PROTOKOLI I PRAVCI RAZVOJA KVANTNE KRIPTOGRAFIJE

Markagić S. *Milorad*, Univerzitet odbrane, Vojna akademija, Katedra telekomunikacija i informatike, Beograd

OBLAST: telekomunikacije
VRSTA ČLANKA: stručni članak

Sažetak:

Uporedo sa razvojem tajnosti podataka razvijaju se i sredstva i sistemi koji bi tu tajnost trebalo da omoguće. Trenutno su u najmasovnijoj upotrebi klasični kriptografski sistemi i kriptografski sistemi sa javnim ključevima. Međutim, nijedan od tih sistema ne omogućava rešenje čuvene „kvake 22" kriptografije. Zahvaljujući intenzivnom razvoju kvantne mehanike, u poslednjih tridesetak godina pojavila se potpuno nova vrsta kriptografije – kvantna kriptografija.

Njen najveći doprinos je u mogućnosti otkrivanja prisluškivanja komunikacionog kanala od treće osobe. Postavlja se pitanje: da li je to zaista tako? Postavlja se i pitanje, ako je kvantna kriptografija toliko dobra, zašto nije u širokoj upotrebi? Cilj ovog rada jeste da se sa jedne strane definišu osnovni mehanizmi kvantne kriptografije IP protokola, a sa druge strane da se ukaže i na nedostatke, i to kako na one vezane za mogućnosti današnjih uređaja tako i na bezbednosne nedostatke u protokolima.

Ključne reči: *kriptografija, ključevi, protokoli, zaštita.*

Uvod

Svrha kriptografije je prenos informacija na način da su one dostupne samo primaocu – osobi kojoj su i namenjene. Na početku je sigurnost šifrovanog teksta zavisila isključivo od tajnosti celog procesa šifrovanja i dešifrovanja. Danas se koriste šifre čiji su algoritmi javno poznati, ali to ne ugrožava bezbednost šifrovane poruke. U takvim sistemima tajni ključ poruke i otvoreni tekst unose se kao parametri u algoritam.

Ako se želi koristiti savršeno siguran kriptografski sistem, onda je odgovor Vernamova šifra, poznatija pod nazivom jednokratna beležnica. Jednokratna beležnica koristi slučajno generisani ključ K najmanje iste dužine kao i poruka koja se šifruje. Glavni problem kod takvog sistema je potreba za razmenom tajnog ključa između pošiljaoca i primaoca poruke (Subjekti "A" i "B"). U velikom broju slučajeva, ključ K je veoma dugačak i time neprikladan za slanje sigurnim kanalom, jer je to nepraktično, sporo i skupo. Ako pošiljalac slučajno

milmarkag@yahoo.com

dva puta iskoristi isti ključ, tada se njen šifrovani tekst menja iz savršeno sigurnog u lako provaljiv. Tako se danas, u većini praktičnih kriptosistema, koristi ključ K koji je konstantne veličine i obično je puno kraći od dužine jasnog teksta. Kao rezultat toga imamo da kriptosistemi više nisu apsolutno sigurni [1].

Međutim, pažljivim izborom metode enkripcije i ključa određeni sistem se može smatrati praktično sigurnim. Praktično siguran kriptosistem znači da iako napadač ("I") može teoretski dekriptovati poruku bez znanja ključa, on to verovatno neće uspeti. Razlog je što su procesorska snaga i vreme potrebno za napad najčešće iznad napadačevih mogućnosti.

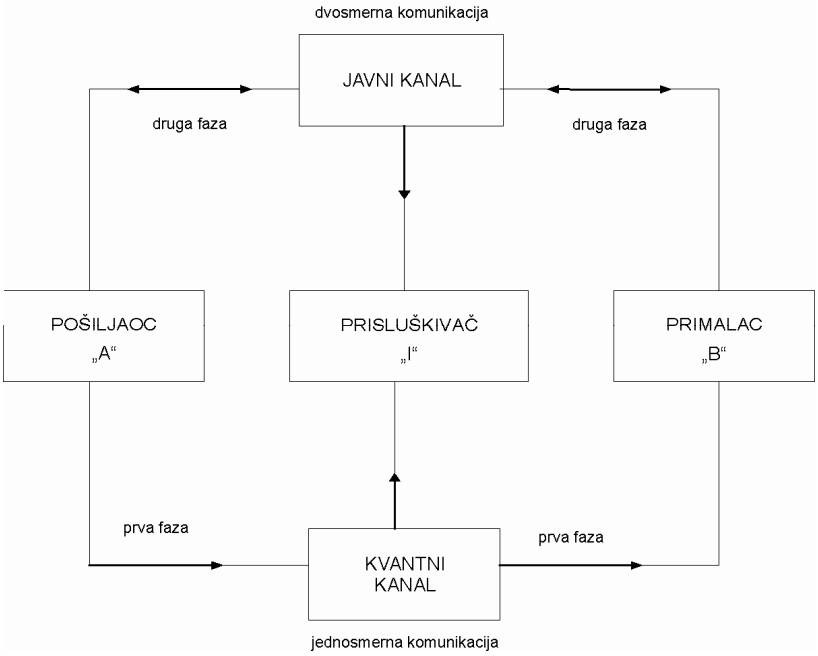
U svakom slučaju, slaba tačka klasičnih kriptografskih sistema je što se sigurna komunikacija može odvijati tek nakon što je ključ sigurno razmenjen komunikacionim kanalom ili prostom fizičkom distribucijom. Taj problem često se naziva „kvaka 22" kriptografije: pre nego što "A" i "B" mogu tajno da komuniciraju, moraju imati isti ključ. Postoji i dodatak tom problemu, poznat pod imenom „kvaka 22a" – čak i ako "A" i "B" uspeju da razmene ključ preko sigurnog komunikacionog kanala, ne postoji mehanizam u klasičnoj kriptografiji koji može garantovati da je ključ poslat sigurno, odnosno da ga "I" nije uspeo prisluškivanjem komunikacionog kanala saznati.

