ROMÂNIA
MINISTERUL EDUCAȚIEI, CERCETĂRII, TINERETULUI ŞI SPORTULUI
UNIVERSITATEA DUNĂREA DE JOS DIN GALAȚI

Strada Domnească nr. 47, cod poştal 800008
Galaţi, România
E-mail: rectorat@ugal.ro

UNIVERSITAS
GALATIENSIS

Tel.: (+4) 0336-130.109; 0336-130.108; 336-130.104
Fax: (+4) 0236 - 461.353
www.ugal.ro

C964 / 28-01-2012

Universitatea " Dunărea de Jos " din Galaţi vă face cunoscut că în data de 09.11.2012 , ora 12.30 , în Corpul G, sala 305 , va avea loc susţinerea publică a tezei de doctorat intitulată: ***"SECURIZAREA SISTEMELOR INFORMATICE ŞI DE COMUNICAŢII PRIN CRIPTOGRAFIA CUANTICĂ"***, elaborată de domnul/doamna ***ing. ANGHEL CĂTĂLIN,*** în vederea conferirii titlului ştiinţific de doctor în Domeniul de doctorat - ***Ingineria sistemelor.***

Comisia de doctorat are urmatoarea componenţă :

Preşedinte:	***Conf.univ.dr.ing. Emilia PECHEANU*** ***Universitatea "Dunărea de Jos" din Galaţi***
Conducător de doctorat:	***Prof.univ.dr.ing. Adrian FILIPESCU*** ***Universitatea "Dunărea de Jos" din Galaţi***
Referent 1:	***Prof.univ.dr.ing. Ştefan PENTIUC*** ***Universitatea "Ştefan Cel Mare " din Suceava***
Referent 2:	***Prof.univ.dr.ing. Vasile MANTA*** ***Universitatea Tehnică "Gheorghe Asachi" din Iaşi***
Referent 3:	***Prof.univ.dr.ing. Victor PATRICIU*** ***Academia Tehnică Militară Bucureşti***

Cu această ocazie vă transmitem rezumatul tezei de doctorat şi vă invităm să participaţi la susţinerea publică. În cazul în care doriţi să faceţi eventuale aprecieri sau observaţii asupra conţinutului lucrării, vă rugăm să le transmiteţi în scris pe adresa Universităţii, str. Domnească nr. 47, 800008 - Galaţi, Fax - 0236 / 461353.

RECTOR,
Prof.dr.ing. Viorel MÎNZU

ROMÂNIA · MINISTERUL EDUCAȚIEI, CERCETĂRII, TINERETULUI ŞI SPORTULUI · UNIVERSITATEA DUNĂREA DE JOS DIN GALAȚI · RECTORAT

SECRETAR DOCTORAT,
Ing. Luiza AXINTE

UNIVERSITATEA "DUNĂREA DE JOS"
GALAȚI

FACULTATEA DE AUTOMATICĂ, CALCULATOARE,
INGINERIE ELECTRICĂ ȘI ELECTRONICĂ

Domeniul : Ingineria Sistemelor
Subdomeniul : Informatică Aplicată în Securitatea Transmisiilor de Date

- REZUMATUL TEZEI DE DOCTORAT -

SECURIZAREA SISTEMELOR INFORMATICE ȘI DE COMUNICAȚII PRIN CRIPTOGRAFIA CUANTICĂ

Conducător științific:
Profesor dr. ing. Adrian FILIPESCU

Doctorand:
ing. Cătălin ANGHEL

GALAȚI
2012

Principalul punct slab al unui sistem criptografic și de comunicații este acela că orice transmisie securizată poate fi făcută numai după ce cheia de criptare este comunicată în secret printr-un canal de comunicații secretizat. Cu alte cuvinte, avem de a face cu un paradox : „Înainte de a comunica în secret, trebuie să comunicăm în secret". Aici intervine criptografia cuantică care profitând de anumite fenomene ce au loc la nivel subatomic nu numai că face imposibilă interceptarea transmisiei dar poate și detecta dacă un atacator interceptează canalul de comunicații.

CUPRINS

1. Introducere

Un algoritm de criptare este de securitate necondiționată dacă textul criptat generat de acesta nu conține destulă informație pentru a extrage textul original, indiferent de volumul de text decriptat care se află în posesia atacatorului.

Cu excepția unui algoritm numit one-time pad, propus de Gilbert Vernam [44, 45] în 1920, nu există algoritm de criptare care să fie de o securitate necondiționată. Securitatea acestui algoritm a fost demonstrată în 1949 de către Claude Shannon, condițiile fiind ca, cheia de criptare să fie de aceeași lungime cu textul clar, să fie secretă și să nu fie folosită decât o singură dată [38].

Cu toate că algoritmul one-time pad a fost demonstrat ca fiind de securitate necondiționată acesta are câteva neajunsuri:

- necesită o cheie perfect aleatoare;
- cheia de criptare trebuie să fie sigură și folosită o singură dată;
- cheia de criptare trebuie să fie de dimensiunea textului criptat.

Pentru rezolvarea acestor neajunsuri ale algoritmului one-time pad putem utiliza criptografia cuantică și anume quantum key distribution – qkd pentru a realiza, în deplină siguranță, schimbului de chei.

1.1 Criptografia cuantică

Criptografia cuantică ne pune la dispoziție noi metode de securizare a comunicațiilor. Procesul de transmitere sau stocare a informației este realizat prin intermediul unui suport fizic, spre exemplu fotonii transmiși prin fibră optică, astfel, cum și ce poate un atacator afla depinde exclusiv de legile fizicii cuantice.

Folosind principiile fizicii cuantice, putem realiza și implementa un sistem de comunicații care va detecta întotdeauna orice încercare de atac [10], datorită faptului că orice încercare de „măsurare" a unui purtător cuantic de informație va modifica particula purtătoare și va lăsa „urme".

Spre deosebire de criptografia clasică, securitatea criptografiei cuantice nu se bazează pe presupusa complexitate a unei probleme matematice, ci pe principiile fizicii cuantice – mai exact, pe *Principiul incertitudinii al lui Heisenberg* [28] și pe *Entanglementul cuantic al particulelor* [23].

1.1.1 Principiul incertitudinii al lui Heisenberg

În 1927, Werner Heisenberg (1901-1976) a stabilit că este imposibil să măsurăm exact atât poziția unei particule, cât și impulsul ei. Cu cât determinăm mai precis pe una dintre ele, cu atât mai puțin o știm pe cealaltă [28]. Acest principiu este denumit *Principiul incertitudinii al lui Heisenberg* și este o proprietate fundamentală a mecanicii cuantice care și stabilește că, măsurând o anumită proprietate cuantică vom modifica într-o anumită măsură o altă proprietate cuantică.

1.1.2 Entanglementul cuantic – perechi EPR

În 1935, Einstein, Podolsky și Rosen (EPR), prezintă o lucrare [22] prin care aduc o provocare fundamentelor mecanicii cuantice arătând un paradox. Există perechi de particule cuantice, numite *perechi EPR* sau *particule entanglate*, care sunt separate spațial dar care sunt legate între ele de așa natură încât stările lor cuantice sunt interconectate, în sensul că, măsurând starea cuantică a uneia dintre particule vom ști automat starea cuantică a celeilalte particule.

Putem obține fotoni *entanglați* printr-un proces numit *spontaneous parametric down-conversion - SPDC* [46]. Astfel, un foton polarizat trece printr-un cristal nonliniar [34] și este divizat în doi fotoni *entanglați* care vor avea stări de polarizare opuse (după măsurare). Particulele cuantice utilizate în criptografia cuantică sunt fotonii polarizați, numiți *qbiți*.

1.1.3 Qbiți – fotoni polarizați

Polarizarea fotonilor se realizează cu ajutorul unor dispozitive speciale, numite filtre de polarizare, care permit trecerea numai a particulelor polarizate într-o anumită direcție.

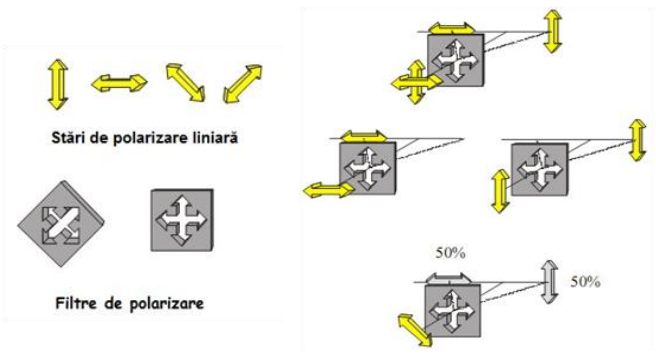

Figura 1.3. Polarizarea liniară

În criptografia cuantică considerăm că un foton poate fi polarizat *liniar* (0^o,90^o), *diagonal* (45^o,135^o) sau *circular* (stânga - spinL, dreapta - spinR), transformându-l prin polarizare în *qbit* [36].

Fotonii polarizați liniar-diagonal, liniar-circular sau diagonal-circular sunt transformați în *qbiți* a căror stări sunt cunoscute ca fiind *stări legate* iar legile fizicii cuantice și anume Principiul incertitudinii al lui Heisenberg spune că este imposibil de măsurat simultan stările oricărei perechi de *variabile legate;* cu alte cuvinte, dacă *inamicul* încearcă să „măsoare" un foton polarizat orizontal, folosind o metoda de „măsurare" a fotonilor polarizați diagonal, acel foton își schimbă polarizarea din orizontală în diagonală.

În tabelul următor vom stabili o convenție de notare pentru codificarea biților prin fotoni polarizați – qbiți.

Baza	**L**(Liniar)	**D**(Diagonal)	**C**(Circular)	**C**(Circular)	**L**(Liniar)	**D**(Diagonal)
Polarizare	0^o	45^o	spinL	spinR	90^o	135^o
Qbit	↔	↗	↺	↻	↕	↘
Bit	0	0	0	1	1	1

Tabelul 1.2. Polarizarea fotonilor - qbiți

Având în vedere cele menționate, rezultă că, folosind principiile fizicii cuantice, putem crea un sistem prin care se poate realiza *distribuirea cheilor cuantice* (QKD – Quantum Key Distribution) în deplină siguranță.

1.1.4 Distribuirea cheilor cuantice – QKD

Prin distribuirea cheilor cuantice [13,14,15,17,21,23,31,33], două entități, *emițătorul* și *receptorul*, stabilesc în comun o cheie unică și sigură care poate fi folosită împreună cu un algoritm de criptare sigur cum ar fi *one-time pad* [44,45].

O schemă clasică de distribuire a cheilor cuantice utilizează două canale de comunicații, unul clasic și unul cuantic și are următoarele etape:

1. *Emițătorul* și *receptorul* generează secvențe de biți aleatoare și independente;
2. *Emițătorul* și *receptorul* folosesc un protocol de distribuire a cheilor cuantice pentru a compara secvențele de biți și pentru a stabili în comun o cheie unică și secretă;
3. *Emițătorul* și *receptorul* execută o procedură de corectare a erorilor.

4. *Emițătorul* și *receptorul* apreciază (funcție de rata de eroare) dacă transmisia a fost interceptată de către *inamic*;
5. *Emițătorul* și *receptorul*, comunică printr-un canal public și execută o procedură numită *privacy amplification* [9,11];
6. *Cheia finală, secretă, unică și sigură* este obținută.

Există două tipuri de scheme de distribuire a cheilor cuantice. Una folosește un generator care emite câte un singur foton și se bazează pe *principiul incertitudinii al lui Heisenberg* (*single-photon*) [13,14,15,17], în care se încadrează algoritmii BB84 și B92. Cealaltă folosește un generator care emite câte o pereche de fotoni entanglați și se bazează pe *entanglementul cuantic* al fotonilor [21,23,31,33], în care se încadrează algoritmul E91.

În cazul schemelor de tipul *single-photon* [13,14,15,17], fiecare bit din cheia transmisă, corespunde unei stări particulare a particulei purtătoare, cum ar fi fotonii polarizați – qbiți. *Emițătorul* cheii trebuie să stabilească o secvență de polarizare a fotonilor, cu care biții din cheie vor fi polarizați, după care vor fi transmiși printr-o fibră optică. Pentru a obține cheia, care este formată dintr-o secvență qbiți, *Receptorul* trebuie să facă o serie de măsurători, cu ajutorul unor filtre speciale, pentru a determina polarizarea fotonilor. Detectarea inamicului se realizează prin metode specifice fiecărui algoritm în parte.

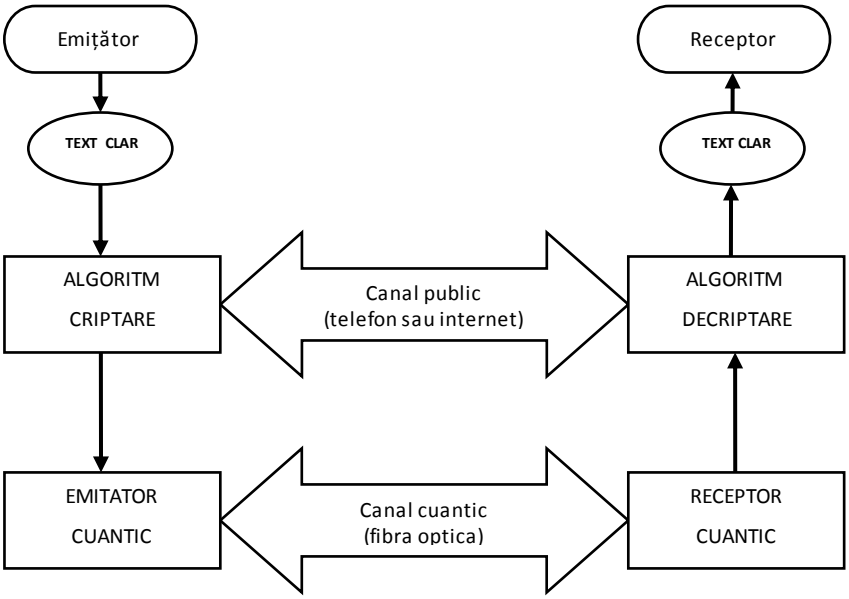

Figura 1.5. Sistem de distribuire a cheilor cuantice de tip single-photon

În cazul schemelor de tipul *entanglement* [21,23,31,33], un generator cuantic, creează perechi entanglate de fotoni polarizați, care sunt separați și transmiși simultan către cele două părți care comunică. Cu ajutorul filtrelor speciale fotonii polarizați sunt citiți și transformați în biți. Detectarea inamicului este determinată folosind *inegalitatea lui Bell* [8].

