Synthesis
International Scientific Conference of IT and Business-Related Research

MOGUĆNOST PRIMENE ELEKTRONSKOG SERVISA ZA GLASANJE PUTEM INTERNETA U SRBIJI

THE POSSIBILITY OF IMPLEMENTING INTERNET VOTING SERVICE IN SERBIA

Marko Marković, Saša Adamović
Univerzitet Singidunum, Srbija, Beograd

Apstrakt:
U radu se ispituje trenutno stanje razvoja elektronskih servisa u e-upravi. Pored različitih servisadetaljno se razmatra i servis koji bi građanstvu omogućio elektronsko glasanje putem Interneta, koje bi otvorilo niz pogodnosti za obe strane. Međutim, servis koji bi omogućio ovu uslugu, dizajniran je u skladu sa standardnim bezbednosnim protokolima koji su trenutno u upotrebi. Kod ovakvih servisa neophodno je obezbediti servis autentifikacije, integriteta, neporecivosti i privatnosti. S obzirom na to da su postojeći servisi za elektronsku trgovinu dostigli visok nivo praktične bezbednosti, tu činjenicu uzimamo kao osnovu za razmatranje i uvođenje servisa za glasanje putem Interneta u Srbiji. Razmotrićemo sve kritične tačke ovih kripto-sistema. Kao najveći problem nameće se aspekt društvene prihvatljivosti, koji podrazumeva poverilački odnos između građana i servisa, problem anonimnosti, prebrojavanja i drugih važnih aktivnosti koji postoje unutar ovog servisa, a koje su se do sada obavljale na vrlo primitivan način u našoj zemlji. Uvođenjem ovog servisa, troškovi čitave organizacije izbornog procesa bili bi smanjeni, a rezultati obrađeni u realnom vremenu sa visokim stepenom preciznosti i pouzdanosti. Sa druge strane, ergonomične osobine uticale bi na povećanje izlaznosti na izbore, što bi uslovilo donošenje kvalitetnijih odluka na nivou cele zemlje.

Ključne reči:
Internet glasanje, elektronsko glasanje, privatnost.

Abstract:
This paper analyses the current development stage of electronic services in e-government. Besides numerous other services, the authors discuss the service that would allow the citizens to electronically vote over the Internet. Such voting would bring numerous benefits to both sides. However, such service is designed based on the standard security protocols that are currently in use and it should provide service authentication, integrity, non-repudiation and privacy. Considering that the existing services for e-commerce have reached a high level of practical security, we shall take this fact as a basis for considering the possibilities of introducing the Internet voting service in Serbia. Moreover, we shall examine all the critical points of the encryption system. The biggest issue is the aspect of social acceptance, which implies creditor relationship between citizens and services, the issue of anonymity, counting and other important activities within the service that have so far been performed in a very primitive way in our country. The introduction of this service would reduce the costs of the entire voting process, and the results would be processed in real time with a high level of accuracy and reliability. On the other hand, ergonomic features would trigger an increase in the election turnout rates, which would also have a positive bearing on the decision-making process at the national level.

Key words:
Internet voting, e-voting, privacy.

1. UVOD

Pravo na biranje predstavnika je osnovni koncept demokratije, to je politički sistem u kome jedan narod svojom slobodnom voljom bira svog vođu. Postoje dva osnovna tipa glasanja: javno i tajno. Servis koji će biti razmatran u ovom radu treba da obezbedi uslove za tajno glasanje. Tajno glasanje je oblik glasanja u kome izbor glasača ostaje anoniman. Glavna svrha ovog sistema je da izbor glasača bude autentičan, odnosno da se spreče spoljni uticaji kao što su zastrašivanje i podmićivanje. Tradicionalni oblik tajnog glasanja se sastoji u tome da glasač svoj glas napiše na listu papira, koji potom ubacuje u kutiju zajedno sa drugim listićima. Glasovi iz kutije se na kraju glasanja prebrojavaju od strane više osoba ili posmatrača izbornog procesa.

