KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

INFORMACIJOS IR INFORMACINIŲ TECHNOLOGIJŲ SAUGOS

STUDIJŲ PROGRAMA

NERIJUS ČEREŠKA

RFID ŽYMŲ APSAUGOS NUO KLASTOJIMO METODO SUDARYMAS IR TYRIMAS

Magistro darbas

Darbo vadovas
doc. dr. A. Venčkauskas

KAUNAS, 2013

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

INFORMACIJOS IR INFORMACINIŲ TECHNOLOGIJŲ SAUGOS

STUDIJŲ PROGRAMA

NERIJUS ČEREŠKA

RFID ŽYMŲ APSAUGOS NUO KLASTOJIMO METODO SUDARYMAS IR TYRIMAS

Magistro darbas

Darbo vadovas
doc. dr. A. Venčkauskas

Recenzentas
prof. dr. E. Sakalauskas

KAUNAS, 2013

AUTORIŲ GARANTINIS RAŠTAS
DĖL PATEIKIAMO KŪRINIO

2013 - gegužės - 24 d.
Kaunas

Autorius,_____,
(vardas, pavardė)

patvirtina, kad Kauno technologijos universitetui pateiktas baigiamasis bakalauro (magistro) darbas (toliau vadinama – Kūrinys)_____
(kūrinio pavadinimas)
_____

pagal Lietuvos Respublikos autorių ir gretutinių teisių įstatymą yra originalus ir užtikrina, kad

1) jį sukūrė ir parašė Kūrinyje įvardyti autoriai;
2) Kūrinys nėra ir nebus įteiktas kitoms institucijoms (universitetams) (tiek lietuvių, tiek užsienio kalba);
3) Kūrinyje nėra teiginių, neatitinkančių tikrovės, ar medžiagos, kuri galėtų pažeisti kito fizinio ar juridinio asmens intelektinės nuosavybės teises, leidėjų bei finansuotojų reikalavimus ir sąlygas;
4) visi Kūrinyje naudojami šaltiniai yra cituojami (su nuoroda į pirminį šaltinį ir autorių);
5) neprieštarauja dėl Kūrinio platinimo visomis oficialiomis sklaidos priemonėmis.
6) atlygins Kauno technologijos universitetui ir tretiesiems asmenims žalą ir nuostolius, atsiradusius dėl pažeidimų, susijusių su aukščiau išvardintų Autorių garantijų nesilaikymu;
7) Autoriai už šiame rašte pateiktos informacijos teisingumą atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

Autorius

_____ _____
(vardas, pavardė) (parašas)

SANTRAUKA

Šiame darbe yra sprendžiama RFID žymų apsaugos nuo klastojimo problema, t.y. kaip neleisti žymų klastotojui išgauti originalios žymos ar visos RFID sistemos identifikacinius ir kitus svarbius duomenis, kurių atskleidimas leistų sukurti originalios RFID žymos klastotę.

Darbo analizės dalyje yra plačiau apžvelgiama RFID žymų apsaugos nuo klastojimo problema, gilinamąsi į bendrus RFID technologijos veikimo principus ir RFID žymų kategorijas. Taip pat nustatinėjami galimi RFID žymų klastojimo būdai, jų išvengimo galimybės, apžvelgiami ir detalizuojami kitų autorių sukurti apsaugos metodai, pateikiamos rekomendacijos naujam RFID žymų apsaugos nuo klastojimo metodo sudarymui.

Tolimesnėje darbo eigoje yra sudarytas naujas RFID žymų apsaugos nuo klastojimo metodas pagal analizės dalyje padarytas rekomendacijas ir suformuluotas išvadas. Pateikiama pradinė metodo saugumo analizė.

Pagal sudaryto RFID žymų apsaugos nuo klastojimo metodo koncepciją ir detalų aprašą yra sukurtas programinis modelis, kuris imituoja metodo veikimą realioje aplinkoje. Naudojantis sukurtu programiniu modeliu ir jo generuojamais rezultatais, buvo atliekamas metodo atsparumo klastojimui įvertinimas.

Darbo rezultatų dalyje yra analizuojami RFID žymų apsaugos nuo klastojimo metodo sudarymo metu gauti rezultatai, pateikiamos viso darbo išvados, įvertinamas darbo įvade iškeltų tikslų ir užduočių išpildymas.

SUMMARY

Subject: Development and research of RFID tags anti-counterfeiting method

Author: Nerijus Čereška

This paper is addressed to RFID tags anti-counterfeiting problem: how to prevent significant counterfeiters get all important information from orginal tags or all RFID system. The disclosure of that information would provide a chance to create a genuine RFID tag means.

A work analysis is a part of a wider survey of RFID tags against counterfeiting problem, explores the general principles of operation of RFID technology and RFID tag categories. It is also explores possible RFID tags manipulation techniques, the avoidance opportunities, an overview and details of other authors to create protection methods and recommendations for a new RFID tags anti-counterfeiting method.

The next workflow is composed of new RFID tags anti-counterfeiting method according to the analysis of the recommendations made and the conclusions drawn, provide an initial approach to security analysis.

The software model is created by concluded RFID tag anti-counterfeiting method and a detailed description of the concept. The model simulates the performance of the method in a real environment. The ratings of resistance to RFID tags counterfeiting were set using this software model and its generated results.

The final part is dedicated to method‘s performance analysis, obtained results and conclusions. It also has objectives and tasks seen in the introduction to the work evaluation.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

- **RFID** (angl. *radio-frequency identification*) – radijo dažnio identifikavimo technologija;
- **RFID žyma** – lustas, kuris turi savo identifikacinę informaciją ir ją galima nuskaityti su specialiais žymų skaitytuvais;
- **RFID sistema** – sistema, sudaryta iš bent trijų komponentų: RFID žymos, žymų skaitytuvo su tarpine programine įranga ir duomenų bazės;
- **RFID žymos klastojimas** – neteisėtas žymos identifikacinės informacijos nuskaitymas, nustatymas ar modifikavimas, siekiant sukurti originalios žymos kopiją ir ją panaudoti neteisėtais tikslais;
- **EPC** (angl. *electronic product code*) – RFID technologija paremta sistema, kuri gali pilnai pakeisti šiuo metu plačiai naudojamą barkodų sistemą;
- **UPC** (angl. *universal product code*) – produktų identifikavimui naudojama barkodų sistema;
- **žymos identifikatorius** (ID) – RFID žymoje naudojamas parametras, kuris RFID sistemoje vienareikšmiškai nusako žymos tapatybę;
- **metaID** arba **UID** – žymos identifikatoriaus maišos reikšmė;
- **maišos užraktas** (angl. *hash-lock*) – metodas, kuomet RFID žymoje saugomas žymos metaID, o serverio duomenų bazėje saugomas žymos identifikatorius ID. Serverio programinė įranga gali suskaičiuoti pagal ID žymos metaID ir tuomet atlikti palyginimą;
- **MD5** – maišos skaičiavimo algoritmas, kuomet bet kokio ilgio duomenų eilutei sugeneruojama unikali fiksuoto ilgio (128 bitų) duomenų reikšmė;
- **SHA-1** – saugesnis nei MD5 maišos skaičiavimo algoritmas, kuomet bet kokio ilgio duomenų eilutei sugeneruojama unikali fiksuoto ilgio (160 bitų) duomenų reikšmė.

ĮVADAS

Šis darbas priklauso informacijos ir informacinių technologijų saugos studijų programai.

Darbo problematika ir aktualumas

Pastaruoju metu vis labiau plečiamos RFID technologija pagrįstos sistemos. Ši technologija vis plačiau naudojama logistikos sprendimuose, mažmeninės prekybos sektoriuje, taip pat visur, kur reikalingas greitas ir modernus objektų identifikavimo procesas bendroje informacinėje sistemoje. Vis didesne problema tampa RFID žymų klastojimas, kuris gali suteikti galimybę klastotojui manipuliuoti kompanijos, kurioje įdiegta RFID sistema, ištekliais bei kitais resursais. Klastotojas, pagaminęs RFID žymos klastotę, gali neteisėtai pasisavinti tam tikrą fizinį resursą, kuriam buvo priskirta originali RFID žyma arba patekti prie išteklių, prie kurių gali patekti tik originalios RFID žymos savininkas.

Darbo tikslas ir uždaviniai

Šio darbo pagrindinis tikslas yra sudaryti RFID žymų apsaugos nuo klastojimo metodą ir atlikti jo visapusišką atsparumo klastojimui įvertinimą. Darbo uždaviniai:

- išanalizuoti ir nustatyti didžiausias galimas grėsmes, pavojus ir pažeidžiamumus, kurių sėkmingi rezultatai galėtų leisti sukurti originalių RFID žymų klastotes;
- apžvelgti keletą esamų RFID žymų apsaugos nuo klastojimo metodų ir išskirti svarbiausius principus, kurių sėkmingas taikymas, galėtų užkirsti kelią RFID žymų klastojimo problemai;
- sukurti naują bei savitą RFID žymų apsaugos nuo klastojimo metodą, pritaikius geriausius nustatytus apsaugos nuo klastojimo principus ir vengiant kituose metoduose pastebėtų trūkumų;
- atlikti sukurto metodo kiekybinį ir kokybinį įvertinimą, bei palyginimąją analizę su apžvelgtais RFID žymų apsaugos nuo klastojimo metodais.

Darbo struktūra

Šiame darbe yra keturi pagrindiniai skyriai.

Pirmame skyriuje yra pateikiama RFID žymų klastojimo problemos analizė, apžvelgti RFID technologijos principai, žymų kategorijos. Taip pat pateikiama detali kitų autorių RFID žymų apsaugos nuo klastojimo metodų analizė, pateikiamos bendros išvados ir rekomendacijos tolimesniam darbui.

Antras skyrius yra skirtas pateikti sudaryto RFID žymų apsaugos nuo klastojimo metodo dokumentaciją. Aprašomi visi metode naudojami parametrai, jų struktūra. Pateikiami detalūs metode vykstančių procesų aprašymai ir struktūrinės schemos. Skyriaus gale pateikiama pradinė sudaryto metodo saugumo analizė, prioritetą skiriant RFID žymų apsaugai nuo klastojimo.

Trečiame skyriuje yra pateikiama sudaryto metodo programinio modelio struktūra ir eksperimentinės eigos pavyzdys, kuriame parodomas detalus programinio modelio veikimo procesas.

Ketvirtas skyrius yra skirtas sudaryto metodo detaliam tyrimui pateikti. Sudarytas RFID žymų apsaugos nuo klastojimo metodas yra įvertintas kiekybiškai ir kokybiškai. Kiekybinis įvertinimas atspindi sudaryto metodo generuojamų duomenų patikimumo skaitines išraiškas, o kokybinis įvertinimas – sudaryto metodo analitinį savybių palyginimą su pirmojo skyriaus metu apžvelgtais saugumo metodais.

Darbo pabaigoje yra pateikiamos galutinės viso darbo išvados ir apibendrinimas, naudotos literatūros sąrašas, bei priedas, kuriame pateikiami tarpiniai entropijos skaičiavimo rezultatai, gauti sudaryto metodo kiekybinio įvertinimo dalyje.

1. RFID ŽYMŲ APSAUGOS NUO KLASTOJIMO PROBLEMA

1.1. Problemos apžvalga

Šiuo metu labai daug dėmesio yra skiriama privatumo didinimo technologijų tobulinimui ir prieigos kontrolės mechanizmams RFID sistemose, nors labai svarbūs saugumo pažeidžiamumai, tokie kaip RFID žymų klastojimas, yra šiek tiek primirštas [1].

Žymų klastojimas yra viena rimčiausių saugumo problemų visoje RFID infrastruktūroje, todėl žymų apsaugos nuo klastojimo technologijos, turėtų būti prioritetas moksliniuose tyrimuose.

Norint suklastoti RFID žymą, reikia tinkamai išgauti jos identifikacinius duomenis. Paprastai tai nebūna sunku įvykdyti, nes žymomis galima manipuliuoti, pasitelkiant įvairius žymų skaitytuvus. Skaitytuvų galima laisvai įsigyti, jie netgi būna įdiegti mobiliuose telefonuose [2].

Kuomet įsilaužėlis nuskaito žymos identifikacinius duomenis, jis gali lengvai pagaminti originalios žymos klastotę ir ją panaudoti įvairiems piktavališkams veiksmams atlikti. Pavyzdžiui, įsilaužėlis gali suklastoti brangesnio produkto RFID žymą su pigesnio produkto žymos identifikaciniais duomenimis. Egzistuoja netgi žymos suklastojimas, įrašant į ją tam tikrą piktavališką kodą [3].

Tokios žymos nuskaitymas RFID sistemoje gali sukelti labai rimtų pasekmių: visos sistemos funkcionalumo sutrikdymą, pavyzdžiui, leisti įvykti atsisakymo tarnauti (angl. *DoS*) atakai.

RFID žymų klastojimo problemos esmė yra tai, jog RFID infrastruktūroje nėra patikimo mechanizmo, kuris atskirtų originalius ir suklastotus sistemos komponentus. Žymų skaitytuvui yra sudėtinga atskirti, ar jis komunikuoja su originalia žyma, ar su jos klastote. Todėl žymų klastojimo problemą galima suformuluoti tokiu klausimu: kaip žymų skaitytuvui suprasti, jog jis komunikuoja su ta RFID žyma, su kuria ir turėtų komunikuoti? [4].

1.2. RFID sistemų kategorijos

Pagal sandarą RFID sistemos skirstomos į dvi pagrindines kategorijas [5]:

- pasyvios sistemos;
- aktyvios sistemos.

Pasyvių sistemų RFID žymos neturi savo siųstuvo ir energijos šaltinio. Jos paprasčiausiai grąžina atgal radijo bangas, kurios ateina iš skaitytuvo antenos. Aktyvių sistemų RFID žymos yra atvirkščias variantas pasyvioms RFID žymoms: jos turi savo siųstuvus ir energijos šaltinį. Energijos šaltiniu dažniausiai būna baterija.

Tolesniuose skyreliuose detaliau apžvelgiamos pasyvių ir aktyvių RFID sistemų savybės.

1.2.1. Pasyvios RFID sistemos

Šio tipo RFID sistemų žymos ir skaitytuvai turi nedidelį tarpusavio komunikavimo nuotolį – nuo kelių milimetrų iki kelių metrų. Pasyvių žymų atsakikliai gali būti montuojami bet kur: plastikinėse kortelėse, plastikinių konteinerių sienelėse ir t.t. Nuo montavimo sudėtingumo, atitinkamai priklausys ir žymos kaina. Tačiau tokios žymos yra daug pigesnės už aktyvias RFID žymas ir nereikalauja didelės priežiūros.

Pasyvios RFID žymos skirstomos į tris kategorijas, kurių parametrai pateikti 1.1 lentelėje:

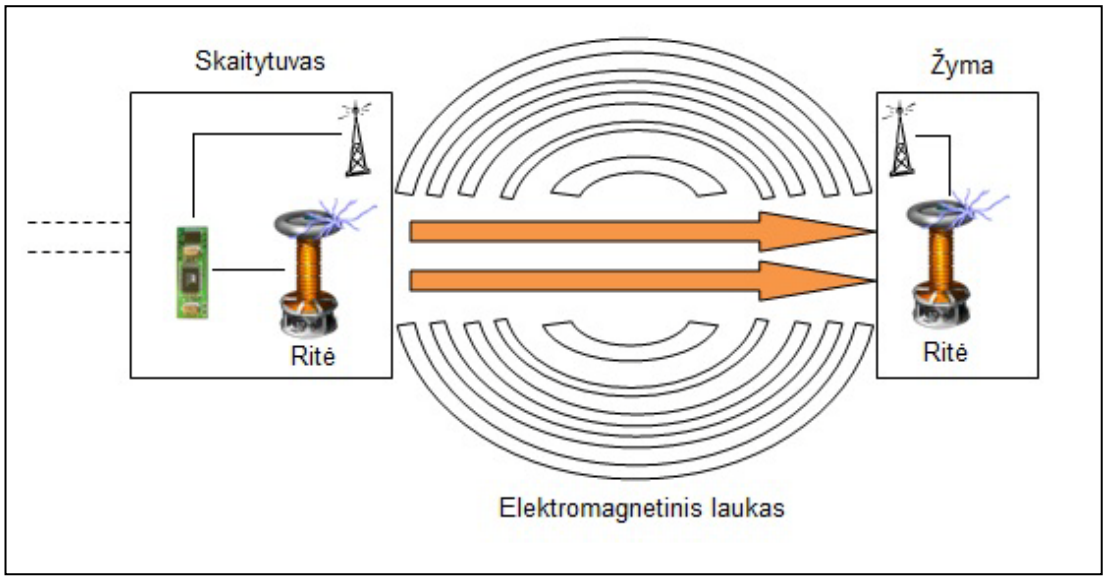
1.1 lentelė. Pasyvių RFID žymų kategorijos

Dažnio tipas	Veikimo dažniai	Atstumas	Naudojamas metodas
Žemas	125 kHz 134 kHz	iki 0,3 metro	Indukcinės sankabos
Aukštas	13,56 MHz	iki 1 metro	
Labai aukštas	860 MHz 960 MHz	iki 3,3 metro ir daugiau	Sklidimo movos

Esminis skirtumas tarp skirtingų dažnio tipų yra tas, jog didinant dažnį, didėja veikimo atstumas tarp pasyvios žymos ir skaitytuvo, tačiau mažėja radijo signalo patikimumas. Žemo dažnio RFID žymas galima sėkmingai nuskaityti per kažkokį trukdį, pavyzdžiui, sieną ar vandenį. Naudojant labai aukšto dažnio RFID žymas, radijo bangos nebegali pereiti per trukdžius. Radijo bangos paprasčiausiai gali atšokti nuo trukdžio ir niekada nepasiekti RFID žymos. Vanduo taip pat „sugeria“ aukšto dažnio radijo bangas. Todėl taikant aukšto dažnio pasyvias RFID žymas, reikia sudaryti idealias sąlygas joms komunikuoti su sistemos žymų skaitytuvais.

Tačiau kuo mažesnis veikimo atstumas, tuo yra sunkiau klastotojui bandyti suklastoti RFID žymas. Taikant pasyvias žymas, klastotojas su savo žymų skaitytuvu, turi patekti praktiškai minimaliu atstumu nuo konkrečios žymos. Nors tai praktiškai sunkiau įgyvendinti, ypač taikant žemo dažnio pasyvias žymas, bet vis dėlto yra įmanoma.

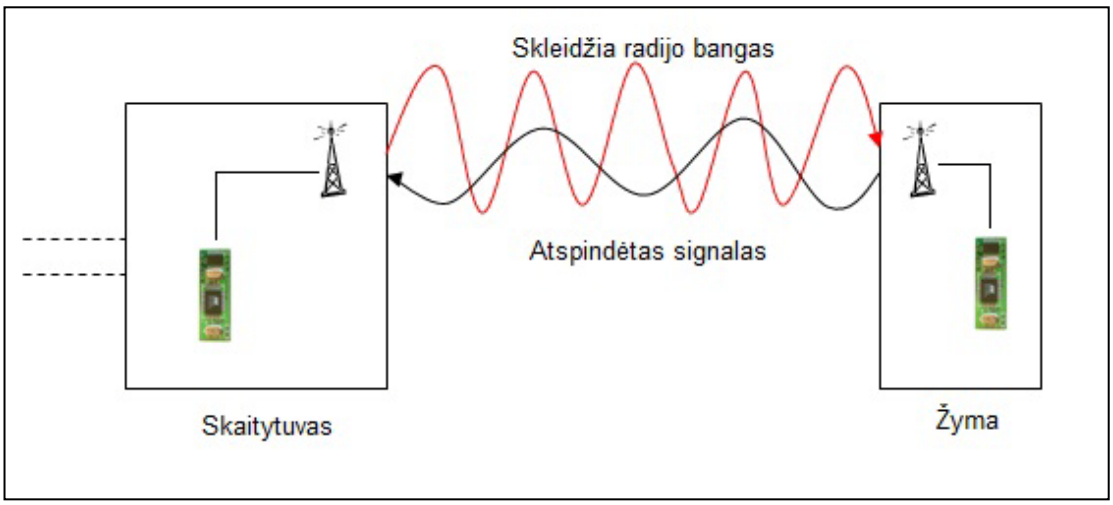
Žemo ir aukšto dažnio RFID žymos naudoja indukcinės sankabos (angl. *inductive coupling)* metodą. Tarp skaitytuvo ritės ir žymoje eančios ritės (1.1 pav.) suformuojamas elektromagnetinis laukas. Laukui suformuoti panaudojama skaitytuvo ritės energija. Pasyvi žyma gauna energiją iš šio lauko, panaudoja tą energiją savo luste ir pakeičia magnetinį lauką ant savo antenos. Tuomet skaitytuvo antena fiksuoja magnetinio lauko pasikeitimus ir konvertuoja juos į nulius bei vienetus, t.y. į dvejetainę sistemą. Pagal gautus duomenis, atitinkamai fiksuojama RFID žymos identifikacinė informacija, pavyzdžiui, unikalus identifikatorius.



1.1 pav. Indukcinės sankabos metodo veikimo schema

Indukcinės sankabos metodas naudojamas tik žemo ir aukšto dažnio pasyviose RFID žymose. Tokiam metodui realizuoti, turi būti nedidelis atstumas (iki 1 metro, žiūr. 1.1 lent.) tarp žymoje esančios ritės ir ritės skaitytuve, nes kitu atveju elektromagnetinis laukas nebus sukuriamas ir nepavyks komunikuoti su RFID žymomis.

Labai aukšto dažnio RFID žymos naudoja sklidimo movos (angl. *propagation coupling*) metodą. Skaitytuvo antena skleidžia radijo bangas (1.2 pav.), tačiau elektromagnetinis laukas, priešingai nei taikant indukcinės sankabos metodą, nesukuriamas. Žyma kaupia siunčiamą energiją iš skaitytuvo antenos ir žymos lustas tą energiją panaudoja pakeisti savo antenos laukui. Tokiu būdu yra atspindimas pakeistas signalas skaitytuvo antenai. Pagal gautą radijo bangos signalą, skaitytuvas identifikuoja RFID žymą.



1.2 pav. Sklidimo movos metodo veikimo schema

Pagrindinis pasyvių RFID žymų trūkumas yra tai, jog jos neturi pakankamai energijos atlikti pilnavertį šifravimą, kuris yra svarbus, jei norima apsaugoti žymas nuo jų klastojimo. Todėl pasyviose žymose dažniausiai naudojami „ypač lengvi“ (angl. *ultra lightweight*) kriptografiniai šifravimo metodai.