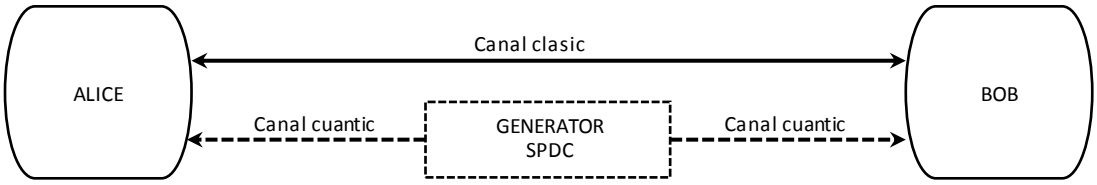

Figura 1.6. Sistem de distribuire a cheilor cuantice de tip entanglement

1.2 Structura tezei

În capitolul 1, intitulat „Introducere", pe lângă partea de istorie a criptografiei și o scurtă introducere în criptografie, este făcută o analiză a securității sistemelor criptografice clasice și a celor moderne arătându-se că, cu o singură excepție, securitatea lor se bazează pe complexitatea matematică a calculelor. În funcție de dimensiunea cheii de criptare folosite, pentru criptanaliză pot fi necesari și câteva mii de ani pentru puterea de calcul a sistemelor informatice existente în zilele noastre. Singurul criptosistem demonstrat a fi sigur este one-time pad – OTP [71,72], dar pentru a fi considerat de securitate necondiționată trebuiesc respectate anumite cerințe legate de cheia de criptare și anume ca aceasta să fie de dimensiunea textului care se dorește a fi criptat, să fie utilizată doar o singură dată și să fie perfect sigură. De aici rezultă un paradox și anume că „înainte de a comunică în secret, trebuie să comunicăm în secret". Aici intervine criptografia cuantică care profitând de anumite fenomene ce au loc la nivel subatomic nu numai că face imposibilă interceptarea transmisiei dar poate și detecta dacă un atacator ascultă canalul de comunicații. Securitatea criptografiei cuantice nu se bazează pe presupusa complexitate a unei probleme matematice, ci pe principiile fizicii cuantice – mai exact, pe principiul incertitudinii al lui Heisenberg și pe entanglementul cuantic al particulelor. În continuare sunt prezentate cele două principii ale fizicii cuantice, sunt

introduși qbiții și tipurile de polarizări ale acestora și modelele sistemelor de distribuire a cheilor cuantice de tip single-photon și de tip entanglement.

În capitolul 2, intitulat „Sisteme de distribuire a cheilor cuantice", sunt prezentate cele mai cunoscute și utilizate sisteme de distribuire a cheilor cuantice care vor fi folosite ulterior pentru dezvoltarea contribuțiilor proprii din cadrul tezei. Sunt descrise modurile de funcționare și implementare a schemelor de distribuire a cheilor cuantice BB84, B92 și E92, sunt prezentați pașii, metodele de detectare a inamicului, etapele distilării cheii finale, pseudocodul și schemele logice ale acestora.

În capitolul 3, intitulat „Analiza securității sistemelor de distribuire a cheilor cuantice", sunt prezentate cele mai cunoscute și utilizate metode de atac asupra schemelor de distribuire a cheilor cuantice și cele mai cunoscute și utilizate metode de detectare a inamicului care vor fi folosite ulterior pentru dezvoltarea contribuțiilor proprii din cadrul tezei. Sunt prezentate și descrise atacurile de tip Intercept-Resend, Photon Number Splitting, Man-in-the-Middle și Quantum Cloning, precum și metodele de detectare a inamicului, cum ar fi Metoda Clasică, Quantum Bit Error Rate și cea care utilizează inegalitatea lui Bell.

În capitolul 4, intitulat „Proiectarea protocolul Base Selection and Transmission Synchronization", am propus un protocol cuantic de comunicații bidirecțional. Acest protocol criptografic cuantic de comunicații, folosește biții din cheia finală, obținută după etapele Secret key reconciliation și Privacy amplification, ale oricărui sistem de distribuire a cheilor cuantice și stabilește cu exactitate parametrii utilizați, de către cele două părți care vor să comunice, pentru realizarea transmisiei cuantice. Sunt prezentate etapele, pseudocodul și schema logică a noului protocol BSTS.

În capitolul 5, intitulat „Proiectarea metodei Quantum Bit Travel Time de detectare a inamicului", am propus o nouă metodă de detectare a unui inamic care interceptează un canal cuantic de comunicații și care poate fi implementată în orice sistem de distribuire a cheilor cuantice. Avantajele oferite de această nouă metodă sunt acelea că inamicul poate fi depistat în timpul transmisiei cuantice, după fiecare qbit recepționat și mai ales că poate fi depistat cu exactitate, fără dubii că ar putea fi confundat cu zgomotele de pe canalul cuantic sau cu erori ale dispozitivelor. Sunt prezentate în continuare modalitățile de implementare a metodei QBTT în sistemele BB84 și B92, schemele logice și pseudocodul.

În capitolul 6, intitulat „Proiectarea protocolului cuantic Base Selection and Polarization Agreement", am propus o variantă simplificată a protocolului BSTS care folosește pentru detectarea inamicului metoda QBTT. Protocolul BSTS cu metoda QBTT realizează o transmisie bidirecțională în totalitate cuantică, rezultând un algoritm cuantic de comunicații între un emițător și un receptor. Sunt prezentate în continuare modalitățile de implementare, pseudocodul și schema logică a noului protocol.

În capitolul 7, intitulat „Simularea sistemelor de distribuire a cheilor cuantice", am prezentat câteva programe de simulare a schimbului de chei cuantice scrise în C++. Sunt prezentate programul de simulare a sistemului BB84 în condiții ideale fără inamic, programul de simulare a sistemului BB84 în condiții ideale cu inamic, programul de simulare a sistemului BB84 cu metoda QBTT și programul de simulare a unui sistem criptografic cuantic BSPA.

În capitolul 8, intitulat „Concluzii, contribuții și direcții de cercetare" sunt prezentate concluziile finale, contribuțiile originale din cadrul tezei, diseminarea rezultatelor cercetării precum și direcțiile viitoare de cercetare.

Rezultatele cercetărilor doctorale au fost prezentate în 6 articole publicate sau acceptate spre publicare din care : 1 lucrare într-o revistă indexată ISI cu factor de impact 0.913, 2 lucrări în reviste indexate BDI (CNCSIS B+), 2 lucrări la conferințe internaționale și 1 lucrare în biblioteca electronică Cornell University Library din SUA.

1.3 Diseminarea rezultatelor

Rezultatele cercetărilor doctorale au fost prezentate în 6 articole publicate sau acceptate spre publicare din care : 1 lucrare într-o revistă indexată ISI cu factor de impact 0.913, 2 lucrări în reviste indexate BDI, 2 lucrări la conferințe internaționale și 1 lucrare în biblioteca electronică Cornell University Library din SUA.

Reviste ISI cu factor de impact

- Anghel C., „Research, Development and Simulation of Quantum Cryptographic Protocols", acceptată pentru publicare în „Electronics and Electrical Engineering", (cotată ISI, factor de impact 0.913).

Reviste indexate BDI

- Anghel C., „New eavesdropper detection method in quantum cryptography", în curs de publicare : The annals of "Dunarea de Jos" University of Galati, fascicula III, vol.34, nr. 1, 2011.
- Anghel C., „New quantum cryptographic protocol", în curs de publicare : The annals of "Dunarea de Jos" University of Galati, fascicula III, vol.34, nr. 1, 2011.

Conferințe internaționale

- Anghel C., „Quantum cryptography algorithm", Proceedings ECIT2008 – 5th European Conference on Intelligent Systems and Technologies, Romania, Iasi, 2008.
- Anghel C. & Coman G., „Base selection and transmission synchronization algorithm in quantum cryptography", Proceedings CSCS17 - 17th International Conference on Control Systems and Computer Science, Romania, Bucharest, ISSN : 2066-4451, vol. 1, pag. 281-284, 2009.

Bibliotecă electronică

- Anghel C., „Creșterea securității Sistemelor Informatice și de Comunicații prin Criptografia Cuantică", Cornell University Library, http://arxiv.org/, cite as: http://arxiv.org/abs/1006.5381v1, 2010.

2. Sisteme de distribuire a cheilor cuantice

2.1 Sistemul de distribuire a cheilor cuantice BB84

Sistemul de distribuire a cheilor cuantice (QKD) BB84, este primul algoritm cuantic [1,10,19,37] și a fost propus în 1984 de către Charles Bennett și Gilles Brassard. Conform acestuia, două entități, *emițătorul* și *receptorul* stabilesc în secret o cheie unică, comună și secretă, folosind fotoni polarizați – *qbiți* [39,40-43].

Pentru implementarea acestui sistem de distribuire a cheilor cuantice, vom folosi pentru polarizarea fotonilor bazele de polarizare liniară (L) și diagonală (D) iar pentru codificarea biților următoarea convenție:

Baza	L	D	L	D
Stare	0^o	45^o	90^o	135^o
Qbit	→	↗	↑	↖
Bit	0	0	1	1

Tabelul 2.1. Polarizarea fotonilor în BB84

2.1.1 Pașii sistemului QKD BB84

1. *Emițătorul* generează o secvență aleatoare de biți – notată "***s***".
2. *Emițătorul* alege aleator ce bază de polarizare să aplice fiecărui foton din "***s***" (liniar "L" sau diagonal "D"). Notăm "***b***" secvența de polarizare.
3. *Emițătorul*, folosind un echipamente speciale, creează o secvență "***p***" de fotoni polarizați – qbiți, a căror direcție de polarizare reprezintă biții din "***s***".
4. *Emițătorul* transmite qbiții din "***p***" prin fibră optică către *receptor*.
5. *Receptorul*, pentru fiecare qbit recepționat – secvența "***p'***" , alege aleator câte o bază de polarizare (liniar "L" sau diagonal "D"). Notăm cu "***b'***" secvența bazelor de polarizare aleasă.
6. *Receptorul*, măsoară fiecare qbit recepționat respectând baza de polarizare aleasă la pct. 5, rezultând o secvență de biți "***s'***".
7. *Emițătorul* îi transmite printr-un canal public *receptorului*, ce bază de polarizare a ales pentru fiecare bit în parte. La rândul sau *receptorul* îi comunică *emițătorului* unde a făcut aceeași alegere a bazei de polarizare. Biții pentru care cei doi nu au avut aceeași bază de polarizare sunt eliminați din "***s***" și "***s'***".

2.1.2 Detectarea inamicului

Pentru qbitul cu numărul n, bitului ***s***[n] îi va corespunde o bază de polarizare ***b***[n] iar bitului ***s***'[n] îi va corespunde o bază ***b***'[n] .

Dacă ***b***'[n] = ***b***[n] va implica că ***s***'[n] = ***s***[n].

În cazul în care un inamic a încercat să citească fotonul purtător al lui ***s***[n], atunci chiar dacă cele două baze alese de *receptor* și *emițător* sunt identice (***b***'[n] = ***b***[n]), vom avea ***s***'[n] ≠ ***s***[n].

Pasul final al algoritmului BB84 constă într-o comparație dintre cele două secvențe de biți, deținute de *emițător* și *receptor* după codificare și decodificare. Acesta cuprinde două etape: *secret key reconciliation* [11] și *privacy amplification* [9,11].

2.1.3 Secret key reconciliation

Etapa *secret key reconciliation* [12] este o procedură de corectare a erorilor din cheia brută, care elimină:

- erorile generate de alegerea diferită a bazelor
- erorile generate de *Inamic*
- erorile generate de zgomote

Etapa *Secret key reconciliation* realizează o căutare binară, interactivă a erorilor. *Emițătorul* și *receptorul* împart secvența de biți rămasă (cheia brută) în blocuri de biți și vor compara paritatea fiecărui bloc. În cazul în care paritatea unui bloc de biți diferă, *emițătorul* și *receptorul* vor împărți blocul respectiv în blocuri mai mici și vor compara paritatea lor.

2.1.4 Privacy amplification

Având în vedere faptul că, în etapa anterioară, comunicația s-a realizat pe un canal nesecurizat, există posibilitatea ca *inamicul* să dețină informații sensibile despre cheia secretă. Pentru a stabili o cheie perfect sigură, *emițătorului* și *receptorului* trebuie să mai realizeze o etapă : *privacy amplification.* Această etapă constă într-o permutare a biților din cheia secretă și eliminarea unui subset de biți, care va fi realizată de către *emițător* și *receptor*.

3. Analiza securității sistemelor de distribuire a cheilor cuantice

3.1 Vulnerabilitățile sistemelor QKD

Vulnerabilitățile teoretice și cele practice ale sistemelor de distribuire a cheilor cuantice – QKD au constituit dintotdeauna principalul punct de plecare al metodelor de atac asupra acestor sisteme.

Există mai multe tipuri de atacuri asupra sistemelor de distribuire a cheilor cuantice, iar dintre cele mai importante amintim :

(1) Atacul de tip Intercept/Resend (Faked-State)
(2) Atacul de tip Photon Number Splitting (PNS)
(3) Atacul de tip Man-in-the-Middle (MiM)
(4) Atacul de tip Quantum Cloning

3.1.1 Atacul de tip Intercept-Resend

Atacul de tip Intercept-Resend [35] numit și Faked-State, este cel mai întâlnit tip de atac folosit asupra sistemelor de distribuire a cheilor cuantice. *Inamicul*, întrerupe canalul cuantic, măsoară fiecare qbit recepționat de la *emițător* în una dintre cele două baze de polarizare și transmite către *receptor* alți qbiți polarizați în baze de polarizare corespunzătoare cu rezultatele obținute de către el, fără a lăsa urme ale atacului [25].

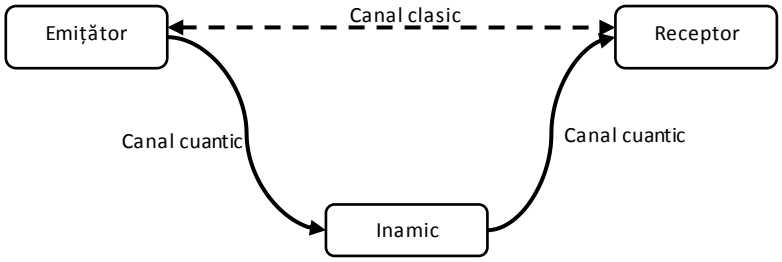

Figura 3.1. Atac de tip Intercept-Resend

Acest tip de atac este nedetectabil prin tehnicile actuale pentru dispozitive a căror rată de erori este mai mare de 25% [26].

3.1.2 Atacul de tip Photon Number Splitting

Atacul de tip PNS [16,30] este cel mai bun tipul de atac asupra unui sistem de distribuire a cheilor cuantice atunci când pentru generarea fotonilor se folosește un laser cu impuls atenuat.

Acest tip de atac se bazează pe faptul că, datorită imperfecțiunilor echipamentelor cuantice, pentru codificarea unui bit sunt utilizați unul sau mai mulți fotoni polarizați. Altfel spus pentru codificarea unui bit, în loc să plece de la *emițător* un impuls care conține un singur foton polarizat, pleacă un impuls care este format din mai mulți fotoni polarizați identic.

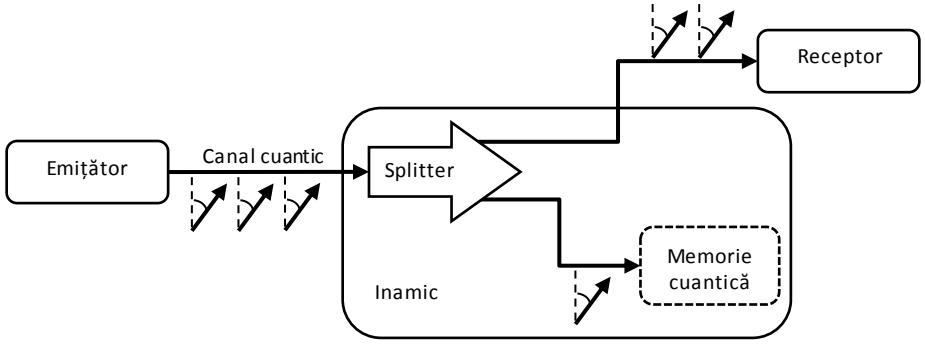

Figura 3.2. Atac de tip PNS

Inamicul, verifică numărul de fotoni din fiecare impuls generat de către *emițător*, fără a perturba polarizarea fotonilor și blochează toate impulsurile care conțin doar un singur foton. Pentru impulsurile care conțin mai mulți fotoni extrage un singur foton pe care îl memorează într-o memorie cuantică lăsând restul să plece spre *receptor*. Ulterior, când *emițătorul* și *receptorul* realizează compararea bazelor de polarizare folosite, *inamicul* măsoară fotonii din memoria cuantică în conformitate cu bazele anunțate, obținând astfel cheia secretă.

