MŰEGYETEM 1782
Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék

Kvantum csatorna integrálása meglévő optikai hálózatokba

TDK dolgozat

Készítette: Sóki András
Konzulens: Gerhátné Dr. Udvary Eszter

2022

Tartalomjegyzék

0. Kivonat

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 szálat 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 mellérakása esetén más-más távolságokon.

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. [3]: Ez a technológia azért nevezhető biztonságosnak, mivel a jelenlegi eszközökkel nem lehet ésszerű időn belül kikövetkeztetni a nyilvános kulcsból a titkos kulcsot. 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, [1] ha az üzenet nem hosszabb, mint a kulcs, akkor a kulcs nélkül lehetetlen megfejteni az üzenetet. Tehát a kulcs kiküldése az egyetlen gyenge pont. A nyilvános kulcsú titkosítások növekvő kockázatai miatt egyre valószínűbb a szimmetrikus kulcsú titkosítás nagyobb térnyerése.

Ahhoz, hogy egy azonos privát kulcs használatával titkosított kommunikációban a kulcsokat elküldjük a feleknek, kvantumkommunikációt használhatunk annak tulajdonképpeni 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-s bit impulzusának elküldéséhez rengeteg (több tízezres, százezres nagyságrend, 0 dBm körüli teljesítmény) fotont küldünk, addig kvantumkommunikáció esetén egy bit küldéséhez mindössze 1 fotont (egy kvantumot). Pontosítás, hogy ez csak DVQKD esetén történik meg, a gyakrabban használt CVQKD esetén egy hagyományos kommunikációnál sokkal kevesebb fotonból álló foton nyalábot küldünk. A Born törvény [2] értelmében egy kvantum (bit) egyszerre a két állapotának szuperpozíciója, vagyis egyszerre értelmezhető 1-nek és 0-nak. Amíg szuperpozícióban van, nem dönthető el, hogy mekkora valójában 1 vagy 0. Ez mindaddig igaz, amíg nem hajtunk végre mérést rajta. 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.

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”. Ugye egy kvantumbit, megfigyelés nélkül, szuperpozícióban van. Vagyis, ha 2 állapotot definiálunk a kvantum valamilyen tulajdonsága szerint, akkor egyszerre mindkét állapotot felveszi. A tétel azt fejti 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.

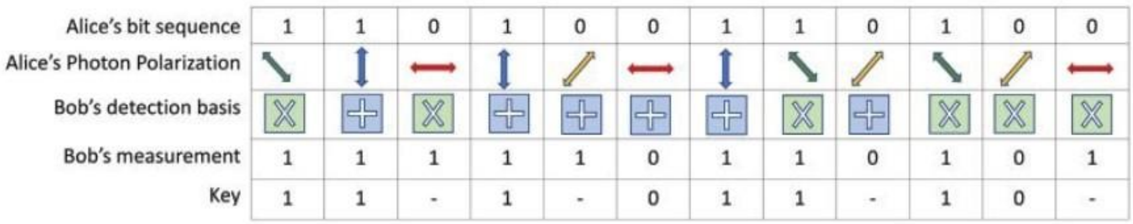
Először Stephen Wiesner [4] írta le a QKD rendszerek teoretikus működését az 1960-as években. A kétféle megoldási módjából az egyik egy olyan broadcast üzenet létrehozásáról szólt, amiben, ha valamelyik üzenetet elolvassák, akkor a többi megsemmisül (ezt kvantum multiplexelésnek nevezte).

1.1.1 BB84 protokoll:

(leírás forrásai: [7], [8], [9]) A következő nagy lépés a BB84 QKD protokoll megjelenése lett, amit 1984-ben dolgozott ki Charles Bennett és Gilles Brassard. 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. [6] Az ezt használó megoldások viszont egyelőre fejletlenebbek és ritkábban használtak. A BB84 protokoll is a prepare and measure módszerből indul ki.

A protokoll bemutatása előtt fontos még megjegyezni, hogy a kvantumos kommunikációt csak a titkos kulcs kiküldésére használják, utána a kódolt üzenet már egy klasszikus csatornán érkezik. Először tisztázzuk, hogy a kvantum milyen tulajdonságait használják fel a protokollhoz. A BB84 négy különböző polarizációs állapottal dolgozik. horizontális, vertikális, illetve ettől π/4-el eltoltak. Ezeket reprezentálhatjuk függőleges, vízszintes, valamint 45 fokban jobbra és balra ferdülő nyilakkal. A másik fontos dolog, hogy a polarizációs állapotok méréséhez két különböző bázist használunk. Ezeket reprezentálhatjuk + alakú és X alakú bázisként. Vagyis ebből adódóan az első két polarizációs állapotot, amit függőleges és vízszintes nyilakkal ábrázolunk, a + alakú bázissal lehet helyesen megmérni, a jobbra és balra 45 fokkal dőlő nyilakkal reprezentált állapotokat pedig az X alakú bázissal lehet helyesen megmérni.

Nézzük meg a mérés menetét. Kiindulásként van egy kvantumbitünk és egy bázisunk, amiben mérjük a kvantumot. Ha a kvantum polarizációja megfelel a bázishoz (vagyis a ferdék X alakúba, a vízszintesek, függőlegesek pedig + bázisba kerülnek, akkor helyes mérés lesz. (vagyis például a + bázisba egy vízszintes kerül, akkor a + bázis „meg tudja mérni”, hogy az vízszintes. Ekkor jelenthet például a vízszintes 0-át, a függőleges pedig 1-et és így kerül eldöntésre a kvantumbit állapota). A kommunikáció közben az állapotuk nem változik és megfejtük az állapotát. Ha viszont a bázis nem megfelelő, akkor 50% az eltalálási esély. Vagyis például, ha egy ferde jön a + bázisba, akkor 50% az esélye, hogy a vízszintes vagy a függőleges részbe kerül, így 50% az esélye, hogy 0-nak vagy 1-nek lesz elkönyvelve. Vagy ha vízszintes vagy függőleges irányú megy az X „alakú” bázisba, akkor 50% az esélye, hogy a bázis jobbra vagy balra dőlő részébe kerül bele. Tehát ahhoz, hogy le tudjuk mérni az állapotokat, mindenképpen tudni kell, hogy milyen bázissal mérjük. A különböző lehetőségeket és a mért eredményt a következő ábrán szemléltetem:



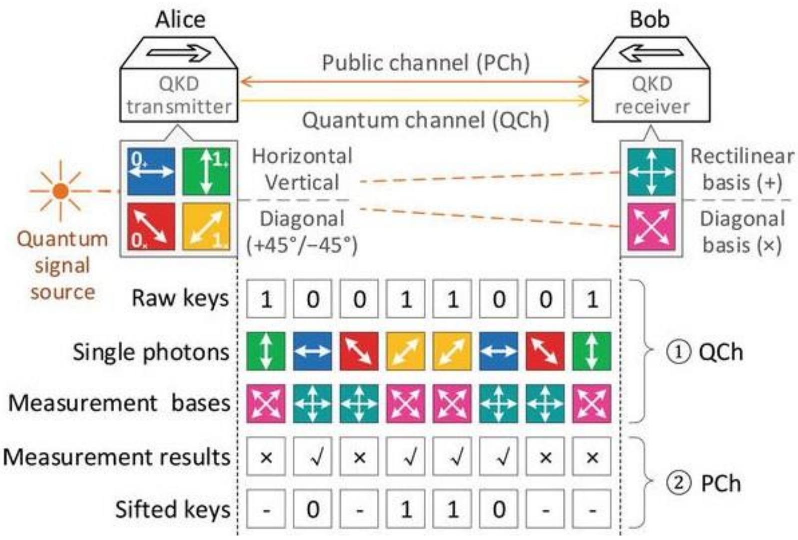
1.1 ábra: BB84 protokoll magyarázata 1

Itt Alice az adó és Bob a vevő, valamint a balra dőlő és a függőleges az 1 és a jobbra dőlő és a vízszintes reprezentálja a 0 bitet.

A protokoll két részből áll. Először küldünk kvantumokat, majd következik egy utófeldolgozás szakasz. Először Alice kiválaszt egy random 0-ákból és 1-ekből álló bitsorozatot. Ezután kiválaszt minden bithez egy random polarizáció típust, vagyis, hogy az adott 0 vagy 1 X-es típusú, vagy +-os típusú polarizációban álljon. (Ezen belül pedig adott, hogy a + és az X melyik része lesz a 0 vagy az 1). A harmadik lépésben kódolja bele a random választott 0-át vagy az 1-et a random választott polarizációba. Vagyis, hogy a + polarizáció vízszintes vagy függőleges, az X pedig jobbra vagy balra dőlő legyen. Ezután már megvannak a különböző kódolt kvantumbitek. Vagyis a jelen reprezentációban van már külön vízszintes, függőleges, jobbra és balra dőlő. Ekkor ezeket kiküldi Bobnak, a vevőnek.

Bob megkapja a kvantumbiteket, majd készít magának egy random sorozatot a 2 fajta bázisból, amikkel megméri a biteket. Mivel nem tudni, hogy Bob adott bázisa helyes-e az érkező kvantumbit méréséhez, ezért a mérésének az eredménye mindenképpen pontatlan lesz. Mindegyik kvantumhoz 50% eséllyel vagy eltalálja a bázist, vagy nem. Ha nem találja el (például X-eset használ egy vízszintes kvantum méréséhez), akkor pedig 50% az esélye, hogy a jóba teszi bele (vagyis pl. a vízszintes – ami 0, az X típusú bázis jobbra dőlőjébe kerül – ami 0).

Ezután már csak klasszikus post processing következik. Ennek az első lépése az, hogy megosztják egymással a használt bázisaikat. Vagyis elmondja Alice, hogy az adott biteket milyen bázisban (+ vagy X típusúba) küldte, és Bob is elmondja, hogy az adott biteket milyen bázisban mérte meg. Ezt egy teljesen klasszikus, akár publikusnak is mondható csatornán teszik meg, tehát ezt bárki lehallgathatja. Ez azért történhet meg, mivel azzal, hogy a bázist megtudták, még nem tudják, hogy „azon belül" 1 vagy 0 van. (vagyis, ha tudják, hogy a 3. bit bázisa + típusú, attól még lehet, hogy vízszintes 0-át, vagy függőleges 1-et küldött Alice. Ezt csak Bob fogja tudni, mivel ő mérte le, így Bob tudni fogja, hogy a 3. bithez, amit mért az jó, mivel ugyanazzal a bázissal mérte, mint amiben kapta Alice-tól. Ezután mindketten eltávolítják azokat a biteket, ahol a használt bázisuk különböző. Így mindkettőjüknek ugyanaz az 1-ekből és 0-ákból álló bitsorozatuk lesz.

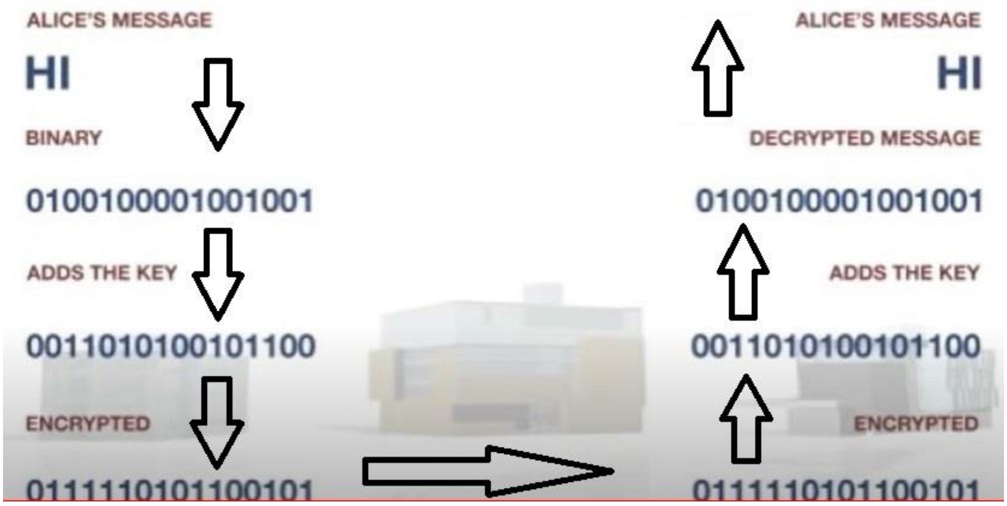


1.2 ábra: BB84 protokoll magyarázata 2

Értelemszerűen, ha egy támadó nem ismeri a használt bázisokat, akkor hiába hallgatja le/méri le a kvantum biteket, nem fogja tudni, hogy melyiket mérte jól, így nem tudja megfejteni a titkos kulcsot. Ekkor viszont felmerülhet még bennünk egy kérdés. Ha egy lehallgató (Eve-nek szokták mondani) hallgatja a kvantumos kommunikációt, eltárolja, majd regenerálja és továbbküldi ugyanazokat a biteket Bobnak, majd miután a klasszikus csatornán megtudja Alice-tól, hogy milyen bázisokat használt, akkor utólag ki tudja választani, hogy az ő mérései közül melyik volt a jó és megtudhatja a kódot. Ha Bob helyett Eve küldi el az általa használt bázisokat Alice-nak, akkor még elvileg fel sem tűnne, hogy baj van. Ezzel viszont van egy probléma. Ha a lehallgató nem küldi tovább a biteket Bobnak, akkor Bob rögtön tudja, hogy valami baj van és egy klasszikus csatornán Alice-nek küldött üzenettel leállítja a kulcsszétosztást. Ha pedig Eve továbbküld biteket, mivel azt a saját mérése után teszi, elrontja a bitrátát, amit szintén észlelhet Bob. Ezen túlmenően, ha Eve valamit továbbküld Bobnak, azt csak akkor tudja megtenni, amikor még nem tudja, hogy jó bázissal mért-e. Ha feltesszük, hogy a 3. bitet rossz bázissal méri le Eve (erre 50% esély van), akkor ezután 50% eséllyel rossz bitnek könyveli el (mondjuk 1 helyett 0-nak). Tehát összesen 25% az esélye, hogy rossz bitet küld tovább Bobnak. Miután a hosszú bitsorozatot megkapja Bob Eve-től, annak kb 25%-a hibás lesz. Így, mikor megküldik egymásnak a használt bázisokat és összehasonlítják a kulcs bitsorozatot, az eredeti Alice és a megtévesztett Bob rögtön tudják, hogy baj van (normál esetben mindkettőjük bitsorozata megegyezik). Így ugyan megtudta Eve a titkos kulcsot, viszont Alice és Bob a különböző kulcs miatt nem fogják elindítani a titkosított kommunikációt a klasszikus csatornán. Tehát titkosított adatot nem tudott lehallgatni Eve.

Ezek alapján csak akkor törhető fel a BB84 protokoll, ha valaki hozzáfér Bobhoz, vagy valaki be tud tenni úgy a hálózatba egy Eve-et, hogy leválasztja Bobot, így Eve lesz az új Bob. Ez viszont az adatforgalom fizikai megszakításával jár, ami megint észlelhető és a kommunikáció leállítható. A protokoll egyetlen gyenge pontja, ha valaki Alice-hez vagy Bobhoz hozzáfér. A jelenleg előforduló feltörési lehetőségek [12] is ezekből fakadnak.

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 visszakapja az eredeti üzenetet.



1.3 ábra: egyszerű kódolás egy közös kulccsal

A kitérőt csak azért tettem, mert ezeknek a tényeknek az ismeretében belátható, hogy a BB84 protokollú kvantumkulcs szétosztás egy nagyon biztonságos technológia, amit egyre többen ismernek fel és a használata is egyre nagyobb.

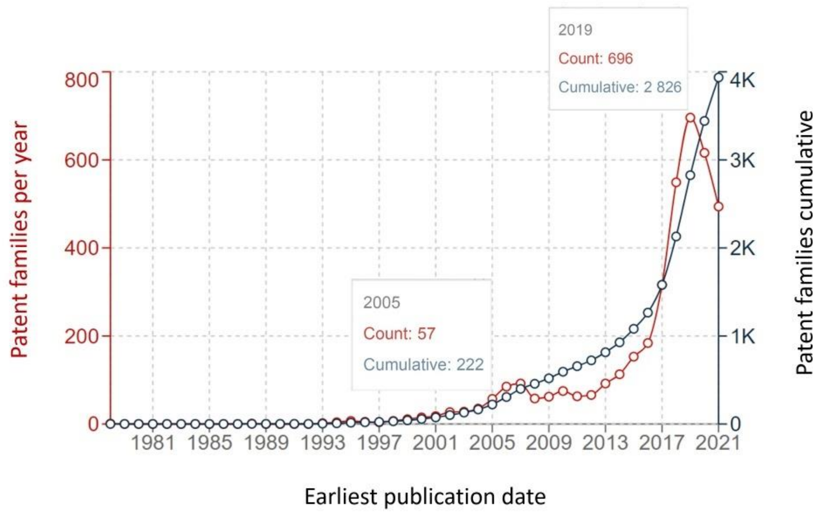
1.1.2 QKD elterjedtsége:

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 [10]. 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 vezeték nélkül 144 km, vezetékkel pedig sokáig 307 km volt, de most már 421 km-re is sikerült kulcsot megosztani [11]). A megoldást használják már bankok, kormányok, titkosszolgálatok, de már olyannal is kísérleteztek, hogy egy blockchain-en belüli titkosítást is QKD technológia segítségével oldanak meg [13].

A QKD egyben előnye és hátránya az is, hogy a legtöbb titkosítási módszerrel szemben itt külön hardverek, és a jelenlegi fejlettségében külön hálózat is kell az alkalmazásához. Ez egyrész megdrágítja (helyhasználat, eszköz vásárlás és hálózat építés) és bonyolultabbá teszi a titkosítás módját. Viszont normál titkosítások esetén hasonló technológiákat, szervereket és egyéb hardvereket használnak, amik régóta forgalomban vannak, így az újabb és teljesen más elven működő eszközök előnyt jelenthetnek. Viszont fizikai léte és fizikai rétegbeli elhelyezkedése megakadályozza abban, hogy a technológiát ott is használják, ahol csak szoftveres (vagy bármilyen, fizikai szintnél fentebb lévő szinten) valósítják csak meg a titkosítást. [14]

A további problémák főként a megoldás pont-pont jellegéből adódnak. Az elterjedést nagyban gátolja, hogy jelenleg kvantumkulcsszétosztást csak olyan sötét szálakon (dark fiber) végeznek, amik kizárólag a QKD-nak vannak dedikálva. Emiatt minden alkalmazáskor új optikai szálat 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 ábrán látható, hogy az utóbbi évtizedekben évente (count) és összességében (cumulative) hány szabadalmat adtak ki valamilyen kvantumos kommunikációval kapcsolatban: [15]. Ebből is látható, hogy a technológia felkapott, és folyamatosan egyre gyorsabb ütemben fejlődik.



1.4 ábra: statisztika QKD-val kapcsolatos szabadalmakról

1.1.3 CVQKD és DVQKD:

A kvantumkulcs szétosztásnak alapvetően két fő fajtája létezik most.

A két alapvető protokoll közül az egyik a DV-QKD (discrete variable quantum key distribution), aminél egy foton tulajdonságait, pl. a polarizációját és fázisát használják fel a kommunikációhoz. A korábban bemutatott BB84 protokoll szemléltetése tulajdonképpen ezt magyarázza el. Itt se feltétlenül minden esetben 1 db foton csinál 1 bitet, mivel az egyfotonforrás sem tökéletes, de ezen esetekben is nagyon kevés fotonról beszélünk. A másik, CVQKD (continous variable QKD) esetén nem egy darab fotonnal, hanem egy kevés fotont tartalmazó „fotoncsomaggal” kommunikálunk. Hagyományos kommunikáció esetén egy bit küldéséhez akár több millió fotont is használhatunk. CVQKD esetén ez inkább több százat vagy több ezret jelent. Ennek az az előnye, hogy a több foton miatt nagyobb távolságra eljut és a különböző zajokra sokkal kevésbé érzékeny.

A DVQKD-t mondhatjuk inkább valódi kvantumkulcsszétosztásnak, mivel ott 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 betenni egy több csatornát tartalmazó, egyébként zajos optikai szálra (vagyis WDM-re), akkor józan ésszel belátható, hogy nagyon kicsi az esélye annak, hogy a foton átjut Alice-tól 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.

A másik megoldás a CVQKD (continuous variable quantum key distribution). Ebben az esetben nem 1 fotont, hanem egy foton nyalábot használunk. Emiatt már nem a foton polarizációját használhatjuk információ kódolásra, hanem a nyaláb tulajdonságait, például amplitúdóját vagy fázisát, így rendelkezésre állnak magasabb rendű modulációk is. Általában amplitúdó vagy fázis modulációt használnak, de például egyre gyakrabban használnak Gaussian Modulation-t. [16] CVQKD esetén a biztonság nem olyan tökéletes, mint a BB84 protokollú DVQKD esetén, mivel itt a titkosságot 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 módszer. A legtöbb rendszer 1 Mbps adatsebességen dolgozik, kb 50 Hz-es ismétlési rátával és átlagosan 25 km-es távolságig jut. [17]

A megismert tulajdonságok alapján, mivel a CVQKD alkalmasabb hálózatba ültetésre, ezért a hangsúlyt a továbbiakban inkább arra fektetem.

1.2 Hálózatba integrálás lehetőségei

1.2.1 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 szálat vagy sötét szálat 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.

1.2.2 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 szétválasztás) 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 belezavar a sokkal kisebb teljesítményű kvantumos kommunikációba. WDM-et jelenleg leginkább a transzport hálózatban szoktak használni. Ez egy városok között menő akár autópályaként is reprezentálható hálózat, amin rengeteg ügyfél adata megy keresztül folyamatosan. Jelenleg akár 96 csatorna is működhet benne, valamint sok erősítő van a hálózaton. A másik nagy probléma itt jön, hiszen, ha DVQKD-t tennénk bele egy WDM hálózatba, akkor valószínűleg a rengeteg zaj szinte lehetetlenné tenné a QKD-csatorna működését. Ha CVQKD-t tennénk bele, akkor viszont az erősítés értelmetlenné tenné a kvantum csatornát, mert ott a titkosítás nagy ereje a kis fotonszámban rejlik. 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.

1.2.3 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 miatt nincs feltétlenül szükség rá. Ellenben, ha a jelenlegi megvalósításokat vesszük alapul, akkor az 50-150 km-ig működő QKD kevés lehet.

A külön QKD-nak dedikált hálózatokban (akár csak 1 csatorna, akár WDM) ha nagyobb területet akarunk lefedni, mindenképpen kellenek 50-80 km-enként köztes Bob-Alice párok, amik köztes kulcsokat generálnak. Itt a legnagyobb probléma az, hogy az összes köztes állomásnak biztonságosnak kell lennie, hiszen ezek a rendszer egyetlen gyenge pontjai. Ha egy ügyfél nem bízik a csomópontok/köztes Bob-ok fenntartójában – legyen az egy szolgáltató, egy állam, vagy mondjuk az EU – akkor az egész QKD értelmetlen. Ez ellen kivédés lehet, ha nem csak a QKD kulcs az egyetlen titkosítás az adott kommunikációban, hanem használnak még ezen felül mást (pl. egy aszimmetrikus kódolást esetleg valamilyen kvantumszámítógépes feltörés ellen hatékony algoritmussal).

