MOGUĆNOSTI DISTRIBUCIJE KRIPTOLOŠKIH KLJUČEVA JAVNIM KANALIMA

Saša Adamović
Univezitet Singidunum
Danijelova 32
Telefon: +381 11 3093-295
E-mail: sadamovic@singidunum.ac.rs

Milan Milosavljević
Univezitet Singidunum
Danijelova 32
Telefon: +381 11 3093-283
E-mail: mmilosavljević@singidunum.ac.rs

Miloš Milenković
Univezitet Singidunum
Danijelova 32
Telefon: +381 11 3093-248
E-mail: mmilenkovic@singidunum.ac.rs

Sažetak

U ovom radu razmatra se mogućnost distribucije kriptoloških ključeva javnim kanalima. Polazeći od teorijskih osnova Šenonovog pojma perfektnih šifarskih sistema analiziraju se konkretna rešenja za distribuciju tajnih ključeva javnim kanalima. Komparativna analiza obuhvata kvantni protokol BB84 i Mauerov protokol zasnovan na satelitskoj distribuciji zajedničkih korelisanih slučajnih nizova. Protokol BB84 je namenjen kvantnoj distribuciji ključeva (QKD) u cilju zamene asimetričnih protokola, zahteva dva komunikaciona kanala. Prvi predstavlja jednosmerni kvantni kanal, a drugi dvosmerni javni kanal. Uočena je velika sličnost izmedju ova dva protokola. Mauerov protokol se u svojoj prvoj fazi izvodi drugačije u odnosu na prvu fazu BB84 protokola. Umesto jednosmernog kvantnog kanala uvodi se satelit koji emituje loše kopije orginalnog slučajnog binarnog niza generisanog na satelitu. Preostale tri faze BB84 protokola su identične ostalim fazama Mauerovog protokola. U radu je prikazana simulacija Mauerovog protokola i diskutovani su neki kvantitativni pokazatelji bitni za praktičnu primenljivost ovog, danas široko analiziranog i diskutovanog načina distribucije tajnih kriptoloških ključeva.
Ključne reči: razmena ključeva, javni kanali, satelitski scenario, BB84, Kvantni kanal

Abstract:

This paper discusses the possibility of distributing cryptographic keys to public channels. Starting from the theoretical basis of the concept of Shannon perfect cryptographic systems are analyzed concrete solutions for the distribution of secret keys to public channels. Comparative analysis includes BB84 quantum protocol and Mauerer's protocol-based satellite distribution binary random sequences. BB84 protocol is designed for quantum key distribution (QKD) in order to replace the asymmetric protocol requires two communication

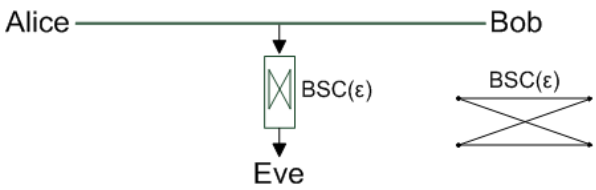
channels. The first is a one-way quantum channel, and the other two-way public channel. Observed a great similarity between these two protocols. Mauerers protocol in its first phase, performed differently in relation to the first phase of the BB84 protocol. Instead of one-way quantum channel introduces the satellite transmitting bad copies of the original random binary sequence generated by the satellite. The remaining three phases BB84 protocol are identical to other stages Mauerers protocol. This paper presents the simulation Mauerers protocol and discussed some quantitative indicators relevant to the practical applicability of this, now widely analyzed method of distribution secret cryptographic keys.

Key words: key-agreement, public discussion, data protection, satellite scenario, BB84, quantum channel

1. UVOD

U profesionalnim sistemima kriptografska zaštita predstavlja neizostavan proces svakog informacionog sistema. Cilj svake organizacije je da štiti poverljive podatke koji se nalaze u bazama podataka i raznim komunikacionim kanalima..Jedan od posrednih uslova za uspešnost rešenja predstavlja i njegova jednostavnost upotrebe.

