Kvantum alapú megoldások vezetékes és vezeték nélküli hálózatokban

Bacsárdi László

Nyugat-magyarországi Egyetem, bacsardi@inf.nyme.hu

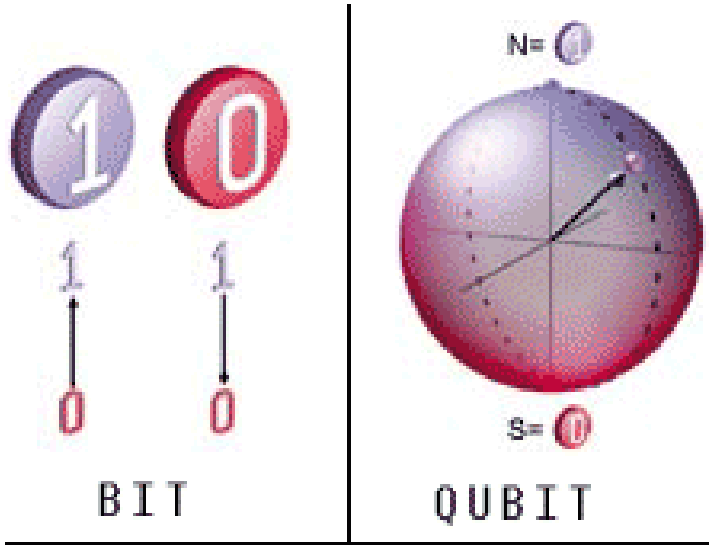
Imre Sándor

BME Hálózati Rendszerek és Szolgáltatások Tanszék

imre@hit.bme.hu

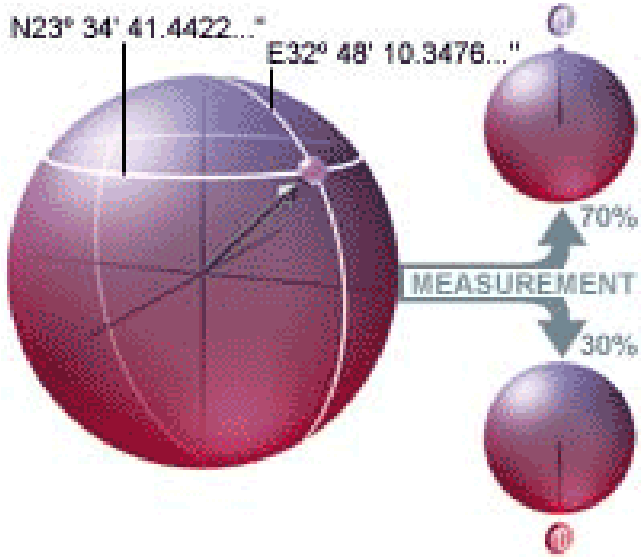
0 és 1

Kvantumbit (qubit)



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

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

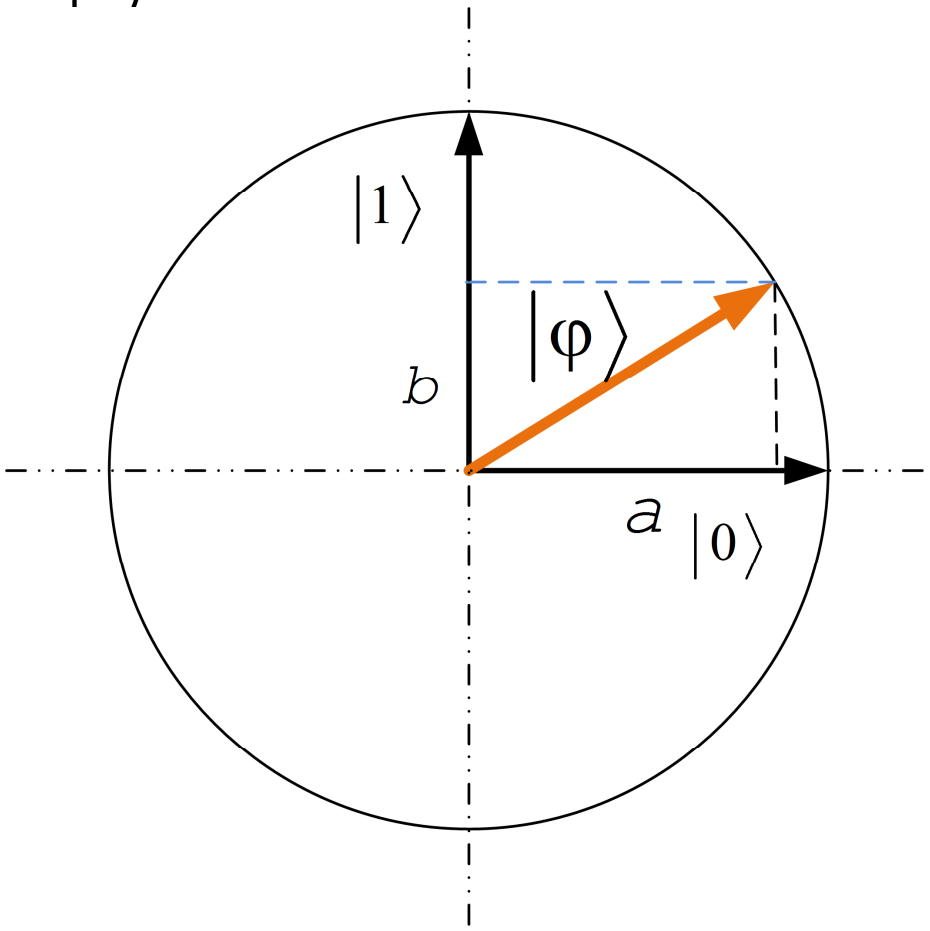


Szemléltetés valós amplitúdókkal

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

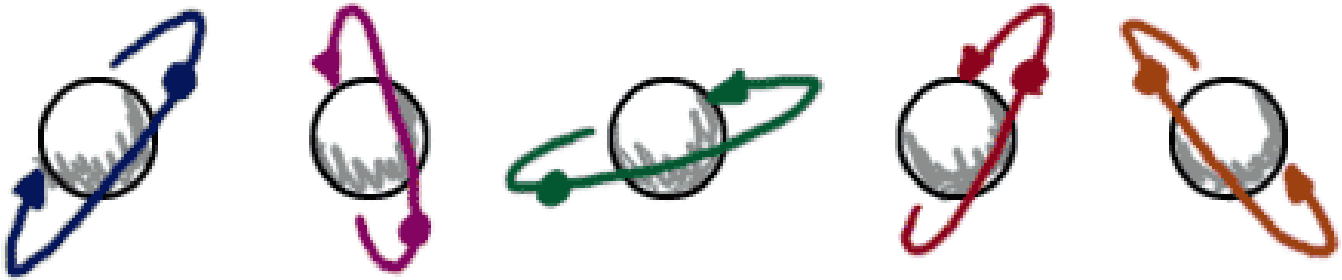
$$|a|^2 + |b|^2 = 1.$$

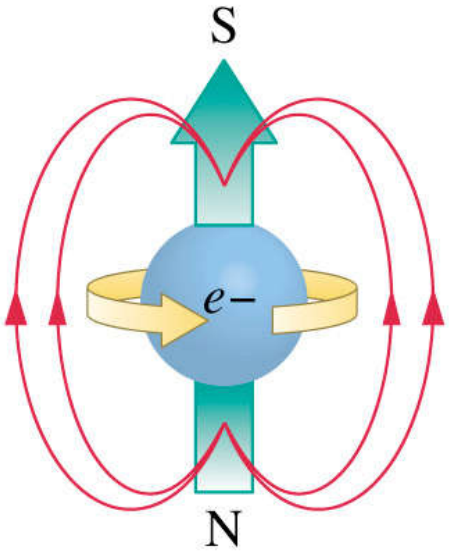
$$a, b \in C$$



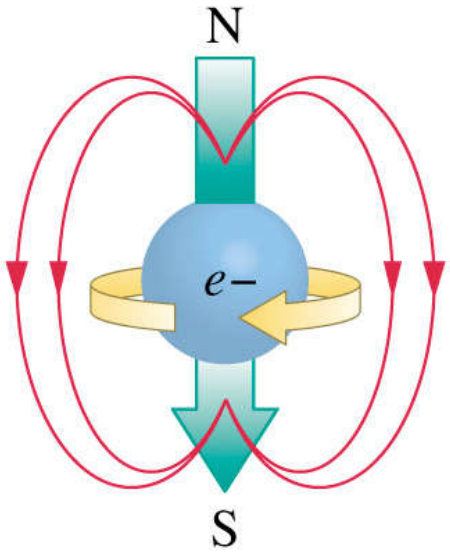
L. Bacsardi, M. Galambos, S. Imre, A. Kiss. "Quantum Key Distribution over Space-Space Laser Communication Links," AIAA Space 2012, Pasadena, California, Sept, 2012.

