



BME
PHYSICS



Kvantumkommunikációs fejlesztések a HunQuTech projektben

Imre Sándor - Gerhátné Udvary Eszter -
Kis Zsolt - Koller István



NEMZETI KUTATÁSI, FEJLESZTÉSI
ÉS INNOVÁCIÓS HIVATAL

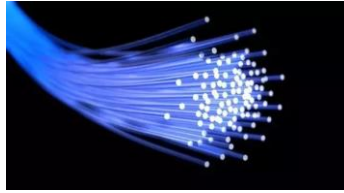
AZ INNOVÁCIÓ LENDÜLETE

AZ NKFI ALAPBÓL
MEGVALÓSULÓ
PROJEKT

Kvantum kommunikációs áttekintés

- **CVQKD**

- Kiss Zsolt
- Gódor Győző
- Ericsson
 - Kovács Bence
 - Suskovics Péter
 - Ladvánszky János



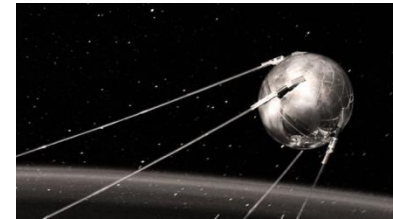
- **QRNG**

- Gerhátné Dr. Udvary Eszter
- Schranz Ágoston
- Bacsárdi László
- Matolcsy Balázs



- **Free Space QKD**

- Koller István
- Kiss Zsolt
- id. Fortágh József
- Galambos Máté
- Zsolczai Viktor
- Bonn Hungary



- **Klasszikus vezérlés**

- Belső Zoltán
- Jánosi Gergely
- Jókai Sándor
- Koller István

- **Kulcs előállítás**

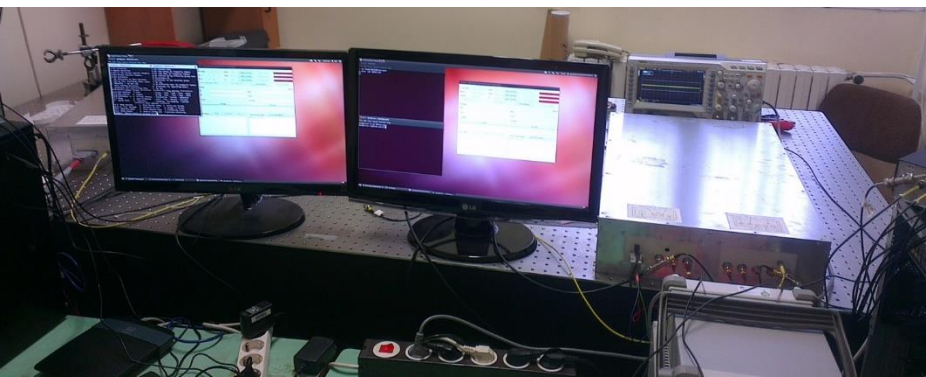
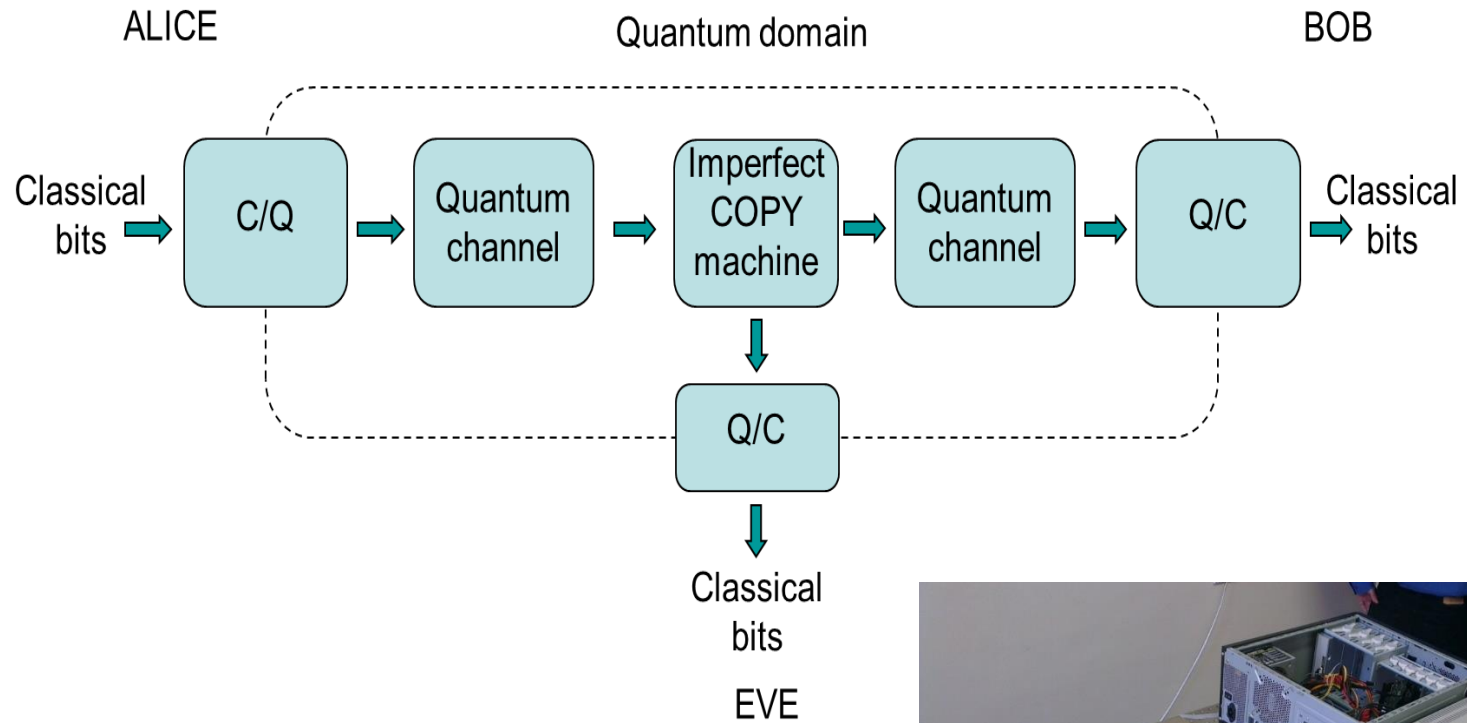
- Imre Sándor
- Bacsárdi László
- Gyöngyösi László

