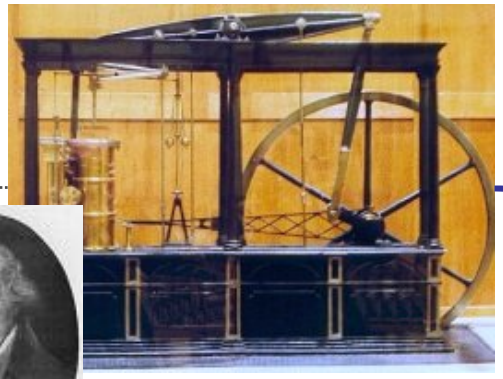
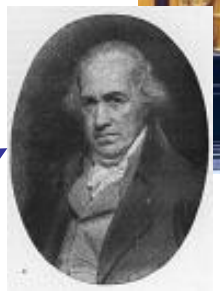
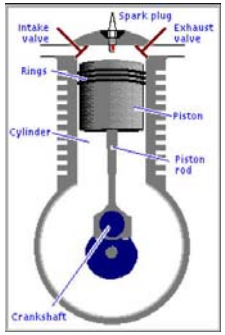
Kvantum infokommunikáció, a titkosítás új lehetőségei

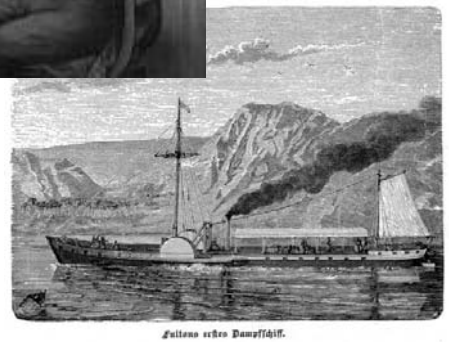
„A ***tudós leírja*** azt, ami van, a ***mérnök*** viszont megalkotja azt, ami soha nem volt."
Gábor Dénes

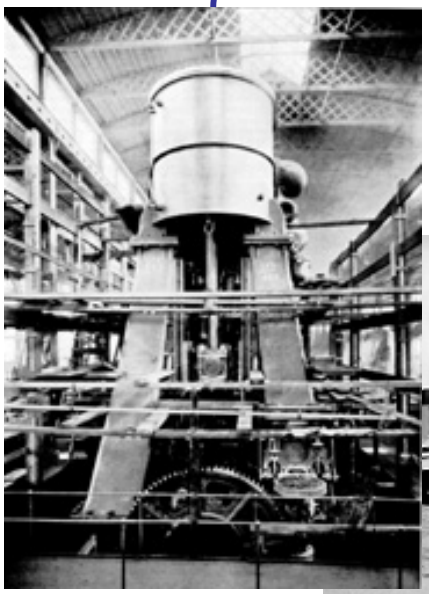
Imre Sándor, BME-HIT



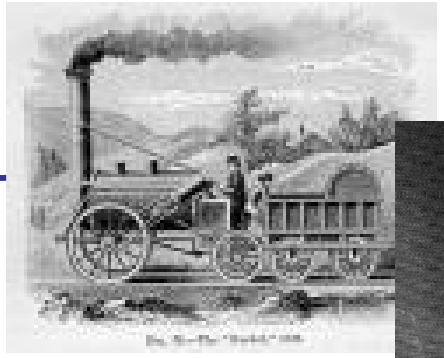



Spark plug
Intake valve
Exhaust valve
Rings
Piston
Cylinder
Piston rod
Crankshaft



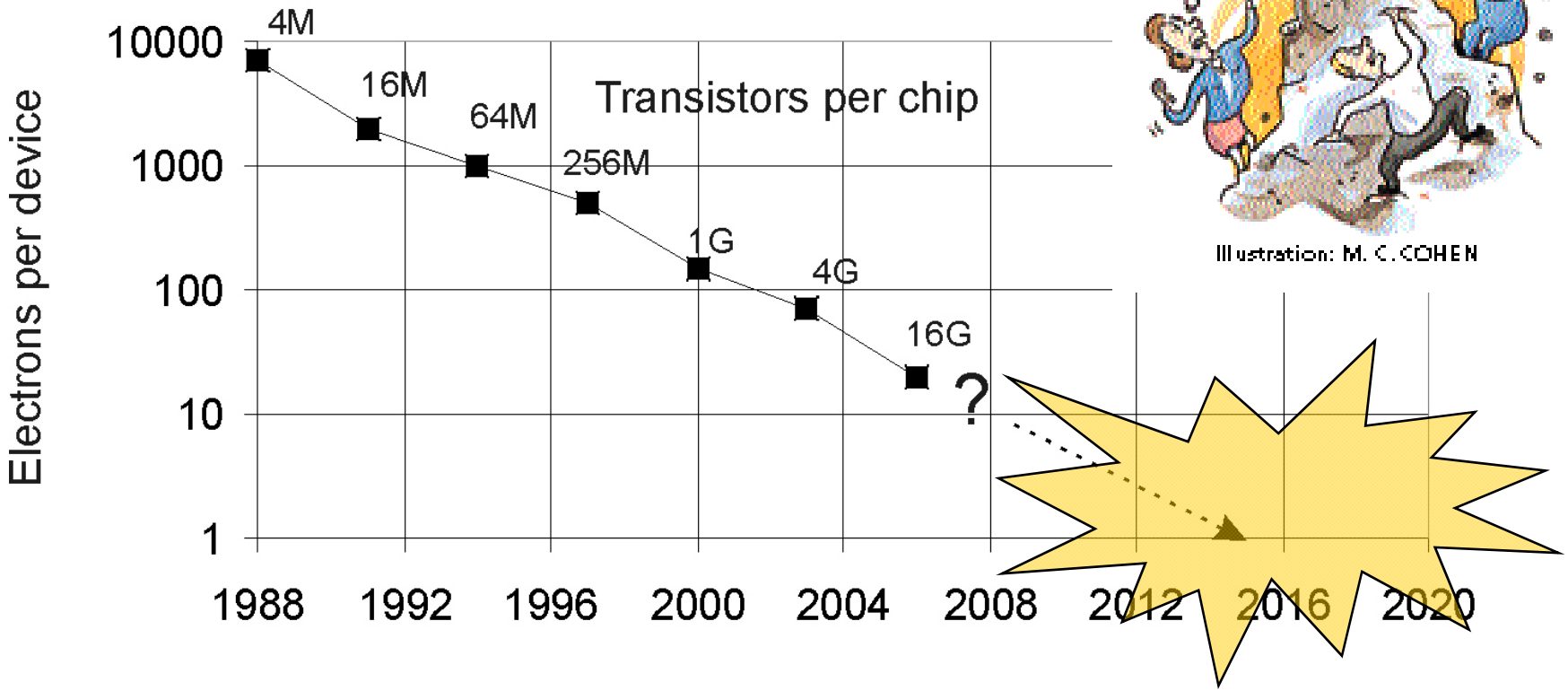



TITANIC
© 1995 Smithsonian Institution

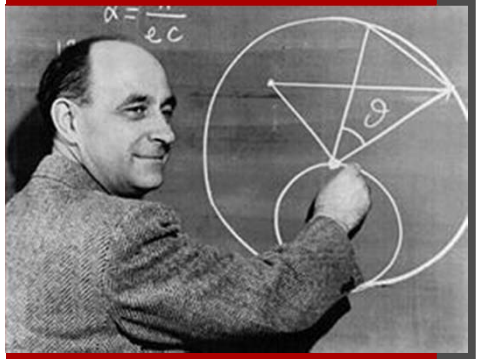


Ki tudja, hogy mi ez?

Moore törvénye



De meddig?



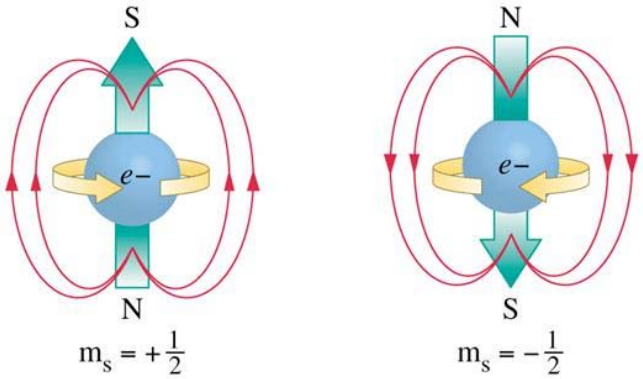
Kísérletezzünk!

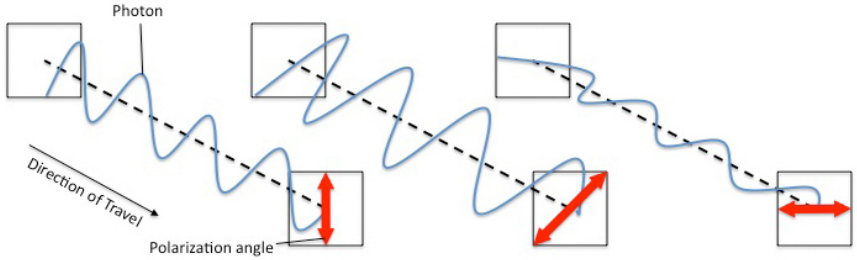
"There are two possible outcomes: If the result confirms the hypothesis, then you've made a measurement. If the result is contrary to the hypothesis, then you've made a discovery."

Enrico Fermi

Az elemi részecskék természete

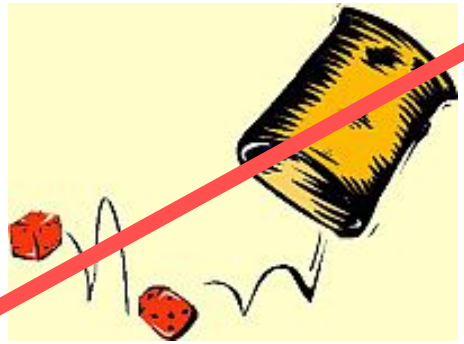
- részecske – hullám
- elektron spinje
- foton polarizációja





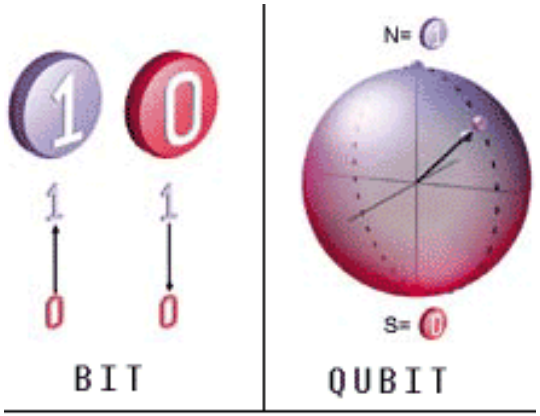
A véletlen természete: tényleg véletlen ☺

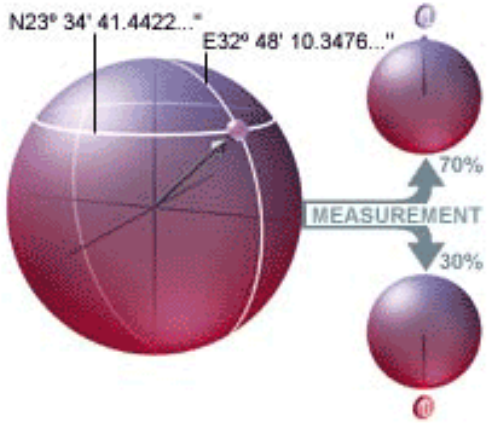
Isten nem dobókockázik a világgal!



