IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014), PP 01-09
www.iosrjournals.org

Quantum Key Distribution Protocols: A Review

Hitesh Singh [1,] D.L. Gupta [2] A.K Singh[3]
[1] *M.tech, Department of Computer Science Engineering, KNIT, Sultanpur, UP, India*
[2] *Member IEEE, Assistant Professor, Department of Computer Science Engineering, KNIT, Sultanpur, UP, India*
[3] *Associate Professor, Department of Electronics Engineering, KNIT, Sultanpur, UP, India*

Abstract : *Quantum key distribution (QKD) provides a way for distribution of secure key in at least two parties which they initially share. And there are many protocols for providing a secure key i.e. BB84 protocol, SARG04 protocol, E91 protocol and many more. In this paper all the concerned protocols that share a secret key is explained and comparative study of all protocols shown.*

Keywords : *Quantum key distribution, BB84 protocol, BB92 protocol, SARG04 protocol, E91 protocol, COW protocol, DPS protocol, KMB09 Protocol, S09 protocol, S13 protocol.*

I. INTRODUCTION

Quantum key distribution (QKD) [1] [2] provides a way for two parties to expand a secure key that they initially share. The best known QKD is the BB84 protocol published by Bennett and Brassard in 1984 [1]. The security of BB84 was not proved until many years after its introduction. Among the proofs [3] [4] [5] [6], the one by Shor and Preskill [6] is relevant to this paper. Their simple proof essentially converts an entanglement distillation protocol (EDP) based QKD proposed by Lo and Chau [5] to the BB84 Protocol. The EDP-based QKD has already been shown to be secure by [5] and the conversion successively leads to the security of BB84 protocol.

Security proofs of QKD protocols were further extended to explicitly accommodate the imperfection in practical devices [7] [8]. One important imperfection is that the laser sources used in practice and coherent sources that occasionally emit more than one photon in each signal. Thus they are not single –photon sources that the other security proofs [3] [4] [6] of BB84 assumed. In particular, BB84 may become insecure when coherent sources with strong intensity are used. For instance Eve can launch a photon-number-splitting (PNS) attack puts severe limits on the distance and the key generation rate of unconditionally secure QKD.

A novel solution to the problem of imperfect devices in BB84 protocol was proposed by Hwang [9]. Which uses extra test states called the decoy states to learn the properties of the channel and/or eavesdropping on the key-generating signal states. An unconditional security proof of decoy-state QKD [10] [11] is presented.

Another method to combat PNS attack was by Scarani et.al. [12], who introduced a new protocol called SARG04, which is very similar to the BB84 protocol. The quantum state transmission phase and the measurement phase of SARG04 are the same as that of BB84, as both use the same four quantum state and the same experimental measurement. The only difference between the two protocols is the classical post-processing phase, the protocol becomes secure even when Alice emits two photon, a situation under which BB84 is insecure .This protocol was proved by [13] who also proved the security of SARG04 with a single-photon source. They also proposed a modified SARG04 protocol that uses same six states as the original six state protocols [14] [15]. The security of SAG04 with a single-photon source was also proved by Branciard et.al [16]. They considered SARG04 protocol implemented with single-sources and with realistic sources. For the single-photon source case, they provided upper and lower bounds of the bit error rate with one-way classical communications. For the realistic source case they considered only incoherent attack by Eve and showed that SARG04 can achieve higher secret key rate and greater source distance than BB84.

Another protocol that is similar to SARG04 is the B92 Protocol [17] which uses two nonorthogonal quantum states. The security of B92 with a single-photon source was proved by Tamaki et al [18] [19]. On the other hand Koashi [20] proposed an implementation of B92 with strong phase-reference coherent light that was proved secure.

The Focus of this paper is to survey the most prominent quantum key distribution protocols and their security. In this paper we briefly describe the necessary principles of quantum mechanics from which the protocols are divided in to two categories those based on the Heisenberg Uncertainty Principles and others are based on quantum entanglement

Rest of the paper is organised as: In section II description of quantum cryptography and there mechanism is explained. Section III depicts all the Quantum key distribution protocols used Heisenberg's uncertainty principles. IV depicts all the Quantum key distribution protocols used quantum entanglement principles and in

section V other protocols that both prepare and measure and entanglement based is shown and in Section VI observation table of all the protocols with their applications is depicted. Finally Conclusion is shown in Section VII.

