Cryptonite, 2014. január 8.

Kvantummechanika hatása a kriptográfiára

Bacsárdi László

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

BME Mobil Kommunikáció és Kvantumtechnológiák Laboratórium,
óraadó

4

Kvantuminformatika

Kvantumszámítógép

4

Shor-algoritmus

Ami még izgalmasabb

2014.01.02

The Washington Post PostTV Politics Opinions Local Sports National World Busi

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

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.

Forrás: http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html

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

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

Rydberg-formula

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

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

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


HEY, SCHRÖDINGER. WHAT'S IN THE BOX?
MY CAT.
OH. IS IT ALIVE OR DEAD?
YES.
2011© www.ALittleWhiteNoise.com

Szuperpozíció

Szuperpozíció

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

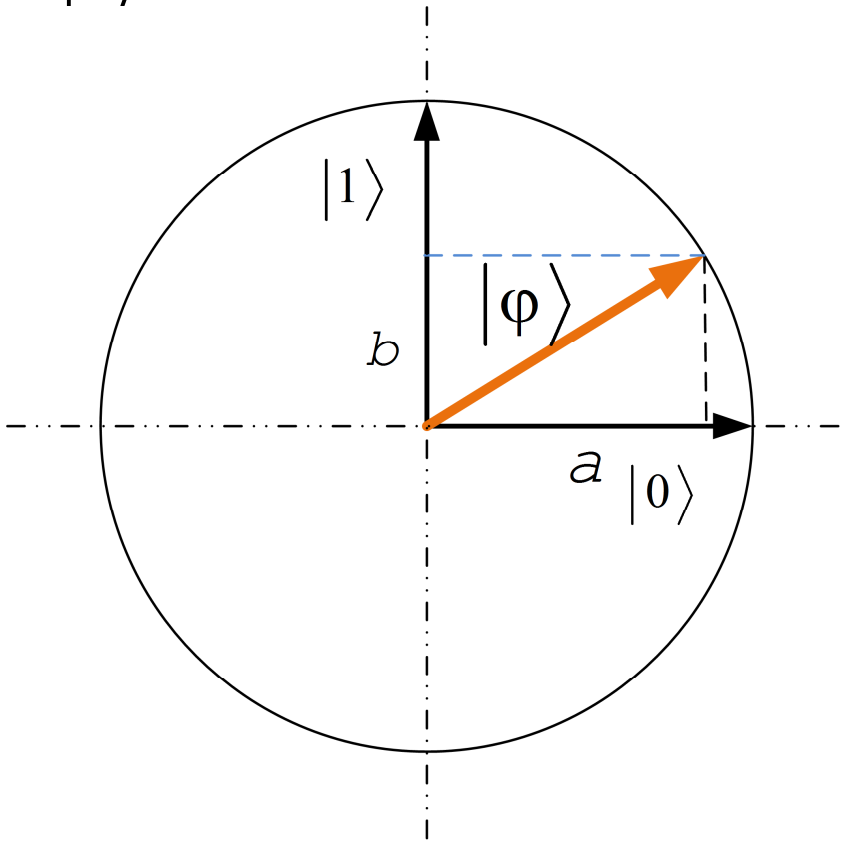
$a, b \in C$ $\qquad$ $|a|^2 + |b|^2 = 1.$

Szuperpozíció

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

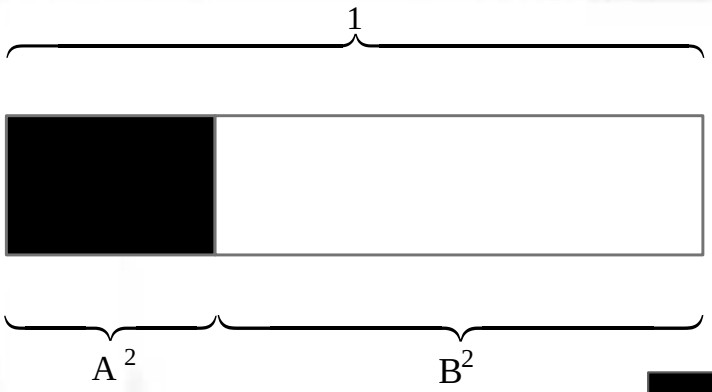
$$|a|^2 + |b|^2 = 1.$$

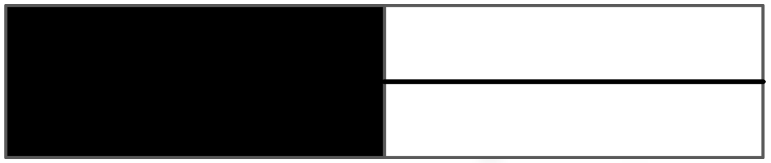
$$a, b \in C$$



L. Bacsardi, M. Galambos, S. Imre, A. Kiss. "Quantum Key Distribution over Space-Space Laser Communication Links," AIAA Space 2012, Pasadena, California, Sept, 2012.

Szuperpozíció





$|0\rangle$

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

$|1\rangle$

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

M. Galambos, S. Imre, “Visualizing the Effects of Measurements and Logic Gates On Multi-Qubit Systems Using Fractal Representation,” *International Journal on Advances in Systems and Measurements,* Vol. 5, No. 1-2, 2012, pp. 1–10.

A kvantummechanika posztulátumai (1)

1. **Állapotleírás**

   Zárt fizikai rendszer aktuális állapota egy olyan $|\varphi\rangle \in \mathrm{H}$ 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:

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

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

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

A mérés után a rendszer állapota az alábbi lesz

$$|\varphi\rangle' = \frac{\mathrm{M}_x|\varphi\rangle}{\sqrt{\mathrm{p}_x}}$$

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

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

Alap építőkövek

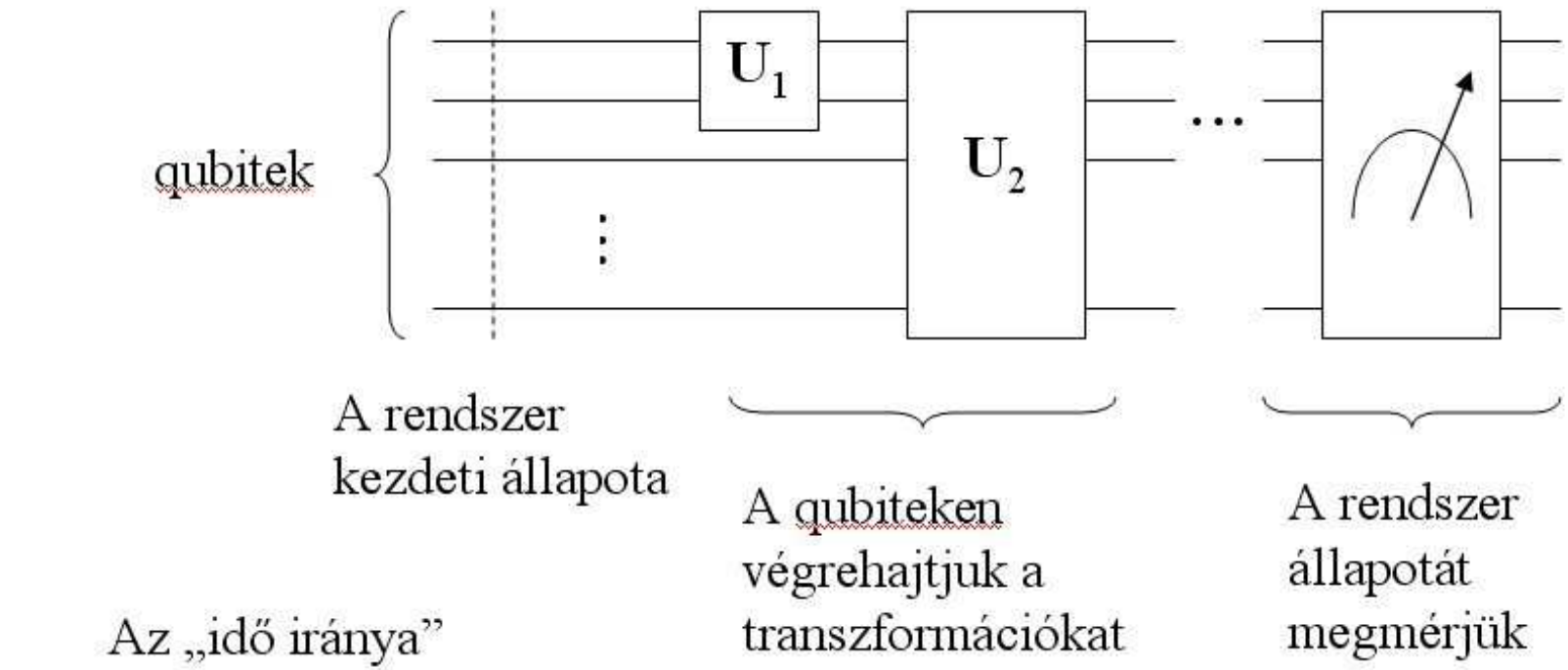
Különböző kvantumkapuk, amelyek a $|\varphi\rangle = a|0\rangle + b|1\rangle$ bemenetre az alábbi kimeneti kvantumbitet állítják elő

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

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

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

Kvantum-áramkör



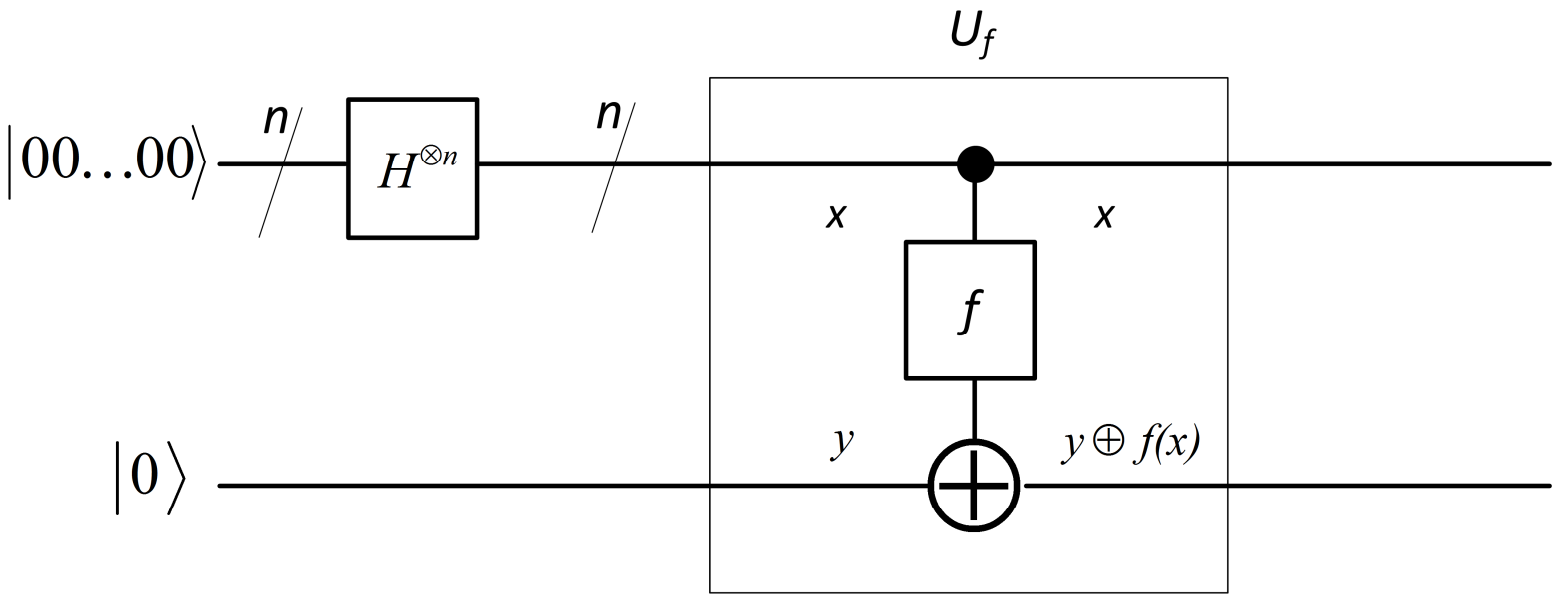
Kvantumpárhuzamosság

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

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

$$|\varphi\rangle = a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle + e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle$$

