UDC: 004.738.5:342.4 Info M: str. 19-25

PREGLED ŠEMA ZA ELEKTRONSKO GLASANJE
OVERVIEW OF AN ELECTRONIC VOTING SCHEMES

Dragoljub Pilipović – Slobomir P univezitet, Bijeljina,
Dušan Starčević – Fakultet organizacionih nauka, Univerzitet u Beogradu

REZIME: Svaka državna struktura se može posmatrati kao servis građana te će tako elektronska vlada biti primena najnovijih informatičko-tehnoloških dostignuća i komunikacione tehnologije za pružanje efikasnih usluga, informacija i potreb nih znanja putem Interneta i drugih srodnih digitalnih tehnologija. Građani očekuju da na Internetu pronađu servise koji se odnose na poslovanje sa državnim sektorom, a sa druge strane i državne strukture imaju svoje razloge za prelazak na implementaciju koncepta e-vlade (npr. uštede). Širom zemaljske kugle se primenjuje e-glasanje na različitim nivoima uprave. U nekim zemljama održani su izbori državnog nivoa sa opcijom e-glasanja. Svaki sistem za e-glasanje ima svoje zahteve, karakteristike i osobine, a na osnovu njih se može izabrati optimalna varijanta za neku situaciju. Opisaće se konkretni sistemi za e-glasanje i šeme na kojima su zasnovani, kao što su mix-net šeme, homomorfne šeme, Prêt-à-vote šeme, biometrijske šeme, šeme zasnovane na vizuelnoj kriptografiji, šeme zasnovane na PKI i smart karticama itd.

KLJUČNE REČI: e-vlada, e-glasanje, šeme za e-glasanje, mix-net, homomorfizam, Prêt-à-vote, biometrija, vizuelna kriptografija, PKI, smart kartice.

ABSTRACT: Each state structure can be regarded as a service to citizens and accordingly electronic government will be the application of the latest informational/technological advances and communication technologies for providing efficient and effective services, information and required knowledge through the Internet or other related digital technologies. In the first place, citizens expect to find on the Internet plenty services related to the operations of the government sector, therefore, on the other hand government structures have their own reasons for the transition to the implementation of e-government (e.g. savings). E-voting is used across the globe in the various levels of government. In some countries, elections were held at the state level with the e-voting option. Any e-voting system (EVS) has its own requirements, characteristics and properties, and based on them it can be choose optimal solution for any situation. It will be describe the specific e-voting systems and e-voting schemes in which based on such as mix-net schemes, homomorphic schemes, Prêt-à-vote schemes, biometric schemes, schemes based on visual cryptography, schemes based on PKI and smart cards, etc.

KEY WORDS: e-government, e-voting, e-voting schemes, mix-net, homomorphism, Prêt-à-vote, biometrics, visual cryptography, PKI, smart cards

1. UVOD

Šema za e-glasanje je osnova za rad nekog sistema za e-glasanje i ona predstavlja niz koraka (algoritam, protokol) za sprovođenje e-glasanja, kao i skup postavki i pravila kako će ono biti obavljeno. Najčešće je šema zasnovana na nekom postojećem, novom ili kombinovanom kriptografskom pristupu.

U ovom radu će se kroz naredne odeljke dati pregled sedam grupa šema za e-glasanje. Grupisanje šema će se obaviti po kriterijumu metoda kojima se kreiraju, prenose, snimaju i obrađuju e-glasovi, kao i po tome na koji način se identifikuju i autorizuju glasači. Iako kod pojedinih šema postoje sličnosti u dosta detalja, ipak smo usvojili najčešću podelu kako se ona navodi u mnogim referencnim radovima uz manje modifikacije. One šeme, koje se ne mogu svrstati u neku određenu grupu po svojim karakteristikama, se nalaze u grupi ostalih. Grupe šema koje se prikazuju u ovom radu su sledeće:

1. Mix-net šeme.
2. Šeme sa homomorfnom enkripcijom.
3. Šeme zasnovane na potpisu na slepo.
4. Šeme zasnovane na biometriji.
5. Šeme zasnovane na vizuelnoj kriptografiji.
6. Šeme zasnovane na PKI i smart karticama.
7. Ostale šeme.

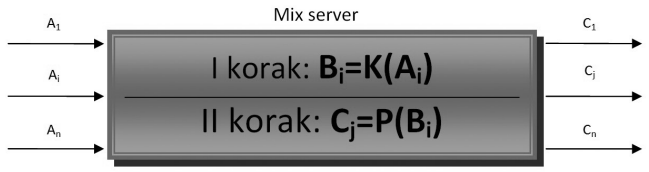
Pre nego se počne sa prvom grupom, napominjemo da se pri opisu šema koriste pojmovi sa podrazumevanim značenjem iz područja kriptografije (kriptografski algoritam, otvoreni tekst, šifrat, kriptovanje i dekriptovanje kao i ključ za iste, simetrične i asimetrične vrste algoritama, javni i privatni ključ, konkretni algoritmi, jednosmerne heš funkcije, digitalni potpis i digitalni sertifikat, PKI infrastruktura i DLP problem).

2. MIX-NET ŠEME

Šeme za elektronsko glasanje zasnovane na mrežama za miksovanje (mix networks, mix-net) su veoma brojne u naučno-istraživačkim radovima bar jednu deceniju unazad, verovatno iz razloga što je pionirski rad David-a Chaum-a iz 1981. godine [1] toliko uticao na istraživače i naučnike. Autor je prvobitno zamislio da se mix-net koristi za nepratljivu (engl. untraceable) e-poštu, ali su druge namene nađene ponajviše u oblastima gde se zahteva anonimnost, poput e-glasanja, e-novca, e-aukcija i sl.

Mix-net predstavlja kriptografsku primitivu čija namena je da oformi komunikacioni kanal koji će pružiti osobinu anonimnosti, slično osobini nedodirljivog komunikacionog kanala, između dve krajnje tačke. Ova mreža se sastoji od povezanog niza mix-eva, elektronskih uređaja sa ciljem da obezbede anonimnost pošiljaoca poruke. Postoje veći broj vrsta i načina korišćenja mix-net šema, ali sve one dele isti koncept i neka zajednička svojstva.