Mi lehet kvantumbit?

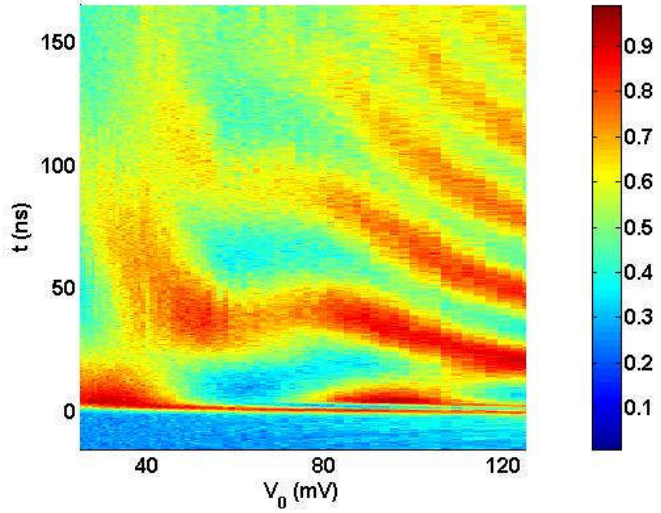




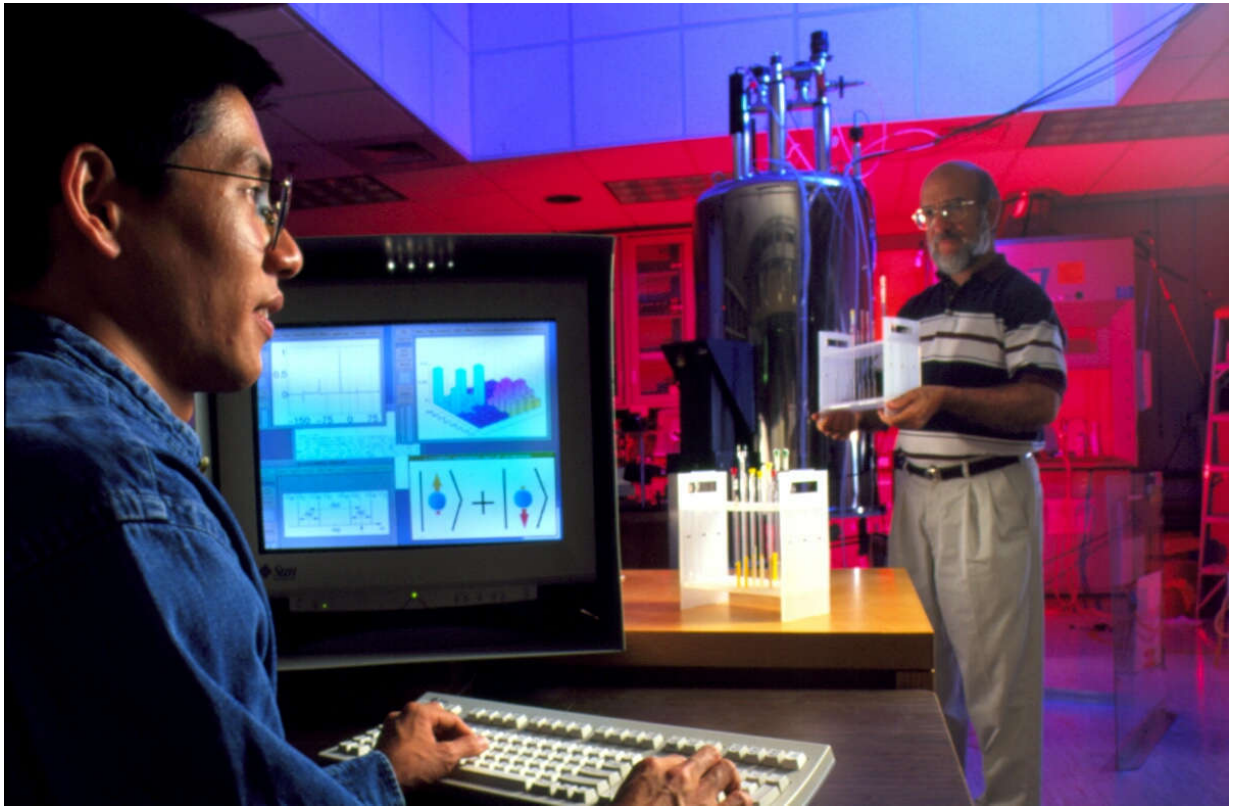
$m_s = +\frac{1}{2}$



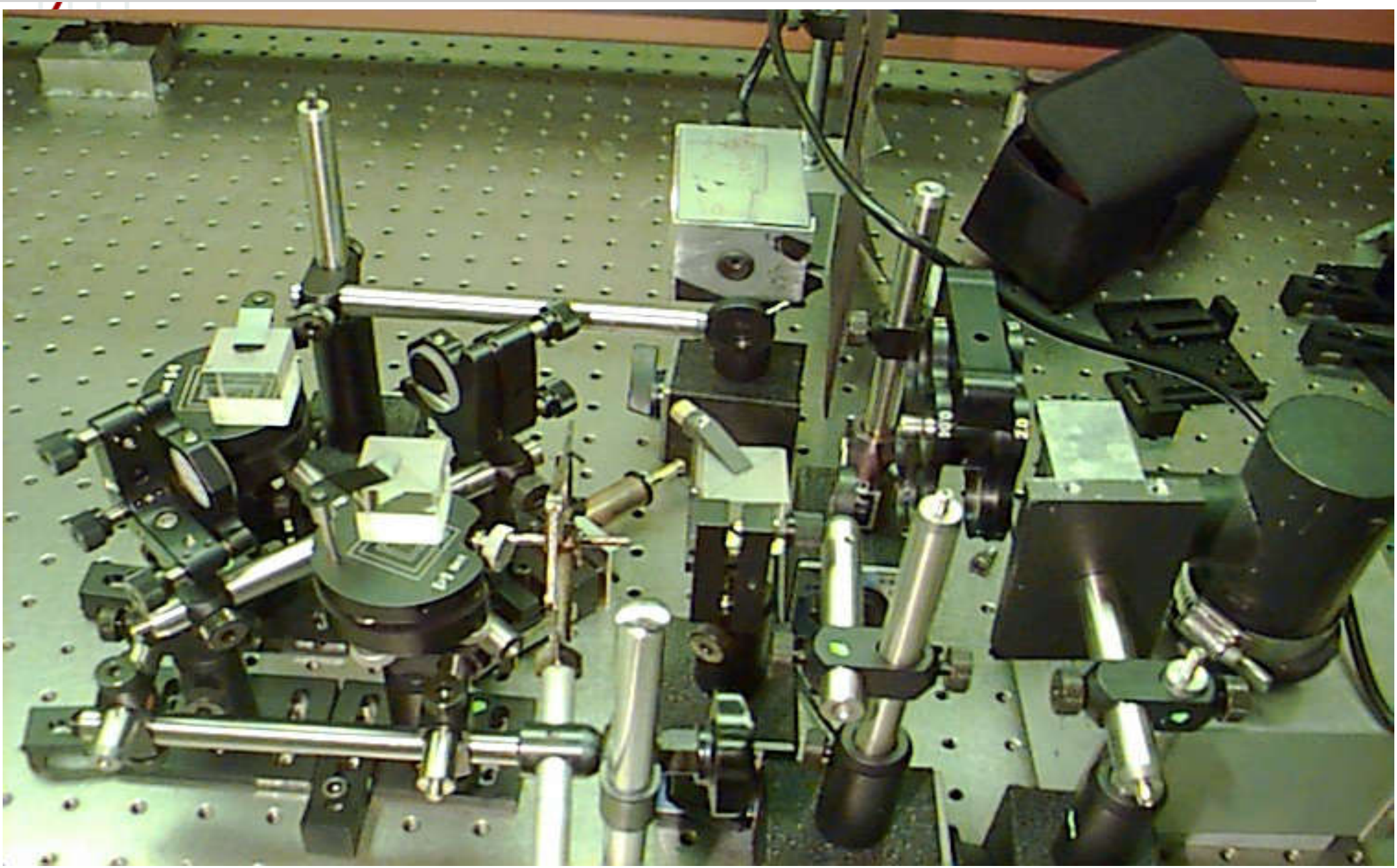
$m_s = -\frac{1}{2}$



Kvantum eszközök (1)