Tu na scenu stupa kvantna kriptografija – kvantna razmena ključeva, koja omogućava dvema stranama ("A" i "B") komunikaciju koja je u potpunosti sigurna. Kvantna kriptografija koristi prirodnu neodređenost kvantnog sveta. Uz njenu pomoć može se uspostaviti komunikacioni kanal koji nije moguće prisluškivati bez ometanja prenosa, odnosno dva korisnika koji međusobno komuniciraju mogu otkriti prisustvo treće strane koja pokušava saznati ključ. Takođe, osoba koja prisluškuje ne može kopirati nepoznate kvantne bitove takozvane qu-bite, tj. nepoznata kvantna stanja, zbog teoreme o nekloniranju koju su prvi prezentovali Wooters i Zureck. Kvantna kriptografija služi samo za dobijanje i distribuciju ključa, a ne za prenos poruka. Tako generisani ključ može poslužiti u nekom kriptosistemu za šifrovanje i dešifrovanje poruke. Kvantna mehanika kaže da se čestice ne nalaze samo na jednom mestu. One se nalaze na nekoliko mesta odjednom, s određenim verovatnoćama da postoje na različitim mestima. Međutim, to sve nema smisla dok ne dođe naučnik i ne „uhvati" česticu koja se nalazi na nekom mestu. Uhvaćenoj čestici nije moguće istovremeno izmeriti sve fizičke veličine. Merenjem neke od veličina čestice uništava se svaka mogućnost merenja nekog drugog njenog svojstva. Ta neodređenost se može iskoristiti za generisanje tajnog ključa. Dok putuju, fotoni titraju pod nekim određenim uglom. Kada velika grupa fotona titra u istom smeru, oni su polarizovani. Polarizacijski filteri propuštaju samo one fotone koji su polarizovani u određenom smeru dok su ostali blokirani.

Kvantna komunikacija uključuje kodovanje informacija u kvantna stanja, ili qu-bite, nasuprot klasičnoj kriptografiji koja koristi bitove. Korišćenjem kvantne superpozicije ili kvantne isprepletenosti i šaljući informacije u kvantnim stanjima, može se implementirati komunikacioni sistem koji otkriva napadača.

Kvantni protokoli

Kvantna kriptografija koristi svojstva kvantnih stanja kako bi osigurala sigurnost sistema. Postoji nekoliko pristupa u distribuciji kvantnih ključeva, ali se uopšteno mogu podeliti u dve grupe, zavisno od toga da li su qu-bitovi nezavisni jedni od drugih ili nisu. Na slici 1. dat je prikaz kvantnog komunikacionog kanala koji se odvija kroz dve faze.



Slika 1 – Prikaz kvantnog komunikacionog kanala
Picture 1 – View of a quantum communication channel

U nastavku su opisani neki od kvantnih protokola.

Protokoli „pripremi i izmeri“

Proces merenja je sastavni deo kvantne mehanike. Uopšteno govoreći, merenje nepoznatog kvantnog stanja promeniće to stanje. To je poznato pod imenom kvantna neodređenost i zasniva se na rezultatima Haiznbergovog principa neodređenosti i teorema o ne-kloniranju. Ovo se može iskoristiti da bi se detektovali pokušaji prisluškivanja komunikacionog kanala i, što je još važnije, da se izračuna količina informacija koja je presretnuta. [2]

Protokoli zasnovani na isprepletenosti

Kvantna stanja dva ili više odvojena objekta mogu postati povezana tako da se opišu kombinovanim kvantnim stanjem, a ne kao individualni objekti. To znači da će sprovođenje merenja na jednom objektu uticati na drugi objekat. Ako se isprepleteni par objekata pošalje komunikacionim kanalom, pokušaj presretanja bilo koje čestice uzrokovaće promenu celokupnog sistema, što će dovesti do otkrića treće strane (napadača) u komunikacionom kanalu.

Ova dva pristupa se dalje mogu podeliti na tri grupe protokola:

– diskretne varijable,
– kontinuirane varijable i
– distribuirano fazno referentno kodovanje.

Protokoli zasnovani na diskretnim varijablama su hronološki nastali prvi i danas su najrasprostranjeniji.

