

Emaranhamento quântico e um novo paradigma para o processamento de informação



Quantum Information and Quantum Matter Group
www.iip.ufrn.br/qiqm

Rafael Chaves

ICTP-SAIFR Física em Casa
Setembro 2020



INCT-IQ
Instituto Nacional de Ciência e
Tecnologia de Informação Quântica



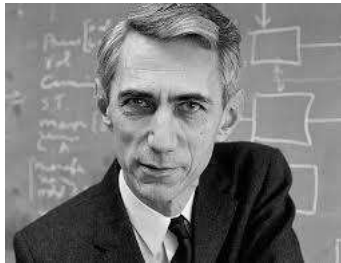
Vivemos na era da informação.





**Vivemos na era da informação.
Mas o que é informação?**

Vivemos na era da informação. Mas o que é informação?

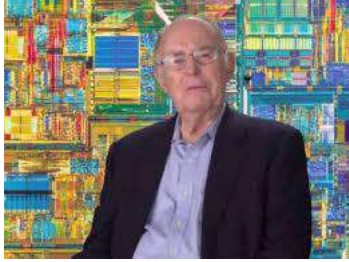


Claude Shannon



Informação é tanto a **incerteza** que temos sob um evento antes de observá-lo. Alternativamente, o **conhecimento** que obtemos ao realizar a observação.

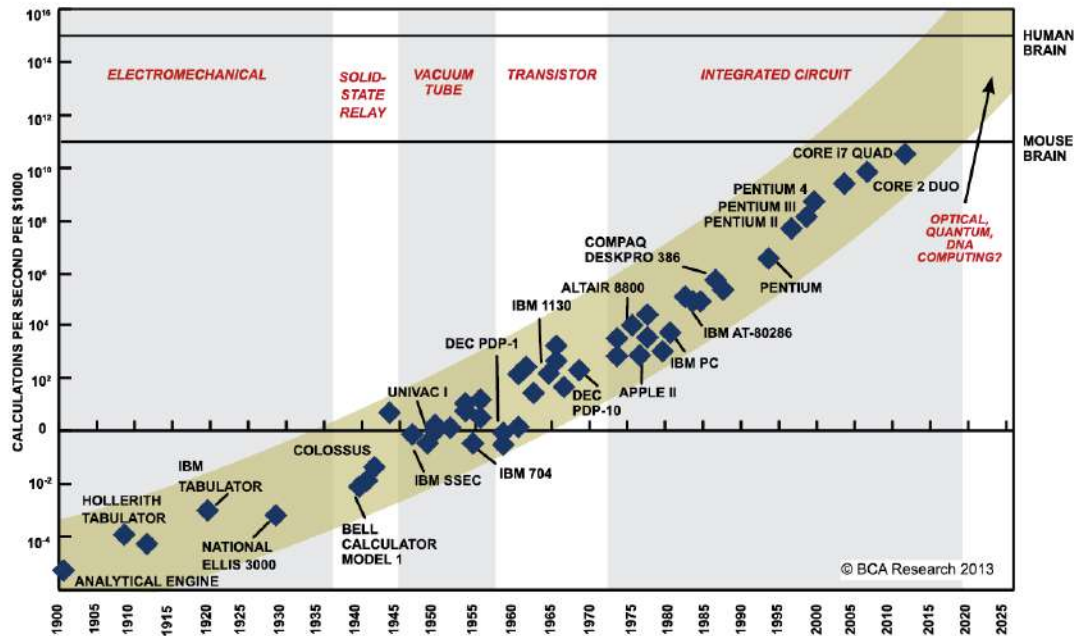
A informação é física...



Gordon Moore



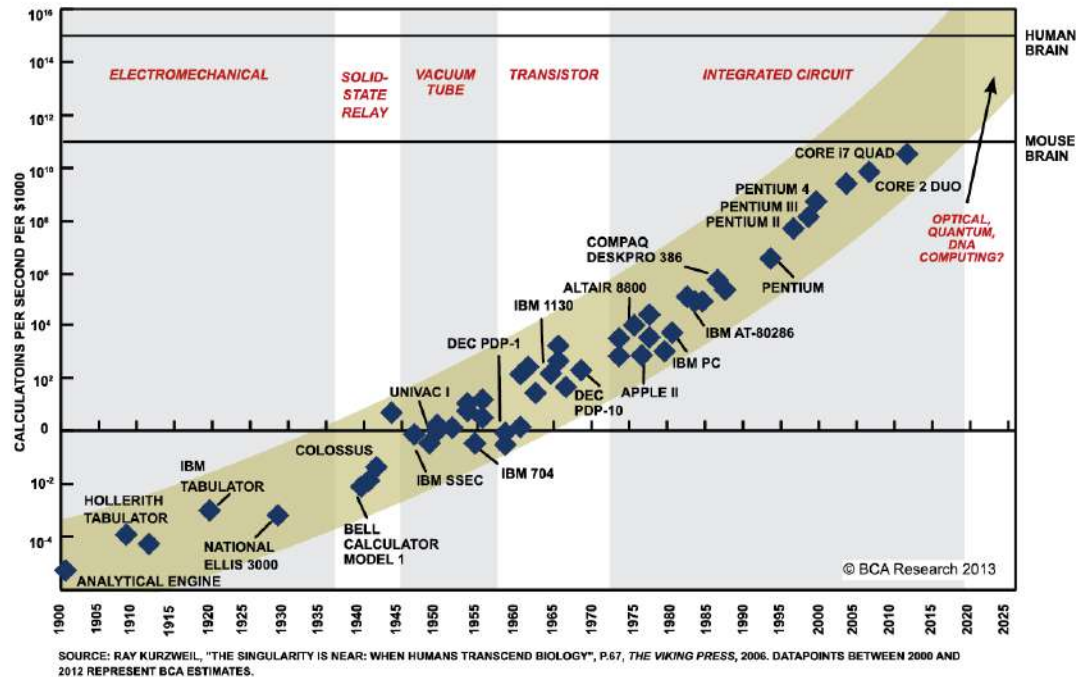
Rolf Landauer



SOURCE: RAY KURZWEIL, "THE SINGULARITY IS NEAR: WHEN HUMANS TRANSCEND BIOLOGY", P.67, THE VIKING PRESS, 2006. DATAPPOINTS BETWEEN 2000 AND 2012 REPRESENT BCA ESTIMATES.

