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

Czermann Márton

BB84 PROTOKOLLON ALAPULÓ KVANTUMKULCSSZÉTOSZTÁS DEMONSTRÁLÁSA SZÁLOPTIKÁS RENDSZEREN

KONZULENSEK:

Dr. Bacsárdi László, Dr. Kis Zsolt,
és Dr. Kovács Benedek

BUDAPEST, 2020

Tartalomjegyzék

Összefoglaló

A napjainkban széles körben elterjedt titkosító eljárások (pl. RSA) és digitális aláírásokat lehetővé tevő protokollok (pl. DSA, ECDSA) életünk szerves részét képezik, melyek nélkül nem tudhatnánk biztonságban pénzügyeinket és adatainkat, cégek, szolgáltatók és szervezetek komplett működése kerülhetne veszélybe és országok válhatnának kiszolgáltatottá egymásnak és bűnszervezeteknek egyaránt. A kvantumforradalomnak nyugodt szívvel nevezhető időszak során korunkba olyan technológiák alapjait dolgozták ki a kutatók, amelyekkel a fent említett felvetések realitássá válhatnak.

A közelmúltban kifejlesztett kvantumszámítógépek – melyeknek hatalmas mérete, gyenge számítási kapacitása és integrálhatóságának hiánya egyelőre komoly hátráltató tényező a kvantumszámítástechnika terén – óriási gyakorlati jelentőséggel rendelkeznek. Peter Shor amerikai matematikus ugyanis 1994-ben egy olyan kvantumszámítógépekre tervezett algoritmust fedezett fel, melynek segítségével polinomiális időn belül elvégezhető egész számok faktorizálása – s ezzel egyúttal feltörhetővé válnak napjaink népszerű nyílt kulcsú titkosításai. 2019 októberében a Google bejelentette, hogy elérték a kvantumfölényt, aminek során az általuk működtetett kvantumszámítógépnek sikerült felülmúlnia egy szuperszámítógép teljesítményét egy adott, bonyolult számítási feladat során. Ahhoz azonban, hogy veszélybe kerüljenek klasszikus módon védett anyagi és szellemi értékeink, lényegesen növelni kell a mai kvantumszámítógépek számítási kapacitását és jelentősen javítani a működésük során bekövetkező hibaarányon is – ennek időskáláját fél tucat évtől évtizedekig jósolják.

Szerencsére már most is számtalan megoldás jött létre a kvantumos éra vívmányaiként a jövő kiber-és kommunikációbiztonsága érdekében. A kvantummechanika törvényei matematikai szabályok és eljárások helyett olyan kvantumprotokollok alkalmazását teszik lehetővé, melyek biztonsága fizikai alapokon nyugszik. Már több évtizede kísérleteznek különböző vezetékes és vezeték nélküli kvantum alapú kulcsszétosztó protokollok (quantum key distribution, QKD) megalkotásán és implementálásán, kvantum linkek és hálózatok megépítésén és a kvantumprotokollok valódi kommunikációs rendszerekbe történő integrálásán. Nem

titkolt célul van kitűzve egy globális kvantumkommunikációs hálózat létrehozása, amihez számtalan ország és szervezet járul hozzá egyéni és közös projektek megvalósításával is.

Az elmúlt évben egy ipari együttműködésben épülő vezetékes kvantumkulcsszétosztó rendszer építésén dolgoztam. A rendszer alapját a BB84 algoritmus fáziskódolt változata adja, ahol két kommunikáló fél (Alice és Bob) között kerül sor kulcsszétosztásra. Az optikai szálas összeköttetésben 1550 nm-es hullámhosszon kibocsájtott fényimpulzusokat használunk, melyeket egyfotonos teljesítményszintre csökkentünk vissza.

Munkám során sikeresen demonstráltam a berendezés fizikai rétegének működését, mérési eredményekkel jellemezve a rendszerben alkalmazott egyedi szoftveres és hardveres megoldások átviteli tulajdonságait.

Abstract

Nowadays, widely spread encrypting methods (e.g., RSA) and protocols enabling digital signatures (e.g., DSA, ECDSA) are an integral part of our life. We could not guarantee the security of our finances and personal data, the complete operation of companies, service providers and organizations could get in danger and countries would be vulnerable to criminal organizations and to each other as well. During the last few decades, scientists invented the basis of quantum technologies, with which the previous assumptions could turn into reality.

Although recently developed quantum computers have low processing capacity, huge dimensions and they have a lack of interoperability, we must underline their practical significance. In 1994, Peter Shor invented a quantum algorithm that makes it possible to factorize integers in polynomial time and with it, todays popular public key cryptographies become breakable. Further on, in October 2019, Google announced to have achieved quantum supremacy, that means they overcame with a complex computing problem with their quantum computer way faster than they would have done with a classical supercomputer. Even after all, the processing capacity and error rates of the quantum computers must be further developed in order to consider our classically secured material and intellectual values to be in danger.

Fortunately, numerous solutions came into sunlight as achievements of the quantum era so far to ensure cyber and communication security in the future. Instead of mathematical rules and methods, quantum mechanics gave us the means of physically secure quantum protocols. Experiments on constructing and testing different types of fiber-based and free space quantum key distribution (QKD) protocols and on how they could be integrated into classical communication networks have already been done for decades now, while huge numbers of quantum links and networks have been built. The ultimate goal of the quantum revolution in communications is to establish a global quantum network to which a great many of countries and associations contribute with either individual or joint projects as well.

In my research, I was working on a fiber based QKD system, that is being built in industry collaboration. The base of the system is phase-coded version of the BB84 QKD protocol, where key distribution occurs between two communicating parties. The system

operates at normal telecom wavelengths. In the fiber-based link, we apply light pulses at 1550 nm wavelength, reducing their power into only 1-photon level.

As a result of my work, I successfully demonstrated the proper operation of the physical layer of the equipment, by describing quantitatively the transmittance characteristics of the unique software and hardware solutions utilized in the system.

1 Bevezetés

A kvantummechanika megszületésével útjának indult egy akkor még végeláthatatlan folyamat, egy technológiai fejlődés, amely mostanra megérett arra, hogy a tudományos élet szerves részét képezze, meghatározza az infokommunikációs rendszerek fejlődési irányait és egy kontinensek közti globális versenyt indítson útjára információbiztonságbéli és gazdasági megfontolások által vezérelve.

A kvantum-számítástechnika és -kommunikáció világában, a sokak által kvantum érának hívott időszakban az egyik meghatározó kérdés az: „Vajon mikor fogja feltörni egy kvantumszámítógép Shor algoritmusának felhasználásával az RSA nyíltkulcsú titkosítást?" Mialatt ez az idő egyre közeledik, kutatók és fizikusok, cégek és kormányok világszerte számtalan kutatóprojektet elindítva igyekeznek többek között megoldásokat találni különféle, fizikai alapokon nyugvó biztonsággal rendelkező kommunikációs rendszerek megtervezésére, megalkotására és azok forgalomba hozatalára, alkalmazására valódi telekommunikációs rendszereken.

A kvantumkommunikáció vezetékes megoldásai közül az egyik legelterjedtebb változat a BB84 protokollt felhasználó, fénnyel kommunikáló rendszer, mely két fél között teremt lehetőséget biztonságos, szimmetrikus titkos kulcs létrehozására. Ezt a kulcsot aztán a kommunikáló felek fel tudják használni titkosító eljárásokban úgy, hogy kulcsukat mindeközben senki sem tudja megszerezni, annak kialakulása során a kommunikációjuk lehallgathatatlanná válik – ideális viszonyok között. Magyarországon is folynak kutatások annak érdekében, hogy Európával együtt lépést tudjunk tartani az USÁ-val, Koreával, vagy Kínával a kvantumkommunikáció terén.

Ebben a dolgozatban egy hazai fejlesztésű kvantumkulcsszétosztó (QKD) rendszert szeretnék bemutatni, amelyen a BME egy ipari partnerrel közösen dolgozik. A cél a BB84 protokoll alapján működő QKD megvalósítása, méghozzá úgy, hogy eközben termékorientált szemléletet kövessenek. Minthogy egy, a Plug & Play jegyében tervezett rendszerről van szó, ez utóbbi irány máris megmutatkozni látszik a projektben, melynek másfél éve jómagam is a tagja vagyok. Az elmúlt év során az volt a feladatom, hogy a tavaly még csak pár alapműködésre képes rendszert tovább fejlesszem és a teljes vezérlését kialakítva megvalósítsam rajta a kvantum alapú kulcsszétosztás fizikai rétegét. Ebben a dolgozatban a BB84 demonstrálását foglalom össze a fizikai rétegen, mérési

eredményeimmel alátámasztva, melyeket vele együtt részletesen bemutatok és a működéshez elengedhetetlen, egyedi hardveres és szoftveres megoldásaimat is prezentálom.

Mindenekelőtt azonban szeretném a kvantumkommunikáció alapfogalmait bevezetni, amit rögtön a 2. fejezetben meg is teszek. Ezt követően a kvantumkommunikációban használt fő protokollcsaládokat és a kommunikáció biztonságát mutatom be a 3. fejezetben. A hazai rendszer felvezetéseként a 4. fejezet során áttekintést nyújtok az elmúlt évek tématerületbe vágó fejlesztéseiről és megépített rendszereiről, így az olvasó is könnyedén el tudja majd helyezni azt a kvantumkommunikáció világtérképén.

Az 5. fejezettől áttérek a saját rendszerünkre, amelyeken a munkáimat folytattam – bemutatom architektúráját és működését. Ezt követően a rendszer működtetésére kerül sor, megemlítve korábbi munkáimat és az azokkal kapcsolatos fejlesztéseimet, javításaimat, illetve természetesen azokat a munkákat is, amelyeket vagy a korábbiakra építettem fel. Ezek mellett bemutatom két új vezérlőkódomat is, melyek során az alapokról indultam el. Végül, a 7. fejezetben demonstrálom a Magyarországon először végrehajtott BB84 alapú kvantumkulcsszétosztást fizikai rétegen, eredmények kiértékelésével alátámasztva a működést, megvizsgálva annak hatékonyságát.

2 A kvantumkommunikáció alapjai

A kvantumkommunikáción olyan kommunikációs rendszereket és eljárásokat értünk, amelyek „kvantumos alapon működnek”. Ez a kifejezés olyan közegekre vonatkozik, melyekben részecskék, vagy azok sokasága van jelen, amikre tulajdonságaikból adódóan (pl. méretük) már érvényesülnek a kvantummechanika törvényei. Ezek a közegek jelentik a kvantumkommunikáció alapjait, aminek egy részét képezik a kvantumkulcsszétosztási eljárások is. Ahhoz, hogy egy kvantumkommunikációs eljárást megvalósíthassunk, szükségünk van információhordozó egységekre.

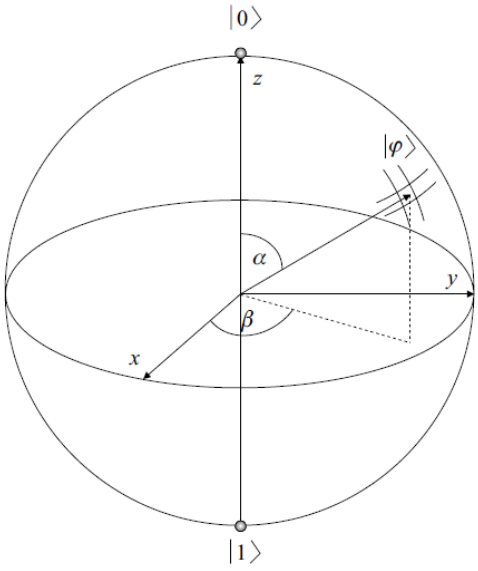
Klasszikus információ kommunikációban ezeket az információhordozó egységeket biteknek hívjuk, melyek értéke felvehet két állapotot (1-est vagy 0-ást) és ezt az információt bennük eltárolhatjuk (pl. elektromos töltések segítségével). Később ezt a bitnyi információt eljuttatjuk egy kommunikációs csatornán egy küldő féltől egy fogadó félig, aki mérést végez az adott biten és nyilvánvalóvá válik számára annak értéke is, miszerint 1-est, vagy 0-ást kapott. Erre pedig, mint tudjuk, felépíthető egy teljes kommunikáció. De miben tér el ettől a kvantumos verzió?

Kvantumbitként (angolul qubit) fel tudunk használni minden olyan részecske- vagy hullámtulajdonságot, amelynek két elkülöníthető állapota van, mondhatni bináris. Megfelelő választás lehet például egy foton vízszintes vagy függőleges polarizációja, vagy egy elektron „felfelé” vagy „lefelé” irányuló spinje is. Ahhoz, hogy kvantumkommunikáció során zárt rendszert alkotó kvantumbitek sokaságát használjuk fel, valamilyen rendszert alkotva belőlük, kvantumállapotuk változtatásával. Alapvető különbség egy klasszikus és egy kvantum bit között, hogy míg előbbi egy determinisztikus működésű, bináris egység, mely az idő minden pillanatában egyik állapotában van, addig utóbbi egy olyan kétállapotú egység, ami folyamatosan, egyidőben mindkét állapotában van egyszerre. Ezt a tulajdonságot hívjuk szuperpozíciónak.

Legegyszerűbb ezt úgy elképzelni, mint amikor feldobunk egy egyszerű pénzérmét a levegőbe. (Érdemes egy frissen nyomottat használni, hiszen annak még jól meg tudjuk különböztetni a fejét az írás részétől.) Mialatt a levegőben van, analógiáját tekintve megfeleltethető egy kvantumbitnek. Két állapota van, a fej és az írás, de amíg ott pörög a szemünk előtt, számunkra úgy tűnik, mintha egyszerre lenne fej és írás is. Ha

szeretném megtudni, milyen értéket is vesz fel, akkor egyszerűen csak el kell kapnom és máris látom, hogy a tenyeremen fej, vagy írás áll-e felfelé. Hasonlóképpen, ha egy kvantumállapotban lévő kvantumbit értékét szeretném megmérni, akkor az addig szuperpozícióban lévő teljes állapot egy klasszikus értékre hanyatlik, melyet már meg tudunk feleltetni egy klasszikus 1-nek vagy 0-nak. Célunkat azonban nem sikerült elérni, a kvantumállapot értékét nem sikerült megtudnunk. Egy mérés tehát, amely kapcsolatot teremt a kvantum- és klasszikus világ között egyúttal meg is változtatja a vizsgált kvantumállapotot, mely a mérés után a továbbiakban már klasszikusan fog viselkedni. De hogyan is néz ki akkor egy kvantumállapot?

Egy kvantumállapot leírható komplex valószínűségi amplitúdókkal a Hilbert-térben, ahol a belső szorzat értelmezve van. A kvantumállapotok egyúttal ábrázolhatóak is az úgynevezett Bloch-gömbön (lásd 1. ábra), egységhosszú vektorok segítségével, de egy 2012-es magyar publikáció például fraktálokkal dolgozik [1]. A szuperpozícióban lévő kvantumbit egy olyan teljes állapotban van, melyben megtalálható valamilyen súllyal mind a két diszkrét állapota. Ezeket a súlyokat írják le az imént említett komplex valószínűségi amplitúdók, melyekre igaz, hogy abszolútértékük négyzetének az összege 1-et ad. Mérés után ugyanis valamilyen valószínűséggel billen be a kvantumbit állapota a klasszikusai egyikébe.



1. ábra – Bloch-gömb [2]

Egy ilyen állapotot görög betűvel jelölünk, az alábbi módon: |φ⟩ (ejtsd: „ket fi”). Az 1. ábrán lévő Bloch egységgömb egy |φ⟩ állapotot ábrázol. Ennek általános képlete:

$|\varphi\rangle = e^{i\gamma}(cos\frac{\alpha}{2}|0\rangle + e^{i\beta}sin\frac{\alpha}{2}|1\rangle)$. Itt $e^{i\gamma}$ az úgynevezett globális fázis, amely egy egyes sorzóként van jelen a képletben, mert bármely γ-ra kvantumállapotunk változatlan marad – így el is hagyható. Ha ezek után komplex valószínűségi változókkal szeretnénk egy egységsugarú körön leírni $|\varphi\rangle$ kvantumállapotunkat, akkor azt a következő, gyakran használt összefüggés segítségével tehetjük meg: $|\varphi\rangle = a|0\rangle + b|1\rangle$, ahol a és b a két komplex valószínűségi amplitúdó. Természetesen nem csak egy, hanem több kvantumbitről is beszélhetünk egyszerre, melyeket együttesen kvantumregiszteknek nevezünk. Kapcsolatukat zárt rendszerben, tenzorszorzás segítségével írhatjuk le. Ennek köszönhetően kvantumregiszterek állíthatók elő kvantumbitekből.