Protokoli ostale dve grupe su uglavnom orijentisani ka prevazilaženju praktičnih ograničenja u eksperimentima.

BB84 protokol

To je prvi kvantni kriptografski protokol koji je stvoren 1984. godine, pa zato i ima ovakvu oznaku. Prezentovao ga je Gilles Brassard.

Pošiljalac (“A“) i primalac (“B“) su povezani kvantnim komunikacionim kanalom koji omogućava razmenu kvantnih stanja. U slučaju fotona, taj komunikacioni kanal je ili optičko vlakno ili slobodan prostor (etar). Takođe, “A“ i “B“ su povezani još nekim javnim klasičnim komunikacionim kanalom (npr. internetom). Nijedan od tih kanala ne mora biti siguran, protokol je dizajniran sa pretpostavkom da treća strana može prisluškivati. Sigurnost protokola dolazi iz kodiranja informacija u neortogonalnim stanjima. BB84 koristi dva para stanja, gde je svaki par konjugovan u odnosu na drugi par, a dva stanja unutar jednog para su ortogonalna jedan prema drugom. Parovi ortogonalnih stanja zovu se baze [3].

Uobičajena polarizacija stanja je:

– linearna horizontalna,
– linearna vertikalna,
– linearna pod 45 stepeni,
– linearna pod 135 stepeni,
– cirkularna leva i
– cirkularna desna.

Bilo koje dve polarizacije iz različitih baza su međusobno konjugovane. Za BB84 se odaberu dve baze polarizacije i svakom od stanja u bazama dodeljuju vrednosti 0 ili 1, čime se pravi kvantna abeceda.

U prvoj fazi komunikacije “A“ šalje “B“ tajni ključ preko kvantnog kanala. Za svaki od impulsa slučajno bira jednu od dve baze polarizacije. “B“ ima detektor polarizacije. On ga može postaviti tako da meri ili jednu ili dru-

gu polarizaciju. Kvantna mehanika mu brani da meri obe polarizacije odjednom. Merenje jedne polarizacije uništava svaku mogućnost merenja druge polarizacije. Ako "B" ispravno postavi detektor, on će registrovati ispravnu polarizaciju, inače će registrovati neko slučajno stanje s jednakom verovatnoćom. "B" ne može odrediti razliku između ta dva slučaja. U sledećem koraku "B" uspostavlja vezu sa "A" preko javnog kanala i obaveštava ga koje je orijentacije polarizatora koristio za detekciju. "A" odgovara "B" koja su podešavanja ispravna. "A" i "B" zadržavaju samo one polarizacije koje su bile ispravno postavljene. Tako dobijeni bitovi čine tajni ključ. U proseku, "B" će pogoditi ispravnu polarizaciju u oko 50% slučajeva [5].

Prisluškivanjem "I" pogađa polarizacije kao i "B". Takođe, može se pretpostaviti da će pogoditi u 50% slučajeva. Budući da pogrešne pretpostavke menjaju polarizaciju impulsa, ona bi na taj način unela greške u sistem. Unošenje grešaka u impulse tokom prisluškivanja pokvariće zajednički tajni ključ jer će "A" i "B" na kraju dobiti različite nizove bitova. Tada "A" i "B" završavaju protokol tako da uporede nekoliko bitova svojih nizova. Ako postoje neusaglašenosti, oni znaju da su bili prisluškivani. U suprotnom, odbacuju bitove koje su koristili za upoređenje i zadržavaju ostale.

Primer BB84 protokola:

"A" šalje "B" niz impulsa fotona gde je svaki impuls kodiran u jedno od 4 neortogonalna stanja. To su sledeća stanja:

– linearna horizontalna,
– linerna vertikalna,
– linearna pod 45 stepeni i
– linearna pod 135 stepeni.

Impulse prikazujemo kao sledeći niz znakova:

–	\	|	–	|	/	–	/	|	\

"B" koristi detektor polarizacije. Detektor može biti postavljen da meri ili jednu ili drugu polarizaciju. Neka je detektor postavljen da meri na sledeći način:

+	+	X	+	X	X	+	X	X	+

Ako "B" ispravno postavi detektor, dobiće ispravne rezultate, inače će dobiti slučajna merenja. "B" ne može razlikovati ta dva slučaja. Pretpostavimo da dobije rezultat:

–	|	/	–	\	/	–	/	/	|

Sada “B“ javlja “A“ preko javnog kanala kako je namestio detektor. “A“ odgovara “B“ koja su podešavanja bila ispravna. U ovom primeru ispravno podešavanje je za impulse 1, 4, 6, 7 i 8.

“A“ i “B“ zadržavaju samo ispravne polarizacije.

–	*	*	–	*	/	–	/	*	*

Koristeći unapred pripremljen kod za svako od 4 moguća stanja polarizacije, “A“ i “B“ prevode merenja u bitove. Neka linearno horizontalna i linearna pod 45 stepeni odgovaraju jedinici, a linearno vertikalna i linearna pod uglom od 135 stepeni nuli. Sada kao rezultat merenja dobijaju kod: 11010.

