(19) LIETUVOS RESPUBLIKA
VALSTYBINIS PATENTŲ BIURAS
V P B

(10) **LT 2012 010 A**

(12) **PARAIŠKOS APRAŠYMAS**

(21) Paraiškos numeris: **2012 010**

(51) Int. Cl. (2011.01): **B61L 27/00**

(22) Paraiškos padavimo data: **2012 02 10**

(41) Paraiškos paskelbimo data: **2012 12 27**

(62) Paraiškos, iš kurios dokumentas išskirtas, numeris: —

(86) Tarptautinės paraiškos numeris: —

(86) Tarptautinės paraiškos padavimo data: —

(85) Nacionalinio PCT lygio procedūros pradžios data: —

(30) Prioritetas: **PV 2011-142, 2011 03 17, CZ**

(71) Pareiškėjas:

AŽD PRAHA s. r. o., Žirovnicka 2/3146, 106 17 Praha 10, CZ

(72) Išradėjas:

doc. RNDr. Štepan KLAPKA, CZ
Mgr. Lucie KARNA, CZ
Ing. Jaroslav SUKUP, CZ
RNDr. Magdalena HARLENDEROVA, CZ

(74) Patentinis patikėtinis/atstovas:

Reda ŽABOLIENĖ, Advokatės Redos Žabolienės kontora METIDA, Verslo centras VERTAS, Gynėjų g. 16, LT-01109 Vilnius, LT

(54) Pavadinimas:

Su saugumu susietų, susidedančių iš sudėtinių nesėkmės-saugumo modulių, elektroninių sistemų išsaugojimo būdas, ypač taikomas geležinkelio sistemose pirštų atspaudų formavimo metu

(57) Referatas:

Išradimas yra susijęs su būdu išsaugoti su saugumu susietas, iš sudėtinių gedimams atsparių modulių susidedančias elektronines sistemas, ypač taikomu geležinkelio sistemose pirštų atspaudų formavimo metu, kai ne mažiau kaip du įrenginiai kartu formuoja pirštų atspaudus, kadangi nė vienas iš jų atskirai neleidžia suformuoti tokio pirštų atspaudo. Pirštų atspaudų formavimo procesas išskaidomas į dalinių pirštų atspaudų formavimo nurodytame laiko intervale sekas, kurių rezultatas yra pradinis pirštų atspaudas, o aptikus gedimą viename iš sąveikaujančių įrenginių gedimo nepatyręs su sugedusiuoju sąveikaujantis įrenginys atsisakys formuoti dalinį pirštų atspaudą, o tai neleis suformuoti pradinio pirštų atspaudo.

LT 2012 010 A

Su saugumu susietų, iš sudėtinių gedimams atsparių modulių susidedančių elektroninių sistemų išsaugojimo būdas, ypač taikomas geležinkelio sistemose pirštų atspaudų formavimo metu.

TECHNIKOS SRITIS

Šis išradimas susietas su būdais, kuriuose yra aprašyti saugumo sprendimai, susidedantys iš sudėtinių gedimams atsparių modulių susidedančių elektroninių sistemų, taikomų ypač geležinkelio sistemose pirštų atspaudų formavimo metu.

TECHNIKOS LYGIS

Bendruoju požiūriu, būtiniausių programų aukščiausio lygio atsparumą galima suskirstyti į techninį atsparumą ir funkcinį atsparumą. Funkcinis atsparumas geležinkelių saugumo technologijose yra pirmiausiai susijęs su eismo saugumo algoritmais, užtikrinančiais rizikų, kylančių daugiausiai dėl pačios atsparumo instaliacijos, ypač prijungtoje geležinkelio infrastruktūroje (pavyzdžiui, bėgių grandinėse, semaforuose, smailėse ir kt.), sumažinimą. Antra vertus, užtikrinant techninį atsparumą pagrindinis dėmesys sutelkiamas į rizikas, kurios kyla daugiausiai dėl pačios atsparumo instaliacijos gedimų režimų. Taigi, techninio atsparumo požiūriu, projektuojant tokias instaliacijas reikia atsižvelgti į gedimų režimų poveikį pačios atsparumo instaliacijos funkcionavimui užtikrinant atsparumą. Kalbant apie atskirų gedimų režimų poveikį, reikia užtikrinti, kad sistemos, kurioms keliami didesni atsparumo reikalavimai, išliktų atsparios ištikus bet kokiai įmanomai atskirai techninės įrangos atsitiktinio gedimo būsenai. Šis principas vadinasi „gedimams atsparus“ ir tam pasiekti yra keli būdai, įskaitant savąjį atsparumą gedimams, sudėtinį atsparumą gedimams ir reaktyvųjį atsparumą gedimams. Remiantis savojo atsparumo principu, atsparumą gedimams užtikrina tai, kad jokio tikėtino pobūdžio įrenginio (instaliacijos) gedimas nesunaikins atsparumo. Gedimų išsprendimas turi būti užtikrinamas, pavyzdžiui, fizinėmis panaudotų komponentų ir jų sujungimo savybėmis. Tokiu atveju susidorojimą su gedimu (aptikimą ir šalinimą) užtikrina iš esmės fizikos dėsniai.

Antra vertus, sudėtiniam ir reaktyviajam atsparumui užtikrinti naudojamas aptikimas, leidžiantis pasiekti atsparumo ir taip užkirsti kelią pavojams. Sudėtinio

atsparumo gedimams atveju gedimai aptinkami balsavimo principu. Reaktyviojo atsparumo atveju greitą ir patikimą aptikimą garantuoja specialus šiam tikslui skirtas įrenginys. Tačiau šis specialus įrenginys ne tiesiogiai atlieka atsparumo funkciją, o tik prižiūri tinkamą pagrindinio (funkcinio) įrenginio atliekamos atsparumo funkcijos vykdymą. Specialiam įrenginiui aptikus, kad pagrindinis įrenginys tinkamai nebevykdo atsparumo funkcijos, specialus įrenginys užtikrina, kad sistema, kuriai taikomi didesni atsparumo reikalavimai, persijungtų į atspariąją būseną. Šiek tiek supaprastinus būtų galima sakyti, kad balsavimo dėl sudėtinio atsparumo gedimams principas pakeičiamas specialiojo reaktyviojo atsparumo įrenginio atliekamu aptikimu. Dabar naudojamose didelės rizikos atvejams skirtose atsparumo instaliacijose paprastai naudojami visi trys principai ir kai kuriais atvejais labai sunku nuspręsti, kuris iš tų principų yra susijęs.

Esant sudėtiniam atsparumui gedimams, atsparumo funkciją atlieka (eismo saugos algoritmus vykdo) daugiau nei vienas įrenginys (instaliacija) arba instaliacijos dalis kartu su kitais įrenginiais. Tokiu atveju nepriklausomi įrenginiai priima sprendimus daugumos principu, balsuoja dėl savo išvesčių ir funkcijų. Pavyzdžiui, sprendimą priima du iš dviejų, du iš trijų, trys iš penkių įrenginių ir t.t. Atsparumo instaliacija gali būti, pavyzdžiui, ETCS (Europos traukinių valdymo sistemos) radijo ryšio blokų centras, kuris dviejų iš trijų įrenginių sistemoje (sprendimų dėl jų funkcijų išvesčių priėmimas balsų dauguma) sukuria komandas traukiniams, perduodamas GSM ryšiu. Dėl GSM ryšio atakavimo tikimybės būtina naudoti kriptografinę apsaugą pasitelkiant DES (duomenų šifravimo standarto) blokinį šifrą. Sudėtinio atsparumo gedimams technologijos atveju būtina, kad pavojinga gedimo būsena viename įrenginyje būtų aptikta ir pašalinta per tokį laiką, kokio pakanka užkirsti keliui tokiai pačiai gedimo būsenai kitame įrenginyje. Būtina, kad gedimo būsena būtų pašalinta greičiau, nei pasirinktas aptikimo būdas (balsavimas) žlugs dėl tolesnio palaipsnio sistemos gedimo.

Viena iš svarbių procedūrų užtikrinant sudėtinio atsparumo gedimams principo veikimą – aptikto gedimo pašalinimo procesas. Paprastai naudojamas negrįžtamas blogai veikiančio įrenginio atjungimas, kad jis daugiau nebefunkcionuotų. Kadangi įrenginiui atjungti paprastai reikia atjungti elektros energijos tiekimą, tai po to iš naujo įprastai paleidžiant sistemą gali rastis tam tikrų nesklandumų. Kitas dažnai

naudojamas būdas – blogai veikiančio komponento izoliavimas, pavyzdžiui, blogai veikiantis įrenginys funkciškai atjungiamas, o atjungti techninės įrangos nereikia. Viena iš galimybių šiam metodui įgyvendinti – atsparumui aktualios informacijos, reikalingos atsparumo užtikrinimo požiūriu svarbios veiklos vykdymui, buvimas, pvz., pasirinktos komunikacijos tarp atsparumo instaliacijų vykdymas. Bendras komponentas, kurį privalo turėti siunčiami pranešimai, yra saugos kodas, kuris yra pranešimo, pridedamo prie perduodamų duomenų jų vientisumui ir autentiškumui patikrinti, dalis. Savo sandara saugos kodas gali būti kriptografinis arba nekriptografinis. Patento CZ 296129 dokumente saugos kodo forma yra pritaikyta sudėtinio atsparumo gedimams reikmėms, bet šis sprendimas tetinka kai kuriems cikliniams kodams ir negali būti naudojamas linijiniams ar kriptografiniams kodams. Būtent todėl jis netinka perdavimo sistemoms, kuriose atakos prieš perduodamą informaciją (t.y., ypač pakeičiant jos turinį ar autentiškumą) galimybė negali būti atmesta. Kriptografinio saugos kodo skaičiavimui galima naudoti dokumente DE 102007032805 A1 aprašytą procedūrą, tačiau tik esant konkrečiai sudėčiai. Tai yra, ribotam saugos kodų kiekiui, o tai apriboja jos panaudojimą. Šios išradimo tikslas – procesas, kurį galima adaptuoti beveik bet kokiam saugos kodo tipui (toliau vadinamam duomenų pirštų atspaudu).

