



HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

A kvantumkommunikáció jelene és jövője

A HTE Vételtechnikai és a Kábeltelevíziós Szakosztály, a Médiaklub és a Rádiótávközlési Szakosztály közös rendezvénye

2022. február 23.

Bacsárdi László

BME Hálózati Rendszerek és Szolgáltatások Tanszék

bacsardi@hit.bme.hu



TERÜLETEINK A BME HIT MOBIL KOMMUNIKÁCIÓ ÉS KVANTUMTECHNOLÓGIÁK LABORATÓRIUMBAN



Mobilhálózatok

Internet-of-Things

5G

Kvantumkommunikáció

A kvantuminformatika és kvantumkommunikáció számos megoldást kínál a legkülönbözőbb területeken

- kvantumszámítógépek
- kvantumkriptográfia
- kvantum alapú véletlenszámok
- kvantum alapú kulcsszétosztás



Egyik fő kérdéskör: a kvantumkommunikációs megoldások hogyan alkalmazhatóak mérnöki (pl. távközlési) rendszerekben a jelenlegi biztonsági szint növelése érdekében

Számos kutatási projektben veszünk részt, emellett több, kvantuminformatikához és kvantumkommunikációhoz kötődő tárgyat oktatunk

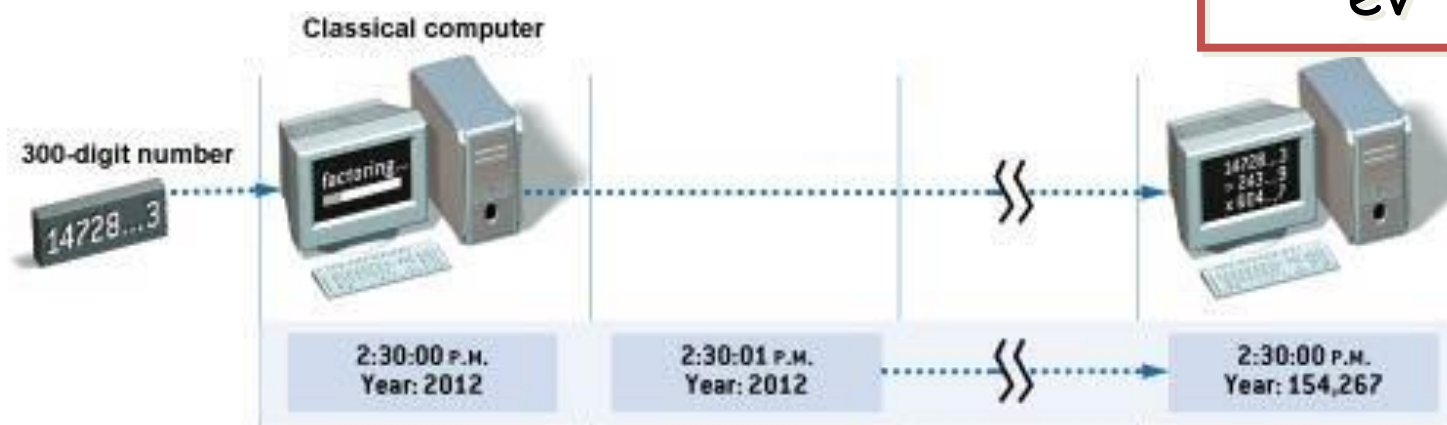
The future is Quantum.

The Second Quantum Revolution is unfolding now, exploiting the enormous advancements in our ability to detect and manipulate single quantum objects. The Quantum Flagship is driving this revolution in Europe.

[LEARN MORE](#)

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

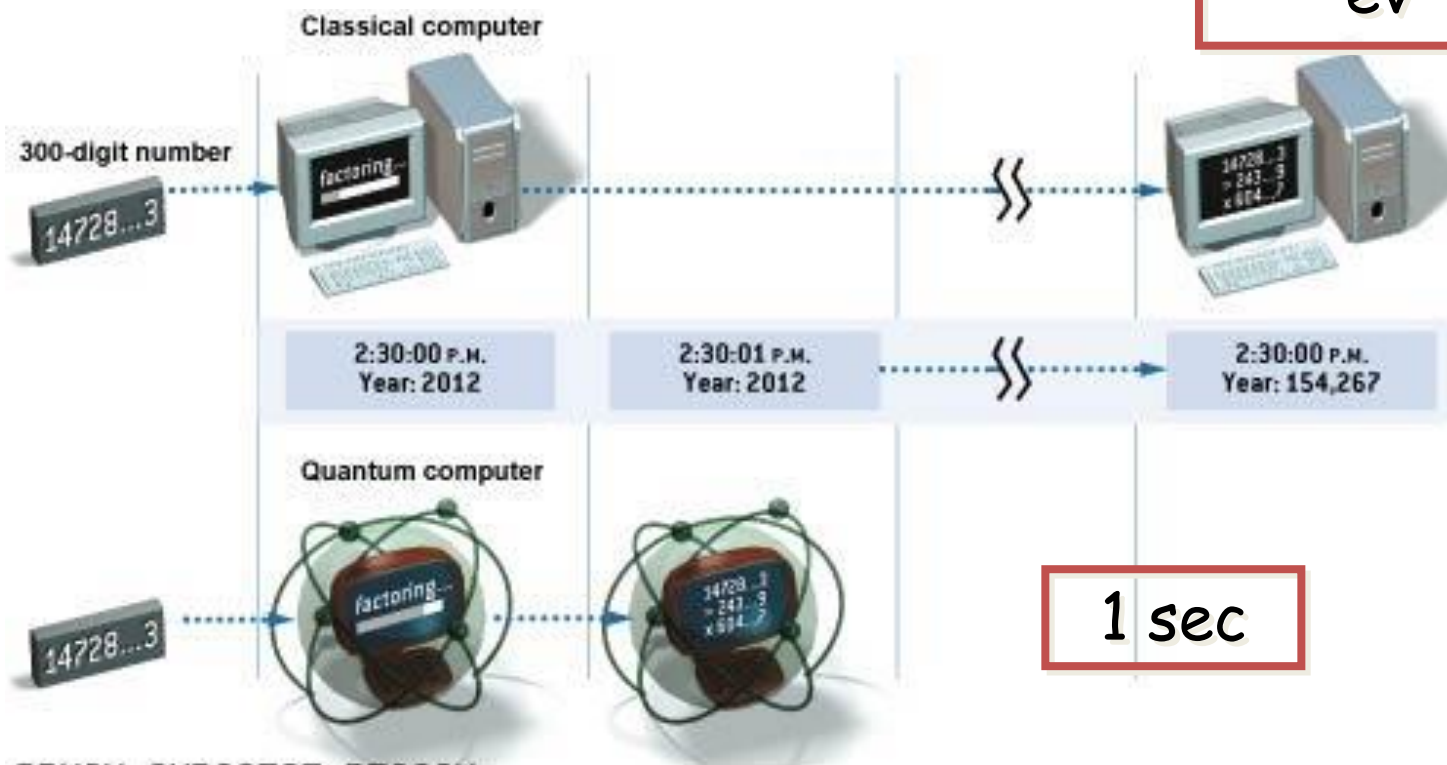
152 000
év



SHOR-ALGORITMUS ÉS AZ RSA TÖRÉSE

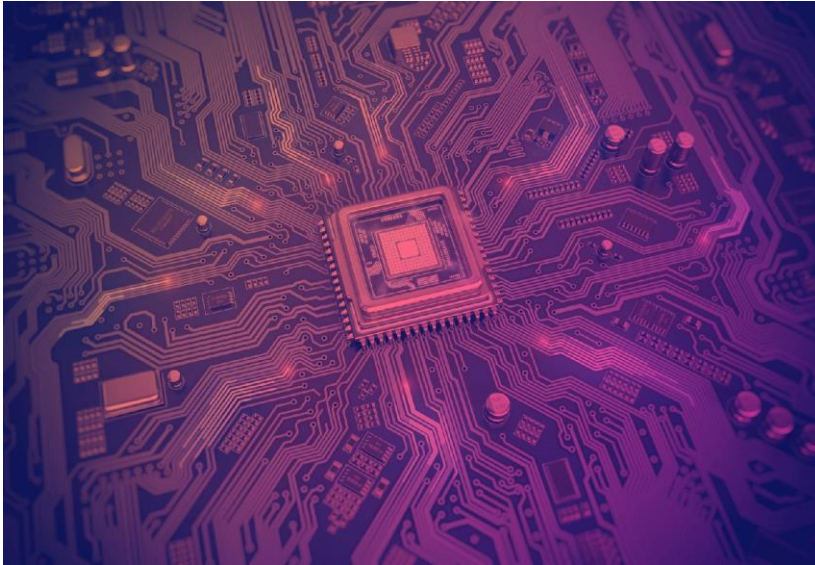
$$O(\log^3(N))$$

152 000
év



BRYAN CHRISTIE DESIGN

MI AZ A KVANTUM?



Egy rendszerre akkor aggasztjuk rá a „kvantum” jelzõt, ha a kvantummechanika törvényei szerint mûködik.

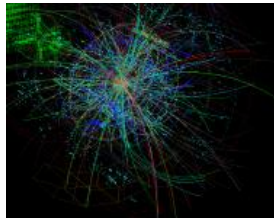
A kvantum alapú rendszereknek speciális jellegzetességei:

- kvantáltság
- hullám-részecske kettõség
- alagúteffektus
- szuperpozíció
- kvantum interferencia
- ...

A kvantum alapú jelenségek alapvetõen a nanométer tartományban jelennek meg

de

a kvantummechanika törvénye jelentik az alapjait sok makroszkopikus rendszernek is.



Ütközések a CERN-ben



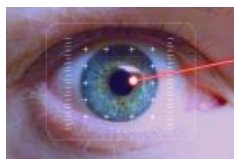
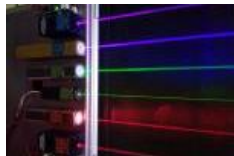
Fotoszintézis



Napelemek



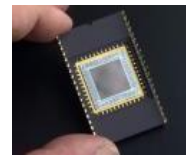
Nukleáris erőművek



Lézerek



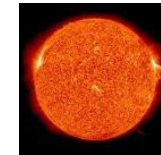
Integrált
áramkörök



CCDk



LEDek



Nukleáris
fúzió

We never experiment with just one electron or atom or (small) molecule. In thought-experiments we sometimes assume that we do; this invariably entails ridiculous consequences... we are not experimenting with single particles, any more than we can raise Ichthyosauria in the zoo"

Erwin Schrödinger [Brit. J. Phil. Sci. 3, 233 (1952)].

Már nem igaz!

