Eksperimentalna kvantna kriptografija

Špoljar, Sabina

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
FIZIČKI ODSJEK

Sabina Špoljar

EKSPERIMENTALNA KVANTNA KRIPTOGRAFIJA

Diplomski rad

Zagreb, 2024.

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
FIZIČKI ODSJEK

INTEGRIRANI PREDDIPLOMSKI I DIPLOMSKI SVEUČILIŠNI STUDIJ
FIZIKA; SMJER NASTAVNIČKI

Sabina Špoljar

Diplomski rad

Eksperimentalna kvantna kriptografija

Voditelj diplomskog rada: dr. sc. Mario Stipčević

Ocjena diplomskog rada: _____

Povjerenstvo: 1. _____

2. _____

3. _____

Datum polaganja: _____

Zagreb, 2024.

Dragi i poštovani Mario,
hvala Vam što ste pristali biti moj mentor i pružili mi priliku da s Vama surađujem. Dapače, pružili ste mi i više nego što je bilo potrebno. Također Vam hvala što ste u tom procesu bili ništa manje nego izvrstan mentor. Boljeg nisam mogla izabrati.

Dragi mama i tata,
hvala vam što ste mi omogućili da završim studij i što ste preživjeli uspone i padove zajedno sa mnom kroz ovaj period. Nije nam bilo lako, ali na kraju ste me uvijek podržali i pomogli mi na koji god način ste mogli i znali. Hvala vam na svim ručkovima, vožnjama na ispite, čekanjima, preživljavanju moje živčanosti prije ispita, strpljenju, veselju zbog mojeg uspjeha i svemu drugom. Ovaj rad posvećujem vama kao simbol završetka dosadašnjeg perioda školovanja kroz koji ste me pratili.

Zahvaljujem i svojoj obitelji (posebno Daji i Hermi) te svim prijateljima na podršci, savjetima i pomoći tokom svih ovih godina.

Na kraju još želim zahvaliti tebi, Dag, na svemu što si učinio, a i dalje činiš za mene.

Sažetak

Razvoj kvantnih računala predstavlja veliku opasnost za sigurnost komunikacije putem interneta, koja trenutno počiva na vremenski zahtjevnom probijanju algoritama za njenu uspostavu. Kada bi postojalo dovoljno jako kvantno računalo, spomenuti algoritmi bi se dokazano mogli probiti izvršavanjem tzv. Shorovog algoritma na navedenom računalu. Zbog tog velikog problema počelo se razmišljati o novim načinima ostvarivanja sigurne komunikacije te se Kvantna Distribucija Ključa pojavila kao jedno od mogućih rješenja. U ovom radu predstavljena je eksperimentalna kvantna distribucija ključa bazirana na BB84 protokolu te pripadajući fizikalni postav. U svrhu implementacije protokola korišteni su, između ostalog, izvori fotona valne duljine 810 nm, SPAD detektori i telekomunikacijsko G.652.D optičko vlakno. Korištenjem ovih komponenti pokazano je kako se telekomunikacijsko vlakno i SPAD detektori mogu uspješno koristiti za provedbu kvantne distribucije ključa na manjim udaljenostima, što otvara mogućnost uspostave jeftinije implementacije protokola u budućnosti. Protokol je uspješno proveden za gušenje do 8.3 dB, što odgovara duljini od 2.7 km optičkog vlakna.

Protokol i rezultati također su predstavljeni i u članku "*Near Infrared Devices and Protocols for Short Distance Quantum Key Distribution via Telecom Fibers*" na hibridnoj međunarodnoj konferenciji MIPRO te će isti biti dostupan u IEEE Xplore databazi.

Ključne riječi: kvantna distribucija ključa, kvantna kriptografija, BB84 protokol

Experimental quantum cryptography

Abstract

The development of quantum computers poses a significant threat to today's communication security, since it currently relies solely on the time-consuming process of breaking algorithms used for its establishment. However, in the advent of sufficiently powerful quantum computers, these algorithms could be effectively broken by executing the so-called Shor's algorithm on the forementioned computer, which would undermine communication security as a whole. Due to this major challenge, new approaches for achieving secure communication have begun to be considered. One potential solution is Quantum Key Distribution (QKD). Therefore, this paper presents an experimental quantum key distribution system based on the BB84 protocol and its corresponding physical setup. For protocol implementation, components such as 810 nm wavelength photon sources, single-photon avalanche diode (SPAD) detectors, and G.652.D telecommunication optical fiber were utilized. It is demonstrated how telecommunication fiber and SPAD detectors can be successfully employed for quantum key distribution over short distances, thus opening the possibility of a more cost-effective protocol implementation in the future. The protocol was successfully implemented for attenuation up to 8.3 dB, corresponding to the length of 2.7 km of optical fiber.

The protocol and results mentioned in this summary were also presented in an article titled "*Near Infrared Devices and Protocols for Short Distance Quantum Key Distribution via Telecom Fibers*" at MIPRO hybrid international convention and will be available in the IEEE Xplore database.

Keywords: quantum key distribution, quantum cryptography, BB84 protocol

Sadržaj

1 Uvod

Kvantna Distribucija Ključa (eng. *Quantum Key Distribution, QKD*) je protokol koji počiva na principima kvantne fizike i rezultira distribucijom tajnog ključa između dvije stranke koje žele komunicirati sigurno. Taj ključ se zatim koristi za simetričnu enkripciju daljnje komunikacije.

Današnji način distribucije ključa počiva na matematičkim algoritmima. Točnije, ključ se distribuira između dvije stranke pomoću niza matematičkih operacija, odnosno njihovim izračunom obje stranke dobivaju isti rezultat koji se koristi kao tajni ključ. Zbog prirode funkcija koje se koriste u tom procesu, zvane jednosmjerne funkcije, vrlo je teško saznati tajni ključ. Jedino kako se on može saznati je pogađanjem, ali ono zahtijeva jako puno vremena, toliko da se ovakav način distribucije ključa smatra posve sigurnim i danas izvrsno funkcionira. [1] [2]

Unatoč današnjoj sigurnosti koju pružaju, ovi algoritmi ugroženi su zbog sve većeg interesa razvijanja kvantnih računala. Pojavom dovoljno jakog kvantnog računala, ti algoritmi se mogu probiti u realnom vremenu izvršavanjem tzv. Shorovog algoritma na spomenutom računalu, što rezultira saznavanjem tajnih ključeva potrebnih za sigurnu komunikaciju. Zbog toga se počelo razmišljati o sigurnijem načinu razmjene ključeva pa se tako, kao jedno od mogućih rješenja, pojavila kvantna distribucija ključa. QKD se ne može probiti putem Shorovog algoritma jer ne počiva na matematičkim, već na fizikalnim principima, stoga je takvo probijanje samog protokola time eliminirano. Jedini drugi način koji ostaje za otkrivanje ključeva je prisluškivanje, no QKD rješava i taj problem, o čemu će biti riječi kasnije. [3]

Prvi QKD protokol predložili su 1984. godine Bennet i Brassard. Njihova implementacija naziva se BB84 protokol. Postav i protokol opisani u nastavku ovog rada počivaju upravo na toj implementaciji, stoga će fokus biti isključivo na njoj (postoje i drugi načini realizacije QKD).

2 Kvantna Distribucija Ključa

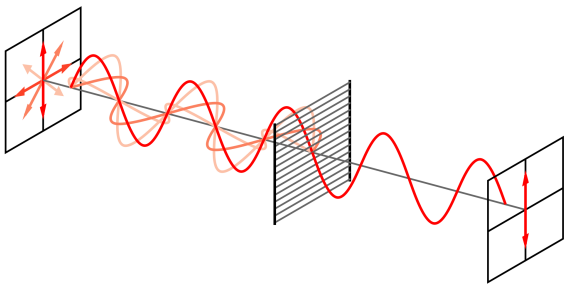
2.1 Fizikalni princip rada QKD protokola

Kao što je ranije spomenuto, QKD protokoli funkcioniraju na fizikalnim, a ne matematičkim principima. Temeljni principi na kojima počiva BB84 protokol su polarizacija te tzv. Heisenbergovo načelo neodređenosti.

2.1.1 Polarizacija

Prema klasičnoj fizici, svjetlost se opisuje kao elektromagnetski val. Elektromagnetske valove čine periodična titranja električnog i magnetskog polja, koja su uvijek okomita na smjer širenja vala, zbog čega ih još nazivamo i transverzalnim valovima. Zbog toga što su transverzalni, moguće ih je polarizirati.

Vidljiva svjetlost, koju primjerice emitira žarulja, nepolarizirana je, što znači da se sastoji od elektromagnetskih valova čija električna i magnetska polja titraju u različitim ravninama. Ako želimo od nepolarizirane svjetlosti dobiti svjetlost čija je ravnina titranja u nekom nama željenom smjeru, možemo koristiti polarizator. Polarizator je optički filter koji propušta elektromagnetsko zračenje u određenom smjeru. Zbog njegove građe (npr. građen od malih kristala), polarizator ima sposobnost apsorpcije titranja svjetlosti u nekim smjerovima (ravninama) te propuštanja titranja u drugima. Tako primjerice polarizator na slici 2.1 apsorbira sve smjerove titranja električnog polja osim vertikalnog, čime se dobiva svjetlost čija je ravnina titranja samo u vertikalnom smjeru. [4]



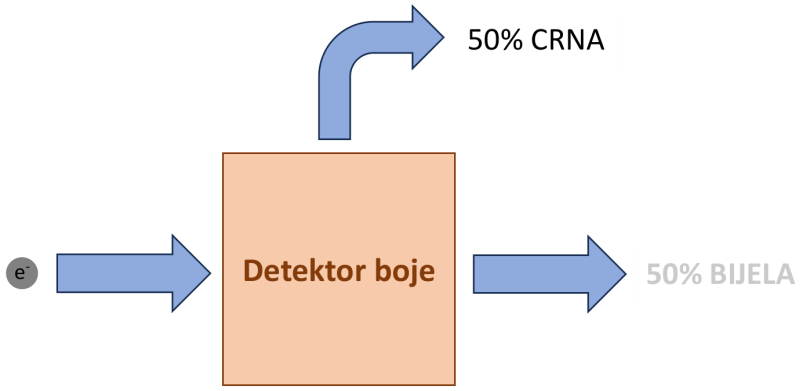
Slika 2.1: U ovom primjeru, polarizator propušta samo svjetlost čija je ravnina titranja električnog polja u vertikalnom smjeru. Izvor: [5]

Danas znamo da je ovakav opis nepotpun, odnosno da elektromagnetske valove također možemo opisati kao mnoštvo čestica koje nazivamo fotonima. Kada bismo intenzitet (broj fotona koji prolazi kroz neku površinu u jedinici vremena) nepolarizirane svjetlosti smanjili do te mjere da možemo promatrati individualne fotone te ako ih zatim usmjerimo u polarizator, uočili bismo da svaki individualni foton sadržava informaciju o polarizaciji. Iz toga zaključujemo da je polarizacija svojstvo fotona. Polarizacija može biti linearna ili cirkularna. [6]

2.1.2 Heisenbergovo načelo neodređenosti

BB84 protokol uz polarizaciju počiva na manifestaciji ovog načela. To načelo ukazuje na činjenicu da mjerenje jednog svojstva sustava nužno poremeti druga svojstva i to posve nasumično.

