Kvantum informatika és kommunikáció: múlt – jelen – jövő

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

Imre Sándor, BME-HIT

IMRE SÁNDOR

imre@hit.bme.hu

- BME

- Villamosmérnöki és Informatikai Kar

- Hálózati rendszerek és Szolgáltatások Tanszék

DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

- 20 éve oktatom, kutatom, fejlesztem a kvantum mechanikára épülő informatikát és kommunikációt!

MIRŐL LESZ MA SZÓ?

- Motivációk
- Mit jelent az, hogy „kvantumos”?
- Alkalmazási területek
- Hol tart ma a világ?

SCHRÖDINGER-EGYENLET

Schrödinger equation

$$i\hbar\frac{\partial\Psi(\vec{r},t)}{\partial t} = \left[\frac{\hbar^2\nabla^2}{2m} + V(\vec{r})\right]\Psi(\vec{r},t)$$

Second Series December, 1926 Vol. 28, No. 6

THE

PHYSICAL REVIEW

AN UNDULATORY THEORY OF THE MECHANICS OF ATOMS AND MOLECULES

By E. SCHRÖDINGER

ABSTRACT

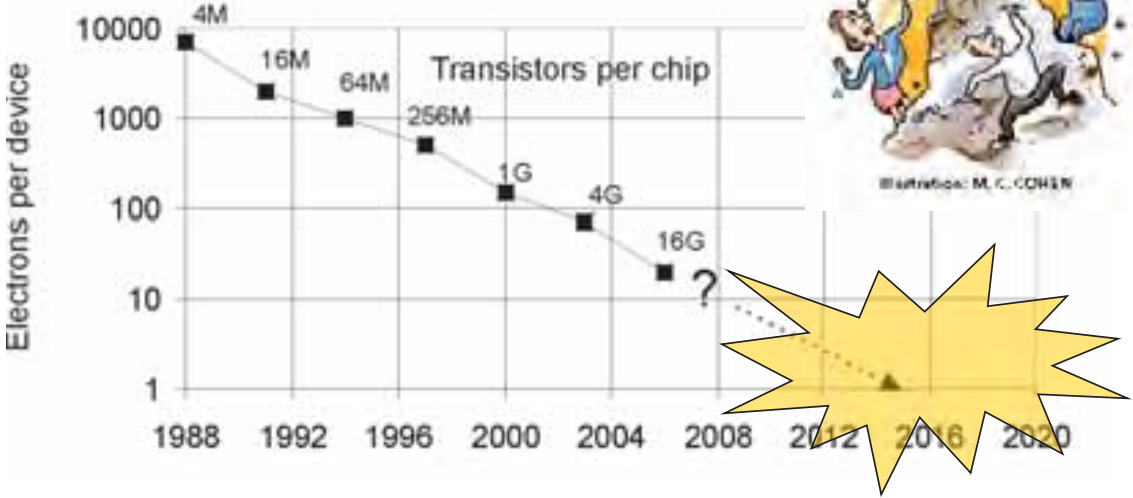
The paper gives an account of the author's work on a new form of quantum theory. §1. The Hamiltonian analogy between mechanics and optics. §2. The analogy is to be extended to include real "physical" or "undulatory" mechanics instead of mere geometrical mechanics. §3. The significance of wave-length;

The Nobel Prize in Physics 1933
Erwin Schrödinger, Paul A.M. Dirac

The Nobel Prize in Physics 1933 was awarded jointly to Erwin Schrödinger and Paul Adrien Maurice Dirac "for the discovery of new productive forms of atomic theory"

MI EZ?

MOORE TÖRVÉNYE



De meddig?

Quantum Manifesto

A New Era of Technology

May 2016

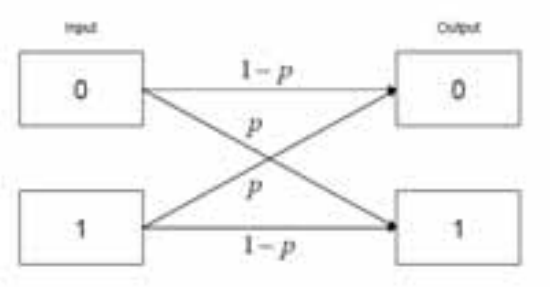
- http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf

A kvantumvilág működése

„Akit nem sokkolt a kvantum elmélet, az biztos nem is értette meg."

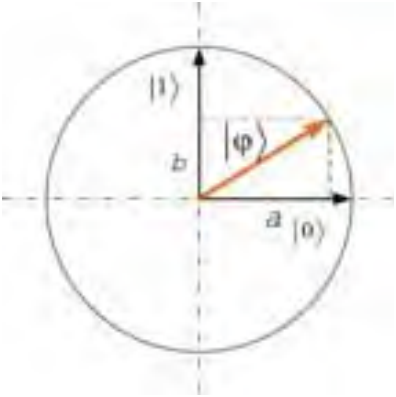
Niels Bohr

KVANTUM BIT (QUBIT)



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

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



MIT LEHET NÉHÁNY QUBITTEL KEZDENI?

$2^{64}-1=18.446.744.073.709.551.615$ búzaszem

Ez 70.097.624.700 t búza

210.624.700 t az EU termése

- 500 qbites regiszter:
  - több számot tartalmaz, mint a világegyetem atomjainak száma
  - És számolni is lehet ennyi számmal egyszerre!

