Kriptografski izazovi u eri kvantnog računarstva

Hrupački, Miran

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Stručni studij

KRIPTOGRAFSKI IZAZOVI U ERI KVANTNOG RAČUNARSTVA

Završni rad

Miran Hrupački

Osijek, 2020.

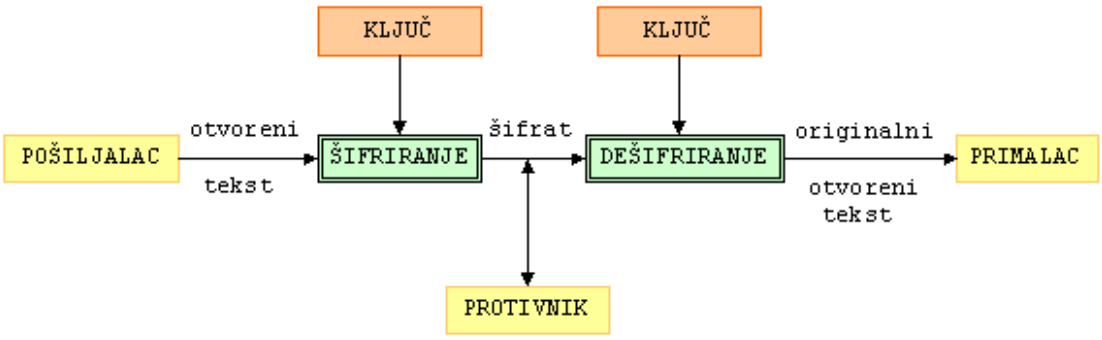
SADRŽAJ

1. UVOD

Radi potrebe za sigurnom komunikacijom došlo je do osmišljavanja raznih strategija kako bi sakrili sadržaj poruke odnosno njenu razumljivost kako ne bi došla u „krive ruke“, ali da je razumljiva onom kojem je poruka namijenjena, a naziva se enkripcija odnosno šifriranje. Kriptografske tehnike su razvijane stoljećima, njeni tvorci trudili su se da budu korak ispred onih koji pokušavaju probiti kod. Kriptografija je za svoju zaštitu osmislila razne simetrične i asimetrične sustave, koji rade na različitim principima, ali osiguravaju komunikaciju. Neki od njih su objašnjeni u daljnjim koracima. Današnje metode koje su najčešće korištene su ugrožene stvaranjem kvantnih računala, no već je razvijena kvantna kriptografija koja obećava puno sigurniju komunikaciju od bilo koje druge tehnike komunikacije te ona ne može biti ugrožena kvantnim računalima. Zahvaljujući jako velikom napretku u tehnologiji te i samoj kriptografiji, nastala je kvantna kriptografija koja omogućuje uspostavljanje komunikacije kroz komunikacijski kanal koji nije moguće prisluškivati bez da se ometa prijenos, što znači da korisnici koji komuniciraju putem komunikacijskog kanala mogu vrlo lako otkriti prisustvo treće strane kojoj je cilj otkriti ključ, što je njen najveći doprinos u kriptografiji. Njeni principi će se objasniti pobliže. Definirat će se sam pojam kriptografije, njeni osnovni principi, razne kriptografske metode. Tako će se objasniti kvantna kriptografija koja nudi razne mogućnosti koje nisu dostupne u klasičnoj kriptografiji, njen princip distribucije tajnog ključa te njene protokole i prijenos fotona. Nastavno na to, objasnit će se veliki problemi nazvan „kvaka 22“. Kvantna razmjena ključeva omogućuje komunikaciju koja je u potpunosti sigurna. Osoba koja pokušava saznati sadržaj poruke putem prisluškivanja kanala ne može kopirati kvantna stanja (*qubite*). Sama kvantna kriptografija je zasnovana na principima kvantne mehanike, te su iskoristili njena svojstva, odnosno stanja. Kvantna kriptografija se koristi za dobivanje i distribuciju ključeva, ali ne i za prijenos poruke. Također će se objasniti njene mane te kako se kvantna kriptografija brani od raznih hakerskih napada. Objasnit će se njen razvitak, odnosno kako je kvantna kriptografija izgledala nekada i danas.

2. KRIPTOGRAFIJA

Riječ kriptografija je grčkog podrijetla te se ona može prevesti kao tajnopis. Nikad nije bilo točno utvrđeno kada je kriptografija osmišljena, no pretpostavlja se da se to dogodilo 2000 godina prije Krista, jer iz tog vremena su pronađeni prvi tragovi šifriranja. Kriptografija je imala jako veliku ulogu u 20. stoljeću kada su se odvijala dva svjetska rata i mnogo raznih sukoba. Kriptografija je metoda zaštite informacije i komunikacije pomoću koje se poruka šifrira, tako da samo oni kojima je poruka namijenjena imaju mogućnost dešifrirati i pročitati. Sama poruka se ne skriva već se skriva značenje sadržaja poruke. Njen zadatak je jednostavan, funkcionira na način da se informacija zaštiti od tzv. „treće strane“. Poruka koju pošiljatelj šalje naziva se otvoreni tekst, a kako bi se zaštitio sadržaj poruke, preoblikuje se otvoreni tekst pomoću dogovorenog ključa, taj postupak nazivamo šifriranje, a rezultat je šifrirana poruka. Ukoliko se dogodi da „treća strana“ dođe do poruke, kriptografija je ta koja omogućuje tajnost poruke te da je ona nejasna za one kojima nije namijenjena. Način komunikacije je bio sljedeći: pošiljatelj i primatelj poruke unaprijed se dogovore oko ključa koji će služiti za šifriranje. Pošiljatelj pomoću ključa pretvara razumljivu poruku u šifrat i šalje ga preko komunikacijskog kanala. Ukoliko netko presretne poruku, on ju ne može razumjeti, već samo doznati sadržaj šifrata. Kada poruka dođe do primatelja, on uz unaprijed dogovoren ključ poruku pretvara u razumljiv tekst. [1], [2], [3]



Sl.1.1. Primjer primjene kriptografije, odnosno komunikacijski kanal [3]

2.1. AES (Advanced Encryption Standard)

AES je napredni kriptografski standard koji spada u simetrične algoritme te ja najpopularniji i najkorišteniji među simetričnim sustavima. AES koristi i američka vlada kako bi

zaštitila svoje podatke, što je dovelo do šireg korištenja u svijetu. Spada u otvoren standard te je besplatno za korištenje u javne, privatne, komercijalne ili ne komercijalne svrhe. Kao što je navedeno AES spada u simetrične enkripcije ključa, što znači da je isti ključ korišten za enkripciju i dekripciju podataka što dovodi do problema kako poslati ključ sigurnim putem. Simetrične šifre, kao što je AES, su pokazale da su jako dobre u čuvanju podataka koji su spremljeni na tvrdim diskovima. Iz tih razloga, simetrične šifre se smatraju superiornijim od asimetričnih, zato što zahtijevaju manju računalnu snagu, što dovodi do toga da se simetrična enkripcija odvija puno brže, a smatraju se čak i tisuću puta brže od asimetričnih. Iz razloga što su brže, više su korisnije u situacijama kada se mora obaviti enkripcija na velikoj količini podataka. AES radi sa blokovima duljine 128 bita i podržava tri duljine ključeva: 129, 192 i 256 bita, što je duljina ključa veća, on je sigurniji, jer tada postoji više kombinacija, što znači da je teže za probiti. Ukoliko je AES dobro postavljen, on se smatra neprobojnim, jer je potrebno jako dugačak period kako bi se ključ otkrio. Prethodnik AES enkripcije je DES koji koristi 56 bitne ključeve. 1998. godine napravljena je računalna mašina koja je uspješno probila DES u samo dva dana, a to su napravili kako bi dokazali kako je vrijeme za novi enkripcijski sustav. [7]

2.2. RSA (Rivest Shamir Adleman)

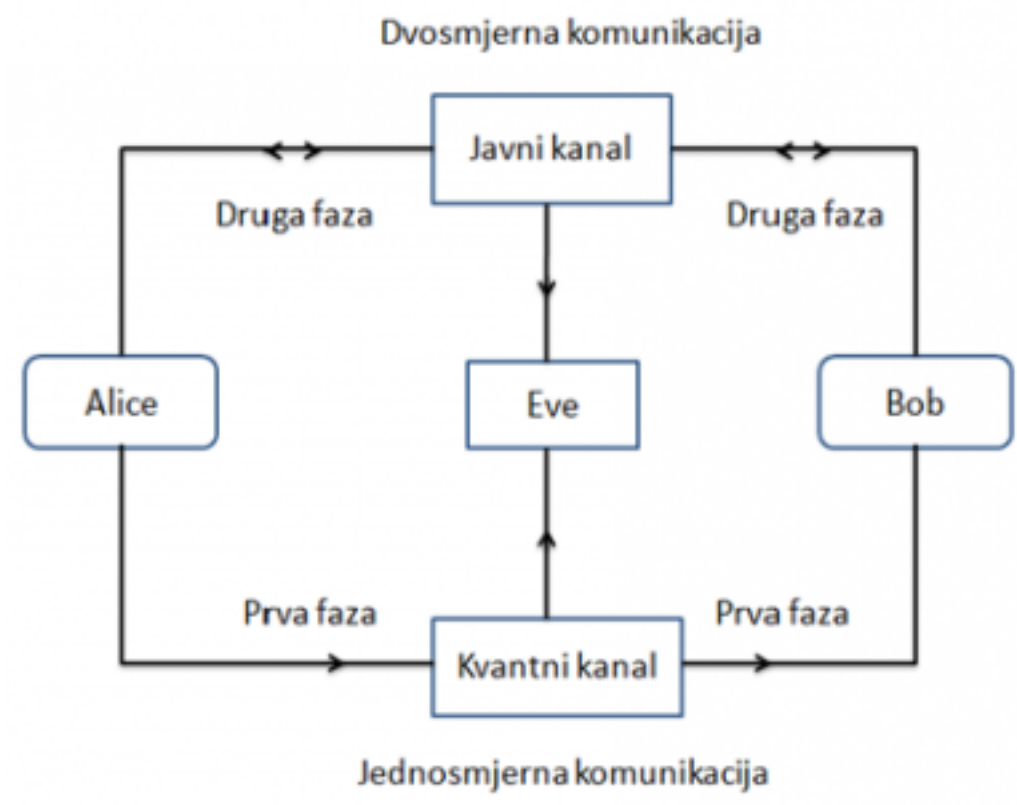
RSA enkripcija spada u asimetrične enkripcije, naziv je dobila po prvim slovima prezimena trojice kriptografa koji su ju osmislili, a njen sustav je riješio jedan od najvećih problema kriptografije, a to je kako poslati nekome šifriranu poruku, bez da se prethodno razmijenio ključ. Moderna tehnologija je omogućila komunikaciju na velikim udaljenostima što je dovelo do problema kako osigurati komunikaciju nesigurnim kanalom nad kojim postoji mogućnost prisluškivanja. U RSA sustavu, poruke su enkriptirane pomoću javnog ključa, što znači da je on javno poznat, ali to nije problem jer jednom kada je poruka enkriptirana pomoću javnog ključa, ona može biti dekriptirana jedino pomoću drugog, ali privatnog ključa. Svaki RSA sustav se sastoji od javnog i privatnog ključa. Sheme šifriranja javnog ključa razlikuju se od šifriranja simetričnog ključa, gdje postupak šifriranja i dešifriranja koriste isti privatni ključ. Te razlike čine šifriranje javnog ključa poput RSA korisnim za komunikaciju u situacijama kada prethodno nije bilo mogućnosti za sigurnu distribuciju ključeva. RSA enkripcija se najčešće koristi u kombinaciji sa nekom drugom enkripcijom ili za digitalne potpise koji mogu dokazati autentičnost i cjelovitost poruke. Generalno nije korišten za enkripciju cijele poruke ili datoteke, jer nije toliko efikasan i potrebno je više resursa nego kod simetrične enkripcije ključa. Kako bi se pojednostavnio odnosno

bio efikasniji, datoteka se enkriptira algoritmom za simetrične ključeve, a nakon toga sam simetrični ključ se enkriptira pomoću RSA enkripcije. [8]