Acest tip de atac este nedetectabil prin metodele actuale de detectare a inamicului.

3.1.3 Atacul de tip Man-in-the-Middle

Sistemele de distribuire a cheilor cuantice sunt vulnerabile la atacurile de tip Man-in-the-Middle atunci când nu sunt folosite metode de autentificare între emițător și receptor deoarece inamicul poate pretinde că este receptorul respectiv emițătorul.

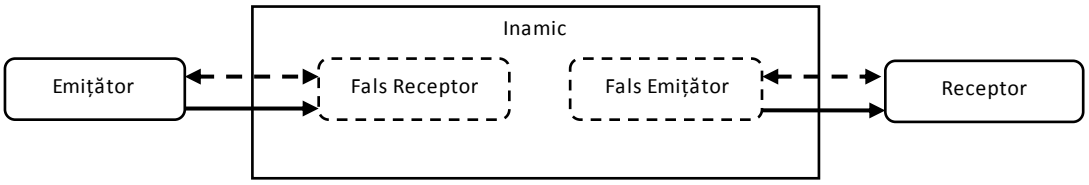

Figura 3.3. Atac de tip Man-in-the-Middle

Inamicul întrerupe ambele canale de comunicații, cuantic și clasic, dintre *emițător* și *receptor*, pretinzând pentru *emițător* că este *receptorul* iar pentru *receptor* că este *emițătorul*. Au fost propuse mai multe metode de implementare a acestui tip de atac folosind o a trei-a parte [48] sau teoria haosului [29].

Acest tip de atac este nedetectabil prin metodele actuale de detectare a inamicului.

3.1.4 Atacul de tip Quantum Cloning

Atacul de tip quantum cloning este o metodă pur teoretică de atac care folosește un dispozitiv de clonare propus de către N. Gisin și B. Huttner [24] numit "Pretty Good Quantum Copying Machine" (PGQCM) și o memorie cuantică.

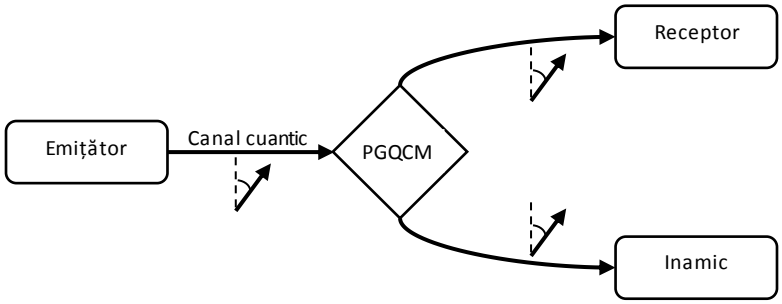

Figura 3.4. Atac de tip Quantum Cloning

Inamicul interceptează fiecare foton transmis de către *emițător* și folosind o mașină de clonare obține doi fotoni identici. Unul dintre fotoni este transmis către *receptor* iar celălalt este păstrat de către *inamic* într-o memorie cuantică. În timpul etapei *bases reconciliation, inamicul* scoate cate un foton din memoria cuantică și îl măsoară în funcție de baza de polarizare anunțată.

Acest tip de atac este nedetectabil prin metodele actuale de detectare a inamicului.

3.2 Detectarea atacurilor asupra QKD

Există mai multe metode de detectare a atacurilor asupra sistemelor de distribuire a cheilor cuantice.

(1) Metoda clasică – identificarea qbiților alterați de către *inamic*
(2) QBER – estimarea ratei de erori din cheia primară
(3) Inegalitatea lui Bell

3.2.1 Metoda clasică

Detectarea inamicului se realizează la finalul transmisiei cuantice, după comunicarea bazelor de polarizare pe canalul public la sfârșitul etapei *bases reconciliation*. Emițătorul și receptorul, compară o parte din biții din cheia primară, pentru care au ales baze de polarizare identice, iar dacă aceștia diferă rezultă că inamicul a intervenit pentru a citi qbiții respectivi, modificându-le polarizarea.

3.2.2 Quantum Bit Error Rate – QBER

Această metodă constă în calcularea procentului de erori din cheia primară, obținută la finalul transmisiei cuantice, după etapa de comunicare a bazelor de polarizare pe canalul public [43]. Metoda QBER – Quantum Bit Error Rate pentru detectarea *inamicului* se poate aplica majorității sistemelor de distribuire a cheilor, fiecare sistem având propria rată de erori acceptată, orice depășire a ei însemnând intervenția unui *inamic*.

3.2.3 Inegalitatea lui Bell

Inegalitatea lui Bell [8] poate fi folosită pentru a detecta prezența sau absența unui *inamic*. Astfel, dacă inegalitatea lui Bell este satisfăcută rezultă că *inamicul* a intervenit pentru a citi qbiții transmiși de către *emițător* iar în caz contrar *inamicul* nu a fost prezent.

4. Proiectarea protocolului Base Selection and Transmission Synchronization

4.1 Necesitatea protocolului BSTS

După etapa *privacy amplification*, *cheia finală*, obținută de către *emițător* și *receptor* este foarte mică comparativ cu secvența inițială pregătită de către *emițător* și de cele mai multe ori insuficient de mare pentru a fi utilizată pentru o criptare cu algoritmul one-time pad [44,45].

În figura 4.1 este prezentată, diferența dintre dimensiunea cheii inițiale și dimensiunea cheii finale.

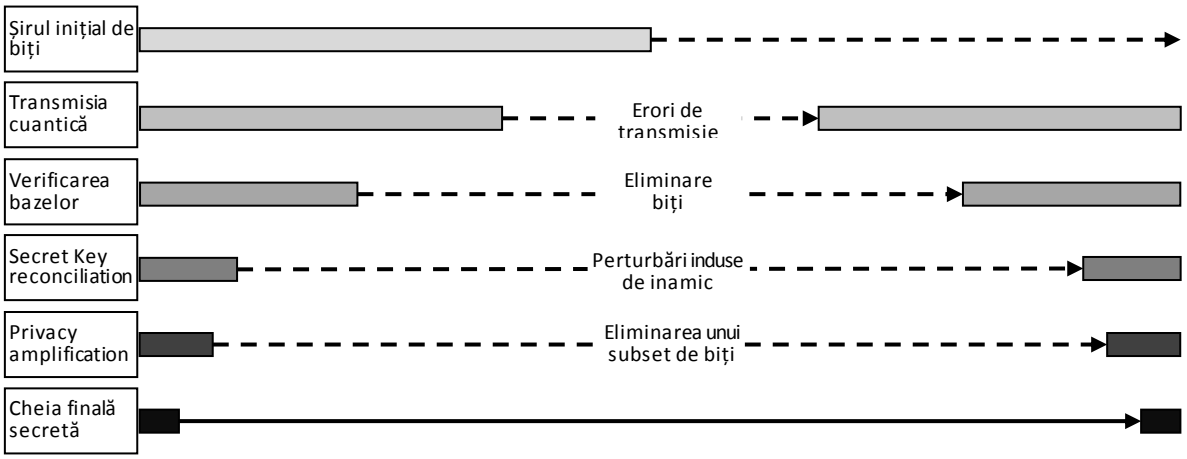

Figura 4.1. Diferența dintre cheia inițială și cea finală în cazul algoritmului BB84

Având în vedere aceste aspecte propun un protocol de comunicare cuantic, bidirecțional, între un emițător și un receptor, pe care l-am numit protocolul Base Selection and Transmission Synchronization – BSTS [2,3].

4.2 Premisele protocolului BSTS

Parametrii vizați în acest protocol sunt:

(1) ce pereche de baze de polarizare dintre cele trei, L (liniară), D (diagonală) și C (circulară), va fi folosită;

(2) intervalul de timp la care *emițătorul* va emite un qbit iar *receptorul* va citi acel qbit;

(3) ce bază de polarizare va fi folosită pentru codificarea fiecărui bit în parte;

(4) verificarea biților recepționați la finalul transmisiei cuantice și retransmiterea blocurilor care conțin erori.

Pentru codificarea biților vom stabili următoarea convenție de codificare și reprezentare a qbiților :

Baza	**L**(Liniar)	**D**(Diagonal)	**C**(Circular)	**C**(Circular)	**L**(Liniar)	**D**(Diagonal)
Polarizare	0^o	45^o	spinL	spinR	90^o	135^o
Qbit						
Bit	0	0	0	1	1	1

Tabelul 4.1. Polarizarea fotonilor - qbiți

Prin acest protocol cuantic de comunicații *emițătorul* și *receptorul* vor stabili în comun, în funcție de biții din *cheia finală*, care pereche, dintre cele trei baze de polarizare, *liniar-diagonal*, *liniar-circular* sau *diagonal-circular* vor fi folosite pentru polarizarea fotonilor – acest proces se va numi *base selection*.

Tot în funcție de biții din *cheia finală*, protocolul cuantic de comunicații, va stabili intervalul de timp în care *emițătorul* va transmite un foton real iar *receptorul* va citi fotonul respectiv, în restul timpului *emițătorul* va transmite fotoni falși pentru inducerea în eroare a unui eventual *inamic* – acest proces se va numi *transmission synchronization*.

În final, în funcție de biții rămași din *cheia finală*, *emițătorul* și *receptorul*, vor ști exact ce baze de polarizare să aplice pentru fiecare foton pe care urmează să-l transmită respectiv să-l recepționeze.

După terminarea transmisiei, *emițătorul* și *receptorul*, împart secvența de biți obținută în blocuri de biți și vor compara paritatea fiecărui bloc. În cazul în care paritatea unui bloc de biți diferă, se va relua transmisia blocului respectiv.

4.3 Pașii protocolului BSTS

Algoritmul va fi executat simultan de către *emițător* și *receptor* și are următoarele etape :

1. Primii doi biți din *cheia finală* vor fi utilizați pentru a stabili bazele de polarizare, care vor fi folosite pentru a polariza fotonii ce urmează a fi transmiși, conform tabelului :

Bitul 1	Bitul 2	**Baza 1**	**Baza 2**
0	0	**L**	**D**
0	1	**L**	**C**
1	0	**C**	**D**
1	1	**L**	**D**

Tabelul 4.2. Selectarea bazelor în funcție de biții 1 și 2 din *cheia finală – base selection*

2. Următorii patru biți din *cheia finală* vor forma un număr în binar a cărui conversie în zecimal, +1, va reprezenta intervalul de timp, exprimat în microsecunde, la care se va realiza transmiterea respectiv recepționarea unui qbit real. *Emițătorul* va transmite qbiți reali către *receptor* la intervalele de timp stabilite în această etapă, în restul timpului *emițătorul* va transmite fotoni falși polarizați aleator.

Bitul 3	**Bitul 4**	**Bitul 5**	**Bitul 6**	**Număr în baza 10**	**Timp (μs) (Număr +1)**
0	0	0	0	0	1
0	0	0	1	1	2
0	0	1	0	2	3
0	0	1	1	3	4
.....				.....	
1	1	0	1	13	14
1	1	1	0	14	15
1	1	1	1	15	16

Tabelul 4.3. Stabilirea intervalului de timp al transmisiei - *transmission synchronization*

3. Biții rămași din *cheia finală* vor reprezenta bazele de polarizare pentru fiecare bit care va fi transmis, respectiv recepționat, conform tabelului 4.4 :

Dacă Bitul este	0	1
Baza de polarizare	**Baza 1**	**Baza 2**

Tabelul 4.4. Stabilirea bazelor pentru polarizarea fiecărui bit

4. După ultimul bit din *cheia finală*, procesul de polarizare al fotonilor va continua de la bitul numărul 7 al cheii finale până la terminarea mesajului care se dorește a fi transmis.
5. *Emițătorul și receptorul* comunică pe canalul clasic și împart secvența de biți obținută în blocuri de biți comparând paritatea fiecărui bloc. În cazul în care paritatea unui bloc de biți diferă, se va relua transmisia blocului respectiv.

4.4 Schema logică a protocolului BSTS

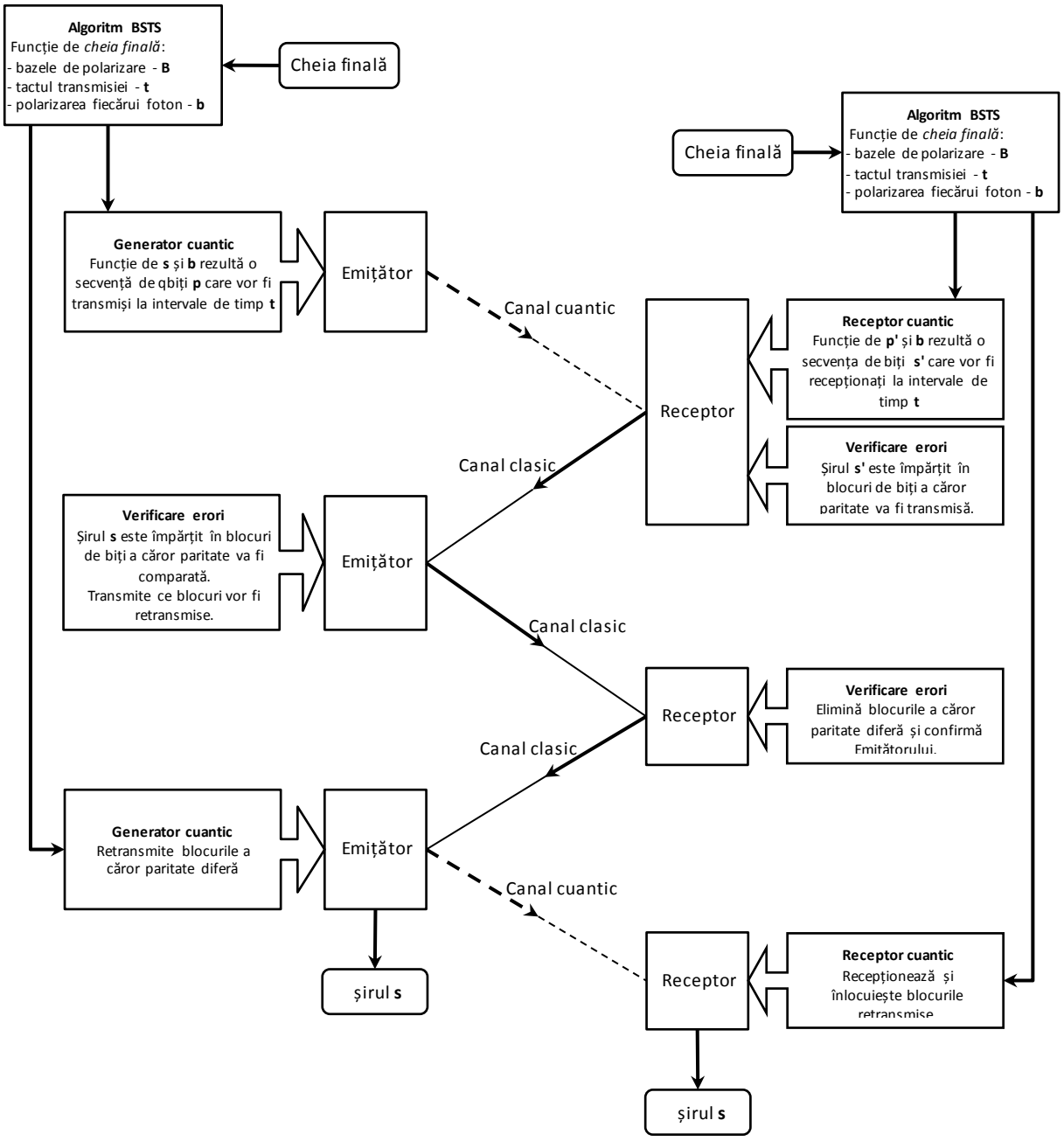

Figura 4.3. Schema logică a protocolului BSTS

4.5 Avantajele protocolului BSTS

Protocolul Base Selection and Transmission Synchronization utilizează *cheia finală* rezultată după etapele *secret key reconciliation* și *privacy amplification*, ale oricărui sistem de distribuire a cheilor cuantice. În funcție de *cheia finală*, *emițătorul* și *receptorul* vor stabili cu exactitate parametrii utilizați în transmisia cuantică, respectiv sistemul de baze de polarizare utilizat, tactul transmisiei și tipul de polarizare aplicat fiecărui foton în parte.