Dehogynem! Sőt, volt annyira nagyvonalú, hogy diffegyenletek helyett olykor elegendő feldobni egy kockát!

Kvantum bit (qbit)





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

$$a, b \in C \text{ és } |a|^2 + |b|^2 = 1$$

Mit lehet néhány qbittel kezdeni?

- Szuperpozíció:
  - *n*=500 hosszú regiszter több állapotot tartalmaz, mint a világegyetem atomjainak száma
  - És számolni is lehet ennyi számmal egyszerre!

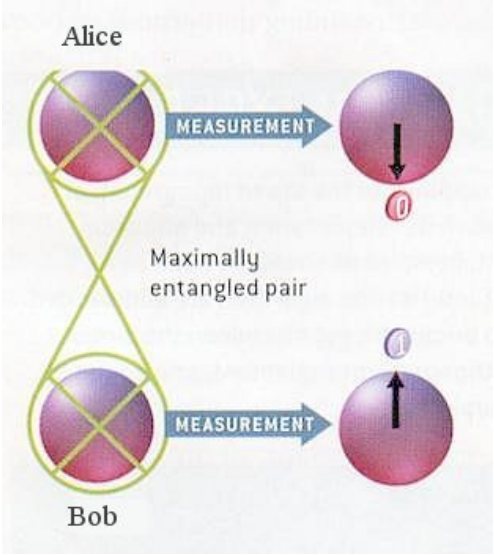
$$|\varphi\rangle = \sum_{i=0}^{2^n-1} \varphi_i |i\rangle$$

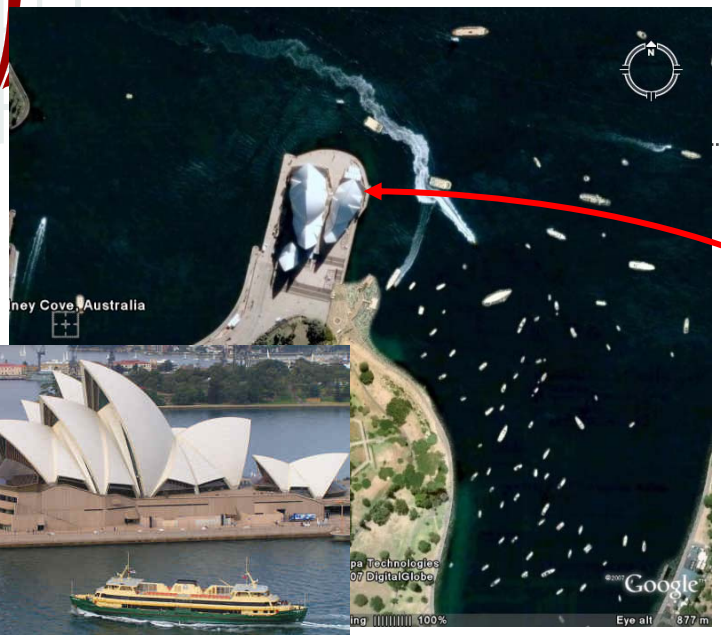
Összefonódás (entanglement)

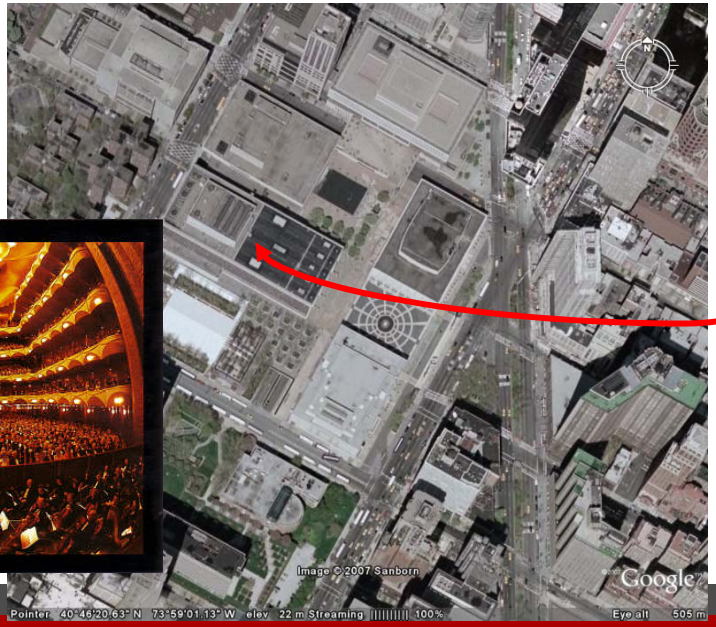
Sőt, az ölelés (összefonódás) másra is jó!

$$|\varphi\rangle = \varphi_0|00\rangle + \varphi_1|01\rangle + \varphi_2|10\rangle + \varphi_3|11\rangle$$

