



Budapesti Műszaki és Gazdaságtudományi Egyetem

Villamosmérnöki és Informatikai Kar

Hálózati Rendszerek és Szolgáltatások Tanszék

Sóki András

Kvantum csatorna integrálása meglévő optikai hálózatokba

OTDK dolgozat

KONZULENS

Dr. Gerhátné Udvary Eszter

BUDAPEST, 2023

Tartalomjegyzék

Összefoglaló.....	4
Abstract.....	5
1.Bevezetés	6
1.1 Titkosítás megoldása kvantumkommunikációval:.....	6
1.2 QKD elterjedtsége:.....	9
1.3 CVQKD és DVQKD:.....	10
1.4 Hálózatba integrálás lehetőségei	11
1.4.1 Összességében optikai hálózatban.....	11
1.4.2 Integrálás meglévő WDM-be	11
1.4.3 Külön WDM, QKD-nak	11
1.4.4 Időosztásos, WDM nélküli külön hálózat	12
1.4.5 Mindegyiknél felmerülő problémák	12
1.4.6 Általán vizsgált módszer	12
1.5 WDM Hálózatok bemutatása	13
1.5.1 WDM (wavelength division multiplexing) bemutatása	13
1.5.2 CWDM	14
1.5.3 DWDM.....	14
2. Egyetemi DWDM mérés	15
2.1 Demultiplexer karakterisztikájának meghatározása.....	15
2.1.1 S-LED bemutatása és a spektrumának meghatározása	15
2.1.2 Demultiplexer átviteli karakterisztika mérése	15
2.2 Áthallás vizsgálata más csatornákra.....	17
2.3 Eredmények összességének értékelése	19
3. Egyetemi CWDM mérés.....	21
3.1 Mérési elrendezés:.....	21
3.1.1 Használt eszközök:	21
3.1.2 Elrendezés:	22
3.2 Csatornák teljesítményének mérése	23
3.2.1 Üres, 1550 nm-es csatorna teljesítménye:	23
3.3 Mérések a spektrumanalizátorral:	23
3.3.1 Mérések a demultiplexer kimenetéről	24
3.3.2 Mérés a multiplexált, közös szakaszcson	25
3.3.3 Mérés a közös szakaszcson 30 km szál után:	27

3.4 Értékelés	27
4. Felmerülő zajok vizsgálata MATLAB számításokkal	28
4.1 Az erősítő zaja:.....	29
4.2 Áthallás a klasszikus csatornákból:.....	32
4.3 Raman szórás:	34
4.3.1 Elméleti háttér:	34
4.3.2 A szórás számítása:.....	36
4.4 Zajok összesítése:.....	38
4.5 Kulcsmegosztási ráta számítása	38
4.5.1 Modell DVQKD kulcsrátá számításra:.....	38
4.5.2 Modell CVQKD kulcsrátá számításra	41
4.5.3 Kulcsrátá számítás és eredmény értékelés:.....	42
4.6 Változtatható paraméterek hatása a CVQKD kulcsrátára	44
4.7 Értékelés és fejlesztési lehetőségek.....	45
5. Mérés a Telekom Laboratóriumában	46
5.1 Labor bemutatása:	46
5.2 Használt eszközök:	46
5.3 Mérések	47
5.3.1 Mérőeszköz zaja	47
5.3.2 Transzponder teljesítménye.....	47
5.3.3 Egy klasszikus csatorna a mux/demux-on át.....	48
5.3.4 Közös szakasz mérése 2 klasszikus és közöttük egy üres csatornával	48
5.3.5. Mérés a demultiplexer után, 2 klasszikus szomszédos csatornával	50
5.3.6 Mérés a WDM szakaszon, távolabbi klasszikus csatornákkal:	51
5.3.7 WDM szakasz mérése a klasszikus csatornák 10 dB-es csillapításával.....	52
5.3.8 WDM szakasz mérése 10 és 100 km szál közbeiktatásával	52
5.4 Értékelés	54
5.4.1 Táblázatos eredmények	54
5.4.2 Megállapítások az eredmények alapján:	55
5.4.3 Zajok eltérése a modellben és a mérésben	55
6. Összefoglalás	56
Források	58

Összefoglaló

A kriptográfia manapság egyre fontosabbá válik, hiszen már nem csak üzleti, kormányzati vagy hadászati okokból használják, hanem szinte mindenki találkozik vele, amikor valamilyen adata kerül továbbításra az interneten. A kinyerhető adatok mennyiségének és értékének hatalmas növekedése miatt az adatainkat egyre több támadás érheti, valamint a komolyabb védelmet igénylő adatokhoz egyre bonyolultabb védelmi technológiákat is kell alkalmazni.

Kvantum alapú kulcsszétosztással (QKD) a kommunikáció titkosításához használt kulcs teljes biztonsággal, lehallgathatatlanul tud eljutni a két félhez. Ráadásul a technológia már nem csak kísérleti fázisban van, hanem kereskedelmi forgalomban is elérhető.

Az elterjedést nagyban gátolja, hogy jelenleg kvantumkulcsszétosztást csak olyan sötét szálakon végeznek, amik kizárólag neki vannak dedikálva. Emiatt minden alkalmazáskor új optikai szál kell kihúzni a kommunikáló felek között, vagy a két fél közötti hálózaton folyamatosan rendelkezésre kell állni egy sötét szálnak. Gondolkodnak csak QKD-ra használt hálózat létrehozásán is, viszont ennek kiépítése hatalmas költségekkel járna.

A kvantum alapú kulcsszétosztás elterjedéséhez szükséges, hogy a technológia együtt tudjon működni a jelenleg alkalmazott és már kiépített, nagy adatátviteli sebességet biztosító klasszikus optikai hálózatokkal. A jelenlegi hálózatok gerinchálózatán egy optikai szálon hullámhossz multiplexálás (WDM) segítségével egyszerre akár 96 csatorna is működhet. Dolgozatomban főleg azt vizsgálom, hogy lehetséges-e egy kvantumos csatornát beleilleszteni egy ilyen hálózatba.

Bemutatom az egyes hálózati szegmensekben alkalmazott hullámhossz osztásos megoldásokat és választ keresek arra, hogy a különböző szegmensekben milyen módszer alkalmazható kvantum csatorna integrálására.

A legnagyobb problémát a klasszikus csatornák zaja jelenti, amik elnyomhatják a kis teljesítményű kvantum csatornát, ezért modellt készítettem Matlabban a különböző zajok hatásáról különböző távolságok és csatornaszámok esetén.

Mérést végzek az egyetemi laborban található CWDM és DWDM rendszerben a hálózati zajokról, valamint a Magyar Telekom központi laboratóriumában is végeztem mérést egy jelenleg a hálózatban is használatban lévő Huawei DWDM rendszeren, ahol azt vizsgáltam, mi történik egy kvantumosnak kiválasztott, üres csatornával különböző teljesítményű klasszikus csatornák mellé rakása esetén más-más távolságokon.

Abstract

Nowadays, cryptography is becoming more and more important, as it is no longer used only for business, government or military reasons, but almost everyone encounters it when some kind of data is transmitted over the Internet. Due to the huge increase in the amount and value of data, our data can be subject to more and more attacks, and more complex protection technologies must be used for data that requires more serious protection.

With quantum-based key distribution (QKD), the key used to encrypt communication can reach the two parties without eavesdropping and with complete security. Moreover, the technology is not only in the experimental phase, but is also commercially available.

The spread is greatly hindered by the fact that quantum key distribution is currently only carried out on dark fibers that are exclusively dedicated to it. For this reason, a new optical fiber must be pulled out between the communicating parties at each application, or a dark fiber must be continuously available on the network between the two parties. Experts and service providers are also thinking about creating a network used only for QKD, but the construction of this would involve huge costs.

In order to spread QKD, it is necessary for the technology to be able to work together with the high data transfer rate provider classical optical networks that are currently used and have already been built. On the backbone of current networks, on an optical fiber, up to 96 channels can operate simultaneously using wavelength division multiplexing (WDM). In my thesis, I examine whether it is possible to insert a quantum channel into such a network.

I measure network noise in the CWDM and DWDM system in the university lab. In addition, I also performed measurements in Magyar Telekom's central laboratory on a Huawei DWDM system which is currently used in the real network too. Here, I investigated what happens to an empty channel selected as quantum channel, when classical channels of different performance are placed next to the empty channel.

1.Bevezetés

1.1 Titkosítás megoldása kvantumkommunikációval:

A kriptográfia manapság egyre fontosabbá válik, hiszen már nem csak üzleti, kormányzati vagy hadászati okokból használják, hanem szinte mindenki találkozik vele, amikor valamilyen adata kerül továbbításra az interneten. A hagyományos titkosítási technológiák használatának növelése és a kinyerhető adatok mennyiségének és értékének hatalmas növekedése miatt az adatainkat egyre több támadás érheti, valamint a komolyabb védelmet igénylő adatokhoz egyre bonyolultabb védelmi technológiákat is kell alkalmazni.

Manapság a kvantum alapú kommunikációra a telekommunikáció új, nagy fejlődési lehetőségeként tekintenek, mivel ennek segítségével sokkal biztonságosabb információ továbbítás valósítható meg. Szinte naponta olvashatunk nagyobb támadásokról, amiben adatokat lopnak el. Ezeknek nagyobb cégek, bankok vagy akár kormányok közti adattovábbításban nem szabad előfordulnia.

Alapvetően kétfajta titkosítási módot használnak. Az egyik az aszimmetrikus, nyilvános kulcsú titkosítás. Ekkor a kulcspár egyik tagja publikus, a másik tagját pedig a nyilvános tagból készítik el különböző bonyolult matematikai műveletek segítségével. Ez a technológia azért nevezhető biztonságosnak, mivel a jelenlegi eszközökkel nem lehet ésszerű időn belül kikövetkeztetni a nyilvános kulcsból a titkos kulcsot. [1] Ugyan a nyilvános kulcsból a mai technológiával rendkívül nehéz és hosszú kikövetkeztetni a titkos kulcsot, viszont egy jövőben elkészülő kvantumszámítógép akár másodpercek alatt feltörheti ezeket. Az is problémaként merülhet fel, hogy támadók gyűjthetik a titkosított adatokat és a nyilvános kulcsokat, később pedig amikor rendelkezésre áll egy fejlettebb eszköz (leginkább kvantumszámítógép), akkor feltörhetik az adatok titkosítását. Ez főként hosszú időre titkosított, például katonai kormányzati vagy bankközi adatközlésre jelenthet nagy veszélyt. Ezekből is látszik, hogy a nyilvános kulcsú titkosítás milyen veszélyeket hordoz magában.

A másik titkosítási mód a szimmetrikus, privát kulcsú titkosítás, amikor a kommunikáló felek ugyanazt a titkos kulcsot használják a titkosításhoz. Vagyis a publikus csatornán egymásnak küldött (más számára nem érthető, titkosított) üzeneteket ugyanazzal a random bitsorozatú kulccsal fejtik meg. Ehhez viszont mindkét félhez el kell juttatni a kulcsot. Matematikai műveletek hiányában itt nem lehet kvantumszámítógépes feltörést alkalmazni, viszont a kulcs közvetítésekor lehetséges különböző lehallgatási módszerekkel megszerezni a kulcsot. Claude Shannon tétele szerint, ha az üzenet nem hosszabb, mint a kulcs, akkor a kulcs nélkül lehetetlen megfejteni az üzenetet [2]. Tehát a kulcs kiküldése az egyetlen gyenge pont. A nyilvános kulcsú titkosítások növekvő kockázata miatt egyre valószínűbb a szimmetrikus kulcsú titkosítás nagyobb térnyerése.

Ahhoz, hogy egy szimmetrikus kulcs használatával titkosított kommunikációban a kulcsokat elküldjük a feleknek, kvantumkommunikációt használhatunk annak tulajdonképpen lehallgathatatlansága miatt. Az alkalmazott megoldást kvantum

kulcsszétosztásnak (quantum key distribution – QKD) nevezik. Ennek a lényege, hogy a kulcsot kvantumkommunikációval juttassuk el a kommunikáló felekhez.

Míg hagyományos kommunikáció esetén az optikai szálon egy 1-es vagy 0-ás bit elküldéséhez rengeteg (több százszáz nagyságrendű, 0 dBm körüli impulzus teljesítményű) fotont küldünk, addig kvantumkommunikáció esetén egy bit küldéséhez mindössze 1 fotont (egy kvantumot) vagy pedig egy párszáz, párezer fotonból álló fotoncsomagot küldünk el. Az 1 foton használatával megvalósított kvantumkommunikációt DVQKD-nak (discrete-variable quantum key distribution – diszkrét változós kvantum kulcsszétosztás), a kisteljesítményű foton csomaggal megvalósítottat CVQKD-nak (continous-variable quantum key distribution – folyamatos változós kvantum kulcsszétosztás) nevezzük.

Azért, hogy megértsük, hogy miért is hasznos a kvantumkommunikáció alkalmazása a titkos kulcsok megosztása esetén, meg kell ismerni a No Cloning Theorem-et, vagyis a „Másolhatatlanság tételét”. A Born törvény [3] értelmében egy kvantumbit, megfigyelés nélkül, szuperpozícióban van. Vagyis, ha 2 állapotot definiálunk a kvantum valamilyen tulajdonsága szerint, akkor egyszerre mindkét állapotot felveszi. A tétel azt fejt ki, hogy lehetséges-e olyan eszközt készíteni, ami arra képes, hogyha a bemenetére adunk egy szuperpozícióban lévő kvantumbitet, akkor a kimenetén képes ugyanazt kiadni. A tétel pedig kimondja, hogy lehetetlen egy tetszőleges, ismeretlen kvantumállapot független és azonos másolatát létrehozni.

A Born törvény értelmében, a szuperpozícióban lévő kvantumot mérés esetén véletlenszerűen vagy 1-nek, vagy 0-nak értelmezhetjük, vagyis megváltoztatjuk a kvantum állapotát. Emiatt pedig egy esetleges lehallgatás észrevehetővé válik, a kulcs kiosztása megszakad, és a támadók, kulcs hiányában nem tudják feltörni a titkosítást. A legtöbb QKD protokoll esetén a kommunikáció második, ellenőrző felében mindenképpen fény derül egy esetleges lehallgatásra.

Először Stephen Wiesner írta le a QKD rendszerek teoretikus működését az 1960-as években. [4]

Érdemes tudni, hogy QKD megoldásokhoz alapvetően kétféle megoldási módszer létezik. Az egyik a prepare and measure (előkészít és lemér) alapján működik, a másik pedig kvantumösszefonódás alapján. Második esetben azt használják ki, hogy léteznek összefonódott kvantumpárok, amik bármilyen távol is vannak egymástól, ha egyszerre lemérjük őket, akkor mindig ugyanabban az állapotban vannak. [5] Az ezt használó megoldások viszont egyelőre fejletlenebbek és ritkábban használtak.

A következő nagy lépés a BB84 QKD protokoll megjelenése lett, amit 1984-ben dolgozott ki Charles Bennett és Gilles Brassard. [6] A BB84 protokoll is a prepare and measure módszerből indul ki. Ez talán a legtöbbet használt kvantumkulcs szétosztó protokoll és az egyfotonos, DVQKD megoldásra épül. Itt a foton polarizációját használják információként. 2 bázisban összesen 4 polarizációs állapot lehetséges. A titkosságát az adja, hogy egy lehallgató nem tudja, hogy melyik bázisban kell mérni a polarizációt, így nem lehetséges a külső lehallgatás. [7], [8]

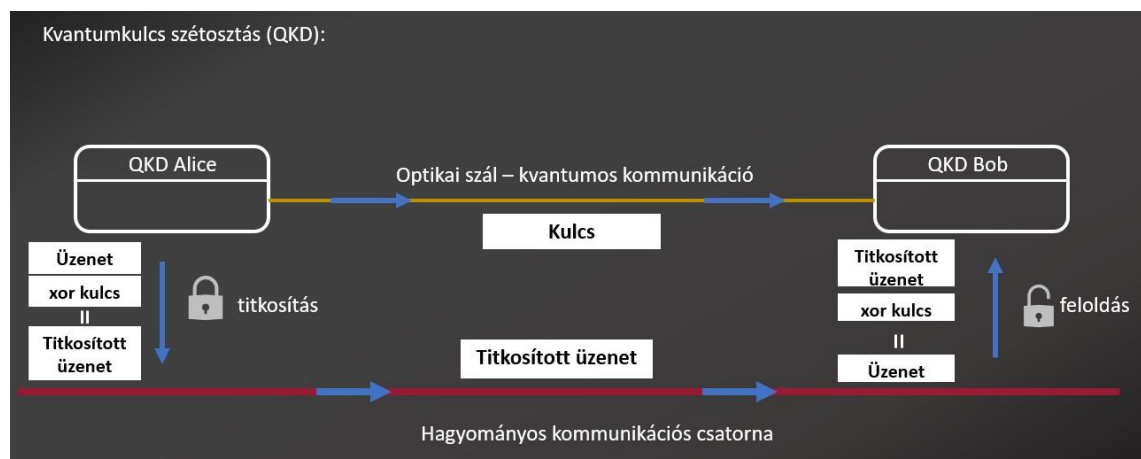
Fontos megjegyezni, hogy a kvantumozs kommunikációt csak a titkos kulcs kiküldésére használják, utána a kódolt üzenet már egy klasszikus csatornán érkezik.

Ha megtörtént a kulcsmegosztás és nem volt olyan körülmény, ami lehallgatásra utalna, akkor a kulcs valamilyen felhasználásával Alice titkosítja az üzenetet, amit utána Bob ugyanezzel a kulccsal megfejt. Legegyszerűbb esetben Alice a bináris üzenetéhez hozzáadja a kulcs bitjeit, majd az így kódolt üzenetet elküldi Bobnak. Bob pedig ugyanezt a kulcsot hozzáadja a kódolt üzenethez, így visszkapja az eredeti üzenetet.



1.1 ábra: egyszerű kódolás egy közös kulccsal (saját ábra)

Ezek alapján egy általánosnak mondható QKD alkalmazás a következőképpen néz ki



1.2 ábra: kvantumkulcsszétosztás sematikus működési vázlata (saját ábra)

Alice egy sötét (más csatornát nem tartalmazó) optikai szálon elküldi a kulcsot Bob-nak valamilyen kvantumkommunikációs protokollal. Miután mindkettőjüknek megvan a kulcs, Alice elküldi a közös kulccsal titkosított üzenetet, amit Bob ugyanazzal a kulccsal fel tud oldani.

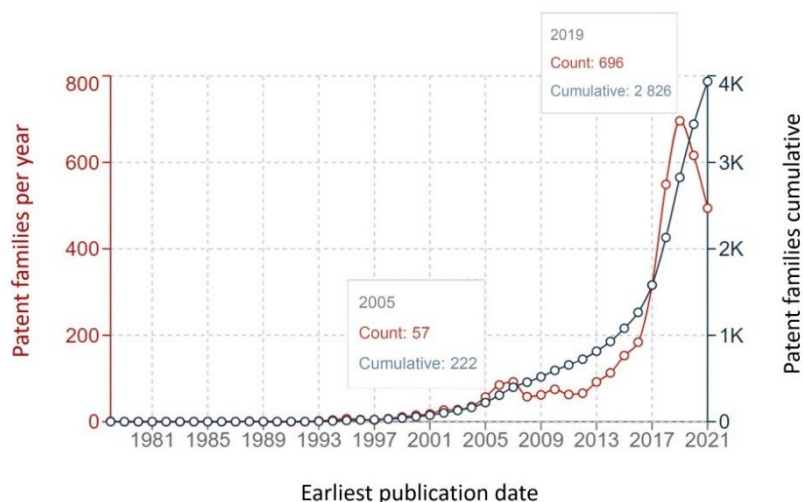
1.2 QKD elterjedtsége:

A 2010-es évek óta egyre több cég foglalkozik QKD berendezésekkel. Kis startupoktól egészen a nagy cégekig, mint a Telekom, Orange, Toshiba; egyetemektől állami kutatóközpontokig egyre népszerűbb és egyre több kutatás irányul a témára. 2007-ben például a svájci választási rendszer titkosításának egy részét is így oldották meg [9]. A QKD technológia bizonyított már optikai szálon, űrbéli pontok között és műhold-Föld közti kommunikációban is. Leginkább optikai szállal használják, mivel ott zavartalanabbul, akár 2x nagyobb távolságokban lehet kommunikálni. (A távolsági rekord földfelszínen vezeték nélkül 144 km, vezetékkel pedig sokáig 307 km volt, de most már 421 km-re is sikerült kulcsot megosztani [10]). A megoldást használják már bankok, kormányok, titkosszolgálatok, de már olyannal is kísérleteztek, hogy egy blockchain-en belüli titkosítást is QKD technológia segítségével oldanak meg [11].

A QKD egyben előnye és hátránya az is, hogy a legtöbb titkosítási módszerrel szemben itt külön hardverek és a külön hálózat is kell az alkalmazásához. Ez egyrészt megdrágítja (helyhasználat, eszköz vásárlás és hálózat építés) másrészt bonyolultabbá teszi a titkosítás módját. Ezen túl a kommunikáció fizikai rétegbeli elhelyezkedése megakadályozza abban, hogy a technológiát ott is használják, ahol csak szoftveres (vagy bármilyen, fizikai szintnél fentebb lévő OSI szinten) valósítják csak meg a titkosítást. [12]

A további problémák főként a megoldás pont-pont jellegéből adódnak. Az elterjedést nagyban gátolja, hogy jelenleg kvantumkulcsszétosztást csak olyan sötét szálakon végeznek, amik kizárólag a QKD-nak vannak dedikálva. Emiatt minden alkalmazáskor új optikai szálakat kell kihúzni a kommunikáló felek között, vagy a két fél közötti hálózaton folyamatosan rendelkezésre kell állni egy sötét szálnak. Dolgozatomban arra próbálok megoldást keresni, hogy miként lehetséges a már kiépített optikai hálózatokba integrálni kvantumcsatornát. Így nem kellene új szálakat kihúzni minden QKD alkalmazás esetére, ami nagyban megkönnyítené a technológia elterjedését és csökkentené az árát.

Az alábbi ábráról is látható, hogy az utóbbi időben mennyit foglalkoztak a témával.



1.3 ábra: látható, hogy az utóbbi évtizedekben évente (count) és összességében (cumulative) hány szabadalmat adtak ki valamilyen kvantumos kommunikációval kapcsolatban: [13].

1.3 CVQKD és DVQKD:

A kvantumkulcs szétosztásnak alapvetően két fő fajtája létezik most. Az egyik a DVQKD (discrete variable quantum key distribution), a másik a CVQKD (continuous variable quantum key distribution).

