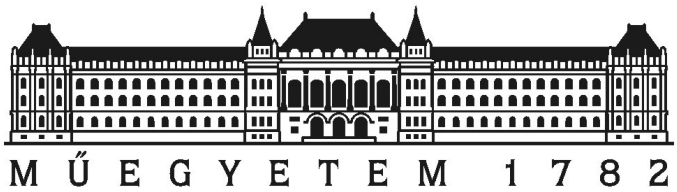


Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Szélessávú Hírközlés és Villamosságtan Tanszék

CVQKD összekötetést megvalósító optikai hálózat szimulációs vizsgálata

Tudományos Diákköri Konferencia 2018

Készítette
Kóbor Dávid

Konzulens
Gerhátné Dr. Udvary Eszter

2018. október 25.

Tartalomjegyzék

Ábrák jegyzéke

1. fejezet

Titkosítás

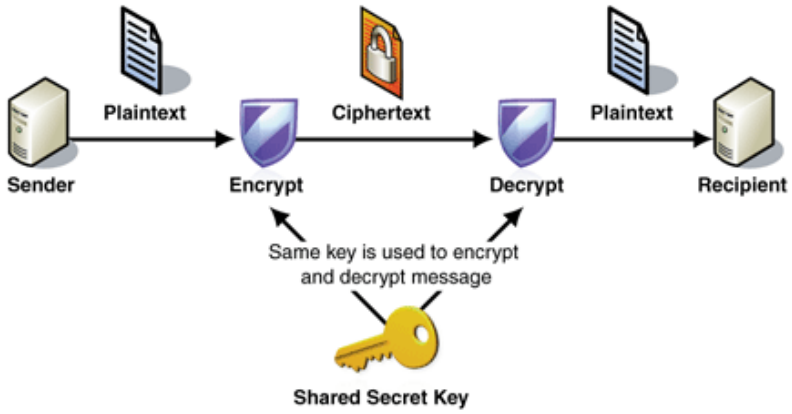
1.1. Klasszikus kriptográfiai technikák

A fejezetben áttekintem a klasszikus titkosítási megoldások két legnagyobb csoportját, kiemelem az ezek működtetése során felmerülő nehézségeket, és egyúttal rámutatok az új megközelítések használatának szükségességére.

1.1.1. Szimmetrikus kulcsú titkosítás

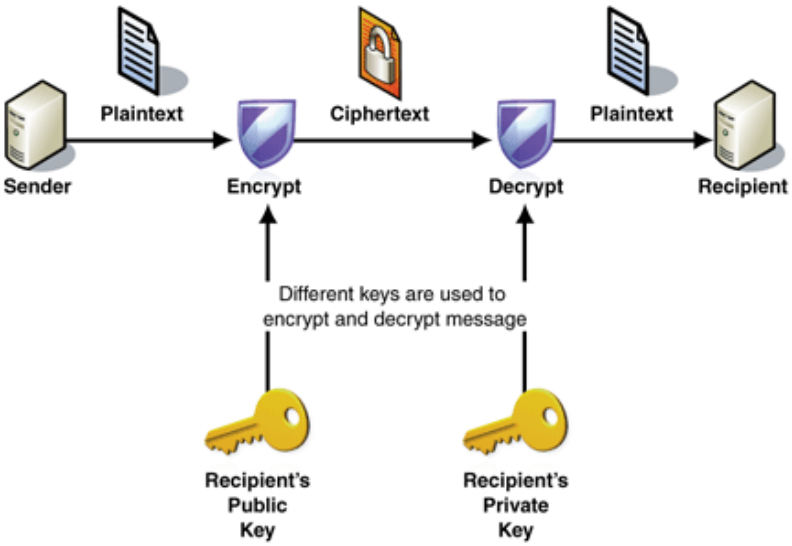
A gyakorlatban használt kriptográfiai eljárásokat két nagy csoportra oszthatjuk. Ezek közül a történelmi szempontból is nagyobb múlttal rendelkező megoldás a szimmetrikus kulcsú (Symmetric-key) titkosítás. Alapja, hogy a két kommunikáló fél egy közös kulcson osztozik, aminek felhasználásával megvalósulhat a küldeni kívánt üzenet titkosítása (adott esetben blokk kódolási vagy adatfolyam alapú/konvolúciós megoldással). A *kulcs* olyan információ, paramétere az adott algoritmusnak aminek segítségével a küldeni kívánt üzenet egyértelműen leképezhető titkosított üzenetre. Az üzenet fogadója a kulcs birtokában képes lesz visszafejteni a kódolt üzenetet, így megismerve annak eredeti tartalmát, míg bárki, aki nem rendelkezik a kulccsal, nem lesz képes elvégezni ugyanezt a műveletet. Fontos továbbá megemlíteni a biztonság forrását: ez az adott titkosítási módszer esetén az a tulajdonság/megfontolás, ami lehetővé teszi számunkra, hogy a módszert megbízhatónak tekintsük. Az említett esetekben az üzenetváltás biztonságát a kulcs rejtett volta garantálja, azaz hogy a beszélgető feleken kívül (akikre hagyományosan Alice-ként és Bob-ként, azaz A-ként és B-ként szokás hivatkozni) senki nem ismeri azt. A hosszantartóan megbízható kommunikáció megvalósítása érdekében fontos, hogy az egyébként titkosnak tekintett kulcsot adott időközönként lecseréljék a résztvevő felek, így védekezve az ellen, hogy egy illetéktelen fél (lehallgató) időközben megszerezze, vagy visszafejtse a huzamosabb ideig használt kulcsot. Lényeges szempont, hogy a későbbi kulcsok ne veszélyeztessék a korábbiak biztonságát, azaz egymástól legnagyobb mértékben függetlenek legyenek. Mivel Alice és Bob tipikusan nagy távolságra helyezkednek el egymástól, az egyik legfontosabb

megoldandó probléma az, hogy egy kapcsolat felépítése esetén, valamint kulcscsere alkalmával miként lehet a kulcsot biztonságosan megosztani egymással.



1.1. ábra. Szimmetrikus kulcsú titkosítás elvi működése [2]

1.1.2. Nyílt kulcsú titkosítás



1.2. ábra. Nyílt kulcsú titkosítás elvi működése [2]

A titkosítások másik nagy csoportját az aszimmetrikus, avagy nyílt kulcsú technikák adják. Ezekben az esetekben megkülönböztetünk két kulcsot, azaz Alice és Bob más-más információt birtokol. A küldő fél az úgynevezett nyilvános kulcs (*public key*) segítségével titkosítja a fogadónak szánt üzenetét, ami a nevének megfelelően nem szorul védelemre, nyilvánosan közzé tehető. A fogadó a hozzá eljutott üzenetet ezután egy újabb kulcs, a titkos kulcs (*secret key*) felhasználásával lesz képes értelmezni. A biztonság alapját a titkos kulcs titkos volt képezi, azaz hogy ez az információ kizárólag az arra feljogsított fogadó fél számára áll rendelkezésre. Továbbá teljesülnie kell annak a feltételnek, hogy

a titkos kulcs visszafejtése a nyilvános kulcsból kiindulva ne történhessen meg. Gyakorlatban ez a feltétel úgy módosul, hogy a visszafejtés irreálisan nagy számítási kapacitást, vagy hosszú időt igényeljen a lehallgatótól. Így a generálás legtöbb esetben olyan matematikai problémákon alapulnak, amik a jelen technológiai fejlettsége mellett *nehezen* megoldhatók. Az aszimmetrikus megoldást tipikusan kisebb adatsebességet igénylő alkalmazásokban használják egyirányú kommunikációra, de segítenek például a privát kulcsok cseréjének megvalósítása során szimmetrikus kulcsú rendszerekben is.

1.2. Perspektívák

Az fent leírt módon működő technológiáknak természetesen vannak nehezen orvosolható gyenge pontjaik. A szimmetrikus titkosítás esetén a már említett kulcsmegosztás a leginkább kritikus momentum, ennek során a leginkább kiszolgáltatott a kommunikáció. Bizonyos kritikus alkalmazások (pl.: katonai, kormányzati) nem engedhetik meg ezt a kiszolgáltatottságot.

Az aszimmetrikus módszereket egy más típusú fundamentális veszély fenyegeti. Az elmúlt évtizedekben jelentős fejlődés kezdődött a kvantuminformatika tudományterületén. A kvantumszámítógépek megvalósítása még napjainkban is gyakorlati nehézségekbe ütközik, de a cégek és kutatóintézetek egyre közelebb hozzák a szélesebb körben való elterjedés időpontját.
1994-ben Peter Shor olyan kvantum algoritmust prezentált [1] , amivel megoldható tetszőleges egész szám prímtényezőkre bontása. Nagy számok prímtényezőkre bontása tipikusan egy olyan matematikai probléma, amit klasszikus számítástechnikai apparátussal nem tudunk bizonyíthatóan megoldani. Ezt kihasználva, a nyílt kulcsú titkosítások jelentős hányada két nagy prímszám szorzatának segítségével generálja a nyilvános kulcsot, a feltörés pedig kizárólag a tényezők megtalálásával történhet. A kvantuminformatikai módszerek finomodásával és a kvantumszámítógép esetleges elterjedésével a jelenleg használt a titkosítási eljárásaink komoly része veszélynek lesznek kitéve, legyen szó akár az aszimmetrikus kulcsú technikákról, vagy aszimmetrikus megoldásokat felhasználó szimmetrikus elven működő rendszerekről.

2. fejezet

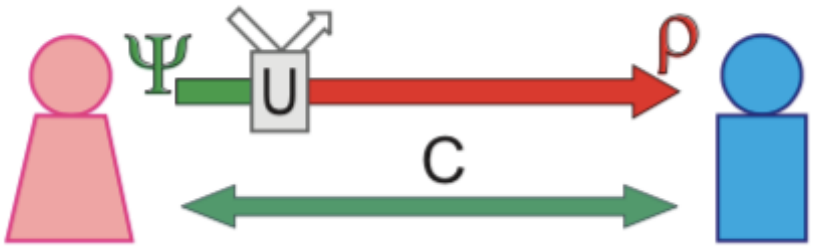
Kvantumos kulcsszétosztás

2.1. Elvi áttekintés

A fent említett okokból eredően új ötletekre van szükség jelenleg üzemelő rendszereink biztosítása érdekében. Az egyik lehetőség a kvantumos elven működő támadások elleni kvantumos alapú védekezés kialakítása. A gyakorlati megvalósítás szempontjából leginkább előrehaladott állapotban levő kutatási terület a kvantumos elvű kulcsszétosztás (quantum key distribution - QKD). A kvantumos kulcsszétosztó protokollok működésük során a szimmetrikus titkosítások leginkább gyenge pontját képező kulcsmegosztás lépését teszik biztonságossá kvantumfizikai alapvetéseket kihasználva. Amennyiben a titkos kulcs cseréje meghatározott időközönként garantált biztonsággal levezényelhető, a szimmetrikus kulcsú titkosítást használó kommunikáció is teljes biztonságban folyhat.

A QKD elvi modellben a két kommunikáló felet (Alice és Bob) klasszikus- és kvantumcsatorna köti össze (2.1 ábra), amiken képesek információt cserélni egymással. Feltesszük, hogy a lehallgató (*eavesdropper* - Eve) a klasszikus összeköttetést megfigyelheti, de nem befolyásolhatja a továbbított információt, valamint méréseket végezni a kvantumcsatornán és ilyen módon manipulálhatja azt. A feltételezés azért helyes, mert a lehallgató célja az észrevétlen működés, ezért nem zavarja a csatornát, hanem kicsatolással, vagy detektálással és ismétléssel igyekszik megismerni a csatornán áramló információt. A kvantum csatornán is ez lenne a célja, de kvantumfizikai alapvetések ezt nem teszik lehetővé. Alice kis energiájú fényimpulzusok (vagy különálló fotonok) formájában információt küld a kvantum csatornán, amit a fogadó megmér. A működés lényegi része, hogy a mérés után a klasszikus csatornát használva a felek egyeztetésbe kezdenek, amihez felhasználják a kvantumos csatornán küldött/fogadott információról megszerzett tudásuk egy részét. Az egyeztetés végén képesek lesznek eldönteni, ha az üzenetváltás során történt lehallgatás és ha arra van szükség megszakíthatják a kommunikációt.

A biztonság alapját az képezi, hogy - a klasszikus rendszerekkel ellentétben - a kvan-



2.1. ábra. CVQKD modell [3]

tumrendszereken végrehajtott mérés megváltoztatja a rendszer állapotát. Kommunikációs csatornákban gondolkodva: a lehallgatás, azaz információ kiszivárgása a csatornából közvetlen hatással van az üzenetváltás minőségére.
Továbbá a *no-cloning theorem* értelmében nem lehetséges eredetileg ismeretlen kvantumállapotról másolatot készíteni. Ebből ered, hogy a lehallgató (Eve) nem folyamodhat olyan módszerekhez, amik klasszikus csatornákban gondolkodva akár sikeresek lehetnének. Egy hagyományos összeköttetés lehetővé tenné, hogy Eve egy köztes ponton megcsapolja a csatornát, megfigyelje a feladótól származó információt, majd újra előállítva tovább küldje azt a fogadónak.

A QKD technológiákat 3 nagy csoportra oszthatjuk:

- Diszkrét változós (*discrete-variable*) QKD
- Folytonos változós (*continous-variable*) QKD
- Elosztott fázisreferenciás (*distributed-phase-reference*) QKD

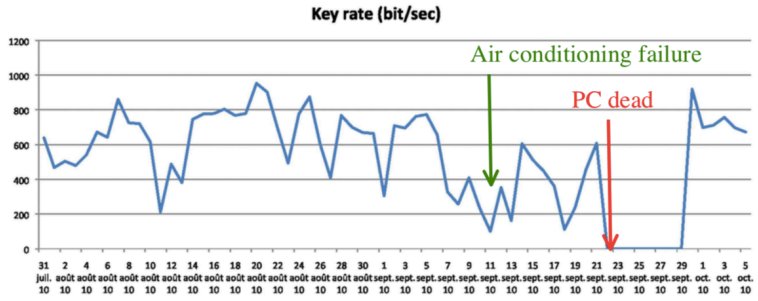
Dolgozatom témája egy folytonos változós QKD optikai összeköttetés. A folytonos változós megvalósítás előnye a többi felsorolttal szemben, hogy egyszerűbb, telekommunikációban már használt, kiforrott eszközök felhasználásával is felépíthető az összeköttetés. A listán szereplő első és utolsó esetben az információt különálló fotonok kódolják, amik előállítása nehézkes, továbbításuk zajos csatornán problémás, detektálásuk pedig csak kis sebességgel valósítható meg. CVQKD rendszerekben az információt a fény amplitúdója és fázisa kódolja, így az optikai jel előállítása történhet hagyományos távközlési lézerekkel, a vevő oldalon pedig nagy sebességű detektálásra alkalmas PIN fotodiódákat is üzembe lehet helyezni.

2.2. Gyakorlati megvalósítás

A folytonos változós kucsszétosztás a többi módszerrel összehasonlított relatív alacsony eszközigénye miatt egyre szélesebb körben kutatott téma. A módszert leíró első publikációk a kétezres évek elején születtek ([4]), azóta már gyakorlatban bizonyították a rendszer

működőképességét, sőt, a CVQKD rendszerek a laboratóriumból is kikerültek, és telepített optikai szálon is tesztelve lettek.

2008 novemberében az European Integrated Project (SECOQC) keretein belül, egy komplex kvantumos kulcsszétosztó hálózat részeként demonstráltak egy működő, 8 km hosszú optikai szálon keresztül felépített CVQKD összeköttetést ([13]). Az optikai szál csillapítása ebben az esteben 2.5 $\frac{dB}{km}$ volt, maximálisan 8 kbps-os kulcssebességet sikerült elérni ([5], [6]).
Hasonló célja volt a Symmetric Encryption with QUantum key REnewal (SEQURE) nevű projektnek. Ebben az esetben egy telekommunikációs célokra fektetett 12 km-es (6.5 dB csillapítás) szálon mutatták be a CVQKD működőképességét ([13]). Az összeköttetés közel 2 hónapon keresztül képes volt folyamatos üzemben működni, maximálisan 1 kbps-os kulcssebességgel.



2.2. ábra. SEQURE CVQKD rendszer kulcssebessége [13]

Ezekből a példákból is látható, hogy nem kis feladat az összeköttetés fenntartása hosszú időn (akár napokon) keresztül. Éppen ezért ezt a paramétert az adott rendszer egyik lényeges leírójának tekinthetjük. Fontos még az elérhető átlagos/maximális kulcssebesség is. Általánosságban elmondható, hogy lényegesen alacsonyabb modulációs sebességgel dolgozunk a kvantumos rendszerekben, mint a hagyományos kommunikációs rendszerekben, továbbá figyelembe kell venni, hogy az átvitt adat egy részétől is kénytelenek vagyunk megválni az utófeldolgozás miatt. Ebből ered, hogy az effektív kulcssebesség lényegesen alacsonyabb lesz, mint az az adatátviteli sebesség, amit a moduláció módja és sebessége alapján várnánk. Nagyobb távolságokat feltételezve az átvitel degradálódik, ezért lényeges kérdés, hogy az adott CVQKD rendszer milyen távolságon képes kapcsolatot létesíteni és fenntartani. A témában folytatott kutatások egy része a távolság kiterjesztésének kérdését járja körbe ([7], [8]), miközben létezik olyan kereskedelmi forgalomban is kapható termék, ami a 80 km-es optikai szálon való fenntartható működést kínál ([13]).
2017-ben a Műegyetem is bekapcsolódott egy olyan kezdeményezésbe, melynek részét képezi egy CVQKD alapú, biztonságos külcsszétosztás laboratóriumi körülmények között történő megvalósítása. A dolgozatban bemutatott munkám is ennek képezi részét.

3. fejezet

Optikai hálózat

A fejezetben a fizikai réteg szintjén bemutatom a CVQKD kulcsszétosztás folyamatát, azaz a kis energiájú kommunikációhoz használt impulzusok átvitelének menetét, valamint az ezt megvalósító optikai hálózatot.