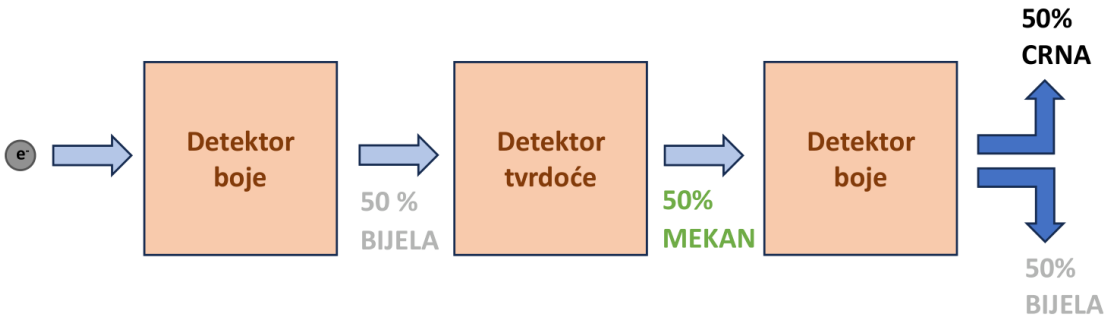
Kao primjer njegove manifestacije, mogu se zamisliti elektroni kojima se želi odrediti jedno njihovo svojstvo - za potrebe primjera korištena su izmišljena svojstva radi jednostavnosti, ali kod mjerenja stvarnih svojstava kao što bi bili primjerice pozicija elektrona ili njegova količina gibanja, uočavaju se isti rezultati kao u ovom zamišljenom primjeru. Dakle, za početak, želi se odrediti jedno svojstvo elektrona, recimo da je to boja, a postoje dva moguća rezultata, da je elektron crne ili bijele boje. Da bi se odredilo koje su boje elektroni, koristi se postav koji sadrži izvor elektrona i uređaj koji će odrediti koje je boje elektron te će bijele elektrone usmjeriti desno, a crne prema gore, kao što je prikazano na slici 2.2.



Slika 2.2: Prikaz postava za mjerenje jednog svojstva elektrona.

Ono što će se uočiti je da će boja elektrona u 50% mjerenja biti crna, a u 50% bijela. To je statistički gledano i očekivano. Ako se pak oni elektroni koji su bili bijeli usmjere u uređaj za određivanje boje elektrona, uočit će se da će svi elektroni na izlazu tog uređaja biti bijeli, što se također slaže sa našom intuicijom. Recimo da se zatim želi izmjeriti drugo svojstvo, a to je jesu li elektroni meki ili tvrdi. Postav bi sada umjesto uređaja za određivanje boje imao uređaj za određivanje tvrdoće elektrona, ali osim te razlike, sama opažanja bila bi u potpunosti ista - u 50% mjerenja elektroni bi bili meki, a u 50% mjerenja tvrdi (te bi primjerice meki elektroni ponovnim prolaskom kroz detektor tvrdoće u 100% slučajeva bili detektirani kao meki).

Zanimljivo opažanje javlja se kada bi se odredila prvo boja, zatim tvrdoća, a onda provjerila boja elektrona (može i prvo tvrdoća, zatim boja pa opet tvrdoća). Ovaj slučaj prikazan je na slici 2.3.



Slika 2.3: Određivanjem tvrdoće elektrona gubi se informacija o boji elektrona.

Ako se prvo mjerenjem određuje boja elektrona, poznato je da će 50% njih biti bijele boje. Ako se zatim ti bijeli elektroni usmjeravaju u uređaj za određivanje tvrdoće, poznato je i da će 50% bijelih elektrona biti meki. Nakon ovog koraka intuitivno bi se moglo zaključiti da su sada ti elektroni bijeli i meki te je očekivanje da će, kada se tim bijelim i mekim elektronima ponovno ide odrediti boja, 100% njih biti bijele boje. No, uočava se nešto neočekivano - ponovnim određivanjem boje elektrona, samo je 50% njih bijele boje, a 50% crne! Mjerenje tvrdoće elektrona kao da je poremetilo prethodno bijele elektrone. Ova pojava opaža se u mjerenju stvarnih svojstava elektrona i to bez obzira od čega je proizveden postav i uređaji za njihovu detekciju. Eksperiment je također ponovljen mnogo puta i opažanja su uvijek ista. Zaključak ovog

eksperimenta je da je nemoguće istovremeno, sa stopostotnom sigurnošću, znati više od jednog svojstva ne samo elektrona, već bilo koje čestice, dakle i fotona. [7]

Upravo se ovo načelo, koje je dio kvantne fizike, iskorištava u QKD protokolu kako bi se osigurala sigurna komunikacija između stranaka.

2.2 Opis protokola

Recimo da dvije osobe, Alice i Bob, žele uspostaviti tajni ključ kako bi mogli sigurno komunicirati. Protokol počinje tako da Alice uzme slučajni niz bitova i enkodira bitove kao jednu od 4 moguće polarizacije fotona, recimo da su to horizontalna (0°), vertikalna (90°), dijagonalna (45°), i anti-dijagonalna (135°). Bit 1 enkodira se kao horizontalna i dijagonalna polarizacija, a bit 0 kao vertikalna i anti-dijagonalna. Zatim te (polarizirane) fotone šalje Bobu putem posebnog kanala koji se naziva kvantnim kanalom (kanal preko kojeg se šalje isključivo takva vrsta prometa).[1] S druge strane, Bob, koji nema nikakve informacije o polarizaciji nadolazećih fotona, nasumično i za svaki foton zasebno odabire tzv. bazu u kojoj će te fotone detektirati. Postoje 2 baze, jedna koja precizno detektira fotone s horizontalnom ili vertikalnom polarizacijom, a druga one s dijagonalnom ili anti-dijagonalnom polarizacijom. [8]

S obzirom da Alice polarizira svaki foton u jednoj od četiri spomenute ravnine, ona im ustvari određuje svojstvo. Ukoliko se jednom od tih fotona, koji primjerice ima svojstvo da je polariziran u ravnini 0°, pokuša odrediti polarizacija sa pogrešnom bazom, odnosno onom koja nema sposobnost detekcije te ravnine, rezultat će biti posve nasumičan i izgubit će se, u potpunosti i nepovratno, informacija o tome u kojoj je ravnini foton polariziran prethodno tom mjerenju. [8]

Kada Bob odabere ispravnu bazu, odnosno onu koja pravilno detektira polarizaciju nadolazećeg fotona, imat će ispravnu detekciju i time ispravan bit. No, i oni fotoni čija polarizacija ne odgovara orijentaciji detektora svejedno mogu biti detektirani i stoga Bob ne zna koje je bitove primio ispravno. [8]

[1] Kanal se, u ovom slučaju, dijeli na klasičan i kvantni kanal - kod klasičnog kanala, kojeg čine npr. optička vlakna ili žice, informacije se razmijenjuju pomoću svjetlosti ili struje, dok se kod kvantnog kanala informacije razmijenjuju pomoću fotona, putem optičkih vlakana.

Alicein niz bitova	1	1	0	1	0	0	1	0
Alicin niz izabranih baza	V	D	D	V	V	D	D	V
Polarizacije koje je Alice poslala	↕	↘	↙	↕	↔	↙	↘	↔
Bobov niz izabranih baza	V	D	V	D	V	D	V	V
Bobove izmjerene polarizacije	↕	↘	↕	↙	↔	↙	↕	↔
Bobov niz bitova	1	1	1	0	0	1	1	0
Zadržani niz bitova nakon što Alice i Bob objave svoje baze	1	1	-	-	0	1	-	0

Tablica 2.1: Vizualni prikaz komunikacije između Alice i Boba putem kvantnog, a zatim klasičnog kanala. Vertikalna baza označena je slovom V (⊕), a slovom D dijagonalna (⊗).

Zbog toga Bob nakon detekcije putem klasičnog kanala šalje Alice baze koje je koristio za detekciju svakog fotona, a Alice mu odgovara je li baza koja je odabrana ispravna ili nije, u odnosu na poslani polarizirani foton. Važno je naglasiti da je ispravnost ili neispravnost baze jedino što Alice otkriva Bobu, ne i što je poslala - ako je Bob koristio dobru bazu trebao bi ispravno detektirati točno što mu je Alice poslala. Bob i Alice nakon ovog koraka zadržavaju samo ispravno detektirane bitove i time su razmijenili tajni ključ, ali u idealnom slučaju, u kojem ništa osim mjerenja polarizacije ne može poremetiti poslane fotone. U stvarnosti, Alice i Bob će sigurno nakon ovog dijela protokola imati neke razlike u ključu. One se javljaju zbog brojnih faktora poput šuma, smetnji, nesavršenosti opreme i sličnog. [8]

2.3 Prisluškivanje

Što ako je treća osoba, zvana Eve, prisluškivala kvantni kanal? Jedino kako to može je da sama detektira polarizacije fotona u tranzitu i to nasumično, jednako kao i Bob. No, zbog Heisenbergovog načela neodređenosti, Eve svakim svojim mjerenjem narušava stanje svakog fotona. Dakle, ona svojim detektiranjem, koje može biti ispravno ili neispravno ovisno o bazi koju odabere, nepovratno uništi dotadašnju polarizaciju fotona. Ona nikako ne može detektirati foton i ujedno ga proslijediti "netaknutog" Bobu. Zbog toga nakon detekcije, za koju ne zna je li ispravna ili nije, mora ponovno polarizirati fotone i poslati ih Bobu.

Bob i Alice svjesni su mogućnosti prisluškivanja i zato, nakon što su odbacili sve pogrešno detektirane bitove, odabiru nasumični niz bitova iz dobivenog ključa te ga

uspoređuju putem klasičnog kanala. Ako su pogreške između njihovih nizova (koje se javljaju zbog nesavršenosti opreme i sl.) unutar očekivane vrijednosti, koja se izražava u postotku, mogu zaključiti da nitko nije prisluškivao kvantni kanal. No, ako je Eve prisluškivala, Alice i Bob uočit će veći postotak pogreške od očekivanog i zbog toga znaju da je netko prisluškivao njihovu komunikaciju. U prijevodu, prisluškivanje će biti detektirano. [8]

2.4 Ispravljanje pogrešaka i pojačavanje privatnosti

Alice i Bob moraju imati potpuno isti ključ da bi ga mogli koristiti za enkripciju podataka. Zbog toga postoje još dvije faze protokola pomoću kojih se osigurava da je ključ identičan i siguran kod obje stranke, a nazivaju se faza ispravljanja pogrešaka i faza pojačavanja privatnosti.

U fazi ispravljanja pogrešaka, Alice i Bob ispravit će sve razlike između njihovih ključeva. Kroz ovaj dio protokola izmjenjuju informacije putem klasičnog kanala i Eve može prisluškivati njihovu komunikaciju čitavo vrijeme. Zbog toga će, nakon usklađivanja ključa, konačno izabrati njegov manji dio, za koji znaju da je gotovo posve siguran.

