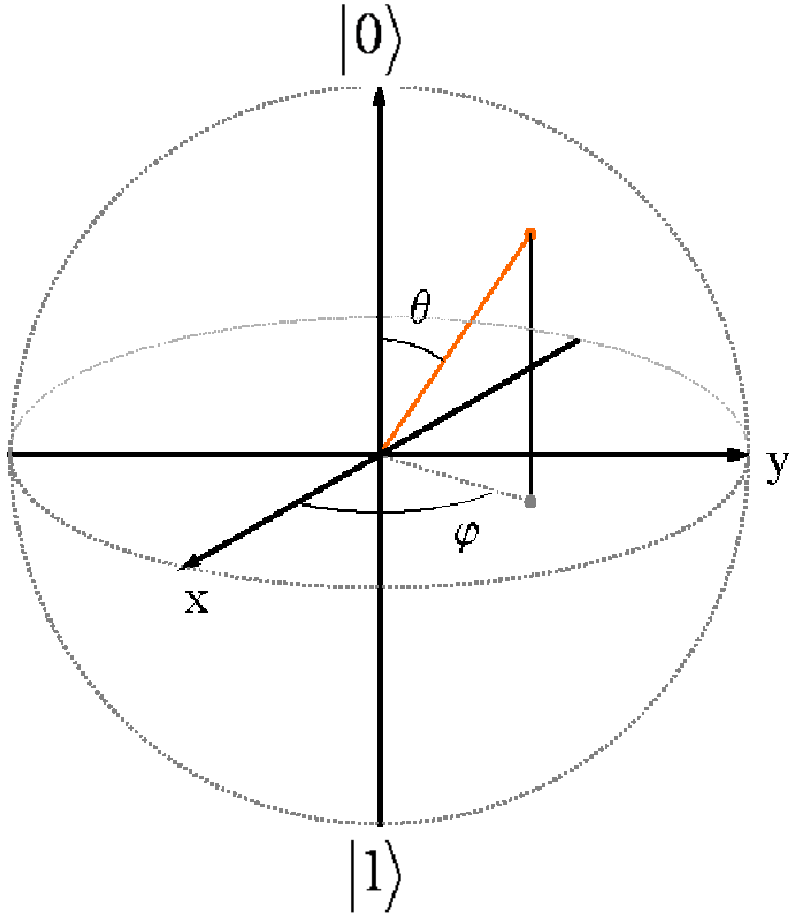
$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi} sen\frac{\theta}{2}|1\rangle$$

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

Representação Matricial

$$|\Psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

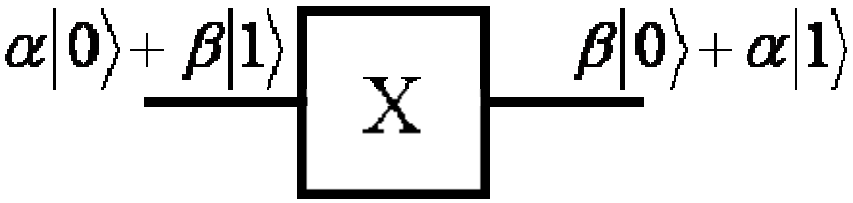


Mas o que é um qubit afinal?

Sistema quântico com
dois autoestados

Spin eletrônico
Polarização do fóton

Portas lógicas

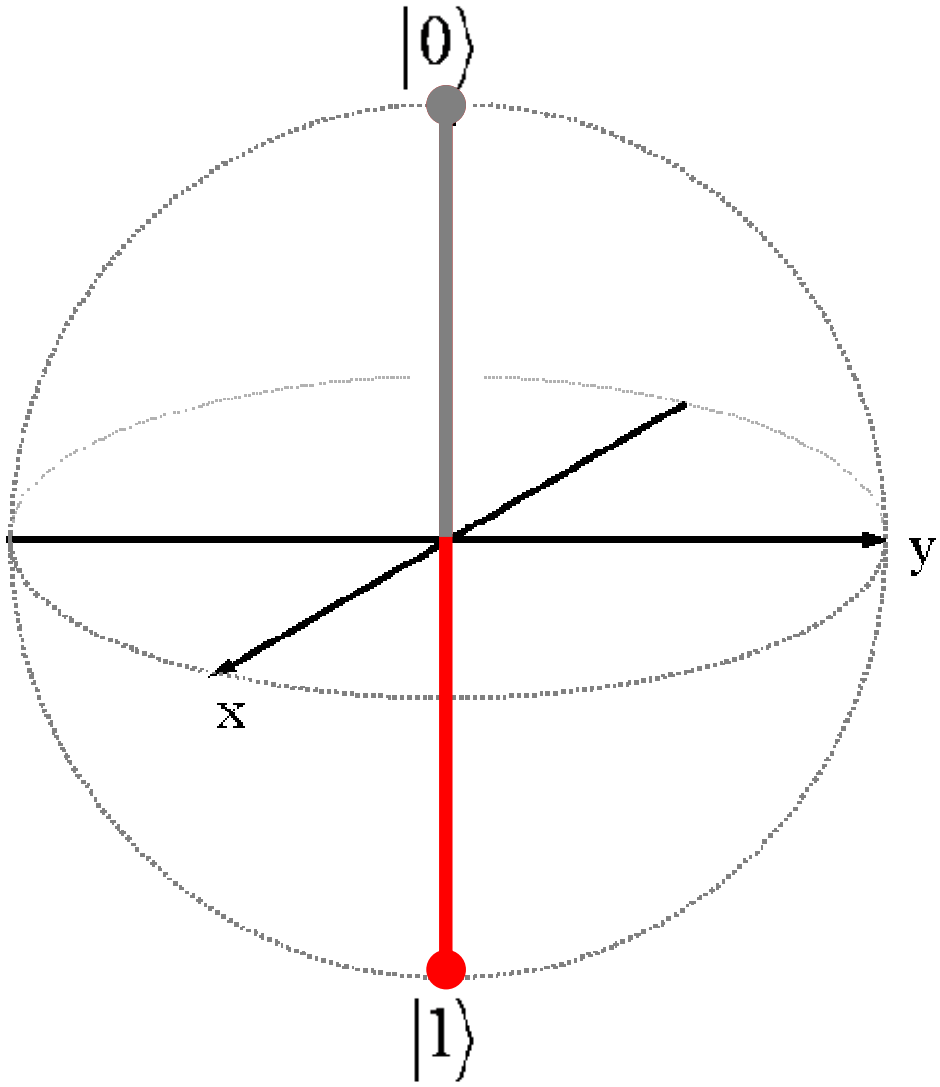


- Reversíveis
- Transformação unitária

$$|\Phi\rangle = U|\Psi\rangle$$

$$U^{+}U = I$$

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$



Portas lógicas

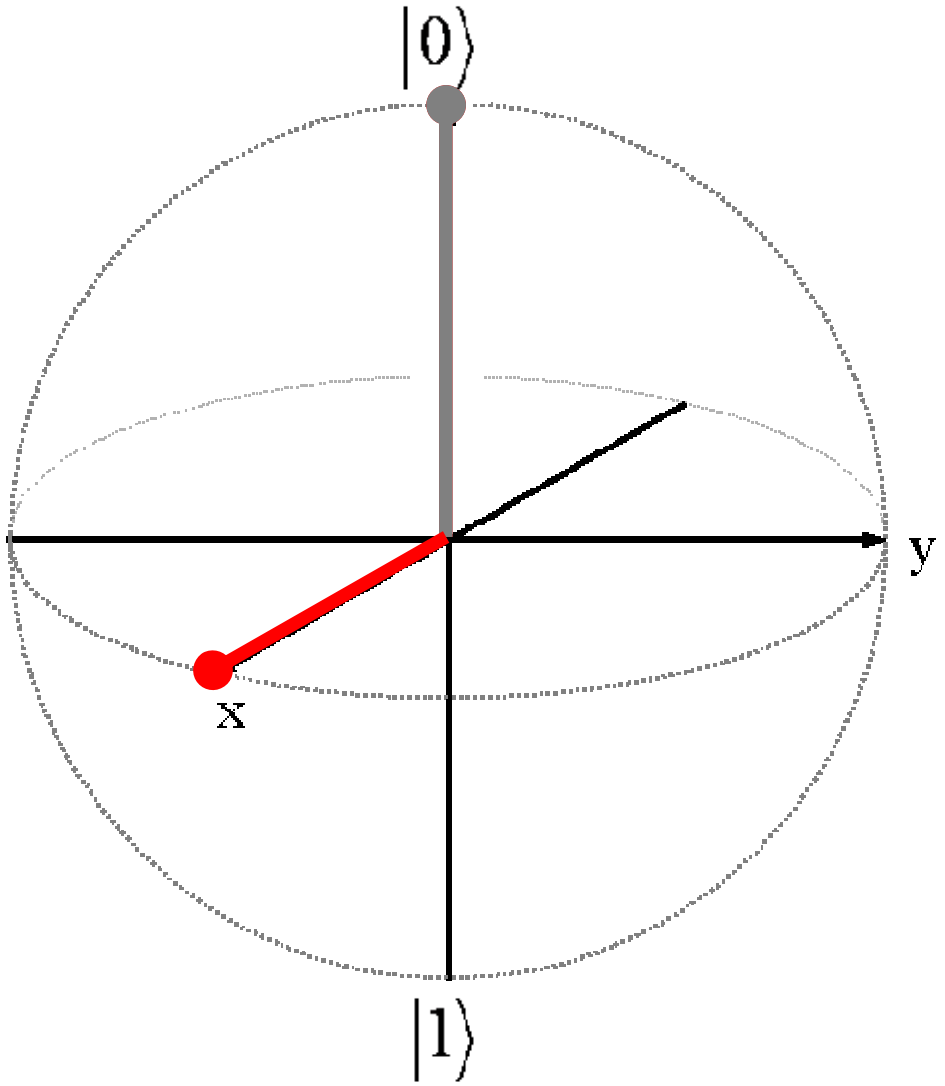
- Reversíveis
- Transformação unitária

$$\alpha|0\rangle + \beta|1\rangle \quad \boxed{\text{H}} \quad \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

