Kvantna kriptografija: razvoj i protokoli

Stjepan Picek
Ring Datacom d.o.o.
Trg J. J. Strossmayera 5, Zagreb, 10000, Hrvatska
Telefon: +38598226407 E-mail: stjepan@ring.hr

Marin Golub
Fakultet elektrotehnike i računarstva
Unska 3, Zagreb, 10000, Hrvatska
Telefon: +38516129967 E-mail: marin.golub@fer.hr

Sažetak - Kako se razvija potreba za tajnošću podataka tako se razvijaju i sustavi koji bi tu tajnost trebali omogućiti. Danas se najčešće koriste klasični kriptografski sustavi i kriptografski sustavi s javnim ključem. No, niti jedan od tih sustava ne omogućuje rješenje čuvene „kvake 22" kriptografije. Zahvaljujući intenzivnom razvoju kvantne mehanike, u posljednjih 30-ak godina pojavila se posve nova vrsta kriptografije: kvantna kriptografija. Njezin je najveći doprinos mogućnost otkrivanja prisluškivanja komunikacijskog kanala od treće osobe. Je li to doista tako? Postavlja se pitanje, ako je kvantna kriptografija toliko dobra, zašto nije u široj uporabi? Smisao ovog rada je, s jedne strane, definirati osnovne mehanizme kvantne kriptografije i protokole, a sa druge strane ukazati na nedostatke kako one vezane uz mogućnosti današnjeg sklopovlja tako i sigurnosne nedostatke u protokolima.

I. UVOD

Svrha kriptografije je prijenos informacija na način da su one dostupne samo osobi kojoj su i namijenjene. Na početku je sigurnost kriptiranog teksta ovisila isključivo o tajnosti cijelog procesa kriptiranja i dekriptiranja. Danas se koriste šifre čiji su algoritmi javno poznati a da to ne ugrožava sigurnost kriptirane poruke. U takvim sustavima tajni ključ poruke i jasni tekst se unose kao parametri u algoritam.

Ako se želi koristiti savršeno siguran kriptografski sustav, onda je odgovor Vernamova šifra, poznatija pod imenom jednokratna bilježnica. Jednokratna bilježnica koristi slučajno generirani ključ K jednake dužine kao i poruka koja se želi šifrirati. Glavni problem kod takvog sustava je potreba za razmjenom tajnog ključa između pošiljatelja i primatelja poruke (Ana i Branko). U većini slučajeva, ključ *K* je veoma dugačak i time ga je nepraktično i preskupo slati sigurnim kanalom. Ako Ana padne u napast da dva puta iskoristi isti ključ tada se njen šifrirani tekst mijenja iz savršeno sigurnog u lako provaljiv. Tako se danas, u većini praktičnih kriptosustava, koristi ključ *K* koji je konstantne veličine i obično je puno kraći od dužine jasnog teksta. Kao rezultat toga kriptosustavi više nisu savršeno sigurni. Međutim, pažljivim odabirom metode enkripcije i ključa može se sustav smatrati praktično sigurnim. Praktično siguran kriptosustav znači da iako napadač (Iva) može teoretski dekriptirati poruku bez znanja ključa, on to vjerojatno neće uspjeti. Razlog tome je što su procesorska snaga i vrijeme potrebno za napad najčešće iznad napadačevih mogućnosti.

U svakom slučaju, slaba točka klasičnih kriptografskih sustava je što se sigurna komunikacija može odvijati tek nakon što je ključ sigurno razmijenjen komunikacijskim kanalom. Taj problem se često naziva „kvaka 22" kriptografije: prije nego Ana i Branko mogu tajno komunicirati, oni moraju tajno komunicirati.

Postoji i dodatak tog problema, poznat pod imenom „kvaka 22a": čak ako Ana i Branko uspiju razmijeniti ključ preko sigurnog komunikacijskog kanala, ne postoji mehanizam u klasičnoj kriptografiji koji može garantirati da je ključ poslan sigurno, tj. da ga Iva nije uspjela prisluškivanjem komunikacijskog kanala saznati.

Tu na scenu stupa kvantna kriptografija – kvantna razmjena ključeva, koja omogućuje dvjema stranama (Ani i Branku) komunikaciju koja je u potpunosti sigurna.

