Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék

Czermann Márton

EGYFOTONON ALAPULÓ KVANTUM KULCSSZÉTOSZTÓ RENDSZER HATÉKONYSÁGVIZSGÁLATA

KONZULENSEK

Dr. Bacsárdi László és Dr. Kovács Benedek

BUDAPEST, 2019

Tartalomjegyzék

Összefoglaló

A közelmúltban minden területen felértékelődött az adatok biztonsága, s ezzel egyre nagyobb hangsúlyt kap a védett, titkosított kommunikáció is. Elég csak a bankszektorra gondolnunk, de igaz ez biztosítási ügynökségeknél, az egészségügyben, de még akár egyes energiaszolgáltatók hálózatainak esetében is. Ahogyan a világ egyre inkább digitalizálódik és a kommunikáció is egyre gyorsabb ütemben fejlődik, úgy válik egyre fontosabbá az is, hogy pénzünket, jelszavainkat, adatainkat biztonságban tudhassuk a rosszindulatú betolakodókkal, hackerekkel, bűnözőkkel szemben.

Gilles Brassard és Charles H. Bennett 1984-ben áttörést értek el a biztonságos kommunikáció területén. Kvantum alapú kulcsszétosztáson dolgoztak (QKD – Quantum Key Distribution), melynek eredményeként megalkották az úgynevezett BB84-protokollt. Ennek a protokollnak köszönhetően ideális esetben egy feltörhetetlen biztonsági kulcs alakítható ki két fél között, miközben a módszer pedig teljesen lehallgathatatlan.

Az utóbbi pár évtized során Ázsiában, Amerikában, de ugyanúgy Afrikában is, mint Európában először kvantum linkeket, majd működő kvantum hálózatokat hoztak létre, megteremtve ezzel a kvantumkommunikáció lehetőségekkel teli fiatal világát és egy hatalmas technológiai versenyt is a kontinensek és országaik között. Az irány nem más, mint egy globális kvantum alapú kommunikációs hálózat létrehozása.

Munkám során egy plug&play elven működő, hazai fejlesztésű kvantum-kulcsszétosztó rendszer vizsgálatával foglalkoztam. Egy egyszerű, de mégis robusztus protokollról van szó, mely foton-átvitellel lehetőséget teremt egy titkos kulcs biztonságos létrehozására egy küldő fél (Alice) és egy fogadó (Bob) között. Munkámban a kvantum alapú kulcsszétosztási eljárásnak vizsgáltam a foton-átviteli tulajdonságait, illetve a rendszer hatékonyságát, különös figyelmet fordítva a különböző környezeti behatások és külső zavaró tényezők beiktatása mellett történő átvitelre tesztek, megfigyelések és számítások alapján.

Abstract

In the recent past, the value of data security has risen at every area, given a central role to safe and secure communications. We can think of the bank sector as much as of insurance agencies, health sector or even energy supplier companies. Since communication and information technology improves rapidly all around the world, people need to know their money, passwords and personal data in safety against malicious intruders, hackers and criminals.

Gilles Brassard and Charles H. Bennett have come to a breakthrough in the area of secure communications in 1984. They have been working on quantum key distribution (QKD) when they finally come up with the idea of the BB84 protocol. Due to this protocol, an unbreakable secure key can be established between two sides – in ideal case –, while it is also totally safe from eavesdropping.

During the past few decades, quantum links then later working quantum networks have been established in Asia, America, Africa and in Europe as well, creating the world of quantum communications full of opportunities pushing these continents and their countries into a vast technological competition. The goal is to create a quantum based global communications network.

In my work, I have been dealing with the inspection of a locally developed QKD system, operating according to plug&play principles. It applies a simple and easy to use protocol that gives the opportunity of safety generation of a secret key between a transmitter (Alice) and a receiver (Bob) based on photon transmission process. In my work, I have inspected the attributes of the photon transmission in this quantum based key distribution system, adding the aspect of its efficiency giving response to the different external and environmental impacts based on tests, observations and calculations.

1 Bevezetés

A kvantumkommunikáció napjainkban egyre elterjedtebb kutatási területként szolgál a világ minden táján. A kommunikáció fejlődése és a digitalizáció ugyanis óhatatlanul is megkívánja az adatok titkosításához szükséges technológiai újítások létrejöttét. Gilles Brassard és Charles H. Bennett 1984-es, a kvantummechanika törvényeire épített kulcsszétosztó protokoll megalkotásával [1] elért áttörése biztosította, hogy az ezredforduló után világszerte kvantum linkek és hálózatok létesülhessenek.

A BB84-es protokoll megszületése óta különféle megoldások születtek tökéletesen biztonságos módszerekkel létrehozott digitális titkosító kulcsok létrehozására mind a protokoll metódusát, mind pedig a két fél közti közvetítő közeget tekintve. Alapvetően megkülönböztetünk ún. „prepare and measure" valamint összefonódás alapú [1] protokollokat, de ezek megvalósítására ugyanúgy megoldást kínál az optikai szálas, mint a szabadtéri összeköttetés. Az utóbbi szempontok pedig felvetik a nagyobb távolságok biztonságos áthidalásának problémáját is, amivel együtt még megvalósításra váró eszközökön és módszereken is dolgoznak napjaink kutatói, mérnökei. Ezeket a különféle protokollokat, gyakorlati megvalósításokat és a terület jövőbeli fejlesztéseit foglalom össze a 2. fejezetben.

Munkám célja egy kvantum link megvalósításához épülő, optikai szálas összeköttetésen alapuló kvantum kulcsszétosztó rendszer fejlesztése volt. A rajta végzett mérésekkel és vezérlő kódok létrehozásával a rendszer hatékonyabbá tételén dolgoztam. A nemzeti HunQuTech program keretében az Ericsson Magyarország Kft. által megvalósuló projekt Műegyetemen épülő rendszeréről és működéséről a 3. fejezetben olvashatnak bővebben.

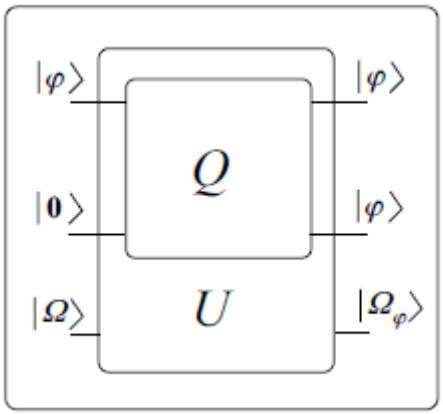
Ezt követően szeretnék betekintést adni a rendszeren végzett munkáimról, melyek magában foglalják a fogadó fél (Bob) oldali fotondetektálás adatainak feldolgozását, melyet kiegészítek egy ún. „time tagging" funkcióval. Meghatározom a küldött kulcsbitek várható beérkezési idejét és a kommunikáció idejét is. A fejezet folytatásaként pedig beszámolok egy, a küldő fél (Alice) általi moduláció időzítésével kapcsolatos mérésről is. Végül pedig megvizsgálom az átvitel minőségét a csillapítás függvényében.

Az elvégzett fejlesztések arra is lehetőséget teremtettek, hogy megvizsgáljam a fotondetektálás és – ennek kapcsán – az átvitel kvantumosságának (minőségének) függését a lézernyaláb csillapításának függvényében. Az ezzel kapcsolatos számításokat és eredményeket az 5. pontban foglaltam össze.

2 Kvantum kulcsszétosztás

A kvantum kulcsszétosztás (angol nevén quantum key distribution – QKD) a legelterjedtebb kvantumkriptográfiai módszer. Népszerűségét a megvalósíthatóságának és egyszerű működésének köszönheti. Hatalmas előnye, hogy a hozzá fejlesztett protokollok leggyakrabban fotonokkal operálnak, így lehetővé téve, hogy akár a meglévő optikai szálon futó nagy sebességű optikai szálas gerinchálózatokkal is integrálhatók legyenek. Ma már több területen is alkalmazzák adatok titkosítására létrehozott biztonsági kulcs kialakítására. Elég, ha a 2007-es svájci választások szavazatainak védelmére [2], vagy a pár éve, shanghai bankszektorokon való tesztelésekre gondolunk [3].

A kvantum kulcsszétosztás biztonságának alapját elsősorban az úgynevezett „No Cloning Theorem” [1] jelenti, amelyet a következő fejezetekben való relevanciája miatt itt ismertetek. A tétel azt mondja ki, hogy csakis ortogonális kvantumállapotokról készíthető másolat, egyéb esetben ez lehetetlen. Ha feltételeznénk egy olyan Q transzformációt, amely bármilyen kvantumállapot „klónozására” képes lenne, akkor azt az 1. ábra alapján egyszerűen lehetne modellezni.



1. ábra – Kvantum másoló [1]

Zárt rendszerre kiterjesztve Q-t, egy U unitér transzformációról beszélhetünk, mely az ábrán látható $|\varphi\rangle$ állapotot duplikálja. A bemeneten szereplő $|0\rangle$ állapot jelenlétét csupán az unitár transzformáció követeli meg, miszerint a be- és kimenetek

számának megegyezőnek kell lenniük a transzformáció irányának megfordíthatósága érdekében. A természet állapotát $|\Omega\rangle$ jelzi az ábrán. A bemenetre felírható és a kimeneten létrejövő kvantumállapotok között U segítségével a következő leképezés adódik: $U\colon |\varphi\rangle|0\rangle|\Omega\rangle \rightarrow |\varphi\rangle|\varphi\rangle\big|\Omega_{\varphi}\rangle$. Ugyanezt a leképezést használva egy másik, $|\psi\rangle$ önkényesen választott kezdeti állapotra, hasonlóan kapjuk, hogy: $U\colon |\psi\rangle|0\rangle|\Omega\rangle \rightarrow |\psi\rangle|\psi\rangle\big|\Omega_{\psi}\rangle$. Az unitár transzformációk jellemző tulajdonsága, hogy skalárszorzat-tartóak. A bemenetre és a kimenetre rendre felírható skalárszorzatok:

$$\langle \Omega, 0, \psi|\varphi, 0, \Omega\rangle = \langle\psi|\varphi\rangle\langle 0|0\rangle\langle\Omega|\Omega\rangle = \langle\psi|\varphi\rangle,$$

$$\langle \Omega_{\psi}, \psi, \psi\big|\varphi, \varphi, \Omega_{\varphi}\rangle = \langle\psi|\varphi\rangle\langle\psi|\varphi\rangle\langle\Omega_{\psi}\big|\Omega_{\varphi}\rangle = \langle\psi|\varphi\rangle^2\langle\Omega_{\psi}\big|\Omega_{\varphi}\rangle.$$

A két szorzat csak és kizárólag akkor lehet egyenlő, ha $\psi = \varphi$ (ez az eset lefedi a $\langle\psi|\varphi\rangle = \frac{1}{\langle\Omega_{\psi}|\Omega_{\varphi}\rangle}$ esetet is, mivel egységvektorokkal dolgozva azok skalárszorzata nem lehet nagyobb 1-nél), vagy pedig, ha $\langle\psi|\varphi\rangle = 0$. A teljesülés feltételeit összegezve kimondható tehát, hogy csakis ortogonális kvantumállapotok másolhatóak.

A No Cloning Theoremben rejlő lehetőséget különböző módon kiaknázva két féle kvantum kulcsszétosztó protokollcsalád is kifejlődött az évek során. Különböző tulajdonságok jellemzik a protokolljaikat és megvalósításuk, megvalósíthatóságuk is sok tekintetben eltér egymástól. A 2.1-es és 2.2-es fejezetekben a két protokollcsaládot, míg a 2.3-mas fejezetben azok létező implementációit foglalom össze.

2.1 „Prepare and measure” elvű QKD

A prepare and measure elven működő protokollokat manapság sok helyen alkalmazzák egyszerűségük és robusztusságuk miatt. Ahogyan a neve is mutatja, mindegyik ide tartozó protokollban hasonló, hogy bennük egy előre generált kulcs valamilyen formában kódolt küldése és mérése játssza a központi szerepet. Az ötlet magja pedig nem más, mint a BB84-protokoll.

2.1.1 BB84 és fejlesztései

1984-ben Gilles Brassard professzor és Charles H. Bennett fizikus közös munkája nyomán létrejött a BB84-protokoll, melyet azóta is sok másik módszer használ alapul a kvantum kulcsszétosztás realizálására. Működésének célja két fél közti

kvantum linken keresztüli digitális biztonsági kulcs létrehozása oly módon, hogy annak lehallgatására tett kísérletek azonnal észlelhetőek, vagy eleve kiküszöbölhetőek legyenek – így megvédve a kommunikáció biztonságát.

A protokoll kvantumos egységként fotonokat vesz alapul. A foton – és ezzel együtt az információtartalom, vagyis pontosabban a rajta végzett moduláció – ugyanis megbízhatóan és gyorsan küldhető el egyik féltől a másikig: optikai kommunikációs eszközök sokasága áll a rendelkezésünkre, hogy kialakítsunk egy ilyen linket. Atomi környezetet tekintve versenytársként (pl. egy elektron) ez sokszor jóval nehezebb, legalábbis ami a kvantumos alapot tekinti. Ez utóbbi esetben ugyanis egy megfelelő kvantumállapot létrehozásához és használatához elengedhetetlen az abszolút 0 fokos hőmérséklet közeli munkakörnyezet. Többek között ez is hozzájárul a kvantumszámítógépek nehézkes gyakorlati megvalósításához.

Minthogy a BB84 is a prepare and measure QKD család része, a módszer egy előre elkészített kulcsból, azaz egy digitális bitsorozatból indul ki. Alice ezt a megadott hosszúságú bináris számsort teljesen véletlenszerűen állítja elő, s ehhez akár egy kvantum alapú randomszám-generátort (QRNG) is használatba vehet. Ezt a kezdeti kulcsot, vagyis inkább az ez alapján elkészített kódot szeretné megosztani Bobbal, hogy aztán azt felhasználhassák kommunikációjuk titkosítására. Ehhez nem tesz mást, mint hogy választ magának két bázist, amiben a fotonokba kódolhatja a bitsorozatát. Legkézenfekvőbb megoldás erre két polarizátort választani, amelyek egyike horizontálisan és vertikálisan, a másik pedig ehhez képest 45°-kal eltolt bázis szerint ($\pm \pi/4$) polarizálja a fényt. Az eltérő irányok bázisonként tekinthetők 0-s vagy 1-es bitnek is, amit a protokoll nagyszerűen fel is használ.

Ugyanis Alice előállít még egy – szintén bináris, random – kulcsot magának, melynek hossza megegyezik az előzőével. Ez azt hivatott megszabni, hogy eredeti kulcsának bitjeit melyik polarizációs bázisban kódolja. Ha ugyanis az első bitet „0 alapján” kell kódolnia, akkor az az egyik, „1 alapján” pedig a másik polarizátort takarja. A kódolás metódusa tehát teljesen véletlenszerűen történik, mi több, fontos kiemelni, hogy Alice eredeti bitsorozata a folyamat során nem-ortogonális kvantumállapotokba kerülnek. Ez azért lényeges, mert ezek az állapotok a No Cloning Theorem alapján bizonyítottan lemásolhatatlanok. Alice tehát a fotonok polarizációjába kódolt,

véletlenszerűen generált kulcsát küldi tovább a fogadóoldalnak, aki hozzá hasonló módszert választ a dekódolásra.

Bob szintén két bázis variálásával (természetesen a küldő félével megegyezővel) járul hozzá a protokollhoz. Alice-hoz hasonlóan ő is generál magának egy bináris számsort, melynek hossza ugyancsak megegyezik Alice-éval. Eszerint a számsor szerint válogatva a bázisokat, megméri a fogadott fotonok állapotát. Természetesen Bob nem tudja, hogy társa milyen bázisokat használt a kódolás során, így átlagosan csak a beérkező bitek fele esetén választ megfelelő mérési bázist.

De honnan is tudja a vevő, hogy melyik fotonok esetén mért a helyes bázissal? A válasz erre nagyon egyszerű. Alice közzéteszi a bitenkénti bázisválasztásait egy klasszikus csatornán (pl. Ethernet) – s mivel csakis ezt közli, magát a kódolást nem, a protokoll továbbra is biztonságos marad. Ezt hívják az angol szakirodalomban „post processingnek", azaz utólagos feldolgozásnak, melynek léteznek még egyéb megoldásai is, amikkel a QBER (Quantum Bit Error Rate), azaz a kvantum-bithiba arány csökkenthető.

