Quantum Key Distribution – Technology Review

Anindita Banerjee[1,2]
Department of Physics and Center for Astroparticle Physics and Space Science,
[1]Bose Institute, Block EN, Sector V, Kolkata 700091, India
E-Mail : anindita@qunulabs.in

Anil Prabhakar[3]
Department of Electrical Engineering,
[3]IIT Madras, Chennai 600036, India
E-Mail : anilpr@iitm.ac.in

And

Mark R Mathias[2]
[2]QuNu Labs Pvt. Ltd. 201/202, Prestige Meridian, M.G. Road,
Bangalore – 01, India
E-Mail : mark@qunulabs.in

Abstract - *In this paper we discuss various aspects of Quantum Key Distribution (QKD) technology and system implementations which can theoretically provide unconditional security for communication networks. This technology is believed to be able to provide security levels which are required to withstand the threats realizable by future computing technologies, including Quantum Computers.*

Keywords: *quantum cryptography, quantum key distribution, public key cryptography, secure key rate, key distillation, security attacks.*

1. INTRODUCTION

1.1 With the spread of more unsecure computer networks in the last few decades, a genuine need was felt to use cryptography in a larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems which are widely used today. Public key cryptography is vulnerable to progress in computing power due to improvements in technology and progress in mathematics. While these systems may be secure today, future computing technologies, including Quantum Computing, are likely to render these systems insecure. This paper investigates systems based on Quantum Key Distribution (QKD) technology which has been theoretically proven to be unconditionally secure and will provide a much higher level of security that can withstand threats which can be realized by future computing technologies.

2. QUANTUM KEY DISTRIBUTION

2.1 Quantum key distribution exploits the fundamental principles of quantum physics. The unconditional security relies on the fact that observation causes perturbation. The power of quantum cryptography (quantum key distribution) is independent of mathematical and computing power of adversary. In Quantum Key Distribution (QKD) two legitimate parties say Alice (sender) and Bob (receiver) can share a secure private key under the nose of eavesdropper. The information can be encoded in the properties of light by its polarization or interferometric methods, and transmitted as quantum information bits or qubits via a quantum channel (optical fibre or wireless). If these qubits are eavesdropped then its state will change. An prior shared authenticated classical channel performs the post processing and key distillation to finally generate the secret key.

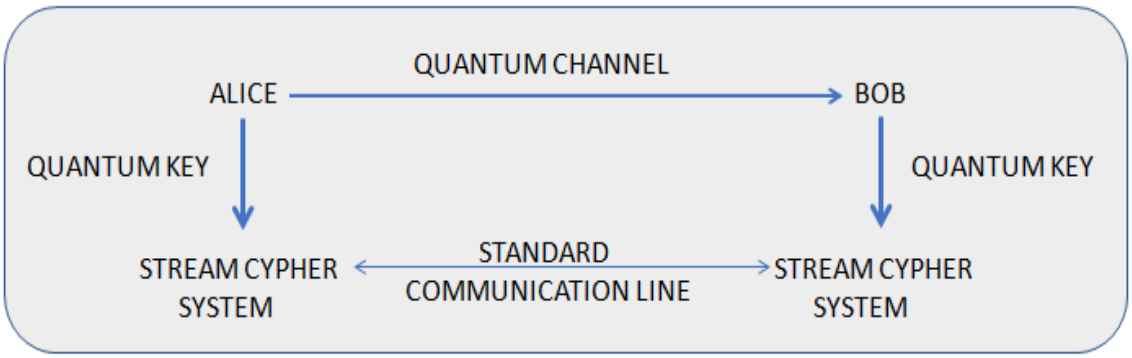

Figure 1: QKD system architecture

3. QKD BACKGROUND

3.1 In 1970 Stephan Wiesner wrote a seminal paper "Conjugate Coding" [1] which introduced the concept of quantum cryptography. In 1984, Bennett and Brassard introduced BB84 [2]. Their work highlighted quantum features like uncertainty, impossibility in discriminating nonorthogonal states and disturbance in measurement etc that can provide unconditional security which is impossible in the classical world. In *1991*, Ekert's protocol E91 [3] introduced another QKD scheme using maximally entangled states, where security was hidden in quantum nonlocality. Further in *1992*, Bennett showed that two non-orthogonal states are sufficient for quantum cryptography [4]. The Goldenberg-Vaidman (GV) protocol [5] implements QKD using orthogonal states. In *1999*, Guo and Shi [6] proposed a protocol based on interaction free measurement which was followed by Noh protocol and this was experimental realized Brida et al. [7]. In *2007*, Antonio Acin et. al [8] analyzed QKD protocol under device

