

Univerzitet u Beogradu

Matematički fakultet

Kvantna kriptografija

student: Dragana Andrejić

broj indeksa: 1098/2012

predmet: Metodologija stručnog i naučnog rada

školska godina: 2012/2013

nastavnik: dr Vladimir Filipović

Sadržaj

1 Uvod

2 Istorijat

3 Kvantni računari

3.1 Princip kvantnih tranzistora. 4

3.2 Današnji ekspreimentalni kvantni kompjuteri. 5

3.3 Potencijal kvantnih kompjutera. 5

4 Kvantna razmena ključa

4.1 Protokoli “pripremi i izmeri” 5

4.2 Protokoli zasnovani na isprepletanosti. 5

5 Primena

6 Zaključak

1 Uvod

Kvantna kriptografija ili kvantna distribucija ključa (QKD) koristi kvantnu mehaniku kako bi omogućila bezbednu komunikaciju. Ona omogućuje dvema stranama da kreiraju zajednički nasumični bit string poznat samo njima, koji se može koristiti kao ključ za enkripciju i dekripciju poruka.

Važno i jedinstveno svojstvo kvantne kriptografije jeste sposobnost dva korisnika koja komuniciraju da uoče prisustvo treće strane koja pokušava da otkrije informacije o ključu. Ovo potiče od osnovnih aspekata kvantne mehanike: proces merenja kvantnog sistema u suštini narušava sam sistem. Treća strana koja pokušava da prisluškuje ključ ga na neki način mora meriti i tako izaziva nepravilnosti koje se mogu primetiti. Koristeći kvantne superpozicije ili kvantne isprepletenosti i prenoseći informacije u kvantnim stanjima može se implementirati sistem komunikacije koji je sposoban da prepozna prisluškivanje. Ako je nivo prisluškivanja ispod određenog praga vrednosti, može se stvoriti ključ koji će sigurno biti bezbedan (tj. prisluškivač neće moći da dođe do informacija o njemu), u suprotnom nije moguće ostvariti bezbedan ključ i komunikacija se prekida.

Bezbednost kvantne kriptografije se oslanja na osnove kvantne mehanike u poređenju sa tradicionalnom kriptografijom javnog ključa koja se oslanja na računsku težinu pojedinih matematičkih funkcija, i ne može da pruži indikacije o prisluškivanju ili garancije za sigurnost ključa.

Kvantna kriptografija se samo koristi za kreiranje i distribuciju ključa, ne i da prenese poruku sastavljenu od podataka. Ovaj ključ se može koristiti sa bilo kojim algoritmom za enkripciju po izboru, za enkripciju (i dekripciju) poruke koja se može prenositi preko standardnog kanala za komunikaciju. Algoritam koji se najčešće dovodi u vezu sa QKD-om je „one-time pad“ i njegova bezbednost je proverljiva kad se koristi sa tajnim, nasumičnim ključem.

2 Istorijat

Kvantna kriptografija je prvi put predstavljena od strane Stephena Wiesnera, na Kolumbija Univerzitetu u Njujorku, koji je ranih 70-ih godina prošlog veka predstavio koncept kvantnog kodiranja. Njegov rad, pod naslovom „Kodiranje konjugata“ (engl. Conjugate Coding) je bio odbačen od strane žurnala IEEE Informaciona Teorija, ali ipak biva objavljen 1983. godine u SIGACT News. U tom radu on je pokazao kako smestiti i poslati dve poruke koje su kodirane u dve „srodne pojave“, kao što je linearna i cirkularna polarizacija svetla, tako da bilo koja, ali ne obe, mogu biti poslate, primljene i dekodirane. Svoju ideju je ilustrovao kroz novčanice koje je nemoguće falsifikovati. Deset godina kasnije, nastavljajući njegov rad, Čarls H. Benet iz IBM centra za istraživanje, i Žiles Brassard sa univerziteta u Montrealu, predložili su metodu za sigurnu komunikaciju koja je bila zasnovana na Wiesnerovim „srodnim pojavama“. Nezavisno od njih Artur Ekert sa univerziteta u Oksfordu je 1990. godine razvio drugačiji pristup kvantnoj kriptografiji zasnovanoj na kvantnim korelacijama poznatim kao kvantna isprepletanost.

