



## 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@hit.bme.hu

- BME



- Villamosmérnöki és Informatikai Kar



- Hálózati rendszerek és Szolgáltatások Tanszék



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

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

## 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. SCHRODINGER

#### ABSTRACT

The paper gives an account of the author's work on a new form of quantum theory. I. The Hamiltonian analogy between mechanics and optics. II. The analogy is to be extended to include not "physical" or "undulatory" mechanics (instead of mere geometrical mechanics). III. The significance of wave-length;



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

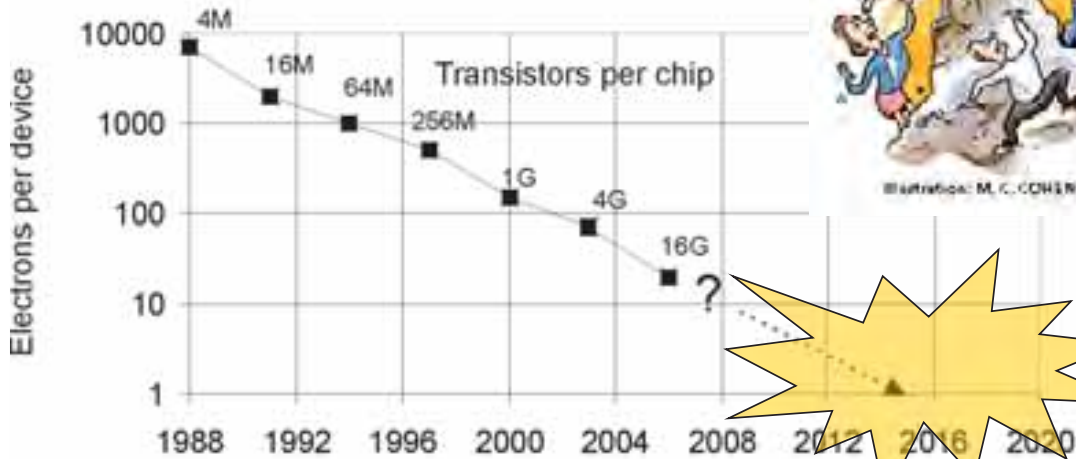
The Nobel Prize in Physics 1933 was awarded jointly to Erwin Schrödinger and Paul Adrien Maurice Dirac "for the discovery of new subatomic forms of a particle theory"



# MI EZ?



# MOORE TÖRVÉNYE



De meddig?

# Quantum Manifesto

A New Era of Technology

May 2016

## Quantum Technologies Timeline



Year	Quantum Cryptography	Quantum Simulation	Quantum Computing	Quantum Communication	Quantum Sensing	Quantum Imaging
2015	Quantum key distribution (QKD) systems are deployed for secure communication.	Quantum simulation of molecular structures is used for drug discovery.	Quantum computing is used for optimization problems in logistics.	Quantum communication networks are established for secure data transfer.	Quantum sensors are used for precision measurements in navigation.	Quantum imaging techniques are used for medical diagnostics.
2020	Quantum key distribution (QKD) systems are widely used for secure communication.	Quantum simulation of molecular structures is used for drug discovery.	Quantum computing is used for optimization problems in logistics.	Quantum communication networks are established for secure data transfer.	Quantum sensors are used for precision measurements in navigation.	Quantum imaging techniques are used for medical diagnostics.
2025	Quantum key distribution (QKD) systems are widely used for secure communication.	Quantum simulation of molecular structures is used for drug discovery.	Quantum computing is used for optimization problems in logistics.	Quantum communication networks are established for secure data transfer.	Quantum sensors are used for precision measurements in navigation.	Quantum imaging techniques are used for medical diagnostics.
2030	Quantum key distribution (QKD) systems are widely used for secure communication.	Quantum simulation of molecular structures is used for drug discovery.	Quantum computing is used for optimization problems in logistics.	Quantum communication networks are established for secure data transfer.	Quantum sensors are used for precision measurements in navigation.	Quantum imaging techniques are used for medical diagnostics.



Atomic quantum clocks can be synchronized with GPS to provide very high levels of timing stability and accuracy even in hostile environments where GPS is unavailable or denied. These timing solutions can be useful within future smart networks, for instance for the synchronization of energy grids, as well as in telecoms, navigation, energy and security.



Quantum sensors that exploit quantum superposition and/or entanglement to achieve a higher sensitivity and resolution will be purchased and used by companies and public institutions for demanding metrological purposes. In particular, to measure earth under the ground and to detect mineral deposits in legacy infrastructure. They will also be used to provide turn-in-time points-of-care diagnosis.