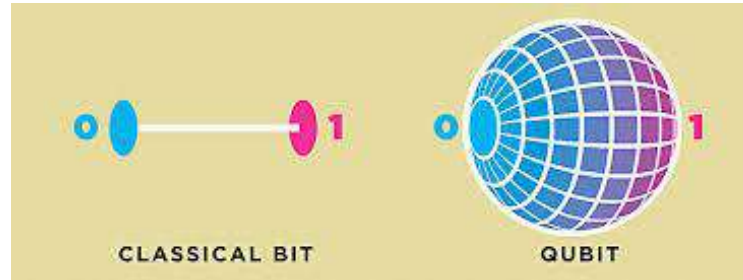
A informação é física...

No limite **quântico** temos **novas formas** de processar a informação.



A informação é física...

Novas formas para processar a informação.

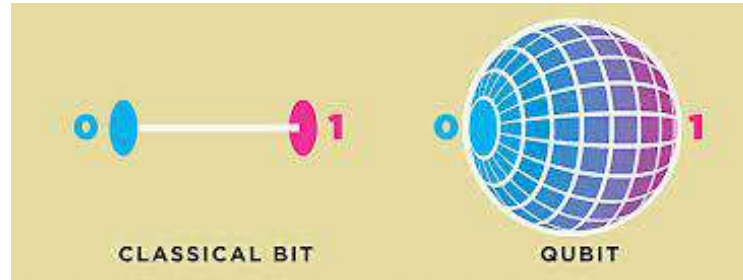


$$\alpha|0\rangle + \beta|1\rangle$$

Superposição

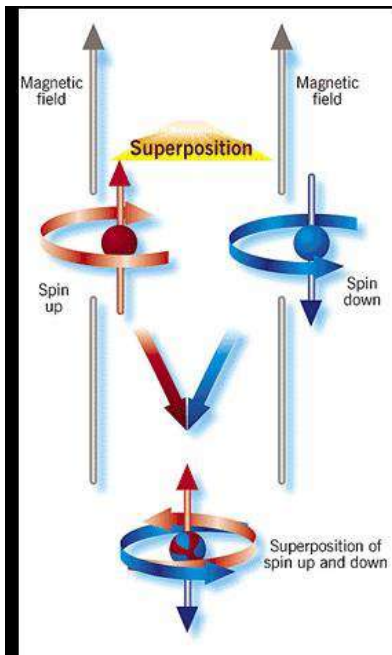
A informação é física...

Novas formas para processar a informação.



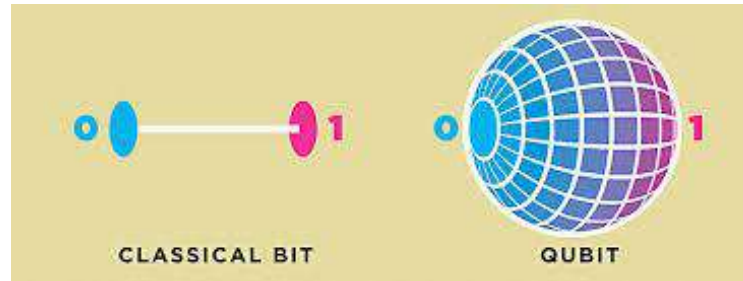
$$\alpha|0\rangle + \beta|1\rangle$$

Superposição



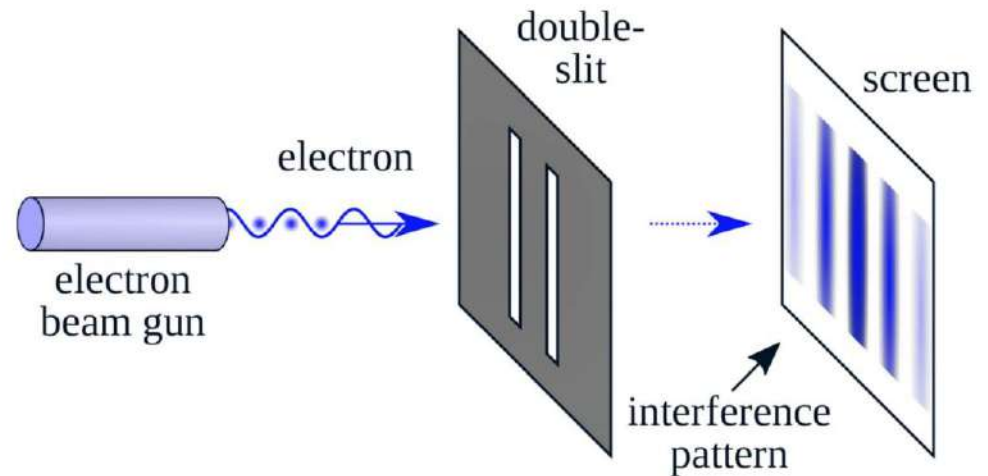
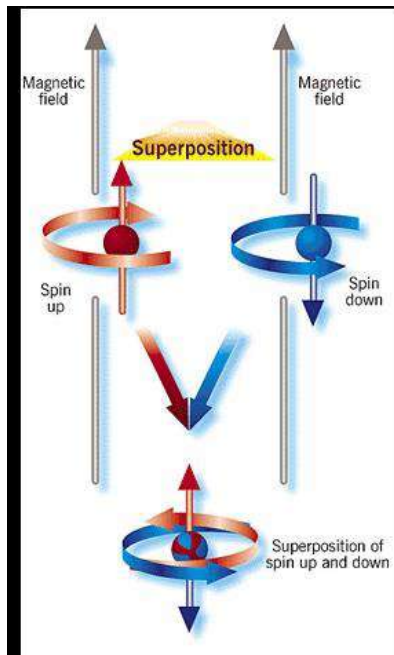
A informação é física...