IŠRADIMO ESMĖ

Šio išradimo objektas – su saugumu susietų, iš sudėtinių gedimams atsparių modulių susidedančių elektroninių sistemų išsaugojimo būdas, ypač taikomas geležinkelio sistemose pirštų atspaudų formavimo metu, kai ne mažiau kaip du įrenginiai kartu formuoja pirštų atspaudus, kadangi nė vienas iš jų atskirai neleidžia suformuoti tokio pirštų atspaudo. Išradimo pagrindą sudaro faktas, kad pirštų atspaudų formavimo procesas išskaidomas į dalinių pirštų atspaudų formavimo nurodytame laiko intervale sekas, kurių rezultatas yra pradinis pirštų atspaudas, o aptikus gedimą viename iš sąveikaujančių įrenginių gedimo nepatyręs su sugedusiuoju sąveikaujantis įrenginys atsisakys suformuoti dalinį pirštų atspaudą, o tai neleis suformuoti pradinio pirštų atspaudo. Todėl pradinį pirštų atspaudą galima suformuoti tik iš įrenginių be jokio gedimo sekos. Atsparumo sistema, į kurią įeina aukščiau minėti įrenginiai, gali būti radijo ryšio blokų centras, skirtas traukinių valdymui radijo ryšiu.

Pirštų atspaudai yra funkcijos, iš kurios duotieji pradiniai duomenys (įvesties informacija) generuoja būdingųjų duomenų imtį pradiniams duomenims pasitelkiant apibrėžtą konkrečią redukciją, rezultatas. Pavyzdžiui, tokią funkciją galima sukurti panaudojant ciklinį kodą, kuriame pirštų atspaudas yra likusioji dalis po įvesties informacijos dalijimo, kurį atliko ciklinio kodo generuojantysis daugianaris. Po to toks pirštų atspaudas naudojamas, pavyzdžiui, duomenų vientisumui ar autentiškumui patikrinti.

Linijinių kodų atveju, kai pirštų atspaudas formuojamas panaudojant generuojančiąją matricą, gaunamas dalinis pirštų atspaudas yra suformuojamas kaip pradinio pirštų atspaudo perstata, kurioje apgrąžinė perstata išskaidyta į dalines perstatas, taip sukuriant dalines transformacijas, kurios suformuos pradinį pirštų atspaudą iš gautojo dalinio pirštų atspaudo. Šiam tikslui pakanka atlikti generuojančiosios matricos stulpelių perstatą.

Jei pradiniam CBC-MAC duomenų pirštų atspaudui CBC (šifruojamo bloko prirakinimo) metodu suformuoti naudojamas blokinis šifras, tai blokinis šifras modifikuojamas taip, kad CBC metodu gautas dalinis pirštų atspaudas skirtųsi nuo pradinio CBC-MAC duomenų pirštų atspaudo, o pradinis CBC-MAC duomenų pirštų atspaudas suformuojamas papildomomis dalinėmis gauto dalinio pirštų atspaudo transformacijomis.

Jei naudojamas DES (duomenų šifravimo standarto) blokinis šifras su pradinio duomenų bloko įvesties perstata, šifravimo dalimi ir užšifruoto duomenų bloko apgrąžine išvesties perstata, tai ši apgrąžinė išvesties perstata išskaidoma į dalines perstatas, o tai sukuria dalines transformacijas pradinio pirštų atspaudo suformavimui iš gautojo dalinio pirštų atspaudo.

Jei naudojamas AES (pažangiojo šifravimo standarto) blokinis šifras, kuris vykdomas skaičiuojant blokus (raundus) panaudojant specifinį raktą kiekvienam raundui, tai skirtingas raktas pridedamas prie užšifruotų duomenų iš pradinio duomenų bloko kiekviename raunde, o paskutinio raundo raktas pridedamas prie kito CBC metodo skaičiavimo žingsnio pirmojo raundo rakto, tai užtikrina skirtumą tarp gautojo dalinio pirštų atspaudo ir pradinio pirštų atspaudo; gautasis pirštų atspaudas

tolesniu daliniu transformavimu pakeičiamas į tokią formą, kurioje jis yra pradinio pirštų atspaudo perstata, o apgrąžinė perstata išskaidoma į dalines perstatas, kurios transformuoja dalinį pirštų atspaudą į pradinį pirštų atspaudą.

Jei naudojami linijiniai kodai, kai pirštų atspaudas formuojamas panaudojant generuojančiąją matricą, tai pirštų atspaudo patikra atliekama gautuoju daliniu pirštų atspaudu, kuris beklaidžiame autentiškame pranešime sutampa su gautuoju pirštų atspaudu, kuriam pritaikyta apgrąžinė perstata, o gaunamas įrenginiams sąveikaujant. Jei naudojama patikros daugianarių sistema, kurių mažiausias bendras kartotinis lygus generuojančiajam ciklinio saugos kodo daugianariui, tai šie patikros daugianariai naudojami vientisumui ir autentiškumui patikrinti.

Jei naudojamas DES blokinis šifras, tai pradinio CBC-MAC duomenų pirštų atspaudo patikroje naudojamas atvirkštinis procesas trimis abipusiai skirtingais raktais K_{s1}, K_{s2}, K_{s3}, kurio metu gautasis pradinis CBC-MAC duomenų pirštų atspaudas pirmiausia iššifruojamas panaudojant trečiąjį raktą K_{s3}, o tuomet užšifruojamas panaudojant antrąjį raktą K_{s2}; jei tikrinamas pirštų atspaudas yra autentiškas ir vientisas, tai šių operacijų rezultatas būna lygus pranešimo, sukurto panaudojant pirmąjį raktą K_{s1}, pirštų atspaudui.

Jei naudojamas AES blokinis šifras, tai pradinio CBC-MAC duomenų pirštų atspaudo patikroje naudojamas atvirkštinis procesas, kurio metu gautasis pradinis CBC-MAC duomenų pirštų atspaudas pirmiausia iššifruojamas, o po to paskutiniuoju duomenų bloku naikinamas XOR užkodavimas ir einama atgal prie pirmojo duomenų bloko; jei pranešimas yra autentiškas ir vientisas, tai skaičiavimo rezultatas būna lygus iniciacijos vektoriui.

Lyginant su žinomais geriausiais ankstesniais sprendimais, pagrindinis šio atspariosios būsenos išsaugojimo sugedus su saugumu susietoms iš sudėtinių gedimams pirštų atspaudų formavimo metu atsparių modulių susidedančioms elektroninėms sistemoms būdo privalumas, numatytas šiame išradime, yra tai, kad naudojant šį būdą nereikia specialios techninės įrangos lyginimui ar balsavimui, kuri kitu atveju būtų reikalinga savojo atsparumo principui įgyvendinti. Šį procedūra

leidžia supaprastinti techninės įrangos konstrukciją, sumažinti išlaidas, taip pat padidinti su atsparumu susijusių elektroninių sistemų patikimumą.

TRUMPAS BRĖŽINIŲ FIGŪRŲ APRAŠYMAS

Pateiktose 1-9 figūrose (paveikslėliuose) yra šio išradimo, kuris vėliau bus aprašytas išsamiau, pritaikymo pavyzdžiai (įgyvendinimo variantai).
Dvejetainis *(n, k)* linijinis sisteminis blokų kodas sudarytas iš *k* informacijos bitų (informacijos dalis) ir $c = n-k$ kontrolinių bitų (kontrolinė dalis), kurie gautajame pranešime yra išdėstyti, kaip parodyta fig. 1 pateiktoje diagramoje.

Jei pradiniam CBC-MAC duomenų pirštų atspaudui CBC (šifruojamo bloko prirakinimo) metodu suformuoti naudojamas blokinis šifras, tai blokinis šifras modifikuojamas taip, kad CBC metodu gautas dalinis pirštų atspaudas skirtųsi nuo pradinio CBC-MAC duomenų pirštų atspaudo, o pradinis CBC-MAC duomenų pirštų atspaudas suformuojamas papildomomis dalinėmis dalinio pirštų atspaudo transformacijomis. Pradinis CBC-MAC skaičiavimo procesas panaudojant DES blokinį šifrą matomas fig. 2 pateiktoje diagramoje.

