Univerzitet Crne Gore
Prirodno-matematički fakultet - Podgorica

Saša Adžić

Elektronsko glasanje

-SPECIJALISTIČKI RAD-

Podgorica, 2011.

Univerzitet Crne Gore
Prirodno-matematički fakultet - Podgorica

Elektronsko glasanje

-SPECIJALISTIČKI RAD-

Kriptografija
Dr Vladimir Božović

Saša Adžić
Računarske nauke
[redacted]

Podgorica, jun 2011.

Sažetak

Elektronsko glasanje (poznato kao i e-glasanje) je termin koji sadrži nekoliko različitih vrsta glasanja, obuhvatajući elektronska sredstva za glasanje i brojenje glasova. Tehnologija elektronskog glasanja uključuje i bušene kartice, elektronske skenere i specijalizovane sisteme za glasanje. Ona takođe sadrži i prenos glasa preko telefonskih linija, privatnih računarskih mreža ili Interneta. Elektronsko glasanje može da ubrza brojenje glasačkih listića i pruži bolju dostupnost glasanja osobama sa invaliditetom.

U ovom radu opisani su značajni algoritmi elektronskog glasanja. Takođe je napravljena i simulacija algoritma Scantegrity II.

Abstract

Electronic voting (also known as e-voting) is a term encompassing several different types of voting, embracing electronic means of casting a vote and electronic means of counting votes. Electronic voting technology include punched cards, optical scan voting systems and specialized voting machines. It can also involve transmission of votes via telephones, private computer networks, or the Internet. Electronic voting can speed the counting of ballots and can provide improved accessibility for disabled voters.

This paper describes the major algorithms of electronic voting. Also it is made simulation of algorithm Scantegrity II.

Sadržaj

Uvod

Izbori i izborni proces odvija se od nastanka ljudske civilizacije. Glasanje u staroj Grčkoj odvijalo se pomoću kamenih pločica, Englezi u srednjem vijeku javno su iznosili svoje opredeljenje, Italijani u doba Renesanse koristili su kuglice, dok su u Pruskoj odluke zapisivali u javnom registru stanovnika. Prvi savremeni demokratski izbori bili su 1789. godine kada je izabran prvi predsjednik Sjedinjenih Američkih Država. Mnoge, pretežno industrijske zemlje krajem 19. vijeka izvršile su reformu svog izbornog sistema. Prvo je uveden princip direktnog i skrivenog glasanja. Kasnije su dodati i principi jednakosti i slobode, prevashodno, dozvoljeno je ženama i siromašnim slojevima stanovništva da glasaju. Prvi parlamentarni izbori u Crnoj Gori održali su 27. septembra 1906. godine.

Vremenom mnoge zemlje su izvršile dalje reforme i dozvolile glasanje pomoću pisma. U Njemačkoj to glasanje je uvedeno 1956. godine, u Švajcarskoj 1991. godine dok u Austriji 2008. godine. Mehaničke a kasnije i elektronske mašine za glasanje uvedene su da bi uštedjele novac i vrijeme. U Njemačkoj, zakon za glasanje pomoću mehaničkih mašina uveden je 1975. godine a pomoću elektronskih 1999. godine. U S.A.D. - u prve mehaničke mašine za glasanje korišćene su 1892. godine u Nju Jorku, dok su tridesetih godina prošlog vijeka svi veći gradovi prešli na korišćenje ovakvih mašina. Revolucija u elektronskom glasanje desila se 1960. godine kada su predstavljene bušene kartice.

Elektronsko glasanje se odnosi na bilo koje glasanje koje koristi elektronska sredstva u tom sistemu. Koristeći se ovom definicijom većina glasačkih sistema u svijetu pripadaju elektronskom glasanju. Elektronskom glasanju pripadaju optički skeneri, specijalizovani glasački sistemi (DRE), sistemi za elektronsko brojenje glasova, Internet ankete i glasanje, SMS ili telefonsko glasanje i td.

U elektronskom glasanju baziranom na papiru koriste se ekrani osjetljivi na dodir koji, nakon što glasač glasa, oštampaju glasački listić koji se ubaca u glasačku kutiju. Glasački listić se nakon toga broji pomoću optičkih skenera. Prednost ovog sistema je što uvijek postoji fizički dokaz glasačkog listića. Ipak i tada može doći do greške u kasnijem brojenju glasova kao i prenosu do optičkih skenera ukoliko se nalaze na cetralnoj lokaciji.

DRE je glasanje u kojem se samo koriste elektronski uređaji. Glasač na ekranu osjetljovom na dodir registruje svoj glas. Glas se čuva na memoriji uređaja i prenosi se do centralizovane stanice u kojoj se broji. Glas se može prebaciti i prebrojiti u trenutku glasanja ili na kraju izbornog procesa. Iako se glas može prebaciti preko javne mreže, ovo se jedino radi u slučaju ubrzanog brojenja. Memorija će se svakako koristiti u verifikaciji glasova. Prednost ovog sistema je brzina kojom se rezultati izbora mogu znati, jer se rezultati mogu dobiti trenutno. U

ovom sistemu se takođe umanjuje mehanička greška. Pošto se glasanje odvija preko računara, korisnički interfej se može prilagoditi potrebama glasača (glasači sa oštećenim vidom mogu da koriste veći font i slično). Ovaj sistem omogućava vladama i organizacijama da uštede novac jer se ne štampaju glasački listići a sistem se uz malo promjena može opet koristiti.

Internet glasanja, s druge strane, može da se odvija na udaljenim lokacijama. Ovaj sistem je već testiran za glasanje u inostranstvu. Estonija, na primer, koristi ovaj tip elektronskog glasanja pružanjem lozinke preko poštanske službe ili jedistvenog nacionalnog mikročipa. Na početku elektronsko glasanje je bilo ograničeno na glasanje pomoću elektronskih mašina za glasanje. Sada, sa bezbjednosne strane suočavamo se sa udaljenim elektronskim glasanjem, glasanje pomoću Interneta sa bilo kog mjesta i bilo kog uređaja koji ima pristup Internetu.

U ovom radu opisani su osnovi principi ,, običnog“ glasanja kao i elektronskog glasanja. Opisana je SAVE arhitektura sigurnog glasanja koja nudi pouzdani glasački proces. Pored toga obrađene su šeme elektronskog glasanja koje koriste optičke skenere sa značajnom zadrškom na Scantegrity II. Obrađena je i šema glasanja otpornog na prinudno glasanje (Coercion-Resistant Electronic Elections).

Witness-Voting System (glasanje pomoću posmatrača)

Poznato je da trenutni sistem javnog glasanja proizvodi rezultate koji su za neke učesnike nepouzdani. Vjekovi glasanja pomoću glasačkih listića i godine pomoću kompjuteralizovanih glasačkih funkcija nijesu značajno promjenile ovu tezu.

Pojednostavljeni sistem glasanja pomoću posmatrača prikazan je u sledećem primjeru. Značajno je da broj posmatrača bude neparan, da bi greške do kojih dolazi prilikom glasanja mogle riješiti pomoću kompromisa. Veći broj posmatrača omogućava bolje dokaze o regularnosti glasanja. Priprema se izborno mjesto, donosi se prazna i neprovidna kutija za glasačke listiće. Po mogućnosti montiraju se video kamere koje prate proces glasanja kao i posmatrače. Svi posmatrači moraju vidjeti da je glasačka kutija prazna prije nego što počnu izbori.

Glasanje se odvija na sledeći način:

- Glasač dolazi na izborno mjesto.
- Provjerava se indetitet.
- Potpisuje se u birački spisak i dobija glasački listić.
- Glasač zaokružuje svoj izbor tajno i ubacuje glasački listić u glasačku kutiju.
- Na kraju glasanja, kutija se otvara u prisustvi svih posmatrača i prebrojavaju se glasovi. Ukoliko je broj glasački listića jednak broju izašlih birača glasanje je validno.

Glasački sistem se sastoji od četiri glavne komponente:

1. Registracionog servisa koji provjerava i registruje legitimiteta birača.
2. Glasačkog mjesta gdje glasač ,,zaokružuje˝ svoj izbor.
3. Uređaja, glasačke kutije gdje se glasavi čuvaju.
4. Servisa koji broji glasačke listove i objavljuje rezultate.

Da bi sistem glasanja bio funkcionalan i pravedan potrebno je ispuniti sledeće zahtjeve:

1. **Privatnost glasača**: Nemogućnost povezivanja glasača sa glasom. Privatnost glasača mora biti zagarantovana čak i ako bi se time dovela funkcionalnost glasanja u pitanje, ili ako su sva izborna sredstva (npr. glasački listići i tajni ključevi) poznati napadaču. Tajnost glasa ne može da zavisi samo od komunikacijskog protokola, kriptografskog algoritma ili korumpiranosti izborne komisije.

