KAUNO TECHNOLOGIJOS UNIVERSITETAS
VYTAUTO DIDŽIOJO UNIVERSITETAS
VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

JONAS MULERAVIČIUS

ELEKTRONINĖS PINIGINĖS REALIZACIJA E. VERSLO SISTEMOJE

Daktaro disertacijos santrauka
Gamtos mokslai, Informatika (N 009)

2019, Kaunas

Disertacija rengta 2014−2018 metais Kauno technologijos universiteto Matematikos ir gamtos mokslų fakultete Taikomosios matematikos katedroje.

Mokslinis vadovas:
prof. dr. Eligijus SAKALAUSKAS (Kauno technologijos universitetas, Gamtos mokslai, Informatika, N 009).

Redagavo:
Vaiva Teniukaitė
Deimantė Petrikienė

Disertacija ginama viešame Informatikos (N 009) mokslo krypties tarybos posėdyje, kuris vyks 2019 m. Lapkričio 22 d., 9 val. Kauno technologijos universiteto Rektorato salėje.

Adresas: K. Donelaičio g. 73-402, 44249 Kaunas, Lietuva.
Tel. (370) 37 300 042; faks. (370) 37 324 144; el. paštas: doktorantura@ktu.lt.

Disertacijos santrauka išsiųsta 2019 m. spalio 22 d.

Su disertacija galima susipažinti internetinėje svetainėje http://ktu.edu ir Kauno technologijos universiteto bibliotekoje (K. Donelaičio g. 20, 44239 Kaunas).

SĄVOKOS IR SUTRUMPINIMAI:

MAC − pranešimų autentifikavimo kodas;

SHA-2 − Maišos funkcijos algoritmas;

TTP − patikima trečioji šalis;

Stebėtojas (angl. Observer) – patikima trečioji šalis, įdiegta įrenginyje;

BAN (Burrowso – Abadi'o – Needhamo) logika − taisyklių rinkinys, skirtas informacijos mainų protokolams apibrėžti ir analizuoti;

CFN − Chaumo, Fiato ir Naoro elektroninių pinigų sistema;

CHL − Camenischo, Hohenbergerio ir Lysyanskaya'os elektroninių pinigų sistema;

q, p – tokie dideli pirminiai skaičiai, kad p tenkintų svarbią savybę $p = 2q + 1$;

G_q – ciklinė subgrupė multiplikatyviosios grupės $\mathbb{Z}_p^*$;

G – generatorius iš multiplikatyviosios grupės $\mathbb{Z}_p^*$;

$h()$ – santraupos funkcija;

$Sig_{ElG}^{X}(m)$ – ElGamalio parašo funkcija, kurioje m atitinka pranešimą, o X – pasirašančiojo ElGamalio privatųjį raktą;

$Ver_{ElG}^{A}(s, m)$ − ElGamalio parašo tikrinimo funkcija, kurioje m atitinka pranešimą, s – parašą, A – pasirašančiojo ElGamalio viešąjį raktą;

i – transakcijos – i-tasis numeris;

$PrK_P = x_P$ − Pirkėjo laikinas privatus raktas;

$PuK_P = \{G, A_P = G^{x_P}\}$ − Pirkėjo laikinas viešasis raktas;

$PrK_O = x_O$ − Stebėtojo privatus raktas;

$PuK_O = \{G, A_O = G^{x_O}, A_P^{Id_P}\}$ − Stebėtojo viešasis raktas;

Id_P − unikalus Stebėtojo lusto identifikavimo numeris;

m_i − Pirkėjo mokamų pinigų suma;

$\widetilde{m}_i$ − tikroji Pirkėjo perkamų produktų kaina;

t_i − elektroninių pinigų išėmimo laiko momentas;

$m_i || t_i$ − sujungtas sumos ir laiko momento kintamasis;

t_{w0}, t_{p0}, t_{d0} − paskutinio elektroninių pinigų išėmimo (mokėjimo, pinigų padėjimo) protokolo laikas;

m_{max}^{P}, m_{max}^{V} − atitinkamai Pirkėjo ir Pardavėjo pinigų suma elektroninėje piniginėje;

$\xi_i^{(1)}, \xi_i^{(2)}$ − Schnorro identifikavimo protokolo atsitiktinės reikšmės;

S_m – pranešimo m parašas;

$MOD_E(y, z)$ – funkcija, grąžinanti moduliarinės funkcijos veikimo laiką $r = g^k \bmod p$;

$M(w), A(w), Mod(w)$ – funkcija, grąžinanti sandaugos, sumos ir modulio operacijų laikus pagal nurodytus kintamųjų dydžius bitais w;

$l(w)$ – funkcija, kuri grąžina bitų ilgį;

S – nurodo uždelsimo operatorių.

ELEKTRONINIŲ SISTEMŲ PARAMETRAI IR SĄVOKOS

Anonimiškumas: klientas, atsiskaitydamas elektroniniais pinigais už produktą, turi likti anonimiškas pinigų gavėjo ir banko atžvilgiu.

Dalinis anonimiškumas: klientas, atsiskaitydamas elektroniniais pinigais už produktą, turi likti anonimiškas pinigų gavėjo ir banko atžvilgiu. Galimybė nustatyti kliento tapatybę turi atsirasti tik tada, kai pinigai išleidžiami neteisėtai.

Pakartotinis nepanaudojimas (angl. Unreusability): elektroniniai pinigai negali būti kopijuojami arba išleidžiami dažniau nei vieną kartą. Tai reiškia, kad elektroninės piniginės sistema turi sumažinti riziką, susijusią su klastojimu ir (arba) turėti galimybę atskleisti nesąžiningo vartotojo tapatybę.

Nepadirbinėjimas(angl. unforgeability): tik įgaliotos šalys (pvz., bankas) gali gaminti elektroninius pinigus.

Mokėjimas neprisijungus (angl. off-line payment): mokėjimo operacija vykdoma neprisijungus prie interneto, tai reiškia, kad mokėjimo metu nėra reikalingas ryšys su banku. Mokėjimas gali būti atliktas tarp dviejų šalių nelaukiant banko ar kitos šalies patvirtinimo.

Mokėjimas prisijungus (angl. on-line payment): mokėjimo operacijai būtinas internetas ir trečios šalies patvirtinimas (pvz., banko), kad mokėtojo sąskaitoje yra pakankamai pinigų arba kt.

Perleidžiamumas (angl. Transferability): gauti elektroniniai pinigai gali būti naudojami kitiems mokėjimams tarp klientų neatsižvelgiant į tai, ar sandoriai vykdomi prisijungus ar neprisijungus (angl. online or offline).

Dalumas: elektroniniai pinigai gali būti išskaidyti į mažesnius vienetus, pvz., klientas, atsiskaitydamas už pirkinius, niekada negaus grąžos.

ĮVADAS

Problema:

pastaruoju metu turime vis didėjantį atsiskaitymų skaičių. Mokėjimai grynaisiais pinigais sudaro apie 50% visų atsiskaitymų, o kita mokėjimų dalis yra atsiskaitymai skaitmeniniais pinigais, prie kurių galima priskirti mokėjimus kortelėmis, bankinius pavedimus, elektroniniais pinigus ir kt. Chaumas ir Pedersenas (Chaum & Pedersen, 1993) įrodė, kad atsiskaitymų elektroniniais pinigais duomenys auga (angl. „is data growing in size then transferred“), jeigu turi tokias savybes: mokėjimai neprisijungus (angl. off-line payment), dalumas, anonimiškumas ir perleidžiamumas.