Osnova ideja ovakve komunikacije se opisuje interakcijom krajnjih korisnika uobičajeno nazvanih Ana i Boban. Ana hoće da pošalje anonimnu poruku Bobanu. Ona će kriptovanu poruku da prosledi do jednog mix servera. I drugi učesnici u anonimnoj komunikaciji će da pošalju svoje kriptovane poruke do mix servera. Kada se nakupi dovoljan broj poruka, taj mix server će da promeni redosled pristiglih poruka na slučajan način i da ih prosledi dalje. To je proces miksovanja. Sledeći mix server će da učini isto itd., sve dok poruka ne izađe iz mix-net oblasti i dođe do Bobana. Proces miksovanja se u osnovi sastoji od dva koraka. U prvom koraku će se pristigle poruke obrađivati kriptografskim algoritmom u zavisnosti od tipa miksovanja (dole je detaljnije objašnjeno). U drugom koraku ide spomenuto nasumično preslagivanje poruka. Kada poruka izađe iz mix oblasti, ona će do Bobana doći u potpuno čitljivom obliku. Na ovaj način je sakrivena veza između ulaznih i izlazni poruka.



Slika 1. *Proces miksovanja na mix serveru*

Neka je A skup ulaznih poruka u mix sa indeksima i, gde $i \in \{1, 2, \ldots, n\}$. Prvi korak u miksu je definisan preko kriptografske funkcije K, koja transformiše ulazne poruke sa $B_i=K(A_i)$. Drugi korak je da tako dobijene poruke treba podvrgnuti permutacijskoj funkciji P tako da se na slučajan način izmešaju poruke $C_j=P(B_i)$. Niko ne može sa strane saznati vezu između indeksa i i j kod permutacijske funkcije, niti tu vezu pamti mix server. Za izlazne poruke C_j važi $j \in \{1, 2, \ldots, n\}$.

U zavisnosti od načina kako se porukama barata u mreži za miksovanje, na nizu mix servera, postoje dva tipa miksovanja:

a) Dekripciono miksovanje (predstavljeno u [1]) i

b) Reenkripciono miksovanje.

Oba tipa miksovanja koriste parove javno-privatnog ključa radi asimetričnog kriptovanja.

Kod ***dekripcionog*** miksovanja označimo niz mix servera sa $M_1, \ldots, M_n$. Svaki od njih ima par ključeva PK_i i JK_i, gde je i redni broj servera u nizu. Postoji ukupno g glasača na izborima i n mix servera. Takođe postoji funkcija za kriptovanje K i funkcija za dekriptovanje D koje koriste spomenute ključeve, javni i privatni, tim redosledom. Svaki glasač će svoj gl. listić kriptovati K funkcijom sa javnim ključevima svih mix servera i to u redosledu od M_n do M_1. Svi tako kriptovani gl. listići će biti poslati na jedno centralno mesto, npr. na javni diskusioni forum, odakle će ih zaprimiti mix server M_1. Moguće je takođe na mix server M_1 direktno poslati sve kriptovane gl. listiće. Gl. listić je kriptovan na sledeći način:

$$\mathbf{K(\ K(\ \ldots\ K(\ \ldots\ K(gl.listić)_{JKn}\ \ldots\ )_{JKi}\ \ldots\ )_{JK2}\ )_{JK1}}$$

Mix server M_1 će svojim privatnim ključem PK_1 i dekripcionom funkcijom D skinuti jedan sloj zaštite sa svakog gl. listića i onda takve gl. listiće poslati na M_2 server (uz preslagivanje gl. listića pre slanja). Sada jedan gl. listić izgleda ovako:

$$\mathbf{K(\ \ldots\ K(\ \ldots\ K(gl.listić)_{JKn}\ \ldots\ )_{JKi}\ \ldots\ )_{JK2}}$$

M_2 mix server će skinuti sledeći sloj kripcione zaštite svojim privatnim ključem PK_2. Proces će se ponavljati na dalje; ovo je izgled i-te iteracije:

$$\mathbf{K(\ \ldots\ K(gl.listić)_{JKn}\ \ldots\ )_{JKi}}$$

Takav proces se nastavlja sve dok mix server M_n ne skine zadnji sloj kripcije i, uz obavezno permutovanje gl. listića, onda ih čitljive napokon objavi u javnosti. Sledi prebrojavanje.

Glasač mora da zna onoliko javnih ključeva koliko ima mix servera u nizu. Dodatno mora obaviti isto toliko računskih operacija za čin kriptovanja gl. listića. To je glavna slabost ovog načina miksovanja. Zato je razrađena drugačija varijanta ove šeme za e-glasanje.

Kod ***reenkripcionog*** miksovanja glasač treba da zna samo jedan javni ključ za kriptovanje svog gl. listića. To je moguće, jer se koriste asimetrični algoritmi koji dozvoljavaju reenkripciju kao što je ElGamal. Glasač šalje kriptovani gl. listić M_1 mix serveru, koji radi reenkripciju svojim privatnim ključem, pa posle permutacije svih dobijenih gl. listića šalje ih sve na sledeći mix server u nizu. Proces se ponavlja sve dok se ne dođe do zadnjeg servera M_n, te se onda mora pristupiti dekriptovanju gl. listića. To se izvodi tako što se primeni dekriptovanje odgovarajućim ključevima koji su raspoređeni po svim mix serverima.

Kod mix-net šema za e-glasanje, glasači šalju kriptovani glasački listić na ulaz mix oblasti. Gl. listić prolazi kroz niz mix servera, da bi se na izlazu iz mix oblasti pojavio čitljiv gl. listić, ali bez naznake čiji je on. Rezultat se onda računa iz takvih gl. listića. Za što viši nivo anonimnosti u niz treba dodati što više mix servera. Mix serveri međusobno mogu komunicirati preko e-pošte ili diskusionih foruma, bilo privatnih bilo javnih (ovo zadnje je moguće jer su gl. listići kriptovani). Mix servere mogu posedovati ili održavati suprostavljene strane, poput svih političkih partija i nevladinih organizacija, te na taj način povećati sigurnost i poverenje u celi tok e-glasanja. Tek saradnjom svih korumpiranih mix servera se može doći do identiteta glasača.