2. **Povjerljivost izbornog integriteta**: Nemogućnost da bilo koji učesnik izbora utiče na ishod izbornog rezultata, osim doprinosa svojim glasom. Za bilo kog glasača sistem mora pružiti da postoji jedan i samo jedan validan glasački listić u glasačkoj kutiji.
3. **Privatnost u verifikaciji**: Nemogućnost da se otkrije indetitet glasača prilikom verifikacije njegovog glasa. Privatnost u verifikaciji ne smije doći u pitanje i kada glasač učestvuje u verifikaciji.
4. **Autetičnost glasača**: Moraju se obezbjediti uslovi za autentičnost glasača. Prije nego što se dozvoli glasanje potencijalnom glasaču, sistem mora imati efikasan mehanizam koji potvrđuje indetitet glasača. Ne smije se dogoditi da druga osoba glasa umjesto ,,pravog" glasača.
5. **Fizičko prebrojavanje i revizija**: Moraju se obezbjediti uslovi za reviziju i ponovno prebrojavanje glasova, sa najmamanjom mogućom greškom.
6. **100% tačnost**: Svaki glas ili odsustvo glasa (nevažeći glasovi) moraju se pravilno izbrojati. Ukoliko postoje greške u prepoznavanju glasa ili brojenju, te graške moraju biti zanemarive i ne smiju uticati na izborni rezultat. Takođe, ponovno brojenje glasova ne smije smanjiti tačnost.
7. **Mrežni sistem**: Mora se koristiti višestruka veza i ključevi, da bi se osigurala autetičnost i kontrola glasačkih listića. Neophodno je izbjeći bilo kakvu grešku ili zagušenje u protoku podataka u svim situacijama. Ukoliko dođe do greške prilikom prenosa podataka, ta greška se mora prepoznati i taj podatak ponovo poslati.
8. **Offline sigurna mrežna struktura**: Mora se obezbjediti sigurna struktura za predstavljanje i prikupljanje informacija od glasača. Potrebno je koristiti digitalne sertifikate u okviru jednog nadležnog organa. Ukoliko postoji mogućnost, mreža ne bi trebalo da bude dijeljena, već apsolutno privatna i prilagođena izbornom sistemu. Ako se koristi javna mreža, ona mora biti sigurna i ukoliko dođe do prekida na meži između dvije tačke mora postojati alternativna putanja.
9. **Autorizovan izbor reprezentacije**: Reprezentacija izbora, uključujući i formu glasačkog listića, mora biti ovjerena i kontrolisana od nadležnog organa.
10. **Korisnički izbor reprezentacije**: Glasač mora da ima mogućnost izbora jezika, pisma, veličine slova i drugih prezentacionih osobina.
11. **Promjena glasa prije glasanja**: Mora se dozvoliti svim glasačima da promjene svoj glas ili da ga pretvore u nevažeći, koliko hoće puta, prije zvaničnog glasanja.
12. **Dozvoliti uzdržanost**: Potrebno je dozvoliti svim glasačima da izaberu sve ili nekog učesnika. Takvim glasačima je samo potrebno ispisati poruku upozorenja ali dozvoliti takvo glasanje. Ta poruka ne smije biti javna, već poznata samo glasaču.

13. **Upozorenje ponovnog glasanja**: Ako je ponovno glasanje dozvoljeno, da bi se spriječile greške ili prevare, potrebno je upozoriti glasača da će prethodni glas biti izbrisan. Nakon toga će biti dozvoljeno ponovno glasanje. Upozorenje će biti vidljivo jedino glasaču i nikome više.
14. **Obezbjediti poništenje glasa**: Glasačima se može dozvoliti da poništе glas ukoliko to žele. Ovo može biti i dio mehanizma za ponovno glasanje.
15. **Nezavisnost tehnologije**: Glasanje ne bi trebalo da zavisi od određene tehnologije da bi se ispunio neki od prethodnih zahtjeva.
16. **Otvoreni kod**: Mogućnost da cio kod bude publikovan i verifikovan.

Sigurna arhitektura za bezbjedno glasanje

Sigurna arhitektura za bezbjedno glasanje (eng. Secure Architecture for Voting Electronically - SAVE) je arhitektura koja nudi pouzdani glasački proces. Ova arhitektura omogućava univerzitetima, kompanijama i organizacijama da lako i jeftino naprave glasački sistem koji odgovara svim važećim standardima.

Nažalost, nekoliko prvih primjera glasačkih mašina nijesu uradili puno da povećaju povjerenje u ovu tehnologiju. Prve mašine na dodir (Direct Recording Electric ili DRE) su imale loš korisnički interfejs, pa je dolazilo do gubitka podataka i one su izazivale frustraciju i nepovjerenje kod glasača.

Iako su se mediji fokusirali na napade i greške elektronskog izbornog sistema bitno je napomenuti da i mehanički i papirni izbori imaju jednakih problema. Problemi se javljaju u sigurnosti, privatnosti i prebrojavanju glasova. Elektronski sistem pokušava da u potpunosti riješi ove probleme. Takođe nudi novi korisnički interfejs koji ne dozvoljava glasačima mogućnost zbunjivanja. U ovom sistemu snimanje i obrada glasova je u potpunosti odvojena od korisničkog interfejsa.

Rješenje u bezbjednosnim propustima u mehaničkim i elektronskim sistemima za glasanje nudi SAVE. SAVE je otporan na greške, zlonamjerne učesnike i čuva tajnost glasanja. Glavni princip SAVE-a je da ne smije postojati ni jedna greška od momenta kada glas prođe kontrolu glasača. Sistem se sastoji od n - modula u kome se svaki modul razvija odvojeno i testira nezavisno prije spajanja u jedinstven sistem. Ovo podrazumjeva da se sistem sastoji od modula koji obavljaju relativno proste operacije.

Glasanje pomoću Interneta takođe ima svojih loših strana. Ukoliko se izuzme bezbjednost, dešavaju se usporavanja kao i potpuni prekidi veze. Sistem mora imati i alternativu u načinu komunikacije, pomoću mobilnih ili satelitskih telefona, kao i drugih načina komunikacije. Sistem mora biti i otporan na nedostatak električne energije. U Brazilu su ovaj problem riješili tako što su sva mjesta u kojima se glasa elektronski snadbjeli sa baterijama koje traju najmanje 14 sati, koliko traje i izborni proces.

Glasanje pomoću papira je podložno velikom broju grešaka. Čak i ako se prebrojavanje glasova vrši elektronski može doći do grešaka. Greške su naravno više moguće ako se prebrojavanje izvršava ručno. Papirni glasački listići mogu se napraviti drugačije nego originalni listići, raspored imena kandidata se može promjeniti tako da kod pored imena ne bude u pravilnom redosledu. Ukoliko se promijeni raspored na glasačkom listiću, na taj način se može prevariti skener da lažne listiće čita kao prave.

SAVE arhitektura se sastoji od sledećih slojeva:

- Korisnički interfejs,
- Uređaja koji su zaduženi za pravilno prepoznavanje glasova (slušaoci),
- Registratora koji kontrolišu da li su glasači i glasovi validni,
- Posmatrača koji su zaduženi za pravilnost i sigurnost,
- Komisije koja objavljuje rezultat izbora.

Pored pomenutih slojeva potreban je i dodatni sloj koje se obično zove mix-network, koji pruža sigurnost između pomenutih slojeva.

Za komunikaciju SAVE koristi XML i SOAP. Ova dva protokola su dostupna na svim modernim platformama i zbog toga su veoma pogodni. Svaki sloj mora registrovati sve dolazne i odlazne poruke. Takođe svaki sloj je podijeljen na module koji ne bi trebali da sadrže više od 1000 linija koda.

Cijeli proces komunikacije obuhvata kriptografske protokole koji su potrebni za prenos podataka. Slušaoci čitaju glasove sa korisničkog interfejsa, enkriptuju i šalju kao glasačke listiće. Kada se šalje glasački listić registrator mora biti siguran da je glasač validan. Registrator ne smije znati kako je glasač glasao. Popunjeni glasački listić mora se razdvojiti od kontrolnog dijela. Ovo se postiže na sledeći način: glasa se, enkriptuje se glasački listić i šalje se zajedno sa registracionim podacima na registracioni server, server vraća nepromjenjene podatke zajedno sa potpisom. Ovaj potpis je enkriptovan i jedino izborna komisija može da ga dekriptuje. Nakon toga izborna komisija dekriptuje, verifikuje, čuva i broji glasačke listiće. Na kraju izbornog procesa ona i objavljuje zvanične rezultate. Posmatrači su zaduženi da cijeli proces protekne kako je propisano.

SAVE arhitektura podrazumjeva da svi moduli imaju najbolje poznate enkripcione algoritme. Sigurnost i pouzdanost ove arhitekture čini njegova modularna struktura. Pored toga primarna osobina SAVE-a je nezavisnost koda i nezavisnost od platforme.