Novas formas para processar a informação.



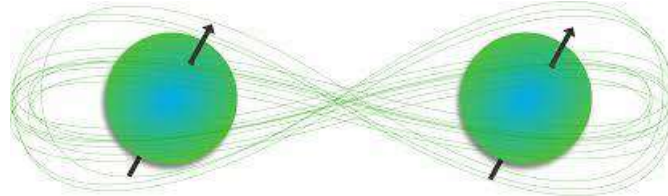
$$\alpha|0\rangle + \beta|1\rangle$$

Superposição



A informação é física...

Novas formas para processar a informação.

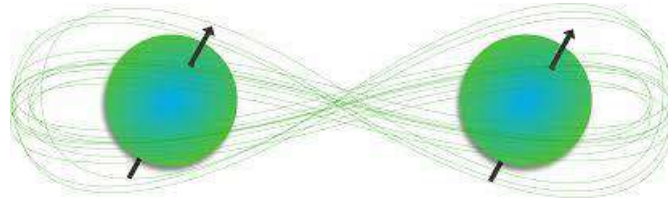


Emaranhamento

$$\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

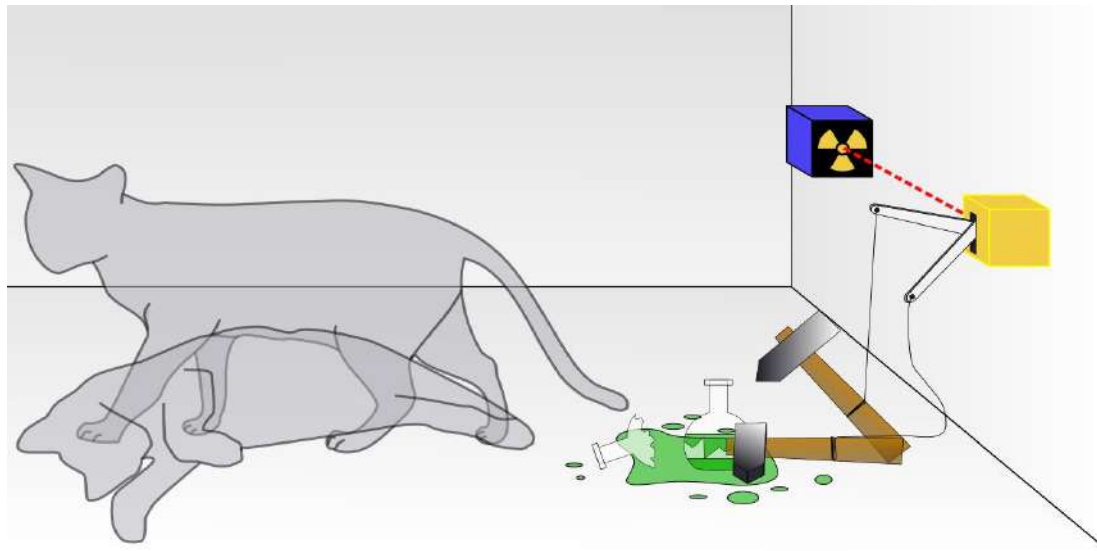
A informação é física...

Novas formas para processar a informação.



Emaranhamento

$$\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

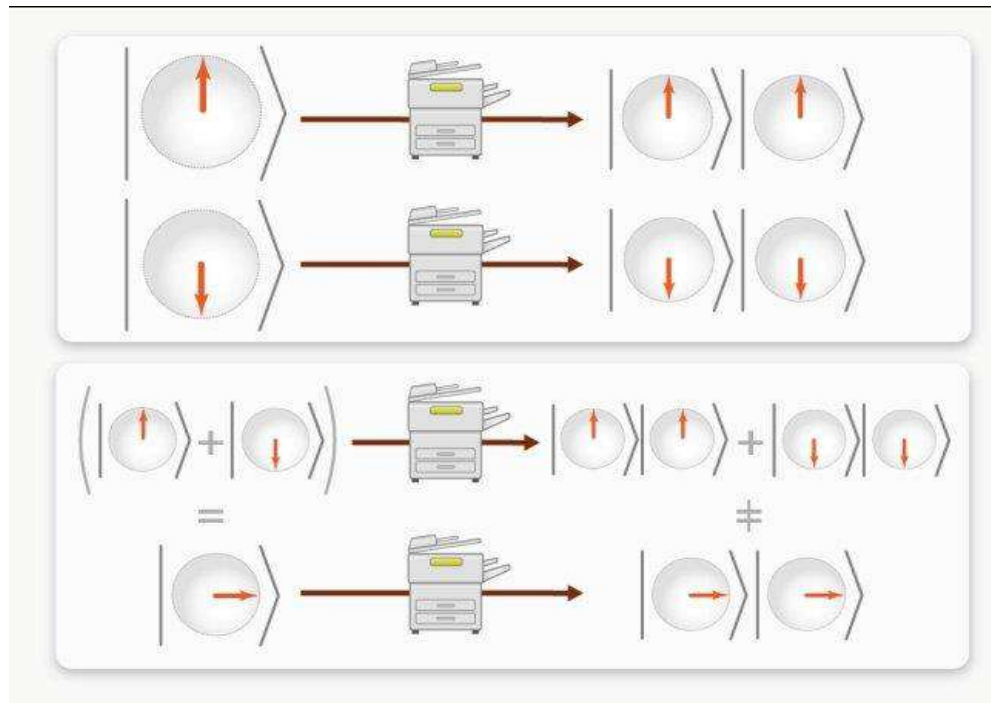


A informação é física...

Novas formas para processar a informação.



