# QUANTUM CRYPTOGRAPHY BASED EMAIL COMMUNICATION THROUGH INTERNET

V.ANUSUYA DEVI

Lecturer
Department of Computer Science and Engineering
National Engineering College, Kovilpatti, Tuticorin-628503, Tamilnadu, India

T.SAMPRADEEPRAJ

Lecturer
Department of Computer Science and Engineering
National Engineering College, Kovilpatti, Tuticorin-628503, Tamilnadu, India

## Abstract

The Secure message authentication is an important part of quantum cryptography. The eavesdropper gains partial knowledge on the key in cryptography. Partial knowledge has little result on the authentication part of the system. Using BB84 protocol, the sender will generate the random number, the random number sent as a secret shared key. The secret shared key also called as “check bits”. The communication parties are getting together and then they form as a single group depending upon the category. It is proposed to share the information among the communicating parties using quantum cryptography without any attack.

***KEYTERMS: Qubits, Checkbits, QuantumBasis, QKD protocol***

## I. Introduction

Conventional cryptosystem such as DES, RSA are based on mixture of guesswork and mathematical background. Information theory shows that traditional secret key cryptosystem cannot be totally secure unless the key used once only. In Quantum mechanics, the information is protected by the law of physics. The Heisenberg uncertainty principle and quantum entanglement can be combined in a system often referred to as “Quantum cryptography”. Quantum cryptography Provide complete security of communication for two parties to exchange an Enciphering key over a private channel. C.H Bennett and G.Brassard [27] had applied quantum mechanical principles to the task of exchanging secret messages. The “BB84” scheme for Quantum key distribution, named after Bennett and Brassard’s seminal 1984 paper. Heisenberg uncertainty principle from quantum physics, which is used to detect the presence of eavesdropping during communication.

A photon is an elementary partial of light, it carries fixed amount of energy. Light may be polarized; polarization is a physical property that emerges when light is regarded as an electromagneticwave.A photon which is rectilinearly polarized has a polarization direction at 0° or 90° with respect to the horizontal. A diagonally polarized photon has a polarization direction at 45° or 135°.It is possible to use polarized photons to represent individual bits in a key or a message. The process of mapping a sequence of bits to a sequence of rectilinearly and diagonally polarized photons is referred to as “conjugate coding”. While the rectilinear and diagonal polarizations are known as conjugate variables.

Comparisons of Quantum basis and binary values are produce the Qubit, which is used to provide secure environment for sharing secret key among communicating parties. The paper has organized to explain the related work in section 2, Table 1.comparision of quantum basis and binary values

| | | | |
|---|---|---|---|
| Rectilinear Polarization node | + | ↑ | → |
| Diagonal Polarization node | × | ↗ | ↖ |
| Bit Value | | 0 | 1 |

Proposed methodology in section 3, experimental result in section 4 and concludes the work in section 5.

**II. Related work**

Mehrdaa S. Sharbaf [1] has proposed that Quantum key distribution protocols implementation is based on sifting, Error detection and Correction, Privacy amplification and Authentication processes.

Justin Mullins [2] has focused that Satellites to communicate across thousands of kilometers using unbreakable codes whose security is provided by the law of quantum physics.

Cederlof .J [3] has discussed that; the sender will generate the random number. The number sent as a secret shared key. The unauthorized person cannot understand the random number. The secret key also called as check bits. Single photons with the qubit coded in the photons polarization QKG system contains the following steps

- Raw key generation
- Sifting
- Error correction or key reconciliation
- Privacy amplification
- Authentication

Moni Naor et al [4] have presented that, in the Computational setting one-way functions are necessary for the existence of protocols and breaking the lower bounds states.Stamatics .V [5] has planned that, optical networks based on the Wavelength Division multiplexing (WDM) technology transport a total traffic that exceeds terabits per second (Tbps) in a single fiber, secure optical links between nodes, helps to avoid that eavesdroppers tapping the light stream from fiber.

Klye Martin [6] has discussed that, in quantum communication, the noise in the hidden channel decreases an eavesdropper is able to learn less and less. Zonelin Hwang et al [7] have proposed that, three-party Quantum Key Distribution Protocol (QKDPs) easily resist replay and passive attacks. Three-party QKDPs have fewer communication rounds than other protocols.