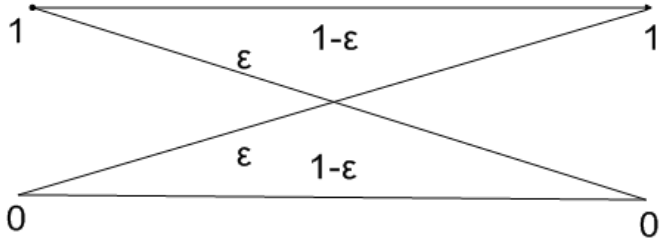
U kriptografskim sistemima nije dovoljno samo da kriptografski algoritam bude tajan, jer se vrlo lako kompromituje, već da zapravo tajnost treba da zavisi od kriptološkog ključa. Pojavili su se razni simetrični kripto sistemi koji su to omogućavali. Međutim ostao je jedan nerešen problem, a to je razmena ili distribucija kriptoloških ključeva između osoba koje žele da uspostave komunikaciju. 1976. Godine W. Diffie i M. Hellman objavljuju protokol za uspostavljanje tajnog ključa između osoba koje prethodno ne dele nikakvu zajedničku tajnu informaciju. Ova ideja je našla primenu i u asimetričnim algoritmima koji koriste dva ključa: javni za šifrovanje i privatni za dešifrovanje.



Sl 1. Simetrični kriptosistem

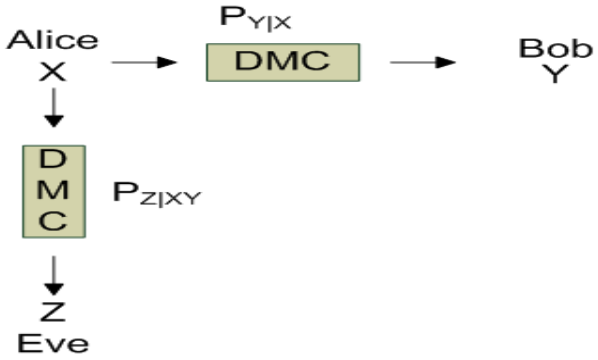
2. BINARNI SIMETRIČNI KOMUNIKACIONI KANALI

1978. godine Csiszar i Korner uočili su da binarni simetrični komunikacioni kanal sa šumom može da ima kriptografsku moć na polju distribucije ključeva. Binarni simetrični (BSK) kanal predstavlja digitalni sistem u kom vrednost transmisione greške ima konstantnu vrednost p, jednaku za nule (0) i jedinice (1). U slučaju greške izlazni bit je komplementaran ulaznom.



Sl 2. Binarni simetrični kanal

U njihovom radu "Broadcast channels with confidental messages", predstavljen je Broadcast kanal sa donjom granicom kapaciteta tajnosti $\mathbf{C_s(P_{YZ|X})\geq max\ [I(X;Y)-I(X;Z)]}$.



Sl 3. Broadcast kanal

Csiszar i Korner su izložili scenario u kom je prenos tajne moguć samo ukoliko su legitimni korisnici povezani kanalom koji ima manji šum (greška) od kanala prisluškivača (Eve), što i nije uvek tačna pretpostavka.

U. Maurer 1993. godine je, nastavljajući se na kvantne protokole, predložio protokol u kom Alice i Bob mogu imati dva manje korelisana niza nego što ga poseduje Eva, a da ipak uspeju da uspostave zajednički ključ. Da bi to bilo moguće Maurer je osmislio poseban scenario u kom Alisa i Bob primaju korelisane nizove iz nekontrolabilnog izvora slučajnog signala i uveo fazu destilacije prednosti u kojoj Alice i Bob postižu prednost naspram Eve i na to dodao preostale dve metode iz *no-cloning* kvantnih protokola.

2.1 KVANTNI PROTOKOL BB84

Primena kvantne kriptografije je u kvantnoj distribuciji kriptoloških ključeva (QKD), odnosno služi kao zamena asimetričnim protokolima. Jedan od najreprezantivnijh kvantnih protokola je BB84. On podrazumeva dva komunikaciona kanala. Prvi je jednosmerni kvantni kanal, a drugi je dvosmerni javni kanal.

