Kvantum titkosítás

Modern fizikai kísérletek szeminárium
2015-2016 tavaszi félév

Dénes Gábor Oszkár

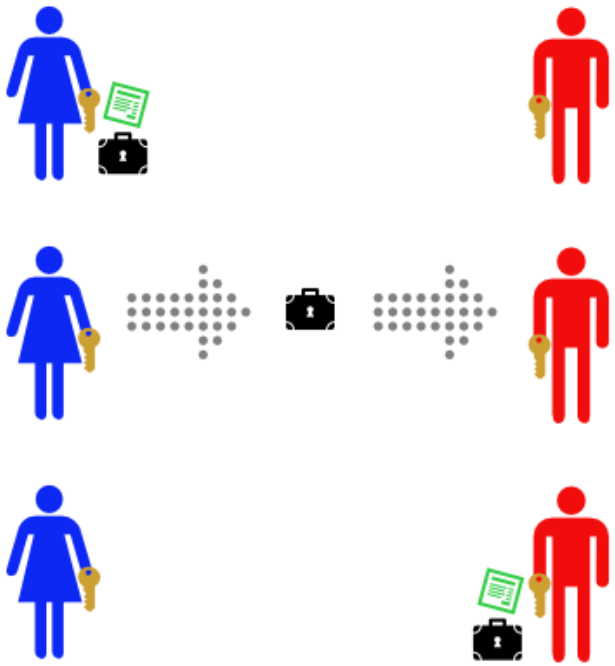
Eötvös Loránd Tudományegyetem

2016. március 8.

Tartalom

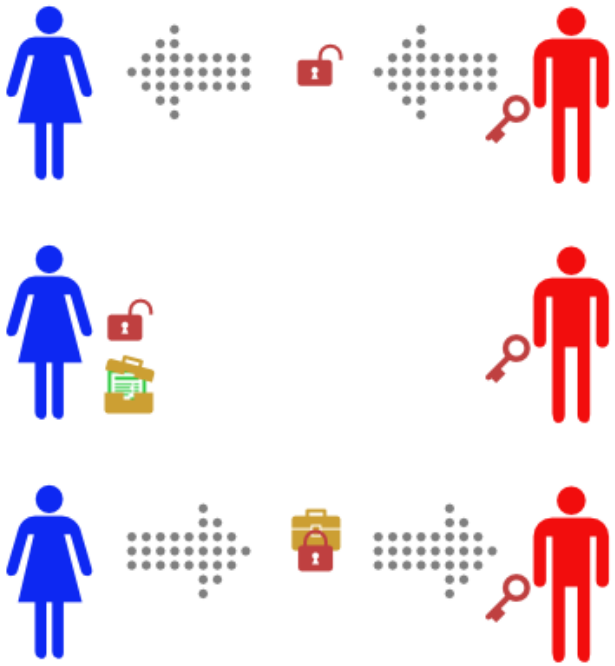
- Klasszikus titkosítás
  - Egyszerű módszerek
  - Problémái
- Kvantummechanika, elméleti bevezetés
- Quantum Key Distribution protokolok
  - Határozatlansági elven alapuló
  - Kvantum összefonódáson alapuló
- Kísérletek, gyakorlati megvalósítások
- Felhasználás, példák

Szimmetrikus titkosítás



- Alice (A) és Bob (B) ismeri a kulcsot.
- Ugyanazzal a kulccsal titkosítják és fejtik meg az üzenetet.
- Probléma: Hogyan tudatják egymással mi a titkos kulcs?

Aszimmetrikus titkosítás



- Bob csak a publikus kulcsot küldi el, a privát kulcs nála marad.
- Szétoszthatják egymás között a szimmetrikus kulcsot.

Klasszikus public key distribution

- Determinisztikus algoritmussal a nyílt kulcs kódolja az üzenetet.
- Egy **gyakorlatilag** kivitelezhetetlen algoritmus tudná visszafejteni.
- Titkos kulccsal egyszerű a visszafejtés.
- Két fő csoport:
  - Prímfelbontáson alapuló
  - Diszkrét logaritmus eljáráson alapuló