$$|\varphi\rangle = \varphi_0|00\rangle + \varphi_3|11\rangle$$







$$|\varphi\rangle = \varphi_0|00\rangle + \varphi_3|11\rangle$$

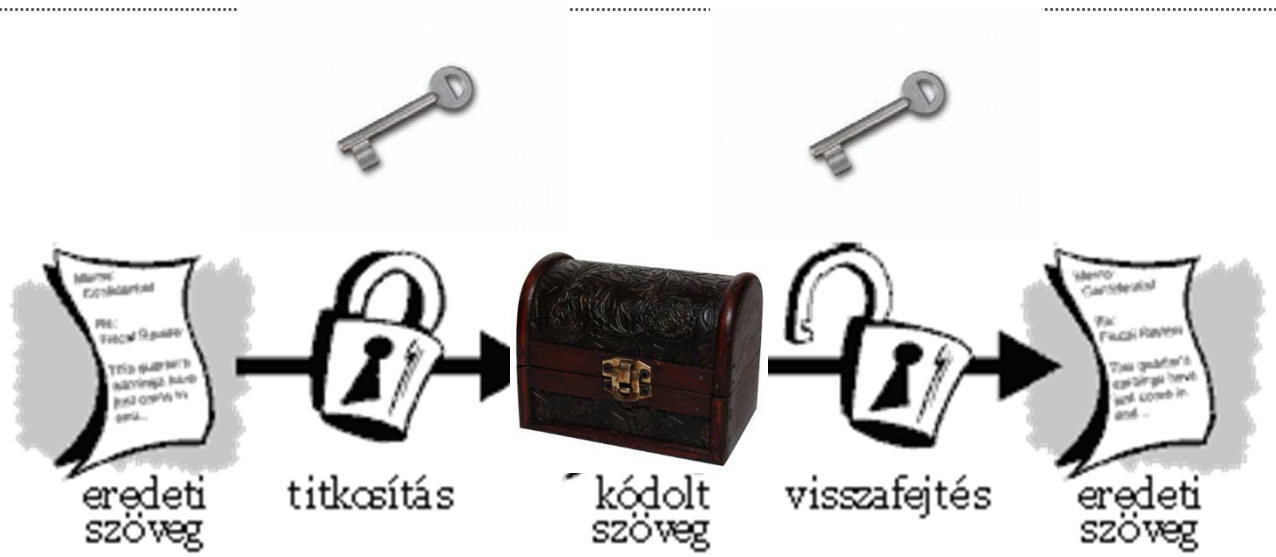
Alkalmazás – Teleportálás

$$|\varphi\rangle = \varphi_0|00\rangle + \varphi_3|11\rangle$$

- 2015. szeptember: 150 km

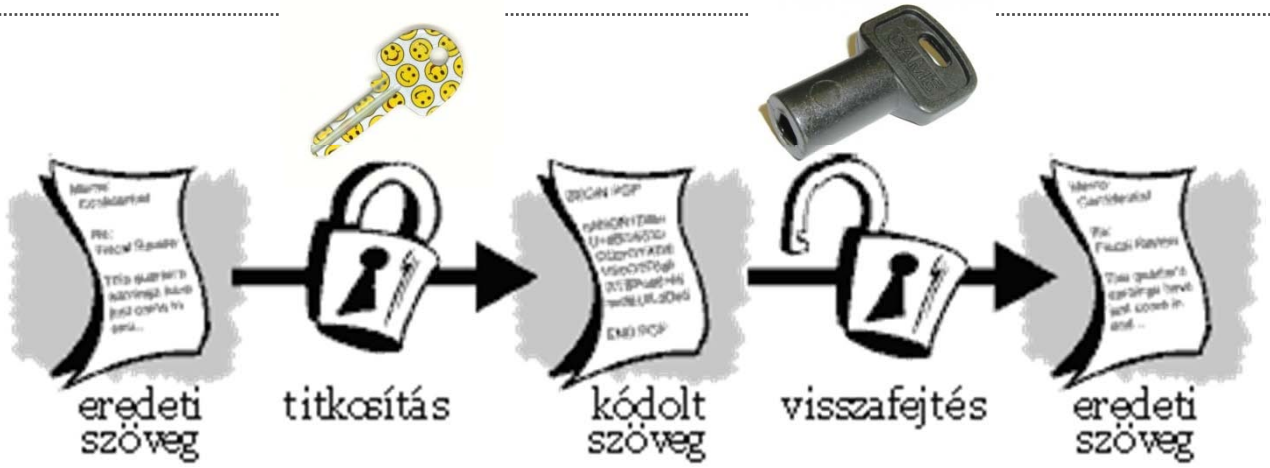
Kvantum infokommunikációs alkalmazások

Szimmetrikus titkosítás



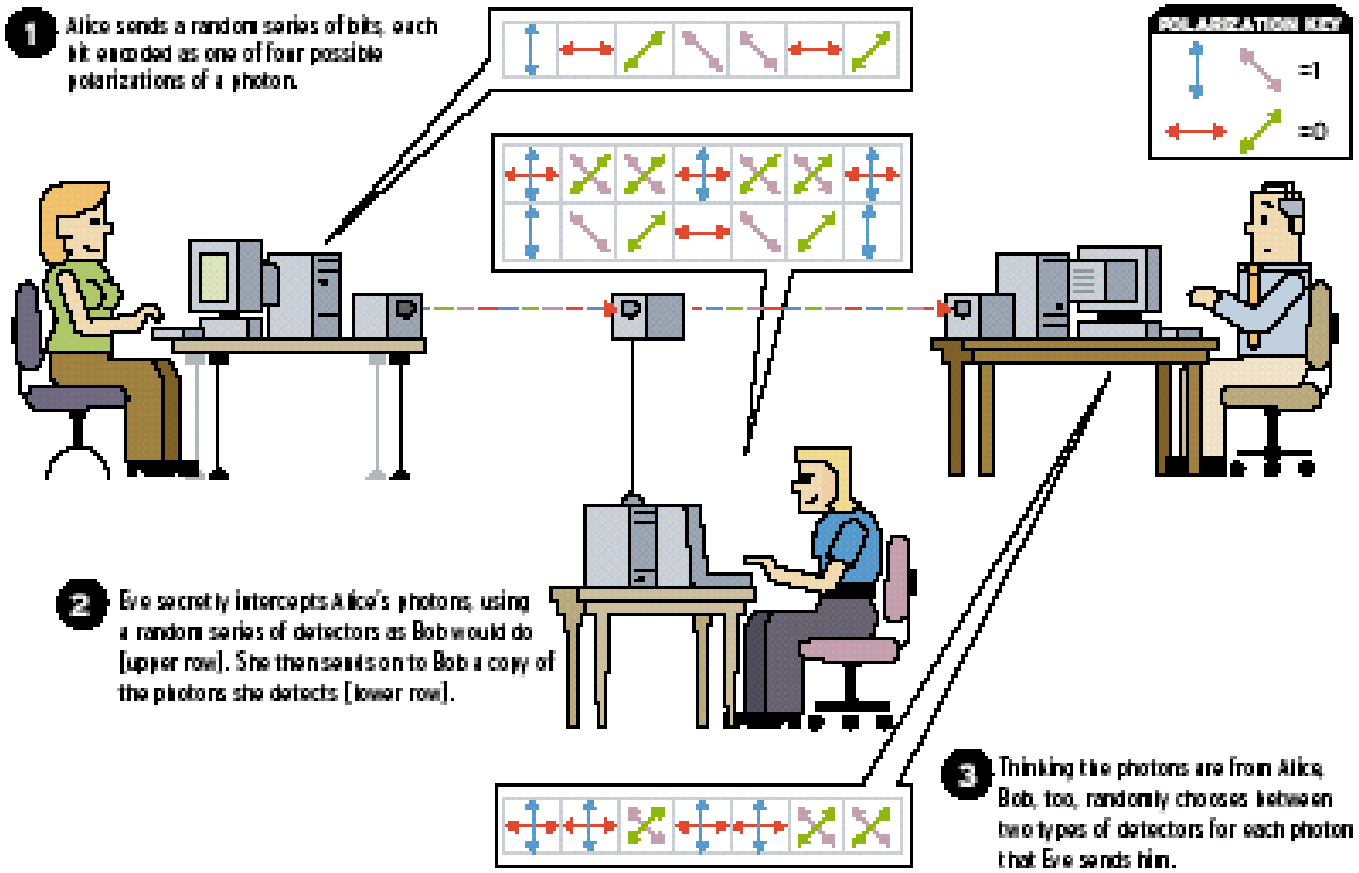
- Szimmetrikus kulcsú titkosítás
  - Egyforma kulcsok mindkét oldalon
- Abszolút biztonságos, ha bizonyos előírásokat betartunk
- Gond, hogy a kulcsot miként juttassuk el a túloldalra????

Nyílvános kulcsú titkosítás

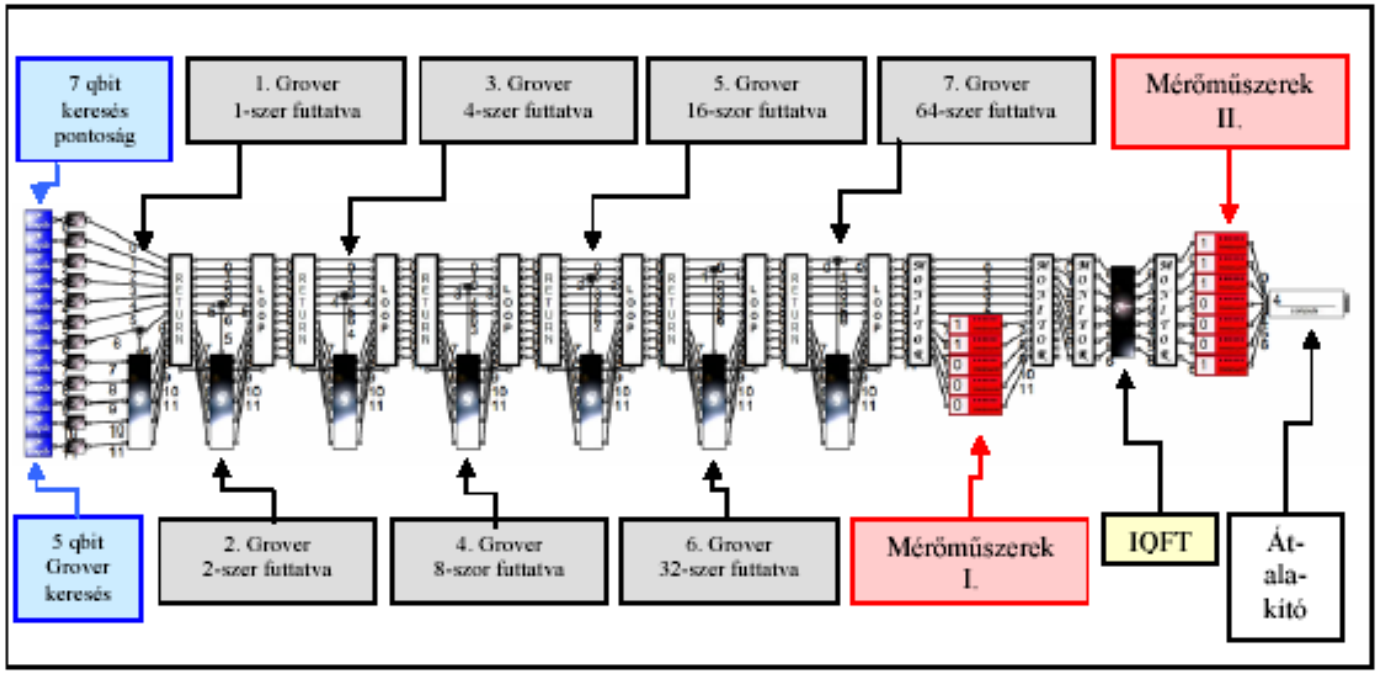


- Nyílvános kulcsú titkosítás
  - nyilvános titkosítókulcs, titkos fejtőkulcs
  - kulcsok előállítása: két nagy prímszám szorzatát felhasználva
  - feltörés: a törzsténye zők meghatározása
- A mai napig nem sikerült bebizonyítani, hogy nincs hatékony algoritmus a feltörésre. Mindenesetre eddig nem sikerült ilyen klasszikus algoritmust találni.
- **De kvantumosat IGEN!**