Pretopostavimo da ima n modula u svakoj od m faza, $M_{n,m}$, i svaki ima vjerovatnoću greške od $F_{n,m}$, i vjerovatnoću napada od $A_{n,m}$. Vjerovatnoća da sistem nije imao grešku u fazi $M_{n,m}$ je $1 - F_{n,m}$, dok vjeravatnoća da sistem nije pretrpio napad u ovoj fazi je $1 - A_{n,m}$. Vjerovatnoća greške cijelog sistema sa ovim parametrima je:

$$F = 1 - \prod_{m_1, m_2, \dots, m_n} (1 - F_{n,m})\,(1 - A_{n,m})$$

Ipak, SAVE je sistem glasanja koji zahtjeva da glas prođe kroz t faza da bi se dobio validan rezultat. Svaki modul određuje da li je iz prethodnog modula dobijen validan rezultat. Za svaki

broj grešaka f postoji $\binom{n}{f}$ mogućih kombinacija grešaka u različitim modulima. Vjerovatnoća greške sistema sa ovom pretpostavkom iznosi:

$$F = 1 - \sum_{u=t}^{n} \binom{n}{u} \prod_{u} (1 - F_{n,m})\,(1 - A_{n,m})$$

U ovom izbornom sistemu postoji jedna i samo jedna putanja glasa između glasača i komisije. Svaki dio ovog sistema ima vjerovatnoću greške i svaka komunikacija između njih ima vjerovatnoću da bude ugrožena. Dakle mora se dodati i vjerovatnoća da dođe do greške u komunikacijama (f_{comm}), pa ukupna vjerovatnoća greške sistema iznosi:

$$F = 1 - (1 - f_{comm}) \sum_{u=t}^{n} \binom{n}{u} \prod_{u} (1 - F_{n,m})\,(1 - A_{n,m})$$

SAVE arhitekturu imaju implementirane mnoge velike kompanije i univerziteti jer postoji velika mogućnost brzog i lakog usavršavanja i proširenja ovog sistema.

Optički skeneri u glasačkim sistemima

Glasanje je kompleksan sistem koji ima stroge zahtjeve i ograničenja. U Sjedinjenim Američkim Državama trenutno se koriste tri vrste glasanja: ručno brojenje listića, bušene kartice i optički skeneri. Bušene kartice su se pojavile 1960. godine, dok su se optički skeniri pojavili u devedesetim godinama prošlog vijeka. Bušene kartice traže od glasača da napravi rupu pored kandidatovog imena. To je i glavni problem kod ovih kartica jer rupa ne mora da bude na pravom mjestu i to otežava u prepoznavanju validnog glasa.

Optički skeneri zahtjevaju od glasača ili da spoji dvije tačke ili da popuni polje. Takođe postoje i dva tipa brojenja glasova: centralno i na biračkom mjestu. U centralnom tipu, glas se prosleđuje centralnoj lokaciji gdje se on skenira, obrađuje i broji. U drugom tipu glas se obrađuje direktno na biračkom mjestu i vraća povratnu informaciju glasaču. U ovom tipu glasanja, glasač može dobiti informaciju da li je glas prepoznat i da li je došlo do greške u glasanju. Ukoliko je došlo do neke greške glasač ima izbor da opet glasa. Iz ovog razloga obrađivanje i brojenje glasova na biračkom mjestu ima prednosti.

Pored ovih postoje i DRE mašine koje imaju ekran osjetljivim na dodir i one istog momenta daju povratnu informaciju. Da bi glasač dobio neku verifikaciju koriste se VVPAT (Voter Verifiable Paper Trail) mašine koje glasaču izdaju papirnu potvrdu njegovog glasa. Glasač ima izbor da potvrdi ili da otkaže glas. Ako glasač potvrdi glas, papirna potvrda se ubaca u zapečaćenju kutiju.

Da bi uvjerili glasače da svaki dio sistema radi kako treba potrebno je zadovoljiti uslove glasačkog sistema koji se zove E2E (end - to - end). E2E daje glasačima sigurnost da su se njihovi glasovi skenirali, obradili kako treba kao i da su se pravilno prebrojali. Dakle, glasačima se garantuje sigurnost da je svaki korak odrađen valjano. Takođe, E2E glasanje garantuje i privatnost, tj. da ne može utvrditi koji glas pripada kom glasaču.

Postoji nekoliko E2E šema kao što su SureVote, Pret-a-Voter, Scratch&Vote, Punchscan, Scantegrity i ThreeBallot. Ove šeme više nijesu pouzdane i vremenom su pronađeni razni napadi da se razbiju. Iz tog razloga glavna preokupacija u ovom poglavlju biće Scantegrity II šema.

Prije nego što opišemo Scantegrity II šemu opisaćemo šeme na koje se on nadovezuje.

Pret-a-Voter

Pret-a-Voter razdvaja glasački listić u dva dijela. Na lijevoj strani su imena kanditata a na desnoj su praznine koje glasač popunjava i koje predstavljaju njegov izbor. Nakon glasanja glasač razdvaja listić na dva dijela, desni dio ubaca u glasačku kutiju dok lijevi zadržava za sebe. Na desnoj strani listića postoji kod koji na jedinstven način označava raspored kandidata.

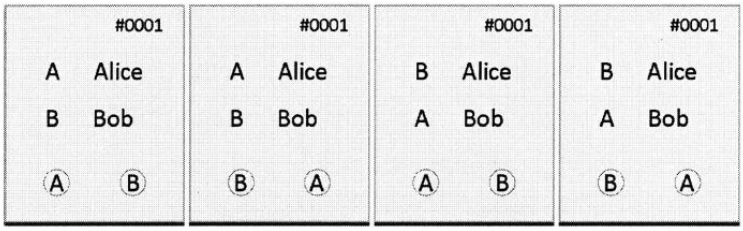
Scratch&Vote

Scratch&Vote je sličan kao Pret-a-Voter, na lijevoj strani se nalazi lista kandidata dok na desnoj mjesta za zaokruživanje. Razlika je u tome što se na desnoj strani nalazi barcode i površina za grebanje. Kada glasač glasa prvo popuni listić i podijeli ga na dva dijela. Nakon toga glasač predaje desni dio listića izbornoj komisiju koja pregleda da li je površina za grebanje netaknuta. Ukoliko je netaknuta ta površina se skine i glasač skenira barcode. Ukoliko je sve u redu glasač ubaca markirani listić dok lijevi dio zadržava za sebe.

Punchscan

U Punchscan šemi glasački listić se sastoji iz dva dijela, gornjeg i donjeg. Gornji dio sadrži imena glasača sa kodom (brojem ili slovom) pored imena glasača. Donji dio mora da ima sve kodove kao gornji dio ali u naizmjeničnom poretku. Pored ovoga glasački listić ima i drugu stranu koja sadrži samo donji dio. Dio koji se poklapa na prvoj strani ima rupu.

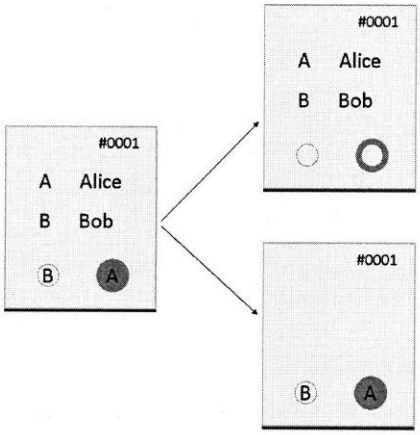
Na slici 1 prikazani su mogući tipovi glasačkog listića ukoliko je izbor između Alise i Boba.



Slika 1.

Da bi glasao glasač mora da nađe kod pored svog kandidata i da taj kod označi na donjem dijelu glasačkog listića. Na ovaj način glasač markira i prvu i drugu stranu. Slika 2

prikazuje glasački listić ukoliko glasač glasa za Alisu. Lijevi dio predstavlja listić ukoliko su prva i druga strana zajedno dok drugi dio predstavlja razdvojene.

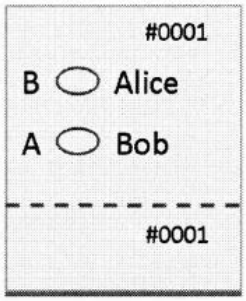


Slika 2.

Glasač sam bira koju stranu glasačkog listića zadržava za sebe a koju ubacuje u glasačku kutiju.

Scantegrity

Scantegrity je šema koja ima značajna poboljšana u odnosu na Punchscan, jer ona kombinuje nasumičnost glasačkih listića iz dva u jedan listić. Glasački listić izgleda slično kao kod Punchscan samo što se kod nalazi pored imena i raspoređen je u naizmjeničnom poretku. Slika 3 prikazuje kako izgleda glasački listić u Scantegrity šemi.



Slika 3.

