KVANTNO ŠIFROVANJE KAO MOGUĆNOST ZAŠTITE INFORMACIJA

Milorad S. Markagić
e- mail: milmarkag@yahoo.com

Izvod- *Cilj ovog rada je da se šira populacija, koja nije usko vezana za oblast kriptologije upozna sa mogućnostima, pravcima razvoja i načinom korišćenja dostignuća kvantne fizike na polju zaštite informacija. Kao jedan vid zaštite informacija, moguće je primeniti kvantno šifrovanje, koje po svojim karakteristikama spada u simetrično šifrovanje, ali se zbog specifičnosti primene načina korišćenja i distribucije ključeva razmatra kao posebna celina.*

Ključne reči: *enkripcija, kvantna kriptologija, šifarski ključevi.*

1. Uvod

Kvantna kriptologija je nova grana kriptologije, koja se počela razvijati uporedo sa novim saznanjima u oblasti kvantne fizike, tako da su saznanja iz domena primene principa kvantne fizike u zaštiti informacija relativno u povoju i na takvom nivou gde se sa sigurnošću ne može tvrditi da su informacije koje bi se štitile ovim načinom u potpunosti bezbedne, kao i da su ključevi izradjeni ovom metodom u potpunosti bezbedni.

Razmotrićemo prilaz izrade ključeva, baziranih na elementarnoj jedinici nosioca, kao i mogućnosti enkripcije informacija ovim sistemima.

Ovde, kao i kod ostalih načina šifrovanja, pošiljalac i primalac poseduju tajni slučajni bitni raspored (binarni brojevi), poznat kao ključ, koji se koristi za kriptovanje (enkripciju) od strane pošiljaoca i za dekriptovanje (dekripciju) od strane primaoca, odnosno služi za prenos informacije o početnim stanjima koja će se koristiti za enkripciju/dekripciju. Ključ materijal je, izuzetno značajno pomoćno sredstvo čak iako sam ne prenosi informacije. Medjutim, početni korak ključ distribucije, pošto obe strane moraju posedovati ključ materijal, mora biti postignut sa velikim nivoom pouzdanosti tako da treća strana ne može da se domogne čak ni delimične informacije o slučajnom bitnom rasporedu.

U standardnim komunikacijama, koje su uvek predmet pasivnog nadgledanja i prisluškivanja, nemoguće je stvoriti verodostojan ključ, tako da su potrebne glomazne fizicke mere bezbednosti za generisanje ključa, distribuciju, čuvanje i uništenje posle korišćenja. Ipak, sigurna ključ distribucija postaje moguća ako dve strane mogu komunicirati sa jednofotonskim prenosima koristeci tehnologiju u razvoju kvantne kriptologije, ili preciznije, kvantum ključ dustribuciju (QKD). Bezbednost QKD-a je bazirana na fundamentalnim principima kvantne fizike. Ova jedinstvana tehnologija, omogućava nesalomivu ekspanziju komunikacija izmedju bezbednih delova preko otvorenih optičkih kablovskih mreža.

QKD nudi dosta sigurnosti i smanjeno korišćenje već postojećih ključ distribucionih metoda. Tradicionalna ključ distribucija koristeći poverljive načine prenosa zahteva

glomazne bezbedonosne procedure za pripremu, transportu i rukovanje ključem pre nego što dodje do bilo koje komunikacije, često je nepraktična.

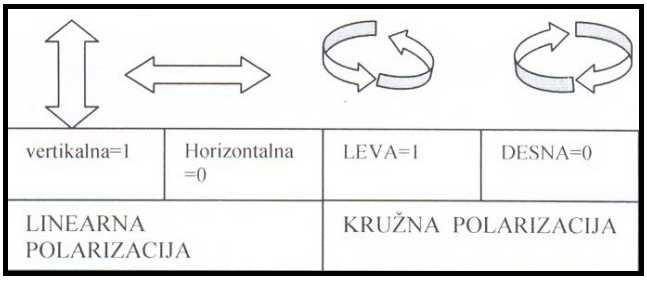
Suprotno tome, kvantum ključevi uopšte ne postoje pre QKD prenosa i ključ može biti generisan u transmisionom vremenu poruke.