3.1. Működés

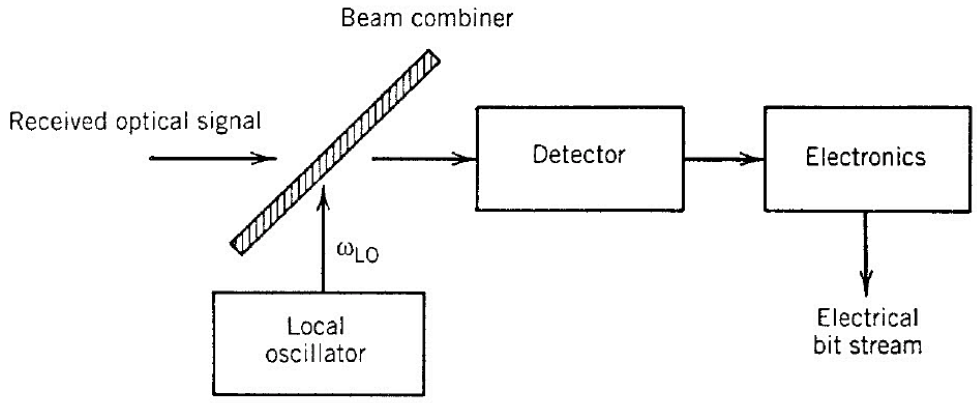
3.1.1. Koherens vétel

Alice fényimpulzusok kvadratúrájába kódolt véletlen komplex számokat állít elő, ezeket optikai szálon Bobnak küldi el, aki homodin detektálási módszerrel dolgozik. Ha a küldeni kívánt komplex szám $z = x + iy$, és $E_x \sim x$ és $E_y \sim y$, akkor a küldött impulzus amplitúdója a k-adik időpillanatban $E(k) = E_x(k) + jE_y(k)$. Egyszerűbben megfogalmazva az adó egy komplex IQ modulációt használ, az információt a fényimpulzusok amplitúdója és fázisa hordozza. A megvalósításhoz ezek szerint egy optikai amplitúdó- és fázismodulátorra van szükség, a vevőben pedig ennek megfelelő detektorra. Jó megoldásnak bizonyul a nagysebességű optikai átviteli rendszerekben már bevált koherens adó-vevő struktúra bevezetése.

A koherens vétel alapja, hogy az adó oldalon optikai IQ modulált jel detekciójához kihasználjuk a fotodióda bemeneti optikai teljesítménye és kimeneti árama közötti négyzetes összefüggést. A detektorra a vett jelnek egy helyi optikai forrással (LO) való keveredési termékét juttatjuk, így a négyzetes karakterisztika miatt a dióda kimenetén megjelennek további keveredés produktumok.

A bemenetre jutó hasznos optikai jel komplex amplitúdója:

$$E_s = A_s e^{-j(\omega_s t + \phi_s)} \tag{3.1}$$



3.1. ábra. Koherens vevő elvi blokkvázlata [9]

A bemenetre jutó helyi oszcillátor (LO) komplex amplitúdója:

$$E_{LO} = A_{LO}e^{-j(\omega_{LO}t+\phi_{LO})} \tag{3.2}$$

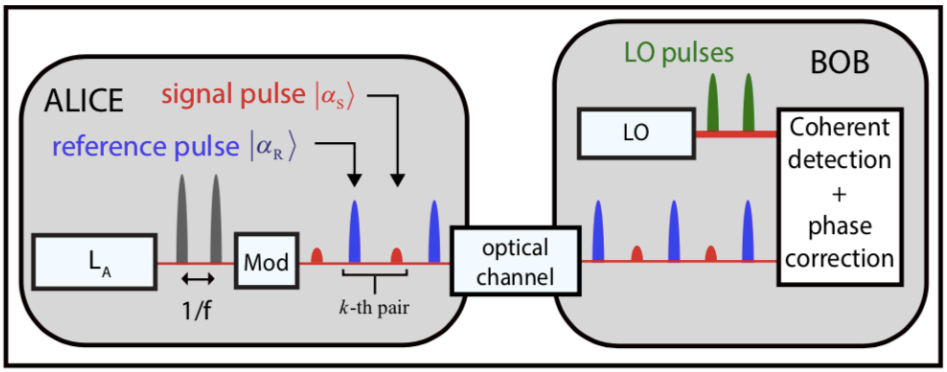
A dióda kimenetén az elektromos teljesítmény időfüggvénye a következő lesz:

$$P(t) = P_s + P_{LO} + 2\sqrt{P_s P_{LO}}\cos(\omega_{IF}t + \phi) \tag{3.3}$$

A koherens vétel előnye, hogy a helyi oszcillátor "erősíti" a hasznos jelet. Ha az optikai keverő modulra a hasznos jelhez fázisban illesztett LO-t kapcsolom, a vevő kimenetén az IQ modulált optikai jel fázisban levő (*in-phase*) vetületével arányos teljesítmény jelenik meg, ha az oszcillátort 90 fokkal késleltetem, a kvadratúra (*quadrature*) vetülettel.

A koherens vevőt működtetve egy fontos megoldandó feladat a fázishelyes referencia jel biztosítása. Ez a feladat a CVQKD működés szempontjából is kimelet fontosságú lesz. Ennek előállításra több lehetőség is kínálkozik [10]:

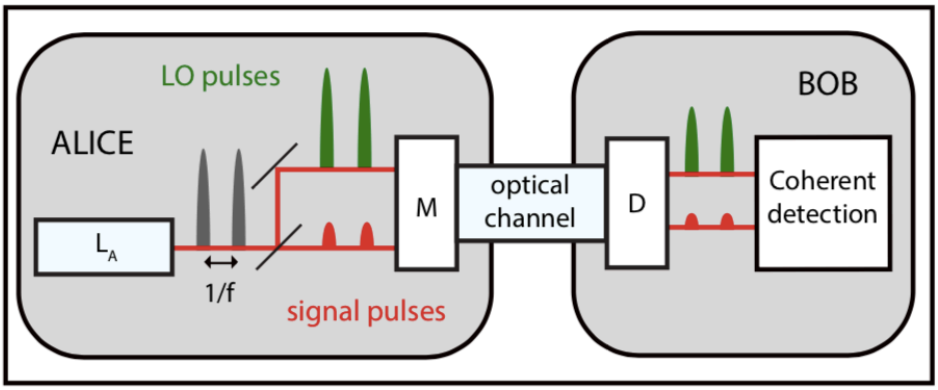
1. Megtehetjük, hogy az adótól a vevőig kizárólag a hasznos jelet továbbítjuk, majd a referenciát a vevő oldalon generáljuk (3.2 ábra). Ezt lehetőséget választva nehézséget okoz, hogy a két forrás (vevő és adó oldalon) nincs fázisszinkronban, ezért a feladat egy újabb szabályozási feladattal bővül. [10] forrásban egy olyan megoldás kerül prezentálásra, amiben az adó a hasznos jellel időben multiplexálva nagy amplitúdójú, fix fázisú szinkronizáló impulzusokat továbbít, amiket a vevő felhasznál a helyi Local Oscillator lézer fázisának szabályozásához. A szerző előnyként emeli ki az ilyen módon elérhető kis fáziszajt, valamint az, hogy referencia jel helyben (vevőn belül) történő előállítása nem nyújt lehetőséget annak továbbítás közben történő manipulálására. Hátránya, hogy a vevőben bonyolult vezérlési feladatokat kell ellátni.



3.2. ábra. Lokális optikai referencia előállítás [10]

2. Az általam szimulált hálózat egy megvalósítás és vezérlés szempontjából egyszerűbb verziót használ (3.3 ábra). A referenciát az adó állítja elő és küldi a vevőnek az optikai szálon keresztül. Továbbra is kérdés marad, hogy a referencia jelet a hasznos jeltől különböző, vagy azonos közegen keresztül továbbítsuk. Jelen pontban bemutatott, és 3.3 ábrán is látható megoldás legtöbb esteben nem alkalmazható, ugyanis az előre telepített hálózatokban cél, hogy egy darab üvegszálat tudjunk használni a kommunikációhoz. Továbbá azért is problematikus a referencia és hasznos jelek külön szálon történő továbbítása, mert a fáziszajra rendkívül érzékeny a rendszer, ilyen módon pedig a fázishiba kézben tartása lényegesen nagyobb feladat két szeparált közeg esetén.

3. A végleges cél ezért az lesz, hogy a két optikai jel (hasznos és referencia) közös fényvezető szálon terjedjenek az adó oldalon történő generálásuk után. Természetesen ez a választás is felvet egy sor problémát. Megoldandó feladat a hasznos jel és a referencia közötti áthallás csökkentése. A CVQKD rendszerben ez hatványozottan nagyobb jelentőségű lesz, mint egy hagyományos, nagysebsségű koherens kommunikációs rendszerben, ugyanis esetünkben a két jel közötti teljesítménykülönbségek több nagyságrendet tesznek ki. Erre nyújt megoldást az impulzusüzemű működés, valamint az időben és polarizációban való multiplexálás, amik jelentőségét a következő alfejezetekben fogom bemutatni.



3.3. ábra. Távoli optikai referencia előállítás [10]

3.2. Impulzusüzemű működés és időbeli multiplexálás

A választott homodin működésmód a referencia és hasznos jel szétválasztása miatt megköveteli az impulzusüzem bevezetését. A folytonosan működő lézer jeléből impulzusokat vágunk ki, ezeket teljesítményosztás alapon hasznos és referencia jelre választjuk szét, majd egymáshoz képest késleltetjük őket, aminek eredménye, hogy időben elválasztva fognak terjedni a hálózaton. Az ilyen módon való szétválasztást értelemszerűen nem lehetett volna folytonos lézerműködés mellett megvalósítani, az impulzusüzem elengedhetetlen. Ezen a ponton az általános tárgyalástól elmozdulva a ténylegesen modellezett CVQKD rendszer blokkvázlata (3.5) segítségével fogom tovább magyarázni a működést. Néhány konkrét eszközparamétert még ebben a fejezetben leírok, de a következő részeben, a modellezési megfontolások között fogom részletesen ismertetni az összes építőelem szimuláció szempontjából releváns paramétereit.

A kialakítás módja: a optikai vivőt az eredeti rendszerben egy 5 mW teljesítményű, 1550 nm-en emittáló lézer biztosítja, amit egy izolátor véd a reflexióktól (3.5 ábra jelölésrendszere szerint: LAS és ISO Alice oldalán). Ezután egy *chopper*, azaz egy megfelelő munkapontra állított amplitúdó modulátor következik, ami impulzusokat vág ki a lézer jeléből. A konkrét rendszerben az impulzusok 4 μs-os periódussal követik egymást, időtartamuk 400 ns (azaz 10%-os kitöltésről beszélhetünk).

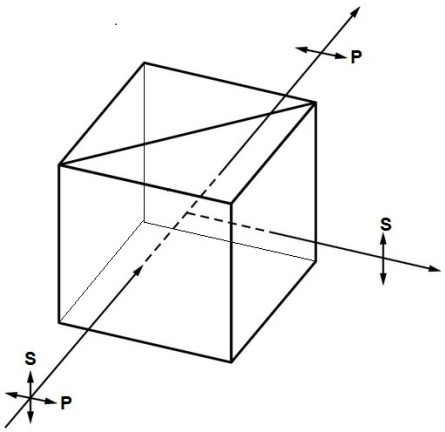
A modulálás utána Alice adójában a BS2 jelű teljesítményosztó 90:10 arányban választja szét az optikai jelet. A 10%-os teljesítményű út lesz a hasznos jel, amit modulálás után a PBS1-en keresztül 50 méteres polarizációtartó szálra kerül, majd reflektálódik, ennek megfelelően időkésleltetést szenved, ezért adott hasznos jel impulzus később kerül a PBS2 összegzőre, mint a hozzá tartozó referencia impulzus. Az 50 méteres késleltetővonal körül látható struktúra a polarizációkezelés szempontjából lényeges, ezt a következő szekcióban magyarázom.

Bob vevőjében a PBS2 hasonlóan szétválasztja a referencia jeleket (ebben az esetben már polarizációs állapot alapján PBS1 segítségével), de itt a referencia jel szenved azonos

mértékű késleltetést, ezért a vevőbe már azonos időben fognak érkezni.

3.3. Polarizáció kezelés

A lehető legnagyobb mértékű szeparáció, azaz legkisebb áthallás érdekében a referencia és hasznos jel elválasztása nem csak időben valósul meg, hanem polarizációs állapotban is, aminek kulcs eszköze a polarizációs nyalábosztó és -kombináló (PBS, PBC). Ezek az eszközök a bekötés módjának megfelelően látnak el szétválasztó, vagy kombináló funkciót, ezért a lenti blokkvázlaton leegyszerűsítve kizárólag osztóként (*polarization beam splitter* - PBS) hivatkozok rájuk.



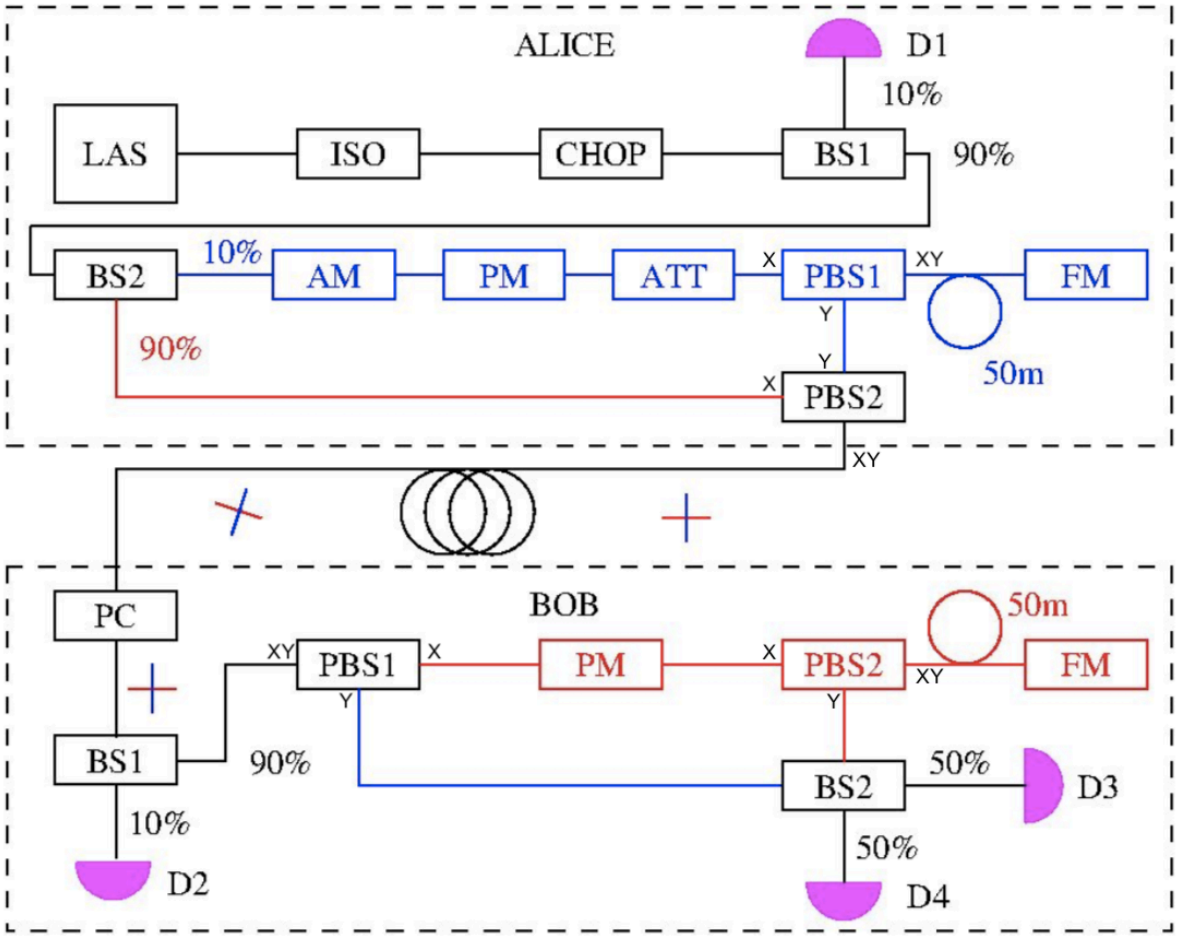
3.4. ábra. PBS theory [11]

A PBS elvi működése a 3.4 ábrán látható. 3 bemenettel rendelkezik, egy közös, valamint kettő polarizált porttal. A közös bemenetre jutó jelet a két, egymásra merőleges polarizációs módusnak megfelelően a polarizált portokra juttatja. Ellenkező irányban működtetve: a polarizált portokra megfelelő módusnak megfelelő lineárisan polarizált jelet juttatva a kombinált jel a közös porton jelenik meg.
Az adóban (Alice, 3.5 ábra) a hasznos jel polarizációs állapotát fogjuk megváltoztatni olyan módon, hogy a referencia jelre merőleges polarizációs módusban terjedjen a fényvezető szálon. Tegyük fel, hogy az adó oldali lézerünk ideálisan működik, teljesítményének teljes egészét egy polarizációs módusban adja le; legyen ez az X tengely mentén polarizált irány. Ebből a jelből impulzusokat formálunk, majd teljesítményosztás és a moduláló szekció után PBS1-re juttatjuk. Tegyük fel hogy az említett jel polarizációs állapota továbbra sem változott. PBS1-nek az X irányban polarizált portjára kapcsoljuk, aminek következménye lesz, hogy a közös porton fog megjelenni. Esetünkben erre van kapcsolva az 50 méteres késleltetővonal. Ezen késleltetést szenved, azaz időben elválik a hasznos impulzustól, majd az FM jelölésű eszközre jut, ami egy Faraday-tükör. Erről a fény 90 fokos polarizációs állapotban való elforgatást szenvedve reflektálódik, azaz Y polarizációs

állapotba kerül. Visszafelé irányban újra PBS1-re jut, de Y irányú polarizációja miatt már nem annak X portján távozik, hanem az Y jelölésűn. PBS2 ezután kombinálja az X polaruzált referncia és Y polaruzált hasznos jeleket, amik itt már időben elkülönítve, egymásra ortogonális polarizációban terjednek. A vevőben (Bob) a hasznos és referencia jel újbóli szétválasztása kiemelt jelentőségű, ezt a PBS1 jelölésű polarizációs nyalábosztó végzi. Ezen az oldalon a referencia jelre egy előzőleg látható módon véghezvitt időbeli késleltetést és polarizációs állapotban való módosítást láthatunk az ott látható PBS1, késleltetővonal és FM segítségével. Így a vevő előtti optikai keverőre (ami egy 2x2 optikai csatoló) a hasznos és referencia jelek azonos időben, közös (Y) polarizációs állapotban jutnak.
A vevő oldali szeparálás (PBS1) szempontjából rendkívüli fontosságú az eredeti polarizációs állapot helyreállítása a vevő bemenetén. A hálózatban nincs lehetőség polarizációtartó szállal dolgozni, ezért az adó kimenetéhez képest a polarizációs állapot dinamikusan, nem megjósolhatóan módosulni fog a terjedés során. A helyreállítást a PC jelölésű kontroller végzi az átvitel működése közben.
Az ideális működés feltevése a valóságban nyilvánvalóan nem áll meg, ezeket az leegyszerűsítéseket kizárólag a működés könnyebb leírása miatt tettem meg. A rendszer zaját éppen az előbb bemutatott eszközök valós, nem-ideális viselkedése fogja adni. A minőséget befolyásolni fogja például nyalábosztók egyes csatornák közti izolációja, valamint a lézer keresztpolarizációs csillapítása, és még jónéhány más paraméter. Dolgozatom elsődleges célja, hogy a valósághoz legközelebb álló módon paraméterezzek a szimulációk során, felhasználva a *datasheet*-eket és mérési eredményeket. Ezután identifikáljam azokat a paramétereket, amik megváltoztatása legnagyobb mértékben hat a rendszer zajára, majd reális keretek között mozgó és költséghatékony javaslatokat tegyek, amiket eszközölve javulás érhető el. Végeredményben a kimeneti zaj csökkentése a cél, ugyanis csak így érhető el, hogy olyan kis energiájú, kevés fotonból álló impulzusok is detektálhatóak legyenek, amilyen kevés fotonnál már érvényesülnek a megbízható működés alapját adó kvantumos hatások.