Kvantumbitjeinken és -regisztereinken műveleteket hajthatunk végre kvantumkapuk segítségével. Művelet lehet például a Bloch-gömbön szemléltetve az, hogy állapotunkat tükrözzük az egyik tengelyre, de fázisát is forgathatjuk. Ezekhez a transzformációkhoz továbbra is zárt rendszerben kell mozognunk és maguknak a transzformációknak unitéreknek kell lenniük, ami annyit jelent, hogy elvégzése után következtetni tudunk a kiindulási állapotra, mielőtt a kapu transzformációs mátrixát alkalmaztuk volna. Az unitér transzformációk ezen kívül megtartják a belső szorzatot is. Ilyen műveletek elvégzésével, kapuk felállításával komplett kvantumáramkörök is építhetők, amikre protokollok fejleszthetők.

A kvantumbitekre vonatkozó állítások és alapigazságok (Hilbert-térben leírhatóak, egységnyi hosszúak, zárt rendszert alkotnak), a kvantumregiszterekre vonatkozóak (tenzorszorzás), az unitér transzformációkkal kapcsolatosak (kvantumkapuk) és a méréssel kapcsolatos megállapítások a kvantumkommunikáció négy posztulátuma, amire építkezhetünk a továbbiakban. (Máshol hárommal, vagy hattal is kimondják őket, de mindhárom megközelítés helyes.)

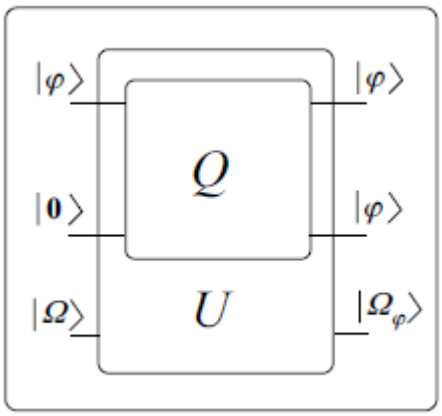
De hogyan tudjuk felhasználni ezeket kommunikációra, ha egy méréssel „mindent elrontunk”? És mi az, ami a biztonság alapját adja egy ilyen elveken épülő kommunikációs rendszer esetén? Több eljárás is létezik, amiken keresztül végig lehetne venni erre a két kérdésre a válaszokat (szupersűrű kódolás, kvantumteleportálás, vagy például a kvantumpárhuzamosság kihasználása) [2], ám ezek csak távolról kapcsolódnak ahhoz a témához, amivel az elmúlt időszakban foglalkoztam. A továbbiakban a kvantumkulcsszétosztási eljárásokon keresztül mutatom be a kvantumvilág működését, egyúttal megválaszolva a fenti kérdéseket is a következő fejezetben.

3 Biztonsági megfontolások és a BB84 protokoll

Többször is említettem már, hogy a kvantum alapú kulcsszétosztási eljárások biztonsága fizikai alapokon nyugszik. Egy QKD protokoll alapvetően két fő okból biztonságos, illetve lehallgathatatlan. Az egyik okot az úgynevezett „Nincs másolás tétel”, vagy angol nevén „No Cloning Theorem” szolgáltatja. A tétel egy önkényesen választott kvantumállapot lemásolásának lehetőségeit veszi végig, tehát azt vizsgálja meg, hogy lehet-e készíteni olyan eszközt, aminek egy szuperpozícióban lévő kvantumbitet adva a bemenetére, vajon képes-e a kimenetén duplikáltan megjeleníteni azt.

3.1 No Cloning Theorem

Ehhez először is szükségünk van egy valamilyen Q transzformációt elvégző kvantumkapura (vagy Q eredményre vezető kvantumkapuk összességére). Egy zárt kvantum rendszeren végzett transzformációnak unitérnek kell lennie, ahogyan azt az előző fejezetben is kikötöttük. Szükségünk van azonban még egy bemenetre, hiszen zárt rendszerről lévén szó a ki- és bemenetek számának meg kell egyeznie egymással. Újabb bemenetként vegyünk fel egy egyszerű $|0\rangle$ értéket, amivel nem törődünk, nem használjuk fel semmire.



2. ábra - Kvantumállapot-klónozó kapu [2]

A transzformáció elvégzésével, ha működik a másoló eszközünk, akkor egy $|\varphi\rangle$ állapotot a bemenetre juttatva kimenetként két, megegyező $|\varphi\rangle$ állapotot kell kapnunk. A kimenetből viszont nem tudunk következtetni a bemenetre, bármit adhatnék $|\varphi\rangle$ mellett

a másik vezetékre, anélkül, hogy meg tudnám mondani, milyen állapotokból sikerült létrehoznom $|\varphi\rangle$-t és másolatát. Ez tehát még nem elégíti ki az unitérség kritériumát. Vegyünk hát Q-t és egészítsük ki úgy, hogy unitér transzformációt kapjunk belőle! Tehát vegyük hozzá a transzformációhoz Q környezetét, kezeljük őket egyben, egy nagy kvantumkapuként, amíg az teljesen zárt nem lesz, s ekkor már unitérnek tekinthetjük rendszerünket (U). A környezet állapotát jelöljük a 2. ábrán látható módon $|\Omega\rangle$-val, a transzformáció utáni megváltozott állapotát pedig $|\Omega_\varphi\rangle$-vel. Úgy néz ki, hogy készen is vagyunk, megalkottunk egy kvantummásolót!

Ha tényleg sikeres volt a procedúra, akkor bármilyen másik kvantumállapoton is el tudjuk végezni a klónozást. Legyen ez az állapot mondjuk $|\mu\rangle$. Ha jól működik a rendszerünk, akkor unitér transzformációról lévén szó, gépünk megtartja a belső szorzatot, ezzel ellenőrizhetjük törekvéseink eredményét. Az első esetben $U: |\varphi\rangle|0\rangle|\Omega\rangle \to |\varphi\rangle|\varphi\rangle|\Omega_\varphi\rangle$, míg a második esetben $U: |\mu\rangle|0\rangle|\Omega\rangle \to |\mu\rangle|\mu\rangle|\Omega_\mu\rangle$ leképezés adódik. Felírva a skalárszorzatot a bemenetre és a kimenetre is, kapjuk, hogy:

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

illetve

$$\langle \Omega_\mu, \mu, \mu|\varphi, \varphi, \Omega_\varphi\rangle = \langle\mu|\varphi\rangle\langle\mu|\varphi\rangle\langle\Omega_\mu|\Omega_\varphi\rangle = \langle\mu|\varphi\rangle^2\langle\Omega_\mu|\Omega_\varphi\rangle.$$

A skalárszorzat megtartásából következően a bemenet és a kimenet skalárszorzatának meg kell egymással egyeznie. Ez pedig csak akkor lehet, ha:

1. $\mu = \varphi$,
2. $\langle\mu|\varphi\rangle = \frac{1}{\langle\Omega_\mu|\Omega_\varphi\rangle}$, vagy
3. $\langle\mu|\varphi\rangle = 0$.

Az első esetben egy ismert kvantumbitről van szó, tehát nem választhatunk önkényesen kedvünkre. A második eset visszavezethető az elsőre, hiszen egységvektorokkal dolgozunk, amelyek skalárszorzata nem lehet nagyobb 1-nél. Végül pedig, az utolsó lehetőség az, hogy másolandó állapotaink egymásra ortogonálisak legyenek.

A tétel tehát az alapigazságnak vett posztulátumokra alapozva kimondja, hogy önkényesen választott kvantumállapotról nem készíthető másolat. Az csakis ismert, vagy

ortogonális állapotok esetén lehetséges. Ez pedig máris ad egy nagyfokú biztonságot a kvantumkommunikációra fejüket adók számára.

3.2 BB84

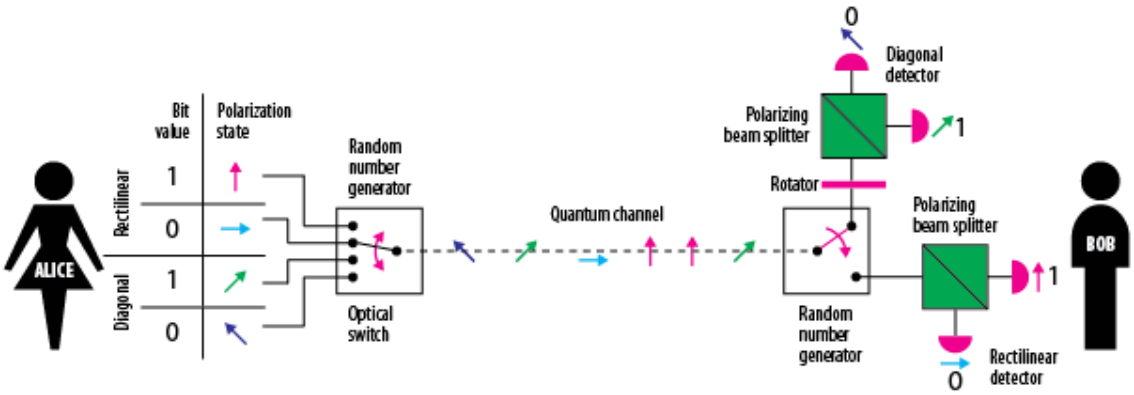
Mielőtt a másik biztonságot jelentő tényezőt is kifejteném, szeretném bemutatni a BB84 protokollt, ami a demonstrációm alapját fogja adni a későbbi fejezetekben, s amihez rögtön utána kapcsolni fogom tudni az említett fizikai biztosítékot is.

Alapvetően két nagy protokollcsaládja létezik a kvantumkulcsszétosztásnak, amikbe a QKD eljárások és protokollok mind besorolhatók. Ezek az „előkészít és megmér” (az angol szakirodalomban „prepare and measure”-ként emlegetett) elven működő protokollok illetve az összefonódás-alapú protokollok. Az elsőbe tartozik Charles Bennett és Gilles Brassard 1984-ben megalkotott QKD protokollja is, a BB84. Ez ösztönözte aztán protokollok tucatjának kialakulását és kvantumlinkek és -hálózatok létrejöttét. Mára már odáig jutott ez a nagyiramú fejlődés, hogy nemzetközi célként van kikiáltva egy globális kvantuminternet létrehozása, ami ugyan még tartogat magában technológiai kihívásokat, de nem áthidalhatatlanokat.

Az „előkészít és megmér”-típusú protokollokban közös az, hogy nulladik lépésként a küldőoldal (Alice) előkészít két megegyező hosszúságú kezdeti kulcsot (bináris számsort), amelyek egyike megadja, hogy milyen értékű információt fog majd belekódolni a kvantumos információszállító egységeibe, míg a másik azt adja meg, hogy ezeket a kódolandó biteket (0/1) milyen bázisban fogja majd kódolni. Mivel kétféle bázis közül választhat, azért a másik kezdeti bináris számsor bitjei tökéletesen megfelelnek erre a célra (0 – egyik bázis, 1 – másik bázis). Közös az is, hogy az így a kvantumos szállítóközegbe kódolt információt a vételi oldalon Bob szintén egy előre generált kulcs alapján fogja majd dekódolni, méghozzá úgy, hogy minden egyes benne lévő bit eldönti, hogy a két lehetséges közül melyik bázisban mérje meg az Alice által küldött kvantumbitek állapotát. Fontos, hogy Bob és Alice kezdeti kulcsai teljesen véletlenszerűen állnak elő. Az így kapott működést a 3. ábra szemlélteti.

A BB84-ben fotonok polarizációját használjuk információátvitelre (horizontális – vertikális, vagy ettől $\pi/4$-gyel eltolt polarizáció), ebbe kódolja bele a kezdeti kulcs bitjeit. Amennyiben Bob egy adott kvantumbitet ugyanabban a bázisban mér meg, mint amelyik bázisban Alice kódolta (tehát ugyanolyan irányultságú polarizátort használ, mint Alice), akkor helyes értéket fog mérni, ha viszont nem, akkor akármit mérhet, véletlenszerűen.

Általánosítva a kódolás menetét elmondható, hogy Alice két olyan bázisban kódolja a bitjeit, melyek egymáshoz képest biztosan nem ortogonálisak, így pedig a „Nincs másolás” tételt kihasználva belátható, hogy Alice bázisválasztáshoz használt bitjeinek hiányában lehetetlen a küldött bitek lemásolása. Így egy „man-in-the-middle” támadás például nem eszközölhető egy támadó fél számára (nevezzük Eve-nek).



Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	ALICE tells BOB which bits to keep		✔		✔		✔	✔	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

3. ábra - A BB84 igazságtáblája [3]

A procedúra után Alice és Bob megosztja egymással egy publikus csatornán a választott bázisokat, s ahol egyezést látnak, az aszerint kódolt bitet megtartják, ahol pedig ellenkező bázist választottak, az aszerint küldötteket kidobják. Bár a küldés során nem tudta lemásolni senki a küldött biteket, mégis, joggal feltételezhetjük, hogy ha Eve hozzáfért a csatornához és le akarta hallgatni a kommunikációt, akkor Bobhoz hasonlóan utólag ő is ki tudja majd találni a kulcsbiteket Alice bázisainak segítségével. (A publikus klasszikus csatornát ugyanis mint tudjuk, le lehet hallgatni.) Ha Bob nevében ő küldi vissza saját bázisbitjeit Alice-nak – tehát Eve utólag lép fel „man-in-the-middle” támadóként a klasszikus kommunikációban –, akkor máris nem biztonságos a kulcsszétosztás. Vagy mégis?

A küldés során átlagosan 1 fotonos jelszintű impulzusok haladnak keresztül a csatornán. Amennyiben Eve le akarja hallgatni a kommunikációt, valahogy neki is meg

kell mérnie a kvantumbitek állapotát. Ám ekkor a méréssel meg is változtatja azokat, s az így Bobhoz tovább haladó impulzusok jócskán el fogják rontani a várt bitrátát – Alice és Bob pedig innen tudomást szereznek Eve jelenlétéről.

A protokoll tehát kimeríti a kommunikáció fogalmát abban az értelemben, hogy egy küldő és egy fogadó fél között titkos kulcs alakul ki információhordozó közeg segítségével. A protokoll egyúttal biztonságos is, hiszen semmiképp nem tud egy harmadik fél szert tenni a kialakuló szimmetrikus kulcsra anélkül, hogy jelenlétét felfedje a felek között. A való életben persze nincsenek ideális esetek és a gyakorlati megvalósításban helyet kapó eszközök lehetséges hibaforrásként vannak jelen. A mai napig nincs tökéletesen működő egyfoton lézer, de a detektorok gyengeségeit is ki lehet használni (pl. holtidő, hatékonyság, érzékenység, …). Ezeket a hibaforrásokat kihasználó támadások (pl. detektor vakító támadás) ellen is számos fejlesztés látott már napvilágot (BB92, „csaliállapotok” protokollja, …), így biztosítva a QKD biztonságosságát.

4 Kvantumösszeköttetések

Az elmúlt néhány évtized során kialakított kvantumlinkek nagy része optikai szálas összeköttetés volt, de akadtak olyanok is természetesen, melyek szabadtéri, vagy jellemzően később már összefonódás-alapú QKD-protokollokat teszteljenek. A kvantumhálózatok zömét is jellemzően földi, vezetékes alapokra tervezték és építették meg. Egy ilyen hálózat remek lehetőséget nyújtott akár több, különböző kvantumprotokoll tesztelésére is egyidőben. Létrejöttek olyan nagyobb kvantumhálózatok is, amelyek akár több várost is összekötöttek, meghatározó szereplőivé válva a kvantumkommunikációs kutatásoknak és jövőképnek.