A secure quantum link between a number of European capitals will allow transmission of highly sensitive data without any risk of interception. It may contain ground or satellite-based ground-based nodes derived from the development of trusted nodes and quantum-repeater.



Quantum simulation will be established for the special purpose of simulating materials or chemical reactions. Simulation allows new processes or properties to be explored before the material exists, as a tool to design new materials that are needed in mobile devices, such as energy or transport.



A global quantum-safe communications network – a quantum internet connecting quantum with classical information and encryption – offers security for many transactions against the threat of a quantum computer breaking private classical encryption schemes.



Universal quantum computers will be available with computational power at a level of performance that will exceed even the most powerful classical computers of the future. They will be reprogrammable machines used to solve demanding computational problems, such as optimization tasks, database searches, machine learning and image recognition. They will contribute to Europe's smart industry, helping to make European manufacturing industries more efficient.



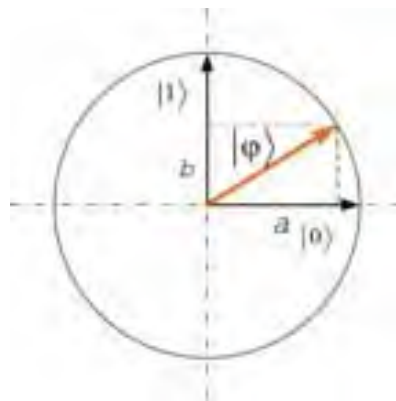
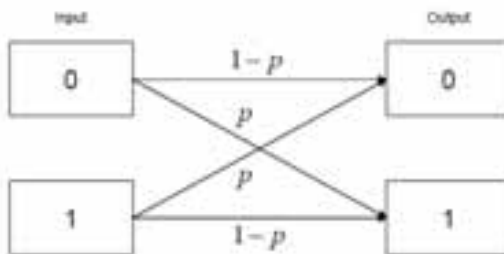
# A kvantumvilág működése

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

*Niels Bohr*



# KVANTUM BIT (QUBIT)



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

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

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

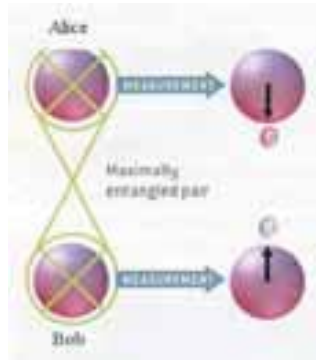


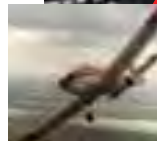
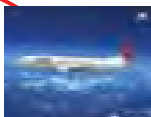
Az ölelés megnyugtat, csökkenti a félelmeket,  
a szorongást, és a magányosság érzését.

# SŐT, AZ ÖLELÉS (ÖSSZEFONÓDÁS) MÁSRA IS JÓ!

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

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



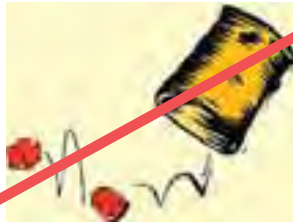


$$|\varphi\rangle = \varphi_0|00\rangle + \varphi_3|11\rangle$$

# A VÉLETLEN TERMÉSZETE: TÉNYLEG VÉLETLEN 😊



Isten nem  
dobókockázik a világgal!