Javni ključ kriptografije takodje izbegava mnoge poteškoće ključ distribucije preko kurira i obezbedjuje samo uslovnu bezbednost neobradivog matematičkog problema kao što je celobrojna faktorizacija. Procene protivničke moći izračunavanja preko praktičnog životnog veka kriptovanih informacija, koje mogu iznositi godine pa čak i decenije, su poznato teške.

Nepredvidjena napredovanja na poljima kao što je kvantno izračunavanje mogu načiniti javne ključ metode ne samo nesigurnim u budućnosti već i retroaktivno ranjivim. QKD može biti korišćen za generaciju realnog vremena u kriptografskim primenama gde je ovaj dugoročan rizik neprihvatljiv.

2.Principi na kojima se zasniva QKD

Ova tehnologija se zasniva na jednom od osnovnih principa kvantne fizike: Hajzenbergovom principu neodredjenosti. Kao što je na slici 1. dato, jedna od osobina fotona- polarizacija podleže sledećem principu:



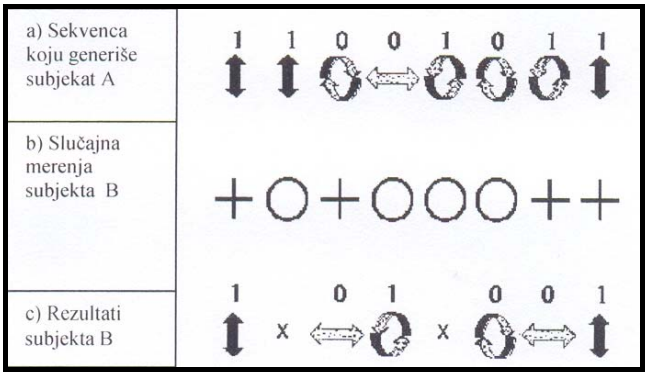
Slika 1: Polarizacija fotona

Fotoni, budući da predstavljaju jednu vrstu elektro-magnetnih talasa mogu biti polarizovani linearno ili kružno. Prilikom detekcije polarizacije jednog usamljenog fotona, moguće je detektovati samo jednu od ove dve vrste polarizacije-kružnu ili linearnu, a nikako obe. Razlog te nemogućnosti nije nesavršena tehnologija koja ne može da detektuje obe polarizacije istovremeno, već princip Hajzenberga kome su ljudi skloniji da veruju nego u priče o složenosti faktorisanja velikih brojeva.

Dakle, pošto je detekcija obe vrste polarizacije fotona nemoguća, nemoguće je i kopiranje informacije koju nosi jedan foton.

Prenos kvantnog ključa: Pretpostavimo da dve indvidue imaju na raspolagaju neki javni kanal, jedan direktni optički kabal i svu potrebnu opremu za prenos pojedinačnih fotona. Neka subjekat A šalje fotone optičkim kablom subjektu B , a na kanalu se nalazi i kriptoanalitičar koji prisluškuje-prati komunikaciju. Prisluškivač može da postavi detektore polarizacije na liniju i da pokuša da snimi fotone koji prolaze, ali on za svaki pojedinačni

foton mora da odabere koju vrstu polarizacije će da detektuje. Proces počinje tako sto A generiše slučajan niz bita i kodira svaki od njih koristeci po jedan foton polarizovan na slučajan način (kružno- levo ili desno, ili linearno – horizontalno ili vertikalno).



Slika 2: Primer prenosa kvantnog ključa

Sekvenca koju generiše subjekat **A** je data na slici 2 pod a). **A** je generisao niz bita 11001011 i koristio linearnu polarizaciju za prvi i drugi bit, kružnu za treći itd. Na prijemnoj strani, **B** nezavisno od **A** za svaki foton koji dobije slučajno odabira vrstu i tip polarizacije koju će da meri.

