KAUNO TECHNOLOGIJOS UNIVERSITETAS
MATEMATIKOS IR GAMTOS MOKSLŲ FAKULTETAS

Giedrius Bagdonas

ELEKTRONINIO BALSAVIMO SISTEMOS ANALIZĖ IR TOBULINIMAS

Baigiamasis magistro projektas

Vadovas
Lekt. Dr. Kęstutis Lukšys

KAUNAS, 2015

KAUNO TECHNOLOGIJOS UNIVERSITETAS

MATEMATIKOS IR GAMTOS MOKSLŲ FAKULTETAS

Giedrius Bagdonas

Taikomoji Matematika (studijų programos kodas 621G10003)

Baigiamojo projekto „Elektroninio Balsavimo Sistemos analizė ir tobulinimas“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

2015 m.06 mėn. 5 d.

Kaunas

Patvirtinu, kad mano, **Giedrius Bagdono,** baigiamasis darbas tema „Elektroninio Balsavimo Sistemos analizė ir tobulinimas “ yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena darbo dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymu nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

_____ _____

(studento vardas ir pavardė, įrašyti ranka) (parašas)

Bagdonas, G., „Analysis and Modification of Electronic Voting System“. *Master* thesis / supervisor Lect. dr. Kęstutis Lukšys; Kaunas University of Technology, faculty of mathematics and natural sciences, department of applied mathematics.
Kaunas, 2015. 45 pg.

Summary

In this work we analyze and modify an Electronic Voting System. This system, proposed by Cao Gang, is based on Secure Multi – Party Computations (SMC). The keystone of this system, analyzed in this paper, is the fact that voters, participating in the elections, calculate encrypted sum of votes$D + R$, here D is the sum of votes and R – random parameter, generated by service institution, by communicating with each other and sending each voter some random part of his original vote. However the actual sum of votes - D – remains unknown to any of voters or service institution. This is ensured by execution of Yao's secure multi – party protocol.

The proposed electronic voting system satisfies main requirements suggested for electronic voting systems: no one can reckon voting choice of any voters; each voter can check that his vote was not modified and counted to the final tally correctly; only eligible voters are allowed to vote. In this work we present and implement Fiat – Feige – Shamir user identification scheme, which, by using zero knowledge proofs, allows for verifier to check if provers identity is correct and he is eligible to vote. Also, an efficient solution for Yao's two millionaire problem was proposed for determination of final voting result.

Finally, we propose two solutions to solve main drawback of original electronic voting system and ensure that all ballots, cast by voters, are valid.

Turinys

1. Įvadas

Elektroninio balsavimo sistemos, leidžiančios rinkėjams balsuoti internetu šiuolaikinėje visuomenėje tampa vis populiaresnės. Pagrindinis elektroninio balsavimo privalumas – efektyvesnis ir lengviau prieinamas balsavimas (rinkėjai balsuoti gali iš bet kurio elektroninio prietaiso, turinčio prieigą prie interneto), greitesnis rinkimų rezultatų paskelbimas. Tačiau, nepaisant balsavimo internetu privalumų, dažnai susiduriama su saugumo problemomis. Pavyzdžiui, daugumoje balsavimo internetu sistemų administratoriai, tikrinantys balsuotojų tapatybę bei teisę balsuoti, turi prieigą ir prie balsuotojų balsų. Taigi, iškyla problemų dėl balsuotojų privatumo, kadangi įmanoma nustatyti rinkėjų balsavimo pasirinkimus. Be to, dažniausiai rinkėjai negali patikrinti, ar jų balsai buvo suskaičiuoti tinkamai.

Šias saugumo problemas galėtų išspręsti darbe tyrinėjama elektroninio balsavimo sistema, paremta saugiais keleto šalių skaičiavimais (Gang, 2008). Darbo pagrindinis tikslas buvo ištirti bei, pasitelkus nulinio atskleidimo įrodomus, patobulinti minėtą elektroninio balsavimo sistemą, suformuluojant metodus, leidžiančius atlikti balso tinkamumo patikrinimą. Kiti darbo uždaviniai buvo

- Suformuluoti reikalavimus, keliamus elektroninio balsavimo sistemoms;
- Sukurti programines priemones, leidžiančias ištirti nagrinėjamos elektroninio balsavimo sistemos skaičiavimų efektyvumą bei priklausomybę nuo rinkimuose dalyvaujančių balsuotojų skaičiaus;
- Ištirti, su kokiais parametrais saugu naudoti tiriamą elektroninio balsavimo sistemą;
- Rasti metodus, suderinamus su tiriama elektroninio balsavimo sistema bei tinkančius balsuotojų identifikacijai ir galutinio rinkimų rezultato nustatymui.

Baigiamojo darbo struktūra: darbo analitinėje dalyje (**2 skyrius**) apibrėžiamos elektroninio balsavimo sistemos bei joms keliami reikalavimai bei aptariamos naudojamos elektroninio balsavimo sistemos. Taip pat, aprašyti pagrindiniai darbe naudojami matematiniai metodai: nulinio atskleidimo įrodymai bei dviejų milijonierių problema. Metodologinėje dalyje (**3 skyrius**) aprašoma darbe analizuojama elektroninio balsavimo sistema, pristatomi vartotojų identifikacijos bei galutinio rinkimų rezultato nustatymo metodai, kurie bus naudojami vystant šią EBS. Tiriamojoje dalyje (**4 skyrius**) bus atlikta detali EBS analizė bei jos modifikacija, apibendrinti darbe gauti rezultatai ir baigiama darbo išvadomis (**5 skyrius**).

2. Analitinė dalis

2.1. Darbe naudojami žymėjimai ir trumpiniai

EBS – Elektroninio balsavimo sistema

P – Pareiškėjas

V – tikrintojas

GT – dviejų milijonierių problema

$V = \{V_1, V_2, \dots, V_n\}$ – rinkėjų aibė

I – valdžios institucija

$X = \{X_1, X_2, \dots, X_k\}$ – galimų balsavimo pasirinkimų aibė

M – slenksčio konstanta

$\lceil n \rceil$ – „lubų“ (***angl.*** *ceiling*) funkcija, lygi mažiausiam sveikajam skaičiui k, ne mažesniam, nei *n*.

2.2. Elektroninio balsavimo sistemos apibrėžimas

1 Apibrėžimas. Elektroninis balsavimas – tai balsavimo procesas, leidžiantis balsuotojams saugiai ir slaptai išreikšti savo balsavimo pasirinkimą, naudojant kompiuterinę techniką bei ryšio technologijas (Gritzalis, 2002).

Pagrindinis elektroninio balsavimo tikslas yra padidinti rinkimuose dalyvaujančių balsuotojų kiekį, suteikiant galimybę balsuoti iš namų arba iš darbo vietos, sumažinti vykdomų rinkimų kaštus (nebereikia žmoniškųjų išteklių balsų skaičiavimui, o investicijos, skirtos elektroninio balsavimo sistemos vystymui – ilgalaikės, kadangi saugią ir tinkamą naudoti sistemą galima naudoti ne vieneriuose rinkimuose) bei pagerinti rinkimų rezultatų tikslumą. Norint, kad elektroninis balsavimas būtų saugus bei patikimas, be sklandaus kompiuterinės technikos bei ryšio technologijų veikimo užtikrinimo reikalinga saugi elektroninio balsavimo schema.

2 Apibrėžimas. Elektroninio balsavimo schema - tai aibė protokolų, apibrėžiančių, kaip bus skelbiami rinkėjų balsai, nustatomas galutinis rinkimų rezultatas bei atliekami kiti su elektroniniu balsavimu susiję veiksmai (vartotojų registracija, rinkėjų balsų tinkamumo patikrinimas). Elektroninio balsavimo schema, kartu su ją įgyvendinančia kompiuterine technika bei ryšio technologijomis, sudaro elektroninio balsavimo sistemą. (Gritzalis, 2002)

Pagal tai, kaip vyksta balsavimo procesas, galima išskirti 3 pagrindinius elektroninio balsavimo sistemų tipus (Quadah, Taha, 2007):

a) Kompiuterinio skaičiavimo sistemos – rinkėjai pažymi savo balsą popieriaus lape (balsavimo kortelėje). Tuomet kortelė nuskenuojama ir rinkėjo balsas išsaugomas centriniame (arba balsavimo stoties, kurioje buvo nuskenuota kortelė) kompiuteryje.

b) Tiesioginio įrašymo elektroninio balsavimo mašina (***angl.*** *Direct – recording electronic voting macine, DRE*) – balsuotojas, naudodamas klaviatūrą arba liečiamąjį ekraną, pažymi savo balsą, kuris išsaugomas balsavimo stoties kompiuteryje. Balsavimui pasibaigus, rezultatai iš balsavimo stočių siunčiami į centrinį kompiuterį bei nustatomas galutinis rinkimų rezultatas.

c) Balsavimas internetu – balsavimui naudojamas kompiuteris bei internetas. Šis balsavimo tipas dar skirstomas į:

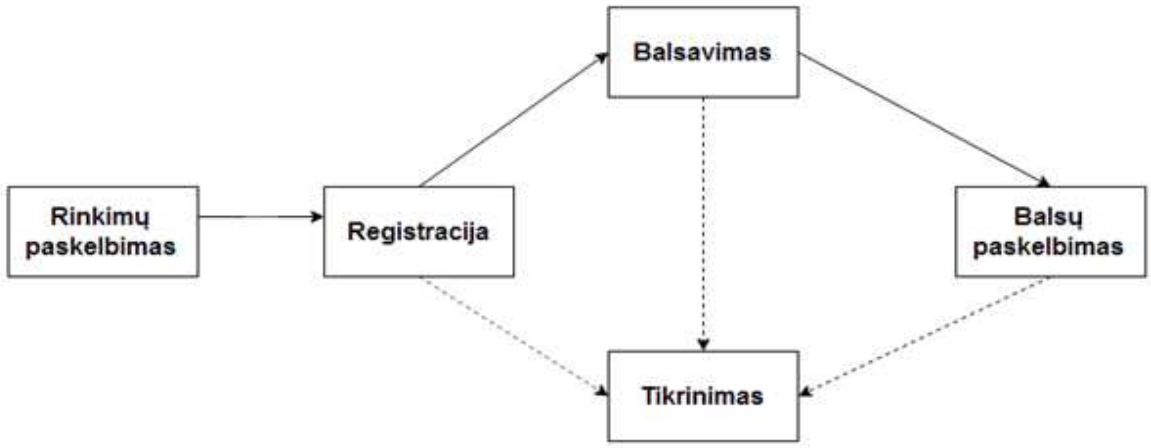
- Balsavimo apylinkių “ (***angl.*** *Poll - site*) elektroninio balsavimo sistemos – rinkėjai balsuoja specialiose rinkimų vietose – apylinkėse, naudodamiesi ten esančiais kompiuteriais. Kompiuterinę techniką bei rinkėjus prižiūri rinkimų atstovai, taip užtikrinant rinkimų saugumą.
- „Balsavimo terminalų“ (***angl.*** *Kiosk*) elektroninio balsavimo sistemos – rinkėjai gali balsuoti balsavimui pritaikytuose terminaluose, išdėstytuose strateginėse

vietose (parduotuvėse, pašto skyriuose, mokymo įstaigose, darbo vietose). Kadangi nuolatinis terminalų stebėjimas nėra būtinas (taip pat terminalų stebėjimą galima atlikti naudojant vaizdo kameras), ši elektroninio balsavimo sistema leidžia didesnę rinkimų trukmę (kelias dienas ar savaites trunkančius rinkimus).

- „Nuotolinio balsavimo“ (***angl** Remote*) sistema – leidžia rinkėjams balsuoti iš bet kokio kompiuterio ar kito elektroninio prietaiso, turinčio prieigą prie interneto, taigi galimas balsavimas iš namų arba darbo vietos.

Bendru atveju, balsavimo modelyje dalyvauja keturi subjektai (Sampigethaya, Poovendran, 2006): balsuotojai (rinkėjai), rinkimų kandidatai, valdžios institucija (***angl.*** *Authority*) ir priešKoji šalis (***angl.*** *Adversary*). Vykstant rinkimams, balso teisę turintys rinkėjai, priklausomai nuo iš anksto nustatyto rinkimų protokolo, pasirenka vieną ar kelis kandidatus iš pateikto sąrašo (arba, jeigu tai numatyta, įrašo naują kandidatą). Tuo tarpu valdžios institucija yra atsakinga už rinkimų eigą – rinkimų saugumo parametrų parinkimą, rinkėjo teisės balsuoti bei jo tapatybės patikrinimą, balsų tinkamumo patikrinimą, galutinio rinkimų rezultato nustatymą. Priešiškoji šalis rinkimų modelyje galimai bando manipuliuoti rinkėjų balsais arba suklastoti galutinį rinkimų rezultatą, bandant papirkti rinkėjus, pažeisti jų privatumą, atskleisti tarpinį rinkimų rezultatą arba papirkti valdžios instituciją.

Elektroninio balsavimo etapus galima pavaizduoti schematiškai(**2.1 pav.**):



2.1 pav. Elektroninio balsavimo etapai

Rinkimų paskelbimo (***angl.*** *Announcement*) etape, įvykdomi numatyti protokolai (rinkėjų bei valdžios institucijų sertifikatų išdavimas, sistemos saugumo parametrų generavimas) bei sudaromas rinkėjų, turinčių balsavimo teisę, sąrašas.

Registracijos (***angl.*** *Registration/Pre-voting*) etape vykdomas balsuotojų tapatybės patikrinimas bei nustatoma, ar nebando balsuoti pakartotinai.

Balsavimo (***angl.*** *Voting/ Ballot - Casting*) etape vykdomi su balso paskelbimu susiję veiksmai (balsavimo pasirinkimo suformavimas bei paskelbimas, jo įrašymas į bendrą balsų sąrašą).

Balsų paskelbimo etape (***angl.*** *Tallying*), patikrinamas balsų teisingumas, atliekami veiksmai rinkimų rezultato nustatymui bei paskelbiamas galutinis rinkimų rezultatas.

Tikrinimas (***angl*** *Verification*) atliekamas kiekvieno iš 3 etapų – Registracijos, Balsavimo bei Balsų paskelbimo – metu, siekiant identifikuoti galimas klaidas ar mėginimus sukčiauti.

2.3. Reikalavimai, keliami elektroninio balsavimo schemoms

Nepaisant to, kad elektroniniame balsavime galima naudoti įvairius balsavimo bei balsų skaičiavimo metodus, tam, kad rinkimai vyktų sklandžiai ir teisėtai, kiekviena elektroninio balsavimo sistema turi atitikti tam tikrus reikalavimus. Vienas iš esminių kriterijų, kurių laikomasis, formuluojant reikalavimus, kuriuos turi tenkinti elektroninio balsavimo sistemos, yra elektroninio balsavimo sistemos suderinamumas su šalies teisine sistema. Tai yra, elektroninio balsavimo įvedimas neturėtų pažeisti iki tol vykdytų rinkimų principų bei balsuotojų teisių, apibrėžtų valstybės konstitucijoje. Pagrindiniai šių rinkimų principai bei juos atitinkantys reikalavimai, keliami elektroninio balsavimo sistemoms, pateikiami **2.1 lentelėje.**

2.1 lentelė. Pagrindiniai rinkimų principai (Gritzalis, 2002)

Konstituciniai reikalavimai	Reikalavimai elektroninio balsavimo sistemoms
Visuotinumas	1.1 Tinkamumas
Laisvė	2.1 Balsavimo laisvė
	2.2 Kandidatų politinės reklamos apribojimai
	2.3 Neleistino balsavimo pasirinkimo galimybė
Lygybė	3.1 Kandidatų lygybė
	3.2 Rinkėjų lygybė
	3.3 Vienas balsuotojas – vienas balsas
Slaptumas	4.1 Slaptumas

Visuotinumo reikalavimas demokratiniuose rinkimuose reiškia, kad kiekvienam asmeniui, turinčiam balsavimo teisę, užtikrinama galimybė dalyvauti rinkimų procese. Jį atitinka tinkamumo (***angl.*** *Eligibility*) reikalavimas, keliamas elektroninio balsavimo sistemoms. Šis reikalavimas užtikrinamas registracijos etape įvedus balsuotojo identifikacijos (tapatybės nustatymo)

procedūrą. Taip pat balsuotojų identifikacija užtikrina, kad balsuoja tik turintis teisę tai daryti asmuo bei nebandoma balsuoti antrą kartą.

