

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

15. novembar 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 kvantne mehanike na zaštitu informacionih sistema.

Sadržaj

1	Uvod	2
2	Principi kvantne kriptografije	2
2.1	Kvantni računari	2
2.2	Kvantni protokoli	3
2.3	Kvantna razmena ključa	4
2.4	Vrste napada na sisteme i odbrana	4
3	Istorijat	4
4	Kvantna kriptografija danas	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 (tzv. *OneTimePad* - OTP). OTP se zasniva na principu generisanju 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 Principi kvantne kriptografije

Kvantna mehanika 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 sprežavanja, 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.

2.1 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

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

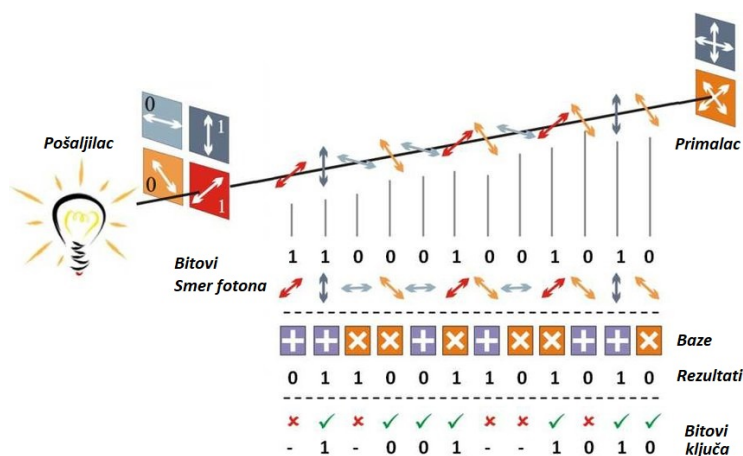
bitovima - kubitima. Kubit može biti neka mikro ili nano čestica (foton, elektron, atom) i radi uz pomoć nekog mikrokontrolera koji će joj zadati sledeće stanje (smer rotacije). Sve informacije se kodiraju u tzv. kvantna stanja. U našem slučaju podatke prenosimo putem optičkih kablova, a osnovne čestice 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).

2.2 Kvantni protokoli

Kvantni protokoli postoji zato što postoji razlika u distribuciji kvantnih ključeva, 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.
- B92 protokol - koristi 2 neortogonalna stanja.
- E91 protokol - 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

2.3 Kvantna razmena ključa

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

Protokoli kvantne razmene ključa	
"Pripremi i izmeri" tip protokola Zasniva se na aspektu neodređenosti kvantnih čestica i njihovog svojstva da promene stanje u odnosu na drugu česticu	Protokoli zasnovani na isprepletanosti Kombinovanje više kubita kako bismo otklonili mogućnost zamene greške prenosa (šumova) sa neovlašćenim napadom.

2.4 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 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).

3 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 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 za kodiranje informacija i osnovnim problemima koji se javljaju pri njenoj realizaciji.

Kvantna kriptografija je prvi put predstavljena 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 (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 gibali kroz 0.30 m dugu cev nazvanu „lijes tete Marthe“. Smer u kojem su fotoni oscilirali te njihova polarizacija predstavljaju 0 ili 1 niza kvantnih bitova ili qubita. 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.

4 Kvantna kriptografija danas

Koristeći BB84 protokol sa (decoy) lažnim pulsevima Univerzitet u Kembridžu u saradnji sa kompanijom Toshiba postiže sistem koji razmenjuje sigurne ključeve na brzini od 1 Mbit/s (preko 20 km optičkih vlakana) i 10 kbit/s (preko 100 km vlakana). On danas ima najveću brzinu prenosa. 2007. godine počevši od marta 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. Bitno je to da je distanca dovoljno velika za svako prožimanje koje može biti potrebno u današnjim mrežama od vlakana. Između dva Kanarska ostrva ostvareno je najveće rastojanje za DKK u slobodnom prostoru koje iznosi 144km. Postignuto je od strane evropskog udruženja pomoću isprepletene fotone (Ekertova šema) 2006. godine i koristeći modifikovan BB84 protokola u 2007. Zahvaljujući nižoj gustini atmosfere na većim visinama, prenos do satelita moguć. Švajcarska kompanija Id Quantique poseduje tehnologiju za kvantnu enkripciju koja se koristila u ženevskom kantonu za prenos izbornih rezultata do prestonice 21. oktobra 2007. Prvi bankovni transfer koji je koristio kvantnu kriptografiju bio je u Beču 2004. godine. Od gradonačelnika ovog grada do Austrijske banke prenesen je važan ček za koji je bila potrebna apsolutna sigurnost. Prva svetska računarska mreža zaštićena kvantnom kriptografijom je im-

plementirana u oktobru 2008. na naučnoj konferenciji u Beču. Ime mreže je SECOQC (Secure Communication Based on Quantum Cryptography), a Evropska unija je finansirala projekat. Kako bi međusobno povezala šest lokacija u Beču i mestu Sant Polten, koji se nalazi 69 km zapadno od Beča mreža koristi standardni kabl od optičkih vlakana dugačak 200 km.

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 što 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. 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.

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] [Stevan Jokić](#), *Kvantna kriptografija*, Institut za nuklearne nauke Vinča, Beograd, 2019.
- [5] Sandra Gašparić, Željka Draženović, *Kvantna kriptografija*. Fakultet organizacije i informatike, Varaždin, 2011.