



Számítógép-hálózatok tehetségápolás

2014. október 16.

Kvantumkommunikációs kalandozások

Dr. Bacsárdi László

NymE Simonyi Károly Kar, Informatikai és Gazdasági Intézet
intézetigazgató, egyetemi docens

BME Mobil Kommunikáció és Kvantumtechnológiák Laboratórium,
óraadó

Kvantuminformatika

Kvantumszámítógép

4

Shor-algoritmus

Ami még izgalmasabb

National Security

In the News Polar vortex Liz Cheney Angela Merkel Green Bay Packers Jahi McMath CES



Koch-backed network raised \$400M in 2012



Liz Cheney to end her U.S. Senate bid



2014.01.02

NSA seeks to build quantum computer that could crack most types of encryption

By Steven Rich and Barton Gellman, Published: January 2 [E-mail the writers](#) ↵

In room-size metal boxes secure against electromagnetic leaks, the National Security Agency is racing to build a computer that could break nearly every kind of encryption used to protect banking, medical, business and government records around the world.

According to documents provided by former NSA contractor Edward Snowden, the effort to build “a cryptologically useful quantum computer” — a machine exponentially faster than classical computers — is part of a \$79.7 million research program titled “Penetrating Hard Targets.” Much of the work is hosted under classified contracts at a [laboratory](#) in College Park, Md.

Kvantuminformatika

Kvantumszámítógép



Shor-algoritmus

Ami még izgalmasabb

III. Hugh Everett formulája:

$$\psi(x) \propto e^{-\frac{x^2}{0.0001}} + e^{-\frac{(x-100)^2}{0.0001}}$$

Heisenberg-féle határozatlansági reláció

$$\Delta X = \sqrt{\langle (X - \langle X \rangle)^2 \rangle}$$

$$\Delta P = \sqrt{\langle (P - \langle P \rangle)^2 \rangle}$$

$$\Delta X \Delta P \geq \frac{\hbar}{2}.$$

Fourier-transzformált alak

$$\left(\int_{-\infty}^{\infty} x^2 |f(x)|^2 dx \right) \left(\int_{-\infty}^{\infty} \xi^2 |\hat{f}(\xi)|^2 d\xi \right) \geq \frac{\|f\|_2^4}{16\pi^2}.$$

$$\left(\int_{-\infty}^{\infty} (x - x_0)^2 |f(x)|^2 dx \right) \left(\int_{-\infty}^{\infty} (\xi - \xi_0)^2 |\hat{f}(\xi)|^2 d\xi \right) \geq \frac{1}{16\pi^2}$$

Bohr-modell

$$L = n \frac{h}{2\pi}, \quad r = \frac{n^2 h^2}{4\pi^2 k_e m e^2}$$

Rydberg-formula

$$R = \frac{k_e e^2}{2a_0 \hbar c}.$$

Időfüggetlen Schrödinger-egyenlet

$$\left(-\frac{\hbar^2}{2m} \Delta + V(x, y, z) \hat{I} \right) |\psi\rangle = E |\psi\rangle,$$

$$\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}.$$

Időfüggő Schrödinger-egyenlet

$$\hat{A}\psi = \lambda_A \psi$$

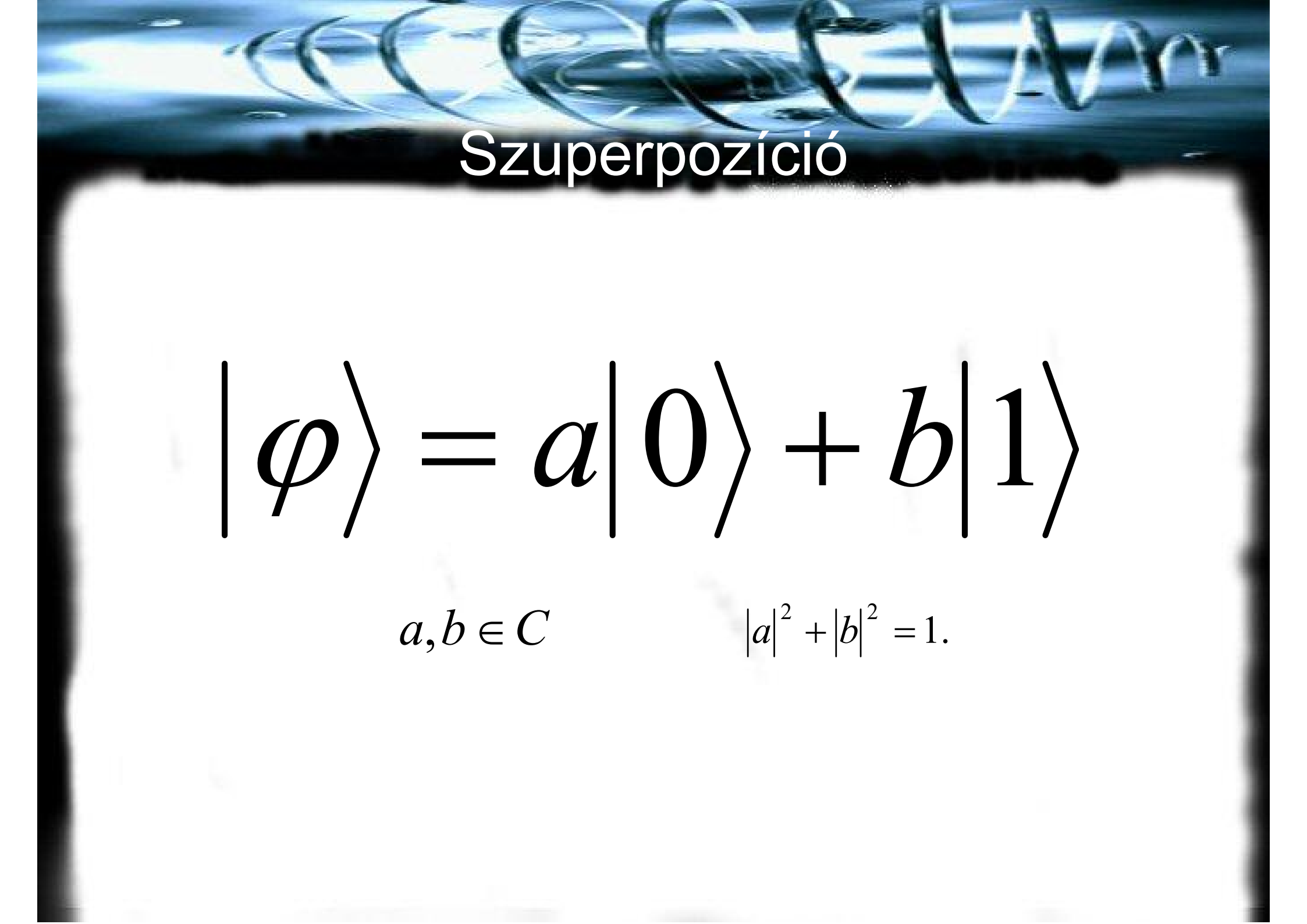
Robertson-Schrödinger reláció

$$\Delta_\psi A \Delta_\psi B \geq \sqrt{\frac{1}{4} |\langle [A, B] \rangle_\psi|^2 + \frac{1}{4} |\langle \{A - \langle A \rangle_\psi, B - \langle B \rangle_\psi\} \rangle_\psi|^2}$$



Szuperpozíció





Szuperpozíció

$$|\varphi\rangle = a|0\rangle + b|1\rangle$$

$$a, b \in \mathbb{C}$$

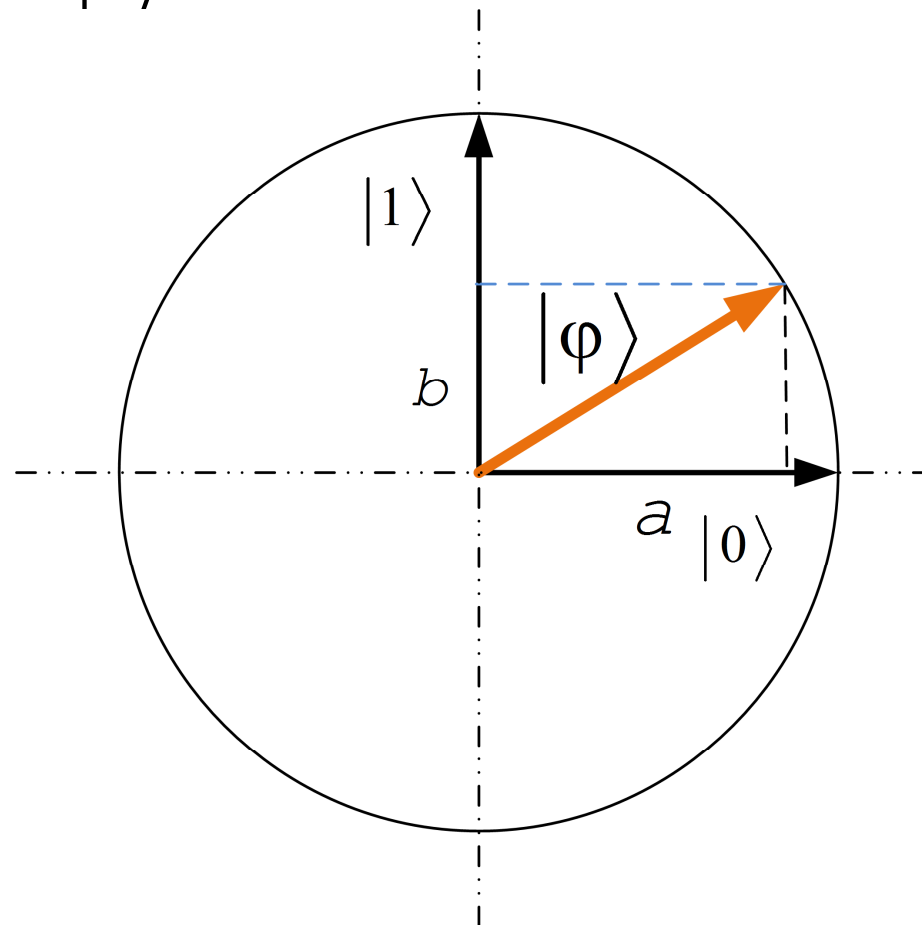
$$|a|^2 + |b|^2 = 1.$$

Szuperpozíció

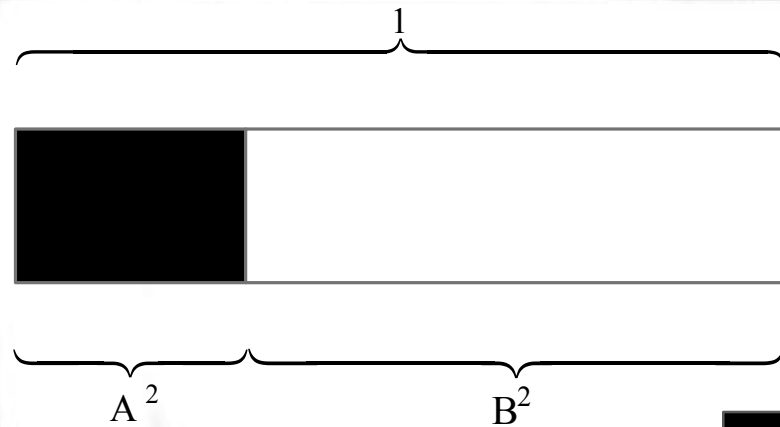
$$|\varphi\rangle = a|0\rangle + b|1\rangle$$

$$|a|^2 + |b|^2 = 1.$$

$$a, b \in \mathbb{C}$$



Szuperpozíció



$|0\rangle$



$(|0\rangle - |1\rangle)/\sqrt{2}$



$|1\rangle$



$(|0\rangle + i|1\rangle)/\sqrt{2}$



A kvantummechanika posztulátumai (1)

1. Állapotleírás

Zárt fizikai rendszer aktuális állapota egy olyan $|\varphi\rangle \in H$ állapotvektorral írható le, amely komplex együtthatókkal rendelkezik, egységnyi hosszú a H Hilbert-térben (egy komplex lineáris vektortérben, amelyben értelmezve van a belső szorzat).

2. A rendszer időbeli fejlődése

A zárt rendszer időbeli fejlődése unitér transzformációval írható le, amely csak a kezdő és végállapottól függ.

A kvantummechanika posztulátumai (2)

3. A mérés

Legyen X a mérés lehetséges eredményeinek a halmaza.

Egy mérés a mérési operátorok halmazával adható meg:

$$M = \{\mathbf{M}_x\}, x \in X, \mathbf{M}_x \in H$$

Ha a megméréendő rendszer állapota $|\varphi\rangle$, akkor annak a valószínűsége, hogy a mérés az x eredményt adja:

$$P(X || \varphi) = \langle \varphi | \mathbf{M}_x^T \mathbf{M}_x | \varphi \rangle$$

A mérés után a rendszer állapota az alábbi lesz

$$|\varphi\rangle' = \frac{\mathbf{M}_x |\varphi\rangle}{\sqrt{p_x}}$$



A kvantummechanika posztulátumai (3)

4. Összetett rendszer

Ha V és Y a két kvantumrendszerhez rendelt Hilbert-tér, akkor az ebből a két rendszerből álló összetett rendszerhez a

$W = V \otimes Y$ Hilbert-tér rendelhető.

