

Luz e Átomos como ferramentas para Informação Quântica



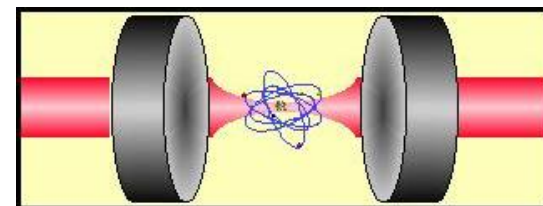
Inst. de
Física

USP

Marcelo
Martinelli



Conselho Nacional de Desenvolvimento
Científico e Tecnológico



Lab. de Manipulação
Coerente de Átomos e Luz



INCT-IQ

Laboratório de Manipulação Coerente de Átomos e Luz

Paulo Nussenzveig (1996)

Marcelo Martinelli (2004)

Alessandro Villar

Márcio Heráclito (Post-doc)

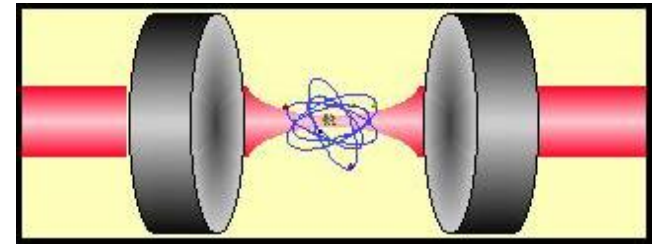
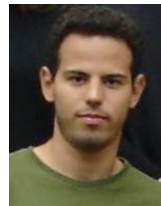
Antônio Sales (PhD – MSc 2008)

Felippe Barbosa (PhD – MSc 2008)

Hans Marin Torres (MSc)

Flávio Moraes (MSc)

Paula Meirelles (PhD)



José Aguirre (U. Concepción)

Luciano Cruz (UFABC - Br)

Paulo Valente (U. República - Uruguay)

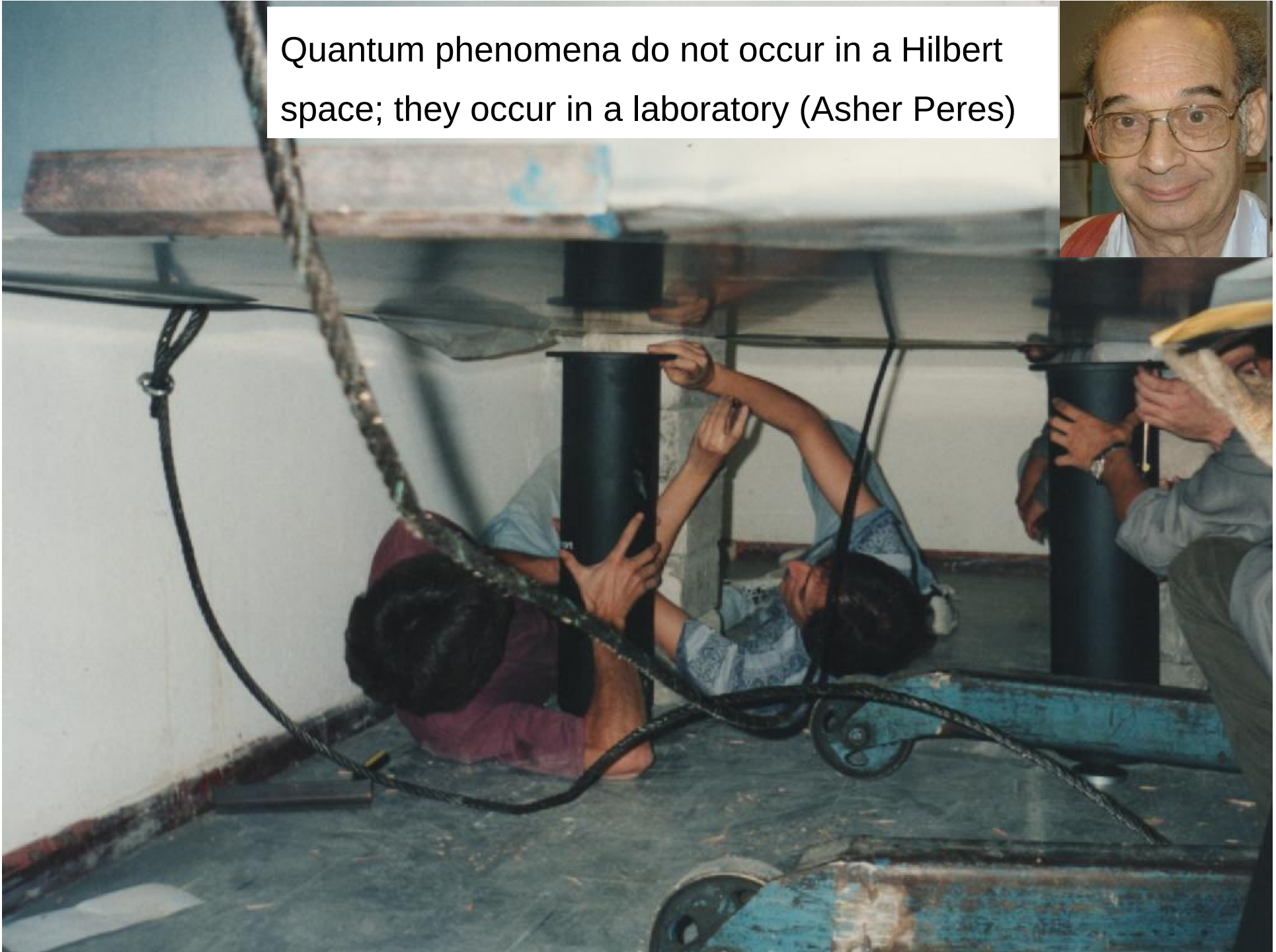
Daniel Felinto (UFPE - Br)

Katiúscia Cassemiro (UFF-Br)



Alessandro Villar (MPI)

Quantum phenomena do not occur in a Hilbert space; they occur in a laboratory (Asher Peres)



Theory: Quantum Mechanics and Quantum Optics

Techniques: Measurement of the Electromagnetic Field

Tools: Rubidium Atoms and Optical Parametric Oscillators

Problems: Entanglement, Sudden Death, Teleportation...



1. Introdução:

Revisão de Mecânica Quântica

Medidas

Princípio de Superposição

Relação de Incerteza

Operador Densidade

Estados Puros e Misturas

Emaranhamento

Paradoxo EPR

Pequena revisão de Mecânica Quântica

|| O estado do sistema contém toda a informação que podemos extrair dele.
|| Descrição completa!

|| Classicamente: Estado de uma partícula pode ser descrito pelo seu espaço
|| de fase → posição e momento.

|| Quanticamente: Função do estado descreve o que podemos saber
|| sobre o sistema

|| Estados podem ser discretos ou contínuos!

- Medidas são descritas por operadores (atuando sobre os estados).
- Valores médios dos operadores definem os valores possíveis dos estados.
- Espectro discreto ou contínuo.

- Estados são descritos por “rótulos”:
- Conjunto de medidas possíveis para reconstruir o estado definem “números quânticos”.

Variáveis discretas:

medidas retornam um
espectro discreto →

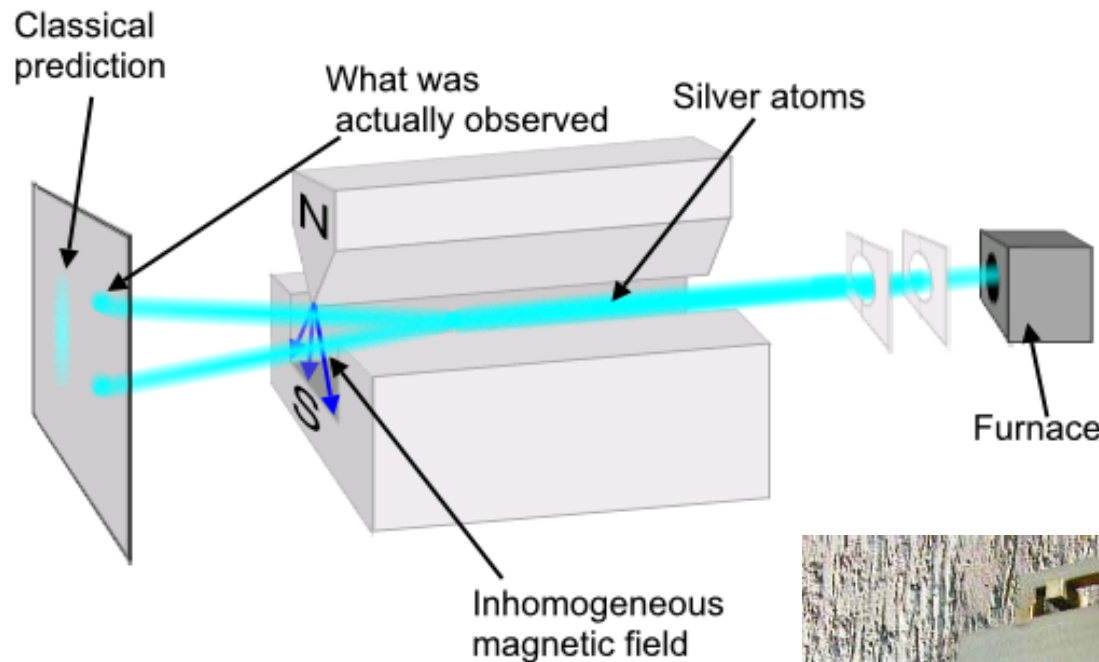
- Polarização (de um fóton),
- Momento angular (de uma partícula),
- Energia (estados ligados),

Variáveis contínuas:

espectro contínuo →

- Energia,
- Posição,
- Momento,
- Polarização, etc.

A experiência de Stern e Gerlach

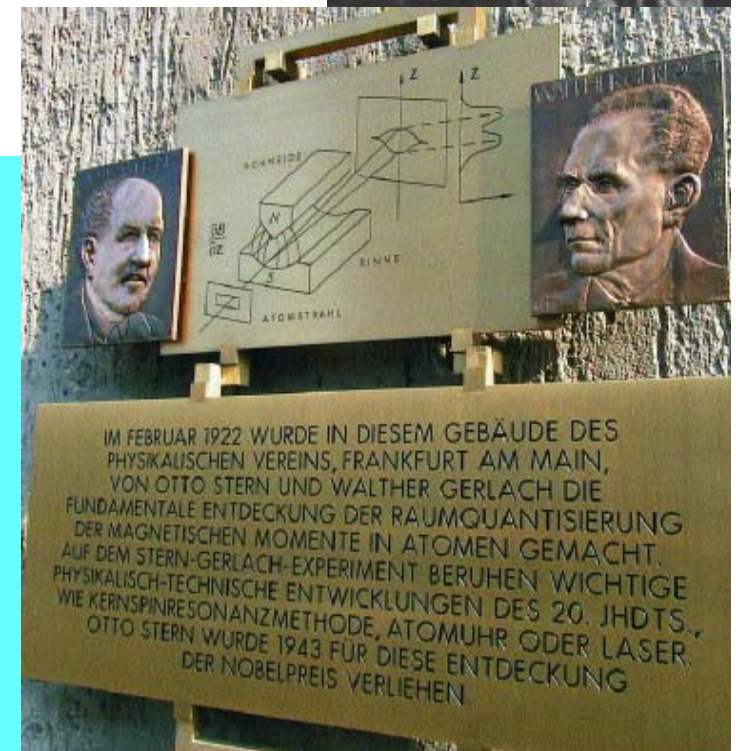


Front



Back

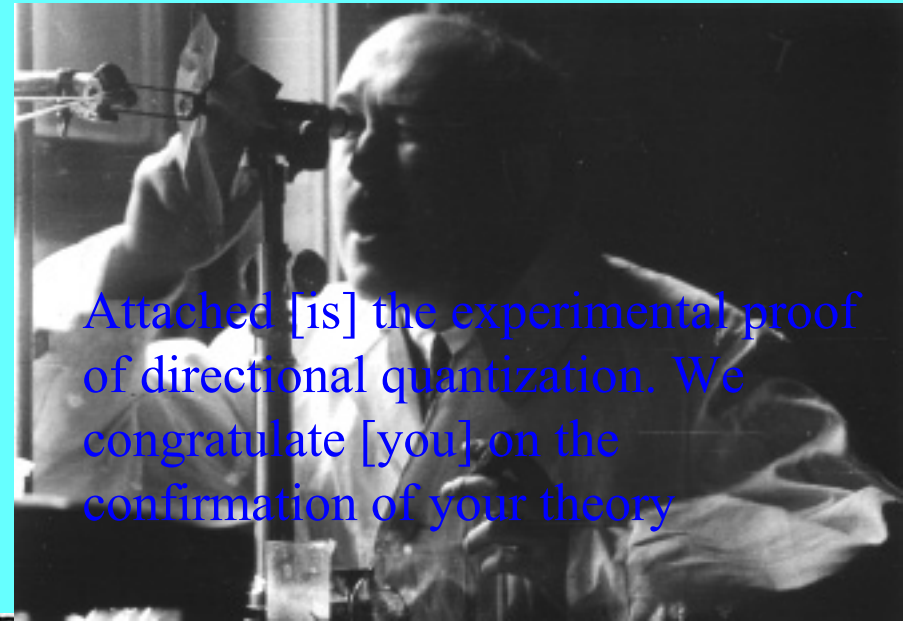
Prêmio Nobel 1943



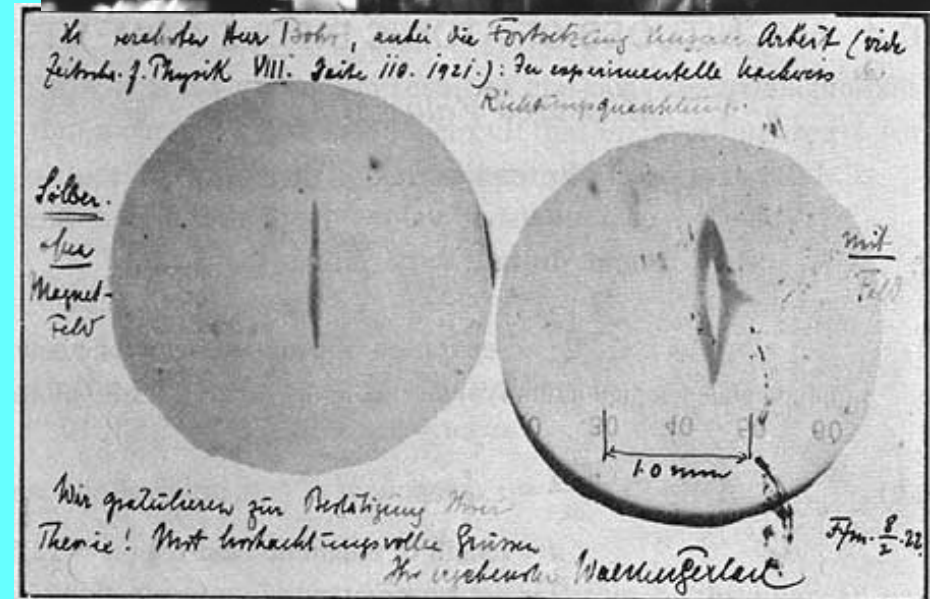
A experiência de Stern e Gerlach

“After venting to release the vacuum, Gerlach removed the detector flange. But he could see no trace of the silver atom beam and handed the flange to me. With Gerlach looking over my shoulder as I peered closely at the plate, we were surprised to see gradually emerge the trace of the beam. . . . Finally we realized what [had happened]. I was then the equivalent of an assistant professor. My salary was too low to afford good cigars, so I smoked bad cigars. These had a lot of sulfur in them, so my breath on the plate turned the silver into silver sulfide, which is jet black, so easily visible. It was like developing a photographic film.”

“If this nonsense of Bohr should in the end prove to be right, we will quit physics!” (Stern e von Laue, 1913)



Attached [is] the experimental proof of directional quantization. We congratulate [you] on the confirmation of your theory



Sistema discreto de dois níveis: Notação de Dirac

$$|\psi\rangle = |+\rangle \text{ ou } |-\rangle$$

Auto-estados do operador momento angular
(direção z) : L_z

Qubit !

$$|\psi\rangle = |0\rangle \text{ ou } |1\rangle$$

Estados do sistema: combinação linear de auto-estados

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

Superposição!