Organizovanje i sprovođenje Internet glasanja je veoma izazovan i odgovoran zadatak. Potrebno je istovremeno obezbediti upotrebljiv i veoma bezbedan servis autentifikacije, integriteta i neporecivosti. Internet glasanje ima dobru osnovu i šansu da bude primenjen u Srbiji. Tehnološki, sistem bi bio implementiran preko standardnih bezbednosnih protokola koji imaju široku primenu u pružanju usluga na Internetu (e-bankarstvo, e-trgovina). Glasanje preko Interneta ima niz pogodnosti, neke od njih su glasanje sa udaljenih lokacija, veća izlaznost mlađeg stanovništva, osoba sa posebnim potrebama i manji troškovi izbornog procesa. Jedan od glavnih ciljeva ovog protokola jeste da se glasanje sprovede na takav način da se zaštiti privatnost građana, omogući korisnicima da provere status glasa i da se na bezbedan način obavi prebrojavanje glasova. U izbornoj proceduri svaki glasač se može smatrati kao potencijalni zlonamerni učesnik. Iz tog razloga, bezbednosni protokoli moraju biti otporni prema velikom broju zlonamernih metoda i aktera, čiji je cilj da smanje objektivnost izbornog procesa.

Prema najnovijim istraživanjima, kompjuterska pismenost za 2011. godinu procentualno iznosi 48,99%, od čega je 14,78% delimično kompjuterski pismeno (Republički zavod za statistiku, 2011). Na osnovu ovog istraživanja, možemo da zaključimo da pored problema koji se odnose na infrastrukturu i tehnologiju, koja je osnov ovog sistema, postoje problemi i na polju razvoja sistema.

E-mail: mmarkovic@singidunum.ac.rs
DOI: 10.15308/Synthesis-2015-76-80

2. PREGLED TRENUTNOG STANJA

Švajcarski polu-direktni demokratski sistem omogućava građanima da učestvuju u donošenju bilo kog zakona predloženog od strane vlasti, odnosno predloženog od strane građana, ukoliko se za to prikupi dovoljan broj potpisa. Kao rezultat toga, Švajcarci izlaze na glasanje u proseku od 4 do 6 puta godišnje, kako bi prihvatili ili odbili predloge novih zakona, što potvrđuje da je dobar glasački sistem neophodan za demokratska prava građana u Švajcarskoj (Geneva State Chancellery, 2010).

Central Electoral Commission (CEC) je centralna izborna komisija koja je oformljena 1. januara 2010. godine, u isto vreme kada je predstavljen sistem elektronskog glasanja u ženevskom kantonu. Po zakonu, *CEC* ima pristup svim operacijama u izbornom procesu, mogućnost provere određenih informacija u bilo kom trenutku nezavisno od izbornih operacija. Zakon propisuje proveru sistema Internet glasanja i javno objavljivanje rezultata istraživanja, svake tri godine. Prva provera sistema izvršena je 2012. godine.

Zatvaranje glasačke kutije obavlja se za vreme sastanka zvaničnika *CEC*-a koji pripremaju, odnosno generišu, više kriptografskih ključeva različite namene. Nakon generisanja ključeva, sledeća faza je konfigurisanje kriptografskih mehanizama, čija je uloga da obezbede neprobojnost glasačke kutije, a to znači da pristup glasovima pre brojanja nije moguć. Glasačka kutija je „bezbedna" kada se glasovi ne mogu prepravljati ili pročitati. Privatni ključ poznat je samo sistemu i on je jedini koji može da zapiše glasove u glasačku kutiju, validan glas je samo onaj koji se može dešifrovati privatnim ključem. Jednom kada je glasačka kutija zapečaćena, veb-sajt preko koga se vrši glasanje može biti otvoren za korišćenje. Kada glasač pristupi veb-sajtu preko Internet pretraživača, tada ostvaruje bezbednu komunikaciju preko *HTTPS* protokola.

Uloga *HTTPS* protokola je da obezbedi uzajamnu autentifikaciju između klijenta i servera i da podaci koji se razmenjuju između njih, budu u šifrovanoj formi. Jednom kada je ova veza ostvarena, *SSL* protokol, unutar *HTTPS*-a obezbeđuje prvi nivo šifrovanja za saobraćaj između klijenta i servera.