Protocolul BSTS poate fi considerat un protocol de rețea cuantic între două calculatoare deoarece poate realiza o legătură bidirecțională între ele. Prin intermediul protocolului BSTS nu se dorește realizarea doar a unui schimb de chei cuantice, ca în cazul celorlalți algoritmi de distribuire a cheilor cuantice gen BB84, B92 sau E91, ci a se realiza o transmisie bidirecțională între cele două părți care comunică.

Prima etapă a algoritmului BSTS, numită și *Base selection*, stabilește funcție de biții din *cheia finală* cele două baze de polarizare care vor folosite dintre cele trei posibile, *liniar-diagonal*, *liniar-circular* sau *diagonal-circular*, astfel încât avem stabilită prima necunoscută a unei transmisii cuantice. Acest procedeu va micșora considerabil probabilitatea ca *inamicul* să poată descifra transmisia deoarece nu știe ce baze de polarizare să folosească pentru citirea qbiților.

A doua etapă a algoritmului BSTS, numită și *Transmission synchronization*, stabilește funcție de biții din cheia finală intervalul de timp în care *emițătorul* va transmite un foton real iar *receptorul* va citi fotonul respectiv, deoarece în restul intervalului *emițătorul* va transmite fotoni falși polarizați aleatoriu. Acest procedeu va face ca *inamicul* să obțină o cantitatea mult mai mare de qbiți falși decât qbiți reali.

A treia etapă a algoritmului stabilește, pentru fiecare bit care trebuie transmis, ce bază de polarizare i se va aplica astfel încât *emițătorul* și *receptorul* vor ști exact cum să polarizeze fotonul purtător respectiv să citească qbitul respectiv.

A patra etapă a algoritmului BSTS realizează corectarea erorilor apărute în timpul transmisiei cuantice, stabilind ce blocuri de biți trebuie retransmiși.

În concluzie putem spune că algoritmul Base Selection and Transmission Synchronization va realiza o transmisie respectiv recepție, fără erori datorită faptului că *emițătorul* și *receptorul* vor ști exact cum să polarizeze, respectiv să citească fiecare qbit în parte iar la sfârșitul transmisie se va realiza o corectare a erorilor.

4.6 Concluzii și contribuții

În acest capitol am propus un nou protocol criptografic cuantic de comunicații, care folosește biții din *cheia finală*, obținută după etapele *secret key reconciliation* și *privacy amplification,* ale oricărui sistem de distribuire a cheilor cuantice și care stabilește cu exactitate parametrii care vor fi utilizați de către *emițător* și *receptor* pentru realizarea transmisiei cuantice.

Datorită faptului că, încă din 1985, au fost descrise principiile de funcționare ale unui calculator cuantic [20], ne putem aștepta ca atunci când va fi operațional, algoritmul one-time pad să poată fi spart. Acest lucru va face ca schemele de distribuire a cheilor cuantice să fie inutile, dar folosind algoritmul Base Selection and Transmission Synchronization – BSTS, care realizează o transmisie bidirecțională în totalitate cuantică vom putea comunica în secret.

Dacă în cazul celorlalte sisteme de distribuire a cheilor cuantice cheia finală poate fi de dimensiuni nesatisfăcătoare ca dimensiune, deoarece aceasta trebuie să fie de dimensiunea textului care se dorește a fi criptat, utilizarea aceste chei în cadrul protocolului BSTS este pe deplin satisfăcătoare.

Contribuțiile din acest capitol sunt :

- Proiectarea, realizarea și implementarea protocolul criptografic cuantic de comunicații Base Selection and Transmission Synchronization.

Aceste contribuții sunt baza următoarelor lucrări științifice :

- Anghel C., „Quantum cryptography algorithm", Proceedings ECIT2008 – 5th European Conference on Intelligent Systems and Technologies, Romania, Iasi, 2008.
- Anghel C. & Coman G., „Base selection and transmission synchronization algorithm in quantum cryptography", Proceedings CSCS17 - 17th International Conference on Control Systems and Computer Science, Romania, Bucharest, ISSN : 2066-4451, vol. 1, pag. 281-284, 2009.

5. Proiectarea metodei Quantum Bit Travel Time de detectare a inamicului

5.1 Necesitatea metodei

Securității sistemelor de distribuire a cheilor cuantice poate fi îmbunătățită prin detectarea „exactă" și „imediată" a *inamicului*.

Detectarea „exactă" a *inamicului* se referă la faptul că acesta nu trebuie să fie confundat cu zgomotele apărute pe canalul cuantic de comunicații sau cu erori ale dispozitivelor.

Detectarea „imediată" a *inamicului* se referă la faptul că acesta trebuie detectat în momentul în care a intervenit pentru a citi un qbit. În cazul celorlalți algoritmilor de distribuire a cheilor cuantice, detectarea *inamicului* se face după finalizarea transmisiei cuantice, după etapa de comunicare a bazelor de polarizare pe canalul clasic, existând astfel posibilitatea ca *inamicul* să obțină prea multe informații legate de cheia transmisă.

Metoda Quantum Bit Travel Time – QBTT de detectare a *inamicului* poate fi implementată în oricare sistem de distribuire a cheilor cuantice și are avantajul că *inamicul* poate fi detectat cu *exactitate* și mai ales *imediat* după ce acesta a intervenit pentru a citi un qbit, în timpul transmisiei cuantice.

5.2 Premisele metodei QBTT

Metoda propusă se bazează pe faptul că filtrele de polarizare induc întârzieri ale particulei purtătoare [47]. Fiecare filtru aplicat va întârzia particula purtătoare cu o anumită perioadă de timp.

Filtrele de polarizare folosite de către *emițător* și *receptor* pentru transformarea biților în qbiți, respectiv a qbiților în biți, induc întârzieri ale particulei purtătoare. Vom nota cu ΔT această întârziere care va fi identică pentru fiecare particulă purtătoare. Această întârziere ΔT se va determina experimental, pentru fiecare tip de schemă folosită, ea fiind condiționată de tipul filtrelor de polarizare utilizate de către *emițător* și *receptor*.

Emițătorul și *receptorul* vor sincroniza ceasurile interne ale dispozitivelor de lucru [18,27,32]. *Emițătorul*, pentru fiecare qbit emis, generează și transmite receptorului, pe canalul clasic, timestamp-ul momentului emisiei, la rândul său *receptorul* pentru fiecare qbit recepționat generează timestamp-ul momentului recepției, diferența dintre cele dintre cele două timestamp-uri, timestamp_receptor - timestamp_emițător, va reprezenta întârzierea ΔT a particulei purtătoare datorate celor două filtre de polarizare aplicate de *emițător* și *receptor*.

Dacă *inamicul* citește un qbit, adică aplică un filtru de polarizare, acesta va induce o întârziere suplimentară a particulei purtătoare, notată Δt, crescând astfel timpul parcurs de către aceasta de la *receptor* la *emițător*.

Inamicul poate fi detectat prin măsurarea timpului parcurs de particula purtătoare de la *emițător* la *receptor*, iar dacă $\Delta T' = \Delta T + \Delta t$ va rezulta că *inamicul* a fost prezent.

Alt avantaj al metodei QBTT rezultă din faptul că se pot face verificări pentru detectarea *inamicului* în timpul transmisiei cuantice, după fiecare qbit transmis de la *emițător* către *receptor* față de celelalte metode la care detectarea *inamicului* se face la sfârșitul transmisiei cuantice, după comunicarea bazelor de polarizare pe canalul clasic.

Noua metodă poate fi implementată cu ușurință în orice sistem de distribuire a cheilor cuantice ca o măsură suplimentară de securitate sau ca metodă de sine stătătoare de detectare a *inamicului*.

5.3 Implementarea metodei QBTT în sistemul BB84

Implementarea noii metode de detectare a inamicului în sistemul de distribuire a cheilor cuantice BB84 cuprinde următoarele etape:

1. *Emițătorul* și *receptorul* își sincronizează ceasurile interne.
2. *Emițătorul* generează o secvență aleatoare de biți - notată "***s***".
3. *Emițătorul* alege aleator ce bază de polarizare să aplice fiecărui foton din "***s***" (liniar "L" sau diagonal "D"). Notăm "**b**" secvența de polarizare.
4. *Emițătorul*, folosind un set de filtre de polarizare, creează o secvență "**p**" de qbiți, a căror direcție de polarizare reprezintă biții din "***s***".

5. *Emițătorul* transmite qbiții din "**p**" prin fibră optică către *receptor*. Pentru fiecare qbit transmis, *emițătorul* transmite *receptorului* pe canalul clasic momentul de timp în care a fost transmis – timestamp_emițător.
6. *Receptorul*, pentru fiecare qbit recepționat, alege aleator câte o bază de polarizare (liniar "L" sau diagonal "D"). Notăm cu "**b'**" secvența bazelor de polarizare aleasă.
7. Pentru fiecare qbit recepționat, *receptorul* generează timestamp_receptor și calculează întârzierea ΔT = timestamp_receptor - timestamp_emițător, dintre momentul transmisiei și momentul recepției. Dacă pentru un anumit qbit întârzierea ΔT este mai mare decât cea normală atunci înseamnă că *inamicul* este prezent și oprește transmisia.
8. *Receptorul*, măsoară fiecare qbit recepționat respectând baza de polarizare aleasă la pct. 6, rezultând o secvență de biți "***s'***".
9. *Emițătorul* îi transmite printr-un canal public *receptorului*, ce bază de polarizare a ales pentru fiecare bit în parte. La rândul sau *receptorul* îi comunică *emițătorului* unde a făcut aceeași alegere a bazei de polarizare. Biții pentru care cei doi nu au avut aceeași bază de polarizare sunt eliminați din "**s**" și "**s'**".

5.4 Detectarea inamicului în sistemul BB84 cu metoda QBTT

Emițătorul, pentru fiecare qbit emis, generează și transmite receptorului, pe canalul clasic, timestamp-ul momentului emisiei, la rândul său *receptorul* pentru fiecare qbit recepționat generează timestamp-ul momentului recepției, diferența dintre cele dintre cele două timestamp-uri, timestamp_receptor - timestamp_emițător va reprezenta întârzierea ΔT a particulei purtătoare datorate celor două filtre de polarizare aplicate la emisie respectiv recepție.

Dacă inamicul încercă să citească un anumit qbit, el va induce o nouă întârziere Δt, rezultând o întârziere totală a qbitului $\Delta T' = \Delta T + \Delta t$. Aceasta îi va permite receptorului să identifice prezența inamicului și să oprească transmisia.

5.5 Avantajele metodei QBTT

Avantajele metodei Quantum Bit Travel Time – QBTT, sunt acelea că *inamicul* poate fi detectat „imediat" și cu „exactitate".

Receptorul poate detecta „imediat" prezența *inamicului* în timpul transmisiei cuantice, după fiecare qbit recepționat, prin măsurarea timpului parcurs de particula purtătoare de la *emițător* la *receptor*. În cazul altor algoritmilor de distribuire a cheilor cuantice, detectarea *inamicului* se face după finalizarea transmisiei cuantice, în etapa de comunicare a bazelor de polarizare pe canalul clasic, lăsând astfel în mâna *inamicului* informații importante legate de transmisie.

Inamicul poate fi depistat cu „exactitate" deoarece perturbările naturale apărute pe canalul cuantic nu produc întârzieri ale particulei purtătoare ci doar modificări ale polarizării. Această proprietate ne ajută să nu confundăm eventualele zgomotele de pe canalul cuantic cu prezența unui *inamic*. Celelalte metode de depistare a inamicului nu pot face diferența între zgomot de e canalul cuantic și prezența unui eventual *inamic*.

Un alt avantaj este acela că această metodă poate fi implementată cu ușurință în orice tip de schemă de distribuire a cheilor cuantice.

5.6 Concluzii și contribuții

In acest capitol am propus o nouă metodă, *exactă* și *rapidă*, de detectare a unui eventual *inamic* care interceptează canalul cuantic de comunicații dintre *emițător* și *receptor*.

Am văzut, în capitolul 3, că există anumite metode de atac, metode pur teoretice deocamdată, în care *inamicul*, chiar dacă interceptează transmisia, nu poate fi detectat prin metodele actuale și care pot compromite în totalitate transmisia cuantică dintre *emițător* și *receptor*. În schimb, prin utilizarea metodei Quantum Bit Travel Time, *inamicul* poate fi detectat imediat ce a intervenit pentru a citi un qbit, indiferent de metoda de atac folosită.

Datorită faptului că nou metodă propusă poate detecta prezența inamicului în timpul transmisiei cuantice, verificare făcându-se după fiecare qbit recepționat, iar inamicul este detectat cu exactitate, fără dubii că ar putea fi confundat cu erorile ale transmisiei de pe canalul cuantic, elimină în totalitate riscul ca *inamicul* să poată intercepta transmisia cuantică fără a fi detectat, indiferent de metoda de atac folosită de către acesta.

În concluzie putem spune că metoda Quantum Bit Travel Time - QBTT de detectare a inamicului poate fi implementată în oricare sistem de distribuire a cheilor

cuantice și are avantajul că *inamicul* poate fi detectat cu *exactitate* și mai ales *imediat* după ce acesta a intervenit pentru a citi un qbit, în timpul transmisiei cuantice.

Contribuțiile din acest capitol sunt :

- Proiectarea, realizarea și implementarea metodei de detectare a inamicului Quantum Bit Travel Time.

Aceste contribuții sunt baza următoarelor lucrări științifice :

- Anghel C., „Creșterea securității Sistemelor Informatice și de Comunicații prin Criptografia Cuantică", Cornell University Library, http://arxiv.org/, cite as: http://arxiv.org/abs/1006.5381v1, 2010.
- Anghel C., „New eavesdropper detection method in quantum cryptography", în curs de publicare : The annals of "Dunarea de Jos" University of Galati, fascicula III, vol.34, nr. 1, 2011.

6. Proiectarea protocolului cuantic Base Selection and Polarization Agreement

6.1 Premisele protocolului BSPA

Parametrii vizați în cazul protocolului cuantic BSPA sunt:

(1) ce pereche de baze de polarizare dintre cele trei, L (liniară), D (diagonală) și C (circulară), va fi folosită;

(2) ce bază de polarizare va fi folosită pentru codificarea fiecărui bit în parte.