Kita vertus, nors pakartotinis balsavimas įprastuose rinkimuose yra neleidžiamas, realizuojant elektroninio balsavimo sistemas praktikoje (Estijos elektroninio balsavimo sistema (Barrat, Esteve, Goldsmith, Turner, 2012)) rinkėjams leidžiama balsuoti keletą kartų, anuliuojant ankstesnius balsavimo pasirinkimus. Ši visuotinumo reikalavimo modifikacija, nors ir neįmanoma įprastiniuose rinkimuose, elektroninio balsavimo sistemose naudojama kaip kovos su sukčiavimu priemonė, pašalinanti balsų papirkinėjimo galimybę (Grimm, Volkammer, 2006), kadangi rinkėjas, kurį buvo bandoma papirkti, vėliau balsavimo pasirinkimą gali pakeisti.

Laisvų rinkimų principas teigia, kad rinkimai turi vykti be smurto, prievartos ar kitokios įtakos tiek valstybiniame, tiek vieno ar kelių žmonių grupės lygmenyje. Todėl balsuojant nuotoliniu būdu, pavyzdžiui, iš darbo vietos, atsiranda grėsmė, kad darbdavys arba sistemų administratorius stebės balsavimo eigą ir bus nustatyti darbuotojų balsavimo pasirinkimai. Tam, kad tokių situacijų būtų išvengta, elektroninio balsavimo sistemose įvedamas balsavimo laisvės (***angl.*** *Incoercibility*) reikalavimas, užtikrinantis, kad neįmanoma nustatyti rinkėjo balsavimo pasirinkimo.

Taip pat turi būti užtikrinta, kad interneto svetainėje, kurioje balsuojama, nebūtų galima rinkimų kandidatų reklama (analogija rinkiminės propagandos draudimui demokratiniuose rinkimuose).

Galiausiai, norint suteikti galimybę balsuotojui pilnai išreikšti savo nuomonę, turėtų būti numatyta galimybė pateikti ir sąmoningai nelegalų balsą (tuščio biuletenio arba neleistino kandidatų pasirinkimo galimybė įprastiniuose rinkimuose) taip, kad šis balsas nepakenktų galutiniam rinkimų rezultatui.

Lygybės principas teigia, kad kiekvieno iš rinkimuose dalyvaujančių kandidatų teisės būtų vienodos (neturi būti faktorių, suteikiančių vienam ar keliems kandidatams pranašumų rinkimuose) bei kiekvieno iš rinkėjų balsavimo teisės būtų vienodos. Elektroninio balsavimo atveju, lygybės reikalavimas reiškia, kad kiekvienas balsuotojas turės vienodą priėjimą prie balsavimo technologijų. Taigi, turi būti užtikrinta galimybė balsuoti ir asmenims, neturintiems prieigos prie balsavimo technologijų, naudojamų elektroninio balsavimo procese (balsavimo apylinkių, terminalų ar balsavimo nuotolinio balsavimo).

Norint įgyvendinti vieno balsuotojo – vieno balso reikalavimą, turi būti užtikrinama, kad balsuotų tik balso teisę turintis rinkėjas tik vieną kartą ir tik vienu iš balsavimo būdų (jeigu yra numatyta keletas balsavimo alternatyvų). Todėl elektroninio balsavimo sistema turi būti apsaugota nuo :

a) Balso dubliavimo (rinkėjas ar kitas asmuo negali nukopijuoti balso ir pateikti jį pakartotinai);
b) pakartotino balsavimo (balsuojant elektroniniu būdu keletą kartų arba po vieną kartą skirtingais balsavimo būdais, jeigu tokių numatyta ne vienas);
c) Paskelbto balso modifikavimo.

Kitas itin svarbus demokratinių rinkimų bruožas yra **slaptumas** – norint užtikrinti balsuotojų apsisprendimo laisvę, neturi būti ryšio tarp rinkėjo ir jo balsavimo pasirinkimo. Todėl elektroninio balsavimo sistemos turi tenkinti šiuos su slaptumu susijusius reikalavimus:

a) Balsų paskelbimo, perdavimo ryšio kanalu ir surinkimo metu turi būti užtikrinamas balsų slaptumas;
b) Jokia šalis, dalyvaujanti rinkimų procese, negali iš balso nustatyti rinkėjo, paskelbusio šį balsą, tapatybės;
c) Aiški atskirtis tarp registracijos ir balsų skelbimo etapų;
d) Joks balsuotojas negali įrodyti savo balsavimo pasirinkimo po balso paskelbimo.

Iš kitos pusės, kad būtų įmanoma teisingai nustatyti galutinį rinkimų rezultatą, prieš šio rezultato skaičiavimą elektroninio balsavimo sistemoje turi būti įvestas balsų teisingumo patikrinimas.

Be paminėtų reikalavimų, keliamų elektroninio balsavimo sistemoms, ne mažiau svarbūs yra ir papildomi reikalavimai, suformuluoti kitame literatūros šaltinyje (Sampigethaya, Poovendran, 2006):

Patikrinamumas (***angl.*** *Verifiability*) – rinkėjas turi galimybę patikrinti, ar jo balsas į galutinį rinkimų rezultatą įskaičiuotas teisingai. Yra du galimi patikrinamumo variantai (Sako, Killian, 1995): individualus (kiekvienas iš rinkėjų gali pasitikrinti, ar jo balsas įskaičiuotas teisingai) ir universalus (kuomet po galutinio rezultatų paskelbimo bet kas gali įsitikinti, kad visi teisėti balsai buvo įskaičiuoti teisingai ir galutinis rezultatas suskaičiuotas teisingai). Nors balso teisingumo patikrinimui reikalingas ryšys tarp balsuotojo ir jo balso (kas prieštarauja slaptumo reikalavimui), tačiau šis reikalavimas itin svarbus, norint įgyti rinkėjų pasitikėjimą elektroninio balsavimo sistema.

Tikslumas (***angl.*** *Accuracy*) – elektroninio balsavimo sistemoje, visi balsai turi būti įskaičiuoti ir suskaičiuoti teisingai, į galutinį rinkimų rezultato skaičiavimą neįtraukiant neteisėtų balsų.

Sąžiningumas (***angl.*** *Fairness*) – neįmanoma suskaičiuoti ir atskleisti tarpinio rinkimų rezultato.

Tvirtumas (***angl.*** *Robustness*) – elektroninio balsavimo sistema turi būti atspari aktyvioms bei pasyvioms atakoms (korumpuotos valdžios institucijos ar rinkėjai) bei galimoms

klaidoms (valdžios institucijų ar rinkėjų nedalyvavimas rinkimuose). Elektroninio balsavimo schema laikoma maksimalaus tvirtumo, jeigu rinkimus sužlugdyti gali tik visų valdžios institucijų susitarimas. Tačiau tokioje schemoje privalomas visų valdžios institucijų dalyvavimas, todėl rinkimus gali sužlugdyti bet kuri nedalyvaujanti valdžios institucija.

Pritaikomumas (***angl*** *Scalability*) – skaičiavimai, vykdant elektroninio balsavimo schemos protokolus, turi būti atliekami efektyviai. Schemoje taip pat neturėtų būti prielaidų, apsunkinančių schemos realizavimą didelėms balsuotojų grupėms.

2.4. Egzistuojančių elektroninio balsavimo sistemų apžvalga

Istoriškai, turbūt vienas primityviausių balsavimo metodų buvo rinkimai, vykdyti senovės Spartoje, daugiau nei prieš 2500 metų. Rinkimai tuomet vykdavo viešoje erdvėje, o rinkimų nugalėtoju būdavo skelbiamas kandidatas, sulaukęs daugiausiai visuomenės ovacijų. Tačiau ši rinkimų forma gyvavo neilgai – netrukus ją pakeitė iš Atėnų perimtas balsavimas, kurio metu balsavimo pasirinkimą atspindėdavo tam tikros spalvos akmenukas, įmestas į urną, skirtą balsavimui. Šis metodas prigijo, nes rinkimų rezultatas buvo objektyvesnis, be to, buvo išsaugomas balsuojančių asmenų privatumas ir išvengiama papirkinėjimų grėsmės.

Tačiau vystantis visuomenei bei augant rinkimų mastams, tobulėjo ir balsavimo metodai. Balsavimą akmenukais pakeitė popieriniai balsavimo biuleteniai (pirmą kartą oficialūs balsavimo biuleteniai rinkimuose buvo panaudoti Australijoje, 1857 metais, o 1859 metais – ir Jungtinėse Amerikos Valstijose), dar vėliau mechaninės balsavimo mašinos su svirtimis, kuomet rinkėjas balsavimo pasirinkimą išreikšdavo nuleisdamas vieną iš svirčių, optiniai skenavimo prietaisai, balsavimas paštu bei elektroniniu paštu bei balsavimas internetu.

Pirmoji valstybė, panaudojusi elektroninį balsavimą internetu nacionaliniuose rinkimuose buvo Estija. Joje nuotolinis balsavimas internetu tęsiasi jau dešimtmetį, nors pastaruoju metu rimtai suabejota Estijoje naudojamos elektroninio balsavimo sistemos saugumu dėl galimo kenkėjiškos programinės įrangos panaudojimo bei kitų galimų atakų bei buvo siūlyta internetinius rinkimus nutraukti, kol nebus išspręstos kompiuterinės įrangos problemos (Halderman et al., 2014). Nepaisant galimų grėsmių, rinkėjų, balsuojančių internetu, skaičius – pakankamai didelis (atitinkamai 31.3% ir 30.5% bendro dalyvavusių rinkėjų 2014 ir 2015 metais skaičiaus, palyginus su 1.9% ir 5.5% - 2005 ir 2006 metais). Be programinės įrangos saugumo problemų, balsuojant internetu nuotoliniu būdu taip pat iškyla papirkinėjimo grėsmė, kurią aptikti pakankamai sudėtinga, nors yra ir elektroninių balsavimo sistemų, atsparių papirkinėjimui bei priverstiniam balsavimui (Wu et al., 2014).

Taigi, pastarieji pavyzdžiai atskleidžia, kad nors rinkėjų, norinčių balsuoti internetu, skaičius auga, tačiau nestinga ir iššūkių, kuriuos dar reikia įveikti, norint, kad elektroninis balsavimas būtų saugus bei patikimas.

Toliau, darbą tęsime apibrėždami pagrindines sąvokas bei metodus, kurie bus reikalingi tolesnės darbo eigos metu.

2.5. Nulinio atskleidimo įrodymai

Šie įrodymai pirmą kartą aprašyti S. Goldwasser, S. Micali, C. Rackoff 1989 metais išleistame straipsnyje „The Knowledge Complexity of Interactive Proof Systems“ (Goldwasser, Micali, Rackoff, 1989). Yra išskiriamos dvi pagrindinės nulinio atskleidimo įrodymų algoritmų klasės (Oppliger, 2005): interaktyvūs ir neinteraktyvūs. Neinteraktyvią įrodymų sistemą sudaro efektyvus įrodymo patikrinimo algoritmas, kuris, turėdamas teiginį ir jo įrodymą, sugeneruoja sprendimą $s \in \{0; 1\}$. Jeigu $s = 1$, įrodymas šiam teiginiui yra teisingas, jeigu $s = 0$, įrodymas yra neteisingas.

Interaktyvūs įrodymai, kurie bus naudojami šiame darbe, yra protokolai, kuriuos gali naudoti šalis P, norėdama teiginį įrodyti šaliai V, naudojant tikimybinius algoritmus. Pirmiausiai, suformuluosime interaktyvios įrodymų sistemos apibrėžimą (Goldreich, Oren, 1994):

3 Apibrėžimas. Interaktyvi įrodymų sistema kalbai L yra protokolas, t.y. lokalių programų pora dviem interaktyvioms, tikimybinėms mašinoms, vadinamoms pareiškėjui P (***angl.*** *Prover*) ir tikrintojui V (***angl.*** *Verifier*), turinčioms priėjimą prie abiems mašinoms žinomų duomenų (įeities juostos). Šios mašinos gali komunikuoti tarpusavyje, naudodamos komunikavimo juostą. Kiekviena mašina turi priėjimą tik prie savo juostos (tik šiai mašinai žinomų duomenų), įeities juostos bei komunikavimo juostos. Tikrintojas V, atlikęs tam tikrą žingsnių (skaičiavimų bei komunikacijų) skaičių, sustoja *priėmimo* arba *atmetimo* būsenoje. Tikrintojui V atliekant iš anksto numatytus veiksmus, turi būti tenkinamos šios dvi sąlygos:

1. Interaktyvių įrodymų pilnumas (***angl.*** *Completeness*): Tikrintojui V, vykdydant numatytą programą, su kiekviena konstanta c ir pakankamai dideliu $x \in L$, galutinė tikrintojo būsena lygi 1 (teiginys $x \in L$ priimamas) su tikimybe, ne mažesne nei $1 - |x|^{-c}$. Tai yra, pareiškėjas gali įtikinti tikrintoją, kad $x \in L$.
2. Pagrįstumas (***angl.*** *Soundness*): kiekvienai programai P^*, vykdomai pareiškėjo, su kiekviena konstanta c ir pakankamai dideliu $x \notin L$, galutinė tikrintojo būsena lygi 0 (teiginys $x \in L$ atmetamas) su tikimybe, ne mažesne nei $1 - |x|^{-c}$. Tai yra, pareiškėjas negali apgauti tikrintojo.

Teiginio $x \in L$ pavyzdžiui galėtų būti toks sveikas skaičius *x*, kad $x^2 = r(mod\ N)$, čia *r* ir *N* – sveikieji skaičiai – įrodymo paslaptis šiuo atveju yra skaičiaus *r* kvadratinė šaknis moduliu *N*).

Tam, kad interaktyvi įrodymų sistema būtų laikoma interaktyvia nulinio atskleidimo įrodymo sistema, turi būti išpildyta trečioji sąlyga:

4 Apibrėžimas. Nulinis atskleidimas (*angl.* Zero knowledge) – kiekvienam tikrintojui V^*, egzistuoja simuliatorius S^* (atsitiktinis, polinominio laiko algoritmas, simuliuojantis tikrintojo *V* komunikacijas su pareiškėju *P*), toks, kad kiekvienam $x \in L$, $\{Com(V^*, P)(x)\} = \{S^*(x)\}$, čia $\{Com(V^*, P)(x)\}$ – komunikacijų tarp V^* ir *P*, esant bendriems duomenims *x*, aibė.

4 apibrėžime simuliatoriaus S^* egzistavimas reiškia, kad jeigu $x \in L$, tikrintojas nesužinos apie *x* nieko daugiau, išskyrus faktą, kad $x \in L$.

Apibendrinant, šios trys savybės reiškia, kad interaktyvi nulinio atskleidimo įrodymo sistema turi leisti pareiškėjui P įtikinti tikrintoją V, kad jo žinomas teiginys yra teisingas (pilnumo reikalavimas), tuo tarpu jokia sukčiavimo strategija neturi apgauti tikrintojo, priverčiant priimti klaidingą teiginį (pagrįstumo reikalavimas). Taip pat nulinio atskleidimo įrodymai yra saugūs šaliai P, kadangi jų metu neatskleidžiama paslaptis, kurią žino pareiškėjas (nulinio atskleidimo reikalavimas).

Nulinio atskleidimo įrodymų veikimas pagrįstas asimetrinės kriptografijos principais ir dažniausiai remiasi vienkryptėmis funkcijomis. Naudojant vienkryptes funkcijas, įrodymo skaičiavimus galima atlikti efektyviai, tačiau, norint atskleisti įrodymo paslaptį, tektų spręsti sudėtingą matematinę problemą (pavyzdžiui, didelio skaičiaus $n = p \cdot q$ faktorizacijos (išskaidymo pirminiais daugikliais) problemą, kvadratinės šaknies moduliu *n* radimo problemą, diskretinio logaritmo problemą ir kt.).