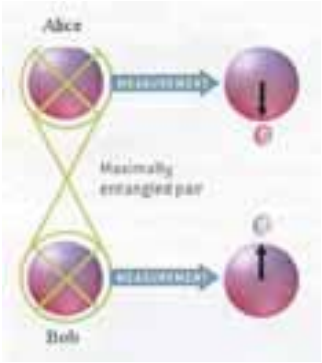
$$|\varphi\rangle = \sum_{i=0}^{2^n-1} \varphi_i |i\rangle$$

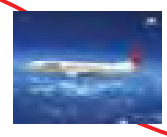
ÖSSZEFONÓDÁS (ENTANGLEMENT)

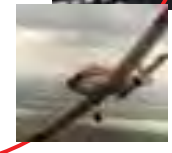
SŐT, AZ ÖLELÉS (ÖSSZEFONÓDÁS) MÁSRA IS JÓ!

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

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



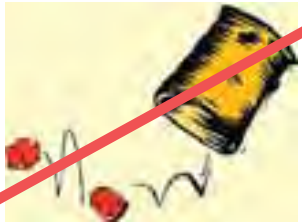




$$|\varphi\rangle = \varphi_0|00\rangle + \varphi_3|11\rangle$$

A VÉLETLEN TERMÉSZETE: TÉNYLEG VÉLETLEN ☺

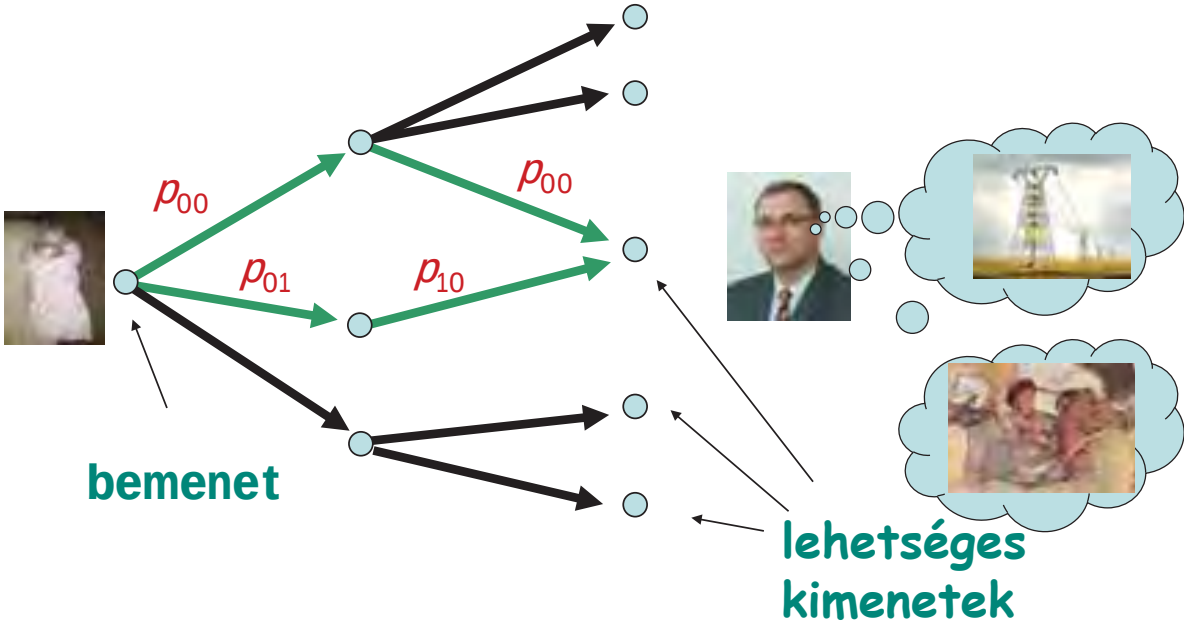
Isten nem dobókockázik a világgal!



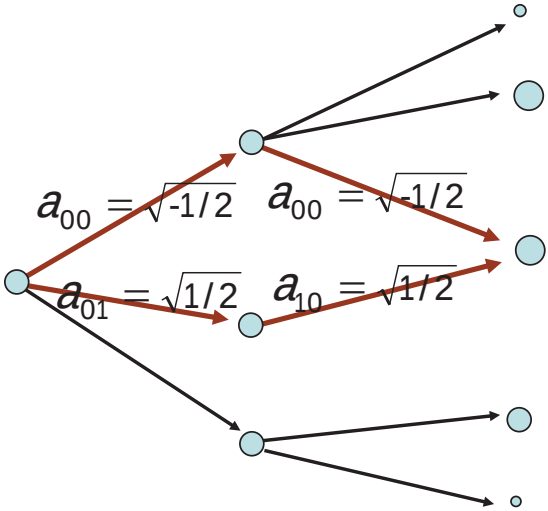
Dehogynem! Sőt, volt annyira nagyvonalú, hogy diffegyenletek helyett olykor elegendő feldobni egy kockát!

DETERMINISZTIKUS – AHOGY NEWTON ELKÉPZELTE A VILÁGOT

VALÓSZÍNŰSÉGI - AHOGY ÖNÖK ELKÉPZELIK A VILÁGOT



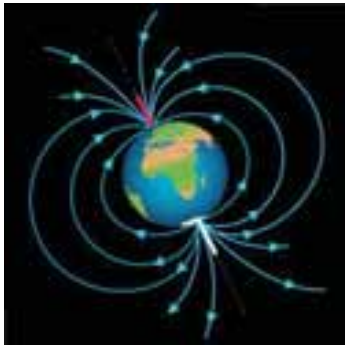
KVANTUM MŰKÖDÉS – ÉS AHOGY A VILÁG VALÓJÁBAN MŰKÖDIK



MAGYARÁZATOK – CSAK FILOZÓFIA IRÁNT ÉRDEKLŐDŐKNEK A TÖBBIEK SZUSSZANJANAK EGYET!