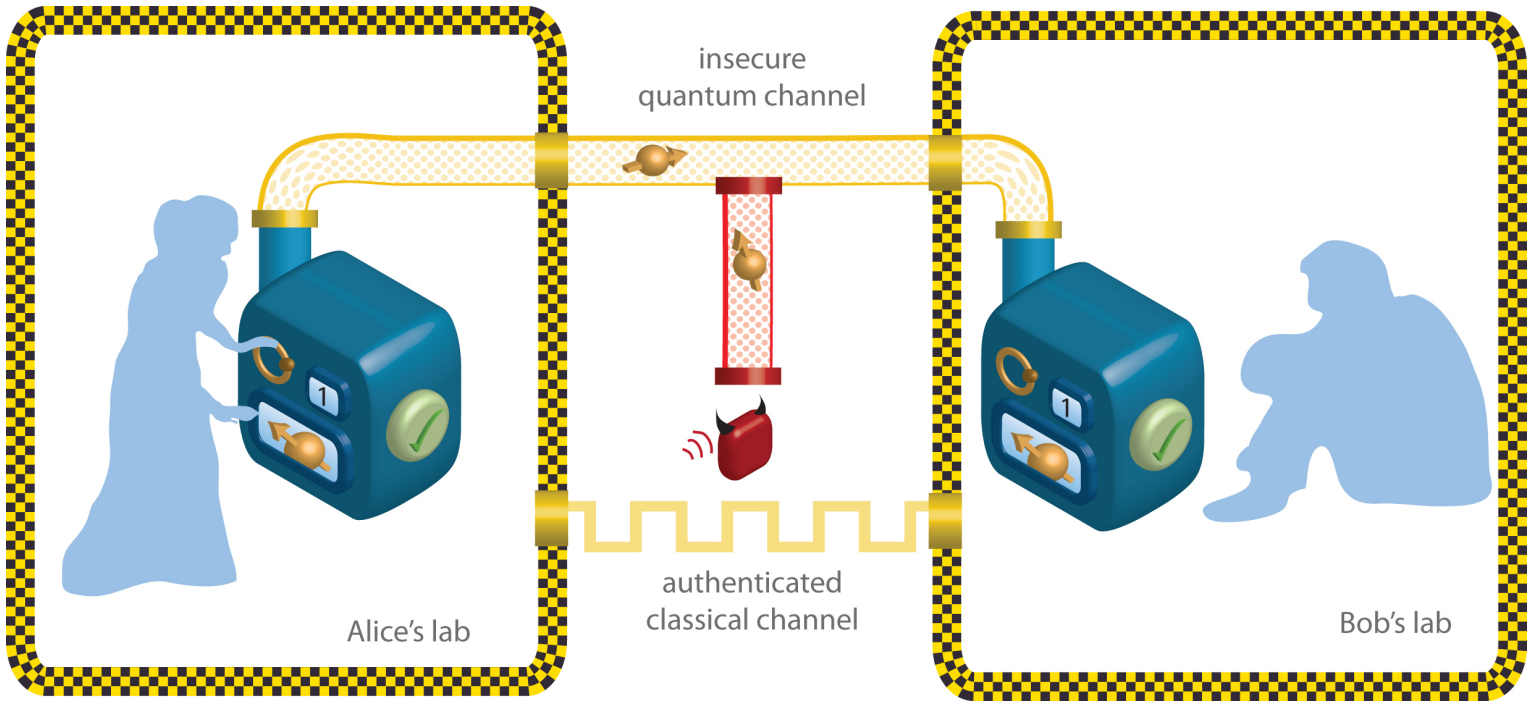
Prímfelbontáson alapuló eljárások problémája

- RSA algoritmus vázlata:
  1. Generálunk p, q prímszámokat.
  2. Publikus kulcs egyik eleme: $n = p \cdot q$.
  3. Titkos kulcs: $d = (p-1) \cdot (q-1)$.
- Felbontva n-t kitalálható d a titkos kulcs.
- 2009 december: RSA-768 (kb. 768 bites publikus kulcs) faktorizációja:
  - 2 évig tartott.
  - Megfelel 2000 évnyi számolásnak 2.2 GHz-es AMD Opteron processzoron.
- 2016-ban ajánlott legalább 2048 bites kulcs.

Prímfelbontáson alapuló eljárások problémája

- Problémák:
  - Mai legjobb prímfelbontó algoritmusok futásideje szám nagyságával exponenciálisan növekednek, de nem bizonyított, hogy nincs *elég gyors* algoritmus a prímfelbontásra.
  - Mindig növelni kell a kulcs méretét
  - Kvantumszámítógépekkel lehet polinomiális időben felbontani prímet.
    Eddigi legnagyobb prím, amit faktorizáltak, 2012-ben 56153.
  - Kvantumszámítógépek ha elterjednek, klasszikus algoritmusok könnyen feltörhetőek.
  - (Hasonló problémák más klasszikus aszimmetrikus kriptográfiára.)

Kvantumkriptográfia alapjai

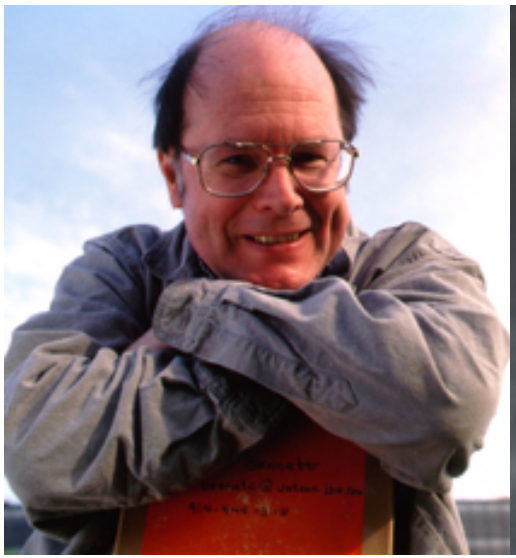


- Kvantumos csatornán osztják meg a kulcsot.
- Kvantumállapotot osztanak meg.
- Például egy foton, aminek a spinje az információ.

