UDC: 659.2:004 Info M: str. 37-42

OPŠTI ASPEKTI KVANTNE KRIPTOGRAFIJE
GENERAL ASPECTS OF QUANTUM CRYPTOGRAPHY

Petar Čisar

REZIME: Kvantna kriptografija je relativno novija oblast računarske sigurnosti koja se bavi obezbeđenjem sigurne komunikacije između pošiljaoca i primaoca informacije, koristeći kvantno-mehanički pristup. Ona predstavlja vid prevazilaženja metoda klasične kriptografije: asimetričnih i simetričnih algoritama, koji se koriste već više desetina godina. Podrazumeva uspostavljanje kvantnog kanala između učesnika, u kome se za prenos informacija koriste fotoni. Bazu kvantne kriptografije čine odgovarajući protokoli, koji definišu algoritam i način razmene i tumačenja informacija. Ovaj vid sigurnosnih mehanizama ima svoje nesumnjive teoretske prednosti, ali ima i čitav niz problema u vezi sa praktičnom realizacijom. Rad predstavlja pregled opštih kvantnih principa i njihovih karakteristika na kojima počiva ova forma kriptografije i u kome se ukazuje na trenutne prednosti i nedostatke kvantne distribucije sigurnosnog ključa.

KLJUČNE REČI: kvantna kriptografija, kvantna distribucija ključa, fotoni, kriptografski protokoli

ABSTRACT: Quantum cryptography is a relatively new area of computer security that deals with providing secure communication between the sender and recipient of information, using quantum-mechanical approach. It represents the vision of overcoming the classical methods of cryptography: asymmetric and symmetric algorithms, which have been used for several decades. It involves the establishment of a quantum channel between the participants, in which the transmission of information is realized using photons. The base of the quantum cryptography is formed by appropriate protocols that define the algorithm and method of exchanging and interpreting information. This type of security mechanisms has its undeniable theoretical advantages, but there are a number of problems related to the practical realization. The paper presents an overview of the general quantum principles and their characteristics underlying this form of cryptography and highlights the current advantages and disadvantages of quantum distribution security key

KEY WORDS: quantum cryptography, quantum key distribution, photons, cryptographic protocols

UVOD

Prilikom pristupa korisnika osetljivim podacima, sigurnosni mehanizmi su od vitalnog značaja za sprečavanje eventualnih zloupotreba. U tom cilju se u korisničke aplikacije implementiraju razni vidovi sigurnosnih zaštita. Postoje aplikacije kod kojih se zahteva manji stepen sigurnosti. Kod njih je dovoljno osloniti se na sigurnost koja je realizovana na nivou mreže. U slučaju aplikacija za finansijske operacije zahteva se visok stepen sigurnosti, pa se kod njih pored sigurnosti na nivou mreže moraju implementirati mere koje obezbeđuju sigurnost i na aplikativnom nivou.

Kada se donese odluka o tipu aplikacije, prenosnim uređajima i mreži koja će se koristiti, moraju se uspostaviti i zahtevi za sigurnost. Na ovom nivou mora se odrediti koji će stepen zaštite i sigurnosti biti obavezan za aplikaciju. U mnogim slučajevima upravo stepen zaštite određuje koji uređaji i koji tipovi mreže će se koristiti.

Sigurnosni napad se može definisati kao bilo koja akcija koja ugrožava sigurnost informacija. Napadi se mogu podeliti na sledeće opšte kategorije:

- Presecanje, prekidanje (engl. *interruption*) – napad na raspoloživost. U slučaju napada ove vrste komunikacija između pošiljaoca i primaoca informacije je prekinuta, što ima za posledicu da primalac nije primio informaciju. Napadač ne dozvoljava da informacija stigne na odredište. Ova vrsta napada se obično detektuje od obe strane (pošiljaoca i primaoca). Mehanizmi za realizaciju presecanja se baziraju na:
  - ✓ onemogućavanju komunikacionog linka – npr. sabotaža (fizičko oštećenje), onemogućavanje interfejsa mrežnih uređaja, stvaranje ometajućih polja i šumova prema linku
  - ✓ onemogućavanju rutiranja – npr. izmena tabela za rutiranje
  - ✓ onemogućavanju servisa – npr. bombardovanje paketima, eliminacija servisa (web, mail, DNS itd.)
- Hvatanje (engl. *interception*) – napad na poverljivost. Kod ovog oblika napada napadač uspeva da primi informaciju koju je pošiljalac poslao, ali je i primalac dobio tu informaciju. Ovaj oblik napada se teško otkriva. Hvatanje se realizuje putem sledećih mehanizama:
  - ✓ prisluškivanje (telefonskih linija, e-mail-a,instant poruka i drugih metoda komunikacija koje se smatraju privatnim)
  - ✓ monitoring komunikacionog linka
  - ✓ hvatanje paketa
  - ✓ kompromitacija sistema (neko od zaposlenih dostavlja poverljive informacije napadaču)

Hvatanje olakšavaju sama priroda bežičnog prenosa informacija, paketska distribucija, višestruki zahtevi raznih aplikacija i protokola, promiskuitetni način rada mrežnih operacija, kao i funkcionisanje mnogih protokola kod kojih se podaci prvo smeštaju, a zatim prosleđuju dalje.