- **Fizikai Intézet**

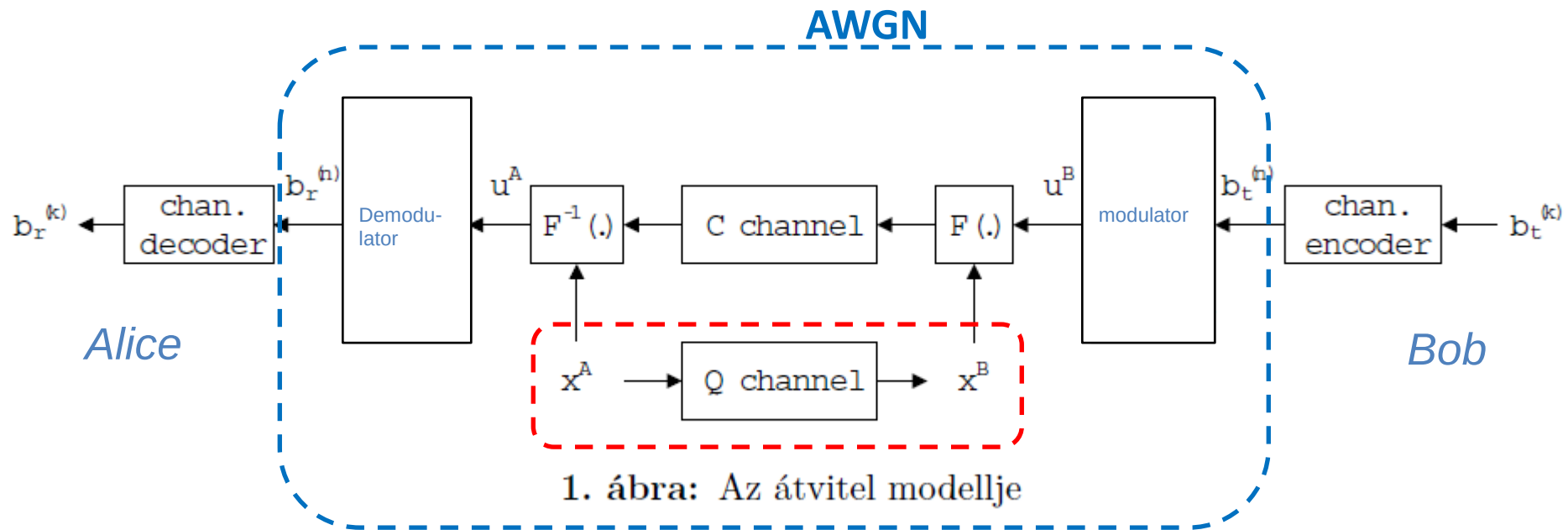
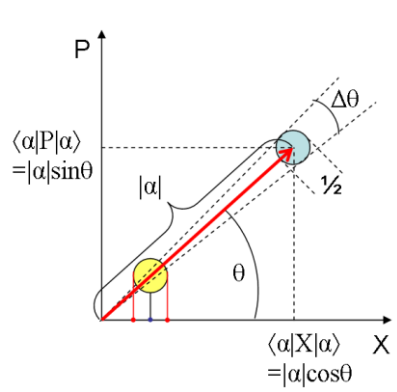
- Koppa Pál
- Kornis János
- Papp Zsolt
- Szabó Áron

10+ hallgató

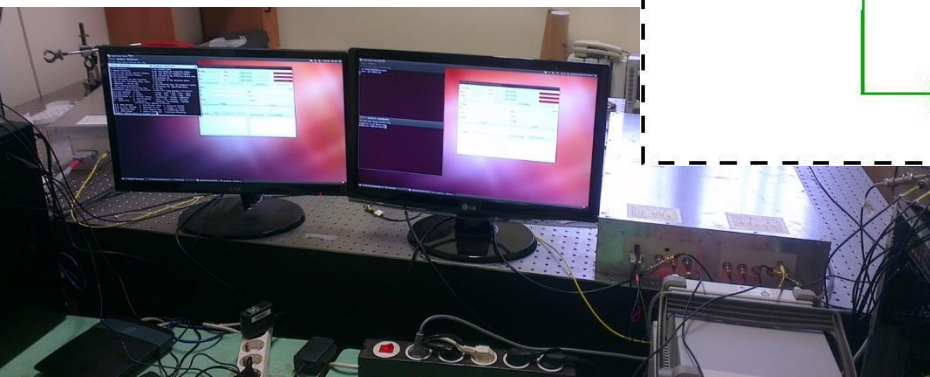
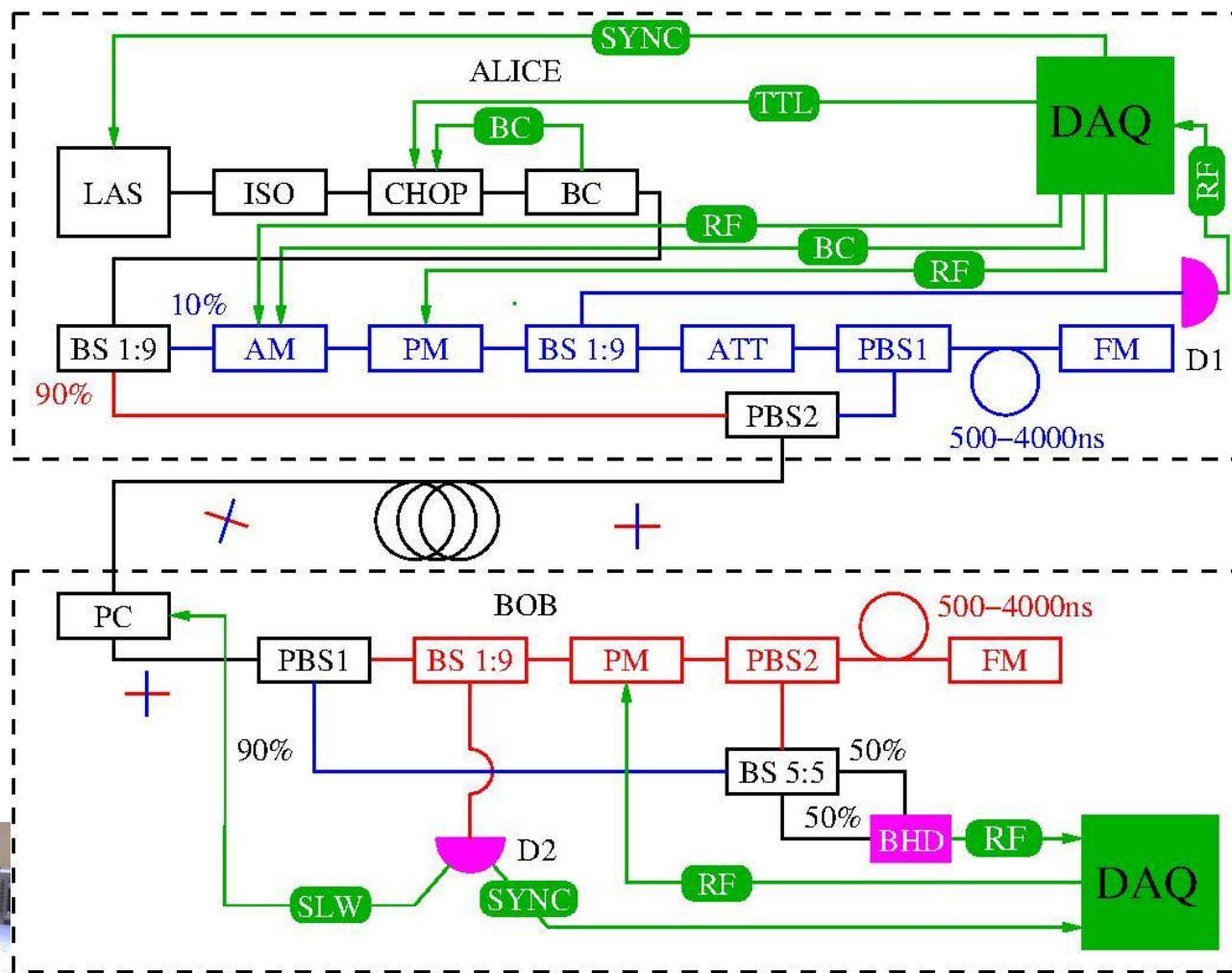
QKD elv



