Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI:
10.15308/SINTEZA-2014-1001-1005

DISTRIBUCIJA KRIPTOLOŠKIH KLJUČEVA PREKO JAVNIH KOMUNIKACIONIH KANALA

Nemanja Menković, Velibor Cekić
Centar za primenjenu matematiku i elektroniku, Beograd, Srbija

Abstract:
U radu je prikazan informaciono teoretski pristup razmeni kriptografskih ključeva, odnosno informaciono teoretski protokol za distribuciju kriptoloških ključeva, koji je baziran na satelitskom scenariju. Opisane su tri faze protokola za distribuciju kriptoloških ključeva: destilacija prednosti, usaglašavanje informacija i pojačavanje privatnosti. Razvijen je simulator protokola za distribuciju kriptoloških ključeva putem javnih komunikacionih kanala. U prvoj fazi destilacije prednosti implementirani su repetitivni protokol, iterativni protokol i bit-pair iterativni protokol. Za drugu fazu korišćen je kaskadni protokol, a u trećoj fazi primenjena je univerzalna klasa hash funkcije H1.

Key words:
distribucija kriptoloških ključeva,
destilacija prednosti,
usaglašavanje informacija,
pojačavanje privatnosti.

UVOD

U ovom radu razmatramo dogovor tajnog ključa (*secret key agreement*, engl.) koji je zasnovan na informaciono teoretskoj sigurnosti. Dogovor tajnog ključa je jedan od najbitnijih faktora u kriptologiji i ima zadatak da reši problem generisanja ključeva i njihove distribucije između korisnika. Tradicionalni načini distribucije kriptoloških ključeva koriste kriptosisteme sa javnim ključevima koji se zasnivaju na teško izračunljivom problemu kao što je faktorizacija velikih brojeva ili korišćenje diskretnih logaritama, iz čega sledi da su oni samo računski bezbedni. Sa druge strane, razvojem računarskih tehnika, kao što su kvantni računari, u budućnosti se može smanjiti nivo njihove kriptografske sigurnosti.

Rad je organizovan na sledeći način: opisan je model informaciono teoretskog dogovora tajnog ključa, zatim je dat opis praktičnog scenarija za dogovor tajnog ključa (satelitski scenario). Obrađene su sve faze protokola za distribuciju kriptoloških ključeva koje uključuju: destilaciju prednosti, usaglašavanje informacija i pojačavanje privatnosti. Za potrebe ovog rada je izrađen simulator protokola za distribuciju kriptoloških ključeva preko javnih komunikacionih kanala. Za prvu fazu destilacije prednosti je implementiran: repetitivni protokol, iterativni protokol i *bit-pair* iterativni protokol, za drugu fazu kaskadni protokol, a za treću fazu univerzalna klasa heš funkcije H1.

DISTRIBUCIJA KRIPTOLOŠKIH KLJUČEVA KAO GLAVNI PROBLEM U KRIPTOGRAFIJI

Upravljanje kriptološkim ključevima podrazumeva: sigurno generisanje, distribuciju i čuvanje ključeva. Sigurnosna metoda upravljanja ključevima je od ekstremnog značaja za celokupan bezbednosni sistem. U kriptološkoj infrastrukturi veliki broj napada nastaje na nivou upravljanja ključevima, dok se napadi na algoritme dešavaju vrlo retko. Učesnici u kriptografskim sistemima moraju biti sposobni da generišu ključeve, odnosno moraju biti dostupni korisnicima u komunikaciji. U slučaju da dođe do kompromitacije ili gubitka ključa od strane učesnika *X*, ostali učesnici u komunikaciji moraju biti upozoreni na vreme. U suprotnom će napadač moći da ukradenim ključem dešifruje poruke koje su tim ključem šifrovane. Takođe, korisnicima mora biti omogućeno da na siguran način čuvaju ključeve i učine ih dostupnim isključivo za legitimnu upotrebu. Održavanje integriteta specifikacija.