- Izmena (engl. *modification*) – napad na integritet. Modifikacija podrazumeva da je napadač u mogućnosti da blokira prenos podataka, primi informaciju, izvrši njenu mo-

difikaciju i tada je tako izmenjenu pošalje primaocu. Ovu formu napada je moguće otkriti ukoliko se primenjuje provera enkripcije, potpisa ili ispravnosti. Mehanizmi za realizaciju modifikacije: slanje podataka sa izmenjenom IP adresom u zaglavlju (engl. *IP spoofing* - primalac je u ubeđenju da sadržaj koji je primio potiče od legitimnog pošiljaoca) i ugrožavanje sistema (podaci se modifikuju dok je informacija još kod pošiljaoca). Smeštanje i kasnije prosleđivanje informacija pružaju mogućnost za realizaciju modifikacije. Savremeni komunikacioni uređaji imaju mogućnost prijema i originalne informacije, čime su stvoreni uslovi za upoređenje, što otežava uspešnost realizacije ovog tipa napada.

- Fabrikovanje (engl. *fabrication*) – napad na autentičnost. Kod ovog tipa napada, napadač generiše informaciju i šalje je primaocu, pretvarajući se da potiče od legitimnog pošiljaoca. Fabrikovanje može biti zastupljeno kod push – tehnologija (reklame (e-mail ili web), pop – up klijenti, agenti i dr.).

Sigurnosni mehanizam je kompleksni skup hardverskih i softverskih komponenata koji je dizajniran da detektuje, predupredi ili oporavi sistem od sigurnosnog napada.

KLASIČNA KRIPTOGRAFIJA - SIGURNOSNI MEHANIZMI NA NIVOU PODATAKA

Razvoj elektronskog poslovanja doneo je problem identifikacije korisnika i institucija na internetu. Najčešće korišćeni posupak asimetrične kriptografije ne nudi rešenje za administraciju javnih ključeva, koja bi svim učesnicima omogućila kreiranje lanca poverenja, neophodnog za sigurno poslovanje. Infrastruktura javnih ključeva (engl. *Public Key Infrastructure – PKI*) daje rešenje za identifikaciju. PKI predstavlja skup postupaka i pravila za kreiranje digitalnih sertifikata, karakterističnih kako za standardnu, tako i za mobilnu sigurnost. U daljem tekstu daće se prvo prikaz kriptografije.

Kriptografiju je moguće definisati na više načina, a jedan od njih je: Kriptografija je nauka o tajnom pisanju (zapisivanju), koja se bavi metodama očuvanja tajnosti informacija[1].

Kriptografija obuhvata matematičke transformacije kojima se modifikuju podaci tako da samo korisnici sa pravom pristupa, odnosno „pravim“ ključem mogu da ih prepoznaju. Tokom kriptografskog postupka originalni podaci, koji se nazivaju čist (čitljiv) tekst (engl. *clear text* ili *plain text*) određenom matematičkom funkcijom se transformišu u zaštićeni ili enkriptovani format (engl. *ciphertext*). Kriptografski algoritam transformiše čitljiv tekst u nečitljiv tekst.

Kriptoanaliza je nauka o dekripciji i analizi kodova i enkriptovanog teksta[2].

Primenjena funkcija se bazira na enkripcionom algoritmu, koji za ulazne parametre ima originalnu poruku i jedan ili više kriptografskih ključeva (specijalno izabranih nizova brojeva konačne dužine). Obrnuti proces, transformacija iz zaštićenog oblika poruke u originalnu poruku naziva se dekripcija i takođe je baziran na primeni matematičke funkcije, koja za ulazne podatke ima prethodno zaštićenu poruku i jedan ili više dekripcionih ključeva, koji mogu biti različiti od enkripcionih ključeva. Pouzdanost i snaga svakog kriptografskog procesa zasniva se ne samo na tajnosti enkripcionog – dekripcionog algoritma (u današnje vreme većina kriptografskih algoritama je u javnom vlasništvu), već i na tajnosti i karakteristikama ključeva.

U kontekstu sigurnosti računarskih sistema, gde kriptografske metode nalaze primenu, mogu se formulisati i sledeće definicije:

Napad je pokušaj namerne eksploatacije računarskih sistema, tehnološki zavisnih preduzeća i mreža[3].

