ROMÂNIA

(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

(11) **RO 132017 A2**

(51) Int.Cl.
H04L 12/26 (2006.01),
H04L 9/16 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2015 00986**

(22) Data de depozit: **10/12/2015**

(41) Data publicării cererii:
30/06/2017 BOPI nr. **6/2017**

(71) Solicitant:
• **IXIA**, *A CALIFORNIA CORPORATION, 26601 WEST AGOURA ROAD, CALABASAS, CALIFORNIA, US*

(72) Inventatori:
• **CIPU ANDREI**, *STR.PRECIZIEI NR.6M, BL.1A, AP.10, BUCUREŞTI, B, RO;*
• **BADEA ALEXANDRU**, *CALEA CRÂNGAŞI NR.30, BL.50, SC.B, AP.39, BUCUREŞTI, B, RO*

(74) Mandatar:
RATZA ŞI RATZA SRL, *B-DUL A.I. CUZA, NR. 52-54, SECTOR 1, BUCUREŞTI*

(54) # METODE, SISTEME ŞI SUPORT CITIBIL DE CALCULATOR PENTRU REDUCEREA UNEI CHEI CRIPTOGRAFICE ÎNTR-UN MEDIU DE SIMULARE A TESTĂRII

(57) **Rezumat:**

Invenţia se referă la o metodă, un sistem şi un suport non-tranzitoriu, care poate fi citit de calculator, destinate reducerii dimensiunii unei chei criptografice într-un mediu de simulare a testării. Metoda conform invenţiei cuprinde determinarea unei valori minime şi a unei valori maxime a dimensiunii cheii, pentru o cheie criptografică privată, pentru fiecare pereche dintr-o multitudine de perechi de numere de schimbare a cheii de criptare, delimitarea, pentru fiecare dintre perechile de numere de schimbare a cheii de criptare, a unei constante de dimensionare a cheii, în funcţie de valorile minimă şi maximă ale dimensiunii cheii, stocarea fiecărei perechi de numere selectate şi a constantei de dimensionare a cheii, asociate, într-un dispozitiv de stocare a datelor, selectarea unei perechi de numere de schimbare a cheii de criptare, pentru a fi aplicată unei sesiuni de simulare a testării efectuate între un prim şi un al doilea punct final de simulare a testării, şi generarea unei chei criptografice private, în funcţie de constanta de dimensionare a cheii, asociată cu perechea de numere de schimbare a cheii de criptare selectate. Sistemul pentru reducerea dimensiunii unei chei criptografice, într-un mediu de simulare a testării, conform invenţiei, cuprinde un dispozitiv de imitare a traficului (**102**) configurat să efectueze metoda conform invenţiei. Suportul non-tranzitoriu conţine instrucţiuni executabile de către calculator care, atunci când sunt executate de un procesor, comandă calculatorul să efectueze etapele metodei conform invenţiei.

Revendicări: 20
Figuri: 3

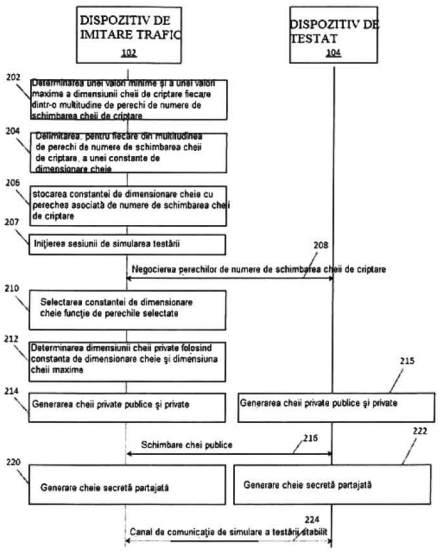

Fig. 2

RO 132017 A2

METODE, SISTEME ȘI SUPORT CITIBIL DE CALCULATOR PENTRU REDUCEREA DIMENSIUNII UNEI CHEI CRIPTOGRAFICE ÎNTR-UN MEDIU DE SIMULARE A TESTĂRII

Domeniul tehnic de aplicare

Prezenta invenție se referă la efectuarea de simulări de trafic de pachete de date într-un mediu de simulare a testării. Mai precis, prezenta invenției se referă la metode, sisteme și suport citibil de calculator pentru reducerea dimensiunii unei chei criptografice într-un mediu de simulare a testării.

Stadiul anterior al tehnicii

Schimbarea cheii de criptare Diffie-Hellman este o parte integrantă a procesului de stabilire a canalului de securitate pe protocolul Internet (IPsec). Cu toate acestea, acest proces de schimbare de cheie necesită o cantitate considerabilă de timp de procesare necesar pentru a stabili un canal de securitate IPsec. Mai exact, generarea unei chei private criptografice, a unei chei publice criptografice și a unei cheii secrete partajată asociată poate necesita un calcul extrem de intensiv. În ciuda acestui neajuns semnificativ, trebuie să fie stabilite, cât mai curând posibil, un număr mare de canale IPsec într-un mediu de simulare a testării. Astfel, orice reducere a timpului asociată cu determinarea cheilor de criptare poate fi extrem de benefică din punct de vedere a eficienței testării.

Astfel, există o nevoie de metode, sisteme și suport citibil de calculator pentru reducerea dimensiunii unei chei criptografice într-un mediu de simulare a testării.

Expunerea pe scurt a invenției

Sunt prezentate metode, sisteme și suport citibil de calculator pentru reducerea dimensiunii unei chei criptografice într-un mediu de simulare a testării. Conform unui exemplu de realizare, o metodă include determinarea unei valori minime și a unei valori maxime a dimensiunii cheii pentru o cheie criptografică privată pentru fiecare dintr-o multitudine de perechi de numere de schimbare cheie de criptare și delimitarea, pentru fiecare din multitudinea de perechi de numere de schimbare cheie de criptare, a unei constante de dimensionare cheie în funcție de valoarea minimă și valoarea maximă a valorii dimensiunii cheii. Metoda mai include stocarea fiecărei dintre multitudinea de

perechi selectate de numere de schimbare cheie de criptare și a constantei de dimensionare cheie într-un dispozitiv de stocare date, selectarea unei perechi de numere de schimbare cheie de criptare pentru a fi aplicată la o sesiune de simulare testare efectuată între un prim punct final de simulare testare și un al doilea punct final de simulare testare, și generarea unei chei criptografice privată în funcție de constanta de dimensionare cheie asociată cu perechea selectată de numere de schimbare cheie de criptare.

Obiectele prezentei invenții pentru reducerea mărimii unei chei criptografice pot fi implementate prin software, hardware, firmware în orice combinaţie unul cu altul. Astfel, așa cum sunt utilizați în prezenta descriere, termenii de „funcție", „modul" sau „nod", așa cum sunt utilizați în continuare se referă la hardware care poate include componente de software și/sau firmware, pentru implementarea caracteristicilor ce vor fi descrise în continuare. Într-un exemplu de realizare a invenţiei, obiectele invenţiei descrise aici pot fi implementate folosind un suport citibil de calculator care are stocate instrucţiuni executabile de către computer, care, atunci când sunt executate de către procesorul unui computer, îi comandă acestuia efectuarea unor paşi. Suportul citibil de calculator, conform invenției, adecvat pentru implementarea obiectului invenţiei descris aici include dispozitive non-tranzitorii, precum discuri de memorie, chip-uri de memorie, dispozitive logic programabile, rețele de porți programabile de către utilizator şi circuite integrate cu aplicaţii specifice. În plus, un suport citibil de calculator care implementează obiectul invenţiei descris aici poate fi situat pe un singur dispozitiv sau platformă de calcul sau poate fi distribuit pe mai multe dispozitive sau platforme de calcul.