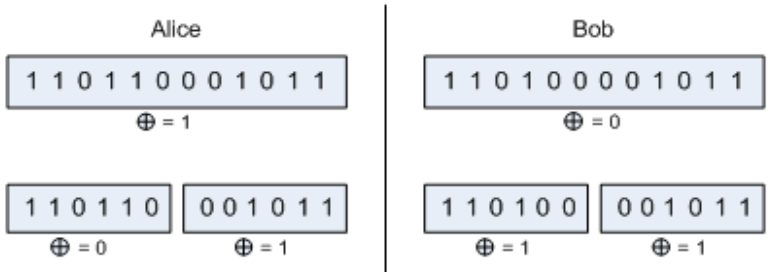
Prva faza protokola je u jednosmernom kvantnom kanalu. Prema Heisenbergovom principu neodređenosti, bit koji šalje Alis niko ne može primiti sa verovatnoćom većom od 75%. Verovatnoća da primaoc izabere bazu koju je izabrala i Alis je 50%. U tom slučaju verovatnoća da će Bob primiti ispravan bit je 1. U suprotnom, ako je Bob izabrao pogrešnu bazu, i dalje postoji 50% verovatnoće da se primljeni bit protumači ispravno. Iz toga sledi proračun:

$$\mathbf{P = 0,5*1 + 0,5*0,5 = 0,75 = 75\%}$$

Nakon do sada opisanog dela protokola Alis i Bob imaju bitne nizove jednake dužine ali ne i iste bite na istim mestima . Eva sada može da ima određeno znanje o tim nizovima, ali Alisa i Bob mogu da odrede gornju granicu na količinu te informacije.

U dvosmernom javnom kanalu postoje dve faze protokola. Prva faza je usaglašavanje informacija (Information Reconciliation), a druga pojačavanje privatnosti (Privacy Amplification).

Prva faza je protokol za usaglašavanje informacija ili error-correction protokol, pri čemu se pretpostavlja da Alisa ima ispravan, a Bob oštećeni niz. Protokol se svodi na usaglašavnje Bobovog niza sa Alisinim. Na početku ove faze Alisa i Bob podele svoj niz na *n* blokova zatim uporede paritete. U blokovima koji imaju različite paritete binarnom pretragom pronalaze različiti bit. U tom slučaju Bob invertuje bit.



Sl 4. Usaglašavanje informacija

Na osnovu procene grešaka u komunikaciji Alisa i Bob saznaju gornju granicu k bitova koji bi mogli biti poznati Evi od ukupno n bitova u njihovom izjednačenom ključu.

Druga faza Sl. 5. u dvosmernom protokolu je pojačavanje privatnosti. Ova faza predstavlja metod koji obezbeđuje na kraju ove faze jedan tajan niz koji se može putem javne komunikacije pretvoriti u kraći vrlo tajan niz ili konačan ključ.



Sl 5. Pojačavanje privatnosti

Ako se nad nizom dužine *n* o kom Eve ima *t* bita informacije izvrši univerzalna hash funkcija na dužinu *r*, onda o dobijenom nizu dužine *r* Eva ima manje od $\mathbf{r = H_2(S \mid U) - s}$ bita informacije, gde je S=***n*-*t*-R** *(security factor)*. Hash funkcija može biti poznata Evi, ali mora biti korišćena jednokratno.

2.2 UELI MAURER – SATELITSKI SCENARIO

U. Maurer 1993. godine je predložio protokol u kom Alisa i Bob mogu imati dva manje korelisana niza nego što ga poseduje Eva, a da ipak uspeju da uspostave zajednički ključ. Cilj protokola je da Alisa i Bob uspostave jedan tajni niz koji će biti samo njima poznat ili zajednički simetrični tajni ključ.Taj bi se niz koristio kao jednokratni ključ za šifrovanje (One Time Pad). Satelitski scenario protokola je moguć čak i kada je greška Evinog kanala ć manja