Tyrimo tikslas:

sukurti naują elektroninių pinigų sistemą, kuri galėtų būti realizuota mobilaus įrenginio elektroninėje piniginėje, turinčioje šias savybes:

1. mokėjimas neprisijungus;
2. elektroniniai pinigai turi būti dalūs;
3. galimybė perleidinėti pinigus tarp vartotojų;
4. kai pinigai perleidžiami tarp vartotojų − duomenys turi neaugti;
5. Pirkėjas privalo likti anonimiškas Pardavėjo atžvilgiu;
6. kriptosistema turi būti saugi.

Pagrindinės užduotys disertacijos tikslui pasiekti:

1. elektroninių pinigų sistemų ir jų pagrindinių savybių analizė;
2. patrauklesnės, saugesnės ir pažangesnės elektroninių pinigų sistemos sukūrimas mobilaus įrenginio elektroninėje piniginėje;
3. patikrinti naujos elektroninių pinigų sistemos patikimumą pagal BAN logiką;
4. naujos elektroninių pinigų sistemos skaitmeninis modeliavimas mokėjimo atlikimo laikui įvertinti;
5. elektroninės pinigų sistemos saugumo įrodymas.

Tyrimo metodai:

disertacijos problemoms spręsti buvo naudojami patikimumo ir saugumo analizės, matematinio bei skaitmeninio modeliavimo metodai. Elektroninės pinigų sistemos kūrimui panaudotos dvi pagrindinės kriptosistemos.

Darbo mokslinis naujumas:

sukurta elektroninių pinigų sistema perdavimo metu nedidinanti duomenų kiekio, tačiau panaikinanti Pirkėjo anonimiškumą banko atžvilgiu. Taip pat ši schema išlaiko pagrindines savybes: mokėjimas neprisijungus (angl. off-line

payment), dalus mokėjimas, Pirkėjo anonimiškumas Pardavėjo atžvilgiu, pinigų padirbimo prevencija, pinigų neatsekamumas ir saugumas.

Pagrindiniai ginamieji teiginiai:

1. Naujoji elektroninių pinigų sistema nedidina duomenų kiekio, kai pinigai perleidžiami tarp vartotojų. Taip pat jai būdingos pagrindinės savybės: mokėjimas neprisijungus (angl. off-line payment), dalūs elektroniniai pinigai ir Pirkėjo anonimiškumas Pardavėjo atžvilgiu.
2. Naujoji elektroninių pinigų sistema yra saugi.
3. Naujoji elektroninių pinigų sistema pagal BAN logiką yra patikima.
4. Naujoji elektroninių pinigų sistema gali būti efektyviai naudojama mobiliuose įrenginiuose.

Darbo rezultatų aprobavimas:

disertacijos tema buvo paskelbti trys moksliniai straipsniai. Du iš jų išspausdinti žurnaluose, turinčiuose citavimo indeksą „ISI Web of Science“ duomenų bazėje. Taip pat išleistas vienas konferencinis pranešimas. Be to, disertacijos tema pristatyta dviejose tarptautinėse konferencijose.

1 ELEKTRONINIŲ PINIGŲ SISTEMŲ APŽVALGA

Elektroniniai pinigai yra skaitmeninių pinigų produktas, kuris suteikia galimybę atsiskaityti už paslaugas nenaudojant fizinės valiutos. Operacijas saugiai ir anonimiškai galima atlikti internetu.

Kaip rašoma literatūroje (Au, Susilo & Mu, 2011; Baseri, Takhtaei & Mohajeri, 2013; Blazy et al., 2011; Brands, 2012; Chaum, Fiat & Naor, 1988; Chaum & Pedersen, 1993; de Solages & Traorè, 1998; Eng & Okamoto, 2006; Eslami & Talebi, 2011; Fan, Huang & Yu, 2013; Fuchsbauer, Pointcheval & Vergnaud, 2009; Kreft & Adi, 2006; Muleravičius, Sakalauskas, & Timofejeva, 2016; Okamoto, 1995; Pfitzmann & Köhntopp, 2007; Rosenberg, 2010; Yan Liang & Zhi-ming, 2016), elektroniniai pinigai susiduria su šiais iššūkiais:

- pinigų plovimas;
- dvigubas pinigų išleidimas;
- elektroninės piniginės saugyklos praradimas;
- klientų anonimiškumo išsaugojimas;
- internetinių operacijų ir duomenų srauto sumažinimas duomenų bazėse;
- elektroninių pinigų klastojimas (tai būdinga ir fiziniams pinigams);
- **duomenų apimties didėjimas:**

elektroninių pinigų sistemų trūkumas yra tas, kad dalūs, anonimiški elektroniniai pinigų duomenys auga, kai yra persiunčiami, t. y. šių elektroninių pinigų duomenys auga (Chaum & Pedersen, 1993). Duomenų didėjimas atsiranda dėl dvigubų išlaidų prevencijai reikalingos informacijos ir tokių charakteristikų, pvz., anonimiškumo, pinigų dalumo galimybės mokėti neprisijungus, išlaikymo.

Buvo sukurti alternatyvūs elektroniniai pinigai (elektroninių pinigų sistema), padėsianti išvengti duomenų gausos (D'Amiano & Di Crescenzo, 2006; Okamoto, 1995). Tačiau Tsiounis (Chan, Frankel & Tsiounis, 1998) aprašė ir pateikė analizes, įrodančias, kad šios elektroninės schemos turi kitų problemų, pvz., mokėjimas negali viršyti mokėjimo dydžio x arba protokolai tampa neveiksmingi ir su apribojimais.

Tik po dviejų dešimtmečių imtasi spręsti minėtą problemą. Šioje „Transferable e-cash without any increase in size" (Fuchsbauer et al., 2009) sistemoje buvo bandoma išspręsti pinigų „didėjimo" problemą, tačiau vis dar labai svarbus išlieka viešojo rakto dydis (Fuchsbauer, 2009; Waters, 2005).

- **sunkiai įrodomas sudėtingų kriptografinių sistemų saugumas:**

anot Rosenbergo (Rosenberg, 2010), didžiausios elektroninių pinigų sistemos problemos yra tokių elektroninių pinigų, kurie yra dalūs su mokėjimais neprisijungus ir išlaiko Pirkėjo anonimiškumą. Brandsas (Brands, 1994) pasiūlė idėją − Pirkėjui atlikti mokėjimus neprisijungus prie banko, pasinaudojant Stebėtoju. „Brands e-cash" sistemos kriptografinis saugumas neįrodytas, todėl ši sistema niekada nebuvo aktyvuota, nes norint įrodyti kriptografinį minėtos sistemos saugumą kiekvienam jos protokolui reikalinga Diffie'io-Hellmano (DDH) prielaida (Brands, 1994; Cramer & Shoup, 2004).

Taip yra todėl, kad Diffie'io-Hellmano raktų mainų negalima įrodyti remiantis tik CFD prielaida (angl. Computational Diffie-Hellman assumption", nes reikalinga ir DDH prielaida. Dėl šios priežasties praktinis elektroninių pinigų panaudojimas lieka atvira problema.

- elektroninių pinigų panaudojimas:

nuo 1980 m. iki šių dienų anoniminiai elektroniniai pinigai nėra plačiai naudojami. CFN pagrindu „DigiCash" (Chaum et al., 1988; Rabin, 1978), „Mojo Nation" naudojo savo elektroninių grynųjų pinigų sistemą, kuri iki šių dienų neišliko. Pagrindinė visų literatūroje aprašytų elektroninių pinigų sistemų problema (Rosenberg, 2010) yra esamų elektroninių pinigų sistemų saugumo analizės trūkumas dėl jų realizavimo sudėtingumo.

Rosenbergas (Rosenberg, 2010) taip pat pabrėžia, kad pastaruoju metu populiari yra dalinai anoniminė elektroninių pinigų sistema. Nauja sistema galėtų visiškai neatsisakyti pirkėjų anonimiškumo, o transformuoti jį į dalinį pirkėjų anonimiškumą, kad būtų išvengta duomenų augimo problemos.