Descrierea pe scurt a desenelor explicative

Exemplele de realizare preferate ale obiectelor prezentei invenții vor fi explicate cu referire la desenele însoțitoare, în care aceleași numere de referință reprezintă elemente similare, în care:

- **Figura 1** ilustrează o diagramă bloc a unui sistem pentru reducerea mărimii unei chei criptografice într-un mediu de simulare a testării, conform unui exemplu de realizare a prezentei invenții;
- **Figura 2** ilustrează o diagramă de semnalizare care prezintă transmiterea mesajelor pentru reducerea mărimii unei chei criptografice într-un mediu de simulare a testării, conform unui exemplu de realizare a prezentei invenții; și

- **Figura 3** ilustrează o diagramă flux a unei metode pentru reducerea mărimii unei chei criptografice într-un mediu de simulare a testării, conform unui exemplu de realizare a prezentei invenții;

Descriere detaliata

Sunt prezentate metode, sisteme și suport citibil de calculator pentru reducerea dimensiunii unei chei criptografice. Conform unui exemplu de realizare, obiectul prezentei invenţii implică calculul, prin unul sau mai multe dispozitive de punct final pentru simulare a testării (de exemplu, dispozitiv de imitare trafic și/sau un dispozitiv de testat), a cel puțin unei constante de dimensionare cheie care poate fi utilizată pentru a reduce dimensiunea unei sau mai multor chei criptografice care sunt utilizate pentru efectuarea unei sesiuni de simulare testare (de exemplu, înainte de orice stabilire efectivă a canalului de comunicaţie IPsec). În special, obiectul prezentei invenţii minimizează timpul pentru calcularea și utilizarea cheilor criptografice cu resurse intensive, care permite, în mod eficient, ca într-un mediu de simulare a testării să fie stabilit un număr mare de canale IPsec.

Figura 1 este o schemă bloc care ilustrează arhitectura unui sistem **100** de simulare a testării, conform unui exemplu de realizare a obiectului prezentei invenţii. Conform Figurii 1, sistemul **100** include un dispozitiv **102** de imitare trafic, care este conectat, din punct de vedere al comunicării, la un dispozitiv controler **101** de testare și la un dispozitiv **104** de testat (DUT). Conform unor exemple concrete de realizare, DUT **104** poate include o poartă de acces de servire (SGW), o poarta de acces reţea de pachete de date (PGW), un dispozitiv de protecţie de tip firewall, un router, un dispozitiv de traducere adresă de rețea (NAT), sau orice dispozitiv sau sistem care ar putea beneficia de capacitate mare de trafic de simulare testare. Conform unui exemplu de realizare, DUT **104** poate fi conectat, din punct de vedere al comunicaţiei, la dispozitivul **102** de imitare trafic printr-o conexiune cu sau fără fir care facilitează transferul de trafic de pachete de date criptate.

Conform unor exemple de realizare, dispozitivul **102** de imitare trafic poate include un dispozitiv sau un echipament hardware care este configurat pentru a genera și transmite traficul de pachete de date la DUT **104** pentru simularea testării propusă. Conform unui exemplu de realizare, dispozitivul **102** de imitare trafic poate include un procesor **106**, o unitate generator de trafic **108**, o unitate interfaţă de reţea **110**, o

unitate receptor de trafic **112**, un modul cu plan de control **113,** unitatea de stocare locală **114** şi memoria **120**. Procesorul **106** poate include o unitate centrală de procesare (CPU), un microcontroler sau orice alt hardware bazat pe procesor care a fost configurat pentru a gestiona și facilita funcționarea modulelor **108** și **112** în dispozitivul **102** de imitare trafic. Procesorul **106** poate, de asemenea, include o unitate de memorie și diferite unităţi specializate, circuite, software și interfeţe pentru furnizarea funcţionalităţilor și caracteristicilor descrise în prezenta invenţie. Conform unor alte exemple de realizare, dispozitivul **102** de imitare trafic poate funcţiona fie ca o entitate client fie ca o entitate server fie ca ambele, în raport cu DUT **104**. De exemplu, dispozitivul **102** de imitare trafic poate include un prim dispozitiv şi un al doilea dispozitiv de punct final pentru simularea testării care stabilesc sesiunile de simulare a testării în sistemul sau dispozitivul de testat.

Conform unor exemple de realizare, unitatea generator **108** de trafic poate include un modul voce, care poate fi configurat pentru a genera date audio de trafic, și un modul video, care poate fi configurat pentru a genera date video de trafic. Într- unul dintre exemple, modulul voce poate include un modul pe bază de software (executat de hardware bazat pe procesorul **106**), care este configurat pentru a genera date tip voce pe baza traficului de simulare pe un anumit protocol L4-L7. De exemplu, unitatea **108** generator de trafic poate fi configurată să genereze date prin protocolul de transport în timp real (real-time transport protocol RTP), date care sunt în cele din urmă transmise la DUT **104**. În unele exemple de realizare, unitatea **108** generator de trafic poate fi configurată pentru a cripta traficul de pachete de date generat, aşa cum ar fi prin utilizarea protocolului de securitate IPsec. Traficul de pachete generat și criptat prin unitatea **108** generator de trafic poate fi transmis la reţea unitatea **110** interfaţă de reţea înainte de transmiterea sa la DUT **104**.

Conform unelor exemple de realizare, unitatea **110** de interfaţă de reţea poate converti traficul de pachete test de ieșire de la unitatea **108** generator de trafic într-un format de semnal electric, optic, sau wireless care este necesar pentru a transmite traficul de testare la DUT **104** prin intermediul unei conexiuni prin cablu, fibră optică, wireless, sau un alte conexiuni de comunicaţie similare. Similar, unitatea **110** de interfaţă de reţea poate recepţiona semnalele electrice, optice sau wireless de la DUT **104** și poate fi configurată pentru a converti semnalele (de exemplu pachete de date) primite în interiorul traficului de testare de intrare într-un format utilizabil de către dispozitivul **102**

de imitare trafic. Pachetele recepţionate pot fi transmise prin unitatea **110** de interfaţă de reţea la unitatea **112** receptor de trafic.

Conform unelor exemple de realizare, unitatea **112** receptor de trafic poate recepţiona traficul test de intrare de la unitatea **110** de interfaţă de reţea. Unitatea **112** receptor de trafic poate fi configurată să determine dacă fiecare pachet de date recepţionat este un element al unul flux de date specific, şi poate acumula statisticile de testare pentru fiecare flux, în conformitate cu instrucţiunile de testare oferite de procesorul **106**. Statisticile de testare acumulate pot include, de exemplu, numărul total de pachete recepţionate, numărul de pachete recepţionate în afara secvenţei, numărul de pachete de date recepţionate cu erori, întârzierea de propagare maximă, medie şi minimă, precum şi alte statistici pentru fiecare flux de date. Unitatea **112** receptor de trafic poate oferi, de asemenea, statistici de testare şi/sau pachetele capturate de la procesorul **106** pentru analize suplimentare, în timpul sau după sesiunea de testare. Conform unor exemple de realizare, unitatea **112** receptor de trafic poate fi de asemenea configurată pentru a decripta traficul de pachete recepţionat de la DUT **104**.

Conform exemplului de realizare, modulul **113** cu plan de control poate include un modul cu plan de control prin protocolul de comunicaţie (GTP) pentru serviciul general de pachete de date radio (GPRS) care este configurat pentru a efectua negocierea asociată cu stabilirea canalelor de comunicaţie prin protocolul IPSec, într-o sesiune de testare. Conform unor exemple de realizare, sesiunea de testare prin protocolul IPsec se desfăşoară între un dispozitiv de imitare trafic şi un DUT, pe un strat de reţea. De exemplu, modulul **113** cu plan de control poate comunica cu DUT **104** (de exemplu via unitatea **110** de interfaţă de reţea) pentru a stabili o multitudine de sesiuni prin protocolul IPsec, care pot fi utilizate pentru a comunica trafic de date media criptat.