1.2.4 Időosztásos, WDM nélküli külön hálózat:

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

1.2.5 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, hiszen az a No cloning theory miatt is, valamint ha lehetne, akkor is teljesen elrontaná a QKD lényegét. Sajnos a kvantum ismétlő még egy inkább elméleti és kísérleti fázisban lévő eszköz, ezért ennek a használata se lehetséges jelenleg [18]. Lehet esetleg olyan köztes Bob-okat tenni a hálózatba, amik megkapják a kulcsot, majd egy újat generálnak és azt küldik tovább a valós Bob-nak, bár erre ki kéne dolgozni egy biztonságos protokollt. Ha valamilyen köztes elem van a hálózatban (de igazából ez a hálózat összes elemére vonatkozik), akkor nagyon kell vigyázni rájuk, hiszen a QKD megoldásoknak csak Alice-nél, Bob-nál és egy esetleges köztes eszköznél van gyenge pontja.

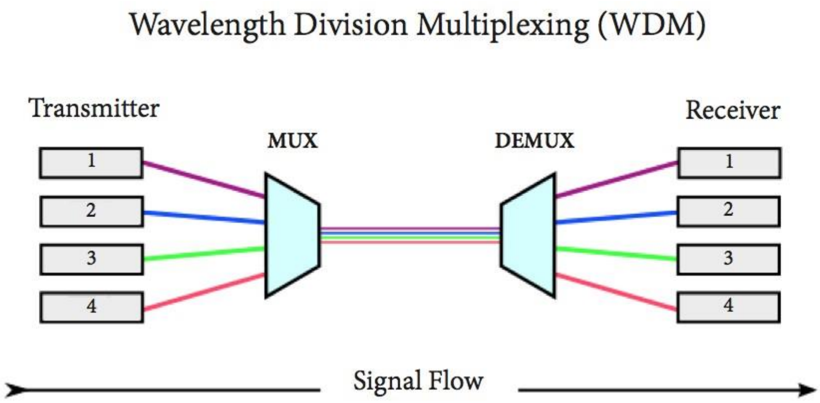
1.2.6 Általam vizsgált módszer:

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. Természetesen nem biztos, hogy a jelenlegi WDM eszközökkel lehetséges lenne és a legnagyobb problémát továbbra is a zajok és az erősítés jelenti, a dolgozatomban főként ennek a megvalósíthatóságára koncentrálok.

1.3 WDM Hálózatok bemutatása

1.3.1 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 fénnyé (multiplexált jel) alakítjuk egy multiplexer segítségével, így egyszerre tudjuk szállítani a különböző hullámhosszú fényeket majd amikor újra kellenek külön, akkor egy demultiplexer segítségével szétszedhetjük a csatornákat (a szemléltetésben újra külön színek lesznek a fehér színből).



1.5 ábra: multiplexeren és demultiplexeren alapuló egyszerű WDM sematikus rajza

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 400-800 Gbps sebességgel is működhetnek ezek. Éppen ezért, ha országos elérhetőségű QKD hálózatban gondolkodunk, akkor új hálózat építésének elkerülése esetén be kell kötni a QKD rendszereket a WDM hálózatba.

A WDM-nek is több fajtája van, de alapvetően kétféle felosztás létezik: CWDM (coarse wavelength division multiplexing) és DWDM (dense wavelength division multiplexing). Mindketten egyszerre több hullámhosszú lézerfényt használnak a jelátvitelhez egyidőben, egyetlen szálon. A csatornatávolság, az átviteli hatótáv, a modulációs lézer és a költségek szempontjából azonban a CWDM és a DWDM sok különbséget mutatnak.

1.3.2 CWDM:

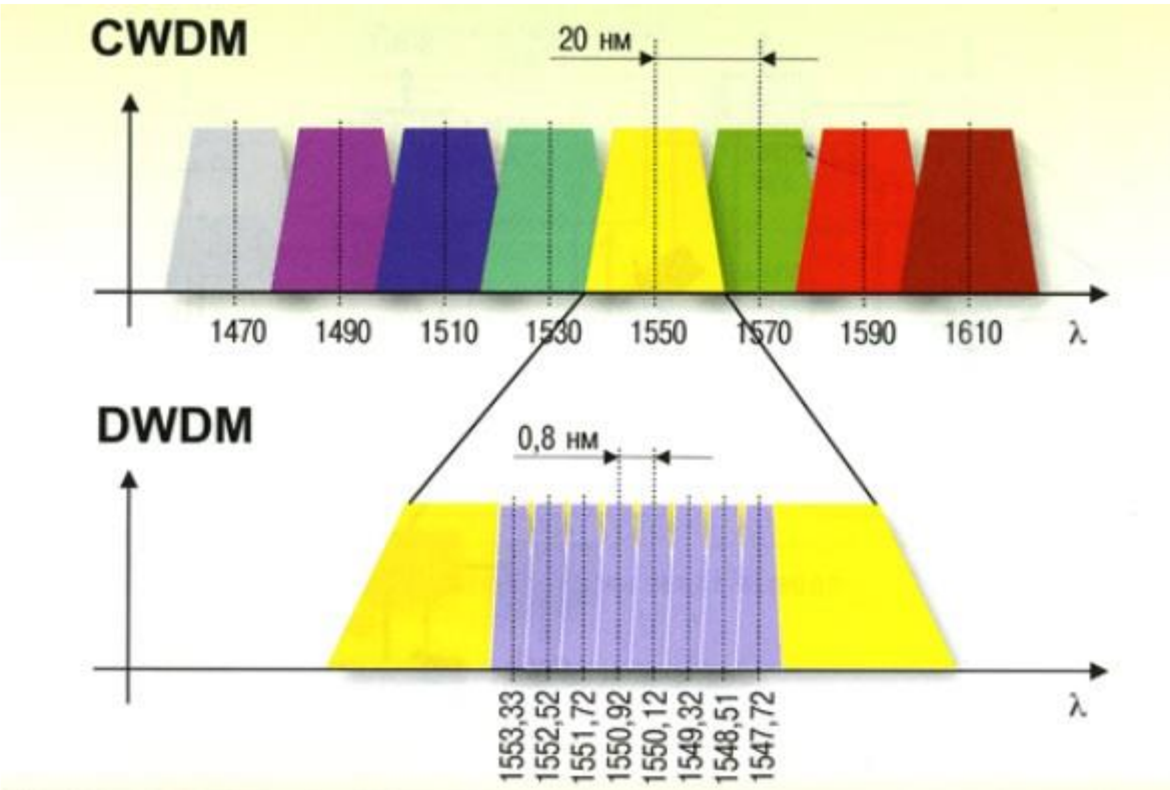
A CWDM technológiát manapság már egyre ritkábban használják és folyamatosan vezetik ki. A megoldás, fénykorában főként alacsonyabb rendű WDM hálózatokban (aggregációs vagy városi /metro) szolgált átviteli technológiaként. Az átvitel általában öt vagy hat hullámhosszon valósul meg 1270 nm és 1610 nm között, 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.

1.3.3 DWDM:

A DWDM általában 40, 80, 96 vagy 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 összességében kevesebb csillapítást szenvedjen el, így a hosszú távú - akár egy kontinensen átívelő long haul hálózatban is. 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.



1.6 CWDM és DWDM közti különbség bemutatása a spektrum, csatornatávolságok és csatornaszámok szemléltetésével

2. Egyetemi DWDM mérés

Tehát hogy be tudjunk tenni egy kvantumos csatornát egy DWDM rendszerbe az kell, hogy a különböző hullámhosszú csatornák minél kevésbé zavarják egymást. Annak megvizsgálását, hogy egy beküldött hullámhossz mennyire „hallatszódik" át, első körben egy Telekomtól leselejtezett, az MCL egyetemi laborjában található DWDM multiplexer/demultiplexer tesztelésével végeztem. A demultiplexer bemeneti oldalára kerül a multiplexált fény, a kimenete pedig a sok, különböző hullámhosszú csatorna. Az első kísérletben a cél az, hogy megtudjuk, hogyha beküldünk egy bizonyos hullámhosszú jelet a demultiplexerbe, akkor ez a jel mennyire „hallatszódik" ki a kimeneti csatornákon. Tehát pl. ha beküldünk egy 1548.7 nm-es jelet, akkor abból mekkora teljesítmény megy ki pl. az 1545 nm-es csatornán. Ideális esetben az alapzajon túl nem érzékelhetnénk jelet és ezért egy kvantumcsatorna is tehető az adott hullámhosszra. A valóságban azonban valamekkora teljesítményű jel átszivárog a többi csatorna kimenetre is, ami rossz esetben már akkora, hogy elnyomna egy QKD csatorna jelét.

2.1 Demultiplexer karakterisztikájának meghatározása egy S-LED segítségével

2.1.1 S-LED bemutatása és a spektrumának meghatározása:

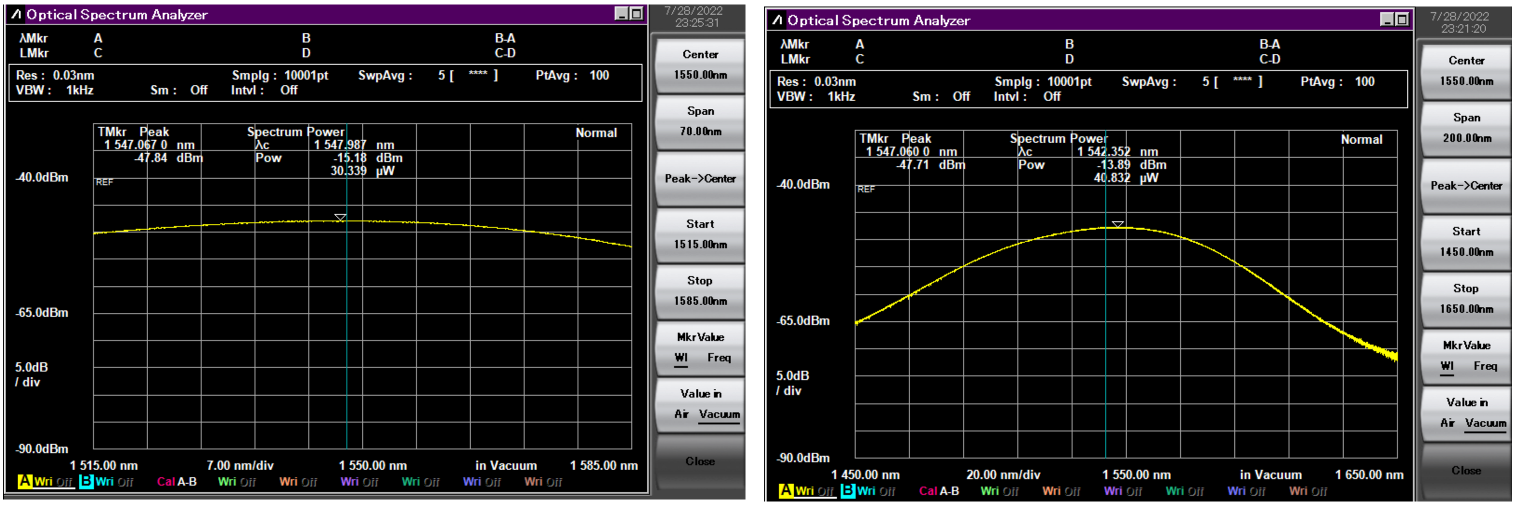
Az S-LED egy olyan fényforrás, ami egy nagyobb hullámhossz spektrumot lefedő fényt képes adni, ezért egy demultiplexerbe bekötve megnézhetjük, hogy az a nagy hullámhossz spektrumból mit enged át tehát meghatározhatjuk a demultiplexer szűrőjének átviteli karakterisztikáját. A használt S-LED egy egyetemi hallgatói munka eredménye. 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 eszköz maximum 2V-os 125 mA-es tápellátást kaphat, de a kísérlet során a biztonság kedvéért csak 100 mA-t adtunk rá. Az s-led szabályzása egy Stanford Model LDC500 lézer szabályzóval történt. A szabályzó közbeiktatása azért fontos, mivel egyrészt ezen keresztül tudjuk beállítani a megfelelő tápellátást (feszültséget vagy áramerősséget lehet megadni), valamint a benne lévő hőmérséklet tartó szabályzási kör vezérli az s-led hűtését. Hűtés nélkül nem tudnánk biztosítani az állandó hőmérsékletet, ezért a kissé változó s-led karakterisztika miatt nem kapnánk pontos eredményt se az s-led spektrumára, se a DWDM szűrő átviteli karakterisztikára.

2.1 ábra: 2.1.1 kísérlet elrendezése

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

Az eredmény a következő lett:



2.2 ábra: S-LED spektruma a spektrumanalizátoron

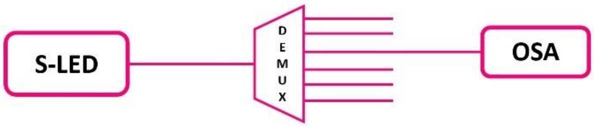
Ez alapján az S-LED 1515 nm és 1580 nm között szinte stabilan képes -15 dBm körüli jelet adni. Mivel a DWDM spektrum (ahol a csatornák vannak) a leggyakoribb esetekben [19] 1525 és 1565 nm közé esik, ezért az S-LED bőven lefedi a tartományát.

2.1.2 Demultiplexer átviteli karakterisztika mérése:

A kísérletet a következő elrendezéssel valósítottuk meg:

2.3 ábra: 2.1.2 kísérlet valós elrendezése

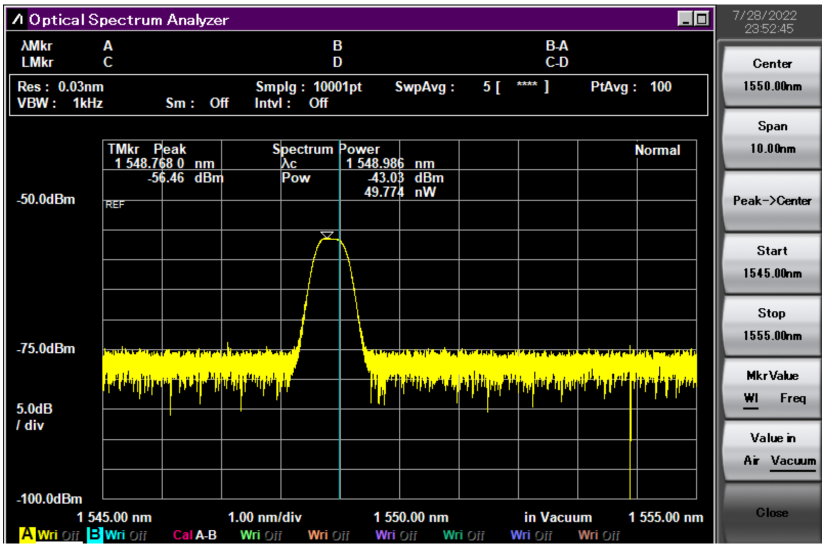
Bal oldalon található a szabályzó, ami táplálja az S-LED-et; ezután az S-LED be van kötve a 24 kiemetű DWDM demultiplexer eszköz (ONS15801) bemenetére, hátra. A demux elején egy véletlenszerűen kiválasztott kimeneti csatornára van rákötve a jobb oldalt látható spektrumanalizátor.



2.4 ábra: 2.1.2 kísérlet vázlatos elrendezése

Mivel az S-LED lefedi a teljes DWDM tartományt, ezért szűrés nélkül kb a fenti képen látható S-LED spektrum teljesítményeit látnánk a spektrumanalizátoron. Viszont mivel a demultiplexernek az a feladata, hogy a bementre kapott multiplexált fényből csak az adott hullámhosszra engedjen ki jelet (vagyis ha pl. a kimenet 1550nm-es, akkor az adott kimenet szűrője más hullámhosszú jelet elvileg nem engedhet át) , ezért ideális esetben csak egy nagyon keskeny hullámhossz sávban láthatunk jelet, ebből pedig még azt is megtudhatjuk, hogy az adott kimenet milyen hullámhosszú.

A mérés eredménye itt látható:



2.5 ábra: 2.1.2 mérés eredménye a spektrumanalizátoron

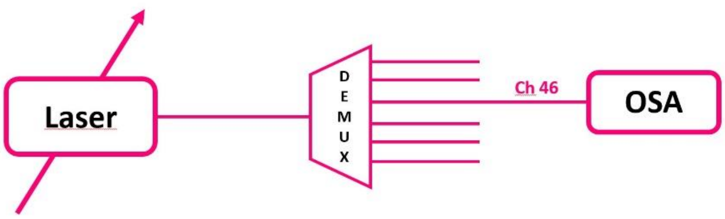
Az alsó vastag sárga a különböző forrásokból származó zaj, a kinyúlás pedig a szűrő által átengedett jel. A mérésből az olvasható ki, hogy a maximum pont 1548.7 nm-nél van, vagyis a kimeneti csatornának, amire rákötöttük a spektrumanalizátort, akkora a hullámhossza. A teljesítménye pedig -56 dBm, ami annak függvényében nem olyan rossz, hogy az S-LED teljesítménye (a karakterisztikát tartalmazó ábra alapján) -15 dBm körüli, de azért kevés. A megfigyelés tehát, hogy egyrészt -56 dBm – (15 dBm) = 41 dB az elnyomása a teljes rendszernek, másrészt pedig az adott (jelen esetben 1548.7 nm-es) csatorna körül kb 1-1 nm-es spektrumban „vágja le” a jelet. 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 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 beküldötthöz 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 kvantumos 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 kvantumos esetben egy erősebb áthallás már elnyomhatja a kvantum csatornát.

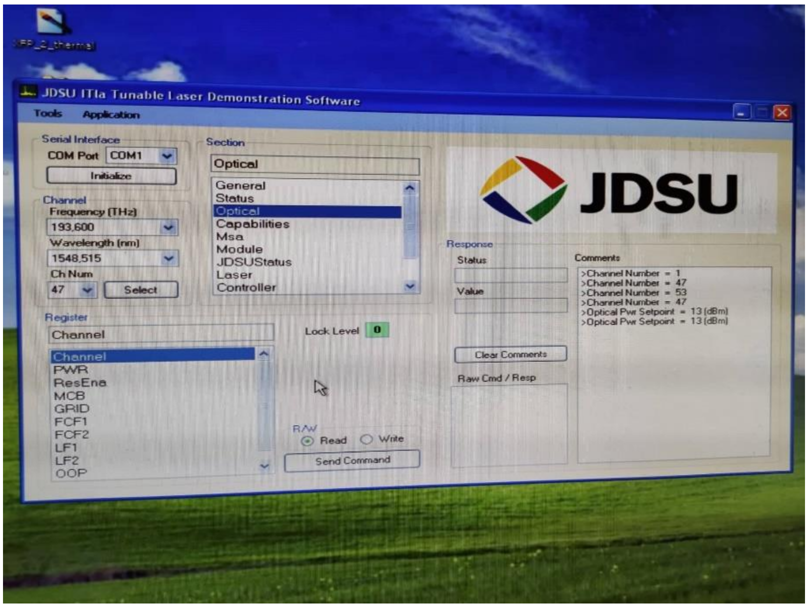
A kísérletet kétféle módon lehet elvégezni. Vagy állandó hullámhosszú fényt adunk a demultiplexer bemenetére és a spektrumanalizátort átdugjuk a különböző kimeneti csatornákba, vagy pedig a lézer hullámhosszát változtatjuk, de ugyanazt a kimeneti csatornát figyeljük a spektrumanalizátorral. Az egyszerűség és a csatlakozók kímélése miatt a második megoldást választottuk.

A méréshez egy egyetemi hallgatói munka során továbbfejlesztett változtatható hullámhosszú lézert használtunk, amit a JDSU ITIa Tunable Laser Demonstration Software-rel irányítottunk. Ez lett rákötve a demultiplexer bemenetére, amin az előzőleg is használt 1548.7 nm-es csatorna kimenetre volt rácsatlakoztatva a spektrumanalizátor.



2.6 ábra: 2.2 mérés vázlatos elrendezése

A programból kiderült, hogy az 1548.7 nm-esnek kimért kimeneti csatornához a szoftverben a 46-os számú kimeneti lehetőség van a legközelebb. (Tehát a változtatható lézert csak diszkréten lehet változtatni – DWDM szabvány értékek között – és ezek a különböző lehetőségeket számozzák.)

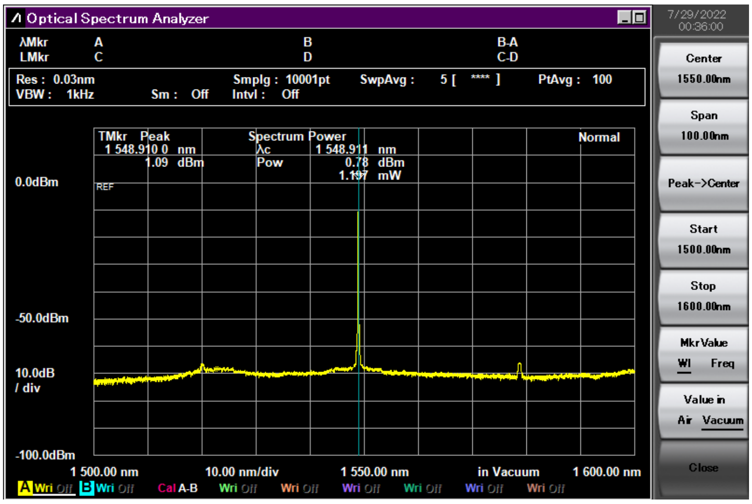


2.7 ábra: változtatható lézer számítógépes kezelőfelülete

A mérés eredménye a következő lett.