$$|\Phi\rangle = U|\Psi\rangle$$

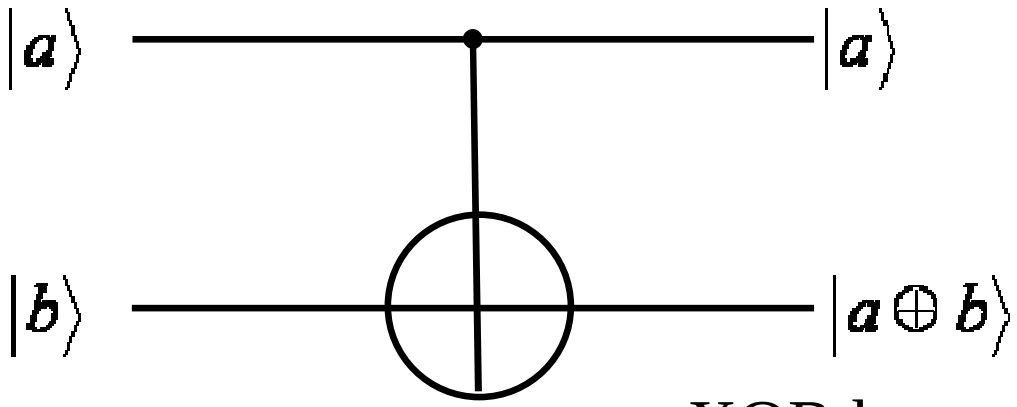
$$U^{+}U = I$$

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$



Portas lógicas

Controlled-Not



$$|\Psi_i\rangle = |a,b\rangle$$

$$|\Psi_o\rangle = |a, a \oplus b\rangle$$

a XOR b
adição modulo 2

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$|a\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}; |b\rangle = |0\rangle \Rightarrow$$

$$|\Psi_i\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

$$\Rightarrow |\Psi_o\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

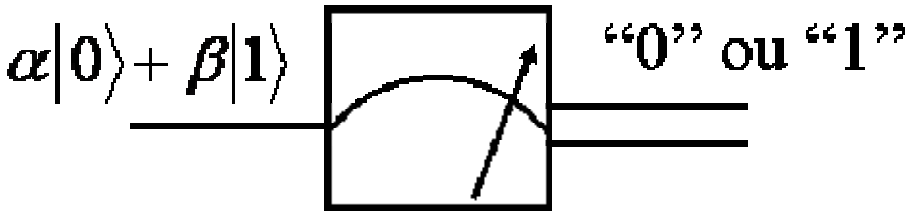
Podemos criar estados inseparáveis no resultado (superposição →emaranhamento)

Medidas

A medida projeta o estado em uma base.

Exemplo: Polarizador

A saída pode ser o resultado final, ou uma etapa intermediária no cálculo

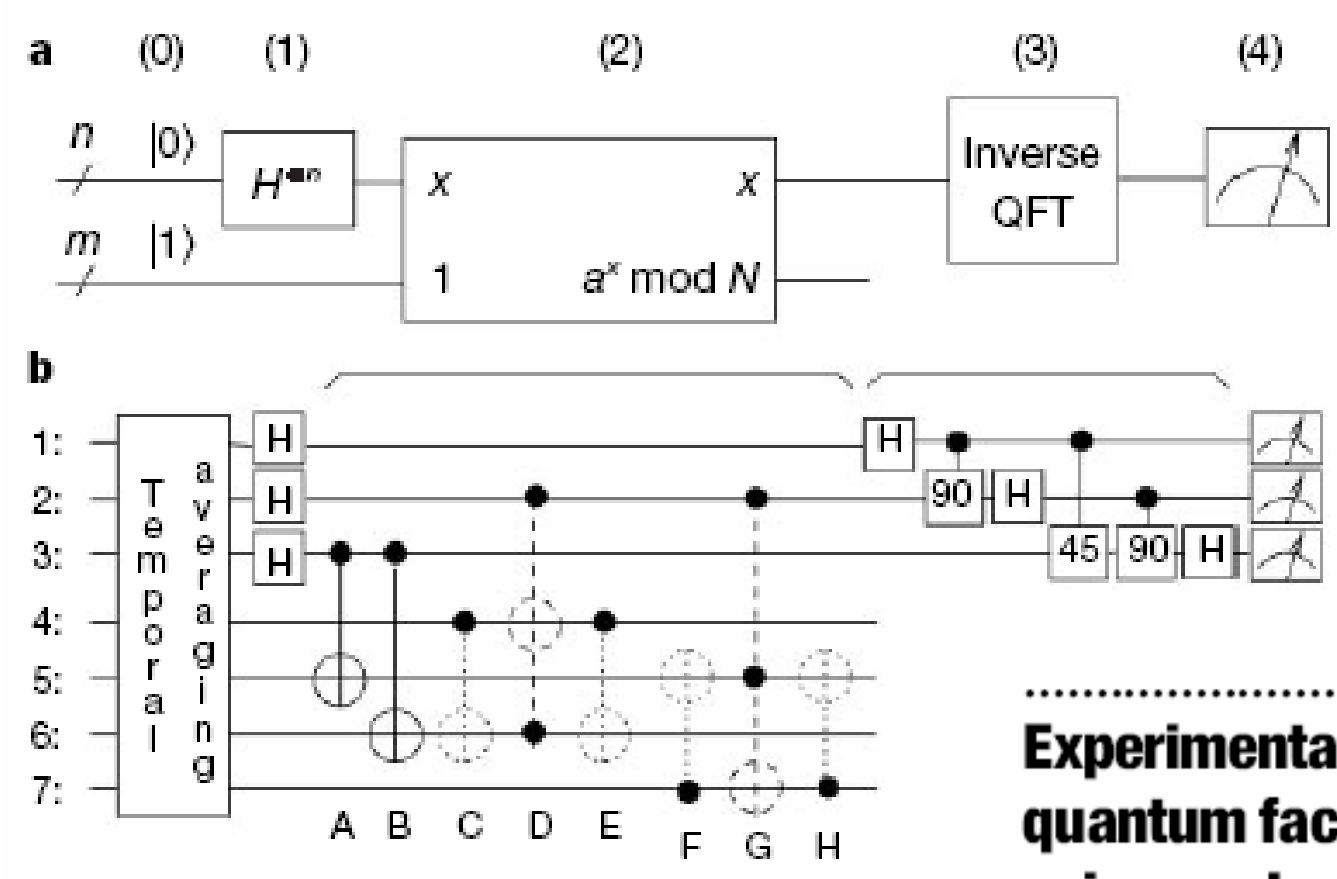


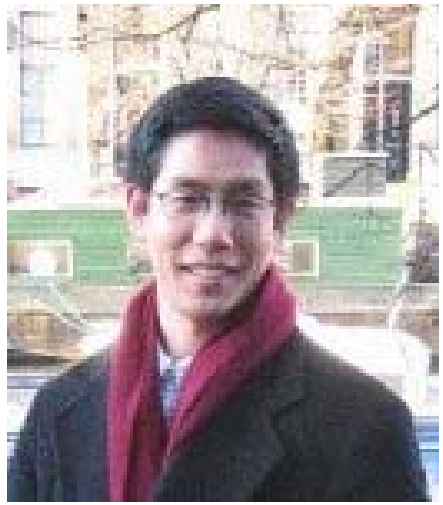
Resultado de uma medida é NECESSARIAMENTE um AUTOVALOR do observável (operador) sendo medido.

Medida é equivalente a PREPARAR um estado:

após a medida de um autovalor, o estado do sistema é o autovetor (auto-estado) correspondente.

Montando a máquina...





Fatorar N=15...

Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance

Lieven M. K. Vandersypen*†, Matthias Steffen*†, Gregory Breyta*, Costantino S. Yannoni*, Mark H. Sherwood* & Isaac L. Chuang*†

** IBM Almaden Research Center, San Jose, California 95120, USA*
† Solid State and Photonics Laboratory, Stanford University, Stanford, California 94305-4075, USA

NATURE | VOL 414 | 20/27 DECEMBER 2001 | www.nature.com

Condições de Implementação

Inicializar o qubit

Implementar portas lógicas

→para um qubit (criar superposições)

→para múltiplos qubits (interação entre qubits)

Ler o estado (medida)

Armazenar o qubit

Escalabilidade

Problema fundamental

Tempo de vida da superposição de estados (descoerência)

O problema da descoerência

PROCURADO

Para terem utilidade, computadores quânticos devem operar sobre *vários* qubits, gerando estados emaranhados de muitas partículas (máximo de partículas emaranhadas em laboratório). Por que é difícil produzir e manter esses estados? A interação com o ambiente gera ***descoerência*** : tudo se passa como se o ambiente estivesse fazendo medidas sobre o sistema de interesse, levando à perda de indistinguibilidade e, portanto, de coerência.

