International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

# A Comprehensive Survey on: Quantum Cryptography

**Pranav Verma[1], Ritika Lohiya[2]**

[1]Department of Computer Science and Engineering, Nirma University, Ahmedabad, India

**Abstract:** ***Quantum cryptography uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages. An 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. The security of quantum cryptography relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography which relies on the computational difficulty of certain mathematical functions, and cannot provide any indication of eavesdropping or guarantee of key security. In this paper we are discussing about various protocol introduced, possible attacks on them and prevention of those attacks.***

**Keywords:** Cryptography; Communication; Key Distribution; Quantum Cryptography; Security attacks;

## 1. Introduction

Cryptography is the secured means of communication between two or more parties who may have trust issues or may not trust one another. The best know example of cryptographic communication is the secret communication where the communicating parties exchange secret messages without any third party intercepting them. The two main type of cryptosytems used are private key cryptography and public key cryptography.

In private key cryptography, two parties say 'Alice' and 'Bob' wish to communicate by sharing a private key, which is known to them only. This private key is used by Alice to encrypt the messages which she wishes to send to Bob. After sending the encrypted information to Bob, he must now recover the original message using the same private key shared between them.
Unfortunately, private key cryptography has some disadvantages in many contexts. The major limitation of private key cryptosystems is how to distribute the keys? The key distribution problem is just as difficult as the communication between the two parties. It may happen that a malicious third party may be eavesdropping on the key distribution and may use this information to decrypt the messages intercepted.

The limitations of private key distribution led to the discovery of quantum computation and quantum mechanics to do the key distribution in such a way that security is not compromised. This later came to be known as quantum cryptography or quantum key distribution. The main goal is to exploit the quantum mechanical principle that observes the disturbance between the communicating parties. Thus if there is any interceptor who is listening to the communication between Alice and Bob will be visible as disturbance of the communication channel. And therefore, Alice and Bob can then throw out the key bits established while the eavesdropper was listening in, and start over.

The first proposal of quantum cryptography was presented by Stephen Wiesner wrote "Conjugate Coding", which took almost ten years to get established. Meanwhile Charles H. Bennett and Gilles Brassard took up the concept and published their work in series of papers with the demonstration of an experimental prototype which established the technological feasibility of quantum cryptography.

Quantum cryptography is based on Heisenberg's uncertainty principle, which says that measuring a quantum system will produce disturbance which in turn will yield incomplete information about its state before the measurement. Eavesdropping on a communication channel which uses quantum cryptography therefore causes an unavoidable disturbance which generates alerts to the legitimate users. This advantage helps a cryptographic system in distributing secret random keys between the communicating parties which initially share no secret information that is secure against an interceptor. After the secret key is established between the users over a channel, it can then be used with classical cryptography such as one time pad (OTP) to permit the users to communicate in absolute secrecy.

Another major type of cryptosystem is the public key cryptosystem. In public key cryptography the communicating parties don't rely on sharing a secret key for establishing a connection. For instance, Bob publishes a 'public key' which is available to all the users. If Alice wants to communicate to Bob he can use this public key to encrypt the messages. Public key cryptography did not achieve much accolade until the mid 1970s, when Whitfield Diffie and Martin Hellman proposed it independently. At the same time another public key cryptosystem was developed by Rivest, Adi Shamir and Leonard Adleman which later was known as RSA cryptosystem. RSA cryptosystem was believed to offer a fine balance of security and practical usability.

The main key to security in public key distribution is that, it becomes difficult to invert the encryption stage if only public key is available. For instance, inverting the encryption stage of RSA is same like a factoring problem. Security of RSA is assumed to come from the belief that factoring is the approach which is very difficult to solve on a classical

computer. The practical application of quantum cryptography to the breaking of the cryptographic codes has raised much of the interest in quantum computation.

Lastly the goal of quantum cryptography is to overcome the limitations of conventional cryptography. Quantum cryptography takes the advantages of the properties of quantum mechanics for example quantum no-cloning theorem and Heisenberg's uncertainty principle. In classical cryptography security is based on computational assumptions which are not yet proven, whereas in quantum cryptography security is based on the law of physics. Thus, most of the proposed applications of quantum cryptography consists of quantum key distribution, quantum bit commitment and quantum coin tossing. And the most successful and important application is quantum key distribution. Quantum cryptography is unconditionally secure and has been experimentally tested over hundreds of kilometres over optical fibres.