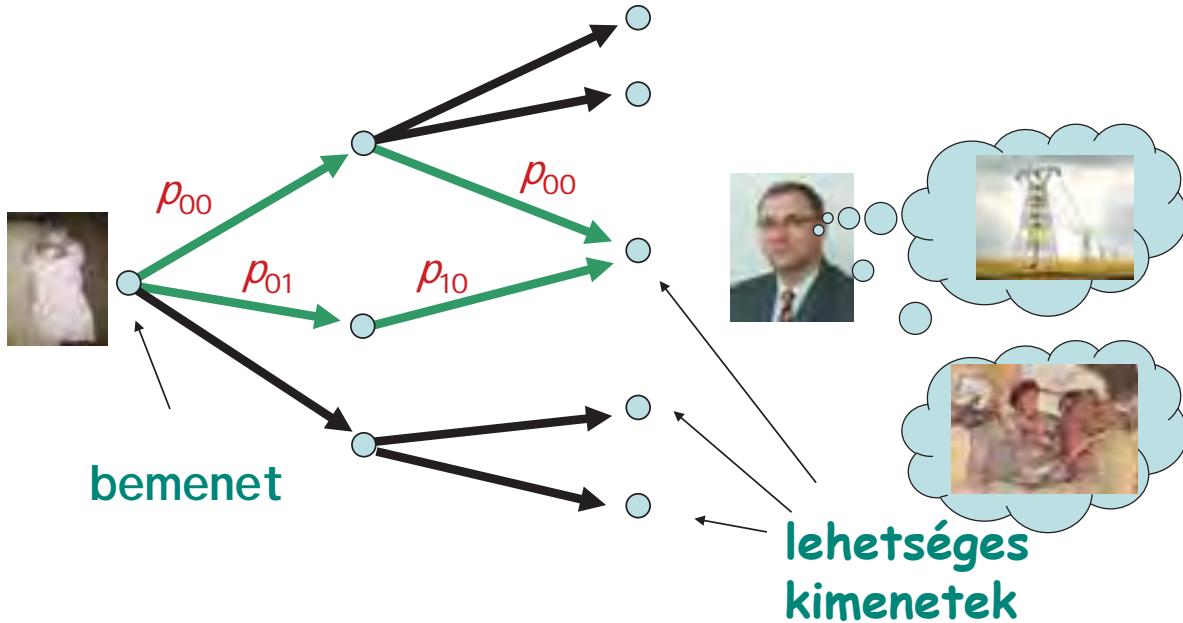


Dehogynem! Sőt, volt  
annyira nagyvonalú, hogy  
diffégenletek helyett  
olykor elegendő feldobni egy  
kockát!

# DETERMINISZTIKUS – AHOGY NEWTON ELKÉPZELTE A VILÁGOT

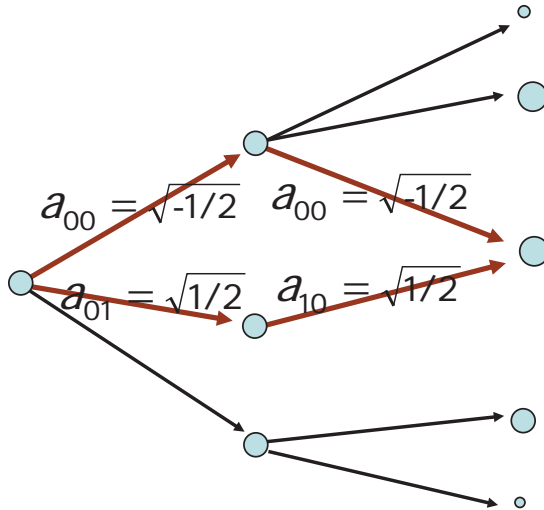


# VALÓSZÍNŰSÉGI - AHOGY ÖNÖK ELKÉPZELIK A VILÁGOT





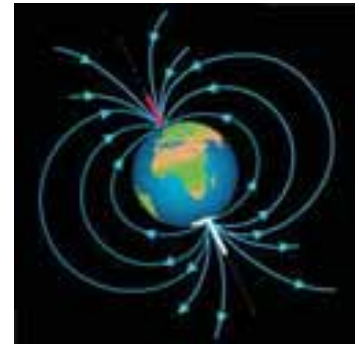
# KVANTUM MŰKÖDÉS – ÉS AHOGY A VILÁG VALÓJÁBAN MŰKÖDIK



# MAGYARÁZATOK – CSAK FILOZÓFIA IRÁNT ÉRDEKLŐDŐKNEK A TÖBBIÉK 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/VRIZA4cCI-U>