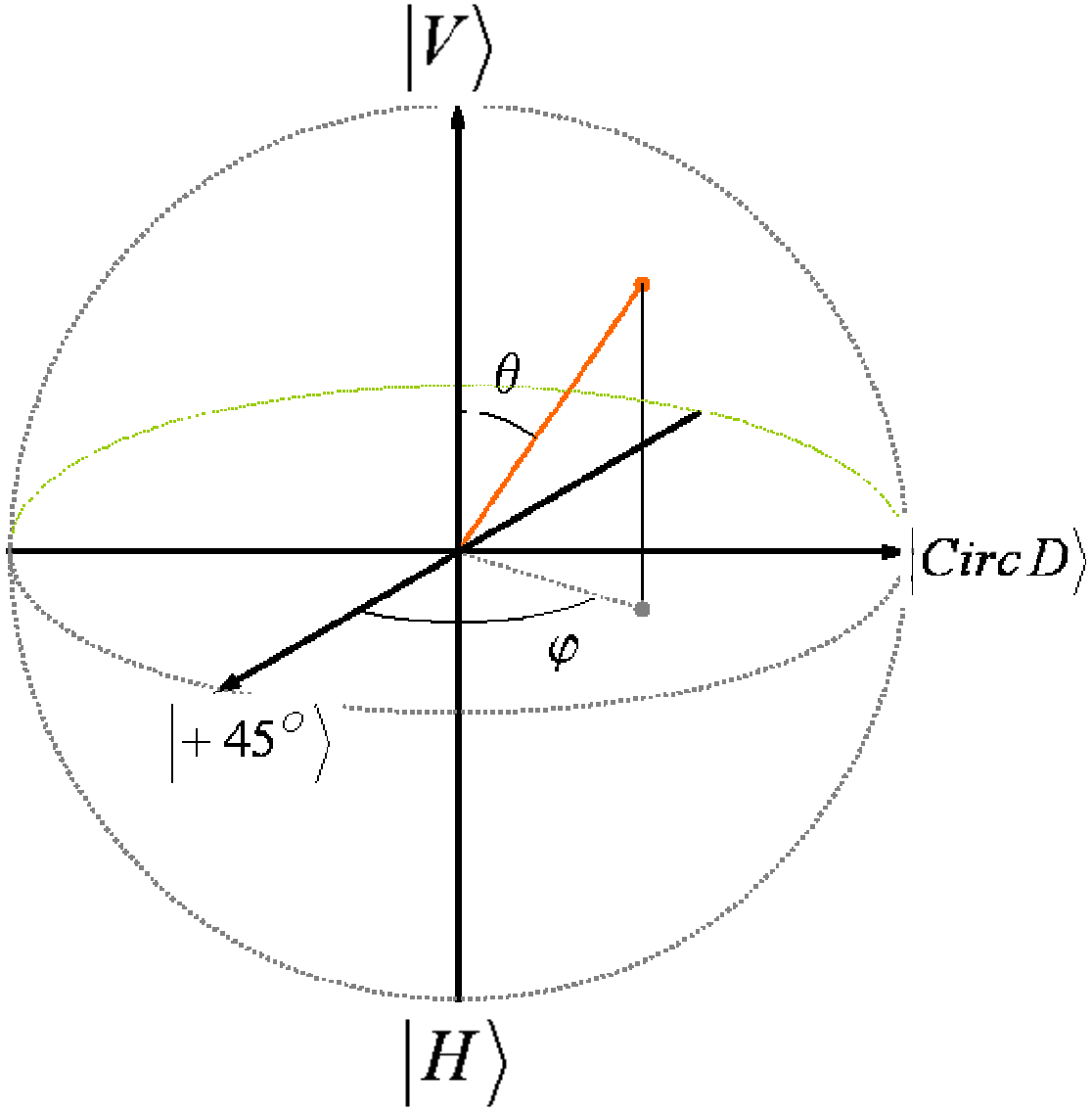
Vivo E Morto

Podemos estudar os fundamentos da Informação Quântica em diferentes sistemas....

Polarização do fóton

Esfera de estados

→ Esfera de Poincaré



Inicializar o qubit →Polarizador

Armazenar o qubit

Implementar portas lógicas

→para um qubit (criar superposições) →Lâminas de onda

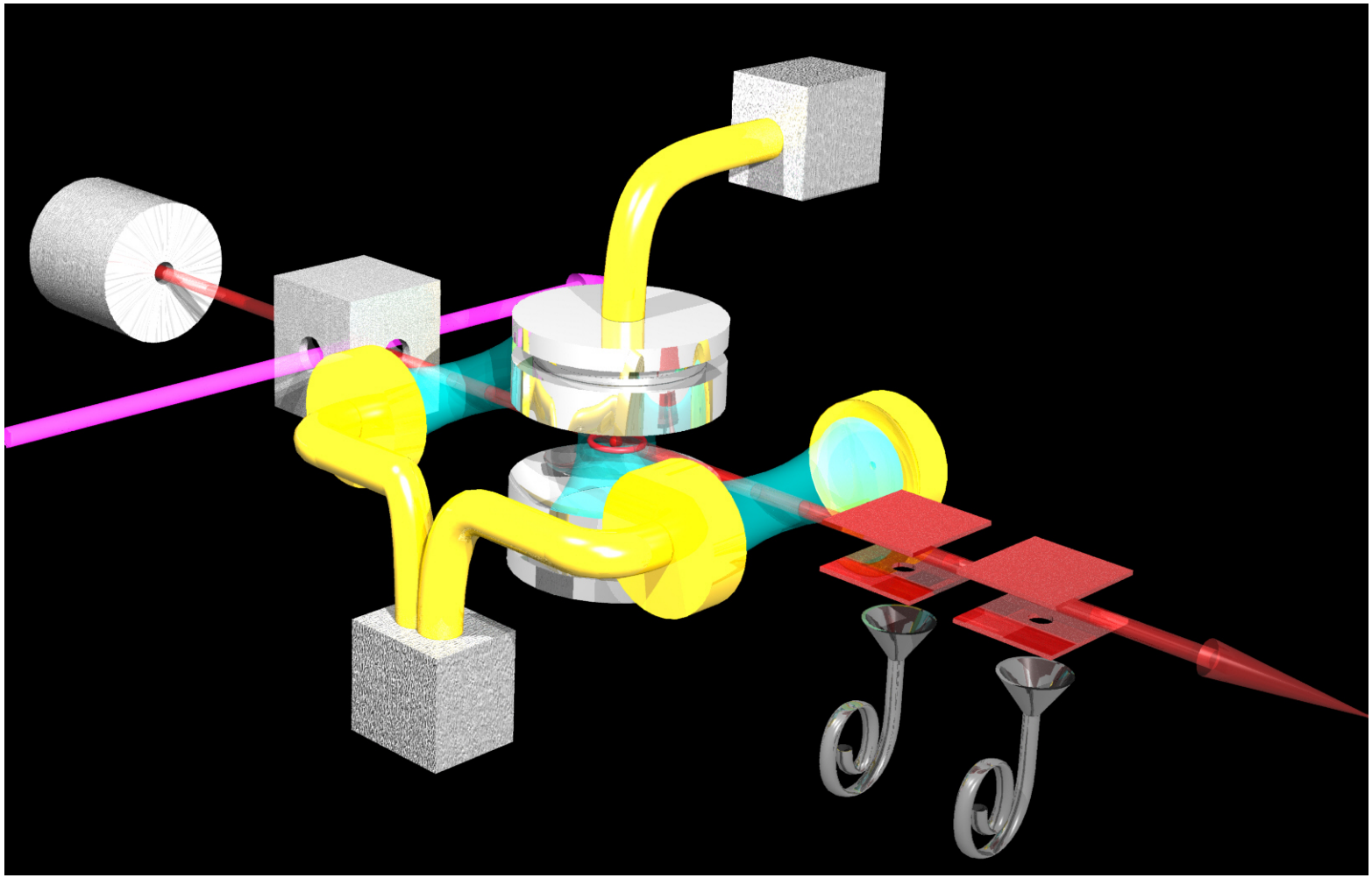
→para múltiplos qubits (interação entre qubits→emaranhamento)

Ler o estado (medida) →Detetores

Descoerência

Estados atômicos e fótons em cavidades

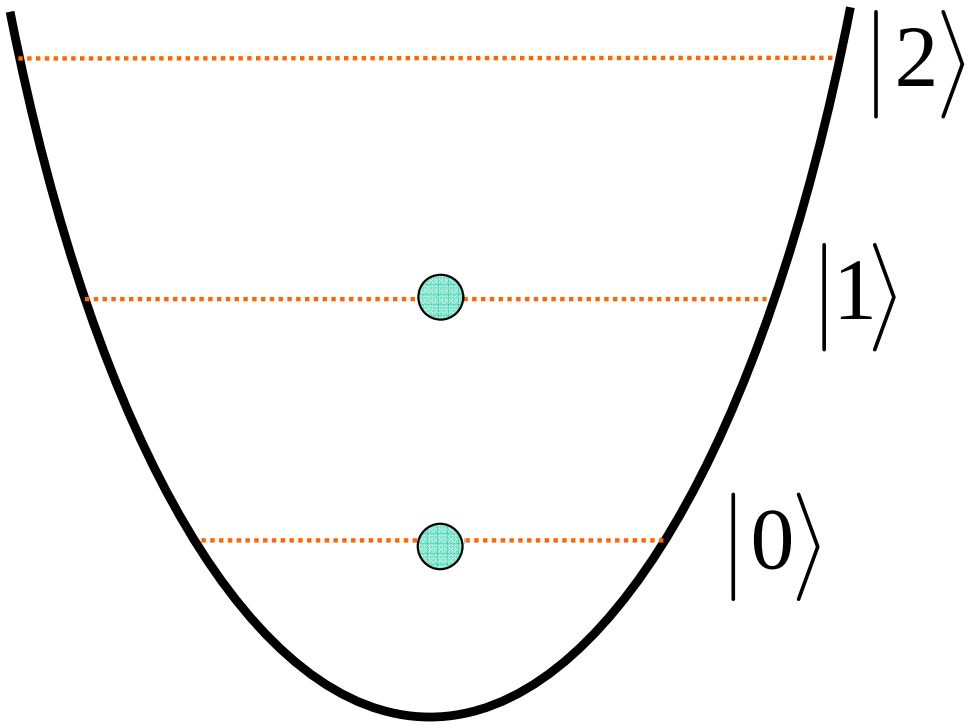
Exemplo:



Átomos e íons em potenciais quadráticos

Oscilador harmônico

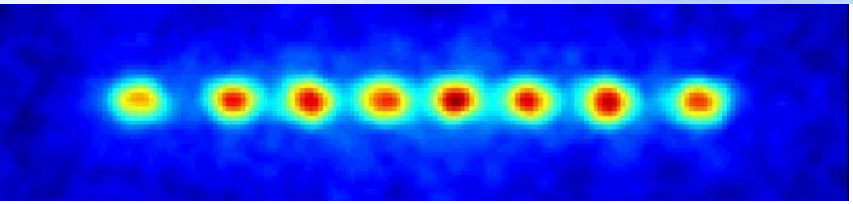
$$|\Psi\rangle = a|0\rangle + e^{i\omega t} b|1\rangle$$

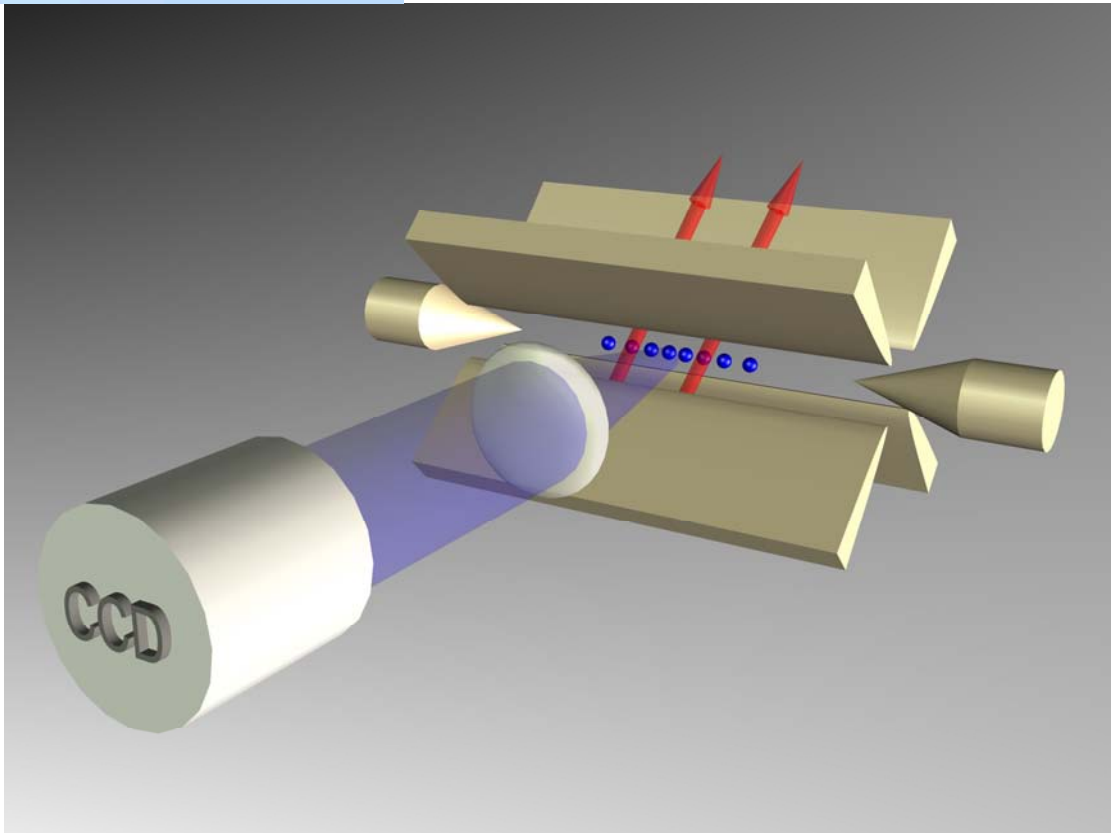


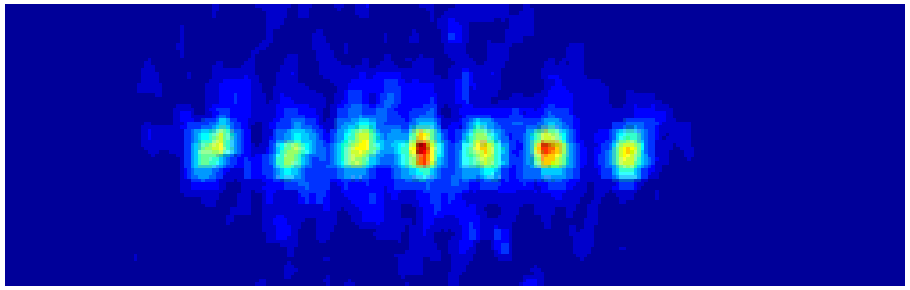
Quantum Optics and Spectroscopy

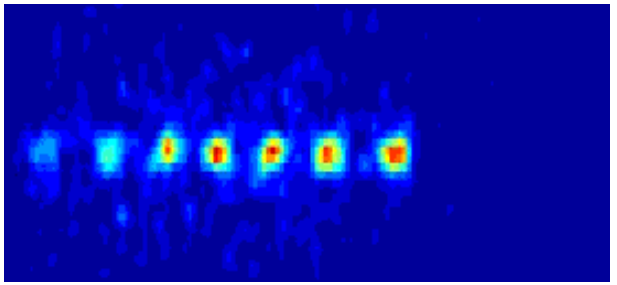
Institut für Experimentalphysik - Universität Innsbruck

Rainer Blatt

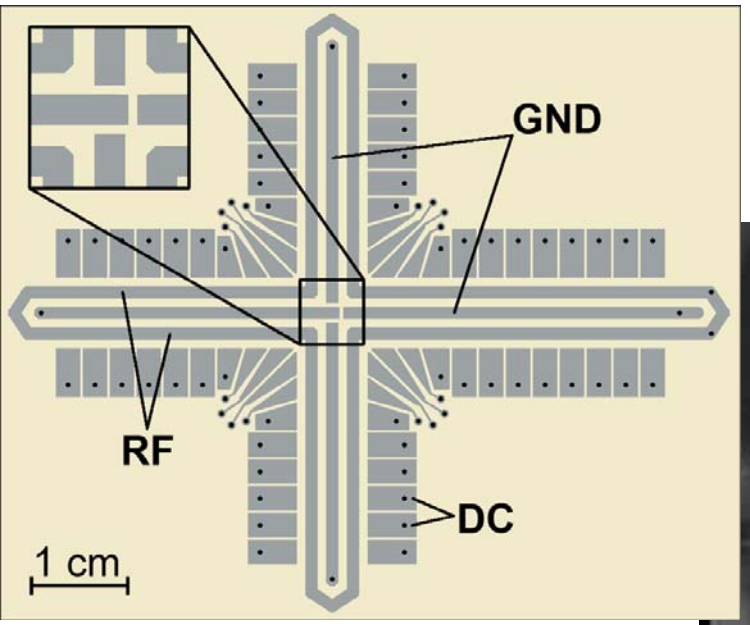








Quanta Group – MIT (Issac Chuang)



Informação Quântica com Átomos e Redes Óticas

- Montagem de redes óticas com átomos frios
- Controle coerente de populações dos estados vibracionais
- Medida dos estados vibracionais
- Interação átomos – redes
- Correlações entre átomos (est. vibracionais) e luz (est. do campo)
- Manipulação da descoerência

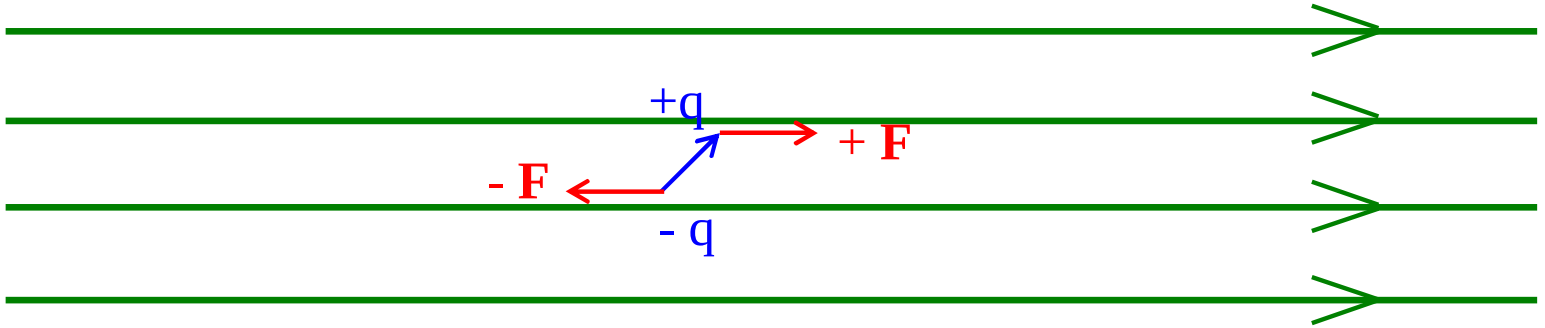
Redes Óticas

- Aprisionamento de átomos neutros no potencial gerado por Efeito Stark AC
- Criação de estruturas periódicas - Controle da localização dos átomos.
- Verificação de efeitos previstos em matéria condensada com átomos e luz.
- Aplicação em Condensados de Bose-Einstein
- Mas muito trabalho em átomos frios (não degenerados)...