3.4. Moduláció

Alice véletlenszerűen állít elő komplex számokat, amiket a fogadó oldalra küld. Az információt a fényimpulzusok fázisa és amplitúdója hordozza, a moduláció Alice oldalán jelölt amplitúdó-modulátorral (3.5 ábra jelölésrendszere szerint: AM) és fázismodulátorral (PM) valósul meg. Az ATT jelölésű eszköz további csillapítást visz a hasznos jel útjába, hogy a kívánt teljesítmény precízen és dinamikusan állítható legyen.
Bob vevőjében a referencia jel útjába iktatott fázismodulátor (PM) arra szolgál, hogy a fogadó fél véletlenszerűen választhassa ki a fogadott jel mért komponensét. A fázismodulátort 0 és 90 fokos fázistolás között kapcsolva megadható a vett jel mért vetülete.



3.5. ábra. A szimulációs programban felépített rendszer blokkvázlata

4. fejezet

Modell

A fejezetben bemutatom a CVQKD összeköttetést megvalósító optikai hálózati modellt, annak korlátait, ismertetem az alapvető szimulációs megfontolásokat, valamint a felmerülő problémákat/kérdéseket.

4.1. Szimulációs program

Munkámhoz a VPI Transmission Maker (továbbiakban VPI) szimulációs környezetet használom, ami egy speciális optikai célú szimulációs környezet. Elsősorban összetett rendszerek vizsgálatára alkalmas, amik előre elkészített eszközmodellekből, ezekből kialakított bonyolultabb modellekből, és külső MATLAB/Python/DLL eszközleíró modellekből épülnek fel. Jelen szimuláció során az utóbbi lehetőséget nem vettem igénybe, nem készítettem saját eszközmodelleket. Amennyiben egy beépített modell részletessége nem volt kielégítő a CVQKD működés szempontjából, vagy lényeges paraméter beállítási lehetősége hiányzott, ahhoz az egyszerűbb megoldáshoz folyamodtam, hogy a már rendelkezésre álló egyéb eszközökből konstruáltam bonyolultabb modellt hierarchikus terezés segítségével.
Az említett szoftverrel kizárólag klasszikus optikai rendszereket lehet szimulálni, ennek megfelelően kvantumfizikai jelenségeket nem vagyok képes modellezni vele. Ezen kívül egy működő CVQKD összeköttetés lényegi részét képezi a magasabb, protokol szintű megvalósítás is, ami a csatorna biztonságának felméréséről gondoskodik a kvantumos csatornán szerzett méréseket felhasználva. Ezt szintén nincs lehetőségem a VPI szoftverrel szimulálni. Viszont ezek nem is tartoznak dolgozatom célkitűzési közé. Egy olyan kiszajú klasszikus optikai rendszert kívánok alkotni, amin lehetséges azokon az energiaszinteken való kommunikáció, amiken már számolni kell a kvantumfizikai hatásokkal. Csak ennek teljesítése után lehet foglalkozni a magasabb szintű működés kidolgozásával, mert annak alapja egy jól működő fizikai rendszer.

4.2. Szimulációs megfontolások

A modellek valós eszközökön alapuló paraméterbeállításain kívül fontosnak tartok megtenni néhány kiegészítést, ugyanis nem minden lényeges paraméter állt rendelkezésemre a szimulációkhoz.

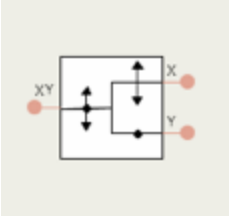
- A lézer működése polarizáció szempontjából nem ideális, azaz nem kizárólag lineárisan polarizált fényt sugároz. Az adatlapon erre vonatkozó információt nem találtam, ezért 20 dB körüli keresztpolarizációs elnyomást feltételeztem, ami egy tipikus értéknek tekinthető, azaz az ortogonális tengelyek mentén sugárzott optikai teljesítmények aránya 1:100.

- Ahogy az eszközök listáján is látható, legtöbb esetben polarizáció tartó eszközökkel lesz felépítve a valós rendszer. Erre a polarizációra érzékeny működés miatt van nagy szükség, a cél az lenne, hogy polarizáció forgató hatásuk 0 legyen. Ezen eszközök esetén definiálva van egy a gyártó által polarizációs kioltási tényezőnek (PER) nevezett paraméter (lenti táblázat), ami az ideális esettől való eltérést számszerűsíti, tipikus értéke 20 dB. Jelentése: ha ezekre az eszközökre tökéletesen X irányban polarizált fényt juttatunk, a kimeneten nem kizárólag X polarizációjú fény jelenik meg. A kívánt és nem kívánt polarizációs irányok/tengelyek teljesítményének arányát adja meg a PER paraméter, 20 dB-re 100-szor kisebb teljesítmény lesz mérhető a nem kívánt polarizációs állapotban (feltéve, hogy a bemenetre lineárisan polarizált fény került). A hatás forgatással is leírható, így 20 dB-es PER- feltételezve kb. 5.71 fokos forgatást fog okozni az adott eszköz. Szimulációim során ezért forgatással modelleztem a polarizációtartó működéstől való eltérést, worst case esetet feltételezve a forgatás iránya azonos minden eszköznél.

- Az Alice és Bob oldalán is fellelhető, monitorozásra használt, BS1 jelű teljesítményosztók első pillantásra elhagyhatónak tűnhetnek, ugyanis a szimulációs programban teljesítmény kicsatolása nélkül is lehetőségünk van az optikai és elektromos jelek változásának megfigyelésére. Ennek ellenére ezeket mégis szükséges beépíteni a szimulációkba. Egyrészt teljesítményt csatolnak ki a jelfolyamól, de ennél is lényegesebb hatásuk, hogy nem tökéletesen polarizációtartó a működésük.

- Polarizációs osztók és összeadók két célból kerülnek beépítésre: hasznos és referencia jelek összeadására és szétválasztására a hozzáférési hálózat elején és végén, valamint cirkulátor szerű működést valósítanak meg a Faraday-tükrös késleltető struktúra segítségével. A magyarázathoz felhasználom a polarizációs osztó VPI grafikus reprezentációját (4.1 ábra). Alice oldalán az 4.1 ábrán látható PBS-re a hasznos jel az X porton kerül, a Faraday-tükrös késleltető struktúra a jelölés nélküli közös portra csatlakozik (nevezzük XY portnak), a késleltetett és polarizációban elforgatott

hasznos jel az Y porton hagyja el a PBS-t. Valós működés esetén áthallás lesz tapasztalható az X és Y portok között, azaz az X portra kerülő jel egy része az Y porton fog távozni a Faraday-tükrös késleltető struktúra kikerülésével. A portok közti áthallásra vonatkozó információt viszont nem találtam az eszköz specifikációjában. A lenti táblázatban jelölt "Kioltási tényező" paraméter sem erre vonatkozik (és nem azonos a PER paraméterrel sem), hanem azt adja meg, hogy a közös (XY) portra jutó Y polarizált jel mekkora része fog az X porton távozni; vagy hogy az X portra jutó Y polarizált jel mekkora csillapítást szenved, amíg a közös (XY) portra jut.
Információ hiányában megmértem az említett áthallást és egy meglehetősen alacsony 60 dB körüli értéket kaptam, azaz az az optikai teljesítmény, ami megkerüli a késleltetős/polarizációforgató struktúrát és azonnal a kimenetre jut, 60 dB-lel alacsonyabb, mint a bemenő teljesítmény.



4.1. ábra. Polarizációs nyalábosztó modell grafikus reprezentációja

- Az amplitúdó- és fázismodulátor polarizációfüggő viselkedéséről nem állt rendelkezésre információ és nem volt lehetőségem megmérni, ezért ideális, polarizációfüggetlen, polarizációtartó működést feltételeztem.

- A vevő oldali polarizáció szabályozás maximális teljesítményre szabályoz, azaz egy referenciapont teljesítményét maximalizálja az által, hogy a bemenetére kapcsolt optikai jel polarizációját változtatja. A szabályozás kérdésével részeletesen nem foglalkoztam, nem igyekeztem kidolgozni új algoritmust.

- A chopper vezérlést a kapott instrukcióknak megfelelően állítottam be, 400 ns hosszú impulzusokat vág ki a lézer jeléből, 4 μs periodicitással. Az chopper vezérlés illesztetlenségéből adódó hullámzást figyelembe vettem a szimulációkban: 12%-os túllövést, 180 ns-os lecsengést állítottam be. Tapasztalataim szerint az átvitel minőségét döntően nem befolyásolja a hullámosság, az egyetlen emiatt adódó probléma, hogy a lecsengés miatt kevesebb idő jut a mintavételezésre, pontosabban kell beállítani azt.

- A hasznos jelútba iktatott adó oldali csillapításról nincs információm, 20 dB csillapítást feltételezek, a hozzáférési hálózatot 10 km hosszú SMF-28 optikai szál reprezentálta.

4.3. Eszközparaméterek

EP 1550-NLW-DX1 (LAS)	Hullámhossz	1550 nm
	Teljesítmény	5 mW
	Polarizációs kioltási tényező	20 dB
	Vonalszélesség	100 kHz
IO-G-1550-APC (ISO)	Izoláció	28 dB
	Beiktatási csillapítás	0.55 dB
	Polarizációs kioltási tényező (PER)	20 dB
LN81S-FC (CHOP és AM)	DC kioltási tényező (DC IL)	20 dB
	PRBS kioltási tényező	13 dB
	Beiktatási csillapítás (IL)	4 dB
LN53S-FC (PM)	Beiktatási csillapítás (IL)	3 dB
PMC1550-90B-APC (BS1, Alice BS2)	Osztásarány	10 / 90 %
	Beiktatási csillapítás	0.95 / 11.3 dB
	Polarizációs kioltási tényező (PER)	18 / 18 dB
PMC1550-50B-APC (Bob BS2)	Osztásarány	50 / 50 %
	Beiktatási csillapítás	3.6 / 3.6 dB
	Polarizációs kioltási tényező (PER)	18 / 18 dB
VOA50PM-APC (ATT)	Polarizációs kioltási tényező (PER)	18 dB
	Beiktatási csillapítás (IL)	0.9 dB
PBC1550PM-APC (PBS)	Beiktatási csillapítás (IL)	1.2 dB
	Kioltási tényező	20 dB
MFI-1550-APC (FM)	Beiktatási csillapítás (IL)	0.5 dB
	Forgatás	45 $\pm$ 1 fok
ILP1550PM-ACP (polarizátor)	Beiktatási csillapítás (IL)	0.8 dB
	Kioltási tényező	28 dB

4.1. táblázat. A próbaösszeköttetésbe beépített eszközök listája

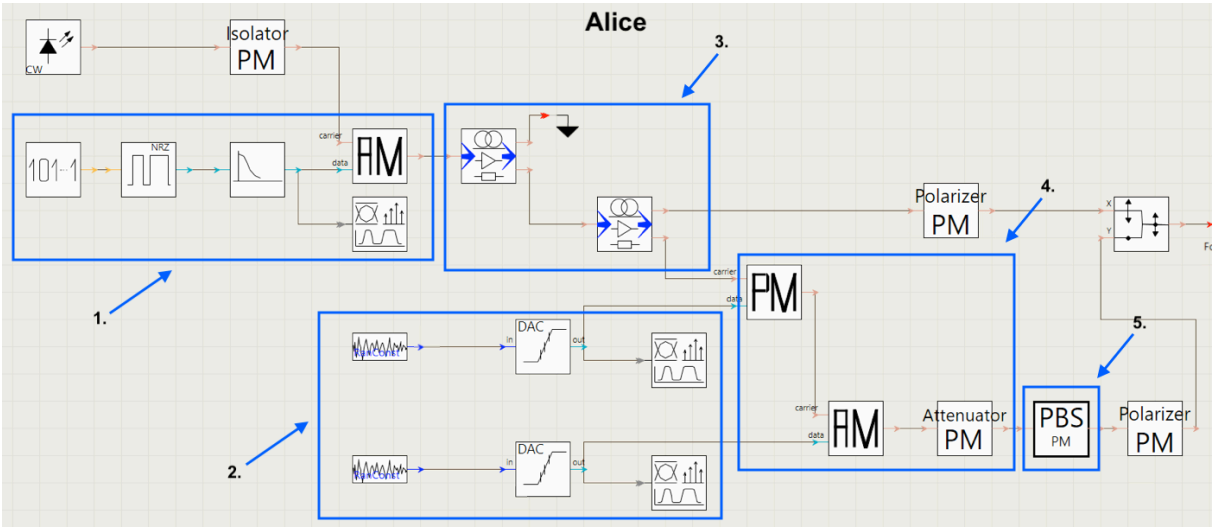
4.4. Felépített VPI modell

4.2 és 4.3 ábrákon a VPI TRansmission Maker szimulációs környezet grafikus kezelőfelületében felépített komplex rendszerek látszanak. Ezekkel szeretnék megmutatni néhány lényeges, jellegzetes struktúrát az adóban és vevőben. Az ezeken látható jelfolyamba kapcsolt elemek, "dobozok" egy része kikapcsoltható, ennek megfelelően nem minden később látható

szimuáció során lesz aktív. Tipikusan ilyen blokk a polarizátor - amiből az összes ábrákon látható elem sosem volt aktív egyszerre-, és a csillapító is.
A tervezés során használtam hierarchikus design megfontolásokat, ezért az ábrán látható blokkok egy jelentős része tovább bontható, nem egy elemi beépített modellt tartalmaz.

4.4.1. Adó

A 4.2 ábra a szimulációs környezet grafikus kezelőfelületén felépített adót mutatja.



4.2. ábra. A szimulációs programban felépített adó modell grafikus reprezentációja

1. Chopper szekció, logikai és elektromos vezérléssel, valamint optikai beavatkozással. Megfelelően időzített logikai jelfolyamot állítok elő, amit aztán elektromos jellé konvertálunk a NRZ kódolás szerint. Ezután egy szűrővel beállítom vezérlőjel túllövését, majd az AM jelű amplitudómodulátorral beavatkozok az optikai jelfolyamba. A párhuzamosan lecsatlakozó, bonyolult jelölésű elem egy analizátor blokk, amivel az adott csomópont idő és frekvenciatartománybeli viselkedését tudjuk megfigyelni.

2. Modulátor elektromos vezérlés. Véletlenszámot állítunk elő, amit aztán az átvinni kívánt állapotok számának megfelelően kvantálunk egy DAC-vel, így elektromos jelet alakítva belőle. Ezen a részen nagyon jól látszik, ahogy a VPI a különböző típusú jeleket hogyan különbözteti meg a kezelőfelület szintjén. A sötét kék nyíllal jelölt blokk kimenet lebegőpontosan ábrázolt számokat jelöl, a világoskék "elektromos" jel reprezentációt, a halvány barna (pl.: a PM carrier bemenete) pedig "optikai" jelet.

3. Monitorozásra és hasznos és referencia jel szétválasztására használt polarizációtartó teljesítményosztók modellje.

4. Modulátor szekció optikai része.

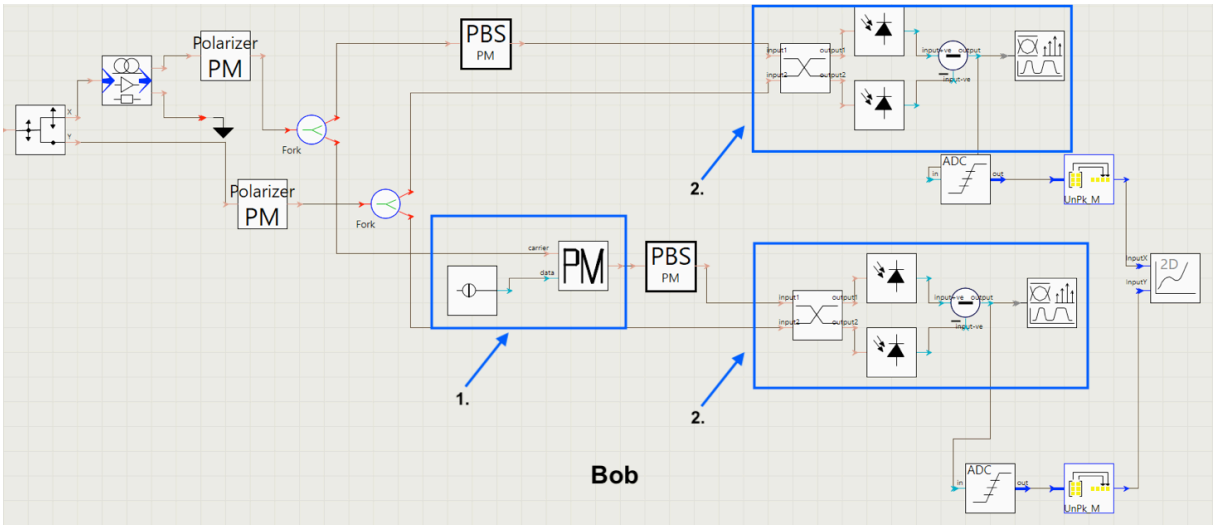
5. A teljes késleltető és polarizációforgató struktúrát megvalósító modell egyszerűsített grafikus megjelenítése.

4.4.2. Vevő

A 4.3 ábra a szimulációs környezet grafikus kezelőfelületén felépített vevőt mutatja.