## Alkalmazások

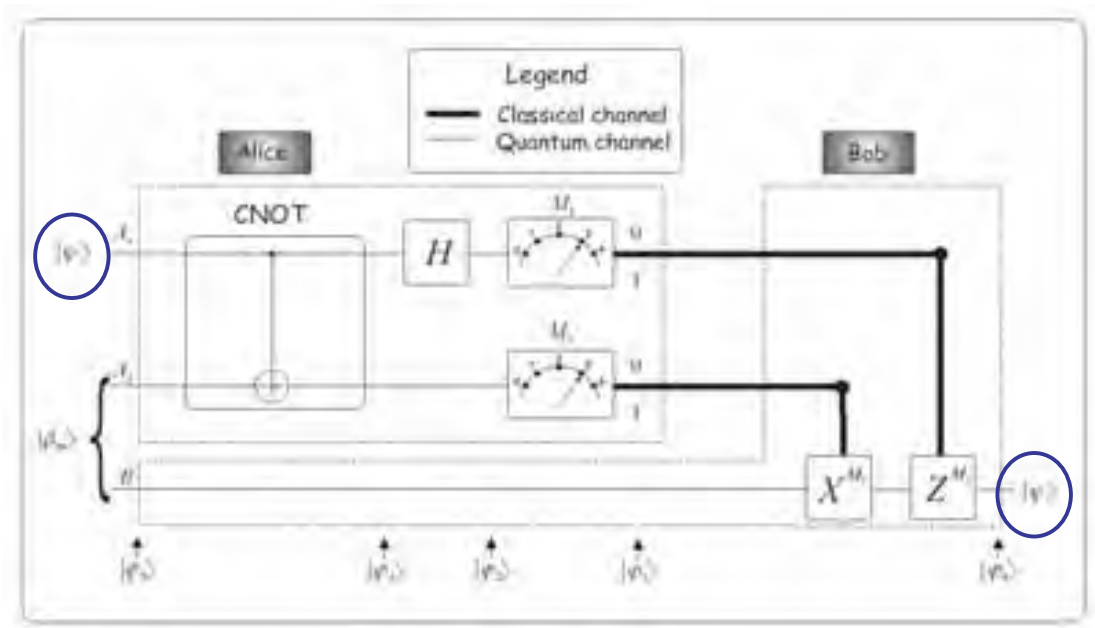
A kvantum elméletről: „Ha ez igaznak bizonyul, én kiszállok a fizikából!”

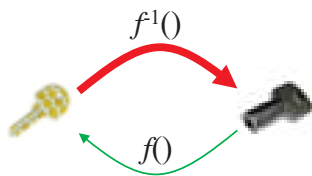
*Max von Laue*

# TELEPORTÁLÁS



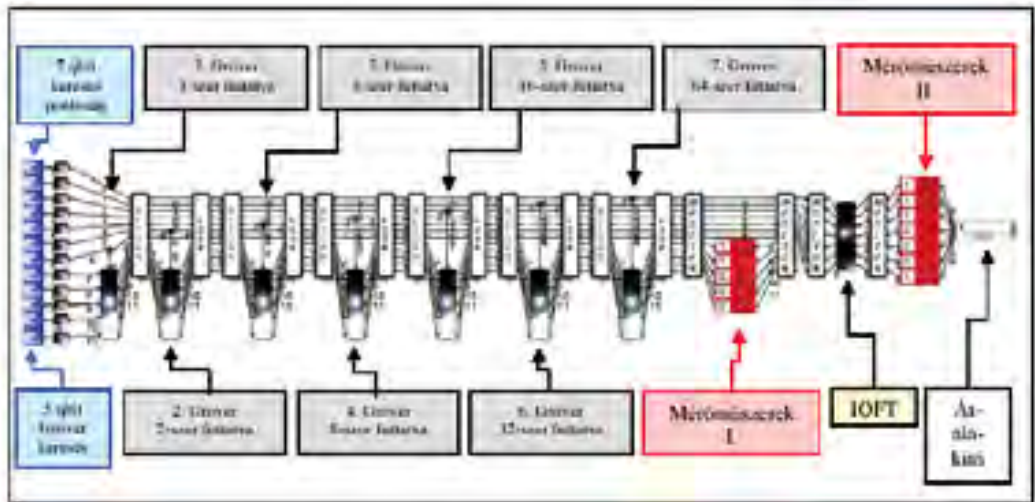
# TELEPORTÁLÁS





- Nyilvános kulcsú titkosítás
  - nyilvános titkosítókulcs, titkos fejtőkulcs
  - kulcsok előállítás: két nagy prímszám szorzatát felhasználva
  - feltörés: a törzstényezők meghatározása
- A mai napig nem sikerült bizonyítani, 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



152 000  
év

Peter Shor (1959-)





Ádám (~ 150 000 BC)

152 000  
év



Starman(2018-2002018)



# SHOR-ALGORITMUS ÉS AZ RSA FELTÖRÉSE

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

152 000 év



1 másodperc

BRYAN CHRISTIE DESIGN

# 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	<b>10000</b> 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  $O(\exp[e \cdot \text{ld}^{\frac{1}{3}}(N) \text{ld}^{\frac{2}{3}}(\text{ld}(N))])$  steps.
- G: *Grover* search based scheme with  $O(N^{\frac{1}{4}})$ .
- S: *Shor* factorization with  $O(\text{ld}(N)^3)$ .