Határozatlansági elven alapuló eljárások

- Eljárás vázlata:
  - Kulcsot szeretnénk generálni, amit csak Alice és Bob ismerhet.
  - A teljes kulcs: bitek, fotonok mérésének eredménye.
  - Alice polarizált fotonokat küld véletlenszerű bázisokban. $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle, \ldots$
  - Bob méri a fotonokat véletlenszerű bázisokban.
  - Összes mérés után kijelentik milyen bázisokban mértek.
  - Ahol a bázisaik megegyeztek, azokból áll a kulcsuk.

BB84 protokol




- Charles Bennett, Gilles Brassard, 1984
- Első kvantumtitkosítási protokol

BB84 protokol

- Alice polarizált fotonokat küld.
- 2 féle bázisban kódolhatja 1-et és 0-t.
  - $(+)$ bázis:
    - 0: $|\rightarrow\rangle$
    - 1: $|\uparrow\rangle$
  - $(\times)$ bázis:
    - 0: $|\nearrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\rightarrow\rangle\right)$
    - 1: $|\nwarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\rightarrow\rangle\right)$
- Alice 4 állapotból összerakott sorozatot küld, pl.

Választott bázis	$+$	$+$	$\times$	$+$	$\times$	$\times$	$\times$	$+$
Küldött foton	$\uparrow$	$\rightarrow$	$\nwarrow$	$\uparrow$	$\nwarrow$	$\nearrow$	$\nearrow$	$\rightarrow$
Küldött bit	1	0	1	1	1	0	0	0

BB84 protokol

- Alice küld egy $|\psi\rangle$ állapotot.
- Bob 2 db mérőműszere:
  - $\hat{P}_+ = |\uparrow\rangle\langle\uparrow|$
    - Ha $|\psi\rangle = |\rightarrow\rangle$, akkor 0-t mér (nincs beütés a fotonszámlálón)
    - Ha $|\psi\rangle = |\uparrow\rangle$, akkor 1-t mér (van beütés a fotonszámlálón)
    - Ha $|\psi\rangle = |\nearrow\rangle$ vagy $|\nwarrow\rangle$ akkor 0-t vagy 1-t mér 50 % valószínűséggel.
  - $\hat{P}_\times = |\nwarrow\rangle\langle\nwarrow|$
    - Ha $|\psi\rangle = |\nearrow\rangle$, akkor 0-t mér (nincs beütés a fotonszámlálón)
    - Ha $|\psi\rangle = |\nwarrow\rangle$, akkor 1-t mér (van beütés a fotonszámlálón)
    - Ha $|\psi\rangle = |\rightarrow\rangle$ vagy $|\uparrow\rangle$ akkor 0-t vagy 1-t mér 50 % valószínűséggel.

BB84 protokol

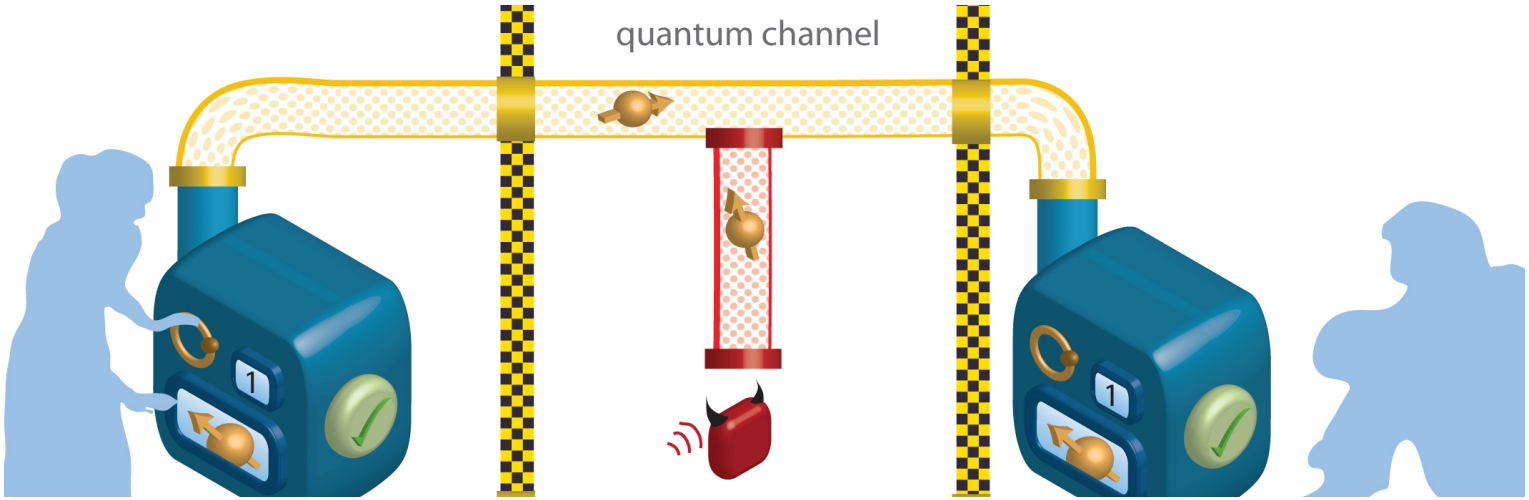
- Példa

Alice bázisa	+	+	×	+	×	×	×	+
Küldött foton	↑	→	↖	↑	↖	↗	↗	→
Bob bázisa	+	×	×	×	+	×	+	+
Bob mért értéke	1		1			0		0