Alap építőkövek

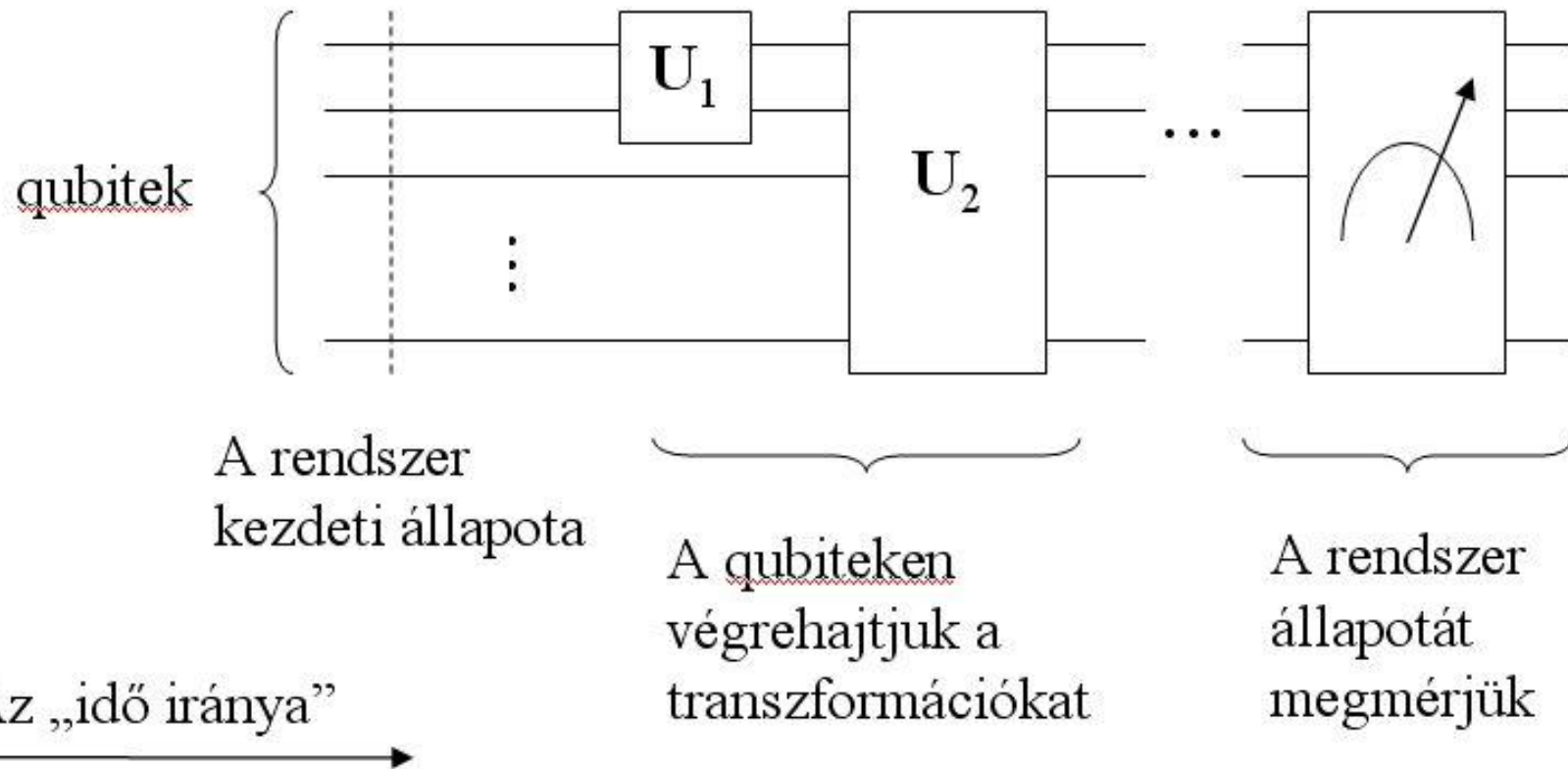
Különböző kvantumkapuk, amelyek a $|\varphi\rangle = a|0\rangle + b|1\rangle$ bemenetre az alábbi kimeneti kvantumbitét állítják elő

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$X|\varphi\rangle = b|0\rangle + a|1\rangle \quad Y|\varphi\rangle = -ib|0\rangle + ia|1\rangle \quad H|\varphi\rangle = \frac{a+b}{\sqrt{2}}|0\rangle + \frac{a-b}{\sqrt{2}}|1\rangle$$

$$Z|\varphi\rangle = a|0\rangle - b|1\rangle$$

Kvantum-áramkör





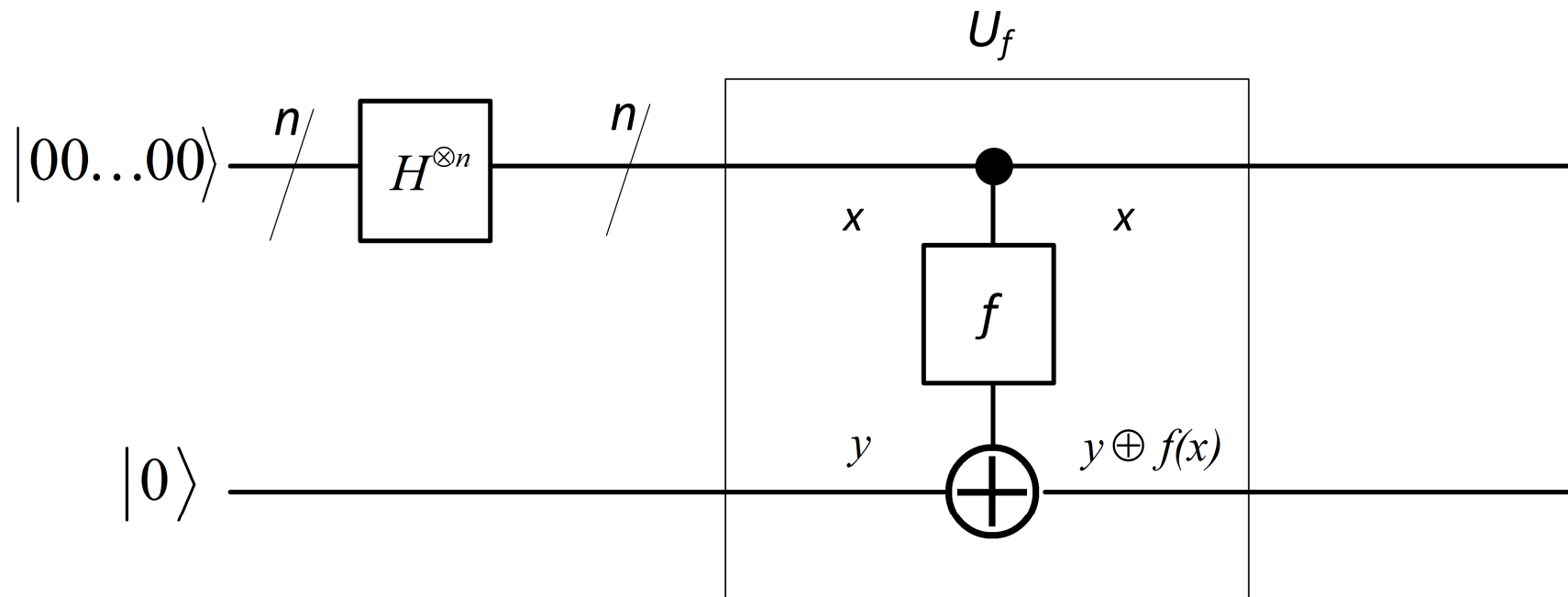
Kvantumpárhuzamoság

$$|\varphi\rangle = a|0\rangle + b|1\rangle$$

$$|\varphi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

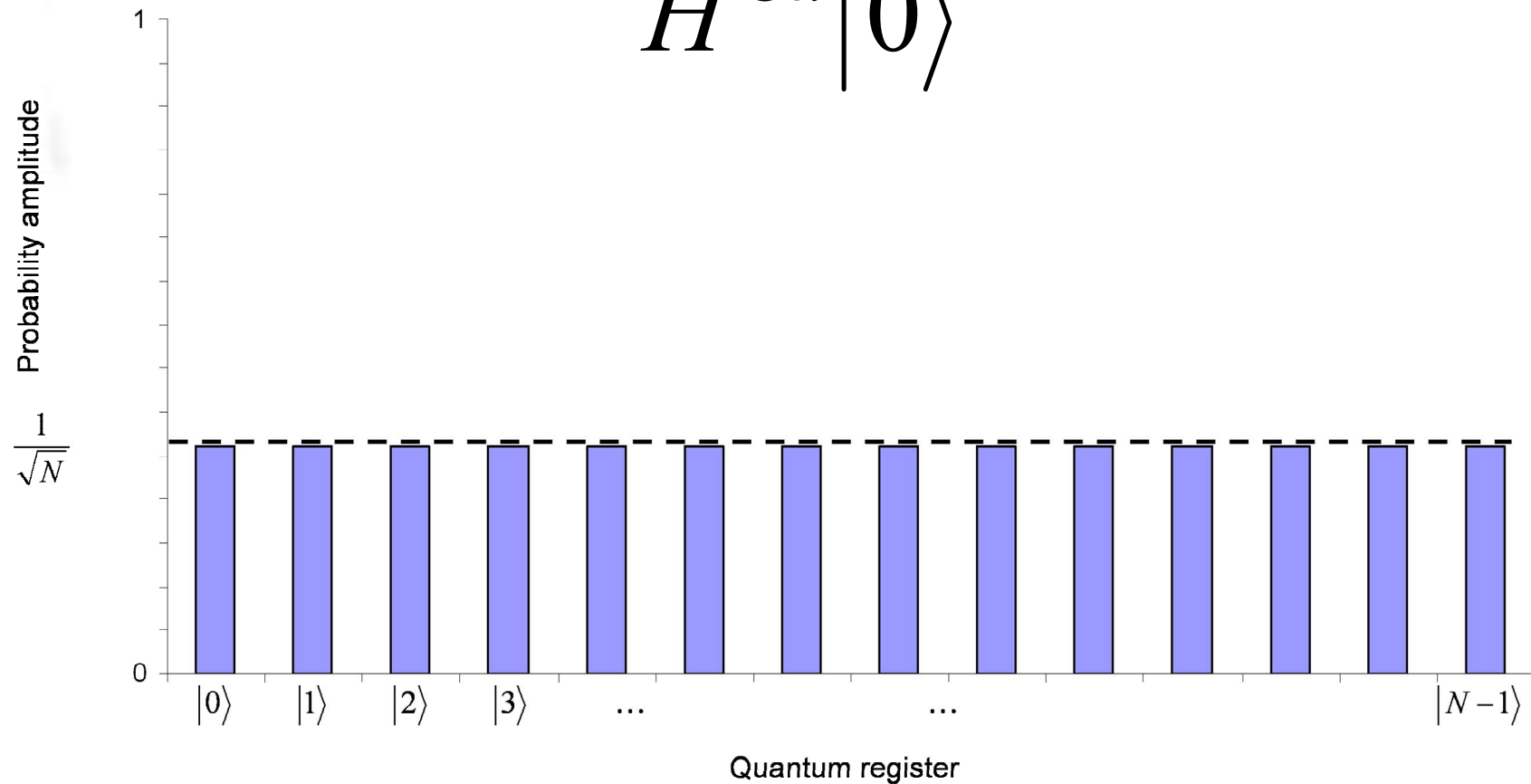
$$\begin{aligned} |\varphi\rangle = & a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle \\ & + e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle \end{aligned}$$

Kvantumpárhuzamosság

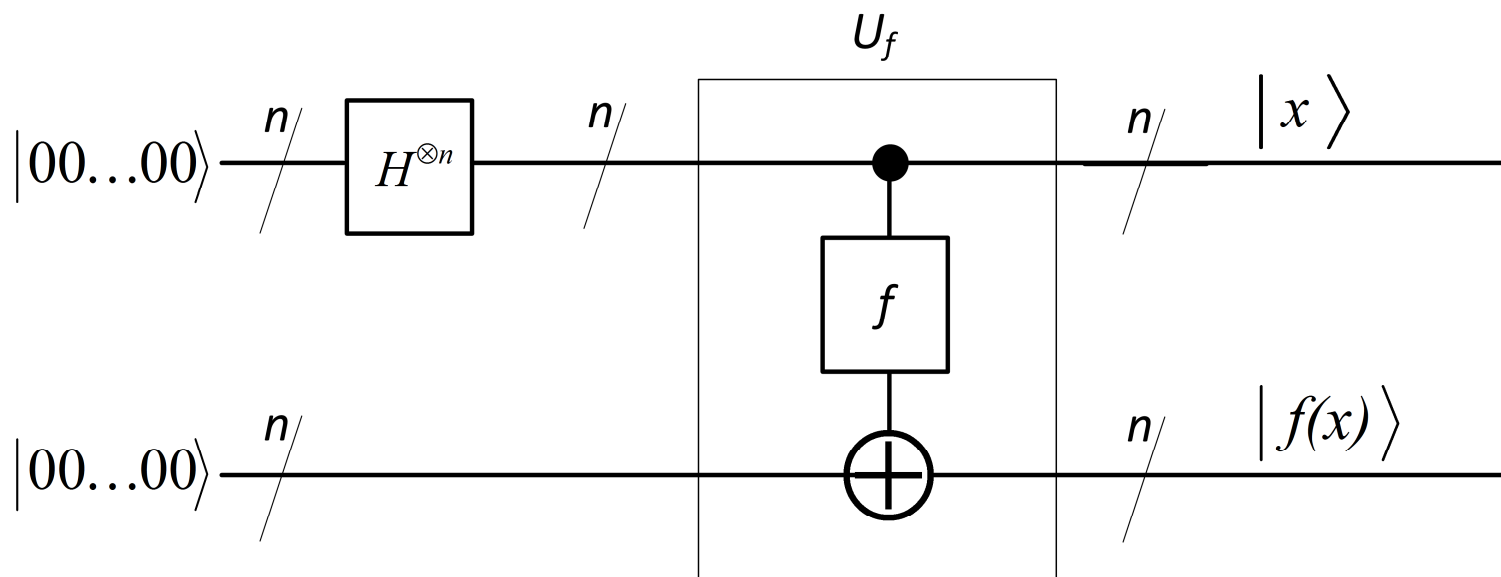


Kvantumpárhuzamoság

$$H^{\otimes n} |0\rangle$$



Kvantumpárhuzamosság





Kvantumpárhuzamosság

Deutsch-Jozsa algoritmus

$$x \in \{0,1\}^n$$

$$f(x) : \{0,1\}^n \rightarrow \{0,1\}^1$$

Kiegyensúlyozott?