Lézer csatornája	OSA-n mért teljesítmény	Mért csúcs hullámhossza (szinte a lézer adási hullámh.)
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	nem készült kép az OSA-ról
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	nem készült kép az OSA-ról
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

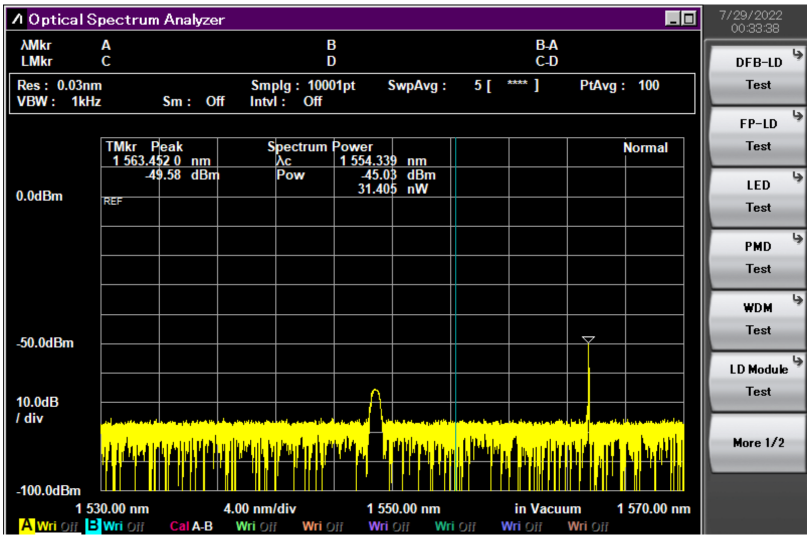
Az eredményeket úgy kell értelmezni, hogy a lézer kiadja az első oszlopban látható csatorna számú hullámhosszt a demultiplexernek. Ebből a jelből valamennyi átjut a (46-hoz legközelebbi) DWDM berendezésen 1548.7 nm-es kimenetbe. Ezt pedig az OSA-n mérjük. Értelemszerűen ott nem az 1548.7 nm-nél lesz a jel, hanem ott, amit a lézer kiadott Példaként a 46-os számú lézer kimenettel a következő jelent meg:



2.8 ábra: 2.2 mérés eredménye a spektrumanalizátoron

1548.9 nm-en ad a lézer, ott van csúcs, és mivel az 1548.7 nm-es kimeneten nézzük, ezért elég magas, 1.09 dBm lesz a teljesítménye.

Ugyanez egy távolabbi hullámhosszal így néz ki:



2.9 ábra: 2.2 második mérésének eredménye a spektrumanalizátoron

A lézeren a 10-es csatornát választjuk. Ez 1563.45 nm-es fényt ad. Hiába az 1548.7 nm-es (kb 46-os lézer csatornának megfelelő) 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 nagyon zavarna.

2.3 Eredmények összességének értékelése:

Ha a lézer változtathatóságától eltekintve újra „normális” -an gondolkodunk, vagyis, hogy valamilyen hullámhosszú fény bemegy a demultiplexerbe, és nézzük, hogy a szomszédos hullámhosszakra mennyi jut át belőle, akkor az szűrhető le a kísérletből, hogyha a megfelelő helyen 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, sőt egy kis teljesítményű kvantum csatorna beillesztéséhez túl rossz. Emiatt érdemes egy jobb minőségű, modernebb DWDM berendezéssel is kísérletet végezni.

[20] A 2022 tavaszán a Telekom, BME és a Wigner Kutatóközpont közös QKD tesztjén a saját készítésű CVQKD eszköz esetén 1550 nm-es csatornát használtak 1µs-onként küldött 1 nW teljesítményű jellel. Egyik fontos adat, hogy mivel 1 foton energiája 0.8 eV, így ebből kiszámolható, hogy egy impulzusban átlag 7793 foton van, ami nagyságrendekkel kisebb, mint a hagyományos kommunikáció esetén, így kvantumosnak tekinthető az átvitel már. A másik fontos megjegyzés, hogy az 1 nW = -60 dBm. Tekintve, hogy ha beteszünk bárhova egy csatornát az egyetemi DWDM berendezésre, akkor azt a távolabbi kimeneteken is -40 - -50 dBm körül érzékeljük, ezért ez megnehezíti a QKD csatorna rákötését.

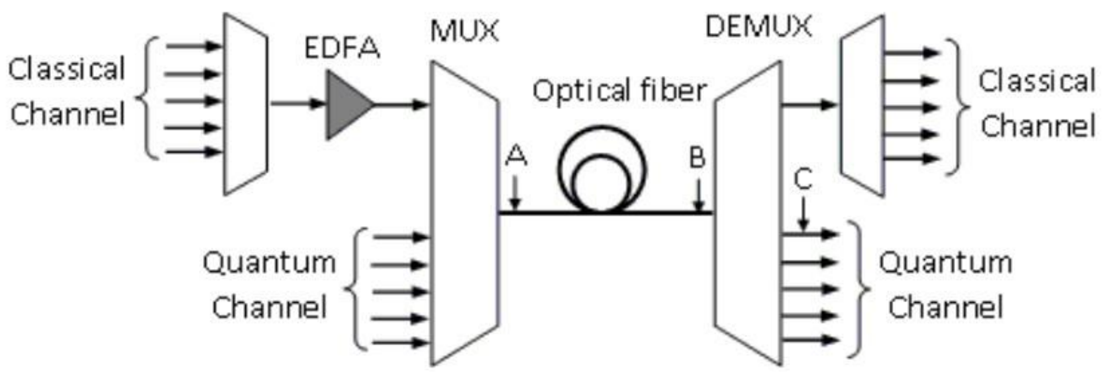
3. Felmerülő zajok vizsgálata MATLAB számításokkal

Az előbb mért csatorna áthalláson túl más problémák is felmerülhetnek egy WDM rendszerbe történő integráláskor; ezek pedig a különböző zajok. 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, sokcsatornás, magasabb rangú (QAM) modulációs 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 „szivárgás”, ami szintén zajt okozhat a kvantum csatornában. Erről szólt az előző mérés. Ezt 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, így az itt használt modellt veszem alapul. Ebben a modellben egy előre nem definiált típusú, klasszikus csatornákat is tartalmazó WDM hálózatba iktattak előre nem definiált számú kvantumos csatornát. A zajokat a hálózat elrendezése alapján a következő sorrendben fogom tárgyalni. Először figyelembe kell venni a klasszikus csatornákat erősítő erősítő zaját, majd az optikai kábel szakaszon a klasszikus csatornákból való szivárgást és a Spontán Raman szórást. A számításokat Matlab segítségével végeztem.

A használt modell ábrája itt található:



3.1 ábra: Matlab szimulációhoz használt modell rajza (forrás: [22 cikk]

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 feltétlenül a multiplexer előtt van fizikailag (sokszor van EDFA a multiplexelt - köztes részén a hálózatnak), de mivel a belőle kimenő zaj is bekerül a WDM jelbe, ezért a modellben most itt is elhelyezhet. Ezután kerülnek multiplexálásra klasszikus csatornák a kvatnum csatornákkal, bár a jelenlegi modellben csak 1 kvantum csatornát feltételeztem. Természetesen a kvantum csatornát nem kell erősíteni, mert akkor elvesztené kvantumos jellegét. Ezután következik az optikai szál. Az összes zaj fotonszáma és a kialakuló kvantumos kulcsszétosztási hatékonyság (secure key rate) is függ a szálhossztól. Mivel az általam használt modell alapján kb. 0 és 60 km között van olyan eredménye a secure key rate-nek, 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.

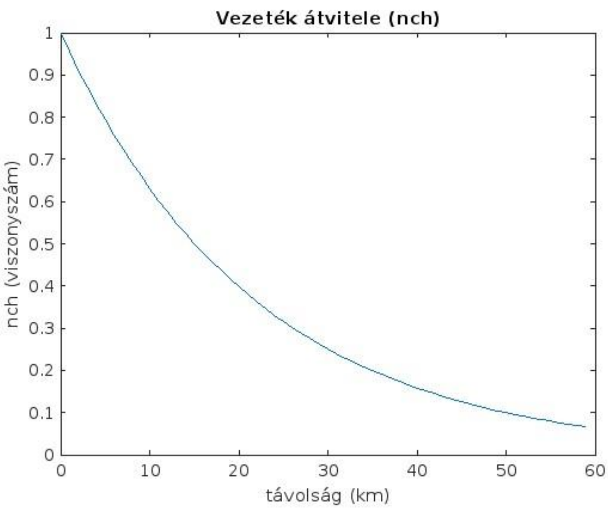
3.1 Az erősítő zaja:

Az ábrán is látható, de még egyszer felhívnám a figyelmet, hogy az erősítő csak a klasszikus csatornákat erősíti, így egy csak kvantumos WDM-ben, vagy erősítetlen klasszikus csatornák esetén nem számít.

Az erősítéshez az optikai kommunikációban megszokott EDFA-t (erbium dopped fiber amplifier) használunk. Tanulmányok is megállapították már [23], hogy sajnos nem létezhet zajmentes erősítő, valamint a legnagyobb zaj az erősítőből érkező spontán emisszió, ez ideálisan 3-4 dB környékén van. [24].

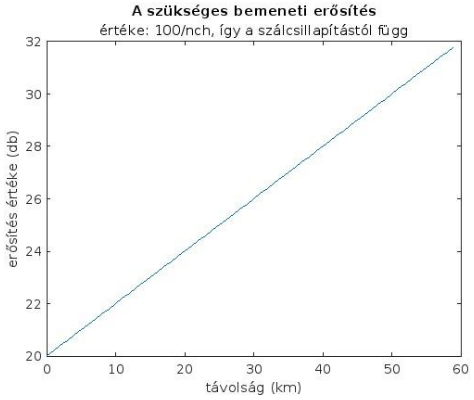
Az erősítés többfajtaképpen is értelmezhető. Egyrészt megadhatunk egy konkrét értéket, amit az erősítő bármilyen szálhossz esetén erősít. (pl 100 dB). Ezesetben minél hosszabb a szál, annál gyengébb lesz a kimeneti jel, ha ugyanazt az erősítőt használjuk. Vagy, meg lehet adni úgy is, hogy tudjuk, hogy 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 hossztól, ezért az erősítésnek is függenie kell a hossztól (hiszen ha hálózatot tervezünk akkor is úgy csináljuk, hogy a



3.2 ábra: Vezeték átvitele a távolság függvényében hossz alapján választunk erősítést.) Ha az általános 0.2 dB/km-es szálcsillapítással számolunk, akkor az optikai szálunk a következő átvitellel fog rendelkezni a hossz függvényében.

Emiatt, ha a szál túlvégén konstans értéket szeretnénk kapni, akkor a távolság függvényében a következő (decibeles) erősítéssel kell dolgozni.



3.3 ábra: Szükséges erősítés a távolság függvényében

Tehát ha azt szeretnénk, hogy az erősítés mindig 100 dB legyen, akkor G=100/nch alapján ilyen erősítéseket kell alkalmazni. Itt nch a szál átvitele.

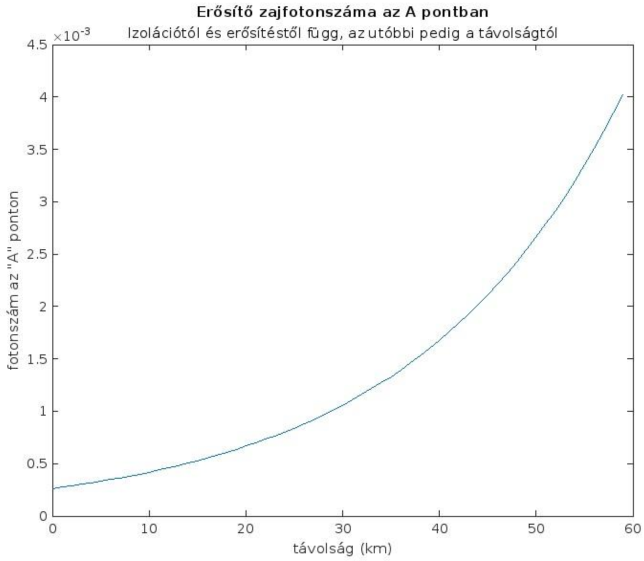
Minden erősítőnek van egy Noise Figure (NF) értéke, ami az adott erősítő zaját jellemzi; általában 5 dB körüli érték szokott lenni [25]. Ennek a segítségével számíthatjuk ki, hogy egy „spatiotemporális mode-ban” fotonszámilag mekkora zajt okoz. [26]

```
nsp= (G*NF-1)/(2*(G-1));
Nase=2*nsp*(G-1);
```

Először kiszámíthatjuk nsp-t, ami a spontán emissziós faktor. Mint látható, ennek az értéke az erősítés függvényében, valamint a noise figure segítségével kerül kiszámításra. Ebből számítható Nase (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 után:

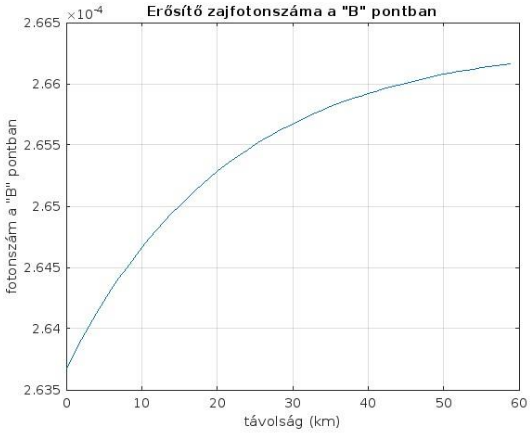
Ha azt vesszük, hogy a multiplexer izolációja xi1 = -80 dB (ami modernebbek esetén már teljesülhet), akkor az A pontban jelentkező zajfotonszám: `Nase_A = xi1*Nase` ahol xi1 már viszonyszámként szerepel.

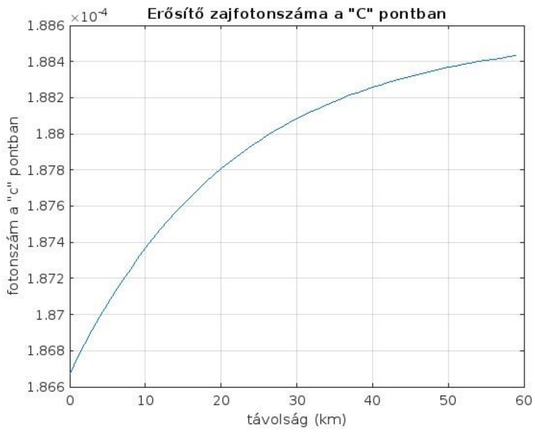


3.4 ábra: Erősítő zajfotonszáma az „A” pontban a távolság függvényében

Itt azért nő a távolság függvényében, mivel az erősítés is nő. Ezt úgy kell értelmezni, hogyha mondjuk 50 km-es szálunk lesz, akkor a nagy csillapítás miatt (az előző előtti ábráról leolvashatóan kb 30 dB) – vagyis nagy erősítés kell, ezért a nagy erősítés miatt a spontán emisszió is nagyobb lesz.

A következőkben látható, hogy B (az optikai szál végén) és C (a demultiplexer után) pontok után mekkora a zajfotonszám. A B ponton lévő fotonszámot úgy kaphatjuk meg, hogy Nase_B=Nase_A*nch, vagyis az A ponton lévő zajfotonszámot (amibe már be van véve a multiplexer izolációja) megszorozzuk a távolságfüggő szálátvitellel. A C ponton lévő zajfotonszámot pedig úgy kapjuk meg, hogy Nase_C=Nase_B*ndmu vagyis a B-nél lévő fotonszámot megszorozzuk a demultiplexer viszonyszámként értelmezett átvitelével. ndmu= -1.5 dB (a kutatás [22], ami ezt a hálózati modellt használja és elvégez hasonló számításokat, ezt használja paraméterként, de a régi egyetemi berendezés jóval nagyobb veszteséggel rendelkezett.)

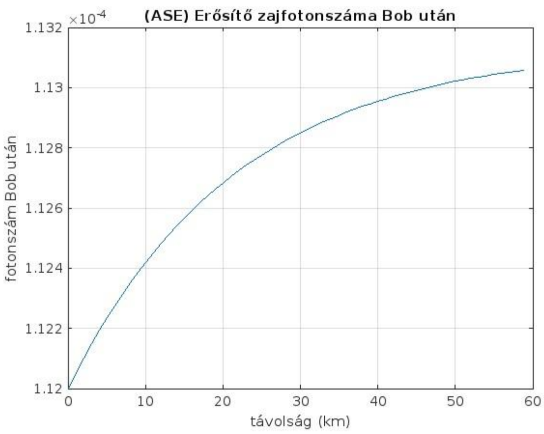




3.5 ábra: Erősítő zajfotonszáma az „B” és „C” pontban a távolság függvényében

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 a távolság függvényében. Viszont mivel itt már belejátszik a zajba a szál csillapítása (ami nagyobb távolság esetén nagyobb), ezért mégiscsak a távolság növelésével a zaj már nem fog olyan nagy mértékben nőni. Tehát ezt úgy kell értelmezni, hogy mondjuk 50 km-es hossz esetén kell 30 dB erősítés, ami az A pontban kb 10^-3 db fotonnyi zajt okoz nanoszekundumonként, de mivel átmegy az optikai szálon, ezért a B pontban a szál végén már csak 2.6*10^-4 db foton lesz, a demultiplexer után a C pontban pedig már csak 1.8*10^-4 db.

Azt is megnézhetjük, hogy ebből mennyi jut el Bobhoz. A [22]-es cikk Bob átvitelét 0.6-os paraméterrel számolta (vagyis a demultiplexertől a C pontban általa megkapott összes foton 60%-át fogja fel). Ez alapján a távolság függvényében Bobhoz a következő számú foton jut el nanoszekundumonként:



3.6 ábra: Erősítő zajfotonszáma Bob után a távolság függvényében

A Nase_A = xi1*Nase képlet alapján látható, hogy az eredmény nagyban függ a multiplexer izolációjától, mivel [22] szerint az Alice oldalán használt MUX sávszűrőként funkcionál és nagymértékben elnyomja ezt a sávon belüli ASE zajt. A 80 dB-es érték először nagynak tűnt, viszont egy hallgató társammal közösen csináltunk a laborban egy kísérletet ennek vizsgálatára. Ebben egy 8 csatornás CWDM rendszerű multi-és demultiplexereket vizsgáltunk és az eredmény meglepő lett, de kijött a 80 dB körüli izoláció. A mérést úgy végeztük, hogy a multiplexerre 1550 nm-es jelet küldtünk, majd megnéztük, hogy a multiplexer 1530 nm-es és 1570 nm-es csatornájában látunk-e bármit.

1530 nm-es kimenet:

3.7 ábra: 1530 nm-es demux kimenet a spektrumanalizátoron

1570 nm-es kimenet:

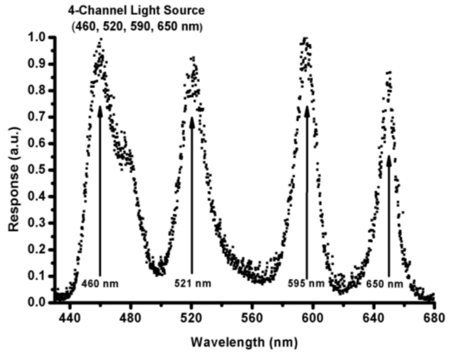
3.8 ábra: 1570 nm-es demux kimenet a spektrumanalizátoron

A leolvasott értékek alapján látható, hogy az 1550 nm-es jelet a 2 környező csatornában lecsillapította annyira, hogy a 80 dB körüli izoláció reális legyen. De ez persze CWDM (és nem DWDM rendszerre igaz, ahol a csatornák sokkal közelebb vannak egymáshoz)

DWDM esetén meg elkészült a mérés, ahol a táblázat alapján az egyetemi demultiplexer 30-50 dB izolációt tudott elérni. A modernebb eszközök képesek 80 körülire, valamint a forrásban is ez a paraméter szerepelt, ezért ezzel végeztem a számításokat.

3.2 Szivárgás a klasszikus csatornákból:

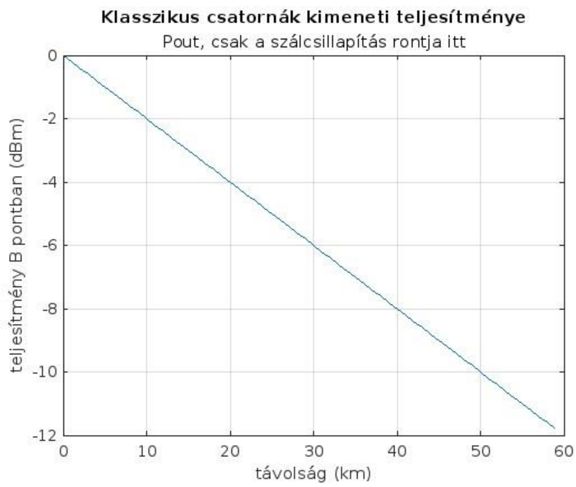
Az nyilvánvaló, hogyha van egy csatorna, akkor ugyan a különböző csatornákban alapvetően más-más hullámhosszú fotonok közlekednek, viszont a lézer tökéletlensége miatt nem csak adott hullámhosszú fotonok lesznek, hanem a spektrumon konvex haranggörbe alakban szomszédos és kevésbé szomszédos hullámhosszú fotonok is megtalálhatóak. Ha sok csatorna van egy WDM rendszerben, akkor természetesen szinte a teljes spektrumot lefedi valamekkora fotonszám. Vizualizáció kedvéért itt van egy 4 csatornás WDM spektruma: [27]



3.9 ábra: 4 csatornás WDM spektruma (forrás: [27])

A demultiplexernek az a dolga, hogy a kimeneteire csak az adott hullámhosszú külön csatornákat engedje át, viszont a tökéletlenségük miatt ez nem lehetséges teljesen. Az előző nagy szakaszban pont ezt vizsgáltuk az egyetemi DWDM demultiplexeren. Bármennyire is nagy ennek az izolációja, mindig lesznek a vevő oldalon zajfotonok.

Ahogy a klasszikus csatornákban 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 ott ahová kerülnek, zajként értelmezhetőek. Ezeknek egy nagy részét a demultiplexer ki tudja szűrni, de bármennyire is nagy ennek az izolációja, mindig lesznek a vevő oldalon zajfotonok. A számításukhoz először is figyelembe kell venni a klasszikus csatornák kimeneti teljesítményét (demultiplexer utáni). 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 egy állandó 0 dBm-es érték a távolság függvényében. A valóságban is gyakori a 0 dBm közeli teljesítmény. [18] Ha úgy vesszük, hogy az erősítés egy minden távolság esetén állandó érték, akkor a távolság függvényében folyamatosan csökkenni fog a kimeneti teljesítmény. A következő ábra azt mutatja, hogy a kezdetben 0 dBm-es jel teljesítménye hogyan csökken.



3.10 ábra: klasszikus csatornák kimeneti teljesítménye a távolság függvényében

Ez tulajdonképpen csupán a klasszikus csatornák teljesítménye a „B" pontban, vagyis az optikai szál végén. Mindössze a szál csillapítása hat rá, a multiplexer által okozott kis veszteséget most hanyagoljuk el. (itt azért lesz lineáris a szál átviteles grafikonnal ellentétben, mivel nem viszonyszámban, hanem decibelben jelenítek meg.)

A másik esetben az erősítés minden szálhossz esetén 0 dBm kimeneti teljesítményt biztosít, vagyis egy konstans 0 dBm teljesítményű ábrát láthatnánk.

Ezután számíthatjuk ki a zajt. Az, hogy a klasszikus csatornákból mennyi szivárgást 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*f), akkor megkaphatjuk, hogy ez hány fotont jelent. Mivel egy időablakban nézzük, ezért ábrázoláskor meg kell szorozni az 1 ns-os időablakkal.

