(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 127706 B1**

(51) Int.Cl.
H04L 9/12 (2006.01);
H04L 9/14 (2006.01);
H04L 9/32 (2006.01)

(12) # BREVET DE INVENŢIE

(21) Nr. cerere: **a 2010 01303**

(22) Data de depozit: **09.12.2010**

(45) Data publicării menţiunii acordării brevetului: **30.09.2014** BOPI nr. **9/2014**

(41) Data publicării cererii:
30.07.2012 BOPI nr. **7/2012**

(73) Titular:
• **UNIVERSITATEA TEHNICĂ DIN CLUJ-NAPOCA**, *STR.MEMORANDUMULUI NR.28, CLUJ-NAPOCA, CJ, RO*

(72) Inventatori:
• **AŞTILEAN ADINA**, *ALEEA CIOPLEA NR.9, BL.S 9, SC.2, ET.2, AP.26, CLUJ-NAPOCA, CJ, RO;*
• **FOLEA SILVIU**, *STR.METEOR NR.6, BL.O Z2, SC.2, ET.3, AP.21, CLUJ-NAPOCA, CJ, RO;*
• **AVRAM CAMELIA**, *STR.REPUBLICII NR.74/E, AP.7, TÂRNĂVENI, MS, RO;*
• **HULEA MIHAI**, *STR.BISTRIŢEI NR.7, CLUJ-NAPOCA, CJ, RO;*
• **MIRON RADU FLORIN**, *STR.SLĂNIC NR.5, AP.11, CLUJ-NAPOCA, CJ, RO;*
• **LEŢIA TIBERIU ŞTEFAN**, *STR.MESTECENILOR NR.8, AP.19, CLUJ-NAPOCA, CJ, RO;*
• **CIUPAN EMILIA**, *STR.MESTECENILOR NR.6, AP.2, CLUJ-NAPOCA, CJ, RO*

(74) Mandatar:
CABINET DE PROPRIETATE INDUSTRIALĂ CIUPAN CORNEL, *STR. MESTECENILOR NR. 6, BL. 9E, AP. 2, CLUJ NAPOCA, JUDEŢUL CLUJ*

(56) Documente din stadiul tehnicii:
WO 2007/117914 A2; EP 1077555 A2; US 2006/0242423 A1; EP 1370022 A1

(54) # METODĂ SECURIZATĂ DE COMUNICAŢIE ÎNTRE DISPOZITIVE FIXE ŞI MOBILE

Examinator: **ing. CRISTUDOR DANA**

RO 127706 B1

Invenția se referă la o metodă securizată de comunicație între dispozitive fixe şi mobile, pe baza amprentelor digitale, în vederea accesului la "Internet Banking", ATM, într-o zonă cu acces limitat sau la o componentă software. De asemenea, metoda poate fi utilizată şi numai în scopul identificării personale, la distanță, a utilizatorilor.

Este cunoscută invenția **KR 20010039815 A**, care prezintă un sistem şi o metodă de criptare, utilizate în transmiterea de date. Acestea presupun existența unor mijloace hardware şi software atât la emisie, cât şi la recepție, şi parcurgerea unor etape precise. Într-o primă fază, care se derulează la partea transmițătoare, se reține, în memoria unui dispozitiv de memorare, amprentele persoanelor autorizate să acceseze sistemul, mai precis, caracteristicile amprentelor într-o formă criptată. La folosirea sistemului, se citeşte amprenta utilizatorului, se extrag caracteristicile acesteia şi se compară cu cele stocate anterior în memoria dispozitivului de memorare. Dacă există o corespondență între amprenta citită şi una dintre amprentele memorate anterior, atunci se generează o cheie de criptare Y, care va servi la criptarea unui mesaj introdus de utilizator de la o tastatură sau selectat dintr-o listă de mesaje afişate pe un display. În continuare, se decriptează caracteristicile amprentelor memorate anterior şi criptate cu un algoritm general, se compară cu caracteristicile amprentei examinate şi, pe baza comparației, se determină un scor care este apoi folosit la generarea unei a doua chei de criptare X. Cheia X este folosită în continuare la criptarea caracteristicilor amprentei examinate. Mesajul transmis părții receptoare este format din ID-ul utilizatorului a cărui amprentă a fost citită, din caracteristicile amprentei citite, criptată cu cheia X, şi din mesajul propriu-zis, introdus de utilizator, criptat cu ajutorul cheii Y. La partea receptoare, mesajul recepționat este prelucrat şi analizat după aceeaşi logică, dar parcursă în sens invers.