Dėl pasyvių RFID žymų energijos šaltinio neturėjimo ir minimalios kainos, jos turi labai minimalias galimybes: saugoti paprastą savo identifikatorių ir labai ribotą kiekį papildomos informacijos. Todėl saugumo metodai privalo būti sudaryti atsižvelgiant į minimalias pasyvių žymų skaičiavimo galimybes ir mažą vidinę atmintį. Tai labai apriboja dabartinių RFID žymų apsaugos nuo klastojimo sprendimų pasirinkimą, nes dažnai srendimas yra teoriškai puikiai įgyvendintas, tačiau praktiškai jį pritaikyti pasyviose RFID žymose yra sunku ar net neįmanoma.

Atsižvelgiant į apsaugos nuo klastojimo sprendimų realizavimo ribotumą, naudojami paprasti kriptografiniai metodai. Tokie metodai paprastai remiasi dalinės informacijos dalinimųsi tarp RFID sistemos elementų (paprastai tarp žymų skaitytuvo ir žymų, bet nebūtinai). Dalinimąsis turi būti atliktas maksimaliai saugiai, t.y. žymos tapatybė turi būti apsaugota nuo pašalinio jos atskleidimo.

1.2.2. Aktyvios RFID sistemos

Aktyvios RFID žymos naudojamos su dideliais kroviniais, pavyzdžiui, jūriniais konteineriais uostuose, kurie turi būti sekami tam tikroje teritorijoje. Tokios žymos veikia 455 MHz, 2,45 GHz arba 5,8 GHz dažniu ir skaitymo nuotolis paprastai būna iki 100 metrų.

Aktyvios RFID žymos būna dviejų tipų:

- atsakikliai (angl. *transpoders*);
- švyturiai (angl. *beacons*).

Atsakikliai yra prikeliami tada, kai gauna signalą iš skaitytuvo. Tokio tipo žymos paprastai naudojamos identifikuoti pro skaitytuvą judantį objektą, pavyzdžiui, į logistikos centrą atvažiavusį sunkvežimį. Sunkvežimiui privažiavus prie logistikos centro vartų, esantis netoliese skaitytuvas aktyvuoja ant priekinio stiklo pritaisytą RFID žymos atsakiklį, kuris persiunčia savo duomenis skaitytuvui. Tokiu būdu nustatomas sunkvežimio identifikacinis numeris. Tuomet numeris perduodamas į valdymo centrą, kur darbuotojai toliau atlieka tam tikrus veiksmus.

Atsakikliai paprastai tausoja savo baterijos gyvavimo laiką, nes jie siunčia savo identifikacinius duomenis tik tada, kai to pareikalauja skaitytuvas.

Švyturiai naudojami realaus laiko pozicijos nustatymo sistemose (angl. *RTLS*), kur reikia nustatyti tikslią objekto buvimo vietą. Švyturys skleidžia signalą su jo unikaliu identifikaciniu numeriu tam tikrais intervalais. Tas signalas yra pagaunamas bent trijų skaitytuvų antenų, kurios išdėstytos teritorijoje, kurioje yra sekamas objektas. Pagal trijų skaitytuvų užfiksuotus duomenis, galima tiksliai

nustatyti objekto buvimo vietą. Tokio tipo RFID žymos paprastai naudojamos automobilių gamyklose, logistikos centruose.

Dėl signalo siuntimo periodiškumo, švyturio baterija nėra tausojama. Todėl šio tipo žymos ne tokios efektyvios kaip atsakikliai.

Yra tokia neformali taisyklė: kuo didesnė žyma, tuo didesnis atstumas iš kurio ją galima nuskaityti.

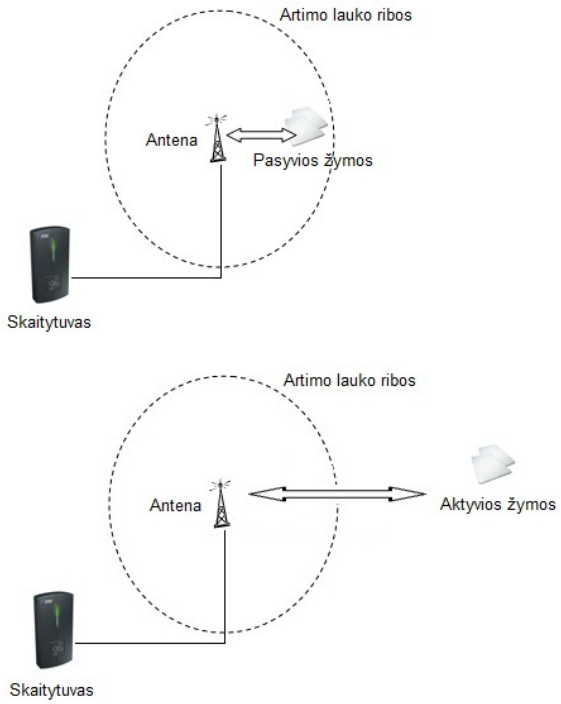
1.3. Artimo lauko reiškinys RFID sistemose

Artimas laukas (angl. *near field*) yra tam tikras reiškinys, kuris vyksta pasyviose ir aktyviose RFID sistemose [6]. Elektromagnetinio lauko magnetinė dalis yra pakankamai stipri tam, kad būtų sukuriamas mažas ir trumpai gyvuojantis elektrinis impulsas. Tokio impulso pilnai pakanka, jog RFID žymai būtų suteikta pakankamai energijos ir ji suspėtų nusiųsti atsakymą skaitytuvui. Artimas laukas veikia tam tikru nuotoliu, kuris apskaičiuojamas pagal tokią išraišką:

$$r = \alpha/2\pi \tag{1}$$

kur α yra bangos ilgis. Pavyzdžiui, pasyvios aukšto dažnio RFID žymos veikia 13,56 MHz dažniu. Tokio dažnio bangos ilgis yra apie 22 metrus, todėl teoriškai pasyvios aukšto dažnio RFID žymos turėtų būti nuskaitomos 22/6,28 = 3,5 metro atstumu.

Artimo lauko reiškinys pasyviose ir aktyviose RFID sistemose pavaizduotas 1.3 paveiksle:



1.3 pav. Pasyvių ir aktyvių RFID žymų palyginimo schema, artimo lauko reiškinio požiūriu

1.4. Duomenys RFID žymose

Priklausomai nuo RFID žymos tipo, duomenų kiekis žymoje gali būti įvairus: nuo kelių bitų iki kelių megabaitų [7]. Duomenys saugomi įvairiais formatais, svarbu tik tai, kad skaitytuvas ir žyma būtų suderinti ir palaikytų atitinkamus formatus. EPC sistema, gali pilnai pakeisti šiuo metų esančią UPC, kitaip dar žinomą kaip barkodų sistemą.

EPC sistema naudoja GID-96 formatą. Toks formatas turi 96 bitus (12 baitų) duomenų. Duomenų laukas sudarytas iš keturių dalių:

- antraštė (8 bitai);
- kompanijos identifikatorius (28 bitai);
- grupės identifikatorius (24 bitai);
- serijinis numeris (36 bitai).

Kitokių tipų RFID žymų struktūra gali būti skirtinga: su daugiau ar mažiau sudedamųjų dalių, tačiau pagrindiniai atminties sudarymo principai išlieka panašūs. Kiekvienoje žymoje yra unikalus identifikatorius, pagal kurį serverio duomenų bazėje yra surandama platesnė informacija apie tos žymos paskirtį.

1.5. RFID sistemų atakos ir pažeidžiamumai

Kaip ir bet kurios kitos technologinės sistemos, RFID sistemos taip pat yra pažeidžiamos. Tai tik laiko, pastangų ir išteklių klausimas.

Prieš analizuojant galimas grėsmes, reikia nustatyti atakuojamą objektą. RFID sistemose atakuojami gali būti tokie objektai:

- galinis serveris su duomenų baze bei programine įranga;
- žymų skaitytuvas;
- RFID žyma.

Taip pat galimos įvairios kombinacijos, pavyzdžiui, atakuojamas duomenų srautas (naudojamas slaptas duomenų nuskaitymas) tarp RFID žymos ir žymų skaitytuvo.

Šiame darbe labiau akcentuojami pažeidžiamumai, kurie leidžia perimti RFID žymos identifikacinius duomenis ir pagal juos sukurti žymos klastotę. Tokie pažeidžiamumai paprastai yra vykdomi tarp žymų skaitytuvo ir žymos. Todėl dėmesys galiniam serveriui bus mažesnis ir bus daroma prielaida, jog žymų skaitytuvas su galiniu serveriu yra sujungtas saugiu kanalu.

Tradicinė IT saugos teorija labiau linkusi koncentruotis į duomenų apsaugojimą. Tačiau nagrinėjant RFID saugos problemas, reikia atsiminti, jog kartais fizinis ir intelektualus turtas yra svarbesnis nei tam tikri duomenys. Pavyzdžiui, neteisėtu būdu yra suklastojama įmonės darbuotojo prieigos prie įmonės išteklių kortelė. Tuomet asmuo turintis suklastotą kortelę, įgyja visas teises į

įmonės turtą, kokias turi ir originalios kortelės turėtojas. Pavyzdžiui, jis gali pasinaudoti tam tikrais fiziniais resursais, o ne duomenimis. Šiuo atveju prieigos kortelės suklastojimas neturėjo neigiamos įtakos duomenų bazės veikimui. Ataka nebuvo nukreipta į duomenų bazę, todėl duomenys joje liko nemodifikuoti ir neištrinti. Buvo atliktas tik kortelės identifikacinių duomenų perėmimas, kur nereikalinga tiesioginė komunikacija su duomenų baze.

RFID sistemų atakas galima suskirstyti į keturias pagrindines grupes [7]:

- radijo dažnių manipuliavimas;
- žymose esančių duomenų manipuliavimas;
- tarpinės programinės įrangos (angl. *middleware*) manipuliavimas;
- atakos, nukreiptos į sistemos galinį serverį, kuriame yra duomenų bazė (angl. *backend database*).

Labai dažnai naudojamos mišrios atakos, t.y. šių atakų deriniai, siekiant vieno tikslo įgyvendinimo.

Tolesniuose skyreliuose pateikiama detalesnė kiekvienos atakų grupės analizė, pirmenybę teikiant galimam atakų panaudojimui, siekiant suklastoti RFID sistemoje esančias žymas.

1.5.1. Radijo dažnių manipuliavimas

Šio tipo atakos remiasi tuo, jog galima neteisėtai manipuliuoti artimo lauko reiškiniu. Pagal manipuliavimo tipą, šias atakas galima suskirstyti į tam tikras radijo dažnio manipuliavimo atakų grupes:

- suklastojimo (angl. *spoofing*) ataka – tiekiama neteisinga informacija, kuri pagal formatą yra teisinga ir RFID sistema ją priima. Pavyzdžiui, siunčiamas neteisingas EPC žymos identifikacinis numeris, kai sistema tikisi sulaukti teisingo. Tokiu būdu trikdomas RFID sistemos darbas, nes galinis serveris neras duomenų bazėje neteisingo identifikacinio numerio;
- slapto pasiklausymo (angl. *eavesdropping*) ataka – slaptas duomenų nuskaitymas, kai klastotojas įsiterpia tarp žymos ir skaitytuvo su savo įrenginiu ir bando nuskaityti keliaujantį duomenų srautą. Paprastai šios atakos sėkmingas rezultatas yra tiesus kelias į RFID žymos klastotės gaminimą, jei yra nuskaitomi originalūs duomenys ir tuos duomenis galima iššifruoti;
- įterpimo (angl. *insert*) ataka – bandoma įterpti sistemines komandas vietoje duomenų. Dažniausiai tokios komandos yra su blogu scenarijumi ir jos gali sustrikdyti RFID sistemos veikimą. Pavyzdžiui, su žymos identifikaciniais duomenimis, bandoma įterpti tokią komandą, kuri ištrintų tam tikrus duomenis duomenų bazėje;

- pakartojimo (angl. *replay*) ataka – sistemos užklausa sustabdoma kelyje tarp RFID žymos ir skaitytuvo. Duomenys perimami ir modifikuojami. Toliau tie modifikuoti duomenys siunčiami į skaitytuvą. Duomenys atrodo kaip teisingi ir skaitytuvas juos priima;
- atsisakymas tarnauti (angl. *DoS*) ataka – signalas užtvindomas daugiau duomenų negu yra numatyta. Todėl sistema nesugeba tinkamai priimti įeinančių duomenų. Taip pat galimas ir žymos užtvindymas dideliu kiekiu užklausų, siekiant išgauti kuo daugiau atsakymų. Atsakymai analizuojami ir bandoma išsiaiškinti žymos identifikacinę informaciją;
- stebėjimo (angl. *tracking*) ataka – piktnaudžiavimas RFID technologija, slaptam vietų ar veiksmų stebėjimui.

Dauguma aprašytų atakų yra daugiau ar mažiau veiksmingos, siekiant pagaminti RFID žymos klastotę. Todėl radijo dažnių manipuliavimas yra pagrindinė grėsmė, sprendžiant RFID žymų apsaugos nuo klastojimo problemą.

1.5.2. Žymose esančių duomenų manipuliavimas

Šio pažeidžiamumo esmė yra tai, jog įsilaužėlis siekia pakeisti žymose esančius duomenis. Pavyzdžiui, įsilaužėlis gali sukeisti prekės RFID žymos identifikatorių su kitos prekės žymos identifikatoriumi. Paprastai siekiama sukeisti brangesnės prekės identifikacinę informaciją su pigesnės prekės analogiška informacija. Todėl nuskaičius skaitytuvu modifikuotą žymą galima patirti tam tikrus nuostolius (produktas parduotas už daug mažesnę kainą ir pan.).

Toks pažeidžiamumas paprastai yra galimas tuomet, kai žymos duomenis gali nuskaityti bet kokie skaitytuvai, t.y. neautentifikuoti žymoje.

1.5.3. Tarpinės programinės įrangos manipuliavimas

Tokios atakos vykdomos tarp skaitytuvo ir nutolusios duomenų bazės. Siekiama perimti siunčiamus duomenis. Kadangi tokių duomenų siuntimą valdo tam tikra programinė įranga, ji ir yra atakuojama.

Ši programinė įranga yra RFID sistemos „smegenys“. Ji apdoroja mažą kiekį informacijos (gautą iš RFID žymos) į tam tikrą platesnį formatą. Pavyzdžiui, iš RFID žymos skaitytuvas nuskaitė tokius duomenis: `Jonas Jonaitis, 5 sandėlis, 8:00-17:00`. Patys šie duomenys nieko nereiškia, todėl tarpinė programinė įranga paverčia juos į prasmingą komandą, su kuria galima atlikti tam tikrą veiksmą: „*Įleisti darbuotoją Joną Jonaitį į 5 sandėlį, jei laikas yra tarp 8:00 ir 17:00.*“ Taip pat suformuota informacija yra įrašoma į duomenų bazę: „*Jonas Jonaitis įėjo į 5 sandėlį, tam tikru laiku. Išėjo tam tikru laiku*“. Tokiu būdu fiksuojami sistemos įvykiai, t.y. vykdomas auditas.

Ši programinė įranga yra pati pažeidžiamiausia visoje RFID sistemoje, nes ji yra beveik pilnai automatizuota ir ja galima manipuliuoti. Tačiau tam reikalingas fizinis priėjimas prie šios programinės įrangos, kuris paprastai būna sunkiai gaunamas. Lengviau yra įvykdyti radijo dažnių manipuliavimą nei šio tipo atakas.

Labai svarbu yra tai, jog tarpinė programinė įranga tinkamai patikrintų, kas yra įrašoma į duomenų bazę. Tinkamas patikrinimas leidžia apsisaugoti nuo suklastotų RFID žymų ir aptikus tokias žymas – jas užblokuoti ar imtis kitų numatytų veiksmų, numatytų RFID sistemos saugos politikoje.

1.5.4. Atakos, nukreiptos į galinėje sistemos dalyje esančią duomenų bazę

Tokios atakos yra pačios efektyviausios, nes dažniausiai, duomenų bazėse yra saugoma labai svarbi informacija (mokėjimų kortelių duomenys, klientų asmeniniai duomenys ir kiti svarbūs RFID žymų identifikaciniai duomenys). Tačiau, duomenų bazės yra toliausiai nutolusios nuo pačios RFID sistemos, todėl šios atakos ir sunkiausiai įvykdomos.

1.6. RFID saugumo metodai

Pageidaujamos saugumo savybės, kurias turėtų užtikrinti kiekvienas RFID sistemos saugumo metodas: privatumas, vientisumas, autentiškumas, pasiekiamumas, anonimiškumas ir nesusekamumas.

Privatumas šiuo atveju apima šiuos aspektus: skirtingi poreikiai skirtingiems vartotojams, autentifikavimas ir identifikavimas.

Norint pilnai išpildyti šias savybes, reikia naudoti stiprius kriptografinius metodus, kurių, deja, neįmanoma tinkamai įdiegti RFID žymose, dėl jų mažų resursų ir kainos. Todėl yra kuriamos alternatyvos – pigūs ir pakankamai saugūs kriptografiniai metodai, kurie padidina komunikacijos saugumo lygį tarp RFID žymos ir skaitytuvo.

Žiūrint į RFID sistemas holistiniu požiūriu, jose egzistuoja labai stiprus ryšys tarp stabilaus veikimo, kainos ir saugumo [9]. Todėl, kuriant kriptografinius sprendimus šioms sistemoms, reikia į juos atsižvelgti. Galima tinkamai įgyvendinti bet kuriuos du kriterijus iš trijų: stabilus veikimas ir saugumas, stabilus veikimas ir kaina, kaina ir saugumas. Tačiau yra labai sudėtinga įgyvendinti juos tinkamai vienu metu.

Šiuo metu egzistuoja gana nemažai lengvų kriptografinių metodų (kartais dar vadinamų tiesiog protokolais), kurie, jų autorių teigimu, užtikrina RFID sistemos apsaugą nuo klastojimo. Tačiau, vertėtų išsiaiškinti kelių metodų atsparumą RFID žymų klastojimui.

Toliau pateikiamas populiarių RFID saugumo metodų analizės tyrimas.

Hoopad Mobahat atliko tyrimą [8], kuriame įvertino šešis RFID žymų apsaugos nuo klastojimo metodus. Įvertinimas buvo atliekamas analizuojant, ar tam tikras metodas yra atsparus tam tikram RFID sistemos pažeidžiamumui. Tyrimo rezultatai pateikti 1.2 lentelėje:

1.2 lentelė. RFID saugumo metodų palyginimas

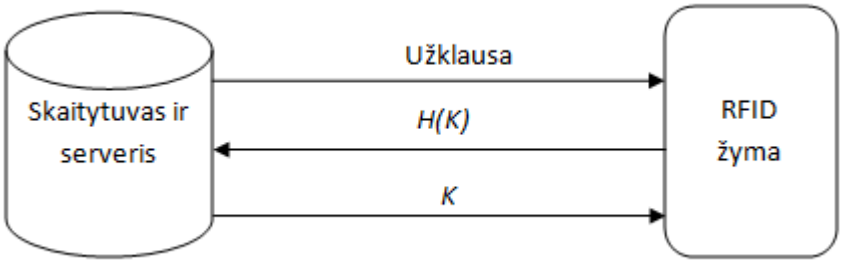
Pažeidžiamumai	**Metodai**					
	RHLK	**HIDV**	**SRAC**	**HBIV**	**LCRP**	**A-SRAC**
Informacijos nutekinimas	-	-	-	-	Apsaugota	Apsaugota
Suklastojimo ataka	Neapsaugota	-	Neapsaugota	Apsaugota	Apsaugota	Apsaugota
Pakartojimo ataka	-	Apsaugota	Neapsaugota	Apsaugota	Apsaugota	Apsaugota
Persiuntimo saugumas	Neapsaugota	-	Apsaugota	Apsaugota	-	-
Desinchronizavi-mas	-	Apsaugota	-	-	Neapsaugota	Apsaugota
Vietos privatumas	Neapsaugota	Apsaugota	Neapsaugota	Neapsaugota	Neapsaugota	-
Abipusė autentifikacija	Yra	Nėra	Yra	Yra	-	-
Atsisakymo tarnauti ataka	Neapsaugota	-	Neapsaugota	Neapsaugota	Neapsaugota	-

Analizuojant tyrimo rezultatus, galima teigti, jog labiausiai grėsmingas pažeidžiamumas, kuris leistų įvykdyti RFID žymų klastojimą, yra informacijos nutekinimas. Kaip matyti, apsaugą nuo informacijos nutekinimo turi tik du metodai: LCRP ir A-SRAC. Taip pat šie metodai yra apsaugoti ir nuo *suklastojimo* bei *pakartojimo* atakų.

Toliau pateikiama detalesnė šio darbo metu atlikta RFID saugumo metodų analizė, kurioje analizuojami jų veikimo principai ir apsaugos galimybės. Esminis aspektas skiriamas RFID žymų apsaugos nuo klastojimo įgyvendinimui.

1.6.1. RHLK metodas

RHLK metodas yra paremtas maišos užrakto (angl. *hash lock*) modeliu. RFID žymoje yra saugoma atsitiktinio rakto *K* maišos reikšmė, dar vadinama žymos *metaID*, t.y. *metaID = H(K)*. Kai skaitytuvas kreipiasi į žymą su skaitymo prašymo užklausa (1.4 pav.), žyma persiunčia savo *metaID*. Skaitytuvas perduoda gautą reikšmę galiniam serveriui. Serveryje esanti duomenų bazė ieško *metaID* reikšmės ir ją suradus, taip pat suranda ir rakto *K* reikšmę, nes jos saugomos kartu. *K* reikšmė perduodama skaitytuvui, kuris ją persiunčia žymai kaip atsakymą. Žyma paskaičiuoja *H(K)* reikšmę ir sulygina su savo *metaID* reikšme. Jei reikšmės sutampa, tuomet žyma veikia kartu su skaitytuvu.



1.4 pav. Maišos užrakto modelio veikimo schema

Tačiau pats maišos užrakto modelis neužtikrina duomenų nenutekėjimo, nes raktas *K* yra persiunčiamas iš duomenų bazės į žymą atviru formatu. Atakuotojas gali atlikti slaptą duomenų srauto stebėjimą ir taip sužinoti *K* raktą. Šis modelis remiasi prielaida, kad atakuotojas atakuos žymą ir sieks išgauti jos identifikatorių, todėl jis saugomas kaip maišos reikšmė. Tačiau, atakuotojas gali atlikti duomenų stebėjimą iš kitos pusės, t.y. iš serverio siunčiamų duomenų stebėjimą.