Slede procedure za obavljanje glasanja preko Interneta:

- Na stranici za autentifikaciju upisuje broj glasačke kartice i ostale lične podatke;
- Prihvataju se uslovi korišćenja;
- Popunjava se glasački listić;
- Proveravaju se uneti podaci i šalje se glas.

Protokol koji treba da obezbedi šifrovanje na nivou aplikacije je *Surencryption*. *Surencryption* se sastoji od šifrovanja podataka na nivou aplikacije pre slanja preko *HTTPS*-a. Šifrovanje je bazirano na simetričnim ključevima, čiji tajni ključ potiče od *UVN* broja koji je upotrebljen za dobijanje heš vrednosti, odnosno otiska koji se koristi za slanje. Podaci se šifruju dva puta, na različite načine, što proces šifrovanja čini snažnijim. Po dobijanju šifrovane poruke i otiska poruke, sistem preko javnog ključa obavlja verifikaciju parametara (digitalni potpis), nakon čega se glas zapisuje u e-glasačku kutiju. Ovaj sistem je zasnovan na konceptu digitalnog potpisivanja.

Trenutni veb-pretraživači ne podržavaju tehnologije potrebne za implementaciju drugog nivoa šifrovanja. Uglavnom je za to pripremljena dodatna aplikacija, koja se preuzima sa zvaničnog sajta za glasanje, preko koje se glasač autentifikuje.

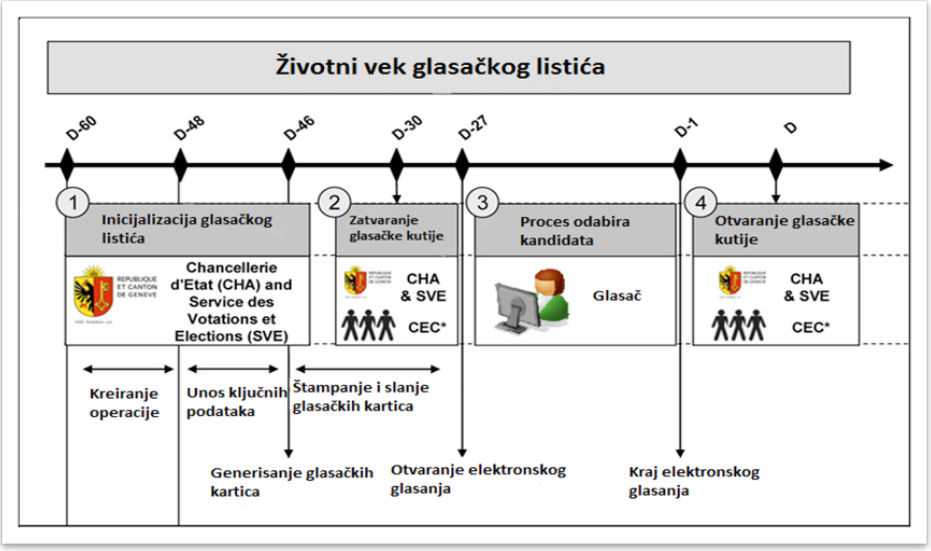
2.1 AUTENTIFIKACIJA OSOBA SA PRAVOM GLASA

Glasači dobijaju glasačku karticu putem pošte. Svi glasači poseduju jedinstveni glasački broj *UVN* koji se nalazi na kartici. Uloga ovog broja je u procesu autentifikacije. Kako ovaj broj ne bi zapao u pogrešne ruke, broj se nikada ne šalje preko kanala za glasanje, umesto njega šalje se otisak (heš), što predstavlja deljenu tajnu između glasača i sistema. Na osnovu otiska, napadač ne može da sazna *UVN* broj (Geneva State Chancellery, 2010).

Pilot projekat započet 2002. godine, završen i prvi put testiran 2005. godine za lokalne izbore saveta, kada je više od 9 hiljada ljudi glasalo putem Interneta. To je bio prvi pokušaj korišćenja glasanja putem Interneta u Estoniji. Zahvaljujući tome, u Estoniji je 2007. godine prvi put u svetu korišćeno glasanje putem Interneta za parlamentarne izbore. Od tada ovaj sistem se uspešno koristi, primenjen je 6 puta na parlamentarnim izborima 2007, jun 2009, oktobar 2009, 2011, 2013, 2014. godine (Vabariigi Valimiskomisjon, 2012).