## 2. Limitations of Classical Cryptography

The classical cryptography solely relies on the random key generated by some mathematical computation. This has led to the following issues:

**Advancement in Computing Technology**
The keys used in modern cryptography are so large, in fact, that a billion computers working in conjunction with each processing a billion calculations per second would still take a trillion years to definitively crack a key .But with the advent of quantum computers in near future, which can perform calculations and operate at speeds no computer in use now could possibly achieve, the codes that would take a trillion years to break with conventional computers could possibly be cracked in much less time . As the keys can be cracked easily, the encryption algorithms would be of no use as they can be readily decrypted once the key is known.

**Key Distribution Problem**
Classical Cryptography suffers from Key Distribution problem, how to communicate the key securely between a pair of users. For years, it was believed that the only possibility to solve the key distribution problem was to send some physical medium – a disk for containing the key. In the digital era, this requirement is clearly unpractical. In addition, it is not possible to check whether this medium was intercepted – and its content copied – or not. Public key cryptography came as a solution to this, but these too are slow and cannot be used to encrypt large amount of data. Public key cryptography suffers because even though one way functions have not been yet reversed with technological and mathematical advances it is possible [1].

**Eavesdropping**
Eavesdropping is an act of capturing packets from the network transmitted by others' computers and reading the data content in search of sensitive information like passwords, session tokens, or any kind of confidential information. In classical cryptography, both the sender and the receiver of information will have absolutely no idea that they are being hacked.

These limitations can be easily overcome by switching over to Quantum Cryptography.

## 3. Un Breakable Nature of Quantum Cryptography

Quantum cryptography uses our current knowledge of physics to develop a cryptosystem that is not able to be defeated - that is, one that is completely secure against being compromised without knowledge of the sender or the receiver of the messages. Quantum communication involves encoding information in quantum states, or qubits, in contrast to classical communication's use of bits. Usually, photons are used for these quantum states. Quantum key distribution is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. Quantum cryptography obtains its fundamental security from the fact that each qubit of information is carried by a single photon, and that each photon will be altered as soon as it is read once. Any attempt to intercept message bits can be easily detected.

## 4. Fundamentals

*Qubit:* Any information in computer is stored using bits. One bit can only store one value at a time, and there are only possible values that a bit can have; either it is 0 or it is 1. In computer system we store these values in capacitors by keeping it either with charge or without charge. Qubit is no different than a bit, when the system is quantum then traditional instead of capacitors we have to store values in quantum particles known as qubits. There are many ways to represent a qubit for example: spin of the atom or polarization of the photons. There will always be two states by which the information can be represented in quantum computing.

*Qubit Representation:* In general, a quantum state |Ψ is an element of a finite-dimensional complex vector space (or Hilbert space) . We denote the scalar product of two states |Ψ) and |Φ) by ( Ψ| Φ ), where ( Ψ|= |Ψ ) T is the conjugate transpose of | Ψ). It is convenient to deal with normalized states, so we require (Ψ| Ψ) = 1 for all states |Ψ) that have a physical meaning. The quantum analog of the bit is called qubit, which is derived from quantum bit. A qubit |Ψ) is an element of a two-dimensional Hilbert space, in which we can introduce an orthonormal basis, consisting of the two states |0) and |1). Unlike its classical counterpart, the quantum state can be in any coherent superposition of the basis states:

j) = |0) + |1)
where |α|2 + |β|2 = 1

***Entanglement:*** Albert Einstein in 1935 (with colleagues Podolski and Rosen EPR theorem citation) gave a paradox (named EPR after them) to invalidate the undefined nature of

quantum systems. Entanglement is the capacity for sets of particles to cooperate over any separation immediately. Particles don't exactly communicate, at the same time there is a measurable relationship between consequences of estimations on every particle that is difficult to comprehend utilizing established physical science. To become entangled, two particles are permitted to associate; they then separate and, on measuring say, the speed of one of them, we can make certain of the estimation of speed of the other one, (before it is measured). The reason we say that they impart immediately is on account of that they store no local state and just have all around characterized state once they are measured. In light of this restriction particles can't be utilized to transmit established messages speedier than the rate of light as we just know the states upon measurement. Entanglement has applications in a wide variety of quantum algorithms and machinery.