3. KVANTNA KRIPTOGRAFIJA

Kao što je već prethodno navedeno, kriptografija funkcionira na način da je informacija dostupna samo osobama koja šalje i onoj koja prima poruku (Alice i Bob). Kada je kriptografija tek bila osmišljena, ona se bazirala na sigurnosti cijelog procesa, odnosno šifriranju i dešifriranju, dok se danas pomoću raznih programa mogu koristiti već gotovi i javni algoritmi, na način da se kao parametar unese ključ poruke i njen sadržaj, a da ona nije ugrožena. Naravno, postoji sustav koji je izuzetno siguran, riječ je o Vernamovoj šifri, koja se još naziva jednokratna bilježnica. Jedini problem kod nje je što generira ključ koji je jednake duljine kao i tekst poruke koju želimo šifrirati. Razlog zašto je to problem je razmjena tajnog ključa između osobe koja šalje i osobe koja prima poruku (Alice i Bob), ukoliko se šalje dugačka poruka, tada je dugačak i ključ, što je dosta nezgodno i preskupo slati sigurnim kanalom. Kao rješenje ovog problema osmislili su ključ koji ima neku konstantnu veličinu, a manji je od teksta te ga većina sustava koristi. Iako se riješio jedan problem, nastao je drugi, a to je da taj kanal više nije toliko siguran ukoliko je ključ kratak, što znači da je poruku lakše dešifrirati čak i bez znanja ključa, iako je mala šansa da se to uspije jer je potrebna velika procesorska snaga, a i potrebno je određeno vrijeme kako bi se to ostvarilo. Komunikacijski kanal je siguran za komunikaciju tek nakon što se ključ razmjeni, što se smatra kao jedna od mana klasične kriptografije. Taj problem je poznat pod nazivom „kvaka 22“. Osim toga, ako pošiljatelj i primatelj (Alice i Bob) uspiju međusobno razmijeniti ključ kroz komunikacijski kanal, nema garancije da je taj ključ u stvari sigurno poslan, odnosno da treća strana (Eve) nije prilikom prisluškivanja uspjela doznati sadržaj ključa. Nama poznata kriptografija ne zna kako riješiti taj problem, odnosno nema rješenja. Zbog toga je osmišljena kvantna kriptografija, a ona funkcionira na način da obavlja kvantnu razmjenu ključeva, zbog čega je komunikacija u potpunosti sigurnija za Alice i Bob. Kvantna kriptografija primjenjuje principe kvantne mehanike kako bi se poruke koje se šalju komunikacijskim kanalom šifrirale na način da se nikad ne može saznati njen sadržaj, odnosno ukoliko treća strana (Eve) pokušava doznati sadržaj, pošiljatelj i primatelj (Alice i Bob) bi bili obavješteni, jer se iskorištavaju kvantna stanja. Kompleksnost kvantne kriptografije je u stvari u kvantnoj mehanici, odnosno njeni principi, a to je da su čestice nesigurne i da mogu istovremeno postojati na više mjesta ili u više stanja. Fotoni su generirani nasumice, odnosno mogu se pojaviti u dva stanja. Ukoliko se dođe do čestice i pokuša izmjeriti njene fizikalne veličine, to neće biti moguće, jer se ne mogu sve veličine istovremeno mjeriti bez da se promjene ili raspadnu. Ta neodređenost, odnosno da ne postoji mogućnost doznati sve o česticama, se pokušava iskoristiti za generiranje tajnog ključa. Neka kvantna svojstva čestice

moguće je klonirati, ali ne i cijelu česticu. Kada fotoni putuju, oni se kreću kroz polarizacijski filter, koji im nasumično daje jedan od 4 moguća polarizacijska stanja, a to su: vertikalni, horizontalni, 45 stupnjeva desno ili 45 stupnjeva lijevo. Fotoni putuju do osobe koja treba primiti poruku, ta osoba koristi dva razdjelnika (horizontalni/vertikalni ili dijagonalni) kako bi „pročitao“ polarizaciju svakog fotona. Osoba koja prima poruku ne zna koji razdjelnik treba koristit te on treba pogoditi koji koristiti. Nakon što je poslana sekvenca fotona, osoba koja je primila poruku kaže pošiljatelju koji razdjelnik je koristio za svaki foton u sekvenci koja je poslana te pošiljatelj uspoređuje informaciju sa sekvencom polarizacije koja je korištena za slanje ključa. Fotoni koji su „pročitani“ pomoću krivog razdjelnika se uništavaju te rezultat sekvence bitova postaje ključ. Ukoliko foton bude pročitan ili kopiran od strane prisluškivača njegovo stanje se mijenja. Drugim riječima, ne može se „pročitat“ foton i proslijediti ga ili napraviti njegovu kopiju bez da se to ne otkrije. [9], [10], [11]



Sl.3.1. Prikaz kvantnog komunikacijskog kanala [4]

4. KVANTNI PROTOKOLI

Kako je kvantna kriptografija zasnovana na kvantnoj mehanici, tako ona iskorištava svojstva kvantnih stanja radi sigurnosti sustava. Za distribuciju kvantnih ključeva postoji nekoliko načina, ali se oni dijele u dvije skupine, a to je da li su qubitovi nezavisni jedni o drugima ili nisu. [11], [12]

4.1. Protokoli „pripremi i izmjeri“

Mjerenje veličina je dio kvantne mehanike. Prema tome, kao što je već navedeno, kada se izvodi mjerenje nepoznatog kvantnog stanja ono se mijenja. Naziva se još i kvantna neodređenost. To se iskorištava kod detektiranja prisluškivanja komunikacijskog kanala te da bi se isto tako dobio izračun koliko je presretnutih informacija. Ovo automatsko otkrivanje treće strane nije moguće napraviti klasičnom kriptografijom. [11], [12], [14]

4.2. Protokoli zasnovani na isprepletenosti

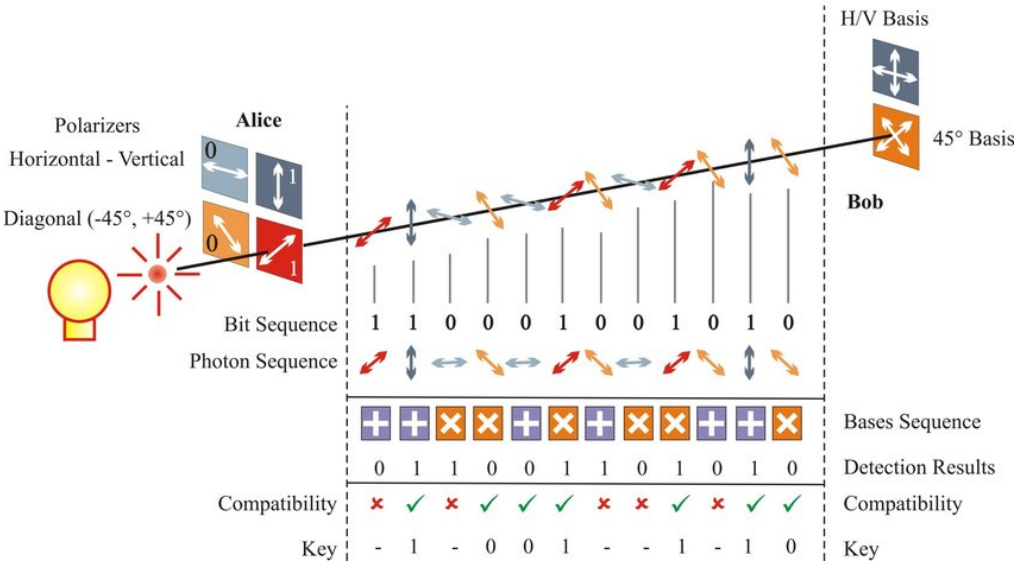
Protokol isprepletenosti kaže, da se dva ili više objekta mogu opisati kombiniranim kvantnim stanjem ukoliko su oni povezani, međutim kada se radi mjerenje na jednom objektu, utjecati će i na drugi. Ukoliko se povezani par šalje komunikacijskim kanalom te treća strana pokuša prisluškivati, odnosno presresti čestice, tada dolazi do promjene cjelokupnog sustava. Ova dva pristupa se mogu podijeliti u tri skupine protokola:

- diskretne varijable
- kontinuirane varijable i
- distribuirano fazno referentno kodiranje

Protokoli koji su nastali na diskretnim varijablama su i prvi koji su smišljeni te su i najrasprostranjeniji. Preostali protokoli su orijentirani na prevladavanje praktičkih ograničenja tijekom eksperimentiranja. [11], [12], [14]

4.3. BB84 protokol

Protokol BB84 osmišljen je kao prvi kvantni kriptografski protokol 1984. godine, a njegovi izumitelji su Charles Bennett i Gilles Brassard. Dvije strane (Alice i Bob) međusobno su povezane kvantnim komunikacijskim kanalom kojim je moguća razmjena kvantnih stanja te su oni povezani javnim klasičnim komunikacijskim kanalom, npr. internetom, a on ne mora biti siguran iz razloga što je ovaj protokol osmišljen s pretpostavkom da treća strana može prisluškivati kanal. Ukoliko se radi o fotonima, tada je taj kanal optičko vlakno ili slobodan prostor. Informacije se kodiraju u neortogonalnim stanjima te je radi njih protokol siguran. Protokol BB84 ima dva stanja, a svaki par je konjugiran s obzirom na drugi par, a dva stanja kod jednog para su ortogonalna jedan prema drugom. Parovi koji imaju ortogonalno stanje nazivaju se baze.



Sl.4.3.1. Protokol BB84 šifriranje bita i princip dobivanja ključa [5]

Polarizacija stanja može biti linearna horizontalna – linearna vertikalna, linearna pod kutom od 45 stupnjeva – linearna pod kutom od 135 stupnjeva, cirkularna lijeva – cirkularna desna polarizacija. Dvije baze koje su iz različitih baza su međusobno konjugirane. Odabiru se dvije baze polarizacije te se svakom stanju u bazama dodijeli vrijednost 0 ili 1, a na taj način se stvara kvantna abeceda. Tijek komunikacije se odvija u više faza, kao prva je ta da Alice šalje Bobu tajni ključ putem komunikacijskog kanala te ona odabire za svaki impuls jednu od dviju baza polarizacije. Bob posjeduje detektor polarizacije, a on pomoću njega može mjeriti samo jednu polarizaciju, a razlog je taj što kvantna mehanika to ne dopušta, jer se tijekom mjerenja jedne polarizacije druga uništava. Bob ne zna koju polarizaciju treba izmjeriti te on to napravi nasumično, odnosno treba

ispravno postaviti detektor kako bi mogao registrirati ispravnu polarizaciju, ukoliko krivo postavi doći će do toga da izmjeri krivu polarizaciju, odnosno neko slučajno stanje koje može imati sličnu vrijednost, a on ne može razlikovati ta dva slučaja. Nakon što Bob odradi svoj dio zadatka, on obavještava Alice preko javnog kanala koje je orijentacije polarizatora koristio tijekom detekcije. Nakon što Alice kaže Bobu koje su bile ispravne, zadržavaju polarizacije koje su bile ispravno postavljene te na taj način dobivaju bitove koju u stvari čine tajni ključ. Iz razloga što Bob pogađa polarizacije, njegove šanse za pogodak su 50 posto, iste šanse ima i Eve koja prisluškuje kanal, ali budući da pogrešne pretpostavke mijenjaju polarizaciju impulsa, ona na taj način unosi greške u sustav. Alice i Bob to mogu lako otkriti jer oni nakon razmjene informacija uspoređuju svoje poslane i dobivene bitove, a nakon što je greška unesena u kanal, kvari se zajednički tajni ključ od Alice i Bob, odnosno njih dvoje dobivaju različite bitove. Nakon međusobnog uspoređivanja, protokol se završava, ukoliko postoje različiti bitovi, oni budu svjesni prisluškivanja, u suprotnom odbace bitove koji su korišteni za usporedbu, a ostale zadržavaju.[11], [14], [15]

