Kvantna kriptografija na BB84 postavu

Mateja Batelić*
Fizički odsjek, Prirodoslovno-matematički fakultet, Bijenička cesta 32, Zagreb

Mentor: dr. sc. Mario Stipčević
Znanstveni centar izvrsnosti za napredne materijale i senzore,
Laboratorij za fotoniku i kvantnu optiku, Zavod za eksperimentalnu fiziku,
Institut Ruđer Bošković, Bijenička cesta 54, Zagreb
(Dated: 23. siječnja 2022.)

U ovom radu opisan je princip rada protokola BB84 - prvog prokola iz područja kvantne kriptografije. Uvedena je nova shifting faza pomoću koje je slanje impulsa, koji stvaraju fotone, i detektiranje istih nekorelirano u vremenu. Algoritmom poravnavanja sinkronizirani su svi izmjereni događaji, točnije poslane i detektirane polarizacije fotona, čime je potvrđena mogućnost ovakvog oblika prijenosa informacija između dvije strane komunikacijskog kanala, bez dodatnog otkrivanja informacija.

I. UVOD

Tijekom povijesti ljudi su uvijek željeli prenositi tajne poruke i to su uspjevali ostvariti kroz kriptografiju - tehniku sigurne komunikacije između dvije osobe u javnom okruženju. Nažalost, klasična kriptografija danas predstavlja problem i nesigurna je zbog povećanja vjerojatnosti probijanja tajnog ključa sa dužim vremenom danim na raspolaganju. Zbog toga je razvoj kvantnih računala omogućio nastanak kvantne kriptografije kao jednog mogućeg rješenja.

BB84 je prvi protokol iz kvantne kriptografije, područja kriptografije koje koristi kvantomehaničke principe za enkripciju podataka i njihovo slanje kako ne bi mogli biti hakirani. Danas postoje razni protokoli, ali ovaj je jedan od najosnovnijih. Naziv BB84 potječe od prvih slova prezimena dvaju autora koji su osmislili taj protokol - Bennett i Brassard, a broj 84 označava godinu 1984. kada su autori objavili prvi članak s tom idejom [1].

U ovom radu opisan je sam princip rada protokola BB84, a sastoji se od dvije faze, kod kojih je druga podijeljena u dva dijela:

1. Kvantna faza: Izmjena tajnog ključa
2. Klasična faza naknadne obrade
    - Reconcilation
    - Privacy amplification

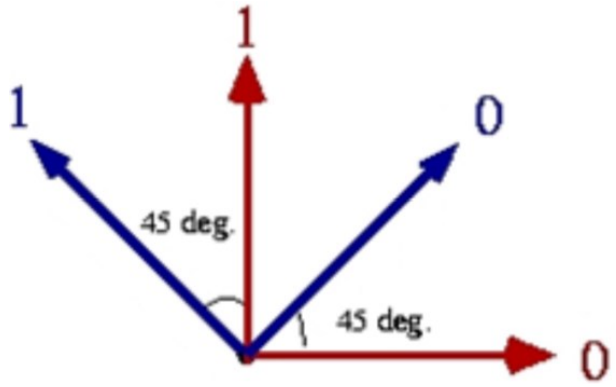
Prva faza naziva se kvantna faza i ona opisuje distribuciju kvantnog ključa, kojom se šalje tajni ključ između dvije osobe nužan za dekodiranje enkodirane poruke. Ona obuhvaća i klasičnu i kvantnu komunikaciju. Druga faza obuhvaća samo klasičnu komunikaciju, a sastoji se od dva dijela - reconcilation protokola i privacy amplification-a. Reconcilation protokol je potreban za oporavak dijela ključa koji je izgubljen prilikom njegovog slanja, dok se kod privacy amplification privatizira cijeli ključ kako bi se smanjila mogućnost pogreške prilikom dekodiranja poruke zbog informacija o ključu koje su procurile tokom druge faze.