Toliau aprašomas CBC-MAC skaičiavimo metodas pagrįstas faktu, kad įvesties perstatos IP inversija DES blokiniam šifrui nėra žinoma jokiame įrenginyje, todėl teisingam rezultatui pasiekti reikia sąveikos tarp įrenginių porų, kurios sukurs reikiamą transformaciją sąveikaudamos tarpusavyje, kaip matyti fig. 3 . Pradinė DES blokinio šifro skaičiavimo diagrama pateikta fig. 4 . Kaip ir DES, AES blokinis šifras taip pat vykdomas raundais, kaip parodyta fig. 5, vaizduojančiame AES blokinio šifro skaičiavimo struktūrą.

Priklausomai nuo rakto ilgio (128, 192 ir 256 bitų), vykdomas atitinkamas ciklų kiekis (Nr = 10, 12 ir 14 raundų). Prieš pirmąjį, o po to po kiekvieno raundo, išplėsto rakto (kodo) atitinkamai daliai yra taikoma operacija XOR, po kurios apdorotas kodas įgauna statuso informacijos vertę. Kadangi CBC-MAC skaičiavimas taip pat pagrįstas operacija XOR, galima pasinaudoti šios operacijos komutatyvumu ir pertvarkyti CBC-MAC skaičiavimą taip, kad išplėsto rakto paskutiniajam 16 B iš anksto būtų taikoma operacija XOR su rakto pirmuoju 16B. Skaičiavimo pokytis parodytas fig. 6 (pradinis) bei fig. 7 (naujas).

Kai naudojamas DES blokinis šifras, pradinio CBC-MAC duomenų pirštų atspaudo patikrai gavus taip pat galima pasitelkti procesą, kuriame nenaudojamas jo atkūrimas (kuris yra paprastai rekomenduojamas metodas). Šis procesas pagrįstas apgrąžine procedūra, kuomet formuojamas pradinis CBC-MAC duomenų pirštų atspaudas panaudojant tris vienas nuo kito besiskiriančius raktus. Gautoje telegramoje reikia iššifruoti (D) CBC-MAC panaudojant trečiąjį raktą K_{s3}, tuomet užšifruoti (E) panaudojant antrąjį raktą K_{s2}, tuomet įsitikinti, kad rezultatas sutampa su pranešimo, sukurto panaudojant pirmąjį raktą K_{s1}, pirštų atspaudu (žr. fig. 8).
Toliau fig. 9 pateiktoje diagramoje vaizduojama galiojančio pranešimo pirštų atspaudo formavimo sistema jo vientisumui ir autentiškumui patikrinti, o tam visuomet reikia būtent dviejų įrenginių sąveikos.

TINKAMIAUSI ĮGYVENDINIMO VARIANTAI

Sudėtinis su geležinkelių sauga susijusių elektroninių sistemų atsparumas gedimams reiškia principą, įgalinantį išlaikyti jų saugumą, kai atsparumo funkciją vykdo daugiau nei vienas įrenginys sąveikoje su kitais nepriklausomais įrenginiais. Pavyzdžiui, jei nepriklausomi įrenginiai sprendimus dėl savo funkcijų vykdymo priima daugumos principu, t.y., du įrenginiai iš dviejų, du iš trijų, trys iš penkių ir t.t.

Toliau esančiame tekste su geležinkelių saugumu susietų, iš sudėtinių gedimams atsparių modulių susidedančių elektroninių sistemų išsaugojimo būdas pirštų atspaudų formavimo metu bus aprašytas analizuojant atvejus, kai yra linijiniai kodai ir DES (duomenų šifravimo standarto) ir AES (pažangiojo šifravimo standarto) blokiniai šifrai, kurie formuoja pradinį CBC-MAC duomenų pirštų atspaudą CBC (šifruojamo bloko prirakinimo) būdu ir modifikuoja blokinį šifrą taip, kad gautasis dalinis CBC metodo pirštų atspaudas skirtųsi nuo pradinio CBC-MAC duomenų pirštų atspaudo, o pradinis CBC-MAC duomenų pirštų atspaudas būtų suformuotas papildomomis dalinėmis gautojo dalinio pirštų atspaudo transformacijomis. Šis pirštų atspaudas yra funkcijos, iš kurios duotieji pradiniai duomenys kuria būdingųjų duomenų imtį pradiniams duomenims apibrėžtojo konkrečiojo redukavimo būdu, rezultatas. Šio pirštų atspaudo paskirtis yra, pavyzdžiui, patikrinti duomenų vientisumą ar jų autentiškumą.

Linijinis kodas apibrėžiamas generuojančiąja matrica, aprašant pradinių duomenų transformavimą į pirštų atspaudą. Kaip jau minėta, pirštų atspaudai yra funkcijos, kuri iš duotųjų pradinių duomenų sukuria būdingųjų duomenų imtį pradiniams duomenims apibrėžtojo konkrečiojo redukavimo būdu ir, pavyzdžiui, duomenų vientisumo patikrai, rezultatas. Tolesnėse pastraipose nagrinėsime dvejetainį *(n, k)* linijinį sisteminį blokinį kodą, sudarytą iš *k* informacijos bitų (informacijos dalis) ir $c = n\text{-}k$ kontrolinių bitų (kontrolinė dalis), kurie gautajame pranešime yra išdėstyti, kaip parodyta fig. 1 pateiktoje diagramoje.

Dvejetainis *(n, k)* linijinis (blokinis) sisteminis kodas yra išsamiai apibūdintas generuojančiąja toliau nurodytos formos dvejetaine matrica. Kiekviena ***c*** bitų vektorius eilutė B_i yra atitinkamas indėlis į kontrolinę dalį, jei pranešimo bitas *i* nėra nulinis.

$$G = [E, B] = \begin{bmatrix} 1 & 0 & \cdots & 0 & B_1 \\ 0 & 1 & \cdots & 0 & B_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & B_n \end{bmatrix} \qquad M = [E, BP] = \begin{bmatrix} 1 & 0 & \cdots & 0 & B_1P \\ 0 & 1 & \cdots & 0 & B_2P \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & B_nP \end{bmatrix}$$

Jei reikiama *P* perstata atliekama su *B* matricos B_i eilutės bitais, tai naujoji generuojančioji *M* matrica suformuoja pirštų atspaudą, kuriame bitai atitinkamai sumaišyti. Tad gautasis dalinis pirštų atspaudas yra *M* matricos suformuojamas tokiu būdu, kad jis yra pradinio pirštų atspaudo perstata, kurią nulemia *P* perstatos matrica. Kodavimo teorijos požiūriu tai šiuo atveju yra ekvivalentiškas linijinis kodas. Tuomet sisteminio dvejetainio kodo dauginimas generuojančiąja *M* matrica reiškia XOR operacijos taikymą B_i vektorių pridėjimui prie kontrolinės dalies. Taigi iš generuojančiosios *M* matricos skaičiavimui tereikia palikti *BP* matricą. Įrenginių sąveikai reikiamos *P* perstatos yra dalis informacijos duomenų struktūroje, kuri identifikuojama kaip pakartotinės paleisties žymė. Darbo su pakartotinės paleisties žyme (atsparumui aktualia informacija) būdai išsamiai aprašyti CZ 298373 patento dokumente.

Kadangi visi cikliniai kodai yra linijiniai, aukščiau aprašytą procedūrą galima naudoti ir visiems cikliniams kodams, sukurtiems ant antrosios charakteristikos ($GF(2^m)$) algebrinių kūnų. Visi šie kodai gali būti suprantami kaip dvejetainiai linijiniai kodai. Į šią ciklinių kodų grupę įeina visi šiuo metu priimti geležinkelių saugos įrenginių aktualių programų atsparumo kodai.

Jei pradiniam CBC-MAC duomenų pirštų atspaudui CBC (šifruojamo bloko prirakinimo) metodu suformuoti naudojamas blokinis šifras, tai blokinis šifras modifikuojamas taip, kad CBC metodu gautas dalinis pirštų atspaudas skirtųsi nuo pradinio CBC-MAC duomenų pirštų atspaudo, o pradinis CBC-MAC duomenų pirštų atspaudas suformuojamas papildomomis dalinėmis dalinio pirštų atspaudo transformacijomis.

Pradinį CBC-MAC skaičiavimo procesą panaudojant DES blokinį šifrą galima pamatyti fig. 2 pateiktoje diagramoje.

Pradinio CBC-MAC duomenų pirštų atspaudo skaičiavimas pradedamas XOR operaciją taikant pirmajam 64 bitų duomenų blokui su iniciacijos vektoriumi. DES (duomenų šifravimo standarto) blokiniai šifrai su Ks_1 raktu panaudojami dirbant su rezultatu, kuomet įvesties perstata pirmiausia naudojama DES skaičiavime, o po paties šifravimo proceso panaudojimo pasitelkiama apgrąžinė perstata. Papildomas 64 bitų duomenų blokas pridedamas prie gauto rezultato taikant operaciją XOR ir skaičiavimas tęsiasi panašiai. Jei į DES algoritmą įeinanti perstata išskaidoma į faktorius prieš XOR operaciją, bus gautas procesas, kuriame vienos perstatos (apgrąžinės perstatos) skaičiavimas praleidžiamas kiekviename žingsnyje. Apgrąžinė perstata panaudojama tik kartą, skaičiavimo pabaigoje.