Não-Clonagem

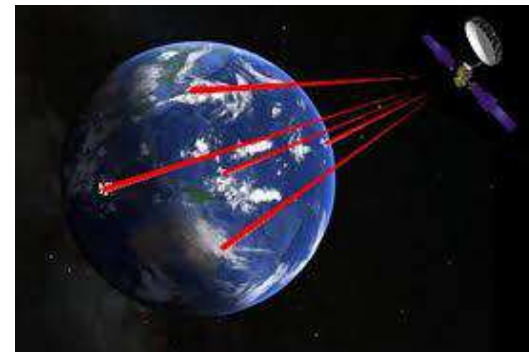


A informação e computação quântica são a ciência que busca entender como utilizar esses novos recursos e ao mesmo tempo contornar novos desafios que se impõe (decoerência).

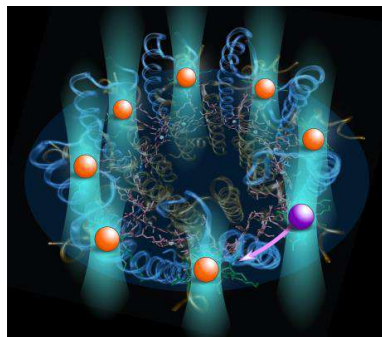
- Algoritmos quânticos



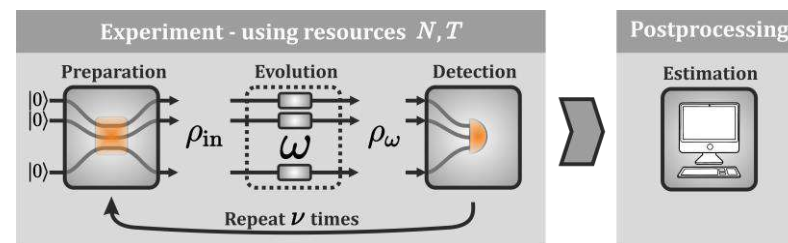
- Comunicação e Criptografia Quântica



- Simulação Quântica

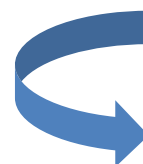


- Metrologia Quântica



Computação quântica: Algoritmo de Shor

Algoritmo eficiente para **fatorizar** números primos.



RSA, o algoritmo criptográfico padrão da internet, pode ser **quebrado** pelo algoritmo de Shor!

Comprimento do número a ser fatorado (em bits)	Tempo de fatora��o por algoritmo cl��ssico	Tempo de fatora��o com o algoritmo de Shor
512	4 dias	34 segundos
1024	100 mil anos	4,5 minutos
2048	100 mil bilh��es de anos	36 minutos
4096	100 bilh��es de quatrilh��es de anos	4,8 horas

Peter Shor



18819881292060796383869723946165043
98071635633794173827007633564229888
59715234665485319060606504743045317
38801130339671619969232120573403187
9550656996221305168759307650257059

=

3980750864240649373971
2550055038649119906436
2342526708406385189575
946388957261768583317

×

4727721461074353025362
2307197304822463291469
5302097116459852171130
520711256363590397527

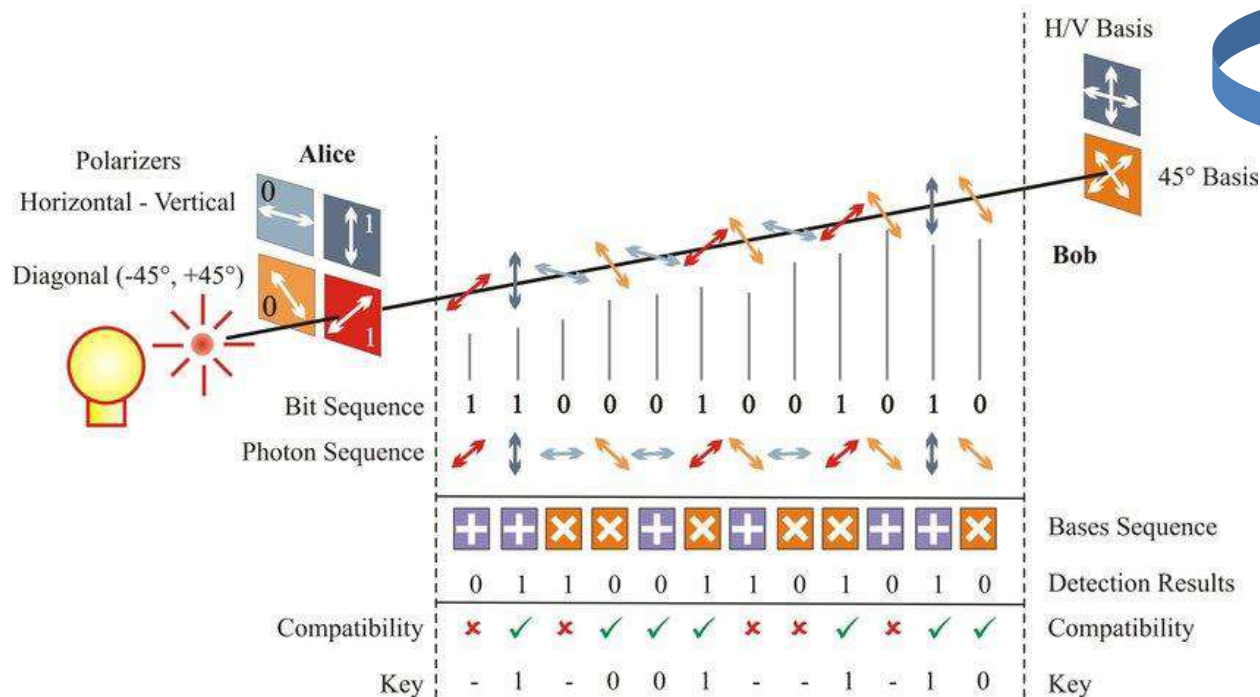
Best classical algorithm
takes time $O(\exp(n^{1/3}))$

Shor's quantum algorithm
takes time $O(n^3 \log n)$

Primeiro Protocolo de criptografia quântica: BB84

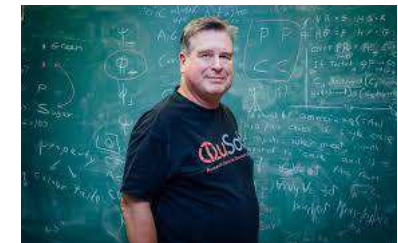


Charles Bennett



Segurança do **BB84** é baseada no teorema da não clonagem.