I.1. Quantum key distribution

Prva faza protokola BB84 je faza distribucije kvantnog ključa. Ideja ove faze je da se kodira svaki bit tajnog ključa u stanje polarizacije ili fazu jednog fotona te pošalje primatelju. Zamislimo osobu A (Alice) koja želi poslati infomaciju o tajnom ključu osobi B (Bob) te osobu E (Eve), koja ih prisluškuje. Alice šalje niz pulseva, od kojih, u idealiziranom slučaju, svaki puls sadrži jedan foton sa drugačijom polarizacijom od ostalih. Također, Alice generira dvije baze - jednu bazu sa horizontalnom i vertikalnom polarizacijom (HV baza) te dijagonalnu bazu (AD baza). U HV bazi je horizontalnoj polarizaciji pridružen broj '0', a vertikalnoj broj '1', dok je u AD bazi 'D' polarizaciji pridružen broj '0', a 'A' polarizaciji broj '1'. Obje baze su prikazane na Slici1 te su zarotirane jedna u odnosu na drugu za 45 stupnjeva. Baza HV je prikazana crvenom bojom, a baza AD plavom.

Ovaj protokol najbolje je opisati na primjeru prikazanom na Slici2 [1]. Primjer niza bitova koje Alice odabire prikazan je u prvom retku pod nazivom 'Alice's bit', a primjer baza koje ona odabire za pojedini foton prikazan je na istoj slici u retku ispod 'Alice's basis'. S obzirom na izabrani bit i bazu, određena je polaziracija svakog pojedinog fotona kojeg Alice šalje Bobu te je prikazana u trećem retku 'Alice's polarization'. Dakle, Alice 50% slučajno izabranih fotona enkodira sa jednom bazom, a 50% sa drugom i šalje ih Bobu koji mjeri polarizaciju fotona.

* mbatelic.phy@pmf.hr



Slika 1. Dvije okomite baze koje generira Alice: horizontalna i vertikalna (HV) baza (crvena boja) te dijagonalna (AD) baza (plava boja).

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Slika 2. Primjer razmjene tajnog ključa između Alice i Boba slanjem polariziranih fotona.

S druge strane, Bob također nasumično odabire baze za svaki pojedini foton koji mjeri, što je vidiljivo u retku 'Bob's basis' na Slici2. Bob ima na raspolganju iste baze kao i Alice pa ako mjeri npr. s HV bazom HV enkodirani foton, onda on može saznati koja je polarizacija tog fotona. Analogno za AD bazu. Nakon odabranih baza, on mjeri polarizacije svakog detektiranog fotona te dobiva niz polarizacija 'Bob's measurements'.

Konačno, posljedni korak u izmjeni tajnog ključa je javna diskusija baza između Alice i Boba u kojoj Bob kaže Alice koju bazu je koristio prilikom mjerenja pojedinog fotona, a Alice mu odgovara da li je ta baza jednaka njezinoj. U 50% slučajeva, njihove polarizacije se preklapaju, što znači da je podijeljeni tajni ključ ispravan, kao što se može vidjeti u zadnjem retku Slike2 'Shared Secret key'. Ostali slučajevi se odbacuju. Time je slanje tajnog ključa završeno iako je duljina ključa prepolovljena, ali su Alice i Bob doista uspjeli razmjeniti tajni ključ bez javnog objavljivanja bitova tj. dijelova ključa [2,3].