Toliau aprašomas CBC-MAC skaičiavimo metodas yra grindžiamas tuo, kad įvesties perstatos IP DES blokiniam šifrui apgrąža nėra žinoma nė viename įrenginyje ir todėl teisingam rezultatui pasiekti reikalinga sąveika tarp įrenginių porų, kurios abipusės sąveikos metu sukurs reikiamą transformaciją, kaip parodyta fig. 3 . Pradinė DES blokinio šifro skaičiavimo diagrama parodyta fig. 4.

AES (pažangiojo šifravimo standarto) blokinio šifro skaičiavimo (užšifravimo ir iššifravimo) schema pasižymi keliais esminiais skirtumais lyginant su DES blokinio šifro atveju. Pirmasis skirtumas yra tai, kad užšifravimas ir iššifravimas yra specializuotos nesukeičiamos procedūros. Kadangi CBC-MAC kūrimui reikalinga tik užšifravimo procedūra, tolesnis aprašymas tegali apsiriboti šios procedūros modifikavimu, kad atitiktų sudėtinio atsparumo gedimams reikmes. Kitas skirtumas tarp AES ir DES yra tai, kad AES nenaudojamos jokios įvesties ir išvesties perstatos. Įdėjus tam tikrų pastangų perstatas galima įterpti į AES užšifravimo procedūrą, tačiau dėl to padidėja skaičiavimo galios poreikis. Būtent todėl geriau modifikuoti AES skaičiavimą taip, kad joks tarpinis rezultatas nebūtų naudojamu pirštų atspaudu, o reikiamas perstatas įterpti tik į galutinę skaičiavimo procedūrą.

Kaip ir DES, AES blokinis šifras irgi vykdomas raundais (žr. fig. 5, kuri parodyta AES blokinio šifro skaičiavimo sandara). Priklausomai nuo rakto ilgio (128, 192 ir 256 bitų), vykdomas atitinkamas ciklų kiekis (Nr = 10, 12 ir 14 raundų). Prieš pirmąjį, o po to po kiekvieno raundo, išplėsto rakto atitinkamai daliai yra taikoma operacija XOR, po kurios apdorotas kodas įgauna statuso informacijos vertę. Kadangi CBC-MAC skaičiavimas taip pat pagrįstas operacija XOR, galima pasinaudoti šios operacijos komutatyvumu ir pertvarkyti CBC-MAC skaičiavimą taip, kad išplėsto rakto paskutiniajai 16 B iš anksto būtų taikoma operacija XOR su rakto pirmaja 16 B. Skaičiavimo pokytis parodytas fig. 6 (pradinis) bei fig. 7 (naujas).

Skirtingai nei pradiniame skaičiavime (žr. fig. 6), paskutinė ir pirma išplėsto rakto dalys visuomet taikomos vienu metu po paskutinio raundo. Dėl to rezultatą skaičiavimo pabaigoje visuomet modifikuoja rakto pirmoji 16 B. Šiam rezultatui padaromos reikiamos perstatos, o tuomet perstatyta rakto dalis pritaikoma perstatytam tarpiniam rezultatui. Tokiu būdu gaunamas reikiamas gautasis dalinis pirštų atspaudas, jis bus užbaigtas taip pat, kaip kitais nurodytų įrenginių sąveikos atvejais.

Diagramoje „Nauja skaičiavimo schema“ (fig. 7) nurodytą skaičiavimo procedūrą galima paspartinti operaciją XOR taikant pirmajam raktui, po kurios raktą išplečiant jis tampa paskutiniojo raundo raktu. Dėl šios modifikacijos tolesniuose skaičiavimuose pradedant antruoju bloku, praleidžiamas vienas rakto taikymas prieš

pirmąjį raundą. Tokiu būdu visas CBC-MAC skaičiavimas padalijamas į tris dalis. Pradinėje dalyje pirmoji išplėsto rakto dalis (t.y., slapto rakto pirmoji 16 B) panaudojama prieš pirmąjį raundą, o po to – kiekviena papildoma atitinkama dalis po kiekvieno raundo.

Pirmoji išplėsto rakto dalis pakartotiniame skaičiavime nebenaudojama, o kitos dalys visuomet panaudojamos tik po kiekvieno raundo. Galutinėje modifikacijoje rezultatas perstatomas ir modifikuojamas perstatyta pirmąja išplėsto rakto dalimi.

Pagrindinis techninio atsparumo vykdant pirštų atspaudų patikrą principas grindžiamas tuo, kad patikros proceso metu nėra suformuojamas teisingas pirštų atspaudas. Taigi neleidžiama jokia patikros procedūra, kurioje naudojamas pirštų atspaudo suformavimas iš naujo. Tokiu procedūriniu patikrinimu būtų galima lengvai piktnaudžiauti ir įgalinti pirštų atspaudo gavėją ir jo teisingumo tikrintoją dėl gedimo patiems suformuoti tokį pirštų atspaudą.

Aciklinių linijinių kodų atveju galima eiti taip: pasitelkiant anksčiau minėta *M* matricą pirmiausia suformuojamas perstatytas pirštų atspaudas, kuris po to palyginamas su gautuoju pirštų atspaudu, kuriam pritaikoma apgrąžinė perstata, sukurta sąveikaujant reikiamam įrenginių kiekiui. Šį procesą taip pat reikia naudoti cikliniams kodams, jei atitinkamo generuojančiojo daugianario negalima suskaidyti į naudingą veiksnių sistemą. Šio tipo linijinis atsparumo kodas kol kas niekur nebuvo taikytas.

Jei yra daugianarių sistema (patikros daugianariai), kurios mažiausias bendras kartotinis lygus generuojančiajam ciklinio atsparumo kodo daugianariui, tai pirštų atspaudo patikros, vykdomos generuojančiojo daugianario, procesą galima pakeisti patikros daugianarių patikrinimu. Ši procedūra išsamiai aprašyta CZ 296129 patento dokumente.

Pradinio CBC-MAC duomenų pirštų atspaudo patikrai kai gavus naudojamas DES blokinis šifras taip pat galima panaudoti procesą, į kurį neįeina jo suformavimas iš naujo (o tai yra dažniausiai rekomenduojamas būdas). Šis procesas pagrįstas apgrąžine procedūra, naudojama kai formuojamas pradinis CBC-MAC duomenų

pirštų atspaudas panaudojant tris skirtingus raktus. Iš gautos telegramos reikia iššifruoti (D) CBC-MAC panaudojant trečiąjį raktą K_{s3}, tuomet užšifruoti (E) panaudojant antrąjį raktą K_{s2}, o po to patikrinti, ar rezultatas atitinka pranešimo, sukurto panaudojant pirmąjį raktą K_{s1}, pirštų atspaudą (fig. 8).

Lyginant su ankstesnėje pastraipoje aprašyta procedūra, ši patikrinimo procedūra turi kelis pranašumus. Gautojo pranešimo vientisumo ir autentiškumo patikrai įrenginių sąveika nėra reikalinga, tačiau ji reikalinga jo suformavimui.

Pradinio CBC-MAC duomenų pirštų atspaudo patikrai kai gavus naudojamas AES blokinis šifras galima naudoti procesą, panašų į aprašytąjį ankstesnėje pastraipoje. Iš gautosios telegramos reikia iššifruoti bloką su pradiniu CBC-MAC duomenų pirštų atspaudu tam panaudojant slaptą raktą, po to vykdyti apgrąžinį procesą (paskutinio duomenų bloko XOR užkodavimo naikinimas, ...) iki atkuriamas iniciacijos vektorius, nuo kurio pradedamas pradinio CBC-MAC duomenų pirštų atspaudo skaičiavimas. Jei bus gauta sutartoji reikšmė, tai reikš, kad gautas pranešimas yra vientisas ir autentiškas. Kadangi AES blokinio šifro iššifravimo procedūrą galima neribotai naudoti viename įrenginyje, ši patikros procedūra įgyvendinama nedalyvaujant papildomiems įrenginiams.

Patikrai galima panaudoti ir nebaigtą pradinio CBC-MAC duomenų pirštų atspaudo konstravimo ant gauto pranešimo duomenų procesą. Jei rezultatui prieš galutinę pradinio CBC-MAC duomenų pirštų atspaudo konstravimo modifikaciją pritaikoma XOR operacija panaudojant gautą pradinį CBC-MAC duomenų pirštų atspaudą, tai reikia gauti panaudoto slaptojo kodo pirmąją 16 B, kad išeitų vientisas autentiškas pranešimas.

Fig. 9 esanti diagrama vaizduoja galiojančio pranešimo pirštų atspaudo formavimo sistemą, kuri leistų patikrinti jo vientisumą ir autentiškumą, o tam visuomet reikia būtent dviejų įrenginių sąveikos.
(Pastaba: Kad įrenginys galėtų suformuoti pirštų atspaudą, būtinas mažiausiai dar vieno tos pačios instaliacijos įrenginio dalyvavimas. Kam to reikia, paaiškės iš toliau pateikto aprašymo).