A lehallgatás



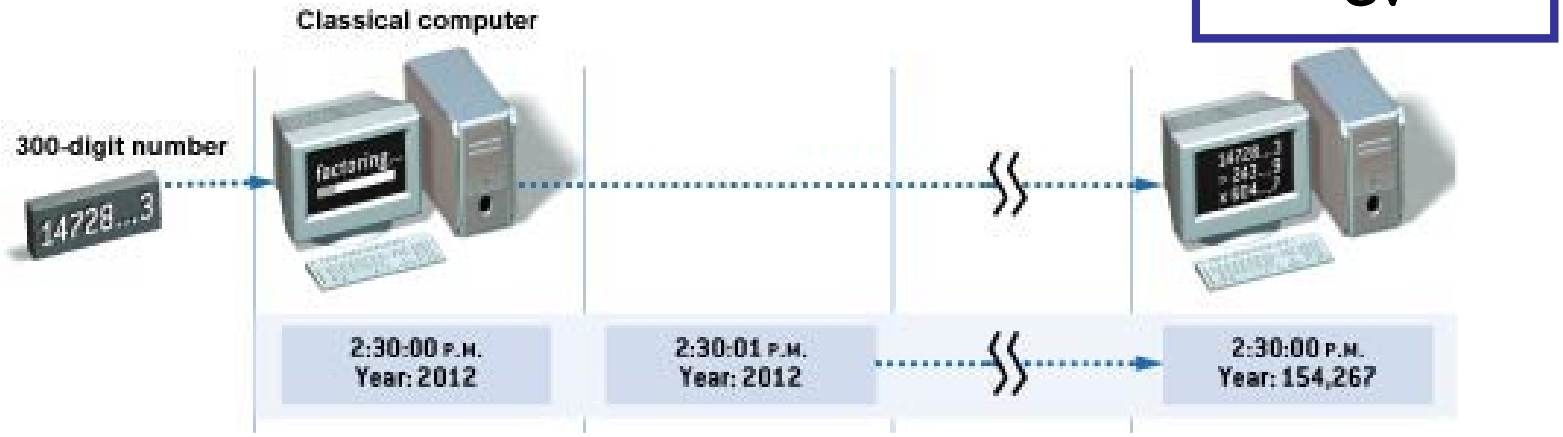
RSA feltörő kvantum áramkör



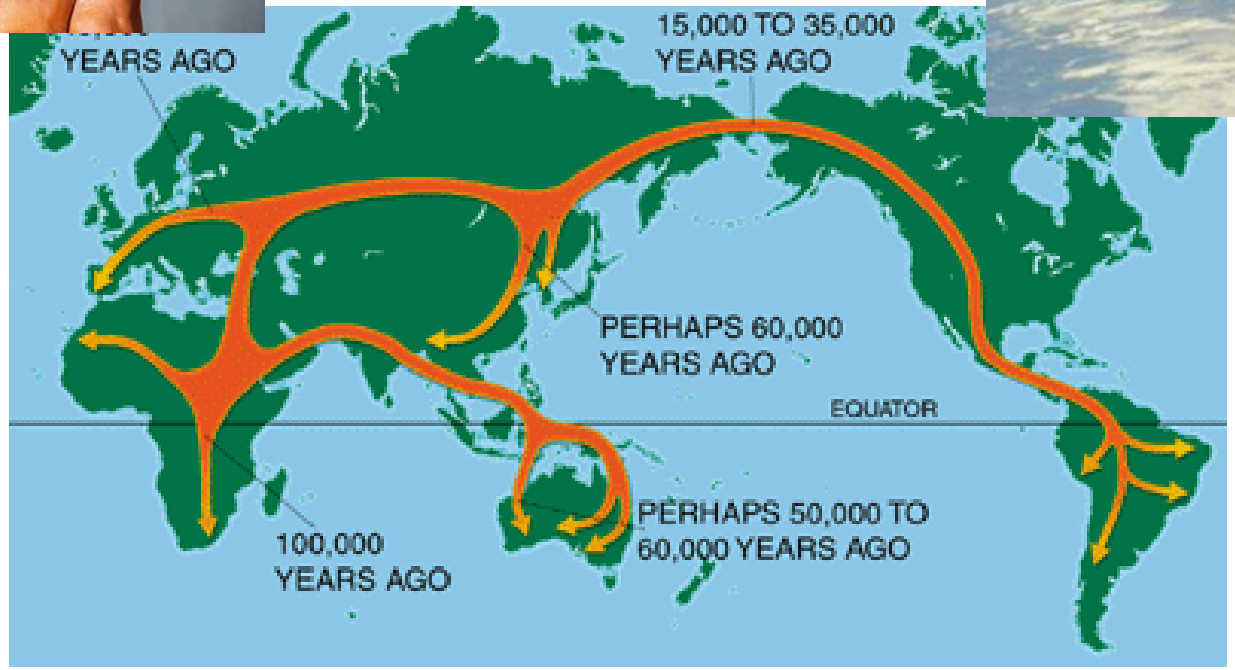
Shor-algotitmus és az RSA feltörése

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

152 000 év



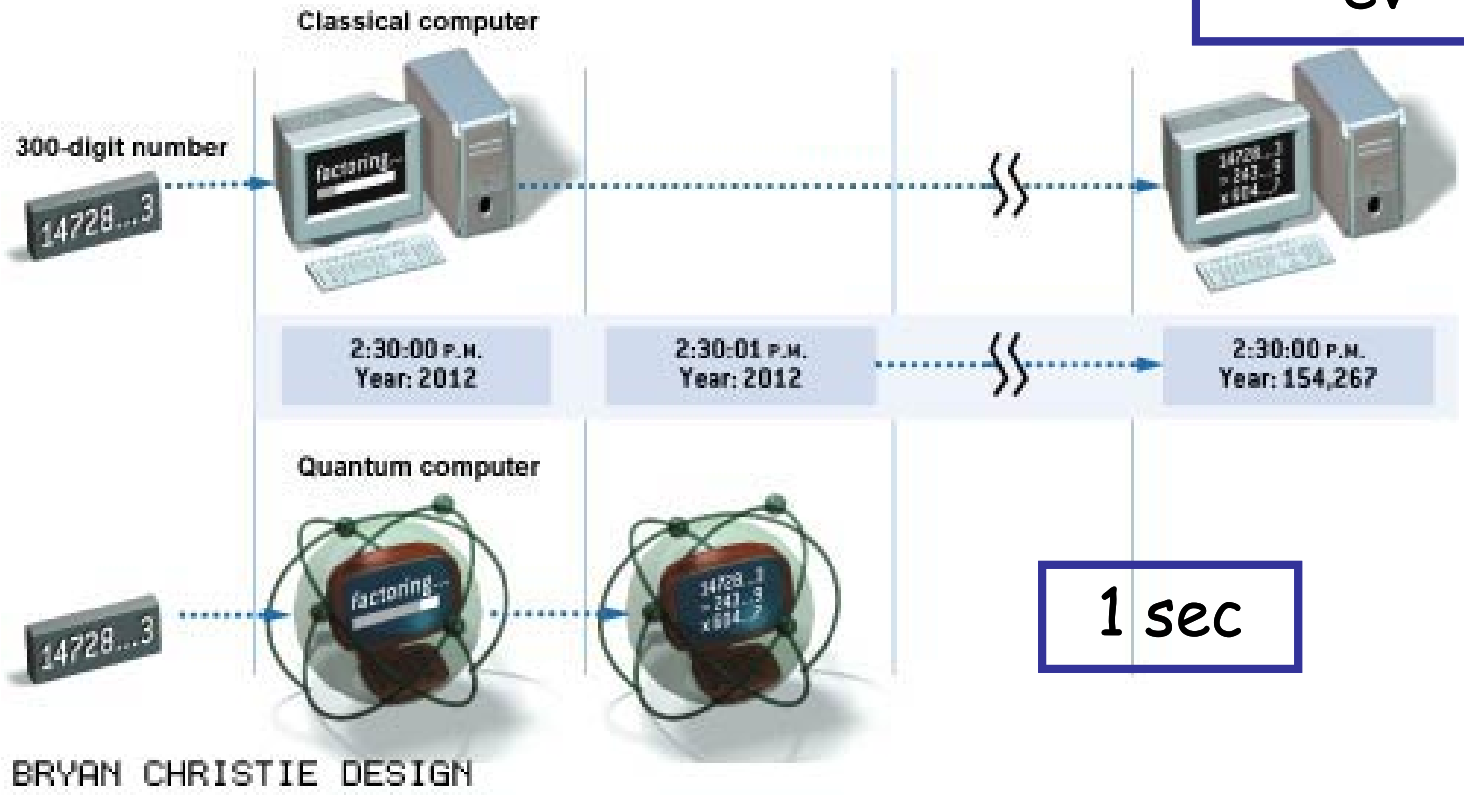
152 000
év


YEARS AGO
15,000 TO 35,000
YEARS AGO
PERHAPS 60,000
YEARS AGO
EQUATOR
PERHAPS 50,000 TO
60,000 YEARS AGO
100,000
YEARS AGO