U fazi pojačavanja privatnosti, ključ se dodatno procesuira kako bi se uklonile sve potencijalne korelacije ili informacije koje bi mogle kompromitirati njegovu sigurnost. Ovaj završni korak protokola rezultirat će konačnim ključem kojeg će Alice i Bob koristiti za enkripciju. [8]

Ova dva dijela protokola neće biti pokrivena u radu zbog više razine kompleksnosti, ali čine neizostavan dio za njegovu stvarnu implementaciju.

2.5 Napomene

Trebalo bi spomenuti još nekoliko informacija vezanih uz QKD protokol. Prije svega, prethodno opisan protokol siguran je čak i od napada osobe koja ima beskonačnu računalnu snagu, ukoliko je ta osoba limitirana na način da može mjeriti fotone (ili, što će biti pokazano kasnije, svjetlosne pulseve) jedan po jedan te ako rezultate tih mjerenja koristi sa informacijama koje je prisluškivala u procesu razmjene putem

klasičnog kanala.

Tu postoji važna pretpostavka, a to je da osoba može prisluškivati, ali ne i utjecati, odnosno izmijenjivati informacije koje se razmijenjuju putem klasičnog kanala. Konkretno, Alice i Bob moraju biti sigurni da zaista komuniciraju jedno s drugim, a ne sa Eve kao posrednikom između njihove komunikacije jer onda ona može razmijeniti posebno svoj ključ sa Bobom i posebno ključ sa Alice, bez njihova znanja da je prisutna. Zbog toga je važno da Alice i Bob imaju sposobnost autentikacije prije samog protokola, što je opisano u BB84 članku [8].

3 Eksperimentalni postav

Kako bi se QKD uspješno implementirala, potrebna je kombinacija prikladnog fizikalnog postava, softvera za njegovu kontrolu i procesuiranje podataka te je potrebno analizirati sve parametre koji omogućavaju određivanje uspjeha ili neuspijeha implementacije.

3.1 Hardver

3.1.1 Predajnik

Predajni uređaj prije svega mora sadržavati izvor fotona. Mogu se koristiti pravi izvori pojedinačnih fotona, poput iona, molekula, kvantnih točaka i sličnog. Obično se radi o sustavima koje je moguće optički ili elektronički pobuditi, a njihovom relaksacijom emitirat će se energija u obliku fotona. U ovom smjeru još postoje istraživanja kako bi ovi izvori postali efikasni.

Zbog svoje praktičnosti se zato često koriste atenuirani (prigušeni) laserski pulsevi koji aproksimiraju pojedinačne fotone. Oni se mogu realizirati pomoću pulsirajućih laserskih dioda i preciznih atenuatora, što će rezultirati stvaranjem slabih koherentnih pulseva. Statistički, takva emitirana svjetlost slijedi Poissonovu distribuciju i jako je niskog intenziteta, sa prosječnim brojem fotona μ tipično približno $0,1$. Ako pogledamo Poissonovu distribuciju, opisanu jednadžbom:

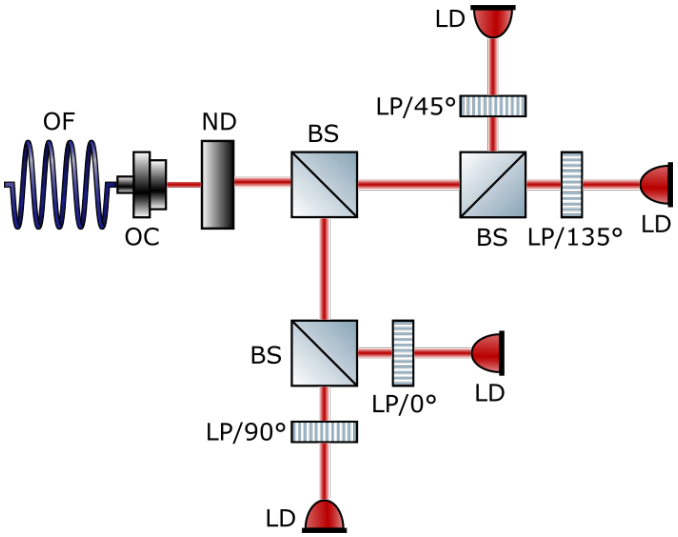
$$P(x) = \frac{\mu^x \cdot e^{-\mu}}{x!}, \quad x \in \mathbb{N}, \tag{3.1}$$

ona izražava vjerojatnost da se bilo koji broj događaja x dogodi u fiksiranom intervalu vremena, ako znamo očekivanu srednju vrijednost vjerojatnosti događaja μ i ako su oni međusobno nezavisni. Dakle, vrijednost $\mu = 0,1$ govori da će srednja vjerojatnost emitiranja 1 fotona po pulsu biti mala, ali će zato vjerojatnost za pojavu više od jednog fotona biti drastično smanjena. To je važno jer stvaranjem više fotona, odnosno multifotona te zatim njihovom polarizacijom i slanjem, postoji mogućnost napada od strane osobe koja prisluškuje, u kojem može saznati informacije o slanim bitovima bez detekcije od strane Alice i Boba. Mala vjerojatnost pojave 1 fotona bit će kompenzirana emitiranjem velikog broja pulseva u sekundi, reda veličine 10^6, što će rezultirati emitiranjem dovoljne količine pojedinačnih fotona za potrebe protokola.

Predajnik izgrađen za potrebe ove implementacije, odnosno predajni uređaj, prikazan na slici 3.4 i shemi 3.5, koristi prethodno opisane četiri laserske diode koje emitiraju svjetlosne pulseve valne duljine 810 nm, dakle svjetlost u blisko infracrvenom području elektromagnetskog spektra.

Slika 3.4: Predajnik izgrađen na Institutu Ruđer Bošković.

Ova valna duljina koristi se zbog nekoliko razloga. Prvi je taj da svjetlost valne duljine 810 nm ima nisku atenuaciju (gušenje) u optičkom vlaknu, što znači da, za takvu svjetlost, nema značajnih gubitaka jačine svjetlosnih signala koji putuju kroz optičko vlakno pa je zbog toga prikladna za dugodosežnu komunikaciju. Također, postoji efikasan način njene generacije i detekcije putem postojeće tehnologije i mnogi poluvodički detektori sposobni su detektirati svjetlost te valne duljine što otvara mogućnost



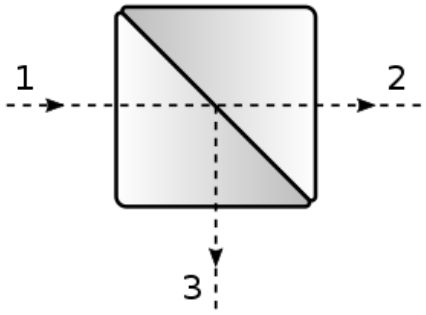
Slika 3.5: Shema predajnika. Tumačenje kratica: LD - laserska dioda (eng. *laser diode*), LP - linearni polarizator (eng. *linear polarizer*), BS - nepolarizirajući razdjelnik snopa (eng. *beam splitter*), ND - filter neutralne gustoće (eng. *neutral density filter*), OC - konektor optičkog vlakna (eng. *optical coupler*) i OF - optičko vlakno (eng. *optical fiber*).

komercijalne upotrebe, koja je i konačni cilj.

Svaka dioda postavljena je na kinematičko postolje. Kinematička postolja omogućavaju pomicanje optičkih komponenti i kalibraciju njihovog položaja pa se pomoću njih može podešavati smjer propagacije fotona. Također je na svako postolje postavljen polarizator, čijim je rotiranjem moguće namjestiti jednu od četiri ravnine polarizacije: 0°,45°,90° ili 135°, po jednu za svaku diodu. Zajedno, ove polarizacije tvore dvije ortogonalne baze pomaknute za 45°.

Važno je da svjetlosne diode emitiraju pulseve potpuno nasumično. Ako bi redoslijed ispucavanja ikako bio predvidljiv, ugrozila bi se sigurnost protokola. Zbog toga redoslijed slanja pulseva određuje kvantni generator nasumičnih brojeva koji se bazira na registru pomaka s linearnom povratnom spregom LSFR (eng. Linear-feedback shift register). On generira nasumični niz bitova koji se zatim kodiraju u polarizacijska stanja fotona, tj. u redoslijed okidanja laserskih dioda.

Nakon polarizacije, svjetlost se usmjerava prema istom optičkom putu uz pomoć tri 50:50 nepolarizirajuća razdjelnika snopa (proizvođača Thorlabs, model BS011). Oni svaku upadnu zraku svjetlosti razdvoje na način da dio svjetlosti propuste (transmitiraju) u smjeru upadne zrake, a dio reflektiraju u smjeru okomitom na smjer upadne zrake, kao što je prikazano na slici 3.6.



Slika 3.6: Prikaz dijeljenja snopa svjetlosti pomoću razdjelnika snopa. Dio upadne svjetlosti je transmitiran, a dio reflektiran. Izvor: [9]

Intenzitet transmitirane i reflektirane zrake je svaki za 50% manji od intenziteta upadne zrake, dakle zraka koja nastavlja u željenom optičkom putu je 50% manjeg intenziteta u odnosu na početni. Kao što je vidljivo iz slike 3.5, svaka zraka prolazi kroz dva razdjelnika snopa, što znači da će nakon prolaska kroz njih imati četvrtinu početnog intenziteta.

Na kraju takva zraka prolazi kroz filter neutralne gustoće, koji služi kako bi joj dodatno smanjio intenzitet. Ovaj cijeli proces smanjivanja intenziteta svjetlosti, putem razdjelnika snopa i putem filtera, služi kako bi se realizirao prethodno opisan intenzitet od u prosjeku 0,1 fotona po pulsu. Uz to, filter neutralne gustoće služi i za simulaciju gubitaka u optičkom vlaknu između prijamnog i predajnog uređaja, o čemu će biti riječ u sljedećem odlomku.

3.1.2 Kvantni kanal

Kvantni kanal je poveznica između predajnog i prijamnog uređaja kojeg u ovoj implementaciji čine 3 jednomodna optička vlakna. Na predajni uređaj spojeno je 780HP optičko vlakno duljine dva metra koje se zatim spaja sa G.652.D telekomunikacijskim optičkim vlaknom duljine pet metara, a ono je zatim spojeno ponovno na 780HP optičko vlakno duljine pet metara koje ulazi u prijamni uređaj.

G.652.D telekomunikacijsko optičko vlakno je, kao što i samo ime kaže, vlakno koje se koristi u telekomunikacijskoj infrastrukturi te je upotrijebljeno kako bi se ispitala mogućnost uspostave QKD protokola upravo preko postojeće infrastrukture. Nedostatak tog vlakna je to što je predviđeno za provođenje svjetlosti valne duljine 1550 nm, dok je korištena valna duljina u eksperimentu 810 nm. Zbog prolaska svjetlosti čija je valna duljina bitno manja od 1550 nm kroz G.652.D vlakno, unutar

njega generira se više od jednog optičkog moda. Ukoliko bi, unatoč tome, protokol bilo moguće provesti putem navedenog vlakna, njegova integracija bila bi puno jednostavnija i jeftinija.