Kvantna kriptografija koristi prirodnu neodređenost kvantnog svijeta. Pomoću nje se može uspostaviti komunikacijski kanal koji nije moguće prisluškivati bez ometanja prijenosa, tj. dva korisnika koja međusobno komuniciraju mogu otkriti prisustvo treće strane koja pokušava saznati ključ. Također, osoba koja prisluškuje ne može kopirati nepoznate kvantne bitove - qubite, tj. nepoznata kvantna stanja, zbog teorema o ne-kloniranju koji su prvi iskazali Wooters i Zureck. [2]

Kvantna kriptografija služi samo za dobivanje i distribuciju ključa, a ne za prijenos poruka. Tako generirani ključ može poslužiti u nekom kriptosustavu za kriptiranje i dekriptiranje poruke.

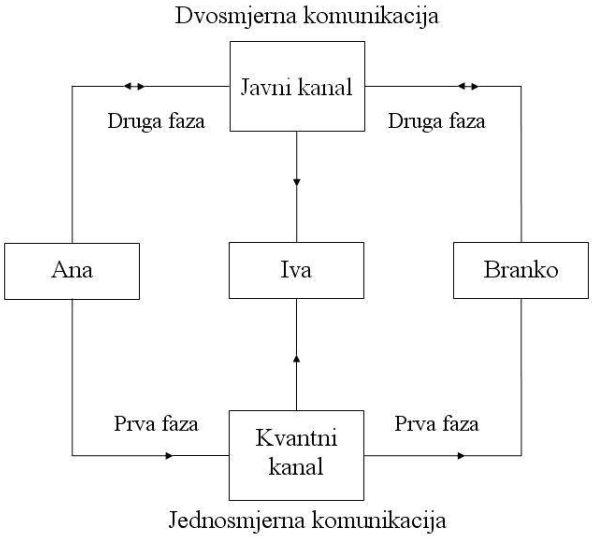
Kvantna mehanika kaže da se čestice ne nalaze na samo jednom mjestu. One se nalaze na nekoliko mjesta odjednom, s određenim vjerojatnostima da postoje na različitim mjestima. Međutim, to sve nema smisla dok ne dođe znanstvenik i „uhvati" česticu koja se nalazi na nekom mjestu. Uhvaćenoj čestici nije moguće istovremeno izmjeriti sve njene fizikalne veličine. Mjerenjem neke od veličina čestice, uništava se svaka mogućnost mjerenja nekog drugog njenog svojstva. Ta neodređenost se može iskoristiti za generiranje tajnog ključa. Dok putuju, fotoni titraju pod nekim kutem. Kada velika grupa fotona titra u istom smjeru tada su oni polarizirani. Polarizacijski filteri propuštaju samo one fotone koji su polarizirani u određenom smjeru dok su ostali blokirani.

Kvantna komunikacija uključuje kodiranje informacija u kvantna stanja, ili qubite, nasuprot klasičnoj kriptografiji koji koristi bitove.

Korištenjem kvantne superpozicije ili kvantne isprepletenosti te šaljući informacije u kvantnim stanjima može se implementirati komunikacijski sustav koji otkriva napadača. [1] [4] [5]

II. KVANTNI PROTOKOLI

Kvantna kriptografija iskorištava svojstva kvantnih stanja kako bi osigurala sigurnost sustava. Postoji nekoliko pristupa u distribuciji kvantnih ključeva, ali se općenito mogu podijeliti u dvije skupine, u ovisnosti da li su qubitovi nezavisni jedni o drugima ili nisu. Na slici 1 dan je prikaz kvantnog komunikacijskog kanala koji se odvija kroz dvije faze.



Slika 1. Prikaz kvantnog komunikacijskog kanala

A. Protokoli "pripremi i izmjeri"

Čin mjerenja je sastavni dio kvantne mehanike. Generalno govoreći, mjerenje nepoznatog kvantnog stanja će promijeniti to stanje. To je poznato pod imenom kvantna neodređenost i počiva na rezultatima Heisebergovog principa neodređenosti te teorema o nekloniranju. To se može iskoristiti kako bi se detektirali pokušaji prisluškivanja komunikacijskog kanala te, važnije, da bi se izračunala količina informacija koja je presretnuta.

B. Protokoli zasnovani na isprepletenosti

Kvantna stanja dva ili više odvojena objekta mogu postati povezana tako da se opišu kombiniranim kvantnim stanjem a ne kao individualni objekti. To znači da će provođenje mjerenja na jednom objektu utjecati na drugi objekt. Ako se isprepleteni par objekata pošalje komunikacijskim kanalom, pokušaj presretanja bilo koje čestice će uzrokovati promjenu cjelokupnog sustava, što će dovesti do otkrića treće strane, tj. napadača u komunikacijskom kanalu.