Conform unor exemple de realizare, procesorul **106** poate fi configurat să comunice cu dispozitivul controler **101** de testare. Dispozitivul controler **101** de testare poate fi un dispozitiv de calcul conţinut în, sau în afară de, dispozitivul **102** de imitare trafic. Dispozitivul controler **101** de testare poate furniza procesorului **106** instrucţiunile şi datele utilizate de dispozitivul **102** de imitare trafic, pentru realizarea testării de către DUT **104**. Instrucţiunile şi datele primite de dispozitivul **102** de imitare trafic de la dispozitivul controler **101** de testare pot include, de exemplu, definiţiile fluxurilor de pachete de date pentru a fi generate de dispozitivul **102** de imitare trafic şi definiţiile statisticilor de performanţă care pot fi acumulate şi raportate de dispozitivul **102** de

imitare trafic. Conform unui exemplu de realizare, dispozitivul **101** de control testare poate fi utilizat de un operator de reţea, un administrator de simulare testare sau orice alt utilizator, pentru a iniţia şi/sau a stabilii parametrii de simulare testare trafic care implică dispozitivul **102** de imitare trafic şi DUT **104**.

Conform unor exemple de realizare, unitatea de stocare locală **114** poate include o memorie, o unitate de stocare bazată pe hardware, o bază de date sau orice altă unitate locală, care este capabilă de stocare electronică de informaţii. De exemplu, unitatea de stocare locală **114** poate fi amplasată în dispozitivul **102** de imitare trafic. Aşa cum se arată în Figura 1, unitatea de stocare locală **114** poate fi utilizată pentru a stoca o bază de date **116** cu un număr de schimbare de chei şi o bază de date **118** cu mapări. Conform unor exemple de realizare, baza de date **116** cu un număr de schimbare de chei poate include intrările bazei de date care conţin perechi de numere de schimbare cheie de criptare care au fost desemnate ca aprobate şi/sau acceptabile pentru a efectua o sesiune de simulare testare cu un DUT. De exemplu, intrările de baza de date poate cuprinde o listă de perechi p - g acceptabile (de exemplu, grupuri Diffie Hellman), care pot fi prezente într-un DUT sau la un al doilea punct final de simulare testare în timpul unei negocieri de numere de schimbarea cheii de criptare. În special, fiecare pereche p-g este compus dintr-o valoare "p" (unde p este un număr prim) şi o valoare "g" (unde g este un modul rădăcină primitivă de p), care sunt aplicate în ultimul timp la o operaţiune de modul pentru a obţine o cheie criptografică publică şi o valoare secretă partajată utilizabilă de către punctul final de testare. În mod similar, baza de date **118** de mapare include intrări de bază de date care mapează fiecare dintre perechile p-g acceptabile pentru o constantă precalculată de dimensionare cheie (care este determinată într-un mod descris mai jos). Utilizarea bazei de date **118** de mapare oferă unui administrator de sistem avantajul de a reduce în mod eficient dimensiunea sau lungimea unei chei criptografice private în scopuri de simulare testare.

Dispozitivul **102** de imitare trafic mai include memoria **120**, care poate cuprinde memoria cu acces aleator (RAM), memoria numai pentru citire (ROM), memorie citire/scriere optică, memoria cache, memoria magnetică citire/scrie, memoria flash, sau orice alt suport non-tranzitoriu care poate fi citit de calculator. În unele exemple, procesorul **106** si memoria **120** pot fi utilizate pentru a executa şi pentru a gestiona funcţionarea dispozitivului de reducere **122** a dimensiunii cheii de criptare (care este

stocată în memoria **120**). În unele exemple, dispozitivul de reducere **122** a dimensiunii cheii de criptare cuprinde un algoritm care, atunci când este executat de către procesorul **106**, efectuează etapele descrise în Figurile 2 și 3. Cu toate că Figura 1 ilustrează numai dispozitivul de reducere **122** a dimensiunii cheii de criptare ca fiind acționat de un dispozitiv **102** de imitare trafic (ex un prim punct final de simulare testare), acesta poate fi operat în mod similar prin DUT **104** sau prin orice alt doilea punct final de simulare testare.

După ce s-a negociat și s-a stabilit un canal de comunicaţie IPSec de unitatea **113** de plan de control, dispozitivul de imitare **102** trafic poate fi configurat pentru a genera trafic de pachete de date criptate (de exemplu, un flux de pachete). De exemplu, datele de trafic criptate pot include date de trafic RTP criptate prin IPsec. Conform unui exemplu de realizare, generatorul **108** de trafic poate fi învăţat de dispozitivul **101** controler de testare să înceapă generarea datelor de trafic necesare pentru sesiunea de testare.

După ce dispozitivul **102** de imitare trafic stabileşte canalul de comunicaţie IPsec pentru a comunica fluxul de date media la DUT **104**, acesta poate cripta datele de trafic de pachete și poate transmite datele de trafic de pachete criptate unității **110** de interfață de reţea. În special, datele de trafic de pachete pot fi criptate cu un secret partajat derivat din dimensiunea redusă a cheii criptografice privată generată de primul punct final de simulare testare. Unitatea **110** de interfață de rețea transmite ulterior traficul de pachete de date criptat la DUT **104** prin canalul de comunicaţie IPsec stabilit. Conform unui exemplu de realizare, datele de trafic simulat sunt criptate și împachetate înainte de a fi trimise prin canalul de comunicaţie IPsec stabilit la DUT **104**.

O ilustrare cu privire la modul de reducere a dimensiunii cheii criptografice este descrisă în Figura 2. În special, Figura 2 ilustrează o diagramă de semnalizare care descrie transmiterea mesajelor pentru reducerea mărimii unei chei criptografice într-un mediu de simulare testare, în conformitate cu un exemplu de realizare a obiectului prezentei invenţii. În unele exemple, dispozitivul **102** de imitare trafic poate determina prima o multitudine de diferite perechi de numere de schimbarea cheii (de exemplu, perechile p-g $pairs_{1...N}$) care pot fi, eventual, utilizate într-un test de simulare a traficului. În special, această etapă este efectuată înainte de inițierea sau stabilirea a oricărei sesiuni de teste sunt. În unele exemple de realizare, dispozitivul **102** de imitare trafic poate accesa propria listă de numere de schimbare cheii de criptare posibile. În unele

exemple, un număr de schimbarea cheii "g" poate fi setat la o valoare numerică care este cunoscută de toate DUT-urile, cum ar fi g = 3. În ceea ce privește numărul de schimbare cheie "p", dispozitivul de imitare trafic poate furniza o unitate de stocare locală (de exemplu, o memorie locală sau o bază de date locală), cu o multitudine de valori "p". În special, unitatea de stocare locală poate conține orice număr de valori "p", fiecare dintre ele fiind mapat la o cheie criptografică privată corespunzătoare și la o cheie criptografică publică corespunzătoare, care au fost predeterminate și/sau precalculate.

La etapa de la blocul **202**, dispozitivul **102** de imitare trafic determină dimensiunea minimă și maximă a cheii de criptare pentru fiecare dintr-o multitudine de perechi de numere de schimbare cheie. În special, dispozitivul **102** de imitare trafic menține o listă de perechi de valoare "p" și "g" (de exemplu, grupuri Diffie-Hellman) care sunt utilizate și/sau acceptate de către dispozitivul **102**. În unele aplicații concrete, dispozitivul **102** de imitare trafic stabilește sau determină valorile numerelor de schimbarea cheii (de exemplu, "p" și "g"), care pot fi utilizate în simulare a de testare cu un DUT.