2 NAUJA ELEKTRONINIŲ PINIGŲ REALIZAVIMO SCHEMA

2.1 Naujos elektroninės piniginės schemos aprašymas

Naują elektroninių pinigų sistemą sudaro šios šalys: Bankas ($\boldsymbol{B}$), Pirkėjas ($\boldsymbol{P}$), Pardavėjas ($\boldsymbol{V}$), Pirkėjo stebėtojas ($\boldsymbol{O_P}$), Pardavėjo stebėtojas ($\boldsymbol{O_V}$).

Pirkėjas gali paimti elektroninius pinigus iš savo Stebėtojo ($\boldsymbol{O_P}$) ir išleisti juos su įvairiais pardavėjais. Pardavėjas taip pat turi savo Stebėtoją ($\boldsymbol{O_V}$), o elektroninius pinigus, kuriuos gauna iš kito vartotojo, jis gali įdėti į savo Stebėtoją. Taip pat po įdėjimo protokolo Pardavėjas gali pervesti tuos pačius pinigus kitiems vartotojams, t. y. Pardavėjas gali tapti Pirkėju. Taip gaunama savybė – perleidžiamumas (angl. Transferability).

Šioje sistemoje Stebėtojas atlieka Banko funkcijas pasirašinėdamas elektroninius pinigus už jį. Tokiu būdu yra užtikrinama mokėjimo neprisijungus galimybė.

Kenkėjiškam Pirkėjui arba Pardavėjui įvykdžius dvigubą pinigų mokėjimą arba dvigubą pinigų padėjimą, Bankas visuomet galės atskleisti kenkėjo tapatybę panaudodamas vienodus elektroninius pinigus.

Visos elektroninių pinigų sistemos paprastai susideda iš tų pačių protokolų rinkinio. Kai kurie aspektai, pvz., registracija, pinigų paėmimas, mokėjimas ir pinigų padėjimas, yra universalūs. Taigi, kituose poskyriuose apžvelgsime šiuos protokolus.

2.2 Registracijos protokolas

Tarkime, kad Pirkėjas yra naujas Banko klientas, pasirengęs naudotis jo teikiama elektroninių pinigų paslauga. Pagal ElGamalio (ElGamal, 1985) parašo ir Schnorro (Schnorr, 1990) identifikavimo schemas, Bankas Pirkėjui sukuria ir persiunčia saugiu kanalu šiuos privačius ir viešus raktus: PrK_P, PuK_P.

Taip pat Bankas saugiu kanalu Pirkėjui perduoda Stebėtoją, kuris turi šiuos duomenis: PrK_O, PuK_O.

Pirkėjas ir Pardavėjas naudojasi tuo pačiu būdu, kad gautų savo raktus. Kitaip tariant, jie atsidaro Banke sąskaitą ir taip gauna viešus ir privačius raktus.

Atkreipkite dėmesį, kad Pirkėjas ir Pardavėjas gauna Stebėtoją, kurį galima įdiegti į mobilųjį telefoną, planšetinį kompiuterį, nešiojamą kompiuterį ar kitą mobilų įrenginį.

2.3 ElGamalio parašo ir Schnorro identifikavimo schemos panaudojimo aprašymas

Iš pradžių Bankas sugeneruoja didelį pirminį skaičių p, kad $p = 2q + 1$, kur q yra pirminis skaičius, o elementas g tenkina sąlygą $g^q \equiv 1 \mathrm{mod} q$. Praktinis būdas sukurti šį elementą yra surasti pirminės grupės $\boldsymbol{Z_p}$ generatorių ir jį kelti kvadratu.

Elementas g gali būti naudojamas generuojant ciklinį pogrupį $\boldsymbol{G_q} = \{g^i | i = \overline{1,q}\}$, vadinamą Silovo pogrupiu. Bankas taip pat pasirenka santraupos funkciją H, kad $H: \{0,1\}^* \rightarrow \boldsymbol{G_q}$. Tarkime, kad Pirkėjas yra naujas Banko klientas ir nori naudotis jo teikiamomis elektroninių pinigų paslaugomis. Pagal ElGamalio parašo ir Schnorro identifikavimo schemas, Bankas sukuria šiuos privačius ir viešus raktus Pirkėjui:

$PrK_P = x_P, PuK_P = \{G, A_P = G^{x_P}\}$.

Bankas taip pat suteikia Pirkėjui Stebėtoją ir pateikia jam šiuos duomenis:

$PrK_O = x_O, PuK_O = \{G, A_O = G^{x_O}, A_P^{Id_P}\}$,

kur $1 < x_P, x_O < q - 1$ ir Id_P yra Pirkėjo identifikacijos numeris, t. y. unikalus sveikasis skaičius, priskirtas kiekvienam Banko klientui. Pažymėtina, kad A_P yra viešasis parametras, susietas su Pirkėju, o reikšmė $A_P^{Id_P}$ yra sertifikuota Banko.

Parašas ant pranešimo $m \in \boldsymbol{G_q}$ yra apskaičiuojamas pagal ElGamalio parašo funkciją $Sig_{ElG}^{X}(\,)$, kur x yra pasirašančiojo privatus parašo raktas:

$S_m = Sig_{ElG}^{X}(m) = \{R, s\} = \{G^k mod\ p, k^{-1}(h(m) - xR) mod\ q\}$,

k yra slaptas, atsitiktinis, nenulinis elementas, mažesnis už q.

Parašo S_m patvirtinimas pranešimui m yra atliekamas naudojant patikros funkciją $Ver_{ElG}^{A}(\,)$, kur A yra viešas pasirašančiojo raktas:

$$Ver_{ElG}^{A}(S_m, m) = \begin{cases} TAIP, jeigu\ R \in \boldsymbol{G_q}\ ir\ A^R R^S = G^{h(m)} mod\ p \\ NE, \text{ Kitais atvejais} \end{cases}.$$

Schnorro identifikacijos protokolas, atliekamas tarp Pirkėjo ir Pardavėjo, susideda iš keturių etapų:

1. Pirkėjas atsitiktinai pasirenka $\xi \in \boldsymbol{Z_q}$ ir siunčia $W = G^{\xi}$ Pardavėjui;
2. Pardavėjas siunčia atsitiktinai sugeneruotą „iššūkį“ $h \in \boldsymbol{Z_q}$ Pirkėjui;
3. Pirkėjas siunčia gautą atsakymą $r = \xi + xh$ Pardavėjui;
4. Pardavėjas priimą atsakymą, jeigu tenkinama sąlyga $G^r \equiv WA^h \text{mod p}$.

2.4 Elektroninių pinigų išėmimo protokolas

Jeigu Pirkėjas ketina įsigyti prekę iš Pardavėjo ir nori jam sumokėti sumą m_i laiko momentu t_i, tai jis generuoja savo laikinuosius raktus: $PrK_P = x_P$ ir $PuK_P = \{G, A_P = G^{x_P}\}$, ir siunčia savo viešą raktą A_P savo Stebėtojui kartu su pageidaujama suma, užklausos laiku t_i ir Pardavėjo identifikacijos numeriu Id_V.

1. Pardavėjas siunčia savo Stebėtojui sumą m_i, kurią nori išleisti laiko momentu: t_i: $P \xrightarrow{m_i, t_i, Id_V, A_P} O_P$.

Atkreipkite dėmesį, kad tik Pirkėjas gali bendrauti su savo Stebėtoju, t. y. teikti užklausas.