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



# IBM KVANTUM SZÁMÍTÓGÉP



2016: 5 qubit



2017: 16 qubit

IBM Q Awards:

<https://qx-awards.mybluemix.net/>

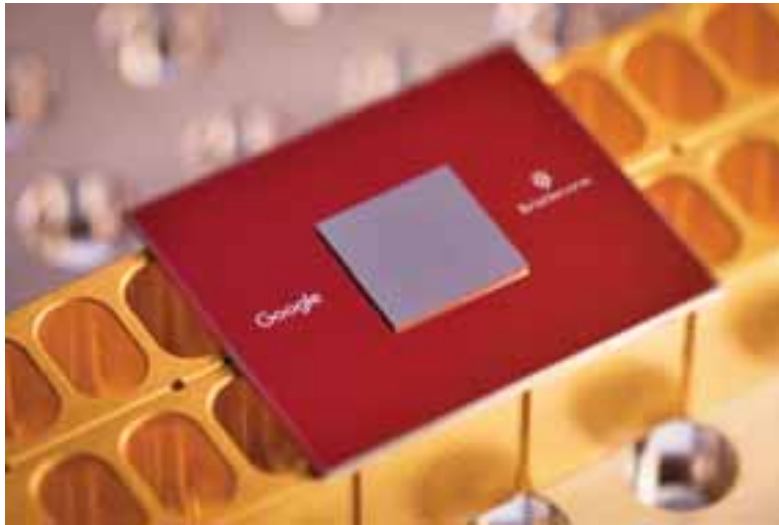
News 2018 !!!



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>





- [https://index.hu/tech/2018/03/07/a\\_google\\_ettol\\_a\\_csiptol\\_varja\\_a\\_kvantumszamitogepes\\_attoreset/](https://index.hu/tech/2018/03/07/a_google_ettol_a_csiptol_varja_a_kvantumszamitogepes_attoreset/)

- Kvantum programozási nyelv: Q#

```
operation MallocTest (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);
    }
}
```

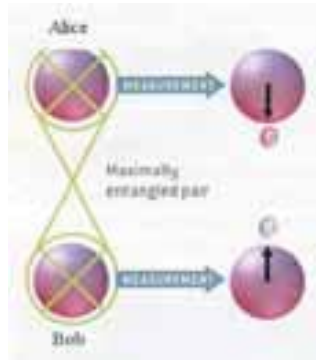


**News 2018 !!!**

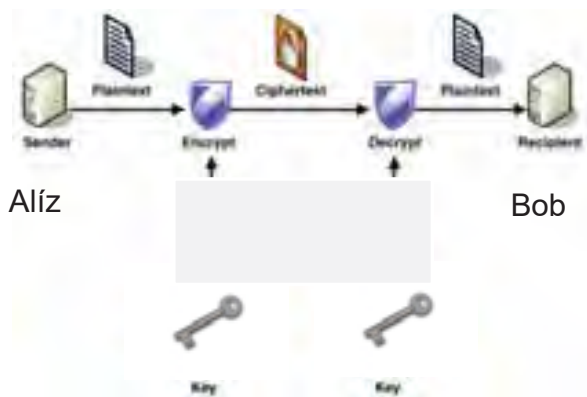
# A LEGNAGYOBB KIHÍVÁS AZ ÖSSZEFONÓDÁS!