independence. In *2007*, first semi-quantum QKD protocol was proposed by Boyer et. al., [9] in this the possibility of QKD with any one of user being classical was explored. Experimental realization of counterfactual quantum cryptography by demonstrated by Avella et. al [10] in 2010. In *2012*, Hoi-Kwong Lo [11] proposed a measurement-device-independent QKD protocol and in *2014* it was experimentally realized [12] over a distance of 200 km.

4. QKD PROTOCOLS

4.1 In this section, some of the commonly used protocols are summarized. In 1984, Bennett and Brassard [2] published the first QKD based on polarization encoding. Alice and Bob are two legitimate users with a prior shared quantum channel and authenticated classical channel respectively. Alice sends a sequence of randomly polarized photons in different polarization states (from two conjugate bases) to Bob over a quantum channel. Bob randomly selects a basis and measures the state. He keeps a note of the resultant state and the basis selected for measurement. Alice and Bob broadcast their measurement bases and thereafter discard the results for which mismatched bases were used and thereby generate a sifted key. They compute the quantum bit error rate verify the presence of an eavesdropper. They then generate a secure key after classical post-processing steps which include error correction and privacy amplification.

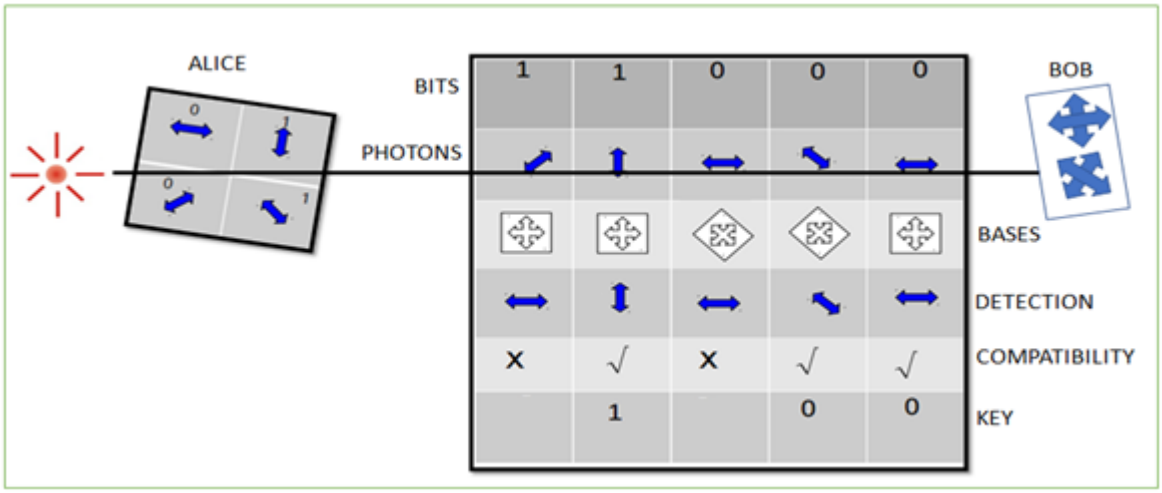

Figure 2: BB84 protocol

4.2 The Ekert scheme (E91) [3] uses entangled pairs of photons. These can be created by either legitimate users (Alice and Bob) or separate source. The photons are distributed so that Alice and Bob possess one photon from each pair. The scheme relies on the fact that the entangled states are perfectly correlated and any attempt at

eavesdropping will destroy these correlations in a way that Alice and Bob can detect the presence of Eve.