- Alice és Bob nyílvánosan megosztja bázisait ezután.
- Ahol bázisaik megegyeznek, ott ugyanaz az érték.
- Az értékeket senki más nem tudhatja, csak a bázist.
- Ahol bázisaik megegyeznek, az lesz a kulcs!
- Titkos kulcs: 1100

BB84 protokol

- Lehallgathatja-e valaki őket?



- $|\psi\rangle$ valamelyik bázis sajátvektora, de nem lehet tudni melyiké!
- Ha véletlen rossz bázisban mérünk, információt vesztünk.
- Módszer lehetne:
  - Lemásoljuk az állapotot.
  - Miután Alice és Bob megmondják bázisaikat, megmérjük azt.

Nemklónozhatósági tétel

- Le lehet-e másolni kvantumállapotot?
- Többrészecskés kvantummechanika: tenzorszorzat tér.
- A másoló gép a következőt tegye:

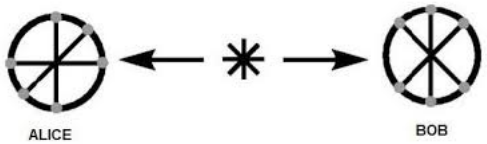
$$U : |\varphi\rangle \otimes |0\rangle \mapsto |\varphi\rangle \otimes |\varphi\rangle \,, \forall\, |\varphi\rangle \tag{1}$$

- Időfejlődés operátor unitér, ezért a gép unitér transzformációt végez.
- Bizonyítani lehet: nincs ilyen unitér transzformáció.

Kvantum összefonódáson alapuló eljárás
E91 protokol

- Artur Ekert, 1991

E91 protokol

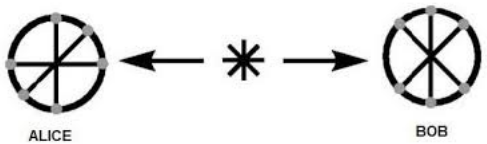


- Közös forrásból elektronokat küldünk Alicenak és Bobnak.

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle\right) \tag{2}$$

- Alice és Bob nem tudják előre mit fognak mérni, de tudják hogy a másik ellentétes spinvetületet mér, ha ugyanabban a bázisban mérünk.
- Legyenek bázisaink:
  $\phi_1^A = 0°, \phi_2^A = 45° \phi_3^A = 90°$ $\phi_1^B = 45°, \phi_2^B = 90° \phi_3^B = 135°$

E91 protokol

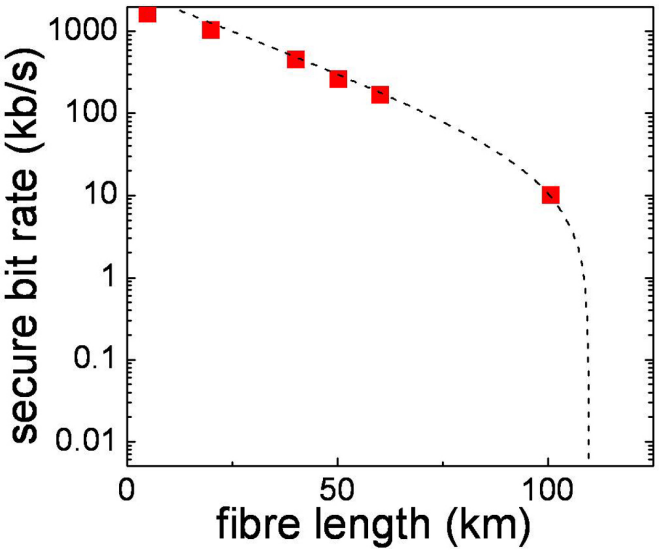


- Kulcskészítés:
  1. Véletlenszerűen választanak minden elektronspin mérésre egy bázist.
  2. Mérések végén megosztják bázisaikat.
  3. Ahol ugyanabban a bázisban mértek, az a kulcs értéke.
- 2/9 valószínűséggel választanak ugyanolyan bázist:
  az összes mérés 2/9-e lesz a teljes kulcs.