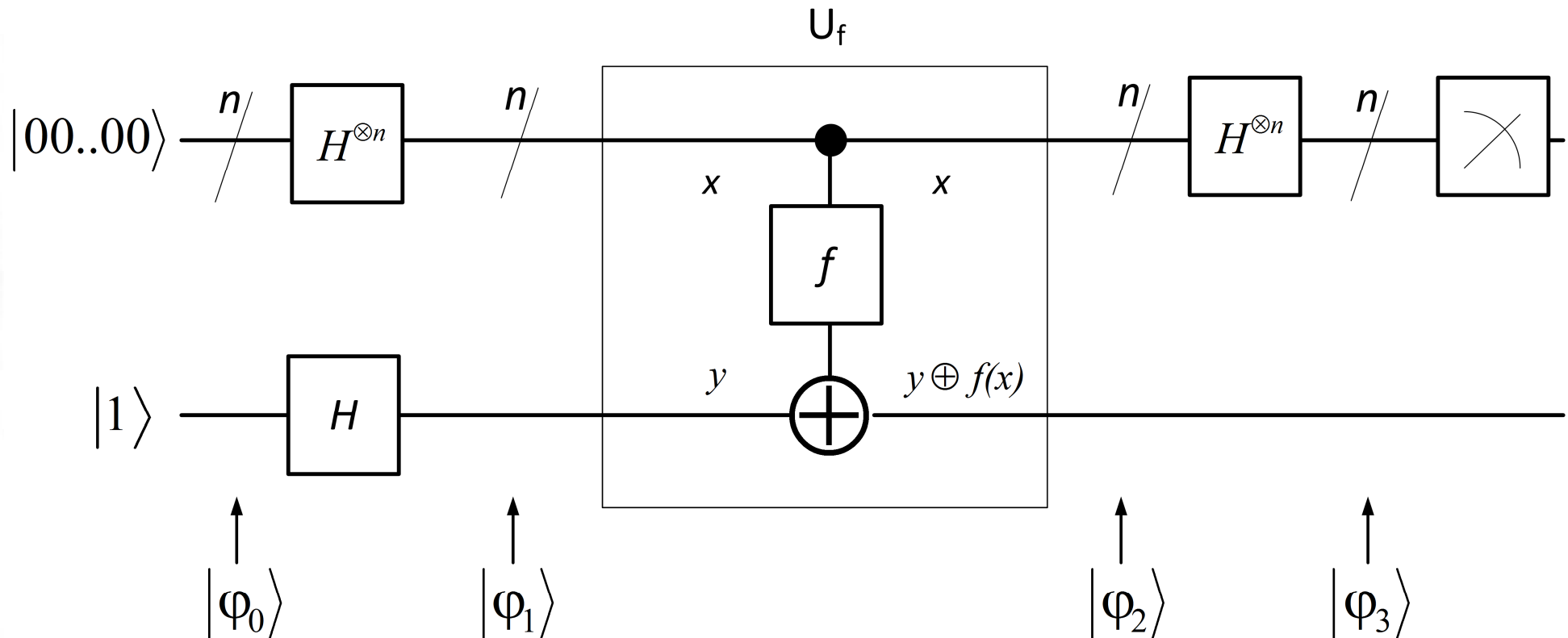
Konstans?

Kvantum párhuzamosság

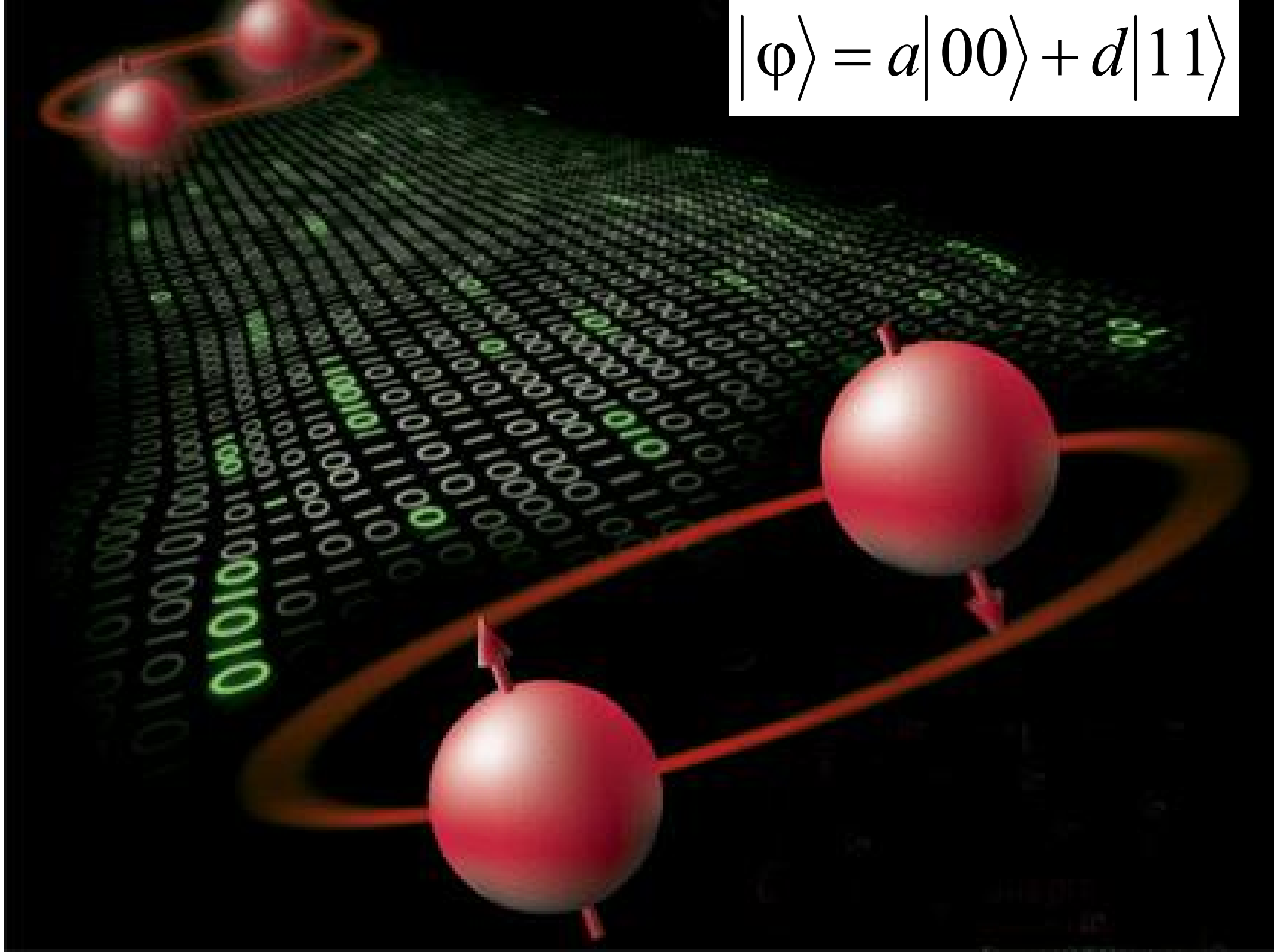
Deutsch-Jozsa algoritmus

$$x \in \{0,1\}^n$$

$$f(x) : \{0,1\}^n \rightarrow \{0,1\}^1$$



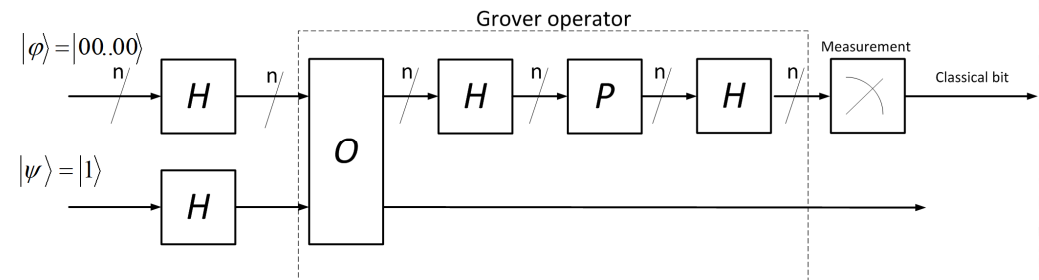
$$|\varphi\rangle = a|00\rangle + d|11\rangle$$



Miért is jó ez nekünk?

- Algoritmusok és protokollok

- Teleportáció
- Szupersűrűségű tömörítés
- Kvantumpárhuzamosság
- ...



- Klasszikus problémák „jobb” megoldása

- Keresés adatbázisban
- Prímtényezőkre bontás
- Rendkeresés
- Szimmetrikus kulcsszétosztó protokollok
- Információelméleti alkalmazások

Nincs másolás

Dekoherencia



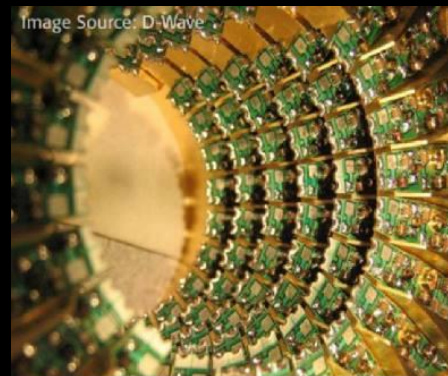
"I still don't understand quantum theory."