Slede procedure za obavljanje glasanja putem Interneta u Estoniji:

- Glasač se identifikuje ličnim dokumentom (slika 2);
- Glasač dobija glasački listić i dve koverte;
- Glasač ispunjava svoj listić i stavlja ga u prvu kovertu na kojoj nema informacija o glasaču;
- Zatim, prva koverta se stavlja u drugu na kojoj se nalaze informacije o glasaču;



Slika 1. Životni vek glasačkog listića.

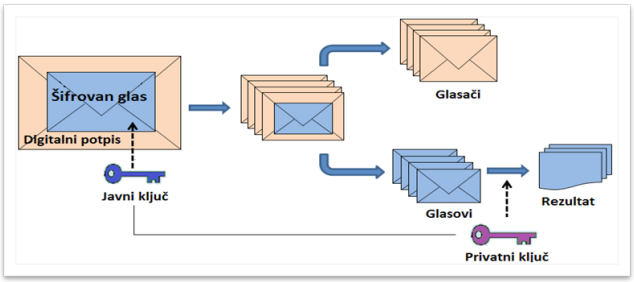
DOI: 10.15308/Synthesis-2015-76-80

- Po prijemu koverti na biračko mesto i utvrđenog prava na glasanje, na osnovu informacije na spoljnoj koverti, ona se otvara i prva koverta odnosno unutrašnja se stavlja u glasačku kutiju.

Ovaj sistem obezbeđuje da glasačev izbor ostane tajan, a da se u isto vreme zabeleži da je glasao. Glasanje preko Interneta u Estoniji zasniva se na predočenom konceptu. Sistem se može predstaviti kao sistem sa dve koverte. Aplikacija koju korisnik dobija na svom računaru, po završetku glasanja šifruje glas javnim ključem servisa za glasanje, što predstavlja prvu neoznačenu kovertu, nakon toga glasač digitalno potpisuje kovertu, čime se autentifikuje pred sistemom, dok glas ostaje tajan. Pre prebrojavanja, servis verifikuje digitalni potpis, lične podatke i anonimno dešifruje unutrašnju kovertu odnosno glas. Metod koristi kriptografsku šemu sa javnim i privatnim ključevima, gde nacionalni komitet za glasanje poseduje privatni ključ. Autentifikacija glasača se vrši biometrijskom ličnom kartom, koja poseduje sertifikat.

Slika 2. Primer lične karte u Estoniji.

Svaki glasač mora da poseduje svoju identifikacionu karticu sa jedinstvenim *PIN* kodom. To je u stvari pametna kartica na kojoj se nalazi mikro čip i ujedno ona predstavlja digitalni identitet osobe. Sve što je potrebno glasaču da bi obavio glasanje je lična karta, čitač, računar i stabilna Internet veza.



Slika 3. Sistem prenošenja glasova u Estoniji.

Ovakav način glasanja u Estoniji je moguć samo 7 dana unapred, u toku izbornog procesa, da bi se obezbedilo vreme u cilju eliminisanja duplih glasova do završetka izbornog procesa. Kako bi obezbedili da glasač izrazi svoju pravu volju, čak i ako se glasač predomisli postoji mogućnost da se glas promeni elektronski ili da se na glasačkom mestu fizički zabeleži glas za vreme trajanja izbora. Primer, ako glasač ode na glasačko mesto i glasa, time se poništavaju svi prethodni elektronski glasovi, i taj poslednji glas se uvažava. Ako se desi da glasač glasa elektronski i fizički, ta informacija se prosleđuje elektronskom odboru za glasanje, i njegov elektronski glas se poništava. Poslednji glas je konačan. Verifikacijom elektronskih sistema, omogućiće se tačna informacija o računaru koji se koristi za glasanje. Visok stepen kompjuterske pismenosti, moderna infrastruktura kombinovana sa e-upravom, čini Internet glasanje u Estoniji mogućim i široko prihvaćenim.