0 vagy 1

0 és 1



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

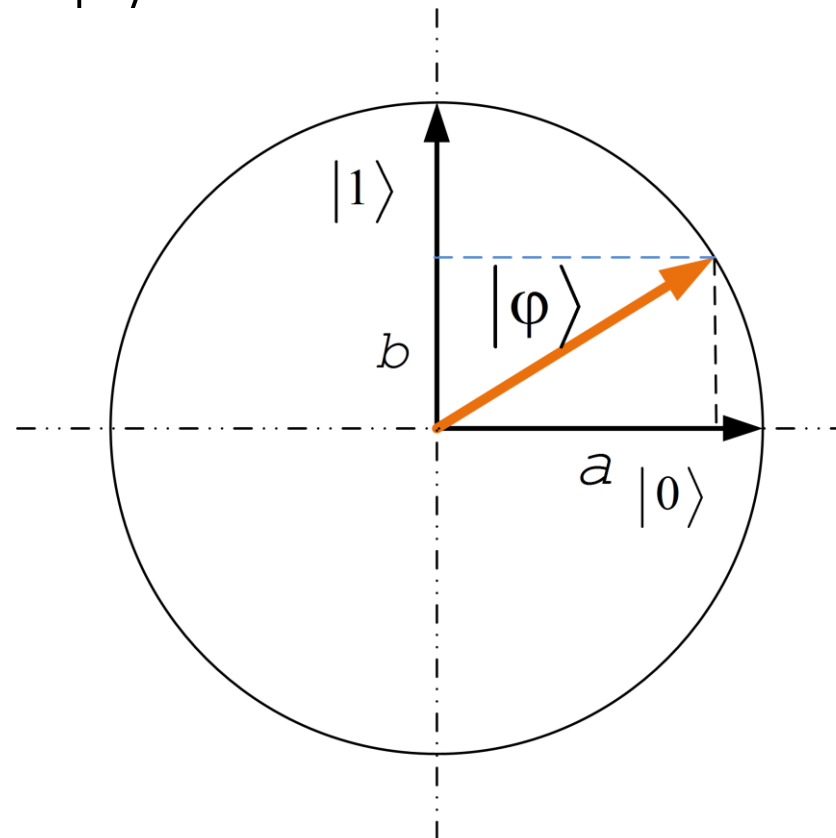
$$a, b \in \mathbb{C} \quad |a|^2 + |b|^2 = 1.$$

Komplex valószínűségi amplitúdók

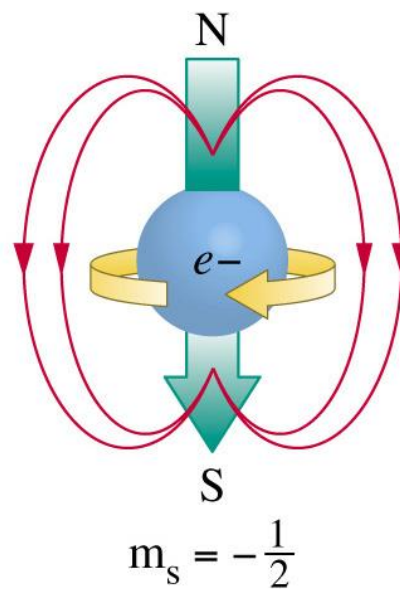
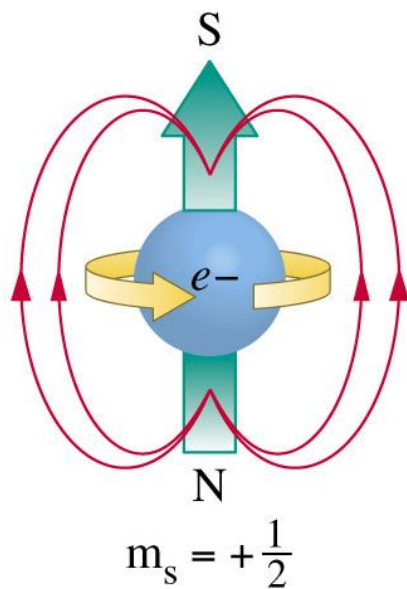
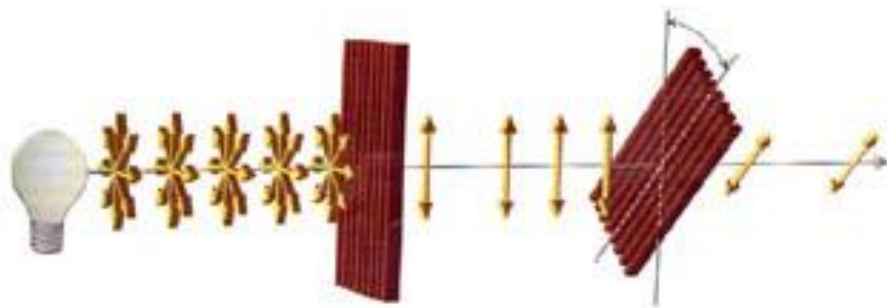
$$|\varphi\rangle = a|0\rangle + b|1\rangle$$

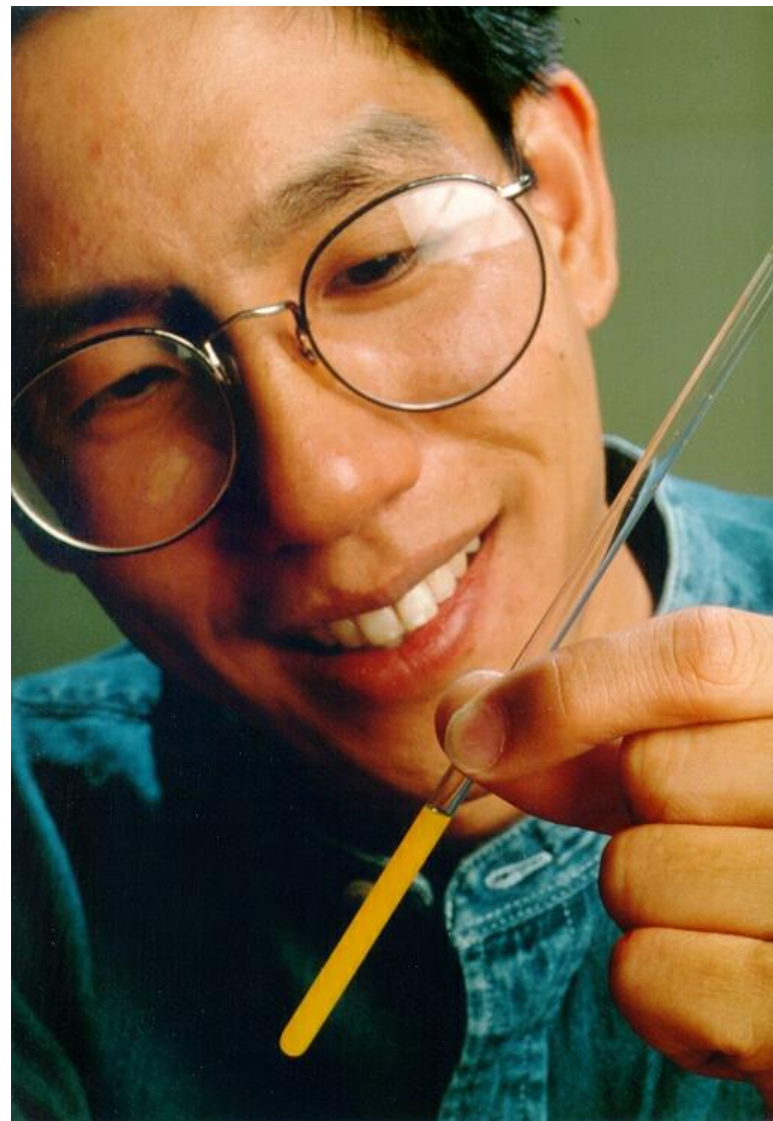
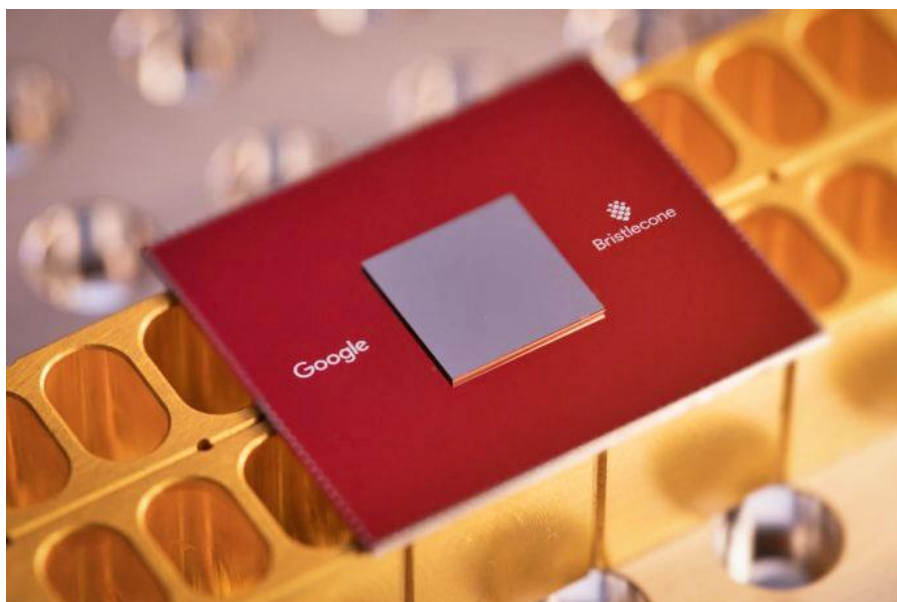
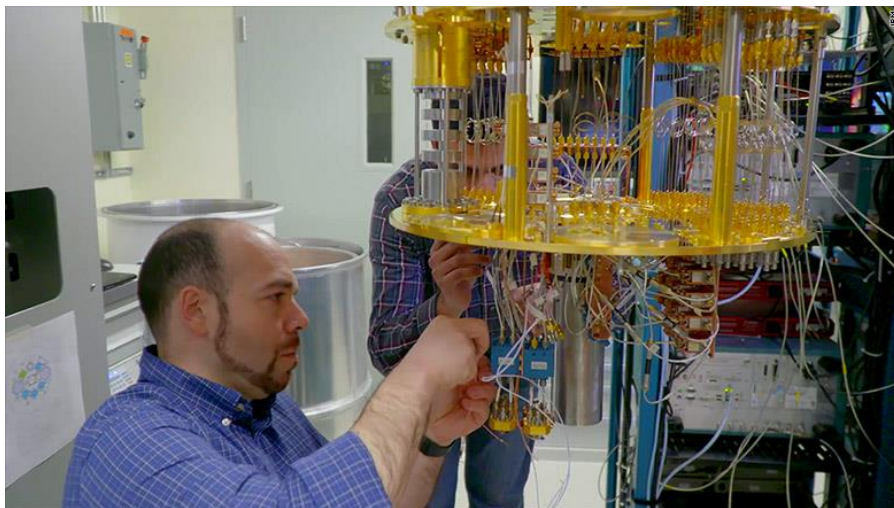
$$|a|^2 + |b|^2 = 1.$$

$$a, b \in \mathbb{C}$$




KVANTUMBITEK A GYAKORLATBAN



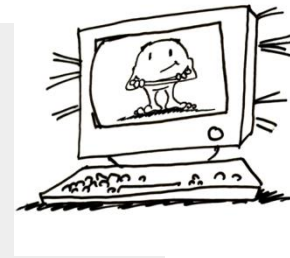


A Desktop Quantum Computer for Just \$5,000

A cheap, portable quantum computer, aimed at schools and colleges will be launched later this year.

 The Physics arXiv Blog | By The Physics arXiv Blog | January 29, 2021 3:00 PM





Size Matters: Advantage's 5000+ qubit and 15-way qubit connectivity powers large-scale, in-production hybrid quantum applications

BURNABY, BC – September 29, 2020 — D-Wave Systems Inc., the leader in quantum computing systems, software, and services, today announced the general availability of its next-generation quantum computing platform, incorporating new hardware, software, and tools to enable and accelerate the delivery of in-production quantum computing applications. Available today in the Leap™



Real quantum computers. Right at your fingertips.

IBM offers cloud access to the most advanced quantum computers available. Learn, develop, and run programs with our quantum applications and systems.

