A SURVEY ON QUANTUM KEY DISTRIBUTION PROTOCOLS

Jasleen Kour[1], Saboor Koul[2] and Prince Zahid[3]

[1]Assistant Professor, Department of CSE, BGSBU, Rajouri, J&K, India
[2,3]UG Scholars, Department of CSE, BGSBU, Rajouri, J&K, India

ABSTRACT

Quantum cryptography is based on quantum mechanics to guarantee secure communication. It allows two parties to produce a shared random bit string known only to them. These random bits can be used as a key to encrypt and decrypt messages. The most important and unique property of quantum cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. It is based on fundamental aspects of quantum mechanics. By using quantum entanglement or quantum super positions and transmitting information in quantum states, a communication system can be implemented which detects eavesdropping. Quantum cryptography is used to produce and distribute a key, not to transmit any message data. This key along with certain encryption algorithm, is used to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. This paper concentrates on comparison between classical and quantum cryptography as well as survey on various quantum key distribution protocols used to generate and distribute the key among communicating parties.

KEYWORDS

Quantum Cryptography, QKD, bits, photons and qubits.

1. INTRODUCTION

Data communication security can be defined as complex process that implies networks, users and applications, all of these connected by a set of modern technologies. So, Information systems are very vulnerable to attacks and illegitimate penetrations, to data incidental or intended data. Cryptography is a concept to protect the information transmission over such networks.

Cryptography is the science where the use of mathematics occurs to encrypt and decrypt data. It enables user to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be interpreted by anyone other than the intended receiver. To achieve such level of security different algorithms are used for secure transmissions which unite the message with additional information to produce a cryptogram. These algorithms are known as Cipher and the additional information is known as the key. This method is termed as encryption. Whereas cryptanalysis is the science of analyzing and breaking secure communication without knowing the encryption technique. Classical cryptanalysis involves an interesting combination of analytical reasoning, pattern finding, patience, determination, and luck. Quantum cryptographic devices generally make use of individual photons of light and take benefit of Heisenberg's Uncertainty Principle, according to this principle cryptographic protocols can invoke up streams of random bits whose values will remain unknown to third parties. When we use these bits as key material for Vernam ciphers, we can get Shannon's ideal of perfect secrecy—cheaply and easily. The development of quantum cryptography was inspired by some limitations of classical cryptography methods. In classical cryptography, communicating parties share a secret sequence of random numbers, the key, that is exchanged by some physical mean and thus open to security

loopholes. The classical cryptography does not detect eavesdropping like quantum cryptography, also with increase in computing power and new computational techniques are developed, the numerical keys will no longer be able to provide satisfactory levels of secure communications. These weaknesses led to the development of quantum cryptography, whose security basis is quantum mechanics. This paper presents the comparison of quantum and classical cryptography on several background, quantum cryptography key protocols and real world application of quantum cryptography.

2. CLASSICAL V/S QUANTUM CRYPTOGRAPHY

Both quantum cryptography and classical cryptography can be compared on following dimensions:

2.1. Fundamental Dimension

In theory, any classical private channel can be easily monitored inertly, without the knowledge to sender or receiver that the eavesdropping has been done. Classical physics is the theory of macroscopic bodies and phenomena such as radio signals that allows a physical property of an object to be measured without disturbing other properties. Cryptographic key like information is encoded in computable physical properties of some object or signal. Thus there is open possibility of passive eavesdropping in classical cryptography.

Quantum theory which is basis of quantum cryptography is believed to direct all objects, but its consequences are mainly noticeable in individual atoms or subatomic particles like microscopic systems. As far as classical cryptography is concerned there is frequent requirement of using longer keys as computational power doubles in every 18 months and cost of computation is reducing rapidly with time [moors law]. Thus an algorithm using k bit key which is secure may not be secure in future, i.e. it needs regular updating. On the other hand, security in quantum cryptography is based on the basic principles of quantum mechanics, so the possibilities of major changes requirements for future are almost negligible.

2.2. Commercial dimensions

Commercial solutions for QC that already exist; they are only suitable for point-to-point connections. On the other hand, crypto chip made by the Siemens and Graz technical university makes possible the creation of networks with many participants, and cost of €100,000 per unit, the system is very expensive and requires a lot of work. On other hand classical cryptography can be implemented in software and its cost for consumer is almost zero. Also, cryptographic system based on classical cryptography can be implemented on small hardware component like smart card , but this is major issue in case of quantum cryptography shrinkage to such a level require too much development.