A presença de um **espião** pode ser detectada!



Gilles Brassard

Quantum Hackers!?



Vadim Makarov

Segurança do BB84 assume que o aparato de medição e de criação dos estados funcionam **perfeitamente**.



Falhas na implementação experimental abrem o caminho para **ataques**.

A mecânica quântica está completa!?



“Observações não somente **perturbam** o que vai ser medido, elas o produzem [...] Nós compelimos o elétron a assumir uma posição bem definida [...] Nós próprios **somos os responsáveis** por produzir os resultados das medições que observamos”

Pascual Jordan

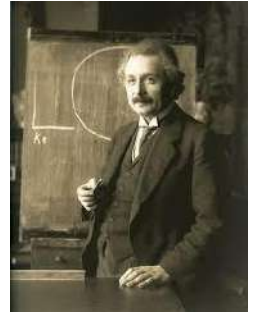
A mecânica quântica está completa!?



Pascual Jordan

“Observações não somente **perturbam** o que vai ser medido, elas o produzem [...] Nós compelimos o elétron a assumir uma posição bem definida [...] Nós próprios **somos os responsáveis** por produzir os resultados das medições que observamos”

“Você realmente acredita que a Lua só **existe** quando **olhamos** para ela?”



Albert Einstein



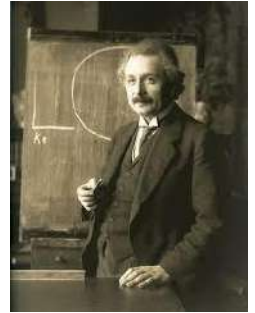
A mecânica quântica está completa!?



Pascual Jordan

“Observações não somente **perturbam** o que vai ser medido, elas o produzem [...] Nós compelimos o elétron a assumir uma posição bem definida [...] Nós próprios **somos os responsáveis** por produzir os resultados das medições que observamos”

“Você realmente acredita que a Lua só **existe** quando **olhamos** para ela?”



Albert Einstein

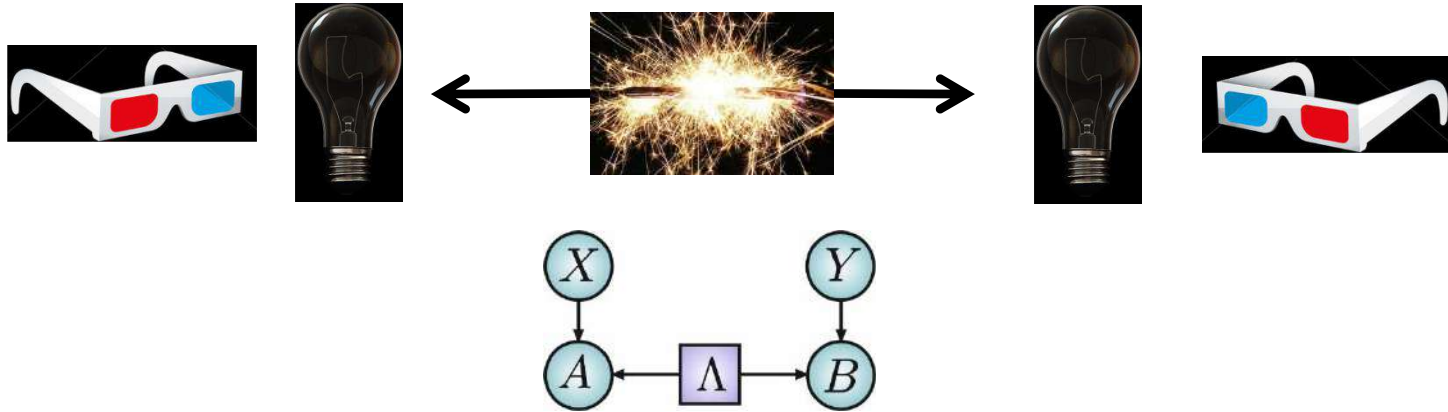


The New York Times.

