(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 130287 A0**
(51) Int.Cl.
H04L 9/08 (2006.01);
H04L 9/12 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2014 00436**

(22) Data de depozit: **12.06.2014**

(41) Data publicării cererii:
29.05.2015 BOPI nr. **5/2015**

(71) Solicitant:
• **FĂLIE DRAGOŞ**,
*STR. BANUL DUMITRACHE NR. 51,
SECTOR 2, BUCUREŞTI, B, RO*

(72) Inventatori:
• **FĂLIE DRAGOŞ**,
*STR. BANUL DUMITRACHE NR. 51,
SECTOR 2, BUCUREŞTI, B, RO*

(54) # METODĂ DE DISTRIBUŢIE A UNEI CHEI DE CRIPTARE

(57) **Rezumat:**

Invenţia se referă la o metodă de distribuţie a unei chei cuantice de criptare, cu aplicaţie în telecomunicaţii, sisteme de criptare şi securizarea transmiterii informaţiei. Metoda conform invenţiei foloseşte un canal de comunicaţie cuantic, pe care sunt transmise secvenţe de biţi, transmiţând cuante aflate în anumite stări cuantice. La recepţie, după detectarea cuantelor, sunt aflate secvenţele de biţi transmise. Identificarea secvenţelor de biţi transmise şi recepţionate fără erori pe canalul de comunicaţie cuantic se realizează prin retransmisia criptată a aceloraşi secvenţe de biţi pe canalul clasic de comunicaţie. Cheia cu care sunt criptate mesajele transmise clasic este formată din valoarea momentului de timp când au fost transmise cuantele, iar la recepţie mesajele sunt decriptate folosind valoarea momentului de timp când acestea au fost detectate.

Revendicări: 10

RO 130287 A0

a 2014 00436
12 -06- 2014

Continuarea rubricii nr. **14.2. Descriere**

Metoda de distribuţie a unei chei de criptare.

Invenţia se refera la o metoda de transmiterea unei chei de criptare sigure cu aplicaţie in telecomunicaţii, sisteme de criptare si securizarea transmiterii informaţiei.

Stadiul actual al domeniului

In momentul de fata, comunicaţiile optice sunt larg utilizate, ele asigura atât o viteza de transmisie mare cat si o cantitate mare de date. Cel mai simplu mod de transmisie a unui bit de informaţie, 0 sau 1, este de a opri sau a laşa sa treacă un fascicul de lumina. In general întreruperea fasciculului însemnă ca s-a transmis bitul cu valoarea 0 si reciproc trecerea fascicolului reprezintă transmiterea bitului cu valoarea 1. Fascicolul de lumina transmis este format dintr-un număr foarte mare de fotoni.

Pe de alta parte, in cazul unei comunicaţii cuantice, aceeaşi informaţie de un bit este transmisa de un singur foton. Un foton se poate afla in mai multe stări cuantice iar transmiterea bitului cu valoarea "0" se face trimiţând un foton intr-o anumită stare cuantica pe care o notam q_0. In mod reciproc transmiterea bitului cu valoarea 1 se face trimiţând un foton având o alta stare cuantica notata q_1. Recepţionarea semnalului transmis se face cu un sistem de detecţie capabil sa separe fotonii cu diferite stări cuantice. Pentru fiecare stare cuantica este prevăzut un detector capabil sa detecteze un singur foton.

Stările cuantice ale unui foton folosite pentru transmiterea informaţiei pot fi: polarizarea, faza sau frecventa .

Cele doua stări cuantice q_0 si q_1 sunt astfel alese încât fotonii sa poată fi separaţi exact in doua fascicole fiecare corespunzând unei sigure stări. Aceste stări cuantice se numesc ortogonale si ele formează o baza de codare. La recepţie sistemul de detecţie este reglat/setat ca sa detecteze precis fotonii codaţi in aceasta baza (b=0); adică daca unul dintre cei doi detectori a detectat un foton atunci acesta a avut starea cuantica q_0 cu o probabilitate apropiata de 1 (100%) si similar daca celalalt detector a detectat un foton atunci acel foton a avut starea cuantica q_1 cu o probabilitate apropiata de 1.

Pentru a sporii securitatea de transmisie a mesajelor astfel încât acestea sa nu poată fi decodate de un interceptor ilegal, in afara de stările cuantice ortogonale q_0 si q_1 ce formează baza b=0 se mai transmit fotoni codaţi in cel puţin încă o baza de stări ortogonale. De exemplu, in protocolul BB84 [1] se folosesc doua perechi de stări ortogonale sau cu alte cuvinte fotonii sunt codaţi in doua baze.