Ova dva pristupa se nadalje mogu podijeliti u tri skupine protokola:

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

Protokoli zasnovani na diskretnim varijablama su kronološki nastali prvi i danas su najrasprostranjeniji. Protokoli ostalih dviju skupina su uglavnom orjentirani ka prevladavanju praktičnih ograničenja u eksperimentima.

U nastavku su opisani neki od kvantnih protokola. [9]

C. BB84 protokol

Prvi kvantni kriptografski protokol je stvoren 1984. godine od strane Gillesa i Brasarda.

Pošiljatelj (Ana) i primatelj (Branko) su povezani kvantnim komunikacijskim kanalom koji omogućuje razmjenu kvantnih stanja. U slučaju fotona, taj komunikacijski kanal je ili optičko vlakno ili slobodan prostor (eter). Također, Ana i Branko su povezani nekim javnim klasičnim komunikacijskim kanalom (primjerice Internetom). Niti jedan od tih kanala ne mora biti siguran; protokol je dizajniran s pretpostavkom da treća strana može prisluškivati. Sigurnost protokola dolazi iz kodiranja informacija u neortogonalnim stanjima. BB84 koristi dva para stanja, gdje je svaki par konjugiran u odnosu na drugi par a dva stanja unutar jednog para su ortogonalna jedan prema drugom. Parovi ortogonalnih stanja se zovu baze. Uobičajena polarizacija stanja je linerana horizontalna – linerna vertikalna, linerana pod 45 stupnjeva – linerana pod 135 stupnjeva, cirkularna lijeva – cirkularna desna polarizacija. Bilo koje dvije polarizacije iz različitih baza su međusobno konjugirane. Za BB84 se odabiru dvije baze polarizacije i svakom od stanja u bazama dodijelimo vrijednost 0 ili 1 čime tvorimo kvantnu abecedu.

U prvoj fazi komunikacije Ana šalje Branku tajni ključ preko kvantnog kanala. Za svaki od impulsa slučajno izabire jednu od dviju baza polarizacije. Branko ima detektor polarizacije. On ga može postaviti tako da mjeri ili jednu ili drugu polarizaciju. Kvantna mehanika mu brani da mjeri obje polarizacije odjednom. Mjerenje jedne polarizacije uništava svaku mogućnost mjerenja druge polarizacije. Ako Branko ispravno postavi detektor, on će registrirati ispravnu polarizaciju, inače će registrirati neko slučajno stanje s jednakom vjerojatnošću. Branko ne može odrediti razliku između ta dva slučaja. U slijedećem koraku Branko uspostavlja vezu s Anom preko javnog kanala i obavještava ju koje je orjentacije polarizatora koristio za detekciju. Ana odgovara Branku koja su podešavanja bila ispravna. Ana i Branko zadržavaju samo one polarizacije koje su bile ispravno postavljene. Tako dobiveni bitovi čine tajni ključ. Prosječno će Branko pogoditi ispravnu polarizaciju u 50% slučajeva. Prisluškivanjem Iva pogađa polarizacije kao i Branko. Također, može se pretpostaviti da će pogoditi u 50% slučajeva. Budući da pogrešne pretpostavke mijenjaju polarizaciju impulsa, ona bi na taj način unijela pogreške u sustav. Unošenje grešaka u impulse tijekom prisluškivanja će pokvariti zajednički tajni ključ jer će Ana i Branko na kraju dobiti različite nizove bitova. Tada Ana i Branko završavaju protokol tako da usporede nekoliko bitova svojih nizova. Ako postoje neusuglašenosti, oni znaju da su bili prisluškivani. U suprotnom, odbacuju bitove koje su koristili za usporedbu i zadržavaju ostale. [1] [2]

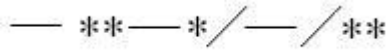
Primjer BB84 protokla glasi:

Ana šalje Branku niz impulsa fotona gdje je svaki impuls kodiran u jedno od 4 neortogonalna stanja. Ta su stanja linerano horizontalan – linearno vertikalan, linearno pod 45 stupnjeva – linearno pod 135 stupnjeva. Ti se impulsi mogu prikazati kao sljedeći niz znakova:

Branko koristi detektor polarizacije. Detektor može biti postavljen da mjeri ili jednu ili drugu polarizaciju. Neka je detektor postavljen na slijedeći način:

Ako Branko ispravno postavi detektor, tada će dobiti ispravne rezultate inače će dobiti slučajna mjerenja. Branko ne može razlikovati ta dva slučaja. Neka dobije rezultat:

Sada Branko javlja Ani preko javnog kanala kako je namjestio detektor. Ana odgovara Branku koja su podešenja bila ispravna. U ovom primjeru ispravno podešenje je za impulse 1, 4, 6, 7 i 8. Ana i Branko zadržavaju samo ispravne polarizacije.