Interação Átomo - Campo

- Átomo funciona como uma ANTENA emissora/receptora, do tipo dipolo

DIPOLO EM CAMPO ELÉTRICO **E**



- **p** = q ℓ $\Rightarrow$ BINÁRIO $\rightarrow$ TORQUE $\tau = \ell \times \mathbf{F} = \mathbf{p} \times \mathbf{E}$

- **ENERGIA DE INTERAÇÃO**

$$\mathbf{H_I = - p \,.\, E = - d \,.\, E}$$

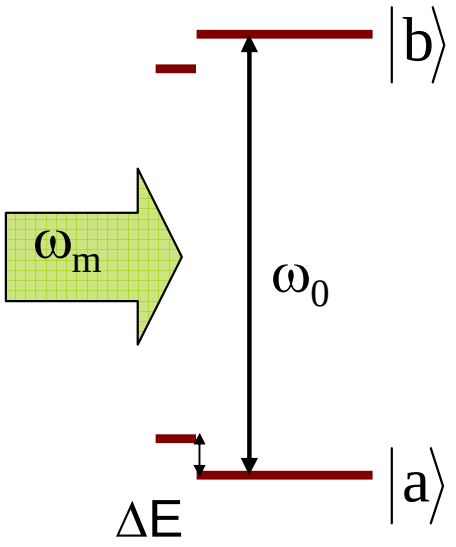
NOTAÇÃO : DIPOLO d

Efeito Stark AC

Átomo + feixe = deslocamento dos níveis de energia

$$\Delta E \propto \frac{1}{\Delta}$$

$$\Delta = \omega_m - \omega_0$$



Potencial visto pelo átomo

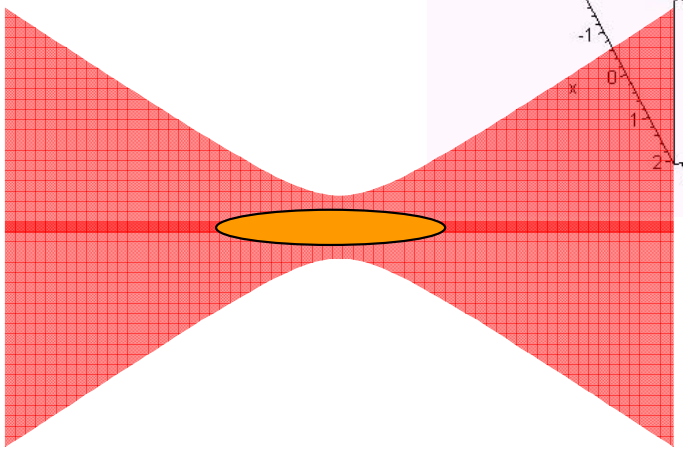
Taxa de espalhamento $\Gamma_{scat} \propto \frac{1}{\Delta^2}$