Rights Available from CartoonStock.com

© Original Artist / Search ID: mshn197

Kvantuminformatika

Kvantumszámítógép



30 Qubit Computer
10 teraFLOPS



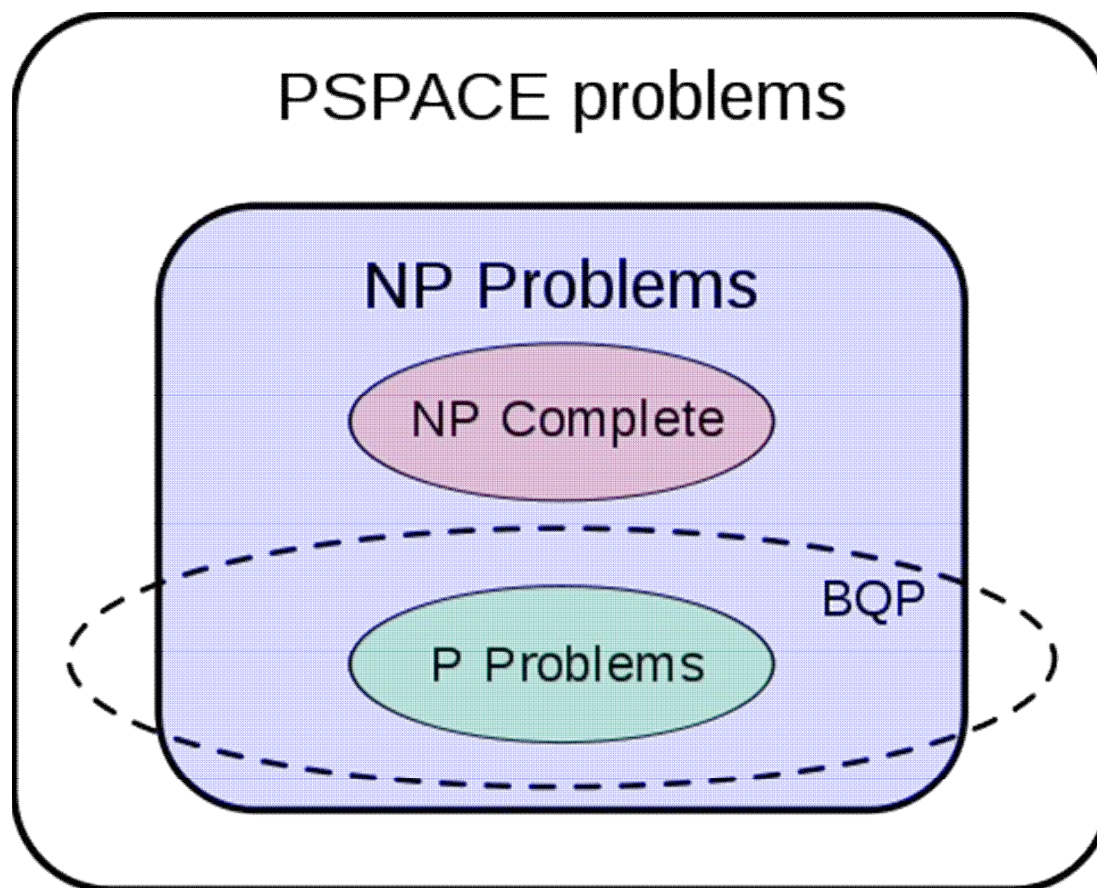
30 Bit Computer
~0.5 megaFLOPS

**Quantum computers perform
2 million times faster**

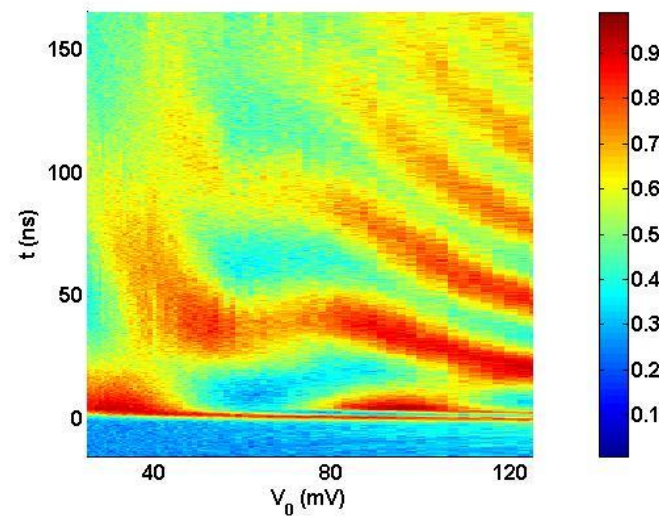
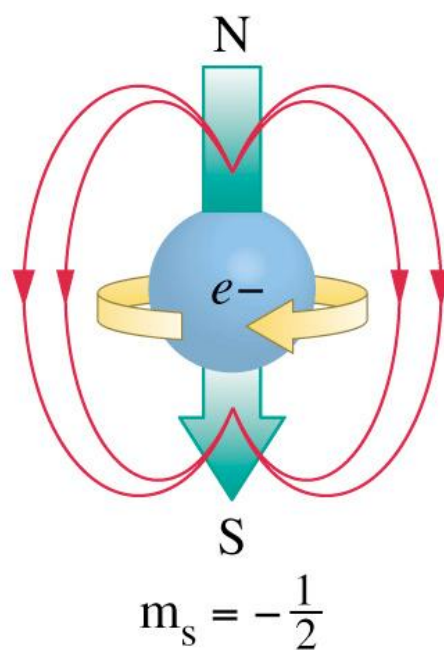
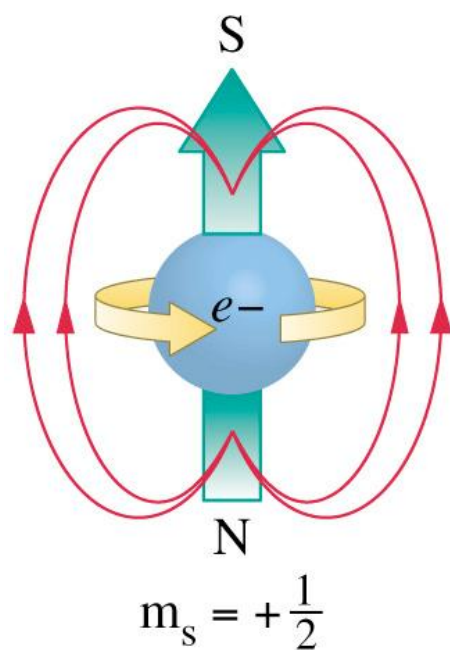
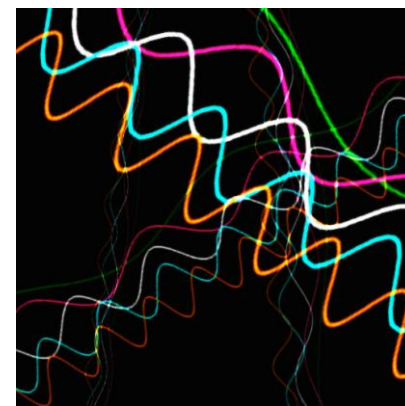
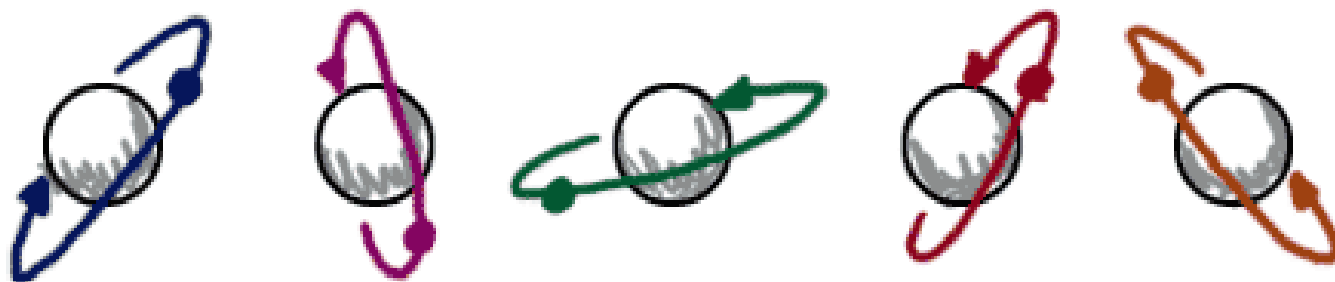


Shor-algoritmus

Ami még izgalmasabb



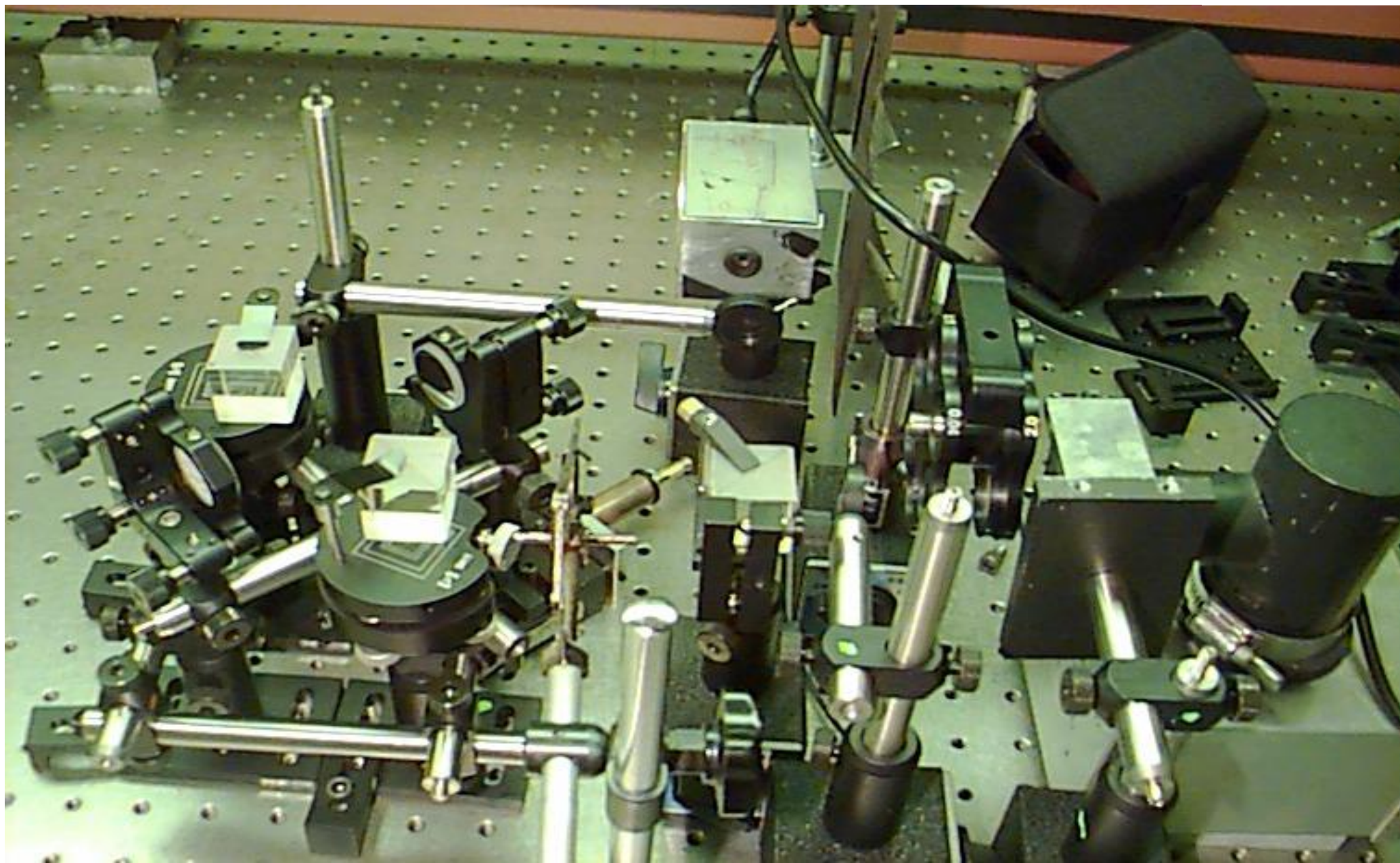
Mi lehet kvantumbit?



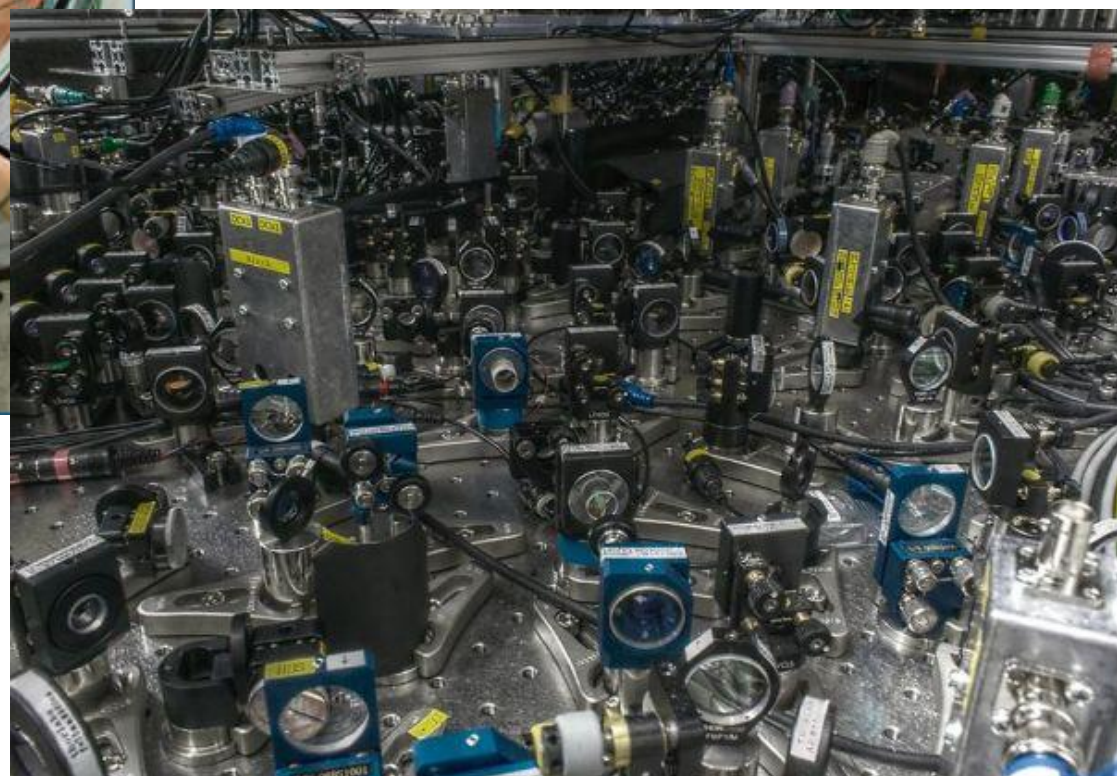
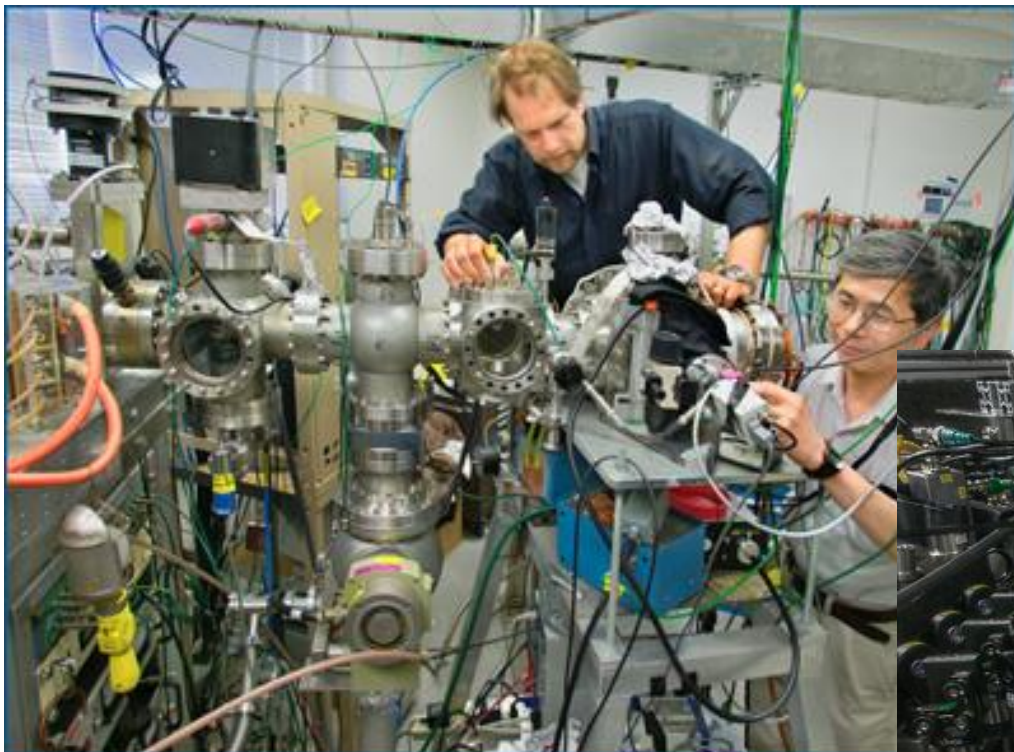
Kvantum eszközök (1)



