Kvantna kriptografija putem optičkog vlakna

Cerović, Antonio

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
FIZIČKI ODSJEK

Antonio Cerović

Kvantna kriptografija putem optičkog vlakna

Diplomski rad

Zagreb, 2024.

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
FIZIČKI ODSJEK

INTEGRIRANI PREDDIPLOMSKI I DIPLOMSKI SVEUČILIŠNI STUDIJ
FIZIKA; SMJER ISTRAŽIVAČKI

Antonio Cerović

Diplomski rad

Kvantna kriptografija putem optičkog vlakna

Voditelj diplomskog rada: dr. sc. Mario Stipčević

Ocjena diplomskog rada: _____

Povjerenstvo: 1. _____

2. _____

3. _____

Datum polaganja: _____

Zagreb, 2024.

Zahvaljujem se mentoru dr. sc. Mariju Stipčeviću na vodstvu, savjetima, strpljenju i pomoći u protekle dvije i pol godine. Posebno se zahvaljujem svojim roditeljima Claudiji Katrin i Alenu, bratu Mariju i Marijanu na podršci tokom cjelokupnog školovanja. Na kraju, zahvaljujem se Karli te svim svojim prijateljima koji su mi uljepšali studentske dane te ih učinili zabavnima i nezaboravnima.

Sažetak

U današnjem svijetu tehnologije, razvoj kvantnih računala predstavlja prijetnju sadašnjim kriptografskim sustavima. Naime, pomoću Shorovog algoritma, koji bi se u budućnosti mogao izvoditi na kvantnim računalima, moguće je razbiti kriptografske algoritme koji su trenutačno u upotrebi. Kao moguće rješenje problema nameće se kvantna distribucija ključa. Kvantna distribucija ključa služi za dijeljenje tajnog ključa u simetričnoj kriptografiji, a sigurnost iste temelji se na zakonima kvantne fizike. U ovom radu predstavljena je eksperimentalna kvantna distribucija ključa putem konvencionalnog G.652.D telekomunikacijskog optičkog vlakna. Implementacija se temelji na BB84 protokolu i koristi polarizacijska stanja fotona valne duljine 810 nm za prijenos informacije. Za razliku od uobičajenih skupih rješenja, u ovom radu korištene su relativno jeftine optičke komponente za spomenutu valnu duljinu te detektori bazirani na SPAD ćelijama. Dodatno, u našem pristupu pošiljatelj i primatelj ne trebaju imati sinkronizirane satove niti sinkronizirajući signal, već se poravnavanje vrši minimiziranjem udjela pogrešaka. Protokol je uspješno proveden za gubitke do 8.3 dB, što odgovara duljini od 2.7 km G.652.D optičkog vlakna. Također, napravljena je analiza eksperimentalnog postava te ustanovljena učinkovitost provedene kvantne distribucije ključa.

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

Quantum cryptography over an optic fibre

Abstract

In today's world of technology, the development of quantum computers poses a threat to current cryptographic systems. Specifically, with Shor's algorithm, which could be executed on future quantum computers, it becomes possible to break cryptographic algorithms currently in use. As a possible solution to this problem, quantum key distribution emerges. Quantum key distribution is used for sharing a secret key in symmetric cryptography, and its security is based on the laws of quantum physics. This paper presents experimental quantum key distribution via conventional G.652.D telecommunications optical fiber. The implementation is based on the BB84 protocol and utilizes polarization states of photons with a wavelength of 810 nm for information transmission. Unlike conventional, expensive solutions, this setup uses relatively inexpensive optical components for this wavelength and detectors based on SPAD cells. In our approach, the sender and receiver do not need synchronized clocks or a synchronizing signal; alignment is achieved by minimizing error rates. The protocol was successfully implemented for losses up to 8.3 dB, corresponding to a length of 2.7 km of G.652.D optical fiber. Furthermore, an analysis of the experimental setup was conducted, and the effectiveness of the implemented quantum key distribution was established.

Keywords: quantum key distribution, quantum cryptography, BB84 protocol

Sadržaj

1 Uvod

Kvantna računala su već neko vrijeme vrlo aktualna tema znanstvenih istraživanja. U posljednih nekoliko godina razvoj istih se ubrzao te trenutačni napredak djeluje obećavajuće za budućnost. Iako su današnja kvantna računala još uvijek u fazi razvoja te trenutno nemaju primjenu, u budućnosti predstavljaju prijetnju standardnim kriptografskim sustavima. Svi trenutni kriptografski sustavi temelje se na teškim matematičkim problemima za čije je rješavanje potrebna velika računalna snaga. Najpoznatiji algoritam koji se koristi za kodiranje komunikacije na internetu je RSA (eng. *Rivest-Shamir-Adleman*). Sigurnost RSA algoritma temelji se na težini faktoriziranja produkta dva velika prosta broja. Trenutno najjačim računalima trebalo bi milijune godina za razbijanje RSA algoritma.

S druge strane, kvantna računala obećavaju faktoriziranje brojeva u mnogo kraćem vremenu. Algoritam za faktoriziranje je razvio američki matematičar Peter Shor već davne 1994. godine. Na sreću, kvantna računala trenutno nemaju dovoljno qubita kako bi se pomoću Shorovog algoritma razbio RSA algoritam, no to ne znači da će i u budućnosti biti tako. Razvoj kvantnih računala napreduje poprilično brzo zbog čega je potrebno poduzeti potrebne mjere kako bi komunikacija bila sigurna i nakon pojave korisnih kvantnih računala. Već se neko vrijeme radi na budućim sigurnosnim rješenjima te postoje dva smjera kojim se pokušava riješiti problem sigurne komunikacije.

Jedno rješenje je takozvana post-kvantna kriptografija, a drugo kvantna kriptografija, odnosno kvantna distribucija ključa. Post-kvantna kriptografija temelji se na matematičkim problemima za koje se vjeruje da se ne mogu riješiti niti pomoću kvantnih računala u razumnom vremenskom periodu, dok se kvantna distribucija ključa temelji na zakonima kvantne mehanike. Obje vrste sigurnosnih sustava imaju svoje prednosti i mane, pa se tako za post-kvantnu kriptografiju ne zna sa sigurnošću je li otporna na moguće buduće vrste napada. S druge strane, post-kvantna kriptografija se može bez puno muke implementirati u postojeće sigurnosne sustave. Sigurnost kvantne distribucije ključa garantiraju zakoni kvantne mehanike, ali praktično izvođenje i implementacija nisu jednostavne. Također, post-kvantna kriptografija bi zamijenila RSA algoritam u asimetričnoj kriptografiji, dok kvantna distribucija ključa služi za sigurnu distribuciju tajnog ključa u simetričnoj kriptografiji. Odluka o

tome koji način kriptografije je bolji ovisi o specifičnoj primjeni, odnosno specifičnom slučaju.

Ovaj se rad bavi eksperimentalnom implementacijom kvantne distribucije ključa. Iako se kvantna distribucija ključa uglavnom poistovjećuje sa skupom opremom i laboratorijskim uvjetima, u ovom radu je razvijen relativno jeftin sustav koji ima potencijal implementacije u postojeću telekomunikacijsku mrežu optičkih vlakana. U nastavku rada opisati će se teorija korištenog protokola u poglavlju *Kvantna distribucija ključa*, a potom i eksperimentalna izvedba u poglavlju *Eksperimentalni postav*. Zatim će se okarakterizirati postav u poglavlju *Karakterizacija postava* te prezentirati rezultati u poglavlju *Rezultati*. Za kraj, zaključna riječ nalazi se u poglavlju *Zaključak*.

2 Kvantna distribucija ključa

Kvantna distribucija ključa je protokol kojim dvije strane koje žele zaštititi međusobnu komunikaciju putem interneta uspostavljaju, odnosno povećavaju, tajni ključ. Uspostavljeni tajni ključ koristi se za šifriranje komunikacije između te dvije strane već poznatim metodama klasične simetrične kriptografije. Kvantna distribucija ključa, kako joj ime sugerira, temelji se na zakonima kvantne fizike koji onemogućavaju neprimjetno prisluškivanje za vrijeme distribucije ključa. Ovakav protokol moguće je rješenje problema uspostave tajnog ključa u simetričnoj kriptografiji.

Ideju su prvi predstavili Charles H. Bennet i Gilles Brassard 1984. godine u radu pod naslovom "Quantum cryptography: Public key distribution and coin tossing" [1]. Oni predlažu kodiranje bitova u linearno polarizirane pojedinačne fotone polarizacija $0°$, $45°$, $90°$ i $135°$ te slanje tako polariziranih fotona kroz kvantni komunikacijski kanal. Ovakvim načinom komunikacije onemogućuje se neopaženo prisluškivanje treće osobe koja ne posjeduje znanje o načinu kodiranja informacija. Također, špijun ne može saznati niti dio poslane informacije bez da nasumično i nepovratno izmijeni polarizaciju, što dovodi do otkrivanja pokušaja prisluškivanja.

2.1 Polarizacija

U kontekstu klasične fizike, polarizacija se definira kao smjer titranja čestica u transverzalnom valu. Kod elektromagnetskih valova, odnosno svijetlosti, polarizacija je definirana kao smjer titranja električnog polja. Razlikujemo linearnu i cirkularnu polarizaciju.

U kvantnoj mehanici su elektromagnetski valovi opisani kao mnoštvo fotona, a foton je kvant elektromagnetskog zračenja. Svaki pojedini foton ima definiranu polarizaciju. Polarizacija je, u kontekstu kvantne fizike, kvantno stanje koje se može prikazati vektorima stanja u dvodimenzionalnom Hilbertovom prostoru. Isti je detaljnije opisan u dodatku A.1. Zapis nekog vektor stanja polarizacije $|p\rangle$, u ortogonalnoj bazi $|b_1\rangle$, $|b_2\rangle$ Hilbertovog prostora je

$$|p\rangle = c_1|b_1\rangle + c_2|b_2\rangle, \tag{2.1}$$

gdje su $c_1 = \langle b_1|p\rangle$ i $c_2 = \langle b_2|p\rangle$ definirani kao skalarni produkt pripadnog vektora

baze i vektora $|p\rangle$. Koeficijenti c_1 i c_2 zovu se amplitude vjerojatnosti, a kvadrati njihovih apsolutnih vrijednosti $|c_1|^2$ i $|c_2|^2$ su vjerojatnosti da će se sustav nakon mjerenja naći u stanju $|b_1\rangle$ ili $|b_2\rangle$. Iz prethodnog zapisa vektora (2.1) može se naslutiti svojstvo kvantne superpozicije A.2. Princip superpozicije kaže da ako neki kvantni sustav može biti u bilo kojem od n stanja, onda može biti i u bilo kojoj linearnoj kombinaciji (superpoziciji) tih n stanja. Svojstvo superpozicije, uz princip neodređenosti, ima ključnu ulogu u sigurnosti predloženog protokola.

Princip neodređenosti kaže da ako znamo vrijednost jedne od dvije konjugirane varijable, onda ne znamo ništa o drugoj varijabli. Na sličan način može se definirati neodređenost u smislu konjugiranih baza. Dvije ortonormirane baze $\{|a_i\rangle\}$, $i \in [1, n]$ te $\{|b_j\rangle\}$, $j \in [1, n]$ su konjugirane ako vrijedi

$$|\langle a_i|b_j\rangle|^2 = \frac{1}{2}, \quad \forall i, j \in [1, n]. \tag{2.2}$$

Drugim riječima, ako je sustav u stanju $|a_i\rangle$ onda postoji jednaka vjerojatnost da će biti nađen u nekom od stanja $|b_j\rangle$. Ovakvo svojstvo imaju baze $\{0°, 90°\}$ te $\{45°, 135°\}$ koje se mogu sastaviti iz skupa predloženih polarizacija.

2.2 Komunikacija putem kvantnog kanala

Predložena kvantna distribucija ključa u radu [1] može se podijeliti na dva dijela, koja se razlikuju prema tipu komunikacijskog kanala. Prvi dio protokola odvija se putem kvantnog kanala kroz koji se šalju polarizirani fotoni. Po završetku transmisije, pošiljatelj i primatelj moraju obraditi informacije poslane kroz kvantni kanal, što se odvija kroz klasični kanal. Standardno, pošiljatelju se daje ime Alice, primatelju Bob, a treća osoba koja prisluškuje zove se Eve. Navedena imena će se također koristiti u nastavku ovog rada.

Kvantnu distribuciju ključa započinje Alice generiranjem slučajnog binarnog niza nula i jedinica. Taj niz se potom kodira u linearne polarizacije fotona od $0°$, $45°$, $90°$ i $135°$. Navedene polarizacije čine dvije ortogonalne baze dvodimenzionalnog Hilbertovog prostora. Baze su $\{0°, 90°\}$, odnosno vertikalna baza, te $\{45°, 135°\}$, odnosno dijagonalna baza. Te baze su međusobno zakrenute za $45°$ što znači da čine konjugirane baze. U svakoj od dviju baza moguće je jednu od polarizacija poistovjetiti sa bitom 0, a drugu s bitom 1, što daje recept za kodiranje niza bitova u niz linearno

polariziranih fotona. Konkretan recept kodiranja nije bitan, već je bitno da Alice i Bob kodiranje ili dekodiranje izvode na isti način, odnosno imaju isti recept. Može se primijetiti da recept ima dvije moguće polarizacije za svaki bit, koje ujedno pripadaju različitim ortogonalnim bazama. To znači da je za kodiranje potreban i niz baza u kojima se bitovi kodiraju. Odabir niza baza za kodiranje slučajnog niza bitova također mora biti nasumičan. Ukratko, generiranje slučajnog niza bitova te kodiranje istih u slučajno izabrane baze je identično generiranju slučajnog niza polarizacija. Po završetku kodiranja, Alice šalje niz linearno polariziranih fotona kroz optičko vlakno, gdje svaki foton odgovara pojedinom bitu.

Bob s druge strane dekodira jedan po jedan foton. Za svaki foton nasumično izabire bazu u kojoj želi izmjeriti njegovu polarizaciju. U ovisnosti o odabiru baze i polarizaciji fotona, postoje dva različita slučaja mjerenja. U slučaju da Bob izabere bazu kojoj pripada polarizacija fotona, odnosno istu bazu u kojoj je Alice kodirala foton, on će izmjeriti točnu polarizaciju. Za primjer se može uzeti baza $\{0°, 90°\}$ i foton polarizacije $90°$. Polarizacija fotona može se zapisati kao

$$|90°\rangle = c_1|0°\rangle + c_2|90°\rangle, \tag{2.3}$$

iz čega se direktno vidi da su amplitude vjerojatnosti $c_1 = 0$ te $c_2 = 1$. S obzirom na to da kvadrat apsolutne vrijednosti amplitude daje vjerojatnost da će rezultat mjerenja biti pripadna polarizacija, iz priloženog primjera je očito da će Bob sa stopostotnom vjerojatnošću izmjeriti polarizaciju fotona od $90°$.