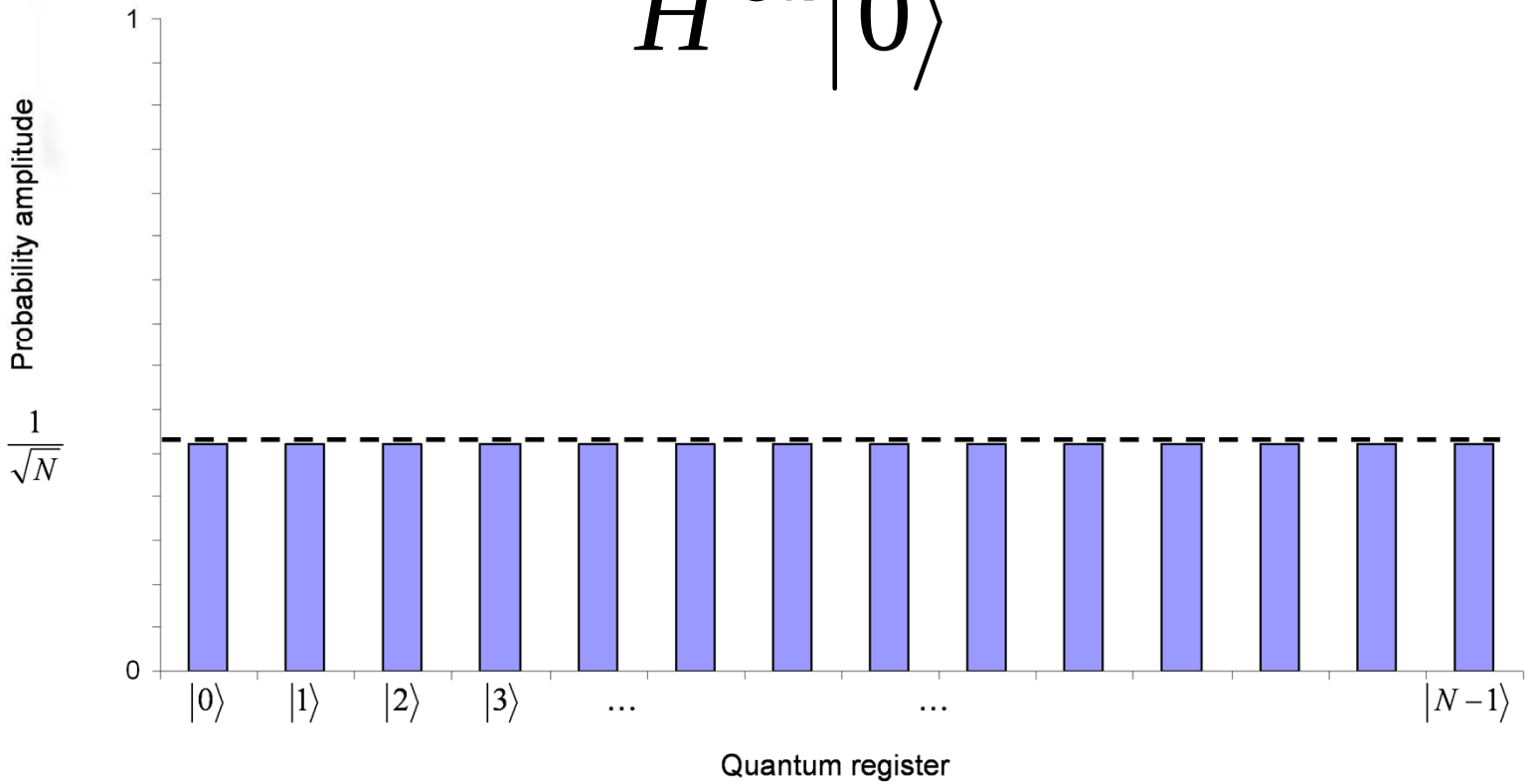
Kvantumpárhuzamosság



Ábra: Bacsárdi L., Galambos M., Imre S., „Kvantumalapú algoritmusok”. Informatikai algoritmusok, III. kötet, pp. 1785-1827. *Mondart Kiadó., 2013*

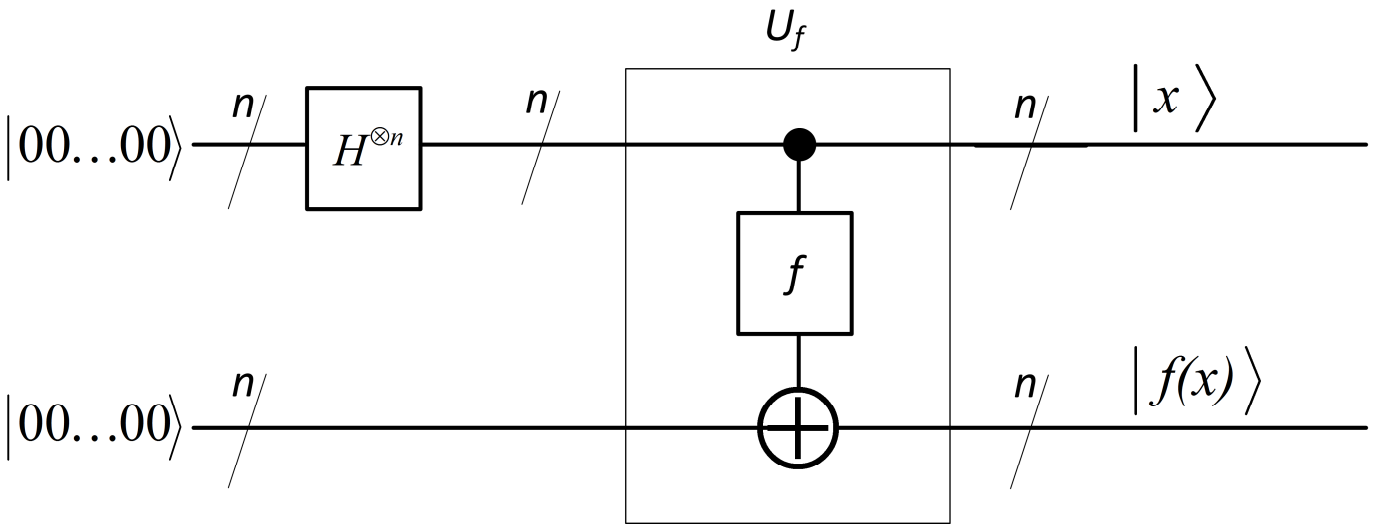
Kvantumpárhuzamosság

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



Ábra: Bacsárdi L., Efficient Quantum Based Space Communications.. LAP , 2013

Kvantumpárhuzamosság



Ábra: Bacsárdi L., Galambos M., Imre S., „Kvantumalapú algoritmusok”. Informatikai algoritmusok, III. kötet, pp. 1785-1827. *Mondart Kiadó., 2013*

Kvantumpárhuzamosság

Deutsch-Jozsa algoritmus

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

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

Kiegyensúlyozott?

Konstans?

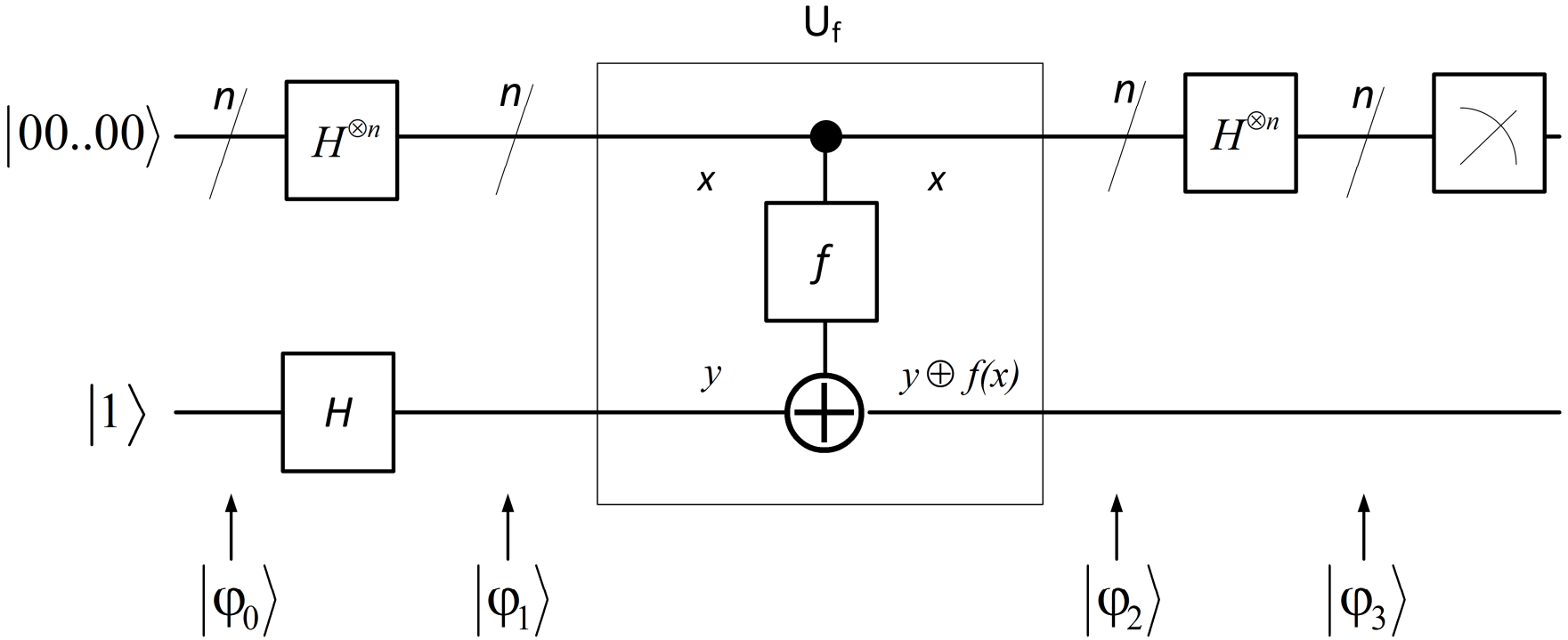
Ábra: Bacsárdi L., Galambos M., Imre S., „Kvantumalapú algoritmusok”. Informatikai algoritmusok, III. kötet, pp. 1785-1827. *Mondart Kiadó., 2013*

