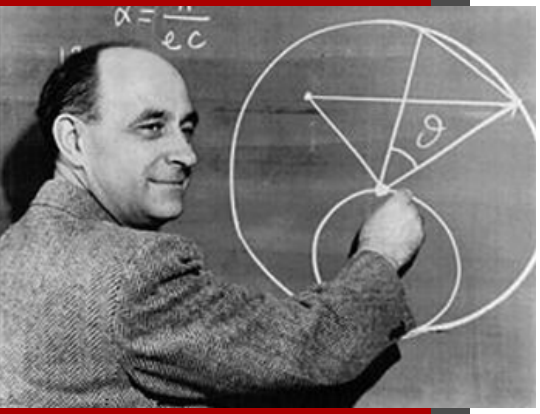
Kvantum informatika és kommunikáció – lehetőségek és kihívások

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

Imre Sándor, BME-HIT

MIRŐL LESZ MA SZÓ?

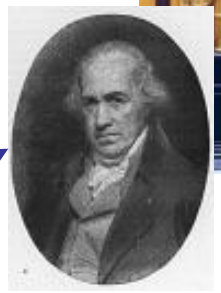
- Motivációk
- A kvantum működés alapelvei – **összefonódás**
- Alkalmazási területek – Hol tart ma a világ?



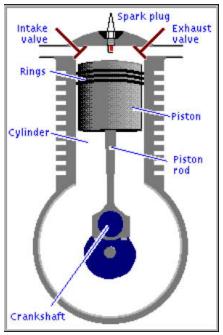
MOTIVÁCIÓK

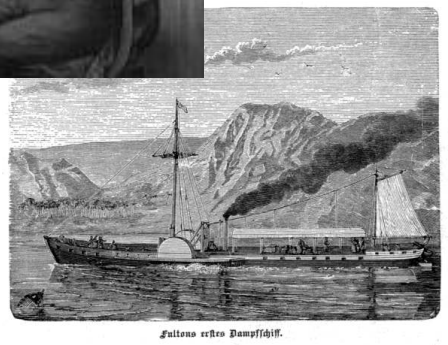
„A két lehetséges végeredmény: ha az eredmény megfelel a várakozásoknak, akkor mértél, ha nem, akkor felfedeztél valamit! “

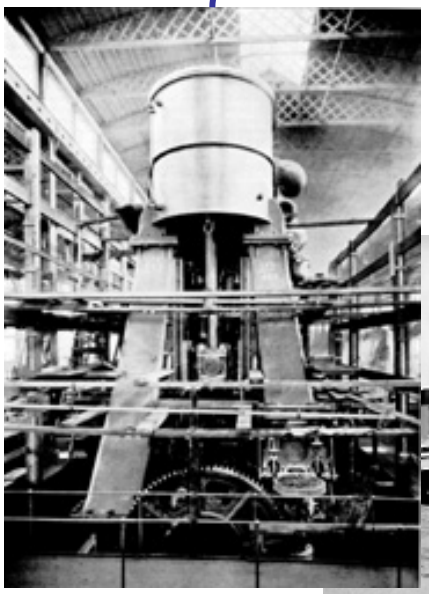
Enrico Fermi

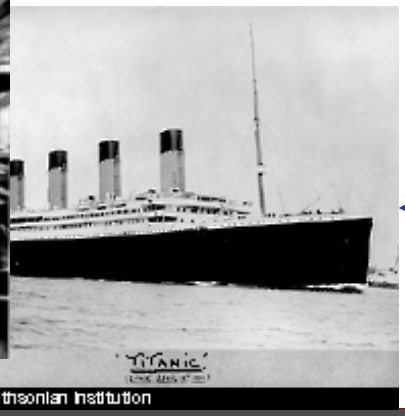


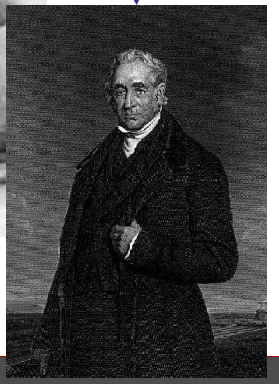
STOP


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

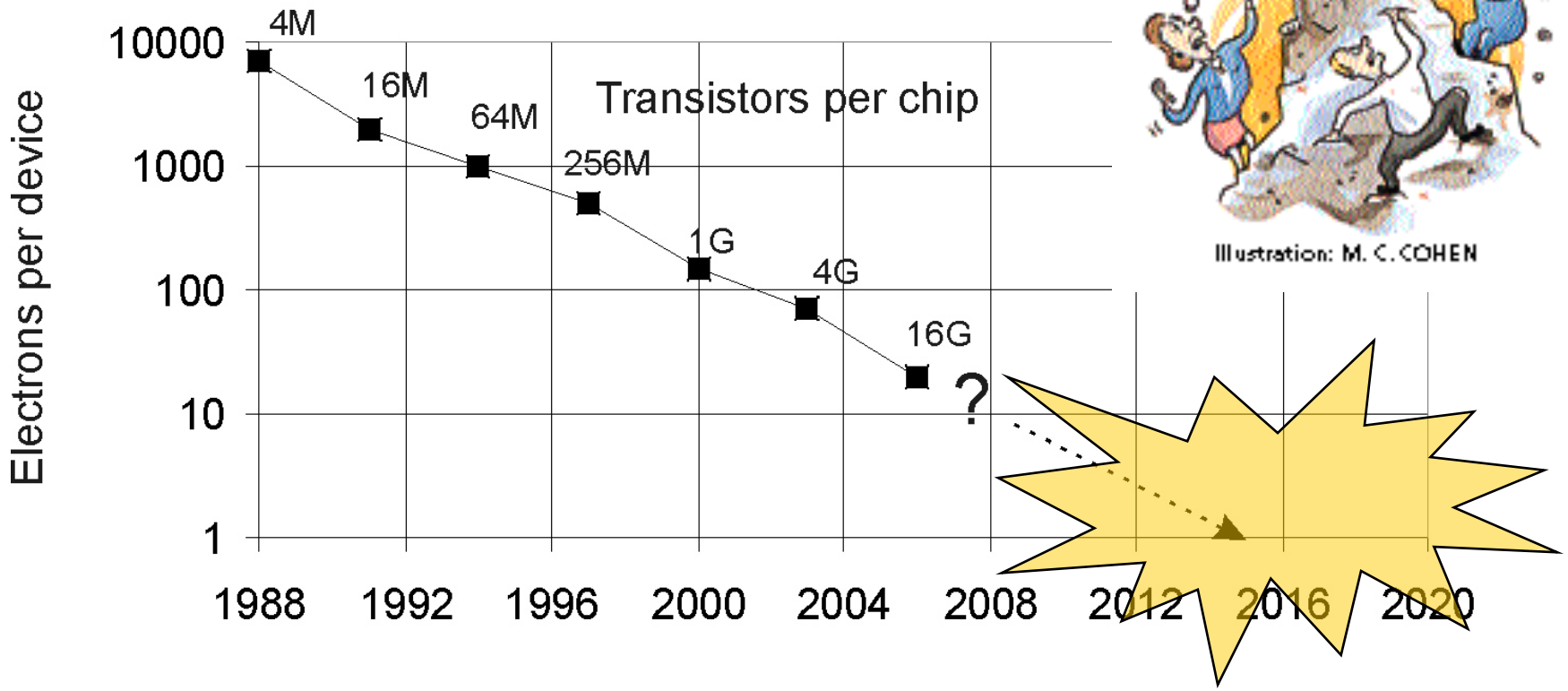

Fultons erstes Dampfschiff.




TITANIC
© 1995 Smithsonian Institution



MOORE TÖRVÉNYE



De meddig?

ÁLLJUNK MEG EGY PILLANATRA!