Prolaskom svjetlosti kroz optičko vlakno njegova polarizacija može se nasumično promijeniti na način da se zakrene ili čak prijeđe u cirkularnu polarizaciju. Zbog toga je potrebno koristiti polarizacijski kontroler, odnosno uređaj koji može modificirati polarizaciju svjetlosti i time kompenzirati navedene promjene.

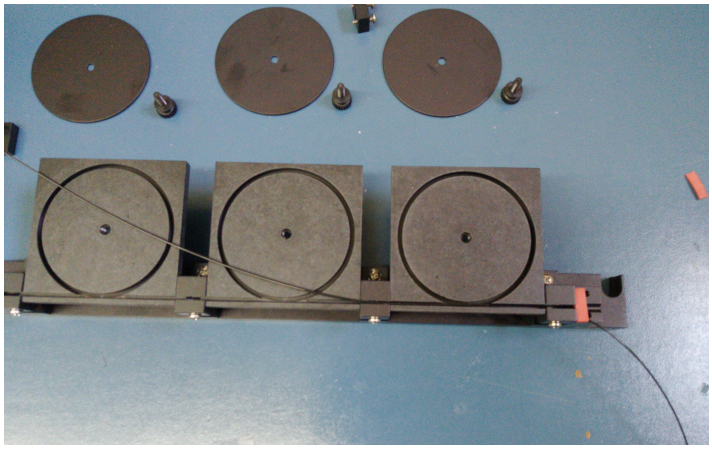
Polarizacijski kontroler korišten u ovoj implementaciji (Thorlabs FPC560, prikazan na slici 3.7) sastoji se od tri pločice oko kojih je moguće namotati optičko vlakno. Ovisno o broju namotaja, pločice se mogu ponašati kao zakretači polarizacije. Zakretači polarizacije su optički uređaji koji utječu na polarizaciju svjetlosti koja kroz njih prolazi. Dva najčešća tipa su $\lambda/2$ i $\lambda/4$ zakretači polarizacije. $\lambda/2$ zakretač koristi se kako bi se promijenila ravnina linearno polarizirane svjetlosti, dok se $\lambda/4$ zakretač polarizacije koristi za pretvaranje linearno polarizirane svjetlosti u cirkularnu. [11]

U ovom slučaju, vlakno je namotano tako da se središnja pločica ponaša kao $\lambda/2$, a druge dvije kao $\lambda/4$ zakretači polarizacije.

Slika 3.7: Polarizacijski kontroler proizvođača Thorlabs, model FPC560. Izvor: [10]

Zakretanjem pločica namotano vlakno se napreže i postaje anizotropno (što znači da njegova fizikalna svojstva poprimaju različite vrijednosti za različite smjerove). Za optičko vlakno to rezultira time da indeksi loma različitih osi u vlaknu više nisu jednaki te zbog toga u njemu komponente elektromagnetskog vala sada putuju različitom grupnom brzinom što rezultira promjenom polarizacije. Rotiranje pločica zapravo je jednako rotiranju zakretača polarizacije i tom rotacijom se kompenzira prethodno spomenuta nasumična promjena polarizacije. [11] [12] [13]

Optičko vlakno G.652.D namotala sam u polarizacijski kontroler. Vlakno je u posebnoj tubi promjera 0,9 mm jer se samo uobičajeno vlakno u njega ne može namotati. Nažalost, namotavanje G.652.D vlakna u kontroler, upravo zbog više optičkih modova, nije rezultiralo zadovoljavajućom kalibracijom polarizacije, dok namotavanje 780HP vlakna jest. Zbog toga su u implementaciji korištena 3 vlakna, prilikom čega je 780HP vlakno koje ulazi u prijamnik namotano na polarizacijski kontroler. Ovakva implementacija i dalje omogućava da se protokol izvrši kroz G.652.D vlakno.



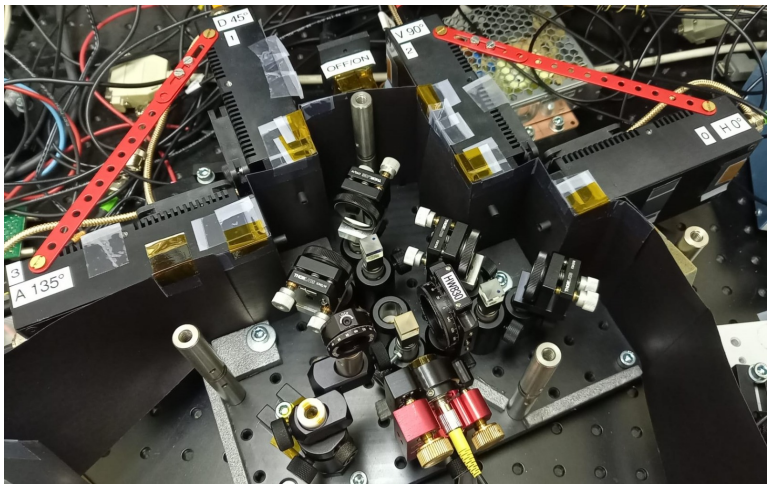
Slika 3.8: Prikaz rastavljenog FPC560 polarizacijskog kontrolera u koji se namotava G.652.D optičko vlakno.

Uz interes uspostave protokola putem telekomunikacijskog vlakna veže se i potreba uspješne uspostave protokola na nekoj značajnijoj udaljenosti. Svjetlost ne može putovati do beskonačne udaljenosti u vlaknu zbog toga što pri prolasku dolazi do njenog gušenja, uzrokovanog apsorpcijom, raspršenjem i drugim efektima. [14]

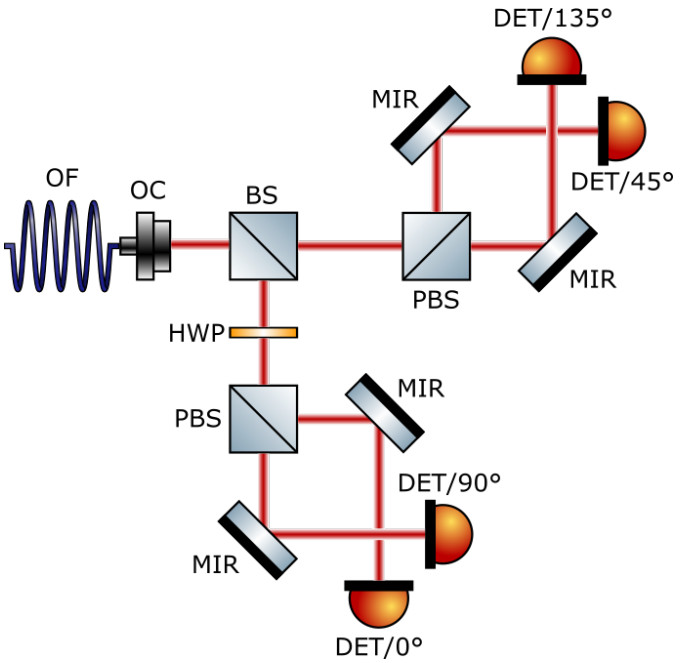
Što je veća komunikacijska udaljenost, doći će do većeg gušenja. Zbog toga se uz pomoć filtera neutralne gustoće želi simulirati gušenje u vlaknu i time ispitati do kojih udaljenosti protokol može dobro funkcionirati, tj. biti uspješno implementiran.

3.1.3 Prijamnik

Prijamni uređaj prikazan je na slici 3.9 i shemi 3.10. Prvo na što će svjetlost naići u prijamniku je 50:50 nepolarizirajući razdjelnik snopa, čija je uloga nasumično biranje baze - kada foton naiđe na razdjelnik snopa, u 50% slučajeva bit će transmitiran, odnosno propušten, a u 50% slučajeva reflektiran.



Slika 3.9: Prijamni uređaj izgrađen na Institutu Ruđer Bošković.



Slika 3.10: Shema prijamnika. Tumačenje kratica: OF - optičko vlakno (eng. *optical fiber*), OC - konektor optičkog vlakna (eng. *optical coupler*), BS - nepolarizirajući razdjelnik snopa (eng. *beam splitter*), HWP - $\lambda/2$ pločica (eng. *half-wave plate*), PBS - polarizirajući razdjelnik snopa (eng. *polarizing beam splitter*), MIR - zrcalo (eng. *mirror*), DET - detektor (eng. *detector*).

Kao što je vidljivo iz slike prijamnika, ovisno o tome je li foton transmitiran ili reflektiran, nastavit će putovati u transmitiranoj ili reflektiranoj grani. Svaka od njih zapravo predstavlja jednu bazu. U slučaju transmisije, odabrana baza je $\{45°, 135°\}$, a u slučaju refleksije $\{0°, 90°\}$.

Svaka baza sastoji se od polarizacijskog razdjelnika snopa, koji će preusmjeriti foton ovisno o njegovoj polarizaciji prema odgovarajućem zrcalu iz kojeg će biti reflektiran u pripadajući detektor. Jedina razlika između fizičkih komponenti baza je

ta što je u $\{0°, 90°\}$ bazi, tj. grani, prije polarizirajućeg razdjelnika snopa postavljen $\lambda/2$ zakretač polarizacije, koji rotira polarizaciju fotona za $45°$. Ako je foton usmjeren u krivu bazu, postoji vjerojatnost od 50% da će biti reflektiran, a 50% da će biti transmitiran. Dakle, postoji vjerojatnost da ga detektira bilo koji od dva detektora u krivoj bazi. Ukoliko je pak usmjeren u ispravnu bazu, polarizacijski razdjelnik snopa će ga preusmjeriti u odgovarajući detektor i njegova polarizacija će se ispravno detektirati.

Detektori fotona korišteni u ovoj implementaciji su SPAD (eng. *Single Photon Avalanche Diode*) detektori. Već iz njihovog imena može se iščitati puno stvari. Prije svega, oni su fotodiode, odnosno uređaji koji svjetlosni signal pretvaraju u električni. Od svih opcija poluvodičkih optičkih detektora, fotodiode su iznjedrile kao najjednostavnije i najjeftinije. Jedna od prednosti SPAD detektora je to da imaju pikosekundnu rezoluciju, dakle mogu sa pikosekundnom preciznošću detektirati dolazak (vrijeme dolaska) fotona. Njihov glavni nedostatak u odnosu na analogne detektore je mrtvo vrijeme (eng. *deadtime*) nakon svake detekcije, koje limitira njihovu maksimalnu sposobnost detektiranja fotona (eng. *count rate*). SPAD detektori također iskaču jer imaju određene prednosti u usporedbi s nekim od najobećavajućih detektora pojedinačnih fotona poput PMT (eng. *Photomultiplier Tubes*) i SNSPD (eng. *Superconductive Nanowire Single-Photon Detectors*) detektora. PMT detektori trebaju visoki prednapon, masivni su, osjetljivi na magnetska polja i ne mogu se integrirati u CMOS elektroniku. SNSPD detektori trebaju kriostat, odnosno trebaju biti u jako hlađenom okruženju do na nekoliko kelvina, što i njih čini masivnima te limitira njihovu primjenu zbog teškoće integracije, unatoč tome što imaju sjajnu efikasnost detekcije fotona, puno bolju u odnosu na SPAD detektore. [15]

Ukratko, SPAD detektori imaju sljedeće prednosti: detektiraju pojedinačne fotone, imaju pikosekundnu preciznost, ali prije svega kompaktni su, jeftini i lako se integriraju. [15]

Važno je moći zabilježiti vrijeme detekcije svakog fotona, stoga su detektori spojeni na snimač vremena detekcije, uređaj ID 900, proizvođača ID Quantique, koji vremena detekcije svakog detektora pohranjuje u zasebne datoteke. Uređaj ima rezoluciju 100 pikosekundi.