Kvantum párhuzamosság

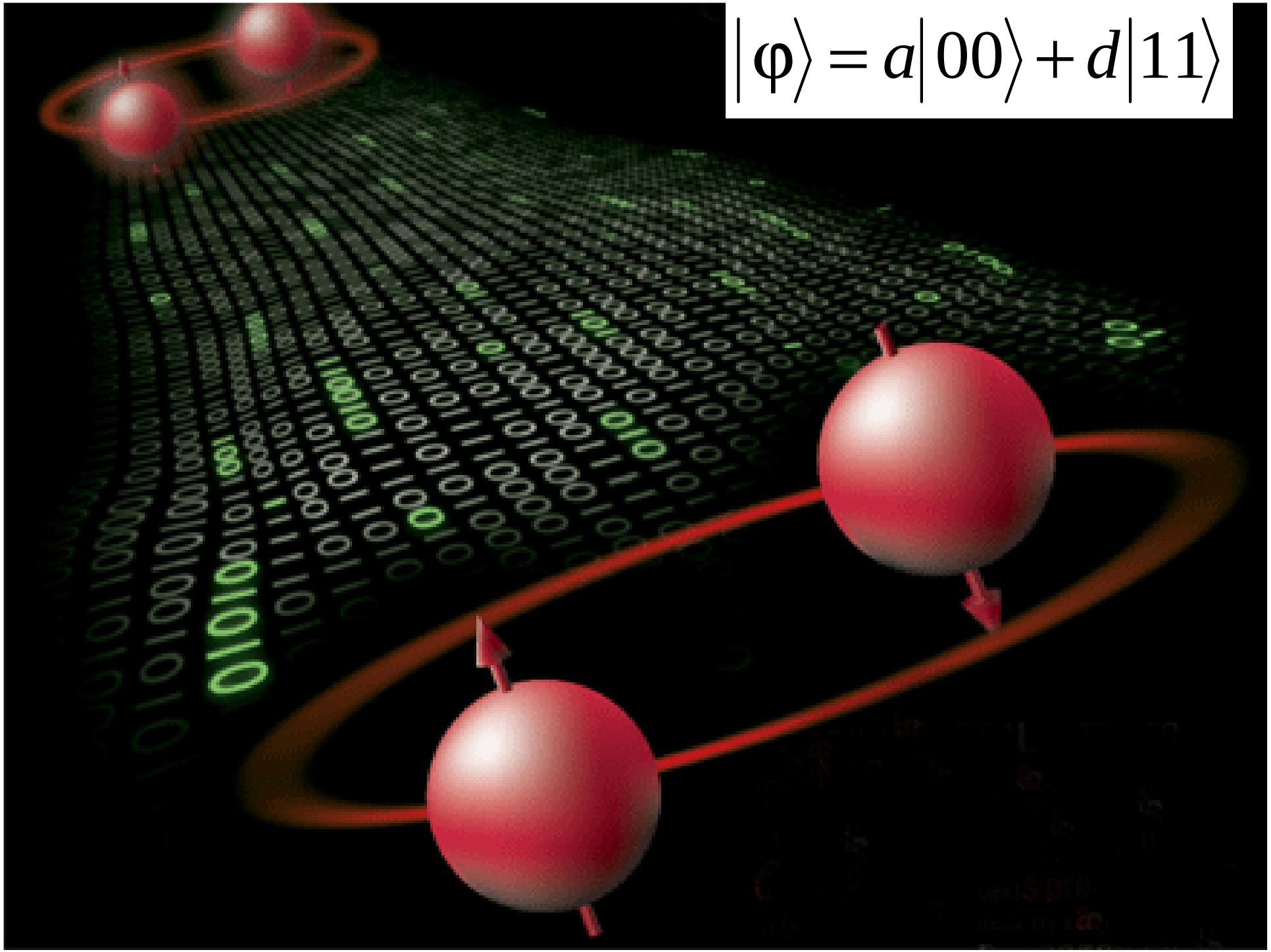
Deutsch-Jozsa algoritmus

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

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

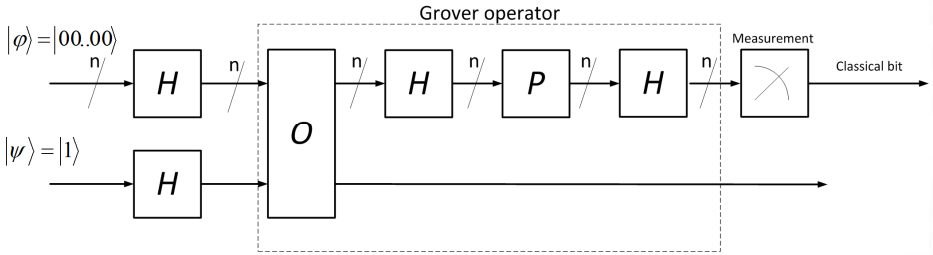


Ábra: Bacsárdi L., Galambos M., Imre S., „Kvantumalapú algoritmusok”. Informatikai algoritmusok, III. kötet, pp. 1785-1827. *Mondart Kiadó., 2013*


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

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

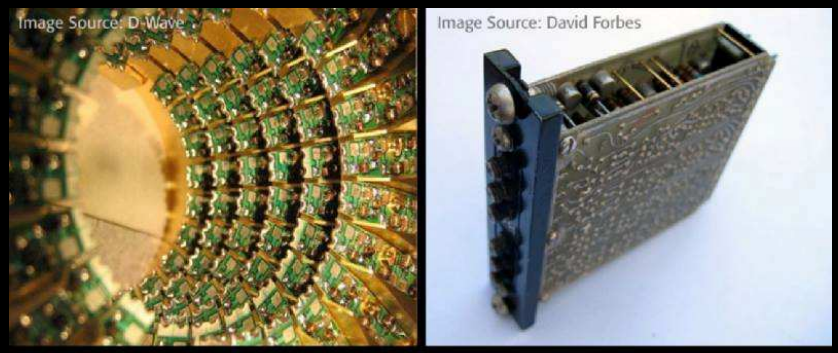
"I still don't understand quantum theory."

© Original Artist / Search ID: mshn197

Rights Available from CartoonStock.com

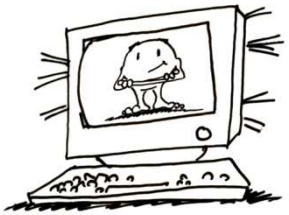
Kvantuminformatika

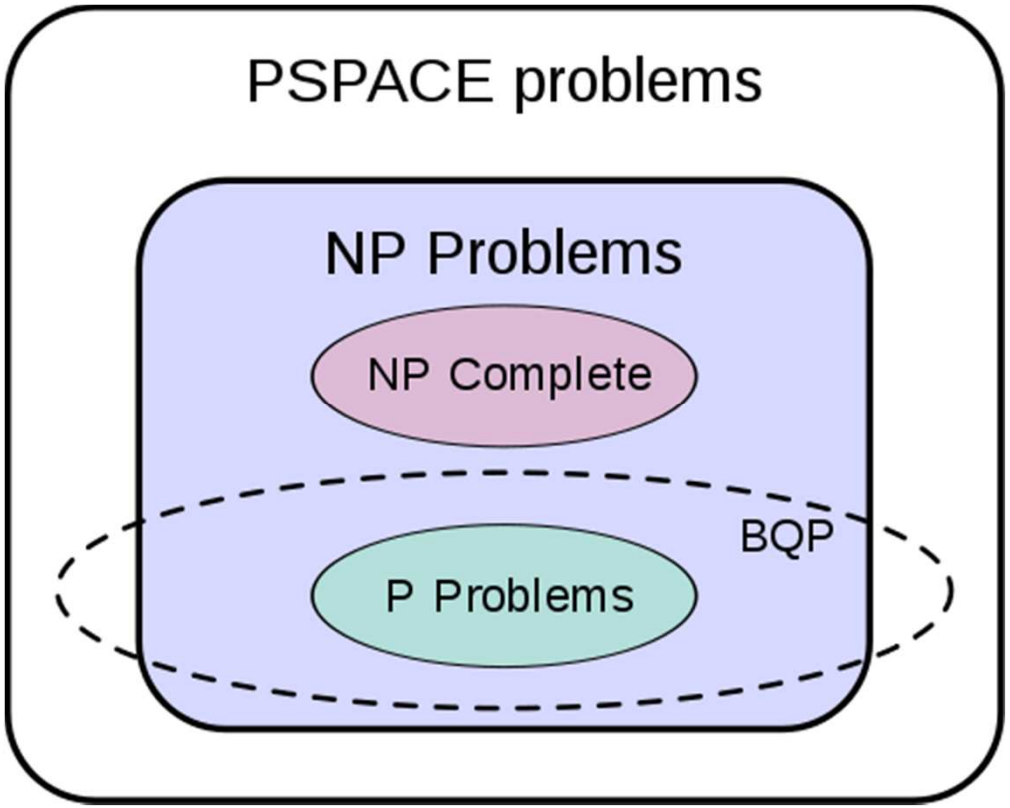
Kvantumszámítógép



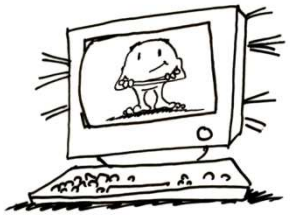
Shor-algoritmus

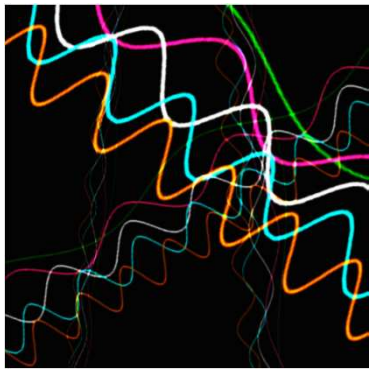
Ami még izgalmasabb

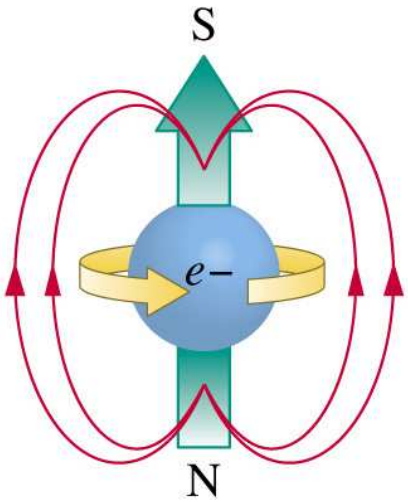



PSPACE problems
NP Problems
NP Complete
BQP
P Problems

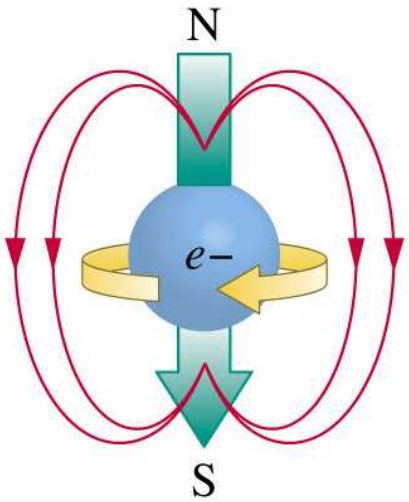
Mi lehet kvantumbit?



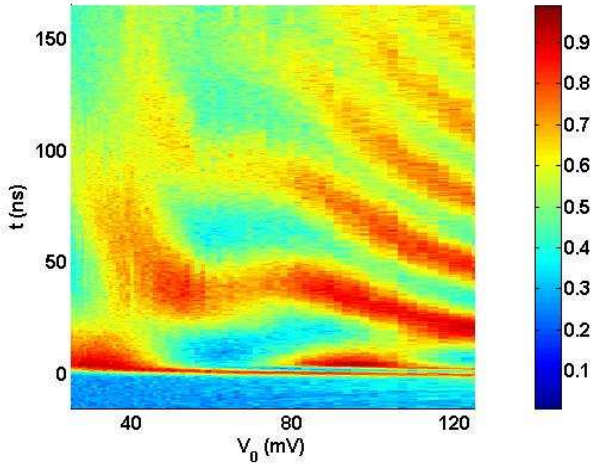




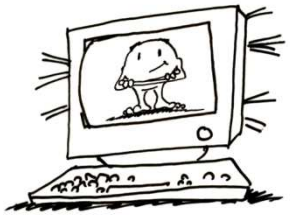
$m_s = +\frac{1}{2}$

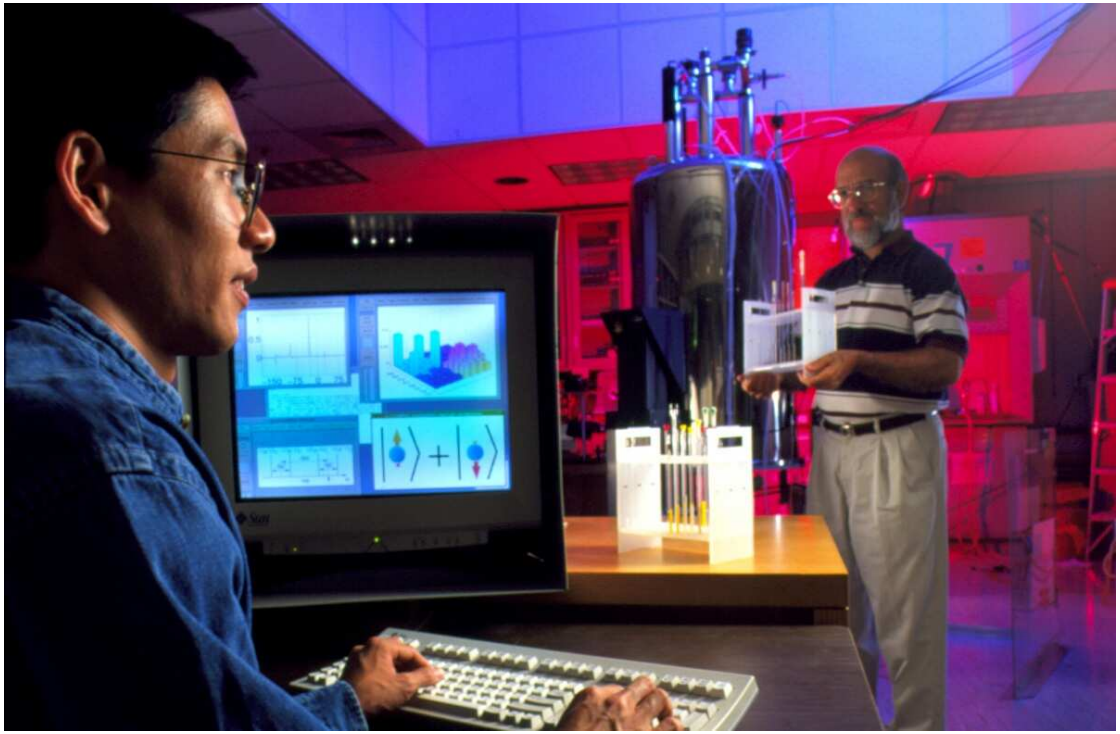


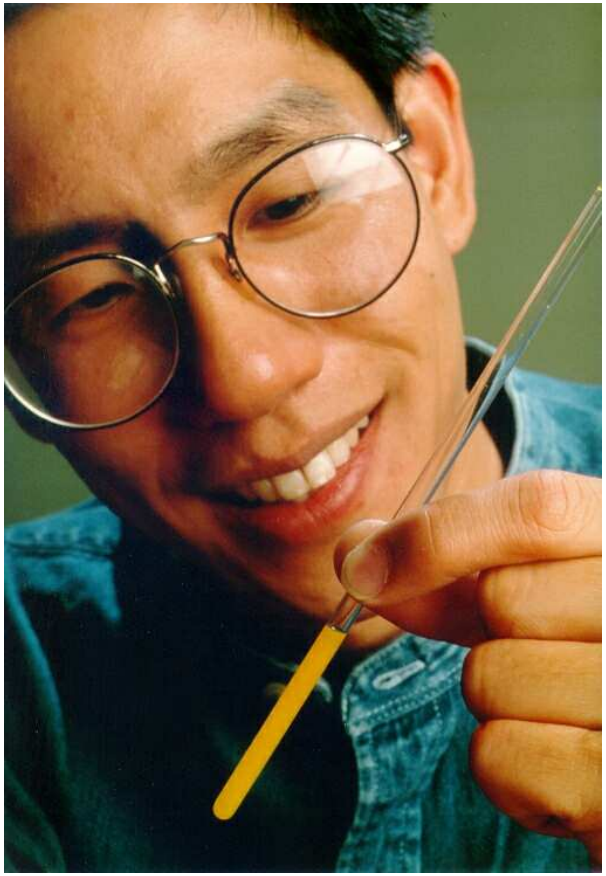
$m_s = -\frac{1}{2}$



Kvantum eszközök (1)