A doua baza este astfel aleasa încât un foton codat in prima baza este detectat cu o probabilitate egala (1/2) de cei doi detectorii. In consecinţa un bit transmis de un foton codat in baza b=0 este detectat cu o eroare maxima de un detector setat sa detecteze fotonii codaţi in cealaltă baza b=1. In acest caz valoarea bitului detectat este tot timpul egala cu a celui transmis doar daca fotonii au fost codaţi si detectaţi in aceeaşi baza.

In protocolul de comunicaţie cuantica BB84 [1] se prevede transmiterea biţilor in doua baze de codare care se schimba in mod aleator. Recepţia se face detectând fotonii tot in doua baze care se schimba tot in mod aleator. In acest fel sunt recepţionaţi corect doar jumătate din biţii transmişi. Pentru ca receptorul sa poată identifica biţii recepţionaţi corect, transmiţătorul trimite un mesaj pe o cale de comunicaţie clasica, acesta conţine baza cu care a fost codat fiecare foton doar se păstrează secret valoarea bitului trimis. Cheia de codare se va forma numai din biţii recepţionaţi corect.

Acest mod de transmisie face posibila depistarea unui interceptor care detectează toţi fotonii si retransmite mai departe fotoni similari cu cei detectaţi. Interceptorul detectează corect starea cuantica doar la jumătate din fotoni si in consecinţa doar pe aceştia ii retransmite corect. Dintre fotonii retransmişi corect, doar jumătate sunt detectaţi corect de către receptorul legal. Acest lucru se întâmpla deoarece si el schimba in mod aleator baza de detecţie. Retansmitatorul clandestin va introduce erori suplimentare si interceptarea mesajelor va fi descoperita.

Una dintre problemele transmisiei cuantice consta in numărul mare de erori ce trebuiesc corectate. Nu toate cuantele transmise sunt detectate la recepţie datorita pierderilor inerenta ale canalului de transmisie. Canalul de transmise nu poate fi perfect etanş ci sunt detectate multe cuante care nu au fost transmise iar

detectoarele dau si semnale de detecţie false. Corectarea acestor erorilor este încă o problema care nu a fost satisfăcător rezolvata.

Un produs existent este Cerberis Quantum key Distribution (QKD) Server fabricat de către ID Quantique SA.

Descrierea invenţiei

Cheia criptografica, pe care o notam cu Q, se distribuie către doi parteneri, pe care ii notam cu T_x si R_x cu scopul de fi folosita pentru criptare unui mesaj secret ce se va transmite de la un partener către celalalt. Cheia Q nu poate fi aflata prin interceptarea mesajelor schimbate intre T_x si R_x in procesul de distribuţie a acesteia. In cazul in care un interceptor, pe care îl notam cu E_x încearcă sa afle cheia recepţionând si retransmiţând parţial sau total, mesajele schimbate intre T_x si R_x aceasta acţiune poate fi descoperita.

Metoda de distribuţie a cheii intre T_x si R_x foloseşte doua canale de comunicaţie unul clasic si celalalt cuantic. Canalul clasic poate fi orice fel de comunicaţie in care informaţia se transmite folosind metode clasice. Pe canalul de comunicaţie cuantic, informaţia se transmite trimiţând cuante având diferite stări cuantice.

De exemplu pentru a transmite un bit dintr-un mesaj, se trimite o cuanta având starea q_0 daca valoarea bitului este zero si o cuanta cu starea q_1 daca valoarea bitului este unu. Cele doua stări cuantice sunt astfel alese incit ele pot fi separate in doua fascicole fapt ce permite receptorului R_x sa afle valoarea bitului transmis. Se spune ca aceste stări q_0 si q_1 sunt ortogonale si formează o baza daca, teoretic, cele doua stări se pot separa perfect. In acest caz, la recepţie, se poate afla (cu o mare probabilitate) daca s-a detectat o cuanta având starea q_0 sau q_1 si in consecinţa se va cunoaşte valoarea bitului transmis.

Cu o singura cuanta se poate transmite o cantitate de informaţie mai mare de un bit daca se folosesc mai multe stări cuantice grupate doua cate doua in mai multe baze. In cazul in care se folosesc b baze atunci mesajul transmis cu o singura cuanta m_x are o lungime de b biţi si numărul de stări cuantice folosite este $2 \cdot b$.

Întrucât cheia Q este un număr aleator atunci fiecare mesaj m_x trebuie sa fie un număr aleator si bazele trebuie sa se schimbe tot aleator.