Koristeći unaprijed pripremljen kod za svako od 4 moguća stanja polarizacije Ana i Branko prevode mjerenja u bitove. Neka linearno horizontalna i linaerna pod 45 stupnjeva odgovaraju jedinici a linaerno vertikalna i linearna pod kutem od 135 stupnjeva nuli. Sada kao rezultat mjerenja dobivamo kod: 11010.

Na ovaj način Ana i Branko mogu generirati onoliko bitova koliko im treba za generiranje ključa. U prosjeku Branko će pogoditi ispravnu polarizaciju u 50% slučajeva. Ako bi Iva prisluškivala ona također mora pogađati polarizacije u kojima će mjeriti te će također pogoditi u prosjeku u 50% slučajeva. Kako pogrešne pretpostavke mijenjaju polarizaciju impulsa, Ana i Branko bi dobili različite nizove ako Iva prisluškuje. Zadnji korak u protokolu je da Ana i Branko usporede nekoliko bitova svojih nizova. Ako postoje nesuglasice onda znaju da su bili prisluškivani. U suprotnom, odbacuju bitove koje su uspoređivali i zadrže ostale.

D. B92 protokol

Za razliku od protokola BB84 koji zahtijeva dvije ortogonalne kvantne abecede (baze), protokol B92 zahtijeva samo jednu neortogonalnu abecedu. Neka se sa θ označi foton koji je polariziran pod kutem φ u odnosu na vertikalu, gdje je $0<\varphi<45^0$ a sa θ' označimo foton polariziran pod kutem $-\varphi$ u odnosu na vertikalu. Tada im se pridjele vrijednosti 0 i 1. Kao i kod protokola BB84, Ana i Branko komuniciraju u dvije faze, prvo preko jednosmjernog kvantnog kanala i drugo preko dvosmjernog javnog kanala. Kako Ana koristi neortogonalni sustav ne postoji način koji bi jednoznačno razlučio ta dva stanja polarizacije. Branko može točno detektirati poslani bit ili primiti dvosmisleni rezultat. Prilikom komunikacije javnim kanalom Branko obavještava Anu o rednim brojevima bitova koje je primio nedvosmisleno a ostali bitovi se odbacuju. Bitovi koji su primljeni nedvosmisleno postaju ključ. Ostatak se odvija kao i u protokolu BB84. Prisutnost Ive se može otkriti velikim brojem grešaka u sustavu. Ovaj protokol je puno jednostavnije implementirati nego BB84 protokol ali još nisu osmišljeni dostatni dokazi koji bi pokazali njegovu sigurnost. [4]

E. E91 protokol

Protokol je dobio ime po Arthuru Ekertu koji ga je 1991. godine izmislio. Ekertova shema koristi isprepleteni par fotona. Oni mogu biti kreirani od strane Ane, Branka ili nekog izvora neovisnog o njima, uključujući Ivu. Fotoni se distribuiraju tako da Ana i Branko dobiju po jedan foton iz svakog para. Ova se shema zasniva na dva svojstva isprepletenosti fotona:

- isprepletena stanja su savršeno povezana;
- bilo koji pokušaj prisluškivanja uništava korelaciju između fotona na način koji Ana i Branko mogu detektirati.

Ana i Branko neovisno biraju bazu u kojoj će mjeriti primljeni foton, s tim da Ana bilježi izmjereni bit a Branko bilježi komplement izmjerenog bita jer je njegov foton ortogonalan onome koji je primila Ana. U komunikaciji javnim kanalom Ana i Branko uspoređuju korištene baze detekcije i izdvajaju bitove u kojima su koristili jednake operacije mjerenja. Oni bitovi na kojima su koristili različite operacije mjerenja ne odbacuju već koriste za otkrivanje prisutnosti Ive u komunikaciji korištenjem Bellove nejednadžbe. Ona se upotrebljava za određivanje postojanja lokalno skrivenih varijabli. Ukoliko je nejednadžba zadovoljena, Iva je prisluškivala. Ostatak protokola je isti kao i u BB84. [7] [9]