A használható, „jó" biteket végül megtartják a felek, így kialakítva a biztonságos kulcsot egymás között. A BB84-protokoll elmélete tehát egyszerű és ideális esetben itt véget is ér. De vajon a gyakorlati alkalmazások során is kijelenthető a totális biztonság? Mit kezd a protokoll egy betolakodóval, aki minden áron le akarja hallgatni a kommunikációt?

2.1.2 További, BB84 alapú protokollok

A valóságban nem ideális esetekkel foglalkozunk, hiszen napjainkban például tökéletes küldő oldali egyfoton lézer nem létezik. A mostani egyfoton lézerek alacsony hatékonyságúak, ezért sokszor gyenge koherens impulzusokat generálnak – mindemellett meglehetősen drágák is. Vagy vegyük például a fogadó oldal helyzetét. A kvantumkommunikációhoz legelterjedtebben használt, lavina-effektuson alapuló egyfoton detektorok (SPAD – Single Photon Avalanche Diode) alapesetben – amikor egyetlen foton kerül a bemenetükre – helyesen, Geiger-módban működnek, számlálják a beérkező fotonok számát. Viszont mihelyst megnő az intenzitása a beérkező impulzusoknak, a műszer lineáris módba lép át és a kimenet arányos lesz a bemenő fény erejével.

Ezek a hibák ugyan nem tűnnek a működést befolyásoló, leküzdhetetlen hibáknak, de egy harmadik fél (Eve) számára lehetőséget nyújtanak bizonyos kvantum támadások indítására annak érdekében, hogy kettejük titkos kulcsára ő is szert tegyen.

2.1.2.1 Decoy state protokoll

Megeshet, hogy a lézerünk 2, vagy több fotont indít el egyszerre, vagy eleve gyenge, koherens lézerimpulzusok küldéséről beszélünk. Ekkor Eve elvégez egy „nem-romboló" hatású mérést [4] az impulzuson, hogy megtudja a fotonok számát. Amikor egy több-fotonos energiacsomagot észlel, blokkolja azt, majd kettéosztja egy sugárnyalábosztó segítségével. Egyszerűen csak megtartja az egyik részét az impulzusnak, a másik részét pedig továbbítja Bobnak. Amikor pedig Alice és Bob egyeztetik a bázisaikat, a közzétett információjuk alapján ő is megbizonyosodhat a kulcsról. Ezt a módszert PNS-nek (photon number splitting-nek) hívják és ezzel elérhető, hogy a küldő és a fogadó fél ne jöjjön rá a beavatkozásra.

Természetesen a BB84 kis változtatásával kiküszöbölhető ez a veszély, ahogyan ezt a korai 2000-es években meg is tették, létrehozva egy új protokollt, a „csali állapot" módszerét (angolul: decoy state method). A módszer lényege a nevében is benne foglaltatik: csali, vagyis hamis állapotokat is felhasználunk a kommunikáció során. Ezek a hamis bitek a lényeges, információtartalommal bíróaktól csupán az impulzusokban lévő várható foton számban különböznek. A céljuk Eve detektálása.

Alice minden egyes impulzushoz hozzárendel vagy egy csali-, vagy egy jelállapotot és modulálja mindegyiknek az intenzitását. Ezeket elküldi Bobnak, aki miután megkapja az összeset, egy hitelesített csatornán keresztül megtudja Alice-tól, hogy melyikek voltak az alapállapotú impulzusok. Több kísérletben is bizonyították a módszer biztonságát, mi több, 2007-ben Rosenberg [5] és Peng[6] is bemutatta gyakorlati megvalósíthatóságát 100 km-es távolságon. Ez azért is fontos, mert a protokoll előtt a PNS támadás lehetősége egy 30 km-es korlátot szabott a QKD linkek biztonságos használatához [7].

Ezzel a módszerrel tehát ki lehet szűrni egy esetleges harmadik fél beavatkozását, s így eltűnik az a bizonyos 30 km-es megszabás is a kommunikáció hosszára. Ez felbátorította a tudósokat, hogy tovább kísérletezzenek a QKD

rendszerekkel. Azonban egy másik probléma is felütötte a fejét, ami már a fogadóoldalon, a detektor tökéletlenségéből fakad.

2.1.2.2 MDI-QKD

Azonban a detektor oldali apró hibákat is kihasználható egy harmadik fél által és többféle támadást is intézhet a két fél között zajló kommunikáció felé. Vegyük például a „detektorvakító” támadást (angolul: detector blinding attack), melynek során Eve megragadja a SPAD-ek hibás, lineáris működése kínálta lehetőséget. Megszakítja az impulzusokat, megméri őket a saját rendszerében, majd elvakítja egy erős impulzussal Bob detektorát. Ezután a mérési eredményének függvényében meghatározott erősségű impulzusokat küld, aminek következtében Bob detektora csakis akkor fog tudni fotont jelezni, ha ugyanabban a bázisban mér, mint ő. Így elérhető, hogy a támadó teljesen rejtve maradjon, míg neki sikerül megszereznie a kommunikáció kulcsát.

Szerencsére azonban ennek a kiküszöbölésére is született egy jó megoldás, ami nem más, mint az MDI-QKD, azaz a mérőeszköz-független kvantum alapú kulcsszétosztás [8]. Itt mind Alice, mind pedig Bob adók, akik a jeleiket egy harmadik, megbízhatatlan félnek küldik el. Ez a fél egy Bell-állapotmérést (BSM – Bell-state measurement) [1] végez, ami egy utólagosan kiválasztott összefonódást hoz létre, majd ezt az eredményt visszaküldi. Ez az összefonódás egyfelől ellenőrizhető Alice és Bob részéről, másfelől pedig egy teljesen különálló fekete dobozként teszi kezelhetővé a harmadik felet, így az nincs veszéllyel a kulcsmegosztásra.

Az MDI QKD nem csak biztonság szempontjából kiemelkedő jelentőségű a kvantumalapú kulcsszétosztásos módszerek között, de jól tűri a magas csatornaveszteséget is, ebből fakadóan pedig nagy távolságokban is használható. Nem olyan régen például sikerült egy 404 km-es kvantum linket létrehozni ezzel a módszerrel egy alacsony veszteségű optikai kábelen keresztül [9], melyen 100 km-es távolságban 3 kbps-os kulcsrátával képesek voltak OTP segítségével hangüzenetet kódolni. Megnövelve 1 GHz-re az MDI-QKD órajelét a rendszer elérte az 1 Mbps-os sebességet is.

A fejezetben bemutatott protokollokon kívül természetesen sok más prepare and measure elven működő megoldás létezik még, mint például a BB84 egy későbbi,

továbbfejlesztett verziója, a B92 [1], vagy az ezen alapuló SARG [10] protokoll is. Dolgozatomnak viszont nem célja, hogy sorra vegyem, csoportosítsam, vagy összehasonlítsam ezeket a megoldásokat, sokkal inkább az, hogy pár példán keresztül bemutassam azt a környezetet, amiben aztán elhelyezhetővé válnak majd a HunQuTech-projekt keretében végzett munkáim. Ezt az elgondolást követve át is szeretnék térni a kvantumkommunikációs protokollok másik nagy csoportjára, melynek központjában az egyik legmeghatározóbb kvantum jelenség található: az összefonódás [1, 11].

2.2 Összefonódás alapú QKD

Az összefonódáson alapuló kvantum kulcsszétosztás megértéséhez először meg kell ismernünk magát a jelenséget és fontosabb tulajdonságait. Alapesetben egy két kvantumbitből álló kvantumregiszter különálló kvantumbitek tenzorszorzatából áll össze, állapotát különböző súllyal (valószínűségekkel) meghatározva. Ebből következően a kvantumregiszterek fel is bonthatóak 1 kvantumbites tényezőkre. Vegyük például a $|\varphi\rangle = a|01\rangle + b|11\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$ kvantum szorzatállapotot, ahol $|\varphi_1\rangle = a|0\rangle + b|1\rangle$ és $|\varphi_2\rangle = |1\rangle$. De mi a helyzet $|\psi\rangle = a|00\rangle + b|11\rangle$ esetében? Láthatóan itt nem működik a felbontás.

Ezek a fel nem bontható, két- vagy több bites kvantum állapotok ugyanis nem egyedüli kvantumbitek egyesülésével hozhatóak létre, sokkal inkább olyan módszerek segítségével, melyek a gyakorlatban egy közös fizikai eseményhez kapcsolódnak. Ezek az események egyszerre hoznak létre kvantum részecskéket, melyek között egy egészen különös kapocs alakul ki. Az így létrejövő részecskéket összefonódott kvantum párnak hívjuk és lehetnek ugyanúgy fény, anyagi, vagy hullámtermészetűek, mint a szorzatállapotok.

A kiváltó esemény a gyakorlatban lehet például egy extrém energiaszintre emelt Ca atom. Ekkor a benne lévő elektron már nem képes egy foton kibocsájtása mellett alapállapotba kerülni és helyette egyszerre két fotont sugároz ki magából. Ezek a részecskék megfelelő irányba elhagyva az atomot, közös polarizációjuk által összefonódott párként viselkednek. Emellett sok más módszer is létezik a gyakorlatban, amivel képesek lehetünk ilyen tulajdonsággal rendelkező kvantum állapotot létrehozni [12]. Elméleti és áramkör tervezési szempontból azonban sokkal kézenfekvőbb megoldásra is bukkanhatunk, ha a kvantum kapukra gondolunk [1]. Egy Hadamard és

egy CNOT kapu használatával, azt megfelelő bittel vezérelve eredményül megkapjuk az összefonódott Bell- vagy másképpen EPR állapotokat (Einstein, Rosen és Podolski után). Ezek a következők:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Az összefonódott párok között egy olyan kapocs áll fent, ami biztosítja, hogy amikor az egyik részecske állapotát szeretnénk megmérni és az így egy adott fix értékre hanyatlik (0/1-ként feldolgozható), párja ugyanabban a pillanatban szintén beáll erre az értékre. Ez a tulajdonság akkor is megmarad, ha két távoli pontban végezzük el a kísérletet – például egy bázisállomáson keltett foton pár egyikét a Földön, a másikat pedig egy műholdon vizsgáljuk. Ez eléggé meglepő lehet első olvasatra, hiszen ez a tapasztalat egy olyan kölcsönhatást enged feltételezni a két részecske között, mely gyorsabban érvényesül, mint maga a fény sebessége – ez pedig elég határozottan szemben áll Einstein relativitás-elméletével. Mégis, bár konkrét magyarázatot a fizika jelenlegi állása nem tud adni, hogyan is lehetne összeférhető Einstein elmélete a kvantummechanika bizonyos törvényszerűségeinek, a gyakorlati fizikusok tapasztalatai egyértelműen bizonyítják az összefonódás létezését. Ezt felhasználva 2017-ben Kínának sikerült elérnie két, a Földön több mint 1000 km-re lévő bázisállomás közötti összefonódáson alapuló kvantum linket, melyben a kettejük között egy műhold, a Micius osztotta szét az összefonódást [13, 14]. Ennek működéséről a fejezet további protokolljai nyújtanak betekintést.

Hogyan is lehet egy ilyen különös fizikai jelenséget egy biztonságos kulcs létrehozására felhasználni? Először is vázoljunk fel egy új koncepciót Alice és Bob között, méghozzá Charlie segítségével. Ezúttal kérjük meg Charlie-t, hogy ő generáljon két kezdeti számsort a protokoll indításához. Az egyik számsort itt is arra használja, hogy a két kódoló bázis között véletlenszerűen változtatva kódolhassa a másik számsor által előkészített kulcsot. A kódolt impulzusokat pedig egy sugárnyalábosztóval elküldi

Alice-nak és Bobnak is egyaránt. Ők pedig, a BB84-protokoll alapján szintén véletlen sorrendben alkalmazott bázisokban megmérik a fogadott kvantumbiteket, majd az eljárás után egy klasszikus csatornán utólagos javítási eljárásokkal egyeztetés útján kialakítják titkos kulcsukat.

Ebben azonban van egy eléggé bizonytalan pont, méghozzá Charlie személyében, akinek a kezében van a két fél biztonsága. Azért, hogy meggyőződjünk arról, hogy megbízott segítőnk ne tudja kompromittálni a protokollt, egy aprócska módosítást hajtunk végre rajta. Eve ebben a változatban szorzatállapotú kvantumbitek helyett összefonódott állapotúakat generál és azok egyik felét küldi Alice-nak, másikat pedig Bobnak. Ezeknek az állapotoknak a tisztasága pedig jól ellenőrizhető a két fél által, pusztán pár bitet kell felhasználniuk a Bell-egyenlőtlenség [15] vizsgálatára. A Bell-egyenlőtlenség sérülése ugyanis bizonyítékként szolgál egy támadó (pl. Eve) összefonódott kvantumállapotokba való belenyúlásáról.

Ha jól megfigyeljük, akkor ennek a protokollnak során a két fél közti kulcs úgy jön létre, hogy a kommunikáló feleknek előzetesen nem kellett egy kezdeti kulcsot előkészíteni. Az összefonódott kvantum állapotokon alapuló kvantum-kriptográfiai protokollok nagyon népszerűek a mai kutatások és gyakorlati alkalmazások, tesztelések körében, hiszen használatukkal jó minőségű kvantumjelek nagy távolságú átvitelére is lehetőség nyílik. Összefonódás alapú protokoll például a kvantum-teleportáció [1, 8, 16], a szupersűrű kódolás [1, 17], vagy az úgynevezett „entanglement swapping” [16].

2.3 Vezetékes és szabadtéri összeköttetések

Az elmúlt 30 évben rendkívül sok próbálkozás látott napvilágot a fent említett protokollok alkalmazására, így gyakorlati tesztekre is sor került. Számtalan kvantum link épült meg kísérleti céllal, ami az ezredforduló után már átalakult egy tudományos versenyfutássá különböző országok kutatócsoportjai között, elősegítve nagy jelentőséggel bíró kvantum hálózatok létrejöttét is.

Eleinte ezek a linkek zömében földi, vezetékes, optikai szálas összeköttetések voltak, s a nagyobb hálózatokat is ezekre az alapokra építve hozták létre. Ez lehetőséget teremtett egy-egy projekten belül egyszerre több protokoll tesztelését is, melyek egymás mellett, párhuzamosan futva különböző linkeket használtak a működésükhöz. Természetesen az optikai szálas kvantum kommunikációnak is meg vannak a maga

előnyei és hátrányai is. Előnyei közé tartozik, hogy a fény továbbítására és annak módosítására szolgáló optikai kommunikációs eszközök már régebb óta a rendelkezésünkre állnak, működőképes hálózatok teljes rendszere és kiépült gerinchálózatok szolgáltatják a gyakorlati tesztelések hátterét, alapját. A foton, mint a fény kvantumos egysége pedig tökéletes hordozója egy kódolt kvantumállapotnak. (A tárolása ugyanakkor már nehézkesebb feladatnak bizonyul.) Így tehát összességében egy kényelmes, jól kezelhető és mérhető kommunikációs formáról beszélhetünk, melyre kiválóan illeszthetjük a kvantum kulcsszétosztás megannyi protokollját. Ezzel egyetemben fennáll a lehetősége annak is, hogy WDM (Wave Division Multiplex) alkalmazásával egy adott optikai szálon egyszerre kommunikáljunk klasszikus adatot és kvantum kulcsot is. Így a költségek csökkenthetők, a robusztusság pedig növelhető.

Sajnos azonban van egy nagy hátulütője is ennek a módszernek: a csatornaveszteség. Az optikai szálon keresztül küldött fény a szál csillapításának következtében nagyjából 100-150 km alatt annyira legyengül, hogy ekkora távolság felett a detektálás valószínűsége elenyészően kicsivé válik. A ma gyártott optikai szálak csillapítása esetében mintegy 40 dB-es csillapítással lehet számolni 100 km-en. Természetesen léteznek extrém alacsony veszteségű szálak is, melyek használata esetén ez az érték feljebb kúszhat, de a nagyobb régiókon átívelő vezetékes kvantum kulcsszétosztás lehetőségét alaposan behatárolják. Még ha távolságban napjainkra egy félezer km-es összeköttetésre alkalmas protokoll fejlesztésén is dolgoznak, annak a kulcsrátája meglehetősen alacsony szinten fog csak maradni.