Vishnu Teja et al [8] have focused that, based on efficiency, recovery time and commercial aspects avalanche photo diodes are used for efficient photon detection unit which will be the deciding parameter for the whole success of quantum cryptography.Rajni Goel et al [9] have presented that, quantum cryptography will be an advanced code making technology which is theoretically uncrackable.This is because of the laws of quantum physics. If an eavesdropper is able to listen in on a line, he could be unable to learn much about the communications traversing it. Toyan et al [10] have proposed that, for maintains of greater safety to use Symmetric cryptographic algorithms for enciphering. Secure key exchange is based on quantum cryptography is provide more security for communication system. William C Barge [11] has discussed that, a new concept called as a hotring and cyber spot are based on webring.Hotrings are used to meet various requirements placed on cyber cafés and cyber spots.

Valdislav .S et al [12] have projected that, encryption process can be done by one time pad. Secure one time pad uses a long key. Secure key agreement protocol is transformed into secure encryption scheme.

Thi Mai Trang et al [13] have focused that, a modified version of the 4-way handshake is quantum handshake. It is used to integrate the BB84 protocol for the distribution of the cryptographic keys used by 802.11.Distributing secret key between users in a manner that it is impossible for a third party to eavesdrops without disturbing the quantum transmission.

Xiao Tang et al [14] have proposed that, a complete fiber - based polarization encoding quantum key distribution system based on the BB84 protocol can be operated at a sifted key rate of more than 4 Mbits/s over optical fiber of length 1 km and mean photon number 0.1.Stamatics V [16] has presented that optical communications technology is a Dense Wavelength division multiplexing, it transfer several terabits per second of aggregate traffic in a single fiber. Quantum cryptography establishes a secret key protected to eavesdropping assuring that the key is unbreakable. Migues et al [17] have proposed that, the best attack could consist of eve preparing N copies of the most entropic state. If this was true, provide a necessary and sufficient condition for a secure QKD over a lossy line using coherent states and homodyne measurements.Nobert [18] has planned that any signal space spanned by two quantum mechanical overlapping signal states. The new protocol can generate unconditionally secure keys for secret communications. A protocol for Quantum Key Distribution is not only test for eavesdropping, it must also establish procedures that allow Alice and Bob to agree via the signal on a common key.

Justin Mullins [23] has focused that, Quantum cryptography solves the problem of key distribution. Cipher text is added with the key .If the receiver knows the key, he (or) she can easily decode the message by subtracting key from the cipher text. Townsend [25] has discussed that depending on link effect, secure QKD results are reduced key rates. The satellite based QKD is feasible of secure key exchange with low earth orbit. Bennett C.H., et al [27] has introduced that, the first QKD protocol and uses two-dimensional quantum systems or qubits as information carriers. A protocol for Coin-tossing by exchange of quantum messages, which is secure against traditional kinds of cheating.

## III. Proposed Methodology

BB84, SARG04, E91, COW, DPS and S09 are Quantum key distribution protocols. Other than BB84 protocols are having the problem of secure identification, handling weak pluses of detectors, create a bit errors during the communication, and using COW protocol in three-way concept situation. Because of these reasons, BB84 is the best of other QKD protocols and this project implementation is based on BB84 protocol.