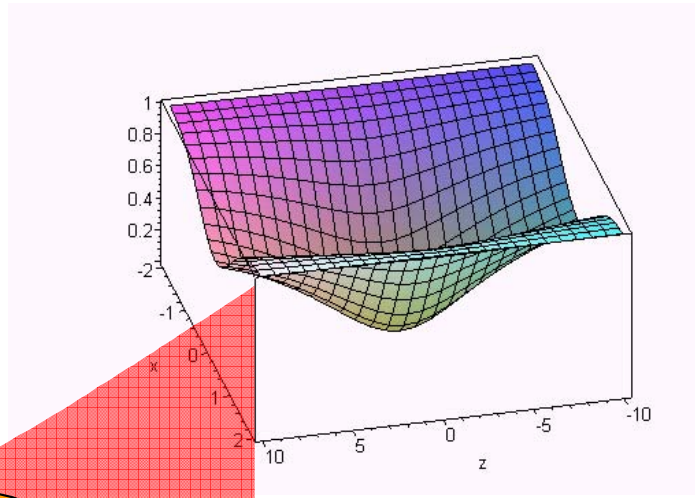
Aprisionar átomos com luz

Um único feixe: pinça ótica

Dessintonia para o vermelho

Mínimo potencial na cintura do feixe



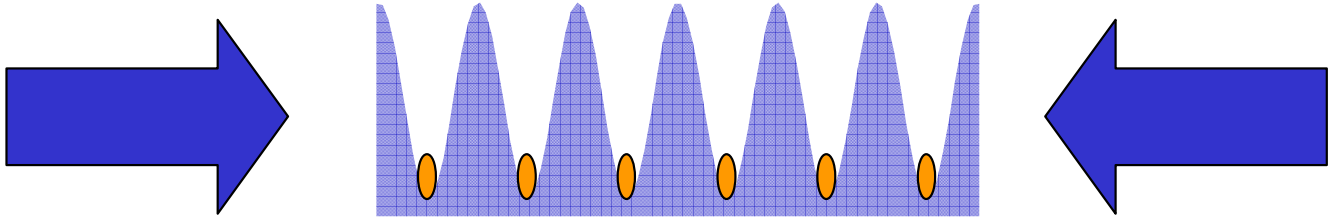


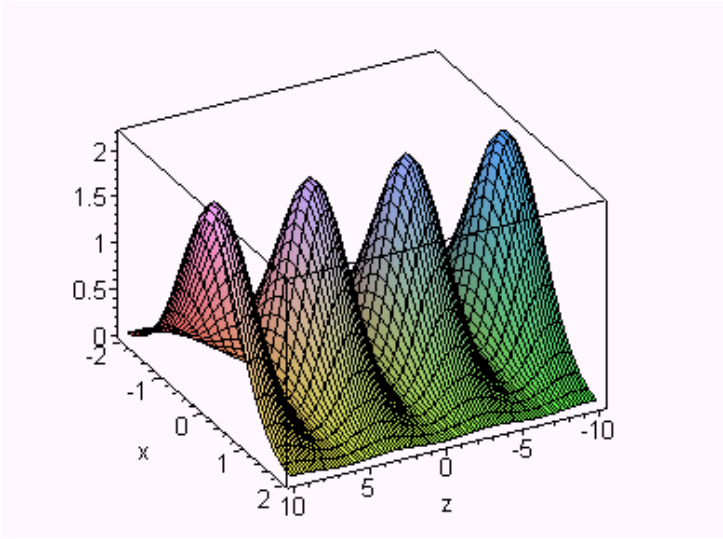
Exemplo: FORT

Dois (ou mais) feixes: Redes óticas

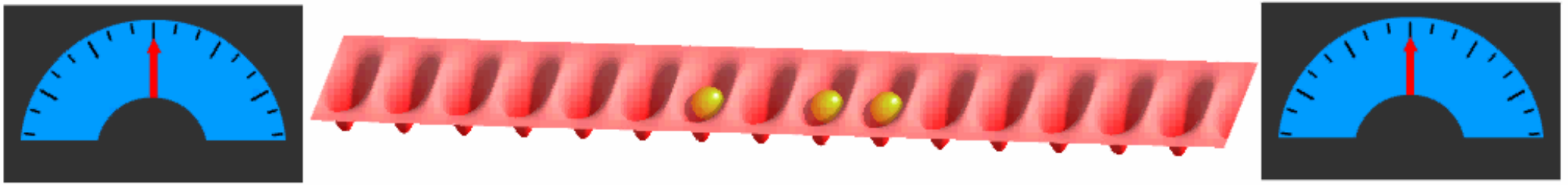
Rede horizontal

Estruturas periódicas formadas por uma onda estacionária

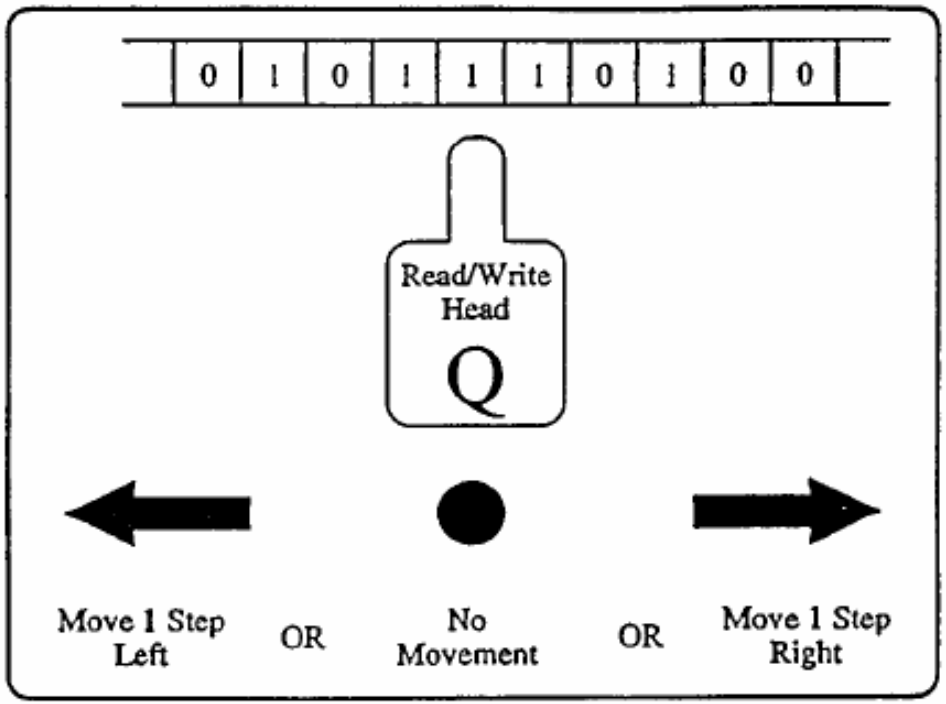




Δ>0: aprisionamento no campo mínimo
Problema: confinamento unidimensional



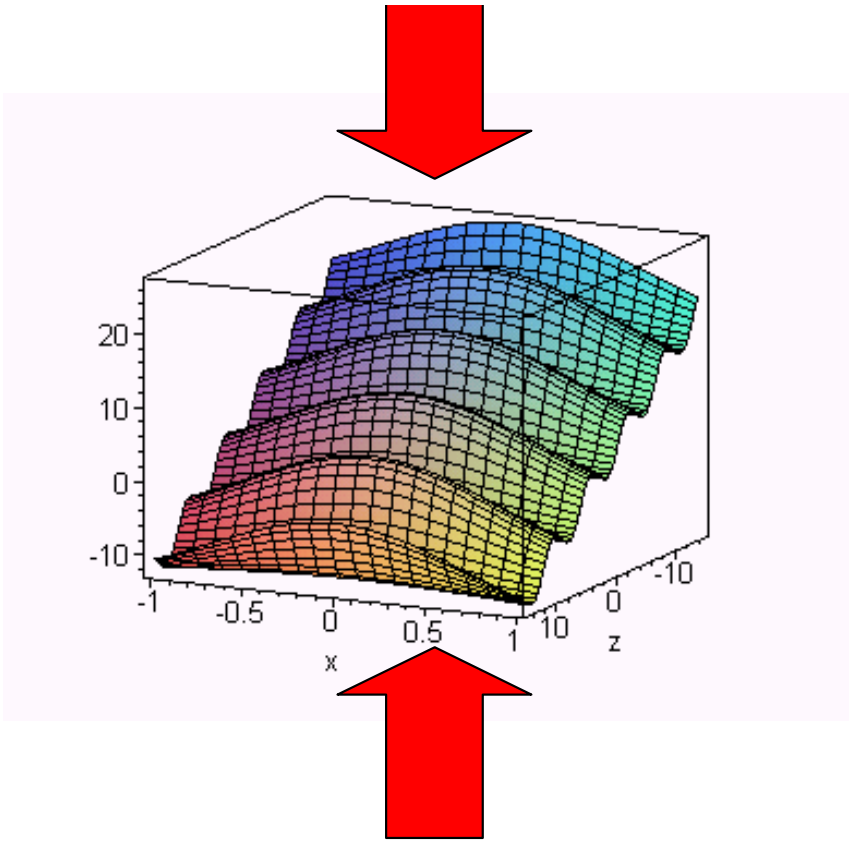
by Dieter Meschede, Univ. Bonn



Rede vertical

Efeito da gravidade

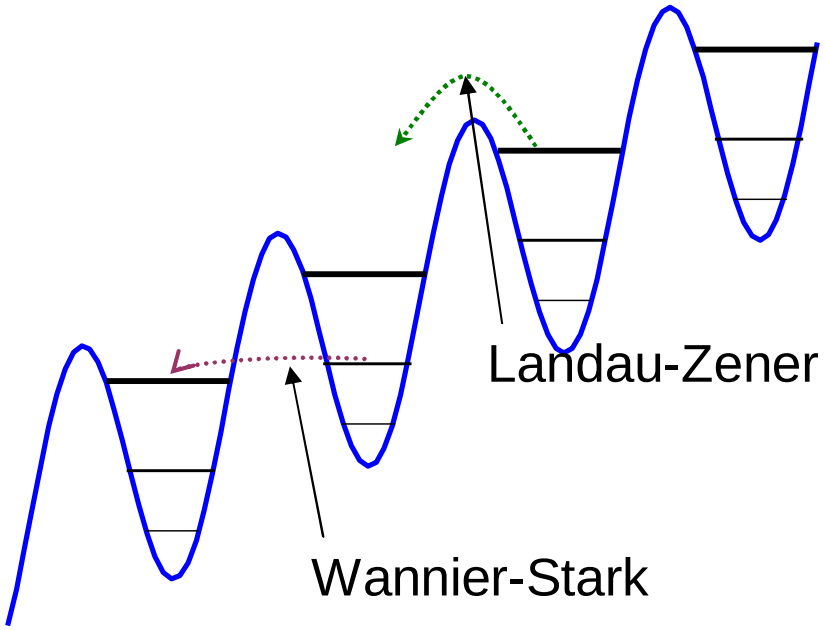
“Washboard potential”



Tempo de vida do estado:

Limitado por tunelamento tipo

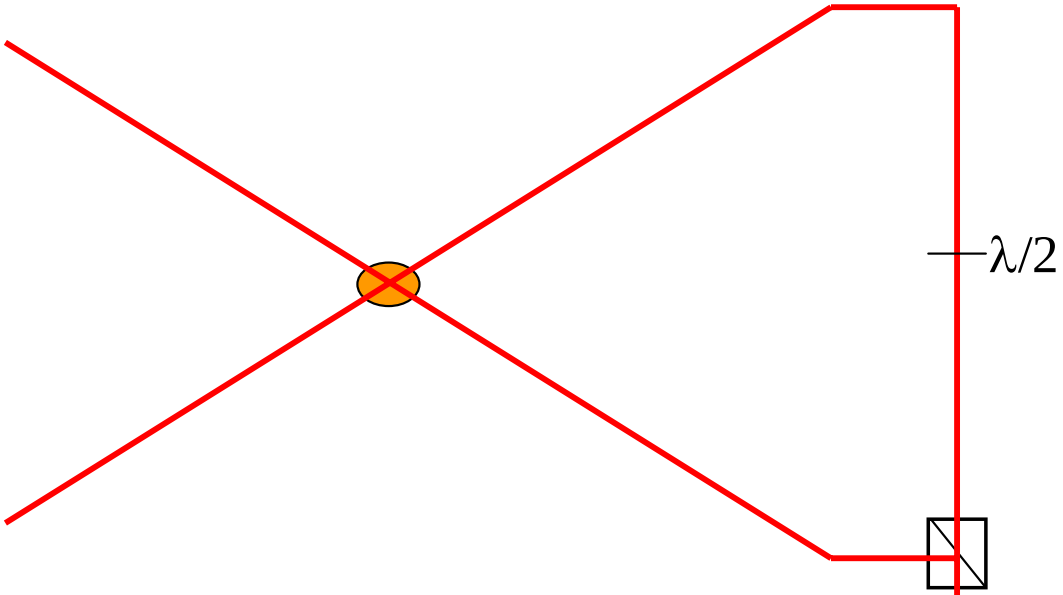
Landau-Zener ou Wannier-Stark



Montagem:

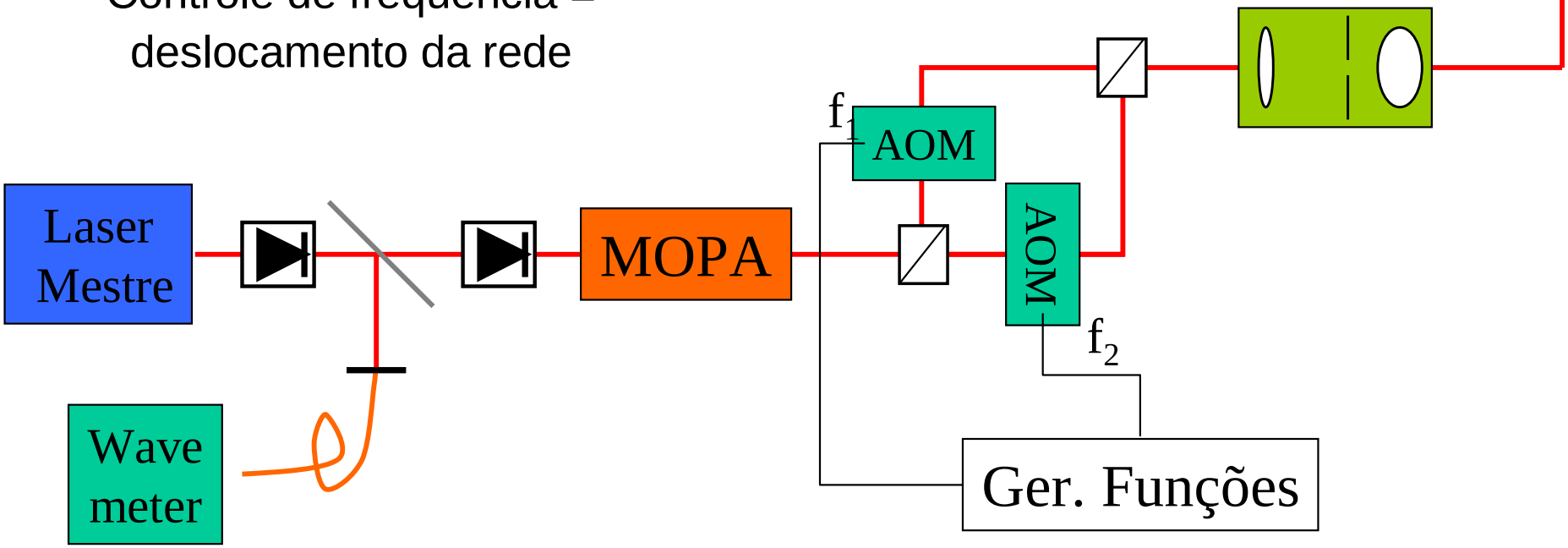
Átomos frios aprisionados em uma MOT
~10^8 átomos, T~30 μK

Feixes da rede
Linha D_2, ^{85}Rb, Δ=30 GHz



Controle de amplitude = Profundidade da rede (níveis aprisionados)

Controle de freqüência = deslocamento da rede



Medida das populações, interações átomo-campo

Interação átomo-campo - Troca de fótons entre os campos através dos átomos.

Medida da intensidade = medida da posição.

Verificação das propriedades sobre o ruído da luz.