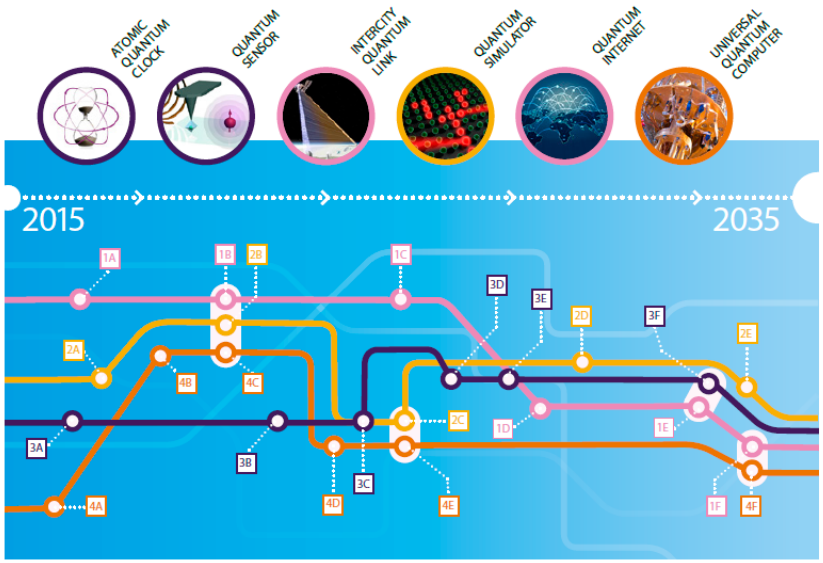
- Új játékszabályok
  - Korlátok és veszélyek
  - Lehetőségek

Quantum Manifesto

A New Era of Technology

May 2016

Quantum Technologies Timeline



1. Communication	2. Simulators	3. Sensors	4. Computers
0 – 5 years			
A Core technology of quantum repeaters	A Simulator of motion of electrons in materials	A Quantum sensors for niche applications (incl. gravity and magnetic sensors for health care, geosurvey and security)	A Operation of a logical qubit protected by error correction or topologically
B Secure point-to-point quantum links	B New algorithms for quantum simulators and networks	B More precise atomic clocks for synchronisation of future smart networks, incl. energy grids	B New algorithms for quantum computers
			C Small quantum processor executing technologically relevant algorithms
5 – 10 years			
C Quantum networks between distant cities	C Development and design of new complex materials	C Quantum sensors for larger volume applications including automotive, construction	D Solving chemistry and materials science problems with special purpose quantum computer > 100 physical qubit
D Quantum credit cards	D Versatile simulator of quantum magnetism and electricity	D Handheld quantum navigation devices	
> 10 years			
E Quantum repeaters with cryptography and eavesdropping detection	E Simulators of quantum dynamics and chemical reaction mechanisms to support drug design	E Gravity imaging devices based on gravity sensors	E Integration of quantum circuit and cryogenic classical control hardware
F Secure Europe-wide internet merging quantum and classical communication		F Integrate quantum sensors with consumer applications including mobile devices	F General purpose quantum computers exceed computational power of classical computers

Atomic quantum clocks can be synchronised with GPS to provide very high levels of timing stability and traceability, 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, broadcasting, 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 construction projects; for instance, to measure voids under the ground and to detect mineral deposits or legacy infrastructure. They will also be used to provide non-invasive point-of-care diagnosis.

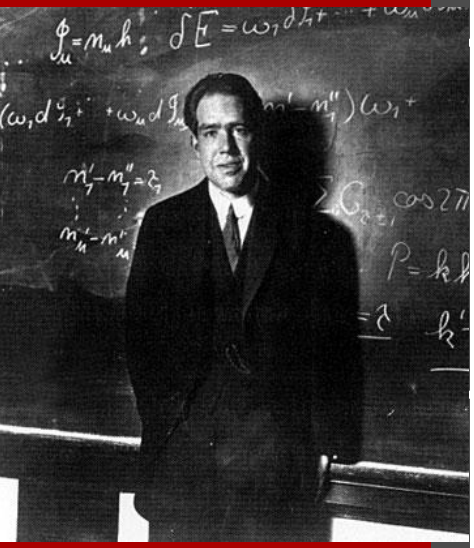
A secure **intercity quantum link** between a number of European capitals will allow transmission of highly sensitive data without any risk of interception. It may contain ground or satellite-based protected nodes derived from the development of trusted nodes and quantum repeaters.

Quantum simulators can be constructed 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 multiple sectors, such as energy or transport.

A global **quantum-safe communication network** – a quantum internet combining quantum with classical information and encryption – offers security for internet transactions against the threat of a quantum computer breaking purely 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 optimisation tasks, database searches, machine learning and image recognition. They will contribute to Europe's smart industry, helping to make European manufacturing industries more efficient.

- 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

A KVANTUM MECHANIKA POSZTULÁTUMAI MÉRNÖKI MEGKÖZELÍTÉSBEN

- 1. Posztulátum: kvantum bit
  - Hilbert-tér
- 2. Posztulátum: logikai kapuk
  - Unitér transzformáció
  - Elemi kvantum logikai kapuk
- 3. Posztulátum: Q/C átalakítás
  - Mérési statisztika
  - Mérés utáni állapot
- 4. Posztulátum: regiszterek
  - Tenzor szorzás

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

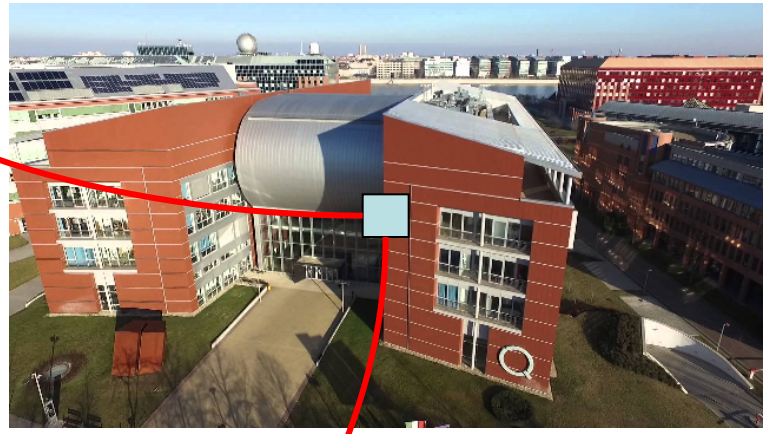
$$U^\dagger \equiv U^{-1}$$

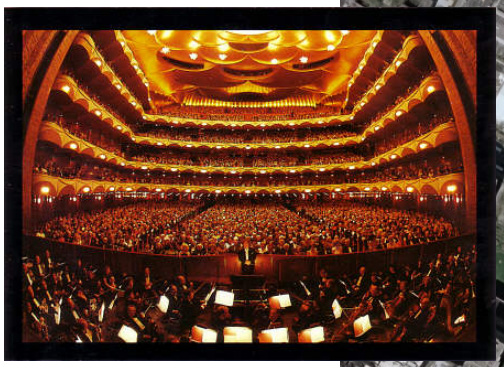
$$P(m \mid |\varphi\rangle) = \langle\varphi|M_m^\dagger M_m|\varphi\rangle$$

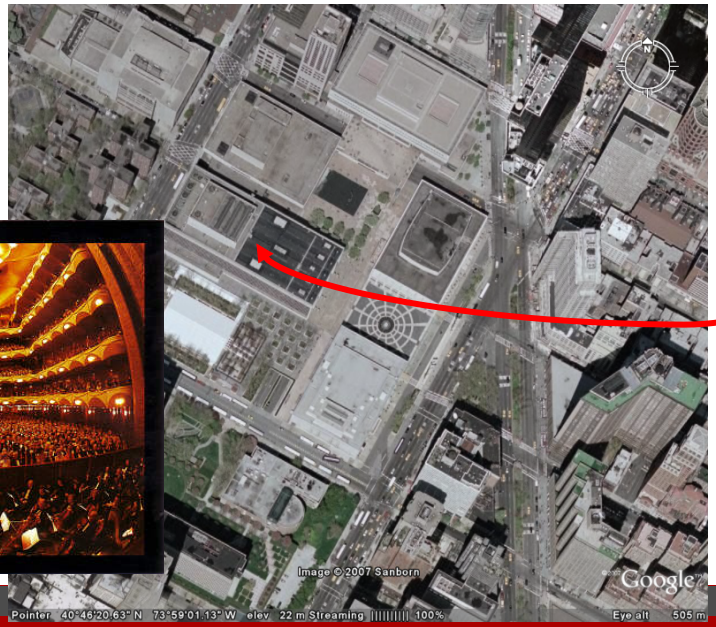
$$|\varphi'\rangle = \frac{M_m|\varphi\rangle}{\sqrt{\langle\varphi|M_m^\dagger M_m|\varphi\rangle}}$$

$$|\varphi\rangle = |0\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

ÖSSZEFONÓDÁS (ENTANGLEMENT)