Representação: Esfera de Bloch Esfera de Poincaré

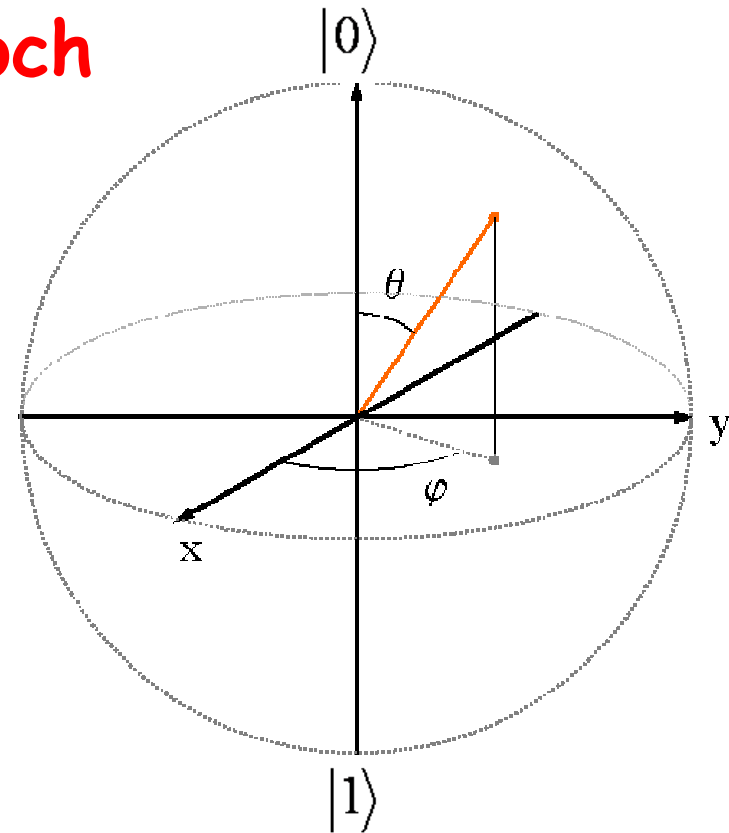
$$|\Psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

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

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

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

Operadores: $|\psi'\rangle = A|\psi\rangle$

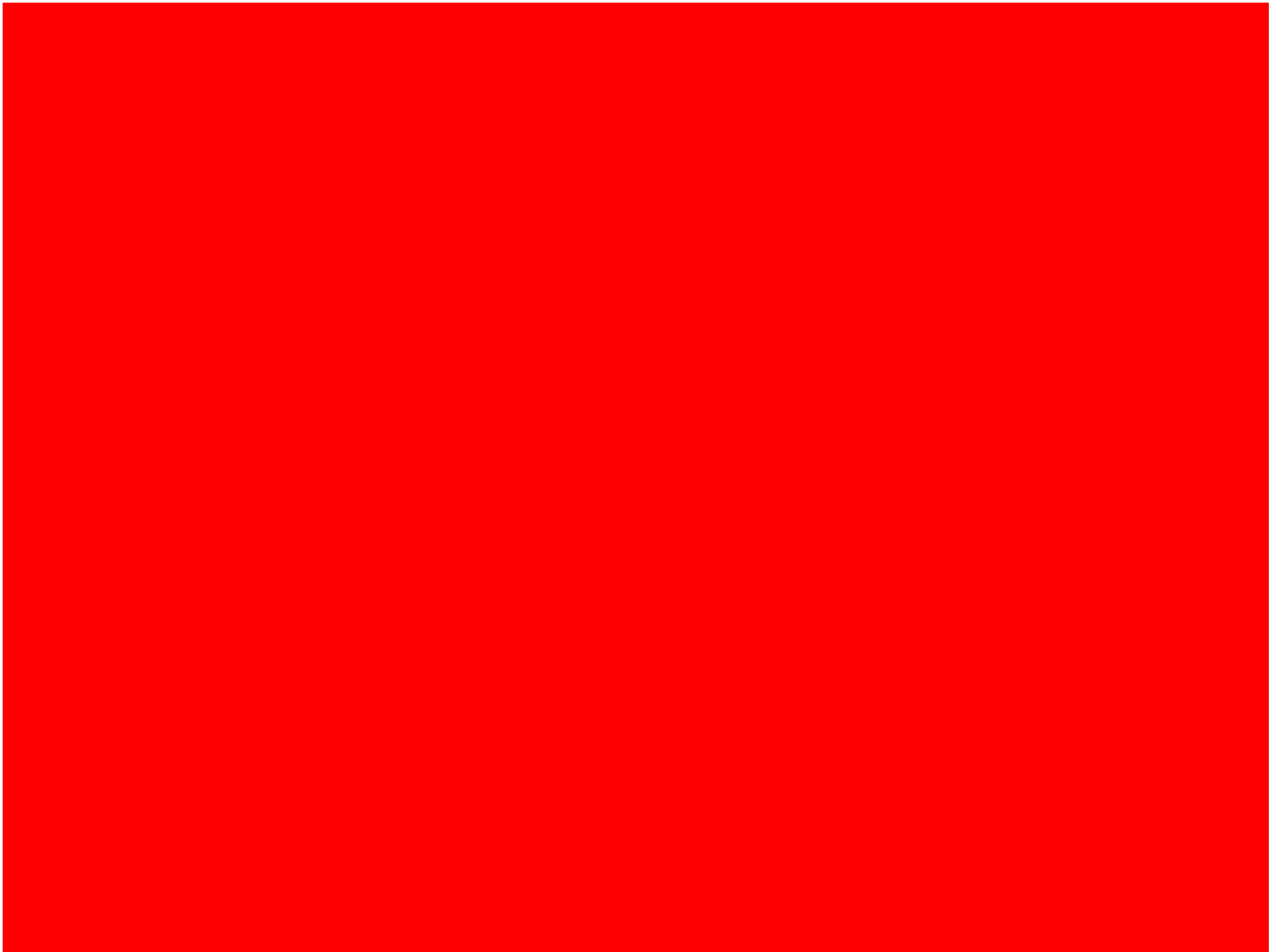
$$\langle\psi'| = \langle\psi|A^\dagger$$

Medidas:

Fazer a medida implica em projetar o estado.

Resultado: $\langle\psi|A|\psi\rangle$

Exemplo: "Stern-Gerlach" com fótons



Princípio da Incerteza e medidas incompatíveis

$$\Delta A = A - \langle A \rangle \qquad \langle (\Delta A)^2 \rangle \langle (\Delta B)^2 \rangle \geq |\langle \Delta A \Delta B \rangle|^2$$

$$\langle \Delta A \Delta B \rangle = \frac{\langle [\Delta A, \Delta B] \rangle}{2} + \frac{\langle \{ \Delta A, \Delta B \} \rangle}{2}$$

$$[\Delta A, \Delta B] = \Delta A \Delta B - \Delta B \Delta A$$

$$\{ \Delta A, \Delta B \} = \Delta A \Delta B + \Delta B \Delta A$$

$$\langle (\Delta A)^2 \rangle \langle (\Delta B)^2 \rangle \geq \frac{|\langle [\Delta A, \Delta B] \rangle|^2}{4}$$

Operador Densidade

Pure X Mixed States

$$|\psi\rangle = \sum c_n |a_n\rangle$$

$$c_n = \langle a_n | \psi \rangle$$

$$\sum |a_m\rangle \langle a_m| = 1$$

$$\langle a_m | a_n \rangle = \delta_{mn}$$

$$\langle A \rangle = \langle \psi | A | \psi \rangle$$

$$\langle a_m | A | a_n \rangle = A_{mn}$$

Introducing the density operator (von Neumann – 1927)

$$c_n c_m^* = \rho_{nm}$$

$$\rho = |\psi\rangle \langle \psi|$$



Operador Densidade

$$\langle A \rangle = \sum \langle a_n | \rho | a_m \rangle \langle a_m | A | a_n \rangle$$

$$= \sum \langle a_n | \rho A | a_n \rangle = \text{Tr}\{\rho A\}$$

Now we can represent a statistical mixture of pure states!

$$\rho = \sum p_k \rho_k \quad \sum p_k = 1 \quad \rho_k = |\psi_k\rangle \langle \psi_k|$$

$$\langle A \rangle = \text{Tr}\{\rho A\}$$

$$\text{Tr} \rho = 1$$

$$\text{Tr} \rho \geq \text{Tr} \rho^2$$

Não há nada que assuste na Mecânica Quântica?

The New York Times

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues
Find It Is Not 'Complete'
Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of
'the Physical Reality' Can Be
Provided Eventually.

PRINCETON, N. J., May 3.—Professor Albert Einstein will attack science's important theory of quantum mechanics, a theory of which he was a sort of grandfather. He concludes that while it is "correct" it is not "complete."

With two colleagues at the Institute for Advanced Study here, the noted scientist is about to report to the American Physical Society what is wrong with the theory of quantum mechanics, it has been learned exclusively by Science Service.

The quantum theory, with which science predicts with some success inter-atomic happenings, does not meet the requirements for a satisfactory physical theory, Professor Einstein will report in a joint paper with Dr. Boris Podolsky and Dr. N. Rosen.

EPR e Desigualdade de Bell

Anybody who is not shocked by quantum theory has not understood it.

Niels Bohr



MAY 15, 1935

PHYSICAL REVIEW

VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality.

Einstein, Podolsky & Rosen's paper

If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.

either (1) the quantum-mechanical description of reality given by the wave function is not complete or (2) when the operators corresponding to two physical quantities do not commute the two quantities cannot have simultaneous reality.

O exemplo de EPR



$$|\psi\rangle \cong \delta(x_1 - x_2 - L)\delta(p_1 + p_2) \quad (\text{localizada em } x_1 - x_2 \text{ e } p_1 + p_2)$$

We see therefore that, as a consequence of two different measurements performed upon the first system, the second system may be left in states with two different wave functions. On the other hand, since at the time of measurement the two systems no longer interact, no real change can take place in the second system in consequence of anything that may be done to the first system.

Uma medida de x_1 fornece x_2 , assim como uma medida de p_1 fornece p_2 . Mas x_2 e p_2 *não comutam!* $\leftrightarrow [x, p] = i \hbar$

A conclusão de EPR

either (1) *the quantum-mechanical description of reality given by the wave function is not complete* or (2) *when the operators corresponding to two physical quantities do not commute the two quantities cannot have simultaneous reality.*

Se (1) é falso, então (2) também é falso! Portanto, (1) deve ser verdadeiro: a teoria quântica, embora forneça previsões corretas, deve ser *incompleta*. As medidas devem apenas revelar estados já pré-existentes, ainda não descritos pela teoria.

A resposta de Bohr

OCTOBER 15, 1935

PHYSICAL REVIEW

VOLUME 48

Can Quantum-Mechanical Description of Physical Reality be Considered Complete?

N. BOHR, *Institute for Theoretical Physics, University, Copenhagen*

(Received July 13, 1935)

$$\begin{aligned} [q_1 p_1] &= [q_2 p_2] = i\hbar/2\pi, \\ [q_1 q_2] &= [p_1 p_2] = [q_1 p_2] = [q_2 p_1] = 0, \end{aligned}$$

$$\begin{aligned} q_1 &= Q_1 \cos \theta - Q_2 \sin \theta & p_1 &= P_1 \cos \theta - P_2 \sin \theta \\ q_2 &= Q_1 \sin \theta + Q_2 \cos \theta & p_2 &= P_1 \sin \theta + P_2 \cos \theta. \end{aligned}$$

$$\begin{aligned} [Q_1 P_1] &= i\hbar/2\pi, & [Q_1 P_2] &= 0, & Q_1 &= q_1 \cos \theta + q_2 \sin \theta, \\ & & & & P_2 &= -p_1 \sin \theta + p_2 \cos \theta, \end{aligned}$$

Bohr introduz a noção de *complementaridade*, mas sua resposta não contém elementos que permitam *descartar* o programa proposto por EPR.

As desigualdades de Bell



Somente em 1964/1966 o “paradoxo” de EPR se tornou mais interessante para a comunidade de físicos. O irlandês John Bell conseguiu demonstrar uma desigualdade que deveria ser satisfeita por teorias de variáveis ocultas que respeitassem a condição de *localidade*. Seria possível realizar *testes experimentais*.

REVIEWS OF MODERN PHYSICS

VOLUME 38, NUMBER 3

JULY 1966

On the Problem of Hidden Variables in Quantum Mechanics*

JOHN S. BELL†

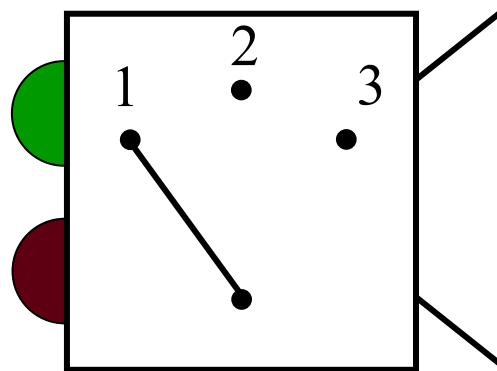
Bringing home the atomic world: Quantum mysteries for anybody

N. D. Mermin

Laboratory of Atomic and Solid State Physics, Cornell University, Ithaca, New York 14853

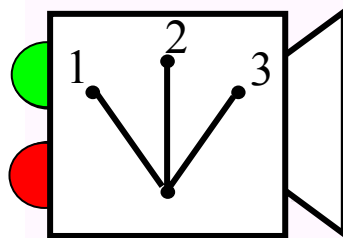
(Received 19 November 1980; accepted 5 January 1981)

940 Am. J. Phys. 49(10), Oct. 1981

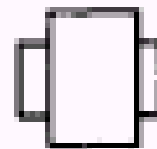


23GR	12GR	11GG	13GR	23RG	33GG	12RG	21GR
11RR	31RG	22GG	11GG	22GG	11RR	32RG	23RG
31RG	32GR	22RR	31RG	13RG	22GG	22RR	12GG
33RR	22RR	21GR	32RG	11GG	32GR	33GG	21GR
32GG	22GG	11RR	11GG	23GG	12RR	32GR	11GG
32RG	12RG	13RG	33GG	21RG	13GR	31RR	32GR
31GR	13GR	21RG	33RR	13GR	11RR	11GG	13RG
12GG	32GR	33GG	21GR	21GG	33RR	23RG	21GG
13GR	11GG	32GG	31GR	32RG	33RR	13RR	13RG
11GG	31RG	33RR	12RG	21GR	11GG	22GG	33GG
33RR	21GG	21RG	12RG	11GG	12RG	11GG	23GG
11GG	12RR	12RG	31GR	23GR	12GR	33GG	31GG
11RR	22RR	12RG	22GG	23GR	12GR	23RG	21RR
13GR	21RR	33RR	33RR	13RG	23RG	33GG	32RR
13RR	32RG	11RR	11RR	11RR	32RG	12RG	21RG
23RG	23RR	21RG	33RR	13GR	12GR	23RG	21RR
13RR	21GR	12RR	31GR	12RG	13GR	13RG	22RR
21RG	23GR	11RR	12RR	33RR	21RG	13GR	21RR
31GR	23GG	13RG	21RG	11GG	12GR	23GR	13GG
11RR	31RG	11GG	31GR	32GR	32RG	32GR	11GG

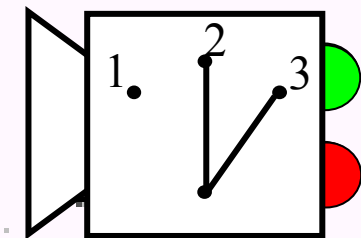
- (a) 11, 22, ou 33: RR e GG com mesma frequência; jamais RG ou GR
- (b) 12, 13, 21, 23, 31, 32: RR e GG com mesma frequência, $\frac{1}{4}$ do total; $\frac{3}{4}$ do tempo RG ou GR (com mesma frequência)



(A)



(C)



(B)

Bringing home the atomic world: Quantum mysteries for anybody

N. D. Mermin

Laboratory of Atomic and Solid State Physics, Cornell University, Ithaca, New York 14853

(Received 19 November 1980; accepted 5 January 1981)

940 Am. J. Phys. 49(10), Oct. 1981

- (a) Partículas têm instrução do tipo: RRR, RRG, RGR, RGG, GRR, GRG, GGR, GGG. Para explicar o caso (a), basta supor que as partículas emitidas são sempre idênticas.
- (b) Vamos analisar o caso (b) de acordo com essa hipótese. Suponhamos que as partículas tenham a instrução RRG. Dos seis arranjos possíveis, só nos casos 12 e 21 lâmpadas de mesma cor acenderão. Como todos os arranjos são supostos aleatórios, o mesmo vale para as instruções RGR, RGG, GRR, GRG e GGR. Nos casos RRR e GGG, as lâmpadas sempre acenderão com a mesma cor. Portanto, a probabilidade de termos lâmpadas de mesma cor no caso (b) deveria ser superior a *um terço*, enquanto os resultados fornecem apenas *um quarto*!

Conclusão: experiência é incompatível com descrição em termos de conjunto de instruções bem definidas *a priori*.

