Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Szélessávú Hírközlés és Villamosságtan Tanszék

Erősített spontán emisszión alapuló kvantum-véletlenszámgenerátor

Készítette:
Marosits Ádám
Konzulens:
Schranz Ágoston, Matolcsy Balázs

Tartalomjegyzék

Bevezetés

A kvantumkommunikáció, illetve a kvantumtitkosítás manapság az egyik legaktívabban kutatott tudományterület. A mai kommunikációs rendszerek, valamint digitális adataink védelme megköveteli a kriptográfia ezen belül a különböző titkosítási eljárások, kulcsszétosztások fejlődését, amihez nélkülözhetetlen véletlenszámok használata. A véletlenszám-generátorok alkalmazási területei között megtaláljuk a szimmetrikus kulcsú titkosítást, banki tranzakciók védelmét, a Monte Carlo szimulációkat továbbá a kulcsszétosztó rendszereket, melyek jelentősége a kvantumszámítógépek korában rendkívül meg fog növekedni. Rendkívül sok helyen használnak költséghatékonysága miatt úgynevezett álvéletlenszám generátorokat (pseudo random number generator, PRNG) melyek véletlennek tűnő, de korántsem valódi véletlen bitsorozatokat állítanak elő, ugyanis a kezdőállapot függvényében determinisztikusan meghatározható a kimenet. Emellett léteznek olyan véletlenszám-generátorok, melyek valamilyen bonyolult fizikai folyamatokat mintavételeznek. Ilyen véletlenszám-generátorral generált számsorozatokhoz megfelelő mérésekkel mások is hozzájuthatnak. A kvantumfizika véletlenszerűsége és a mérések által okozott hullámfüggvény-összeomlás számos lehetőséget kínál nagy bitgenerálási sebességgel rendelkező generátorok létrehozására.

Léteznek nem optikai elven működő véletlenszám-generátorok is, melyek a kvantumos folyamatokhoz hasonlóan, tisztán véletlen folyamatot használnak ki. Ilyen generátor a radioaktív bomláson alapuló véletlenszám-generátor. Probléma ezzel, hogy a természetes eredetű sugárzás mértéke másodpercenként csak néhány detekcióhoz elégséges, emiatt nagy mennyiségű radioaktív anyagra van szükség, ami komoly biztonsági intézkedéseket feltételez, így is csak néhány Mbps -os sebesség érhető el. Egyéb véletlen folyamatok, melyek ugyan használhatók véletlenszám generálásra, nem felelnek meg a biztonságos és gyors generálás követelményeknek: Brown-mozgás, kaotikus áramkörök zaja, elektromos hőzaj.

Az optikai elven működő véletlenszám-generátorok közül is több különböző összeállítást különböztetünk meg. A teljesség igénye nélkül szeretném bemutatni a legjellemzőbbeket. Az első ilyen az útelágazáson alapuló- véletlenszám generátor, melynél fotonokat juttattunk egy olyan eszközre, mely véletlenszerűen továbbít utak egyikére. Mind a két út végén egy-egy detektor áll, és a véletlen bit értékét a detektor sorszáma határozza meg. A második ilyen lehetőség a fotonszámláláson alapuló véletlenszám-generátor, mely során egy T időablak alatt beérkező fotonokat számlálunk és egy előre meghatározott módon (pl.: paritásvizsgálattal) hozunk döntést. A harmadik lehetőségünk a beérkezési időn alapuló véletlenszám-generátor, melynél a fotonok beérkezése közti időkülönbségek fluktuációjából szeretnénk véletlen biteket kinyerni. Ez a módszer nagyban hasonlít a radioaktivitást használó véletlenszám-generátorokra, a különbség pusztán annyi, hogy részecskesugárzás helyett fotonokat használ, ami jóval biztonságosabb, továbbá egyes optikai architektúrák esetében sokkal nagyobb bitgenerálási sebességet érhetünk el, mivel nem a természetes eredetű sugárzás mértéke szab korlátot ennek. A fent vázoltak mellett nyilvánvalóan léteznek

másfajta optikai elven működő véletlenszám-generátorok is (pl.: Raman-szóráson, vákuumfluktuáción, vagy lézerek fáziszaján alapuló véletlenszám-generátorok), ám ezekre dolgozatomban nem térek ki.

Az általunk használt optikai elvű véletlenszám-generátor az erősített spontán emisszió [3] véletlenségén alapszik, mely módszerrel több kutatás is foglalkozott. Dolgozatomban szeretném bemutatni az általunk kidolgozott kvantum-véletlenszámgenerátort. Szó lesz a jelenség elméleti hátteréről, a kísérleti összeállításokról, a megfelelő mintavételezési frekvencia kiválasztásáról, az utófeldolgozás sikerességéről, valamint a valós idejű bitgenerálásról.

Elméleti áttekintés

Ebben a fejezetben szeretném bemutatni a kísérleteink során fellépő jelenségeket, azok elméleti hátterét, továbbá néhány korábbi cikket, amelyek hozzájárultak a megfelelő összeállítás, a mintavételi frekvencia kiválasztása, illetve az utófeldolgozás sikerességéhez.

1.1 Erősített spontán emisszió

Az optikai távközlési rendszerekben használt optikai erősítők, illetve lézerek jelentős része az indukált emisszió [2] jelenségét használja ki. Az indukált emisszió során a beérkező foton hatására a magasabb energiaszinten lévő részecske visszatér az alapállapotba és kibocsát egy, az eredeti foton tulajdonságaival megegyező fotont. Ilyen tulajdonság például az optikai frekvencia és az ezzel egyenesen arányos energia. Ahhoz, hogy az indukált emisszió legyen a domináns az egyéb fény-anyag kölcsönhatási jelenségekkel (abszorpció, spontán emisszió) szemben, populációinverzió szükséges. A populációinverzió során az aktív anyagok vagy ionok két ideális energiaszintjét különböztetjük meg: egy magasabb és egy alacsonyabb energiaszintet. Míg hőmérsékleti egyensúlyban az alapállapotban található a részecskék nagy többsége, inverzió során a részecskék többségének a magasabb energiaszinten, tehát gerjesztett állapotban kell lennie.

Ahogy azt fentebb említettem, az optikai erősítők ezt a jelenséget használják ki. Ilyen erősítők például a félvezető optikai erősítő (semiconductor optical amplifier, SOA), melynél árammal hozzák gerjesztett állapotba az elektronokat, illetve az erbium-ionokkal adalékolt optikai szálerősítő (erbium doped fiber amplifier, EDFA), ahol az erősítéshez szükséges energiát egy pumpáló fotonforrás biztosítja. Ezen fotonforrás hullámhossza eltér az erősítendő jelétől. Bemeneti jel hiányában, ha fennáll a populációinverzió, a gerjesztett állapotban levő részecskék egy része spontán, teljesen véletlenszerűen visszatér az alapállapotba, kibocsátva egy fotont, mely utána részt vehet az indukált emisszióban, tehát ebben az esetben az optikai erősítő a zajt is felerősíti. A bemeneti jel hiánya több okból is előnyös: nem szükséges kiszűrni a determinisztikus komponenseket, illetve az erősítésre használt energia szinte teljes mértékben a spontán emisszió felerősítésére fordítódik. Ezt a folyamatot nevezzük erősített spontán emissziónak (amplified spontaneous emission, ASE). A kibocsátott fotonok véletlenszerű tulajdonságokkal – például frekvenciával – rendelkeznek, így azok felerősített összessége, gyorsan fluktuáló zajként jelennek meg a kimeneten. Ezek a fotonok tehát nem korrelálnak a jelfotonok paramétereivel. Az erősített spontán emisszió jelensége nem írható le klasszikus elektrodinamikával, csak kvantumfizikai elveken, így eredően véletlenszerű folyamat, mely egyszerűen mérhető véletlen amplitúdójú jellé erősödik. Az ASE-n alapuló eszközök kiváló lehetőséget jelentenek valódi véletlen számokat generálására (true random bits, TRB). A bitgenerálási sebességet a legkisebb sávszélességű eszköz, általában a detektor korlátozza.

1.2 Más kutatócsoportok elrendezései

Williams et.al. [9] véletlenszám-generátorában az előzőnél egy komplexebb összeállítást használtak. ASE-forrásként egy erbium/itterbium-adalékolt optikai szálerősítő jelenik meg. Ezután ezen forrás szűrt jelét egy EDFA-n keresztül egy polarizációs osztóra vezetik. Ezzel egy kisebb sávszélességű nagy teljesítményű jelet kaptak. Az ASE-forrásból érkező jel polarizálatlan, tehát nincs szükségük kiegyenlítő áramkörre, így az ortogonálisan szétválasztott komponenseket egyetlen különbségképzővel szimmetrikus nulla középértékű jellé tudták alakítani. A fennmaradt minimális korrelációt önkésleltetésű XOR technikával sikerült minimalizálni. Ez azt jelenti, hogy az eredeti bitsorozat és az önmagával 20 bittel eltolt bitsorozat kizáró vagy kapcsolatát vették. Ezzel az összeállítással 12.5 Gbps generálási sebességet sikerült elérnie a kutatócsoportnak.

A Li et. al. [10] által 2011-ben bemutatott véletlenszám-generátor SLED (Superluminescent Light Emitting Diode)-et használ ASE-forrásként. Ezen forrás spektruma széles frekvenciasávban konstansnak tekinthető. Ezt kihasználva több hullámhosszcsatornára bontották a jelet, majd az ezeken a csatornákon megjelenő teljesítményt egy küszöbszinthez hasonlították, ennek eredményéhez rendeltek véletlen biteket. Utófeldolgozásként itt is az önkésleltetésű XOR technikát alkalmazták. Ezzel az elrendezéssel 20 Gbps bitgenerálási sebességet értek el, ez azonban több hullámhosszcsatorna párhuzamosításokkal tovább növelhető.

Kiemelkedően magas, 560 Gbps bitgenerálási sebességet sikerült elérni az Argyris et.al. [8] által bemutatott véletlenszám-generátornak. Ehhez egy egyszerű ASE-forrás-optikai csillapító-O/E átalakító összeállítást használtak. ASE-forrásként külön-külön vizsgálták egy bemenet nélküli SOA, illetve EDFA erősített spontán emissziós zajjelét. Ebben az összeállításban nem végeztek optikai előszűrést, a csillapítóval szabályozták a rendszer által leadott teljesítményt kihasználva, hogy a fotodetektor sávszélességén (12 GHz) belül a jel teljesítménye állandónak tekinthető. A bitek közti korreláció elkerüléséhez, egy XOR technikát alkalmaztak, majd az elektromos jelet 40 GSa/s sebességgel mintavételezték 16 biten. Az egyenletes eloszláshoz a 16 bitből 14-et megtartottak, ezzel elérve 560 Gbps generálási sebességet.

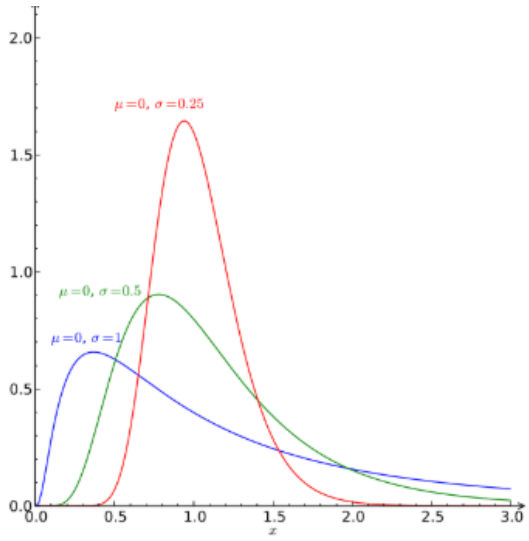
1,6 Tbps bitgenerálási sebességet értek el a 2013-ban, Liu. et. al. [12] által bemutatott véletlenszám-generátorral. Ebben az összeállításban az SLED jelét egy fotodiódára vezetve, az utófeldolgozással és a mintavételezéssel operálva értek el ilyen eredményeket. Első összeállításban 10 GHz (ennyi volt az általuk használt fotovevő sávszélessége) mintavételezéssel 32 bites kvantálással dolgoztak, ezzel 100 Gbps sebességet elérve. A 32 bitből a felső 12-t eldobták, ugyanis az MSB-k (most significant bit) növelték a hosszú idejű korrelációt. Egy második megoldásban 80 GHz-en mintavételezve nagy korrelációt tapasztaltak az egymáshoz közeli bitek között is, melyet hasonlóan az előzőekben megismerthez, XOR technikával csökkentettek, ezzel sikeresen teljesítették a NIST

teszteket (véletlenséget ellenőrző tesztek, lásd később), 1.6 Tbps bitgenerálási sebesség mellett.

Li et. al. [11] által 2014-ben bemutatott véletlenszám-generátor ASE-forrásként szintén egy SLED-et használ. Ez az összeállítás egy teljesítményosztóval két detektorra küldi a jeleket (az egyiket kissé késleltetve), majd ezen jelek különbségét képezve egy szimmetrikus eloszlású intenzitásfluktuációt kaptak. Ezzel a módszerrel 2.5 Gbps bitgenerálási sebességet értek el.

1.3 Intenzitásfluktuáció aszimmetriája

Rendkívül sok problémát okozott összeállításainkban az oszcilloszkópon megjelenő intenzitásfluktuáció aszimmetriája, emiatt döntöttem úgy, hogy egy nagyon rövid összefoglalót érdemel az elméleti áttekintésen belül. Az aszimmetria oka az, hogy a fotovevő kimenetén megjelenő, az optikai intenzitással arányos feszültségjel közelítően gamma-eloszlást követ.



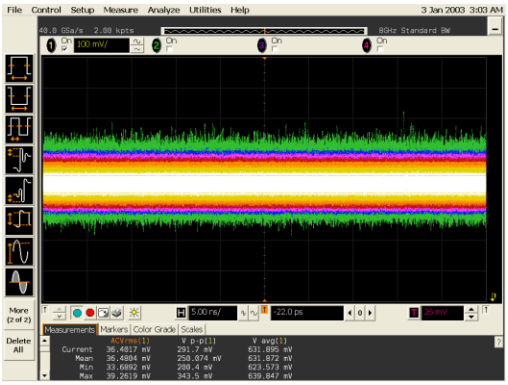
1. ábra Gamma-eloszlás különböző paraméterek esetén

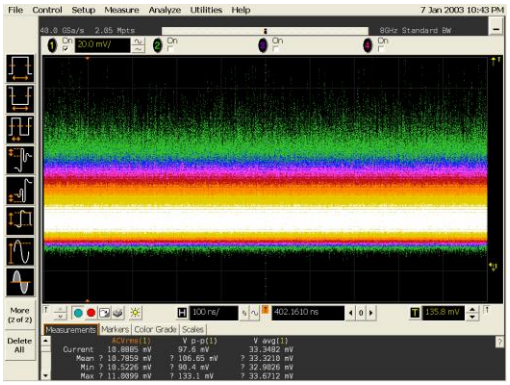
A p-edrendű λ paraméterű eloszlás sűrűségfüggvénye:

$$f(x) = \frac{\lambda^p \cdot x^{p-1} \cdot e^{-\lambda x}}{\Gamma(p)},$$

ahol Γ(p) a gamma-függvény, p és λ pedig az eloszlás két (pozitív) paramétere. Nagy paraméterek esetén ezen eloszlás a szimmetrikus normális eloszláshoz tart, ami biztosítja

számunkra az 1-es, illetve a 0-s bitek 50-50%-os megosztását, amennyiben a generált bitek meghatározását a középértékhez komparálással végezzük.