Baza in care a fost trimisa fiecare cuanta nu este cunoscut de receptor si acest caz la recepţie bazele in care sunt detectate cuantele se schimba tot aleator. In cazul in care la recepţie bazele ar fi schimbat după o relaţie cunoscuta, atunci aceasta ar putea fi aflata de E_x fapt ce ar ajuta la aflarea cheii Q. Probabilitatea ca o cuanta sa fie detectata in aceeaşi baza in care a fost trimisa este $\frac{1}{b}$. Lungime mesajului transmis de un număr nr_Q de cuante măsurata in biţi este $nr_Q \cdot b \cdot \frac{1}{b} = nr_Q$, deci lungimea mesajului rămâne constanta. Avantajul folosirii mai multor baze este ca se sporeşte securitatea de distribuţie a cheii Q deoarece probabilitatea ca E_x sa detecteze o cuanta in aceeaşi baza cu R_x este $\frac{1}{b} \cdot \frac{1}{b} = \frac{1}{b^2}$.

Pentru distribuţia cheii Q, transmiţătorul T_x trimite către R_x, pe calea cuantica de comunicaţie, un mesaj M_x care este o succesiune aleatoare de biţi si din acest mesaj se va selecta un se de biţi cunoscut doar de T_x si R_x din care se va forma cheia criptografica Q. Pentru a se identifica cuantele transmise de T_x si recepţionate de R_x, T_x retransmite pe o cale de comunicaţie clasica fiecare mesaj m_x transmis cu fiecare cuanta. Aceste mesaje $K(t_i, m_i)$ sunt cifrate cu o relaţie matematica K unde m_i este mesajul transmis cu cuanta i iar t_i este valoarea numerica a momentului de timp când aceasta a fost trimisa.

Transmiterea unor impulsuri de sincronizare pe calea de comunicaţie cuantica fata de care se măsoară atât momentului de timp t_i când a fost emisa o cuanta cat si momentul când aceasta a fost detectata la recepţie r_i simplifica procedura de aflare (la recepţie) a cheii cu care au fost codate mesaje retransmise pe calea clasica, in acest caz $t_i = r_i$.

Intervalul de timp t_{xr} de la trimiterea unei cuante pana la detecţia acesteia are aceeaşi valoare numerica pentru majoritatea cuantelor cu care s-au transmis

mesajele m_x. In acest caz intre un număr nr_{TR} de mesaje din şirul $K(t_i, m_i)$ si mesajele recepţionate pe calea cuantica este valabila relaţia:

$$K(t_i, m_i) = K(r_j - t_{xr}, m_j) \quad (1)$$

unde r_j este momentul de timp la care s-a detectat cuanta j si m_j reprezintă mesajul recepţionat fără erori $m_j = m_i$. Daca t_{xr} nu este cunoscut atunci valoarea lui este cea pentru care relaţia (1) se verifica pentru un număr maxim de perechi $(i_1, j_1), (i_2, j_2), \cdots, (i_{nr_{TR}}, j_{nr_{TR}})$. Cu alte cuvinte, daca s-a primit mesajul cifrat i si s-a detectat o cuanta j astfel încât se verifica relaţia (1) atunci cuanta i transmisa la momentul t_i a fost detectata fără erori de receptorul R_x la momentul r_j.

In pasul următor R_x transmite clasic către T_x şirul de valori $[i_1, i_2, ...]$. Din şirul de valori ale biţilor $[m_{i1}, m_{i2}, ...]$ se formează cheia de criptare $Q(m_{i1}, m_{i2}, ...)$ folosind o relaţie cunoscuta atât de T_x cat si de R_x.

Metoda permite transmiterea unei chei de criptare de lungime dubla fata de alte protocoale [1].

Metoda de identificare a biţilor recepţionaţi de R_x, prezentata mai sus, face inutila interceptarea mesajelor de către un receptor ilegal E_x. Folosind aceeaşi metoda E_x poate identifica biţii interceptaţi corect dar aceştia nu vor fi recepţionaţi de R_x si deci nu sunt folosiţi la formarea cheii de criptare Q.

Detecţia mesajelor retransmise de către un interceptor ilegal

O metoda posibila de aflare a cheii Q este recepţia si retransmisia către R_x a unor cuante similare cu cele recepţionate. In aceasta situaţie cuantele retransmise vor ajunge la R_x după un interval de timp t_{xer} egal cu durata de timp in care cuanta parcurge distanta de la T_x la E_x si apoi de la E_x la R_x plus timpii de detecţie si retransmisie. Întrucât $t_{xer} > t_{xr}$ relaţia (1) nu se verifica si mesajele retransmise nu sunt folosite la formarea cheii Q. Aceasta tentativa de aflarea cheii poate fi descoperita căutând un număr $t_{xer} > t_{xr}$ pentru care relaţia

$$K(t_i, m_i) = K(r_i - t_{ver}, m_i) \quad (2)$$

se verifica pentru un număr mare de indici (i, j).