Na primer izabraće linernu polarizaciju za prvi i drugi foton, kružnu za treći, četvti, linearnu za peti, šesti itd. Merenja koja je B dobio data su na slici 2 pod c); sa **x** su označeni intervali u kojima je došlo do greške u merenju usled uticaja šuma ili jednostavno foton nije stigao do **B**. Potom **B**, preko javnog kanala izveštava **A** da je uspeo da detektuje prvi, drugi, treći, peti, šesti i osmi bit koristeći linearnu, linearnu, kružnu, kružnu, linearnu i linearnu polarizaciju. Važan detalj je da **B** ne saopštava i šta je dobio kao informaciju, već samo koju je vrstu polarizacije koristio za detekciju. **A** mu zatim (preko javnog kanala) saopštava da zadrži bitove 1, 3 i 8 a da ostale odbaci. Na ovaj način oni dolaze do sekvence bita 101 koja predstavlja njihov polazni, takozvani sirovi ključ.

Ako kriptoanalitičar prisluškuje vezu izmedju **A i B**, pokušava da kopira fotone koje detektuje i pošalje ih **B**, u 50% slučajeva kriptoanalitičar će pogoditi vrstu polarizacije koju ja **A** koristio i saznaće te bitove. Medjutim, u 50% slucajeva kriptoanalitičar neće pogoditi vrstu polarizacije. Što je još važnije u polovini od tih bita će generisati fotone sa suprotnom informacijom od one koja je bila poslata. Ovo sve rezultuje time da je 25% bita, za koje su se **A i B** složili da su koristili istu polarizaciju, pogrešno.

2.1.Sirovi ključ

Da bi ovo otkrili, A i B (preko javnog kanala) nastavljaju da ispituju sirovi ključ. Podele ga na blokove i saopšte jedan drugom parnost svakog od tih blokova. Kada otkriju blokove u kojima im je parnost različita, nastavljaju sa deljenjem tih blokova i ispitivanjem parnosti, i tako mogu tačno da utvrde procenat i lokaciju pogrešnih bita u ključu. Ako vide da je procenat pogrešnih bita visok (25% i veći), mogu sa sigurnošću da zaključe da ih neko prati, ubacuje se u vezu, i da počnu ponovo sa procedurom prenošenja ključa.

Kriptoanalitičar po ovom pitanju ne može ništa da uradi. Postoje metode koje smanjuju procenat pogrešno generisanih fotona, ali na račun smanjivanja informacije koju kriptoanalitičar može da dobije. Bitno je da teorija kvantne fizike garantuje da je količina informacije koju kriptoanalitičar može da dobije prsluškivanjem direktno proporcionalna procentu greške koju on unosi u prenesenu informaciju i da kriptoanalitičar ne može da prisluškuje razgovor izmedju A i B, a da to oni ne saznaju.

Nećemo razmatrati komplikacije koje nastaju u slučaju da kriptoanalitičar može da modifikuje poruke koje se prenose preko javnog kanala i da odgovara na poruke subjekta A, pretvarajuci se da je B i obrnuto. Kriptolozi su tome posvetili posebnu pažnju, pa postoje kriptografske metode proveravanja autentičnosti javnih poruka koje eliminišu i tu mogućnost, koristeći ključ za koji se sigurno zna da je tajni.

3 Eksperimenti kvantne kriptografije

Jedan sproveden eksperiment u SAD krajem 20-og veka pokazao je izvesne prednosti QKD prenosa u odnosu na klasični prenos ključeva.

Fizički sistemi koji mogu podržavati QKD prenose, odredjuju potencijalnu upotrebu kvantne kriptografije. Pokazano je da je QKD moguć preko velikog broja kilometara puta optičkih kablova: neophodna kvantum koherencija QKD prenosa istrajna je čak i izvan kontrolisanog okruženja fizičke laboratorije. U potrebnoj infra-crvenoj talasnoj dužini germanijum ili indijum-galijum arsenid, izazivaju lavinu fotodioda i mogu biti navedene da detektuju pojedinačne fotone, ali se javlja visok nivo greške zbog velike buke.

Otklanjajući ove greške smanjujemo obim ključa (materijala) i ograničenje prenosnih daljina na 100 kilometara i više. Optički filter se ne može koristiti da bi se povećalo ovo rastojanje zato što ne može da umnožava neortogonalna kvantum stanja koja se koriste u QKD. U ovom eksperimentu demonstrira se preko 24 km optičkog kabla koji je postavljen za aplikacione mreže izmedju dve LANL tehničke oblasti. Nedavno je ova udaljenost povećana na 48 kilometara.