Alice random bits	0	1	1	0	1	0	0	1
Alice sending Basis	+	×	+	×	×	+	×	+
Alice polarization	→	↖	↑	↗	↖	→	↗	↑
Eve basis measurement	+	+	×	×	+	×	×	+
Polarization Eve measures and sends	→	→	↗	↗	↑	↗	↗	↑
Bob basis measurement	+	×	×	×	+	×	+	+
Polarization Bob measures	→	↗	↗	↗	↑	↗	→	↑
Shared secret key	0	0	-	0	-	-	-	1
Error generated	√	x		√				√

Sl. 4.3.2. Protokol BB84 slanje i primanje bitova između Alice i Boba te pokušaj presretanja poruke od strane Eve [6]

4.4. Protokol B92

Protokol B92 zahtjeva samo jednu neortogonalnu kvantnu abecedu, dok BB84 zahtjeva dvije ortogonalne. Alice i Bob komuniciraju u dvije faze, kao i kod protokola BB84, prvo preko jednosmjernog kvantnog kanala, a zatim preko javno dvosmjernog kanala. Bob može detektirati poslani bit ili primiti dvosmisleni rezultat iz razloga što Alice koristi neortogonalni sustav, što znači da nema načina koji bi mogao jednoznačno razlučiti dva stanja polarizacije. Nakon izmjene poruka, Bob putem javnog kanala prenese Alice o rednim brojevima bitova koje je primio nedvosmisleno te oni postaju ključ, dok se ostali bitovi odbacuju. Ukoliko se pojavi veliki broj pogrešaka, to može naznačiti da je Eve prisluškivala kanal. Ostatak procesa se odvija kao i u BB84 protokolu, ali je protokol B92 puno jednostavniji, pa ga je isto tako lakše implementirati, međutim nije još u potpunosti dokazana njegova sigurnost. [12]

4.5. Protokol E91

Ime je dobio po Arthuru Ekertu koji ga je osmislio 1991. godine, te njegova shema koristi isprepleteni par fotona. Njih može bilo tko kreirati, pa čak i Eve. Distribucija fotona se odvija na način da Alice i Bob dobiju svaki po jedan foton iz svakog para. Postoje dva svojstva isprepletenosti fotona:

- njihova isprepletena stanja su savršeno povezana
- prilikom prisluškivanja uništava se koleracija između fotona na način koji Alice i Bob mogu detektirati

Alice i Bob svako za sebe bira bazu u kojoj bi se mjerio foton na način da Alice zapisuje bit koji je izmjeren, dok Bob zapisuje njegov komplement iz razloga što je foton koji je on odabrao ortogonalan onome kojeg je Alice zaprimila. Bitovi na kojima su se obavljale razne operacije mjerenja ne odbacuju, već ih koriste kako bi otkrili prisutnost Eve na način da koriste Bellove nejednadžbe, koja se koristi kako bi se odredilo ukoliko postoje lokalno skrivene varijable. Ako se ispostavi da je nejednadžba zadovoljena, to znači da je postojala prisutnost Eve. Nakon toga, odrađuje se isti proces kao i kod protokola BB84. [12], [14]

4.6. Protokol SARG04

SARG04 je definiran 2004. godine od strane Scarani i suradnici. On je izveden iz BB84 protokola. On je namijenjen u situacijama gdje se šalje Poissonov izvor putem informacija koji stvara slabe pulseve (njegova srednja vrijednost fotona koja je poslana je manja od 1) i informacije prima nesavršeni detektor. Njegova prednost je robusnost kod nekoherentnih PNS napada naspram BB84 protokola. [12]

4.7. Protokol šest stanja

Kako bi ovaj protokol predstavio stanja 0 ili 1, on koristi tri para ortogonalnih polarizacijskih stanja. Protokol ima veću otpornost na pogreške, što se ne može navesti kod protokola BB84 i B92, ali ima manu kod prijenosa ključa gdje je manje učinkovit. [12]

5. KVANTNA DISTRIBUCIJA KLJUČA (QKD – *Quantum Key Distribution*)

Kvantna kriptografija omogućuje kvantnu distribuciju ključa u situacijama gdje je moguće prisluškivanje kanala. Dio izmjerenih fotona može biti pogrešno detektiran između Alice i Bob, te ukoliko Eve pokuša izmjeriti fotone koje je Alice poslala, greške se mogu pojaviti jer Eve pokušava izmjeriti podatke o polarizaciji fotona. Takve situacije se ne mogu razlikovati jer prirodan i umjetan šum isto izgledaju. Preko procjene razine šuma, može se procijeniti količina informacija koje je Eve doznala. Protokol koji se odvija kroz tri faze omogućuje Alice i Bobu da na temelju toka podataka sa šumom dogovore manji tajni kriptografski ključ. Naziv te tri faze je sljedeći, procjena greške, poravnanje informacija i pojačanje privatnosti. [17]

5.1. Procjena greške

Princip procjene greške je sljedeći, Alice ili Bob odabiru nasumičan broj *t* prethodno poslanih bitova koji su izmjereni točno i javi ih primatelju. Primatelj informacija uspoređuje bitove sa svojim bitovima te javlja broj grešaka *e.* Nakon uzimanja dovoljno velikog uzorka, omjer *e/t* se smatra kao razumna procjena broja pogrešaka koje su neobjavljen dio ključa. [17]

5.2. Poravnanje informacija

Kako bi se osigurala identičnost oba ključa, koristi se poravnavanje informacija, koja predstavlja ispravku greške. Ovaj postupak provodi se javnim kanalom. Najvažnije je u što manjem broju slati informacije o ključevima, jer ukoliko Eve prisluškuje kanal, može ih lako pročitati. Uobičajeni protokol je kaskadni protokol. Kaskadni protokol se odvija u više faza, gdje se ključevi dijele na blokove u svakoj fazi i uspoređuje se njihov paritet. Ukoliko se uoči razlika u paritetu, tada se treba provesti binarna pretraga kako bi se pronašla greška te ispravila. Ovaj proces je rekurzivan, odnosno neće biti gotov skroz dok se ne usporede svi blokovi te dok se sve faze ne dovrše, a nakon tog procesa Alice i Bob će imati iste ključeve sa visokom vjerojatnošću. Eve će imati benefit od ovog procesa jer će i ona dobiti dodatne informacije o ključu. [17]

5.3. Pojačanje privatnosti

Pomoću ove metode mogu se ukloniti djelomične informacije koje Eve posjeduje o ključu Alice i Boba. Eve je do tih djelomičnih informacija došla na način da prisluškuje kvantni kanal dok se ključ prenosi ili preko javnog kanala kada se informacije poravnavanju. Eve posjeduje samo zanemarive informacije i novom ključu jer je pojačana privatnost kada Alice i Bob stvaraju novi, odnosno kraći ključ, a oni to postižu na način da se prilikom korištenja funkcija sažimanja kao ulazni parametar prima binaran niz dužine ključa, a na izlazu se daje binaran niz kraće dužine. Novi ključ se stvara nakon što Alice i Bob saznaju koliko je informacija Eve saznala o starom ključu iz količine grešaka koje postoje te na taj način Alice i Bob smanjuju mogućnost da Eve ima bilo kakve informacije o novonastalom ključu na vrlo male vrijednosti. [17]

6. QKD simulator

QKD simulator je web aplikacija koja simulira i analizira protokole kvantne distribucije ključeva. Ovaj simulator pokreće QKD Simulation Toolkit, koji ima mogućnosti uređivanja širokog spektra parametara za pojedinu komponentu i razne pod-protokole. U sljedećim slikama se može vidjeti pokretanje simulatora sa različitim postavkama. QKD simulator se odvija u 7 faza, a to su:

- BB84 kvantni prijenos (BB84 Quantum Transmission),
- Provjera izmjerenih podataka (Sifting),
- Provjera autentičnosti izmjerenih podataka (Sifting Authentication – Linear Feedback Shift Register (LFSR) Universal Hashing),
- Procjena pogreške (Reconciliation – Error estimation),
- Popravak pogrešaka (Reconciliation – Error Correction, Cascade),
- Potvrda i autentifikacija ispravka pogrešaka (Error Correction Confirmation and Authentication) i
- Pojačavanje privatnosti (Privacy Amplification). [18]

6.1. Prvi primjer QKD simulatora

Initial Configuration							
Property Qubit Count	Basis choice bias delta	Eve basis choice bias delta	Eavesdropping	Eavesdropping rate	Error estimation sampling rate	Biased error estimation	Error tolerance
500	0.5	0.5	1	0.1	0.2	0	0.11

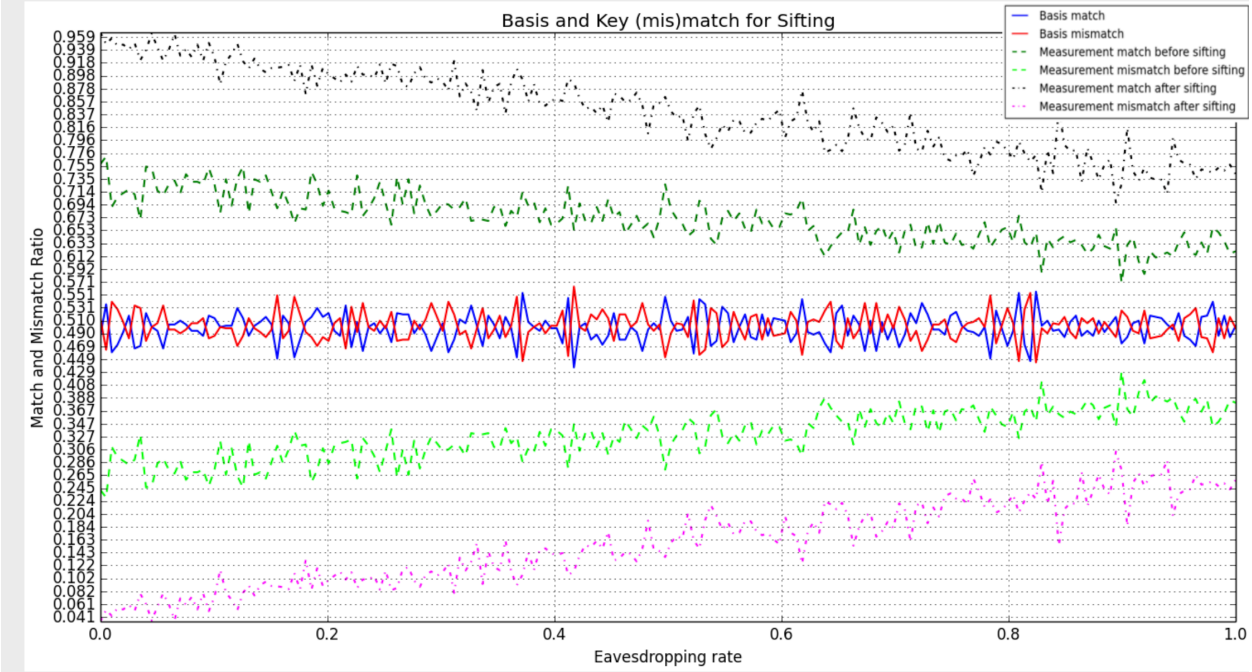
Sl. 6.1.1. Default postavke primijenjene za ovaj primjer[18]