Bringing home the atomic world: Quantum mysteries for anybody

N. D. Mermin

Laboratory of Atomic and Solid State Physics, Cornell University, Ithaca, New York 14853

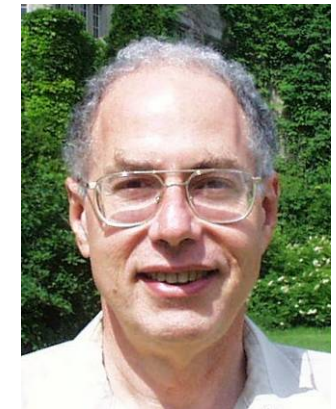
(Received 19 November 1980; accepted 5 January 1981)

Como fazer isso na prática? Podemos, por exemplo, fazê-lo com partículas de spin meio, num estado do tipo

$$\frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}}$$

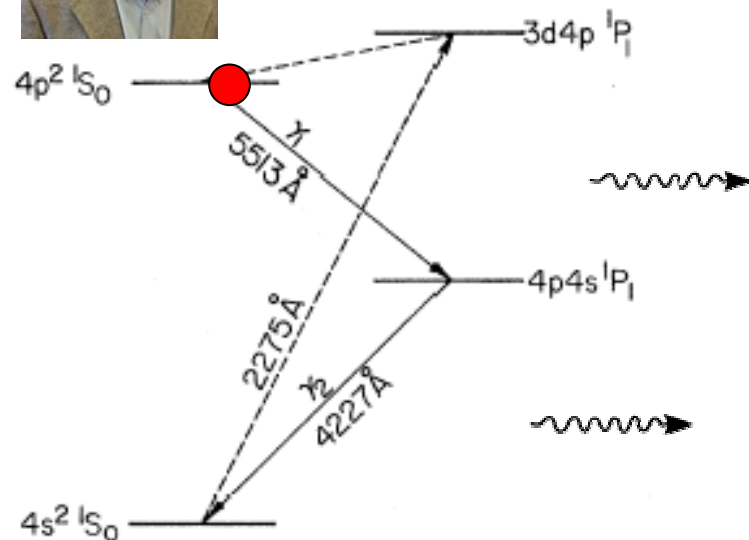
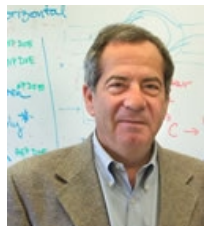
Os detetores são dispositivos tipo Stern-Gerlach com três posições possíveis: alinhados, ou a $\pm 120^\circ$. A probabilidade de medir spins opostos vale $\cos^2(\theta/2)$. Os detetores são codificados com cores invertidas. Desigualdades foram obtidas por J. S. Bell, *Physics* **1**, 195 (1964). Medidas foram feitas por: S. J. Freedman and J. S. Clauser, *Phys. Rev. Lett.* **28**, 938 (1972) e A. Aspect, J. Dalibard, and G. Roger, *Phys. Rev. Lett.* **47**, 1804 (1982).

Clauser, Horne, Shimony e Holt (CHSH)



Desigualdades em forma mais apropriada para teste experimental

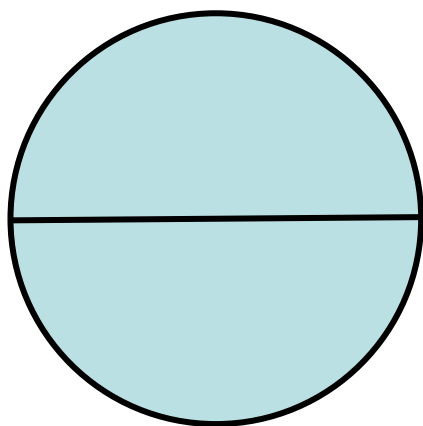
Freedman e Clauser (PRL, 1972)



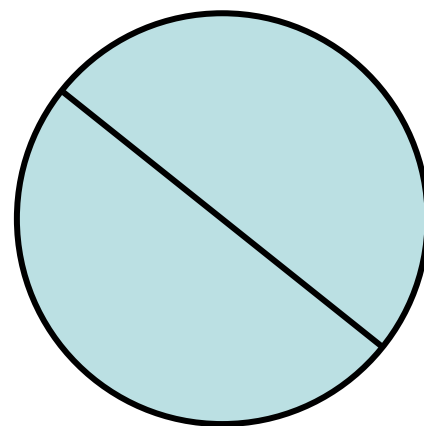
Fótons têm mesma polarização, embora a polarização de cada um não esteja bem definida. $\Rightarrow$ estado emaranhado.

Einstein: conceito de *quanta de luz* é difícil.

Anton Zeilinger: “photons are clicks on photodetectors”.



..



$$-1 \leq \Delta(\varphi) \leq 0$$

$$\Delta(22\frac{1}{2}^\circ) = 0.104 \pm 0.026$$

$$\Delta(67\frac{1}{2}^\circ) = -1.097 \pm 0.018$$

"Loopholes", segundo Bell

"... it is hard for me to believe that quantum mechanics works so nicely for inefficient practical set-ups and is yet going to fail badly when sufficient refinements are made. Of more importance, in my opinion, is the complete absence of the vital time factor in existing experiments. The analyzers are not rotated during the flight of the particles."

John Bell



As experiências de Alain Aspect

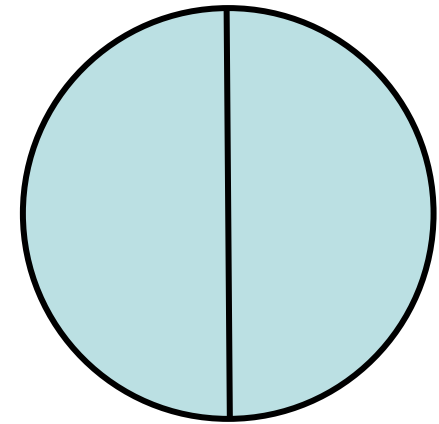
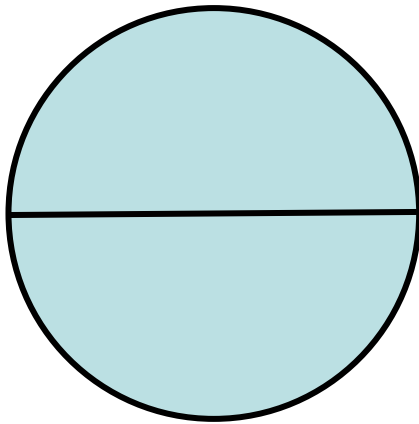


Experimental Test of Bell's Inequalities Using Time-Varying Analyzers

Alain Aspect, Jean Dalibard,^(a) and Gérard Roger
Institut d'Optique Théorique et Appliquée, F-91406 Orsay Cédex, France
(Received 27 September 1982)

PHYSICAL REVIEW LETTERS

VOLUME 49, 1804 20 DECEMBER 1982



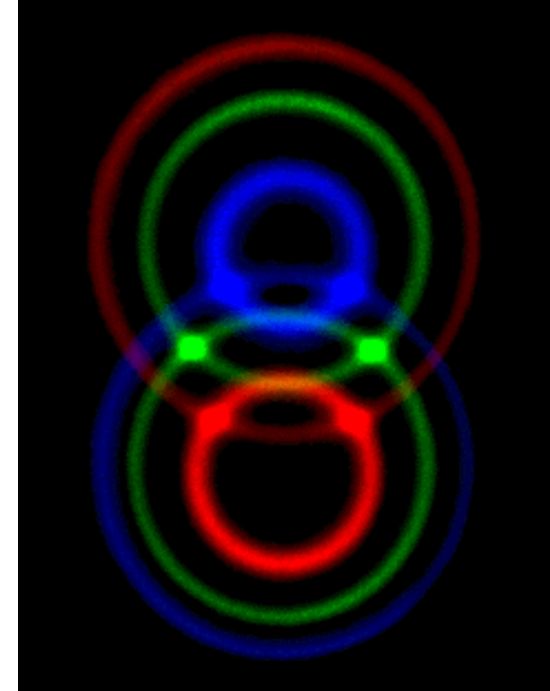
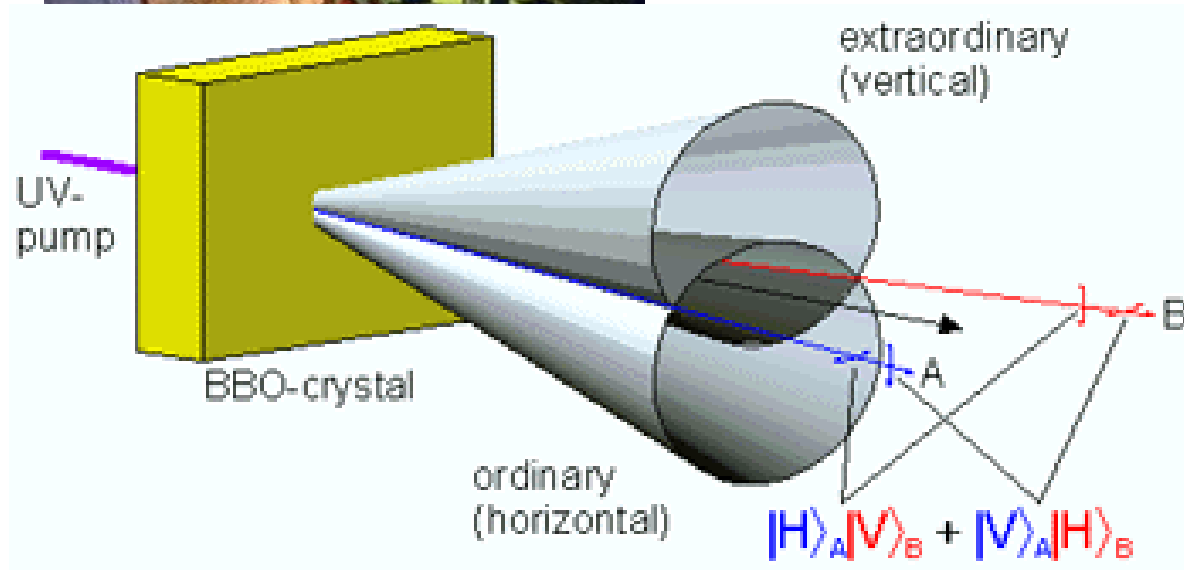
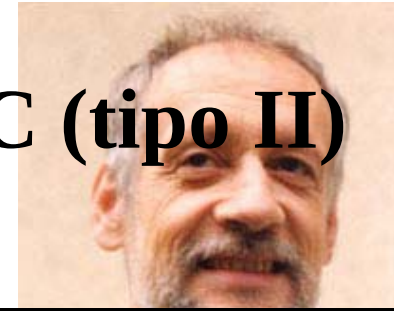
$$-1 \leq S \leq 0$$

$$S_{\text{exp t}} = 0.101 \pm 0.020$$

$$S_{\text{QM}} = 0.112$$

Experiências mais recentes nos grupos de Anton Zeilinger e Nicolas Gisin

Geração de Fótons Gêmeos por PDC (tipo II)



Estado gerado é *emaranhado*.

PHYSICAL REVIEW LETTERS

VOLUME 81

7 DECEMBER 1998

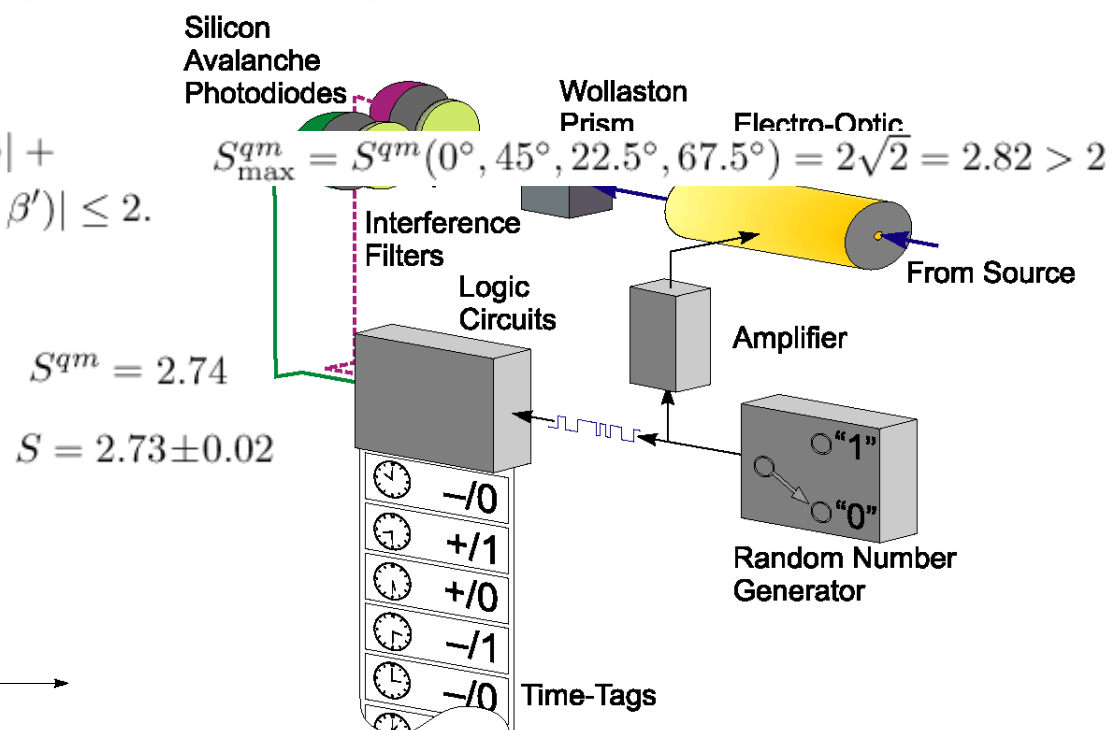
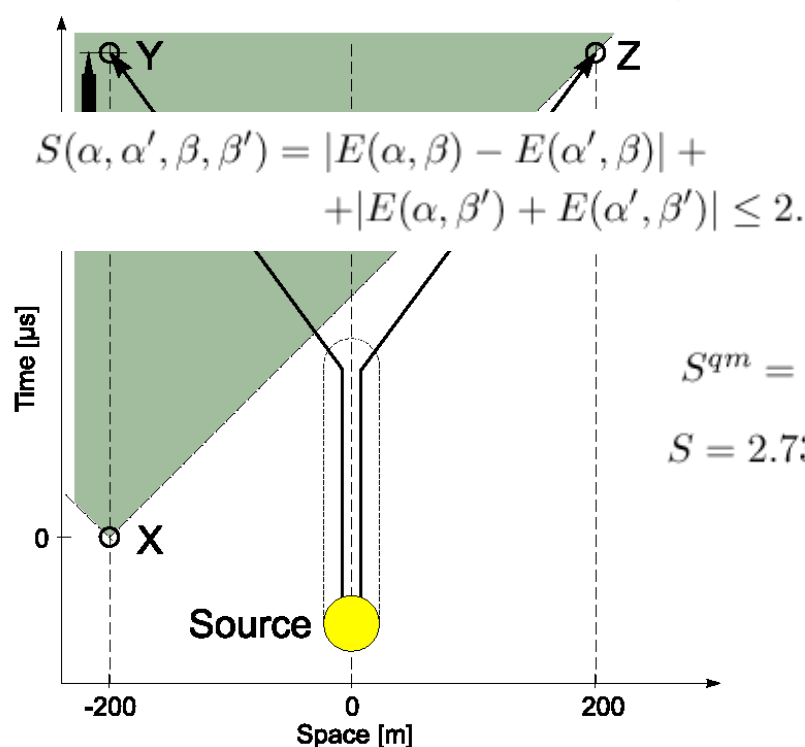
NUMBER 23

Violation of Bell's Inequality under Strict Einstein Locality Conditions

Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger

Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria

(Received 6 August 1998)

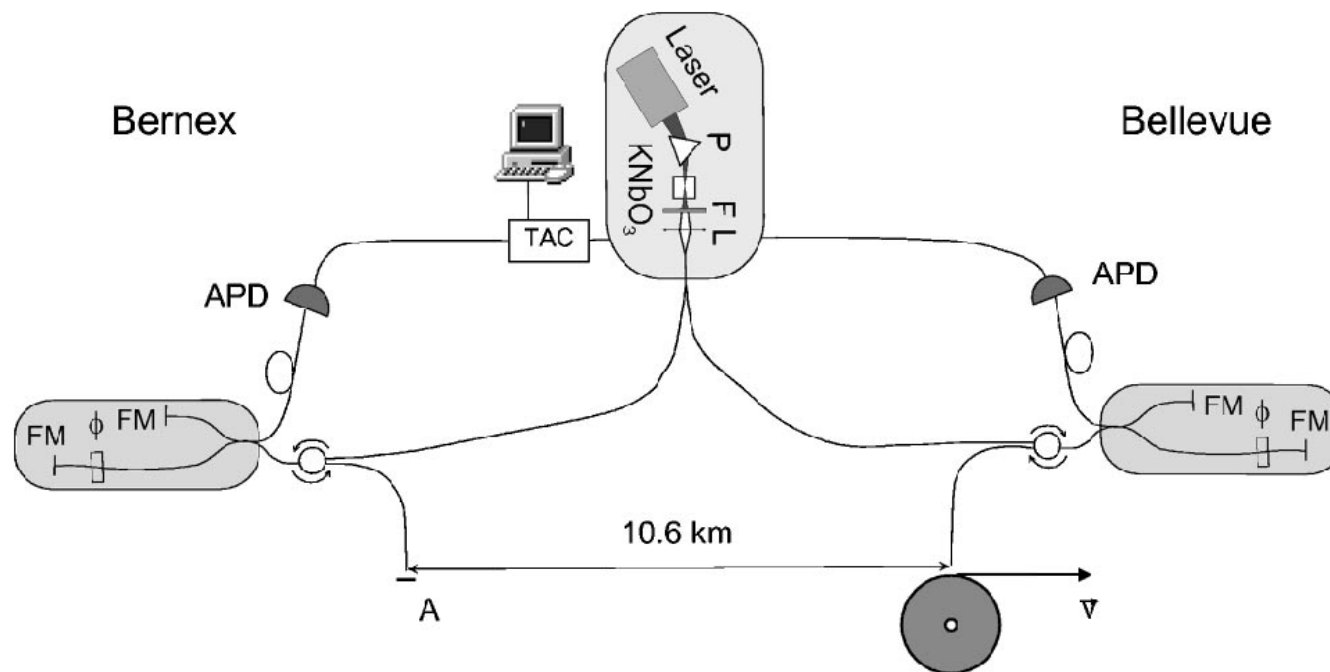


Experimental test of nonlocal quantum correlation in relativistic configurations

H. Zbinden, J. Brendel, N. Gisin, and W. Tittel

Group of Applied Physics, University of Geneva, 1211 Geneve 4, Switzerland

(Received 5 July 2000; published 17 January 2001)



Projeção? Como os eventos têm separação tipo-espaco, o movimento relativo elimina a noção de *simultaneidade*. A ordem temporal dos eventos depende do referencial (no referencial próprio de cada detector, é ele quem recebe primeiro o fóton e, portanto, “projeta” o estado do outro fóton).