DVQKD esetén egy foton tulajdonságait, jellemzően a polarizációját használják fel a kommunikációhoz. Például a BB84 protokoll is ezen alapszik. Itt se feltétlenül minden esetben 1 db foton jelent 1 bitet, mivel az egyfotonforrás sem tökéletes, de ilyenkor is nagyon kevés fotonról beszélünk. Ezt a megoldást mondhatjuk inkább valódi kvantumkulcsszétosztásnak, mivel itt egy kvantumbit egy információs bitnek felel meg. Viszont nagy hátránya, hogy egyfoton forrást kell használni, ami egy sokkal drágább és bonyolultabb szerkezet. Ezen túl, ha elképzeljük, hogy 1 db fotont kéne küldeni egy több csatornát tartalmazó, egyébként zajos optikai szálra (vagyis WDM-re – wavelength division multiplexing), akkor józan ésszel belátható, hogy nagyon kicsi az esélye annak, hogy a foton átjut Alice-től Bob-ig és Bob ki tudja találni, hogy a sok zaj között melyik az üzenetértékű foton. Emiatt a DVQKD megoldást inkább csak sötét szálon érdemes használni, ami nagyban nehezíti az elterjedést, hiszen rendkívül költséges lenne annyi pont-pont hálózatot kiépíteni. Ezen kívül ritka az is, hogy egymástól messzebb levő eszközök esetén az eszközök közti hálózaton végig rendelkezésre áll üres szál.

CVQKD esetén nem egy darab fotonnal, hanem egy kevés (párszáz, párezer) fotont tartalmazó fotoncsomaggal kommunikálunk. Ennek az az előnye, hogy a több foton miatt nagyobb távolságra eljut és a különböző zajokra sokkal kevésbé érzékeny. Ennél a módszernél már nem a foton polarizációját használhatjuk információ kódolásra, hanem a nyaláb folyamatosan változó tulajdonságait, például amplitúdóját vagy fázisát, így rendelkezésre állnak magasabb rendű modulációk is. Általában amplitúdó vagy fázis modulációt használnak. [14] CVQKD esetén a biztonság nem olyan tökéletes, mint a BB84 protokollú DVQKD esetén, mivel itt a nehéz lehallgatást inkább a klasszikusnál nagyságrendekkel kisebb fotonszám adja. Hatalmas előnye viszont, hogy hagyományos optikai eszközökkel is kivitelezhető, így nem kell drága egyfoton érzékelőt és egyfoton forrást venni, hanem használható gyengített lézer és homodin detektor, amik jóval olcsóbbak és a beszerzésük könnyebb. A technológia előnye még a sokkal jobb zajtűrés, így ezzel a megoldással elérhetőbbé válik, hogy egy klasszikus csatornákat tartalmazó WDM hálózatba integrálják. Hátránya viszont a lassúság és az erősíthetőség hiánya: természetesen az erősítéssel értelmét vesztené a kvantumkommunikáció is. A legtöbb rendszer 1 Mbps adatsebességen dolgozik (vagy kevesebb), kb 50 Hz-es ismétlési rátával és átlagosan 25 km-es távolságig jut. [15]

A megismert tulajdonságok alapján, előzetesen a CVQKD mondható alkalmasabbnak egy jelenlegi hálózatba való integráláshoz.

1.4 Hálózatba integrálás lehetőségei

1.4.1 Összességében optikai hálózatban

Mivel a QKD során fotonokkal kommunikálunk, a kommunikáció mai ismereteink alapján leghatékonyabban optikai szálon történhet.

Ha a jövőben azt szeretnénk, hogy a QKD széles körben el tudjon terjedni, akkor hasznos lenne akár a jelenlegi hálózatba integráláson gondolkodni, vagy pedig különálló QKD hálózat létrehozásának a lehetőségeit is meg kell fontolni. A jelenlegi olyan pont-pont kapcsolat alapon működő megvalósítások, ahol új szálát vagy sötét szálát kell biztosítani a kulcsmegosztásnak (vagy bármilyen más később felmerülő kvantumkommunikációnak), nem hatékony se költségekben, se fenntartásban, se a megvalósítási időben. Igaz, hogy egyelőre kicsi az igény a QKD alkalmazására, viszont, ha később nagyobb lesz, akkor sem tudjuk kielégíteni költséghatékony és gyors megoldásokkal. Tekintsük át, hogy milyen lehetőségek merülnének fel egy QKD hálózathoz.

1.4.2 Integrálás meglévő WDM-be

A hagyományos optikai kommunikációban lehetséges, hogy egyidőben, azonos szálon több adatcsatorna működjön egyszerre. Ebben az esetben a csatornákat WDM-mel (wavelength division multiplexing – hullámhossz alapú multiplexelés) választják el egymástól. Így több csatorna futhat egyszerre, különböző hullámhosszokon. Ezen ötletet alapul véve feltételezhetjük, hogy a klasszikus csatornák mellé egy azokhoz közeli, vagy akár azoktól távolabbi hullámhosszra be lehet tenni egy kvantumcsatornát. A kihívás az, hogy a klasszikus csatornák zaja zavarhatja a sokkal kisebb teljesítményű kvantumos kommunikációt. Típusától függően, jelenleg akár 96 csatorna is működhet benne, valamint sok erősítő van a hálózaton. A következő problémák ezekből fakadnak. Ha DVQKD-t integrálnánk egy WDM hálózatba, akkor valószínűleg a rengeteg zaj szinte lehetetlenné tenné a QKD-csatorna működését. CVQKD esetén jobb lehet a helyzet. Az erősítés is problémát jelent, mivel az értelmetlenné tenné a kvantum csatornát, hiszen a kvantuminformáció nem másolható, így nem erősíthető. Ha a sok zaj túl nagy problémát jelent, akkor megoldás lehet a kvantum csatorna 1310 nm körüli csatornára tétele, míg a klasszikusak maradnak 1500 nm körül.

1.4.3 Külön WDM, QKD-nak

Felmerülhet megoldási módszerként, hogyha elterjed megfelelő mértékben a kvantumos kommunikáció használata, akkor egy, csak kvantumcsatornákból álló, WDM alapú különálló hálózatot is lehet építeni (bár ez egy elég költséges megoldás). Ebben az esetben az erősítés problémája kevésbé lép fel, mivel a klasszikus csatornák hiánya miatt nincs szükség rá.

1.4.4 Időosztásos, WDM nélküli külön hálózat

Felmerülhet még, hogyha nem akkorák az igények, hogy egy sokcsatornás hálózat szükséges, akkor elég egy 1 szálon 1 csatorna típusú, hagyományos hálózat. Ezesetben, ha egy QKD eszköz adni szeretne, akkor vagy a saját időszeletében adhatna, vagy jelezhetné valamilyen központi elemnek az adási szándékát.

1.4.5 Mindegyiknél felmerülő problémák

A legfontosabb talán az erősítés problémája. Mivel az nem lehetséges és a kvantumos jel nem tud elég messzire menni, ezért, ha távolra akarunk kommunikálni, akkor azt valamilyen közvetítővel lehet megoldani. Megmérni az adott fotont majd egy ugyanolyat tovább küldeni nem lehet a No cloning theory miatt. Sajnos a kvantum ismétlő még egy inkább elméleti és kísérleti fázisban lévő eszköz, ezért ennek a használata se lehetséges jelenleg [16].

Bármilyen módszerrel megvalósított QKD hálózatokban (akár jelenlegi hálózatba integrált, akár csak 1 külön QKD-csatorna, akár QKD WDM) ha nagyobb területet akarunk lefedni, mindenképpen kellenek 50-80 km-enként köztes Bob-Alice párok, amik köztes kulcsokat generálnak. Itt két probléma is felmerül. A könnyebbik probléma, hogy a köztes kulcsokkal, valamilyen protokoll szerint kell készíteni egy olyan kulcsot, ami a két végen lévő Bob-nak és Alice-nek is megvan és ugyanaz. Erre jelenleg kezdetleges protokollok és ötletek vannak. [17] A szerintem nagyobbik probléma az, hogy az összes köztes állomásnak biztonságosnak kell lennie, hiszen ezek a rendszer egyetlen gyenge pontjai. Ha egy ügyfél nem bíz a csomópontok fenntartójában – legyen az egy szolgáltató, egy állam, vagy mondjuk az EU – akkor az egész QKD értelmetlen. Ez ellen megoldást nyújthat, ha nem csak a QKD kulcs az egyetlen titkosítás az adott kommunikációban, hanem használnak még ezen felül más titkosítást is

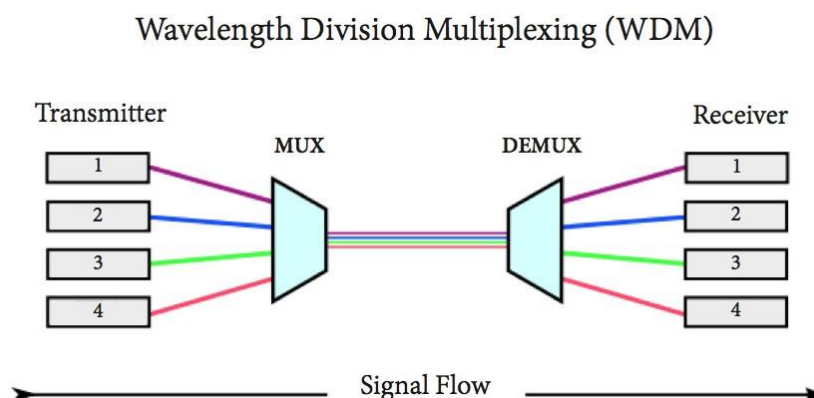
1.4.6 Általam vizsgált módszer

Szerintem talán a jelenleg legközelebb lévő megoldási módszer, amelyet érdemes vizsgálni az az, hogy egy jelenlegi WDM hálózatba hogyan lehet esetleg kvantum csatornát integrálni, mivel ez a megoldás nem jár új hálózat kiépítésével. Mivel a legnagyobb problémát a zajok jelentik, a dolgozatomban főként erre koncentrálok.

1.5 WDM Hálózatok bemutatása

1.5.1 WDM (wavelength division multiplexing) bemutatása

A közelmúltban robbanásszerűen megnövekedett hálózati igények hamar elfogyasztották a 20. század végén lefektetett fényvezető szálak kapacitását. A magas szálfektetési költségek elkerülése érdekében, valamint egy jövőt álló nagyságrendi kapacitásnövekedést eredményező megoldásként létrejöttek az ún. WDM hálózatok. Ezen hálózatok elve, hogy a különböző hullámhosszú/frekvenciájú optikai vivőket egy optikai szálon egyszerre, egy időben lehet továbbítani. Vagyis egy optikai szálon egyszerre több, különböző hullámhosszú csatorna fut. A hullámhossz multiplexálás működését legkönnyebben akkor érthetjük meg, ha a fehér fényre és egy prizma segítségével előállított „szivárványra” gondolunk. A szivárványt (különböző csatornák) fehér fénné (multiplexált jel) alakítjuk egy multiplexer segítségével, így egyszerre tudjuk szállítani a különböző hullámhosszú fényeket majd amikor újra kellene külön, akkor egy demultiplexer segítségével szétszedhetjük a csatornákat (a szemléltetésben újra külön színek lesznek a fehér színből).



1.4 ábra: multiplexeren és demultiplexeren alapuló egyszerű WDM sematikus rajza [18]

A WDM megoldást általában a hálózat core-nak vagy transport-nak nevezett részén használják, például egy olyan hálózatban, ami a nagyvárosokat köti össze, így hatalmas forgalmat bonyolít le. A mai változatokban akár 800-1200 Gbps sebességgel is működhetnek ezek.

A WDM-nek is több fajtája van, de alapvetően kétféle felosztás létezik: CWDM (coarse wavelength division multiplexing – durva felosztású hullámhossz multiplexálás) és DWDM (dense wavelength division multiplexing – sűrű felosztású hullámhossz multiplexelés). Mindketten egyszerre több hullámhosszú lézert fényt használnak a jelátvitelhez egyidőben, egyetlen szálon. A csatornatávolság, az átviteli hatótáv és a költségek szempontjából azonban a CWDM és a DWDM sok különbséget mutat.

1.5.2 CWDM

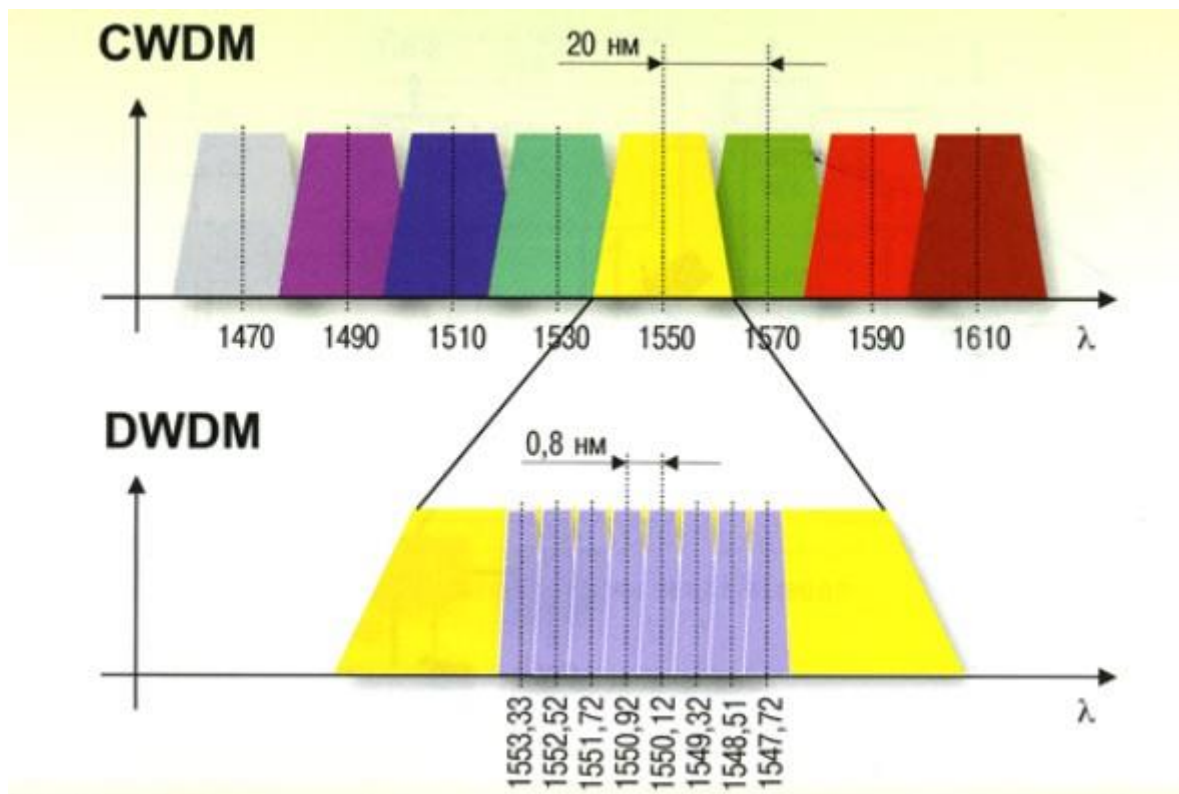
A CWDM technológiát manapság már egyre ritkábban használják és folyamatosan vezetik ki. A megoldás, fénykorában főként alacsonyabb rendű WDM hálózatokban (aggregációs vagy városi /metro) szolgált átviteli technológiaként. Az átvitel általában öt vagy hat hullámhosszon valósul meg 1270 nm és 1610 nm között, 20 nm-es intervallumokkal, de láthatóan a spektrumba belefér 16 csatorna is. A CWDM egy alacsonyabb költségű rendszer mivel egyszerűbb és olcsóbb lézer is elég a megfelelő működéshez.

A DWDM rendszerrel ellentétben a CWDM nem tud szinte korlátlan távolságot megtenni, mivel CWDM hálózatot nem lehet vagy elég nehéz erősíteni a túl széles használt spektrum miatt. A CWDM maximális hatótávolsága körülbelül 160 kilométer.

1.5.3 DWDM

A DWDM általában 40, 80, 96 vagy jelenleg legfeljebb 160 hullámhosszt tud továbbítani, szűkebb, 0,8 nm, 0,4 nm vagy 0,2 nm távolsággal az 1525 nm és 1565 nm közötti hullámhosszokon (C sáv) vagy 1570 nm és 1610 nm közötti (L sáv) sávon. Leggyakrabban 0,4 nm-es csatornák közti távot használnak. Az erősítés lehetővé teszi a DWDM számára, hogy hosszú távú - akár egy kontinensen átívelő long haul hálózatban is működhessen. Ezen okok miatt manapság már inkább DWDM hálózatokat használnak, így dolgozatomban is többnyire ezzel fogok foglalkozni.

Mindkét rendszerrel az a legnagyobb probléma, hogy az optikai átvitelnél felmerülő alapzajok (pl. Raman szórás, lézer háttérzaja) mellett még a szomszédos csatornákból érkező zajok is zavarnak.



1.5 CWDM és DWDM közti különbség bemutatása a spektrum, csatornatávolságok és csatornaszámok szemléltetésével [18]

2. Egyetemi DWDM mérés

Tehát hogy integrálni tudjunk egy kvantumcsatornát egy DWDM rendszerbe az kell, hogy a különböző hullámhosszú csatornák minél kevésbé zavarják egymást. Egy előzetes mérés keretében meg szerettem volna vizsgálni, hogy körülbelül mekkora zajra lehet számítani egy üresen hagyott csatornán, hogyha egy klasszikus csatornát teszünk valamelyik hullámhosszra. Ezzel az volt a célom, hogy megtudjam, hogy egyáltalán érdemes-e tovább foglalkozni DWDM-mel, vagy olyan nagy a zaj a kiválasztott üres csatornán, hogy lehetetlen lenne egy kvantumcsatornát odatenni. Annak megvizsgálását, hogy egy adott hullámhosszra beküldött csatorna mennyire „hallatszódik” át, egy Telekomtól leselejtezett, az MCL egyetemi laborjában található DWDM multiplexer/demultiplexer tesztelésével végeztem. Ideális esetben az alapszalon túl nem érzékelhetnénk áthallást más csatornáktól. A valóságban azonban a beküldött csatorna zaja a csatorna közelében erősebb lesz, valamint a csatorna elnyomott maradványa megjelenhet a demultiplexer után is a saját hullámhosszán.

2.1 Demultiplexer karakterisztikájának meghatározása

2.1.1 S-LED bemutatása és a spektrumának meghatározása

Az S-LED egy olyan fényforrás, ami egy nagyobb hullámhossz spektrumot lefedő fényt képes adni, ezért egy demultiplexerbe bekötve megnézhetjük, hogy az a nagy hullámhossz spektrumból mit enged át, tehát meghatározhatjuk a demultiplexer szűrőjének átviteli karakterisztikáját. Először érdemes meghatározni, hogy milyen spektrumot tud lefedni, mivel így láthatjuk, hogy tényleg lefedi-e a DWDM tartományt és tényleg tudunk-e vele demultiplexer átviteli karakterisztikát mérni.

Az S-LED spektrumának meghatározásához egy Anritsu MS9740B (modern) optikai spektrumanalizátort használtunk. A méréshez egy lézer szabályzó segítségével kapott tápot és hűtést az S-LED, aminek kimenetét rákötöttük a spektrumanalizátorra.

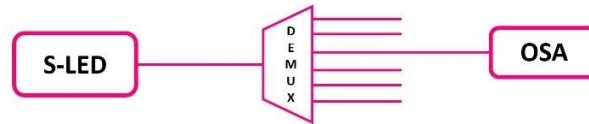
Az eredmény alapján az S-LED 1515 nm és 1580 nm között szinte stabilan képes -15 dBm körüli jelet adni. Mivel a DWDM spektrum (ahol a csatornák vannak) a leggyakoribb esetekben 1525 és 1565 nm közé esik [19], ezért az S-LED bőven lefedi a tartományát.

2.1.2 Demultiplexer átviteli karakterisztika mérése

Mivel az S-LED lefedi a teljes DWDM tartományt, ezért szűrés nélkül a teljes S-LED spektrum teljesítményeit látnánk a spektrumanalizátoron. Viszont mivel a demultiplexernek az a feladata, hogy a bemenetre kapott multiplexált fényből csak az adott hullámhosszra engedjen ki jelet (vagyis, ha pl. a kimenet 1550 nm-es, akkor az adott kimenet szűrője más hullámhosszú jelet elvileg nem engedhet át), ezért ideális esetben

csak egy nagyon keskeny hullámhossz sávban láthatunk jelet. Ebben a mérésben ezt ellenőriztük.

A kísérletet a következő elrendezéssel valósítottuk meg:

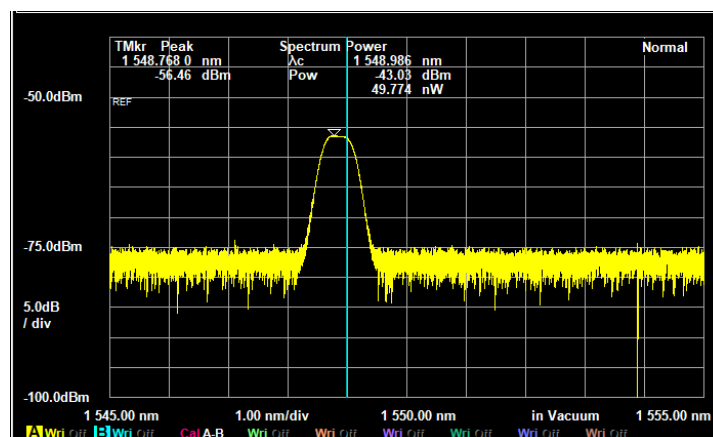


2.1 ábra: 2.1.2 kísérlet vázlatos elrendezése. Magyarázat 2.2 ábra leírásában



2.2 ábra: 2.1.2 kísérlet valós elrendezése. Bal oldalon található a szabályzó, ami táplálja az S-LED-et; ezután az S-LED be van kötve a 24 kiemelt DWDM demultiplexer eszköz (ONS15801) bemenetére, hátra. A demux elején egy véletlenszerűen kiválasztott kimeneti csatornára van rákötve a jobb oldalt látható spektrumanalizátor.

A mérés eredménye itt látható:



2.3 ábra: 2.1.2 mérés eredménye a spektrumanalizátoron. Magyarázat a kép alatti bekezdés szövegében

Az alsó vastag sárga a különböző forrásokból származó zaj, a csúcs pedig a szűrő által átengedett jel. A mérésből az olvasható ki, hogy a maximum pont 1548.7 nm-nél van, vagyis a kimeneti csatornának, amire rákötöttük a spektrumanalizátort, akkora a hullámhossza. A teljesítménye pedig -56 dBm, ami annak függvényében nem olyan rossz, hogy az S-LED teljesítménye (1548 nm-en) -47 dBm körüli. A megfigyelés tehát, hogy

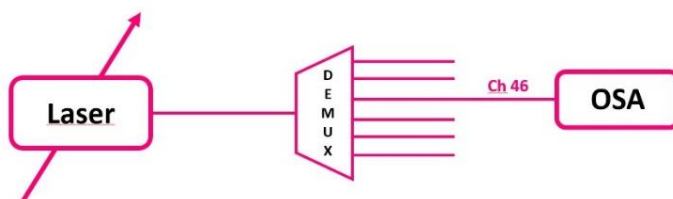
egyrészt $56 \text{ dBm} - 47 \text{ dBm} = 9 \text{ dB}$ a csillapítása a demultiplexernek az átengedett csatornán, másrészt pedig az adott (jelen esetben 1548.7 nm -es) csatornát kb 2 nm -es spektrumban engedi át. Tekintve, hogy 0.8 nm -es távolságban vannak a csatornák egymástól, ez már arra utal, hogy nem biztos, hogy elég jó a szűrő. Ezen kívül a magas csillapítás (9 dB) is rossz lehet egy kvantum csatornánál.