Kompromitovani računar se definiše kao bilo koji računarski resurs na čiju je poverljivost, integritet i dostupnost nepovoljno uticao nepoznati izvor, namerno ili nenamerno[4].

Kriptografski algoritmi se generalno dele na simetrične i asimetrične. Simetrični su bazirani na korišćenju istog tajnog ključa (ili ključeva) za enkripciju i dekripciju (engl. *shared secret key cryptography*). Asimetrični su bazirani na korišćenju različitih ključeva za enkripciju i dekripciju, od kojih je jedan javni i poznat svima, a drugi je tajni i poznat je samo jednom od učesnika u komunikaciji (engl. *public key cryptography*).

Simetrična kriptografija - Kod simetrične kriptografije postupak enkripcije i dekripcije zasniva se na dve matematički srodne funkcije. Enkripciona funkcija E na osnovu ključa k i ulazne poruke m, kreira zaštićenu poruku c (ciphertext). Dekripciona funkcija D na osnovu istog ključa k i zaštićene poruke c, kreira originalnu, ulaznu poruku m. Simetrični kriptografski algoritmi pružaju visok stepen zaštite sve dok ključ znaju samo pošiljalac i primalac poruke. Zato osnovnu meru sigurnosti simetričnih algoritama čini metod distribucije ključeva.

Najpoznatiji i najrasprostranjeniji simetrični algoritam je DES (Data Encryption Standard) i unapređena verzija 3DES. Ovaj algoritam je 1977. razvio IBM i doskora je korišćen kao međunarodni standard za transakcije u informacionim sistemima. Enkripcioni – dekripcioni ključ je dužine 56 bita, a sam kriptografski proces se odvija nad blokovima poruke dužine 64 bita. Donedavno je najmoćnijim računarima bilo potrebno nekoliko godina da generišu i isprobaju sve moguće kombinacije ključeva.

Da bi se dokazalo da DES algoritam više nije dovoljno siguran metod, američka kompanija RSA Data Security raspisala je konkurs za pronalaženje najbržeg i najpouzdanijeg metoda za razbijanje DES algoritma. 1999. godine DES algoritam je razbijen za 22 sata i 15 minuta, pomoću specijalno izgrađenog crack-uređaja i 100000 PC-a. Da bi se produžio vek DES algoritma dok noviji i moćniji algoritmi ne budu pronađeni, korišćene su poboljšane verzije originalnog DES-a. Najpopu-

1 Pleskonjić, D., Maček, N., Đorđević, B., Carić, M.: „Sigurnost računarskih mreža“, Viša elektrotehnička škola Beograd, 2006.

2 Techopedia, http://www.techopedia.com/definition

3 isto kao referenca 2

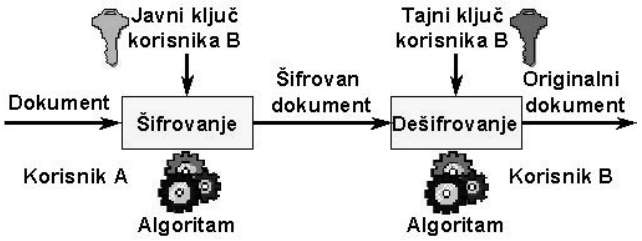
4 Carnegie Mellon University, http://www.cmu.edu/iso/governance/procedures/compromised-computer.html

larnija modifikovana verzija zasniva se na izvršavanju enkripcione (dekripcione) funkcije tri puta, pa otuda naziv 3DES.

Kao pobednik na konkursu za DES-ovog naslednika oktobra 2000. godine proglašen je Rijndael algoritam, koji su razvila dvojica belgijskih kriptografa Daemen (Joan Daemen) i Rijmen (Vincent Rijmen). Kao i DES, Rijndael predstavlja simetrični kriptografski algoritam koji proces enkripcije – dekripcije izvršava nad blokovima poruke dužine 128, 192 ili 256 bita. Na taj način moguće je kreirati 2128, 2192, odnosno 2256 različitih ključeva. Zasad su isprobani svi mogući kriptoanalitički postupci i Rijndael se pokazao potpuno „otpornim". Njegova primena u komercijalne svrhe je počela tokom 2002. godine.

Asimetrična kriptografija - Proces enkripcije i dekripcije se kod asimetrične kriptografije takođe zasniva na dve srodne matematičke funkcije: enkripciona funkcija *E* i dekripciona funkcija *D* manipulišu originalnom i zaštićenom porukom *m* i *c* korišćenjem dva srodna, ali različita ključa, od kojih se jedan koristi za enkripciju (ključ *e*), a drugi za dekripciju (ključ *d*). Prvi se naziva javni ključ (engl. *public key*), a drugi ključ je privatni ili tajni (engl. *private key*). Javni ključ je poznat svima, dok je privatni poznat samo jednoj strani.