Toliau, suformuluosime nulinio atskleidimo įrodymo protokolą, skirtą pareiškėjui įrodyti, kad jis žino kvadratinę šaknį (liekaną) moduliu *n* (Oppliger, 2005). Šio algoritmo viešieji parametrai yra kvadratinė liekana *v* bei modulis *n* (dviejų didelių pirminių skaičių *p* ir *q* sandauga), kuriuo bus atliekami veiksmai. Modulio *n* daugikliai *p* ir *q* bei kvadratinės liekanos *v* šaknis s: $s^2 \equiv v \pmod n$ laikomi paslaptyje ir žinomi tik šaliai P.

Kiekvieno protokolo vykdymo metu šalis P, norėdama įrodyti tikrintojui V, jog žino algoritmo paslaptį (kvadratinę šaknį *s*), sugeneruoja atsitiktinį sveikąjį skaičių $r \in \mathbb{Z}_n^*$ bei apskaičiuoja parametrą $x = r^2 \pmod n$. Atsitiktinį skaičių *x* šalis P siunčia tikrintojui V. Šalis V sugeneruoja atsitiktinį bitą $b \in \{0; 1\}$ ir nusiunčia jį P. P apskaičiuoja skaičių $y = r \cdot s^b \pmod n$ bei nusiunčia jį V, kuris patikrina, ar $y^2 \equiv x \cdot v^b (mod\ n)$. Jeigu ši lygybė galioja, vadinasi, pareiškėjas P žino slaptą šaknį *s* su tikimybe lygia $\frac{1}{2}$, kadangi atsitiktinis bitas *b*, kurį sugeneruoja šalis V, gali įgyti 2 reikšmes: 0 arba 1.

Norint sumažinti sukčiavimo tikimybę (sukčiavimo tikimybė lygi $\frac{1}{2^k}$, čia k – įvykdytų protokolų skaičius, o sukčiavimo tikimybė kiekvieno protokolo metu lygi $\frac{1}{2}$), protokolas kartojamas. Viešieji parametrai *n* ir *v* nusiunčiami šaliai V pirmojo protokolo vykdymo pradžioje, kartojant protokolą, šis žingsnis praleidžiamas, algoritmą kartojant nuo atsitiktinio skaičiaus *r* generavimo. Protokolo schema pateikiama **2.2 lentelėje.**

2.2 lentelė. Kvadratinės šaknies moduliu *n* nulinio atskleidimo įrodymo schema (Oppliger, 2005)

P $(\boldsymbol{n}, \boldsymbol{s})$		**V** $(\boldsymbol{n}, \boldsymbol{v})$
$\boldsymbol{r} \in \mathbb{Z}_{\boldsymbol{n}}^{*}$		
$\boldsymbol{x} = \boldsymbol{r}^{\boldsymbol{2}} (\mathbf{mod}\ \boldsymbol{n})$	$\xrightarrow{\boldsymbol{x}}$	
	$\xleftarrow{\boldsymbol{b}}$	$\boldsymbol{b} \in \{\mathbf{0}, \mathbf{1}\}$
$\boldsymbol{y} = \boldsymbol{r} \cdot \boldsymbol{s}^{\boldsymbol{b}} (\mathbf{mod}\ \boldsymbol{n})$	$\xrightarrow{\boldsymbol{y}}$	
		$\boldsymbol{y}^{\boldsymbol{2}} \stackrel{?}{=} \boldsymbol{x} \cdot \boldsymbol{v}^{\boldsymbol{b}} (\boldsymbol{mod}\ \boldsymbol{n})$ (Įvykdomas patikrinimas)

Kvadratinės šaknies moduliu *n* nulinio atskleidimo protokolą, nepriklausomai nuo šalies V atsitiktinai sugeneruoto bito *b*, sėkmingai gali įvykdyti tik pareiškėjas P, žinantis viešai paskelbtos kvadratinės liekanos *v* kvadratinę šaknį *s* (algoritmo paslaptį). Žinant kvadratinę liekaną *v*, rasti jos šaknį moduliu *n* sudėtinga – ši problema ekvivalenti modulio $n = p \cdot q$, kuriuo atliekami veiksmai, išskaidymui pirminiais dauginamaisiais.

Kai atsitiktinis bitas $b = 0$, $y_0 = r$ (*r* – žinomas, nes jį sugeneravo P pirmajame protokolo žingsnyje (žr. **2.2 lentelėje).** Kai bitas $b = 1$, $y_1 = r \cdot s^1 = r \cdot s$ – ir šiuo atveju, abu parametrai *r* ir *s* žinomi tik šaliai P. Tuo tarpu kenkėjui E (***Angl.*** Eavesdropper), nežinančiam algoritmo paslapties – šaknies *s*– tikimybė sėkmingai įvykdyti aprašytą protokolą lygi $\frac{1}{2}$, kadangi E gali pasiruošti tik vienai iš dviejų bito *b* reikšmių.

Tikimybė, jog kenkėjui E pavyks įvykdyti protokolą nežinant šaknies s, lygi $\frac{1}{2}$. Jeigu bitas *b* bus lygus 0, tuomet jis gaus teisingą rezultatą, laikydamasis protokolo, kadangi šiuo atveju reikalingas tik atsitiktinis skaičius *r*, kurį gali sugeneruoti ir kenkėjas, o šaknies *s* žinoti nereikia. Tačiau jeigu $b = 1$, norint sėkmingai įvykdyti protokolą, kvadratinę šaknį moduliu *n* žinoti reikia, kitu atveju sėkmingai įvykdyti protokolo nepavyks ir bus aptiktas sukčiavimas.

Iš kitos pusės, jeigu E atspėja, jog atsitiktinis bitas b bus lygus 1, jis gali sugeneruoti x, pasirinkdamas atsitiktinį skaičių t ir apskaičiuodamas reiškinį $x = \frac{t^2}{v}$ bei vietoje $y = r \cdot s^b$ siųsdamas $y = t$ Tuomet V, paskutiniame protokolo žingsnyje patikrinęs, ar $y^2 \equiv x \cdot v^b$, gaus teisingą tapatybę, kadangi $x \cdot v^b = \frac{t^2}{v} \cdot v = t^2 \equiv y^2$. Tačiau, jeigu $b = 0$, tapatybė negalios: $x \cdot v^b = \frac{t^2}{v} \cdot v^0 = t^2 \cdot v^{-1} \not\equiv y^2$ ir bus aptiktas sukčiavimas.

Vykdant šį nulinio atskleidimo įrodymo protokolą, svarbu kiekvieną kartą sugeneruoti naują atsitiktinį skaičių r (pirmas algoritmo žingsnis). Kitu atveju nesąžiningas tikrintojas V gali įvykdyti du protokolus: vieną kartą nusiųsti bitą $b = 0$, o antrojo protokolo metu bitą $b = 1$. Tokiu atveju, pareiškėjui P kartojant protokolą ir nesugeneravus naujo atsitiktinio skaičiaus r, tikrintojas gaus du rezultatus: $x_1 = r$ ir $x_2 = r \cdot s$ su ta pačia r reikšme ir bus lengva apskaičiuoti algoritmo paslaptį s: $s = r^{-1} \cdot x_2$.

Protokolo metu neatskleidžiama nauja informacija. Jeigu egzistuotų pašalinis stebėtojas E, stebintis bendravimą tarp šalių P ir V, tuomet, jeigu atsitiktinis bitas $b = 0$, E sužinotų atsitiktinį skaičių r bei jo kvadratą x. Kai $b = 1$, E sužinos skaičių $r \cdot s$ ir $x = \frac{(r \cdot s)^2}{v}$. Tačiau šiuos skaičius r ir x kenkėjas E gali sugeneruoti ir nežinodamas bendravimo tarp P ir V, kadangi tai – atsitiktiniai skaičiai, kintantys kiekvieno protokolo pakartojimo metu. Kiekvieno protokolo metu tikimybė, jog pareiškėjas nežino kvadratinės šaknies s, lygi $\frac{1}{2}$. Ši tikimybė sumažinama, protokolą pakartojant keletą kartų. Sukčiavimo tikimybė, protokolą įvykdžius k kartų, lygi $\frac{1}{2^k}$.

Praktikoje nulinio atskleidimo įrodymai naudojami, kai norima apsikeisti slapta informacija, tačiau reikia tik šių duomenų žinojimo pavirtinimo, o pačios informacijos atskleidimas nėra būtinas. Nulinio atskleidimo įrodymų praktinio taikymo pavyzdžiai yra kredito kortelės savininko tapatybės patvirtinimas (klientas įrodo, kad žino savo identifikacinį numerį (slaptažodį), kuris lieka nežinomas), elektroninių pinigų sistemos (korektiško atsiskaitymo elektroniniais pinigais užtikrinimas), elektroninio balsavimo sistemos (rinkėjas įrodo, kad jo balsas yra tinkamas, neatskleisdamas savo pasirinkimo). Šiame darbe nulinio atskleidimo įrodymai bus naudojami atliekant vartotojų identifikaciją bei balso tinkamumo patikrinimą. Toliau pristatysime Yao dviejų milijonierių problemą – nulinio atskleidimo įrodymų atšaką, kuri bus naudojama, atliekant EBS modifikaciją.

2.5.1. Yao dviejų milijonierių problema

Andrew C. Yao, nagrinėdamas saugių skaičiavimų protokolus (Yao, 1982), siekė išspręsti dviejų milijonierių problemą (***angl.*** *GT(„greater than“)* problema): kaip dviem žmonėms (milijonieriams) nustatyti, kuris iš jų – turtingesnis, neatskleidžiant turimos pinigų sumos.

Apibendrintame problemos variante, m žmonių $P_1, P_2, \dots, P_m$ siekia apskaičiuoti funkciją $f(x_1, x_2, \dots, x_m)$. Čia $x_i \in [a, b], i = \overline{1, m}$ bei funkcijos f reikšmė – sveikieji skaičiai. Daroma prielaida, kad asmuo P_i žino parametrą x_i, bet nežino parametrų $x_j, i \neq j$. Uždavinio tikslas – šalims P_i, bendradarbiaujant tarpusavyje bei išsaugant savo paslaptis x_i, apskaičiuoti funkcijos $f(x_1, x_2, \dots, x_m)$ reikšmę.

Parinkę funkciją

$$f(x_1, x_2) = \begin{cases} 1, x_1 < x_2 \\ 0, x_1 \geq x_2 \end{cases},$$

gausime dviejų milijonierių problemos formuluotę, kuri bus naudojama ir šiame darbe, analizuojant elektroninio balsavimo sistemą bei nustatant galutinį rinkimų proceso rezultatą.

2.5.2. Dviejų milijonierių problemos sprendimas

Suformulavęs GT problemą, A. C. Yao pasiūlė ir pirmąjį šios problemos sprendimą (protokolą) (Yao, 1982). Tarkime, GT uždavinyje dalyvauja dvi šalys: *A* ir *B*, o jų saugomos paslaptys – atitinkamai *a* ir *b*. Protokolas Π, skirtas šio uždavinio sprendimui, turi tenkinti šiuos reikalavimus:

1. Šalys *A* ir *B* vykdo visus protokolo žingsnius, kadangi nori sužinoti, kurios paslaptis – didesnė, tačiau gali bandyti išsiaiškinti kitos šalies paslaptį.
2. Protokolas Π grąžina reikšmę 1 tada ir tik tada, kai $a > b$.
3. Protokolo metu šalys *A* ir *B* negali nustatyti priešingos šalies paslapčių.

Šiame darbe GT problemos sprendimui bus naudojamas protokolas, pasiūlytas A. Amirbekyan ir V. E. Castro (Amirbekyan, Castro, 2009). Šiame protokole naudojamas faktas, kad funkciją $f(a, b)$ galima išskaidyti į dalis s_A, kurią žino šalis *A* ir s_B, kurią žino šalis *B* taip, kad dalių suma būtų lygi funkcijos reikšmei: $r_A + r_B = f(a, b)$, tačiau nei viena šalis negali nustatyti funkcijos rezultato, žinodama tik savo dalį.

Taigi, įvykdžiusios šį protokolą, šalis *A*, sauganti paslaptį *a* ir šalis *B*, sauganti paslaptį *b* gauna ne funkcijos $f(a, b)$ reikšmę, nurodančią, ar $a > b$, bet paslapties dalis r_A ir r_B, kur

$$r_A + r_B = \begin{cases} 1, \text{jeigu } a > b \\ 0, \text{jeigu } a \leq b \end{cases} = f(a, b)$$

Galima pastebėti, kad tuo atveju, kai $f(a,b)=1$, protokolas baigiamas, nes abi šalys įsitikina, kad $a>b$. Tačiau tuo atveju, kai $f(a,b)=0$, lieka dvi galimybės: $a<b$ arba $a=b$. Šią dilemą galima išspręsti protokolą pakartojus bei apskaičiavus funkcijos $f(b,a)$ reikšmę. Tuomet, priklausomai nuo antrojo abiejų funkcijos *f* reikšmių,

$$\begin{cases} f(a,b)=0, f(b,a)=0 \Rightarrow a=b \\ f(a,b)=0, f(b,a)=1 \Longrightarrow a<b \end{cases}.$$

Taip pat akivaizdu, jog norint patikrinti, ar $a>b$, pakanka patikrinti, ar $a-b>0$. Šiame protokole taip pat dalyvaus ir trečioji šalis *C*, nesužinanti funkcijos $f(a,b)$ rezultato, tačiau padedanti atlikti protokolo veiksmus. Protokolas, skirtas dviejų milijonierių problemos sprendimui, bus pateiktas **3.2** skyrelyje.

2.6. Darbo temos ir uždavinių pagrindimas

Atlikus literatūros apžvalgą matome, jog augantis rinkėjų, balsuojančių internetu, skaičius, remiantis pastarojo dešimtmečio rinkimų statistika Estijoje, bei naujų elektroninio balsavimo sistemų vystymas, patvirtina visuomenės susidomėjimą balsavimu internetu. Taigi, elektroninio balsavimo sistemos yra aktuali tema šiandieninėje visuomenėje. Siekiant išvengti daugelio EBS spragų, kuomet nėra užtikrinamas balsuotojų privatumas (slaptumo reikalavimas, suformuluotas **2.3** skyrelyje), buvo pasirinkta EBS, kurioje naudojami keleto šalių skaičiavimai, užtikrinantys, kad nebus galima nustatyti atskirų rinkėjų balsavimo pasirinkimų. Pagrindinė priežastis, kodėl reikėjo tobulinti darbe analizuojamą EBS – joje nebuvo numatyta balsų tinkamumo patikrinimo. Taip pat reikėjo tiksliau apibrėžti šioje elektroninio balsavimo sistemoje naudojamus parametrus bei pasiūlyti metodus, kuriuos būtų galima pritaikyti vartotojų identifikacijos bei galutinio rinkimų rezultato nustatymo etapams.

Tolesnėje darbo dalyje bus pateiktas pradinės EBS aprašymas bei nulinio atskleidimo įrodymų protokolai, reikalingi EBS modifikacijai.

3. Metodologinė dalis

3.1. Nagrinėjama elektroninio balsavimo sistema

Šiame darbe nagrinėjama elektroninio balsavimo schema, paremta saugiais keleto šalių skaičiavimais (***angl.*** *Secure Multi – Party Computation*, *SMC*) (Gang, 2008). Taip pat sistemoje daroma prielaida, kad balsuotojai turi du balsavimo pasirinkimus. Šioje elektroninio balsavimo schemoje dalyvauja keturios šalys:

1. Balsuotojai V (***angl.*** *Voter*). Daroma prielaida, kad schemoje dalyvauja *n* balsuotojų: $\{V_1, V_2, \dots, V_n\}$;
2. Valdžios institucija I, atsakinga už atsitiktinių skaičių generavimą, balsų užšifravimą ir galimų balsavimo pasirinkimų *X* sudarymą;
3. Balsų skaičiavimo institucija VC(***angl.*** *„Vote Counting“*), atliekanti tarpininko vaidmenį tarp baluotojų V ir valdžios institucijos I, nustatant galutinį rinkimų rezultatą;
4. Kandidatai $\{C_1, C_2\}$, už kuriuos balsuojama.