Az egyetemünkön lévő QKD rendszer is a vezetékes megoldások közé tartozik. Ennek a fajta architektúrának is megvannak természetesen a maga előnyei és hátrányai is egyaránt. Az optikai szálas összeköttetésekben fényt alkalmaznak információszállító közegként, hiszen a foton kifejezetten ideális kvantumos részecskének felel meg (vegyük a polarizációját, vagy megfelelő fázisforgatását). A fénytávközlés technológiája, a kommunikációra használt optikai eszközök és maga az optikai infrastruktúra a rendelkezésünkre áll, ezért a fény használata egy kifejezetten előnyös tulajdonsága ezeknek az összeköttetéseknek. Könnyen kezelhetőek és jól integrálhatóak. Már nem számít az sem újdonságnak, hogy léteznek olyan kvantumhálózatok, melyeknek az alkalmazásbéli infrastruktúráját nagyvárosi gerinchálózatok biztosítják. Mindezek mellett ott lebeg a lehetőség a szemünk előtt, hogy megfelelőkörülmények és paraméterek mellett akár egy kvantum-klasszikus WDM-et (Wavelength Division Multiplex) is megvalósíthassunk.

Legnagyobb hátránya és egyben korlátja a vezetékes összeköttetéseknek az a csatornacsillapítás. Egy 100km-es szálszakaszon akár 30-40dB-lel is képes csökkenteni a fény energiáját, ami önmagában egy nagy érték, főleg akkor, ha egy kvantumkommunikációs rendszer csatornakarakterisztikájáról beszélünk. Ez azt jelenti, hogy ez alatt a távolság alatt annyira lecsökken a jelszintje, hogy a fogadó oldali detektor már nem igazán fogja tudni detektálni. Országokon, vagy nagyobb távolságokon átívelő összeköttetések létrehozása így csakis kvantumismétlőkkel lenne megoldható, de a technológia mai állása ezt nem teszi lehetővé (szükséges lenne kvantummemóriák használata is hozzá, de ez a technológia még csak kísérleti stádiumban és alacsony

hatékonysággal létezik). Alternatív megoldásként marad a megbízható relék használata, melyek azonban csak akkor jelentenek biztonságot, ha fizikailag elszeparált egységekről beszélhetünk.

Városokon belül viszont nincsenek ekkora távolságok – legalábbis, ha Magyarországot tekintjük –, így ilyen léptéket tekintve előnyösnek bizonyulhat. Fénnyel ugyanis nehéz nappal kommunikálni, a vezetékes rendszer ezzel szemben viszont külső zajtól jóval védettebb. Napjainkban is használnak néhány helyen aktívan működő városi, vezetékes QKD rendszert, melyben a „csaliállapotok" módszerét is kihasználják a biztonság növelése érdekében. Erre jó példa a Shanghai-ban alkalmazott, 66km-es, 3,6Tbps-os telekommunikációs gerinchálózatba integrált QKD hálózat [4].

A jelentősebb, mérföldkőnek is tekinthető vezetékes kvantumhálózatok közé a következőket sorolnám; A 2003-ban az Egyesült Államokban a DARPA (Defense Advanced Research Projects Agency) által létrehozott kvantumhálózat volt az első, működőképes QKD hálózat, melyben koherens impulzusokkal valósítottak meg kvantumkulcsszétosztást 4 csomópont között. További 2 csomópont pedig szabadtéri QKD-re volt kialakítva, de azok is csatlakoztak a teljes rendszerhez [5].

A 2004 és 2008 között futó SECOQC (Secure Communication based on Quantum Cryptography) project Ausztriában hatalmas információforrás volt a tudományos élet számára. A pont-pont kapcsolatra épülő, megbízható reléket is igénybe vevő hálózat 6 csomópontja között összesen 8 különböző protokollt tesztelt, melyek között főleg vezetékes QKD implementálása volt a jellemző (pl. plug & play architektúra is) [6].

Hasonló felépítéssel rendelkezett a Svájcban felállított SwissQuantum, melynek rétegvezérelt hálózatának huzamos tesztelésén volt a hangsúly 2009 és 2011 között. A 3 réteg, melyből összeállt a hálózat a kvantum-, kulcs-menedzsment és az applikációs réteg. A 21 hónapon át tartó működés során a kvantumbit-hibaarány (QBER, quantum bit error rate) alacsony szinten maradt, míg csatornától függően napi 3-900 000 titkos kulcs generálódott [7].

Végül pedig a vezetékes kvantum-összeköttetések közül nem maradhat ki Kína 2000km-es linkje, amely 2016-ra 16 városi kvantumhálózatot kötött már össze Peking és Shanghai között, 32 csomópont felhasználása mellett. [8] A Mícius nevű kínai műhold segítségével (megbízható relé) Bécset is sikerült elérni, amely során tesztelés céljából egy kvantumkulcsszétosztással titkosított videokonferenciát tartottak a felek [9].

5 A magyarországi Plug & Play rendszer

Az elmúlt időszakban a BME Hálózati Rendszerek és Szolgáltatások Tanszéken lévő kvantumkommunikációs rendszeren dolgoztam, amely architektúráját tekintve egy 2002-es publikációt [10] vesz alapul. Száloptikás, vezetékes összeköttetésről van szó, amiben a polarizációs BB84 protokollal analóg, fáziskódoláson alapuló kvantumos átvitel valósul meg. Az adó-vevő egységek együtt egy nagy méretű interferométert alkotnak, az interferométer karjaiban gyenge, egyfotonos energiájú fényimpulzusok terjednek, a klasszikus 0 és 1 bitértéknek pedig a fényimpulzusok burkolóján végrehajtott fázistolások felelnek meg.

A rendszer kialakítása és működtetése a Plug & Play elgondolásának jegyében született meg. Telepítésekor egy automatizált inicializációs fázis teszi lehetővé a felhasználó beavatkozásának nélkülözhetőségét, mi több, használata során sem szükséges külön felhasználói monitorozás sem, ugyanis az esetleges hibaforrások (pl. hőmérséklet-ingadozás, támadások kiszűrése, …) kiszűrését is automatikusan végzi a rendszer. Ezen kívül az optikai út során bekövetkező lehetséges polarizációváltozás stabilitása és az interferencia kialakulásának feltételeül szabott egyidejűség is egyaránt biztosított benne.

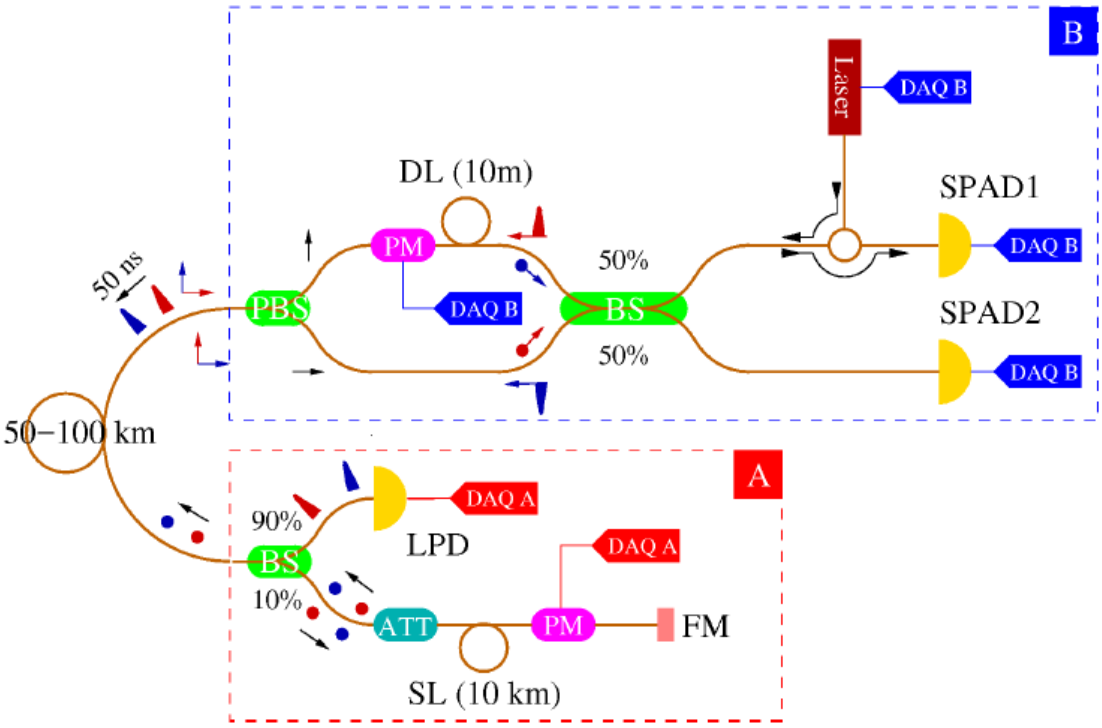
Nem szabad megfeledkeznünk az elrendezésből adódó költséghatékonyságról sem; a rendszerben helyet kapó eszközök közül a legdrágábbak és legérzékenyebbek – azaz a lavinaeffektuson alapuló egyfoton detektorok (single-photon avalanche diode - SPAD) és az impulzusvonatokat (frame) kibocsájtó lézer is – Bob oldalán, tehát a fogadó oldalon helyezkednek el. Ennek következménye az, hogy egy többfelhasználós szcenárió esetén csak a vevő oldali berendezés kerül kimagaslóan magasabb összegbe, a küldő oldaliéhoz viszonyítva. Ilyen kedvező eset állhat fent, ha például egy bankrendszerre gondolunk, ahol a bank oldalán van a vevőegység és az ügyfeleknél pedig csupán a lényegesen egyszerűbb, olcsóbb és meghibásodásra kevésbé hajlamos egység.

5.1 Felépítése és működése

A rendszeren elvégzett munkák felvezetéseként szeretném ebben az alfejezetben bemutatni magának az összeállításnak a működését, így még teljesebb képet nyújtva a projektben lévő szerepemről és a rendszer fejlesztésével, javításával és működtetésével

kapcsolatban felmerülő problémák és feladatok beható értelmezhetőségéhez. A működést a 4. ábrán látható sematikus elrendezésen lehet végig kísérni.

Habár a kvantumkommunikációs linkek és hálózatok túlnyomó többségében – mint ahogyan a legtöbb kommunikációs rendszer esetében is – a lézerforrást (vagy azt az eszközt, amit az információ előállítására alkalmaznak) az adóoldalon találjuk meg, érthető okokból kifolyólag. Esetünkben ez nem így van; a 20ns széles, 1550nm-es hullámhosszon kibocsájtott fényimpulzusaink forrása Bob oldalán helyezkedik el. E mögött a furcsa megoldás mögött az interferencia-alapú QKD protokoll azon követelménye áll, hogy az interferométerben a két interferáló gyenge fényimpulzus pontosan ugyan azt az utat járja be, ebből kifolyólag a karhosszak relatív megváltozása ne befolyásolja az interferencia kimenetelét. Ez azt is magával vonja, hogy az impulzuspárok egyszerre érkeznek a Bob detektorai előtt található 50/50 nyalábosztóhoz, ahol az interferencia történik. Ezt a feltételt pedig egyszerűen teljesíthetjük, ha Bob oldaláról indítjuk frame-jeinket. Hogy miért is?



4. ábra - A Plug & PLay rendszer sematikus ábrája

5.1.1 Bob oldala

A lézerből nagy fényintenzitással (>3mW) kibocsájtott fényimpulzusokat 5MHz frekvenciával, 200ns-onként küldjük egymás után, melyekből összesen 480 darab alkot egy frame-et. A kezdeti nagy intenzitás a megfelelő impulzusüzemű lézerműködés és nem a protokoll helyes működése érdekében megkövetelt paraméter. Éppen ezért, még mielőtt az iránycsatoló szerepét betöltő cirkulátorhoz elérkezhetne az impulzusvonat, áthalad egy csillapítón és egy izolátoron. Előbbinek az a szerepe, hogy a cirkulátor visszaérkező ágára csatlakoztatott detektort megóvjuk egy esetleges elvakulástól, míg utóbbi a lézert rendeltetett megvédeni a visszaszórt fénytől.

A protokoll következő állomása egy 50/50-es nyalábosztó (beam splitter, BS), mely a fényimpulzusok energiáját kettéosztják és két külön útra terelik: egy rövidebb, alsó karra és egy felső, hosszabb karra. A két kar közti különbséget a felsőn beiktatott 10 méteres késleltető szál (delay line, DL) adja, mely pontosan 50ns-mal késlelteti meg az ezen az ágon haladó impulzusokat – jelöljük ezeket piros színnel az ábrán – párjukhoz képest. Ezen túl található még hosszabb karon egy fázismodulátor is (phase modulator (bob), PMb), amit majd az impulzuspárok visszatérésénél fogunk felhasználni. Ekkor még csak a beiktatási csillapítását kell figyelembe venni, ami megközelítőleg 3,1dB. Fontos megjegyeznünk még azt a tényt, hogy Bob oldalán az összes szál polarizáció tartó. Emiatt, a polarizációs nyalábosztóhoz (polarization beam splitter, PBS) érkezve, az összetartozó fotonpárok annak működéséből eredően a PBS ugyanazon kivezetésén fognak tovább haladni, egymásra merőleges polarizácóval és egymást 50ns-mal követve.

5.1.2 Alice oldala

Az immár 960 impulzus (480 pár) egy 50-100km-es optikai szálon keresztülhaladva érkeznek meg Alice oldalára. Az építési fázisban csak néhány méter hosszú szálat iktattunk be Alice és Bob egysége közé. Egy több tíz kilométeres szál egyrészt nagyobb csillapítást eredményez – ennek értékét viszont szabályozni tudjuk Alice oldalán. Másrészt a fázissebesség-diszperzió miatt az impulzusok hosszának növekedését, valamint a rendszer időbeli stabilitásának csökkenését eredményezi. Ahogy egy frame beérkezik Alice-hoz, mindenekelőtt egy 90/10-es BS-en halad át, ami az impulzusok energiájának 90%-át egy lineáris detektorra (LPD) irányítja, ami az első monitorozási pont a rendszerünkben. A detektor jele alapján fogjuk tudni meghatározni, hogy mikor kell indítanunk a BB84-hez szükséges modulációt. A szükséges csillapítás

beiktatása miatt fontos, hogy a tovább haladó jelünk energiája csupán az eddiginek a 10%-a legyen – a nagy jelszint detektorba való kicsatolása pedig nem okoz problémát annak lineáris működéséből adódóan.

A gyengített jelünk ezek után egy szabályozható csillapítóhoz érkezik (attenuator, ATT), amellyel pontosan be tudjuk állítani a szükséges egyfotonos jelszintet, ami majd elvárt lesz a Bob oldalra való visszatéréskor. Az impulzusvonatunk ezt követően áthalad egy 10km-es tároló szálon (storage line, SL). Ennek az a szerepe, hogy az összesen 96μs hosszúságú frame minden impulzusa beérkezzen és összegyűljön Alice oldalán – a 10km hosszú szálra pedig fel is tud sorakozni mind a 480 impulzuspár oda-vissza. Alice oldalán ugyanis helyet kap egy Faraday-tükör (Faraday mirror, FM), amiről a fényt visszafordítjuk ugyanezen az útvonalon Bob irányába. Ezt azt vonja maga után, hogy a tükör felé haladó és az onnan visszaverődő impulzusok össze fognak találkozni a rendszer valamely pontján. SL nélkül ennek a helye bőven beleesne a két felet összekötő hosszú szálba, ahol Alice felé még viszonylag nagy fotonszámú, Bob felé viszont már csupán csak átlagosan egyfotonos impulzusok találkoznának. Alice felé haladva a nagy fotonszámú impulzusból Rayleigh-szórással visszaszóródó fény ekkor hozzáadódik a Bob oldala felé tartó frame-hez, így fals detektálást és megnövekedett zajszintet eredményezne a kommunikációban. A SL-on belül viszont közel megegyezik a jelszint a két haladási irány között, így ilyen probléma nem merül fel – főleg, ha azt nézzük, hogy a tároló szálat elhagyva visszaúton még egyszer áthaladnak impulzusaink a szabályozható csillapítón, amit ennek megfelelően állítunk be még az inicializálás során.