3.1.4 Kalibracija

Prije izvođenja eksperimenta potrebno je kalibrirati postav. Kalibracija se može podijeliti u više manjih koraka.

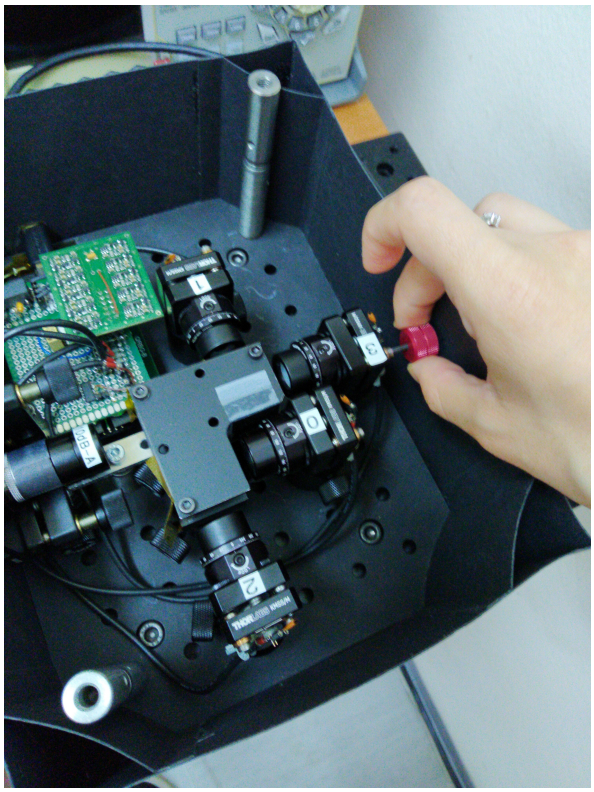
Prije svega, potrebno je kalibrirati prijamni uređaj pomoću nepolarizirane svjetlosti na način da se ona usmjeri u prijamnik putem vlakna (koje se iz njega više ne vadi). Zatim se pomicanjem zrcala u prijamniku treba postići da sva 4 detektora detektiraju istu razinu svjetla. Nakon toga, iza ulaznog vlakna stavlja se vrlo precizan polarizator visoke ekstinkcije. On se nalazi na rotatoru i ima označene stupnjeve te se zatim pomoću njega namješta da svaki detektor detektira samo svoju polarizaciju. Kada je ovaj korak uspješno proveden, miče se polarizator i prijamni uređaj je kalibriran.

Nadalje, potrebno je postići jednak intenzitet pulseva svih laserskih dioda u predajnom uređaju. Zbog toga sam izlaz predajnog uređaja optičkim vlaknom spojila u SPCM-NIR pomoćni detektor proizvođača Excelitas Technologies koji sam pak spojila u frekvenciometar čije se očitanje prikazuje putem programa za kalibraciju u obliku stupca te sa pripadnom vrijednosti frekvencije.

Slika 3.11: Pomoćni detektor proizvođača Excelitas Technologies korišten za potrebe kalibracije predajnog dijela QKD.

Zatim sam, putem zakretanja kinematičkog postolja svake laserske diode unutar predajnika, pomoću vijka, nastojala podesiti jednaku frekvenciju detekcije na frekvenciometru, odnosno intenzitet pulseva za svaku lasersku diodu dok za sve nije jednak. Za potrebe navedenog, pokrenula bih program i kroz njega postavljala te mijenjala trajanje signala i laserske diode čiji sam intenzitet htjela podesiti. Kada bih

postigla zadovoljavajuće rezultate, pokrenula bih program koji provjerava uniformnost intenziteta svih lasera kako bih potvrdila da je ovaj korak uspješno proveden.



Slika 3.12: Zakretanjem kinematičkog postolja pomoću crvenog vijka podešavala sam intenzitet pulseva dioda.

Zatim slijedi spajanje predajnika i prijamnika, putem vlakana, sa polarizacijskim kontrolerom pozicioniranim kako je opisano u odlomku 3.1.2. Vlakno kojim je predajnik spojen na pomoćni detektor potrebno je iz njega izvaditi i spojiti s prijamnikom, preko polarizacijskog kontrolera. Emitiranjem svjetlosti iz prijamnika, za svaku polarizaciju posebno, namještala sam položaj polarizacijskog kontrolera dok za promatranu polarizaciju nisam postigla minimum detekcije suprotne polarizacije koja pripada istoj bazi, pri čemu je ugađanje položaja polarizacijskog kontrolera za jednu polarizaciju često poremetilo ugođenost položaja za ostale. Postupak sam ponavljala dok nisam dobila zadovoljavajuće rezultate za sve polarizacije odjednom. Nakon ugađanja putem programa provjerila bih rezultate kako bih potvrdila kalibraciju.

Kao zadnji korak, u mraku se otvara prijamni uređaj i ugađaju se zrcala u njemu kako bi se postigla jednaka frekvencija detekcija pripadajućih polarizacija, odnosno osiguralo da detektori dobro primaju signal. Zatim je potrebno vratiti se na prethodni korak i provjeriti njegovu uspješnost. Po potrebi se zatim ponovno izvode drugi i

treći korak, sve dok rezultati kalibracije nisu zadovoljavajući, nakon čega se može pokrenuti eksperiment.

Cijeli kalibracijski postupak u ovom je slučaju pokrenut i praćen putem programa na kompjuteru napisanog za kalibraciju i njenu provjeru, koji je napisan na Institutu Ruđer Bošković. Postupak kalibracije ponavljala sam više puta, prije svakog izvršavanja protokola.

3.2 Softver

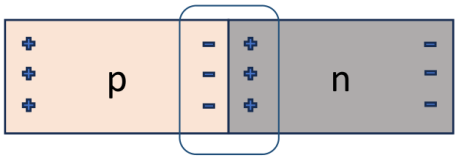
Kako bi se postav mogao kontrolirati, kalibrirati te zatim obraditi podatci, potrebno je imati i prikladan softver. On se sastoji od algoritama za poravnanje, ispravljanje pogrešaka te pojačavanje privatnosti, koji su implementirani u programskom jeziku C. Sav softver napisan je na Institutu Ruđer Bošković.

Cilj algoritma za poravnanje je dobiti jedan na jedan korespondenciju Aliceinog i Bobovog niza polarizacija. Nakon transmisije polariziranih fotona, Bob pomoću snimljenih vremena detekcije sortira svoj niz izmjerenih polarizacija. No, s obzirom da sustav ima gubitke, a dodatno svaki puls sadrži samo 0,1 foton u prosjeku, Bob ne može detektirati svaki Alicein puls, stoga se njihovi nizovi polarizacija sigurno razlikuju. Također, neke Bobove detekcije uopće ne potječu od fotona koje je Alice poslala, nego od šuma i zakašnjelih lavina u SPAD detektorima, što će biti pojašnjeno u poglavlju 4. Zbog toga je potrebno razlučiti koje detekcije dolaze od Aliceinih fotona te prepoznati i označiti sve Aliceine fotone koje Bob nije detektirao. Tada postoji jedan na jedan korespondencija između njihovih nizova.

Tek nakon završetka poravnanja, dolazi do dijela gdje Bob odbacuje sve bitove koje je detektirao u krivoj bazi. Uz to, Alice mora odbaciti sve bitove koje Bob nije primio te one gdje je detektirao više njih u različitim detektorima. Nakon toga mogu nastaviti na faze ispravljanja pogrešaka i pojačavanja privatnosti, spomenute u poglavlju 2.4, korištenjem prikladnih algoritama.

4 Princip rada SPAD detektora te parametri koji iz njega proizlaze

Kao što je ranije spomenuto, SPAD detektori su fotodiode. Dioda nastaje spajanjem 2 tipa poluvodiča - pozitivnim p-tipom i negativnim n-tipom. Kada se spoje, jedan dio viška naboja zbog privlačenja krene, s jedne i s druge strane, na suprotnu. Zbog tih prelazaka naboja, u okolini njihovog spoja (eng. *junction*) dolazi do formiranja nove regije nakupljenog naboja koja stvori barijeru za daljnje prelaske, što je prikazano na slici 4.13. Ova regija naziva se zonom osiromašenja (eng. *depletion region*), upravo zbog prelazaka naboja koji za sobom ostavljaju pozadinsko područje koje postaje ili sve više negativno ili sve više pozitivno nabijeno. Kada se zaustavi prelazak naboja, postignuta je ravnoteža.

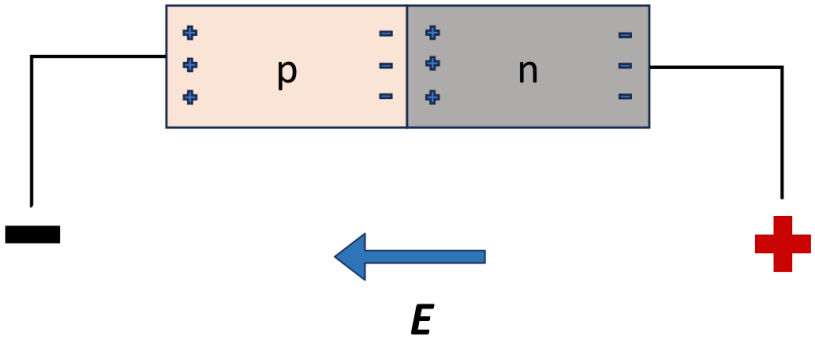


Slika 4.13: Prikaz formiranja barijere - lijevo nakupljeni negativni naboj odbija ostali višak elektrona iz n-tipa i time ih sprječava da prelaze u p-tip. Isto se događa sa desne strane gdje nakupljeni pozitivni naboji (odnosno šupljine) sprječavaju daljnji prelazak.

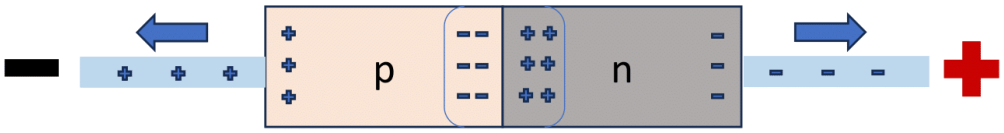
Ukoliko se sada izvor napona spoji na diodu, ovisno o tome koji pol je spojen na koji tip poluvodiča, doći će do različitih efekata. U ovom slučaju, negativan pol spojen je na p-tip, a pozitivan pol na n-tip, kao što je prikazano na slici 4.14. Ovako spojen napon na diodu naziva se reverzni napon (eng. reverse bias voltage).