Temalabor tajekoztato Visualizations seed 2291

H \oplus \oplus \oplus \otimes I T S Z T^\dagger S^\dagger P RZ ● $|0\rangle$ \otimes^z if ⋮ \sqrt{X} \sqrt{X}^\dagger ⓘ ⋮


OpenQASM 2.0 ▼

Y RX RY U RXX RZZ + Add

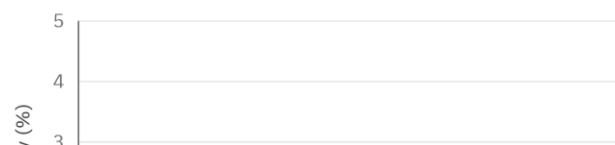
[Open in Quantum Lab](#)

q 0

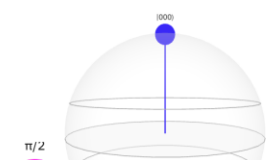
q 1



Probabilities ▼ ⓘ ⋮



Q-sphere ▼ ⓘ ⋮



```

1 OPENQASM 2.0;
2 include "qelib1.inc";
3 qreg q[3];
4 creg c[3];
5

```

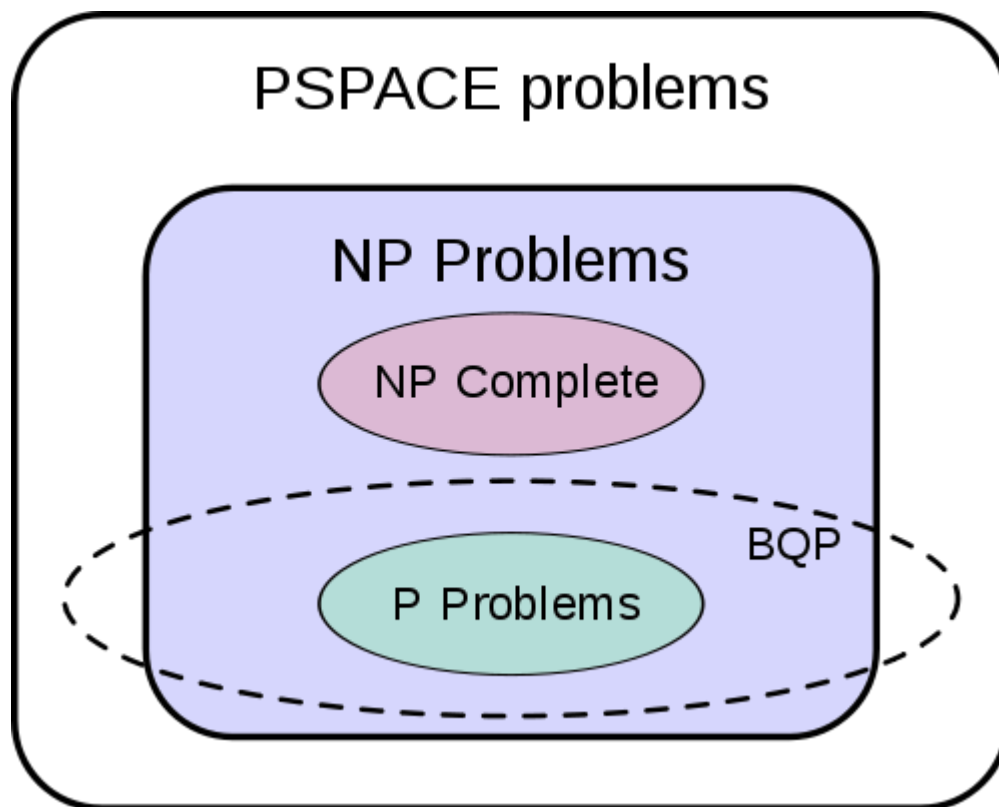
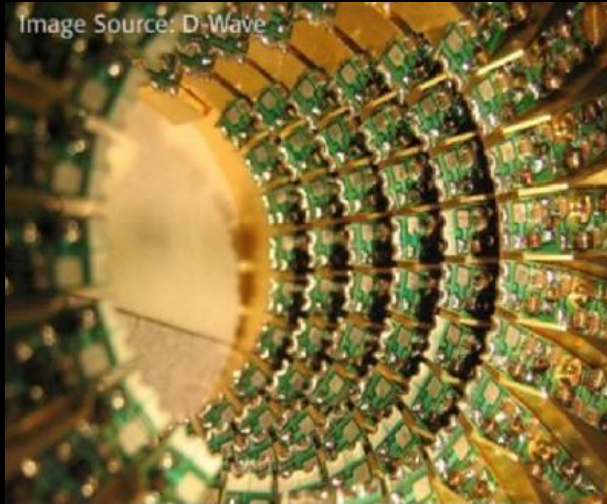


Image Source: D-Wave



30 Qubit Computer
10 teraFLOPS

Image Source: David Forbes



30 Bit Computer
~0.5 megaFLOPS

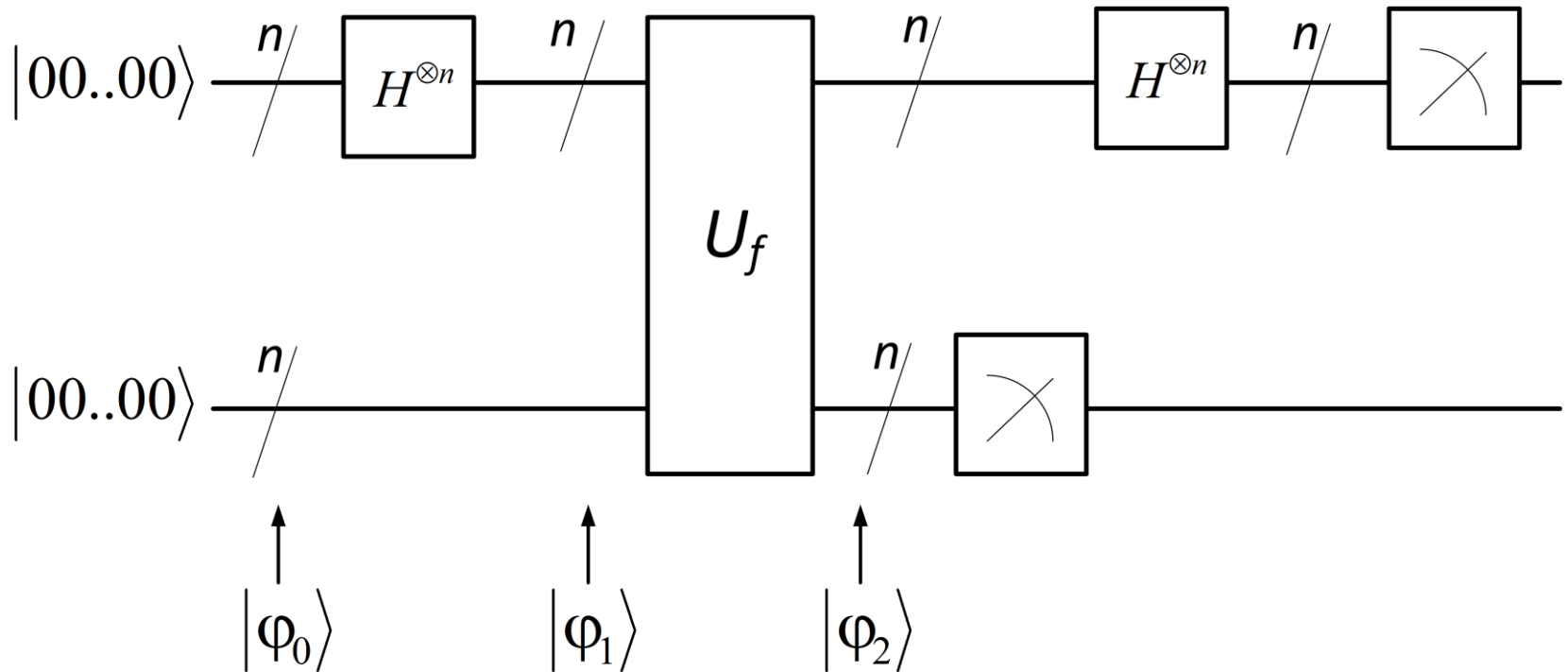
**Quantum computers perform
2 million times faster**

