(19) Lietuvos Respublikos valstybinis patentų biuras

(10) **LT 6809 B**

(12) **PATENTO APRAŠYMAS**

(11) Patento numeris: **6809**

(51) Int. Cl. (2021.01): **G06N 3/00**

(21) Paraiškos numeris: **2020 540**

(22) Paraiškos padavimo data: **2020-07-27**

(41) Paraiškos paskelbimo data: **2021-02-25**

(45) Patento paskelbimo data: **2021-03-25**

(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: —

(72) Išradėjas:

Timofey MOCHALOV, RU

(73) Patento savininkas:

Timofey MOCHALOV, Kirova 18a-47, Sosensky, Kaluga, RU

(74) Patentinis patikėtinis/atstovas:

Jurga PETNIŪNAITĖ, AAA Law, A. Goštauto g. 40B, Verslo centras „Dvyniai", LT-03163 Vilnius, LT

LT 6809 B

(54) Pavadinimas:

Duomenų perdavimo lygiarangių tinkle (P2P) apsaugos būdas, naudojant neuroninę kriptografiją

(57) Referatas:

Duomenų šifravimo ir iššifravimo tinkle būdas, naudojant dirbtinį neuroninį tinklą, įdiegtą kiekviename tinklo mazge. Duomenų apsaugos elementai - šifravimo raktai, šifravimo algoritmai ir šifravimo maskavimai - sukuriami arba pasirenkami atitinkamai nauju ryšio tinkle atveju ir jokie duomenų apsaugos elementai neperduodami tinkle. Dirbtinis neuroninis tinklas mokosi blokų grandinėje, pridedant kiekvieną naują bloką prie blokų grandinės, ir yra naudojamas generuoti baigtinį šifravimo raktų rinkinį kiekviename mazge vienu metu. Tokie šifravimo raktai, šifravimo algoritmai ir šifravimo maskavimai yra susieti su kiekvienu mazgu neuroniniame tinkle ir paskui naudojami perduodamų duomenų iššifravimui.

IŠRADIMO SRITIS

Šis išradimas yra susijęs su kriptografijos būdu, ypač su kompiuteryje įdiegtu duomenų šifravimo ir iššifravimo būdu, naudojant dirbtinį neuroninį tinklą ir blokų grandinės duomenų struktūros saugumą.

TECHNIKOS LYGIS

Duomenų saugumas yra svarbiausias duomenų perdavimo sistemų rūpestis. Neuroninė kriptografija yra duomenų kodavimo ir dekodavimo būdas naudojant dirbtinį neuroninį tinklą. Dirbtiniai neuroniniai tinklai (toliau – DNT) yra gerai žinomi dėl savo gebėjimo selektyviai ištirti tam tikros problemos sprendimo erdvę. Ši savybė yra natūrali taikymo niša kriptovaliutų srityje. Tuo pačiu metu neuroniniai tinklai siūlo naują požiūrį į atakų šifravimo algoritmus, pagrįstus principu, kad bet kokią funkciją gali atkurti neuroninis tinklas, pasiteisinęs kaip galingas skaičiavimo įrankis, naudojant bet kokio kriptografinio algoritmo atvirkštinei funkcijai rasti. Neuroninė kriptografija paprastai grindžiama privačių raktų poros sukūrimu viešoje aplinkoje, naudojant neuroninius tinklus; blokų grandinės naudojimu šifravimo raktams maišos pavidalu saugoti arba kaupti DNT elementų blokų grandinėje. Paprastai neuroninė kriptografija nagrinėja „raktų mainų“ tarp dviejų neuroninių tinklų problemą, naudojant tarpusavio mokymosi koncepciją. Du tinklai keičiasi savo išėjimo duomenimis (bitais), o raktas tarp dviejų bendraujančių šalių galiausiai pateikiamas galutiniuose išmoktuose svoriuose, t.y. kai sakoma, kad abu tinklai yra sinchronizuoti. Neuroninės sinchronizacijos saugumui kyla pavojus, jei įsilaužėlis mokymosi metu gali sinchronizuoti veiksmus su viena iš dviejų šalių.

Dirbtinio neuroninio tinklo kriptografijos būdą straipsnyje „Neuroniniu tinklu paremta kriptografija“ aprašė Apdullah Yayık ir Yakup Kutlu 2014 m. gegužės mėn. „Neural Network World“, psl. 177-192, DOI: 10.14311/NNW.2014.24.011. Būdą sudaro du etapai. Pirmame etape sugeneruojami neuroninio tinklo pseudoatsitiktiniai skaičiai (NTPAS) ir rezultatų atsitiktinumas tiriamas, naudojant Nacionalinio standartinės technologijos instituto (NSTI) atsitiktinumo testus. Antrame etape, naudojant NTPAS, suprojektuojama neuroninio tinklo kriptosistema. Šioje kriptosistemoje duomenys, kurie yra užšifruoti netiesiniais būdais, yra iššifruojami dviem identiškais dirbtiniais neuroniniais tinklais. Naudojant pirmąjį neuroninį tinklą, netiesinis šifravimas modeliuojamas, naudojant santykių kūrimo funkciją. Užšifruoti

duomenys iššifruojami, naudojant antrąjį neuroninį tinklą, naudojant sprendimų priėmimo funkciją.