U prvom slučaju datom na slici 1, pošiljalac poruke (korisnik A) u želji da ostvari privatnu komunikaciju sa primaocem (korisnik B), koristi primaočev javni ključ da enkriptuje originalnu poruku. Pošto je odgovarajući privatni ključ u vlasništvu primaoca, samo on je u mogućnosti da zaštićenu poruku dekriptuje. Na taj način je ostvarena tajnost komunikacije između pošiljaoca i primaoca poruke. Međutim, primalac poruke nije siguran ko mu je poslao poruku, jer je njegov javni ključ opštepoznat – zahtev autentikacije nije zadovoljen. Ovaj problem je rešen uvođenjem digitalnih potpisa.



Slika 1: *Asimetrična kriptografija*[5]

U drugom slučaju, pošiljalac ne može da bude bilo ko. Da bi se razmena zaštićenih poruka obavila, pošiljalac mora da bude identifikovan kod primaoca poruke. Pošiljalac koristi svoj privatni ključ da zaštiti poruku, a svako ko zna pošiljaočev javni ključ može poruku da dekriptuje. U ovom slučaju ostvareni su identitet pošiljaoca poruke, kao i nemogućnost njegovog poricanja da je poruku poslao, ali tajnost komunikacije nije ostvarena, jer svako ko zna javni ključ pošiljaoca može da dekriptuje poruku.

Prednosti i mane – Asimetrični kriptografski algoritmi imaju nekoliko prednosti u odnosu na simetrične algoritme. Prva se ogleda u broju različitih ključeva potrebnih za sigurnu komunikaciju između *N* korisnika. Da bi svaki korisnik ostvario sigurnu komunikaciju sa svakim korisnikom kod simetričnih kriptografskih algoritama potrebno je *Nx(N-1)/2* različitih ključeva. U slučaju asimetrične kriptografije, za isti vid komunikacije potrebno je samo *2xN* ključeva. Samim tim i metod distribucije tih ključeva ne zahteva zaštićeni komunikacioni metod. Druga prednost asimetričnih algoritama je u tome što oni pružaju mogućnost identifikacije i nemogućnost poricanja. Najveća mana asimetričnih algoritama jeste kompleksnost samog algoritma, sporiji rad i neprikladnost za šifriranje velikih količina podataka.

Osnove kriptografije bazirane na asimetričnim algoritmima definisane su Difi – Helman algoritmom, koji su 1976. godine osmislili Vitfild Difi (Whitfield Diffie) i Martin Helman (Martin Hellman) u cilju rešenja problema generisanja, razmene i kontrole ključeva. Danas najpoznatiji algoritam u grupi asimetričnih kriptografskih metoda je RSA. Asimetrični algoritmi posebnu primenu nalaze u oblasti identifikacije.

Specifičnost funkcija kojima se javni i privatni ključevi kreiraju, kao i veličina samih ključeva, uzrokuje nemogućnost izračunavanja privatnog ključa u razumnom vremenu na osnovu poznavanja samo javnog ključa. Dakle, tajni ključ je moguće izračunati i njime dekriptovati poruku, ali je za to potrebno toliko vremena da svaka tako dobijena informacija gubi praktičan značaj.

I pored toga, i dalje postoje istraživačke aktivnosti usmerene ka pronalaženju kriptosistema koji bi bio neprobojan i čije bi ključeve bilo nemoguće saznati. Dva osnovna razloga za to su:

Povećanje procesorske snage računara, kao i sve kompleksniji i moćniji višeprocesorski sistemi omogućavaju sve brže faktorizacije velikih brojeva tj. izračunavanje privatnih iz javnih ključeva. No ukoliko znamo da se vreme potrebno za takvo izračunavanje povećava eksponencijalno sa povećanjem broja cifara ključa, zaključuje se da ne postoji neka realna pretnja sa te strane.

Za detaljnije razumevanje, edukaciju i praktičnu primenu klasičnih kriptografskih algoritama koriste se razne pomoćne metode. Jedna od tih metoda je i softverski sistem za vizuelnu reprezentaciju[6]. On omogućava brzo generisanje adekvatnih primera, pomoću kojih je olakšano upoznavanje sa načinom rada algoritama.

Za razliku od klasičnih, kvantni računari bi problem faktorizacije velikih brojeva i izračunavanja diskretnih logaritama u konačnim grupama trebali rešavati vrlo brzo, tj. linearnom složenošću. U vezi sa tim, postoje već i gotovi algoritmi za tu namenu, kao npr. algoritam P.W. Šora (Shor, 1997). Stav koji se logično nameće je da nije racionalno povećavati broj cifara ključa, jer bi vreme za kriptovanje podataka raslo jednako kao i vreme pronalaženja privatnog ključa. Razlog zašto se i pored takve očigledne opasnosti i dalje koriste asimetrični algoritmi leži u činjenici da su kvantni računari i njihovi algoritmi još uvek nedovoljno razvijeni, a kao takvi za sada ne predstavljaju konkretnu pretnju. Ali je to ipak perspektivno područje na kojem se intenzivno radi, pa će se od budućih kriptosistema očekivati odgovor i na tu pretnju.