- **Lokalitás**: két pont között legrövidebb út az egyenes: papírlap
- **Létezés**: bizonyos tulajdonságok csak a megfigyeléskor kapnak értéket vagy folyamatosan keletkeznek az új univerzumok minden megfigyeléskor.
- **Logika**: Gödel tétele. „Minden ellentmondásmentes, a természetes számok elméletét tartalmazó, formális-axiomatikus elméletben megfogalmazható olyan állítás, mely se nem bizonyítható, se nem cáfolható.”

ERITHACUS RUBECULA – AZAZ VÖRÖSBEGY



https://youtu.be/VRIZA4cCl-U

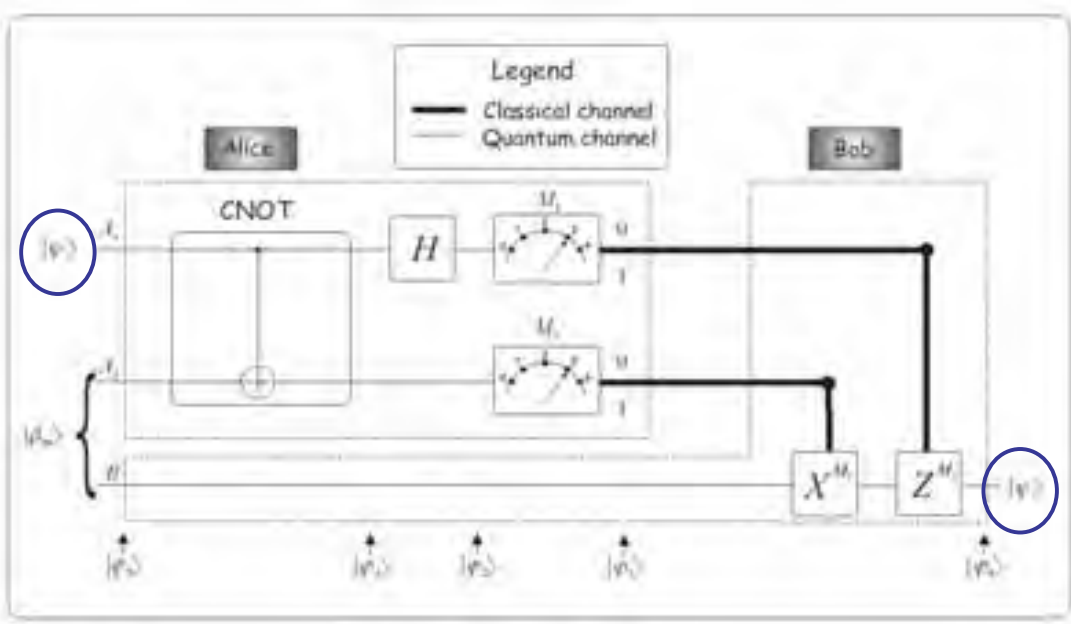
Alkalmazások

A kvantum elméletről: „Ha ez igaznak bizonyul, én kiszállok a fizikából!“

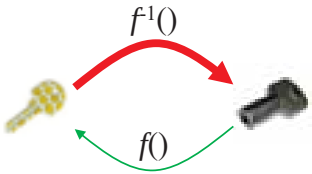
Max von Laue

TELEPORTÁLÁS

TELEPORTÁLÁS

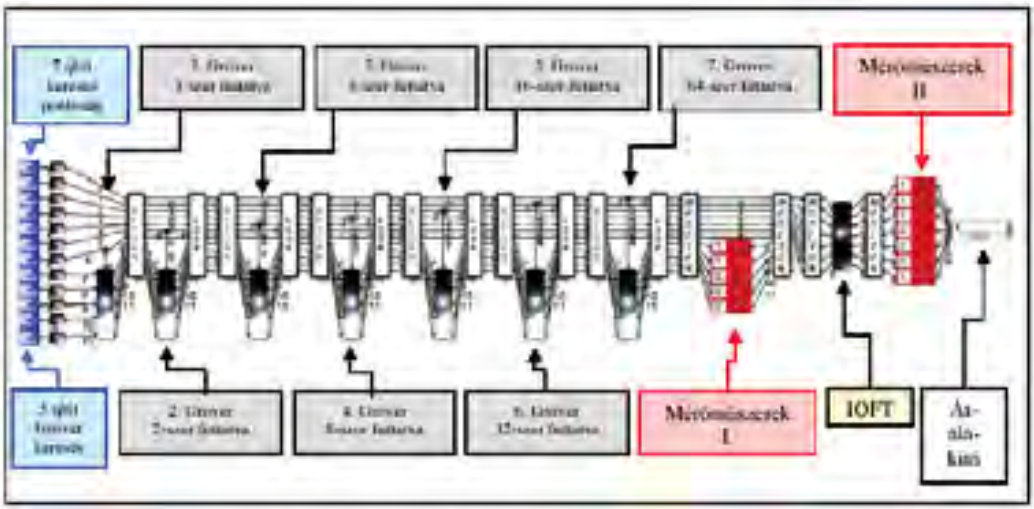


NYILVÁNOS KULCSÚ TITKOSÍTÁS



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

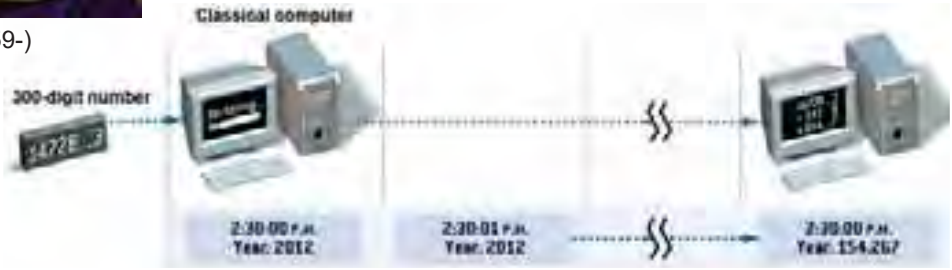
RSA FELTÖRŐ KVANTUM ÁRAMKÖR

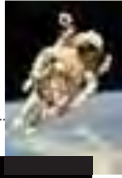


SHOR-ALGOTITMUS ÉS AZ RSA FELTÖRÉSE

Peter Shor (1959-)

152 000 év





Ádám (~ 150 000 BC)

152 000
év

Starman(2018-2002018)

SHOR-ALGORITMUS ÉS AZ RSA FELTÖRÉSE

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

152 000 év

1 másodperc

A KÓDTÖRÉS HATÉKONYSÁGA