Ovaj sistem ujedinjuje enkripcone/dekripcione odlike koje dozvoljavaju korišćenje kvantum ključ materijala da bi se kriptovale kratke tekstualne poruke na računaru pošiljaoca i dekriptovale na računaru primaoca. Ovaj eksperiment pokazuje da QKD može da se koristi za stvaranje kriptografskih ključeva preko otvorenih optičkih kablovskih veza medju bezbednim stanicama, kao što je to uradjeno medju različitim državnim organima u Vašingtonu.

U posebnom i odvojenom eksperimentu razvijan je QKD za vazdušni prostor, linija posmatranja komunikacija kao zemlja-avion. Do sada se postigao nizak nivo greške prenosa preko 205 metara, unutar laboratorije, ali daljina će se povećavati na nekoliko kilometara.

Ovi novi eksperimenti će se obavljati na otvorenom prostoru i dozvoliće da se proceni pozadina dnevne svetlosti i pitanja atmosferske optike koje će uticati na dužinu ključa i nivo greške. Kvantna kriptografija će verovatno biti prva praktična aplikacija koja

će koristiti osnove kvantne mehanike, što ilustruje česte neočekivane vrednosti osnovnih istraživanja.

4. Kratko o kvantnom izračunavanju

Ranih 80-ih godina prošloga veka Ricard Finmen (izmedju ostalih) počinje da istražuje pojam konvencionalne informatičke nauke u kvantnim fizičkim procesima. On razmatra predstavu binarnih brojeva sa ortogonalnim kvantum stanjima s (| 0>| ili | 1>|) kvantnog sistema na dva nivoa. Predstava jednog bita informacije u ovom obliku postala je poznata kao "qubit.". Sa dva ili više qubit-ova postaje moguće razmatrati kvantne logičke gate operacije u kojima kontrolisano medjusobno delovanje izmedju qubit-ova stvara (koherentnu) promenu stanja jednog qubit-a koji je zavisan od stanja drugog qubit-a.

Ove gate operacije su temelji kvantum računara (QC), koji je u principu mnogo moćnija naprava nego bilo koji klasični računar zato što superpozicioni princip dozvoljava izvanredno veliki broj izračunavanja koja se mogu izvesti.

Najvažniji rezultat u ovoj oblasti postigao je P. Sor pokazavši da se faktorizacija broja može izvršiti u polinomijalnom vremenu na kvantnom računaru, odnosno pokazano je da ovaj kvantni paralelizam može da se koristi da se efikasno pronadju glavni činioci složenih celih brojeva. Celobrojna faktorizacija i srodni problemi koji se ne mogu izračunati na običnim računarima su osnove sigurnosti modernog javnog ključ kriptosistema. Ipak, kvantni računar bi mogao da provali ključeve ovih kriptosistema u trenu (suprotno mesecima i godinama potrebnim za obične računare). Ovi pojedinačni rezultati su okrenuli kvantno izračunavanje od striktno akademske vežbe do predmeta čija prakticna izvodljivost mora biti hitno odredjena.

Arhitektura kvantum računara je koncepcijski vrlo slična konvencionalnom računaru: multi- qu- bit registri se koriste za ulaz podataka; sadržaj registara izražava logičke gate operacije da bi postigla željeno izračunavanje pod kontrolom algoritma i konačno rezultat mora biti prikazan kao sadržaj registra.

Osnovne smetnje u konstrukciji praktičnog kvantum računara su:

- teškoće konstruisanja potrebnih kvantum stanja,
- fenomen "dekoherencije" koji je svojstven za ova kvantum stanja da gube njihove koherencione osobine kroz interakcije sa okolinom, i
- kvantum veličine potrebne da bi se prikazali rezultati kvantum izračunavanja.