În unele exemple de realizare, dispozitivul **102** de imitare trafic poate fi configurat pentru a efectua teste de măsurare a traficului pe baza unei încercări și a unei erori pentru a determina dimensiunea minimă și maximă a cheii de criptare (pentru a fi utilizată o cheie criptografică privată) pe baza valorilor p și g folosite. De exemplu, încercarea de simulare testării poate stabili că L_{min} = 160 bytes și L_{max} = 1600 bytes sunt asociate cu o anumită pereche numere de schimbare a cheii care include valori de p = 17 și g = 3. În mod similar, L_{min} și L_{max} pot fi derivate pentru fiecare pereche de numere de schimbarea cheii menținută de dispozitivul **102** de imitare trafic după stabilirea experimentală a câtorva canale de comunicaţie (și se omite uneori configurarea). De exemplu, sistemul poate stabili câteva tuneluri și înregistrează timpii asociate înființat și introduceți valorile în algoritmul.

La etapa de la blocul **204**, o constantă de dimensionarea cheii de criptare pentru fiecare pereche de numere de schimbarea cheii este derivată. În unele exemple de realizare, dispozitivul **102** de imitare trafic calculează o constantă de dimensionare cheie prin împărțirea valorii minime a dimensiunii cheii la valoarea maximă a dimensiunii cheii pentru fiecare pereche de numere de schimbarea cheii asociată. Revenind la exemplul inițial, în cazul în care L_{min} = 160 bytes și L_{max} = 1600 bytes, constanta de dimensionare cheie va fi determinată de dispozitivul **102** de imitare trafic pentru a fi egală cu 0,1.

La etapa de la blocul **206**, fiecare dintre constantele principale de dimensionare este stocată cu perechile de numere de schimbarea cheii asociate. Conform unor exemple, dispozitivul **102** de imitare trafic mapează și, respectiv înregistrează multitudinea de de constante de dimensionarea cheii pentru perechea de numere de schimbarea cheii pereche respectivă. Mai exact, dispozitivul **102** se imitare de trafic poate stoca aceste mapări înregistrate de constante de dimensionarea cheii și perechile de numere de schimbarea cheii ca şi intrări în baza de date **114**.

La etapa de la blocul **207**, este făcută o determinare pentru a iniția o sesiune de testare între un prim punct final de simulare testare (de exemplu, dispozitivul **102** de imitare trafic) și un al doilea punct final de simulare testare (de exemplu, DUT **104**). Conform unor exemple de realizare, această determinare se poate face printr-un operator de rețea care utilizează un dispozitiv de control de testare (de exemplu, dispozitivul controler de testare **101** în Figura 1). În cazul în care o sesiune de testare IPsec este inițiată și condusă între dispozitivul **102** de imitare de trafic și DUT **104**, metoda **200** continuă la etapa **208**.

La linia **208**, perechile de numere de schimbarea cheii sunt negociate de dispozitivul **102** de imitare trafic și DUT **104**. La debutul acestui negocieri, dispozitivul **102** de imitare testare selectează pentru început o multitudine de perechi de valoare de schimbarea cheii pentru a fi propuse la DUT **104**. De exemplu, dispozitivul **102** de imitare testare poate selecta perechile $pairs_{1\text{-}5}$ p-g pentru transmiterea la DUT **104**. După selectarea menţionată, dispozitivul **102** de imitare trafic poate transmite perechile selectate de numere de schimbarea cheii (de exemplu, perechile $pairs_{1\text{-}5}$ p-g de schimbarea cheii) la DUT **104**. La primire, DUT **104** poate analiza valorile p și g propuse și fie i) consideră un anumită valoare p și g acceptabilă, fie, ii) respinge toate perechile de valoare p și g propuse. De exemplu, DUT **104** determină dacă " $pair_1$ p-g " este compatibilă cu și acceptată de DUT **104** în scopuri de testare. Dacă " $pair_1$ p-g " nu este acceptată sau utilizabilă de DUT **104**, acesta poate selecta oricare dintre alte numere de schimbarea cheii primite (de exemplu, "p-g $pair_2$" - "p-g $pair_5$"). Dacă niciuna dintre perechile "p" și "g" transmise de dispozitivul **102** de imitare trafic nu este utilizabilă de DUT **104**, DUT 104 poate contacta dispozitivul **102** de imitare trafic pentru a solicita perechi suplimentare de valori de numere de schimbarea cheii pentru examinare. Odată ce perechea p-g este aprobată de DUT **104**, DUT **104** informează dispozitivul **102** de imitare trafic de selecție.

În exemple de realizare alternative, numărul "g" de schimbarea cheii poate avea o valoare predeterminată (de exemplu, g = 3), care este cunoscută și utilizată de către dispozitivul **102** de imitare trafic și DUT **104**. În mod similar, dispozitivul **101** controler de testare poate fi de asemenea utilizat pentru a selecta unul sau numere potențiale de schimbarea cheie „p_1-p_n", care sunt susceptibile de a fi compatibile cu și acceptate de DUT **104**. Conform unor exemple de realizare, de unul sau mai multe numere potențiale de schimbarea cheii pot fi stocate ca numere **116** de schimbarea cheii stocate în baza de date **114** locală.

La etapa de la blocul **210**, dispozitivul **102** de imitare trafic selectează o constantă de dimensionare cheie în funcție de perechea negociată de numere de schimbarea cheii. Conform unor exemple de realizare, de dispozitivul **102** de imitare trafic utilizează perechea de numere de schimbarea cheii care a fost negociată/selectată la linia **208** pentru a accesa baza de date **114** pentru a obține constanta corespunzătoare de dimensionarea cheii mapată din baza de date. De exemplu, dispozitivul **102** de imitare trafic poate utiliza o interogare a bazei de date care conține perechea p și g.

La etapa de la blocul **212**, dimensiunea pentru cheia criptografică privată este determinată utilizând constanta selectată de dimensionare cheie. În unele exemple de realizare, de dispozitivul 102 de imitare trafic determină mărimea cheii criptografice private prin aplicarea constantei de dimensionare cheie la o dimensiune sau lungime cheie implicită. De exemplu, în cazul în care constanta de dimensionare cheie a fost determinată să fie egală cu 0,1 și dimensiunea cheie implicite este stabilită pentru a fi 2048 bytes, atunci dispozitivul **102** de imitare trafic desemnează dimensiunea (sau lungimea) cheii criptografice private să fie 26 bytes prin calcularea produsului a acestor doi parametri (de exemplu, 256 bytes x 0,1 = 25,6 sau 26 bytes). În special, un calcul folosind constanta de dimensionare cheie precalculată are nevoie să fie efectuată doar o dată, deoarece se bazează pe perechea de numere de schimbarea cheii care a fost negociată între cele două dispozitive de simulare testare (de exemplu, dispozitivul **102** de imitare trafic și DUT **104**).

La etapa de la blocul **214**, sunt generate cheile criptografice privată și publică. Conform unor exemple de realizare, dispozitivul **102** de imitare trafic generează o cheie criptografică privată în conformitate cu dimensiunea cheii stabilită în blocul **212**. Conform unor exemple de realizare, dispozitivul **102** de imitare trafic poate genera o cheie criptografică privată "a", înainte de a stabili o sesiune de testare, caz în care "a" este de 26 bytes. La generarea cheii criptografice private, dispozitivul **102** de imitare

trafic poate fi configurat pentru a genera ulterior o cheie criptografică publică. În unele exemple de realizare, dispozitivul **102** de imitare trafic poate genera o cheie criptografică publică "A" înainte de inițierea sesiunii de testare. De exemplu, cheia criptografică publică poate fi generată de dispozitivul **102** de imitare trafic pe baza formulei, $A = g^a$ * modul p, unde "a" este cheia privată criptografică a dispozitivului de imitare trafic **102**. De remarcat, dimensiunea cheii criptografice publice va fi, de asemenea, redusă în mod eficient, deoarece mărimea cheii publice criptografice este bazată direct pe dimensiunea cheii criptografice privată.