2. ábra A bal oldali ábrán látható a nagy átlagértékkel rendelkező, a jobb oldali ábrán kis átlagértékkel rendelkező intenzitásfluktuáció színskálás megjelenítése.

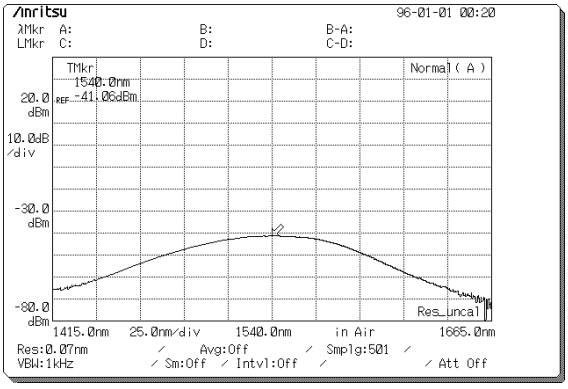
Felhasznált eszközök leírása

A következő pontokban szeretném bemutatni azokat az eszközöket, melyeket felhasználtunk kísérleteink során, a végső összeállítás megalkotásához hozzásegítettek.

2.1 SLED

Az SLED (Superluminescent Light Emitting Diode) egy optoelektronikai félvezető eszköz. A p-n átmenetben az elektron-lyuk párok rekombinációja során felszabaduló energiának megfelelő fotonokat kibocsátó dióda, és ahogy az spektrumából megállapítható, ASE elvén működik, mivel a fotonok, melyeket a dióda kibocsát, különböző hullámhosszúságúak, így nagyon széles spektrumot adnak. Az eszköz egy input nélküli félvezető optikai erősítőként is felfogható, ahol a gyenge spontán emissziót, az indukált emisszióval erősíti fel. Így beszélhetünk ASE-ról. A maximális teljesítménye 1550 nm körül van, ami egybeesik a manapság leggyakrabban használt távközlési sávval.

Az OMT laborban található SLED nem tudott elég teljesítményt leadni az EDFA bekapcsolásához, mivel utóbbi egy DWDM (dense wavelength division multiplexing) távközlési rendszer részét képezte, ahol fontos szempont az energiatakarékosság, így a jelnek megfelelő bemeneti teljesítménnyel kell rendelkezni, emiatt nem tudtuk felhasználni kísérleteinkhez. Az alternatívák kutatása során megtaláltuk azt a megoldást, hogy az input nélküli SOA, mely egy valódi optikai erősítő, tökéletesen helyettesítheti az SLED-et kísérleteinkben.

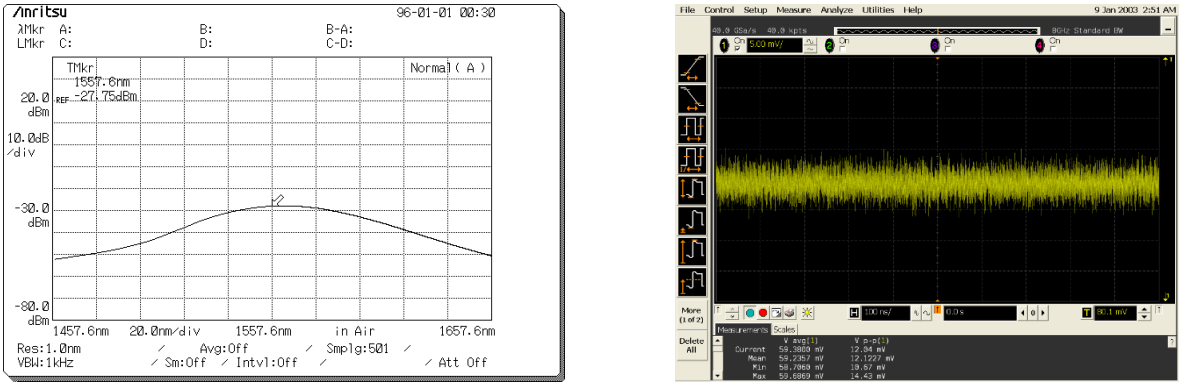


3. ábra SLED spektruma 25 °C-ra szabályozva, 125 mA gerjesztéssel

2.2 SOA

A SOA (Semiconductor Optical Amplifier) [4] egy indukált emisszió révén működő félvezető optikai erősítő, melynek spektruma és intenzitásfluktuációja (ahogy azt feljebb már említettem), bemeneti jel nélkül használva az SLED tulajdonságaira hajaz. Bemeneti jel hiányában az erősítő nem a beérkező fotonokra, hanem a saját spontán emissziójából származó fotonokra használja fel az erősítéshez akkumulált energiát, így ebben az üzemmódban ASE-zajforrásként funkcionál. Áramgerjesztéssel populáció-inverziót létrehozva az elektronok nagy része magasabb energiaszintre kerül, így az abszorpció helyett a spontán emisszió fog dominálni.

Hátránya az EDFA-val szemben, hogy sokkal kisebb erősítésre képes, így erősítőként nem fogadható el kísérleteinkben, viszont zajforrásként elég nagy teljesítménnyel rendelkezik az EDFA bekapcsolásához. Az alábbi, 4. ábrán látható a SOA ASE-spektruma. 220 mA-es, maximális előfeszítő áram esetén a konkrét eszköz spektrumának maximuma 1557,6 nm-en található, a spektrumkép jellege a hasonló eredet miatt hasonlít a szuperlumineszcens LED-éhez. A nagy sávszélesség miatt nem állt rendelkezésünkre pontosan kalibrált optikai teljesítménymérő, a teljesítményre csak körülbelüli értéket tudtunk mondani. Ez -6 dBm volt. A SOA-t mindig maximális árammal üzemeltettük, mert ez biztosítja az elegendő kimeneti optikai teljesítményt.

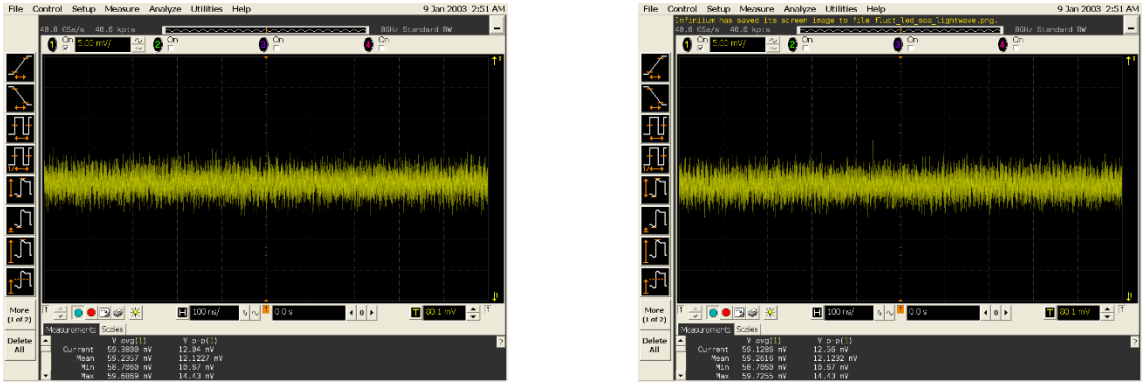


4. ábra A SOA spektruma 220mA gerjesztéssel, illetve időtartománybeli intenzitásfluktuációja

Érdekesség, hogy a SOA polarizációérzékeny erősítéssel rendelkezik. Ennek kiküszöbölésének egy lehetséges módja, hogy két erősítőt építenek egy eszközbe úgy, hogy a második erősítő az elsőhöz képest 90°-al elforgatott jelek erősítésére szolgál. Egy másik lehetséges megoldás, ha Faraday-rotátorral (magneto-optikai eszköz) a polarizációt a SOA erősítésének megfelelő síkjába forgatjuk.

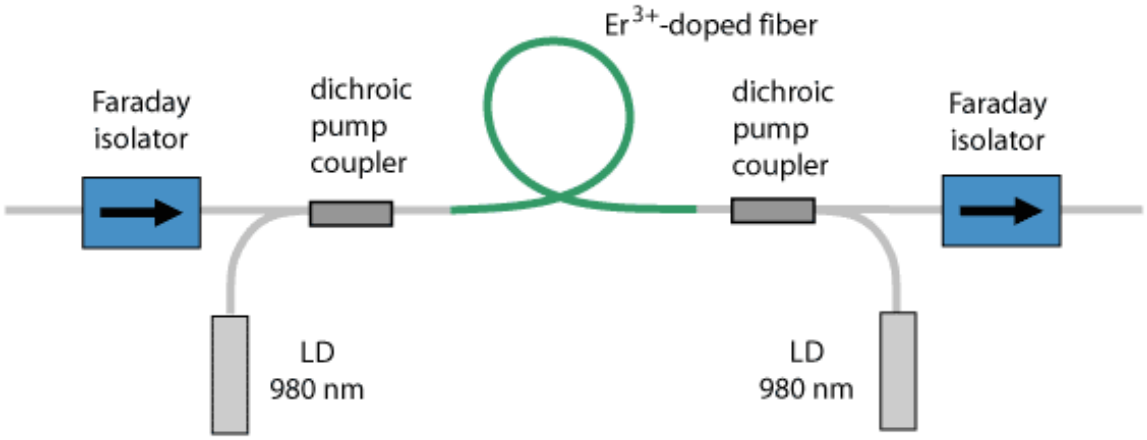
Felmerülhet a kérdés, miért nem erősítjük fel az SLED szűrt jelét SOA-val. Az 5. ábrán látható időtartománybeli intenzitásfluktuációk között nincs lényeges eltérés, sem átlagérték,

sem amplitúdó szempontjából, tehát az SLED használata nem indokolt a mérési elrendezésben.



5. ábra Időtartománybeli intenzitásfluktuációk: bal oldalon az SLED szűrt jelének SOA-val történő erősítése, jobb oldalon a SOA kimeneti intenzitásfluktuációja

2.3 EDFA

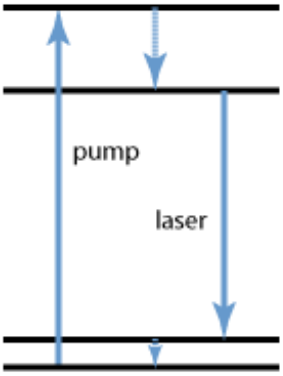


6. ábra EDFA blokkvázlata (forrás: rp photonics [5])

Az EDFA (Erbium Doped Fiber Amplifier) [5] egy erbium ionokkal (Er^{3+}) adalékolt optikai szálerősítő. Az elrendezése a 6. ábrán található. Az eszköz blokkvázlatán látható pumpáló lézerekre azért van szükség, hogy populáció-inverziót hozzunk létre a szálban. Ezek a lézerek általában vagy 980 nm-en, vagy 1450 nm-en működnek. Az ionok a gerjesztés után egy metastabil energiaszintre kerülnek, ahonnan indukált emisszió révén jutnak vissza az alapállapotba, így 1550 nm körüli fotonokat kibocsátva. Ezt a jelenséget a továbbiakban szeretném részletesebben ismertetni. Egy foton energiája az alábbi képlet alapján számítható ki:

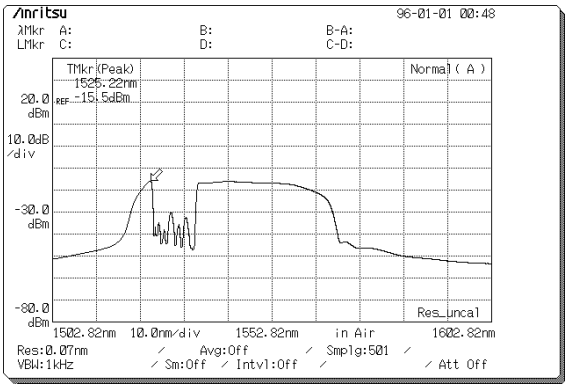
$$E = h \cdot f = \frac{h \cdot c}{\lambda}$$

Ebben az esetben látható, hogy a pumpáló lézerek egy magasabb energiaszintre helyezik az ionokat, amik nem radiatív módon visszatérnek egy metastabil állapotba, ahonnan már indukált emisszió révén jutnak vissza az alapállapotba. EDFA esetében a 7. ábrán látható kvázi-háromszintes [6] átmenetről beszélhetünk. Ekkor az alapállapot közelében lehet egy hőmérsékleti egyensúlyban lévő populáció, ekkor a metastabil állapotból visszatérő részecskék ebbe az állapotba térhetnek vissza, így kisebb energiájú fotonokat bocsátva ki, ezt az energiaveszteséget reabszorpciós veszteségnek nevezzük. A Faraday-izolátorok szükségessége a spontán emisszió során bekövetkező visszaverődések elkerülése miatt szükséges.



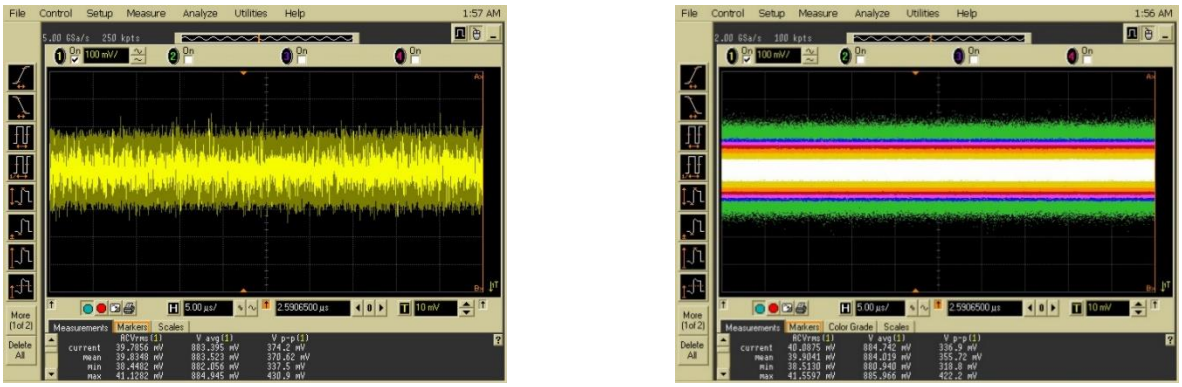
7. ábra Kvázi három szintes átmenet (forrás: rp photonics [6])

Az általunk használt EDFA maximális erősítése 1540 nm körül van (egy pontban eléri 1525,22 nm-en is, de az utószűrés során szélesebb sávot eresztünk át, így jobb, ha inkább az 1540 nm körül szűrünk). Mivel az erősítőnk egy DWDM-rendszer részét képezte, ahol fontos az energiatakarékosság, ezért alacsony, -29 dBm alatti teljesítményeknél nem kapcsol be, így az EDFA bemeneti jelének is elég nagy teljesítménnyel kell rendelkeznie.



8. ábra Az EDFA kimeneti jelének spektruma, bemenetén a SOA ASE-zajával (jellegre hasonló az EDFA saját spektrumához, melyet az adott eszközön nem tudunk mérni).