Obzirom da ključevi imaju ograničen životni vek, najvažniji razlog za njihovu periodičnu zamenu je zaštita od kriptoanalize. Kod svake uspostave zaštićene komunikacije, kada se ključ upotrebi, generiše se šifrat određene dužine i veličine. Ukoliko dođe u posed šifrata napadač može da prikupi podatke neophodne za kriptoanalizu. Iz tog razloga neophodno je da ključevi imaju ograničen životni vek. Ukoliko vlasnik ključa posumnja da je napadač

nabavio ključ potrebno je stopirati upotrebu kompromitovanog ključa i generisati novi ključ tj. ključeve.

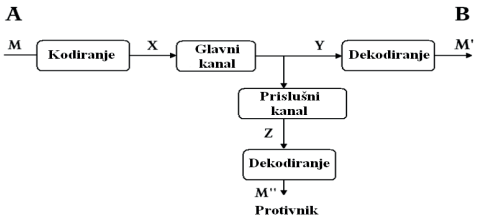
Istraživanjima su otkrivene potencijalne slabosti i napadi, pa se u proteklim periodima (koji traju u proseku nekoliko godina) povećava preporučena minimalna dužina ključa za određene algoritme. Npr. za RSA (Rivest-Shamir-Adlemann) algoritam trenutno se preporučuje minimalna dužina ključa od 512 bita. Ovo se odnosi na privremene ključeve čiji je vremenski indeks upotrebe jedan ili nekoliko dana. Preporučena dužina ključa za dužu upotrebu je minimalno 1024 bita. U opštem slučaju ključeve delimo na simetrične, javne i privatne ključeve, a samo su simetrični i privatni ključevi su po svojoj prirodi tajni ključevi. Za dešifrovanje poruke strana B mora posedovati validne alate koji je strana *A* koristila za šifrovanje, ali i ključ kojim je poruka šifrovana.

Problem distribucije ključeva je stalno prisutan u istoriji kriptografije. Bez obzira koliko je u teoriji kriptografski algoritam siguran, poverljivost njegovog mehanizma može ugroziti problem distribucije ključa. Pitanje distribucije ključa može se činiti trivijalnim, međutim u kriptografskom sistemu to je najslabija karika. Ako dve osobe žele da razmenjuju podatke u bezbednom okruženju, moraju da veruju trećoj strani od poverenja *C*, koja distribuira ključeve što, u ovom slučaju, postaje slaba karika u lancu bezbednosti u odnosu na prethodne dve. Iako postoje tvrdnje da je problem distribucije kriptoloških ključeva nerešiv problem, sredinom sedamdesetih godina prošlog veka otkriveno je pouzdano rešenje. Obzirom da je računarska tehnika preobrazila primenu kriptografskih algoritama, činjenica je da je najveću promenu u kriptografiji dvadesetog veka izazvao razvoj tehnika za distribuciju ključeva. Ovo otkriće smatra se najvećim kriptografskim ostvarenjem od izuma monoalfabetske metode kriptovanja (jedne od najranijih metoda kriptovanja poruka) pre dve hiljade godina [1].

INFORMACIONO TEORETSKI DOGOVOR TAJNOG KLJUČA

Šenonova pretpostavka da neprijatelj primi potpuno istu poruku kao i legitimni učesnik uzima se u obzir ukoliko se koristi komunikacioni kanal u kojem nema grešaka. Međutim, u komunikacionim kanalima javlja se šum, pa se u malom broju slučajeva ovi kanali pretvaraju u kanale u kojima gotovo i da ne postoji greška prenosa podataka (sa smanjenom brzinom informacija), što se izvodi korišćenjem kodova za ispravljanje greške. Ova naizgled nebitna opservacija ukazuje na činjenicu da je Šenonova tvrdnja nepotrebno restriktivno ako osnovnim kanalima u kojima postoji šum može da se pristupi kriptografskom aplikacijom, oblika tajne komunikacije kroz kanale emitovanja (*secret communication using broadcast channels*, engl).