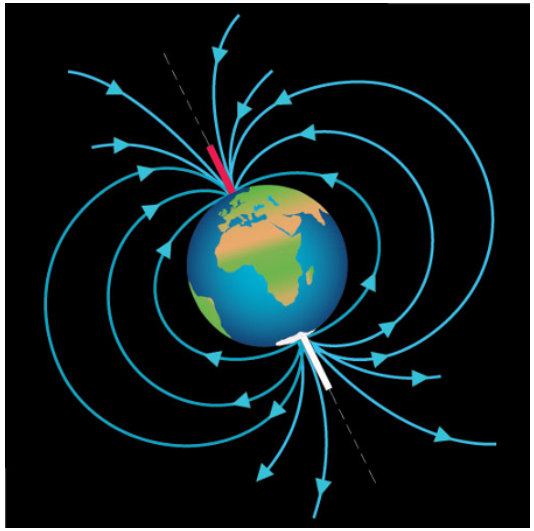






$$|\varphi\rangle = \varphi_0|00\rangle + \varphi_3|11\rangle$$

ERITHACUS RUBECULA – AZAZ VÖRÖSBEGY



https://youtu.be/VRIZA4cCI-U

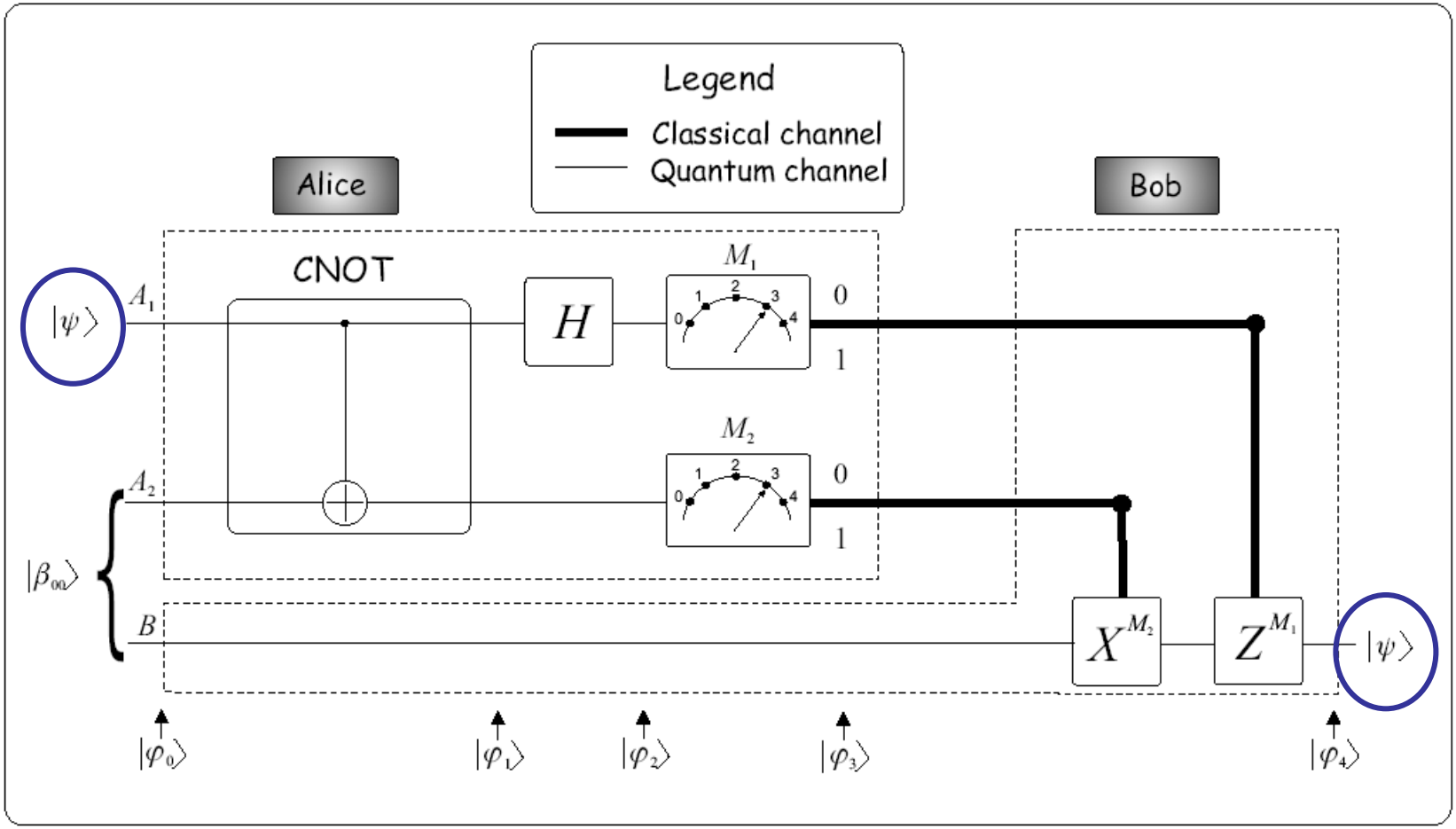
ALKALMAZÁSOK

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

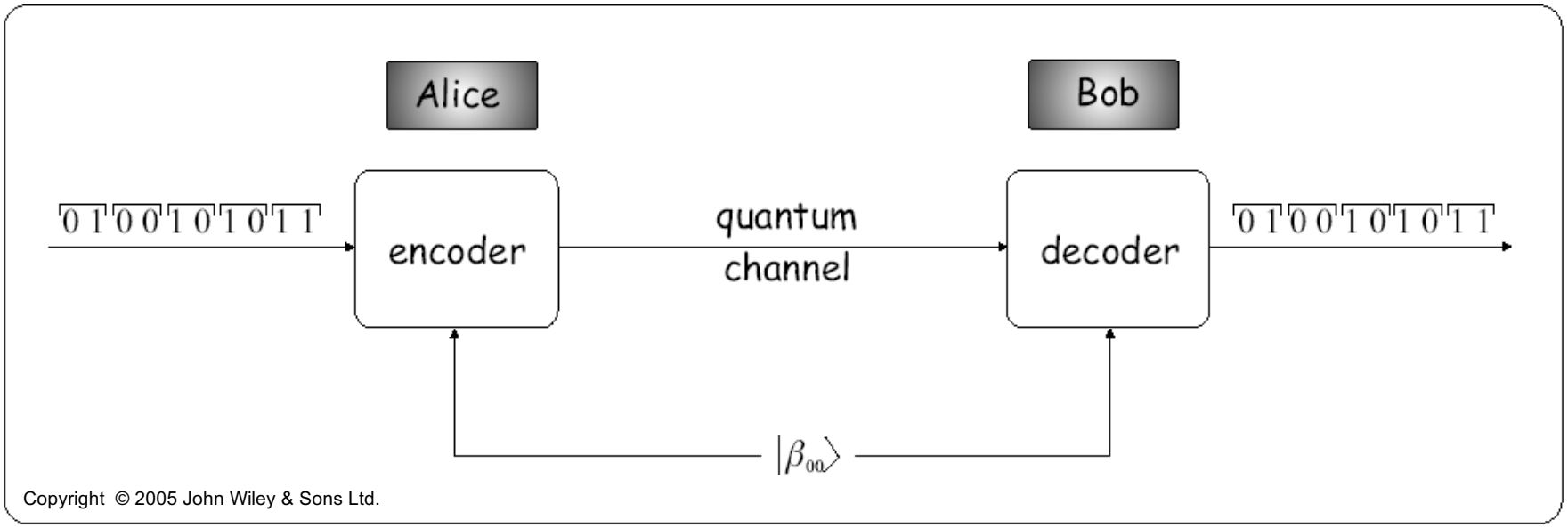
Max von Laue

TELEPORTÁLÁS

TELEPORTÁLÁS

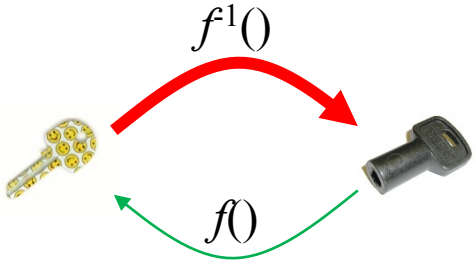


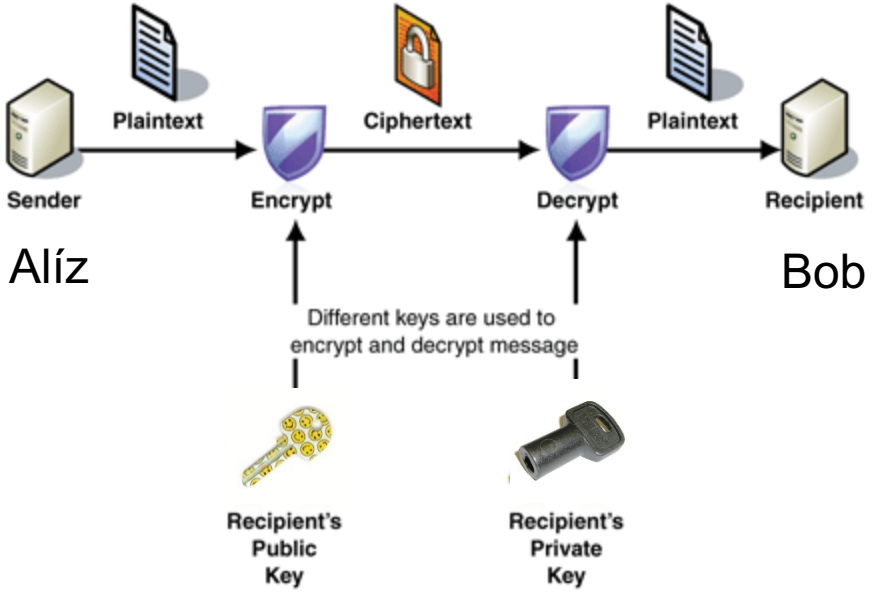
SUPERDENSE KÓDOLÁS



dibit	transform	joint state
00	I	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$
01	Z	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$
10	X	$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}}$
11	jY	$\frac{\|01\rangle-\|10\rangle}{\sqrt{2}}$

NYILVÁNOS 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!**

SHOR-ALGORITMUS

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	0.5		$4 \cdot 10^{134}$ year	80 bit
BC	$6 \cdot 10^{-4}$ s	$1.9 \cdot 10$		11.29 year	273 bit
G	$4 \cdot 10^{-3}$ s	$1.3 \cdot 10$		$3.7 \cdot 10^{57}$ year	159 bit
S	$2 \cdot 10^{-5}$ s	$6.6 \cdot 10$		$3.4 \cdot 10^{-11}$ year	**10000** bit

Peter Shor (1959-)

- 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!