2.2 Áthallás vizsgálata más csatornákra

Azt tudjuk, hogy a kimenet, amire csatlakoztattuk a spektrumanalizátort 1548.7 nm -es. Azt szeretnénk megvizsgálni, hogy ha beküldünk egy bizonyos hullámhosszú fényt (pl. 1548.7 nm), akkor a különböző csatornákon mekkora teljesítmény jut át. Nyilván a legnagyobb ott fog megjelenni, aminek a hullámhossza a legközelebb van a beküldöthöz és elméletileg minél távolabbi csatornán nézzük, annál kevesebb jön át. Azért fontos ezt megvizsgálni, hogy tudjuk, ha pl. egy 1555 nm -es hullámhosszon van egy hagyományos csatorna, akkor lehetséges-e beküldeni, mondjuk 1548 nm -re egy kvantum csatornát, vagy az 1555 -ös annyira áthallatszik, hogy értelme sincs próbálkozni. Ezek az áthallások hagyományos esetben nem olyan lényegesek, mert minden csatornán viszonylag nagy teljesítménnyel adnak, viszont kvantum esetben egy erősebb áthallás már elnyomhatja a kvantum csatornát.

A 2.6 ábrán is látható, hogy a kísérletet úgy végeztük el, hogy a demultiplexer bemenetére változtatható hullámhosszú lézert csatlakoztattunk, amivel végigpásztáztuk a demultiplexer csatornáit. A túloldalon pedig kiválasztottuk a demultiplexer egyik kimenetét, amire csatlakoztattuk a spektrumanalizátort.

A kiválasztott, 1548.7 nm -esnek kimért kimeneti csatornához a szoftverben a 46-os számú csatorna lehetőség tartozik. (a változtatható lézert csak diszkrétan lehet változtatni – DWDM szabvány értékek között – és ezek a különböző lehetőségeket számozzák.)



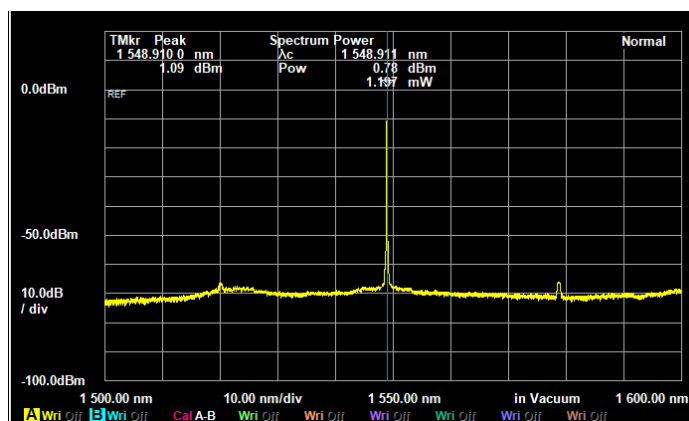
2.4 ábra: 2.2 mérés vázlatos elrendezése. Bal oldalt a változtatható hullámhosszú lézer, amivel végigpásztázzuk a csatornákat, jobb oldalt pedig a 46. csatornát mérjük a spektrumanalizátoron.

A mérés eredménye táblázatos formában a következő lett.

Lézer csatornája	OSA-n mért teljesítmény	Csúcs hullámhossza
1	-43.7 dBm	1567.13 nm
10	-49.37 dBm	1563.45 nm
35	-44.7 dBm	1553.32 nm
42	-44.3 dBm	1550.51 nm
43	-46.51 dBm	1550.11 nm
44	-33.91 dBm	1549.71 nm
45	-13.3 dBm	1549.12 nm

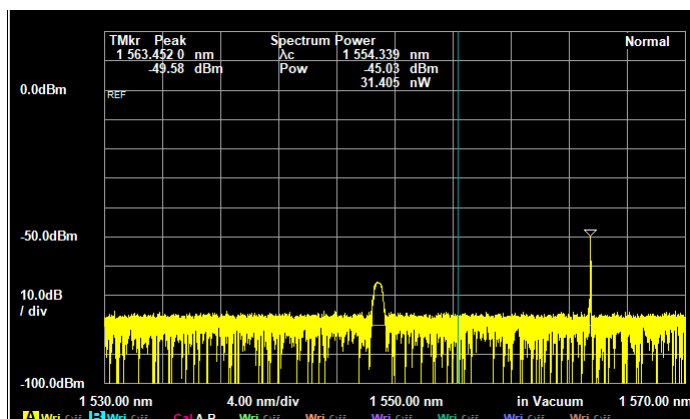
46	1.09 dBm	1548.91 nm
47	-4.45 dBm	1548.51 nm
48	-33.31 dBm	1548.11 nm
49	-37.52 dBm	1547.71 nm
50	-52.84 dBm	1546.91 nm
60	-43.22 dBm	1543.33 nm
70	-49.88 dBm	1539.3 nm
80	-50.46 dBm	1535.42 nm
90	-51.67 dBm	1531.5 nm
96	-48.45 dBm	1529.16 nm

A táblázatos eredményeket úgy kell értelmezni, hogy a lézer kiadja az első oszlopban látható csatorna számú hullámhosszt a demultiplexernek. Ebből a jelből valamennyi átjut a DWDM berendezésen az 1548.7 nm-es (46-os számú) kimenetre. Ezt pedig az OSA-n mérjük. Értelemszerűen ott nem az 1548.7 nm-nél lesz a jel, hanem ott, amit a lézer kiadott. Nézzünk meg példaként két eshetőséget:



2.5 ábra: spektrumanalizátor képe a 46-os csatornáról (1548,7 nm), amikor a 46-os csatorna hullámhosszával adunk a lézeren.

2.5-ös ábrán látható, hogyha a 46-os számú, 1548.7 nm-es hullámhosszon ad a lézer és a multiplexer 46-os, 1548,7 nm-es csatornáját nézzük a spektrumanalizátoron, akkor 1548.7 nm-en van a csúcs és elég magas, 1.09 dBm a teljesítménye.

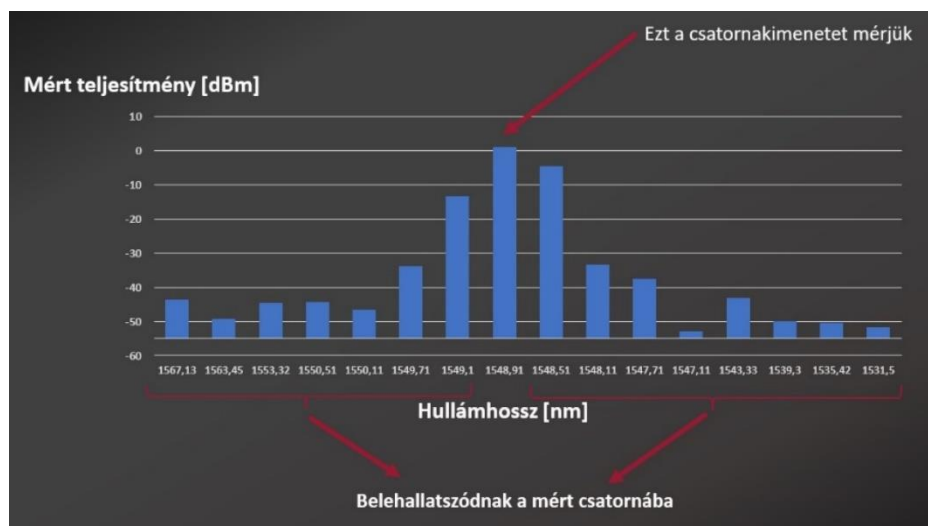


2.6 ábra: a spektrumanalizátor képe a 46-os csatornáról (1548,7 nm), amikor a 10-es csatorna hullámhosszával (1563.45 nm) adunk a lézeren. A jobb oldali csúcs a 10-es csatorna elnyomott maradványa, a középen lévő csúcs csak a lézer zaja

2.6-os ábrán látható, amikor a lézeren a 10-es csatornát választjuk. Ez 1563.45 nm-es fényt ad. Hiába az 1548.7 nm-es (46-os csatornájú) demultiplexer kimenetet nézzük, az 1563.45 nm-re kiadott jel így is -49.5 dBm-mel megjelenik. Ez hagyományos kommunikáció esetén nem lenne probléma, mivel egy >0 dBm körüli csatorna bőven elnyomná ezt, de egy sokkal kisebb teljesítményű QKD-csatornát már lehet, hogy zavarna.

2.3 Eredmények összességének értékelése

Azt kaptuk eredményként, hogyha a megfelelő csatornán nézzük a kimenetet, akkor 1 dBm körüli jelszintet kapunk, ha a szomszédos, vagy közelebbi csatornákon nézzük, akkor -30...-40 dBm körüli jelszintet mérhetünk, ha pedig a távolabbi csatornákon, akkor az derül ki, hogy oda -40...-50 dBm körüli jel szűrődne át. Vagyis a demultiplexer szűrése nem tökéletes. Emiatt érdemes egy jobb minőségű, modernebb DWDM berendezéssel is kísérletet végezni



2.7 ábra: 2.2 mérés eredményei grafikonon.

Nézzük az eredményt DVQKD (1 fotonos megoldás) szemszögből. Egyrészt a 2.5-ös és 2.6-os ábrából látszik, hogy ott, ahol nincs semmi áthallatszódás, ott is -70 dBm körüli a zajteljesítmény. Áthallatszódás esetén az elnyomott de áthallható csatornák értelemszerűen nem a kvantumos csatorna helyén vannak. Viszont DVQKD-nál a vevő egy egyfoton detektor, így a -70 dBm-es átlagos zajszint és az áthallatszott csatornák elnyomott verziói is zajfotonokat jelentenek a detektornak. Ez akkora, hogy megállapításunk szerint ilyen környezetbe lehetetlen lenne integrálni egy egyfotonos DVQKD-csatornát, a távolabbi csatornák áthallásán egy szűrő segíthet, de a kvantumos csatornán is jelen levő zajszinten nem.

Nézzük az eredményt CVQKD szemszögből. CVQKD esetén nem egyfoton detektor az érzékelő, így azok a fotonok, amik nem a kvantumcsatorna hullámhosszán vannak, nem fognak zajnak számítani.

A 2022 tavaszán a Telekom, BME és a Wigner Kutatóközpont közös QKD tesztjén a saját készítésű CVQKD eszköz esetén 1550 nm-es csatornát használtak 1 μ s-onként küldött 1 nW teljesítményű jellel [20]. Egyik fontos adat, hogy mivel 1 foton energiája 0.8 eV, így ebből kiszámolható, hogy ebben az eszközben egy impulzusban átlagosan 7793 foton van, ami nagyságrendekkel kisebb, mint a hagyományos kommunikáció esetén használt több százezer foton, így kvantumcsatornának tekinthető az átvitel már. A másik fontos megjegyzés, hogy 1 nW = -60 dBm. Mivel a 2.1.2 mérésnél megállapítottuk, hogy a demultiplexer csillapítása 9 dB, ezért ez a -60 dBm-es CVQKD-csatornát már a -70 dBm-es zajszintbe nyomná bele.

Tehát az a végső eredmény, hogy az előzetes mérés alapján a régebbi típusú egyetemi DWDM rendszerbe nem lehet se DVQKD, se CVQKD-csatornát integrálni. Viszont nincs annyira messze a megvalósíthatóságtól, ezért érdemes lenne megvizsgálni egy CWDM rendszert, valamint egy modernebb DWDM rendszert.

3. Egyetemi CWDM mérés

Miután megnéztük az egyetemi laborban található DWDM berendezést, úgy gondoltam, hogy CWDM-mel is érdemes kipróbálni, hogy a különböző csatornák mekkora zajt generálnak egy kvantumosnak képzelt üres csatorna helyén.

A CWDM technológiát részleteztem már, de az egyik legfontosabb jellemzője, hogy jóval nagyobbak a csatorna távok (20 nm a 0.8 nm helyett), így valószínűleg kevesebb zavarás jutna a kvantum csatornára ezért az integrálás céljából jobb megoldás lenne. A másik fontos jellemzője, hogy a maghálózatokon a legtöbb CWDM megoldást már DWDM váltotta ki, hiszen ott jóval több csatornát lehet használni (8 helyett akár 96-ot), így jelenleg vagy régebbi hálózatokon fordul elő, vagy pedig ahol többszintű WDM rendszer van ott lehet, hogy a fő hálózat DWDM és az azalatti alsósíkú „metro” hálózatok CWDM technológiát használnak. Emiatt sajnos jövőállás szempontjából nem ez a legjobb megoldás.

3.1 Mérési elrendezés:

3.1.1 Használt eszközök:

Jelforrásként Link Pro Fiber Link 360 media convertereket használtunk SFP-kel. A media converterbe lehet beletenni az SFP-ket, amik a fizika fényforrások. Az SFP egy kis, moduláris eszköz és minden SFP más-más (előre meghatározott) fix hullámhosszon ad jelet. A media converterek azok az eszközök, amik az SFP fényforrásokat irányítják, modulálják, elektromosan táplálják és hőstabilitást biztosítanak.

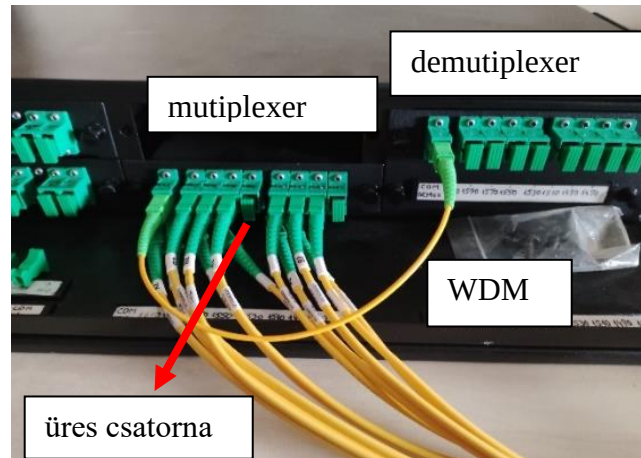
A mi tesztünkben kiválasztottuk az 1550 nm-es csatornát üresnek, vagyis kvantumosnak képzeltnék és a két oldalára 3-3 klasszikus csatornát tettünk, mindegyiket külön SFP-vel, SFP-nként külön media converterrel.



3.1 ábra: összes használt SFP és media converter. Az SFP-k a különálló alumínium borítású eszközök, a media converterek pedig a képen felettük látható fekete eszközök.

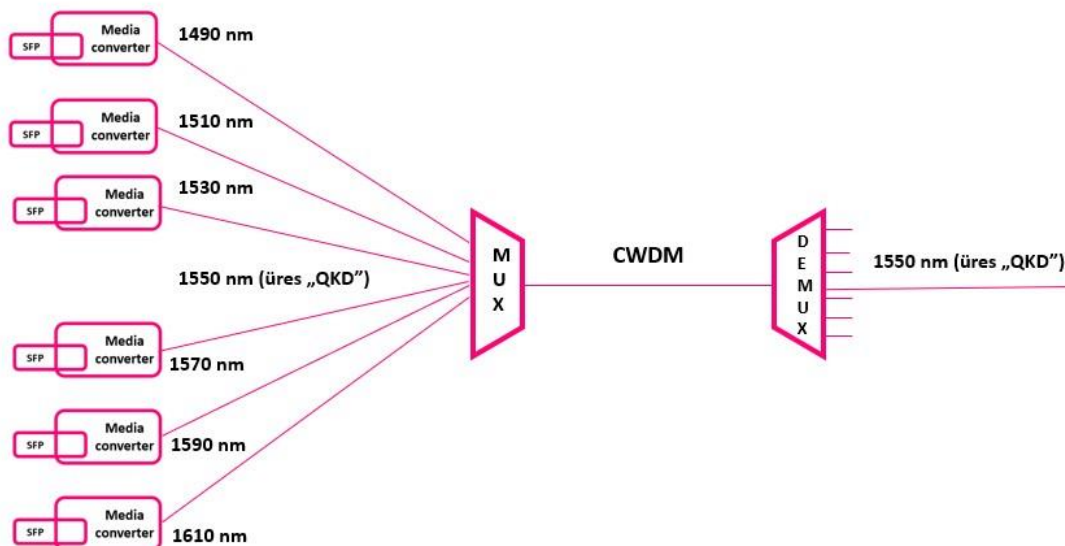
A 4.1 ábrán látható, hogy az adó oldali eszközök a következő képpen néznek ki. Balról jobbra haladva 1610 nm, 1590 nm, 1570 nm, majd az üres „kvantum csatorna után” látható az 1530 nm, 1510 nm és 1490 nm-t biztosító adó.

Ezek vannak bekötve a CWDM multiplexerbe, ami szintén egy régebbi modell. A CWDM eszközön külön található multiplexer és demultiplexer, ezek a közös porton össze vannak kötve, ahol a 6 csatorna multiplexálva, közösen halad. A demultiplexeren pedig újra szétválasztásra kerülnek. Itt mérjük különböző körülmények között az 1550 nm-es csatornát, hogy mekkora zaj található rajta.



3.2 ábra: DWDM eszköz – multiplexer és demultiplexer

3.1.2 Elrendezés:



3.3 ábra: mérési elrendezés vázlata a 3. fejezet méréseihez. Bal oldalt látható az 1550 nm-es, „kvantumosan” kiválasztott, így üresen hagyott csatorna, valamint a 3-3 klasszikus csatorna. A bal oldalon lévő multiplexer összeadja a csatornákat. Jobb oldalt látható a demultiplexer, aminek 1550 nm-es kimenetén mérünk a legtöbb mérésnél.

3.2 Csatornák teljesítményének mérése

Azért, hogy lássuk, hogy a klasszikus csatornáknak mekkora teljesítményük van és hogy lássuk a teljes rendszer csillapítását, csináltunk egy egyszerű teljesítmény mérést.

Sajnos minden converterből más-más teljesítményű jel jön ki, így nagyon nehéz lenne általánosítani és modellt alkotni a mérésből kiindulóan arra, hogy a klasszikus csatornák a teljesítményük alapján mekkora zajt okoznak egy üres csatornán.

Azért, hogy láthassuk a rendszer csillapítását és fogalmunk legyen a demultiplexer (demux) kimenetén a klasszikus csatornák teljesítményéről, azokat is megmértük. Ezek alapján pedig kiszámolható a csillapítás is.

Hullámhossz (nm)	Adás teljesítménye (dBm)	Demux után mért teljesítmény (dBm)	Csillapítás (dB)
1490 nm	-2.41 dBm	-6.44 dBm	4,03 dB
1510 nm	-3.35 dBm	-6.14 dBm	2,79 dB
1530 nm	3.52 dBm	0.4 dBm	3,12 dB
1550 nm	0.33 dBm	-3.2 dBm	3,53 dB
1590 nm	3.2 dBm	-0.8 dBm	4 dB
1610 nm	-2.6 dBm	-6.14 dBm	3.54 dB

A csillapítások alapján azt láthatjuk, hogy sajnos ez sem egységes, viszont **átlagosan 3.5 dB**. Így, ha az üres 1550 nm-es csatorna helyére teszünk QKD-t, akkor arra is kb 3.5 dB csillapítás vonatkozna. Ráadásul itt a mux és demux közti összeköttetés is nagyon rövid, ez látható a feljebbi képen, így a szálon történő csillapítások is jóval kevésbé játszanak szerepet, mint egy valós hálózatonál.

3.2.1 Üres, 1550 nm-es csatorna teljesítménye:

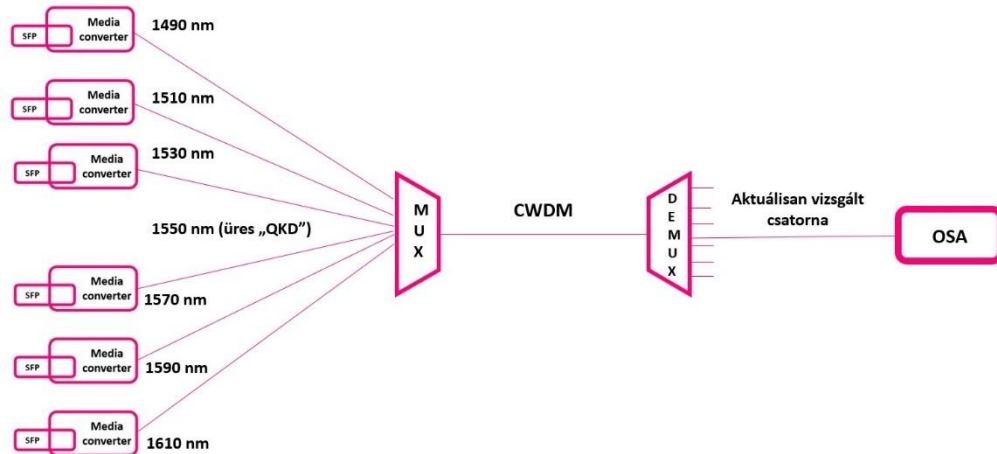
Talán a legfontosabb információ, hogy mekkora lett a kvantumcsatorna képzeletbeli helyén a zaj teljesítménye. – **67.5 dBm** optikai teljesítményt mértünk, ami ugyan nagyságrendekkel kisebb, mint a klasszikus csatornák helyén lévők, viszont a kvantumcsatorna zavartalanságához (főleg DVQKD-hoz) már lehet, hogy sok.

3.3 Mérések a spektrumanalizátorral:

A mért teljesítmények ugyan sokat elárulnak a rendszer zajairól és arról, hogy érdemes lehet-e kvantum csatorna integrálásával foglalkozni, viszont azt, hogy milyen hullámhosszokon mekkora teljesítményeket láthatunk, valamint, hogy ezek milyen spektrumon vannak jelen, csak optikai spektrumanalizátorral tudhatunk meg többet.