2. Gavęs duomenis iš Pirkėjo, Stebėtojas atlieka šiuos veiksmus:

patikrina gauto laiko momento t_i teisingumą ir ar norima suma yra elektroninėje piniginėje, t. y.:

$Ver(t_i > t_{w0})$,

$Ver(m_i < m_{max}^P)$,

kur t_{w0} žymi paskutinio pinigų paėmimo laiką, o m_{max}^P šiuo metu esančią pinigų sumą elektroninėje piniginėje.

3. Stebėtojas sugeneruoja atsitiktinius skaičius: $\xi_i^{(1)}, \xi_i^{(2)} \in \boldsymbol{Z_q}$.

4. Ir apskaičiuoja Schnorro identifikacijos protokolo reikšmes: $W_i^{(1)} = G^{\xi_i^{(1)}}$ ir $W_i^{(2)} = G^{\xi_i^{(2)}}$.

5. Tada jis apskaičiuoja reikšmes – $N_i^{(1)}, N_i^{(2)}, P_i^{(1)}, P_i^{(2)}$, ir pasirašo ant šių reikšmių – $P_i^{(1)}, P_i^{(2)}, {A_P}^{N_i^{(1)}}, {A_P}^{Id_P}$:

$N_i^{(1)} = m_i || t_i || Id_V$

$N_i^{(2)} = Id_P \cdot N_i^{(1)}$

$P_i^{(1)} = {A_P}^{N_i^{(1)}} \cdot w_i^{(1)}$

$P_i^{(2)} = {A_P}^{N_i^{(2)}} \cdot w_i^{(2)}$

$S_i^{(1)} = Sig_{ElG}^{x_O}(P_i^{(1)})$

$S_i^{(2)} = Sig_{ElG}^{x_O}(P_i^{(2)})$

$S_i^{(3)} = Sig_{ElG}^{x_O}({A_P}^{N_i^{(1)}})$

$S_i^{(4)} = Sig_{ElG}^{x_O}({A_P}^{Id_P})$,

kur $||$ žymi sumos m_i ir laiko momento t_i konkatenaciją, o rezultatas $N_i^{(1)}$ atvaizduojamas kaip vienas sveikasis skaičius.

6. Stebėtojas išsaugo gautą laiko egzempliorių t_i kaip paskutinio pinigų išėmimo laiką: $t_{w0} \leftarrow t_i$.

7. Stebėtojas gautą sumą atima iš pinigų sumos Pirkėjo elektroninėje piniginėje:

$m_{max}^P \leftarrow m_{max}^P - m_i$.

8. Stebėtojas siunčia šiuos duomenis Pirkėjui:

$O_P \xrightarrow{\xi_i^{(1)}, \xi_i^{(2)}, w_i^{(1)}, w_i^{(2)}, N_i^{(1)}, N_i^{(2)}, S_i^{(1)}, S_i^{(2)}, S_i^{(3)}, S_i^{(4)}} P$.

Pasibaigus elektroninių pinigų išėmimo protokolui, galima vykdyti mokėjimo protokolą.

2.5 Elektroninių pinigų mokėjimo protokolas

Schnorro identifikavimo protokolas yra įtrauktas į mokėjimo protokolą, kad Pirkėjas galėtų įrodyti savo tapatybę Pardavėjui.

1. Pirkėjas siunčia Pardavėjui mokėjimo sumą m_i, kurią jis ketina išleisti, ir laiko momentą t_i kartu su visais šiais parašais – $S_i^{(1)}, S_i^{(2)}, S_i^{(3)}, S_i^{(4)}$, gautais iš savo Stebėtojo, ir Schnorro protokolo reikšmėmis – $W_i^{(1)}, W_i^{(2)}$:

$$P \xrightarrow{m_i||t_i,\, A_P,\, {A_P}^{Id_P}, w_i^{(1)}, w_i^{(2)}, S_i^{(1)}, S_i^{(2)}, S_i^{(3)}, S_i^{(4)}} V.$$

2. Pardavėjas tikrina gauto laiko teisingumą t_i, taip pat patikrina, ar gauta suma yra lygi faktinei kainai, kurią jis turėtų gauti:

$Ver(t_i > t_{p0})$

$$Ver(m = \widetilde{m}_i).$$

3. Pardavėjas patikrina parašus, kad apsidraustų, jog gauti duomenys nebuvo suklastoti:

$Ver_{ElG}^{Ao}({A_P}^{Id_P}, S_i^{(4)})$

$Ver_{ElG}^{Ao}({A_P}^{m_i||t_i||Id_V}, S_i^{(3)})$

$Ver_{ElG}^{Ao}({A_P}^{m_i||t_i||Id_V} \cdot w_i^{(1)}, S_i^{(1)})$

$$Ver_{ElG}^{Ao}\left(\left({A_P}^{Id_P}\right)^{(m_i||t_i||Id_V)} \cdot w_i^{(2)}, S_i^{(2)}\right),$$

kur t_{p0} yra paskutinio mokėjimo laikas. Jei šiame etape įvyksta kokių nors gedimų, protokolas nutraukiamas, nes Pardavėjas nustato, kad gauti duomenys suklastoti. Pirkėjas gauna klaidos pranešimą, nurodantį problemą. Pirkėjas nebegali naudoti šio sandorio duomenų naujiems mokėjimams.

4. Pardavėjas nori būti tikras, kad vartotojas, su kuriuo jis bendrauja, yra Pirkėjas ir todėl inicijuoja Schnorro identifikavimo protokolą. Iš pradžių sukuriamas atsitiktinis skaičius $h_i \in \boldsymbol{Z_q} : Gen \to h_i$.

5. Po to siunčiamas atsitiktinis „iššūkis“ h_i Pirkėjui: $V \xrightarrow{h_i} P$.

6. Gavęs „iššūkį“, Pirkėjas apskaičiuoja Schnorro protokolo reikšmes – $r_i^{(1)}, r_i^{(2)}$, ir siunčia jas atgal Pardavėjui:

$r_i^{(1)} = h_i \cdot x_P \cdot N_i^{(1)} + \xi_i^{(1)}$

$r_i^{(2)} = h_i \cdot x_P \cdot N_i^{(2)} + \xi_i^{(2)}$

$P \xrightarrow{r_i^{(1)}, r_i^{(2)}} V.$

7. Pasinaudodamas Pirkėjo viešomis reikšmėmis – $w_i^{(1)}$, $w_i^{(2)}$– Pardavėjas patikrina gautų atsakymų teisingumą:

$$Ver\left(G^{r_i^{(1)}} \cdot \left({A_P}^{m_i||t_i||Id_V}\right)^{-h_i} = w_i^{(1)}\right),$$

$$Ver\left(G^{r_i^{(2)}} \cdot \left(\left({A_P}^{Id_P}\right)^{(m_i||t_i||Id_V)}\right)^{-h_i} = w_i^{(2)}\right).$$

Jei šiame etape atsiranda neatitikimas – protokolas nutraukiamas. Pirkėjas gauna klaidos pranešimą, nurodantį identifikavimo problemą. Jis gali

bandyti inicijuoti mokėjimo protokolą, jei Pardavėjas suteikia šią galimybę, nes priešingu atveju šio sandorio duomenys nebegali būti naudojami.

Jei minėtais veiksmais operaciją įvykdyti pavyko, mokėjimas buvo atliktas. Tačiau Pardavėjas turi patvirtinti, kad mokėjimas tikrai įvyko.

8. Pardavėjas siunčia savo Stebėtojui mokėjimo sumą m_i, laiko žymą t_i ir parašą $S_i^{(3)}$:$V \xrightarrow{m_i||t_i,S_i^{(3)}} O_V$.

9. Pardavėjo Stebėtojas patvirtina gautų duomenų tikrumą, patikrindamas parašą $S_i^{(3)}$: $Ver_{ElG}^{A_O}(A_P{}^{m_i||t_i||Id_V}, S_i^{(3)})$.