(3) detectarea *inamicului* prin monitorizarea timpului parcurs de către fiecare particulă purtătoare de la *emițător* la *receptor*.

(4) verificarea biților recepționați la finalul transmisiei cuantice și corectarea erorilor prin retransmiterea blocurilor care conțin inadvertențe.

Pentru codificarea biților vom stabili următoarea convenție de codificare și reprezentare a qbiților :

Baza	**L**	**D**	**C**	**C**	**L**	**D**
Polarizare	0^o	45^o	spinL	spinR	90^o	135^o
Qbit						
Bit	0	0	0	1	1	1

Tabelul 6.1. Polarizarea fotonilor - qbiți

Prin protocolul cuantic de comunicații BSPA, *emițătorul* și *receptorul* vor stabili în comun, în funcție de biții din *cheia finală*, care pereche, dintre cele trei baze de polarizare, *liniar-diagonal*, *liniar-circular* sau *diagonal-circular* vor fi folosite pentru polarizarea fotonilor.

În funcție de biții rămași din *cheia finală*, *emițătorul* și *receptorul*, vor ști exact ce baze de polarizare să aplice pentru fiecare foton pe care urmează să-l transmită respectiv să-l recepționeze.

În timpul transmisie cuantice, după fiecare qbit recepționat, *receptorul* va verifica dacă intervalul de timp parcurs de particula purtătoare, de la *emițător* la *receptor* se încadrează în limitele normale. În cazul în care intervalul de timp este

mai mare decât normalul înseamnă că un *inamic* a interceptat particula purtătoare și oprește transmisia.

După terminarea transmisiei cuantice, *emițătorul* și *receptorul*, împart secvența de biți obținută în blocuri de biți și vor compara paritatea fiecărui bloc. În cazul în care paritatea unui bloc de biți diferă, se va relua transmisia blocului respectiv.

6.2 Implementarea protocolul BSPA

Protocolul va fi executat simultan de către *emițător* și *receptor* și va utiliza biții din *cheia finală* obținută după etapele *secret key reconciliation* și *privacy amplification* ale oricărui sistem de distribuire a cheilor cuantice :

1. Primii doi biți din *cheia finală* vor fi utilizați pentru a stabili bazele de polarizare, care vor fi folosite pentru a polariza fotonii ce urmează a fi transmiși, conform tabelului :

Bitul 1	Bitul 2	**Baza 1**	**Baza 2**
0	0	**L**	**D**
0	1	**L**	**C**
1	0	**C**	**D**
1	1	**L**	**D**

Tabelul 6.2. Selectarea bazelor în funcție de biții 1 și 2 din *cheia finală – base selection*

2. Biții rămași din *cheia finală* vor reprezenta bazele de polarizare pentru fiecare bit care va fi transmis, respectiv recepționat, conform tabelului 6.3 :

Dacă Bitul este	0	1
Baza de polarizare	**Baza 1**	**Baza 2**

Tabelul 6.3. Stabilirea bazelor pentru polarizarea fiecărui bit

3. După ultimul bit din *cheia finală*, procesul de polarizare al fotonilor va continua de la bitul numărul 3 din *cheia finală* până la terminarea mesajului care se dorește a fi transmis.
4. Pentru fiecare qbit transmis, *emițătorul* transmite *receptorului* pe canalul clasic momentul de timp în care a fost transmis – timestamp_emițător. Pentru fiecare qbit recepționat, *receptorul* generează timestamp_receptor și calculează

întârzierea ΔT = timestamp_receptor - timestamp_emițător, dintre momentul transmisiei și momentul recepției. Dacă pentru un anumit qbit întârzierea ΔT este mai mare decât cea determinată experimenta atunci înseamnă că *inamicul* este prezent și oprește transmisia.

5. *Emițătorul și receptorul* comunică pe canalul clasic și împart secvența de biți obținută în blocuri de biți comparând paritatea fiecărui bloc. În cazul în care paritatea unui bloc de biți diferă, se va relua transmisia blocului respectiv.

6.3 Schema logică a protocolului BSPA

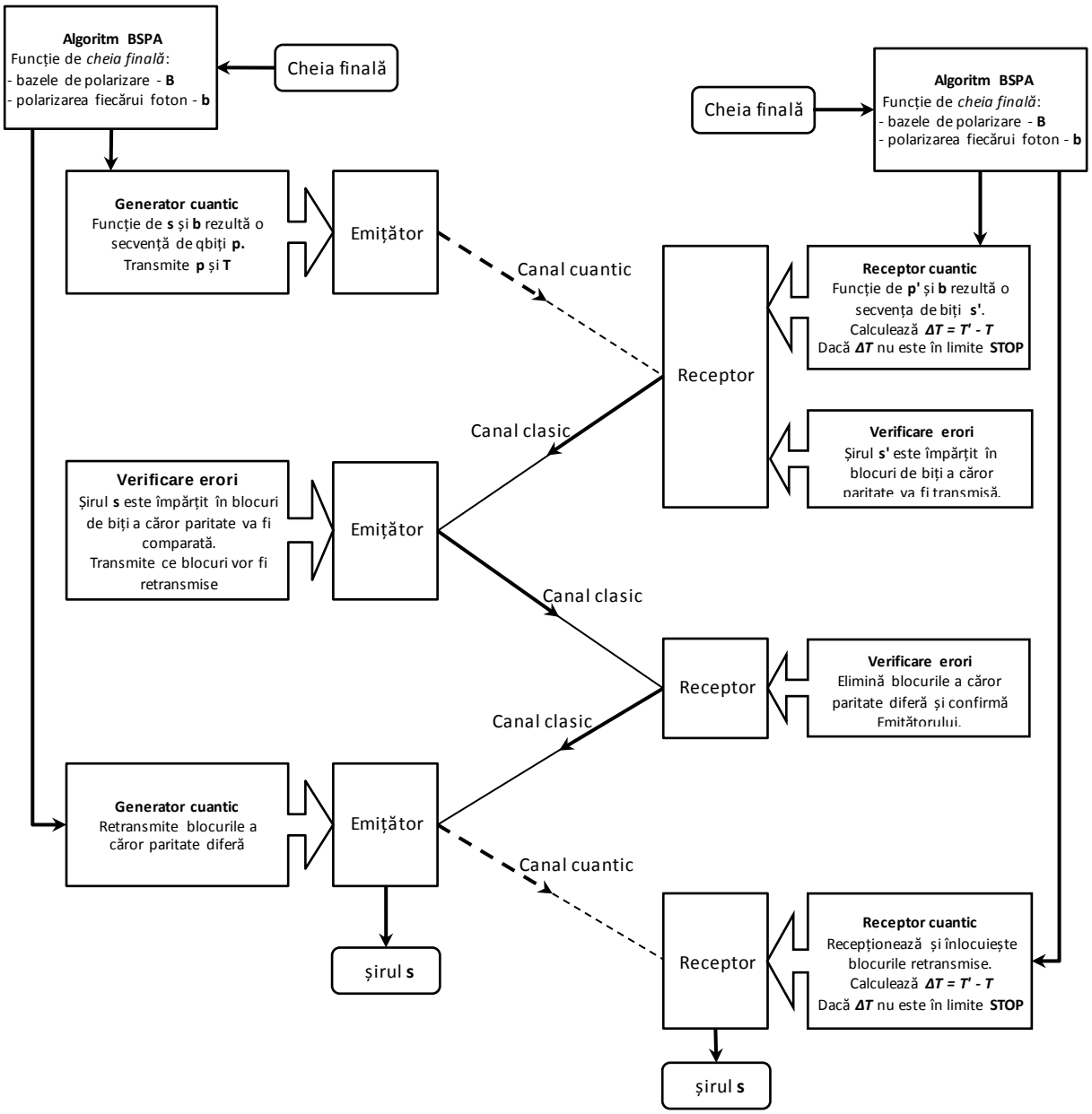

Figura 6.2. Schema logică a protocolului BSPA

6.4 Avantajele protocolului BSPA

Prin implementarea metodei Quantum Bit Travel Time de detectare a inamicului în protocolul cuantic de comunicații Base Selection and Transmission Synchronization obținem protocolul cuantic de comunicații Base Selection and Polarization Agreement în care inamicul poate fi detectat în timpul transmisiei cuantice, după fiecare qbit recepționat și fără dubii că ar putea fi confundat cu perturbări de pe canalului cuantic deoarece zgomotele de pe canalul cuantic nu produc întârzieri ale particulei purtătoare.

Protocolul BSPA este mai simplu, mai sigur și mai rapid, datorită implementării metodei Quantum Bit Travel Time de detectare a inamicului și a eliminării etapei *Transmission Synchronization*.

Având în vedere faptul că un eventual *inamic* este practic depistat imediat ce încearcă să intercepteze transmisia cuantică, algoritmul BSPA realizează un protocol cuantic de comunicații care poate fi implementat pentru a realiza o rețea cuantică de comunicații.

6.5 Concluzii și contribuții

Utilizarea metodei Quantum Bit Travel Time de detectare a inamicului în coroborare cu protocolul cuantic de comunicații Base Selection and Transmission Synchronization duce la obținerea unui nou protocol cuantic de comunicații numit Base Selection and Polarization Agreement - BSPA, în care inamicul poate fi depistat în timpul transmisiei cuantice, după fiecare qbit recepționat și fără dubii că ar putea fi confundat cu perturbări ale transmisiei deoarece zgomotele de pe canalul cuantic nu produc întârzieri ale particulei purtătoare.

Spre diferență de ceilalți algoritmi cuantici care au ca obiectiv doar schimbul cuantic de chei de criptare utilizate în combinație cu algoritmul de one-time pad, algoritmul BSPA realizează o transmisie bidirecțională în totalitate cuantică, rezultând un algoritm cuantic de comunicații între un emițător și un receptor.

Având în vedere faptul că un eventual *inamic* este practic depistat imediat ce încearcă să intercepteze transmisia cuantică, algoritmul BSPA realizează un protocol cuantic de comunicații care poate fi implementat pentru a realiza o rețea cuantică de comunicații.

In concluzie putem spune că implementând metoda de detectare a inamicului QBTT în protocolul BSTS obținem un nou protocol, protocolul BSPA, bidirecțional cuantic de comunicații care realizează corectarea erorilor și stabilește parametrii transmisiei.

Contribuțiile din acest capitol sunt :

- Proiectarea, realizarea și implementarea protocolului criptografic cuantic de comunicații Base Selection and Polarization Agreement.

Aceste contribuții sunt baza următoarelor lucrări științifice :

- Anghel C., „New eavesdropper detection method in quantum cryptography", The annals of "Dunarea de Jos" University of Galati, fascicula III, vol.34, nr. 1, pag. 1-8, 2011.
- Anghel C., „New quantum cryptographic protocol", The annals of "Dunarea de Jos" University of Galati, fascicula III, vol.34, nr. 2, pag. 7-13, 2011.

7. Simularea sistemelor de distribuire a cheilor cuantice

Programele de simulare sunt scrise în C++ și au schema bloc din figura 7.1.

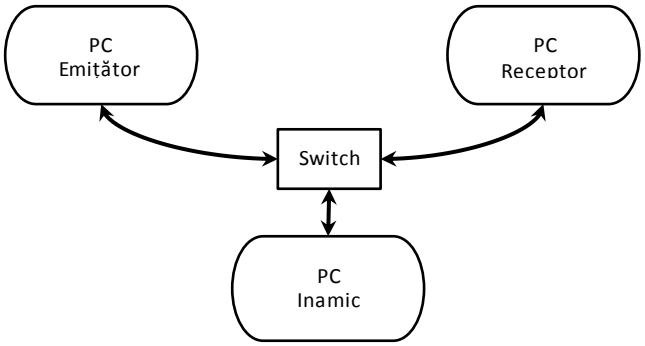

Figura 7.1. Schema bloc a programului de simulare

Pentru reprezentarea qbiților vom folosi convenția din tabelul 7.1.

Baza	Bit	Qbit	Simbol
L	0	→	a
	1	↑	b
D	0	↖	c
	1	↗	d

Tabelul 7.1. Reprezentarea biților în programul de simulare BB84-ideal

7.1 Simularea sistemului BB84 în condiții ideale fără *inamic*

7.1.1 Implementarea software

Pentru implementarea programului de simulare BB84-Ideal am folosit limbajul C++. *Emițătorul* și *Receptorul* vor comunica prin canalul cuantic și cel clasic fără prezența *Inamicului* iar legătura între ei se va face prin intermediul unui switch.

Această aplicație software este formată din 4 obiecte: *Emițătorul*, *Receptorul*, canalul cuantic și canalul clasic. *Emițătorul* va transmite qbiții prin canalul cuantic iar *Receptorul* va extrage acești qbiți din canalul cuantic. La finalul transmisiei cuantice, *Emițătorul* și *Receptorul* vor comunica pe canalul clasic și vor executa etapele *bases reconciliation*, *secret key reconciliation* și *privacy amplification*.

7.1.2 Implementarea hardware

Schema bloc a programului BB84-Ideal este prezentată în figura 7.2.

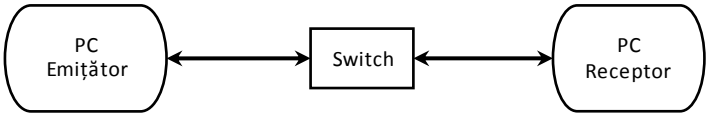

Figura 7.2. Schema bloc a programului de simulare BB84-Ideal

Echipamentele utilizate pentru implementarea programului de simulare BB84-Ideal sunt:

- 2 calculatoare
- 1 switch

Echipamentele sunt conectate între ele prin intermediul unui switch. Fiecare calculator va avea IP static, pentru a putea comunica prin intermediul switch-ului și va rula un program specific emițătorului respectiv receptorului.