2.3. Technological dimensions

Chinese scientists accomplished the world`s most long-distance of quantum communication transmission (teleportation), or as "instant matter transmission technology" technology. From the China University of Technology and researchers at Tsinghua University, Hefei National Laboratory in their free-space quantum communication experiments, and effectively enlarges the communication distance to 10 miles [9]. But classical cryptography can be used to communication distance of several million miles. According to the latest research, Toshiba achieve new record bit rate for quantum key distribution, that is, 1 Mbit/s on average [10]. On the other hand the bit rate of classical cryptography depends on the computational power largely.

2.4. Other dimensions

Communication medium is not an issue in classical cryptography because its security depends only on the computational complexity. Thus, this removes the need for excessively secure channels. On the other hand communication of quantum cryptography require a quantum channel like optical fiber or through air (wireless), also, there is constantly a likelihood of modification in polarization of photon due to Birefringence effect or rough paths that cause change in refractive index due to damage sometimes. Also, an n-bit classical register can store at any moment exactly one n-bit string. Whereas an n-qubit quantum register can store at any moment a superposition of all 2n n-bit strings.

Quantum cryptography is based on mixture of concepts from quantum physics and information theory. The security standard in QC is based on theorems in classical information theory and on the Heisenberg's uncertainty principle. Experiments have demonstrated that keys can be exchanged over distances of a few miles at low bit rate. Its combination with classical secret key cryptographic algorithms permits increasing the confidentiality of data transmissions to an extraordinary high level. From comparison, it's obvious that quantum cryptography (QC) is having more advantage than Classical Cryptography (CC) though some issues are yet to be solved. This is mainly due to the implementation problems but in future there exist possibilities that most of the problems in quantum cryptography will get resolved.

3. QUANTUM KEY DISTRIBUTION PROTOCOLS

Quantum key distribution is a key establishment protocol which generates symmetric key material by using quantum properties of light to transfer information from one Client to another Client in a manner which uses the results of quantum mechanics. By using the quantum properties of light, current lasers, fibre-optics and free space transmission technology can be used for QKD (Quantum key distribution), so that many observers claiming security can be based on the law of quantum physics only. Based upon the necessary principles of Quantum mechanics the QKD protocols are divided into two categories some are based on Heisenberg Uncertainty Principles and others are based on quantum entanglement.

3.1. Protocols based on Heisenberg Uncertainty Principle:

3.1.1. BB84 protocol

In 1984 Charles Bennet and Gilles Brassard for the first time proposed a protocol known as BB84 protocol which depends upon the Heisenberg Uncertainty principle.

Quantum key Distribution (QKD) is used in quantum cryptography for generating a secret key shared between two parties using a quantum channel and an authenticated classical channel. The private key obtained then used to encrypt message that are sent over an insecure channel (such as a conventional internet connection) as shown fig. below .A bit can be represented by polarising the photon in either of the two bases i.e. Rectilinear base(R) and Diagonal base (B).Binary 0 represents the polarisation of 0° degree in rectilinear base or 45° degree in diagonal base. Similarly binary 1 represents the polarisation of 90° degree in the rectilinear base or 135° degree in diagonal base. [1][5][15][16]

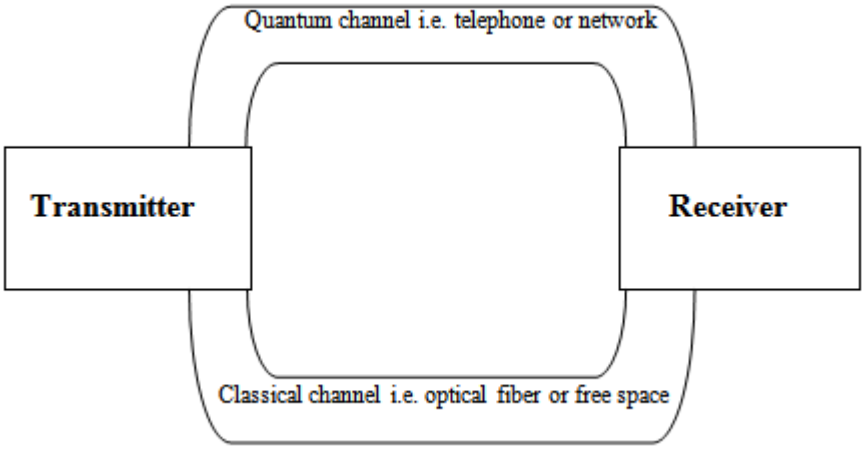

Figure 1A. Quantum cryptographic communication System for securely transferring Random key.