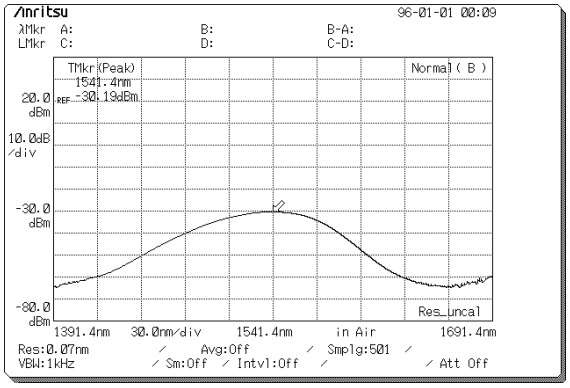
Optikai spektrumanalizátorral (8. ábra) és oszcilloszkóppal (9. ábra) megvizsgáltuk az EDFA-val erősített SOA kimeneti jelét. A 9. ábrán látható, hogy az időtartománybeli jel szinte teljesen szimmetrikus az átlagra (a fentebb leírt aszimmetrikusságot sikerült kiküszöbölnünk), ami a véletlenszám-generálás szempontjából előnyös. A fluktuáció mértékéhez képest magas egyenszint jellemzi, ami nem hordoz információt, ezt szűrőkkel vagy csillapítókkal próbáltuk orvosolni (viszont nem tudjuk teljesen eltüntetni, ha meg akarjuk tartani jelünk szimmetrikusságát). A peak-to-peak érték elegendően nagy ahhoz, hogy jó minőségű véletlen bitsorozatokat állítsunk elő (jelentősen meghaladja a vevőrendszer saját elektromos zajszintjét).



9. ábra Időtartománybeli intenzitásfluktuációk: A SOA jelének intenzitásfluktuációja EDFA-val erősítve: bal oldali ábrán egy adott időbeli realizáció, a jobb oldalin a perzisztens színskálás megjelenítés

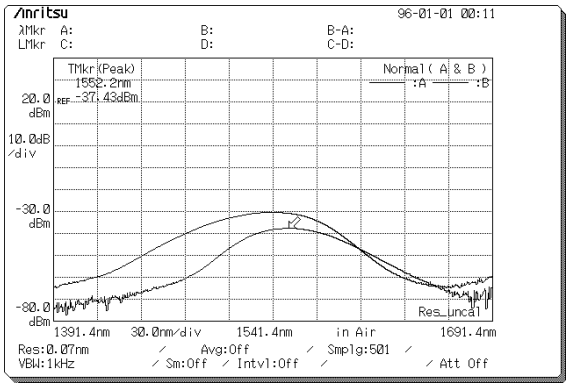
2.4 Perkin-Elmer nagyteljesítményű forrás

A rendelkezésünkre állt a laborban egy nagyteljesítményű forrás (továbbiakban HPS, high power source), melynek belső működése ismeretlen. Viselkedésére kimeneti jelének a széles spektrumából (10.ábra) és annak alakjából következtettünk, az SLED-hez hasonlóan szintén erősített spontán emisszió elvén működik.



10. ábra HPS ASE-spektruma

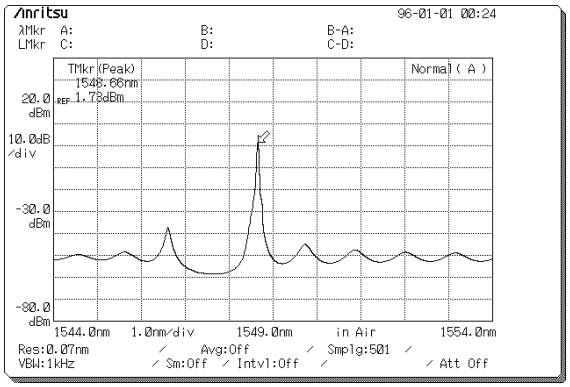
A 11. ábrán a SOA ASE-zajspektrumának és a HPS spektrumának összehasonlítása látható. Utóbbi maximuma 8-9 dB-el nagyobb teljesítményű, mint a SOA-é, így zajforrásként nemcsak teljes mértékben kiválthatja a SOA-t a további kísérletekben, hanem előnyösebb tulajdonságokkal is bír annál. Ennek ellenére önálló eszközként nem tudjuk használni, mivel az intenzitásfluktuáció nem rendelkezik elegendően nagy peak-to-peak értékkel. A HPS jele lesz a következőkben az EDFA bemenetén, amivel már elérjük a kívánt értéket. A forrás teljes optikai teljesítménye körülbelül 0,75 dBm, de a széles spektrum miatt itt sem tudunk pontos értéket mérni.



11. ábra SOA, illetve HPS spektrumának összehasonlítása (a nagyobb csúcsértékkel rendelkező a HPS spektrum)

2.5 DWDM lézer

Tipikus lézerműködéssel bíró kis vonalszélességű egy longitudinális módusú lézerről van szó, mely megfelel a DWDM szabványnak. A lézert 20 mA munkaponti áram mellett üzemeltetve, hőmérsékletét 25 °C-ra szabályozva a 12. ábrán látható spektrumképet kaptuk. A teljesítmény nagy hányada (kb. 1,73dBm) az 1548,66 nm-es hullámhossz közelében összpontosul. A mért összteljesítménye körülbelül 1,9 dBm.

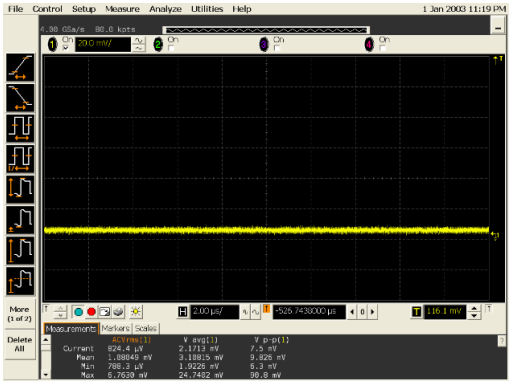


12. ábra DWDM lézer spektrumképe

2.6 Lightwave converter

A lightwave converter egy optikai-elektromos átalakító, mely a benne lévő fotodióda segítségével a beérkező optikai teljesítményt alakítja elektromos feszültséggé. A mi összeállításunkban az oszcilloszkóp és az optikai rendszer összeköttetéséért felel. A fotodióda egy fényérzékeny dióda, mely a fotoeffektus szerint működik: a vegyértéksávban lévő elektronok a beérkező fotonok hatására a vezetési sávba kerülnek (a fotonok kiütik őket a vegyértéksávból). A fotodióda tehát a beérkező fotonokat elnyeli (abszorpció történik) és ennek hatására elektromos töltéshordozók keletkeznek (értelemszerűen itt is felléphet egyfajta konverziós veszteség, hiszen a bejövő fotonoknak csak egy része képes elektronokat generálni). Így azt mondhatjuk, hogy a fotodióda kimenetén lényegében egy áram (fotoáram) indul meg, ezt az áramot egy transzimpedancia-erősítő segítségével alakítják elektromos feszültséggé. Az elektromos feszültség az intenzitással, tehát a térerősség négyzetével lesz arányos.

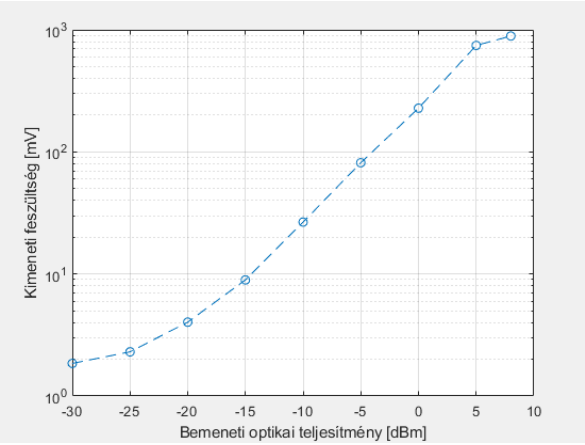
A többi elektromos eszközhöz hasonlóan az optikai vevőnk is rendelkezik saját elektromos zajjal (13. ábra). Ez a zaj a mi esetünkben 3mV átlagfeszültségű volt, emiatt lényegében elhanyagolhatjuk, hiszen az ASE-zajforrásunk intenzitásának fluktuációja két nagyságrenddel nagyobb.



13. ábra Lightwave converter zaja

Sokkal nagyobb problémát okozhat vevőnk telítődése, ugyanis a téves mérési eredmények mellett az eszközünk is elromolhat, ha túl nagy optikai teljesítményt teszünk a bemenetére. Telítődésről akkor beszélhetünk, ha az optikai teljesítmény növelésének hatására a kimeneten megjelenő elektromos feszültség nem képes lineárisan nőni. A laborban található fotovevő teljesítmény-feszültség karakterisztikája a 14. ábrán látható, az értékek az 1. táblázatban vannak összefoglalva. A fotodióda P-V karakterisztikája 5 dBm-ig lineáris, 5 dBm felett nem nő tovább ugyanolyan linearitással, tehát a telítődés itt következik be. Ebből levonva a konklúziót az optikai rendszerünk kimenetén megjelenő teljesítménynek 5 dBm-nél kisebbnek kell lennie, viszont a fentebb tárgyalt aszimmetria elkerülése

érdekében a lehető legnagyobb, még telítést el nem érő teljesítménnyel kell rendelkeznie, ezt az összeállításoknál figyelembe vettük.

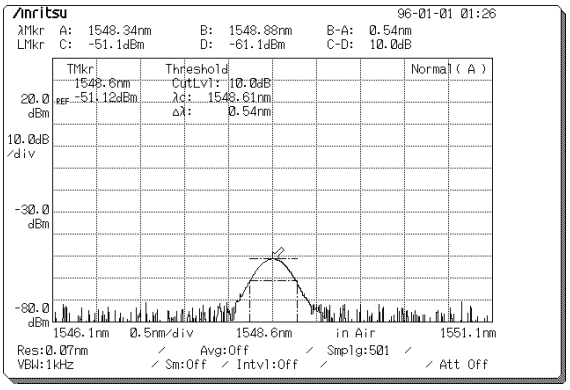


14. ábra Lightwave converter P-V karakterisztikája

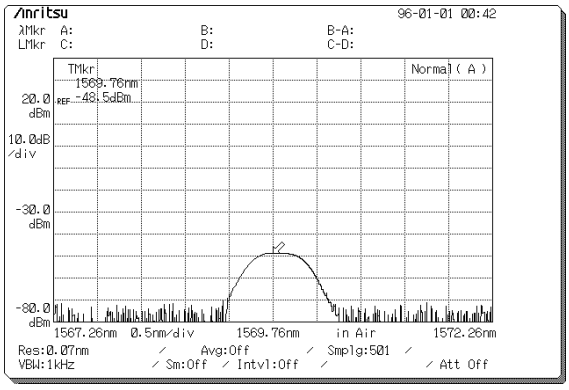
Bemeneti optikai teljesítmény [dBm]	Kimeneti átlagfeszültség [mV]
-30	1,85
-25	2,3
-20	4,03
-15	8,93
-10	26,6
-5	81,5
0	228
5	745
7.2	889

2.7 Optikai szűrők

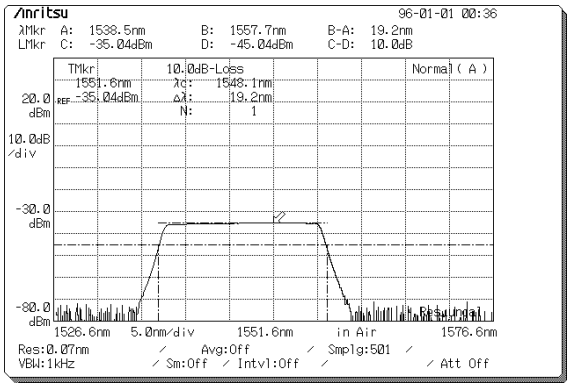
A feleslegesen nagy egyenszint elkerülése és az ehhez képest nagy fluktuáció elérése érdekében szűrőket alkalmazunk. Az OMT-laborban több szűrő is található, ezek mindegyikét megvizsgáltuk. A következőkben szeretném ismertetni az egyes szűrők jellegzetességeit, kitérve a sávszélességre, a beiktatási csillapításra, illetve a hangolhatóságra. Célunk egy olyan szűrő megtalálása volt, mely elegendő teljesítményt enged át ahhoz, hogy elkerüljük a fent említett időtartománybeli intenzitásfluktuáció aszimmetriáját, viszont eleget szűr le a jelünkből ahhoz, hogy ne vigyük telítésbe a fotovevőt. Az alábbi ábrákon látható a különböző szűrők átviteli karakterisztikája. Bemenetként a SOA zaját használtuk, hiszen ezen eszköz teljesítménye konstansnak tekinthető az összes szűrő sávszélességében. A SOA gerjesztése minden esetben 246 mA, hőmérséklete 25 °C volt.



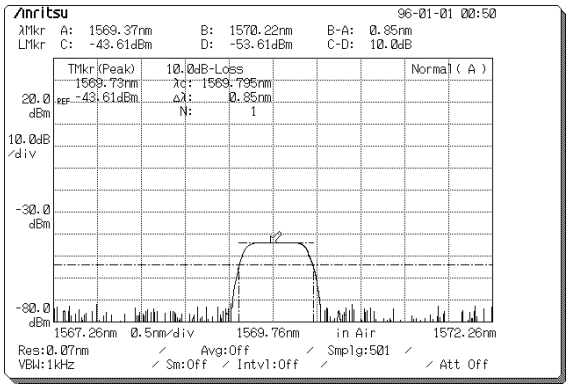
15. ábra OTF



16. ábra Yenista XTM-50



18. ábra CWDM ADM



17. ábra DWDM Demultiplexer

OTF

Hangolható szűrő, mely 1548 nm sávközepi hullámhosszra állítottunk. Sávszélessége fix 0,54 nm. Beiktatási csillapítása 1556 nm-en 5,2 dB.

Yenista XTM-50

Szintén hangolható, melyet 1551,9 nm sávközepi hullámhosszra állítottunk, ezen szűrő előnye az előzőhöz képest, hogy a sávszélessége is állítható, ezt mi a legnagyobb, 0,85 nm-re állítottuk, hogy a lehető legtöbb teljesítményt tudjuk a rendszerből kivenni.

CWDM add-drop multiplexer

A CWDM (coarse wavelength division multiplexing) add-drop multiplexer drop csatornája a CWDM szabványból ismert, kb. 20 nm sávszélességgel rendelkező sáváteresztő szűrő. A nagy sávszélesség előnyös lesz kísérleteinkben, hogy a lehető legtöbb teljesítményt tudjuk kinyerni a rendszerből, mely az aszimmetria elkerülése miatt jelentős számunkra. Több csatornával rendelkezik, ezek közül mi az 1550 nm körülit használtuk, a sávszélesség itt 19,2 nm-re adódott. Beiktatási csillapítása gyakorlatilag elhanyagolható.

DWDM demultiplexer

A DWDM demultiplexer a DWDM szabványból ismert, kb. 0,8 nm sávszélességgel rendelkezik. A multiplexerünk több különböző csatornával rendelkezik, melyek mind más

sávközépi hullámhosszal rendelkeznek. 1556,1 nm-en 9,6 dB beiktatási csillapítás adódott, ami a többi szűrőhöz képest kiemelkedően sok.

2.8 ESP8266 mikrokontroller

Egy WiFi chippel rendelkező egyszerű mikrokontroller, mely processzorának órajele választható 80 MHz és 160MHz közül. Számunkra fontos tulajdonsága, hogy rendelkezik UART (Universal asyncronous receiver-transmitter) ki-, illetve bemenettel, valamint egy 10 bites ADC-vel, mely 0 V és 3.3 V között képes működni (ténylegesen 0 V és 1 V között, viszont rendelkezik egy feszültségosztóval a bemenetén).