II. QUANTUM CRYPTOGRAPHY

Quantum cryptography is a relatively recent arrival in the information security world. It harnesses the laws of quantum Mechanics to create new cryptographic primitives. There is however, one quantum cryptographic primitive which is achievable with today's technology i.e. Quantum key distribution. By using the quantum properties of light, current lasers, fibre-optics and free space transmission technology can be used for QKD, so that many observers claim security can be based on the law of quantum physics only.

Quantum key distribution is a key establishment protocol which creates symmetric key material by using quantum properties of light to transfer information from Client A to Client B in a manner which, through the incontrovertible results of quantum mechanics, will highlight any eavesdropping by an adversary.

2.1 The Heisenberg Uncertainty Principle

According the Heisenberg Uncertainty principle, it is not possible to measure the quantum state of any system without disturbing that system. Thus the polarization of photon or light particle can only be known at the point when it is measured. This principle play a critical role in thwarting the attempts of eavesdroppers in a cryptosystem based on quantum cryptography.

For any two observable properties linked together like mass and momentum

$$\langle(\Delta A)^2\rangle\langle(\Delta B)^2\rangle \geq \frac{1}{4}\| \langle [A, B] \rangle \|^2$$

Where $\Delta A = A - \langle A \rangle$ and $\Delta B = B - \langle B \rangle$

And where $[A, B] = AB - BA$

According to the principle two interrelated properties cannot be measured individually without affecting the others. The principle is that since you cannot partition the photon in to two halves measuring the state of photon will affect it value. So if someone tries to detect the state of photons being send to the receiver the error can be detected [21]

2.2 Quantum Entanglement

The other important principle on which QKD can be based is the principle of quantum entanglement. It is possible for two particles to become entangled such that when a particular property is measured in one particle, the opposite state will be observed on the entangled particle instantaneously. This is true regardless of the distance between the entangled particles. It is impossible, however to predict prior to measurement what state will be observed thus it is not possible to communicate via entangled particles without discussing the observation over classical channel. The process of communicating using entangled states, aided by a classical information channel is known as quantum teleportation and is the basis of Eckert's protocol [22].

III. Qkd Protocols Using Heisenberg's Uncertainity Prinicples

Quantum cryptography exploits the quantum mechanical property that a qubit cannot be copied or amplified without disturbing its original state i.e. No-Cloning Theorem [23] [24]. Key distribution using quantum cryptography would be almost impossible to steal because Quantum key distribution (QKD) [25] [26] [27] systems continually and randomly generate new private keys that both parties shares automatically. A compromised key in a QKD system is able to decrypt only a small amount of encoded information because of continuously changes in private key. A secret key can be build from a stream of a single photon where each photon is encoded with a bit value of 0 or 1, typically by a photon superposition state such as polarization. These photons are emitted by a conventional laser as pulses of dim light so that most pulses do not emit a photon. This approach ensures that few pulses contain more than one photon travel through the fiber-optic line. In the end only a small fraction of the received pulses actually contains a photon [28]. The photons that are reached to the receiver are used. The key is generally encoded in either the polarization or the relative phase of the photon.

3.1 BB84 protocol

Quantum cryptography is based upon conventional cryptographic methods and extends these through the use of quantum effects. 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 as show in figure 6. The private key obtained then used to encrypt message that are sent over an insecure channel (such as a conventional internet connection).