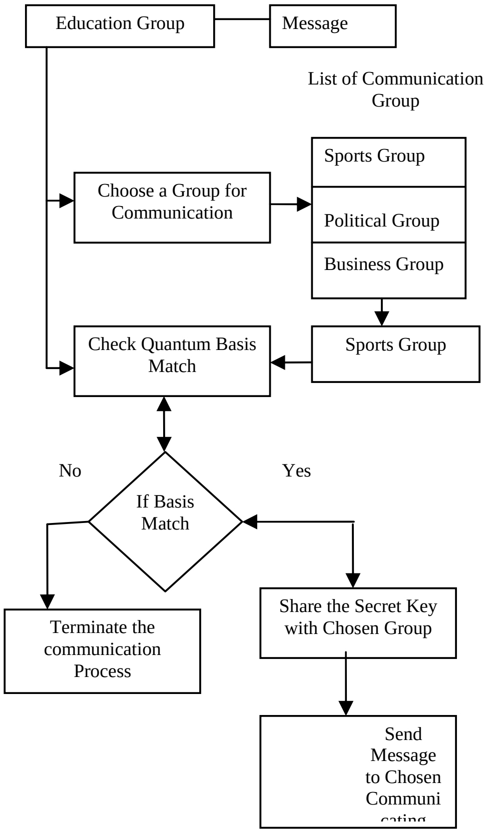

Education Group
Message
List of Communication Group
Sports Group
Political Group
Business Group
Choose a Group for Communication
Check Quantum Basis Match
Sports Group
No
Yes
If Basis Match
Terminate the communication Process
Share the Secret Key with Chosen Group
Send Message to Chosen Communi cating

**Fig 1.Functional flow diagram for secure group communication**

With the help of Qubits and Quantum basis which are the elements of Quantum cryptography is used to share a message among various group of people in the secure manner. The message can be received by the receiver is in the form of unidentifiable format. Through the BB84 protocol only the authorized peoples can retrieve the original information. The BB84 protocol is one of the Quantum Key Distribution protocol.

The core concept of this project is, to generate the Quantum Key which are at both the sender side and receiver side are same. Concept is covered by the Following steps

A. Group Formation
B. Simulation of BB84 protocol
  - Qubit Generation
  - Check bits Generation
  - Quantum Key Generation

C. Message Sharing

### A. Group Formation

The Communicating parties are getting together and then they form as a single group depending upon the category. Separate group is formed to share information through internet between group members. Then the SMTP protocol is implemented for transferring mail messages. The lists of groups are given below,

- Education group
- Political group
- Sports group
- Business group
- Entertainment group

### B.Simulation of BB84 protocol

#### Qubits Generation

Create a random string and convert it into binary bits. Then the Quantum basis is generated in the sender side. While comparing the Quantum basis and random binary string gives the Qubits for generate the Quantum key. Sender sends Qubits to receiver
as shown in fig 2.

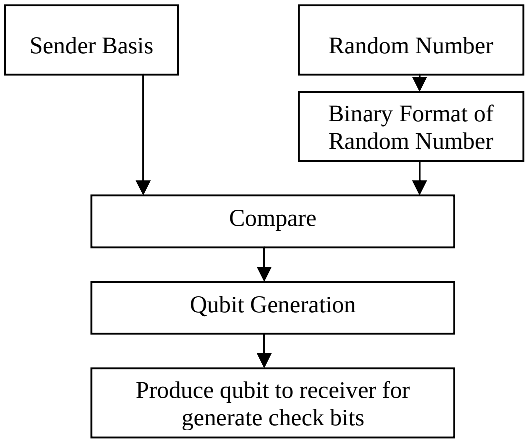

Sender Basis
Random Number
Binary Format of Random Number
Compare
Qubit Generation
Produce qubit to receiver for generate check bits

Fig: 2 Qubit Generation Flow Diagrams

Table 2.Quantum Key Generation

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Alice's random bit | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| Alice's random sending basis | + | + | × | + | × | × | × | — |
| Photon polarization Alice sends | ↑ | → | ↘ | ↑ | ↘ | ↗ | ↗ | → |
| Bob's random measuring basis | + | × | × | × | + | × | + | — |
| Photon polarization Bob measures | ↑ | ↗ | ↗ | ↘ | → | ↗ | ↑ | → |
| Shared secret key | 0 | | | | | 0 | | 1 |

**Check bits Generation**

Receiver collects the Qubits and then compares the Qubits with receiver basis representation. From this, receiver generates the check bits. Then receiver sends its basis to the sender. When sender collects the receiver's Quantum basis, he can generate the Quantum key based on finding Quantum basis match.

**Quantum Key Generation**

Sender got the receiver basis and then compare receiver's basis with his assumption Quantum basis which is involved in generate the Qubit.If both sender and receiver basis are matched from that sender generates the Quantum Key for secure communication as shown in table no.2.

**C.Message Sharing**

Message can be shared with the communicating groups. The message is converted into bits .The Quantum secret key is added with message and sends to the receiver. The receiver has already known about the secret key. So receiver can extract the secret key from Message. Finally the original information can be received by the receiver with the help of Secret key. The members from the outside of the communicating group can receive only the scrambled information as shown in fig 3.