A SL és a FM között helyet kap még az Alice oldali modulátor (PMa), amely kulcsfontosságú szerepet játszik a protokoll során, hiszen PMa és PMb segítségével fogjuk megvalósítani a fázistoláson alapuló BB84 protokollt. Alice választ két bázis közül, hogy az itt áthaladó fotonopárok közül a későbbit melyikben fogja majd modulálni. Választása minden impulzus esetén véletlenszerű. A két bázis egymásra ortogonális: 0 – π és π/2 – 3π/2 közül válogathat. Ezen kívül azt is eldönti, hogy egy adott bázisban egy adott fotont milyen fázistolással modulálja – természetesen itt is minden esetben véletlenszerűen. Ezeket a döntéseket két, 480 hosszú, random előállított bináris bitsorozat alapján végzi el, melynek egyike a bázist, a másik pedig a fázistolás értékét felelteti meg a benne lévő 0-s és 1-es biteknek. Nagyon fontos azonban, hogy minden impulzuspár esetén csak és kizárólag a második, 50ns-mal késleltetett felet modulálja meg, hogy a másik megmaradjon referenciaként Bob számára. És mivel az impulzusok szélessége

20ns, így elméleti maximumként is csupán egy 30ns-os ablak áll a rendelkezésünkre a moduláció helyes időzítéséhez. Ez a 30ns viszont csak ideális esetben feltételezhető, a gyakorlatban sajnos még ennél is szűkebb a megtalálandó időrés.

A protokoll azonban itt még nem teljes. Az interferencia teljesüléséhez két feltétel szükséges, melyből az egyik a már korábban is emlegetett egyidejűség. A másik pedig nem más, mint a két interferenciára szánt hullám párhuzamos polarizációjának megléte. Hogyan is teljesülnek ezek a feltételek a fent leírt működés alapján?

5.1.3 Az interferencia kihasználása a protokollban

A Faraday-tükörről visszaverődő fény a tükör miatt 90-fokos polarizációfordulást szenved el. Ennek következtében a Bob oldalára visszatérő impulzuspárok fordítva csatolódnak a rövidebb, illetve a hosszabb karra és emiatt az interferencia helyéhez érkezve (50/50 BS) mindkét fél pontosan ugyanolyan hosszú úton lesz túl, hiszen most az szenved el 50ns-os késleltetést, amelyik eddig előrébb volt a másikhoz képest. S bár Alice oldalán a szálak Bobéival ellentétben nem polarizációtartóak, mivel oda-vissza áthalad rajtuk a frame-ünk, összességében ez nem fog változást okozni annak polarizációs állapotában. Így tehát összességében elmondhatjuk, hogy teljesül mindkét feltétel az interferenciára vonatkozóan.

A felső ágon haladó, eddig modulálatlan kék impulzus fázisát Bob a modulátorával megváltoztathatja, s ezt meg is követeljük tőle, hiszen része a BB84-protokollnak. Ugyanis Bob is véletlenszerűen váltakoztatni fogja a beérkező impulzusvonatok mindegyik tagjára vonatkozóan, hogy 0, vagy $\pi/2$ fázist tol-e rajta. Ez azért fontos, mert amennyiben egy adott foton esetében előbbit választja bázisnak és Alice is ebben a bázisban modulálta annak a konkrét fotonnak a párját még az ő oldalán – azaz 0 vagy π fázistolást végzett rajta –, akkor determinisztikus lesz az interferencia eredménye Bob oldalán. Amennyiben a bázisok megegyeznek, és az impulzuspár fáziskülönbsége 0, akkor a felső detektor szólal meg, amennyiben a fáziskülönbség π, úgy az alsó. A két SPAD detektálási eseményei végül megfeleltethetőek 1-es és 0-s biteknek, attól függően, melyikre érkeztek.

Ha viszont Bob nem találja el Alice bázisát, véletlenszerűen fog megszólalni vagy az egyik, vagy a másik detektor, így 50%-ban rossz értéket kapunk. Emiatt a BB84-protokoll szerint el kell végezni a bázisegyeztetést a két fél között és az azonos bázisválasztások esetén létrejövő biteket megtartva kialakul kettejük között a

szimmetrikus titkos kulcs. Ez a protokoll is azért lesz biztonságos, mert abban a pillanatban, hogy egy harmadik fél beleavatkozik a kommunikációba, a vételben kialakuló bitráta drámai szinten esni fog, így jelezve a betolakodó szerepét. S azt feltételezzük, hogy ezt csakis a két fél közti 50-100km-es szálon tudja megtenni, mert Alice és Bob egysége náluk van, fizikailag szeparáltan a külvilágtól. Ezen a szakaszon pedig már megközelítőleg egyfotonos jelszint mérhető az impulzusok energiáját tekintve, ahol már érvényesülnek a kvantummechanika törvényei, így biztosítva további, fizikai alapokon nyugvó védelmet a kvantumkulcsszétosztás procedúrájának.

Egyetlen dolog maradt már csak ki a rendszerarchitektúra bemutatásából, ami nem más, mint az Alice oldalán lévő másik lineáris detektor (LPD_m), melynek a visszatérő frame-ek esetében van szerepe. Ez a rendszerünk másik monitorpontja, amit az inicializációs protokoll során használunk fel. A két LPD detektorba érkező impulzusok alapján kiszámolható ugyanis az Alice oldali optikai úthossz, s innen meghatározható a PMa vezérléséhez szükséges moduláló jel késleltetésének nagysága, tehát az az idő, amennyivel az LPDs (az Alice felé tartó frame-eket detektáló első lineáris detektor Alice oldalán) jelzése után modulálnunk kell a kommunikáció során.

A rendszer működtetését, s az elmúlt egy évben elvégzett munkáimat a következő fejezetben szeretném bemutatni, a felmerülő nehézségekkel és a rájuk alkalmazott megoldásokkal együtt. A 7. fejezetben pedig mérési eredményekkel alátámasztva szeretném demonstrálni a QKD-ben implementált BB84 protokoll helyes működését és paramétereit.

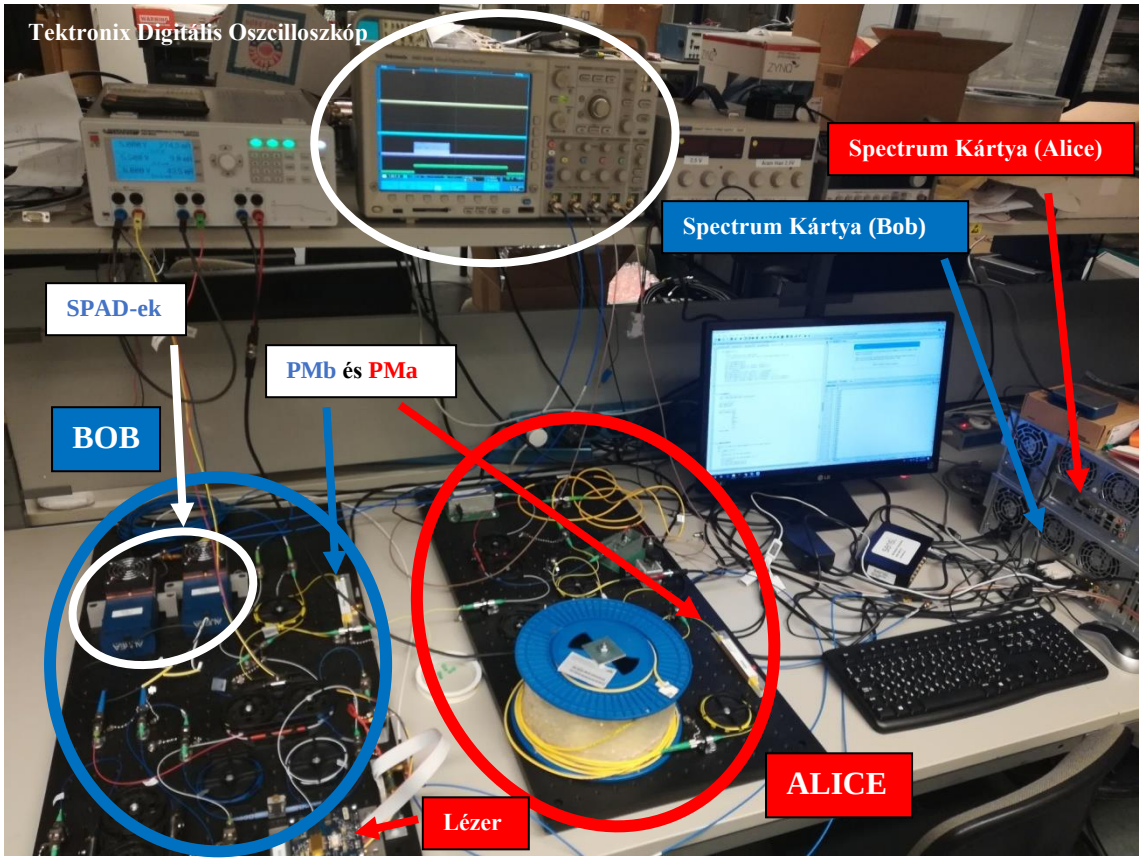
6 A rendszer működtetése

A jelen pillanatban meglévő összeállítás természetesen még nem áll készen a forgalomba hozatalra. Szempont az egyszerű, kompakt kialakítás, az olcsó és hatékony megoldások a működtetésre vonatkozóan, valamint a Plug & Play jelleg megvalósítása. Ezek eléréséig a folyamatos fejlesztése érdekében tesztelési és kutatási célokat tölt be a rendszer a projektben.

Működtetésének bemutatásához érdemes két külön részre bontani az architektúrát, melyet Alice és Bob panelje ki is jelöl számunkra. A paneleken kívül felhasználunk még két 16 bites önkényes jelforma generátort a Spectrum Instrumentation-től [11] (a küldő és fogadó oldal számára egyet-egyet), egy 2 csatornás tápegységet a lézer működtetéséhez, egy National Instruments által gyártott multifunkciós I/O adatgyűjtő (data acquisition, DAQ) kártyát [12] és végül egy Tektronix MSO 4140 típusú digitális oszcilloszkópot is, amire a működés alapjait építettük. Természetes az oszcilloszkóp alapú működés csak laboratóriumi mérések és demonstrálások céljára alkalmazható, ha kereskedelmi célokban gondolkodunk, akkor létezik egy ennél minden tekintetben (sebesség, ár, méret és gyakorlati megvalósítás) hatékonyabb megoldás a SensL időbélyegző kártyájának tekintetében (vagy idő-digitális átalakító – time-to-digital converter, TDC). Ez a kártya azonban sok kezdeti kalibrálást igényel, illetve a rendszerbe illeszthetőségét tekintve is kifejezetten nehézkes a használata. Ezek miatt ennek az eszköznek a használatát egyelőre félretettük arra az időre, amíg a projekt következő lépéseként a rendszer optimalizálása kerül majd terítékre.

A rendszernek mostanra alapvetően kétféle működését különböztethetjük meg: inicializálás és kommunikáció. Előbbire egy telepített rendszer esetében ritkán van szükség, hiszen a kezdeti paraméterek felvétele kerül sor alatta annak érdekében, hogy a kulcsszétosztás aztán megfelelően működhessen. Az inicializálás során beállítjuk a szükséges jelszinteket, megmérjük az Alice oldali optikai úthosszt és a Spectrum kártya alapkésleltetését, majd ebből kiszámoljuk a szükséges Alice oldali késleltetést a moduláló jel számára. Nagyszámú (pár ezer) frame-küldés után pedig kiszámoljuk a detektált fotonok beérkezési időiből a hasznos jel detektáláshoz szükséges vevő oldali rasztert is, azaz a nyers kulcsbitek várható érkezési időit. Ezen feladatok mindegyikében végeztem

fejlesztéseket és teszteléseket az elmúlt egy évet figyelembe véve, ezért is állhatott össze ez idő alatt a teljes inicializációs protokoll működőképes szintre.



5. ábra – A rendszer főbb részei

Utóbbi, tehát a kommunikáció során a kvantumkulcsszétosztást valósítjuk meg. Ehhez tudnunk kell a különböző bázisválasztásokhoz szükséges fázistolások megvalósításához szükséges vezérlő feszültségszinteket Bob és Alice oldalán is, melyek az architektúra következtében nem egyeznek meg, így kimérésre szorultak. Alice oldalán ezen kívül az LPDs által érzékelt beérkező frame-re válaszul képesnek kell lennünk egy megfelelő modulációs jel előállítására, amihez szükség volt a küldő oldali számítógépbe ültetett Spectrum jelgenerátor kártyának a teljes vezérlését kialakítani, ami alatt a kártya inicializálását, a trigger mechanizmus kialakítását, szükséges késleltetés beiktatását és a moduláló jel generálását kell érteni. Bob oldalán a beeső bitek feldolgozására van szükség, amivel egyidejűleg egy zajszűrés is megvalósul, majd az Alice által eltárolt kezdeti kulcs (véletlenszerű bázisok) saját bázisválasztásaival való összehasonlítása következik. Eredményül pedig megkapjuk a két fél közös szimmetrikus kulcsainak bitjeit.

6.1 Inicializálás

Az inicializációs eljárás 4 lépésből tevődik össze:

1. A szükséges jelszintek beállítása Alice és Bob oldalán egyaránt
2. Optikai úthosszok kimérése (Alice oldal, illetve a két oldalt összekötő 50-100km-es szál hossza)
3. Alice oldali alapkésleltetés és az ebből, illetve a 2. pontból összetevődő, a modulációba beiktatandó, szükséges késleltetés kiszámítása
4. Sok ezer detektálás alapján a Bobhoz beérkező fotonok várható időpontjai, detektálási raszter alapján

Célunk az, hogy ezek a lépések automatikusan végbe menjenek a rendszer telepítése során.

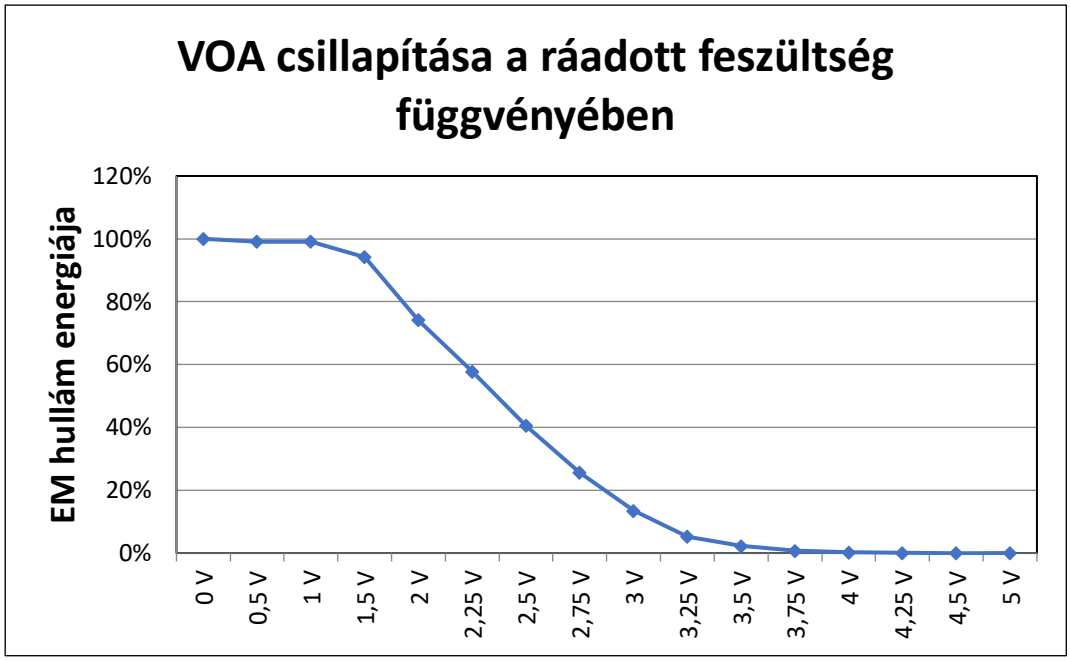
6.1.1 Jelszintek beállítása

Az inicializációs eljárás első lépéseként be kell állítanunk a rendszer két különböző pontján lévő állítható csillapítók szükséges jelszintjét. Az egyik Bob oldalán közvetlenül a lézer után kap helyet, a másik pedig Alice oldalán a SL előtt. Bob oldalon figyelni kell arra, hogy a lézer fényének a cirkulátorról a detektor felé való visszaszóródása ne legyen túl nagy, hiszen időlegesen elvakíthatja, vagy rongálhatja a fotodiódát. Ugyanakkor erős impulzusokat küldünk ki a lézerből, melyet annak működése követel meg. Így szükséges egy csillapító beiktatása közvetlenül a forrás után. Ideális értékeket kapunk a kommunikációs fázis során a frame-ek detektálására (3-4, néha 5 beütés egy detektorra), amikor a manuális (csavaros) optikai csillapítót 18,88dB-es csillapítási értékre állítjuk. Ekkor Alice oldalán az első lineáris detektorra érkező jel peak-to-peak feszültségértéke 2,7-2,9V között mozog és az Alice oldali állítható csillapítóval pedig 16,8dB-es csillapítást kell elérnünk.