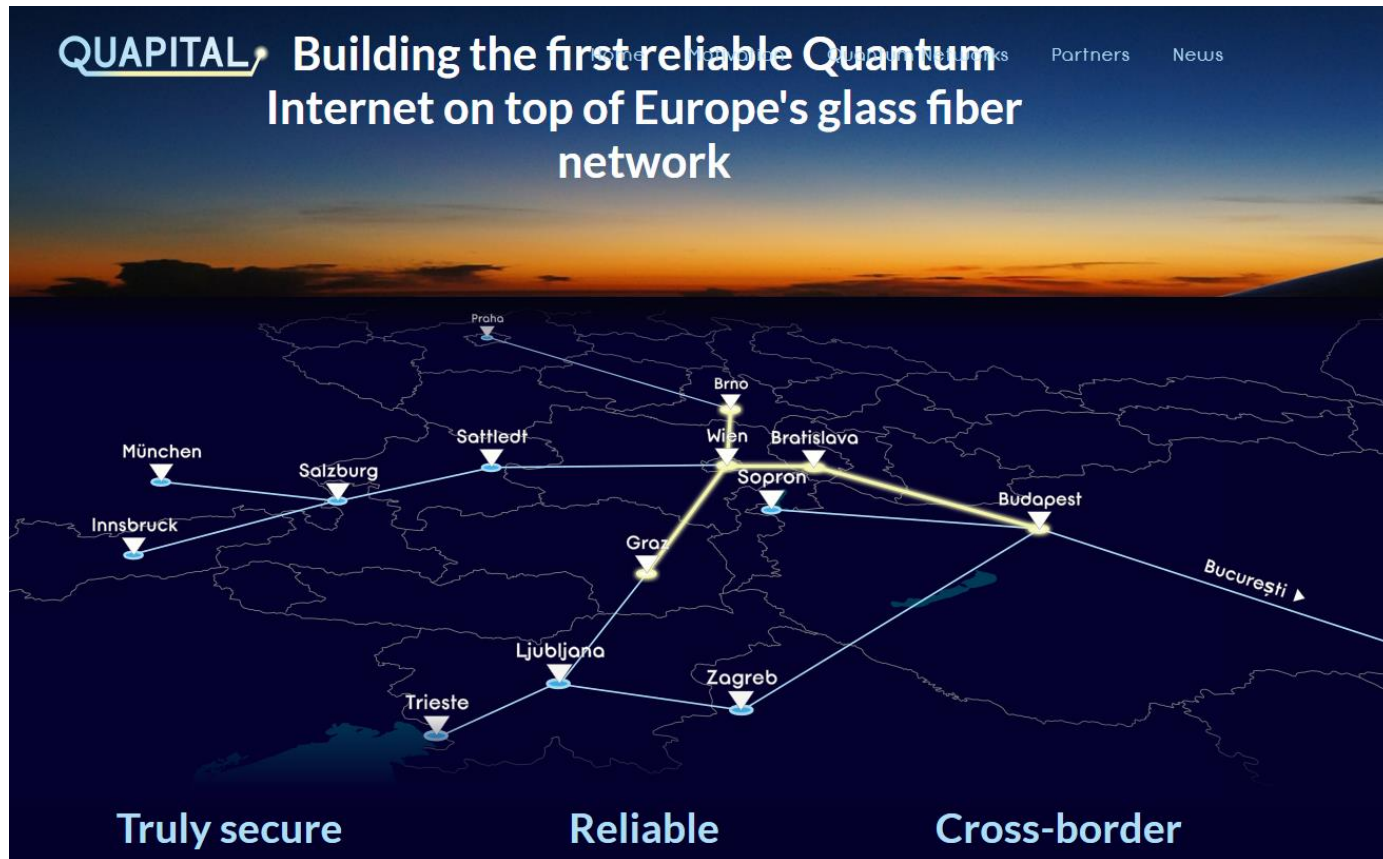
CVQKD architektúra



CVQKD fizikai réteg rendszerterv



QUAPITAL



QUAPITAL will be the first Quantum Internet to achieve truly quantum secure connections over hundreds of kilometers 24 hours a day, 7 days a week, 365 days a year.