Statistics and Overview

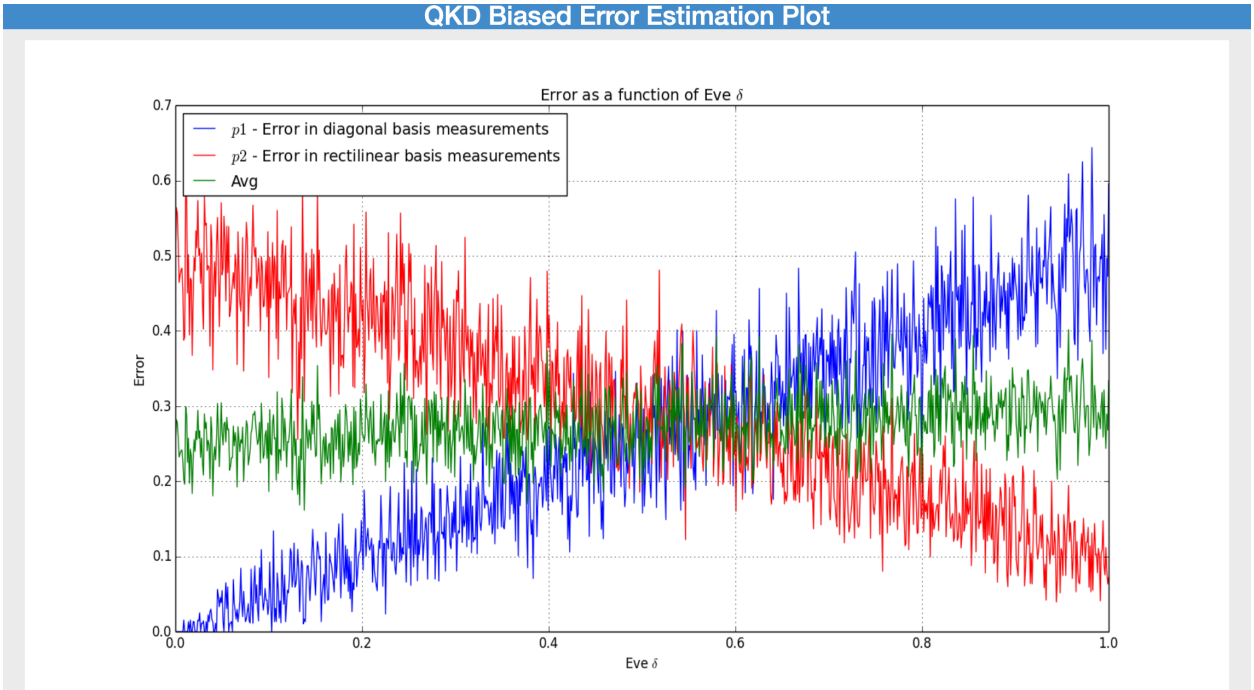
Property	Value
Initial number of qubits	500
Final key length	40
Estimated error	0.0784
Eavesdropping enabled	1
Eavesdropping rate	0.1
Alice/Bob basis selection bias	0.5
Eve basis selection bias	0.5
Raw key mismatch before error correction	0.0856
Raw key mismatch after error correction	0
Information leakage (Total number of disclosed bits)	146
Overall key cost for authentication	256
Key length before error correction	206
Bit error probability	0.0874
Bits leaked during error correction	114
Shannon bound for leakage	89
Security parameter	20

Sl. 6.1.2. Statistika i osvrt na rezultate [18]

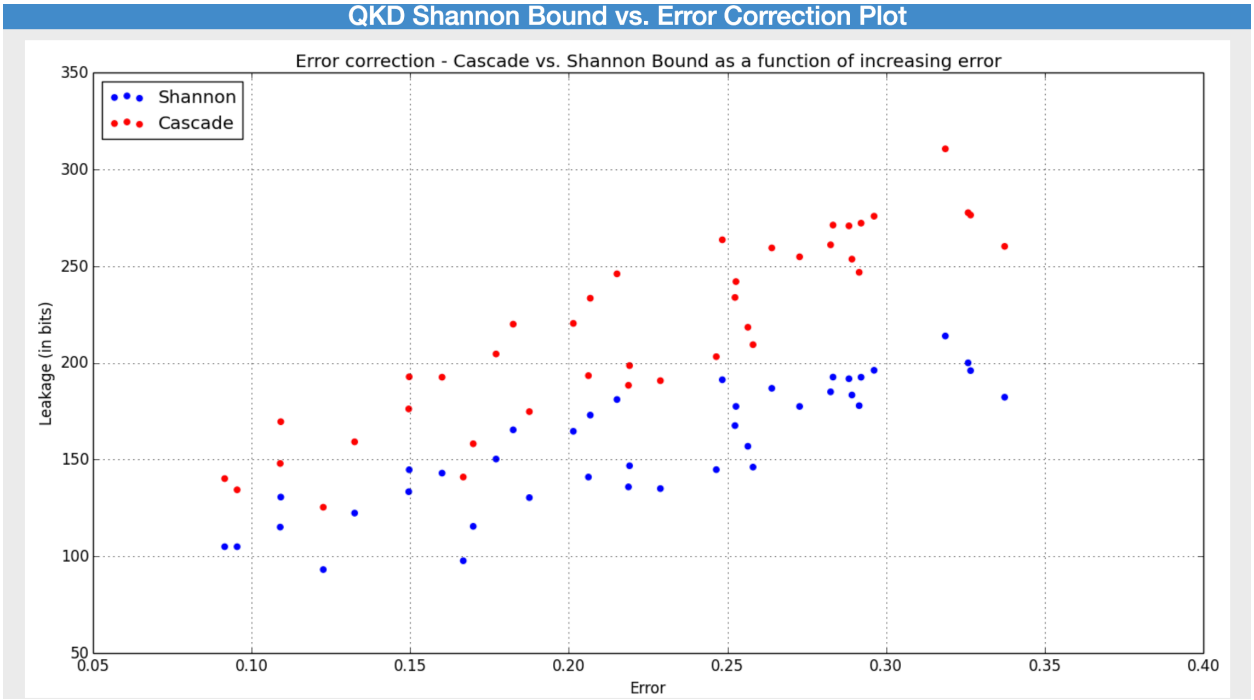
QKD Sifting Plot



Sl. 6.1.3. Omjer podudaranja i nepodudaranja [18]



Sl. 6.1.4. QKD procjena pogreške [18]



Sl. 6.1.5. QKD Shannon Bound naspram ispravke pogrešaka [18]

U prvom primjeru možemo vidjeti kako smo pripremili slijed od 500 *qubite* koje se šalje Bobu putem kvantnog kanala te se nakon tog odrađuje slučajan odabir polarizacije za svaki *qubite*. Možemo primijetiti Eve-ino prisustvo te ona presreće informacije koje se šalju. Budući da se polarizacija fotona mora pogađati, dolazimo do vrijednosti od 50% šanse za pogodak. Tako

možemo vidjeti da je Bob pogodio nešto više od 50% bitova, od ukupnih 500, on je pogodio 257. U drugoj fazi možemo primijetiti koliko su se rezultati poboljšali nakon provjere izmjerenih podataka, nego što su bili prije provjere. Nakon toga dolazimo u fazu autentifikacije provjere rezultata te Bob obavještava Alice što je uspio izmjeriti, sama autentifikacija ima svoj utrošak te je potrošeno 64 materijala u smislu ključnog materijala. Isto tako i baza ima svoj utrošak koji je jednak prošlom te i Alice-ine osnove koje je odabrala prilikom pripreme *qubite*-a. U fazi procjene pogrešaka, jedan od glavnih utjecaja ima stopa uzorkovanja. Premda je prag tolerancije procijenjen na 11%, a stopa uzorkovanja 0,2 dolazimo do dosta niske stope pogrešaka. Prilikom ispravljanja pogrešaka također dolazi do gubitka bitova, koristi se shema nazvana Cascade, koja se obavlja na javnom kanalu kako bi se pronašao i ispravio pogrešan bit u nizu te se ona ponavlja u više faza, odnosno onoliko koliko je to potrebno. Na kraju cijelog procesa dolazi do pojačavanja privatnosti kako mi umanjili Evino znanje stečeno na ključu prilikom prisluškivanja kanala, a to čine primjenom Toeplitzovim matricama te se definira sigurnosni parametar kako bi se dodatno Evino znanje o ključu sveli na proizvoljan iznos.

6.2. Drugi primjer QKD simulatora

Initial Configuration

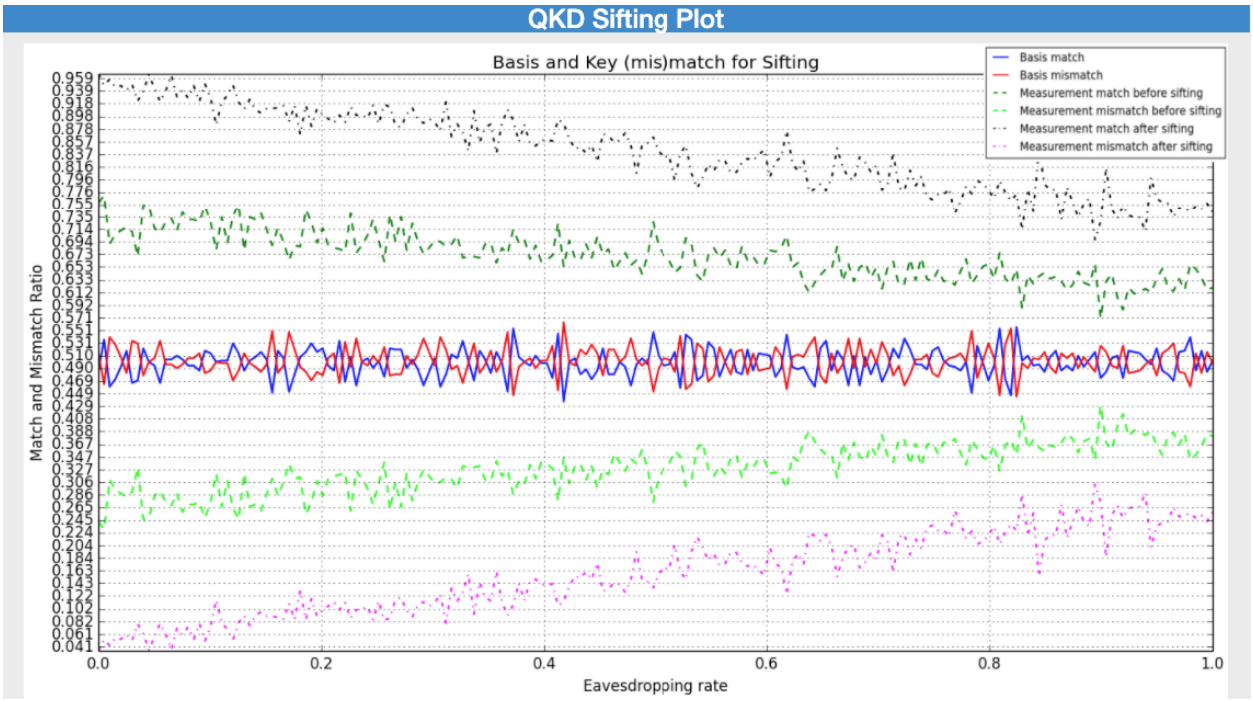
Property Qubit Count	Basis choice bias delta	Eve basis choice bias delta	Eavesdropping	Eavesdropping rate	Error estimation sampling rate	Biased error estimation	Error tolerance
600	0.3	0.2	0	0.35	0.25	0	0.15

Sl. 6.2.1. Početne postavke drugog primjera [18]