2. Informação Quântica:

Uso do emaranhamento

Criptografia e Decodificação

Gato de Schroedinger

Descoerência

Usos do Emaranhamento:

Informação Quântica

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

Mecânica Quântica → *teoria de informação*.

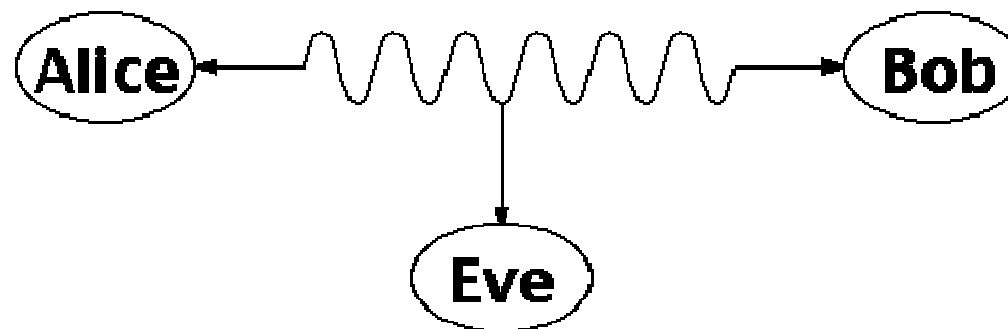
- Vivemos numa “sociedade de informação”: a velocidade de progresso do processamento, armazenamento e transmissão de informação é enorme. Há algum limite?
- Toda informação é processada, armazenada e transmitida por algum sistema físico.

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...

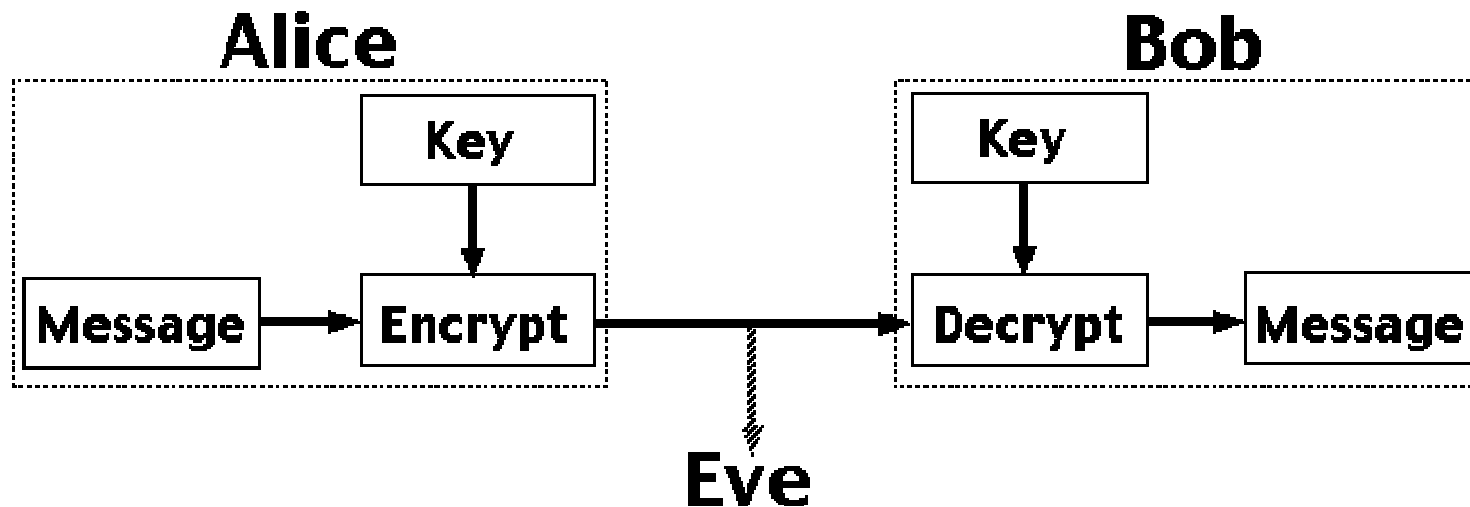
Estações A e B dispõem de um canal de comunicação...



...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

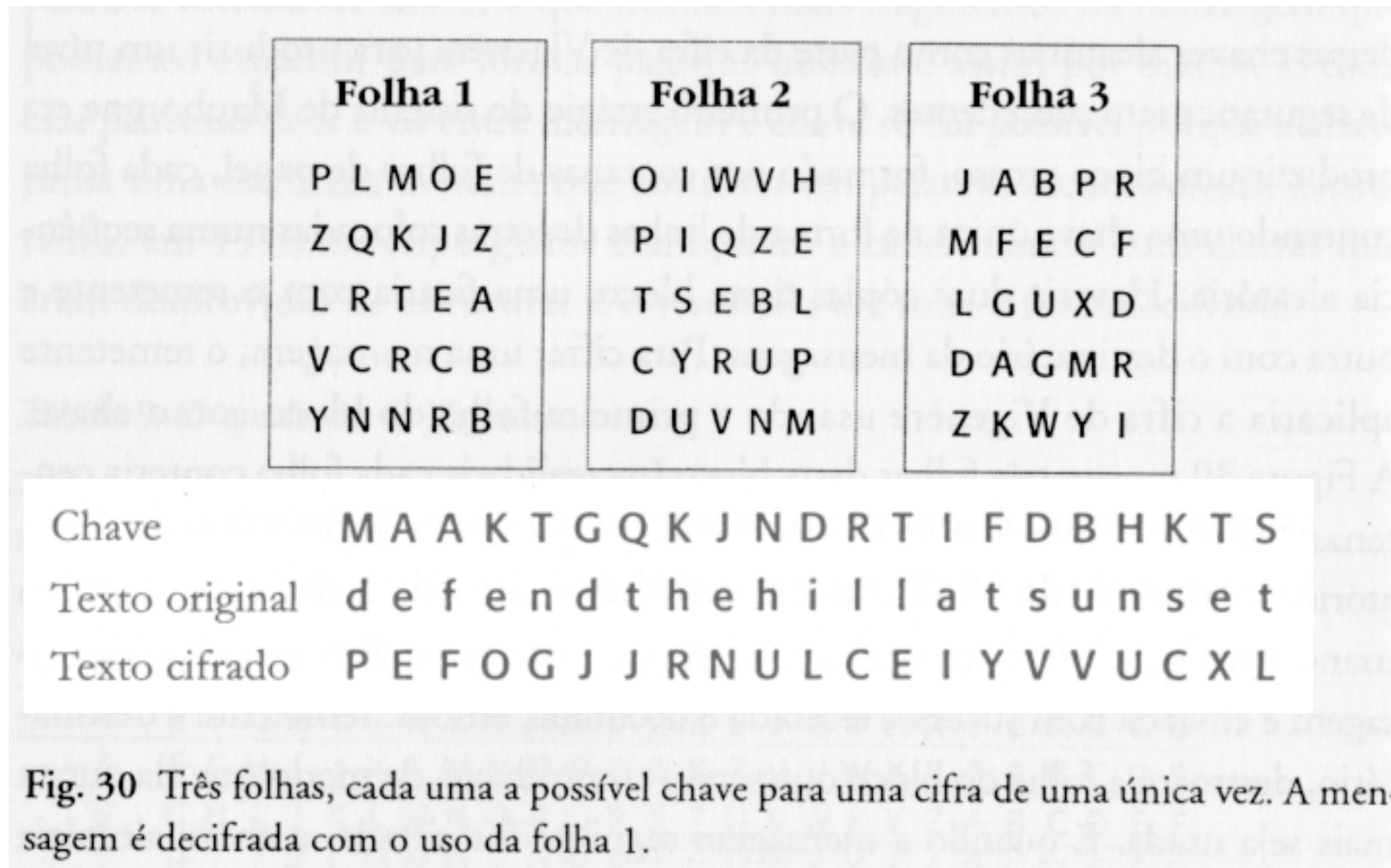
Bloco de cifras de utilização única (1918)

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

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?

Bloco de cifras de utilização única (1918)



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?

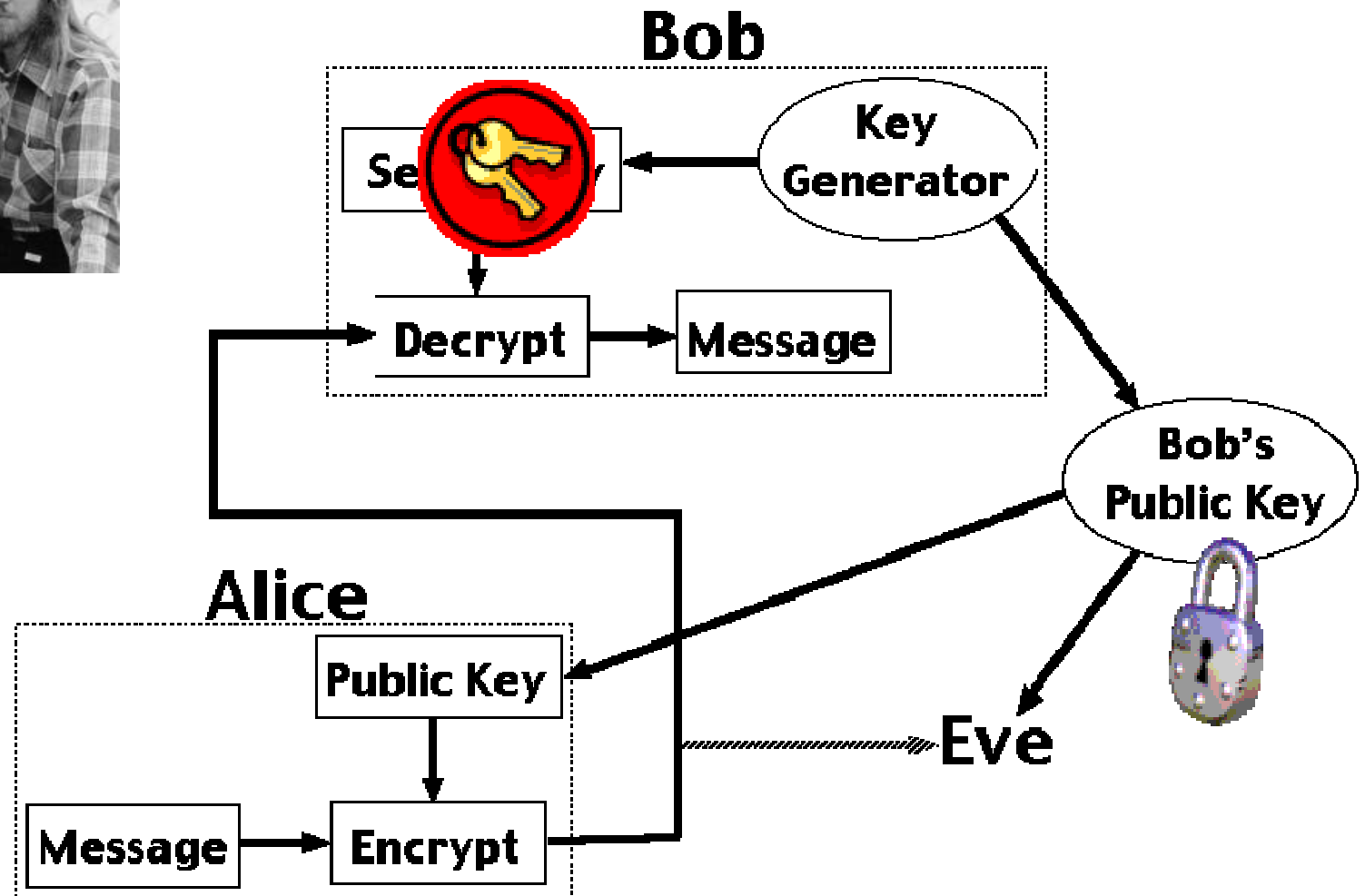
Criptografia com chave assimétrica: encripta com chave pública, decodifica com chave secreta



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

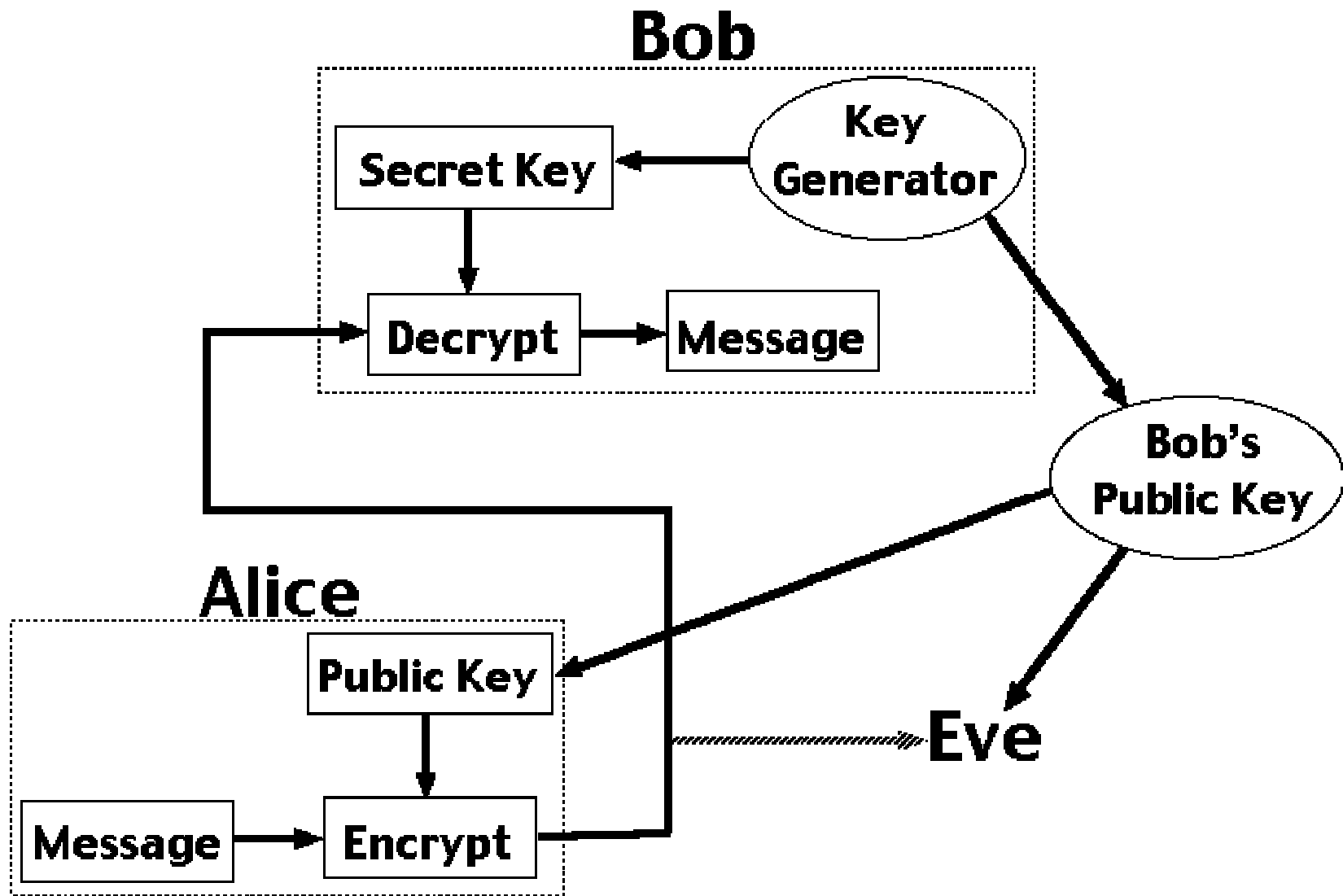
- *Escolha p, q (primos)*
- *Calcule $n = p q$*
- *Calcule $m = (p-1)(q-1)$*
- *Escolha um número e (co-primo com m)*
- ***Dado p, q , calcule d , tal que***
$$d e = 1 \pmod{m}$$
- *Chave pública: e, n*
- *Chave secreta: d, n*