Free Space - rendszer

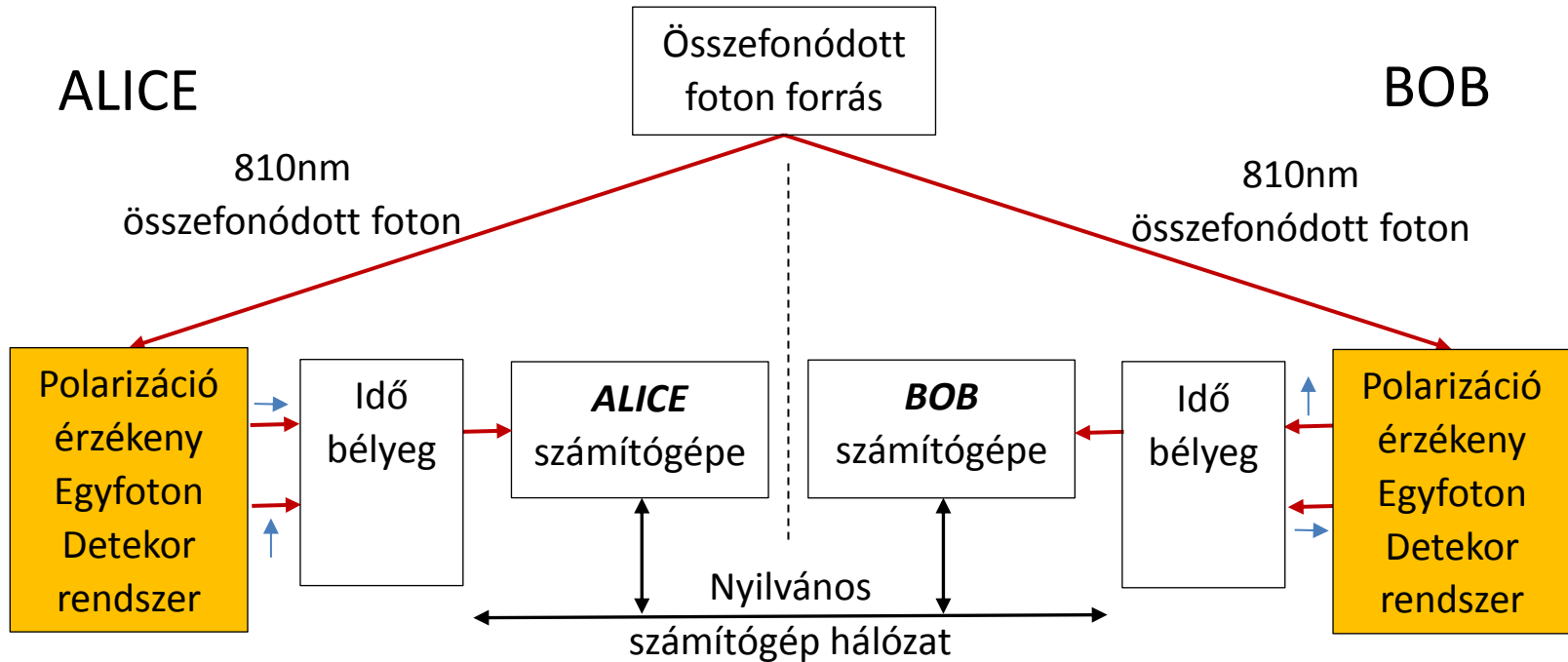
Koller István

Free Space QKD

Motiváció: *vezeték nélküli*
biztonságos titkosító kulcs szétosztása
két partner (ALICE, BOB) között

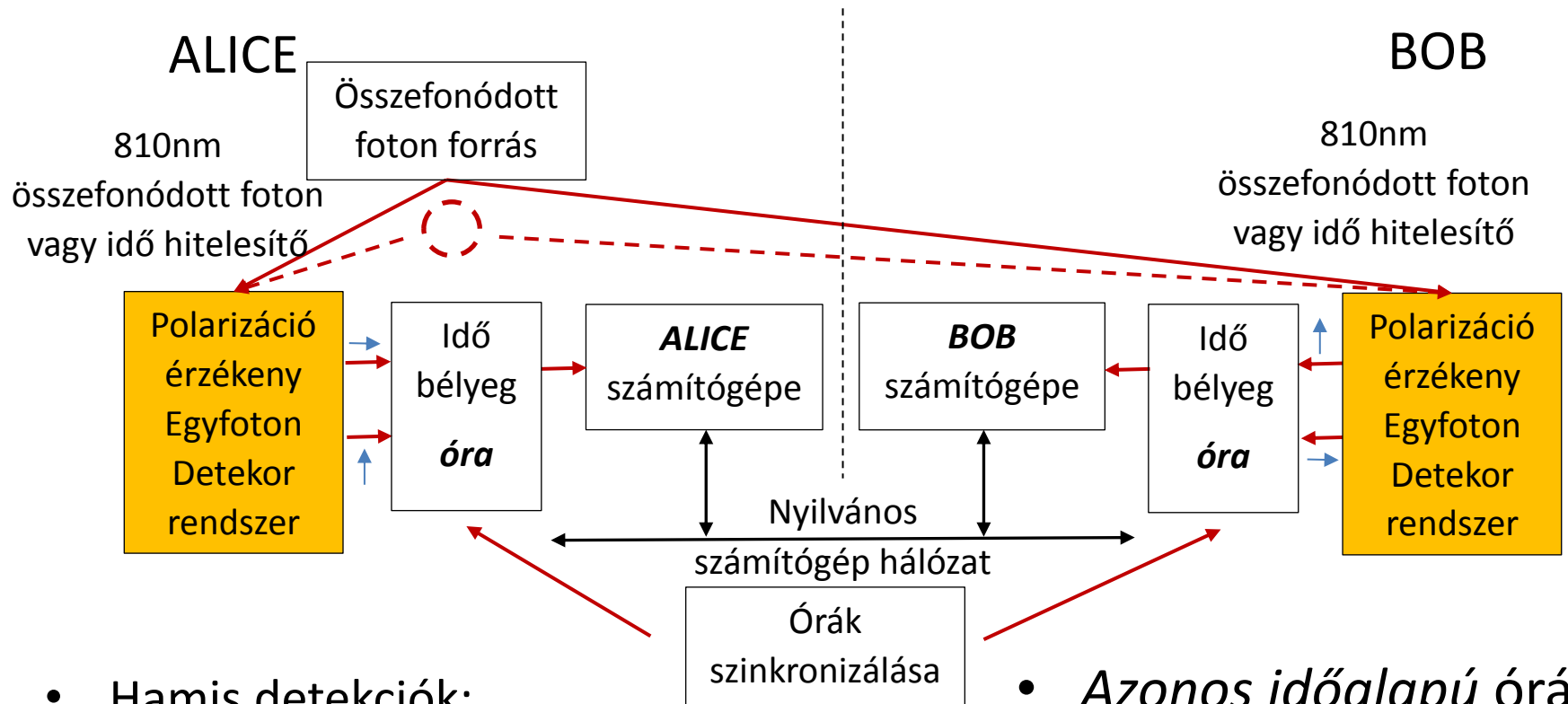
- Alkalmazási igény
 - szimmetrikus kulcsú titkosítás, kulcsszétosztó rendszerek
 - Végtelen erőforrással rendelkező *lehallgatóval* szemben is biztonságos kommunikáció
- A ***biztonság*** alapja ***kvantumfizikai*** eredetű
 - Összefonódott foton párok detekciója
 - ***Lehallgatott foton nem vesz részt a kódgenerálásban***
- Másodlagos előnyök
 - Nem engedély köteles kommunikáció – olcsó lehet
 - Nem igényel fényvezetős összeköttetést
 - Mobilan telepíthető változat is elképzelhető

Free Space QKD működése



- *Polarizációban* (lineáris) összefonódott foton forrás
- Alice detekciója meghatározza Bob detekcióját:
 - Ha Alice: $\wedge$ akkor Bob: $>$
 - Ha Alice: $>$ akkor Bob: $\wedge$
- Alice és Bob feljegyzi a detektálás
 - Idejét,
 - Polarizációját
- Alice és Bob kicseréli a detektálási időket nyilvános hálózaton
 - Egyidejű detekció kulcsbitet hoz létre

Free Space QKD megvalósítása, kihívások



- Hamis detekciók:
 - Detektor sötét zaja
 - Napfényből származó, sávba eső fotonok
- Egyidejű keletkezés meghatározásának nehézsége
 - Különböző jelút hosszak
 - Különböző órák

- Azonos időalapú órák szükségesek
 - Optikai úton átvitt órajel
 - GPS alapú órajel
- Abszolút idő meghatározása
 - Hitelesítő fénypulzussal

Free Space QKD - Hol tartunk?