7.1.3 Implementarea protocolului

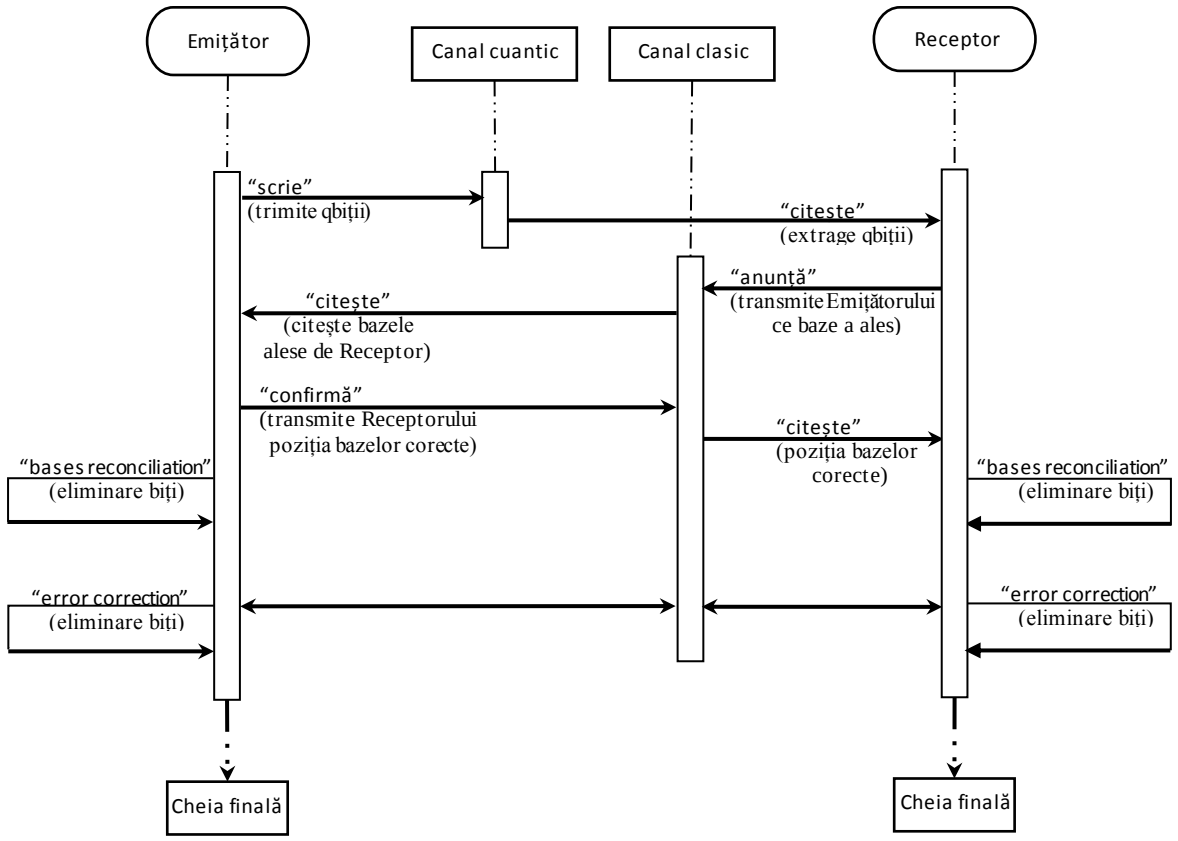

Figura 7.3. Schema funcțională a simulării protocolului BB84-Ideal

7.1.4 Rezultate

În urma rulării programului de simulare BB84-ideal de 10 ori, obținem următoarele rezultate, tabelul 7.2, pentru o *cheia inițială* care are dimensiunea de 320 biți:

Cheia inițială	Cheia finală	QBER %
320	162	49.4
320	161	49.7
320	152	52.5
320	172	46.3
320	158	50.6
320	153	52.2
320	165	48.4
320	163	49.1
320	150	53.1
320	160	50.0

Tabelul 7.2. Simulare BB84 în condiții ideale

Analizând datele obținute putem constata că quantum bit error rate – QBER din *cheia finală* este aproximativ 50%.

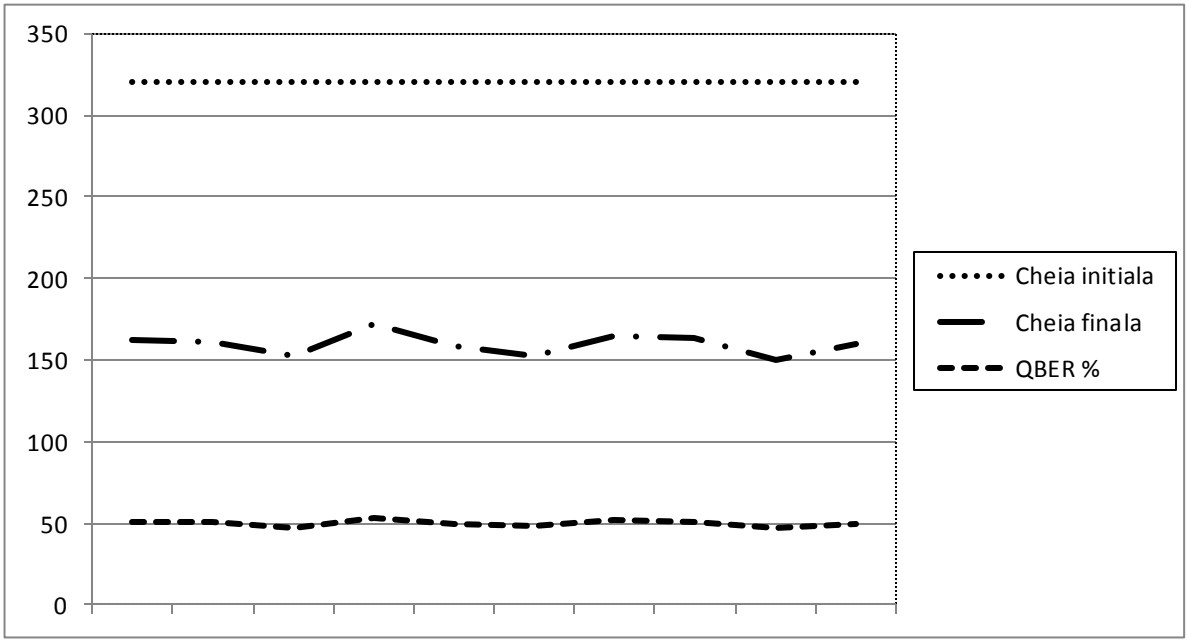

Figura 7.4. Detalii simulare BB84 în condiții ideale

7.2 Simularea sistemului BB84 în condiții ideale cu inamic

7.2.1 Implementarea software

Pentru implementarea programului de simulare BB84 am folosit limbajul C++. *Emițătorul* și *Receptorul* vor comunica prin canalul cuantic și cel clasic, cu sau fără prezența *Inamicului* iar legătura între ei se va face prin intermediul unui switch.

Această aplicație software este formată din 5 obiecte: *Emițătorul*, *Receptorul*, *Inamicul*, canalul cuantic și canalul clasic. *Emițătorul* va transmite qbiții prin canalul cuantic către *Receptor*. *Inamicul*, va întrerupe canalul cuantic, va intercepta qbiții transmiși de către *Emițător*, pe care îi va citi în conformitate cu bazele alese de el și va transmite către *Receptor* alți qbiți în conformitate cu bazele alese de către *Inamic*. *Receptorul* va extrage acești qbiți din canalul cuantic iar la finalul transmisiei cuantice, *Emițătorul* și *Receptorul* vor comunica pe canalul clasic și vor executa etapele *bases reconciliation*, *secret key reconciliation* și *privacy amplification*.

7.2.2 Implementarea hardware

Schema bloc a programului de simulare BB84 este prezentată în figura 7.1. Echipamentele utilizate pentru implementarea programului de simulare BB84 sunt:

- 3 calculatoare
- 1 switch

Echipamentele sunt dispuse în aceeași încăpere și sunt conectate între ele prin intermediul unui switch. Fiecare calculator va avea IP static, pentru a putea comunica prin intermediul switch-ului și va rula un program specific emițătorului, receptorului și respectiv inamicului.

7.2.3 Implementarea protocolului

Schema funcțională a simulării sistemului cuantic de comunicații BB84 cu prezența *Inamicului* este prezentată în figura 7.5.

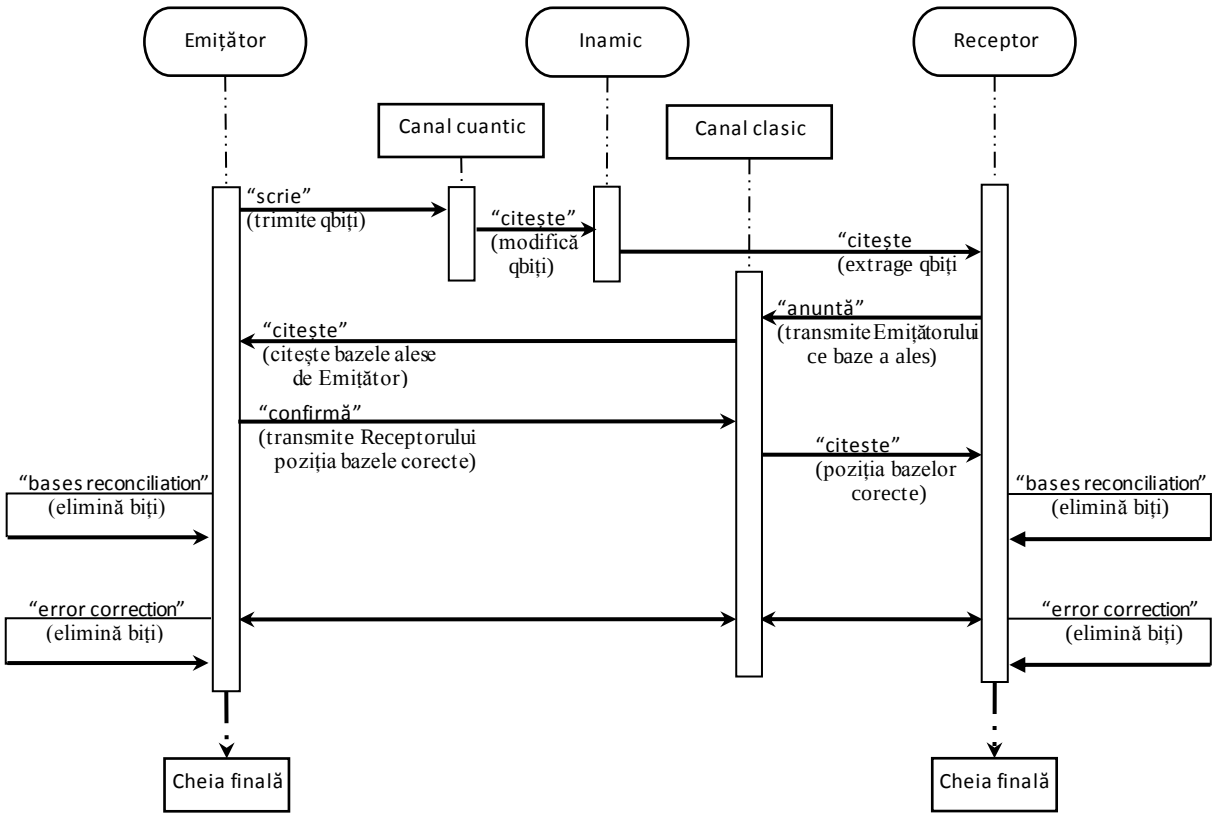

Figura 7.5. Schema funcțională a simulării protocolului BB84

7.2.4 Rezultate

În urma rulării programului de simulare BB84 cu inamic de 10 ori, obținem următoarele rezultate, tabelul 7.3, pentru o cheia inițială care are dimensiunea de 320 biți:

Cheia inițială	Cheia brută	Cheia finală	QBER %
320	149	110	65.6
320	156	114	64.4
320	172	129	59.7
320	164	131	59.1
320	167	126	60.6
320	144	105	67.2
320	159	105	67.2
320	133	108	66.3
320	162	117	63.4
320	171	123	61.6

Tabelul 7.3. Simulare BB84 în condiții ideale cu inamic

Analizând datele obținute putem constata că quantum bit error rate – QBER din *cheia finală* este aproximativ 64 %.

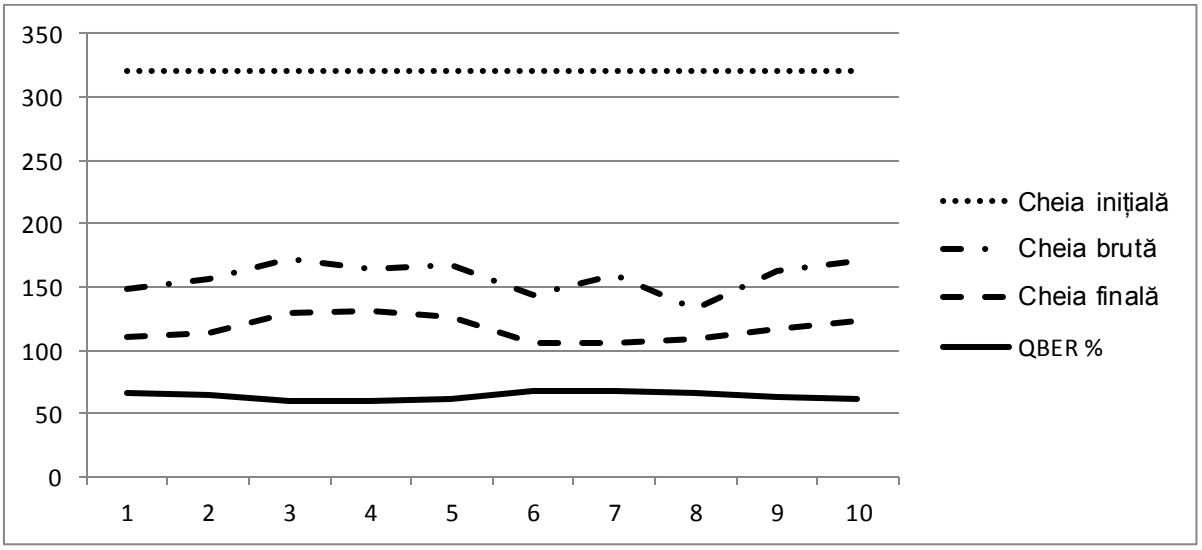

Figura 7.6. Detalii simulare BB84 în condiții ideale cu inamic

7.3 Simularea sistemului BB84 cu metoda QBTT

Programul BB84-QBTT, simulează sistemul de distribuire a cheilor cuantice BB84 și folosește pentru detectarea inamicului metoda QBTT.

Acest program de simulare este aproximativ identic cu programul BB84 cu excepția că detectarea inamicului se face de către *Receptor*, în timpul transmisiei cuantice după fiecare qbit recepționat.

7.3.1 Rezultate

În urma rulării programului de simulare BB84 cu metoda QBTT de 10 ori, obținem următoarele rezultate, tabelul 7.4, pentru o cheia inițială care are dimensiunea de 320 biți:

Cheia inițială	Cheia brută	Cheia finală	QBER %
320	148	148	46.2
320	150	150	46.8
320	167	167	52.1
320	157	157	49
320	159	159	49.6
320	152	152	47.5
320	168	168	52.5
320	157	157	49
320	158	158	49.3
320	162	162	50.6

Tabelul 7.4. Simulare BB84 în condiții ideale cu metoda QBTT

Analizând datele obținute putem constata că quantum bit error rate – QBER este aproximativ 50%.

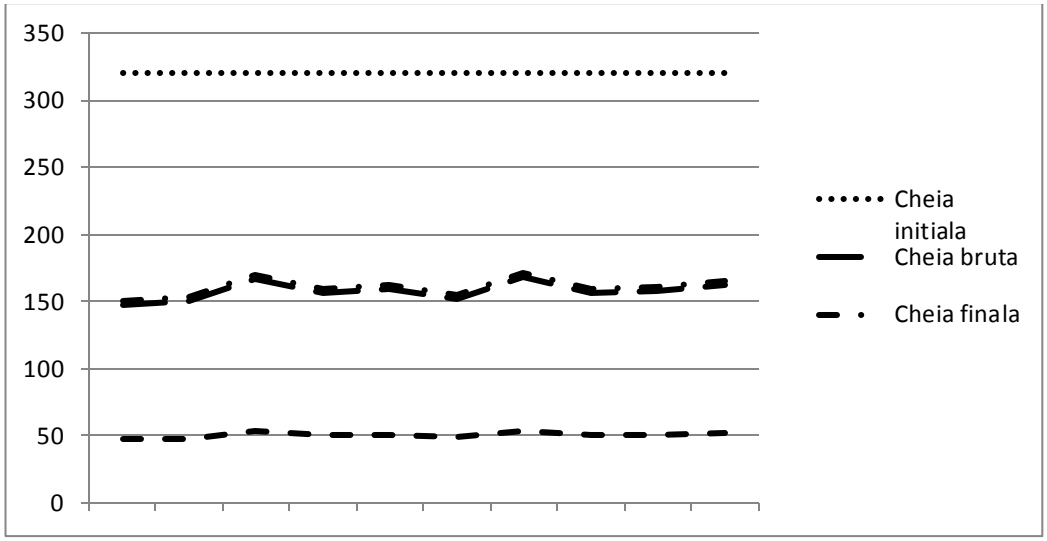

Figura 7.7. Detalii simulare BB84 în condiții ideale cu inamic

7.4 Simularea protocolului BSPA

7.4.1 Implementarea software

Pentru implementarea programului de simulare BSPA am folosit limbajul C++. *Emițătorul* și *Receptorul* vor comunica prin canalul cuantic și cel clasic, cu sau fără prezența *Inamicului* iar legătura între ei se va face prin intermediul unui switch.