2.9 Raspberry Pi 3 B+

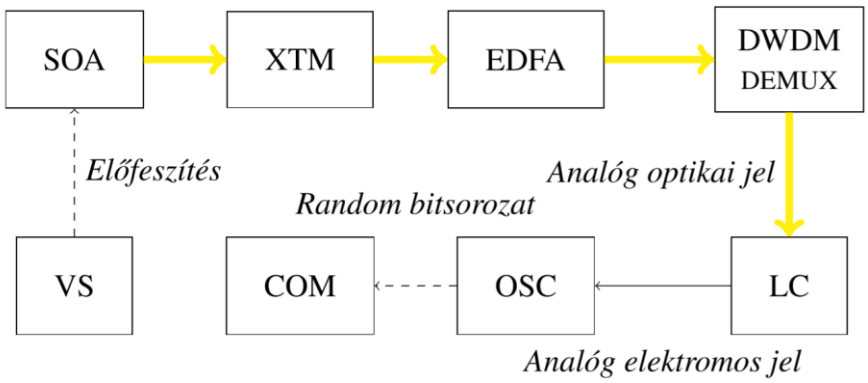
Egy miniszámítógép 64 bites, 4 magos 1.4 GHz-es processzorral rendelkezik, weboldal létrehozása céljából használtuk. Mivel nem rendelkezik ADC-vel, így a demo weboldal létrehozása érdekében az ESP8266-ot használtuk az analóg jelünk mintavételezésére, mellyel UART portjain keresztül kommunikált.

Összeállítások vizsgálata

Ebben a részben szeretném bemutatni az általunk kipróbált összeállításokat. Ezen kísérleti összeállítások a végső véletlenszám-generátor prototípusainak tekinthetők, ezek alapján sikerült tökéletesítenünk saját rendszerünket. Az összeállításokat két nagy csoportra bonthatjuk: vannak olyan elrendezések, melyek a SOA-t használják ASE-forrásként, és vannak olyanok, melyek a Perkin-Elmer nagyteljesítményű forrást (HPS). Kezdetben az SLED-el kísérleteztünk, viszont ezen eszköz teljesen mellőzve lett kis teljesítménye miatt, ami nemcsak a véletlen bitek minőségi generálásához nem volt elég, de még az EDFA-t sem sikerült vele bekapcsolni, emellett a SOA-ra bemenetként kötve teljesen elnyomta a félvezető erősítő eszköz saját zaja. Ezen okok miatt az ezzel az eszközzel készült elrendezéseket nem is ismertetem.

3.1 SOA alapú elrendezések

3.1.1 Első változat

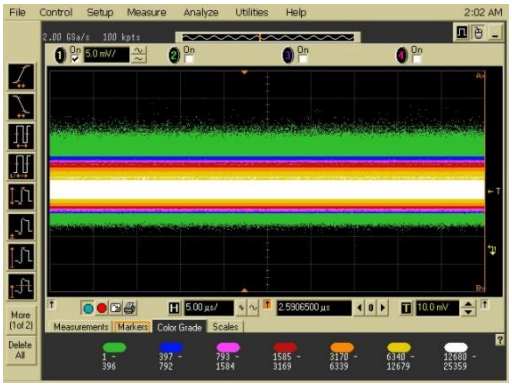


Legelső összeállításunkban ASE-forrásként a félvezető optikai erősítőt használtuk, viszont ahogy azt a felhasznált eszközök bemutatása során már megmutattuk, a SOA zajteljesítménye, illetve fluktuációja (4. ábra) nem elég nagy ahhoz, hogy megfelelő minőségű véletlen biteket tudjunk generálni, viszont ahhoz elég, hogy az EDFA-t bekapcsolja (P_{zaj} > -29 dBm). Ha közvetlenül az EDFA bemenetére kötöttük volna a SOA kimenetét, a nagy sávszélesség miatt a kimeneti teljesítmény nagy hányadát képezné az EDFA saját zaja (ami egyébként szintén egy ASE zaj, tehát nem okozna problémát, pusztán szerettük volna, ha a SOA-t használnánk valódi ASE-forrásként), ezért egy szűrőn keresztül vezettük rá (XTM, sávközepi hullámhossz 1553 nm, 0,92 nm-es sávszélesség). Figyelnünk kellett, hogy az EDFA leszívási tartományától (8. ábra) elegendően távol legyünk. Az EDFA után található a DWDM szűrő, melynek a 25-ös csatornáját használva (sávközepi hullámhossz 1552,8 nm, DWDM szabvány szerinti 0,8 nm-es sávszélesség) újra leszűrtük a jelünket. Ezt annak érdekében tettük, hogy az EDFA-ból kijövő teljesítmény jóval nagyobb,

mint amennyit a vevő telítődés nélkül elbírt volna. Ezután egy optikai-elektromos átalakító segítségével elektromos feszültséggé alakítottuk az optikai teljesítményt, majd ezt egy oszcilloszkópon megvizsgáltuk.

Konklúzió az elrendezéssel kapcsolatban

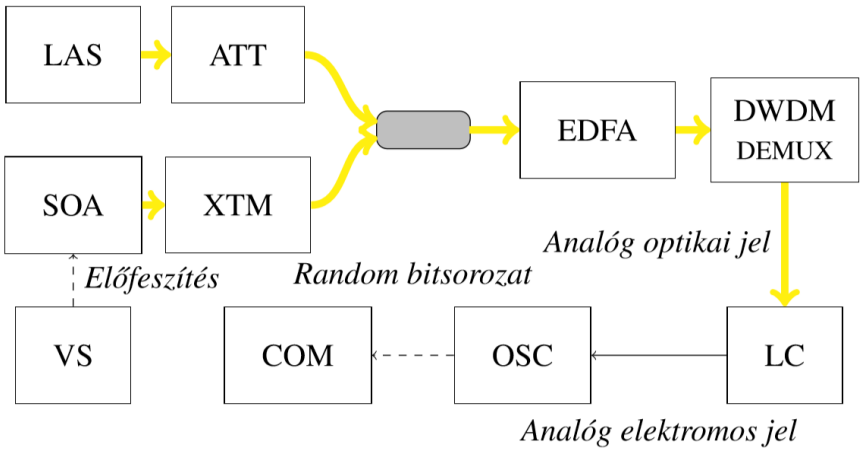
Az első elrendezésünknél három súlyos problémával találtuk szemben magunkat. Az első ilyen az XTM szűrő kimenetén megjelenő kb. -28,7 dBm teljesítmény volt, ugyanis ez teljesen az EDFA bekapcsolási határán (-29 dBm) mozog, és a zajszint ingadozása (pl.: hőmérsékleti viszonyok miatt) erősen befolyásolja a teljesítményt, így az EDFA nem minden esetben kapcsolt be. A második probléma az erősen aszimmetrikus intenzitásfluktuáció volt, ami kiegyenlítetlenséget okozott az 1-es, illetve 0-s bitek között (amennyiben a mintákat az átlaghoz komparálva vizsgáljuk). A harmadik gond az összeállítással, hogy az EDFA saját zaja csak kis mértében van elnyomva a SOA szűrt jeléhez képest. Mivel az EDFA is egy ASE-forrás, ez nem okoz nagy problémát és egy utószűrővel könnyedén megoldható.



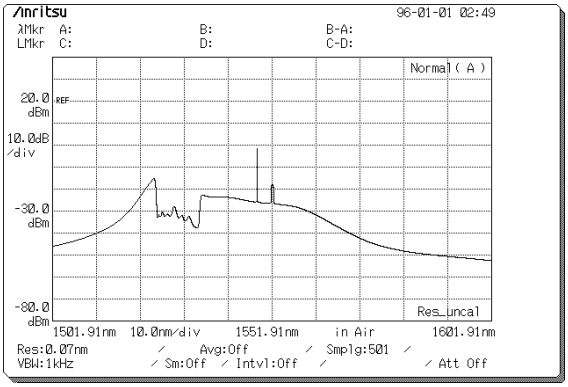
19. ábra Az összeállítás teljesen aszimmetrikus intenzitásfluktuációja

3.1.2 Második változat

A második változattal szerettük volna kijavítani az első változat hibáit (nagyobb bemeneti teljesítmény az EDFA-ra, EDFA saját zajának elnyomása, illetve aszimmetria elkerülése). Ahogy lentebb látható, a kísérleti összeállítás szinte teljesen megegyezik, azt leszámítva, hogy használtunk egy DWDM lézert is. Ennek oka az, hogy az EDFA eddig a teljes zajszintet erősítette, így arra gondoltunk, ezzel a megoldással az erősítésre szánt energia a DWDM lézer, illetve a szűrt SOA jelének hullámhosszán összpontosulna. Ezzel csökkenne az egyenszint, nőne az AC-szint, és a szűrés után is több teljesítményünk maradna.



Mivel a DWDM lézer egy megadott hullámhosszon működik, így csak a SOA saját zajából nyert szűrt jelet tudtuk másik hullámhosszra tenni az elkülöníthetőség érdekében. Utóbbit az 1569.76 nm hullámhosszra hangoltuk, ami a demultiplexer 9-es csatornájának felel meg. A DWDM lézer előtti csillapítóra azért van szükség, mert ha túl nagy a lézer teljesítménye a szűrt ASE zajhoz képest, akkor utóbbit nem fogja erősíteni az EDFA. A csillapítót 30 dB-re hangoltuk, de még így sem volt elegendő ahhoz, hogy megfelelő mértékben elnyomja a lézer jelét. A másik megoldás szerint hanyagoltuk a csillapítót, viszont 20 mA helyett 13 mA-el gerjesztettük, ami ugyan elég lett volna a megfelelő elnyomáshoz, de ugyanabba a problémába ütköztünk, mint a 30 dB-nél nagyobb csillapításnál: az eszközünk nem kapcsolt be. Ebben a hozzáadott SOA jel sem tudott segíteni, ugyanis ezen a hullámhosszon már jóval alacsonyabb volt a SOA zajteljesítménye. A 20. ábrán látható, hogy a SOA teljesítménye nem tud dominálni, sem az EDFA saját zajához, sem a 20 mA-el gerjesztett csillapítatlan DWDM lézer erősített teljesítményéhez képest.



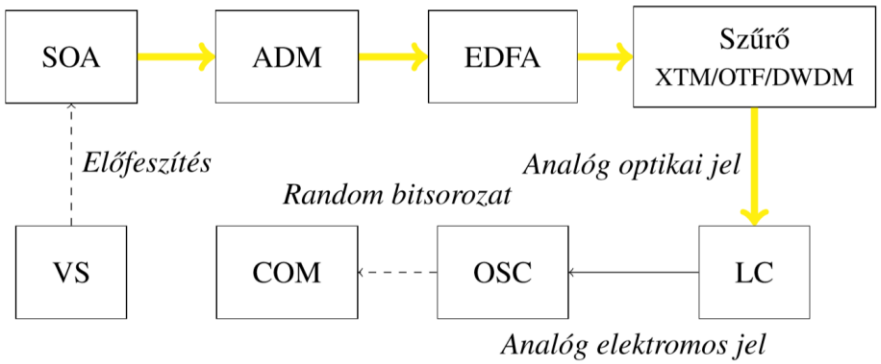
20. ábra A SOA, illetve a DWDM lézer spektruma, EDFA-val erősítve

Konklúzió az elrendezéssel kapcsolatban

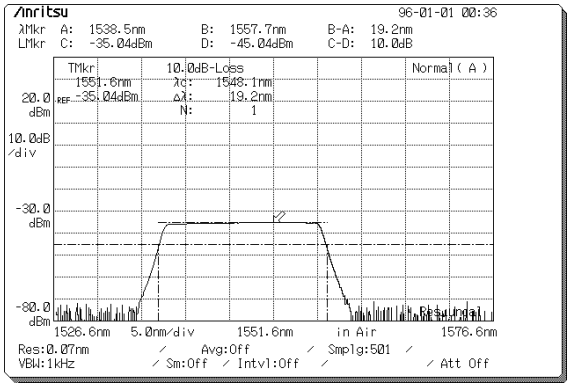
A fentebb említett okok eredményeképp ezt a megoldást elvetettük, mert egyik problémát sem tudta megoldani.

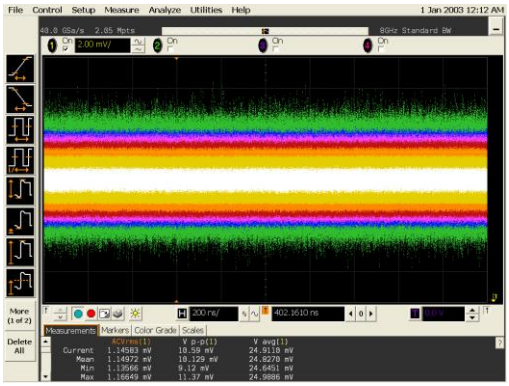
3.1.3 Harmadik változat

Ezzel a megoldással is ugyanazt a három problémát szerettük volna elkerülni, mint az előbbivel: az EDFA-ra elegendően nagy teljesítmény érkezzen, szerettük volna jobban kiemelni a SOA ASE zaját, továbbá elkerüljük az oszcilloszkópon megjelenő amplitúdó eloszlásának aszimmetriáját.



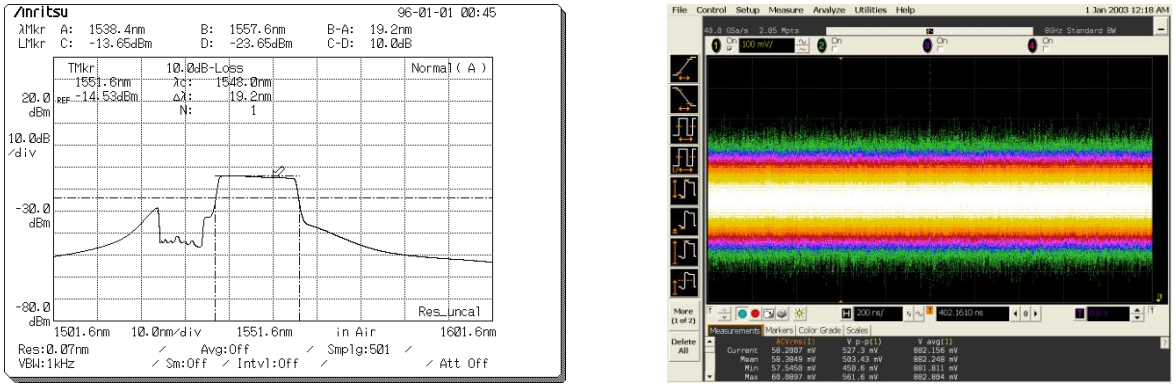
Ezen megoldás lényege, hogy minél nagyobb teljesítményt szerettünk volna rákötni a fotovevő előtti szűrőnkre, ugyanis ahogy azt az elméleti összefoglalóban már taglaltam az aszimmetria a gamma eloszlás paramétereitől függ, ami a mi esetünkben az átlagteljesítmény növelésével hasonlít egyre jobban a normális eloszláshoz. Ehhez egy nagyobb sávszélességű (CWDM szabvány: 20 nm) szűrővel próbálkoztunk, ami garantálja az EDFA bekapcsolását, továbbá nagyobb teljesítményt biztosít az EDFA kimenetén is. A SOA-t 250 mA árammal gerjesztettük, kimenő jelét tehát egy CWDM add-drop multiplexerrel szűrtük le.