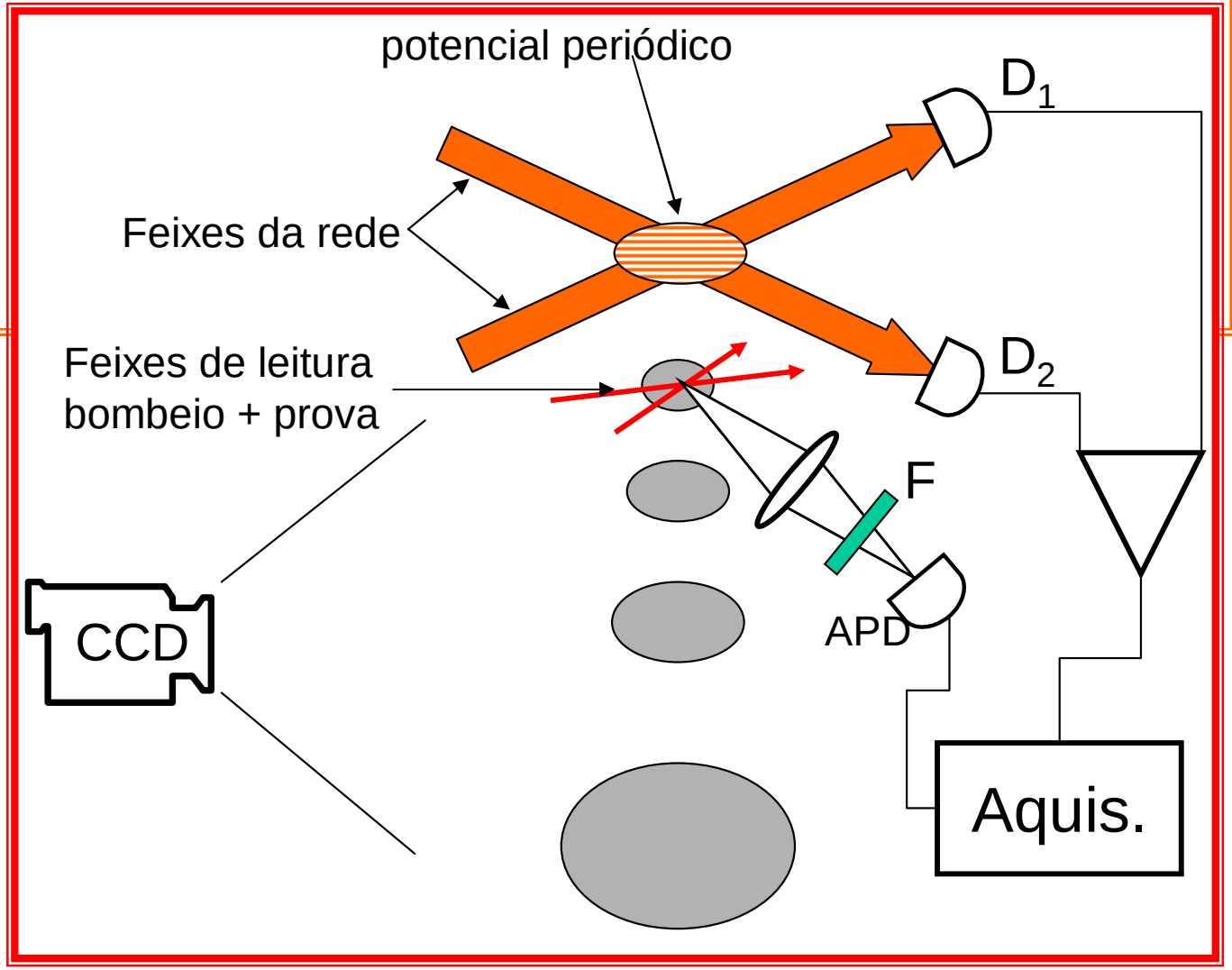
Fase e amplitude dos campos da rede.

Relação com estado dos átomos.

Correlações entre campos

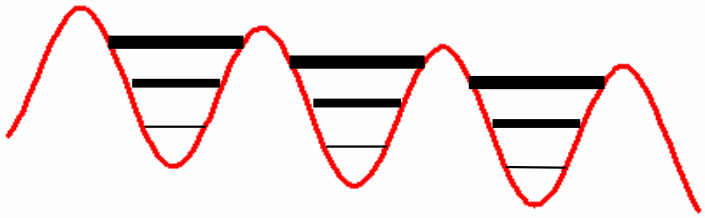
Estado do campo –

Estado vibracional

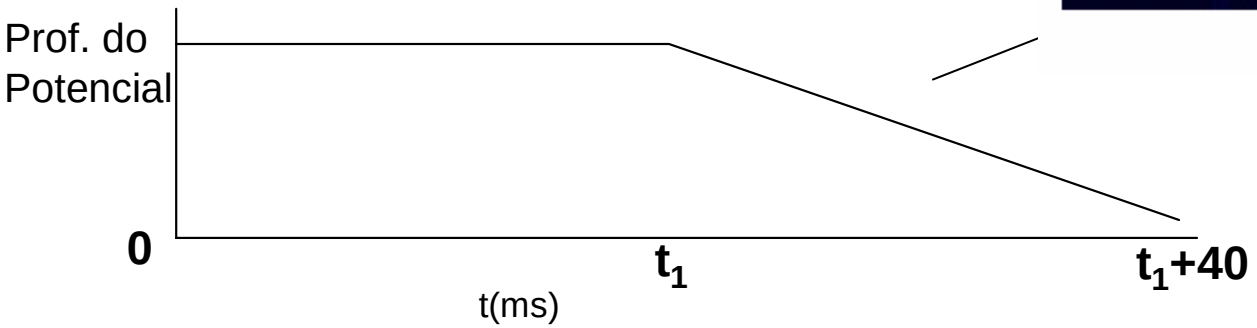


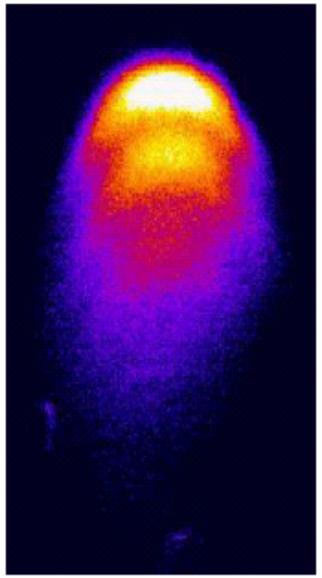
Medindo a população dos estados vibracionais

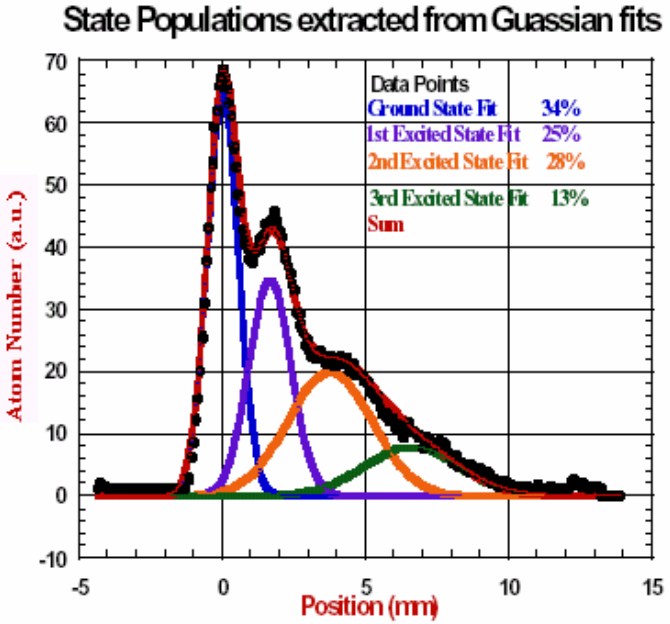
Rede Inicial



Redução adiabática do potencial

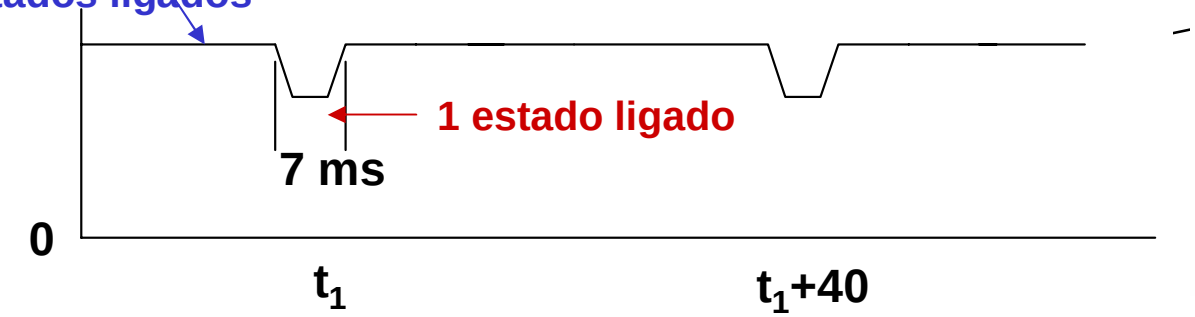


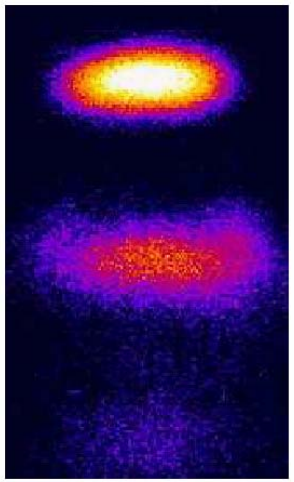


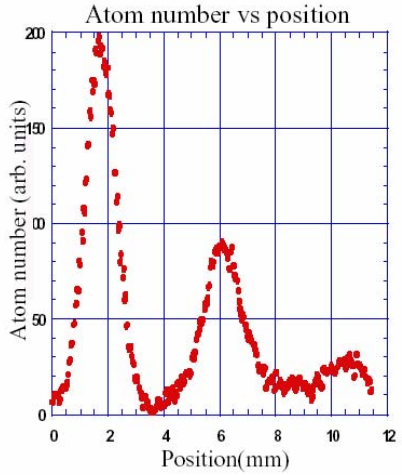


Medindo populações (2 estados)