S druge strane, ako Bob izabere bazu kojoj polarizacija fotona ne pripada, odnosno suprotnu bazu od one u kojoj je Alice kodirala, rezultat mjerenja biti će slučajan. Kao primjer može se uzeti baza $\{0°, 90°\}$ i foton polarizacije $45°$. Bob će u 50% slučajeva izmjeriti polarizaciju od $0°$, dok će u drugih 50% slučajeva izmjeriti polarizaciju od $90°$. Matematički se to može zapisati na način

$$|45°\rangle = c_1|0°\rangle + c_2|90°\rangle, \tag{2.4}$$

gdje su $c_1 = \cos 45° = \frac{1}{\sqrt{2}}$ te $c_2 = \sin 45° = \frac{1}{\sqrt{2}}$. Iznos amplituda vjerojatnosti može se jednostavno iščitati iz trigonometrijske kružnice. Vjerojatnost mjerenja bilo koje od polarizacija $|0°\rangle$ ili $|90°\rangle$ je 50%. Također treba uočiti da izmjerena polarizacija u tom slučaju nikad neće biti jednaka originalnoj.

Alicein niz bitova	1	0	0	0	1	1	0	1	0	1	0	1
Alicein niz baza	D	D	R	D	R	R	R	D	D	R	R	D
Aliceine polarizacije	↘	↗	↔	↗	↕	↕	↔	↘	↗	↕	↔	↘
Bobov niz baza	R	D	R	D	D	R	D	R	D	R	D	R
Bobove polarizacije	↕	↗	↔	↗	↗	↕	↗	↔	↗	↕	↘	↕
Bobov niz bitova	1	0	0	0	0	1	0	0	0	1	1	1

Tablica 2.1: Primjer komunikacije između Alice i Boba putem kvantnog kanala. Baza označena sa slovom R je vertikalna (eng. *rectilinear*), a slovom D dijagonalna (eng. *diagonal*).

Primjer komunikacije putem kvantnog kanala dan je tablicom 2.1. Tablica je napravljena redoslijedom kako teče komunikacija. Za početak, Alice nasumično generira nizove bitova i baza, te bitove kodira u odgovarajuće polarizacije fotona unutar izabrane baze. Bob potom nasumično generira niz baza te mjeri polarizacije dolaznih fotona u istima. U slučaju da Bob izabere istu bazu kao i Alice, vidi se da je mjerenje točno, dok je u suprotnom krivo i slučajno. Očito, ovakvi nizovi nisu jednaki jer je u 50% slučajeva Bob izabrao krivu bazu. Pošto je mjerenje u krivoj bazi nasumično, niz koji je poslala Alice i onaj koji je izmjerio Bob razlikovati će se u 25% bitova, što je vidljivo u tablici 2.1. Kako bi nizovi postali jednaki, Alice i Bob će zadržati samo one bitove čije je polarizacije Bob mjerio u istoj bazi kao i Alice. Postupak odbacivanja bitova izmjerenih u krivoj bazi izvodi se u drugom dijelu protokola koji se odvija putem klasičnog komunikacijskog kanala.

Iz prethodnog opisa Bobovog mjerenja polarizacije fotona jasno se vidi prednost ovog protokola koja počiva na principima superpozicije i neodređenosti. Kada bi Eve htjela prisluškivati komunikaciju morala bi nekako izmjeriti polarizaciju fotona. S obzirom da Eve, kao ni Bob, ne zna točnu bazu u kojoj je foton polariziran, mora ju nasumično izabrati. To znači da je proces Eveinog mjerenja jednak Bobovom. Pošto Alice i Bob na kraju odbacuju sve bitove u kojima je Bob mjerio u krivoj bazi, promotriti ćemo samo slučaj u kojem Bob mjeri u točnoj bazi. Eve nasumično bira bazu u kojoj će odraditi mjerenje polarizacije te u 50% slučajeva izabere krivu bazu, odnosno izmjeri krivu polarizaciju. Potom Eve prosljeđuje Bobu foton izmjerene polarizacije. Bob s druge strane mjeri polarizacije fotona u točnoj bazi te će ishod njegovog mjerenja ovisiti o Eveinom odabiru baze. U slučaju da Eve mjeri u krivoj bazi, različitoj od Alice i Boba, Bob će sa 50% vjerojatnosti izmjeriti točnu, odnosno krivu polarizaciju.

To znači da će na kraju Bob imati 25% bitova različito od Alice, iako je cijelo vrijeme mjerio u točnoj bazi te bi svi bitovi trebali biti jednaki. Na taj će način Alice i Bob otkriti prisluškivanje od strane Eve.

2.3 Komunikacija putem klasičnog kanala

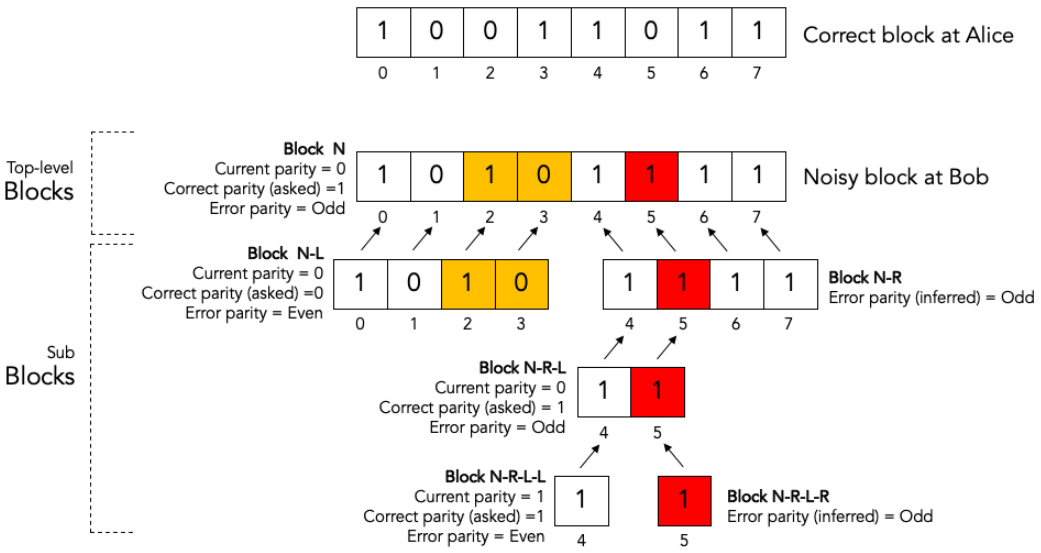
Komunikacija putem klasičnog kanala služi za obradu informacija poslanih putem kvantnog kanala. Ova komunikacija mora biti autentificirana, ali ne mora biti šifrirana. To znači da Eve može vidjeti sve informacije koje Alice i Bob međusobno izmjenjuju, ali ne može mijenjati poruke. Da bi to bilo moguće, Alice i Bob moraju imati prethodno definiran zajednički tajni ključ kojim će autentificirati poruke.

Ovaj dio protokola započinje nakon transmisije putem kvantnog kanala. Kao što je već spomenuto, Alice i Bob trebaju odbaciti sve bitove koje je Bob izmjerio u krivoj bazi. To se odvije na način da Bob navede redoslijed baza u kojima je mjerio, a Alice vraća informaciju o tome koje su od njih točne, a koje krive. Nakon toga, oboje znaju koje bitove treba odbaciti.

Do sada se podrazumijevalo da Alice i Bob posjeduju savršene izvore pojedinačnih fotona, odnosno savršene detektore sa stopostotnom efikasnosti te nisu uzeti u obzir gubitci u kvantnom kanalu. Dodatno, nije uzeto u obzir prisluškivanje. U realnom slučaju, dakako, nije sve tako jednostavno. Oprema nije savršena, nema savršenih izvora pojedinačnih fotona niti detektora sa stopostotnom efikasnosti, postoje gubitci u kvantnom kanalu, a također može biti i prisluškivanja. Sve to unosi dodatne komplikacije u obliku pulseva koji sadrže više od jednog fotona, nedetektiranih fotona te pojava pogrešaka kod mjerenja čak i kada se mjeri u točnoj bazi. Problem nedetektiranih fotona moguće je na jednostavan način riješiti i to tako da Alice odbaci sve bitove koja je poslala, a koje Bob nije detektirao. O problemu nesavršenih izvora pojedinačnih fotona bit će više govora u poglavlju 2.4.2, a postupak ispravljanja pogrešaka je detaljno objašnjen u poglavlju 2.3.1. Nakon ispravljanja svih pogrešaka, ključ i dalje nije potpuno tajan već Eve može imati neke informacije o njemu. Da bi ključ bio potpuno tajan potrebno je žrtvovati dio niza bitova kako bi se Eveino znanje o ključu smanjilo na tek mali dio jednog bita. Pojačavanje privatnosti bit će objašnjeno u poglavlju 2.3.2. Tek nakon pojačavanja privatnosti moguće je reći da je niz tajan te se može koristiti kao tajni ključ u kontekstu simetrične kriptografije.

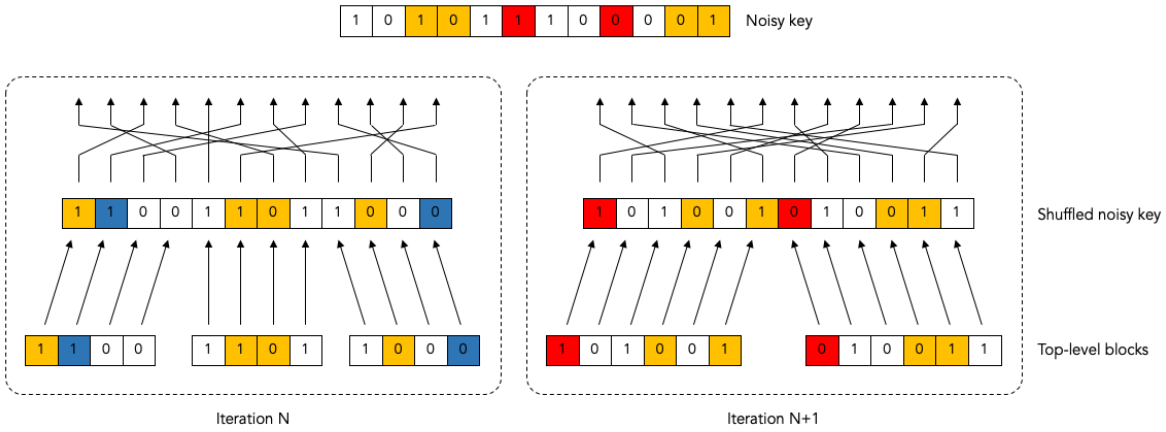
2.3.1 Ispravljanje pogrešaka

Jedan od algoritama koji je predložen za ispravljanje pogrešaka zove se Cascade. Modificirana verzija tog algoritma koristiti će se i u ovom radu pa će se njegov princip rada pobliže razmotriti. Cascade algoritam prvi put je predložen u radu "Secret-Key Reconciliation by Public Discussion" [2], a temelji se na otkrivanju i ispravljanju pogrešaka uspoređivanjem pariteta podnizova. Algoritam započinje tako da Bob podijeli niz bitova, koji se dobije nakon odbacivanja svih bitova izmjerenih u krivoj bazi te onih koje Bob nije detektirao, na n blokova jednake dužine. Svakom bloku potom izračuna paritet, koji se definira kao ostatak pri cjelobrojnom dijeljenju zbroja vrijednosti svih bitova sa brojem dva. Drugim riječima, ako je broj jedinica u bloku paran, paritet će biti nula, dok će u suprotnom biti jedan. Informacije o paritetu blokova šalju se putem klasičnog kanala prema Alice. Alice potom dijeli svoj niz bitova na isti način na n jednakih blokova te im računa paritete. Po završetku istoga, Alice daje do znanja Bobu u kojim blokovima imaju jednake paritete, a u kojima imaju različite. U blokovima za koje Alice i Bob izračunaju jednake paritete ne postoje pogreške ili postoji paran broj pogrešaka. U suprotnom, ako su pariteti različiti, dotični blok sadrži neparan broj pogrešaka.



Slika 2.1: Slika postupka binarnog pretraživanja u kontekstu algoritma Cascade. Sa "Top-level Blocks" označeni su blokovi koji nastaju inicijalnom podjelom niza bitova. Ako za takav blok Alice i Bob izračunaju različiti paritet, kreće se u binarno pretraživanje pogreške koja je označena crvenom bojom. Blokovi u binarnom pretraživanju označeni su sa "Sub Blocks". Svaki sljedeći red označava sljedeću podjelu. Žutom bojom označene su pogreške koje neće biti ispravljene u ovom krugu. Preuzeto sa [3].

Blokove u kojima su pariteti jednaki na trenutak će se zanemariti, te će se prionuti na ispravljanje pogrešaka u blokovima sa različitim paritetima. Alice i Bob koriste binarno pretraživanje kako bi locirali i ispravili pogrešku na način prikazan slikom 2.1. Proces se sastoji od dva koraka. Prvi korak je dijeljenje bloka na dva jednaka dijela te izračunavanje njihovih pariteta. U drugom koraku Alice i Bob otkrivaju svoje paritete te odabiru blok u kojem su izračunati pariteti različiti, nakon čega se vraćaju na prvi korak sa novim blokom dvostruko manje veličine. Postupak ponavljaju sve dok ne dođu do bloka veličine jednog bita te taj bit isprave. Ovakvim postupkom moguće je ispraviti samo jednu pogrešku u pojedinom bloku nakon čega pariteti Aliceinog i Bobovog bloka postaju jednaki.



Slika 2.2: Slika pojave kaskada između konfiguracije N i N+1 koje su dobivene miješanjem. Žutom bojom označene su pogreške koje neće biti ispravljene u konfiguraciji N+1, dok su crvenom prikazane pogreške koje će biti ispravljene. Plavom bojom prikazani su isti bitovi u konfiguraciji N koji su prikazani crvenom bojom u konfiguraciji N+1. Očito je da se ispravljanjem tih bitova u konfiguraciji N+1 otkrivaju pogreške, odnosno blokovi različitih pariteta, u prethodnoj konfiguraciji N. Preuzeto sa [3].