Sistemul şi metoda, descrise în brevetul **KR 20010039815 A**, prezintă mai multe dezavantaje, unul dintre cele mai importante fiind acela că necesită transportul prealabil al unor informații inițiale de la emisie la recepție, sub formă înregistrată. Sistemul necesită o multitudine de dispozitive hardware şi software, plasate atât la emițător, cât şi la receptor; dispozitivele părții transmițătoare par a fi plasate într-o locație fixă.

De asemenea, metoda descrisă în brevetul **KR 20010039815 A** nu beneficiază de o fundamentare matematică corespunzătoare, probabilitatea de a genera aceeaşi cheie de două ori nefiind suficient studiată.

Problema tehnică, pe care o rezolvă invenția, este realizarea unei comunicații securizate între dispozitive fixe şi mobile.

Metoda securizată de comunicație, conform invenției, presupune transmiterea-receptarea unui mesaj criptat, folosind un algoritm de criptare cu cheie simetrică şi cu durată de viață limitată. Metoda de generare a cheii simetrice se bazează pe un algoritm de tipul Diffie-Hellman şi utilizează informațiile rezultate din citirea amprentei digitale a participanților la sesiunea de comunicație (minuțiile) şi pe cele referitoare la pozițiile acestora. Autentificarea se realizează conform unui protocol, care implică, pe lângă cele două informații enumerate mai sus (amprenta digitală şi poziția utilizatorului), codurile de identitate ale entităților implicate în procesul de comunicație, precum şi numărul sesiunii de comunicație între utilizatorii implicați. Acesta modifică cele două coduri de identitate, conform unui algoritm prestabilit.

Metoda de securizare a comunicației între dispozitive fixe şi mobile, conform invenției, prezintă următoarele avantaje:

- generarea automată a unei chei unice pe sesiune, aceeaşi la emisie şi recepție, fără a necesita, sub nicio formă, transportul prealabil şi riscant al unor date înregistrate. Volumul necesar de date memorate este mic;

- metoda se bazează pe o combinație formată nu numai din elemente de unicitate caracteristice persoanei (amprenta), ci şi din elemente de unicitate generate prin aplicarea unor funcții cunoscute (SHA), ale căror proprietăți au fost riguros stabilite;

- pentru realizarea comunicației, nu este neapărat necesar ca utilizatorul să dispună de un calculator sau de un telefon mobil, fiind suficient un dispozitiv hardware mobil, special realizat şi prevăzut cu o unitate de procesare şi capacitate de memorie. Dispozitivul se caracterizează prin costuri, dimensiuni şi consum de putere reduse, şi este prevăzut cu posibilități de comunicație radio, bazate pe tehnologii larg răspândite (Wi-Fi, Bluetooth, GPRS);

- dispozitivul hardware, utilizat la citirea amprentei, la generarea cheii de criptare şi la criptarea informațiilor de transmis, este mobil, cu precizarea că utilizarea acestuia trebuie să se facă în perimetrul unor locații prestabilite;

- terminalul mobil (aflat la partea transmițătoare) nu trebuie să dispună de o bază de date care să stocheze informațiile folosite la compararea cu amprenta citită. Această bază de date este stocată la nivelul unui server de aplicație distribuit;

- includerea informației, privind poziția actuală şi poziția anterioară a utilizatorilor, printre informațiile care fac obiectul verificării înaintea autorizării accesului, sporeşte securitatea comunicației.

Se dă, în continuare, un exemplu de realizare a invenției, în legătură cu fig. 1...3, care reprezintă:

- fig. 1, arhitectura hardware a sistemului de acces securizat;
- fig. 2, arhitectura software a sistemului de acces securizat;
- fig. 3, schema de generare a cheii unice pe sesiune.