Da bi glasao za kandidata glasač markira polje pored kandidata i skenira na optičkom skeniru gornji dio glasačkog listića. Ukoliko je skeniranje uspješno prošlo, glasač jedinstveni kod

koji je pored imena njegovog kandidata zapisuje na donji dio listića. Gornji dio listića ubacuje u glasačku kutiju dok donji dio zadržava za sebe. Na kraju izbornog dana objavljuju se lista glasačkih listića, serijski broj i kod listića. Na osnovu ove liste glasač može da provjeri da li je njegov glas regularno upisan. Ukoliko nije, glasač može da se žali. Ako uloži žalbu na svoj izbor dolazi do narušavanja privatnosti glasača, jer tom prilikom glasač mora da otkrije svoj izbor glasačkoj komisiji.

TreeBallot

ThreeBallot je jedinstveni E2E glasački sistem koji ne koristi nikakvu kriptografiju. Svaki glasač dobija ,,višestruki glasački listić“ koji se sastoji od tri standardna glasačka listića i svaki od njih ima jedinstveni identifikator. Da bi glasao za svog kandidata glasač markira praznine pored imena svog kandidata na tačno dva od tri glasačka listića i na tačno jednom glasačkom listiću glasač markira kandidate koje neće da glasa. Nakon toga glasač skenira sva tri glasačka listića i skener javlja da li su listići markirani kako treba. Ukoliko je sve u redu glasač može da izabere jedan od tri listića kao dokaz o glasanju i dobija kopiju tog listića.

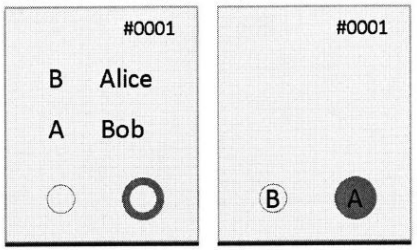
Na kraju izbornog dana objavljuju se svi glasački listići i glasač može da provjeri da li su njegovi glasovi validno izbrojani.

Napadi na pomenute izborne šeme

Jedan od najpoznatih napada na E2E šeme jeste da napadač slučajnim izborom objavi listu naizmjeničnih glasova i primora glasače da dođu da se žale zbog neprepoznavanja njihovih glasova.

U nekim slučajevima je moguće i primorati glasače da glasaju za određenog kandidata. Na sledećem primjeru vidjećemo napad na Punchscan šemu. U ovom primjeru izbori se odvijaju između dva kandidata Alise i Boba.

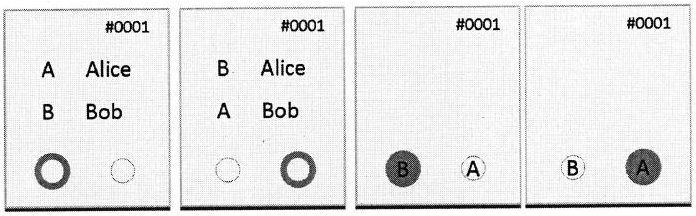
Pretpostavimo da napadač favorizuje Alisu. Da bi primorao glasača da glasa za Alisu napadaču je potrebno da glasač ne smije imati ni jedan tip glasačkog listića prikazanog na slici 4.



Slika 4.

Ako glasač ima glasačke listiće tipa 1, 2 i 3 prikazanih na slici 1, on može glasati kako želi ako za tip 1 ubaci ili gornju ili donju stranu (gornja i donja strana glasačkog listića na slici 1 nemaju isti raspored kao na slici 4, pa glasač nije u mogućnosti da donese listiće kao na slici 4), ako za tip 2 ubaci gornju stranu (da ne bi donio glasački listić sa slike 4) i ako za tip 3 ubaci donju stranu (takođe da ne bi donio glasački listić sa slike 4). Ako glasač dobije tip 4 on mora glasati za Alisu da bi donio jednu od strana prikazanih na slici 4. Dakle sa vjerovatnoćom 0,25 glasač će biti primoran da glasa sa Alisu.

Pored ovoga glasač se može natjerati da glasa Alisu sa vjerovatnoćom 0,5. Od glasača se traži da donese jednu stranu glasačkog listića kao na slici 5, za razliku od prošlog primjera gdje nije smio da donese glasački listić kao na slici 4.



Slika 5.

Ako glasač dobije tip glasačkog listića 2 ili 4 sa slike 1, ubaca u kutiju donju stranu. Glasač je glasao za Boba i napadaču je donio tip 1 sa slike 5 (ako je glasački listić tipa 2 sa slike 1) ili tip 2 sa slike 5 (ako je glasački listić tipa 4 sa slike 1). Ukoliko glasač dobije tip listića 1 ili 3 sa slike 1 glasač mora donjeti neki tip sa slike 5 i zbog toga mora glasati za Alisu. Ako bi glasač glasao za Boba na tipovima 1 i 3 glasačkih listića sa slike 1 onda glasač ne bi bio u mogućnosti da donese ni jedan tip glasačkog listića sa slike 5 i zbog toga mora glasati za Alisu. Na ovaj način se glasač tjera da glasa sa Alisu sa vjerovatnoćom 0.5.

Zbog svih ovih propusta napravljena je nova glasačka šema Scantegrity II, koja je otporna na ovakve napade.

Scantegrity II

Scantegrity II je E2E sistem elektronskog glasanja za optičke skenere koji omogućava svakom glasaču da provjeri da li je njegov glas ispravno prepoznat, verifikovan i prebrojan. Glasački listić kod Scantegrity II je sličan kao i kod ostalih sistema koji koriste optičko glasanje, samo što još ima i nevidljivi znak koji omogućava glasaču da dobije privatni dokaz njegovog glasa.

Glavne prednosti Scantegrity II sastoje se od sledećh stavki:

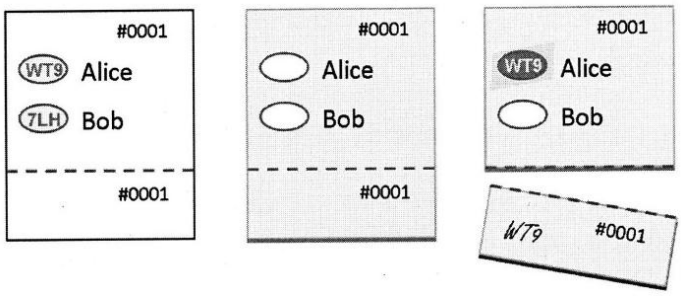
- Kompatibilan sa optičim skenerima.
- Prepoznatljivi glasački listići. Glasač zaokružuje glas pored imena na glasačkom listiću.
- Otporan na naizmjenične napade.

Izborna procedura se sastoji od sledećih koraka:

- Glasač se prijavljuje i provjerava se njegova vjerodostojnost.
- Da bi označio koga glasa glasač skida zaštitni sloj i otkriva kod pored imena svog kandidata.
- Ukoliko želi, glasač može da zapiše kod koji se nalazi pored imena svog kandidata, i da provjeri svoj glas u izbornoj verifikaciji.
- Glasač odvaja ,, račun“ od glavnog glasačkog listića.
- Skenira se optičkim skenerom glasački listić. Ukoliko je otkriveno više kodova, glasački listić se smatra nevalidnim.
- Kada se izbori završe objavljuje se lista kodova i glasova. Glasač može da provjeri da li je njegov glas prebrojan pravilno.

Svaki glasački listić ima različit jedinstveni broj, ID. ID može da izgleda kao ,, MA-2011-05-04-123456789“. U ovom radu koristićemo ID koji se sastoji od četiri cifre.

Glasački listić se sastoji od liste kandidatksih imena, i pored svakog imena se nalazi kod za optičke skenere koji je prekriven zaštitnim slojem. Na slici 6 (lijeva) prikazan je glasački listić sa ID 0001 na kome se nalaze dva kandidata Alisa i Bob. Prije nego što se glasa, svi kodovi koji se nalaze pored imena se sakriju (srednja). Na slici 6 (desno) ukoliko glasač glasa za Alisu on otkrije kod pored njenog imena i taj isti kod zapiše na donji dio glasačkog listića. Račun, donji dio glasačkog listića, sadrži takođe ID glasačkog listića.



Slika 6.

Kod za potvrdu mora da zadovoljava sledeće osobine:

- Mora da bude jedinstven na svakom glasačkom listiću.
- Mora da bude slučajan.
- Mora da bude sakriven pored kandidatovog imena osim ukoliko glasač glasa za njega.
- Potrebno je eliminisati cifre i brojeve koji su vizuelno slični (npr. 1 i I, ili 0 i O).