Jei šis patikrinimas nepavyksta, Stebėtojas blokuoja mokėjimą. Pardavėjas nebegali padėti šios m_i į savo elektroninę piniginę.

10. Pardavėjo Stebėtojas sugeneruoja parašą $S_V = Sig_{ElG}^{x_O}(Id_V^{m_i||t_i})$ ir siunčia jį Pardavėjui: $O_V \xrightarrow{Id_V^{m_i||t_i},S_V} V$.

11. Pardavėjas siunčia šiuos duomenis Pirkėjo patikrinimui:

V $\xrightarrow{Id_V^{m_i||t_i},S_V} P$.

12. Pirkėjas atlieka šiuos veiksmus, kad užtikrintų, jog nesusidūrė su kenkėjišku Pardavėju:

a. reikšmę $Id_V^{m_i||t_i}$ kelią laipsniu $(m_i||t_i)^{-1}$ ir patikrina su reikšme Id_V:

$$Ver\left(\left(Id_V^{m_i||t_i}\right)^{(m_i||t_i)^{-1}}, Id_V\right);$$

b. patikrina laiko žymą ir parašą S_V: $Ver_{ElG}^{x_O}(Id_V^{m_i||t_i}, S_V)$.

Jei patikrinimas yra sėkmingas, tada abi šalys gauna pranešimus apie šį rezultatą ir sandoris bus sudarytas. Priešingu atveju sandoris neįvyksta, o Pirkėjas gali kreiptis į Banką elektroniniu būdu arba fiziškai ten nuvykti, kad atkurtų savo piniginę. Abi šalys gauna klaidų pranešimus.

13. Pardavėjas išsaugo gautą laiką kaip paskutinio Pirkėjo mokėjimo laiką: $t_{p0} \leftarrow t_i$

Sėkmingai baigęs mokėjimo protokolą, Pardavėjas gauna pinigus už prekes, kurias gali siųsti elektroniniu būdu arba fiziškai. Jei įvyko kokių nors klaidų – apie kaltininką pranešama Bankui.

2.6 Elektroninių pinigų padėjimo protokolas

1. Pardavėjas siunčia savo Stebėtojui šiuos duomenis, kuriuos gavo iš Pirkėjo:

$$V \xrightarrow{m_i||t_i,\, A_P\, ,A_P{}^{Id_P},w_i^{(1)},w_i^{(2)},S_i^{(1)},S_i^{(2)},S_i^{(3)},S_i^{(4)}} O_V.$$

2. Gavęs duomenis, Stebėtojas patikrina gauto laiko momentą t_i: $Ver(t_i > t_{d0})$

Atkreipkite dėmesį, kad Stebėtojo (O_V) tikrinamas laiko momentas nebūtinai turi atitikti esamą laiko momentą, t. y. šis protokolas gali būti vykdomas bet kuriuo metu.

Jei nepavyksta atlikti šio veiksmo, atsiranda klaidos pranešimas, rodantis, kad šis pinigų padėjimas jau įvyko anksčiau. Tada pinigų padėjimo protokolas nutraukiamas.

3. Pardavėjo Stebėtojas (O_V) patikrina gautų parašų teisingumą:

$Ver_{ElG}^{A_O}(A_P{}^{Id_P}, \mathrm{S}_i^{(4)})$

$Ver_{ElG}^{A_O}(A_P{}^{m_i||t_i||Id_V}, \mathrm{S}_i^{(3)})$

$Ver_{ElG}^{A_O}(A_P{}^{m_i||t_i||Id_V} \cdot w_i^{(1)}, \mathrm{S}_i^{(1)})$

$Ver_{ElG}^{A_O}\left((A_P{}^{Id_P})^{(m_i||t_i||Id_V)} \cdot w_i^{(2)}, \mathrm{S}_i^{(2)}\right)$.

4. Pardavėjo Stebėtojas (O_V) atnaujina paskutinio pinigų padėjimo laiką:

$t_{d0} \leftarrow t_i$.

5. Pardavėjo Stebėtojas (O_V) atnaujina pinigų sumą, esančią elektroninėje piniginėje: $m_{max}^V \leftarrow m_{max}^V + m_i$.

3 PRIEŠIŠKŲ ATAKŲ MODELIAVIMAS IR SAUGUMO ANALIZĖ

3.1 Saugumo analizė nuo priešiškų atakų

Šiame skyriuje aptarsime mūsų schemos apsaugojimą nuo prisitaikančio vidinio kenkėjo, t. y. manome, jis yra vienas iš vartotojų (Pirkėjas arba Pardavėjas). Įrodyta, kad sistema yra atspari šioms atakoms:

1. Kenkėjiško Pirkėjo ataka (**MP**):

(a) dvigubas išleidimas, t. y. naudojant tuos pačius duomenis pirkti prekes daugiau nei vieną kartą iš Pardavėjo;

(b) transakcijos suklastojimas, t. y. mokėjimo sumos suklastojimas, laiko momento ar bet kokių Pardavėjui siunčiamų duomenų padirbinėjimas. Yra dvi šios atakos alternatyvos: išleisti mažiau pinigų nei reikalauja Pardavėjas (mokėjimo suma) arba pateikti ankstesnį sandorį kaip naują (laiko momento suklastojimas).

2. Pašalinio vartotojo ataka (angl. Man, in the Middle Attack) (**MitM**):

(a) apsimetimas Pirkėju suklastojant jo identifikaciją Id_P, t. y. tam, kad neteisėtai įsigytų prekes, naudojami teisėto Pirkėjo elektroninės piniginės pinigai;

(b) apsimetimas Pardavėju suklastojant jo identifikaciją, Id_V, t. y. tam, kad neteisėtai gautų elektroninius pinigus vietoj teisėto Pardavėjo.

3. Kenkėjiško Pardavėjo ataka (**MV**):

(a) dvigubas pinigų padėjimas į elektroninę piniginę, t. y. naudojant tuos pačius duomenis Pardavėjo elektroninės piniginės likutis papildomas daugiau nei vieną kartą;

(b) mokėjimo protokolo nutraukimas, kai pinigai gauti, t. y. gauti Pirkėjo pinigus, bet neperduoti prekių;

(c) transakcijos suklastojimas, t. y. mokėjimo sumos, laiko momento ar bet kokių duomenų, gautų iš Pirkėjo, suklastojimas. Yra dvi šios atakos alternatyvos: į savo elektroninę piniginę įsidėti daugiau pinigų nei gauta iš Pirkėjo arba įsidėti jau prieš tai įdėtą pinigų sumą į savo elektroninę piniginę (dvigubas pinigų padėjimas).

3.2 Elektroninių pinigų sistemos patikimumo analizė

Pateikiamos elektroninių pinigų sistemos patikimumas analizuojamas naudojant BAN logiką. Remiantis šia logika siekiama nustatyti, ar vykdant informacijos mainus tarp skirtingų šalių yra priežasčių nepasitikėti vienas kitu ir nustatyti saugumo spragas saugantis nuo kenkėjiškų asmenų, pvz., kenkėjiško Pardavėjo, Pirkėjo ar kt. BAN logikos tikrinimas prasideda nuo teiginių, kuriuos reikia įrodyti pasitelkiant prielaidas.

Reikėtų nepamiršti, kad BAN logika skirta kriptografinių protokolų saugumui pagrįsti. Ši logika remiasi prielaidomis ir taisyklėmis, kurios naudojamos norint įrodyti tam tikrus teiginius.

Mokėjimo protokolo teisingumas ir saugumas remiasi šiais teiginiais:

1 teiginys: $V \mid\equiv m_i$,

2 teiginys: $V \mid\equiv P$,

3 teiginys: $P \mid\equiv V$.