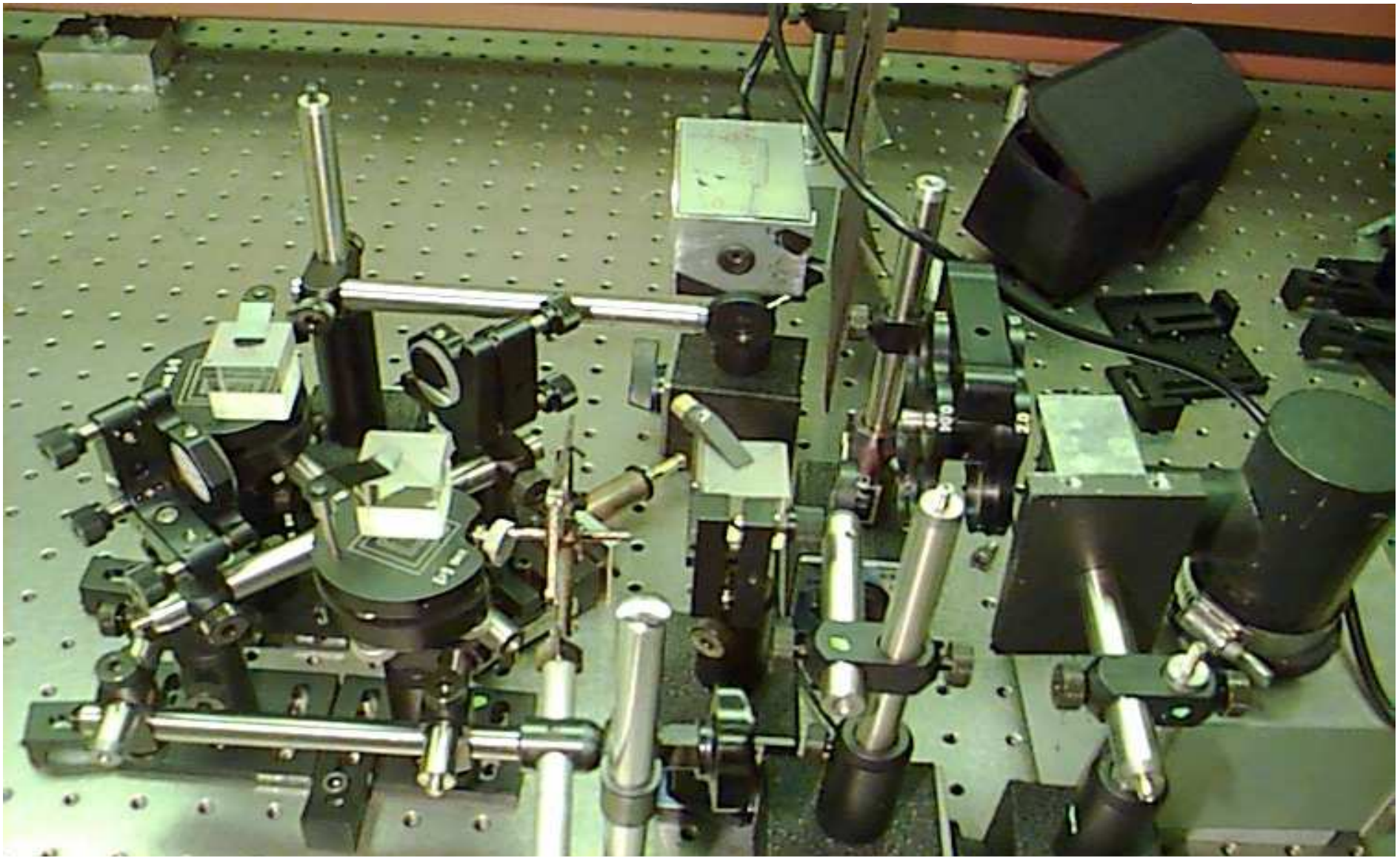




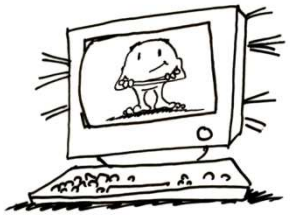


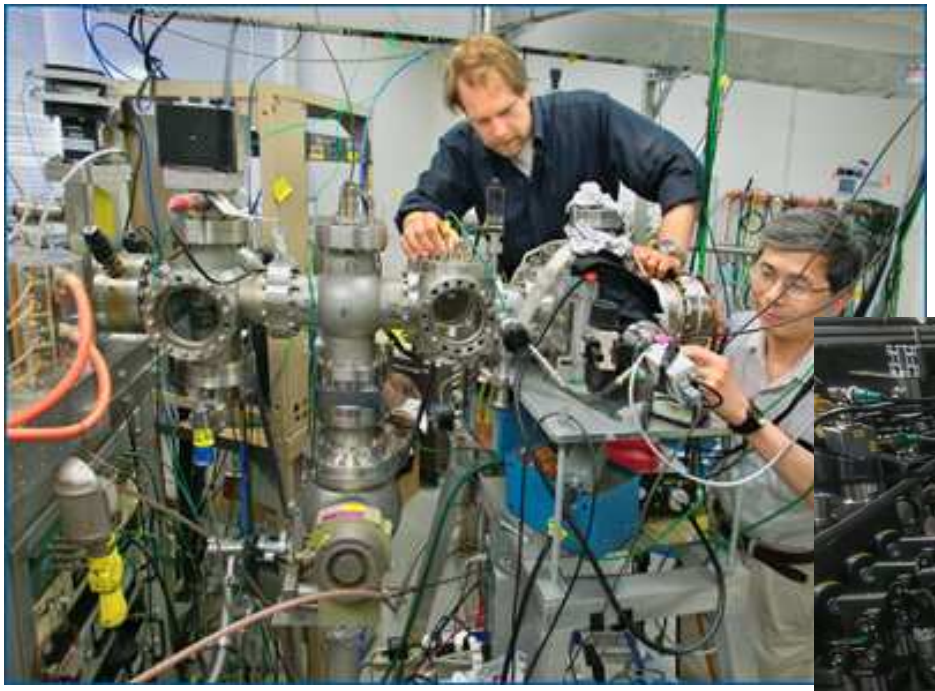
Képek forrása: *IBM's* Almaden Research Center (San Jose, CA.),

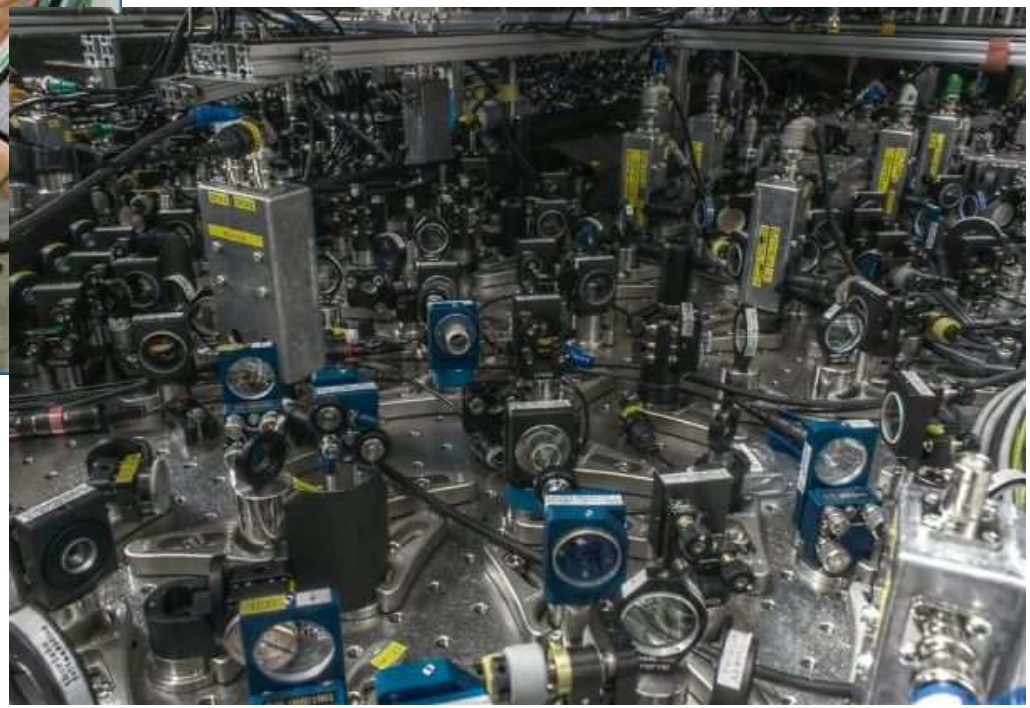
Kvantum eszközök (2)



Kvantum eszközök (3)

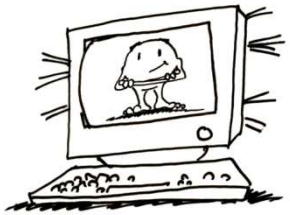




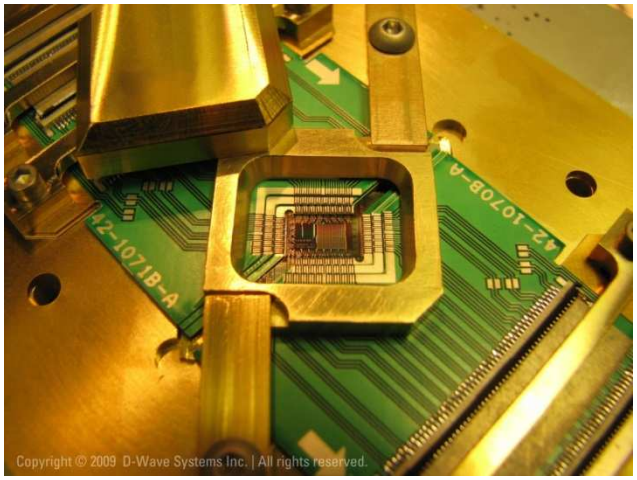


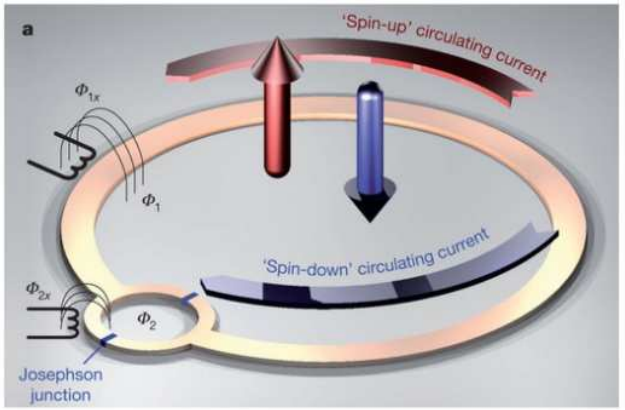
Fénykép: Roy Kaltschmidt, forrás: http://www.lbl.gov/Science-Articles/Archive/sabl/2005/June/02-quantum-comp.htm
Forrás: http://wikis.lib.ncsu.edu/index.php/Image:Quantum_Computer.jpg