Neka je N broj kandidata a B broj glasačkih listića. Prije izbora generiše se naizmjenično N * B kodova i tabela:

- $P \coloneqq (p_i)_{B \cdot N}$. Tabela P sadrži sve generisane kodove. Kodovi su grupisani po ID-u glasačkog listića. Kod za kandidata k na glasačkom listiću j je $p_{(N(j-1)+k)}$. Tabela P se generiše zbog štampanja glasačkih listića i za generisanje tabele Q. P se javno ne objavljuje.
- $Q \coloneqq (q)_{B \cdot N}$. Tabela Q sadrži sve kodove iz tabele koji su nasumično permutovani za svaki pojedinačni glasački listić. Za svaki glasački listić j kodovi $p_{(N(j-1)+1)}, \dots, p_{(N(j-1)+k)}$ su permutovani u kodove $q_{(N(j-1)+1)}, \dots, q_{(N(j-1)+k)}$. Tabela Q se javno objavljuje.
- $R \coloneqq (r)_{B \cdot N \cdot 3}$. Tabela R ima dvije kolone koje sadrže sve kodove iz tabele P kao i indikator. Prva kolona je permutacija kodova iz tabele Q. Indikator se postavlja u post izbornom procesu, ako je kod otkriven na glasačkom listiću. Treća kolona su pokazivači ka tabeli S. Tabela R se takođe javno objavljuje.
- $S \coloneqq (s)_{B \cdot N}$. U tabeli S svaki red odgovara kodu iz tabele Q. Kodovi su grupisani po kandidatima. Tabela S se javno objavljuje.

Nakon što se izbori završe izborna komisija objavljuje table Q, R i S. Tabela P ostaje sakrivena i ona služi da se kod koji je skenirao optički skener poveže sa kandidatom. Izborna komisija objavljuje tabelu Q sa kodovima koji odgovaraju skeniranim kodovima kao i indikatore u tabelama R i S koji takođe odgovaraju skeniranim kodovima. Za svaki red u tabeli R, izborna komisija objavljuje ili Q - pokazavač ili S pokazivač, koji se biraju nasumično.

Nakon što se rezultati objave, glasač koji ima zapisan kod može pogledati da li ID njegovog glasačkog listića odgovara kodu koji je objavljen. Glasač provjerava da li je u redu koji odgovara njegovom ID-u nalazi samo jedan pravi kod. Ukoliko se pravi kod ne nalazi u odgovarajućem redu glasač treba da uloži žalbu.

Na kraju izbornog procesa potrebno je provjeriti da li je jednak broj glasova na kraju prebrojano sa brojem glasača izašlih na izbore, kao i da li je broj svih indikatora u tabeli R jednak broju svih indikatora u tabeli S. Ovo može da provjeri svaki učesnik izbora.

U sljedećem primjeru biće opisan Scantegrity II u izbornoj trci izmedju tri kandidata: Alise, Boba i Karla. Pretpostavimo da su u primjeru glasovi 0001 i 0003 pripali Alisi, 0002 Karlu, 0005 Bobu, dok glas 0004 je potrebno revidirati.

ID	Alice	Bob	Carl
0001	WT9	7LH	JNC
0002	KMT	TC3	J3K
0003	CH7	3TW	9JH
0004	WJL	KWK	H7T
0005	M39	LTM	HNN

Tabela P

ID			
0001	7LH	WT9	JNC
0002	J3K	TC3	KMT
0003	9JH	CH7	3TW
0004	KWK	H7T	WJL
0005	M39	HNN	LTM

Tabela Q

Indikator	Q - Pokazivač	S - Pokazivač
	(0005; 1)	(2; 1)
	(0003; 3)	(4; 2)
	(0002; 1)	(4; 3)
	(0001; 3)	(3; 3)
	(0001; 2)	(4; 1)
	(0005; 3)	(3; 2)
	(0004; 2)	(5; 3)
	(0003; 1)	(2; 3)
	(0004; 3)	(3; 1)
	(0002; 3)	(1; 1)
	(0001; 1)	(2; 2)
	(0002; 2)	(5; 2)
	(0004; 1)	(1; 2)
	(0003; 2)	(5; 1)
	(0005; 2)	(1; 3)

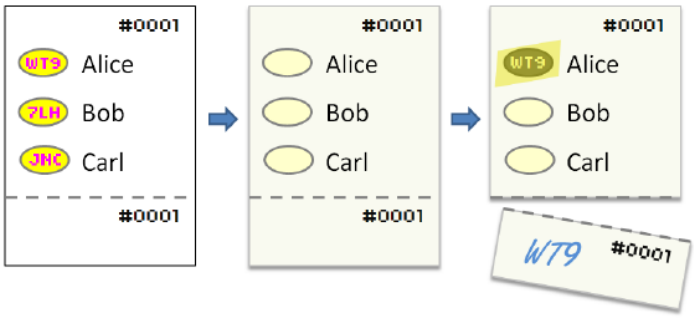
Tabela R

Alice	Bob	Carl

Tabela S

Slika 8.

Na slici 8 prikazane su tabele P, Q, R i S koje su generisane prije nego što je započeo izborni proces. Tabela P se ne objavljuje dok se tabele Q, R i S objavljuju nakon završenih izbora ali ne sa svim informacijama.



Slika 7.

Slika 7 je slična slici 6 samo što u ovom slučaju izbori se odvijaju između tri kandidata. Na njoj je prikazano kako izgleda glasački listić ukoliko glasač glasa za Alisu.

Ukoliko glasač sa glasačkim listićem 0002 hoće da glasa za Karla on mora otkriti kod J3K. Ovaj kod se nalazi u drugom redu a prvoj koloni u tabeli Q. Odgovarajući red u tabeli R je treći, koji sadrži (0002; 1) i (4; 3). (0002; 1) je pokazivač na tabelu Q za glasački listić 0002 i prvu kolonu, tj. kod J3K. (4; 3) odgovara četvrtom redu i trećoj koloni u tabeli S što odgovara i glasu za Karlu. U tabelu S se postavlja indikator koji odgovara trećem redu u tabeli R.

ID			
0001		WT9	
0002	J3K		
0003		CH7	
0004	KWK	H7T	WJL
0005			LTM

Tabela Q

Indikator	Q - Pokazivač	S - Pokazivač
		(2; 1)
	(0003; 3)	
•		(4; 3)
		(3; 3)
•	(0001; 2)	
•	(0005; 3)	
	(0004; 2)	(5; 3)
		(2; 3)
	(0004; 3)	(3; 1)
	(0002; 3)	
	(0001; 1)	
	(0002; 2)	
	(0004; 1)	(1; 2)
•		(5; 1)
	(0005; 2)	(1; 3)

Tabela R

Alice	Bob	Carl
	•	
•		•
•		

Tabela S

Slika 9.

Na slici 9 prikazane su tablele Q, R i S koje su objavljene nokon izbora. Za svaki red u tabeli R ili je Q - pokazivač ili S - pokazivač objavljen. Možemo primjetiti da za glasački listić 0004 u tabeli R su ,,objavljeni" podaci jer je ovaj glasa izabran za revidiranje.

Postoji pet razloga zbog kojih može doći do žalbi:

1. Greška glasača kada je upisivao kod na račun.
2. Otkriveni kod odgovara glasu glasača ali glasač želi da poremeti izborni rezultat.
3. Došlo je do greške tokom skeniranja.
4. Došlo je do prevare u procesu. Napadač je uspio da tokom izbornog procesa podmetne pogrešne kodove.
5. Napadač pokušava da prekrije prevaru tako što pogađa naizmjenične kodove koji nisu generisani kodovi.

Kada glasač uloži žalbu izborna komisija provjera da li kod koji je je donio glasač pripada tom glasačkom listiću. Ukoliko ne pripada smatra se da je žalba neosnovana i ona se odbacuje. Ukoliko taj kod pripada tom glasačkom listiću smatra se da je glasač donio pravi kod, jer glasač ne zna koji sve kodovi postoje na tom glasačkom listiću. Ako je glasač otkrio više kodova na glasačkom listiću, glasački listić je već proglašen nevalidnim prilikom skeniranja pa se žalba takođe odbacuje. Nakon što izborna komisija utvrdi da je žalba validna, u tabeli R traži se pokazivač ka tabeli Q koji odgovara kodu koji je donio glasač. U istom redu postavlja se indikator. Nakon toga gledajući S - pokazivač postavlja se indikator u tabelu S, i otkriva se nasumičnom metodom S ili Q pokazivač.

Pokazali smo da Scantegrity II ima značajna poboljšana u odnosu na pomenute sisteme sa optičkim glasanjem. Ipak Scantegrity II je ranjiv ukoliko napadač uspije da na neki način izbriše neke glasačke listiće. Ukoliko se ovo dogodi glasač će moći da vidi prevaru ali neće moći da da dokaz izbornoj komisiji.

Kodovi za potvrdu treba da budu jedinstveni. Ako se kodovi nisu ispravno generisali, tj. postoji kod koji se pojavljuje na više glasačkih listića onda nije moguće da glasač provjeri svoj glas.

Scantegrity II čuva privatnost glasača, i napadač ne može da otkrije kako je koji glasač glasao. Pored ovoga Scantegrity II je takođe imun na uticaj na glasače, jer prije nego što glasač glasa svi kodovi su sakriveni i pored ID jedino što se može vidjeti je lista imena kandidata. Svaki otkriveni kod jednako može da pripada svakom kandidatu i zbog toga kod na računu se ne može povezati sa izborom glasača.