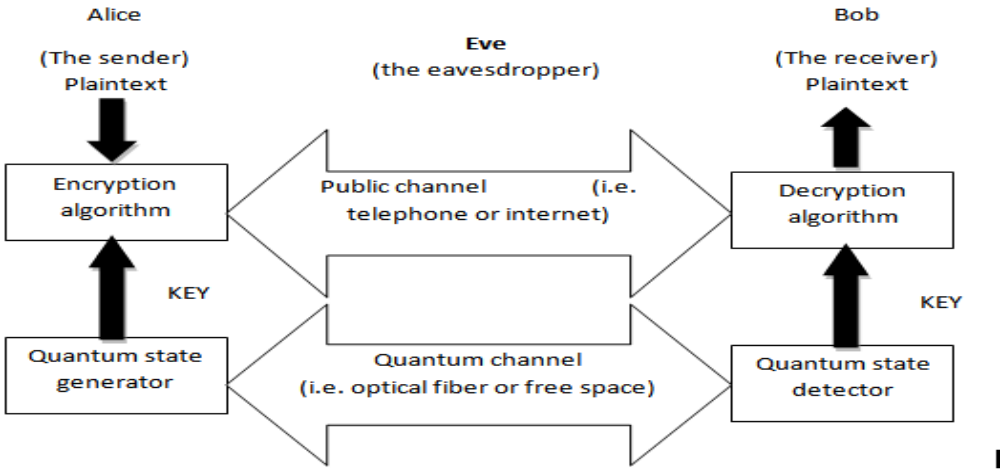

Figure 1: Quantum cryptographic communication System for securely transferring Random key

The BB84 protocol described using Photon polarization state to transmit the information. It was originally developed by Charles Bennett and Gilles Brassard in 1984 [1].

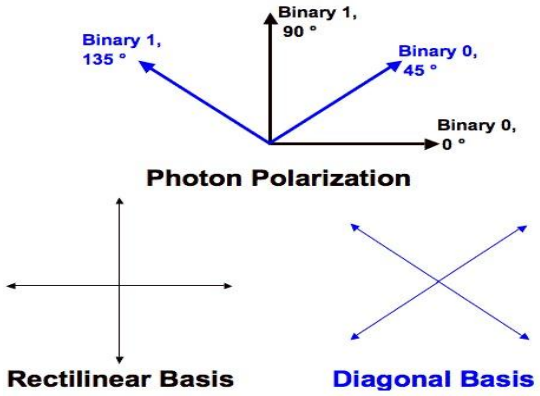

Figure 2: BB84 Bit Encoding

Below are the steps of the BB84 protocol for exchange the secret key in the BB84 protocol [29], client A and client B must do as follow:

STAGE 1 PROTOCOL Communication over quantum channel

- Client A prepare photon randomly with either rectilinear (+) or diagonal polarization (×) therefore Client A transmit photons in the four polarization states (0, 45, 90,135 degree).
- Client A records the polarization of each photon and sends it to Client B.
- Client B receives a photon and randomly records its polarization according to the rectilinear or diagonal basis. The Client B records the measurement type (basis used) and the resulting polarization measured. Client B doesn't know which of the measurement are deterministic, i.e. measured in the same basis as the one used by client A. Half the time Client B will be lucky and chose the same quantum alphabet as the third person. In this case, the bit resulting from his measurement will agree with the bit sent by Client A. However the other half time he will be unlucky and choose the alphabet not used by client A. In this case, the bit resulting from his measurement will agree with the bit sent by client A only 50% of the time. After all these measurement, client B now has in hand a binary sequence

Client A and Client B now proceed to communicate over the public two-way channel using the following stage 2 protocol.

STAGE 2 PROTOCOL: Communication over a public channel

Phase 1. Raw Key extraction

- Over the public channel, client B communicates to client A which quantum alphabet he used for each of his measurements.
- In response client A communicate to client B over the public channel which of his measurement were made correct alphabet.

Client A and Client B then delete all bits for which they used incompatible quantum alphabet to produce their resulting raw keys. If the third person has not eavesdropped, then their resulting keys will be the same. If the third person has eavesdropped their resulting key will not be in total agreement.

Phase 2**.** Error estimation

Over the public channel, Client A and client B compare small portion of their raw keys to estimate the error-rate R, and then delete the disclosed bits from their raw keys to produce their tentative final keys. If through their public disclosures Client A and Client B find no errors (i.e., R=0), then they know that the third person was not eavesdropping and that their tentative keys must be the same final key. If they discover at least one error during their public disclosures (i.e., R>0), then they know that the third person has been eavesdropping. In this case, they discard their tentative final keys and start all over again.

3.2 BB92 protocol

Soon after BB84 protocol was published, Charles Bennett realized that it was not necessary to use two orthogonal basis 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 [30], which is otherwise identical to BB84 protocol.

The key difference in BB92 is that only two states are necessary rather than the possible 4 polarization states in BB84 protocol.

