

Kvantna kriptografija

Seminarski rad u okviru kursa
Tehničko i naučno pisanje
Matematički fakultet

Igor Glišović
mi22292@alas.matf.bg.ac.rs

Željko Zekavičić
mi22130@alas.matf.bg.ac.rs

Nađa Lazarević
mi22175@alas.matf.bg.ac.rs

Ana Mladenović
mi22119@alas.matf.bg.ac.rs

18. decembar 2022.

Sažetak

Čuvanje podataka sa klasičnom kriptografijom u moderno doba postaje teže, jer su se sa razvojem tehnologija razvijali i načini za lakše saznavanje tajnih ključeva. Javila se velika potreba za načinom na koji se može spoznati da li sistemu pristupaju treća lica. Rešenje se može naći primenom principa kvantnih čestica u sistemu kvantne mehanike i njihove neodređenosti i sprežanja na zaštitu informacionih sistema.

Sadržaj

1	Uvod	2
2	Istorijat	2
3	Principi kvantne kriptografije	3
3.1	Kvantni računari	3
3.2	Kvantni protokoli	4
3.3	Kvantna razmena ključa	4
3.4	Vrste napada na sisteme i odbrana	5
4	Implementacija kvantne kriptografije	5
5	Zaključak	6
	Literatura	7

1 Uvod

Kriptografija je nauka koja se bavi očuvanjem tajnosti informacija. Cilj je da se informacije prenesu od pošiljaoca do primaoca tako da smo sigurni da one nisu dospele do nekog trećeg lica. Pri samom nastanku kriptografije glavni problemi su bili na koji način sačuvati tajnost procesa enkripcije/dekripcije podataka (neki od prvih primera klasične kriptografije su Cezarova šifra¹ i Skital²), jer bi se nakon saznavanja procesa na koji se šifruju podaci, oni mogli lako dešifrovati.

Nakon mnogo vekova, nastankom i razvojem informacionih tehnologija, očuvanje sigurnosti podataka postaje još bitnije (ali i teže) nego što je nekad bilo. Kao jedan od najboljih načina za enkripciju podataka iz ere klasične kriptografije izdvaja se Vernamova šifra[3] tzv. *OneTimePad* - OTP). OTP se zasniva na principu generisanja nasumičnog dugačkog ključa dužine kao izvorna poruka koju šaljemo. Ovakav sistem radi samo ako svaki put generišemo novi kod, jer ako dva puta prosledimo isti, lako se može dešifrovati ono što smo poslali. Takođe, veliki problem kod ovakvog načina enkripcije predstavlja prenos dugačkog ključa, te bi sam proces slanja poruke trajao duže. Ovaj problem se rešava tako što ključ skraćuje na fiksnu dužinu za svaku poruku. Međutim, moderna kriptografija sada nailazi na novi problem (poznatiji kao Kvaka 22):

Komunikacija između pošiljaoca i primaoca je sigurna, samo ako znamo da je sigurna.

Ovde dolazimo do zaključka da se klasičnom kriptografijom nikako ne može znati da li je informacija kompromitovana od strane trećih lica u toku slanja poruke. Ovaj problem se rešava primenom osobina kvantne mehanike na prenos informacija u nekom informacionom sistemu.

2 Istorijat

Kroz celu istoriju čovečanstva postojala je potreba za sigurnom razmenom informacija. Problemom sigurne komunikacije bavili su se već Egipćani i Indijci pre više od 3000 godina i od tada do danas osnovna ideja se nije promenila, preneti neku poruku s jednog mesta na drugo što je sigurnije moguće.

Krajem dvadesetog veka čovečanstvo je ušlo u eru informacionih tehnologija. IT industrija, koja se bavi proizvodnjom, obradom, skladištenjem i prenosom informacija, postala je sastavni deo globalnog ekonomskog sistema, potpuno nezavisan i prilično značajan sektor privrede. Zavisnost savremenog društva od informacionih tehnologija je toliko velika da propusti u informacionim sistemima mogu dovesti do značajnih incidenata. Telekomunikacije su ključna industrija informacionih tehnologija. Međutim, informacije su tokom transporta veoma osetljive na razne vrste zloupotreba. Jedinice za skladištenje i obradu podataka mogu biti fizički zaštićene od nedobronamernih, što se ne može reći za komunikacione linije koje se protežu na stotine ili hiljade kilometara i koje je gotovo nemoguće

¹Cezarova šifra (1. vek p.n.e) se zasnivala na supstituciji, gde bi se pri šifriranju svaki karakter pomerio unapred za n-pozicija u alfabetu, a pri dešifrovanju pomerio unazad za n-pozicija

²Skital (5. vek p.n.e) je parče štafete koji su Grci koristili kako bi obavijali sakrivenu poruku oko nje i nakon toga došli do ispravne poruke

zaštititi. Stoga je problem zaštite informacija u sferi telekomunikacija veoma značajan. Kriptologija kao nauka i posebno njen deo kriptografija upravo se bave ovom problematikom.