Motivisan ovakvim razmišljanjima Vejner je smatrao da je scenario komunikacije u kojem Alisa može da pošalje informacije Bobu preko diskretnog kanala tako da prisluškivač Eva može da primi Bobov kanal (signal) samo kroz dodatne kaskadne nezavisne kanale koji smanjuju kapacitet kanala koji koristi Eva . Vejner je dokazao da u takvom (u opštem slučaju nerealnom) okruženju Alisa može da šalje informacije Bobu u gotovo potpunoj tajnosti, bez potrebe da pre toga razmene ključ. Vejnerov prislušni kanal prikazan je na Slici 1.



SL. 1. Vejnerov prislušni kanal

Vejnerov model i rezultate, generalizovali su Sizar i Korner koji smatraju da diskretni kanal za emitovanje koji koristi prisluškivač Eva nije obavezno degradirana verzija poruke, koju je primio legitimni učesnik Bob . Zajednički unos glavnom kanalu i kanalu koji koristi Eva je slučajna promenljiva *X* koju je odabrala Alisa prema distribuciji verovatnoće P_X, i slučajne promenljive koje su primili Bob i Eva su *Y* i *Z*. *X, Y* i *Z* uzimaju vrednosti ili brojeve određene alfabetom X, Y i Z . Karakteristike kanala su potpuno određene uslovnom distribucijom verovatnoće $P_{YZ|X}$. Vejnerovo početno podešavanje *X, Y* i *Z* prave Markovljev niz $P_{Z|XY} = P_{Z|Y}$ koji ukazuje na $I(X;Z|Y) = 0$.

Kapacitet tajnosti $C_s(P_{YZ|X})$ opisanog kanala emitovanja sa tranzicijom distribucije verovatnoće $P_{YZ|X}$ je definisana kao maksimalna brzina kojom Alisa može pouzdano da šalje informacije Bobu tako da je brzina kojom Eva koristi ovu informaciju proizvoljno mala, tj. kapacitet tajnosti je maksimalan broj bita koji koristi kanal, tako da Alisa može tajno da šalje podatke Bobu.

U odnosu na prethodno opisani model, Maurer je unapredio model, dodajući mu javni kanal između Alise i Boba, tako da je između njih omogućena interaktivna komunikacija. Ako je javni kanal autentičan, tj. emitovanje preko javnog kanala ne može da modifikuje Eva, moguće je postići tajnu komunikaciju, i u slučajevima kada je kanal koji koristi Eva bolji od onog koji koristi Bob. U tekstu koji sledi prikazan je Maurerov model tajnog sistema (*secrecy system*, engl.):

1. Alisa, Bob i Eva imaju pristup
   a) komunikacionim kanalima sa šumom
   b) javnom, nebezbednom kanalu bez greške.
2. Ukoliko je C' informacija u vezi otvorenog teksta M, koja je dostupna Evi izvesna korelacija između C' i M je dozvoljena.

Bilo koja poruka emitovana kroz komunikacioni kanal sadrži određen nivo šuma, što implicira da ni Bob ni Eva ne dobijaju uvek identičnu kopiju poruke koju je poslala Alisa. Iz tog razloga *C'* označava Evinu informaciju u vezi *M*. Ova pretpostavka u vezi javnog kanala je takođe prihvatljiva jer se lako postiže kroz ovakav kanal. U suprotnom, koristeći tehniku za ispravljanje grešaka, svaka poruka putem javnog kanala se prihvata kao tačna, tj. bez greške.

U Šenonovom modelu postignuta je informaciono teoretska sigurnost uslovom $I(C;M) = 0$. U Maurerovom

modelu dozvoljena je mala korelacija između C' i M, i opisuje se kao $I(C;M) < \epsilon, tj. H(M|C') = H(M) - \epsilon$, za $\epsilon > 0$. Kada ϵ teži nuli, *M* poseduje veliki stepen tajnosti (*highly secret*, engl.).