Dakako, ovaj postupak nije dovoljan jer treba ispraviti i potencijalne pogreške u blokovima sa istim paritetima. Rješenje za to je nasumično miješanje bitova te ponavljanje dosad opisanog postupka. Treba imati na umu da će nakon prvog kruga ispravljanja pogrešaka Alice i Bob imati jednake paritete u svim blokovima. Nasumično miješanje služi tome da se u sljedećem krugu blokovi formiraju od različitih bitova u odnosu na prethodni krug te postoji velika mogućnost da će novi blokovi imati različite paritete kod Alice i Boba. U idealnom slučaju, svaki blok bi sadržavao samo jednu pogrešku, što u stvarnosti naravno neće biti slučaj pa će se postupak miješanja ponavljati nekoliko puta. Na kraju drugog, odnosno k-tog kruga postoji

dodatan postupak ispravljanja pogrešaka koji nije moguć jedino u prvom krugu. Naime, ispravljanjem pogrešaka u drugom krugu može se dogoditi da Aliceina i Bobova konfiguracija blokova iz prvog kruga više nema iste paritete, što znači da su otkrivene nove pogreške koje je moguće ispraviti. Primjer tog slučaja dan je slikom 2.2. Ova pojava nazvana je efektom kaskada, otkuda je i sam algoritam dobio svoj naziv. Sada je potrebno vratiti se na konfiguraciju iz prvog kruga te ponoviti postupak ispravljanja pogrešaka. Dakako, ovaj postupak ponovno utječe na konfiguraciju blokova u drugom krugu pa je moguće ponovno otkrivanje novih pogrešaka koje se prije nisu vidjele. Postupak ispravljanja pogrešaka potrebno je iterativno provoditi u oba kruga sve dok ne ponestane vidljivih pogrešaka, odnosno blokova različitih pariteta, koje je moguće ispraviti. Tek se tada niz bitova ponovno može izmiješati te se cijeli postupak ponavlja. U originalnoj verziji Cascade algoritma, bitovi se miješaju ukupno četiri puta nakon čega se proglašava da su Alicein i Bobov niz bitova jednaki sa određenom vjerojatnošću.

2.3.2 Pojačavanje privatnosti

Posljednji korak koji slijedi nakon ispravljanja pogrešaka je pojačavanje privatnosti. Ideja pojačavanja sigurnosti je minimiziranje informacije koju posjeduje Eve tako da se ključ dobiven nakon ispravljanja pogrešaka smanji za određeni dio. Alice i Bob žele javno izabrati kompresijsku funkciju $g(W)$, gdje je W slučajna varijabla niza bitova nakon ispravljanja pogrešaka, tako da Eve posjeduje minimalno informacija o dobivenom ključu $K = g(W)$. Funkcija koju Alice i Bob javno biraju mora biti iz klase univerzalnih$_2$ hash funkcija. Za univerzalnu$_2$ klasu hash funkcija G iz skupa W u skup K vrijedi da je vjerojatnost preslikavanja dva različita niza iz W u dva ista niza iz K nakon što se nasumično odabere funkcija g najviše $\frac{1}{m}$, gdje je m broj nizova u skupu K [4], [5].

Krajnja duljina tajnog ključa dana je relacijom $r = n - l - t - s$, gdje je r krajnja duljina ključa, n duljina niza bitova nakon ispravljanja pogrešaka, l maksimalni broj bitova koje je Eve sakupila tijekom transmisije fotona, t broj otkrivenih pariteta tijekom ispravljanja pogrešaka te s sigurnosni faktor. Ovim postupkom smanjuje se informacija koju Eve ima o ključu na samo $\frac{2^{-s}}{\ln 2}$ bitova [6], [7], [8].

2.4 Prisluškivanje

Za kraj ovog opisa, predstavit ćemo dva napada na ovaj protokol. Ovi napadi pojašnjeni su također u radu ”Experimental Quantum Cryptography” [9]. Radi se o napadima ”Presretni i pošalji” te ”Dijeljenje snopa”.

2.4.1 Presretni i pošalji

U napadu pod nazivom ”Presretni i pošalji” Eve presretne polarizirani foton koji je Alice poslala prije nego što dođe do Boba te mu izmjeri polarizaciju. S obzirom na to da Eve, kao ni Bob, ne zna točnu bazu u kojoj mora izmjeriti polarizaciju, mora ju izabrati nasumično. Nakon što izmjeri polarizaciju fotona, Eve generira novi foton iste takve polarizacije te ga pošalje Bobu. Pošto je bazu birala nasumično, u 50% slučajeva će izmjeriti krivu polarizaciju. U slučaju da je Eve polarizaciju fotona izmjerila u krivoj bazi, a Bob potom u točnoj bazi, odnosno istoj bazi kao i Alice, on će imati krivo izmjerenu polarizaciju u 50% slučajeva. To znači da će Bob u slučaju mjerenja u točnoj bazi umjesto 100% točno imati tek 75% točno i 25% pogrešno izmjerenih polarizacija fotona. Odmah je jasno da će u slučaju čestog prisluškivanja Alice i Bob primijetiti veliki broj pogrešaka te posumnjati na prisluškivanje. Maksimalan broj bitova koje Eve može saznati iz ovakvog napada je

$$l = 2\sqrt{2}n\beta + 5\sqrt{(4 + 2\sqrt{2})n\beta}, \tag{2.5}$$

gdje je n duljina niza, a β udio pogrešaka. Drugi pribrojnik predstavlja sigurnosni dodatak od 5σ, gdje je σ standardna devijacija.

2.4.2 Dijeljenje snopa

Drugi način prisluškivanja je dijeljenje snopa te mjerenje samo jednog dijela, dok drugi dio ostaje netaknut. Štoviše, u teoriji Eve može sačuvati sakupljene fotone te ih izmjeriti tek u trenutku kada su točne baze javno objavljene putem klasičnog komunikacijskog kanala. Ovo je teško izvedivo u praksi pa se neće razmatrati. Ova vrsta napada je posljedica načina pripremanja fotona, odnosno pulsa. Puno je lakše generirati koherentni puls koji može sadržavati više fotona nego puls koji sadrži samo jedan foton. Broj fotona u koherentnom pulsu dan je Poissonovom raspodjelom prema formuli

$$P(f) = \frac{\mu^f e^{-\mu}}{f!}, \tag{2.6}$$

gdje je f broj fotona, a μ prosječan broj fotona u pulsu. S obzirom na to da je ovakav napad moguć jedino u slučaju kada se puls sastoji od dva ili više fotona, cilj je smanjiti postotak takvih pulseva. Postotak pulseva sa dva ili više fotona jednak je

$$P(f \geq 2) = 1 - P(f = 0) - P(f = 1) = 1 - (1 + \mu)e^{-\mu}. \tag{2.7}$$

Iz prethodne formule jasno se vidi da se oslabljivanjem intenziteta pulsa smanjuje i učinkovitost ovakvog napada. Također, smanjuje se i broj pulseva koji sadrže jedan foton, a kojih želimo da bude čim više, tako da je potrebno pronaći kompromis između te dvije krajnosti. Maksimalan broj bitova koje Eve može saznati iz ovakvog napada je

$$l = n\mu + 5\sqrt{n\mu(1-\mu)}, \tag{2.8}$$

gdje je n broj bitova izmjerenih u točnoj bazi, a μ prosječan broj fotona u pulsu. Drugi pribrojnik predstavlja dodatak od 5σ, gdje je σ standardna devijacija.

Kombiniranjem oba napada, Eve može maksimalno saznati

$$l = n\left(\mu + 2\sqrt{2}\beta\right) + 5\sqrt{n\left[\mu(1-\mu) + (4+2\sqrt{2})\beta\right]} \tag{2.9}$$

bitova [9].

3 Eksperimentalni postav

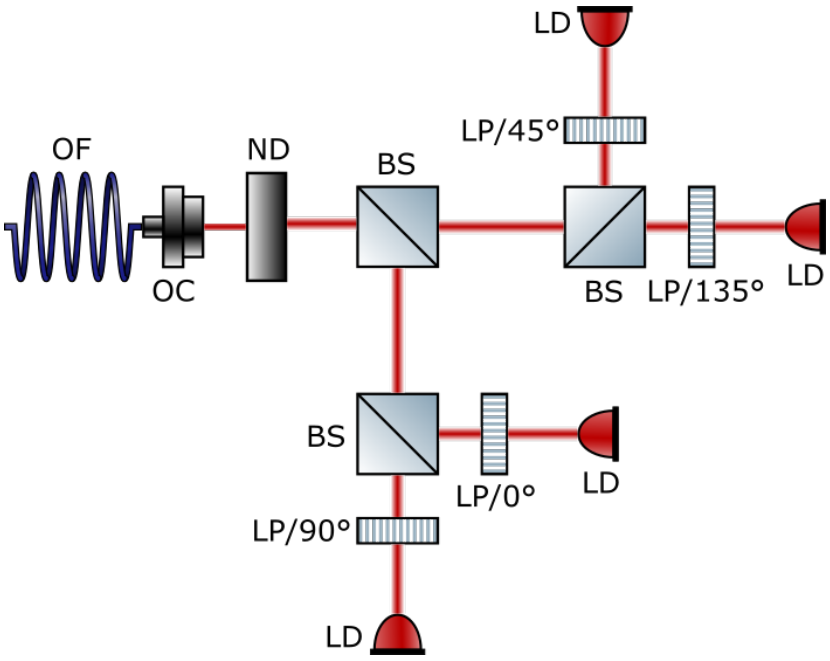
Naša implementacija kvantne distribucije ključa temelji se na BB84 protokolu objašnjenom u prethodnom poglavlju. Za prijenos informacije koriste se polarizacijska stanja fotona. Eksperimentalni postav sastoji se od hardvera i softvera. Pod hardver spadaju predajni i prijamni uređaj, optičko vlakno, kontroler polarizacije, uređaj za snimanje vremena detekcije te dva računala. Softver se sastoji od algoritma za poravnavanje nizova, algoritma za ispravljanje pogrešaka, algoritma za pojačavanje privatnosti tajnog ključa te dodatnih algoritama za kalibraciju. Uređaji koji spadaju u hardver, izuzev računala, potrebni su za generiranje, prijenos i detekciju polariziranih fotona putem kvantnog kanala. S druge strane, računala i popratni algoritmi za obradu poslane informacije putem kvantnog kanala su korišteni u drugom dijelu protokola gdje se komunikacija odvija putem klasičnog kanala.

3.1 Hardver

3.1.1 Predajnik

Predajnik, čija je shema prikazana slikom 3.1, je uređaj koji generira slučajan niz bitova, kodira ih u polarizacije fotona te ih potom odašilje. Uređaj smo sastavili na malom prijenosnom optičkom stolu, a sastoji se od optičkih i optomehaničkih komponenti te popratne kontrolne elektronike. Izvori polariziranih fotona izvedeni su pomoću četiri laserske diode valne duljine 810 nm. Svaka dioda postavljena je na kinematičko postolje sa dva stupnja slobode pomoću kojeg se može podešavati smjer propagacije fotona. Na svako postolje također je postavljen i polarizator, koji služi za podešavanje polarizacije pojedine diode. Polarizatore smo konfigurirali tako da svaka dioda odašilje jednu od sljedećih polarizacija: $0°$, $45°$, $90°$ i $135°$. Redoslijed slanja pulseva određuje kvantni generator nasumičnih brojeva koji se bazira na registru pomaka s linearnom povratnom spregom LSFR (eng. *Linear-feedback shift register*). Kvantni generator slučajnih brojeva generira nasumični niz bitova koji se, kao što je ranije objašnjeno, kodira u polarizacijska stanja fotona, odnosno u redoslijed okidanja laserskih dioda. Uređaj može slati pulseve frekvencijom do 8 MHz. Laserske diode same po sebi ne mogu emitirati samo jedan foton, već emitiraju koherentni puls koji ne mora sadržavati samo jedan foton, što je već objašnjeno u poglavlju 2.4.2. Iz tog

razloga potrebno je prigušiti intenzitet pulsa kako bi se emitirao u prosjeku 0.1 foton po pulsu. Način na koji se to radi objasniti će se u poglavlju 3.1.4.



Slika 3.1: Shema predajnika. Korištene kratice su: BS - nepolarizirajući razdjelnik snopa (eng. *beam splitter*), LD - laserska dioda (eng. *laser diode*), LP - linearni polarizator (eng. *linear polarizer*), OF - optičko vlakno (eng. *optical fiber*), OC - konektor za optičko vlakno (eng. *optical coupler*), ND - filter neutralne gustoće (eng. *neutral density filter*).

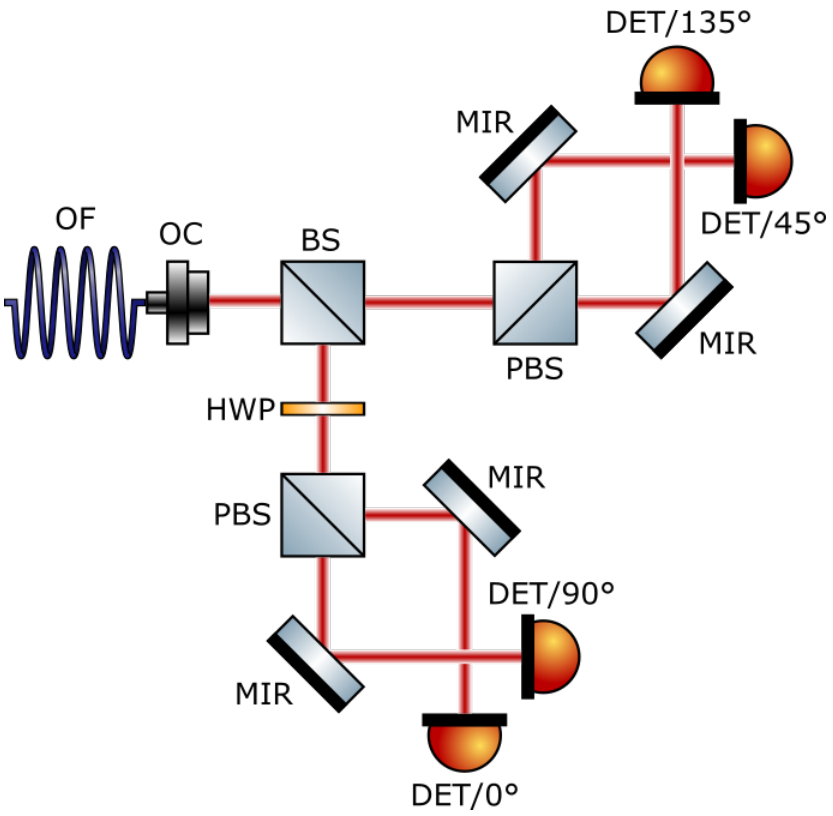
Nakon polariziranja fotona, zrake se spajaju u jednu pomoću seta od tri $50:50$ kockasta nepolarizirajuća razdjelnika snopa (eng. *nonpolarizing beamsplitter cube*) proizvođača Thorlabs, model BS011. Svaki takav razdjelnik snopa dijeli zraku na dvije okomite zrake jednakih intenziteta od kojih je jedna dobivena transmisijom, a druga refleksijom. Stoga se na svakom nepolarizirajućem razdjelniku snopa gubi 50% intenziteta zrake. Konačna zraka sastoji se od četiri različito polarizirane zrake od kojih svaka ima intenzitet jednak četvrtini početnog intenziteta. Spojena zraka potom prolazi kroz filter neutralne gustoće (eng. *neutral density filter*) koji joj dodatno smanjuje intenzitet te ulazi u 780HP jednomodno optičko vlakno. Filter neutralne gustoće također doprinosi realizaciji od u prosjeku 0.1 fotona po pulsu. Drugi razlog postavljanja filtera je simulacija gubitaka u vlaknu između prijamnog i predajnog uređaja. Variranjem filtera različitih jačina gušenja moguće je simulirati različita gušenja u optičkom vlaknu, što je potom moguće povezati i sa dužinom optičkog vlakna, odnosno udaljenošću između prijamnika i predajnika. Na slici 3.2 prikazan je predajni uređaj koji je izgrađen na Institutu Ruđer Bošković.