4.3 Bennet proposed another protocol called B92 [4] which utilizes only two nonorthogonal states. The protocol has been proven to be unconditionally secure. Like the BB84, Alice transmits to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses dictates which bases she must use. Bob still randomly chooses a basis by which to measure but if he chooses the wrong basis, he will not measure anything; a condition in quantum mechanics which is known as an erasure. Bob can simply tell Alice after each bit she sends whether or not he measured it correctly.

4.4 Coherent One-Way protocol (COW protocol) [13] is a new protocol for Quantum cryptography proposed by N. Gisin et al with time encoding. The experimental set up is simple and it is tolerant to reduced interference visibility and to PNS attacks. It generates a higher secret bit rate.

4.5 Differential Phase Shift QKD (DPS-QKD) [14] is a new quantum key distribution scheme that was proposed by K. Inoue et al. Alice randomly phase-modulates a pulse train of weak coherent states by {0,π} for each pulse and sends it to Bob. Bob measures the phase difference between two sequential pulses using MZ-Interferometer and single photon detectors. He records the photon arrival time and the detector which had clicked. Bob notifies Alice about the time instances at which detector clicked. In the end, Alice and Bob obtain an identical bit string. The DPS-QKD scheme is easy to implement in optical fibre due to its simple configuration and it is robust against PNS attack.

4.6 The SARG04 protocol [15] is somewhat similar to BB84. During reconciliation, Alice does not directly announce her bases as in BB84 rather, she tells Bob about the pair of non-orthogonal state used by her. Bob will get correct state if he implemented the correct basis.

4.7 MDI-QKD [11] protocol is immune to detector imperfections, and is secure even if the detectors are in eavesdropper's possession. The security relies on the violation of a Bell inequality and can be proven without knowing the implementation details. Quantum steering experiments aim to demonstrate that two parties can share verifiable entanglement even if one measurement device is untrusted.

5. QUANTUM KEY DISTRIBUTION PROCEDURE

5.1 Quantum key distribution consists of three steps:

5.1.1 Key Exchange: The photons which are sent by Alice to Bob via quantum channel constitutes the raw key.

5.1.2 Key Sifting: The raw key then undergoes the sifting process in which photons with same bases (criteria will differ for different QKD schemes) are selected and rest of them are discarded thus, resulting in a sifted key.

5.1.3 Key distillation: The sifted key will be abundant in errors which are generated either by an eavesdropper or due to imperfections in the QKD device and transmission line. Key distillation comprises mainly of error correction and privacy amplification.

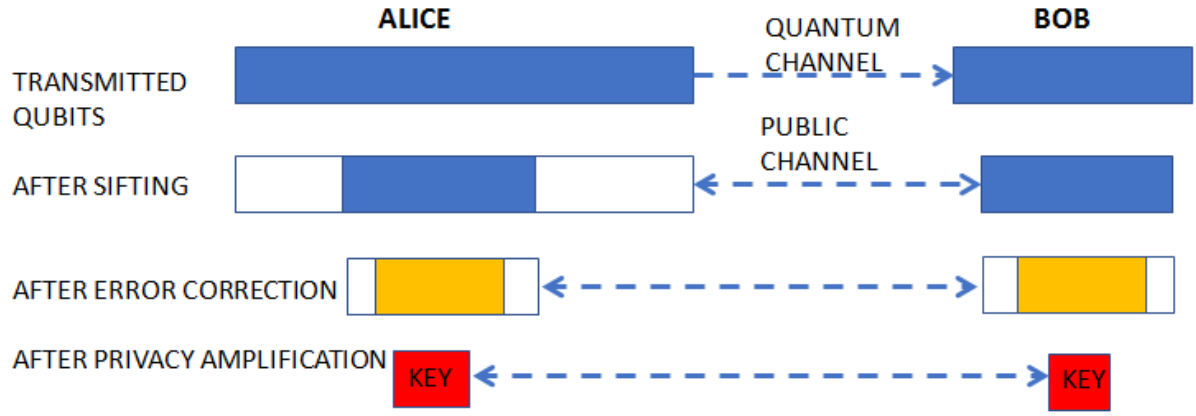

Figure 3. Impact of key distillation on key length

5.2 Error correction or Reconciliation is a process where Alice and Bob with given sifted key arrive to a common sequence. The cascade protocol is most common for error correction but it is highly interactive, the sifted key is divided into blocks, thereafter parity is calculated and compared. If the result does not match then the error is identified and corrected by binary search method, this process continues and at the end Alice and Bob have identical raw keys. However, the process is time consuming and will limit the key generation rate. At present Low-Density Parity-Check codes are used which improvises the efficiency of the process.