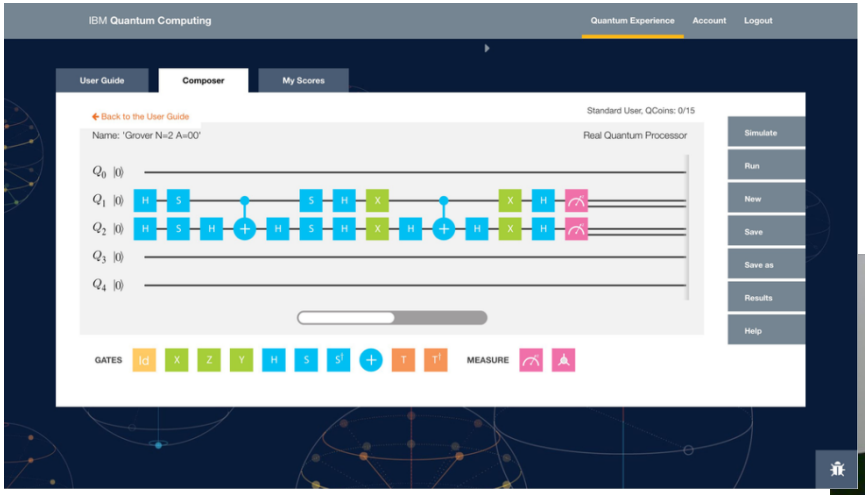
Arnold Schwarzenegger (1947-)

D-WAVE

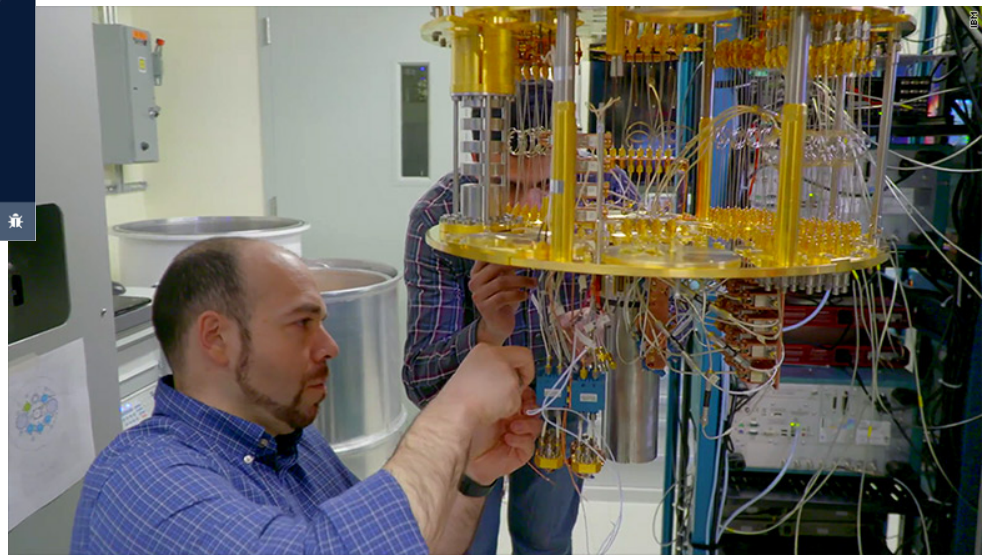
- 2017 jan: D-Wave2000Q

D:wave
The Quantum Computing Company™

IBM KVANTUM SZÁMÍTÓGÉP



2016: 5 qubit



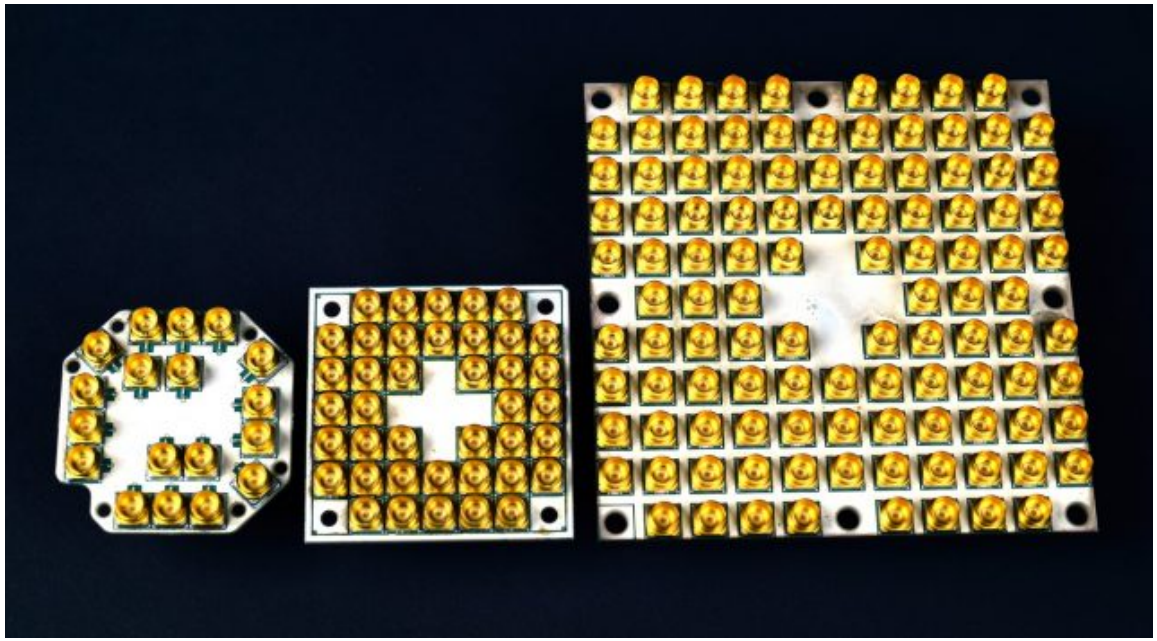
2017: 16 qubit

IBM Q Awards:

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

News 2018 !!!