Blokų grandinės naudojimo kartu su dirbtiniu neuroniniu tinklu būdas yra aprašytas straipsnyje „Dirbtinio intelekto įgyvendinimas blokų grandinėje. Naudojimo atvejai ir būsimos programos“, Konstantinos Sgantzos, Ian Grigg, „Future Internet“ 2019, 11, 170; doi: 10.3390/fi11080170.

Pagrindiniai iki šiol pasiekto lygio trūkumai yra tai, kad neuroniniai tinklai yra naudojami arba šifravimo raktui sukurti, arba asimetrinei šifravimo raktų porai sukurti, arba šifravimo raktus vienokia ar kitokia forma saugoti blokų grandinėje.

Šis išradimas skirtas pašalinti aukščiau išvardintus trūkumus ir sukurti papildomus pranašumus, palyginti su ankstesniais būdais.

IŠRADIMO ESMĖ

Čia aprašytas išradimas yra duomenų šifravimo ir iššifravimo tinkle būdas, naudojant dirbtinį neuroninį tinklą, įdiegtą kiekviename tinklo mazge. Duomenų apsaugos elementai – šifravimo raktai, šifravimo algoritmai ir šifravimo užmaskavimas – sukuriami arba pasirenkami atitinkamai nauju ryšio tinkle atveju ir jokie duomenų apsaugos elementai tinkle neperduodami. Dirbtinis neuroninis tinklas mokosi, blokų grandinėje pridedant kiekvieną naują bloką prie blokų grandinės ir yra naudojamas generuoti baigtinį šifravimo raktų rinkinį kiekviename mazge vienu metu. Tokie šifravimo raktai, šifravimo algoritmai ir šifravimo užmaskavimas yra susieti su kiekvienu neuroninio tinklo mazgu ir po to naudojami perduodamų duomenų iššifravimui.

TRUMPAS BRĖŽINIŲ APRAŠYMAS

Išradimo, kuris yra naujas ir neakivaizdus srities specialistui, požymiai yra pateikti išradimo apibrėžtyje. Išradimas gali būti geriausiai suprantamas, remiantis šiuo išsamiu išradimo aprašymu, kuriame pateikiami pavyzdiniai išradimo variantai kartu su neribojančiais pavyzdžiais bei pridedamais brėžiniais, kuriuose:

1 pav. yra pavaizduota pirminio tinklo kliento identifikavimo schema. Kai klientas pirmą kartą prisijungia prie tinklo, jo kliento ID atsitiktinai sugeneruojamas ir saugomas blokų grandinėje, per pirmąją duomenų mainų tarp dviejų klientų sesiją keičiamasi identifikatoriais ir asmeninėmis paslaptimis, taip pat sesijos iniciatorius

sesijos pradžioje perduoda atsitiktinius baitus.

2 pav. yra pavaizduota perduodamų duomenų šifravimo schema, šifravimo algoritmo ir šifravimo rakto parinkimas kiekvienai duomenų perdavimo sesijai.

3 pav. yra pavaizduotas neuroninių tinklų sinchronizavimo ir perkvalifikavimo principas, norint pakeisti šifravimo algoritmų pasirinkimo logiką (naudojant apmokančius duomenis iš blokų grandinės tinklo), taip pat renkantis naują šifravimo raktų kūrimo būdą.

Toliau aprašomi tinkamiausi išradimo variantai su nuorodomis į brėžinius.

IŠSAMUS IŠRADIMO APRAŠYMAS

Siekiant išsamaus ir suprantamo išradimo įgyvendinimo aprašymo, yra pateikta daugybė specifinių detalių. Tačiau specialistas supras, kad šie pateikiami pavyzdžiai neriboja išradimo taikymo, kurį galima įgyvendinti be šių konkrečių instrukcijų. Norint išvengti klaidinimo, išsamiai nebuvo aprašyti gerai žinomi metodai, procedūros ir komponentai. Be to, šis aprašymas neturėtų būti laikomas išradimą ribojančiu pateiktais įgyvendinimo pavyzdžiais, o pavyzdžiai pateikti tik kaip galimi išradimo įgyvendinimo būdai.

Nors šiame išradimo aprašyme yra išvardinta daugybė požymių ir pranašumų, taip pat struktūrinės detalės ir ypatybės, aprašymas pateiktas kaip išradimo įgyvendinimo pavyzdys. Nenukrypstant nuo išradimo principų, gali būti keičiamos detalės, ypač forma, dydis ir išdėstymas, atsižvelgiant į plačiausiai suprantamas sąvokų ir apibrėžimų, vartojamų išradimo apibrėžtyje, reikšmes.

Trumpas terminų paaiškinimas:

Duomenys – paprastas tekstas bei kita stabilioje kompiuterio laikmenoje saugoma informacija.

Klientai – kompiuteriniai įrenginiai, pavyzdžiui, belaidžiai įrenginiai, kompiuterių procesoriai, jutikliai, kiti įrenginiai, galintys apdoroti duomenis.

Mazgai – tik klientai.

Siuntėjas ir gavėjas – kiekvienoje duomenų perdavimo sesijoje vienas kliento mazgas siunčia duomenis ir yra siuntėjas, ir bent vienas kliento mazgas gauna duomenis ir yra gavėjas.