3. ŠEME SA HOMOMORFNIM KRIPTOVANJEM

Glavna razlika između homomorfnog kriptovanja i običnog kriptovanja se ogleda u postojanju algebarske operacije nad šifratima koja za posledicu ima algebarsku operaciju nad polaznim čitljivim podacima. Sama vrsta ovih algebarskih operacija zavisi od kriptografskog algoritma.

Pretpostavimo da razmatramo asimetrični kriptografski sistem. Neka je AK funkcija za asimetrično kriptovanje, O_1 i O_2 polazni čitljivi podaci i K privatni ili javni ključ. Ako postoje takve algebarske operacije $\oplus$ i $\otimes$ da vredi

$$\mathbf{AK(O_1)_K \oplus AK(O_2)_K = AK(O_1 \otimes O_2)_K}$$

onda postoji osobina homomorfizma odnosno takvo kriptovanje zovemo homomorfno kriptovanje.

U opštem slučaju algebarske operacije $\oplus$ i $\otimes$ mogu biti iste. Ipak obično je $\oplus$ operacija sabiranja, a od operacije $\otimes$ zavisi koje dve osnovne vrste homomorfnih osobina postoje:

a) Aditivna, kada je $\otimes$ sabiranje i

b) Multiplikativna, kada je $\otimes$ množenje.

Homomorfnu osobinu, na primer, imaju ElGamal i Paillier kriptosistemi. Po svojoj prirodi ElGamal ima osobinu multiplikativnog homomorfizma, dok kod Paillier-a homomorfizam je aditivnog tipa. Moguće je prilagoditi ElGamal da ima aditivni homomorfizam zbog pogodnosti koje u tom slučaju ima kod e-glasanja.

Zaključak koji se može izvesti iz kriptografskog homomorfizma je sledeći: mogu se izmeniti kombinovani šifrati bez potrebe da se koriste polazni čitljivi podaci i bez znanja ključa kriptovanja. Tako polazni podaci ostaji tajni.

Kod homomorfnih šema za e-glasanje, svaki glasač će da kriptuje svoj gl. listić javnim ključem izborne komisije $AK(gl.\ listić_i)_K$ i onda će ih svi poslati izbornoj komisiji u virtuelnu glasačku kutiju. Ako korišćeni kriptografski sistem ima osobinu aditivnog homomorfizma, izborna komisija će uraditi sabiranje kriptovanih gl. listića

$$\sum_{i=1}^{n} \mathbf{AK}\left(\mathbf{gl.listi}_{\mathbf{i}}\right)_{\mathbf{K}}$$

što ima za posledicu da važi sledeće

$$\mathbf{AK}\left(\sum_{i=1}^{n} \mathbf{gl.listi}_{\mathbf{i}}\right)_{\mathbf{K}}$$

Pošto sada imamo zbir gl. listića koji je kriptovan, potrebno je da izborna komisija svojim privatnim ključem skine taj sloj zaštite i onda objavi rezultat u javnosti.

Na ovaj način je zadržana privatnost glasača jer ni jedan gl. listić nije prebačen u čitljivu formu, već je od svih gl. listića izračunat zbir dok su još u kriptovanom stanju. Dekriptovan je samo zbir koji je sam po sebi anoniman. Ako su kriptovani gl. listići pre prebrojavanja na ovaj način objavljeni u javosti, onda svako može da 1) vidi da li je njegov glas uzet u obzir i 2) da li je zbir dobro napravljen jer to svako može uraditi prostim zbrajanjem svih javno dostupnih gl. listića.

Pored navedenih dobrih osobina, ostaju važna pitanja: a) kako se glasač mora identifikovati i b) kako konstruisati gl. listić da bude pogodan za prebrojavanje. Uzmimo za primer e-glasanje tipa referenduma sa dva moguća odgovora: DA i NE. Ako za potvrdni odgovor uzmemo da vredi 1, a za odrični da vredi -1, onda sadržaj gl. listića su upravo te brojčane vrednosti. Glasač kriptuje željeni broj i šalje izbornoj komisiji, koja zbraja kriptovane vrednosti koristeći homomorfnu osobinu. Na kraju, dekriptovan zbir će biti pozitivan (što znači da je DA opcija pobedila), negativan (NE je pobedilo) ili je nula (te odluka nije donešena).

4. ŠEME ZASNOVANE NA POTPISU NA SLEPO

Poruke se potpisuju na slepo kada pored spomenutih Ane i Bobana imamo treći entitet u koga imaju poverenje prva dva entiteta ali ne postoji obostrano poverenje između Ane i Bobana. Neka se treći entitet zove Ceca. Ana šalje poruku Bobanu koju potpisuje Ceca, ali pošto poruka treba da ostane tajna, potpis je izveden na slepo. Analogija je korišćenje koverte koja ima unutrašnje strane obložene indigo bojom, pa zatvorenu poruku unutar koverte preko indiga spolja potpisuje Ceca, ne znajući šta je sadržaj poruke. Onda Ana odbacuje kovertu i tako potpisanu poruku predaje Bobanu.

Simbolima zapisano Ceca ima javni ključ *JK*, privatni ključ *PK* i bira broj *k* na slučajan način i za koji važi $1<k<N$, gde je *N* moduo po kome se izvode operacije. Poruka koju želi poslati je *p*, nju prvo Ana kovertira da se njen sadržaj ne može pročitati

$$\dot{\mathbf{p}} = \mathbf{p} \cdot \mathbf{k}^{\mathbf{JK}} \bmod \mathbf{N}$$

Ceca ovako dobijenu kovertiranu poruku potpisuje

$$\ddot{\mathbf{p}} = \dot{\mathbf{p}}^{\mathbf{PK}} \bmod \mathbf{N} = \left(\mathbf{p} \cdot \mathbf{k}^{\mathbf{JK}}\right)^{\mathbf{PK}} \bmod \mathbf{N} = \mathbf{p}^{\mathbf{PK}} \cdot \mathbf{k} \bmod \mathbf{N}$$

Sada Ceca vraća na slepo potpisanu poruku Ani koja uklanja sloj kovertiranja

$$\dddot{\mathbf{p}} = \left(\ddot{\mathbf{p}} / \mathbf{k}\right) \bmod \mathbf{N} = \mathbf{p}^{\mathbf{PK}} \bmod \mathbf{N}$$

Ana šalje poruku Bobanu koji javnim ključem Cece skida zaštitu (što podrazumeva da je tu poruku potpisala upravo Ceca) i tako dobija čitljivu poruku.