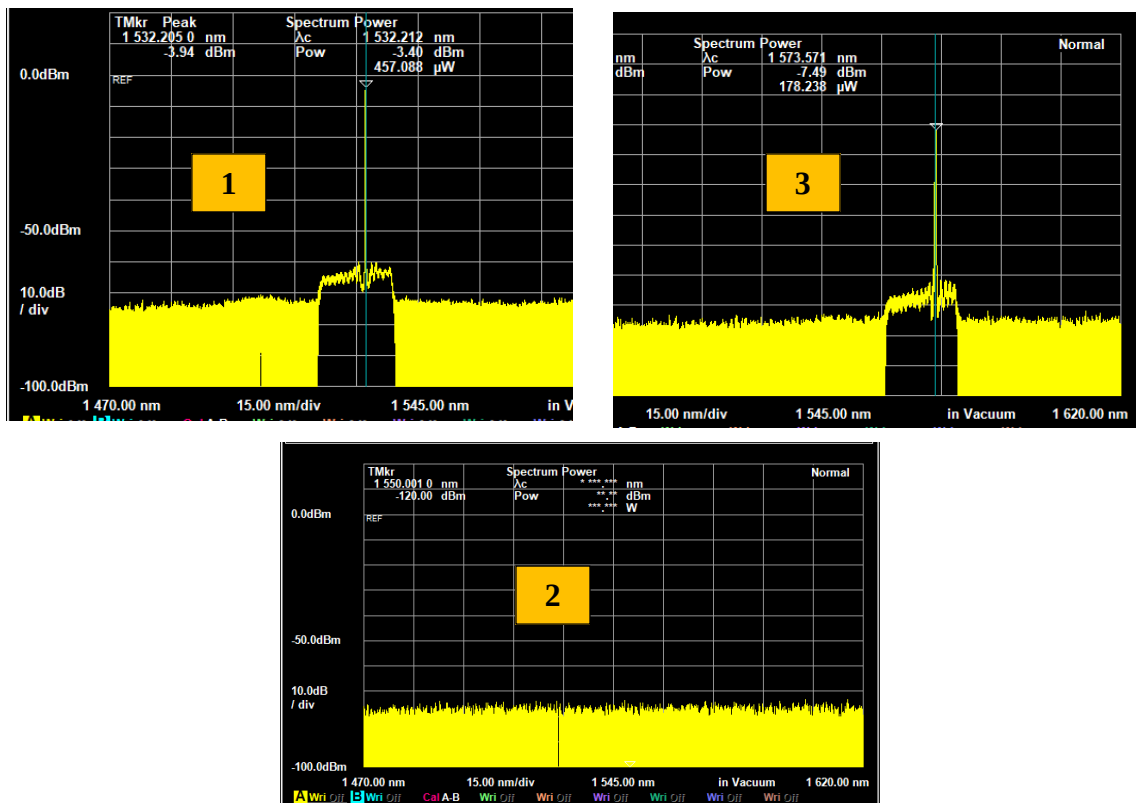
3.3.1 Mérések a demultiplexer kimenetéről

Az első mérés körét úgy állítottuk fel, hogy be van kötve a multiplexerre a 3-3 szomszédos csatorna és az előző pontban tárgyalt teljesítményekkel adnak. Az 1550 nm-es csatorna továbbra is üresen van hagyva a QKD-nak. A demultiplexer „szétszedi” a jeleket és az ő oldalán csak az aktuálisan vizsgált csatorna van bekötve a spektrumanalizátorba. Így, ha pl. az 1550 nm-es kimenetet nézzük, akkor semminek, ha pl. az 1530 nm-eset nézzük, akkor pedig csak annak a csatornának szabadna látszódnia, hiszen a demultiplexer szűrői minden mást leszűrnek.



3.4 ábra: 4.3.1 mérések elrendezése. Ugyanaz, mint a 3.3 ábra esetén, csak a kiválasztott csatornát csatlakoztattuk a spektrumanalizátorhoz

Elsőként megnéztük a demultiplexer 1530 nm-es kimenetét (1), ezután az 1550 nm-eset (2) majd az 1570 nm-eset (3).



3.5 ábrák: Mérési eredmények a demultiplexer után. Klasszikus csatorna van téve az 1530 nm-es (1-es képen mérjük) és 1570 nm-es (3-as képen mérjük) kimenetre. 2-es képen mért 1550 nm-es kimeneten van az üres „kvantumos” csatorna

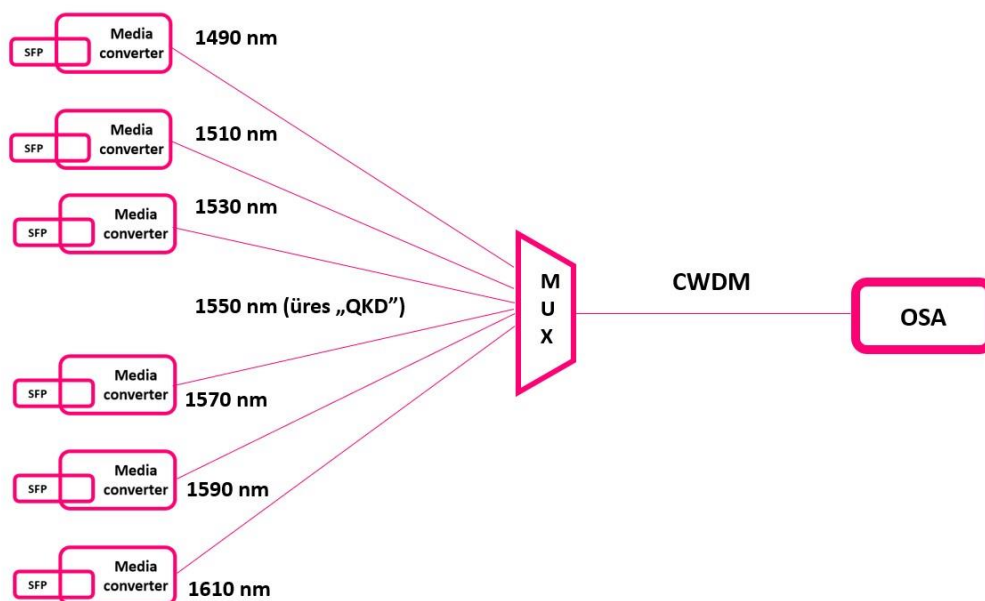
3.5 ábra 1. képen látható, hogy 1530 nm-es kimeneten a mért maximális teljesítmény (a küldött csatorna teljesítménye) -3.94 dBm, 2. képen látható, hogy 1550 nm-en csak zaj van, aminek átlagos teljesítménye -70 dBm körüli, 3. képen látható, hogy 1570 nm-en pedig -11.8 dBm lett a csatorna teljesítménye. Elmondható, hogy a CWDM szűrői a különböző kimeneteken látványosan kiszűrrik azokat a csatornákat, amik nem az adott kimenetre valók. (vagyis pl. az 1570nm-es kimeneten nem látható az 1530 nm-es csatorna.) Az is elmondható, hogy az átlagos zajszint -75 dBm körül van ott, ahol nincs csatorna, valamint 1. és 3. ábra alapján egy működő csatorna átlagos spektruma kb 20-30 nm.

Ha azt nézzük, hogy az egyetemi CVQKD rendszer teljesítmény szintje -60 dBm körül van, akkor - ha a demultiplexer utáni zajokat vesszük csak figyelembe – a CVQKD jel bőven elkülöníthető a -75 dBm körüli zajszintből. Természetesen a demultiplexer csillapítását is figyelembe kell venni. Mivel az csak 3.5 dBm, még így is marad -63.5 dBm-es QKD jel teljesítmény, ami szintén elkülöníthető a zajszinttől. Így azt mondhatjuk, hogy ebbe a rendszerbe integrálható lenne egy CVQKD-csatorna.

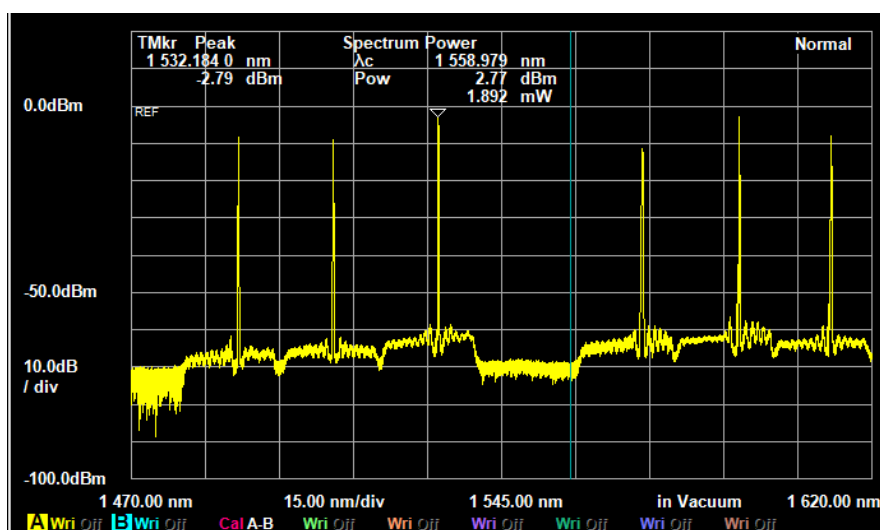
Viszont a multiplexált, közös szakaszon ennél nagyobb lehet az „alsó” zajszint. mivel ott a különböző klasszikus csatornák sincsenek leszűrve. Az egyetlen kérdés az, hogy jelent-e problémát a kvantumos csatornának az, hogyha a közös szakaszon a saját csatornáján is nagyobb a zajszint.

3.3.2 Mérés a multiplexált, közös szakasról

Arra voltam kíváncsi, hogy a közös szakaszon mekkora lehet a zajszint összességében és a kvantumos csatorna helyén. Ezért itt kihagyjuk a mérésekből a demultiplexert és a közös szakaszra kötjük a spektrumanalizátort.



Az első mérés a teljes CWDM spektrumot mutatja:



3.7 ábra: Közös szakasz képe a spektrumanalizátoron

Klasszikus csatornák:

Az eredmény egyik része az, hogy a szakasz végén (pár méteres optikai szállal dolgozunk) a klasszikus csatornák a 3.2 táblázatánál mért jelteljesítményükből vesztek, viszont nagyságrendileg hasonlóak. Az ábrán látható teljesítmények -3 és -10 dBm körül vannak, a 3.2 mérés alapján a media converterekből kijövő teljesítmények pedig 0 és -3 dBm közöttiek. Ez alapján elég nagy csillapítást szenvednek a csatornák, akár 5-6 dB-nyit is. Ez az előző mérés után elég meglepő eredmény, valószínűleg a műszerek eltéréséből adódik, valamint lehetséges, hogy a demultiplexernek előző gondolataimmal ellentétben nincs akkora szerepe a csillapításban (bár ez furcsa lenne).

Üres „kvantumos” csatorna:

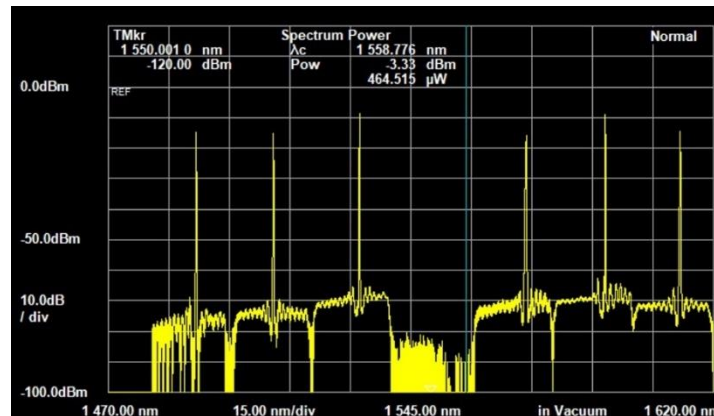
Ha nézzük a klasszikus csatornák körüli átlagos zajszintet, akkor láthatjuk, hogy -60 dBm körül van. Viszont, ha ránézünk az 1550nm-es üres csatorna környékére, akkor ott azt látjuk, hogy kb 20 nm-es spektrumban az átlagos -60 dBm-es **zajszint -70 dBm-esre** csökken. Ez nekünk nagyon jó, hiszen azt jelenti, hogy a közös szakaszon sincsen magasabb zaj, mint egy átlagos CVQKD rendszer jelteljesítménye, így biztos, hogy nem zavarják annyira a zajok, hogy ne lehessen felismerni a QKD jelét. Sőt, itt is beláthattuk, hogy a demultiplexer csillapítása 3.5 dB körül van és ez a zajokat is csillapította.

Ugyanezt a mérést átlagolással is elvégeztük és ott még pontosabban látható, hogy az üres sávban 1550 körül egy kb 20 nm-es spektrumban -70 dBm körül van a zaj teljesítményszintje.

3.3.3 Mérés a közös szakaszcól 30 km szál után:

A következő lépésben, hogy jobban szimuláljuk a valóságot, 30 km-nyi (feltekert) optikai szálát teszünk a CWDM multiplexer kimenetére a spektrumanalizátor előtt. A kereskedelmi forgalomban is kapható QKD eszközök általában (attól függően, hogy CVQKD vagy DVQKD technológiát használnak) 50-70 km hosszan tudnak működni, így a 30 km-es szakasz bőven a realitásokat tükrözi.

A mérés eredményét 3.8 ábrán lehet megtekinteni:



3.8 ábra: közös szakasz képe a spektrumanalizátoron. Átlagolást használtunk az ábrázoláshoz

Az eredményből elmondható, hogy kisebb a zaj, mint a 3.3.2, 30 km-es extra szál nélküli mérésnél.

A nagyobb távolság esetén mért kisebb zaj egy érdekes jelenség, hiszen szembe megy a következő 4-es fejezetben tárgyalt Matlab modell eredményével. A magyarázata lehet esetleg a műszer pontatlansága ilyen kis teljesítményeken, vagy pedig az, hogy nem a szálon keletkező zajok (pl. Raman szórás) volt a legnagyobb hozzájáruló, hanem pl. a lézer zaja, amit a Matlab modellben az eszközök közti nagy eltérés miatt nem vettem bele. Valószínűleg a szál hosszúsága a domináns zajt jobban csillapítja, mint amennyire a Raman szórást (az volt a leginkább távolság függvényében növekvő zaj) növeli.

3.4 Értékelés

Az üres csatornán a 30 km-es szál nélkül -70 dBm körül volt a zaj teljesítménye, 30 km után pedig az átlagolós mérés esetén akár -80 dBm-et is elérte. Ha azt nézzük, hogy az egyetemi építésű és a kereskedelmi forgalomban kapható CVQKD eszközök is -60...-65 dBm körüli jelszinten működnek, ezért azt mondhatjuk, hogy CWDM esetén tudunk CVQKD típusú kvantumos csatornát integrálni a hálózatba. Ezt leginkább annak köszönhetjük, hogy a csatornák elég messze vannak ahhoz, hogy a szűrők megfelelően el tudják nyomni a klasszikus csatornák zaját.

4. Felmerülő zajok vizsgálata MATLAB számításokkal

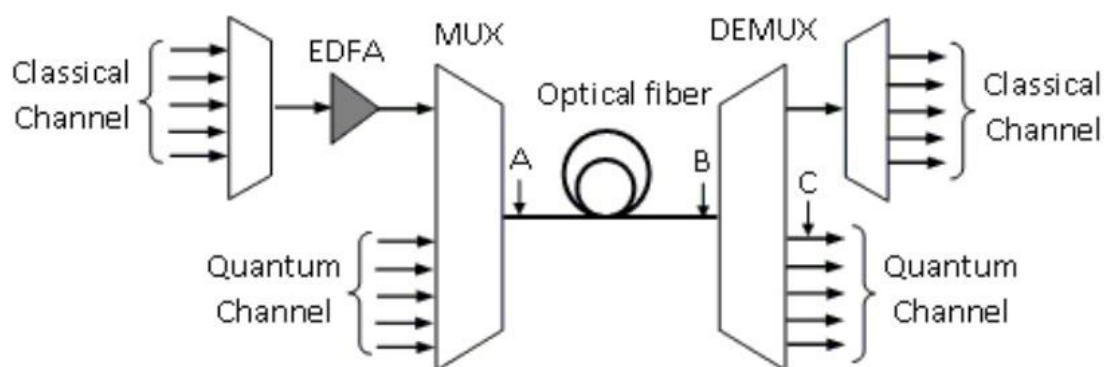
Tehát megtudtuk, hogy a régebbi típusú, egyetemi DWDM eszközön valószínűleg nem működne, bár nem állunk messze tőle, viszont az egyetemi CWDM rendszeren már működne az integrálás. Mindkét esetben leginkább a zajoktól függ a sikeresség, ezért készítettem egy Matlab szimulációt a legalapvetőbb zajok számításáról.

A kvantumcsatornát többféle zaj is terheli. Ezek adódhatnak a WDM rendszer sajátosságaiból, vagy pedig összességében az optikai távközlés tulajdonságaiból. Kiszámításuk, modellezésük és minimalizálásuk a fő feladatok között van ahhoz, hogy megismerhessük a vázolt ötlet használhatóságát.

A jelenlegi optikai rendszerek általában tartalmaznak erbiummal adalékolt erősítőket (EDFA), ezekkel a teljes DWDM spektrumot (így az összes csatornát) erősíteni lehet, viszont pont emiatt széles sávon keltenek spontán emissziós zajt. A klasszikus csatornákból is származhat „áthallás”, ami szintén zajt okoz az adott csatorna hullámhosszán. Ezek voltak láthatóak a 2.2 kísérletben is. Ezeket esetleg különböző közbeiktatott szűrőkkel, vagy egyszerűen jobb minőségű multiplexerekkel csökkenteni lehet. A legnagyobb zajt a Raman szórás okozhatja. Ez nemlineáris folyamatok során keletkezik és a hullámhossz tartomány nagy részére kiterjedhet. Ha az ebből származó zajfotonok hullámhossza egybeesik a kvantumcsatorna hullámhosszával, akkor egyáltalán nem lehet kiszűrni. A negyedik nagy zajforrás, az úgynevezett 4 hullám keverésből (four wave mixing) keletkezik. Ez kisebb távolságokon nagy zajt jelent, viszont hasonló témájú kutatás [21] arra jutott, hogy ez a Raman szórásnál kisebb veszélyt jelent és a megfelelő csatornakiosztással jól csökkenthető.

A zajok számításához a következő, hasonló témájú cikk kutatását vettem alapul [22]. Az itt használt hálózati modell megfelel az én elképzeléseimnek is. Ebben a modellben egy előre nem definiált típusú, klasszikus csatornákat is tartalmazó WDM hálózatba iktattak előre nem definiált számú kvantumcsatornát. A kutatás figyelembe vette a klasszikus csatornákat erősítő erősítő zaját, majd az optikai kábel szakaszon a klasszikus csatornákból való szivárgást és a Spontán Raman szórást

A használt modell ábrája itt található:



4.1 ábra: Matlab szimulációhoz használt modell rajza [22].
Bővebb magyarázat a következő oldal tetején.

Itt a klasszikus csatornák a multiplexálás után egy EDFA (erbium-doped fiber amplifier) erősítővel kerülnek erősítésre. Ezt hagyományos kommunikáció esetén mindig szokták alkalmazni, bár nem a multiplexer előtt van fizikailag (hanem a multiplexelt - közös szakaszon, hogy egyszerre erősítse az összes csatornát), de mivel a tőle származó zaj is bekerül a WDM jelbe, ezért a modellben most itt is elhelyezhető. Természetesen a kvantum csatornát nem kell erősíteni, mert akkor elvesztené kvantumos jellegét. Ha egy valós hálózatban a teljes WDM szakasz kerül erősítésre, akkor ott le kell választani a kvantumos csatornát az erősítő előtt, majd újra multiplexálni az erősítő után.

Ezután kerülnek multiplexálásra klasszikus csatornák a kvantum csatornákkal, bár a számításaimban csak 1 kvantum csatornát feltételeztem.

Ezután következik az optikai szál. Az összes zaj fotonszáma és a kialakuló kvantumos kulcsszétosztási ráta (secure key rate) is függ a szálhossztól. Mivel az általam használt modell alapján kb. 0 és 60 km között van olyan eredménye a kulcsrátának, amire azt mondhatjuk, hogy érdemes vizsgálni a kvantumos kommunikáció lehetőségét, ezért (minden zaj esetében) 0 és 60 km közötti szálhosszt használok.

A szál után következnek a demultiplexerek. Az első szétválasztja a kvantumos és hagyományos csatornákat, a másik pedig csatornákra bontja a hagyományos oldalt. A kvantumos részen itt következik „Bob”, aki megkapja az adó „Alice” jelét.

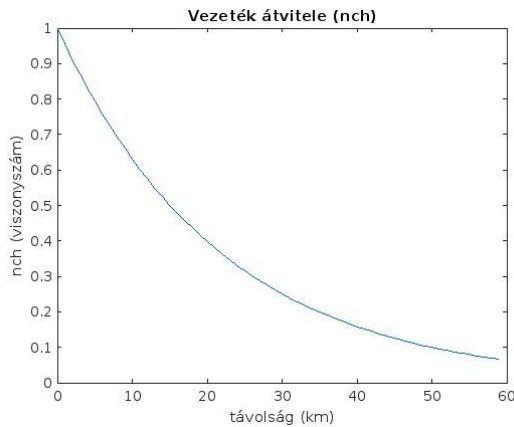
A következőkben a fontosabb zajokat külön-külön tárgyalom a Matlabban végzett számításokkal együtt.

4.1 Az erősítő zaja:

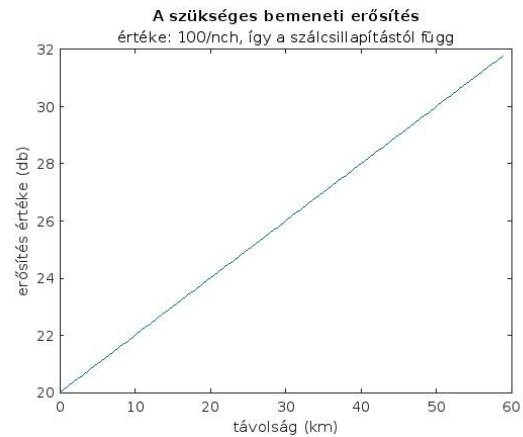
Az erősítéshez az optikai kommunikációban megszokott EDFA-t használunk. Tanulmányok is megállapították már [23], hogy sajnos nem létezhet zajmentes erősítő, valamint a legnagyobb zaj az erősítőből érkező spontán emisszió. Az erősítő zajtényezője ideálisan 3-4 dB környékén van [31].

Az erősítés többfajtaképpen is értelmezhető. Egyrészt megadhatunk egy konkrét értéket, amit az erősítő bármilyen szálhossz esetén erősít. (pl 100 dB). Ezesetben minél hosszabb a szál, annál gyengébb lesz a kimeneti jel, ha ugyanazt az erősítőt használjuk. Vagy, meg lehet adni úgy is, hogy tudjuk, hogy milyen jelszintet akarunk a túloldalon, ismerjük a szál csillapítását és az erősítést a hossz függvényében változtatjuk azért, hogy a szál végén minden hossz esetén ugyanakkora jelteljesítményt kapjunk.

Mivel mi a zajoknál leginkább arra vagyunk kíváncsiak, hogy azok hogyan függenek a hosszától, ezért az erősítésnek is függenie kell a hosszától (hiszen, ha hálózatot tervezünk akkor is hossz alapján választunk erősítést.) Ha az általános 0.2 dB/km-es szálcscillapítással számolunk, akkor az optikai szálunk a következő, 4.2 ábrán látható átvittel fog rendelkezni a hossz függvényében.



4.2 ábra: Optikai szál átvitele a távolság függvényében 0.2 dB/km csillapítás esetén



4.3 ábra: Szükséges erősítés a távolság függvényében (dB-ben)

A 4.2 ábrán látható szálcsillapítás miatt, ha a szál kimenetén konstans értéket szeretnénk kapni, akkor a távolság függvényében a 4.3 ábrán látható erősítéssel kell dolgozni.