Această aplicație software este formată din 5 obiecte: *Emițătorul*, *Receptorul*, *Inamicul*, canalul cuantic și canalul clasic.

În primă fază *emițătorul* și *receptorul* își vor sincroniza ceasurile interne ale dispozitivelor de lucru, în cazul nostru al calculatoarelor.

Prin protocolul cuantic de comunicații BSPA, *emițătorul* și *receptorul* vor stabili în comun, în funcție de biții din *cheia finală* obținută cu ajutorul oricărui sistem de distribuire a cheilor cuantice, care pereche, dintre cele trei baze de polarizare, *liniar-diagonal*, *liniar-circular* sau *diagonal-circular* vor fi folosite pentru polarizarea fotonilor.

În funcție de biții rămași din *cheia finală*, *emițătorul* și *receptorul*, vor ști exact ce baze de polarizare să aplice pentru fiecare foton pe care urmează să-l transmită respectiv să-l recepționeze.

Emițătorul, pentru fiecare qbit transmis către *receptor* va transmite, pe canalul clasic timestamp-ul momentului emisiei time-stamp_e. La rândul său, *receptorul*, pentru fiecare qbit recepționat, citește timestamp-ul transmis de către *emițător* și generează timestamp-ul momentului recepției time-stamp_r, calculând întârzierea ΔT= time-stamp_r - time-stamp_e.

Dacă *inamicul* interceptează qbiții transmiși de către *emițător*, *receptorul* va sesiza acest lucru prin creșterea timpului parcurs de qbit și va opri transmisia, prin calcularea întârzierii ΔT = time-stamp_r - time-stamp_e.

7.4.2 Implementarea hardware

Schema bloc a programului de simulare BSPA este prezentată în figura 7.1. Echipamentele utilizate pentru implementarea programului de simulare BB84 sunt:

- 3 calculatoare și 1 switch;

Echipamentele sunt dispuse în aceeași încăpere și sunt conectate între ele prin intermediul unui switch. Fiecare calculator va avea IP static, pentru a putea comunica prin intermediul switch-ului și va rula un program specific emițătorului, receptorului și respectiv inamicului.

7.4.3 Implementarea protocolului

Schema funcțională a programului de simulare a protocolului BSPA este prezentată în figura 7.8.

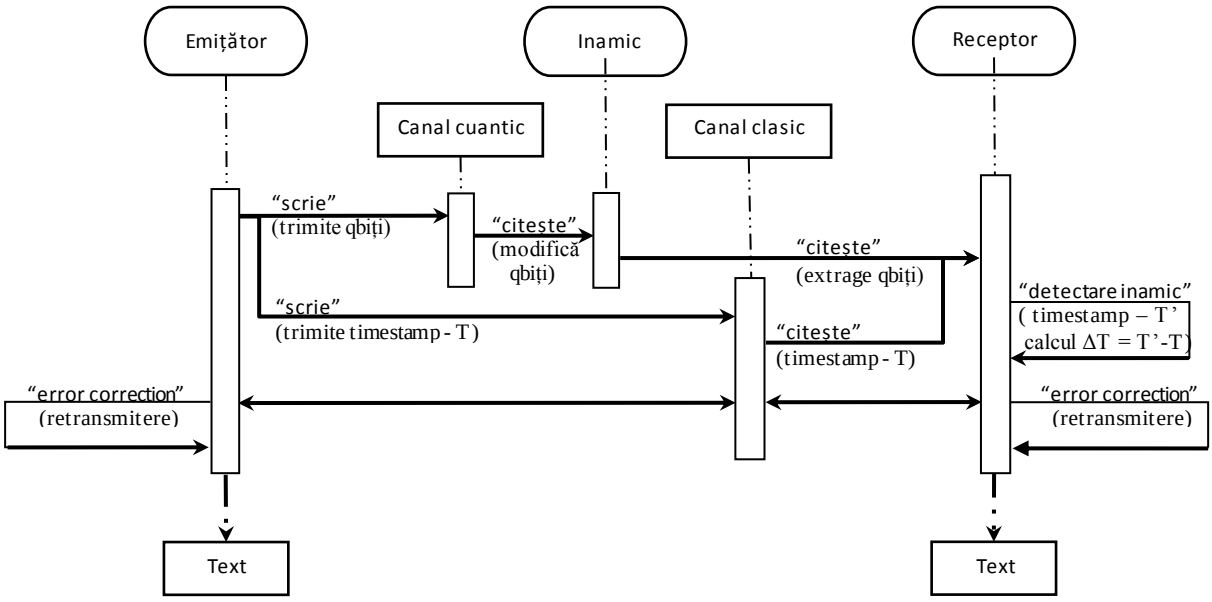

Figura 7.8. Schema funcțională a programului de simulare BSPA

7.4.4 Rezultate

În urma rulării programului de simulare BSPA de 10 ori, obținem următoarele rezultate, tabelul 7.5, pentru o cheie inițială care are dimensiunea de 320 biți:

Cheia inițială	Cheia finală	QBER %
320	320	0.0
320	317	0.9
320	320	0.0
320	319	0.3
320	320	0.0
320	317	0.9
320	320	0.0
320	319	0.3
320	320	0.0
320	319	0.3

Tabelul 7.5. Simulare BSPA

Analizând datele obținute putem constata că, *cheia finală* are aproximativ aceeași lungime cu *cheia inițială* iar procentul de erori din *cheia finală*, quantum bit error rate – QBER este de 0.27 % - figura 7.9.

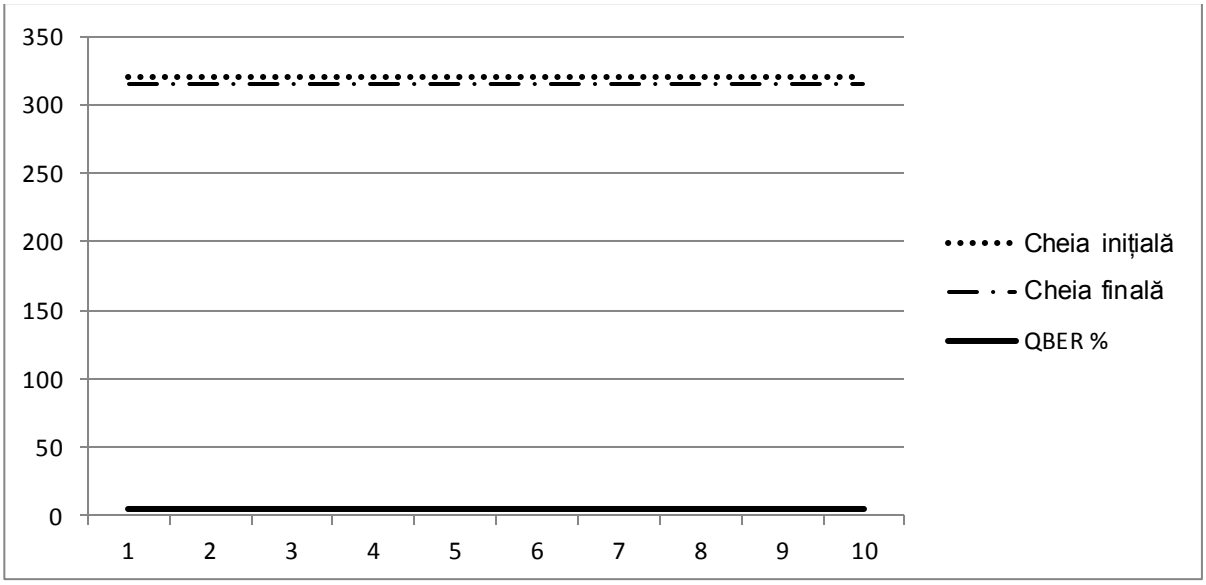

Figura 7.9. Detalii simulare BSPA

7.5 Concluzii și contribuții

Programele de simulare realizate, simulează protocolul Base Selection and Polarization Agreement și un sistem de distribuire a cheilor cuantice realizat cu ajutorul algoritmului BB84, în diverse situații, cum ar fi în condiții ideale fără inamic, în condiții ideale cu inamic și în condiții ideale cu inamic dar folosind metoda QBTT de detectare a inamicului.

Comparând dimensiunea cheii finale, rezultată în urma rulării celor patru programe de simulare BB84 ideal, BB84 inamic, BB84 QBTT și BSPA, observăm că algoritmul BSPA ne oferă cea mai mare cheie iar metoda QBTT de detectare a inamicului îmbunătățește semnificativ dimensiunea cheii finale în cazul algoritmul BB84 cu inamic, tabelul 7.6 și figura 7.10.

Cheia inițială	Cheia finală BB84 ideal	Cheia finală BB84 inamic	Cheia finală BB84 QBTT	Cheia finală BSPA
320	159.6	116.8	157.8	318.7

Tabelul 7.6. Comparație între cheia inițială și cheia finală

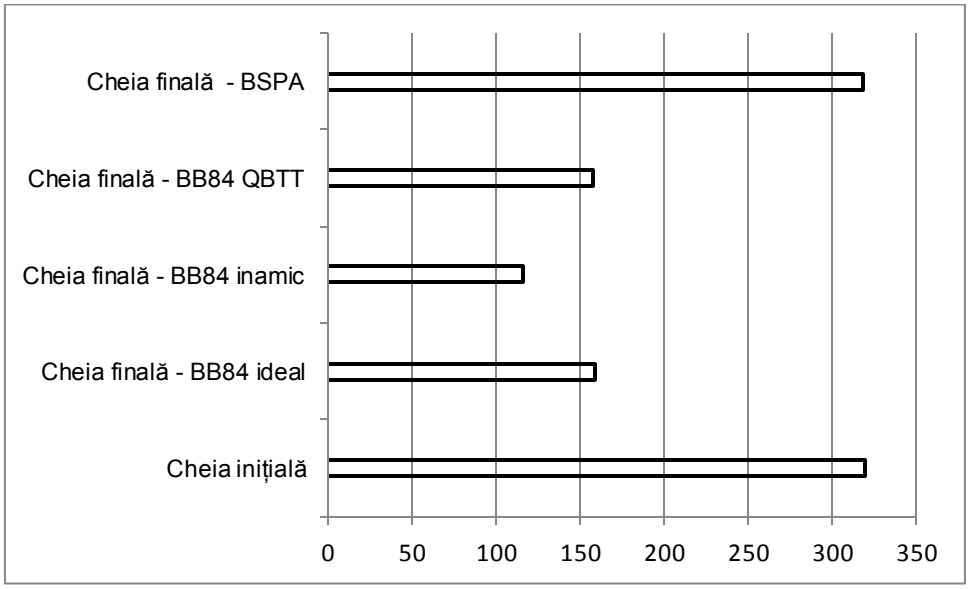

Figura 7.10. Comparație între cheia inițială și cheia finală

Se pot observa avantajele metodei QBTT de detectare a inamicului prin scăderea procentului de erori din cheia finală – QBER și avantajele protocolului cuantic BSPA prin reducerea aproape de 0 a procentului de erori din cheia finală, tabelul 7.7 și figura 7.11.

QBER % BB84 ideal	QBER % BB84 inamic	QBER % BB84 QBTT	QBER % BSPA
50.1	63.5	49.1	0.2

Tabelul 7.7. Comparație între QBER ale celor patru programe de simulare

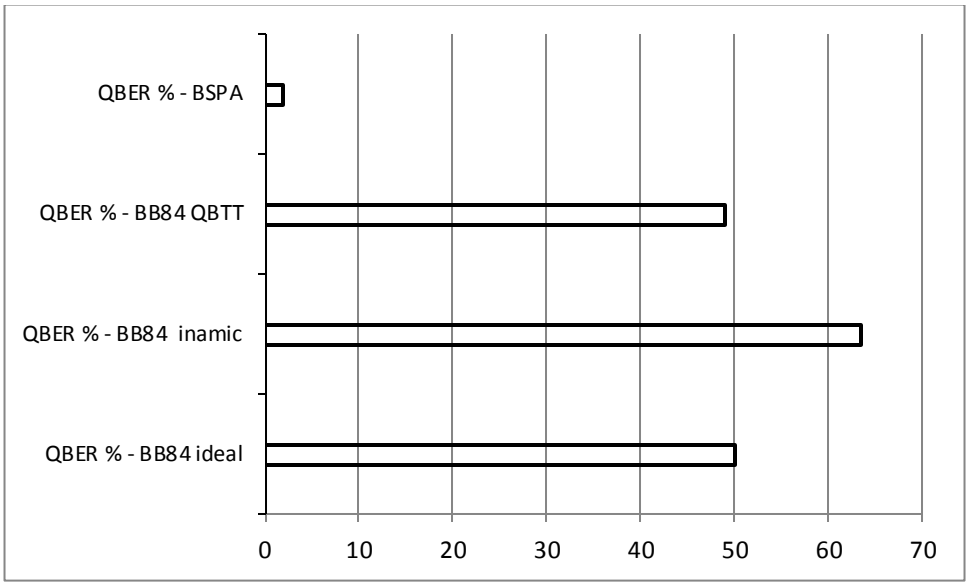

Figura 7.11. Comparație între QBER ale celor patru programe de simulare

Contribuțiile din acest capitol sunt :

- Proiectarea, realizarea și implementarea programelor de simulare a sistemelor de distribuire a cheilor cuantice.

Aceste contribuții sunt baza următoarelor lucrări științifice :

- Anghel C., „Research, Development and Simulation of Quantum Cryptographic Protocols", acceptată pentru publicare în revista „Electronics and Electrical Engineering".

8. Concluzii, contribuții și direcții de cercetare

8.1 Concluzii

Criptografia cuantică și în special sistemele de distribuire a cheilor cuantice – Quantum Key Distribution, realizează un schimb de chei cuantice între *emițător* și *receptor*. Acest schimb de chei cuantice se face în două etape, printr-un canal cuantic (fibră optică) și printr-un canal public (internet sau telefon). Cea mai importantă caracteristică a unui sistem de distribuire a cheilor cuantice și în special a criptografiei cuantice este că, orice încercare de interceptare a comunicației, nu numai că nu poate fi realizată, dar alertează și părțile legitime care comunică.

Protocol Base Selection and Transmission Synchronization [3] utilizează *cheia finală* rezultată după etapele *secret key reconciliation* și *privacy amplification*, ale oricărui sistem de distribuire a cheilor cuantice. În funcție de *cheia finală*, *emițătorul* și *receptorul* vor stabili cu exactitate parametrii utilizați în transmisia cuantică, respectiv sistemul de baze de polarizare utilizat, tactul transmisiei și tipul de polarizare aplicat fiecărui foton în parte.

Datorită faptului că, încă din 1985, au fost descrise principiile de funcționare ale unui calculator cuantic [20], ne putem aștepta ca atunci când va fi operațional, algoritmul one-time pad să poată fi spart. Acest lucru va face ca schemele de distribuire a cheilor cuantice să fie inutile, dar folosind algoritmul Base Selection and Transmission Synchronization – BSTS, care realizează o transmisie bidirecțională în totalitate cuantică vom putea comunica în secret.