Schemoje balsavimo procesą sudaro trys etapai: balsuotojų registracija, balsavimas ir balsų surinkimas. Prieš prasidedant balsavimui, kiekvienas balsuotojas turi prisiregistruoti (už rinkėjų autorizaciją atsakinga institucija I).

3.1.1. Balsuotojų registracija

Balsuotojų registracijos metu, kiekvienam iš rinkėjų $V_i, i = \overline{1,n}$, n – rinkėjų, dalyvaujančių balsavime skaičius, institucija *I* sugeneruoja atsitiktinį skaičių $R_i, R_i \epsilon [a, b]$, $a, b \in \mathbb{Z}$ bei apskaičiuoja parametrą

$$R = n \cdot \sum_{i=1}^{n} R_i.$$

Parametras R žinomas tik jį apskaičiavusiai institucijai I. Apskaičiavus parametrą R, kiekvienam balsuotojui V_i siunčiamas atsitiktinis skaičius R_i ir tuščias balsavimo biuletenis. Taip pat paskelbiama galimų balsavimo pasirinkimų aibė $X = \{X_1, X_2\}$, $X_i \in \mathbb{N}, i = \overline{1,2}$ bei slenksčio konstanta *M*, kuri bus reikalinga galutinio rinkimų rezultato nustatymui.

3.1.2. Balsavimas

Balsavimo metu, kiekvienas iš rinkėjų V_i išskaido savo balsavimo pasirinkimą $x_i \in X$ į n dalių, laikomų paslaptyje ir žinomų tik rinkėjui V_i. Balsavimo pasirinkimo skaidinys bus $(x_{i1}, x_{i1}, \dots, x_{in})$, $x_{ij} \epsilon \mathbb{N}$. Be to, elementai x_{ij} tenkina lygybę $\sum_{j=1}^{n} x_{ij} = x_i$.

Visų balsuotojų pasirinkimų skaidinius dalimis patogu užrašyti matriciniame pavidale, kai i – tojoje matricos eilutėje įrašomas balsuotojo V_i balsavimo pasirinkimo skaidinys:

$$x = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix}.$$

Atlikus balsavimo pasirinkimo išskaidymą, kiekvienas rinkėjas V_i apskaičiuoja n sumų $x_{ij} + R_i$ ir siunčia kiekvieną iš sumų likusiems balsuotojams V_j. Šiuos skaičiavimus taip pat patogu užrašyti matriciniame pavidale:

$$x_R = \begin{pmatrix} x_{11} + R_1 & \cdots & x_{1n} + R_1 \\ \vdots & \ddots & \vdots \\ x_{n1} + R_n & \cdots & x_{nn} + R_n \end{pmatrix}.$$

Čia i – tojoje matricos x_R eilutėje surašyti rinkėjo V_i apskaičiuoti duomenys.

Visiems rinkėjams atlikus šią procedūrą ir apsikeitus duomenimis (rinkėjas V_i siunčia apskaičiuotą sumą $x_{ij} + R_i$balsuotojui V_j, ,$j = \overline{1,n}$), kiekvienas iš rinkėjų V_j sužino $k = n + +(n-1) = 2n - 1$ matricos x_R elementų:

$$x_R^{(j)} = \begin{pmatrix} * & x_{1j} + R_j & * \\ x_{j1} + R_j & \vdots & x_{jn} + R_j \\ * & x_{nj} + R_j & * \end{pmatrix}.$$

Čia simboliu $*$ žymimi rinkėjui V_j nežinomų matricos $x_R^{(j)}$ elementų blokai. Apsikeitus duomenimis, balsuotojai V_j, $j = \overline{1,n}$ suskaičiuoja matricų $x_R^{(j)}$ elementų, esančių j – tuosiuose stulpeliuose, sumas $S_j = \sum_{i=1}^{n}(x_{ij} + R_j)$ ir pasidalina jomis su likusiais rinkėjais.

Galiausiai, kiekvienas rinkėjas apskaičiuoja visų gautų duomenų sumą, kuri lygi

$$\sum_{j=1}^{n} S_j = \sum_{j=1}^{n}\left(\sum_{i=1}^{n} x_{ij} + R_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_{ij} + n \cdot \sum_{i=1}^{n} R_i = \sum_{i=1}^{n}\sum_{j=1}^{n} X_{ij} + R.$$

Paprastumo dėlei, sumą $\sum_{i=1}^{n}\sum_{j=1}^{n} X_{ij}$ pažymėsime D. Taigi, kiekvienas balsuotojas gali apskaičiuoti sumą $D + R$, iš kurios bus nustatomas balsavimo rezultatas bei rinkimų nugalėtojas.

3.1.3. Rinkimų rezultato nustatymas

Rinkimų nugalėtojas nustatomas išsprendus Yao dviejų milijonierių problemą (**2.5.1** skyrelis). Šios problemos sprendimas (**2.5.2, 3.3** skyreliai) buvo pritaikytas ir nagrinėjamos elektroninio balsavimo sistemos (Gang, 2008) balsų skaičiavimo etape. Rinkimų nugalėtojo nustatymo etape įvykdomi šie žingsniai:

1. Prieš balsavimą, valdžios institucija *I* sugeneruoja slenksčio konstantą $M = \max(X_1, X_2) \cdot \left\lceil \frac{n}{2} \right\rceil + \min(X_1, X_2) \cdot \left(n - \left\lceil \frac{n}{2} \right\rceil\right)$, kuri paskelbiama viešai.
2. Kiekvienas rinkėjas V_i apskaičiuoja parametrą T: $T = (D + R) - M$.
3. Kiekvienas balsuotojas $V_i, i = \overline{1,n}$ su valdžios institucija įvykdo dviejų milijonierių problemos sprendimo protokolą (**3.3** skyrelis) ir nustato: jeigu $T > R$, tuomet $D - M > 0$, t.y. $D > M$. Analogiškai, jeigu $T < R$, gauname, kad $D < M$. Proceso metu išsaugoma balsavimo paslaptis – balsų suma *D*, kuri išlieka nežinoma nei rinkėjams, nei valdžios institucijai I.

3.2. Feige – Fiat – Shamir vartotojų identifikacijos schema

Vienas iš šio darbo uždavinių – tobulinant elektroninio balsavimo sistemą (**3.1** skyrelis) pritaikyti vartotojų tapatybės nustatymo metodą. Norint įgyvendinti šią užduotį, buvo pasirinktas vartotojų identifikavimas, taikant nulinio atskleidimo įrodymų protokolus. Nulinio atskleidimo įrodymais paremta ir Feige – Fiat – Shamir (Trappe, 2006) vartotojų identifikacijos schema, kuri buvo naudojama šiame darbe.

Pirmiausiai, tikrintojas V parenka schemos saugumo parametrą – dviejų didelių pirminių skaičių p ir q sandaugą $n = p \cdot q$. Parametras n paskelbiamas viešai, tuo tarpu daugikliai p ir q saugomi paslaptyje ir žinomi tik institucijai tikrintojui. Tuomet vyksta viešų ir privačių parametrų generavimas: pareiškėjas P sugeneruoja atsitiktinių skaičių seką $(s_1, s_2, \dots, s_k)$, $\gcd(s_i, n) = 1$, žinomą tik pareiškėjui, bei apskaičiuoja skaičius $(v_1, v_2, \dots, v_k)$, $v_i = s_i^{-2} \bmod n$, $i = \overline{1,k}$ ir skaičiai $(v_1, v_2, \dots, v_k)$ nusiunčiami tikrintojui.

Tikrintojas galės patikrinti pareiškėjo tapatybę, įsitikindamas, kad jis žino skaičius $(s_1, s_2, \dots, s_k)$, įvykdydamas protokolą:

1. *P* sugeneruoja atsitiktinį skaičių *r*, apskaičiuoja $x = r^2 \bmod n$ ir siunčia *x* tikrintojui *V*.
2. *V* sugeneruoja atsitiktinių bitų seką $(b_1, b_2, \dots, b_k)$, $b_i \in \{0,1\}$, kurią siunčia *P*.
3. *P* apskaičiuoja sandaugą $y = r \cdot \prod s_i^{b_i} \bmod n$, kurią siunčia *V*.
4. *V* patikrina, ar $x = y^2 \prod v_i^{b_i} \bmod n$
5. 1 – 4 protokolo žingsniai pakartojami keletą kartų su skirtingomis *r* ir b_i reikšmėmis.

Taigi, kiekvieno protokolo vykdymo (raundo) metu tikrintojas *V* prašo pareiškėjo apskaičiuoti skaičiaus $x \cdot \prod v_l$, $v_l = \begin{cases} 1, & \text{kai } b_l = 0 \\ v_i, & \text{kai } b_l = 1 \end{cases}$, $i, l = \overline{1,k}$ kvadratinę šaknį moduliu *n*.

Pareiškėjas šią kvadratinę šaknį gali suskaičiuoti tik žinodamas atsitiktinį skaičių *r* ir skaičius v_l. Kitu atveju, tektų spręsti kvadratinės šaknies moduliu *n* radimo problemą, kas, nežinant modulio *n* faktorizacijos, laikoma sunkiai išsprendžiama problema, nuo kurios priklauso naudojamo protokolo saugumas.

Iš kitos pusės, pareiškėjas *P* (arba kitas asmuo, mėginantis apsimesti pareiškėju *P*) , gali sėkmingai įvykdyti identifikacijos protokolą ir nežinant skaičių $s_1, s_2, \dots, s_k$. Tačiau tam reikėtų teisingai atspėti atsitiktinių bitų $(b_1, b_2, \dots, b_k)$ seką dar prieš apskaičiuojant ir išsiunčiant atsitiktinį skaičių $x == r^2 \bmod n$ (šis skaičius apskaičiuojamas pirmame, o atsitiktinių bitų seka gaunama antrame protokolo žingsniuose). Tuomet pirmame protokolo žingsnyje pareiškėjas sugeneruoja atsitiktinį skaičių *y* ir išsiunčia tikrintojui $x = y^2 \prod v_i^{b_i} \bmod n$, o trečiame protokolo žingsnyje – atsitiktinį skaičių *y* ir tikrintojas, ketvirtame žingsnyje atlikdamas patikrinimą, klaidos neranda. Bet bitų sekos neatspėjus, 3 protokolo žingsnyje pareiškėjui tektų pakeisti *y* pasirinkimą, surandant skaičiaus, lygaus netuščiai parametrų v_i sandaugai, kvadratinę šaknį moduliu *n*

Tarkime, *P* spėja, kad antrame žingsnyje gauta bitų seka bus $(1,0,1,0,0, \dots ,0)$. Tuomet, nusiuntus *x* reikšmę, gautą anksčiau aprašytu metodu, *P* bus pasirengęs pateikti skaičiaus xv_1v_3 kvadratinę šaknį. Tačiau jeigu antrame žingsnyje gauta seka bus $(0,1,1,0,0, \dots ,0)$, tai yra, bus pareikalauta atsiųsti xv_2v_3 kvadratinę šaknį moduliu *n*, pareiškėjui (įvertinus iš anksčiau turėtą informaciją apie skaičiaus xv_1v_3 kvadratinę šaknį moduliu *n*), reikės apskaičiuoti $v_1v_2^{-1}$ kvadratinę šaknį moduliu *n*, ką padaryti nebus galima.

Taigi, kadangi galimų antrame protokolo žingsnyje gautų kombinacijų skaičius yra 2^k ir tik viena iš kombinacijų leidžia sėkmingai vykdyti protokolą, nežinant reikšmių $s_1, s_2, \dots, s_k$, tikimybė, kad protokolas bus sėkmingai įvykdytas sukčiaujant, lygi 2^{-k} (o atlikus *t* protokolo raundų, ši tikimybė sumažėja iki 2^{-kt}).

3.3. Skaičiaus ženklu paremtas dviejų milijonierių problemos protokolas su dalinėmis paslaptimis

Kitas svarbus baigiamojo darbo uždavinys buvo papildyti nagrinėjamos elektroninio balsavimo sistemos rinkimų rezultato nustatymo etapą (**3.1.3** skyrelis) GT problemos sprendimo protokolu. Kaip paminėta **2.5.2** skyrelyje, protokole, kuris bus naudojamas šiame darbe, dalyvauja 3 šalys: šalys A ir B, saugančios paslaptis *a* ir *b* bei trečioji šalis C, atliekanti pagalbinius skaičiavimus.

Protokolo eiga:

1. Trečioji šalis *C* sugeneruoja atsitiktinį skaičių R_A, kurį siunčia šaliai *A*.

2. *A* sugeneruoja atsitiktinį skaičių $R \in \mathbb{Z}/\{0\}$ ir siunčia šaliai *B* $(R, a \cdot R + R_A)$.
3. *B* prie antrosios žinutės, gautos antrajame protokolo žingsnyje, dalies prideda reiškinį $(-b \cdot R)$ ir siunčia šaliai *C* reiškinį $(a - b) \cdot R + R_A$.
4. *C* iš gautos išraiškos atima atsitiktinį skaičių R_A, sugeneruotą pirmame protokolo žingsnyje, ir patikrina, ar $(a - b) \cdot R > 0$.
5. *C* sugeneruoja dvi poras reikšmių: (r_a^0, r_b^0) bei (r_a^1, r_b^1), kurių sumos $r_a^0 + r_b^0 = 0 \pmod 2$ ir $r_a^1 + r_b^1 = 1$, o $r_a^0, r_b^0 r_a^1$ ir $r_b^1 \in \{0,1\}$ – atsitiktiniai bitai. Jeigu $(a - b) \cdot R < 0$, šaliai *A* siunčiama skaičių pora(r_a^0, r_a^1), o šaliai *B* - (r_b^0, r_b^1). Kitu atveju, šaliai *A* siunčiama skaičių pora (r_a^1, r_a^0), o šaliai *B* - (r_b^1, r_b^0).
6. Šalys *A* ir *B* padaro sprendimą: jeigu $sign(R) = 1$ $(R > 0)$, šalių paslapties dalys bus pirmieji žinutės, gautos iš *C* 5 protokolo žingsnyje, skaičiai. Tuo tarpu, jeigu $sign(R) = (-1)$ – antrieji šios žinutės skaičiai. Šie skaičiai toliau bus žymimi r_A ir r_B.
7. Šalys *A* ir *B*, apsikeitusios gautais duomenimis r_A ir r_B, apskaičiuoja funkcijos $f(a,b) = \begin{cases} 1, \text{jeigu } a > b \\ 0, \text{jeigu } a \leq b \end{cases}$ reikšmę, t.y. nustato, ar $a > b$.

3.3.1. Protokolo saugumo analizė

Iš tiesų, pateiktas protokolas tenkina dviejų milijonierių problemos sprendimo protokolui keliamus reikalavimas, suformuluotus **2.5.1** skyrelyje. Pirmiausiai, jeigu abi šalys *A* ir *B* vykdo visus protokolo žingsnius, protokolo rezultatas bus lygus 1 tada ir tik tada, kai šalies *A* saugoma paslaptis *a* bus didesnė už šalies *B* paslaptį *B*.