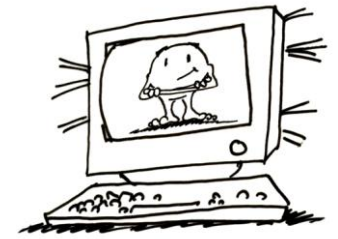
Kvantum eszközök (2)



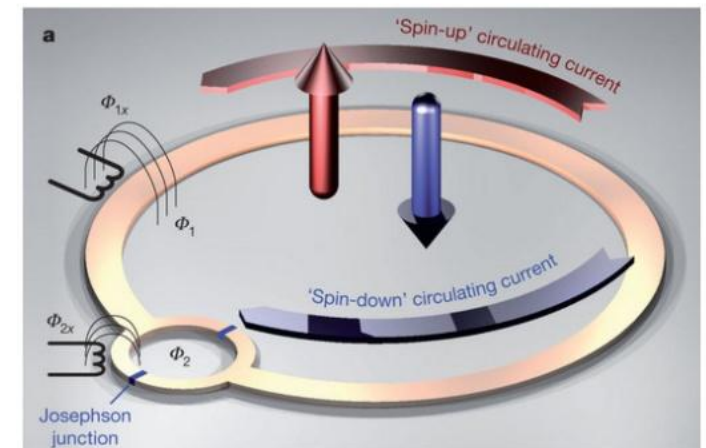
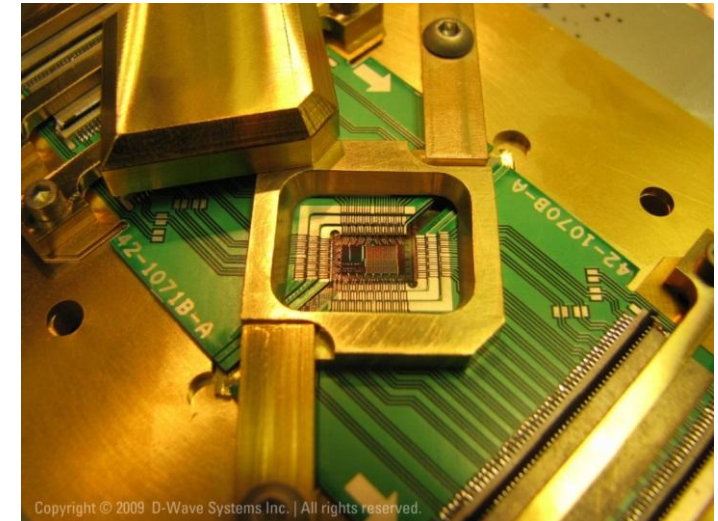
Kvantum eszközök (3)

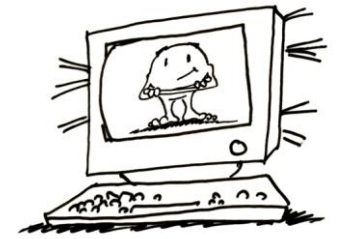


Fénykép: Roy Kaltschmidt, forrás: <http://www.lbl.gov/Science-Articles/Archive/sabl/2005/June/02-quantum-comp.htm>
Forrás: http://wikis.lib.ncsu.edu/index.php/Image:Quantum_Computer.jpg



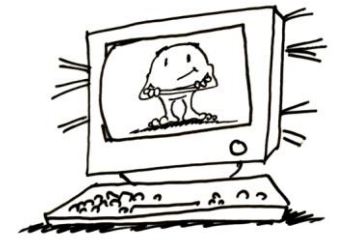
- Fluxuskvantumokon alapuló adiabatikus rendszer
- 2007 Orion Systems, 16 kvantumbites gép bemutatója három alkalmazással:
 - Adatbázis keresés
 - Ülésrend tervezés
 - Sudoku fejtés
- 2009 Neural Information Processing Systems Conference
 - Képfelismerő rendszer betanítása





- 2011, D-Wave One
 - 128 qubit
 - 10 000 000 \$
- 2013, D-Wave Two
 - 512 qubit



A wide banner with a dark blue background featuring abstract, glowing geometric patterns and lines. The text "QUANTUM ARTIFICIAL INTELLIGENCE LABORATORY" is centered in a light blue, sans-serif font.

QUANTUM ARTIFICIAL INTELLIGENCE LABORATORY

The image shows a man in a blue shirt and khaki pants standing next to a large, dark-colored quantum computer unit. The unit has the Google logo on its side. The top of the image shows a close-up of the quantum computer's internal components, which are gold-colored and have many wires connected to them. The man is standing in front of the unit, which is open, revealing the internal components. The text "Google & NASA's Quantum Computer" is overlaid on the image in white. The text "So...that's a Quantum Computer?" is overlaid at the bottom in a white, italicized font.

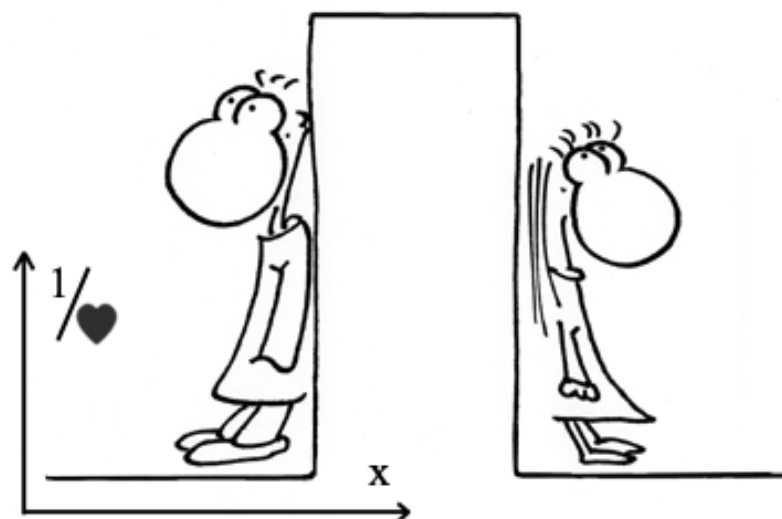
Google & NASA's Quantum Computer

Google

So...that's a Quantum Computer?

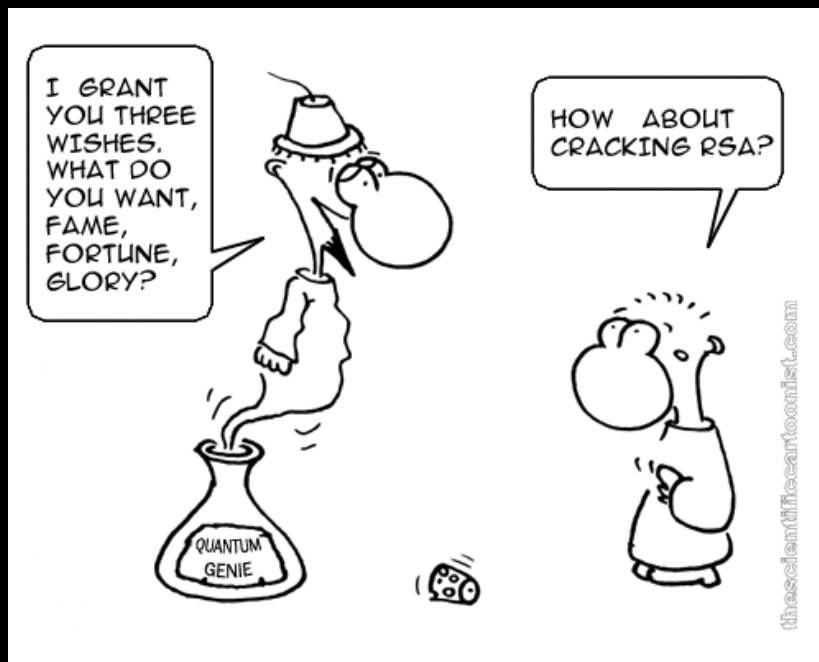


thescientificcartoonist.com



Waiting for the tunnel effect.