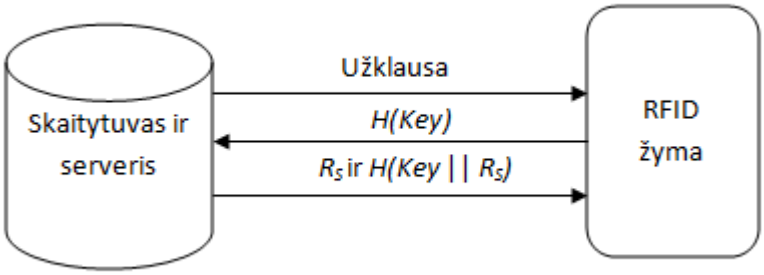
Pats RHLK metodas yra patobulintas maišos užrakto modelis, kuris naudoja atsitiktinius žymos atsakymus į skaitytuvo užklausas, o ne fiksuotus, kaip yra tradiciniame maišos užrakto modelyje. Šis metodas neužtikrina vietos privatumo, nes skaitytuvas visada atsako su statiniu žymos identifikaciniu numeriu. Taip pat nėra užtikrinamas ir duomenų nenutekėjimas, o tuo pačiu ir apsauga nuo klastojimo.

Aprašytuose maišos užrakto tipo metoduose, skaitytuvas tikisi, jog žyma atsakys į skaitytuvo užklausą, atsiųsdama maišos reikšmę su savo identifikacine informacija. Tuomet skaitytuvas kreipsis į galinį serverį su prašymu autentifikuoti RFID žymą. Tačiau, netgi nekreipiant dėmesio į tai, kad maišos funkcijos skaičiavimas pasyviose RFID žymose yra labai neefektyvus (techniniai resursai dėl žymų kainos nėra pakankami), tokie maišos užrakto tipo metodai turi nemažai problemų: sinchronizacijos ir lankstumo problema, neatsparumas *suklastojimo* ir *slapto stebėjimo* atakoms.

Pats maišos užrakto modelis nėra tinkamas spręsti RFID žymų apsaugos nuo klastojimo problemą, tačiau yra modifikuotų metodų, kurie išsprendžia maišos užrakto modelio problemas.

1.6.2. SRAC ir A-SRAC metodai

Taikant SRAC protokolą [10] kiekviena RFID žyma turi savo unikalų raktą *Key*. Supaprastinta veikimo schema pateikta 1.5 paveiksle. Pirmiausiai žymų skaitytuvas siunčia skaitymo užklausą žymai. Tai beveik standartinė procedūra visuose saugumo metoduose. RFID žyma atsako į užklausą siųsdama savo *metaID*, t.y. *metaID = H(Key)*.



1.5 pav. SRAC protokolo veikimo schema

Skaitytuvas, gavęs žymos *metaID* reikšmę, perduoda ją galiniam serveriui. Serverio programinė įranga ieško rakto *Key* duomenų bazėje pagal gautą *metaID*. Reikia pabrėžti, jog duomenų bazėje saugomos žymų *metaID* ir Key reikšmės.

Atlikęs paiešką ir suradęs žymos identifikatorių, serveris generuoja atsitiktinį skaičių R_S ir tikrina, ar reikšmė $H(Key \oplus R_S)$ yra unikali tarp kitų *metaID*, saugomų duomenų bazėje.

Tuomet yra atnaujinama *Key* reikšmė pagal dvi sąlygas:

Jei $H(Key_{Dabartinis}) = metaID$, tuomet atliekamos tokios atnaujinmo operacijos:

$$Key_{Ankstesnis} \leftarrow Key_{Dabartinis}$$

$$Key_{Dabartinis} \leftarrow H(Key_{Dabartinis} \oplus R_S)$$

Jei $H(Key_{Ankstenis}) = metaID$, tuomet aliekama tokia atnaujinimo operacija:

$$Key_{Dabartinis} \leftarrow H(Key_{Ankstesnis} \oplus R_S)$$

Galiausiai atliekama paskutinė atnaujinimo operacija:

$$Key \leftarrow Key_{Ankstesnis}$$

Serveris per žymų skaitytuvą persiunčia žymai dvi reikšmes: R_S ir $H(Key \,||\, R_S)$.

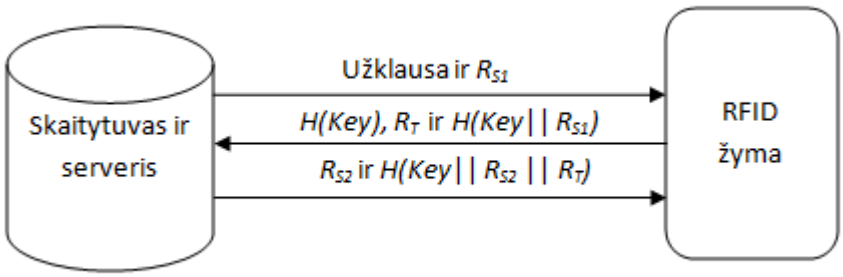
RFID žyma patikrina, ar tikrai gautos reikšmės yra tinkamos, t.y. paima gautą R_S reikšmę ir apskaičiuoja savo $H(Key \,||\, R_S)$. Jei apskaičiuota reikšmė sutampa su gautąja $H(Key \,||\, R_S)$ reikšme, žyma atnaujina savo raktą:

$$Key \leftarrow H(Key \oplus R_S)$$

Šiame metode apsauga nuo klastojimo yra realizuota pasitelkiant atsitiktinę informaciją, kuri yra saugoma RFID žymoje. Kiekviena žyma turės savo slaptą informaciją ir vienos žymos slaptos informacijos atskleidimas neturės jokių pasekmių kitų RFID sistemoje esančių žymų saugumui.

Tačiau, protokolo autoriai vis dėlto neužtikrina, jog protokolas apsaugos nuo *pakartojimo* atakos, kurios metu galima taip pat išgauti svarbios informacijos, reikalingos žymų klastojimui.

Todėl autoriai pasiūlė kitą alaternatyvą – A-SRAC protokolą (1.6 pav.), kuris jau nebeturi SRAC protokolo pažeidžiamumo.



1.6 pav. A-SRAC protokolo veikimo schema

Šiame protokole skaitytuvas siunčia užklausą RFID žymai su papildoma atsitiktine reikšme R_{S1}.

Žyma atsako siųsdama tris reikšmes: $H(Key)$, atsitiktinę reikšmę R_T ir $H(Key \,||\, R_{S1})$.

Toliau serveris, gavęs visas reikšmes, atlieka analogiškus veiksmus, kaip ir SRAC protokole, tačiau prieš tai dar patikrina ar gauta reikšmė $H(Key \,||\, R_{S1})$ yra teisinga.

Atlikęs paiešką ir suradęs žymos identifikatorių, serveris generuoja atsitiktinį skaičių R_{S2} ir tikrina, ar reikšmė $H(Key \oplus R_{S2})$ yra unikali tarp kitų *metaID*, saugomų duomenų bazėje.

Tuomet yra atnaujinama *Key* reikšmė pagal dvi sąlygas:

Jei H($Key_{Dabartinis}$) = *metaID*, tuomet atliekamos tokios atnaujinmo operacijos:

$$Key_{Ankstesnis} \leftarrow Key_{Dabartinis}$$

$$Key_{Dabartinis} \leftarrow H(Key_{Dabartinis} \oplus R_{S2})$$

Jei H($Key_{Ankstenis}$) = *metaID*, tuomet aliekama tokia atnaujinimo operacija:

$$Key_{Dabartinis} \leftarrow H(Key_{Ankstesnis} \oplus R_{S2})$$

Galiausiai atliekama paskutinė atnaujinimo operacija:

$$Key \leftarrow Key_{Ankstesnis}$$

Serveris per žymų skaitytuvą persiunčia žymai tokias reikšmes: R_{S2} ir $H(Key \,||\, R_{S2} \,||\, R_T)$.

Žyma patikrina gautos reikšmės $H(Key \,||\, R_{S2} \,||\, R_T)$ teisingumą ir atnaujina savo raktą:

$$Key \leftarrow H(Key \oplus R_{S2})$$

A-SRAC protokole yra įvesta abipusė autentifikacija, t.y. serveris autentifikuoja žymas tikrindamas $H(Key \,||\, R_{S1})$ reikšmes, o žymos autentifikuoja serverį tikrindamos $H(Key \,||\, R_{S2} \,||\, R_T)$ reikšmes. SRAC protokolas turi tik vienpusę autentifikaciją. Todėl A-SRAC yra atsparus *pakartojimo* atakoms.

1.6.3. Metodas pagal *Jemal Abawajy*

Jemal Abawajy siūlo kiek sudėtingesnį [11], nei SRAC ir A-SRAC metodai, RFID žymų apsaugos nuo klastojimo metodą, kuris gali būti įgyvendintas pritaikant standartines kriptografines maišos funkcijas.

Metodas turi du pagrindinius – registracijos ir komunikavimo etapus.

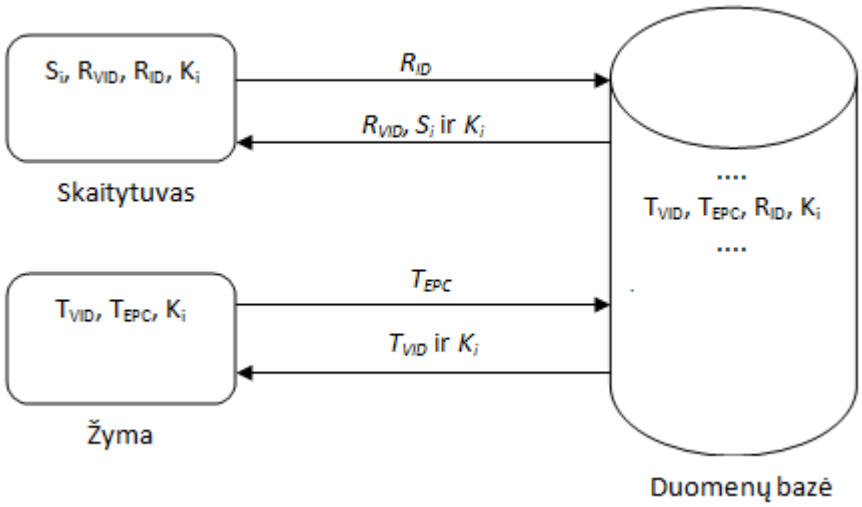
Serverio duomenų bazėje yra saugomi tokie duomenys:

$$D \leftarrow (T_{VID}, T_{EPC}, R_{ID}, K_i)$$

čia:

- T_{EPC} ir T_{VID} atitinka realius ir virtualius žymų identifikatorius;
- R_{ID} ir R_{VID} atitinka realius ir virtualius skaitytuvų identifikatorius;
- K_i atitinka galiojantį raktą, kuris naudojamas komunikuoti T_i žymai ir R_i skaitytuvui.

Raktas K_i yra generuojamas atsitiktinai, realūs žymos ir skaitytuvo identifikatoriai yra priskiriami jų gamintojų arba sistemos diegėjų.



1.7 pav. Metodo skaitytuvo ir žymos registracijos su serverio duomenų baze procesai

1.6.3.1. Skaitytuvo registracija

Kiekviename RFID sistemos skaitytuve R_i yra saugomi tokie duomenys:

$$R_i \leftarrow (S_i, R_{VID}, R_{ID}, K_i)$$

čia parametras S_i atitinka atsitiktinių skaičiaus generatoriaus sužadinimo reikšmę (angl. *seed*), kuri bus vienoda kiekvienai skaitytuvo ir serverio porai.

Skaitytuvo su serveriu registracijos metu, skaitytuvas iš serverio gaus tokias reikšmes (7 pav.):

$$R_i \leftarrow (S_i, R_{VID}, K_i)$$

čia parametras R_{VID} apskaičiuojamas pagal tokią išraišką:

$$R_{VID} \leftarrow h((D_{ID})_L \,||(R_{ID})_R) \otimes S_i$$

čia $(D_{ID})_L$ yra kairioji duomenų bazės identifikatoriaus pusė, o $(R_{ID})_R$ yra dešinioji registruojamo skaitytuvo identifikatoriaus pusė. Tarkime, dvejetainėje sistemoje $(D_{ID})_L = 11010$, o $(R_{ID})_R = 01110$. Tuomet R_{VID} bus maišos reikšmė: $R_{VID} \leftarrow h(1101001110) \otimes S_i$.

Parametras S_i yra atnaujinamas kiekvieną kartą, kai skaitytuvas komunikuoja su serveriu.

1.6.3.2. RFID žymos registracija

Kiekvienoje RFID žymoje T_i yra saugomi tokie duomenys:

$$T_i \leftarrow (T_{VID}, T_{EPC}, K_i)$$

Registracijos metu, kiekviena žyma gauna tokius duomenis:

$$T_i \leftarrow (T_{VID}, K_i)$$

Parametras T_{VID} apskaičiuojamas ta pačiai, kaip ir R_{VID}, tačiau nėra įtraukiamas parametras S_i, nes jis skirtas tik skaitytuvo ir serverio komunikavimui:

$$T_{VID} \leftarrow h((D_{ID})_L \,||(R_{ID})_R)$$

1.6.3.3. Komunikavimo etapas tarp žymos ir skaitytuvo

Šio etapo metu yra užtikrinama, kad skaitytuvas komunikuotų tik su originaliomis RFID žymomis, o ne suklastotomis.

Sistemoje yra *x* kiekis žymų, t.y. $T = (T_1, \dots, T_x)$ ir *y* kiekis skaitytuvų $R = (R_1, \dots, R_y)$.

Šis metodas tinkamas naudoti su pasyviomis žymomis, todėl komunikavimo procesą inicijuoja žymų skaitytuvas. Kai skaitytuvas užklausia RFID žymą, ji skaičiuoja ir siunčia atgal tokius duomenis:

$$T_i \leftarrow ((T_a)_L \,||\, (T_v) \,||f(S))$$

čia parametras $(T_a)_L$ atitinka kairiąją žymos realaus identifikatoriaus pusę. Parametras T_v yra virtualus žymos identifikatorius, o funkcija *f(S)* sugeneruoja atsitiktinį skaičių.

Kai skaitytuvas gauna iš žymos duomenis T_i, jis pradeda vykdyti autentifikavimo procesą tam, kad išsiaiškintų, jog žyma yra tikrai ta, kuri ir turi būti. Pirmiausiai yra sukuriamas slaptas raktas K_s:

$$K_s \leftarrow (T_a)_L||(R_i)_R$$

čia $(T_a)_L$ yra žymos identifikatoriaus kairioji pusė, o $(R_i)_R$ yra komunikuojančio skaitytuvo dešinioji identifikatoriaus pusė.

Toliau yra apskaičiuojama slaptojo rakto K_s maišos funkcija $C \leftarrow h(K_s)$. Rezultatas C yra palyginamas su T_v ir jei jie sutampa, tuomet laikoma, kad RFID žyma yra originali ir nesuklastota. Priešingu atveju, skaitytuvas atmeta žymą ir laikoma, jog ji yra suklastota.

1.6.3.4. Metodo saugumo analizė

Metodo autoriaus teigimu, šis metodo yra praktiškas dėl šių priežasčių:

- reikalauja išties labai nedaug skaičiavimų, todėl gali būti realizuotas pasyviose RFID žymose;
- metodas užtikrina privatumą, nesusekamumą ir autentifikavimą, kas leidžia sistemai išvengti žymų klastočių priėmimo.

Šio metodo saugumo esmė yra ta, jog RFID žyma niekada nesiunčia savo realaus identifikatoriaus ar jo maišos reikšmės. Vietoje to yra siunčiama tik kairioji identifikatoriaus pusė $(T_a)_L$. Įsilaužėliui žinant tik vieną identifikatoriaus dalį, praktiškai yra neįmanoma sukurti tokios žymos klastotės, kuri patenkintų žymų skaitytuvo autentifikaciją.

Įsilaužėliui skenuojant siunčiamus pranešimus tarp žymos ir skaitytuvo, svarbi informacija nėra atskleidžiama, nes kiekvieną kartą, kai žyma siunčia reikšmę $((T_a)_L \,||\, (T_v) \,||f(S))$, ji yra paskaičiuojama su atsitiktinės funkcijos *f(S)* reikšme.

Jei žymos atsakymo reikšmė yra atsitiktinė, tuomet yra labai sunku įvykdyti *pakartojimo* ir *suklastojimo* atakas, nes šioms atakoms tinkamai įvykdyti reikia, kad siunčiami duomenys (tarp žymos ir skaitytuvo) būtų pastovūs, o ne kintami atsitiktinai.

Svarbiausias aspektas, kurį pastebėjome analizuojant šį metodą, yra tai, jog RFID žymoje yra saugomas unikalus jos identifikatorius T_{EPC}. Nors jis tiesiogiai ir nedalyvauja komunikuojant skaitytuvui ir žymai, tačiau jis vistiek saugomas laisvai prieinama forma. Kituose protokoluose, pavyzdžiui, SRAC ir A-SRAC, identifikatoriai yra saugomi žymose kaip maišos reikšmė, t.y. *H(ID)*.

1.6.4. Metodai pagal *Tassos Dimitriou*

Tassos Dimitriou pasiūlė paprastesnį metodą [12], kuriuo galima apsaugoti RFID žymas nuo jų klastojimo. Yra sudarytos dvi metodo versijos: paprastas ir sustiprintas metodai.

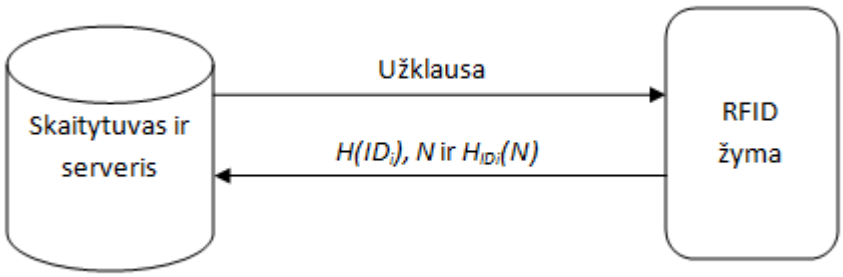
1.6.4.1. Paprasta metodo versija

Tiek paprastas, tiek sustiprintas metodai remiasi paslapties padalijimo principu tarp RFID žymos ir žymų skaitytuvo. Paprastai, paslaptis gali būti vienoda visoms žymoms, tačiau vienos žymos paslapties atskleidimas gali lemti visos RFID sistemos žymų nulaužimą. Todėl galima taikyti skirtingą

paslaptį kiekvienai žymai RFID sistemoje. Tačiau tai apkrauna žymų skaitytuvą ir serverį, nes jam tenka atskirti, kuri paslaptis, kuriai žymai priklauso.

Taikant paprastą *Tassos Dimitriou* metodą, slapta informacija yra žymos identifikacinis numeris, o paieška ir identifikavimas atliekamas naudojant identifikacinio numerio maišos reikšmę, t.y. *metaID*.

Metodas remiasi šiuo principu: jei žymos identifikacinis numeris keičiasi kiekvieną kartą po kiekvienos skaitytuvo užklausos, tuomet *slapto stebėjimo*, *pakartojimo* ir *suklastojimo* atakos negali sutrikdyti RFID sistemos saugumo.



1.8 pav. Paprasto metodo veikimo schema

Sistemos diegimo metu, RFID žymoje yra įrašomas pradinis identifikatorius ID_0, kuris yra parinktas kaip atsitiktinis numeris. Galinio serverio duomenų bazėje yra saugoma tapati informacija, kaip ir žymoje, bei maišos reikšmė $H(ID_0)$. Maišos reikšmė ir tampa pagrindiniu raktu ieškant informacijos apie konkrečią žymą.

Visą komunikavimo procesą galima aprašyti tokiais žingsniais (1.8 pav.):

- skaitytuvas siunčią užklausą RFID žymai;
- žyma sugeneruoja atsitiktinį kamšalą N ir siunčia atgal skaitytuvui tokią informaciją: $H(ID_i)$, N ir $H_{IDi}(N)$;
- skaitytuvas perduoda gautą informaciją galiniam serveriui;
- serverio duomenų bazė pagal gautą $H(ID_i)$ reikšmę ieško ir nustato žymos identifikatorių ID_i, nes jis yra saugomas kartu su jo maišos reikšme. Tuomet naudojama $H_{IDi}(N)$ reikšmė, kuri patvirtina žymos siųstos atsakymo žinutės autentiškumą.

Esminis šio metodo aspektas yra maišos reikšmė $H_{IDi}(N)$, kuri leidžia išvengti suklastotų žymų priėmimo į sistemą. Ši išraiška dar vadinama žinutės autentifikavimo kodu (angl. *message authentication code*), kur maišos reikšmei skaičiuoti įvedamas papildomas parametras K – simetrinis raktas: $H_K(M)$. Serverio duomenų bazėje yra saugomas žymos identifikacinis numeris ID_i, kuris ir tampa simetriniu raktu. Serveris skaičiuoja $H_{IDi}(N)$ ir sulygina su gautąja reikšme.

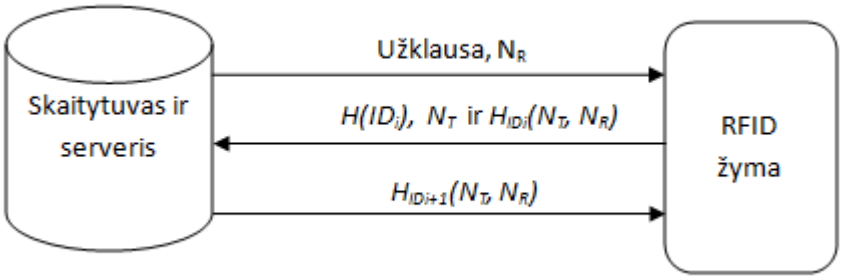
Kai tik patvirtinamas žymos autentiškumas, duomenų bazė atnaujina žymos identifikaciją. Identifikatoriui atnaujinti naudojamas „negrįžtamas“ skaičiavimas ir tokiu būdu yra gaunama ID_{i+1}

reikšmė. Žymoje taip pat įrašomas naujas identifikatorius ir ištrinama iš atminties sena informacija N ir ID_i.

1.6.4.2. Sustiprinta metodo versija

Sustiprintoje metodo versijoje autentifikavimas atliekamas kiekvienoje pusėje, t.y. skaitytuvo pusėje žymos autentifikavimą atlieka serveris, o žymos pusėje yra atliekama skaitytuvo autentifikacija. Paprastas metodo turi tik vienpusę autentifikaciją – serveris autentifikuoja RFID žymą.