E91 protokol

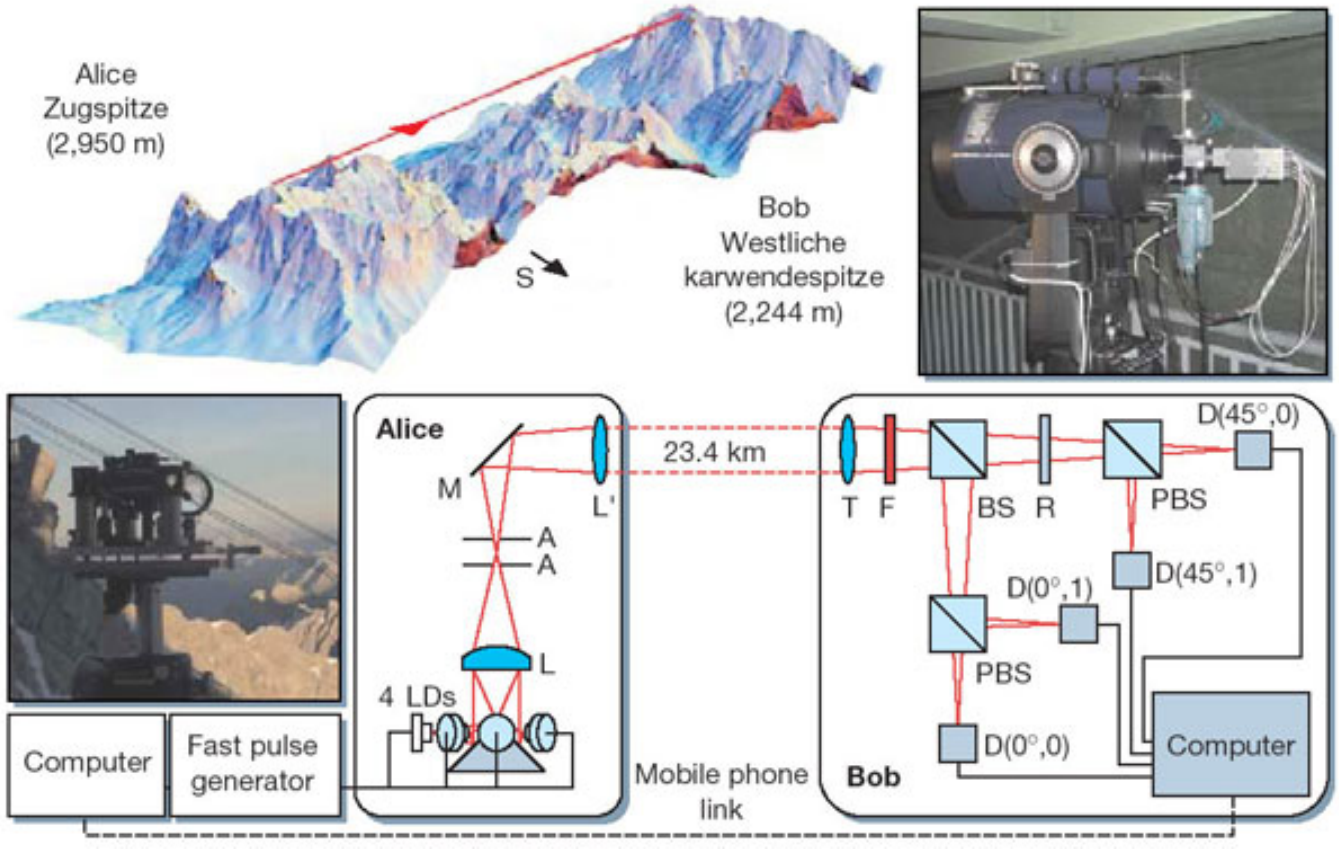
- Valaki megváltoztathatja Bob vagy Alice elektronjait.
- Így nem lesznek ugyanazok a kulcsok.
- Ellenőrzés:
  - Nem azonos bázisban mért elektronok korrelációját mérjük.
  - Ezek megoszthatók: nem a kulcs részei.
  - $E(a,b) = P_{++}(a,b) + P_{--}(a,b) + P_{+-}(a,b) + P_{-+}(a,b)$
  - $S = E(\phi_1^A, \phi_1^B) - E(\phi_1^A, \phi_3^B) + E(\phi_3^A, \phi_1^B) + E(\phi_3^A, \phi_3^B)$
  - $S = 2\sqrt{2}$, ha nincs lehallhatás (Bell egyenlőtlenségek).
  - $S \leq 2$, ha minden elektron lehallgatódott.
- BB84 protokolban ahhoz, hogy megtudjuk jók-e a kulcsok meg kell azokat osztani részben.