Na ovaj način “A“ i “B“ mogu generisati onoliko bitova koliko im treba za generisanje ključa. U proseku, “B“ će pogoditi ispravnu polarizaciju u 50% slučajeva. Ako bi “I“ prisluškivao, on takođe mora pogađati polarizacije u kojima će meriti te će takođe pogoditi u proseku u 50% slučajeva. Kako pogrešne pretpostavke menjaju polarizaciju impulsa, “A“ i “B“ bi dobili različite nizove ako “I“ prisluškuje. Zadnji korak u protokolu je da “A“ i “B“ uporede nekoliko bitova svojih nizova. Ako postoje nesuglasice, onda znaju da su bili prisluškivani. U suprotnom, odbacuju bitove koje su uporedili i zadržavaju ostale.

B92 protokol

Za razliku od protokola BB84 koji zahteva dve ortogonalne kvantne abecede (baze), protokol B92 zahteva samo jednu neortogonalnu abecedu. Neka se – označi foton koji je polarizovan pod uglom od 45 stepeni u odnosu na vertikalu, gde je $0<-<45^0$, a sa –‘ označimo foton polarizovan pod uglom 135^0 u odnosu na vertikalu. Tada im se dodaju vrednosti 0 i 1. Kao i kod protokola BB84, “A“ i “B“ komuniciraju u dve faze, prvo preko jednosmernog kvantnog kanala i drugo preko dvosmernog javnog kanala. Kako “A“ koristi neortogonalni sistem, ne postoji način koji bi jednoznačno razlučio ta dva stanja polarizacije. “B“ može tačno detektovati poslati bit ili primiti dvosmisleni rezultat. Prilikom komunikacije javnim kanalom “B“ obaveštava “A“ 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 “I“ može se otkriti velikim brojem grešaka u sistemu. Ovaj protokol je mnogo jednostavnije implementirati nego BB84 protokol, ali još nisu osmišljeni verodostojni dokazi koji bi pokazali njegovu apsolutnu sigurnost [4] [6].

E91 protokol

Protokol je dobio ime po Arturu Ekertu koji ga je 1991. godine izmislio. Ekertova šema koristi isprepleteni par fotona. Oni mogu biti kreirani od strane “A“, “B“ ili nekog izvora nezavisnog od njih, uključujući i “I“. Fo-

toni se distribuiraju tako da “A“ i “B“ dobiju po jedan foton iz svakog para. Ova šema zasniva se na dva svojstva isprepletenosti fotona:

– isprepletena stanja su savršeno povezana i

– bilo koji pokušaj prisluškivanja uništava korelaciju između fotona na način koji “A“ i “B“ mogu detektovati.

“A“ i “B“ nezavisno biraju bazu u kojoj će meriti primljeni foton, s tim da “A“ beleži izmereni bit, a “B“ beleži komplement izmerenog bita jer je njegov foton ortogonalan onome koji je primio “A“. U komunikaciji javnim kanalom “A“ i “B“ upoređuju korišćene baze detekcije i izdvajaju bitove u kojima su koristili iste operacije merenja. Oni bitovi na kojima su koristili različite operacije merenja ne odbacuju se, već se koriste za otkrivanje prisutnosti “I“ u komunikaciji korišćenjem Belove nejednačine. Ona se upotrebljava za određivanje postojanja lokalno skrivenih varijabli. Ukoliko je nejednačina zadovoljena, “I“ je prisluškivao. Ostatak protokola je isti kao i u BB84.

SARG04

Ovaj protokol je izveden iz protokola BB84. SARG04 su definisali Skarani i saradnici 2004. godine. SARG04 protokol namenjen je za situacije gde informacije šalje Poisonov izvor koji stvara slabe pulseve (gde je srednja vrednost poslatih fotona manja od 1) i informacije prima nesavršeni detektor. Prednost SARG04 nad BB84 protokolom je njegova robusnost kod nekoherentnih PNS napada.

Protokol šest stanja

Ovaj protokol koristi tri para ortogonalnih polarizacijskih stanja da bi predstavio stanja 0 ili 1. Pokazao se manje korisnim u prenosu ključa, ali je pokazao veću otpornost na greške nego protokoli BB84 i B92.

Kriptografija kvantnih podataka

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

Slede neki primeri.

Kvantna jednokratna sveska

U ovom sistemu “A“ i “B“ unapred dele par maksimalno isprepletenih čestica i koriste ih za teleportaciju proizvoljnog qu-bita. Jedinu komunikaciju javnim kanalom predstavlja par slučajnih bitova poslatih od subjekta “A“ subjektu “B“, koji mu omogućavaju rekonstrukciju originalnog stanja koje je “A“ hteo poslati.

Vernamova kvantna šifra

Koristi se klasični ključ koji može imati 4 moguće vrednosti. “A“ primenjuje jedan od 4 unarna (Paulijeva) operatora na proizvoljnom sistemu od jednog qu-bita koji onda može biti poslat subjektu “B“. “B“ dekriptuje stanje upotrebom inverznog unarnog operatora. Kvantni opis poslatog stanja je isti bez obzira na originalno stanje koje je poslato dok god je ključ uniformno distribuisan i nepoznat subjektu “I“. Uspešno je izvedena demonstracija kako se tajni ključ za Vernamovu kvantnu šifru može upotrebiti i više puta, ako se koristi klasični javni tekst.