P_{LEAK}_C=xi2.*P_{OUT};

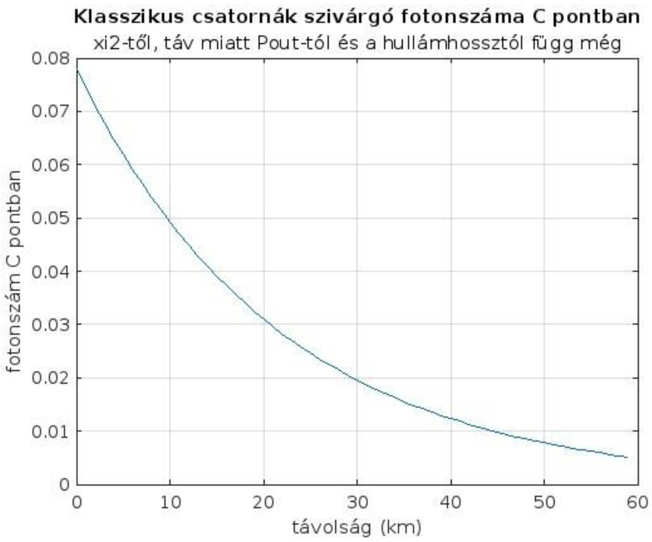
(C pontra jutó zajteljesítmény a tárgyalt zajból - ahol xi2 a demultiplexer izolációja, Pout a demultiplexert érő klasszikus csatorna teljesítmény (1 csatorna teljesítménye),

Ez alapján kiszámítható a zajfotonszám

f=c/$\lambda_{klasszik}$;
N_{LEAK}_C=P_{LEAK}_C./(h*f);

Itt lambda_klasszik 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 Pout (demuxra jutó klasszikus csatorna teljesítmény) függni fog a távolságtól, (a felső ábra alapján, minél nagyobb a távolság, annál kisebb Pout), akkor eredmény a távolság függvényében a következő grafikonon látható:



3.11 ábra: klasszikus csatornák szivárgása változó kimeneti teljesítmény esetén, C pontnál, a távolság függvényében

Ebben az esetben, ha az erősítés állandó így a kimeneti teljesítmény a távolság függvényében csökken, akkor a klasszikus csatornák szivárgó fotonszáma 0.08-0 között van. Mivel folyamatosan csökken a teljes kimenet teljesítménye, ezért a kimenő zaj is csökkenni fog.

A másik esetben ismert előre 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.

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

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

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 ez sem meghatározó zaj, az összes zaj számításánál és a secure key rate számításánál mindkét módszer esetén szinte teljesen azonos eredmény jön ki.

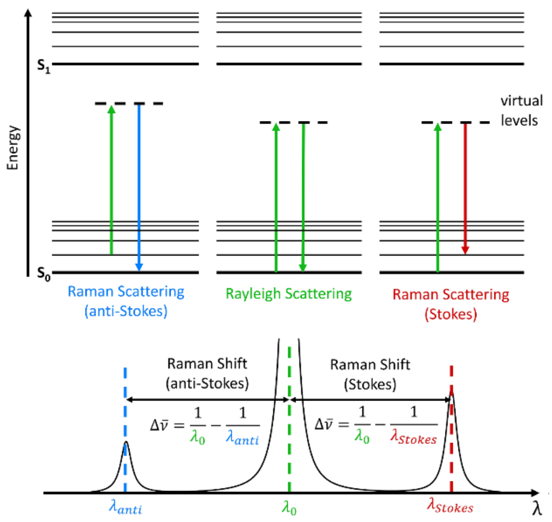
3.3 Raman szórás:

3.3.1 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. Itt az anyag a fényt vezető üvegszál. Ha a szétszóródó fotonnak ugyanaz marad a hullámhossza, mint a beesőnek, akkor ezt Rayleigh scattering-nek hívjuk, ha nem egyezik meg, akkor beszélünk Raman scattering-ről. Ezesetben a következő események történnek. A bejövő foton $E=h*f_{be}$ energiát adhat át az anyag egyik elektronjának, amitől az egy magasabb energiaszintre kerül (ezt virtuális energiaszintnek nevezik). Ezután az elektron energiát veszt és visszaesik egy (lehet, hogy az eredetitől eltérő) energiaszintre. A leadott energia legyen $h*f_{ki}$. Ha az eredeti fotonnal megegyező h*f_be-nyi energiát [18] vesztett, akkor $h* f_{be} =h* f_{ki}$, amiből következik, hogy $f_{be} =f_k$, tehát az energiavesztés közben az eredeti fotonnal megegyező (frekvenciájú és) hullámhosszú 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. Ez azt eredményezi, hogy az energialeadás során kiadott fotonnak más energiája lesz, mint a bejövőnek, vagyis $h* f_{be}!= h* f_{ki}$ ---> $f_{be}!= f_{ki}$, tehát más hullámhosszú foton fog kijönni az anyagból. Ez a Raman szórás. Ha az anyagból kijövő fotonnak kisebb a frekvenciája (nagyobb a hullámhossza), mint a bejövő fotonnak, akkor ezt Stokes Raman szórásnak hívjuk, ha pedig a kijövő fotonnak nagyobb a frekvenciája (kisebb a hullámhossza), mint a bejövő fotonnak, akkor pedig antistokes Raman szórásnak hívjuk. Stokes esetén az elektron energiát nyel el, anti-stokes esetén, pedig energiát veszít el. Mivel az üvegszálban folyamatosan találkoznak az üveg kristályszerkezetével a fotonok, ezért folyamatosan történik valamilyen szórás folyamat. Ezért minél távolabb vagyunk a forrástól, annál több olyan foton lesz, ami elkerül a saját hullámhosszáról és egy másik hullámhosszú csatornát szennyez. Mivel itt kis energiákat nyelnek el vagy veszítenek az elektronok egy fotonnal való találkozás során, ezért csak kis hullámhossz távolságokra kerülnek el a fotonok. Vagyis a Raman szórás szennyezését a kvantum csatornára csökkenthetjük úgy, hogy egyszerűen a hagyományos sávoktól távolabbi hullámhosszra tesszük a kvantum csatornát.

A szemléltetés kedvéért itt egy ábra a folyamatról.



3.13 ábra: Raman szórás szemléltető ábra (forrás: link)

3.3.2 A szórás számítása:

A Matlabos számításokat [22] mellett a következő két cikk Raman szórás számítási módszerei alapján készítettem el: [28], [29]

A számítást úgy kezdem, hogy a spontán anti-stokes Raman szórás teljesítményét számítom ki a következő képlettel: $\mathbf{P_{SASRS} = P_{in}*\beta*r*\eta_{ch}*d\lambda = P_{out}*\beta*r*d\lambda}$. Ezt a képletet a [29] cikk készítette egy jóval bonyolultabb, kétváltozós deriváltfüggvény egyszerűsítésével.

Itt P_{out} a klasszikus csatornák lézerének kimeneti teljesítménye wattban, jelen esetben (nem wattos formában) 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 a szóródni, így annál nagyobb lesz a Raman szórás teljesítménye. Ez a képletben az egyetlen változó.

A β a spontán Raman szórás együtthatója. Értéke $4*10^{-9}$ (km nm) $^{-1}$. Az együttható láthatóan távolságfüggő, viszont az erre vonatkozó [22] cikk kísérlete alapján 40 km-en, legrosszabb körülmények között lett $4*10^{-9}$, így egyszerűsítésként lehet használni ezt az értéket. Mivel nagyon kis szorzóról van szó, ezért változtatása vagy távolságfüggővé tétele nem befolyásolná jelentősen az eredményt.

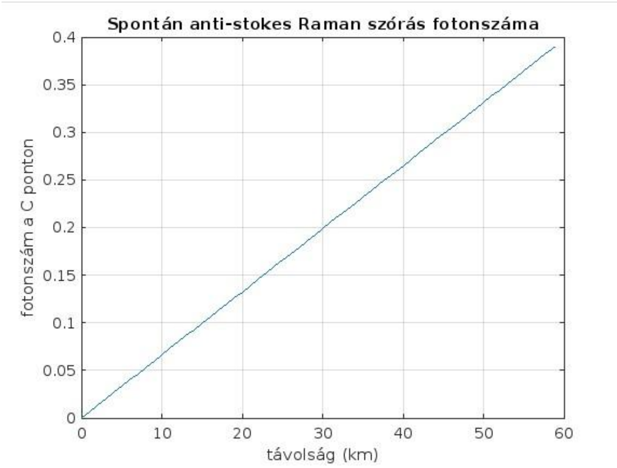
dλ = c/df, ahol df a klasszikus csatornák/csatorna sávszélessége frekvenciában, így dλ lesz a sávszélesség hullámhosszban. A számításhoz értékül [22] cikk df=75 GHz-es sávszélességet választott, amit én is jónak találtam, mivel ez a csatorna szélesség manapság is gyakran előfordul WDM rendszerek esetén. A többi népszerű 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) miatt a 75 GHz egy jó átlagértéknek is tekinthető.

Ezután a teljesítményből fotonszámot kell készíteni, amihez [29] megoldását használom.

$$N_{SASRS} = ((P_{SASRS} * \lambda) / (h*c)) * \eta*dt.$$

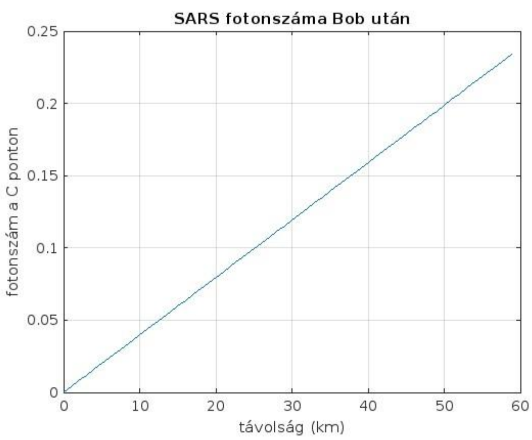
Itt λ a klasszikus csatorna hullámhossza, vagy több csatorna esetén közép hullámhossza. A DWDM megoldások során leggyakrabban használt 1550 nm-es hullámhosszt választottam ide. „h” a Planck állandó, illetve „c” a fénysebesség, amik a teljesítményből fotonszám számításhoz kellenek. Ezután a kapott fotonszám még megszorzásra kerül η-nel, ami a képletben egy konstans arra vonatkozóan, hogy a zaj mekkora részét érzékeljük. [29] 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. [22] cikk és én is először ennek a helyére a demultiplexer hatékonyságát helyezem (-1.5 dB veszteség), mivel az optikai szálban létrejött szórt fotonok a szál végén először a rendszer következő elemével, a kvantumos csatorná(kat) és a klasszikus csatornákat szétválasztó demultiplexerrel találkozik. Ezen kívül meg kell még szorozni dt-vel (1 ns), mint az összes többi zajt, hogy egy és ugyanazon időablakban láthassuk a zaj fotonszámát.

Az eredmény a távolság függvényében a következő:



3.14 ábra: Raman szórás fotonszáma a távolság függvényében

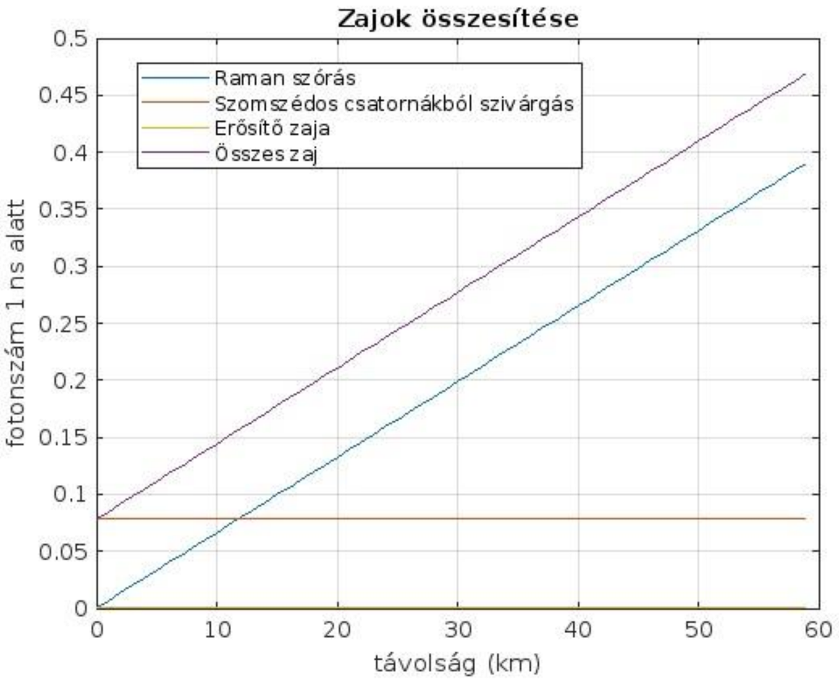
Ezután megnézhetjük, hogy ebből mennyi jut el Bob-hoz. Ehhez annyit kell még tenni, hogy a fotonszámot megszorozzuk Bob „átvitelével”, amit rosszabb esethez igazítva 0.6-nak veszünk.



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

3.4 Zajok összesítése és értékelésük:

Ha egy időablakban nézzük a kiszámított zajokat, akkor a következő grafikont láthatjuk:



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

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

3.5 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 másikban homodin detektorral CVQKD-t használunk. Természetesen a két modell eredményei eléggé el fognak térni, hiszen míg az egyfoton detektor minden zajfotont érzékel, ha az ő érzékelési tartományának megfelelő spektrumban van és hiheti „QKD fotonnak", addig a homodin detektor, mivel a fotonnyaláb tulajdonságait nézi, ezért kevésbé érzékeny a zajfotonokra.

3.5.1 Modell DVQKD kulcsráta számításra:

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

Az egyfoton detektort a gyakran használt InGaAs (indium gallium arsenide) fotodiódával megvalósítottnak képzeljük. Ennek lesz egy érzékelési ablaka, ami abból áll, hogy mekkora frekvenciaspektrumon érzékel és mennyi ideig van nyitva, vagyis meddig érzékel. Ez a kódban paraméteresen állítható, de alapból, ahogy a cikk is, az ablakot 75 GHz-esnek vettem (ez egyébként az 50 és 100 GHz mellett egy gyakran használt WDM-csatorna szélesség), az időt pedig 1 ns-umnak vettem (mivel a zajszámítások is ekkora időablakban történtek, így az ottani eredmények ide is konvertálhatóak).

$\mathbf{N_{Mod}=df*dt}$ ahol df= 75 GHz és dt= 1ns

Ezután ki kell számolni az egyfoton detektor egy ablakában érkező zajfotonok számát.

Nspd_C= N_{Mod}*η_{ch}*η_{dmu}*N_{ASE}_A + N_{leak}_C*dt + N_{Mod} *Nsars_C

- Nspd_C: az elrendezés C pontjánál (demux után, Bob előtt) lévő zajfotonok száma (spd: single photon detector)

Az egyenlet első része az erősítő zajáról szól: (csak a klasszikus csatornát erősíti, de a zaja közbejátszik az egész spektrumon)

- **N_{Mod}** : az 1 ns-os, 75 GHz-es ablak
- **η_{ch}**: optikai szál átvitele (távolság függvényében változó érték, 0.2 dB/km csillapítással számolva)
- **η_{dmu}**: demultiplexer átvitele (-1.5 dB csillapítással számolva alapból 0.7079 értékű)
- **N_{ASE}_A**: erősítő zaja az A pontban, 3.1-ben lett kiszámítva

A második rész a klasszikus csatornákból történő szivárgást hozza be

- **N_{LEAK}_C**: ebből származó fotonszám a C pontban (3.2-ben számolva). A konstansnak számított, egyszerűsített szivárgás verziót használom
- **dt**: csak az 1 ns-os ablakot kell behozni, mivel Nleak számításánál már figyelembe vesszük a frekvenciát

A harmadik rész a Raman szórást veszi figyelembe

- **N_{SARS}_C**: a C pontban lévő fotonszám.

Ezután [31] cikk által készített módszerrel lehet a C pontnál lévő zajfotonszám alapján kiszámítani a kulcsgenerálási sebességet. Ehhez a következő képletrendszerre lesz szükség:

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

R fogja jelenteni a sebesség értéket, vagyis a generált kulcsok számát 1 másodperc alatt. A kiszámításához szükséges elemek képletei a következők:

$$Y_0 = Y_0^0 + \eta_{\mathrm{Bob}}\langle N_{\mathrm{SPD}}^{\mathrm{tot}}\rangle.$$
$$Q_\mu = Y_0 + 1 - \mathrm{e}^{-\eta\mu},$$
$$E_\mu = [e_0 Y_0 + e_{\mathrm{det}}(1 - \mathrm{e}^{-\eta\mu})]/Q_\mu,$$
$$Q_1 = (Y_0 + \eta)\mu \mathrm{e}^{-\mu},$$
$$e_1 = (e_0 Y_0 + e_{\mathrm{det}}\eta)\mu \mathrm{e}^{-\mu}/Q_1.$$

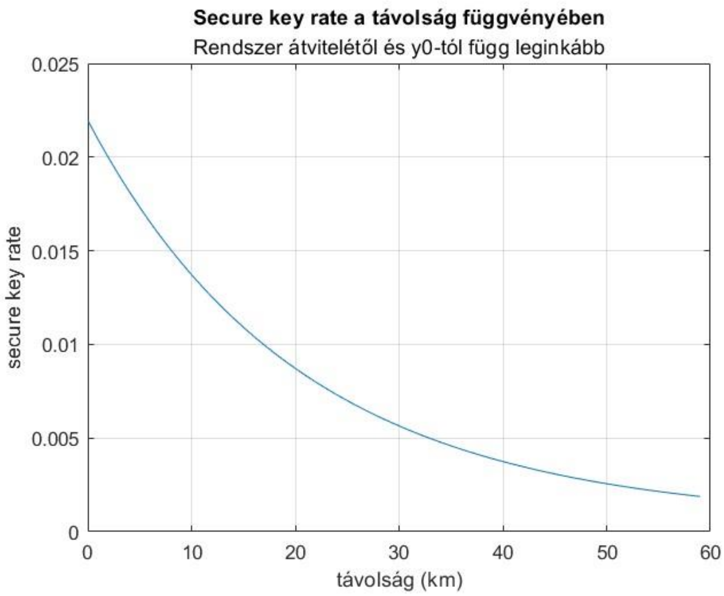
Jelentésük:

- **Y_0**: rossz észlelések száma (amikor a fotodióda zajfotont kap információt tartalmazó foton helyett). Ezt a rajzon Bob pontján kell értelmezni.
- **Y_00**: rendszer egyéb háttérzaja, cikk alapján 5*10^-6 fotonszámnyi értékkel
- **ηbob**: Bob átvitele ([22] cikk 0.6-nak vette, ami az ideálistól messze van, így szerintem megfelelő lesz
- **N_{SPD}_C**: előbb kiszámolt, C pontban lévő fotonszám (azért kell megszorozni Bob átvitelével, mert nem engedi át teljes egészét)
- **n**: (a Q_mű képleténél jelenik meg először) a teljes rendszer átvitele, vagyis n=nch*ndmu*nbob
- **µ**: egy paraméter, értéke 0.5. DVQKD megvalósítási módonként eltérhet, de BB84 protokoll esetén azért lesz ½, mivel a fotonok polarizációja az esetek felében nem egyezik a detektor

bázis polarizációjával (ez részletesebben szerepelt 1.1.1 -ben) 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 a forrás 0.003 valószínűséget adott)
- **Q_μ**: a jelállapotok erősítése/nyeresége-ként hivatkoznak rá, akként nevezik. Ha megnézzük a képletet, az exponenciális tagban szereplő átvitel a távolság függvényében csökken, míg mű állandó marad, így az exponenciális tag is csökken. Matlabban látható, hogy ez a „nyereség” a távolság függvényében csökken, értéke 0.2 és 0.064 között van (60 km-ig elmenve)
- **E_μ** ez lesz a kvantumbit hiba ráta
- **Q_1** és **e_1** olyan tagok, amiket a könnyebb kiszámíthatóság érdekében vezették be.
- Az R képletében található függvényeket inkább nem vezetném le írásosan, a [31] cikkben megtalálhatóak.

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 a következőképpen néz ki:



3.17 ábra: Kulcsráta DVQKD esetén a távolság függvényében

Az oka az, hogy egyszerűen a klasszikus csatornákból származó szivárgás 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 még ha zajt is teszünk hozzá, akkor hihetetlenül le fog lassulni a kulcsmegosztási folyamat.

A megoldás irányába vihet minket, ha minél rövidebb időablakos egyfoton detektort használunk és jobban összeszinkronizáljuk Alice-t és Bobot. Sajnos esélytelen, hogy foton megjövetelenkénti gyorsasággal nyitogassuk a detektort, így azért mindenképpen lesz zaj 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, kicsit eltérő hullámhosszú zajfotont ki tudunk zárni.

Utolsó módszer, hogy inkább CVQKD felé fordulunk, ha WDM hálózatba szeretnénk integrálni QKD-t.

3.5.2 Modell CVQKD kulcsráta számításra

Ahogy már korábban tárgyaltam, ezesetben 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 kulcsráta itt egy kicsit mást jelent. Mivel a kommunikáció sebessége a pulzusok gyorsaságától függ, (ami hagyományos technológiával történik kiadásra, csupán jóval kisebb fotonszámmal), valamint egy pulzus nem feltétlenül egy bitet fog takarni, ezért a sokszor inkább a pulzusonként létrejövő kulcsokat adják meg kulcsrátának. A [22]-es, a számítási modellekhez alapul vett cikk a [32] és [33] modelleket javasolta, amik leírnak egy Gauss moduláción alapuló, fordított egyeztetésen („reverse reconciliation") alapuló CVQKD protokollt és a kulcsráta számítási módjukat. Ezek segítségével készítettem el saját számításaim. Itt a számítás sokkal bonyolultabb, mint előző esetben, nem is szeretnék mindent teljesen levezetni. Azért, hogy több klasszikus csatorna esetére is megmutathassak eredményeket, a Matlabban minden számítást külön függvénnyel végzek.