Kvantum eszközök (2)



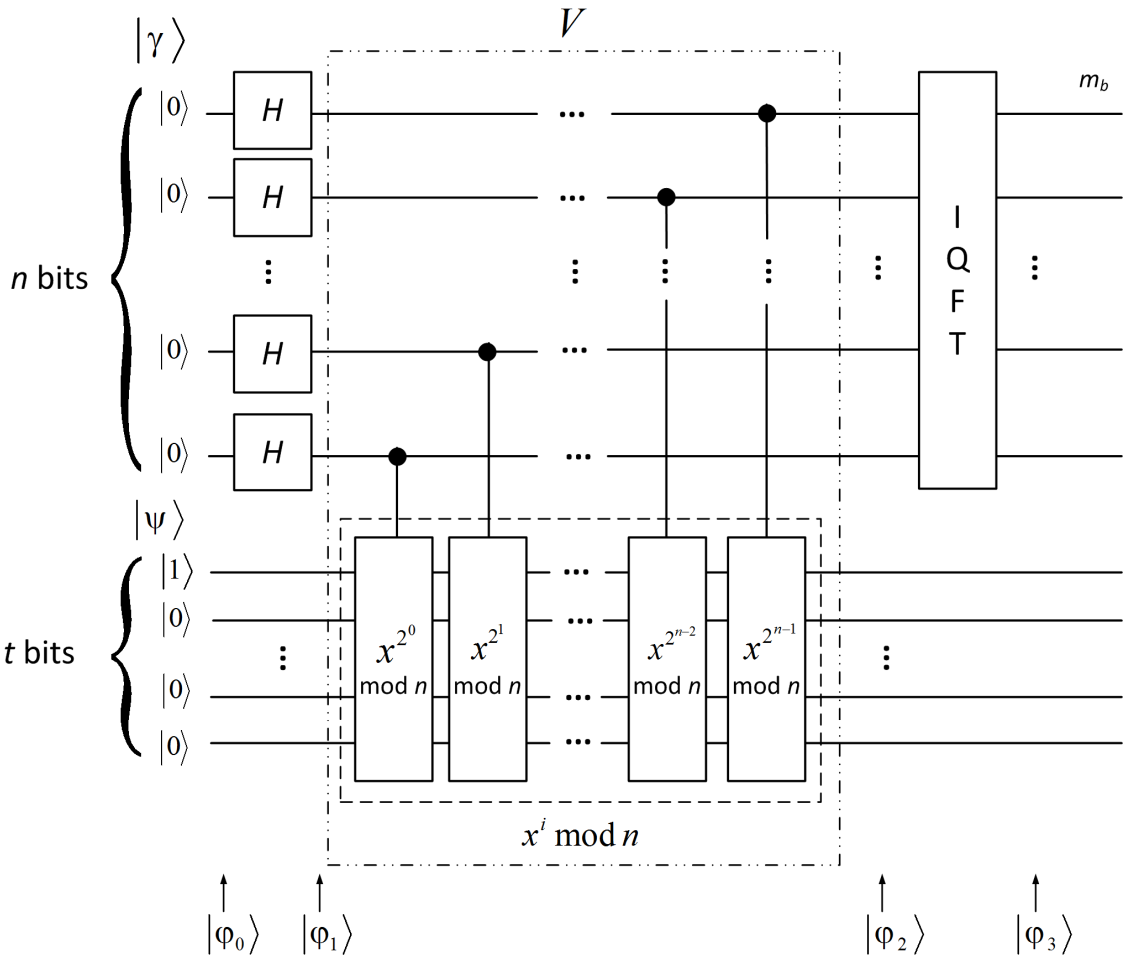
Kvantumregiszter

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

$$|\varphi\rangle^{\otimes 2} = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

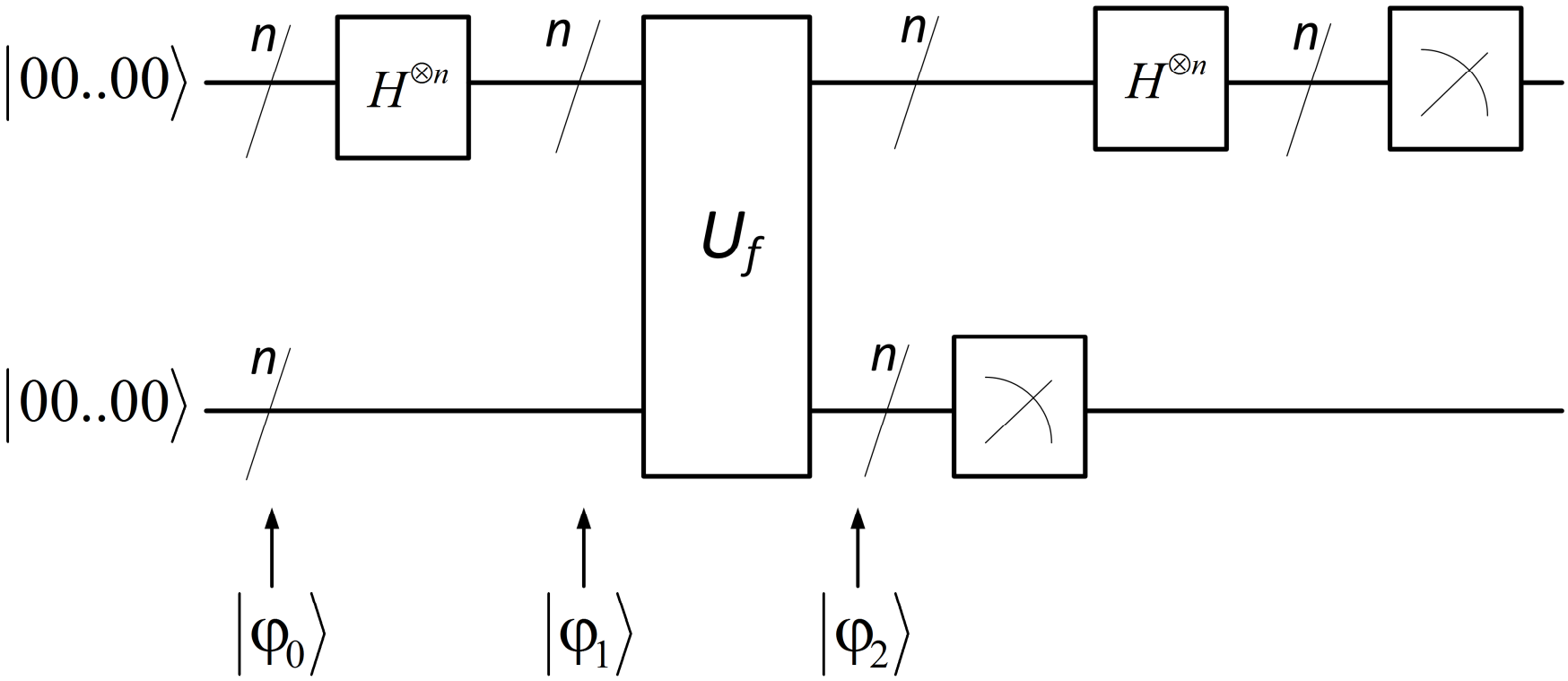
$$|\varphi\rangle^{\otimes 4} = a|0000\rangle + b|0001\rangle + \ldots + o|1110\rangle + p|1111\rangle$$