„Dviejų iš trijų" sistemoje pirštų atspaudo formavime dalyvauja trys įrenginiai, nė viename iš jų nėra žinoma visa pirštų atspaudo formavimo procedūra, jis visada formuojamas vykstant priverstinei dviejų iš trijų įrenginių sąveikai. Pasinaudojant sukurto u pranešimo duomenimis (paveikslėlyje pažymėta kaip DUOMENŲ laukas), F(u) pirštų atspaudas suformuojamas toliau aprašytu būdu, kaip pavaizduota paveikslėlyje.

1. Panaudodamas F_{PAIC} funkciją kiekvienas iš trijų įrenginių (A, B, C) suformuoja gautąjį dalinį pirštų atspaudą (F) iš duomenų vientisumo patikrai, vadinamai PAIC (pirminės autorizacijos vientisumo patikra, angl. Primary Authorisation Integrity Check). F_{PAIC} funkcija suformuoja gautąjį dalinį pirštų atspaudą, kuris perstatomas panaudojant P_{PAIC} perstatą, kad nesuformuotų galiojančio pranešimo su tais duomenimis; t.y., tai yra sudėtinė funkcija $F_{PAIC} = P_{PAIC} \circ F$. F_{PAIC} funkcija visuose trijuose įrenginiuose yra tokia pati ir turi būti įgyvendinta, kad nesėkmingai ją vykdant nebūtų galima suformuoti galiojantį pirštų atspaudą $\mathbf{F}(u)$. Taigi, neįmanoma pirma atlikti **F** funkciją, o po to P_{PAIC} perstatą; sudėtinė F_{PAIC} funkcija turi būti neskaidoma įrenginyje.
2. A įrenginys atlieka duomenų lauko apdorojimą panaudojant PAIC funkciją P_{AB1} ir taip sukuria antrinės autorizacijos pirštų atspaudą $SAIC_{AB}$ (antrinės autorizacijos vientisumo patikra, angl. Secondary Authorisation Integrity Check), kuris yra dalinė gautojo dalinio pirštų atspaudo transformacija – ši funkcija atliks PAIC lauko, kuris sistemoje yra unikalus, bitų perstatą; minėtą perstatą geba atlikti tik A įrenginys ir ją galima panaudoti tik sąveikai su B įrenginiu. Tuo pačiu metu P_{AC1} perstata naudojama antrajam antrinės autorizacijos pirštų atspaudui $SAIC_{AC}$, skirtam sąveikai su C įrenginiu, suformuoti.
3. Tuo pačiu metu B įrenginyje naudojamos P_{BA1} ir P_{BC1} perstatos, kad iš PAIC lauko, skirto sąveikai su A ir C įrenginiais, būtų suformuoti antrinės autorizacijos pirštų atspaudai $SAIC_{BA}$ ir $SAIC_{BC}$.
4. Tuo pačiu metu C įrenginyje naudojamos P_{CA1} and P_{CB1} perstatos, kad iš PAIC lauko, skirto sąveikai su A ir B įrenginiais, būtų suformuoti antrinės autorizacijos pirštų atspaudai $SAIC_{CA}$ ir $SAIC_{CB}$.
5. Kiekviena P_{XY1} perstata (kurioje X ir Y gali turėti reikšmes A, B arba C) sistemoje yra unikali; žinoma tik X įrenginiui ir ją galima panaudoti tik sąveikai su įrenginiu Y.

6. Po to įvyksta antrinių pirštų atspaudų (gautojo dalinio pirštų atspaudo dalinių transformacijų) mainai tarp įrenginių: A įrenginys siunčia pirštų atspaudą $SAIC_{AB}$ į B įrenginį, o pirštų atspaudą $SAIC_{AC}$ į C įrenginį, B įrenginys siunčia pirštų atspaudą $SAIC_{BA}$ į A įrenginį, o pirštų atspaudą $SAIC_{BC}$ į C įrenginį, galiausiai C įrenginys pirštų atspaudą $SAIC_{CA}$ siunčia į A įrenginį, o pirštų atspaudą $SAIC_{CB}$ į B įrenginį (žr. paveikslėlį).
7. A įrenginyje apdorojamas antrinės autorizacijos pirštų atspaudas $SAIC_{BA}$ (kurį jis gavo iš B įrenginio) pasinaudojant P_{BA2} perstata, kuris suformuoja galutinės autorizacijos pirštų atspaudą $FAIC_{BA}$. Tuo pačiu metu P_{CA2} perstata taikoma $SAIC_{CA}$ autorizacijos pirštų atspaudui (gautam iš C įrenginio) ir suformuoja galutinės autorizacijos pirštų atspaudą $FAIC_{CA}$.
8. Tuo pačiu metu B įrenginyje naudojama P_{AB2} perstata, kad iš antrinės autorizacijos pirštų atspaudo $SAIC_{AB}$ (gauto iš A įrenginio) būtų sukurtas galutinės autorizacijos pirštų atspaudas $FAIC_{AB}$, taip pat P_{CB2} perstata, kad iš antrinės autorizacijos pirštų atspaudo $SAIC_{CB}$ (gauto iš C įrenginio) būtų sukurtas galutinės autorizacijos pirštų atspaudas $FAIC_{CB}$.
9. Galiausiai C įrenginyje naudojama P_{AC2} perstata, kad iš antrinės autorizacijos pirštų atspaudo $SAIC_{AC}$ (gauto iš A įrenginio) būtų sukurtas galutinės autorizacijos pirštų atspaudas $FAIC_{AC}$, taip pat P_{BC2} perstata, kad iš antrinės autorizacijos pirštų atspaudo $SAIC_{BC}$ (gauto iš B įrenginio) būtų sukurtas galutinės autorizacijos pirštų atspaudas $FAIC_{BC}$.
10. Vėlgi, kiekviena P_{XY2} perstata (kuriose X ir Y gali turėti reikšmes A, B arba C) sistemoje yra unikali; žinoma tik Y įrenginiui ir ją galima panaudoti tik X įrenginio sukurto antrinio pirštų atspaudo apdorojimui.
11. P_{XY1} ir P_{XY2} perstatos (X ir Y gali turėti reikšmes A, B arba C) parenkamos taip, kad P_{XY1} ir P_{XY2} perstatų kompozicija sukurtų tą pačią perstatą kiekvienai X, Y porai, kuri yra P_{PAIC}^{-1} perstata, atvirkštinė P_{PAIC} perstatai (t.y., $P_{AB1} \circ P_{AB2} = P_{AC1} \circ P_{AC2} = \ldots = P_{CB1} \circ P_{CB2} = P_{PAIC}^{-1}$). Todėl jei visi įrenginiai veikia be sutrikimų, visi galutiniai pirštų atspaudai $FAIC_{XY}$ būna tokie patys. (Kadangi, pavyzdžiui, $FAIC_{AB} = P_{AB2}(P_{AB1}(F_{PAIC}(u)))) = P_{PAIC}^{-1}(P_{PAIC}(\mathbf{F}(u)) = \mathbf{F}(u)$.

Skirtingų įrenginių DUOMENŲ lauko abipusio atitikimo patikra atliekama prieš pirštų atspaudo skaičiavimo pradžią. Be to, prieš įtraukiant DUOMENŲ lauką į FAIC pirštų

atspaudą įrenginys patikrina, ar FAIC pirštų atspaudas atitinka jo teikiamus duomenis.

Šis išradimas tinka iš sudėtinių gedimams atsparių modulių susidedančių su sauga susijusių elektroninių sistemų atsparumo išsaugojimui, ypač taikomas geležinkelio sistemose pirštų atspaudų formavimo metu.

IŠRADIMO APIBRĖŽTIS

1. Su saugumu susietų, iš sudėtinių gedimams atsparių modulių susidedančių elektroninių sistemų išsaugojimo būdas, ypač taikomas geležinkelio sistemose pirštų atspaudų formavimo metu, kai ne mažiau kaip du įrenginiai kartu formuoja pirštų atspaudus, kadangi pavieniui nė vienas iš jų neleidžia suformuoti tokio pirštų atspaudo, **b e s i s k i r i a n t i s tuo, kad** pirštų atspaudų formavimo procesas išskaidomas į dalinių pirštų atspaudų formavimo sekas konkrečiame laikotarpyje, kurio rezultatas – pradinis pirštų atspaudas, o bent vienam iš sąveikaujančių įrenginių aptikus gedimą gedimo nepatyręs su sugedusiuoju sąveikaujantis įrenginys atsisako formuoti dalinį pirštų atspaudą, kas neleidžia po to suformuoti pradinio pirštų atspaudo.

2. Būdas pagal 1 punktą, **b e s i s k i r i a n t i s tuo, kad** linijinių kodų atveju, kai pirštų atspaudas formuojamas panaudojant generuojančiąją matricą, gautasis dalinis pirštų atspaudas formuojamas kaip pradinio pirštų atspaudo perstata, kurioje apgrąžinė perstata išskaidoma į dalines perstatas ir taip sukuriamos dalinės transformacijos, kurios iš gautojo dalinio pirštų atspaudo suformuos pradinį pirštų atspaudą.