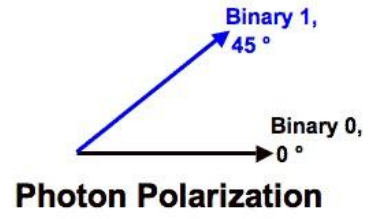

Figure 3: BB92 2-State Encoding

As shown in figure 3, 0 can be encoded as 0 degrees in the rectilinear basis and 1 can be encoded by 45 degrees in the diagonal basis. Like the BB84 protocol, Client A transmit to Client B a string of photons encoded with randomly chosen bits but this time the bits Client A chooses dictates which bases Client B must use. Client B 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. Client B can simply tell Client A after each bit Client B sends whether or not he measured it correctly [31].

3.3 SARG04 protocol

The SARG04 protocol is built when researcher noticed that by using the four states of BB84 with different information encoding they could develop a new protocol which would more robust when attenuated laser pulses are used instead of single- photon sources. SARG04 protocol was proposed in 2004 by Scarani et.al [32].

The SARG04 protocol shares the exact same first phase as BB84. In the second Phase when Client A and Client B determine for which bits their bases matched, Client A does not directly announce her bases rather than Client A announces a pair of non-orthogonal states one of which she used to encode her bit. If Client B used the correct basis, he will measure the correct state. If he chose incorrectly he will not measure either Client A states and will not be able to determine the bit. If there are no errors, then the length of the key remaining after the sifting stage is ¼ of the raw key.

The SARG04 protocol provides almost identical 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.

However SARG04 protocol provides more security than BB84 in the presence of PNS attack, in both the secret key rate and distance the signal can be carried (limiting distance).

3.4 Six-State protocol (SSP)

The 6-state or 3 bases cryptographic is nothing but the well-known BB84 4-state scheme with an additional basis [33]. Six-State Protocol (SSP) is proposed by Pasquinucci and Gisin in 1999 [34].

When represented on the Poincare sphere the BB84 protocol makes use of four spin-1/2 states corresponding to ±x and ±y direction. In brief summary Client A sends of the four states to Client B, who measures the qubits he receives in either the X or Y basis. A priori this gives a probability ½ that Client A and Client B use the same

basis. On an average Client A and Client B have to discard half of the qubits even before they can start extracting their cryptographic key.

In the 6 state protocols the two extra states correspond to ±z, i.e. the 6 states are ±x, ±y, and ±z on the Poincare sphere. In this case Client A sends a state chosen freely among the 6 and Client B measures either in the x, y or z-basis. Here the prior probability that Client A and Client B use the same basis is reduced to 1/3, which means that they have to discard 2/3 of the transmitted qubits before they can extract a cryptographic key. However, this scheme does hold an advantage compared to the BB84 protocol – higher symmetry. As it will be seen this fact together with the use of symmetric eavesdropping strategies dramatically reduced the number of free variables in the problem under investigation.

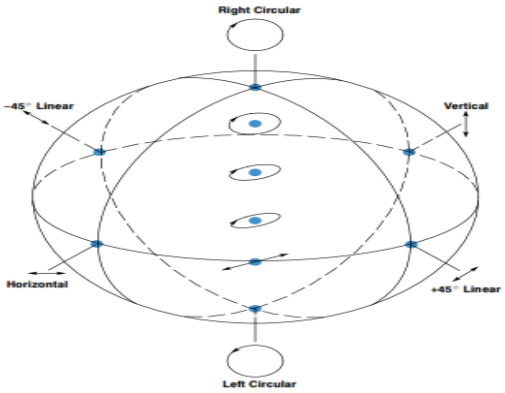

Figure 4: Poincare sphere

IV. Qkd Protocols Using Quantum Entanglement

A new approach to quantum key distribution where the key is distributed using quantum teleportation

4.1 E91 protocol

The Ekert scheme uses entangled pairs of photons [2]. These can be created by created by Client A, by Client B, or by some source separate from both of them, including eavesdropper Eve. The photons are distributed so that Client A and Client B each up with one photon from each pair.

The Scheme relies on two properties of entanglement. First the entangled states are perfectly correlated in the sense that if Client A and Client B both measure whether their particles have vertical or horizontal polarizations, they will always get the same answer with 100% probability. The same is true if they both measure any other pair of complementary (orthogonal) polarization However the particular results are completely random, it is impossible for Client A to predict if and Client B will get vertical polarization or horizontal polarization.