Kitais žodžiais tariant, Pardavėjas neabejoja, kad gauta reikiama pinigų suma (1 teiginys), Pardavėjas pasitiki Pirkėju (2 teiginys), Pirkėjas pasitiki Pardavėju (3 teiginys). Minėtiems teiginiams įrodyti yra naudojamos šios prielaidos:

1 prielaida: Pardavėjas mano, kad vieši parametrai (Pirkėjo parametrai – $G, A_P, A_P^{Id_P}$, ir jo Stebėtojo (O_P) viešasis raktas A_O) nėra suklastoti:
$P, V \mid\equiv G, A_P, A_O,\ G, A_P^{Id_P}$.

2 prielaida: Pardavėjas pasitiki Banko atstovu, t. y. Stebėtojais: $V \mid \equiv O_P, O_V$.

3 prielaida: Pardavėjas gauna teisingą viešą informaciją iš Pirkėjo: $\overset{A_P, A_O,\ G, A_P^{Id_P}}{\rightarrow} V$.

4 prielaida: Pirkėjas gauna teisingą viešą informaciją iš savo Stebėtojo: $\overset{A_O,\ G, A_P^{Id_P}}{\rightarrow} P$.

Taigi, pasinaudojus minėtomis prielaidomis ir visa informacija, kurią vienas kitam siunčia sistemos vartotojai, BAN logika patvirtina, kad ši sistema pagal nurodytus teiginius yra patikima.

4 NAUJOS ELEKTRONINĖS PINIGINĖS SKAITMENINĖ SIMULIACIJA

Kadangi didelė mokėjimo operacijų dalis tenka Stebėtojui, turinčiam ribotus skaičiavimo išteklius, naujos elektroninės piniginės sistemos efektyvumas priklauso nuo veikimo laiko.

Skaičiavimo laikas yra tiesiogiai susijęs su procesoriaus laikrodžio dažniu. Jei procesorius veikia esant 1 GHz laikrodžio dažniui, procesoriaus taktas užima $10^{-9}\ s = 1ns$ laiko.

Operacijoms, reikalingoms protokolų veikimo laikui įvertinti skaitmenine simuliacija, mums reikės dauginimo, sudėties, perkėlimo ir modulio funkcijos skaičiavimo įvertinimo funkcijų. Šias operacijas pavadinome elementariosiomis operacijomis.

Apskaičiuojant protokolų skaičiavimo trukmę, turime įvertinti elementarių operacijų, reikalingų moduliarinei eksponentinei funkcijai $r = g^k \bmod p$, skaičiavimo laiką procesoriaus taktais.

Pasak Hwango, Su'o, Yeho, Cheno, Knutho (Hwang, Su, Yeh, & Chen, 2005; Knuth, 1998), moduliarinė eksponentinė funkcija gali būti apskaičiuojama naudojant grandinės papildymo metodą (angl. Addition chain method) (Knuth, 1998). Operacijų skaičiaus nustatymo formulės yra šios:

$$MOD_E(k,p) = 1{,}5 \cdot l(k)[M(l(p)) + 2Mod(l(p)) + 1],$$

kur:

$M(w) = 3M(w/2) + 5A(w) + 2S$

$A(w) = w/32$

$$Mod(w) = Mod(w/2) + 4M(w/2) + 1{,}5A(w) + 3S.$$

- $\boldsymbol{MOD_E(y,z)}$ – grąžina skaičiavimo taktų skaičių moduliarinei eksponentei $r = g^k \bmod p$;
- $\boldsymbol{M(w)}$, $\boldsymbol{A(w)}$, $\boldsymbol{Mod(w)}$ – grąžina skaičiavimo taktų skaičių sandaugos, sudėties ir modulio funkcijoms pagal nurodytą bitų skaičių w skaičiuojamiems kintamiesiems;
- $\boldsymbol{l(w)}$ – grąžina reikšmės w bitų skaičių;
- $\boldsymbol{S}$ – perkėlimo operatorius.

Schemos kintamųjų bitų ilgiai pateikti pirmoje lentelėje.

1 lentelė. *Reikšmių ilgis bitais*

Reikšmės	**Ilgis bitais, *b***
$p, q, x_P, x_O\ A_P, A_O, G, Id_P, Id_V, h_i, R$	$2048\ b$
$\xi_i^{(1)}, \xi_i^{(2)}, w_i^{(1)}, w_i^{(2)}, N_i^{(1)}, N_i^{(2)}, S_i^{(1)}, S_i^{(2)}, S_i^{(3)}, r_i^{(1)}, r_i^{(2)}, S_V$	$2048\ b$
m, t	$\sim 24\ b$
$m_i \| \| t_i \| \| Id_V$	$\sim 2072\ b$
$H(m)$	$\sim 256\ b$

Nustačius procesoriaus taktų skaičių N, operacijos laikas gali būti įvertintas taip: $Time = N \cdot T$, kur $T = 1/F$ ir F yra laikrodžio dažnis. Mūsų sistemos palyginimas su Brandso ir CHL sistemomis pateikiamas žemiau esančioje antroje lentelėje.

2 lentelė. *Skaičiavimo laiko palyginimas su kitomis sistemomis*

Protokolas	**Naujoji sistema**	**Brandso**	**CHL**
Pinigų išėmimo	740	-	-
Pinigų mokėjimo	1 333	-	-
Pinigų padėjimo	776	-	-
Viso	2 849	2 996	2 111

Pasak Hinterwälderio, Rieko ir Paario (Hinterwälder, Riek, & Paar, 2015), Brandso elektroninių pinigų sistemos visų protokolų suminis laikas yra apie 2966 ms, o CHL elektroninių pinigų protokolų skaičiavimo laikas (Au, Susilo, & Mu, 2007) atliekant vienkartinį mokėjimą yra 30 moduliarinių eksponenčių, kurios užima apie 2111 ms. Anot Juango (Juang, 2010), sunku apskaičiuoti kiekvieno protokolo veikimo trukmę, nes tai priklauso nuo to, kiek sandorių buvo įvykdyta anksčiau ir su kokia pinigų suma jie buvo atlikti.

Naujoji elektroninių pinigų sistema sėkmingai gali būti naudojama mobiliuosiuose įrenginiuose. Visas išgryninimo, mokėjimo ir pinigų įnešimo procesas trunka 2849 ms. Tai yra toks pat arba geresnis rezultatas, palyginti su kitomis elektroninių pinigų sistemomis.

Palyginus naująją elektroninių pinigų sistemą su kitomis analizuotomis sistemomis, galima teigti, kad ji yra pažangesnė ir patrauklesnė vartotojui.

IŠVADOS

Pagrindinės atliktos užduotys disertacijos tikslui pasiekti:

1. Esamų elektroninių pinigų sistemų ir jų pagrindinių savybių analizė.
2. Sukurta patraukli , saugi ir tinkama (atsižvelgiant į laiką, reikalingą mokėjimui atlikti) elektroninių pinigų sistema mobiliems įrenginiams, kuriai reikia gerokai mažesnių skaičiavimo išteklių.
3. Naujos elektroninių pinigų sistemos patikimumas patikrintas pagal BAN logikos pagrindinius tikslus: Pardavėjo užtikrintumas dėl sumos, kurią jis turi gauti, Pardavėjo pasitikėjimas Pirkėju ir Pirkėjo pasitikėjimas Pardavėju.
4. Skaitmeninio modeliavimo būdu buvo apskaičiuotas teorinis naujos elektroninių pinigų sistemos paėmimo, mokėjimo ir padėjimo laikas, kuris atitinkamai yra 740, 1333 ir 776 ms, o viso proceso trukmė – 2849 ms.
5. Įrodytas sukurtos elektroninių pinigų sistemos saugumas, kai susiduriama su kenkėjiško Pirkėjo, pašalinio vartotojo (angl. Man in The Middle) ir kenkėjiško Pardavėjo atakomis.