2.2 HOMOMORFNO ŠIFROVANJE

Homomorfno šifrovanje obezbeđuje zahtevane osobine za implementaciju bezbednog sistema za Internet glasanje. Ideja koja stoji iza ovog sistema je dovoljno jednostavna. Sa standardnim šemama za šifrovanje, šifrovani podaci moraju prvo da se dešifruju kako bi mogli da se obrade. Homomorfno šifrovanje omogućava različite operacije nad šifrovanim podacima, odnosno omogućava rad sa šifrovanim podacima, a da pre toga nema potrebe za dešifrovanjem. U prevodu, moguće je uzeti dva dela šifrata, uraditi određenu operaciju nad njima, i njihov rezultat na kraju dešifrovati.

Primer funkcija šifrovanja koji poseduje multiplikativnu homomorfnost je *El-Gamal*. Ako se šifrat poruke *m1* i šifrat poruke *m2* pomnože, rezultat je šifrat čitave poruke *m*.

$$E(m1) * E(m2) = E(m1 * m2)$$

Dva primera homomorfnih kripto sistema su *RSA* i *El-Gamal*. U *RSA* sistemu posle šifrovanja otvorenog teksta *P* u šifrat *C*, možemo pomnožiti *C* sa 2, onda dešifrovati *2C* i tako dobiti *2P*. Ovo ne bi bilo moguće u nekom simetričnom sistemu. Na primer, ako bi u *AES* šifratu pomnožili *C* sa 2 i onda dešifrovali, kao rezultat bi dobili neku slučajnu vrednost umesto *P* (Stenbro, 2010).

El-Gamal je kriptološki sistem baziran na diskretnim algoritmima koji je dobio ime po svom pronalazaču *Taher El Gamal-u*. Ovo je odličan sistem sa javnim ključem koji se koristi za generisanje digitalnog potpisa, baziran na *Diffie-Hellman* protokolu. U slučaju *El-Gamal* protokola, možemo uzeti šifrate glasova i na kraju dobiti tačan rezultat.

Šema rada:

- Bob generiše prost broj p i broj g koji predstavlja vrednost između 1 i (p-1).
- Generiše se slučajna vrednost x koja predstavlja njegov privatni ključ.
- Bob računa y, $y=g^x mod P$.
- Ključ koji Bob šalje Alisi je p, g i y.
- Alisa kada dobije vrednosti, uzima vrednosti koju je dobila i poruku M koju hoće da pošalje, zatim generiše svoju slučajnu vrednost k.
- Računa svoju vrednost a: $a = g^k mod P$.
- Nakon toga izračunava b: $b = y^k M mod P$.
- a i b kao šifrovane vrednosti šalje Bobu.
- Šifrat C predstavljaju parametri (a, b), a to znači $(g^k, My^k)=C$.

Dešifrovanje:

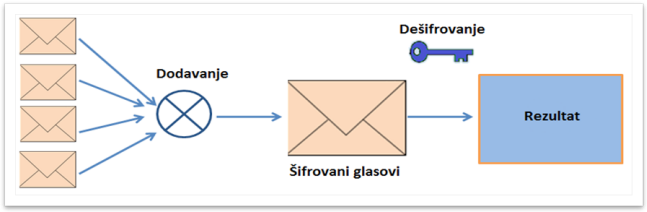
$$C = \frac{b}{a^x} = M\frac{y^k}{(g^k)^x} = M\frac{y^k}{(g^x)^k} = \frac{My^k}{y^k} = M$$

Koristeći x možemo izvršiti faktorizaciju drugog dela šifrata i doći do poruke.