Kvantuminformatika



Shor-algoritmus

Kvantumszámítógép

Ami még izgalmasabb

RSA törése

$$O(\log^3(N))$$

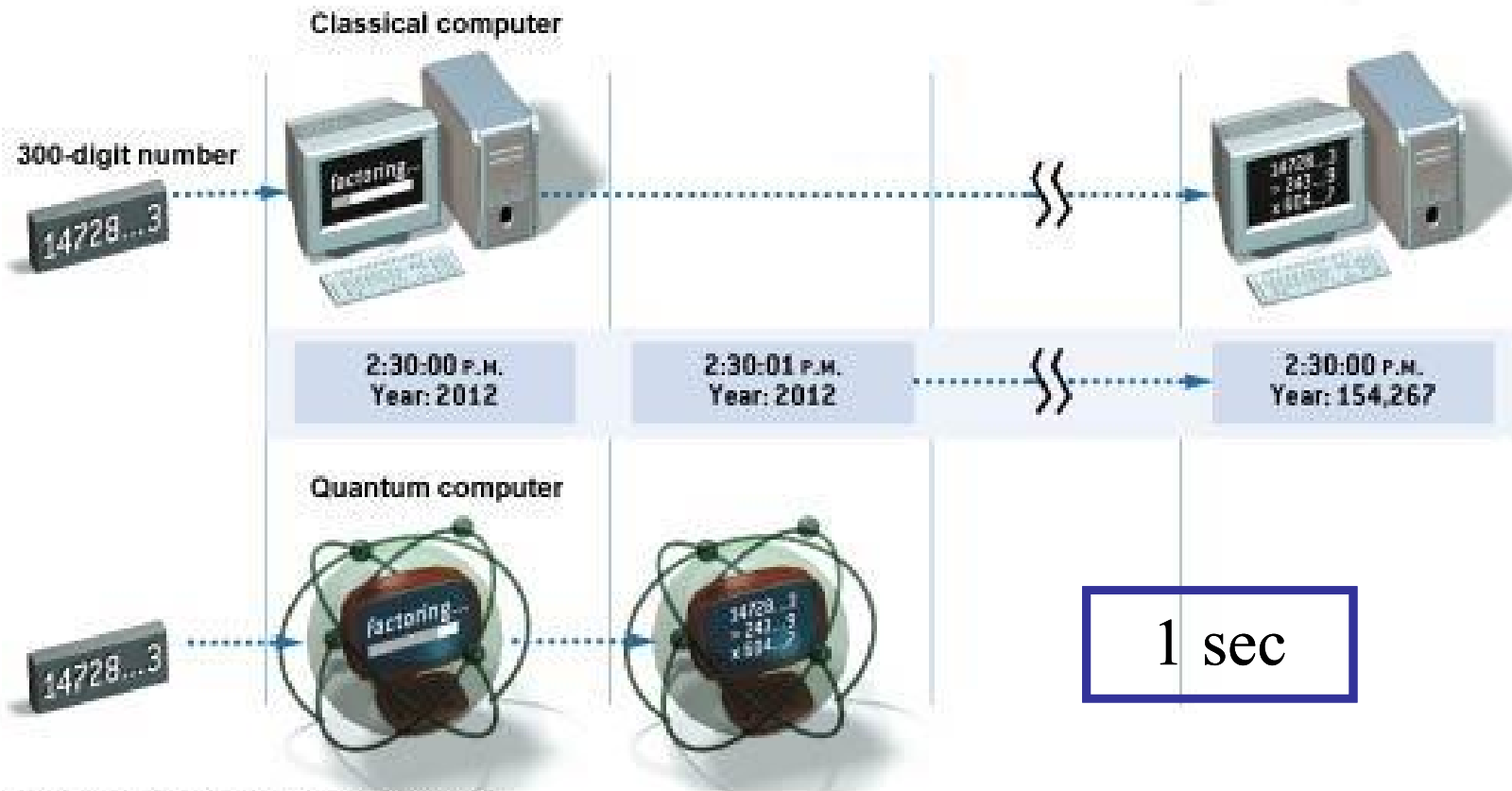
152 000 év



Shor-algoritmus és az RSA feltörése

$$O(\log^3(N))$$

152 000 év



BRYAN CHRISTIE DESIGN



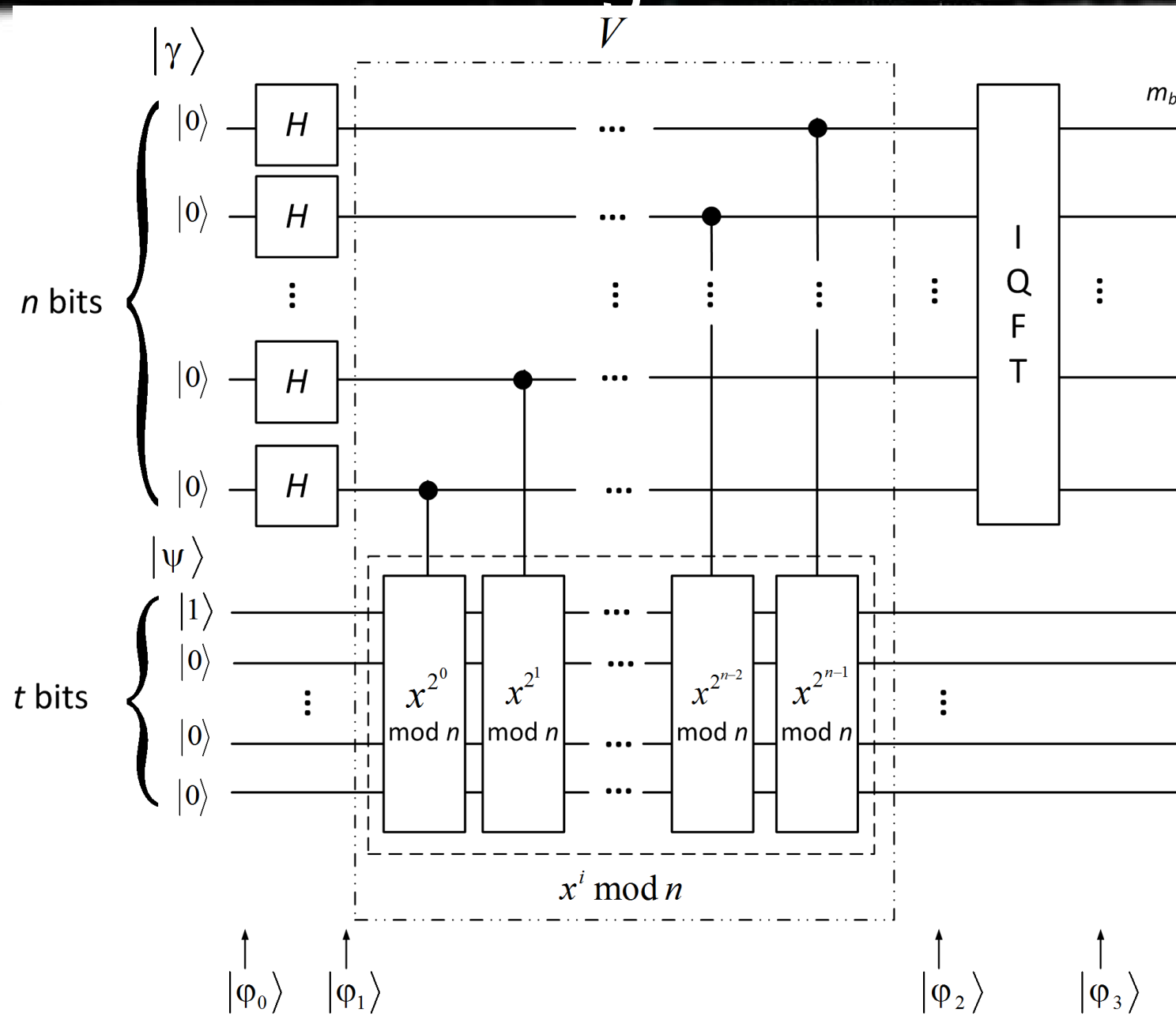
Shor-algoritmus

- Egy olyan szám megtalálását, amelynek a felbontandó számmal van közös osztója, átfogalmazhatjuk egy függvény periódusának meghatározására
- Klasszikus rendszerben nehéz feladat, viszont a perióduskeresésre gyors kvantumalgoritmust lehet találni
- Amíg a prímfaktorizáció klasszikus rendszerekben exponenciális, addig kvantum rendszerekben négyzetes növekményű végrehajtási időt igényel

$$O(d^3(N))$$

Részletes leírás: http://www.mcl.hu/quantum//foliak/kvantum_primfakt1.pdf

Shor-algorithmus





15

21

143

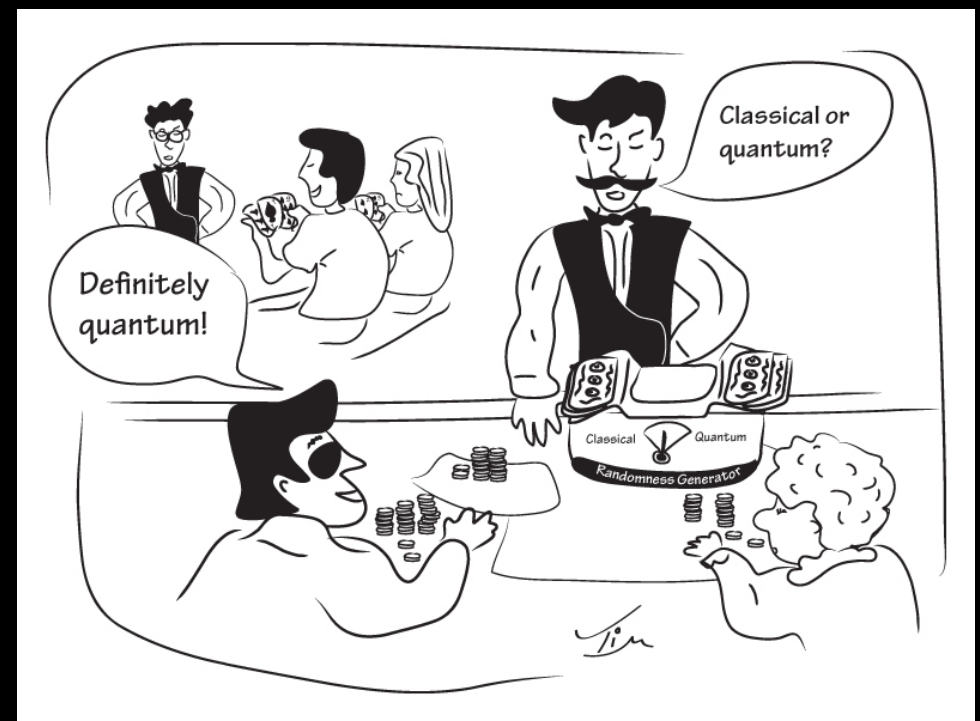
*Martín-López, Enrique et al. „Experimental realization of Shor's quantum factoring algorithm using qubit recycling”,
Nature Photonics 6, 773–776, (2012)*

*Nanyang Xu, Jing Zhu, Dawei Lu, Xianyi Zhou, Xinhua Peng, and Jiangfeng Du, Quantum Factorization of 143 on a
Dipolar-Coupling Nuclear Magnetic Resonance System, Phys. Rev. Lett. 108, 130501 (2012).*

Kvantuminformatika

Shor-algoritmus

Kvantumszámítógép



Ami még izgalmasabb

Teleportálás

1993: elmélet

1998: sikeres kísérlet

2004: 600 méter

2012: 97 km (Kína)

2012: 143 km (Kanári-szigetek)

C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters, Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels, Phys. Rev. Lett. 70, 1895-1899 (1993)

Juan Yin et. al, Quantum teleportation and entanglement distribution over 100-kilometre free-space channels, Nature 488 185-188 (2012)

Ma, X. S.; Herbst, T.; Scheidl, T.; Wang, D.; Kropatschek, S.; Naylor, W.; Wittmann, B.; Mech, A. et al. (2012). "Quantum teleportation over 143 kilometres using active feed-forward". Nature 489 (7415): 269–273

C. Nölleke, A. Neuzner, A. Reiserer, C. Hahn, G. Rempe, S. Ritter}, Efficient Teleportation Between Remote Single-Atom Quantum Memories, Phys. Rev. Lett. 110, 140403 (2013)

Kvantum alapú kulcsszétosztás (QKD)

E91

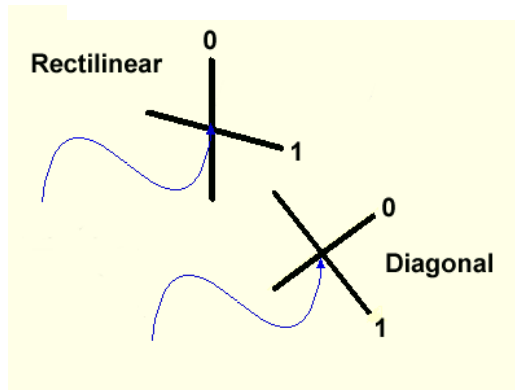
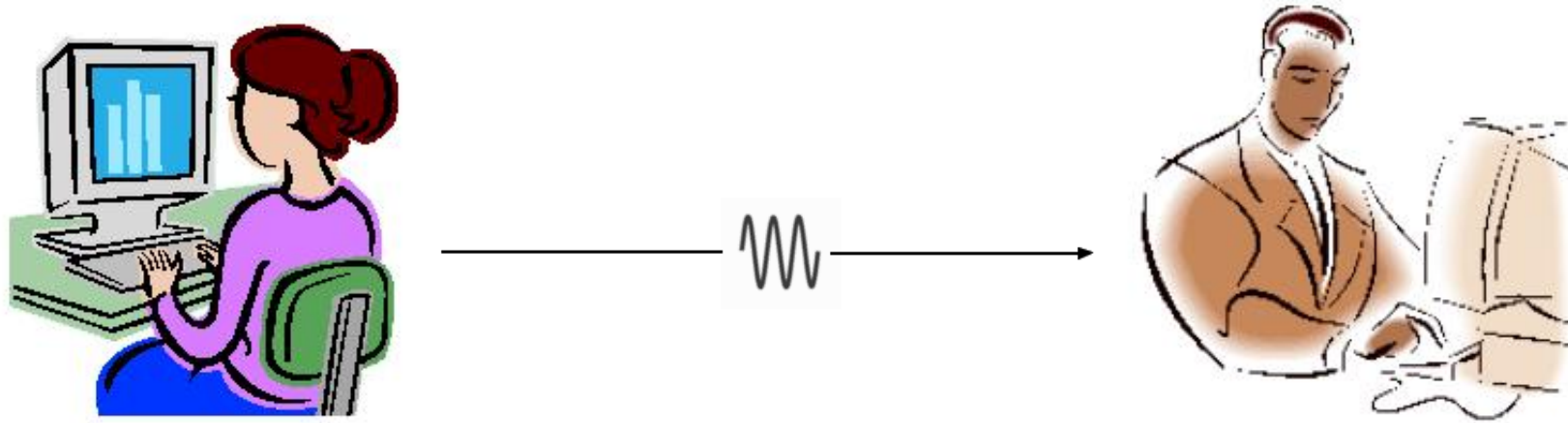
BB84