***Superposition:*** Superposition means a system can be in two or more of its states simultaneously. For example a solitary particle can be going along two separate ways immediately. This infers that the particle has wave-like properties, which can imply that the waves from the diverse ways can meddle with one another. Obstruction can bring about the particle to act in ways that are difficult to clarify without these wave-like properties.

***QBER*:** Quantum Bit Error Rate is equivalent to the ratio of the probability of getting a false detection to the total probability of detection per pulse.

## 5. Quantum Cryptography Protocols

There have been several protocols proposed for the quantum cryptography and key distribution. The first among them was BB84 protocol proposed by B and B. There after researchers improved this base protocol and came up with newer variations with more and more security. Before going for those protocols first we will discuss about basic quantum mechanics theorems which are the bases of all these quantum bit based protocols.

**Heisenberg's uncertainty principle[2]**

In the classical physics Schrodinger attempted to present that by observing electron waves then we can determine future of the charge of the electron. Later Max Born showed that the wave function of Schrodinger cannot represent the destiny of a charge but it certainly shows probability of finding a charge at some certain point. Heisenberg took this theory one notch up and said if we are able measure the present position and momentum and all the forces acting on the particle; then we can calculate its destiny. The uncertainty principle does not follow this, it says that we can calculate only the range of possibilities of each motion. But again we can calculate exact probable value for each point of this range. According to the principle two interrelated properties cannot be measured individually without affecting the others. The standard is that since you can't segment the photon into two parts measuring the condition of photon will influence its value. So in the event that somebody tries to recognize the condition of photons being send to the recipient the blunder can be recognized.

**No Cloning Theorem [3]**

The quantum no-cloning theorem was stated by Wootters, Zurek, and Dieks in 1982, and has profound implications in quantum computing and related fields. As per the theorem it is not possible to clone any photon. When we read the photon position or try to capture and process it it's entanglement must be changed. Meaning that if we have traced any photon and we want another photon to be exactly similar to that, then it is not possible. Proof of this theorem is given here[4] for further studies.

**BB84 Protocol**

This protocol was proposed by Bennett and Brassard in 1984 [5] and hence named as BB84. This was the first protocol proposed to use photons for secure data transmission over the network. As per this protocol any two conjugate state pairs can be used by two parties for information exchange using photons on optical communication channel. This protocol uses two main steps the quantum state transmission step and the classical post processing step as discussed in [6] . BB84 uses Heisenberg's uncertainty principle of quantum mechanics discussed earlier. BB84 protocol was the first and is most widely used quantum cryptography protocol. Working of BB84 is well explained in [7]. The two parties 'Alice' and 'Bob' uses the polarised photons to establish a session key. The sequence they follow has following steps:[8]

a) *Transmitting a qubit string via the quantum channel:* Sender Alice sends polarized single photons; photons are polarized either in rectilinear or orthogonal basis. The basis are chosen randomly, and thus Bob also selects basis randomly to receive the qubits.

b) *Generating the source session key via the open channel:* Bob informs Alice about his selection of basis and Alice replies him how much he succeeded to detect the sent qubits correctly. After synchronization they discards the incorrect qubits. All these communication is done via public channel.

c) *Detecting the eavesdroppers on the open channel:* In public channel communication the security is on the stake. There are chances that the attacker(Eve) may have intercepted the photons in between and if she is lucky then her basis are similar to that of Bob's. If this happens then the key agreed on by Alice and Bob is also available to Eve, and she is un detectable by either users. In other case if the basis of Bob and Eve are different, then also there are 50% chances that Bob still gets the polarizations same as sent by Alice. So now the probability of Eve not being detected by Alice or Bob is 0.75 (0.5+0.5*0.5)

This is for one photon, similarly if we have to photons then the probability will be 0.752, thus for n photons ($0.75^n$). Or in other words the probability of eavesdropping if n photons are used is $1-(0.75^n)$ which will be near to 1 if large number of photons are used.