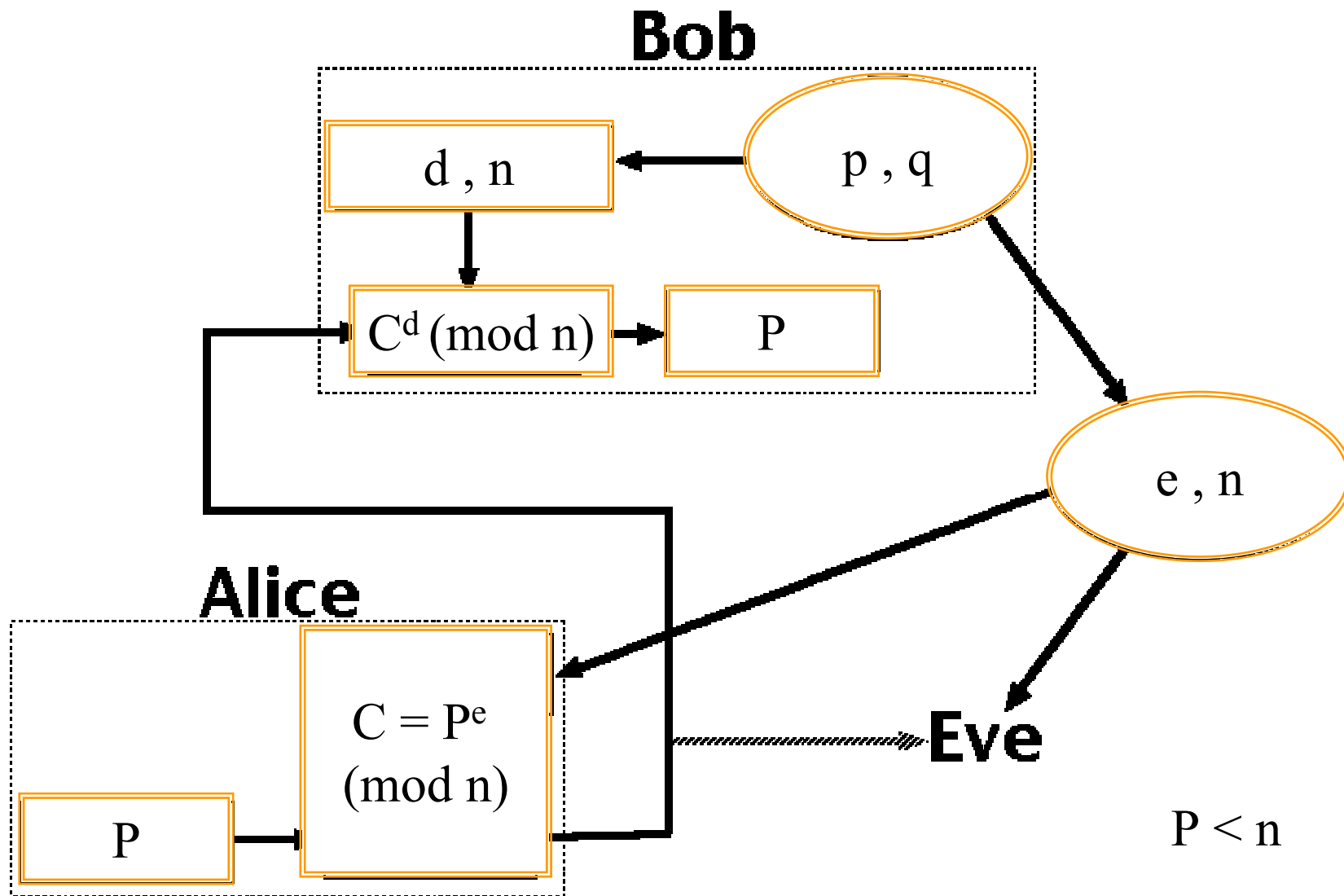
Slide 42

P.N.1

Martin Hellman, Whitfield Diffie, Ralph Merkle

Paulo A. Nussenzveig; 18/10/2005





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.

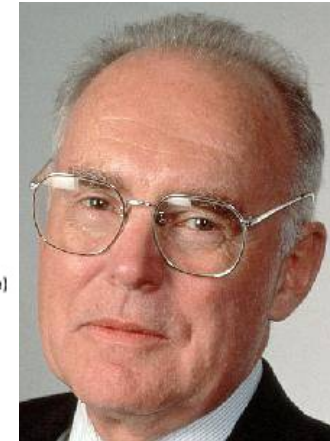
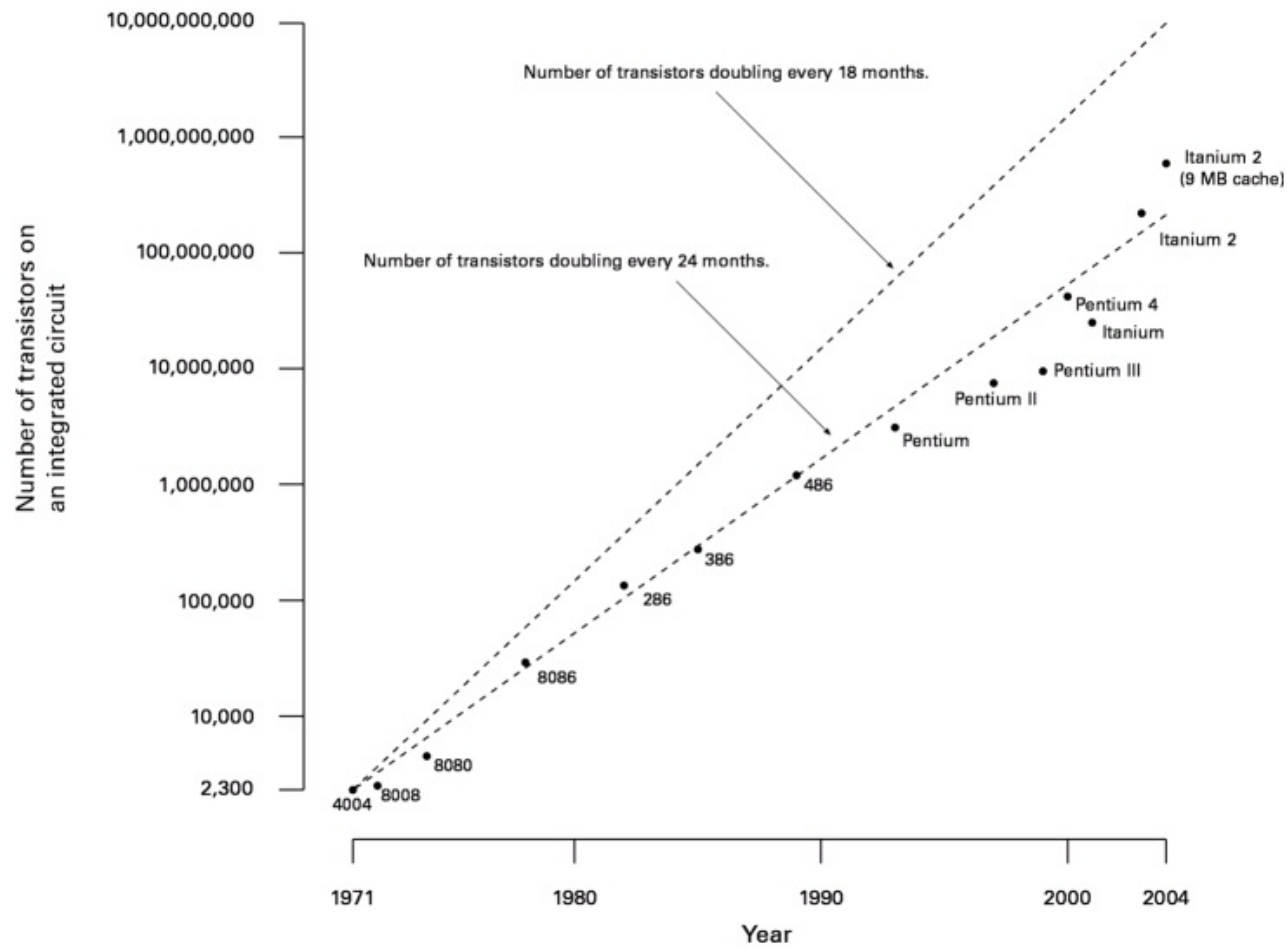
Fatoração de chave.

- 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



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

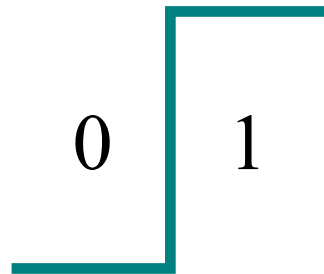


**Peter Shor (1994): algoritmo quântico eficiente
para decomposição em fatores primos**

Computador clássico:

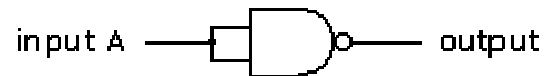
BIT

Dois estados possíveis

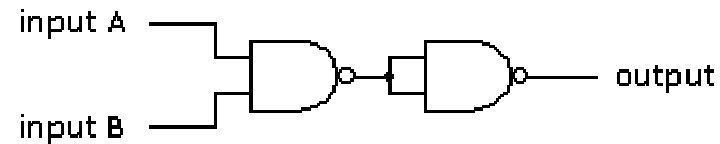


Portas lógicas

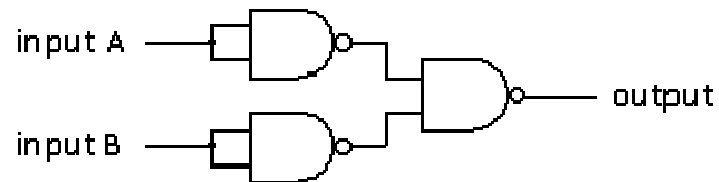
NOT gate (inputs joined together)



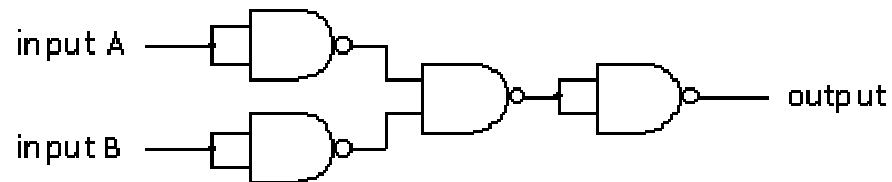
AND gate (NAND followed by NOT)



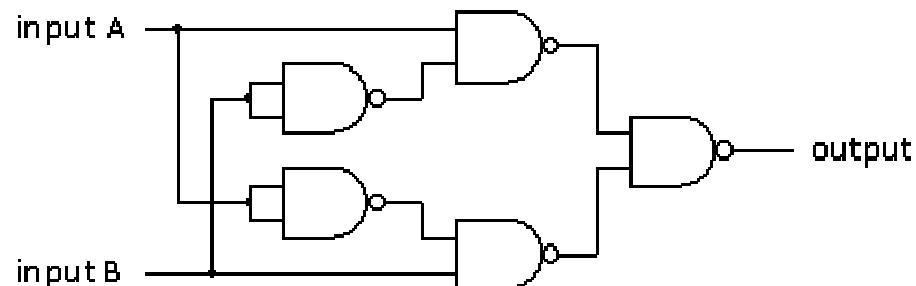
OR gate (NOT of each input followed by NAND)

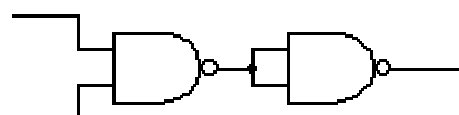


NOR gate (OR followed by NOT)



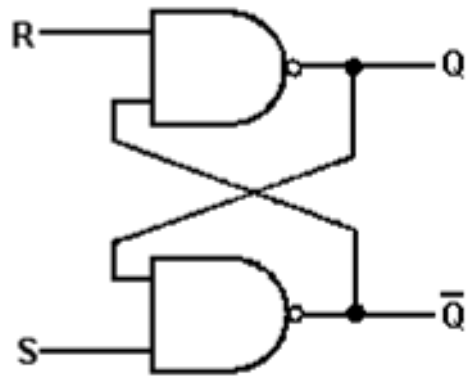
EXOR gate



Name	Graphic Symbol	Algebraic Function	Truth Table															
AND gate (NAND followed by NOT)		$F = A \cdot B$ or $F = AB$	<table><tr><th>A</th><th>B</th><th>F</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>	A	B	F	0	0	0	0	1	0	1	0	0	1	1	1
A	B	F																
0	0	0																
0	1	0																
1	0	0																
1	1	1																
OR gate (NOR followed by NOT)		$F = A + B$	<table><tr><th>A</th><th>B</th><th>F</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>	A	B	F	0	0	0	0	1	1	1	0	1	1	1	1
A	B	F																
0	0	0																
0	1	1																
1	0	1																
1	1	1																
NOT gate		$F = \bar{A}$ or $F = A'$	<table><tr><th>A</th><th>F</th></tr><tr><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td></tr></table>	A	F	0	1	1	0									
A	F																	
0	1																	
1	0																	
NAND gate		$F = (\overline{AB})$	<table><tr><th>A</th><th>B</th><th>F</th></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>	A	B	F	0	0	1	0	1	1	1	0	1	1	1	0
A	B	F																
0	0	1																
0	1	1																
1	0	1																
1	1	0																
NOR gate		$F = \overline{(A + B)}$	<table><tr><th>A</th><th>B</th><th>F</th></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>	A	B	F	0	0	1	0	1	0	1	0	0	1	1	0
A	B	F																
0	0	1																
0	1	0																
1	0	0																
1	1	0																

Registradores (memórias)

Estáticas



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

The R-S flip.flop

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

Dinâmicas

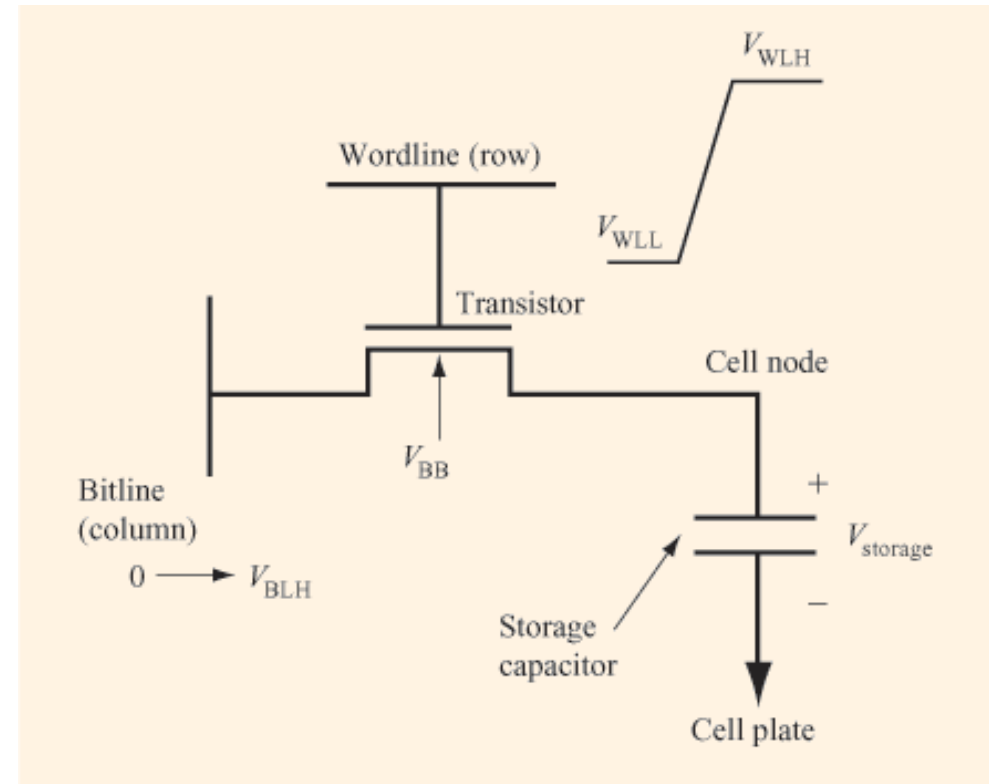
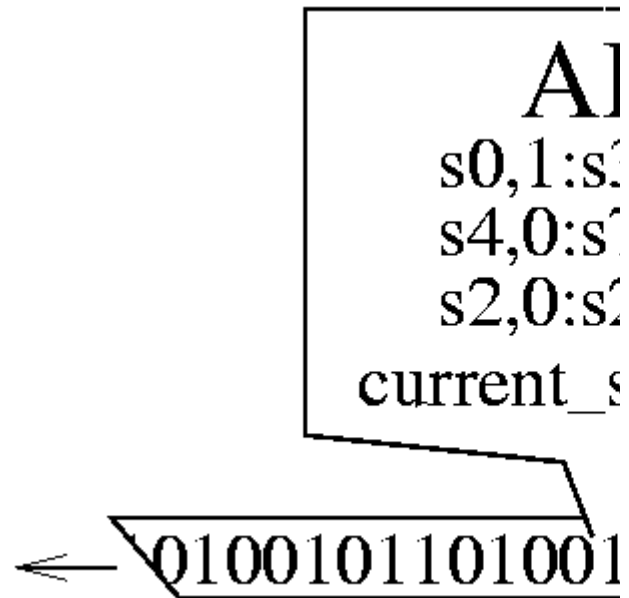