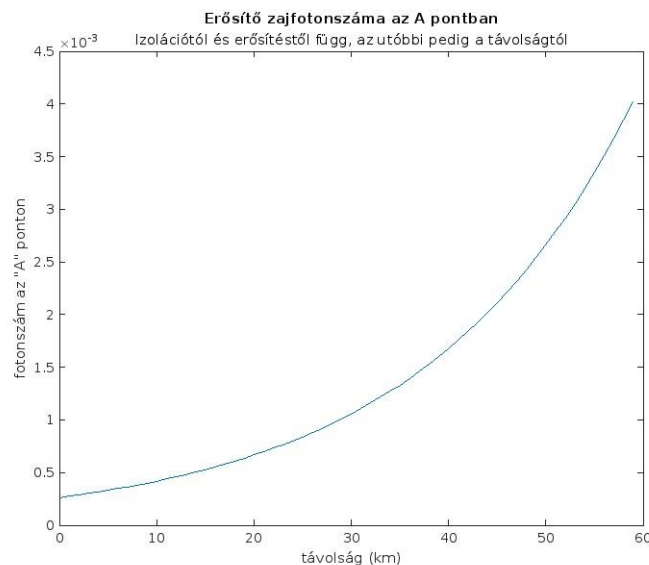
Minden erősítőnek van egy zajtényezője (Noise Figure - NF), ami az adott erősítő zaját jellemzi és általában 5 dB körüli értékű [32]. Ennek a segítségével számíthatjuk ki, hogy mekkora zajfotonszámot okoz. [26]

$$\eta_{SP} = \frac{G \cdot NF - 1}{2 \cdot (G - 1)} \quad (1)$$

$$N_{ASE} = 2 \cdot \eta_{SP} \cdot (G - 1) \quad (2)$$

Először (1) segítségével kiszámíthatjuk η_{SP} -t, ami a spontán emissziós faktor. Ennek az értéke az erősítés függvényében, valamint a zajtényező (NF) segítségével kerül kiszámításra. Ebből számítható (2) segítségével N_{ASE} (amplified spontaneous emission – erősített spontán emisszió) fotonszáma. A képletek alapján meghatározható, hogy a minta hálózat egyes pontjain mekkora ennek a zajnak a fotonszáma.

Az „A” pontban, a klasszikus és kvantum csatornákat összefogó multiplexer 4.4 ábrán látható:



4.4 ábra: Erősítő zajfotonszáma az „A” pontban

Ha azt vesszük, hogy a multiplexer izolációja $\xi_1 = -80$ dB (ami modernebb eszközök esetén már teljesülhet), akkor az A pontban jelentkező zajfotonszám: $N_{ASE_A} = \xi_1 \cdot N_{ASE}$, ahol ξ_1 már viszonyyszámként szerepel. A zajfotonszám azért nő a távolság függvényében, mivel az erősítés is nő.

A 4.5 és 4.6 ábrákon látható, hogy „B” (az optikai szál végi) és „C” (a demultiplexer utáni) pontoknál mekkora a zajfotonszám.

A „B” ponton lévő fotonszámot a (3) képlettel kaphatjuk meg.

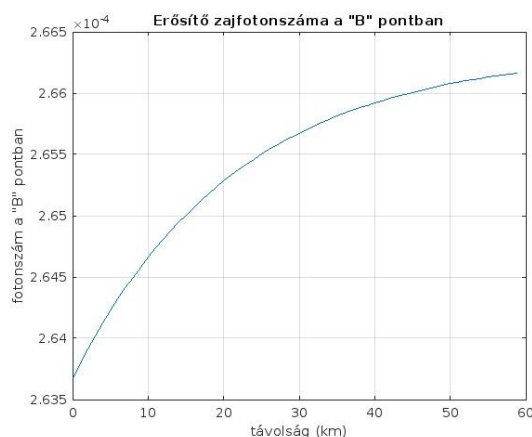
$$N_{ASE_B} = N_{ASE_A} \cdot \eta_{CH} \quad (3)$$

Vagyis a B pontnál lévő zaj számításához az A ponton lévő zajfotonszámot megszorozzuk a távolságfüggő szálátvitellel.

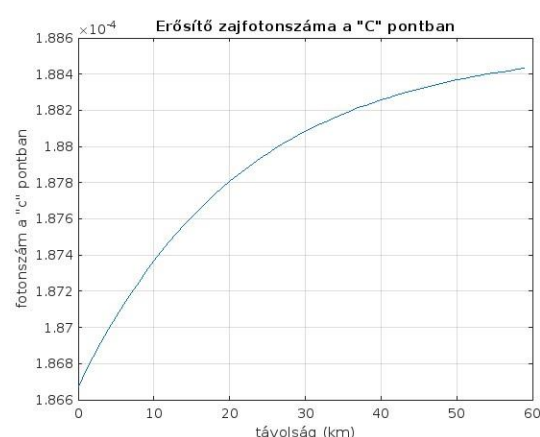
A C ponton lévő zajfotonszámot pedig (4) képlettel kaphatjuk meg, hasonló számítási móddal.

$$N_{ASE_C} = N_{ASE_B} \cdot \eta_{DMU} \quad (4)$$

A különbség annyi, hogy itt a B pontnál lévő fotonszámot megszorozzuk a demultiplexer viszonyyszámként értelmezett átvitelével. $\eta_{DMU} = -1.5$ dBm [22].



4.5 ábra: Erősítő zajfotonszáma a „B” pontban a távolság függvényében



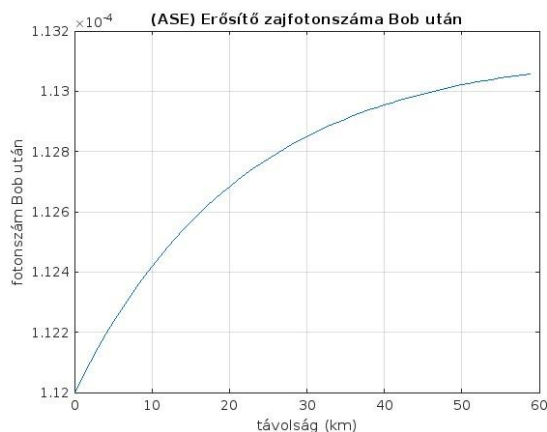
4.6 ábra: Erősítő zajfotonszáma a „C” pontban a távolság függvényében

A grafikonokból több következtetés is levonható. Mivel az A pontnál még nem ment át az optikai szálon, ezért képes konvex módon, szinte exponenciálisan növekedni a zaj mértéke. Viszont mivel itt már belejátszik a zajba a szál csillapítása (ami nagyobb távolság esetén nagyobb), ezért a távolság növelésével a zaj már nem fog olyan nagy mértékben nőni.

Az eredményeket úgy kell értelmezni, hogy például 4.3 ábra alapján 50 km-es hossz esetén kell 30 dB erősítés. Ez 4.4 ábra alapján az „A” pontban kb 10^{-3} darab fotonnyi zajt okoz nanoszekundumonként. Mivel átmegy az optikai szálon, ezért 4.5 alapján a B pontban a szál végén már csak $2.6 \cdot 10^{-4}$ darab foton lesz. 4.6 alapján pedig a

demultiplexer után, a „C” pontban pedig már csak $1.8 \cdot 10^{-4}$ darab zajfoton fog az erősítőtől származni.

Azt is megnézhetjük, hogy ebből mennyi jut el Bobhoz. A [22] alapján Bob átvitelét 0.6-os paraméterrel számoltam (vagyis a demultiplexertől a „C” pontban általa megkapott összes foton 60%-át detektálja). Így a távolság függvényében Bobhoz a 4.7 ábrán látható számú zajfoton jut el nanoszekundumonként az erősítőtől:



4.7 ábra: Erősítő zajfotonszáma Bob után a távolság függvényében

A $N_{ASE_A} = \xi_1 \cdot N_{ASE}$ képlet alapján látható, hogy az eredmény nagyban függ a multiplexer izolációjától. A [22] forrásban talált 80 dB-es érték először nagynak tűnt, viszont egy hallgató társammal közösen csináltunk egy kísérletet ennek vizsgálatára. Ebben 8 csatornás CWDM multi-és demultiplexereket vizsgáltunk és eredményként kijött a 80 dB körüli izoláció.

4.2 Áthallás a klasszikus csatornákból:

Sajnos a demultiplexerek nem tökéletesek. Alapvetően az lenne a feladatuk, hogy csak az adott csatorna hullámhosszához tartozó fotonokat engedjék ki az adott csatorna kimenetén. Viszont az izolációjuk nem végtelen, így átengednek más hullámhosszú fotonokat is. Sőt a csatornák elnyomott maradványai is látszódnak a kimenetén. Ez a 2. fejezetben bemutatott mérésekből is látszik (2.8 ábra).

Ahogy a klasszikus csatornában forgalom halad a szálon, a különböző optikai törvények és tulajdonságok (pl. Raman szórás, diszperziós hatások) miatt a klasszikus csatornák hullámhosszáról a környező hullámhosszokra is kerülnek át fotonok, amik aztán zajként értelmezhetőek. Ezeknek egy nagy részét a demultiplexer ki tudja szűrni, viszont a klasszikus csatornák maradványai nagy szerepet játszanak a demultiplexer által ki nem szűrt zajokban.

A számításokhoz figyelembe kell venni a klasszikus csatornák optikai szál végén mérhető teljesítményét. Ezt az erősítés módszere alapján kétfajta módon kezelhetjük.

Ha úgy vesszük, hogy az erősítés a távolságtól függ és a cél az, hogy a kimeneten minden távolság esetén ugyanakkora legyen a teljesítmény, akkor ez a kimeneti teljesítmény

például egy állandó 0 dBm-es érték a távolság függvényében. A valóságban is gyakori a 0 dBm közeli teljesítmény. [16]

Ha úgy vesszük, hogy az erősítés egy minden távolság esetén állandó érték, akkor a távolság függvényében folyamatosan csökkenni fog a kimeneti teljesítmény.

Ezután számíthatjuk ki a zajt. Az, hogy a klasszikus csatornákból mennyi áthallást enged át a demultiplexer, az izolációján múlik. Ha a kimeneti teljesítményt (legyen az a konstans vagy a csökkenő verzió) megszorozzuk az izolációval, akkor megkapjuk azt, hogy mekkora a szivárgás teljesítménye. Ha ezt leosztjuk a foton energiájával ($h \cdot f$), akkor megkaphatjuk, hogy ez hány fotont jelent. Mivel egy időablakban nézzük, ezért ábrázoláskor meg kell szorozni az 1 ns-os időablakkal. Mindez az (5) képletcsoporthoz található.

$$P_{LEAK_C} = \xi_2 \cdot P_{OUT} \quad (5.1)$$

Tehát a „C” pontra jutó zajteljesítmény az áthallásból a demultiplexer izolációjának (ξ_2) és a demultiplexerbe csatlakozó klasszikus csatorna teljesítmény (P_{OUT}) szorzata (1 klasszikus csatorna teljesítménye),

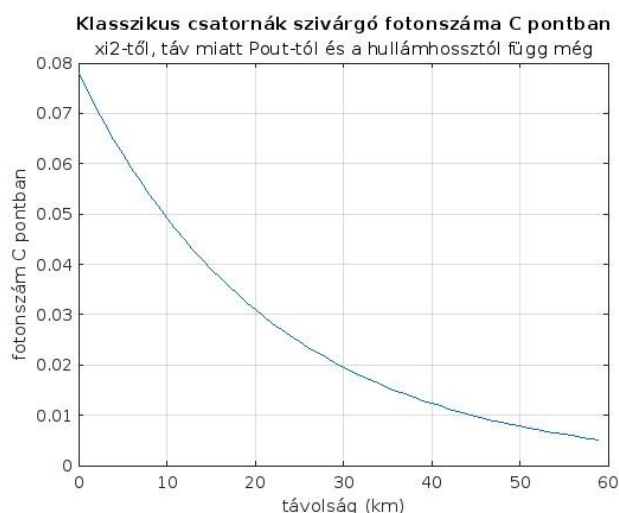
Ez alapján kiszámítható a zajfotonszám:

$$f = \frac{c}{\lambda_{KLASSZIKUS}} \quad (5.2)$$

$$N_{LEAK} = P_{LEAK_C} \cdot \frac{h}{f} \quad (5.3)$$

A képletekben $\lambda_{KLASSZIKUS}$ a klasszikus csatorna hullámhossza, c a fénysebesség.

Ha az erősítés elvével az első verziót követjük, tehát van egy adott erősítésű erősítőnk, minden szálhossz esetén azt használjuk, akkor a P_{OUT} (demultiplexerre jutó klasszikus csatorna teljesítmény) függeni fog a távolságtól úgy, hogy, minél nagyobb a távolság, annál kisebb lesz P_{OUT} . Ekkor az eredmény a távolság függvényében a következő grafikonon látható:



4.8 ábra: klasszikus csatorna szivárgása szálhosszal változó kimeneti teljesítmény esetén „C” pontnál a távolság függvényében (klasszikus csatornával)

Ebben az esetben 4.8 ábrán látható, hogy ha az erősítés állandó, így a kimeneti teljesítmény a távolság függvényében csökken, akkor a klasszikus csatornák áthallása 0 és 0.08 foton között van nanoszekundumonként. Mivel folyamatosan csökken a teljes kimenet teljesítménye, ezért a kimenő zaj is csökkenni fog.

A másik esetben előre ismert az optikai szál hossza és az a cél, hogy a szálvégre felerősítsék a jelet. Tehát a távolság növelésével nő az erősítés, viszont így a kimeneti teljesítmény konstans tud lenni a távolság függvényében. Emiatt a szivárgó fotonszám is konstans lesz.



4.9 ábra: klasszikus csatornák szivárgása konstans kimeneti teljesítmény esetén a távolság függvényében

Látható a 4.9 ábrán, hogy az eredmény ugyanabba a nagyságrendbe esik és végig hasonló értékű, mint az előző elképzelésnél, 4.8 ábránál.

Mivel az erősítő zajának számítását úgy végeztem, hogy az erősítés a távolság függvényében nő, ezért a modell szempontjából az a helyes értelmezés, ha itt a konstans zajjal (a 2. értelmezéssel) számolok a továbbiakban. Egyébként mivel mindkét módszer esetén szinte teljesen azonos eredmény jön ki, ezért nem igazán számít, hogy melyik modellezést választjuk. Ugyan nagyobb ez a zaj, mint az erősítőé, de még mindig viszonylag kicsinek mondható a következő zaj ismeretében.

4.3 Raman szórás:

4.3.1 Elméleti háttér:

A számítások során azt az eredményt kaptam, hogy az emiatt keletkező zajnak van a legnagyobb fotonszáma, így ez játssza a legnagyobb szerepet a kvantumcsatorna zavarásában.

A Raman hatást általában spektroszkópiában szokták használni, mert segítségével fel lehet ismerni különböző anyagokat. Viszont az optikai kommunikációban komoly zajforrást jelent. Ha egy monokromatikus fény (a lézerek fénye ugyan nem tökéletesen az, de annak tekinthető) elér valamilyen anyagot, akkor a fény egy része sértetlenül átmegy az anyagon, kis része pedig szétszóródik. A szóródás leginkább anyagbeli anomáliáknak köszönhető. Itt az anyag a fényt vezető üvegszál. Ha a szétszóródó

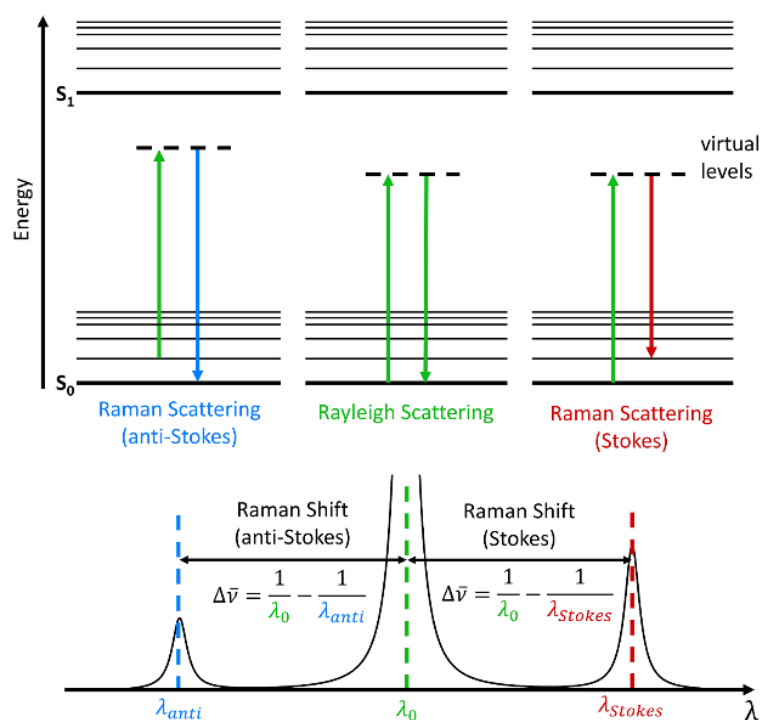
fotonnak ugyanaz marad a hullámhossza, mint a beesőnek, akkor ezt Rayleigh szórásnak hívjuk, ha nem marad ugyanaz, akkor beszélünk Raman szórásról. Ezesetben a következő események történnek. A bejövő foton $E = h \cdot f_{be}$ energiát adhat át az anyag egyik elektronjának, amitől az egy magasabb energiaszintre kerül. A magasabb energiaszintről, viszont minél hamarabb szeretne visszakerülni alacsonyabbra, ezért energiát fog leadni. Ezt foton kibocsátással tudja megtenni. A leadott energia legyen $E = h \cdot f_{ki}$.

Legtöbb esetben ugyanarra az energia szintre tér vissza az elektron, mint ami az alapállapota volt. Ha az eredeti fotonnal megegyező energiát adott le, akkor $h \cdot f_{be} = h \cdot f_{ki}$ amiből következik, hogy $f_{be} = f_{ki}$. Tehát az energiavesztés közben az eredeti fotonnal megegyező frekvenciájú foton tud létrejönni. Így keletkezik a Rayleigh szórás.

Viszont néha a virtuális energiaszintre felkerülő elektron nem ugyanakkora energiát ad le, mint amennyit felvett, így egy másik energiasávba esik vissza az energiavesztés során. Ekkor $h \cdot f_{be} \neq h \cdot f_{ki}$ tehát más frekvenciájú, így hullámhosszú foton ad le az elektron. Ez a Raman szórás. Ha a leadott fotonnak kisebb a frekvenciája (nagyobb a hullámhossza), mint a bejövő fotonnak, akkor ezt Stokes Raman szórásnak hívjuk, ha pedig a leadott fotonnak nagyobb a frekvenciája (kisebb a hullámhossza), mint a bejövő fotonnak, akkor anti Stokes Raman szórásnak hívjuk.

A megváltozott hullámhosszú fotonok is tovább szóródhatnak, ezért minél távolabb vagyunk a forrástól, annál több olyan foton lesz, ami elkerül a saját hullámhosszáról. Mivel az elektronok nem kerülnek jóval távolabbi energiaszintekre, így a leadott fotonok esetleges hullámhossz változása is kicsi. Vagyis a Raman szórás szennyezését csökkenthetjük úgy, hogy egyszerűen a hagyományos sávoktól távolabbi hullámhosszra tesszük a kvantum csatornát.

A szemléltetés kedvéért 4.10 ábra bemutatja a folyamatot.



4.10 ábra: Raman szórás szemléltető ábra (forrás [25])

3.3.2 A szórás számítása:

A Matlabos számítások elkészítéséhez [22], [26], [27] források számítási módszereit használtam.

A számítást úgy kezdem, hogy a spontán Raman szórás teljesítményét számítom ki a (6) képlettel:

$$P_{SRS} = P_{IN} \cdot \beta \cdot r \cdot \eta_{CH} \cdot d\lambda = P_{OUT} \cdot \beta \cdot r \cdot d\lambda \quad (6)$$

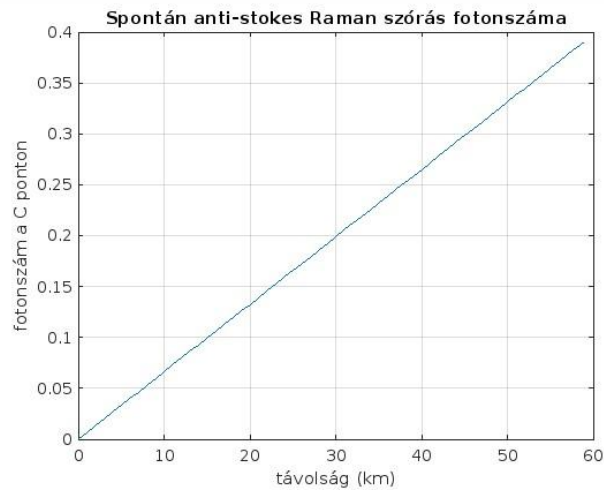
- Itt P_{OUT} a klasszikus csatornák lézérének kimeneti teljesítménye 0 dBm-nek (vagyis 1 mW-nak) választva. Tehát ez egy konstans érték, amit a kezdetekben választhatunk meg, nem függ a távolságtól és egyéb tényezőktől.
- r a távolság km-ben. Értelemszerűen, minél távolabb vagyunk, annál hosszabban lesz lehetőségük a fotonoknak szóródni, így annál nagyobb lesz a Raman szórás teljesítménye.
- A β a spontán Raman szórás együtthatója. Értéke $4 \cdot 10^{-9} \text{ (km nm)}^{-1}$. Az együttható távolságfüggő, viszont az erre vonatkozó [22] cikk kísérlete alapján 40 km-en, legrosszabb körülmények között lett $4 \cdot 10^{-9}$ az értéke. Így egyszerűsítésként ezt használom. Mivel nagyon kis szorzóról van szó, ezért változtatása vagy távolságfüggővé tétele nem befolyásolná jelentősen az eredményt.
- A $d\lambda$ a $d\lambda = \frac{c}{df}$ képletből származik, ahol df a klasszikus csatornák/csatorna sávszélessége frekvenciában. Így $d\lambda$ lesz a sávszélesség hullámhosszban. A számításbeli értéke [22] alapján $df=75 \text{ GHz}$. Ez gyakran előfordul WDM rendszerek esetén. A többi gyakori csatorna szélesség 50 GHz és 100 GHz, amikkel még érdemes lehet számolni. Viszont az újabban szintén alkalmazott flex grid megoldások (amikor nincs előre definiált csatorna sávszélesség, hanem adaptívan változik a forgalom alapján), a 75 GHz egy jó átlagértéknek is tekinthető.

Ezután a teljesítményből fotonszámot kell készíteni, amihez [27] megoldását használom.

$$N_{SRS} = \frac{P_{SRS} \cdot \lambda}{h \cdot c} \cdot \eta \cdot dt \quad (7)$$

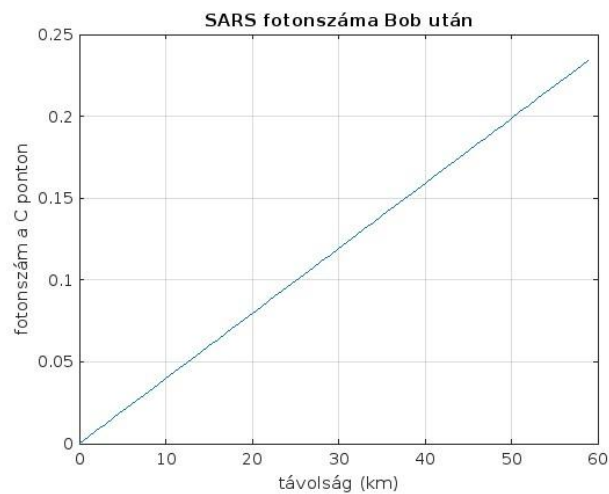
- λ a klasszikus csatorna hullámhossza, vagy több csatorna esetén közép hullámhossza. A DWDM megoldások során leggyakrabban használt 1550 nm-es hullámhosszt választottam ide.
- h a Planck állandó, illetve „ c ” a fénysebesség, amik a teljesítményből való fotonszám számításához kellenek.
- η egy konstans arra vonatkozóan, hogy a zaj mekkora részét érzékeljük. A [27] forrás számítása egy egyszerű (WDM nélküli) DVQKD-ban gondolkodott és ezért ide csak a detektor hatékonyságát helyezte, mivel az egyfoton detektor nem minden fotont fog érzékelni a Raman szórásból sem. Viszont a [22] forrás és én is először ennek a helyére a demultiplexer hatékonyságát helyezem (-1.5 dB veszteség). Azért gondolom jobb megoldásnak, mivel a létrejött szórt fotonok a szál végén először a kvantum csatorná(kat) és klasszikus csatornákat szétválasztó demultiplexerrel találkoznak.
- dt (1 ns), azért szükséges, hogy egy és ugyanazon időablakban láthassuk a Raman szórás fotonszámát, mint a többi zaj esetén.