Umesto da opišemo opšti postupak kod šema za e-glasanje zasnovanih na potpisima na slepo, navešćemo detalje konkretne šeme po nazivom Sensus. U ovoj šemi postoje četiri modula: registrator, virtuelno gl. mesto (u originalu pollster), validator i brojač. Registrator je odgovoran za registraciju birača pre početka glasanja. Virtuelno glasačko mesto pomaže biraču da završi sve računske i ostale proceduralne korake. Validator će proveriti da li je birač stvarno registrovan i onemogućiti dvostruko glasanje. Brojač će prikupljene gl. listiće prebrojati i tako dobiti izborni rezultat. Sledi opis koraka u ovoj šemi:

1. Registrator šalje identifikacioni broj birača *ID* i tajni token broj *T* svim biračima registrovanim kod njega.
2. Svaki birač (sam ili u saradnji sa virtuelnim gl. mestom) generiše asimetrični par ključeva *(ie, id, in)* a onda šalje svoj javni ključ *(ie, in)* registratoru, zajedno sa *ID* i *T* brojem radi autentifikacije. Birač takođe generiše par ključeva za kovertiranje *(se, sd)*.
3. Validator preuzima par *(ID, ie)* za sve birače od registratora, a onda objavljuje u javnosti svoj javni ključ *(ve, vn)*.
4. Brojač generiše sopstveni asimetrični par ključeva i onda objavljuje javni ključ *(te, tn)*.
5. Proces e-glasanja počinje. Birači šalju virtuelnom gl. mestu svoj glas, koji onda pravi kovertirani gl. listić $b = m \bullet k^{ve} \ mod \ vn$ i onda šalje validatoru (b, ID, b^{id}) kriptovano sa *ve*.

6. Validator dekriptuje zadnje sa *vd*, pa poverava da li vredi $(b^{id})^{ie} = b$ i ako jeste potpisuje na slepo gl. listić i vraća $b^v \bullet d$.
7. Virtuelno gl. mesto dekriptuje zadnje sa *id*, skida kovertu b^{vd} računajući $m^{vd} = b^{vd}/k \bmod vn$ i onda proverava da li je $(m^{vd})^{ve} = m$.
8. Ako je odgovor potvrdan, onda on šalje brojač (m^{vd}, V^{se}) kriptovano sa *te*, gde *V* predstavlja popunjen gl. listić.
9. Brojač dekriptuje dobijeno sa *td*, proverava da li vredi $V^{se} = (m^{vd})^{ve}$ i onda potpisuje V^{se} tako što računa $(V^{se})^{td}$. Lista birača se ažurira da bi se njegov gl. listić označio upotrebljenim i njemu se dodeljuje potvrda u vidu slučajnog broja *R* i onda njega i $(V^{se})^{td}$ šalje virtuelnom gl. mestu.
10. Virtuelno gl. mesto ispituje da li vredi $((V^{se})^{td})^{te} = V^{se}$ i onda šalje *(R, sd)* brojaču.
11. Brojač dekriptuje V^{se} sa *sd* i ažurira rezultat u zavisnosti šta je pročitao u dekriptovanom tekstu. Birač se tada u listi birača označava kao neko ko je iskoristio svoje pravo na glas.

5. ŠEME ZASNOVANE NA BIOMETRIJI

Šeme za e-glasanje zasnovane na biometriji glasača koriste biometrijske karakteristike za identifikaciju glasača. Ovo je od velikog značaja naročito kod udaljenog tipa e-glasanja, jer predstavlja dosta dobar način da se utvrdi da na udaljenom mestu, sa druge strane veze, stoji upravo osoba koja se tako predstavlja [8].

Biometrijski sistemi za identitetsku proveru glasača analiziraju njegove fizičke karakteristike, ali i karakteristike ponašanja. Inače, u opštoj literaturi se navode tri načina za proveru identiteta: nešto što osoba zna (lozinka je najpoznatiji primer), nešto što osoba ima (npr., smart kartica ili vremenski token) i nešto što osoba jeste (to je područje biometrije). Da bi neke ljudske karakteristike kvalifikovali kao biometrijske, one moraju biti univerzalnog tipa (svako ih mora posedovati), jedinstvene (jedinstvenost za sve glasače), nepromenljive (vremenski i prostorno) i karakteristike se moraju tehnički obraditi tj. one moraju biti merljive. Najpoznatija fizička karakteristika u biometriji je otisak prstiju, koja se čak uspešno koristila i pre početka elektronske obrade u policijskom radu. Ostale su izgled oka, crte lica itd. Neke od karakteristika ponašanja su potpisivanje, način govora, dinamika hoda itd. Krajnja biometrijska karakteristika, koja bi bila odlična po mnogim osobina, je analiza DNK lanca osobe, ali ona još uvek nije dovoljno jeftina i jednostavna za implementaciju.

Nijedan savremeni biometrijski sistem nije do kraja precizan. Ipak, za potrebe e-glasanja granica ili prag koji treba da se pređe je dosta strog u odnosu na neke druge moguće primene biometrije. Dva pokazatelja koja se najčešće koriste za prikazivanje preciznosti su FRR i FAR. **FRR** (false rejection rate) predstavlja procenat pogrešnog odbijanja biometrijskog sistema u odnosu na ukupan mogući broj uspešnih provera identiteta. Pogrešno odbijanje se događa kada pravog glasača biometrijski sistem ne prepoznaje zbog nedovoljnog podudaranja ulaznih biometrijskih podataka sa podacima u bazi podataka svih glasača, te mu tako pogrešno odbije identifikaciju. **FAR** (false acceptance rate) predstavlja procenat pogrešnog prihvatanja biometrijskog sistema u odnosu na ukupan mogući broj pokušaja sa nevalidnim biometrijskim podacima. Pogrešno prihvatanje se događa kada lažnog glasača biometrijski sistem prepoznaje kao pravog glasača, pronašavši u bazi podataka biometrijske podatke slične ulaznim biometrijskim podacima.