Shor-algoritmus



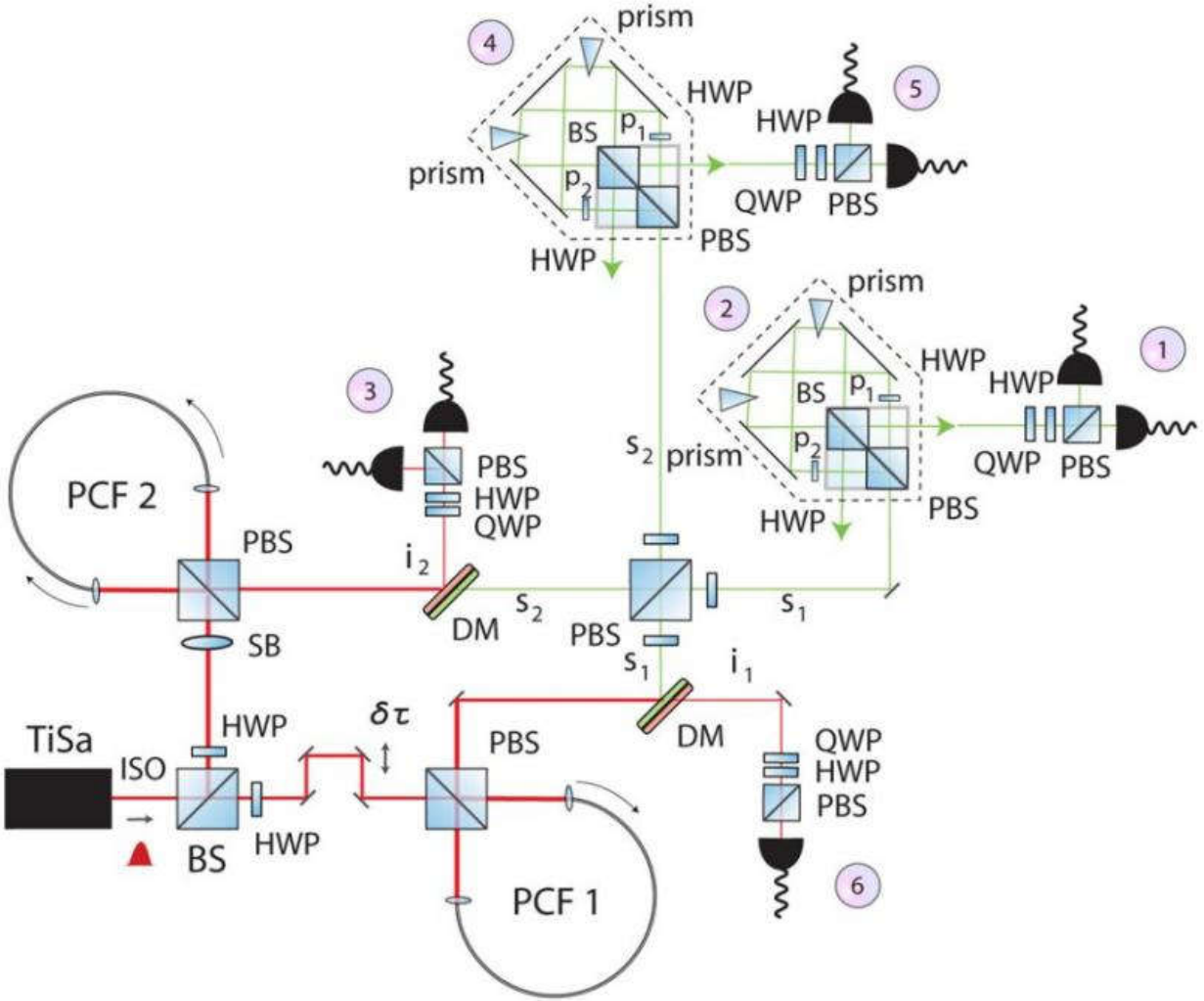
Simon-algoritmus

$$x \in \{0,1\}^n$$
$$f(x) : \{0,1\}^n \rightarrow \{0,1\}^n$$
$$f(x) = x \oplus s$$



Ábra: Bacsárdi L., Galambos M., Imre S., „Kvantumalapú algoritmusok”. Informatikai algoritmusok, III. kötet, pp. 1785-1827. *Mondat Kiadó., 2013*

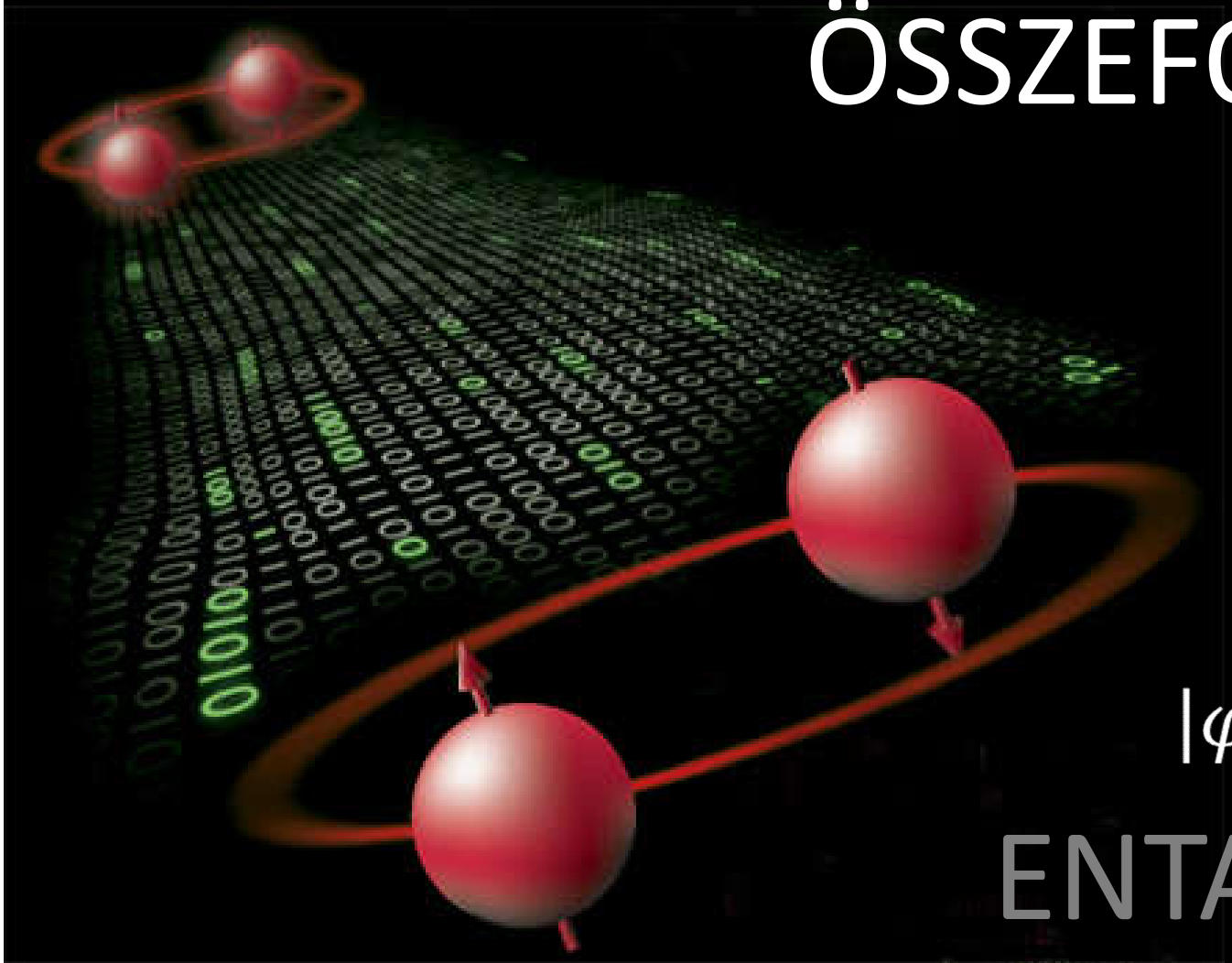
Simon-algoritmus



„Experimental Realization of a One-Way Quantum Computer Algorithm Solving Simon's Problem",
M. S. Tame, B. A. Bell, C. Di Franco, W. J. Wadsworth, and J. G. Rarity, Phys. Rev. Lett. 113, 200501, 2014