O alta metoda de verificare consta in analiza mesajelor recepţionate cu erori

$$K(t_i, m_i) = K(r_i - t_{ver}, m_i^*) \quad (3)$$

In cazul in care se folosesc b baze, probabilitatea de a recepţiona un mesaj cu erori este $1 - \frac{1}{b}$ iar in cazul mesajelor retransmise aceasta probabilitate creste la $1 - \frac{1}{b^2}$.

O metoda mai buna este ca suplimentar sa se analizeze si cauza care a provocat eroarea. Mesajele m_x se pot fi reprezentate in binar astfel $m_x = q_{01} b_{1b}$, unde q_{01} este primul bit si are valoarea stării cuantice q_0 sau q_1 iar b_{1b} sunt următorii biţi si reprezintă numărul bazei in care trebuiesc detectate cuantele. Pot sa apară trei tipuri de mesaje eronate $m_x^* = q_{01}^* b_{1b}$, $m_x^* = q_{01} b_{1b}^*$ si $m_x^* = q_{01}^* b_{1b}^*$, unde cu asterisc s-au marcat secvenţele recepţionate eronat.. Probabilităţile de producere a celor trei tipuri de erori $p(q_{01}^* b_{1b})$, $p(q_{01} b_{1b}^*)$, $p(q_{01}^* b_{1b}^*)$ se pot determina. si in general sunt stabile. Probabilităţile de apariţie a erorilor in cazul in care baza de detecţie a fost cea corecta $p(q_{01}^* b_{1b})$ sau in cazul in care starea cuantica a fost corect detectata cu toate ca baza a fost greşit aleasa $p(q_{01} b_{1b}^*)$ sunt semnificativ mai mici decât $p(q_{01}^* b_{1b}^*)$. In cazul mesajelor retransmise $p(q_{01}^* b_{1b})$ si $p(q_{01} b_{1b}^*)$ cresc semnificativ. Evitarea repercusiunilor ce pot apărea in cazul in care E_x interceptează si retransmite toate mesajele necesita întreruperea folosirii cheii Q in cazul in care oricare dintre $p(q_{01}^* b_{1b})$, $p(q_{01} b_{1b}^*)$, $p(q_{01}^* b_{1b}^*)$ depăşeşte o anumita limita peste care distribuţia cheii poate fi nesigura.

Relaţia (3) se foloseşte pentru determinarea erorilor constatate la recepţie si cu datele obţinute se pot evalua probabilităţile $p(q_{01}^* b_{1b})$, $p(q_{01} b_{1b}^*)$ si $p(q_{01}^* b_{1b}^*)$. Cu valorile obţinute se poate evalua securitatea transmisiei si in anumite cazuri cu valorile m_x^* corectate se poate forma o cheie de criptare Q^*.

Exemplu de transmisie a unei chei de codare criptografica

Cuantele transmise sunt fotoni, stările cuantice sunt polarizarea orizontala (H) sau verticala (V). Polarizările orizontala si verticala sunt definite fata de un anumit sistem de referita numita "baza" in alta baza aceste polarizări devin oblice. Astfel baza reprezintă setarea (orientarea) sistemului de detecţie in care se detectează fotonii.

Convenim ca, trimiţând un foton polarizat orizontal, se transmite un bit a cărui valoare este zero (0) si cu un foton polarizat vertical se transmite bitul cu valoarea unu (1). In acest fel informaţia este codata cuantic.

Codarea clasica se face similar : se transmite un bit a cărui valoare este 0 sau 1 trimiţând un fascicol de fotoni polarizaţi orizontal sau vertical.

Esenţial in codarea cuantica este faptul ca se codează foton cu foton iar in cea clasica se codează un fascicol de fotoni. O consecinţa imediata a acestui fapt este ca detectând un singur foton nu se poate afla (cu precizie) starea lui cuantica. La detecţie cele doua stări se pot separa perfect, folosind un beam-spliter polarizat, perfect orientat doar in cazul când fotonul este polarizat doar orizontal sau vertical. Intr-o direcţie vor trece doar fotonii polarizaţi orizontal si in cealaltă cei polarizaţi vertical. Pe fiecare direcţie este un detector si in funcţie de care dintre aceştia a detectat un foton se poate afla cu o mare probabilitate (~99%) polarizarea fotonului trimis.