Kod e-glasanja postoje dva slučaja pogrešnog prihvatanja. U prvom slučaju, lažni glasač koristi tuđe pravo glasa, što ima dve posledice: a) glasao je neko ko to nije uopšte ni trebao uraditi i b) oduzeo je mogućnost glasanja pravom glasaču, što će ovoga dovesti do pogrešnog odbijanja. U drugom slučaju glasača prepoznaju kao neku drugu osobu, ali takođe sa pravom glasa. Ovaj glasač nije oštećen po pitanju prava glasa, ali će druga osoba za koju je zamenjen biti pogrešno odbijena.

Neki biometrijski sistem ima uobičajeno pet sastavnih modula [8]:

1. senzorski uređaj, koji skenira neku biometrijsku karakteristiku i konvertuje u digitalni oblik (npr., skener za otiske prstiju),
2. modul za izdvajanje biometrijskih karakteristika, koji obrađuje digitalizovni biometrijski podatak radi izdvajanja karakteristika koje nekoga čine jedinstvenim i koje se mogu smestiti u šablon,
3. modul za skladištenje podataka (baza biometrijskih podataka),
4. modul za poređenje, koji služi za poređenje izdvojene karakteristike sa podacima iz šablona sačuvanog u bazi podataka,
5. modul za donošenje odluke, koji uz eventualnu pomoć ljudskog faktora prihvata/odbija identitet (to je verifikacija) ili utvrđuje identitet na osnovu rezultata poređenja (to je identifikacija).

Za potrebe e-glasanja se može koristiti OASIS-ov standard XCBF (XML Common Biometric Format) koji je 2003. usvojen u toj organizaciju.[9] To je XML format sa odgovarajućom šemom kojom se "opisuju podaci za proveru identiteta preko čovekovih karakteristika kao što su DNK, otisci prstiju, izgled oka i oblik šake. (On) … omogućava osiguravanje, prikazivanje, zapisivanje i izvršavanje upita prema bazi podataka sa biometrijskim informacijama".

Mislimo da će biometrijske šeme za e-glasanje postati dosta zastupljene onda kada senzori za čitanje čovekovih karakteristika postanu svuda dostupni (= jeftini, brzi, pouzdani). Imajući u vidu da firma Apple prodaje mobilne telefone u milionskim količinama, treba svakako imati u vidu njihov najnoviji proizvod iPhone verzije 5S koji ima standardno ugrađen podepidermalni skener otisaka prstiju sa rezolucijom od 500ppi, a koji se prvenstveno koristi za otključavanje mobilnog telefona, ali su i druge primene već najavljene [10]. Verovatno će i drugi proizvođači slediti ovog "tehnološkog pionira".

6. ŠEME ZASNOVANE NA PKI I SMART KARTICAMA

PKI (public key infrastructure) predstavlja računarsku infrastrukturu javnih ključeva koji je vrsta distribuiranog mrežnog sistema sa funkcijama skladištenja digitalnih sertifikata, izdavanja, obnove i poništavanja digitalnih sertifikata, kao i funkcija za uspostavljanje relacija poverenja. Koristi se asime-

trično kriptovanje, a osnovna komponenta je sertifikacioni autoritet (CA, certificate authority). Pametne kartice (smart cards) su plastične kartice koje liče po izgledu na platne kartice i imaju u sebi elektronski uređaj, najčešće mikrokontroler. Naziv "pametne" su dobile po mogućnostima što im pruža ugrađeni mikrokontroler. Pametne kartice se koriste u e-glasanju za identifikaciju glasača, kao i za kriptografske radnje neophodne pojedinim šemama za e-glasanje. Često imaju smešten u sebi ključ osobe, te se tako smatraju delom PKI infrastrukture [7].

Ovde će se prikazati sa realnih i uspešnih e-izbora održanih u Estoniji. Njihovo e-glasanje se odigrava sedmicu dana pre dana klasičnih, papirnih izbora i to mogućnost važi za ceo taj period. Pri tome svaki glasač može više puta glasati tj. menjati svoj glas, a važi samo zadnji iskorišteni gl. listić. Ako se glasa na klasičnim izborima, elektronski glas se poništava. Izborna komisija može u potpunosti suspendovati e-izbore ako proceni da je došlo do značajnih napada i ometanja toka e-izbora [3].

Funkcije	
Auth	Autentifikacija
Cast	Glasanje
Rand	Generisanje slučajnog broja
Enc	Kriptovanje
Sign	Digitalno potpisivanje kriptovanog gl. listića
Save	Skladištenje gl. listića
Count	Prebrojavanje gl. listića
Svojstva	
PK	Javni ključ sistema za e-glasanje
SK	Privatni ključ sistema za e-glasanje
PK[i]	Javni ključ za potpisivanje i-tog glasača
SK[i]	Privatni ključ za potpisivanje i-tog glasača
PK[0]	Javni ključ pozadinskog servera
SK[0]	Privatni ključ pozadinskog servera
v	Gl. listić
r	Slučajno generisani broj
ID	Datoteka sa ličnim podacima glasača

Tabela 1. *Funkcije i svojstva šema za e-glasanje zasnovanih na PKI*

Postoje tri osnovne komponente: glasačka aplikacija, javni server i pozadinski server. Glasačka aplikacija se nalazi na glasačevom računaru i preko nje se glasa. Javni server je on-line računar koji glasaču pruža mogućnost da glasa. Pozadinski server čuva popunjene glasačke listiće i sa njih računa izborni rezultat. Sledi kraći opis procesa e-glasanja sa ovakvim šemama. Glasač se konektuje na javni server i autentifikuje se svojim akreditivima. Sa dobijene liste opcija bira jednu željenu opciju *v*. Sada glasač generiše slučajan broj *r*, pa ga zajedno sa izabranom opcijom kriptuje javnim ključem sistema za e-glasanje *PK*. Šalje javnom serveru potpisan kriptovani glas svojim privatnim ključem *Sign(Enc(v, r, PK), SK[i])*. Javni server potpisano šalje dalje pozadinskom serveru koji, radi provere prava glasa, gleda da li ta osoba ima pravo glasa i da li ga je dosad već iskoristila. Uskladišten je glas *v*, a glasaču se šalje potpisana potvrda *Sign(ID, SK[0])*, koja ne sadrži šta je glasač izabrao. Glasač tu potvrdu može dekriptovati sa javnim ključem *PK[0]*. Posle perioda glasanja, mrežni server izvodi računanje izbornih rezultata i objavljuje ih u javnosti.