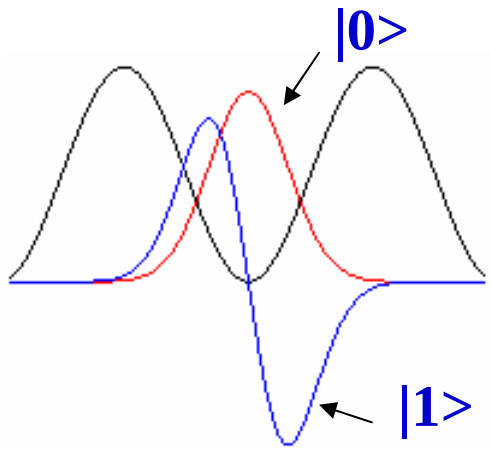
2 estados ligados







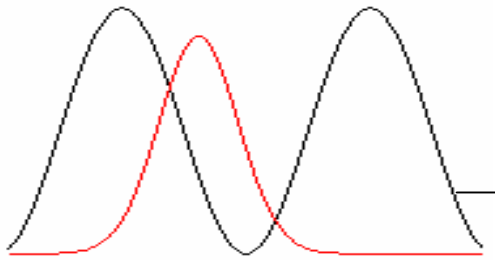
Manipulando o estado fundamental



Partindo do estado fundamental

Operador deslocamento $D(\alpha) = \exp(\alpha \hat{a}^{+} - \alpha^{*} \hat{a})$

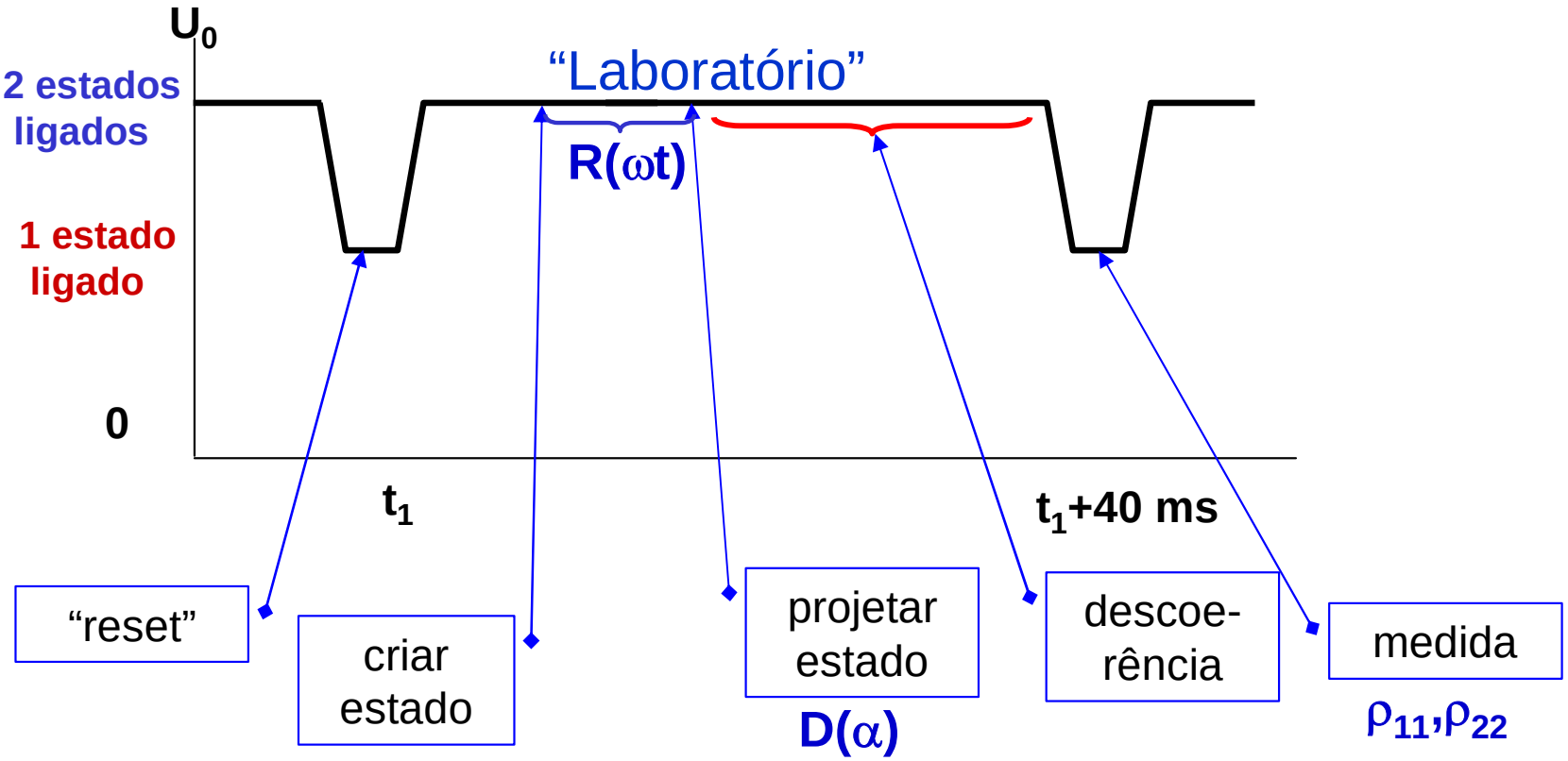
com α real



$D(\alpha)|0\rangle = a|0\rangle + b|1\rangle +$ átomos livres

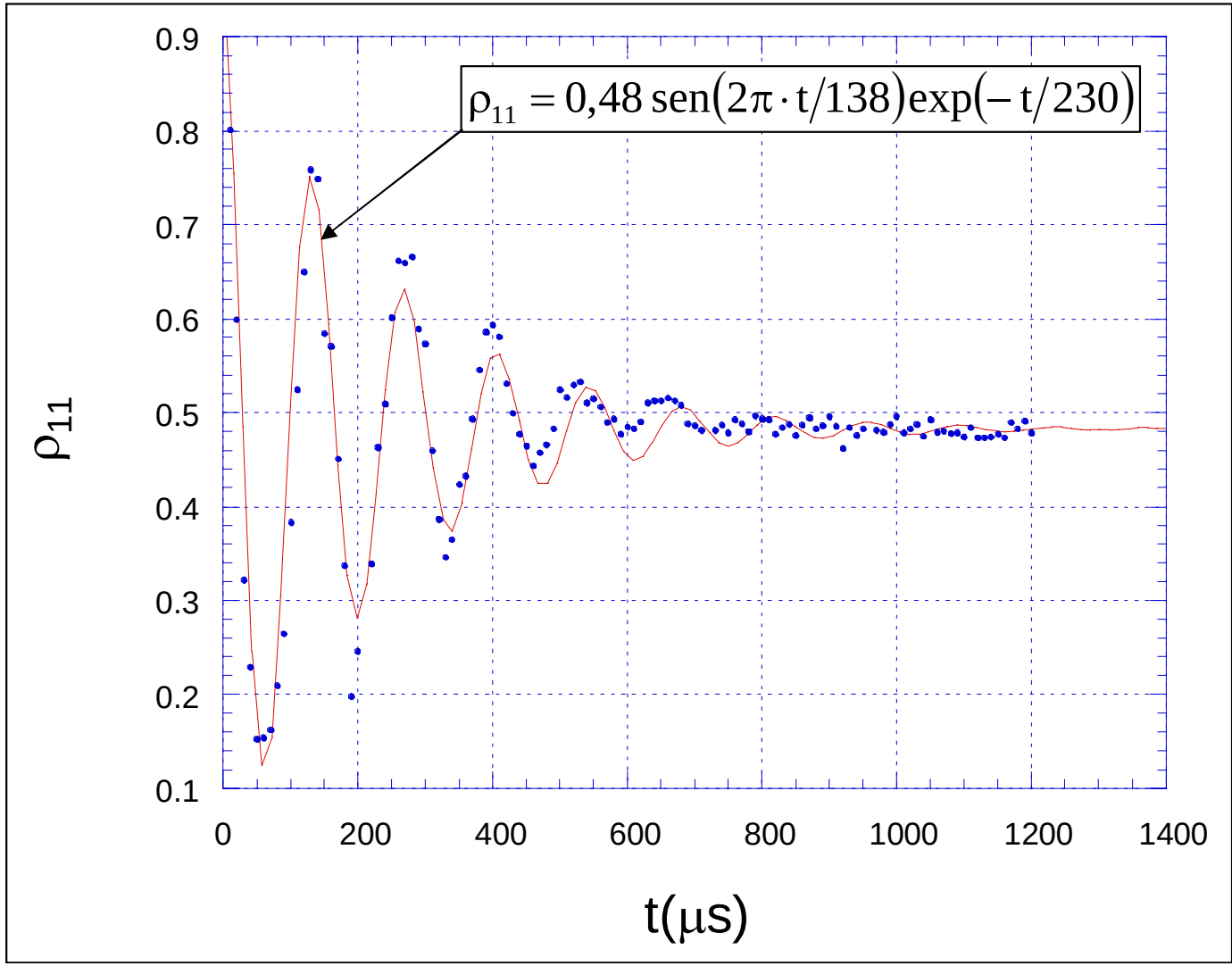
Operador rotação $R(\omega t) = \exp(-i \hat{a}^{+} \hat{a}\, \omega\, t)$

Acesso ao espaço de fase



Período de oscilação

- Deslocamento de |0>
- Evolução de fase (Time delay)
- Desfaz deslocamento
- Descoerência
- Medida da população de |0>



Conclusão

Seguindo a montagem proposta por ***A. Steinberg*** (U. Toronto), estamos implementando um sistema de controle do estado vibracional de átomos frios em redes óticas, como ferramentas para testes fundamentais em Informação Quântica.

Ou seja, Manipulação Coerente de Átomos com Luz

Conclusão

Informação Quântica

- Ferramenta básica para estudo dos princípios da Mecânica Quântica.
- Permite modelar o funcionamento de um computador quântico.
- Novos princípios para problemas insolúveis classicamente.
- Aplicações em simulações quânticas
- Aplicação em cripto-análise

Fim da segurança de dados?