Simon-algoritmus

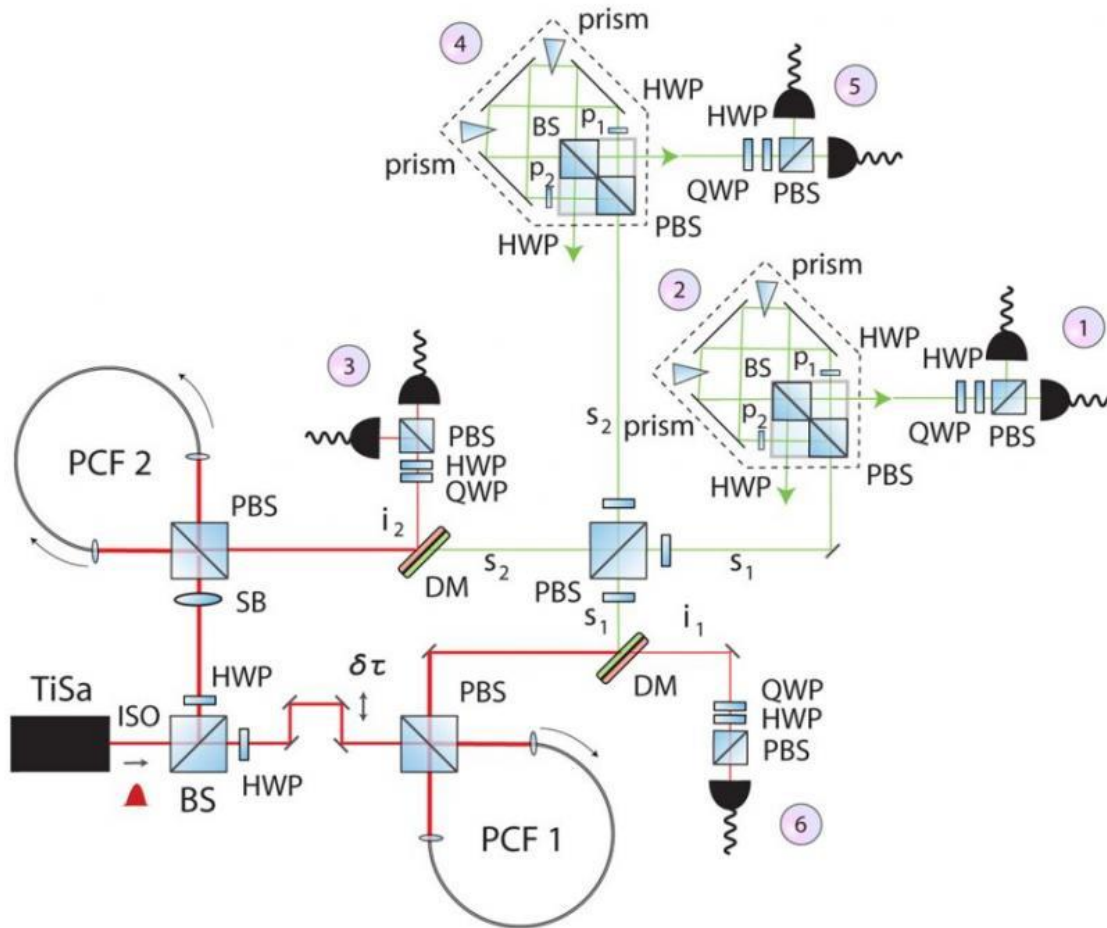
$$x \in \{0,1\}^n$$

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

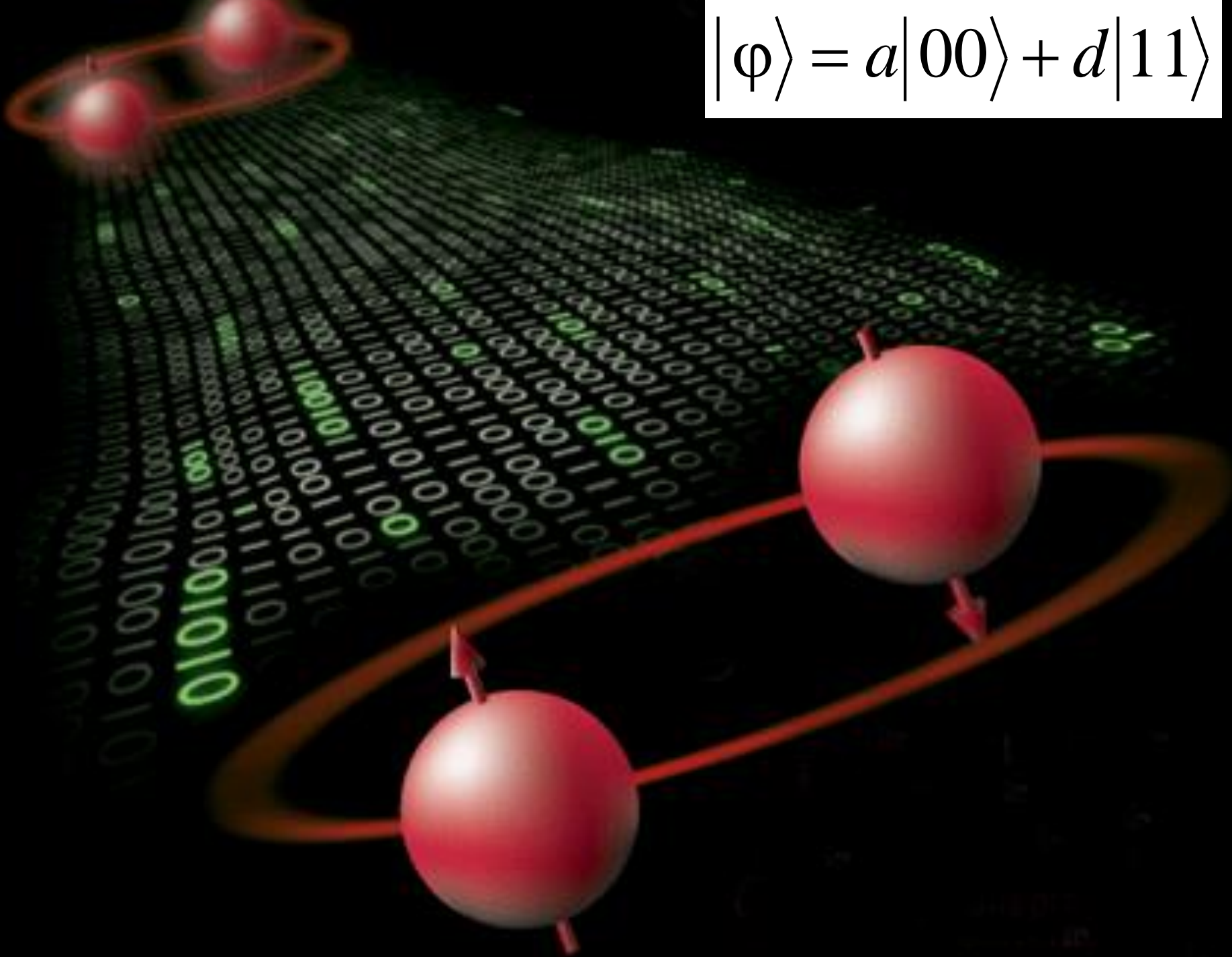
$$f(x) = x \oplus s$$



Simon-algorithmus



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







Afalfjd

Open Question

[Show me another »](#)

Is teleportation allowed in table tennis or ping pong?

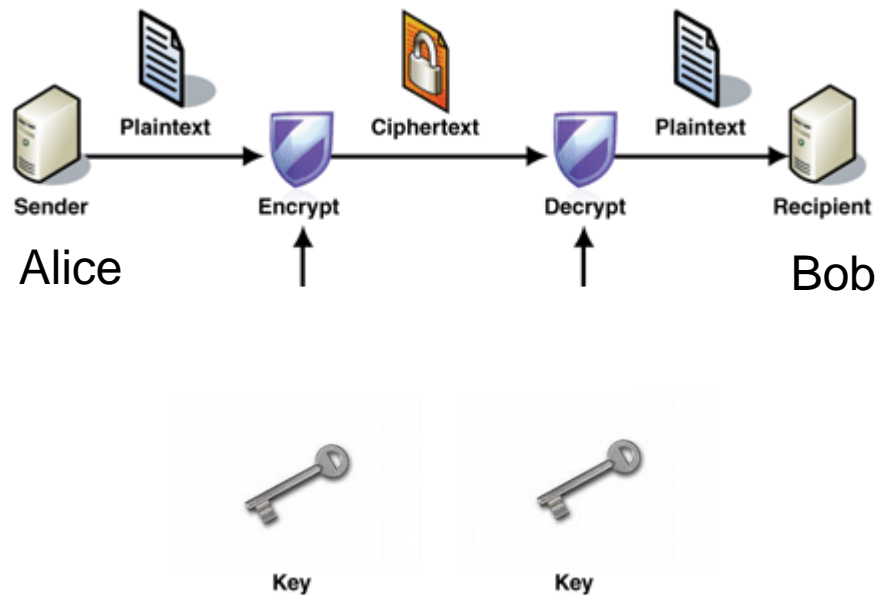
What if the opponent hits it really far back and I can't reach it and so I decided to shift/teleport into that location that I couldn't quickly reach and then return the ball? So is teleportation allowed?

3 days ago - 1 day left to answer.

[Report Abuse](#)

[Answer Question](#)

Kvantum alapú kulcsszétosztás



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

Kulcsok megosztása

Kvantummechanika elvei alapján lehallgathatatlan

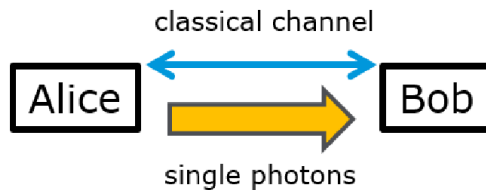
Kvantummechanika elvei alapján aktív támadó felfedi magát



Két típus

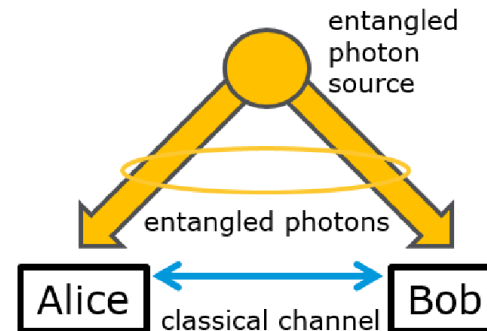
① Előállít és megmér

Prepare and Measure QKD



② Összefonódáson alapuló

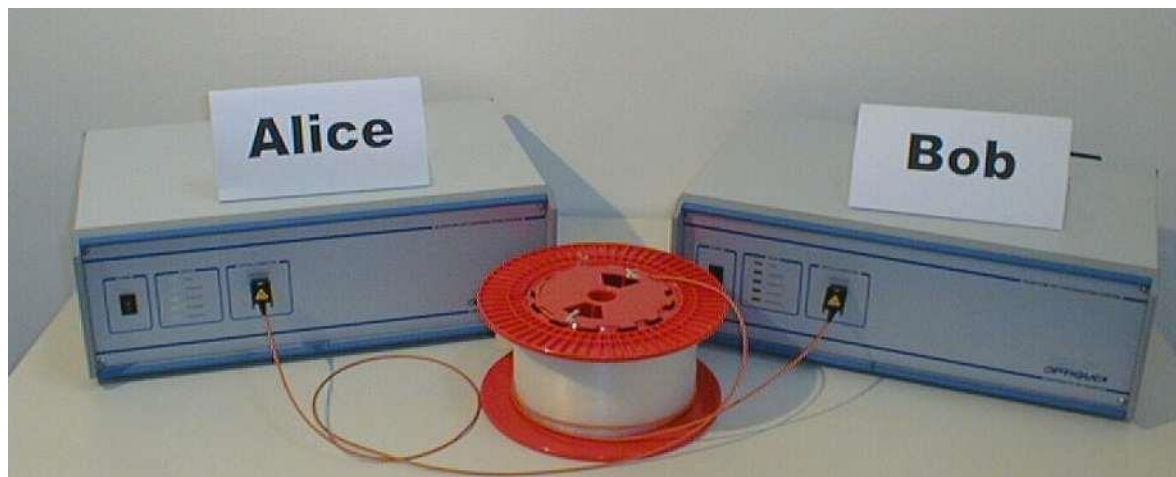
Entanglement based QKD



Két generáció

Első generáció: Diszkrét változójú (Discrete Variable, DV QKD)

Második generáció: Folytonos változójú (Continues Variable, CV QKD)



TOSHIBA



qtlabs

Quantum Technology Laboratories

SPECTRAL



AUREA
TECHNOLOGY



QUSIDE

id Quantique



MagiQ



IDQ
EUROPE


LUXQUANTA



'Much better than expected': Chinese 'hack-proof' quantum communication satellite put into service

Published time: 19 Jan, 2017 04:43

[Get short URL](#)



Beijing Aerospace Control Center. © Ju Zhenhua / Xinhua / Global Look Press via ZUMA Press