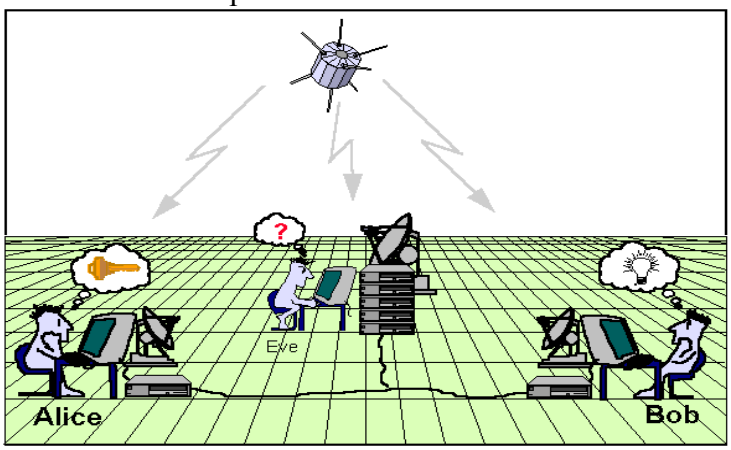
od grešaka Alisinog (α) i Bobovog kanala (β). Scenario jedino nije moguć, ako je Evina greška ε=0 (idealan pristup satelitu), ili ako Alisa i Bob ne mogu da prime emitovane nizove.

Satelitski scenario sadrži četri faze. U prvoj fazi Alice, Bob i Eva primaju svoje početne nizove sa satelita putem binarnog simetričnog kanala (BSK). Svi su nizovi različiti, ali postoji određen stepen korlacije među njima.

Nizovi su svi dužine N, ali nisu potpuno jednaki i predstavljaju nesavršene kopije nekog orginala koji nije nikome poznat.

$$p(a_i \neq s_i) = \varepsilon_A$$
$$p(b_i \neq s_i) = \varepsilon_B$$
$$p(e_i \neq s_i) = \varepsilon_E$$

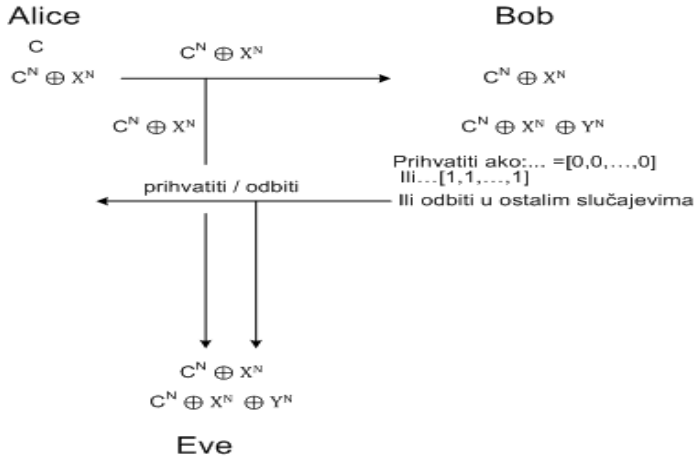
Ako je Evina greška manja od Alisine i Bobove, Alisa i Bob nemaju prednost nad Evom i ne mogu odmah ući u treću i čtvrtu fazu protokola.



Sl 6. Prva faza satelitskog scenaria

Druga faza je destilacija prednosti. Destilacija prednosti je proces generisanje prednosti u odnosu na Evu zahvaljujući autentičnosti javnog kanala.

Protokol se realizuje na sledeći način. Alisa i Bob dele svoje nizove na parove i određuju paritet svakog para. Parove kod kojih je paritet različit odbacuje se, a kod kojih je isti zadržava se samo prvi bit. Bitovi koji nisu odbačeni čine niz koji ulazi u sledeći korak. Eksponencijalnim kraćenjem polaznog niza, Alisa i Bob ostvaruju prednost.



Sl 7. Prva faza satelitskog scenaria

Treća faza protokola je usaglašavanje informacija ili ispravljanje grešaka. Nakon *n* iteracija protokola za destilaciju prednosti Alisin i Bobov niz su još uvek različiti. Cilj protokola za usaglašavanje informacija je da verovatnoća $p(A \neq B)$ bude manja od neke unapred zadane vrednosti.