Az eredmény a távolság függvényében 4.11 ábrán látható.



4.11 ábra: Raman szórás fotonszáma a távolság függvényében a „C” pontnál

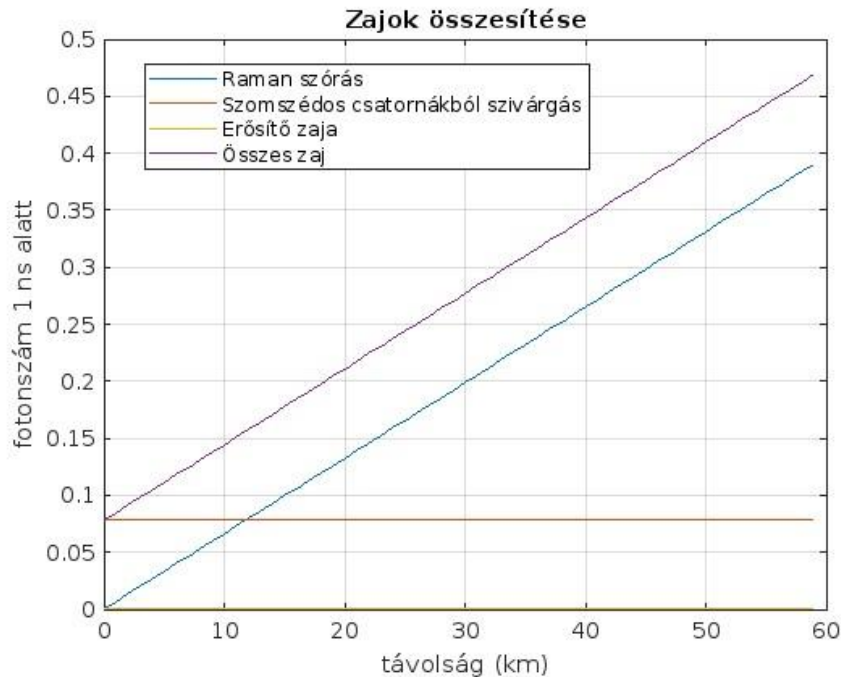
Ezután kiszámíthatjuk, hogy ebből mennyi jut el Bob-hoz. Ehhez annyit kell még tenni, hogy a fotonszámot megszorozzuk Bob „átvitelével”, amit rosszabb esethez igazítva 0.6-nak veszünk. Az eredmény 4.11 ábrán látható.



4.11 ábra: Raman szórás fotonszáma, Bob után, a távolság függvényében

4.4 Zajok összesítése:

Ha egy időablakban nézzük a kiszámított zajokat, akkor 4.12 grafikont kapjuk:



4.12 ábra: Összes kalkulált zaj fotonszáma, zajonként lebontva, a távolság függvényében

Első ránézésre nem tűnik soknak a 0.1-0.5 közötti fotonszám 1 ns alatt, viszont azt érdemes figyelembe venni, hogy ez 1 másodperc alatt már 100 millió – 500 millió fotont jelent.

4.5 Kulcsmegosztási ráta számítása

A ráta azt jelenti, hogy bizonyos idő alatt hány kulcsot lehet megosztani Alice és Bob között. 2 különböző modellt is készítettem. Az elsőben egyfoton detektorral DVQKD-t alkalmazunk, a másodikban homodin detektorral CVQKD-t használunk. Természetesen a két modell eredményei eléggé el fognak térni. Az egyfoton detektor minden zajfotont érzékel, ha a detektor érzékelési tartományának megfelelő spektrumban van. A homodin detektor, mivel a fotonnyaláb tulajdonságait nézi, ezért kevésbé érzékeny a zajfotonokra.

4.5.1 Modell DVQKD kulcsráta számításra:

DVQKD esetén egy bitet 1 db foton ad. A klasszikus csatornák által okozott várhatóan nagy zaj miatt a számításban csak 1 klasszikus csatornával dolgozok. A számítás menetét [22] forrás módszere alapján készítettem el.

Az egyfoton detektort a gyakran használt InGaAs (indium gallium arsenide) fotodiódával megvalósítottak képzeljük. Ennek van egy érzékelési ablaka, ami abból áll, hogy mekkora frekvenciaspektrumon érzékel és mennyi ideig van nyitva. Ez a kódban paraméteresen állítható, de alapból, ahogy a cikk is, az ablakot 75 GHz-esnek vettem, az időt pedig 1 ns-nak.

Tehát az időablakot (8) képlet szerint számolhatjuk.

$$N_{Mod} = df \cdot dt \quad (8)$$

Ezután ki kell számolni az egyfoton detektor egy ablakában érkező zajfotonok számát. (9) képlet megadja az elrendezés C pontjánál lévő zajfotonok számát.

$$N_{SPD_C} = N_{Mod} \cdot \eta_{ch} \cdot \eta_{DMU} \cdot N_{ASE_A} + N_{LEAK_C} \cdot dt + N_{Mod} \cdot N_{SRS_C} \quad (9)$$

Az egyenlet első része az erősítő zajáról szól:

- N_{Mod} : az 1 ns-os, 75 GHz-es ablak
- η_{ch} : optikai szál átvitele (0.2 dB/km csillapítással számolva)
- η_{DMU} : demultiplexer átvitele (-1.5 dB csillapítással számolva 0.7079 értékű)
- N_{ASE_A} : erősítő zaja az A pontban (4.1-ben számolva)

A második rész a klasszikus csatornák áthallásáról szól:

- N_{LEAK_C} : áthallásból származó fotonszám a C pontban (4.2-ben számolva).
- dt : csak az 1 ns-os ablakkal kell dolgozni, mivel N_{LEAK} számításánál már figyelembe vettük a frekvenciát

A harmadik rész a Raman szórást veszi figyelembe:

- N_{SRS_C} : a C pontban lévő Raman szórásból származó fotonszám.

Ezután [31] által készített módszerrel, (10) egyenlet segítségével lehet kiszámítani a kulcsgenerálási sebességet a C pontnál lévő zajfotonszám alapján.

$$R = \frac{1}{2} [Q_1 - f(E_\mu) \cdot Q_\mu \cdot H_2(E_\mu) - Q_1 \cdot H_2(e_1)] \quad (10)$$

- R jelenteni a sebesség értéket, vagyis a generált kulcsok számát 1 másodperc alatt. A kiszámításához szükséges elemek képletei (10.1 – 10.5) csoportban láthatók:

$$Y_0 = Y_0^0 + \eta_{BOB} [N_{SPD}^{tot}] \quad (10.1)$$

$$Q_\mu = Y_0 + 1 - e^{-\eta_\mu} \quad (10.2)$$

$$E_\mu = [e_0 \cdot Y_0 + e_{det}(1 - e^{-\eta_\mu})] / Q_\mu \quad (10.3)$$

$$Q_1 = (Y_0 + \eta) \cdot \mu \cdot e^{-\mu} \quad (10.4)$$

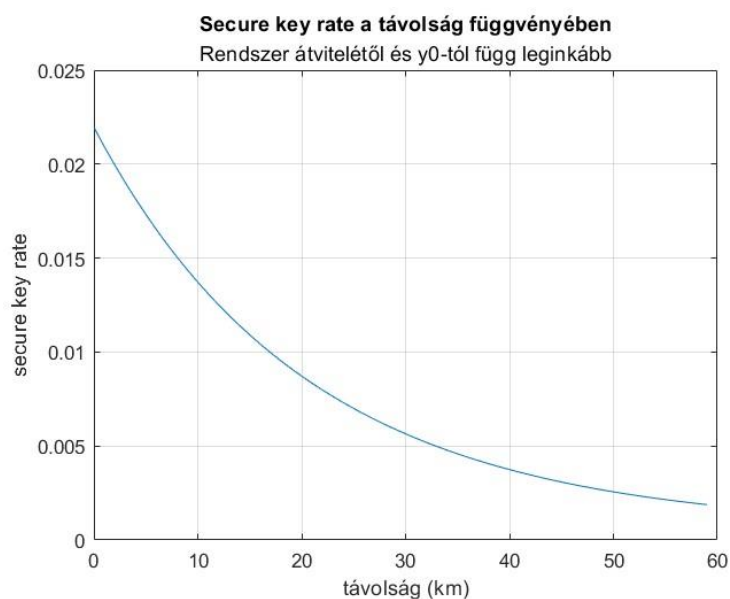
$$e_1 = (e_0 \cdot Y_0 + e_{det} \cdot \eta) \cdot \mu \cdot e^{-\mu} / Q_1 \quad (10.5)$$

Változók a 10.1 - 10.5 képletekben:

- Y_0 : rossz észlelések száma (amikor a fotodióda zajfotont kap információt tartalmazó foton helyett). Ezt a rajzon Bob pontján kell értelmezni.
- Y_0^0 : rendszer egyéb háttérzaja, [22] alapján $5 \cdot 10^{-6}$ fotonszámnyi értékkel
- η_{BOB} : Bob átvitele. [22] cikk 0.6-al számolt, ami az ideálistól messze van, így szerintem megfelelő lesz
- N_{SPD}^{tot} : előbb kiszámolt, C pontban lévő zajfotonszám. (Azért kell megszorozni (10.1)-ben Bob átvitelével, mert Bob nem engedi át a hozzá érkező jel egészét)

- η : teljes rendszer átvitele, vagyis $\eta = \eta_{ch} \cdot \eta_{DMU} \cdot \eta_{BOB}$.
- μ : egy paraméter, értéke 0.5. DVQKD megvalósítási módonként eltérhet, de a leggyakoribb DVQKD protokoll, a BB84 esetén azért lesz $\frac{1}{2}$, mivel a fotonok polarizációja az esetek felében nem egyezik a detektor bázis polarizációjával és így csak a megérkezett hasznos (nem zaj) fotonok feléből lesz kódbit
- e_{det} : annak a valószínűsége, hogy nem találja el a detektort a foton (ennek [22] forrás 0.003 valószínűséget adott)
- Q_μ : a jelállapotok nyeresége. Ha megnézzük 10.2 képletet, az exponenciális tagban szereplő átvitel a távolság függvényében csökken, míg μ állandó marad, így az exponenciális tag is csökken. Matlabban látható, hogy Q_μ a távolság függvényében csökken, értéke 0.2 és 0.064 között van (0-60 km-ig számolva)
- E_μ : a kvantumbit hiba ráta
- Q_1 és e_1 olyan tagok, amiket a könnyebb kiszámíthatóság érdekében vezették be.
- A ráta (10) képletében található függvények leírása a [28] cikkben megtalálható.

Az eredmények várhatóak voltak, de sajnos kicsit elszomorítóak. A szimuláció azt mutatta, hogy tulajdonképpen nem keletkezik kulcs, mivel a kulcsráta 0.02 alatt van és távolság függvényében még csökken is. Az eredmény 4.13 ábrán látható:



4.13 ábra: Kulcsráta DVQKD esetén a távolság függvényében

A rossz kulcsráta oka az, hogy a klasszikus csatornákból származó áthallás és az ottlétükből fakadó egyéb zajok (Raman szórás, erősítő zaja) miatt túl sok a zajfoton. Ha belegondolunk, hogy a BB84 protokoll az Alice által küldött fotonok felét el is dobja (mert rossz bázissal mérte), akkor, ha még zajt is teszünk hozzá, rendkívül le fog lassulni a kulcsmegosztási folyamat.

A megoldás irányába vihet minket, ha Bob-ban minél rövidebb időablakos egyfoton detektort használunk és jobban szinkronizáljuk Alice-t és Bobot. Sajnos esélytelen, hogy olyan gyorsan nyitogassuk a detektort, ahogy a fotonok érkeznek, így mindenképpen maradnak zajfotonok a kulcsmegosztás közben. A másik segítség az lehet, ha olyan adónk van, ami nagyon pontos hullámhosszú fotonokat küld és olyan vevőnk,

ami nagyon szűk szűrővel rendelkezik, mert akkor sok, eltérő hullámhosszú zajfotont ki tudunk zárni.

További megoldási lehetőség, hogy inkább CVQKD felé fordulunk, akkor, ha WDM hálózatba szeretnénk integrálni QKD-t.

4.5.2 Modell CVQKD kulcsráta számításra

Ahogy már korábban tárgyaltam, CVQKD esetén nincs szükség egyfoton detektorra, valamint nem a foton polarizációja hordozza az információt, hanem a kevés (ezres nagyságrendű) fotont tartalmazó fotonnyaláb tulajdonságai – leginkább fázisa. Mivel nem egy foton tulajdonságot kell érzékelni, hanem egy nyaláb tulajdonságot, ezért sokkal zajtűrőbb a megoldás. A [22] cikk, amit a számítási modellekhez alapul vettem, a [29] és [30] modelljeit javasolta, amik leírnak egy Gauss moduláción és fordított egyeztetésen alapuló CVQKD protokollt és a kulcsráta számítási módjukat. Ezek segítségével készítettem el saját számításaim. Itt a számítás sokkal bonyolultabb, mint előző esetben. Azért, hogy több klasszikus csatorna esetére is megmutathassak eredményeket, a Matlabban minden számítást külön függvénnyel végzek.

Magát a kulcsrátát a (11) képlet adja:

$$\Delta I = \gamma \cdot I_{AB} - \chi_{BE} \quad (11)$$

Itt γ a fordított egyeztetés algoritmusának hatékonysága (0.9-nek választva), a másik két elemet, pedig külön kell számolni (11.1-11.) képletekkel: (képletek forrása: [22], részletesebben levezetve: [30])

$$I_{AB} = \frac{1}{2} \cdot \log_2 \left(\frac{V + \chi_{tot}}{1 + \chi_{tot}} \right) \quad (11.1)$$

$$\chi_{BE} = \Theta \left(\frac{\sigma_1 - 1}{2} \right) + \Theta \left(\frac{\sigma_2 - 1}{2} \right) + \Theta \left(\frac{\sigma_3 - 1}{2} \right) + \Theta \left(\frac{\sigma_4 - 1}{2} \right) \quad (11.2)$$

$$\Theta(x) = (x + 1) \log_2(x + 1) - x \log_2 x \quad (11.3)$$

$$\chi_{tot} = \chi_{line} + \frac{\chi_{hom}}{\eta_{ch}} \quad (11.4)$$

$$\chi_{line} = \frac{1}{\eta_{ch}} - 1 + \epsilon \quad (11.5)$$

$$\chi_{hom} = \frac{1 + v_{cl}}{\eta' - 1} \quad (11.6)$$

$$\sigma_{1,2}^2 = \frac{1}{2} (A \pm \sqrt{A^2 - 4B}) \quad (11.7)$$

$$\sigma_{3,4}^2 = \frac{1}{2} (C \pm \sqrt{C^2 - 4D}) \quad (11.8)$$

$$A = V^2(1 - 2\eta_{ch}) + 2\eta_{ch} + \eta_{ch}^2(V + \chi_{line})^2 \quad (11.9) \quad B = \eta_{ch}^2(V\chi_{line} + 1)^2 \quad (11.10)$$

$$C = \frac{V\sqrt{B} + \eta_{ch}(V + \chi_{line}) + A\chi_{hom}}{\eta_{ch}(V + \chi_{tot})} \quad (11.11)$$

$$D = \sqrt{B} \cdot \frac{V + \sqrt{B} \cdot \chi_{hom}}{\eta_{ch}(V + \chi_{tot})} \quad (11.12)$$

$$V = V_A + 1 \quad (11.13)$$

$$\eta' = \eta_{DMU} \cdot \eta_{BOB} \quad (11.13)$$

$$\epsilon = \epsilon_0 + \frac{\epsilon_{in}}{\eta_{ch} \cdot \eta_{DMU} \cdot \eta_{BOB}} \quad (11.14)$$

Ezeknek a képleteknek a használhatóságához viszont még sok adatot tisztázni kell.

Először is ennél a megoldásnál homodin detektort használunk, aminek van egy helyi oszcillátora. Ez „mód” szűrőként is tud szolgálni, mivel csak az adott frekvenciájú és fázisú zajt detektálja, a többi elnyomja. Emiatt lesznek csatolt és csatolatlan módú zajfotonok attól függően, hogy milyen viszonyban állnak a helyi oszcillátorral. Ennek a jelenlegi modellben a frekvenciája 1 MHz és 1 nyalábjában kb 10^8 db foton van.

4.5.2 /1 Csatolt módú zaj:

Nézzük meg a csatolt módú fotonok számát, hiszen ez játssza a valódi szerepet a Bobot érő zajban:

$$N_{GMCS}^{in} = \frac{1}{2} m (\eta_{ch} \cdot \eta_{DMU} \cdot N_{ASE}^{(A)} + N_{SRS}^{(C)}) \quad (12)$$

Itt (12) képletben „ m ” a klasszikus csatornák száma. Ezután a csatornaszámmal szorozódik az erősítő zaja a C ponton, valamint a Raman szórás. A cikkek úgy veszik, hogy az áthallási zaj egésze a nem csatolt zajba kerül, mivel CVQKD esetén a nem kvantum csatorna hullámhosszán lévő zaj nem számít.

Mind az erősítő általi zaj, mind a Raman szórás modellezhető kaotikus forrással rendelkező Bose-Einstein fotonstatisztikával. Vagyis a (13) képletben látható statisztikával kenődik el a spektrumon a zaj.

$$(\Delta X)^2 = (\Delta Y)^2 = 2n + 1 \quad (13)$$

Ebből (14) képlettel számolható a Bobot elérő csatolt módú fotonok száma

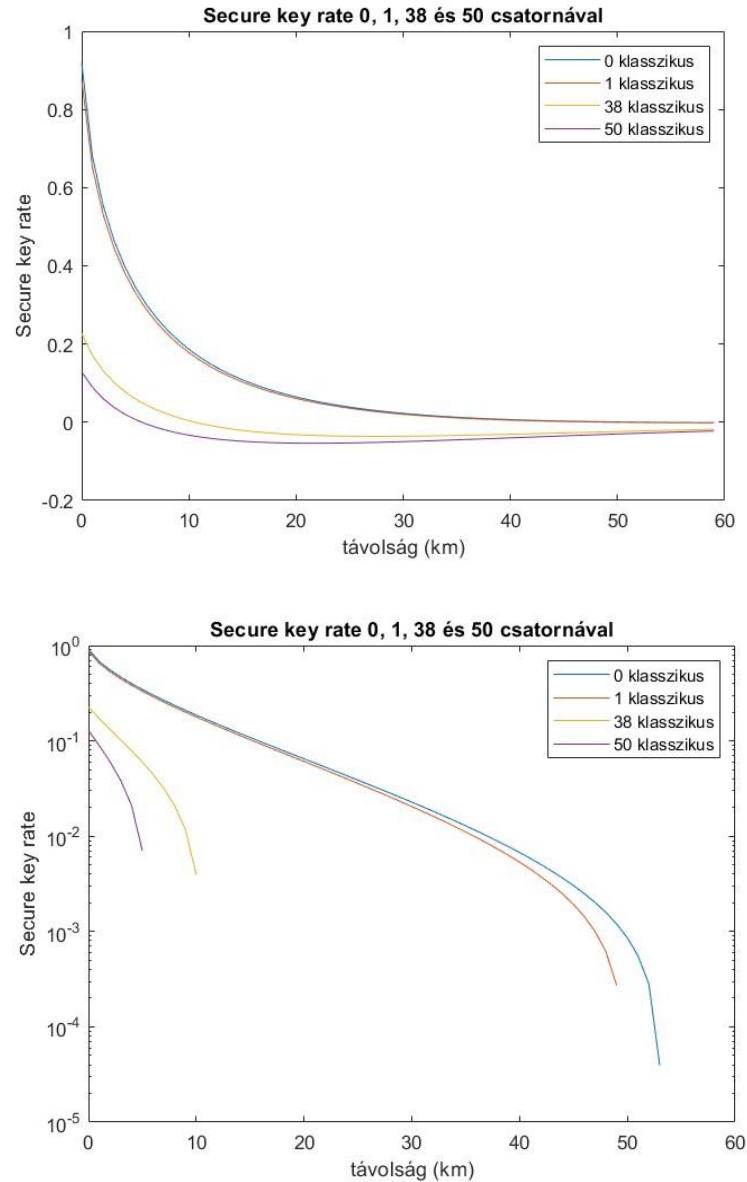
$$\varepsilon_{in} = 2\eta_{BOB} \cdot N_{GMCS}^{in} \quad (14)$$

Ez az eredmény már konkrétan felhasználható a fentebb lévő egyenletrendszerbe.

4.5.3 Kulcsrata számítás és eredmény értékelés:

Az utolsó megadandó változó ahhoz, hogy elvégezhető legyen a (11) egyenletrendszer, az a V_A . Ez a modulációs variancia és alapértéke 10. „ V ” kiszámításához szükséges, ami az Alice által készített koherens állapot kvadratúra varianciája. (ez egy jellemző arra, hogy Alice modulálása milyen varianciájú jeleket készít a konstellációs ábrára)

Ezután már mindent beírhatunk (11) egyenletrendszerbe. Lefuttattam különböző számú klasszikus csatornára és az eredmény 4.14 ábrán látható. Először viszonyoszámként, utána dB-ben.



3.14 ábrák: Kulcsrátá CVQKD esetén a távolság függvényében felső ábrán viszonzyszámként, alsó ábrán dB-ben

Több érdekesebb megfigyelést is tehetünk. Egyrészt a klasszikus csatorna nélküli és az 1 klasszikus csatornás megoldás között alig van különbség kulcsrátában. Ezen esetekben kb. 15-25 km-ig lehet hatékony a megosztás. A nagy távolságú (BME I épület – Telekom Fehérvári út) CVQKD mérésnél 4.67 dB szálcsillapítást mértek [20], ami egy rosszabb szállal nézve (0.25 dB/km) kb 18 km-nek felel meg. Ott sikeres volt ekkora távolságon a CVQKD kulcsmegosztás, vagyis ez, az én számításomnak azon felét igazolja, hogy 1 csatornával akár 25 km-ig is jó marad a kulcsrátá. 38 és 50 csatornával a modell szerint inkább csak 5-10 km-ig tud működni a kulcsmegosztás, utána túl nagy lesz a zaj.

4.6 Változtatható paraméterek hatása a CVQKD kulcsráta

A Matlab szimuláció elején a különböző modellrészekhez különböző adatokat meg lehet adni, így többféle paraméterrel is lefuttathatóak. Én most a fontosabbakat emelném ki.