21. ábra A SOA CWDM add-drop multiplexerrel megszűrt jelének spektrális, illetve időtartománybeli jele

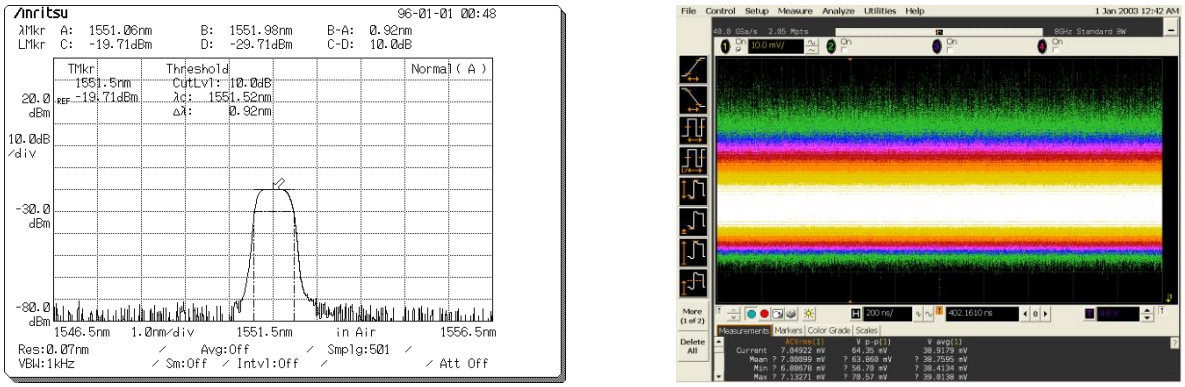
A jel csúcsteljesítményéhez tartozó hullámhossza 1548,1 nm, a multiplexer kimeneti összteljesítménye pedig -10,01 dBm, ami bőven elegendő ahhoz, hogy bekapcsolja az EDFA-t. Az intenzitásfluktuáció időtartománybeli képéről leolvasható, hogy 24,8 mV-os átlagérték, illetve 10,1 mV-os peak-to-peak értékkel rendelkezik, az amplitúdóeloszlás teljesen szimmetrikus. Ez már egy elfogadható jel lenne kicsit nagyobb AC-értékkel. Ehhez erősítőként az EDFA-t használjuk, ami nagymértékű erősítést visz a rendszerbe: a kimeneti jel teljesítménye 1551,6 nm-en -14,53 dBm, viszont a SOA szűrt sávján kívül is nagy zajteljesítményt ad le. Az 1525 nm körüli csúcs elnyomása kb. 15 dB, ami az első megoldáshoz képest 11 dB-es javulást jelent. Ahogy már fentebb említettem, a kisebb és nagyobb hullámhosszon megjelenő komponensek eltávolítására egy utószűrőt fogunk használni. A detektált jel, illetve a spektrális kép az EDFA kimenetén megjelenő jelről a 22. ábrán látható, ahol észrevehető, hogy sokkal nagyobb energia fordítódik erősítésre, mint az előző esetekben. Ahogy lentebb látható az intenzitásfluktuáció nagy egyenszinttel (882 mV), ami számunkra nem előnyös, hisz ezen érték nem hordoz információt, viszont nagy peak-to-peak, illetve AC_{RMS} értékkel rendelkezik (503, illetve 58,4 mV). A fluktuáció színskálás megjelenítésén látszik, hogy a jelünk egyáltalán nem aszimmetrikus. További feladatunk az utószűrő kiválasztása volt.



22. ábra Az EDFA kimenetén megjelenő spektrális, illetve időtartománybeli jel

Yenista XTM

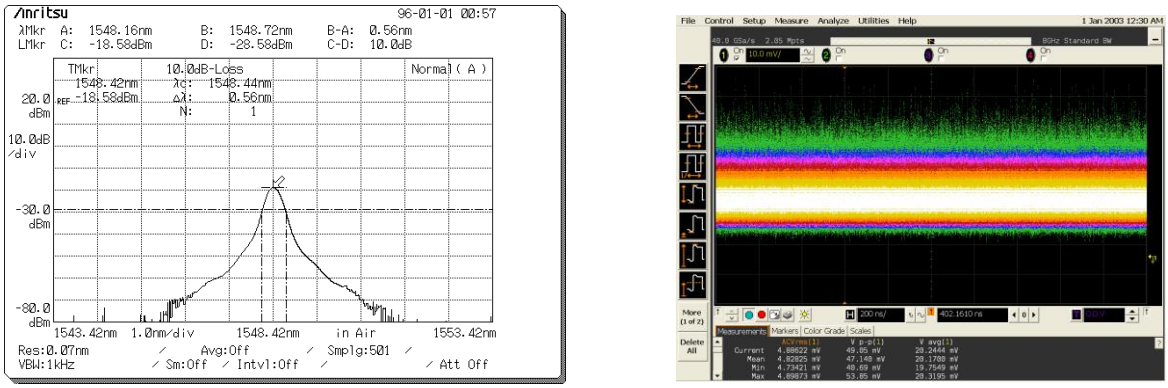
Az XTM szűrőt a 1551,5 nm hullámhosszra hangoltuk, itt -19,7 dBm kimeneti teljesítményt értünk el. Az elért 38,76mV-os átlagérték, illetve fluktuáció (a peak-to-peak érték 63,86 mV, az AC_{RMS} kb. 7 mV) a legnagyobb a három szűrő közül, azonban az aszimmetria újra megjelent a detektált amplitúdóeloszlásban, így ezt a megoldást is el kellett vetnünk. (Később kiderül, hogy a másik kettővel együtt).



23. ábra A SOA alapú elrendezés spektrumképe, illetve időtartománybeli intenzitásfluktuációjának színskálás megjelenítése Yenista XTM-50 utószűrőt alkalmazva

OTF

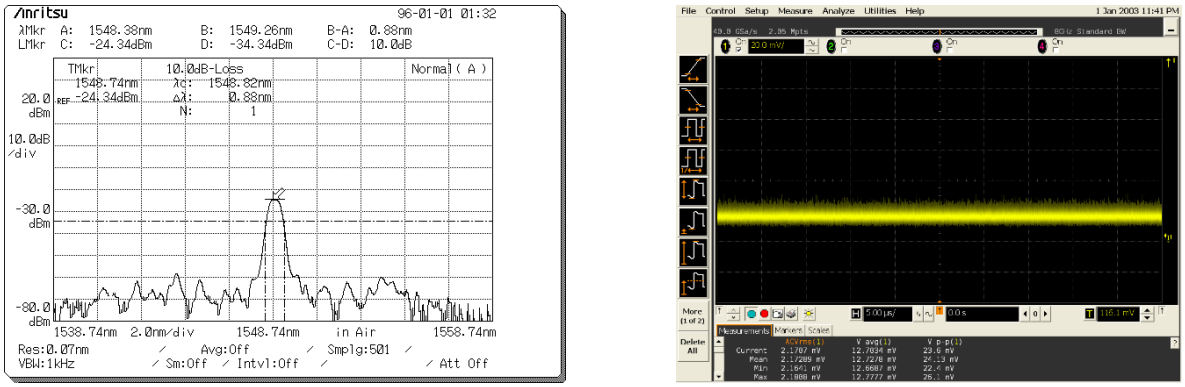
Második szűrőként az OTF szűrőt használtuk. Ezen hangolható szűrőt 1548,42 nm-re állítottuk, a teljesítmény -18,58 dBm, ami a csúcsteljesítmény a szűrő kimenetén. A detektált jelünk paraméterei: az átlagérték 12,7 mV-re, a peak-to-peak érték 24,1 mV-ra, az AC_{RMS} 2,2 mV értékre adódott. Természetesen, ahogy a fentebb vázolt esetben, itt is megjelent az időtartománybeli jelünk aszimmetriája.



24. ábra A SOA alapú elrendezés spektrumképe, illetve időtartománybeli intenzitásfluktuációjának színskálás megjelenítése OTF utószűrőt alkalmazva

DWDM demultiplexer

A DWDM szűrő 20-as csatornáját használtuk (1548,7 nm), itt az optikai teljesítményre 4,6 dB-el kisebb érték adódott, mint az első esetben. Az optikai teljesítmény csökkenésének hatására csökkent az átlagérték (12,7 mV), peak-to-peak (24,1 mV), illetve az AC_{RMS} (2,2 mV) érték is. Ahogy az várható, itt is megjelent a gamma-eloszlásra kis paraméterek esetén jellemző aszimmetria, így ezt a megoldást is elvetettük.



25. ábra A SOA alapú elrendezés spektrumképe, illetve időtartománybeli intenzitásfluktuációjának megjelenítése utószűrőként DWDM demultiplexert alkalmazva

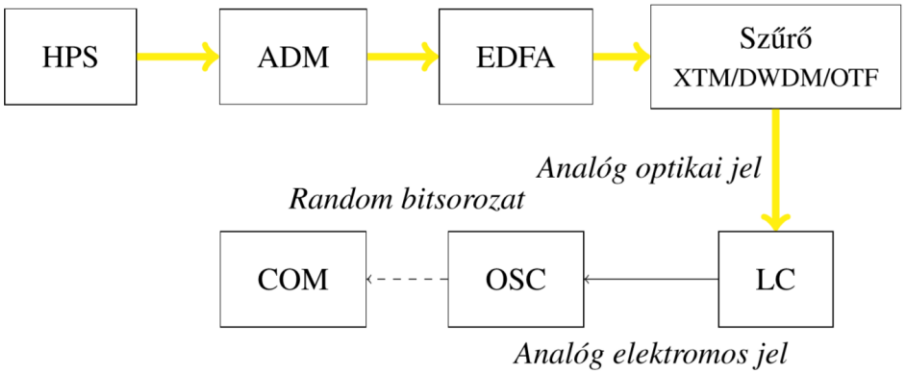
Konklúzió az elrendezéssel kapcsolatban

Tanulságként a következőt fogalmazhatjuk meg: ezen szűrők közül az XTM szűrő a legjobb választás, hiszen a legnagyobb fluktuációt itt értük el. Ennek ellenére láthatjuk, hogy további összeállításokat kell keresnünk, ugyanis, habár a három probléma közül kettő megoldódott, az aszimmetria még mindig fennáll. Ez a megoldás jó alapot szolgált a HPS alapú elrendezésekhez, illetve az utószűrő kiválasztásában is sok tanulságot hordozott.

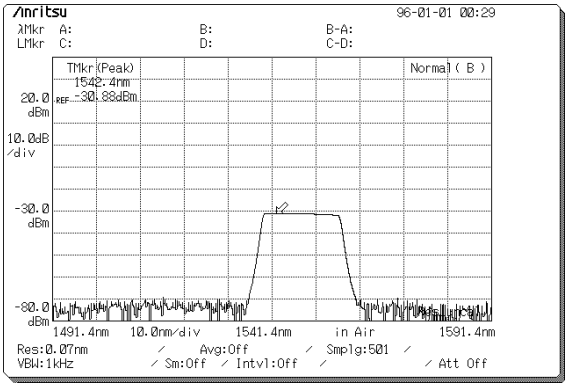
3.2 HPS alapú elrendezések

3.2.1 Az első elrendezés

Az előző fejezetben láthattuk, hogy azok az elrendezések, melyek ASE-forrásként a SOA-t használják, nem vezettek megoldásra. A kísérletezések közben hozzájutottunk a Perkin-Elmer nagyteljesítményű forráshoz, melynek spektruma nagyon hasonlít a SOA-ra (tipikus, széles ASE-spektrum), csak abban különbözik, hogy a HPS nagyobb teljesítményt képes leadni (kb. 10 dB-el), mint a maximális előfeszítő árammal gerjesztett SOA. Spektrumaik összehasonlítása a 11. ábrán látható. A SOA-nál megismert elrendezések közül értelemszerűen az utolsót használjuk fel. Az elrendezés az alábbi ábrán látható, ahol már a HPS szerepel ASE-forrásként. Ezen összeállítást részletesebben fogom bemutatni, hiszen ez lesz a végső, tökéletesen megfelelő kialakítás alapja.

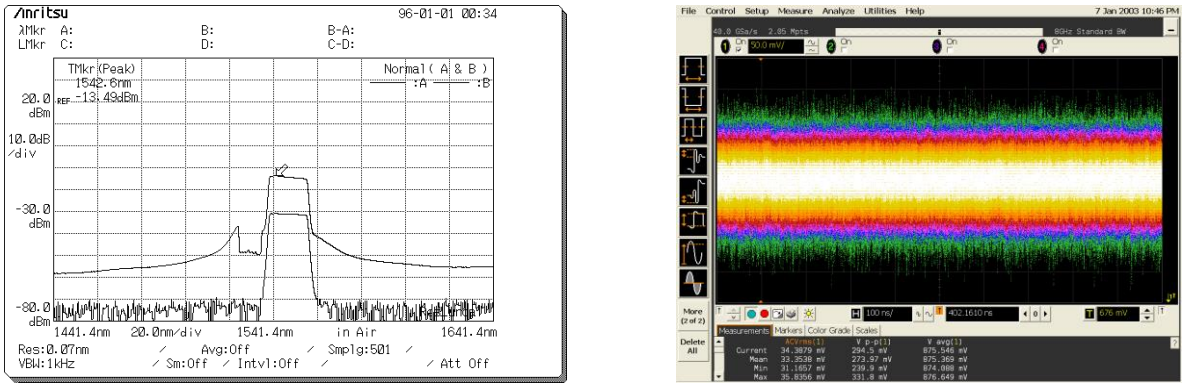


Az ASE-forrás után az előző elrendezéshez hasonlóan a CWDM add-drop multiplexert használtuk, mellyel egy kb. 20 nm szélességű sávot kivágva a forrás spektrumából a 26. ábrán látható spektrumképet kaptuk. A szűrt, majd detektált jel feszültségének átlagértéke 82,5 mV, az AC_{RMS} értéke 4,7 mV, míg a peak-to-peak érték 35.4mV. Beláthatjuk, hogy sokkal magasabb értékeket kapunk, mintha a SOA-t használtuk volna. Az optikai jelünk csúcsteljesítménye -30,88 dBm volt.



26. ábra A HPS CWDM add -drop multiplexerrel szűrt jelének spektruma

A CWDM add-drop multiplexerrel szűrt jelet ezután egy EDFA-ra kötöttük, ami jelentős mértékben felerősítette azt, a jelünk új csúcsteljesítménye -13,49 dBm lett, 1542,6 nm hullámhosszon. Itt azt feltételezhetnénk, hogy nem sokat nyertünk a SOA-s elrendezésekhez képest, hiszen csak 1,04 dB-el nőtt a maximális teljesítmény, azonban a HPS használatával az EDFA saját zajának elnyomása 15 dB-ről 22,4 dB-re nőtt, ami kísérleteinkben előnyös. Az EDFA-ból kimenő jel intenzitásfluktuációja, illetve spektruma a 27. ábrán látható. Az intenzitásfluktuáció szimmetrikusnak tűnik a 875,3mV-os átlagérték miatt, a 273,97 mV peak-to-peak és a 33,35mV AC_{RMS} érték elegendően nagy fluktuációt jelentenek a megfelelő minőségű véletlenszám-generáláshoz. Feltűnhet, hogy kisebb fluktuációt tapasztalunk a SOA alapú elrendezés 503 mV peak-to-peak, illetve 58.84 mV AC_{RMS} értékéhez képest. Ez az EDFA saját zajának nagyobb mértékű elnyomásával magyarázható.