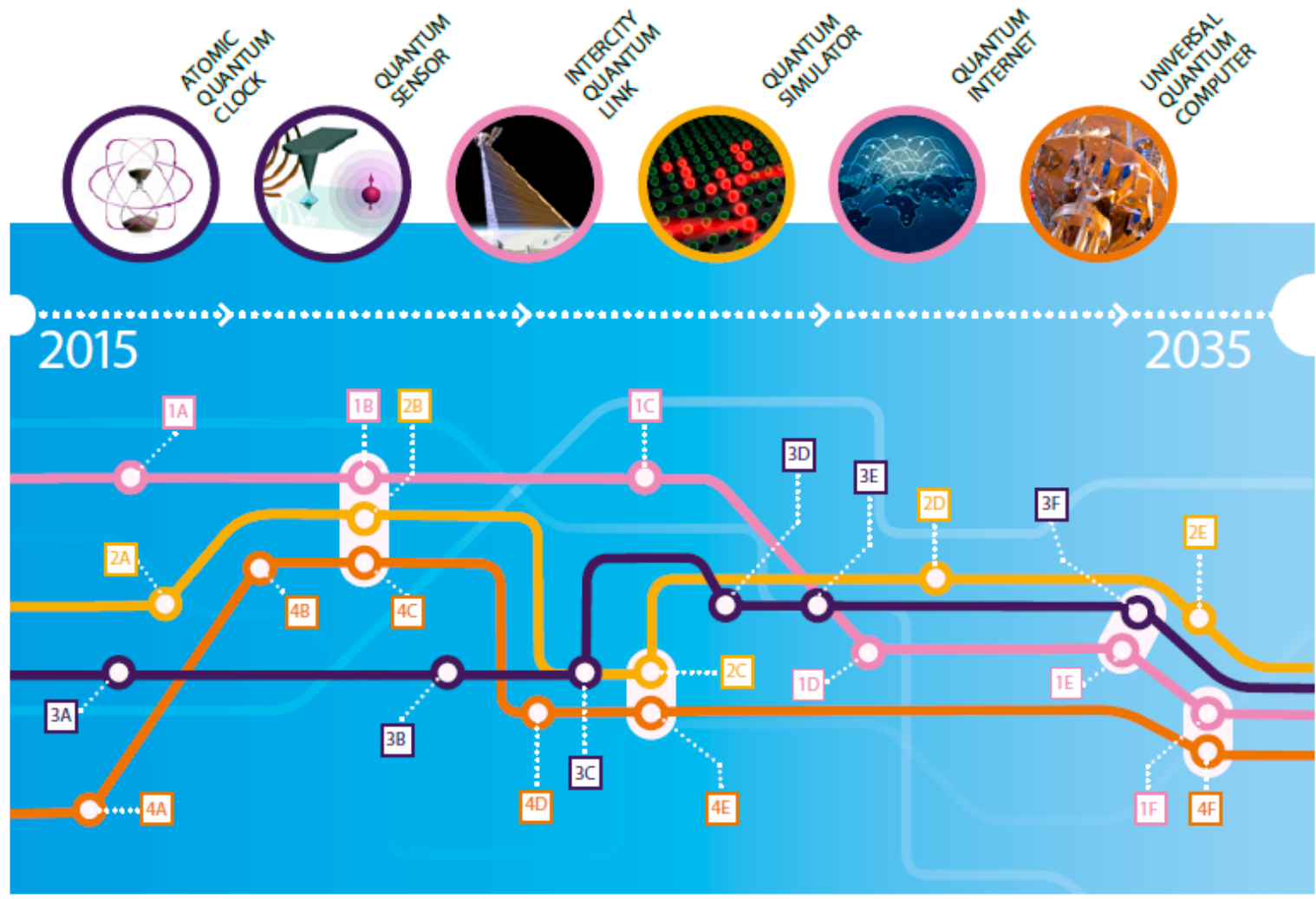


The world's first quantum communication satellite is now officially operational following months of in-orbit testing, the Chinese Academy of Sciences (CAS) announced, saying that performance of the device is "much better" than was initially expected.

Quantum Manifesto

A New Era of Technology

May 2016



• https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf

10.08.2021 10:55

Teilen:   

First quantum-secured video conference between German Federal agencies: QuNET demonstrates quantum communication

Desiree Haak *Strategie / Marketing / Koordination*

Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF

Today, two German federal authorities communicated via video for the first time in a quantum-secure manner. The QuNET project, an initiative funded by the German Federal Ministry of Education and Research (BMBF) to develop highly secure communication systems, is thus demonstrating how data sovereignty can be guaranteed in the future. This technology will not only be important for governments and public authorities but also to protect everyday data.

It was a foretaste of the communication of the future - or rather, the "data security" of the future. Because when Federal Research Minister Anja Karliczek invited members of the Federal Office for Information Security (BSI) to a video conference today, everything looked the same, at least for outsiders. Together with Andreas Könen, Head of Department CI "Cyber and IT Security" at the Federal Ministry of the Interior, Building and Community (BMI) and BSI Vice President Dr. Gerhard Schabhüser, the minister talked via video stream.

DECLARATION ON A QUANTUM COMMUNICATION INFRASTRUCTURE FOR THE EU

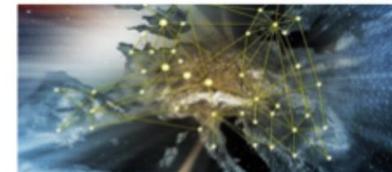
All 27 EU Member States

have signed a declaration agreeing to **work together** to explore how to **build a quantum communication infrastructure (QCI)** across Europe, boosting European capabilities in **quantum technologies, cybersecurity and industrial competitiveness.**

@FutureTechEU #EuroQCI



EuroQCI terrestrial segment



EuroQCI Space – indicative timeline



2021 22 23 24 25 26 27 28

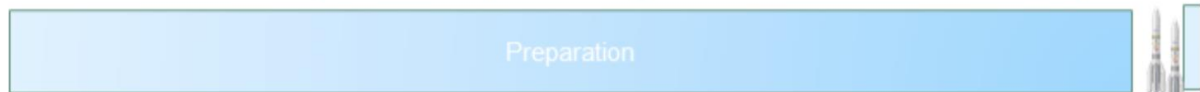
Eagle 1 – First in orbit demonstration



1st Generation – First end to end system



2nd Generation – Operational system integrated with Secure Connectivity



Key technologies

- Urban optical ground station
- QKD key management systems
- Quantum transmitter
- Detectors
- Optical Space Terminal
- Software

Legend
● 2 years for development (not available before 2023)
● 1 year for development (available before 2023)
● Available today



Számos helyen



<https://wigner.hu/quantumtechnology/>

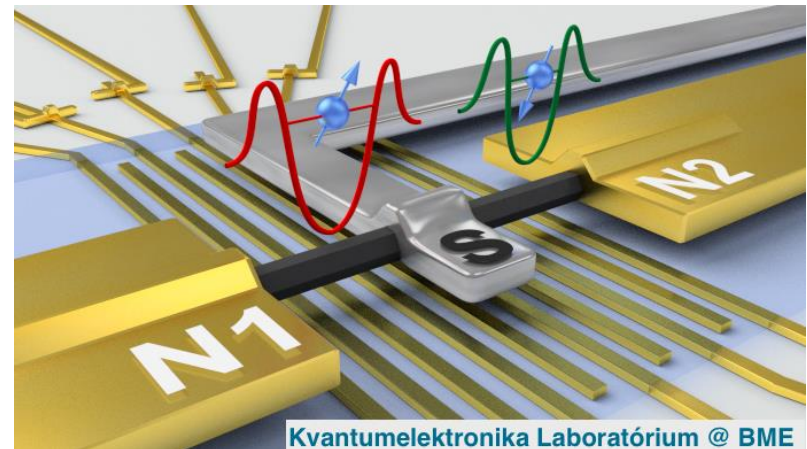
Kvantuminformatikai Nemzeti Laboratórium



<http://qi.nemzetilabor.hu/>

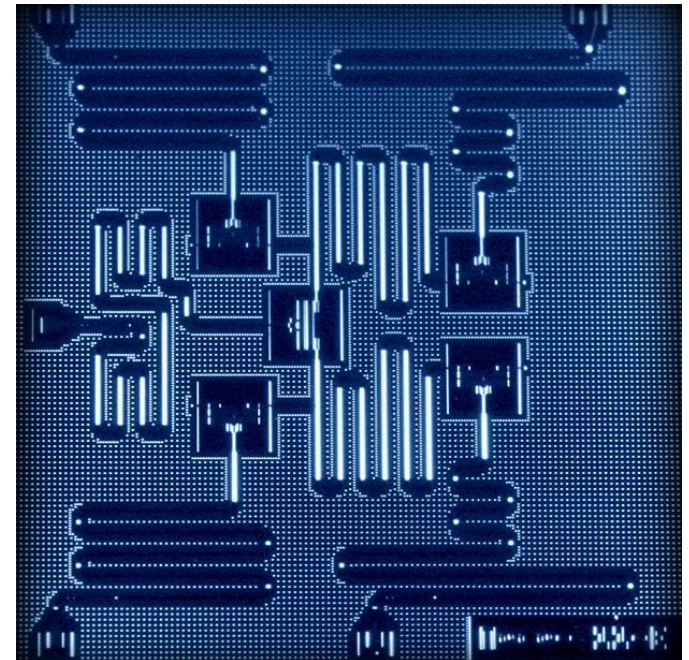
Stratégiai cél 2.

Atomokon és mesterséges atomokon alapuló hardverkomponensek fejlesztése kvantuminformatikai műveletekhez, és az ehhez szükséges laboratóriumi háttér fenntartása a nemzetközi élvonal szintjén.



Stratégiai cél 3.

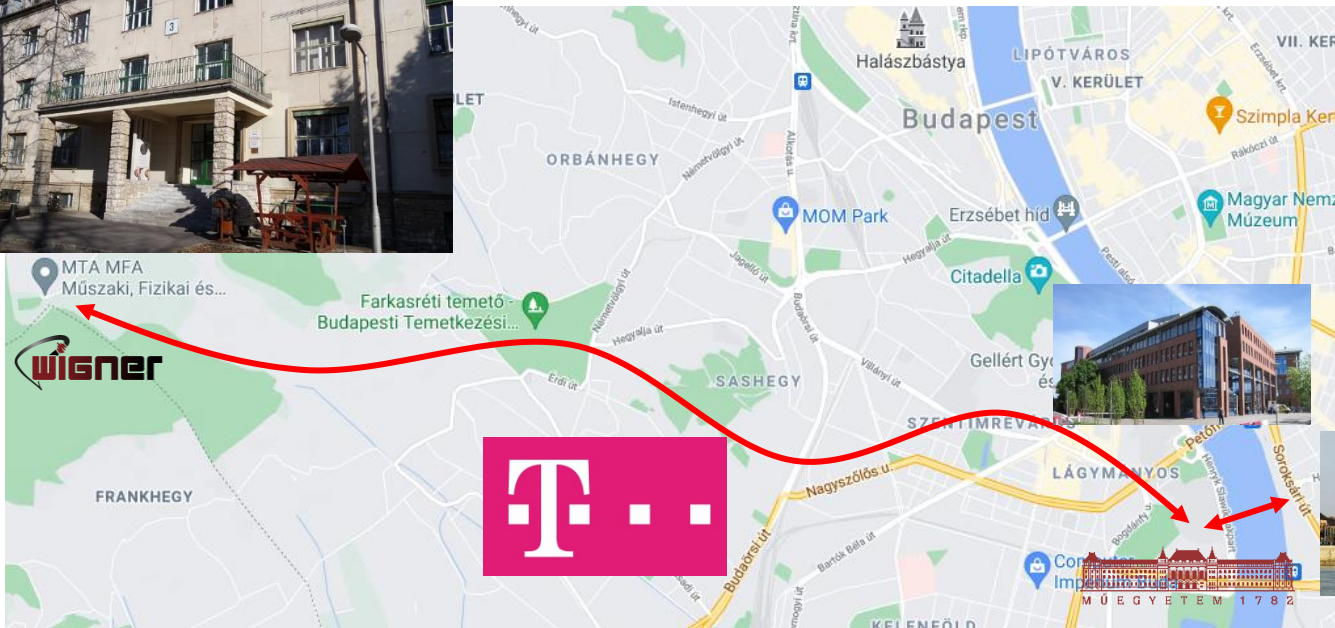
Kvantumszámításban élvonalbeli tudással rendelkező, a nagy infrastruktúráként működtetett kvantumszámítógépeket felhasználóként alkalmazni tudó hazai szakértelem felépítése.



Stratégiai cél 1.

Regionális kvantumkommunikációs hálózat létrehozása, amely csatlakoztatható az Európai Unióban tervezett kvantuminternethez.





MTA MFA
Műszaki, Fizikai és...



Farkasréti temető -
Budapesti Temetkezési...