►

Tarkime, $a > b$, t.y. $a - b > 0$. Jeigu atsitiktinis skaičius $R > 0$, šalis *A* 5 protokolo žingsnyje gauna bitų porą (r_a^1, r_a^0), o šalis *B* – atitinkamai (r_b^1, r_b^0). Kadangi $R > 0$, šalių dalinės paslaptys – pirmieji žinučių skaičiai ir $f(a,b) = r_a^1 + r_b^1 = 1$. Tuo tarpu kai $R < 0$ $((a - b) \cdot R < 0)$, šalis *A* gauna bitų porą (r_a^0, r_a^1), o šalis *B* - (r_b^0, r_b^1). Kadangi parametras $R < 0$, šalių dalinės paslaptys – antrieji žinučių, gautų 5 protokolo žingsnyje, skaičiai, kurių suma lygi 1. Nesunku įsitikinti, jog atvirkščias teiginys taip pat teisingas: jeigu dalinių paslapčių suma lygi $1 (\text{mod } 2)$, tuomet $a - b > 0$.▲

Taip pat tenkinamas ir trečiasis reikalavimas: protokolo metu šalys *A* ir *B* nesužino viena kitos paslapčių (jų nesužino ir šalis *C*, atliekanti pagalbinius veiksmus). Protokolo vykdymo metu, jame dalyvaujančios šalys sužino skirtingas reikšmes bei reiškinius:

1. Šalis *A*, be savo saugomos paslapties *a*, papildomai sužino šalies *C* sugeneruotą atsitiktinį skaičių R_A, atsitiktinį skaičių *R* (kurį ir sugeneravo ši šalis) bei bitų porą (r_a^0, r_a^1) (tačiau nežino, kuris parametras yra pirmasis, o kuris – antrasis skaičius, kadangi 5 protokolo žingsnyje, priklausomai nuo reiškinio $(a-b)\cdot R$ ženklo, kinta ir parametrų $\{r_a^0, r_a^1\}$ tvarka).
2. Šalis *B*, be savo saugomos paslapties *b*, iš šalies *A* gauna atsitiktinį skaičių *R* bei reiškinį $a \cdot R + R_A$, bei iš šalies *C* gauna atsitiktinių bitų porą (r_b^0, r_b^1), tačiau nežino parametrų tvarkos (dėl tų pačių priežasčių, kaip ir šalis *A*).
3. Trečioji šalis *C* savo sugeneruotą atsitiktinį skaičių R_a, atsitiktinius bitus $r_a^0, r_b^0 r_a^1$ ir r_b^1 bei jų tvarką bei reiškinį $(a-b)R$.

Pastebėtina, kad šalis *C*, nors ir sužino reikšmę $(a-b)R$, negali nustatyti paslapčių *a* ir *b*, kadangi ji nežino parametro *R* reikšmės. Be to, šalis *C* negali išsiaiškinti ir santykio tarp šalių *A* ir *B* paslapčių, t.y. nustatyti, ar $a < b$, kadangi $\text{sign}(R) \in \{-1,1\}$. Vienintelis dalykas, ką gali išsiaiškinti šalis *C* apie paslaptis *a* ir *b* – patikrinti, ar $a = b$, tačiau net ir šiuo atveju paslapčių reikšmės išlieka neatskleistos.

Taip pat tenkinamas ir trečiasis reikalavimas, keliamas protokolams, skirtiems dviejų milijonierių problemos sprendimui (šalys *A* ir *B* nesužino viena kitos paslapčių), kadangi šalis *A* tiesiogiai iš *B* negauna jokios informacijos, o iš *C* gauna tik atsitiktinius skaičius. Tuo tarpu šalis *B* iš *A* gauna reikšmių porą $(R, a \cdot R + R_A)$, tačiau, nežinodama atsitiktinio skaičiaus R_A, paslapties *a* nustatyti negali.

3.4. Darbo priemonių pasirinkimas

Sparčiai tobulėjant kompiuterinei įrangai, keičiasi ir kompiuterių programinė įranga bei programavimo kalbos. Programavimo kalbos bei sistemos pasirinkimą dažniausiai lemia pastarųjų galimybės bei sprendžiamų uždavinių pobūdis. Darbe naudojamų algoritmų (Feige – Shamir identifikacinės schemos bei Yao dviejų milijonierių problemos sprendimo protokolo) ir nagrinėjamos elektroninio balsavimo sistemos tyrimo programinei realizacijai buvo pasirinkta Python programavimo kalba, sparčiai populiarėjanti pasaulyje. Šios kalbos pasirinkimą lėmė tai, kad ši programavimo kalba tinkama darbui su didelės apimties (2048 bitų ir didesnės) skaičiais, kas buvo itin aktualu atliekant darbe naudojamos vartotojų identifikacijos protokolo skaičiavimų efektyvumo tyrimą, naudojant šiuolaikinius saugumo standartus atitinkančius parametrus bei veiksmus atliekant su 2048 bitų ilgio sveikaisiais skaičiais.

3.5. Tyrimo aprašymas

Tiriant elektroninio balsavimo sistemą (Gang, 2008 bei atliekant jos tobulinimą), bus atsižvelgiama į dvi pagrindines charakteristikas: skaičiavimų efektyvumą bei priklausomybę nuo balsuotojų skaičiaus bei sistemos saugumo parametrų. Bus tiriamos laiko sąnaudos kiekviename iš EBS etapų, naudojant Python.3 programavimo kalbą bei kompiuterį su Intel(R) Core i3-2348M CPU, 2.30 GHz procesoriumi. Turint darbo metu sukurtas algoritmų programines realizacijas bei Python programavimo kalbos interpretatorių, skaičiavimo efektyvumo tyrimą bus galima pakartoti ir kitame kompiuteryje. Atlikus etapų atlikimo laiko skaičiavimus, bus ieškoma pagrindinių veiksnių, lemiančių skaičiavimų laiko augimą (tai gali būti balsuotojų, dalyvaujančių rinkimuose, skaičius, sistemos saugumo parametrų parinkimas ar tam tikra operacija, reikalinga analizuojamame EBS etape).

Taip pat bus atliekamas teorinė EBS analizė bei tiriama, kurie elektroninio balsavimo reikalavimai, suformuluoti **2.3** skyrelyje, yra tenkinami bei ieškoma EBS spragų, kurias būtų galima ištaisyti ar patobulinti.

Tiriamojoje dalyje taip pat bus pateikti darbe naudotų protokolų bei analizuotos EBS vykdymo skaitiniai pavyzdžiai, leidžiantys lengviau įsisavinti jų teorinius aprašymus.

4. Tiriamoji dalis

4.1. Protokolų bei analizuojamos EBS pavyzdžiai

4.1.1. Balsuotojų identifikacijos protokolo pavyzdys

Tarkime, norima atlikti vieno vartotojo identifikacijos protokolą, aprašytą **3.2** skyrelyje. Be to, tikrintojas V įsitikina pareiškėjo P tapatybės teisingumu, kai sukčiavimo tikimybė sumažinama iki $\frac{1}{2^4}$. Viešasis identifikacijos protokolo parametras - modulis $n = p \cdot q = 13 \cdot 17 = 221$. Vartotojas P sugeneruoja bei apskaičiuoja viešąjį ir privatųjį raktus, kuriuos sudaro po du skaičius: $PR = (s_1, s_2) = (15,4)$, $VR = (v_1, v_2) = \left(\frac{1}{s_1^2}, \frac{1}{s_2^2}\right) = (59^2, 166^2) = (166,152)$ Viešasis raktas $VR = (166,152)$ nusiunčiamas tikrintojui. Identifikacijos protokolą pradeda P:

1. P sugeneruoja atsitiktinį skaičių $r = 15$ ir apskaičiuoja $x = r^2 \bmod n = 225 \bmod 221 = 4$ ir siunčia *x* tikrintojui *V*.
2. V sugeneruoja atsitiktinių bitų seką $(b_1, b_2) = (1,1)$, kurią siunčia P.
3. P apskaičiuoja sandaugą $y = r \cdot \prod s_i^{b_i} \bmod n = 15 \cdot 15^1 \cdot 4^1 \bmod 221 = 16$, kurią siunčia *V*.
4. V patikrina, ar $x = y^2 \prod v_i^{b_i} \bmod n$: $y^2 \prod v_i^{b_i} \bmod n = 16^2 \cdot 166 \cdot 152 \bmod 221 = 35 \cdot 38 \bmod 221 = 4 = x$

Antrojo protokolo vykdymo rezultatai pateikti **4.1** lentelėje:

4.1 lentelė. Identifikacijos protokolo skaičiavimai

r	x	(b_1, b_2)	y	$y^2 \prod v_i^{b_i} \bmod n$
164	155	(1,0)	29	155

Kadangi kiekvieno protokolo raundo metu tikrintojas V sugeneruoja po 2 atsitiktinius bitus, tikimybė, kad pareiškėjas sėkmingai įvykdys kiekvieną iš protokolo raundų, nežinodamas privataus rakto $PR = (s_1, s_2)$, lygi $\frac{1}{2^2}$. Kadangi protokolas buvo kartojamas du kartus, tikimybė, kad abu kartus nebuvo aptikta bandymų sukčiauti lygi $\frac{1}{2^2} \cdot \frac{1}{2^2} = \frac{1}{2^4}$. Tuo tarpu pasikliovimo tikimybė, tai yra, tikimybė, kad pareiškėjas žino privatųjį raktą *PR*, lygi $1 - \frac{1}{2^4}$.

4.1.2. Skaičiaus ženklu paremto dviejų milijonierių problemos sprendimo su dalinėmis paslaptimis protokolo pavyzdys

Tarkime, šalies *A* saugoma paslaptis yra $a = 25$, o šalies *B* paslaptis - $b = 37$. Įvykdomas protokolas:

1. Trečioji šalis *C* sugeneruoja atsitiktinį skaičių $R_A = 45$ ir siunčia šį skaičių šaliai *A*.
2. *A* sugeneruoja atsitiktinį skaičių $R = -14$ ir siunčia žinutę $m = (R, a \cdot R + R_A) = (-14{,}25 \cdot (-14) + 45) = (-14, -305)$ šaliai *B*.
3. *B* apskaičiuoja $(a - b) \cdot R + R_A = -305 - (-14 \cdot 37) = 213$ ir siunčia šį skaičių šaliai *C*.
4. *C* atlieka patikrinimą: $(a - b) \cdot R = 213 - 45 = 168 > 0$.
5. *C* sugeneruoja bitų poras $(r_a^0, r_b^0) = (0{,}0)$ ir $(r_a^1, r_b^1) = (0{,}1)$. Kadangi $(a - b) \cdot R = 168 > 0$, šaliai *A* nusiunčiama skaičių pora $(r_a^1, r_a^0) = (0{,}0)$, o šaliai *B* – pora $(r_b^1, r_b^0) = (1{,}0)$.
6. Kadangi $\text{sign}(R) = -1$, šalių dalinės paslaptys bus antrieji 5 protokolo žingsnyje gauti skaičiai: $r_A = r_B = 0$.
7. Apskaičiuojama funkcijos reikšmė: $f(a, b) = r_A + r_B = 0 + 0 = 0 \Rightarrow a \leq b$.

   Taigi, įvykdžiusios šį protokolą, šalys žino, kad $a \leq b$. Norėdamos įsitikinti, kad $a \neq b$, šalys turėtų apsikeisti vaidmenimis bei įvykdyti protokolą antrą kartą ir įsitikinti, kad $b > a$.

   Antrasis protokolo vykdymas:

1. Trečioji šalis *C* sugeneruoja atsitiktinį skaičių $R_B = 19$ ir siunčia šį skaičių šaliai B.
2. B sugeneruoja atsitiktinį skaičių $R = 23$ ir siunčia žinutę $m = (R, b \cdot R + R_B) = (23{,}37 \cdot (23) + 19) = (23{,}870)$ šaliai *A*.
3. *A* apskaičiuoja $(b - a) \cdot R + R_B = 870 - 23 \cdot 25 = 295$ ir siunčia šį skaičių šaliai *C*.
4. *C* atlieka patikrinimą: $(b - a) \cdot R = 295 - 19 = 276 > 0$.
5. *C* sugeneruoja bitų poras $(r_a^0, r_b^0) = (1{,}1)$ ir $(r_a^1, r_b^1) = (1{,}0)$. Kadangi $(b - a) \cdot R = 276 > 0$, šaliai *A* nusiunčiama skaičių pora $(r_a^1, r_a^0) = (1{,}1)$, o šaliai *B* – pora $(r_b^1, r_b^0) = (0{,}1)$.
6. Kadangi $\text{sign}(R) = 1$, šalių dalinės paslaptys bus pirmieji 5 protokolo žingsnyje gauti skaičiai: $r_A = 1,\ r_B = 0$.

7. Apskaičiuojama funkcijos reikšmė: $f(a,b) = r_A + r_B = 1 + 0 = 1 \Rightarrow b > a$.

Taigi, galiausiai įvykdžius protokolą du kartus, šalys gauna nelygybių sistemą, iš kurios nustatomas galutinis rezultatas:

$$\begin{cases} a \leq b \\ b > a \end{cases} \Rightarrow a < b.$$

4.1.3. Nagrinėjamos elektroninio balsavimo sistemos pavyzdys

Tarkime, rinkimuose dalyvauja 3 balsuotojai: V_1, V_2, V_3 ir 2 kandidatai: (C_1, C_2), kuriuos atitinka balsavimo pasirinkimai $X = (X_1, X_2) = (7,16)$, t.y. rinkėjas, norėdamas balsuoti už kandidatą C_1, pasirenka skaičių 7, o norėdamas balsuoti už kandidatą C_2 - skaičių 16.

Balsuotojų registracijos metu, valdžios institucija A sugeneruoja atsitiktinius skaičius $(R_1, R_2, R_3) = (4,11,8)$. Taip pat, apskaičiuojamas parametras $R = n \cdot \sum_{i=1}^{n} R_i = 3 \cdot (4 + 11 + 8) = 69$ ir parametrai $(R_1, R_2, R_3) = (4,11,8)$, kartu su tuščiais balsavimo biuleteniais, nusiunčiami balsuotojams V_1, V_2 bei V_3.

Tarkime, kad pirmasis balsuotojas pasirinko kandidatą C_2, tuo tarpu antrasis bei trečiasis rinkėjai – kandidatą C_1. Rinkėjų balsavimo pasirinkimų skaidiniai surašomi į matricą:

$$x = \begin{pmatrix} 8 & 3 & 5 \\ 4 & 2 & 1 \\ 3 & 2 & 2 \end{pmatrix}.$$

Tuomet, kiekvienas rinkėjas V_i prie kiekvieno i – tosios eilutės elemento matricoje X prideda savo atsitiktinį skaičių:

$$x_R = x + \begin{pmatrix} R_1 & R_1 & R_1 \\ R_2 & R_2 & R_2 \\ R_3 & R_3 & R_3 \end{pmatrix} = \begin{pmatrix} 12 & 7 & 9 \\ 15 & 13 & 12 \\ 11 & 10 & 10 \end{pmatrix}.$$

Po duomenų apsikeitimo etapo, kiekvienas iš balsuotojų žino $k = 2n - 1 = 5$ matricos x elementus. Šios matricos su žinomais elementais bei nežinomais elementais, pažymėtais simboliu$*$, yra:

$$x_R^{(1)} = \begin{pmatrix} 12 & 7 & 9 \\ 15 & * & * \\ 11 & * & * \end{pmatrix}, x_R^{(2)} = \begin{pmatrix} * & 7 & * \\ 15 & 13 & 12 \\ * & 10 & * \end{pmatrix} x = \begin{pmatrix} * & * & 9 \\ * & * & 12 \\ 11 & 10 & 10 \end{pmatrix}.$$

Toliau, kiekvienas rinkėjas apskaičiuoja žinomų stulpelių sumas $S_{j,}\ j = \overline{1,3}$:

$$S_1 = 12 + 15 + 11 = 38, S_2 = 30, S_3 = 31.$$

Balsuotojams pasidalinus apskaičiuotomis sumomis S_j, kiekvienas gali apskaičiuoti sumą

$$D + R = 38 + 30 + 31 = 99.$$

Balsavimo pradžioje, valdžios institucija I turėjo parinkti slenksčio konstantą $M = \max(X_1, X_2) \cdot \left\lceil \frac{n}{2} \right\rceil + \min(X_1, X_2) \cdot \left(n - \left\lceil \frac{n}{2} \right\rceil\right) = \max(7,16) \cdot \left\lceil \frac{3}{2} \right\rceil + \min(7,16) \cdot \left(3 - \left\lceil \frac{3}{2} \right\rceil\right) = 16 \cdot 2 + 7 \cdot 1 = 39$. Šiuo balsavimo atveju, kadangi yra du galimi balsavimo pasirinkimai: 7 arba 16 bei trys balsuotojai, jeigu balsų suma D yra didesnė arba lygi $16 \cdot 2 + 7 = 39$, vadinasi bent du rinkėjai balsavo už kandidatą C_2, kurį atitinka skaičius 16, kitu atveju – bent du rinkėjai pasirinko kandidatą C_1, kurį atitinka skaičius 7.