Folosind invenţia propusa se pot identifica fotonii recepţionaţi corect iar valoare mesajului transmis cu fiecare foton poate fi aflata doar de cel care a detectat fotonul. In cazul in care se folosesc doua sau mai multe baza de codare care se modifică aleator atunci cantitatea de informaţie transmisa este dubla fata de protocoalele existente [1]

Fotonii recepţionaţi si retransmişi pot fi identificaţi uşor. Pentru acest lucru rezoluţia de măsurare a timpului trebuie sa fie mai mica decât timpul de retransmisie $t_{xer} - t_{xr}$.

Mesajele $m_x = q_{01} b_{1b}$ sunt codate cu relaţia matematica $K(t_i, m_i) = t_i + 4 \cdot m_i$ si retransmise pe o cale clasica către R_x. In cazul in care se folosesc doar doua baze relaţia devine $K(t_i, m_i) = t_i + 4 \cdot q_i + 8 \cdot b_{12}$, unde q_i este bitul corespunzător stării cuantice iar b_{12} este bitul corespunzător bazei selectate, b_{12}=0 cat fotonii au fost

codaţi in prima baza si b_{12}=1 când aceştia au fost codaţi in a doua baza. Cantitatea de informaţie transmisa cu un foton este de 2 biţi, fata de unul singur in cazul altor protocoale [1].

Fotonii transmişi fără erori se identifica folosind relaţia:

$$K(r_i, m_j) - K(t_i, m_i) = r_j - t_i + 4 \cdot (m_j - m_i) = t_{xr}$$

Fotonii retransmişi fără erori sunt identificaţi cu o relaţie similara $K(r_i, m_j) - K(t_i, m_i) = t_{xr} > t_{xr}$.

Fotonii detectaţi cu erori se identifica cu relaţia:

$$K(r_i - t_{xr}, m_j) - K(t_i, m_i) = 4 \cdot (q_i - q_i) + 8 \cdot (b_j - b_i)$$

REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics,* vol. 74, pp. 145-195, 2002.

- Continuarea rubricii nr. **14.3. Revendicări**

1. Folosirea de către transmutator, a momentului de timp când este transmisă o cuanta, pe calea cuantica, pentru crearea unei chei de codare, aceasta cheie poate fi aflata de către orice receptor, doar pentru cuantele pe care le-a detectat, măsurând momentul de timp când a detectat fiecare cuantă si scăzând din fiecare dintre aceste momente de timp o valoare fixa, egala cu intervalul de timp scurs de la transmisie pana la detecţie si astfel rezulta cheia de decodare.
2. Transmiterea unor impulsuri de sincronizare pe calea de comunicaţie cuantica fata de care se măsoară momentului de timp când a fost emisa si detectata o cuanta simplifica procedura de aflare a cheii de codare la recepţie deoarece, in cazul aceleaşi cuante, valoarea momentului de timp când a fost transmisa este egala cu valoarea momentului de timp când a fost detectata la recepţie, cu aceasta valoare numerica se formează cheia de codare a mesajelor retransmise pe calea clasica.
3. Corectarea erorilor de comunicaţie pe calea cuantica, prin retransmiterea mesajelor transmise cu fiecare cuanta, pe o cale de comunicaţie clasica, codate cu o cheie ce se foloseşte o singura data.
4. Mărirea lungimii mesajelor transmise cuantic transmiţând cuante codate in mai multe baze, folosind un număr ***b*** de baze de codare cuantica, care se schimba aleator, rezulta ca fiecare cuanta se poate afla in 2***b*** stări cuantice si astfel se pot transmite ***b*** biţi de date.
5. Creşterea securităţii de distribuţie a cheii mărind numărul de baze ***b***, care se schimba aleator, fără scăderea cantităţii de informaţie transmise pe calea cuantica.
6. Identificarea cuantelor transmise si recepţionate cu si fără erori cat si corectarea mesajului transmis cu acestea pe calea de comunicaţie cuantica
7. Reducerea erorilor de formare a cheii de criptare aceasta fiind formata doar din biţii corect transmişi.
8. Posibilitatea de dublare a lungimii cheii de criptare fără a reduce securitatea acesteia.
9. Depistarea retransmiterii mesajelor de către un interceptor ilegal..
10. Identificarea cuantelor recepţionate si retransmise de către un interceptor ilegal folosind mesajul retransmis pe calea de comunicaţie clasica.