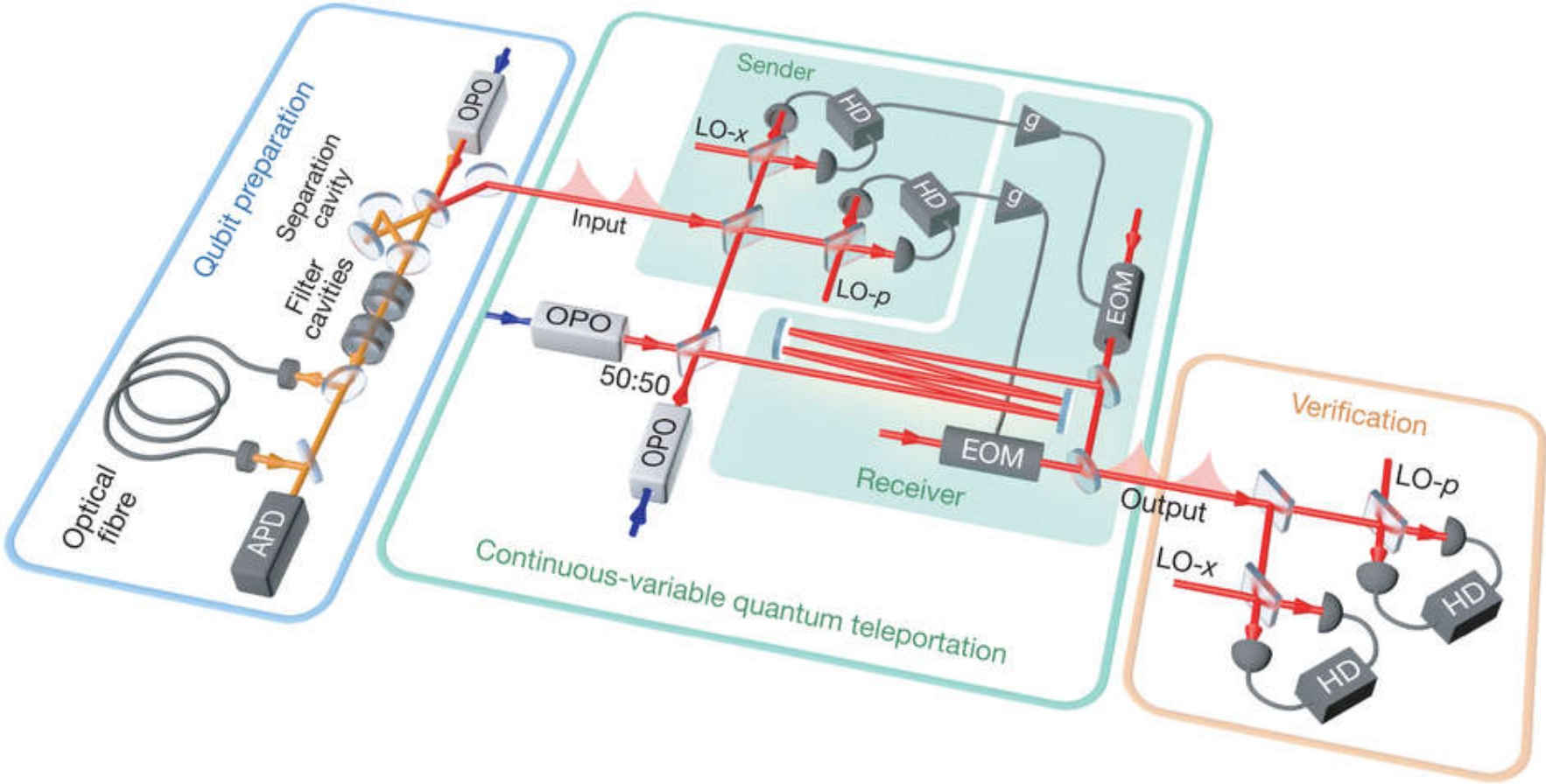
„D-Wave Systems Raises an Additional $29M, Closing 2014 Financing at $62M” (Jan 29, 2015)

ÖSSZEFONÓDÁS



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

ENTANGLEMENT


Qubit preparation
OPO
Separation cavity
Filter cavities
Optical fibre
APD
Sender
LO-x
HD
g
HD
g
Input
LO-p
OPO
50:50
OPO
EOM
EOM
Receiver
Continuous-variable quantum teleportation
Verification
Output
LO-p
LO-x
HD
HD