Duomenų perdavimo sesija – laikotarpis, per kurį vienas kliento mazgas yra siuntėjas, o mažiausiai vienas kliento mazgas yra gavėjas, ir visi mazgai turi sinchronizuotus identifikavimo raktus.

Kliento ID – unikalus 256-512 bitų raktas, X509 sertifikatas, arba ir vienas, ir kitas.

Dirbtinis neuroninis tinklas (DNT) – informacijos apdorojimo ir modeliavimo sistema, imituojanti biologinių sistemų gebėjimo suprasti nežinomą procesą ar jo elgesį mokymąsi. Dirbtinis neuroninis tinklas yra daugelio labai paprastų procesorių (vienetų) tinklas, kurių kiekvienas gali turėti (nedaug) vietinės atminties. Įrenginiai yra sujungti vienkrypčiais ryšio kanalais, kurie perduoda skaitmeninius duomenis. Įrenginiai veikia tik su vietiniais duomenis ir įvestimis, kuriuos gauna per jungtis.

Blokų grandinė – pilnutinai pasidalijamas konsensuso registras, kuris yra visuotinai matomas visoms šalims, kai sandoris įrašomas į jį be jokios patikimos centrinės institucijos.

Simetrinis šifravimas – šifravimas naudojant simetrinį raktą, slaptas raktas bendrinamas tarp siuntėjo ir gavėjo. Žodis „simetrinis“ reiškia, kad tiek siuntėjas, tiek gavėjas naudoja tą patį raktą informacijai užšifruoti ir iššifruoti.

Asimetrinis šifravimas – neuroninio šifravimo ir iššifravimo būdas, kuris apima neuroninių tinklų naudojimą kartu su simetriniais šifravimo algoritmais kompiuteriniame tinkle. Pageidautina, kad kompiuterinis tinklas būtų blokų grandinės tipo kompiuterinis tinklas.

Šifravimo užmaskavimo būdai – kai paprastas tekstas užšifruojamas vienu šifravimo algoritmu su vienu simetriniu šifravimo raktu, o po to užšifruojamas kitu šifravimo algoritmu kitu simetriniu šifravimo raktu, atsitiktinai pridedant prie paprasto teksto atsitiktines šiukšles (neužšifruotus simbolius ar atsitiktinius baitus), prieš šifravimo procesą pridedant šiukšles (atsitiktinį bitų rinkinį skirtingose vietose) jau užšifruotuose duomenyse arba atskiruose blokuose, perkeliant šifravimo tekstą virš konkretaus vektoriaus ir kita.

Pagal vieną išradimo variantą, kompiuteriu įdiegtas neuroninės kriptografijos būdas duomenų perdavimui tinkle apsaugoti, naudojant sinchronizuotas DNT kopijas kiekviename mazge, pašalina duomenų apsaugos parametrų perkėlimą per tinklą. Tinklas yra interneto ar vietinis kompiuterių tinklas, apimantis mažiausiai du kliento

mazgus duomenims siųsti ir priimti, kur kiekvienas mazgas saugo DNT kopiją. Šiuo atveju duomenų perdavimas turi decentralizuotą tinklo tipo schemą, kuri gali veikti tiek internete, tiek vietiniame tinkle.

Pačioje kliento darbo tinkle pradžioje, automatiškai ir atsitiktinai, yra sukuriamas kliento ID, kuris yra saugomas blokų grandinėje. Pradėjus kontaktą tarp dviejų unikalių klientų, jie apsikeičia asmeniniais raktais raktų pavidalu arba užšifruotu pavidalu, naudodami QR kodą ar kitas parinktis, kurios bus tik identifikatoriai jų keitimosi duomenimis sesijose. Be to, sesijų tarp dviejų klientų pradžioje ryšio iniciatorius siunčia gavėjui atsitiktinį bitų rinkinį, kuris gali būti užšifruotas kaip atskiras blokas, QR kodas ar kitu duomenų eilutės formatu. 1 pav. parodyta tinklo identifikavimo schema, skirta nustatyti duomenų perdavimo sesiją tarp dviejų klientų.

Kiekviename tinklo mazge DNT sinchronizuojamas, naudojant kliento ID, privačius raktus, kuriais du klientai apsikeičia per pirmąjį kontaktą, ir atsitiktinius baitus, kuriuos ryšio iniciatorius perduoda duomenų perdavimo sesijos pradžioje, kad būtų suformuotas vienas raktų ir algoritmų, naudojamų tarp siuntėjo ir gavėjo, rinkinys. Kiekvienos duomenų perdavimo sesijos metu šifravimo raktai generuojami vienu metu visuose mazguose naudojant DNT, o šifravimo algoritmai ir supainiojimo procedūros pasirenkami vienu metu visuose DNT mazguose iš baigtinio šifravimo protokolų rinkinio.

Sukurtus šifravimo raktus, pasirinktus šifravimo algoritmus ir maskavimo procedūras DNT naudoja, šifruodamas ir iššifruodamas duomenis perdavimui tarp siuntėjo ir gavėjo mazgų, kaip parodyta 2 pav.