Slika 3.2: Predajni uređaja korištenog u eksperimentu. Uređaj je izgrađen na Institutu Ruđer Bošković.

3.1.2 Prijamnik

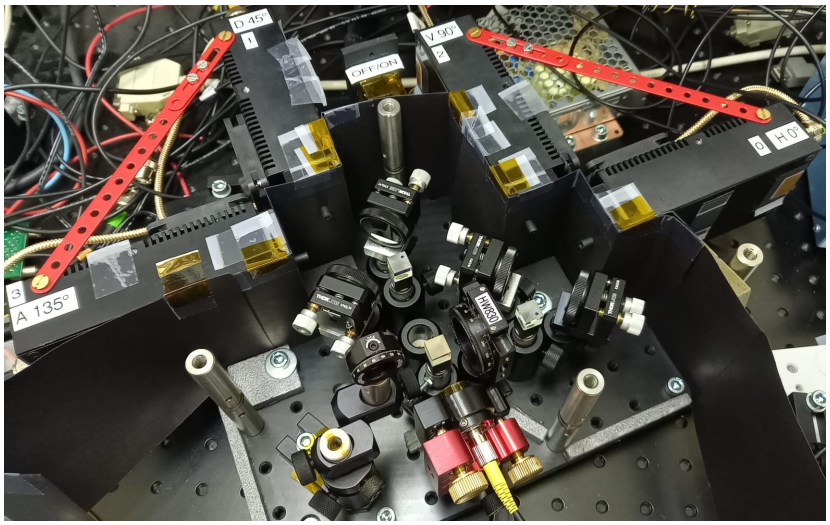
Prijamni uređaj, čija je shema prikazana na slici 3.3, je uređaj koji mjeri polarizacije poslanih fotona. Kao i predajnik, ovaj uređaj smo izgradili na malom prijenosnom optičkom stolu. Nasumično biranje baze u kojoj se mjeri polarizacija fotona realizirano je pomoću $50:50$ kockastog nepolarizirajućeg razdjelnika snopa koji preusmjerava foton u jednu od baza u kojoj se izvršava mjerenje. U slučaju transmisije, odabrana baza je $\{45°, 135°\}$, dok je u slučaju refleksije odabrana baza $\{0°, 90°\}$.

Svaka baza sastoji se od dva detektora, dva zrcala (Thorlabs PF10-03-P01) te polarizirajućeg razdjelnika snopa (Thorlabs PBS102). Dodatno, grana $\{0°,90°\}$ ima $\lambda/2$ pločicu (eng. *half-wave plate*) koja zakreće polarizaciju fotona, a funkcionira na principu dvoloma. U ovom slučaju, $\lambda/2$ pločica je namještena tako da zakreće polarizaciju fotona za $45°$. Po ulasku u neku od grana te prolaskom kroz $\lambda/2$ pločicu, polarizacijski razdjelnici snopa preusmjeravaju fotone u ovisnosti o njihovoj polarizaciji. U slučaju da je foton preusmjeren u krivu bazu, polarizacijski razdjelnik snopa će ga propustiti, odnosno reflektirati, sa vjerojatnošću od 50%. Treba napomenuti da polarizacijski razdjelnici snopa i ulazne polarizacije nisu savršene što će rezultirati da mali broj fotona koji bi trebali proći kroz razdjelnik snopa budu reflektirani, i obrnuto. Ovo je jedan od izvora pogrešaka koje će kasnije biti potrebno ispraviti. Preusmjereni fotoni se potom reflektiraju na zrcalima te ulaze u odgovarajući detektor. Detektori su bazirani na silicijskim SPAD ćelijama (eng. *Single Photon Avalance Diode*) te imaju efikasnost od približno 35%. Prikaz prijamnog uređaja korištenog u ovom eksperimentu



Slika 3.3: Shema predajnika. Kratice korištene su: BS - nepolarizirajući razdjelnik snopa (eng. *beam splitter*), PBS - polarizirajući razdjelnik snopa (eng. *polarizing beam splitter*), MIR - zrcalo (eng. *mirror*), DET - detektor (eng. *detector*), OF - optičko vlakno (eng. *optical fiber*), OC - konektor za optičko vlakno (eng. *optical coupler*), HWP - $\lambda/2$ pločica (eng. *half-wave plate*).

dan je slikom 3.4.



Slika 3.4: Prijamnik korišten u eksperimentu. Uređaj je izgrađen na Institutu Ruđer Bošković.

Snimanje vremena detekcije fotona implementirali smo pomoću uređaja ID900, proizvođača ID Quantique. Ovaj uređaj može snimati vremena detekcije sa rezoluci-

jom od 100 pikosekundi. Sva četiri detektora spojena su na posebne kanale uređaja te uređaj zapisuje vrijeme detekcija fotona za svaki detektor u posebnu datoteku. Ovo je bitan dio sustava jer će vremena detekcije omogućiti vremensko sortiranje detektiranih fotona koji će se potom moći poistovjetiti sa fotonima koje je poslala Alice. Slika 3.5 prikazuje korišteni uređaj.

Slika 3.5: Uređaj za snimanje vremena detekcije fotona. Model uređaja je ID900, a proizvođač ID Quantique.

3.1.3 Kvantni kanal

Kvantni kanal u ovom eksperimentu izveli smo pomoću tri optička vlakna. Dva jednomodna optička vlakna 780HP duljine dva i pet metara spojena su sa jedne strane na predajni, odnosno prijamni uređaj dok su sa druge strane spojena na konvencionalno G.652.D telekomunikacijsko optičko vlakno dugo pet metara. Prednost korištenja telekomunikacijskog optičkog vlakna je integracija u postojeću mrežu. Naime, postavljanje potpuno nove mreže jednomodnih optičkih vlakana je velik i skup pothvat. U slučaju da je moguće provesti transmisiju fotona kroz već postavljenu mrežu optičkih vlakana bez da se polarizacije fotona potpuno međusobno izmjene, uštedilo bi se puno novaca te bi integracija kvantne distribucije ključa u mrežu bio relativno jednostavan zadatak. Nedostatak tog optičkog vlakna za naš eksperiment leži u njegovoj namjeni za provođenje fotona valne duljine $1550\ nm$, dok se u eksperimentu koristi svjetlost valne duljine $810\ nm$. Jedna od ideja ovog rada je ispitati mogućnost korištenja tog optičkog vlakna za kvantnu distribuciju ključa. Razlog zašto u ovom eksperimentu nismo koristili samo jedno telekomunikacijsko optičko vlakno je kontroler polarizacije.

S obzirom na to da se u optičkom vlaknu linearna polarizacija može zakrenuti ili čak preći u eliptičnu, odnosno cirkularnu na nasumičan način, potreban je uređaj

Slika 3.6: Kontroler polarizacije.

koji bi kompenzirao takvu promjenu polarizacije. Uređaj koji smo koristili u ovom radu je kontroler polarizacije Thorlabs FPC560 (Slika 3.6). Ovaj uređaj sastoji se od tri pločice na koje je predviđeno namotavanje optičkog vlakna. U ovisnosti o broju namotaja, pločice se mogu ponašati kao $\lambda/2$ ili $\lambda/4$ zakretači polarizacije. Izvedba zakretača polarizacije pomoću kružnih namotaja optičkog vlakna temelji se na efektu dvoloma uzrokovanog savijanjem optičkog vlakna. Pokušaj namotavanja G.652.D optičkog vlakna nije dao zadovoljavajuće rezultate kao jednomodno 780HP optičko vlakno, te smo iz tog razloga odlučili zadržati tri optička vlakna. Dvolom se u ovom slučaju pojavljuje uslijed savijanja optičkog vlakna zbog čega ono prestaje biti izotropno. Indeksi loma različitih osi više nisu jednaki što znači da komponente elektromagnetskog vala putuju različitom grupnom brzinom te se polarizacija mijenja. Rotiranjem pločica kontrolera polarizacije zakreće se upadna polarizacija što je u principu jednako rotiranju obične $\lambda/2$, odnosno $\lambda/4$ pločice. U ovom eksperimentu, kontroler polarizacije smo konfigurirali tako da je u sredini $\lambda/2$ pločica, a na krajevima su $\lambda/4$ pločice. Matematički, upotrebom Jonesovog formalizma, ovakva se transformacija polarizacije može prikazati relacijom

$$|P_{\text{iz}}\rangle = J_{\text{QWP}}(\theta_3) J_{\text{HWP}}(\theta_2) J_{\text{QWP}}(\theta_1) |P_{\text{ul}}\rangle, \tag{3.1}$$

gdje vektori $|P_{\text{ul}}\rangle$ i $|P_{\text{iz}}\rangle$ predstavljaju ulaznu i izlaznu polarizaciju, a $J_{\text{HWP}}(\theta)$ i $J_{\text{QWP}}(\theta)$ predstavljaju operator transformacije uzrokovane $\lambda/2$, odnosno $\lambda/4$ pločicom. Kutovi θ_1, θ_2 i θ_3 odgovaraju kutovima zakrenutosti pločica. Vektori polarizacije mogu se zapisati kao linearna kombinacija Jonesovih vektora horizontalne $|H\rangle$ i vertikalne $|V\rangle$ polarizacije. Jonesov formalizam je detaljno opisan u dodatku B.

3.1.4 Kalibracija

Prije provođenja eksperimenta potrebno je kalibrirati eksperimentalni postav. Postupak kalibracije sastoji se od nekoliko koraka. Za početak je potrebno podesiti da svaka od četiri polarizirane zrake ima jednak intenzitet. To se učini tako da se optičko vlakno, koje je s jedne strane spojeno na predajni uređaj, spoji u pomoćni detektor te se ugađanjem kinematičkog postolja diode podešava intenzitet. Postupak se izvodi za svaku diodu posebno dok se ne postigne podjednak intenzitet svake od njih.

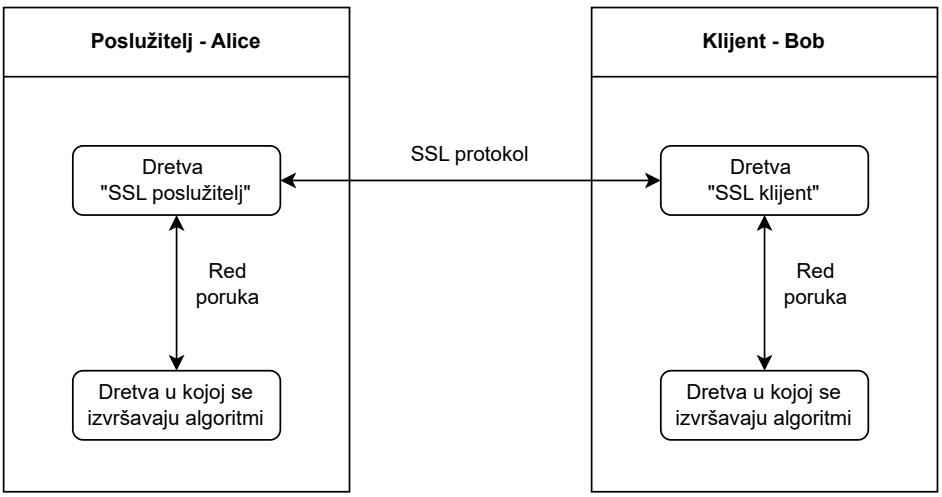
U drugom koraku potrebno je spojiti predajni i prijamni uređaj pomoću optičkih vlakana te između instalirati kontroler polarizacija. Potom se odašilje svijetlost samo jedne polarizacije te se zakretanjem pločica kontrolera polarizacije pokušava dobiti minimalna detekcija okomite polarizacije koja pripada istoj bazi. Postupak se ponavlja redom za sve polarizacije te se moraju dobiti zadovoljavajući rezultati za sve polarizacije odjednom.

Treći korak je otvaranje prijamnog uređaja u mraku te podešavanje zrcala kako bi frekvencija detekcija različitih polarizacija bila jednaka. Potom je potrebno vratiti se na prethodni korak te iterativno ponavljati drugi i treći korak dok se ne dobiju zadovoljavajući rezultati. Nakon kalibracije, postav je spreman za izvođenje eksperimenta.

3.2 Softver

Kao što je već objašnjeno ranije, softverski dio služi u obradi podataka. Sastoji se od algoritama za poravnavanje, ispravljanje pogrešaka te pojačavanje privatnosti koje smo implementirali u programskom jeziku C. Klasičnu komunikaciju implementirao sam pomoću SSL (eng. *Secure Sockets Layer*) protokola upotrebom programskog paketa *openssl* unutar programskog jezika C. Implementacija je bazirana na principu poslužitelj-klijent, gdje Alice obnaša funkciju poslužitelja, a Bob je klijent. Komunikacija između Alice i Boba je autentificirana i šifrirana upotrebom simetrične kriptografije i nasumično generiranog tajnog ključa koji prije početka eksperimenta posjeduju i Alice i Bob. I Alicein i Bobov program sastoje se od dvije dretve koje komuniciraju putem reda poruka. U jednoj dretvi izvršava se algoritam za SSL komunikaciju koji konstantno čeka nove poruke. Ako poruka stigne iz druge dretve, on ju šalje preko SSL protokola prema drugoj strani, dok ju u suprotnom šalje drugoj dretvi. U drugoj

dretvi izvršavaju se svi spomenuti algoritmi za obradu poslanih, odnosno primljenih podataka. Shema implementacije dana je na slici 3.7.



Slika 3.7: Shema implementacije softvera. Alice ima ulogu poslužitelja, dok je Bob klijent. Oba softvera se sastoje od dvije dretve od kojih je jedna zaslužna za SSL komunikaciju, a druga za izvršavanje algoritama protokola. Dvije dretve komuniciraju putem reda poruka.

3.2.1 Poravnavanje

Nakon transmisije polariziranih fotona, te nakon što Bob pomoću snimljenih vremena detekcije sortira svoj niz izmjerenih polarizacija potrebno je poravnati nizove polarizacija. S obzirom na to da sustav ima gubitke te svaki puls sadrži samo 0.1 foton u prosjeku, Bob ne može detektirati svaki Alicein puls. Dodatno, Bob ima detekcije koje potječu od šuma (eng. *DCR - Dark Count Rate*) te zakašnjelih lavina u SPAD ćelijama (eng. *afterpulsing*). To znači da je prvo potrebno razlučiti detekcije Aliceinih fotona od ostatka, te prepoznati i označiti sve Aliceine fotone koje Bob nije detektirao. Tada postoji jedan naprema jedan korespondencija između Aliceinog i Bobovog niza. Dodatno, uz uspostavljanje jedan na jedan korespondencije, potrebno je poravnati Alicein i Bobov niz polarizacija tako da se n-ti Alicein foton nalazi na n-tom mjestu u Bobovom nizu polarizacija.