Figure 1

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

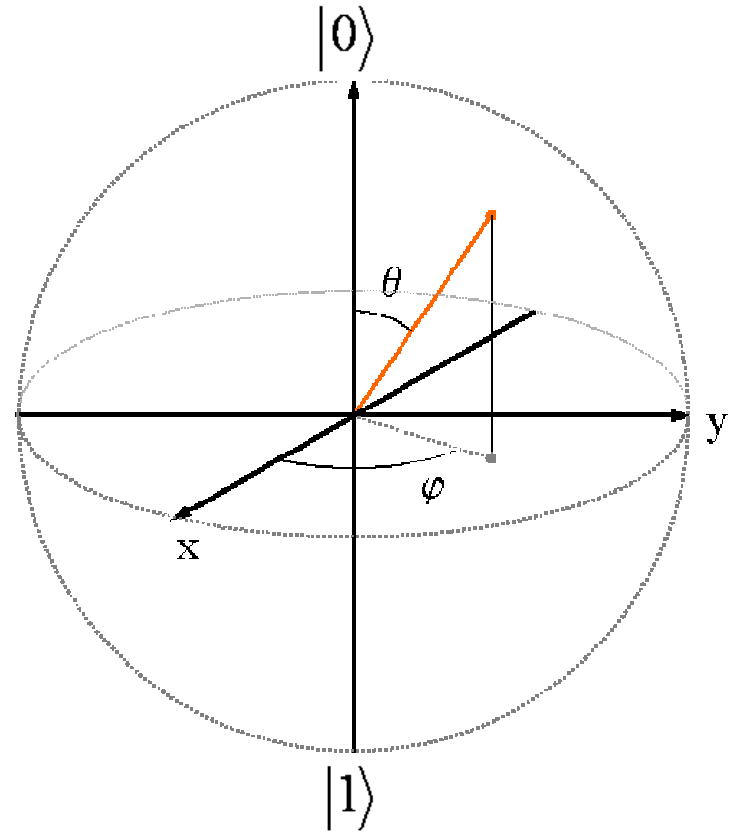
Qubit

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

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

Representação Matricial

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



Portas lógicas

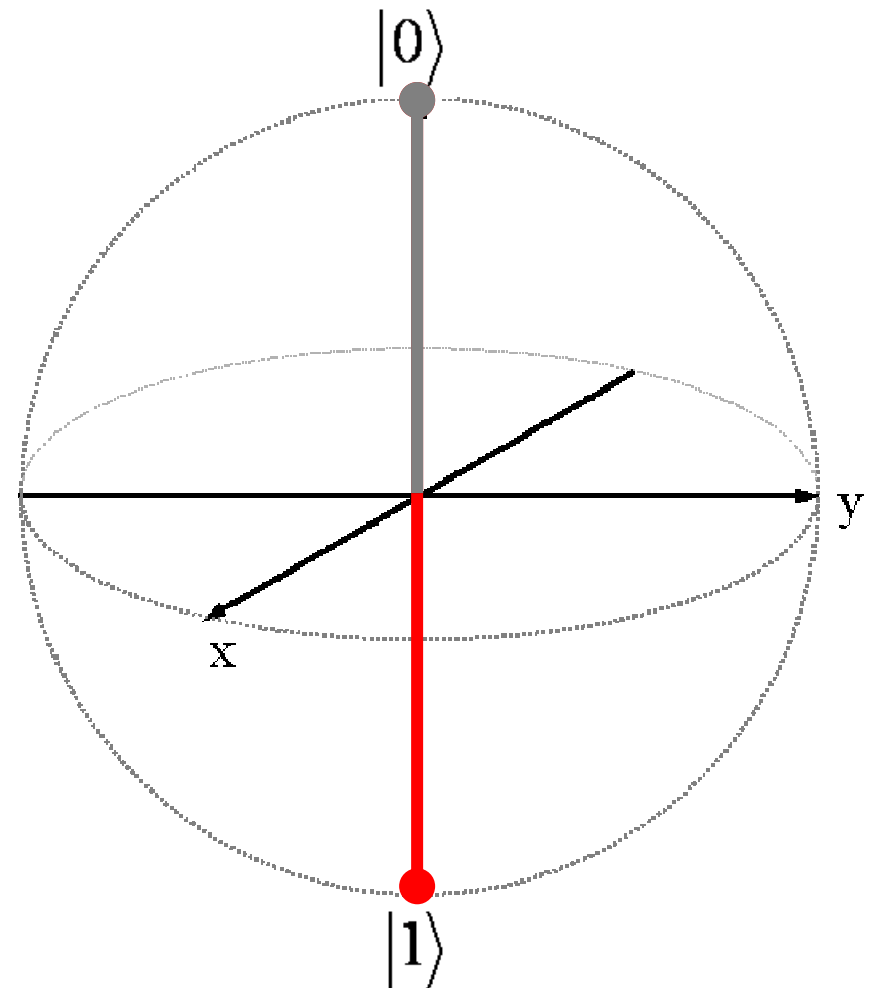
- Reversíveis
- Transformação unitária

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

$$U^\dagger U = I$$

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

$$\alpha|0\rangle + \beta|1\rangle \quad \boxed{X} \quad \beta|0\rangle + \alpha|1\rangle$$



Portas lógicas

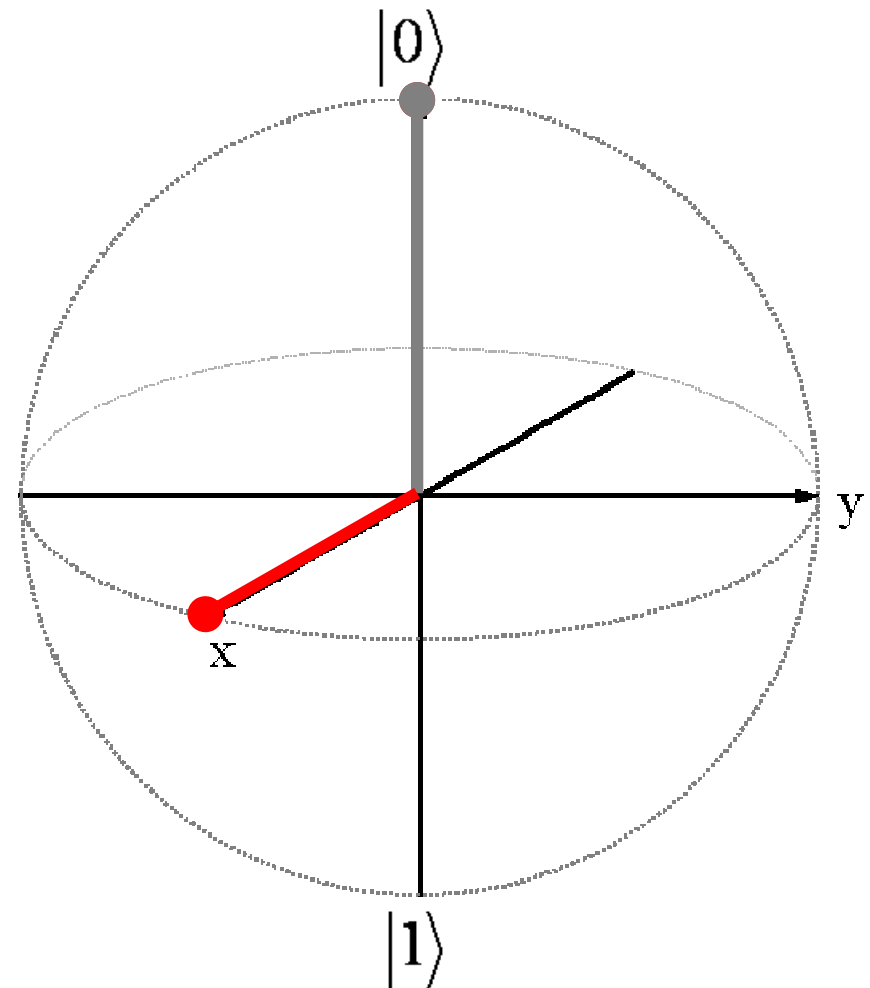
- Reversíveis
- Transformação unitária

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

$$U^\dagger U = I$$

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

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



Portas lógicas

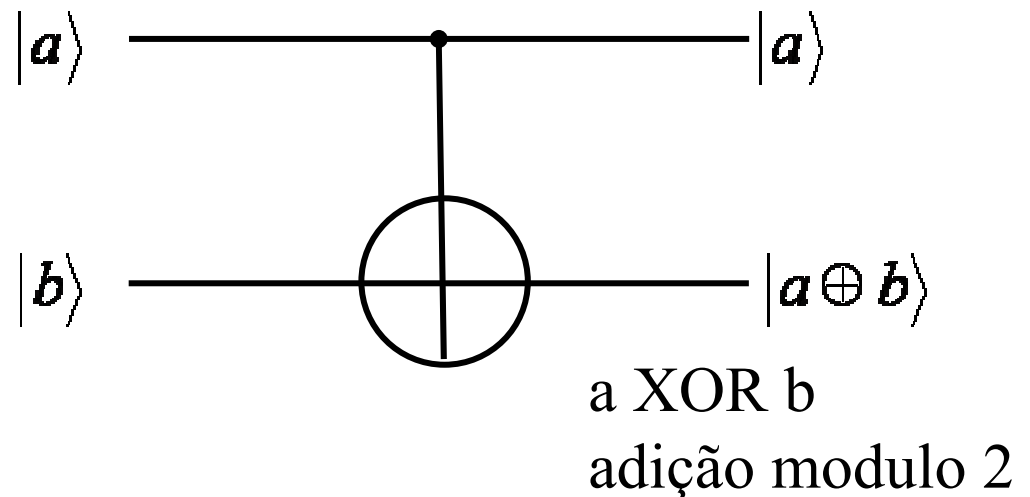
Controlled-Not

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

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

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

Podemos criar estados inseparáveis no resultado (superposição $\rightarrow$ emaranhamento)



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

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

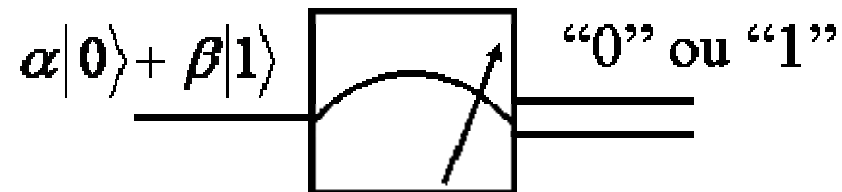
$$\Rightarrow |\Psi_o\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Medidas

A medida projeta o estado em uma base.

Exemplo: Polarizador

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

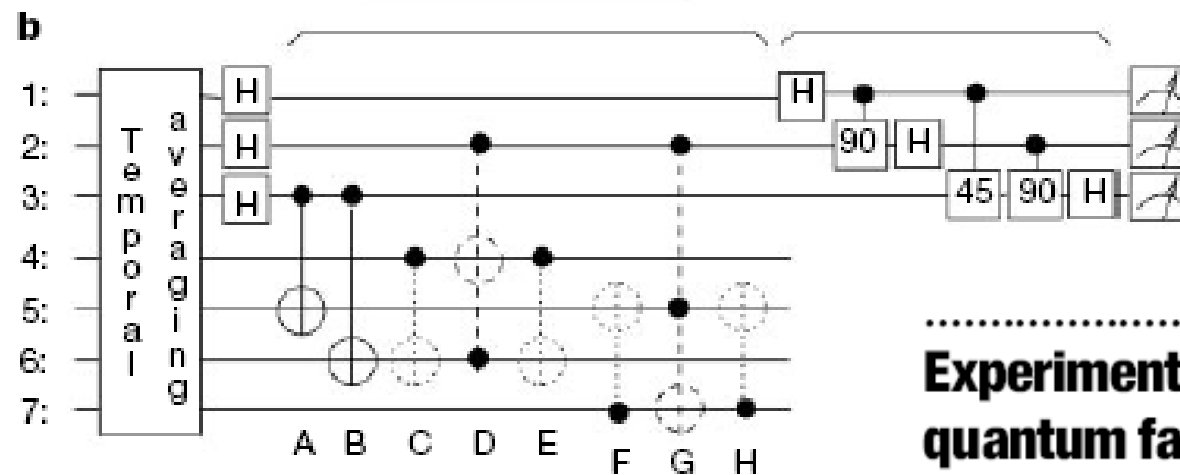
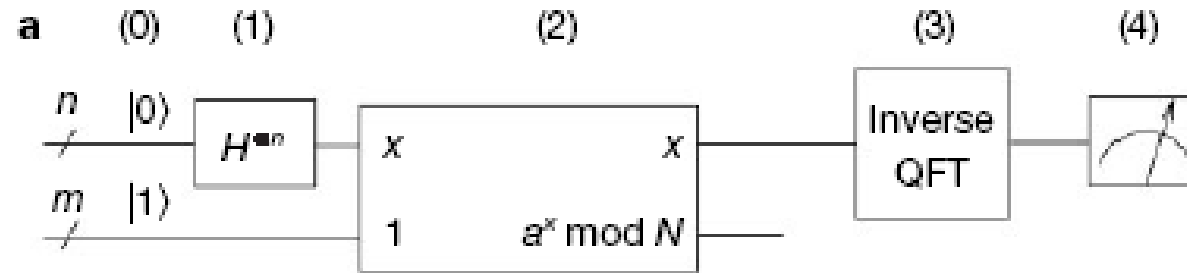


Resultado de uma medida é NECESSARIAMENTE um AUTOVALOR do observável (operador) sendo medido.

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...



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

Fatorar $N=15$...

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

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.

Exemplo famoso: o paradoxo do(a) “Gato(a) de Schrödinger” (1935). Por que não observamos superposições de estados no mundo macroscópico (clássico)?



O problema da descoerência

PROCURADO



Vivo E Morto



Criptografia quântica

Bennett e Brassard em 1984 (BB84)

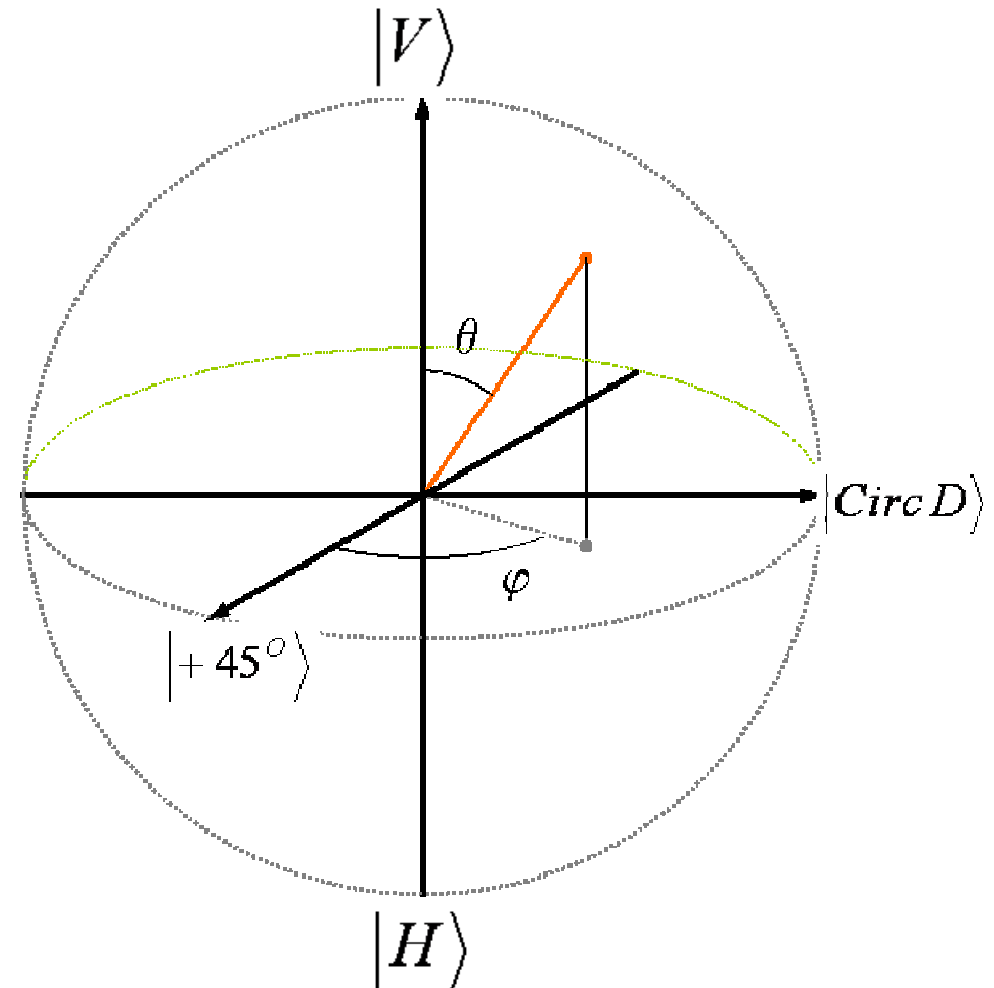


Artur Ekert em 1991
(emaranhamento)



Medidas em MQ - um pouco de formalismo

- Ouvimos falar muito que o observador perturba a medida em MQ. Como isso acontece?
- Função de onda $\psi \rightarrow$ VETOR DE ESTADO $|\psi\rangle$
OBSERVÁVEIS $\rightarrow$ OPERADORES (matrizes)
- Exemplos com estados de polarização da luz (sistemas de dois níveis em geral).
POLARIZADOR: filtro de polarização, só permite a passagem de uma componente de polarização.