Zbog spajanja reverznog napona na diodu, doći će do privlačenja naboja u svakoj strani poluvodiča prema izvoru napona. Taj odlazak naboja rezultira povećavanjem zone osiromašenja, čime se povećava razlika potencijala u toj zoni. Proces je prikazan na slici 4.15.

S obzirom da je zona osiromašenja veća, barijera koja sprječava prelazak naboja iz jednog tipa u drugi je također veća, odnosno snažnija. Sada više niti jedan elektron i šupljina ne bi trebali biti u mogućnosti prijeći iz jednog tipa u drugi, no ipak,

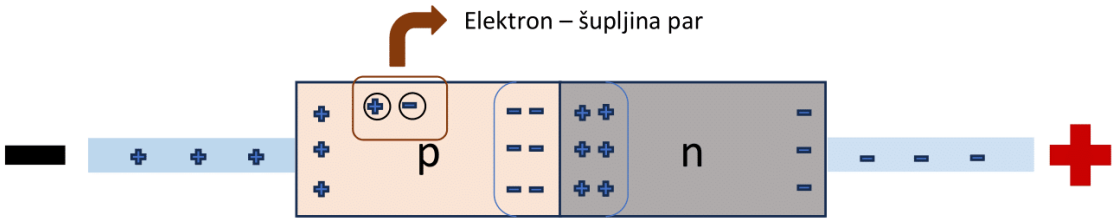


Slika 4.14: Spajanjem reverznog napona na krajeve diode stvara se električno polje u smjeru prikazanom na slici.



Slika 4.15: Prikaz procesa koji se odvija u diodi prilikom spajanja na reverzni napon. Naboje privlače polovi izvora napona te oni napuštaju diodu, ostavljajući za sobom naboje suprotnog predznaka.

dolazi do prolaska elektrona. Naime, zbog termalnih efekata rijetko dolazi do stvaranja elektron-šupljina para u osiromašenoj zoni. Prilikom njihovog stvaranja oni se ne uspiju rekombinirati, već bivaju privučeni kao što je prikazano na slici 4.16.



Slika 4.16: Prilikom termalne generacije elektron-šupljina para, vidljivo je da će šupljina biti privučena u lijevo, a elektron će biti privučen prema snažno pozitivnoj desnoj strani, te će poteći struja kroz diodu.

Ako se napon nastavi povećavati do kritične vrijednosti koju nazivamo Geigerov napon proboja (eng. *Geiger breakdown voltage*) i iznad, onda elektroni nastali termal-

nom generacijom zbog visokog napona imaju veću energiju dok putuju te se pri tom putu sudaraju sa atomima i izbacuju valentne elektrone iz orbite, koji sada postaju također slobodni, čime dolazi do povećanja struje elektrona. Ti izbačeni elektroni također imaju visoku energiju te se i oni sudaraju sa atomima, izbacuju nove elektrone i stvaraju isti efekt, čiji je naziv simboličnog karaktera - lavina (eng. *avalanche*). Rezultat tog procesa je protok struje kroz diodu unatoč barijeri.

Upravo se ovaj efekt iskorištava za detektiranje fotona. Kada je reverzni napon na fotodiodi iznad kritične vrijednosti, upadni foton koji dolazi na zonu osiromašenja fotodiode stvara elektron-šupljina par, zatim taj elektron ”generira” još elektrona putem sudara, čime se stvori struja koja se može mjeriti i koja će implicirati upravo da je foton stigao do diode. Na taj način se foton detektirao.

Doduše, efekt lavine treba zaustaviti, tj. ugušiti (eng. *quench*), kako bi se foton mogao ponovno detektirati. To se može postići smanjenjem napona ispod kritične vrijednosti, pomoću aktivnih ili pasivnih sklopova. Primjer jednostavnih pasivnih sklopova je otpornik spojen u seriju sa diodom. Proces bi izgledao ovako:

1. Potekla je struja kroz diodu i time kroz strujni krug - foton je detektiran;
2. Struja poteče i kroz otpornik - dolazi do pada napona (zona osiromašenja slabi), napon je sada manji od napona proboja;
3. Dolazi do zaustavljanja lavine;
4. Nakon smanjenja napona, postoji predeterminirano vrijeme, tzv. mrtvo vrijeme (eng. *dead time*), tijekom kojeg SPAD, odnosno fotodioda, ostaje u prigušenom stanju i za to vrijeme detektor nije osjetljiv na upadne fotone; u tom vremenu napon se ponovno povećava tako da se uspostavi povećanje zone osiromašenja da se može ponovno proizvesti efekt;
5. Nakon mrtvog vremena, ponovno su se uspostavili ranije opisani uvjeti za efekt lavine, odnosno za detekciju fotona.

Cijeli postupak ponavlja se za svaku detekciju.

4.1 Parametri

Opis rada SPAD detektora važan je kako bi bilo jasno od kud proizlaze parametri o kojima će biti riječ u ovom odlomku.

SPAD detektori imaju svoja neidealna ponašanja koja se moraju pažljivo karakterizirati. Imaju svoje izvore šuma (npr. termalne generacije, zakašnjele lavine), imaju limitiranu osjetljivost na svjetlost koja varira sa valnom duljinom i imaju vremenski odziv koji ovisi o apsorpcijskoj poziciji.

Sve parametre analizirala sam putem programa koje sam napisala u programskom jeziku Python.

4.1.1 Izvori šuma

Detekcije koje nisu nastale uslijed vanjske pobude u obliku svjetlosti karakteriziraju se kao šum. Kod SPAD detektora, neki od izvora šuma su termalne generacije i tuneliranje.

Termalne generacije, odnosno pobuđenja, nastaju zbog termalnih vibracija čestica. Vibracije čestica uzrokuju sudare unutar kristalne rešetke zbog kojih može doći do pobuđivanja elektrona iz valentne u vodljivu vrpcu, čime se stvaraju elektron-šupljina parovi zbog kojih nastaju lavine. Kao što i samo ime implicira, termalna pobuđenja jako ovise o temperaturi; šum se najčešće udvostruči kada se temperatura poveća za 10°C oko sobne temperature, te je na toj temperaturi termalna generacija dominantni izvor šuma.

Tuneliranje je kvantnomehanički efekt kod kojeg čestica (u ovom slučaju elektron) može preći energetsku barijeru unatoč tome što nema energiju veću od vrha barijere. Kod tuneliranja nije potrebno pobuđivanje elektrona. Konkretno, elektron može bez promjene energije preći iz valentne u vodljivu vrpcu i time pridonijeti struji elektrona koja izaziva lavine. Doprinos šumu zbog tuneliranja ne raste puno sa povećanjem temperature, ali se povećava sa povećanjem reverznog napona iznad napona proboja.

Kada se govori o šumu, najčešće se zapravo ova dva izvora šuma karakteriziraju zajedno (eng. *Dark Count Rate, DCR*) pa se šum definira kao srednja vrijednost rate izlaznog pulsa kada nema svjetlosti koja bi interagirala sa detektorom. U prijevodu, kada je detektor u mraku, tj. unatoč tome što nema svjetlosti koja bi proizvela lavinu, vidjet će se da postoje nekakve detekcije. To su detekcije uzrokovane šumom.

S obzirom da šum nastaje nasumičnim procesima (slijedi Poissonovu distribuciju), ne može se lako otkloniti od mjerenja zbog svoje statističke fluktuacije. Najlakše se odredi upravo mjerenjem broja detekcija po sekundi u mraku bez svjetlosnih pobuda. Na taj način šum je određen i u ovom eksperimentu. Mjerenje je provedeno nakon

kalibracije, ali prije same distribucije ključa. Frekvencija izmjerenog šuma je u prosjeku iznosila 100 do 300 Hz za sve provedene distribucije ključa. Također, sva četiri detektora imala su podjednak broj detekcija po sekundi. [15]

4.1.2 Zakašnjele lavine

Zakašnjele lavine (eng. *afterpulsing*) direktno su povezane sa detekcijama fotona. Svaka zakašnjela lavina ima svoju primarnu detekciju.

Tokom lavine, duboke zamke prisutne u kristalnoj rešetci detektora mogu "uhvatiti" nosioce naboja i otpustiti ih nakon dobro definiranog vremena u kojem se očekuje detekcija fotona. Ako se nosioc naboja otpusti taman kada se SPAD pripremi za novu detekciju fotona, dolazi do stvaranja sekundarne lavine čije vrijeme života može varirati od nekoliko nanosekundi do nekoliko mikrosekundi i smanjuje se na većim temperaturama (primijetimo da se smanjivanjem temperature mogu smanjiti termalne generacije, ali se zato produljuje vrijeme života zakašnjelih lavina).

Kako bi se smanjile zakašnjele lavine, nakon svake lavine SPAD detektori se ugase na vremenski interval od nekoliko nanosekundi tako da se većina zarobljenih nosioca naboja otpusti prije ponovnog osposobljavanja detektora za detekciju. Treba oprezno odrediti to vrijeme jer ono može značajno smanjiti ratu detekcije fotona.

Vjerojatnost pojave zakašnjelih lavina ovisi o broju nosioca koji pridonose struji prilikom svake lavine. Smanjivanje struje fundamentalno je za smanjivanje njihove pojave. Također, uzrok zakašnjelih lavina može biti i šum. Povećanjem frekvencije transmisije fotona povećava se i broj detekcija uzrokovanih zakašnjelim lavinama. [15]

Zakašnjele lavine prikazala sam i analizirala crtanjem histograma vremenskih intervala između uzastopnih vremena detekcije lavina. U svrhu karakteriziranja zakašnjelih lavina, iz podataka sam izračunala vrijeme τ koje reprezentira srednje vrijeme za koje se amplituda signala zakašnjelih lavina smanji za 1/e u odnosu na početnu amplitudu. Obično vrijeme τ u kontekstu SPAD detektora predstavlja karakterističnu vremensku skalu trnuća zakašnjelih lavina.