Sustiprinto metodo veikimo schema pateikta 1.9 paveiksle:



1.9 pav. Sustiprinto metodo veikimo schema

Abipusis autentifikavimas atliekamas tokiais žingsniais:

- skaitytuvas siunčia užklausą žymai. Užklausoje yra įdėtas atsitiktinis kamšalas N_R;
- žyma sugeneruoja naują atsitiktinį kamšalą N_T ir siunčia atgal skaitytuvui tokią informaciją: $H(ID_i)$, N_T ir $H_{IDi}(N_T, N_R)$;
- skaitytuvas perduoda gautą informaciją galiniam serveriui;
- serverio duomenų bazė autentifikuoja žymą (ta pačiai, kaip ir paprastame metode) ir jei autentifikacija pavyksta, suskaičiuoja naują žymos identifikatorių ID_{i+1}.
- serverio duomenų bazė sudaro naują pranešimą $H_{IDi+1}(N_T, N_R)$, pasinaudodama nauju identifikatoriumi ID_{i+1}. Pranešimas nusiunčiamas RFID žymai, kuri sugeneruoja naują identifikatorių ir suskaičiuoja savo maišos reikšmę $H_{IDi+1}(N_T, N_R)$.
- jei gauta $H_{IDi+1}(N_T, N_R)$ reikšmė lygi suskaičiuotai, tuomet žyma priima skaitytuvą kaip autentifikuotą ir tik tada ištrina iš atminties senąjį identifikatorių ID_i ir kamšalą N_T. Kitu atveju žyma atmeta skaitytuvo pranešimą ir laiko senąjį identifikatorių ID_i.

1.6.4.3. Metodų saugumo analizė

Klastotojas gali perimti tik RFID žymos identifikatoriaus reikšmę $H(ID_i)$. Negana to, ji bus naudojama tik vienam komunikavimo etapui su žymų skaitytuvu, nes po kiekvieno komunikavimo etapo, galinis serveris atnaujina žymos identifikatorių. Todėl bet koks seno identifikatoriaus atskleidimas yra beprasmis, nes autentifikacija su suklastota žyma bus negalima.

Naudojant maišos funkciją praktiškai yra neįmanoma nustatyti originalų žymos identifikatorių ir ryšį tarp ID_i ir ID_{i+1}. Net jeigu informacija ir būtų atskleista, klastotojas negalėtų susieti dabartinio žymos identifikatoriaus su praeities veiksmais, nes iš žymos atminties yra ištrinama visa sena informacija. Todėl garantuojama būsimoji apsauga (angl. *forward security*).

Paprasta metodo versija yra neatspari serverio duomenų bazės ir žymų desinchronizavimo problemai. Galima vykdyti *atsisakymo tarnauti* ataką, kur atakuotojas naudos savo žymų skaitytuvą. Tuomet žyma bus užtvindoma dideliais kiekiais užklausų, kurie prašys leidimo skaityti informaciją. Svarbi informacija nebus atskleista, nes žyma neišduos svarbios informacijos. Tačiau žyma vykdys metodo eigą ir atnaujins savo identifikatorių ID_i į ID_{i+k}, kur k yra užklausų kiekis. Kitą kartą, kai vyks komunikacija su legaliu sistemos žymų skaitytuvu, serveris stengsis rasti duomenų bazėje $H(ID_{i+k})$ reikšmę, kurios paprasčiausiai joje nebus. Žyma bus atmesta kaip suklastota, nors ji yra originali, tik su įvykdyta neteisėta ataka ir pakeistais duomenimis, todėl bus įvykęs RFID žymų desinchronizavimas.

Tokia situacija atsiranda dėl to, jog šiame paprastoje metodo versijoje nėra autentifikavimo, kurį atlieka RFID žyma. Autentifikavimas atliekamas tik žymų skaitytuvo pusėje.

Ši problema yra išsprendžiama sustiprintoje metodo versijoje, kur atakuotojo skaitytuvas gali siųsti užklausas RFID žymai, tačiau žyma nebepakeis savo ID_i į ID_{i+k}, nes pakeitimas yra vykdomas tik tuo atveju, kai gaunamas teisingas atsakymas iš skaitytuvo. Todėl, bandymas nuskaityti žymos informaciją su neautentifikuotu žymų skaitytuvu, neturės jokio efekto žymos funkcionalumui.

Taip pat atakuotojui nėra jokių šansų suklastoti $H_{IDi+1}(N_T, N_R)$ reikšmės, nes čia apsaugą užtikrina parametras N_R.

1.7. Analizės išvados

Atlikus RFID žymų klastojimo problemos analizę, buvo išsiaiškinti svarbūs aspektai, kuriuos pritaikius, galima sudaryti veiksmingą RFID žymų apsaugos nuo klastojimo metodą:

- RFID žymos neturi pakankamai didelio energijos šaltinio, todėl joms aktyvuoti yra naudojami indukcinės sankabos ir sklidimo movos metodai, kurie negali sukurti pakankamai energijos, atlikti sudėtingiems kriptografiniams skaičiavimams. Sudarinėjant žymų apsaugos nuo klastojimo metodą, rekomenduojama taikyti kuo paprastesnes kriptografines operacijas, kad sudarytą metodą būtų galima pritaikyti ir praktiškai, o ne tik teoriškai;

- pavojingiausias pažeidžiamumas, kurio sėkmingo vykdymo rezultatai gali išaukti galimybę klastotojui sukurti RFID žymos klastotę, yra radijo dažnių manipuliavimas: *slapto stebėjimo*, *suklastojimo* ir *pakartojimo* atakos. Labai svarbu užkirsti kelią ir žymose esančių duomenų manipuliavimui, kad klastotojams nebūtų galima pakeisti žymoje esančių duomenų savais;
- sudarinėjant apsaugos nuo klastojimo metodą, reikia taikyti holistinį požiūrį ir atsižvelgti į tris svarbius kriterijus: stabilus veikimas, kaina ir saugumas.

Atlikus keleto populiarių RFID žymų apsaugos nuo klastojimo metodų analizę, buvo nustatyti kriterijai, kurie yra rekomenduojami taikyti, apsaugant RFID žymas nuo jų klastojimo:

- yra saugumo metodų, kurie naudoja tik vienpusę autentifikaciją, t.y. žymos autentiškumas yra tikrinamas tik žymų skaitytuvo pusėje, o pati žyma netikrina skaitytuvo autentiškumo. Tai sudaro galimybę atakuotojams, pasinaudojus savu žymų skaitytuvu, komunikuoti su RFID žyma. Tokiu atveju galimybė suklastoti žymą yra gan didelė. Norint sumažinti klastojimo galimybę, rekomenduojama naudoti abipusę autentifikaciją: skaitytuvo pusėje vyksta žymos autentifikacija, o žymos pusėje – skaitytuvo ir serverio autentifikacija;
- nerekomenduojama perduoti atviru komunikavimo kanalu (tarp žymų skaitytuvo ir žymos) tikrąją žymos identifikatoriaus reikšmę;
- perduodant svarbius duomenis tarp RFID žymos ir skaitytuvo, rekomenduojama naudoti maišos funkcijas, jei tik tai yra įmanoma. Tai klastotojui apsunkins ar neleis iššifruoti svarbių duomenų, pavyzdžiui, originalaus žymos identifikatoriaus;
- rekomenduojama naudoti atsitiktinių skaičių generatorius. Atsitiktinius skaičius, pridėjus prie svarbių duomenų, perduoti daugumoje komunikavimo užklausų tarp žymų skaitytuvo ir žymos. Tokiu būdu yra apsunkinama *slapto stebėjimo* atakos rezultatų analizė, nes atsitiktiniai skaičiai įneša papildomos painiavos;
- kiekvieną kartą atlikus pilną komunikavimo etapą tarp žymų skaitytuvo ir žymos, rekomenduojama pakeisti žymos identifikatorių. Dinamiškas identifikatorių keitimas labai apsunkina žymų klastojimą;
- reikia stengtis nesaugoti ankstesnių komunikavimo etapų duomenų (pavyzdžiui, senų identifikatorių, kamšalų, anksčiau sugeneruotų atsitiktinių skaičių reikšmių). Ypač tai galioja RFID žymose, kur turi būti saugomi tik aktualūs duomenys, o ne istoriniai (kaip tai realizuota sustiprintoje *Tassos Dimitriou* metodo versijoje).

2. RFID ŽYMŲ APSAUGOS NUO KLASTOJIMO METODO SUDARYMAS

Analizės dalyje apžvelgus ir detaliai išanalizavus kelis RFID žymų apsaugos nuo klastojimo metodus, buvo suformuluotos išvados ir pateiktos rekomendacijos, kurios apibrėžia geriausias apžvelgtų metodų savybes. Šios rekomendacijos ir buvo pagrindiniai kriterijai, kuriais buvo remiamąsi kuriant naują RFID žymų apsaugos nuo klastojimo metodą. Todėl galima teigti, jog sudarytas metodas yra apžvelgtų skirtingų RFID saugumo metodų savybių mišinys.

Taip pat sudarytame metode yra įvesta naujovė, kurios principo nebuvo nė viename apžvelgtame RFID saugumo metode. Kiekviena RFID žyma skaičiuoja dvi atsitiktinai parinktas aritmetines operacijas su trimis atsitiktiniais skaičiais x_i. Skaičiai kiekvieno naujo komunikavimo etapo metu yra sugeneruojami vis nauji, o aritmetinės operacijos nekinta – jos yra sugeneruojamos ir įrašomos į kiekvieną žymą registracijos etapo metu.

Tolesniuose skyreliuose pateikiamas detalus sudaryto metodo koncepcinis aprašas.

2.1. Metodo realizavimo galimybės

Buvo siekiama sukurti tokį metodą, kuris būtų atsparus RFID žymų klastojimui, t.y. buvo sprendžiama problema, kaip apsaugoti RFID žymas nuo jų identifikacinių duomenų atskleidimo, kurių paviešinimas turėtų neigiamų pasekmių visai RFID sistemai ar konkrečiam sistemos objektui.

Sudarytame apsaugos nuo klastojimo metode yra naudojamos aritmetinės skaičiavimo operacijos, maišos reikšmių skaičiavimas, o tai yra gana „sunkūs“ skaičiavimai. Todėl metodas teoriškai turėtų būti realizuotas aktyviose RFID sistemose, o ne pasyviose, nes pasyvios RFID žymos neturi techninių galimybių atlikti tokius skaičiavimus. Tačiau RFID technologijos sparčiai tobulėja ir vis labiau populiarėja antros kartos pasyvios RFID žymos [13], kurios turi nemažai technologinių naujovių. Šios kartos žymos su tinkamais skaitytuvais yra nuskaitomos iki 10 kartų greičiau, nei pirmosios kartos žymos. Žymoje gali būti įdiegta virš 50 000 tranzistorių, tačiau pačios žymos dydis yra mažesnis, lyginant su pirmosios kartos pasyviomis RFID žymomis. Taip pat antros kartos pasyvios RFID žymos gali pasiūlyti didesnę atmintį ir galingesnius skaičiavimo mechanizmus. Todėl šiame darbe nėra akcentuojamas konkretus sudaryto metodo priskyrimas jį naudoti būtent aktyviose ar pasyviose RFID sistemose.

2.2. Metodo parametrų aprašymas

Pagrindiniai duomenys yra saugomi RFID žymoje ir serverio pusėje esančiose duomenų bazėje. Žymoje duomenys yra saugomi jos vidinėje atmintyje, o serverio pusėje duomenų saugojimas atliekamas reliacinėje duomenų bazėje.

RFID žymoje saugomi tokie duomenys:

- *H(ID)* – unikalaus žymos identifikatoriaus sistemoje maišos reikšmė;
- atsitiktinis kintamas skaičius k;
- aritmetinės operacijos $op_i \in (+,-,*,/)$, kai $i = (1;2)$, kurios bus atliekamos su gautais skaičiais x_j, kai $j = (1;2;3)$, iš žymų skaitytuvo.

Sistemos duomenų bazėje, kiekvienoje lentelės eilutėje, saugomi tokie duomenys:

- *ID* – unikalus žymos identifikatorius sistemoje;
- *H(ID)* – unikalaus žymos identifikatoriaus sistemoje maišos reikšmė;
- atsitiktinis skaičius k;
- unikalios loginės operacijos $op_i \in (+,-,*,/)$, kai $i = (1;2)$, kurios bus atliekamos su atsitiktinai sugeneruotais skaičiais x_j, kai $j = (1;2;3)$.
- kiti duomenys, pagal kuriuos sistemos programinė įranga atliks tam tikrus veiksmus, jei žyma komunikavimo proceso metu bus pripažinta kaip nesuklastota.

2.3. Metodo etapai

RFID žymų apsaugos nuo klastojimo metodas yra sudarytas iš trijų pagrindinių etapų:

- registracijos etapo;
- žymos autentifikavimo serverio pusėje;
- serverio autentifikavimo žymos pusėje.

Tolesniuose skyreliuose yra pateikiami detalūs kiekvieno etapo aprašymai ir jų metu vykstantys procesai.

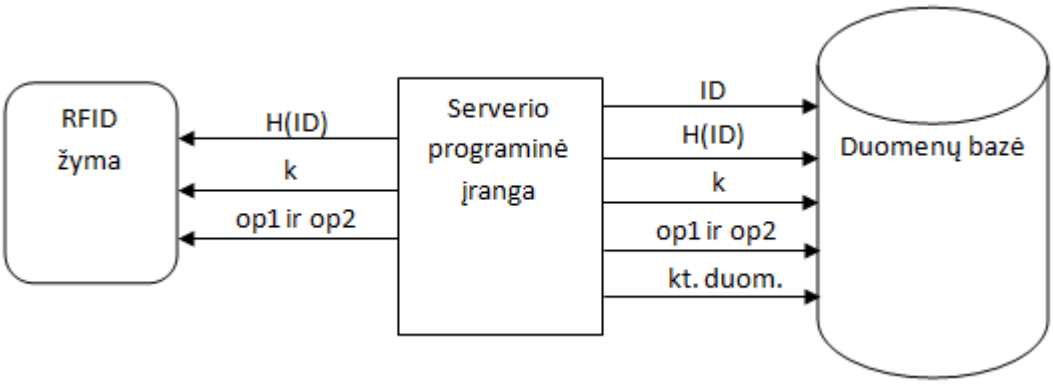
2.3.1. Registracijos etapas

Šis etapas yra vykdomas tuomet, kai į visą RFID sistemą reikia įtraukti naują žymą. Svarbiausias veiksmas yra bendrų duomenų tarp duomenų bazės ir RFID žymos padalijimas (2.1 pav.), kurio metu yra generuojami nauji duomenys ir įrašomi į sistemos komponentų atmintį.

Visą registracijos etapą galima išskaidyti į šiuos žingsnius:

1. atsitiktinai sugeneruojamas visoje RFID sistemoje unikalus žymos identifikatorius ID;

2. apskaičiuojama identifikatoriaus maišos reikšmė H(ID), taikant MD5 arba SHA-1 maišos skaičiavimo algoritmus;
3. sugeneruojamas pradinis atsitiktinis skaičius $k \in [0{,}001; 0{,}999]$;
4. iš galimų aritmetinių operacijų aibės yra atsitiktinai išrenkamos dvi operacijos op_1 ir op_2. Operacijos išrenkamos nepriklausomai viena nuo kitos, t.y. gali būti išrinktos ir dvi identiškos operacijos arba operacijų poros RFID žymai;
5. žymai yra priskiriami kiti duomenys, tokie kaip leidimai ar draudimai patekti į tam tikras patalpas, priklausomai nuo visos sistemos reikalavimų;
6. visi sugeneruoti ir apskaičiuoti duomenys yra surašomi į RFID žymą ir sistemos duomenų bazę.



2.1 pav. Registracijos etape vykstantis duomenų padalijimas

Pabrėžiama, jog registracijos etapas turi vykti saugiai, t.y. neturi būti galimybės pašalinių asmenų įrenginiams nuskaityti įrašomų į sistemos komponentų atmintį pradinių duomenų.

2.3.2. Žymos autentifikavimas serverio pusėje

Žymos autentifikavimo etapo (2.2 pav.) tikslas yra nustatyti ar žyma yra nesuklastota. Jei yra nustatoma, jog žyma negali autentifikuotis serverio pusėje, tuomet sistema stabdo komunikavimo procesą tarp neautentifikuotos žymos ir žymų skaitytuvo, bei informuoja atsakingą asmenį apie susidariusią informaciją.

Žymos autentifikavimo etapo žingsniai:

1. žymų skaitytuvas RFID žymai siunčia užklausą ir tris atsitiktinai sugeneruotus skaičius: x_1, x_2 ir x_3, kur $x_i \in [1; 100]$;
2. žyma, gavusi tris skaičius x_1, x_2 ir x_3, atlieka registracijos etape jai priskirtas aritmetines operacijas ir apskaičiuojamas operacijų rezultatas r:

$$r = (x_1\ (op1)\ x_2\ (op2)\ x_3); \quad (1)$$

3. prie apskaičiuoto rezultato *r* yra prijungiamas žymos atmintyje saugomas atsitiktinis skaičius *k* ir apskaičiuojama maišos reikšmė:

$$H(r \,||\, k); \tag{2}$$

4. apskaičiuota maišos reikšmė ir žymos identifikatoriaus maišos reikšmė *H(ID)* yra persiunčiama atgal žymų skaitytuvui;
5. žymų skaitytuvas kreipiasi į duomenų bazę su gautąją *H(ID)* reikšme ir pagal ją yra ieškoma žymos informacijos įrašas;
6. duomenų bazė, suradusi reikalingą informaciją, grąžina žymų skaitytuvui žymoje saugomą atsitiktinį skaičių *k* ir dvi logines operacijas op_1 ir op_2, kurios yra priskirtos žymai;
7. žymų skaitytuvas dabar turi visą reikalingą informaciją ir atlieka žymos autentifikavimą;
8. pagal iš duomenų bazės gautus aritmetinių operacijų duomenis ir prieš tai sugeneruotus x_i skaičius, yra apskaičiuojama operacijų rezultato *s* reikšmė:

$$s = (x_1\ (op1)\ x_2\ (op2)\ x_3); \tag{3}$$

9. prie apskaičiuotos *s* reikšmės yra prijungiamas *k* skaičius ir apskaičiuojama maišos reikšmė:

$$H(s \,||\, k); \tag{4}$$

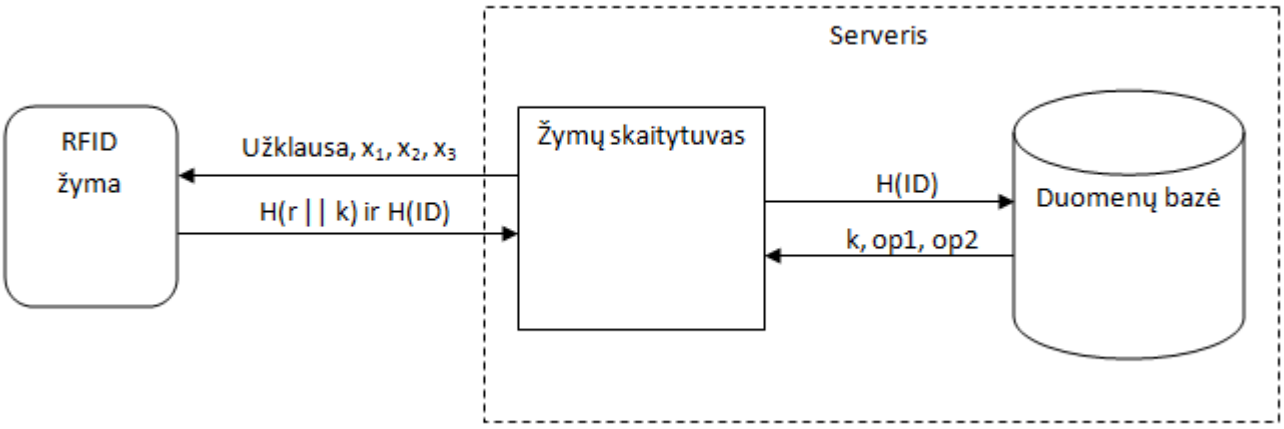
10. jei apskaičiuota maišos reikšmė *H(s || k)* yra lygi gautąjai iš žymos maišos reikšmei *H(r || k)*, t.y.

$$H(s \,||\, k) == H(r \,||\, k); \tag{5}$$

tuomet žymos autentifikavimo etapas yra sėkmingai baigiamas ir pradedamas kitas etapas. Jei reikšmės yra nelygios, t.y.

$$H(s \,||\, k)\ != H(r \,||\, k); \tag{6}$$

tuomet komunikavimo procesas yra sustabdomas ir yra spėjama, jog žyma gali būti suklastota.