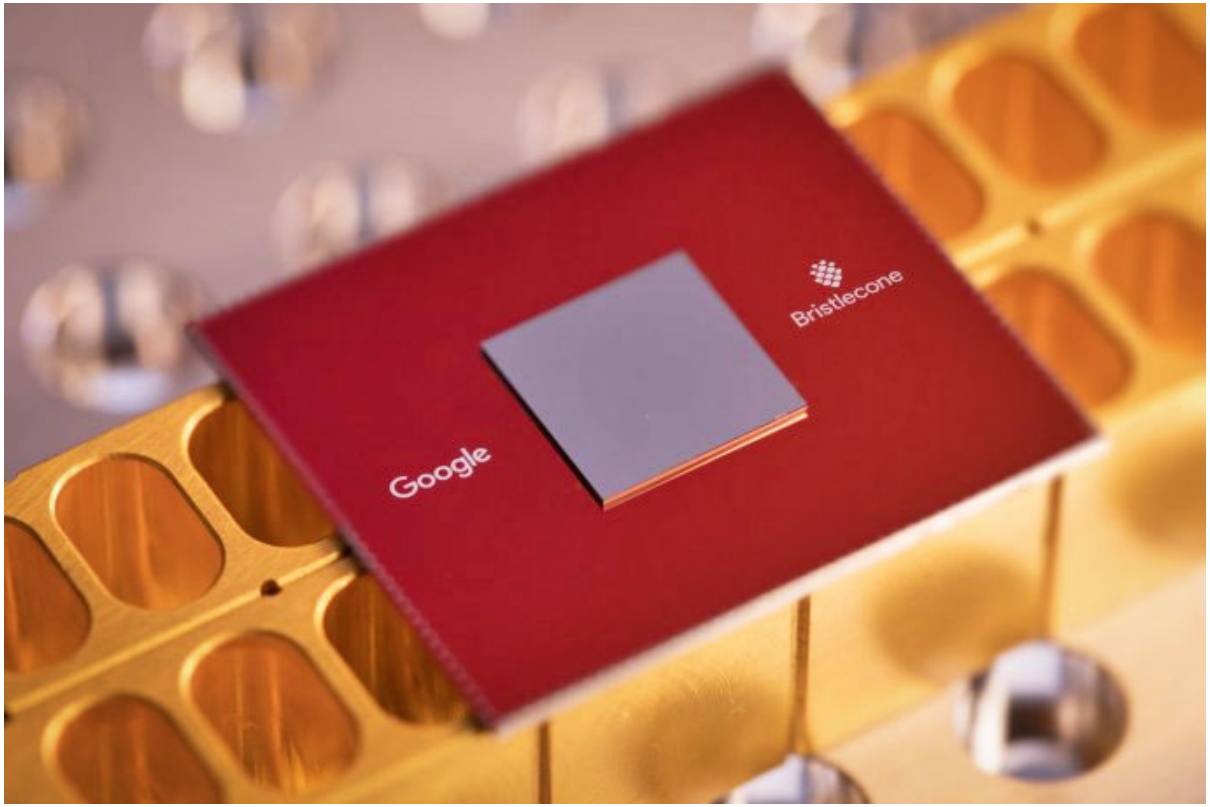
INTEL KVANTUM PROCESSZOROK



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



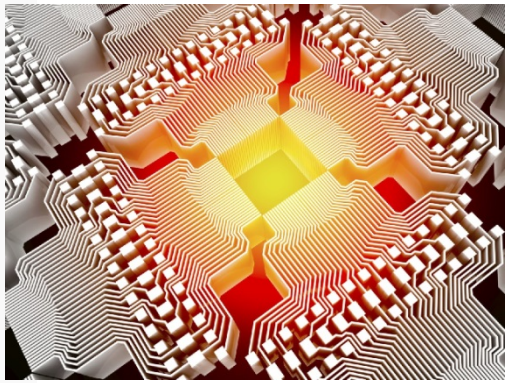
https://index.hu/tech/2018/03/07/a_google_ettol_a_csiptol_varja_a_kvantumszamitogepes_attorest/

- A legnagyobb kihívás az ÖSSZEFONÓDÁS!

MICROSOFT KVANTUM FEJLESZTŐ RENDSZER

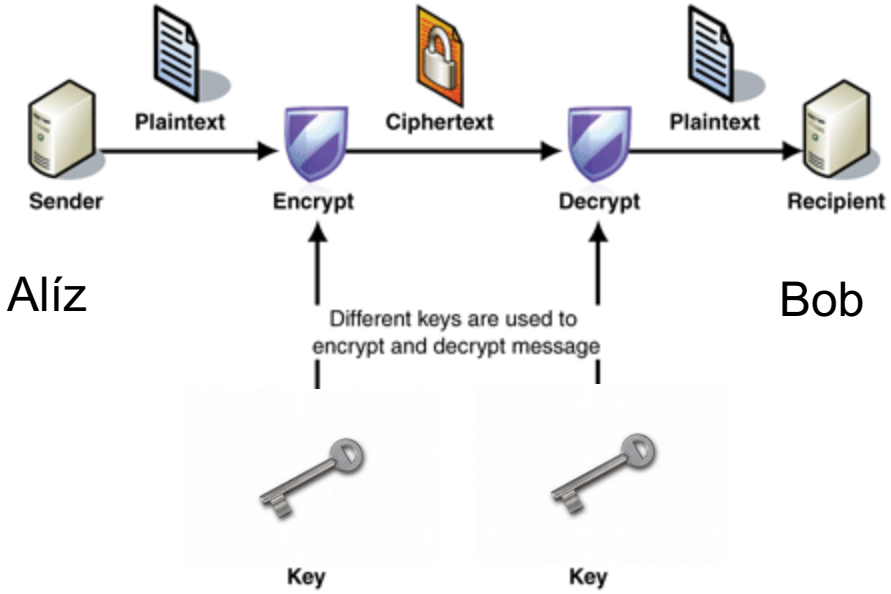
- Kvantum programozási nyelv: Q#

```
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);
    }
}
```



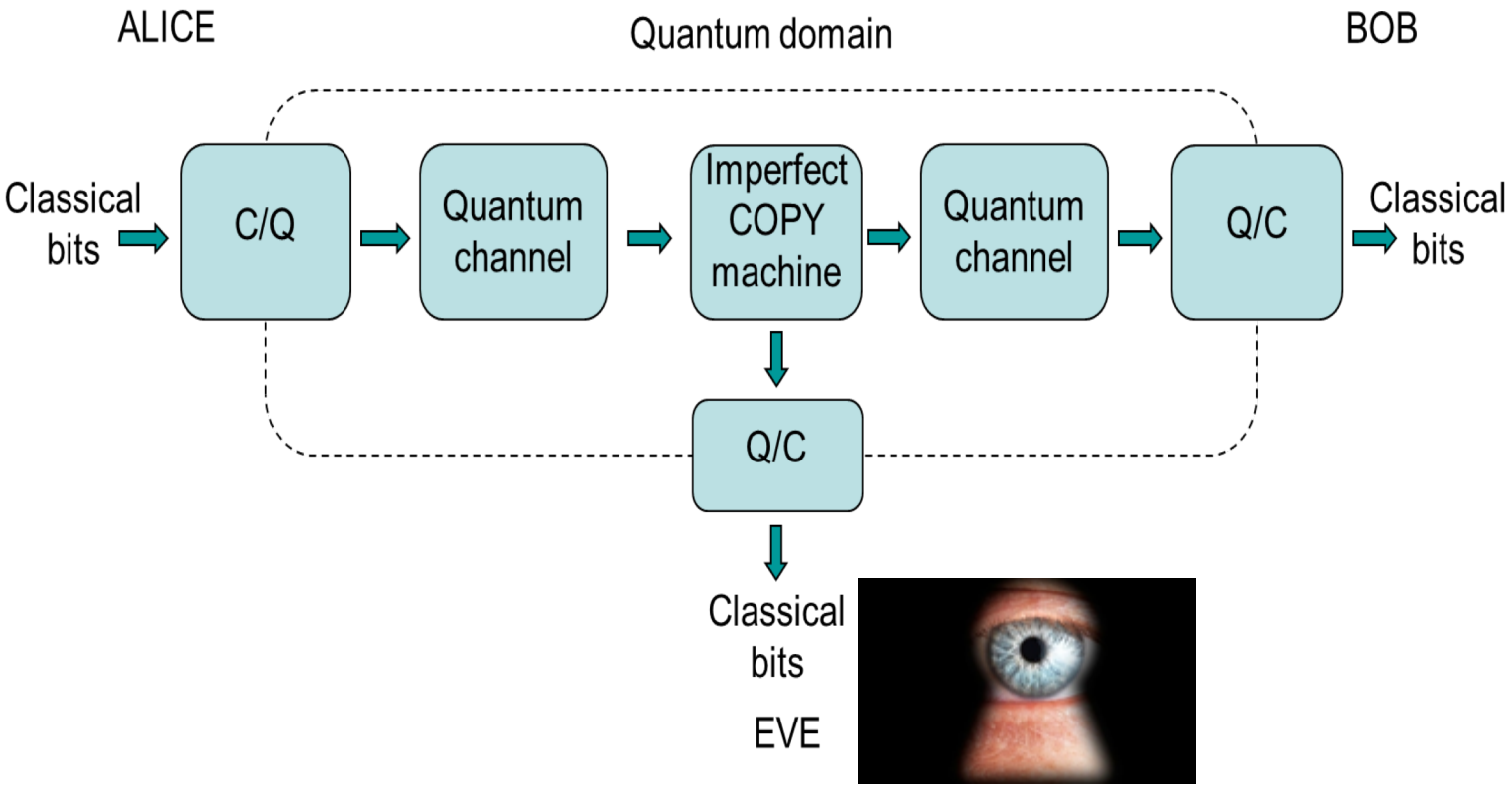
News 2018 !!!