Shor-algotitmus és az RSA feltörése

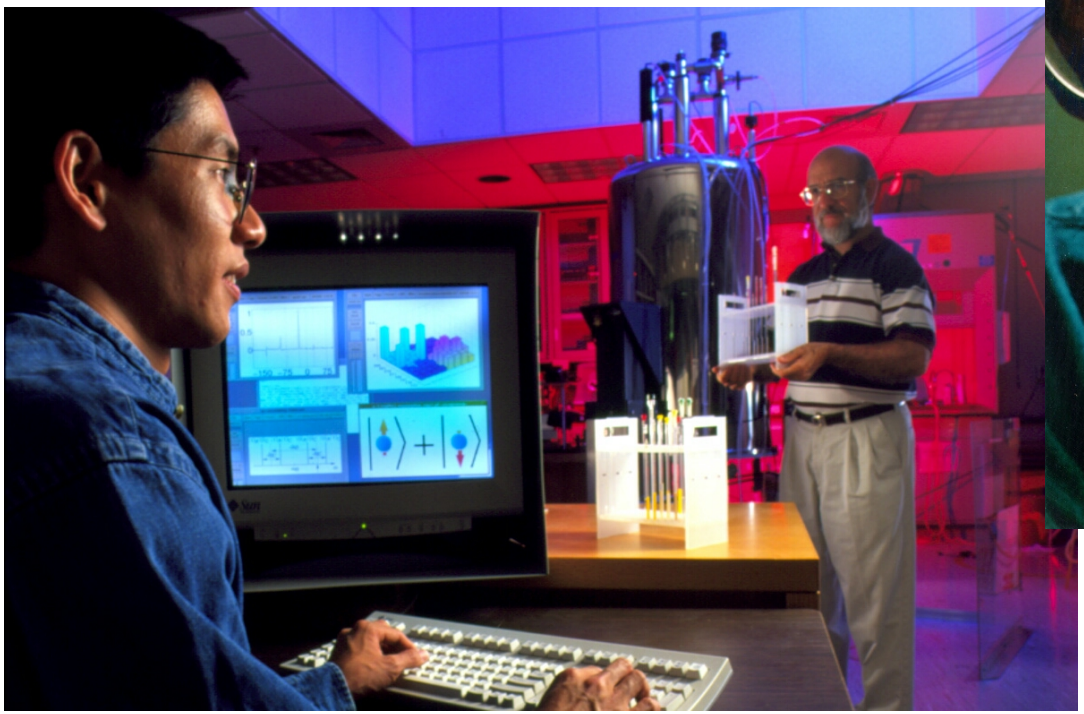
$$O\left(\log^3(N)\right)$$

152 000 év

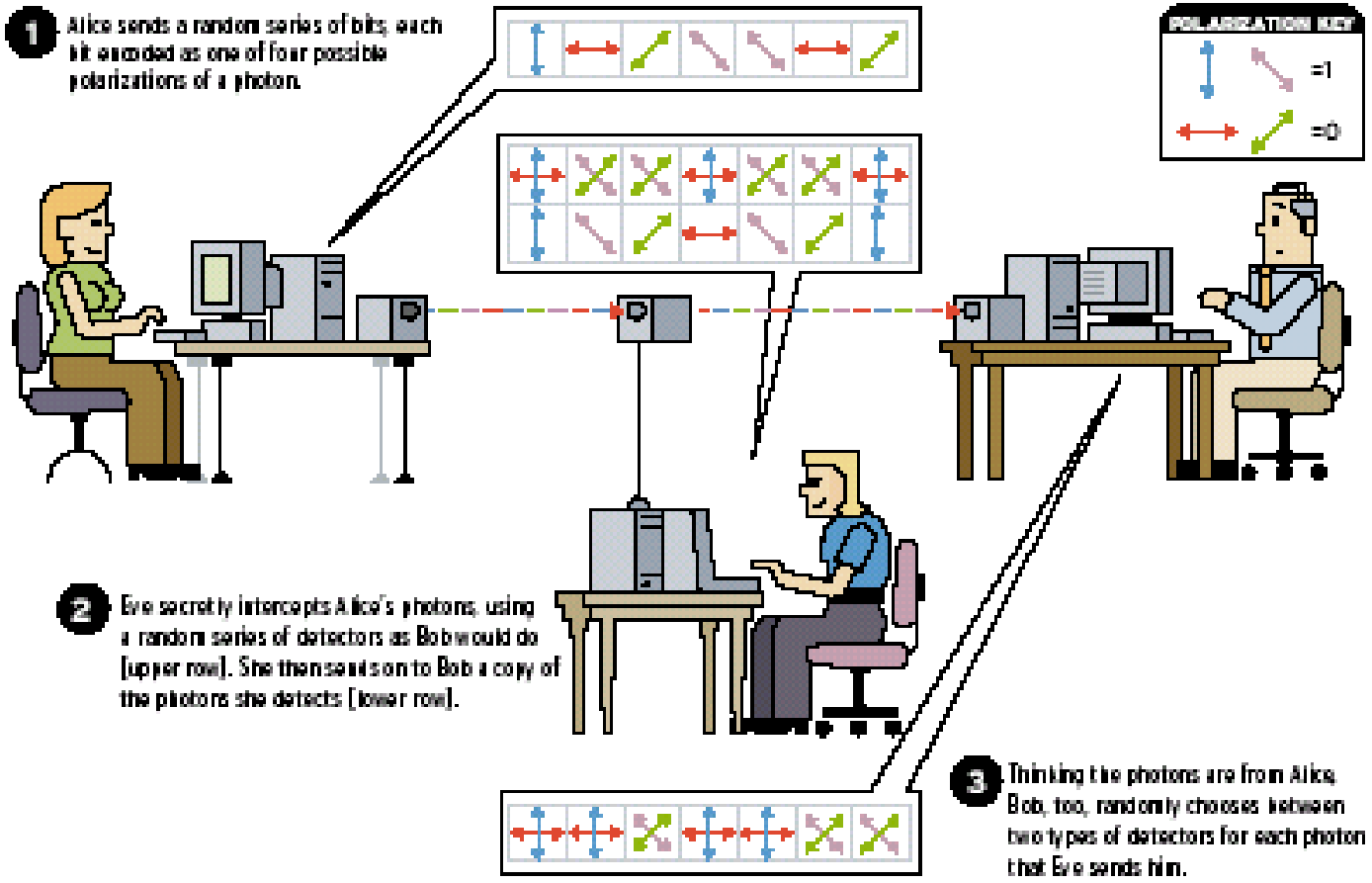


Ahogy ma faktorizálunk

$15=5\times3$



Védekezés – kvantumos kulcsszétosztás

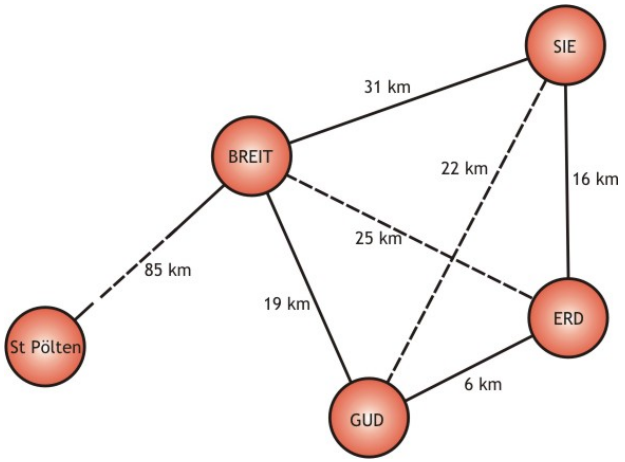


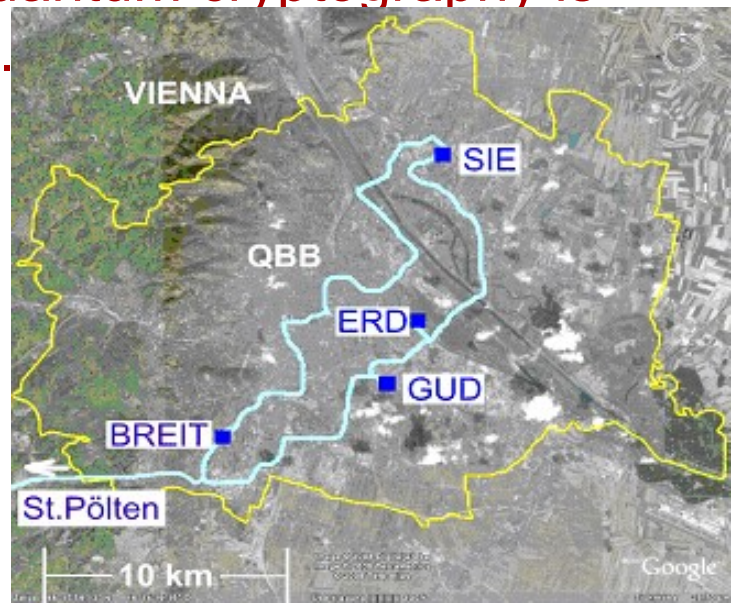
Első sikeres demonstráció

SECOQC

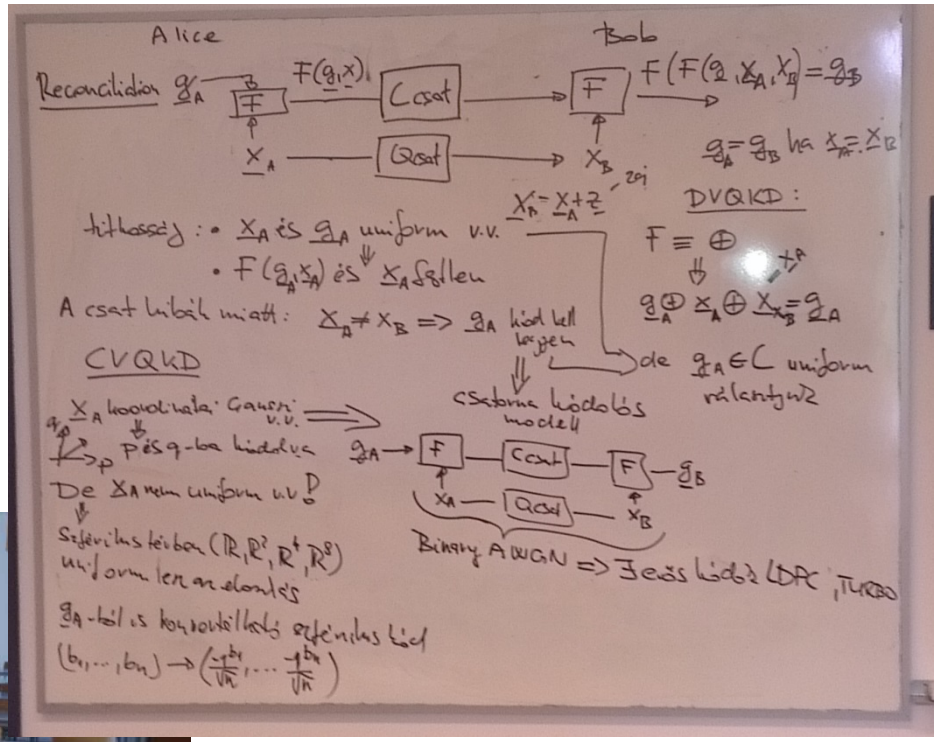
Development of a Global Network for Secure Communication based on Quantum Cryptography