To prevent certain form of "Man-in-the-middle" attack there is a need of initial authentication before any exchange of a secret key over a secure communication channel could take place.

**E91 Protocol**

Artur Ekert proposed an algorithm based on entanglement often referred as EPR protocol too. The basis of his proposal was entanglements or quantum correlation of the photons[9] as we have discussed about entanglement in the earlier section. According to EPR Paradox if one part of the photon is read or tampered then status of the other on will also be disturbed, no matter how far they are physically and hence both the parties can detect the present of eavesdropper in the network. It is three state protocol where Alice and Bob where a portion of the entangled photon is sent by one of the user or by a third party on behalf of other user. One measures the basis and both the parties then communicate over the public channel. They divide the bits into two parts referred as raw and rejected key. The raw key part has the bits which were matched and other are kept in rejected key part. Over the public channel Alice and Bob compares their rejected key bits instead of raw keys, if they follow the Bell's inequality then a third party has been detected. Thus entanglement is a sufficient (but not necessary) condition for a secure key in this protocol.

**S13 Protocol**

S13 protocol was proposed by Eduin [10]. This protocols uses *Private Reconciliation* from a *Random Seed* and *Asymmetric Cryptography*. This helps in longer key generation and since it is based on *seed* it is completely random and secure. The random seed is used in place of a set of photons and asymmetric cryptography mechanism instead of encoded qubits, this makes the quantum key distribution process purely lossless. BB84 in which the expected percentage of coincidence of the recon ciliated key against the size of the raw key is 50% in S13 protocol it is 100%. S13 protocol similar to SARG04 uses the same quantum manipulations as the BB84 does, the difference is in the classical part. This makes it more easy to implement on already available hardware without making any changes.

A comparison of various protocols proposed in quantum cryptography, in tabular form is shown in table-1.

## 6. Possible Attacks on the System

A. *Individual Attack*: Performed by individual attackers. The eavesdropper tries to sense the data from communication channel. Same as Man-in-the-middle-attack it is referred as intercept-resend attack which gives bit error rate of 25%, which is readily detectable by two parties.

B. *Collective attack*: It is more general type of attack, the attacker captures each photon and attaches it with ancillary quantum, keeping the original to itself it forwards the tampered photon to the second part. By this way the attacker delays it's measurement basis assumption. After sensing traffic from both side for some period he determines his basis.

C. *Joint Attack*: The most general class of attacks is joint attack. In a such attack, attacker treats all the signals as a single quantum system, rather interacting with each signal independently. He then couples the signal system with her ancila and evolves the combined signal and ancilla system unitarily. He hears the public discussion between two parties before deciding on which measurement to perform on his ancilla.

D. *Photon Number Splitting Attack*: The security of BB84 protocol lies in no cloning theorem as we have seen in previously, this requires the two parties (say Alice and Bob) need to communication with single photon source only. But it is hard to get such device which can produce single photons in such a huge amount and that too constantly for a duration. If Alice is using multi photon source then it is possible for Eve to split those photons and keep a portion of it to herself in quantum memory. This action will however does not disturbs the other photons so no cloning theorem still holds here but the information has compromised.

E. *Timing Attack*: When transiting any bit in any communication channel there are some kind of timing information included in that, attackers have idea to exploit them and get knowledge about the information being transmitted. There have been several such timing attacks proposed for quantum channels also. In 2007 [11] researchers working in National University if Singapore showed how Eve can eavesdrop without introducing error in communication using timing information leaked during public discussion between both parties.

*Time-Shift Attack* against quantum key distribution protocols introduced in [12] this was very first attack on any commercial QKD. In this attack the attacker, first cuts the communication between Alice and Bob and then joins it with optical switches, but this time he/she makes two connections one shorter and other one longer than the cut sections.