SZIMMETRIKUS TITKOSÍTÁS

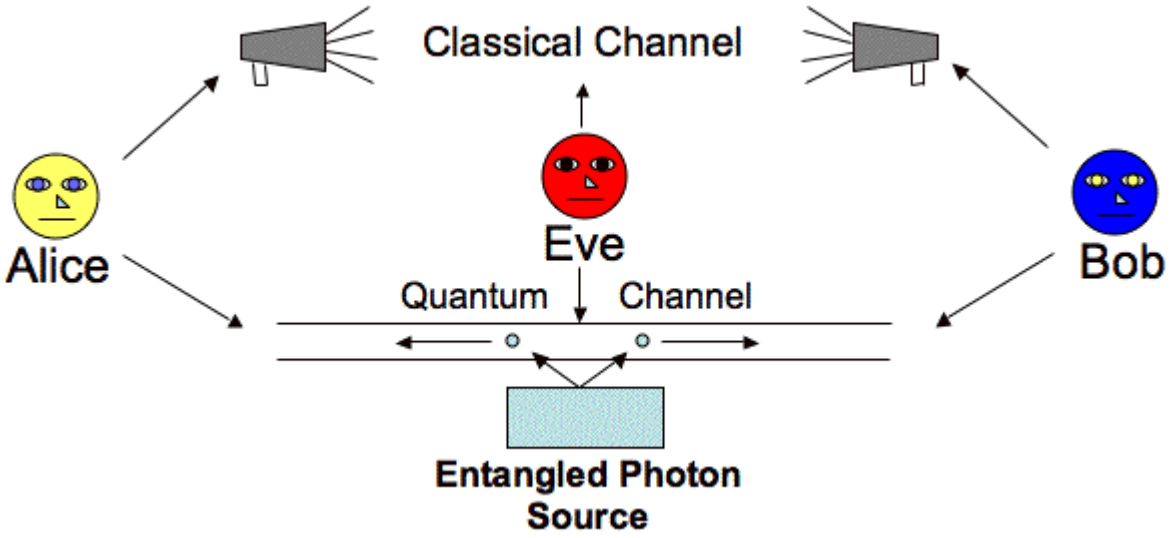


- Szimmetrikus kulcsú titkosítás
  - Egyforma kulcsok mindkét oldalon
- Abszolút biztonságos, ha bizonyos előírásokat betartunk
- Gond, hogy a kulcsot miként juttassuk el a túloldalra????

KVANTUM KULCSSZÉTOSZTÁS (QKD)



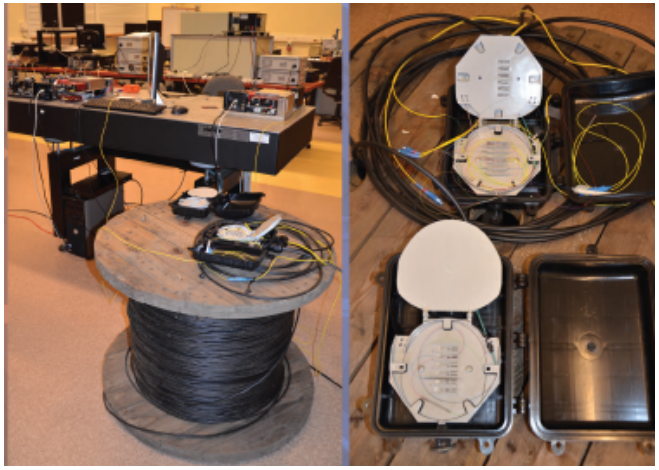
ÖSSZEFONÓDÁS ALAPÚ



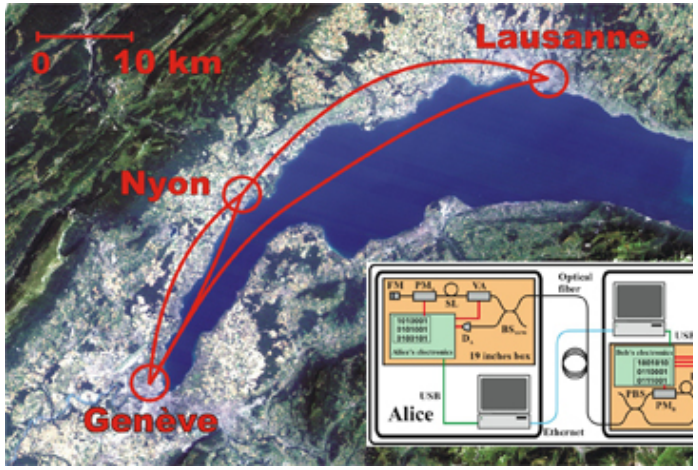
$$|w_2\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

- Probléma: $|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

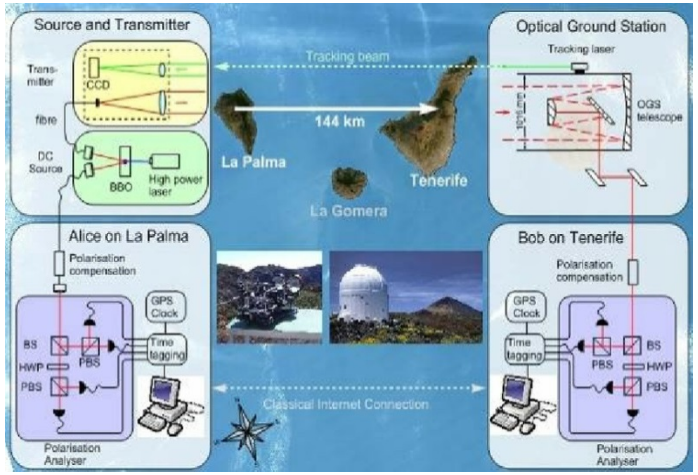
A KULCSSZÉTOSZTÁS TÖRTÉNETE



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

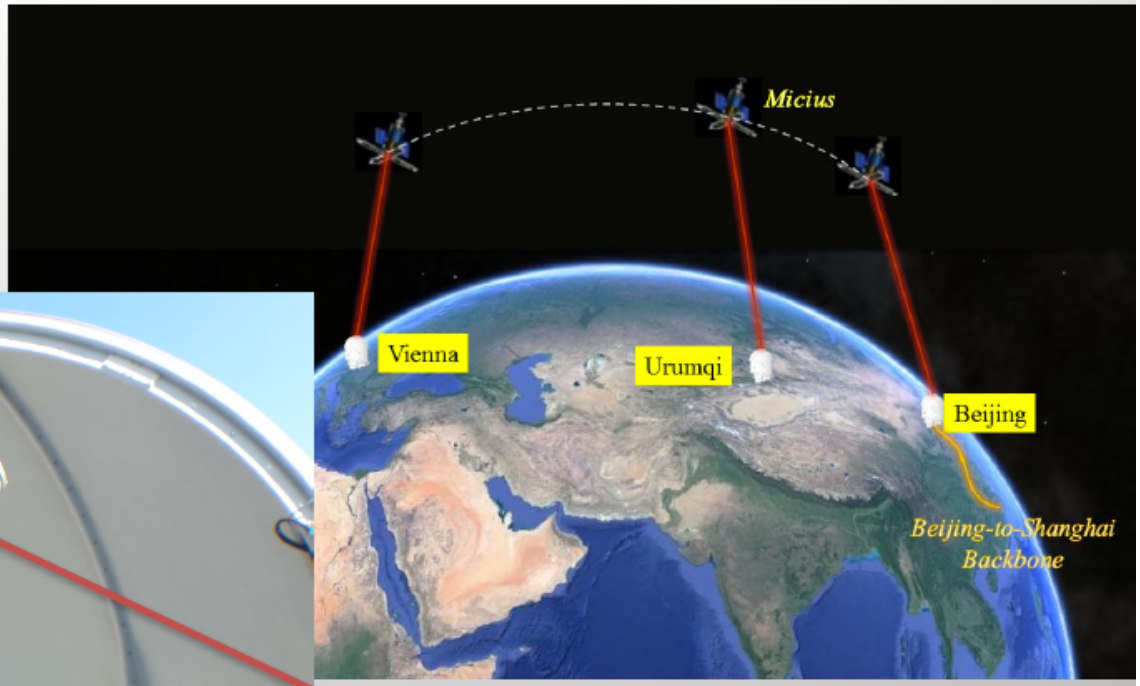


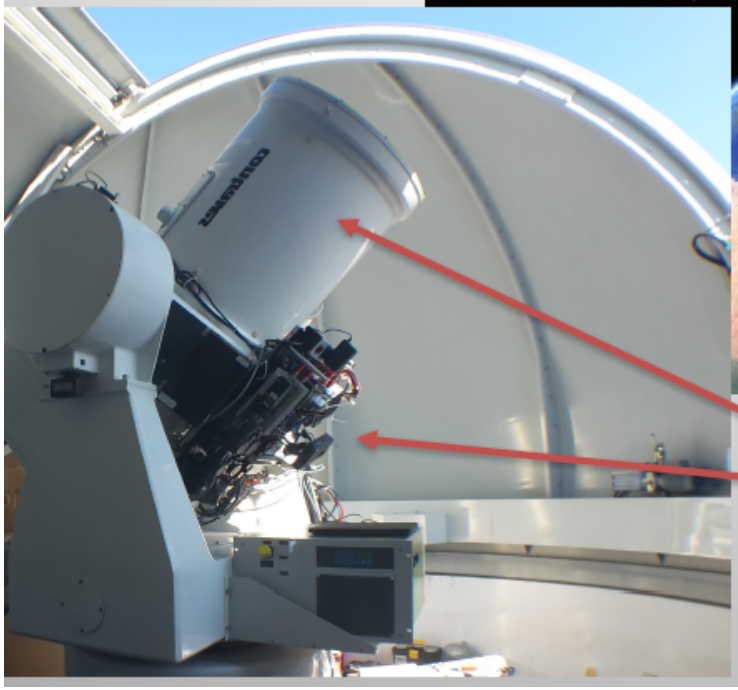
Szabad légkör	
1996	75 m
1998	1 km
2001	2 km
2002	10 km
2007	144 km