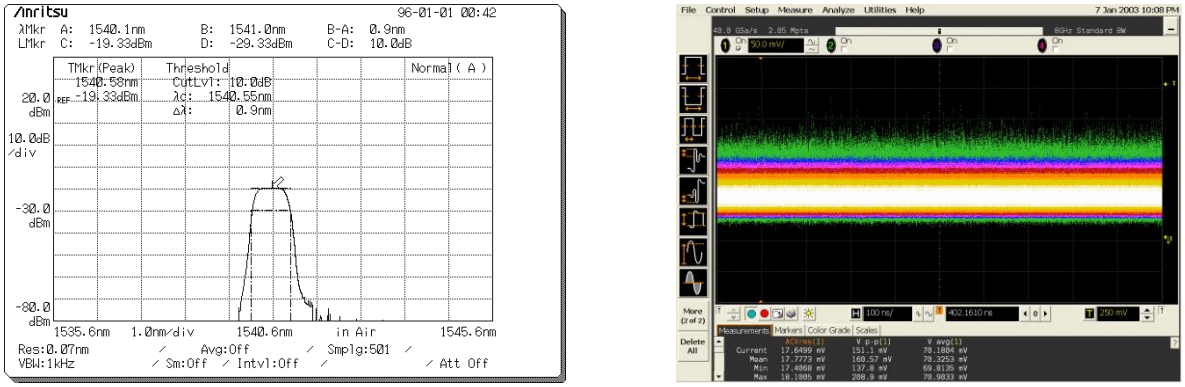


27. ábra A HPS szűrt jele, illetve azon jel felerősített spektrális képei a bal oldali ábrán,a jobb oldali ábrán ezen elrendezés intenzitásfluktuációja

A következő feladatunk a megfelelő utószűrő megtalálása volt, ehhez a szokásos XTM, OTF, DWDM demultiplexer hármasból szerettünk volna egyet választani.

Yenista XTM

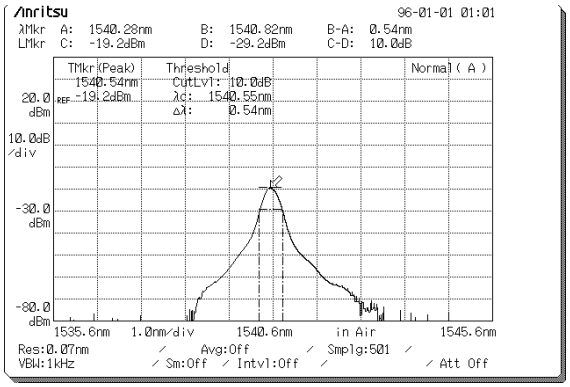
A hangolható szűrőt a maximális 0,9 nm sávszélességre, illetve 1540,55 nm-re állítottuk, hogy a lehető legtöbb teljesítményt tudjuk kivenni a rendszerünkből azért, hogy elkerüljük az aszimmetriát. Ezen a hullámhosszon a csúcsteljesítmény -19,33 dBm volt. Az optikai-elektromos átalakító után detektált jel 70,33 mV-os átlagértékkel, 160,57 mV-os peak-to-peak értékkel, továbbá 17,78 mV AC_{RMS} értékkel rendelkezik. Kikövetkeztethetjük, hogy ekkora átlagteljesítmény mellett a jelünk aszimmetrikus lesz, ahogy azt a 28. ábrán is láthatjuk.

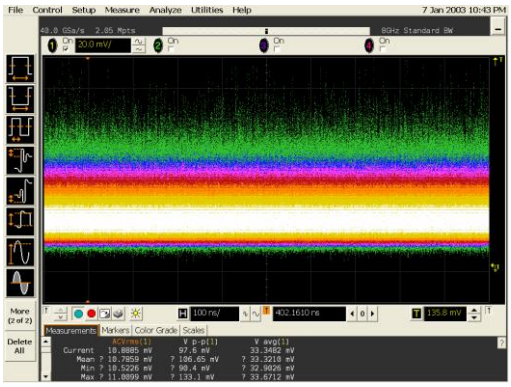


28. ábra Az EDFA-ból kijövő az XTM szűrővel szűrt jel spektruma a bal oldali ábrán, a jobb oldali ábrán ezen elrendezés intenzitásfluktuációja.

OTF

Az XTM-hez hasonlóan az 1540,54 nm-re állítottuk, illetve a csúcsteljesítmény -19,2 dBm lett. A detektált jel átlagértéke 33,32 mV, peak-to-peak értéke 106,65 mV, az AC_{RMS} feszültség értéke 10.79mV. Ezek jóval alacsonyabbak, mint az előző szűrőnél mért értékek. Természetesen az itt detektált jelünk, ahogy az lentebb is látható, teljesen aszimmetrikus lett, így ezt a megoldást sem tudjuk alkalmazni.

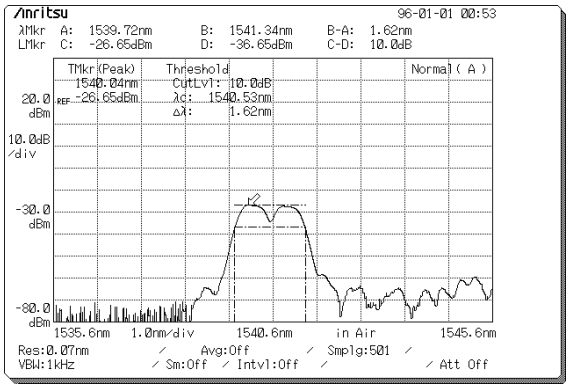


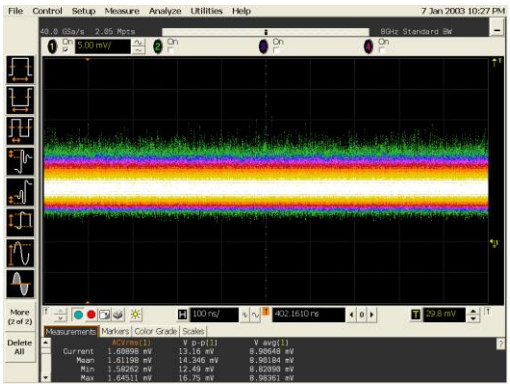


29. ábra Az EDFA-ból kijövő az XTM szűrővel szűrt jel spektruma a bal oldali ábrán, a jobb oldali ábrán ezen elrendezés intenzitásfluktuációja.

DWDM demultiplexer

A DWDM szűrőt nagyon kicsi, 0,8 nm-es sávszélesség miatt nem is érdemes használni, azonban kitaláltunk egy érdekes megoldást. A 9-es, illetve a 10-es csatornát együtt használtuk, majd ezeket egy összegzőre vezettük, azonban ezzel a megoldással is csak 8,9 mV-os átlagfeszültséget, illetve 1,62 mV-os peak-to-peak értéket sikerült elérni. A spektrális kép, illetve az időtartománybeli intenzitásfluktuáció lentebb látható.





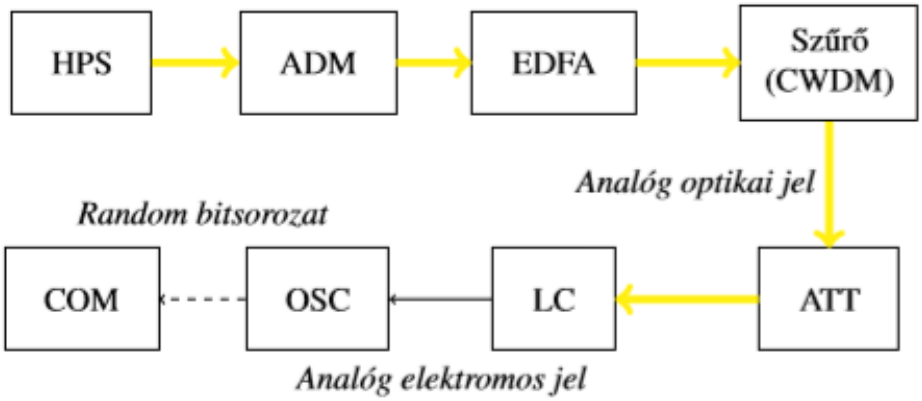
30. ábra Az EDFA-ból kijövő az XTM szűrővel szűrt jel spektruma a bal oldali ábrán, a jobb oldali ábrán ezen elrendezés intenzitásfluktuációja.

Konklúzió az elrendezéssel kapcsolatban

Abban az esetben, ha konklúziót szeretnénk levonni, azt kell megállapítanunk, hogy az utószűrő előtti elrendezés megfelelő, más utószűrő és csillapító alkalmazásával, ugyanis minden problémát az elérhető források függvényében sikerült megoldanunk vele. Ennek ellenére az utószűrő kiválasztása továbbra is gondot okoz, ugyanis látható, hogy az XTM szűrő volt a legalkalmasabb erre a feladatra, mivel ebben az esetben értük el a legnagyobb fluktuációt, továbbá itt vagyunk a legközelebb az elegendően nagy átlagfeszültséghez is, ennek ellenére nem tudjuk azt mondani, hogy az összeállításunk tökéletes, mivel az aszimmetria továbbra is fennáll az időtartománybeli intenzitásfluktuációban.

3.2.2 A végleges elrendezés

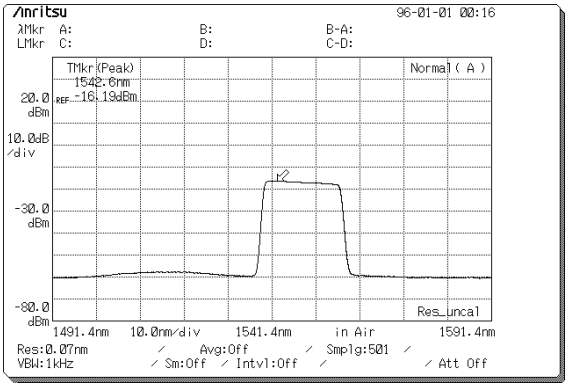
A végleges elrendezésben az előző részben említett összeállítást használjuk, leszámítva az utószűrőt és egy csillapítót. Ezt az összeállítást röviden fel is vázolom. ASE-forrásként a HPS-t használjuk, majd ennek CWDM add-drop multiplexerrel szűrt jelét vezetjük rá az EDFA-ra, ami ezt a jelet felerősíti. Erre azért van szükség, hogy az „ASE zaj" dominájon a fotovevőnk saját zaja helyett. Utolsó feladatunk a megfelelő utószűrő kiválasztása, mely az aszimmetria elkerülése miatt fontos. Az utószűrésre tehát azért van szükség, hogy csökkentsük a teljesítményt annyira, hogy ne lépjen fel telítődés, de elég nagy teljesítmény legyen, hogy a gamma-eloszlás a normálishoz tartson, illetve az EDFA saját zaját elnyomjuk (habár az EDFA szinten ASE-forrás, mi mégis szeretnénk, ha a HPS zaja dominálna vele szemben). A további részleteket az elrendezésről a 3.2.1-es fejezetben olvashattuk.



31. ábra A végleges elrendezésünk blokkvázlata

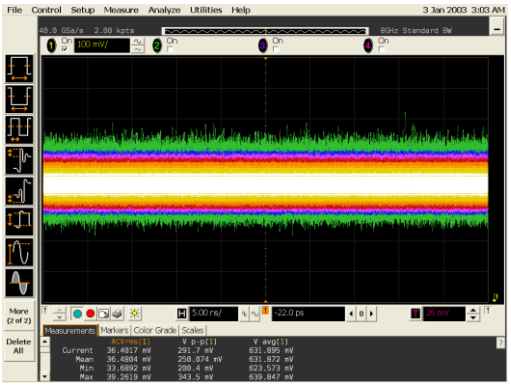
Az előző részekben beláttuk, hogy az olyan szűrők, melyek kis sávszélességgel (1 nm körüli) rendelkeznek (pl.: DWDM szűrők) nem megfelelőek a fent említett célra, mivel a HPS EDFA-val felerősített jele is csak nagyon kis teljesítményt tud kibocsátani ekkora sávszélesség mellett. Az előzetes kísérletek alapján kézenfekvő megoldás volt a CWDM

add-drop multiplexerrel azonos sávban egy CWDM szűrőt használni, ugyanis a -10 dB-hez tartozó sávszélesség ebben az esetben 19,2 nm-re adódott, így biztosan elegendő teljesítményt tud az optikai-elektromos átalakítóra küldeni. Ezen szűrő 1550 nm körüli tartományban mindössze 2.5 dB beiktatási csillapítással rendelkezik. Az elrendezés a 31.ábrán, a spektruma a 32. ábrán látható.



32. ábra Az elrendezésünk CWDM szűrő utáni spektrális képe

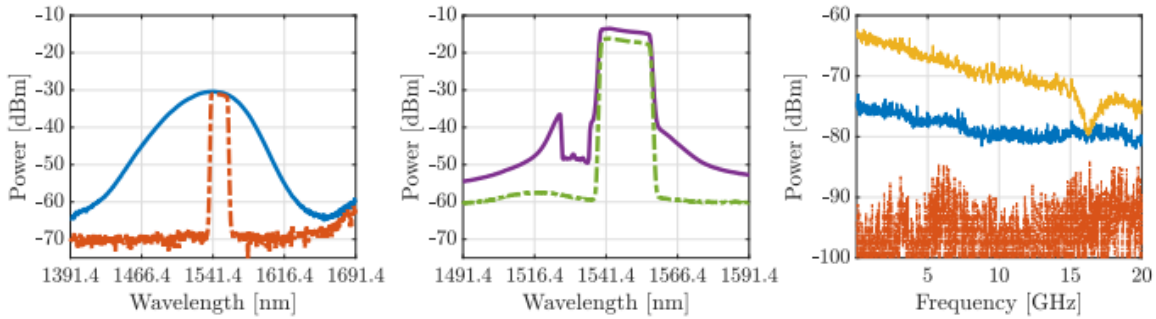
A szűrő kimeneti összteljesítménye a nagy sávszélesség miatt ekkor 8.1 dBm, így már bőven meghaladja a vevő telítési teljesítményét, ami 5dBm, tehát a vevő elé be kellett iktatnunk egy csillapítót. A csillapítót úgy hangoltuk (3.5 dBm csillapítás), hogy az átlagteljesítmény 4.6 dBm legyen. Ezzel egyfajta kompromisszumot sikerült kötnünk, hiszen az időtartománybeli amplitúdóeloszlásunk erősen szimmetrikus lett, mivel a gamma-eloszlás paramétere elegendően nagy értékkel rendelkezik, valamint sikerült elkerülnünk a vevőnk telítődését, tehát a P-V diagram lineáris szakaszán működtetni a vevőt.



33. ábra Az összeállításunk időtartománybeli intenzitásfluktuációja

A fenti ábrán látható a szimmetrikus jelünk, mely 631,87 mV átlagértékkel, 250,07 mV peak-to-peak értékkel, illetve 36,48 mV AC_{RMS} értékkel rendelkezik. Ahogy már említettem ez elég magas egyenszinttel rendelkezik ahhoz, hogy elkerüljük az

aszimmetriát, és elég alacsony, hogy elkerüljük a vevőnk telítődését, emellett sikerült elnyomni az EDFA zaját, valamint elérni egy elég magas fluktuációt.



34. ábra Optikai, illetve elektromos spektrumok. Balra: a HPS ASE-zajspektruma szűretlenül (kék), illetve a CWDM add-drop multiplexerrel szűrve (narancssárga); középen: az EDFA által felerősített jel szűrés előtt (lila), illetve a CWDM szűrővel szűrve (zöld); jobbra: a HPS zajának elektromos spektruma (kék), a vett jel csillapítás nélküli elektromos spektruma(sárga), illetve a spektrumanalizátor sajátzaja(vörös).

A fenti ábrán láthatjuk az optikai, illetve az elektromos spektrumok összehasonlítását. Az optikai vevő sávszélessége leolvasható a jobb oldali ábráról (15 GHz).