U kriptografskom protokolu Internet glasanja, identitet glasača može da se koristi za šifrovanje, tako da glasač ima mogućnost da proveri tačnost svog zapisanog glasa. U slučaju spajanja glasova, originalan glas neće biti dostupan kao u slučaju kad se glasovi šifruju odvojeno. U glasačkom sistemu množenja glasova, onemogućena je provera njihovog integriteta. Rešenje bi bio neki protokol koji sabira glasove i na kraju prikazuje ukupan zbir glasova. Glavna prednost homomorfnog sabiranja glasova je u tome da nije potrebno dešifrovanje pojedinačnih glasova, već se privatni ključ koristi samo jednom za dešifrovanje konačnog zbira za svaki izborni proces. Na ovaj način sve vreme se čuva

DOI: 10.15308/Synthesis-2015-76-80

tajnost pojedinačnih glasova. Primer protokola homomorfnog sabiranja (slika 4).



Slika 4. Homomorfno dodavanje glasova.

Svaki od ovih primera dozvoljava operacije nad tekstom samo na jedan način (sabiranje ili množenje). Kriptološki sistem koji u isto vreme podržava obe operacije je poznat kao potpuno homomorfno šifrovanje. Postojanje efikasne i potpune homomorfnosti ima velike praktične implementacije na primer u *cloud computing-u*.

3. PREGLED PREDLOŽENOG REŠENJA

Homomorfnost je kriptografska forma koja omogućava određene računske operacije nad šifratom. Na izlazu generiše šifrovan rezultat, koji kada se dešifruje odgovara rezultatu operacija nad originalnim tekstom. Ovo je poželjna funkcija u arhitekturi modernih komunikacionih sistema. Homomorfna kriptografija predstavlja dobru osnovu za povećanje bezbednosnih mera nad nepoznatim sistemima i aplikacijama koje pristupaju osetljivim informacijama.

Za glasački softver postoje dva moguća homomorfna algoritma sa osobinom dodavanja: *Paillier* i *El-Gamal*. *Paillier* algoritam je već sam po sebi dobar za slučaj dodavanja glasova i mnogo češće se koristi. Ovaj algoritam nam daje mogućnost dodavanja glasova, i ako su oni predhodno šifrovani. Originalna *El-Gamal* šema koristi osobine multiplikacije i ona se može modifikovati tako da poseduje osobine homomorfnog dodavanja, ali može doći do problema u slučaju velikog broja glasača kada ova šema postaje neefikasna, dok *Paillier* pruža jednostavniju implementaciju i dobre performanse. *Paillier-ov* algoritam je kriptološki sistem baziran na sistemu javnih ključeva koji je dizajnirao Francuski istraživač *Pascal Paillier* 1999. godine (Choinyambuu, 2009).

Primer generisanja ključeva:

- (n, g) – javni ključevi za šifrovanje;
- (λ, μ) – privatni ključevi za dešifrovanje;
- (α, β) – slučajni brojevi;
- *gcd* – najveći zajednički delilac;
- *lcm* – najmanji zajednički sadržalac;
- *Zn* – skup celih brojeva *n*;
- *Zn** – skup uzajamno prostih brojeva do *n*;

Javni ključ *n*: $n = pq$;

Privatni ključevi: $= lcm(p - 1, q - 1)$,

$$\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n;$$

Funkcija *L* je definisana kao:

$$L(u) = \frac{u-1}{n};$$

Generišu se dva prosta broja, p i q nezavisno jedan od drugog, gde važi:

$$gcd(pq, (p - 1)(q - 1)) = 1.$$

Postoje dva načina za generisanja g gde $g \in Zn^*$.

Prvi način:
Slučajno izabran g iz skupa Zn^* gde važi:

$$gcd(\frac{g^{\lambda} \bmod n^2 - 1}{n}, n) = 1$$

Drugi način:
Slučajno izabrani α i β iz skupa Zn^* gde važi:

$$g = (\alpha n + 1)\beta^n \bmod n^2$$

Šifrovanje:

m – poruka (izbor glasača), $m \in Zn$;
r – slučajan broj, $r \in Zn^*$;
$E(m)$ – šifrat;

$$E(m) = g^m * r^n \bmod n^2$$

Dešifrovanje:

$$m = L(c^{\lambda} \bmod n^2) * \mu \bmod n$$

Pretpostavimo da imamo *Nv* - broj glasača. Svaki glas moramo da predstavimo u numeričkoj formi i šifrujemo *Paillier-om*. Svako šifrovanje datim algoritmom zahteva slučajan broj, tako da je svaki glas različito šifrovan. Serverska baza *b* mora da ispuni uslov $b > Nv$. Na kraju izbornog procesa izborni zvaničnici imaće broj *Nv* od šifrovanih glasova. Tako mogu izračunati rezultat svih šifrovanih glasova na *mod* n^2.