Protocolul BSTS poate fi considerat un protocol de rețea cuantic între două calculatoare deoarece poate realiza o legătură bidirecțională între ele. Prin intermediul protocolului BSTS nu se dorește realizarea doar a unui schimb de chei cuantice, ca în cazul celorlalți algoritmi de distribuire a cheilor cuantice gen BB84, B92 sau E91, ci a se realiza o transmisie bidirecțională între cele două părți care comunică.

În concluzie putem spune că algoritmul Base Selection and Transmission Synchronization va realiza o transmisie respectiv recepție, fără erori datorită faptului că *emițătorul* și *receptorul* vor ști exact cum să polarizeze, respectiv să citească fiecare qbit în parte iar la sfârșitul transmisie se va realiza o corectare a erorilor.

Metoda Quantum Bit Travel Time – QBTT [5], prezintă avantajele că *inamicul* poate fi detectat „imediat" și cu „exactitate".

Receptorul poate detecta „imediat" prezența *inamicului* în timpul transmisiei cuantice, după fiecare qbit recepționat, prin măsurarea timpului parcurs de particula purtătoare de la *emițător* la *receptor*. În cazul altor algoritmilor de distribuire a cheilor cuantice, detectarea *inamicului* se face după finalizarea transmisiei cuantice, în etapa de comunicare a bazelor de polarizare pe canalul clasic, lăsând astfel în mâna *inamicului* informații importante legate de transmisie.

Inamicul poate fi depistat cu „exactitate" deoarece perturbările naturale apărute pe canalul cuantic nu produc întârzieri ale particulei purtătoare ci doar modificări ale polarizării. Această proprietate ne ajută să nu confundăm eventualele zgomotele de pe canalul cuantic cu prezența unui *inamic*. Alte metode de depistare a inamicului nu pot face diferența între zgomot și *inamic*.

Am văzut, în capitolul 3, că există anumite metode de atac [16,30,35], metode pur teoretice deocamdată, în care *inamicul*, chiar dacă interceptează transmisia, nu poate fi detectat prin metodele actuale și care pot compromite în totalitate transmisia cuantică dintre *emițător* și *receptor*. În schimb, prin utilizarea metodei Quantum Bit Travel Time, *inamicul* poate fi detectat imediat ce a intervenit pentru a citi un qbit, indiferent de metoda de atac folosită.

În concluzie putem spune că metoda Quantum Bit Travel Time - QBTT de detectare a inamicului poate fi implementată în oricare sistem de distribuire a cheilor cuantice și are avantajul că *inamicul* poate fi detectat cu *exactitate* și mai ales *imediat* după ce acesta a intervenit pentru a citi un qbit, în timpul transmisiei cuantice.

Prin implementarea metodei Quantum Bit Travel Time de detectare a inamicului în protocolul cuantic de comunicații Base Selection and Transmission Synchronization obținem un nou protocol cuantic de comunicații numit Base Selection and Polarization Agreement – BSPA [6], în care inamicul poate fi detectat în timpul transmisiei cuantice, după fiecare qbit recepționat și fără dubii că ar putea fi confundat cu perturbări ale transmisiei deoarece zgomotele de pe canalul cuantic nu produc întârzieri ale particulei purtătoare.

Spre diferență de ceilalți algoritmi cuantici care au ca obiectiv doar schimbul cuantic de chei de criptare utilizate în combinație cu algoritmul de one-time pad,

algoritmul BSPA realizează o transmisie bidirecțională în totalitate cuantică, rezultând un algoritm cuantic de comunicații între un emițător și un receptor.

Având în vedere faptul că un eventual *inamic* este practic depistat imediat ce încearcă să intercepteze transmisia cuantică, algoritmul BSPA realizează un protocol cuantic de comunicații care poate fi implementat pentru a realiza o rețea cuantică de comunicații.

În concluzie putem spune că implementând metoda de detectare a inamicului QBTT în protocolul BSTS obținem un nou protocol, protocolul BSPA, bidirecțional cuantic de comunicații care stabilește parametrii transmisiei și realizează corectarea erorilor.

8.2 Contribuții

Principalele contribuții din cadrul tezei de doctorat sunt :

- Proiectarea, realizarea și implementarea protocolul criptografic cuantic de comunicații Base Selection and Transmission Synchronization – BSTS.
- Proiectarea, realizarea și implementarea metodei de detectare a inamicului Quantum Bit Travel Time – QBTT.
- Proiectarea, realizarea și implementarea protocolului criptografic cuantic de comunicații Base Selection and Polarization Agreement – BSPA.
- Proiectarea, realizarea și implementarea programelor de simulare a sistemelor de distribuire a cheilor cuantice.

8.3 Diseminarea rezultatelor cercetării

Rezultatele cercetărilor doctorale au fost prezentate în 6 articole publicate sau acceptate spre publicare din care : 1 lucrare în revistă indexată ISI cu factor de impact 0.913, 2 lucrări în reviste indexate BDI, 2 lucrări la conferințe internaționale și 1 lucrare în biblioteca electronică Cornell University Library din SUA.

Reviste ISI cu factor de impact

- Anghel C., „Research, Development and Simulation of Quantum Cryptographic Protocols", acceptată pentru publicare în „Electronics and Electrical Engineering", (cotată ISI, factor de impact 0.913).

Reviste indexate BDI

- Anghel C., „New eavesdropper detection method in quantum cryptography", The annals of "Dunarea de Jos" University of Galati, fascicula III, vol.34, nr. 1, pag. 1-8, 2011.
- Anghel C., „New quantum cryptographic protocol", The annals of "Dunarea de Jos" University of Galati, fascicula III, vol.34, nr. 2, pag. 7-13, 2011.

Conferințe internaționale

- Anghel C., „Quantum cryptography algorithm", Proceedings ECIT2008 – 5th European Conference on Intelligent Systems and Technologies, Romania, Iasi, 2008.
- Anghel C. & Coman G., „Base selection and transmission synchronization algorithm in quantum cryptography", Proceedings CSCS17 - 17th International Conference on Control Systems and Computer Science, Romania, Bucharest, ISSN : 2066-4451, vol. 1, pag. 281-284, 2009.

Biblioteca electronică

- Anghel C., „Creșterea securității Sistemelor Informatice și de Comunicații prin Criptografia Cuantică", Cornell University Library, http://arxiv.org/, cite as: http://arxiv.org/abs/1006.5381v1, 2010.

8.4 Direcții de cercetare

Direcțiile de cercetare în domeniul criptografiei cuantice sunt concentrate pe mai multe planuri: *mărirea dimensiunii cheii de criptare finale*, *securitatea algoritmilor de distribuire a cheilor cuantice*, *mărirea distanței dintre părțile care comunică*, *crearea unor algoritmi noi și îmbunătățirea celor existenți*, *utilizarea sateliților pentru realizarea transmisiei*, *repetoare cuantice*, *memorii cuantice*, *rețele cuantice*, *calculatoare cuantice*.

BIBLIOGRAFIE

[1]. Alleaume R., et al., „SECOQC White Paper on Quantum Key Distribution and Cryptography", arXiv:quant-ph/0701168v1, 2007.

[2]. Anghel C., „Quantum cryptography algorithm", Proceedings ECIT2008 – 5th European Conference on Intelligent Systems and Technologies, Romania, Iasi, 2008.

[3]. Anghel C. & Coman G., „Base selection and transmission synchronization algorithm in quantum cryptography", Proceedings CSCS17 - 17th International Conference on Control Systems and Computer Science, Romania, Bucharest, ISSN : 2066-4451, vol. 1, pag. 281-284, 2009.

[4]. Anghel C., „Creșterea securității Sistemelor Informatice și de Comunicații prin Criptografia Cuantică", Cornell University Library, http://arxiv.org/, cite as: http://arxiv.org/abs/1006.5381v1, 2010.

[5]. Anghel C., „New eavesdropper detection method in quantum cryptography", The annals of "Dunarea de Jos" University of Galati, fascicula III, vol.34, nr. 1, pag. 1-8, 2011

[6]. Anghel C., „New quantum cryptographic protocol", The annals of "Dunarea de Jos" University of Galati, fascicula III, vol.34, nr. 2, pag. 7-13, 2011.

[7]. Anghel C., „Software simulation of quantum key distribution systems", acceptată pentru publicare în : „Electronics and Electrical Engineering", (cotată ISI, factor de impact 0.913).

[8]. Bell J.S., „On the Einstein-Podolsky-Rosen paradox", Physics 1, vol. 1, nr. 3, pag. 195-200, 1964.

[9]. Bennett C.H., Brassards G. & Jean-Marc R., „Privacy amplification by public discussions", Siam Journal on Computing, vol. 17, nr. 2, pag. 210-229, 1988.

[10]. Bennett C.H. & Brassard G., „Quantum cryptography : Public key distribution and coin tossing", Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, pag. 175-179, 1984.

[11]. Bennett C.H., Bessette F., Brassard G., Salvail L., & Smolin J., „Experimental quantum cryptography", Journal of Cryptology, vol. 5, no. 1, pag. 3-28, 1992.

[12]. Bennett C.H., „Quantum cryptography using any two nonorthogonal states", Physical Review Letters, vol. 68, pag. 3121-3124, 1992.

[13]. Bouwmeester D., Ekert A. & Zeilinger A., „The Physics of Quantum Information. Quantum Cryptography, Quantum Teleportation, Quantum Computation", Springer, pag. 314, 2000.

[14]. Branciard C., Gisin N., Kraus B. & Scarani V., „Security of two quantum cryptography protocols using the same four qubit states", Physical Review A, vol. 72, nr. 3, 2005.

[15]. Brassard G., Lutkenhaus N., Mor T. & Sanders B., „Limitations on practical quantum cryptography", Physical Review Letters, vol. 85, nr. 6, pag. 1330-1333, 2000.

[16]. Brassard G., Lütkenhaus N., Mor T & Sanders B.C., „Limitation on practical quantum cryptography", Physical Review Letters, Vol. 85, pag. 1330-1333, 2000.

[17]. Bruss D., „Optimal Eavesdropping in Quantum Cryptography with Six States", Physical Review Letters, vol. 81, nr. 14, pag. 3018-3021, 1998.

[18]. De Burgh M. & Bartlett S.D., „Quantum methods for clock synchronization: Beating the standard quantum limit without entanglement", Physical Review A, vol. 72, 2005.

[19]. Desurvire E., „Classical and Quantum Information Theory", Cambridge University Press, vol. 691, 2009.

[20]. Deutsch D., „Quantum theory, the Church-Turing principle and the universal quantum computer", Proceedings of the Royal Society of London A, vol. 400, pag. 97-117, 1985.

[21]. Durt T., Kaszlikowski D., Chen J.L. & Kwek L.C., „Security of quantum key distributions with entangled qudits", Physical Review A, vol. 69, nr. 3, pag. 1-11, 2004.

[22]. Einstein A., Podolsky B. & Rosen N., „Can quantum, mechanical description of physical reality be considered complete?", Physical Review, vol. 47, pag. 777-780, 1935.

[23]. Ekert A., „Quantum cryptography based on Bell's theorem", Physical Review Letters, vol. 67, nr. 6, pag. 661-663, 1991.

[24]. Gisin N. & Huttner B., „Quantum cloning, eavesdropping and Bell's inequality", Physics Letters A, vol. 228, pag. 13-21, 1997.

[25]. Gisin N., Ribordy G., Tittle W. & Zbinden H., "Quantum cryptography", Reviews of Modern Physics, vol. 74, 2002.

[26]. Gupta N.L., Mehrotra D.R. & Saxena A., „Quantum cryptographic protocols for secure communication", Journal of Computer Science, vol. 8, nr.1, pag. 65-74, 2009.

[27]. Harrelson C. & Kerenidis I., „Quantum clock synchronization with one qubit", http://arxiv.org/abs/cs/0103021v3, 2001.

[28]. Heisenberg W., „About the perceptual content of quantum kinematics and mechanics", Journal of Physics, vol. 43, pag. 172-198, 1927.

[29]. Huang D., Chen Z., Guo Y. & Lee M., „Quantum secure direct communication based on chaos with authentication", Journal of the Physical Society of Japan, vol. 76, 2007.

[30]. Huttner B., Imoto N., Gisin N. & Mor T., „Quantum cryptography with coherent states", Physical Review A, vol. 51, pag. 1863-1869, 1995.

[31]. Inamori H., Rallan L. & Vedral V., „Security of EPR-based quantum cryptography against incoherent symmetric attacks", Journal of Physics A, vol. 34, nr. 35, pag. 6913-6918, 2001.

[32]. Jozsa R., Abrams D.S., Dowling J.P. & Williams C.P., „Quantum Clock Synchronization Based on Shared Prior Entanglement", Physical Review Letters, vol. 85, pag. 2010-2013, 2000.

[33]. Kaszlikowski D., Christandl M. et al., „Quantum cryptography based on qutrit Bell inequalities", Physical Review A, vol. 67, nr. 1, 2003.

[34]. Kwiat P.G., Mattle K., Weinfurter H., Zeilinger A., Sergienko A.V. & Shih Y., „New High-Intensity Source of Polarization-Entangled Photon Pairs", Physical Review Letters, nr. 75, pag. 4337, 1995.

[35]. Makarov V., Anisimov A. & Skaar J., „Effects of detector efficiency mismatch on security of quantum cryptosystems", Physical Review A, vol. 74, pag. 1-11, 2005.

[36]. Nielsen M.A. & Chuang I.L., „Quantum Computation and Quantum Information", Cambridge University Press, 2000.

[37]. Scarani V., Bechmann-Pasquinucci H., Cerf N.J. et al., „The security of practical quantum key distribution", Review of Modern Physics, vol. 81, pag. 1301-1350, 2009.

[38]. Shannon C., „Communication theory of secrecy systems", Bell System Technical Journal, vol. 28, pag. 656-715, 1949.

[39]. Simon J.P., & Townsend P.D., „Quantum cryptography: how to beat the code breakers using quantum mechanics", Comtemporay Physics, vol. 36, nr. 3, pag. 165-195, 1995.

[40]. Townsend P.D., Rarity J.G. & Tapster P.R., „Single photon interference in 10km long optical fibre interferometer", Electronic Letters, vol. 29, pag. 634-635, 1993.

[41]. Townsend P.D., „Secure key distribution system based on quantum cryptography", Electronic Letters, vol. 30, nr. 10, pag. 809-811, 1994.

[42]. Townsend P.D. & Thompson I., „A quantum key distribution channel based on optical fibre", Journal of Modern Optics, vol. 41, nr. 12, pag. 2425-2433, 1994.

[43]. Treiber A., „A fully automated quantum cryptography system based on entanglement for optical fibre networks", New Journal of Physics, vol. 11, 2009.

[44]. Vernam G., „Secret signaling system", U.S. patent No. 1310719, 1919.

[45]. Vernam G., „Cipher printing telegraph system for secret wire and radio telegraphic communications," Journal of lEEE, vol. 55, pag. 109-115, 1926.

[46]. Zeilinger A., „Dance of the Photons: From Einstein to Quantum Teleportation", pag. 205, New York, 2010.

[47]. Zhao S. & De Raedt H., „Event-by-event Simulation of Quantum Cryptography Protocols", Journal of Computational and Theoretical Nanoscience, vol. 5, nr. 4, pag. 490-504, 2008.

[48]. Zhang Z., Liu J., Wang D. & Shi S., „Quantum direct communication with authentication", Physical Review A, vol. 75, 2007.