Alice oldalán eredetileg egy hiszterézises, manuális csillapító állt, amely tökéletesen megfelelt arra a célra, hogy a Bob oldali vezérlőkódok működését, tehát a lézer használatát és az interferenciát tesztelhessük, hiszen csak a fent említett értékeket kellett beállítani a két oldalon fixen. Azonban a gyakorlati alkalmazás megköveteli a különböző módok használatát, így az inicializálás során a kommunikációs fázisban használttól eltérő feszültségszintet is. Az optikai úthossz méréséhez ugyanis nagyobb energiájú impulzusokra van szükség Alice oldalán. Az LPDs-be irányított nagy energia

miatt 10dB-t veszítenek az impulzusvonatok, amikor beérnek a küldő panelre, majd áthaladnak oda-vissza a csillapítón és végül azért, hogy egy részük megérkezhessen LPDm-re, újra át kell haladniuk a 90/10-es BS-en, ami újabb 10dB-t jelent. Már csak a BS-t figyelembe véve is legalább 20dB csillapítást szenved el a frame, összességében pedig – belevéve a többi eszköz beiktatási csillapítását is – egy ilyen szcenárióban jóval a lineáris detektor jelszintje alá kerül a jelteljesítménye. (Gondoljunk csak bele, hogy a visszatérő impulzusoknak egyfotonos körüli energiaszintre kell visszacsökkenniük ez alatt az út alatt.) Milyen jól jönne egy olyan csillapító, amit számítógépről tudunk vezérelni és kedvünkre változtathatjuk az értékét akkor is, amikor puszta kézzel már nem férünk hozzá az egyes panelekhez!

Szerencsére van is egy ilyen eszközünk, amit tavaly a csatornakarakterisztika kimérésére használtunk! Ez nem más, mint a Thorlabs V1550 elektromosan vezérelhető optikai csillapítója (voltage-controlled optical attenuator, VOA). A számunkra szükséges hullámhosszon is működik, bár más hullámhosszokra is megadták a karakterisztikáját az adatlapjában. Ezt a karakterisztikát egy éve ki is mértük és azt mondhattuk, hogy megfelel az előírtaknak. Vezérléséhez a National Instruments USB-ről működtethető multifunkcionális I/O eszközét használjuk, melynek soros portján többek között ±10V feszültséget is ki tudunk adatni, ráadásul a működtetésére készítettek egy pythonos könyvtárat is (nidaqmx.py), ami azért előnyös, mert a teljes rendszer összes vezérlőkódja és adatfeldolgozó script-jei egytől egyik Pythonban íródtak. Így tehát ezt is könnyedén rendszerbe tudtuk illeszteni.



6. ábra - A Thorlabs V1550 VOA egy éve általunk kimért karakterisztikája

Egy ideig azonban sajnos azt tapasztaltuk, hogy eszközünk az előírt maximális beiktatási csillapítás helyett közel 8dB-lel többel rendelkezik, ami egy eléggé magas érték. Karakterisztikája azonban megfelelő volt tesztelésekhez. Aztán később, egy hónappal ez előtt újra megmértem a beiktatási csillapítását, mely ezúttal tökéletesen az előírt értékeken belül helyezkedett el, 1,2dB-nek adódott. Ekkor kimértem, hogy mekkora a maximális csillapítása: a teljesítménymérő 36dB csillapítást jelzett, ami egybecseng a tavaly mért eredményekkel, hiszen ekkora érték megfelel egy, az eredetihez képest 0,25 ezrelékű teljesítményszintnek. A 16,8dB-es hiszterézises csillapítóból kiindulva 33,6dB csillapítást kellett elérnem a VOA-val ahhoz, hogy ki tudjam váltani vele elődjét. Teljesítménymérő használata mellett megállapítottam, hogy ez az érték 4,2V vezérlőfeszültségnél helyezkedik el. Eredményül Alice panelje kompaktabbá vált és lehetőség nyílt automatikus váltásra a kommunikációs protokoll és az inicializálás között, egy lépéssel közelebb érve a Plug & Play megvalósításához. Minthogy azonban az LPDm zajszintjének lényeges átlépése érdekében elegendően nagy jelszint (mérhető, felhasználható) eléréséhez még így is alacsony szinten voltunk, elhatároztuk, hogy Bob oldalára is beszerzünk egy ugyanilyen eszközt, hogy teljesen automatikussá válhasson a váltás, akár működés közben is.

6.1.2 Optikai úthossz mérése

Az optikai úthossz kimérése két szempontból fontos előkészület. Az egyik szempont az Alice oldalán található PMa megfelelő időben való modulálása, amihez tudnunk kell az Alice panelén helyet kapó szálak teljes optikai úthosszát. A másik pedig akkor lesz fontos, amikor a rendszert a gyakorlatban is telepítjük. Ekkor a két oldalt összekötő 50-100 km-es szál esetén pontosan (pár ns pontossággal) meg kell tudnunk mondani, hogy milyen hosszú a beiktatandó szál. Bár a gyártó feltüntet egy névleges értéket, a valóságban ez az érték ettől különbözhet, akár métereket is. (100km szál esetén 10 méter eltérés is csupán 0,01%-os hiba, cserébe közel 50ns optikai úthosszkülönbségnek felel meg.) Ez utóbbi méréssel nem foglalkoztunk behatóan, hiszen egy frame elküldése esetén LPDs-be beérkező nagy teljesítményű impulzusvonat első impulzusának és a küldés pillanatának különbségéből könnyedén megkapjuk a keresett értéket.

Az érdekesebb rész az Alice oldalának pontos megmérése. Érdekünkben áll ugyanis legfeljebb 1-2ns pontossággal meghatározni az aktuális hosszt, hiszen a modulációs ablak megtalálásához a késleltetést is nagyon pontosan kényszerülünk megadni. (Erről részletesebben a 6.1.3 alfejezetben olvashat.) A méréshez azt a kódot használtam fel, melyet egy évvel ez előtt a tárolószál hosszának ingadozásmérésére készítettem. Ez azon az elven működik, hogy a panelre beérkező frame-et odafelé LPDs, visszafelé pedig LPDm fogja érzékelni és a jelét kiküldeni a Tektronix digitális oszcilloszkópunkra. A két jelet a kód segítségével beolvassuk, analizáljuk és a két első impulzus felfutó élei közti távolságot kiszámoljuk. A kihívást az jelentette, hogy megtaláljuk azt a legkisebb jelteljesítményt, amely elegendő ahhoz, hogy LPD_m-re érkező jelet már fel tudjuk dolgozni (azaz, hogy magasabb legyen a teljesítménye a jelnek, mint a detektor saját zajának), de az ehhez szükséges Bob oldali alacsonyabb csillapítás még ne okozzon gondot a SPAD-ekre nézve. Ahogy elértük ezt a stabil jelszintet LPD_m-re nézve, a programunk segítségével erre az esetre is sikerült elérni a maximum 2ns-os bizonytalanságot. Korábbi mérésekkel ellentétben itt már nincs szükség a SPAD-ek leválasztására és az Alice oldali manuális csillapító kivételére, beavatkozás nélkül vagyunk képesek a hosszmérés elvégzésére.

6.1.3 Beiktatandó késleltetés számítása

Ott tartunk tehát, hogy megkaptunk egy optikai úthosszt, ami a két LPD között áll fent. De hogyan tovább? Amit szeretnénk meghatározni, az az az idő, ami alatt a fotonok eljutnak LPD_s-től PMa-ig. Ez a számunkra rendelkezésre álló idő arra, hogy az LPD_s a Spectrum kártyának triggerként szolgáló jelére az általunk előre elkészített moduláló jelalakot megfelelő késleltetés után kiadjuk a kártya kimenetén PMa-nak.

6.1.3.1 A késleltetést meghatározó körülmények

Vegyünk egy modulálandó impulzuspárt a 480 felsorakozó közül. A párból az elsőt még nem szabad modulálnunk, meg kell hagynunk Bob számára referenciaként. Így tehát meg kell várnunk, amíg az első, nagyobb energiájú impulzus elhagyja a modulátort visszafelé is, s csak ez után kezdhetjük el a modulációt. Minthogy 50ns-mal követi egymást egy összetartozó, 20ns széles impulzuspár, a kettejük közti különbség 30ns. Azt már tudjuk a hosszmérésekből származó tapasztalataink alapján, hogy Alice optikai úthosszát 2ns-os pontosság mellett meg tudjuk mérni, de a biztonság kedvéért számoljunk 3ns-mal. A 16 bites Spectum jelgenerátor kártya, amit a moduláló jel generálására használunk 500 és 625MSa/s mintavételezésre is képes, ami legjobb esetben is 1,6ns-os bizonytalanságot hozzátesz az időzítésünkhöz jitteréből adódóan, de számoljunk inkább 2ns-mal. Ezek az apró pontatlanságok pedig oda vezetnek, hogy 30ns-nál is kisebb időablak megtalálására kell kényszerülnünk. De mekkora is pontosan ez az ablak?

A 30ns-ból le kell vonnunk 3ns-ot a hosszmeghatározás miatt és legrosszabb esetben még 4ns-ot a jitterből adódó bizonytalanság következtében, azaz már csak 23ns résünk van a moduláció időzítéséhez. Ez még elsőre teljesíthetőnek is tűnik, azonban van egy kis bökkenő, ami nem más, mint a Spectrum kártyán beprogramozható késleltetés felbontása. Ugyanis a generálandó jelet természetesen nem tudjuk akármilyen felbontással tolni az időben – ez a mintavételezési képességükhöz szabott érték. 500MSa/s órajel esetén 16*2ns, 625MSa/s esetén pedig 16*1,6ns lépésközök oldhatóak meg. Ebből az következik, hogy előbbi esetet alapul véve mi csak 32ns-os pontossággal tudjuk időzíteni a jelünket, pedig legalább 23ns-osra lenne szükségünk. Ha kihasználjuk a kártyánk minden adottságát és a lehető legjobb mintavételezéssel működtetjük, akkor ez már kedvezőbben alakul: 25,6ns-os lépésközökkel késleltethetünk legfeljebb, viszont ekkor már 23,8ns is elegendő lenne. Azonban még mindig találnunk kellene valahol 1,8ns-ot a biztosan helyes működéshez. Természetesen éltünk még egy biztonsági

ráhagyással is az optikai úthossz mérésénél, amikor azt mondtuk, hogy számoljunk 3ns-on belüli pontossággal. Ezt is elhagyva már csak 0,8ns-mal vagyunk a határértéken kívül. De kívül vagyunk!

Persze ez csak akkor okoz gondot, hogyha minden egyes hibaforrás maximális értékkel jelenik meg és ha mindezek mellett a modulációhoz szükséges kiszámolt beiktatandó késleltetés egy olyan hosszértéknek felel meg, ami pontosan azok közé az intervallumok közé esik, ami legjobb felbontású késleltetéssel is ± 0,8ns-mal az ablakon kívülre időzítené a modulációt. Itt azért érdemes megállni és megvizsgálni, hogy milyen értékekről is beszélünk; az optikai úthossz esetén 4,8671 méterenként 16,36cm-es szakaszok azok a tiltott sávok, amik esetében nem tudunk pontos időzítést biztosítani és rosszkor kezdünk modulálni. Ez 3,36%-os valószínűségnek felel meg, ami annak az esélye, hogy az Alice oldali úthossz lemérése esetén olyan értéket kapunk, ami pont egy ilyen tiltott sávba esik.

A rendszer optimalizálása érdekében természetesen gondolkodtunk megoldásokon ennek a problémának az áthidalására is, melyek közül az elektromos jelút hosszának változtatása tűnt a legkézenfekvőbb és legegyszerűbbnek (a DL, vagy az SL változtatása mellett). A mérések eredményei viszont azt mutatták, hogy az Alice oldal hossza megengedi számunkra még a kisebb mintavételezés alkalmazását is a kártyán, ekkor képesek vagyunk a modulátortól elhaladó első impulzus után pár ns-mal elindítani a moduláló jelünket. A szükséges késleltetés kiszámítását pedig a [6.1.3.2] alfejezetben leírtak szerint végeztem.

6.1.3.2 Számítás menete

Először is a Spectrum kártya adatlapját vizsgáltam meg, ahol a késleltetésnél a már említett összefüggésen kívül ($T_{delay} = N * 16 * T_{CLK}$, ahol N természetes egész szám) az alábbi fontos paramétert találtam:

Trigger to Output Delay	sample rate ≤ 625 MS/s	238.5 sample clocks + 16 ns
	sample rate > 625 MS/s	476.5 sample clocks + 16 ns

7. ábra - Részlet a Spectrum jelgenerátor adatlapjából

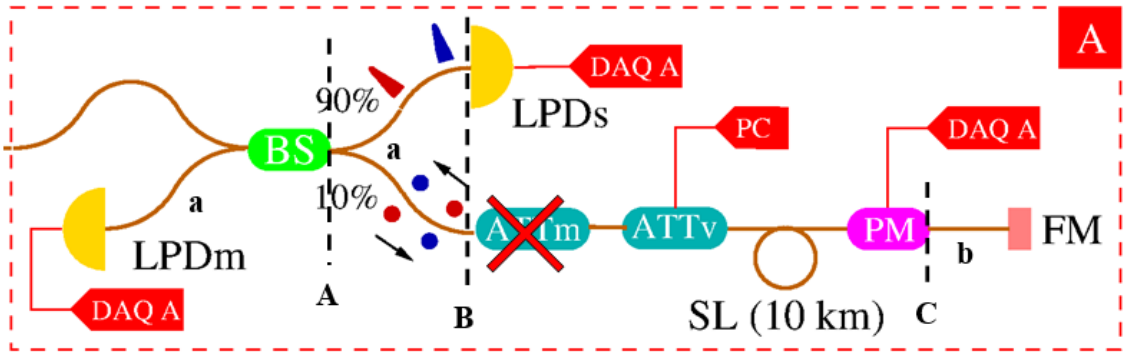
Mivel a mi rendszerünk az első kategóriába tartozik, ezért 238,5 * T_{CLK} +16ns alapkésleltetést bele kellett számolnom a végeredménybe. Ez 500MSa/s esetén 493ns. Ez természetesen nem okoz problémát, hiszen a fotonok detektálása után azok még áthaladnak a SL-on, ami közel 50µs ideig tart. Az már inkább problémát okoz, hogy ez

csak a kártya alapvető késleltetése, amihez még hozzá kell vennünk a koaxiális kábeleink hosszából fakadó átfutási időt is. Nagyfelbontású oszcilloszkópos méréseinkből kiderül, hogy ennek összértéke 510ns körül mozog, de ez vezetéktől függően változhat. Érdemes tehát ezt a távolságot indításkor megmérni.

Ekkor, ha a rendszer úgy van összeállítva, hogy T-csatlakozó segítségével egyszerre kap trigger jelet a kártya (LPD_s-ről), ami így monitorozható is az oszcilloszkóppal, illetve a generált moduláló jellel hasonló módon eljárva a hosszmérő kód segítségével ez is szépen mérhető. Le kell ugyan vonni belőle az ehhez az összeállításhoz szükséges plusz kábelek hosszát (az oszcilloszkóp és a kártya, illetve az oszcilloszkóp és PMa között beiktatott kábelekét). Pontosabb értéket kaphatunk, ha átszereljük az elrendezést, és oszcilloszkópon, kurzorok segítségével, elegendően kicsi időalappal előbb a trigger jelet, majd a moduláló jelet kötjük a detektor csatornáira. Így azonban elveszítjük az inicializálás Plug & Play jellegét.