Kiekvienas iš rinkėjų, žinodamas slenksčio konstantą $M = 39$ bei sumą $D + R = 99$, apskaičiuoja parametrą $T = D + R - M = 99 - 39 = 60$ (**2** rinkimų rezultato nustatymo žingsnis).

Toliau, kiekvienas iš rinkėjų nustato, ar parametras $T > R$. Šiuo atveju, valdžios istitucijos I paslaptis – parametras $R = 69$, o kiekvieno iš rinkėjų saugomos paslaptys yra parametras $T = 60$.

Įvykdomas *GT* protokolas su vienu iš rinkėjų (**3.3** skyrelis):

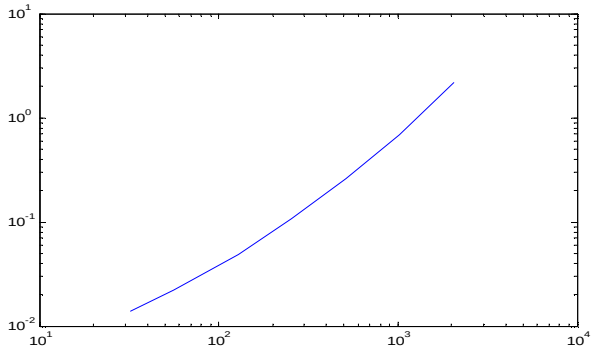
1. Balsų skaičiavimo institucija **VC** sugeneruoja atsitiktinį skaičių $R_A = 28$, kurį siunčia šaliai *A* (valdžios institucijai *I*).
2. *A* sugeneruoja atsitiktinį skaičių $U = -5$ ir siunčia šaliai *B* (vienam iš balsuotojų) pranešimą $(U, R \cdot U + R_A) = (-5, -317)$.
3. *B* prie antrosios žinotės, gautos antrajame protokolo žingsnyje, dalies prideda reiškinį $(-T \cdot U)$ ir siunčia šaliai **VC** reiškinį $(R - T) \cdot U + R_A = -317 - 60 \cdot (-5) = -17$..
4. **VC** iš gautos išraiškos atima atsitiktinį skaičių R_A, sugeneruotą pirmame protokolo žingsnyje, ir patikrina, ar $(R - T) \cdot U > 0$: $-17 - 28 < 0 \Rightarrow (R - T) \cdot U < 0$.
5. **VC** sugeneruoja dvi poras atsitiktinių bitų: $(r_a^0, r_b^0) = (0,0)$ bei $(r_a^1, r_b^1) = (0,1)$ ir, kadangi Jeigu $(R - T) \cdot U < 0$, šaliai *A* siunčiama skaičių pora$(r_a^0, r_a^1) = (0,0)$, o šaliai *B* - $(r_b^0, r_b^1) = (0,1)$.
6. Kadangi $sign(U) = -1$ $(U < 0)$, šalių paslapties dalys bus antrieji žinučių, gautų iš **VC** 5 protokolo žingsnyje, skaičiai: $r_A = 0$ ir $r_B = 1$.
7. Šalys *A* ir *B*, apsikeitusios gautais duomenimis r_A ir r_B, apskaičiuoja funkcijos $f(R,T)$ reikšmę: $f(R,T) = r_A + r_B = 1$. Taigi, nustatyta, kad $R > T$. Kadangi $T < R$, rinkėjų balsų suma D mažesnė už parinktą slenksčio konstantą M ir nustatoma, kad dauguma rinkėjų balsavo už pirmąjį kandidatą C_1.

4.2. Elektroninio balsavimo sistemos etapų analizė bei modifikacija

4.2.1. Vartotojų identifikacija

Nagrinėjamos ir **3.1** skyrelyje aprašytos elektroninio balsavimo sistemos vartotojų registracijos etape tik užsiminta apie rinkėjų identifikaciją (tapatybės ir teisės balsuoti patikrinimą), tačiau konkretaus metodo, kaip tai bus atliekama, nėra. Taigi, siekiant, kad būtų tenkinamas **2.3** skyrelyje suformuluotas elektroninio balsavimo schemos tinkamumo reikalavimas (balsuoti gali tik balso teisę turintys rinkėjai), buvo įvesta rinkėjų identifikacija, taikant nulinio atskleidimo įrodymus. Tam šiame darbe buvo naudojama Feige – Fiat – Shamir identifikavimo schema (Trappe, 2006).

Tiriant vartotojų identifikacijos efektyvumo priklausomybę nuo parametrų (buvo daroma prielaida, kad laikas, reikalingas vartotojų identifikacijai atlikti, priklauso nuo schemos saugumo parametro – modulio *n* – ilgio bitais, skaičiaus *k*, nurodančio, kiek privačių duomenų $s_1, s_2, \dots, s_k$ turi kiekvienas vartotojas bei *t*, nurodančio, kiek kartų bus kartojamas identifikacijos protokolas), identifikacijos etapas buvo išskaidytas į du mažesnius etapus. Pirmajame etape, atliekamame tik vieną kartą, buvo generuojami sistemos saugumo parametrai: pirminiai skaičiai p ir q, apskaičiuojamas modulis $n = pq$ sugeneruojami atsitiktiniai skaičiai $(s_1, s_2, \dots, s_k)$ bei apskaičiuojami parametrai $(v_1, v_2, \dots, v_k)$, $v_i = s_i^{-2} \bmod n$. Antrajame etape atliekamas identifikacijos protokolas. Tiriant antrojo etapo veikimo efektyvumą, buvo padaryta prielaida, kad tikrintojas *V* įsitikina pareiškėjo tapatybės teisingumu, kai sukčiavimo tikimybė sumažinama iki 2^{-20}. Tiriant pirmojo identifikacijos etapo veikimą, pirmiausiai buvo tiriama parametrų generavimo laiko priklausomybė nuo modulio *n*. Buvo naudojami 7 skirtingo ilgio: (32, 56, 128, 256, 512, 1024 ir 2048 bitų) moduliai, schemoje dalyvaujant 100 rinkėjų, turinčių po 5 privačius duomenis. Bandymas su skirtingo ilgio raktais buvo atliekamas po 10 kartų bei apskaičiuojamas vidutinis laikas. Rezultatai pateikiami **4.2** lentelėje bei **4.1 pav.** duomenis pavaizduojant logaritminėje skalėje:



4.1 pav. Pirmojo idendifikacijos etapo veikimo laiko priklausomybė

4.2 lentelė. Pirmo identifikacijos etapo veikimo laiko priklausomybė

Rakto ilgis bitais	Vidutinis laikas (s)
32	0.0139
56	0.0224
128	0.0488
256	0.1074
512	0.2588
1024	0.6897
2048	2.1595

Iš **4.1** grafike bei **4.2** lentelėje pateikiamų duomenų matome, jog nors naudojamos identifikacijos schemos parametrų generavimo laikas priklauso nuo viešojo rakto *n* ilgio, ir auga greičiau, nei tiesiškai (laiko sąnaudos padidėja atitinkamai 2.66 ir 3.13 karto, lyginant 512 – 1024 ir 1024 – 2048 bitų ilgio poras).

Tačiau be laiko, reikalingo skaičiavimams atlikti, svarbu ir identifikacnės schemos saugumas, užtikrinantis, kad tikrintojas *V*, žinodamas viešus pareiškėjo *P* duomenis $(v_1, v_2, \dots, v_k)$, negalės apskaičiuoti slaptų duomenų $s_i = \frac{1}{v_i^2} \bmod n$. Todėl toliau bus analizuojamas algoritmų veikimas, kai modulio *n* ilgis – 1024 arba 2048 bitai (atsižvelgiant į JAV Nacionalinio Standartų ir Technologijos instituto (NIST) rekomendacijas, iki 2010 metų buvo siūloma naudoti 1024 bitų ilgio modulį *n*, tačiau nuo 2011 metų naudoti jau 2048 bitų ilgio modulį, kurio turėtų pakakti iki 2030 metų) (Barker, Dang, 2015).

Antrajame identifikacinės schemos etape, kiekvienas rinkėjas bando įtikinti tikrintoją, jog žino privačių duomenų $(s_1, s_2, \dots, s_k)$ rinkinį. Kaip minėta anksčiau, daroma prielaida, kad rinkėjas, atliekantis pareiškėjo *P* vaidmenį, įtikina tikrintoją savo tapatybės teisingumu, kai sukčiavimo tikimybė sumažinama iki 2^{-20}. Kadangi ši tikimybė priklauso nuo pareiškėjo privačių duomenų skaičiaus *k* ir identifikacijos protokolo kartojimų skaičiaus *t*, bus tiriamas identifikavimo laikas, esant skirtingiems parametrams *k* ir *t*. Tyrimo rezultatai, kai buvo kiekvienu atveju buvo bandoma identifikuoti 100 rinkėjų, pateikiami **4.3** lentelėje:

4.3 lentelė. Vartotojų identifikacijos priklausomybė

Rakto ilgis bitais	*k*	*t*	Pirmo etapo laikas (s)	Antro etapo laikas (s)	Bendras laikas (s)
2048	1	20	0.432	0.532	0.964
2048	2	10	0.862	0.32	1,182
2048	4	5	1,696	0.217	1.913
2048	5	4	2.153	0.194	2.347
2048	10	2	4.2312	0.146	4.377

Iš **4.3** lentelėje pateiktų duomenų pastebime, jog didėjant privačių duomenų kiekiui, auga ir laikas, reikalingas identifikacijai atlikti. Šio laiko augimą lemia pirmojo identifikacijos etapo skaičiavimai, tai yra, sistemos saugumo parametrų bei vartotojų viešų ir privačių parametrų generavimas. Nors šis etapas atliekamas tik vieną kartą (prieš prasidedant rinkimams), tačiau norint apskaičiuoti parametrus $s_i = \frac{1}{v_i^2}$, reikia rasti atvirkštinį elementą moduliu *n*. Ši operacija ir lemia bendro laiko, reikalingo skaičiavimams, augimą. Tačiau, nors veiksmai atliekami greičiausiai (nevertinant laiko, kurio reikia, norint apsikeisti pranešimais identifikacijos protokolo metu), kai parinkti parametrai $k = 1, t = 20$, tokiu atveju reikalingas ir didžiausias komunikacijų tarp pareiškėjo *P* ir tikrintojo *V* skaičius (kiekvieno identifikacijos protokolo raundo metu atliekamos 3 komunikacijos, taigi iš viso susidaro 60 komunikacijų tarp tikrintojo ir kiekvieno iš rinkėjų). Tuo tarpu kitu kraštutiniu atveju ($k = 10, t = 2$) išauga tikimybė, kad pareiškėjas nežino kažkurio iš skaičių s_i, kadangi protokolą pakartojus 2 kartus, tikimybė, kad abu kartus vienas iš gautų bitų b_i bus lygus 0, lygi $\frac{1}{4}$.

Taigi, atsižvelgus į šių parametrų kombinacijų ($k = 1, t = 20$ bei $k = 10, t = 2$) trūkumus, siūloma identifikaciją vykdyti naudojant parametrus $k = 4, t = 5$. Tuomet skaičiavimų, reikalingų identifikacijai atlikti, laikas, naudojant 2048 bitų ilgio raktą, bus apytiksliai 1.9 sekundės.

4.2.2. Vartotojų registracija ir balsavimas

Atlikus balsuotojų identifikaciją (**3.1** skyrelis), analizuojamoje elektroninio balsavimo sistemoje kiekvienam iš rinkėjų $V_i, i = \overline{1,n}$ institucija *I* sugeneruoja atsitiktinį skaičių bei apskaičiuoja parametrą R_i

$$R = n \cdot \sum_{i=1}^{n} R_i$$

Originalioje elektroninio balsavimo sistemoje kiekvienas rinkėjas, pasirinkęs vieną iš dviejų galimų balsavimo galimybių, priklausančių aibei $X = \{X_1, X_2\}$, savo balsavimo pasirinkimą x_i išskaido į *n* atsitiktinių dalių bei gaunamas balsavimo pasirinkimo skaidinys $(x_{i1}, x_{i2}, \dots, x_{in})$. Tuomet prie kiekvienos iš skaidinio dalių x_{ij} pridedamas atsitiktinis skaičius R_i bei gaunamas naujas skaidinys: $(x_{i1} + R_i, x_{i2} + R_i, \dots, x + R_i)$. Taip pat pastebėtina, jog norint atlikti balsavimo pasirinkimo x_i išskaidymą dalimis, x_i turi būti bent 2 – 3 kartus didesnis už dalių skaičių *n*.

Siekiant sumažinti atliekamų veiksmų skaičių, siūloma atlikti modifikaciją: prie rinkėjo V_i balsavimo pasirinkimo x_i pirmiausiai pridėti atsitiktinį skaičių $n \cdot R_i$ ir tuomet atlikti modifikuoto balsavimo pasirinkimo $x_i + n \cdot R_i$ išskaidymą į *n* atsitiktinių dalių. **4.3** lentelėje pateikiami originalaus bei modifikuoto skaidinių sudarymo efektyvumo tyrimo rezultatai.

4.4 lentelė. Skaidinių sudarymo algoritmų palyginimas

Bandymo nr.	Originalaus metodo laikas	Modifikuoto metodo laikas	Skirtumas
1	4.506	4.218	0.288
2	4.33	4.236	0,094
3	4.299	4.1272	0.172
4	4.35	4.36	-0.01
5	4.307	4.271	0.036

Iš tyrimo rezultatų matome, jog nors skaidinių sudarymo algoritmų laikai skiriasi (skirtumai gali priklausyti nuo atsitiktinių skaičių R_i bei balsavimo pasirinkimų kombinacijų), tačiau dažniausiai modifikuotas algoritmas yra greitesnis už pradinėje elektroninio balsavimo schemoje pasiūlytą algoritmą. Tyrimas buvo atliekamas esant 1000 balsuotojų bei parenkant skirtingus atsitiktinius skaičius R_i ir leistinus balsavimo pasirinkimus (atsitiktinių skaičių bei balsavimo pasirinkimų generavimas nebuvo įtrauktas į lyginamų algoritmų veikimo laiką).