Vienas iš nuolat sichronizuojamo ir savaime besimokančio DNT, kuriam naudojamas savarankiškai identifikuojantis vartotojo raktas (kliento ID) ir blokų grandinės duomenys, skirti mokyti DNT, išpildymo variantų yra parodytas 3 pav. DNT perkvalifikavimas įvyksta, pridedant kiekvieną naują bloką blokų grandinėje prieš pradedant duomenų perdavimą. Atnaujinimo dažnumas arba naujų blokų atsiradimas blokų grandinėje priklauso nuo užduoties ir konkrečios tinklo struktūros. Tai gali būti kartą per savaitę, kartą per dieną arba kartą per valandą ir kitaip.

Pavyzdiniame decentralizuoto tinklo įgyvendinimo variante yra naudojamas „*viešosios blokų grandinės*“ arba „*viešo leidimo blokų grandinės*“ tipo grandinės, kur

kiekvienas klientas gali veikti kaip tinklo blokų grandinės mazgas. Kiekvienas kitas mazgas, siuntėjo mazgas ir bent vienas priimantis mazgas turi blokų grandinės duomenų kopijas. Kiekvienas tinklo elementas ar mazgas gali sukurti naujus blokus, o blokų grandinė atnaujinama, atsižvelgiant į naujų blokų atsiradimą. Kiekvieną kartą, kai blokų grandinė keičiasi, pridedant naują bloką ar tam tikrą skaičių blokų, DNT yra perkvalifikuojamas visuose mazguose ir visiems tinklo klientams, remiantis parametrais, kurie nustatomi, renkantis blokų grandinės tipą ir tinklo logiką. Duomenys iš blokų grandinės naudojami kaip įvestis, keičiant DNT svorį visuose mazguose.

Tinklo elementai yra visi klientai, galintys dirbti tinkle, blokų grandinės tinklo mazgai yra tie tinklo klientai, kurie gali sukurti blokų grandinės tinklo blokus.

Tolesniuose decentralizuoto tinklo pavyzdžiuose tinklo blokų kūrimo principas bus apibrėžtas pagal vieną iš dviejų schemų. Pirmuoju atveju tam tikras klientas sukurs naujus blokų grandinės tinklo blokus, atsižvelgiant į srautą ir iš nurodyto kliento perduodamus duomenis. Antruoju atveju rizika, kad vienas ar keli klientai, iš kurių kyla pavojus, gali visiškai užvaldyti tinklą (atitinka „51% išpuolio“), yra sumažinama, sumažinant neuroninio tinklo perkvalifikavimo greitį arba perkvalifikuojant neuroninį tinklą pagal prisijungimų skaičių ir kliento aktyvumą tinkle arba pagal tam tikrą skaičių blokų grandinės tinklo blokų.

Kliento identifikavimo kliento ID lygyje variantai gali būti įgyvendinami toliau aprašytais būdais. Pirma, pradinio kontakto metu du klientai prideda vienas kitą prie gavėjų ir keičiasi asmeniniais raktais. Tai gali būti vykdoma, pavyzdžiui, per tinklą perduodant duomenis, naudojant QR kodą, arba perkeliant raktus į kitą laikmeną ir atsisiunčiant juos atskirai į sistemą. Raktai yra unikalūs pradiniam dviejų klientų kontaktui ir vėliau bus naudojami kaip papildomi duomenys, mokant neuroninį tinklą ir šifruojant duomenų perdavimo sesijas kartu su kliento ID ir atsitiktiniais baitais.

Kliento ID yra unikalus kliento identifikatorius blokų grandinėje. Šie identifikatoriai gali ir turėtų būti sukurti automatiškai, remiantis tam tikrais parametrais ir kliento identifikatoriais, tokiais kaip slapyvardis, įrenginio identifikatorius, registracijos tinkle data ir laikas ir kt. Kliento identifikatorius (kliento ID) gali būti duomenų rinkinio dalis, skirta mokymuisi šifravimo proceso metu ar patekti į neuroninio tinklo įvesties neuronus, arba būti naudojamas tik kaip konkretaus kliento identifikatorius visiems kitiems blokų grandinės tinklo klientams. Be to, toks

identifikatorius supaprastina blokų grandinės tinklo valdymą, kad būtų galima sekti galimas grėsmes, iš anksto perspėti apie galimą „51% išpuolio“ ar jo ekvivalento grėsmę, taip pat supaprastinamas bendravimas tarp tinklo klientų.

Kitame įgyvendinimo variante kiekviename mazge DNT sinchronizuojami du kartus. Pirmasis DNT sinchronizavimas vyksta, pridedant naują bloką prie bloko grandinės, kuri yra sukonfigūruota kiekvienai sistemai atskirai. Antra, pakartotinis sinchronizavimas vyksta su perdavimu, naudojant kliento ID ir šifravimo raktus, gautus per pirmąjį kontaktą tarp dviejų klientų, ir atsitiktinius baitus tarp siuntėjo ir gavėjo. Kliento ID, be kitų duomenų, yra įtrauktas į duomenų rinkinį, kuris tiekiamas įvestiems neuronams naujos duomenų perdavimo sesijos metu. DNT kiekviename tinklo mazge nuolat keičia bendrą šifravimo logiką, nuolat mokantis savarankiškai, naudojant save identifikuojantį vartotojo raktą (kliento ID) ir blokų grandinės duomenis. Savarankiškas mokymasis ir tinklo sinchronizavimas grindžiami naujais blokų grandinės blokais, tam tikras tinklo klientas sesijos pradžioje sinchronizuojamas naudojant atsitiktinius duomenis, perduodamus iš kliento siuntėjo (atsitiktinius baitus) raktus, gautus per pirmąjį kontaktą tarp dviejų klientų ir priimančio mazgo kliento identifikatorių iš blokų grandinės tinklo.