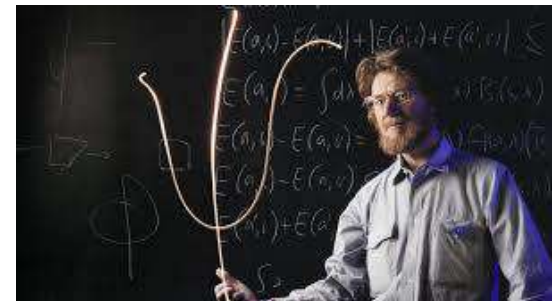
EINSTEIN ATTACKS QUANTUM THEORY

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

Teorema de Bell

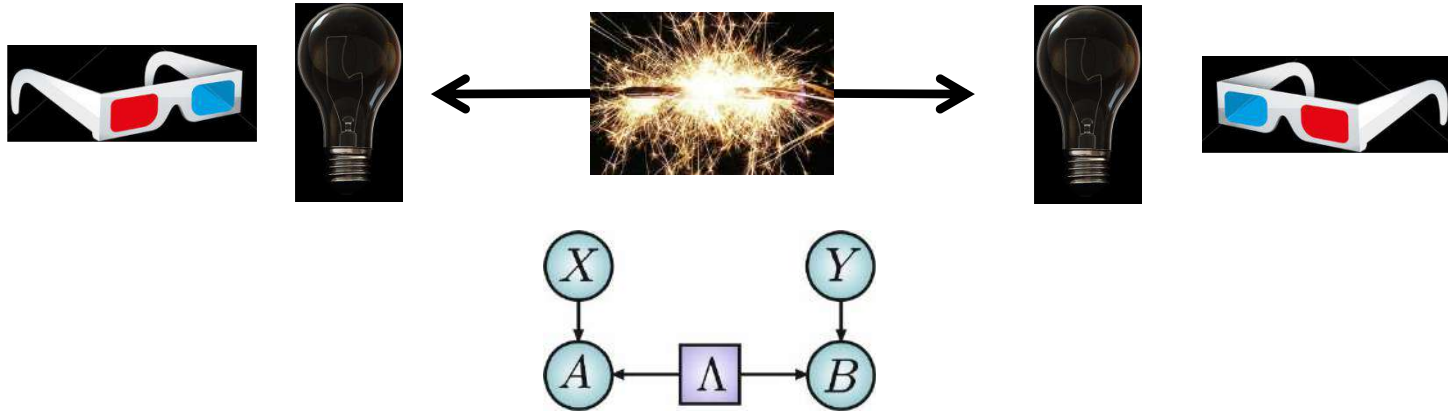


- Alice e Bob medem dois possíveis observáveis cada: A_0 , A_1 , B_0 , B_1

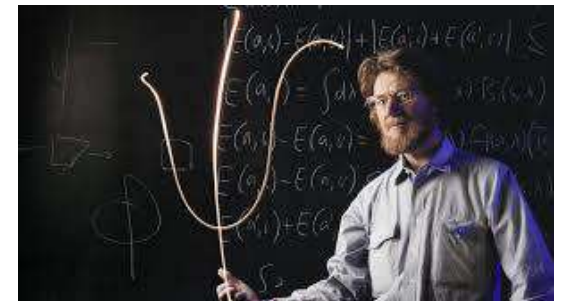


John Bell

Teorema de Bell

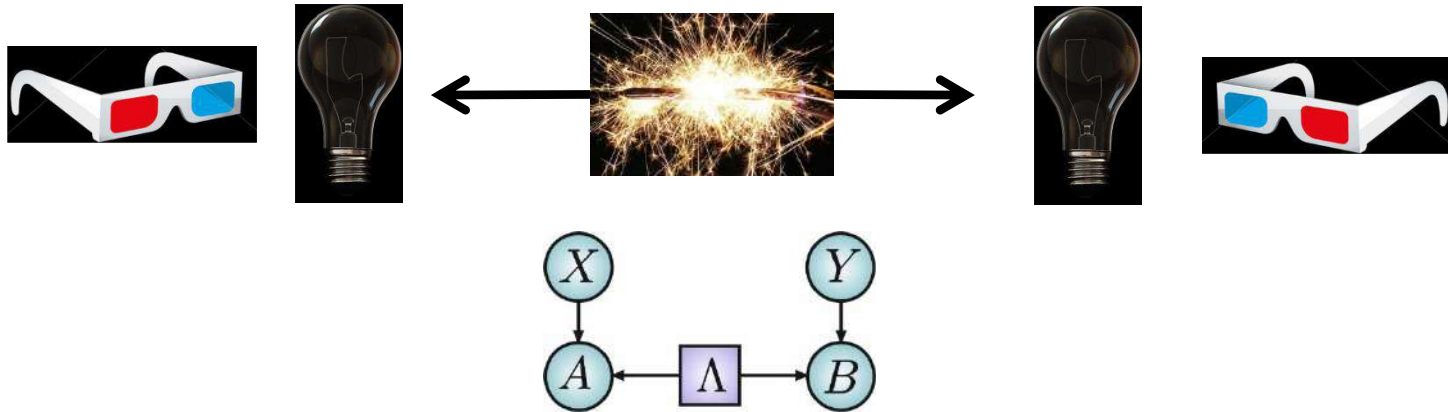


- Alice e Bob medem dois possíveis observáveis cada: A_0, A_1, B_0, B_1
- Após um número suficiente de medições eles podem estimar quantidades estatísticas. O experimento é descrito em termos de $p(a, b|x, y)$



John Bell

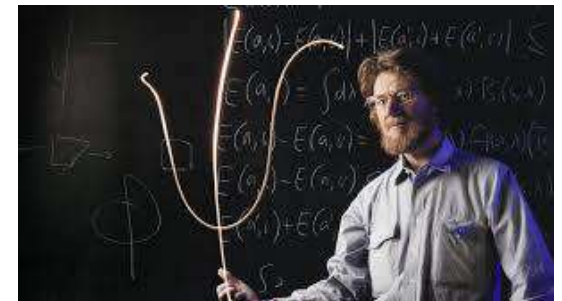
Teorema de Bell



- Alice e Bob medem dois possíveis observáveis cada: A_0, A_1, B_0, B_1
- Após um número suficiente de medições eles podem estimar quantidades estatísticas. O experimento é descrito em termos de $p(a, b|x, y)$
- Além da hipótese do realismo, temos duas hipóteses causais no teorema de Bell

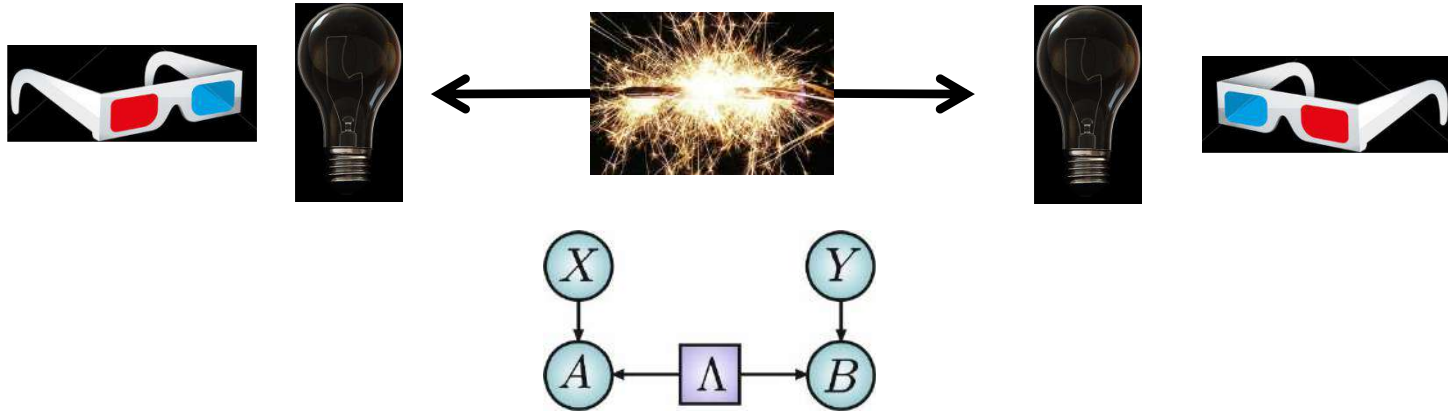
“Livre arbítrio”: $p(x, y, \lambda) = p(x)p(y)p(\lambda)$