Be greitesnio veiksmų atlikimo, modifikuotas algoritmas taip pat leidžia galimų balsavimo pasirinkimų aibei priskirti mažesnius skaičius (tarkime, 0 ir 1, atitinkančius „taip arba ne“ balsavimo pasirinkimus), kadangi esant trims ir daugiau rinkėjų bei mažiems balsavimo pasirinkimams (tarkime, $\{0,1\}$), kiekvieno rinkėjo skaidinys $(x_{i1}, x_{i2}, \dots, x_{in})$, priklausomai nuo balsavimo pasirinkimo, bus arba (0,0,...,0), arba (0,...,1,0,...,0). Taigi, atlikus naujo skaidinio formavimą pagal originalią elektroninio balsavimo sistemą, naujas skaidinys bus arba $(R_i, R_i, \dots, R_i)$, arba $(R_i, \dots, R_i + 1, \dots, R_i)$. Todėl bet kurie likę balsuotojai, V_k, V_l, $k, l \neq i$, iš balsuotojo V_i gavę jo pasirinkimo skaidinio dalis $x_k + R_i$ bei $x_l + R_i$ bei pasidalinę šiais duomenimis, galės nustatyti slaptą atsitiktinį skaičių R_i, o tuo atveju, kai $x_k + R_i \neq x_l + R_i$ – ir

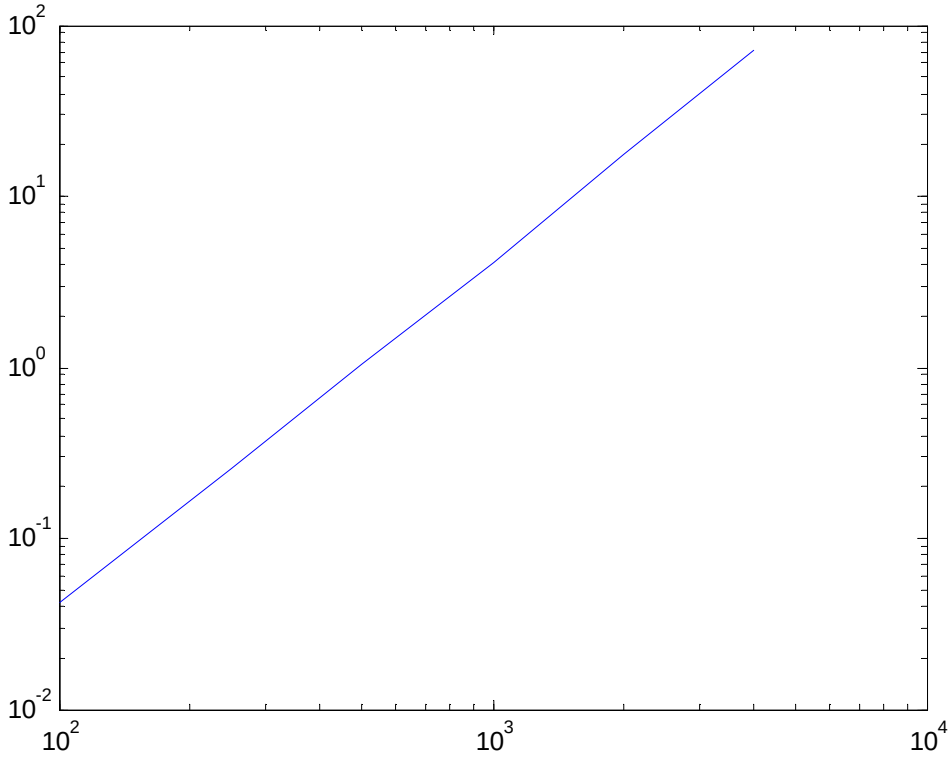
tai, jog rinkėjo V_i balsavimo pasirinkimas lygus 1. Tuo tarpu skaidinį sudarius modifikuotu būdu, šito padaryti nepavyks.

Iš kitos pusės, galimų skaidinių skaičių galima padidinti padarius prielaidą, kad skaidyti galima ir į neigiamas dalis. Tokiu atveju balsavimo pasirinkimo 0 skaidinys galėtų būti $(1, -4{,}3)$ ir rinkėjo balsavimo pasirinkimą bus galima nustatyti tik jeigu bus žinomos visos skaidinio dalys.

Dėl to, siekiant išlaikyti rinkėjų balsus paslaptyje, balsavimo pasirinkimo x_i skaidinyje bus leistinos ir neigiamos reikšmės, tačiau, siekiant išvengti galimų skaičiavimo paklaidų, apsiribojama sveikaisiais skaičiais. Taip pat, naudojamas šiek tiek efektyvesnis, modifikuotas skaidinio sudarymo algoritmas. Toliau, **4.5** lentelėje, pateikiami laiko, reikalingo balsavimo etapo skaičiavimams įvykdyti, priklausomybės nuo rinkėjų skaičiaus, duomenys bei rezultati atvaizduojami grafiškai, logaritminėje skalėje.

4.5 lentelė. Balsavimo etapo priklausomybė nuo rinkėjų skaičiaus

Rinkėjų skaičius	Balsų paskelbimo laikas (s)
100	0.042
250	0.257
500	1.034
1000	4,14
2000	17.46
4000	71,42



4.2 pav. Balsavimo etapo priklausomybė nuo rinkėjų skaičiaus

Iš gautų rezultatų matome, jog balsuotojų skaičiaus didėjimas stipriai veikia balsų paskelbimo laiko sąnaudas. Įvertinus galimas laiko matavimo paklaidas, galima daryti prielaidą, kad rinkėjų skaičiui padvigubėjus, laiko sąnaudos išauga 4 kartus. Šiam laiko sąnaudų didėjimui didžiausią įtaką daro balsavimo pasirinkimų skaidinių sudarymas: esant 100 rinkėjų, kiekvienas rinkėjas savo balsavimo pasirinkimą turi išskaidyti į 100 dalių, tai yra, atlikti po 99 skaidymo į atsitiktines dalis operacijas. Iš viso tokiu atveju reikia atlikti $100 \cdot 99 = 990$ skaidymo operacijų. Analogiškai, rinkimuose dalyvaujant 200 rinkėjų, iš viso reikės atlikti $200 \cdot 199 = 39800$ skaidymo dalimis operacijų. Taigi, rinkėjų skaičiui padvigubėjus, skaidymo operacijų skaičius išauga 40 kartų. Tai siejasi ir su bendrų balsavimo etapo laiko sąnaudų didėjimu.

Vienas pagrindinių analizuojamos sistemos balsavimo etapo trūkumų – nėra numatyta rinkėjo balso teisingumo patikrinimo. Tai yra, negalima patikrinti, ar rinkėjo V_i balsavimo pasirinkimas x_i priklauso galimų balsavimo pasirinkimų aibei. Pagrindinė priežastis, komplikuojanti šį patikrinimą - analizuojamoje sistemoje užšifruotą balsų sumą $D + R$ apskaičiuoja ne valdžios institucija, bet patys rinkėjai (**3.1.3** skyrelis), tuo tarpu valdžios institucija, kurai rinkėjas turėtų įrodyti, jog balsavimo pasirinkimas yra teisėtas, balsų sumos skaičiavime nedalyvauja (negali sužinoti balsų sumos anksčiau, negu ją apskaičiuoja rinkėjai). Taigi, valdžios institucija, net ir įsitikinusi balsavimo pasirinkimo x_i teisingumu, negalės įsitikinti, kad vėliau (sudarant balsavimo pasirinkimo skaidinį bei išsiunčiant jo dalis likusiems rinkėjams) bus sudaromas to paties balsavimo pasirinkimo skaidinys, kurio teisingumas buvo įrodytas. Balsavimo pasirinkimo teisingumo patikrinti neišeis ir rinkėjams, dalyvaujantiems užšifruotos balsų sumos $D + R$ skaičiavime, kadangi rinkėjas V_j gauna tik vieną iš n rinkėjo V_i balsavimo pasirinkimo skaidinio dalių, t.y. dalį $x_{ij} + R_i$ (skaidinį sudarant pagal pradinės elektroninio balsavimo schemos siūlomą metodą), arba $(x_i + n \cdot R_i)_j$ (modifikuotas skaidinio sudarymas). Taigi, ši dalis gali būti tiek teisėto, tiek netinkamo balsavimo pasirinkimo skaidinio dalis. Šią problemą būtų galima išspręsti, jeigu užšifruotas balsas būtų siunčiamas vienai ar kelioms institucijoms, kurios, gavusios balsų šifrogramas bei įsitikinusios, kad jos atitinka teisėtą balsavimo pasirinkimą, galėtų iššifruoti gautų šifrogramų sumą. Tačiau tuomet tektų atsisakyti saugių keleto šalių skaičiavimų, taigi – vietoje nagrinėjamos elektroninio balsavimo schemos naudoti alternatyvias elektroninio balsavimo sistemas. Keletas alternatyvų – elektroninio balsavimo sistema, paremta homomorfine Paillier šifravimo sistema (Damgard, Jurik, Nielsen, 2003), arba elektroninio balsavimo sistema, paremta paslapties pasidalijimo schema (Schoenmakers, 1999).

4.2.3. Rinkimų rezultato nustatymas

Pradinėje elektroninio balsavimo sistemoje galutinį rinkimų rezultatą siūloma nustatyti išsprendus dviejų milijonierių problemą bei nustatant, ar balsų suma *D* yra didesnė, ar mažesnė už parinktą slenksčio konstantą *M*. Nors toks rinkimų rezultato nustatymas galimas, tačiau šio metodo trūkumas – negalima nustatyti, kiek ir kuris kandidatas gavo balsų. Iš kitos pusės, faktas, jog niekas nesužino balsų sumos (o tuo pačiu ir atskirų rinkėjų balsų) užtikrina, kad bus išsaugotas rinkėjų privatumas.

Yao dviejų milijonierių problemos sprendimui buvo pasirinktas A. Amirbekyan ir E. V. Castro pasiūlytas protokolas, pateiktas **3.3** skyrelyje. Šiame protokole dalyvauja trys subjektai: šalys *A* ir *B*, saugančios paslaptis bei siekiančios išsiaiškinti, kurios šalies paslaptis didesnė (tiriamos EBS atveju, šių šalių vaidmenis atlieka valdžios institucija I, sauganti parametrą $R = n \cdot \sum_{i=1}^{n} R_i$, o šalies *B* – vienas iš rinkėjų V, saugantis parametrą $T = (D + R) - M$) bei trečioji šalis *C*, atsakinga už atsitiktinių skaičių generavimą bei pagalbinius veiksmus. Kadangi tiriamos sistemos aprašyme buvo apibrėžta balsų skaičiavimo institucija VC, tačiau ji elektroninio balsavimo schemoje neatliko jokių veiksmų, buvo pasiūlyta ją panaudoti Yao protokole, atliekant šalies *C* vaidmenį.

Toliau, pateikiamos bendros laiko, reikalingo Yao protokolams atlikti, sąnaudos, esant skirtingam rinkėjų skaičiui.

4.6 lentelė. Yao protokolų skaičiavimų sąnaudos

Balsuotojų skaičius	Yao protokolų vykdymo laikas, s
100	0.002
1000	0,026
10000	0,255

Iš **4.6** lentelėje pateiktų rezultatų matome, kad Yao protokolų vykdymo laiko priklausomybė nuo balsuotojų skaičiaus (kiekvienam iš rinkėjų protokolą atliekant po vieną kartą) yra tiesinė. Taigi, net darant prielaidą, kad, norėdami įsitikinti rinkimų rezultatu, visi rinkėjai atlieka Yao protokolus su valdžios institucija, nekyla grėsmės, kad rinkimų rezultato nustatymas užtruks per ilgai.

4.3. Tiriamos elektroninio balsavimo sistemos reikalavimų analizė

Pagrindiniai reikalavimai, kuriuos turėtų tenkinti elektroninio balsavimo sistemos, buvo suformuluoti **2.3** skyrelyje. Pirmiausiai atliksime reikalavimų, kuriuos tenkina tyrinėta bei tobulinta EBS:

Visuotinumas – modifikavus elektroninio balsavimo sistemą, balsuotojų registracijos etape įgyvendinta vartotojų identifikacija, naudojant Feige – Fiat – Shamir vartotojų identifikacijos schemą. Tai užtikrina, kad balsavimo etape dalyvaus tik balso teisę turintys rinkėjai, kurių tapatybės patikrina valdžios institucija I.

Vieno rinkėjo – vieno balso principas – nagrinėjamoje EBS numatytas tik vienas balso paskelbimo būdas (žr. **3.1.2** skyrelį), taigi balsavimas keletu galimų būdų nėra įmanomas. Taip pat rinkėjas negali baluoti keletą kartų, kadangi balso paskelbimo metu kiekvienam likusiam balsuotojui išsiunčiama tam tikra balsavimo pasirinkimo dalis. Taigi, likę rinkėjai pastebės bandymą balsuoti pakartotinai.

Slaptumas – rinkėjų balsai išlieka paslaptyje, kadangi balsuotojas V_i kiekvienam iš likusių rinkėjų V_j atskleidžia tik $\frac{1}{n}$ - tąją, n – balsuotojų skaičius rinkimuose, savo balsavimo pasirinkimo dalį. Be to, netgi visi rinkėjai $V_j, j \neq i$, pasidalinę iš V_i gauta informacija tarpusavyje, negalės nustatyti šio rinkėjo balsavimo pasirinkimo. Tuo tarpu valdžios institucija I iš rinkėjų jokių pranešimų negauna ir sužino tik tai, ar balsų suma didesnė, ar mažesnė už slenksčio konstantą M, taigi sužinoti atskirų rinkėjų balsų negali. Taip pat nagrinėta EBS užtikrina, kad po balsavimo rinkėjas negalės įrodyti savo balsavimo pasirinkimo, kadangi rinkėjų balsai bei balsų suma lieka paslaptyje.

Patikrinamumas - Balsų skaičiavimo metu, kiekvienas iš rinkėjų gali apskaičiuoti užšifruotą sumą $D + R$, čia D – rinkėjų balsų suma, R – atsitiktinis skaičius, žinomas tik valdžios institucijai. Taigi, jeigu kurio nors iš rinkėjų balsavimo pasirinkimą būtų bandoma modifikuoti, balsą modifikavusio rinkėjo suma $D + R$ skirtųsi nuo kitų balsuotojų apskaičiuotų sumų, tad toks sukčiavimas būtų pastebėtas. Ši elektroninio balsavimo sistemos ypatybė užtikrina, kad bus tenkinamas individualus patikrinamumas: kiekvienas rinkėjas žinos, kad jo balsas nebuvo pakeistas ir į bendrą balsų sumą buvo įrašytas teisingai ir visi teisėti balsai suskaičiuoti tinkamai.

Sąžiningumas – kadangi balsų suma D lieka nežinoma nei rinkėjams, nei valdžios institucijai, o rinkimų nugalėtojas nustatomas tik visiems rinkėjams apskaičiavus sumą $D + R$, niekas negalės atskleisti tarpinio rinkimų rezultato.

Nors tyrinėta EBS tenkina nemažai elektroninio balsavimo sistemoms keliamų reikalavimų, tačiau joje nėra numatyta balso tinkamumo patikrinimo etapo. Tai reiškia, kad nėra

galimybės patikrinti, ar rinkėjo balsavimo pasirinkimas priklauso galimų balsavimo pasirinkimų aibei. Dėl to netenkinamas **tikslumo** reikalavimas, reiškiantis kad į balsų sumą bus įtraukti tik teisėti balsai. Taip pat tik iš dalies tenkinamas **pritaikomumo** reikalavimas. Iš **4.4** lentelėje pateiktų rezultatų matome, kad balsų paskelbimo etapo skaičiavimų apimtis, didėjant rinkimuose dalyvaujančių rinkėjų skaičiui (šio etapo skaičiavimų apimtis bei komunikacijų tarp balsuotojų apimtis didėja du kartus greičiau, nei dalyvių skaičius).

4.4. Rinkėjo balso tinkamumo patikrinimas

Atlikus detalią darbe tiriamos EBS analizę, išryškėjo du šios sistemos trūkumai. Didžiausia sistemos spraga – nėra numatyta rinkėjų balsų tinkamumo patikrinimo. Tai reiškia, jog iškyla grėsmė, kad galutinis rinkimų rezultatas bus nustatytas neteisingai. Šią prielaidą pagrindžia elementarus balsavimo pavyzdys. Tarkime, rinkimuose dalyvauja 3 kandidatai, o galimų balsavimo pasirinkimų aibė $X = \{0,1\}$, slenksčio konstanta $M = 2$. Balsavimo metu, rinkėjų paskelbti balsai buvo: $x_1 = x_2 = 0,\ x_3 = 2$. Šiuo atveju daugiausiai balsų surinko pirmasis kandidatas (daugumos balsavimo pasirinkimas buvo 0). Tačiau slenksčio konstanta $M = 2$, o rinkėjų balsų suma taip pat lygi 2, taigi, atlikus Yao protokolą, bus nustatyta, jog rinkimus laimėjo antrasis kandidatas, kurį atitinka balsavimo pasirinkimas $X_2 = 1$. Taigi, akivaizdu, kad sukčiaujantis rinkėjas gali pakeisti galutinį rinkimų rezultatą norima linkme ir balsų tinkamumo patikrinimas yra būtinas.

Kitas nagrinėjamos EBS trūkumas – greitai didėjančios skaičiavimų sąnaudos balsavimo etape, augant rinkėjų skaičiui (**4.5** lentelė). Toliau bus pasiūlyti du metodai šių trūkumų pašalinimui.

4.4.1. Pirmasis balso tinkamumo patikrinimo metodas

Tarkime, kad balsavimo pasirinkimų aibė *X* sudaryta taip, kad skirtumas tarp dviejų galimų balsavimo pasirinkimų lygus 1 ir balsavimo pasirinkimai išdėstyti didėjimo tvarka, t.y. $X = \{X_1, X_2\}, X_2 - X_1 = 1$.