Magát a kulcsrátát a következő képlet adja:

$$\Delta I = \gamma I_{AB} - \chi_{BE},$$

Itt gamma a fordított egyeztetés algoritmusának hatékonysága (0.9-nek választva), a másik két elemet, pedig külön kell számolni: (kép forrása: [22], részletesebben levezetve: [33])

$$I_{AB} = \frac{1}{2}\log_2[(V+\chi_{\mathrm{tot}})/(1+\chi_{\mathrm{tot}})], \tag{22}$$

$$\chi_{BE} = \Theta\left(\frac{\sigma_1-1}{2}\right) + \Theta\left(\frac{\sigma_2-1}{2}\right) - \Theta\left(\frac{\sigma_3-1}{2}\right) - \Theta\left(\frac{\sigma_4-1}{2}\right) \tag{23}$$

with $\Theta(x) = (x+1)\log_2(x+1) - x\log_2 x$; $\chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + \chi_{\mathrm{hom}}/\eta_{\mathrm{ch}}$; $\chi_{\mathrm{line}} = 1/\eta_{\mathrm{ch}} - 1 + \epsilon$; $\chi_{\mathrm{hom}} = (1+\upsilon_{\mathrm{el}})/\eta' - 1$; $\sigma_{1,2}^2 = \frac{1}{2}(A \pm \sqrt{A^2-4B})$; $\sigma_{3,4}^2 = \frac{1}{2}(C \pm \sqrt{C^2-4D})$; $A = V^2(1-2\eta_{\mathrm{ch}}) + 2\eta_{\mathrm{ch}} + \eta_{\mathrm{ch}}^2(V+\chi_{\mathrm{line}})^2$; $B = \eta_{\mathrm{ch}}^2(V\chi_{\mathrm{line}}+1)^2$; $C = \frac{V\sqrt{B}+\eta_{\mathrm{ch}}(V+\chi_{\mathrm{line}})+A\chi_{\mathrm{hom}}}{\eta_{\mathrm{ch}}(V+\chi_{\mathrm{tot}})}$; $D = \sqrt{B}\frac{V+\sqrt{B}\chi_{\mathrm{hom}}}{\eta_{\mathrm{ch}}(V+\chi_{\mathrm{tot}})}$. Here, $V = V_A + 1$ is the quadrature variance of the coherent state prepared by Alice. $\eta' = \eta_{\mathrm{DMU}}\eta_{\mathrm{Bob}}$ is the equivalent efficiency of Bob's system. ϵ denotes noise contribution from outside of Bob's system, which can be further separated into two terms:

$$\epsilon = \epsilon_0 + \frac{\varepsilon_{\mathrm{in}}}{\eta_{\mathrm{ch}}\eta_{\mathrm{DMU}}\eta_{\mathrm{Bob}}}. \tag{24}$$

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 többit elnyomja. Emiatt lesznek „matched" (amit én most csatoltnak fordítok) és „unmatched" (csatolatlannak fordítva) 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.

3.5.2 /1 Csatolt módú zaj:
Először nézzük meg a csatolt módú fotonok számát, hiszen ez játssza a valódi szerepet a Bobot érő zajban:

$$\langle N^{\text{in}}_{\text{GMCS}} \rangle = \tfrac{1}{2} m (\eta_{\text{ch}} \eta_{\text{DMU}} \langle N^{(A)}_{\text{ASE}} \rangle + \langle N^{(C)}_{\text{SASRS}} \rangle).$$

Itt az ½ arra szolgál, mert azt feltételezzük, hogy a helyi oszcillátor (továbbiakban: LO – mint local oscillator) kiválasztja magának valamelyik polarizációt és csak az abban lévő fotonokat érzékeli. „m” a klasszikus csatornák száma. Ezután a csatornaszámmal szorzódik a zajok összege, pontosabban az erősítő zaja a C ponton (ezért kell az átviteli adatokkal szorozni), valamint a Raman szórás. A cikkek úgy veszik, hogy az átszivárgó zaj egésze a nem csatolt zajba kerül.

Mind az erősítő általi zaj, mind a Raman szórás modellezhető kaotikus forrással rendelkező Bose-Einsten fotonstatisztikával. Vagyis ezzel szimbolizálhatjuk az „elkenődésüket” a spektrumon.

$$(\Delta X)^2 = (\Delta Y)^2 = 2\langle n \rangle + 1.$$

Ebből számolható a Bobot elérő csatolt módú fotonok száma a következő képlettel:

$$\varepsilon_{\text{in}} = 2\eta_{\text{Bob}} \langle N^{\text{in}}_{\text{GMCS}} \rangle.$$

Ez az eredmény már konkrétan felhasználható a fentebb lévő egyenletrendszerbe

3.5.2 /2 Csatolatlan módú zaj:
Ennek kiszámítása nem elsődleges a kulcsráta kiszámításához, viszont érdekesség képpen röviden bemutatom a levezetését. Talán azért érdemes ennyit foglalkozni vele, hogy látni lehessen, hogy milyen zajt tud kizárni egy homodin detektor.

$$\Delta T = \frac{1}{2\pi \Delta f}$$

ahol df az LO frekvenciája

$$\langle N^{\text{out}}_{\text{GMCS}} \rangle = \frac{\Delta T}{\Delta t} \langle N^{\text{tot}}_{\text{SPD}} \rangle.$$

Ahol N_SPD az a fotonszám, ami kiszámításra került az egyfoton detektoros megoldás esetén, dt pedig az időablak.

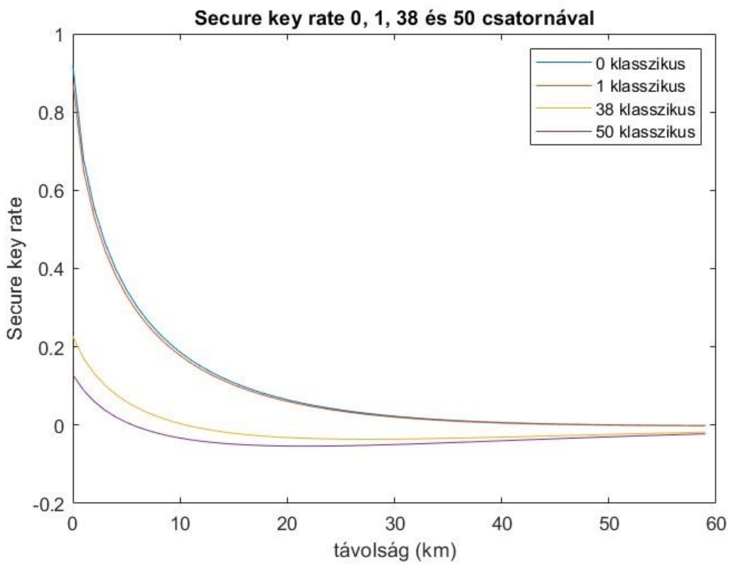
$$\varepsilon_{\text{out}} = \eta_{\text{Bob}} \langle N^{\text{out}}_{\text{GMCS}} \rangle / \langle n_{\text{LO}} \rangle.$$

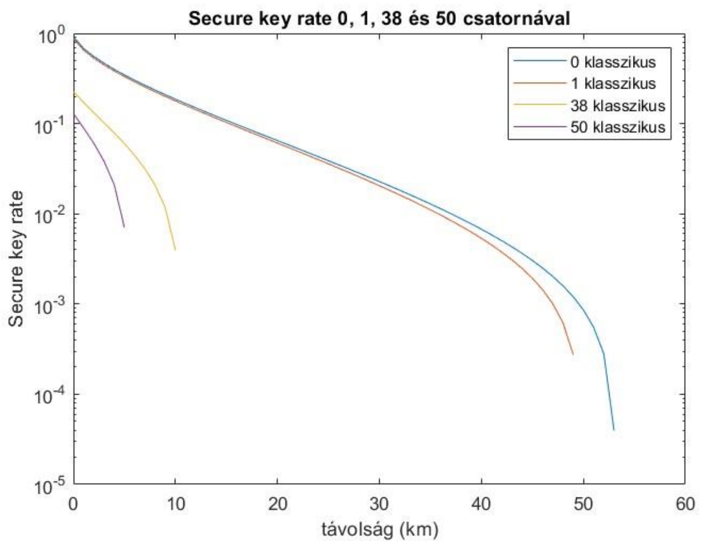
Ez a végső fotonszám, itt n_LO az LO fotonszáma (10^8)

A zajfotonok száma ebben a módban 10^2 nagyságrendű, amit a Matlab számítás és a cikk is igazolt. Mivel az LO fotonszáma 10^8 nagyságrenden van, ezért ez a zajfotonszám kevés ahhoz, hogy úgymond az LO helyébe lépjen és megváltoztassa, hogy mit fogad be a detektor.

3.5.2 /3 Kulcsráta számítás és eredmény értékelés:
Már majdnem minden paraméter megvan ahhoz, hogy elvégezhető legyen az egyenletrendszer. Amit még meg kell adni, az a „Va”, ami a modulációs variancia és az alapértéke 10. Ez „V” kiszámításához kell, ami az Alice által készített koherens állapot kvadratúra varianciája. (létezik a konstellációs ábra és magyarul ez egy jellemző arra, hogy Alice modulálása milyen varianciájú jeleket készít oda)

Ezután már mindent beírhatunk az egyenletrendszerbe. Lefuttattam különböző számú klasszikus csatornára és az eredmény a következő lett: Először viszonyszámként, utána dB-ben látható a diagram.





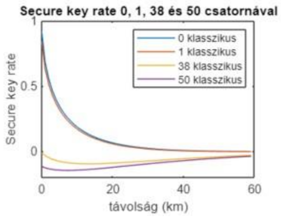
3.17 ábrák: Kulcsráta CVQKD esetén a távolság függvényében felső ábrán viszonyszámként, alsó ábrán dB-ben

Több érdekesebb megfigyelést is tehetünk. Egyrészt a klasszikus csatorna nélküli és az 1 klasszikus csatornás megoldás között alig van különbség használhatóságban. Ezen esetekben kb. 15-25 km-ig lehet hatékony. [20] esetében a nagytávolságú (BME I – Telekom Fehérvári út) mérésnél 4.67 dB szálcsillapítást mértek, ami egy rosszabb szállal nézve (0.25 dB/km) kb 18 km-nek felel meg. Mivel ott sikeres volt ekkora távolságon a CVQKD kulcsmegosztás, ezért ez igazolni tudja, bár ők kulcsrátát nem mértek, tehát az értékeket nem igazolja. 38 és 50 csatornával a modell szerint inkább csak 5-10 km-ig tud működni a kulcsmegosztás, utána túl nagy lesz a zaj.

3.6 Változtatható paraméterek hatása a CVQKD kulcsrátára

A Matlab szimuláció elején a különböző modellrészekhez különböző adatokat meg lehet adni, így többféle paraméterrel is lefuttathatóak. Az összes paraméter megtalálható hátul, a 8.-as pontú Függelék első oldalán a teljes kóddal együtt, 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 „használhatatlannak” nyilvánítsam. A használhatatlan az én értelmezésemben azt takarja, hogy a kulcsráta függvényei szinte 0-tól indulnak, pl. az alább szemléltetett kis ábrán:



3.18 ábra: Olyan CVQKD kulcsráta szemléltetése, ahol a sokcsatornás esetek 0 közeli kulcsrátáról indulnak (a távolság függvényében)

A „kulcsráta elrontási határértéke klasszikus csatornákkal együtt” oszlopban azt veszem határértéknek, ha a 38 csatornás kulcsráta már 0 közeléből indul. (Az 1 klasszikus + 1 kvantum csatorna rátája, tapasztalat alapján szinte együtt mozog az önálló kvantum csatorna kulcsrátájával, tehát 1 klasszikus + 1 kvantum csatornát szinte az 1 kvantumos határértékéig el lehet vinni. 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	Kulcsráta Kb. Elrontási határértéke klasszikus csatornákkal együtt	Kulcsráta kb. 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	csak ha 0 fölé megyünk, de ilyen nem létezik	Kicsit

3.7 Értékelés és fejlesztési lehetőségek

Összességében azt foglalnám össze eredményként, hogy CVQKD alkalmazásával lehetséges lehet kvantumos csatornát integrálni egy WDM hálózatba. Ahogy a 3.5.2 /3 pontban is értékeltem a kulcsráta 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. Ha emlékszünk, akkor pl. 3.5.2 /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 4. 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 [32] és [33] által készített CVQKD kulcsráta 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 4-es 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, de a kis távolságon való kulcsráta értékén biztosan változtat, hogy van egy zaj, ami a szál kezdetétől akár 10-20 km-ig is dominálhat (de a szálcsillapítás miatt csökken). Ennek a problémának a kibontása az 5. fejezet végén folytatódik a mérés eredményének megismertetése után.

4. 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 (20nm a 0.8nm 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 abból lejövő alsósíkú „metro" hálózatok CWDM technológiát használnak. Emiatt sajnos jövőállás szempontjából nem ez a legjobb megoldás.

4.1 Mérési elrendezés:

4.1.1 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. Ezek kapják meg a jelet, végzik el a modulációt, hőstabilitást biztosítanak az SFP-nek és az SFP elektromos táplálását is ezek biztosítják.

4.1 ábra: SFP-k a laborban

4.2 ábra: media converter a laborban

Az első képen az SFP-k, a másodikon egy media converter látható.

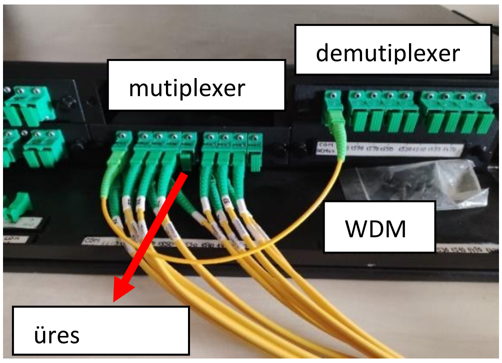
A mi tesztünkben kiválasztottuk az 1550 nm-es csatornát üresnek, vagyis kvantumosnak képzeltnek és a kétoldalára 3-3 klasszikus csatornát tettünk, mindegyiket külön SFP-vel, SFP-nként külön media converterrel.

4.3 ábra: vázlat az SFP beillszetéséről a media converterbe

4.4 ábra: összes használt SFP és media converter

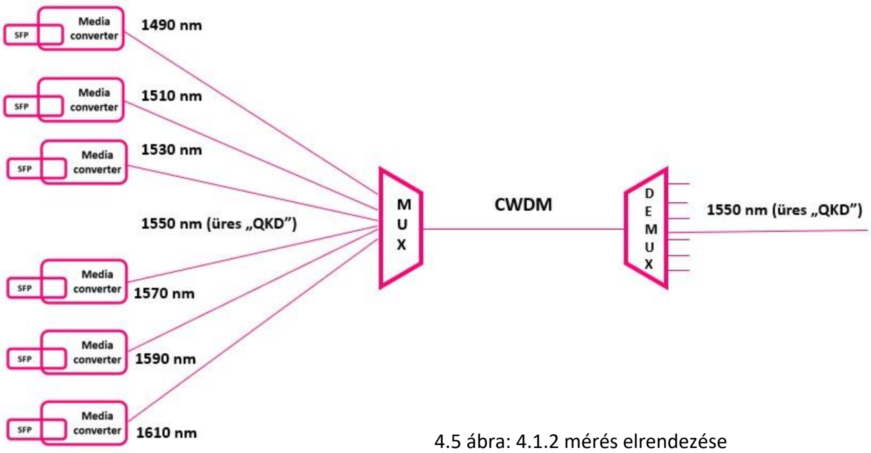
Tehát az adó oldali eszközök így néznek ki. Balról jobbra haladva 1610nm, 1590nm, 1570nm, majd az üres „kvantumos csatorna után” látható az 1530nm, 1510nm és 1490nm-t biztosító adó.

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.



4.4 ábra: DWDM eszköz – multiplexer és demultiplexer

4.1.2 Elrendezés:



4.5 ábra: 4.1.2 mérés elrendezése

4.2 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. A teljesítményeket egy egyszerű, kézben elférő, hordozható AFL CSM 1 optikai teljesítménymérővel mértük ki.

4.2.1 Media converterből kijövő teljesítmények:

Először ezt néztük meg. 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.

Hullámhossz	Teljesítmény (dBm)
1490 nm	-2.41 dBm
1510 nm	-3.35 dBm
1530 nm	3.52 dBm
1570 nm	0.33 dBm
1590 nm	3.2 dBm
1610 nm	-2.6 dBm

1550 nm

4.2.2 Demultiplexerről mért teljesítmények:

Azért, hogy láthassuk a rendszer csillapítását és fogalmunk legyen a kimeneten a klasszikus csatornák teljesítményéről, azokat is megmértük. Ezek alapján pedig kiszámolható a csillapítás is érdekesség képpen.

Hullámhossz (nm)	Teljesítmény (dBm)	Csillapítás (dB)
1490 nm	-6.44 dBm	4,03 dB
1510 nm	-6.14 dBm	2,79 dB
1530 nm	0.4 dBm	3,12 dB
1570 nm	-3.2 dBm	3,53 dB
1590 nm	-0.8 dBm	4 dB
1610 nm	-6.14 dBm	3.54 dB

1550 nm

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 egy valós hálózatinál.

4.2.3 Üres, 1550 nm-es csatorna teljesítménye:

Talán a legfontosabb információ, hogy mekkora lett a kvantumosnak képzelt csatorna helyén a zaj teljesítménye. Ideális esetben semmilyen optikai teljesítménynek se kéne megjelennie ott, de a 3. pontban tárgyalt zajok miatt természetesen nem ez lesz a helyzet. A kis teljesítmény mérővel **– 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.

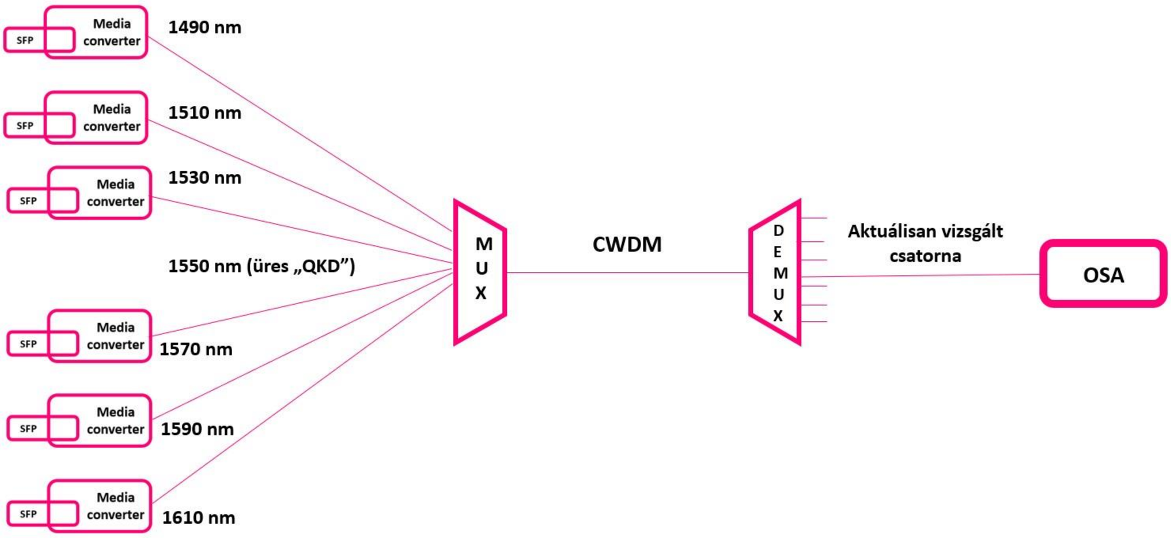
4.6 ábra: laborban rendelkezésre álló hordozható optikai teljesítménymérő

4.3 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.

4.3.1 Mérések a demultiplexer kimenetéről

Az első méréskört 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 újra „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



4.7 ábra: 4.3.2 mérés elrendezése

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

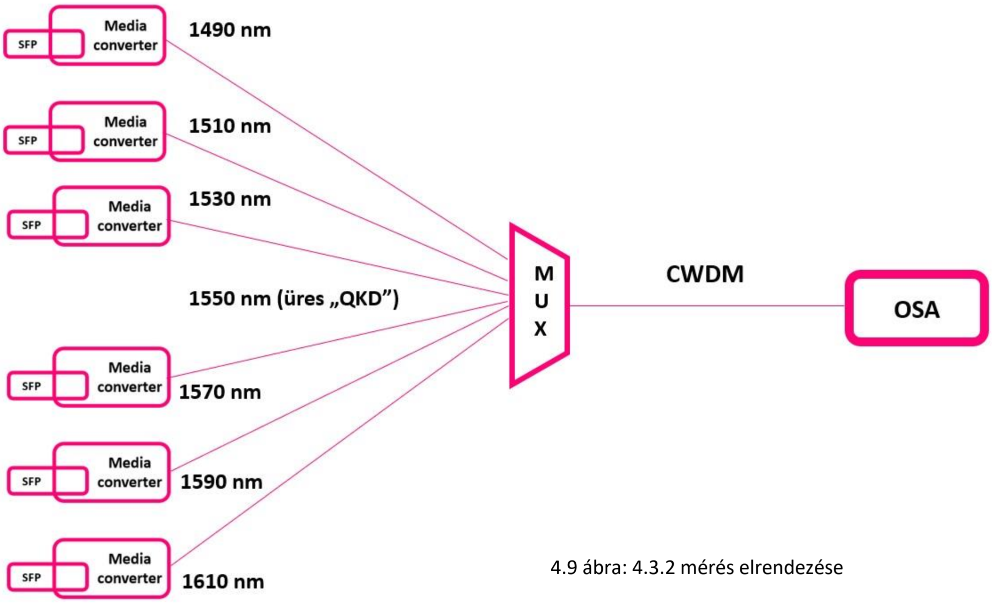
4.8 ábra: demultiplexer különböző kimenetei a spektrumanalizátoron

1530 nm-es kimeneten a mért maximális teljesítmény (a küldött csatorna teljesítménye) -3.94 dBm, 1550 nm-en csak zaj látható, aminek átlagos teljesítménye az ábra alapján -70 dBm körüli, 1570 nm-en pedig -11.8 dBm lett a csatorna teljesítménye. Az ábrák 1470nm – 1620 nm-es spektrumot ábrázolnak, ami azt jelenti, hogy lefedi a teljes CWDM tartományt. Emiatt elmondható, hogy a CWDM szűrői a különböző kimeneteken látványosan kiszűrik 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.

Ennek a mérésnek a hátránya az, hogy a demultiplexernek is van egy nagy (4.2.2 alapján) 3.5 dB csillapítása, ami a zajokra is hat, ezért az itt látott -75 dBm körüli zajszint csalóka. A multiplexált, közös szakaszon ennél nagyobb az „alsó” zajszint (ráadásul ott a különböző klasszikus csatornák sincsenek leszűrve, így összességében ott sokkal nagyobb zajok keletkezhetnek. Ha azt nézzük, hogy az egyetemi CVQKD rendszer teljesítmény szintje -60 dBm körül van, akkor az bőven kilógna és elkülöníthető lenne a -75 dBm körüli zajszintből, viszont azt is figyelembe kell venni, hogy a demultiplexer nem hagyná meg -60 dBm körüli jelszintet, hanem csillapítana rajta, így a könnyű elkülöníthetőség a zajból már nem olyan biztos. Ha akkora lenne egy CVQKD adó teljesítménye, hogy a demux után is megmaradjon kb. -60 dBm teljesítmény, akkor az nyugodtan integrálható lenne ebbe a CWDM rendszerbe.