Vezetékes megoldások

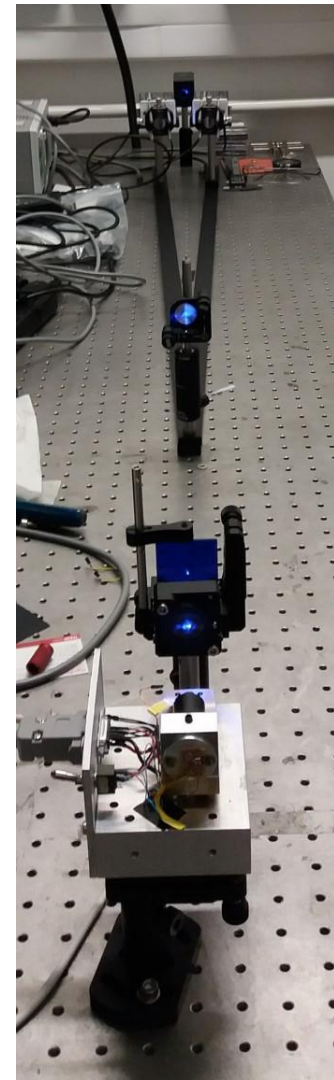
- Egyfotonon alapuló kvantum kulcsszétosztás (QKD), együttműködésben egy hazai távközlési céggel
- Nagy távolságú kvantumos kulcsszétosztás demonstrációja, második generációs QKD technológiával (CV-QKD)
- Együttműködés egy közép-európai fővárosokat összekötő QKD hálózat kialakításában a QUAPITAL projekt keretében
- Túl a QKD-n:összefonódáson alapuló közeghozzáférés, kvantum-internet megoldások

Szabadtér és világűr

- Összefonódáson alapuló szabadtéri kulcscsere a Duna felett
- Kisműholdas megoldások vizsgálata
- Optikai vevőállomások kialakítási lehetőségeinek vizsgálatas

Különböző hazai és nemzetközi kapcsolatok

- Együttműködés két hazai úripari céggel, együttműködés hazai távközlési cégekkel
- Több nemzetközi együttműködésben is részt veszünk (pl. európai QuantumSpaceship, EuroQCI)





2019-05-08

**Tanszékvezetőnk a Tudós Társaság
levelező tagja lett**

European Commission organises event on quantum communication infrastructure

Published on: 04/10/2019

On 30 September, the European Commission and the European Space Agency (ESA) organised a joint industry day on "quantum communication infrastructure (QCI) for Europe – space segment". This event was aimed at helping European industry and researchers develop the necessary technology for this emerging sector. The main goal was to share and discuss various options for potential space infrastructure for different use cases with QCI stakeholders.



Tanszékvezetőnket, Imre Sándort az Akadémia 191. Közgyűlésén a Tudós Társaság tagjai levelező taggá választották

„Ahhoz, hogy kvantumkommunikációs eszközöket lehessen fejleszteni, olyan fiatalokra van szükség, akik természettudományokat vagy műszaki tudományokat tanulnak.

Ahhoz, hogy ezekből termékek legyenek és az üzletekbe kerüljenek, olyan fiatalokra van szükség, akik jogot, marketinget vagy menedzsmentet tanulnak.

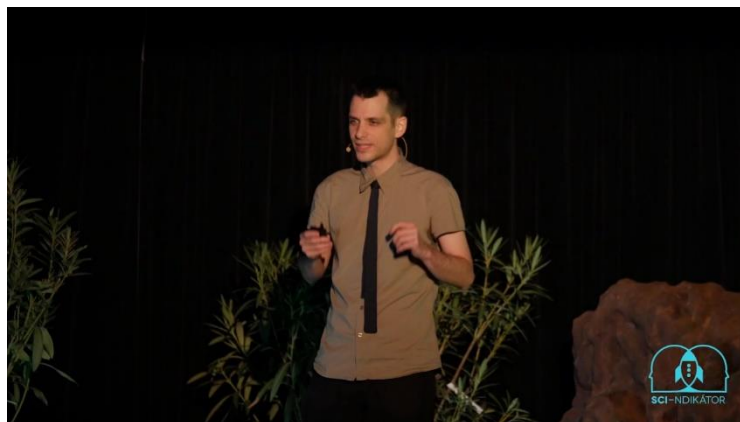
Ahhoz, hogy a rendszerek létezéséről beszélhessünk, olyan fiatalok kellene, akik média-kommunikáció ismereteket tanulnak.

Ahhoz, hogy vizuálisan megmutassuk, milyenek ezek a rendszerek, olyan fiatalok kellene, akik grafikát és alkalmazott művészeteket tanulnak.

Ahhoz, hogy a diákok következő generációit lehessen nevelni, olyan fiatalok kellene, akik tanárok lesznek.”



- Extraktorok alkalmazása kvantum alapú véletlenszám-generátorokban
- Kvantum véletlenszám-generátor tesztelési eredményeinek megjelenítése
- Kvantumszámítógépen futtatható algoritmusok alkalmazási lehetőségei
- Megbízható csomópontokon alapuló műholdas kvantumkommunikációs rendszer szimulációja
- Folytonos üzemű lézerműködésen alapuló kvantum-véletlenszámgenerátor
- Nyalábosztós struktúrán alapuló kvantum-véletlenszámgenerátor
- Folytonos változójú kvantumkulcsszétosztó rendszer működésének vizsgálata
- Kvantum gépi tanulás megvalósítási lehetőségeinek vizsgálata
- A korlátozott kvantumoptimalizálási módszer hatásának összehasonlító vizsgálata heterogén feldolgozási erőforrások nagy skálájában.
- Hitelesítési eljárások vizsgálata kvantumkommunikációs hálózatokban



Link Analysis of a Cubesat Based Quantum Key Distribution Platform

71st International Astronautical Congress 2020
IAC-20-B2.8.-GTS.3.1



Dominik Jakab, Laszlo Bacsardi
Budapest University of Technology and Economics, Budapest, Hungary

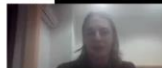


Kvantumkommunikáció hallgatói szemmel



QUANTUM COMMUNICATIONS IN SPACE

- „The art of transferring a quantum state from one place to another.”
- Advances in quantum optics are making space applications possible
 - Space is a good medium for transmission
 - Already major projects, like Micius satellite, EuroQCI



[4] "Position-Based Quantum Cryptography: Impossibility and Constructions,"
SIAM J. Comput., 2013.

Is Quantum Position Verification **Secure?**

● **Classical attacks?**



○ Secure!

● **Quantum attacks?**



○ Maybe
(Like RSA)

So, this is where things stand right now.



35. ORSZÁGOS
TUDOMÁNYOS
DIÁKKÖRI
KONFERENCIA
2021

ELISMERŐ OKLEVÉL

amely tanúsítja, hogy

Czermann Márton

A 35. ORSZÁGOS TUDOMÁNYOS DIÁKKÖRI KONFERENCIA

Informatika Tudományi

Szekciója

Kiberbiztonság

tagozatában bemutatott pályamunkájával

második

helyezést ért el.

Budapest, 2021. április 1.

Dr. Tóth Melinda
a Szekció ügyvezető elnöke

Dr. Kozsik Tamás
a Szakmai Bizottság elnöke

Prof. Dr. Szendrő Péter
az OTDT elnöke



Infocommunications Journal

A PUBLICATION OF THE SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS (HTE)

June 2021

Volume XIII

Number 2

ISSN 2061-2079

MESSAGE FROM THE EDITOR-IN-CHIEF

Recent Advances in Communication System Management,
Security and Performance *Pal Varga* 1

SELECTED INVITED PAPERS

Checking the Accuracy of Siitperf *Gábor Lencse* 2

Enhancing the operational efficiency of quantum random number
generators *Botond L. Márton, Dóra Istenes and László Bacszárdi* 10

Effects of selected noises on the quantum memory of satellite
based quantum repeaters *András Mihály and László Bacszárdi* 19

Infocommunications Journal

ELISMERŐ OKLEVÉL

amely tanúsítja, hogy

Czermann Márton

A 35. ORSZÁGOS TUDOMÁNYOS DIÁKKÖRI KONFERENCIA

Informatika Tudományi

Szekciója

Kiberbiztonság

tagozatában bemutatott pályamunkájával

második

helyezést ért el.

Budapest, 2021. április 1.

Dr. Tóth Melinda
a Szekció ügyvezető elnöke

Dr. Kozsik Tamás
a Szakmai Bizottság elnöke

Prof. Dr. Szendrő Péter
az OTDT elnöke



HIT HÁLÓZATI RENDSZEREK ÉS SZOLGÁLTATÁSOK TANSZÉK
www.hit.bme.hu

ÚJGENERÁCIÓS KVANTUMKOMMUNIKÁCIÓS HÁLÓZATOK

- További kvantumkommunikációs protokollok alkalmazása
 - Kvantumteleportáció
 - Szupersűrű tömörítés
- Fizikai korlátok
 - Nem klónozhatósági tétel
 - Memória



© Hálózati Rendszerek és Szolgáltatások Tanszék

4

több mint 20 éve oktatunk önálló tárgyként
kvantuminformatikát

számos szakdolgozat, diplomadolgozat

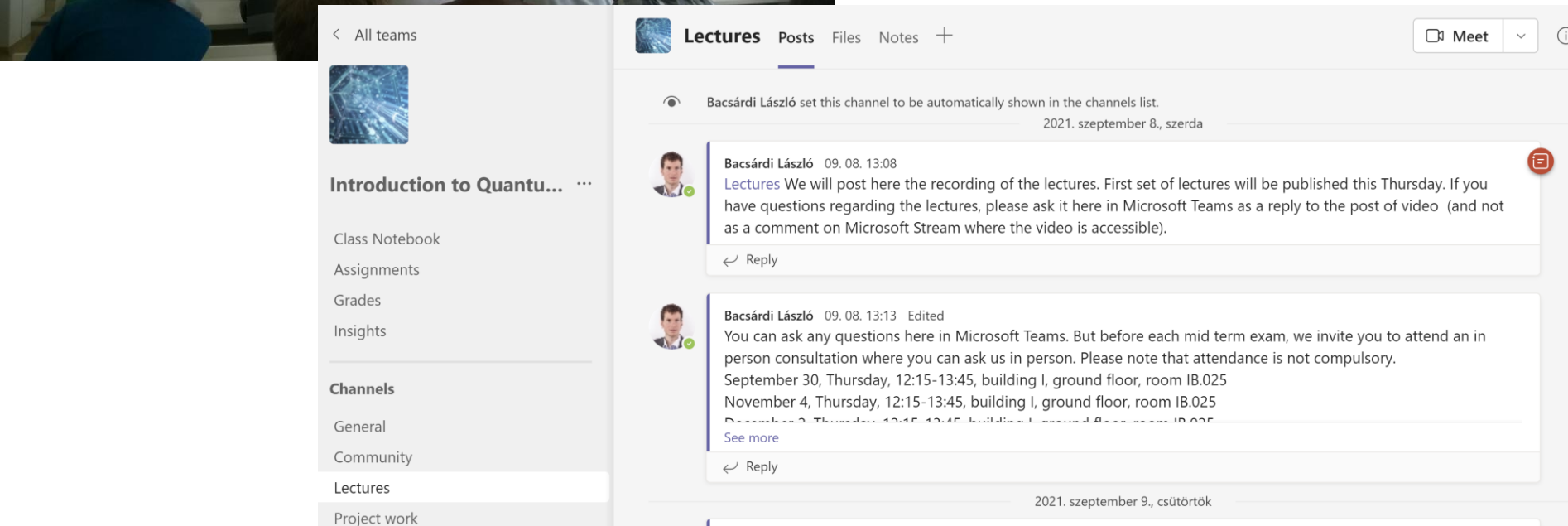
tanulmányi
versenyek

TDK, OTDK





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



The screenshot shows a Microsoft Teams channel named 'Lectures'. The left sidebar lists various team resources: 'Introduction to Quantu...', 'Class Notebook', 'Assignments', 'Grades', 'Insights', 'Channels', 'General', 'Community', 'Lectures' (highlighted), and 'Project work'. The main chat area shows two messages from 'Bacsárdi László':

- Message 1:** Posted on 09.08.13:08. Text: 'Lectures We will post here the recording of the lectures. First set of lectures will be published this Thursday. If you have questions regarding the lectures, please ask it here in Microsoft Teams as a reply to the post of video (and not as a comment on Microsoft Stream where the video is accessible).' Includes a 'Reply' button.
- Message 2:** Posted on 09.08.13:13, edited. Text: 'You can ask any questions here in Microsoft Teams. But before each mid term exam, we invite you to attend an in person consultation where you can ask us in person. Please note that attendance is not compulsory. September 30, Thursday, 12:15-13:45, building I, ground floor, room IB.025 November 4, Thursday, 12:15-13:45, building I, ground floor, room IB.025 December 2, Thursday, 12:15-13:45, building I, ground floor, room IB.025' Includes a 'See more' link and a 'Reply' button.