- Rendszertervezés
 - Optikai és elektromos vezérlés rendszertervei készen állnak
- Rendszerépítés optikai és elektronikai eszközökkel
 - Eszköz beszerzés folyamatban
- Kulcsgeneráló algoritmus tervezés és kódolása
 - Algoritmus tervezés, szimuláció folyamatban

Free Space – összefonódott fotonpárok

Kis Zsolt

Összefonódott kvantumállapotok

Összefonódott állapot A és B között: $|\Psi_{AB}\rangle \neq |\Psi_A\rangle \otimes |\Psi_B\rangle$

Spinek vagy fotonok esetében:

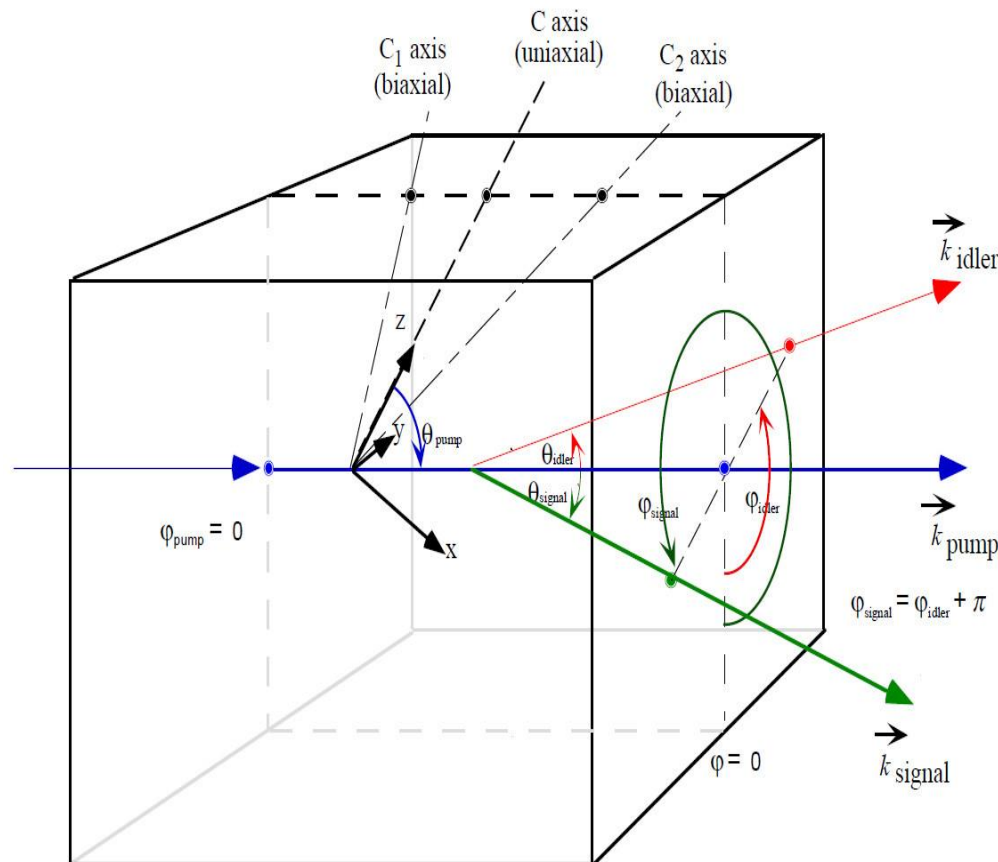
$$|\Psi_{AB}\rangle = (|\uparrow_A\rangle \otimes |\rightarrow_B\rangle + e^{i\vartheta} |\rightarrow_A\rangle \otimes |\uparrow_B\rangle) / \sqrt{2}$$

Alkalmazás:

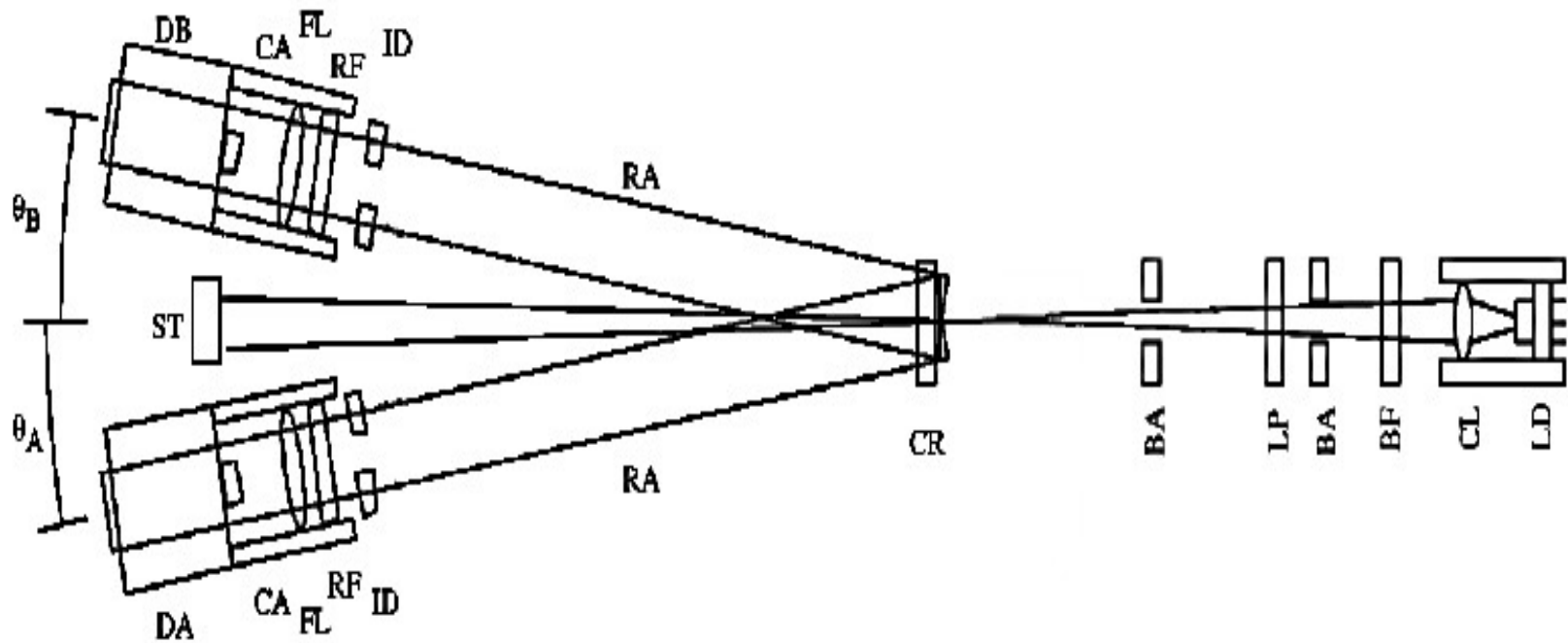
- megfigyelt egyfoton forrás (heralded single photon source)
- összefonódott erőforrás kvantumszámítógépben
- összefonódott erőforrás kvantumkommunikációban

Sztohasztikus összefonódott fotonpár forrás

Parametrikus lekonverzió nemlineáris kristályban: Type I pm.