Utófeldolgozás

Ebben a részben ki fogok térni a mintavételezés hatására a véletlenségre, ismertetem az alkalmazott utófeldolgozást, valamint a generált véletlen bitek tesztelését.

Az oszcilloszkópon rögzítettük az időtartománybeli intenzitásfluktuációt, majd ezen értékeket eltároltuk, ezután offline módon a Matlab programot használva számítógépen végeztük el a bitgenerálást és az utófeldolgozást, így megfelelő minőségű véletlen biteket sikerült generálnunk. A vett mintákat minden esetben a középértékhez (medián) komparáltuk, ezzel biztosítva az 50-50%-os eloszlást 0-s, illetve 1-es bitek között. Itt felmerülhet a kérdés, mi történt a mediánnal egybeeső mintákkal: 1μV-al csökkentettük a komparálási szintet, így ezek mind „1”-es bitnek számítottak. Ez kissé elrontja az 50-50-es arányt, viszont ez a szándékos hiba jobban kiemeli a mintavételi frekvenciák közti különbségeket, illetve nem volt szükség minták eldobására. Annak érdekében, hogy elkerüljük a kiegyenlítetlenséget a mediánt minden $1*10^6$. alkalommal újraszámoltuk. A bitgenerálási sebesség növelése érdekében a [8] hivatkozásban felvázolt véletlenszám-generátornál alkalmazott több bites mintavételezést is használhatnánk, viszont a megfelelő mintavételezési frekvencia kiválasztása egy bites mintavételezésnél egyszerűbb, ugyanis itt a generált véletlen-bitek minőségi különbségei nagyobb kontrasztot mutatnak.

A mintavételezést 0,1; 0,2; 0,5; 1; 2; 4; 10 és 20 GSa/s mintavételi frekvencián végeztük el. Ezen frekvenciák kiválasztása során figyelembe vettük, hogy az oszcilloszkóp sávszélessége 8 GHz (a vevőnké ennél több, 15 GHz, tehát a bitgenerálási sebességet egyértelműen a szkóp szabja meg), emiatt úgy választottunk, hogy az analóg sávszélesség értéke körül széles tartományt fedjenek le: legyen olyan frekvencia is, ami távol van tőle mindkét irányban, illetve olyan is, ami nagyon közel. Szerettünk volna az oszcilloszkóp sávszélességének megfelelő frekvencián is (8 GSa/s) mintavételezni, de a szkóp ezt nem támogatta.

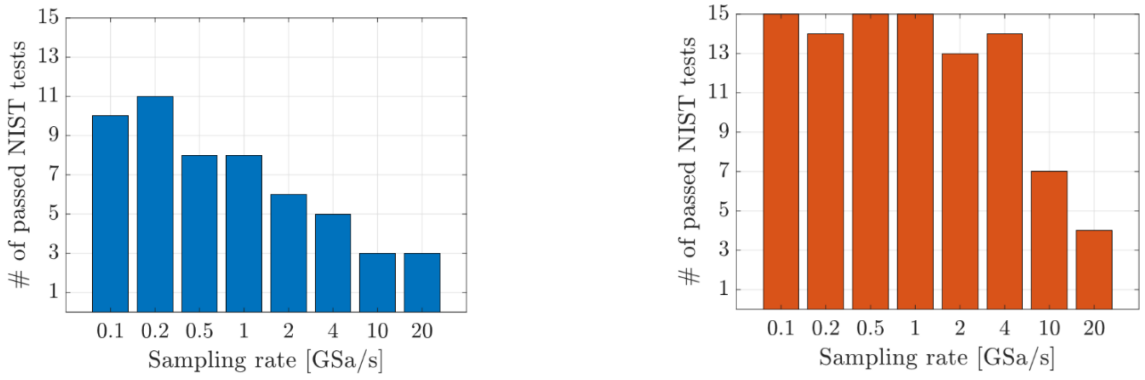
Minden mintavételi sebesség mellett egymilliárd mintát gyűjtöttünk. A nagyobb mintavételi frekvenciákon az oszcilloszkóp nem volt képes ugyanolyan hosszú sorozatokat elmenteni, így ez a szám alacsonyabb mintavételi frekvenciákon 200 darab ötmillió hosszú mintasorozatból, magasabb mintavételi frekvenciákon 408 darab $2{,}05*10^6$ mintából tevődött össze. Előzetes elvárásaink szerint a véletlenség minősége a mintavételi frekvencia növelésével csökkeni fog, ugyanis ez egyre nagyobb korrelációt okoz az egymáshoz közeli bitek között.

Az így generált bitsorozatokat statisztikus véletlenségi teszteknek vetettük alá. Ehhez a NIST (National Institute of Standards and Technology) Statistical Test Suite tesztsorozatát [7] használtuk, mely 15 tesztet tartalmaz, amelyek különböző szemszögből vizsgálják a véletlenséget (pl.: korreláció, ismétlődések keresése). Minden 10^9 bitsorozatot 1000 darab 10^6 hosszú bitsorozatra bontottuk, amely alsorozatokat egyesével teszteltük minden egyes mintavételi frekvencián. A teszt minden esetben kiszámít egy p értéket, ami a nullhipotézis („a sorozat véletlen”) elfogadásának valószínűségét jellemzi. Ezzel megtudhatjuk, hogy a

generátor kimenete mennyire véletlen, illetve egyenletes eloszlású. Abban az esetben, ha p értéke nagyobb, mint az α szignifikanciaszint akkor a sorozat véletlennek tekinthető. Az általunk használt szignifikanciaszint α=0.01. Több feltételünk van, ami alapján egy véletlenszám-generátor által előállított sorozat sikeresen átmegy egy adott teszten. Egyrészt az ezer alsorozatból legalább 1-nek, de legfeljebb 20-nak szabad elbuknia azon, hogy a p értéke kisebb, mint a szignifikanciaszint. Utóbbi eset nyilvánvaló, mert ha sok teszten elbukik, nem nevezhetjük véletlennek a sorozatot, előbbi magyarázatra szorul: az egyenletes eloszlás miatt minden lehetséges sorozatnak ugyanakkora valószínűséggel kell előállnia, emiatt lennie kell számunkra nem véletlennek tűnő sorozatnak is (pl.: $5*10^5$ 01 tagból álló sorozat). Ezen kívül az 1000 p értéknek egyenletes eloszlást kell követnie, amit újabb statisztikai tesztelés és egy egyenletességi p érték előállításával állapíthatunk meg. Amennyiben ez az érték meghaladja a 0,0001 értéket a teszt sikeresnek mondható. Ezen feltételek együtt kell teljesüljenek, a teszt sikeressége érdekében. Fontos megjegyezni, amennyiben a sorozat teljesíti a tesztet, akkor sem bizonyítható véges számú teszttel, véges hosszú sorozaton, hogy az véletlennek tekinthető, így ez nem elégséges, csupán szükséges feltétele a véletlenségnek.

A tesztek elvégzése után láthatjuk, hogy az előzetes elvárásaink teljesültek. A mintavételi frekvencia növelésével csökken a sikeres tesztek aránya (kivéve a 0.1 GSa/s, illetve a 0.2 GSa/s sorozatot, utóbbi jobban teljesített a teszteken). Látható, ha egy teszten elbukott a rendszerünk alacsonyabb mintavételi sebességgel, biztosan elbukott a nagyobb mintavételi sebességgel is (kivételt képez ez alól az előző mondatban említett két mintavételi sebesség).

Az 35. ábrán látható, hogy a nyolc nyers bitsorozat közül egyik sem teljesítette mind a 15 tesztet, viszont a mintavételi frekvencia növelésével egyre nagyobb mértékben csökkent a sikeres tesztek aránya. A 36. ábrán látható, hogy a szándékos komparálási hiba miatt a frequency teszten (mely a 0-k, illetve 1-esek relatív gyakoriságát vizsgálja) nagyon rosszul teljesítettek a sorozatok.



35. ábra A sikeres tesztek jelölése a mintavételi sebesség függvényében: bal oldalon utófeldolgozás előtt, jobb oldalon az XOR technika alkalmazásával.

A kiegyenlítetlenség és a korreláció elkerülése érdekében egy önkésleltetésű XOR technikát alkalmaztunk. Ez azt jelenti, hogy az eredeti és az önmagához képest 20 bittel eltolt bitsorozat kizáró vagy kapcsolatát vettük. Ahogy a 35. ábrán látható ezzel nagy mértékben

nőtt a sikeres tesztek aránya a feldolgozás előtti állapothoz képest. Mivel a korreláció csak az egymáshoz közeli bitek között állt fent az XOR technika ezt szinte teljesen kiszűrte. Hosszú idejű korrelációt csak több biten történő mintavételezés esetén észlelhetünk, így ez egy bites mintavételezésnél nem volt jellemző.

Teszt	Mintavételi sebesség [GSa/s]							
	0,1	0,2	0,5	1	2	4	10	20
Frequency	✗	✗	✗	✗	✗	✗	✗	✗
Block frequency	✗	✗	✗	✗	✗	✗	✗	✗
Runs	✗		✗	✗	✗	✗	✗	✗
Longest run					✗	✗	✗	✗
Rank								
Discrete Fourier transform							✗	✗
Non-overlapping templates	✗	✗	✗	✗	✗	✗	✗	✗
Overlapping templates			✗	✗	✗	✗	✗	✗
Universal						✗	✗	✗
Linear complexity								
Serial					✗	✗	✗	✗
Approximate entropy			✗	✗	✗	✗	✗	✗
Cumulative sums	✗	✗	✗	✗	✗	✗	✗	✗
Random excursions							✗	✗
Random excursions variant								

Teszt	Mintavételi sebesség [GSa/s]							
	0,1	0,2	0,5	1	2	4	10	20
Frequency					✗		✗	✗
Block frequency						✗	✗	✗
Runs							✗	✗
Longest run								✗
Rank								
Discrete Fourier transform								✗
Non-overlapping templates		✗					✗	✗
Overlapping templates							✗	✗
Universal								✗
Linear complexity								
Serial							✗	✗
Approximate entropy							✗	✗
Cumulative sums					✗		✗	✗
Random excursions								
Random excursions variant								

36. ábra A bal oldali ábra az utófeldolgozás előtti, a jobb oldali az utófeldolgozás utáni sikeres NIST teszteket mutatja a mintavételezési sebesség függvényében

Az utófeldolgozás után a 0.1 GSa/s, a 0.5 GSa/s, illetve az 1 GSa/s sebességgel mintavételezett sorozatok minden teszten megfeleltek. A 0.2 GSa/s és 4 GSa/s-el mintavételezett sorozatok csak egy teszten buktak el. Előbbi a non-overlapping template tesztcsalád egyikét csak 0.979 arányban teljesítette az elvárt 0.98 helyett, így ez minimális, egyszerűen kiküszöbölhető. A 2 GSa/s-al mintavételezett sorozat is csak 2 teszten bukott el, viszont a rendszerünk sávszélességénél (8 GHz) nagyobb mintavételezési sebességgel digitalizált jelek még az utófeldolgozás után is rengeteg teszten elbuktak, így ezek használatát egyértelműen el kellett vetnünk. A 8 GSa/s sebességnél lassabb mintavételezések esetén felmerülő hibák kiküszöbölhetők, ha az utófeldolgozást tökéletesítjük.

Konklúzió és további lehetőségek

Megállapíthatjuk, hogy a mintavételezés, illetve az utófeldolgozás nagy hatással van a véletlen bitek minőségére. Az elvárásoknak megfelelően az analóg sávszélességnél jóval kisebb mintavételi frekvenciáknál jobb minőségű véletlen biteket kapunk, ez azonban a bitgenerálási sebesség rovására megy. Belátható az is, hogy az önkésleltetésű XOR technikával szintén nagyban javíthatjuk a véletlen bitek minőségét. A legjobb választás a mi esetünkben a 4 GSa/s, mely utófeldolgozással 1 tesztet kivéve minden teszten átment, ez volt a legnagyobb mintavételezési sebesség, ami jól teljesített a NIST teszten.

A fent említettek mellett további lehetőségek is rendelkezésünkre állnak, hogy továbbfejlesszük rendszerünket, ilyen például az átlagértékhez való komparálás, mely során nem kell szándékosan kiegyenlítetlenséget vinni a rendszerbe. Amennyiben a XOR késleltetését növeljük, nagyobb mértékben javíthatunk a véletlen bitek minőségén. Emellett lehetőségünk van növelni a bitgenerálási sebességet, ha több biten mintavételezünk. Ez

problémát is okozhat, hiszen az MSB-k hosszú idejű korrelációt visznek a rendszerbe, melyet az LSB-k csökkentenek. Ez a korreláció az adott számú MSB eldobásával küszöbölhető ki.

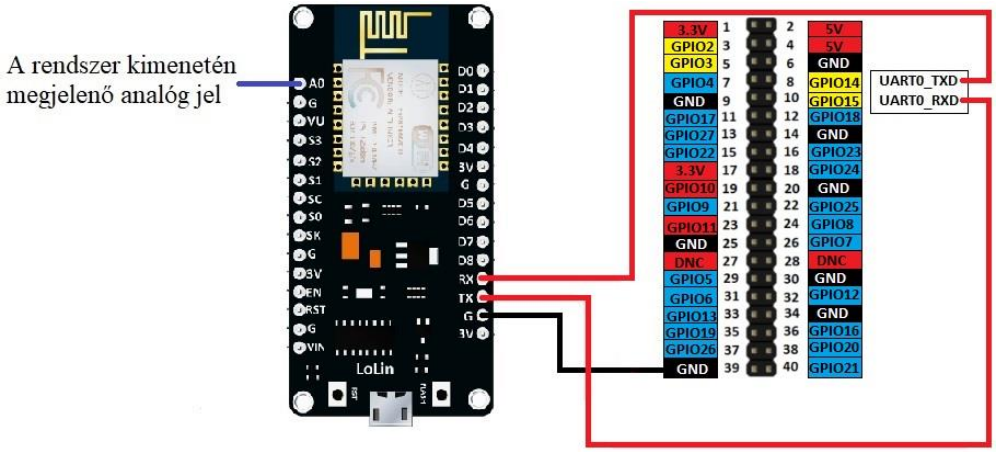
Az eredmények publikálása

Ebben a fejezetben részletezett és ismertetett eredmények alapján tudományos publikáció is készült, melyet elbírálás után elfogadott a *21st International Conference on Transparent Optical Networks* (ICTON 2019) nemzetközi konferencia szerkesztőbizottsága. Az esemény az angers-i egyetem (Université d'Angers) természettudományos karának szervezésében zajlott 2019. július 9. és 13. között. A 20 perces előadást Schranz Ágoston tartotta meg július 12-én, az esemény kvantumkommunikációs szekcióinak egyikében. A tudományos munka (*Effects of sampling rate on amplified spontaneous emission based single-bit quantum random number generation*) [15] a dokumentum végéhez csatolva megtalálható.

Bitek valós idejű generálása

Ebben a fejezetben szeretném bemutatni az általam fejlesztett weboldalt, mely lényegében csak egy próba verziója egy valódi ADC-vel működő, Raspberry Pi-n futó, mindenki számára elérhető online felületnek, azonban már ez a verzió is képes véletlen bitek generálására. Raspberry Pi-hez illeszthető ADC nem volt elérhető a laborban, így ezt egy ESP8266 fogja helyettesíteni a próbaelrendezésben.

A hardveres elrendezés a 37. ábrán látható, aminek rövid magyarázata a következő: az optikai-elektromos átalakítóból kijövő jelet egy 10 bites ADC mintavételezi, mely 0 V és 3,3 V között működik. Az ESP8266 és a Raspberry Pi 3 B+ közötti kommunikáció UART-on történik.