At the bottom right of the chat area, the date '2021. szeptember 9., csütörtök' is displayed.



Quantum Technology Open Master

Bringing together the shared knowledge of experts in quantum technology from over 30 top institutions across Europe and around the World

Study for ECTS credits in Quantum Technology at top institutions across Europe



Hand-drawn diagrams and logos on the glass facade:

- A red diagram of a circular structure with internal connections.
- A red diagram of a vertical structure with a circular top.
- A white cloud icon with a dashed line leading to a red square containing a white 'R'.
- A white logo with the letters 'BME'.
- A white logo with the word 'SECURITY' and a shield icon.

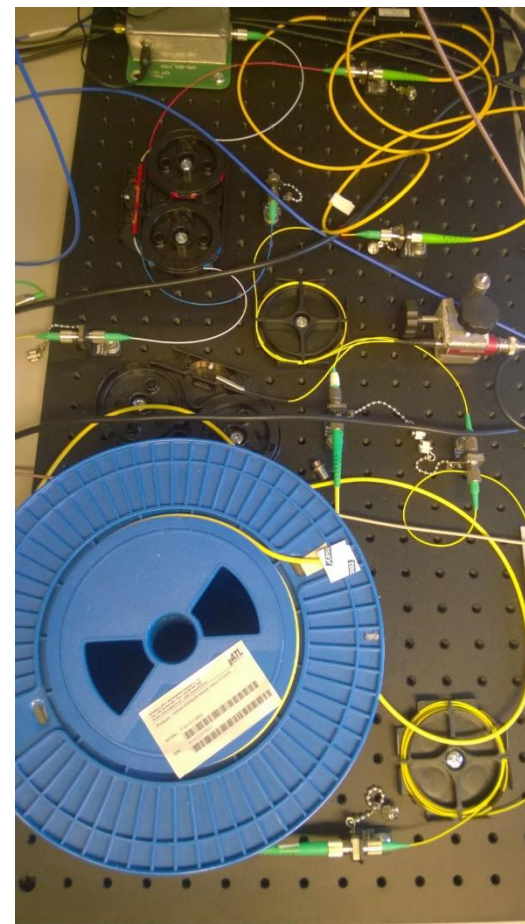
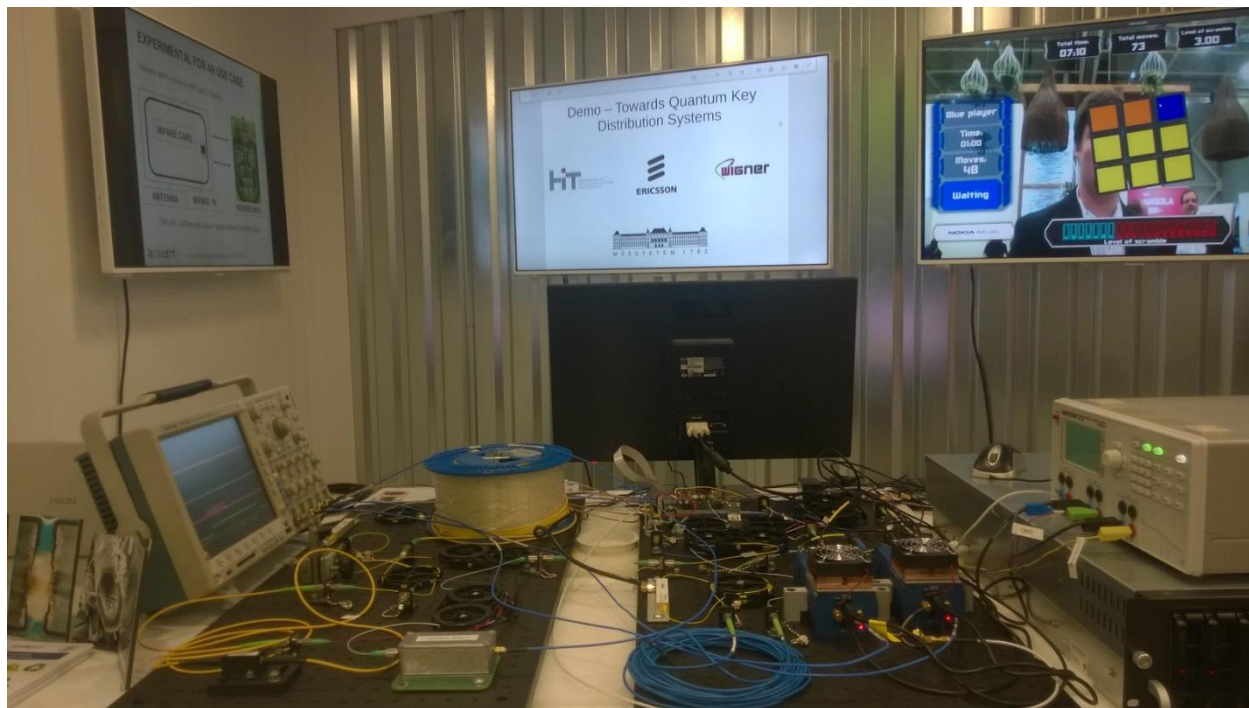
Yellow sign on the brick pillar: "PLEASE DO NOT BLOCK THE ENTRANCE"

Signs on the glass entrance doors:

- "PLEASE DO NOT BLOCK THE ENTRANCE"
- "PLEASE DO NOT BLOCK THE ENTRANCE"