3 Kvantni računari

Šta je to, u stvari, kvantni računar?

Kvantni računari su računari koji pri svom funkcionisanju koriste kvantna svojstva mikro čestica. Oni se suštinski razlikuju od klasičnih kompjutera kod kojih se informacije bazično predstavljaju u obliku bitova (0 i 1). Kod njih su osnovne jedinice operacije tzv. kubiti, koji koriste kvantni fenomen superpozicije, tunel efekta i druge za operaciju nad informacijama.

Mogućnost ovakvih informacija su velike i ogledaju se u tome da bi neki matematički problemi mogli biti rešeni mnogo brže, nego kod klasičnih. Primer za to je Šorov, kvantni algoritam, koji bi mogao biti apsolutno najbrži način za faktORIZACIJU brojeva i koji bi bez problema dekriptovao svaku RSA šifru koja je danas u upotrebi (naši bankovni računi, šifre od mail naloga, vojne i državne tajne itd.)

Razvoj modernih kompjutera obeležava izuzetno brz rast brzine kompjuterskih procesora, koji možda i najbolje definiše čuveni Murov zakon, koji je postavio osnivač Intela Gordon Mur 1965.godine, a koji predviđa udvostručavanje količine tranzistora na procesoru svakih 18 – 24 meseca. Trend ovog ogromnog rasta je zahvaljujući velikom razvoju tehnologije važio preko 40 godina, ali se poslednjih godina primećuje njegovo usporavanje, pre svega usled toga što aktuelna silicijumska tehnologija mikroprocesora dolazi do svojih prirodnih i tehničkih granica. Iako je obeležila krucijalan period razvoja računara, sasvim je izvesno da će je uskoro zameniti nove tehnologije.

Već nekoliko decenija se razvijaju prototipi sa potpuno drugačijom tehnologijom tranzistora, kao što su: optički, molekulski, DNK, kvantni itd.

3.1 Princip kvantnih tranzistora

Kvantni tranzistori se suštinski razlikuju od klasičnih, silicijumskih tranzistora, kod kojih je princip rada jednostavniji i bazira se na tome da li u strujnom kolu ima struje (1 u binarnom kodu) ili nema struje (0 u binarnom kodu). Oni se, slično bitnovima kod klasičnih kompjutera nazivaju kubiti i predstavljaju osnovne jedinice operacije kvantnih računara. Njihov mehanizam rada je zasnovan na kvantnim slojevima čestica, koje imaju jedinstvenu sposobnost superpozicije, odnosno činjenici da jedna čestica u jednom trenutku može biti u više stanja sve dok ne izvršimo merenja i ne delujemo spoljašnom silom na nju. Oni mogu u binarnom sistemu predstavljati u određenom trenutku sve superpozicije stanja 0 i 1.

Uzmimo primer trobitnog registra kod klasičnih računara, stanje računara, odnosno tranzistora u bilo kom trenutku može biti jedno od $2^3=8$, odnosno 000,001,010,011,100,110,111, svakako znamo da se ovaj računar sigurno nalazi u jednom od ovih stanja i ukupna verovatnoća svih stanja je jednaka 1, s druge strane kod kvantnih računara kubiti mogu istovremeno biti u više ovih stanja. Kada bi neki klasični kompjuter izvršavao n operacija, teorijski bi sa istim brojem kubitova na kvantnom kompjuteru moglo da se izvrši 2^n operacija u istom

vremenskom intervalu, odnosno rast kapaciteta i brzine takvog, hipotetičkog kompjutera bi bio eksponencijalni.