1. Mérési kvadartúra kiválasztásához használt fázismodulátor.

2. Homodin vevő struktúra. A működő rendszerben kizárólag egy vevő egység található, a mérési kvadartúra szimbólumidőnként véletlenszerűen változik a fázismodulátor állásának módosításával. A szimulációkban két vevőt használtam, hogy egyszerre tudjam mérni a két kvadratúrát, ezzel megkönnyítve az eredmények értékelését.



4.3. ábra. A szimulációs programban felépített vevő modell grafikus reprezentációja

5. fejezet

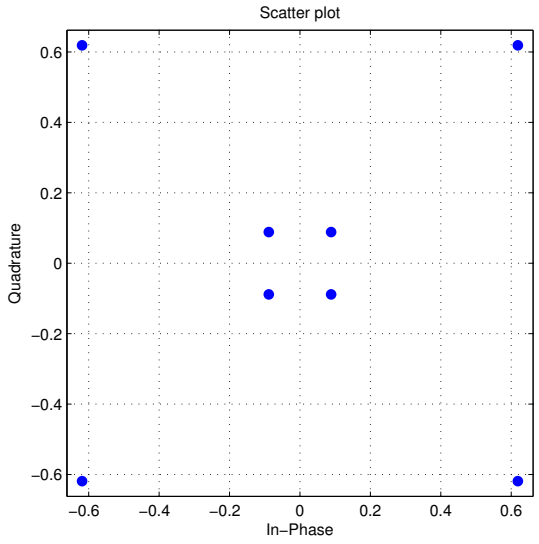
Minősítés

A rendszert először leegyszerűsítve építettem fel a szimulációs környezetben, majd fokozatosan bővítettem ki, így növelve annak bonyolultságát. Már az első szimulációk során felmerült a probléma, hogy milyen paraméterek alapján minősítsem a működést, milyen célfüggvényt fogalmazzak meg a finomhangolás során. A szimulációs program lehetővé teszi, hogy a vevő kimenetén megjelenő elektromos jel időbeli lefutását és frekveciatartománybeli viselkedését is vizsgáljuk, majd ezeket az adatokat felhasználva, adott esetben mintavételezéssel számszerű kimeneti értékeket kapjunk.
Az értékelés során fontos szem előtt tartani, hogy annak ellenére, hogy a rendszernek számos olyan kiegészítése van, ami nem konvencionális a hagyományos nagysebességű optikai távközlés szempontjából, továbbra is egy koherens vételi rendszerről beszélhetünk. Ebből a felfogásból adódik, hogy a jól bevált leíró metrikák - BER, SER, EVM, konstellációs diagram, szemábra - kisebb megkötésekkel bevezethetők lesznek. Ezek közül az EVM-et fogom használni, miután a mintavételezést az impulzusok idejének utolsó harmadában végeztem el. Az így kapott adatsorból MATLAB feldolgozással készítettem konstellációs diagramot az adott szimbólumsorozat ismeretében, majd számítottam EVM-et (*Error Vector Magnitude*). Az EVM következő definícióját használom a számításhoz, a modulációs sémák konstellációs diagramjai a 7.11 ábrán láthatóak:

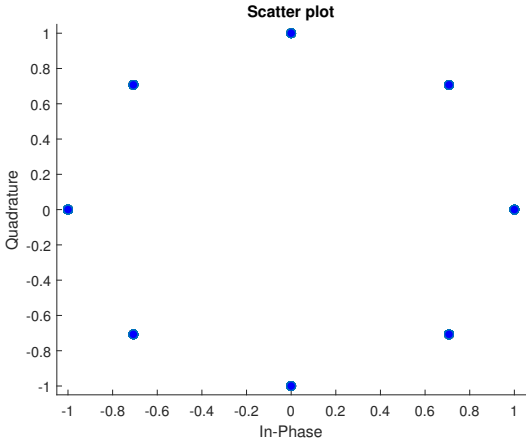
$$\mathrm{EVM}(\%) = \sqrt{\frac{\mathrm{A}^2_{\mathrm{error}}}{\mathrm{A}^2_{\mathrm{reference}}}} \times 100\% \tag{5.1}$$

Így adódik két lehetőség az átvitel vizsgálatára: a konstellációs diagram grafikus elemzése, amiből a jel-zaj viszonyra következtethetünk, továbbá a hibavektor átlagos hossza (EVM), amiből tulajdonképpen szintén az SNR változásáról vonhatunk le számszerű következtetéseket, ami előnyös, ugyanis a fő cél a kimeneti jel-zaj viszony csökkentése.

A félkész modell tesztelése során korán felmerült, hogy azok a leíró metrikák, amik a jelből vett mintákkal dolgoznak, nem biztosítanak teljes rálátást a valódi működésre, bi-



(a) QAM jellegű 8 állapotú moduláció



(b) 8PSK moduláció

5.1. ábra. Teszteléshez használt modulációk konstellációs diagramja

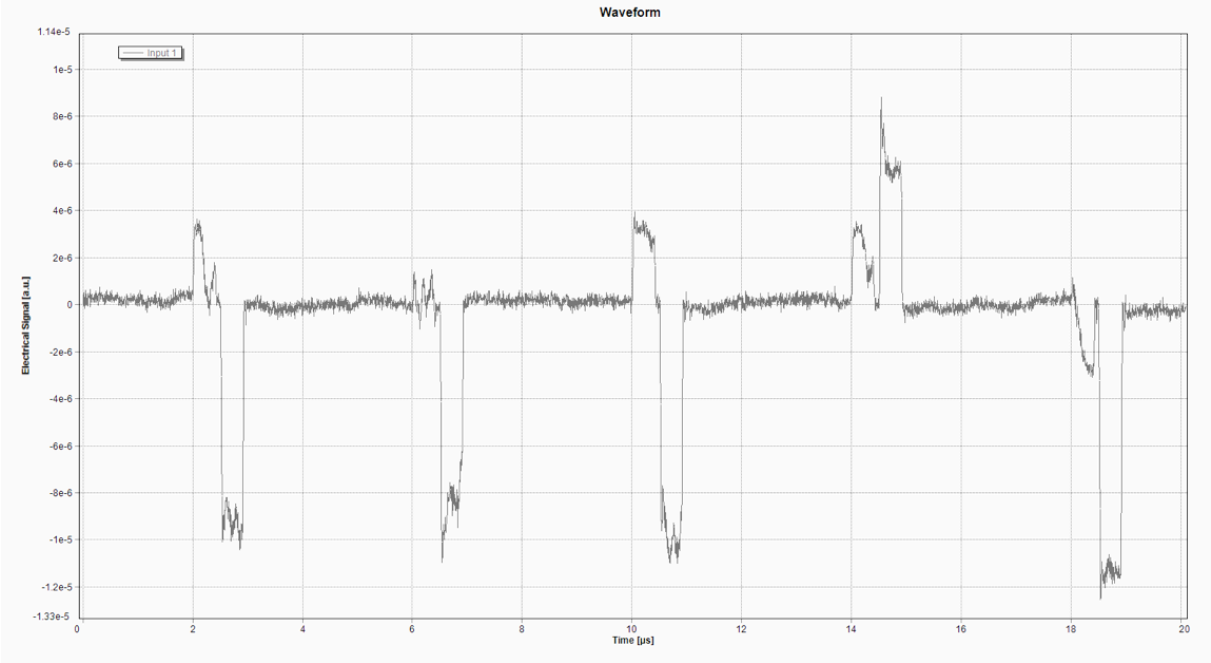
zonyos hibaforrásokra. Feltétlenül szükséges tehát a kimeneti hullámformák megfigyelése is. A későbbiekben látható lesz, hogy ezek elemzése lesz a kulcs egyes bonyolult, az átvitelt rontó jelenségek felismeréséhez, majd magyarázatához. Továbbá annak az egyszerű megállapításnak a megtételéhez is elegendő lesz, hogy az átvitel "teljesen elromlott" egy adott módosítás hatására. Ezért nincs értelme minden esetben konstellációt vagy egyéb számszerű leírókat vizsgálni.

Az eredmények ismertetése előtt célszerű tisztázni, hogy mit tekintek ideális kimenetnek. Az átvitel akkor tekinthető jónak, ha a kimeneten az impulzusok leginkább négyszögjelhez hasonlóan jelennek meg a küldéstől számított 500 ns késéssel (az üvegszálon terjedéshez szükséges időt nem véve figyelembe), egymástól 4 μs távolságra, a lehető legkisebb zajjal. A zajt egy adott ponton túl már nem tudjuk tovább csökkenteni az elektromos eszközök miatt. Ha a hasznos jelútba iktatott csillapítást növeljük, a vevő oldalon mérhető impulzusok amplitúdója csökken, ezért az impulzusok platójának relatív zajossága is növekedni fog, ezért rögzített értékű (20 dB-es) csillapítást használok.

6. fejezet

Főbb minőségrontó mechanizmusok

A 6.1 ábrán az első szimulációs eredmény látható: a fent leírt paramétereket betáplálva futtattam körülbelül 1000 véletlenszerűen generált szimbólum (8QAM) küldését, majd kirajzoltam az I (*In-phase*) vetület időbeli lefutásából az első 5 szimbólumnyi időt.



6.1. ábra. Első szimulációs eredmény

A 6.1 ábrán 5 darab impulzusnyi időt nagyítottam ki, így jól megfigyelhető a kimeneti hullámforma jellege. Látható, hogy az ideálistól nagy mértékben eltér az eredmény. További szimulációkkal végül 3 lényeges mechanizmust identifikáltam, ami jelentős hatással van a kimenetre:

1. Korábban már utaltam a teljesítmény kérdésére. Minél nagyobb teljesítménnyel van lehetőségünk dolgozni, annál nagyobb amplitúdójú impulzusokra számíthatunk, azaz a rendszer saját zajától annál jobban elkülönülnek a hasznos impulzusok. Jelen

esetben a detektorra jutó teljesítmény adott, komolyabb befolyásolására nincs lehetőségünk a rendelkezésre álló eszközök miatt (a lézer teljesítménye, az osztók osztásaránya, az optikai szál hossza adottnak tekinthetőek). Ezért ebben a tekintetben nincs különösebb mozgásterünk, de az nyilvánvaló, hogy kisebb beiktatási csillapítással üzemelő eszközök, nagyobb lézer teljesítmény, vagy rövidebb összeköttetés némileg javítanák a minőséget. A kérdés trivialitásából fakadóan ezzel a továbbiakban nem kívánok foglalkozni.

2. Ugyan a hasznos és referencia jeleket időben és polarizációban is igyekszünk szétválasztani, ennek ellenére a nem ideális eszközműködésből adódóan a továbbiakban is lesz némi egymásra hatás. Eredmény az impulzusok zajossága lesz, ami a 6.1 hullámformán is megjelenik, mégpedig az impulzusok négyszögjeltől való eltérése formájában. Ennek csökkentésére szintén teszek javaslatot és bemutatom, hogy pontosan melyik eszközparaméterek javításával lehetne a legnagyobb mértékű javulást elérni. A 6.1 szekcióban ennek kérdésével foglalkozok.

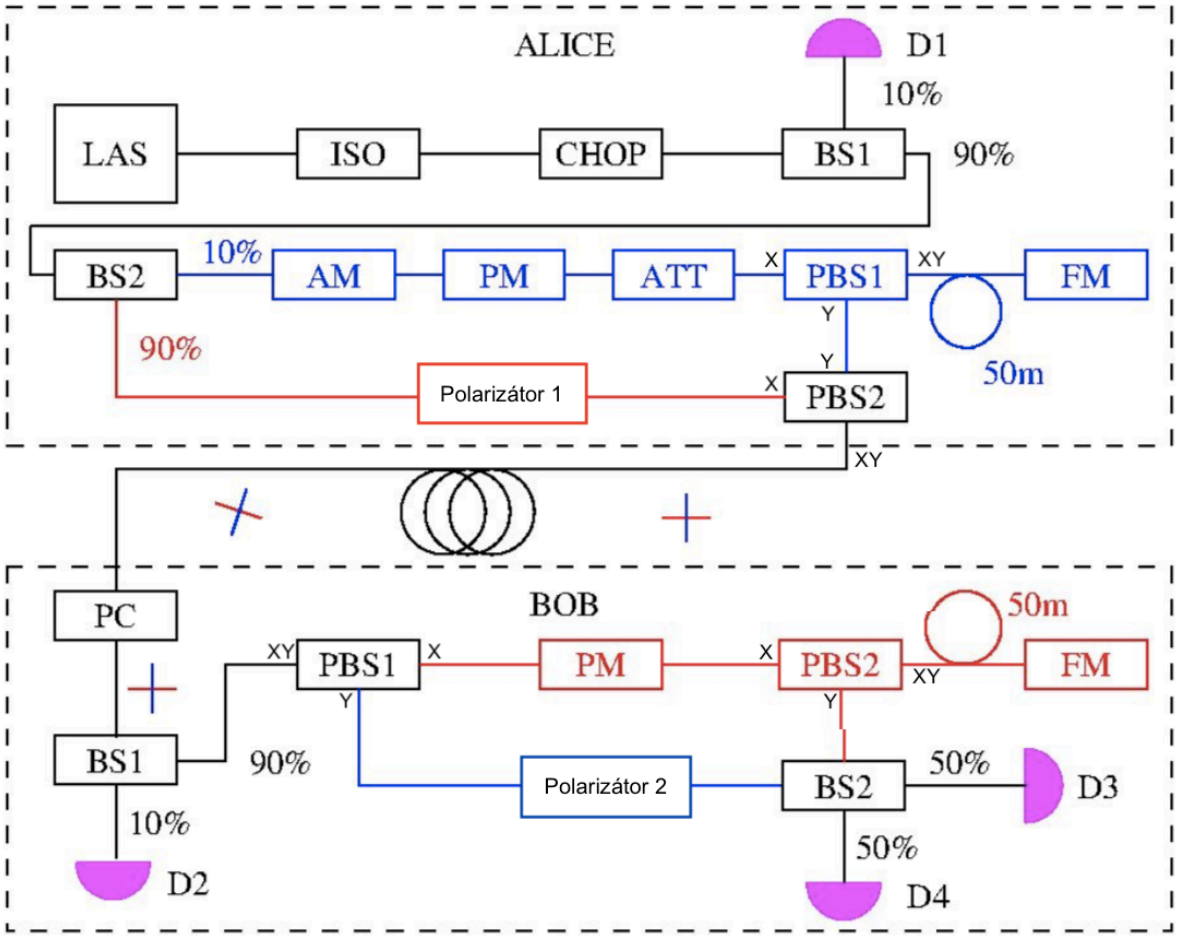
3. A mellékelt első hullámformán (6.1) is látszik, hogy egymás után szorosan két impulzus jelenik meg minden szimbólumidőben, azaz a küldött impulzusok valamilyen oknál fogva "duplázódnak". Ha az időbeli lefolyást jobban megvizsgáljuk, észre vehetjük, hogy minden esetben az páros első impulzusa lesz a nem kívánt hatás, a második pedig a hasznos impulzus. Előbbieket hívhatjuk "előimpulzusoknak" is. Előfordulhat, hogy hatásukra a vevő dióda telítődhet, vagy hibás jelzést adhat, valamint a polarizáció kontroller szabályozása szempontjából is okozhatnak gondot, így nem kívánatos jelenségnek számítanak. A 6.2 szekcióban leírom kialakulási mechanizmusukat és az általam talált védekezési lehetőségeket.

6.1. Hasznos és referencia jel áthallása

Az időben és polarizációban való elválasztás elméletben teljesen szeparálja terjedés során a hasznos és referencia impulzusokat. Valójában viszont az eszközök nem tökéletesen polarizáció tartó működése és áthallása miatt ez nem valósulhat meg tökéletesen. Az eredmény az lesz, hogy jelen struktúrában az időbeli elválasztással, és a polarizációs működéssel is lesznek problémák. Ezekkel azért fontos foglalkozni, mert a referencia és hasznos jelek között több nagyságrendnyi teljesítménykülönbségre számíthatunk. A nem tökéletesen polarizációtartó működésű eszközök miatt (például már a lézer miatt is, aminek keresztpolarizációs elnyomása nem végtelen) a fény polarizációjának tartása már az adó és vevőn belül sem valósulhat meg. Polarizáció szabályzóval kizárólag a hozzáférési hálózaton való terjedés forgató hatását vagyunk képesek kompenzálni, ezért alapos tervezési megfontolásokkal semlegesítenünk kell az adó és vevő eszközeinek nem kívánt működését.
Az adó oldalán (6.2 ábra) a legnagyobb problémát az okozza, hogy a BS2-re érkező fény

esetében már közel sem beszélhetünk lineáris polarizációról. Ezért BS2-n, mikor a referencia és hasznos jelút szétválasztásra kerül, mindkét ágra jut a két ortogonális polarizációs módusból. A hasznos ágon eredetileg is kisebb a teljesítmény a 10%-os osztás miatt, ezen kívül még csillapítjuk is a jelet az ATT jelzésű eszközzel. Mikor az adó kimenetén a PBS2 jelzésű kombinálóra kerül, az Y irányban polarizált hasznos jelszint minimális lesz, ezért a referencia jelúton (ahol az Y polarizált fénynek nem szabadna megjelennie) Y módusban terjedő teljesítmény összemérhető lesz vele.
Mit tehetünk ennek elkerülése érdekében?