There are two steps involved in key distribution for BB84 protocol, as explained below:

a) One way communication channel (via quantum channel).

Step i) User A (Alice) randomly chosen polarized photon and send it to the user B (Bob) over Quantum channel.
Step ii) In this, user B receives photons using random basis either rectilinear or random.

b) Two way communication (via classical channel).

Step i) User A will use classical channel to inform user B about the polarisation A chose for every bit sent to B without disclosing the bit value.
Step ii) Now user will compare the polarisation sequence he receives from user A with the sequence he generated.
Step iii) Bits of same orientation of those two sequences can be used as secret key.

3.1.2. BBM92 protocol

It is the modified version of BB84 protocol which uses only two states instead of four states which were used in BB84 protocol. Charles Bennett, Brassard and Mermin devised another, the so-called BBM92 protocol. They realized that it was not necessary to use two orthogonal bases for encoding and decoding. It turns out that a single non-orthogonal basis can be used instead, without affecting the security of the protocol against eavesdropping. This idea is used in the BB92 protocol, which is otherwise identical to BB84 protocol.

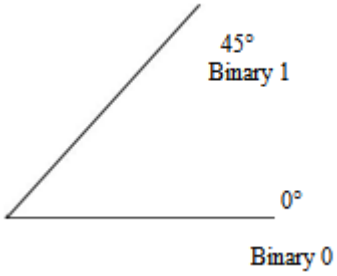

Fig 1B: BB92 protocol state encoding

As shown in fig 1B. BB92 above, 0 represents 0°degree in the rectilinear basis and 1 represents 45°degree in the diagonal basis. Client A transmits string of photons to client B which were encrypted by randomly chosen bits just like in BB84 protocol. But here client A chooses the bits by an authoritative rule to which base client B must use. But still Client B chooses randomly a basis by which to measure but if Client B chooses wrong base he will not measure anything; a condition in quantum mechanics which is known as an erasure. After every step Client B tells Client A that the bits end by client A whether or not he measured it correctly.[2][3][7]

3.1.3. SARG04 protocol

SARG04 protocol was proposed by Scarani et.al in 2004. In this protocol the four states of BB84 protocol is used with different information such a new protocol is developed which is capable of performing without failure under a wide range of conditions when attenuated laser pulses instead of single photon source.

Its first phase is similar to BB84 protocol. In the second Phase Client A instead of directly announcing her base to Client B, it announces a pair of non-orthogonal states one of which client A uses it to encode its bit. Client B measures the correct state if it has used the correct base. Client B will not be able to determine the bit or will not measure the correct states of client A if he chooses the wrong base. The length the key will remain ¼ of the raw key after shifting stage if there are no errors.

The SARG04 protocol has almost same security to BB84 in perfect single-photon implementations, If the quantum channel is of a given visibility (i.e. with losses) then the QBER of SARG04 is twice that of BB84 protocol, and is more sensitive to losses.SARG04 is more secure than BB84 protocol in presence of PNS attacks.[1][4][5][14]

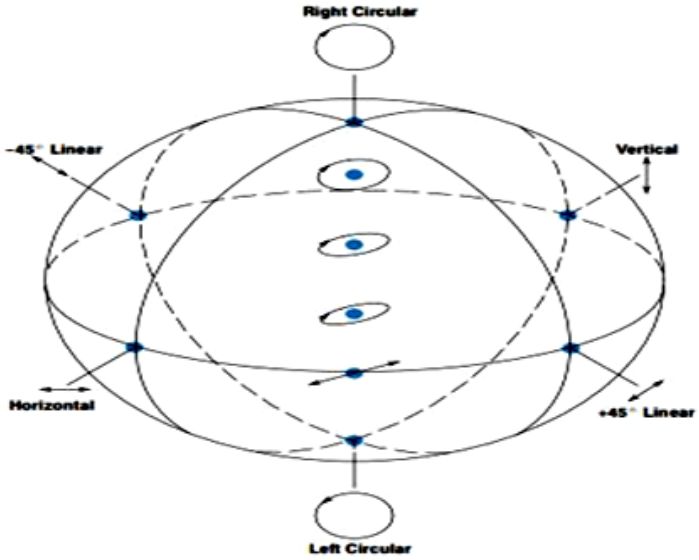

Fig 2A: Poincare sphere

3.2. Protocols based on Quantum Entanglement.

3.2.1 E91 protocol

Ekert, in 1992, performed the process of key distribution through entanglement of photons in a quantum channel. He proposed a method of harnessing Bell`s inequalities. In this method any of the three, A (Alice), B (Bob), or the third party could produce entangled photons. Separation in each pair is such that the communicants, A and B could receive one of each pair. Quantum