Kvantna distribucija ključa

Svrha kvantne distribucije ključa je omogućavanje dvema poštenim stranama, dogovor o slučajnom kriptografskom ključu u situacijama gde je moguće prisluškivanje. Međutim, u komunikaciji između subjekta “A“ i “B“ može se desiti da će deo tačno izmerenih fotona biti detektovan pogrešno. Takođe, ako “I“ pokuša da izmeri fotone koje je subjekat “A“ poslao pre nego što stignu do subjekta “B“, greške će nastati zbog činjenice da “I“ pokušava da izmeri podatke o polarizaciji fotona. Ove dve situacije ne mogu se razlikovati: prirodan ili veštački šum izgledaju isto. Procena o nivou šuma vodi do procene o količini informacija koje je “I“ dobio. Posledično, protokol u tri faze dozvoljava “A“ i “B“ da dobiju i da se slože oko manjeg, tajnog kriptografskog ključa na temelju njihovog toka podataka sa šumom koji je prisluškivan. Te tri faze nazivaju se procena greške, poravnanje informacija i pojačanje privatnosti [3].

Procena greške

Sprovodi se na način da “A“ ili “B“ odaberu slučajan broj t od prethodno poslatih bitova koji su tačno izmereni i jave da drugoj strani. Druga strana tada upoređuje bitove sa onima koje ona ima i javlja broj grešaka e. Za dovoljno velike uzorke, rezultanta e/t trebalo bi da bude razumna procena broja grešaka koje su ostale u neobjavljenom delu ključa.

Upoređivanje i izjednačavanje informacija

Predstavlja način ispravke grešaka koji se sprovodi između ključeva “A“ i “B“, u pokušaju osiguravanja identičnosti oba ključa. Postupak se sprovodi javnim kanalom pa je tako od najveće važnosti minimizovati poslate informacije o ključevima jer ih “I“ može pročitati. Uobičajeni protokol je kaskadni protokol. On se odvija u nekoliko faza, gde se oba ključa dele u blokove u

svakoj fazi i upoređuje se paritet tih blokova. Ako se pronađe razlika u paritetu, provodi se binarna pretraga da bi se našla i ispravila greška. Ovaj proces sprovodi se rekurzivno i nakon što se svi blokovi uporede te sve faze završe, "A" i "B" imaće iste ključeve sa visokom verovatnoćom. Međutim, "I" će takođe dobiti dodatne informacije o ključu iz ovog procesa.

Pojačanje privatnosti

Predstavlja metodu za uklanjanje delimičnih informacija koje "I" ima o ključu "A" i "B". Te delimične informacije mogu biti rezultat prisluškivanja kvantnog kanala tokom prenosa ključa ili javnog kanala tokom upoređivanja informacija. Pojačanje privatnosti koristi ključ "A" i "B" za stvaranje novog, kraćeg ključa na način da "I" ima samo zanemarive informacije o novom ključu. To se može postići korišćenjem 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 "I" mogao saznati o starom ključu što se zna iz količine grešaka koje postoje. Na taj način se smanjuje verovatnoća da "I" ima bilo kakve informacije o novom ključu na vrlo male vrednosti.

Mogući napadi na kvantne kriptografske sisteme

Kako bi kvantni kriptografski sistem bio potpuno siguran, moraju biti zadovoljeni sledeći uslovi:

– "I" ne može pristupiti uređajima za enkripciju i dekripciju u vlasništvu subjekata "A" i "B";

– slučajni generator brojeva koji koriste "A" i "B" mora zaista davati slučajne brojeve;

– klasični komunikacioni kanal mora biti autentifikovan korišćenjem potpuno sigurne šeme autentifikacije.

U nastavku su opisani neki od najpoznatijih napada na kvantne kriptografske sisteme [7] [8].

Napad „osoba u sredini"

Kvantna kriptografija je osetljiva na ovaj napad kada nema autentifikacije kao i klasična kriptografija. "A" i "B" ne mogu autentifikovati jedno drugo i uspostaviti sigurnu vezu bez nekog načina provere identiteta, kao na primer bez tajne poznate obema stranama. Ako "A" i "B" imaju takvu tajnu, onda mogu koristiti šemu savršeno sigurne autentifikacije (Karter-Vegman šema) zajedno sa kvantnom distribucijom ključa da bi eksponencijalno proširili ključ i koristeći mali deo novog ključa da bi autentifikovali novo razdoblje razmene podataka.