Sledi detaljniji opis estonske šeme zasnovane na PKI i smart karticama. Glasačka aplikacija je jedna mrežna aplikacija koja koristi SSL (secure socket layer) protokol da zaštiti komunikaciju do javnog servera. Kada glasačka aplikacija radi na Windows operativnom sistemu potrebno je koristiti Internet Explorer, a sama aplikacija je potpisana ActiveX kontrola. Ključ *PK* je zapisan u glasačku aplikaciju. Pozadinski server se sastoji od dva dela: skladišta glasova i brojača glasova. Javni server šalje gl. listiće skladištu glasova, a glasaču zauzvrat prosleđuje potvrdu da je glasao. Brojač je server van javne Internet mreže, a gl. listiće dobija od skladišta glasova. On ne dobija podatke sa kojima može saznati identitet glasača. Estonski sistem za e-glasanje kreira i održava pet odvojenih log datoteka u kojima se beleže pojedini koraci glasanja opisani kroz faze gl. listića. Izborna komisija može, radi potreba revizije i rešavanja sporova, da pregleda ove zapise. Prvo se proveri njihov integritet, pa onda relacije između logova (npr., unija LOG2 i LOG3 treba biti isto što i LOG1, dotle LOG4 i LOG5 unijom daju LOG3). Postoje sledeće log datoteke:

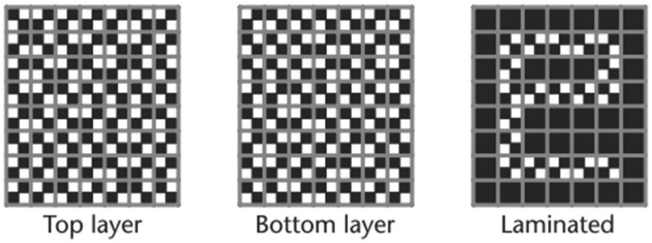
- LOG1 – primljeni potpisani kriptovani gl. listići,
- LOG2 – odbačeni potpisani kriptovani gl. listići sa razlogom odbacivanja,
- LOG3 – potpisani kriptovani gl. listići prebačeni do brojača,
- LOG4 – nepravilno formatirani kriptovani gl. listići,
- LOG5 – prebrojani gl. listići.

U Estoniji postoji nacionalna PKI infrastruktura RSA tipa i velika većina građana poseduje ličnu kartu sa čipom tj. smart karticu radi autentifikacije i digitalnog potpisivanja. Svako ko hoće da e-glasa mora posedovati ovakvu ličnu kartu. Zato je uloga nacionalnog sertifikacionog autoriteta veoma važna za njihovo e-glasanje. Skladište glasova uvek kontaktira nacionalni CA radi provere digitalnih potpisa. Dodatno, skladište glasova će odbaciti sve e-glasove koje je jedan glasač potpisao odnosno višestruke e-glasove jednog glasača će prebaciti u LOG2 datoteku. Posle dekriptovanja privatnim ključem na brojaču glasova, njihov format se poredi sa striktnim pravilima kako gl. listić treba izgledati. Gl. listići koji nisu uspešno prošli proveru formatiranja idu u LOG4 datoteku, tako da se broje samo pravilno formatirani gl. listići i to se zapisuje u datoteku LOG5.

7. ŠEME ZASNOVANE NA VIZUELNOJ KRIPTOGRAFIJI

Kriptografija kao nauka o tajnom pisanju može vizuelne informacije poput slika ili teksta da kriptuje, pa se takav pristup zove vizuelna kriptografija. Sa druge strane, proces dekriptovanja u ovom slučaju može biti obavljen bez računarske podrške. Od šema za e-glasanje zasnovanih na vizuelnoj kriptografiji opisaćemo najpoznatiju već spominjanog autora David-a Chaum-a iz 2004. godine [2].

Kao glasačka mašina, može se koristiti DRE ili čak običan PC računar, ali moraju biti opremljeni posebnim štampačem. Glasački listić se na ekranu prvo popuni. Štampač će onda odštampati dva transparentna lista sa spoljnih strana jer su listovi spojeni jedan preko drugog. Slika i tekst se formiraju kroz XOR operaciju odštampanih tačaka sa oba lista, tako da ako su listovi razdvojeni na njima se nalazi nečitljiva tj. kriptična šuma tačaka (slika 2). Kada glasač proveri da li je ono što je izabrao na ekranu isto što dobija od štampača, potvrđuje da je u redu i uzima jedan od listova (donji ili gornji). Onaj drugi list treba odmah ručno ili mašinski da iseče na deliće.