Az alapkésleltetés megmérése után lefuttatom az Alice oldali úthossz mérésére írt kódomat. Ez megadja a két lineáris detektor közti távolságot. Mi azonban nem ezt, hanem az első detektorra beérkező jel és PMa-ra a visszaverődés után való megérkezés közti időt keressük. A két detektor közt eltelt idő fele pedig éppen ez a számunkra szükséges idő, ami azonban nem triviális. A BS karjai egyforma hosszúak, így a két detektorhoz vezető út is egyforma hosszúságú onnan, jelöljük *a*-val. Amikor LPD_s jelzi az első hozzá beérkezett impulzust, addigra frame-ünk már megtett *a* utat a VOA (ATTv) felé. Tehát a jelzés pillanatában az első impulzus éppen a 10%-os kivezetés végén tart. Innentől megteszi az FM-ig tartó úthosszt oda és vissza is, majd még kétszer az *a* távolságot, mire LPD_m-hez ér.

A PMa utáni (a 8. ábrán C-vel jelölt) pont az a pont, ahova várjuk a modulálandó impulzust, de csak visszaverődés után. A Faraday-tükör és a fázismodulátor között oda-vissza egy nagyjából 100cm-es szálszakasz helyezkedik el (2*b*, az ábrán). Összegezve tehát a távolságokat, a 8. ábrán alkalmazott jelölés alapján $t_{mért}$ = BC + 2*b* + CB + 2*a* felel meg a teljes, mért távolságnak, amiből mi a BC + *2b* értéket keressük. Minthogy *a* = 1m, *b* = 50cm és BC = CB, utóbbira adódik, hogy BC = $t_{mért}/2 - a - b = t_{mért}/2 - 1{,}5$m. Innen pedig már nem nehéz kiszámolni, hogy a keresett szükséges késleltetés hosszának értéke $t_{mért}/2 - 2{,}5$ns.



8. ábra – Alice oldali optikai úthossz számítása (segédábra)

Ezt az értéket kell tehát a korábban megadott képletek segítségével leprogramoznom, kivonva belőle az alapkésleltetést. Ezt sikeresen meg is tettem, legutóbbi beállításaimmal (98300ns volt a mért optikai úthossz és 508,4ns az alapkésleltetés) sikerült 6,9ns-mal az első impulzus vége utánra időzítenem a moduláló jelemet, ami 500MSa/s esetén is még éppen hibahatáron belül van. Maximális mintavételezéssel akár 13,62ns is lehet ez az érték, aminél tökéletesebbre nincs is szükség. (Ez 1,38ns távolságra van a keresett ablakunk közepétől.)

6.1.4 Raszter felállítása

Az inicializáló fázis utolsó lépésében a Bob oldalra beérkező jelfotonok várható detektálási időit kell megtalálnunk. Ehhez azt a kódomat használtam fel, amiről a 2019-es szakdolgozatomban be is számoltam. A kódot újbóli használata előtt végig néztem és átellenőriztem. Két apró hibát is javítani kellett benne, illetve az egyik algoritmust is felülbíráltam és átírtam.

A módszer során sok (ezres nagyságrendű) frame-küldés detektálásait dolgozom fel és összesítem. A nagy adathalmazból egyértelműen kirajzolódik, hogy vannak olyan szakaszok az időtengelyen, ami egy nagyobb beütésszámot foglal magába, nevezzük csoportosulásnak. Emellett elszórtan, más időpontokban is található egy-egy beütés. A csoportosulások meghatározzák a várható detektálási helyeket, míg az elszórt beütések zajból származnak. Minden egyes beérkezett fotonnak kiszámolom a szomszédjaitól vett távolságát, s ezek alapján könnyedén elhatárolódik, hogy mely beütések származnak biztosan a beérkezési idők köré csoportosuló jelbitekből és melyek azok, amelyek zajnak, vagy csak nagyon a csoportosulás szélére helyezkedett jelfotonoknak feleltethetőek meg. Itt, egy előjelhibát kijavítva, sikerült ezt az elhatárolást sokkal egyértelműbbé tenni, ezzel pontosítva az adatokból származtatott várható beütési rasztert.

A másik hibám egy elvi hiba volt. A távolságok alapján csoportosított jelbiteket eltároltam és beérkezési időik átlagát véve – melyet azért tehetek meg, mert Gauss-eloszlást követ a beérkezésük – egy közelítő értéket kaptam minden egyes bithez a 480 fotonból álló frame-ben. Ezután előállítottam több, 480 pontú rasztert, melyekben a raszterpontok távolságát, azaz a beérkezési periódusidőt apró lépésenként növeltem. 199ns és 201ns között kerestem ennek ideális értékét, méghozzá úgy, hogy megvizsgáltam, melyik periódusidejű raszter tér el legkisebb mértékben a feldolgozott csoportosulások beérkezési átlagaitól. Amikor megvizsgáltam a kódomat, észrevettem, hogy ezt az iterálást az első csoportosulás első fotonjához képest rögzítem, nem pedig az első csoportosulás átlagához. Ezt javítottam is. (Azért pont az első csoportosulást vizsgálom, mert minden frame legelső bitjének a legnagyobb az esélye arra, hogy detektálja egy 10%-os hatásfokkal rendelkező detektor, amilyen nekünk is van. Ebből következik, hogy az első csoportosulás lesz a legnagyobb sokaságú csoport. És az is következik belőle, hogy bizony lehetnek olyan beérkezési raszterpontok, ahova egyetlen foton sem érkezett az adatgyűjtés során.)

Végül pedig pont ezen a részen végeztem egy teljesítménybéli javítást, aminek köszönhetően gyorsabban fut végig a kód. Sikerült egy többszöri iterációs cikluson belül, egy egymásba ágyazott feltételvizsgálást eggyel megoldanom. Az alábbiakban látható előbb a régi, majd pedig az új verziója is a kódrészletemnek, melyek kiválthatják egymást (helyes működést eredményezve):

```
for j in self.groups_avg1:
    for idx,itm in enumerate(try_raster1):
        if idx < len(try_raster1)-1:
            if itm < j < try_raster1[idx+1]:
                  distance += min(abs(itm-j),abs(j-try_raster1[idx+1]))

for j in self.groups_avg1:
    mindist = 200
    for idx, itm in enumerate(try_raster1):
        dist = abs(itm-j)
        if dist < mindist:
            mindist = dist
    distance += mindist
```

A javítás után pedig többszöri, egyre pontosabb iteráció után sikerült végül megállapítanom 2ps-os pontossággal a beérkezés periódusidejét, ami $SPAD_1$ csatornáján 199,996ns-nak, míg $SPAD_2$-n 199,994ns-nak adódott. Első beérkezési helynek pedig 4500 frame-nyi adat alapján az első, feldolgozott csoportosulás beérkezési időátlagát vettem, ami körülbelül 450 érkezési időből adódó Gauss-eloszlású halmazból számolt

átlag. Ezt a nagy beütésszámot azért emelem ki, mert az egy évvel ezelőtti tesztek során csupán ezer frame kiküldésével teszteltem ezt a módszeremet. Ez az érték az első csatornán 98964,089ns, míg a másikon 98974,460ns (ezutóbbi tartozik $SPAD_2$-höz).

A kapott értékek a várakozásaimnak megfelelnek, hiszen egyfelől a periódusidőre egy 200ns-hoz nagyon közeli értéket kaptam, ami megfelel a kiküldési frekvenciához tartozó periódusidőnek, s ezzel a pontossággal 480 impulzus esetén is kevesebb, mint 1ns-os hibát véthetek. Másfelől pedig, ha az első raszterpontokat veszem figyelembe, akkor észre lehet venni egy 10ns-os különbséget köztük. Ez pedig éppen visszatükrözi azt a 2 méternyi optikai szálat, amit a $SPAD_2$ előtti cirkulátor ad hozzá az ebbe a detektorba beérkező fotonok úthosszához.

A rasztert tehát ezeknek az értékeknek megfelelően felépítettem külön-külön, mind a két csatornára, s a továbbiakban azokat a beérkező fotonokat fogom majd a kommunikációs fázisban jelfotonoknak tekinteni, melyek ezek köré az érkezési idők köré 25ns-os intervallumba esnek. Az ezeken kívülieket pedig zajnak fogom tekinteni.

6.2 A kommunikációs fázis kialakítása

A kommunikációs fázis a BB84 szerinti interferencia-alapú kvantumkulcsszétosztási protokoll implementálását foglalja magába. Ennek működtetéséhez az inicializálás során ehhez a fázishoz beállított jelszintek szükségesek és természetesen azok a vezérlőkódok, melyekkel a lézert, a detektorok gate-jeit, a paneleken található fázismodulátorokat és a frame-ek feldolgozásához alkalmazott, etherneten csatlakoztatott digitális oszcilloszkópot irányítjuk. Ezek közül a vezérlőkódok közül az Alice oldali modulátor vezérléséhez szükséges két Python kódot (*qkd_alice.py* és *spcm_utils_alice.py*) teljes egészében idén írtam, az oszcilloszkópra érkező frame-ek feldolgozásához tavaly írott kódjaimat pedig kiegészítettem a kulcsbitek meghatározásához a BB84 alapján (*pdp_mod_3.py*).

6.2.1 spcm_utils_alice

Ebben a modulban alapvetően a Spectrum Instrumentation 16 bites jelgenerátor kártyájának konfigurálása és vezérlése történik. A modul pusztán függvényekből áll, melyeket a Bob oldali kártya vezérlő modulja és 134 oldalas manuálja alapján írtam meg. Ahhoz, hogy tudjak rajta dolgozni, nulladik lépésként a kártya driverét telepíteni is kellett az Alice-hoz csatlakoztatott számítógépbe. Bár fel tudtam használni a Bob oldalt irányító

modult, mégis, sok esetben ez félrevezetett, vagy hátráltatott, mivel a két oldal Spectrum kártyájának konfigurálása nagy mértékben eltér egymástól. A memóriától kezdve, a triggeren át, egészen addig, hogy milyen ki- és bemeneti csatornákat és hogyan használunk, mindenben különböznek. Ezeknek a beállításaira egytől egyig oda kellett figyelni és a manuált maximálisan igénybe kellett venni a modul megírásához.

A 172 soros modul a telepített kártya beazonosítása (*open_card*) mellett képes a trigger mechanizmus kialakítására (*setup_card*) és ezzel együtt a trigger késleltetésének beállítására is. Megadja a kártya számára alapvetően fontos paramétereket (*setup_card*), mint például a mintavételezés sebességét vagy a memória és a buffer méretét, melyek a trigger eseményre való jelgeneráláshoz szükségesek. Itt lehet megadni azt is, hogy milyen jelalakot szeretnénk vele generálni (analóg/digitális, csatornaválasztás, generálás módja, stb.). Gondoskodik a szükséges jelalak bufferbe való betöltéséről (*load_data*) és a kártya programozott működésének indításáról is (*start_card*). Ezt a modult fogja majd a *qkd_alice* vezérlőkód importálni, hogy azon keresztül tudja lekommunikálni a kártyának a szükséges működést.

6.2.2 qkd_alice

Ez az a python vezérlőkód, amit az Alice oldalán lévő fázismodulátor vezérléséhez szükséges Spectrum kártyához írtam. A kód lényegi része az a függvény, ami a moduláló jelet állítja elő. Ehhez 4 különböző feszültségszintet állítunk elő, melyek segítségével 0, π, π/2 és 3π/2 fázistolást tudunk eszközölni az iXblue lítium-niobát elektromos-optikai fázismodulátorunkkal. A négy fázist szándékosan írtam ebben a sorrendben, hiszen az első kettő határozza meg az egyik, míg az utolsó kettő a másik bázisát Alice-nak, amelyekbe kódolni fogja a kezdeti kulcsbitjeit. A moduláló jel előállításához készítettem egy saját fejlesztésű python kódot.

A kód használatához természetesen szükségünk van a 4 moduláló feszültségszintre, ami sajnos egyáltalán nem triviális. Először is Bob oldalán a referenciafotonok összesen csak egyszer haladnak át PMb-n, míg Alice oldalán a modulációs információt hordozók jó esetben teljes egészében kétszer PMa-n. Ezen túl ezek a fázismodulátorok nem teljesen ugyanúgy működnek az egyik irányba, mint a másikba, fázisforgatásuk kismértékben eltér a két esetben. Így, bár korábban a Bob oldalán dolgozó kollégák PMb 0 és π fázistolását már kikísérletezték, számunkra ez nem jelent túl sok kapaszkodót a PMb feszültségértékeinek megadásában. Bob esetében 0-nak

a 0,0V, míg π-nek a 3,1V felelt meg, így gyanítani lehetett, hogy a szükséges π/2 fázistolásnak megfelelő feszültség a kettő felénél, 1,55V-nál kellett, hogy legyen, lineáris működést feltételezve.

Amennyiben Alice oldalán nem modulálunk, azaz a moduláló feszültség 0,0V, úgy csakis Bobtól függ, hogy milyen interferenciát kapunk. Így, ha Bob oldalán 0,0V-ot állítunk be – azaz ott sem történik moduláció –, akkor egyszerűen egy konstruktív interferencia történik, míg 3,1V-nál destruktív. Ha a kettő között modulálnánk, a feltételezett 1,55V-os feszültséggel, az azt jelentené, hogy a két detektorra egyenlő arányban érkeznének beütések, hiszen másik bázisba léptettem át Bobot a π/2 fázistolással. Az 1:1 arányt viszont a $SPAD_2$ előtt álló cirkulátor módosítani fogja, hiszen nem tekinthetünk el annak beiktatási csillapításától. Ezt a csillapítást egy útra kell ellenőriznem, mégpedig a visszaérkezés esetére (itt különbözik csak egymástól az impulzusok útja).

Ekkor P2 kivezetéséről P3 kivezetésére irányul a fény, s ez alatt 0,66dB csillapítást szenved el. Ez az érték teljesítményben 0,859-es szorzónak felel meg, aminek következtében a $SPAD_2$-re beérkező fotonimpulzusok energiája is ennyied részére csökken. Ez pedig azt jelenti, hogy a $SPAD_2$:$SPAD_1$ detektálási arány is ezzel fog megegyezni, ha átlagosan egyenlő számú impulzus érkezik rájuk. 100 frame küldésével ellenőrizve az 1,55V pontosságát a beütéseket feldolgozva 0,867-es arányt kaptam. Ez, átlagosan 3-4 beütéssel számolva frame-enként és detektoronként, 600-800 beütésre vetítve mi 100 frame esetén kevesebb, mint két beütéssel tér el a várt aránytól. Ez egy mérési pontatlanságnak is betudható érték, így az 1,55V-os értéket elfogadtam π/2 fázistolásnak.

Hasonlóan jártam el Alice oldalán. Az eddigiek függvényében már csak 3 feszültségértéket kellett beazonosítanom, π/2, π és 3π/2-nek megfelelőt. Minthogy rendelkezésemre állt már Bob oldalán mindkét bázis, így azokhoz igazítva, az előző módszer szerint tudtam keresni az azoktól különböző Alice oldali bázisértékeket. Először a π/2-höz szükséges gerjesztőfeszültséget kerestem, felhasználva a *qkd_alice* vezérlőkódot. Beállítottam, hogy melyik két feszültségérték között szeretnék vizsgálódni, majd azt is, hogy milyen lépésközönként szeretném ezt megtenni. Minden lépésköz során 100 frame-et küldtem ki Bobbal, amire válaszul Alice végig a lépésköznek megfelelő adott feszültségértéken modulált, majd lépett egyet. Így, önkényesen megválasztott

felbontás mellett képes voltam a detektálási adatokat feldolgozva megvizsgálni, hogy melyik értéknél van a legközelebb a két csatorna aránya a célul kitűzött 0,859-hez.