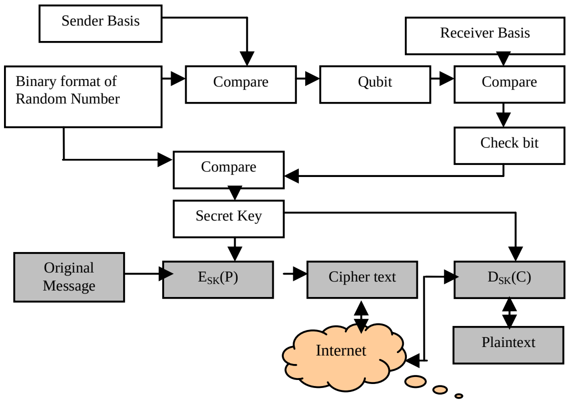


Fig 3 Secure group Communication based on BB84 protocol

### IV. Experimental Results

When the Proposed system is applied on the secure communicating environment, In the Sender side Quantum Keys are generated and added with cipher text then send to the receiver side in the secure manner. Receiver collects the information through internet with the help of mail. jar and activation. jar. Cipher text of information is retrieval with the help of Quantum key and information sharing through BB84 protocol is shown in

## V. Result Analysis

### i)Time Calculation for Quantum key Generation:

Table 3. Time Calculation for Quantum key Generation

| Quantum Basis | Time taken for Generate Quantum Key.<br>(Milliseconds) |
|---|---|
| 40 | 31 |
| 120 | 47 |
| 600 | 156 |
| 900 | 175 |
| 980 | 234 |
| 1020 | 287 |
| 1080 | 328 |
| 1140 | 375 |
| 1180 | 407 |

In Fig 4. the graph shows that, When the Quantity of Basis increases the time required to generate Quantum key is also increases, The time required to generate a Quantum key for basis of 40 and 120 are low, and 980 are high .For remaining number of basis of time to generate the corresponding Quantum key is normal.

ii) **Comparison of Quantum Cryptography Protocols**

If error rate is lower value, then Eavesdroppers participation rate in the Communication is reduced. When compare the proposed method with B92 protocol, the proposed method having the less error rate than B92 protocol. So the proposed method gets the fewer eavesdroppers disturbance. Quantum Cryptography protocols are having Quantum Bit Error Rate; it will affect the security of the information as shown in fig 6.

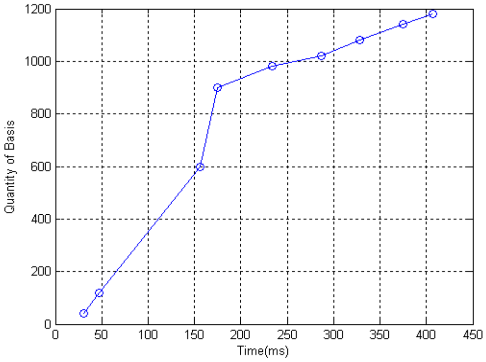


Fig 4. **G**raph for Time calculation of Quantum key Generation

$$\text{QBER}=\frac{N_{Wrong}}{N_{Total}}$$

$N_{Wrong}$ = Number of Quantum Error Bits are presented in the transmitted information

$N_{Total}$= Total Number of bits presented in the information

Table 4. Comparison of Quantum Cryptography Protocols

| B92 | | The proposed method using BB84 | |
|---|---|---|---|
| QBER | Simulation No | QBER | Simulation No |
| 340 | 1 | 283 | 1 |
| 328 | 2 | 253 | 2 |
| 284 | 3 | 257 | 3 |
| 327 | 4 | 250 | 4 |
| 357 | 5 | 260 | 5 |
| 310 | 6 | 247 | 6 |
| 328 | 7 | 278 | 7 |
| 334 | 8 | 287 | 8 |
| 311 | 9 | 237 | 9 |
| 314 | 10 | 210 | 10 |

In Fig 7. shows that, Kak's, SARG04 protocol are Quantum cryptography protocols. The proposed method using BB84 protocol is having lower QBER value than other Quantum cryptography protocols. So the proposed method is having minimum chance to loss the information when compare with other given QC (Quantum cryptography) protocols.