Prvi korak algoritma za poravnavanje je ustanoviti jedan naprema jedan korespondenciju tako da se označe svi nedetektirani fotoni u Bobovom nizu izmjerenih polarizacija. S obzirom na to da je poznato kojom frekvencijom Alice šalje fotone, Bob zna da Aliceine fotone može detektirati samo u vremenskom razmaku koji je višekratnik vremenskog razmaka između dva pulsa. Svi ostali fotoni pripadaju ili

šumu ili zakašnjelim lavinama. Također, potrebno je označiti slučajeve u kojima je Bob u isto vrijeme detektirao foton sa različitim detektorima jer će se takva mjerenja kasnije odbaciti. Kako bi Bob bio siguran da će prikupiti sve fotone koje je Alice poslala, neće se oslanjati na Alicinu frekvenciju slanja već će iz svojih podataka izračunati frekvenciju. Frekvencija koju će Bob izračunati minimalno će se razlikovati od onoga što je rekla Alice, ali dovoljno da nakon nekog vremena fotoni počnu ispadati iz prozora koincidencije. Prozor koincidencije je vremenski interval u kojem Bob očekuje puls. Taj vremenski interval je eksperimentalno određen te iznosi 6.5 ns, a ovisi o fluktuaciji vremena odašiljanja, odnosno detekcije fotona (eng. *jitter*). Drugim riječima, ako je period transmisije fotona jednak T, a vremenska fluktuacija j, Bob očekuje detektirati Alicein foton u vremenskom intervalu $\left[T - \frac{j}{2}, T + \frac{j}{2}\right]$. Ovakav način traženja Aliceinih fotona jako dobro zaobilazi sve ostale detektirane fotone.

Nakon što su pronađeni svi Aliceini fotoni, označeni svi nedetektirani i višestruki fotoni, Alice i Bob imaju jedan naprema jedan korespondenciju između nizova polarizacija. Preostalo je poravnati njihove nizove polarizacija tako da polarizacije odgovarajućih fotona stoje na istim mjestima u oba niza. Poravnavanje se odvija usporedbom dva podniza iz Alicinog i Bobovog niza polarizacija. Za početak, Bob izračunava potrebnu duljinu podniza polarizacija koji će služiti za poravnavanje pomoću relacija

$$n_{\text{check}} = \frac{75 + 1050\epsilon}{p} \tag{3.2}$$

za $0 \leq \epsilon \leq 0.1$, i

$$n_{\text{check}} = \frac{285 - 2550\epsilon + 15000\epsilon^2}{p}, \tag{3.3}$$

gdje je p vjerojatnost detekcije fotona, a ϵ inicijalna gornja granica na pogrešnu detekciju pri mjerenju u točnoj bazi. Prethodne formule empirijski smo dobili simulacijama, a sigurnosni faktor korišten u obradi podataka je $\epsilon = 0.01$. Bob potom traži od Alice da mu pošalje niz polarizacija duljine $4n_{\text{check}}$ iz sredine svojeg niza polarizacija. U slučaju da je duljina Aliceinog niza jednaka N, Bob će dobiti podniz koji počinje na mjesu $\frac{N}{2} - 2n_{\text{check}}$ u Aliceinom nizu. Bob traži niz duljine $4n_{\text{check}}$ umjesto n_{check} tako da bi mogao i približno izračunati udio pogrešaka, o čemu će biti riječi kasnije.

Algoritam poravnavanja radi na način da prolazi kroz Alicein i Bobov niz te uspoređuje polarizacije koje su izmjerene u točnoj bazi. Program traži koliko ima

uzastopnih podudaranja polarizacija, odnosno broji koliko puta se prekida niz podudaranja. Po završetku provjere, početak Bobovog niza za poravnavanje pomiče se za jednu polarizaciju te se postupak nastavlja. Početak Bobovog niza pomiče se dovoljno puta kako bi bilo sigurno da će se naići na podniz koji se podudara s Aliceinim. Po završetku procesa, uzima se onaj slučaj koji je imao najmanje prekida podudaranja, te se Bobov niz pomiče u odnosu na Alicein za odgovarajući broj mjesta.

Nakon poravnavanja nizova potrebno je izračunati udio pogrešaka na nizu duljine $4n_{\text{check}}$. Ova informacija bit će potrebna kod algoritma za ispravljanje pogrešaka jer će se duljine blokova određivati u ovisnosti o udjelu pogrešaka. Veći udio pogrešaka značit će manje duljine blokova, i obrnuto. Udio pogrešaka želimo izračunati s preciznošću od oko $\pm 1\%$, pa je prema tome okvirno uzeta duljina $4n_{\text{check}}$. Treba imati na umu da je taj niz polarizacija poslan preko klasičnog kanala, što znači da Eve ima potpunu informaciju o njemu. Zbog toga će se taj niz morati u potpunosti odbaciti. Stoga je potrebno da ovaj niz bude čim kraći, ali da istovremeno daje zadovoljavajuću preciznost izračunatog udjela pogrešaka.

Po završetku algoritma za poravnavanje, moguće je krenuti na već objašnjene korake obrade transmitiranih fotona. Kao što je već rečeno, prvi u nizu je odbacivanje svih bitova koje je Bob detektirao u krivoj bazi. Dodatno, Alice mora odbaciti sve bitove koje Bob nije primio, a i one gdje je istovremeno detektirao više njih u različitim detektorima. Komunikacija se odvija tako da Bob pošalje niz baza, odnosno izostanka ili višestrukih detekcija na što Alice odgovara koje su baze točne, a koje ne.

3.2.2 Ispravljanje pogrešaka

Algoritam za ispravljanje pogrešaka implementiran u ovom radu je modificirana verzija originalnog Cascade algoritma [10], [11], [12]. Prvi korak algoritma je nadopunjavanje niza bitova s nulama do prvog sljedećeg broja djeljivog sa $2^8 = 512$. Nadopunjavanje niza bitova s nulama je bitan korak jer je ideja da duljina svakog bloka bude potencija broja 2, što omogućava da podblokovi za vrijeme binarnog pretraživanja uvijek budu djeljivi s 2. Maksimalna duljina inicijalnih blokova biti će 512, zbog čega je potrebno osigurati da niz bitova bude djeljiv najviše s tim brojem. Dodatno je potrebno izračunati duljinu inicijalnih blokova. Kako je već prethodno spomenuto, ona ovisi o udjelu pogrešaka. Duljine blokova odredio sam na sličan način kao i u radu "Demystifying the Information Reconciliation Protocol Cascade" [11]. Formule su

malo izmijenjene zbog želje da duljine blokova uvijek budu potencije broja 2 te zbog toga što su ključevi u ovom eksperimentu dosta kraći nego nizovi koji su korišteni u njihovim simulacijama. U prvom krugu ispravljanja pogrešaka, duljina inicijalnih blokova računa se prema relaciji

$$k_1 = 2^{\lceil \alpha \rceil}, \tag{3.4}$$

gdje je $\alpha = \log_2 \frac{1}{q} - \frac{1}{2}$, a q udio pogrešaka. U drugom krugu računa se po formuli

$$k_2 = 2^{\lceil \frac{\alpha+12}{2} \rceil}, \tag{3.5}$$

dok se u svakom sljedećem krugu računa kao

$$k_m = min\left(2^{\lfloor \log_2 \frac{n}{8} \rfloor}, 512\right), \tag{3.6}$$

gdje je n duljina niza bitova. U slučaju da duljine k_1 ili k_2 ispadnu veće nego k_m, uzima se duljina k_m koja u konačnici ograničava da duljina blokova prijeđe 512.

Potom kreće već objašnjeni proces podjele na blokove te binarnog pretraživanja. S obzirom na to da bi ispravljanje pogrešaka blok po blok zahtjevalo jako puno komunikacije, gdje bi jedna komunikacija sadržavala samo jedan paritet, algoritam sam napravio tako da šalje sve paritete odjednom. Tek nakon Aliceinog odgovora, blokovi koji imaju različite paritete dijele se na dva dijela te se ponovno šalje niz pariteta svih blokova u jednoj poruci. Također, Bob zapisuje i pamti paritete svih blokova koje mu je Alice poslala, kako bi se u sljedećim krugovima kod efekta kaskada izbjegle nepotrebne komunikacije. Na kraju svakog kruga Bob dodatno šalje hash trenutnog ključa koji je izračunat pomoću algoritma SHA-3 te je dugačak 512 bitova, koji Alice uspoređuje sa izračunatim hashom svog ključa. U slučaju da su hashevi različiti, bitovi se nasumično miješaju te se postupak ponavlja. Postupak ispravljanja pogrešaka, umjesto 4 puta kao u originalnoj verziji Cascade algoritma, ponavlja se toliko dugo dok se hashevi Aliceinog i Bobovog ključa u potpunosti ne poklapaju. U tom trenutku, Alice i Bob su sigurni da su sve pogreške ispravljene te da su njihovi ključevi jednaki.

3.2.3 Pojačavanje privatnosti

Pojačavanje privatnosti implementirao sam pomoću Toeplitzovih matrica [13], [14]. Toeplitzova matrica je matrica kojoj je svaka dijagonala, koja pada s lijeva na desno, konstantna. Topilzove matrice mogu se koristiti kao univerzalne hash funkcije. U ovom slučaju, Toeplitzova matrica sastojat će se samo od nula i jedinica. Privatnost se pojačava pomoću kompresijske funkcije na način

$$k = g \cdot w, \tag{3.7}$$

gdje je k konačni ključ, w niz bitova nakon ispravljanja pogrešaka, a g kompresijska funkcija. Kompresijska funkcija g je nasumično izabrana iz univerzalne$_2$ klase Toeplitzovih matrica.

Za početak je potrebno nasumično generirati Toeplitzovu matricu. Za to sam koristio programski paket *openssl* unutar programskog jezika C. U paketu je omogućeno generiranje slučajnog niza bajtova pomoću pseudo slučajnog generatora. Generirani bajtovi se potom pretvore u bitove koji definiraju nasumično odabranu Toeplitzovu matricu. Matrica je dimenzija $r \times n$, gdje je r konačna duljina ključa, a n duljina ključa nakon ispravljanja pogrešaka. Za generiranje matrice $r \times n$, potrebno je $r + n - 1$ nasumičnih bitova. Generirani niz bitova Bob šalje Alice putem SSL protokola.

Preostalo je pomnožiti matricu sa ključem kako bi se dobio konačan tajni ključ. Množenje matrice sa vektorom je kompleksnosti $O(n^2)$, odnosno kvadratna kompleksnost, što je vremenski skupa kalkulacija. U ovom slučaju bila bi pogotovo skupa pošto duljina ključa n u ovom eksperimentu doseže i desetak tisuća bitova. Dodatno, ovaj eksperiment ima frekvenciju slanja pulseva od nekoliko MHz, dok napredniji eksperimenti imaju puno veće frekvencije, što dodatno povećava duljinu ključa. Drugim riječima, standardno množenje matrica nije ni približno dovoljno brzo. Srećom, Toeplitzova matrica je posebna, te je množenje iste sa vektorom jednako konvoluciji vektora koji definira tu matricu sa drugim vektorom [15]. Za primjer, konvolucija vektora $a = [a_4, a_3, a_2, a_1, a_0]$ duljine $n + r - 1 = 5$ i $b = [b_0, b_1]$ duljine $n = 2$ je

$$\begin{aligned} c_1 &= [a_4, a_3, a_2, a_1, a_0] * [b_0, b_1] \\ &= [a_4 b_0, a_3 b_0 + a_4 b_1, a_2 b_0 + a_3 b_1, a_1 b_0 + a_2 b_1, a_0 b_0 + a_1 b_1, a_0 b_1]. \end{aligned} \tag{3.8}$$

S druge strane, umnožak Toeplitzove matrice, definirane vektorom a, i vektora b

jednak je

$$c_2 = \begin{bmatrix} a_3 & a_4 \\ a_2 & a_3 \\ a_1 & a_2 \\ a_0 & a_1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} a_3 b_0 + a_4 b_1 \\ a_2 b_0 + a_3 b_1 \\ a_1 b_0 + a_2 b_1 \\ a_0 b_0 + a_1 b_1 \end{bmatrix}. \tag{3.9}$$

Očito je da je srednjih r vrijednosti vektora c_1 u relaciji (3.8) jednako vrijednostima vektora c_2 u relaciji (3.9), što pokazuje da se umnožak Toeplitzove matrice i vektora može izračunati konvolucijom. Računanje konvolucije u vremenskoj domeni je također kompleksnosti $O(n^2)$, ali u frekvencijskoj domeni je kompleksnosti $O(n)$. Srećom, izumom FFT (*Fast Fourier Transform*) algoritma, prelazak iz vremenske u frekvencijsku domenu ima kompleksnost $O(n \log n)$. To znači da je ukupno računanje konvolucije pomoću frekvencijske domene i FFT-a kompleksnosti $O(n \log n)$, što je za velike n mnogo brže nego standardno množenje matrica. U ovom radu implementirao sam takvo rješenje pomoću programskog paketa *fftw3*.

4 Karakterizacija postava

Karakterizacija postava bitan je korak u izvođenju eksperimenta. Već je u prošlom poglavlju, kod opisa algoritma ponavljanja moguće uočiti poteškoće koje nastaju uslijed nesavršenosti sustava. Naizgled jednostavan protokol opisan u poglavlju 2, tehnički je zahtjevno provesti. U algoritmu koji poravnava Alicein i Bobov niz, najveće su poteškoće stvarale detekcije koje nisu Alicini fotoni. Dvije vrste nepoželjnih detekcija koje se mogu razlikovati u detektorima baziranim na silicijskim SPAD ćelijama su šum (eng. *DCR - Dark Count Rate*) i zakašnjele lavine (eng. *afterpulsing*). Takve detekcije su fizikalno jednake detekcijama Aliceinih fotona. Jedini način razlikovanja je po vremenu kada se pojavljuju.

Druga vrsta poteškoća nastaje uslijed vremenskog podrhtavanja (eng. *jitter*) laserskih dioda, odnosno detektora. U ovom kontekstu, podrhtavanje se odnosi na varijacije trenutka emisije i detekcije. Drugim riječima, proteklo vrijeme između slanja električnog signala i emisije svjetlosnog pulsa nije konstantno. Također nije konstantno niti vrijeme između apsorpcije fotona i detekcije makroskopske struje. Oba efekta pridonose varijacijama vremena između detekcije dva uzastopna fotona.

4.1 Princip rada SPAD ćelije

SPAD ćelija je dioda, odnosno p-n spoj, koji radi u Geigerovom načinu rada. Drugim riječima, na krajeve diode je postavljen reverzni napon veći od napona proboja. U tom su slučaju elektroni i šupljine privučeni na krajeve diode, odnosno elektrode, te se u sredini stvara zona osiromašenja. Dolazni foton pogađa zonu osiromašenja te pobuđuje elektron iz valentne u vodljivu vrpcu, odnosno generira par elektron-šupljina. S obzirom da je reverzni napon veći od napona proboja, u diodi postoji jako električno polje koje ubrzava elektrone do velikih brzina. Elektroni imaju dovoljno energije da na svom putu prema elektrodi pobude druge elektrone, koji ponovno imaju dovoljno energije da pobude sljedeće itd. te nastaje lavina. Lavina ima dovoljno nosioca naboja da poteče makroskopska struja koju je moguće detektirati. Nastala lavina neće sama nestati pa je potreban dodatan elektronički sklop koji će dovesti diodu u početno stanje. Postoje pasivni i aktivni sklopovi za dovođenje diode u početno stanje. Jedan od jednostavnijih pasivnih sklopova je otpornik spojen u seriju sa diodom. Kada kroz njega poteče struja, doći će do pada napona i reverzni

napon će postati manji od napona proboja. Time se generiranje novih lavina prekida, struja prestaje teći i napon se ponovno povećava iznad napona proboja. Ostali kompliciraniji sklopovi neće se ovdje razmatrati.