Rezultat T je predstavljen formulom:

$$T = \prod_{i=1}^{Nv} ci \bmod n^2.$$

Ove homomorfne osobine mogu biti korišćene od strane sigurnih elektronskih sistema. Pretpostavimo jednostavan izborni sistem gde glasač bira "za" ili "protiv" u svom glasu. Neki broj glasača *m* bira svoj glas (1 ili 0). Svaki glački listć je šifrovan pre popunjavanja. Izborni zvaničnici uzimaju rezultat šifrovanih glasova koje dešifruju, rezultat sadrži vrednost *n* koja predstavlja zbir svih "za" glasova. Tako zvaničnici mogu izračunati *(m-n)* što predstavlja "protiv" glasove. Uloga slučajnog broja *r* osigurava da će dva ekvivalentna glasa biti šifrovana u identičan šifrat sa zanemarljivom verovatnoćom, sa ciljem da sačuvamo servis anonimnosti.

Predstavljeno rešenje (slika 5) sadrži 3 glasača koji u ovom primeru imaju dve izborne opcije, „za" (DA) i „protiv" (NE) odnosno *true* ili *false*. U nastavku ovog dela detaljno ćemo diskutovati o funkcionalnostima koje su predstavljene u ovoj šemi, koja zadovoljava sve osobine glasačkih sistema.

Posmatraćemo šemu kroz četiri faze:

Faza 1: Glasaču su putem posebnog interfejsa ponuđene dve izborne opcije. Glasač može da se opredeli samo za jednu opciju. Tačan korisnički interfejs u ovom radu nije bio predmet istraživanja. Ovaj deo rada se odnosi na samu šemu glasačkog procesa unutar predloženog algoritma.

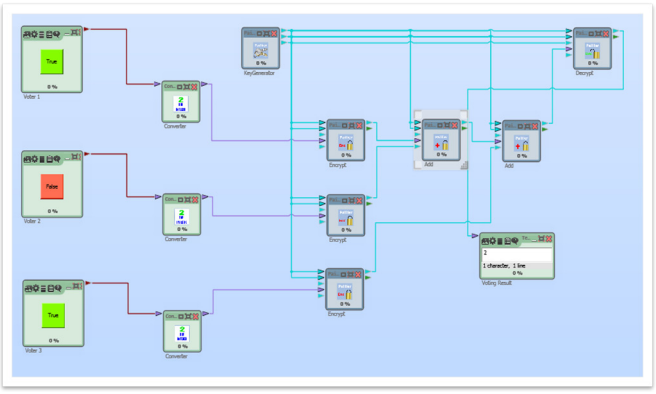
DOI: 10.15308/Synthesis-2015-76-80

Faza 2: Nakon odabira glasa, glas se šifruje sa *Paillier*-ovim algoritmom, sa ključevima *n* i *g*. Ključevi *n* i *g* su generisani preko kriptografskog generatora koji je definisan od strane *Paillier* algoritma. Treba zapaziti da se svi glasovi u šemi šifruju istim ključem nezavisno od broja glasača i tipa glasa.

Faza 3: Sa pretpostavkom da postoje 3 glasača, kako je to prikazano na šemi. Nakon prvog i drugog dobijenog šifrata (šifrovani glasovi) za glasača 1 i 2, koristi se *Paillier*-ova funkcija dodavanja (kriptografska konkatenacija) sa ključevima *n* i *g*, što rezultuje sa novim podatkom (koji u potpunosti enkapsulira glasača 1 i glasača 2) koji se na identičan način funkcijom dodavanja povezuje sa šifratom glasača 3 i tako generiše novi enkapsulirani podatak. Proces enkapsulacije u slučaju više glasača u potpunosti bi odgovarao osobinama binarnog stabla. Enkapsulirani podatak u ovoj šemi obezbeđuje glasačima potpunu anonimnost u odabiru glasa, ova vrsta anonimnosti je upravo proizvod homomorfnog svojstva *Paillier* algoritma, što i predstavlja jedan od glavnih doprinosa predložene šeme.