Darbo mokslinio naujumo apžvalga:

pasiūlyta elektroninių pinigų sistema nedidina duomenų kiekio pervedimų metu, kai panaikinamas anonimiškumas tarp Banko ir Pirkėjo. Tokia sistema išlaiko jai būtiniausias savybes: mokėjimą neprisijungus, pinigų dalumą, Pirkėjo anonimiškumą Pardavėjo atžvilgiu, dvigubų išlaidų prevenciją, neatsekamumą ir saugumą.

Pabaigai:

1. Naujoji elektroninių pinigų sistema nedidina duomenų kiekio, kai atliekami pervedimai tarp vartotojų. Taip pat ji turi ir tokias būtiniausias savybes, kaip mokėjimas neprisijungus, elektroninių pinigų dalumas, pervedimų galimybė tarp vartotojų.
2. Naujoji elektroninių pinigų sistema yra apsaugota nuo kenkėjiško Pirkėjo, pašalinio vartotojo ir kenkėjiško Pardavėjo atakų. Be to, ši sistema apsaugo nuo dvigubų išlaidų.
3. Naujoji elektroninių pinigų sistema yra patikima pagal BAN logiką. Pardavėjui nėra reikalo nepasitikėti Pirkėju ir atvirkščiai Pardavėjas neabejoja, kad Pirkėjas sumokės reikiamą sumą.
4. Naujoji elektroninių pinigų sistema sėkmingai gali būti naudojama mobiliuosiuose įrenginiuose. Visas išgryninimo, mokėjimo ir pinigų įnešimo procesas trunka 2849 ms. Tai yra toks pat arba geresnis rezultatas, palyginti su kitomis elektroninių pinigų sistemomis.

5. Palyginus naująją elektroninių pinigų sistemą su kitomis analizuotomis sistemomis, galima teigti, kad ji yra pažangesnė ir patrauklesnė vartotojui.

LITERATŪROS SĄRAŠAS

Au, M. H., Susilo, W., & Mu, Y. (2011). Electronic cash with anonymous user suspension. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-22497-3_12

Baseri, Y., Takhtaei, B., & Mohajeri, J. (2013). Secure untraceable off-line electronic cash system. *Scientia Iranica*. https://doi.org/10.1016/j.scient.2013.05.002

Blazy, O., Canard, S., Fuchsbauer, G., Gouget, A., Sibert, H., & Traoré, J. (2011). Achieving optimal anonymity in transferable e-cash with a judge. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-21969-6_13

Brands, S. (1994). Untraceable Off-line Cash in Wallets with Observers (Extended abstract). *Advances in Cryptology—CRYPTO'93*. https://doi.org/10.1007/3-540-48329-2_26

Brands, S. (2012). Off-line electronic cash based on secret-key certificates. https://doi.org/10.1007/3-540-59175-3_86

Chan, A., Frankel, Y., & Tsiounis, Y. (1998). Easy come — easy go divisible cash. In *Advances in Cryptology — EUROCRYPT'98*. https://doi.org/10.1007/BFb0054154

Chaum, D., Fiat, A., & Naor, M. (1988). Untraceable Electronic Cash. In *Advances in Cryptology — CRYPTO' 88*. https://doi.org/10.1007/0-387-34799-2_25

Chaum, D., & Pedersen, T. P. (1993). Transferred cash grows in size. In *Advances in Cryptology — EUROCRYPT' 92*. https://doi.org/10.1007/3-540-47555-9_32

Cramer, R., & Shoup, V. (2004). Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack. *SIAM Journal on Computing*. https://doi.org/10.1137/s0097539702403773

D'Amiano, S., & Di Crescenzo, G. (2006). Methodology for digital money based on general cryptographic tools. https://doi.org/10.1007/bfb0053432

de Solages, A., & Traorè, J. (1998). An efficient fair off-line electronic cash system with extensions to checks and wallets with observers. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/BFb0055489

ElGamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based

on Discrete Logarithms. *IEEE Transactions on Information Theory*, *196 LNCS*, 10–18. https://doi.org/10.1007/3-540-39568-7_2

Eng, T., & Okamoto, T. (2006). Single-term divisible electronic coins. https://doi.org/10.1007/bfb0053446

Eslami, Z., & Talebi, M. (2011). A new untraceable off-line electronic cash system. In *Electronic Commerce Research and Applications*. https://doi.org/10.1016/j.elerap.2010.08.002

Fan, C. I., Huang, V. S. M., & Yu, Y. C. (2013). User efficient recoverable off-line e-cash scheme with fast anonymity revoking. *Mathematical and Computer Modelling*. https://doi.org/10.1016/j.mcm.2012.07.012

Fuchsbauer, G. (2009). Automorphic Signatures in Bilinear Groups and an Application to Round-Optimal Blind Signatures. *IACR Cryptology EPrint Archive*, *2009*, 320.

Fuchsbauer, G., Pointcheval, D., & Vergnaud, D. (2009). Transferable constant-size fair E-cash. In *Cryptology and Network Security*. https://doi.org/10.1007/978-3-642-10433-6_15

Hinterwälder, G., Riek, F., & Paar, C. (2015). Efficient e-cash with attributes on MULTOS smartcards. In *Radio Frequency Identification*. https://doi.org/10.1007/978-3-319-24837-0_9

Hinterwälder, G., Zenger, C. T., Baldimtsi, F., Lysyanskaya, A., Paar, C., & Burleson, W. P. (2013). Efficient e-cash in practice: NFC-based payments for public transportation systems. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-39077-7_3

Hwang, R. J., Su, F. F., Yeh, Y. S., & Chen, C. Y. (2005). An efficient decryption method for RSA cryptosystem. In *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*. https://doi.org/10.1109/AINA.2005.97

Juang, W. S. (2010). RO-cash: An efficient and practical recoverable pre-paid offline e-cash scheme using bilinear pairings. *Journal of Systems and Software*. https://doi.org/10.1016/j.jss.2009.11.006

Knuth, D. E. (1998). *The Art of Computer Programming, Volume 3: (2nd Ed.) Sorting and Searching*. *Computer*. https://doi.org/10.2307/2283757

Kreft, H., & Adi, W. (2006). fairCASH - A digital cash candidate for the proposed GCC gulf dinar. In *2006 Innovations in Information Technology, IIT*. https://doi.org/10.1109/INNOVATIONS.2006.301916

Muleravičius, J., Sakalauskas, E., & Timofejeva, I. (2016). *On methodology of e-wallet construction for partially off-line payment system*. *Communications in Computer and Information Science* (Vol. 639). https://doi.org/10.1007/978-3-319-46254-7_61

Okamoto, T. (1995). An efficient divisible electronic cash scheme. In *CRYPTO '95 Proceedings of the 15th Annual International Cryptology Conference on*

Advances in Cryptology. https://doi.org/10.1007/3-540-44750-4_35
Pfitzmann, A., & Köhntopp, M. (2007). Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology. https://doi.org/10.1007/3-540-44702-4_1
Rabin, M. (1978). Digitalized Signatures and Public-Key Functions as Intractable as Factorization. *Foundations of Secure Computations*. https://doi.org/10.1080/09720529.2013.858478
Rosenberg, B. (2010). *Handbook of financial cryptography and security*. *Handbook of Financial Cryptography and Security*. https://doi.org/10.1201/9781420059823
Schnorr, C. P. (1990). Efficient identification and signatures for smart cards. In *Advances in Cryptology — CRYPTO' 89 Proceedings*. https://doi.org/10.1007/3-540-46885-4_68
Waters, B. (2005). Efficient identity-based encryption without random oracles. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 114–127).
Yan Liang, Z. X., & Zhi-ming, Z. (2016). An Electronic Cash System Based on Certificateless Group Signature. *International Journal of Security and Its Applications*, 237–300.