entanglement means to define the quantum states of one object without referencing the quantum states of another object far away from it. The fact that entangled states are used conceals the information about the key from the eavesdroppers, hence more secure method. The states of particle are not collapsed until the moment of measurement, so trying to access the system is as looking for something that doesn`t exist yet.

Both A and B choose randomly and independently from two different orientations of their analysers to measure the polarization of photons. A typically physical set-up is shown in fig3A: given below, using active polarization rotators (PR), polarizing beam splitter (PBS) and avalanche photodiodes (APD). [8][11][13]

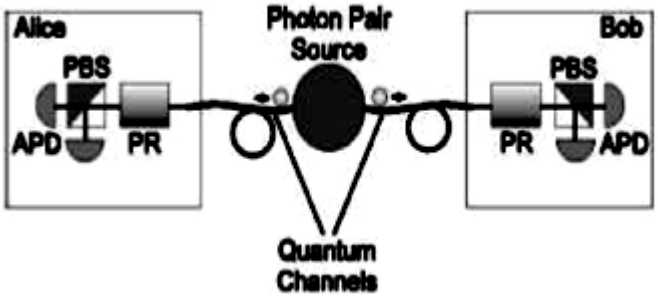

Fig 3A: Typical System Using Entangled Photon Pairs

3.2.2. COW protocol

A new protocol, given by Nicolas Gisin et al in 2004, was proposed for QKD based on the weak coherent pulses at high bit rates. The protocol was termed as Coherent One-Way protocol l(COW protocol). The main feature of the method was the setup being experimentally simple and resistant to interference visibility and to photon numbers splitting attacks, hence more efficient in terms of distilled secret bits per qubit.

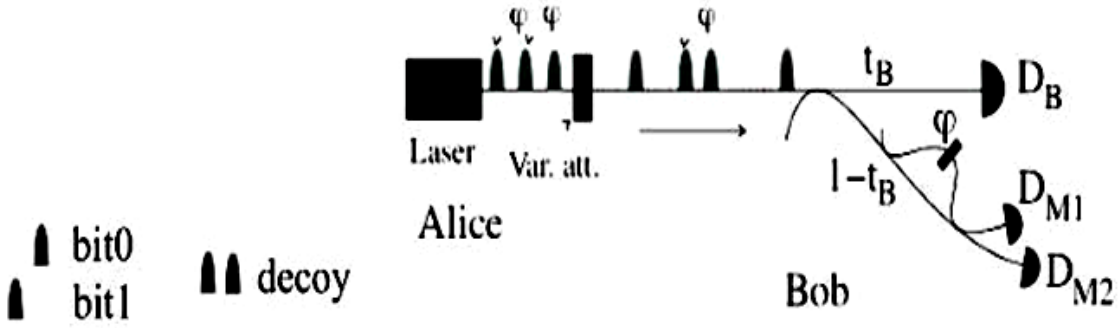

Fig4A: Scheme of the COW protocol.

The figure 4A above represents the COW protocol. The message is encoded in time. Alice sends Coherent pulses that are either empty or have a mean photon number $\mu < 1$. Each logical bit of information is encoded by sequences of two pulses, μ-0 for a logical ―0‖ or 0-μ for a logical ―1‖.

Alice sends decoy sequences μ-μ for security needs. Bob measures the arrival time of the photon on his data-line, detector DB to obtain its key. Bob randomly measure the coherence between successive non-empty pulses, bit sequence ―1 -0‖ or decoy sequence, with interferometer and detectors DM1 and DM2. If wavelength of the laser and the phase in the interferometer are well aligned, we have all detection on DM1 and no detection on DM2. A loss of coherence and

therefore a reduction of the visibility reveal the presence of an eavesdropper, in which case the key is simply discarded, hence no information will be lost.[1][11][12][7]

3.2.3. DPS protocol

Differential –phase-shift QKD (DPS-QKD) is a new quantum key distribution scheme that was proposed by K. Inoue et al. Figure 5A mentioned below shows the setup of the DPS-QKD scheme.