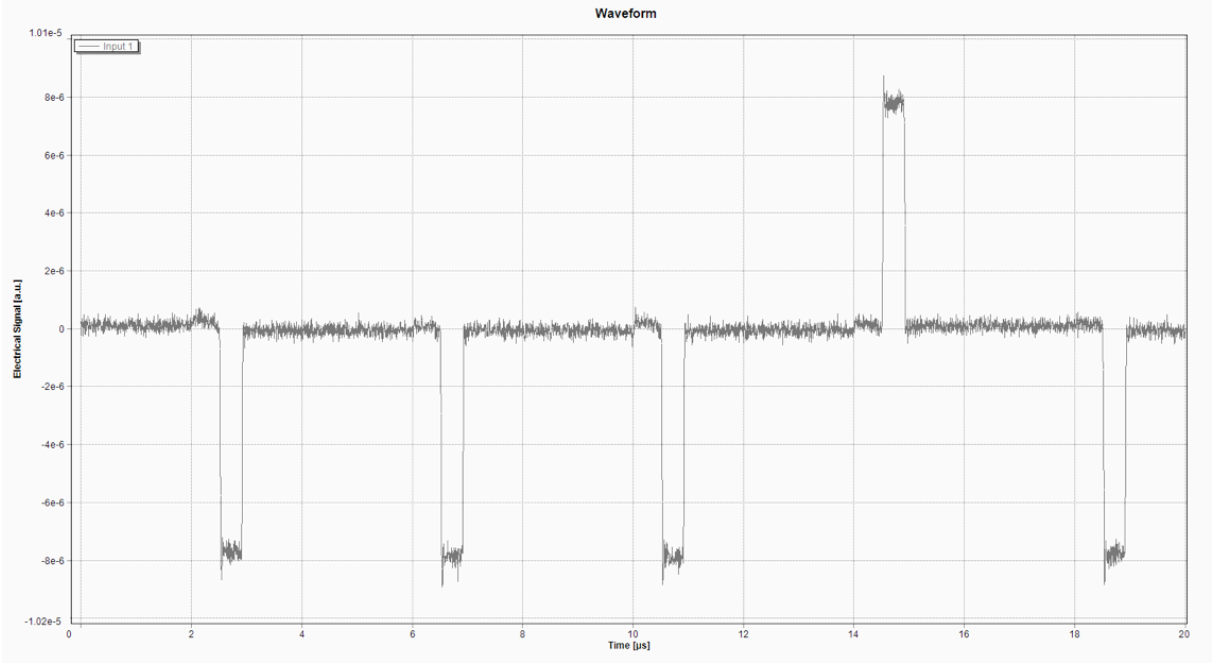
- Felmerülhet, hogy a lézer után polarizátort építsünk a rendszerbe, hogy az a leginkább lineárisan polarizált fényt bocsásson ki, de ez nem bizonyul jó megoldásnak. Az Alice oldalán található, elméletben polarizáció tartó, de valójában nem teljesen így működő eszközök további forgatást fognak eszközölni, azaz az erőfeszítés feleslegessé válik, bár a polarizációs módusok közötti áthallás némileg csökkeni fog a BS2 osztón.



6.2. ábra. Rendszer blokkvázlata, a javasolt helyeken polarizátorral

- Az előbb említett polarizátort egy ideálisabb helyen is lehet használni az adó oldalon. Ez a hely a referencia jel útján, közvetlenül a kimeneti kombinálásra használt

PBS előtt van. Az említett hely a 6.2 ábrán megfigyelhető, a "Polarizátor 1" jelölésű eszközről/helyről van szó. Így még az üvegszálas terjedés előtt sikerül minimalizálni a nem kívánt polarizációs állapotban terjedő teljesítmény káros hatást és komoly mértékben semlegesíteni a nem tökéletesen PM eszközök nemideális működését. A 6.3 ábrán az említett változtatás eredménye látható. A szimulációban a Thorlabs oldalán talált, 1550 nm-en használható polarizátorral dolgoztam, aminek elnyomása 28 dB. A 6.2 ábrán látható "Polarizátor 2" eszköz itt még nem szerepel a szimulációban, jelentősége a későbbiekben lesz.



6.3. ábra. Polarizátor beépítésének hatása a referencia ágon

Jól megfigyelhető, hogy az amplitúdók nagyságrandileg nem változtak, az előimpulzusok továbbra is jelen vannak, de egy relatíve kis bonyolultságú és olcsó eszköz beépítésével nagy mértékű javulás érhető el. Az impulzusok jellege jóval hasonlóbb a négyszögjelhez, a platókon megjelenő zaj itt már termikus zajhoz hasonlatos, ezért arra következtethetünk, hogy ténylegesen az áthallást redukáltuk.

- A polarizáló működést kevésbé explicit módon is produkálhatjuk. Azonos hatás figyelhető meg, ha az Alice oldalán a hasznos és referencia jelek kombinálására használt kimeneti PBS kioltási tényezője nagyobb, azaz nagyobb mértékben csillapítja az X portra került Y polarizációjú jelet, mielőtt az a közös (XY) portra kerül, mint most (20 dB, táblázatból látszik). Véleményem szerint ez a megoldás alapvetően nem ad akkora mozgásteret, mint a polarizátor, ugyanis 28 dB-vel nagyobb elnyomás nem érhető el. Ezért ez a valóságban önmagában nem lehet életképes, de kiegészítésként használható lehet.

- Ahogy közvetlenül a lézer kimenetén használt polarizátor, úgy az adó oldalon referencia ágba kerülő polarizátor sem javítja az átvitel minőségét a további szimulációk tanulsága szerint. Ezeket figyelembe véve kimondható, hogy szignifikáns minőségbeli javulást érhetünk el, ha csökkentjük az adó oldali referencia ágban, nem kívánt módusban terjedő fény teljesítményét. Ennek legegyszerűbb módja egy polarizátor beépítése a fent javasolt helyre, de egy tökéletesebben működő PBS-ek használata is segíteni tud.

6.2. Előimpulzusok

Az említett nem kívánt impulzusok a hasznos impulzusok előtt jelennek meg pontosan 500 ns-mal, amplitúdójuk pedig nem elhanyagolható. A hasznos impulzusokhoz viszonyított 500 ns-os sietés feltételezni engedi, hogy az impulzusok oka a cirkulátorként használt PBS-ek áthallása az X és Y (lassú és gyors tengely mentén polarizált) portok között, azaz a jel egy része kikerüli az 500 ns-ot okozó késleltető vonalat és a detektorra jut. A homodin elvű vevő berendezés miatt szükség van rá, hogy mindkét jelútról kerüljön jel a detektorra, valamint, hogy a jelek azonos polarizációs állapotban érkezzenek; máskülönben nem detektálnánk az előimpulzusokat.
A jelenség oka első megközelítésben az lehetne, hogy a vevő oldalon a hasznos jel egy része (60 dB-lel lejjeb) kikerüli a késleltető vonalat és Faraday-tükröt, majd az üvegszálon terjedés után a vevőre jut az eredeti (legyen X) polarizációs állapotban. A referencia jel teljesítményosztás után azonnal az üvegszálra jut, majd a vevő oldalon egy része kikerüli a késleltető vonalat és a hasznos jel előbb említett kis részével egy időben a detektorra jut. Ezen feltevés szerint az előimpulzusok azonos módon alakulnak ki, mint hasznos impulzusok, mindkét jelágban a késleltető és polarizációforgató struktúra kikerülésével, a "cirkulátor" áthallása miatt. Ebben az esetben azt kellene látnunk, hogy a hasznos impulzusok előtt 500 ns-mal az impulzusok kisebb amplitúdójú másolata jelenik meg. A szimulációs eredmények viszont nem ezt igazolják. Az előimpulzusok közel azonos amplitúdójúak és azonos polaritásúak, ráadásul számottevő mértékben kizárólag az egyik kvadartúrában jelennek meg (azaz a vevő oldali fázismodulátor kikapcsolt állapota esetén, ami az *In-phase* kvadratúrát jelenti). További szimulációkkal ellenőriztem, hogy Alice oldalán a cirkulátorként használt PBS X és Y portok közötti áthallása nincs befolyással az előimpulzusokra. Ebből arra következtettem, hogy az adó oldali folyamatok és eszközparaméterek minimális mértékben befolyásolják a jelenséget. Az eredeti feltevés ezért nem lehet helyes.

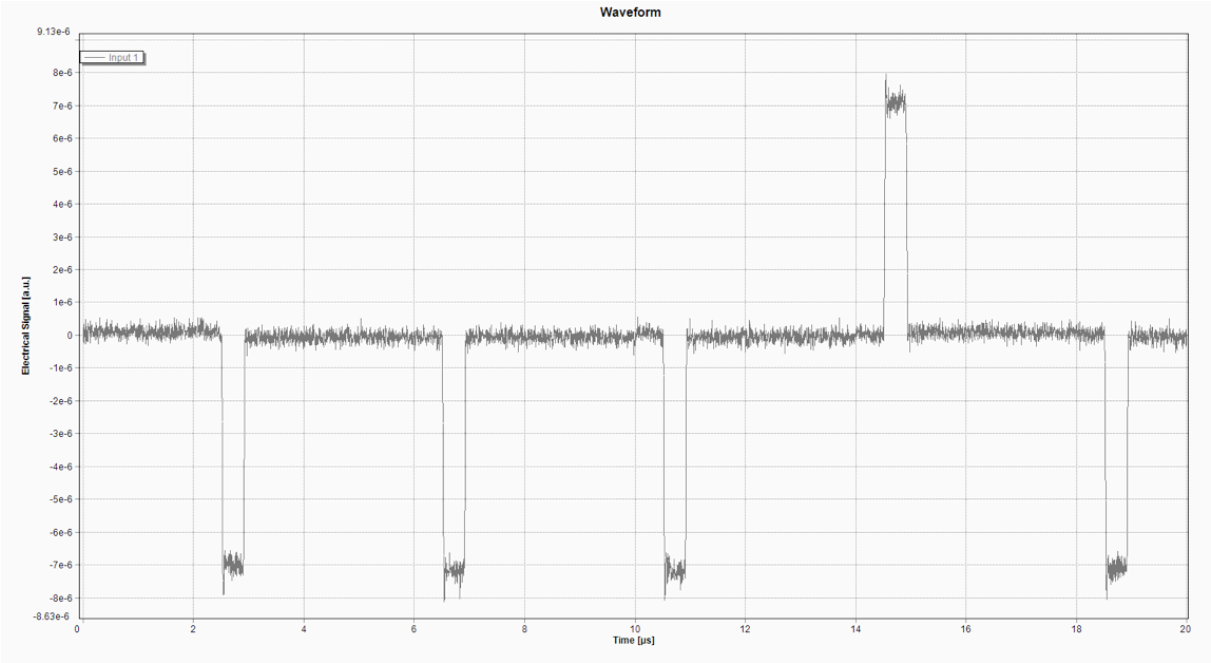
A vizsgálatok eredményeiből kiindulva arra következtetek, hogy a jelenség valódi oka a referencia jel, azaz a referencia jel önmagával való találkozása mindkét jelúton a vevő detektorában. Az általam feltételezett hatásmechanizmus a következő: A referencia jel

relatíve nagy teljesítménnyel jut az adó kimenetére késleltetés nélkül (teljesítményének jelentősebb része X polarizációban), majd a vevő oldalon a szétosztást végző PBS-re jut. Ideális működés esetén teljesítményének X irányban polarizált része teljes egészében az X portja kerülne, de valójában egy 20 dB-lel kisebb X irányban polarizált jel kerül az Y portra is, azaz egyből a hasznos jel útjára, ahol a detektorra jut 500 ns-mal a hasznos impulzus előtt. Teljesítményének egy része továbbra is a neki kijelölt jelúton halad, ahol a késleltető vonalat és Faraday-tükröt tartalmazó struktúrára kerül. A PBS X és Y portok közötti áthallása viszont azt okozza, hogy a jel egy része (szimulációnkban 60 dB-lel lejjebb) kikerüli az említett Faraday-tükrös struktúrát és azonnal a detektort éri el. Itt az előbb említett, hasznos jelútra jutott referencia jellel találkozik, így jönnek létre az ábrán is látható impulzusok. Az elmélet egyik bizonyítéka, hogy az impulzusokat nem befolyásolja az Alice oldali cirkulátorként használt PBS áthallása, a Bob oldali viszont igen, továbbá a vevő bemenetén található PBS kioltási tényezőjének (azon tulajdonsága, hogy milyen jól szeparálja szét a két polarizációs irányt) javítása csökkenti a nem kívánt előimpulzusok amplitúdóját.
Ehhez kapcsolódó javaslatok:

- Bob oldalán cirkulátorként használt PBS X és Y portok közötti áthallását minimalizálva az előimpulzusok csökkenthetők, mert így azon a jelúton jóval kisebb teljesítményhányad tud a detektorra jutni a 500 ns-mal a hasznos jel érkezése előtt.

- A vevő oldali PBS kioltási tényezőjét javítva szintén azonos eredmény érhető el. Megjegyezném, hogy ha a két eszköz közül már egyik tökéletesen ideális működést produkálna az említett szempontokból, az előmipulzusok megszűnnének.

- Ha a már meglevő eszközökön nincs lehetőség módosításokat eszközölni, polarizátor beépítésével is megoldható a probléma. A probléma fő oka a hasznos jel útjára (azaz Y polaritású portra; a hasznos jel a vevőben már Y irányban polarizált) jutó X irányban polarizált referencia jel. Ha ennek a referencia jelnek a szintje tovább csökkenthető egy megfelelő működésű polarizátorral (ami az X irányt szűri), nagy mértékben javítható a működés. A polarizátor beépítésének helye a 6.2 ábrán figyelhető meg, a "Polarizátor 2" jelű eszközről/helyről van szó, hatása a 6.4 ábrán látható ("Polarizátor 1" is szerepelt a szimulációban, tehát két polarizátor együttes beépítésének eredménye látható a 6.4 ábrán): Az eredmény egyértelmű javulás. A hasznos impulzusok amplitudója nem változott, de az előimpulzus jelentősen csökkent.



6.4. ábra. Polarizátor beépítésének hatása a hasznos ágon

6.3. Architektúra megváltoztatása

A 3.5 ábrán látható rendszeren lehetséges nagyobb változásokat is eszközölni, mint polarizátorok beépítése. A lehetőség, amit szimulációkkal vizsgáltam a késleltető/Faraday-tükrös/polarizációforgató struktúra áthelyezése, hogy Alice oldalán a referencia ágba legyen beiktatva, Bob oldalán pedig a hasznos jelútba, azaz az eredetihez képest fordítva. A megoldás legfőbb előnye, hogy az előimpulzusok megszűnnek, vagy elhanyagolhatóan kis szintre redukálódnak, ugyanis sem a referencia jelnek, sem a hasznos jelnek nem juthat jelentős hányada a detektorra a késleltetés előtt, mivel a siető impulzusok túl alacsony szintre csökkennek. Eddig nem tapasztalt hátrányok is megjelennek, elsősorban a hasznos és referencia jelek szeparáltsága fog csökkeni. 2 fontosabb mechanizmust sikerült identifikálni, amik együtt okozzák az átvitel degradálódását:

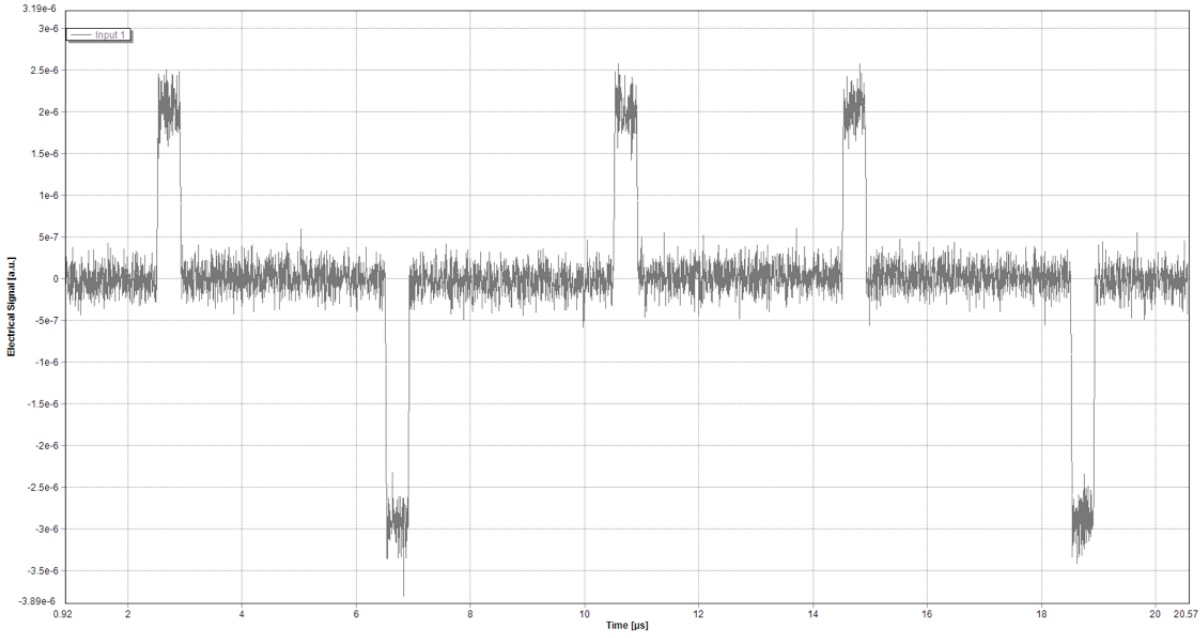
1. Adó oldali PBS áthallása nem elhanyagolható, ezért az áthallott X polarizációjú referencia jel együtt fog terjedni a hasznos jellel, teljesítményben pedig összemérhetők lesznek. Ez hibát fog okozni. Az áthallott referencia és hasznos jel kölcsönhatásának mértékét az Alice oldali cirkulátorként használt PBS sturktúra áthallása és az Alice oldali szál bemeneti PBS kioltási tényezője határozza meg.

2. Ezen kívül gondot okoz a Bob oldali mindkét PBS nem ideális működése. Alice oldalán a referencia ágon késleltetett impulzus Y polarizációs állapotba kerül és a szálon terjed. A szálon a referencia ezen állapota nem kerül interakcióba a hasznos jellel, ugyanis időben is, polarizációban is el van választva (természetesen a referencia jel egy másik része interakcióba kerül, ennek mechanizmusát az előző pontban írtam

le). A vevő oldalon szétválasztó PBS következik, ami nem ideális (ha ideális, ezen mechanizmus nem játszódik le), így jut Y polarizált jel is az X portra, amelyik porton aztán a hasznos jel késleltetése fog következni. Az említett, már késleltetett, Y irányú referencia impulzus egy része átjut a Bob cirkulátorként használt PBS-én (az áthallásnak megfelelően) és a detektorra a most már késleltetett hasznos jellel azonos időben, azonos polarizációs állapotban, azzal összemérhető teljesítménnyel fog érkezni.

A fent bemutatott két mechanizmus szempontjából a rendszer összes (4 darab) PBS-e lényeges. Ha áthallásukat és kioltási tényezőjüket javítjuk, vagy idealizáljuk, a hasznos és referencia jelek egymásra hatása csökken/megszűnik, így jobb minőségű átvitel érhető el. Szimulációim eredményeit értékelve azt tapasztaltam, hogy ugyan az előimpulzusok egyáltalán nem jelennek meg, de hasznos impulzusok rendkívül zajosak, értékelhetetlenek. Eredményes működésről tehát nehezen lehet beszélni abban az esetben ha az eredeti eszközök állnak rendelkezésre a korábban ismertetett paraméterekkel.
Két darab polarizátorral való kiegészítés ebben az esetben is megoldotta a problémát, ugyanazokon a helyeken, mint azt az eredeti rendszer esetében is bemutattam, de most mindkét polarizátornak az ellentétes állapotot/tengelyt kell majd szűrnie. A késleltető struktúra áthelyezése, és polarizátorok beépítése a 6.5 ábrán látható eredményt adja.