Second any attempt at eavesdropping by Eve will destroy these correlations in a way that Client A and Client B can detect.

A typical physical set-up is shown in figure 5, using active polarization rotators (PR), polarizing beam-splitters (PBS) and avalanche photodiodes (APD)

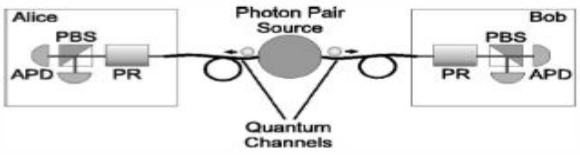

Figure 5: A Typical System Using Entangled Photon Pairs [35]

The measurement in the figure 5 is divided into two groups; the first is when different orientations of the analyser were used and the second when the same analyser orientation was employed. Any photon which was not registered is discarded. Alice and Bob then reveal the result of the first group only, and check that they correspond to the value expected from Bell's inequality. If this is so then Alice and Bob can be sure that the results they obtained in the second group are anti-correlated and can be used to produce a secret key string. Eve cannot obtain any information from the photons when they are transit as there is simple no information there. Information is only present once the authorized user performs their analyser measurements and key sifting. Eve's only hope is to inject her own data for Alice and Bob, but as she doesn't know their analyser orientations, she will always be detected (the Bell's inequality value will be too low).

4.2 COW protocol

Coherent One-Way protocol (COW protocol) is a new protocol for Quantum cryptography elaborated by Nicolas Gisin et al in 2004 [37].

A new protocol for QKD tailored to work with weak coherent pulses at high bit rates [36]. The advantage of this system are that the setup is experimentally simple and it is tolerant to reduced interference visibility and to photon numbers splitting attacks, thus resulting in a high efficiency in terms of distilled secret bits per qubit

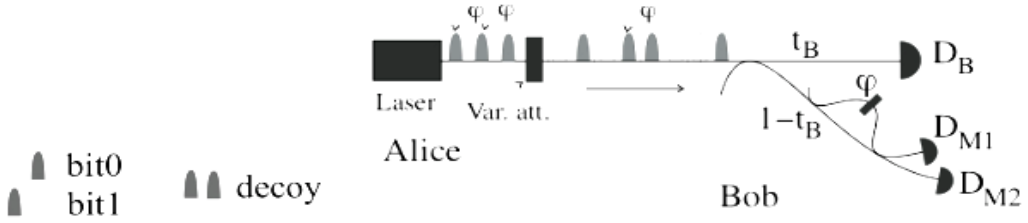

Figure 6: Scheme of the COW protocol [37]

The figure 6 presents the COW protocol. The information 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".

For security reason, Alice can also send decoy sequences μ-μ. To obtain the key, Bob measure the time-of-arrival of the photon on his data-line, detector D_B. To ensure the security Bob randomly measures the coherence between successive non-empty pulses, bit sequence "1 -0" or decoy sequence, with the interferometer and detectors D_{M1} and D_{M2}. If wavelength of the laser and the phase in the interferometer are well aligned, we have all detection on D_{M1} and no detection on $D_{M2.}$ 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.

4.3 DPS protocol

Differential –phase-shift QKD (DPS-QKD) is a new quantum key distribution scheme that was proposed by K.Inoue et al. [38]. Figure 7 shows the setup of the DPS-QKD scheme.

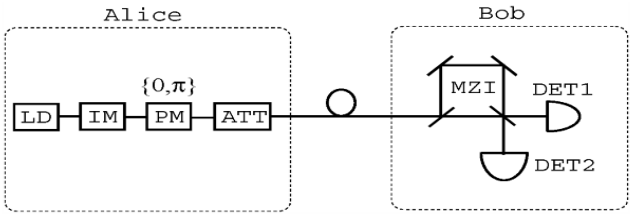

Figure 7: Schematic diagram of DPS protocol [38]

Alice randomly phase-modulates a pulse train of weak coherent states by {0,π} for each pulse and sends it to Bob with an average photon number of less than one per pulse. Bob measure the Phase difference between two sequential pulses using a 1-bit delay. Mach-Zehnder interferometer and photon detectors, and records the photon arrival time and which detector clicked. After transmission of the optical pulse train, Bob tells Alice the time instances at which a photon was counted. From this time information and her modulation data. Alice knows which 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 [38] [39].