F. SARG04

Ovaj protokol je izveden iz protokola BB84. SARG04 su definirali Scarani i suradnici 2004. godine. SARG04 protokol je namijenjen za situacije gdje informacije šalje Poissonov izvor koji stvara slabe pulseve (gdje je srednja vrijednost poslanih fotona manja od 1) i informacije prima nesavršeni detektor. Prednost SARG04 nad BB84 protokolom je njegova robusnost kod nekoherentnih PNS napada. [9]

G. Protokol šest stanja

Protokol koristi tri para ortogonalnih polarizacijskih stanja da bi predstavio stanja 0 ili 1. Protokol se je pokazao manje učinkovit u prijenosu ključa ali je pokazao veću otpornost na greške nego protokoli BB84 i B92. [9]

III. KRIPTOGRAFIJA KVANTNIH PODATAKA

Predstavlja kriptografiju kvantnih podataka gdje se kriptografski alati razvijaju za informacije koje su ugrađene u kvantne sustave.

A. Kvantna jednokratna bilježnica

U ovom sustavu Ana i Branko unaprijed dijele par maksimalno isprepletenih čestica i koriste ih za teleportaciju proizvoljnog qubita. Jedinu komunikaciju javnim kanalom predstavlja par slučajnih bitova poslanih od Ane Branku, koji mu omogućuju rekonstrukciju originalnog stanja koje je Ana htjela poslati. [3]

B. Vernamova kvantna šifra

Koristi se klasični ključ koji može poprimiti 4 moguće vrijednosti. Ana primjenjuje jedan od 4 unarna (Paulieva) operatora na proizvoljnom sustavu od jednog qubita koji onda može biti poslan Branku. Branko dekriptira stanje upotrebom inverznog unarnog operatora. Kvantni opis poslanog stanja je isti bez obira na originalno stanje koje je poslano dok god je ključ uniformno distribuiran i nepoznat Ivi. Uspješno je demonstrirano kako se tajni ključ za Vernamovu kvantnu šifru može upotrijebiti i više puta ako se koristi klasični javni tekst. [3]

IV. KVANTNA DISTRIBUCIJA KLJUČA

Svrha kvantne distribucije ključa je omogućavanje dvjema poštenim stranama, dogovor o slučajnom kriptografskom ključu u situacijama gdje je moguće prisluškivanje. Međutim, u komunikaciji između Ane i Branka može dio točno izmjerenih fotona biti detektiran pogrešno. Također, ako Iva pokuša izmjeriti fotone koje je Ana poslala prije nego stignu do Branka, greške će nastati zbog činjenice da Iva pokušava izmjeriti podatke o polarizaciji fotona. Ove dvije situacije se ne mogu razlikovati: prirodan ili umjetan šum izgledaju jednako. Procjena o razini šuma vodi do procjene o količini informacija koje je Iva dobila. Posljedično, protokol u tri faze dozvoljava Ani i Branku da dobiju i da se slože oko manjeg, tajnog kriptografskog ključa na temelju njihovog toka podataka sa šumom koji je prisluškivan. Te tri faze se nazivaju procjena greške, poravnanje informacija i pojačanje privatnosti. [3]

A. Procjena greške

Provodi se na način da Ana ili Branko odaberu slučajan broj *t* od prethodno poslanih bitova koji su točno izmjereni i javi ih drugoj strani. Druga strana tada uspoređuje bitove s onima koje ona ima i javlja broj grešaka *e*. Za dovoljno velike uzorke, omjer *e/t* bi trebao biti razumna procjena broja grešaka koje su ostale u neobjavljenom dijelu ključa. [3]

B. Poravnanje informacija

Predstavlja način ispravke grešaka koji se provodi između ključeva Ane i Branka, u pokušaju osiguravanja identičnosti oba ključa. Postupak se provodi javnim kanalom te je tako od najveće važnosti minimizirati poslane informacije o ključevima jer ih Iva može pročitati. Uobičajeni protokol je kaskadni protokol. On se odvija u nekoliko faza, gdje se oba ključa dijele u blokove u svakoj fazi i uspoređuje se paritet tih blokova. Ako se pronađe razlika u paritetu provodi se binarna pretraga da bi se našla i ispravila greška. Ovaj se proces provodi rekurzivno i nakon što se svi blokovi usporede te sve faze završe Ana i Branko će imati iste ključeve sa visokom vjerojatnošću. Međutim, Iva će također dobiti dodatne informacije o ključu iz ovog procesa. [3]