5 Pošta Srbije – Centar za elektronsko poslovanje Pošte, www.cepp.rs

6 Stanisavljević, Ž., Stanisavljević, J.: „Softverski sistem za vizuelnu reprezentaciju klasičnih kriptografskih algoritama", InfoM, No. 48/2013.

Kvantna kriptografija pokušava da odgovori na taj izazov i ponudi način za razmenu informacija koji bi bilo nemoguće kompromitovati. Ona bi bila zamena za danas široko korišćene asimetrične algoritme, čija je najznačajnija primena u razmeni tajnih ključeva za simetrične algoritme. Same poruke se gotovo nikada ne kriptuju asimetričnim algoritmima zbog toga što su 10 000 do 100 000 puta sporiji od simetričnih algoritama.

KVANTNA KRIPTOGRAFIJA – OSNOVNA IDEJA

Dugi niz godina su mnogi naučnici tražili način ostvarenja takve komunikacije između dve osobe koja bi garantovala privatnost. Nakon dužeg istraživanja, rešenje problema je nađeno u fizici, u tzv. Heisenbergovom principu neodređenosti. Prema tom principu, svako merenje u kvantnom sistemu unosi poremećaj u taj sistem i rezultuje nepotpunom informacijom o njegovom stanju pre merenja tj. smanjivanje merne nesigurnosti jedne varijable dovodi neizbežno do povećanja merne nesigurnosti druge varijable.

U skladu sa tim, Benet (Bennett) i Brasar (Brassard) kreirali su 1984. godine prvi protokol za sigurnu komunikaciju kvantnim kanalom koji su nazvali BB84. On se ne temelji na metodama klasične kriptografije, već se koristi činjenicom kvantne mehanike da prisluškivanje kvantnog komunikacionog kanala neizbežno uzrokuje poremećaj u informacijama, koji upozorava korisnike na prisutnost nekog prisluškivača.

Iako se kvantni kanal najčešće u praksi realizuje pomoću fotona, on se može jednako uspešno opisati i za bilo koji drugi kvantni sistem sa dva stanja. Foton može biti polarisan pomoću jedne od tri ortogonalne baze polarizacije (Slika 2):

- linearna horizontalna i linearna vertikalna (oznaka +)
- linearna pod uglom 45^0 i linearna pod uglom 135^0 (oznaka X)
- cirkularna leva i cirkularna desna

Bilo koje dve polarizacije iz različitih baza su međusobno konjugovane, što znači da se ne mogu razlikovati samo jednim merenjem. Ako se za komunikaciju koriste dve baze polarizacije, tada detektor fotona ima na raspolaganju samo jedno merenje kojim mora da utvrdi dve varijable. Kako se radi o kvantnom sistemu, merenjem jedne varijable nepovratno se gubi informacija o vrednosti druge varijable, pa stoga nije moguće napraviti kopiju fotona koja bi bila u potpunosti jednaka originalu. Ta činjenica je temelj kvantne kriptografije ili kvantne distribucije ključa (engl. *Quantum Key Distribution – QKD*).

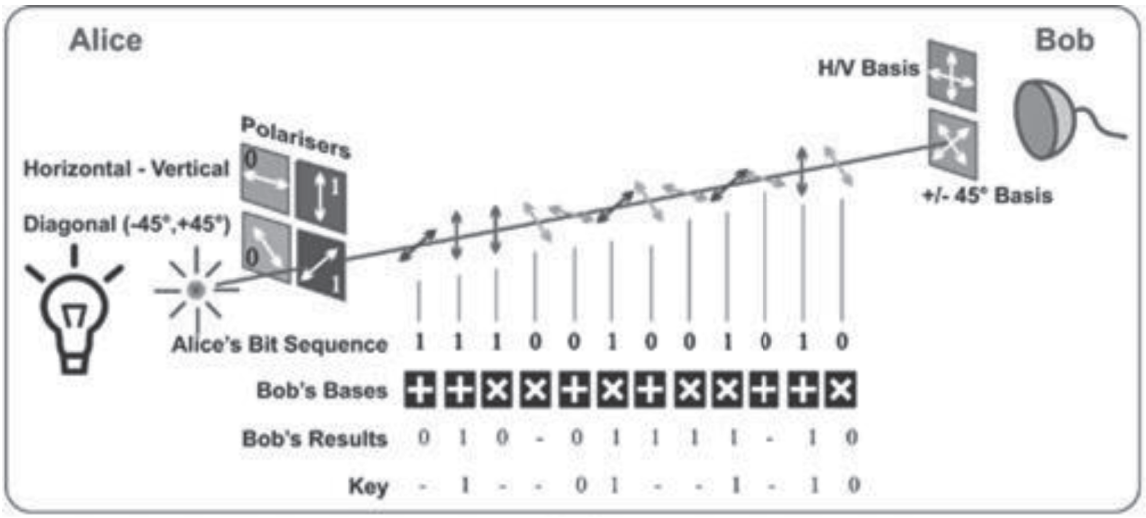
Kvantna kriptografija se u praksi koristi samo za kreiranje i distribuciju ključa, a ne i za prenos same poruke. Ovaj ključ se može koristiti sa bilo kojim uobičajenim kriptografskim algoritmom za enkripciju (i dekripciju) poruke koja se može prenositi preko standardnog kanala za komunikaciju. Algoritam koji se najčešće dovodi u vezu sa QKD-om je tzv. „one-time pad“ metoda šifrovanja. Njene karakteristike su:

- algoritam ključa je simetričan
- ključ i poruka imaju istu dužinu
- ključ je generisan slučajnim putem
- svaki ključ se upotrebljava samo jednom

DISTRIBUCIJA KVANTNOG KLJUČA

Kvantna komunikacija podrazumeva kodovanje informacija u kvantna stanja ili kubite (engl. *qu-bit*), slično bitima 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 sigurnost u prenosu podataka. Postoji nekoliko različitih pristupa distribuciji kvantnog ključa koji se mogu podeliti u dve glavne kategorije u zavisnosti od toga koja svojstva koriste.

Protokoli “pripremi i izmeri“ (Andrejić, 2013) - Za razliku od klasične fizike, postupak merenja predstavlja sastavni deo



Slika 2: *Principi kvantne kriptografije*[1]

1 Universite de Geneve, Faculte des Sciences, www.cms.unige.ch/gap/optics/

kvantne mehanike. Postupak merenja nepoznatog kvantnog stanja dovešće do promene tog stanja. Ova pojava zasniva se na rezultatima kao što je Hajzenbergov princip neodređenosti, Teorema o narušavanju informacija i Teorema o nekloniranju i poznata je kao kvantna neodređenost. Ima primenu u otkrivanju pokušaja prisluškivanja komunikacionog kanala kao i izračunavanje presretnute količine informacija.

Protokoli zasnovani na isprepletanosti (Andrejić, 2013) - Kvantna stanja dva ili više odvojena objekta mogu da postanu povezana tako da se mogu opisati kao kombinovano kvantno stanje, a ne kao individualni objekti. Drugim rečima, merenje koje se vrši na jednom objektu istovremeno će uticati i na drugi objekat. Kada se isprepleteni par objekata pošalje komunikacionim kanalom, pokušaj presretanja bilo koje mikro-čestice (fotona) dovešće do promene celokupnog sistema i kao rezultat dovesti do otkrivanja treće strane tj. uljeza u komunikacionom kanalu. Takođe, biće otkrivena i količina informacija do koje je uljez došao.

Dva prethodno navedena pristupa mogu se podeliti u tri familije protokola: diskretne varijable, kontinualne varijable i distribuirano fazno referentno kodovanje. Prvo su nastali protokoli zasnovani na diskretnim varijablama i do danas su najrasprostranjeniji. Protokoli koji pripadaju drugim dvema grupama pretežno su usmereni ka savladavanju praktičnih ograničenja u eksperimentima.

KVANTNI PROTOKOLI

U oblasti kvantne kriptografije je u primeni više protokola: BB84 (Bennett & Brassard, 1984), B92 (Bennett, 1992), E91 (Ekert, 1991), EPR (Einstein, Podolsky & Rosen, 1935), SARG04 (Scarani et al., 2004) i drugi. U daljem tekstu biće dat prikaz dva najčešće korišćena protokola.