V. Qther Protocols

There are many other protocols in existence, both prepare-and-measures and entanglement based. They are as follows:

5.1. KMB09 protocol

KMB09 protocol is an alternative quantum key distribution protocol [40]. Where Alice and Bob use two mutually unbiased bases with one of them encoding a '0' and the other one encoding a '1'. The security of the scheme is due to a minimum index transmission error rate (ITER) and quantum bit error rate (QBER) introduced by an eavesdropper.

The ITER increase significantly for higher dimensional photon states. This allows for more Noise in the transmission line, thereby increasing the possible distance between Alice and Bob Without the need for intermediate nodes

5.2 S09 protocol

S09 protocol is quantum protocol based on public private key cryptography for secure transmission of data over a public channel [41]. The security of the protocol derives from the fact that Alice and Bob each use secret keys in multiple exchange of the qubit. Unlike the BB84 protocol [1] and its many variants. Bob Know the key to transmit, the qubits are transmitted in only one direction and classical information exchanged thereafter, the communication in the proposed protocol remains quantum in each stage. In the BB84 protocol, each transmitted qubit is in one of four different states in this protocol transmitted qubit can be in any arbitrary states

5.3 S13 protocol

S13 protocol is a new quantum protocol [42] that is identical to the BB84 protocol for all the quantum manipulation, but differs from it by using Private Reconciliation from a Random Seed and Asymmetric Cryptography. Thus allowing the generation of larger secure keys.

VI. Observation

In this section all the concerned QKD Protocols are observed and show all the application of each protocol and by whom it was published in which year respectively.

Table I
List of Protocols and their applications

No	Year	Name of Protocol	Principles	Applications	References	Authors
1	1984	BB84	Heisenberg Uncertainty Principles	It uses Photon Polarization state to transmit the information it has four polarization states (0^0,45^0,90^0,135^0).	.[1]	C.H.Bennett and G.Brassard
2	1991	E91	Quantum Entanglement	It uses entangled pair of photons	[2]	Ekert A.K
3	1992	BB92	Heisenberg Uncertainty Principles	The only difference between the BB84 is that only two states are necessary rather than four polarization states i.e. (0^0, 45^0).	[30]	C.H. Bennett
4	1999	SSP	Heisenberg Uncertainty Principles	It is BB84 protocol with an additional basis i.e. it has 6 states are ±x, ±y, ±z on the Poincare sphere	[33],[34]	Bechmann-Pasquinucci.H and Gisin.N
5	2003	DPS	Quantum Entanglement	It has certain advantageous feature including a simple configuration, efficient time domain use and robustness against PNS attack.	[38], [39]	K.Inoue, E.Waks and Y.Yamanoto
6	2004	SARG04	Heisenberg Uncertainty Principles	It is an equivalent to BB84 but more robust when using attenuated laser pulses instead single photon sources. The QBER of SARG04 is twice that of BB84 i.e. more sensitive to losses. But provide more security than BB84 in the presence of PNS attack.	[32]	Scarani.V, A.Acin, Ribordy G , Gisin.N
7	2004	COW	Quantum Entanglement	To work with weak coherent pulses at high bit rates. The setup is experimentally simple and tolerant to reduced PNS attack Hence no information will be lost	[36],[37]	Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N and Scarani V
8	2009	KMB09	Heisenberg Uncertainty Principles	In this two parties used two bases: one for encoding '0' and the other for encoding '1' instead of using two direction of one single base	[40]	Muhammad Mubashir Khan, Michael Murphy and Almut Beige
9	2012	S09	Public private key cryptography	It allows massive key distribution between n-1 computers and one key message distribution centre.	[41]	Eduin Esteban Hernadez Serna

				It also immune to man-in-the-middle-attack as it does not use classical channels. Implementation of this protocol may be harder because the qubits get exchanged multiple times.		
10	2013	S13	Heisenberg Uncertainty Principles	It differs from BB84 using random seed and asymmetric cryptography. In this QKD becomes a process of zero information loss. It differs only in the classical procedure. This protocol can be implemented in existing device without modification.	[42]	Eduin H.Serna

VII. Conclusions

QKD Protocols are based on principles from quantum physics and information theory. Quantum key distribution is clearly an unconditionally secure means of establishing secret keys. Combined with unconditionally secure authentication, and an unconditionally secure cryptosystem.