D-Wave
The Quantum Computing Company™

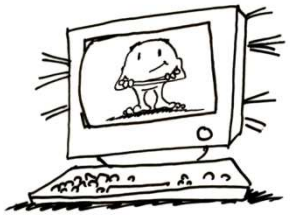


- Fluxuskvantumokon alapuló adiabatikus rendszer
- 2007 Orion Systems, 16 kvantumbites gép bemutatója három alkalmazással:
  - Adatbázis keresés
  - Ülésrend tervezés
  - Sudoku fejtés
- 2009 Neural Information Processing Systems Conference
  - Képfelismerő rendszer betanítása





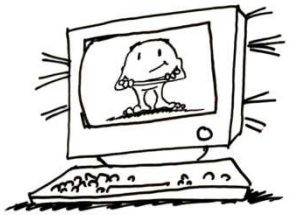
D:wave
The Quantum Computing Company™



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

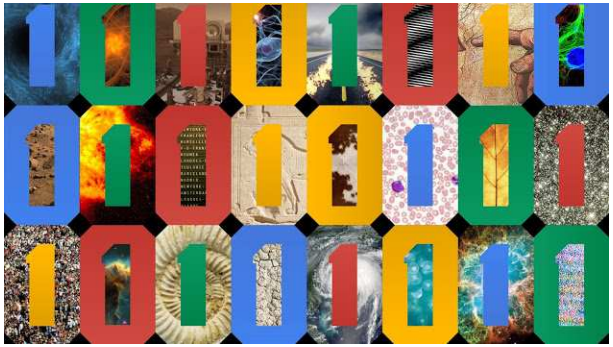
D-Wave

The Quantum Computing Company™



LOCKHEED MARTIN

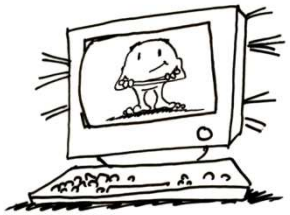
NASA QuAIL

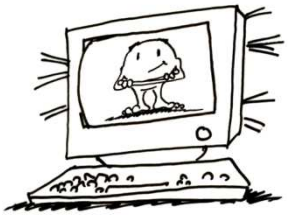


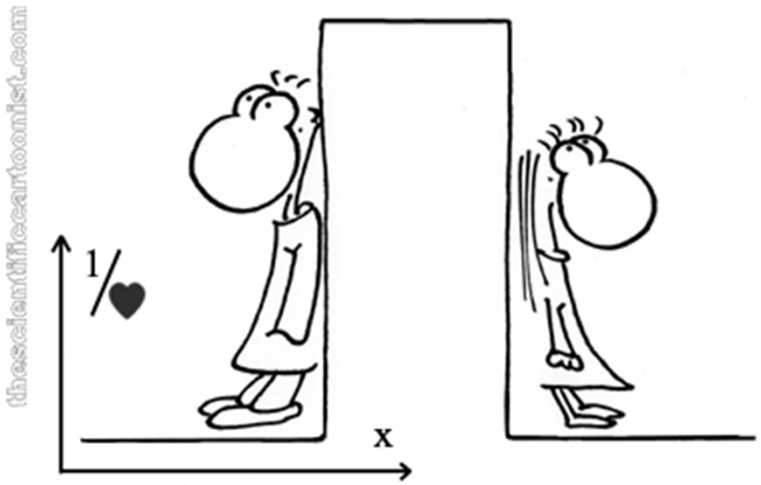
QUANTUM ARTIFICIAL INTELLIGENCE LABORATORY


Google & NASA's
Quantum Computer
D-Wave
So...that's a Quantum Computer?

Videó





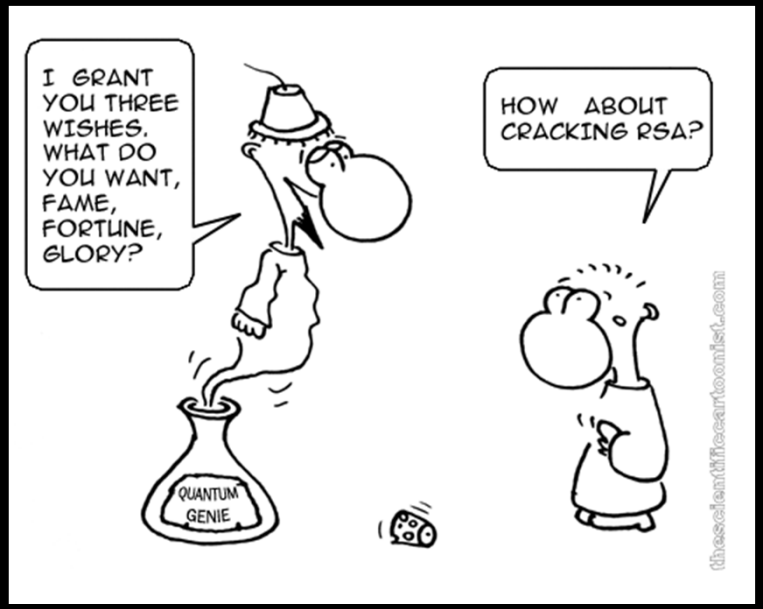


thescientificcartoonist.com

Waiting for the tunnel effect.

Kvantuminformatika

Kvantumszámítógép



Shor-algoritmus

Ami még izgalmasabb

RSA törése

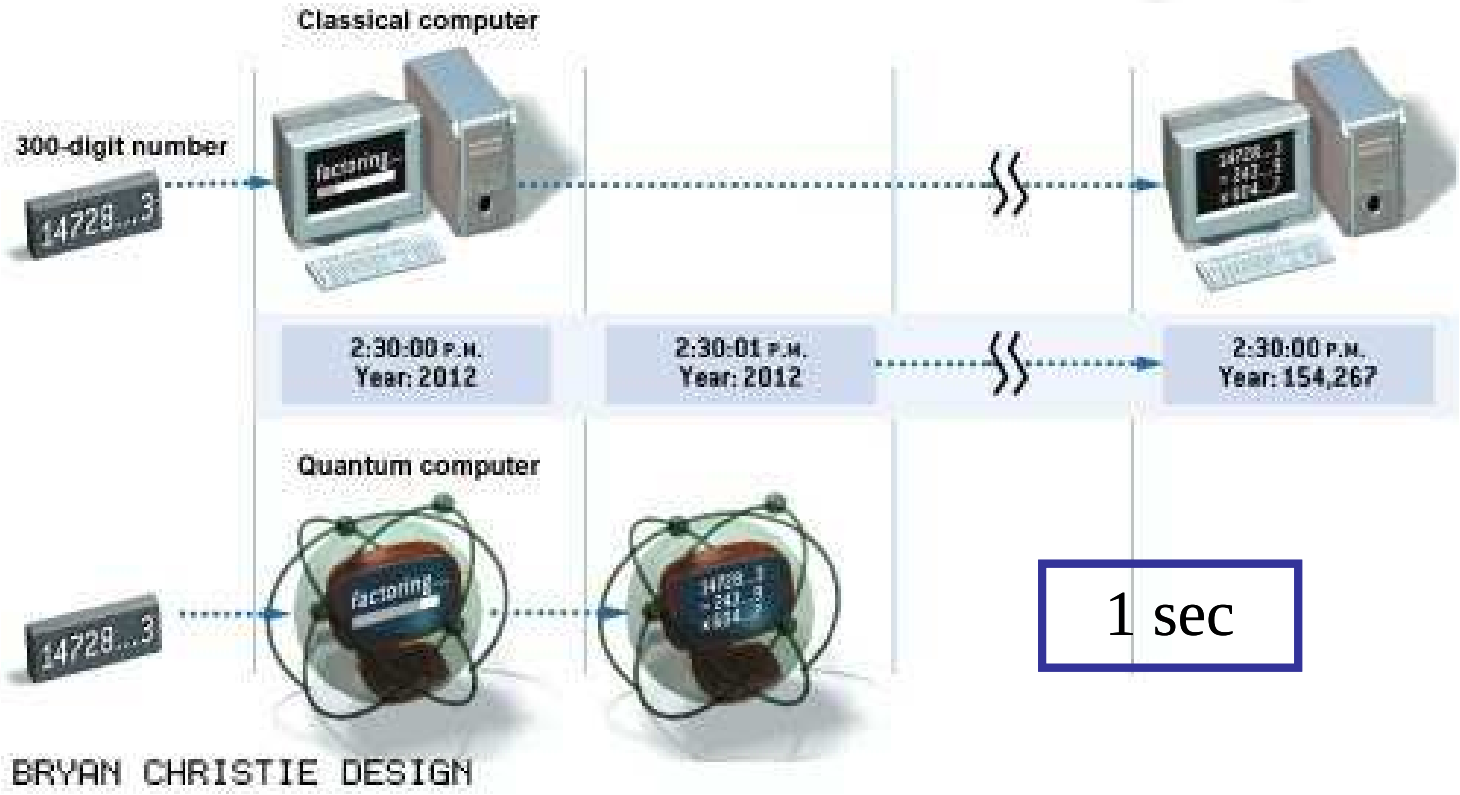
$$O\left(\log^3(N)\right)$$

152 000 év

Shor-algoritmus és az RSA feltörése

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

152 000 év



1 sec

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 kvantumos rendszerekben négyzetes növekményű végrehajtási időt igényel

$$\mathrm{O}\left(\mathrm{ld}^3(N)\right)$$

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

Rendkeresés

Vegyünk két pozitív egész számot $x < N$, amelyek relatív prímek, vagyis $\text{lnko}(x, N) = 1$.

Az *x* multiplikatív rendjét modulo *N* definiáljuk úgy, mint a legkisebb *r* számot, amelyre igaz, hogy

$$x^r \bmod N = 1 \text{ és } 1 < r < N$$

Rend szoros kapcsolatban a periodicitással:

$$f(z) = x^z \bmod N$$

$$f(z+r) = x^{z+r} \bmod N = \left(x^z \bmod N\right)\left(x^r \bmod N\right) \bmod N = f(z)$$

Rendkeresés

A

Rendkeresés

Ha *A* páros, 2-vel osztjuk, amíg páratlan B_1

$x_1 < B_1$ véletlenszerűen választott egész

$\mathrm{lnko}(x_1, B_1) = b_1$ és nem relatív prím x_1,B_1

$$B_2 = B_1 / b_1$$

ismételve *n*-szer, amíg b_1=1, ekkor b_n=N

Rendkeresés

Tegyük fel, hogy az *r*=*x* mod *N* multiplikatív rend páros: $y \equiv x^{r/2}$

$$y \bmod N = 1$$

$$\left(y^2 - 1\right) \bmod N = 0$$

$$\left(y - 1\right)\left(y + 1\right) \bmod N = 0$$

$$\left(\left(y - 1\right) \bmod N\right)\left(\left(y + 1\right) \bmod N\right) \bmod N = 0 \qquad 0 \le b_{+1}, b_{-1} < 1$$

b_{+1} b_{-1}

$$c_{+1} \equiv \text{lnko}\left(b_{+1}, N\right), c_{-1} \equiv \text{lnko}\left(b_{-1}, N\right)$$

Rendkeresés

$$\underbrace{((y-1) \bmod N)}_{b_{+1}}\underbrace{((y+1) \bmod N)}_{b_{-1}} \bmod N = 0$$

csak három módon

$$b_{+1} = 0, \text{ekkor } c_{+1} = N, b_{-1} = N-2, c_{-1} = 1$$

$$b_{-1} = 0, \text{ekkor } c_{-1} = N, b_{+1} = 2, c_{+1} = 1$$

$$b_{+1}b_{-1} = kN, 0 < k < N \Rightarrow 0 < b_{-1} < b_{+1} < 1$$

Egyik sem osztója *N*-nek, de kell, hogy legyen közös osztója a $b_{+1}b_{-1}$ szorzatnak *N*-nel: c_{-1}, c_{+1}

Ha *x*-re nem teljesül, hogy $0 \le c_{+1}, c_{-1} < 1$

akkor új *x*-et kell választani, hogy a többi prímtényezőt is megtaláljuk.

Honnan tudjuk az *r* rendet?

Válasz: Shor-algoritmus

P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM Journal on Computing, Vol. 26, No. 5, pp. 1484–1509, 1997.