Medidas de Polarização

- Polarizador serve como instrumento de medida. Como representar medida de polarização H?

$$A_H = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \rightarrow \text{observável}$$

Autovalores e autovetores

$$1: |H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad 0: |V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

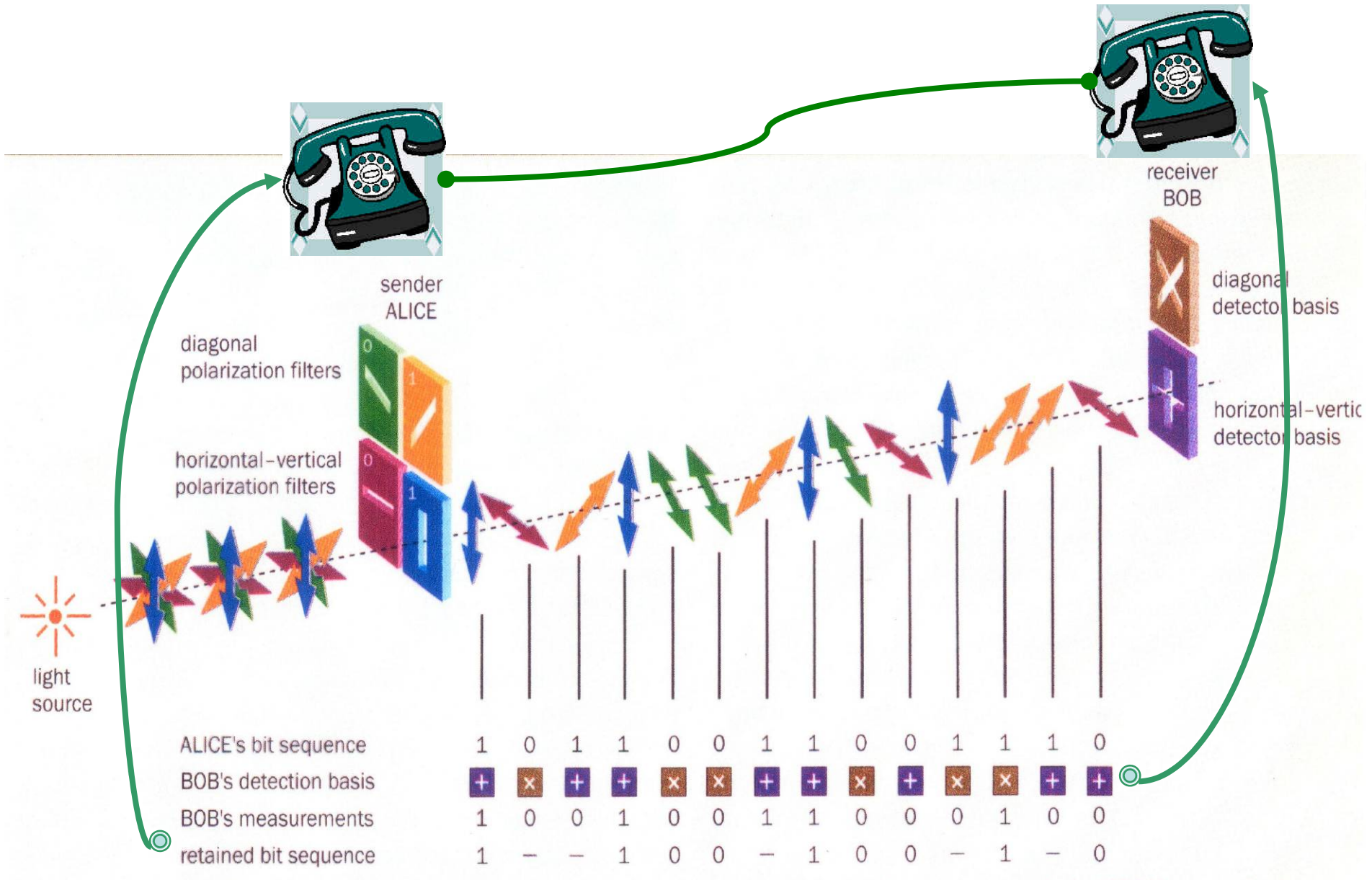
• REGRAS QUÂNTICAS

- 1) Resultado de uma medida é NECESSARIAMENTE um AUTOVALOR do observável (operador) sendo medido.
- 2) Medida é equivalente a PREPARAR um estado: após a medida de um autovalor, o estado do sistema é o autovetor (auto-estado) correspondente.

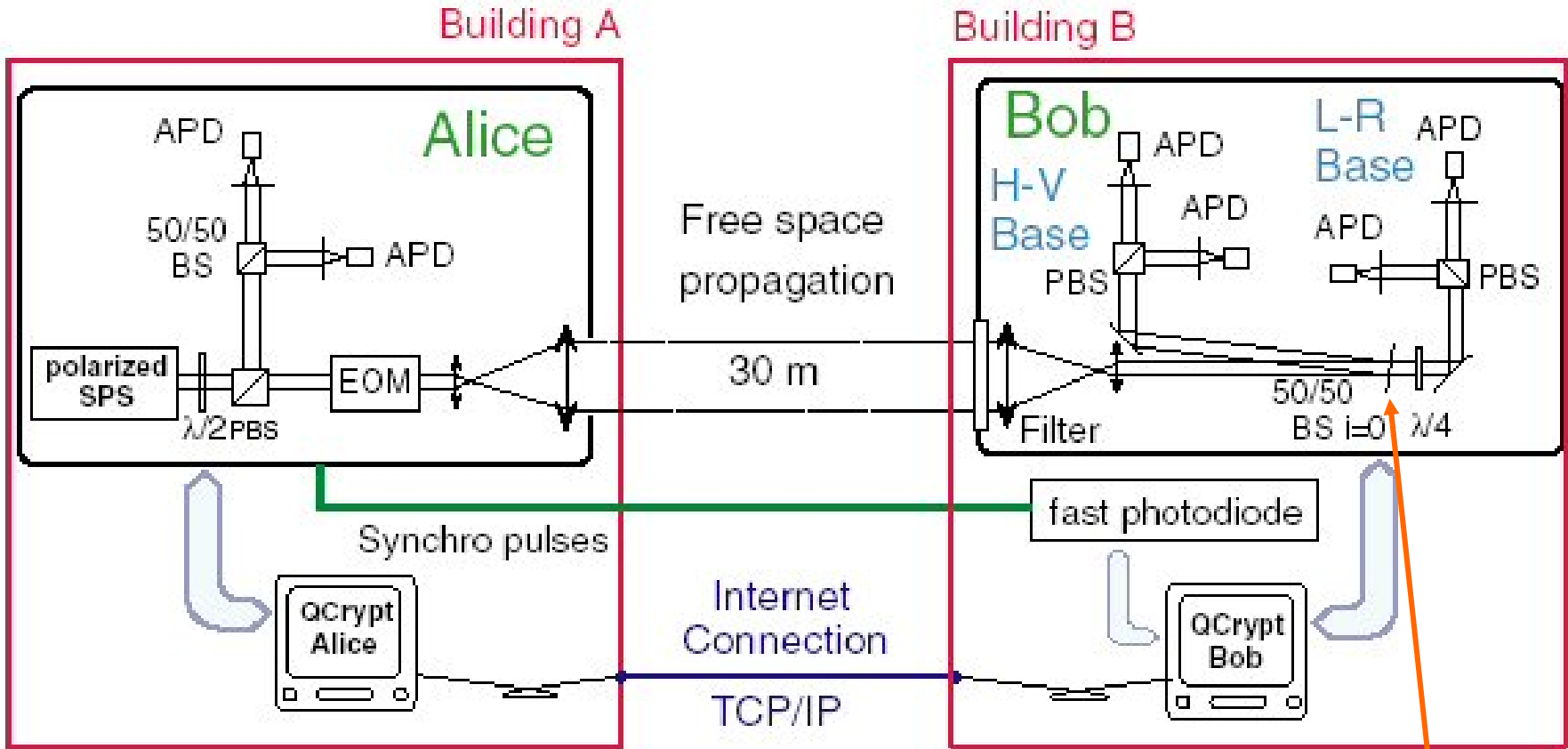
• PRINCÍPIO DE INCERTEZA DE HEISENBERG

→ impossibilidade de se medir, com precisão absoluta, simultaneamente duas grandezas cujos OPERADORES NÃO COMUTAM

BB84 - O canal quântico



Aparato para BB84



Lab. do Prof. Ph. Grangier, Orsay

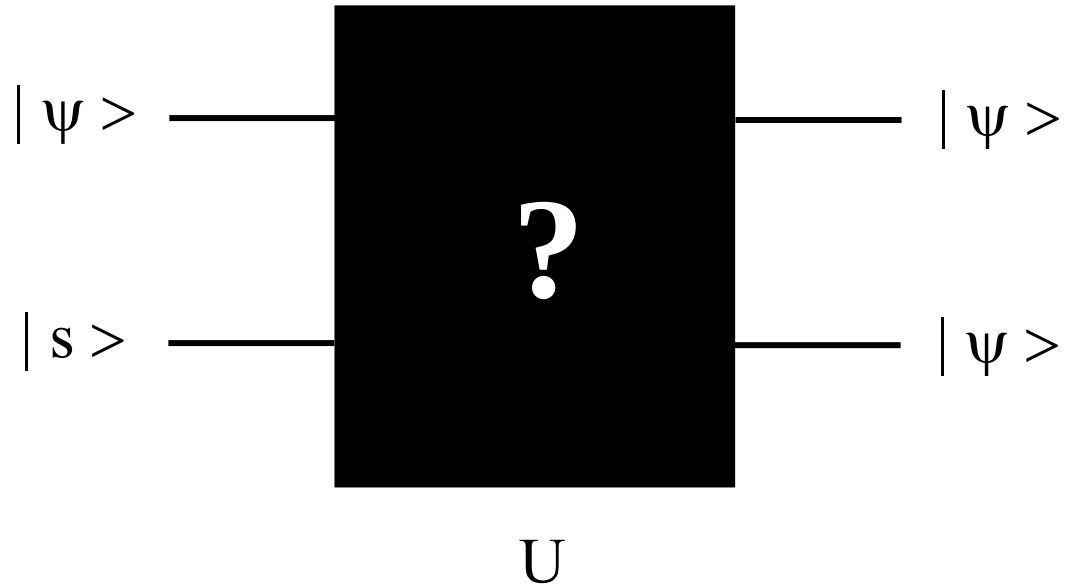
RND #

É possível construir uma “copiadora” quântica?

Clássico



Quântico?



$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \quad \Rightarrow \langle \phi | \psi \rangle \langle s | s \rangle = (\langle \phi | \psi \rangle)^2$$

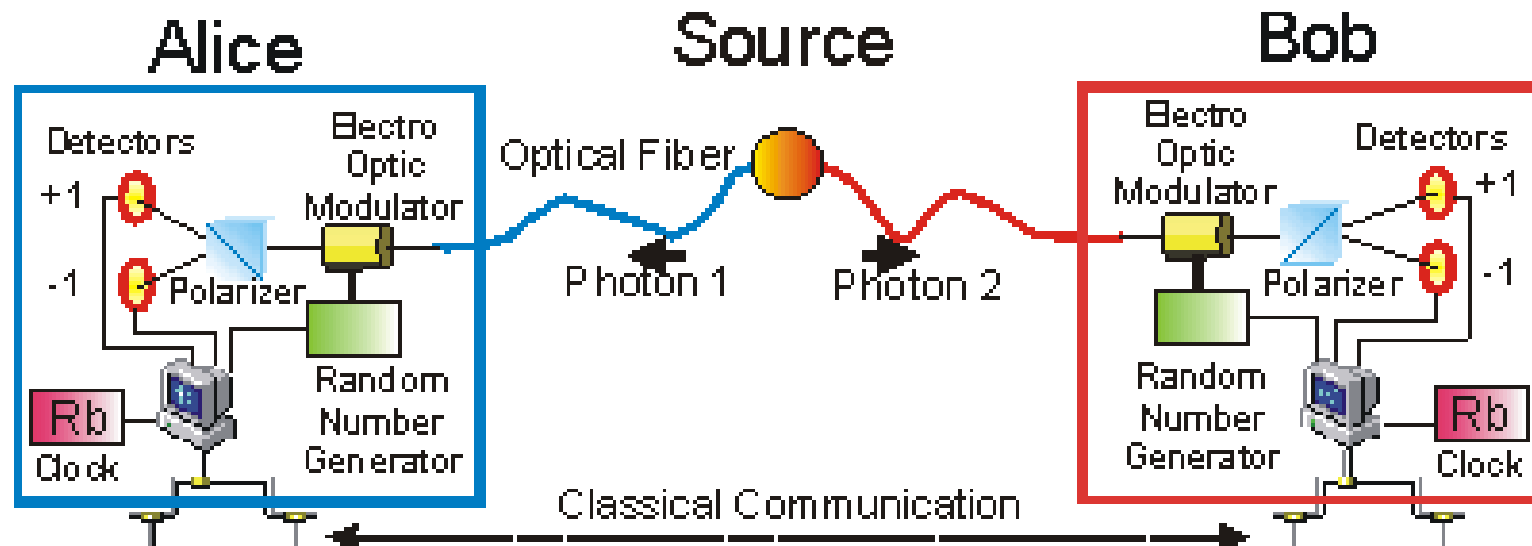
$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle$$

$$\Rightarrow \langle \phi | \psi \rangle = (\langle \phi | \psi \rangle)^2 \Rightarrow \langle \phi | \psi \rangle = 0 \text{ ou } 1$$

- Impossibilidade de “clonar” um bit é um resultado fundamental da Mecânica Quântica e uma das diferenças em relação à Mecânica Clássica. Resultado é consistente com o princípio de incerteza (noção de que a medida introduz, em geral, uma perturbação no sistema). É um dos ingredientes essenciais para o aumento de segurança na *criptografia quântica*.

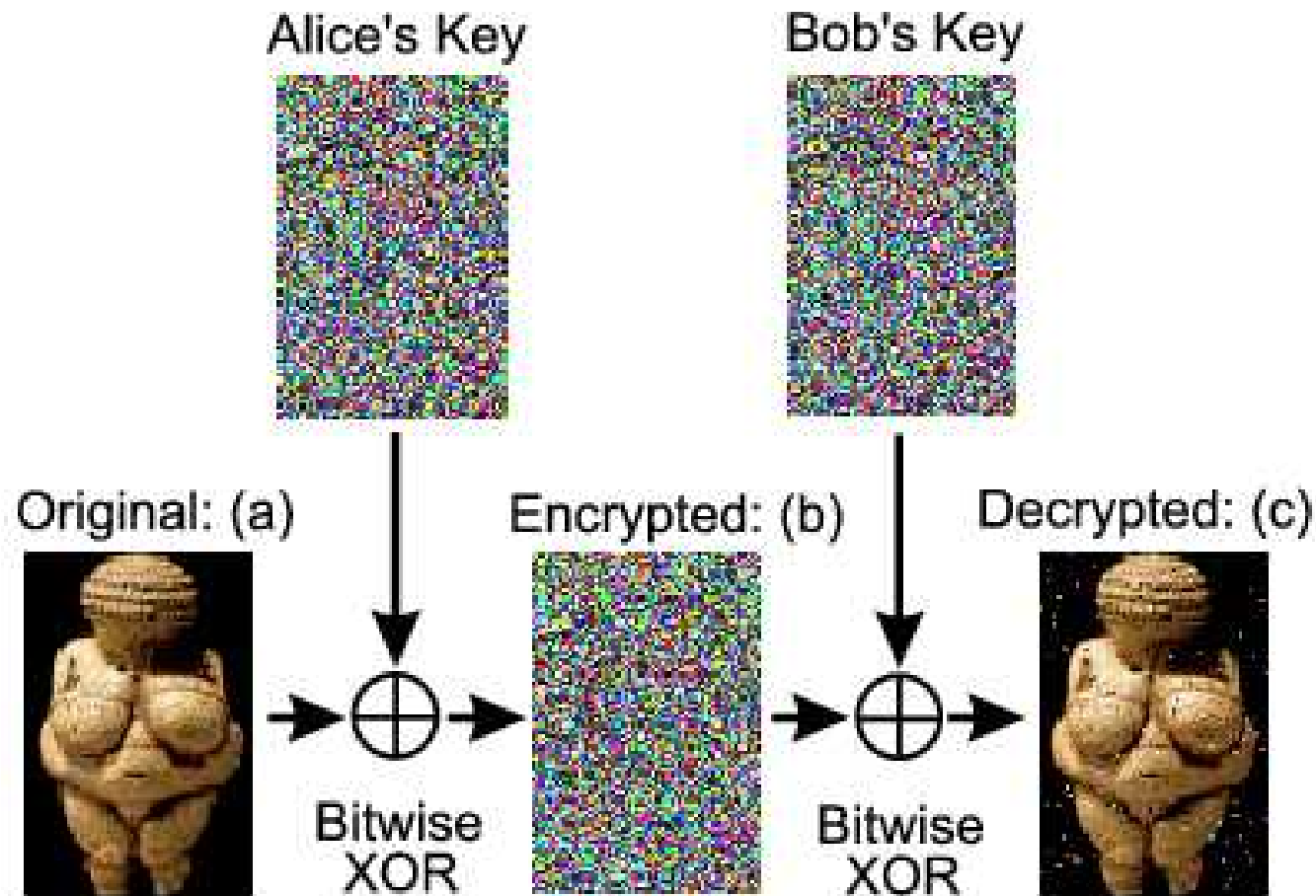
- A Mecânica Quântica tem outro “recurso” que não está disponível na Mecânica Clássica: a possibilidade de haver *emaranhamento* entre partículas distintas, gerando correlações não-locais. A inexistência desse recurso no “mundo” clássico é demonstrada pela violação de desigualdades de Bell.