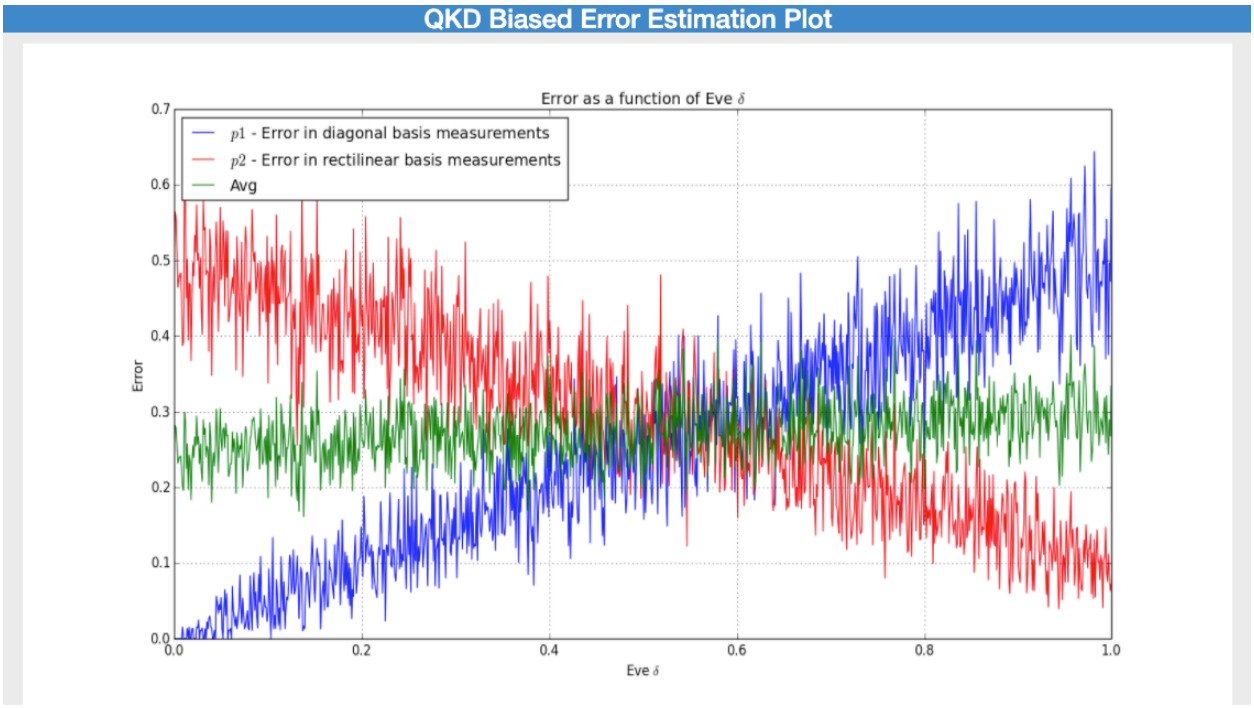
Statistics and Overview

Property	Value
Initial number of qubits	600
Final key length	183
Estimated error	0.0
Eavesdropping enabled	0
Eavesdropping rate	0.35
Alice/Bob basis selection bias	0.3
Eve basis selection bias	0.2
Raw key mismatch before error correction	0.0
Raw key mismatch after error correction	0
Information leakage (Total number of disclosed bits)	52
Overall key cost for authentication	256
Key length before error correction	255
Bit error probability	0.0
Bits leaked during error correction	20
Shannon bound for leakage	0
Security parameter	20

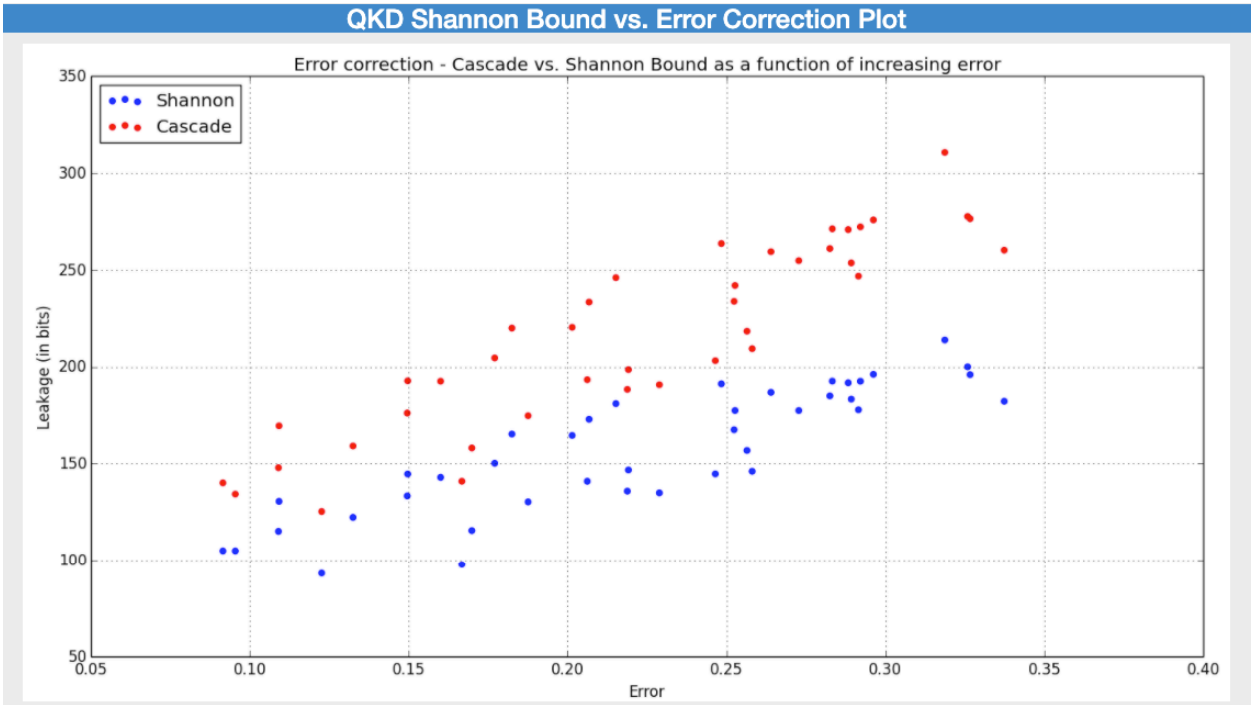
Sl. 6.2.2. Statistika i osvrt na rezultate [18]



Sl. 6.2.3. Omjer podudaranja i nepodudaranja [18]



Sl. 6.2.4. QKD procjena pogreške [18]



Sl. 6.2.5. QKD Shannon Bound naspram ispravka pogrešaka [18]

U ovom primjeru možemo primijetiti kako je broj početne vrijednosti slanja qubite-a nešto veći, ali Eve ne prisluškuje kanal što utječe na duljinu ključa na kraju cijelog procesa i može se vidjeti velika razlika u odnosu na prijašnji primjer, a isto tako i puno je manje informacija izgubljeno prilikom korištenja protokola.

6.3. Treći primjer QKD simulatora

Initial Configuration

Property Qubit Count	Basis choice bias delta	Eve basis choice bias delta	Eavesdropping	Eavesdropping rate	Error estimation sampling rate	Biased error estimation	Error tolerance
700	0.4	0.3	0	0.4	0.35	0	0.2

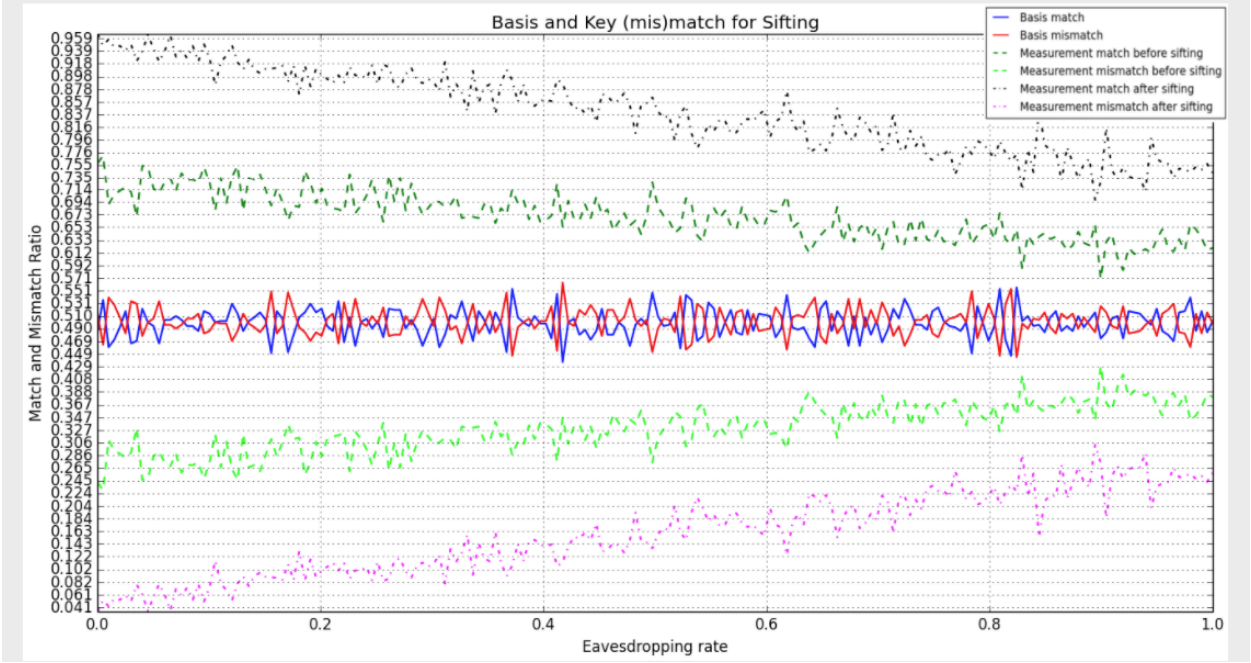
Sl. 6.3.1. Početne postavke drugog primjera [18]

Statistics and Overview

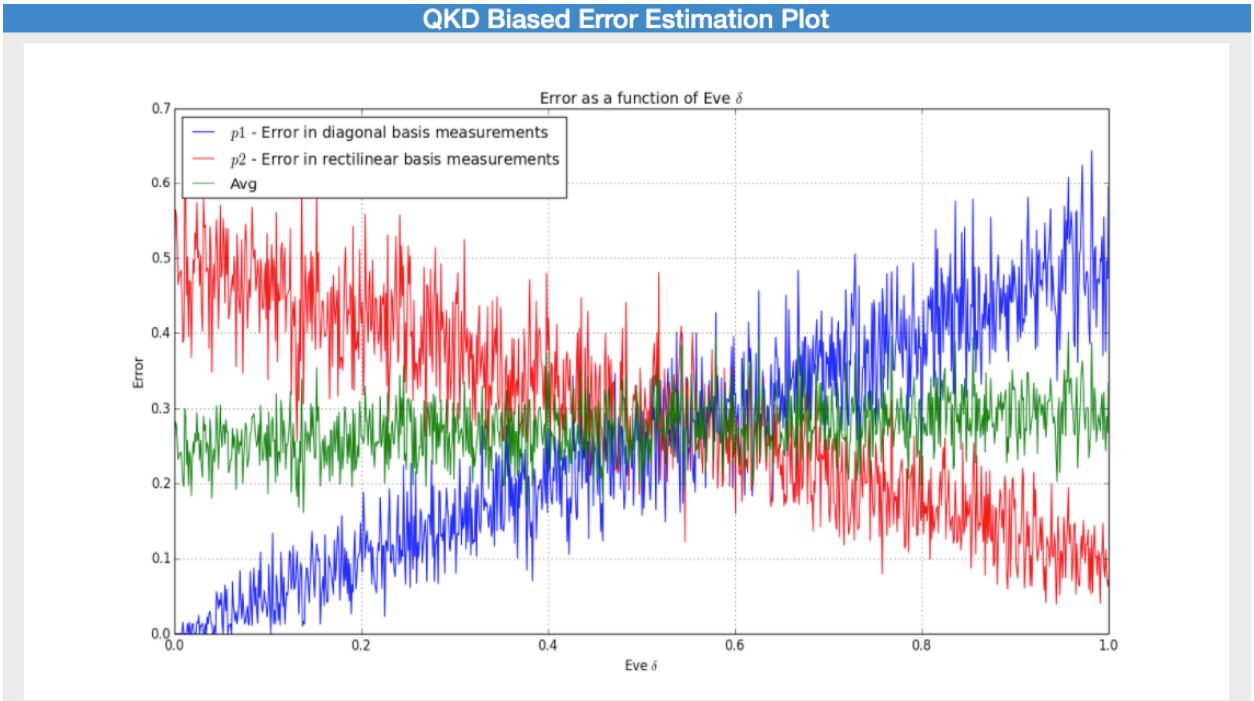
Property	Value
Initial number of qubits	700
Final key length	187
Estimated error	0.0
Eavesdropping enabled	0
Eavesdropping rate	0.4
Alice/Bob basis selection bias	0.4
Eve basis selection bias	0.3
Raw key mismatch before error correction	0.0
Raw key mismatch after error correction	0
Information leakage (Total number of disclosed bits)	52
Overall key cost for authentication	256
Key length before error correction	259
Bit error probability	0.0
Bits leaked during error correction	20
Shannon bound for leakage	0
Security parameter	20