Shor-algoritmus

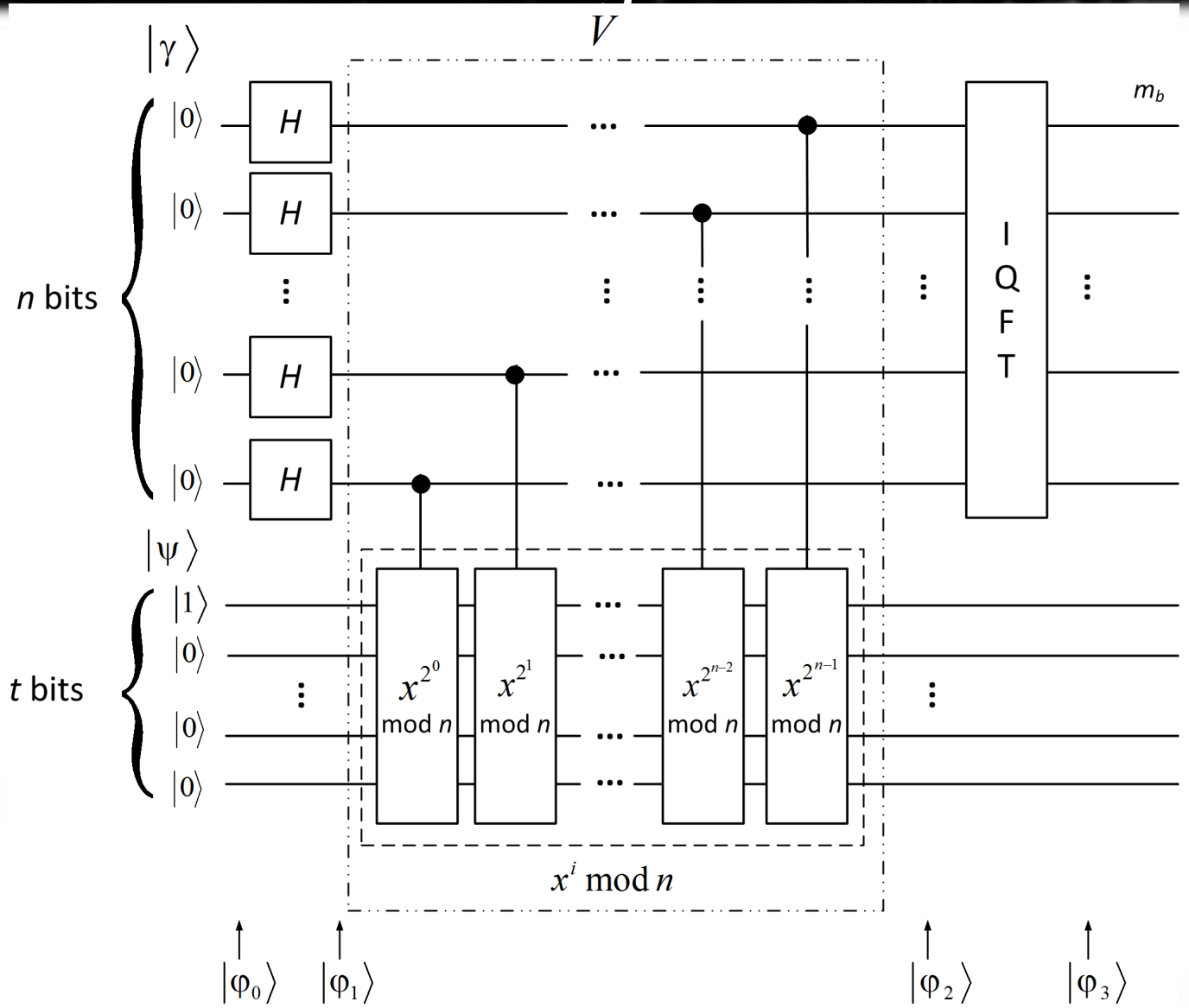
1. Kiszámolni az összes: $x^k \bmod N, 0 \le k < N$

   tárolni a *k* értékkel együtt két kvantumregiszterben

2. Erősíteni a kívánt állapotot: $\left| x^k \bmod N = 1 \right\rangle$

3. Mérés a második regiszteren. Nagy valószínűséggel a keresett *r* rendet adja vissza

Shor-algoritmus



Shor-algoritmus (klasszikus kód – 1)

```
qcl> shor(15)
: chosen random x = 4
: measured zero in 1st register. trying again ...
: chosen random x = 11
: measured 128 , approximation for 0.500000 is 1 / 2
: possible period is 2
: 11 ^ 1 + 1 mod 15 = 12 , 11 ^ 1 - 1 mod 15 = 10
: 15 = 5 * 3
```

Forrás: http://tph.tuwien.ac.at/~oemer/doc/quprog/node18.html

Shor-algoritmus (klasszikus kód – 2)

```
procedure shor(int number) {
  int width=ceil(log(number,2));   // size of number in bits
  qureg reg1[2*width];             // first register
  qureg reg2[width];               // second register
  int qmax=2^width;
  int factor;                      // found factor
  int m; real c;                   // measured value
  int x;                           // base of exponentiation
  int p; int q;                    // rational approximation p/q
  int a; int b;                    // possible factors of number
  int e;                           // e=x^(q/2) mod number

 if number mod 2 == 0 { exit "number must be odd"; }
  if testprime(number) { exit "prime number"; }
  if testprimepower(number) { exit "prime power"; };
```

Forrás: http://tph.tuwien.ac.at/~oemer/doc/quprog/node18.html

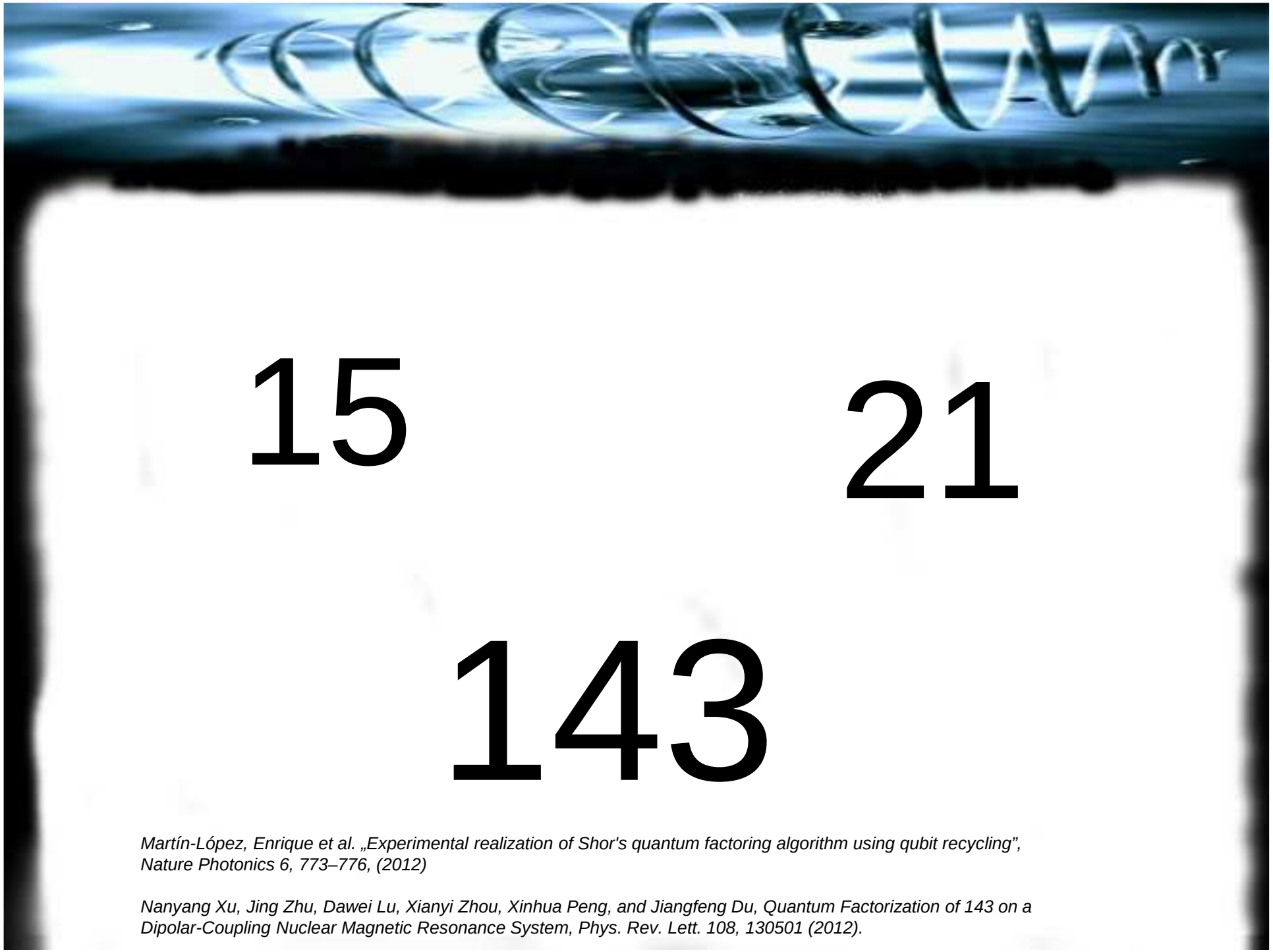
Shor-algoritmus (klasszikus kód – 3)

```
{
   {                                  // generate random base
     x=floor(random()*(number-3))+2;
   } until gcd(x,number)==1;
   print "chosen random x =",x;
   Mix(reg1);                         // Hadamard transform
   expn(x,number,reg1,reg2);          // modular exponentiation
   measure reg2;                      // measure 2nd register
   dft(reg1);                         // Fourier transform
   measure reg1,m;                    // measure 1st register
   reset;                             // clear local registers
```

Forrás: http://tph.tuwien.ac.at/~oemer/doc/quprog/node18.html

Shor-algoritmus (klasszikus kód – 4)

```
if m==0 {                       // failed if measured 0
      print "measured zero in 1st register. trying again ...";
    } else {
      c=m*0.5^(2*width);            // fixed point form of m
      q=denominator(c,qmax);        // find rational approximation
      p=floor(q*m*c+0.5);
      print "measured",m,", approximation for",c,"is",p,"/",q;
      if q mod 2==1 and 2*q<qmax { // odd q ? try expanding p/q
        print "odd denominator, expanding by 2";
        p=2*p; q=2*q;
      }
      if q mod 2==1 {               // failed if odd q
        print "odd period. trying again ...";
      } else {
        print "possible period is",q;
        e=powmod(x,q/2,number);     // calculate candidates for
        a=(e+1) mod number;         // possible common factors
        b=(e+number-1) mod number; // with number
        print x,"^",q/2,"+ 1 mod",number,"=",a,",",
              x,"^",q/2,"- 1 mod",number,"=",b;
        factor=max(gcd(number,a),gcd(number,b));
      }    }
  } until factor>1 and factor<number;
  print number,"=",factor,"*",number/factor; }
```



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).

Post-quantum

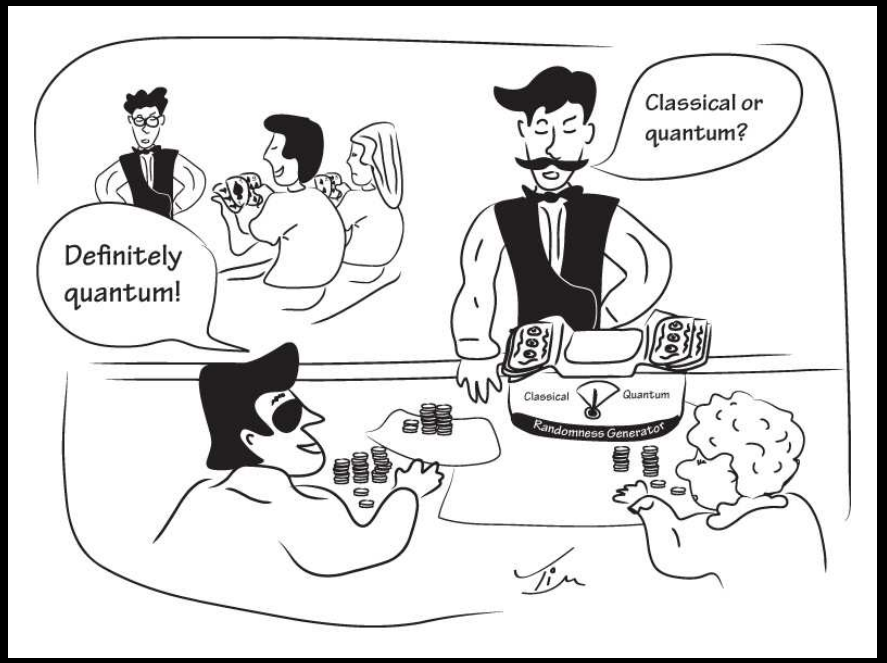
- lattice problems
- closest vector problem
- combinatoric group theory
- solution of multi-variate quadratic systems over finite fields

- lattice based signatures
- code based signatures (Courtois, Finiasz, and Sendrier)
- signatures from Multi-Variate Quadratic Systems
- Okamoto et al.: public-key systems that use quantum computers in the key generation process.