Simulacija Scantegrity II

Za potrebe ovog rada napravljenja je web aplikacija koja simulira Scantegrity II algoritam. Programski jezici koji su korišćeni za izradu aplikacije su PHP i JavaScript, i MySQL kao sistem za upravljanje bazama podataka.

Šema baze podataka sastoji se od entiteta: izbori (koji sadrži listu svih izbora generisanih u aplikaciji) i kandidati (koji sadrži sve kandidate svih izbora). Šema takođe sadrži i entitete P_izbor, Q_izbor, R_izbor i S_izbor. Riječ ,,izbor" predstavlja jedinstveni identifikator izbora, dakle svaki izbor ima svoje entitete posebne P, Q, R i S.

Pošto se Scantegrity II zasniva na slučajno generisanim kodovima, za njihovo generisanje koristila se PHP funkcija koja se zasniva na Mersenne twister, algoritmu koji je uspješno završio mnoge statističke testove za slučajne brojeve uključujući i ,, Diehard tests".

Slika 10.

Na slici 10 prikazana je početna stranica aplikacije. Meni aplikacije ima sledeće stravke:

- Početna strana.
- Pregled izbora. Na ovoj stranici prikazani su izbori koji su generisani u aplikaciji. Ovdje se može vidjeti izborno pitanje, ukupan broj prijavljenih glasača i lista

kandidata sa informacijama koliko je koji kandidat osvojio glasova (brojno i procentualno). Postoji i mogućnost promjene aktivnih izbora. Stavke menija Aktivni izbori, Glasanje i Verifikacija odnose se samo na aktivne izbore.

- Novi izbori. Pomoću ove stranice kreiraju se novi izbori. Unesu se naziv izbora, izborno pitanje, broj glasača i imena kandidata, a nakon toga pritisne se dugme ,,Napravi" koje generiše tabele P, Q, R i S.
- Aktivni izbori. Na ovoj stranici mogu se vidjeti pomenute tabele. Postoji mogućnost prikaza ovih tabela u javnom i privatnom obliku, kao i njihova selekcija po glasačkom listiću i kodu.
- Glasanje. Ova stranica je napravljena kao simulacija procesa glasanja. Za Scantegrity II potrebno je da glasač dobije nasumični glasački listić. Svaki glasački listić ima svoj jedinstveni identifikator i taj broj je potrebno unijeti u polje Glasački listić. Kada se unese ovaj broj, pored imena svog kandidata glasač pritisne na prikazano polje. Nakon toga aplikacija provjerava da li je identifikator glasačkog listića validan i ako jeste nudi mogućnost glasaču da potvrdi glasanje. Kada glasač potvrdi da želi da glasa za željenog kandidata on dobija poruku, koja sadrži ID glasačkog listića i kod koji se nalazio pored imena glasača.
- Verifikacija. Na ovoj stranici glasaču se nudi mogućnost da provjeri da li je njegov glas validno prebrojan. Kada unese ID glasačkog listića glasaču se prikazuje kod koji bi ukoliko je sve prošlo u redu trebalo da bude isti kao što je dobio nakon završenih izbora.

Coercion-Resistant Electronic Elections (Elektronsko glasanje otporno na prinudno glasanje)

U tradicionalnim sistemima za glasanje, glasač se indetifikuje u vrijeme direktong glasanja. Ovo se postiže pomoću digitalnog potpisa ili nekog protokola za potvrdu indetiteta. Glavna ideja koja stoji iza ovog algoritma jeste da indetitet glasača ostane sakriven tokom procesa glasanja. Kada glasač glasa, on sadrži skrivene akreditive. Ovo podrazumjeva da svaki glasač ima vrijednost σ koja je jedinstvena za svakog glasača. Da bi se uvjerili u vjerodostojnost glasanja, evidicioni organ τ odrađuje poređenje između skrivene akreditive i liste L koja sadrži kriptovane akreditive iz zvaničnog registra glasača R.

Putem slijepog poređenja moguće je vidjeti da li je akreditiva u listi L ili nije bez znanja koja akreditiva pripada kom glasaču.

Ovaj sistem glasanja se sastoji od sledećih skupova entiteta:

1. Registri: $R = \{R_1, R_2, R_3, \dots, R_{nR}\}$ je skup entiteta koji su zaduženi za izdavanje akreditiva glasačima.
2. Izborne komisije: $T = \{T_1, T_2, T_3, \dots, T_{nT}\}$, autoritet koji obrađuje i broji glasačke listiće kao i objavljuje izborni rezultat.
3. Glasači: $V = \{V_1, V_2, V_3, \dots, V_{nV}\}$, entiteti koji imaju pravo glasanja dato od autoriteta R.

Glasačka kutija koju označavamo sa *BB* je memorija na koju svi učesnici izbora imaju pravo pisanja ali nemaju pravo brisanja.

Neka je skup $C = \{C_1, C_2, C_3, \dots, C_{nC}\}$ koji odgovara izborima birača (npr. lista partija ili kandidata). Skup C možemo predstaviti kao skup prirodnih brojeva {1, 2, 3, … , n_C} i radi lakše oznake samo n_C. Neka je X uredjeni skup prirodnih brojeva x_1, x_2, x_3, …, x_{nC} gdje x_j označava broj glasava za određeni izbor.

Funkcije koji čine izborni sistem su sledeće:

- Registracija: Funkcija (SK_R, i, k_1)→ (sk_i, pk_i), gdje je SK_R privatni registracioni ključ, i je glasač a k_1 bezbjednosti parametar. Izlaz je uređena dvojka (sk_i, pk_i) koja predstavlja ključ (privatni i javni).
- Glasanje: Funkcija (sk, PK_T, n_C, β, k_2) → glasački listić. Ulazini parametri su privatni ključ, javni ključ dat od autoriteta T (izborna komisija), lista kandidata n_C, izbor glasača β, k_2 je bezbjedosni parametar. Izlaz je glasački listić.
- Brojenje: Funkcija (SK_T, BB, n_C, $\{\mathrm{pk_i}\}_{i=1}^{nV}$, k_3) →(X,P). Ulazni parametri su privatni ključ autoriteta T, glasačka kutija BB, pun sadržaj liste kandidata n_C, sve javne

ključeve i bezbjednosni parametar k_3. Izlaz je uređena dvojka X (rezultati glasanja) i P kao dokaz o regularnosti brojenja.

- Verifikacija: Funkcija (PK_T, BB, n_C, X, P) →(0, 1) koja verifikuje proces glasanja i vraća 1 ako je glasanje u redu a 0 ako nije.

A je oznaka za napadača. Šemu glasanja označavamo sa ES i ovo je skup koji sadrži navedene funkcije ES={registracija, glasanje, brojenje, verifikacija}.

Osobine koje glasački proces mora da zadovolji su ispravnost, proveljivost i otpornost od prisile.

Prvo razmotrimo osobinu ispravnosti. Napadač ne može da poništi, preglasa ili zamjeni glas pravog glasača, kao i ne može da od jednog pravog glasa napravi više glasova. Slijedeći eksperiment karakteriše ispravnost (ako je rezultat 1 A je uspio da falsifikuje izbore):

$\boldsymbol{EXP}_{ES,A}^{ispravnost}(k_1, k_2, k_3, n_C, n_V)$
$\{(sk_i, pk_i) \leftarrow registracija\ (SK_R, i, k_2)_{i=1}^{n_V}\}$ - glasači se registruju
$V \leftarrow A\ (\{pk_i\}_{i=1}^{n_V})$ - napadač korumpira glasače
$\{\beta_i\}_{i\notin V} \leftarrow A$ - napadač bira glas za poštnenog glasača
$BB \leftarrow \{glasanje\ (sk_i, PK_T, n_C, \beta_i, k_2)\}_{i\notin V}$ - glasač glasa
$(X, P) \leftarrow (SK_T, BB, n_C, \{pk_i\}_{i=1}^{nV}, k_3)$ - broje se glasovi svih glasača
$BB \leftarrow A(\text{pravi glasovi}, BB)$ - napadač postavlja svoje glasove
$(X1, P1) \leftarrow (SK_T, BB, n_C, \{pk_i\}_{i=1}^{nV}, k_3)$ - broje se svi glasovi
$ako\ je\ verifikacija(\mathrm{PK}_T, \mathrm{BB}, \mathrm{n}_C, \mathrm{X1}, \mathrm{P1}) = 1$ i $(\{\beta_i\} \notin X1\ ili\ |X1| - |X| > |V|)$
$onda\ output = 1\ inače\ output = 0$

Slijedeća osobina koju razmatramo je provjerljivost. Ukoliko napadač A promijeni neki ključ kod organa T ne možemo uvijek biti sugurni da je brojenje glasova odrađeno tačno. Provjerljivost je osobina da svaki učesnik u izbornom procesu može da provjeri da li je X pravilno izračunat, i ako nije da otkrije nedostatke u T prilikom brojenja glasova. Slijedeći eksperiment karateriše provjerljivost.