La etapa de la blocul **215**, DUT **104** utilizează numerele de schimbare cheie (de exemplu, "p_1" și "g_1" ale perechilor p-g $pair_1$ selectate) pentru a genera o cheie criptografică "B" public. De exemplu, cheia criptografică publică poate fi generată de dispozitivul **102** de imitare trafic pe baza formulei, $B = g^a$ * modul p, unde "b" este cheia criptografică privată a DUT **104**. Conform unor alte exemple de realizare, DUT **104** poate fi de asemenea configurat pentru a reduce dimensiunea cheii propriei chei private "b" în același mod în care dispozitivul de imitare trafic reduce dimensiunea cheii private criptografice "a".

În etapa de la blocul **216**, cheile criptografice publice sunt schimbate. În unele exemple de realizare, de dispozitivul **102** de imitare trafic și DUT **104** pot face schimb, din punct de vedere al comunicației, de chei de criptare publice (de exemplu, prin mesaje). De exemplu, dispozitivul **102** de imitare trafic poate transmite cheia criptografică "A" publică la DUT **104**. În mod similar, DUT **104** poate transmite cheia publică criptografică "B" pe dispozitivul **102** de imitare trafic.

În etapele de la blocurile **220** și **222**, dispozitivul **102** de imitare trafic și DUT **104** generează câte o cheie secretă partajată. De exemplu, dispozitivul de imitare trafic **102** poate utiliza cheia publică criptografică primită de la DUT **104**, împreună cu propria cheie de criptare privată pentru a genera o valoare a cheii secrete partajată. În mod similar, DUT **104** poate utiliza cheia publică criptografică primită de la dispozitivul de imitare trafic **102**, împreună cu propria cheie de criptare privată pentru a genera valoarea cheii secrete partajată. De exemplu, atât dispozitiv de imitare trafic **102** cât și DUT **104** sunt configurate pentru a genera o cheie secretă partajată. În unele exemple de realizare, dispozitivul de imitare trafic utilizează cheia sa privată criptografică (de exemplu, cheia criptografică privată "a") și cheia de criptare publică primită de la DUT (de exemplu cheia publică criptografică "B") pentru a determina un cheia secretă partajată "s", unde s este egal cu produsul dintre B^a și mod p. Mai exact, dispozitivul

102 de imitare trafic poate folosi de cheia criptografică "B" publică recepţionată pentru a calcula cheia secretă partajată "s_{te}", în cazul în care $s_{te} = B^a$ mod p, unde mod este o operație matematică de modul. În mod similar, DUT **104** poate utiliza cheia criptografică "A" publică recepţionată pentru a calcula cheia secretă partajată "s_{DUT}", unde $s_{DUT} = A^b$ mod p. De notat, S_{te} este egal cu s_{DUT}. De remarcat că valoarea cheii secrete partajată generată de fiecare dintre dispozitivele **102** de imitare trafic și DUT **104** va creşte la aceeași valoare și/sau la același număr și va fi, de asemenea, redusă în dimensiune sau lungime datorită cheii criptografice publice de bază și cheia criptografice private. Fiecare dintre dispozitivul **102** de imitare trafic și DUT **104** poate utiliza ulterior cheia secretă partajată pentru a stabili canale de comunicaţie pentru sesiunea de simulare testare (de exemplu, o sesiune de testare IPSec).

În etapa de la blocul **224**, este stabilit un canal de comunicaţie securizat IPsec. Conform unui exemplu de realizare, dispozitivul **102** de imitare trafic și DUT **104** utilizează cheia secretă partajată pentru a schimba cererea de canal de comunicaţie şi mesajele canalului pentru a stabili cel puțin un un canal IPsec între dispozitivul **102** de imitare de trafic și DUT **104**.

Figura 3 ilustrează o diagramă de flux a unei metode pentru reducerea mărimii unei chei criptografice într-un mediu de simulare testare, conform unui exemplu de realizare a prezentei invenţii. În etapa **302**, sunt determinate o dimensiune minimă de cheie (L_{min}) și o dimensiune maximă de cheie (L_{max}) pentru fiecare dintr-o multitudine de perechi de numere de schimbarea cheii de criptare. În unele exemple de realizare, un prim punct final de simulare testare (de exemplu, un dispozitiv de imitare testare) accesează o listă acceptabilă care conține intrările în baza de date a perechilor de numere de schimbarea cheii de criptare (perechile p-g Diffie-Hellman). Pentru fiecare pereche p-g unică, algoritmul determină și/sau desemnează o lungime maximă şi o lungime miniimă de cheie. De exemplu, pentru o prima pereche p-g, algoritmul poate stabili că L_{min} = 160 bytes și L_{max} = 256 bytes. Cu toate acestea, pentru o a doua pereche p-g (de exemplu, în cazul în care p este mai mare), algoritmul poate stabili că L_{min} = 256 bytes și L_{max} = 512 bytes.

În etapa de la blocul **304**, dimensiunea cheii minime și dimensiunea cheii maxime sunt utilizate pentru a obține o constantă de dimensionare cheie pentru fiecare pereche de numere de schimbarea cheii de criptare. Conform unor exemple, algoritmul poate deriva o constantă de dimensionare cheie ("k") prin calcularea coeficientului de L_{min} și L_{max}. Mai precis, $k = L_{min}/L_{max}$. În cele din urmă, algoritmul determină o constantă de

dimensionare cheie pentru fiecare pereche de numere de schimbarea cheii de criptare bazată pe faptul că valorile L_{max} şi L_{min} sunt asociate perechii p-g. De notat că acest calcul al constantelor de dimensionare cheie este efectuat înainte de inițierea oricăror sesiuni de simulare testare (de exemplu, simulări de testare IPSec).

În etapa de la blocul **306**, fiecare constantă de dimensionare cheie este stocată cu perechea sa de numere de schimbarea cheii de criptare asociată. Conform unor exemple, algoritmul poate înregistra respectiv și/sau mapa constantele de dimensionare cheie derivate a perechilor p-g corespunzătoare din înregistrările în baza de date (de exemplu, conținute într-o bază de date locală sau externă).

În etapa de la blocul **308**, este selectată o pereche de numere de schimbarea cheii de criptare pentru utilizare într-o sesiune de simulare testare. În unele exemple de realizare, primul punct final de simulare testare (de exemplu, un dispozitiv de imitare testare) și al doilea punct final de simulare testare (de exemplu, a DUT) sunt configurate pentru a efectua o sesiune de simulare testare (de exemplu, o simulare de test IPSec). Înainte de stabilirea sau de deschiderea unei simulări de testarea de canal de comunicaţie IPSec, primul punct final de simulare testare și al doilea punct final de simulare poate negocia valorile p și g care să fie utilizate pentru a determina cheile criptografice și valoarea secretă partajată. În unele exemple de realizare, primul punct final de simulare testare poate propune una sau mai multe perechi de numere de schimbarea cheii de criptare la al doilea punct final de simulare test. Ca răspuns, al doilea punct final de simulare test poate i) selecta o singură pereche de numere de schimbarea cheii de criptare dintre grupurile incluse în listă sau ii) să respingă toate perechile de numere de schimbarea cheii de criptare propuse. În cazul în care al doilea punct final de simulare test indică faptul că este necesară o anumită pereche de numere de schimbarea cheii de criptare, al doilea punct final de simulare de test va transmite un mesaj care indică selecția sa la primul punct final de simulare test.