3. Būdas pagal 1 punktą, **b e s i s k i r i a n t i s tuo, kad** jei pradiniam CBC-MAC duomenų pirštų atspaudui CBC (šifruojamo bloko prirakinimo) metodu suformuoti naudojamas blokinis šifras, tai blokinis šifras modifikuojamas taip, kad CBC metodu gautas dalinis pirštų atspaudas skirtųsi nuo pradinio CBC-MAC duomenų pirštų atspaudo, o pradinis CBC-MAC duomenų pirštų atspaudas suformuojamas papildomomis dalinėmis gauto dalinio pirštų atspaudo transformacijomis.

4. Būdas pagal 3 punktą, **b e s i s k i r i a n t i s tuo, kad** jei naudojamas DES (duomenų šifravimo standarto) blokinis šifras su pradinio duomenų bloko įvesties perstatos IP, šifravimo dalimi ir užšifruoto duomenų bloko apgrąžine išvesties perstata, tai ši apgrąžinė išvesties perstata išskaidoma į dalines perstatas, o tai sukuria dalines transformacijas pradinio pirštų atspaudo suformavimui iš gautojo dalinio pirštų atspaudo.

5. Būdas pagal 3 punktą, **b e s i s k i r i a n t i s tuo, kad** jei naudojamas AES (pažangiojo šifravimo standarto) blokinis šifras, kuris vykdomas skaičiuojant blokus (raundus) panaudojant specifinį raktą kiekvienam raundui, tai skirtingas raktas pridedamas prie užšifruotų duomenų iš pradinio duomenų bloko kiekviename raunde, o paskutinio raundo raktas pridedamas prie kito CBC metodo skaičiavimo žingsnio pirmojo raundo rakto, tai užtikrina skirtumą tarp gautojo dalinio pirštų atspaudo ir pradinio pirštų atspaudo; gautasis pirštų atspaudas tolesniu daliniu transformavimu pakeičiamas į tokią formą, kuri yra pradinio pirštų atspaudo perstata, o apgrąžinė perstata išskaidoma į dalines perstatas, kurios transformuoja dalinį pirštų atspaudą į pradinį pirštų atspaudą.

6. B8das pagal 2 punktą, **b e s i s k i r i a n t i s tuo, kad** jei naudojami linijiniai kodai, kai pirštų atspaudas formuojamas panaudojant generuojančiąją matricą, tai pirštų atspaudo patikra atliekama gautuoju daliniu pirštų atspaudu, kuris beklaidžiame autentiškame pranešime sutampa su gautuoju pirštų atspaudu, kuriam pritaikyta apgrąžinė perstata, o gaunamas įrenginiams sąveikaujant, kaip nurodyta 1 paraiškoje.

7. Būdas pagal 2 punktą, **b e s i s k i r i a n t i s tuo, kad** jei naudojama patikros daugianarių sistema, kurių mažiausias bendras kartotinis lygus generuojančiajam ciklinio saugos kodo daugianariui, tai šie patikros daugianariai naudojami vientisumui ir autentiškumui patikrinti.

8. Būdas pagal 4 punktą, **pasižymintis tuo, kad** jei naudojamas DES blokinis šifras, tai pradinio CBC-MAC duomenų pirštų atspaudo patikroje naudojamas atvirkštinis procesas trimis abipusiai skirtingais raktais (K_{s1}, K_{s2}, K_{s3}), kurio metu gautasis pradinis CBC-MAC duomenų pirštų atspaudas pirmiausia iššifruojamas panaudojant trečiąjį raktą K_{s3}, o tuomet užšifruojamas panaudojant antrąjį raktą K_{s2}; jei tikrinamas pirštų atspaudas yra autentiškas ir vientisas, tai šių operacijų rezultatas būna lygus pranešimo, sukurto panaudojant pirmąjį raktą K_{s1}, pirštų atspaudui.

9. Būdas pagal 5 punktą, **b e s i s k i r i a n t i s tuo, kad** jei naudojamas AES blokinis šifras, tai pradinio CBC-MAC duomenų pirštų atspaudo patikroje naudojamas atvirkštinis procesas, kurio metu gautasis pradinis CBC-MAC duomenų pirštų

atspaudas pirmiausia iššifruojamas, o po to paskutiniuoju duomenų bloku naikinamas XOR užkodavimas ir einama atgal prie pirmojo duomenų bloko; jei pranešimas yra autentiškas ir vientisas, tai skaičiavimo rezultatas būna lygus iniciacijos vektoriui.

10. Būdas pagal 1 punktą, **b e s i s k i r i a n t i s tuo, kad** atsparumo sistema, į kurią įeina įrenginiai, nurodyti 1 punkte, yra radijo ryšio blokų centras, skirtas traukinių valdymui radijo ryšiu.

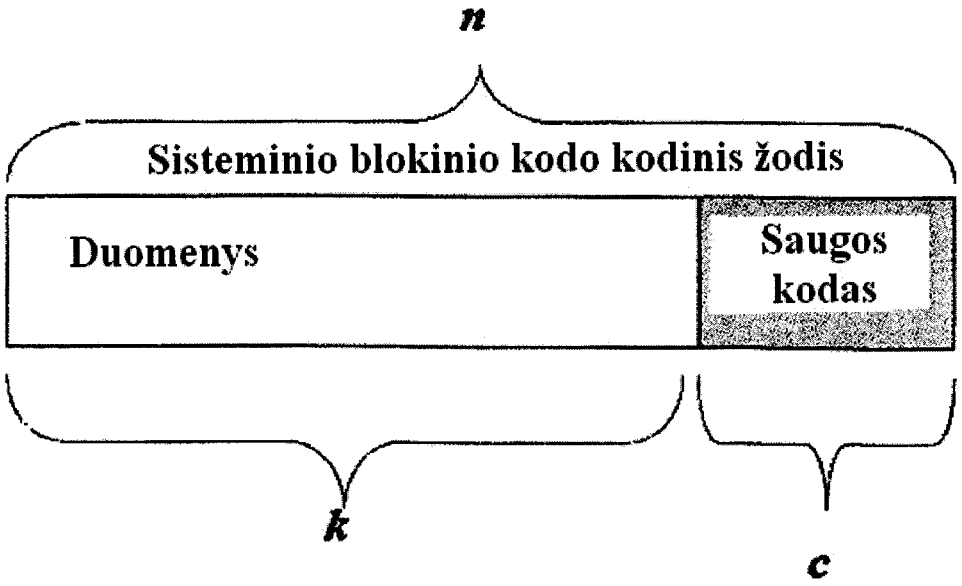

n
Sisteminio blokinio kodo kodinis žodis
Duomenys
Saugos kodas
k
c

Fig. 1

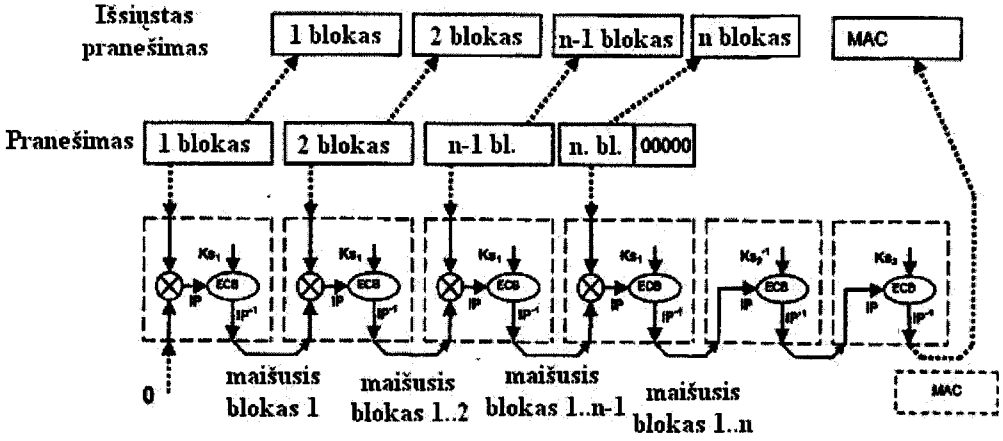

Išsiųstas pranešimas
1 blokas
2 blokas
n-1 blokas
n blokas
MAC
Pranešimas
1 blokas
2 blokas
n-1 bl.
n. bl.
00000
0
maišusis blokas 1
maišusis blokas 1..2
maišusis blokas 1..n-1
maišusis blokas 1..n
MAC