5.3 The process of error correction is accompanied by the leakage of information due to continuous interaction hence further security is provided by privacy amplification. The reconciled key is further processed to final key by compressing the key to an

appropriate factor. This process decreases the mutual information between Alice and Eavesdropper and enhances the security of the key.

6. SECURITY OF QKD

6.1 QKD is basically a mathematical procedure. Unconditional security implies information theoretic security and it lies in following results of quantum physics [16]:

6.1.1 Nocloning theorem intuitively follows from the Heisenberg's Uncertainty Principle which states that if Alice sends a qubit to Bob prepared randomly from a set of states which are not mutually orthogonal, then Eve cannot copy the state of the qubit and thus she has to measure it in order to find the state of the qubit.

6.1.2 Nonrealism: The wave function collapse is manifestation of nonrealisitic (nondeterministic) nature of quantum mechanics. Thus one cannot perform a measurement without perturbing the system. When Eve measures a qubit the wave function (superposition state) collapses to one of the possible states and the system is perturbed.

6.1.3 Non commutivity; The theorem states that two nonorthogonal states cannot be discriminated with certainty and this forms the basis of BB84, B92, LM05 and all other conjugate coding based protocols.

7. PRACTICAL CHALLENGES:

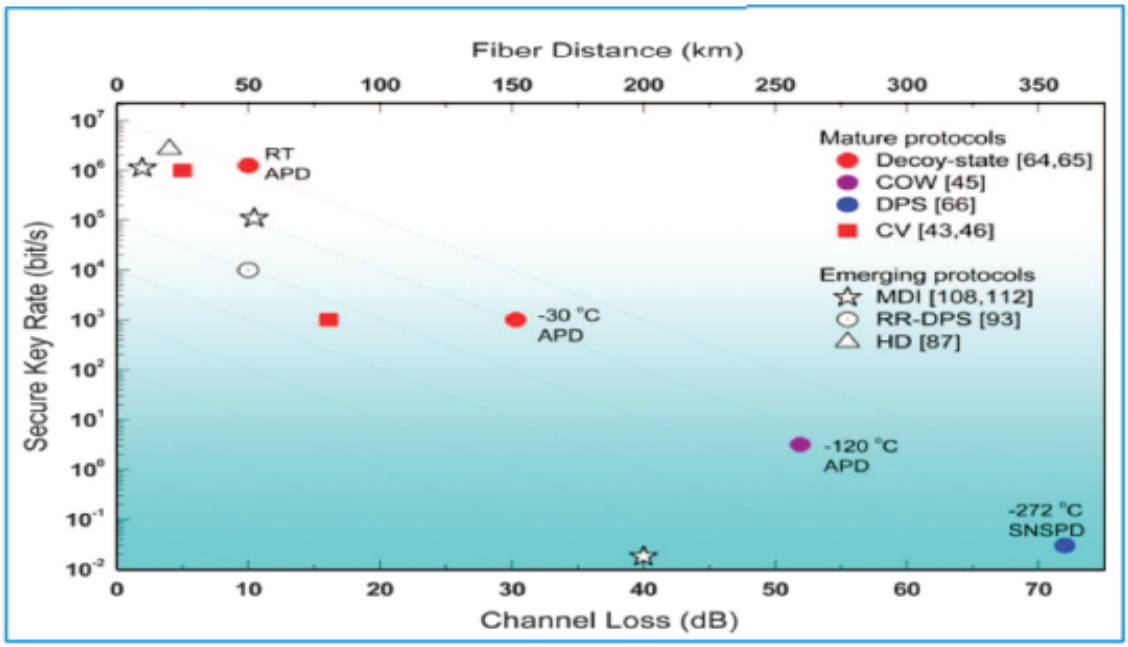

Figure 4: Secret key generation rates in recent QKD schemes. (Source: npj Quantum Information vol. 2, pp.16025, 2016)

7.1 A critical performance criteria of a QKD system is the key generation rate for increased transmission distances with no compromise on the security aspects. This performance parameter is dependent on several factors including the robustness of the implementation, the protocol and quantum efficient of photon detectors.