Egy táblázatba foglalom össze, hogy a szimuláció szerint a különböző alapparamétereknek mik az alapértéke, és mekkora érték esetén romlik már el a kulcsráta klasszikus csatornákkal együtt, illetve azok nélkül. Az értékek próbálgatásával mindig újra futtattam a kódot és megnéztem, hogy a kulcsráta mikor romlik el annyira, hogy már „használatatlannak” nyilvánítsam. A használhatatlan az én értelmezésemben azt takarja, hogy a kulcsráta értékei 0 közeliek.

A „kulcsráta elrontási határértéke klasszikus csatornákkal együtt” oszlopban azt veszem határértéknek, ha a 38 csatornás kulcsráta már kis távolságnál is 0 közeléből indul. Az 1 klasszikus + 1 kvantum csatorna rátája, tapasztalat alapján szinte együtt mozog az önálló kvantum csatorna kulcsrátájával. Így az 1 és 38 közötti számú klasszikus csatornákkal való integrálás határértékei pedig kb. a kettő határérték közé esnek.

A javítási lehetőség pedig azt takarja, hogyha a megfelelő irányba változtatjuk az értéket, akkor mennyit tudunk javítani a kulcsrátán.

Név	Alapérték a szimulációban	Kulcsráta elrontási határértéke klasszikus csatornákkal együtt	Kulcsráta elrontási határértéke csak kvantum csatorna esetén	Javítási lehetőség	Változtatása milyen mértékben változtatja a kulcsrátát
NF (EDFA „noise figure” paramétere)	5.5 dB	33 dB	50 dB	nincs érdemi javulás	kicsit
mux/demux izoláció	-80 dB	-40 dB	-10 dB	nincs érdemi javulás	sok csatorna esetén nagyon, 1 csatorna esetén minimálisan
klasszikus csatornák teljesítménye	0 dBm	2 dBm	1 klassz. + 1 kvantum: 13 dBm	-10 dBm-nél már közel egybeesik a 4 ábrázolt kulcsráta	Nagyon
mux/demux vesztesége	-1.5 dB	-30 dB	-50 dB	0 fölé nem lehet menni, így nincs	Kicsit

4.7 Értékelés és fejlesztési lehetőségek

Összességében azt foglalnám össze eredményként, hogy CVQKD alkalmazásával lehetséges lehet kvantumos csatornát integrálni egy WDM hálózatba. Ahogy a 4.5.2 és 3 pontban is értékeltem a kulcsrátá eredményeket, attól függően, hogy hány csatorna van, a modell alapján 5-25 km-es távolságban is létrejöhet kulcsmegosztás.

A modellt más modellek és számítási módszerek segítségével állítottam össze, amik hasonló eredményre jutottak. Ennek ellenére van pár olyan elem, ami szerintem hiányzik, és fejlesztési lehetőségként, pontosításként bele lehetne implementálni.

Egyrészt a modell nem tudja kezelni, hogy a klasszikus csatornák milyen hullámhosszon vannak. Például. 4.5.2 /1 szakasz utolsó két egyenlete arról szól, hogy a zajfotonokat egy statisztika alapján osztja el, vagyis tulajdonképpen elkeni a teljes spektrumon. Ezt a részt már a 3. és 5. fejezetben részletezett mérések elvégzése után írom, így tudom, hogy van szerepe annak, hogy pl. a szomszéd csatornákon helyezkednek el klasszikus csatornák vagy pedig a kvantumos csatornától távolabb.

Egy másik kissé hiányzó elem az, hogy a [29] és [30] által készített CVQKD kulcsrátá számító algoritmus nem veszi figyelembe a kvantumos csatorna pontos teljesítményét, csak - értelmezésem szerint – azt nézi, hogy egy 100-1000 körüli fotonszámmal operáló fényimpulzus milyen kulcsrátát tud elérni a zajok, csatornaszámok és távolság függvényében. Itt még esetleg lehetne pontosítani.

Az utolsó, szerintem kissé hiányzó elem az, hogy a források zaját nem veszi bele. A 3-as és 5-ös fejezet méréseinek elvégzése után jöttem rá, hogy ez is fontos és megváltoztatja a zajképet. Ennek ellenére szerintem a modell összeredményét nem változtatja meg teljes mértékben. A kis távolságon való kulcsrátá értékén viszont biztosan változtat, hogy van egy zaj, ami a szál kezdetétől akár 10-20 km-ig is dominálhat (de a szálcillapítás miatt csökken). Ennek a problémának a kibontása az 5. fejezet végén folytatódik a mérés eredményének megismertetése után.

5. Mérés a Telekom Laboratóriumában

5.1 Labor bemutatása:

A Magyar Telekom rendelkezik egy rendszertechnológiai laboratóriummal Győrben. Ez egy 3 szintes épület több gépteremmel és irodákkal. Arra a célra szolgál, hogy minden olyan eszköz, ami bekerül a hálózatba, egy darab megtalálható legyen itt, így bármi probléma vagy fejlesztési lehetőség tesztelése esetén itt az eszközöket különböző körülmények között ki lehet próbálni, kísérletezni lehet velük, akár szét lehet szedni őket. Így nem kell az előhálózati eszközökkel kísérletezni valamilyen furcsa hiba keresése, vagy valami új dolog kipróbálása esetén.

A WDM hálózatok a transzport hálózathoz (maghálózathoz) tartoznak, ezért a méréseimet a földszinti transzport laboratóriumban végeztem. Mivel gyakornokként dolgozom a Telekom Transport Network Tribe-jában, ezért volt lehetőségem a mérések elvégzésére.

5.2 Használt eszközök:

Az összes eszköz olyan, amik jelenleg is benne vannak az élő hálózatban. Vagyis attól még, hogy egy laborban, laboreszközökkel mértünk, olyan eszközökön próbálhattuk ki a mérést, amire rákerülne a QKD-csatorna a tényleges hálózatban.

Az adó az 5.1 ábrán látható 2 db Huawei LSX Transponder volt. Ez egyszerre 1 csatornát tud adni, viszont 96 különböző hullámhosszon hangolható, hogy egy 96 csatornás WDM-be is bármilyen csatornát adhasson. Sajnos csak 2 transzponder állt rendelkezésre a laborban, így 2-nél több klasszikus csatornával nem tudtuk kipróbálni



5.1 ábra: kísérlethez használt transzponderek



5.2 ábra: multiplexer és demultiplexer

A multiplexer és demultiplexer az 5.2 ábrán látható 40 csatornás Huawei Optix 1800 termékcsaládból származik.

Ezen túl a rendszerbe nem tettünk be más elemet. Egy valódi WDM rendszerben lennének még erősítők és egyéb eszközök, viszont erősítő mellé nem lehet betenni kvantumos csatornát, a kikerüléssel pedig nem akartuk bonyolítani a kísérletet.

5.3 Mérések

A fő cél itt is az volt, mint az előző mérésekben, vagyis, hogy egy kvantumosnak képzelt csatornát hagyjunk üresen és köré rakjunk klasszikus csatornákat majd megnézzük, hogy mekkora a zaj az üres „kvantumos” csatornában. Így megállapíthatjuk, hogy lehetne-e integrálni QKD eszközt a rendszerbe.

5.3.1 Mérőeszköz zaja

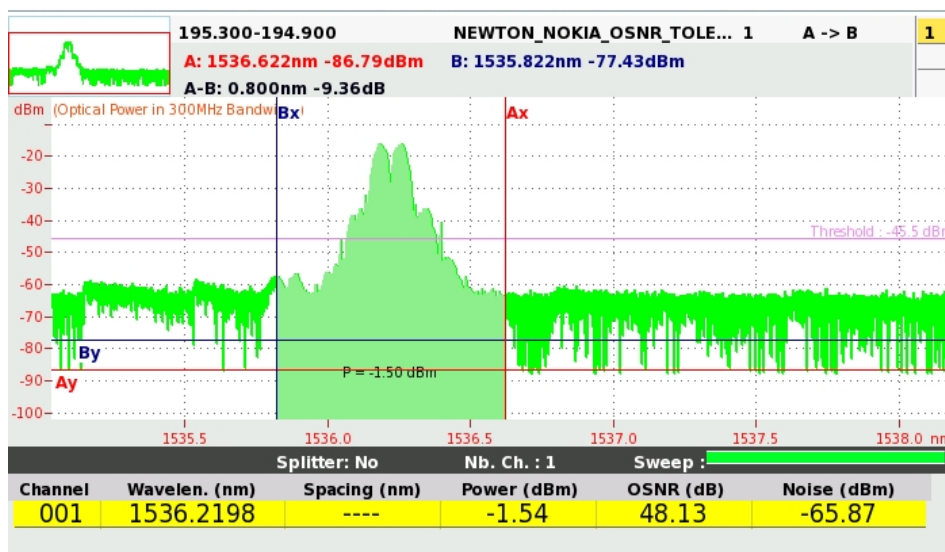
Ahhoz, hogy pontosan tudjuk értékelni a mérési eredményeket, fontos ismerni, hogy mekkora a mérőeszköz saját zaja. Vagyis azt nézzük meg, hogy mit mér az eszköz, ha semmi sincs rákötve.

A mérés szerint az eszköz saját zaja átlagosan -75 dBm alatti, ekkora szintig biztosan pontos a teljesítmény mérés. Sőt, kurzoros mérés esetén a kurzornál képes volt megmérni -86.79 dBm -et. Ezért azt, hogy egy -60...-70 dBm körüli CVQKD integrálható-e, azt meg tudjuk mérni, de hogy egy ennél jóval kisebb teljesítményű DVQKD-val mi a helyzet, azt nem tudhatjuk sajnos, mert nem tudjuk, hogy lehet-e -87 dBm alatti teljesítményszint az üres csatornán és hogy -75 dBm alatt mennyire pontosan tud mérni az eszköz.

5.3.2 Transzponder teljesítménye

Azért, hogy tudjuk, hogy mekkora teljesítményű csatornákat teszünk a kvantumos mellé, ismernünk kell a transzponderből kijövő pontos jelteljesítményt.

A spektrumanalizátor automatikusan megtalálta a kiadott csatornát (1536 nm-es csatorna) és kiírta a teljesítményét is.

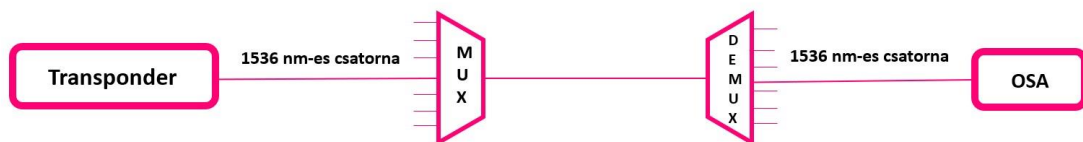


5.3 ábra: egy transzponder csatornája és annak teljesítménye a spektrumanalizátoron

A teljesítményt úgy számolja, hogy meghatározza a csatorna szélességét (kb. ide állítottam be a kurzorokat is), majd az ott lévő jeltartományt integrálja. Így a csalóka csúcsleolvasás helyett, egy sokkal realisabb teljesítményt lehet kapni. Mint 5.3 ábrán látható, ez **-1.54 dBm** lett, ami megfelel a hagyományos optikai kommunikáció csatorna teljesítményének.

5.3.3 Egy klasszikus csatorna a mux/demux-on át

A mérés célja az, hogy lássuk, hogy milyen csillapításon esik át a klasszikus csatorna, hogyha átmegy a rendszerünkön. Ez azért fontos, mert nyilvánvalóan a kvantumos csatorna is ugyanekkora csillapításon fog átesni. Egyébként a valós rendszerben az erősítők miatt nem jelentkezik ez a nagyságú csillapítás.



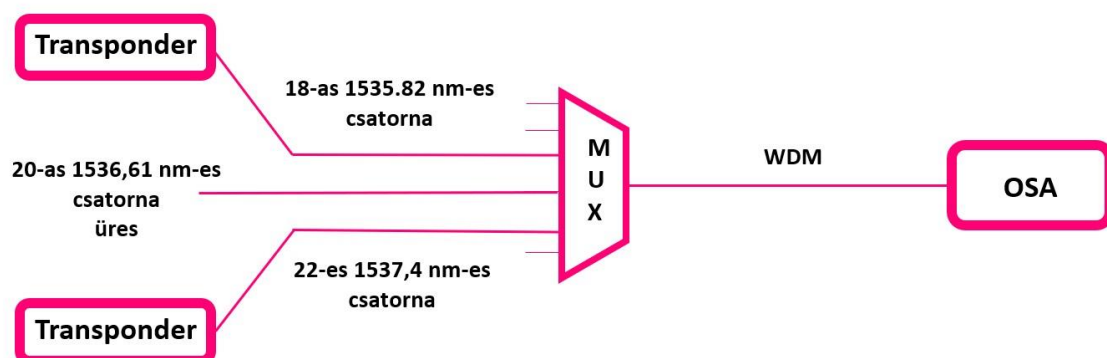
5.4 ábra: Egy klasszikus csatorna csillapításának mérése egy multiplexeren és demultiplexeren keresztül

A mérés előtt már mind a két transzponder teljesítményét külön-külön megmértük.

Az eredetileg -1.5 dBm körüli csatornák **-10...-13 dBm** teljesítményre estek vissza. Ez legnagyobb részben a multiplexerek és demultiplexernek, valamint kis részben a szál csillapításának köszönhető.

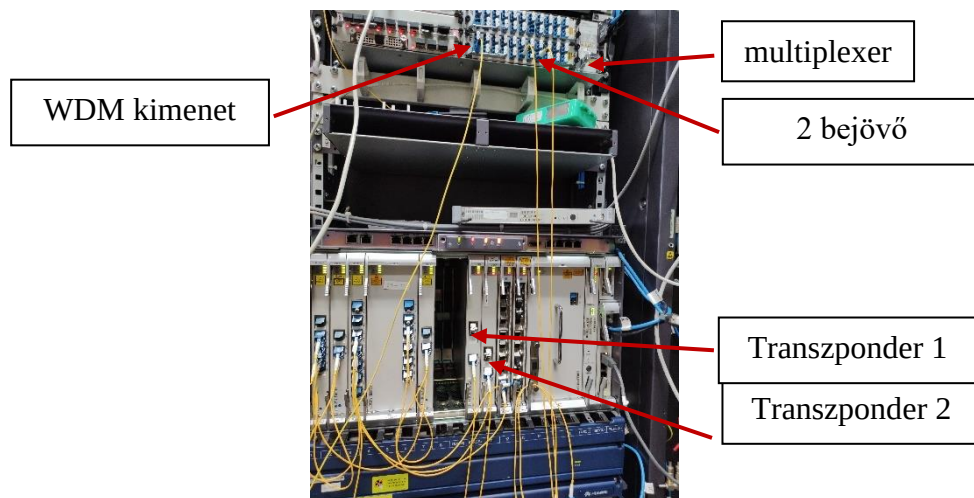
5.3.4 Közös szakasz mérése 2 klasszikus és közöttük egy üres csatornával

Ezt tekinthetjük akár a fő mérésnek is, hiszen azt szimuláljuk, hogy mi történik 2 klasszikus csatorna közé illesztett üres „kvantumos” csatornával. A mérési ebben a mérésben a WDM-es közös szakaszon van, mivel így mindenféle demultiplexeres szűrés nélkül láthatjuk, hogy mi történik a rendszer belsejében.



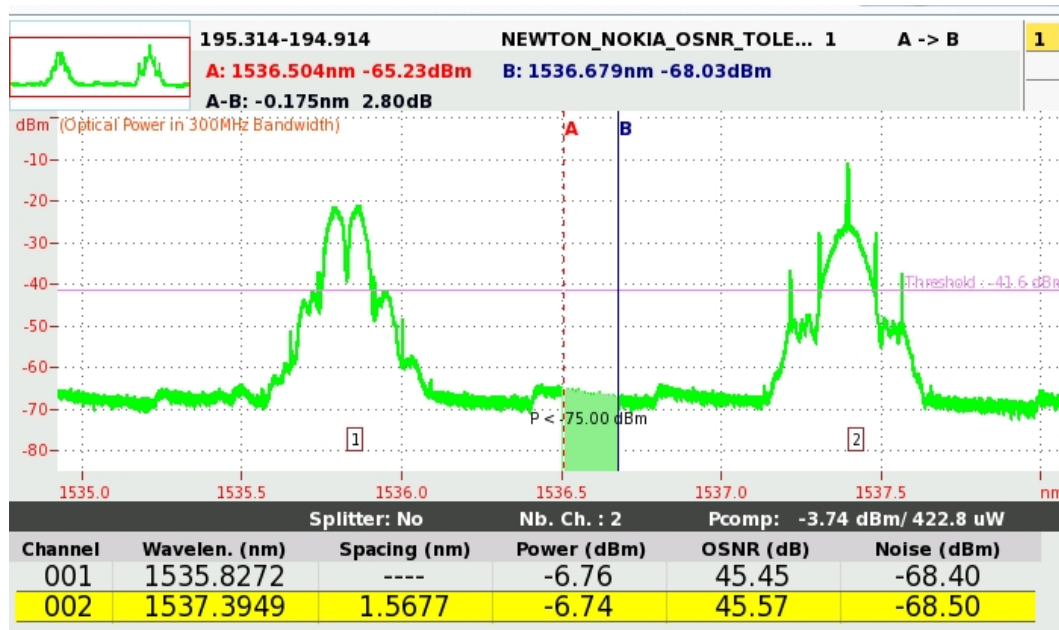
5.5 ábra: két klasszikus csatorna közé illesztett üres csatorna mérése a közös szakaszon

A mérési elrendezés a valóságban 5.6 ábrán látható:



5.6 ábra: 5.3.4 mérés elrendezése a valóságban

A mérés eredménye 5.7 ábrán található:



5.7 ábra: 5.3.4 eredménye, két oldalt két klasszikus csatorna, középen az üres csatorna

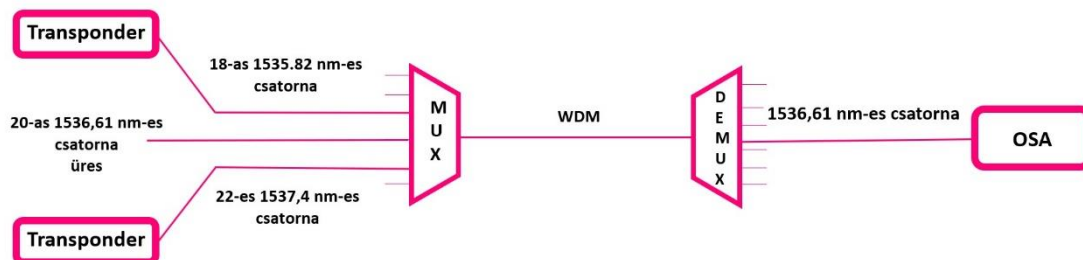
Láthatjuk mind a 18-as (1535.8 nm) mind a 22-es csatornát (1537.4 nm). Kiolvashatjuk a csatornák integráltjából kapott teljesítményeket, amik -6.7 dBm környékén vannak. Ha azt nézzük, hogy a kiindulási teljesítmény 5.3.2 alapján -1.5 dBm körül volt, akkor elmondhatjuk, hogy 5.2 dB-t (vagyis kicsit kevesebb, mint harmadára) csillapodtak a klasszikus csatornák. Ez valószínűleg a multiplexernek és a csatlakozási pontoknak köszönhető.

Nézzük a kvantumosnak kiválasztott csatorna helyét (1536.6 nm körül). Sajnos a kurzorokkal működő beépített teljesítménymérő nem működik megfelelően, mivel $P < -75$ dBm-et mutat. A kurzorokkal mért teljesítmény **-65 dBm** és **-68 dBm** körül van.

A másik fontos dolog, hogy láthatóan a szomszédos csatornák teljesítményének fel és lefutásai sem érnek bele a kvantumosan kiválasztott csatornába, hiába csak kb 0.5 nm-re vannak tőle. Úgy gondolom, hogy ez az alacsonyságú zajszint már elég lehet ahhoz, hogy érzékeltetni lehessen mellette egy CVQKD-csatornát. Azt is érdekes látni, hogy mindenféle szűrő nélkül is (a kísérletben nincs a hálózatban a demultiplexer), milyen szépen elkülönülnek egymástól a csatornák és nem foglalnak el túl nagy spektrumot.

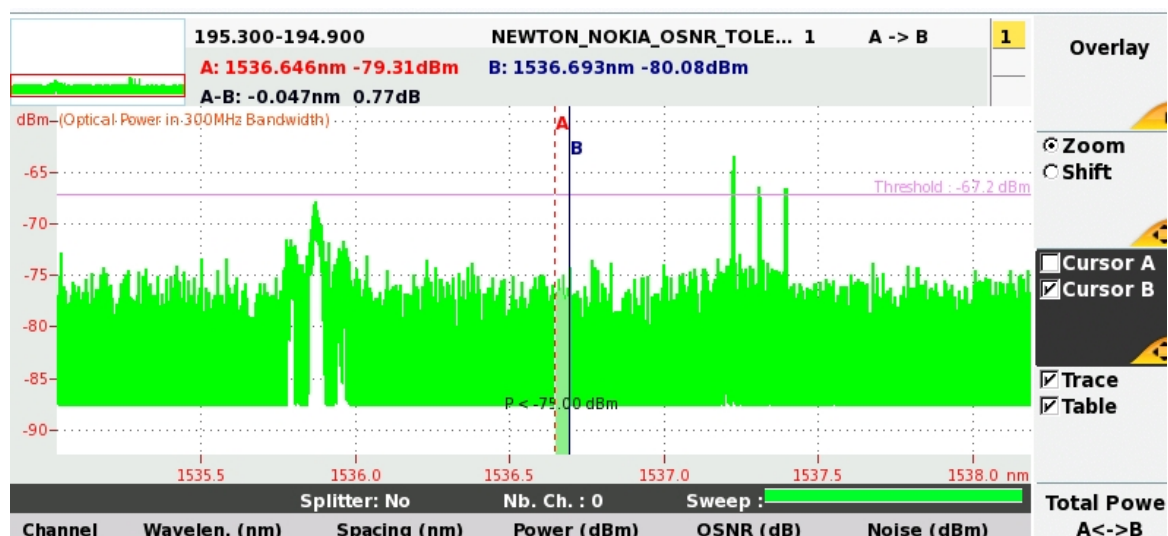
5.3.5. Mérés a demultiplexer után, 2 klasszikus szomszédos csatornával

Ezt a mérést mondanám a másik legfontosabbnak. Az elrendezés itt annyiban más, hogy a WDM szakasz után ott van a demultiplexer, aminek az 1536.61 nm-es 20-as számú csatornájára csatlakozunk a spektrumanalizátorral. Az eredmény annyiban lesz más, hogy a demultiplexer elméletileg csak az adott csatornán lévő tartalmat engedi át, így a 2 szomszédos csatornán lévő jelek nem fognak látszódní.



5.8 ábra: Két klasszikus közé illesztett üres csatorna mérése a demultiplexer után

A mérés eredménye 5.9 ábrán tekinthető meg.