Nagyvárosi környezetben azonban ez a probléma nem áll fent, így városi léptékben kifejezetten előnyösnek bizonyulnak. Sok nagyvárosban már most is használatra készen állnak QKD készülékek, melyek decoy state protokollt és a kialakult kulcsra OTP (One-Time Pad) titkosítást használva gyors (akár több 100 Gbps-os gerinchálózatokkal kombinált) és biztonságosan működő kommunikációs rendszert biztosítanak. (Lásd pl. a korábban is említett shanghai rendszert, vagy egy 3,6 Tbps-os 66 km-es telekommunikációs gerinchálózatba integrált QKD hálózatot [18].) A nagyméretű kvantum kommunikációs kapcsolatok létrehozásához különböző megoldásokhoz folyamodtak az évek során, s vannak olyanok is, melyek a technológia jelenlegi állása miatt még csak a jövő zenéi.

2.3.1 Kvantumismétlők és -memóriák

Ha a földi dimenziókban szeretnénk maradni a nagytávolságú kvantum összeköttetések elérésének érdekében, akkor még mindig folyamodhatunk a kvantumismétlők (quantumrepeater) [19] logikus elgondolásának megvalósításához. Sajnos ez nem olyan egyszerű, mint ahogyan azt elképzeljük, mondjuk egy optikai jelismétlő esetében; az ismétlő a küldőtől 100 km-re megkap egy kvantum jelet, majd felerősítve továbbítja azt, hogy egy újabb, 100 km-re lévő ismétlő fogadja azt, majd, mint egy kaszkádosított rendszer esetében ez tetszőleges számú ismétlő beiktatásával akármeddig kiterjeszthető. A No-Cloning Theorem ennek sajnos határt szab.

Amihez ma folyamodhatunk, az egy megbízhatatlan relék által kínált lehetőség, melynek a lényege az, hogy a küldő Alice és a fogadó Bob közé beiktatunk egy köztes pontot, amit megbízható csomópontnak tekintünk a küldés során. A köztes állomással mindketten kialakítanak egy titkos kulcsot, így kettejük között a maximális távolság a kétszeresére növelhető (hiszen Alice a relével, a relé pedig Bobbal képes titkos kulcs segítségével kommunikálni). Ez a módszer tetszőlegesen kiterjeszthető is több relés összeköttetésre. Feltétele a biztonságnak, hogy a köztes relék fizikailag zártak, hozzáférhetetlenek legyenek. Ugyanilyen megoldás az összefonódás szétosztása entanglement swapping segítségével, ebben az esetben azonban nincs szükségünk megbízható csomópontokra. Ebben az esetben összefonódást osztjuk végig több relén keresztül, míg végül a fogadó fél is csatlakozik a rendszerhez.

Mennyivel egyszerűbb lenne ugyanakkor a dolgunk, hogyha meg lenne a lehetőségünk kvantumismétlők használatára. Ezek az ismétlők az optikai ismétlők jelerősítő tulajdonságát szeretnék felhasználni, oly módon, hogy a kvantumbitek állapota ne sérüljön. Ehhez persze olyan megoldásokra van szükség, mint a kvantum memóriák [20] használata. Ennek azonban az egyik legnagyobb nehézsége a kvantumállapotok koherenciájának hosszabb ideig tartó eltárolása. Hideg atomi gázokon [21], vagy ritka-földfémekkel adalékolt kristályokon alapuló [22] kvantum memóriákat ugyan mutattak már be az elmúlt években, azonban a rövid koherencia-idő mellett a hatékonyságuk sem volt megnyugtató (50% és 69%).

2.3.2 Műholdas összeköttetések

Az utolsó lehetőség ugyanakkor talán a leghatékonyabb megoldás egy interkontinentális kvantum hálózat kialakítására, ez pedig nem más, mint a szabadtéri összeköttetések létrehozása. Műholdakat használva megbízhatatlan relékként létrehozhatunk két nagyon távoli bázisállomás között is kvantum kulcsszétosztást, mégpedig úgy, hogy a két bázisállomás külön-külön összeköttetésben áll a műholddal egy-egy titkosított csatornán. Ezzel a módszerrel akár nagyvárosi hálózatok is összekapcsolhatók, hiszen a földi bázisállomást optikai szál használatával már könnyedén csatlakoztathatjuk hozzá.

A szabadtéri összeköttetések nagy előnye, hogy a csatornaveszteség töredékére csökken, így elérve a nagy távolságok áthidalását. Ez, egy műholddal való kommunikáció során jelentős mértékben stabilizálhatja a kvantum kulcsrátát. Nehézsége ugyanakkor, hogy a lézerrel pontosan eltaláljuk azt a küldési szöget, amivel a műhold detektorába találhatunk a fénynyalábbal. Emellett természetesen éjjel, a sötétebb napszakokban a zajok csökkenésével a küldés hatékonysága radikálisan megnő, míg a rossz időjárás és a felhős égbolt könnyedén gátat szabhat a sikeres kommunikációnak.

2.3.3 Linkek és hálózatok

Ebben az alfejezetben szeretnék bemutatni öt jelentősebb kvantum hálózatot, amik meghatározták, vagy még ma is meghatározzák a kvantum kommunikáció fejlődését. Amerikától kezdve Svájcon át Kínáig, mindenhonnan röviden kiemelve a leglényegesebb aspektusait, jellemzőit a rendszereknek, egy átfogó képet szeretnék adni a kutatási terület helyzetéről, méretéről és a korábban említett protokollok használatára is mutatva néhány példát.

2.3.3.1 DARPA [23]

A legelső működőképes kvantum hálózat 2003-ban jött létre az Amerikai Egyesült Államokban a BBN Technologies, a Harvard Egyetem és a Bostoni Egyetem közös munkájának eredményeként. A DARPA (Defense Advanced Research Projects Agency) hálózata kvantum kulcsszétosztáson alapuló linkekből állt, összesen 6 csomóponttal. 4 csomópont között gyenge koherens impulzusokon alapuló QKD-t implementáló rendszerek futottak 5 MHz-es frekvencián telekommunikációs

hullámhosszal (1550nm) optikai szálon. A másik két csomópont között (Ali és Baba) egy nagysebességű szabadtéri QKD rendszert állítottak fel.

Később egy új linket létesítettek két új, összefonódás-alapú csomópont között, amiket Alexnek és Barbnak neveztek el. Az optikai szálas és szabadtéri összeköttetések egyidejű hibrid használata ugyanazon hálózaton belül ebben az évben az első lépés volt egy interkontinentális kvantum hálózat – avagy a „kvantum internet" – megalkotása felé, ami a mai napig is a kutatási terület végső célja, egyik mozgató rugója.

2.3.3.2 SECOQC [24]

2004 és 2008 között épült meg és futott le az elmúlt bő évtized egyik legjelentősebb QKD hálózat, a bécsi SECOQC-é (SEcure COmmunications based on Quantum Cryptography), mely a legszélesebb körben alkalmazott tesztelési célzattal kvantumprotokollokat. A hálózat pont-pont kapcsolatra és megbízható relék technikájára épült, összesen 8 különböző linken 6 kvantum protokoll futott átlagosan 25 km-es szálhosszokon. Az összefonódás alapú QKD mellett plug&play, fázis- és időkódolás alapú, CV és szabadtéri QKD-t is implementáltak.

A fenti protokollok leírása a [24] publikációban részletesen olvasható, tulajdonságaikról pedig készítettem egy összefoglaló összehasonlítást, amely az 1. táblázatban tekinthető meg.

QKD protokoll	Előnyök	Hátrányok	Egyéb jellemzők
Plug&play	**nagy stabilitás; passzív elrendezés; kulcs menedzselése csomóponton belül**	**csak a visszajövő impulzusok hordoznak kódolási információt**	**titkoskulcs-ráta: 1kbps 25km-en (6dB veszteség)**
Fáziskódolásos	**minden lehallgatásos támadás ellen védett a csali állapotok miatt**	***nincs kiemelkedő hátrány***	**titkoskulcs-ráta: 11kbps 20km-en (4dB veszteség) 5,7kbps 25 km-en (5dB veszteség)**

Időkódolásos	**PNS támadások észlelhetők; kompatibilis az általános távközlési elemekkel, érzéketlen a polarizációs ingadozásokra**	***nincs kiemelkedő hátrány***	**az impulzusok 10%-át a kvantum koherencia ellenőrzésére fordítják**
CV	**stabil, automata rendszerek; folyamatos működés; hatékony nagyvárosi hálózatokban**	**nem hatékony nagyobb távolságok áthidalására**	**titkoskulcs-ráta: 8kbps 6,2km-en (2,8dB veszteség); idő és polarizáció multiplexálás**
Összefonódás alapú	**teljesen automata indítás; hosszútávú működés beavatkozás igénye nélkül; magas tisztaságú összefonódott kvantumállapotok**	**a hosszútávú stabil kulcsráta fenntartása érdekében sok aktív és automatizált stabilizációs modulra van szükség**	**titkoskulcs-ráta: 2,5kbps 16km-en; QBER=3,5%**
Szabadtéri	**éjjel-nappal egyaránt használható; a csali állapotok módszere által kínált minden előnnyel rendelkezik**	**nappal a nagy távolságok és a gyenge jelek nehézkessé teszik a kommunikációt**	**titkoskulcs-ráta: 17kbps 80 méteren**

1. táblázat – SECOQC kvantum protokolljainak összefoglaló táblázata

2.3.3.3 SwissQuantum [10] – rétegvezérelt QKD hálózat

A SECOQC nem csak az alkalmazott protokolljainak színes palettája miatt jelentős, de a többrétegű QKD hálózatok ötletéért is. A 2009 és 2011 között megépített SwissQuantum QKD hálózata egy, a bécsihez hasonló rétegzett struktúrának a működését mutatja be. Az alapötlet három különböző kommunikációs réteg használata: a kvantum-, kulcs-menedzsment és az applikációs rétegé.

A projekt célja az volt, hogy teszteljék a megbízhatóságát és robusztusságát a kvantum rétegeknek 3 csomópont közötti linkek 21 hónapon át tartó működtetésével. A QBER stabilan alacsony szinten volt ez idő alatt, míg a titkoskulcs-rátára kapott értékeket figyelve az SQ1 és SQ2 linkeken nagyjából napi 3-400.000, SQ3-on pedig 8-

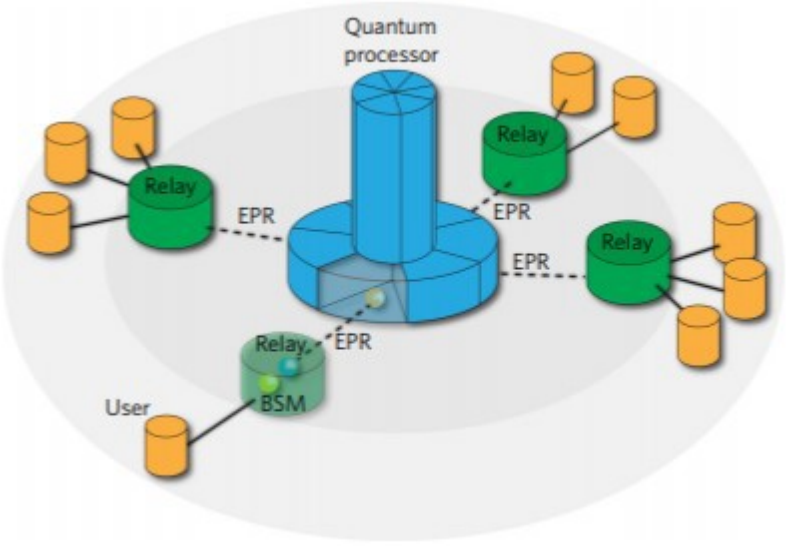
900.000 256-bites titkos kulcs generálása adódott. (A különbség a kisebb csillapítású SQ3 link miatt volt tapasztalható.)

2.3.3.4 Két kvantum teleportáláson alapuló hálózat

Nem csak klasszikus prepare and measure elvű kvantum hálózatok születtek az elmúlt években. 2016-ban egyszerre két, egymástól független publikáció is napvilágot látott, melyben egy kvantum teleportáláson alapuló hálózatot mutatnak be: Kanadában [25] és Kínában [26].

A kanadai Albertában felállított hálózatban egy távközlési hullámhosszúságú foton állapotának 795nm-es fotonra történő teleportálása történik egy másik, 1550nm-essel való interakció következtében, 8,5km-es távolság megtétele után a Calgary optikai szálas hálózatban. Ennek azért van nagy jelentősége, mert ez az eddigi legnagyobb távolságú olyan teleportálási eredmény, ahol a Bell-állapotmérés a protokollban közrejátszó fotonok keletkezési helyétől messze történik meg.

A kínai Hefei városában egy csillagtopológiájú kvantumhálózatnak egy ágát valósították meg, rajta független forrású teleportálást végrehajtva.



2. ábra – Hefei kvantum-teleportációs hálózatának sémája [26]

A 2. ábrán látható kvantum processzor (központi csomópont) és a relé-csomópont között összefonódás oszlik meg, így a felhasználó a központi relé Bell-állapotmérése segítségével kvantumállapotot tud teleportálni a processzornak. Ez az a három-csomópontos rendszer, amit Hefeiben realizáltak. A link 15.7km-es szálon, 5dB-es

csillapítással működött, míg az összefonódott párokat 100kHz-es rátával hozták létre. A csillagtopológiának előnye, hogy a kommunikáció legdrágább eszköze – a detektor – egyetlen központi csomópontban van elhelyezve, így csökkentve a kommunikáló felek – küldők – költségét.

2.3.3.5 Kína kiterjeszti a kvantum kommunikációt

Kína a 2010-es években egy olyan volumenű projektbe vágott bele, mely 2016-ra rekorderré tette, és ami történelmi jelentőségű lépésként könyvelhető el a globális kvantuminternetre való törekvések terén. A 2016-ra létrehozott, 2000km hosszú, optikai szálas QKD hálózat összesen 32 megbízható csomópontot foglal magába, s ezzel a világ eddigi leghosszabb földi vezetékes kvantumkommunikációs összeköttetése [27]. A link négy nagyvárosi kvantumhálózatot is összeköt: Beijinget, Jinant, Hefeit és Shanghait, melyek mindegyike legalább 10 csomóponttal és különböző topológiával rendelkezik. A 2000km-es link minden szomszédos és csakis szomszédos csomópontja között kvantumalapú kulcsszétosztást alkalmaznak, ami egyszerűvé teszi magát a hálózatot és annak bővíthetőségét is.

Később a rendszert kiegészítették a Micius nevezetű műholddal is, amit egy szabadtéri kvantumlink köt össze a földi bázisállomással Xinglongban. A földi állomás és Beijing között optikai szálas összeköttetés húzódik. A műhold Európai oldalról Béccsel létesített kapcsolatot, így kialakítva egy interkontinentális kvantum hálózatot két, egymástól 7600km-re lévő nagyváros között. A Micius 1Mbps feltöltési és 4Mbps letöltési sávszélességgel rendelkezett. Működése során bitenkénti kizáró VAGY művelettel operál a két földi bázisállomással való kulcsok kialakításához, megbízható reléként működve.

A hálózat tesztelésekor egy videokonferenciát hívtak össze a két ország között, amit a rendszeren keresztül tartottak meg [28]. A hálózatot azóta bankszektorokban, biztonsági rendszerekben és biztosítások kezelésében hasznosítják.