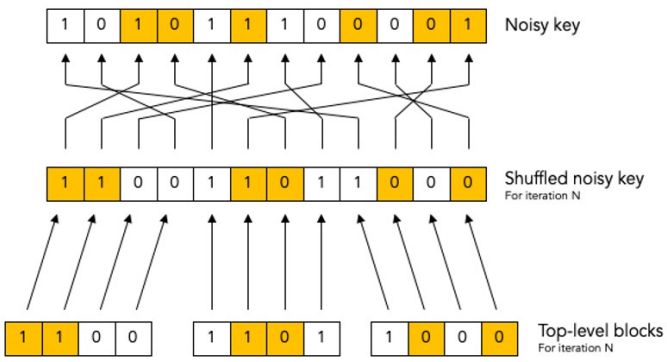
Pretpostavimo sada da Eve presreće fotone nakon što ih Alice pošalje Bobu. S obzirom da Eve, kao niti Bob, ne zna koje baze Alice koristi, ona također nasumično izabire baze za svaki presretnuti foton. Ako uspije pogoditi bazu, tada šalje Bobu ispravan foton. No, u slučaju da pogriješi bazu, a Bob pogodi, tada Bob ima samo 50% šanse da pogodi polarizaciju fotona tj. bit jer se Eve umiješala. Da nije bilo Eve, Bob bi bio siguran da je izmjerio ispravnu polarizaciju, a ovako postoji mogućnost da Alice i Bob nemaju jednaki ključ tj. bitove, odnosno došlo je do određenih razlika. Zbog toga, nakon što su Alice i Bob razmijenili informacije o korištenim bazama, oni tada uzimaju npr. 10% preostalih informacija o ključu i uspoređuju ih. U slučaju da su primjećene neke razlike, oni znaju da je Eve pokušala prisluškivati pa se cijeli ključ odbacije, a procedura sa kodiranjem i slanjem tajnog ključa se ponovo ponavlja ispočetka. Uspješnost uspoređivanja dijela ključa kod kojih Alice i Bob rade samo 20 uspoređivanja je iznimna jer se vjerojatnost da je Eve presrela foton smanjuje se na manje od 1 u milijun, što ukazuje na visoku efikasnost protokola uz minimalne gubitke informacija.

I.2. Reconcilation

U praksi, prethodno opisana distribucija ključa ima dva problema. Prvi problem je da detektori fotona imaju određeni šum, što znači da će se i bez prisluškivanja Alicini i Bobovi bitovi razlikovati. Drugi problem je što generatori fotona stvaraju fotone tj. svjetlosne impulse sa zadanim prosječnim brojem fotona po impulsu, što znači da u određenom vremenskom intervalu nije nužno samo jedan foton, već ih može biti i više. To znači da Eve ima dobre šanse da podijeli impulse, promatrajući jedan foton dok drugi neometano nastavlja do Boba. Ako je broj tako stvorenih fotona m, tada je vjerojatnost da Eve podijeli puls $m^2/2$ te time sazna dio informacije o ključu [4].

Zbog toga, nakon distribucije ključa, Alice i Bob uspoređuju dijelove ključa javnom raspravom, kao što je već spomenuto, ne otkrivajući Eve ništa više od onoga što je ona možda već otkrila tijekom faze kvantne transmisije, jer svaki novi bit informacije koji Eve dobije prepolavalja broj ključeva koje Eve treba isprobati kod napada grubom silom. Pritom Alice i Bob odabiru otprilike 10% bitova, ali na točno određeni način. Takav postupak se naziva Reconcilation protokol. Postoji više vrsta takvog protokola,a u ovom radu korišten je kaskadni algoritam [2], prikazan na Slici3.

Kaskadni algoritam radi tako što se Alice i Bob prvo dogovore o nasumičnoj permutaciji bitova, a zatim dijele permutirani niz na blokove duljine b. Konstanta b je eksperimentalno odabrana tako da je vjerojatnost da će pojedini blok sadržavati više od jedne pogreške (dva žuta kvadratića na Slici3) vrlo mala. Nakon tog koraka,



Slika 3. Kaskadni algoritam za reconcilation protokol. Žuti kvadratići označavaju bitove koji su pogrešno preneseni.

Alice i Bob zatim uspoređuju paritet svakog bloka. Ako pronađu par blokova s neusklađenim paritetima, oni kontinuirano dijele blok na sve manje i manje blokove, uspoređujući paritete svaki put, sve dok se ne pronađe greška. Kako bi osigurali da Eve ništa ne nauči iz ovog procesa, Alice i Bob odbacuju zadnji bit svakog bloka čiji paritet otkrivaju.