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

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

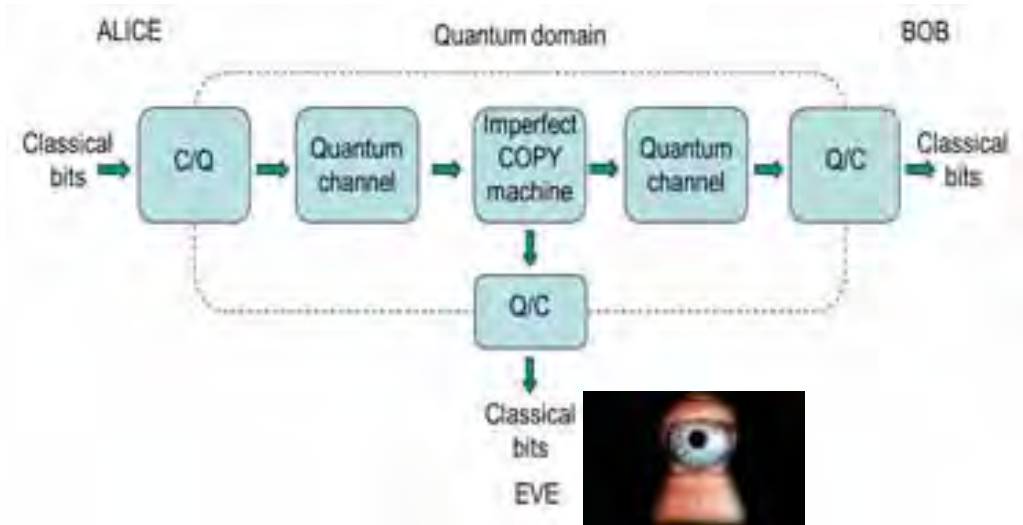


# SZIMMETRIKUS TITKOSÍTÁS

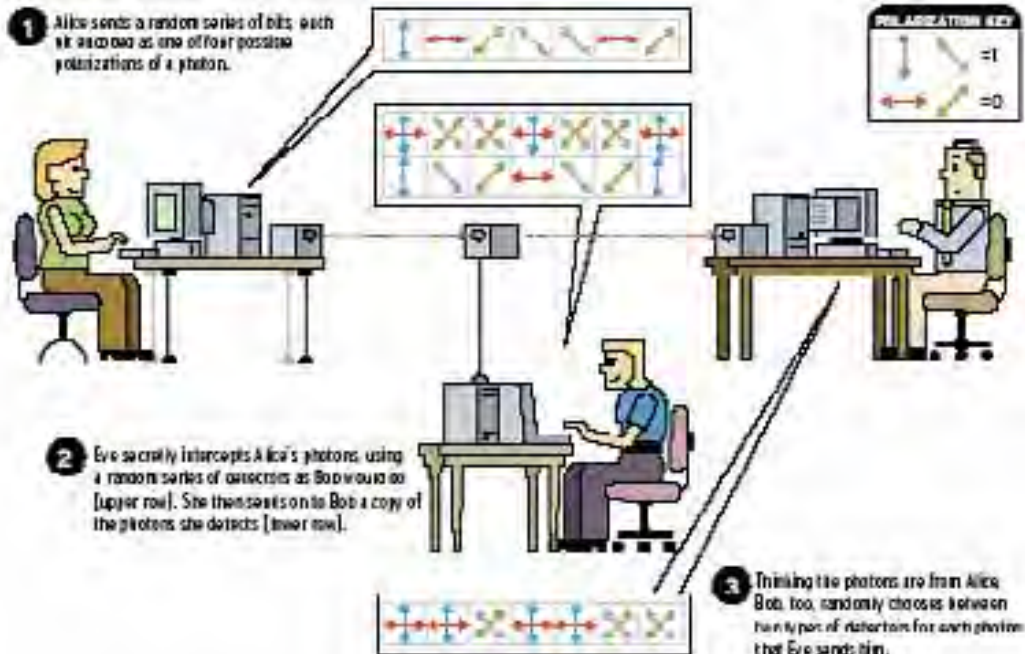


- Szimmetrikus kulcsú titkosítás
  - Egyforma kulcsok mindkét oldalon
- Abszolút biztonságos, ha bizonyos előírásokat betartunk
- Gond, hogy a kulcsot miként juttassuk el a túloldalra????

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



# KVANTUM KULCSSZÉTOSTÁS



# A KULCSSZÉTOSTÁS TÖRTÉNETE



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



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



# QUESS 2017 (QUANTUM EXPERIMENTS AT SPACE SCALE)





**Micrus**  
600 km Polar  
Sun synchronous  
Graz (soon Tenerife)

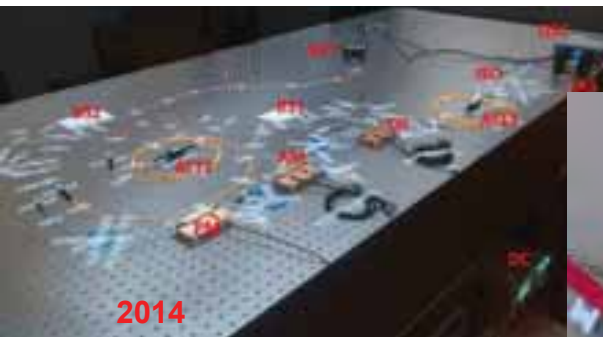
**ÖAW OGS Graz (Mt. Lustbühel)**  
Telescope 60 cm diameter  
Quantum hardware (4 Det. Scheme)