3 Saját rendszer

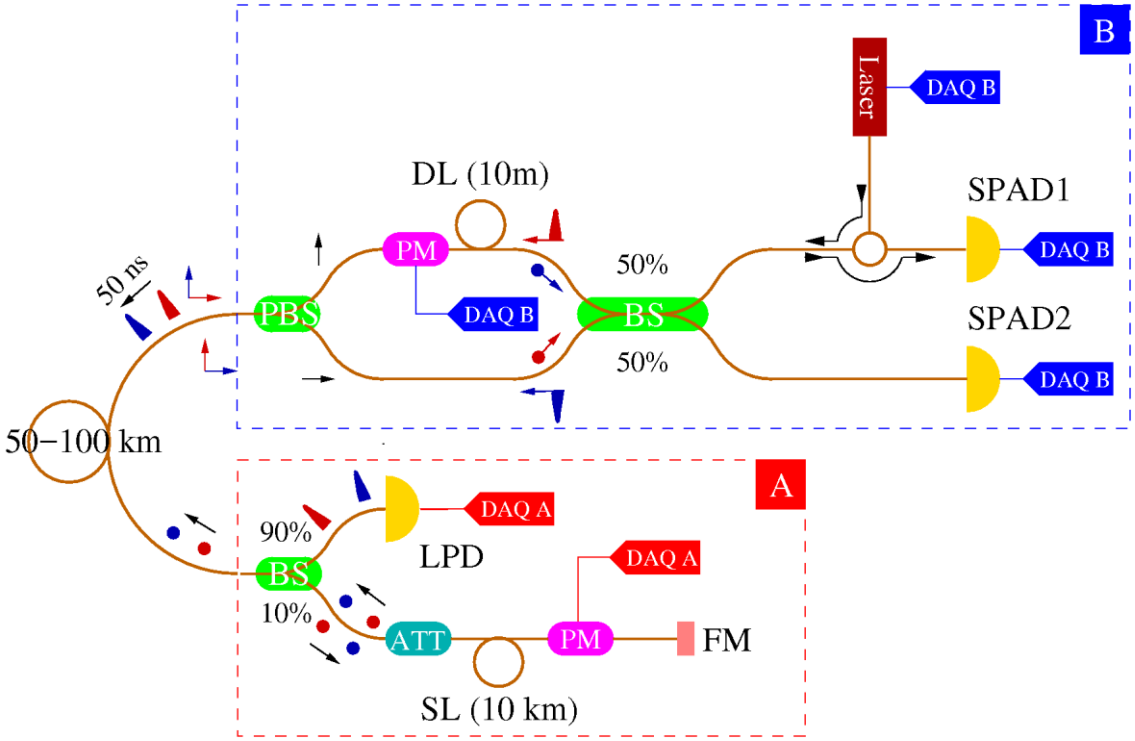
A nemzeti HunQuTech program keretében folyó Ericssonos QKD projekt műegyetemi fejlesztéséhez 2019 nyarán csatlakoztam, hogy tanulmányaimhoz szorosan kötődő szakmai gyakorlatban vehessek részt. A projekt egy egyfotonon alapuló, vezetékes, plug&play kvantum kulcsszétosztó rendszer megépítését és működtetését tűzte ki célul maga elé. A QKD a BB84-protokollt implementálja, és a kulcs kialakítása során a fényimpulzusok interferenciáját veszi alapul. Az Ericsson Magyarország Kft. a BME Hálózati Rendszerek és Szolgáltatások Tanszékének közreműködésével dolgozik a projekt megvalósításán.

3.1 A rendszer felépítése és működése

A projekt egy 2002-es rendszer architektúráját veszi alapul [29], melynek fizikai felépítése a plug&play jegyében született. Ez azt takarja, hogy minden értékesebbnek mondható, vagy éppen bonyolultabb eszköz, vagy megoldás – egyfoton detektorok, lézerforrás, vagy akár a fényimpulzusok szétválasztása a későbbi interferencia elérése érdekében – a két kommunikáló fél közül csak az egyiknél van jelen, ami nem más, mint a fogadó fél, Bob. Ehhez az elrendezéshez és az ezen alapuló protokollhoz anyagi és felhasználásügyi megfontolások vezettek. Vegyünk például egy bankrendszert, melyben az ügyfelek szeretnék biztonságos, titkosított csatornán intézni pénzügyeiket. Egy ilyen rendszerben csupán a banknak szükséges egy nagyobb összeget költeni a fogadóoldali berendezésre, míg az ügyfelek eszközei egyszerűek és olcsók. Emellett a rendszer felállításához sem szükséges komoly stabilizáció az interferencia úthosszának kialakításához, sem pedig aktív vezérlés a szükséges polarizáció fenntartásához. Nevét a rendszerhez való egyszerű csatlakoztathatóságáról kapta.

A felépítés megvalósításához szükséges protokoll során a fény a fogadó oldalról indul egy 1550nm hullámhosszúságon működő lézerből, mely 200ns-onként lő egy fényimpulzust, így 5MHz-es frekvencián generálva a kvantum alapon létrejövő biteket. Ahhoz, hogy a kommunikáció megvalósuljon (Alice, a küldő fél bele tudja kódolni a fotonokba a kezdeti kulcsát) a fénynek be kell járnia Bob és Alice között a teljes úthosszt oda és vissza is. Ez az egyszerű megállapítás magával vonja azt a kritériumot,

miszerint az Alice oldaláról a fotonok modulálása után visszatérő impulzusok nagyságrendileg már az egy fotonos teljesítménybe essenek – azaz, hogy a Bob által fogadott impulzusok megközelítőleg 1 fotonos valószínűséggel rendelkezzenek. Ez garantálja ugyanis az átvitel kvantumos jellegét és nem mellesleg a lehallgatási próbálkozások kiszűrését is. A rendszer sematikus rajza a 3. ábrán látható.



3. ábra – Az Ericssonos QKD projekt rendszerének sematikus ábrája [30]

A protokoll a Bob oldali lézertől indul. A lézer által keltett erős fényimpulzusok első állomása egy kezdeti csillapítón keresztül egy cirkulátorhoz vezet, amely küldési irányban Alice felé, fogadási irányban pedig a detektorok felé tereli azokat. Fontos azonban a megfelelő csillapítás beiktatása rögtön a lézert követően, hiszen az erős fény a cirkulátornál átszórhat a detektorok felé, ami hamis adatokat generál, vagy rosszabb esetben elvakíthatja azt – még ha az ablakozás módszerét használva erre az időre „becsukjuk” a detektorokat, az SPAD-ek olyan érzékeny műszerek, amiket jobb ilyen terhelésnek nem kitenni.

A cirkulátort egy 50-50%-os sugárnyalábosztó (Beam Splitter – BS) követi, ami az impulzusokat kettéosztja és két külön út bejárására tereli őket. Egy ilyen BS-t a legcélszerűbben egy féligáteresztő tükör alkalmazásával valósíthatunk meg, ami az impulzusokat 50%-ban továbbengedi egy adott optikai szálon, míg a másik felét tovább

tükrözi egy másik szálra. Esetünkben a hosszabbik ágon egy 10 méter hosszú késleltető vezetéken keresztül vezetve a fényt (Delay Line – DL) elérjük, hogy 50ns lemaradást szenvedjen el „társához” képest. Ugyanezen az úton egy fázismodulátor (Phase Modulator – PM_B) segítségével $\frac{\pi}{2}$ fázistolást végezhetünk az itt áthaladó fényimpulzusokon, ám ezt a lehetőséget majd csak az Alice-tól való visszatükrözés után használjuk ki. A két kart egy polarizációs nyalábosztóba (Polarization Beam Splitter – PBS) vezetve az impulzusok kettéosztódva, 50ns időkésleltetéssel fogják egymást követni. Fontos megjegyezni, hogy amíg a rendszer minden optikai szála polarizációtartó, a rövidebb ágon áthaladó fény 90°-os polarizációfordulást szenved el, aminek majd később, az interferenciánál lesz fontos szerepe.

A fény útja innen egy hosszú (akár 50-100km-es) optikai szálon keresztül Alice-hoz vezet. Ennek a távolságnak a megvalósítása esetünkben szükségtelen, hiszen a protokoll működésén nem változtat. Egészen addig, ameddig a jel még megfelelő valószínűséggel észlelhető a fogadóoldalon, a távolság növelhető. Az inicializálás során alkalmazott folyamatok ugyanis a távolság függvényében állítják a megfelelő szintre a csillapítás és időzítés paramétereit. Praktikai okokból így egy rövidebb szál köti össze a küldő és fogadó felet.

Alice oldalára érve egy újabb nyalábosztó ($BS_{90/10}$) a beérkező impulzusok energiájának 90%-át egy lineáris detektorra irányítja. Ez a detektor szolgáltatja azokat az információkat, amelyek szükségesek a megfelelő csillapítási és időzítési paramétereket a rá becsapódó, nagy energiájú impulzusok alapján. A küldő ugyanis fázismoduláció segítségével fogja kódolni a bitjeit kvantumállapotokba, ehhez viszont szükséges tudnia, hogy mikor is kell ezt a modulációt végrehajtania. A detektorba érkező fény idejéből ezt ki is lehet számolni, energiájából pedig meghatározható a szükséges további csillapítás mértéke a maradék 10%-os fénycsomagokon. A BS-t elhagyva át is haladnak az impulzusok az erre a célra szolgáló szabályozható csillapítón (Variable Attenuator – VA), majd ezt követően beérnek egy hosszú, tároló elemként szolgáló 10 km-es optikai szálba (Storage Line – SL).

A SL-nak zajszűrő szerepe van [31]. A küldés során ugyanis sokféle zajjal találkozhatunk, ami növeli a QBER-t – ilyen a fény terjedése során, a szálakon való visszaszóródás is. A plug&play séma felépítéséből adódóan a Bobtól Alice felé közlekedő, nagy energiájú és az onnan visszaérkező, átlagosan kevesebb, mint 1 fotonos

impulzusoknak a rendszerben valahol találkozniuk kell. Ekkor, a számottevő energiakülönbség (megközelítőleg több mint 30dB) miatt a kis eséllyel ugyan, de megjelenő visszaszórt fény a gyenge jelimpulzusokhoz társulva hamis detekciókhoz vezethet, így a kvantum bithiba rátát csökkentve. Ezen a 10km-en oda-vissza 200ns-onként felsorakozva összesen 480 fényimpulzus „fér el", melyet egy frame-nek tekintünk. Ha Bob csupán egy ilyen impulzusvonatot küld ki és a következővel megvárja ennek visszaérkezését, akkor a fény csak Alice oldalán, a SL-ban fog összetalálkozni és nem a kommunikációs csatornában. Ez azért lényeges, mert ez a tároló szál az Alice-oldali csillapító után van elhelyezve, így az onnan visszaszóródó fény energiája jóval alacsonyabb és zajszempontból elhanyagolható. Az egy frame-ben küldhető impulzusok száma természetesen arányos ennek a szálnak a hosszával, viszont figyelembe kell venni, hogy egy adott hossz felett a szálból adódó csillapítás túlságosan magas lesz, megnehezítve Bob dolgát a rövid impulzusok küldésében, melyeknek ezzel együtt is szükséges elérniük a bizonyos 1 alatti (~ 0.4-0.6) átlagos foton számot.

A protokollból már csak a küldő-oldali fázismodulátor (PM_A) és egy Faraday-tükör (Faraday Mirror – FM) maradt hátra. A fázismodulátort vezérelve a kettéválasztott impulzusokból a másodikat moduláljuk, az elsőt pedig meghagyjuk Bob részére referenciának. Alice két különböző bázisból választhat a kódolás során véletlenszerűen, minden egyes impulzus esetén. Ennek segítségével vagy egy $0 - \pi$, vagy pedig egy $\frac{\pi}{2} - \frac{3\pi}{2}$ fázistolást eszközöl rajtuk, előre előkészített kulcsok alapján – a BB84-protokollban leírtak szerint. Bázisonként az első érték feleltethető meg 0-s, a második pedig 1-es bitnek. Ez a kódolt információ jut vissza Bobhoz, a Faraday-tükörről visszaverődve. A tükör fontos tulajdonsága, hogy polarizációfordító, így Bob oldalára érve a PBS ezúttal pont az ellenkező ágakra tereli a gyenge impulzusokat: a 90°-os polarizációs szálon a másik fél is áthaladva újra párhuzamos polarizációba kerülnek. Ez az interferencia miatt egy fontos kritérium, hiszen a protokoll a detektorokba érkező fotonok interferenciáján alapszik, így kiemelkedő fontosságú, hogy ez a művelet a lehető legtisztább, legláthatóbb legyen. Az interferencia két hullám között pedig akkor a legtökéletesebb, ha párhuzamos polarizációban és időben egyszerre találkoznak. Az első kritérium teljesülése a leírtak alapján egyértelmű, utóbbi pedig a Faraday-tükör miatti polarizációfordulás következtében alakul ki, hiszen mindkét fél ugyanazt az úthosszt járja be – amelyik odafelé a hosszabbik ágon haladt Bob oldalán, az visszafelé a

rövidebben fog és fordítva. A rendszer tehát auto-kompenzált, vagyis nem szükséges az interferenciára vezető időzítések felügyelete, hiszen a rendszer felépítéséből adódóan egyszerre érkeznek az impulzuspárok a BS-hez.

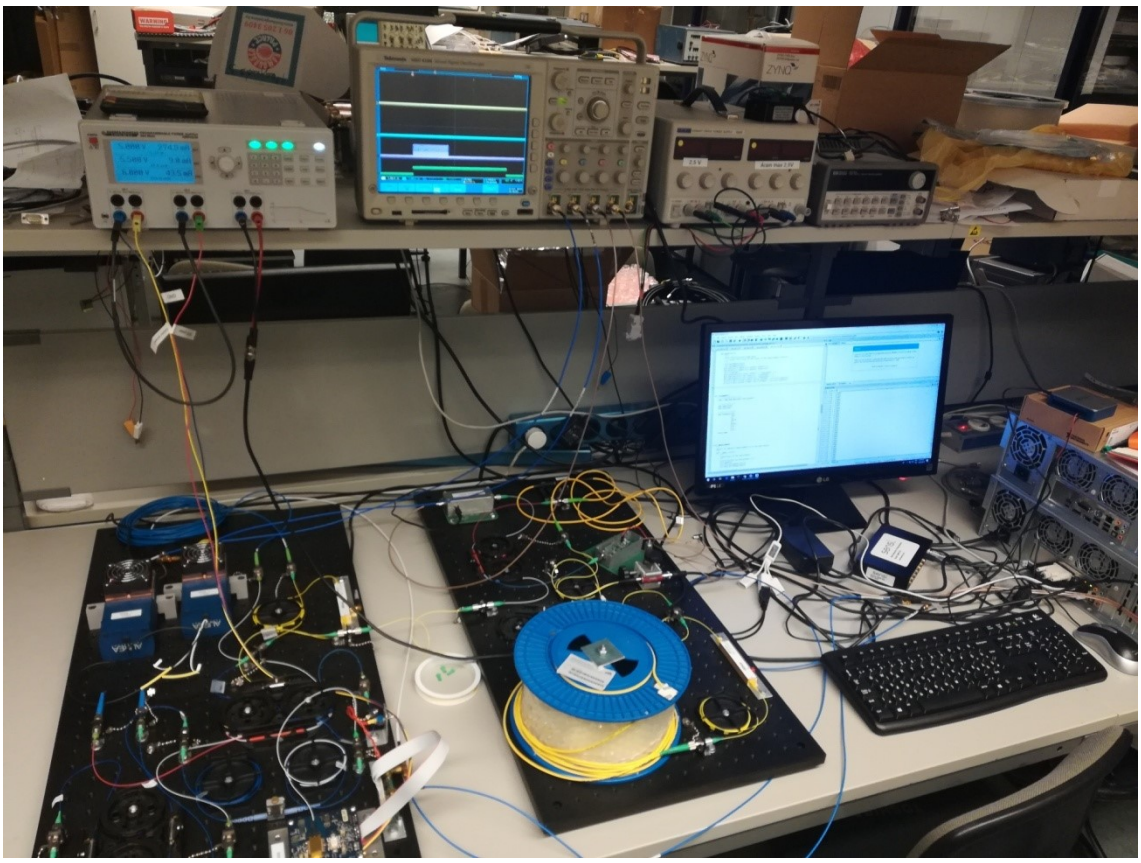
A titkos kulcs kialakulása az interferencia függvénye, ami pedig Bob bázisválasztásától függ. Ugyanis a hosszabb ágon visszaérkező referenciaimpulzuson Bob választhat, hogy 0, vagy $\frac{\pi}{2}$ fázistolást végez. Ez ekvivalens azzal, hogy Alice első, vagy második bázisában „méri meg" az általa kódolt állapotot. Ezek alapján a két fél impulzus az 50-50%-os BS csatolási pontján vagy megegyező fázisban van egymással – ekkor konstruktív –, vagy pedig ellentétesben – ekkor pedig destruktív interferenciáról beszélhetünk és vagy az egyik (SPAD1), vagy a másik detektorba (SPAD2) fog beérkezni. Ez a determinisztikus végkifejlet akkor következik be, amikor Bob eltalálja Alice bázisát. Ellenkező esetben teljesen valószínűségi alapon fog eldőlni minden egyes impulzus esetében, hogy éppen az első, vagy a második detektort fogja majd megszólaltatni. A detektorokat ugyancsak felfoghatjuk 0-s és 1-es bitként, attól függően, melyik észlel foton-beütést. Innentől már csak a beérkezett bitsorozat szokásos utólagos feldolgozása marad hátra, melyet Alice bázisainak klasszikus csatornán történő megosztásával el is lehet végezni.