A π/2 fázistolás esetén ezt az arányt 1,22V-nál tudtam legjobban közelíteni, hasonlóan kicsi hibával, mint Bob oldalán 1,55-nél. 3π/2-nél azonban következetesen eltérő értékeket kaptam a már jónak hitt feszültségek esetén is (3,56V körül). Hosszabb idő eltelte után sem voltak pontosabb eredményeim, s ez arra adott gyanakvást, hogy itt talán máshogy viselkedik a modulátor, nemlinearitás lép fel a működésében, tehát a feltételezett szinuszos karakterisztika módosul. Ezt a feltételezést labortársam, Trócsányi Péter – BME-TTK mesterszakos hallgató – számolásokkal ellenőrizte és bár biztosra ő sem tudta megerősíteni, számolásai arra utaltak, hogy a szinuszos karakterisztika -π és π tartományon vehetőek jó közelítésnek. Ezen a tartományon kívül más, 8-ad fokú polinom illesztésével kaphatunk az eszköz működéséről pontosabb képet – itt már a moduláció pár ns-os pontatlansága és a mérési hiba összejátszása eredményezhet várakozásainktól eltérő feszültségértékeket.

Szerencsére, a fázismodulátor gerjeszthető negatív feszültséggel is, s ilyen jelalak előállítása nem jelent akadályt a Spectrum kártyánknak sem. 0-ra tükrözött értékként ki is próbáltam a -1,22V feszültséget is, ahol javulást véltünk felfedezni a korábbi mérésekhez képest, így kis keresgélés után meg is találtam a megfelelő működést biztosító -1,23V-ot. Nem maradt más hátra, csak a π fázistolás megkeresése. Ezt a pozitív feszültségek között maradva szerettem volna megtalálni, hiszen π/2-re és 3π/2-re is volt már eredményem (utóbbira csak közelítő). Szinuszos karakterisztikát feltételezve π helye pont e között a két érték között lesz félúton. (1,22 + 3,56) / 2 = 2,39. 2,39V-nál tehát teszteltem a rendszert (Bob oldalán 1,55V feszültséggel) és a teszteredmény meg is adta a várt 0,86 közeli arányt.

Természetesen, ezek után nyomban megvizsgáltam, vajon megegyező bázisok esetén tényleg csak az egyik csatorna szólal-e meg és bár kismértékben zajosabbnak tűnt a kommunikáció, mégis, egyértelmű volt a tendencia a jó működésre. A bázisaink fázisai tehát Bob oldalán 0.0 és 1,55 volttal (0 – π/2), míg Alice oldalán 0,0 és 2,39 (0 – π), illetve 1,22 és -1,23 volttal (π/2 – 3π/2) állíthatóak be. Nem maradt más hátra, minthogy teszteljük a kvantumkulcsszétosztásra felépített rendszerünket.

7 BB84 protokoll demonstrálása

A kitűzött cél az volt, hogy kidolgozzam egy működő, BB84-nek megfelelő protokoll fizikai rétegét a korábban felépített száloptikai hálózatból kiindulva. Az ehhez szükséges hardver és szoftver munkákat el is végeztem, a vezérlőkódokat kifejlesztettem. A működés demonstrálásához determinisztikus bázisválasztásokat alkalmaztunk, annak érdekében, hogy minél pontosabb képet kapjunk arról, hogy mennyire eredményesen követi le a rendszerünk a BB84 igazságtábláját. Ezt az igazságtáblát a saját rendszerünkre vetítve az 1. táblázatban prezentálom.

1. táblázat - BB84 igazságtáblája, vezérlőfeszültségek feltüntetésével

Alice bázisa	0	0	0	0	1	1	1	1
PMa feszültsége	**0,0**	**0,0**	**2,39**	**2,39**	**1,22**	**1,22**	**-1,23**	**-1,23**
Alice küldése	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**
Bob bázisa	0	1	0	1	0	1	0	1
PMb feszültsége	**0,0**	**1,55**	**0,0**	**1,55**	**0,0**	**1,55**	**0,0**	**1,55**
Bob fogadása	**0**	**-**	**1**	**-**	**-**	**0**	**-**	**1**

A kulcsszétosztás demonstrálásához mind a 8 esetben 100-100 frame küldése alapján vizsgáltuk meg annak eredményességét. Amit kapnunk kellett, az megegyező bázisoknál a fogadott jelbitek minél nagyobb arányú, Alice küldésével megegyező bit, kevés hibázás mellett. Amennyiben ez mindössze 50% körüli érték, az azt jelenti, hogy egy véletlengenerátornál nem sikerült többet alkotni. Ettől elkülöníthetően magasabb arány esetén már beszélhetünk kulcsszétosztásról – legalábbis, ami a fizikai réteget illeti. Hibás bázisválasztás esetén pedig a két detektorra eső beütések arányának vissza kellett tükröznie a már megállapított 0,859-es arányszámot, azok után is, hogy már kiszűrtük

belőlük a zajnak tekinthetőeket. Ettől jócskán eltérő érték esetén a rendszerünk hibás működést mutat. Ellenkezőleg viszont, minél jobban megközelíti ezt az arányt, annál eredményesebbnek mondható.

A mérés során először elvégeztük az inicializálás fázisát, kivéve a raszterpontok kiszámítását. Detektáltuk a 100-100 frame-et minden esetben, majd az összesített adatokat felhasználva a várható értékek meghatározását is elvégeztük, így pontosabb eredmények felé terelve a procedúrát. Joggal feltételezhetné az olvasó azt, hogy ezzel csaltunk, hiszen a beérkező adatok alapján állítottunk fel olyan paramétereket, amik segítségével feldolgozhatjuk magukat a beérkező adatokat. Nos, ha arra gondolunk, hogy a gyakorlatban is elképzelhető némi ingadozás hosszabb idő elteltével akár az úthosszban, akár az eszközök paramétereiben vagy teljesítményében, akkor máris elengedhetetlenné válik egy folyamatos, működés közben elvégzett korrekció, ami minimális ugyan, de a protokoll eredményességét ennyivel is javítva tulajdonképpen egy nagyobb bitrátát érhetünk el vele. Ez a menet közbeni korrekció pedig csak és kizárólag a működés során beérkező adatok monitorozásából származhat.

A frame-ek első impulzusa CH0-án 98976,032ns-nál volt a kiküldés után, s itt 199,992ns-os periódusidővel vártuk a biteket, míg a másik csatornán ezek az értékek 98985,778ns-nak (10ns-mal több most is, mint a másikon) és 199,996ns-nak adódtak. A protokoll eredményességét a 8 különböző esetre megvizsgálva a 2. és 3. táblázatokban foglalom össze. Előbbiben a megegyező bázisválasztásokat, utóbbiban az eltérőket mutatom be.

Zajbitnek nevezem azokat a detektálásokat, melyek a várható beérkezési pontoktól 25ns-os sugáron kívül helyezkednek el, a maradékot pedig jelbiteknek. Hibásnak nevezem a jelbitek azon bitjeit, melyek nem felelnek meg a determinisztikus működésből adódóan a várt értéknek (nem egyeznek meg Alice-éval). Végül pedig kiszámolom, hogy az összes jelbitnek detektált foton hány százaléka az, amelyik megegyezik az Alice által küldött bittel.

A 3. táblázat a 2-kal ellentétben nem a protokollban küldött bitek feldolgozásának konkrét sikerességét adja meg, hanem azt, hogy mennyire sikerült helyesen beállítani a bázisokat a protokollhoz. Mivel eltérő bázisválasztás esetén nem tudhatjuk, hogy helyes vagy helytelen értéket mértünk egy bitnek, felhasználni sem tudjuk a titkos kulcsunk kialakításához. Minthogy az interferencia-pontnál nem párhuzamos a polarizációja a fotonpárnak, teljesen véletlenszerűen, 50-50%-ban érkeznek meg az egyik, vagy a másik

detektorra. Ebből következik, hogy ha a bázisokat sikerült egymáshoz képest tökéletesen ortogonálisan felvennem (ami a gyakorlatban a feszültségek kimérésének pontosságán múlik), az eredmények is visszatükröznék ezt a fele-fele arányú detektálást – figyelve a cirkulátor csillapítására, 1:1 arány helyett 0,859 értéket mutatva.

2. táblázat – BB84 eredményessége százalékban kifejezve, megegyező bázisválasztások esetén

Megegyező bázisválasztás esetén				
Feszültségek (Bob – Alice) [V]	0,0 – 0,0	0,0 – 2,39	1,55 – 1,22	1,55 – (-1,23)
Fázisok (Bob – Alice)	0 - 0	0 - π	π/2 – π/2	π/2 - 3π/2
zajbit	25	34	46	53
jelbit	439	423	464	482
hibás (jelbitből)	11	34	65	105
sikeresség aránya [%]	**97,49**	**91,96**	**85,99**	**78,22**

Mivel zaj mind a két csatornán egyenlő mértékben jelen van, a zajnak minősített bitek nélkül is meg kéne kapnunk ezt az arányt, ha összehasonlítjuk 0-s és 1-es értékű bitjeinket. Nyilván tökéletesen pontosan nem fogjuk visszakapni ezt az arányértéket, de megfelelően közel lehetünk hozzá. Az aránytól való eltérés megmutatja, hogy pontosabb fázisok esetén hány bit kerülne még jó helyre. Természetesen ez is csak egy hibaforrás (a detektálás és az időzítés mellett), így ideális bázisokkal sem lenne tökéletes a rendszer, minden esetre a 3. táblázat utolsó sorából azt lehet látni, hogy legrosszabb esetben (tehát a két legpontatlanabb fázis esetén) 5,33%-kal térünk el a várt aránytól. Ez alapján azt lehet mondani, hogy a fotonok helyes detektorba való beérkezésének arányát – ezt megfeleltethetjük a 4 megegyező bázisban mért eredmények összesítésével – legalább ekkora mértékben javítani lehetne ezek tökéletes működése esetén. Az is megfigyelhető, hogy mivel a PMb gerjesztetlen állapotában nincs fázistolás, 2,21%, valamint további 4,67% javulást érhetnénk el ezek pontosításával.

3. táblázat - BB84 sikeressége eltérő bázisválasztások esetén

Eltérő bázisválasztás esetén								
Feszültségek (Bob – Alice) [V]	0,0 – 1,22		0,0 – (-1,23)		1,55 – 0,0		1,55 – 2,39	
Fázisok (Bob – Alice)	0 - π/2		0 - 3π/2		π/2 – 0		π/2 - π	
zajbit	46		44		53		49	
jelbit	671		659		679		653	
CH0 (0-s bit) és CH1 (1-es bit) beütései	353	318	371	288	356	323	370	283
CH1/CH0 --> 0,859	**0,901**		**0,776**		**0,907**		**0,765**	
Ideális aránytól vett eltérés	**2,21%**		**4,67%**		**2,52%**		**5,33%**	
Eltérés mértékéből fakadó hibás jeldetektálás	14,83		30,78		17,11		34,80	

Nyilvánvalóan az, hogy a rossz detektor helyett a jó detektorra érkezik egy impulzus, még nem garancia arra, hogy jelnek lesz feldolgozva, s természetesen tökéletes pontossággal sem vagyunk képesek beállítani a bázisfeszültségek előállításához szükséges feszültségszinteket. De egyértelműen látszik, hogy pontosításukkal a protokoll sikerrátája is javulhatna.

Ez a sikerráta pedig nem rossz, ha az igazságtábla eredményeit tekintjük (2. táblázat). A 0 – π bázisban való kommunikáció 90% feletti sikeressége magáért beszél, míg az eltolt, pontatlan fázisokat alkalmazó bázisban is biztonsággal 75% felett vagyunk. Ha pedig összesítjük ezeket az eredményeket, akkor determinisztikus viselkedés alapján, mind a 4, azonos bázisú (tehát kulcsbitet szolgáltató) esetet figyelembe véve átlagosan 88,11%-os hatékonyságról beszélhetünk. (Lásd a 4. táblázatban.) Nyomatékosan fel kell

hívnom a figyelmet arra, hogy ez az eredmény még nem a kulcsbitek létrejöttének sikeressége, hiszen ez után még sok, klasszikus lépésből álló utólagos feldolgozás és hibajavítás következik. Erre a későbbi fázisra azonban már nem terjed ki a kutatásom.

4. táblázat - Összesített sikeresség, a megegyező bázisok eredményeit figyelembe véve

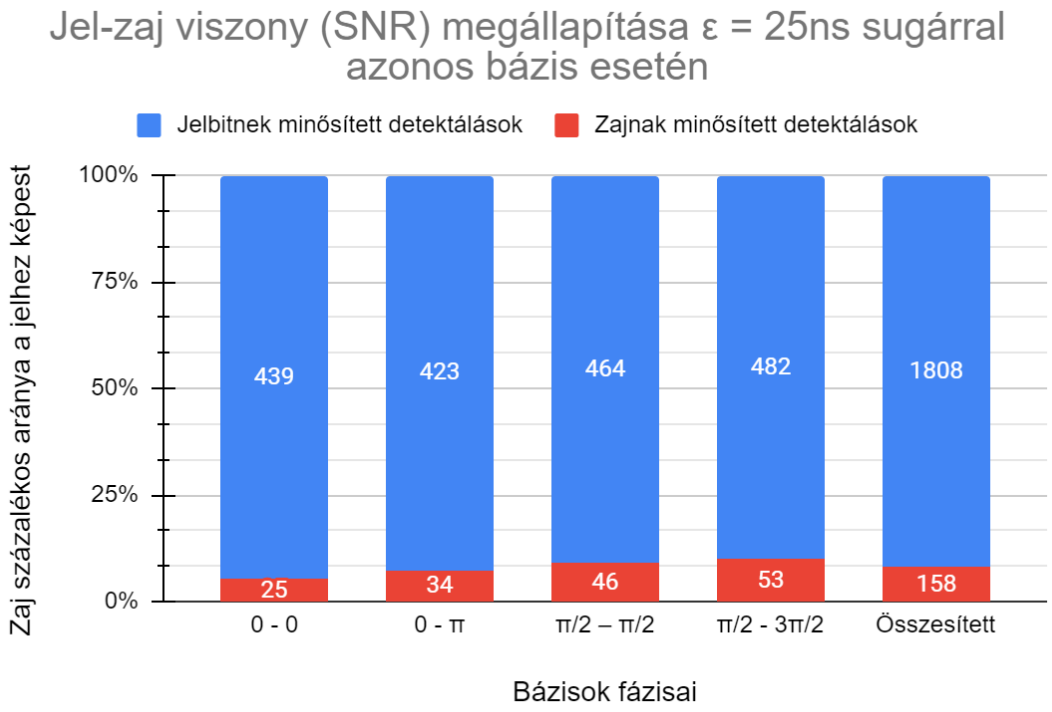
Összesített adatok (azonos bázisra)	
zajbit	158
jelbit	1808
hibás (jelbitből)	215
sikeresség aránya	**88,1084 %**

A módszernek van egy kulcsfontosságú része, ami nagymértékben beleszól sikerrátánkba. Ez nem más, mint az a beérkezési időpontoktól vett sugár, amin belül jelbitnek nyilvánítjuk a beeső impulzusokat, s amin kívül már csak zajról beszélünk. A fenti eredményeket ε = 25ns-mal kaptam, azaz egy detektálás távolsága, ha több volt ennél, már zajnak tekintettem. Felmerült bennem a kérdés, hogy mennyivel változik a sikerességem, ha ezt az ε-t csökkentem. Ekkor az történik, hogy szűkebb tartományon belül fogadjuk csak el a beérkező fotonokat jelből származónak és többet fogunk zajnak megfeleltetni. Viszont a beeső jelfotonok egy adott beérkezési hely körül gauss-eloszlást követnek. Ebből azt a következtetést vontam le, hogy egy meghatározott értékig csökkentve a tartomány szélességét, növelni tudom a sikerességi arányomat, bár a jelfotonjaim egy részét is el fogom így veszteni. ε = 25ns helyett megvizsgáltam a beérkezési időkből álló adathalmazomat ε = {12,5; 10; 5} ns-ra is.