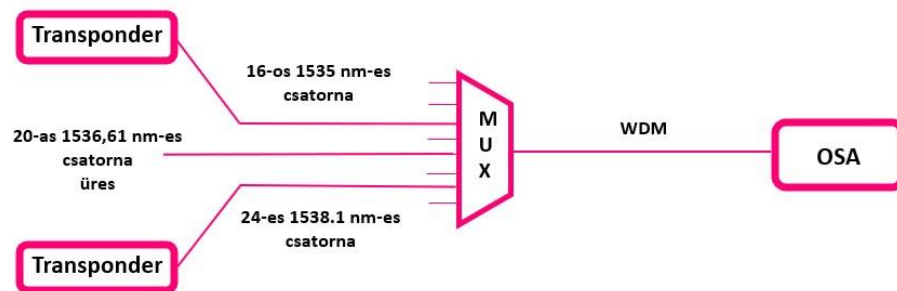


5.9 ábra: 5.3.5 eredménye, középen az üres csatorna, a két szélén pedig a klasszikus áthallatszó maradványai

Az eredményből 2 fontos tanulságot vonnék le. Az egyik, hogy a két szomszédos csatorna láthatóan egy kicsit áthallatszik, viszont ez a (kurzorokkal kijelölt) kvantum csatorna helyére nem „szivárog” át. A másik, hogy az alapzaj szintje („A” és „B” kurzorok mérése alapján) **-80 dBm** körül van. Az 5.3.4 mérés eredményénél kisebb zajt elsősre 3 dolog miatt tartanám lehetségesnek. Az egyik az, hogy a hosszabb WDM szakasz miatt a szálcscsillapítás nő és a távolság függvényében növekvő zajok nem nőnek annyira, mint amekkora a csillapítás. Így összességében csökken a zaj teljesítménye. Ezt kevésbé tartom lehetségesnek, mivel a szál alig lett hosszabb. A másik elképzelésem, hogy a demultiplexer szűrője jó annyira, hogy a zajt lecsökkenti -60-ról -80 dBm környékére. Ezzel viszont az az érdekes, hogy az a szakasz, amit a szűrő átenged (20-as csatorna, 1536 nm környéki sáv, ami kurzorokkal van jelezve), ugyanúgy kis zajú. Ha a szűrő lenne jó, akkor az átengedett spektrumon valószínűleg nagyobb zajnak kellene lennie (hiszen a szűrő nem tudja, hogy az adás-e vagy zaj), és csak a többi részen lévő zajt kellene ennyire elnyomni. A harmadik dolog, a legvalószínűbb, hogy maga a demultiplexer eszköz többi belső eleme okozza a nagy csillapítást. Probléma, hogy a QKD jel is csillapítódni fog, viszont, ha a jel és a zaj is egyenlő mértékű csillapításon esik át, akkor ugyanúgy ki fog látszódni a QKD (leginkább CVQKD) jel.

5.3.6 Mérés a WDM szakaszon, távolabbi klasszikus csatornákkal:

Itt az elrendezés hasonló, mint 5.3.4 mérés esetén, viszont a két klasszikus csatornát nem az üres csatorna szomszédjába, hanem kicsit messzebb helyeztük. Így az üres csatorna maradt a 20-as számú 1536.6 nm-es helyen, de a két klasszikus a 16-os számú 1535 nm-es és a 24-es számú 1538.18 nm-es csatornára került. A mérést a közös szakaszból végezzük.



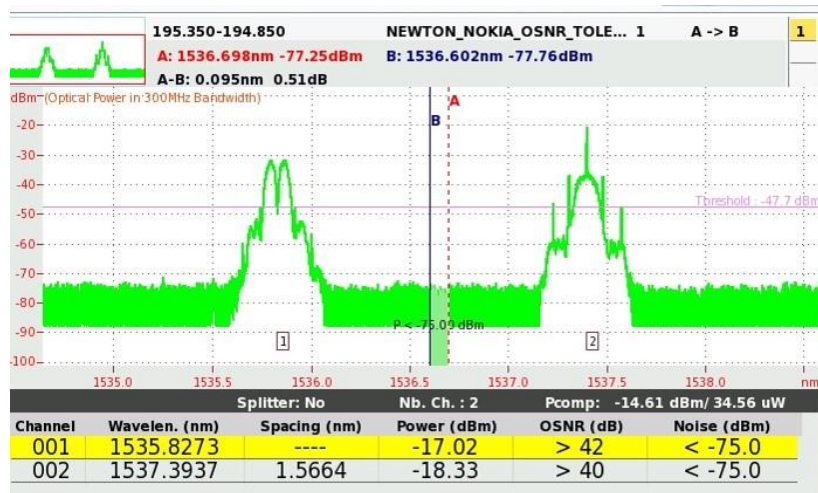
5.10 ábra: Két klasszikus közé illesztett üres csatorna mérése a közös szakaszon. 16-os és 24-es csatornán található a klasszikus jel.

Az eredmény a várakozásoknak megfelelően alakult. A 2 klasszikus csatorna teljesítménye maradt -7 dBm környékén, az üres csatornán pedig 5.3.4-hez képest kisebb, **-70 dBm** körüli zajszint mérhető.

Az eredmény azt jelenti, hogy ezzel a megoldással egy CVQKD eszköz jele már szinte biztosan érzékelhető.

5.3.7 WDM szakasz mérése a klasszikus csatornák 10 dB-es csillapításával

Ebben a mérésben az lett az ötlet, hogy ne a kvantumcsatornán vagy a környezetén változtassunk valamit, hanem a klasszikus csatornákkal. A transzponderek kimenetére 1-1 darab 10 dB-es csillapítót helyeztünk. A klasszikus csatornákat a szomszédos csatornákra tettük, hogy lehető legnagyobb zavarás mellett tudjunk értékelni.



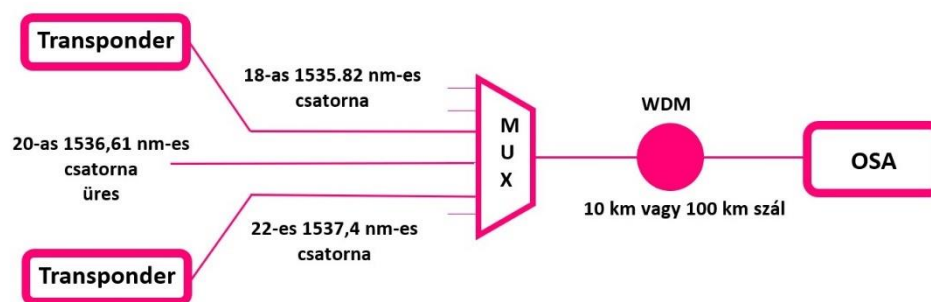
5.11 ábra: 5.3.7 mérés eredménye a spektrumanalizátoron.
Két oldalt a csillapított klasszikus csatornák, középen a
kurzoroknál az üres „kvantumcsatorna”

Az eredmény azt mutatja, hogy az üres csatorna helyén **-77 dBm** környékén van a zajszint, ami az eddigi legjobb eredmény. Tehát a klasszikus csatorna elnyomás nagyon sokat javítana egy QKD-csatorna integrálhatóságán.

Sajnos ezzel a legnagyobb probléma az, hogy a valós hálózatban 0 dBm körüli jelteljesítményt használnak, így ennek a lehetőségnek a kiaknázásához komolyabban bele kellene nyúlni az alapvető hálózati elvekbe. Viszont érdemes lehet vizsgálni, hogy 10 dB-el kisebb teljesítménnyel mennyire működnek jól a WDM rendszerek, hiszen így lehetőség lenne CVQKD-csatornát integrálni.

5.3.8 WDM szakasz mérése 10 és 100 km szál közbeiktatásával

Klasszikus csatornákhöz a szomszédos csatornákat használtuk. Mivel a valóságban is nagy utakat kell bejárnia a jelnek, ezért mindenképpen érdemes megnézni, hogy a távolság miatti szálcsillapítás hogyan hat a zajra és a klasszikus csatornákra. Így ebből következtetni tudunk a kvantumcsatorna sorsáról.



5.12 ábra: hosszú szál beillesztése a közös szakaszra

Az eredményeket táblázat formájában adom meg:

10 km szál közbeiktatása esetén:

Csatornaszám	Hullámhossz	Mért teljesítmény:
18	1535.8 nm	-8.8 dBm
20 (üres)	1536.6 nm	~ -70 dBm
22	1537.4 nm	-10.1 dBm

100 km szál közbeiktatása esetén:

Csatornaszám	Hullámhossz	Mért teljesítmény:
18	1535.8 nm	-26.3 dBm
20 (üres)	1536.6 nm	~ -86 dBm
22	1537.4 nm	-25.95 dBm

Az eredmény több érdekességet is mutat. Az egyik, hogy 10 km szál közbeiktatása nem számít olyan sokat, hiszen az extra szál nélküli 6-8 dBm-es klasszikus csatorna teljesítmény csak kb. 2 dB-el csökkent. A másik érdekesség, hogy a 100 km-es szál esetén jóval kisebb volt az üres csatornán a zaj (-86 dBm), mint a 30 km-es esetén (-70 dBm) és ez kisebb volt, mint a szálhosszabbítás nélküli állapot (-66 dBm). Ez egybevág a 3.3.3 mérés eredményével is és azt jelenti, hogy a zajok a távolság növelésével csökkennek. Ez csak úgy lehetséges, hogyha a szálcsillapítás dominánsabb, mint a szálban keletkező zajok (leginkább a Raman szórás). Vagyis hiába nő a zajfotonszám a távolság növelésével, a legtöbb zaj valószínűleg nem a szálban keletkezik, hanem pl. a jelforrásokban, így ahogy nő a szálhossz, nő a szálcsillapítás, és a forrásnál keletkezett zajok teljesítménye csökken.

5.4 Értékelés

5.4.1 Táblázatos eredmények

Az eredményeket először táblázatszerűen értékelem, a benne lévő értékek átlagok és kerekítések.

Kezdeti klasszikus csatorna teljesítmény: -1.5 dBm, Kezdeti kvantumos „képzelt” jelteljesítmény: -65 dBm (CVQKD-val)

Szám	Kísérlet lényege	Klasszikus csatorna teljesítmény [dBm]	Rendszer csillapítás [dB]	Üres csatornán zaj [dBm]	Várható kvantumos jelteljesítmény [dBm]	Integrálható-e
5.3.4	WDM mérés, szomszéd csatornák	-6.75	5.25	-66.5	-71.75	Nem
5.3.5	Demux utáni mérés, szomszéd csatornák	elnyomott/kiszűrt, nem értelmezhető -12 (5.3.3 alapján)	10.5 (5.3.3 alapján)	-80	-75.5	igen
5.3.6	WDM, távolabbi csatornák	-7.6	6.1	-69.1	-71.1	Határeset
5.3.7	WDM, szomszéd csatornák, 10dB csillapító	-17.6	6.1 (17.6 -10-1.5 mivel a csillapítót nem kell figyelembe venni)	-77.5	71.1	igen
5.3.8/1	WDM, szomszéd csatornák, 10 km szál	-9.45	7.95	-70	-72.9	Nem
5.3.8/2	WDM, szomszéd, 100 km	-26.1	24.6	-86	-89.6	Nem

5.4.2 Megállapítások az eredmények alapján:

- Nyilvánvalóan, ahol a kvantumozó jel várható teljesítménye a vevőnél (6. oszlop) kisebb, mint a csatornáján lévő zajszint (5. oszlop), ott nem tud kvantumozó kommunikáció létrejönni.
- A demultiplexer jelenléte segít, mivel a klasszikus csatornák elnyomásával kisebb lesz a kvantumozó csatornán a zaj ([5.3.4 és 5.3.5 alapján] -66 dBm-ről 14 dB csökkentéssel, -80 dBm-re csökkenti). A kiválasztott csatornán viszont csak kb 5 dB extra csillapítást okoz.
- A klasszikus csatornáktól való távolság növelési is segít. Ha nem a szomszéd csatornákra tesszük a klasszikust, hanem csak a 2-vel a kvantumozó csatorna mellett lévőre, akkor már kb. 3 dB-el csökkent a kvantumozó csatornán lévő zaj
- A klasszikus csatornák csillapítása sokat segít. Nem gondolnám, hogy 10 dB-nél nagyobb csillapítás elképzelhető lenne egy élő hálózatban, de már ez is 8.5 dB-el csökkenti a kvantumozó csatornán lévő zajt, ha a klasszikusok a szomszédos csatornákon vannak.
- A szálhossz ugyan összességében csökkenti a zajt a kvantumozó csatornán (100 km akár 10 dB-el is), viszont a szálcsillapítás ennél jóval nagyobb mértékben csökkenti a jelet (100 km-en 24 dB), ezért túl hosszú szálon – hiába lett kisebb a kvantumozó csatornán a zaj – jóval nehezebb lesz a kulcsmegosztás.
- Az előző állítás és 5.3.8-ban megfogalmazott gondolataim alapján valószínűleg a legtöbb a szál elején (még 100 km esetén is) a forrásból származik. Emiatt csökkennek a szálhossz növelésével (mivel a szálcsillapítás ezt is lecsillapítja). Viszont látva, hogy a klasszikus csatornán 100 km 24.6 dB csillapítást okozott, míg a zajon 100 km csak kb 10 dB csillapítást okozott, így a szálon kialakuló zajok (pl. Raman szórás) mégis elég sokat számít. Ez alapján úgy gondolom, hogy a zajok egy ideig csökkennek, de egyre lassabban, majd egy idő után növekedésbe fordulnak.

5.4.3 Zajok eltérése a modellben és a mérésben

Folytatva az előző gondolatmenetet, azért nem mutathatja az elején nagyobb és szálhossz függvényében egy ideig csökkenő zajokat, mivel a forrás zaját nem ilyen nagynak vettem figyelembe.

Ennek ellenére a 3.5-ben a modell végső eredményeként számolt kulcsráta közel lehet a valósághoz. Abban térhet el, hogy a hossz függvényében talán nem olyan hirtelen csökken, hanem egy kicsit alacsonyabbról indul, de azon a „szinten” tovább marad.

6. Összefoglalás

Tulajdonképpen a modelleknek és a méréseknek is az az eredménye, hogy határeset, de megvalósítható egy kvantum csatorna integrálása WDM hálózatba, de csak feltételekkel. Tovább lépési lehetőségként én már csak azt tudnám mondani, hogy ki kell próbálni. Persze lehet finomítani a méréseken, lehet még modernebb műszerekkel még modernebb WDM eszközöket mérni és lehet dolgozni a modell valóságosabbá tételén. Ennek ellenére, ha nem sikerülne elsőre, akkor szerintem hasznos információkkal szolgálhat ez a dolgozat.

A téma körüljárásából kiderült, hogy inkább CVQKD protokollt használó megoldással érdemes próbálkozni, mert egy fotonpáron alapuló, vagy egy DVQKD módszernél a sok zaj valószínűleg lehetetlenné tenné a kulcsgenerálást.

Kiderült, hogy CWDM-en egyszerűbb lenne a nagyobb csatorna számok és távolságok miatt, de ezt már olyan kevés helyen használják, hogy nem biztos, hogy ebbe az irányba kellene menni.

Az egyetemi DWDM mérésével kiderült, hogy régebbi eszközökkel nem feltétlenül érdemes próbálkozni, mert túl kicsi lesz az izoláció és túl nagy a zaj.

Az egyetemi CWDM mérésből kiderült, hogy CWDM-mel, szinte biztosan működne az integrálás a nagy csatornatávok miatt, valamint, hogy a szálhossz növelése furcsán hat a zajra és lehet, hogy mégsem a modellben dominánsnak ítélt Raman szórás a legnagyobb zaj.

A modellből kiderült, hogy a Raman szórás a domináns zaj, valamint elemzésre került a többi zaj is, amiknek a csökkentésével lehet próbálkozni. Továbbá kiderült, hogy a klasszikus csatornák teljesítményének kis visszavételével már nagy változásokat lehet elérni, ezen kívül a multiplexer és demultiplexer izolációja és veszteségeik is rengeteget számítanak egy megfelelő kulcsrátá előállításában. Kiderült, hogyha az erősítő úgy helyezkedik el, hogy csak a klasszikus csatornákat erősíti, akkor a zaja nem akkora befolyásoló tényező. Ezen kívül egész jól használható adatot kaptunk arra, hogy különböző paraméterek és csatornaszámok esetén mekkora lesz a kulcsrátá.

Győrből pedig kiderült, hogy különböző feltételek mellett DWDM-mel is lehetséges az integrálás. Ha van egy jó demultiplexer, az sok zajt kiszűrhet. Ha távolabb tesszük a klasszikus csatornákat, az is segít, bár azért nem lesz nagyságrendekkel jobb a helyzet. Ha a klasszikus csatornák teljesítményét egy kicsit visszavennénk, akkor szinte biztosan működhetne együtt egy kvantum csatorna a rendszerrel. Ezen kívül megfejtésre került a furcsaság a szálhosszal és a zajokkal kapcsolatban: a klasszikus csatornák forrásának széles spektrumra elkenődő zaja nagyobb lehet, mint amit a modellezésnél a különböző kutatások és így én is figyelembe vettem.

Első próbás megoldás lehet, hogy sokszor az 1550 nm körül működő DWDM rendszerekben van pár 1310 nm körüli csatorna különböző szerviz célokra, amin esetleg ki lehetne próbálni egy CVQKD-csatorna működését.

Én nem gondolnám, hogy a földi, optikai QKD-nak olyannak kell lennie, hogy egy teljesen új hálózrendszer építünk neki. Persze ha WDM-be integrált hálózatot építünk QKD-val, akkor is kellenek ellenőrzött, mindenki által bizalommal kezelt köztes csomópontok, de sokkal egyszerűbb lenne a már kiépített hálózattal együtt kezelni. Ráadásul úgy néz ki, hogy ez akár lehetséges is.

Köszönetnyilvánítás:

Elsősorban szeretném megköszönni a rengeteg segítséget konzulensemnek, Gerhátné Dr. Udvary Eszternek. Az összes egyetemi mérés során ott volt és rengeteg tanácsot és segítséget adott ezek kivitelezéséhez. Ezen kívül mindig adott tanácsokat akkor is, amikor a Matlab-os modellel akadtak gondjaim.

Szeretném még megköszönni Rétsán Dánielnek és Meskó Örsnek, akik mentoraim a Telekomnál és nagyon sok tudást adtak át a teljes szakmáról, így segítették a munkámat. Továbbá szeretném még megköszönni Liska Péternek is, aki a győri transzport labor vezetőjeként lehetővé tette és segítette az ottani mérések elvégzését, valamint Rétsán Dánielnek, aki elkísért és sok tanáccsal segítette a mérést.

A kutatás részben a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a 2022-2.1.1-NL-2022-00004 számú projekt finanszírozásában valósult meg.

Források

- [1] Emerging Trends In Ict Security 2014 (könyv)
- [2] Communication Theory of Secrecy Systemes by C. E. Shannon 1949
<https://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf>
- [3] Born rule https://en.wikipedia.org/wiki/Born_rule
- [4] Wiesner S. Conjugate coding. ACM SIGACT News. 1983
- [5] Quantum key distribution with entangled photons generated on demand by a quantum dot: <https://www.science.org/doi/10.1126/sciadv.abe6379>
- [6] Quantum Computing and the Future Internet By Tajdar Jawaid
https://www.researchgate.net/publication/359228217_Quantum_Computing_and_the_Future_Internet#pf3
- [7] Quantum Cryptography in Advanced Networks Oleg G Morozov
<https://www.intechopen.com/chapters/63116>
- [8] BB84 protokollon alapuló kulcsmegosztás
<http://tdk.bme.hu/vik/DownloadPaper/BB84-protokollon-alapulo1>
- [9] <https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/>
- [10] <https://www.idquantique.com/quantum-key-distribution-qkd-achieved-over-record-421-km/>
- [11] <https://business.blogthinkbig.com/we-apply-quantum-technology-to-real-use-cases-of-blockchain-and-iot/>
- [12] ANSSI – Technical Position Paper: QKD v2.1 Should Quantum Key Distribution be Used for Secure Communications?
<https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/#note7>
- [13] A new patent insight report 8 November 2021 Quantum technologies and space,
<https://www.epo.org/searching-for-patents/helpful-resources/patent-knowledge-news/2021/20211108b.html>
- [14] <https://www.sciencedirect.com/science/article/pii/S003040182030451X> és
<https://arxiv.org/pdf/1703.09278.pdf>
- [15] <https://www.sciencedirect.com/science/article/pii/S003040182030451X>
- [16] Research Progress Of Quantum Repeaters To cite this article: Qiao Ruihong and Meng Ying 2019 <https://iopscience.iop.org/article/10.1088/1742-6596/1237/5/052032/pdf>
- [17] Implementation of a 46-node quantum metropolitan area network Teng-Yun Chen
<https://www.nature.com/articles/s41534-021-00474-3>

- [18] <https://www.fiber-optic-components.com/differences-between-cwdm-and-dwdm-2.html>
- [19] <https://www.wwt.com/article/cwdm-or-dwdm-which-should-you-use-and-when>
- [20] Kis Zsolt: Kvantumkommunikációs kísérletek a Magyar Telekom hálózatán (belső anyag)
- [21] Quantum key distribution and 1 Gbps data encryption over a single fibre: P Eraerds, N Walenta, M Legré, N Gisin and H Zbinden ----- 2.3 fejezet
https://www.researchgate.net/publication/230939448_Quantum_key_distribution_and_1_Gbps_data_encryption_over_a_single_fibre
- [22] Feasibility of quantum key distribution through a dense wavelength division multiplexing network: Bing Qi, Wen Zhu, Li Qian and Hoi-Kwong Lo
<https://iopscience.iop.org/article/10.1088/1367-2630/12/10/103042>
- [23] Quantum limits on noise in linear amplifiers, Carlton M. Caves
<https://journals.aps.org/prd/abstract/10.1103/PhysRevD.26.1817>
- [24] <https://www.fiber-optic-components.com/differences-between-cwdm-and-dwdm-2.html>
- [25] <https://www.edinst.com/us/blog/what-is-raman-spectroscopy/>
- [26] Optical networking for quantum key distribution and quantum communications T E Chapuran <https://iopscience.iop.org/article/10.1088/1367-2630/11/10/105001>
- [27] Quantum key distribution and 1 Gbps data encryption over a single fibre P Eraerds <https://iopscience.iop.org/article/10.1088/1367-2630/12/6/063027/pdf>
- [28] Practical decoy state for quantum key distribution Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo <https://arxiv.org/abs/quant-ph/0503005>
- [29] Quantum key distribution using gaussian-modulated coherent states Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger,
<https://www.nature.com/articles/nature01289>
- [30] Experimental study on Gaussian-modulated coherent states quantum key distribution over standard telecom fiber Bing Qi, Lei-Lei Huang, Li Qian, Hoi-Kwong Lo <https://arxiv.org/abs/0709.3666>
- [31] Govind P. Agrawal, in Applications of Nonlinear Fiber Optics (Third Edition), 2021 4.2.3 Amplifier noise
<https://www.sciencedirect.com/topics/engineering/spontaneous-emission-factor>
- [32] GAIN AND NOISE FIGURE PERFORMANCE OF ERBIUM DOPED FIBER AMPLIFIERS (EDFA), A.Cem ÇOKRAK 1 Ahmet ALTUNCU 2
<https://www.electricaljournal.org/Content/files/sayilar/37/1111-1122.pdf>
- [33] Desurvire E 1994 Erbium-Doped Fiber Amplifiers (New York: Wiley)
<https://www.scribd.com/document/449087080/Desurvire-E-Erbium-doped-fiber-amplifiers-principles-and-applications-John-Wiley-Sons-Inc-2002-pdf>