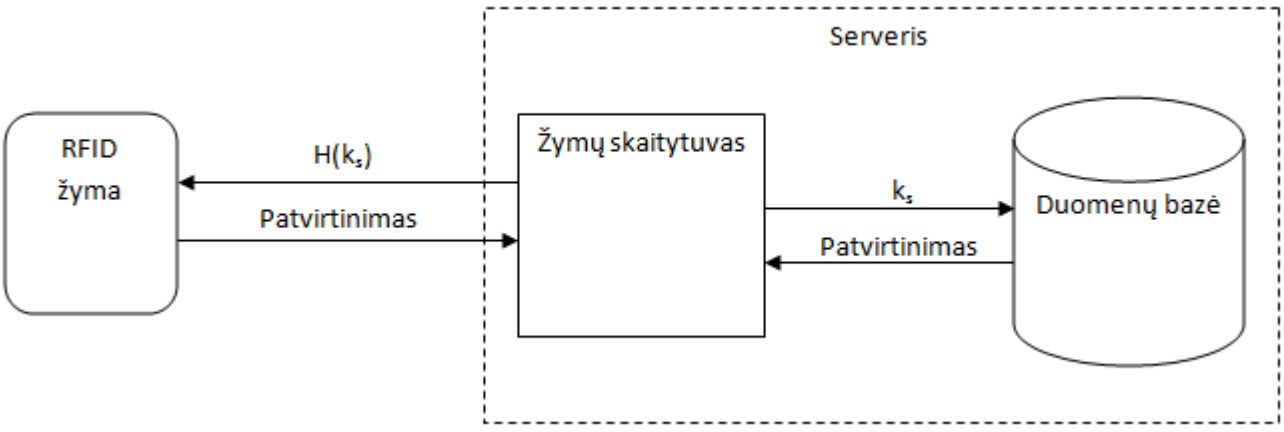


2.2 pav. Žymos autentifikavimo etapas

2.3.3. Serverio autentifikavimas žymos pusėje

Tik sėkmingai atlikus žymos autentifikavimą serverio pusėje, galima atlikti atvirkštinį etapą, t.y. serverio pusės autentifikavimą pačioje žymoje (12 pav.). Sekantys žingsniai yra vykdomi iškart po žymos autentifikavimo serverio pusėje sėkmingos pabaigos:

1. Žymų skaitytuvas padinina atsitiktinio skaičiaus *k* reikšmę, kurią gavo iš duomenų bazės:
$$k_s = k + 0{,}001; \quad (7)$$
2. k_s reikšmei yra apskaičiuojama maišos reikšmė $H(k_s)$, kuri yra persiunčiama RFID žymai. Taip pat nauja k_s reikšmė yra persiunčiama į duomenų bazę, kur yra įrašoma vietoje senosios *k* reikšmės;
3. Šiuo metu žymos atmintyje yra saugoma senoji *k* skaičiaus reikšmė. Todėl žyma apskaičiuoja naują k_r reikšmę, t.y. padidina *k* skaičiaus reikšmę analogiškai kaip ir žymų skaitytuvas:
$$k_r = k + 0{,}001; \quad (8)$$
4. Apskaičiuojama maišos reikšmė $H(k_r)$ ir atliekama palyginimo operacija:
$$H(k_s) == H(k_r); \quad (9)$$
5. Jei reikšmės yra lygios, tuomet senoji *k* reikšmė yra ištrinama iš žymos atminties ir vietoje jos yra įrašoma nauja k_r reikšmė.
   Jei reikšmės yra nelygios, tuomet senoji *k* reikšmė lieka nepakitusi, nes yra spėjama, jog su RFID žyma bando komunikuoti neautentifikuotas sistemoje žymų skaitytuvas.
6. Žyma išsiunčia skaitytuvui patvirtinimą apie sėkmingą arba nesėkmingą serverio autentifikavimą.



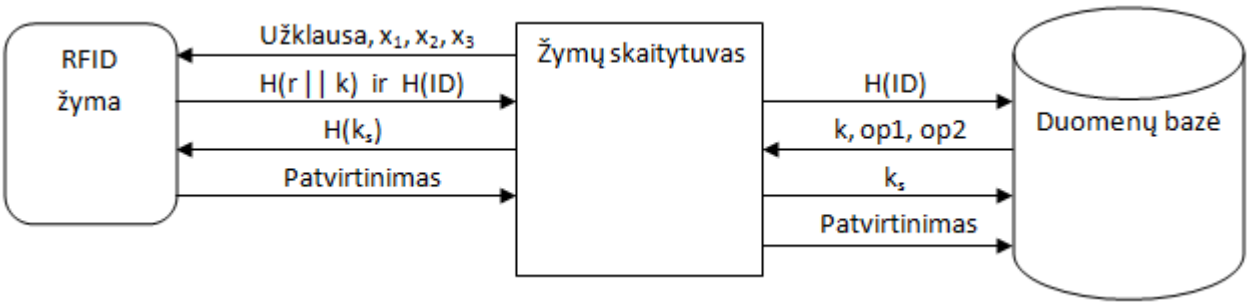
2.3 pav. Serverio autentifikavimo etapas

Tik sėkmingai atlikus abu autentifikavimo etapus, RFID sistemos programinė įranga vykdo žymai priskirtus veiksmus, kurie yra saugomi duomenų bazėje. Jei nors vienas etapas yra atliekamas

nesėkmingai, tuomet jokie žymai priskirti veiksmai sistemoje yra negalimi. Tokiu atveju RFID sistemoje yra užfiksuojamas žymos klastojimo atvejis.

2.4. Struktūrinė schema ir algoritmas

Pateikiama viso sudaryto RFID žymų apsaugos nuo klastojimo metodo struktūrinė schema ir algoritmas:



2.4 pav. Sudaryto metodo struktūrinė schema

1. Žymų skaitytuvas RFID žymai siunčia užklausą ir tris atsitiktinai sugeneruotus skaičius x_1, x_2, x_3.
   1.1. Žyma priima duomenis ir apskaičiuoja:
   $r = x_1$ (op1) x_2 (op2) x_3;
   H(r || k).
   1.2. Reikšmės H(r || k) ir H(ID) persiunčiamos atgal žymų skaitytuvui.
2. Žymų skaitytuvas kreipiasi į sistemos duomenų bazę su raktažodžiu H(ID).
   2.1. jei duomenų bazė suranda H(ID) reikšmę, tuomet:
   žymų skaitytuvui perduodamos k, op1, op2 reikšmės.
   2.2. jei duomenų bazė nesuranda H(ID) reikšmės, tuomet:
   komunikavimo procesas stabdomas.
3. Pagal gautus duomenis, žymų skaitytuvas apskaičiuoja:
   $s = x_1$ (op1) x_2 (op2) x_3;
   H(s || k).
   3.1. jei H(s || k) == H(r || k), tuomet:
   $k_s = k + 0{,}001$;
   $H(k_s)$;
   $H(k_s)$ persiunčiama žymai, o k_s persiunčiama duomenų bazei.
   3.2. jei H(s || k) != H(r || k), tuomet:
   žymos autentifikacija nepavyko, procesas stabdomas.
4. Žyma priima duomenis ir apskaičiuoja:

$k_r = k + 0{,}001$;

$H(k_r)$.

4.1. jei $H(k_r) == H(k_s)$, tuomet:

senoji k reikšmė atnaujinama: $k = k_r$;

patvirtinimas = 1.

4.2. jei $H(k_r) != H(k_s)$, tuomet:

serverio autentifikacija nepavyko;

patvirtinimas = 0.

5. Žyma persiunčia žymų skaitytuvui galutinį patvirtinimą.

2.3. Metodo saugumo analizė

Sudaryto metodo įgyvendinama apsauga nuo RFID žymų klastojimo yra paremta šiais teiginiais:

- atsitiktiniai skaičiai x_i yra sugeneruojami tik vienam komunikavimo su RFID žyma etapui. Taip pat, skaičiai yra trys ir jų atsitiktinumo intervalas yra nuo 1 iki 100, todėl tikimybė, jog bus sugeneruoti vienodi skaičiai skirtingiems komunikavimo etapams, yra viena iš milijono (1/100*100*100);
- kiekviena RFID žyma atlieka skirtingas atsitiktinai išrinktas skaičiavimo operacijas su atsitiktiniais skaičiais x_i. Tokių operacijų gali būti daug, priklausomai kokios yra žymos resursų galimybės. Todėl vienos žymos skaičiavimo logikos atskleidimas neturės įtakos kitoms sistemoje esančioms RFID žymoms, nes jos skaičiuoja skirtingas išraiškas;
- žymoje yra saugomas atsitiktinis skaičius *k*, kurio išgauti tiesiogiai yra praktiškai neįmanoma, nes jis siunčiamas kaip maišos reikšmė;
- jei klastotojo žymų skaitytuvas bandys nuskaityti originalios žymos duomenis (pasiųsdamas užklausą ir atsitiktinius skaičius x_i), jis gaus visiškai neiššifruojamą rezultatą, nes $H((x_1\ (op1)\ x_2\ (op2)\ x_3) \mid\mid k)$ išraiškoje yra atsitiktinis skaičius *k*, kurio reikšmės išgauti nepavyks iš RFID žymos. Kitaip tariant, bandymo atlikti visų skaičiavimo operacijų rinkinius (*,/,+,-) sėkmingi rezultatai neduos jokios naudos, nes nebus aišku, kokia yra *k* reikšmė ir kaip ji yra interpretuojama (pavyzdyje *k* reikšmė yra tiesiog prijungiama, tačiau, priklausomai nuo sistemos konfigūracijos, su šia reikšme galima atlikti logines / aritmetines operacijas ar kitus veiksmus);
- po kievienos sėkmingos žymos autentifikacijos serverio pusėje, yra vykdoma (atvirkštinis procesas) serverio autentifikacija žymos pusėje, t.y. palaikoma griežta abipusė autentifikacija. Tik sėkmingai įvykdžius abu autentifikavimo etapus, sistemos programinė įranga atliks veiksmus, kurie yra priskirti RFID žymai;

- tik serveriui sėkmingai atlikus autentifikavimą RFID žymoje, senoji *k* reikšmė yra ištrinama ir vietoje jos yra įrašoma nauja $k_r = k + 0.001$. Tai leis apsisaugoti nuo klastotojų skaitytuvų atakų, nes tik sėkmingai atlikus autentifikaciją, galima modifikuoti žymoje esančius duomenis. Bet kokie kiti bandymai jungtis prie RFID žymos nesukels jokių pakeitimų žymoje esantiems duomenims, nes *k* reikšmė liks nepakitus. Todėl metodas apsaugo ne tik nuo klastojimo, bet ir nuo visos sistemos darbo sutrikdymo, kuomet yra sugadinami žymose esantys duomenys (vienos žymos sukompromitavimas neturės įtakos kitų žymų saugumui);
- atliekant vis skirtingus komunikavimo etapus tarp RFID žymos ir skaitytuvo, vienintelė nekintama reikšmė yra žymos identifikatoriaus maišos reikšmė H(ID), kurios paskirtis yra identifikuoti žymą serverio pusėje, t.y. atrinkti žymos duomenis iš duomenų bazės. Be to visą komunikavimo procesą visuomet pradeda sistemos žymų skaitytuvas, o ne RFID žyma.

3. PROGRAMINIO MODELIO APRAŠYMAS

Šiame skyriuje yra pateikiamas sudaryto RFID žymų apsaugos nuo klastojimo metodo programinio modelio aprašas. Sudaryto metodo programinis modelis yra sukurtas remiantis ankstesniame skyriuje pateiktu metodo aprašu. Programinis modelis leidžia teoriškai ištirti sukurto RFID žymų apsaugos nuo klastojimo metodo sąvybes ir ypatumus.

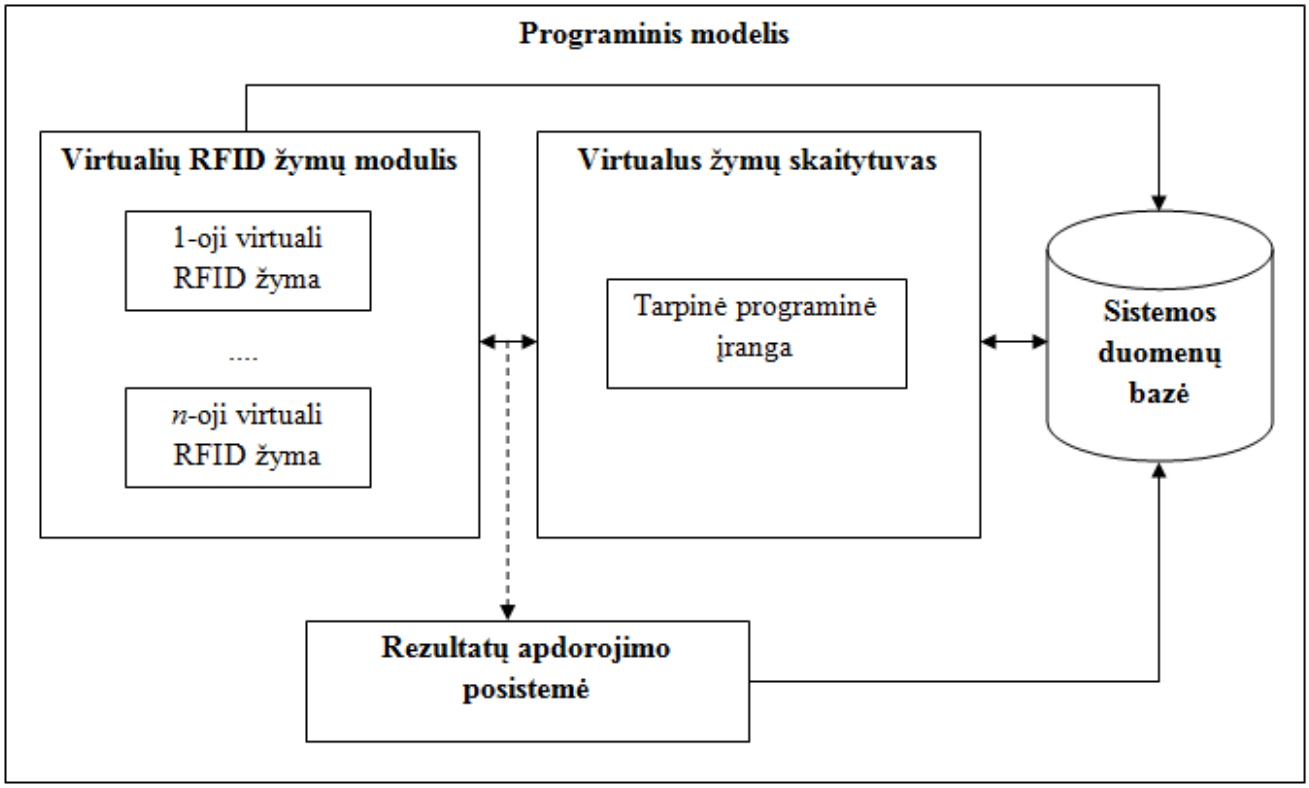
Programinis modelis yra sudarytas iš dviejų dalių: registracijos ir komunikavimo etapų simuliacijos. Registracijos etape yra simuliuojamas RFID žymos įtraukimo į sistemą procesas: ryšio su žymų skaitytuvu užmezgimas, duomenų įrašymas į abi puses – žymos atmintį ir RFID sistemos duomenų bazę.

Komunikavimo etapo simuliacija apima du smulkesnius procesus, t.y. žymos autentifikavimą serverio pusėje ir serverio autentifikavimą žymos pusėje.

3.1. Modelio struktūra

Sudaryto metodo programinis modelis yra sudarytas iš virtualių RFID žymų valdymo modulio, virtualaus žymų skaitytuvo, rezultatų apdorojimo posistemės bei sistemos duomenų bazės.

Modelio struktūrinė schema pateikta 3.1 paveiksle:



3.1 pav. Programinio modelio struktūrinė schema

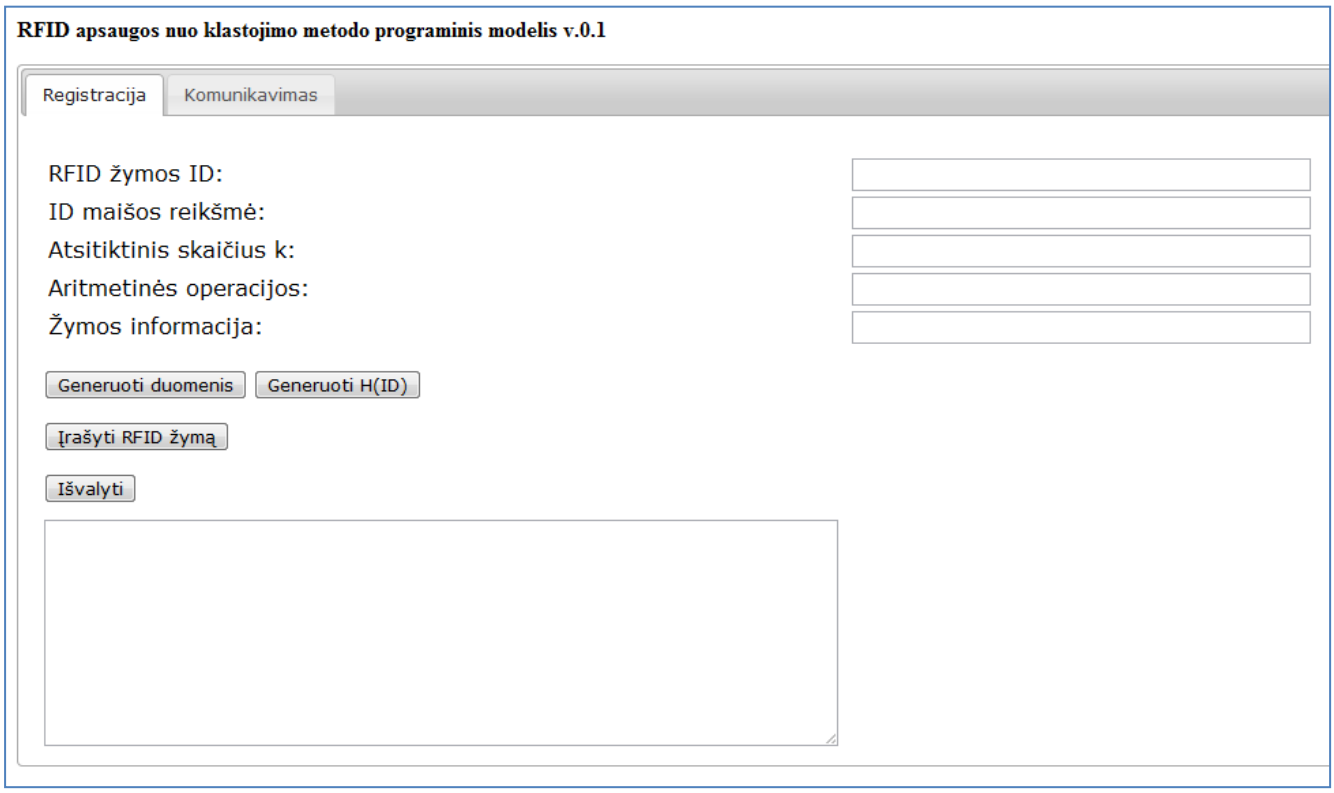
Virtualių RFID žymų valdymo modulyje yra atliekamas virtualių žymų generavimo procesas ir sugeneruotų žymų registravimo į sistemos duomenų bazę etapas. Taip pat valdymo modulyje yra parenkama virtuali RFID žyma, su kuria komunikuoja virtualus žymų skaitytuvas. Kiekviena virtuali RFID žyma turi savo vidinę atmintį, kurioje saugomi jai sugeneruoti duomenys.

Virtualus žymų skaitytuvas turi savo tarpinę programinę įrangą, kuri valdo komunikavimo etapą tarp žymų skaitytuvo ir RFID žymų, kreipiasi į duomenų bazę su duomenų užklausomis ir atlieka skaičiavimus.

Rezultatų apdorojimo posistemė fiksuoja keliaujančius duomenis tarp virtualios RFID žymos ir žymų skaitytuvo jų tarpusavio komunikavimo etapuose ir tuos duomenis išsaugo sistemos duomenų bazėje tolimesniems tyrimams ir apdorojimui. Taip pat ši posistemė gali apskaičiuoti keliaujančių duomenų entropijos rodiklius, kurie bus panaudoti atliekant sudaryto metodo kiekybinį tyrimą tolimesnėje darbo eigoje.

3.2. Eksperimentinė eiga

Realizuoto programinio modelio vartotojo sąsajos langas pateiktas 3.2 paveiksle:

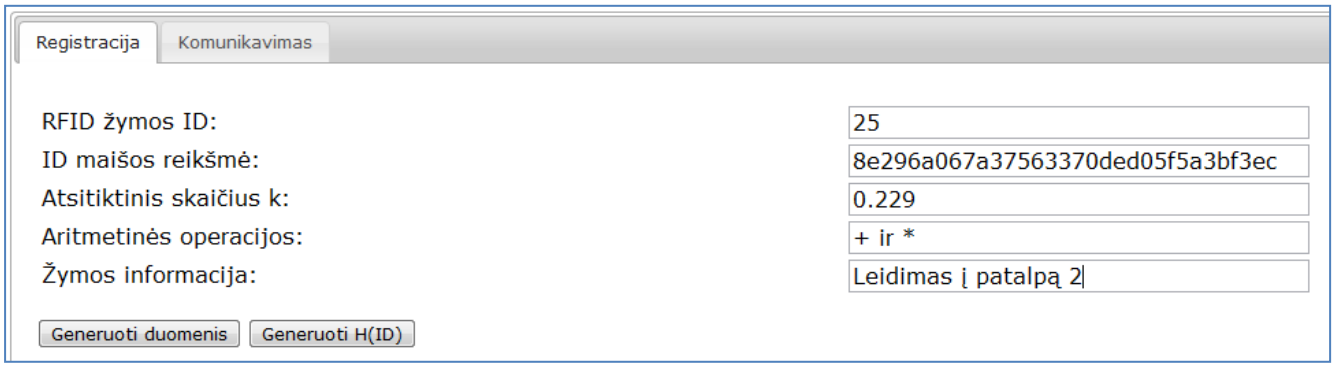


3.2 pav. Programinio modelio vartotojo sąsajos langas

Registracijos etape galima sugeneruoti atsitiktinius duomenis, kuriuos bus galima įrašyti į naują virtualią RFID žymą. Atsitiktiniai duomenys generuojami standartinėmis programinėmis priemonėmis.

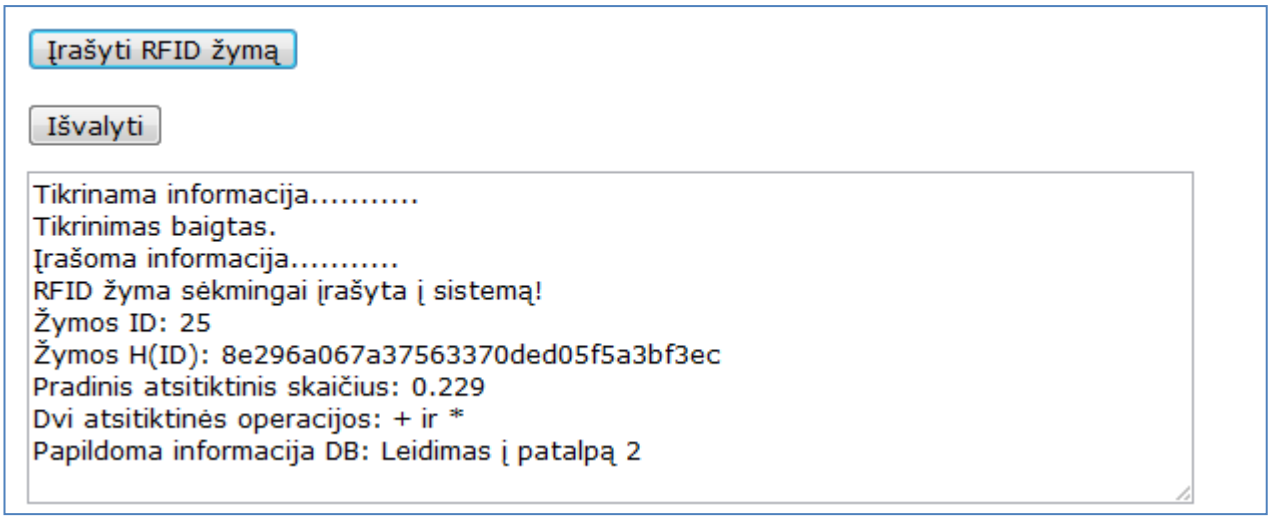
Privalomai sugeneruojami tokie duomenys: naujos RFID žymos identifikacinis numeris, identifikacinio numerio maišos reikšmė (galima parinkti MD5 arba SHA-1 algoritmus), dvi atsitiktinai parinktos aritmetinės operacijos bei atsitiktinis skaičius *k*.