The current commercial systems are aimed mainly at governments and corporations with high security requirements. The major difference of quantum key distribution is the ability to detect any interception of the key, whereas with courier the key security cannot be proven or tested. QKD system has the advantage of being automatic, with greater reliability and lower operating costs than a secure human courier network

References

Journal paper

[1]. C. H. Bennett and G. Brassard, "*Quantum cryptography: public key distribution and coin tossing*," Proc. of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179, 1984.
[2]. E. Artur "Quantum cryptography based on Bell's theorem.", Physical review Letters, Vol. 67, No, 6,5 august 1991, pp 661-663.
[3]. D.Mayers, Journal. of ACM 48, 351 (2001), preliminary version in Mayers, D. Advances in Cryptology-Proc. Crypto 96, vol 1109 of Lecture Notes in Computer Science, Kobiltz, N.Ed.(Springer-Verlag, New York, 1996) pp. 343-357.
[4]. E.Biham, M.Boyer, P.O.Boykin, T.Mor and V.Roychowdhury, in Proc of the thirty second annual ACM symposium on theory of computing (Portland, Oregon, United States, 2000), pp. 715-724
[5]. H.K.Lo and H.F.Chau Science 283, 2050 (1999)
[6]. P.W.Shor and J.Preskill, Phys.Rev. Lett 85,441(2000), arXiv: quant-ph/0003004.
[7]. [7] D.Gottesman, H.K.Lo, N.Liikenhaus and J.Preksill, 'Quantum Information and Computation 5, 325 (2004), arXiv: quant-ph/0212066.
[8]. H.Inamori, N.Liikenhaus, and D.Mayers (2001), arXiv.quant-ph/0107017.
[9]. W.Y.Hwang, Phys.Rev. Lett. 91, 057901 (2003).
[10]. H.K.Lo, X.Ma and K.Chen, Phys.Rev. Lett 94, 230504 (2005)
[11]. H.k.Lo, in Proc of IEEE International Symposium on Information Theory (ISIT) (2004), p.137, arXiv.quant-ph/0509076.
[12]. V.Scarani, A.Acin, G.Ribordy, and N.Gisim, Phys.Rev. Lett. 92, 057901 (2004).
[13]. K.Tamaki and H.K.Lo (2004), arXiv.quant-ph/0412035.
[14]. D.Bruss, Phys.Rev. Lett. 81.3018 (1998)
[15]. H.K.Lo Quantum Information and Computation1.81 (2001) arXiv.quant-ph/0102138.
[16]. C.Branciard, N.Gisin, B.Kraus, and V.Scarani. Phys.Rev.A 72 032301 (2005) arXiv.quant-ph/0505035.
[17]. C.H.Bennett.Phys.Rev.Lett. 68.3121 (1992).
[18]. K.Tamaki, M.Koashi, and N.Imoto, Phys.Rev.Lett.90.167904 (2003).
[19]. K.Tamaki and N.Liikenhaus, Phys.Rev. A 69.032316 (2004).
[20]. M.Koashi. Phys.Rev.Lett.93.120501 (2004). arXiv.quant-ph/0403131.
[21]. M.D.Dang and M. Riguldel, "Usage of secure networks built using quantum technology", 2004
[22]. [Ekert, A.k. "Quantum cryptography based on Bell's Theorem", Physical Review Letters vol.67.no6 5th august 1991, pp.661-663.
[23]. Dieks, D., Phys.Lett. 92, (1982), p 271
[24]. [Wootters, W.K., and W.H. Zurek, A Single quantum cannot be cloned, Nature, 299 (1982), pp982-983
[25]. G. Brassard and L. Salvail "*Secret key reconciliation by Public discussion*", Advances in Cryptology: Euro crypt 93 Proc. Pp.410-23, 1993.
[26]. C. Gobby, Z. L. Yuan and A. J. Shields, "*Quantum key distribution over 122 km telecom fiber*", Appl. Phys. Lett. 84, pp.3762–3764, 2002.
[27]. [D. Gottesman, H. K. Lo, N. Lutkenhaus and J. Preskill, "*Security of quantum key distribution with imperfect devices*", Quantum Information Computation. 4, pp.325–360, 2004.
[28]. K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova and P. D. Townsend, "*Quantum key distribution system clocked at 2 GHz*," Optics Express 13, pp.3015–3020, 2005.
[29]. F.Henle, BB84 online demo <http://monet.mercersburg.edu/henle/bb84/>. An online demonstration of the original BB84 algorithm from, Bennett et al. 1991.
[30]. C.H. Bennett Quantum cryptography using any two non orthogonal states, Physical Review Letters 68 (21) (1992) 3121-3124
[31]. Mart Haitjema, "A Survey of the Prominent Quantum Key Distribution Protocols "http://www.cs.wustl.edu/~jain/cse571-07/ftp/quantum/index.html#b92
[32]. Scarani, A.Acin, Ribordy, G.Gisin.N."Quantum Cryptography protocols robust against Photon number Splitting attack." Physical Review Letters, vol.92.2004 http://www.qci.jst.go.jp/eqsi03/program/papers/O26-Scarani.pdf