Įgyvendinimo variante, kuriame naudojama sinchronizacija, DNT pasirenka šifravimo algoritmą ir šifravimo maskavimą, taip pat šifravimo raktą siuntėjo ir gavėjo pusėje tuo pačiu metu. Tinkamiausiame variante naudojami simetriniai šifravimo algoritmai, tokie kaip *AES 256, 3DES, ChaCha, Salsa20, Blowfish, Twofish, DES, Kuznechik*. Kitame įgyvendinimo variante patys šifravimo algoritmai ir įvairios užmaskavimo schemos arba vieno šifravimo algoritmo naudojimas, yra įgyvendinami programiškai programinės įrangos modulyje, kuris yra atskiras nuo neuroninio tinklo. Kuriant naują kliento-kliento duomenų perdavimo sesiją, gaunamas baigtinis šifravimo raktų ir veiksmų rinkinys, kuris pritaikomas specialiai sesijai.

Dar kitame įgyvendinimo variante perkvalifikavimas, pagrįstas blokų grandinės duomenimis, kurie gali būti atskiros maišos iš blokų rinkinio, maišos medžio arba „Merkle“ medžio, pas klientą įvyksta, kai blokų grandinėje atsiranda naujas blokas. Po perkvalifikavimo pasikeičia DNT svoriai ir išėjimo vertės, kurias sukuria DNT duomenų perdavimo sesijos pradžioje. Atitinkamai, kontroliuojant neuroninio tinklo svorių keitimo procesą, mokantis iš duomenų, gaunamų iš blokų grandinės, ir pateikiant unikalius duomenis į neuroninio tinklo įvestį kiekvienai

prognozei, gaunami šifravimo raktai, unikalūs kiekvienai sesijai ir klientui, bei su šifravimu susijusių veiksmų rinkinys, pavyzdžiui, šifravimo algoritmų ir jų keitimo tvarkos pasirinkimas, vieno šifravimo algoritmo pritaikymas kitam, šifruotų duomenų papildymas šiukšlėms – visa tai bus naudojama tik vienai sesijai ir vienam klientui. Naujai duomenų perdavimo sesijai DNT išvesties rinkinys bus kitoks.

Visi tinklo elementai, tokie kaip kliento mazgai, turi panašią architektūrą: blokų grandinė, tapačios būklės DNT ir programinės įrangos modulis, apdorojantis DNT išvesties parametrus, kad būtų priimtas galutinis sprendimas renkantis algoritmą ir naudojant šifravimo raktus.

Kiekvienos duomenų perdavimo sesijos pradžioje ryšį inicijuojantis klientas sukuria ir siunčia gavėjui atsitiktinių parametrų rinkinį (256-512 bitų) kaip DNT įvestį. Siuntėjas turi gavėjo kliento ID, kuris saugomas blokų grandinėje, taip pat raktus, kuriais klientai apsikeitė per pirmąjį kontaktą, ir atsitiktinius baitus, kuriuos siuntėjas atsiuntė duomenų perdavimo pradžioje. Siuntėjas gali dubliuoti gavėjo DNT būseną ir išvestinius duomenis iš savo pusės, pasirinkdamas tą patį raktų rinkinį, tą pačią veiksmų seką ir tuos pačius šifravimo algoritmus, kurie buvo pasirinkti šiai sesijai gavėjo pusėje.

Toliau pateikiamas pavyzdys yra kompiuterio įdiegtas neuroninės kriptografijos būdas duomenų perdavimui apsaugoti. DNT yra apmokytas tam tikru duomenų rinkiniu ir DNT turi tam tikrą skaičių įvesties neuronų, pageidautina, kad jis būtų lygus įvesties duomenų kiekiui numatytam DNT naudojimui. Pavyzdžiui, gali būti naudojami du parametrų rinkiniai. Originalus 256–512 bitų atsitiktinių duomenų rinkinys perduodamas tinklu kliento – kliento ryšio metu nuo prisijungimą inicijuojančio kliento, antrasis duomenų rinkinys yra asmeninis kliento ID, kuris gali būti unikalus 256–512 bitų raktas, X509 sertifikatas arba abu, atsižvelgiant į galutinę užduotį. Duomenų rinkinio parametrai ne tik identifikuoja klientą, bet ir yra DNT mokymo duomenų rinkinys.

Kliento - kliento ryšio metu, per duomenų perdavimo sesiją, per DNT siunčiami du duomenų rinkiniai, kurių bendra įvesties apimtis yra 512-1024 bitai. Neuronų išvesties sluoksnyje gaunami trys duomenų rinkiniai, kurie yra 256–512 bitų šifravimo rakto elementai ir kurie priklauso nuo galutinio tikslo ir neuroninio tinklo naudojimo užduoties. Antrasis duomenų rinkinys yra pirmojo rinkinio elementų poslinkio seka, skirta sukurti raktų diapazoną, remiantis duomenimis, gautais

pirmajame duomenų rinkinyje.