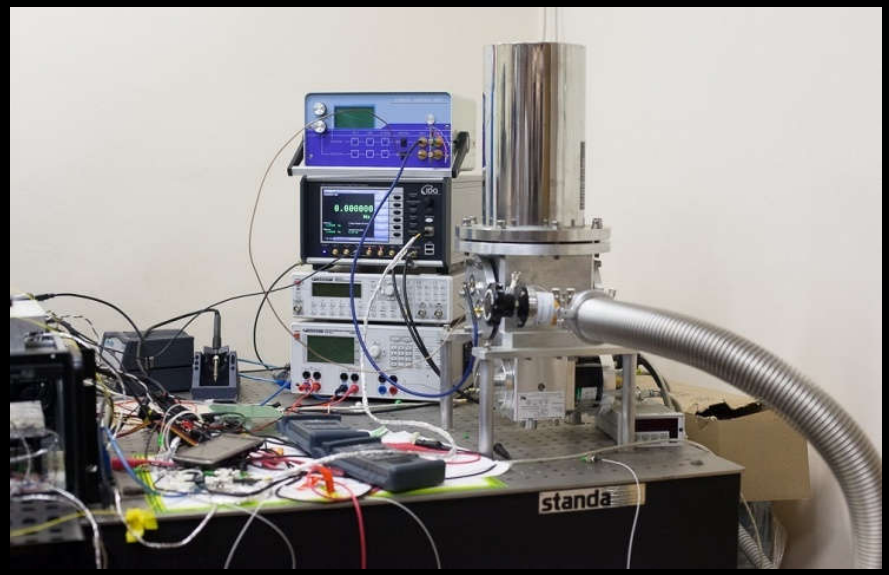
id Quantique

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

MagiQ

quintessence labs

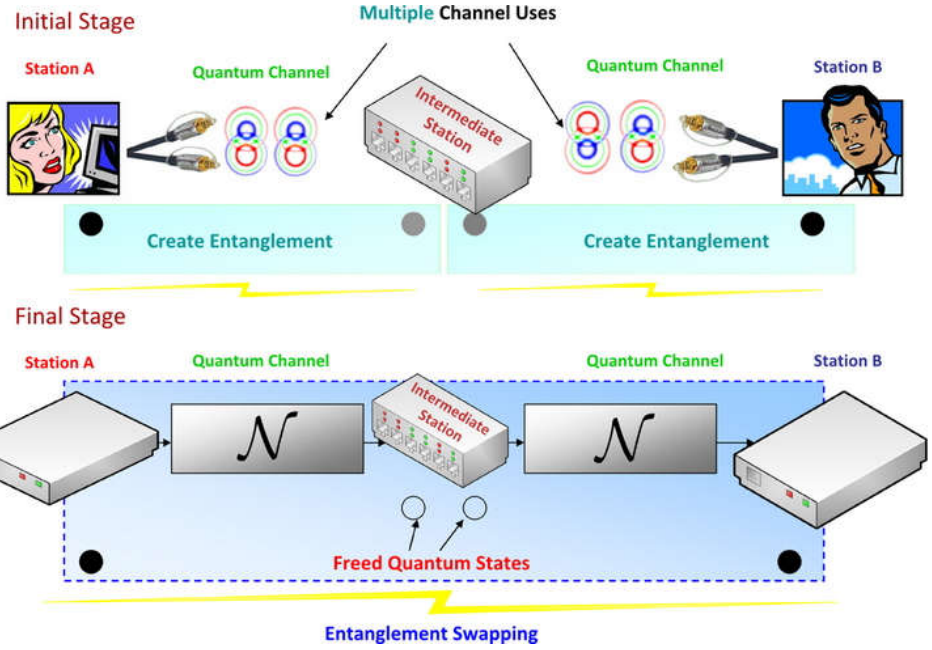
305

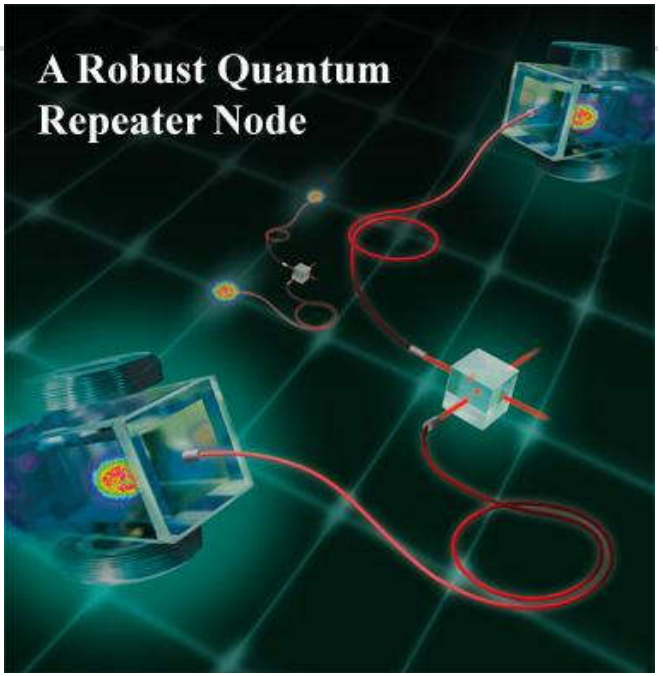


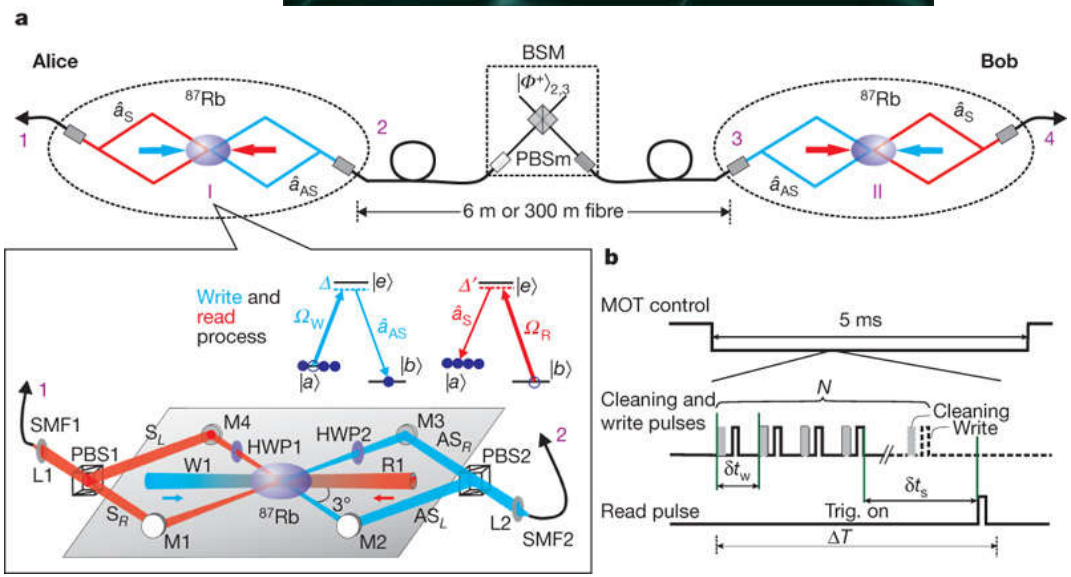
250

20

Kvantum repeater

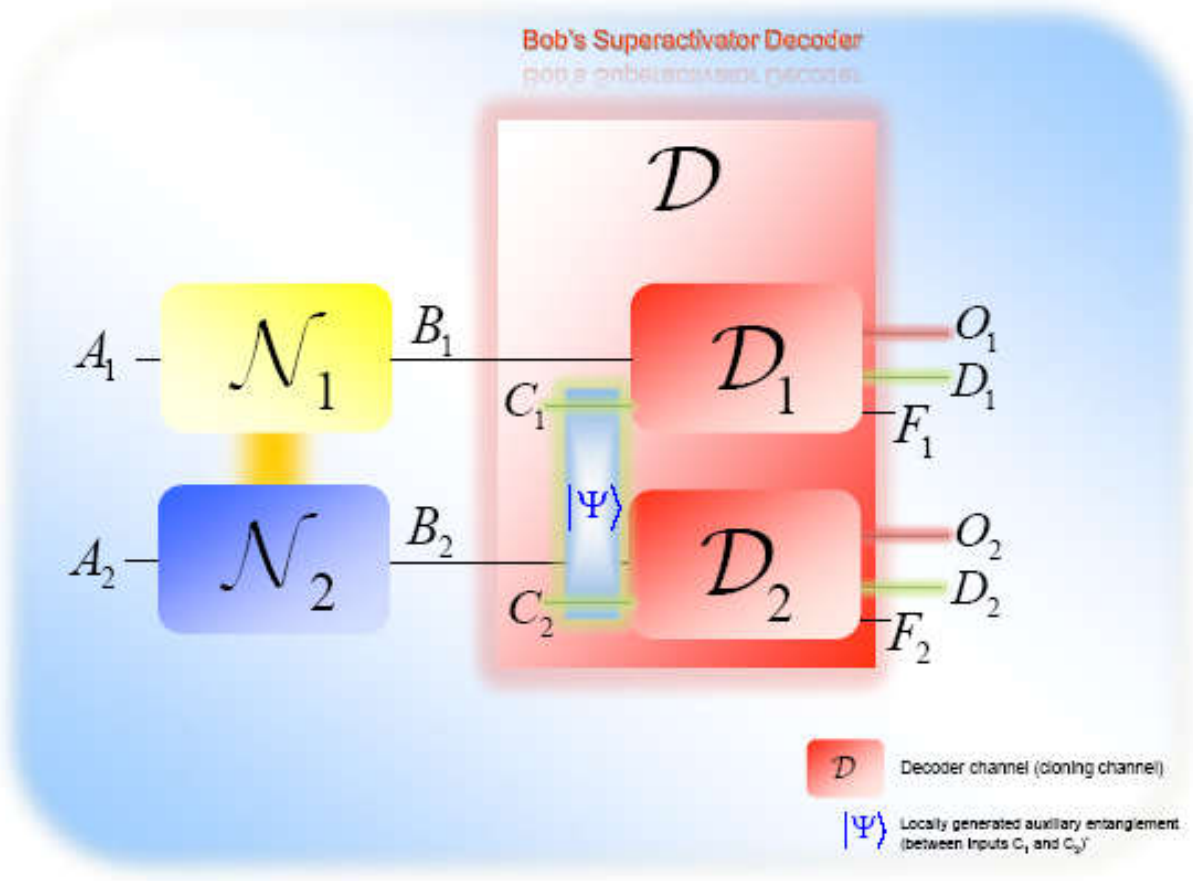






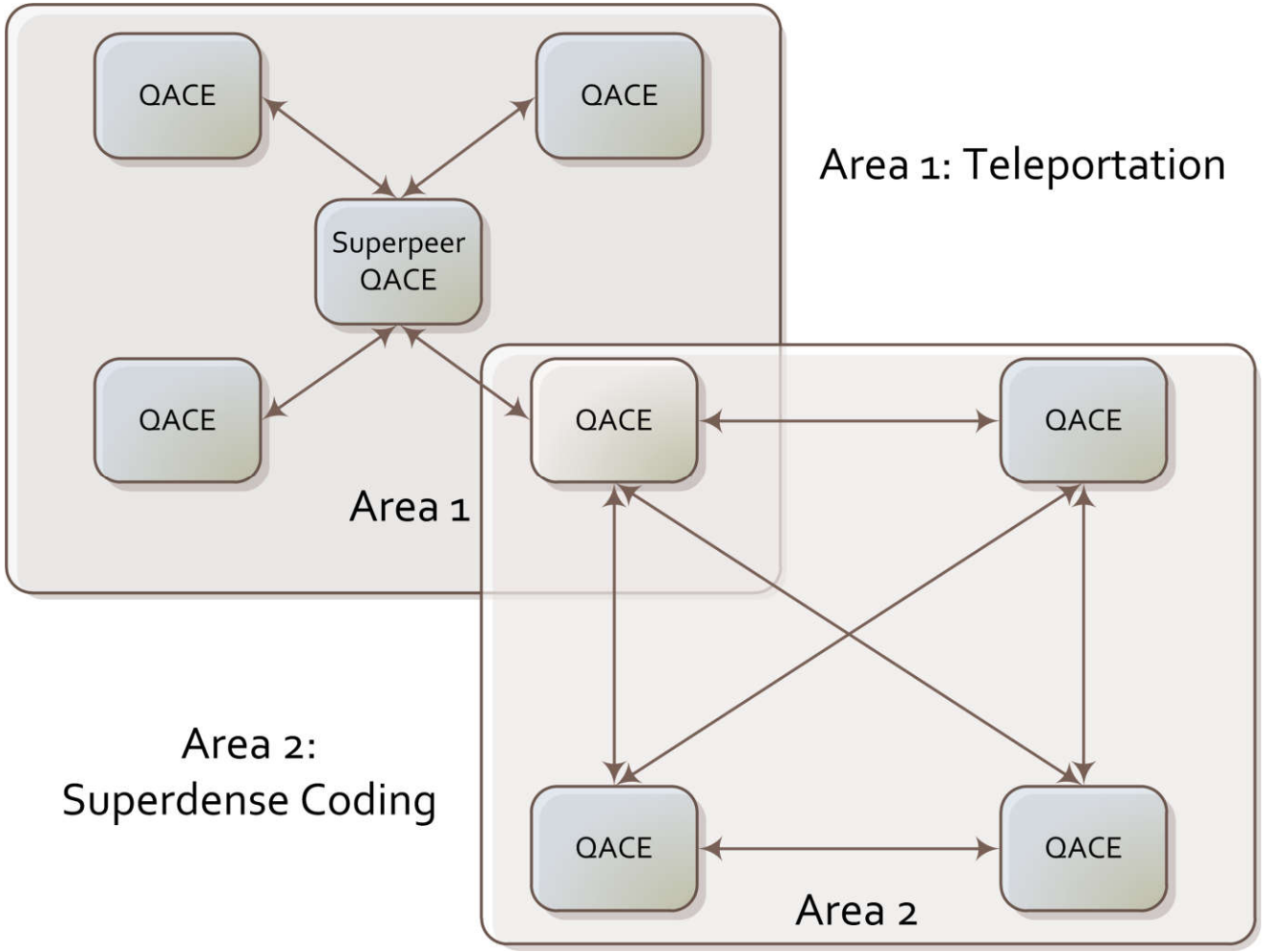
L. Gyongyosi, S. Imre, „Superactivated Quantum Repeaters”, Proc. of QIP2012, Montreal, Kanada, 2011.
Zhen-Sheng Yuan et al., „Experimental demonstration of a BDCZ quantum repeater node”, Nature 454, 1098-1101(28 August 2008)