Sl. 6.3.2. Statistika i osvrt na rezultate [18]

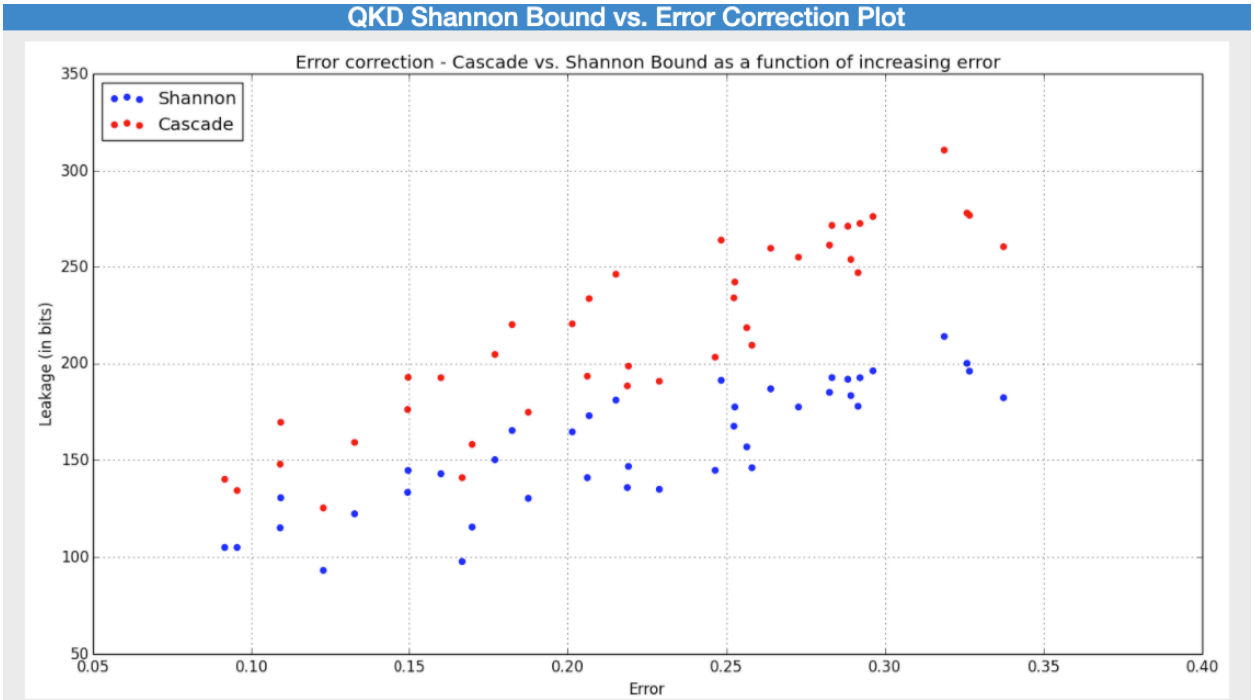
QKD Sifting Plot



Sl. 6.3.3. Omjer podudaranja i nepodudaranja [18]



Sl. 6.3.4. QKD procjena pogreške [18]



Sl. 6.3.5. QKD Shannon Bound naspram ispravka pogrešaka [18]

Treći primjer nije nešto previše različit od drugog osim što se može vidjeti da je povećana vrijednost početnih *qubite-a* koja je u ovom trenutno 700, s time je i ključ na kraju procesa veći, ali ništa značajno te Eve i dalje ne prisluškuje kanal.

6.4. Četvrti primjer QKD simulatora

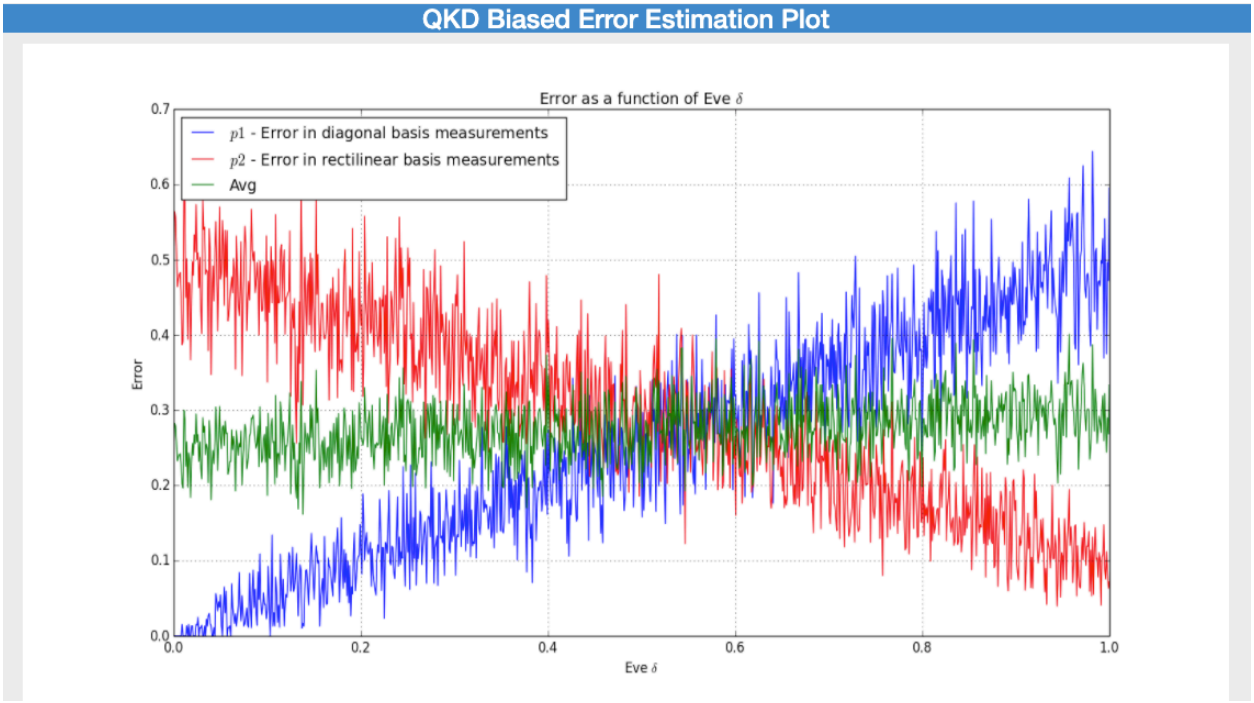
Initial Configuration							
Property Qubit Count	**Basis choice bias delta**	**Eve basis choice bias delta**	**Eavesdropping**	**Eavesdropping rate**	**Error estimation sampling rate**	**Biased error estimation**	**Error tolerance**
850	0.75	0.6	1	0.6	0.45	0	0.81

Sl. 6.4.1. Početne postavke drugog primjera [18]

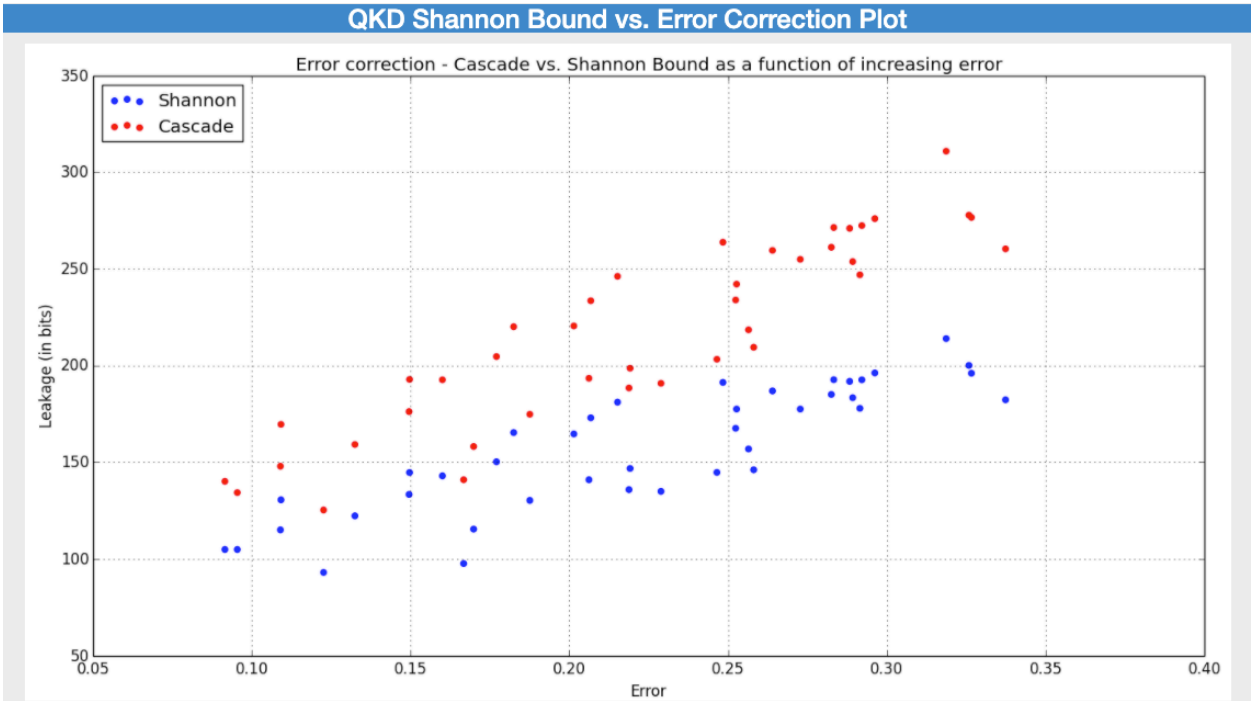
Statistics and Overview	
Property	**Value**
Initial number of qubits	850
Final key length	40
Estimated error	0.1504
Eavesdropping enabled	1
Eavesdropping rate	0.6
Alice/Bob basis selection bias	0.75
Eve basis selection bias	0.6
Raw key mismatch before error correction	0.1369
Raw key mismatch after error correction	0
Information leakage (Total number of disclosed bits)	242
Overall key cost for authentication	256
Key length before error correction	302
Bit error probability	0.1258
Bits leaked during error correction	210
Shannon bound for leakage	165
Security parameter	20

Sl. 6.4.2. Statistika i osvrt na rezultate [18]

Sl. 6.4.3. Omjer podudaranja i nepodudaranja [18]



Sl. 6.4.4. QKD procjena pogreške [18]



Sl. 6.4.5. QKD Shannon Bound naspram ispravka pogrešaka [18]

U četvrtom primjeru ima dosta različitih podataka nego u prijašnjim primjerima, ovdje je početni broj *qubite-a* postavljen na 850 te Eve opet prisluškuje kanal, a njene baze su povećane kao i stupanj prisluškivanja, što je dovelo do manjeg konačnog ključa jer je izgubljeno dosta informacija, iako je velika vrijednost početnih *qubite-a,* međutim Eve-ine postavke su utjecalo na to.