Nakon što jednom dovrše ovaj proces, i dalje će postojati neusklađenosti u tim blokovima koji sadrže paran broj pogrešaka. Stoga bi Alice i Bob mogli ponoviti postupak još nekoliko puta s povećanjem veličine bloka sve dok ne povjeruju da je ukupan broj pogrešaka nizak. No, ovakva strategija postaje neučinkovita jer Alice i Bob moraju odbaciti bit za svaki blok koji uspoređuju, a vjerojatnost pronalaska greške u svakom bloku je niska. Zbog toga Alice i Bob prelaze na novu strategiju, koju provode više puta. Svaki put biraju nasumični podskup pozicija bitova u svojim kompletnim nizovima i uspoređuju parnosti. Vjerojatnost neslaganja ako nizovi podskupa nisu identični je točno 1/2. Ako dođe do neslaganja, izvodi se bisektivno traženje pogreške, ali ovaj put koristeći nasumične podskupove umjesto blokova. Posljednji bit svakog podskupa se odbacuje. Na kraju će sve pogreške biti uklonjene, a Alice i Bob će proći kroz dovoljno provjera pariteta bez otkrivanja pogrešaka za koje bi mogli pretpostaviti da su njihovi nizovi identični.

I.3. Privacy amplification

U ovom trenutku, Alice i Bob posjeduju identične nizove bitova, ali ti nizovi nisu potpuno privatni jer je Eve možda dobila neke informacije o njima bilo dijeljenjem impulsa ili presretanjem/ponovnim slanjem fotona. Iako ova druga strategija može uzrokovati neke pogreške u Bobovom nizu, ako ga Eva koristi na samo malom broju bitova, inducirane pogreške će se izgubiti među pogreškama uzrokovanim šumom u detektorima i drugim fizičkim problemima. Tijekom faze usklađivanja, Eve nije dobila nikakve informacije, budući da je zadnji bit svakog skupa provjere pariteta bio odbačen. Međutim, neke od njezinih izvornih informacija o određenim bitovima možda su pretvorene u informacije o paritetnim bitovima. Na primjer, ako je znala vrijednost bita x u nizu y, a Alice i Bob su otkrili paritet y i odbacili x, Eve bi tada mogla znati paritet preostalih bitova od y [5]. Kažemo da Eve može znati najviše k paritetnih bitova ključa nakon reconcilation faze ako poznaje najviše k fizičkih bitova ključa.

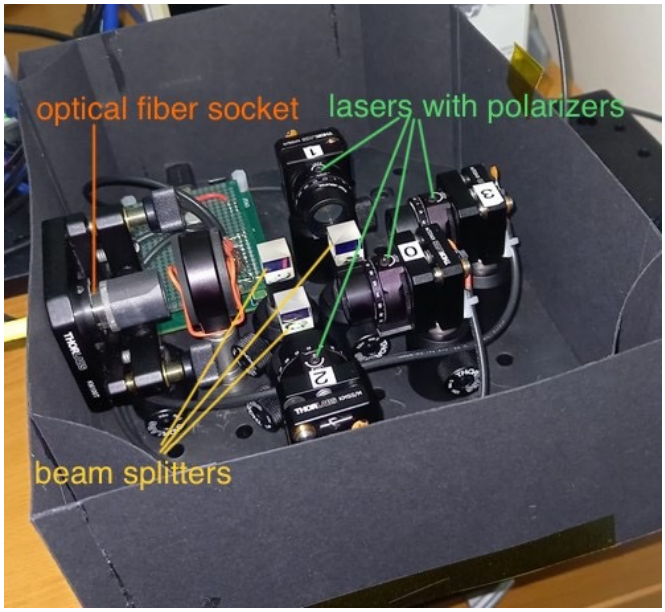
Mogli bismo se zapitati kako Alice i Bob određuju vrijednost k, tj. koliko je informacija procurilo do Eve. Kao konzervativnu procjenu, oni jednostavno mogu pretpostaviti da su sve pogreške u prijenosu uzrokovane prisluškivanjem, iako su neke najvjerojatnije proizašle iz pogrešaka detekcije. Alice i Bob mogu koristiti intenzitet snopa m i stopu bitne pogreške za izračunavanje očekivanog udjela koji je Eva naučila. Ako su konzervativni u svojim pretpostavkama i dodaju nekoliko standardnih devijacija svojim rezultatima, imat će sigurnu gornju granicu za broj bitova koji su procurili Eve.