Kvantum szuperaktiválás



L. Gyongyosi, S Imre, „Opening of Hidden Capacity-Domains of Quantum Channels", Proc. Of SPIE, 10: pp. 10-25. (2013)

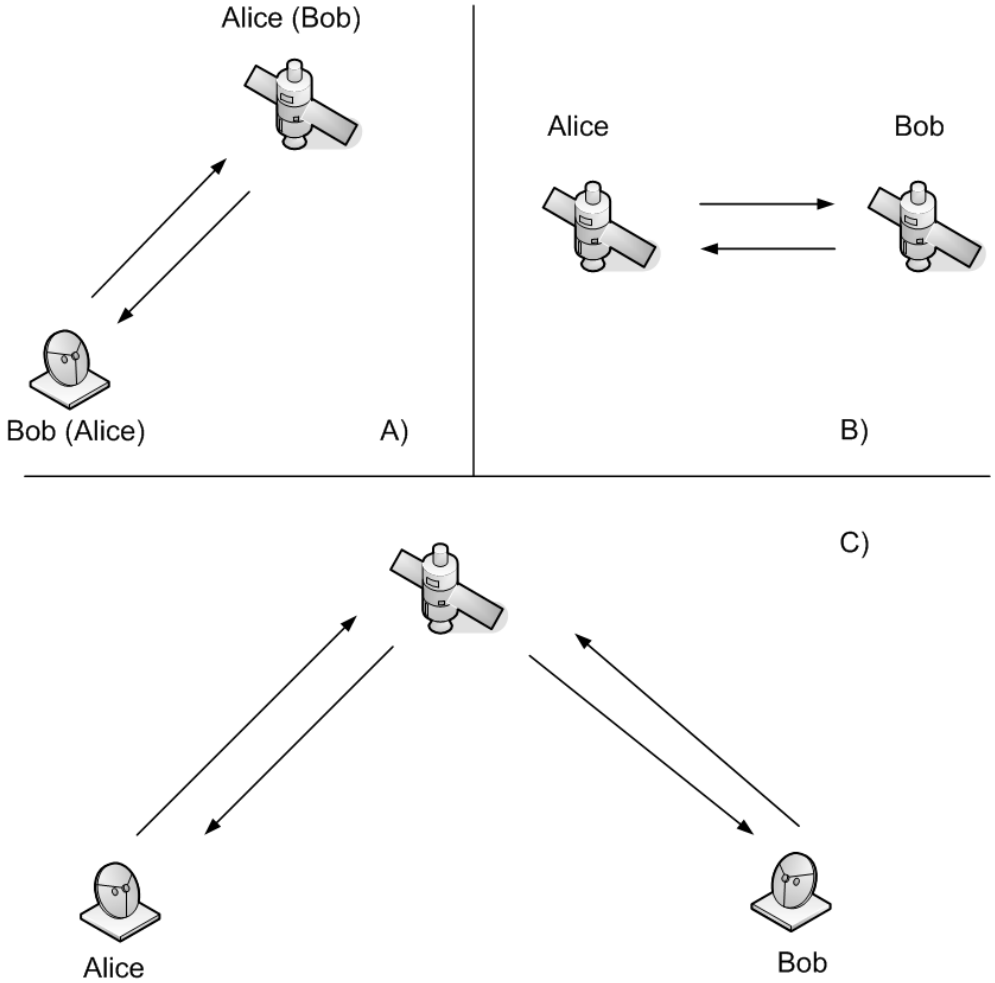
Kvantum ad-hoc hálózatok



L. Bacsardi, D. Banyai, S. Imre, „Analyzing Communication in Quantum Based Mobile Ad Hoc Networks”, AQIS'13 - Asian Quantum Information Science Conference. Chennai, India, 2013.08.25-2013.08.30. pp. 123-124.

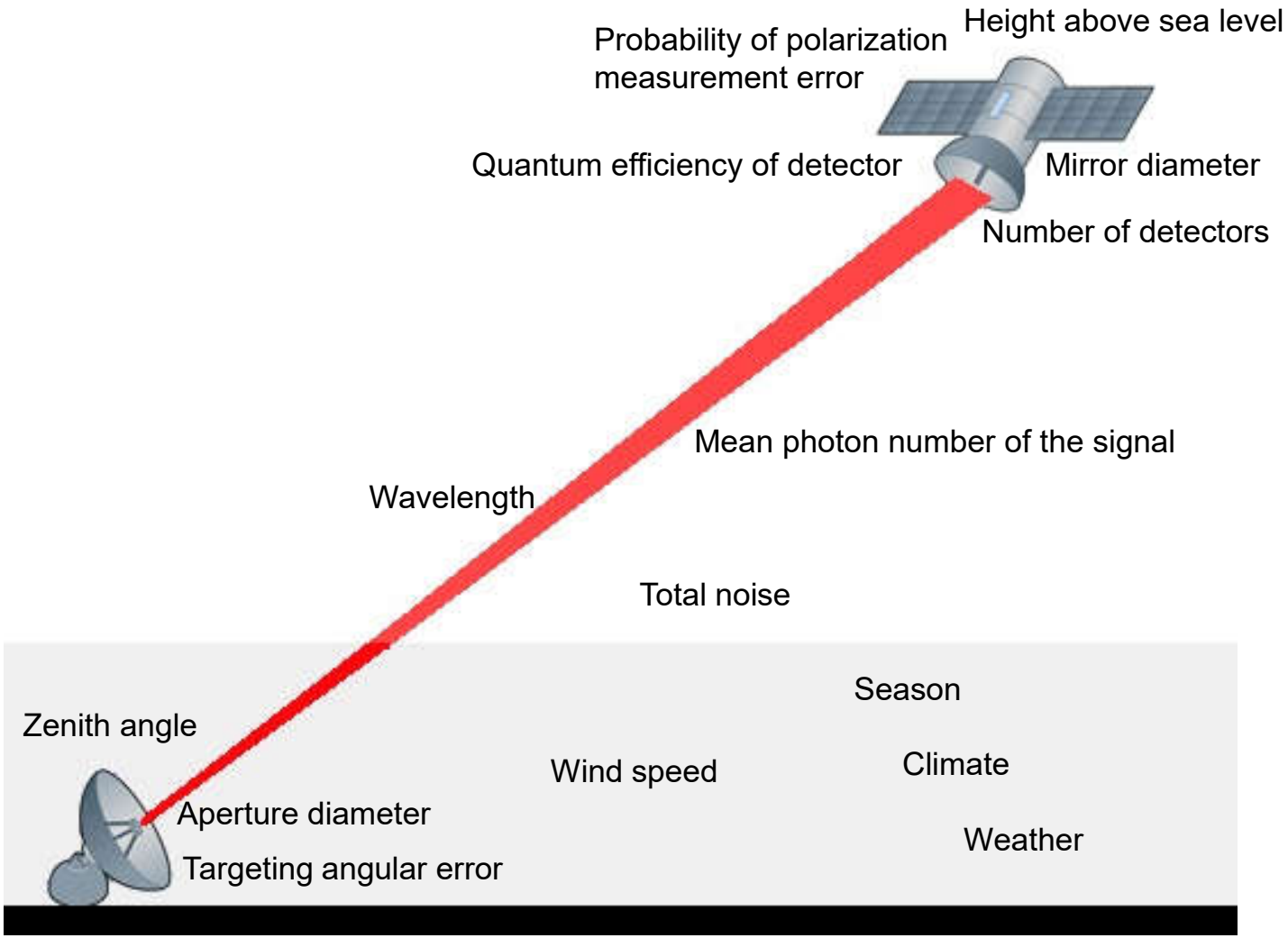
L. Bacsardi, „Quantum Based Solutions for Efficient Communication Networks”, IEEE 17th International Conference on Intelligent Engineering Systems, Monte de la Cruz, Costa Rica, 2013.06.19-2013.06.21. IEEE, pp. 45-49.