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

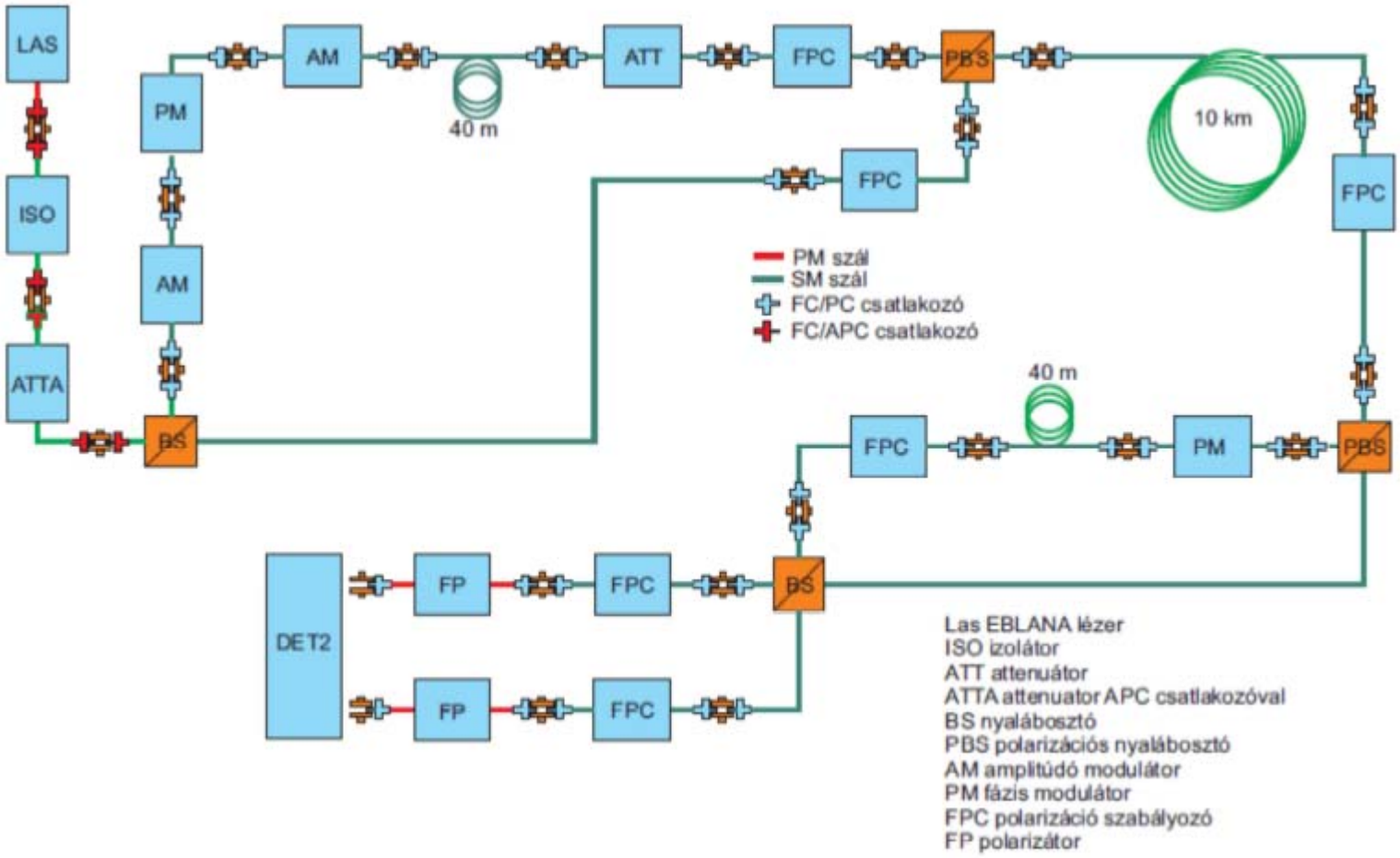




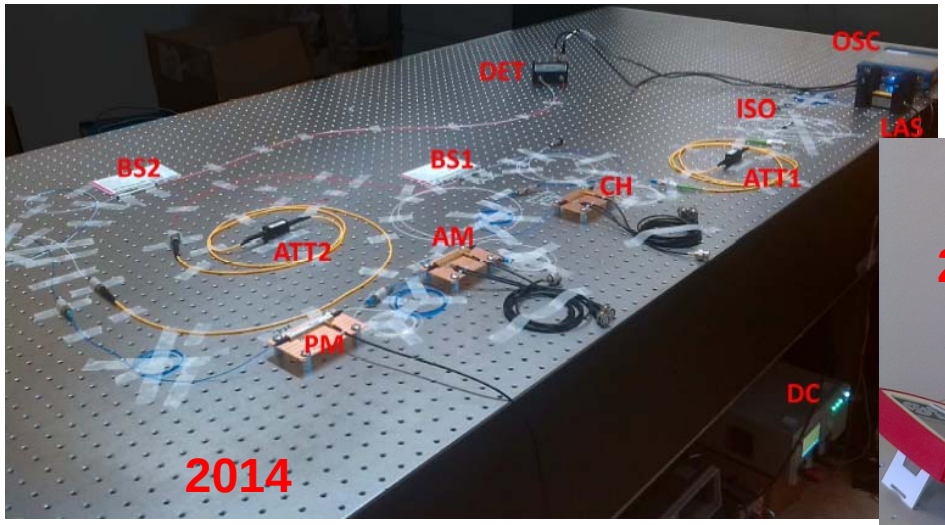
Ahogy mi kulcsszétosztunk - 2013



Ahogy mi kulcsszétosztunk - 2014



Ahogy mi kulcsszétosztunk – 2015

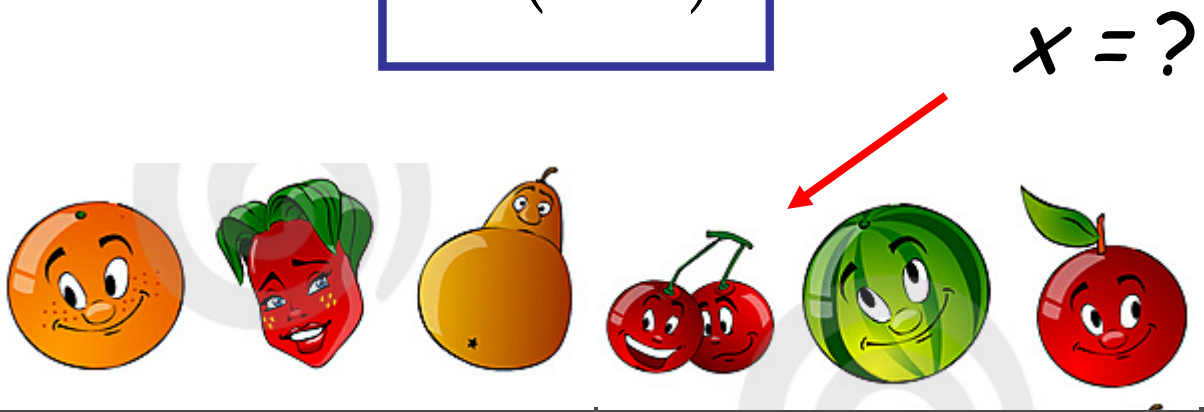


Adatbázis-keresés története

Adatbázis keresés története v4: Grover-algoritmus

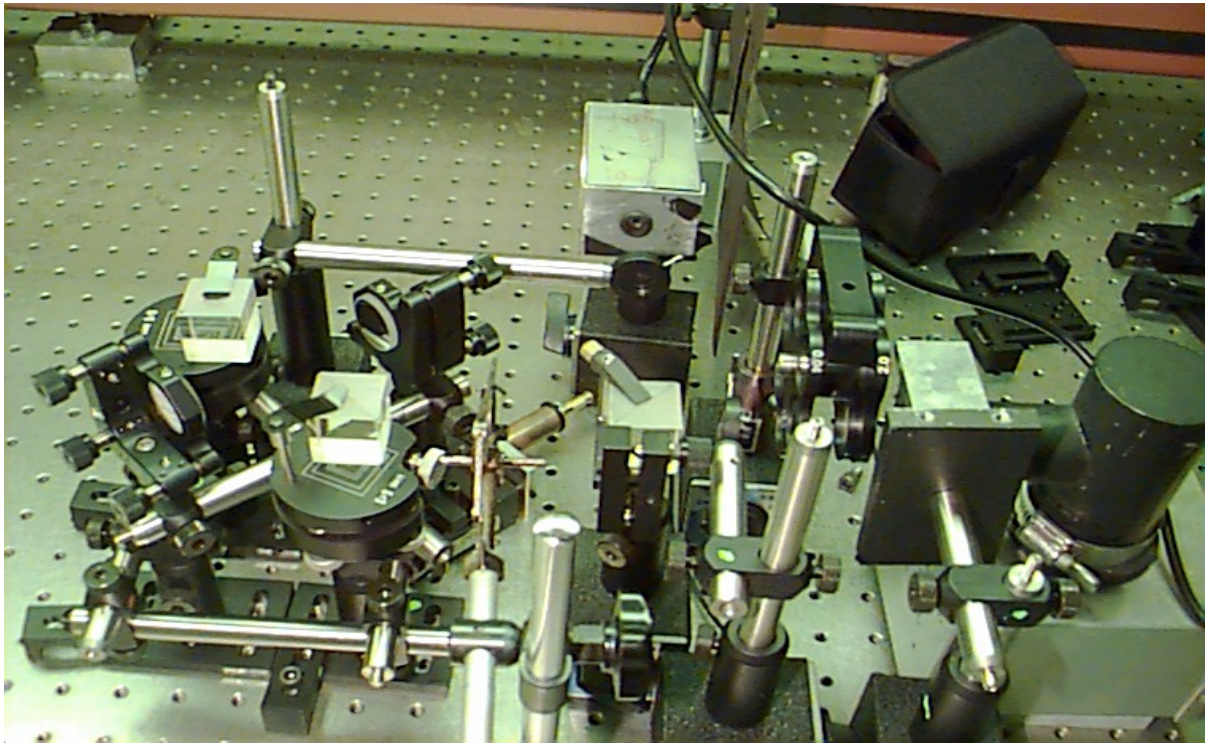
- Aki keres, talál! De nem mindegy mennyi idő alatt.
- Rendezetlen adatbázis *N* különböző elemmel.
- Klasszikusan *N* kérés szükséges.
- Ugyanakkor kvantum módon:

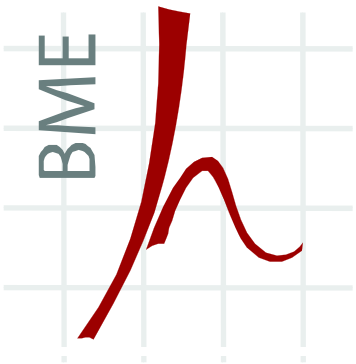
$$O\left(\sqrt{N}\right)$$



Ahogy ma adatbázis keresünk

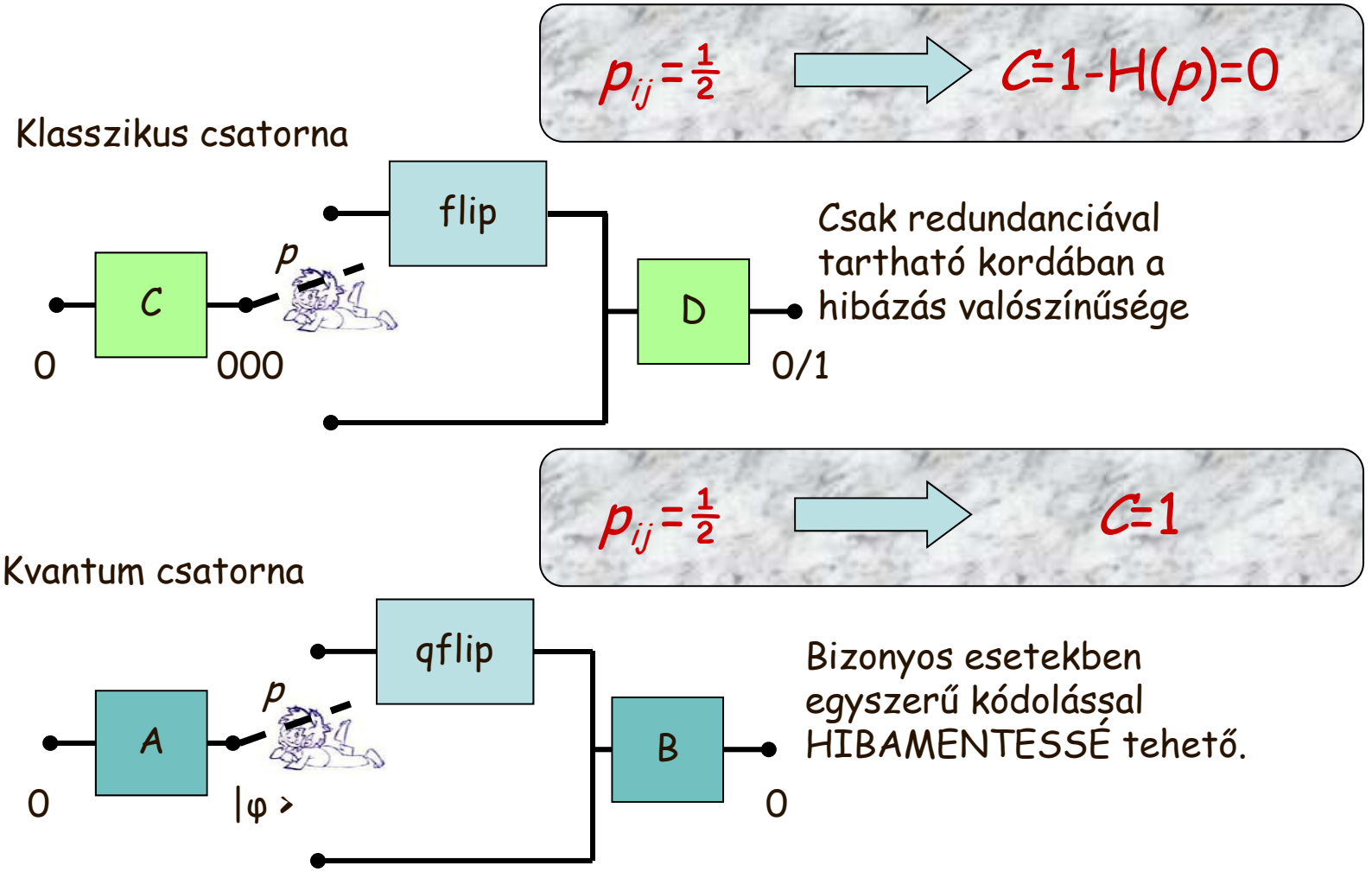
- Miért örülünk ennek?
  - Informatika: pl. adatbázis kezelés
  - Távközlés: pl. útvonalválasztás, jelfeldolgozás