C. Pojačanje privatnosti

Predstavlja metodu za uklanjanje djelomičnih informacija koje Iva ima o ključu Ane i Branka. Te djelomične informacije mogu biti rezultat prisluškivanja kvantnog kanala tijekom prijenosa ključa ili javnog kanala tijekom poravnanja informacija. Pojačanje privatnosti koristi Anin i Brankov ključ za stvaranje novog, kraćeg ključa na način da Iva ima samo zanemarive informacije o novom ključu. To se može postići korištenjem funkcija sažimanja, koje kao ulazni parametar primaju binarni niz dužine ključa i kao izlaz daju binarni niz kraće dužine. Novi ključ se sažima na temelju količine informacija koje je Iva mogla saznati o starom ključu što se zna iz količine grešaka koje postoje. Na taj način se smanjuje vjerojatnost da Iva ima bilo kakve informacije o novom ključu na vrlo male vrijednosti. [3]

V. MOGUĆI NAPADI

Kako bi kvantni kriptografski sustav bio potpuno siguran neki uvjeti moraju biti zadovoljeni:

- Iva ne može pristupiti uređajima za enkripciju i dekripciju u Aninom i Brankovom vlasništvu.
- Slučajni generator brojeva koji koriste Ana i Branko mora uistinu davati slučajne brojeve.
- Klasični komunikacijski kanal mora biti autentificiran korištenjem potpuno sigurne sheme autentifikacije.

U nastavku su opisani neki od najpoznatijih napada na kvantne kriptografske sustave.[9]

A. Napad "osoba u sredini"

Kvantna kriptografija je osjetljiva na ovaj napad kada nema autentifikacije kao i klasična kriptografija. Ana i Branko ne mogu autentificirati jedno drugo i uspostaviti sigurnu vezu bez nekog načina provjere identiteta kao naprimjer bez tajne poznate objema stranama. Ako Ana i Branko imaju takvu tajnu onda mogu koristiti shemu savršeno sigurne autentifikacije (kao naprimjer Carter-Wegman shema) zajedno sa kvantnom distribucijom ključa da bi eksponencijalno proširili ključ, te koristeći mali dio

novog ključa da bi autentificirali novo razdoblje razmjene podataka. [9]

B. Napad razdvajanjem broja fotona (PNS napad)

U protokolu BB84 Ana šalje kvantna stanja Branku koristeći pojedinačne fotone. U praksi se koriste oslabljeni laserski pulsevi za slanje kvantnih stanja. Ti pulsevi sadržavaju malu količinu fotona raspodijeljenih po Poissonovoj razdiobi. To znači da neki pulsevi ne sadržavaju niti jedan foton, neki jedan a neki dva ili više fotona. Ako puls sadrži više od jednog fotona tada Iva može razdijeliti dodatne fotone i poslati jedan foton Branku. Tada Iva može spremiti dodatne fotone u kvantnu memoriju dok Ana ne otkrije koje su kodirajuće baze. Iva može izmjeriti fotone u ispravnoj bazi i time dobiti podatke o ključu bez uvođenja grešaka koje se mogu detektirati. [9]

C. Hakerski napadi

Takvi napadi ciljaju nesavršenost u implementacijama protokola umjesto samih protokola. Ako je oprema korištena u kvantnoj kriptografiji komprimitirana tada se mogu generirati ključevi koji nisu sigurni pomoću napada generatorom slučajnih brojeva.

Drugi način napada je napad trojanskim konjem. U takvom napadu osoba koja prisluškuje šalje jaki svjetlosni puls Ani između fotona koji se šalju. Oprema koju Ana koristi tada reflektira dio svjetlosti natrag, otkrivajući koja je polarizacija korištena.

Također, postoji i napad lažnim stanjima, napad promjenom faze i napad vremenskim pomakom. Napad vremenskim pomakom je bio i uspješno demonstriran na komercijalnom kvantnom kriptografskom sustavu. [9]

Sve vrste hakerskih napada je relativno lako onemogućiti modificiranjem opreme.