QUESS 2017 (QUANTUM EXPERIMENTS AT SPACE SCALE)

Micius
600 km Polar
Sun synchronouse
Graz (soon Tenerife)



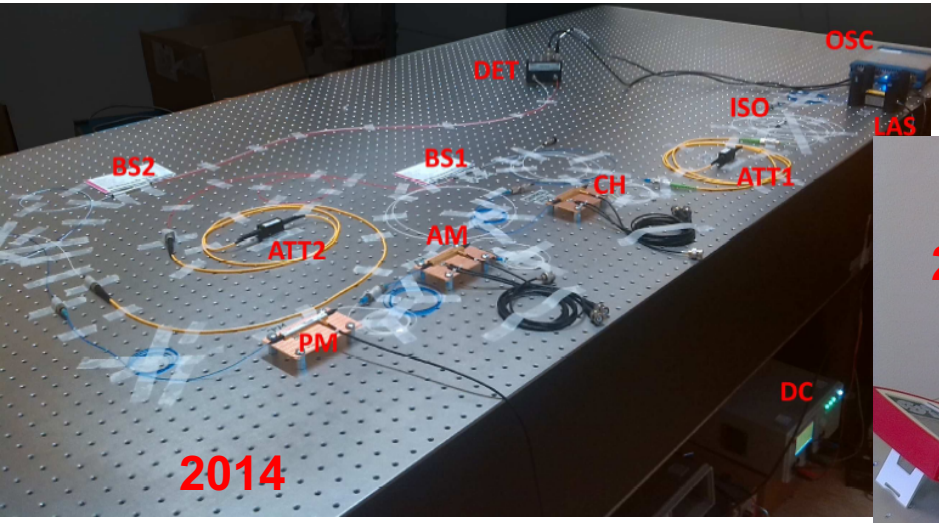


ÖAW OGS Graz (Mnt. Lustbühel)
Telescope 60 cm diameter
Quantum hardware (4 Det. Scheme)

26

Rupert.Ursin@oeaw.ac.at

AHOGY MI KULCSSZÉTOSZTUNK



MÁR BOLTBAN IS KAPHATÓ!

id Quantique
A Quantum Leap for Cryptography

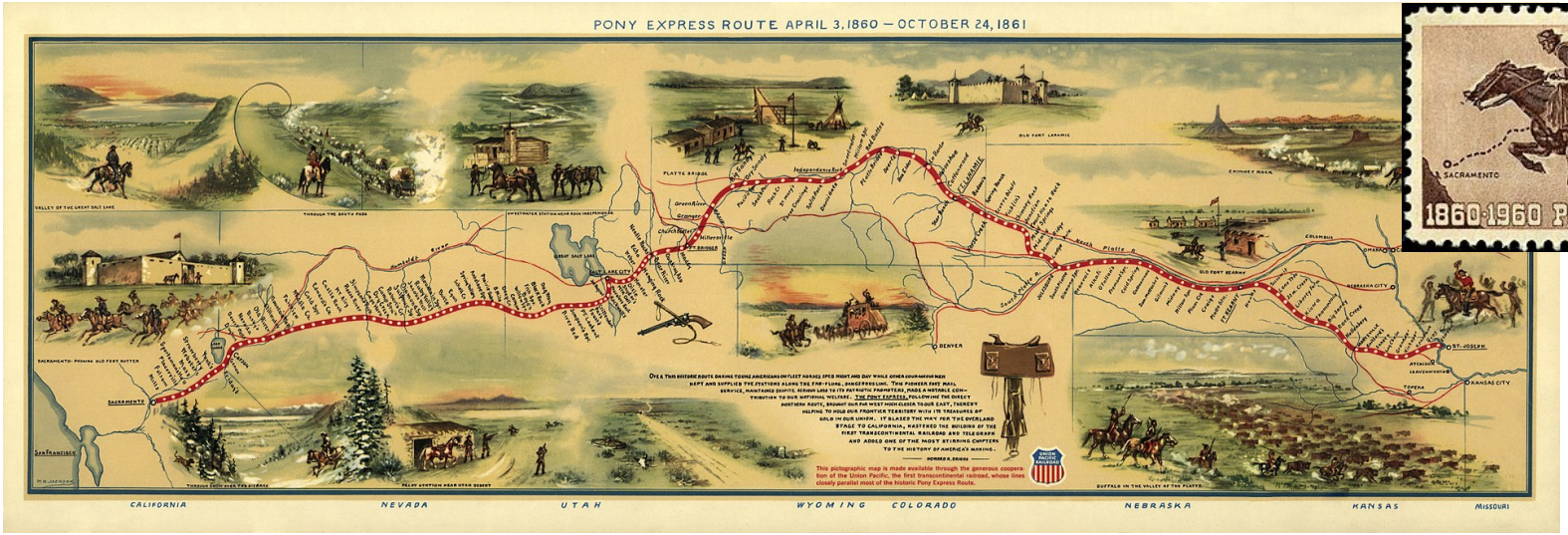
MagiQ Technologies

quintessence labs

KIHÍVÁSOK

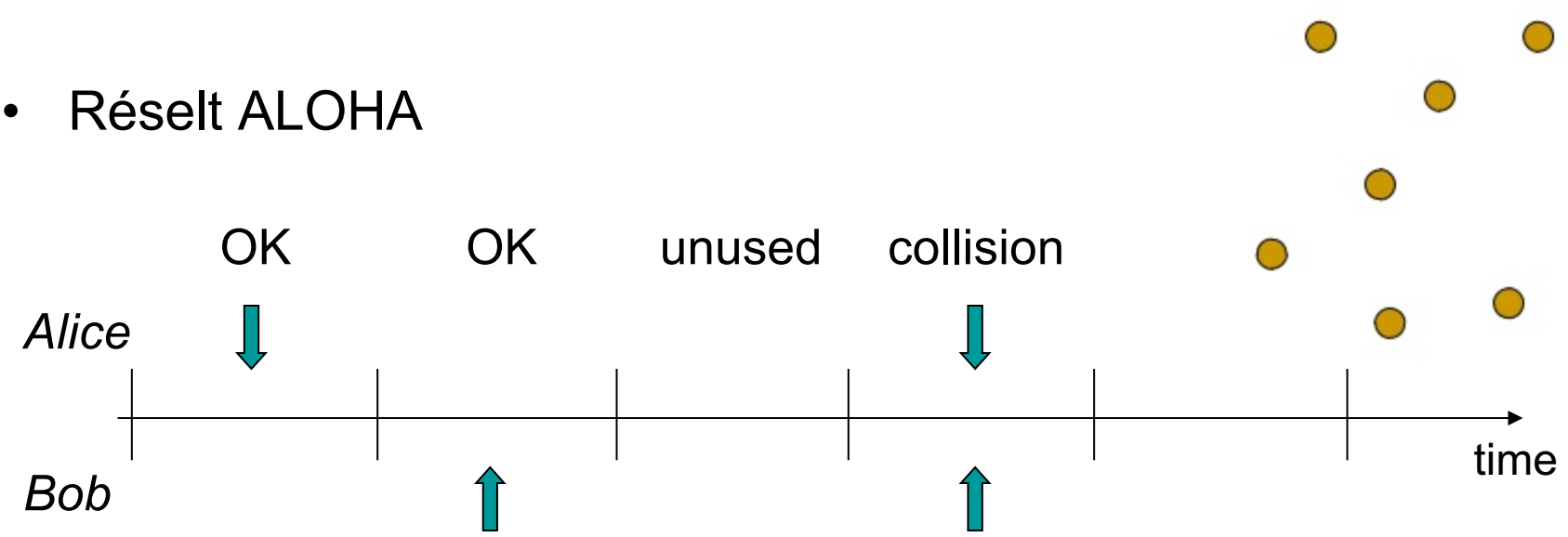
- Csak pont-pont összeköttetések működnek, véges távolságra.
- A jelenleg használt távközlési optikai szálak is alkalmasak.