Kubiti su sačinjeni od neke mikro čestice (atoma, elektrona, fotona...) i kontrolnih mikro uređaja, koji kontrolišu rad čestice i zadaju joj naredjenja, odnosno definišu njihovo stanje.

3.2 Današnji eksperimentalni kvantni kompjuteri

Većina današnjih kvantnih kompjutera se koristi na temperaturama bliskim apsolutnoj nuli, zbog specifičnih osobina superprovodljivosti, koje se javljaju na tim temperaturama. Mnogi eksperimentalni „kompjuteri“ koji uspešno funkcionišu se stvaraju iz dana u dan, a može se reći da je ovo trenutno jedna od najživljih oblasti nauke.

3.3 Potencijal kvantnih kompjutera

Iako su ovi računari tek na početku svog razvoja, njihov potencijal i mogućnosti su ogromne, pogotovo ako uspemo da otklonimo određene tehničke probleme i optimizujemo ih za rad u realnim uslovima (normalna temperatura, adekvatna veličina.) Kao pokazatelj potencijalnih mogućnosti ovih računara, najbolje je predložiti neke primere. Ako pri pretraživanju određenog broja nerazvrstanih informacija n , današnji kompjuteri obavljaju prosečno $n/2$ operacija, kvantni kompjuteri bi obavljali $\sqrt{n}$ operacija. To bi značilo da je kod velikog broja podataka brzina pretrage mnogo veća kod kvantnih nego kod klasičnih računara. Takođe, kada bi klasičnim putem faktorizovali broj od 300 cifara, za izračunavanje bi nam trebale hiljade godina, dok je kod kvantnih potrebna jedna sekunda.

4 Kvantna razmena ključa

Kvantna komunikacija podrazumeva kodiranje informacija u kvantna stanja ili qubit-e, nasuprot bitovima koji se koriste u klasičnoj komunikaciji. Obično se fotoni koriste za ova kvantna stanja. Kvantna kriptografija koristi pojedina svojstva ovih kvantnih stanja da bi osigurala bezbednost. Postoji nekoliko različitih pristupa distribuciji kvantnog ključa koji se mogu podeliti u dve glavne kategorije u zavisnosti od toga koja svojstva koriste.

4.1 Protokoli “pripremi i izmeri”

Za razliku od klasične fizike, postupak merenja je sastavni deo kvantne mehanike. Opšte uzevši, merenje nepoznatog kvantnog stanja će promeniti to stanje. Ova pojava je poznata kao kvantna neodređenost i počiva na rezultatima poput Hajzebergovog principa neodređenosti, Teoreme o narušavanju informacija i Teorema o ne-kloniranju. To se može iskoristiti kako bi se otkrivali pokušaji prisluškivanja komunikacijskog kanala i, što je još važnije, da bi se izračunala količina informacija koja je presretnuta.

4.2 Protokoli zasnovani na isprepletanosti

Kvantna stanja dva ili više odvojena objekta mogu postati povezana tako da se mogu opisati kao kombinovano kvantno stanje, a ne kao individualni objekti. To znaci da će

sprovođenje merenja na jednom objektu uticati na drugi objekat. Ako se isprepleteni par objekata pošalje komunikacijskim kanalom, pokušaj presretanja bilo koje čestice ce prouzrokovati promenu kompletnog sastava, što ce dovesti do otkrića treće strane, tj. napadača u komunikacijskom kanalu (kao i količine informacija do koje se dospelo). Ova dva pristupa se nadalje mogu podijeliti u tri porodice protokola: diskretne varijable, kontinuirane varijable i distribuirano fazno referentno kodiranje. Protokoli zasnovani na diskretnim varijablama su prvi nastali i do današnjih dana su najrasprostranjeniji. Protokoli ostalih dveju grupa su uglavnom orijentisani ka savladavanju praktičnih ograničenja u eksperimentima.