A megváltoztatott struktúrát összehasonlítva az eredetivel kimondható, hogy az eszkö-



6.5. ábra. Kimeneti hullámforma megváltoztatott architektúra mellett

zölt módosítás nem elvetendő. A módosított struktúra egyik hátránya a nagyobb zavaró hatás a hasznos és referencia jelek között, előnye pedig az előimpulzusok megszűnése. Két polarizátor alkalmazásával azonos mértékű zajosodást, közel azonos amplitúdójú impulzusokat figyelhetünk meg, de az eredeti struktúra esetén továbbra is megjelennek kis

méretű előimpulzusok, a módosított struktúra viszont kiküszöböli ezeket.
Egy rendkívül lényeges ok miatt ez a struktúra mégsem lesz bevethető a valós CVQKD rendszerben. A biztonság alapját az az elv képezi, hogy a hálózaton való terjedés során a hasznos impulzusok alacsony energiája miatt kvantumfizikai hatásokkal kell számolni. Ha jel késleltetését a vevő oldalon akarjuk elvégezni, akkor ahhoz, hogy azonos vételi teljesítményt kapjunk, nagyobb teljesítménnyel kell továbbítani a hozzáférési hálózaton, ugyanis a késleltető/polarizációforgató struktúrának nem elhanyagolható csillapítása lesz. Ha viszont növeljük az adási teljesítményt (ehhez nem szükséges a lézert lecserélni, elég a csillapítást csökkenteni az adóban), a terjedő jelnek klasszikus fizikai jelenségekkel való leírhatóságának határán fogunk mozogni. Ennek nyilvánvaló hatása, hogy az elvben titkos kommunikációt biztosító rendszerünk értelmét veszi, nem lesz alkalmas eredeti rendeltetésének betöltésére, a titkosság megszűnik.

7. fejezet

Részletes szimulációs eredmények

A fejezetben részletesen megvizsgálom, hogy néhány korábban listázott eszköz lecserélése kereskedelmi fogalomban kapható, jobb minőségű építőelemekre milyen változásokat hoz a rendszerben. Az új eszközök típusa és a modellezés szempontjából lényeges paramétereik a 7.1 táblázatban láthatók.

A szimuláció paraméterezését fokozatosan változtatom meg, mindig csak egy darab

PN1550R1A1 (Alice BS2)	Osztásarány	1 / 99 %
	Beiktatási csillapítás	10.5 / 1 dB
	Polarizációs kioltási tényező (PER)	22 / 27.5 dB
PN1550R2A1 (BS1)	Osztásarány	10 / 90 %
	Beiktatási csillapítás	1 / 10.5 dB
	Polarizációs kioltási tényező (PER)	22 / 27.5 dB
PN1550R5A2 (Bob BS2)	Osztásarány	50 / 50 %
	Beiktatási csillapítás	3.4 / 3.4 dB
	Polarizációs kioltási tényező (PER)	20 / 20 dB
AFW Technologies PBS/C (PBS)	Beiktatási csillapítás (IL)	0.6 dB
	Kioltási tényező	26 dB
ILP1550PM-ACP (polarizátor)	Beiktatási csillapítás (IL)	0.8 dB
	Kioltási tényező	28 dB

7.1. táblázat. Új eszközök listája

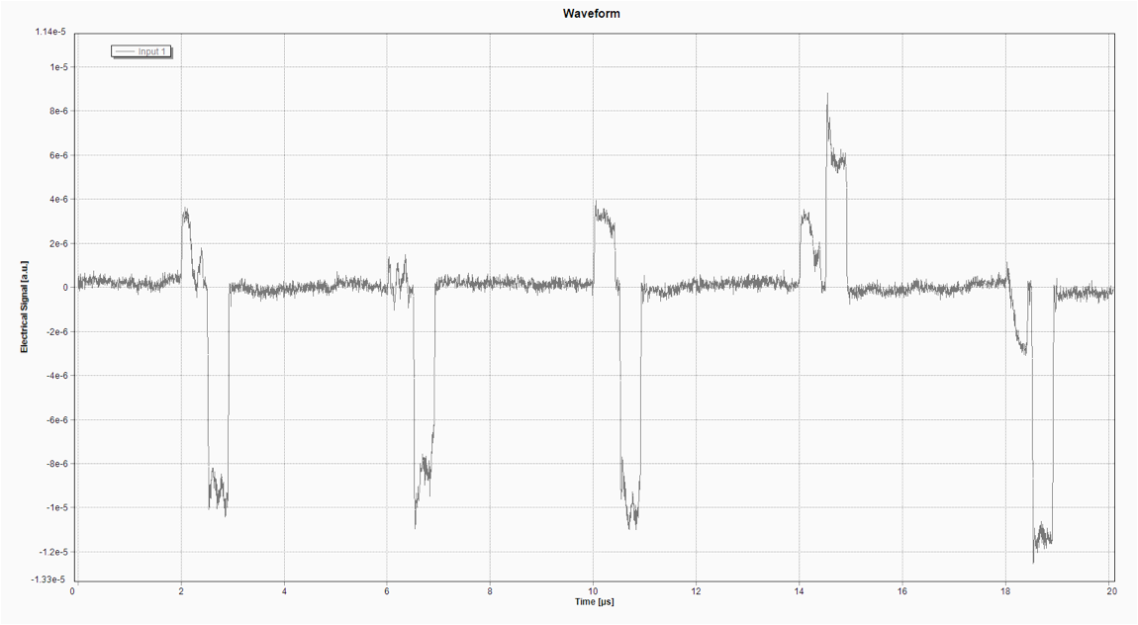
eszköz új paramétereit állítom be, hogy ilyen módon jól elkülöníthetők legyenek, hogy melyik változtatás pontosan milyen hatásért felelős. Az összehasonlítás könnyítése érdekében a moduláló jel minden esetben azonos. A tapasztalható jelenségek magyarázata során többször vissza fogok utalni az előző fejezetre, amiben nagy részletességgel írtam le azokat a mechanizmusokat, amikkel számolni kell a minőség szempontjából. Valójában ezen mechanizmusok feltérképezése párhuzamosan zajlott a továbbiakban ismertetésre

kerülő szimulációkkal, de az érthetőség szempontjából fontosnak tartottam előbbre venni őket a tárgyalásban.

7.1. Eszközcserék hatása a kimenetre

1. szimuláció

Paraméterek:
Eredeti PBS 20 dB elnyomással (polarizációs állapotok szétválasztási képessége), 90/10% osztásarány a referencia/hasznos nyalábosztón, mindenhol az eredeti osztók (első táblázat paraméterei szerint), polarizátorok beépítése nélkül.



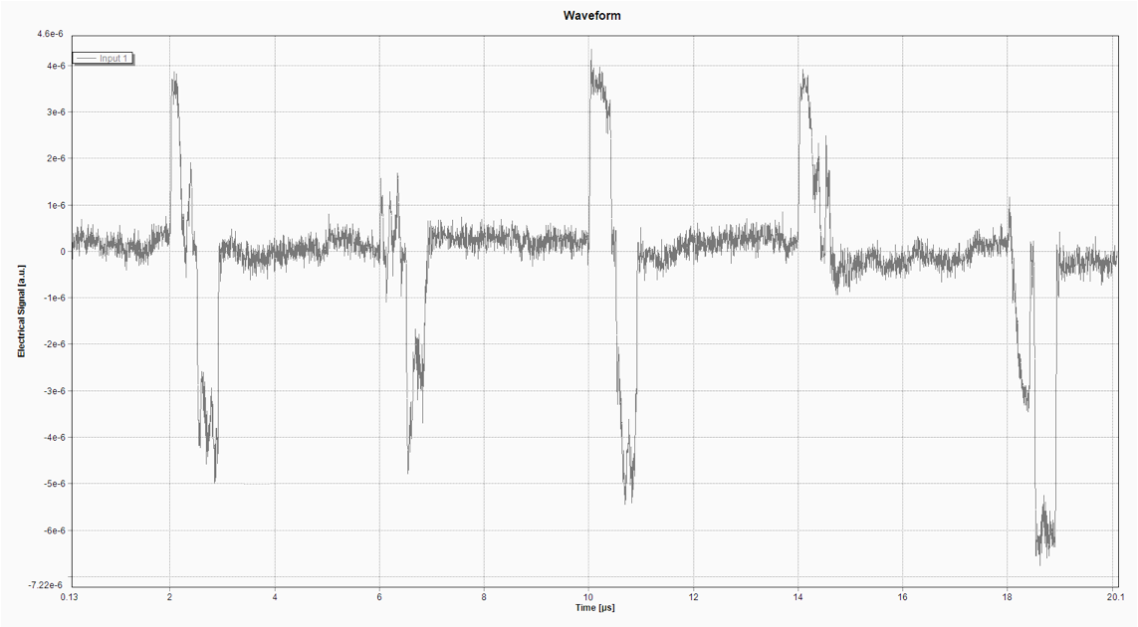
7.1. ábra. 1. szimulációhoz tartozó kimenet

A hálózati modell itt még megegyezik az előző fejezetekben részletesen bemutatott modellel. Ebből kifolyólag a továbbiakban csak azokat a eszköz paramétereket és szimulációs elrendezésre vonatkozó jellemzőket tüntetem fel, amiket változtatok. Az ezután következő szimulációkban egy-egy paramétert változtatok, majd értékelem a változtatás hatását. A módosítást vastagon szedve jelzem.

2. szimuláció

20 dB PBS elnyomás, 20 dB áthallás a PBS kimeneti és bemeneti portjai között, **99/1% osztásarány a referencia/hasznos nyalábosztón**, polarizátorok beépítése nélkül.

A változtatás eredménye, hogy a referencia-hasznos teljesítményviszony elmozdul, a referencia szintje nagyobb lesz, a hasznos jelé kisebb. Ebből kifolyólag az előimpulzusok



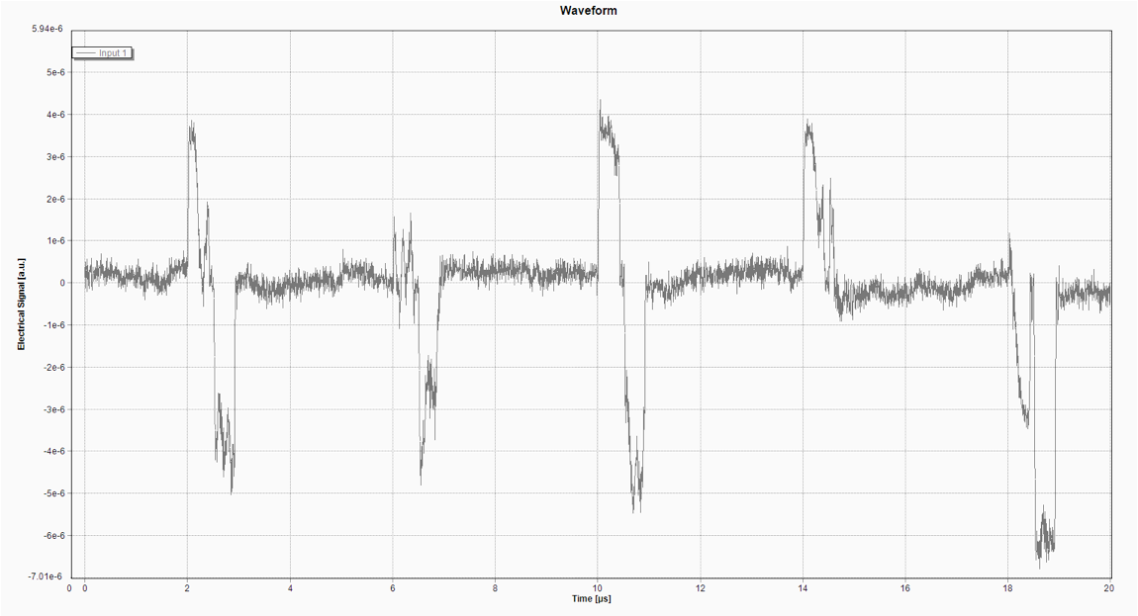
7.2. ábra. 2. szimulációhoz tartozó kimenet

amplitúdója megnő, a hasznos impulzusoké csökken, az ábrán pedig jól látható, hogy emiatt nagyjából azonos mértékűek lesznek az előimpulzusokkal. A hasznos jel amplitúdójának csökkenése önmagában nem káros jelenség, ugyanis ehhez tudatosan is hozzájárulunk egy csillapítóval, hogy így érjünk el kvantumfizikai működést. Ezért az osztó lecserélése 10 / 90 %-ról 1 / 99 %-ra annyit fog jelenteni, hogy elegendő lesz kisebb csillapítást beállítani. Sokkal inkább gondot okoz, hogy a nem kívánt előimpulzusok nagy amplitúdójúak maradnak.

3. szimuláció

28 dB elnyomás Alice oldalán a cirkulátorként késleltetésre használt PBS-en, összes többin marad az eredeti 20 dB, 99/1% osztásarány a referencia/hasznos nyalábosztón, polarizátorok beépítése nélkül.

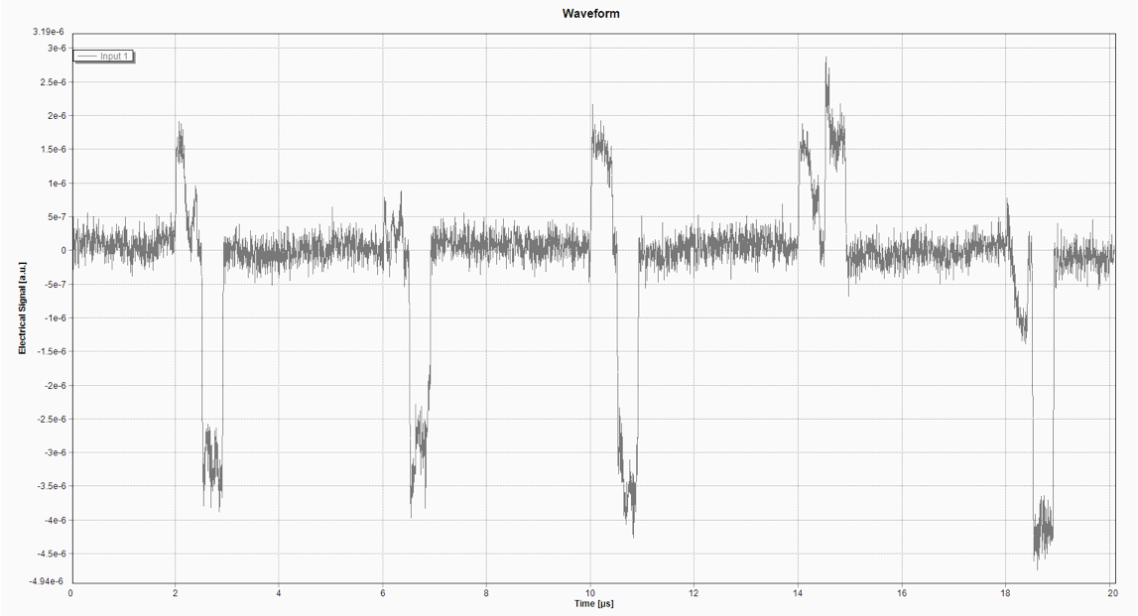
Alice oldalán a cirkulátorként használt PBS elnyomását növelve egy polarizáló hatást viszünk a hasznos jelútba az adó oldalon, azaz kb. 20 dB-lel csökkentjük a referencia jelúton nem kívánatos polarizációs módus szintjét (mivel a jel kétszer halad át rajta, összesen kétszer 8dB polarizáló hatást nyerünk). A kis teljesítmények miatt a hatás nem lesz jelentős, ugyanis a hasznos jelből polarizációs állapotából a referencia jel állapotába átcsatolódó teljesítmény eredetileg is alacsony volt. Összefoglalva: lényeges javulást ezzel nem érünk el.



7.3. ábra. 3. szimulációhoz tartozó kimenet

4. szimuláció

28 dB elnyomás Alice oldalán az összes PBS-en (azaz mindkettő lecserélve), Bob oldalán 20 dB, 99/1% osztásarány a referencia/hasznos nyalábosztón, polarizátorok beépítése nélkül.



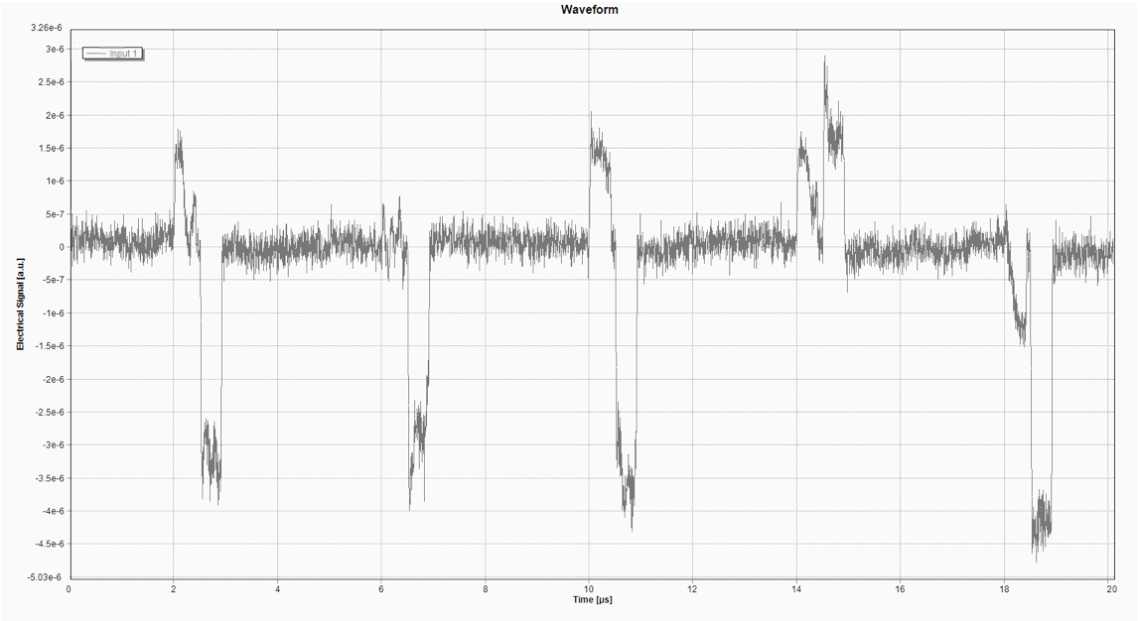
7.4. ábra. 4. szimulációhoz tartozó kimenet

A kimeneti PBS elnyomásának az előző változtatáshoz hasonló hatása van. A hatás azzal egyenértékű, mintha a hasznos és referencia jelútba is kb. 10 dB-es polarizátort építenénk a kimeneti kombinálás előtt. Előnyösnek mondható, mert annak ellenére, hogy a teljesítmények csökkennek, az előimpulzusok relatív amplitúdója is csökken a hasznos

impulzushoz képest, valamint a hasznos impulzusok platójának zajossága is mérséklődik. Az előnyös hatás oka a referencia jel nagyobb mértékű polarizáltsága. Ezen az úton mérhető nagyobb teljesítmények miatt kisebb mértékű átcsatolódás is jelentős interferenciát okoz a hasznos és referencia jelek között, a változtatással ezt mérsékeltük. Tehát ebben az esetben azért érzékelünk változást, mert a lényegesen nagyobb teljesítményű referencia jelet polarizáltuk.