$\boldsymbol{EXP}_{ES,A}^{provjerljivost}(k_1, k_2, k_3, n_C, n_V)$
$\{(sk_i, pk_i) \leftarrow registracija\ (SK_R, i, k_2)_{i=1}^{n_V}\}$ - glasači se registruju
$(BB, X, P) \leftarrow A(SK_T, \{(sk_i, pk_i)\}_{i=1}^{n_V})$ - napadač korumpira izbore
$(X1, P1) \leftarrow (SK_T, BB, n_C, \{pk_i\}_{i=1}^{nV}, k_3)$ - broje se svi glasovi
$ako\ X \neq X1\ i\ verifikacija(\mathrm{PK}_T, \mathrm{BB}, \mathrm{n}_C, \mathrm{X1}, \mathrm{P1}) = 1\ onda\ output = 1\ inače\ output = 0$

Treća osobina koju razmatramo je otpornost od prisile. Otpornost od prisile je nadogradnja jedne od najbitnih osobina izbora, privatnosti. Privatnost u izbornom procesu jeste da suparnik ne može da utiče na izbor glasača. Otpornost od prisile je jača osobina od privatnosti, gdje se podrazumjeva da će suparnik pokušati da utiče na glasača. Slijedeći eksperiment karakteriše otpornost od prisile. U ovom eksperimentu postoji promjenjiva b, koja uzima vrijednosti 0 ili 1. Ako je $b = 0$ onda glasač glasa β i izbjegava prinudu.

$\boldsymbol{EXP}_{ES,A}^{otpornost\ od\ prisile}(k_1, k_2, k_3, n_C, n_V)$
$V \leftarrow A(\text{glasači})$ - napadač korumpira glasače
$\{(sk_i, pk_i) \leftarrow registracija\ (SK_R, i, k_2)_{i=1}^{n_V}\}$ - glasači se registruju
$(j, \beta) \leftarrow A(bira\ metu\ i\ glas)$
$ako\ je\ |V| \neq n_A\ ili\ j \notin \{1, 2, \dots, n_V\}\ ili\ B \notin \{1, 2, \dots, n_V\}\ onda\ output = 0$
$b \in \{0,1\}$ - slučajno se izabere 0 ili 1
$ako\ je\ b = 0\ onda$ - glasač izbjegava prinudu
$BB \leftarrow glasanje\ (sk_i, PK_T, n_C, \beta, k_2)$
inače $sk1 \leftarrow sk$ - glasač je prinudno glasao
$BB \leftarrow glasanje\ (sk_{i,i\neq j\ i\notin V}, PK_T, n_C, \beta 1, k_2)$ - glasa pošten glasač
$BB \leftarrow A(sk1, BB)$ - napadač mjenja BB
$(X, P) \leftarrow (SK_T, BB, n_C, \{pk_i\}_{i=1}^{nV}, k_3)$ - broje se svi glasovi
$b1 \leftarrow A(X, P, b)$ - A pogađa b
$ako\ je\ b = b1\ onda\ output = 1\ inače\ output = 0$

Šamirovo tajno dijeljenje

Da bi se objasnio izborni protokol koji ću prikazati u ovom radu, prvo je neophodno objasniti algoritam Šamirovog tajnog djeljenja. Ovo je algoritam gdje se tajna dijeli na dijelove, i samo neki dijelovi ili svi su potrebni za rekonstrukciju tajne.

Formalno naš cilj je da se neki podaci D podjele na n dijelova D_1, D_2, D_3,..., D_n gdje su ispunjeni sledeći uslovi:

1. Znanje k ili više djelova čini lako dešifrovanje D.
2. Znanje k-1 ili manje dijelova čini veoma teško za dešifrovanje D.

Ovaj algoritam se označava sa (k, n), gdje je k broj dijelova potrebnih za rekonstrukciju poruke. Ako je k=n onda su potrebni svi dijelovi da se rekonstruiše D.

Ideja koju je Šamir predložio zasniva se na tome da su potebne dvije tačke da se definiše prava, tri parabola i td. Potrebno je k-1 tačaka da se definiše polinom k-tog stepena.

Slučajno se izabere k-1 koeficjenata $a_1, a_2, \dots, a_{k-1}$, i neka je $a_0 = S$(tajna). Napravi se polinom $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$. Konstruiše se n tačaka (i, f(i)), i = 1, 2, 3, … , n. Svakom učesniku se da po jedna tačka, i samo k učesnika polinomnom interpolacijom mogu rekostruisati početni polinom a samim tim i S.

Povoljnosti ovog algoritma su višestruke:

1. Veličina svakog dijela ne prelazi veličinu originalnog podatka, što je veoma povoljno pri prenosu podataka.
2. Kada je k fiksirano, D_i se može mijenjati, dodavati ili brisati bez uticaja na ostale dijelove.
3. Bezbjedost se može brzo poboljšati da se ne mijenja S, nego se samo generiše novi polinom.
4. Fleksibilan je za izbor broj k, odnosno broj učesnika potrebnih da otkriju S se lako može mijenjati.

Izborni protokol

Kriptosistem koji će se koristiti u ovom izbornom sistemu je modifikovani El Gamalov algoritam. El Gamal šemu enkripcije predložio je Taher Elgamal 1985. godine. Sigurnost El Gamalovog algoritam se bazira na težini problema računanja diskretnog logaritma.

Neka je G algebarska grupa na kojoj ćemo primjeniti El Gamalov algoritam i q generator te grupe. Javni i privatni ključ El Gamalovog algoritama je uređena dvojka (y, x), gdje je $y = g^x$ i $x \in_U Z_q$, $\in_U$ označava uniformi slučajni izbor iz skupa. Privatni ključ x može se podijeliti ka izbornoj komisiji T, koristeći (t, n_T) - Šamir tajno djeljenje gdje je $t > \frac{n_T}{2}$. Svaki član izborne komisije ima par (y_i, x_i), gdje je x_i tačka u polinomu koji se koristi u Šamirom algoritmu. Kriptovani tekst u El Gamalu na poruci $m \in G$, je oblika $(\alpha, \beta) = (my^r, g^r)$, $r \in_U Z_q$. Ovo možemo da označimo sa $E_y[m]$. Dekripcijom kriptoteksta (α, β) dobija se $m = \frac{\alpha}{\beta^x}$.

Kao što je i ranije pomenuto algoritam koji se ovdje koristi je modifikovani El Gamalov algoritam. Razlika je u tome što se generiše x_1 i x_2, i $h = g_1^{x_1} g_2^{x_2}$. Šalje se uređena trojka $(A, B, C) = (g_1^r, g_2^r, h^r m)$. Dekripcija se računa na slijedeći način $m = C\ (A^{x_1} B^{x_2})^{-1}$.

Algoritam

Podešavanje: Generišu se parovi ključeva (SK_R, PK_R) i (SK_T, PK_T). Objavljuju se PK_R i PK_T zajedno sa svim parametrima.

Registracija: Poslije dokaza o podobnosti glasača V_i, R generiše i prenosi ka V_i naizmjeničan string $\sigma_i \in_U G$, koji iznačava akreditiv glasača i ovo se predstavlja sk_i. R takođe generiše i $S_i = E_{PK_T}(\sigma_i)$ koji predstavlja pk_i. S_i se čuva na L. U ovom algoritmu smatra se da je većina u R ,,poštena", i da će za V_i dostaviti prave akreditive. Ove akreditive glasač može da koristi na više izbora.

Objava liste kandidata: R objavljuje listu kandidata C koji sadrže imena i jedinstvene indetifikator u G. R takođe objavljuje naizmjeničan indefikator ϵ.

Glasanje: V_i glasa za kandidata c_j koristeći modifikovani El Gamalov kriptotekst $(E_1^{(i)}, E_2^{(i)})$ i akreditiv σ_i. Za $a_1,\ a_2 \in_U Z_q$ važi:

$E_1^{(i)} = (\alpha_1,\ \alpha_1`,\ \beta_1) = (g_1^{a_1}, g_2^{a_1},\ c_j h^{a_1})$ i

$E_2^{(i)} = (\alpha_2,\ \alpha_2`,\ \beta_2) = (g_1^{a_2}, g_2^{a_2},\ \sigma_i h^{a_1})$.

$E_1^{(i)}$ je kriptotekst izbora glasača, dok je $E_2^{(i)}$kriptotekst akreditiva glasača.