Papildomai galima rankiniu būdu įrašyti informaciją apie RFID žymą.



3.3 pav. Sugeneruoti pradiniai RFID žymos duomenys

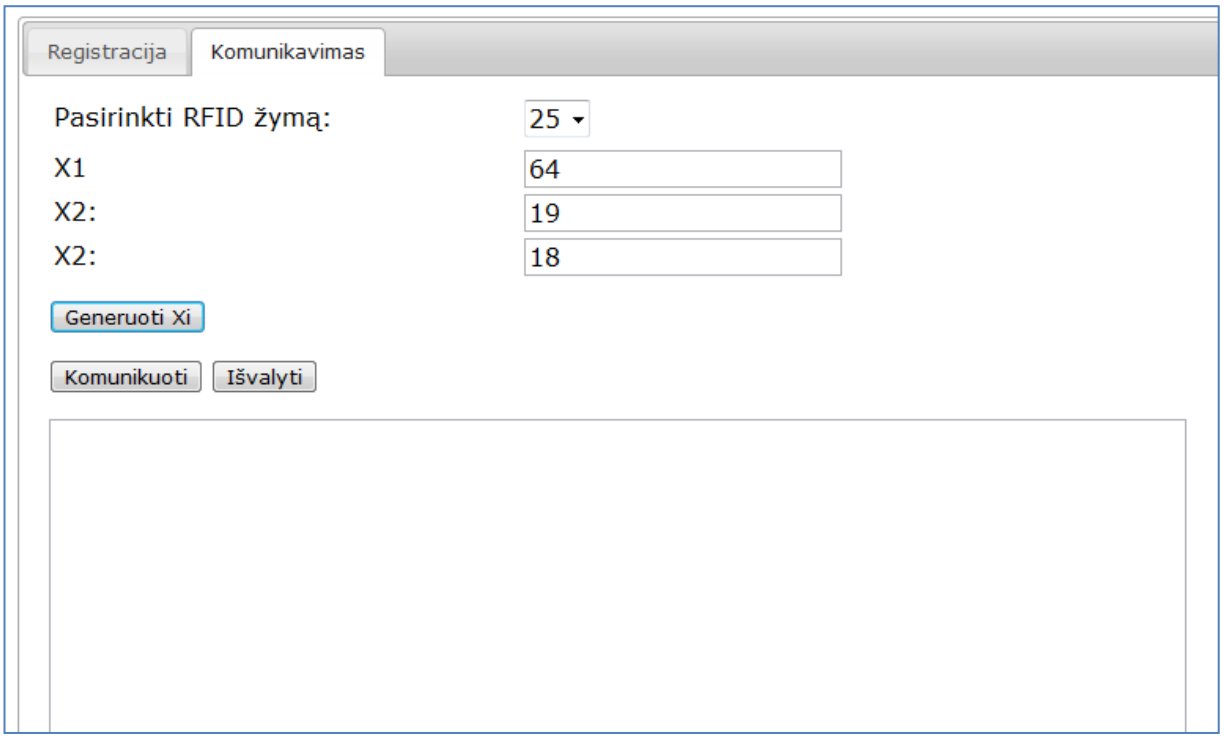
Sugeneravus reikiamus duomenis jie yra įrašinėjami į virtualią RFID žymą. Paspaudus mygtuką *Įrašyti RFID žymą*, yra pradedamas naujos žymos kūrimo etapas, tikrinant ar sugeneruoti duomenys yra korektiški.



3.4 pav. Naujos RFID žymos įrašymas

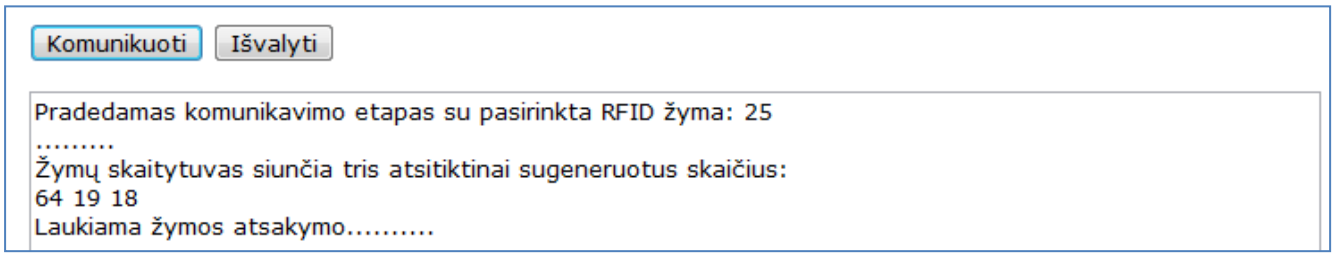
Sėkmingai pabaigus žymos registracijos etapą, sugeneruoti duomenys atsiranda sistemos duomenų bazėje ir iš karto galima vykdyti komunikavimo etapą tarp žymų skaitytuvo bei RFID žymos.

Pirmiausiai yra iš sistemoje saugomų virtualių žymų aprašų pasirenkama viena žyma, su kuria bus imituojamas komunikavimo procesas. Toliau virtualus žymų skaitytuvas sugeneruoja tris atsitiktinius skaičius x_i.



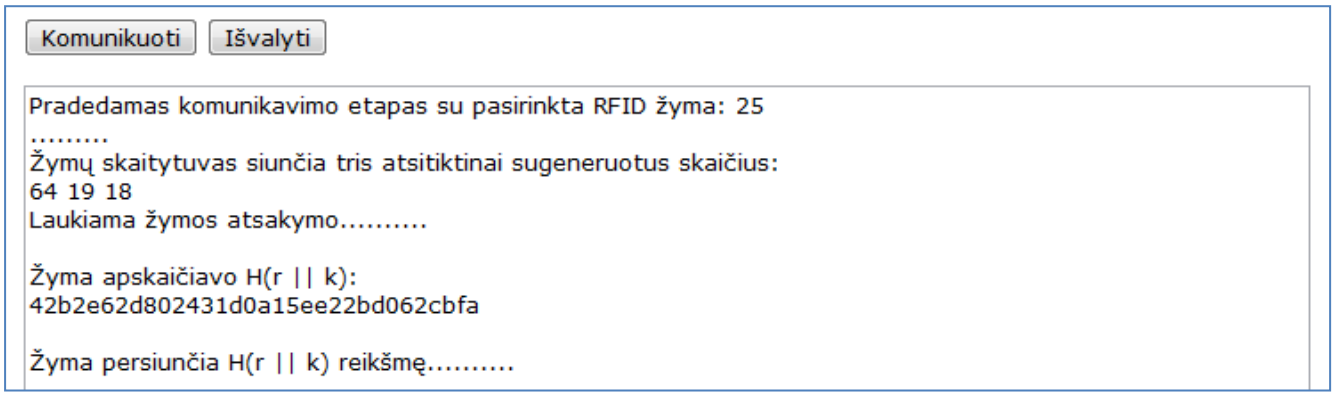
3.5 pav. Žymos parinkimas ir trys atsitiktiniai skaičiai

Paspaudus mygtuką *Komunikuoti* pradedamas komunikavimo procesas su pasirinkta 25-ąja žyma. Pirmiausiai skaitytuvas siunčia žymai anksčiau sugeneruotus tris atsitiktinius skaičius:



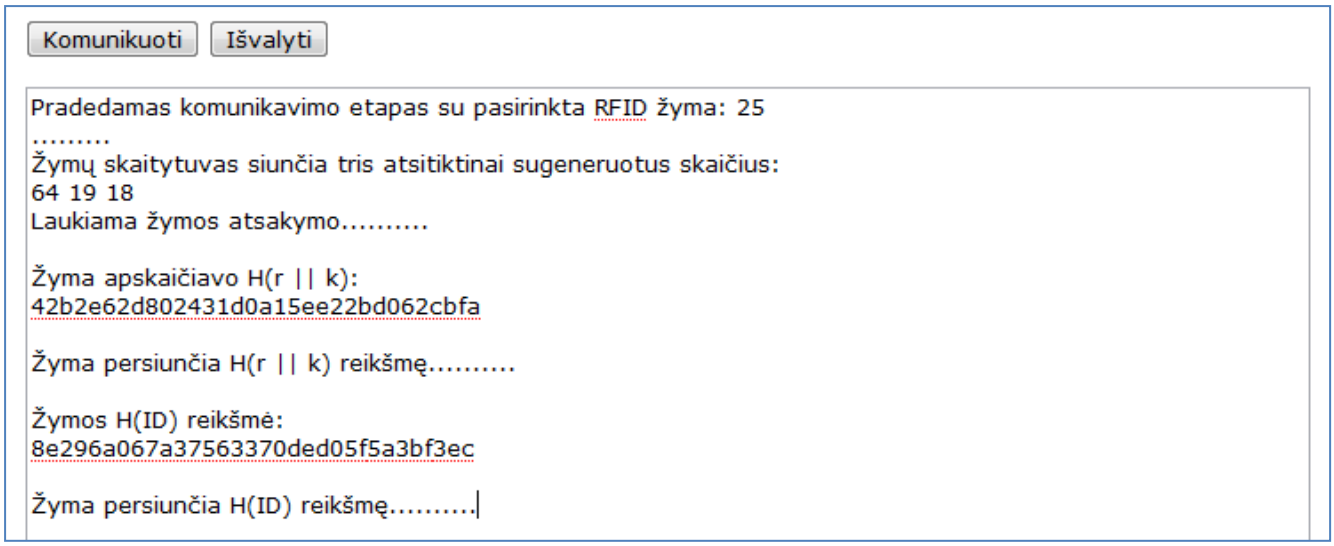
3.6 pav. Komunikavimo proceso pradžia

Žyma persiunčia atgal sugeneruotą *H(r || k)* išraišką:



3.7 pav. Žymos atsakymas į skaitytuvo užklausą

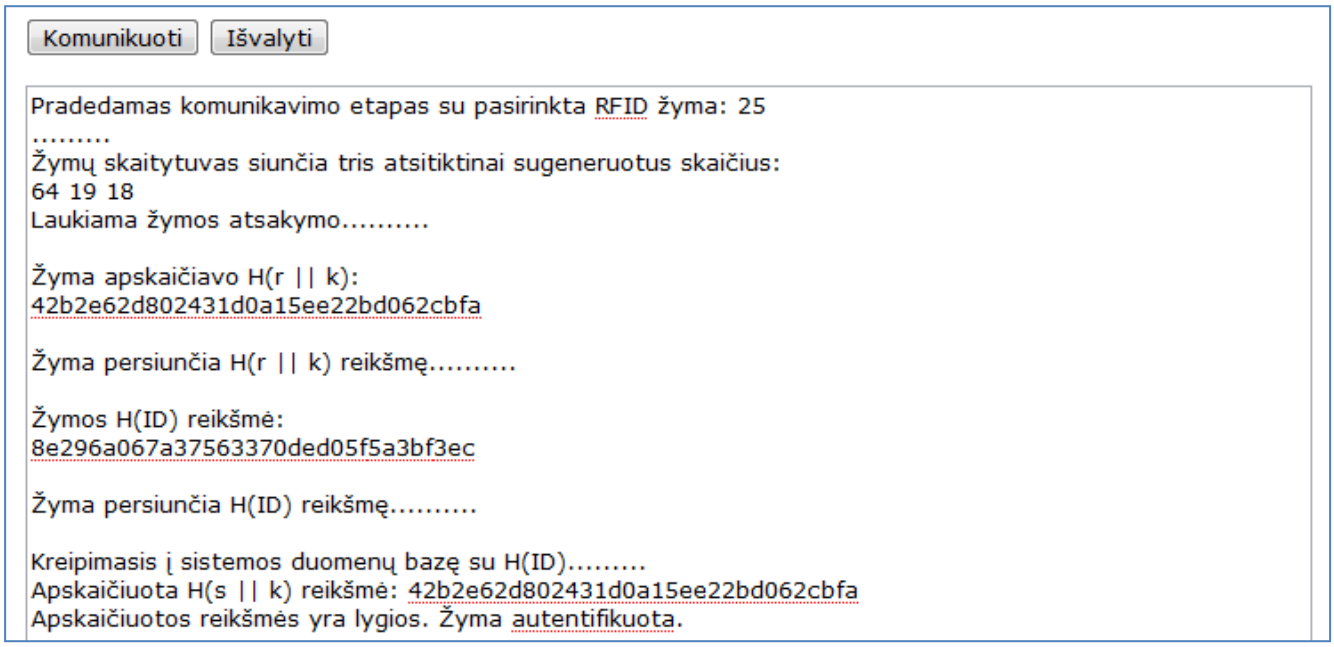
Taip pat žyma persiunčia savo *H(ID)* reikšmę, kuri saugoma jos atmintyje:



3.8 pav. Žyma grąžina savo identifikatoriaus maišos reikšmę

Toliau serverio pusėje yra pradedamas žymos autentifikavimo procesas. Skaitytuvas kreipiasi į duomenų bazę su gautu žymos identifikatoriumi. Iš ten yra išrenkami atitinkami duomenys, pagal kuriuos yra suskaičiuojama *H(s || k)* reikšmė. Reikšmė yra palyginama su gautąja iš žymos *H(r || k)* ir jei jos yra lygios, tuomet žymos autentifikavimas serverio pusėje yra sėkmingai baigtas.

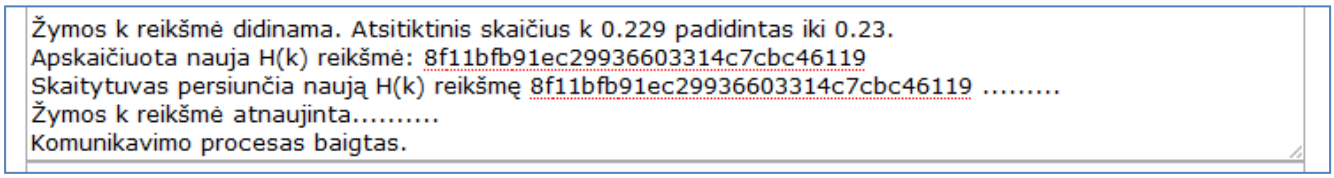
Jei reikšmės yra nelygios, tuomet fiksuojamas RFID žymos klastojimo atvejis ir tolimesnis komunikavimas yra sustabdomas.



3.9 pav. Žymos autentifikavimas serverio pusėje sėkmingai baigtas

Toliau seka atvirkštinis procesas, t.y. serverio autentifikavimas žymos pusėje. Reikšmė *k* yra padidinama ir apskaičiuojama *H(k)* išraiška. Ši išraiška yra persiunčiama žymai.

Žyma sulygina savo pusės *H(k)* išraišką su gautąja. Jei jos lygios, tuomet žymoje *k* reikšmė atnaujinama ir serveris yra autentifikuotas.



3.10 pav. Serverio autentifikavimas žymos pusėje sėkmingai baigtas

Programinio modelio eksperimentinės eigos rezultatas parodo viso komunikavimo proceso metu tarp RFID žymos ir skaitytuvo „keliaujančius“ duomenis, kurie yra siunčiami radijo dažniu, t.y. nesaugiu kanalu:

3.11 pav. „Keliaujantys“ duomenys tarp žymos ir skaitytuvo (nesaugus kanalas)

4. SUDARYTO METODO TYRIMAS

Ankstesniame skyriuje aprašytas sudaryto RFID apsaugos nuo klastojimo metodo programinis modelis buvo panaudotas atlikti tyrimui ir įvertinti metodo atsparumą RFID žymų klastojimui.

Visas tyrimas yra sudarytas iš dviejų dalių:

- kiekybinis įvertinimas, kurio metu buvo atliekamas fiksuotas skaičius sėkmingų komunikavimo etapų tarp keleto sugeneruotų virtualių RFID žymų ir žymų skaitytuvo. Kiekvieno etapo rezultatas buvo tam tikra duomenų eilutė, kuriai buvo skaičiuojamas entropijos rodiklis, siekiant įvertinti bendrą metodo generuojamų duomenų patikimumą;
- kokybinis įvertinimas, kuriame pateiktas analitinis sudaryto metodo įvertinimas. Analitinis įvertinimas skirtas palyginti sudarytą metodą su šio darbo analizės dalyje apžvelgtais RFID saugumo metodais, išskirti jo privalumus ir trūkumus.

Iš atlikto tyrimo buvo suformuluotos galutinės darbo išvados ir pateiktos rekomendacijos tolimesniems tyrimams.

4.1. Kiekybinis sudaryto metodo įvertinimas

Siekiant įvertinti sudaryto RFID žymų apsaugos nuo klastojimo metodo atsparumą duomenų klastojimui buvo atliktas kiekybinis tyrimas. Kiekybinio tyrimo metu buvo skaičiuojamos tarp RFID žymos ir žymų skaitytuvo keliaujančių duomenų entropijos. Entropija buvo pasirinkta todėl, kad tai yra geras būdas įvertinti skirtingų RFID žymų apsaugos nuo klastojimo metodų generuojamų duomenų patikimumą. Įvertinus sudarytą metodą entropijos požiūriu, buvo gauti entropijos rodiklių vidurkiai, kuriuos bus galima palyginti kuriant kitus RFID žymų apsaugos nuo klastojimo metodus ar sudaryto metodo modifikacijas. Todėl sudaryto RFID žymų apsaugos nuo klastojimo metodo entropijos rodikliai bus etalonas kitų autorių tyrimams, nes nei vieno analizės dalyje apžvelgto RFID saugumo metodo dokumentacijoje nebuvo pateikta jokio kiekybinio įverčio, pagal kurį būtų galima palyginti skirtingus metodus pagal vieną bendrą sistemą ir įverinti, kuris jų yra patikimesnis.

Informacijos teorijoje entropija yra traktuojama kaip neapibrėžtumo dydis tam tikroje duomenų eilutėje [14]. Šiuo atveju entropija buvo skaičiuojama kaip vienetų ir nulių santykis bitų lygmenyje (dvejetainėje sistemoje), kuris reiškia vidutinį bitų skaičių vienam simboliui, norint jį šifruoti, kur santykis $\in [0; 1]$. Todėl, kuo santykis yra arčiau vieneto reikšmės, tuo yra manoma, jog duomenų patikimumas yra didesnis, o santykiui artėjant į nulio pusę – duomenų patikimumas mažėja, nes vienam simboliui šifruoti praktiškai lieka labai maža bito dalis.

Programiniame modelyje atsitiktinai sugeneruotos penkios virtualios RFID žymos, kurių parametrai pateikti 4.1 lentelėje:

4.1 lentelė. Sugeneruotų virtualių RFID žymų parametrai

Žymos nr.	Atsitiktinės operacijos		*H(ID)*	Pradinis *k*
	Op. 1	Op. 2	MD5	
			SHA-1	
1	+	+	b6d767d2f8ed5d21a44b0e5886680cb9	0,139
			12c6fc06c99a462375eeb3f43dfd832b08ca9e17	
2	+	/	98f13708210194c475687be6106a3b84	0,845
			91032ad7bbcb6cf72875e8e8207dcfba80173f7c	
3	*	*	c20ad4d76fe97759aa27a0c99bff6710	0,389
			7b52009b64fd0a2a49e6d8a939753077792b0554	
4	/	/	1ff1de774005f8da13f42943881c655f	0,348
			4d134bc072212ace2df385dae143139da74ec0ef	
5	*	-	1f0e3dad99908345f7439f8ffabdffc4	0,404
			b3f0c7f6bb763af1be91d9e74eabfeb199dc1f1f	

Su kiekviena sugeneruota RFID žyma buvo atliekami septyni sėkmingi komunikavimo etapai naudojant MD5 ir SHA-1 maišos algoritmus. Kiekvieno etapo rezultatui (duomenų eilutei, kuri buvo sugeneruota tarp RFID žymos ir žymų skaitytuvo) buvo suskaičiuota atskira entropija. Pirmiausiai buvo skaičiuojamos entropijos, sugeneravus skirtingus pradinius x_i ir k parametrus, nepriklausomai nuo to, koks maišos algoritmas naudojamas programiniame modelyje – MD5 ar SHA-1.