5. szimuláció

28 dB elnyomás Alice oldalán az összes PBS-en és Bob bementi PBS-én, Bob cirkulátorként használt PBS-e továbbra is 20 dB elnyomással működik, 99/1% osztásarány a referencia/hasznos nyalábosztón, polarizátorok beépítése nélkül.

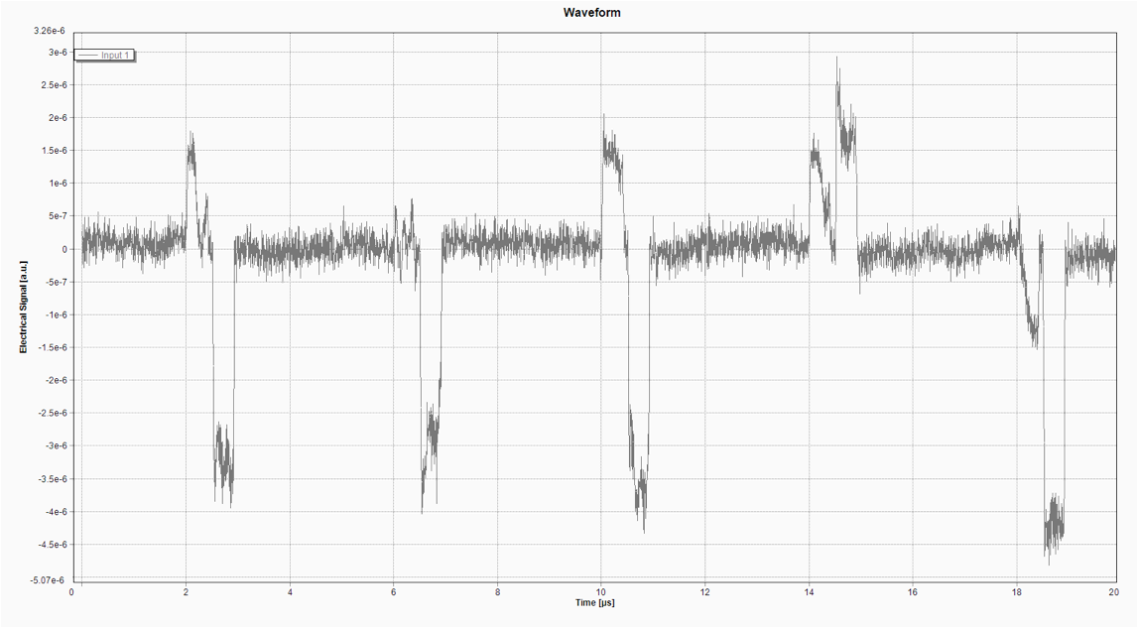


7.5. ábra. 5. szimulációhoz tartozó kimenet

A Bob oldali PBS-ek elnyomásának növelése a nagy energiájú referencia impulzusok miatt megjelenő előimpuzlusok amplitúdóját csökkenti azáltal, hogy redukálja a vevőben az egyes jelutakon terjedő nem kívánt polarizációs módusok hatását. Azaz a cserék hatása előnyös, de nem szignifikáns.

6. szimuláció

28 dB elnyomás az összes (4 darab) PBS-en, 40 dB áthallás a PBS kimeneti és bemeneti portjai között, 99/1% osztásarány a referencia/hasznos nyalábosztón, polarizátorok beépítése nélkül.

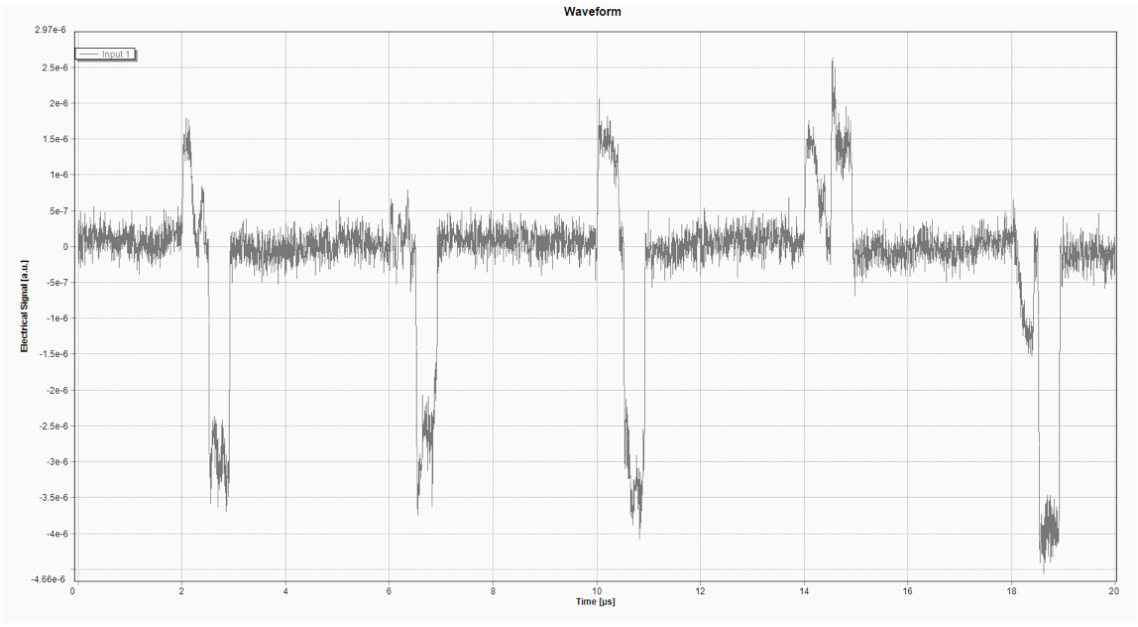


7.6. ábra. 6. szimulációhoz tartozó kimenet

Az itt tapasztalható változások azonos irányúak, és mértékűek az előző szimuláció (5. szimuláció) során tapasztaltakkal.

7. szimuláció

28 dB elnyomás az összes (4 darab) PBS-en, 99/1% osztásarány a referencia/hasznos nyalábosztón, **Alice kimenetén a hasznos ágban polarizátorral**, monitorpontok nélkül.



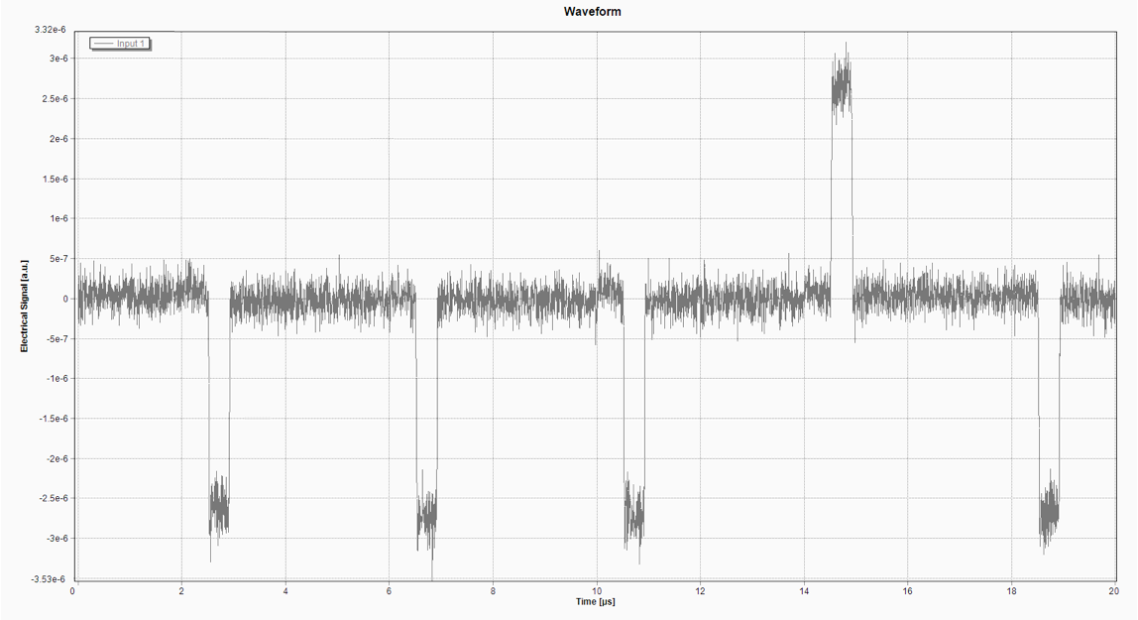
7.7. ábra. 7. szimulációhoz tartozó kimenet

A kimeneti kombinálás előtt a hasznos ágban elvégzett polarizálás nincs lényeges ha-

tással az átvitelre.

8. szimuláció

28 dB elnyomás az összes (4 darab) PBS-en, 99/1% osztásarány a referencia/hasznos nyalábosztón, **Alice kimenetén a referencia ágban polarizátorral**.

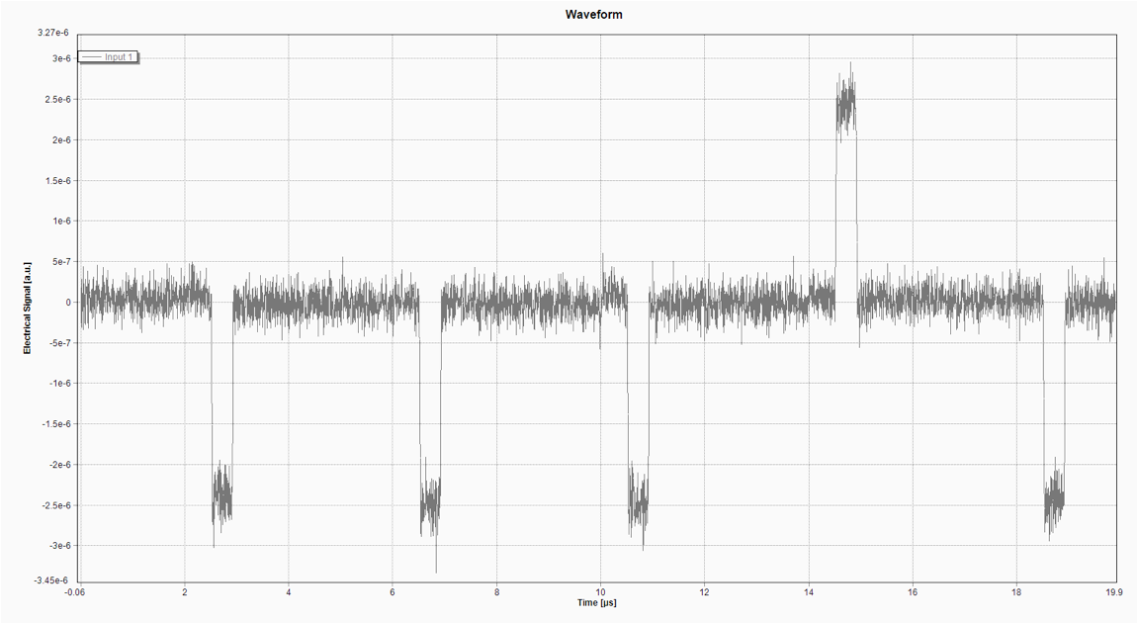


7.8. ábra. 8. szimulációhoz tartozó kimenet

A kimeneti kombinálás előtt a referencia ágban elvégzett polarizálás jelentős hatással lesz a kimeneti minőségre. Az amplitúdók csökkentek, de az impulzusok formája közeledett a várthoz (négyszögjel), zajosságuk csökkent. Kimondható, hogy az egyik leginkább előnyös szóbajöhető módosítás a polarizátor jelölt helyre való beiktatása. A jelenség okát a 6. fejezetben részletesen leírtam.

9. szimuláció

28 dB elnyomás az összes (4 darab) PBS-en, 99/1% osztásarány a referencia/hasznos nyalábosztón, **Alice kimenetén a referencia ágban polarizátorral, Bob bemenetén a referencia ágban polarizátorral**.

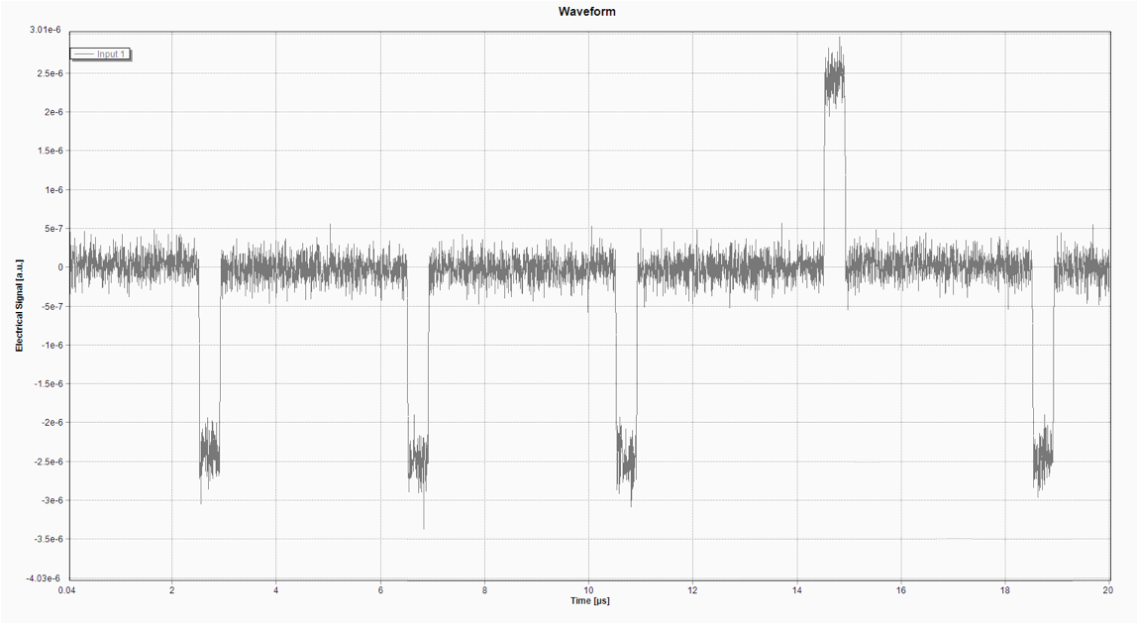


7.9. ábra. 9. szimulációhoz tartozó kimenet

Vevő oldalon a referencia ág polarizálása nem javítja nagy mértékben az átvitel minőségét. Az amplitúdók kis mértékben csökkentek, de egyéb változást nem figyelhetünk meg.

10. szimuláció

28 dB elnyomás az összes (4 darab) PBS-en, 40 dB áthallás a PBS kimeneti és bemeneti portjai között, 99/1% osztásarány a referencia/hasznos nyalábosztón, **Alice kimenetén a referencia ágban polarizátorral, Bob bemenetén a hasznos ágban polarizátorral**, monitorpontok nélkül. Vevő oldalon a hasznos jelút polarizálása tovább csökkenti az előimpulzusok amplitúdóját, azáltal, hogy mérsékeli a hasznos jelútra jutó X irányban polarizált hasznos jelet. Ezt a jelenséget is részleteztem a 6 fejezetben.



7.10. ábra. 10. szimulációhoz tartozó kimenet

7.2. Hibavektor vizsgálat

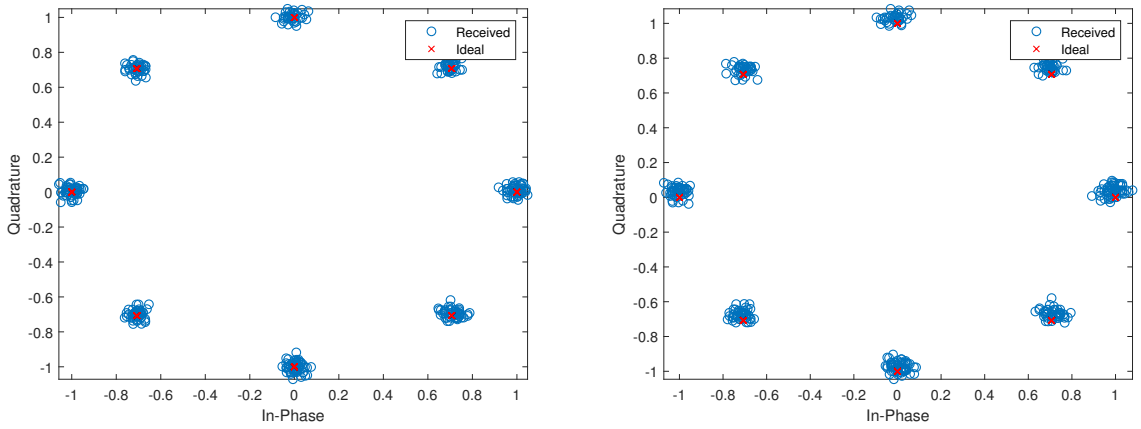
Alapvetően azt mondhatjuk, hogy az összes új eszköz beiktatása javítja az átvitelt, de ennek kimondása során legalább annyira támaszkodtunk elvi megfontolásokra, mint az ábrákra és az azokon látható változásokra. A probléma alapja az, hogy a hullámformák nem adnak lehetőséget egy kellően explicit, számszerű analízisre. Abból a szempontból elengedhetetlenek, hogy az előimpulzusok amplitúdójának változását jól meg tudjuk figyelni, de a hasznos impulzusokról mégis előnyös lenne többet mondani az eszközparaméterek változásának függvényében. Az igazán szemmel látható változást a polarizátorok megfelelő helyekre való beiktatása okozza. Ennek hatására válnak az impulzusok "értékelhetővé" és ezután nyílik meg a lehetőség a hibavektor vizsgálatra - polarizátorok nélkül a nagy áthalás, és az emiatt elfajult impulzusalak ezt nem tette lehetővé.