Sistemul de acces securizat permite comunicația între dispozitive mobile (subsistem emițător) şi dispozitive fixe (subsistem receptor) sau între dispozitive fixe (adică între emițător fix şi receptor fix). Un subsistem emițător **1** are în componența sa un cititor de amprentă FPS (Finger Print Sensor), prevăzut cu unitate de memorare şi procesare, cu posibilitate de comunicare utilizând tehnologiile Bluetooth, Wi-Fi (la distanță mică) sau GPRS (la distanță mare), un dispozitiv GPS (Global Positioning System) care comunică cu senzorul de amprentă FPS şi un terminal mobil MT (de exemplu, un telefon mobil sau un PDA) care are înglobată tehnologie GPRS, sau un PC, prin intermediul acestui ultim dispozitiv (MT sau PC), realizându-se, de regulă, conectarea la subsistemul receptor **2**. Conectarea unui subsistem emițător **1**, cu subsistemul receptor **2**, se poate realiza într-un punct de acces **4**, cu ajutorul tehnologiei de comunicație fără fir sau într-un nod de comunicație **3**, prin intermediul unei legături fizice (cu fir). Subsistemul receptor **2** constă într-un server de aplicație distribuit S_x, x= 1, 2, ..., m, conectat la Internet, serverele componente S_x, x= 1, 2, ..., m fiind fixe.

Metoda de securizare, conform invenției, este implementată pe un dispozitiv hardware, mobil, FPS, special realizat, prevăzut cu o unitate de procesare şi capacitate de memorie. Dispozitivul FPS este prevăzut cu posibilități de comunicație radio, bazate pe tehnologii larg răspândite (Wi-Fi, Bluetooth, GPRS). Nu este necesară, în mod obligatoriu, existența suplimentară a unui PC sau a unui telefon mobil, dispozitivul putând funcționa şi independent.

Operațiile destinate procesării locale a amprentelor au loc la nivelul dispozitivului FPS şi sunt urmate de transmiterea informațiilor esențiale (amprentele, locația şi codul de identificare) către un server de aplicație distribuit. Validarea datelor şi accesul sunt posibile numai în locații având poziții predefinite, care pot fi determinate folosind GPS-ul în exteriorul clădirilor, respectiv, cu ajutorul tehnologiei Wi-Fi, în interiorul clădirilor. Transmiterea securizată a informațiilor între entitățile implicate se poate face utilizând tehnologii de comunicație fără fir (Wi-Fi, Bluetooth sau GPRS) sau cu fir.

În cazul subsistemului emițător **1**, cheia de criptare unică pe sesiune se generează la nivelul dispozitivului FPS, fără a necesita transportul prealabil şi riscant al unor date înregistrate.

Inițializarea sesiunii de comunicație pe canalul securizat şi prelucrarea datelor în vederea autorizării accesului la informație se realizează folosind un server de aplicație, la nivelul căruia sunt verificate amprentele, locația şi codurile de identificare. Acestea sunt stocate într-un sistem distribuit de baze de date.

Comunicația cu fir este utilizată doar între PC-uri, prin intermediul unor noduri de comunicație. Terminalele mobile MT şi calculatoarele PC comunică cu senzorul de amprentă FPS şi cu receptorul GPS, folosind tehnologie Bluetooth B sau Wi-Fi (W).

Conform fig. 2, aplicația software, care rulează pe terminalul mobil (calculator sau telefon mobil), conține funcțiile prezentate în continuare, împreună cu rolurile acestora:

- FPSFunction - realizează interfața cu senzorul de amprentare;
- GPSReader - citeşte periodic datele de la receptorul GPS;
- BluetoothInterface - comunicația cu senzorul de amprentare şi receptorul GPS se face folosind tehnologia Bluetooth. Această interfață interpretează datele din formatul Bluetooth şi le converteşte într-un format utilizat mai departe;
- Autentification - modulul realizează verificarea şi identificarea locală a amprentei;
- Security - informațiile transmise către/dinspre server sunt criptate/decriptate folosind mai mulți algoritmi de criptare, în funcție de nivelul de securitate impus;
- GPRSComm / WiFiLAN - în funcție de tipul de acces la Internet, informația este structurată pe pachete de date (GSM sau LAN).

Terminalele mobile MT sau/şi serverul sunt inițializate cu amprentele martor ale partenerilor de dialog, date de senzorul FPS şi pozițiile lor furnizate de receptorul GPS sau determinate prin tehnologia Wi-Fi.