4.2 Šum

Šum sačinjavaju detekcije koje nisu nastale uslijed vanjske pobude u obliku svjetlosti. U kontekstu SPAD ćelija, neki od uzroka šuma su termalna pobuđenja i tuneliranje [17].

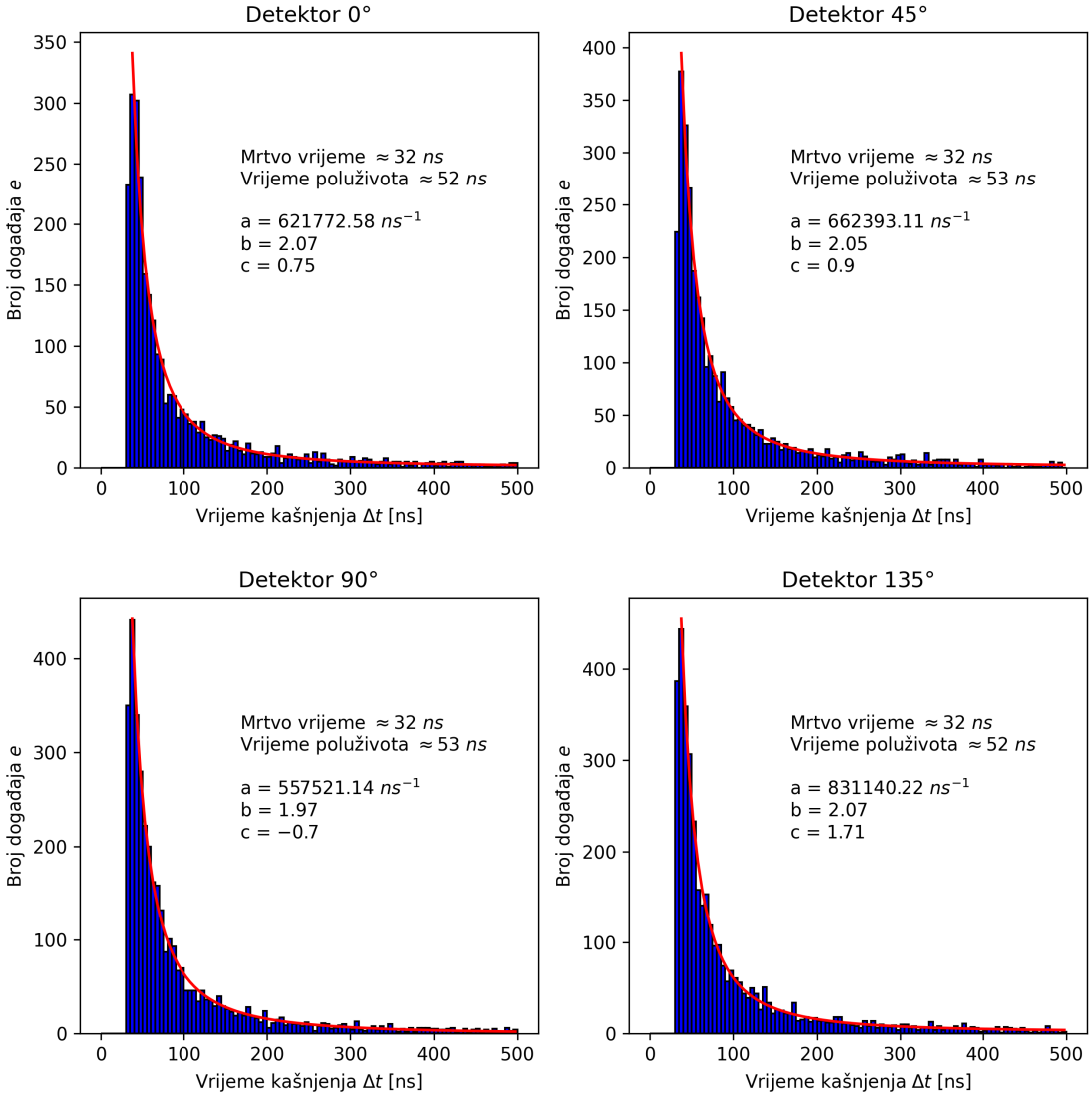
Termalna pobuđenja su najlakši i najočitiji uzrok šuma. Zbog termalnih vibracija, odnosno gibanja čestica, događaju se sudari unutar kristalne rešetke koji mogu rezultirati pobuđivanjem elektrona iz valentne u vodljivu vrpcu. Drugim riječima, generiraju se parovi elektron-šupljina koji pokreću lavinu čime dolazi do detekcije. Kako već i ime sugerira, ovakve detekcije ovise o temperaturi. Što je veća temperatura, pojavljuje se više ovakvih događaja.

Tuneliranje se može podijeliti u dvije podvrste. Postoji direktno tuneliranje te tuneliranje potpomognuto zamkama. Za razliku od termalnih pobuđenja, kod tuneliranja nije potrebno pobuđivanje elektrona. Kvantna mehanika nalaže da čestica može sa vjerojatnošću većom od nula proći kroz energetsku barijeru čak i ako nema energiju veću od vrha barijere. Tuneliranja se događaju u području osiromašenja jer u tom području elektron bez promjene energije može preskočiti iz valentne u vodljivu vrpcu, i obrnuto. Direktno tuneliranje je upravo takav efekt. S druge strane, tuneliranje potpomognuto zamkama ovisi o defektima u kristalnoj rešetki. Defekti mogu imati energetska stanja u zabranjenom području što pomaže elektronima u tuneliranju. Umjesto direktnog tuneliranja između vrpci, elektron prvo tunelira u energetska stanja uzrokovana defektima, a tek onda tunelira u drugu vrpcu.

Šum je teško otkloniti u analizi podataka jer nastaje nasumičnim procesima. To znači da šum slijedi Poissonovu raspodjelu. Najlakši način za njegovo određivanje je u mraku bez ikakvih svjetlosnih pobuda. Na taj način smo šum detektora odredili i u ovom eksperimentu. Nakon kalibracije, a prije distribucije ključa, u mraku su unutar nekoliko sekundi izbrojane detekcije uzrokovane šumom. Sva četiri detektora imali su podjednaki broj detekcija po sekundi. U prosjeku, među svim provedenim distribucijama ključa, frekvencija šuma iznosila je od 100 do 300 Hz.

4.3 *Zakašnjele lavine*

Zakašnjele lavine, s druge strane, nisu nasumični procesi već ovise o primarnim detekcijama. Svaka zakašnjela lavina ima svoju primarnu detekciju. Povećanjem frekvencije transmisije fotona, povećat će se i broj detekcija uzrokovanih zakašnjelim lavinama. S druge strane, treba primijetiti da uzrok zakašnjele lavine ne mora biti detekcija fotona već to može biti i šum. Također, zakašnjele lavine mogu stvoriti i elektroni iz zakašnjelih lavina. Takve lavine zovemo zakašnjelim lavinama drugog, odnosno n-tog reda.



Slika 4.1: Prikaz analize zakašnjelih lavina za svaki od četiri detektora.

Uzrok zakašnjelih lavina su elektroni zarobljeni u dubokim stanjima. Tokom primarne lavine dio elektrona završi u dubokim stanjima koja imaju dugo vrijeme

poluživota. O vremenu poluživota ovisi kada će se elektroni relaksirati. U slučaju da je dioda tada aktivna, elektron će kreirati sljedeću lavinu na isti način kao što je bila kreirana i prva. To dovodi do naknadnih detekcija nakon svake primarne detekcije. Jedan od najjednostavnijih načina sprječavanja, ili barem umanjivanja broja zakašnjelih lavina, je isključivanje diode na neko vrijeme nakon primarne detekcije. To se u određenoj mjeri i radi, ali predugo držanje diode isključenom dovelo bi do velikog smanjivanja rezolucije diode. Zakašnjele lavine također su ovisne o temperaturi. Smanjivanjem temperature vrijeme poluživota dubokih stanja se povećava što znači da i zakašnjele lavine duže traju. S obzirom na to da šum i zakašnjele lavine imaju obrnutu ovisnost o temperaturi, temperatura detektora se mora održavati takvom da su obje vrijednosti zadovoljavajuće. Broj zakašnjelih lavina može se dodatno smanjiti snižavanjem reverznog napona. Naime, vjerojatnost nastanka lavine ovisi o struji lavine, odnosno broju pobuđenih elektrona. Smanjivanjem napona, smanjuje se i električno polje, a posljedično i kinetička energija elektrona. Zbog toga se u konačnici pobuđuje manje elektrona.

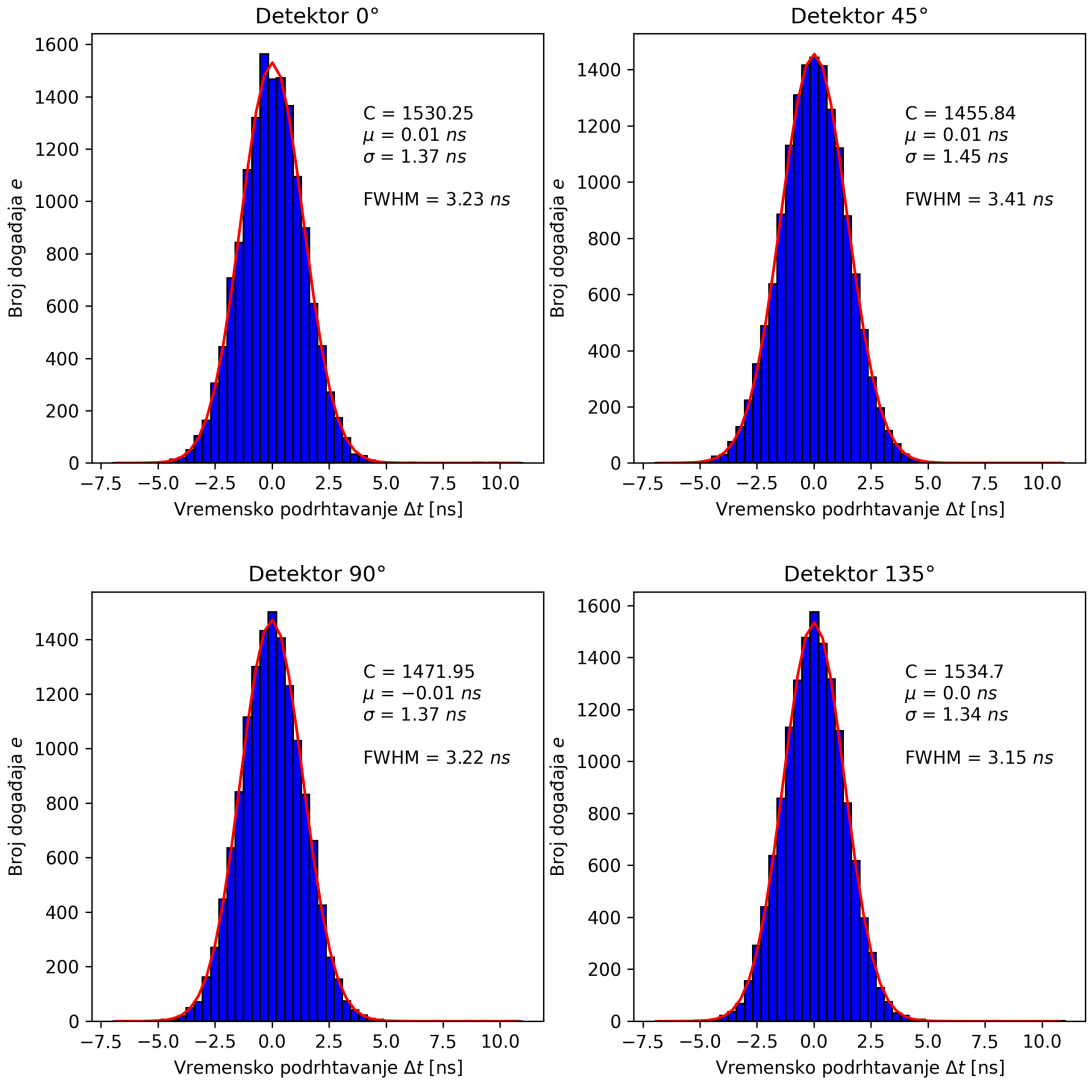
Analiza zakašnjelih lavina detaljno je provedena u radu [16]. Autori su usporedili tri različita modela te zaključili da niti jedan nije univerzalno najbolji već uspješnost modela ovisi o pojedinom detektoru. Usprkos tome, ovdje sam koristio model "zakon potencije" [16]. Zakašnjele lavine u tom modelu opisane su pomoću relacije

$$e = a \cdot \Delta t^{-b} + c, \tag{4.1}$$

gdje je e broj događaja, Δt vremenska razlika između dvije detekcije, a a, b i c su konstante koje treba odrediti. Iz grafova prikazanih slikom 4.1 vidljivo je da model dobro opisuje zakašnjele lavine u slučaju ovih detektora. S obzirom na to da karakteristike zakašnjelih lavina ne ovise o frekvenciji emisije pulseva u distribuciji ključa, mogu se koristiti podaci iz više mjerenja. Dakako, pod uvjetom da se temperatura ili reverzni napon nisu mijenjali u međuvremenu. To je napravljeno u ovom slučaju kako bi se dobila veća statistika događaja. Na prikazanim grafovima jasno se vidi mrtvo vrijeme detektora koje iznosi oko 32 ns za svaki detektor. Također, iz podataka je moguće izračunati vrijeme poluživota zakašnjelih lavina. Ispada da je to vrijeme približno jednako za sve detektore što je i očekivano jer su detektori jednaki, a iznosi 52-53 ns.

4.4 *Vremensko podrhtavanje*

Kao što je već spomenuto, vremensko podrhtavanje je varijacija vremena između električnog signala i emisije pulsa, odnosno apsorpcije fotona i detekcije struje. Vremensko podrhtavanje u detektoru, odnosno SPAD ćeliji ovisi o generiranju lavine. S obzirom na to da je nastanak lavine stohastički proces jasno je da vrijeme između apsorpcije fotona i detekcije struje neće biti konstantno. U kontekstu laserske diode, postoji više efekata koje utječu na podrhtavanja. Vremensko podrhtavanje diode je puno manje nego ono od detektora te nije značajno za analizu pa se neće detaljnije opisivati.



Slika 4.2: Prikaz analize kombiniranog vremenskog podrhtavanja laserske diode i detektora za svaki od četiri detektora.