Ova rasprava pretpostavlja da Eve poznaje samo deterministične bitove, pa je drugo pitanje bi li joj možda bilo korisnije dobiti informacije o vjerojatnostima. Drugim riječima, umjesto da mjeri fotone u istim bazama kao Alice i Bob, mogla je odabrati bazu na pola puta između njih. To će joj dati rezultat koji odgovara Aliceinom s vjerojatnošću od približno 85%, bez obzira na to koju osnovu Alice koristi [5]. Ona neće dobiti nikakve informacije kada Bob otkrije svoje odabire mjerenja, tako da su s ovom strategijom sve njezine informacije u obliku vjerojatnosti, a ne deterministične. Moguće je da bi ove informacije mogle biti otpornije na povećanje privatnosti od deterministične informacija. Međutim, pokazalo se da to nije slučaj [3,6,7], pa ako Eve želi optimizirati svoje očekivane informacije o konačnom ključu, treba koristiti iste baze kao Alice i Bob, dobivajući samo deterministične bitove.

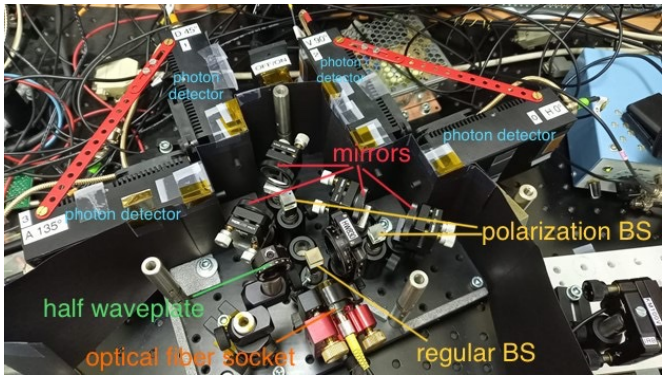
II. EKSPERIMENTALNA METODA

Eksperimentalni postav sastojao se od pošiljatelja Alice, prikazanog na Slici4, primatelja Bob, prikazanog na Slici5, te računala. Trenutno se svi podaci prikupljaju i obrađuju na jednom računalu, no ideja je da se u konačnici podaci uzimaju zasebno sa Boba i Alice, svatko na svojem računalu, od kojih se svaki nalazi na jednom kraju komunikacijskog puta i koji su povezani klasičnim kanalom (internet) i kvantnim kanalom (tamno optičko vlakno).

Alice se sastoji od četiri lasera sa polarizatorima, čije



Slika 4. Eksperimentalni postav za Alice



Slika 5. Eksperimentalni postav za Boba

zrake upadaju na razdjelnike zraka[1] (BS), koji potom sažimaju sve četiri zrake u jednu. Ta rezultantna zraka prolazi kroz optičko vlakno do Boba.

Bob se sastoji ulaza za optičko vlakno kroz koje dolaze fotoni poslani od Alice. Iza vlakna koje dovodi nepolarizirano svjetlo stavljen je rotirajući linearni polarizator za namještanje half waveplate-a (HW pločica). Prvo je određeno gdje su 0 i 90 deg rotirajući polarizatori tako da je minimalni broj pogodaka na analizatorima 90 i 0 stupnjva respektivno. Nakon toga se polarizator zakrene za 45 ili 135 stupnjeva te vrti HW pločica kako bi se dobili minimumi detekcije na 135 odnosno 45 stupnjeva. U tim namještanjima se pokazalo da transmisija polarizirajućih BS (PBS) razdjelnika doista ne čuva sasvim polarizaciju, te da omjer grananja nije 50%-50% nego bliže 40%-60% na valnoj duljini od 810 nm. Osim običnog i polariziranih razdjelnika zraka, u Bobu se još nalaze i četiri detektora, od kojih svaki detektira određenu polarizaciju fotona.