Protocolul de autentificare şi asigurare a confidențialității informațiilor transmise între dispozitive fixe şi mobile se bazează pe execuția următorului algoritm de pe un terminal mobil MT sau de pe server, ce execută:

- autentificarea utilizatorului terminalului prin citirea amprentei şi compararea acesteia cu amprenta martor, de care trebuie să difere cu mai puțin decât o valoare specificată;
- citirea poziției curente a terminalului;
- crearea cheii parțiale de criptare K' din amprenta curentă şi poziția curentă.
- transmiterea cheii K', partenerului de dialog;
- recepționarea cheii parțiale de criptare similare, K", de la partenerul de dialog.
- calculul cheii de criptare K din cheile parțiale K' şi K";
- criptarea cu ajutorul cheii K şi transmiterea spre partenerul de dialog a informațiilor cuprinse în amprenta curentă, poziția curentă, poziția anterioară şi identificatorul sesiunii;
- recepționarea, de la partenerul de dialog, a unui mesaj criptat cu ajutorul cheii K, ce conține informațiile cuprinse în amprenta curentă, poziția curentă, poziția anterioară şi identificatorul sesiunii;
- extragerea, prin decriptare, din mesajul primit, a informațiilor cuprinse în amprenta curentă a partenerului de dialog, a poziției sale curente şi anterioare;
- compararea amprentei curente a partenerului de dialog cu cea martor, corespunzătoare. Se refuză dialogul, dacă diferența dintre amprenta transmisă a partenerului şi cea martor corespunzătoare diferă cu mai mult decât o valoare specificată, sau poziția anterioară nu coincide cu cea stocată în terminalul curent;
- actualizarea pozițiilor celor două perechi de terminale mobile;
- desfăşurarea sesiunii de comunicație în mod criptat;
- închiderea sesiunii de lucru.

Generarea cheii unice pe sesiune şi transmiterea acesteia între utilizatori, conform fig. 3, se bazează pe algoritmul Diffie-Hellman, modificat, noutatea constând în modul în care se generează exponenţii cheii secrete. Caracteristicile distinctive ale acestor exponenţi se datorează caracteristicilor diferite ale amprentei, respectiv, minuţiilor, precum şi aplicării funcţiilor Hash, în scopul prelucrării minuţiilor. Chiar şi în cazul aceleiaşi persoane, citirea succesivă a aceleiaşi amprente prezintă modificări, datorită poziţionării diferite a degetului pe cititorul de amprente.

Suplimentar, aplicarea funcţiilor SHA asupra şirului de biţi, care reprezintă un număr de minuţii, va conduce la reprezentări binare sensibil diferite, pentru fiecare citire de amprentă.

Aceste şiruri de biţi vor fi partajate şi transmise bidirecţional între cele două terminale (emiţător - receptor), pentru a genera cheia secretă.

Generarea cheii private K, din algoritmul de autentificare şi asigurarea confidenţialităţii informaţiilor prezentate mai sus se realizează parcurgând următorii paşi:

- se concatenează şirul de biţi care reprezintă minuţiile cu şirul de biţi care reprezintă poziţia utilizatorului;
- se aplică un algoritm de tipul Secure Hash Algorithm (SHA) şirului de biţi;
- se segmentează şirul de caractere rezultate în urma aplicării funcţiei SHA, în scopul efectuării operaţiilor ulterioare; subşirurile obţinute la cele două terminale sunt notate cu t_{ij} (unde i reprezintă numărul terminalului, iar j ia valori de la 1 până la valoarea corespunzătoare numărului de subşiruri);
- se alege un număr prim, notat cu b în fig. 3;
- se alege un număr prim, suficient de mare, p;
- terminalul 1 calculează valorile $u_1 = b^t_{1j}$, mod p;
- terminalul 1 transmite, utilizatorului 2, valorile b, p şi u_1;
- terminalul 2 calculează valorile $u_2 = b^t_{2j}$, mod p;
- terminalul 2 transmite, utilizatorului 1, valorile u_2;
- ambii utilizatori calculează aceleaşi componente ale cheii secrete K_j:

$$K_j = b^t_{1j} * ^t_{2j}, \text{ mod } p, \text{ pentru } j = 1, 2,...n;$$

- utilizând componentele K_j şi o relaţie de compunere prestabilită, la cele două terminale, se calculează aceeaşi cheie secretă K';
- în scopul obţinerii unei chei finale K, de lungime precizată, se aplică o funcţie SHA, cheii secrete K'.