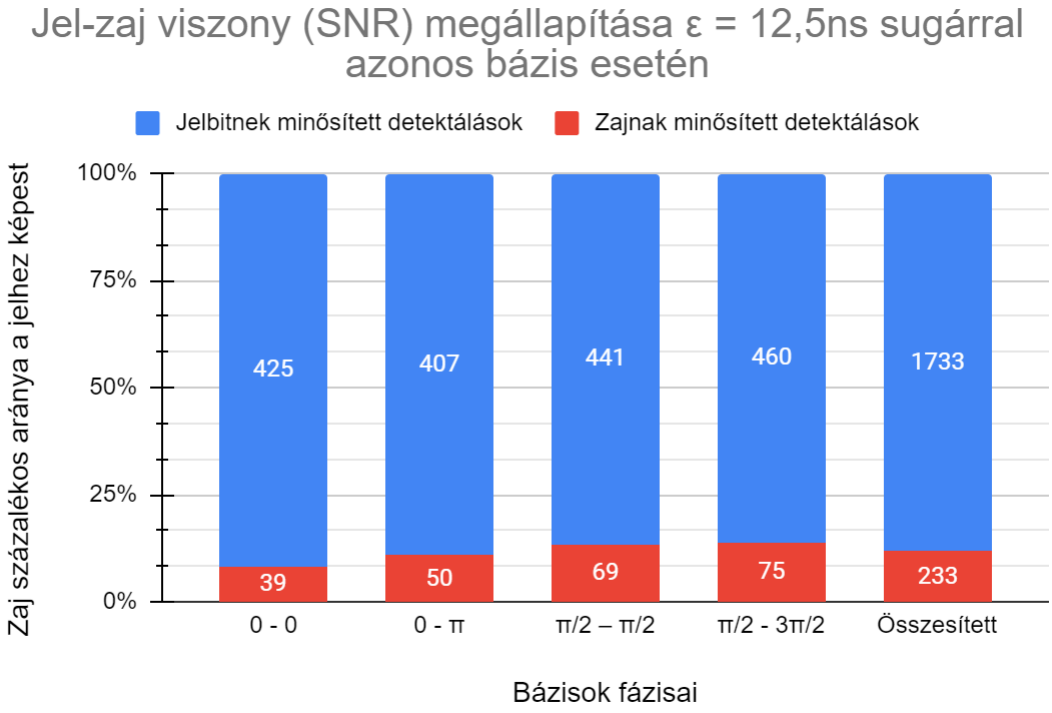
Az eredmények, melyek a 13. ábrán láthatók, szembetűnők. A sugár csökkentésével egyértelműen növelni tudjuk a sikerrátánkat, amit a legtöbb adattal leírt összesített eredményünkben lehet legszebben látni: 88,11%-ról 96,73%-ig sikerült javítani a bitek helyességét, ha 5ns-ig lecsökkentettük azt a tartományt, ahova a jelbitjeimet várom. Sajnos azonban csak áldozat árán tudtam megtenni ezt a javítást, hiszen ezalatt jelbitjeim nagyrészét is eldobtam: 91,96%-os jel-zaj viszonyból (SNR) ε = 5ns-ra csupán 49,90% maradt. Ez a javítás összességében egy helyesebb, de lassabb nyers kulcsbitsorozatot eredményez számunkra.

A karakterisztikából, melyet több ε értékre való feldolgozás mellett pontosabban becsülhetünk, látható az is, hogy egy ε egy adott értéke után lényegesen elkezd esni az SNR. Ahol ez a csökkenő görbe és a sikerráta növekedő görbéje metszi egymást, ott javíthatjuk nyers jelbitjeink sikerrátáján a legkevesebb áldozat árán a legkedvezőbben. Érdemes megfigyelni, hogy modulálatlan állapotban (azaz a moduláció általi hibaforrást kiiktatva) nem kapunk metszéspontot, de ε növekedése felé a két görbe közti távolság csökken. Így arra a következtetésre juthatunk, hogy moduláció nélkül a zajszint olyan kicsi, hogy megérné ebben az esetben még nagyobbra állítani a várható beérkezési tartományt annak érdekében, hogy esetleg találok még jelbiteket a zóna határa felé. (Anélkül, hogy több zajból származó beütést találnék, mint kinnrekedt jelbitet.)

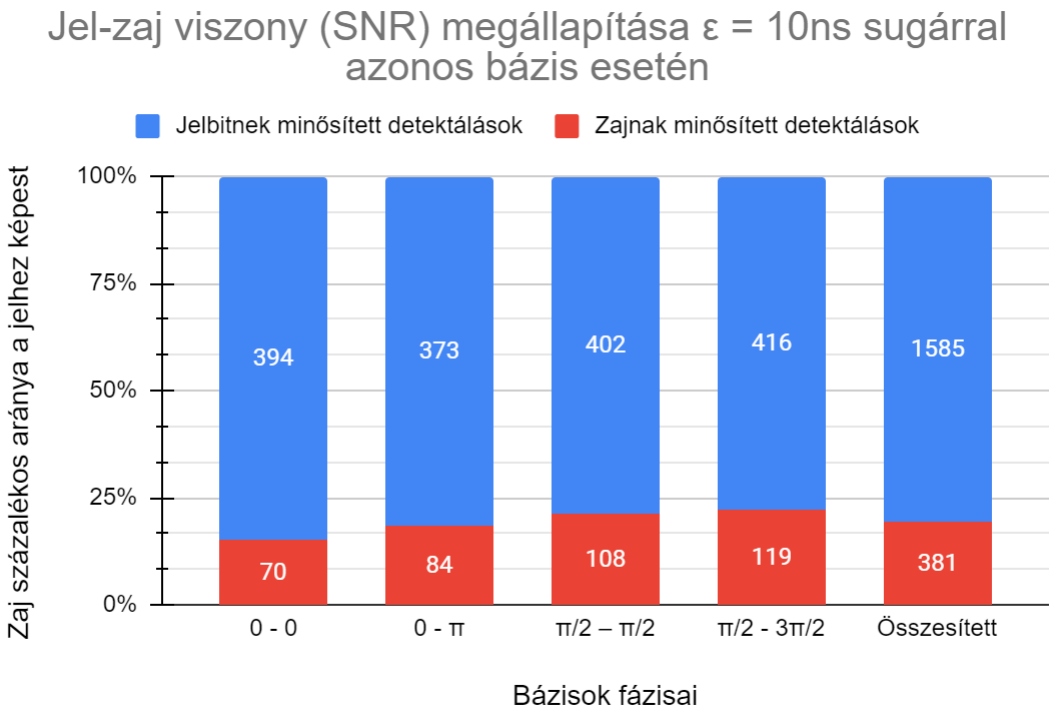
Itt is az összesített értékeket érdemes megfigyelni, hiszen az egyes szcenáriók teljességét adja meg. A 13. grafikonon lilával megtalálható görbék metszéspontja pedig 10 és 15ns között, 13ns környékén helyezkedik el. 400 frame feldolgozása alapján tehát azt lehet mondani, hogy a legjobb nyers kulcs létrehozásához a várható beérkezési időpontok körül megközelítőleg ±13ns-on belül beeső fotonokat érdemes jelbiteknek tekinteni. Az egyesített görbéket tartalmazó grafikon alapját képező értékeket a 9.-12. ábrák jelenítik meg.



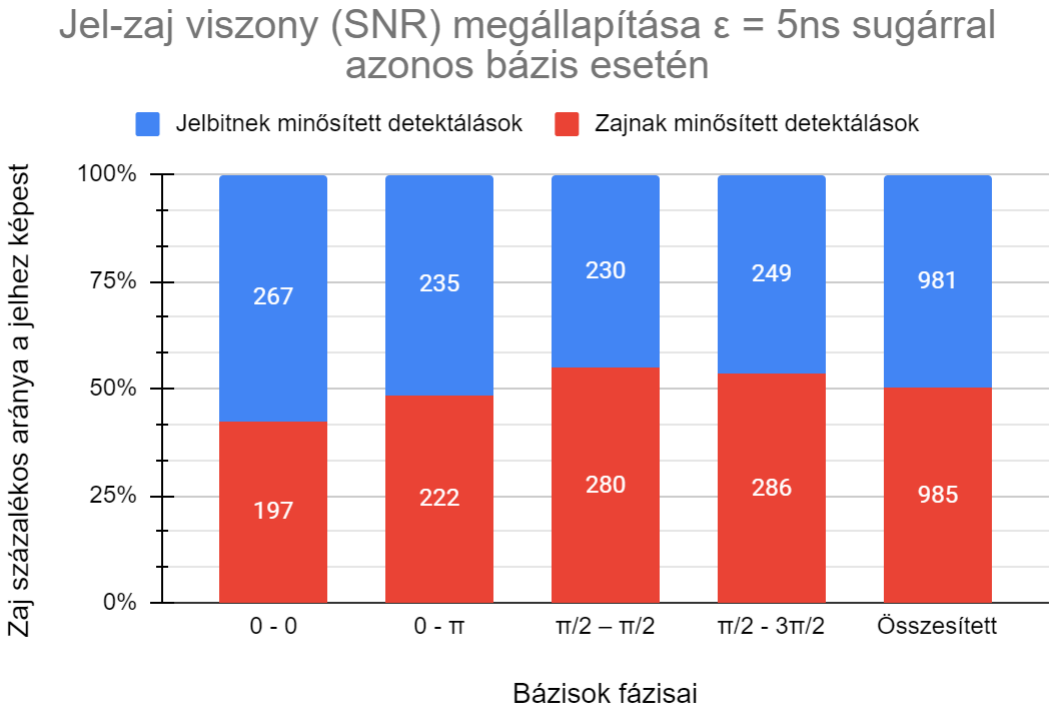
9. ábra



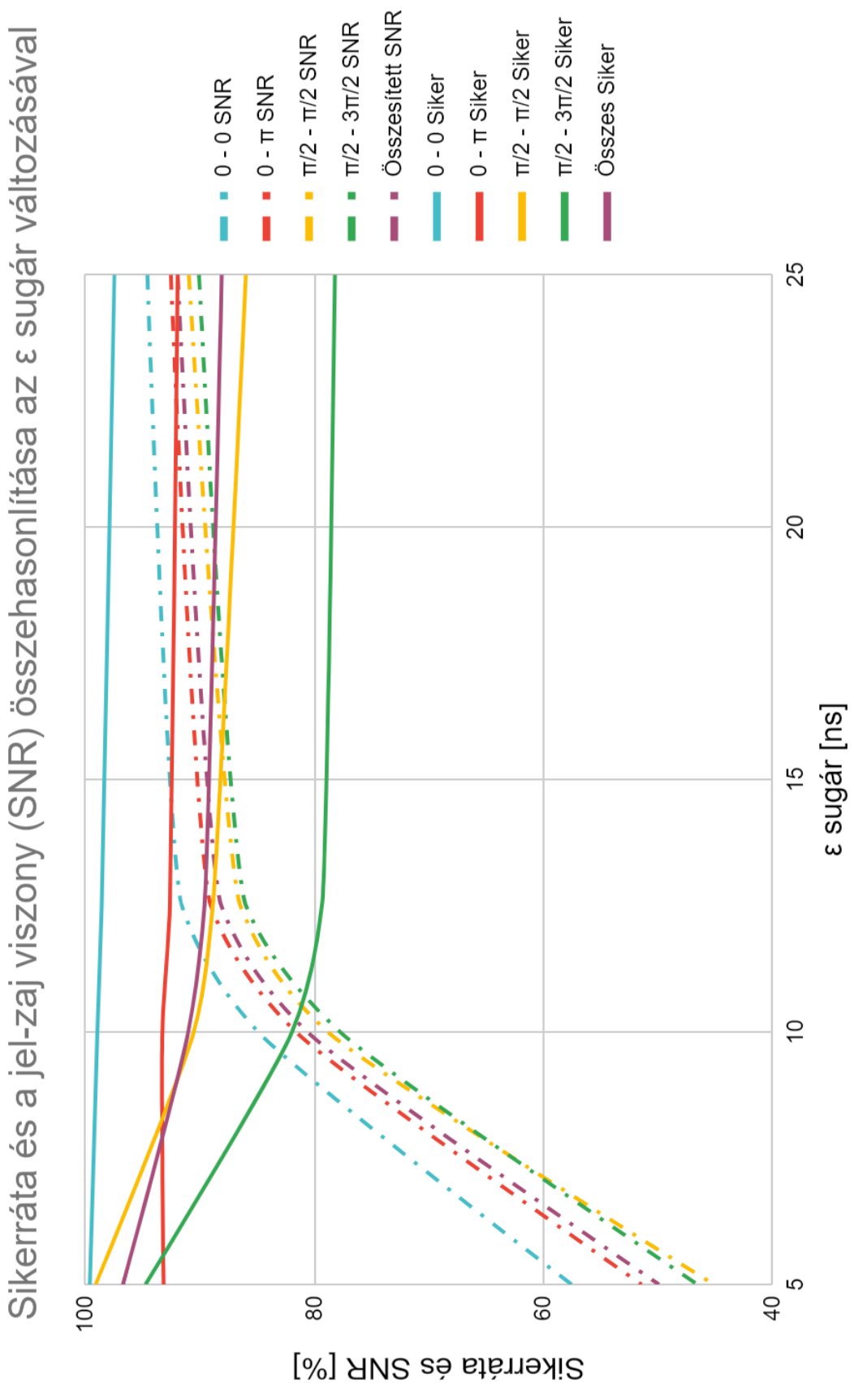
10. ábra



11. ábra



12. ábra


Sikerráta és a jel-zaj viszony (SNR) összehasonlítása az ε sugár változásával
0 - 0 SNR
0 - π SNR
π/2 - π/2 SNR
π/2 - 3π/2 SNR
Összesített SNR
0 - 0 Siker
0 - π Siker
π/2 - π/2 Siker
π/2 - 3π/2 Siker
Összes Siker
Sikerráta és SNR [%]
100
80
60
40
5
10
15
20
25
ε sugár [ns]

13. ábra

8 Összegzés

A dolgozatban demonstráltam az első magyar, BB84 protokollt implementáló kvantumkulcsszétosztó rendszer fizikai rétegének működését. Mindamellett, hogy a rendszer több helyén is számolhatunk hibaforrással, mely a kulcsszétosztás sikerességét befolyásolhatja, az eredmények biztatóak, kezdeti várakozásainkat pedig túl is teljesítették. Meg kell jegyezni, hogy a véletlenszerű működés alapos demonstrálására még nem volt lehetőség, így továbbra is izgalommal várjuk az eredmények teljességét elhozó teszteket.

Azt azonban látni lehet, hogy ahogyan a korábbi munkáimra is sikerült építkeznem és az onnan fennmaradó hibákat, tökéletlenségeket kijavítanom, ez esetben is bízom abban, hogy az eredmények kiértékelése során levont következtetések alapján – melyek javítási és optimalizálási lehetőségeket mutattak – a közeljövőben még magasabb szintre tudom fejleszteni QKD rendszerünket.

Felemelő érzés, hogy elsőként demonstrálhatok Magyarországon helyesen működő kvantumkulcsszétosztási protokollt, s ezennel is köszönöm Konzulenseimnek az idáig vezető út során a tőlük kapott segítséget.

Köszönetnyilvánítás

Köszönöm a munka elkészítése során nyújtott támogatását Trócsányi Péternek *(BME-TTK, fizikus mesterszakos hallgató)*, valamint Jánosi Gergelynek és Jókai Sándornak *(BME Hálózati Rendszerek és Szolgáltatások Tanszék, ESD-labor)*.

Köszönjük az Ericsson Magyarország Kft.-nek a munkában nyújtott támogatását.

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] M. Galambos, S. Imre, “Visualizing the Effects of Measurements and Logic Gates On Multi-Qubit Systems Using Fractal Representation,” International Journal on Advances in Systems and Measurements, **5**(1-2) (2012), 1–10.

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

[3] UNS Nice (France), Department of Physics, http://physique.unice.fr/sem6/2014-2015/PagesWeb/PT/Tomographie/?page=bb84

[4] 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, Optics Express **26(**5) (2018), 6010–6020.

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

[6] 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

[7] 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

[8] 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)

[9] 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)

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

[11] Spectrum Instrumentation: M4i.66xx-x8, M4x.66xx-x4, high-speed 16 bit, AWG, Arbitrary Waveform Generator, for PCI Express bus and PXI Express bus, Hardware Manual, Software Driver Manual (eng: 2020. feb.)

[12] National Istruments: *LabVIEW grafikus fejlesztői környezet leírása*, http://www.ni.com/ (2010. nov.)