Alice bitjei	**0**	**1**	**0**	**1**
Alice bázisai	0	0	$\pi/2$	$\pi/2$
Alice küldése	0	π	$\pi/2$	$3\pi/2$
Bob bázisa	0	$\pi/2$	0	$\pi/2$
Bob kiolvasása	0	1 (50%)	0 (50%)	1
Bázisegyeztetés	**jó**	**rossz**	**rossz**	**jó**
Titkoskulcs bitek	**0**	**-**	**-**	**1**

2. táblázat – Alice és Bob közötti titkoskulcs kialakulásának menete a bázisok váltakoztatásával – összefoglaló táblázat [30]

3.2 Vezérlés és előzmények

A megépített rendszerben jelenleg a Bob-oldali fázis-modulációt és a lézerimpulzusok generálását tudjuk vezérelni, amiknek segítségével működő foton-átvitel vizsgálható. Az SPAD-ok jelét egy digitális oszcilloszkóp segítségével tudjuk megjeleníteni, melynek mintavételező képessége (5GS/s) eléggé nagy ahhoz, hogy az impulzusok érkezésének idejét pár ns-os nagyságrenden belül vizsgálhassuk – hisz 200ps-onként képes a mintavételre. A Tektronix MSO 4140 „Mixed Signal Oscilloscope” 4 bemenetét is használatba vesszük, mégpedig a következőképpen: két csatornára a fogadóoldali SPAD-ok, a harmadikra a küldő-oldali lineáris detektor, végül, utolsó analóg csatornájára a triggerként szolgáló spektrum kártya jelét kötjük, azaz kezdő időpontnak (t_0) a lézer indítását vesszük.



4. ábra – A képen a QKD rendszer két panelje és a szükséges műszerek láthatóak, mint a 3 csatornás feszültséggenerátor, és a Tektronix MSO 4140-es digitális oszcilloszkópja.

A spektrum kártyát számítógépről, egy erre a célra megírt programmal vezéreljük („bob_gui_launcher.bat”). Segítségével beállítható az alkalmazott lézerforrás hullámhossza (1550nm) és frekvenciája (5MHz), ezen kívül a fényimpulzusok

szélessége is (20ns). A programban megadhatók a frame-ek paraméterei is, azaz, hogy hány fotonból álljon, mennyit várjunk két frame között, illetve persze az is, hány frame-et küldjünk. A Bob-oldali PM vezérlése feszültségszint és bitsorozat függvénye; egy darab 0-ás bitet választva például logikailag magas feszültségszint esetén 0°-ot, míg alacsony szint esetén 90°-ot tudunk modulálni az érkező fotonokon, s így az első, vagy a második detektorba érkező beütéseket ellenőrizhetjük az oszcilloszkópon.

A detektorok az Aurea Technologies lavinaeffektuson alapuló egyfoton diódás detektorai. A letörési feszültségnél nagyobb feszültség szintre záró irányban előfeszített félvezetőben már gyenge elektromágneses hullám (akár egyetlen foton) hatására is elindul egy önfenntartó, exponenciális lavina folyamat. A kinetikus energiára szert tevő, helyéről kilépő töltéshordozó lavinaáramot indít, amely pár milliamper nagyságrendűre is erősödhet. Ez egészen addig tart, amíg az előfeszítést el nem kezdjük csökkenteni addig, amíg a töltéshordozókat már nem képes a meggyengült elektromos mező ionizációs ütközések elérésére felgyorsítani – azaz egészen a letörési feszültség alá. A lavina kialakulásával párhuzamosan a detektor egy kimeneti feszültség-impulzust generál, így lehetővé téve a fotonok beérkezésének megjelenítését például egy oszcilloszkópon.

5. ábra – Az Aurea Technologies egyfoton detektorai

A lavinaeffektus lezajlása és csillapodása időt vesz igénybe. Ez azzal a sajnálatos következménnyel jár, hogy a detektor egy adott detekció után nem képes a további beérkező fotonokat azonnal észlelni. Ezt az időt „dead-time”-nak, vagyis holtidőnek hívjuk és t_d-vel jelöljük. Ezen kívül, mint minden eszköz, a SPAD is jellemezhető egy arányszámmal, a hatásfokkal. Ez a tényező esetünkben csupán 10%, ami azt jelenti, hogy minden 10 beérkező fotonból átlagosan mindössze 1-et képes

detektálni. Ha ehhez hozzávesszük a holtidejét is a detektoroknak, nem meglepő eredményként adódik, hogy egy frame 480 fotonjából pusztán 4-5 bitünk érkezik. Ha a teljes küldés idejét vesszük, ami közel 200μs, láthatjuk, hogy 1 milliszekundum alatt 20-25 bit, míg 1 másodperc alatt megközelítőleg 20-25kbit átvitelére van lehetőségünk. Utólagos feldolgozás után az átküldött bitek nagyjából 75%-a fel is lesz használható a létrejövő titkos kulcsunkhoz.

A fotonok beérkezésének feldolgozásához a másik út egy time-to-digital konverteren keresztül vezet, mely a Sense Light (SensL) terméke. Ennek a működése alapvetően kiváltja az oszcilloszkópon megjelenő impulzusok kezdeti eltárolását, hiszen digitális időbélyegeket szolgáltat a detektor által közvetített időpontokkor. Ennek a nagy felbontású konverternek a vezérlésére munkám során csak betekintést nyertem, s később, hibásnak vélt működése miatt a digitális oszcilloszkóp SensL-t helyettesítő alkalmazása mellett tettük le a voksunkat – így én is ezen az úton indultam el.

4 A rendszeren végzett munkák

Kezdetben az alapvető feladatom a digitális oszcilloszkóp által kijelzett fotondetekciók feldolgozása volt. Innen a kulcsok kialakításához feltétlenül szükséges szinkronizációs eljárás alapjául szolgáló „time tagging”, azaz időbélyegek meghatározása és a beérkező bitek sorszámozása következett, hogy meg tudjuk határozni egy adott beütésből, melyik frame-ben, hányadik bitként érkezett és mennyi a legelső bit előtti útidő, azaz a kommunikációs csatorna bejárásához szükséges idő. Végül pedig az Alice-oldali tároló szál hosszának mérésére került sor, amelynek elvégzése fontos információval szolgál a küldő oldali időzítések precíz kialakításához. Ezzel párhuzamosan pedig lehetőségem nyílt egy szabályozható csillapító segítségével megvizsgálnom az foton-detektálás és a csillapítás közti összefüggést.

4.1 Fotondetekció, feldolgozás

A fotondetekciók feldolgozásához mindenekelőtt szükséges volt az oszcilloszkópon megjelenített jelalakok kódjaimba történő átemelése, és ezzel együtt magának az eszköznek a szoftveres vezérlése. Munkám során Python 3.7 fejlesztői környezetben dolgoztam, az Anaconda Spyder felületét használtam. Első kódom során megismertem a Tektronix MSO 4140 márkájú digitális oszcilloszkóp vezérlését a hozzá tartozó programmer manual felhasználói összefoglaló alapján. Az oszcilloszkópot Etherneten keresztül értem el a számítógépről a National Instruments által fejlesztett NI-VISA program segítségével. Ebben a tesztkódban megtanultam, hogyan kell a műszer által ábrázolt függvényeket átemelni Pythonba pontonként, illetve azok ábrázolását is. Sikerült ezen kívül az oszcilloszkóp beállításaitól függetlenül meghatároznom a bemeneteire adott jel tényleges nagyságát, értékeit is. Az alábbi kódrészletben az oszcilloszkóp inicializálása látható.

```
import visa

#initialization
rm= visa.ResourceManager(visa_library='C:\\WINDOWS\\system32\\visa32.dll')
resources = rm.list_resources()
print(resources)

instr = rm.open_resource('TCPIP::172.29.249.180::INSTR')
print(instr.query('DATa:ENCdg?'))
```

Ez alapján a modul alapján megírtam a „meas_obj_4000.py” programkódot, amiben már strukturált formában létrehoztam egy „mso” és egy „measurement” osztályt. Előbbi az oszcilloszkóp pythonos interfészének felel meg, míg utóbbi egy adott mérés elvégzésére szolgál. Ebben a kódban megoldottam a beolvasott pontok tárolását és azok feldolgozását oly módon, hogy egy TXT file-ba kiírva őket rendezett módon, majd onnan kiolvasva meghatározható legyen a közel egy helyre eső feszültségimpulzusok várható érkezési ideje. Az impulzusokat a programban úgy kerestem meg, hogy minden pontnak adtam egy logikai „high” vagy „low” értéket és ahol felfutó élt tapasztaltam, azt számításba vettem. Innen meg tudtam határozni az impulzusok érkezési idejét, majd onnan az összesített adatokból egy adott bit beérkezésének várható időértékeit is. Tesztelési célzattal egy jelgenerátor négyszögjelét használtam. A különböző frekvenciákon való mérések során a négyszögjel felfutó éleit a mérési intervallumon belül helyesen gyűjtötte ki a program.

Következő lépésként szerettem volna szimulálni a tényleges összeállításban a detektorban keltett jeleket. A fotonok beérkezésének detektálását a legjobban Gauss-eloszlással lehet közelíteni. Egy adott egyfotonos fényimpulzus burkolóján belül ugyanis a fotonunk bárhol elhelyezkedhet a becsapódás pillanatában. Egy 20ns széles impulzusban például legvalószínűbb, hogy 10ns-nál (a felénél) detektáljuk, de az is meglehet, hogy pár ns eltéréssel ez előtt vagy után. Sok frame küldése esetén, az ugyanazon a helyen küldött kvantumbitek (pl. minden 480-ból a 42.-ek) egy Gauss haranggörbe szerint fognak beérkezni. Ennek kipróbálására létrehoztam egy újabb tesztkódot, ahol a numpy könyvtár random.normal() függvényét használva a valósághoz közeli értékeket szimuláltam, ezeken is tesztelve az előző programkódot.

Annak érdekében, hogy megpróbáljam minél jobban szimulálni a QKD rendszer frame-jeit, nekivágtam a zajjal együtt generált érkezési adatok létrehozásának és onnan a zajok kiszűrésének – felhasználva a „meas_obj_4000.py” kódban foglalt várható érték számítást is. A simulation osztályban sikeresen tudtam szimulálni a fix raszterre érkező fotonokat, melyeknek file-ból való feldolgozásaként visszakaptam azok várható értékét (raszterpontokat). A meglévő raszter segítségével pedig már meg tudtam határozni a zajból származó impulzusokat is. A raszterpontok körül (20ns-os immpulzusokat vizsgálva) egy $\varepsilon = \pm 10$ ns széles intervallumon kívülre eső impulzus nem lehet más,

mint zaj (pl. sötét zaj – „dark count”). Ez a programkód a „frame_simulation.py” nevet kapta.

Mind a „meas_obj_4000.py”, mind pedig a „frame_simulation.py” az elvártak szerint működik, ám az előbbi egy általános jelre általános megoldást kínál, így nem használható az elrendezés által felvetett konkrét problémák megoldására, értékek kiszámítására. Utóbbi pedig csupán egy szimuláció az elrendezés közelítésére – itt már ugyan zajszűrést is használva. Megoldásként a két kód összeillesztését választottam, létrehozva a „pulse_detect_proc.py” programkódot, melyet először – a rendszerben alkalmazott 5MHz helyett – 1MHz-es négyszögjelekre teszteltem, ahol a megegyező biteknek megfelelő érkezési helyek körül az éleket kézzel állítottam, a zajt pedig továbbra is szimuláltam. A teszt eredményes volt, hiszen a különálló zajokat sikerült visszaadnom, az egy kupacban csoportosuló „impulzusokra” pedig a várható érkezési időpontokat megkaptam.

Végül magán a rendszeren is lefuttattam a programomat, ahol több észrevétel is adódott. Egyfelől a valós, fotonok által keltett impulzusokat és azok érkezési idejét tökéletesen rögzíti és file-ba menti a kód, azonban a várható érték meghatározásához nagyon sok mérési adatra van szükség. Minthogy a program megírása során ideális feltételeket szabtam (480 fotonos frame-ekkel számolva), a gyakorlati megvalósítás esetén beérkező frame-enkénti 4-5 kvantumbit detektálása nagyon kevés. A sok frame kiküldése a „bob_gui_launcher.bat” vezérlőprogramnak a kezelőfelület szempontjából nem jelent akadályt, az eddig a pontig létrehozott kódjaimban való használathoz viszont a hozzá tartozó Python kódot át kellett alakítani.

4.2 Time tagging

A korábbi próbálkozásnál jobb módszernek tűnt minden impulzus-tömörülés külön álló vizsgálata helyett ezt egyben megtenni. Az elképzelés az volt, hogy minden impulzus érkezési idejét leosztjuk modulo 200-zal (hiszen 5MHz-cel indítjuk őket útnak a lézerből), így megkapva egy 0-199 között, egyetlen érték körül csoportosuló időket, melyek várható értéke már pontosan az az érték lesz, ami megmutatja, hogy a 200ns-onként érkező bitek mikor érkeznek ezen az intervallumon. Innentől már csak egy rács felállítása szükségeltetik, méghozzá elindulva a kapott várható értéktől (ez lesz az első foton érkezési ideje) megkapva a rácspontokat az alábbi formulával, ahol $n =$

$1,2,3,\dots,480$ és T_0 az átvitel ideje megegyezik az első foton érkezésének és a lézer indításának különbségével:

$$t_{érkezés} = (T_0 + n \cdot 200)ns = [(t_1 - t_0) + n \cdot 200]ns.$$

Erre a megoldásra is igaz, hogy minél több frame-et küldünk, annál pontosabb eredményt kapunk a rácspontok helyzetére a várható érték számításakor. Emellett a bitek érkezési idejének 200-as modulóval való kongruencia eredménye azt is megadja, hogy hányadik frame-ben érkezett az adott bit. A zajszűrés módja pedig továbbra is ugyanaz, mint eddig: ami a rasztertől tolerálható távolságon kívül esik, sötét zajnak minősíthető.