7.2 The key generation rate is also affected by the optical loss in the fibre and the transmission distance. Several emerging protocols have been recently proposed to make the QKD system resilient to any form of eavesdropping. Measurement device independent QKD (MDI-QKD), Round Robin DPS-QKD and loss-tolerant QKD are being realized.

8. GENERAL QUANTUM ATTACKS

8.1 QKD is proven to be unconditionally secure but its implementation is vulnerable to several attacks. The required measures are adopted accordingly for example, inserting decoy photons etc and, modified protocols are introduced to counter these attacks. However, we have to keep in mind that we have considered the eavesdropper with power which can be limited by nature and not by technology. The quantum attacks listed below are generic and it applies to different types of QKD depending on the nature of the protocol and the implementation technology.

8.1.1 Beam splitting attack: Eve can replace the quantum channel with a loss-less one and place a beam splitter in its path. She will store the photons in her quantum memory and measure them after Bob's announcement.

8.1.2 Entanglement and measure attack: Eve can entangle her qubit with the photon and will extract the information by performing the measurement on her qubit.

8.1.3 Intercept resend (IR) attack: Eve intercepts the photon, measures it and then prepares the photon with same encoding and sends it to Bob. This results in 25% of BER in BB84.

8.1.4 Photon Number Splitting: If Alice does not have a true single photon source then there is non negligible probability that she sends two photons in a pulse. Eve will then

take out one of the photons and keep it with herself in her quantum memory till Alice reveals her encoding.

8.1.5 Timing attack: If the light source and detectors are not synchronized then Eve can obtain the information about the detector which had clicked by hearing the time signature announced by Bob.

8.1.6 Trojan attack: Eve shines bright light at Alice/Bob and by analyzing its reflection she can obtain the information about the base. This particular attack has been successful against QPN-5505 (MagiQ Technologies) and Clavis 2 (IDQuantique).

8.1.7 Denial of service: Eve can disrupt the photons in the channel by either applying some unitary or simply blocking the line. She does not gain any information in the process by hampers the key distribution between legitimate parties.

8.1.8 Man-in-the-middle attack: Eve impersonates as Bob and directly communicates with Alice and hence authentication of legitimate parties is essential to avoid such attacks.

8.2 The security level of a protocol is decided by its security against the different type of attacks. It is a critical issue both from the information theoretic perspective and a major challenge for implementation. Several QKD protocols have been experimentally analysed to provide security against collective attacks with practical set ups. Decoy state BB84 enables security against most general attacks. Continuous variable (CV)-QKD and Coherent one way (COW)-QKD provides security against collective attacks [17] however it does not provide an efficient key rate.

9.

9.1 QKD IMPLEMENTATION

Quantum Key Distribution (QKD) rapidly progressed from the early experimental demonstrations to field trials. Several commercial products are available in market

making QKD deployment feasible. At present, QKD is performed over 100km in standard telecom fibres as well as in free space and secure key rate has now reached few Mbps.

Figure 5: Current and upcoming deployments of QKD

9.2 COMMERCIAL PRODUCTS

There is substantial on-going research and technology development at educational institutions, research establishments and corporate around the globe. Some of the companies who offer QKD solutions are listed below:

9.2.1 In 2001, ID Quantique, [18] a private company is presently the global leader in QKD market, it has deployed several QKD networks in recent years. In 2007 their Cerberus QKD system was used in vote counting in Geneva, Switzerland. In 2009 they started Swiss quantum project to test the long-term reliability of their QKD system which was also deployed for the Soccer World Cup held in South Africa in 2010. QKD-as-a-Service was launched in 2011 and uses the Cerberus system to secure communications in a metropolitan area network (MAN) with connection distances up to 30 km. It is expert in high speed encryption and has a broad portofolio of solutions in layer 2 encryption. Its QKD box is called Clavis and it can perform key exchange upto 100km. Cerberis is a server with automatic creation and key exchange over a fibre(FC-1G, FC-2G and FC-4G) and can transmit key upto 50km and carry out 12 parallel calculations. IDQ uses AES for encryption and BB84 and SARG04 for QKD.