Rupert Ursin@oaw.ac.at

- Tengerfenéki kábel
- Prof. Rupert Ursin



# AHOGY MI KULCSSZÉTO SZTUNK



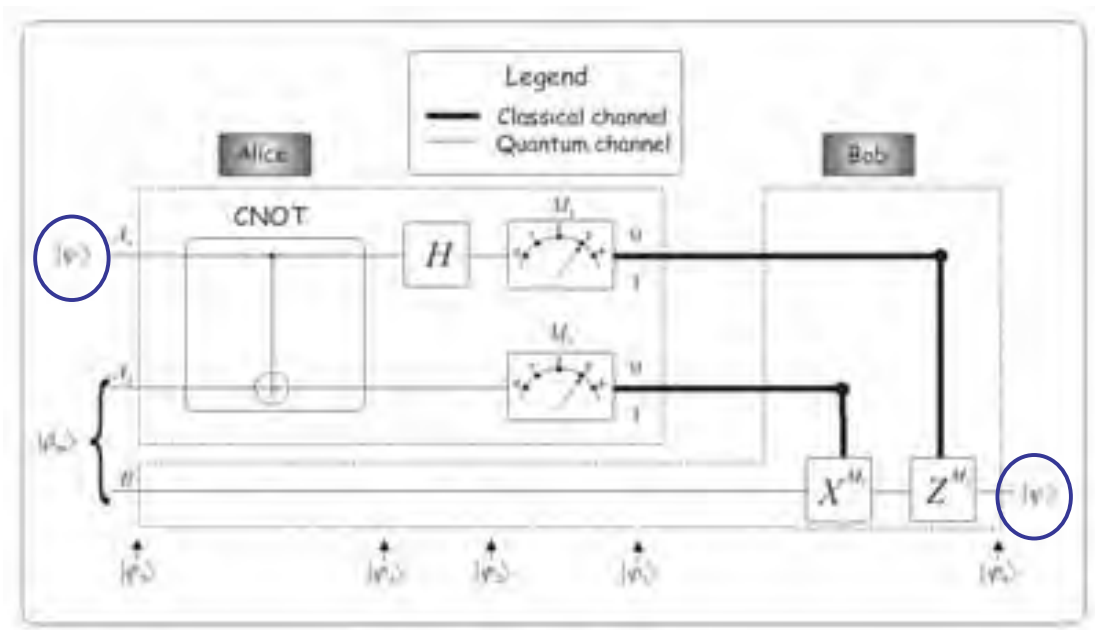
# MÁR BOLTBAN IS KAPHATÓ!



- 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



- 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:

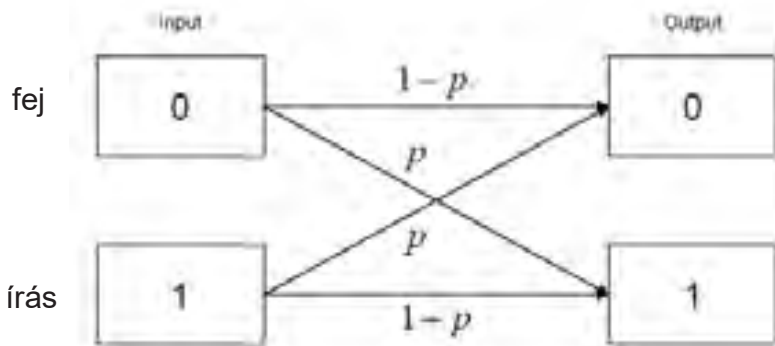
$$O(\sqrt{N})$$

$X = ?$



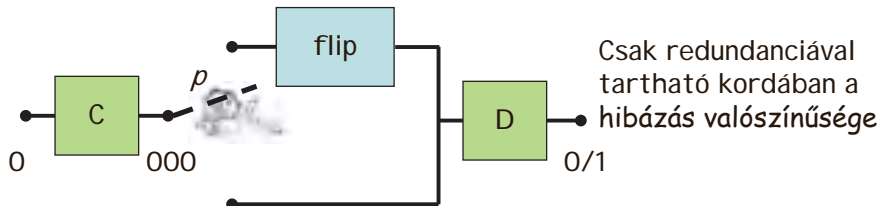
- **Miért örülünk ennek?**
  - Informatika: pl. adatbázis kezelés
  - Távközlés: pl. útvonalválasztás, jelfeldolgozás

# PÉNZÉRME MINT KOMMUNIKÁCIÓS CSATORNA



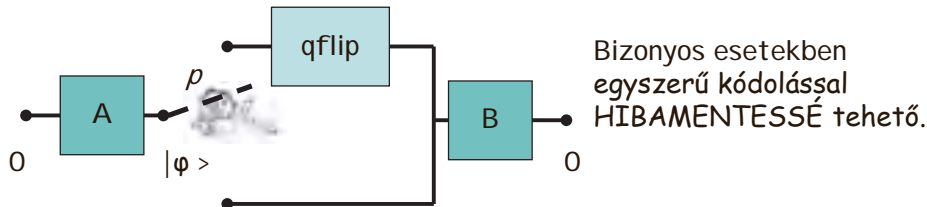
Kérdés: mennyi információt lehet rajta továbbítani?