Napad razdvajanjem broja fotona (PNS napad)

U protokolu BB84 “A“ šalje kvantna stanja “B“ koristeći pojedinačne fotone. U praksi se koriste oslabljeni laserski pulsevi za slanje kvantnih stanja. Ti pulsevi sadrže malu količinu fotona raspodeljenih po Poisonovoj raspodeli. To znači da neki pulsevi ne sadrže nijedan foton, neki jedan, a neki dva ili više fotona. Ako puls sadrži više od jednog fotona onda “I“ može razdeliti dodatne fotone i poslati jedan foton “B“. Tada “I“ može sačuvati dodatne fotone u kvantnoj memoriji dok “A“ ne otkrije koje su kodirajuće baze. “I“ može izmeriti fotone u ispravnoj bazi i time dobiti podatke o ključu bez uvođenja grešaka koje se mogu detektovati.

Hakerski napadi

Ovi napadi ciljaju na nesavršenost u implementacijama protokola umesto samih protokola. Ako je oprema korišćena u kvantnoj kriptografiji kompromitovana, mogu se generisati ključevi koji nisu sigurni pomoću napada generatorom slučajnih brojeva. Drugi način napada je napad trojanskim konjem. U takvom napadu osoba koja prisluškuje šalje jak svetlosni signal i tada reflektuje deo svetlosti nazad, otkrivajući koja je polarizacija korišćena. Takođe, postoji i napad lažnim stanjima, napad promenom faze i napad vremenskim pomakom. Napad vremenskim pomakom bio je i uspešno prikazan na komercijalnom kvantnom kriptografskom sistemu.

Sve vrste hakerskih napada relativno je lako onemogućiti modifikacijom opreme.

DoS napad (Denial of Service)

Budući da se za kvantnu kriptografiju koriste optički kablovi ili foton kao medij prenosa informacija, napad se može pokušati prekidajući ili blokirajući liniju, odnosno prisluškujući liniju.

Pravci razvoja kvantne kriptografije

Početak kvantne kriptografije može se pratiti od ranih sedamdesetih godina kada je naučnik Stefen Veisner napisao rad „*Conjugate Coding*“. Veisner je predlagao dva područja primene:

– stvaranje bankovnih potvrda koje nije moguće kopirati i

– umnožavanje dve ili tri poruke na način da čitanje jedne uništava ostale.

Nažalost, do objavljivanja tog rada bilo je potrebno više od deset godina. U međuvremenu, Čarl Benet (koji je znao o Veisnerovoj ideji) i Brasard počeli su da rade na istom području, najpre kroz nekoliko članaka, a posle i eksperimentalnim prototipom koji je demonstrirao tehnološku ostvarivost koncepta.

Taj prototip sastojao se od fotona koji su se kretali kroz 0,30 m dugu cev nazvanu *„lijes tete Marth"*. Zavisno od smera u kojem su fotoni oscilirali, njihove polarizacije predstavljaju 0 ili 1 niza kvantnih bitova ili qu-bita.

Kvantna kriptografija DAS

Defense Advanced Research Projects Agency (DARPA) je 2004. godine pokrenula projekt povezivanja šest mrežnih čvorova između kompanije BBN Technologies univerziteta Harvard i Boston. Ključevi za šifrovanje šalju se kvantnim kanalom, a poruke šifrovane tim ključem internetom. Ta mreža predstavlja prvu kvantno-kriptografsku mrežu koja je konstantno u pogonu a nalazi se van laboratorije.

Godine 2004. u Beču se dogodio prvi bankarski prenos pomoću kvantne kriptografije. Tada je neki važan ček, za koji je bila zahtevana apsolutna sigurnost, prenesen u jednu austrijsku banku. U jesen 2005. godine kompanija *idQuantique* i internet provajder iz Ženeve *Deckpoint* predstavili su mrežu koja omogućava skupu poslužilaca koji se nalaze u Ženevi bezbedno memorisanje podataka na lokaciju koja je udaljena 10 km, uz upotrebu ključeva distribuisanih kvantnom enkripcijskom vezom. U martu 2007. godine demonstrirana je kvantna razmena ključa na udaljenosti od 148,7 km, uspeh koji je postigla Los Alamos/NIST grupa korišćenjem BB84 protokola. Kompanija *idQuantique* je osigurala opremu u kantonu Ženeva, Švajcarska, da bi se poslali rezultati izbora koji su održani 21. 8. 2007. U oktobru 2008. godine kompanija *idQuantique* upotrebila je svoju opremu za uspostavljanje kvantnih mreža u Beču i Durbanu, za obezbeđenje izbora u Švajcarskoj.

Prvi računar na svetu zaštićen kvantnom kriptografijom implementiran je u avgustu 2008. godine na naučnoj konferenciji u Beču. Mreža je koristila 200 km standardnih optičkih kablova za povezivanje šest lokacija u Beču i grada St. Poeltena koji se nalazi 69 km zapadno. Evropska unija je 2004. godine pokrenula projekat zaštite komunikacionih kanala kvantnom kriptografijom, delimično i da spreči moguće prisluškivanje pomoću satelita Ešelon.

U eksperimentu 2004. godine kompanija NEC ostvarila je prenos ključa kvantnom kriptografijom na udaljenost većoj od 150 km.