Prvi predlozi za izračunljivi hardver, baziran na raznim neobičnim tehnologijama, podlegao je jednom ili više ovih problema. Ipak, je predloženo da osnovne logičke gate operacije kvantum izračunavanja mogu biti eksperimentalno izvedene sa laserskim rukovanjem hladnim, zarobljenim jonima: qu-bit bi sadržavao podlogu stanja (| 0>|) i pogodno izabrano metastabilno pobudjeno stanje (|1>|), jona izolovanog od okoline sa elektromagnetnim poljima linearne radiofrekvencije quadrupole (RFQ) zarobljenog jona. Osnovni elementi ove tehnologije su već dobro razvijeni za frekvencioni standard i visokoprecizan spektroskopski rad. Postojeći eksperimentalni podaci nagoveštavaju da adekvatna vremena koherencije mogu biti dostignuta i prikazne metode bazirane na takozvanim kvantum skokovima, su već demonstrirane sa pojedinačnim zarobljenim jonima. Osim toga, logičke kvantum gate operacije su nedavno demonstrirane sa verzijom

ove ideje od strane **NIST** grupe u **Boulder, CO**. Oni razvijaju eksperiment kvantum računara zarobljenog jona koristeci kalcijum jone sa osnovnom objektivnošću prikazivanja višestrukih gate operacija na registru nekoliko qubit-ova (i mogućnost malih izračunavanja) da bi se odredile i moguće fizičke granice ove tehnologije.

5. Prednosti i nedostaci ovog metoda

Važno je napomenuti da je prenošenje podataka posredstvom pojedinačnih fotona još uvek nepraktična metoda. Brzina prenosa podataka po ovakvoj liniji je nekoliko stotina bita u sekundi, pa se ovakav kanal koristi samo za dogovor oko tajnog ključa, dok se prava komunikacija, koju treba zaštititi, odvija preko javnog kanala, šifrovana ovako prenesenim ključem.

Postoje i druge prepreke za praktičnu primenu kvantne kriptografije. Domet pojedinačnog fotona kroz optičko vlakno, je uz današnju tehnologiju, svega stotinak kilometara, što sprečava pošiljaoca i primaoca poruke da budu na vecoj udaljenosti. Ipak ako su oni računari, može postojati mreža računara direktno povezanih u celo svetu. Sve ovo zahteva puno vremena i računarske opreme, ali je ostvarljivo u bliskoj buducnosti.

6. Zaključak

Iz izlaganja možemo zaključiti da ne postoji idealana enkripcija informacija. Ukoliko jedan metod ima nedostataka u odredjenom pravcu, u drugom metodu, koji se pojavi kao ispravka, obavezno sejave poteškoće neke druge prirode.Kod simetričnog šifrovanja,kao najjednostavnijeg metoda sa velikom propusnom moći, svi napadi na ovaj sistem su napadi na metod korišćen za generisanje niza znakova ključa. Ako se u tu svrhu koristi kriptografski slab algoritam, to može da izazove nesagledive posledice. Ako se koristi pravi izvor slučajnih brojeva, to je teže izvodljivo i sistem se može smatrati sigurnim.

Problem se u ovim metodama javlja u distribuciji samog ključa od pošiljaoca do primaoca jer oni mogu biti veoma udaljeni jedan od drugog.

Medjutim ovaj metod rešava glavni problem tajnosti ključa u simetričnoj metodi, jer se zasniva direktno na Hajzenbegovom principu neodredjenosti polarizacije fotona. Ostaje da se u budućnosti povećaju tehnološke granice da bi ovaj način prešao, sa eksperimentalnog u globalno korišćenje.

Što se razvoja kriptologije tiče, može se reći da će 1024-bitni RSA ključevi ostati sigurni još najmanje 10 godina, isključujući neočekivana otkrića kompletno novog algoritma koji je bolji od GNFS-a, ili razvoj praktičnog kvantnog računara.

Literatura:

[1] Quantum Information at Los Alamos National Laboratory,1994.g
[2] Zoran Budimirović, Kvantna kriptografija, 1999.g.
[3] dr Miodrag Živković, Algoritmi, Beograd 2000.g.
[4] Internet

QUQNTUM ENCRIPTION AS MODE SCREEN WITHIN TELLING

Abstract – *The aim of this paper is that people who are not so associated to cryptology domain get familiar with capabilities, directions of development and methods of quantum physics usage in the information protection area.*
As one way of information protection, the quantum encryption can be performed. Considering the characteristics of that kind of encryption, it might be supposed as a symmetric encryption. Because of the specific usage and key distribution, it can be deliberated as a totally different area.

Key words: *encryption, quqntum cryptology, encryption keys.*