Table 9.1 Code-breaking methods and related complexity

Method	$n = 128$	$n = 128$	$n = 1024$	$n = 1024$	1s barrier
BF	$1.8 \cdot 10^{7}$ s	0.58 year	$1.3 \cdot 10^{142}$ s	$4 \cdot 10^{134}$ year	80 bit
BC	$6 \cdot 10^{-4}$ s	$1.9 \cdot 10^{-11}$ year	$3.5 \cdot 10^{8}$ s	11.29 year	273 bit
G	$4 \cdot 10^{-3}$ s	$1.3 \cdot 10^{-10}$ year	$1.1 \cdot 10^{65}$ s	$3.7 \cdot 10^{57}$ year	159 bit
S	$2 \cdot 10^{-5}$ s	$6.6 \cdot 10^{-14}$ year	**0.01** s	$3.4 \cdot 10^{-11}$ year	**10000** bit

- BF: *brute force* classical method which scans the integer numbers from 2 to $\lceil \sqrt{N} \rceil$ with complexity $O(\sqrt{N})$.
- BC: *best classical* method requiring $O(\exp[c \cdot \mathrm{ld}^{\frac{1}{3}}(N)\mathrm{ld}^{\frac{2}{3}}(\mathrm{ld}(N))])$ steps.
- G: *Grover* search based scheme with $O(N^{\frac{1}{4}})$.
- S: *Shor* factorization with $O(\mathrm{ld}(N)^3)$.

Brutális!

Arnold Schwarzenegger (1947-)

"... 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)

D-WAVE

- 2017 jan: D-Wave2000Q

D-Wave

IBM KVANTUM SZÁMÍTÓGÉP

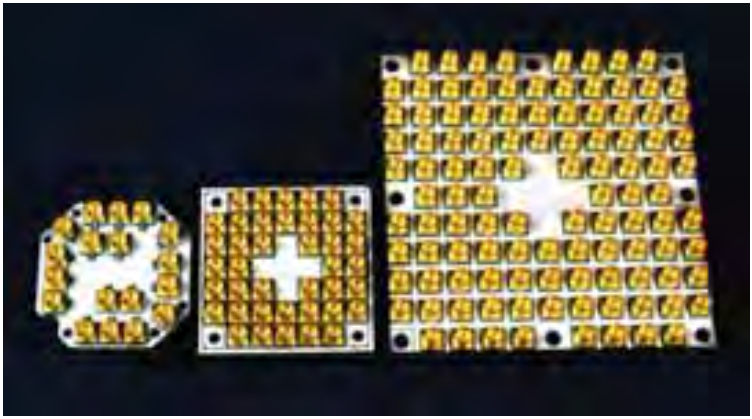
2016: 5 qubit

2017: 16 qubit

IBM Q Awards:
https://qx-awards.mybluemix.net/

News 2018 !!!

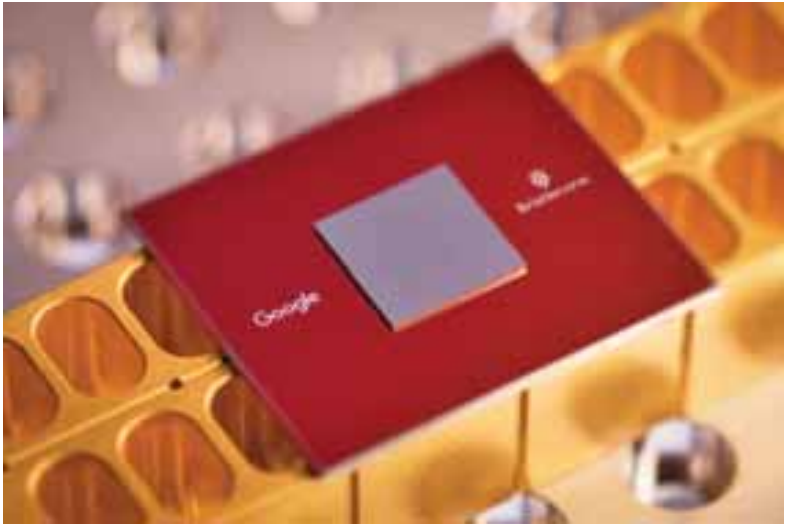
INTEL KVANTUM PROCESSZOROK



News
2018 !!!