Slika 2. *Spajanje dva sloja glasačkog listića sa vizuelnom kriptografijom* **[2]**

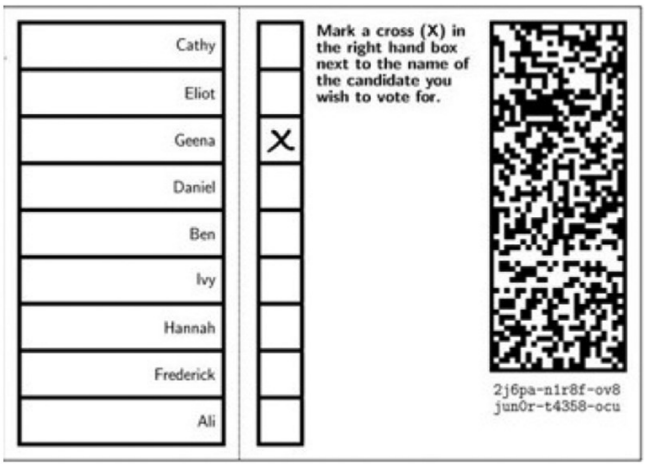
List koji je izabrao, glasaču služi kao potvrda kako je glasao. Na taj list, u trenutku pre nego je izašao iz štampača, je na ivici odštampan pseudo slučajan niz brojeva i javni ključ izborne komisije. Sa ovim podacima se odmah može proveriti da li je glasački listić ispravno kriptovan kroz javno dostupan softver za verifikaciju. Pošto se završi period glasanja, svi listovi koje su zadržali glasači će se objaviti na javnom sajtu, te tako glasač može proveriti da li je njegov glas uzet u obzir i, ako to nije slučaj, on sa svojim listom, kao dokazom, ipak može iskoristiti svoje pravo na glasanje.

8. OSTALE ŠEME

Od ostalih šema opisaćemo dve koje uključuju korišćenje papirnih gl. listića i jednu koja je besplatna i otvorenog programskog kôda. Pri tome, kod prve dve šeme glasač će doći na glasačko mesto i na poseban način označiti specijalno pripremljen gl. listić. Posle će moći da elektronskim putem proveri da li mu je gl. listić uzet u obzir prilikom računanja rezultata i to koristeći informacije zapisane na papirnoj potvrdi koja se izdaje glasaču nakon čina glasanja.

8.1 Prêt-à-Vote šema

Prêt-à-Vote šema (dalje ćemo koristi skraćeno: PaV šema) je najpoznatija šema sa specijalno napravljenim gl. listićem, čak se ponegde klasa šema sa sličnim pristupom zove po ovoj šemi. Gl. listić se sastoji iz dva dela koji su uspravno podeljeni perforacijom. Na levoj strani se nalazi spisak opcija koje su poređane nasumičnim redosledom i koji je različit na svakom drugom gl. listiću. Odmah uz spisak opcija, ali sa druge strane perforacije, na desnom delu, nalaze se kvadrati za izbor opcije. Na desnoj strani se još nalazi bar-kôd u kome je enkriptovan redosled opcija sa tog gl. listića. Njega ne može jedna strana učesnica u procesu e-glasanja sama dekriptovati, jer su delovi potrebnog ključa raspodeljeni na više strana i obično su to suprostavljene partije/kandidati tj. zastupnici pojedinih opcija [4].



Slika 3. *Izgled gl. listića za PaV šemu* **[11]**

Kada glasač označi željenu opciju, odcepiće levi deo i uništiti ga. Desni deo će se skenirati radi prebrojavanja i on onda ostaje glasaču kao dokaz kako je glasao (ili se pravi kopija, a original ostaje na izbornom mestu). Po završetku glasanja, svi desni delovi gl. listića će se objaviti u javnosti. Na serveru će se prvo promešati gl. listići, a onda će sve strane upotrebiti delove ključeva da dekriptuju glasove, koji će potom biti prebrojani, a krajnji rezultat će se objaviti u javnosti.

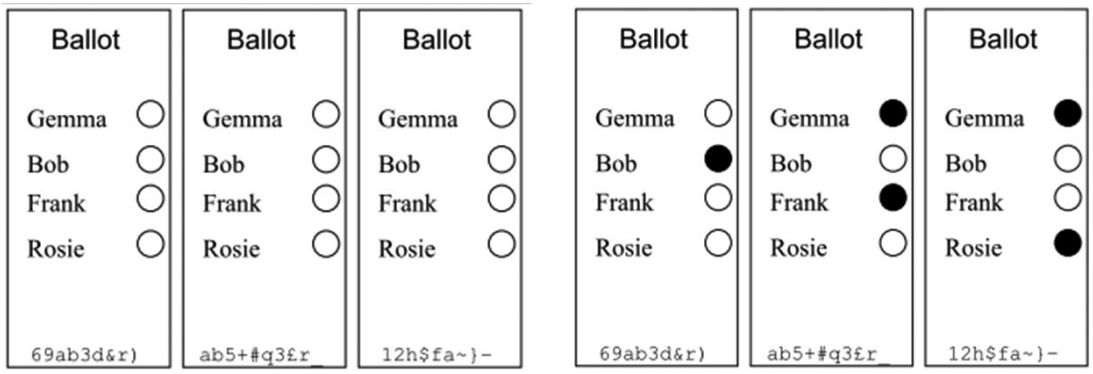
8.2 ThreeBallot šema

ThreeBallot je šema koja preko papirnih gl. listića i bez kriptografskih metoda ima svojstva koja uobičajeno poseduju ostale šeme za e-glasanje, poput proverljivosti. Postoje tri odvojena gl. listića za jednog glasača. Svi gl. listići su isti po izgledu osim jedinstvenog ID broja pri dnu listića, koji je nasumično odabran i koji je osmišljen tako da ga ljudi teško pamte. Glasač bira sa gomile praznih gl. listića tri listića i onda mora ispoštovati pravilo za glasanje: dva popunjena kruga za željenu opciju, a jedan popunjen krug protiv neželjene opcije. Pošto su opcije poravnate po redovima, lako se proverava koliko koja opcija ima popunjenih krugova (mora biti jedan ili dva kruga po opciji). Nepoštovanje ovog pravila za glasanje dovodi do toga da trostruki gl. listić postaje nevažeći [5].

Sada glasač bira jedan od tri listića. Pošto su za ispravan glas potrebna sva tri listića, napraviće se kopija izabranog listića i nju glasač čuva kod sebe. Kopija izabranog listića služi glasaču kao potvrda. Svi gl. listići se sada stavljaju u jednu glasačku kutiju. Po završetku izbora se računa krajnji rezultat uzimajući u obzir da za izabrane opcije postoji duplo više popunjenih krugova nego za neizabrane opcije.