Ebből kifolyólag a következő módszert fogom használni: a teljes, 12. szimulációban bemutatott rendszert veszem alapul, azaz azt a verziót, amiben az összes új eszköz szerepel, két darab beépített polarizátorral, a 6.2 ábrán látható helyeken. Majd megváltoztatom néhány eszköz paraméterét, végső soron az új eszközöket régiekre cserélem, ezután számítom a hibavektort, és ezt vetem össze a kiindulási, ideális esettel.

A 7.2 táblázat alapján látszik, hogy az egyes építőelemek kevésbé ideálisra cserélése valóban minden esetben ront az átviteli minőségen, de egyik esetben sem drasztikus mértékben. Ha viszont a különbségeket összeadjuk (az utolsó kivételével), már számottevő romlással számolhatunk. Azaz az újabb eszközök lényegesen redukálják a rendszer zajosságát, csökkentik az áthallást, és a referencia jel hasznos jelet zavaró hatását - bár

Változtatás	EVM (%)	Különbség (%)
Eredeti paraméterek	3.465422	0
Teljesítményosztó PER: 28 dB ⇒ 20 dB	3.742135	0.276713
Alice PBS1 ER: 28 dB ⇒ 20 dB	3.7659	0.300478
Alice PBS2 ER: 28 dB ⇒ 20 dB	4.36075	0.895328
Bob PBS2 ER: 28 dB ⇒ 20 dB	3.75242	0.286998
Bob PBS1 ER: 28 dB ⇒ 20 dB	3.75413	0.288708
Alice BS2: 1/99 ⇒ 10/90	1.30	-2.165422

7.2. táblázat. Eszközcserék hatása a hibavektorra



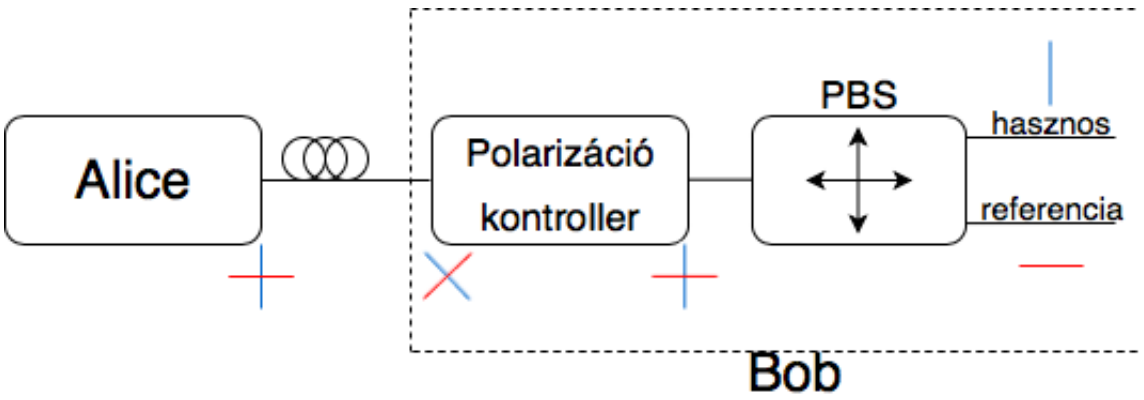
(a) Eredeti pararméterbeállítás (b) Legnagyobb eltérést mutató paraméterezés

7.11. ábra. Vételi konstellációs diagramok

továbbra is igaz, hogy egy polarizátor megfelelő használata felülmúlja az új eszközök együttes hatását. A táblázat utolsó bejegyzése az adó oldali nyalábosztó 99:1-es osztásának 90:10-esre változtatásáról szól. Ez annyiban különbözik a többi módosítástól, hogy a rendszer teljesítményviszonyaiban eszközöl változtatást. Ha a hasznos jel szintjét növeljük - jelen esetben a teljes teljesítmény 1 %-áról 10 %-ra -, értelemszerűen javítunk a jel-zaj viszonyon és ezzel egyidejűleg a vételi minőségen. Hasonló hatást érnénk el azzal, ha a lézer teljesítményét növelnénk. Éppen emiatt ez nem egy életszerű javító lehetőség: a valós rendszerben a hasznos impulzusok energiájának/amplitúdójának csökkentésén kell dolgozni (ezért próbáljuk eliminálni az egyéb interferencia és zajforrásokat), így ehhez hasonló "trükköket" nem engedhetünk meg magunknak.

7.3. Polarizáció szabályozás

A polarizáció szabályozás kérdésköre rendkívül fontos a helyes működés szempontjából. A blokkvázlaton PC jelölésű, vevő bemenetén helyet foglaló kontroller végzi a hozzáférési hálózaton való terjedés közben bekövetkezett polarizációs elfordulást. Hibás működés esetén a Bob oldalán PBS1 jelölésű polarizációs osztó nem lesz képes szétválasztani a hasznos és referencia jelet, tolerálhatatlan mértékű áthallás jelentkezik, az átvitel pedig teljesen elromlik. A valódi rendszerben a General Photonics POS - 002 típusú szabályója került beépítésre. A szabályozási algoritmus részletes megismerése nem tartozott a célkitűzések közé, de annyit érdemes tudni róla, hogy egy referencia pont teljesítményét maximalizálja azáltal, hogy a bemenetére kerülő optikai jel polarizációját módosítja. Azaz a kontroller helye fix (a vevő bemenetén foglal helyet), de a referenciapontot szabadon megváltoztathatjuk. A szimulációs környezet korlátai miatt dinamikus működést nem volt lehetőségem vizsgálni, de 2 lényeges aspektusból végeztem vizsgálatokat: megfigyeltem a szabályozási hiba hatását, valamint a referenciapont megválasztásával is foglalkoztam.

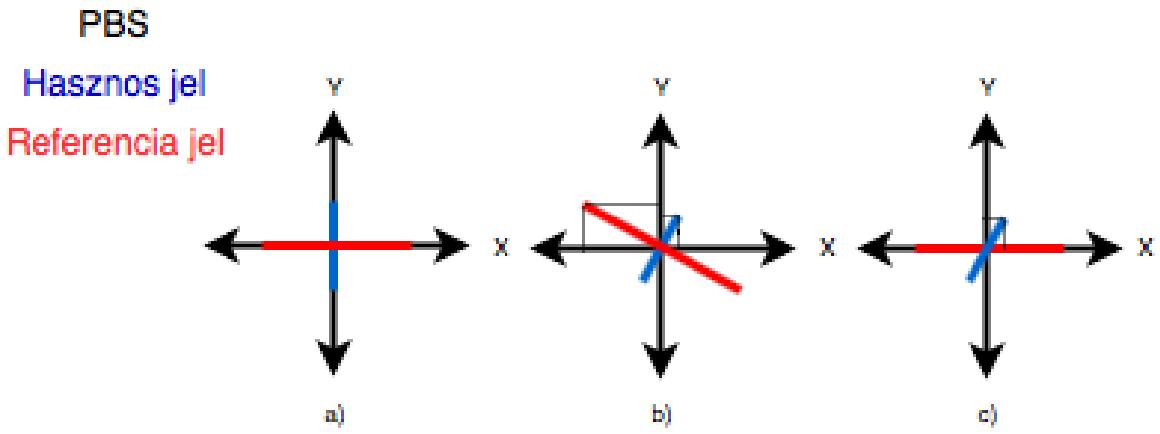


7.12. ábra. Polarizáció kontoller elvi működése

7.3.1. Monitorpont megválasztása

A dolgozatomban leírt problémák legnagyobb részének oka a hasznos és referencia jel közötti áthallás volt, elsősorban polarizációs eszközök miatt. A polarizáció kontroller is ezt igyekszik minimalizálni, és a szabályozási referenciapontak is egy olyan helyet kell választani, aminek mérésével ezt a feltételt teljesíteni lehet. Szintén a korábbi megfontolások alapján tudjuk, hogy a hasznos jel áthallása a referencia jel polarizációs módusába okozza a legnagyobb hibát, elsősorban a teljesítménybeli eltérések miatt. Azaz a hatás ebben az értelemben nem nevezhető kölcsönösnek, a referencia jel megfelelő kezelése sokkal nagyobb jelentőségű.

A 7.13 ábrán sematikusan ábrázoltam, hogy a polarizációs osztó miként állítja elő kimeneti jeleit. Az a) ábra egy ideális esetet ábrázol, azaz hasznos és a referencia jel



7.13. ábra. PBS működési modell különböző bemenetek esetére

egymásra ortogonális polarizációs állapotban terjed, a vevő oldali szabályozás pedig tökéletesen működik, azaz a PBS tengelyeire 0 szöghibával érkeznek. Ebben az esetben az X kimeneten megjelenik a hasznos jel teljes egész és semmi más (tekintsünk el az eszköz kioltási tényezőjétől, ami az itt tárgyalt jelenségek leírásának szempontjából kevésbé lényeges), az Y kimeneten pedig a teljes hasznos jel és semmi más. Egy kevésbé ideális esetet ábrázol a 7.13 b) része, amin a két jel szintén egymásra merőleges módusban terjed, de a polarizáció helyreállítása a vevőben nem sikerült tökéletesen, azaz konstans szöghibával érkezik a PBS-re. Ebben az esetben az X kimeneten megjelenik a referencia jel egy jelentős része - a vetületeknek megfelelően -, valamint a hasznos jel egy bizonyos hányada: ez okozza a kisebb problémát. Az Y kimeneten szintén megjelenik a hasznos jel nagyobb része, de egy bizonyos mértékben referencia jel is: ez okozza a problémát, mert a referencia jel teljesítmény nagyságrendekkel nagyobb, mint a hasznos jelé.
Értelemszerű, hogy melyik az ideális helyzet, és hogy melyikre törekszünk; ez az a) állapot. Muszáj belátni viszont, hogy ez akkor sem következhet be, ha a kontroller ideálisan működik, ugyanis a valóságban a két jel nem tökéletesen ortogonális polarizációs módusban fog terjedni. Ennek oka, hogy a vevőben szétválasztjuk a két jelet, majd különböző számú és különböző típusú eszközt iktatunk a jelfolyamba. Ezek többnyire polarizációtartó működésűek, de ez tökéletesen nem valósul meg, azaz a kimeneti és bemeneti jel polarizációja nem lesz teljesen azonos. Ezért mikor a hasznos és referencia jelet összegezzük az adó kimenetén, már nem teljesen merőleges polarizációs módusban terjednek.
Az említett észrevételt kihasználhatjuk a szabályzási referenciapont megválasztásánál. A gondok forrása - ahogy azt többször már leírtam - a referencia jel hasznos jelre gyakorolt hatása. Ezt úgy tudjuk minimalizálni szabályozás segítségével, hogy a vételi oldali első PBS X kimenetét, azaz a referencia ágat igyekszünk teljesítményben maximalizálni, azaz a referenciapontot a kontroller utáni PBS X (referencia) kimenetére helyezzük. Azt az állapotot mutatja a 7.13 ábra c) része. A kontroller tökéletesen működik, azaz a biztosítja referencia ág maximális teljesítményét azáltal, hogy a referencia jelet ráhúzza a PBS X

tengelyére. A hasznos jel az ortogonalitás hiánya miatt nem az Y tengellyel párhuzamosan áll be, aminek némi teljesítményveszteség lesz az eredménye. Cserébe viszont elérjük fő célunkat, hogy az Y állapotban ne jelenjen meg a referencia jel, azaz ne hasson a hasznos jelre.
A fenti megfontolások alapján, maximális teljesítményre való szabályozást választva a referenciapont ideális helyének a vevő oldali PBS1 X (referencia) kimenetét jelöltem meg.

7.3.2. Szabályozási hiba

Az előzőekhez hasonló szimulációs megfontolásokkal megvizsgáltam a szabályozási hiba hatását, 0.001 fokos hibától, logaritmikus lépésekkel. Az eredmény - ahogy azt korábban leírtam -, az ortogonális polarizációs módusok közötti áthallást lesz. A polarizáció kontroller és a vételi oldali PBS1 jelű polarizációs osztó közötti szakasz rendkívüli fontosságú, mert ha ezen a szakaszon nem biztosított az áthallásmentesség (például egy nem tökéletesen polarizációtartó eszköz, vagy szabályozási hiba miatt), akkor a későbbiekben már nem lesz lehetőség ezt korrigálni.
A táblázatból jól látható, hogy 0.01 fok hibáig az EVM romlása nem szignifikáns, század százalékokról beszélhetünk. 0.1 foknál, és fölötte viszont tolerálhatatlan mértékű romlás tapasztalható, 1 foknál pedig már tulajdonképpen elromlott az átvitel. Decibelben kifejezve a 0.1 fok -55 dB környéki áthallást jelent abban az esetben, ha két jelet tökéletesen ortogonális polarizációs állapotban terjedőnek feltételezzük. Ez alacsonynak tűnhet, de a rendszer rendkívül érzékeny rá a hasznos és referencia jelek magas relatív teljesítménykülönbsége miatt 1 fok hiba pedig kb. -35 dB áthallást visz a rendszerbe a polarizációs módusok között.

Változtatás	**EVM (%)**	**Különbség (%)**
Eredeti paraméterek	3.465422	0
0.001 fok szabályozási hiba	3.465626	0.000204
0.01 fok szabályozási hiba	3.493022	0.0276
0.1 fok szabályozási hiba	4.962083	1.496661
1 fok szabályozási hiba	33.133976	29.668554

8. fejezet

Összefoglalás

Munkám során megismerkedtem a kvantumos alapú kulcsszétosztás elméletével, annak motivációival és főbb fajtáival. Részletesen tanulmányoztam egy folytonos változós (CVQKD) megvalósítás alapjául szolgáló optikai hálózati architektúrákat és az erről szóló szakirodalmat. VPI Transmission Maker szimulációs programban több lépésben felépítettem egy ilyen optikai hálózatot, az elemeket részét egy létező próbaösszeköttetéshez igazodva paramétereztem. Megválasztottam azokat a leírókat, amik segítségével értékelem a kapott kimenetet. Az elkészült modellt felhasználva rengeteg lehetőség nyílt az átvitel optimalizálásához. Szimulációk segítségével identifikáltam néhány lényeges jelenséget, amivel a működő rendszerben számolni kell, azonosítottam a rendszer néhány kritikus pontját. További részletes szimulációkkal megvizsgáltam, hogy a nagyobb jelentőségű eszközök ideálisabbra cserélése milyen hatással van a kimeneti minőségre. Érintőlegesen foglalkoztam a szabályozás kérdésével is. Megállapítottam, hogy a polarizációtartás mértéke az egyes ezközöknél kiemelt fontosságú, nem kielégítő működés nagy mértékben növeli a kimenet zajosságát. Elengedhetetlennek bizonyult továbbá a polarizációs osztók kellően nagy kioltási tényezője és kis mértékű áthallása. Rámutattam azokra az eszközökre, amik cseréje jobb minőségűekre komolyan hozzájárul az ideális működéshez. Rájöttem, hogy polarizátorok beiktatásával a nem kívánt hatások egy jelentős hányada kiküszöbölhető és megfelelő helyre való beépítésükkel a kevésbé jól működő eszközök cseréje is feleslegessé válhat. Megtaláltam azokat a helyeket, ahol a polarizátorok teljesítik ezt a követelményt. Összefoglalásként kimondható, hogy klasszikus fizikai/telekommunikációs megfontolásokkal széleskörűen megvizsgáltam a CVQKD kulcsszétosztó rendszer optikai hálózati alaprétegét. A hálózati modell bonyolultsága kis mértékben még növelhető lenne, de egy részletesebb kidolgozás várakozásaim szerint nem befolyásolná döntően az eredményeket. Úgy gondolom, hogy a lényegi, szem előtt tartandó tendenciákra sikeresen rámutattam, kevés további lehetőség nyílik a rendszernek ezen az alacsony, klasszikus fizikai szinten való tárgyalására. Ilyen módon megnyílik az út a magasabb szintű működés kidolgozásához.

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani Kis Zsoltnak, a Wigner Fizikai Kutatóközpont munkatársának, hogy szakmai iránymutatásával hozzájárult dolgozatom elkészítéséhez.

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] CSE 599d - Quantum Computing Shor's Algorithm;
David Bacon;

[2] Symmetric and asymmetric key cryptography;
http://ehindistudy.com/2015/10/01/symmetric-and-asymmetric-key-cryptography-in-hindi/
Letöltve: 2018. 05. 07.

[3] The Security of Practical Quantum Key Distribution;
Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lutkenhaus, Momtchil Peev;
September 30, 2009

[4] Continuous variable quantum cryptography using coherent states;
Frédéric Grosshans and Philippe Grangier;

[5] The SECOQC Quantum Key Distribution Network in Vienna;
Momtchil Peev, Andreas Poppe, Oliver Maurhart, Thomas Lorunser, Thomas Langer, Christoph Pacher;
2009 35th European Conference on Optical Communication

[6] Results from the SECOQC Quantum Key Distribution Network;
A. Poppe, T. Langer, T. Lorunser, O. Maurhart, C. Pacher, M. Peev;
CLEO/Europe - EQEC 2009 - European Conference on Lasers and Electro-Optics and the European Quantum Electronics Conference

[7] Improving the Maximum Transmission Distance of Continuous Variable Quantum Key Distribution by using a Noiseless Linear Amplifier;
Bingjie Xu and Bing Zeng;
2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS)

[8] Experimental demonstration of continuous-variable quantum key distribution over 80 km of standard telecom fiber;

P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti;
2013 Conference on Lasers and Electro-Optics Europe and International Quantum Electronics Conference CLEO EUROPE/IQEC

[9] WHAT IS COHERENT LIGHTWAVE COMMUNICATION SYSTEM?;
https://www.fiberoptics4sale.com/blogs/archive-posts/95043526-what-is-coherent-lightwave-communication-system
Letöltve: 2018. 10. 03.

[10] Self-coherent phase reference sharing for continuous-variable quantum key distribution;
Adrien Marie, Romain Alléaume;
August 31, 2016

[11] Polarizing Beamsplitter Cubes (PBSC);
https://www.artifex-engineering.com/index.php/en/optics-en/beamsplitters/polarizing-beamsplitter-cubes
Letöltve: 2018. 10. 09.

[12] Field test of a continuous-variable quantum key distribution prototype;
S Fossier, E Diamanti, T Debuisschert, A Villing, R Tualle-Brouri and P Grangier;
December 17, 2008

[13] Quantum Optics and Quantum Information with Continuous Variables;
Philippe Grangier;
Laboratoire Charles Fabry de l'Institut d'Optique, UMR 8501 du CNRS, 91127 Palaiseau, France

[14] Theoretical study of continuous-variable quantum key distribution;
Anthony Leverrier;
January 28, 2010