Nakon uspešnog dogovora tajnog ključa između Alise i Boba, OTP mogu da budu korišćene za emitovanje otvorenog teksta sa savršenom tajnošću. [2], [3], [4].

PRAKTIČNI SCENARIO ZA DOGOVOR TAJNOG KLJUČA (SATELITSKI SCENARIO)

Maurer je 1993. godine 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 tajni niz koji će biti samo njima poznat ili zajednički simetrični ključ. Taj niz se koristi kao jednokratni ključ za šifrovanje (*one-time-pad*). Satelitski scenario (Slika 2.) je moguć čak i kada je greška Evinog kanala ϵ manja od grešaka Alisinog i Bobovog kanala. Scenario nije moguć u slučajevima u kojima je Evina greška $\epsilon = 0$ (idealan pristup satelitu), ili ukoliko Alisa i Bob ne mogu da prime emitovane nizove. Satelitski scenario sastoji se od tri faze:

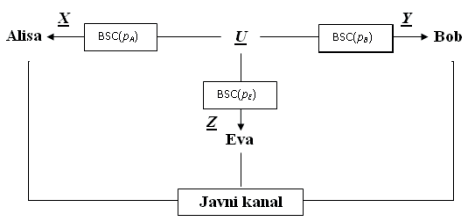
1. Faza inicijalizacije (*initialization phase*, engl.): Alisa, Bob i Eva dobijaju slučajne vrednosti promenljivih *X, Y* i *Z*, respektivno, distribuirane sa nekom verovatnoćom P_{XYZ} sa satelita putem binarnog simetričnog kanala (BSK). Svi nizovi primljeni sa satelita su različiti, ali postoji određen stepen korelacije među njima. Nizovi su dužine *N*, ali nisu istovetni i predstavljaju nesavršene kopije nekog originala koji nikome nije poznat. Odavde sledi da je:

$$p(A_i \neq U_i) = \epsilon_A$$

$$p(B_i \neq U_i) = \epsilon_B$$

$$p(E_i \neq U_i) = \epsilon_E$$

Ukoliko je Evina greška manja od Alisine i Bobove, Alisa i Bob nemaju prednost nad Evom i ne mogu da uđu u drugu i treću fazu protokola.



SL. 2 . Satelitski scenario

2. Faza komunikacije (*communication phase*, engl.): Alisa i Bob razmenjuju informacije putem javnog kanala. Ova faza je poznatija kao javna diskusija (rasprava), i dalje se deli u tri faze:
   a) Za vreme faze destilacije prednosti (*advantage distillation*, engl.), Alisa i Bob razmenjuju informacije, označene slučajnom promenljivom *U*. Alisa dobija novu slučajnu promenljivu *A* od *X* i *U*. Slično, Bob dobija novu slučajnu promenljivu *B* od *Y* i *U*. Ovim bi trebalo dobiti rezultat, u situaciji da Bob ima više informacija Alisine slučajne promenljive *A* nego što Eva ima, ili da Alisa ima više informacija u vezi Bobove slučajne promenljive *B* nego što ih ima Eva, tj.

$$H(A|X,U) = 0, H(B|Y,U) = 0, i H(A|B) < H(A|Z,U)$$

ili $H(B|A) < H(B|Z,U)$.