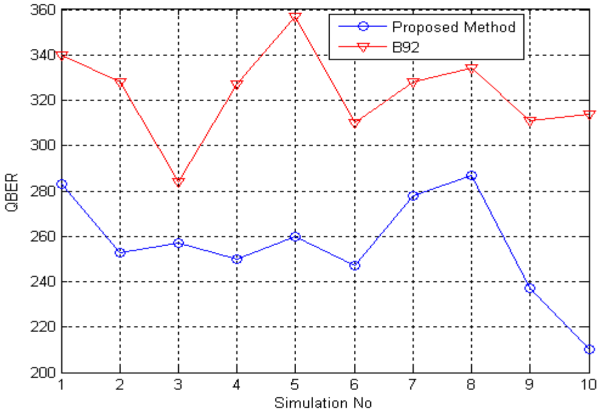


Fig 5. Comparison of Quantum Cryptography protocol's Error rate with proposed method using BB84protocol

Table 5. Comparison of Quantum Cryptography protocol's Error Rate with proposed method using BB84protocol

| Quantum Basis | Quantum Protocol's QBER value | | |
|---|---|---|---|
| | Kak's protocol | SARG04 | Proposed method using BB84 protocol |
| $0^0$ | 1.32 | 4.9 | 1.5 |
| $45^0$ | 2.54 | 3.5 | 1.8 |
| $90^0$ | 2.20 | 2.5 | 2.31 |
| $135^0$ | 4.75 | 2.9 | 2.35 |

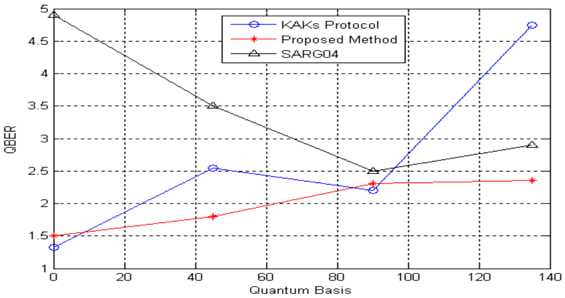
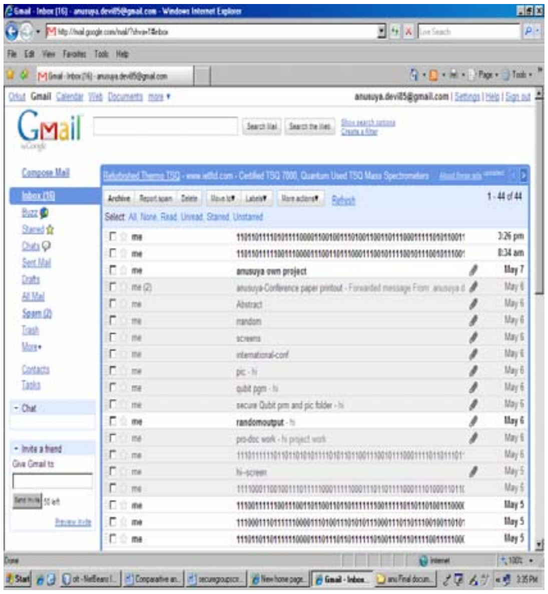


Fig 6. Comparison of Quantum Cryptography Protocol's QBER with Proposed method using BB84 protocol

## VI. Conclusion

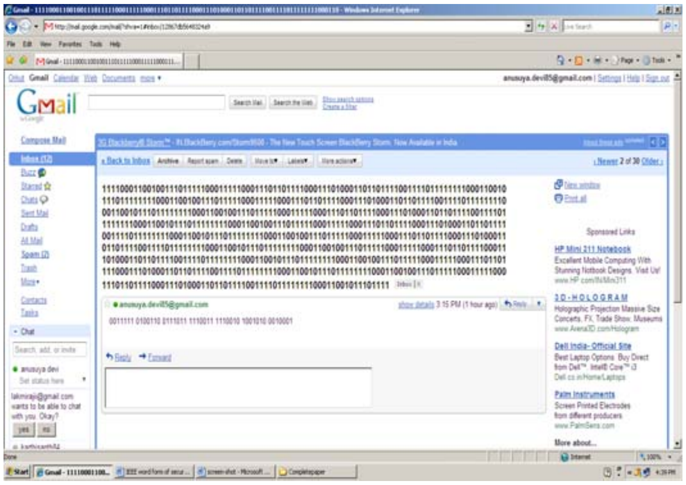
In this work is implemented based on the BB84 protocol. Groups are formed depending upon the category and then Qubits are generated for message sharing between two users in the secure way. By using the QKD protocol can be protected the information from the hackers through insecure channel.