Kísérletek:
2008, Toshiba, University of Cambridge



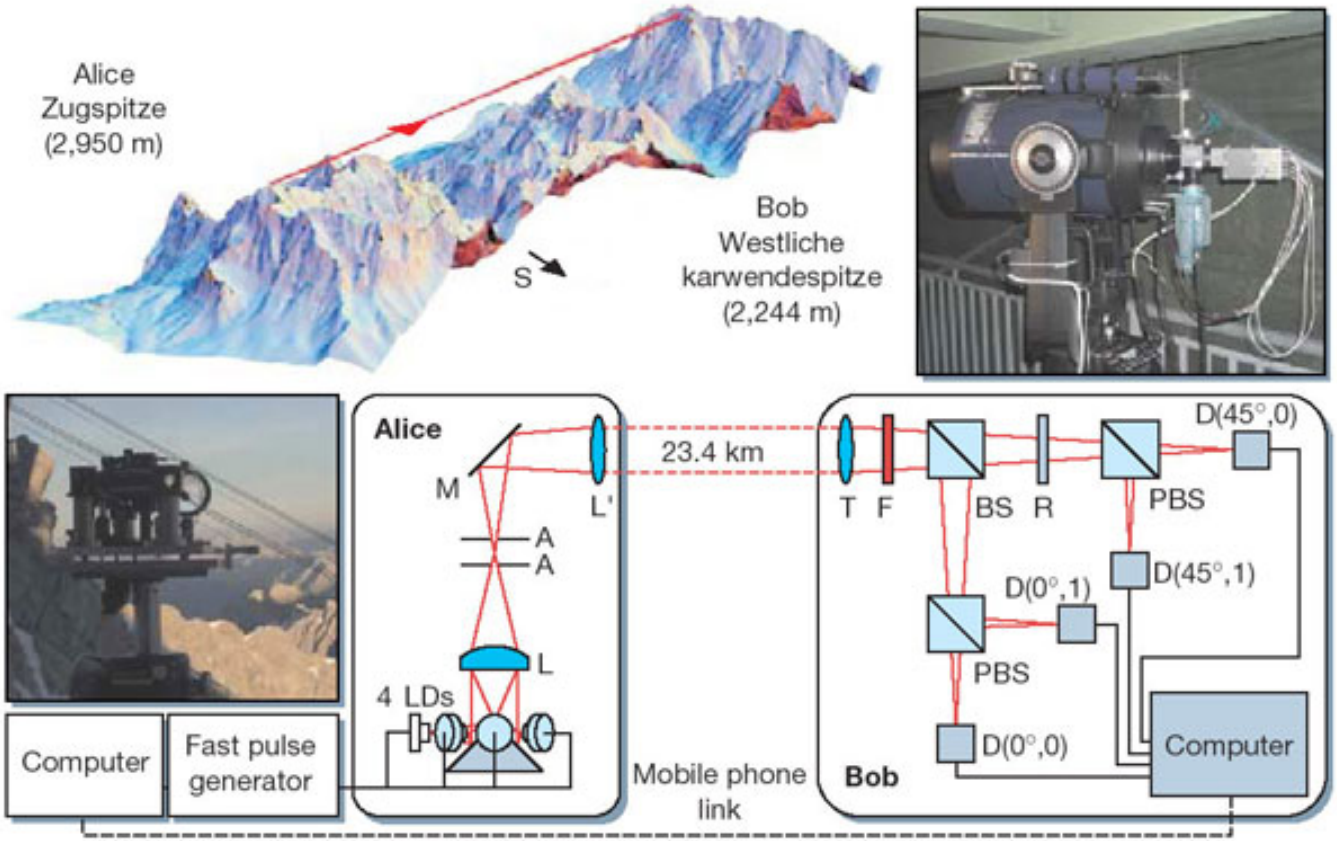
- BB84 módosított változatát használták.
- Leggyorsabb adatátvitel titkos kulcsokra: 1 Mbit/s: 20 km optikai szálon, 10 kbit/s: 100 km-en.
- Fotonokat InGaAs Avalanche Photo Diode (APD) mérték
  Sok idő kell amíg újra használhatóak: nagy "dead-time",
  ez limitálja az adatsebességet.

Kísérletek:
Kurtsiefer, 2002, A step towards global key distribution



- Ausztria, 23.4 km szabad optikai út
- BB84 módosított változata

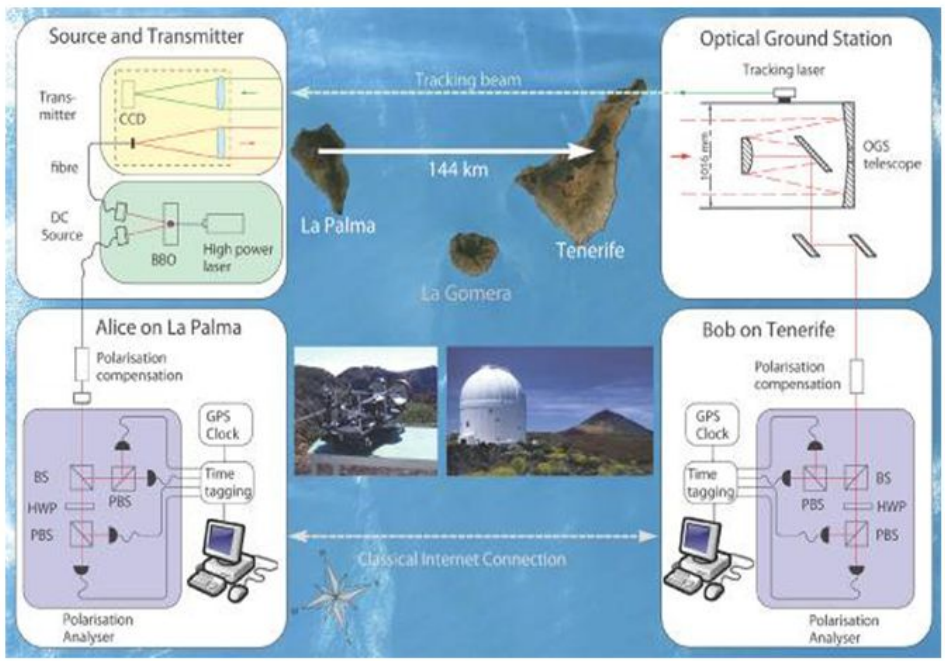
Kísérletek:
Kurtsiefer, 2002, A step towards global key distribution