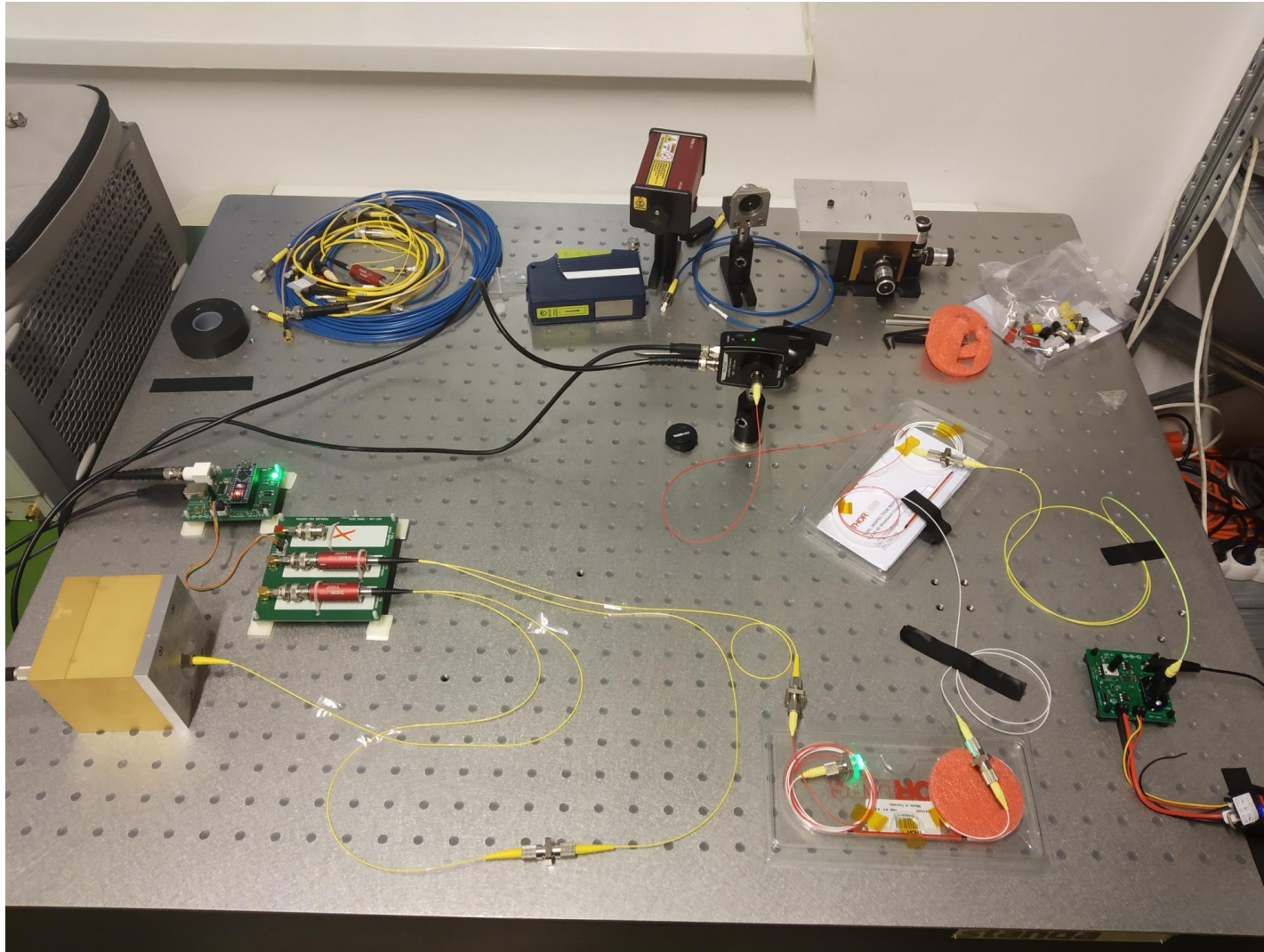


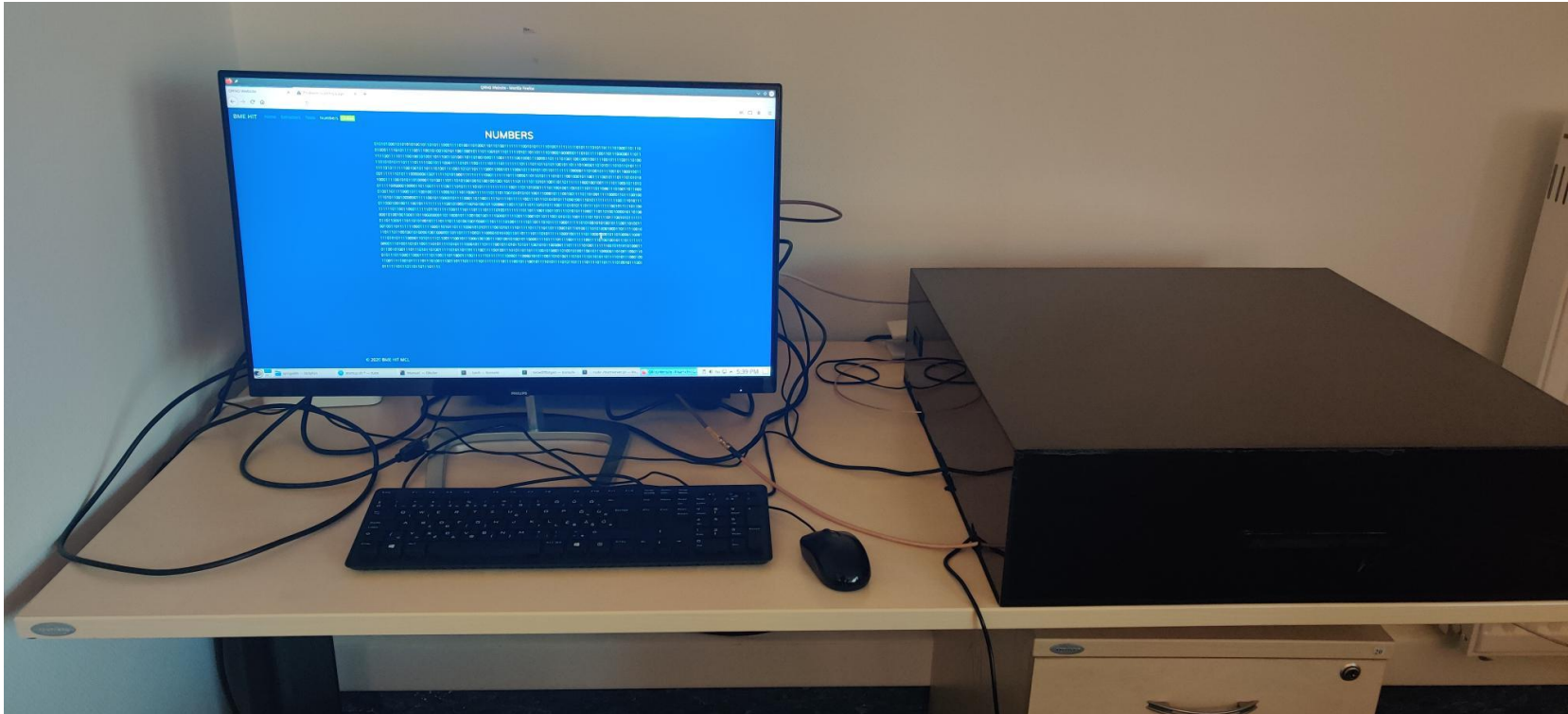
Partnerünk a Relcom Kft.
www.relcom.hu

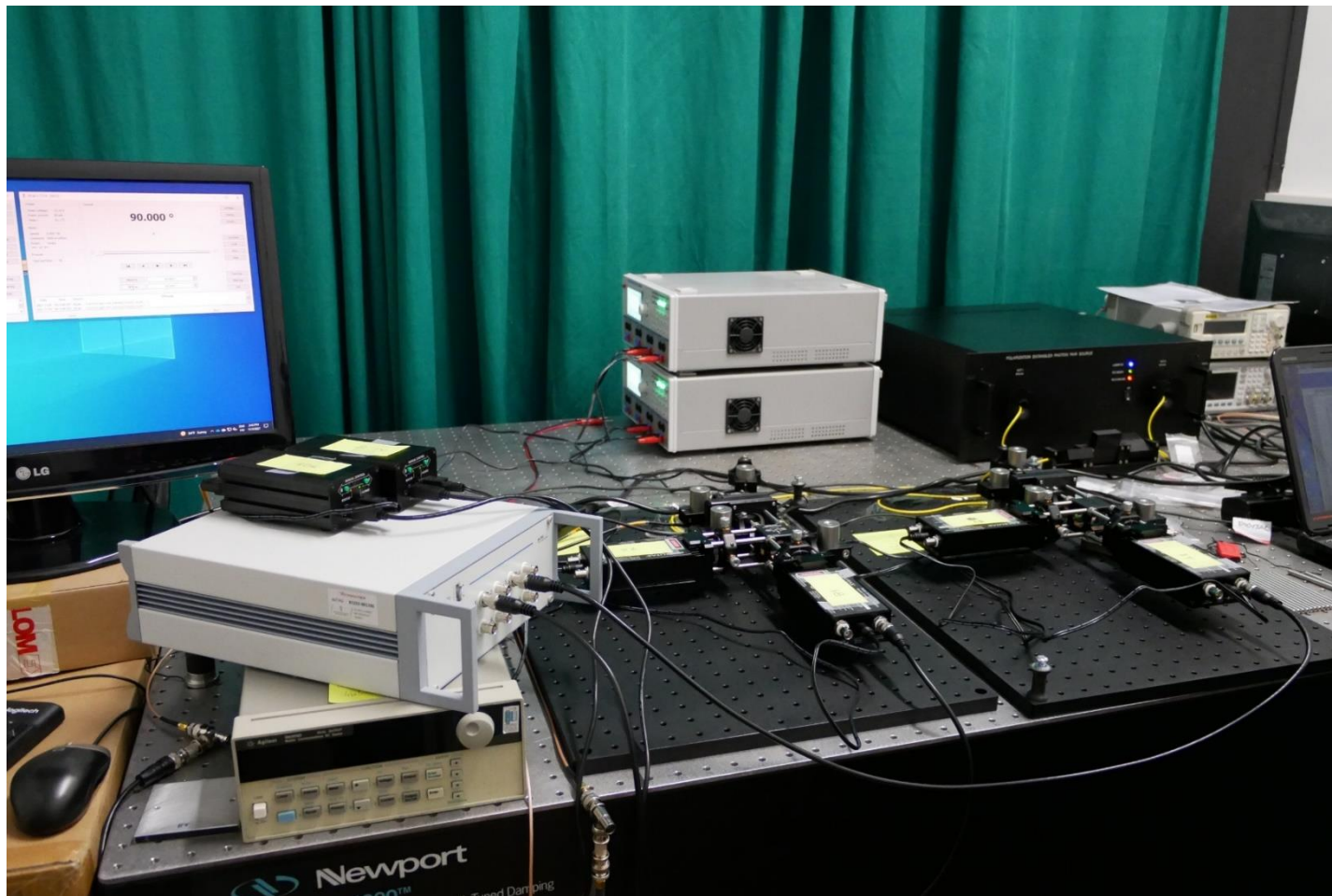


BB84 protokoll
Partnerünk az Ericsson





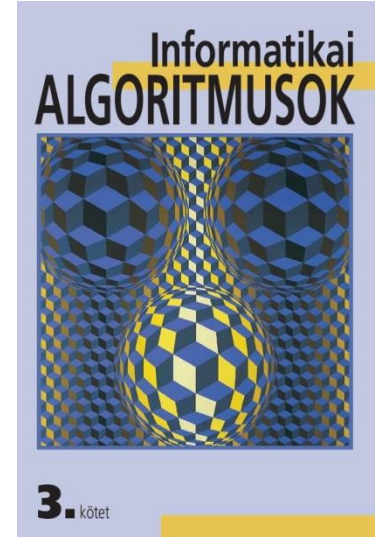
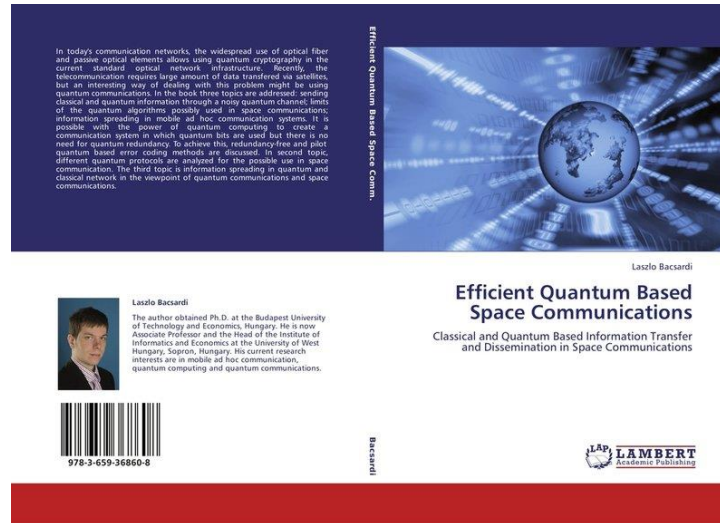
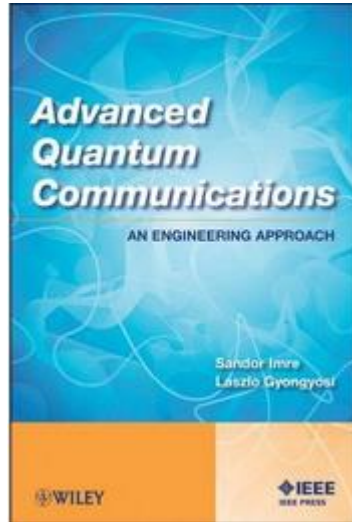
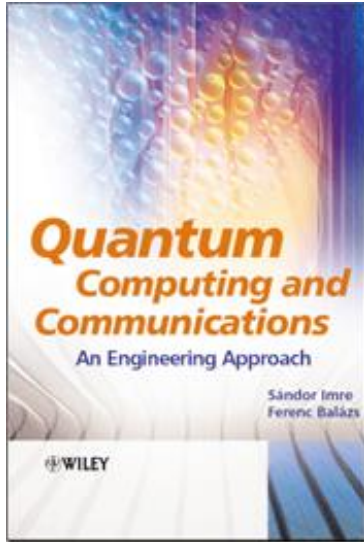






Összefonódáson alapuló protokoll
Partnerünk a Vodafone Hungary





BME Mobil Kommunikáció és Kvantumtechnológiák Laboratórium
<http://www.mcl.hu/quantum/>

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

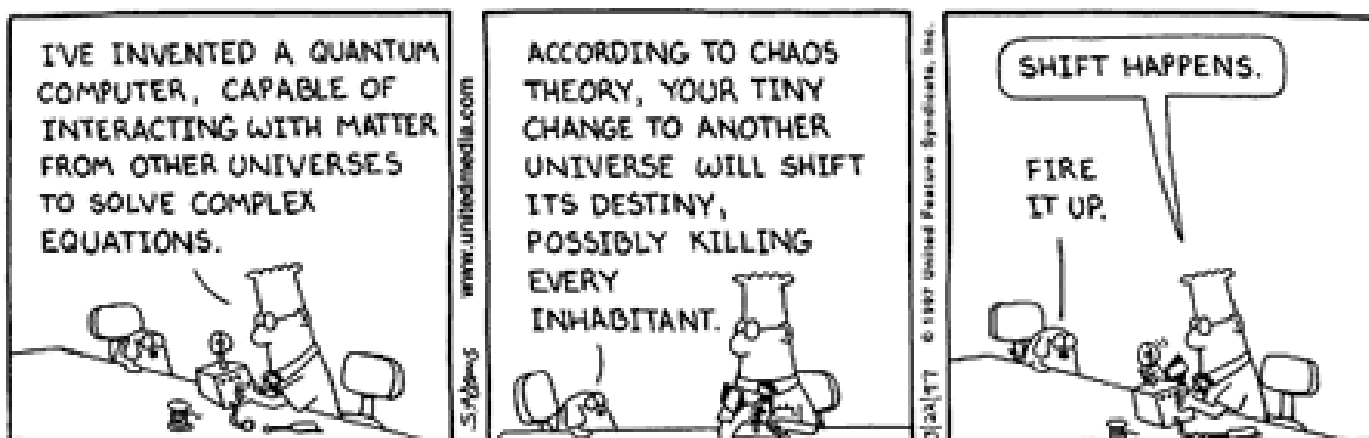
Bevezetés a kvantum informatikába és kommunikációba
<https://www.vik.bme.hu/kepzes/targyak/VIHIAV06/>

A kutatást az Innovációs és Technológiai Minisztérium és a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal támogatta a Kvantuminformatika Nemzeti Laboratórium keretében.

Bacsárdi László kutatását a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíja támogatja.

Az Innovációs és Technológiai Minisztérium ÚNKP-21-5 kódszámú Új Nemzeti Kiválósági Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.





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

bacsardi@hit.bme.hu