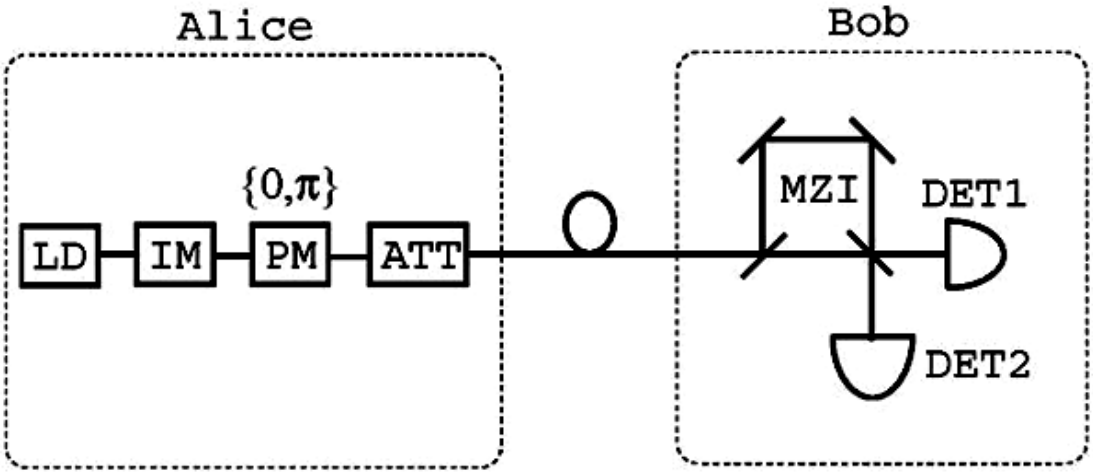

Fig 5A: Schematic diagram of DPS protocol

From the Alice site, a pulse train of weak coherent states is phase-modulated randomly by $\{0, \pi\}$ for every pulse and then to Bob with an average photon number less than one per pulse. From the Bob`s site, the phase difference is measured between the two sequential pulses using one bit delay. Mach-Zender interferometer and photon detectors record the photon arrival time and which detector clicked. Bob, after transmission of the optical pulse train, tells Alice the time at which photon was counted. Alice comes to know from this time information and her modulation data about the detector clicked at Bob`s site. Under an agreement that a click by detector 1 denotes ―0‖ and click by detector 2 denotes ―1‖, for example Alice and Bob obtain an identical bit string.

The DPS-QKD scheme has certain advantageous features including a simple configuration, efficient time domain use, and robustness against photon number splitting attack. [9][10][11]

4. APPLICATIONS OF QUANTUM CRYPTOGRAPHY

The study of quantum cryptography is heavily application-oriented. Therefore, a fundamental question is: Who really needs it rather than classical cryptography? The most significant advantage of quantum cryptography is the forward security. That is, if a classified message is appropriately encrypted with quantum cryptography, its distribution will stay secure as long as quantum mechanics is valid. In contrast, a classified message that is encrypted with classical cryptographic algorithm may stay safe only for a certain period of time. The length of this "secure period" is predictable only if the increase of computational power is predictable. Quantum cryptography can be a favored choice for applications that require long-term information security. There can be a long list of potential (or maybe present) clients. Here we raise a few examples.

4.1. Government agencies.

This includes intelligence, diplomatic, and military agencies. Often under the name of national interest, some information (like some pictures taken in Guantanamo Bay detention camp) is expected to be kept confidential for decades, during which such confidential information may be extensively distributed among different government agencies. Note that the Canadian census data are kept secret for 92 years. Therefore, if we conducted a census in 2009, the data would not be released until 2101, which is the next century! Quantum cryptography can help keep these sensitive data secure during transmission.

4.2. Financial institutes.

Financial information is very sensitive and needs long-time confidentiality. Quantum encrypted links between financial institutes can substantially reduce the risk of leaking the clients' information during communication.

4.3. Health care providers.

Health care records are being digitized gradually. Digital records of patients are often distributed between different health care providers facilitate medical treatments. The distribution of a patient's health record may have to be kept secure for the life span of the patient, and quantum cryptography can certainly be of help. Note that quantum cryptography is not the only method to guarantee unconditional communication security. It is not even the only solution to the key distribution problem.