- 18-20 dB veszteség
- 1.5-2 kbit/s
- Földközeli keringésű műhold kulcstovábbításhoz majdnem jó.

Kísérlet:
Kanári szigeteki kvantum összefonodás kísérlet, 2006

Entanglement over 144km free-space

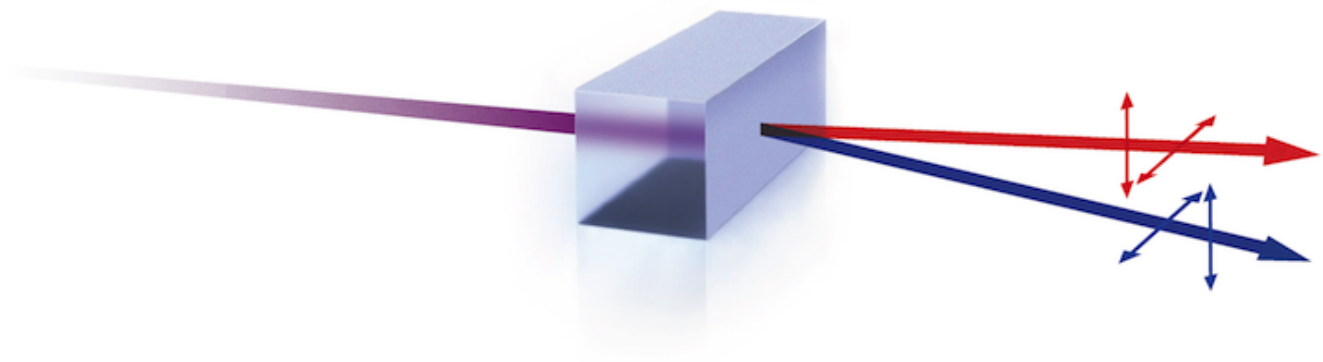


In collaboration with:

Free-Space distribution of entanglement and single photons over 144 km,
R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, A. Zeilinger, submitted

Kísérlet:
Kanári szigeteki kvantum összefonodás kísérlet, 2006

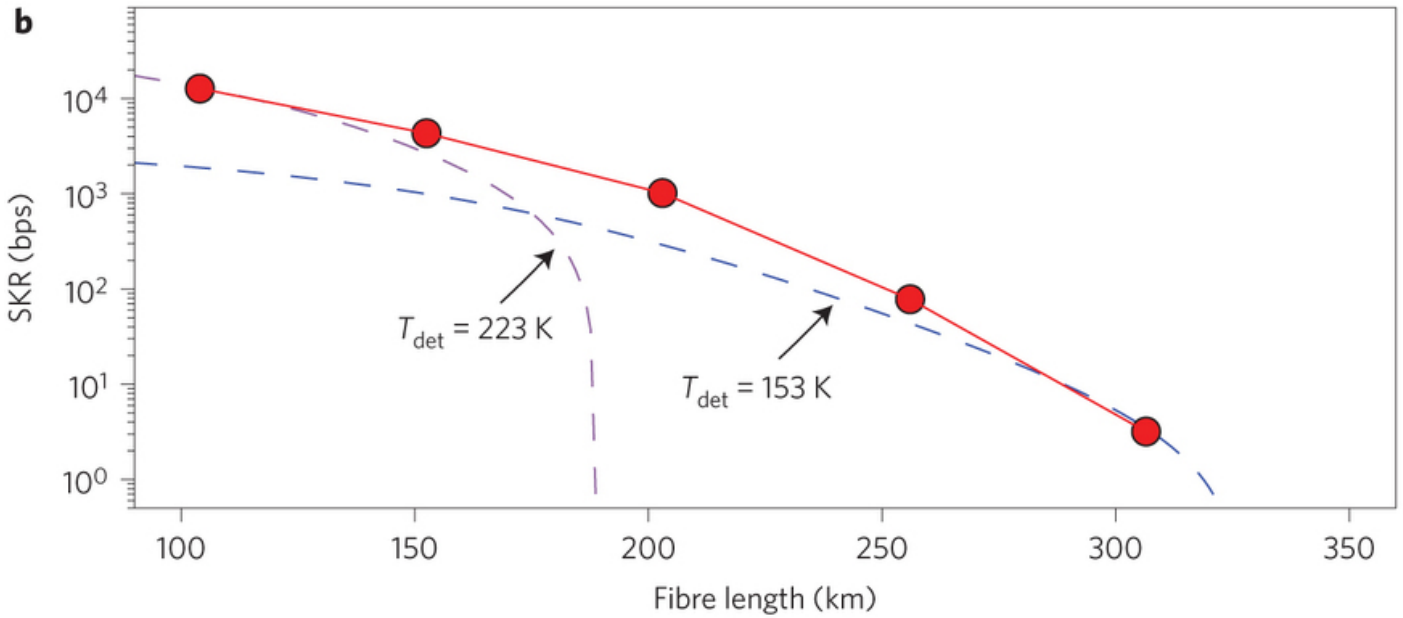
- 144 km, szabad optikai út
- 355 nm hullámhosszú lézer
- Összefonódott fotonokat küldtek: $\frac{1}{\sqrt{2}}\left(|H\rangle_A |V\rangle_B - |V\rangle_A |H\rangle_B\right)$
- Beta Barium Borate (BBO) nemlineáris kristályt használtak.