Entropijos rodiklių skaičiavimo rezultatai 1-ai virtualiai RFID žymai, taikant MD5 maišos algoritmą, pateikti 4.2 lentelėje:

4.2 lentelė. Pirmos RFID žymos entropijos skaičiavimas taikant MD5

Nr.	1-a žyma: operacijos + ir +, naudojant MD5 maišą				
	x_i			Duomenys	Entropija
	x_1	x_2	x_3		
1.	86	92	14	869214a7e21ca627404a8c0b5f0829a0ccf21cb6d7 67d2f8ed5d21a44b0e5886680cb934ed9b9812dcaa 14a4334279f76926b5	0,74732
2.	24	73	60	2473607996f63d9021c8dec40c07a61996d7bbb6d7 67d2f8ed5d21a44b0e5886680cb98d8961aa7cf32b 24ecc50065c2a6d1aa	0,76242
3.	63	66	43	636643b6a4e0147dfe426b420f1e5a6e830b41b6d7 67d2f8ed5d21a44b0e5886680cb9b5dc71a61afb0a 53336fa617577152a2	0,76623
4.	74	55	20	745520920f4a690b1fd3f3da6c62b6a0365858b6d7 67d2f8ed5d21a44b0e5886680cb9674cc7d16948bd 81ef834bb2163973fb	0,76623
5.	37	94	20	3794206f5d858725a93d3e809b2040c65cf44fb6d7 67d2f8ed5d21a44b0e5886680cb95432a9a1dc5fbd 67236258a950bf76c9	0,77391
6.	1	53	22	153227235f0028b00bc79277871dbe8fe1390b6d76 7d2f8ed5d21a44b0e5886680cb98a566b1f10606f4	0,74514

				e9a77b90282284834	
7.	100	90	65	100906586e36f36ddff8ff67144484e64663132b6d767d2f8ed5d21a44b0e5886680cb9c150a3ce6a5529bda42501c6bf625b02	0,74636
				Vidurkis:	**0,75823**

Entropijos rodiklių skaičiavimo rezultatai 1-ai virtualiai RFID žymai, taikant SHA-1 maišos algoritmą, pateikti 4.3 lentelėje:

4.3 lentelė. Pirmos RFID žymos entropijos skaičiavimas taikant SHA-1

Nr.	**1-a žyma: operacijos + ir +, naudojant SHA-1 maišą**				
	x_i			**Duomenys**	**Entropija**
	x_1	**x_2**	**x_3**		
1.	40	73	63	4073630748b8d43c533ebd0a1da987f85b7f8efc40566512c6fc06c99a462375eeb3f43dfd832b08ca9e1749de5698ff5e97aa92651dd85352adb7299070f4	0,80000
2.	27	18	94	271894dd41e837209e332776ee9a5b91aba0456727649412c6fc06c99a462375eeb3f43dfd832b08ca9e17f319cb212301b7695f51bf6c8a3daf6c38cd19ae	0,80645
3.	27	57	41	275741644d88bdf54e3bd391dfbf213299eee7e441423312c6fc06c99a462375eeb3f43dfd832b08ca9e17e15316688f329c21599d094d3698107ff5981f4b	0,76623
4.	85	46	49	8546494aae87348fc03ba98cb2cf1655912f1b6285906e12c6fc06c99a462375eeb3f43dfd832b08ca9e17a3f72f110907bbee0bdfa71f19ddfbba28c662bc	0,77465
5.	39	34	61	3934617b48ba9639c33d4ae1a25f094bd83f405659b2c912c6fc06c99a462375eeb3f43dfd832b08ca9e176df5a6d5204aa8274d8dae5d0a5daeb3f39dd1ba	0,76532
6.	55	78	83	5578837490fe228919d58abb9dbdd03be64444de876db812c6fc06c99a462375eeb3f43dfd832b08ca9e17358b08595286dc4470985db4caf7c277c737f56a	0,79679
7.	4	85	15	485152b30907621374499bacd76aedcfbf002266f204612c6fc06c99a462375eeb3f43dfd832b08ca9e17cc09817c03d61b280422ec6331c3f0387a685e78	0,77620
				Vidurkis:	**0,78803**

Sekančioje lentelėje yra pateiktas entropijų rodiklių palyginimas, kuomet buvo sugeneruoti tie patys (vienodi) pradiniai parametrai taikant MD5 ir SHA-1 maišos algoritmus:

4.4 lentelė. Entropijų skaičiavimų palyginimas pirmai žymai

1-a žyma: operacijos + ir +				
x_i			Entropijos	
x_1	x_2	x_3	MD5	SHA-1
24	73	60	0,72145	0,76224
74	55	20	0,76623	0,77153
1	53	20	0,74514	0,82482
27	18	94	0,76623	0,80645
85	46	49	0,72462	0,77465
55	78	83	0,73617	0,79679
Vidurkiai:			**0,74331**	**0,78941**

Lygiai tokios pačios struktūros bandymai buvo atlikti su kitomis keturiomis virtualiomis RFID žymomis. Lentelės su skaičiavimų rezultatais yra pateiktos darbo priede.

Visų entropijos skaičiavimų rezultatų suvestinė pateikta 4.5 lentelėje:

4.5 lentelė. Kiekybinio tyrimo rezultatų suvestinė

Žymos nr.	Skirtingi pradiniai duomenys		Vienodi pradiniai duomenys	
	MD5	SHA-1	MD5	SHA-1
1	0,75823	0,78803	0,74331	0,78941
2	0,76110	0,80511	0,75886	0,81353
3	0,76624	0,79592	0,75245	0,80645
4	0,75240	0,76410	0,74663	0,77441
5	0,78061	0,80181	0,75269	0,79070
Vidurkiai:	**0,76372**	**0,79099**	**0,75079**	**0,79490**

Iš gautų kiekybinio tyrimo rezultatų suformuluotos tokios išvados:

- sudarytą RFID žymų apsaugos nuo klastojimo metodą pritaikius veikti naudojant SHA-1 maišos algoritmą, toms pačioms RFID žymoms, sugeneravus skirtingus pradinius parametrus x_i ir atsitiktinius skaičius k, entropijos rodiklis yra 3,57% didesnis, nei metodą pritaikius veikti naudojant MD5 maišos algoritmą;
- sugeneravus vienodus pradinius parametrus ir atlikus komunikavimo etapus vienodomis sąlygomis su abiem maišos algoritmais, taikant SHA-1 maišos algoritmą, entropijos rodiklis yra 5,88% didesnis nei taikant MD5 maišos algoritmą;
- entropijų skaičiavimai su penkiomis RFID žymomis parodo, jog sudarytame RFID žymų apsaugos nuo klastojimo metode maišos algoritmo parinkimas svarbios įtakos duomenų klastojimo atsparumui neturi;
- žinant, jog RFID žymose yra riboti techniniai resursai skaičiavimams, sudarytame apsaugos nuo klastojimo metode pilnai pakanka naudoti MD5 maišos algoritmą. MD5 maišos

algoritmas yra paprastesnis ir išnaudoja mažiau techninių resursų [15], nes generuojama 128 bitų seka, vietoje 160 bitų SHA-1 algoritmo atveju.

4.2. Kokybinis sudaryto metodo įvertinimas

Šio darbo analizės dalyje yra apžvelgti keturių tipų RFID saugumo metodai:

- RHLK metodas;
- SRAC ir A-SRAC metodai;
- *Jemal Abawajy* metodas;
- *Tassos Dimitriou* metodai.

Toliau pateikta sudaryto RFID žymų apsaugos nuo klastojimo metodo palyginamoji analizė su jau apžvelgtais metodais (žiūr. 4.6 lent.).

Sudarytą metodą galima išskaidyti į du etapus: registracijos ir komunikavimo. Iš dalies visi apžvelgti metodai turi tokius pat etapus, tačiau kai kurių metodų etapus galima skaidyti į dar smulkesnes dalis.

Sudaryto metodo registracijos etape yra vykdomas duomenų įrašymas į abi sistemos puses: RFID žymą ir sistemos duomenų bazę.

Taikant paprasčiausią RHLK metodą, žymoje yra saugomi žymos identifikatorius ir atsitiktinis skaičius *k*. Sudarytame metode žymoje yra saugomi žymos identifikatoriaus maišos reikšmė H(ID), atsitiktinis skaičius *k* ir dvi skaičiavimo operacijos.

SRAC protokolo žymoje saugoma žymos identifikatorius ir kintamas skaičius R_S. Žymos identifikatorius yra dinaminis, t.y. po kiekvieno sėkmingo komunikavimo etapo vis pakinta. Sudarytas metodas dinaminio identifikatoriaus neturi.

A-SRAC protokolas papildomai naudoja dar vieną kintamąjį R_T didesniam saugumui užtikrinti. Sudarytas metodas naudoja vieną kintamą skaičių *k* ir tris papildomus atsitiktinius skaičius x_i.

Jemal Abawajy metodas įveda sudėtingesnius duomenis. Žymoje yra saugomi virtualus žymos identifikatorius T_{VID}, kuris yra skaičiuojamas sujungiant atitinkamas duomenų bazės ir žymų skaitytuvo identifikatorių puses ir apskaičiuojant gautos išraiškos maišos reikšmę. Taip pat saugomas realus žymos identifikatorius T_{EPC}, bei atsitiktinis skaičius *k*. Kaip ir SRAC šeimos metodai, šis metodas siūlo galimybę po kiekvieno sėkmingo komunikavimo etapo pakeisti žymos identifikatorių, t.y. identifikatoriai yra dinamiškai kintantys. Mūsų sudarytas RFID žymų apsaugos nuo klastojimo metodas tokio funkcionalumo neturi ir žymos identifikatorius yra statinis.

Kitas labai svarbus aspektas yra abipusė autentifikacija, kuri leidžia išvengti RFID žymose esančių duomenų modifikavimo ir nuskaitymo, kurį gali bandyti atlikti klastotojo žymų skaitytuvas. Komunikavimo etapo metu pirmiausiai yra atliekama RFID žymos autentifikavimas serverio pusėje ir

jei žyma yra originali bei nesuklastota, tuomet atliekamas atvirkštinis procesas – serverio pusės autentifikavimas RFID žymoje. Tik sėkmnigai atlikus serverio autentifikavimą, RFID žymoje esantys duomenys gali būti modifikuoti. Sudarytas metodas taiko šį funkcionalumą kaip ir A-SRAC, *Jemal Abawajy* ir *Tassos Dimitriou* metodai.

4.6 lentelė. Sudaryto ir apžvelgtų RFID saugumo metodų palyginimo lentelė

	RHLK	SRAC	A-SRAC	*Jemal Abawajy*	*Tassos Dimitriou*	Sudarytas metodas
Dinaminis identifikatorius	Neturi	Neturi	Turi	Turi	Neturi	Neturi
Atsitiktinis skaičius	Turi	Turi	Turi	Turi	Taip	Turi
Papildomi atsitiktiniai skaičiai	Neturi	Neturi	Turi	Neturi	Neturi	Turi
Abipusė autentifikacija	Neturi	Neturi	Turi	Turi	Turi	Turi
Ar realus indentifikatorius perduodamas tarp RFID žymos ir skaitytuvo?	Ne	Ne	Ne	Ne	Ne	Ne
Naudojamos maišos reikšmės svarbių duomenų apsikeitimui	Taip	Taip	Taip	Taip	Taip (maišos užrakto principas)	Taip
Ar realus identifikatorius saugomas RFID žymose?	Taip	Ne	Ne	Taip	Ne	Ne
Ar saugomi istoriniai duomenys RFID žymose?	Ne	Ne	Taip	Ne	Ne	Ne

Nei vienas iš apžvelgtų RFID saugumo metodų nesiunčia nesaugiu kanalu (tarp RFID žymos ir žymų skaitytuvo) realių RFID žymos identifikatorių. Visuose metoduose yra naudojami maišos algoritmai, kurie suskaičiuoja identifikatoriaus maišos reikšmę ir siunčia ją. Sudarytame metode žymos identifikatorius bei kiti tarpiniai svarbūs duomenys taip pat siunčiami kaip maišos reikšmė.

Metodas kiekybinio tyrimo metu buvo ištirtas su dviem maišos algoritmais: MD5 ir SHA-1. Nustatyta kurio maišos algoritmo naudojimas yra patikimesnis ir kokiu skirtumu. Apžvelgtų metodų dokumentacijose konkretaus maišos algoritmo parinkimas nebuvo akcentuojamas ar ištirtas.

Kitas svarbus veiksnys kuris gali turėti įtakos RFID žymų klastojimo galimybei atsirasti yra senų, istorinių duomenų saugojimas RFID žymose. Iš apžvelgtų metodų tik vienas A-SRAC metodas saugo senąją bei naująją *Key* reikšmes tuo pačiu metu. Sudarytas metodas tai pat nesaugo istorinių duomenų – realiu laiku yra saugomi tik tuo metu aktualūs duomenys, kurie po sėkmingo komunikavimo etapo, RFID žymoje yra pakeičiami ir senos reikšmės ar reikšmės prieš pakeitimus nėra saugomos atmintyje.

Apibendrinus atliktą kokybinį tyrimą suformuluotos tokios išvados:

- iš visų nustatytų esminių kriterijų, pagal kuriuos buvo vertinti analizės dalyje apžvelgti RFID saugumo metodai ir sudarytas metodas, yra vienas kriterijus, kurio sudarytas metodas netenkina – neturi dinaminio identifikatoriaus;
- yra tik du metodai, kurie naudoja dinaminius RFID žymų identifikatorius: A-SRAC ir *Jemal Abawajy* metodai;
- dinaminis RFID žymų identifikatorius yra naudojamas A-SRAC metode, tačiau šiame metode yra saugomi istoriniai duomenys RFID žymose, o tai yra trūkumas, kurio mūsų sudarytas metodas neturi;
- dinaminis RFID žymų identifikatorius taip pat yra naudojamas *Jemal Abawajy* metode, kuris nenaudoja papildomų atsitiktinių skaičių, o mūsų sudarytas metodas naudoja. Tačiau *Jemal Abawajy* metode RFID žymos realus identifikatorius yra saugomas pačioje RFID žymoje, o mūsų sudarytame metode realus žymos identifikatorius nėra saugomas;
- pagal likusius kriterijus sudarytas metodas nenusileidžia arba lenkia kitus metodus.

4.3. Atsparumo RFID žymų klastojimui įvertinimas

RFID žymų pagrindinė funkcija yra identifikuoti save pateikiant savo unikalų identifikatorių (UID).

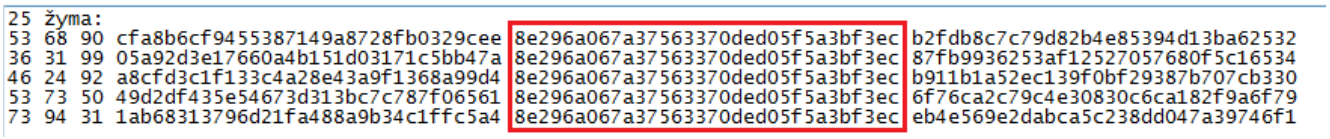
Sudarytame RFID žymų apsaugos nuo klastojimo metodo programiniame modelyje UID atitinka maišos reikšmė H(ID).

Yra žinoma, jog UID kocepcija yra RFID technologijos kertinis akmuo. Jei turime RFID sistemą su labai daug žymų, tuomet tikėtina, jog UID unikalumo sąlyga gali būti pažeista ir sistemoje gali atsirasti dvi žymos su vienodais UID. Todėl sudarytame RFID žymų apsaugos nuo klastojimo metodo teoriniame apraše UID generavimas nėra vienareikšmiškai ir griežtai apibrėžtas, o programiniame modelyje generuojamas H(ID), kur ID yra sveikas natūralus skaičius (1, 2, 3, ...). Šio darbo kontekste to visiškai pakanka, tačiau realiose sistemose ID turėtų būti generuojamas atsitiktinai įtraukiant ir raidinius simbolius, pavyzdžiui, A12H21. Tuomet sugeneruota atsitiktinio žymos ID reikšmė H(ID) bus tikrai unikali ir jos unikalaus identifikatoriaus nustatymas bus sudėtingas (ar net neįmanomas) atliekant žymos klastojimo atakas. Jei realioje RFID sistemoje žymos identifikatoriai būtų sveiki skaičiai, tuomet atlikti RFID žymos klastojimą ir atspėti iš H(ID) realų ID gali būti nesudėtingas uždavinys.

Šiuo metu RFID sistemų gamintojai netgi taiko patentuotus algoritmus, kurie generuoja visiškai unikalius ir ilgus UID [14]. Tokie algoritmai tikimybę surasti du vienodus UID tarp visų pagamintų RFID žymų (ne vienos sistemos ribose) praktiškai sumažina iki nulio. Todėl tokių žymų klastojimas tampa išties sudėtingu uždaviniu.

Sudarytas apsaugos nuo klastojimo metodo programinis modelis žymų UID skaičiuoja pasirinktinai naudojant MD5 arba SHA-1 maišos skaičiavimo algoritmą. Tačiau metodą galima pritaikyti naudoti ir kitus maišos skaičiavimo algoritmus.

Programiniame modelyje atliekant kelis sėkmingus komunikavimo su ta pačia RFID žyma etapus, galima pastebėti, jog atvirame kanale kiekviename etape yra vienodų perduodamų duomenų:



4.1 pav. Pasikartojantys duomenys tarp žymos ir skaitytuvo

Pavyzdyje pateiktas 25-os žymos UID, kuris klastotojui yra gerai „matomas“ ir suprantamas. Čia pasireiškia sudaryto metodo (kaip ir daugumos analizės dalyje aprašytų RFID žymų apsaugos nuo klastojimo metodų) paradoksas – klastotojas gali turėti svarbiausią RFID žymos informaciją UID, tačiau pats klastotės sukūrimas ir jos panaudojimas tampa sudėtingu uždaviniu. Klastotojas nežino, kas RFID žymoje yra padaroma su prieš tai siunčiama informacija. Netgi sužinojus tam tikros žymos aritmetinių operacijų rinkinį ir bandant suskaičiuoti žymos grąžinamą atsakymo reikšmę $H(s \,||\, k)$, kur $s = (x_1\ (op1)\ x_2\ (op2)\ x_3)$, lieka nežinomasis k, kuris po kiekvieno sėkmingo komunikavimo etapo su RFID sistemos žymų skaitytuvu pasikeičia. Todėl klastotojas turi atsekti k kitimo logiką. Išsiaiškinus vien žymos UID ir sukūrus tariamą žymos klastotę, sistema jos nepriims, nes yra naudojamas abipusis autentifikavimas.

Realizuotame programiniame modelyje k kitimo logika iš esmės yra paprasta. Kintamasis k po kiekvieno sėkmingo komunikavimo etapo su RFID žymų skaitytuvu yra padidinamas 0.001, kur pradinis $k \in [0.001; 0.999]$. Tačiau realiose sistemose kintamojo k kitimo logiką galima keisti pagal įvairius aspektus:

- k didinimas atsitiktinai sugeneruotu statiniu Δk parametru;
- kiekvieną kartą k didinimas vis naujai sugeneruotu dinaminiu Δk parametru;
- pradinis k sugeneruojamas pagal RFID žymoje esantį konkretų unikalų parametrą (pavyzdžiui, gamyklinį RFID lusto kodą ir pan.).

Kitas labai svarbus sudaryto metodo privalumas yra tai, jog jei klastotojui vis dėlto pavyktų pagaminti veikiančią originalios RFID žymos klastotę (atsitiktinumo faktorius išlieka), kitos sistemos žymos liktų nesukompromituotos. Dažnai praktikoje pasitaikantis ir literatūroje minimas reiškinys yra visos RFID sistemos klastojimas, kuomet vienos RFID žymos slaptos informacijos atskleidimas suteikia galimybę atskleisti visų sistemos žymų informaciją ir suklastoti praktiškai visą RFID sistemą. Kitaip tariant, visos sistemos RFID žymos veikia pagal bendrą schemą, kurios veikimo principo

atskleidimas gali suteikti galimybę įsilaužėliui perimti visos sistemos resursus. Sudarytame metode kiekvienoje sistemos RFID žymoje yra atliekami saviti skaičiavimai, tad vienos žymos skaičiavimo logikos atskleidimas neturi įtakos kitų sistemos žymų kompromitavimui.

Programiniame modelyje buvo realizuota aritmetinių operacijų generavimo procedūra, kuri visiškai nepriklausomai gali sugeneruoti dvi aritmetines operacijas. Operacijos yra įrašomos į RFID žymą ir pagal jas bus atliekami atitinkami skaičiavimai. Priklausomai nuo realios sistemos techninių reikalavimų, opereacijų generavimo procedūra gali būti pritaikyta ir loginėms ar kitokioms unikalioms operacijoms generuoti.

Sudarytame metode su kiekviena RFID žyma klastotojo įrenginys gali komunikuoti neribotą kiekį kartų ir vis bandyti išgauti svarbią informaciją, bandyti atlikti brutalaus įsilaužimo (angl. *brute-force*) atakas ir pan. Šiuo metu RFID žymose nėra įprasta naudoti tokius apsaugos mechanizmus, kaip neteisingų bandymų nuskaityti informaciją fiksavimas ir neteisėtų įrenginių prisijungimo blokavimas. Taip yra todėl, kad RFID technologija yra gana nestabili, nes duomenys keliauja bekontakčiu būdu, taip pat yra negarantuotas energijos tiekimas žymos procesoriui, jei naudojamos pasyvios RFID sistemos. Tai iš dalies sumažina atsparumą žymų klastojimui, nes žymų klastotojo įrenginys gali komunikuoti su žyma *n* kartų ir bandyti atspėti veikimo schemos logiką.

Sudarytame žymų apsaugos nuo klastojimo metode realizuotas serverio autentifikavimas RFID žymoje, kuris neleidžia modifikuoti žymoje esančių duomenų. Jeigu serverio autentifikavimas žymoje nepavyko, tuomet žymoje esantys duomenys išlieka nepakeisti ir nesuklastoti.

5. IŠVADOS

Atlikus RFID žymų apsaugos nuo klastojimo metodo sudarymą ir tyrimą, buvo suformuluotos galutinės viso darbo išvados:

- atlikus išsamią galimų pažeidžiamumų RFID sistemose analizę, buvo nustatyta, jog pavojingiausias pažeidžiamumas, kurio sėkmingo vykdymo rezultatai gali išaukti galimybę klastotojui sukurti RFID žymos klastotę, yra radijo dažnių manipuliavimo grupės atakos: *slapto stebėjimo, suklastojimo* ir *pakartojimo* atakos. Todėl mūsų sudarytame RFID žymų apsaugos nuo klastojimo metode pagrindinis dėmesys yra skirtas šių atakų sėkmingo atlikimo galimybių sumažinimui;
- išnagrinėjus keletą sukurtų RFID saugumo metodų, nustatyti esminiai RFID žymų apsaugos nuo klastojimo taikymo principai, kurie galėtų panaikinti arba sumažinti galimybę suklastoti žymas: abipusės autentifikacijos taikymas, vengimas perduoti duomenis atviru formatu tarp žymos ir skaitytuvo, maišos funkcijų naudojimas perduodant svarbius duomenis, atsitiktinių skaičių naudojimas, kuris apsaunkina duomenų analizę, dinamiškas žymos identifikatorių keitimas, vengimas kaupti senų komunikavimo etapų duomenis žymose. Dauguma šių principų buvo pritaikyti mūsų sudarytame RFID žymų apsaugos nuo klastojimo metode;
- sudarytam metodui apskaičiuotas perduodamų duomenų entropijos rodiklis tarp virtualių RFID žymų ir virtualaus žymų skaitytuvo vidutiniškai kinta tarp 0,75 – 0,80, priklausomai nuo to koks maišos algoritmas naudojamas: MD5 ar SHA-1. Pasiektas rezultatas rodo neblogą duomenų patikimumą, nes maksimalus entropijos rodiklis yra 1,00;
- sudaryto metodo kiekybinio įvertinimo rezultatai parodo, jog metodą pritaikius veikti naudojant SHA-1 maišos algoritmą, perduodamų tarp žymos ir skaitytuvo duomenų entropija yra 3,57% – 5,88% (apie 4,73%) didesnė, nei metodą pritaikius veikti naudojant MD5 maišos algoritmą. Šiuo atveju skirtumas yra nelabai didelis, todėl pagrindinis pasirinkimo kurį maišos algoritmą naudoti kriterijus galėtų būti jų naudojamų techninių resursų geresnis išpildymas, nes RFID žymose esantys techniniai resursai yra labai riboti;
- kokybiškai įvertinus ir palyginus sudarytą metodą su analizės dalyje apžvelgtais RFID saugumo metodais, nustatyta, jog yra du metodai (A-SRAC ir *Jemal Abawajy*), kuriems sudarytas metodas nusileidžia savo savybėmis, nes neturi dinaminių žymų identifikatorių. Ši savybė gana stipriai padidintų apsaugą nuo žymų suklastojimo. Tačiau mūsų sudarytas metodas turi du privalumus, kurių neturi anskčiau minėti RFID saugumo metodai: nesaugo savo realaus žymos identifikatoriaus žymos atmintyje (kaip tai daroma *Jemal Abawajy* metode) ir nesaugo istorinių komunikavimo etapų duomenų (kaip tai realizuota A-SRAC metode);

- palyginus su kitais likusiais RFID saugumo metodais (RHLK, SRAC, *Tassos Dimitriou*), mūsų sudarytas metodas jiems nenusileidžia arba lenkia, pagal naudojamas savybes ir teikiamas galimybes, kurios leidžia išvengti RFID žymų klastojimo,.