Faza 4: U poslednjoj fazi, na strani subjekta koji prebraja glasove, utvrđuje se broj glasova "za" i "protiv". Do ovih informacija se dolazi primenom *Paillier*-ovog algoritma u režimu za dešifrovanje sa odgovarajućim ključevima. U ovoj fazi je moguće dešifrovati sve glasove, utvrditi izborne opcije (prebrojati glasove), ali nije moguće saznati identitet glasača ili napraviti tačnu vezu između glasača i izborne opcije. Ovakva vrsta anonimnosti je zahtevna kod ovakvih sistema, naravno ovi sistemi podrazumevaju nezavisan sistem ili podsistem za obavljanje autentifikacije glasača, radi provere glasačkog prava, koji su u skladu sa zakonom koji je država propisala.

U nastavku, prikazana je simulacija našeg glasačkog sistema sa 3 glasača u *cryptool* kriptografskom razvojnom okruženju, koje implementira sve kriptografske funkcije prema *NIST* standardu.



Slika 5. Simulacija praktične upotrebe glasačkog sistema sa primenom homomorfne kriptografije

4. ZAKLJUČAK

Na osnovu istraživanja u ovom radu i uvida u postojeće sisteme koji se već nekoliko godina uspešno koriste u stranim zemljama, smatramo da sistem ima dobar osnov za implementaciju i realizaciju u Srbiji. Bezbednosni protokoli koji predstavljaju osnovu ovog sistema danas se široko koriste u našoj zemlji u različitim granama ekonomije, trgovine i drugim aktivnostma na Internetu. Pored svih zahtevanih bezbednosnih mera i dalje je najveći problem poverenje.

Uvođenje ovog sistema blagovremeno bi uticalo na povećanje izlaznosti, pretežno mlađe generacije. Takođe, starijim osobama našeg društva i osobama sa posebnim potrebama stvorile bi se mogućnosti za izlazak na glasanje. Korišćenjem ovog Internet servisa postigle bi se ogromne uštede u državnom budžetu, iz koga se finansira čitav izborni proces.

Osnovni motiv ovog rada je bio da se dizajnira generički model sistema za glasanje koji će pomoću implementacije različitih kriptoloških protokola u kasnijim verzijama onemogućiti sve tipove kompromitacije i moguće manipulacije nad sistemom.

Nakon istraživanja različitih protokola za brojanje i šifrovanje glasova kao što su *El-Gamal* i *Paillier* došli smo do zaključka da homomorfne osobine sabiranja i *Paillier-ov* algoritam predstavljaju dobar osnov za postizanje anonimnosti i brojanje glasova. Dobar sistem definitivno postoji, na jednostavan način smo demonstrirali model koji predstavlja osnovu i početak nekog mnogo većeg sistema. O značaju ove teme i potrebe da se tehnološki unapredi, završićemo sa citatom:

"Oni koji glasaju ne odlučuju ništa, oni koji broje glasove odlučuju sve." - Joseph Stalin

LITERATURA

Choinyambuu, S. (2009). *Homomorphic Tallying with Paillier Cryptosystem:E-Voting seminar*. Preuzeto sa http://security.hsr.ch/msevote/seminarpapers/HS09_Homomorphic_Tallying_with_Paillier.pdf

Geneva State Chancellery. (2010). *Uncovering the veil on Geneva's internet voting solution*. Geneva: Geneva Information Tehnology Centre.

Republički zavod za statistiku. (2011). *Rezultati popisa 2011*. Preuzeto sa http://popis2011.stat.rs/?page_id=1221

Stenbro, M. (2010). *A Survey of Modern Electronic Voting Technologies*. Trondheim, Norway: Norwegian University of Science and Technology.

Vabariigi Valimiskomisjon. (2012). *Internet Voting in Estonia*. Preuzeto sa http://vvk.ee/voting-methods-in-estonia/engindex/

DOI: 10.15308/Synthesis-2015-76-80