   b) Alisa i Bob, razmene neke suvišne informacije da bi ispravili neslaganje između njihovih slučajnih promenljiva u toku faze usaglašavanja informacija (*information reconciliation*, engl.). Ukoliko je suvišna informacija *V* tada, koristeći *V*, Alisa i Bob dolaze do zajedničkog niza *S*, a Eva i dalje ima određenu neizvesnost vezanu za *S*. U formuli,

$$H(S|A,V) = 0, H(S|B,V) = 0, i\ H(S|Z,U<V) > 0$$

   v) Faza pojačanja privatnosti (*Privacy amplification* (PA), engl.) obezbeđuje Alisi i Bobu da generišu tajan niz *S'* od zajedničkog ali delom tajnog niza *S*. Put do kompletiranja PA je da Alisa izabere odgovarajuću *hash* funkciju koja je označena sa *G*, i da je pošalje Bobu. Onda oni računaju *hash* vrednost $S' = G(S)$, i očekuju da bude $H(S'|G,Z,U,V) = H(S') - \epsilon\ za\ malo\ \epsilon$.

3. Faza odlučivanja (*decision phase*, engl.): Alisa i Bob zajednički prihvataju ili odbacuju izvršenje protokola, u zavisnosti od toga da li veruju da niz $S' = G(S)$ može služiti kao tajni ključ [4], [5], [6].

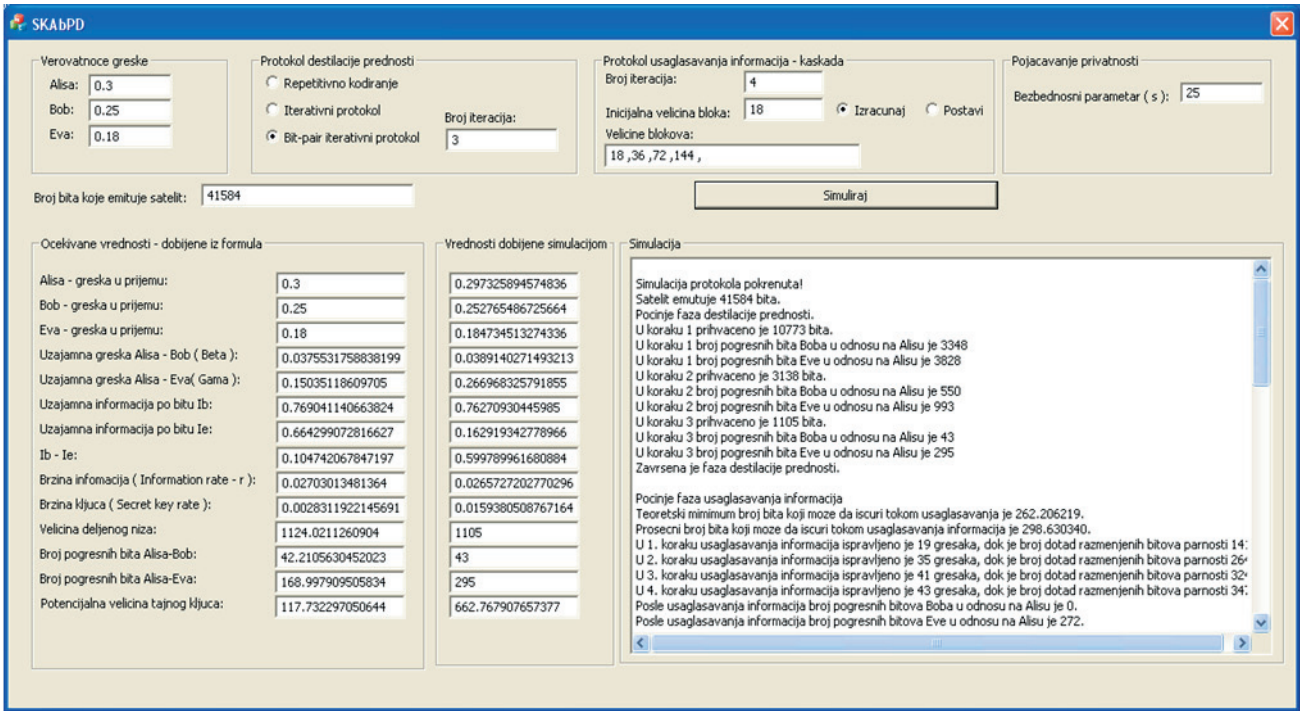
SIMULATOR

Za potrebe ovog rada je izrađen simulator protokola za distribuciju kriptoloških ključeva preko javnih komunikacionih kanala. U simulatoru su implementirane sve faze protokola. Simulator je razvijen u programsku jeziku *C++*, korišćenjem *Microsoft Visual Studio 2010* platforme i primenom MFC biblioteke za grafički prikaz interfejsa. Na Slici 3. dat je grafički prikaz interfejsa.