Posebna novost u ovom radu je što Alice i Bob ne znaju kad je Alice počela slati fotone tj. njihovi satovi nisu usklađeni, čime se smanjuje mogućnost presretanja fotona. Time je uvedena nova faza protokola BB84 koja je nazvana shifting faza. U toj fazi Alice šalje Bobu milijun pulseva putem optičkog vlakna, nakon čega Bob u svojim mjerenjima pronalazi fotone poslane od Alice, koji su karakterizirani time da se jedan od drugoga nalaze udaljeni za višekratnik perioda ispaljivanja svjetlosnih pulseva od strane Alice. Taj višekratnik je unaprijed poznat Bobu s točnošću do na 0.1% u najgorem slučaju, npr. 1 u 1000 ns. Nakon toga, Bob određuje broj poznatih polarizacija i šalje ih Alice, potom "poravnava" svoje fotone s Alicinim pulsevima te joj šalje i polazni broj te niz svojih baza u kojima je detektirao fotone. U posljednjem koraku, Alice odgovara vektorom "da/ne" o tome koje bitove zadržati, a koje odbaciti. Time je shifting protokol završen.

Nakon ove faze, Alice i Bob imaju nizove koji su uvelike slični, ali i sa nešto razlika, koje se nakon toga analiziraju pomoću reconcilation protokola. U ovom radu je obrađena shifting faza, dok će reconcilation protokol i privacy amplification biti proučavani u daljnjem nastavku istraživanja.

Program za uzimanje podataka, `take_data.exe`, kontrolira Alice i prikuplja od nje podatak o redoslijedu polarizacija (lasera), a od Boba putem ID900 skuplja podatke o signalima s četiriju detektora, dok program `Alice.exe` analizira podatke (okuplja analize Boba i Alice). Nakon što su prikupljeni podaci s Alice i Boba, stvorene su dvije datoteke od kojih prva sadrži redosljed lasera, koje je Alice izabrala slučajnim redosljedom, dok druga datoteka sadrži vremena kada je foton detektiran i na kojem detektoru. Dio prikupljenih podataka prikazan je na Slici6.

Alice	Bob	
3	1759271600	3
3	3083155400	1
1	3138506000	1
1	3545543900	1
2	7198548900	2
0	8083942900	0
3	8466621500	3
1	12130132300	1
3	13393631200	3
0	14091175200	3
3	14152081000	3

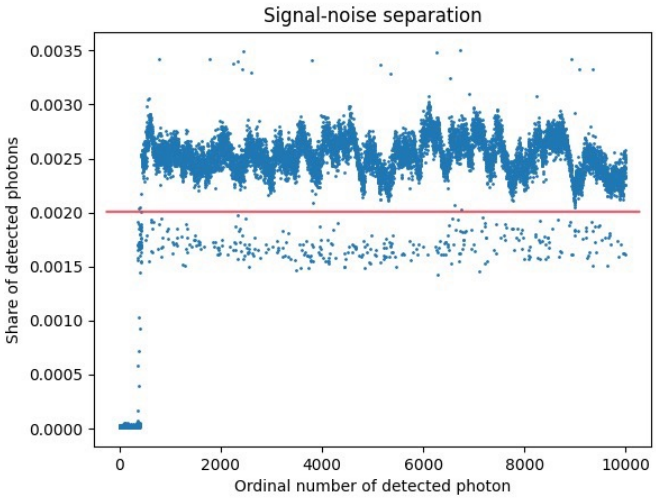
Slika 6. Prikupljeni podaci od Alice i Boba. Alicini podaci prikazuju lasere koje je odabrala, dok Bobovi podaci prikazuju vremena detekecije fotona i lasere na kojima su detektirani.