Na slici 4.2 je prikaz analize vremenskog podrhtavanja za svaki detektor posebno.

Treba uzeti u obzir da se podaci podrhtavanja na ovim grafovima sastoje od podrhtavanja određenog detektora i podrhtavanja svih laserskih dioda. Što se tiče laserskih dioda, najviše podataka ima o podrhtavanju diode iste polarizacije, potom duplo manje podataka o diodama druge baze i minimalno podataka o diodi ortogonalne polarizacije unutar iste baze. Ova analiza je potrebna kako bi se odredila veličina prozora koincidencije u algoritmu za poravnavanje. Ranije je spomenuto da je uzet prozor širine 6.5 ns, što okvirno odgovara dvostrukoj vrijednosti FWHM. Vremensko podrhtavanje modelirano je Gaussovom raspodjelom koja je dana relacijom

$$e = a \cdot e^{-\frac{1}{2}\left(\frac{\Delta t \quad \mu}{\sigma}\right)^2}, \tag{4.2}$$

gdje je e broj događaja, Δt odstupanje perioda između dva mjerenja od srednjeg perioda, μ srednja vrijednost, a σ standardna devijacija.

5 Rezultati

Proveo sam deset grupa eksperimenata sa različitim postavkama. Također, prije svakog mjerenja podesio sam postav na način opisan u poglavlju 3.1.4. Svaka grupa se sastoji od osam kvantnih distribucija ključa frekvencija transmisije 1, 2, 4 i 8 MHz, od kojih su po dvije distribucije jednake frekvencije. Razlike među grupama su jačina gušenja, šum te broj transmitiranih fotona. Atenuacija je varirana pomoću različitih filtera neutralne gustoće kako je već ranije objašnjeno, a šum se nadodao uključivanjem lampe pored prijamnog uređaja. U tablici 5.1 prikazana su sva izvršena mjerenja sa pripadnim postavkama. Iz tablice se može vidjeti da su mjerenja bez dodatnog šuma u potpunosti uspješna, dok kod onih sa dodanim šumom postoje poteškoće. Poteškoće se javljaju u algoritmu za poravnavanje. Zbog previše šuma algoritam ne uspijeva poravnati nizove. Također je jasno da se poteškoće povećavaju kako šum raste.

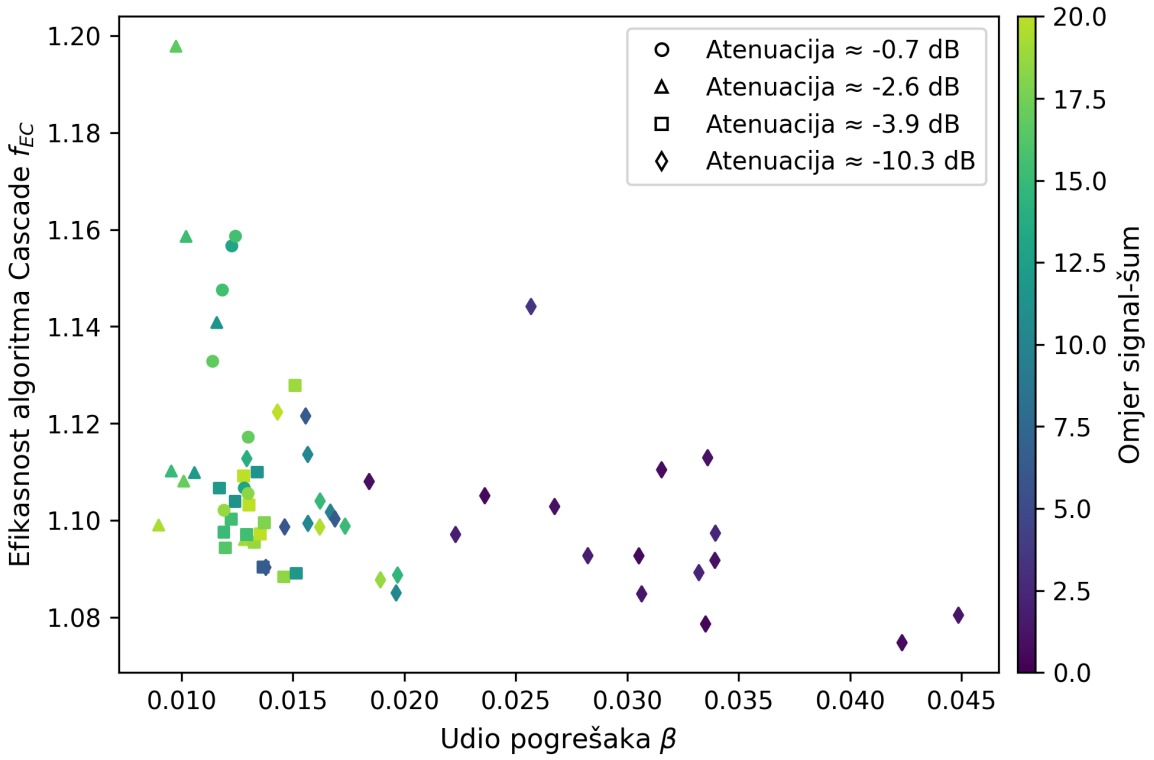
Indeks	Atenuacija	Broj pulseva	Dodatni šum	Uspješne distribucije
1	≈ -2.6 dB	1 milion	1x	8
2	≈ -10.3 dB	1 milion	1x	8
3	≈ -10.3 dB	10 miliona	1x	8
4	≈ -10.3 dB	2 miliona	10x	5
5	≈ -10.3 dB	2 miliona	20x	4
6	≈ -10.3 dB	5 miliona	20x	4
7	≈ -10.3 dB	5 miliona	40x	2
8	≈ -3.9 dB	2 miliona	1x	8
9	≈ -3.9 dB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

Tablica 5.1: Prikaz izvršenih grupa mjerenja i njihove značajke. Unutar svake grupe je izvršeno osam distribucija ključa frekvencija transmisije 1, 2, 4 i 8 MHz, od kojih su po dvije distribucije jednake frekvencije.

Na grafu 5.1 prikazana je efikasnost implementiranog Cascade algoritma. Efikasnost je prikazana kao funkcija udjela pogrešaka preko relacije

$$f_{\text{EC}} = \frac{1 - R}{h(\beta)}, \tag{5.1}$$

gdje je $R = 1 - \frac{t}{n}$, jedan minus omjer otkrivenih pariteta i duljine ključa prije ispravljanja pogrešaka, a $h(\beta)$ je Shannonova entropija. Shannonova entropija određuje minimalni udio ključa koji je potrebno otkriti da bi se ispravile sve pogreške. Prema tome, formula f_{EC} je omjer otkrivenih pariteta i minimalnog broj bitova koje je potrebno otkriti da bi se sve pogreške ispravile. Relacija (5.1) je uzeta po uzoru na rad [11] pa je moguća direktna usporedba efikasnosti. S obzirom na to da Cascade algoritam sadrži korak miješanja niza bitova koji je nasumičan, proveo sam dvadeset obrada podataka čija je svrha bila dobivanje reprezentativnije distribucije. Dvadeset ponavljanja očito nije dovoljno te bi za dobivanje jasne krivulje postupak obrade podataka trebalo ponoviti puno više puta.



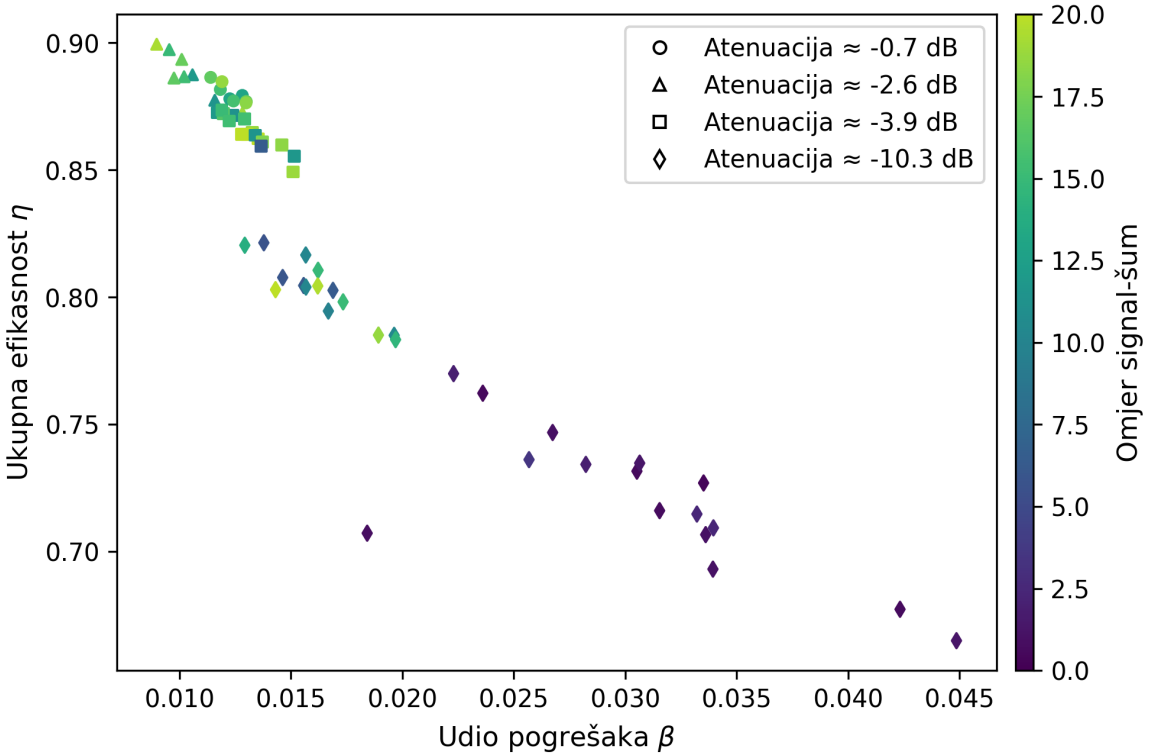
Slika 5.1: Prikaz efikasnosti Cascade algoritma u ovisnosti o udjelu pogrešaka prema relaciji (5.1). Simboli prikazuju grupe mjerenja različitih atenuacija, a boje prikazuju odnos signal-šum.

Na grafu su simbolima označene grupe različitih atenuacija, a bojama je označen odnos signal-šum za svako mjerenje. Zbog premalo ponavljanja obrade podataka, vrijednosti su i dalje raspršene pa ih je teško usporediti sa grafovima iz rada [11]. Usprkos tome, izgleda da je trend sličan, ali efikasnost malo manja.

Na slici 5.2 prikazana je ukupna efikasnost obrade sirovog ključa. Efikasnost se računa prema formuli

$$\eta = \frac{n - 4n_{\text{check}} - t - s}{n}, \tag{5.2}$$

gdje je n duljina ključa nakon odbacivanja mjerenja u pogrešnim bazama, $4n_{\text{check}}$ broj bitova korištenih za poravnavanje i računanje udjela pogrešaka, t broj otkrivenih pariteta, a s sigurnosni faktor. Ukupna efikasnost kreće se od približno 90% za mjerenja sa najmanjim do nešto manje od 70% za mjerenja sa najvećim udjelom pogrešaka. Također, postoji jedno mjerenje koje iz nepoznatog razloga jako odstupa od ostalih. Iz prikazanih podataka moglo bi se zaključiti da ukupna efikasnost ovisi o atenuaciji, ali to nije slučaj. U grupama sa velikom atenuacijom smo također testirali i povećani šum, koji je u stvari odgovoran za manju efikasnost. Ako se mjerenja sa dodanim šumom ne uzmu u obzir, vidi se da atenuacija ima mali ili nikakav utjecaj na udio pogrešaka, odnosno efikasnost. Osim o šumu, udio pogrešaka prije svega ovisi o kalibraciji polarizacije. Preciznost kalibracije varira između skupina mjerenja, čineći usporedbe između različitih skupina manje preciznima.



Slika 5.2: Prikaz ukupne efikasnosti obrade sirovog ključa. Simboli prikazuju grupe mjerenja različitih atenuacija, a boje prikazuju odnos signal-šum.

6 Zaključak

Kvantna distribucija ključa predmet je mnogih istraživanja u cilju zadržavanja sigurne komunikacije i nakon potencijalne pojave korisnih kvantnih računala. U ovom smo se radu bavili eksperimentalnom izvedbom kvantne distribucije ključa koja se temelji na BB84 protokolu. Za početak je opisan BB84 protokol koji se sastoji od kvantnog i klasičnog dijela. Također, opisani su mogući napadi na kvantni dio protokola.

Nadalje, implementirani su i opisani hardver i softver korišteni u eksperimentalnom postavu. Za razliku od uobičajenih rješenja, predajni i prijamni uređaji sagrađeni su od relativno jeftinih optičkih komponenti za valnu duljinu od 810 nm te detektora baziranih na SPAD ćelijama. Opisani su algoritmi za poravnavanje, ispravljanje pogrešaka te pojačavanje privatnosti koji su implementirani u programskom jeziku C. Također je opisan postupak kalibracije postava koji je potrebno provesti prije distribucije ključa.

Potom je okarakteriziran sustav, odnosno detektori fotona, pošto su upravo oni najkompleksniji dio postava te je potrebno bolje razumijevanje njihovog rada za cjelovito razumijevanje implementiranog postava. Iz snimljenih podataka, to jest vremena kada su detektirani fotoni, izračunate tu zakašnjele lavine te kombinacija vremenskog podrhtavanja detektora i laserskih dioda. Kako bi analiza bila kompletna, u mraku je izmjeren šum detektora.

Na samom kraju je provedena analiza učinkovitosti ostvarene kvantne distribucije ključa. Konkretno, analizirana je učinkovitost algoritma za ispravljanje pogrešaka te ukupna učinkovitost klasičnog dijela protokola. Učinkovitost Cascade algoritma uspoređena je sa analizom obavljenom u radu [11] te izgleda da je implementacija u ovom radu malo lošija. Ukupna učinkovitost je definirana kao omjer duljine krajnjeg tajnog ključa te broja fotona izmjerenih u točnoj bazi, a kreće se u rasponu od oko 90% za najmanji do ispod 70% za najveći udio pogrešaka.

Realizirani postav može poslužiti kao baza za daljnji razvoj kvantne distribucije ključa. Jedno od najvećih pitanja je kako kalibrirati polarizaciju fotona u slučaju prisluškivanja komunikacije od treće strane. Također, za lakše i preciznije korištenje bilo bi potrebno implementirati automatsku kalibraciju. Dodatno, potrebno je poraditi na algoritmu poravnavanja kako bi bio otporniji na povećani šum te na algoritmu za ispravljanje pogrešaka kako bi se dobila veća učinkovitost. Za kraj, predajni i pri-

jamni uređaj moguće je integrirati u zasebne silicijske čipove što bi uvelike smanjilo dimenzije uređaja te osiguralo veću preciznost kvantne distribucije ključa.