*After-gate attack on quantum cryptosystem*: in 2010 group of researchers proposed this[13] This has perhaps been the most powerful and the best-performing hack on QKD so far. In 2011, they targeted yet another imperfection of these SPDs and based on the idea of faked states, they were able to remotely control the measurement outcome in Bob [14]

F: *Large Pulse Attack*: Each and every optical element reflects some amount of incoming light. This might be small in optical fiber (about -70dB/m) and angle-polished connectors (typically -40dB), medium for integrated optics components, like phase-modulators (≈ −20 dB) and large for mirrors (≥-1 dB). In Large Pulse Attack the attacker Eve send some very large pulses to the sender or Alice. Generally the sender uses black or dark equipment to send the signals, but no matter how dark the equipment is it will reflect some of the photons back to Eve, and hence she will be able to know the polarization which Alice is using. This is the attack where Eve does not have to read or change the qubits being exchanged between Alice and Bob, and she is able to get the polarization from source of the communication itself. This attack cannot be detected by analysing the photon

polarizations, as they have not been touched by the Eavesdropper.

## 7. Prevention techniques for attacks

*Heralded Photons*: A "heralded" photon is one of a pair whose existence is announced by the detection of its partner the "herald" photon. In photon pair generation, a laser pumps photons into a material whose properties cause two incoming pump photons to spontaneously generate a new pair of frequency-shifted photons. However, while these new photons emerge at precisely the same time, it is impossible to know when that will occur [15]

*Decoy State*: In 2002 Won-Young Hwang [16] proposed that Decoy State photons can be used to make the BB84 more secure. The security of BB84 protocol relies on the type of photon source, it must be single photon generator. But in real time implementation it is very hard to get a single photon generator, and sometimes the generated pulses has more than one photon in them which leads to Photo Number Splitting(PNS) attack. Decoy states are the solution for PNS attack, this state of photons are used specially for detection of eavesdropping. Alice now sends two types of pulses, one decoy state pulses and other pulses with states defined in BB84 protocol. In this manner Alice do not require single photon source for communication.

## 8. Challenges in Implementing QC

We have seen that quantum cryptography provides us next level of security which is unbreakable, though certain possible attacks have been proposed as we discussed in the previous section. Security comes with some cost and like every security mechanism quantum cryptography is also not untouched with challenges. The security of QKD has been thoroughly demonstrated in various late papers. There has been colossal enthusiasm for experimental QKD. Sadly, every one of those energizing late trials are, on a basic level, unreliable because of real life flaws. Major challenge is to create single photon source as the name suggest this source generated only one photon at a time and not more than that. The original BB84 protocol demanded for the same source , but in practical this has not possible yet. A lot of scientist groups and labs have tried to make such source which emits just one photon at a time but none of them has succeeded. To overcome this issue Decoy State quantum key distribution came into picture removing necessity of single photon source.

Another technique which is used widely in implementation of BB84 is use of faint coherent pulses instead of single photons, it is much simpler to prepare then true single photons. It uses an attenuator to generate faint coherent pulse. The major drawback of such implementation is that they are very much prone to *photon number splitting* attacks, as discussed earlier.

Use of trusted relays QKD network can increase distance reachable by QKD link. The relay nodes need to be trusted, although having the sender use a secret sharing scheme can reduce trust. It is particularly useful when the network operator is already a network user, as in the case of internal bank networks. Global key distribution is performed over a QKD path, i.e. a one-dimensional chain of trusted relays connected by QKD links, establishing a connection between two end nodes.

Secret keys are forwarded, in a hop-by-hop fashion, along QKD paths. To ensure their secrecy one can use one-time pad encryption and unconditionally secure authentication, both realized with a local QKD key. The trusted relays QKD network has been used in the DARPA and Vienna Network.

Speed of key exchange and reachable distance of QKD links are challenging factors today. According to SECOQC reports as of 2007 [17] one can expect to exchange between 1 and 10 kbits of secret key per second, over a point-to-point QKD link of 25 km (at 1550 nm, on dark fibres). The maximum span of QKD links is roughly 100 km at 1550 nm on telecom dark fibres. This range is suitable for metropolitan area scale QKD. Both secret bit rate and maximum reachable distance are expected to continue their progression during the next years due to combined theoretical and experimental advances. Significant speed increase is expected in forthcoming future, though it will require very fast detectors at telecommunications wavelengths, with good quantum efficiency and low dark count.