B92

S09

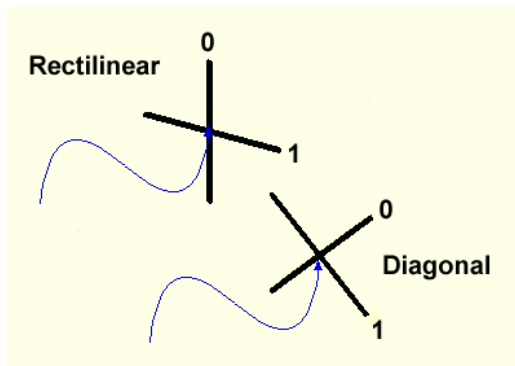
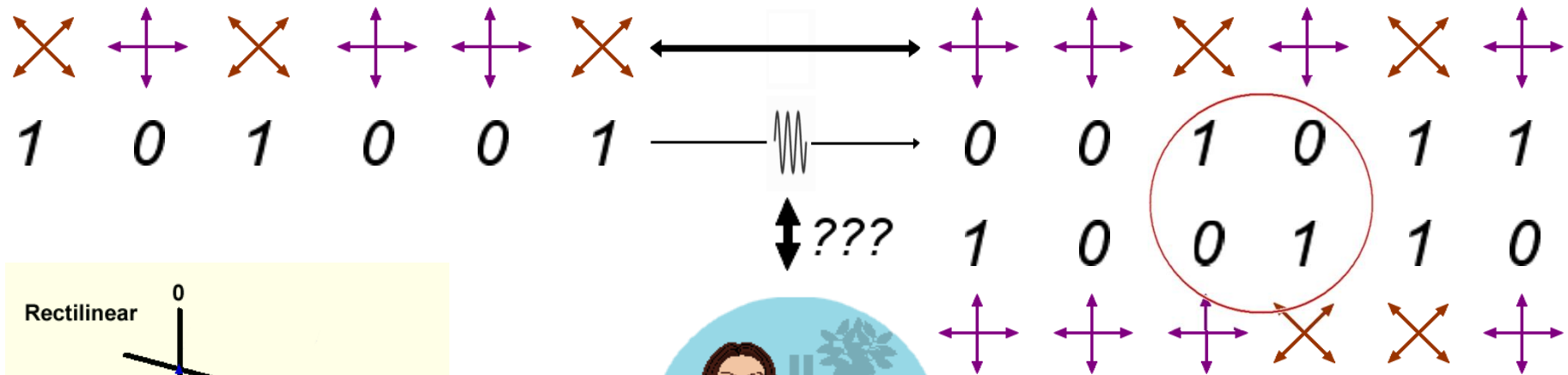
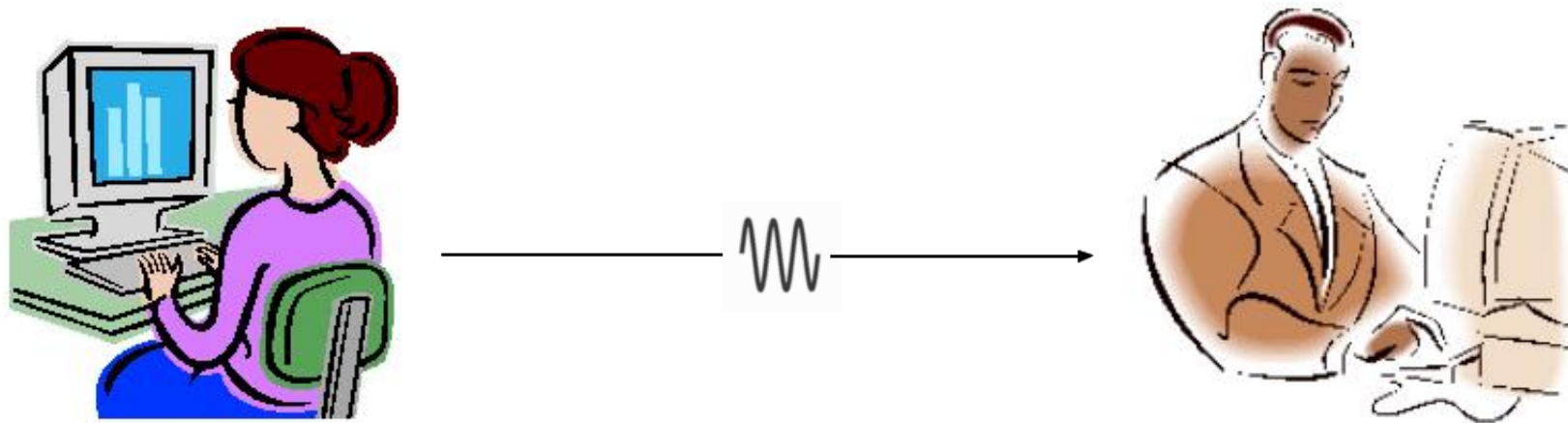
Bacsardi, L.; Kiss, A.; Galambos, M.; Imre, S., "Examining quantum key distribution protocols in laser based satellite communications," Communication, Networks and Satellite (ComNetSat), 2012 IEEE International Conference on , vol., no., pp.187-91, 12-14 July 2012

BB84 protokoll



Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

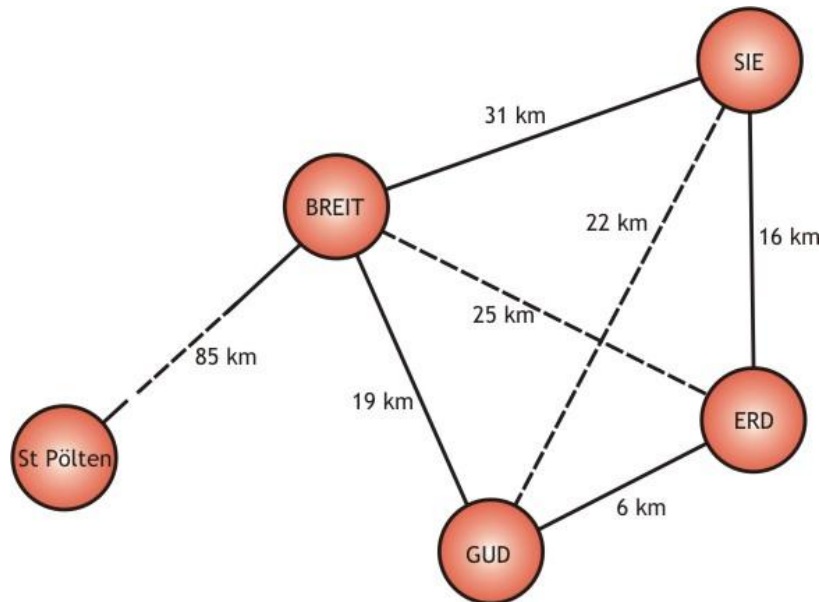
BB84 protokol



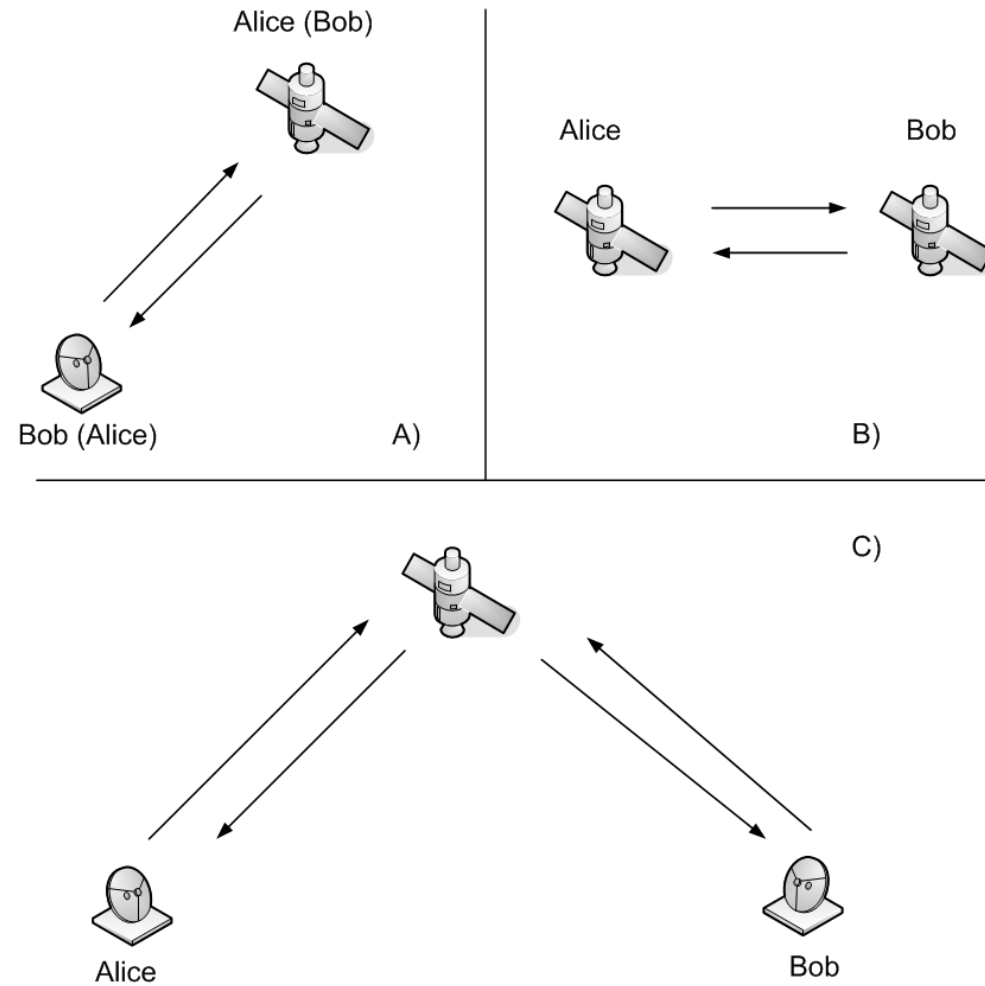
<http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/index.html>

Charles H. Bennett, Gilles Brassard, 'Quantum Cryptography: Public Key Distribution and Coin Tossing', International Conference on Computers, Systems & Signal Processing, Bangalore, India (December 10-12, 1984)

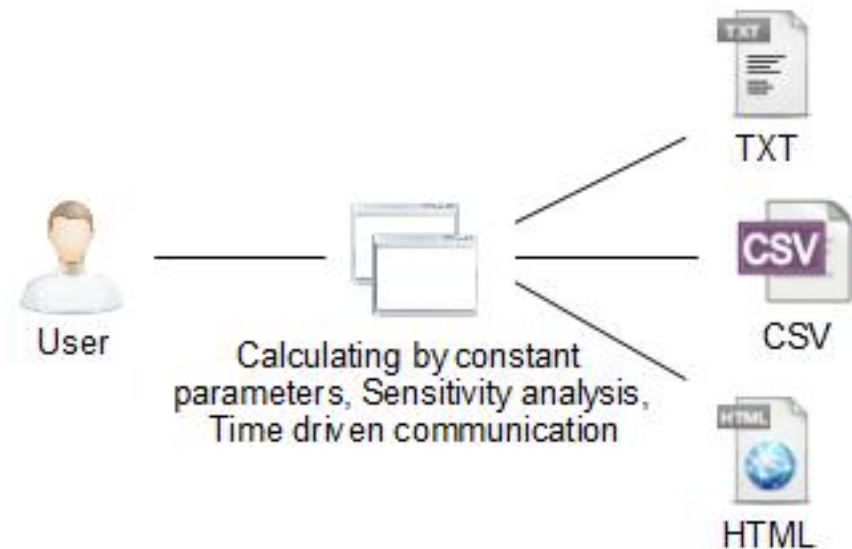
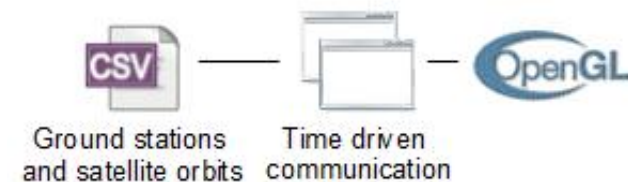
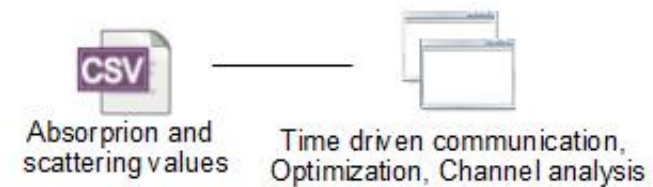
Vienna, October 8, 2008. Today, the first commercial communication network using quantum cryptography is demonstrated in Vienna, Austria.