D. DoS napad(Denial of Service)

Budući se za kvantnu kriptografiju koriste optički kablovi ili zrak kao medij prijenosa informacija, napad se može pokušati prekidajući ili blokirajući liniju, te prisluškujući liniju. [9]

VI. RAZVOJ KVANTNE KRIPTOGRAFIJE

Početak kvantne kriptografije se može pratiti u rane 1970.-e godine kada je znanstvenik Stephen Weisner napisao rad „*Conjugate Coding*“. Weisner je predlagao dva područja primjene:

- stvaranje bankovnih potvrda koje nije moguće krivotvoriti;
- umnožavanje dvije ili tri poruke na način da čitanje jedne uništava druge.

Nažalost, do objavljivanja tog rada je trebalo proći više od 10 godina. U međuvremenu, Charles H. Bennet (koji je znao o Weisnerovoj ideji) i Gilles Brassard su počeli raditi na istom području, najprije kroz nekoliko članaka, a poslije i eksperimentalnim prototipom koji je demonstrirao tehnološku ostvarivost koncepta. Taj se prototip sastojao od fotona koji su se gibali kroz 0.30 m dugu cijev nazvanu „*lijes tete Marthe*“. Smjer u kojem su fotoni oscilirali te njihova polarizacija predstavljaju 0 ili 1 niza kvantnih bitova ili qubita. [3] [6]

VII. KVANTNA KRIPTOGRAFIJA DANAS

Defense Advanced Research Projects Agency (DARPA) je 2004. godine pokrenula projekt povezivanja šest mrežnih čvorova između tvrtke BBN Technologies te sveučilišta Harvard i Boston. Ključevi za kriptiranje se šalju kvantnim kanalom a poruke šifrirane tim ključem Internetom. Ta mreža predstavlja prvu kvantno kriptografsku mrežu koja je konstantno u pogonu a da se nalazi izvan laboratorija.

Godine 2004. u Beču se dogodio prvi bankarski prijenos pomoću kvantne kriptografije. Tada je neki važan ček, za koji je bila zahtijevana apsolutna sigurnost, prenešen u jednu austrijsku banku.

U jesen 2005. godine tvrtka *idQuantique* i internet davatelj usluga iz Ženeve *Deckpoint* su predstavili mrežu koja omogućuje skupu poslužitelja koji se nalaze u Ženevi sigurnosnu pohranu podataka na lokaciju koja je udaljena 10 km, uz uporabu ključeva distribuiranih kvantnom enkripcijskom vezom.

U ožujku 2007. godine je demonstrirana kvantna razmjena ključa na udaljenosti od 148.7 km, uspjeh postignut od strane Los Alamos/NIST grupe korištenjem BB84 protokola.

Tvrtka *idQuantique* je osigurala opremu u kantonu Ženeva, Švicarska da bi se poslali rezultati izbora koji su održani 21.08.2007.

U listopadu 2008. godine tvrtka *idQuantique* je upotrijebila svoju opremu za uspostavljanje kvantnih mreža u Beču i Durbanu, te osiguravanje izbora u Švicarskoj.

Prvi kompjuter na svijetu zaštićen kvantnom kriptografijom je implementiran u osmom mjesecu 2008. godine na znanstvenoj konferenciji u Beču. Mreža je koristila 200 km standardnih optičkih kabela za povezivanje šest lokacija u Beču te grada St. Poeltena koji se nalazi 69 km zapadno.

Europska Unija je 2004. godine pokrenula projekt zaštite komunikacijskih kanala kvantnom kriptografijom, dijelom i da spriječi moguće prisluškivanje pomoću satelita Echelon.

U eksperimentu 2004. godine tvrtka NEC je ostvarila prijenos ključa kvantnom kriptografijom na udaljenost veću od 150 km.

Kako bi se povećala udaljenost na koju je moguće razmjenjivati podatke istraživači traže i druge medije za uspostavljanje kriptografske mreže.

Eksperiment 2002. godine proveden od strane Los Alamos nacionalnog labaratorija je uspostavio vezu u slobodnom prostoru na udaljenosti od 10 km. Iste godine su tvrtka *QinetiQ* iz Engleske i sveučilište *Maximilian* iz Munchena, uspostavili zračnu vezu između dva planinska vrha u južnim Alpama na udaljenosti od 23.4 km. Europska Svemirska Agencija je u ranim fazama ostvarivanja zračnog kriptografskog kanala između Zemlje i satelita.

Najveća udaljenost postignuta u slobodnom prostoru je 144 km, što predstavlja udaljenost između dva otoka iz

Kanarskog otočja, uspjeh postignut od strane europskog udruženja korištenjem isprepletenih fotona 2006. godine, te korištenjem modificiranog BB84 protokola 2007. godine. Ovi eksperimenti pokazuju da bi prijenos podatka do satelita bio moguć, zbog niže gustoće atmosfere na većim visinama.