Localidade: $p(b|a, x, y, \lambda) = p(b|y, \lambda)$



John Bell

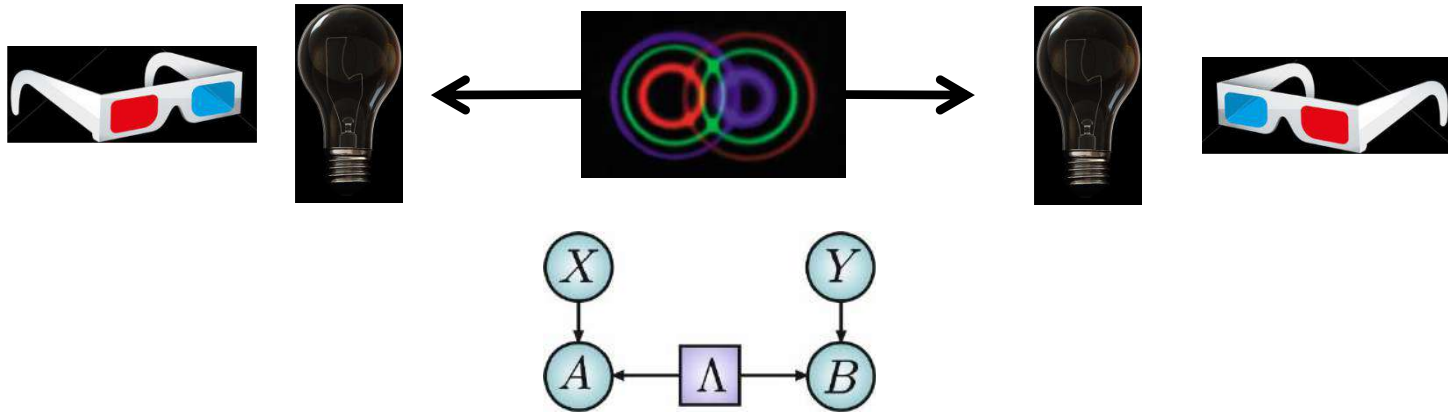
Teorema de Bell



- Estas 3 hipóteses impõe limites ao que pode ser observado.
- Estes limites são chamados **desigualdades de Bell** :

$$\text{CHSH} = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2$$

Teorema de Bell



- Estas 3 hipóteses impõe limites ao que pode ser observado.

- Estes limites são chamados **desigualdades de Bell** :

$$\text{CHSH} = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2$$

- Estes limites são **violados** através do **emaranhamento quântico**

$$\text{CHSH}_{\text{QM}} \leq 2\sqrt{2}$$

Quem está certo?

Einstein com seu sonho de uma teoria local e realista?

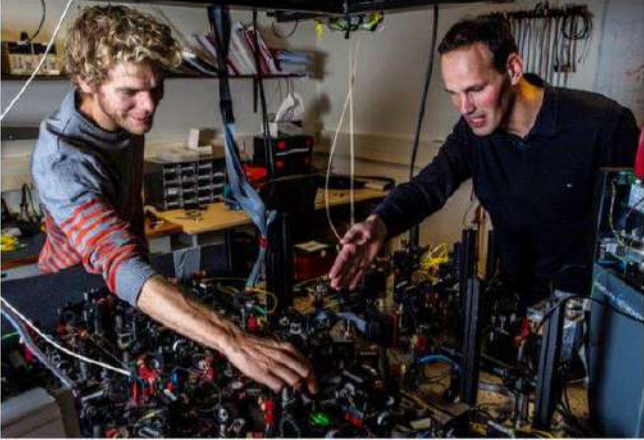
Ou a mecânica quântica?

Quem está certo?

Einstein com seu sonho de uma teoria local e realista?

Ou a mecânica quântica?

ESSENTIAL READING



FRANK AUERLE/DELFT UNIVERSITY OF TECHNOLOGY

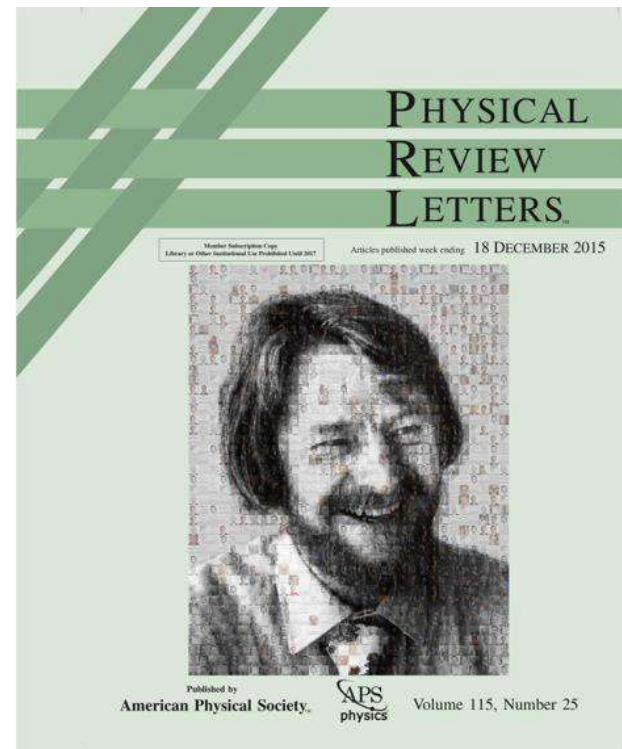
Sorry, Einstein. 'Spooky Action' Looks Real.