Kraće, odnosno malo vrijeme τ ukazuje na brže smanjivanje amplitude signala zakašnjelih lavina, što ujedno znači i kraće vrijeme života zakašnjelih lavina. S druge strane, dulje, odnosno veće vrijeme τ ukazuje na dugoživuće zakašnjele lavine kojima

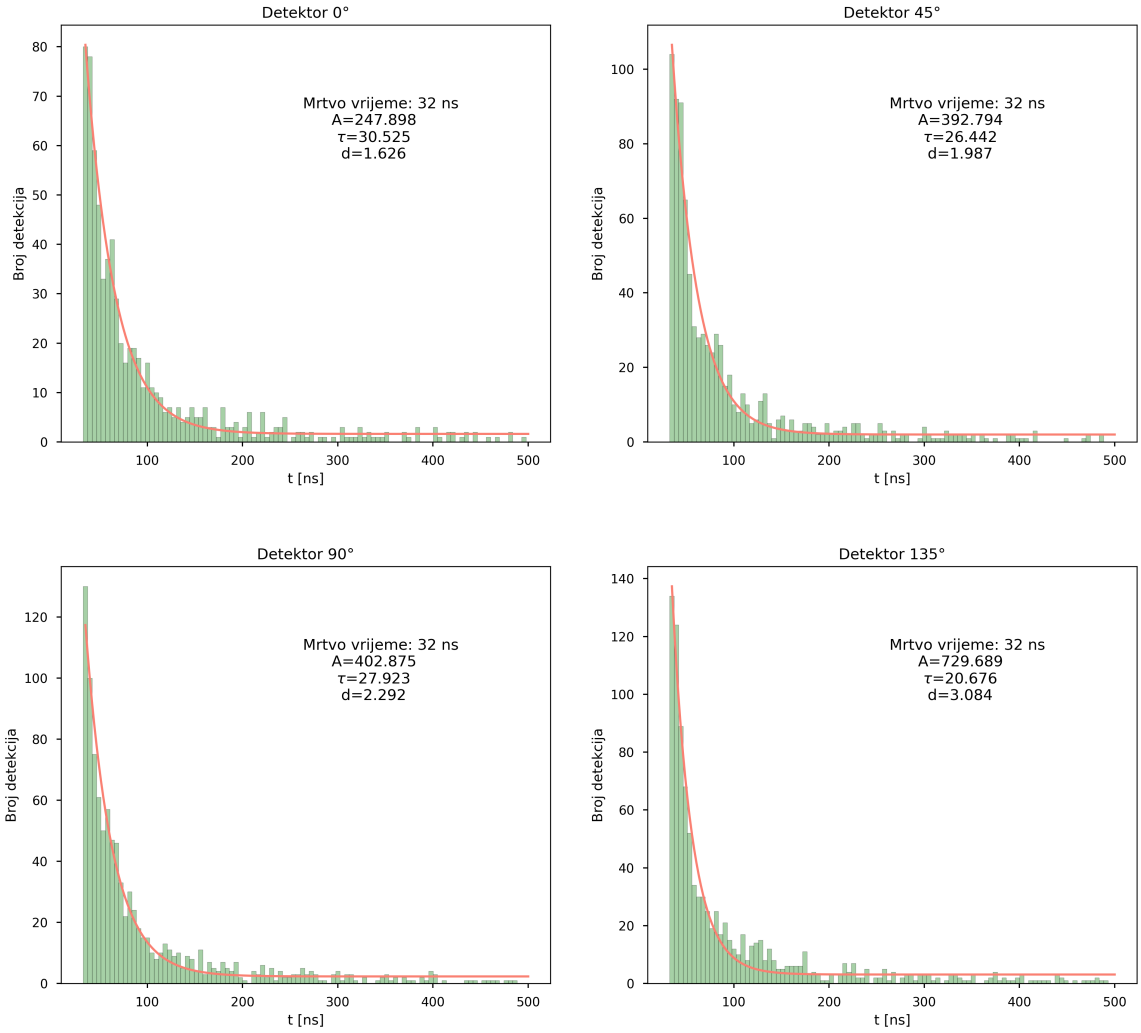
signal sporo trne.

Informaciju o vremenu τ dobila sam iz histograma, modeliranjem njegovog trnuća pomoću funkcije. U članku [16] predložena su tri modela od kojih se prvi, tzv. "multi-eksponencijalni model", pokazao kao prikladniji od ostalih za zakašnjele lavine SPAD detektora. Zbog toga je sam u ovoj obradi koristila funkciju po uzoru na taj model.

Modelirajuća, eksponencijalna funkcija dana je relacijom:

$$f(t) = Ae^{-\frac{t}{\tau}} + d, \tag{4.2}$$

gdje je A početna amplituda zakašnjelih lavina, τ je spomenuto karakteristično vrijeme, a d je pomak uzrokovan šumom. Na slici 4.17 prikazala sam histograme za sva četiri detektora sa modelirajućom funkcijom i izračunatim parametrima. Iz grafova je vidljivo kako je karakteristično vrijeme τ kratko što pokazuje da zakašnjele lavine traju kratko, njihovo gušenje je brzo i uspješno se sprječava njihov značajniji utjecaj na detekcije fotona. Na prikazu se vidi i mrtvo vrijeme detektora koje iznosi 32 ns za svaki detektor.



Slika 4.17: Prikaz histograma i analize zakašnjelih lavina za svaki detektor.

4.1.3 Vremensko podrhtavanje

Između svake apsorpcije fotona u detektoru i signala generiranog lavinama koje te apsorpcije uzrokuju postoji predviđeni vremenski razmak. Vremensko podrhtavanje je odstupanje od (varijacija) tog vremena. Kao posljedica vremenskog podrhtavanja detektirani signal bit će vremenski rasprostranjen oko očekivanog vremena detekcije fotona. [15]

U ovoj implementaciji postoje dva doprinosa vremenskom podrhtavanju - doprinos od detektora i doprinos od pulsirajućih laserskih dioda. U detektoru se podrhtavanje javlja zbog toga što je generiranje lavine stohastički proces. Kod dioda se javlja zbog raznih efetaka poput fluktuacija u temperaturi koje utječu na diodu, nestabilnosti frekvencije emitirane svjetlosti i sl. Za ovaj slučaj doprinos detektora je

puno manji u odnosu na doprinos dioda stoga će biti zanemaren jer nije značajan za analizu.

Analizom vremenskog podrhtavanja može se odrediti tzv. prozor koincidencije, odnosno vremenski interval u kojem će foton sigurno biti detektiran, što je jako važno za kasniji proces poravnanja.

Vremensko podrhtavanje također sam analizirala crtanjem histograma vremenskih intervala između uzastopnih vremena detekcije lavina, no u ovom sam slučaju graf fokusirala samo na kratki vremenski interval oko detekcije fotona. Zatim sam na histogram modelirala krivulju Gaussove raspodjele jer se očekuje da vremensko podrhtavanje slijedi upravo Gaussovu raspodjelu (odnosno da će se na detektiranom signalu vidjeti maksimum te eksponencijalni pad signala sa svake strane).

Gaussova raspodjela opisana je relacijom:

$$f(t) = A\, e^{-\frac{1}{2}(\frac{t-\mu}{\sigma})^2}, \tag{4.3}$$

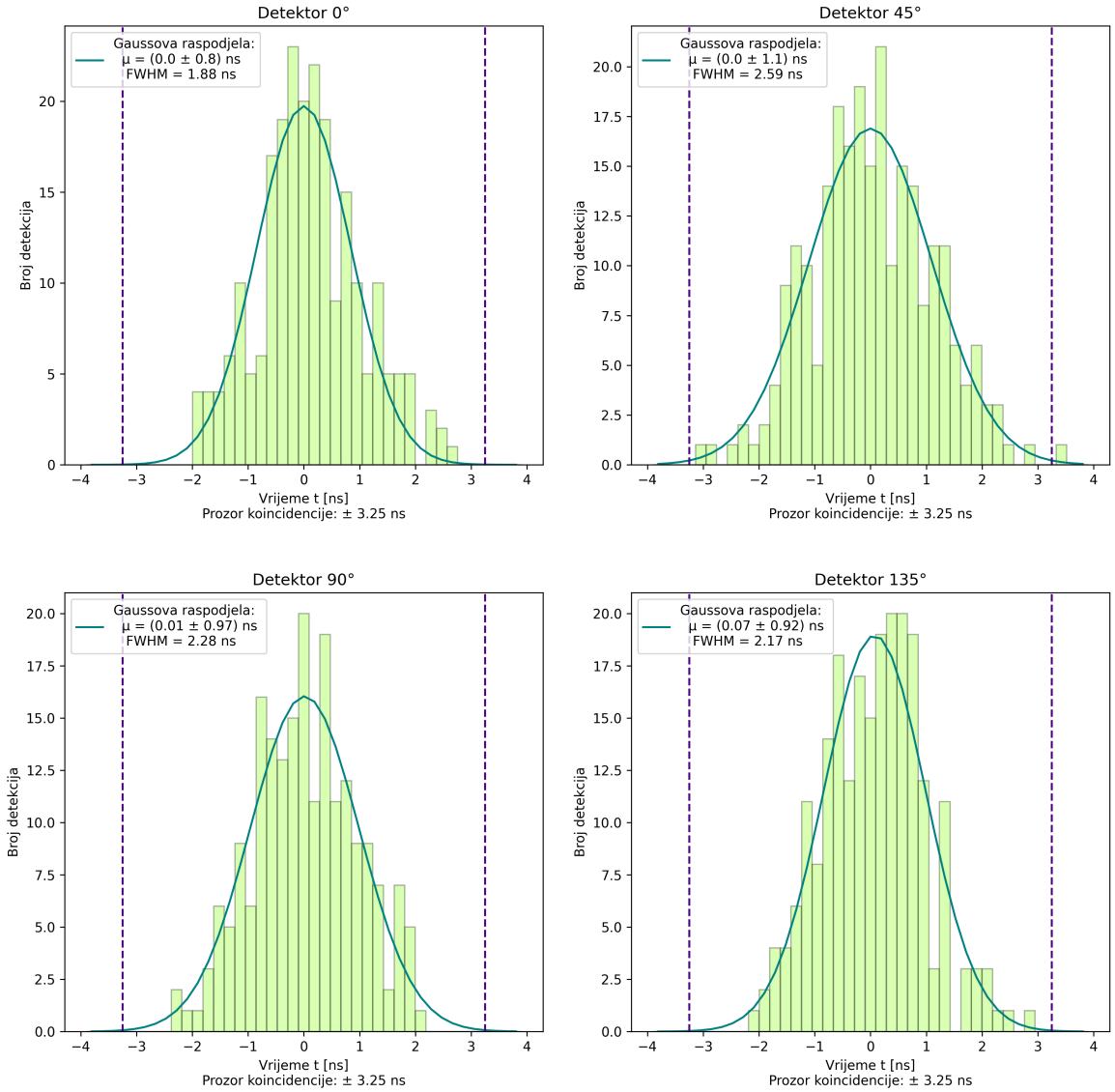
gdje je μ srednja vrijednost ili očekivana vrijednost distribucije, A je amplituda, a σ je standardna devijacija odnosno odstupanje od srednje vrijednosti. U kontekstu analize vremenskog podrhtavanja, očekivana vrijednost je vrijeme u kojem se očekuje detekcija fotona, primjerice ako je frekvencija ispucavanja diode 1 MHz, to znači da se detekcija fotona očekuje svake mikrosekunde. Standardna devijacija onda daje vrijednost vremenskog odstupanja od te očekivane vrijednosti.

Na slici 4.18 prikazala sam grafove vremenskog podrhtavanja za svaki detektor, sa pripadnim srednjim vrijednostima te standardnim devijacijama.

Standardna devijacija direktno je povezana sa FWHM (eng. *Full Width at Half Maximum*) vrijednosti upadnog laserskog pulsa na fotodetektor preko relacije:

$$FWHM = 2,3548 \cdot \sigma. \tag{4.4}$$

FWHM vrijednost izračunala sam za svaki detektor. Ona govori o tome koliko je ukupno vremensko podrhtavanje na svakom od njih. Primjerice, za detektor 0°, FWHM iznosi 1.88 ns, odnosno 1880 ps. Doprinos tom podrhtavanju od strane detektora je tek nekih 140 ps, zbog čega vremensko podrhtavanje mogu praktički u



Slika 4.18: Prikaz histograma i analize vremenskog podrhtavanja za svaki detektor. Na svakoj slici označen je i prozor koincidencije.

potpunosti pripisati laserskim diodama. Na slikama je također vidljivo da fotoni dolaze u očekivanim vremenskim intervalima, sa prozorom koincidencije od 6,5 nm.