Fig. 2

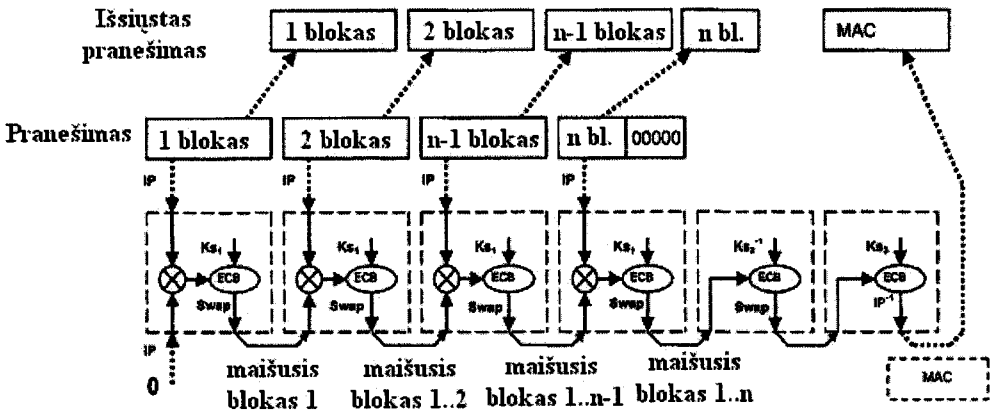

Išsiųstas pranešimas
1 blokas
2 blokas
n-1 blokas
n bl.
MAC
Pranešimas
1 blokas
2 blokas
n-1 blokas
n bl.
00000
IP
ECB
Swap
0
maišusis blokas 1
maišusis blokas 1..2
maišusis blokas 1..n-1
maišusis blokas 1..n
MAC

Fig. 3

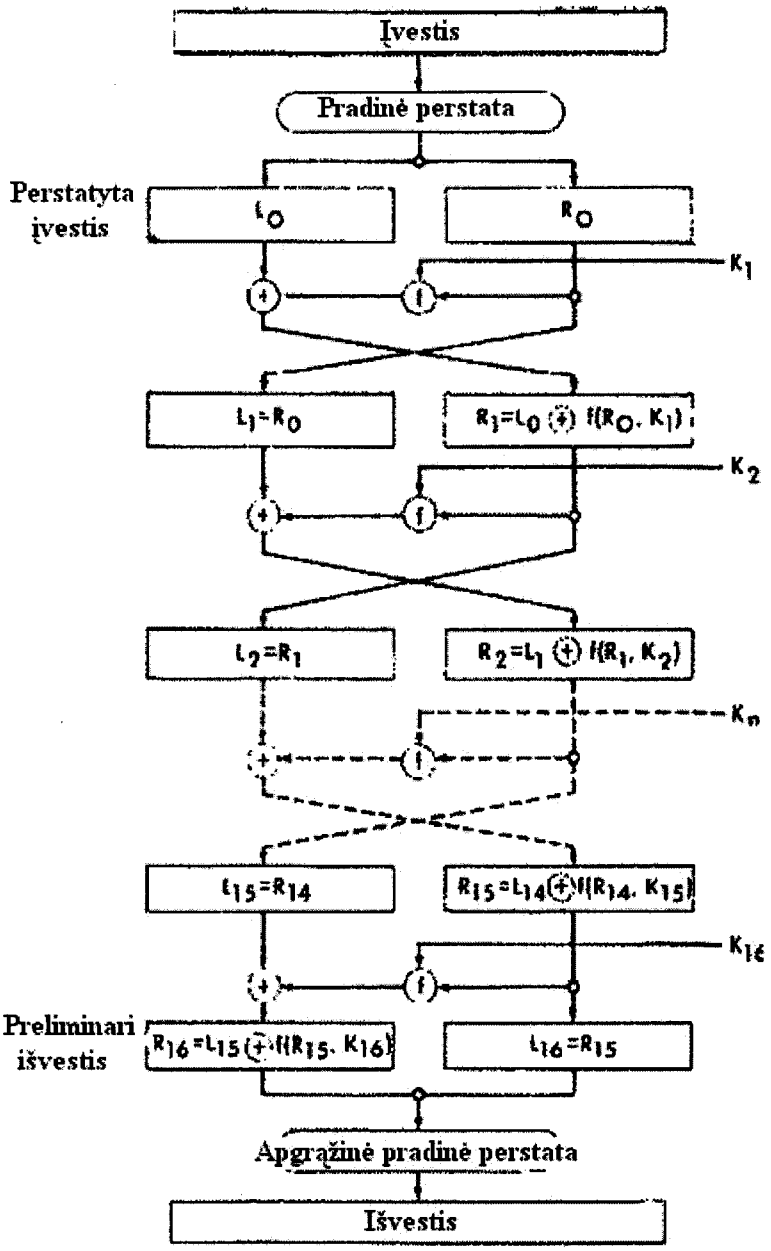

Įvestis
Pradinė perstata
Perstatyta įvestis
L_0
R_0
K_1
f
$L_1=R_0$
$R_1=L_0 \oplus f(R_0, K_1)$
K_2
$L_2=R_1$
$R_2=L_1 \oplus f(R_1, K_2)$
K_n
$L_{15}=R_{14}$
$R_{15}=L_{14} \oplus f(R_{14}, K_{15})$
K_{16}
Preliminari išvestis
$R_{16}=L_{15} \oplus f(R_{15}, K_{16})$
$L_{16}=R_{15}$
Apgrąžinė pradinė perstata
Išvestis

Fig. 4

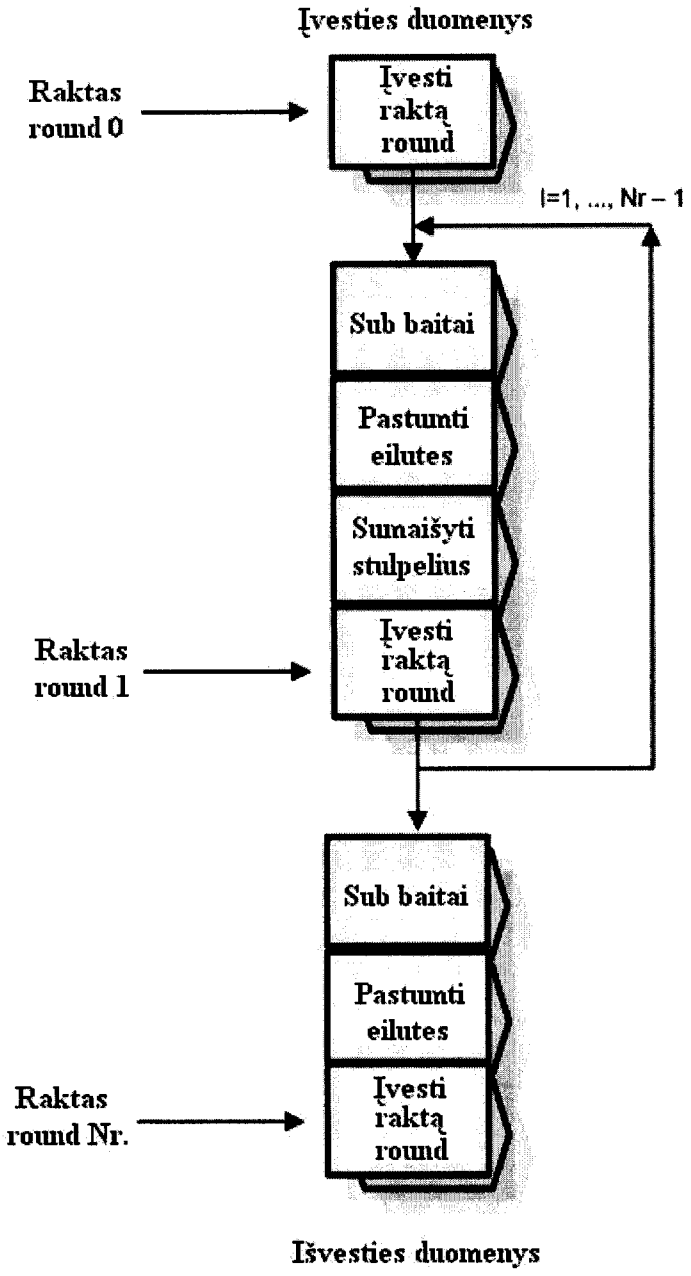

Įvesties duomenys
Raktas round 0
Įvesti raktą round
I=1, ..., Nr – 1
Sub baitai
Pastunti eilutes
Sumaišyti stulpelius
Raktas round 1
Įvesti raktą round
Sub baitai
Pastunti eilutes
Raktas round Nr.
Įvesti raktą round
Išvesties duomenys