- Intel Corporation's 49-qubit quantum computing test chip, code-named "Tangle Lake," is unveiled at 2018 CES in Las Vegas.
- https://www.extremetech.com/computing/261734-intel-unveils-new-quantum-computer-declares-quantum-breakthrough

GOOGLE 2018 MÁRCIUS



- https://index.hu/tech/2018/03/07/a_google_ettol_a_csiptol_varja_a_kvantumszamitogepes_attorest/

MICROSOFT KVANTUM FEJLESZTŐ RENDSZER

- Kvantum programozási nyelv: Q#

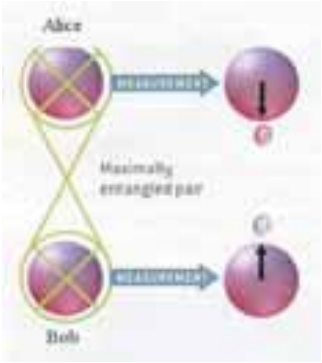
```
operation BellTest (count : Int, initial: Result) : (Int,Int)
{
    body
    {
        mutable numOnes = 0;
        using (qubits = Qubit[1])
        {
            for (test in 1..count)
            {
                Set (initial, qubits[0]);

                let res = M (qubits[0]);

                // Count the number of ones we saw:
                if (res == One)
                {
                    set numOnes = numOnes + 1;
                }
            }
            Set(Zero, qubits[0]);
        }
        // Return number of times we saw a |0> and number of times we saw a |1>
        return (count-numOnes, numOnes);
    }
}
```

News 2018 !!!

A LEGNAGYOBB KIHÍVÁS AZ ÖSSZEFONÓDÁS!

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

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

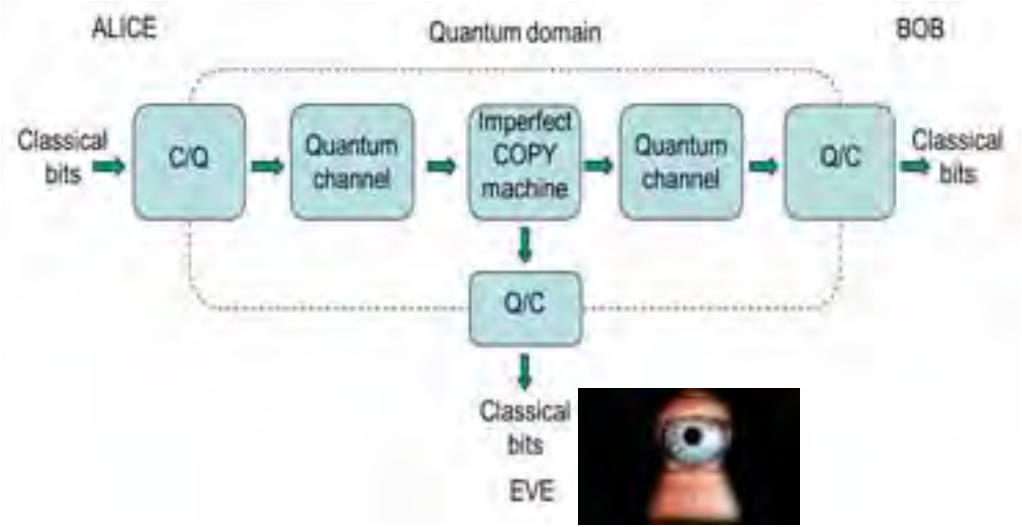


SZIMMETRIKUS TITKOSÍTÁS

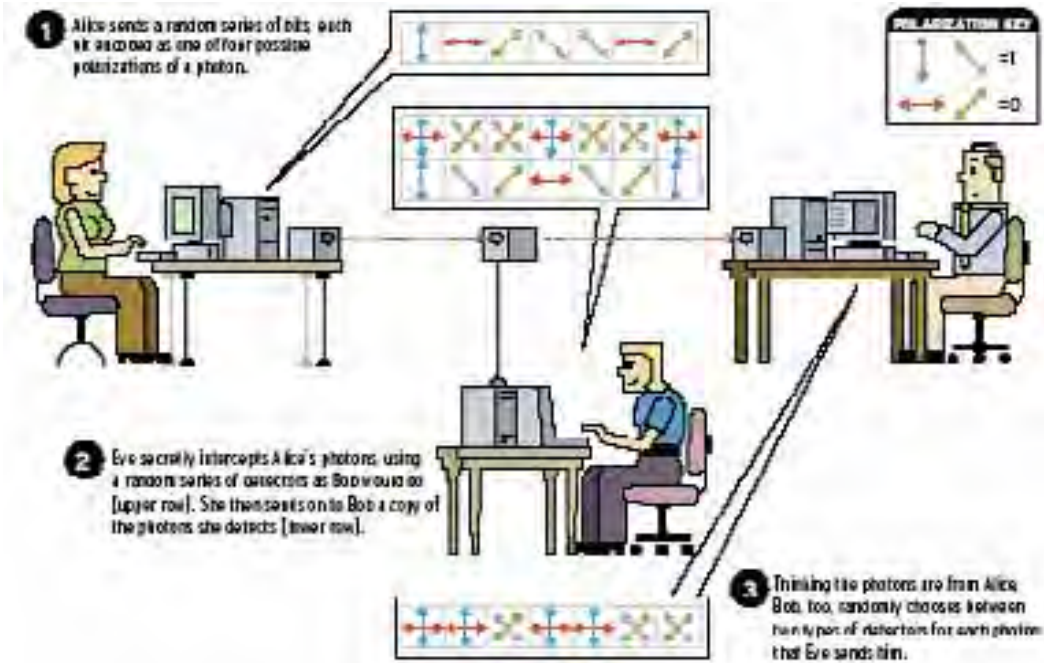
- Szimmetrikus kulcsú titkosítás
  - Egyforma kulcsok mindkét oldalon
- Abszolút biztonságos, ha bizonyos előírásokat betartunk
- Gond, hogy a kulcsot miként juttassuk el a túloldalra????