Pavyzdžiui, duomenų rinkinys, kurį sudaro 256–512 bitai pirmajame duomenų rinkinyje (šifravimo raktui sukurti), antrame duomenų rinkinyje turime poslinkio parametrų rinkinį, taikydami jį pirmajam duomenų rinkiniui kaip kaukę arba kaip poslinkio vektorių, iš gautų bitų galime gauti 256 poslinkio parinktis raktuose (arba didesnį variantų skaičių, atsižvelgiant į galutinį užduočių rinkinį), tada apdorojant programine įranga ir gaunant raktus, bus naudojami tiksliai tie patys raktai, gauti, remiantis pirmuoju duomenų rinkiniu, atsižvelgiant į antrojo duomenų rinkinio sudedamąjį poslinkį.

Atitinkamai, duomenų perdavimo sesijos pradžioje bus naudojamas pirmasis iš gautų raktų rinkinio, o po to antrasis ir t. t. iki 256 poslinkio variantų (arba bet koks kitas diapazonas, nustatytas pradinio DNT sukūrimo metu).

Trečiasis DNT duomenų rinkinys yra atsakingas už pasirinktą šifravimo algoritmą, šifravimo algoritmų keitimo seką ir kitas užduotis, susijusias su šifravimo proceso užmaskavimu.

Pavyzdžiui, gali būti naudojamas algoritmų rinkinys iš 3 simetrinių šifravimo algoritmų, keičiant jų seką ir darbo su jais logiką, remiantis trečiaisiais duomenų rinkinio parametrais, gautais iš neuroninio tinklo.

Būdas taip pat gali būti naudojamas centralizuotoje sistemoje su centriniu identifikavimo serveriu ir tik su vienu serverio bloko grandinės mazgu, kuriame ne kiekvienas klientas gali veikti kaip bloko grandinės tinklo mazgas, kaip ir decentralizuotoje schemoje.

Pagal centralizuotą schemą serveris yra atsakingas už naujų blokų kūrimą blokų grandinėje. DNT nuolat keis bendrąją šifravimo logiką, vykdydamas nuolatinį savarankišką mokymąsi, kuriam naudojamas savęs identifikavimo vartotojo raktas (kliento ID), taip pat duomenys iš blokų grandinės tinklo, kurie naudojami kaip duomenų rinkinys, perkvalifikuojant neuroninį tinklą, bet ne tam, kad būtų galima saugoti raktus ar generuoti juos, remiantis blokų grandine.

Čia aprašytas būdas gali būti naudojamas apsaugai nuo kvantinio skaičiavimo dėl kintančios duomenų šifravimo logikos, poreikio perduoti raktą per tinklą nebuvimo ir simetrinių šifravimo algoritmų, kurie atsparūs kvantiniam skaičiavimui, naudojimo.

Nors šiame išradimo aprašyme buvo išvardytos daugybė savybių ir pranašumų, taip pat struktūrinės detalės ir ypatybės, aprašymas pateiktas kaip išradimo įgyvendinimo pavyzdys. Nenukrypstant nuo išradimo principų, gali būti keičiamos detalės, ypač forma, dydis ir išdėstymas, atsižvelgiant į plačiausiai suprantamas sąvokų ir apibrėžimų, vartojamų apibrėžtyje, reikšmes.

IŠRADIMO APIBRĖŽTIS

1. Kompiuterinis duomenų šifravimo ir iššifravimo tinklo, kuriame naudojamas dirbtinis neuroninis tinklas, mazguose būdas, b e s i s k i r i a n t i s tuo, kad būdas apima:

dirbtinio neuroninio tinklo kopijų saugojimą bent jau pirmojo mazgo kliento kompiuterio įrenginyje ir bent vieno kito mazgo kliento kompiuterio įrenginyje;

įvesties parametrų rinkinių iš bent vieno pirmojo mazgo kliento kompiuterio ir bent iš vieno kito mazgo siuntimą;

dirbtinio neuroninio tinklo sinchronizavimą kiekviename mazge, naudojant įvesties parametrus;

šifravimo raktų kūrimą, naudojant dirbtinį neuroninį tinklą ir įvesties parametrus kiekviename tinklo mazge;

išvesties parametrų rinkinio sudarymą, naudojant dirbtinį neuroninį tinklą, blokų grandinės duomenis ir šifravimo raktus;

šifravimo algoritmo parinkimą, naudojant dirbtinį neuroninį tinklą ir išvesties parametrus;

šifravimo maskavimo tipo parinkimą, naudojant dirbtinį neuronų tinklą ir išvesties parametrus;

šifravimo raktų, šifravimo algoritmų ir šifravimo maskavimo sinchronizavimą kiekviename tinklo mazge;

duomenų užšifravimą, naudojant šifravimo raktus, pasirinktą šifravimo algoritmą ir pasirinktą šifravimo maskavimą;

užšifruotų duomenų iš pirmo kliento kompiuterio perdavimą į bent vieną kitą kliento kompiuterio įrenginį;

duomenų iššifravimą pas klientą, naudojant šifravimo raktus, pasirinktą šifravimo algoritmą ir pasirinktą šifravimo maskavimą;

iššifruotų duomenų perdavimą galutiniam gavėjo mazgui;

naujo blokų grandinės bloko skaičiavimą bent viename kliento tinklo mazge;

atnaujintos blokų grandinės perdavimą iš bent vieno kliento mazgo į pirmąjį mazgą ir kiekvieną kitą tinklo mazgą;

dirbtinio neuroninio tinklo perkvalifikavimą kiekviename tinklo mazge, naudojant atnaujintą blokų grandinę.