4.3.2 Mérés a multiplexált, közös szakaszról

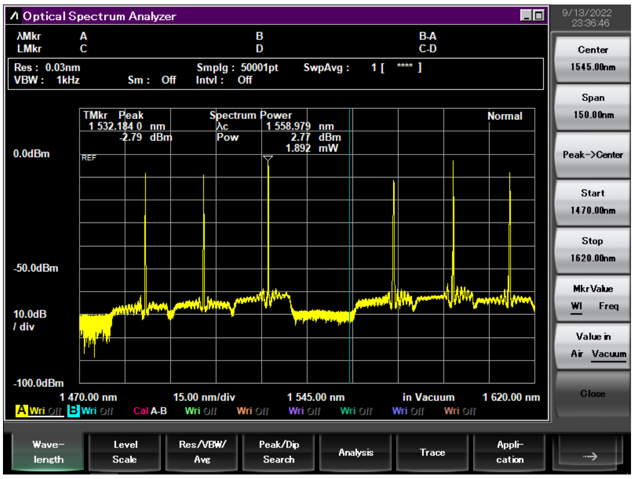
Itt kihagyjuk a mérésekből a demultilexert és a közös szakaszra kötjük a spektrumanalizátort.



4.9 ábra: 4.3.2 mérés elrendezése

Ennél a mérésnél azért kaphatunk jobb eredményt, mivel nem kerül rá a zajra a demultiplexer csillapító hatása.

Az első mérés a teljes CWDM spektrumot mutatja átlagolás nélkül:



4.10 ábra: 4.3.2 mérés eredménye a spektrumanalizátoron

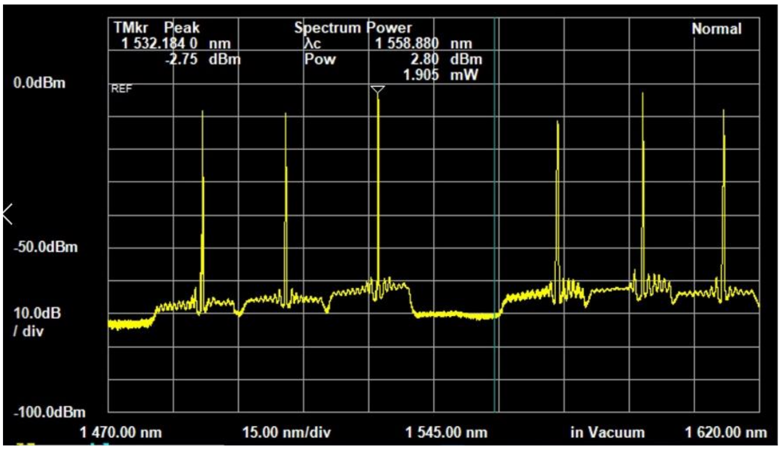
Klasszikus csatornák:

Az eredmény egyik része az, hogy a szakasz végén (pár méteres optikai szálal dolgozunk) a klasszikus csatornák a 4.2.1 táblázatánál mért jelteljesítményükből vesztettek, viszont nagyságrendileg hasonlóak. Az ábrán látható teljesítmények -3 és -10 dBm körül vannak, a 4.2.1 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 tapasztaljuk, hogy kb 20 nm hosszúságban 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 nem zavarják annyira a zajok, hogy ne lehessen felismerni a QKD jelét.

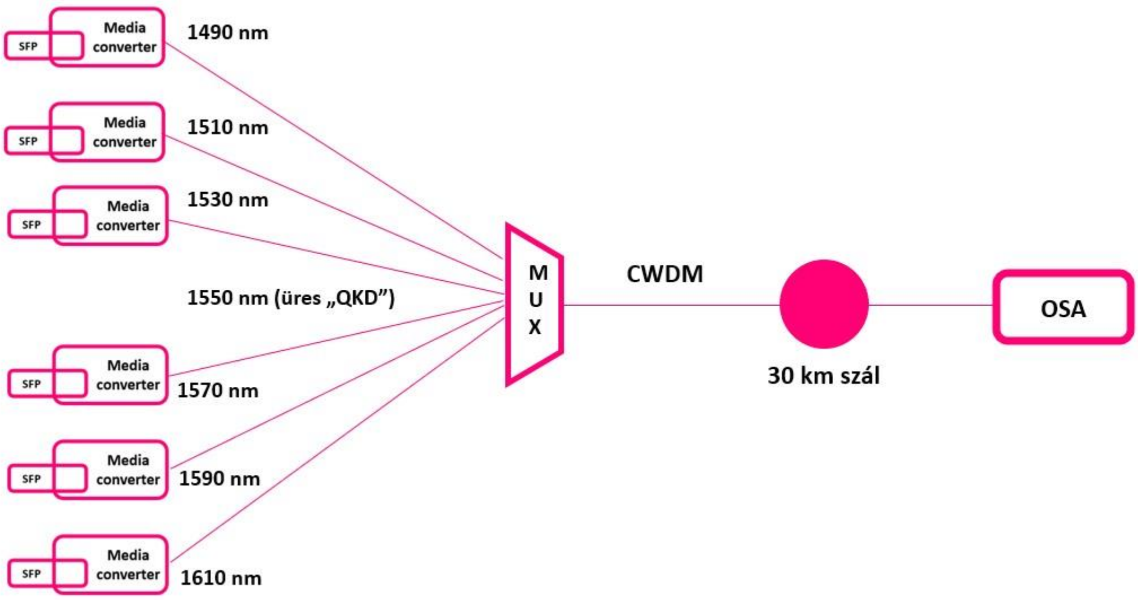
Ha ugyanezt a mérést átlagolással végezzük el, akkor a következő ábrát kapjuk, ahonnan még pontosabban az látható, hogy az üres sávban 1550 körül egy kb 20 nm-es spektrumban -70 dBm körül van a teljesítményszint.



4.11 ábra: 4.3.2 mérés eredménye a spektrumanalizátoron, átlagolás használatával

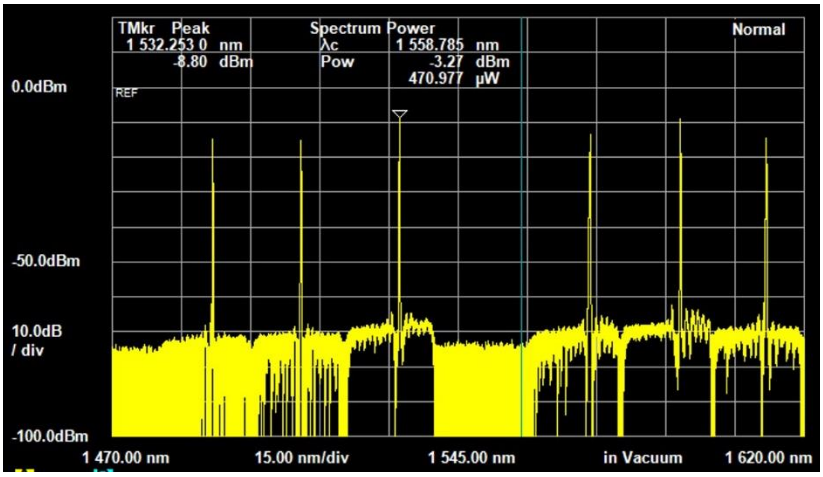
4.3.3 Mérés a közös szakaszról 30 km szál után:

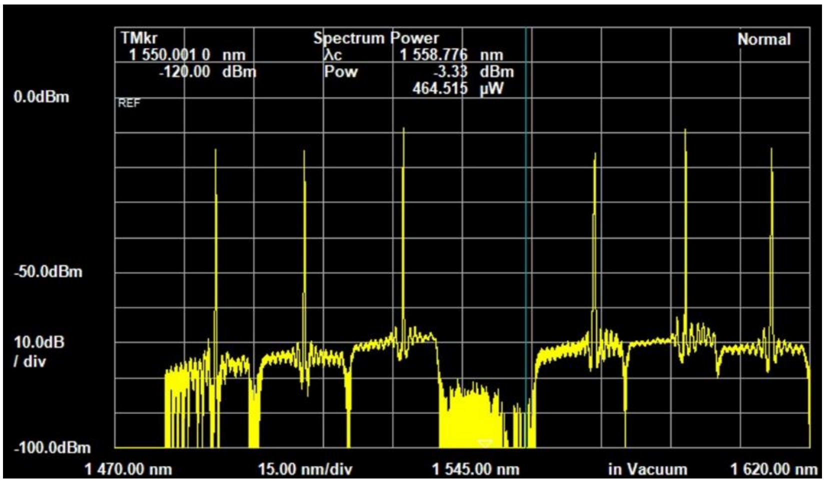
A következő lépésben, hogy jobban szimuláljuk a valóságot, 30 km-nyi (feltekert) optikai szálat teszünk a CWDM multiplexer kimenetére a spektrumanalizátor előtt. A kereskedelmi forgalomban is kapható QKD eszközök általában (attól függően, hogy CVQKD vagy DVQKD technológiát használnak) 50-70 km hosszan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



4.12 ábra: 4.3.3 mérés elrendezése

A mérés eredményét megint bontsuk külön. Az első képen látható egy átlagolás nélküli eredmény, a másodikon pedig átlagolással.





4.13 ábra: 4.3.3 mérés eredménye a spektrumanalizátoron

Az eredményből úgy gondolom, hogy két nagy következtetést vonhatunk le. Az egyik, hogy az átlagolt és átlagolás nélküli mérés között itt sokall nagyobb különbség van, mint az előző mérésnél. A másik, pedig az, hogy mindkét féle mérésnél elmondható, hogy kisebb a zaj, mint a 4.3.2, 30 km-es extra szál nélküli mérésnél.

Az átlagolásos mérés kisebb eredményének több oka lehet. Figyelembe kell venni, hogy itt már -70 dBm körüli teljesítményekről beszélünk, így a műszer pontatlansága is jobban szerepet játszik. Valószínűleg a felső, átlagolás nélküli képen egymástól nagyon sűrűn találhatóak csúcsok és miniális teljesítmény szintek, amik az átlagolásnál kiegyenlítettebb képet mutatnak. Az átlagolás folyamata úgy történik, hogy egymás után többször vesz mintát az adott hullámhosszról, emiatt összességében az átlagolásos verziót tekinthetjük pontosabb eredménynek.

A nagyobb távolság esetén mért kisebb zaj egy érdekes jelenség, hiszen szembe megy a Matlab modell eredményével. A magyarázata lehet esetleg a műszer pontatlansága ilyen kis teljesítményeken, vagy pedig, 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.

4.3.4 Értékelés

Az üres csatornán a 30 km-es szál nélkül -70 dBm körül volt a zaj teljesítménye, 30 km után pedig az átlagolásos 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.

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. Azért a célért szolgál, hogy minden olyan eszköz, ami bekerül a Magyar Telekom hálózatába, 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 élőhálózati 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 elvégésére.

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 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: transzponderek a győri laboratóriumban

A multiplexer és demultiplexer a Huawei Optix 1800 termékcsaládból származik. 40 csatornával rendelkezik, így figyelni kellett arra, hogy a 96 csatornát adni tudó transzponderből olyan hullámhosszú

5.2 ábra: multiplexer és demultiplexer a győri laboratóriumban csatornát válasszunk ki, ami létezik a multiplexeren is, mert különben a multiplexer és demultiplexer egyszerűen kiszűrné.

Ezen túl a rendszerbe nem tettünk be más elemet. Egy valódi WDM rendszerben lennének még erősítők és egyéb eszközök, viszont azt ugye tudjuk, hogy erősítő mellé nem lehet betenni kvantumos csatornát.

Mérőeszközként egy az egyetemihez képest más típusú (inkább terepre gyártott), Anritsu JDSU MTS 8000 típusú spektrumanalizátort használtunk. Ez egy nagy, hordozható, érintőképernyős, számítógépről is irányítható eszköz.

5.3 ábra: spektrumanalizátor a győri laboratóriumban

5.3 Mérések:

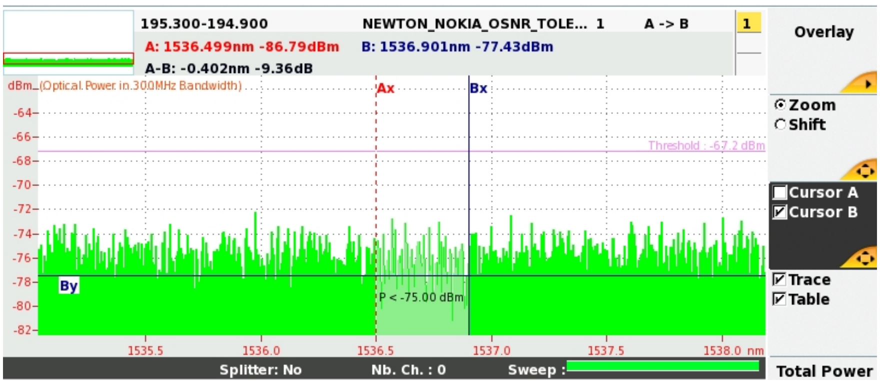
A fő cél itt is az volt, mint az előző mérésekben, vagyis, hogy egy kvantumosnak képzelt csatornát hagyjunk üresen és köré rakjunk klasszikus csatornákat és megnézzük, hogy mekkora a zaj az üres „kvantumos” csatornában, így megállapíthassuk, hogy lehetne-e integrálni QKD eszközt a rendszerbe.

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.

5.4 ábra: 5.3.1 mérés elrendezése

Az eredmény a következő:

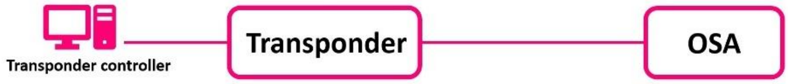


5.5 ábra: spektrumanalizátor saját zaja (magán a spektrumanalizátoron mutatva)

Vagyis az eszköz saját zaja átlagosan -75 dBm alatti, ekkora szintig biztosan pontos a teljesítmény mérés. Az „A” kurzornál viszont látható, hogy képes volt megmérni a -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.

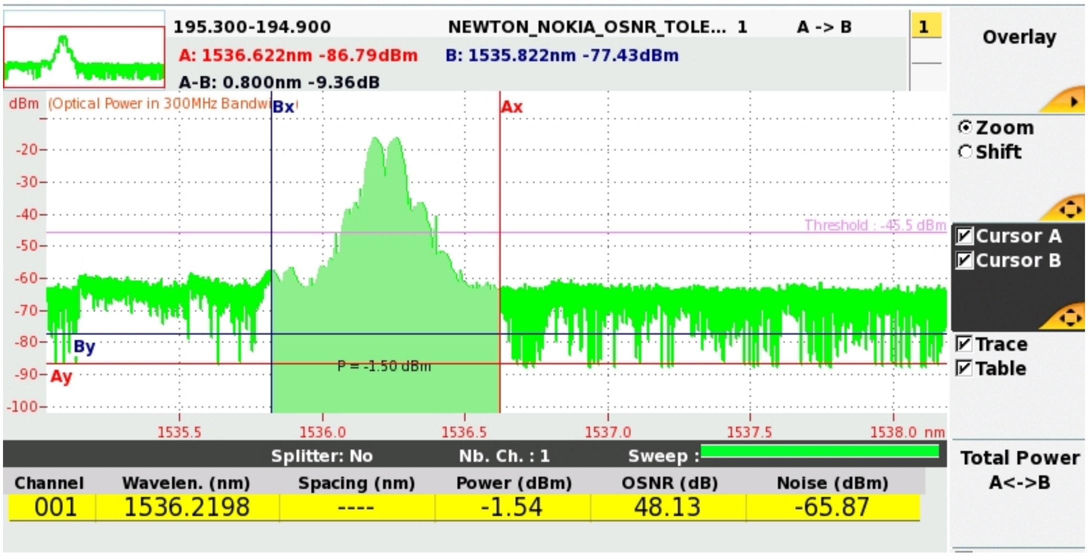
5.3.2 Transzponder teljesítménye:

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



5.6 ábra: 5.3.2 mérés elrendezése

Először a transzponder kezelő felületén be kellett állítani a kiválasztott csatornát. A spektrumanalizátor automatikusan megtalálta a kiadott csatornát (1536 nm-es csatorna) és kiírta a teljesítményét is.

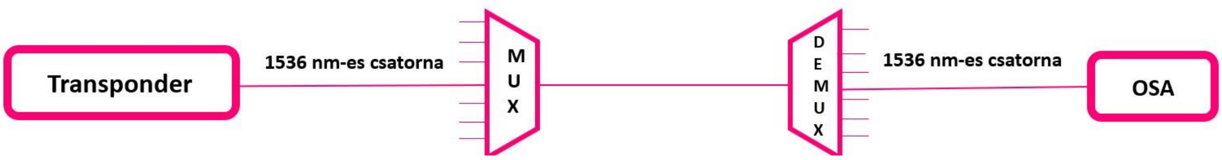


5.7 ábra: egy transzponder csatornája és annak teljesítménye a spektrumanalizátoron

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 reálisabb teljesítményt lehet kapni. Mint látható, ez **-1.54 dBm** lett, ami megfelel a hagyományos optikai kommunikáció csatorna teljesítményének.

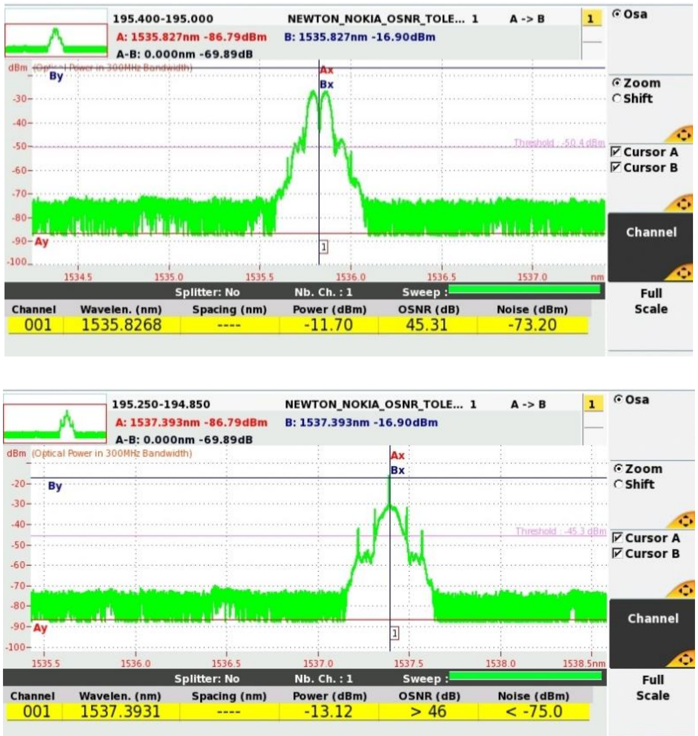
5.3.3 Egy klasszikus csatorna a mux/demux-on át

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.



5.8 ábra: 5.3.3 mérés elrendezése

Itt már mind a két transzpondert külön-külön megmértük, érdekesség képpen, hogy eltér-e a csillapításuk. Az eredmények a következők lettek:

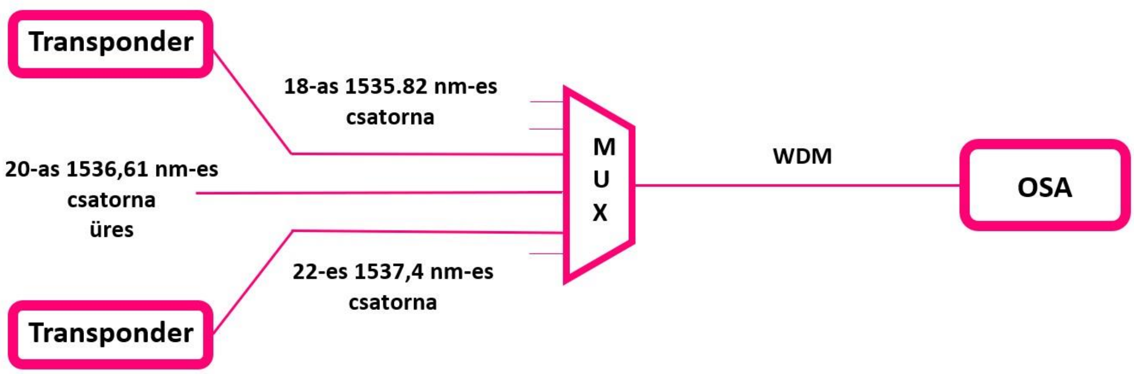


5.9 ábrák: egy-egy transzponder adása multiplexeren és demultiplexeren keresztül

Mint látható, 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.