KVANTUM KULCSSZÉTOSZTÁS (QKD)

- No Cloning tétel: ismeretlen, egymásra nem merőleges állapotokat lehetetlen tökéletesen lemásolni.

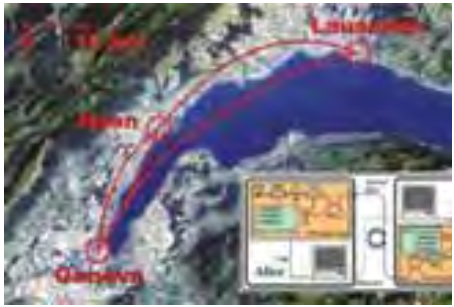


KVANTUM KULCSSZÉTOSZTÁS

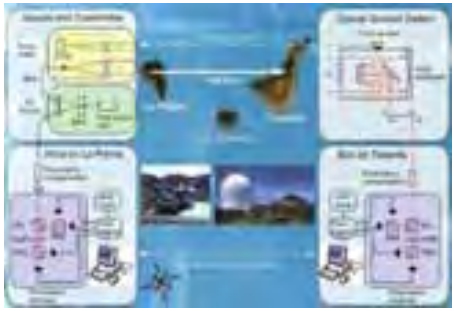


A KULCSSZÉTOSZTÁS TÖRTÉNETE

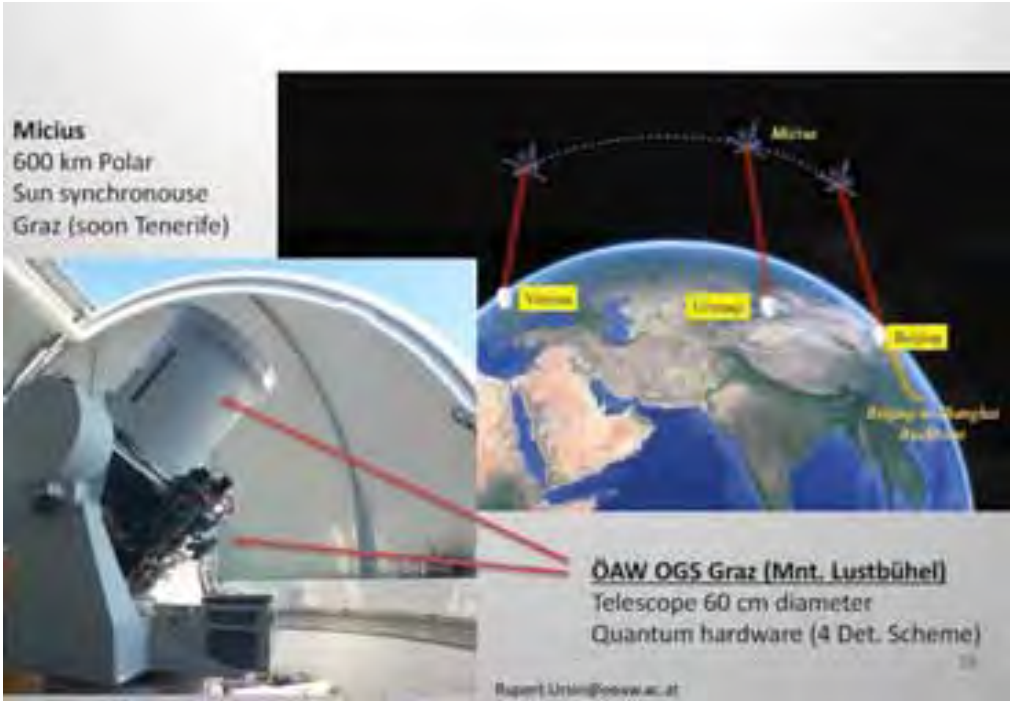
Optikai kábel	
1989/91	30 cm
1993	1100 m
1995	23 km
2007	67 km
2016	404 km



Szabad légkör	
1996	75 m
1998	1 km
2001	2 km
2002	10 km
2007	144 km



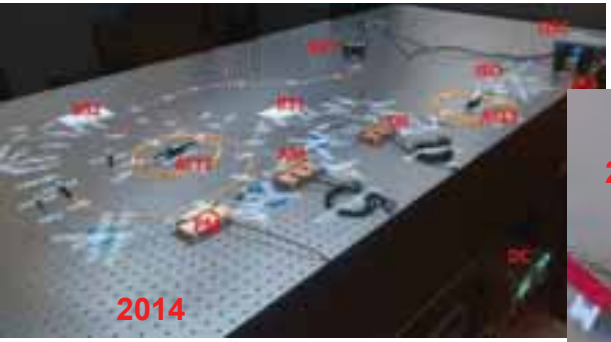
QUESS 2017 (QUANTUM EXPERIMENTS AT SPACE SCALE)