Conform unor exemple de realizare, dispozitivul de imitare trafic poate transmite un mesaj care conține o multitudine de valori p pentru DUT. De exemplu, dispozitivul de imitare de trafic poate transmite valorile p-g potențiale p-g $pair_1$ p-g $pair_2$, p-g $pair_3$, p-g $pair_4$, și p-g $pair_5$. La primirea mesajului ce conține valorile potențiale ale perechii p-g, DUT face o determinare dacă p-g $pair_1$ poate fi utilizată pentru simulare a de testare. Dacă p-g $pair_1$ poate fi utilizată de către DUT, apoi DUT utilizează în cele din urmă valorile p și g din $pair_1$ p-g pentru a genera o cheie criptografică B publice.

Dacă perechea p-g $pair_1$ nu poate fi folosită (de exemplu, este incompatibilă) de DUT, DUT apoi determină dacă una dintre perechile p-g $pair_2$, p-g $pair_3$, p-g $pair_4$, și p-g $pair_5$ poate fi utilizată în simulare a de testare. Dacă se constată că una dintre perechile p-g $pair_2$, p-g $pair_3$, p-g $pair_4$, și p-g $pair_5$ poate fi utilizată, atunci DUT transmite un mesaj de notificare către dispozitivul de imitare trafic indicând o pereche p-g desemnată de DUT. Dacă se stabilește că niciuna dintre perechile p-g $pair_1$, p-g $pair_2$, p-g $pair_3$, p-g $pair_4$, și p-g $pair_5$ nu poate fi utilizată de către DUT, acesta transmite un mesaj la dispozitivul de imitare trafic indicând faptul că toate perechile p-g furnizate anterior sunt incompatibile.

În etapa de la blocul **310**, constanta de dimensionare cheie asociată cu perechea de numere de schimbarea cheii de criptare selectată este selectată pentru utilizarea în sesiunea de simulare testare pentru a fi stabilită. În unele exemple de realizare, primul punct final de simulare de test (care găzduiește algoritmul) poate primi mesajul care indică perechea de numere de schimbarea cheii de criptare aleasă de al doilea dispozitiv de punct final de simulare testare și, ulterior, accesează intrările în baza de date, folosind perechea de numere de schimbarea cheii de criptare selectată asociată cu constanta de dimensionare cheie.

În etapa de la blocul **312**, este generată o cheie criptografică privată folosind constanta de dimensionare cheie selectată. Conform unor exemple de realizare, primul punct final de simulare test determină ca mărimea cheii criptografice privată să fie generată. De exemplu, primul punct final de simulare testare poate stabili dimensiunea cheii criptografice privată prin înmulțirea unei lungimi a cheii implicite (de ex, o lungime a cheii sau dimensiunea care este de obicei folosită pentru securitatea criptării în condiții de rețea reală) cu constanta de dimensionare (k) cheie selectată. După efectuarea acestei determinări, algoritmul poate genera cheia criptografică privată, în conformitate cu mărimea cheii determinate.

La etapa **314**, canalul de comunicaţie de simulare testare se stabilește cel puțin cu ajutorul cheii criptografice private de dimensiuni reduse. Conform unor exemple, dispozitivul de imitare testare stabilește un canal de comunicaţie IPsec cu un DUT folosind cheia privată criptografică a dispozitivului imitare testare. În special, canalul de comunicaţie IPSec poate fi stabilit folosind o cheie criptografică privată generată de DUT, precum și valoarea secretă partajată care este derivată de oricare din cheile private. Mai exact, pentru a finaliza negocierea, fiecare dintre dispozitivul de imitare

a 2015 00986
10/12/2015

trafic şi DUT utilizează cheia sa secreta partajată pentru a stabili sesiunea canalului de comunicaţie IPsec.

Se va înţelege că diverse detalii referitoare obiectul dezvăluit în prezenta cerere de brevet pot fi schimbate fără a ne îndepărta de la scopul prezentei invenţii. În plus, descrierea de mai sus este în scop de prezentare şi nu în scopul limitării.

a 2015 00986
10/12/2015

REVENDICĂRI

1. Metodă pentru reducerea dimensiunii unei chei criptografice într-un mediu de simulare a testării care constă în:
   - determinarea, printr-un punct final de simulare a testării, a unei valori minime și a unei valori maxime a dimensiunii cheii de criptare pentru o cheie criptografică privată pentru fiecare dintr-o multitudine de perechi de numere de schimbarea cheii de criptare;
   - delimitarea, pentru fiecare din multitudinea de perechi de numere de schimbarea cheii de criptare, a unei constante de dimensionare cheie în funcție de valoarea minimă și valoarea maximă a dimensiunii cheii;
   - stocarea fiecărei dintre multitudinea de perechi selectate de numere de schimbarea cheii de criptare și a constantei de dimensionare cheie într-un dispozitiv de stocare date;
   - selectarea unei perechi de numere de schimbarea cheii de criptare pentru a fi aplicată la o sesiune de simulare testare efectuată între un prim punct final de simulare testare și un al doilea punct final de simulare testare, și
   - generarea unei chei criptografice privată în funcție de constanta de dimensionare cheie asociată cu perechea selectată de numere de schimbarea cheii de criptare.
2. Metodă, conform revendicării 1, **caracterizată prin aceea că** perechea selectată de numere de schimbarea cheii de criptare este determinată prin negociere între primul punct final de simulare testare și al doilea punct final de simulare testare.
3. Metodă, conform revendicării 1, **caracterizată prin aceea că** mai constă în generarea, prin primul punct final de simulare testare, a unei chei secrete partajată prin utilizarea unei chei publice criptografice recepționate de la al doilea punct final de simulare testare și a cheii de criptare privată generate.
4. Metodă, conform revendicării 1, **caracterizată prin aceea că** generarea cheii criptografice privată în funcție de constanta de dimensionare cheie constă în accesarea bazei de date pentru a obține constanta de dimensionare cheie folosind perechea selectată de numere de schimbarea cheii de criptare.
5. Metodă, conform revendicării 1, **caracterizată prin aceea că** atât primul punct final de simulare testare cât și al doilea punct final de simulare testare sunt componente

ale unui singur dispozitiv de imitare testare care sunt, din punct de vedere al comunicaţiei, conectate printr-un dispozitiv supus testării.

6. Metodă, conform revendicării 1, **caracterizată prin aceea că** primul punct final de simulare testare este un dispozitiv de imitare testare și al doilea punct final de simulare testare este un dispozitiv supus testării.
7. Metodă, conform revendicării 1, **caracterizată prin aceea că** delimitarea constantei de dimensionare de cheie include împărțirea valorii dimensiunii cheii minime la valoarea dimensiunii cheii maxime.
8. Sistem pentru reducerea dimensiunii unei chei criptografice într-un mediu de simulare a testării, sistemul cuprinzând:
   - un dispozitiv de imitare trafic configurat pentru a determina, înainte de inițierea unei sesiuni de de simulare testare cu un dispozitiv de testat (DUT), a unei valori minime și a unei valori maxime a dimensiunii cheii de criptare pentru o cheie criptografică privată pentru fiecare dintr-o multitudine de perechi de numere de schimbarea cheii de criptare, pentru a delimita, pentru fiecare din multitudinea de perechi de numere de schimbarea cheii de criptare, o constantă de dimensionare cheie în funcție de valoarea minimă și valoarea maximă a dimensiunii cheii, pentru a stoca fiecare dintre multitudinea de perechi selectate de numere de schimbarea cheii de criptare și constanta de dimensionare cheie într-un dispozitiv de stocare date şi pentru a genera o cheie criptografică privată în funcție de constanta de dimensionare cheie asociată cu perechea selectată de numere de schimbarea cheii de criptare pentru aplicarea la o sesiune de simulare a testării efectuată între dispozitivul de imitare trafic şi DUT
9. Sistem, conform revendicării 8, **caracterizat prin aceea că** perechea selectată de numere de schimbarea cheii de criptare este determinată prin negociere între primul între dispozitivul de imitare trafic şi DUT.
10. Sistem, conform revendicării 8, **caracterizat prin aceea că** mai cuprinde generarea, prin dispozitivul de imitare trafic, a unei chei secrete partajată prin utilizarea unei chei publice criptografice recepţionate de la DUT și a cheii de criptare privată generate.
11. Sistem, conform revendicării 8, **caracterizat prin aceea că** dispozitivul de imitare trafic este configurat suplimentar pentru a accesa baza de date pentru a obține constanta de dimensionare cheie folosind perechea selectată de numere de schimbarea cheii de criptare.