2. Būdas pagal 1 punktą, kur tinklas yra internetas arba vietinis tinklas.

3. Būdas pagal 1 punktą, kur atsitiktinai sugeneruojamas vienas iš mažiausiai dviejų

įvesties parametrų rinkinių.

4. Būdas pagal 1 punktą, kur vienas iš mažiausiai dviejų įvesties parametrų rinkinių yra unikalus 256–512 bitų raktas, X509 sertifikatas arba abu.

5. Būdas pagal 1 punktą, kur šifravimo raktai sukuriami pirmame mazge ir bent viename kitame mazge vienu metu.

6. Būdas pagal 1 punktą, kur šifravimo algoritmas yra simetriškas šifravimo algoritmas.

7. Būdas pagal 6 punktą, kur šifravimo algoritmas yra pasirinktas iš AES 256, 3DES, ChaCha, Salsa20, Blowfish, Twofish, DES, Kuznechik ir kitų.

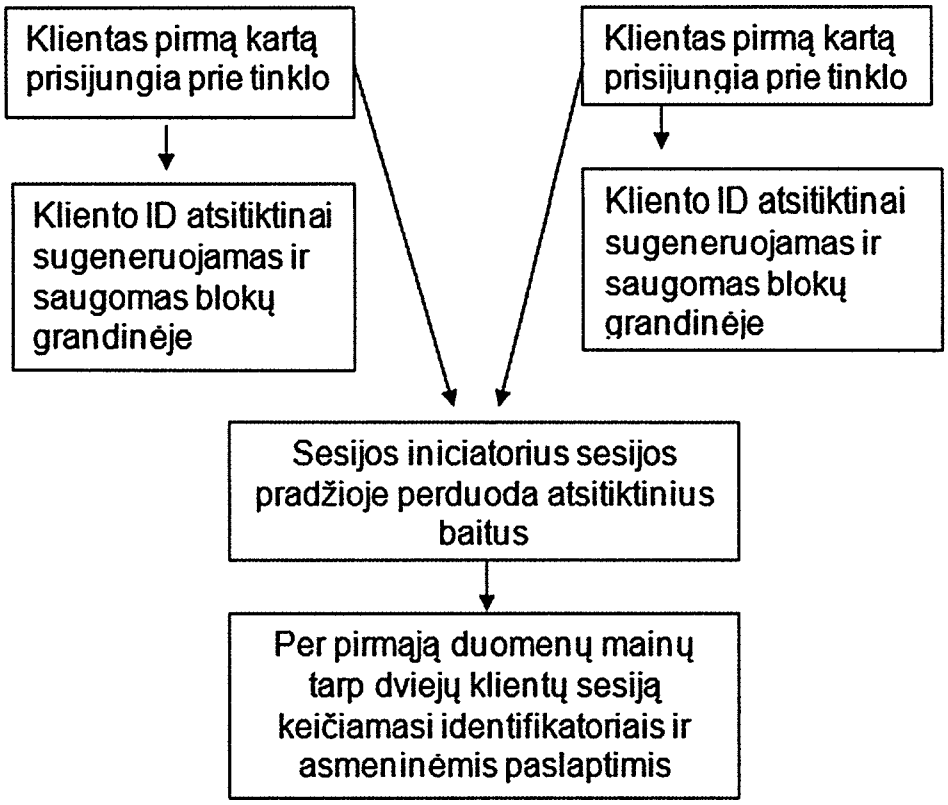
8. Būdas pagal 1 punktą, kur šifravimo raktas neperduodamas tinklu.