[1] eng. beam splitters

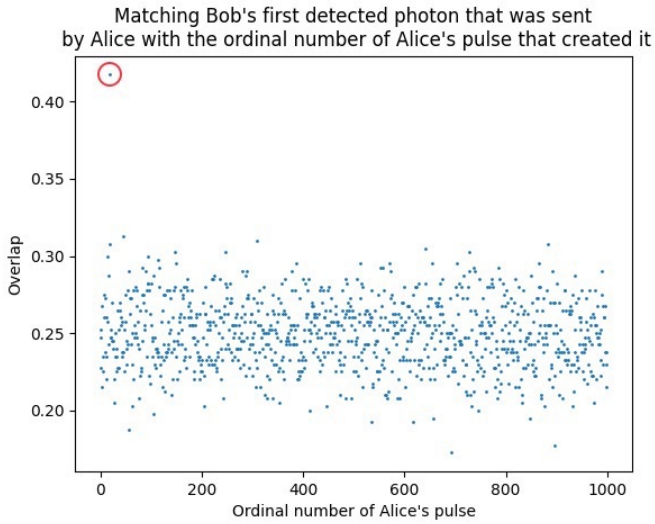
III. REZULTATI I DISKUSIJA

Sinkronizacija ispaljivanja Alicinih pulseva i Bobovih detekcija odvijala se u dva koraka:

1. Izdvajanje signala iz šuma,
2. Pronalaženje podudarnosti između prvog detektiranog fotona s Alicinim pulsom koji je stvorio taj foton.



Slika 7. Prva faza sinkronizacije Alicinih pulseva i Bobovih detekcija: Izdvajanje signala iz šuma.



Slika 8. Druga faza sinkronizacije Alicinih pulseva i Bobovih detekcija: Pronalaženje podudarnosti između prvog detektiranog fotona s Alicinim pulsom koji je stvorio taj foton.

Na Slici7 je jasno vidljiva razlika između šuma i detektiranih fotona, čija vjerojatnost detekcije je puno viša. Crvena linija razgraničava to područje. U sljedećem koraku, odbacuje se šum i pristupa se traženju prvog fotona proizvedenog pomoću prvog Alicinog impulsa. Detekcija tog fotona prikazana je na Slici8 i lako je uočljiva jer je ta detekcija izdvojena daleko iznad ostalih (zaokruženo crveno na Slici8).

Preklop između Alicinih impulsa koji stvaraju fotone i Bobovog detektiranja fotona stvorenih tim impulsima obrađeno je u programskom jeziku Python. Taj algoritam radi na principu da se traži točan pomak kod kojeg se pojavi najveći broj preklopa polarizacija između dva niza. Pretpostavimo da Alice šalje 1 000 000 fotona. Tada Alice šalje središnjih N polarizacija, tj. redni broj u intervalu [500 000 - N/2, 500 000 + N/2 - 1], a Bob traži najbolji preklob oko svoje sredine ±1000 mjesta, što je ukupno 2000 provjera preklopa. Kao kriterij za točan preklop uzet je onaj na kojem se javlja najveći broj podudarnih polarizacija između onog što je Bob primio i onoga što mu je Alice poslala. Najveći broj preklopa se pojavljuje u prosjeku na 47.5% mjesta. Donja granica koja osigurava da je preklop moguć obuhvaća vjerojatnost Bobove detekcije fotona p i vjerojatnost da su fotoni ušli u ispravnu bazu, ali završili u pogrešnom detektoru ϵ:

$$N \geqslant \frac{125}{p}\sqrt{\frac{\epsilon}{0.05}} = \frac{560\sqrt{\epsilon}}{p} \tag{1}$$