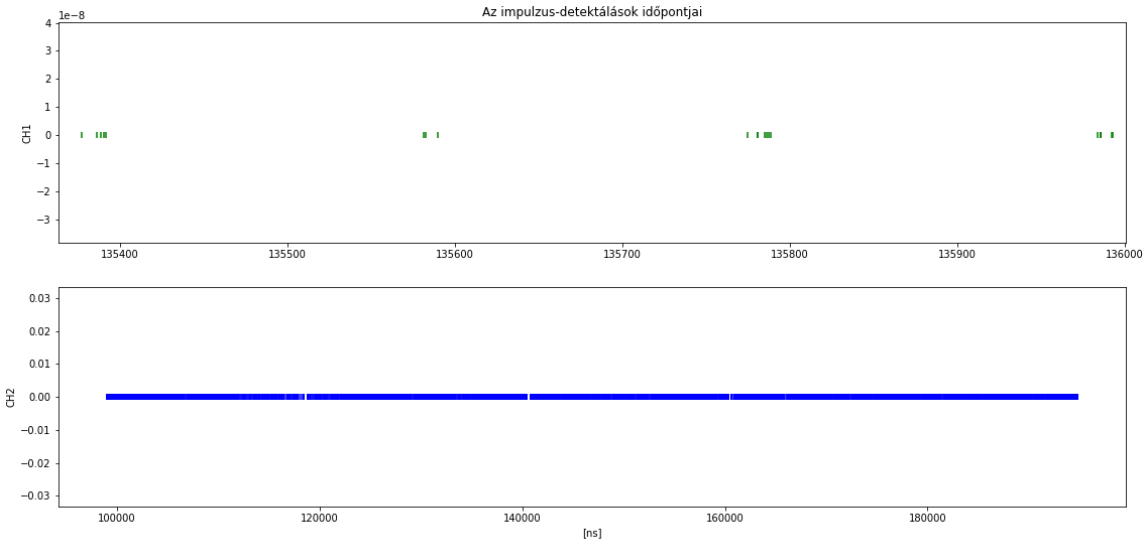
Ezt a változatot is implementáltam a kódomba, azonban a futtatás során fény derült a metódus egy apró hibájára. Ha ugyanis végiggondoljuk, hogy egészen pontosan mit is csinálunk a 200-as modulóval való kongruencia számításával, rájövünk, hogy bár elméletben minden stimmel, a gyakorlatban alkalmazva viszont problémába ütközünk, méghozzá a csatorna változó hossza miatt. Ez a program ugyanis, funkcióját tekintve elsősorban egy újonnan felállított rendszer első használata előtti inicializációs eljárás része. Feladata, hogy egy ismeretlen csatornahossz esetére meg tudja mondani, hogy a küldéstől számítva pontosan mennyi idő elteltével számíthatunk a fotonok visszaérkezésére, azaz, hogy mennyi idő múlva érkezik majd meg az első bit. Ez a csatornahossz viszont minden rendszernél más és más, de akár két napszak között is változhat a hőmérsékletváltozás hatására. Így a trigger – lézer indítása – után a beérkező impulzusok érkezési idejéből nem fogjuk tudni egyértelműen meghatározni kongruencia számításával sem, hogy melyik volt közülük az első, illetve, hogy jelbit volt-e egyáltalán, vagy csak zaj. Hiszen a kommunikációs csatorna számítására alkalmazott különbség $(t_1 - t_0)$ eredménye 5MHz-es küldési frekvenciával számolva már akkor negatív lenne a kongruencia számítása után, hogyha 200ns-nál hosszabb időbe telne a fénynek a rendszer bejárása. (Esetünkben ez közel 200μs!)

Így tehát egy harmadik, még kifinomultabb és körültekintőbb megoldást kellett választanom. Ilyen megoldás például a detekciók kirajzoltatása és függvényként való kezelése. Onnantól kezdve, hogy nagyon sok mérést végzek a rendszeren, egy idő után összegyűlik mind a 480 bit várható helyénél legalább egy, de inkább több beütés. A tömörülésekre alkalmazva a várható érték számítását, itt is kiszűrhetők a hamis detekciók. A megmaradt impulzusok eloszlása – elegendő mérési eredmény

feldolgozása után – kiad egy „szinuszos” burkolót Gauss-görbék sorozataként. Ha ezt, mint függvényt tekintem, akkor periodikus függvényként alkalmazhatunk rá FFT-t, azaz folytonos Fourier-transzformációt.

Ennek eredményeképpen meg is kapjuk a detektálás frekvenciáját. Ez az érték meglepően nem triviális. Annak ellenére, hogy a lézerforrást periodikusan gerjesztjük 5 MHz-en, a detekció-feldolgozás pár ppm nagyságrendben eltérhet ettől az értéktől. 480 foton detekciója esetén pedig ez a hiba összegződik, rossz eredményekre vezetve minket. Tehát, ha mérőeszköztől függetlenül (oszcilloszkóp / SensL konverter) szeretnénk minél pontosabban mérni, kénytelenek vagyunk az FFT módszeréhez folyamodnunk. A frekvenciából már generálható egy rács, amit ráilleszthetünk a függvényünkre. Ha a rács és a függvényünk korrelációja a legnagyobb értéket adja eredményül, akkor meg is kaptuk a bitjeinket – és velük együtt az első bit érkezési idejét is. Ekkor már alkalmazható a $(t_1 - t_0)$ a csatorna hosszának számításához.

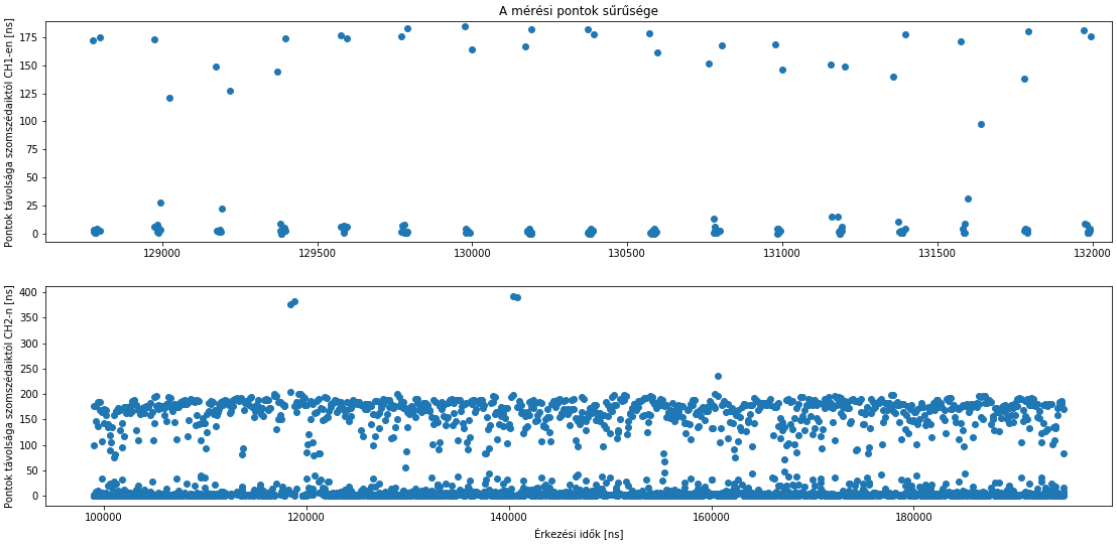
Az oszcilloszkópot használva azonban hiába engedné bármelyik kód, hogy rövid idő alatt sok frame-et futtassak és azok eredményét fel is dolgozzam, az Etherneten keresztül csatlakoztatott műszer pontjainak kiolvasása is időigényes. A qkd_bob modul használata lényegesen leegyszerűsítette ugyan a méréseket, az oszcilloszkóp adatainak átemelését viszont ilyen módon nem lehet rövidíteni. Minden egyes frame feldolgozása közel 2 másodpercbe telik.



6. ábra – Az impulzus-detektálások időpontjai az oszcilloszkóp 1-es és 2-es csatornájának adatai alapján, 1000 frame küldése esetén. Az idők [ns]-ban vannak ábrázolva, CH2-n a teljes idősáv

látszik a SPAD2 által detektált összes impulzussal, míg CH1-en a teljes idősáv egy kinagyított része – jól megfigyelhetőek a közel 200ns-onként jelen lévő impulzus-sűrűsödések

Végül a legelső módszerhez hasonló megoldást választottam. Ezer frame kiküldésére vállalkozva, „01”-es ismétlődő bitsorozatot küldve mind a két detektorba közel egyenlő aránnyal érkeznek beütések, így duplázva a detektálások mennyiségét. Ezeket az egymástól való távolságuk alapján csoportosítottam hamis, illetve valós bitekre. Ezzel a módszerrel pár bitet elveszthettem ugyan (vegyük például egy adott hely körül csoportosuló impulzusok közül a szélsőket), de minthogy jelen esetben a time-tagging kialakítása és nem a biztonsági kulcshoz szükséges maximális bitszám megőrzése a cél, ettől a kis veszteségtől eltekintünk. A valós bitek érkezésének az átlagát csoportonként véve kaptam egy egyenetlen rasztert. Ez a raszter több helyen hiányos is volt, hiszen nem minden helyre érkezett beütés, vagy sok helyen csupán egyetlen detekciót lehetett felfedezni – ez utóbbiak a szomszédjaiktól való nagy távolság miatt eleve kiestek a csoportosított bitek közül.



7. ábra – A mérési pontok távolságai szomszédjaiktól CH1-en és CH2-n. Minél kisebb a távolság, annál inkább vannak közel egymáshoz. Az 50ns alatti távolsággal rendelkezők jól elkülöníthetőek a nagyobb kitérésektől, melyek zajnak, vagy egy csoport szélső bitjeinek tekinthetőek. Az alsó diagram a CH2 teljes időtartományát ([ns]-ban), míg a felső a CH1 egy nagyított szakaszát mutatja.

Az így kapott, nagyjából 200ns-onként elhelyezkedő átlagos időpontokból páronként különbséget képezve eredményül sok, 200 körüli értéket kaptam, aminek újra az átlagát vettem. Ez az átlag pedig már nem más, mint egy elég jó közelítés a

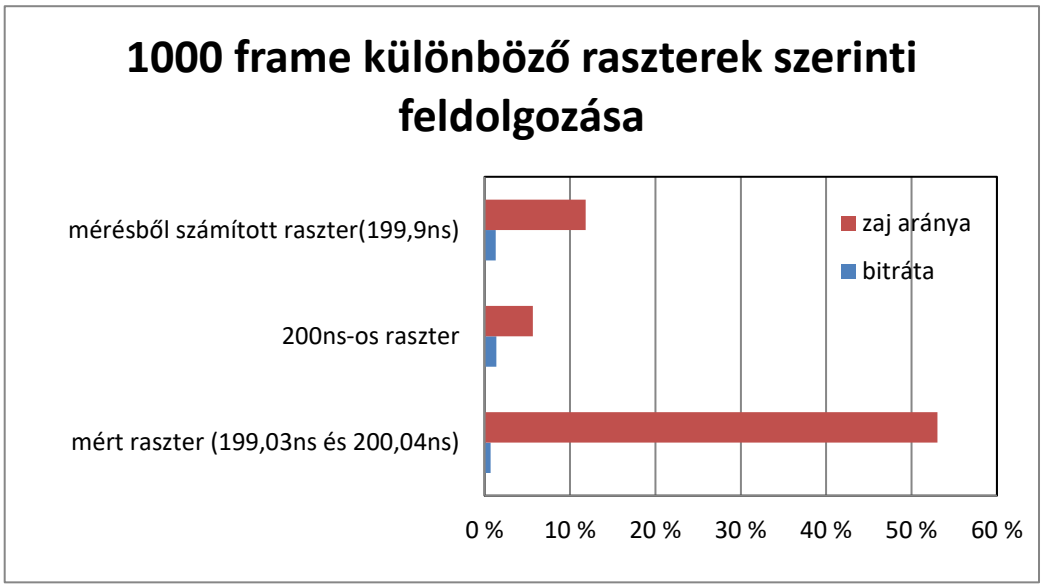
detektálás valódi rács periódusidejére. A program futtatása után kapott periódusidő a CH1 és CH2 csatornán detektált impulzusokra rendre 199,03ns és 200,04ns adódott. Látszik, hogy jó közelítés, hiszen az 5MHz-es küldő frekvencia periódusidejéhez nagyon közeli értékeket kaptam, azonban a módszer pontatlansága is megmutatkozik a két csatorna közti különbségben. Ez alapján a két érték alapján egy 480 elemből álló rácsot készítettem, melyet a beérkezési időkből számított átlagokra illesztettem, hogy a lehető legpontosabb várható érkezési időket kapjam a kettő korrelációjából. Ahol az átlagok eltérése a rácstól minimális, ott a periódusidő megadja, hova várhatóak a fotonjaink a legnagyobb valószínűséggel. Mivel az első bit detektálásának van a legnagyobb esélye, így 1000 küldött frame esetén biztosan detektálunk belőle elegendőt ahhoz, hogy az első impulzustömörülést betudhassuk az első bitek érkezésének. A rács illesztéséhez annak első pontját így az első tömörülés átlaga körül léptettem, 1ns-os léptékben.

A beérkezett adatokat ez alapján a várható érkezési rács szerint feldolgozva már könnyen eldönthető, hogy egy adott impulzus zajtól származik-e, vagy a küldött frame egy bitje – a meghatározott intervallumon kívülre vagy belülre esik. De mennyi is ez az intervallum? A korábban említett ±10ns nagyszerű közelítés, ha a fényimpulzusok burkolóin belüli foton detektálása pillanatában kialakuló maximumát vesszük. Azonban ezres, vagy nagyobb nagyságrendű frameküldések esetében, hosszú optikai szálas összeköttetéseknél már tapasztalható egy ettől eltérő szórás is a fény beérkezésének idejében, ami rendszerünkben a 10km-es szál és a frame-ek korrelálásának tudható be. A fotonjaink emiatt egy ±25ns-os sugáron belül, egy 50ns-os intervallumban találhatóak a várható érkezési idők körül. Ezt alapul véve a küldött bitek 0,6849%-át (frame-enként 3,29 bit) tudtam beazonosítani, ami 10%-os detektálás és 20µs-os holtidő mellett nem rossz arány, bár hozzávéve azt is, hogy a detektált impulzusok nagyjából felét (53%) zajnak könyvelte el a program, már nem annyira fényes eredmény.

Tovább finomítva a dolgot, a detektált impulzusok és a meglévő programkód alapján egy „finomhangolást” végeztem a rácson. Most nem a csoportok átlagaiból alakítottam ki a beérkezés periódusidejét, hanem a küldési frekvenciából kiindulva. A kiszámolt átlagok korrelációját most különböző periódusidejű rácsokkal vizsgáltam: 199 és 210ns között, 0,3ns-os lépésközzel változtattam annak értékét. Így számoltam a létrejövő rácsoktól való távolságok minimumát. Ennek a módszernek a nagymértékű

pontosságát mutatja, hogy a két csatornán létrejövő raszter pontjainak távolsága immár megegyezett, értéke 199,9ns volt. Ez azt mutatja, hogy az ideális raszter – a mért adatok alapján – 199,75 és 200,05ns között helyezkedik el. Ismét elvégezve az impulzusok feldolgozását, most dupla hatékonysággal működött a programom: 1,286%-os fogadott bitráta mellett mindössze 11,8%-os zajszintet jelezve.

Érdekességként a mért adatoktól teljesen függetlenül, kereken 200ns-mos periódusidővel felállított raszterrel is teszteltem a programot, ami így még egy fokkal jobb eredményt hozott (1,376% a fogadott bitekre és mindössze 5,66% a zajszintre). Ez azt mutatja, hogy ez a módszer is sokkal effektívebben működik, ha még ennél is több frame-et használunk fel a rendszer kezdeti értékeinek meghatározásához.



8. ábra – A grafikon három különböző módon előállított raszter szerinti fotondetektálás feldolgozásának eredményét mutatja be, „01”-es ismétlődő bitsorozatú frame-ek küldése esetén

A legjobb közelítésként szolgáló 200ns-os raszter illesztése után kapott várható érkezési idő az első bitre CH1-en 99009,4ns, azaz 99,0094µs, míg CH2-n 99,0198µs. Ez azt jelenti, hogy az egyes detektorra (SPAD1) a lézer indítási parancsának kiadása után 99,0094µs-mal a legvalószínűbb, hogy az első kiküldött bit megérkezik. Ezáltal – a 25ns-os bizonytalanságot is beleszámolva – a küldés után legkésőbb 98,7594µs-mal már biztosan élesíteni kell a detektorunkat a bitek biztonságos fogadásához. Sokkal előbb viszont nem érdemes, s így, egy pontos raszternek köszönhetően csökkenthető a zajból származó detekciók aránya. A két csatorna első bitjének érkezése közti különbség a rendszerben helyet kapó cirkulátor 2m-es szálhosszának is betudható lehetne, ami pont

10ns-mal növeli meg az egyik detektorra érkező fotonok útidejét. Sajnos azonban pont fordítva kéne adódnia az időknek, hogy azt lehessen mondani, ennyire pontos a módszer. A módszer hibája (ennyi adat esetén) ebből adódóan megközelítőleg 20ns.