Revendicări

1. Metodă securizată de comunicație între dispozitive fixe şi mobile, pentru transmiterea-receptarea unui mesaj criptat, folosind un algoritm de criptare cu cheie simetrică şi cu durată de viață limitată, **caracterizată prin aceea că**:

- se citesc amprentele celor doi utilizatori, care comunică cu un dispozitiv mobil FPS de citire a amprentei;
- se extrag minuțiile amprentelor;
- se citesc coordonatele GPS sau, în locații interioare, se utilizează tehnologia Wi-Fi, pentru precizarea pozițiilor utilizatorilor;
- se generează cheia privată, folosind datele achiziționate;
- se realizează autentificarea conform unui protocol care implică amprenta digitală şi poziția utilizatorului, codurile de identitate ale entităților implicate în procesul de comunicație, precum şi numărul sesiunii de comunicație între utilizatorii implicați, protocolul modificând cele două coduri de identitate, conform unui algoritm prestabilit, cheia de criptare fiind unică, pentru fiecare sesiune.

2. Metodă securizată de comunicație între dispozitive fixe şi mobile, conform revendicării 1, **caracterizată prin aceea că** generarea cheii secrete de criptare, unice pe sesiune, se realizează astfel:

- se concatenează şirul de biți care reprezintă minuțiile cu şirul de biți care reprezintă poziția utilizatorului;
- se aplică un algoritm de tipul Secure Hash Algorithm (SHA) şirului de biți;
- se segmentează şirul de caractere rezultate în urma aplicării funcției SHA, în scopul efectuării operațiilor ulterioare; subşirurile obținute la cele două terminale sunt notate cu t_{ij} (unde i reprezintă numărul terminalului, iar j ia valori de la 1 până la valoarea corespunzătoare numărului de subşiruri);
- se alege un număr prim, notat cu b;
- se alege un număr prim, suficient de mare, p;
- terminalul 1 calculează valorile $u_1 = b^t_{1j}$, mod p;
- terminalul 1 transmite, utilizatorului 2, valorile b, p şi u_1;
- terminalul 2 calculează valorile, $u_2 = b^t_{2j}$, mod p;
- terminalul 2 transmite, utilizatorului 1, valorile u_2;
- ambii utilizatori calculează aceleaşi componente ale cheii secrete K_j:

$$K_j = b^t_{1j} * ^t_{2j}, \text{ mod } p, \text{ pentru } j = 1, 2,...n;$$

- utilizând componentele K_j şi o relație de compunere prestabilită, la cele două terminale, se calculează aceeaşi cheie secretă K';
- în scopul obținerii unei chei finale K, de lungime precizată, se aplică o funcție SHA cheii secrete K'.

3. Metodă securizată de comunicație între dispozitive fixe şi mobile, conform revendicărilor 1 şi 2, **caracterizată prin aceea că** utilizează un protocol de autentificare şi asigurare a confidențialității informațiilor transmise între dispozitive fixe şi mobile, care se bazează pe un algoritm ce se execută pe un terminal mobil MT sau pe un server, astfel:

i) autentificarea utilizatorului terminalului prin citirea amprentei şi compararea acesteia cu amprenta martor, de care trebuie să difere cu mai puțin decât o valoare specificată;

ii) citirea poziției curente a terminalului;

iii) crearea cheii parțiale de criptare K' din amprenta curentă şi poziția curentă;

iv) transmiterea cheii K partenerului de dialog;

v) recepționarea cheii parțiale de criptare similare, K", de la partenerul de dialog;

vi) calculul cheii de criptare K din cheile parțiale K' şi K";

vii) criptarea cu ajutorul cheii K şi transmiterea, spre partenerul de dialog, a informațiilor cuprinse în amprenta curentă, poziția curentă, poziția anterioară şi identificatorul sesiunii;

viii) recepționarea, de la partenerul de dialog, a unui mesaj criptat, cu ajutorul cheii K ce conține informațiile cuprinse în amprenta curentă, poziția curentă, poziția anterioară şi identificatorul sesiunii;

ix) extragerea, prin decriptare, din mesajul primit, a informațiilor cuprinse în amprenta curentă a partenerului de dialog, a poziției sale curente şi anterioare;

x) compararea amprentei curente a partenerului de dialog cu cea martor corespunzătoare, se refuză dialogul dacă diferența dintre amprenta transmisă a partenerului şi cea martor corespunzătoare diferă cu mai mult decât o valoare specificată sau poziția anterioară nu coincide cu cea stocată în terminalul curent;

xi) actualizarea pozițiilor celor două perechi de terminale mobile;

xii) desfăşurarea sesiunii de comunicație în mod criptat;

xiii) închiderea sesiunii de lucru.