5. CONCLUSION & FUTURE WORK

The techniques adapted from classical computer science are applicable to quantum key distribution protocols is an appropriate sign that quantum cryptography is a rousing new area of research work. In this paper we endeavored to introduce quantum cryptography, QKD protocols and QC applications. It explains about different quantum key distribution protocols. These protocols can be used along with encryption technique to achieve higher level of security. There is much more to describe about quantum cryptography

REFERENCES

[1] Abhishek Parakh, (2015), "New Protocol for Quantum Public Key Cryptography", IEEE ANTS 2015 1570203267 .

[2] Otilia Cangea, Carmen Silvia Oprina, Mihai-Octavian Dima, (2016), "Implementing Quantum Cryptography Algorithms for Data Security" ,ECAI 2016 - International Conference – 8th Edition Electronics, Computers and Artificial Intelligence 30 June -02 July, 2016, Ploiesti, ROMÂNIA.

[3] V. Padamvathi, B. Vishnu Vardhan, A.V.N. Krishna,(2016), "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey", Advanced Computing (IACC), 2016 IEEE 6th International Conference.

[4] H. Bennett, (May 1992),"Quantum cryptography using any two no orthogonal states",‖ Phys. Rev. Lett., vol. 68, no. 21, pp. 3121–3124,.

[5] Tamaki, K., M. Koashi, and N. Imoto, (2003), "Unconditionally secure key distribution based on two non orthogonal states",‖ Physical Review Letters 90, 167904 [preprint quant-ph/0210162].

[6] M. Christandl, R. Renner, and A. Ekert, (Mar. 2004), "A generic security proof for quantum key distribution",‖ arXiv:quant-ph/0402131.

[7] M. A. Nielsen and I. L. Chuang, (2000), "Quantum Computation and Quantum Information", Cambridge, UK: Cambridge University Press.

[8] Eduin H. Serna, (2009), "Quantum Key Distribution Protocol with Private-Public Key"‖, Quantum Physics (quant-ph), http://arxiv.org/PS_cache/arxiv/pdf/0908/0908.2146v3.pdf.

[9] E. Biham, T. Mor, (1997), "Security of quantum cryptography against collective attacks", Physical Review Letters 78 (11) 2256–2259.

[10] Ekert, Artur K.,(August 1991), "Quantum cryptography based on Bell's theorem, Physical Review Letters", Vol. 67, No. 6, 5, pp 661 - 663.

[11] Inoue K, Woks E and Yamamoto Y, (2002), "Differential phase shift quantum key distribution", Phys. Rev. Lett. 89037902.

[12] M. Lucamarini, S. Mancini, (2005), "Secure deterministic communication without entanglement, Physics Review Letters", 94140501.

[13] M. Elboukhari, M. Azizi, A. Azizi, (2009), "Implementation of secure key distribution based on quantum cryptography‖", in Proc. IEEE Int. Conf Multimedia Computing and Systems (ICMCS'09), pp 361 – 365.

[14] M. Elboukhari, Mostafa Azizi, and Abdelmalek Azizi, (2009), "Integration of Quantum Key Distribution in the TLS Protocol‖", IJCSNS, Vol. 9 No. 12 , pp.21-28,. http://paper.ijcsns.org/07_book/200912/20091204.pdf.

[15] N. Lutkenhaus, (1996), "Security against eavesdropping in quantum cryptography, Physical Review", A 54 (1) 97–111.

[16] P. W. Shor and J. Preskill,(July 2000), "Simple proof of security of the BB84 quantum key distribution protocol", Phys. Rev. Lett, vol. 85, no. 2, pp. 441– 444.

[17] R.Hughes,J.Nordholt,D.Derkacs,C.Peterson, (2002), "Practical free-space quantum key distribution over 10km in daylight and at night", New journal of physics 4 (2002)43.1-43.14.URL: http://www.iop.org/EJ/abstract/1367-2630/4/1/343.

[18] C. H. Bennett and G. Brassard, (1984), "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Intl. Conf. on Computers, Systems, and Signal Processing, pp. 175–179.

[19] U. Vazirani and T. Vidick, (Sep 2014), "Fully device-independent quantum key distribution.", Phys. Rev. Lett., 113:140501,.

[20] S.-A. Wang and C.-Y. Lu.(Aug 2013), "Quantum secure direct communication network In Nanotechnology (IEEE-NANO)", 13th IEEE Conference, pp 752–755.

[21] Verma Deepankar, Kour Jasleen, (June 2014), "Image Steganography Based on Hybrid Cryptography Algorithm Designed by making use of Blowfish, AES, RSA Algorithm", IJARCSSE, Vol. 4, Issue 6.