BB84 (Picek, Golub, 2009) – Pošiljalac informacije (*A*) i primalac informacije (*B*) kao učesnici međusobne komunikacije povezani su kvantnim kanalom koji omogućava razmenu kvantnih stanja. U slučaju kvantne komunikacije, taj kanal se realizuje putem optičkog vlakna ili slobodnog prostora (etar). Pored toga, *A* i *B* su povezani i nekim javnim telekomunikacionim kanalom (npr. Internetom). U opštem slučaju, nijedan od tih kanala ne mora biti siguran. Ovde se pod sigurnošću podrazumeva obezbeđenje sledećih sigurnosnih ciljeva: poverljivost (zaštita od otkrivanja podataka - ostvaruje se adekvatnom enkripcijom), integritet (podaci nisu izmenjeni u toku prenosa) i raspoloživost (servis mora biti dostupan onima kojima je potreban, kada je potreban i gde je potreban - postiže se upotrebom kvalitetnih hardverskih i softverskih rešenja). Kvantni protokol je dizajniran pod pretpostavkom da postoji mogućnost prisluškivanja komunikacije između *A* i *B*. Sigurnost kvantnog protokola potiče od načina kodovanja informacija u neortogonalnim stanjima. Protokol BB84 koristi dva para stanja, kod kojih je jedan par konjugovan u odnosu na drugi, a dva stanja unutar jednog para su ortogonalna jedan prema drugom. Parovi ortogonalnih stanja nazivaju se baze. Uobičajene polarizacije stanja su linearna horizontalna – linearna vertikalna, linearna pod 45^0 – linearna pod 135^0 i cirkularna leva – cirkularna desna polarizacija. Bilo koje dve polarizacije iz različitih baza su međusobno konjugovane. Kod BB84 se biraju dve baze polarizacije i svakom od stanja u bazama se dodeljuje vrednost 0 ili 1, čime se stvara kvantna abeceda.

U početnoj 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 drugu polarizaciju. Imajući u vidu principe kvantne mehanike, primalac ne može da meri obe polarizacije istovremeno - merenje jedne polarizacije isključuje mogućnost merenja druge polarizacije. Ako *B* postavi detektor u odgovarajući položaj, on će registrovati ispravnu polarizaciju. U protivnom će registrovati neko slučajno stanje sa jednakom verovatnoćom. *B* ne može da odredi razliku između ta dva slučaja. U sledećem koraku, *B* uspostavlja vezu sa *A* preko javnog kanala i obaveštava ga koju je orijentaciju polarizatora koristio za detekciju. *A* odgovara *B* koja su podešavanja bila ispravna. *A* i *B* zadržavaju samo one polarizacije koje su bile ispravno podešene. Na ovaj način dobijeni biti čine tajni ključ. U proseku će *B* pogoditi ispravnu polarizaciju u 50% slučajeva. Prisluškivanjem osoba *I* pogađa polarizacije isto kao i *B*, odnosno 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 će promeniti zajednički uspostavljen tajni ključ, jer će *A* i *B* na kraju dobiti različite nizove bita. Tada *A* i *B* završavaju komunikaciju u skladu sa protokolom tako da uporede nekoliko bita svojih nizova. Ako postoje neusaglašenosti, oni zaključuju da su bili prisluškivani. U suprotnom, odbacuju bite koje su koristili za upoređenje i zadržavaju ostale (Schneier, 1996).

E91 (Picek, Golub, 2009) – Ovaj protokol je dobio ime po Arturu Ekertu (Arthur Ekert) koji ga je 1991. godine osmislio. Njegov princip je baziran na isprepletenom paru fotona - fotoni se distribuiraju na takav način da *A* i *B* dobiju po jedan foton iz svakog para. Oni mogu biti kreirani od strane *A*, *B* ili nekog nezavisnog izvora, uključujući i *I*. Ova principska šema se temelji na sledeća dva svojstva:

- ✓ isprepletena stanja su savršeno povezana;
- ✓ bilo koji pokušaj prisluškivanja, remeti korelaciju između fotona na način koji *A* i *B* mogu da detektuju.

A i *B* nezavisno biraju bazu u kojoj će meriti primljeni foton, s tim da *A* registruje neki određeni bit, a *B* komplement tog bita, jer je njegov foton ortogonalan fotonu koji je primila osoba *A*. U komunikaciji javnim kanalom *A* i *B* upoređuju korišćene baze detekcije i izdvajaju bite u kojima su koristili jednake uslove merenja. Oni biti na kojima su koristili različite uslove merenja ne odbacuju, već ih koriste za otkrivanje eventualne prisutnosti osobe *I* u komunikaciji korišćenjem Bellove nejednačine. Ona se koristi za određivanje postojanja lokalno skrivenih varijabli. Ukoliko je nejednačina zadovoljena, osoba *I* je prisluškivala. Ostatak protokola je isti kao i u BB84 (Lomonaco, 1998).

PREDNOSTI I NEDOSTACI QKD

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

Postoje i druge prepreke za praktičnu primenu kvantne kriptografije. Domet pojedinačnog fotona kroz optičko vlakno je, uz današnju tehnologiju, oko stotinak kilometara, što sprečava pošiljaoca i primaoca poruke da budu na većoj udaljenosti. Ukoliko su oni računari, može postojati mreža direktno povezanih računara. Sve ovo zahteva puno vremena i računarske opreme, ali je ipak ostvarivo.