A study in the Netherlands supports a long-held claim of quantum theory, one that Einstein refused to accept, that objects separated by great distance could affect each other's behavior.

New York Times

VIA **nytnow**

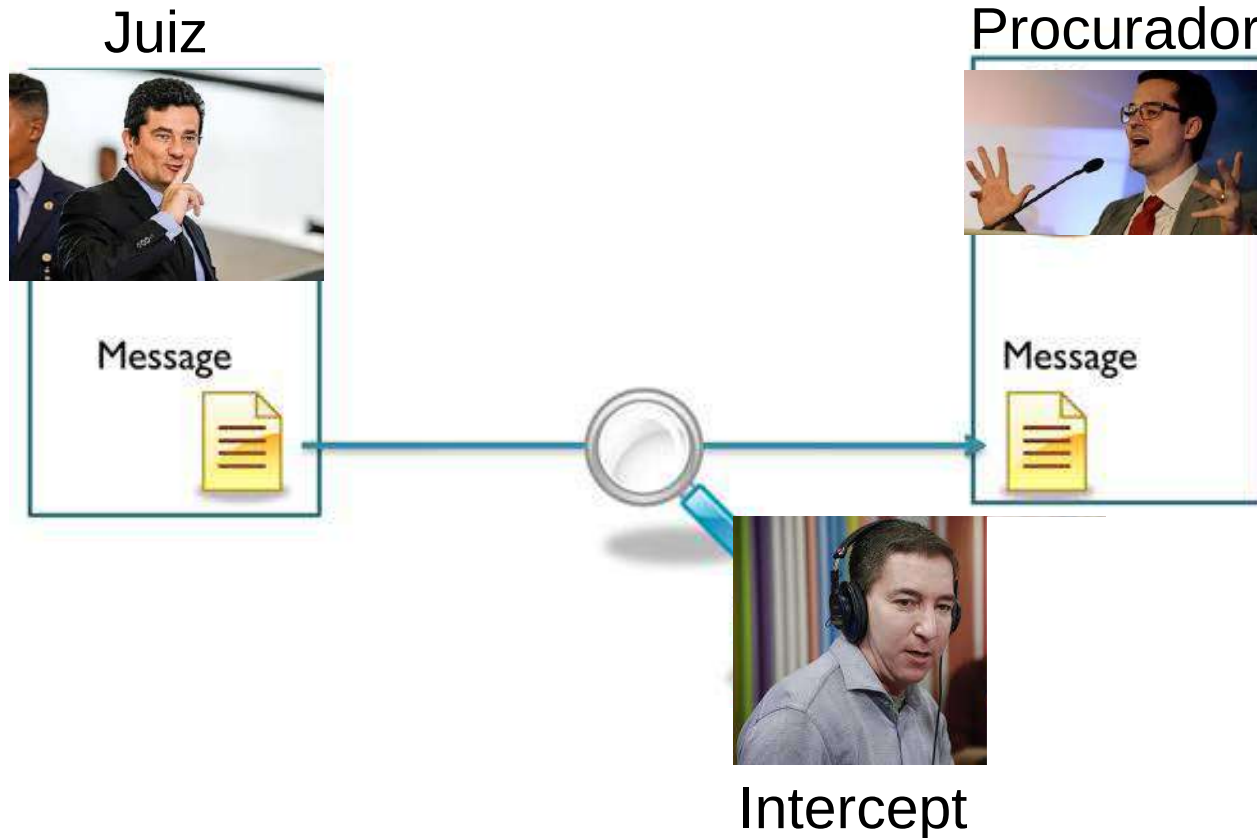
Download our iPhone app.



Commemorative cover from PRL 2015

Criptografia quântica 2.0

A **não-localidade quântica** permite se fazer criptografia de maneira **fundamentalmente** segura sem quaisquer hipóteses sobre complexidade computacional nem sobre o aparato físico.



- A não ser que o hacker **viole as próprias leis da natureza**, temos garantia de segurança!



O que podemos esperar?



A China lançou um satélite capaz de compartilhar **emaranhamento** entre longas distâncias.

Teleportação quântica entre laboratórios separados 6 Km usando uma rede de urbana de fibras ópticas.



FIG. 1. Aerial view of Calgary. Alice is located in Manchester, Bob at the University of Calgary (UofC), and Charlie in a building next to City Hall in Calgary downtown. The teleportation distance — in our case the distance between Charlie and Bob — is 6.2 km. All fibres belong to the Calgary telecommunication network but, during the experiment, they only carry signals created by Alice, Bob or Charlie and were otherwise “dark”.

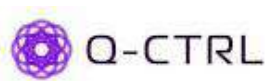


Sistemas de **criptografia quântica** já são comercializados.

Google, Microsoft, IBM e muitas outras gigantes da tecnologia estão investindo pesado em **computação quântica**.



A União Européia investiu 1 bilhão de Euros para em pesquisas de novas tecnologias quânticas. EUA, Canada, Australia, China estão investindo de forma massiva.



Dezenas de “**quantum startups**”

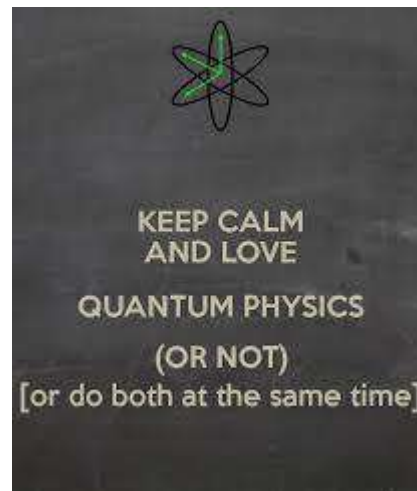
Podcast Qubits e Quasares



anchor.fm/iif-ufrn



cienciafundamental.blogfolha.uol.com.br/



www.iif.ufrn.br/qiqm
https://twitter.com/qiqm_iif