9.2.2 MagiQ Techonologies [19] in *USA* introduced QPN-8505 Security Gateway, using single photon and implementing BB84, 3DES and AES. It proposes VPN security using QKD (upto 100 of 256 bit keys per second, upto 140 km). It multiplexes QKD with classical communication channels on the same fibre line. It provides always ON industry standard , IPSec site-to-site VPN connection. They also provide Q-Box Work bench QKD system forr research purpose in academics, commercial and government sectors.

9.2.3 SeQureNet [20] is a start-up company in *Paris* and it implements the CV-QKD. Its QKD system communicates at 100 bit/sec at 80 km and 10 kbit/sec at 20 km.

9.2.4 Quintessence Labs [21], in *Australia* utilize continuously variable QKD system that increases the data rate of first-generation single photon systems.

9.2.5 Toshiba Research Europe Ltd [22] in *Great Britain* presented Quantum Key Server, it allows key distribution across 50km in length and 1Mbps key generation rate and telecom fibre links exceeding 100 km. It has also developed multi user quantum network.

9.2.6 *China* Quantum Technologies (QTEC) [23] is a quantum information company based at Hangzhou. It is looking into quantum government affairs, quantum finance, quantum energy, and quantum commerce. QTEC is very active in establishing quantum communications networks around the country, including the Shanghai-Hangzhou trunk network. It has recently collaborated with IDQ which will eventually reduce the cost of QKD products worldwide.

9.2.7 QuNu Labs [24] is the first *Indian* company to establish real time secret key generation up to a distance of 40 km with kbps key generation rates. The implementation is based on standard telecommunication fibre and single photon source simulated by an attenuated weak coherent source. Subsequent product releases will be based on a single photon source.

9.3 QKD NETWORK PROJECTS

In addition to Point-to-Point QKD implementations, QKD networks are also being developed. Some efforts in this direction are mentioned below.

9.3.1 Townsend et al. [25] presented and realized the first QKD network.

9.3.2 European quantum cryptography and single photon technologies (EQCSPOT) [26] was a 3 years project aimed to implement QKD in industrial section and was coordinated by British Defence Evaluation and Research Agency(DERA).

9.3.3 In 2008, European FP6 project Secure Communication based on quantum cryptography (SECOQC) project [27] was launched in Vienna which integrated 6 different QKD systems together through trusted repeaters. It included organizations from Austria, Belgium, UK, Canada, Czech Republic, Denmark, France, Germany, Italy, Russia, Sweden and Switzerland. Here, coherent one way(COW) was realized by GAP-Universite de Geneva, distributed phase COW was realized by IDQ, entanglement based QKD was realized by Australian-Sweden consortium, free space QKD was realized by university of Munich using BB84 and low-cost QKD by University of Bristol

by Rarity's team (secure banking). Interestingly, from this project, the European Telecommunications Standards Institute (ETSI) launched a forum for QKD standards.

9.3.4 In 2010, the US Defense Advanced Research Projects Agency (DARPA) [28] together with BBN Technologies, Boston University and Harvard University designed DARPA quantum network across a metropolitan area.

9.3.5 The SwissQuantum [29] project which ran from 2009 for one and a half years was tested with real traffic.

9.3.6 Durban Network in South Africa [30] was developed by Durban-Quantum city project. Cambridge Network.

9.3.7 Thereafter, in 2007 China realized QKD network in the commercial telecommunication fiber network in Beijing and "Q-Government network" [31] in 2009. Recently, China has launched the $100 million satellite mission named Quantum Experiments at Space Scale (QUESS).

9.3.8 In 2010,Tokyo QKD network [32] successfully demonstrated high-speed QKD network where video conferencing was presented using one-time-pad (OTP) encryption. Latest QKD technologies and different QKD protocols like decoy based BB84, DPS-QKD, BBM92 and SARG04 were deployed.