Rekord u brzini prijenosa kvantno kriptiranih podataka je ostvario NIST (National Institute of Standards and Technology) s brzinom od 4 milijuna bitova u sekundi kroz optički kabel dužine 1 km. Tvrtka NEC, National Institute of Information and Communications Technology te Japan Science and Technology Agency su u 9. mjesecu 2004. godine ostvarili kvantni kripotografski kanal brzine 100 kb/s na udaljenost od 40 km.

Početkom 2003. godine tvrtke *idQuantique* iz Ženeve i *MaqiQ Technologies* iz New Yorka su predstavile proizvode koji mogu slati kvantne kriptografske ključeve na udaljenosti prihvatljive za komercijalnu upotrebu tih sustava. Prosječna cijena takvih sustava je od 70 000 do 100 000 dolara.

Trenutno postoje četiri tvrtke koje nude komercijalna rješenja iz područja kvantne kriptografije: *idQuantique*, *MagiQ Technologies, Quintessence Labs* te *Smart Quantum*. Također, tvrtke *IBM*, *HP*, *Fujitsu*, *NEC* i *Toshiba* imaju svoje programe istraživanja kvantne kriptografije. [8] [9]

VIII. ZAKLJUČAK

Kvantna kriptografija je u zadnjih dvadesetak godina doživjela snažan razvoj. Dalek je put pređen od prvog eksperimenta u kome su fotoni poslani kroz cijev dužine 0.30 m. Danas je tehnologija napredovala dovoljno da se kvantna kriptografija može koristiti u velikom broju praktičnih primjena. Ipak, to nije tako. Glavni je razlog svakako visoka cijena kvantnih kriptografskih sustava ali i način razmišljanja kako kvantna kriptografija spada u domenu znanstvene fantastike.

Kvantna kriptografija će svoj procvat doživjeti, ako ne prije, onda kada kvantna računala postanu stvarnost. Tada algoritmi iz domene klasične kriptografije više neće pružati dostatnu zaštitu od napada kao što je Shorov kvantni algoritam za faktorizaciju brojeva. Naravno, tada će nastati problem zaštite svih onih podataka koji su u prošlosti zaštićeni klasičnim kriptografskim sustavima a postoji potreba za tajnošću tih podataka kroz duži niz godina.

Naravno, i kvantna kriptografija nije u potpunosti imuna na napade, no za razliku od klasičnih napada, ti su napadi usmjereni na probleme implementacije i autentifikacije. Takvi napadi se mogu spriječiti bez većih problema, ili implementacijom modificiranih protokola ili sigurnijom i dodatnom opremom.

LITERATURA

[1] B. Schneier, “Applied Cryptography”, 2nd Edn. John Wiley & Sons, 1996.

[2] D. Hrg, L. Budin, M. Golub, “Quantum Cryptography and Security of Information Systems”, Proceedings of the 15th International Conference on Information and Intelligent Systems, IIS2004, Varaždin, Croatia, 2004.

[3] H. C. A. Van Tilborg, “Encyclopedia of Cryptography Security”, Springer, 2005.

[4] M. Jakuš, “Kvantna Kriptografija”, seminarski rad (na Hrvatskom), Faculty of Electrical Engineering and Computation, Zagreb, 2004.

[5] R. A. Mollin, “An Introduction to Cryptography”, 2nd Edn, Chappman & Hall/CRC, 2007.

[6] R. Oppliger, “Contemporary Cryptography”, Artech House, 2005.

[7] S. J. Lomonaco, “A Quick Glance at Quantum Cryptography”, arXive e-print quant.ph/9811056, 1998.

[8] Scientific American Magazine, Best-Kept Secrets, p. 65-69, January 2005.

[9] Internet stranice:
http://idquantique.com/ (01.02.2009.)
http://magiqtech.com/ (01.02.2009.)
http://www.quintessencelabs.com/ (01.02.2009.)
http://www.smartquantum.com/-rubrique2-.html (01.02.2009.)
http://en.wikipedia.org/wiki/Quantum_cryptography (01.02.2009.)
http://www.nec.co.jp/press/en/0409/2701.html (04.02.2009.)
http://news.illinois.edu/scitips/02/0711quantumcrypt.html (05.02.2009.)