12. Sistem, conform revendicării 8, **caracterizat prin aceea că** dispozitivul de imitare trafic include o componentă client și o componentă server care sunt în mod comunicativ conectate prin DUT.
13. Sistem, conform revendicării 8, **caracterizat prin aceea că** delimitarea constantei de dimensionare de cheie include împărțirea valorii dimensiunii cheii minime la valoarea dimensiunii cheii maxime.
14. Suport non-tranzitoriu care poate fi citit de calculator care conţin instrucţiuni executabile de calculator care atunci când sunt executate de către un procesor, comandă calculatorul să efectueze etapele care constau în: - determinarea, printr-un punct final de simulare a testării, a unei valori minime și a unei valori maxime a dimensiunii cheii de criptare pentru o cheie criptografică privată pentru fiecare dintr-o multitudine de perechi de numere de schimbarea cheii de criptare;
    - delimitarea, pentru fiecare din multitudinea de perechi de numere de schimbarea cheii de criptare, a unei constante de dimensionare cheie în funcție de valoarea minimă și valoarea maximă a dimensiunii cheii;
    - stocarea fiecărei dintre multitudinea de perechi selectate de numere de schimbarea cheii de criptare și a constantei de dimensionare cheie într-un dispozitiv de stocare date;
    - selectarea unei perechi de numere de schimbarea cheii de criptare pentru a fi aplicată la o sesiune de simulare testare efectuată între un prim punct final de simulare testare și un al doilea punct final de simulare testare, și
    - generarea unei chei criptografice privată în funcție de constanta de dimensionare cheie asociată cu perechea selectată de numere de schimbarea cheii de criptare.
15. Suport non-tranzitoriu, conform revendicării 14, **caracterizat prin aceea că** perechea selectată de numere de schimbarea cheii de criptare este determinată prin negociere între primul punct final de simulare testare și al doilea punct final de simulare testare.
16. Suport non-tranzitoriu, conform revendicării 14, **caracterizat prin aceea** mai conţine generarea, prin primul punct final de de simulare testare, a unei chei secrete partajată prin utilizarea unei chei publice criptografice recepţionate de la al doilea punct final de simulare testare și a cheii de criptare privată generate.
17. Suport non-tranzitoriu, conform revendicării 14, **caracterizat prin aceea** generarea cheii criptografice privată în funcţie de constanta de dimensionare cheie constă în

accesarea bazei de date pentru a obține constanta de dimensionare cheie folosind perechea selectată de numere de schimbarea cheii de criptare.

18. Suport non-tranzitoriu, conform revendicării 14, **caracterizat prin aceea** atât primul punct final de simulare testare cât și al doilea punct final de simulare testare sunt componente ale unui singur dispozitiv de imitare testare care este, din punct de vedere al comunicaţiei, conectat printr-un dispozitiv supus testării.
19. Suport non-tranzitoriu, conform revendicării 14, **caracterizat prin aceea** primul punct final de simulare testare este un dispozitiv de imitare testare și al doilea punct final de simulare testare este un dispozitiv supus testării.
20. Suport non-tranzitoriu, conform revendicării 14, **caracterizat prin aceea** delimitarea constantei de dimensionare de cheie include împărțirea valorii dimensiunii cheii minime la valoarea dimensiunii cheii maxime.