5 Rezultati

Na postavu sam za potrebe ovog rada provela deset grupa eksperimenata s različitim postavkama. Također sam prije svakog mjerenja postav kalibrirala na način opisan u ulomku 3.1.4. Svaka grupa mjerenja sastoji se od osam slanja polariziranih fotona, podijeljenih još na po dva za svaku frekvenciju - 1 MHz, 2 MHz, 4 MHz i 8 MHz.

Grupe se razlikuju po jačini gušenja (koja je kontrolirana pomoću ranije spomenutih filtera neutralne gustoće), šumu (koji je pojačavan uključivanjem lampe pored prijamnog uređaja) te broju transmitiranih fotona. U tablici 5.2 prikazane su sve grupe slanja (mjerenja) sa pripadajućim postavkama. Iz tablice je vidljivo da neka od mjerenja sa dodatnim šumom nisu bila uspješna. Razlog tome je što zbog previše šuma algoritam za poravnanje ne uspijeva poravnati nizove. Također, povećanjem šuma smanjuje se broj uspješnih distribucija.

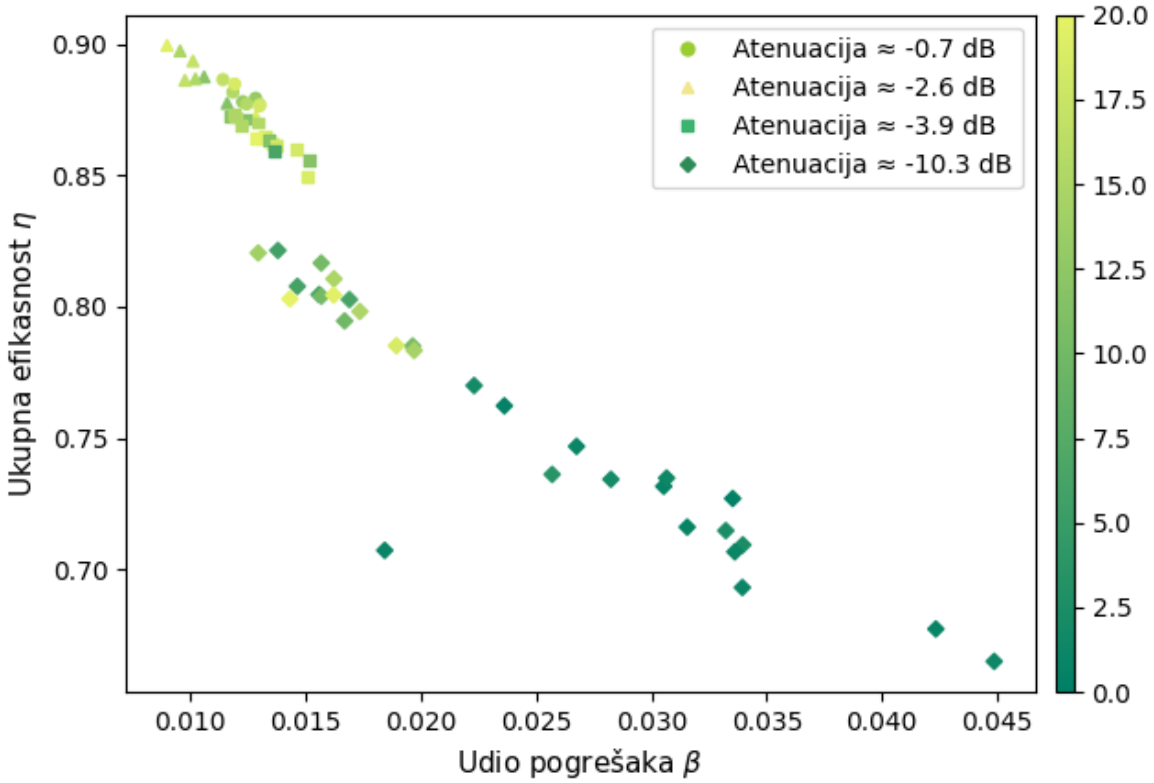
Grupa	Atenuacija	Broj pulseva	Dodatni šum	Uspješne distribucije
1	≈ -2.6 dB	1 milijun	1x	8
2	≈ -10.3 dB	1 milijun	1x	8
3	≈ -10.3 dB	10 milijuna	1x	8
4	≈ -10.3 dB	2 milijuna	10x	5
5	≈ -10.3 dB	2 milijuna	20x	4
6	≈ -10.3 dB	5 milijuna	20x	4
7	≈ -10.3 dB	5 milijuna	40x	2
8	≈ -3.9 dB	2 milijuna	1x	8
9	≈ -3.9 dB	2 milijuna	1x	8
10	≈ -0.7 dB	2 milijuna	1x	8

Tablica 5.2: Prikaz svih grupa mjerenja sa postavkama i brojem uspješnih distribucija.

Za svaku kvantnu distribuciju ključa izračunala sam njenu ukupnu efikasnost η te udio pogrešaka β (eng. *Bit Error Rate, BER*). Visoka ukupna efikasnost pokazuje da se velika količina transmitiranih fotona uspješno detektira i time koristi za generaciju ključa, dok BER ukazuje koliko se precizno detektiraju bitovi kroz protokol. Što je njegova vrijednost manja, ključ dobiven putem distribucije je pouzdaniji. Ova dva parametra ustvari opisuju koliko je distribucija uspješna.

Na slici 5.19 prikazala sam graf ukupne efikasnosti i udjela pogrešaka za sva uspješna mjerenja iz prethodne tablice.

Ukupna efikasnost od približno 90% najveća je za mjerenja s najmanjim udjelom pogrešaka te se smanjuje do oko 70% za mjerenja s najvećim udjelom pogrešaka. Iz prikazanih podataka moglo bi se zaključiti kako ukupna efikasnost ovisi o atenuaciji, odnosno da povećanje atenuacije smanjuje ukupnu efikasnost te ujedno povećava udio pogrešaka. No, efikasnost se zapravo smanjuje (i udio pogrešaka povećava) zbog šuma koji je povećan upravo u mjerenjima sa većom atenuacijom. Ukoliko se zanemare mjerenja sa povećanim šumom vidljivo je da atenuacija ima mali ili nikakav utjecaj na efikasnost te udio pogrešaka. Na udio pogrešaka također utječe i preciznost



Slika 5.19: Prikaz ukupne efikasnosti u ovisnosti o udjelu pogrešaka.

kalibracije polarizacija, koja u ovom slučaju varira između skupina mjerenja, što čini usporedbe između skupina manje preciznima.

Ukratko, iz prikaza je vidljivo da se polarizirani fotoni uspješno šalju i detektiraju putem korištenog postava i telekomunikacijskog optičkog vlakna, u slučaju niskog šuma.

6 Zaključak

Zbog fizikalnih principa na kojima počiva, kvantna distribucija ključa mogla bi pružiti razinu sigurnosti komunikacije koju ne bi mogla ugroziti čak ni kvantna računala. Iz prikazanih rezultata vidljivo je kako se kvantna distribucija ključa može uspješno izvesti putem opisanog postava, gdje su korištenje SPAD detektora i telekomunikacijskog vlakna ključni dijelovi implementacije. Protokol je uspješan za gušenje do 8.3 dB, što odgovara duljini od 2.7 km optičkog vlakna. Uspješno implementiranje telekomunikacijskog vlakna pokazuje da se ono može koristiti za distribuciju ključa na manjim udaljenostima, primjerice unutar zgrade ili manjeg kampusa te pokazuje obećavajuću mogućnost njehovog korištenja i na većim udaljenostima što bi uvelike smanjilo troškove implementacije same kvantne distribucije ključa. Korištenje SPAD detektora također smanjuje troškove implementacije te otvara mogućnost njihovog integriranja na fotoničke čipove. Realizirani postav može se koristiti kao baza za daljni razvoj kvantne distribucije ključa.

Bibliography

[1] Secret Key Exchange (Diffie-Hellman), (15.12.2017.), Computerphile, https://www.youtube.com/watch?v=NmM9HA2MQGI, 17.3.2024.

[2] Stanford Seminar - The Evolution of Public Key Cryptography, (1.3.2018.), Stanford Online, https://www.youtube.com/watch?v=Tev3tVzH91s, 17.3.2024.

[3] Quantum cryptography: basics and technology with Vadim Makarov, (14.11.2014.), Institute for Quantum Computing, https://www.youtube.com/watch?v=wF-BWgnpYmI, 18.3.2024.

[4] The Feynman Lectures on Physics, Volume I, Chapter 33: Polarization, https://www.feynmanlectures.caltech.edu/I_33.html, 12.4.2024.

[5] Wire grid polarizer, (21.4.2006.), Wikipedia, https://en.wikipedia.org/wiki/File:Wire-grid-polarizer.svg, 12.4.2024.

[6] Photons and polarization, UBC Physics & Astronomy: Physics 200 Course https://phas.ubc.ca/~mav/p200/photpol.pdf, 12.4.2024.

[7] Lecture 1: Introduction to Superposition, (18.6.2014.), MIT OpenCourseWare, https://www.youtube.com/watch?v=lZ3bPUKo5zc&list=PLUl4u3cNGP61-9PEhRognw5vryrSEVLPr&index=2, 2.4.2024.

[8] Bennett, C. H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. A. Experimental quantum cryptography, Journal of Cryptology, Vol. 5, (1991), str. 3.-28.

[9] Beam splitter, (1.4.2021.), Wikipedia, https://en.wikipedia.org/wiki/Beam_splitter, 12.4.2024.

[10] FPC560 - Fiber Polarization Controller, 3 Ø56 mm Paddles, No Fiber, Thorlabs, https://www.thorlabs.com/thorproduct.cfm?partnumber=FPC560, 13.4.2024.

[11] Introduction to Waveplates, Newport, https://www.newport.com/n/introduction-to-waveplates, 14.4.2024.

[12] Manual Fiber Polarization Controllers, Thorlabs, https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=343, 13.4.2024.

[13] Feynman, R. P.; Leighton, R. B.; Sands M. The Feynman Lectures on Physics, Vol. I: Mainly Mechanics, Radiation, and Heat. The New Millennium Edition. Sjedinjene Američke Države : Basic Books, 2011.

[14] Optical Fiber Loss and Attenuation, FOSCO., https://www.fiberoptics4sale.com/blogs/archive-posts/95048006-optical-fiber-loss-and-attenuation, 14.4.2024.

[15] Cusini, I.; Berretta, D.; Conca, E.; Incoronato, A.; Madonini, F.; Maurina, A. A.; Nonne, C.; Riccardo, S.; Villa, F., Historical Perspectives, State of art and Research Trends of Single Photon Avalanche Diodes and Their Applications (Part 1: Single Pixels) // Frontiers in Physics. Vol. 10, 2022

[16] Ziarkash, A.; Joshi, S.; Stipčević, M.; Ursin, R. Comparative study of afterpulsing behavior and models in single photon counting avalanche photo diode detectors // Scientific reports. Vol. 8, 2018.