Dugi niz godina su mnogi naučnici tražili način ostvarenja takve komunikacije između dve osobe koja bi garantovala privatnost. Kvantna kriptografija je relativno novija oblast koja se bavi obezbeđenjem sigurne komunikacije između pošiljaoca i primaoca informacije, koristeći zakone kvantne fizike. Cilj rada je da se upoznamo sa principima kvantne distribucije ključa (o čemu će biti reči u sekciji 3.2) za kodiranje informacija i osnovnim problemima koji se javljaju pri njenoj realizaciji.

Kvantna kriptografija je prvi put predstavljena[2] od strane Stephena Weisnera, 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. U međuvremenu, Charles H. Bennet[6] (koji je znao o Weisnerovoj ideji) i Gilles Brassard su počeli raditi na istom području, najpre kroz nekoliko članaka, a posle i eksperimentalnim prototipom koji je demonstrirao tehnološku ostvarivost koncepta. Taj se prototip sastojao od fotona koji su se provlačili kroz 30 cm dugu cev. Smer u kojem su fotoni oscilirali te njihova polarizacija predstavljaju 0 ili 1 niza kvantnih bitova ili kubita. 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 Principi kvantne kriptografije

Kvantna mehanika[5] se zasniva na sledećim aspektima:

- aspekt prirodne neodređenosti, isprepletanosti - superpozicije, odnosno da se čestice koje postoje ne nalaze samo na jednom mestu (mogu se naći na dva mesta istovremeno)
- aspekt kvantnog sprezanja, što znači da su dve nezavisne čestice uvek nerazdvojno povezane, čak iako ne postoji mogućnost njihovog međusobnog delovanja
- delovanje jedne čestice na drugu, pa čak i odmeravanje, promeniće prirodu druge čestice

Ovi aspekti su ključni za kvantnu kriptografiju, jer obezbeđuju sigurnost očuvanja ključa.

3.1 Kvantni računari

Ključna razlika između klasičnih računara i kvantnih računara je vid predstavljanja podataka. Na klasičnim računarima, podaci se predstavljaju pomoću bitova (0,1), dok se na kvantnim predstavljaju u kvantnim bitovima - kubitima. Kubit može biti neka mikro ili nano čestica (foton, elektron, atom) i radi uz pomoć nekog mikrokontrolera koji će joj zadati sledeće stanje (smer rotacije). Sve informacije se kodiraju u tzv. kvantna

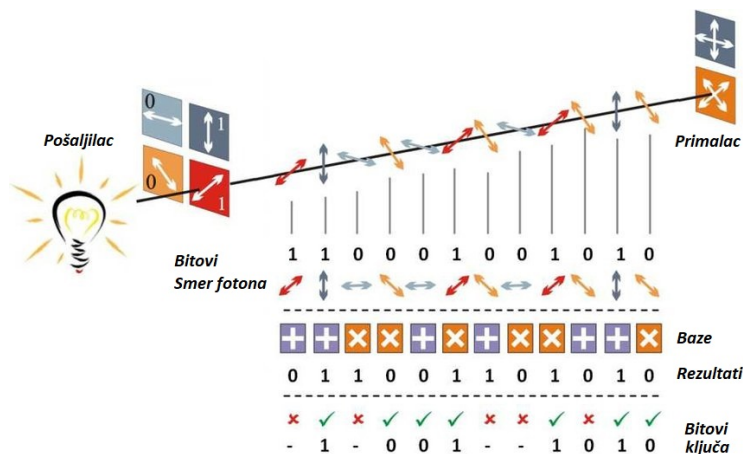
(neortogonalna) stanja. U našem slučaju podatke prenosimo putem optičkih kablova, a osnovne čestice su fotoni. Fotoni se pri kretanju rotiraju pod nekim uglom, a kada se više fotona rotira u istom smeru, onda su oni polarizovani fotoni. Polarizacioni filteri propištaju isključivo fotone koji su polarizovani u jednom određenom smeru, a ostale blokiraju. Prepoznavanje promene smera je zapravo indikacija da neko pokušava da sazna informacije, jer je pokušao da sazna ključ, a samim tim promenio smer rotacije nekih kubita.