10. CONCLUSION

10.1 There will be doubts whether practical QKD really offer absolute security. The answer to this question is very simple. The performance of every security system will depend on its fundamental operation principle and implementation. While, the security of QKD is based on laws of quantum mechanics the implementation scheme will determine the strength of security that will be provided. Potential applications include securing critical infrastructures like smart grid, financial institutions, national security and defence, Further, free space QKD implementations will enhance the range of applications, including secure satellite to ground station communication.

REFERENCES

1. S. Wiesner, Conjugate coding, ACM SIGACT News, vol. 15, pp. 78-88 (1983).

2. C. H. Bennett and G. Brassed, Quantum cryptography: Public key distribution and coin tossing, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, pp. 175-179 (1984).
3. A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett., vol. 67, pp. 661-663 (1991).
4. C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett., vol. 68, pp. 3121-3124 (1992).
5. L. Goldenberg and L. Vaidman, Quantum cryptography based on orthogonal states, Phys. Rev. Lett., vol. 75, pp. 1239-1243 (1995).
6. G.-C. Guo and B.-S. Shi, Quantum cryptography based on interaction-free measurement, Phys. Lett. A, vol. 256, pp.109 (1999).
7. G. Brida et al., Experimental realization of counterfactual quantum cryptography, Laser Phys. Lett., vol. 9, pp. 247 (2012).
8. A. Acin et al., Device independent security of quantum cryptography against collective attacks, Phys. Rev. Lett., vol. 98, pp. 230501 (2007).
9. M. Boyer, D. Kenigsberg and T. Mor, Quantum key distribution with classical bob, Phys. Rev. Lett., vol. 99, pp.140501 (2007).
10. A. Avella et al., Experimental quantum cryptography scheme based on orthogonal states, Phys.Rev. A, vol. 82, pp. 062309 (2010).
11. Hoi-Kwong Lo, Marcos Curty and Bing Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett., vol. 108, pp. 130503 (2012).
12. Yan-Lin Tang et al., Measurement-device independent quantum key distribution over 200 km, Physical review letters, vol. 113, pp.190501 (2014).
13. D. Stucki, et al., Fast and simple oneway quantum key distribution. Appl. Phys. Lett. vol. 87, pp.194108 (2005).
14. K. Inoue, et al., Differential phase shift quantum key distribution, Phys. Rev. Lett., ol. 89, pp. 037902 (2002).
15. V. Scarani et al., Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations, Physical Review Letters., vol*. 92, issue* 5, pp. 057901 (2004).
16. A. Pathak, Elements of Quantum Computation and Quantum Communication, CRC Press, May, 2013.
17. V. Scarani et al., The security of practical quantum key distribution, Rev. Mod. Phys., vol. 81, pp.1301 (2009).
18. http://www.idquantique.com/
19. *USA* http://www.magiqtech.com/
20. http://www.sequrenet.com/news.html
21. http://www.quintessencelabs.com/
22. http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information- Group/Quantum-Key-Distribution/Toshiba-QKD-system/
23. *China* Quantum Technologies (QTEC), Hangzhou, China http://www.idquantique.com/idq-qtec/
24. http://qunulabs.in/
25. P. D. Townsend, Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing, Electron. Lett., vol. 33, pp. 188-190 (1997).
26. D.A. Alekseev and A.V. Korneyko, Practice reality of quantum cryptography key distribution systems, Information Security, No. 1, pp. 72–76 (2007).
27. M. Peev et a., The SECOQC quantum key distribution network in Vienna, New J. Phys., vol. 11, 075001 (2009).
28. C. Elliott, Current status of the DARPA quantum network, in Quantum Information and Computation III, Proc.SPIE, vol. *5815*, pp. 138-149 (2005).

29. D. Stucki, et al., Long-term performance of the SwissQuantum quantum key distribution network in a field environment, New J. Phys., vol. 13, 123001 (2011).
30. A. Mirza and F. Petruccione, Realizing long term quantum cryptography, J. Opt. Soc, Am B, vol. 27, Issue 6, A185-A188 (2010).
31. F. X. Xu, et al., Field experiment on a robust hierarchical metropolitan quantum cryptography network, Chinese Sci. Bull. 54, vol. 2991 (2009).
32. M. Sasaki et al., Field test of quantum key distribution in the Tokyo QKD Network, Optics Express Vol. 19,Issue 11, pp. 10387-10409 (2011).