Irány az űr



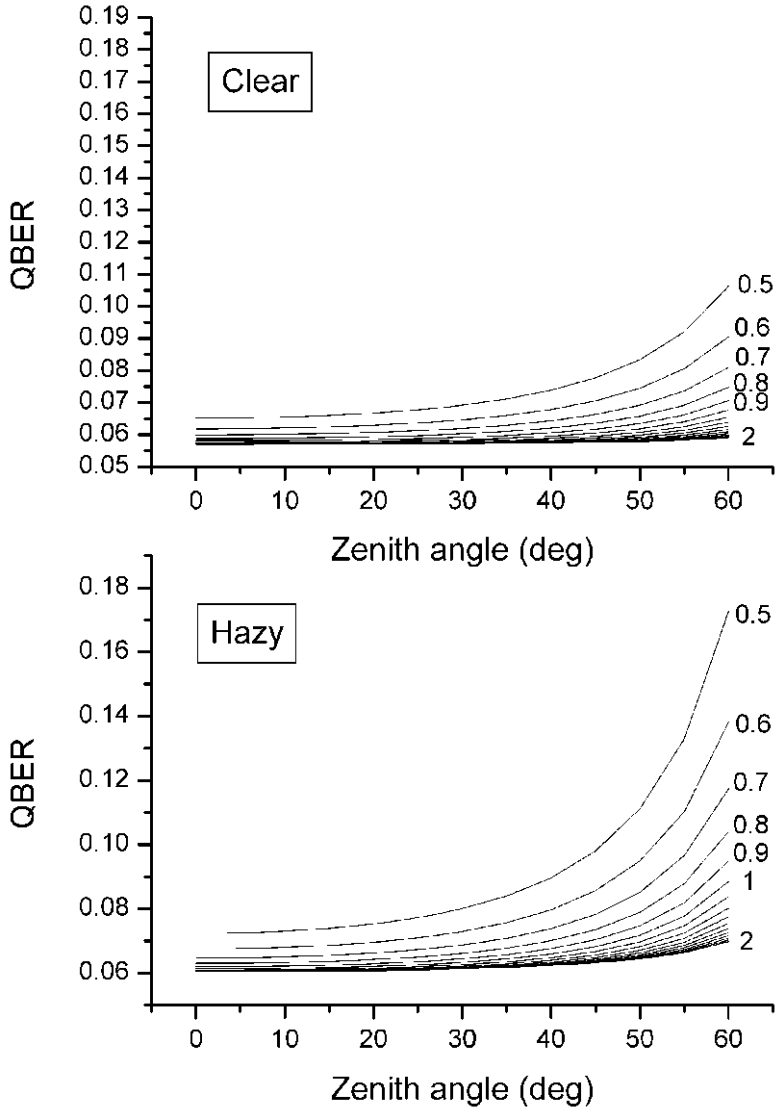
L. Bacsardi, „On the way to Quantum Based Satellite Communication”, IEEE Communications Magazine, 51:(08) pp. 50-55.

Irány az űr



L. Bacsardi and S. Imre, “Supporting Space Communications with Quantum Communications Links”, Global Space Exploration Conference. Washington D.C., USA, 2012, Paper 12300.

A BB84 protokoll vizsgálata



$$QBER = p_{pol} + \frac{p_{dark} \cdot n}{\tau \cdot \eta \cdot 2 \cdot \mu}$$

Mérsékelt égövi terület, nyár.
Műhold pályamagassága: 300 km
Tiszta idő: 23 km
Ködös idő: 5 km
Alice apertúra mérete: 0,2 m
P_{pol}=0.05;
P_{dark}=$2 \cdot 10^{-4}$;n=4; μ=0.1; η= 0.7

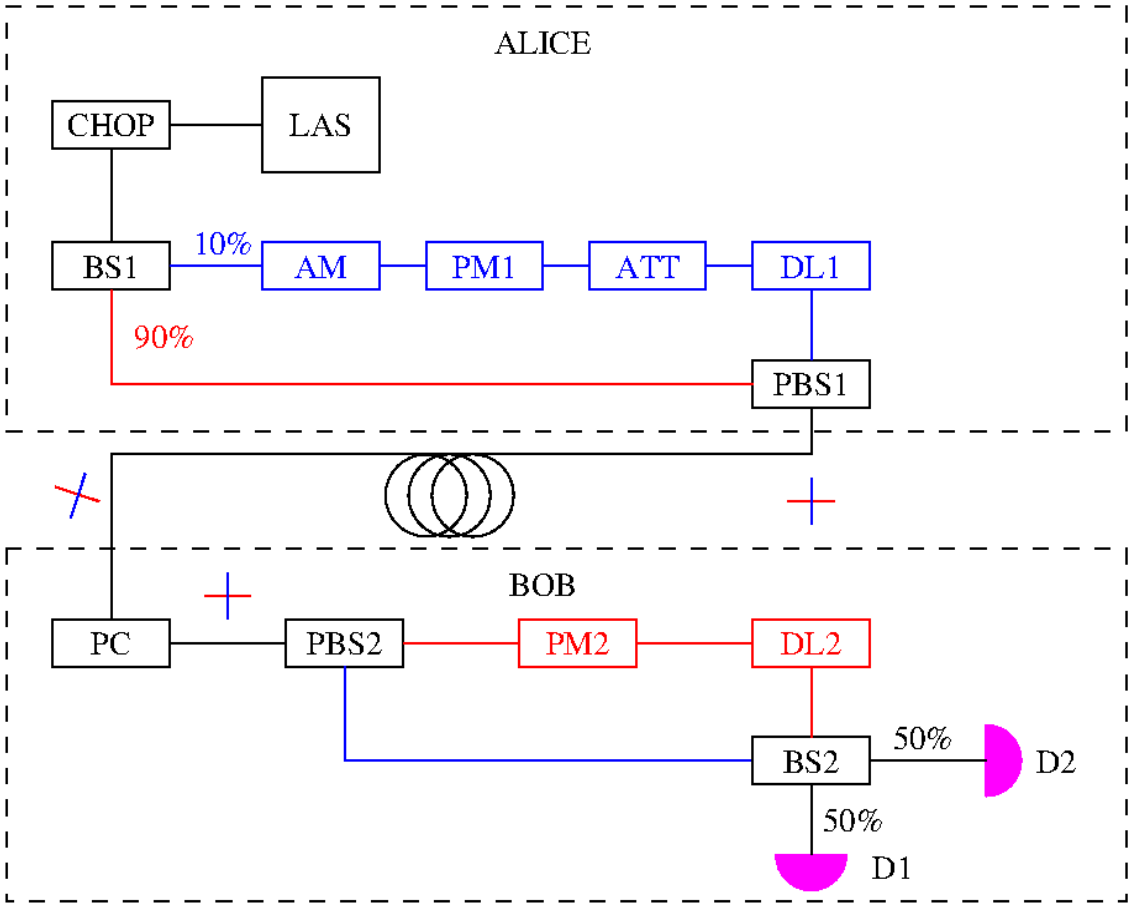
Kulcszétosztás itthon

Az első magyar, biztonságos kulcscserét megvalósító kvantumeszközök

Qrypt Solutions

Bacsárdi L, Belső Z, Bérces M, Gombkötő B, Gulácsi L, Gyöngyösi L, Imre S, Jahn K, Kis Zs, Koller I, Kornis J, Mazroe D, Mráz A, Orosz L, Paksy G, Papp Zs, Szabó Á, „Kísérletek folytonos változójú kvantumos kulcsmegosztó eszköz megvalósítására”
Kvantumelektronika 2014: VII. Szimpózium a hazai kvantumelektronikai kutatások eredményeiről. Budapest, Hungary, 2014

Kísérleti rendszer



$$\frac{1}{\sqrt{2}}\left|\text{bacsardi@inf.nyme.hu}\right\rangle+\frac{1}{\sqrt{2}}\left|\text{imre@hit.bme.hu}\right\rangle$$

KVANTUM ALAPÚ MEGOLDÁSOK VEZETÉKES ÉS VEZETÉK NÉLKÜLI HÁLÓZATOKBAN