4.3 SL mérése

A projekt tovább haladásához fontos feladat, hogy az Alice oldali hosszú tároló elméleti hosszának pontos, gyakorlati kimérhetősége. A küldő ugyanis az egymást 50ns-mal követő két impulzus közül csak a másodikat modulálhatja, a 3.1-es fejezetben leírtak alapján. Ez azt jelenti, hogy 20ns széles impulzusokkal számolva maximum 30ns időintervalluma lesz a PM_A vezérlésének, amibe „bele kell találnia" a moduláció elindításával. Ehhez egy nagyon pontos időzítési mechanizmus szükséges, melynek része az is, hogy bármikor meg tudjuk határozni az Alice-oldali úthosszat a lehető legpontosabban. Ezen a panelen pedig a SL – 10km-es hosszával több nagyságrenddel a többi elemhez tartozó optikai szál fölé nőve – hosszváltozása a meghatározó tényező, amitől az időzítés pontossága függ.

Célom az volt, hogy egy vezérlő kódot írjak, melynek futtatásakor a SL mérése megtörténik. Ilyenkor a Bob oldali detekció nem is lényeges, a detektorokat ki is kapcsolhatjuk, a csillapítás értékét csökkenthetjük. Ez utóbbi művelet azért is fontos, mert az SL hosszát két lineáris detektor segítségével mérem meg. Az egyik a már ismert D_A, amelybe a küldő oldali BS a fotonok energiájának a 90%-át irányítja. A másik pedig egy teljesen ugyanolyan lineáris detektor, amit az említett nyalábosztó eddig üresen hagyott kivezetésére kötünk.

A két detektor jelét oszcilloszkópra kötve, majd azon keresztül Pythonban a már megírt kódok segítségével analizálva a beérkező fotonok idejét (természetesen elég mindkét detektor esetében az első foton idejét megmérni), különbségük megadja az Alice oldali úthosszt. Mivel 1 métert nagyjából 5ns alatt tesz meg a fény optikai szálban, a SL-on kívüli szálak hossza pedig nem haladja meg ezt a távolságot, ha ezt a kis időt (vagy biztonsági okokból a kétszeresét) később ráhagyjuk a moduláció időpontjára kapott értékre, a SL idejét vehetjük az Alice oldali úthossz idejével megegyezőnek. Ezzel együtt a ráhagyással együtt is beleférünk még a 30ns-os keretünkbe.

A két detektor által felfogott 480-480 impulzus jeléből elég csak az elsők különbségét venni a két detektor között eltelt idő kiszámolásához. Annak érdekében, hogy megkapjuk a tároló szál pontos hosszát, nem kell mást tenni, mint még egy frame-et kiküldenünk – ezúttal a SL nélkül. Az elrendezésben a tároló hiányától eltekintve minden ugyanaz. A két detektoron megjelenő első impulzusok különbségét kivonva az előző útidőből pontosan a SL útidejének értékét fogjuk megkapni – kétszer. Ugyanis a Faraday-tükörről visszaverődve a kérdéses szálon kétszer fog áthaladni a fény, mire a másik detektorhoz ér. Az egymódusú optikai szálban a fény terjedésére – 1,467-es törésmutatót véve alapul – $2{,}04499 \times 10^8\, {}^{m}/_{s}$ -os sebesség adódik. Innen már számolható a szál hossza is.

Három mérést végeztem, 2 órás időközönként, dél és koraeste között. Az első két mérés szobahőmérsékleten, az utolsó már nyitott ablak mellett történt, így finoman szabályozva a szál hőmérsékletét is. A mérés eredményeit a 3. táblázatban foglaltam össze, amiben jól látszik az optikai szál hőmérsékletre való érzékenysége is.

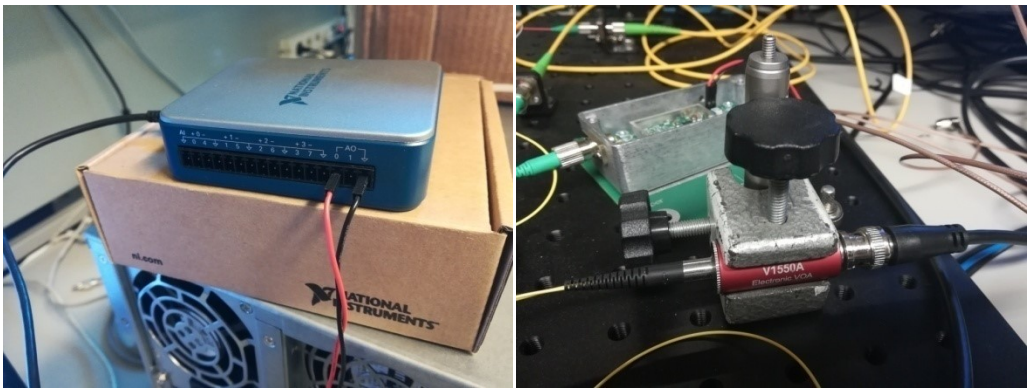
Mérés időpontja	**Tároló szál hossza**
12:23 – légkondicionáló nélküli szoba	10046,6258m
14:26 – napos idő, szoba melegszik	10046,8712m; $\mathbf{\Delta l = +24,54cm}$
16:30 – nyitott ablak, lehűlés	10046,7893m; $\mathbf{\Delta l = -8,19cm}$

3. táblázat – SL hosszváltozásának mértéke szobahőmérsékleten

A táblázatból kiolvasható, hogy a mérés során fellépő hosszváltozás a cm-es nagyságrendbe esik, amely egy 10km-es szál esetén elenyésző, 1-2ns-os bizonytalanságot ad hozzá a fotonok érkezési idejéhez. Emellett kiemelendő még az a tény, hogy az optikai szál gyártója fél százalékos hibahatáron belül volt képes előállítani a kommunikációhoz szükséges passzív elemet.

5 Fotondetekció függése a csillapítástól

A rendszeren végzett munkák során lehetőségem adódott egy küldő oldali, feszültséggel vezérelhető csillapító megismerésére és felhasználására. A felépítésben említett VA két különböző módon működő csillapító eredő csillapítását jelzi. Mindkét csillapítás változtatható, azonban a Thorlabs V1550 elektromos VOA-ja (Variable Optical Attenuator) az NI USB-6001-es I/O eszköz használatával programozható is, legalábbis ez utóbbi DAQ-mx driveréhez (Data AQuisition) tartozik Python modul is (nidaqmx).

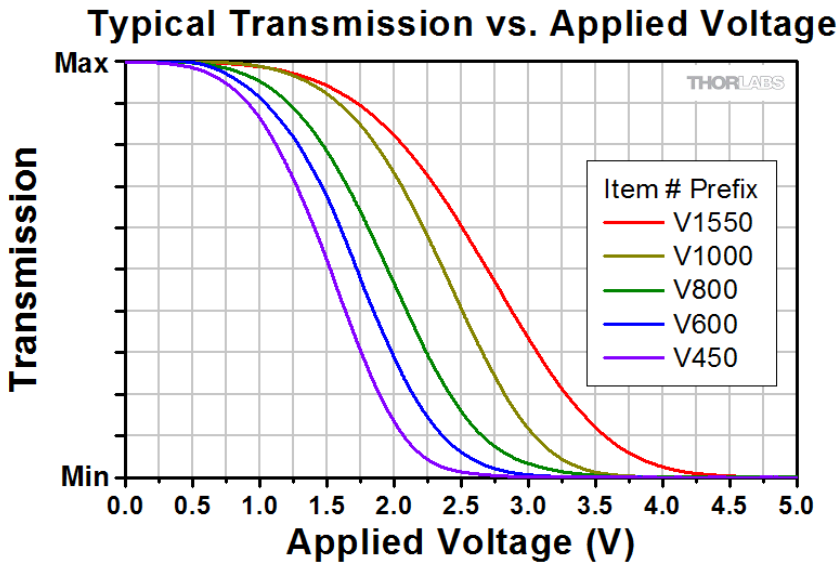


9. ábra – Balra látható az NI USB-6001-es I/O eszköz, míg a jobb oldali képen a Thorlabs V1550 elektromosan vezérelhető optikai csillapítója látható

Ez a multifunkcionális USB eszköz sok egyéb tulajdonsága mellett képes egy soros porton analóg feszültséget generálni ± 10 V-os tartományban. A két analóg csatornáján 5 kS/s-os rátában képes a vezérlés által megszabott feszültségszintek előállítására, mely akár egy megadott függvény szerint is változhat. Egyenfeszültséggel való gerjesztés hatására a VOA elkezd lezárni. Durván 2 és 3,5V között lineárisnak tekinthető a karakterisztika, 4V felett pedig már maximális csillapítással rendelkezik, nem enged át fotont. Figyelni kell ugyanakkor arra, hogy habár Zener diódás védelemmel van ellátva, vezérlése során maximum 5V-tal gerjeszthető.

Egy QKD rendszert átviteli tulajdonságai közül leginkább a QBER és a kvantum kulcsráta jellemez. Ez utóbbi hatalmas mértékben függ a kommunikációs csatornában fellépő csillapítástól, hiszen nagy csillapítás esetén a gyengülő EM hullámok detekciója igencsak nehézkessé válhat, s az átvitel távolságát is behatárolja. Mégis, az egyfoton

átvitelén alapuló kulcsszétosztó protokollok legfőbb erőssége, hogy az átvitelt lehallgatni próbáló fél minden beavatkozása észlelhetővé válik a hirtelen megugró kvantum bithiba-arány következtében. Ehhez viszont egyfotondetektorok is szükségesek, amelyek nagyobb energiájú beérkező fény esetén hibás működést is produkálhatnak.

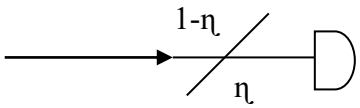


10. ábra – A Thorlabs V1550 VOA csillapítójának ideális karakterisztikája piros színnel látható [32]

Az Alice oldali VOA-ban rejlő lehetőségeket kihasználva megvizsgáltam az átvitel QBER és kulcsráta jellemzőit a csillapítás függvényében. A tesztelés matematikai hátterét és eredményeit a következő két alfejezetben foglaltam össze.

5.1 Matematikai háttér

Egy véges hatásfokú detektorral mért, koherens állapotú fény beütésszámának számolásának levezetéséhez mindenekelőtt készítsük el a SPAD detektoraink modelljét:



Jelölje $0 \leq \eta \leq 1$ a detektor hatásfokát, mely esetünkben $\eta = 0{,}1$. Vegyük figyelembe azt is, hogy $N \geq 1$ fotonszámú hullámcsomag esetén is csak 1 beütést ad az eszköz! A koherens kvantumállapotú, N-fotonos lézerimpulzus a következő formulával írható le, ahol $|\alpha|^2 = \bar{N}$, a fotonszám várható értéke:

$$|\,\alpha\,\rangle = e^{-\frac{|\alpha|^2}{2}} \cdot \sum_n \frac{\alpha^n}{\sqrt{n!}} |\,n\,\rangle$$

A foton-statisztika Poisson-eloszlást követ. Az n-fotonos állapot valószínűsége:

$$P_n = e^{-|\alpha|^2} \cdot \frac{|\alpha|^{2n}}{n!}$$

A detektor-veszteséget modellező nyalábosztó egy $|\,n\,\rangle$ foton-állapotból k darabot küld a detektor felé, (n – k) pedig elvész. Ez egy binomiális eloszlással írható le:

$$P_{k,n-k} = \binom{n}{k} \eta^k (1-\eta)^{n-k}$$

Ha Poisson foton-statisztikája van a bejövő fénynek, akkor a nyalábosztó kimenetén megjelenő fény-fotonszám eloszlása:

$$P^{(n)}{}_{k,n-k} = e^{-|\alpha|^2} \cdot \frac{|\alpha|^{2n}}{n!} \cdot \binom{n}{k} \eta^k (1-\eta)^{n-k} = e^{-\bar{N}} \cdot \frac{\bar{N}^k \cdot \bar{N}^{n-k}}{k!\,(n-k)!} \cdot \eta^k (1-\eta)^{n-k}$$

Ha az így kapott egyenletet n-re összegezzük, megkapjuk az ideális detektorra érkező fény foton-statisztikáját:

$$P_k(\eta) = \sum_{n \geq k} P^{(n)}{}_{k,n-k} = e^{-\bar{N}\cdot\eta} \frac{(\bar{N}\cdot\eta)^k}{k!} \cdot \sum_{m=n-k} e^{-\bar{N}\cdot(1-\eta)} \cdot \frac{\left(\bar{N}(1-\eta)\right)^m}{m!}$$

Mivel $\sum_{m=n-k} e^{-\bar{N}\cdot(1-\eta)} \cdot \frac{\left(\bar{N}(1-\eta)\right)^m}{m!} = 1$, adódik, hogy:

$$\boxed{P_k(\eta) = e^{-\bar{N}\cdot\eta} \frac{(\bar{N}\cdot\eta)^k}{k!}}$$

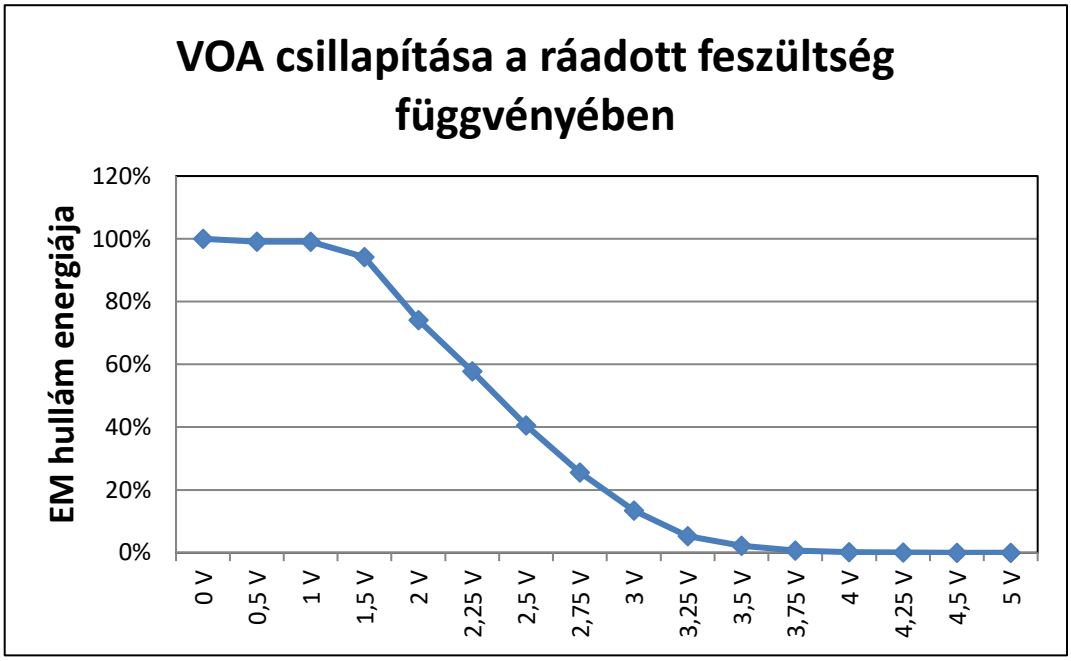
A foton-statisztika egyenletéből most már kiszámolhatjuk a számunkra érdekes valószínűségét annak, hogy a beérkezett impulzusban legalább 1 foton érkezett. (Azért lényeges a „legalább” szócska, mert ahogyan arra a levezetés előtt felhívtam a figyelmet, a detektor 1-nél több fotonos impulzusok esetén is csupán egyetlen foton érkezését tudja jelezni. Emiatt ahhoz, hogy detekciónk legyen, 1 vagy annál több fotonnal rendelkező impulzusok érkezését vizsgáljuk.)

$$P_{n\geq 1} = 1 - P_0 = 1 - e^{-\eta\bar{N}} \approx \eta\bar{N}$$

A közelítés kicsi fotonszám és kicsi hatásfok esetén engedhető meg.

5.2 Mérési eredmények

A változtatható optikai csillapító hatását 16 különböző feszültségszint mellett vizsgáltam meg 0 és 5 Volt között. Először is teljesítménymérővel megmértem, mekkora csillapítást ad ezekre a gerjesztésekre, decibelben. Ez alapján azt is ki tudtam számolni, hogy ha gerjesztetlen állapotban éppen egyfotonos energiaszintre csillapodnak az impulzusok a Bob oldali detektorokhoz érve, akkor ezen csillapítás értékek mennyivel csökkentik egy impulzus várható fotonszámát. Ennek eredménye éppen a csillapító karakterisztikáját kell, hogy visszaadja, amit a 11. ábrán szemléltetek.