8.3 Helios šema

Helios je sistem za e-glasanje namenjen situacijama gde sigurnost nije prva stavka u prioritetima. Sistem je otvorenog programskog kôda po GPL licenci i zato je besplatan za svakog ko ga hoće koristiti za svoje potrebe, ali isto tako na njihovom matičnom sajtu postoji stranica http://vote.heliosvoting.org/ gde se može učestvovati u tekućim glasanjima ili se tu može napraviti novo e-glasanje. Autor i glavni programer sistema je Ben Adida. Zadnja verzija sistema je v3, a dosad je ostavljeno 25 hiljada glasova na sistemu.



Slika 4. *Prazan gl. listić i gl. listić sa izabranom Gemma opcijom kod ThreeBallot šeme*

Glasač će dobiti na adresu e-pošte pozivnicu za izbore sa stranicom za e-glasanje, korisničkim imenom i lozinkom. Osnovna ideja je da se odvoji posao kreiranja e-glasačkog listića i posao autentifikacije glasača, s tim da ova dva posla idu baš ovim redosledom. Priprema gl. listića se odvija u nekoliko koraka kroz JavaScript program integrisan na web stranici i taj posao se može obaviti bez sukcesivnih konekcija ka web serveru tj. bez Interneta. Inače svako može na ovaj način proveriti kako ide proces pripreme gl. listića. Pripremljeni gl. listić se čuva dovoljno dugo do trenutka kada ide jedini trenutak gde se glasač predstavlja sistemu – trenutak glasanja tj. predaje gl. listića sistemu ("ubacivanja u e-glasačku kutiju"). Čak i tada je moguće proveriti šta se događa sa e-glasom [6].

Gl. listić se kriptuje pre nego što napusti glasačev web browser. Na serveru se čuva takođe u kriptovanom obliku. Svi gl. listići se prebrojavaju kriptografskim pristupom koji daje kriptovani konačni rezultat. Na kraju se samo taj kriptovani rezultat dekriptuje. Posle kriptovanja se dobija ID broj sa kojim glasač može kasnije da pronađe e-glasački listić.

9. ZAKLJUČAK

Pažnja u ovom pregledu je posvećena šemama sistema za elektronsko glasanje (EVS, electronic voting systems), polazeći od osnovnih kriptografskih pojmova. Analizirano je sedam grupa šema za e-glasanje, koje predstavljaju osnovu svakog sistema za elektronsko glasanje, i to: mix-net šeme, šeme sa homomorfnom enkripcijom, šeme zasnovane na potpisu na slepo, šeme zasnovane na biometriji, šeme zasnovane na vizuelnoj kriptografiji, šeme zasnovane na PKI i smart karticama, kao i grupa preostalih šema. Konstrukcija šema je često složena, a osobine i karakteristike koje one poseduju su različite i zavise u dobroj meri od načina implementacije šeme i uopšte od stepena organizacije elektronskog glasanja. U daljem istraživačkom radu bi se šeme za e-glasanje trebale uporediti međusobno na više razina apstraktnosti, kao i po osobinama koje poseduju. Većina šema su poprilično teške za implementaciju u realnom izbornom procesu, što bi oduzelo dosta resursa (vremena, novca itd.) za njihovo uvođenje. I pored dobrih i poželjnih karakteristika koje poseduju, prema njima većina glasača bi imala otpor, jer im tolika tehnička složenost ne bi bila shvatljiva. To na kraju dovodi do nepoverenja u izbore i posledično do smanjenja izlaska na glasanje, što je u suprotnosti sa jednim od važnih proklamovanih ciljeva uvođenja e-glasanja. Vidimo da u kategoriji ostalih šema ima zanimljivih predloga za manju (ili čak nikakvu) upotrebu elektronske obrade kod glasanja u cilju većeg poverenja glasača. Mislimo da bi za početak trebalo uvesti e-glasanje kao dodatni, neobavezni deo izbornog procesa. Takođe bi kombinacija neke od šema za e-glasanje sa npr. biometrijskim šemama povećala sigurnost izbornog procesa do nivoa koji je viši nego kod klasičnih izbora.

10. LITERATURA

[1] David Chaum, "Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms", Comunications of the ACM Vol 24 Num 2, 1981.
[2] David Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections", IEEE Security & Privacy 1540-7993/04, 2004.
[3] Epp Maaten, "Towards remote e-voting: Estonian case", 2004.
[4] Peter Y. A. Ryan, Thea Peacock, "Pret a Voter: a Systems Perspective", 2005.
[5] Roberto Araújo, Peter Y. A. Ryan,"Improving the Farnel Voting Scheme", 2008.
[6] Fatih Karayumak, Maina M. Olembo, Michaela Kauer, Melanie Volkamer, "Usability Analysis of Helios - An Open Source Verifiable Remote Electronic Voting System", 2011.
[7] Jurlind Budurushi, Stephan Neumann, Melanie Volkamer, "Smart Cards in Electronic Voting: Lessons Learned from Applications in Legally-Binding Elections and Approaches Proposed in Scientific Papers", EVOTE2012 Bregenz, Austria, 2012.
[8] Saša Paunović, Dušan Starčević, "Biometrijski sistemi za utvrđivanje identiteta", Međunarodna konferencija i Izložba Infotech 2013, Aranđelovac, 2013.
[9] www.oasis-open.org/committees/xcbf/, pristupljeno 15. maja 2014.
[10] "Apple predstavio iPhone 5S, uz A7 čip i fingerprint senzor", pristupljeno 15. maja 2014., http://mobile.benchmark.rs/mobile_vesti/apple_predstavio_iphone_5s_uz_a7_cip_i_fingerprint_senzor
[11] http://www.pretavoter.com/about.php, pristupljeno 15. maja 2014.

Dragoljub Pilipović – Slobomir P univezitet, Bijeljina
Kontakt: dragoljub.pilipovic@spu.ba
Oblast interesovananja: metodologije razvoja softvera, elektronsko obrazovanje, obrazovanje u IKT, sigurnost računarskih sistema, elektronsko glasanje, digitalne valute, cloud computing

Dušan Starčević – redovni profesor, Fakultet organizacionih nauka, Beograd
Kontakt: starcev@fon.bg.ac.rs
Oblast interesovananja: računarska grafika, interakcija čovek-računar, multimediji, računarske mreže