Refurbished Thermo TSQ - www.ietltd.com - Certified TSQ 7000, Quantum Used TSQ Mass Spectrometers

| | | |
|---|---|---|
| me | [illegible] | 3:26 pm |
| me | [illegible] | 8:34 am |
| me | anusuya own project | May 7 |
| me (2) | anusuya-Conference paper printout - Forwarded message From: anusuya d | May 6 |
| me | Abstract | May 6 |
| me | random | May 6 |
| me | screens | May 6 |
| me | international-conf | May 6 |
| me | pic - hi | May 6 |
| me | qubit pgm - hi | May 6 |
| me | secure Qubit pm and pic folder - hi | May 6 |
| me | randomoutput - hi | May 6 |
| me | pro-doc work - hi project work | May 6 |
| me | [illegible] | May 6 |
| me | hi-screen | May 5 |
| me | [illegible] | May 5 |
| me | [illegible] | May 5 |
| me | [illegible] | May 5 |
| me | [illegible] | May 5 |

Fig 7. Cipher text is received in the Head Email id



```
11110001100100111011111000111110001110110111100011101000110110111100111011111111100011 0010
1110111111111000110010011101111100011111000111011011110001110100011011011110011101111111110
0011001011101111111110001100100111011111000111110001110110111100011101000110110111100111101
111111100011001011101111111100011001001110111110001111100011101101111000111010001101101111
00111101111111110001100101110111111111000110010011101111100011111000111011011110001110100011
011011110011101111111110001100101110111111110001100100111011111000111110001110110111100011
1010001101101111001110111111111000110010111011111111100011001001110111110001111100011101101
111000111010001101101111001110111111111000110010111011111111100011001001110111110001111000
1110110111100011101000110110111100111011111111100011001011101111
```

anusuya.devi85@gmail.com 3:15 PM (1 hour ago)

```
0011111 0100110 0111011 1110011 1110010 1001010 0010001
```

Fig 8. Cipher text Content and Quantum Key is Received in the mail Box

## References

[1] [1] Mehrdaa S.Sharbaf, “Quantum cryptography: A new Generation of Information Technology Security System,” IEEE Sixth International Conference on Information Technology, Vol: 3, pp: 1644-1648, 2009.

[2] [2]Justin Mullins, “Breaking Quantum cryptography in 150 kilometer,” IEEE Transaction on Spectrum, Vol: 45, Issue: 9, pp: 15-15, September 2008.

[3] [3] Cederlof J, Larson .A, “Security Aspects of the Authentication used in Quantum cryptography,” IEEE Transaction on Information Theory, Vol: 54, Issue: 4, pp: 1735-1741, April 2008.

[4] [4] Moni Naor,GilSegev,and Adam Smith,”Tight Bounds For Unconditional Authentication Protocols In The Manual Channel And Shared Key Models,”IEEE Transaction on Information technology,Vol:54,pp:2408-2425,june 2008.

[5] 5]Stamatics, V.Kartalpoulos, “Quantum cryptography For Secure Optical Networks, “IEEE Transaction on Communication, pp: 1311-1316, 2007..

[6] [6] Klye Martin,”Secure Communication Without Encryption?,”IEEE Transaction on Security &Privacy,Vol:15,pp:68-71,March 2007.

[7] [7] Tzonelin Hwang, Kuo-Chang Lee and Chuan-Ming Li, “Provably Secure Three- Party Authentication Quantum Key Distribution Protocols,” IEEE Transaction on Dependable and Secure Computing, Vol: 4, pp: 71-80, January-March 2007.

[8] [8] Vishnu Teja, Payel Banerjee, N.N Sharma, “Quantum cryptography: State of Art, Challenges, and Future Perspectives,” IEEE International Conference on Nanotechnology, pp: 1296-1302, August 2-5, 2007.