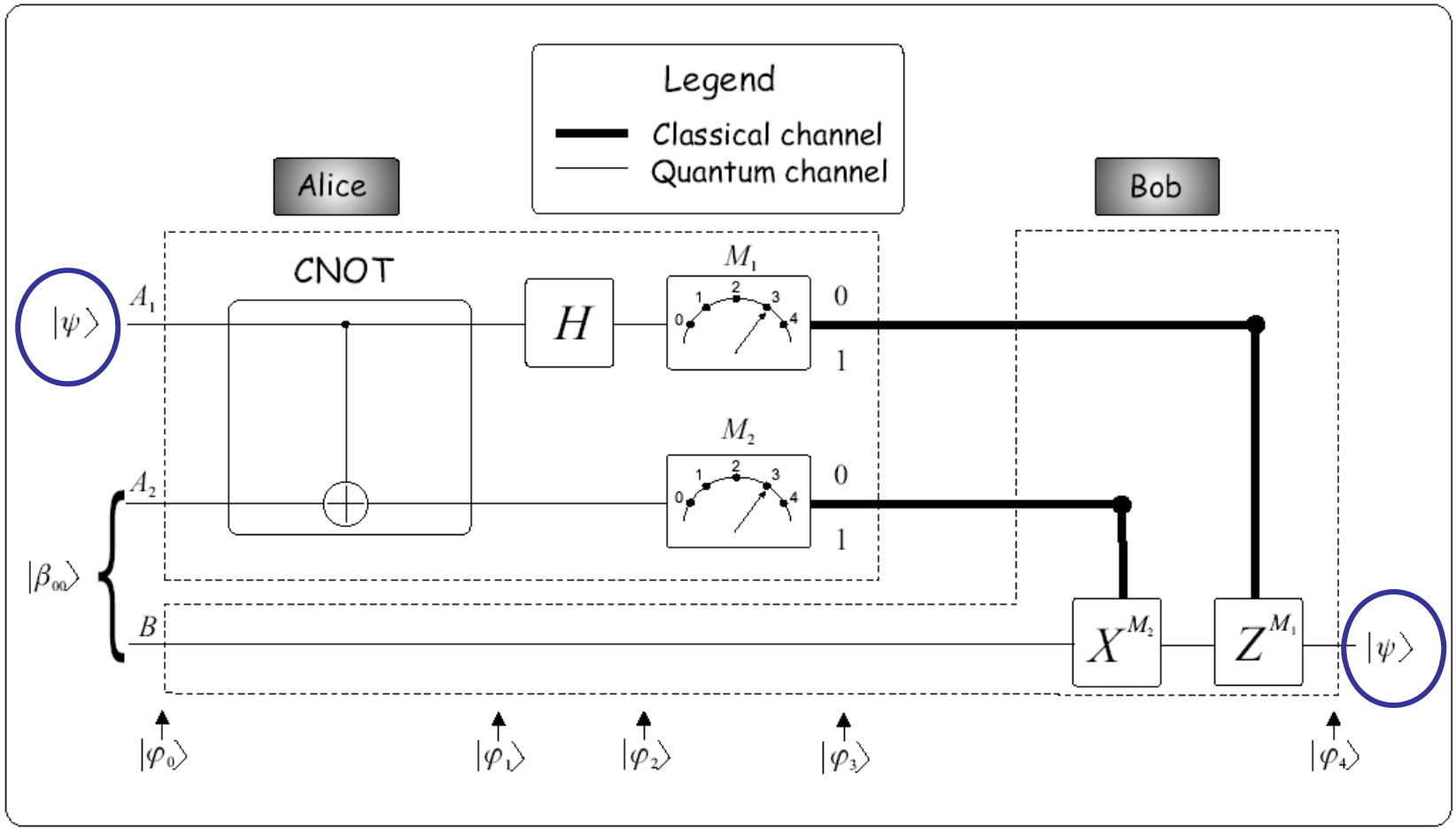


Lazításként egy kis infoelmélet

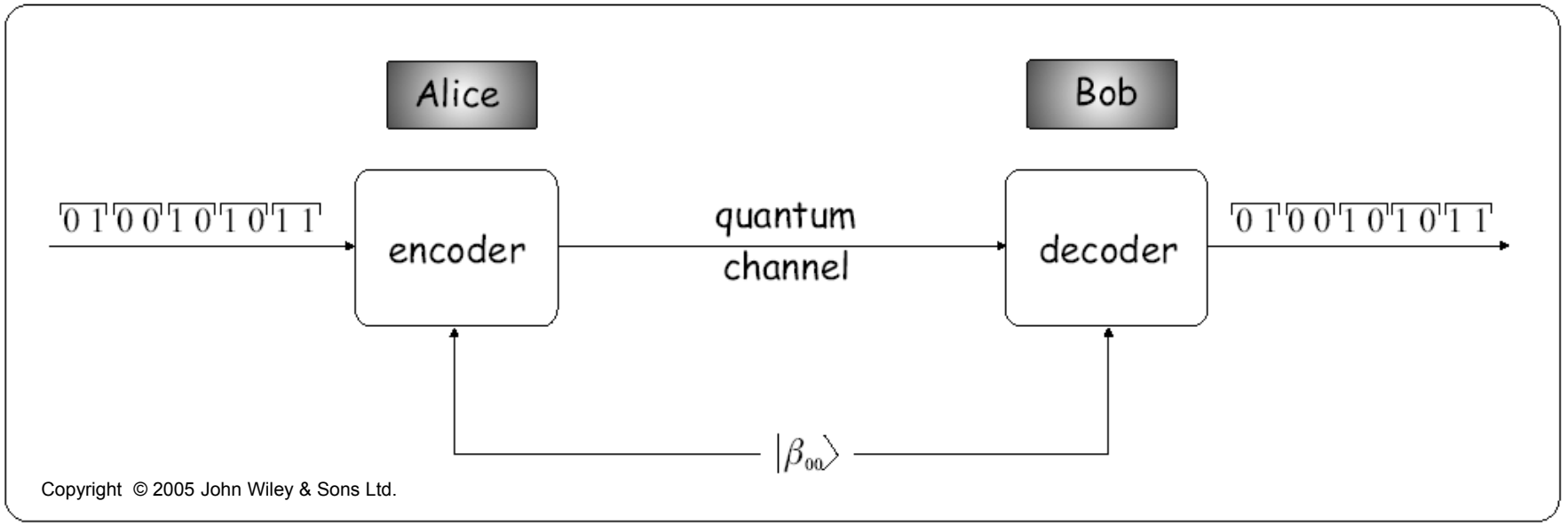
Egy egyszerű csatorna modell
(mintha már láttuk volna valahol…)



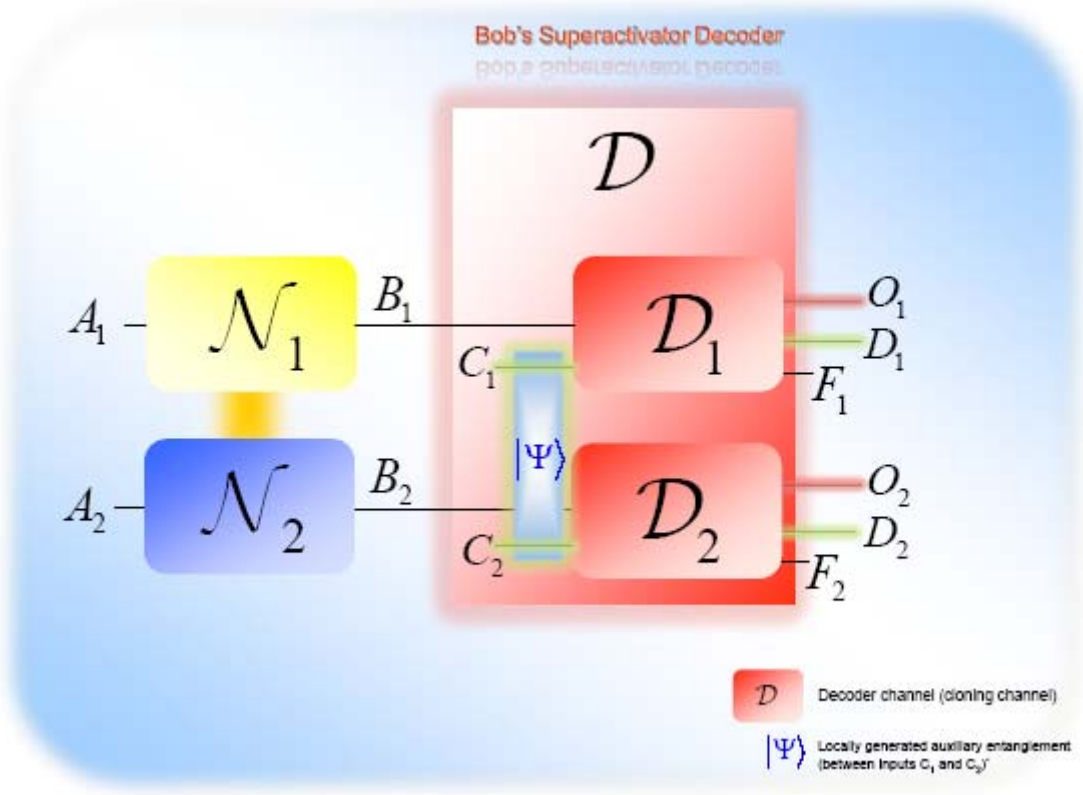
Teleportálás



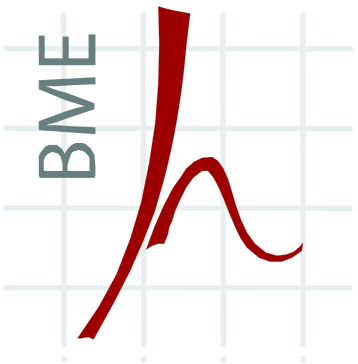
Szupersűrűségű tömörítés



OK, ezt még lenyeltük, de ilyen állat nincs:



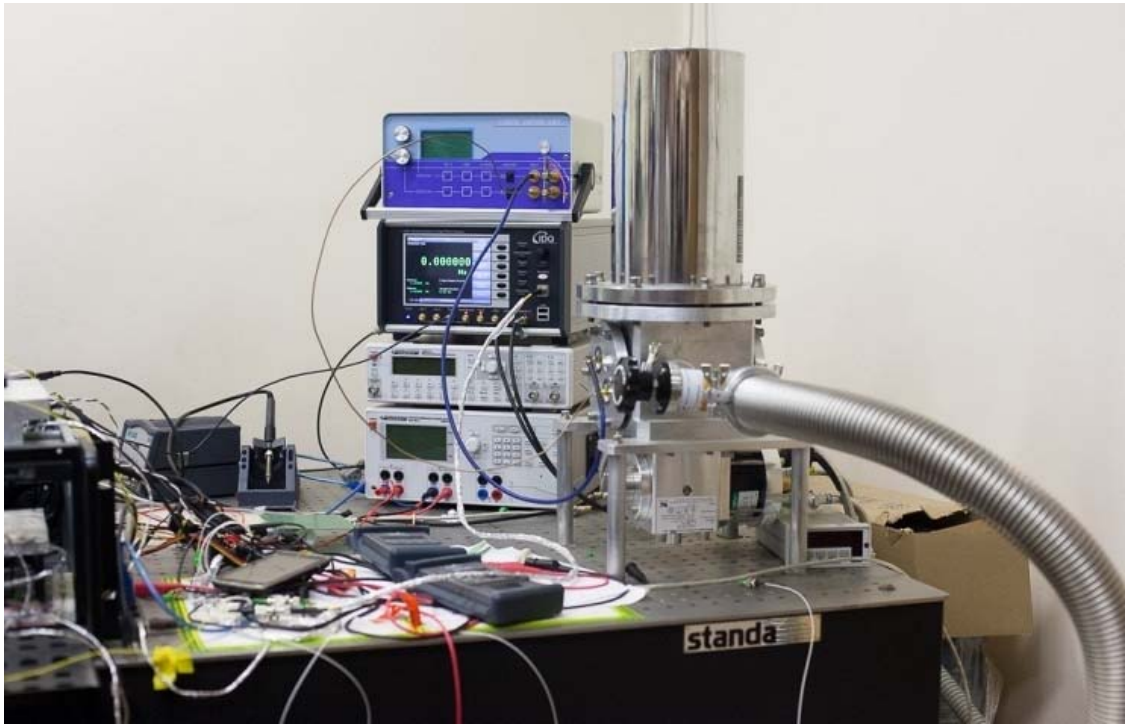
- 2 db. külön-külön $C = 0$ kapacitású csatorna ügyesen összekapcsolva mégis képes információt átvinni!