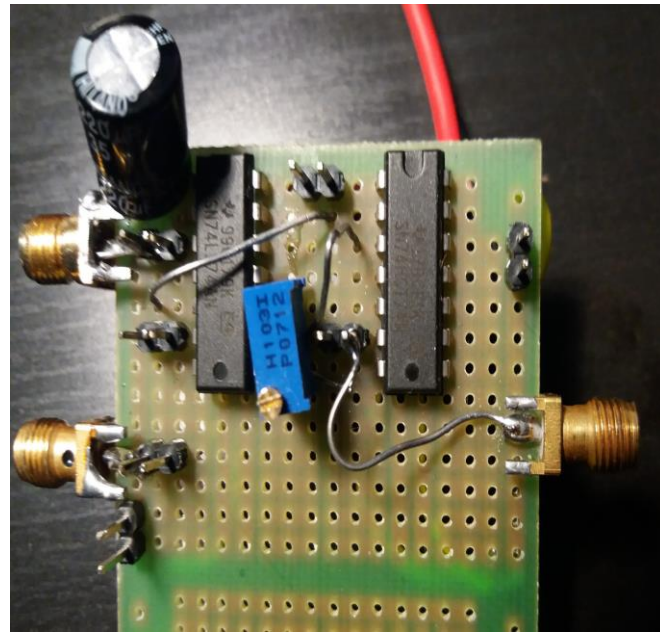
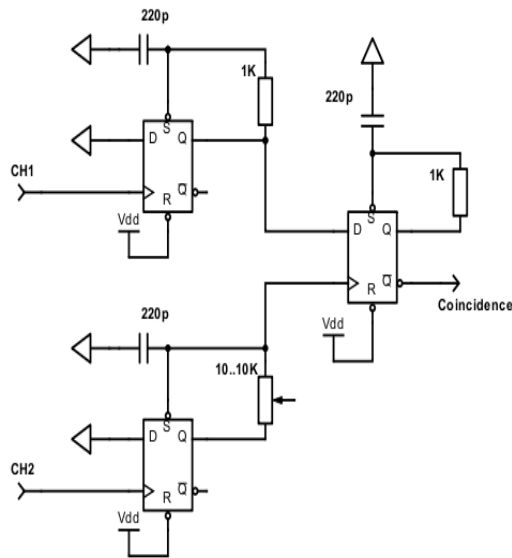
Kísérleti elrendezés



Koincidencia mérés

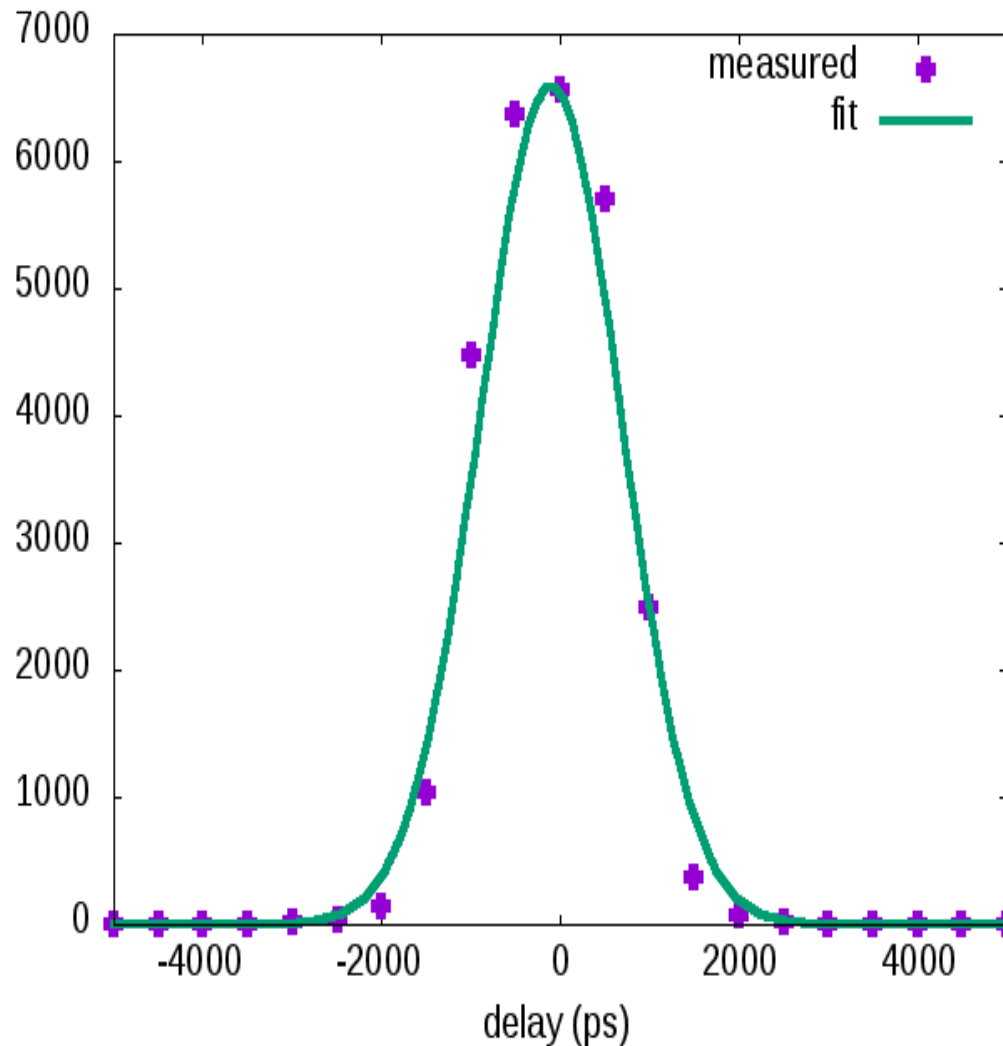
Gyors mérés a beállításhoz, oszcilloszkópon