Kísérlet:
Kanári szigeteki kvantum összefonodás kísérlet, 2006

- 75 s alatt 178 bites kulcsot küldtek.
- Mért $S \approx 2.508$ ($2\sqrt{2} \approx 2.828$).
- kb. 30 dB veszteség
- Low Earth Orbit műholdak - Föld között kb. 1 nagysegrenddel nagyobb lenne a veszteség

Kísérlet: University of Geneva, 2015



- Leghosszabb út: 307 km, University of Geneva, 2015 (COW protokol).
- 307 km-en 3.2 kbit/s

Üzleti felhasználás

- QKD-t nyújtó vállalatok: ID Quantique, MagicQ Technologies, QuintessenceLabs, SeQureNet

Felhasználás

- 2004, Bécs, első banki transzfer.
- 2007, Svájcban népszavazáshoz először használtak adatovábbításra
- DARPA 2004 óta 10 csomópontos quantum key distribution network
- Los Alamos Nation Laboratory: QKD network, de van központi hub
- 2008 óta EU Quantum Cryptography network: SECOQC (Secure Communication Based on Quantum Cryptography)
- Kvantum titkosított rendszerek ma még nagyon kevés helyen használatosak, ezek szinte mind kísérleti jellegűek.

Források

- Bob és Alice grafika: https://wordtothewise.com/2014/09/cryptography-alice-bob/
- Diszkrét logaritmus eljárás: https://en.wikipedia.org/wiki/Discrete_logarithm
- RSA algoritmus: https://en.wikipedia.org/wiki/RSA_%28cryptosystem%29
- RSA-768 faktorizáció: https://en.wikipedia.org/wiki/RSA_numbers#RSA-768
- Prímfaktorizáció kvantumszámítógéppel: https://en.wikipedia.org/wiki/Shor%27s_algorithm
- Kvantumos Alice és Bob grafika: http://www.proselex.net/Pages/SecretCommunication.aspx
- QKD: https://en.wikipedia.org/wiki/Quantum_key_distribution
- BB84: https://en.wikipedia.org/wiki/BB84
- Benedikt Mihály jegyzete: http://titan.physx.u-szeged.hu/~benedict/KvinfJ04.pdf
- Bennet kép: http://www.cs.bu.edu/new-CS-web/content/research/colloquium/10-Bennett.shtml
- Brassard kép: http://www.iro.umontreal.ca/~brassard/
- Nemklónozhatósági tétel: https://en.wikipedia.org/wiki/No-cloning_theorem
- Artur Ekert: https://en.wikipedia.org/wiki/Artur_Ekert
- E91 protokol: http://physweb.bgu.ac.il/COURSES/QuantumMechCohen/Contributions/yoav.pdf
- E91 protokol: http://www.ux1.eiu.edu/~nilic/Nina%27s-article.pdf

Források

- Toshiba kísérlet: http://spie.org/newsroom/technical-articles-archive/1519-record-quantum-cryptography-bit-rate-enables-ultrasecure-fiber-networks?ArticleID=x34398
- Toshiba kísérlet arxiv: http://arxiv.org/pdf/0810.1069.pdf
- Kurtsiefert, A step towards global key distribution: http://www.nature.com/nature/journal/v419/n6906/abs/419450a.html
- Kurtsiefert, A step towards global key distribution: http://xqp.physik.uni-muenchen.de/publications/files/articles_2002/nature_419_450.pdf
- Kanári szigeteki kísérlet: http://lanl.arxiv.org/pdf/quant-ph/0607182v2
- Spontaneous parametric down-conversion: https://en.wikipedia.org/wiki/Spontaneous_parametric_down-conversion
- BBO kristály: http://nautil.us/issue/2/uncertainty/the-rise-of-the-uncertain
- Leghosszabb QKD: http://arxiv.org/pdf/1407.7427v1.pdf

Vége.