Hol tart ma a világ?

Optikai szálon

Az orosz medve: 225 km – 2016



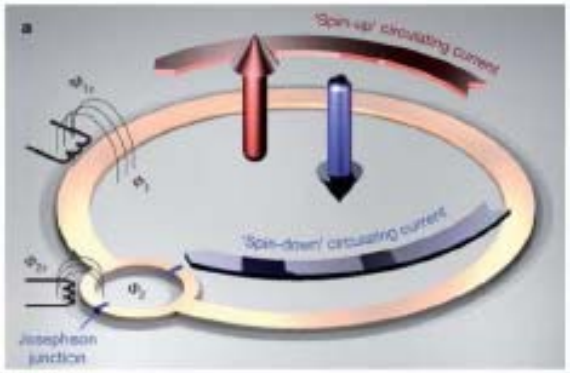
A svájci óra: 307 km - 2015

Biztató jelek - szabadtér

- 1991
  - első megvalósítás, 30 cm-es távon
  - laboratóriumi körülmények között: 205 méter
  - külső körülmények között: 75 méter
- 1998
  - Los Alamos National Laboratory, 950 méteres táv, éjszakai körülmények
- 2002
  - ugyanez a kutatólaboratórium demonstrálta 10 kilométeres távon (9,81 km), nappali és éjjeli időszakban is
- 2006
  - 144 km nemzetközi kutatócsoport
- 2016
  - Kínai-osztrák műhold pályára állítása, várjuk az eredményeket!

D-Wave
The Quantum Computing Company™

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

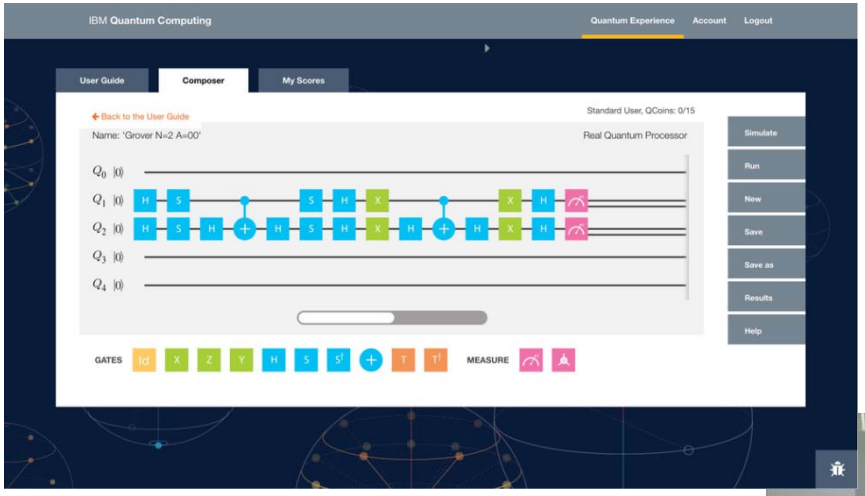


D:wave
The Quantum Computing Company™

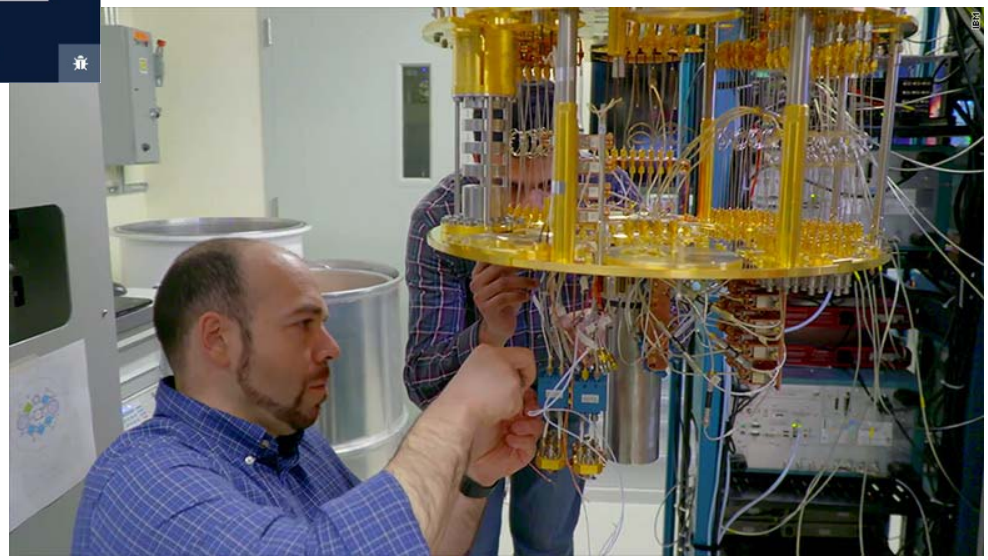
- 2011: D-Wave One
  - 128 qubit
  - 10 000 000$
- 2013: D-Wave Two
  - 512 qubit

- 2016:
  - D-Wave's flagship product, the 1000-qubit D-Wave 2X quantum computer, is the most advanced quantum computer in the world. It is based on a novel type of superconducting processor that uses quantum mechanics to massively accelerate computation.

IBM kvantum számítógép hozzáférés!



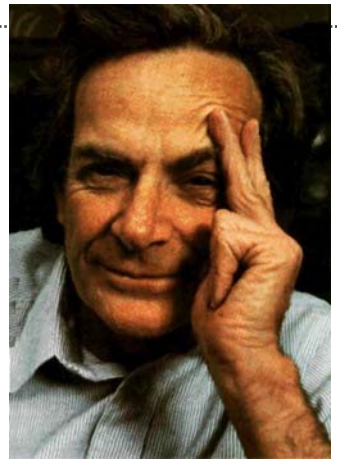
2016-os újdonság!!!



https://quantumexperience.ng.bluemix.net/

Tanulságok

- Ígéretes algoritmusok,
- Ígéretes kísérletek és demonstrációk.
- Sőt egyes alkalmazások már ki is férnek a gyárkapun.
- De akad még néhány „APRÓBB” probléma:
  - „árnyékolás”
- Az asztali kvantum PC-re még néhány évet bizonyosan várni kell.
- Viszont a kvantum kommunikáció előtt szabad az út!



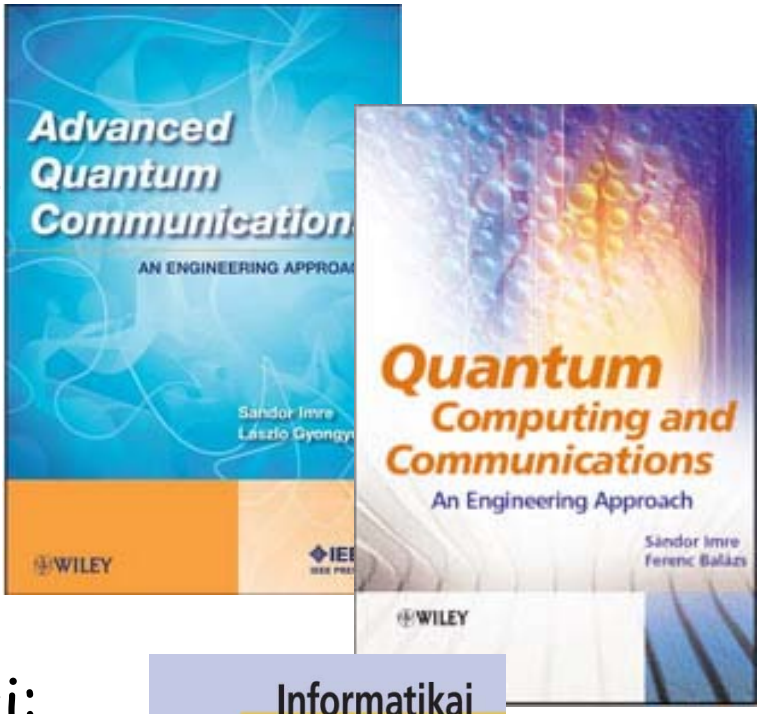
"... it seems that the laws of physics present no barrier to reducing the size of computers until bits are the size of atoms, and quantum behavior holds sway."

Richard P. Feynman (1985)

Ne éljetek „klasszikusan"! Az élet kerek mivoltához nélkülözhetetlen a szuperpozíció.

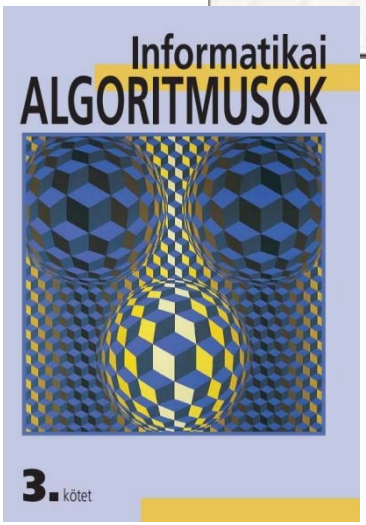
Imre Sándor 2010

További információk



IMRE@HIT.BME.HU

Aki a kvantumos világra kíváncsi:
http://www.mcl.hu/quantum//



Aki esetleg rám kíváncsi:
http://www.hit.bme.hu/people/imre/

Akik a mozgóképet szeretik ☺

- Bevezetés a kvantum-informatikába (12 publikus felvétel)
- http://videotorium.hu/hu/channels/details/1291,Bevezetes_a_kvantum-informatikaba