Potencijal kvantnih računara je veliki jer bi se za n -operacija kod klasičnog računara, sa istim brojem kubita kod kvantnog računara moglo uraditi 2^n operacija (eksponencijalno rastući kapacitet).

3.2 Kvantni protokoli

Različiti kvantni protokoli[1] postoje zato što postoji razlika u distribuciji kvantnih ključeva (engl. QKD - Quantum Key Distribution), te razlikujemo nekoliko različitih protokola:

- BB84 protokol - prvi i najrasprostranjeniji protokol. Koristi jedan jednosmerni kvantni kanal i jedan dvosmerni javni kanal; bazira se na 4 neortogonalna stanja koja se mogu videti na Slici 1.
- B92 protokol - koristi 2 neortogonalna stanja.
- E91 protokol (Ekertova šema) - koristi isprepletani par fotona.
- SARG04 - otporniji BB84.
- Protokol šest stanja - tri para ortogonalnih polarizacionih stanja (najnoviji, ali najmanje efikasan).



Slika 1: Metodika rada BB84 protokola

3.3 Kvantna razmena ključa

Sigurni prenos informacija nemoguće je izvesti bez sigurnog prenosa ključa, stoga postoji nekoliko setova pravila (protokola) koje koristimo pri razmeni ključeva, a mi ćemo navesti dva najosnovnija.

Prvi tip je *"pripremi i izmeri"* tip protokola. On se zasniva na aspektu neodređenosti kvantnih čestica. Ovaj protokol koristi svojstvo kubita da promene stanje u odnosu na drugu česticu i tako otkriva potencijalan napad trećeg lica na ključ.

Drugi tip je zasnovan na osobini isprepletanosti kubita. Kubiti se kombinuju u veće celine (blokove kubita). Protokol kontroliše da se moguće greške u prenosu kao što je šum, ne poistoveti sa neovlašćenim napadom.

3.4 Vrste napada na sisteme i odbrana

Postoji nekoliko vrsta napada na kvantne kriptografske sisteme, i to:

- "Middleman"(središnja osoba) napad - dešava se jer nismo obezbedili autentifikaciju u sistemu
- PNS (photon-number splitting) napad - koriste oslabljene laserske pulseve kako bi došli do male količine informacije
- Hakerski napadi - ciljaju nesavršenost u implementacijama protokola umesto samih protokola (najčešće koriste lažna stanja ili "Trojance")
- DOS (Denial of Service) napad - blokiranje protoka informacije, "presretanje"

Kvantni kriptografski sistem biće siguran ako i samo ako obezbedimo da će svi delovi sistema raditi besprekorno. Moramo da se postaramo da nijedno treće lice ne može da pristupi uređajima za enkripciju/dekripciju koji se nalaze kod pošaljioca/primaoca informacije koje prenosimo. Pored toga moramo obezbediti da se svaki put generiše potpuno nasumična vrednost ključa (bez ikakve mogućnosti nalaska pravilnosti). Na kraju, moramo obezbediti da naš komunikacioni medijum ima siguran proces autentifikacije (potvrda identiteta).

4 Implementacija kvantne kriptografije

Naučnici su pokazali da kvantna distribucija ključa funkcioniše, ali se ne koristi previše zbog značajnih tehnoloških ograničenja. Da bi poslao kvantni ključ, laser sa jednim fonom emituje signal, preko optičkog kablova. Ova metoda je sporija od trenutnih telekomunikacionih tehnologija i zahteva namenski optički kabl između dve strane. Na primer, multinacionalna kompanija Amazon nije mogla da obezbedi transakcije klijenata korišćenjem kvantne enkripcije, jer bi joj bili potrebni kablovi između njenih internih servera i pojedinačnih uređaja koji vrše kupovinu. Udaljenost je takođe faktor. Kada se optički kablovi koriste za prenos podataka, kao u vašem kućnom internetu i kablovskim sistemima, oni koriste repetitore za slanje podataka na veće udaljenosti. Međutim, ti repetitori remete delikatno kvantno stanje koje je ključno za kvantnu distribuciju ključa.