Brojenje: Glasovi se postavljaju na BB. Brojenje glasova sastoji se od sledećih koraka:

1. T kontroliše sve kriptotekstove postavljene na BB. Svaki glas sa nevalidnim dokazom se odbacuje. Za sve preostale validne dokaze neka je A_1 skup kriptotekstova izbora glasača (E_1) a B_1 skup kriprotekstova akreditiva glasača (E_2).
2. T eliminiše duplikate. Kada se neki element ukloni iz B_1 odgovarajući element se eleminiše i iz A_1. Sa $A_1`$ i $B_1`$ označimo skup bez uklonjenih vektora. Ovim postupkom omogućavamo sigurnost da jedan izdati akreditiv odgovara jednom glasu.
3. T primjenjuje MN algoritam nad $A_1`$ i $B_1`$ koji vrši istu permutaciju ovih skupova tako da napadač ne može otkriti koji ulazni kriptotekst odgovara kojem izlaznom kriptotekstu. Rezultajuće skupove možemo označiti sa A_2 i B_2.
4. MN algoritam takođe vrši permutaciju nad listom L. Nakon ovoga T vrši poređenje između B_2 i L. T vraća skup A_3 koji sadrži kriptotekstove od A_2 koji su se poklopili u prethodnom poređenju.

5. T vrši enkripciju nad A_3, broji glasove i saopštava rezultate.

Simulacija otpornosti od prisile

U ovom poglavlju detaljnije će biti opisana osobina otpornost od prisile ovog algoritma.

Prije svega opisat ću orakle koji će se koristi u ovom algoritmu: MN, PET, DEC i OW.

- MN je orakle koji za ulazne elemente ima uređeni skup $E = \{E_1, E_2, \dots, E_d\}$ i javni ključ PK_T. Izlazni parametar je $E` = \{E`_{\pi(1)}, E`_{\pi(2)}, \dots, E`_{\pi(d)}\}$, tajna naizmjenična permutacija.
- PET ima ulazni parametar par kriptotekstova $(\mathrm{E}, \mathrm{E}`)$ a izlazni parametar je 1 ako ova dva kriptoteksta imaju iste enkriptovane tekstove a 0 ako su različiti.
- DEC ima ulazne parametre kriptotekst E i PK_T. Izlazni je odgovarajući enkriptovani tekst.
- OW ima ulazne parametre {0, 1} a izlazni je jedna od ovih vrijednosti uključujući bezbjednosni parametar k_1, k_2, k_3.

Podešavanje: Na početku simulator dobija uređenu četvorku elemenata (g_1, g_2, h_1, h_2). Ova četvorka je ili Diffie - Hellman ili slučajno izabrana. Ukoliko je sakriveni bit d=1 riječ je DH a ukoliko je d=0 radi se o slučajnoj uređenoj četvorci. Cilj simulacije jeste da se vidi o kojoj se situaciji radi. Simulator S bira dva elementa $x_1, x_2 \in_U Z_q$, i $h = g_1^{x_1} g_2^{x_2} mod\ p$. S publikuje javni ključ (g_1, g_2, h) i naizmjeničnu listu kandidata $C = \{c_i\}_{i=1}^{n_C}$, gdje je $c_i = g_1^{r_i}$ i $r_i \in_U Z_q$.

Registracija: S simulira R i generiše skup akreditiva $\{\sigma_i = g_1^{s_i}\}$ za $s_i \in_U Z_q$. Za ekriptovanu listu aktreditiva L_0, S objavljuje listu od n_V kriptotekstova.

Korupcija napdača: Napadač uzima skup V1 od n_V glasača koje želi da korumpira i glasača j kome želi da dodjeli glas β. Ako je $j \notin V - V1$ ili $\beta \notin C \cup \emptyset$ onda se simulacija prekida.

Baca se novčić: $b \in \{0,1\}$

Dodjeljuju se akreditivi: Dodjeljuju se akreditivi $\{\sigma_i\}_{i \in V1}$. Akreditiv σ je akreditiv koji pripada glasaču j. Ako je b=1 onda je $\sigma = \sigma_j$, a ako je b=0 je σ naizmjeničan string.

Simulacija poštenog glasača: Za svaki glasački listić W, simulator postavlja dva kriptoseta $(\alpha_{i,1}, \alpha_{i,1}`, \beta_{i,1})$ i $(\alpha_{i,2}, \alpha_{i,2}`, \beta_{i,2})$. Neka je A_0 skup ovih glasačkih listića. A^* su svi glasački listići gdje se akreditivi podudaraju. Simulacija glasanja se odvija tako što se za svaki glasački listić biraju dva elementa r_i i k_i tako da je:

$$\alpha_{i,1} = h_1^{r_i}, \qquad \alpha_{i,1}` = h_2^{r_i}, \qquad \beta_{i,1} = h_1^{r_i x_1} h_2^{r_i x_1} c_j$$

$$\alpha_{i,2} = h_1^{k_i}, \qquad \alpha_{i,2}` = h_2^{k_i}, \qquad \beta_{i,2} = h_1^{k_i x_1} h_2^{k_i x_1} c_j.$$

Simulacija napadača: Napadač A postavlja skup B_0 na BB.

Dekripcija glasova postavljenih od napadača: Neka je B_1 skup pravih akreditiva. Za svaki element iz skupa B_1 i za svaki akreditiv $\{\sigma_i\}_{i \in V1} \cup \sigma_j$, simulator ih dekriptuje sa svojim privatnim ključem.

Simulacija brojenja: S simulira ponašanje poštenih autoriteta. Pošto su oni većina svako odstupanje A od autoriteta brojenja može se ignorisati. Ova simulacija se sastoji od:

- **Provjera dokaza:** Neka je E_0 kombinacija skupova A_0 i B_0. S simulira brojenje i odbacuje sve nepravilne glasove. E_1 je rezultat ovog odbacivanja.
- **Eliminacija duplikata:** S simulira eliminaciju duplikata. Dobijeni skup označimo sa E_2.
- **MN aloritam:** Primjenjuje se MN algoritam na E_2 i dobija se skup E_3. S takođe vrši simulaciju upoređivanja sa L_0 i dobija se L_1.
- **Provjera akreditiva:** Primjenjuje se PET algoritam između E_3 i L_1. Ukoliko dolazi do poklapanja glasački listić se odobrava a ukoliko ne glasački listić se odbija. Neka je E_4 rezultat ove simulacije.
- **Dekripcija:** Odrađuje se dekripcija.

Zaključak

Elektronsko glasanje ima potencijala da postane najpouzdani i najsigurniji oblik glasanja. Digitalna tehnologija i kriptografija nude mogućnost da zabilježe, prenose i skladištenje glasova mnogo pouzdanije nego papir. Elektronsko glasanje omogućava lakši izborni proces za sve njegove učesnike, za glasače, kandidate, posmatrače i izborne komisije.

U svakom glasanju postoji mogućnost zloupotrebe. Bez obzira da li su se koristile kuglice, glasački listići ili nešto treće, glasanje je bilo podložno veoma maštovitim i različitim izbornim podvalama. Elektronsko glasanje nije savršeno. Ono kao i obično glasanje ima niz nedostataka. Moguće su softverske greške, bezbjedonosni propusti u kojima se pogrešno označavaju birači ili, što je najčešće, jedan broj glasova jednostavno nestane, biva obrisan ili nije na odgovarajući način zapamćen.

I pored svega elektronsko glasanje ima budućnost. Pitanje je vremena kada će ono da postane dio naše svakodnevnice. Izbori na državnom nivou u nekim državama se već odvijaju elektronskim putem. Elektronske mašine za glasanje su prvi korak. Uvođenje Interneta kao osnove za prenos i obradu glasačkih podataka vjerovatno će smanjiti broj onih koji ne glasaju. Uskoro će i upotreba Interneta biti moguća kada je riječ o glasanju. Tada će svaki čovek koji ima računar kod kuće ili u neposrednoj blizini moći da glasa na taj način. Pored toga, ovaj tip glasanja će omogućiti i državljanima koji su na privremenom boravku u drugim država da lako i bezbjedno glasaju. To će imati velikog uticaja na politiku, političare, političke partije, na načine propagande i još mnogo toga.

Literatura

[1] Ed Gerck, The Witness-Voting System, San Diego CA, 2001

[2] Ari Juels, Dario Catalano, and Markus Jakobsson, Coercion-Resistant Electronic Elections, Bedford, USA, 2005

[3] Melanie Volkamer, Evaluation of Electronic Voting: Requirements and Evaluation Procedures to Support Responsible Election Authorities, 2009

[4] Jonathan K. Hodge, Richard E Kilma, The Mathematics of Voting and Elections: A Hands-On Approach, 2000

[5] Jonathan A. Goler, Edwin J. Selker, A Secure Architecture for Voting Electronically (SAVE), 2009

[6] Jun Furukawa, Kengo Mori, Kazue Sako, An Implementation of a Mix-Net Based Network Voting Scheme and Its Use in a Private Organization, 2002

[7] Emily Shen, End-to-End Voter-Verifiable Optical-Scan Voting, 2008

[8] Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, Alan T. Sherman, Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation, 2008