Klasszikus csatorna



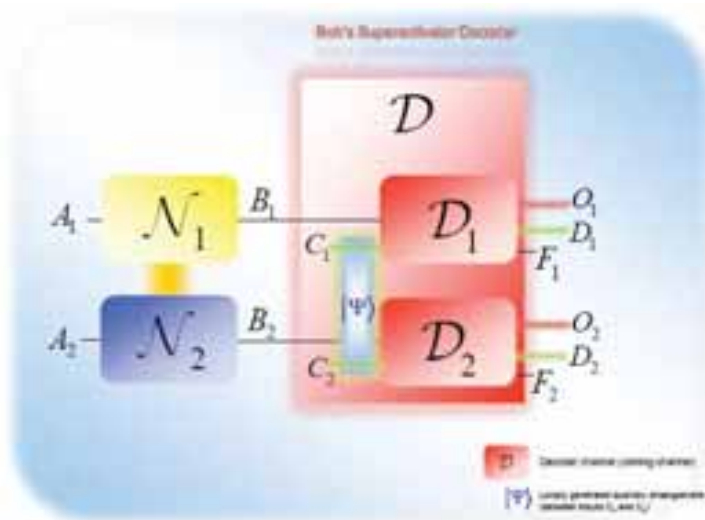
$$p_{ij} = \frac{1}{2} \longrightarrow C = 1 - H(p) = 0$$

Kvantum csatorna



$$p_{ij} = \frac{1}{2} \longrightarrow C = 1$$

# OK, EZT MÉG LENYELTÜK, DE ILYEN ÁLLAT NINCS:



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

## MEGHÍVÓ

sajtótájékoztatóra

### PROGRAM

10.00

Készítők

**Dr. Lovász László**

Hagyai Tudományos Akadémia Elnöke

**Dr. Pálincás József**

a Nemzeti Kifejtési, Fejlesztési,  
és Innovációs Hivatal elnöke

10.10

A program szakmai  
ismertetése

**Dr. Domokos Péter**

HunQutech kutatócsoport vezetője,  
MTA Wigner Fizikai Kutatóközpont

10.40 Kérdések-válaszok

11.15 Befeje

A Hálózati Rendszerek, Szolgáltatások Tanszék  
száma: 0636-4630000, honlap: [www.hit.tud.elte.hu](http://www.hit.tud.elte.hu)

A HunQutech projekt a Nemzeti Kifejtési, Fejlesztési, és Innovációs Hivatal (NKFIH) támogatásával valósul meg. A projekt célja a magyarországi tudományos és technológiai kutatások és fejlesztések közötti együttműködés erősítése, valamint a nemzetközi kapcsolatok kiépítése. A projekt keretében a HUNQUTECH projekt a Nemzeti Kifejtési, Fejlesztési, és Innovációs Hivatal (NKFIH) támogatásával valósul meg.

A HunQutech konzorciuma

a ELTE, ELTE-BRC, ELTE-ÁNYOS, ELTE-ÁNYOS-ELTE

és a Magyar Tudományos Akadémia (MTA) Wigner Fizikai Kutatóközpontjának

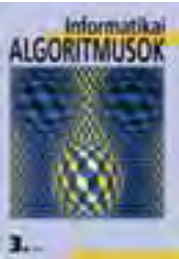
kooperatív partnerségében működik.

## SAJTÓTÁJÉKOZTATÓJUKRA

az MTA Széchenyi Konferenciaközpontjában  
2018. február 7-én, szerdán 10.00 órára.



- 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!

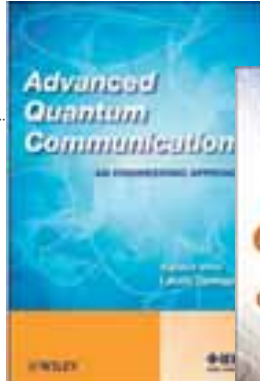


ATI RENISZTER  
LGALTATÁSOK  
EK

## TOVÁBBI INFORMÁCIÓK



**IMRE@HIT.BME.HU**



Aki a kvantumvilágra kíváncsi:

<http://www.mcl.hu/quantum//>

SZVT: Bevezetés a kvantum informatikába és kommunikációba

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

Aki esetleg rám kíváncsi:

<http://www.hit.bme.hu/people/imre/>

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