Rinkėjas V_i balsavimo metu pasirenka vieną iš galimų balsavimo pasirinkimų $x_i \in X$ bei apskaičiuoja užšifruotą balsą $y_i = x_i + n \cdot R_i$ ir parametras y_i nusiunčiamas tarpinei valdžios institucijai, nežinančiai atsitiktinių skaičių R_i (jos vaidmenį gali atlikti balsų skaičiavimo institucija VC). Tuomet, norint patikrinti, ar balsavimo pasirinkimas $x_i \in X$, VC su valdžios institucija I atliekami du Yao protokolai: $Yao(y_i, (X_2 + 1) + n \cdot R_i)$ ir $Yao(y_i, X_1 + n \cdot R_i)$. Čia protokolas $Yao(a, b)$, pateiktas **3.3** skyrelyje, grąžina reikšmę 1, jeigu $a < b$ ir 0, jeigu $a \geq b$. Jeigu balsavimo pasirinkimas x_i yra galimas, I pirmojo protokolo metu įsitikins, kad

$Yao(y_i, (X_2 + 1) + n \cdot R_i) = 1$, tai yra, $x_i < X_2 + 1$, o antrojo protokolo metu – kad $Yao(y_i, X_1 + n \cdot R_i) = 0$, tai yra, $x_i \geq X_1$. Taigi, po abiejų Yao protokolų I žinos, kad balsavimo pasirinkimas $x_i \in [X_1, X_2 + 1)$, o įvertinus tai, jog $x_i \in \mathbb{Z}$, šis sąryšis ekvivalentus $x_i \in X$. Sėkmingai atlikus abu Yao protokolus, VC paskelbia užšifruotą balsavimo pasirinkimą y_i balsų lentoje, matomoje tik rinkėjams. Paskelbus visus balsus y_i, kiekvienas iš rinkėjų gali apskaičiuoti užšifruotą balsų sumą $D + R = \sum_{i=1}^{n} y_i$ bei nustatyti rinkimų nugalėtoją pradinėje elektroninio balsavimo sistemoje pateiktu būdu (**3.1.3** skyrelis).

Taigi, pasiūlytas metodas užtikrina, kad į galutinę balsų sumą $D + R$ bus įskaičiuoti tik tinkamai suformuoti balsai y_i. Deja, jis tinka tik tuo atveju, jeigu tarpinė institucija, dalyvaujanti balso tinkamumo patikrinime, yra sąžininga ir nemėgina sukčiauti. Viena iš tarpinės institucijos sukčiavimo galimybių – parametrą y_i VC gali perduoti valdžios institucijai. Tokiu atveju, sužinojusi parametrą $y_i = x_i + n \cdot R_i$, I, žinodama ir atsitiktinį skaičių R_i, gali nustatyti rinkėjo balsavimo pasirinkimą. Galimas ir kitas sukčiavimo atvejis – norėdama pakeisti galutinį rinkimų rezultatą, VC, atlikusi balso tinkamumo patikrinimą, gali parametrą y_i pakeisti ir balsų lentoje paskelbti ne y_i, bet $\widehat{y_i} = y_i + c$, $c \in \mathbb{Z}$. Tačiau nuo pastarosios sukčiavimo galimybės galima apsisaugoti, kadangi rinkėjai, matydami visus paskelbtus balsus y_i, galės pasitikrinti, ar jo balsas patenka į paskelbtų parametrų y_i sąrašą. Tam tereikia, kad kiekvieno rinkėjo parametras $y_i = x_i + R_i$ būtų skirtingas, kadangi esant dviems vienodiems parametrams (tarkime, $y_i = y_j$ vietoje vieno iš šių parametrų gali būti įrašytas bet koks kitas skaičius, nors abu rinkėjai - V_i ir V_j – matys, kad jų balsavimų pasirinkimai patenka į paskelbtą sąrašą). Tai galima užtikrinti atsitiktinių skaičių R_i generavimo metu patikrinant, ar kiekvienas iš skaičių R_i, $i = \overline{1, n}$ skiriasi bent per 2 vienetus.

Pirmojo balsų tinkamumo patikrinimo atveju atsisakoma užšifruoto balsavimo pasirinkimo y_i skaidymo dalimis. Tai sumažina laiko, reikalingo balsavimo etapo skaičiavimams atlikti, sąnaudas, o atskiri rinkėjų balsavimo pasirinkimai išlaikomi paslaptyje. Iš tiesų, iš užšifruoto balso $y_i = x_i + R_i$, nežinant atsitiktinio skaičiaus R_i, neįmanoma nustatyti balsavimo pasirinkimo x_i – rinkėjo V_i paslapties. Taigi, to negalės padaryti nei bet kuris iš rinkėjų, nei tarpinė valdžios institucija VC. Tuo tarpu Yao protokolas užtikrina, kad valdžios institucija I, žinanti atsitiktinius skaičius R_i, nesužinos užšifruoto balso y_i.

Kita galima grėsmė – nesąžininga valdžios institucija I gali paviešinti atsitiktinius skaičius R_i. Tokiu atveju, tarpinė institucija VC gali sužinoti rinkėjo balsavimo pasirinkimą bei tarpinį rinkimų rezultatą (pažeidžiami slaptumo ir sąžiningumo reikalavimai). Taigi, balso tinkamumo patikrinimui taikant šį metodą, turi būti daroma prielaida, kad abi institucijos – I ir VC – bus sąžiningos (tačiau apsisaugoma nuo galimo rinkėjų sukčiavimo).

Siekiant panaikinti valdžios institucijų sukčiavimo galimybę, buvo pasiūlytas kitas balso tinkamumo patikrinimo metodas.

4.4.2. Antrasis balso tinkamumo patikrinimo metodas

Tarkime, turime tokią pačią galimų balsavimo pasirinkimų aibę $X = \{X_1, X_2\}$, kaip ir **4.3.1** skyrelyje. Rinkėjas V_i balsavimo metu pasirenka $x_i \in X$ ir apskaičiuoja parametrą $y_i = x_i + n \cdot R_i$, kurį išskaido į 2 atsitiktines dalis: $y_i^{(p)}$ ir $y_i^{(v)}$, $y_i^{(p)} + y_i^{(v)} = y_i$, $y_i^{(p)}, y_i^{(v)} \in \mathbb{Z}$. Nusiuntus parametrą $y_i^{(v)}$ valdžios institucijai I, atliekami du Yao protokolai: $Yao\left(y_i^{(p)}, (X_2 + 1) - y_i^{(v)} + n \cdot R_i\right)$ ir $Yao\left(y_i^{(p)}, X_1 - y_i^{(v)} + n \cdot R_i\right)$. Pirmojo protokolo metu įsitikinama, kad $y_i^{(p)} + y_i^{(v)} < (X_2 + 1) + n \cdot R_i$, o po antrojo – kad $y_i^{(p)} + y_i^{(v)} \geq X_1 + n \cdot R_i$. Arba, atitinkamai $x_i < (X_2 + 1)$ ir $x_i \geq X_1$.

Tuomet valdžios institucija išskaido viešąją užšifruoto balsavimo pasirinkimo dalį $y_i^{(v)}$ į $n - 1$ dalių, kurios surašomos į balsų matricą ir paskelbiamos viešai prieinamoje balsų lentoje (i – toji šios matricos dalis būtų (x_{i1} ⋯ x_{i-1} * x_{i+1} ⋯ x_{in}), čia * – nepaskelbta ir tik rinkėjui V_i žinoma privati balsavimo pasirinkimo dalis $y_i^{(p)}$. Toliau kiekvienas iš rinkėjų apskaičiuoja tik jam žinomų stulpelių sumas $S_i = \sum_{j=1}^{n} x_{ij}$ ir, apjungus gautus rezultatus, gaunama užšifruotų balsų suma $\sum_{i=1}^{n} S_i = D + R$ ir nustatomas rinkimų nugalėtojas (**3.1.3** skyrelis).

Antrasis pasiūlytas balso tinkamumo patikrinimo metodas gali padėti apsisaugoti nuo netyčinių rinkėjo klaidų balsavimo pasirinkimo sudarymo etape. Deja, nėra numatyta mechanizmo, leidžiančio patikrinti, ar teisingai suskaičiuotos dalinės sumos S_i, taigi išlieka rinkėjų sukčiavimo galimybė šių sumų apskaičiavimo metu.

Pagrindinis šio metodo privalumas – atsisakoma tarpinės valdžios institucijos, kuri buvo reikalinga pirmajame balso tinkamumo patikrinimo metode. Taigi, sumažinamas galimai nesąžiningų šalių skaičius. Taip pat išlaikoma galimybė rinkėjams įsitikrinti, ar jų balsas į matricą, paskelbtą balsų lentoje, buvo įrašytas tinkamai, patikrinant, ar $y_i^{(v)} = \sum_{j \neq i} x_{ij}$. Be to, išlaikoma pradinės elektroninio balsavimo sistemos struktūra, paremta balsavimo pasirinkimų skaidymu į n dalių bei dalinių sumų S_i skaičiavimu.

Taigi, nors antrasis metodas apsaugo nuo nesąžiningų valdžios institucijų veiksmų ir užtikrina balsuotojų anonimiškumą, kyla grėsmė, kad rinkėjai mėgins sukčiauti po balso tinkamumo patikrinimo pakeisdami balsavimo pasirinkimą.

4.5. Pradinės ir modifikuotos EBS palyginimas

Ankstesniame skyrelyje buvo pasiūlyti du būdai išspręsti pagrindinį darbe analizuojamos elektroninio balsavimo sistemos trūkumą pridedant balso tinkamumo patikrinimo galimybę. Nors abu būdai leidžia patikrinti balsų tinkamumą, neatskleidžiant rinkėjo balsavimo pasirinkimo, tačiau jie turi ir trūkumų: pirmuoju atveju kyla grėsmė, kad nesąžiningi tarpinės valdžios institucijos VC veiksmai gali atskleisti atskirų rinkėjų balsus. Tuo tarpu antrasis metodas, nors ir apsaugo nuo galimų klaidų balso suformavimo etape, neužtikrina, kad balsavimo pasirinkimas vėliau nebus pakeistas. **4.6** lentelėje pateikti reikalavimai, kuriuos pilnai (arba iš dalies) tenkina pradinė bei modifikuota EBS, su įvestu balso tinkamumo patikrinimu.

4.6 lentelė. EBS reikalavimų palyginimas

Reikalavimas	Pradinė EBS	Pirmasis metodas	Antrasis metodas
Visuotinumas	+	+	+
Vienas rinkėjas – vienas balsas	+	+	+
Slaptumas	+	+/-	+
Patikrinamumas	+	+	+
Sąžiningumas	+	+/-	+
Tikslumas	-	+	+/-
Pritaikomumas	+/-	+	+/-

Taigi, matome, kad pritaikius balso tinkamumo patikrinimą, arba visiškai (pirmasis metodas), arba iš dalies (antrasis metodas) užtikrinama, kad rinkėjų balsai priklausys galimų balsavimo pasirinkimų aibei. Tačiau atsiranda kitų sistemos spragų: pritaikius pirmąjį metodą, iškyla grėsmė rinkėjų privatumui, be to, atsiranda galimybė nustatyti tarpinį rinkimų rezultatą. Tuo tarpu antrasis metodas tik dalinai apsaugo nuo galimo rinkėjų sukčiavimo.

5. Išvados

Baigiamojo darbo metu buvo pateikti pagrindiniai elektroninėms balsavimo sistemoms keliami reikalavimai. Tobulinant pradinę elektroninio balsavimo sistemą, buvo pridėtas vartotojų identifikacijos etapas, pritaikant Feige – Fiat – Shamir vartotojų identifikacijos schemą bei įgyvendintas galutinio rinkimų rezultato apskaičiavimo etapas, leidžiantis efektyviai nustatyti rinkimų nugalėtoją. Ištyrus pradinės elektroninės balsavimo sistemos atitikimą keliamiems reikalavimams, pastebėta, kad ji atitinka visus keliamus reikalavimus, išskyrus tikslumą (nėra numatyta balso tinkamumo patikrinimo) ir pritaikomumą (sistema netinkama didelio masto (daugiau, nei 10000 rinkėjų) dėl smarkiai išaugančių skaičiavimo laiko sąnaudų balsavimo etape). Siekiant ištaisyti šiuos trūkumus, buvo pateikti du galimi balso tinkamumo patikrinimo metodai, kuriuose buvo pritaikytas Yao dviejų milijonierių sprendimo protokolas. Tačiau taikant pirmąjį metodą, reikėtų atsižvelgti į galimas grėsmes vartotojų balsavimo privatumui bei išankstinio rinkimų rezultato nustatymo galimybę. Tuo tarpu antrasis metodas apsaugo tik nuo netyčinių klaidų balso suformavimo etape.

6. Literatūra

1. Sampygethaya K., Poovendran R., „A Framework and taxonomy for comparison of electronic voting schemes“ // Computers & Security, Vol. 25, Issue 2, p. 137 – 153, 2006

2. Quadah, G. Z., Taha R., „Electronics voting systems: Requirements, design and implementation“ // Computer Standards & interfaces, Vol. 29, Issue 3, p. 376 – 386, 2007

3. Gritzalis A. D., „Principles and requirements for a secure e – voting system“ // Computers & Security, Vol. 26, Issue 6, p. 539 – 556, 2002

4. Sako K., Killian J., „Receipt – free mix – type voting scheme – a practial solution to the implementation of a voting booth“ // Advanes in Cryptology – EUROCRYPT’95, Vol. 921, p. 393 – 403, 1995.

5. Gang C., „An Electronics Voting Scheme Based On Secure Multi – Party Computation“ // International Symposium on Computer Service and Computational Tehnology, 2008

6. Yao A. C., „Protocols for secure computations“ (extended abstract) // 21st Annual IEEE Symposium on Foundations on omputer Sciene, IEEE Press, 1982, p. 160 – 164

7. Amirbekyan, A., Estivill – Castro, V., „Practical protocol for Yao’s millionaires problem enables secure multi-party computation of metrics and efficient privacy-preserving k-NN for large data sets“ // Knowledge and Information Systems, Vol. 21, Issue 3, p. 327 – 363, 2009

8. Goldwasser, S., Micali S., Rackoff C., „The Knowledge Complexity of Interactive Proof Systems“ (Extended Abstract), *SIAM Journal of Computing,* Vol. 18, No. 1, pp. 186–208

9. Oppliger R., „Contemporary Cryptography“, 2005, p. 426–439

10. Brandon, L. J. J., „Implementing Zero – Knowledge Authentication with Zero Knowledge“ // The Python Papers Monograph, ISSN: 1837–7092, Vol 2 (2010), p. 1–2

11. Barrat i Esteve, J., Goldsmith B., Turner J., „International Experience with E – Voting. Norvegian E – vote Project.“, 2012.

12. Volkammer, M., Grimm, R., „Multiple Casts in E – Voting: Analyzing Chances“ // 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC, 2006, p. 97 – 107

13. Trappe, W., „Introduction to Cryptography with Coding Theory“, 2006, p. 319 – 321.

14. Barker, E., Dang, Q., „Recommendation for key management“, 2015

15. Damgard, I., Jurik, M., Nielsen, J. B., „A Generalization of Paillier‘s Public Key Cryptosystem with Applicatios to Electronic Voting“ // Research in Computer Science, 2003

16. Schoenmakers, B., „A Simple Publicly Verrifiable Secret Sharin Scheme and its Application to Electronic Voting“// Advances in Cryptology – CRYPTO’99, Vol. 1666, p. 148-164, 1999.

17. Goldreich, O., Oren, Y., „Definitions and Properties of Zero – Knowledge – Proof Systems“

18. Halderman, J. A., Hurst, H. Et al., „Independent Report on E – Voting in Estonia“ [online]. [viewed 20 05 2015]. Available from https://estoniaevoting.org/findings/summary/

19. Wu Z.Y., Wu J.C., Lin S.C., Wang C., „An electronic voting mechanism for fighting bribery and coercion“ // Journal of Network and Computer Aplications 2014; 40:139–150