4. Metodă securizată de comunicație între dispozitive fixe şi mobile, conform revendicărilor 1, 2 şi 3, **caracterizată prin aceea că** cheia de criptare, unică pe sesiune, se generează la nivelul subsistemului emițător (**1**), de către dispozitivul mobil (**FPS**), prin intermediul unităților de procesare şi memorare, cu care acesta este prevăzut.

5. Metodă securizată de comunicație între dispozitive fixe şi mobile, conform revendicării 1, **caracterizată prin aceea că**, în cadrul informațiilor de autentificare, se include şi poziția actuală şi poziția anterioară a utilizatorului, poziție în jurul căreia se acceptă schimbul de informații.

6. Metodă securizată de comunicație între dispozitive fixe şi mobile, conform revendicării 1, **caracterizată prin aceea că**, la închiderea sesiunii de comunicație, valabilitatea cheii de criptare expiră.

(51) Int.Cl.
H04L 9/12 (2006.01);
H04L 9/14 (2006.01);
H04L 9/32 (2006.01)

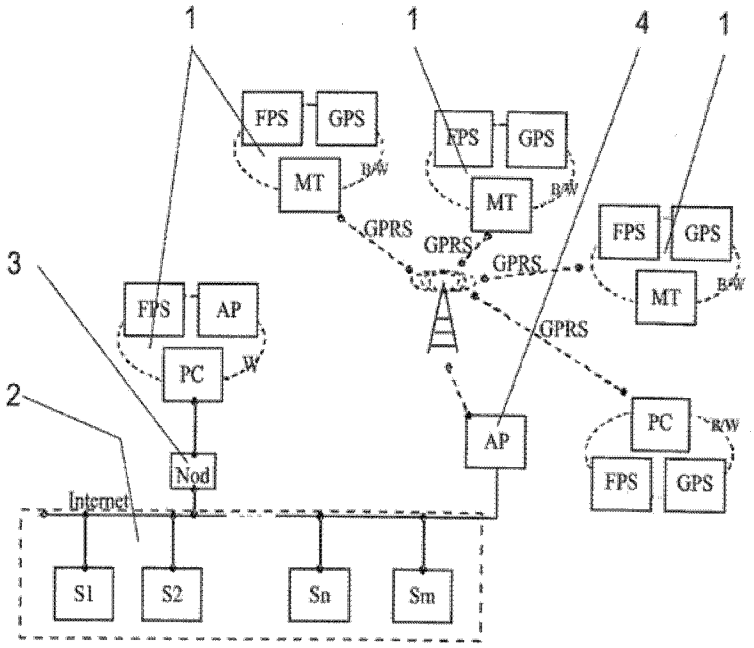

Fig. 1

(51) Int.Cl.
H04L 9/12 (2006.01);
H04L 9/14 (2006.01);
H04L 9/32 (2006.01)

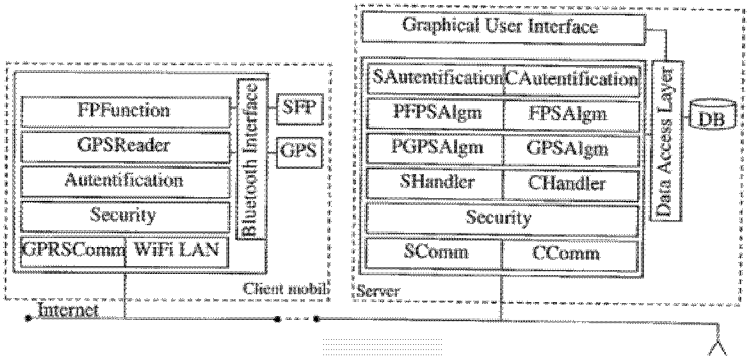

Fig. 2

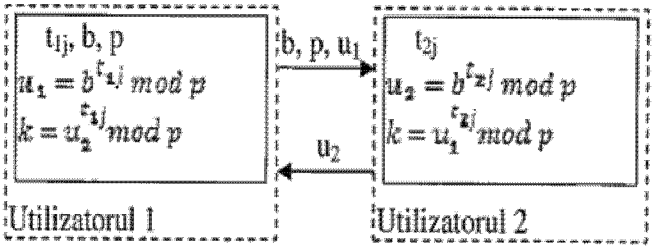

Fig. 3

Editare şi tehnoredactare computerizată - OSIM
Tipărit la: Oficiul de Stat pentru Invenţii şi Mărci
sub comanda nr. 654/2014