MOKSLINIŲ PUBLIKACIJŲ DISERTACIJOS TEMA SĄRAŠAS

Mokslinės informacijos instituto duomenų bazės „ISI Web of Science“ leidiniuose, turinčiuose citavimo indeksą

Sakalauskas, E., Timofejeva, I., Michalkovič, A., & Muleravičius, J. (2018). A Simple Off-line E-Cash System with Observers. Information Technology and Control, 47(1), 107-117.

Muleravičius, J., Timofejeva, I, Sakalauskas, E., &. Mihalkovich, A. (2019). Security, Trustworthiness and Effectivity Analysis of an Off-line E-Cash System with Observers. Informatica, Vol. 30, No. 2, 327–348.

Mokslinės informacijos instituto duomenų bazės „ISI Web of Science“ leidinyje, neturinčiame citavimo indekso

Muleravičius, J., Sakalauskas, E., & Timofejeva, I. (2016, October). On Methodology of E-wallet Construction for Partially Off-line Payment System. In International Conference on Information and Software Technologies (p. 753–765). Springer, Cham.

Iš konferencijos pranešimo paskelbtas straipsnis

Sakalauskas, E., Muleravicius, J., & Timofejeva, I. (2017, June). Computational resources for mobile E-wallet system with observers. In Electronics, 2017 (p. 1–5). IEEE.

INFORMACIJA APIE DISERTACIJOS AUTORIŲ

Jonas Muleravičius gimė 1989 metų gegužės 31 dieną Kaune, Lietuvoje. 2008–2012 metais studijavo *Kauno technologijos universitete*. 2012 metais sėkmingai atliko praktiką *Lietuvos banke* ir tais pačiais metais įgijo Taikomosios matematikos bakalauro laipsnį.

2012–2014 metais studijavo *Kauno technologijos universitete* ir įgijo taikomosios matematikos magistro laipsnį.

2014 metais įstojo į *Kauno technologijos universiteto* trečios pakopos doktorantūros studijas ir 2019 metais gynėsi disertacijos darbą.

Nuo 2014 metų rugsėjo iki dabar dirba tarptautinėje mažmeninės prekybos įmonėje, kurioje eina vyresniojo analitiko pareigas.

Elektroninis paštas: jonas.muleravicius@gmail.com, jonas.muleravicius@ktu.edu.

Autoriaus domėjimosi sritys – akcijų rinka, matematinio skaičiavimo, analizės ir modeliavimo algoritmai, kriptografinių elementų panaudojimas finansuose ir ekonomikoje, mažmeninė prekyba, dirbtinis intelektas.

SUMMARY

Problem: these days, a great number of various payment transactions are taking place. Almost half of them involve cash, while the other part of transactions are digital payments. The latter consists of card payments, bank transfers, e-payments and more. However, e-payments that take place off-line involve divisibility, and full anonymity which has resulted in data expansion when e-cash transfers are made, as was shown by Chaum & Pedersen (1993).

The aim of the research is as follows:

Propose a new e-cash system which will aid in the construction of an e-wallet for mobile devices, with these characteristics:

1.The ability to make off-line payments;

2.Ensuring that e-cash is properly divisible;

3.Transfers between users has to be possible;

4.Data which is required to prevent 'double spending' - fraud - should not expand when carrying out transfers between users;

5.The purchaser must retain anonymity from the vendor;

6.System has to be secure.

Basic tasks that are being aimed at in this work:

1.Carry out an analysis of the existing e-cash systems and their main properties;

2.Work towards the construction of a more attractive, secure, and advanced e-cash system for an e-wallet on a mobile device;

3.Check the trustworthiness of BAN logic under the new e-cash scheme;

4.Estimate digital simulation time of the new e-cash scheme in terms of theoretical processing time;

5.Certify security of the newly constructed e-cash system.

Research methods:

Research methods used in this work in order to reach the desired conclusions included those with a mathematical basis, plus a trustworthiness analysis, a security analysis, as well as a digital simulation. The construction of a new e-cash system can be achieved using two of the main crypto systems, both of which are well known when it comes to analysing the existing e-cash systems.

An overview of the novelty:

The proposed e-cash system will ensure that data will not expand when transfers are made, thanks to the fact that it removes anonymity between the bank and the purchaser. This scheme retains the following main properties: off-line and divisible payments, anonymity between the purchaser and the vendor, a prevention of 'double spending', as well as untraceability and security.

The benefits of the new system as it is proposed here:

1.The new e-cash system will not expand in size when data is transferred between users. In addition, it has all of the other main properties of such a system: off-line payments; divisible e-cash; the ability to transfer e-cash between users;

data not expanding in size when funds are transferred between users; and the purchaser retaining anonymity from the vendor;

2.The new e-cash system is secure;

3.The new e-cash system can be fully trusted under BAN logic;

4.The new e-cash system can effectively be used on mobile devices.

Approbation of the research:

Two scientific papers have been published on this subject and both have been included in the list of papers in the ISI database. In addition, one paper was published in the ICIST journal without a bibliography and conference proceedings were published in Electronica, neither of which are required here. The theme of this dissertation was also presented at two international conferences.

The structure and volume of the dissertation:

The introduction of this dissertation provides an overview of crypto systems. Section 2 shows methodology which is used for the model proposed. Section 3 contains a definition in abstract form of the main protocols (regarding withdrawal, payment, and deposit), as well as it outlines the scheme of the suggested e-cash system.

After the new system was published in Section 4 of the dissertation, it was checked for BAN logic and security, then, a digital simulation was carried out in terms of the new e-cash system. In this section we used previously published papers such as 'A simple off-line e-cash system with observers', when constructing the e-system protocols in Section 3, we referred to 'Security, trustworthiness, and effectiveness analysis for an off-line e-cash system with observers' for the security analysis and related improvements in Section 4, and also used the conference proceedings 'Computational resources for a mobile e-wallet system with observers' for digitally simulating the new e-system in Section 4. Finally, the last section contains results and conclusions, the afterward and acknowledgements, as well as references and publication details.

Dissertation Conclusions:

1.The new e-cash system does not produce data expansion when transfers are made between users, at the same time having all the other main properties: off-line payments; divisible e-cash; transferability between users; and the purchaser retaining anonymity from the vendor. It was proved that, in order to gain some advantages such as data not expanding when transfers are made, anonymity from the bank had to be removed;

2.The new e-cash system is secure from an attack by a 'Malicious Purchaser', an attack by a 'Man in the Middle', and an attack by a 'Malicious Vendor'. In addition, it continues to prevent 'double spending'.

3.The new e-cash system can be fully trusted when using BAN logic. There is no reason for the vendor not to trust the purchaser and, vice versa, there is no reason for the purchaser not to trust the vendor. In addition, the vendor can trust a payment amount which is received from the purchaser.

4.The new e-cash system can effectively be used on mobile devices. All of the processing time that is involved in withdrawal, payment, and deposit procedures amounts to 2,849 milliseconds. In comparison to other e-cash systems, this system is approximately equal to them or better than them, while also maintaining important properties.

UDK - 336.74:004.056](043.3)

SL344. 2019-10-04, 1,75 leidyb. apsk. l. Tiražas 50 egz.
Išleido Kauno technologijos universitetas, K. Donelaičio g. 73, 44249 Kaunas
Spausdino leidyklos „Technologija“ spaustuvė, Studentų g. 54, 51424 Kaunas