Četvrta faza protokola je pojačavanje privatnosti u kojoj se eleminiše Evina informacija univerzalnim heširanjem Sl. 5.

3 KOMPARATIVNA ANALIZA

Ukoliko se uspostavljeni tajni ključ koristi za šifrovanje (One Time Pad), kvantna kriptografija nudi dokazivu sigurnost od napadača s neograničenom kompjuterskom moći i neograničenom memorijom.

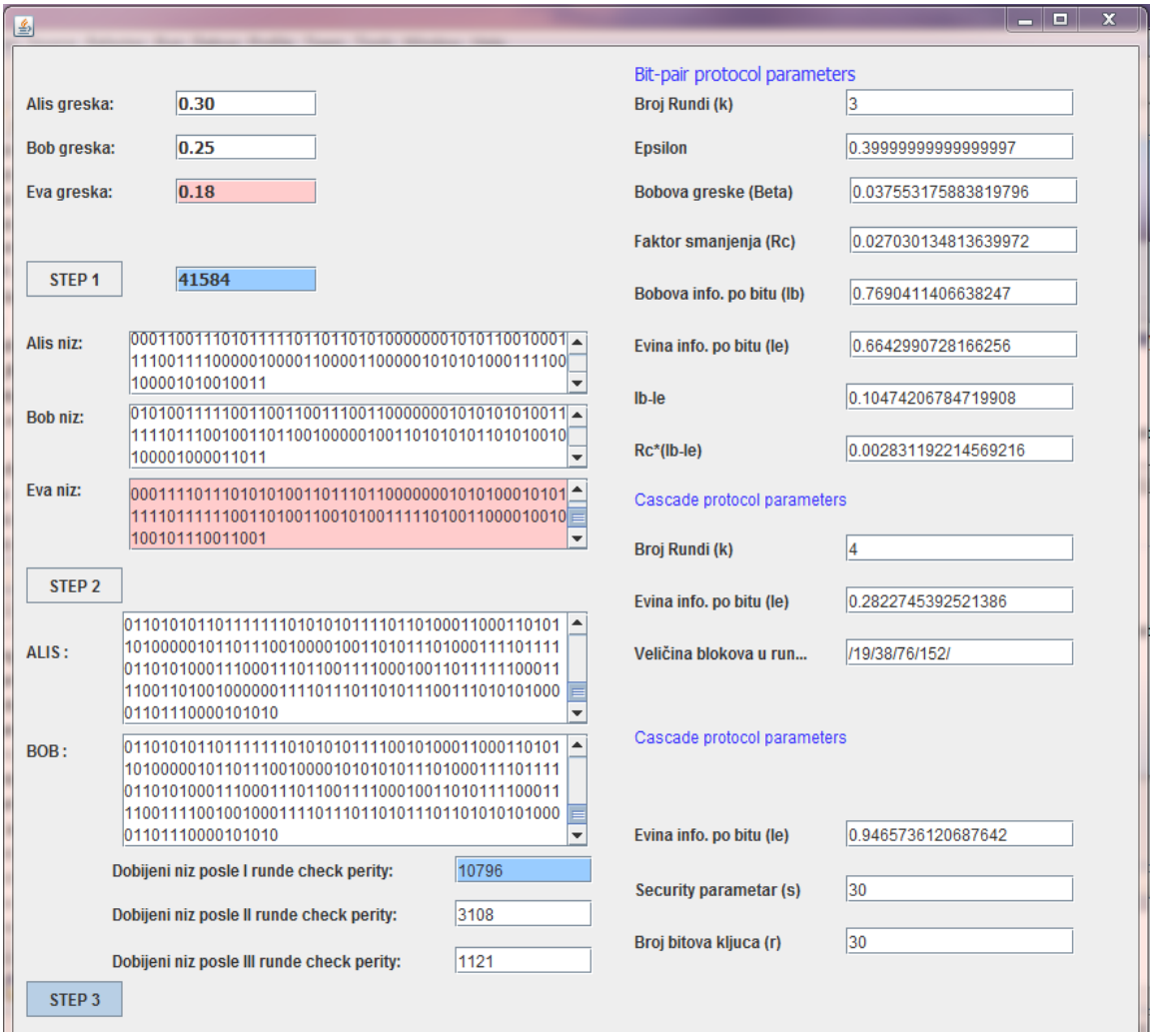
TABELA 1: KOMPARATIVNA ANALIZA

Komparativna analiza protokola za distribuciju kriptoloških ključeva javnim kanalima	
Kvantni protocol (BB84)	**Ueli Maurer (Satelitski scenario)**
Dokaziva sigurnost vredi za aktivnog napadača na kvantni i pasivnog na klasični kanal.	Dokaziva sigurnost vredi samo za pasivnog napadača.
Alisa i Bob moraju biti povezani i javnim i kvantnim kanalom.	Za Satelitski scenario potreban je samo javni kanal.
Skupa oprema koja ograničava širu upotrebu.	Teško izvodljiva postavka koja zahteva nekontrolabilni izvor slučajnosti.
Parametri protokola lako merljivi.	Glavni parametar protokola je greška. Grešku prisluškivača, nije moguće meriti.
Domet ograničen.	Domet neograničen.

U tabeli 1. su uporedno prikazane neke od bitnih osobina protokola .

4 PROGRAMSKA SIMULACIJA SATELITSKOG SCENARIJA

Za potreba rad napisana je u java programskom jeziku simulacija protokola (Satelitski scenario). Praktični testovi i rezultati merenja biće detaljnije analizirani i ilustrovani u drugom radu.



Sl 8. Programska simulacija

Trenutno dobijeni rezultati iz simulacije ukazuju da je potrebno imati početne nizove dužine 29300 bita za generisanje tajnog (ključa) sa kontrolom šuma (greške).

5 ZAKLJUČAK