11. ábra – A lézerimpulzus fogadóoldali beérkezésekor vett egyfotonos energiája 100%

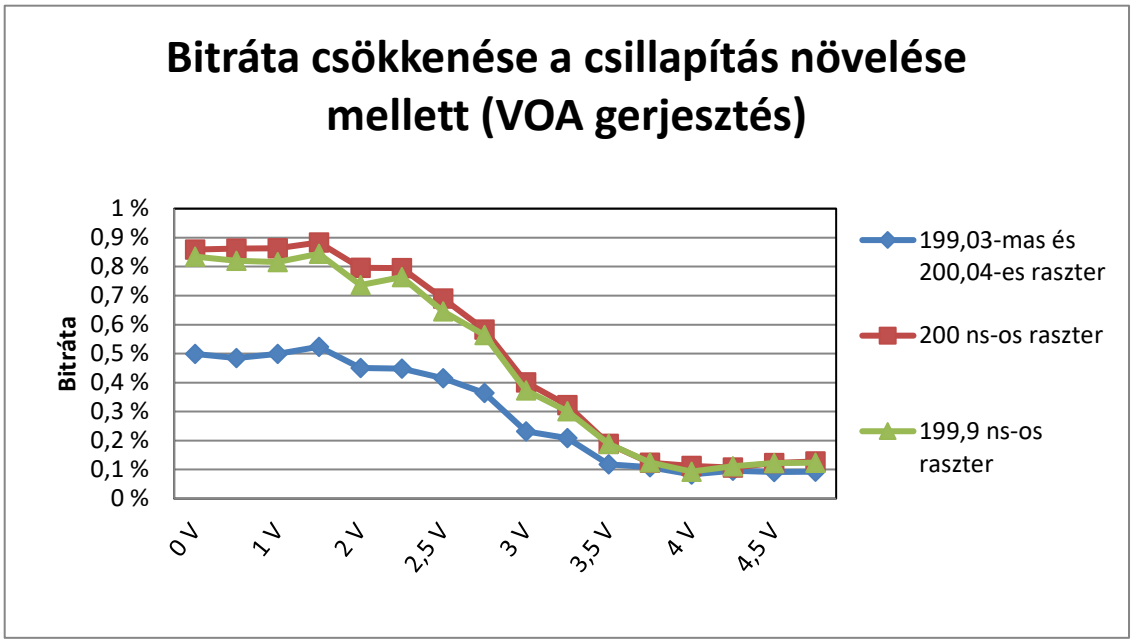
A 11. ábra szépen összevethető a 10. ábrán felvázolt karakterisztikával. 4V-os feszültségszint felett már szinte teljesen lezár a csillapító, így a Bobhoz érkező impulzusok jóformán kizárólag csak az átvitel zajából származnak. Az ugyanezen az ábrán is jelölt feszültségszintek mindegyike mellett 150 frame küldését figyeltem meg, egyszerű, „1”-es bitek esetén. Ebben az esetben csakis az egyik detektor jele hordozza az kódolt tartalmat, a másikra érkező beütések egészen biztosan zajnak tudhatók be. Feltételezve, hogy Bob számára a küldött bitek mivolta ismeretlen, nem végeztem külön erre vonatkozó zajszűrést. A mérések összefoglaló eredményei a 4. táblázatban szerepelnek.

feszültség [V]	-dBm (1 útra)	-dBm (oda-vissza)	Impulzus energiája csillapítás után [%]	beütések		mérés alapú raszter (199.0264ns, 200.0445ns)		200ns-os raszter		számított raszter (199,9ns)	
				CH1	CH2	fogadott bitek aránya [%]	zaj aránya [%]	fogadott bitek aránya [%]	zaj aránya [%]	fogadott bitek aránya [%]	zaj aránya [%]
0	ref.	ref.	100	123	583	0,4987	49,15	0,8584	12,465	0,8347	14,873
0,5	0,02	0,04	99	112	591	0,4847	50,356	0,8625	11,664	0,8208	15,932
1	0,02	0,04	99	113	597	0,4987	49,437	0,8639	12,394	0,8153	17,324
1,5	0,13	0,26	94	135	588	0,5236	47,856	0,8833	12,033	0,8444	15,906
2	0,65	1,3	74	111	558	0,45	51,57	0,7959	14,35	0,7361	20,777
2,25	1,19	2,38	58	111	548	0,4487	50,986	0,7944	13,202	0,7639	16,54
2,5	1,96	3,92	41	107	464	0,4153	47,636	0,6903	12,96	0,6459	18,564
2,75	2,96	5,92	26	101	413	0,3639	49,027	0,5833	18,288	0,5639	21,012
3	4,36	8,72	13	88	288	0,232	55,585	0,4013	23,138	0,3736	28,457
3,25	6,09	12,18	5	109	219	0,2084	54,268	0,3223	29,268	0,3013	33,842
3,5	8,25	16,5	2	98	115	0,118	60,094	0,1889	36,15	0,1889	36,15
3,75	10,8	21,56	1	90	93	0,1084	57,377	0,1236	51,366	0,1251	50,82
4	13,7	27,4	0	100	74	0,0833	65,517	0,1125	53,448	0,0931	61,494
4,25	16,9	33,84	0	89	89	0,0959	61,236	0,1069	56,742	0,1111	55,056
4,5	20,3	40,56	0	100	87	0,0916	64,706	0,1223	52,941	0,1223	23,941
5	26,1	52,16	0	101	77	0,0931	62,36	0,1277	48,315	0,1236	50

4. táblázat – 16 különböző feszültségszinten gerjesztett VOA általi csillapítás hatása az átvitelre, szintenként 150 frame-mel tesztelve mind a három, különböző rasztert felhasználva

Láthatóan alacsonyabb a detektált bitek aránya már a VOA gerjesztetlen állapotában is, mint amikor 1000 frame-et küldtünk. Ez egyrészt azért lehet így, mert a sokkal sűrűbb, 1000 frame-es küldés esetén is pontatlan volt a raszterünk. Ezt a pontatlan rasztert használom itt is – egy sokkal kevesebb pontból álló adathalmazra – melynek átlaghelyei valószínűleg sokkal kevésbé ideálisan alakulnak ehhez a raszterhez viszonyítva, mint az eredeti ezres halmazéi. Ezen kívül itt „01” helyett sima „1”-es ismétlődő bitet küldök, ami ideális esetben csak az egyik detektort szólaltatja meg, így arányaiban kevesebb kulcsbitet szolgáltat.

Ezen túlmenően nagyon szépen kirajzolódik a feszültség növelésének hatására csökkenő detektálás szám a CH2-es csatornán (ide várjuk a beérkező biteket). CH1-en ez a szám azért nem változik – vagy legalábbis nem nagymértékben –, mert a VOA a rajta áthaladó jelsorozatot csillapítja csak, a rendszer saját zaját nem. Megfigyelhető még az is, hogy 4V-os feszültségszint felett már nem csökken tovább egyértelműen az egyik csatornán detektált impulzusok száma sem. Triviális, hogy a maximálisnál jobban nem lehet csillapítani a jelet, tehát e fölé a szint fölé már hiába növelem a gerjesztést, a detektorok már csak a zajt fogják számunkra mutatni. Ezen az utolsó szakaszon a bitráta sem csökken tovább, beáll egy adott szintre.



12. ábra

S hogy miért is fontos számolgatni ezeket az értékeket? Miért nem küldünk egyszerűen csak 1 fotonos várható értékre csillapított impulzusokat? Éppen azért, mert

ez csak várható érték; a Poisson-eloszlást követő fotonszám várható értéke egy impulzusban hiába 1, meglehet, hogy beérkezéskor még 2 fotont tartalmaz, de persze az is, hogy egyet sem. Csökkentve ezt az értéket ugyan csökken a saját bitrátánk is, viszont ugyanakkor a kommunikáció megtámadásának lehetőségét is minimalizáljuk.

Természetesen, ahogy ezer frame esetében is láttuk, most is szembetűnő a különböző módokon megválasztott raszterek eltérő hatékonysága. Bármilyen módszert is választunk a fotonok várható beérkezési időinek meghatározására, a legnagyobb pontosság érdekében kezdetben megfelelően sok frame küldése szükségeltetik. A SensL time-to-digital konverterével egy folyamatos adatrögzítésre nyílna lehetőség, amellyel nagyon rövid idő alatt elegendő impulzust lehetne feldolgozni, és egy jóval hatékonyabb módszer segítségével kialakítható lenne egy közel tökéletesen pontos bit-érkezési rács. Végül pedig, a dolgozat zárásaként szemléltetem a 12. ábrán látható bitráta esését a csillapítás függvényében – mind a három, eltérő raszter esetében.

Köszönetnyilvánítás

Köszönöm a munka elkészítésében nyújtott segítségét Kis Zsoltnak *(Wigner Fizikai Kutatóintézet)*, valamint Jánosi Gergelynek és Jókai Sándornak *(BME Hálózati Rendszerek és Szolgáltatások Tanszék, ESD-labor).*

A munka a Kvantumbitek előállítása, megosztása és kvantuminformációs hálózatok fejlesztése nevű, 2017-1.2.1-NKP-2017-00001 számú projekt a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a "Nemzeti kiválósági program" pályázati program finanszírozásában valósult meg.

Irodalomjegyzék

[1] Sándor Imre, Ferenc Balázs. Quantum Computing and Communications, An Engineering Approach. John Wiley & Sons, Ltd, 2005

[2] Optics.org: Cryptography secures Swiss elections https://optics.org/article/31646 (29 Oct 2007)

[3] Chinese Academy of Sciences: Beijing-Shanghai Quantum Communication Network Put into Use, http://english.cas.cn/newsroom/archive/news_archive/nu2017/201703/t20170324_175288.shtml (Sep 01, 2017)

[4] T.C.Ralph, S.D.Bartlett, J.L.O'Brien, G.J.Pryde and H.M.Wiseman: Quantum Non-demolition Measurements on Qubits, arXiv:quant-ph/0412149v1 20 Dec 2004

[5] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-distance decoy-state quantum key distribution in optical fiber," Phys. Rev. Lett. 98(1), 010503 (2007).

[6] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," Phys. Rev. Lett. 98(1), 010505 (2007).

[7] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in Proceedings of International Symposium on Information Theory, p. 136 (IEEE, 2004).

[8] QIANG ZHANG,1,2 FEIHU XU,1,2 YU-AO CHEN,1,2 CHENG-ZHI PENG1,2 AND JIAN-WEI PAN1,2. Large scale quantum key distribution: challenges and solutions.

[9] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," Phys. Rev. Lett. 117(19), 190501 (2016).

[10] D Stucki1, M Legr´e, F Buntschu, B Clausen, N Felber: Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New Journal of Physics 13 (2011) 123001

[11] Sándor Imre, László Gyöngyösi. Advanced Quantum Communications, An Engineering Approach. Wiley-IEEE Press, 2011

[12] Forbes: How Do You Create Quantum Entanglement?, https://www.forbes.com/sites/chadorzel/2017/02/28/how-do-you-create-quantum-entanglement/#7337e5661732 (Feb 28, 2017, 09:48am)

[13] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, Yang Li, Qi Shen, Yuan Cao, Feng-Zhi Li, Jian-Feng Wang, Yong-Mei Huang, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Li Li, Nai-Le Liu1, Franz Koidl, Peiyuan Wang, Yu-Ao Chen, Xiang-Bin Wang, Michael Steindorfer, Georg Kirchner, Chao-Yang Lu, Rong Shu, Rupert Ursin, Thomas Scheidl, Cheng- Zhi Peng, Jian-Yu Wang, Anton Zeilinger, Jian-Wei Pan: Satellite relayed intercontinental quantum network.

[14] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu,Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, Jian-Wei Pan: Satellite-Based Entanglement Distribution Over 1200 kilometers

[15] Hraskó Péter: A Bell-egyenlőtlenség, http://www.termeszetvilaga.hu/X-Aknak/docs/kve2/bellineq.html

[16] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein: Advances in Quantum Teleportation, arXiv:1505.07831v1 [quant-ph] 28 May 2015

[17] Brian P. Williams, Ronald J. Sadlier, and Travis S. Humble: Superdense coding over optical _ber links with complete Bell-state measurements, arXiv:1609.00713v1 [quant-ph] 2 Sep 2016

[18] Y. Mao, B.-X. Wang, C.-X. Zhao, G.-Q. Wang, R.-C. Wang, H.-H. Wang, F. Zhou, J.-M. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan: Integrating quantum key distribution with classical communications in backbone fiber network, Opt. Express 26(5), 6010–6020 (2018)

[19] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin: Quantum repeaters based on atomic ensembles and linear optics, Rev. Mod. Phys. 83(1), 33–80 (2011)

[20] S.-J. Yang, X.-J. Wang, X.-H. Bao, and J.-W. Pan: An efficient quantum light–matter interface with sub-second lifetime, Nat. Photonics 10(6), 381–384 (2016)

[21] Yang, S.-J., Wang, X.-J., Bao, X.-H. & Pan, J.-W. Nat. Photon. 10,381–384 (2016)

[22] Hedges, M. P., Longdell, J. J., Li, Y. & Sellars, M. J. Nature 465,1052–1056 (2010)

[23] Chip Elliott: The DARPA Quantum Network. ACM SIGCOMM 2003

[24] M Peev, C Pacher, R Alléaume, C Barreiro, J Bouda, W Boxleitner, T Debuisschert, E Diamanti, M Dianati, J F Dynes, S Fasel, S Fossier, M Fürst, J-D Gautier, O Gay, N Gisin, P Grangier, A Happe, Y Hasani, M Hentschel, H Hübel, G Humer, T Länger, M Legré, R Lieger, J Lodewyck, T Lorünser, N Lütkenhaus, A Marhold, T Matyus, O Maurhart, L Monat, S Nauerth, J-B Page, A Poppe, E Querasser, G Ribordy, S Robyr, L Salvail, A W Sharpe, A J Shields, D Stucki, M Suda1,C Tamas1, T Themel1, R T Thew, Y Thoma, A Treiber, P Trinkler, R Tualle-Brouri, F Vannel, N Walenta, H Weier, H Weinfurter, I Wimberger, Z L Yuan, H Zbinden and A Zeilinger: The SECOQC quantum key distribution network in Vienna. New Journal of Physics 11 (2009) 075001

[25] Raju Valivarthi, Marcel.li Grimau Puigibert, Qiang Zhou, Gabriel H. Aguilar, Varun B. Verma: Quantum teleportation across a metropolitan fibre network. 19 SEPTEMBER 2016 | DOI: 10.1038/NPHOTON.2016.180

[26] Qi-Chao Sun, Ya-Li Mao, Si-Jing Chen, Wei Zhang, Yang-Fan Jiang, Yan-Bao Zhang: Quantum teleportation with independent sources and prior entanglement distribution over a network. 19 SEPTEMBER 2016 | DOI: 10.1038/NPHOTON.2016.179

[27] Chinadaily: Beijing-Shanghai quantum link a 'new era', http://www.chinadaily.com.cn/china/2017-09/30/content_32669593.htm (2017-09-30 06:33)

[28] Wired: Why This Intercontinental Quantum-Encrypted Video Hangout Is a Big Deal, https://www.wired.com/story/why-this-intercontinental-quantum-encrypted-video-hangout-is-a-big-deal/ (01.20.2018 12:30 AM)

[29] D Stucki et al 2002 New J. Phys. 4 41

[30] Dr. Kis Zsolt, Wigner Fizikai Kutatóközpont, 1121 Budapest, Konkoly-Thege Miklós út 29-33

[31] Grégoire Ribordy, Jean-Daniel Gautier, Nicolas Gisin, Olivier Guinnard, Hugo Zbinden: FAST AND USER-FRIENDLY QUANTUM KEY DISTRIBUTION. Journal of Modern Optics

[32] Thorlabs: Electronic Variable Optical Attenuators (VOA), Voltage Controlled & Fiber Coupled, https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_ID=10884#ad-image-0