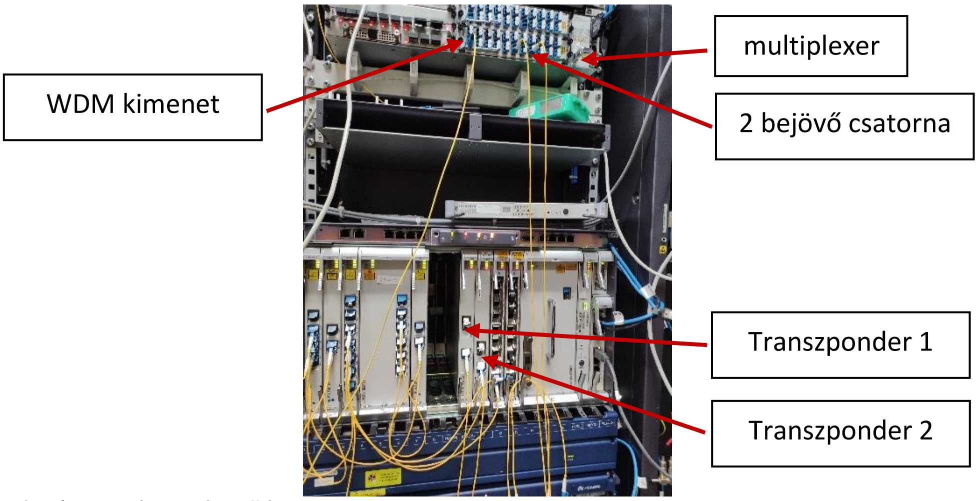
5.3.4 Közös szakasz mérése 2 klasszikus és közötte egy üres csatornával

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



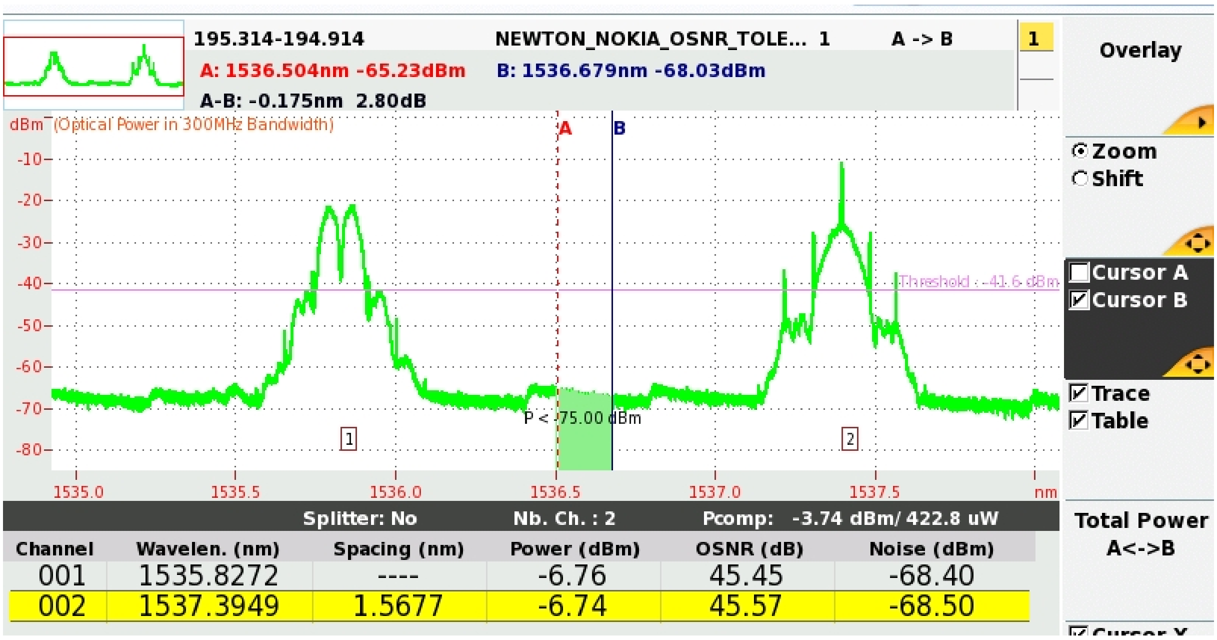
5.10 ábra:5.3.4 mérés elrendezése

A mérési elrendezés a valóságban így nézett ki:



5.11 ábra: 5.3.4 mérés elrendezése a valóságban

A mérés eredménye a következő lett:

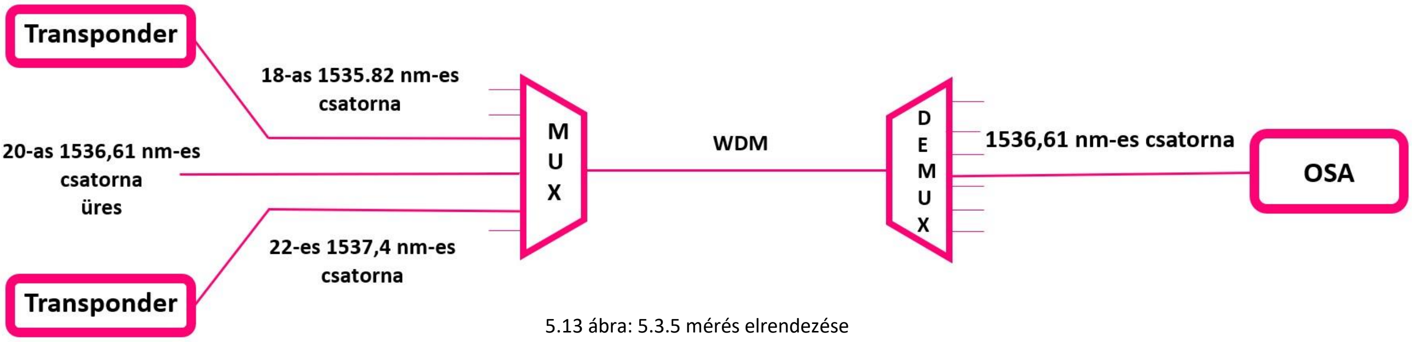


5.12 ábra: 5.3.4 mérés eredménye a spektrumanalizátoron

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 (eredeti/3.31)) csillapodtak a klasszikus csatornák. Ez valószínűleg a multiplexernek és a csatlakozási pontoknak köszönhető.

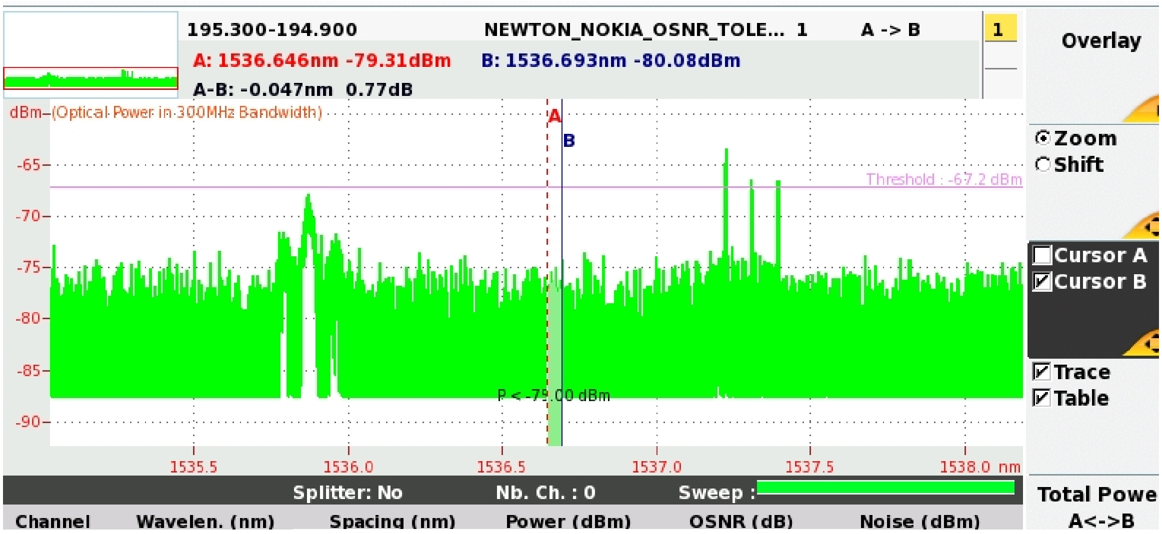
Nézzük a kvantumosnak kiválasztott csatorna helyét (1536.6 nm körül). Sajnos a kurzorokkal működő beépített teljesítménymérő nem működik megfelelően, mivel P<-75 dBm-et mutat. Az A és B kurzorokat beállítottam a megfelelő helyre, így a mért teljesítmény **-65 dBm** és **-68 dBm** körül van. A másik fontos dolog, hogy láthatóan a szomszédos csatornák teljesítményének fel és lefutásai sem érnek bele a kvantumosnak kiválasztott csatornába, hiába csak kb 0.5 nm-re vannak tőle. Úgy gondolom, hogy ez az alacsonyságú zajszint már elég lehet ahhoz, hogy érzékelni lehessen mellette egy CVQKD-csatornát, de erről majd később készítek bővebb értékelést. Azt is érdekes látni, hogy mindenféle szűrő nélkül is (itt ugye nincs bent 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



5.13 ábra: 5.3.5 mérés elrendezése

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 látszódni.

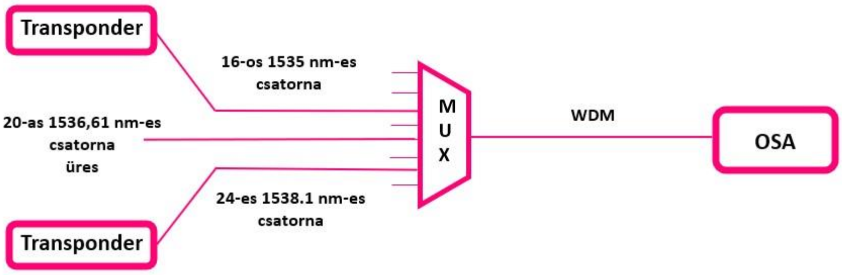


5.13 ábra: 5.3.5 mérés eredménye a spektrumanalizátoron

Az eredményből 2 fontos tanulságot vonnék le. Az egyik, hogy a két szomszédos csatorna láthatóan egy kicsit áthallatszik, viszont ez a (kurzorokkal kijelölt) kvantumos csatorna helyére nem szivárog át. A másik, hogy az alapzaj szintje („A” és „B” kurzorok mérése alapján) -80 dBm körül van. A kisebb zajt elsőre 3 dolog miatt tartanám lehetségesnek. Az egyik az, hogy a hosszabb WDM szakasz miatt a szálcsillapítás nő és a távolság függvényében növekvő zajok nem nőnek annyira, mint amekkora a csillapítás, így összességében csökken a zaj teljesítménye. Ezt kevéssé 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), miért úgyanúgy 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.

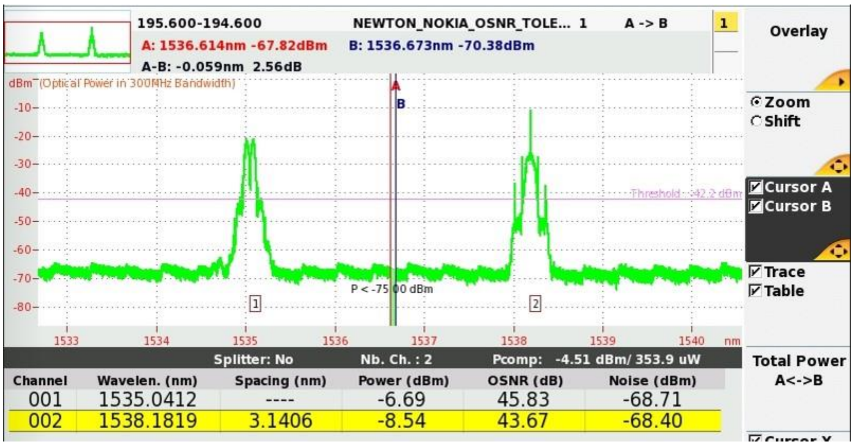
5.3.6 Mérés a WDM szakaszon, távolabbi klasszikus csatornákkal:

Itt ugyanaz történik, mint 5.3.4 mérés esetén, viszont a 2 klasszikus csatornát nem a szomszédba, 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.



5.14 ábra: 5.3.6 mérés elrendezése

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.

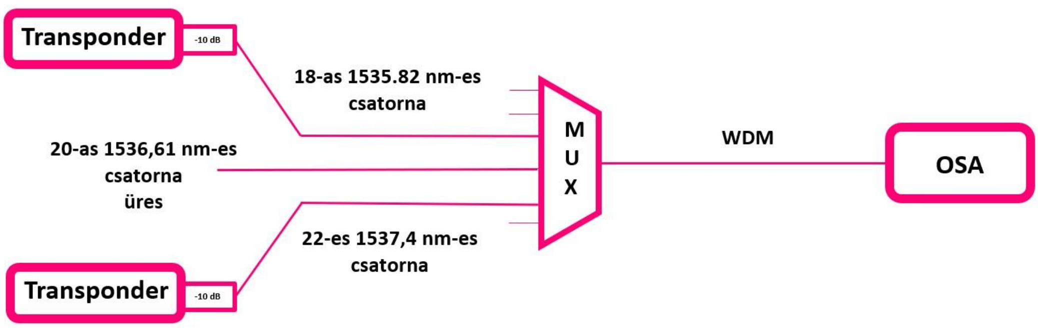


5.15 ábra: 5.3.6 mérés eredménye a spektrumanalizátoron

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

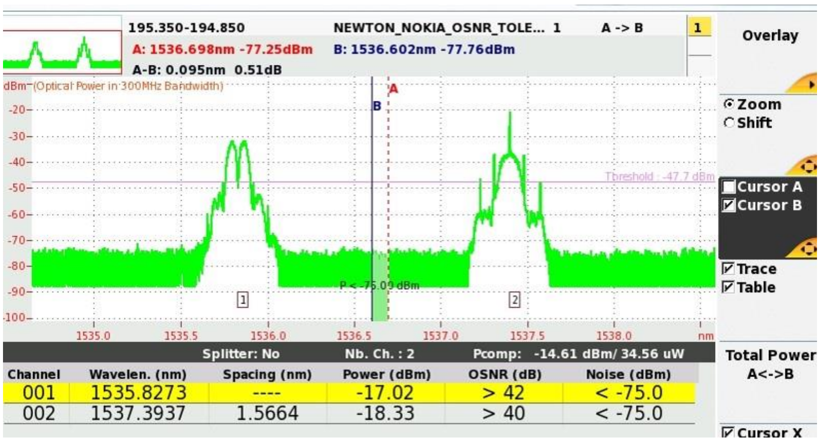
5.3.7 WDM szakasz mérése a klasszikus csatornák 10 dB-es csillapításával

Ebben a mérésben az lett az ötletünk, hogy ne a kvantumos csatornával vagy a környezetével próbáljunk tenni valamit, hanem a klasszikus csatornákkal. A transzponderek kimenetére 1-1 10 dB-es csillapítót helyeztünk. A klasszikus csatornákat a szomszédos csatornákra tettük, hogy lehető legnagyobb zavarás mellett tudjunk értékelni.



5.16 ábra: 5.3.7 mérés elrendezése

Az eredmény azt mutatja, hogy az üres csatorna helyén -77 dBm környékén van a zajszint, ami az eddigi legjobb eredmény.

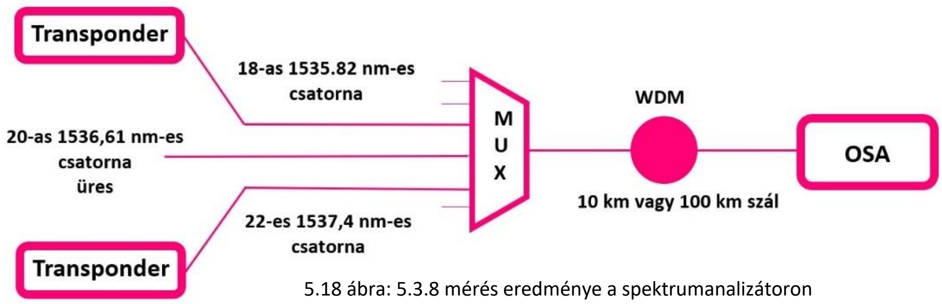


5.17 ábra: 5.3.7 mérés eredménye a spektrumanalizátoron

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 csatornákhoz 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, hogy ebből következtetni lehessen a kvantumcsatorna sorsáról.



5.18 ábra: 5.3.8 mérés eredménye a spektrumanalizátoron

Az eredményeket inkább 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 4.3.3 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 táblázat szerűen 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 (klasszikus csatornák alapján) [dB]	Üres csatornán zaj [dBm]	Várható kvantumos jelteljesítmény (eredeti-csillapítás) [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	itt elnyomott/kiszűrt, nem értelmezhető -12 (5.3.3 alapján)	10.5 (5.3.3 alapján)	-80	-75.5	Inkább igen
5.3.6	WDM, távolabbi csatornák	-7.6	6.1	-69.1	-71.1	Talán
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	Inkább 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 kvantumos jel várható teljesítménye a vevőnél (6. oszlop) kisebb, mint a csatornáján lévő zajszint (5. oszlop), ott nem tud kvantumos kommunikáció létrejönni.
- A demultiplexer jelenléte segít, mivel a klasszikus csatornák elnyomásával kisebb lesz a kvantumos 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 kvantumos csatorna mellett lévőre, akkor már kb. 3 dB-el csökkent a kvantumos 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 8.5 dB-el csökkenti a kvantumos csatornán lévő zajt, ha a klasszikusak a szomszédos csatornákon vannak.
- A szálhossz ugyan összességében csökkenti a zajt a kvantumos 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 kvantumos csatornán a zaj – jóval nehezebb lesz a kulcsmegosztás.
- A zajokról: 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. Továbblépési 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, lehet dolgozni a modell valóságosabbá tételén, de végül úgy is az igazi valóság győz. 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.

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 kulcsráta előállításában. Kiderült, hogyha az erősítő úgy helyezkedik el, hogy csak a klasszikus csatornákat erősíti (a kvantumos csatornákat is bevevő multiplexer előtt), akkor a zaja nem akkora befolyásoló tényező. Ezen kívül egész jól használható adatot kaptunk arra, hogy különböző paraméterek és csatornaszámok esetén mekkora lesz a kulcsráta.

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.

Győrben 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 klaszikus 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 hálózatrendszer építünk neki. Persze ha WDM-be integrált hálózatot építünk QKD-val, akkor is kellenek köztes Bob-ok és ellenőrzött, mindenki által bizalomban kezelt köztes csomópontok, de sokkal egyszerűbb lenne a már kiépített hálózattal együtt kezelni.

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.

7. Források

[1]: Communication Theory of Secrecy Systemes by C. E. Shannon 1949 https://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf

[2]: Born rule https://en.wikipedia.org/wiki/Born_rule

[3]: Emerging Trends In Ict Security 2014 (könyv)

[4]: Wiesner S. Conjugate coding. ACM SIGACT News. 1983

[5]: Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing

[6]: Quantum key distribution with entangled photons generated on demand by a quantum dot: https://www.science.org/doi/10.1126/sciadv.abe6379

[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]: Quantum Computing and the Future InternetBy Tajdar Jawaid https://www.researchgate.net/publication/359228217_Quantum_Computing_and_the_Future_Internet#pf3

[10]: https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/

[11]: https://www.idquantique.com/quantum-key-distribution-qkd-achieved-over-record-421-km/

[12]: Hacking commercial quantum cryptography systems by tailored bright illumination Lars Lydersen,1, 2, a) Carlos Wiechers,3, 4, 5 Christoffer Wittmann,3, 4 Dominique Elser,3, 4 Johannes Skaar,1, 2 and Vadim Makarov1 https://arxiv.org/pdf/1008.4593.pdf

[13]: https://business.blogthinkbig.com/we-apply-quantum-technology-to-real-use-cases-of-blockchain-and-iot/

[14]: 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

[15]: 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

[16] https://www.sciencedirect.com/science/article/pii/S003040182030451X és https://arxiv.org/pdf/1703.09278.pdf

[17]: https://www.sciencedirect.com/science/article/pii/S003040182030451X

[18]: 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

[19]: https://www.wwt.com/article/cwdm-or-dwdm-which-should-you-use-and-when

[20]: Kis Zsolt: Kvantumkommunikációs kísérletek a Magyar Telekom hálózatán (belsős 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]: 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

[25]: GAIN AND NOISE FIGURE PERFORMANCE OF ERBIUM DOPED FIBER AMPLIFIERS (EDFA), A.Cem ÇOKRAK 1 Ahmet ALTUNCU 2 https://www.electricajournal.org/Content/files/sayilar/37/1111-1122.pdf

[26]: 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

[27]: Development of Cholesteric Liquid-Crystal Spectral Filters for Visible WDM Channels Over Polymer Optical Fibres https://www.researchgate.net/figure/The-typical-spectrum-of-the-4-channels-WDM-light-source-The-Fig4-displays-the-reflected_fig2_315705776

[28]: Optical networking for quantum key distribution and quantum communications

T E Chapuran https://iopscience.iop.org/article/10.1088/1367-2630/11/10/105001

[29]: 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

[30]: Security of quantum key distribution with imperfect devices

Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, John Preskill https://arxiv.org/abs/quant-ph/0212066

[31]: Practical decoy state for quantum key distribution Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo https://arxiv.org/abs/quant-ph/0503005

[32]: Quantum key distribution using gaussian-modulated coherent states

Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, https://www.nature.com/articles/nature01289