Na početku simulacije potrebno je postaviti početne parametre. Prvo se definišu verovatnoće greške za sva tri kanala odnosno učesnika (Alisa, Bob i Eva). To predstavlja greške u nizovima bita primljenih sa satelita. Potom se unosi parametar za dužinu niza koji se prima sa satelita, odnosno broj bita koji emituje satelit iznosi 41584.

Prva faza protokola je protokol destilacije prednosti. Za izvršenje prve faze destilacije prednosti na raspolaganju su tri mogućnosti:

1. Protokol repetitivnog kodiranja
2. Iterativni protokol
3. *Bit-pair* iterativni protokol.



SL. 3 . Grafički prikaz interfejsa

Za svaki protokol potrebno je postaviti početne parametre, tj. broj iteracija. Pri izboru Repetitivnog kodiranja definiše se jedna iteracija. Dužina kodne reči se postavlja proizvoljno. Iterativni protokol takođe zahteva postavljanje broja iteracija i dužine kodne reči, pri čemu su obe vrednosti proizvoljne.

Kod *Bit-pair* iterativnog protokola broj iteracija je proizvoljan, dok je kodna reč fiksne dužine.

U drugoj fazi protokola implementiran je kaskadni protokol za ispravljanje grešaka, odnosno protokol za usaglašavanje informacija. Potrebno je postaviti parametar za broj iteracija, odnosno rundi. Preporučen broj rundi je 4. Nakon izvršenja sve četiri runde velika je verovatnoća da su nizovi usaglašeni, što je objašnjeno u radu[7].

Inicijalna veličina bloka se može definisati proizvoljno ili sam simulator može postaviti ovu vrednost. Nakon svake izvršene runde veličina bloka se udvostručava. Npr. ako je početna vrednost veličine bloka 18, u drugoj rundi će iznositi 36, a u trećoj i četvrtoj rundi 72 i 144, respektivno.

Izvršavanjem simulacije, dobijaju se sledeći podaci o simulaciji:

- Alisina greška u prijemu
- Bobova greška u prijemu
- Evina greška u prijemu
- Uzajamna greška Alise i Boba
- Uzajamna greška Alise i Eve
- Uzajamna informacija po bitu Ib
- Uzajamna informacija po bitu Ie
- Razliku uzajamnih informacija Ib – Ie
- Brzina informacija (*information rate,* engl.)
- Brzina ključa (*secret key rate*, engl.)
- Veličinu deljenog niza
- Broj pogrešnih bita između Alise i Boba
- Broj pogrešnih bita između Alise i Eve
- Potencijalna veličina ključa.

Nakon izvršenja simulacije dobija se tekstualni izveštaj prikazan na Slici 3. koji uključuje sve faze protokola.

Poslednja faza je pojačavanje privatnosti u kojoj se smanjuje Evina informacija po bitu o ključu. Binarno je prikazan tajni ključ dogovoren između Alise i Boba, kao i ključ koji ima Eva.

ZAKLJUČAK

U ovom radu dat je opis problema razmene tajnih ključeva za potrebe sigurne komunikacije između dve strane sa posebnim osvrtom na informaciono teoretski pristup. Prikazano je kako se modifikacijom Šenonovog modela sigurne komunikacije (njegove pesimističke pretpostavke da mora da važi $H(K) \geq H(M)$) perfektna sigurnost može prevazići.