[33]. N.Gisin. talk presented at the workshop on Quantum Computation, Torino. July 1997; D.bruss. Physical review letter. Vol 81.no3018 (1998)
[34]. Bechmann-Pasquinucci, H and Gisin.N "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography." Physical Review Letter A59, 4238-4248; (1999).
[35]. N.Gisin, G.Ribordy, W.Tittel, H.Zbinden, "Quantum Cryptography", Review of Modern Physics, Vol 74 No 1, pp145-194, 2002
[36]. D.Stucki et al., Appl. Phys. Lett.87, 194108 (2005)
[37]. [Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N and Scarani V 2004, " Towards practical and fast quantum cryptography", arXiv:quant-ph/0411022
[38]. K.Inoue, E.Waks and Y.Yamanoto." Differential-phase-shift quantum key distribution using coherent light." Phys.Rev. A 68.022317 (2003).
[39]. E.Waks, H.Takesue and Y. Yamamoto, "Security of differential-Phase-Shift quantum key distribution against individual attacks." Phys.Rev.A 73,012344 (2006).
[40]. Muhammad Mubashir Khan et al. "High error-rate quantum key distribution for long distance communication" New J.Phys. 11 063043 http://iopscience.iop.org/1367-2630/11/6/063043/
[41]. Eduin Esteban, Hernandez Serna, "Quantum Key Distribution protocol with private- public key" arXiv: 0908.2146v4 quant-ph 12th may 2012
[42]. Eduin H.Serna, "Quantum Key Distribution from a random seed" arXiv: 1311.1582v2 quant-ph 12th Nov 2013

Hitesh Singh has completed his B.Tech degree in Computer Science & Engineering from Ideal institute of technology, Ghaziabad, Uttar Pradesh Technical University, Lucknow, India in the year 2007. He is pursuing M.Tech in Computer Science & Engineering from Kamla Nehru Institute of technology (An Academic Autonomous Govt. Engg. Institute), Sultanpur (U. P.), India, affiliated to U. P. Technical University, Lucknow, India. He has presented two paper in National Conferences and published paper in international journal of computer applications. His research interests are in cryptography and Network Security

Dharmendra Lal Gupta is currently working as an Assistant Professor in the Department of Computer Science & Engineering at KNIT, Sultanpur (U.P.) India. He received B.Tech. (1999) from Kamla Nehru Institute of Technology (KNIT) Sultanpur (U.P.), in Computer Science & Engineering, M.Tech. Hons (2003) in Digital Electronics and Systems from Kamla Nehru Institute of Technology (KNIT) Sultanpur (U.P.) India. He is a member of IEEE Computer Society. He has published about 14 papers in International/National Journals/workshops/conferences and seminars His research interests are Software Quality Engineering, Software Engineering, Cryptography &Network Security

Anil Kumar Singh is currently working as an Associate Professor in the Department of Electronics Engineering at KNIT, Sultanpur (U.P.) India. He received B.Tech.in Electronics & Telecommunication in 1982 from Government College Jabalpur (M.P.) India. He completed M.Tech. in Digital Electronics and Systems in 1988 from Kamla Nehru Institute of Technology (KNIT) Sultanpur (U.P.) India. He has published about 15 papers in International/National Journals/workshops/conferences and seminars. His area of interests involves optical communication system, Communication Networks, Microprocessor Based system etc.