6. LITERATŪRA

[1] Securing RFID Systems by Detecting Tag Cloning / Mikko Lehtonen, Daniel Ostojic, Alexander Ilic, Florian Michahelles // Proceedings of 7th International Conference on Pervasive Computing. 2009. p. 291-308.

[2] Nokia 5140 RFID Reader. [interaktyvus], [žiūrėta: 2013-05-21]. Prieiga per internetą: <http://www.mobilemag.com/2004/03/16/nokia-5140-rfid-reader/>.

[3] Is Your Cat Infected with a Computer Virus? / M. R. Rieback, B. Crispo, Tanenbaum // IEEE Conference on Pervasive Computing and Communications. 2006. p. 169-179.

[4] Enhancing RFID Tag Resistance against Cloning Attack / Abawajy J. // Network and System Security, NSS '09. Third International Conference. 2009. p. 18-23.

[5] The Basics of RFID Technology. [interaktyvus], [žiūrėta: 2013-05-21]. Prieiga per internetą: <http://www.rfidjournal.com/article/articleview/1337/1/129/>.

[6] About NFC. [interaktyvus], [žiūrėta: 2013-05-21]. Prieiga per internetą: <http://www.nfc-forum.org/aboutnfc/>.

[7] RFID Security / Frank Thornton, Chris Lanthem. Kanada, 2006. 448 p. ISBN 1-59749-047-4.

[8] Authentication and lightweight cryptography in low cost RFID / Mobahat H. // Software Technology and Engineering (ICSTE), 2nd International Conference. 2010. p. 123-129.

[9] A Survey of Lightweight-Cryptography Implementations / Eisenbarth T, Kumar S. // Design & Test of Computers, IEEE. 2007. p. 522-533.

[10] Secure and Low-cost RFID Authentication Protocols / Yong Ki Lee, Ingrid Verbauwhede // University of California, Los Angeles. 2010. p. 1-5.

[11] Enhancing RFID Tag Resistance against Cloning Attack / Abawajy J. // Network and System Security, NSS '09. Third International Conference. 2009. p. 18-23.

[12] A Lightweight RFID Protocol to protect against Traceability and Cloning attacks / Dimitriou T. // Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2008. First International Conference. 2008. p. 59-66.

[13] RFID Gen 2 What is it? [interaktyvus], [žiūrėta: 2013-05-21]. Prieiga per internetą: <http://www.skyrfid.com/RFID_Gen_2_What_is_it.php>.

[14] The Operational Meaning of Min- and Max-Entropy / Konig, R. // IEEE Information Theory Society. 2010. p. 4337-4347

[15] IT Security Stack Exchange [interaktyvus], [žiūrėta: 2013-05-21]. Prieiga per internetą: <http://security.stackexchange.com/questions/19705/is-sha1-better-than-md5-only-because-it-generates-a-hash-of-160-bits>.

7. PRIEDAS. TARPINIAI ENTROPIJOS SKAIČIAVIMAI

Entropijos skaičiavimo rezultatai 2-ai RFID žymai, taikant MD5 maišos algoritmą, pateikti 7.1 lentelėje:

7.1 lentelė. Antros RFID žymos entropijos skaičiavimas taikant MD5

Nr.	2-a žyma: operacijos + ir /, naudojant MD5 maišą				
	x_i			Duomenys	Entropija
	x_1	x_2	x_3		
1.	11	99	24	119924b152ebf2b50c22fd723126f3c30fcfc598f1 3708210194c475687be6106a3b8470ca5bb1701534 e8e898cc7d57809d80	0,76623
2.	25	94	28	259428703c4d6230f3330e3f9aa8d12250939c98f1 3708210194c475687be6106a3b84465094128269d2 5da3ed0a3e3a8e3142	0,74359
3.	1	13	77	11377eb8b262bfa11f4d11b4fe0f5ebcd8c4a98f13 708210194c475687be6106a3b84a20286bfe94bfd6 dfadf37a43c86de57	0,76035
4.	85	17	19	851719ab2dc8534f4a69e9294e2256581c557498f1 3708210194c475687be6106a3b843d80dd15a1c2ae 3782dabd771d4b87ca	0,77007
5.	37	79	64	37796480b178b025e68d98db5b64f419131e0398f1 3708210194c475687be6106a3b849fb4b64605b52a c56e7ca8eba2719f0c	0,76623
6.	43	32	94	433294282aa9b176f0d1df8c9ce12dd9dbbaf298f1 3708210194c475687be6106a3b84d794216038d640 34cec73b93b64bad2c	0,74732
7.	74	29	45	742945c0b7daf5735484957313a1b5b863500098f1 3708210194c475687be6106a3b84711ad51d1d8b43 7c5425ca486f7e4d3c	0,77391
				Vidurkis:	**0,76110**

Entropijos skaičiavimo rezultatai 2-ai RFID žymai, taikant SHA-1 maišos algoritmą, pateikti 7.2 lentelėje:

7.2 lentelė. Antros RFID žymos entropijos skaičiavimas taikant SHA-1

Nr.	2-a žyma: operacijos + ir /, naudojant SHA-1 maišą				
	x_i			Duomenys	Entropija
	x_1	x_2	x_3		
1.	22	70	37	227037e4ec9f7f50c82ca0117aa727d7e76e9b829c 632f91032ad7bbcb6cf72875e8e8207dcfba80173f 7c66ea51d0c31b5b0c86f8ecfa06ad0c5511c2cf3a	0,80645
2.	92	20	88	922088810dbcb985fd9f8a7d5636aa6395066a42e1 721a91032ad7bbcb6cf72875e8e8207dcfba80173f 7c6363e5d617ccb718a2d35196e7bed7c1fdf09b88	0,79359
3.	46	22	12	4622125e74aeb6649fe44c5ebd6330f63547b0ec69 de8391032ad7bbcb6cf72875e8e8207dcfba80173f 7ce477bf9beac681b738b872c0f8051a57e48d20d7	0,80322
4.	75	87	59	75875933c46e849318629625e244627a6208194cc9 c97c91032ad7bbcb6cf72875e8e8207dcfba80173f	0,83607

				7cae8da6775825b02f9455ec767cf3c503da2c2715	
5.	4	97	88	4978804aa01e580271bc2c167e1f021725efd3b7a852d91032ad7bbcb6cf72875e8e8207dcfba80173f7c007cb04bd149678e2247a33b9fba3ca93f0b919b	0,76678
6.	96	59	53	9659537336f5f6f775419c2b5580eeaf5e58a35f9c98cb91032ad7bbcb6cf72875e8e8207dcfba80173f7c26de660149325fc0be5bb05df0c83fee8ad7e3e7	0,83607
7.	26	75	66	26756671cb6f374af8fde2bdb0d0e26663aefb68ceae6291032ad7bbcb6cf72875e8e8207dcfba80173f7cc0dd337029fc8526690bf90070fd2143cc0553e5	0,79359
				Vidurkis:	**0,80511**

Entropijų palyginimas, kuomet buvo sugeneruoti vienodi pradiniai parametrai taikant MD5 ir SHA-1 maišos algoritmus:

7.3 lentelė. Entropijų skaičiavimų palyginimas antrai žymai

2-a žyma: operacijos + ir /				
x_i			**Entropijos**	
x_1	**x_2**	**x_3**	**MD5**	**SHA-1**
92	20	88	0,72881	0,79359
75	87	59	0,78947	0,83607
96	59	53	0,77391	0,83617
25	94	28	0,74359	0,79679
85	17	19	0,77007	0,82413
43	32	94	0,74732	0,79452
Vidurkiai:			**0,75886**	**0,81353**

Entropijos skaičiavimo rezultatai 3-iai RFID žymai, taikant MD5 maišos algoritmą, pateikti 7.4 lentelėje:

7.4 lentelė. Trečios RFID žymos entropijos skaičiavimas taikant MD5

Nr.	**3-ia žyma: operacijos * ir *, naudojant MD5 maišą**				
	x_i			**Duomenys**	**Entropija**
	x_1	**x_2**	**x_3**		
1.	57	90	99	57909952f1931765b38290f8b3d8fe1854e6bdc20ad4d76fe97759aa27a0c99bff6710d5a637cd11aa722a9b4c922c7b740a63	0,76532
2.	81	99	52	819952bd34b2bd83fde77e2ce9dfcaa5562218c20ad4d76fe97759aa27a0c99bff6710e3c232763592623cd10e507f84bd957b	0,77153
3.	58	80	6	588066d29713d3bf3ded4b89f65c660639969c20ad4d76fe97759aa27a0c99bff6710d65e982af8c58ed56df23606e496417d	0,77465
4.	46	69	28	466928d2e8b965c394fd701ba8c6db46f71a92c20ad4d76fe97759aa27a0c99bff6710d05847bfd20258c3586f53947618411e	0,76224
5.	59	3	23	5932387e7f6dbe0a03bd58ab7f59362c42014c20ad4d76fe97759aa27a0c99bff671024a078c4a9087f3	0,75304

				002459acdf39ac841	
6.	1	23	52	12352bab94e4267bd0730183a597f6bbe5072c20ad4d76fe97759aa27a0c99bff67108f8712cab7334dfb6013a5e9fcfeb972	0,76224
7.	15	10	8	151088a6db9a780fb02e3963a20cca9ec035ac20ad4d76fe97759aa27a0c99bff6710b708f037dcb1edb933c41be560551f01	0,77465
				Vidurkis:	**0,76624**

Entropijos skaičiavimo rezultatai 3-iai RFID žymai, taikant SHA-1 maišos algoritmą, pateikti 7.5 lentelėje:

7.5 lentelė. Trečios RFID žymos entropijos skaičiavimas taikant SHA-1

Nr.	**3-ia žyma: operacijos * ir *, naudojant SHA-1 maišą**				
	x_i			**Duomenys**	**Entropija**
	x_1	**x_2**	**x_3**		
1.	20	100	1	2010018a91c656d39de29f7fed1cd79233ccb41e723d0a7b52009b64fd0a2a49e6d8a939753077792b0554bfd4f75d6f521352303743a085eb7460255bd0b0	0,80531
2.	12	62	29	126229bce383c4f45056bcb42741761042353a186153c07b52009b64fd0a2a49e6d8a939753077792b0554b6d2c56dd3f0699c3faf906f9b9ba285c8864d3a	0,81333
3.	64	27	26	6427266c62730ac25c6a71d5db25c036e58dcd6ba344897b52009b64fd0a2a49e6d8a939753077792b0554062ed6fb7dca45c2be9c21bd90306a1e2f61fc48	0,81573
4.	93	36	26	933626474e016ce794ff702ccb0cf565b5a38c8d982beb7b52009b64fd0a2a49e6d8a939753077792b0554de4ffb200e4d6c8000c4c6db27898abd95892948	0,78947
5.	13	99	80	139980c49f2333534c54cf68a51d780eb552aeae6660147b52009b64fd0a2a49e6d8a939753077792b0554d780392a2daf1d1105f1be469a9926184894d480	0,77582
6.	60	77	85	607785dbef84ec2c7ce5f881ab244b1e85984ef112a16a7b52009b64fd0a2a49e6d8a939753077792b0554fc8cdeac2a81b0207ddddb769eca1b1fea4e8bb7	0,80761
7.	91	59	69	915969e59ee0236923259107cb6a9cd0b7f9841be1f74a7b52009b64fd0a2a49e6d8a939753077792b055446af0df6442c01d989c564781692f50f41392d01	0,76419
				Vidurkis:	**0,79592**

Entropijų palyginimas, kuomet buvo sugeneruoti vienodi pradiniai parametrai taikant MD5 ir SHA-1 maišos algoritmus:

7.6 lentelė. Entropijų skaičiavimų palyginimas trečiai žymai

3-ia žyma: operacijos * ir *				
x_i			**Entropijos**	
x_1	**x_2**	**x_3**	**MD5**	**SHA-1**
12	62	29	0,74254	0,81333
93	36	26	0,75396	0,78947
60	77	85	0,75145	0,80761

81	99	52	0,77153	0,80125
46	69	28	0,76224	0,79341
1	23	52	0,76224	0,82550
		Vidurkiai:	**0,75245**	**0,80645**

Entropijos skaičiavimo rezultatai 4-ai RFID žymai, taikant MD5 maišos algoritmą, pateikti 7.7 lentelėje:

7.7 lentelė. Ketvirtos RFID žymos entropijos skaičiavimas taikant MD5

Nr.	**4-a žyma: operacijos / ir /, naudojant MD5 maišą**				
	x_i			**Duomenys**	**Entropija**
	x_1	**x_2**	**x_3**		
1.	50	46	18	504618bf66e3d08053a42d1942cf515e6650531ff1de774005f8da13f42943881c655fbd1c42a7f1c3e1a8e7ac6e4c2e20e23d	0,76623
2.	16	60	59	16605929e8c6c4a5a4f3074b9d185a0a0b43c91ff1de774005f8da13f42943881c655f8ce3fac7e23a02ab4e00cf0f1e03310a	0,73987
3.	28	10	63	281063a460140c6ae12ae5200eac0bd82316791ff1de774005f8da13f42943881c655fcfdbf9cdea3adf86354db4611df22a7c	0,73987
4.	83	60	40	8360405a17c224b99e36b4f1b9a99d445b8e031ff1de774005f8da13f42943881c655feba8791b946b9a70f082a495906dc704	0,75107
5.	61	89	1	618914595d9c940ffe8b88924a9f14360f2241ff1de774005f8da13f42943881c655fb5f84c0de25be7043e378a83e2327848	0,76419
6.	28	47	97	28479774f51e9c764695e1a40afb5fb9bdc1ab1ff1de774005f8da13f42943881c655fff0be796ef2d5cf616a2fd9b65fd3303	0,73546
7.	84	63	37	8463374678997b782567b4fddf6aca29d545eb1ff1de774005f8da13f42943881c655f1a6be42a143a049501b32c8d3abd2642	0,77007
				Vidurkis:	**0,75240**

Entropijos skaičiavimo rezultatai 4-ai RFID žymai, taikant SHA-1 maišos algoritmą, pateikti 7.8 lentelėje:

7.8 lentelė. Trečios RFID žymos entropijos skaičiavimas taikant SHA-1

Nr.	**4-a žyma: operacijos / ir /, naudojant SHA-1 maišą**				
	x_i			**Duomenys**	**Entropija**
	x_1	**x_2**	**x_3**		
1.	70	97	26	709726aa7dacc945a463771f671631888488323c41d1884d134bc072212ace2df385dae143139da74ec0ef450da336723e9ecee54e5fd818e5ee4183e0d490	0,78092
2.	54	93	6	5493604eadf4aeb61f53681a1895c70183e69da7be5bc4d134bc072212ace2df385dae143139da74ec0ef1738cf22a7c0d7b3756745da08f55aa19d96666a	0,78891

3.	22	34	74	223474a658adf54c645add880ce3baa54317d6bc34a9854d134bc072212ace2df385dae143139da74ec0efe53a215b79340636fca600944b078deda36db4bb	0,75000
4.	38	26	76	382676fcd6fbd8e8b46b938d0457501e756d44916a31894d134bc072212ace2df385dae143139da74ec0ef475c0ddbaca2b4934093ca664146fe70c8475c5e	0,74625
5.	23	5	41	23541f87bcf9d47a3dc80a8c54329df33e071a567b82d4d134bc072212ace2df385dae143139da74ec0ef69527126a90b331ca803eefb8c9e3416cec0452a	0,77305
6.	56	36	70	563670ae16dc184c6f80880bb6e9f1bde8164df8bf45bd4d134bc072212ace2df385dae143139da74ec0efdffbbdf837e53f6517f0209b5cf3c891711fc273	0,77465
7.	51	74	68	517468e82a3d218659c48de238e40f709c26d010cd32e44d134bc072212ace2df385dae143139da74ec0effa818505012424bea38a45e0d54a2336ebd3c27f	0,73494
				Vidurkis:	**0,76410**

Entropijų palyginimas, kuomet buvo sugeneruoti vienodi pradiniai parametrai taikant MD5 ir SHA-1 maišos algoritmus:

7.9 lentelė. Entropijų skaičiavimų palyginimas ketvirtai žymai

4-a žyma: operacijos / ir /				
x_i			**Entropijos**	
x_1	**x_2**	**x_3**	**MD5**	**SHA-1**
16	60	59	0,73987	0,79041
83	60	40	0,75107	0,78092
28	47	97	0,73546	0,76532
54	93	6	0,77354	0,78891
38	26	76	0,74365	0,74625
56	36	70	0,73617	0,77465
Vidurkiai:			**0,74663**	**0,77441**

Entropijos skaičiavimo rezultatai 5-ai RFID žymai, taikant MD5 maišos algoritmą, pateikti 7.10 lentelėje:

7.10 lentelė. Penktos RFID žymos entropijos skaičiavimas taikant MD5

Nr.	**5-a žyma: operacijos * ir -, naudojant MD5 maišą**				
	x_i			**Duomenys**	**Entropija**
	x_1	**x_2**	**x_3**		
1.	14	90	31	149031c5d607c0cc1b870d92a5e50216a116331f0e3dad99908345f7439f8ffabdffc4706e3aa806192d0e869c1228f2c41cfc	0,75484
2.	38	89	86	388986bb3b17a2989254a3af000d26ee75348c1f0e3dad99908345f7439f8ffabdffc4fb599752ceff4ac27c57c0c5ca430e8c	0,79736
3.	31	3	54	3135464d4738763c1519f6f88a3d67f10d8191f0e3dad99908345f7439f8ffabdffc4698cbd388bf8558a073a5e8ba16e467f	0,79955

4.	69	19	36	691936d9a7a4a02728260d880ba06267524f401f0e3dad99908345f7439f8ffabdffc48babb1ad431bf052b9a05a73e3a41256	0,73248
5.	36	62	85	366285af5f9a82e41235776d1e3a7dca165d1f1f0e3dad99908345f7439f8ffabdffc456d7ee3b01473171873786b0d6ab5dfa	0,81333
6.	72	45	16	724516fe7d5595d694e2780c6a5918f06a41171f0e3dad99908345f7439f8ffabdffc4f4d175f9a1a4403edb6ee59f4154cc1e	0,76541
7.	39	87	73	398773da4aebd1b17162fd7f452c736488ec631f0e3dad99908345f7439f8ffabdffc49971e8c129b2680dd5a696d65b055aca	0,80132
				Vidurkis:	**0,78061**

Entropijos skaičiavimo rezultatai 5-ai RFID žymai, taikant SHA-1 maišos algoritmą, pateikti 7.11 lentelėje:

7.11 lentelė. Penktos RFID žymos entropijos skaičiavimas taikant SHA-1

Nr.	**5-a žyma: operacijos * ir -, naudojant SHA-1 maišą**				
	x_i			**Duomenys**	**Entropija**
	x_1	**x_2**	**x_3**		
1.	10	12	13	101213ee6888b8878eb65946b22b0b17dd34776ec17148b3f0c7f6bb763af1be91d9e74eabfeb199dc1f1f13799fdf3e2135687e9375ba61913ee908aee876	0,81949
2.	87	5	73	87573512db154d2c87fb50565a2f0381605be5cf0367bb3f0c7f6bb763af1be91d9e74eabfeb199dc1f1f3d5d1fd14ffe415aac4a0ef048e75f406eb47723	0,79533
3.	58	43	75	5843751d4551e4c133ed7f9692cb6839498ee6b59b24f7b3f0c7f6bb763af1be91d9e74eabfeb199dc1f1f62504826b9b3a247924e73987a8da4ad699f7a94	0,82278
4.	36	12	52	361252d3b32b45118555ee0a5bf546b5bf4eff0fef4b1db3f0c7f6bb763af1be91d9e74eabfeb199dc1f1f6ac9310c66d1b118088c36c570c8bb4d8e4ff8fb	0,77465
5.	64	3	27	643276f5f8805513c2cd838f6c4d3d7f1caae1f06881ab3f0c7f6bb763af1be91d9e74eabfeb199dc1f1f71ff6f6b6783f81dced9d27e7cb49d42879ac0a2	0,81159
6.	11	71	12	11711251adfd21d2171654949cf1131a1d96e39debf58cb3f0c7f6bb763af1be91d9e74eabfeb199dc1f1f5a03b697df2c2ebb88c058badcf316d8f09498fd	0,77778
7.	61	9	13	61913e24e8b812ce660e03ed33e8353b857495086d73bb3f0c7f6bb763af1be91d9e74eabfeb199dc1f1f3ffae02d547deec7447d13ed0f359df3b3a7e256	0,81105
				Vidurkis:	**0,80181**

Entropijų palyginimas, kuomet buvo sugeneruoti vienodi pradiniai parametrai taikant MD5 ir SHA-1 maišos algoritmus:

7.12 lentelė. Entropijų skaičiavimų palyginimas penktai žymai

5-a žyma: operacijos * ir -				
x_i			**Entropijos**	
x_1	**x_2**	**x_3**	**MD5**	**SHA-1**
87	5	73	0,76419	0,79533
36	12	52	0,73125	0,77465
11	71	12	0,72546	0,77778
38	89	86	0,79736	0,81239
69	19	36	0,73248	0,80000
72	45	16	0,76541	0,78407
Vidurkiai:			**0,75269**	**0,79070**