Dodaci

Dodatak A Kvantna mehanika

Kao što je u klasičnoj fizici sustav opisan pomoću varijabli, u kvantnoj fizici je opisan pomoću kvantnih stanja. Kvantna mehanika opisuje nastanak kvantnih stanja, njihovu evoluciju kroz vrijeme te mjerenje istih [18]. Kvantna stanja bilo kojeg sustava mogu se prikazati vektorima u n-dimenzionalnom Hilbertovom prostoru.

A.1 Hilbertov prostor

Hilbertov prostor je kompleksni vektorski prostor na kojemu je definiran skalarni produkt dva vektora. Skalarni produkt ima sljedeća svojstva

1. $\langle x|y\rangle = \langle y|x\rangle^*$
2. $\langle ax_1 + bx_2|y\rangle = a\langle x_1|y\rangle + b\langle x_2|y\rangle$
3. $\langle x|ay_1 + by_2\rangle = a^*\langle x|y_1\rangle + b^*\langle x|y_2\rangle$.

Takvom prostoru moguće je definirati bazu. Baza vektorskog prostora je bilo koji skup vektora koji potpuno razapinju taj prostor. Drugim riječima, svaki vektor u vektorskom prostoru moguće je prikazati kao linearnu kombinaciju vektora baze. Za bazu $\{|b_i\rangle\}$, $i \in [1, n]$ se kaže da je ortogonalna ako vrijedi

$$\langle b_i|b_j\rangle = 0, \quad \forall i, j \in [1, n]. \tag{A.1}$$

A.2 Superpozicija

Princip superpozicije nalaže da u slučaju da se sustav može naći u bilo kojem od $|\psi_i\rangle$ stanja, onda se može naći i u superpoziciji tih stanja

$$|\psi\rangle = \sum_i c_i|\psi_i\rangle, \tag{A.2}$$

gdje su c_i kompleksni brojevi. Taj princip proizlazi iz linearnosti Schrödingerove jednadžbe.

Dodatak B Jonesov formalizam

U optici, polarizirana svjetlost može se opisati pomoću Jonesovog formalizma [19] kojeg je razvio R. C. Jones. U ovom formalizmu, polarizirana svjetlost reprezentirana je vektorom, a linearni optički elementi reprezentirani su Jonesovim matricama. Uvjet korištenja Jonesovog formalizma je to da je svjetlost potpuno polarizirana.

B.1 Jonesovi vektori

Koristi se šest Jonesovih vektora koji reprezentiraju tri konjugirane baze. Horizontalno-vertikalna baza sastoji se od vektora

$$|H\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |V\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{B.1}$$

gdje vektor $|H\rangle$ predstavlja horizontalnu, a $|V\rangle$ vertikalnu polarizaciju. Dijagonalna baza sastoji se od vektora

$$\begin{aligned} |D\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(|H\rangle + |V\rangle\right) \\ |A\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(|H\rangle - |V\rangle\right) \end{aligned} \tag{B.2}$$

gdje vektor $|D\rangle$ predstavlja dijagonalnu, a $|A\rangle$ antidijagonalnu polarizaciju. Treća baza je cirkularna, a sastoji se od vektora

$$\begin{aligned} |R\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix} = \frac{1}{\sqrt{2}} \left(|H\rangle - i|V\rangle\right) \\ |L\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} = \frac{1}{\sqrt{2}} \left(|H\rangle + i|V\rangle\right) \end{aligned} \tag{B.3}$$

gdje vektor $|R\rangle$ predstavlja desno, a $|L\rangle$ lijevo cirkularnu polarizaciju.

B.2 Jonesove matrice

B.2.1 Polarizatori

Polarizatori su optički elementi koji propuštaju samo svjetlost određene polarizacije. Postoje linearni i cirkularni polarizatori. Opći linearni polarizator koji polarizira svjetlost pod kutem θ u odnosu na horizontalu zapisan je sljedećom matricom, odnosno operatorom

$$J_{\text{LP}}(\theta) = \begin{bmatrix} \cos^2\theta & \sin\theta\cos\theta \\ \sin\theta\cos\theta & \sin^2\theta. \end{bmatrix} \tag{B.4}$$

Desno i lijevo cirkularni polarizatori dani su matricama

$$J_{\text{RCP}} = \frac{1}{2}\begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}, \quad J_{\text{LCP}} = \frac{1}{2}\begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}, \tag{B.5}$$

gdje operator J_{RCP} predstavlja desno, a J_{LCP} lijevo cirkularni polarizator.

B.2.2 λ pločice

λ pločice su anizotropni optički elementi koji pokazuju efekt dvoloma. U ovom kontekstu dvolom je pojava kada polarizirana svjetlost različitih polarizacija propagira drugačijom grupnom brzinom kroz medij. Drugim riječima, materijal ima dva različita indeksa loma za dvije okomite osi. Os manjeg ideksa loma zove se brza os, dok se os većeg indeksa loma zove spora os. U nastavku je dan matrični zapis linearnih $\lambda/2$, $\lambda/4$ i opće linearne λ pločice, te opis općenitog materijala koji pokazuje svojstvo dvoloma.

$\lambda/2$ pločica dobila je ime po tome što komponenta elektromagnetskog vala koja je polarizirana paralelno sa sporom osi prolaskom kroz $\lambda/2$ pločicu kasni za pola valne duljine u odnosu na komponentu polariziranu paralelno sa brzom osi. Ovaj optički element zakreće polarizaciju. Matrični zapis $\lambda/2$ pločice kojoj je brza os pod kutem θ u odnosu na horizontalu je sljedeći

$$J_{\text{HWP}}(\theta) = e^{-\frac{i\pi}{2}} \begin{bmatrix} \cos^2\theta + i\sin^2\theta & \sin 2\theta \\ \sin 2\theta & \sin^2\theta - \cos^2\theta \end{bmatrix}. \tag{B.6}$$

$\lambda/4$ pločica dobila je ime po tome što komponenta elektromagnetskog vala koja

je polarizirana paralelno sa sporom osi prolaskom kroz $\lambda/4$ pločicu kasni za četvrtinu valne duljine u odnosu na komponentu polariziranu paralelno sa brzom osi. Ovaj optički element pretvara linearnu polarizaciju u cirkularnu i obrnuto. Matrični zapis $\lambda/4$ pločice kojoj je brza os pod kutem θ u odnosu na horizontalu je sljedeći

$$J_{\text{QWP}}(\theta) = e^{-\frac{i\pi}{4}} \begin{bmatrix} \cos^2\theta + i\sin^2\theta & (1-i)\sin\theta\cos\theta \\ (1-i)\sin\theta\cos\theta & \sin^2\theta + i\cos^2\theta \end{bmatrix}. \tag{B.7}$$

Kod opće, odnosno λ/n pločice, komponenta elektromagnetskog vala koja je polarizirana paralelno sa sporom osi kasni n-ti dio valne duljine u odnosu na komponentu polariziranu paralelno sa brzom osi. Matrični zapis λ/n pločice kojoj je brza os pod kutem θ u odnosu na horizontalu je sljedeći

$$J_{\text{GWP}}(\theta) = e^{-\frac{i\eta}{2}} \begin{bmatrix} \cos^2\theta + e^{i\eta}\sin^2\theta & (1-e^{i\eta})\sin\theta\cos\theta \\ (1-e^{i\eta})\sin\theta\cos\theta & \sin^2\theta + e^{i\eta}\cos^2\theta \end{bmatrix}, \tag{B.8}$$

gdje η fazna razlika između komponenata elektromagnetskog vala izražena u radijanima.

Najopćenitiji operator u Jonesovom formalizmu prikazuje opći materijal sa svojstvom dvoloma. Zapis je dan matricom

$$J_{\text{GWP}}(\theta) = e^{-\frac{i\eta}{2}} \begin{bmatrix} \cos^2\theta + e^{i\eta}\sin^2\theta & (1-e^{i\eta})e^{-i\phi}\sin\theta\cos\theta \\ (1-e^{i\eta})e^{i\phi}\sin\theta\cos\theta & \sin^2\theta + e^{i\eta}\cos^2\theta \end{bmatrix}, \tag{B.9}$$

gdje ϕ označava cirkularnost. Linearne λ pločice imaju $\phi = 0$, cirkularne imaju $\phi = \dfrac{\pi}{2}$, a kod eliptičnih je $\phi \in \left[\dfrac{-\pi}{2}, \dfrac{\pi}{2}\right]$.

Dodatak C Toeplitzovo univerzalno hashiranje

Toeplitzova matrica, nazvana po matematičaru Ottu Toeplitzu, je matrica koja ima konstante dijagonale koje padaju s lijeva na desno te je definirana relacijom

$$T_{i,j} = T_{i+1,j+1}, \quad \forall i, j. \tag{C.1}$$

Opći zapis $r \times n$ Toeplitzove matrice je sljedeći

$$T = \begin{bmatrix} t_{r-1} & t_r & t_{r+1} & t_{r+2} & t_{r+3} & \dots & t_{r+n-2} \\ t_{r-2} & t_{r-1} & t_r & t_{r+1} & t_{r+2} & \ddots & \vdots \\ t_{r-3} & t_{r-2} & t_{r-1} & t_r & t_{r+1} & \ddots & \vdots \\ t_{r-4} & t_{r-3} & t_{r-2} & t_{r-1} & t_r & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ t_0 & \dots & \dots & \dots & \dots & \dots & t_{n-1} \end{bmatrix}. \tag{C.2}$$

U univerzalnom hashiranju koriste se binarne Toplitzove matrice [13], [14]. Binarna Toeplitzova matrica definirana je binarnim vektorom t duljine $r+n-1$. Veza između elemenata Toeplitzove matrice T i vektora t koji ju definira dana je relacijom

$$T_{i,i+k} = t_{k+r-1}, \quad \forall i,k \in [0,n-1] \text{ tako da je } i+k \in [0,n-1] \tag{C.3}$$

Nasumično biranje Toeplitzove matrice jednako je nasumičnom generiranju pripadnog vektora iz skupa $\{0,1\}^{r+n-1}$.

C.1 Množenje Toeplitzove matrice sa vektorom

Standardno množenje matrice sa vektorom je kompleksnosti $O(n^2)$. Množenje $r \times n$ Toeplitzove matrice sa vektorom može se izračunati kao r srednjih vrijednosti konvolucije vektora koji definira matricu i drugog vektora [15]. Množenje Toeplitzove matrice T sa nekim vektorom v zapisuje se kao

$$x = T \cdot v, \tag{C.4}$$

a i-ti element vektora x kao

$$x_i = \sum_{j=0}^{n-1} T_{i,j} v_j \tag{C.5}$$

Kombiniranjem relacija (C.3) i (C.5) dobije se

$$x_i = \sum_{j=0}^{n-1} t_{j+r-1-i} v_j \tag{C.6}$$

što je upravo zapis jednog elementa konvolucije vektora t_{rev} i v

$$y = t_{\text{rev}} * v, \tag{C.7}$$

gdje je t_{rev} zrcaljeni vektor vektoru t. Drugim riječima, prvi element vektora t je zadnji element vektora t_{rev}. Konačno, vektor x se sastoji od srednjih r elemenata vektora y. Prebacivanjem u frekvencijsku domenu gdje konvolucija postaje jednostavno množenje dobije se

$$y = \mathcal{F}^{-1}\left(\mathcal{F}(t_{\text{rev}}) \cdot \mathcal{F}(v)\right), \tag{C.8}$$

gdje $\mathcal{F}$ označava Fourierov transformat, a $\mathcal{F}^{-1}$ inverzni Fourierov transformat. Računanje konvolucija u kompleksnom prostoru je kompleksnosti $O(n)$, a računanje Fourierovog transformata je zahvaljujući FFT (eng. *Fast Fourier Transform*) algoritmu kompleksnosti $O(n \log n)$. Ukupna kompleksnost računanja produkta Toeplitzove matrice sa vektorom u frekvencijskoj domeni je $O(n \log n)$.

Literatura

[1] Bennett, C. H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. // Theoretical Computer Science. Vol. 560, 1(2014), str. 7-11.

[2] Brassard, G.; Salvail, L. Secret-Key Reconciliation by Public Discussion. // Advances in Cryptology — EUROCRYPT '93, LNCS. Vol. 765, (2014), str. 410-423.

[3] Cascade-Python Documentation, (2022), Read the Docs, `https://cascade-python.readthedocs.io/en/latest/`, 11.3.2024.

[4] Carter, J. L.; Wegman, M. N.; Universal Classes of Hash Functions. // Journal of Computer and System Sciences, Vol. 18, (1979), str. 143–154.

[5] Carter, J. L.; Wegman, M. N.; New Hash Functions and Their Use in Authentication and Set Equality. // Journal of Computer and System Sciences, Vol. 22, (1981), str. 265–279.

[6] Bennett, C. H.; Brassard, G.; Robert, J-M. Privacy Amplification by Public Discussion. // SIAM Journal on Computing, Vol. 17, 2(1988), str. 210–229.

[7] Maurer, U. Secret Key Agreement by Public Discussion from Common Information. // IEEE Transactions on Information Theory, Vol. 39, 3(1993).

[8] Bennett, C. H.; Brassard, G.; Crpeau, C.; Maurer, U. M. Generalized Privacy Amplification. // IEEE Transactions on Information Theory, Vol. 41, 6(1995).

[9] Bennett, C.H.; Bessette, F.; Brassard, G. i sur. Experimental Quantum Cryptography. // Journal of Cryptology, Vol. 5, (1992), str. 3-28.

[10] Elkouss, D.; Martinez-Mateo J.; Martin, V. Information Reconciliation for Quantum Key Distribution. // Quantum Information and Computation, Vol. 11, 3&4(2011), str. 226-238.

[11] Martinez-Mateo, J.; Pacher, C.; Peev, M. i sur. Demystifying the Information Reconciliation Protocol Cascade. // Quantum Information and Computation, Vol. 15, 2014.

[12] Brochmann Pedersen, T.; Toyran, M. High Performance Information Reconciliation for QKD with CASCADE. // Quantum Information and Computation, Vol. 15, 5&6(2015), str. 419-434.

[13] Van Assche, G. Quantum Cryptography and Secret-Key Distillation. Doktorski rad. Brussels : University of Brussels, 2005.

[14] Bang-Ying, T.; Bo, L.; Yong-Ping, Z.; Chun-Qing, W.; Wan-Rong, Y. High-speed and Large-scale Privacy Amplification Scheme for Quantum Key Distribution. // Sci Rep, Vol. 9, 15733(2019).

[15] Chu, E.; George, A. Inside the FFT Black Box: Serial and Parallel Fast Fourier Transform Algorithms. CRC Press, 2019.

[16] Ziarkash, A.W.; Joshi, S.K.; Stipčević, M. i sur. Comparative study of afterpulsing behavior and models in single photon counting avalanche photo diode detectors. // Sci Rep, Vol. 8, 5076(2018).

[17] Cusini, I.; Berretta, D.; Conca, E.; Incoronato, A. i sur. 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).

[18] Auletta, G.; Fortutano, M.; Parisi, G. Quantum Mechanics. 1st ed. New York : Cambridge University Press, 2009.

[19] Collett, E. Field Guide to Polarization. Bellingham : SPIE Press, 2005.