K. Tanaka und S.Uchiyama T.Okamoto, Quantum public key cryptosystems, Proc. Of CRYPTO 2000, LNCS 1880 (2000), 147–165, SpringerVerlag.
Johannes Buchmann et al., Post-Quantum Signatures, 2004

Kvantuminformatika

Kvantumszámítógép



Shor-algoritmus

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

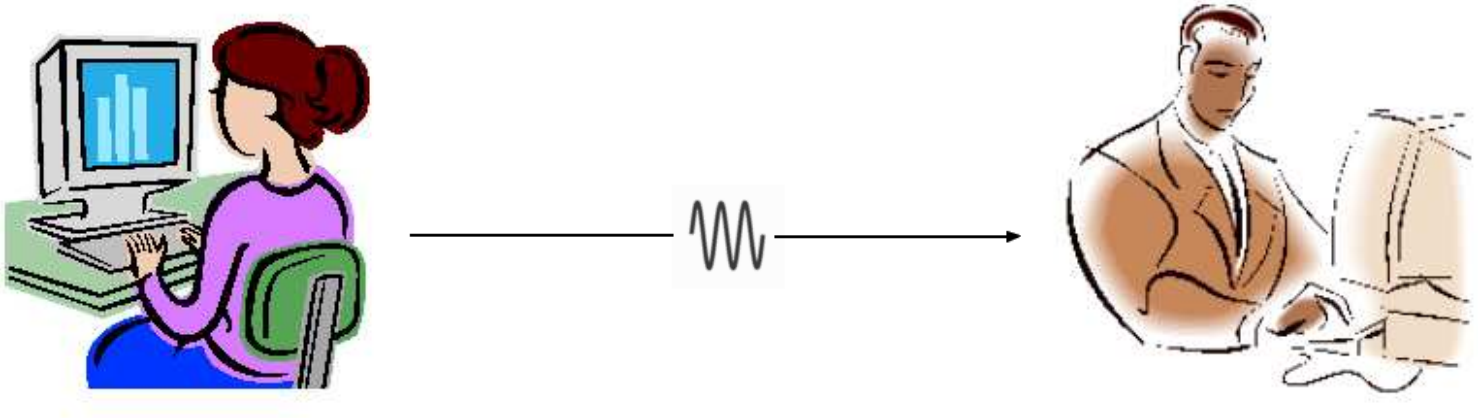
BB84

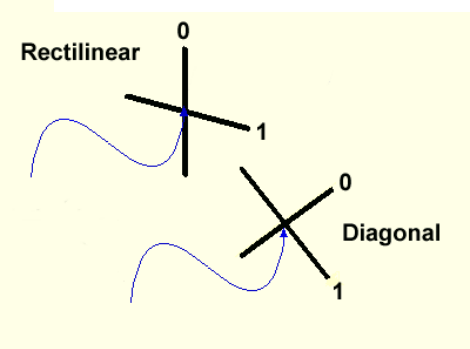
B92

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

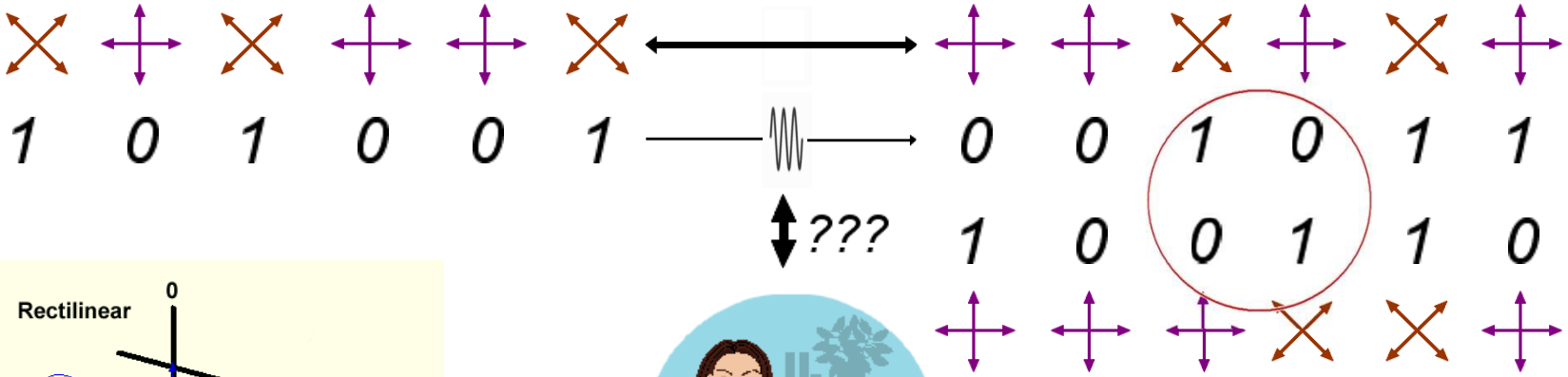


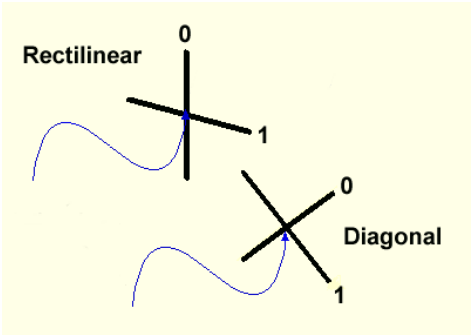


Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/index.html
Charles H. Benett, Gilles Bassard, 'Quantum Crryptography: Public Key Distribution and Coin Tossing', International Conference on Computers, Systems & Signal Processing, Bangalore, India (December 10-12, 1984)

BB84 protokoll

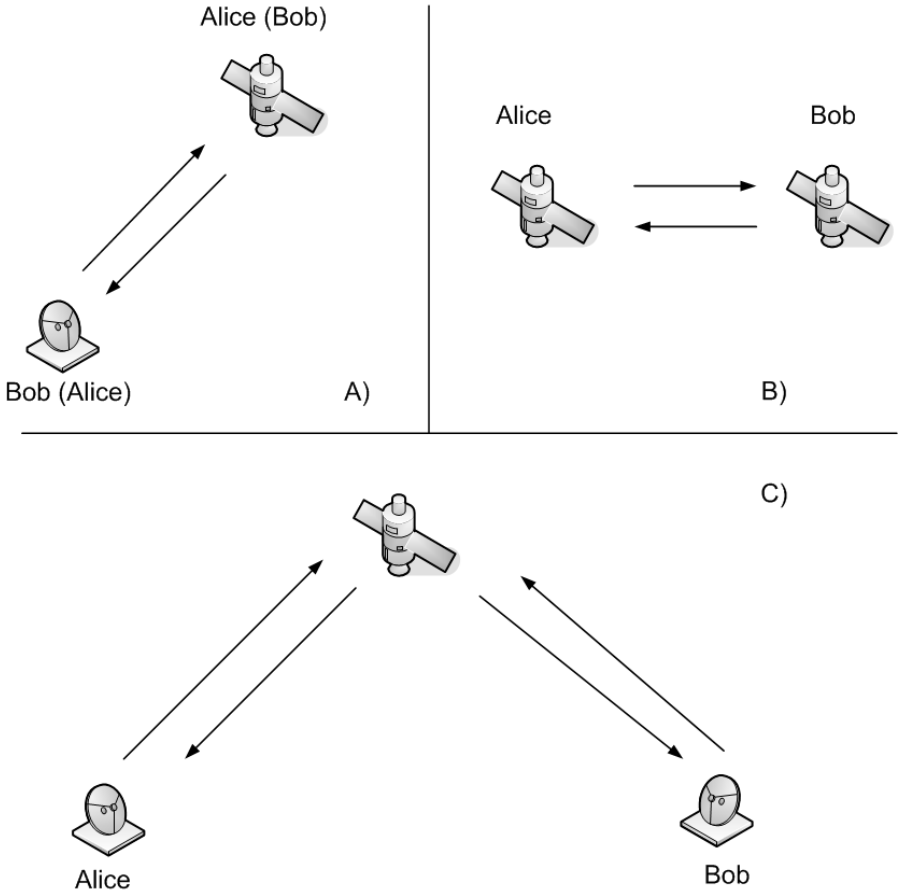




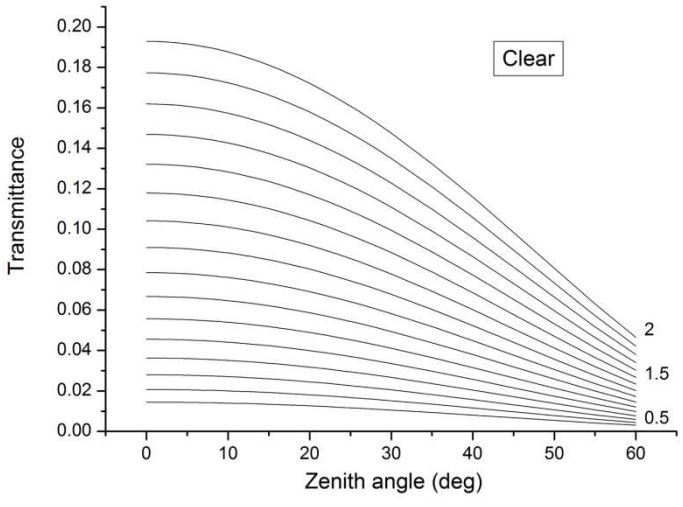
http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/index.html

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

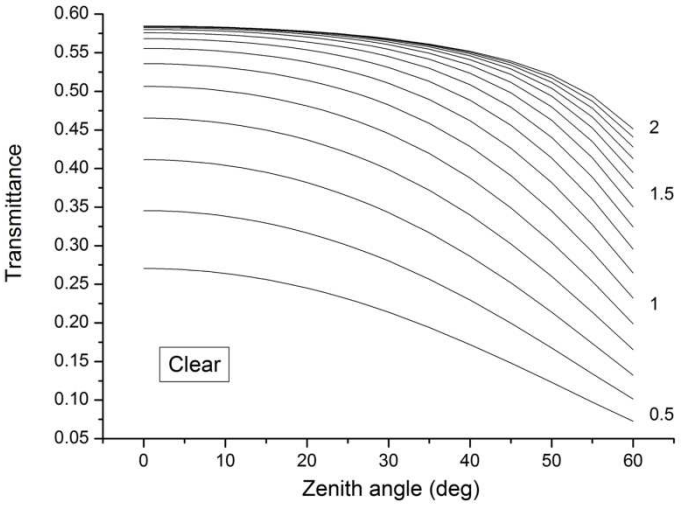
Irány az űr



L. Bacsardi, „On the way to Quantum Based Satellite Communication”, IEEE Communications Magazine, 51:(08) pp. 50-55.



A



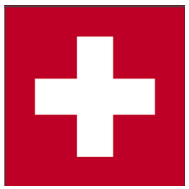
B

L. Bacsardi, „On the way to Quantum Based Satellite Communication", IEEE Communications Magazine, 51:(08) pp. 50-55.

Cégek

- D-wave :
  - Kanadai cég
  - 1999-ben alapították
  - Állításuk szerint kvantumszámítógépet árulnak

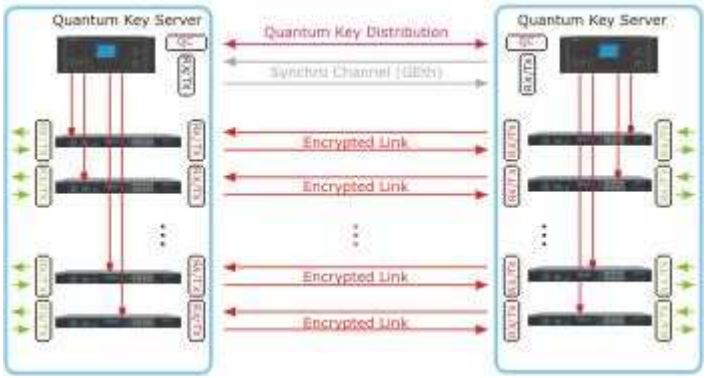
- IdQuantique
  - Svájci cég
  - Senatas-al együttműködésben
  - 2001 óta létezik, University of Geneva Spinoff
  - Kvantum kulcsszétosztás, randomszám generálás