5 Primena

Sistem sa najvećom brzinom prenosa razmenjuje sigurne ključeve na brzini od 1 Mbit/s (preko 20 km optičkih vlakana) i 10 kbit/s (preko 100 km vlakana), što se postiže u saradnji Univerziteta u Kembridžu i kompanije Tošiba koristeći BB84 protokol s decoy/lažnim pulsevima.

Od marta 2007. najveća udaljenost na kojoj je razmena kvantnog ključa demonstrirana koristeći optička vlakna je 148.7km, ostvarena od strane Los Alamos National Laboratory/NIST grupe koristeći BB84 protokol. Važno je to da je distanca dovoljno velika za svako prožimanje koje može biti potrebno u današnjim mrežama od vlakana. Najveće ostvareno rastojanje za DKK u slobodnom prostoru je 144km između dva Kanarska ostrva, postignuto od strane evropskog udruženja koristeći isprepletene fotone (Ekertova šema) 2006. godine i koristeći modifikovan BB84 protokol u 2007. Eksperiment nalaže da je prenos do satelita moguć, zahvaljujući nižoj gustini atmosfere na većim visinama.

Trenutno postoje četiri kompanije koje nude komercijalne kvantne kriptografske sisteme: id Quantique (Ženeva), MagiQ Technologies (Njujork), SmartQuantum (Francuska) i Quintessence Labs (Australia). Nekoliko drugih kompanija ima aktivne istraživačke programe u ovoj oblasti, uključujući kompanije Toshiba, HP, IBM, Mitsubishi, NEC i NTT. Tehnologija za kvantnu enkripciju švajcarske kompanije Id Quantique je korišćen u ženevskom kantonu za prenos izbornih rezultata do prestonice 21. oktobra 2007.

Prvi bankovni transfer uz korišćenje kvantne kriptografije desio se u austrijskom gradu Beču 2004. god. Važan ček za koji je bila potrebna apsolutna sigurnost je prenesen od gradonačelnika ovog grada do Austrijske banke. Prva svetska računarska mreža zaštićena kvantnom kriptografijom je implementirana u oktobru 2008. na naučnoj konferenciji u Beču. Ime mreže je SECOQC (Secure Communication Based on Quantum Cryptography), a Evropska unija je finansirala projekat. Mreža koristi 200 km standardnog kabl od optičkih vlakana kako bi međusobno povezala šest lokacija u Beču i mestu Sant Polten, koji se nalazi 69 km zapadno od Beča.

6 Zaključak - perspektiva

Postojeći komercijalni sistemi su uglavnom orijentisani na zvanične insitucije i korporacije sa visokim sigurnosnim potrebama. Distribucija ključeva preko kurira se uglavnom koristi gde tradicionalna distribucija ključa ne pruža zadovoljavajuću sigurnost. Ovo ima prednost jer nema razdaljinsko ograničenje, i bez obzira na dugo vreme putovanja stopa transfera je visoka zbog postojeće infrastrukture koja nudi velike kapacitete uređaja za čuvanje podataka.

Najveća odlika kvantne kriptografije je mogućnost da se otkrije bilo kakvo presretanje sigurnosnih ključeva, dok kod kurira sigurnost ključa nije dokazana. Sistemi za kvantnu distribuciju ključa imaju i prednost što su automatski, imaju veću pouzdanost i manju cenu.

Faktori koji sprečavaju širu primenu kvantne kriptografije van visoko bezbednosnih oblasti su cena neophodne opreme, kao i činjenica da još uvek nije dokazano da postoji pretnja postojećim protokolima za razmenu ključeva. Ipak, mreže sa optičkim kablovima već postoje u nekim zemljama, tako da to daje nagoveštaj da će doći do šire primene.

References

1. *Informacione tehnologije- sadašnjost i budućnost*, Krstajić Božo (2012)
2. Slobodna enciklopedija, *Wikipedia* <http://www.wikipedia.org>.