Informaciono teoretski pristup razmeni ključeva pokazuje kako da se od delimično poznatog deljenog niza bitova dođe do značajnog kraćeg deljenog tajnog ključa. Obrađen je Maurerov satelitski model informaciono teoretske razmene ključeva koji se sastoji iz sledećih faza: destilacija prednosti, usaglašavanje informacija i pojačavanje privatnosti. Korišćena su tri moguća pristupa destilacije prednosti: repetitivni protokol, iterativni protokol i *bit pair* iterativni protokol.

Za date varijante destilacije prednosti prikazani su teorijski rezultati dobijanja značajnih informacija o ovoj fazi kao što su: uzajamna greška između Alise i Boba posle destilacije prednosti, uzajamna greška između Alise i Eve posle destilacije prednosti, brzina prihvatanja bitova koji se razmenjuju itd. Teorijski rezultati pokazuju da navedena tri protokola imaju kao rezultat iste uzajamne greške, ali se razlikuju po brzini prihvatanja tajnih ključeva i brzini prihvatanja deljenih bitova. Najefikasniji od njih je *bit pair* protokol. Rezultati dobijeni simulacijom potvrđuju teorijske navode.

U drugoj fazi usaglašavanja informacija izvršena je analiza kaskadnog protokola za usaglašavanje informacija. Za potrebe ovog rada pretpostavljeno je da se radi o autentičnom kanalu i kao metodu pojačavanja privatnosti primenjena je univerzalna klasa funkcije H_1.

Za potrebu potvrde teorijskih nalaza razvijen je simulator u programskom jeziku *C++*, korišćenjem *Microsoft Visual Studio 2010* platforme i korišćenje MFC biblioteke za grafički prikaz interfejsa. Simulator implementira sve tri faze informaciono teoretskog protokola.

U daljem istraživanju potrebno je detaljnije proučiti moguća poboljšanja usaglašavanja informacija i proučiti realnije scenarije pojačavanja privatnosti.

LITERATURA

[1] M. Čajić, M. Veinović and B. Brkić, Distribucija kriptoloških ključeva u mobilnim uređajima pod android operativnim sistemom, INFOTEH-Jahorina, Vol. 9, Ref. E-VI-2, pp. 823-826, Mart 2010.

[2] I. Csiszar and J. Korner, Broadcast channels with confidential messages, IEEE Transations on Information Theory, Vol. 24, pp. 339-348, 1978.

[3] A.D. Wyner, The wire-tap channel, Bell System Technical Journal, Vol. 54,No. 8, pp. 1355-1387.

[4] U.M. Maurer, Secret key agreement by public discussion from common information, IEEE Trans. Inform. Theory, Vol. 39, pp. 733–742, May 1993.

[5] M. Milosavljević, S. Adamović, and M. Milenković, Mogućnosti distribucije kriptoloških ključeva javnim kanalima, Sinergija 2010., Beograd., 2010.

[6] S. Liu., Information-theoretic secret key agreement, Eindhoven: Technische Universiteit Eindhoven, 2002.

[7] T.I. Calver, An Empirical Analysis Of The Cascade Secret Key Reconciliation Protocol For Quantum Key Distribution, Department of the Air Force Air University, Air Force Institute of Technology, 2011.

SECRET KEY AGREEMENT OVER THE PUBLIC CHANNELS

Abstract:
This paper presents information-theoretic secreet key agreement approach to the exchange of a secret key as well as the information-theoretic protocol for secret key distribution, which are based on a satelite scenario. A secret key distribution protocol is presented through the advantage distillation, information reconciliation and privacy amplification phases. A simulation of the secret key distribution over public channels is created as follows: in the advantage distilation phase a repetition code, iteration and bit-pair iteration protocols are implemented. The second phase is based on the Cascade protocol. Universal hash function H1 is used to the privacy amplification.

Key words:
secret key distribution, advantage distillation, information reconciliation; privacy amplification.