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



KÖZEGHOZZÁFÉRÉS ELOSZTOTT KÖRNYEZETBEN

- Réselt ALOHA



$$p_i = \frac{1}{M}$$

$$\lim_{M\to\infty} \max_{p_i} \mathrm{E}(s) = \lim_{M\to\infty} \left(1-\frac{1}{M}\right)^{M-1} = \lim_{M\to\infty} \frac{1}{1-\frac{1}{M}} \left(1-\frac{1}{M}\right)^{M} = \frac{1}{e}$$

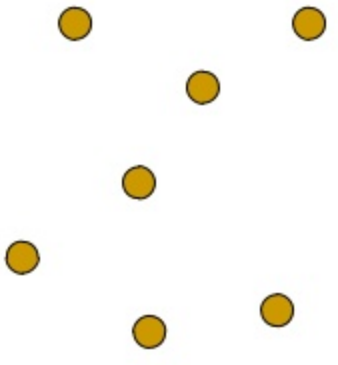
KVANTUM MAC

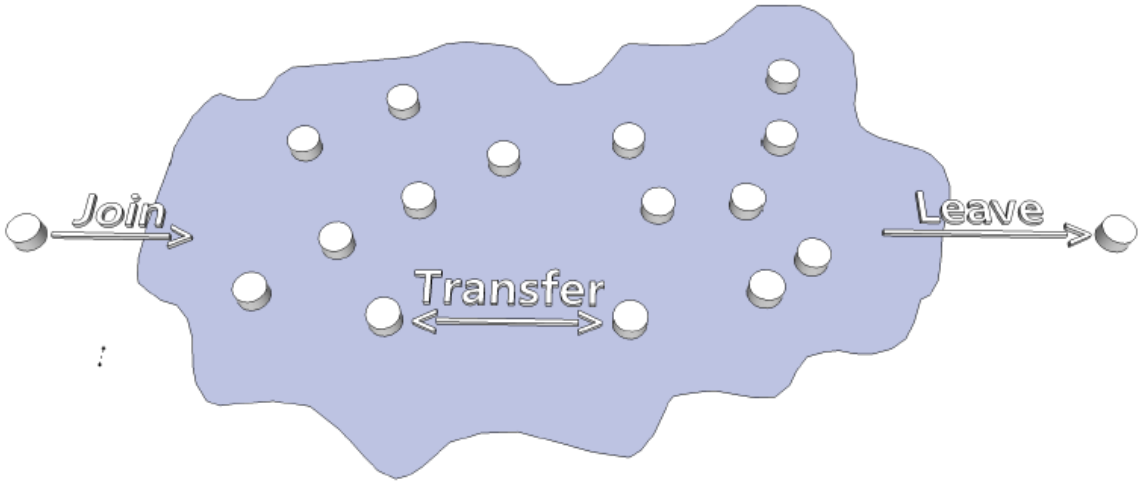
- W-állapotok

$$|w_2\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|w_3\rangle = \alpha\,|001\rangle + \beta\,|010\rangle + \gamma\,|100\rangle$$

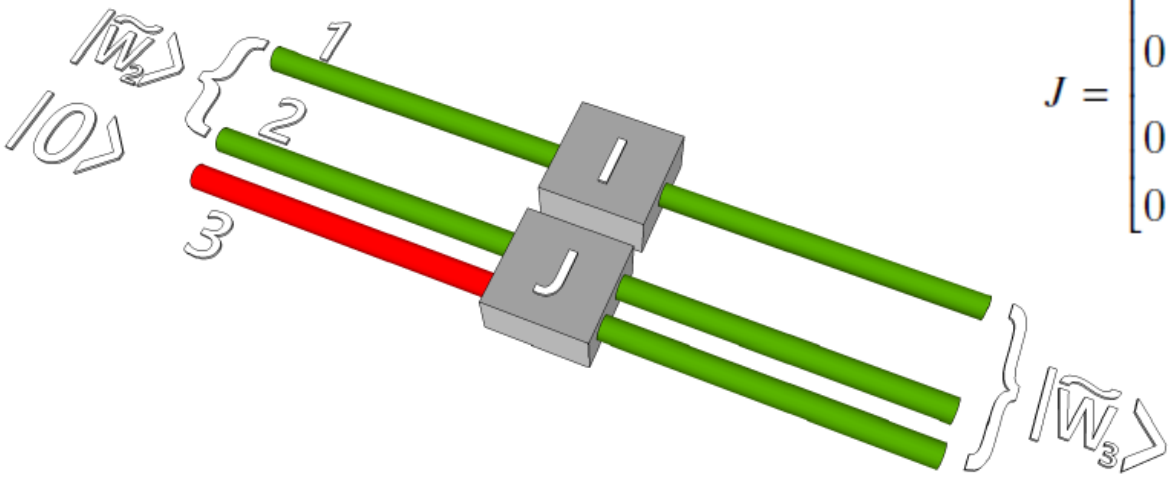
$$|w_n\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |2^{(n-i)}\rangle$$





QUANTUM MAC - JOIN

- W-állapotok lépésről-lépésre generálhatók elosztott környezetben is.
- Join, Leave és valószínűség Exchange operátorok



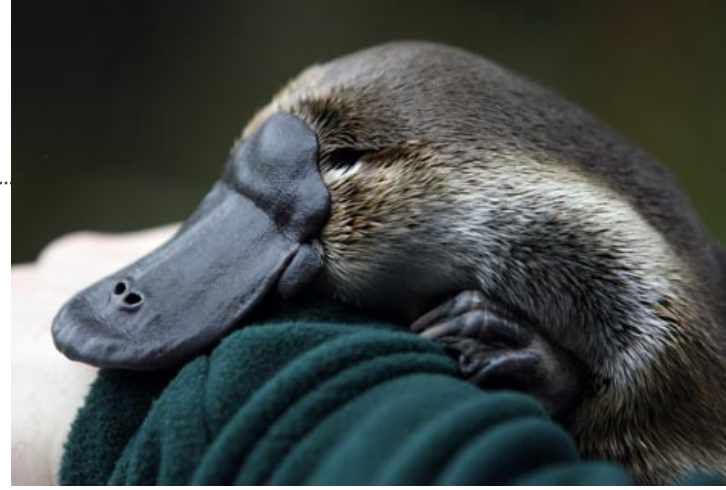
$$J = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -\sqrt{\frac{R_J}{R_J+1}} & \sqrt{\frac{1}{R_J+1}} & 0 \\ 0 & \sqrt{\frac{1}{R_J+1}} & \sqrt{\frac{R_J}{R_J+1}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$R_J = \frac{p_{3,2}}{p_{3,3}}$$

Figure 2: New node joins the system: node1 and node2 have already formed a medium access system; node3 connects to node2 and performing the JOIN operation node3 becomes part of the system.

- Csak a birtokolt valószínűséget lehet megosztani!

ÉRDEKESSÉG

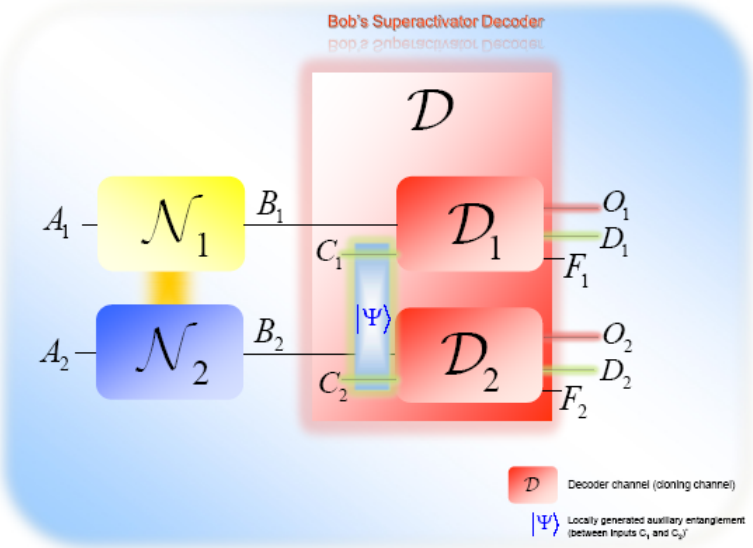


- A klasszikus csatornák additívak

$$C_{ALL}(\mathcal{N}_1 \otimes \mathcal{N}_2) = C_{ALL}(\mathcal{N}_1) + C_{ALL}(\mathcal{N}_2)$$

- De ha összefonódott állapotokba kódolva küldjük a szimbólumokat a kvantum csatornába, akkor

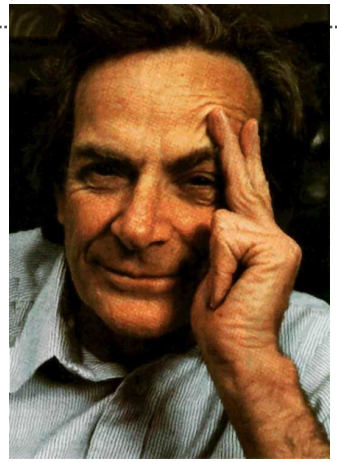
$$C_{ALL}(\mathcal{N}_1 \otimes \mathcal{N}_2) > C_{ALL}(\mathcal{N}_1) + C_{ALL}(\mathcal{N}_2)$$



TANULSÁGOK

- Az összefonódás olyan, mint a kőbalta, „áldás” és „átok” is egyben.
- Megkerülni nem lehet, ahogy leárnyékolni sem.
- Okosan kezelve viszont rendkívüli „erőforrást” jelent.

- 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)

KÉRDÉSEK/MEGJEGYZÉSEK