Najniža izmjerena vrijednost curenja u krivi kanal je 2 % u HV bazi te 4% u AD bazi. Dodaju li se na to i pogreške Alice, tada se dobiva vrijednost za ϵ od minimalno 5%. Pogreške kod Alice su nastale zbog toga što su BS razdjelnici dizajnirani tako da dijele laserski snop na dva dijela, dok u ovom eksperimentalnom postavu kod Alice, oni služe za skupljanje dva snopa u jedan, što znači da se radi o obrnutom korištenju tog optičkog elementa. Trenutno korišteni BS razdjelnici imaju transmisiju 99.5% u refleksiji i 90% u transmisiji, s time da dosta mijenjaju polarizaciju, što ograničava kvalitetu Alice. Zamjena BS razdjelnika s kvalitetnijim modelima dala bi preciznije rezultate jer bi došlo do manjeg rasipanja snopa.

Ovim rezultatima je pokazano da je prijenos tajnog ključa pomoću shifting protokola uspješno proveden jer, u suprotnom, podudarnosti ne bi bilo.

IV. ZAKLJUČAK

Kvantna kriptografija predstavlja sadašnjost i budućnost sigurne komunikacije pa je zbog toga uvijek na fronti modernih znanstvenih istraživanja. Ovaj seminar dio je istraživanja vezanog uz poboljšanje protokola BB84 - jednog od prvih protokola u kvantnoj

kriptografiji. Cilj eksperimenta bio je proslijediti tajni ključ od osobe pošiljatelja do osobe primatelja kroz shifting protokol, koji opisuje sinkronizaciju poslanih i detektiranih polarizacija fotona zbog njihove nekoreliranosti u vremenu.

U ovom radu opisan je BB84 protokol kroz dvije faze - kvantnu fazu, koja opisuje shifting protokol, i klasičnu fazu naknadne obrade, koja obuhvaća reconcilation protokol i privacy amplification. Eksperimentalno je potvrđena samo kvantna faza kao prvi korak u uspostavljanju uspješne komunikacije prilikom distribucije tajnog ključa.

Prikupljeni podaci su obrađeni u programskom jeziku Python i pokazano je da je shifting protokol uspješan jer je moguće dobiti preklop između ispaljenih laserskih impulsa i detektiranih fotona kao višekratnika s točnošću do na 0.1%. Ovime je postavljen temelj za razvijanje daljnjih koraka u sigurnoj komunikaciji kod ovakve vrste protokola u kvantnoj kriptografiji.

V. ACKNOWLEDGMENTS

Iskrene zahvale mentoru dr. sc. Mariu Stipčeviću na objašnjavanju svih nejasnoća i spremnosti da prenese svo svoje znanje u svakom trenutku. Također, hvala kolegi Antoniu Ceroviću na suradnji i pomoći tokom ovog istraživanja i izrade seminara.

[1] Bennett, C. H., Brassard, G., "Quantum cryptography: Public key distribution and coin tossing" in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE, New York, pp. 175-179, 1984.

[2] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J., "Experimental Quantum Cryptography", Journal of Cryptology, vol. 5, no.1, pp. 3-28, 1992.

[3] Bennett, C. H., Brassard, G., and Ekert, A. K., "Quantum Cryptography", Scientific American, pp. 50-57, 1992.

[4] Brassard, G., Salvail, L., "Secret key reconciliation by public discussion," Lecture Notes in Computer Science, vol. 765, pp. 410–423, 1994.

[5] Bennett, C. H., Brassard, G., Crépeau, C. and Maurer, U. M., "Generalized Privacy Amplification", IEEE Transactions on Information Theory, 1995.

[6] Bennett, C. H., Brassard, G., Cr=E9peau, C., and Skubiszewska, M.-H., "Practical Quantum Oblivious Transfer", Advances in Cryptology – Proceedings of Crypto '91, Lecture Notes in Computer Science, Vol. 576, Springer-Verlag, Berlin, pp. 351-366, 1992.

[7] Brassard, G., Cr=E9peau, C., Jozsa, R., and Langlois, D., "A Quantum Bit Commitment Scheme Provably Unbreakable By Both Parties", Proceedings of the 34th IEEE Symposium on Foundations of Computer Science, pp. 362-371, 1993.