Istraživači u Kini^[7] su demonstrirali kvantnu distribuciju ključa na velikim udaljenostima koristeći kombinaciju optičkih kablova sa "pouzdanim relejnim čvorovima" kao repetitorima i satelitom koji prenosi fotone kroz vazduh. Međutim, potrebno je više istraživanja da bi se stvorio sistem koji prenosi ključeve pouzdano i efikasno. U teoriji, kvantna kriptografija se ne može hakovati, jer bi prisluškivanje uvek bilo otkriveno, ali je njena praktična upotreba ograničena. „*Ako izgradite kuću, ona će biti jaka samo koliko i najslabiji stub*“, kaže Thomas Vidick³. „*Da biste imali istinski*

³Thomas Vidick je profesor na Kalifornijskom institutu za tehnologiju, poznat po radu u kvantnoj kriptografiji

upotrebljiv sistem, možda ćete morati da kombinujete kvantnu kriptografiju sa elementima koji nisu kvantni, a ti drugi elementi mogu biti ranjivi na napade koje teoretičari nisu predvideli.”

Shorov⁴ algoritam[4] je jedan od razloga zbog kojih je izvesna implementacija kvantnih sistema u budućnosti. Naime, ovaj kvantni algoritam se koristi za brzo izračunavanje prostih činioca nekog broja N , ma koliko taj broj veliki bio. Ovo predstavlja veliku opasnost za algoritme koji se danas koriste (poput RSA algoritma, kojeg koristi https protokol, ili Diffie-Helman razmenu ključa) jer oni rade na principu generisanja velikih prostih brojeva.

Postoji nekoliko značajnih produkta kvantne kriptografije početkom XXI veka, koji su hronološki poredani u tabeli ispod.

Naziv i godina projekta	Dužina prenosa
Prenos novca Creditanstalt banke, Austrija 2004.	1.45 km
IdQuantique i Deckpoint kolaboracija, Švajcarska 2005.	10 km
Povezivanje Kanarskih ostrva, Španija 2006.	144 km
SECOQC, prvi kvantno-kriptografski računar, Austrija 2008.	200 km

Tabela 1: Razvoj dužine prenosa kvantno-kriptografskih sistema

Kvantni računari se danas još više razvijaju, a komercijalne kvantne kriptografske sisteme danas mogu da ponude čak četiri kompanije: id Quantique (Ženeva), MagiQ Technologies (Njujork), SmartQuantum (Francuska) i Quintessence Labs (Australija). U ovoj oblasti postoji nekoliko kompanija koje poseduju aktivne istraživačke programe uključujući kompanije Toshiba, HP, IBM, Mitsubishi, NEC i NTT.

5 Zaključak

U poslednjoj deceniji je kvantna kriptografija doživela veliki razvoj. Postojeći komercijalni sistemi su uglavnom orijentisani na zvanične institucije i korporacije sa visokim sigurnosnim potrebama. Distribucija ključeva preko kurira se uglavnom koristi gde tradicionalna distribucija ključa ne pruža zadovoljavajuću sigurnost. Najveća prednost ovog sistema je to da u budućnosti neće imati razdaljinsko ograničenje, i bez obzira na dugo vreme putovanja stopa transfera je visoka zbog postojeće infrastrukture koja nudi velike kapacitete uređaja za čuvanje podataka. Visoka cena kvantnih kriptografskih sistema je jedan od faktora koji utiče na njenu širu primenu. Najveći svoj procvat doživeće, ako ne pre, onda kada kvantni računari postanu stvarnost. Nakon toga algoritmi iz domena klasične kriptografije neće pružati dovoljno dobru zaštitu kao što je Shorov kvantni algoritam za faktORIZACIJU brojeva. Tada će nastati problem zaštite svih onih podataka koji su zaštićeni klasičnim kriptografskim sistemima.

⁴Peter Shor je profesor na institutu u Massachusetts-u, tvorac post-kvantne kriptografije, zaslužan je za algoritme kvantnih izračunavanja

Literatura

- [1] Stjepan Picek, Marin Golub, *Kvantna kriptografija: razvoj i protokoli*. Fakultet elektrotehnike i računarstva, Zagreb, 2009.
- [2] Dragana Andrejić, *Kvantna kriptografija*. MATF, Beograd, 2013.
- [3] Mario Stipčević, *Kvantna kriptografija*, Institut Ruder Bošković, Zagreb, 2003.
- [4] Eduard Vojvodić, *Shorov algoritam za kriptiranje*, Fakultet prometnih znanosti, Zagreb, 2019.
- [5] [Stevan Jokić](#), *Kvantna kriptografija*, Institut za nuklearne nauke Vinča, Beograd, 2019.
- [6] Sandra Gašparić, Željka Draženović, *Kvantna kriptografija*, Fakultet organizacije i informatike, Varaždin, 2011.
- [7] Jennifer Torres, *How Will Quantum Technologies Change Cryptography?*, Institute of Technology, California, 2022.