9. Būdas pagal 1 punktą, kur duomenys perduodami decentralizuoto tinklo tipo duomenų perdavimo forma.

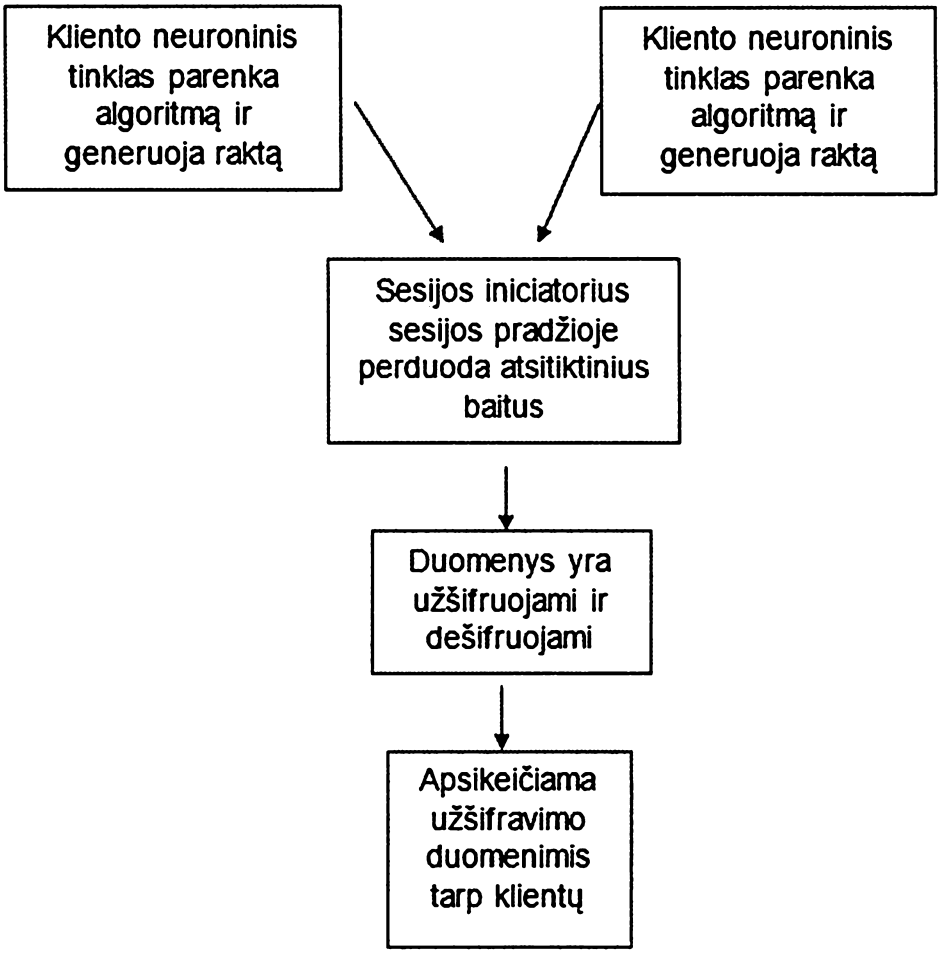
10. Būdas pagal 1 punktą, kur dirbtinis neuroninis tinklas mokomas blokų grandinėje.

11. Būdas pagal 10 punktą, kur šifravimo raktas nėra saugomas blokų grandinėje.

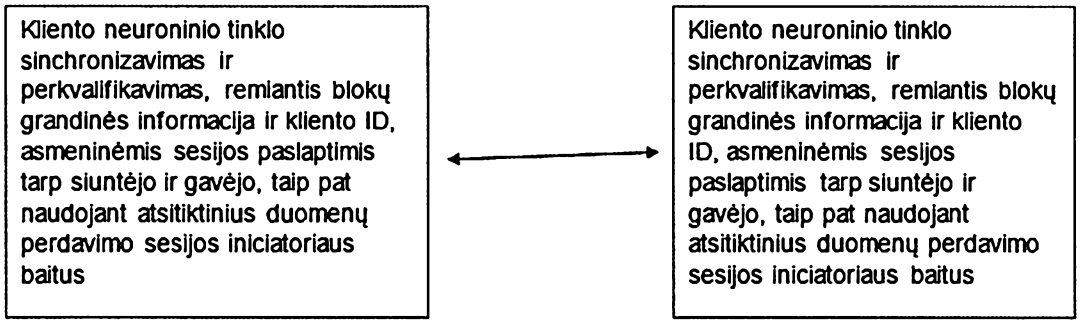
12. Būdas pagal 10 punktą, kur jokie dirbtinio neuroninio tinklo elementai nėra saugomi blokų grandinėje.


Klientas pirmą kartą prisijungia prie tinklo
Klientas pirmą kartą prisijungia prie tinklo
Kliento ID atsitiktinai sugeneruojamas ir saugomas blokų grandinėje
Kliento ID atsitiktinai sugeneruojamas ir saugomas blokų grandinėje
Sesijos iniciatorius sesijos pradžioje perduoda atsitiktinius baitus
Per pirmąją duomenų mainų tarp dviejų klientų sesiją keičiamasi identifikatoriais ir asmeninėmis paslaptimis

1 pav.


Kliento neuroninis tinklas parenka algoritmą ir generuoja raktą
Kliento neuroninis tinklas parenka algoritmą ir generuoja raktą
Sesijos iniciatorius sesijos pradžioje perduoda atsitiktinius baitus
Duomenys yra užšifruojami ir dešifruojami
Apsikeičiama užšifravimo duomenimis tarp klientų

2 pav.


Kliento neuroninio tinklo sinchronizavimas ir perkvalifikavimas, remiantis blokų grandinės informacija ir kliento ID, asmeninėmis sesijos paslaptimis tarp siuntėjo ir gavėjo, taip pat naudojant atsitiktinius duomenų perdavimo sesijos iniciatoriaus baitus
Kliento neuroninio tinklo sinchronizavimas ir perkvalifikavimas, remiantis blokų grandinės informacija ir kliento ID, asmeninėmis sesijos paslaptimis tarp siuntėjo ir gavėjo, taip pat naudojant atsitiktinius duomenų perdavimo sesijos iniciatoriaus baitus

3 pav.