U radu su razmatrane mogućnosti za distribuciju kriptoloških ključeva. Analizirane su neke od metoda (QKD) preuzetih iz kvantne kriptografije. Utvrđeno je da sigurnost ovakvih sistema zavisi od individualnosti greške pri prijemu početnih nizova. Da je moguće uspostavljanje tajnog ključa o kojem prisluškivač ima proizvoljno malo informacije (<0,5 po bitu). Da bilo koje dve strane koje žele uspostaviti tajni ključ moraju biti povezane javnim kanalom. Da je na osnovu komparativne analize Maurerov protokol otporan samo na pasivnog prisluškivača, a ukoliko dve strane koje komuniciraju, dele malu prethodnu tajnu, sistem postaje otporan i na aktivnog prisluškivača.

Rezultati ovog rada pokazuju da performanse današnjih PC računara i visoke cene opreme nisu dovoljne za potpuno iskorišćenje mogućnosti kriptografskih mehanizama. Dobijeni eksperimentalni rezultati ukazuju na potrebu za dodatnim hardverom umesto softverskog rešenja. Potreba za izučavanjem i razvijanjem metoda kriptografije je sve veća od kako se primenjuju računari, računarske mreže, a sa njima i baze podataka kao jedini vid arhiviranja i

kontrolisanja podataka među ljudima. Značaj ove oblasti ima više dimenzija kao što su politička, vojna, ekonomska, socijalna, etička itd.

Ovim radom nisu obuhvaćeni rezultati programske simulacije, što će biti predmet daljih istraživanja.

LITERATURA

[1] C. Shannon, Communication Theory of Secrecy Systems, Interna publikacija Bell Systems

[2] D. Knuth, The art of computer programming, Vol 2. Seminumerical algorithms, Addison-Wesley1998

[3] U. Maurer, Secret Key Agreement by Public Discussion, IEEE Trans. INFORM. THEOR. 39(1993)733-742

[4] C.H.Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India 1984, pp 175-179

[5] Csiszar, J. Koerner, Broadcast channels with confidential messages, IEEE Trans.Inform. Theor. 24(1978)339-348

[6] Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. LETT. 67(1991)661-663