a 2015 00986
10/12/2015

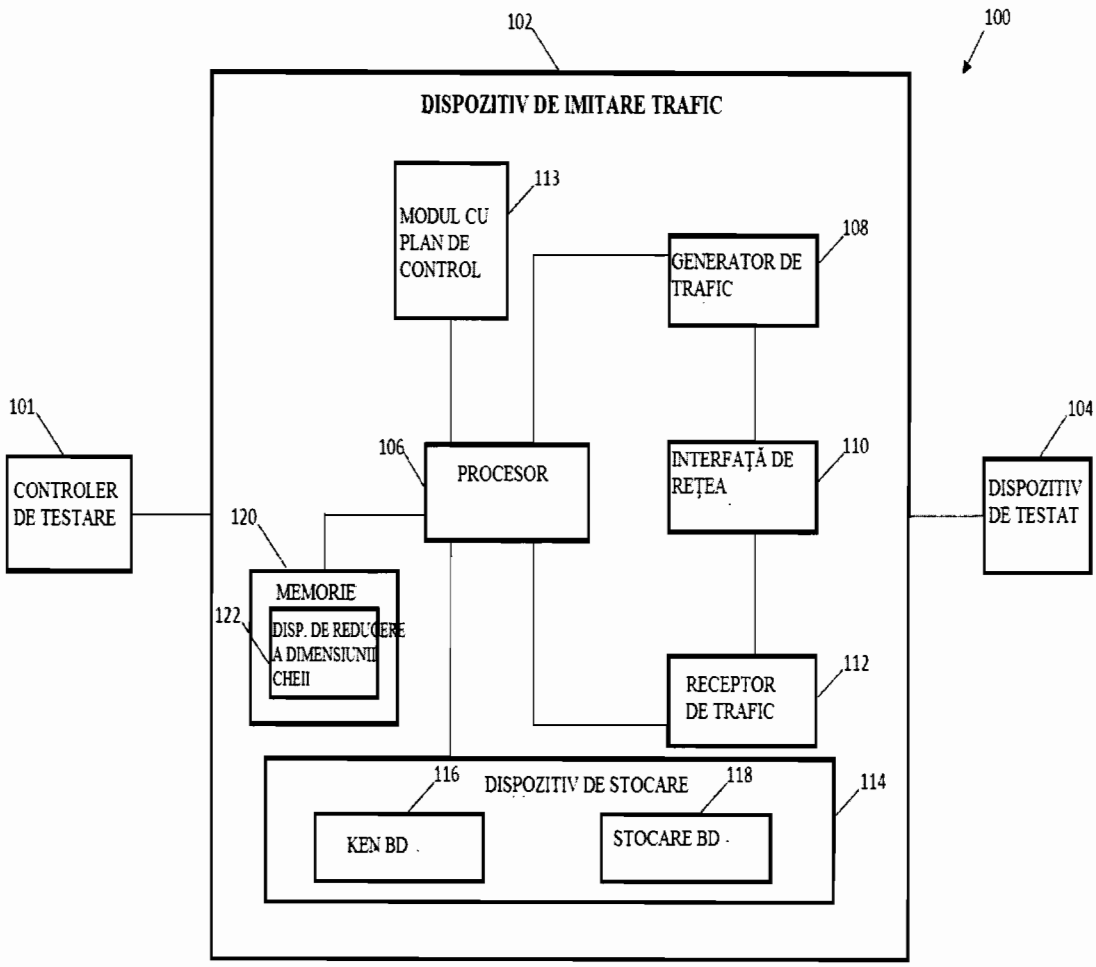

FIG. 1

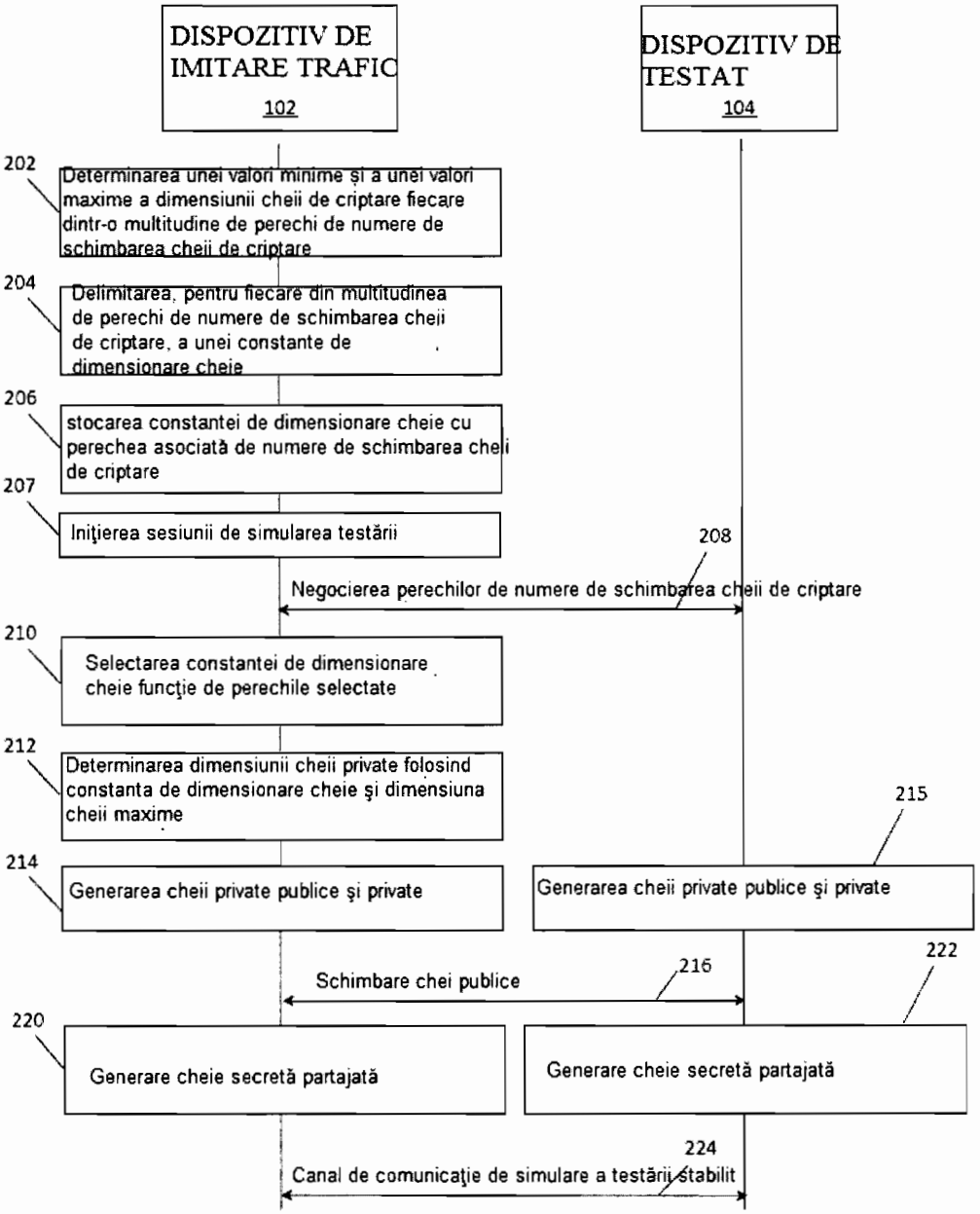
DISPOZITIV DE IMITARE TRAFIC
102
DISPOZITIV DE TESTAT
104
202
Determinarea unei valori minime şi a unei valori maxime a dimensiunii cheii de criptare fiecare dintr-o multitudine de perechi de numere de schimbarea cheii de criptare
204
Delimitarea, pentru fiecare din multitudinea de perechi de numere de schimbarea cheii de criptare, a unei constante de dimensionare cheie
206
stocarea constantei de dimensionare cheie cu perechea asociată de numere de schimbarea cheii de criptare
207
Iniţierea sesiunii de simularea testării
208
Negocierea perechilor de numere de schimbarea cheii de criptare
210
Selectarea constantei de dimensionare cheie funcţie de perechile selectate
212
Determinarea dimensiunii cheii private folosind constanta de dimensionare cheie şi dimensiuna cheii maxime
214
Generarea cheii private publice şi private
215
Generarea cheii private publice şi private
216
Schimbare chei publice
220
Generare cheie secretă partajată
222
Generare cheie secretă partajată
224
Canal de comunicaţie de simulare a testării stabilit

FIG. 2

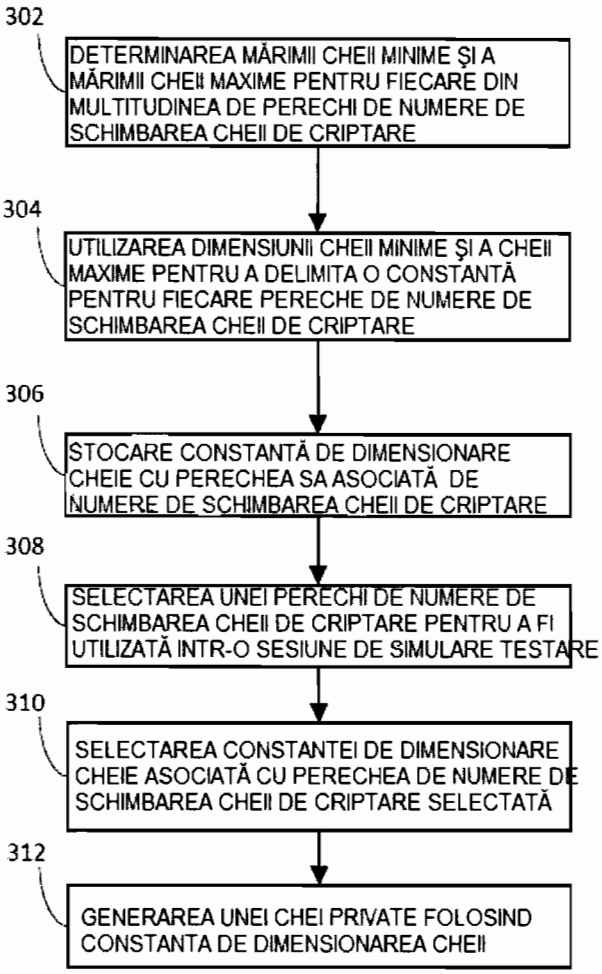
302
DETERMINAREA MĂRIMII CHEII MINIME ŞI A MĂRIMII CHEII MAXIME PENTRU FIECARE DIN MULTITUDINEA DE PERECHI DE NUMERE DE SCHIMBAREA CHEII DE CRIPTARE
304
UTILIZAREA DIMENSIUNII CHEII MINIME ŞI A CHEII MAXIME PENTRU A DELIMITA O CONSTANTĂ PENTRU FIECARE PERECHE DE NUMERE DE SCHIMBAREA CHEII DE CRIPTARE
306
STOCARE CONSTANTĂ DE DIMENSIONARE CHEIE CU PERECHEA SA ASOCIATĂ DE NUMERE DE SCHIMBAREA CHEII DE CRIPTARE
308
SELECTAREA UNEI PERECHI DE NUMERE DE SCHIMBAREA CHEII DE CRIPTARE PENTRU A FI UTILIZATĂ INTR-O SESIUNE DE SIMULARE TESTARE
310
SELECTAREA CONSTANTEI DE DIMENSIONARE CHEIE ASOCIATĂ CU PERECHEA DE NUMERE DE SCHIMBAREA CHEII DE CRIPTARE SELECTATĂ
312
GENERAREA UNEI CHEI PRIVATE FOLOSIND CONSTANTA DE DIMENSIONAREA CHEII

FIG. 3