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

Eksperiment koji je 2002. godine sprovela LosAlamos nacionalna laboratorija uspostavio je vezu u slobodnom prostoru na udaljenosti od 10 km. Iste godine kompanija *QinetiQ* iz Velike Britanije i univerzitet *Maximilian* iz Minhena uspostavili su vazdušnu vezu između dva planinska vrha u južnim Alpima na udaljenosti od 23,4 km. Evropska svemirska agencija je u ranim fazama ostvarivanja vazdušnog kriptografskog kanala između Zemlje i satelita. Najveća udaljenost postignuta u slobodnom prostoru je 144 km, što predstavlja udaljenost između dva ostrva iz Kanarskog ostrvlja, uspeh koji je postiglo evropsko udruženje korišćenjem isprepletenih fotona 2006. godine, korišćenjem modifikovanog BB84 protokola 2007. godine.

Ovi eksperimenti pokazuju da bi prenos podataka do satelita bio moguć, zbog niže gustine atmosfere na većim visinama.

Rekord u brzini prenosa kvantno kripovanih podataka ostvario je NIST (National Institute of Standards and Technology) brzinom od 4 miliona bitova u sekundi kroz optički kabal dužine 1 km. Kompanija NEC, National Institute of Information and Communications Technology i Japan Science and Technology Agency su u septembru 2004. godine ostvarili kvantni kripotografski kanal brzine 100 kb/s na udaljenosti od 40 km. Početkom 2003. godine kompanije *idQuantique* iz Ženeve i *MaqiQ Technologies* iz New Yorka predstavile su proizvode koji mogu slati kvantne kriptografske ključeve na udaljenosti prihvatljive za komercijalnu upotrebu tih sistema. Prosečna cena takvih sistema je od 70.000 do 100 000 dolara. Trenutno postoje četiri kompanije koje nude komercijalna rešenja iz područja kvantne kriptografije: *idQuantique*, *MagiQ Technologies, Quintessence Labs* i *SmartQuantum*. Takođe, kompanije *IBM*, *HP*, *Fujitsu*, *NEC* i *Toshiba* imaju svoje programe istraživanja kvantne kriptografije.

Zaključak

Kvantna kriptografija je u poslednjih dvadesetak godina doživela snažan razvoj. Pređen je veliki put od prvog eksperimenta u kojem su fotoni poslati kroz cev dužine 0,30 m. Danas je tehnologija napredovala dovoljno da se kvantna kriptografija može koristiti u velikom broju praktičnih primena. Ipak, to nije tako. Glavni je razlog svakako visoka cena kvantnih kriptografskih sistema, ali i način razmišljanja prema kojem kvantna kriptografija spada u domen naučne fantastike.

Kvantna kriptografija će svoj procvat doživeti ako ne pre onda kada kvantni računari postanu stvarnost. Tada algoritmi iz domena klasične kriptografije više neće pružati pouzdanu zaštitu od napada kao što je Šorov kvantni algoritam za faktorizaciju brojeva. Naravno, tada će nastati problem zaštite svih onih podataka koji su u prošlosti zaštićeni klasičnim kriptografskim sistemima, a postoji potreba za tajnošću tih podataka kroz duži niz godina [9,10].

Naravno, i kvantna kriptografija nije u potpunosti imuna na napade, ali za razliku od klasičnih napada, ti napadi su usmereni na probleme implementacije i autentifikacije. Takvi napadi mogu se sprečiti bez većih problema, ili implementacijom modifikovanih protokola ili sigurnijom i dodatnom opremom.

Literatura

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

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

[3] Tilborg, H., Encyclopedia of Cryptography Security, Springer, 2005.

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

[5] Oppliger, R., Contemporary Cryptography, Artech House, 2005.

[6] Lomonaco, S. J., A Quick Glance at Quantum Cryptography, arxive e-print quant.ph/9811056, 1998.

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

[8] Internet stranice:

-http://idquantique.com/

-http://magiqtech.com/

-http://www.quintessencelabs.com/

-http://www.smartquantum.com/-rubrique2-.html

-http://en.wikipedia.org/wiki/Quantum_cryptography

-http://www.nec.co.jp/press/en/0409/2701.html

-http://news.illinois.edu/scitips/02/0711quantumcrypt.html

[9] Kuljanski, S., *RSA algoritam i njegova praktična primena,* Vojnotehnički glasnik/Military Technical Courier, Vol. 58, No. 3, pp. 65–77, Ministarstvo odbrane Republike Srbije, Beograd, 2010.

[10] Evseev, S. P. (Евсеев, С. П.), Dorokhov, O. V. (Дорохов, А. В.), Korol, O. G. (Король, О. Г.), Mechanisms of protection of information in computer networks and systems (Механизмы и протоколы защиты информации в компьютерных сетях и системах), Vojnotehnički glasnik/Military Technical Courier, Vol. 59, No. 4, pp. 15–39, Ministarstvo odbrane Republike Srbije, Beograd, 2011.

PROTOCOLS AND PLAN OF QUANTUM CRYPTOGRAPHY

FIELD: Telecommunications
ARTICLE TYPE: Professional Paper

Summary

Along with the development of confidentiality of data and resources, there is a need to develop systems that would provide confidentiality. Currently, the most used systems are classical cryptographic systems and encryption public key systems. However, none of these systems provides a solution for the famous "catch 22" of cryptography. Owing to the intensive development of quantum mechanics, in the last 30 years emerged an entirely new kind of cryptography-quantum cryptography.