következő

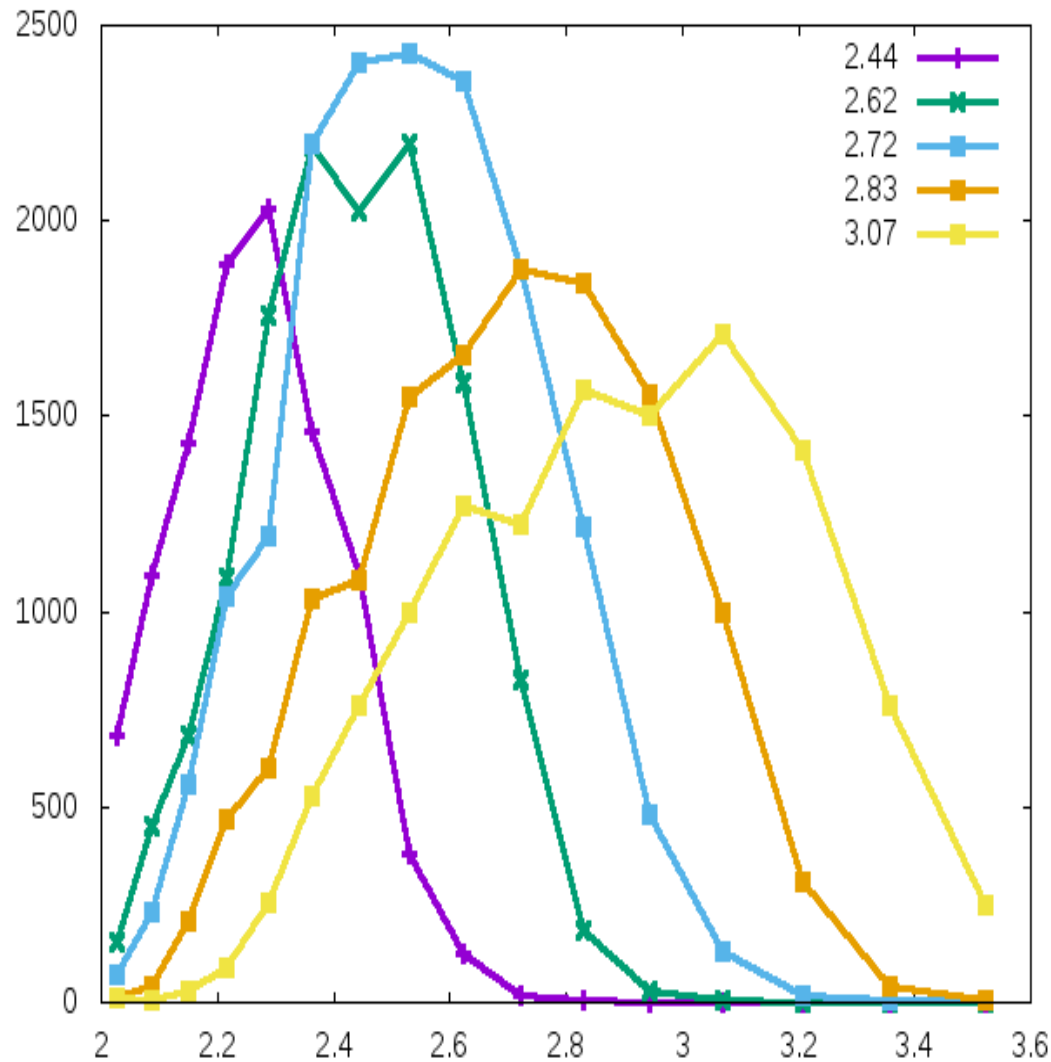


Pontos mérés: időbélyeg kártya (SensL Timeharp),
27ps felbontás

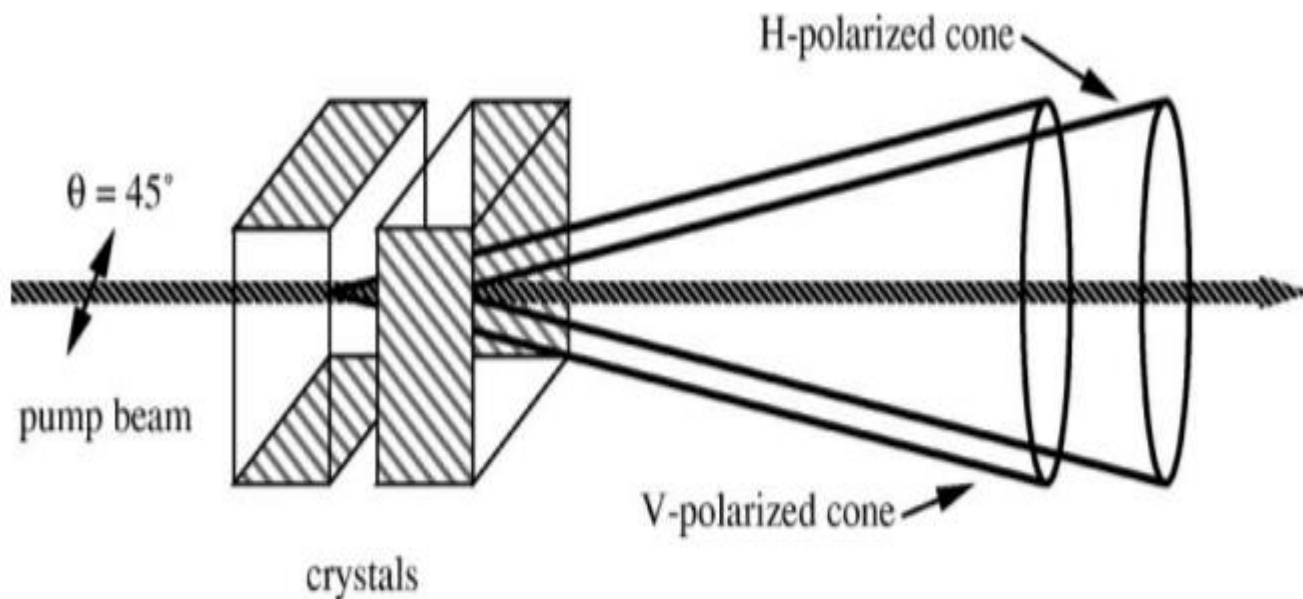
Mérési eredmény I: korreláció rögzített irányokban



Mérési eredmény II: korreláció irányfüggése



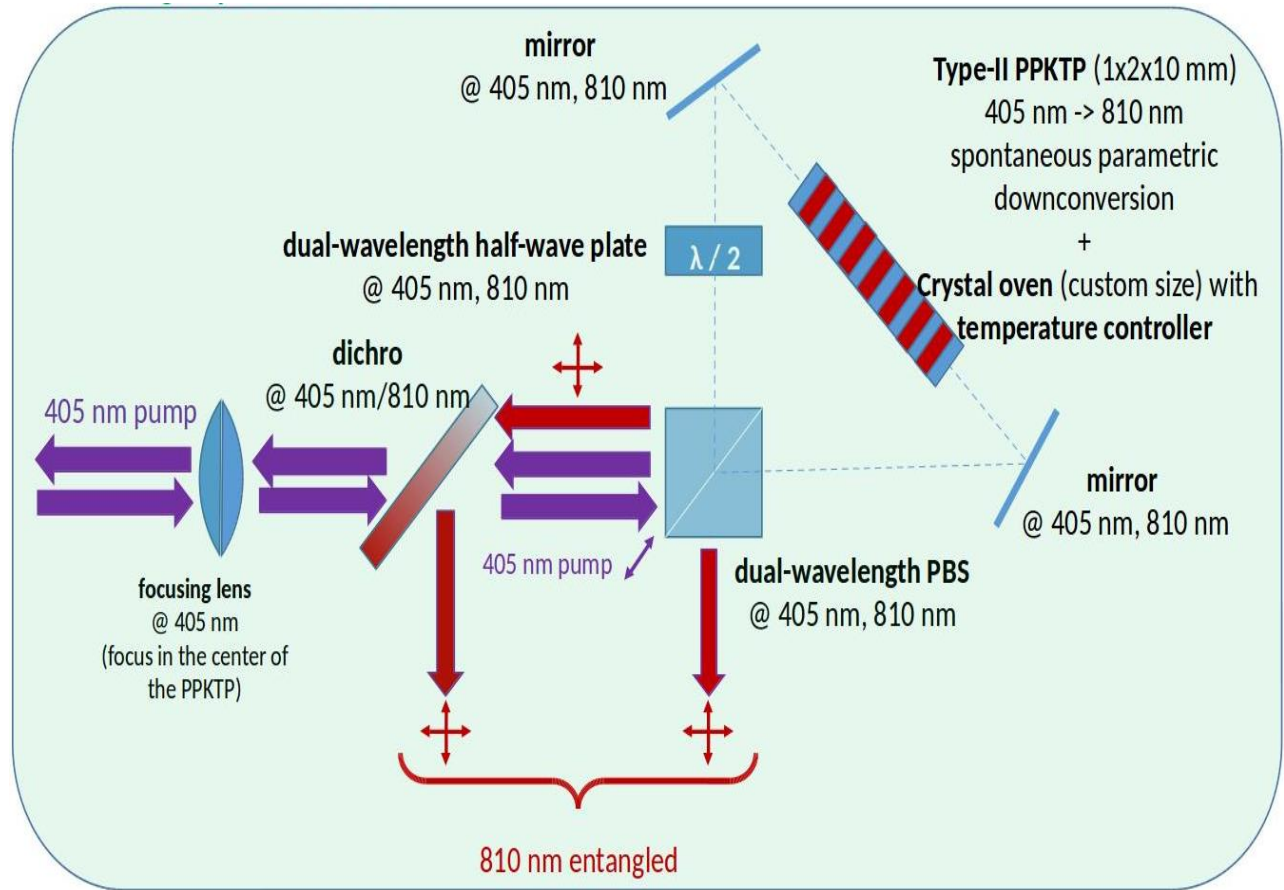
Polarizációban összefonódottság kimutatása