[9] [9] Rajni Goel Moses Garuba, Antech Gima, “Research Directions in Quantum cryptography,” IEEE International Conference on Information Technology, pp: 779-784, 2007.

[10] [10] Toyran, M Tubitak, Kocaeli, “Quantum Cryptography,” IEEE Publication on Signal Processing and Communications Applications, pp: 1 – 4, June 2007.

[11] [11] William C Barge, “User Authentication at Cyber spots,” IEEE Transaction on EIT, pp 574-576, 2007.

[12] [12]Valdislav S.Igumnov, Vadim N.Lis, “Influence of Quantum Computers on Classical cryptography,” International Siberian workshop and tutorials, Session IV, pp: 220-224, July1-5, 2007.

[13] [13]Thi Mai Trang Nguyen, Mohamed Ali, Sfaxi, and Solange Ghernaouti-Helie,”Integration of Quantum Cryptography in 802.11 Networks,”IEEE First Internation conference on Availability, Reliability and Security, pp: 2567-2574, 2006.

[14] [14] Xiao Tang,Lijun Ma,Alan Mink,Anastase Nakassis,Hai Xu,Barry Hershman,Joshua Bienfang,David Su,Ronald F.Bosivert,Charles Clark and Carl Williams,”Quantum Key distribution system operating at sifted –key rate over 4 Mbits/s,” Proceeding SPIE Quantum Information and Computation IV,Vol:6244,pp:66440P-1 to 66440P-8

[15] [15] Kartalopoulos, S.V, “ A Primer On Cryptography In Communications,” IEEE CommunicationsMagazine,Vol:44,Issue:4 , pp:146 – 151, April 2006.

[16] [16] Stamatias V.kartalopoulos, “Identifying Vulnerabilities of quantum cryptography in secure optical Data transport,”IEEE Transaction on Military Communication, pp:2788-2796, Oct 2005.

[17] [17] Miguel Navescues and Antonio Acin, “Security Bounds For Continuous Variables Quantum Key Distribution, “Physical Review Letter, Vol: 94, Issue: 2, 21 January 2005.

[18] [18] Nobert Lutkenhous, “Quantum Key Distribution How do we know its Secure? ,” IEEE Transaction on Optics and Photonics, March 2004.

[19] 19] Grau, B.C, “How to teach basic quantum mechanics to computer scientists and electrical engineers, IEEE Transactions on Education,”Vol: 47, Issue: 2 ,pp: 220 – 226, May 2004.

[20] [20] Elliott, C, “ Quantum cryptography,” IEEE Transactions on Security & Privacy, vol:2, Issue: 4, pp: 57 – 61, Jul-Aug 2004.

[21] [21] Ato K, Hirota. O, “Square-Root Measurement for Quantum Symmetric Mixed State Signals,” IEEE Transactions on Information Theory,” Vol: 49, Issue: 12, pp: 3312 – 3317, Dec. 2003.

[22] [22] Yablonovitch, E. Jiang, H.W. Kosaka, H. Robinson, H.D. Rao, D.S. Szkopek, T. , “Optoelectronic Quantum Telecommunications Based On Spins In Semiconductors,” IEEE Transactions on Information Theory, Vol: 91, Issue: 5 , pp: 761 – 780, May 2003.

[23] [23]Justin Mullins, “Making Unbreakable code,” IEEE Transaction on Spectrum, Vol: 39, Issue: 5, pp: 40-45, May 2002.

[24] [24] Bethune, D.S. Risk, W.P, “An Autocompensating Fiber-Optic Quantum Cryptography System Based On Polarization Splitting Of Light,” IEEE Journal of Quantum Electronics”, Vol: 36, Issue: 3, pp: 340 – 347, March 2000.

[25] [25]Townsend, “Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems,” IEEE Transactions on Photonics Technology Letters, vol: 10, Issue: 7, pp: 1048-1050, July1998.

[26] [26]Allen Michalski Duncan Buell,”A scalable Architecture for RSA cryptography on large FPGAS” Mathematics of computation, No: 44, pp 519-521, 1985.

[27] [27]Bennett, C.H., Brassard G.”Quantum cryptography: public key distribution and coin tossing,” IEEE Conference on Computer, Systems and signal Processing, pp:175-190, 1984.