Its greatest contribution is a possibility to discover an intercepted communication channel from a third party. The question is: is this really true? The question arises: 'If the quantum cryptography is so good, why is not widely used?' The aim of this paper is, on the one hand, to define the basic mechanisms of quantum cryptography IP, and, on the other hand, to point to the shortcomings, as they related to the opportunities of today's devices and flaws in protocols.

Introduction

The aim of cryptography is the transmission of information data in a way that they are only available to the recipient, i.e. the person to whom they are designed for. At first the security of the encrypted text depended solely on the secrecy of the process of encryption and decryption. Today we use codes whose algorithms are publicly known, but it does not jeopardize the security of encrypted messages. In such a system secret key messages and clear text are entered as parameters in the algorithm.

Quantum protocols

Quantum cryptography exploits the properties of quantum states to ensure the safety of the system. There are several approaches to quantum key distribution, but they can generally be divided into two groups, depending on whether the qubits are independent from each other or not.
Some of the quantum protocols are as follows:

Prepare and measure protocols

A measurement process is an integral part of quantum mechanics. In general, the measurement of an unknown quantum state will change this situation. This is known as quantum ambiguity and is based on the results of the Heisenberg uncertainty principle and the no cloning theorem.

Entanglement based protocols

Quantum states of two or more separate objects can be linked in order to be described as a combined quantum state rather than as individual objects. This means that the implementation of measurements on one object affects the other one. If a pair of entangled objects is sent through a communications channel, an attempt to intercept any particle will cause a change in the whole system, which will lead to the discovery of the third party- an attacker in the communication channel.

BB84 protocol

The first quantum cryptographic protocol was created in 1984 (hence the name) by Gilles Brassard.

A sender ("A") and a receiver ("B") are linked by a quantum communication channel that enables the exchange of quantum states. In the case of photons, the communication channel is either an optical fiber or free space (ether).

B92 protocol

Unlike the BB84 protocol, which requires two orthogonal quantum alphabets (bases), the B92 protocol requires only one nonorthogonal alphabet. Let the – denote a photon polarized at an angle of 45^0 to the vertical where 0 <- <4 5^0 and let the - ' denote a photon polarized at an angle of 135^0 with respect to the vertical.

E91 protocol

The protocol is named after Artur Ekert who invented it in 1991. The Ekert scheme uses an entangled pair of photons. They can be created by A, B, or by any other separate source, including E. The photons are distributed so that A and B receive one photon from each pair.

Quantum cryptography data

I*t represents a quantum cryptography where data encryption tools are developed for information embedded in quantum systems. Some examples are as follows:*

Quantum one-time volumes

In this system, A and B share in advance a few maximally entangled particles and use them for the teleportation of an arbitrary qubit. The only public communication channel represents a few random bits sent by A to B, which enable the reconstruction of the original condition A wanted to send.

Quantum key distribution

The purpose of quantum key distribution is to enable two honest parties to agree on a random cryptographic key in situations where the interception is possible. However, in the communication between A and B, it can happen that a part of the accurately measured photons is detected incorrectly.

Error Measurement

Comparison and alignment of information
Privacy amplification

Possible attacks on a quantum cryptography system

Man-in-the-middle attack

Quantum cryptography is vulnerable to this attack when there is no authentication and classical cryptography. A and B cannot authenticate each other and establish a secure connection without any authentication methods such as a secret known to both parties.

Photon number splitting attack (PNS attack)

In the BB84 protocol, A sends quantum states to B using single photons. In practice, weakened laser pulses are used to send quantum states. These pulses contain a small amount of photons distributed according to a Poissonian distribution.

Directions of the development of quantum cryptography

The beginnings of quantum cryptography can be traced to the early 1970s, when Stephen Wiesner wrote a paper "Conjugate Coding". Wiesner suggested two areas of application:

• the creation of bank certificates that cannot be falsified and

• reproduction of two or three messages in a way that reading one destroys the other.

Quantum cryptography das

In 2004, the Defense Advanced Research Projects Agency (DARPA) launched the project of connecting six network nodes between the company BBN Technologies and Harvard and Boston Universities. The

encryption keys are sent through the quantum channel, and the messages encrypted by that key are sent through the Internet. This network represents the first quantum cryptographic network that is constantly in operation outside the laboratory.

Conclusion

In the past twenty years, quantum cryptography has experienced a strong growth from the first experiment in which the photons were sent through a tube 0:3 m long. Today's technology has progressed enough that quantum cryptography can be used in many practical applications. However, it is not. The main reason is certainly a high price of a quantum cryptography system and a way of thinking that quantum cryptography is one of the realms of science fiction.

Keywords: cryptography, keys, protocols, protection

Datum prijema članka: 28. 12. 2010.

Datum dostavljanja ispravki rukopisa: 05. 10. 2011.

Datum konačnog prihvatanja članka za objavljivanje: 06. 10. 2011.