Obim problema QKD se može sagledati iz sledećih činjenica (Jakuš, 2004):

- Polarizatori su nesavršeni, što utiče i na produkciju i na detekciju i povećava mogućnost pogrešnog prenosa.
- Smerovi osa polarizatora na predajnoj i prijemnoj strani nikada se ne poklapaju savršeno, što povećava grešku.
- Fotonski emiteri ne generišu uvek pojedinačne fotone. Oni uglavnom emituju određeni broj fotona odjednom, raspodeljenih po Poisson-ovoj raspodeli. Za snop sa manje od 1% primese višestrukih fotona, efikasnost emitera za ispaljivanje jednog fotona je oko 10%.
- Pri prolazu kroz svetlovod, fotoni bivaju apsorbovani i menja im se polarizacija, što povećava mogućnost pogrešne detekcije.
- Detektori fotona imaju efikasnost 10%-30%, što znači da se mnogi fotoni uopšte ne detektuju.
- Detektori fotona imaju šum, pa se događa od 10-100 lažnih detekcija u sekundi.

ZAKLJUČAK

Na osnovu u radu elaboriranih karakteristika, može se zaključiti da ne postoji idealna, apsolutno sigurna enkripcija informacija. Ukoliko jedan metod ima nedostataka u određenom segmentu, u drugom metodu, koji se pojavi kao unapređenje prethodnog, po pravilu se javljaju poteškoće neke druge prirode. Kod simetričnog šifrovanja, kao najjednostavnijeg metoda enkripcije sa velikom propusnom moći, svi napadi na ovaj sistem su napadi na metod korišćen za generisanje znakova ključa. Ako se u tu svrhu koristi kriptografski nepouzdan algoritam, to može da izazove ozbiljne sigurnosne posledice. Ako se koristi pravi izvor slučajnih brojeva, uspešan napad je teže izvodljiv i sistem se može smatrati sigurnim.

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

Međutim, kvantni metod distribucije rešava glavni problem tajnosti ključa u simetričnoj metodi, jer se zasniva direktno na Hajzenbergovom principu neodređenosti polarizacije fotona. Ostaje da se u budućnosti unaprede trenutna tehnološka ograničenja, kako bi ovaj način obezbeđenja sigurnosti u prenosu informacija prešao sa eksperimentalnog u globalno korišćenje.

LITERATURA

[1] Andrejić, D. (2013): *Kvantna kriptografija*, Univerzitet u Beogradu, Matematički fakultet, http://poincare.matf.bg.ac.rs/~vladaf/Courses/Matf MNSR/Prezentacije Individualne Stare/Andrejic_Kvantna_kriptografija.pdf

[2] Bennett, C.H. & Brassard, G. (1984): *Quantum cryptography: Public key distribution and coin tossing*, In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York

[3] Bennett, C.H. (1992): *Quantum Cryptography Using Any Two Nonorthogonal States*, Phys. Rev. Lett. 68, 3121.

[4] Brassard, G.: *A Bibliography of Quantum Cryptography*, http://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html

[5] Einstein, A., Podolsky, B. & Rosen, N. (1935): *Can quantum-mechanical description of physical reality be considered complete?* Phys. Rev. 47 777.

[6] Ekert, A. (1991): Phys. Rev. Lett. 67, pp. 661-663.

[7] Jakuš, M. (2004): *Kvantna kriptografija*, Faculty of Electrical Engineering and Computation, Zagreb, http://os2.zemris.fer.hr/kvant/2004_jakus/

[8] Lomonaco, S.J. (1998): *A Quick Glance at Quantum Cryptography*, arXive e-print quant.ph/9811056

[9] Picek, S. & Golub, M. (2009): *Kvantna kriptografija: razvoj i protokoli*, Proceedings of the Information Systems Security, MIPRO 2009, Opatija, Croatia. pp. 122-127.

[10] Pleskonjić, D., Đorđević, B., Maček, N., & Carić, M. (2006): *Sigurnost računarskih mreža*. Beograd: Viša elektrotehnička škola

[11] Scarani, V., Acín, A., Ribordy, G. & Gisin, N. (2004): *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations*, Phys. Rev. Lett. 92, 057901.

[12] Schneier, B. (1996): *Applied Cryptography*, 2nd Edn. John Wiley & Sons

[13] Shor, P. (1997): *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal on Computing, Volume 26 Issue 5, Society for Industrial and Applied Mathematics Philadelphia, pp. 1484-1509.

[14] Stanisavljević, Ž. & Stanisavljević, J. (2013): *Softverski sistem za vizuelnu reprezentaciju klasičnih kriptografskih algoritama*, InfoM, No. 48.

doc. dr Petar Čisar, Kriminalističko-policijska akademija, Zemun
Kontakt: petar.cisar@kpa.edu.rs
Oblasti interesovanja: digitalna forenzika, sigurnost informacionih sistema, mobilne tehnologije, računarske mreže, fuzzy-teorija