6.5. Peti primjer QKD simulatora

Initial Configuration

Property Qubit Count	Basis choice bias delta	Eve basis choice bias delta	Eavesdropping	Eavesdropping rate	Error estimation sampling rate	Biased error estimation	Error tolerance
970	0.25	0.4	1	0.7	0.15	0	0.85

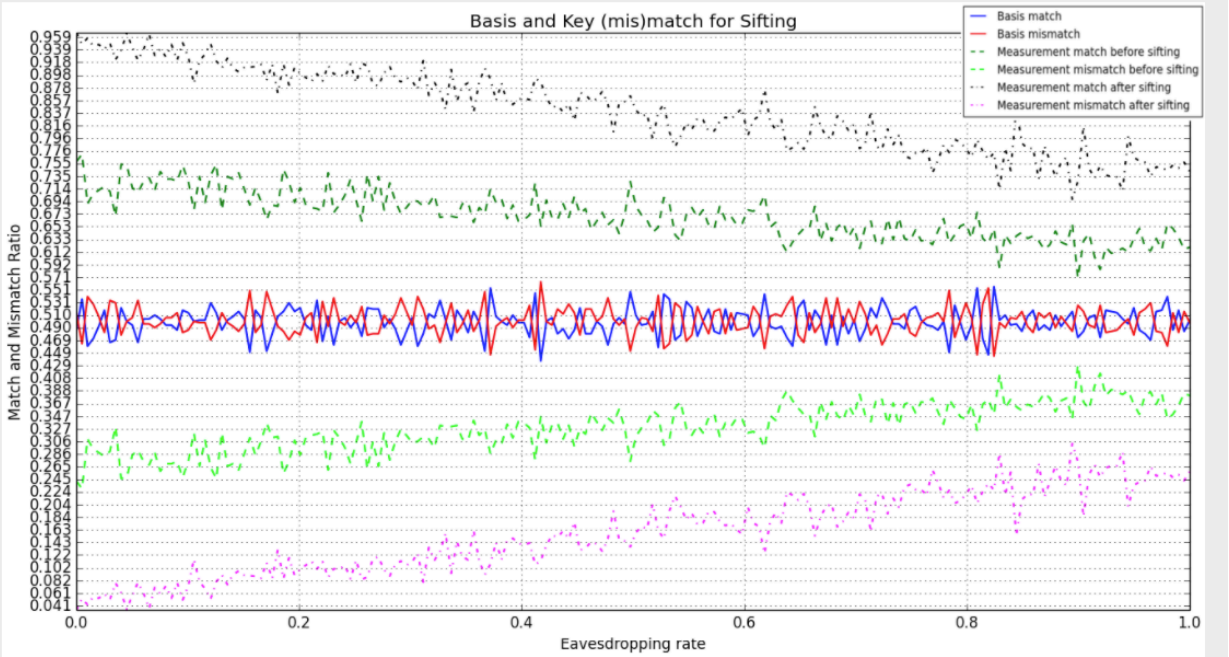
Sl. 6.5.1. Početne postavke drugog primjera [18]

Statistics and Overview

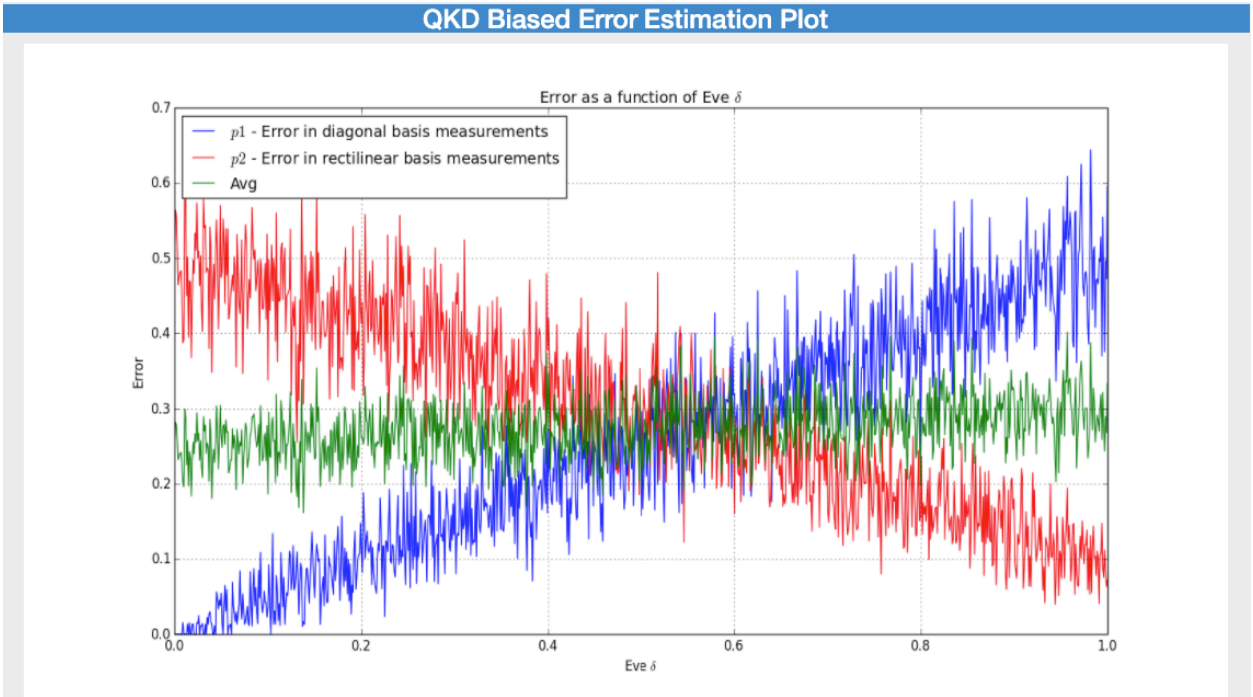
Property	Value
Initial number of qubits	970
Final key length	104
Estimated error	0.1429
Eavesdropping enabled	1
Eavesdropping rate	0.7
Alice/Bob basis selection bias	0.25
Eve basis selection bias	0.4
Raw key mismatch before error correction	0.1293
Raw key mismatch after error correction	0
Information leakage (Total number of disclosed bits)	396
Overall key cost for authentication	256
Key length before error correction	520
Bit error probability	0.1269
Bits leaked during error correction	364
Shannon bound for leakage	286
Security parameter	20

Sl. 6.5.2. Statistika i osvrt na rezultate [18]

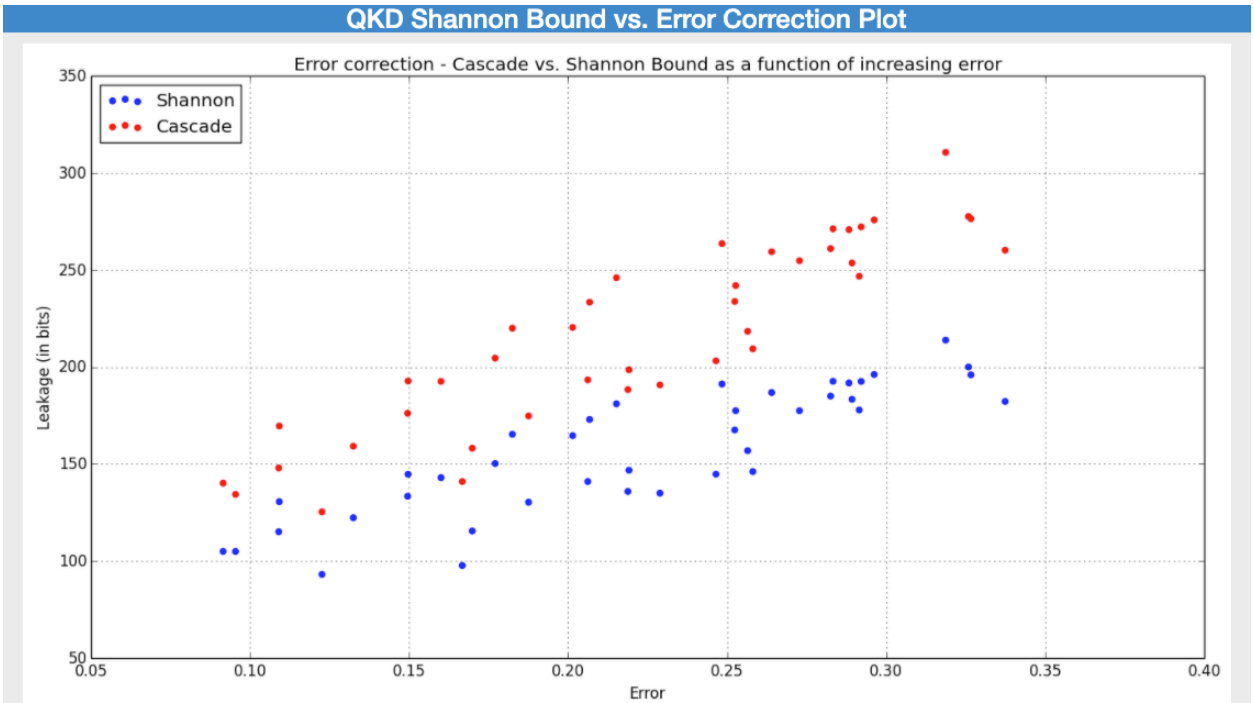
QKD Sifting Plot



Sl. 6.5.3. Omjer podudaranja i nepodudaranja [18]



Sl. 6.5.4. QKD procjena pogreške [18]



Sl. 6.5.5. QKD Shannon Bound naspram ispravka pogrešaka [18]

U zadnjem primjeru, vidimo da je vrijednost qubite-a koje Alice šalje Bobu putem kvantnog kanala poprilično velika, Eve opet prisluškuje kanal, međutim ovaj put su njene baze nešto manje. Iz razloga što se radi sa velikim brojem qubite-a, dolazi i do većeg gubljenja informacija, ali i duljine ključa, veće mogućnosti za pogreške.

6.6. Konačan osvrt na rezultate

Vrijednosti koje se nalaze u tablici ispod su vrijednosti iz prijašnjih 5 primjera QKD simulatora kako bi se na jednom mjestu moglo lakše vidjeti i usporediti što se događa kada se parametri izmjenjuju. Kako se povećava vrijednost početnih *qubite-a* i mijenjanje da li Eve prisluškuje kanal možemo vidjeti razne promjene u vrijednostima, broj pogrešaka, informacija koje su izgubljene, što se događa sa bitovima prije i nakon autentifikacije, kao i sama duljina ključa. Možemo primijetiti ukoliko Eve prisluškuje kanal da se duljina ključa smanjuje, a ukoliko ne prisluškuje on je veći. Naravno ta dva parametra nisu jedina i ključna podatka koji utječu na krajnji rezultat, tu su i stvari poput vrijednosti baze od Alice i Boba te Eve-ine. Koliko je protokol koristan, možemo vidjeti da nakon ispravka grešaka ima 0 neusklađenosti u ključevima. Parametar za sigurnost je kroz svaki primjer isti, a on iznosi 20.