- MagiQ Technologies
  - Amerikai
  - 1999-ben alapították
  - Kvantum kulcsszétosztás

- Quintessence Labs
  - Amerikai-ausztrál együttműködés
  - Kulcsszétosztás, randomszám generálás

Id Quantique



Cerberis

- Hibrid rendszer
- Kvantum:
  - BB84
  - SARG
- Klasszikus:
  - AES (Advanced Encryption Standard) 256-bit
  - CFB mode (1 Gbps-ig)
  - CTR mode (10 Gbps-ig)
- Dark fiber vagy wavelength-division multiplexing (WDM) kábel
- 50 km-ig (kérésre 100 km)
- Prototípus 250 km-ig

Forrás: Galambos Máté előadása (BME)

Id Quantique

USB


PCI


PCI Express

OEM

Quantis

- Kvantum alapú randomszám generátor
- USB
  - 4 Mbits/sec
- PCI Express (PCIe) kártya
  - 4 Mbits/sec
- PCI kártya
  - 4 Mbits/sec
  - 16 Mbits/sec
- OEM (Original Equipment Manufacturer)
  - 4 Mbits/sec

Forrás: Galambos Máté előadása (BME)

MagiQ

Q-Box Workbench

- Point-to-point kommunikáció optikai és ethernet kábelen
- Hibrid rendszer
- BB84
- 3DES, AES
- Kulcsfrissítés 1000 bit/s-ig
- 50 km maximális linktávolság
- Valódi random szám generátor

From Computer Desktop Encyclopedia
© 2005 MagiQ Technologies

MagiQ

QPN 8505 Security Gateway

- Multi-Site Network Security
- Másodpercenként 100-szor frissíthető 256 bites kulcsok
- Intrusion Detection
- Hibrid rendszer
- BB84
- 3DES, AES

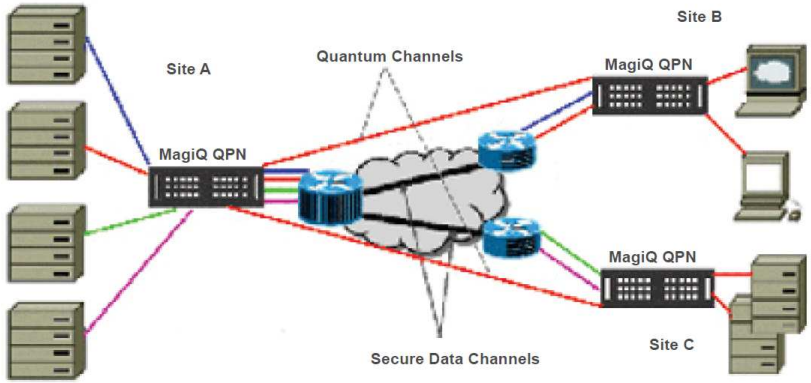
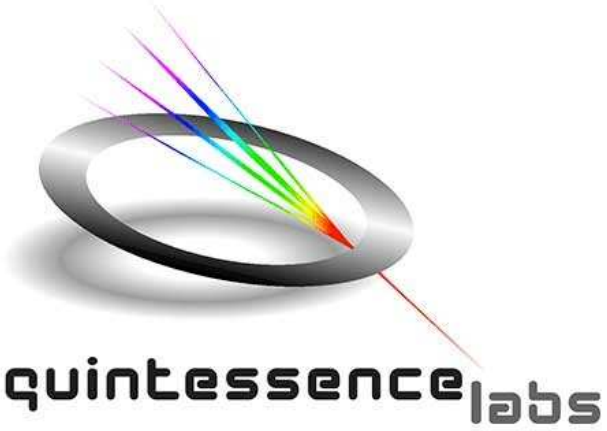


Figure 2: MagiQ QPN Security Gateway: Multi-Site Network Security

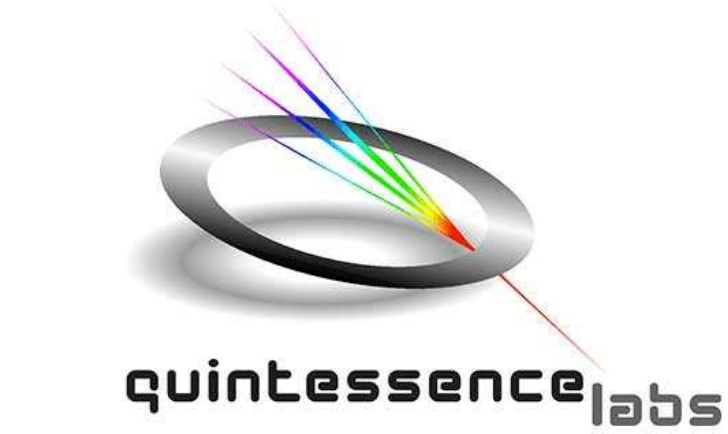
Quintessence Labs

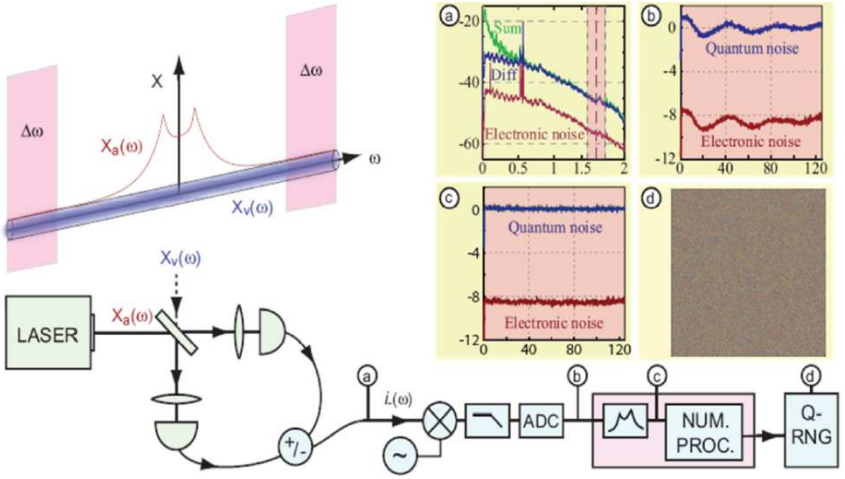


Quantum Key Distribution

- One time pad
- Optikai szál és free space
- 100 km-ig
- 28e optikai szálat használnak (SMF-28e 1270 nm és 1610 nm között 20 nm csatornaszélességgel)
- Titkos kulcsok generálása 10 Mbit/s-al

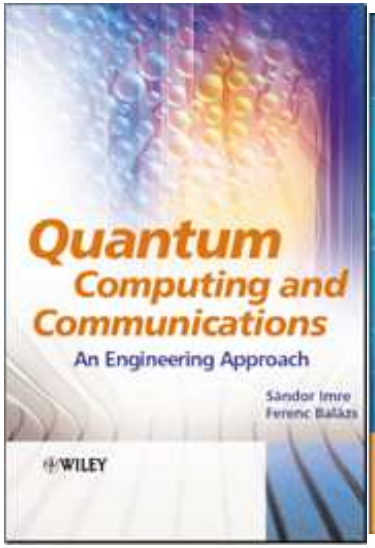
Quintessence Labs

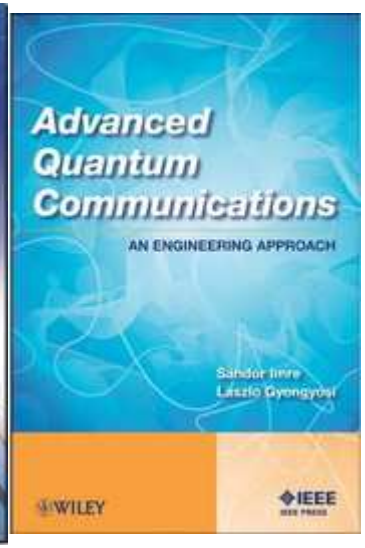


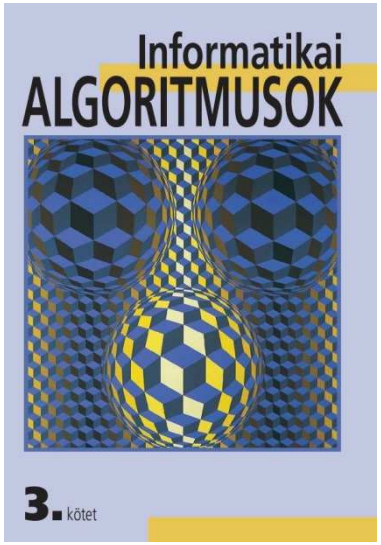


Random Number Generator

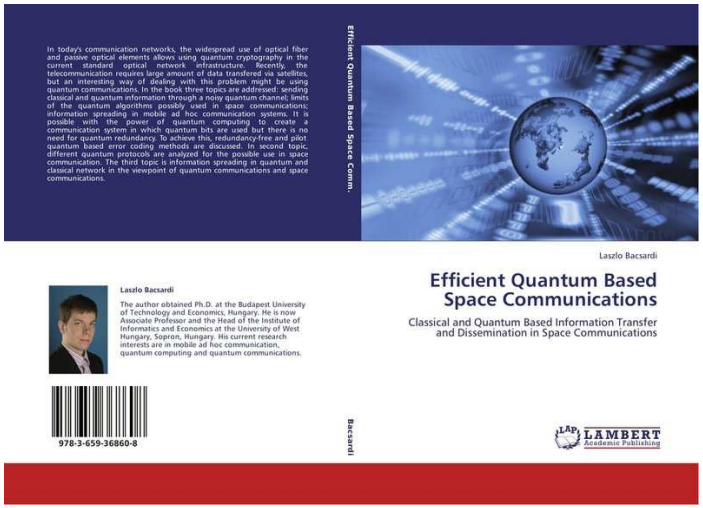
- Véletlen szám generálás 1 Gbit/s-tól 10 Gbit/s-ig
- Raw (Gaussian) eloszlás
- Conditioned (Uniform) eloszlás







qnews levelezőlista

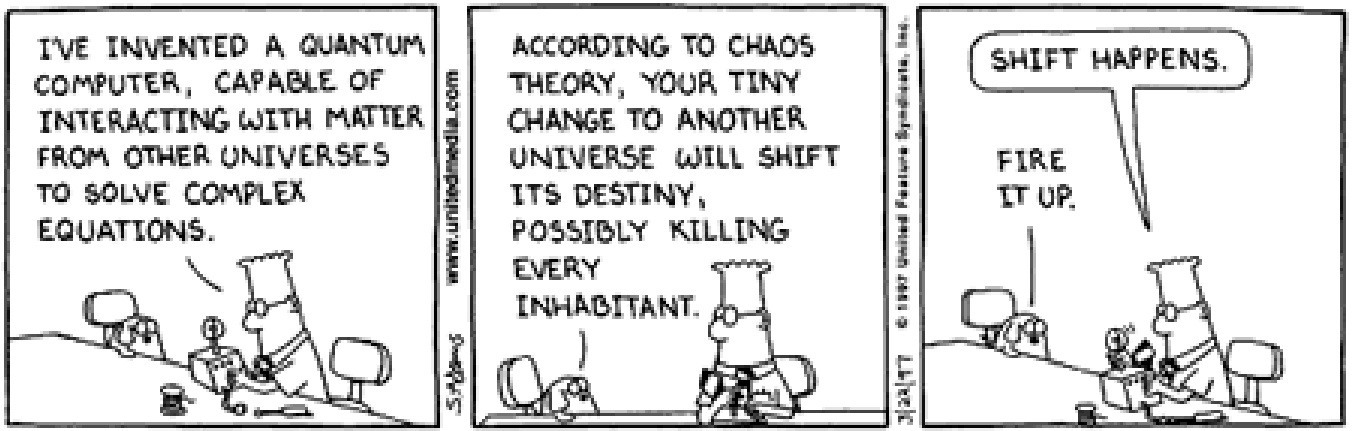


BME Hálózati Rendszerek és Szolgáltatások Tanszék
http://www.mcl.hu/quantum/

MTA WFI Kvantumoptikai és Kvantuminformatikai Osztály
http://optics.szfki.kfki.hu/

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

Kérdések?



Copyright © 1997 United Feature Syndicate, Inc.
Redistribution in whole or in part prohibited

bacsardi@hit.bme.hu