37. ábra A optikai- elektromos átalakítóra kötött áramkör, mely a bitek valós idejű generálására szolgál (a bal oldali egység az ESP8266, a jobb oldali a Raspberry Pi lábkiosztása)

A szoftveres működés a következő: egy PHP program létrehozza a weboldalt, ez tud kommunikálni az SQL adatbázissal, illetve ezen programkódon belül végre tudjuk hajtatni a Python kód lefuttatását is.

Az ESP8266 működése

Ezen eszköz programozása C nyelven történik, és a program a következők szerint működik: arra vár, hogy a soros port aktívvá váljon, ha ez megtörténik, soros porton beolvassa a kért bitek számát. Ezután az előre meghatározott maximum tároló értékig (a weblap gátolja ennél nagyobb érték beírását) feltölt az analóg portról egy int-eket tartalmozó tömböt. Ezt minden alkalommal újra megteszi, ezzel garantálva azt, hogy ezeket a biteket ne használjuk többször. Ezek az értékek mind 0 és 1024 közti értékek lesznek a mintavételezés miatt. Ez, habár pazarlónak tűnik, az ezután következő átlagképzés miatt fontos, hisz minél több értékből számoljuk az átlagot, annál pontosabban megközelíti a jelünk valódi középértékét nullától a végtelenig véve. Ezután az átlaghoz komparálva feltölti a tárolónkat 0-s, illetve 1-es bitekkel. Ekkor kiválaszt a kért számú bitnek megfelelő mennyiségű adatot, összefűzi őket egy string-be, majd soros porton továbbítja a Raspberry Pi felé.

A Raspberry Pi működése

Ezen eszköz programozása során HTML, CSS, PHP, Python és SQL nyelvet használtam. A PHP-fájl bemutatásával szeretném kezdeni, majd párhuzamosan kitérni a Python-fájlra, illetve az SQL-táblára. Ebben a fájlban létrehozom a HTML weboldalt, ahol bemenetként meg tudjuk adni, hány bitet szeretnénk kapni. Ekkor a generálás gombra kattintva létrehoz egy SQL bejegyzést, melyet elküld a MySQL szervernek. Ebben a bejegyzésben közli, hogy a folyamat az 1-es fázisban van, azaz biteket kér a weboldal. Ezután elindítja a Python-fájlt, mely lekéri az SQL-táblából, hogy melyik bejegyzés van 1-es fázisban. Ekkor megkapja a bitszámot, melyet továbbít a soros porton keresztül az ESP8266-nak, melynek működését már fentebb leírtam. Ezután a .py kiterjesztésű fájl beolvassa a soros porton érkező véletlen biteket, és beilleszt egy 2-es fázisban lévő bejegyzést a táblába, elküldve a véletlen biteket. Ezután a működés a .php kiterjesztésű fájlban folytatódik, ahol a megkapott maximum 10 bitet kiteszi a weboldalra.

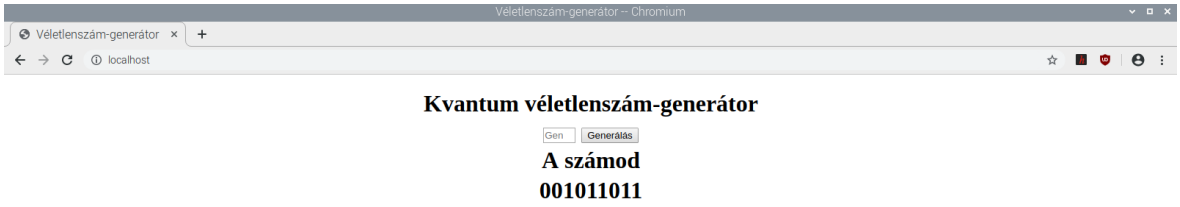
id	src	dst	msg	number	bitnumber	sending	processing	ready
326	WEB	SRV	GetRndBits	0	7	0	0	1
327	SRV	WEB	SetRndBits	1011101	7	0	0	1
328	WEB	SRV	GetRndBits	0	8	0	0	1
329	SRV	WEB	SetRndBits	10111	8	0	0	1
330	WEB	SRV	GetRndBits	0	7	0	0	1
331	SRV	WEB	SetRndBits	1011111	7	0	0	1
332	WEB	SRV	GetRndBits	0	5	0	0	1
333	SRV	WEB	SetRndBits	0	5	0	0	1
334	WEB	SRV	GetRndBits	0	9	0	0	1
335	SRV	WEB	SetRndBits	111000	9	0	0	1
336	WEB	SRV	GetRndBits	0	9	0	0	1
337	SRV	WEB	SetRndBits	1010101	9	0	0	1

38. ábra A kérések naplózása az SQL adatbázisban

További lehetőségeink

Nem véletlenül említettem, hogy a program csak egy demó verzió, egy prototípus. A megalkotása során több továbbfejlesztési lehetőségre fény derült. Az első ilyen, ha egy valódi ADC-t használnánk az ESP8266 helyett. Ennek előnye az lenne, hogy egy kiegészítő áramkörrel együtt építenénk be, ami a kb. 800 mV középértékű jelből eltávolítaná a 800 mV átlagértéket és kiterjesztené a fluktuációt egy szorzó áramkörrel az egész tartományra, majd visszatolná az értéket a tartomány felére offset feszültséggel. Ezzel sokkal jobb minőségű véletlen biteket sikerülne generálnunk, nem lenne szükség egy mikrokontrollerrel végzett átlagképzésre és az ahhoz való komparálásra. Emellett problémaként merült fel, hogy az int csak 4 byte-os ebben az esetben, ha egy bináris számot szeretnénk benne tárolni int-ként, mintha egy decimális szám lenne, akkor csak 10 számjegyig tudjuk megtenni. Ezt a problémát ki tudjuk küszöbölni, ha bigint-ként tároljuk, ezzel nyernénk további 9 véletlen bitet, mivel a bigint 8 byte-os. Egy másik megoldás, ha előtte átkonvertálnánk decimális számmá a bináris számot, és így tárolnánk el, ezzel int-ként 32 bitet tudnánk tárolni. A két megoldást ötvözve bigint-ként tárolva összesen 62 bitet lennénk képesek tárolni. Ezt

továbbfejlesztve, ha annyi bejegyzést írnánk az SQL-táblába, amennyi lehetséges, akkor elméletileg korlátlanul növelhetnénk a kapacitást, a tárolási kapacitás függvényében. A harmadik probléma, hogy jelenleg csak helyi hálózaton keresztül érhető el, ezen is tudnánk javítani, ha valódi webszerverként funkcionálna a Raspberry. A korreláció kiszűrése érdekében itt is tesztelhetnénk a mintavétel hatását a véletlenség minőségére, végezhetnénk utófeldolgozást (pl.: önkésleltetésű XOR technika) az egymáshoz közeli bitek közti korreláció elkerülésére, továbbá eldobhatnánk néhány MSB bitet a hosszú idejű korreláció eltüntetésére. Ezek megvalósítása nem témája a dolgozatomnak, a jövőben fog rájuk sor kerülni.



39. ábra A weboldal működés közben, 9 bitet generálva

Összefoglalás, további lehetőségek

Munkám során megalkottam egy, a kvantumszámítógép világában már feltétlenül szükséges véletlenszám-generátort. Ehhez az irodalomkutatás során korábban megalkotott generátorokat elemeztem, azon elrendezések előnyeit és hátrányait feltártam. Ezután információt gyűjtöttem a saját rendszertervem összeállításához szükséges, a laborban megtalálható eszközökről, majd kísérleti összeállításaimat elemeztem. A megfelelő rendszerterv kiválasztása után a mintavételi frekvencia tökéletes kiválasztásához egy tanulmányt végeztem, mely során megállapítottam a mintavételi frekvencia hatását a véletlenségre. Ezután utófeldolgozást végeztem, amivel biztosítottam a megfelelő minőségű véletlen bitek létrehozását, majd kifejlesztettem egy prototípus áramkört, mellyel lehetővé teszem a valós idejű véletlenszám generálást.

A rendszerünk erősített spontán emisszió elvén működik, mely egy teljesen véletlen folyamat. ASE-forrásként a HPS-t használtuk, mely jelét egy CWDM add-drop multiplexerrel szűrve egy EDFA-val felerősítettük. Ezután ezt a jelet újra egy nagy sávszélességgel rendelkező CWDM szűrővel szűrtük, majd egy optikai-elektromos átalakító segítségével az optikai teljesítményt elektromos feszültséggé konvertáltuk, majd offline módon az oszcilloszkóp segítségével mintavételezést végeztünk különböző mintavételi frekvenciákon. Az így kapott véletlen bitek minőségét utófeldolgozással javítottuk egy önkésleltetésű XOR technika segítségével. Ezután a rendszerhez kifejlesztett Raspberry Pi-n futó webszervert hoztam létre, mely online bitgenerálási lehetőséget biztosít.

További lehetőségek

Abban az esetben, ha nem a mediánhoz, hanem az átlaghoz hasonlítanánk, nem vinnénk szándékos komparálási hibát rendszerünkbe. Lehetőség továbbá, hogy több biten mintavételezünk, mely kis korrelációs hibát vinne a rendszerbe, azonban ez néhány MSB eldobásával, illetve az XOR technikával kiküszöbölhető lenne. Ezzel nagy sebességemelkedést érnénk el.

A legtöbb fejlődési potenciál az online feldolgozó felületben van, ezeket az előző fejezetben kifejtettem, így csak felületesen felsorolom ezeket: ADC használata az ESP8266 helyett, int típus használata és a bináris érték decimálisként tárolása helyett bigint típusként tárolás, illetve decimálisba váltás bináris értékből, még a tárolás előtt, továbbá még azzal is növelhetnénk a generálható bitek számát, ha több bejegyzést is tudna a Python program írni az SQL táblába. A helyi hálózaton működés helyett kiterjeszthetnénk ezen online felület elérését. Tesztelhetnénk a mintavétel hatását a véletlenre, továbbá végezhetnénk utófeldolgozást ezen online felületen is.

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani felelős konzulensemnek Schranz Ágostonnak, aki bevezetett az optikai hálózatok világába, a mérésekben használandó eszközök használatát bemutatta, valamint a mérések elvégzésében, illetve az elméleti háttér elsajátításában nagy segítségemre volt. Emellett szeretnék köszönetet mondani Matolcsy Balázsnak, aki a weboldal szerkesztésében megjelenő problémák során eligazítást adott. Végül, de nem utolsó sorban szeretnék köszönetet mondani Gerhátné dr. Udvary Eszternek, aki először javasolta a témával való foglalkozást, valamint megteremtette kutatásom lehetőségét.

A kutatás az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg (EFOP-3.6.2-16-2017-00013, Innovatív Informatikai és Infokommunikációs Megoldásokat Megalapozó Tematikus Kutatási Együttműködések).

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

Irodalomjegyzék

[1] R. Paschotta, article on 'quantum cryptography' in the Encyclopedia of Laser Physics and Technology, 1. edition October 2008, Wiley-VCH, ISBN 978-3-527-40828-3

[2] R. Paschotta, article on 'stimulated emission' in the Encyclopedia of Laser Physics and Technology, 1. edition October 2008, Wiley-VCH, ISBN 978-3-527-40828-3

[3] R. Paschotta, article on 'amplified spontaneous emission' in the Encyclopedia of Laser Physics and Technology, 1. edition October 2008, Wiley-VCH, ISBN 978-3-527-40828-3

[4] R. Paschotta, article on 'semiconductor optical amplifiers' in the Encyclopedia of Laser Physics and Technology, 1. edition October 2008, Wiley-VCH, ISBN 978-3-527-40828-3

[5] R. Paschotta, article on 'erbium-doped fiber amplifiers' in the Encyclopedia of Laser Physics and Technology, 1. edition October 2008, Wiley-VCH, ISBN 978-3-527-40828-3

[6] R. Paschotta, article on 'four-level and three-level gain media' in the Encyclopedia of Laser Physics and Technology, 1. edition October 2008, Wiley-VCH, ISBN 978-3-527-40828-3

[7] A. L. Rukhin et al., „A statistical test suite for random and pseudorandom number generators for cryptographic applications," tech. rep., National Institute of Standards & Technology, Gaithersburg, MD, United States, 2010. Spec. Pub. 800-22, Rev. 1a

[8] A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, „Sub-tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals," Journal of Lightwave Technology, vol. 30, no. 9, pp. 1329–1334, 2012.

[9] C. R. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, „Fast physical random number generator using amplified spontaneous emission," Optics express, vol. 18, no. 23, pp. 23584–23597, 2010.

[10] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, „Scalable parallel physical random number generator based on a superluminescent led," Optics letters, vol. 36, no. 6, pp. 1020–1022, 2011.

[11] L. Li, A. Wang, P. Li, H. Xu, L. Wang, and Y. Wang, „Random bit generator using delayed self-difference of filtered amplified spontaneous emission," IEEE Photonics Journal, vol. 6, no. 1, pp. 1–9, 2014.

[12] Y. Liu, M. Zhu, B. Luo, J. Zhang, and H. Guo, „Implementation of 1.6 Tbs^{-1} truly random number generation based on a super-luminescent emitting diode,"Laser Physics Letters,vol.10, no. 4, p. 045001, 2013.

[13] A. Martin, B. Sanguinetti, C. C. W. Lim, R. Houlmann, and H. Zbinden, „Quantum random number generation for 1.25-ghz quantum key distribution systems," Journal of Lightwave Technology, vol. 33, no. 13, pp. 2855–2859, 2015.

[14] T. Yamazaki and A. Uchida, „Performance of random number generators using noise-based superluminescent diode and chaos-based semiconductor lasers," IEEE Journal of Selected Topics in Quantum Electronics, vol. 19, no. 4, pp. 0600309–0600309, 2013.

[15] Á. Schranz, Á. Marosits, and E. Udvary, „Effects of sampling rate on amplified spontaneous emission based single-bit quantum random number generation," in 2019 21st International Conference on Transparent Optical Networks (ICTON), pp. 1–4, IEEE, 2019.

Ábrajegyzék

Rövidítésjegyzék

QRNG	Quantum random number generator	Kvantum-véletlenszámgenerátor
PRNG	Pseudo random number generator	Pszeudo véletlenszám-generátor
TRNG	True random number generator	Valódi véletlenszám-generátor
ASE	Amplified spontaneous emission	Erősített spontán emisszió
SLED	Superluminescent light emitting diode	Szuperlumineszcens fénykibocsátó dióda
SOA	Semiconductor optical amplifier	Félvezető optikai erősítő
EDFA	Erbium doped fiber amplifier	Erbium adalékolt optikai erősítő
HPS	High power source	Nagyteljesítményű forrás
ADM	Add-drop multiplexer	
ATT	Attenuator	Csillapító
LC	Lightwave converter	Optikai vevő
OSC	Oscilloscope	Oszcilloszkóp
TRB	True random bit	Valódi véletlen bit
CWDM	Coarse wavelength division multiplexing	(Többcsatornás optikai szabvány)
DWDM	Dense wavelength division multiplexing	(Többcsatornás optikai szabvány)
DC	Direct current	Egyenáram
AC	Analog current	Váltóáram
MSB	Most significant bit	Legnagyobb helyiértékű bit
ADC	Analog to digital converter	Analóg-digitális konverter
UART	Universal asyncronous receiver-transmitter	Univerzális aszinkron adóvevő
NIST	National Institute of Standards and Technology	Nemzeti Szabványügyi és Technológiai Hivatal