Bell-méréssel lehet igazolni a polarizációs összefonódottságot

További lépések

- polarizációban összefonódott fotonok előállítása és tesztelése
- kisebb és stabilabb összefonódott fotonpár forrás építése PPKTP kristály alkalmazásával





Kvantum véletlenszám generálás - QRNG

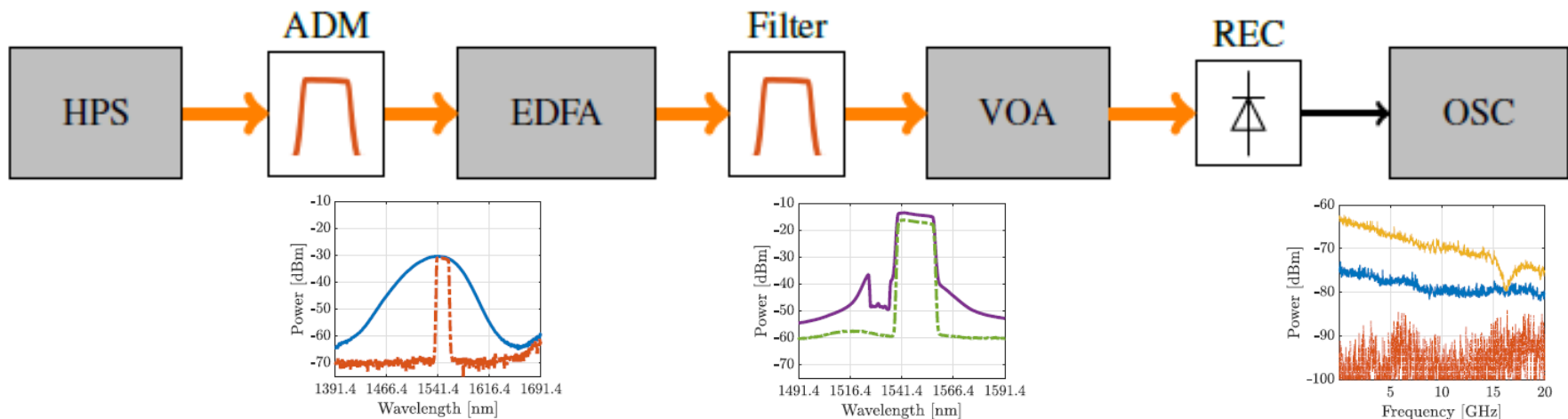
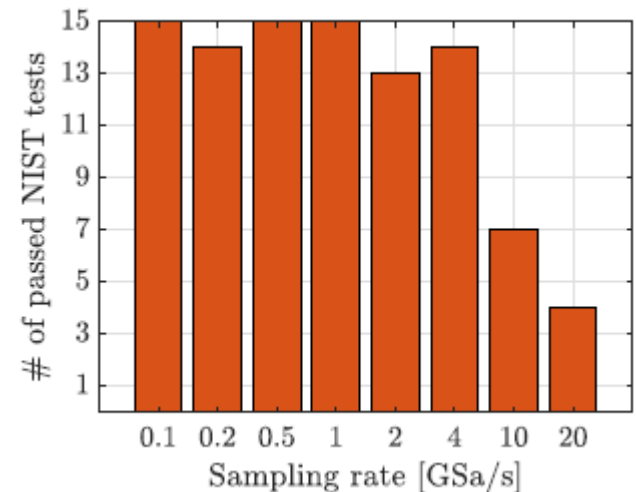
Gerhátné Udvary Eszter

Motiváció: Jó minőségű véletlenszám-sorozatok

- Alkalmazási igény
 - szimmetrikus kulcsú titkosítás, kulcsszétosztó rendszerek, kriptográfia
 - Monte-Carlo szimulációk, szerencsejátékok...
- álvéletlen-generátorok (PRNG, pseudo random number generator)
 - kimenetük determinisztikusan meghatározható a kezdeti állapot függvényében
=> nem használhatóak kriptográfiai célokra
- Kvantumfizika
 - véletlenszerűség & a mérések által okozott hullámfüggvény-összeomlás
 - elvben tökéletesen random, nagysebességű bitsorozatok előállítása, amihez senki más nem juthat hozzá

A kutatás jelenlegi helyzete

- Erősített spontán emissziós generátorok
 - Szélessávú fényforrás intenzitásfluktuációjának mintavételezése (8 GHz) és középértékhez komparálása
 - Számos felépítési lehetőséget vizsgálva választottuk ki a legjobbat
- Egyszerű utófeldolgozással 1 Gbps sebességgel mintavételezett, a NIST véletlenségi tesztjeit sikerrel teljesítő bitsorozatot generáltunk
 - A feldolgozás kismértékű finomításával várhatóan legalább 4 Gbps sebességig megvalósítható a rendszer alapvető változtatása nélkül



További feladatok, kihívások

- Több bites mintavételezéssel ez a sebesség megsokszorozható, a korlátot a digitális feldolgozás sebessége jelenti
- A beszerzésre kerülő eszközökkel újabb architektúrák megépítése és vizsgálata
 - Útelágazáson alapuló (nyalábosztós) módszer
 - Fotonok beérkezési idő-különbségén, ill. fotonszámláláson alapuló módszer
- Eredmények kiértékelése, összehasonlítása
- Működő, online elérhető QRNG megépítése és beüzemelése az előzetes tesztek alapján