Initial number of qubits	500	600	700	850	970
Final key length	40	183	187	40	104
Estimated error	0.0784	0.0	0.0	0.1504	0.1429
Eavesdropping enabled	1	0	0	1	1
Eavesdropping rate	0.1	0.35	0.4	0.6	0.7
Alice/Bob basis selection bias	0.5	0.3	0.4	0.75	0.25
Eve basis selection bias	0.5	0.2	0.3	0.6	0.4
Raw key mismatch before error correction	0.0856	0.0	0.0	0.1369	0.1293

Raw key mismatch after error correction	0	0	0	0	0
Information leakage (Total number of disclosed bits)	146	52	52	242	396
Overaall key cost for authentication	256	256	256	256	256
Key length before error correction	206	255	259	302	520
Bit error probability	0.0984	0.0	0.0	0.1258	0.1269
Bit leaked during error correction	114	20	20	210	364
Shannon bound for leakage	89	0	0	165	286
Security parametar	20	20	20	20	20

Tablica 6.6.1. Prikaz vrijednosti iz prethodnih primjera QKD simulatora [18]

7. MOGUĆI NAPADI

Uvjeti koji se moraju zadovoljiti kako bi kvantni kriptografski sustav bio siguran:

- Uređaji za enkripciju koji su u vlasništvu Alice i Boba, Eve ne može pristupiti
- Slučajni generator brojeva mora isključivo davati slučajne brojeve
- Kako bi klasični komunikacijski kanal bio autentificiran, mora koristiti sheme autentifikacije koje su u potpunosti sigurne [12], [15], [16], [17]

7.1. Napad „osoba u sredini“

Ovaj napada je najopasniji kada kvantna kriptografija nema autentifikaciju. Alice i Bob nisu u mogućnosti uspostaviti sigurno vezu ukoliko nisu provjerili identitet kao na primjer, bez provjere tajne poznate objema stranama. Ukoliko imaju tajnu, postoji shema savršeno sigurne autentifikacije (Carter-Wegman shema), koju mogu koristiti zajedno sa kvantnom distribucijom ključa kako bi eksponencijalno proširili ključ, te koristeći dio novog ključa kako bi autentificirali novo vrijeme za razmjenu podataka. [12], [15], [16], [17]

7.2. Napad razdvajanjem broja fotona (PNS napad)

Kao što je navedeno u protokolu BB84, Alice šalje Bobu kvantna stanja koristeći fotone. Koriste se oslabljeni laserski pulsevi za slanje kvantnih stanja, fotoni su raspodijeljeni po Poissonovoj razdiobi. Neki pulsevi ne moraju sadržavati fotone, neki mogu imati jedan, neki dva ili više. Eve najviše odgovara kada ima dva ili više fotona, na taj način Eve razdvoji dodatne fotone, a jedan pošalje Bobu. Eve svoj dio spremi u kvantnu memoriju, a Alice to ne može primijetiti dok ne otkrije kodirajuće baze. Za to vrijeme Eve može izmjeriti fotone i na taj način doći do podataka o ključu, bez da unosi grešku koju se može detektirati. [12], [15], [16], [17]

7.3. Hakerski napadi

Takvi napadi se baziraju više na neispravnost implementiranih protokola od njih samih. Ukoliko se koristi neispravna oprema, kod nasumičnog generatora ključeva generiraju se ključevi koji nisu sigurni. Još jedan od mogućnih napada je trojanski konj, u toj situaciji šalje se jaki svjetlosni puls između fotona koji se šalju komunikacijskim kanalom. Benefit toga je da se puls svjetlosti reflektira nazad i time šalje polarizacije koje su korištene. Neki od ostalih napada su: napad lažnim stanjima, napad vremenskim pomakom i napad promjenom faze. Sve hakerske napade je relativno lako zaustaviti ukoliko se oprema nadograđuje i modificira. [12], [15], [16], [17]

7.4. DoS napad (Denial of Service)

Kvantna kriptografija za prijenos informacija koriste medije kao što je optički kabel ili zrak, pa se takav napad može odraditi na način da se blokira, prisluškuje ili prekida linija. [12], [15], [16], [17]

8. KVANTNA KRIPTOGRAFIJA DANAS

Koliko se kvantna kriptografija razvila to mogu dokazati razni „pokusi“. Prva kriptografska mreža koja je konstantno u pogonu, a da nije dio laboratorijskih pokusa je poveznica šest mrežnih čvorova koja spaja tvrtke BBN Technologies i sveučilišta Harvard i Boston. Ključevi se šalju putem kvantnog kanala, a poruke koje su se kriptirale pomoću tog ključa šalju se javnim kvantnim kanalom putem interneta. 2004. godine obavio se prvi bankarski prijenos čeka, koji je prenesen u austrijsku banku. Kroz dugi niz godina počeli su se obavljati razni prijenosi na većim udaljenostima, prvi takav dogodio se 2005. godine kada se obavio prijenos na lokaciju koja je na udaljenosti od 10 kilometara, naravno uz pomoć ključeva koji su distribuirani kvantnom enkripcijskom vezom. Isto tako, prvo računalo koje je u potpunosti zaštićeno kvantnom kriptografijom bio je implementiran 2008. godine, a predstavljen je u Beču, te je koristio mrežu dugačku 200 kilometara koja je spajala 6 raznih lokacija. Najveća udaljenost koja je postignuta u slobodnom prostoru je 144 kilometara duga, koja je predstavljala udaljenost dva otoka u Kanarskom otočju. Svi ovi eksperimenti, a navedeni su samo neki, dokazuju kako bi prijenos do satelita bio moguć, jer atmosfera ima manju gustoću na većim visinama. Do sada je zabilježen rekord u brzini slanja bitova, a to je 4 milijuna bitova u sekundi kroz optički kabel koji je bio dužine 1 kilometar, a to je ostvario NIST (National Institute of Standards and Technology). IBM i Intel su objavili 2018. godine kako su napravili kvantno računalo za 50 i 49 *qubite,,* samo za usporedbu, to je jednako milijun bitova klasičnom računalu. RSA i ostale asimetrične algoritme kvantna kriptografija može probiti, lako može doći do njihovih javnih ključeva, što dokazuje njen razvoj i njenu jačinu, dok kod AES nije takva situacija, on se i dalje smatra sigurnim, jer koriste veće ključeve. Iako kvantna računala trenutno ne predstavljaju veliku prijetnju, jer su još u svojim počecima, naravno treba se pripremati za dane kada oni postanu stvarnost, odnosno kada dobiju svoju punu moć, ali znanstvenici pretpostavljaju da se to neće dogoditi još skorije vrijeme.[12], [19], [20]

9. ZAKLJUČAK

Kriptografija je u svojim počecima imala jako velik doprinos u zaštiti poruka od onih kojima ona nije bila namijenjena. Njena zadaća je da omogući dvjema osobama očuvati tajnost poruke, pa čak i u nesigurnim komunikacijskim kanalima. Kriptografija se dugi niz godina primjenjivala pretežito u vojne i diplomatske svrhe. Kako su godine prolazile, otkrivali su se razni načini kako bi se dekriptirao sadržaj poruke. Danas, kako je tehnologija napredovala, proširile su se mogućnosti komunikacije, poruke se mogu slati iako su pošiljatelj i primatelj na velikoj udaljenosti, što u stvari dovodi do situacija gdje je moguće presresti poruku. Iz raznih primjera, znanstvenici su otkrili kako nije toliko bitan sam kriptosustav, već njegov tajni ključ, što je dovelo do kvantne kriptografije. Kvantna kriptografija je u zadnja dva desetljeća izrazito napredovala u razvoju. U počecima se eksperimentiralo slanjem fotona kroz cijev dužine samo 0.30 metara. Kako je napredovala tehnologija to je dovelo do većeg obujma korištenja kvantne kriptografije, iako se očekuje kako će biti još veći s obzirom da je jako visoka cijena kvantnih kriptografskih sustava, ali i to što se kvantna kriptografija svrstava u znanstvenu fantastiku. Kvantna kriptografija čeka da kvantna računala postanu stvarnost što bi dovelo do njenog jako velikog razvitka. Kada se to ostvari, algoritmi klasične kriptografije će oslabiti, odnosno neće više pružati kvalitetnu sigurnost i zaštitu, što će dovesti i problem zaštite podataka koji su ranije zaštićeni klasičnim kriptografskim sustavima, a ti podaci trebaju iz nekog razloga još dug niz godina zaštite. Kvantna kriptografija nije u potpunosti sigurna, ali je definitivno sigurnija od klasične kriptografije, njeni napadi se mogu spriječiti unapređenjem opreme i njenom modifikacijom. [17]

10. LITERATURA

1. M. Rouse, Cryptography, April, 2020. https://searchsecurity.techtarget.com/definition/cryptography (9-9-2020)
2. A. Dujella, M. Maretić. „Kriptografija“, Element, Zagreb, 2007. (9-9-2020)
3. https://web.math.pmf.unizg.hr/~duje/kript.html (18-9-2020)
4. https://security.foi.hr/wiki/index.php/Kvantna_kriptografija.html (18-9-2020)
5. researchgate.net/figure/Key-exchange-in-the-BB84-protocol-implemented-with-polarization-of-photons-adapted-from_fig1_324115273 (18-9-2020)
6. https://www.semanticscholar.org/paper/Analysis-of-Various-Attacks-over-BB84-Quantum-Key-Rahul-Heeren/200099146ddfb8c2de14fb5698f0290d70d912c0 (18-9-2020)
7. D. Crawford, How does AES encryption work?, February 2019. https://proprivacy.com/guides/aes-encryption (16-9-2020)
8. J. Lake, What is RSA encryption and how does it work?, December, 2018 (16-9-2020) https://www.comparitech.com/blog/information-security/rsa-encryption/
9. D. Cardinal, „Quantum Cryptography Demystified: How it Works in Plain Language“, March, 2019. (9-9-2020) https://www.extremetech.com/extreme/287094-quantum-cryptography
10. M. Korolov, D. Drinkwater, „What is quantum cryptography? It's no silver bullet, but could improve security“, March, 2019. (9-9-2020) https://www.csoonline.com/article/3235970/what-is-quantum-cryptography-it-s-no-silver-bullet-but-could-improve-security.html
11. QuantumXChange, „Quantum Cryptography, Explained“ (9-9-2020) https://quantumxc.com/quantum-cryptography-explained/
12. S. Picek, M. Golub, „Kvantna kriptografija: razvoj i protokoli“, Opatija, 2009. https://www.bib.irb.hr/397255?&lang=EN&rad=397255
13. M.Mafu, M. Senekane, „Security of Quantum Key Distribution protocols“, May, 2018. https://www.intechopen.com/books/advanced-technologies-of-quantum-key-distribution/security-of-quantum-key-distribution-protocols (9-9-2020)
14. S.J. Lomonaco, „A Quick Glance at Quantum Cryptography“, 1998. (9-9-2020)
15. B. Schneier, „Applied Cryptography“, 2nd Edn. John Wiley & Sons, 1996. (9-9-2020)

16. D. Hrg, L. Budin, M. Golub, „Quantum Cryptography and Security of Information Systems“, Proceedings of the 15 th International Conference on Information and Intelligent Systems, IIS2005, Varaždin, Croatia, 2004. (9-9-2020)
17. H. C. A. Van Tilborg, „Encyclopedia of Cryptography Security“, Springer, 2005. (9-9-2020)
18. https://qkdsimulator.com/ (20-9-2020)
19. Scientific American Magazine, Best-Kept Secrets, p. 65-69, January 2005. (16-9-2020)
20. C. Dodt, Quantum computation and its effects on cryptography, March, 2019 (17-9-2020) https://resources.infosecinstitute.com/quantum-computation-and-its-effects-on-cryptography/#gref

11. SAŽETAK

Radi sve veće potrebe za zaštitom podataka, pogotovo u današnje vrijeme kada je internet svuda, razvijaju se sustavi koji tu tajnost mogu omogućiti. U današnje vrijeme najčešće korišteni su klasični kriptografski sustavi te kriptografski sustavi koji imaju javni ključ. Nažalost, niti jedan kriptografski sustav ne može riješiti poznati problem zvan „kvaka 22“. Zahvaljujući velikom usponu tehnologije, njenim razvitkom osmišljena je u potpunosti nova vrsta kriptografije, kvantna kriptografija. Uz pomoć kvantne kriptografije lakše možemo otkriti da li netko prisluškuje komunikacijski kanal. Međutim, iako se kvantna kriptografija smatra veoma sigurnom, nije uvijek tako, ali ako je sigurnija od klasične zašto se ona ne koristi više? Cilj ovog rada je pojasniti osnovne mogućnosti kvantne kriptografije i njene protokole, ali i predočiti njene nedostatke.

12. ABSTRACT

Due to the growing need for dana protection, especially nowadays when the Internet is everywhere, systems are being developed that can enable this secrecy. Nowadays, the most commonly used are classic cryptographic systems and cryptographic systems that have a public key. Unfortunately, no cryptographic system can solve a known problem called „handle 22“. Thanks to the great rise of technology, its development has led to a completely new type of cryptography, quantum cryptography. With the help of quantum cryptography, we can more easily detect if someone is eavesdropping on a communication channel. However, although quantum cryptography is considered very secure, it is not always so, but if it is more secure than classical why it is not used more often? The aim of this paper is to explain the basic possibilities of quantum cryptography and its protocols, but also to point out its shortcomings.