[33]: 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

8. Függelék

Szimuláció Matlab kódja: (kimásolva Matlab live script-ként futtatható is akár)

```
%start
clear all;
clc;
%változtatható értékek:
%általános
NF_db= 5.5;                    % EDFA noise figure (dB)
xi1_db=-80;                   % multiplexer izolációja (dB)
xi2_db=-80;                   % demultiplexer izolációja (dB)
lambda_klasszik_nm=1550;     % klasszikus csatornák hullámhossza (nm)
Pout_laser_dBm=0;            % a klasszikus csatornák lézerének kimeneti teljesítménye
beta=4*10^(-9);              % spontán Raman szórás együtthatója
z=1:1000:60000;              % kábelhossz (m)
ndmu_db=-1.5;                % demux vesztesége (dB)
nmux_db=-1.5;                % multiplexer vesztesége (dB)
P_laserzaj_dbm=-70;          % laser háttérzaja (kimérték -20 dBm-es klasszikus csatornával) (dBm)
szalcsillapitas_dbperkm=0.2;% km-enkénti csillapítás dB-ben
% 1 klasszikus 1 kvantum modell
dt_ns=1;                     % single photon detector időablaka (nanosecond)
df_GHz=75;                   % klasszikus csatorna sávszélessége (GHz)
dlambda_nm=0.6*10^(-9)       % sávszélesség hullámhossz tartományban (7. oldal alsó bekezdés)
nbob=0.6;                    % Bob rendszerének átvitele (nem dB)
y00=5*10^(-6);               % az eredeti qkd rendszer háttérzaja (minden más nélkül ennyi zajfoton van)
edet=0.003;                  % annak a valószínűsége, hogyha Alice és Bob ugyanazt az alapot választják (?), akkor a foton rossz detektort
talál el
f1=1.22;                     % hibajavító algoritmus hatástalansági tényezője
mu=0.5;                      % expected photon number of the signal state (nem írják mennyi-fogalmam sincs)
https://iopscience.iop.org/article/10.1088/1367-2630/8/1/004/pdf itt írnak róla
e0=0.5;                      % az y00 háttérzaj hibája
% homodin detektoros modell
f_LO_MHz= 1;                % homodin detektor local oscillator-jának frekije (MHz)
lambda_kvantum_nm=1550;     % kvantum csatorna hullámhossza (nm) - csak 1 kis számításhoz kell
```

```
pulsefoton=10^8;           % egy pulzusban a lézerből érkező fotonok száma
m=38;                       % klasszikus csatornák száma
dfhomodin_MHz= 1;          % homodin detektor sávszélessége (MHz)
df_demux_GHz=75;           % demultiplexer sávszélessége (GHz)
nlo=10^8;                  % local oscillatorban az átlagos fotonszám
Va=10;                     % modulációs variancia
e_0=0.01;                 % egy GMCS paraméter
vel=0.01;                  % egy GMCS paraméter
gamma=0.9;                 % a reverse reconcilation algoritmus hatékonysága
Pkvantum_dbm=-19;
%Mértékegység átváltások
NF=dbtonumber(NF_db);
xi1=dbtonumber(xi1_db);
xi2=dbtonumber(xi2_db);
lambda_klasszik=lambda_klasszik_nm*10^(-9);
Pout_laser=dbmtowatt(Pout_laser_dBm);
ndmu=dbtonumber(ndmu_db);
nmux=dbtonumber(nmux_db);
Plaserzaj=dbmtowatt(P_laserzaj_dbm);
dt=dt_ns*10^(-9);
df=df_GHz*10^(9);
f_LO=f_LO_MHz*10^6;
lambda_kvantum=lambda_kvantum_nm*10^(-9);
dfhomodin=dfhomodin_MHz*10^(6);
df_demux=df_demux_GHz*10^9;
z_km=z./1000;
Pkvantum=dbmtowatt(Pkvantum_dbm);
% egyéb állandók
%c=physconst('lightspeed);
c=3*10^8;
h=6.626070040e-34;
% Erősítés és nch (optikai szál átvitel) távolság függővé tétele:
nch_db=-(szalcsillapitas_dbperkm*z_km);
nch=dbvektortonumber(nch_db);
plot(z_km,nch), xlabel('távolság (km)'), ylabel('nch (viszonyszám)'), title('Vezeték átvitele (nch)');
G=100./nch; % az erősítés csillapításfüggővé tétele

% 1. EDFA erősítő zaja
% Nase=2*nsp*(G-1); megadott képlet
% NF= (1+2*nsp*(G-1))/G; megadott képlet
nsp= (G*NF-1)/(2*(G-1));   %2. képletből levezetve, mivel NF van megadva
Nase=2*nsp*(G-1);          %zajfoton szám
Nmod=dt*df;                %
Nase_A=xi1*Nase;    %"A" ponton - a mux kimenetén - mérhető zajfoton szám egy mod-ban
plot(z_km,(Nmod.*Nase_A)),xlabel('távolság (km)'), ylabel('fotonszám az "A" ponton'), title('Erősítő zajfotonszáma az A pontban'),
subtitle('Izolációtól és erősítéstől függ, az utóbbi pedig a távolságtól');
Nase_B=Nase_A.*nch;        % B ponton - a demux bemenetén mérhető zajfoton szám
plot(z_km,(Nmod.*Nase_B)), xlabel('távolság (km)'), ylabel('fotonszám a "B" pontban'), title('Erősítő zajfotonszáma a "B" pontban');
Nase_C=Nase_B*ndmu;        % C ponton - a demux kimenetén mérhető zajfoton szám
plot(z_km, (Nmod.*Nase_C)), xlabel('távolság (km)'), ylabel('fotonszám a "c" pontban'), title('Erősítő zajfotonszáma a "C"
pontban'),grid;
```

```
Nase_bob=Nase_C.*nbob;
plot(z_km, (Nmod.*Nase_bob)), xlabel('távolság (km)'), ylabel('fotonszám Bob után'), title('(ASE) Erősítő zajfotonszáma Bob után'),grid;
Nase_C_abra=Nmod.*Nase_C;
% G: EDFA erősítése
% nsp: spontán emissziós faktor (>1) (ha ez az egyetlen zajforrás az erősítőből, akkor =1
% NF: EDFA noise figure - gyakorlatban ezt szokták megadni
% xi1: multiplexer izolációja
% nch: csatorna (optikai szál) átvitele
% ndmu: demultiplexer átvitele
% nbob: Bob átvitele

% 2. szivárgás a klasszikus csatornákból
% Nleak= (xi2*Pout)/(h*f);  Pleak=xi2*Pout;  megadott képletek
Pout=Pout_laser*nch;  %mW - klasszikus csatornák kimeneti teljesítménye "B" pontban
Pout_dbm=watttodbm(Pout);
plot(z_km,Pout_dbm), ylabel('teljesítmény B pontban (dBm)'), xlabel('távolság (km)'), title('Klasszikus csatornák kimeneti
teljesítménye'), subtitle('Pout, csak a szálcsillapítás rontja itt'),grid;
Pleak_C=xi2.*Pout;  % C pontban (a kvantumcsatornáknál) mért zajteljesítmény
f=c/lambda_klasszik;
Nleak_C=Pleak_C./(h*f);  % C pontban a zajfotonok száma
plot(z_km,(dt*Nleak_C)), xlabel('távolság (km)'), ylabel('fotonszám C pontban'), title('Klasszikus csatornák szivárgó fotonszáma C
pontban'), subtitle('xi2-től, táv miatt Pout-tól és a hullámhossztól függ még'),grid;
%plot(z_km,(nbob.*dt.*Nleak_C)), xlabel('távolság (km)'), ylabel('fotonszám Bob után'), title('Klasszikus csatornák szivárgása Bob
után'), subtitle('xi2-től, táv miatt Pout-tól és a hullámhossztól függ még');
%plot(z_km,(Nmod.*nbob.*dt.*Nleak_C)), xlabel('távolság (km)'), ylabel('fotonszám Bob után'), title('Klasszikus csatornák szivárgása Bob
után'), subtitle('xi2-től, táv miatt Pout-tól és a hullámhossztól függ még');
Nleak_C_abra=dt*Nleak_C;
% számítás, ha Pout nem függ a távolságtól mert az erősítés megoldja, hogy 0 dB legyen a kimeneten
Pout_const=Pout_laser;
Pout_const_dbm=watttodbm(Pout_const);
plot(z_km,ones(size(z_km)).*Pout_const_dbm), ylabel('teljesítmény B pontban (dBm)'), xlabel('távolság (km)'), title('Klasszikus csatornák
konstans kimenő teljesítménye'),grid;
Pleak_const_C=xi2.*Pout_const;
Nleak_const_C=Pleak_const_C./(h*f);
plot(z_km,ones(size(z_km)).*(dt*Nleak_const_C)), xlabel('távolság (km)'), ylabel('fotonszám C pontban'), title('Klasszikus csatornák
szivárgása const Pout esetén'), subtitle('xi2-től, táv miatt Pout-tól és a hullámhossztól függ még'),grid;
Nleak_C=Nleak_const_C;  %ha ezt a megoldást akarjuk aktiválni a teljesre
% Pout: a klasszikus csatornák demultiplexer előtt mért teljesítménye
% xi2: demultiplexer izolációja

% 3. Spontán anti-stokes Raman szórás
% Psars=Pin*beta*z*nch*dl = Pout*beta*z*dl  megadott képlet a B pontban (demux előtt) lévő zajteljesítményre
dlambda=c/df;
kisPramf=Pout_laser.*z_km.*beta.*dlambda;  %-alfa=nch
nagyPramf=(kisPramf.*lambda_klasszik)./(h.*(3*10^8)).*ndmu.*dt;
Nsars_C9=nagyPramf;%/(h.*(3*10^8));
Nsars_C=Nsars_C9;
%Nsars_C=(lambda_klasszik^3/(h.*(3*10^8).^2)).*Pout_laser.*beta.*z.*ndmu;   ez a jó
plot(z_km,(Nmod.*Nsars_C)), xlabel('távolság (km)'), ylabel('fotonszám a C ponton'), title('Spontán anti-stokes Raman szórás
fotonszáma'), grid; %subtitle('hullámhossztól, Pout-tól, beta-tól és ndmu-tól függ még');
```

```
plot(z_km,(nbob.*Nmod.*Nsars_C)), xlabel('távolság (km)'), ylabel('fotonszám a C ponton'), title('SARS fotonszáma Bob után'),
%subtitle('hullámhossztól, Pout-tól, beta-tól és ndmu-tól függ még');


%Tesztek 2 - másfajta képletek használata
ujNmod=((c/lambda_klasszik^2)*dlambda);

Psars=Pout_laser.*beta.*z.*dlambda;
ujNsars=(Psars./(h*(c/lambda_klasszik)*Nmod)).*ndmu;
plot(z_km, Nmod.*ujNsars), title('ujNsars1');


Psars2=Pout_laser.*beta.*z_km.*nch.*dlambda_nm;
ujNsars2=(Psars2./(h*(c/lambda_klasszik)*Nmod)).*ndmu;
plot(z_km, ujNmod.*ujNsars2), title('ujNsars2');
% beta: spontán Raman szórás együtthatója
% Pin: klasszikus csatornák "A" pontban (mux után) mért teljesítménye
% z: kábelhossz
% nch: optikai szál áteresztő képessége - nem kell

% 4. Lézer háttérzaja
P_egyfoton=h*f;
Nlaser_Gnelkul=Plaserzaj/P_egyfoton;
Nlaser=G*Nlaser_Gnelkul;
plot(z_km,Nlaser), xlabel('távolság (km)'), ylabel('fotonszám'), title('Lézer háttérzajának fotonszáma a távolság függvényében'),
subtitle('A lézer alapzajától és az erősítéstől függ');
%valamiért a cikk azt írja, hogy egy spatiotemporal mode-ban csak 0.01 foton van

% 5. modell 1 klasszikus és 1 kvantum csatornára
G_db=vektortodb(G);  % azért alakítom át, hogy látható legyen, hogy mekkora távolság esetén milyen erősítés kell
plot(z_km,G_db), xlabel('távolság (km)'), ylabel('erősítés értéke (db)'), title('A szükséges bemeneti erősítés'), subtitle('értéke:
100/nch, így a szálcsillapítástól függ');
Nspd_C1=Nmod.*nch.*ndmu.*Nase_A + Nleak_C*dt + Nsars_C;  % ez jó a secure key-hez
Nspd_C2=Nmod.*nch.*ndmu.*Nase_A + Nleak_C*dt + Nmod.*Nsars_C;  % ez jó az y0-hoz
Nspd_C=Nspd_C1; %Nspd_C kiválasztása
y0=y00+nbob*Nspd_C;  % rossz észlelések száma (amikor zajt észlel "kvantumcsatorna foton" helyett)
%egy időablakban lévő zajfotonok ha beleszámítjuk a lézer háttérzaját
Nspd_pluslaserhatter=Nspd_C+Nmod.*nch.*ndmu.*Nlaser;
y0_pluslaserhatter=y00+nbob.*Nspd_pluslaserhatter;
% Nspd és y0 ábrázolása távolság függvényében
plot(z_km,Nspd_C), xlabel('távolság (km)'), ylabel('az egy időablakban lévő zajfotonszám'), title('Nspd_C, Zajfotonok száma egy
időablakban'), subtitle('demux veszteségtől, zajoktól,és Nmod-tól függ leginkább'), grid on;
plot(z_km,y0), xlabel('távolság (km)'), ylabel('rossz észlelések száma'), title('Y0, Rossz észlelések száma'), subtitle('zajfotonszámtól,
QKD rendszer háttérzajától és bob átvitelétől függ'), grid on;
% secure key rate teszt
% n=nch.*ndmu.*nbob;  %teljes rendszer átvitele
% qmu=y0+1-exp(n*mu);
% emu=(e0*y0+edet*(1-exp(n*mu)))/qmu;
% q1=(y0+n).*mu.*exp(mu);
% e1=(e0*y0+edet*n)*mu*exp(mu)/q1;
%
% R=1/2*(q1-(f_fgv(emu)*qmu*H2(emu))-(q1*H2(e1)));
```

```
% a=f_fgv(emu)*qmu*H2(emu);  %debugoláshoz néztem
% b=q1*H2(e1);               %debugoláshoz néztem
% plot(z_km,R), xlabel('távolság (km)'), ylabel('secure key rate'), title('Secure key rate a távolság függvényében'), subtitle('Rendszer átvitelétől és y0-tól függ leginkább');
% secure key rate
n=nch*ndmu*nbob;  %teljes rendszer átvitele
qmu=y0+1-exp(-n*mu);
emu=(e0*y0+edet*(1-exp(-n*mu)))/qmu;
q1=(y0+n).*mu.*exp(-mu);
e1=(e0*y0+edet*n)*mu*exp(-mu)/q1;


R=1/2*(q1-(f_fgv(emu)*qmu*H2(emu))-(q1*H2(e1)));
%a=f_fgv(emu)*qmu*H2(emu);  %debugoláshoz néztem
%b=q1*H2(e1);               %debugoláshoz néztem
plot(z_km,R), xlabel('távolság (km)'), ylabel('secure key rate'), title('Secure key rate a távolság függvényében'), subtitle('Rendszer átvitelétől és y0-tól függ leginkább'), grid;
plot(z_km,R), xlabel('távolság (km)'), ylabel('secure key rate'), title('Logaritmikus Secure key rate a távolság függvényében'), subtitle('Rendszer átvitelétől és y0-tól függ leginkább');
set(gca,'Yscale','log');


% az R képletében használt H2() és f() függvények itt találhatóak: https://arxiv.org/pdf/quant-ph/0503005v5.pdf
%df: klasszikus sávszélessége
%dt: single photon detector időablaka
%nch: optikai szál átvitele
%innen talán az y0 a legfontosabb, ami megadja a single photon detector dt
%időablakába eső zajfotonok számát
% 1s alatt (dt időablakot 1*10^9 ns-re állítva) 4.68*10^7 db zajfoton érkezik Bobhoz

% 6. modell homodin detektoros vevő esetén - 1 féle csatornaszámmal

% kvantum csatorna teljesítménye


t_pulse=1/f_LO;    %pulzus ideje
f_kvantum=c/lambda_kvantum;    %kvantum csatorna frekije a teljesítmény számoláshoz
P_kvantum=0.94*pulsefoton*(h*f_kvantum)/t_pulse;  % képlet forrás: https://www.rp-photonics.com/peak_power.html
p_kvantum_dbm=watttodbm(P_kvantum);  % (-19 dBm lett nekik, nekem nem :( )) verzio2: nekem is :)


% matched mód


%tesztel Ngmcs_in-re
%Ngmcs_in=1/2.*m.*(nch.*ndmu.*Nase_A + Nsars_C);  % matched módú zajfotonok száma egy spatiotemporal mode-ban (1/2 szorzás az LO polarizáció szelektálása miatt van)
%Ngmcs_in=1/2.*90.*(nch.*ndmu.*Nase_A + Nsars_C+Nleak_C_abra./100);  %%m=1-el 50 körül lesz, m=38al 30 körül lesz, m=138nál 10 körül lesz a secure key
%Ngmcs_in=Ngmcs_in*10^(-99);
Ngmcs_in=1/2.*(nch.*ndmu.*Nase_A +Nsars_C);
```

```
%teszt a matched módú fotonszámra a cikk eredménye alapján


%Ngmcs_in=1/2.*m.*(nch.*ndmu.*Nase_A+(0.26/20000).*z+0.08);
%plot(z_km,Ngmcs_in), title('Ngmcs_in');
%plot(z_km,((0.26/20000).*z)), title('uj Sasrs');


%Ngmcs_in=1/2.*m.*(nch.*ndmu.*Nase_A + Nsars_C+Nleak_C_abra./28); %m=0-val 50 körül lesz, m=1-el 50 körül lesz m=38-al 10 körül lesz,
ein=2.*nbob.*Ngmcs_in;  % Bobhoz eljutó zajfotonok száma   -- dt=1s-os időablak esetén 4.78*10^-8 ami nagyon kevésnek tűnik
%plot(z_km,ein), xlabel('távolság (km)'), ylabel('fotonszám'), title('Matched módú Bobhoz eljutó fotonok száma'), subtitle('a zajoktól és a klasszikus csatornák számától függ, 1 pulzusban értendő');
plot(z_km,Nmod.*ein), xlabel('távolság (km)'), ylabel('fotonszám'), title('Matched módú Bobhoz eljutó fotonok száma');


% unmatched mód


dtnagy=1/(2*pi*dfhomodin);    % homodin detektor integrációs ideje
Ngmcs_out=(dtnagy/dt).*Nspd_C;        % detektor bemenetére kerülő unmatched módú fotonok száma
eout=nbob*Ngmcs_out/nlo;
plot(z_km,eout), xlabel('távolság (km)'), ylabel('fotonszám'), title('Unmatched módú Bobhoz eljutó fotonok száma'), subtitle('1 pulzusban értendő');

% secure key rate:


%adatok
V=Va+1;                      % Alice által készített koherens állapot kvadratúra varianciája
nvesszo=ndmu*nbob;           % Bob rendszerének hatékonysága
e=e_0 + (ein/(nch*ndmu*nbob));
lambda_line=(1./nch)-1+e;
lambda_hom=((1+vel)./nvesszo)-1;
lambda_tot=lambda_line+(lambda_hom./nch);


%paraméterek:
A=V^2.*(1-2.*nch)+2.*nch+nch.^2.*(V+lambda_line).^2;
B=nch.^2.*(V.*lambda_line+1).^2;
C= (V.*sqrt(B)+nch.*(V+lambda_line)+A.*lambda_hom)./(nch.*(V+lambda_tot));
D=sqrt(B).* ((V+sqrt(B).*lambda_hom)./(nch.*(V+lambda_tot)));


sigma1negyzet=1./2.*(A+sqrt(A.^2-4.*B));
sigma2negyzet=1./2.*(A-sqrt(A.^2-4.*B));
sigma1=sqrt(sigma1negyzet);
sigma2=sqrt(sigma2negyzet);


sigma3negyzet=1/2.*(C+sqrt(C.^2-4.*D));
sigma4negyzet=1/2.*(C-sqrt(C.^2-4.*D));
sigma3=sqrt(sigma3negyzet);
sigma4=sqrt(sigma4negyzet);
```

```
%nagyobb számítások
lambda_be=teta((sigma1-1)./2) + teta((sigma2-1)./2) - teta((sigma3-1)./2) - teta((sigma4-1)./2);
Iab=1/2.*log2((V+lambda_tot)./(1+lambda_tot));
dI=gamma.*Iab-lambda_be;



plot(z_km,dI), xlabel('távolság (km)'), ylabel('Secure key rate'), title('Secure key rate homodin detektoros módszerrel');
plot(z_km,dI), xlabel('távolság (km)'), ylabel('Secure key rate'), title('Logaritmikus Secure key rate homodin detektoros módszerrel');
set(gca,'Yscale','log');

% 7 Több secure key függvény egymáson


%Ngmcs_in=1/2.*(nch.*ndmu.*Nase_A + Nsars_C+Nleak_C_abra./28); %ez a jó
%Ngmcs_in=1/2.*(Nsars_C+Nleak_C_abra./28);
%Ngmcs_in=1/2.*m.*(nch.*ndmu.*Nase_A+(0.26/20000).*z+0.08);
Ngmcs_in=1/2.*(nch.*ndmu.*Nase_A +Nsars_C);


%jókat adtam be a függvénybe? teszt
teszt=[Ngmcs_in, nch, 0, ndmu, nbob, Va, e_0, vel, gamma];
a=teszt(1:60);
b=teszt(61:120); % nch
c=teszt(121);   % m=0 jelen esetben
d=teszt(122);    % ndmu=0.7079
e=teszt(123);  %nbob=0.6


% secure key függvények elkészítése
% a tömb 3. helyére adjuk meg m-et (vagyis a csatornaszámot) ---> utána plot-ba ki kell rajzolni
key0=secure_key([Ngmcs_in, nch, 0, ndmu, nbob, Va, e_0, vel, gamma]);
key1=secure_key([Ngmcs_in, nch, 1, ndmu, nbob, Va, e_0, vel, gamma]);
key38=secure_key([Ngmcs_in, nch, 38, ndmu, nbob, Va, e_0, vel, gamma]);
key50=secure_key([Ngmcs_in, nch, 50, ndmu, nbob, Va, e_0, vel, gamma]);


% nem logaritmikus ábrázolás
plot(z_km,key0),
hold on;


plot(z_km,key1),
hold on,


plot(z_km,key38),
hold on,
```

```
plot(z_km,key50),
hold off,


xlabel('távolság (km)'), ylabel('Secure key rate'), title('Secure key rate 0, 1, 38 és 50 csatornával'),
legend ('0 klasszikus','1 klasszikus','38 klasszikus','50 klasszikus');

% logaritmikus ábrázolás
plot(z_km,key0),
hold on,


plot(z_km,key1),
hold on,


plot(z_km,key38),
hold on,


plot(z_km,key50),
hold off,


xlabel('távolság (km)'), ylabel('Secure key rate'), title('Secure key rate 0, 1, 38 és 50 csatornával'),
legend ('0 klasszikus','1 klasszikus','38 klasszikus','50 klasszikus');
set(gca,'Yscale','log');
```

```
function kiadottfuggveny=secure_key(megadottak)


    %megadott adatok felhasználása
    kezdo_Ngmcs_in=megadottak(1:60);
    nch=megadottak(61:120);
    m=megadottak(121);
    ndmu=megadottak(122);
    nbob=megadottak(123);
    Va=megadottak(124);
    e_0=megadottak(125);
    vel=megadottak(126);
    gamma=megadottak(127);


    Ngmcs_in=m*kezdo_Ngmcs_in; %m=0-val 50 körül lesz, m=1-el 50 körül lesz m=38-al 10 körül lesz,
    ein=2.*nbob.*Ngmcs_in;  % Bobhoz eljutó zajfotonok száma   -- dt=1s-os időablak esetén 4.78*10^-8 ami nagyon kevésnek tűnik
    %plot(z_km,ein), xlabel('távolság (km)'), ylabel('fotonszám'), title('Matched módú Bobhoz eljutó fotonok száma '+m+' csatornaszám
esetén');
```

```
    % secure key rate:


    %adatok
    V=Va+1;                      % Alice által készített koherens állapot kvadratúra varianciája
    nvesszo=ndmu*nbob;           % Bob rendszerének hatékonysága
    e=e_0 + (ein/(nch*ndmu*nbob));
    lambda_line=(1./nch)-1+e;
    lambda_hom=((1+vel)./nvesszo)-1;
    lambda_tot=lambda_line+(lambda_hom./nch);


    %paraméterek:
    A=V^2.*(1-2.*nch)+2.*nch+nch.^2.*(V+lambda_line).^2;
    B=nch.^2.*(V.*lambda_line+1).^2;
    C= (V.*sqrt(B)+nch.*(V+lambda_line)+A.*lambda_hom)./(nch.*(V+lambda_tot));
    D=sqrt(B).* ((V+sqrt(B).*lambda_hom)./(nch.*(V+lambda_tot)));


    sigma1negyzet=1./2.*(A+sqrt(A.^2-4.*B));
    sigma2negyzet=1./2.*(A-sqrt(A.^2-4.*B));
    sigma1=sqrt(sigma1negyzet);
    sigma2=sqrt(sigma2negyzet);


    sigma3negyzet=1/2.*(C+sqrt(C.^2-4.*D));
    sigma4negyzet=1/2.*(C-sqrt(C.^2-4.*D));
    sigma3=sqrt(sigma3negyzet);
    sigma4=sqrt(sigma4negyzet);


    %nagyobb számítások
    lambda_be=teta((sigma1-1)./2) + teta((sigma2-1)./2) - teta((sigma3-1)./2) - teta((sigma4-1)./2);
    Iab=1/2.*log2((V+lambda_tot)./(1+lambda_tot));
    dI=gamma.*Iab-lambda_be;

    kiadottfuggveny=dI;


end

function ertek=dbvektortonumber(db)
    ctr=1;
    ertek=zeros(1,60);
    while(ctr<61)
        ertek(ctr)=10.^(db(ctr)./10);
        ctr=ctr+1;
    end
end
```

```
function db=vektortodb(ertek)
    ctr=1;
    db=zeros(1,60);
    while(ctr<61)
        db(ctr)=10.*log10(ertek(ctr));
        ctr=ctr+1;
    end
end

function ertek=dbtonumber(db)
    ertek=10^(db/10);
end


function watt=dbmtowatt(dbm)
    watt=10^((dbm-30)/10);
end


function dbm=watttodbm(watt)
    dbm=10*log10(watt)+30;
end


function dbm=wattvektortodbm(watt)
    ctr=1;
    dbm=zeros(1,60);
    while(ctr<61)
        dbm(ctr)=10.*log10(watt(ctr)+30);
    end
end


function eredmeny=teta(x)
    eredmeny=(x+1).*log2(x+1)-x.*log2(x);
end


function h2eredmeny=H2(x)
    h2eredmeny=-x*log2(x)-(1-x)*log2(1-x);
end


function feredmeny=f_fgv(x)
    feredmeny=x*1.22;
end
```