Fig. 5

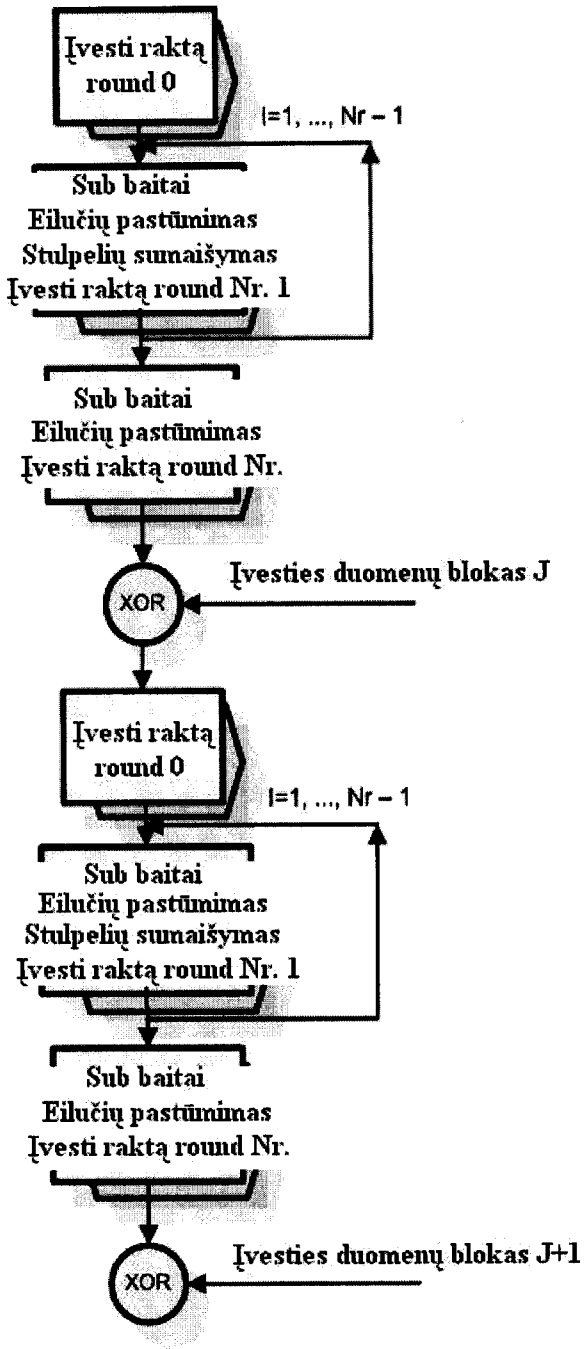

Įvesti raktą
round 0
I=1, ..., Nr – 1
Sub baitai
Eilučių pastūmimas
Stulpelių sumaišymas
Įvesti raktą round Nr. 1
Sub baitai
Eilučių pastūmimas
Įvesti raktą round Nr.
XOR
Įvesties duomenų blokas J
Įvesti raktą
round 0
I=1, ..., Nr – 1
Sub baitai
Eilučių pastūmimas
Stulpelių sumaišymas
Įvesti raktą round Nr. 1
Sub baitai
Eilučių pastūmimas
Įvesti raktą round Nr.
XOR
Įvesties duomenų blokas J+1

Fig. 6

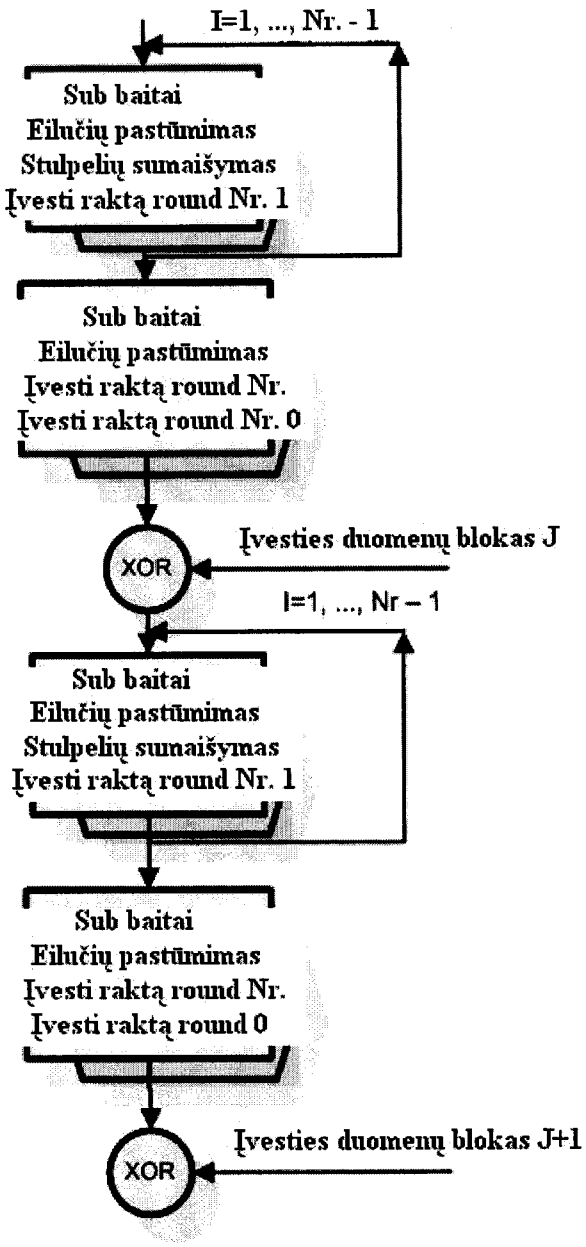

I=1, ..., Nr. - 1
Sub baitai
Eilučių pastūmimas
Stulpelių sumaišymas
Įvesti raktą round Nr. 1
Sub baitai
Eilučių pastūmimas
Įvesti raktą round Nr.
Įvesti raktą round Nr. 0
XOR
Įvesties duomenų blokas J
I=1, ..., Nr – 1
Sub baitai
Eilučių pastūmimas
Stulpelių sumaišymas
Įvesti raktą round Nr. 1
Sub baitai
Eilučių pastūmimas
Įvesti raktą round Nr.
Įvesti raktą round 0
XOR
Įvesties duomenų blokas J+1

Fig. 7

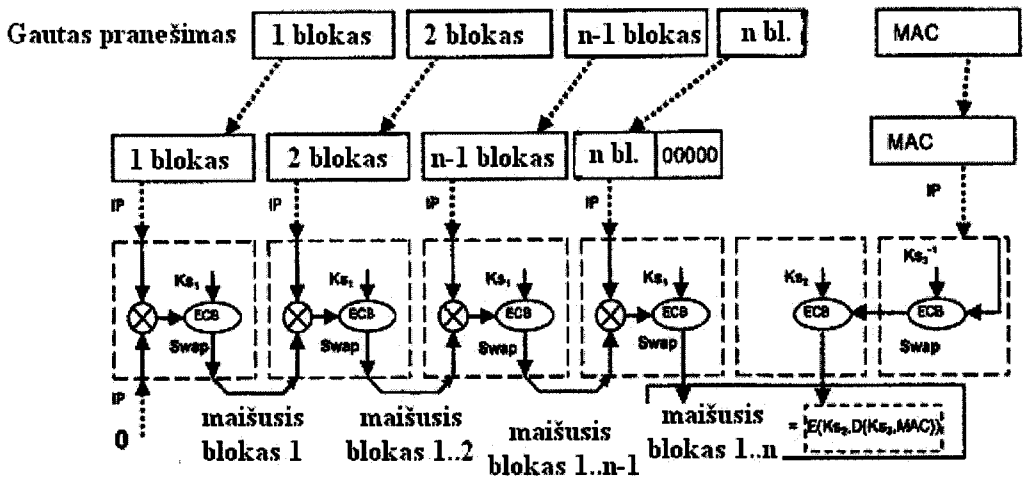
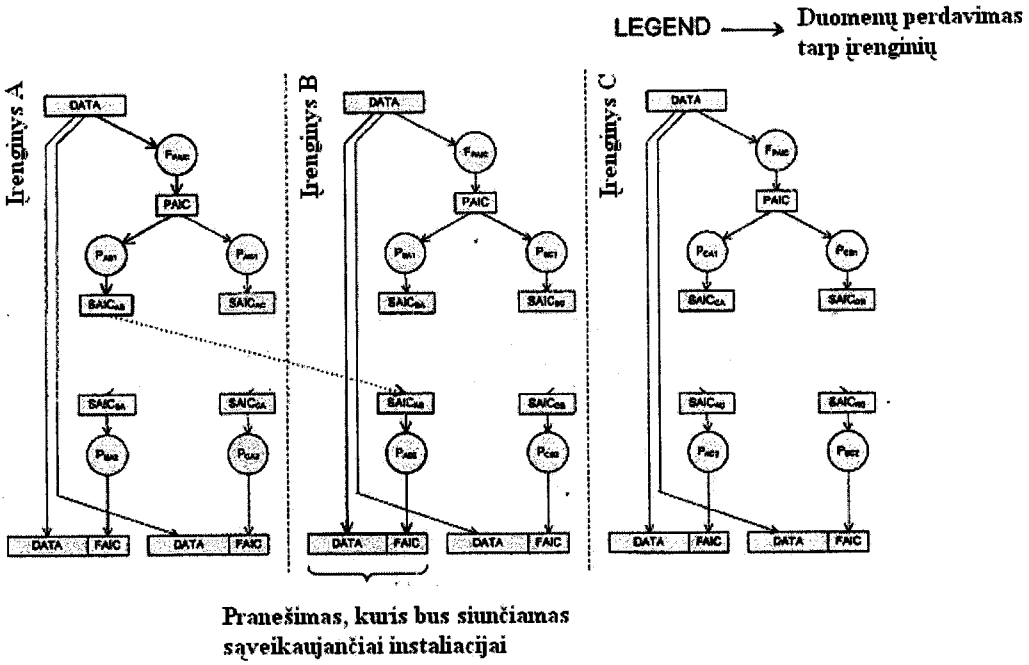

Gautas pranešimas
1 blokas
2 blokas
n-1 blokas
n bl.
MAC
1 blokas
2 blokas
n-1 blokas
n bl.
00000
MAC
IP
ECB
Swap
0
maišusis blokas 1
maišusis blokas 1..2
maišusis blokas 1..n-1
maišusis blokas 1..n

Fig. 8



Pirštų atspaudo kūrimas

Fig. 9