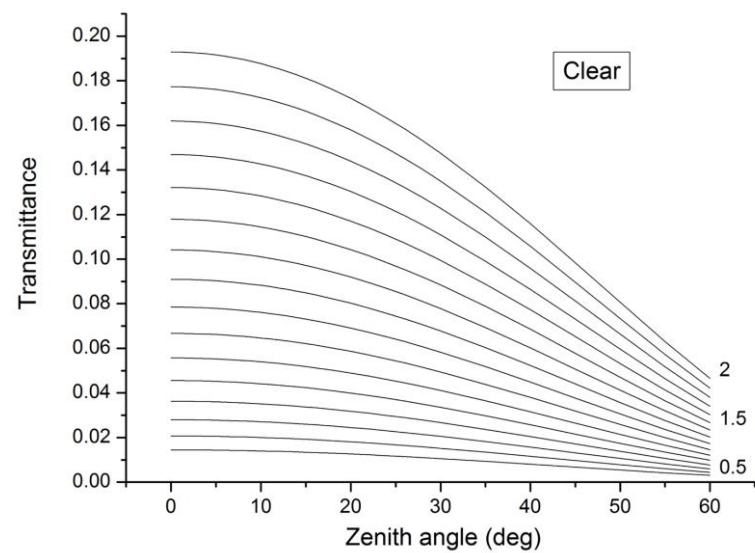


Irány az űr

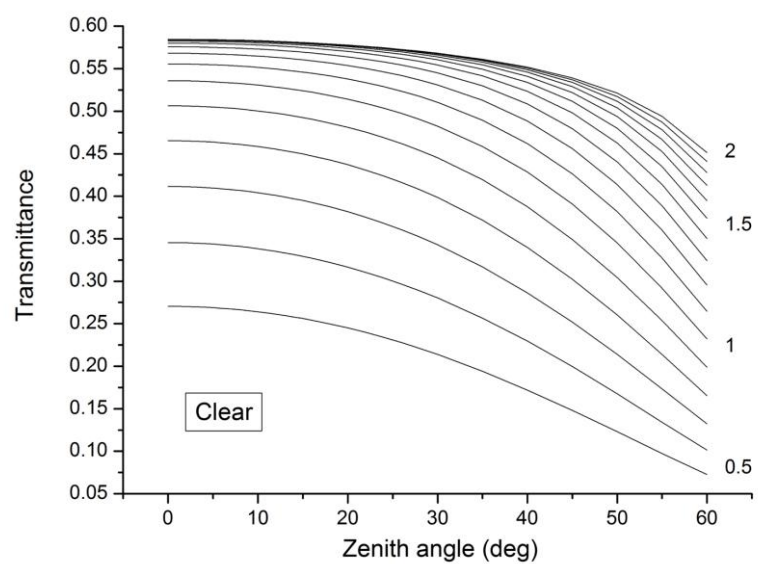


Quantum Satellite Communication Simulator





A



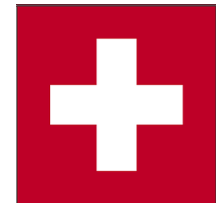
B

Műholdas QKD hálózat

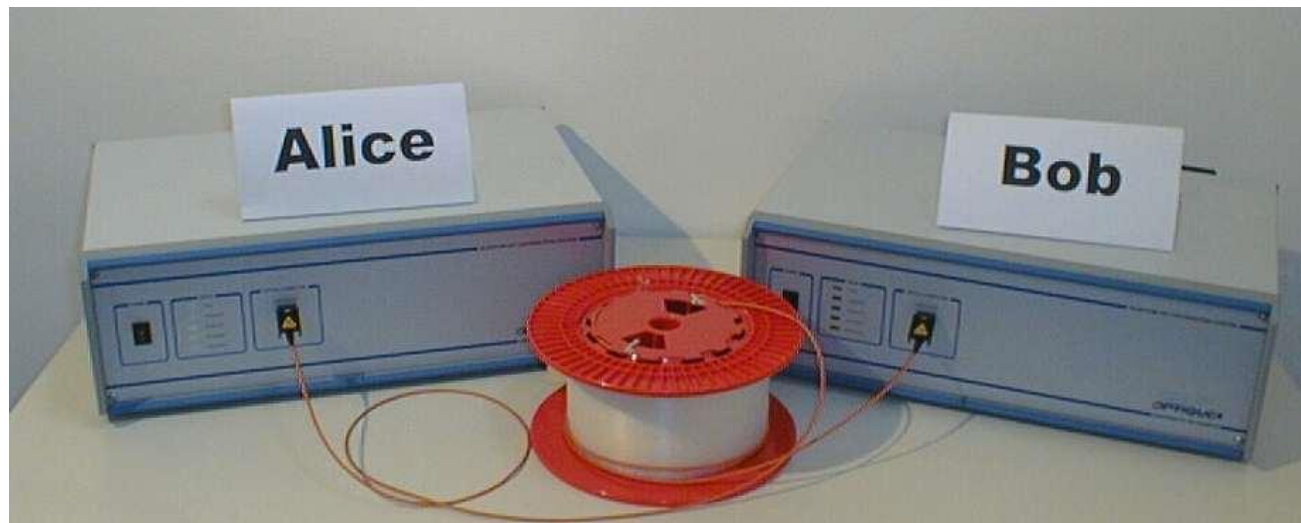
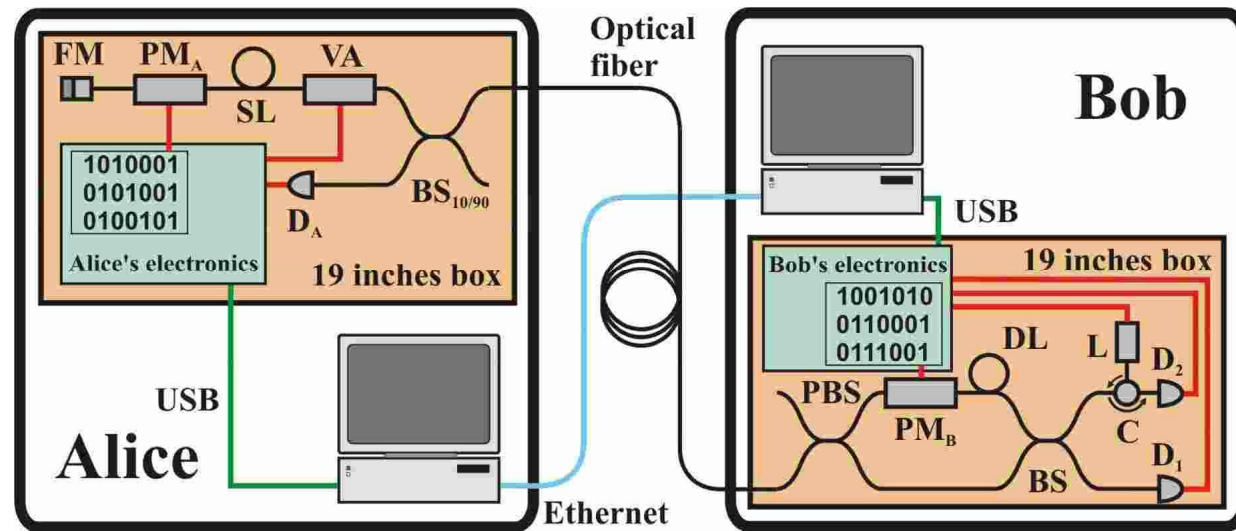
Satellite's orbit	Number of requested satellites for the path	Total QBER
300	3	0.0101
400	3	0.0151
500	2	0.0214
600	2	0.0295
700	2	0.0391
800	1	0.0501
900	1	0.0627
1000	1	0.0767
1500	1	0.1694
2000	1	0.2692

Cégek

- D-wave :
 - Kanadai cég
 - 1999-ben alapították
 - Állításuk szerint kvantumszámítógépet árulnak
- IdQuantique
 - Svájci cég
 - Senatas-al együttműködésben
 - 2001 óta létezik, University of Geneva Spinoff
 - Kvantum kulcsszétosztás, randomszám generálás
- MagiQ Technologies
 - Amerikai
 - 1999-ben alapították
 - Kvantum kulcsszétosztás
- Quintessence Labs
 - Amerikai-ausztrál együttműködés
 - Kulcsszétosztás, randomszám generálás



Ahogy ma mások kulcsszétosztanak



Ahogy mi kulcsszétosztunk

Ahogy mi kulcsszétosztunk



Dr. Imre Sándor

- szakmai vezető

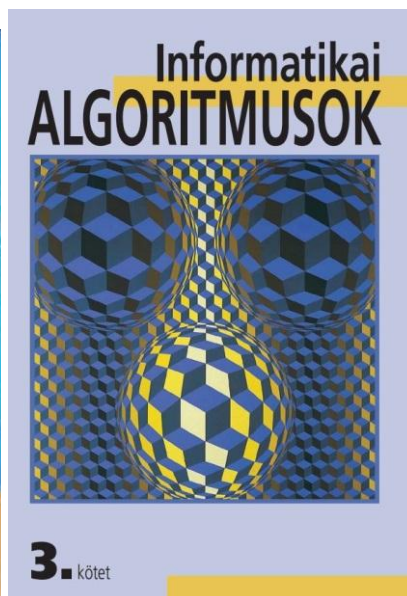
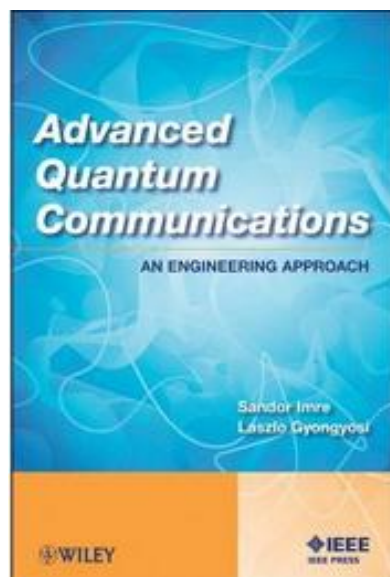
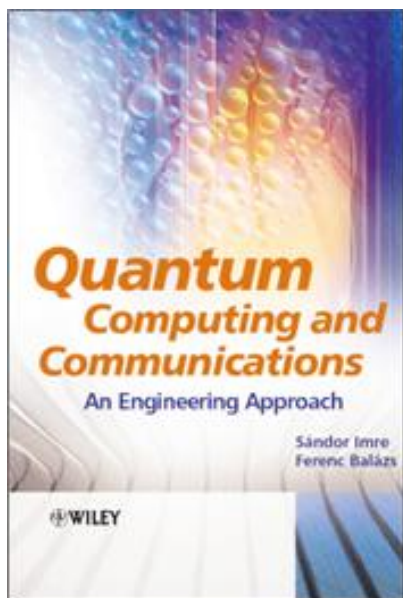
Mérnökök, fizikusok, hallgatók
(*BME TTK, BME VIK, Wigner FKK*)



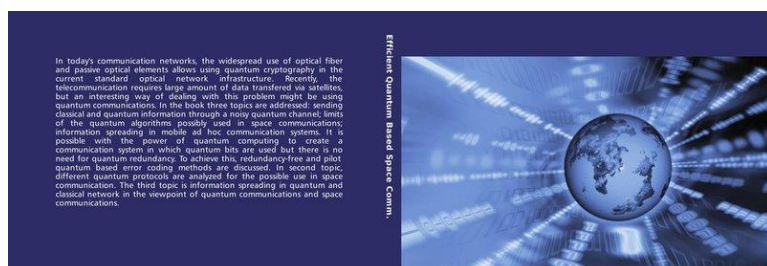
Dr. Bacsárdi László

- szakmai vezető-helyettes





Kvantumos híreket tartalmazó
qnews levelezőlista
Feliratkozás: előadónak küldött levél



László Bacsardi

The author obtained Ph.D. at the Budapest University of Technology and Economics, Hungary. He is now Associate Professor and the Head of the Institute of Informatics and Economics at the University of West Hungary, Sopron, Hungary. His current research interests are in mobile ad hoc communication, quantum computing and quantum communications.



978-3-659-36860-8

Bacsardi

Efficient Quantum Based Space Communications

Classical and Quantum Based Information Transfer and Dissemination in Space Communications



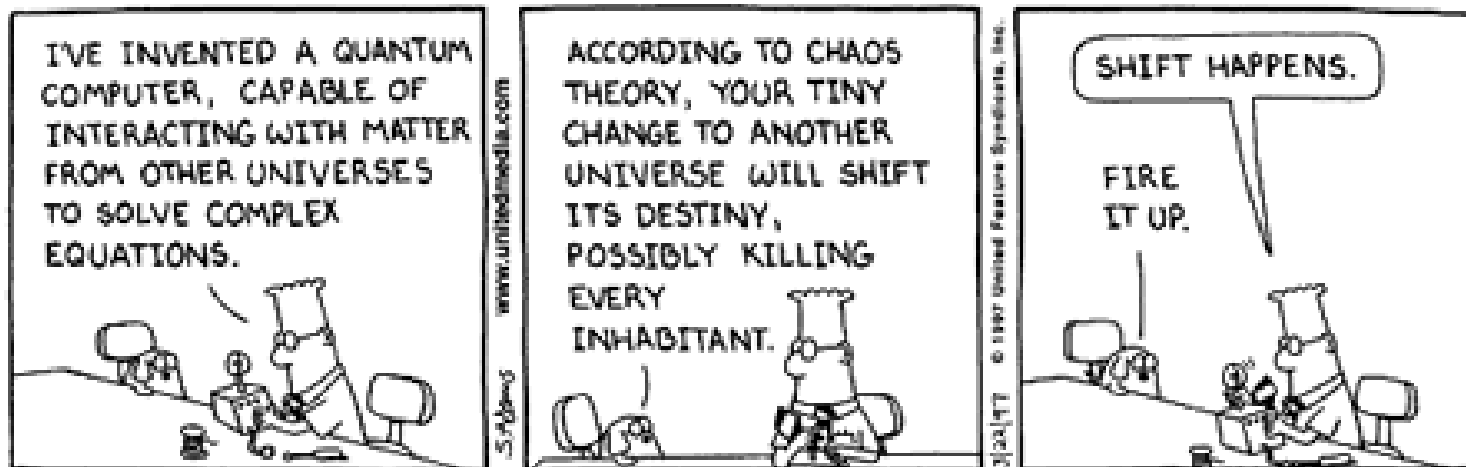
Választható tárgy (tavasszal indul)
Bevezetés a kvantum informatikába és kommunikációba

<https://www.vik.bme.hu/kepzes/targyak/VIHIAV06/>

BME Hálózati Rendszerek és Szolgáltatások Tanszék
<http://www.mcl.hu/quantum/>

Publikációk angolul:
<http://arxiv.org/archive/quant-ph>

Kérdések?



bacsardi@hit.bme.hu