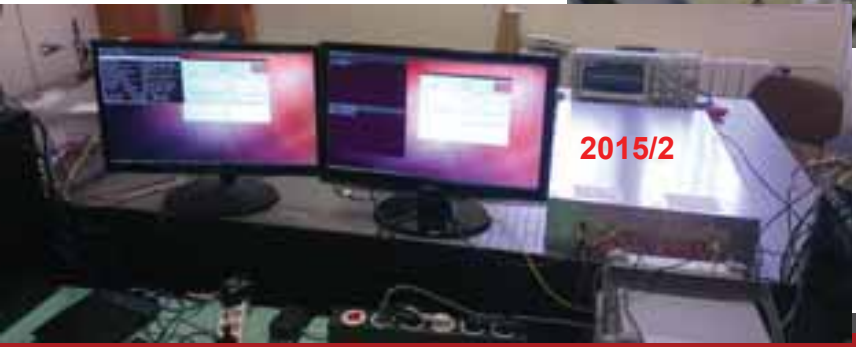

Micius
600 km Polar
Sun synchronouse
Graz (soon Tenerife)
ÖAW OGS Graz (Mnt. Lustbühel)
Telescope 60 cm diameter
Quantum hardware (4 Det. Scheme)

ENTANGLEMENT ALAPÚ KÍSÉRLET 2017

- Tengerfenéki kábel
- Prof. Rupert Ursin

AHOGY MI KULCSSZÉTOSZTUNK





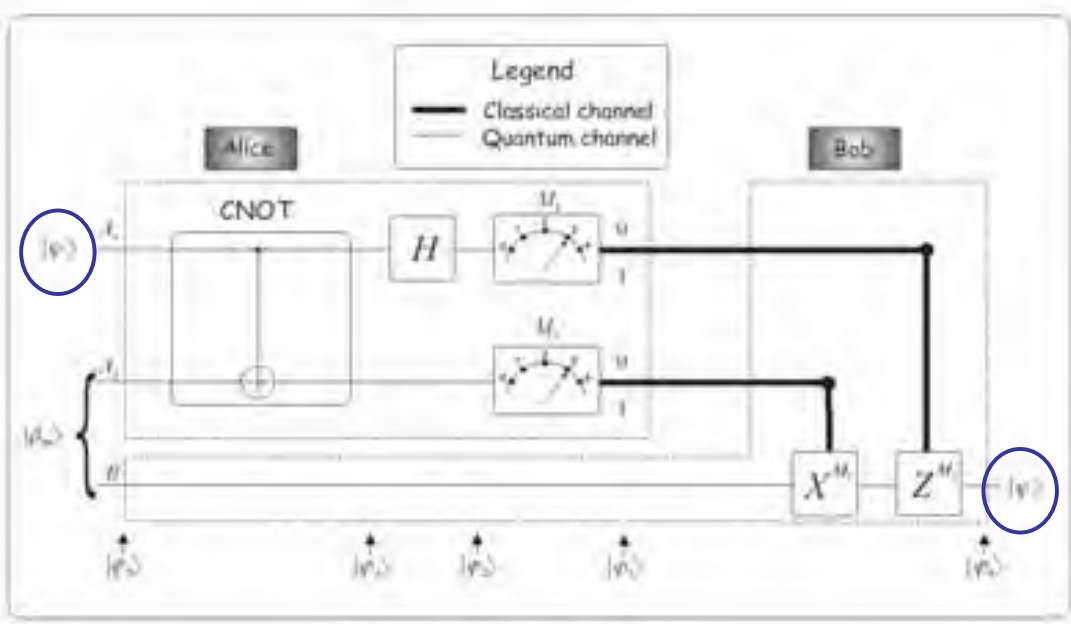
MÁR BOLTBAN IS KAPHATÓ!

KIHÍVÁSOK

- Csak pont-pont összeköttetések működnek, véges távolságra.
- A jelenleg használt távközlési optikai szálak is alkalmasak.

- Hogyan növeljük a távolságot?
  - Erősíteni kellene, DE NO-cloning tétel az utunkba áll…

TELEPORTÁLÁS



KIHÍVÁSOK

- Hogyan érjünk el több felhasználót?
  - Kapcsolók, útvonalválasztók

PuskásTivadar (1844-1893)

ADATBÁZIS KERESÉS TÖRTÉNETE V3

ADATBÁZIS KERESÉS TÖRTÉNETE V4: GROVER-ALGORITMUS

Lov Grover (1961-)

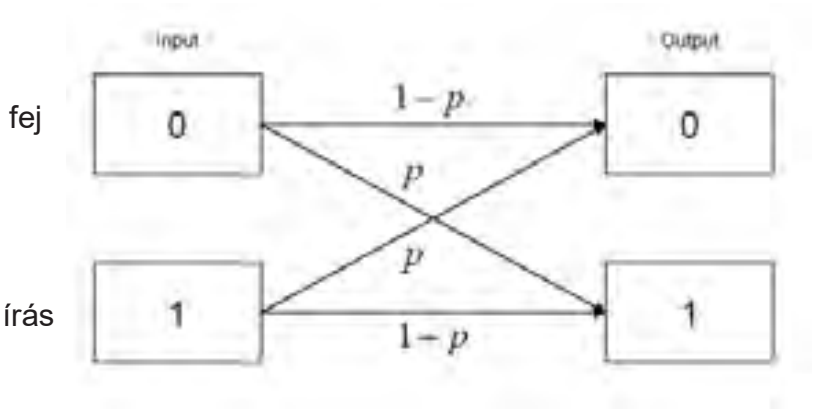
- Aki keres, talál! De nem mindegy mennyi idő alatt.
- Rendezetlen adatbázis *N* különböző elemmel.
- Klasszikusan *N* kérés szükséges.
- Ugyanakkor kvantum módon:

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

$x = ?$

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

PÉNZÉRME MINT KOMMUNIKÁCIÓS CSATORNA

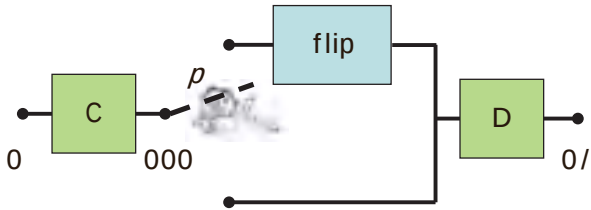


Kérdés: mennyi információt lehet rajta továbbítani?

EGY EGYSZERŰ CSATORNA MODELL

$p_{ij}=½ \Rightarrow C=1-H(p)=0$

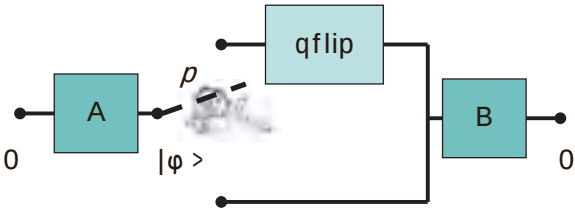
Klasszikus csatorna



Csak redundanciával tartható kordában a hibázás valószínűsége

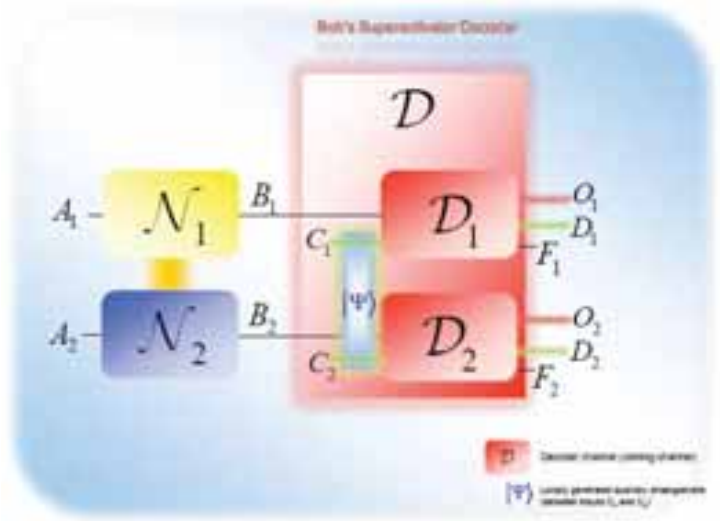
$p_{ij}=½ \Rightarrow C=1$

Kvantum csatorna



Bizonyos esetekben egyszerű kódolással HIBAMENTESSÉ tehető.

OK, EZT MÉG LENYELTÜK, DE ILYEN ÁLLAT NINCS:



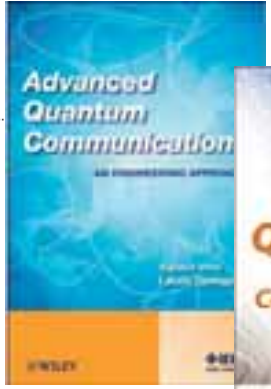
- 2 db. külön-külön $C = 0$ kapacitású csatorna ügyesen összekapcsolva mégis képes információt átvinni!

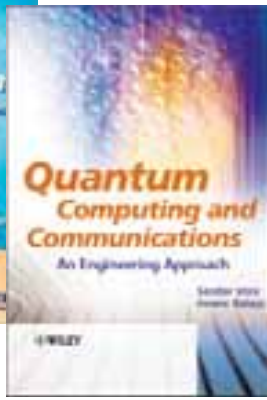
HUNQUTECH PROJECT

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!

TOVÁBBI INFORMÁCIÓK





IMRE@HIT.BME.HU

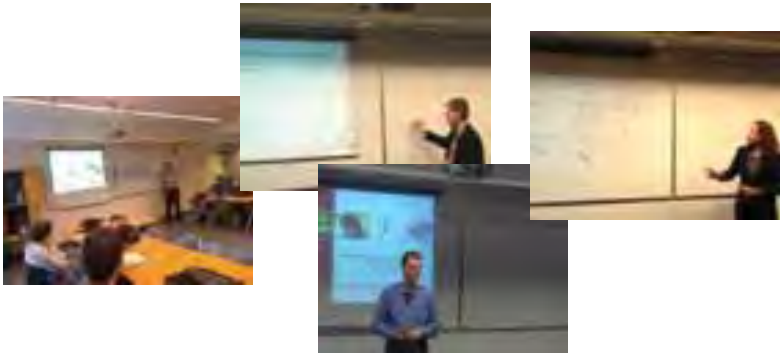
Aki a kvantumos világra kíváncsi:
http://www.mcl.hu/quantum//

SZVT: Bevezetés a kvantum informatikába lés kommunikációba
https://www.vik.bme.hu/kepzes/targyak/VIHIAV06/

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

BEVEZETÉS A KVANTUM-INFORMATIKÁBA (12 PUBLIKUS FELVÉTEL)

- http://videotorium.hu/hu/search/any/Bevezet%C3%A9s%20a%20kvantum-informatik%C3%A1ba



KÉRDÉSEK/MEGJEGYZÉSEK