Criptografia Quântica com fótons emaranhados



Alice e Bob recebem fótons de pares emaranhados em estados do tipo $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$
Eles fazem medidas de polarização variando aleatoriamente o eixo do polarizador. Comparando as direções por um canal clássico, conseguem extrair a “chave”.

Finalmente, Alice manda uma mensagem codificada a Bob através de um canal clássico: só ele pode ler, pois é o único a possuir a chave.



“Venus von Willendorf ”

T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000)



• **Main features**

- First commercial quantum key distribution system
- Key distribution distance: up to 60 km
- Key distribution rate: up to 1000 bits/s
- Compact and reliable

www.idquantique.com



Quantum Information Solutions for the Real World.

www.magiqtech.com



MagiQ QPN
QPN datasheet



Q-Box
Q-box datasheet

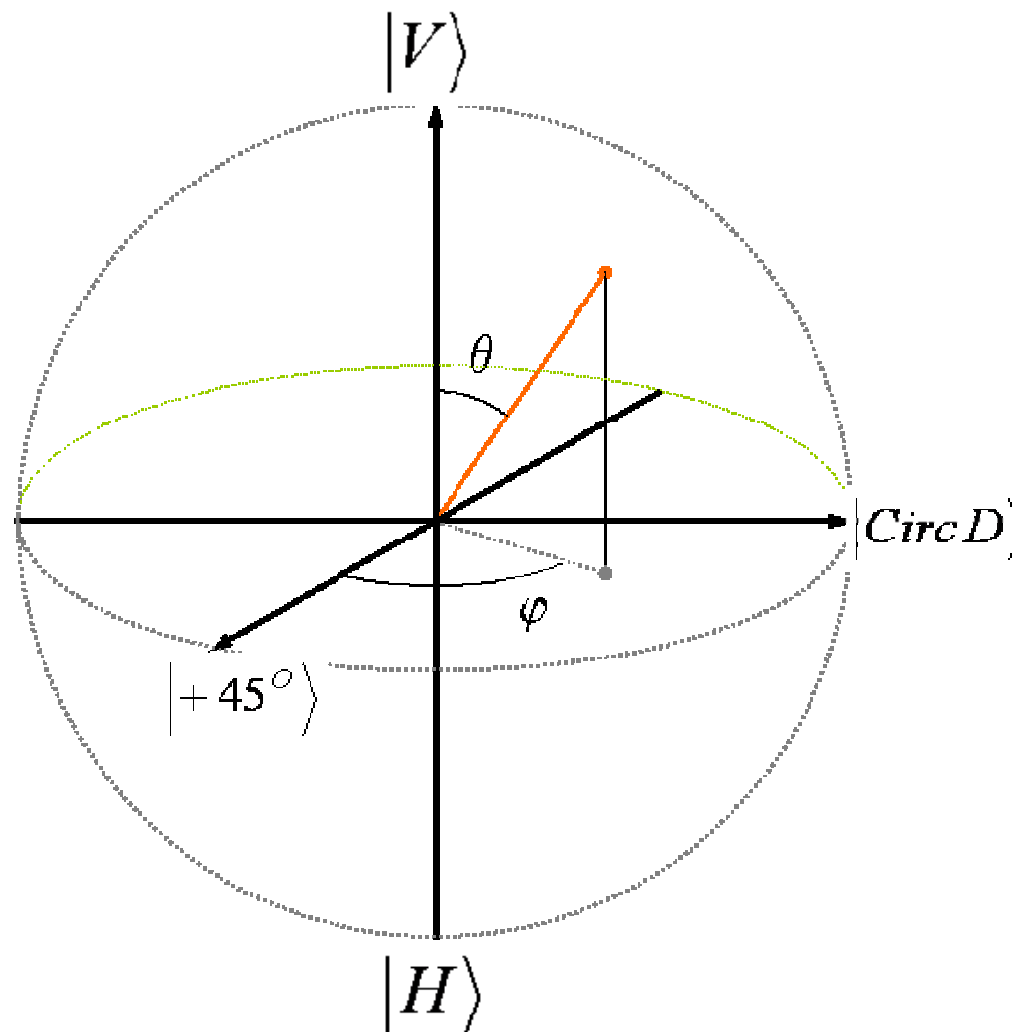
Presenting the **first**
commercial quantum
cryptography solutions.

**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

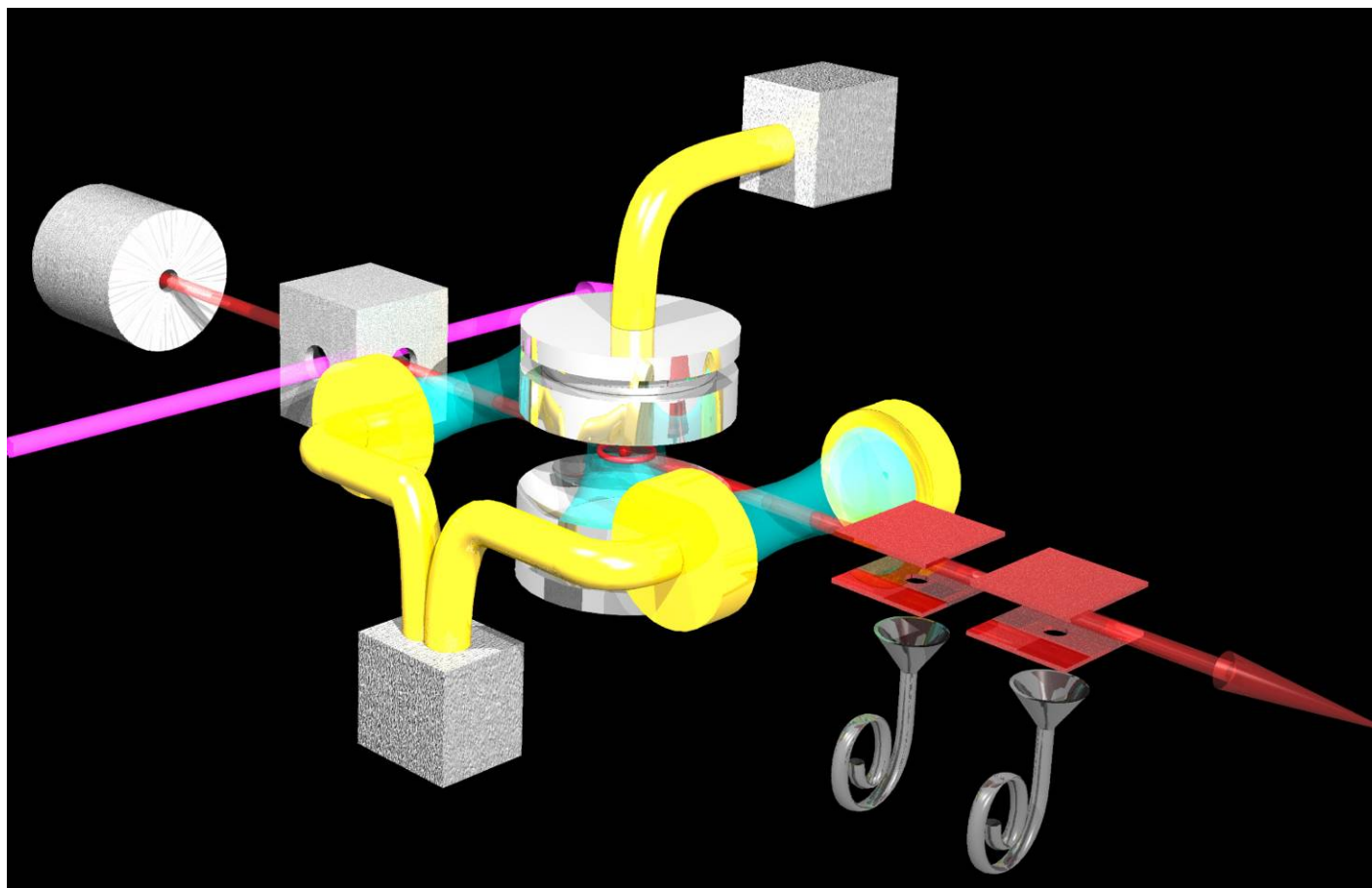
→ para múltiplos qubits (interação entre qubits → emaranhamento)

Ler o estado (medida) → Detetores

Descoerência

Estados atômicos e fótons em cavidades

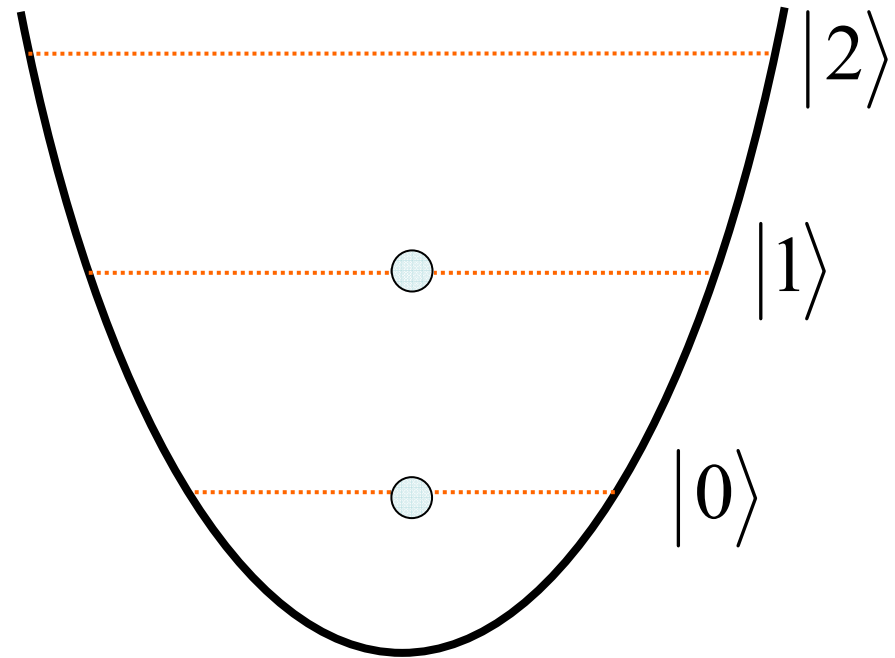
Exemplo:



Átomos e íons em potenciais quadráticos

Oscilador harmônico

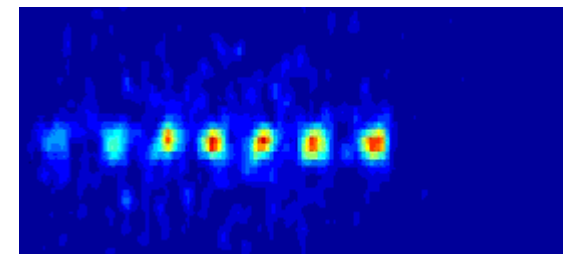
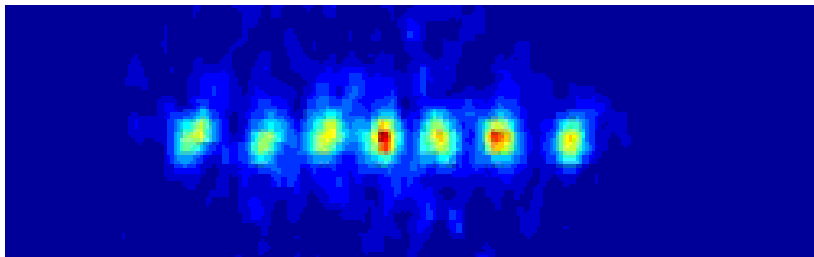
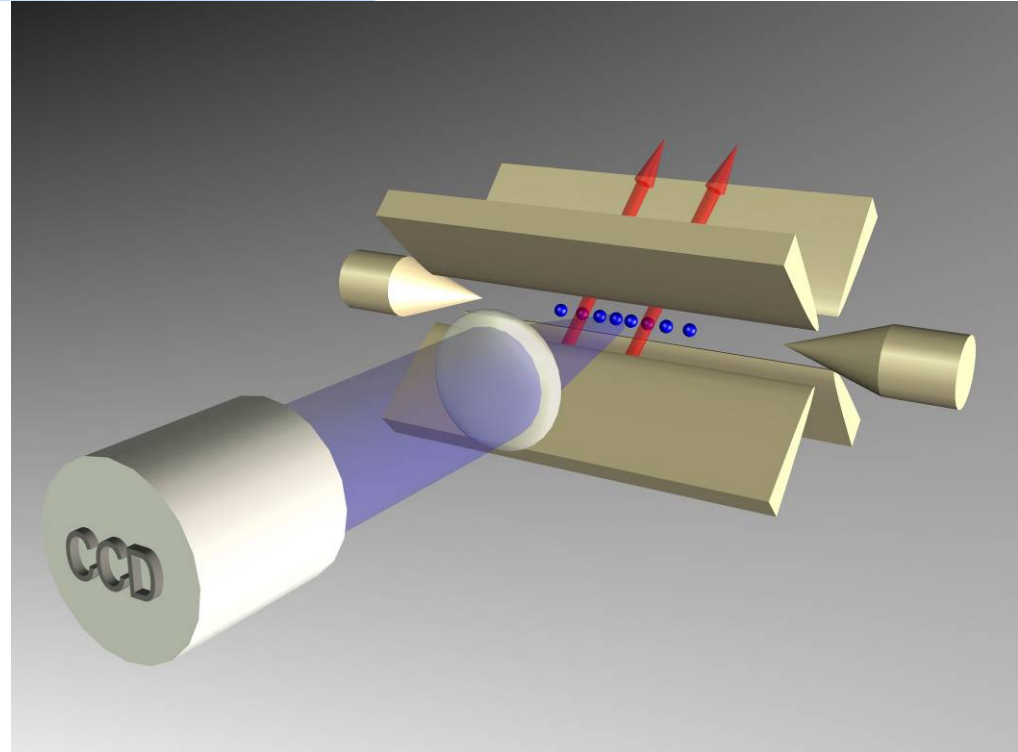
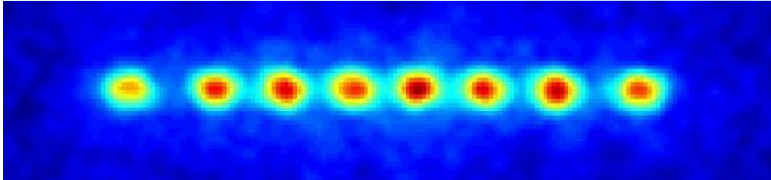
$$|\Psi\rangle = a|0\rangle + e^{i\omega t}b|1\rangle$$



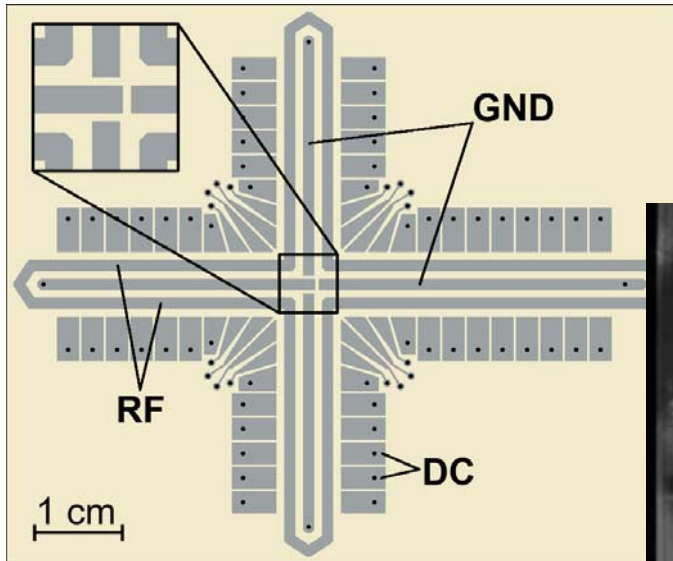
Quantum Optics and Spectroscopy

Institut für Experimentalphysik - Universität Innsbruck

Rainer Blatt



Quanta Group – MIT (Issac Chuang)



Para Saber Mais:

- ❑ O Livro dos Códigos (The Code Book); Simon Singh.
- ❑ Quantum Cryptography, N. Gisin, R. W. Tittel, H. Zbinden (Rev. Mod. Phys, **74**, 145 (2002).
- ❑ SSH Communications Security
(<http://www.ssh.com/support/cryptography/introduction/>)
- ❑ Seminários do Convite à Física (<http://fma.if.usp.br/convite/>)
 - Paulo Teotônio (Computação);
 - Luis Davidovitch (Decoerência);
 - Paulo Nussenzveig (EPR + Criptografia).