## 9. Conclusion

As we discussed in the above sections that the Quantum Cryptography is far more secure than the classical cryptography mechanisms and it's security has been proven by several ways. But considering that attacker may have unlimited resources and every possible technology to eavesdrop the communication, there are certain limitations or one should say space for improvement. Though this has been successfully implemented at lots of places, there are still issues to implement it for wide range of usage as we seen in section 8. Photon generator or source and transmission of photons without loss is the highest priority for researchers to make this mechanism work for more general public communication. At last there are many concepts and theories in the quantum physics which are not yet clear to researchers themselves, or some of them are having contradiction in their opinions so that is one thing which will lead the progress in this field with more practical implementation research by the time.

## References

[1] Tan, Xiaoqing. "Introduction to quantum cryptography." *Theory and Practice of Cryptography and Network Security Protocols and Technologies, ISBN* (2013): 978-953.
[2] Wheeler, John Archibald, and Wojciech Hubert Zurek, eds. Quantum theory and measurement. Princeton University Press, 2014.
[3] Etengu, R., et al. "Performance comparison of BB84 and B92 satellite-based free space quantum optical communication systems in the presence of channel

effects." *Journal of Optical Communications* 32.1 (2011): 37-47.
[4] Wootters, W. K., Zurek, W. H., "A single quantum cannot be cloned" Nature, vol. 299, Oct. 28, 1982, p. 802, 803.
[5] Bennett, Charles H., and Gilles Brassard. "WITHDRAWN: Quantum cryptography: Public key distribution and coin tossing." *Theoretical Computer Science* (2011).
[6] Fung, C-HF, and Hoi-Kwong Lo. "A survey on quantum cryptographic protocols and their security." *Electrical and Computer Engineering, 2007. CCECE 2007. Canadian Conference on*. IEEE, 2007.
[7] Elboukhari, Mohamed, Abdelmalek Azizi, and Mostafa Azizi. "Implementation of secure key distribution based on quantum cryptography." *Multimedia Computing and Systems, 2009. ICMCS'09. International Conference on*. IEEE, 2009.
[8] Chung, Yu Fang, Zhen Yu Wu, and Tzer Shyong Chen. "Unconditionally secure cryptosystems based on quantum cryptography." *Information Sciences* 178.8 (2008): 2044-2058.
[9] Ekert, Artur K. "Quantum cryptography based on Bell's theorem." *Physical review letters* 67.6 (1991): 661.
[10] Serna, Eduin H. "Quantum Key Distribution from a random seed." *arXiv preprint arXiv:1311.1582* (2013).
[11] Singh, Hitesh, et al. "Quantum Key Distribution Protocols: A Review." *Journal of Computational Information Systems* 8.7 (2012): 2839-2849.
[12] Zhao, Yi, et al. "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems." *Physical Review A* 78.4 (2008): 042333.
[13] Wiechers, Carlos, et al. "After-gate attack on a quantum cryptosystem." *New Journal of Physics* 13.1 (2011): 013043.
[14] Wiechers C, Lydersen L, Wittmann C, Elser D, Skaar J, Marquardt Ch, Makarov V and Leuchs G, 2011, After-gate attack on quantum cryptosystem, New Journal of Physics 13, 013043.
**[15]** NIST: Hark! Group Demonstrates First Heralded Single Photon Source Made from Silicon http://www.nist.gov/cnst/herald-062712.cfm
[16] Hwang, Won-Young. "Quantum key distribution with high loss: Toward global secure communication." *Physical Review Letters* 91.5 (2003): 057901.
[17] Johny, Shiji, and Anil Antony. "A Review on BB84 Protocol in Quantum Cryptography."
[18] Brassard, Gilles, et al. "Limitations on practical quantum cryptography." *Physical Review Letters* 85.6 (2000): 1330.
[19] Ojha, Vibha, et al. "Limitations of Practical Quantum Cryptography." *International Journal of Computer Trends and Technology-March to April* 2011.
[20] Rubya, T., N. Prema Latha, and B. Sangeetha. "A survey on recent security trends using quantum cryptography." *IJCSE* 2.9 (2010): 3038-3042.
[21] Lo, Hoi-Kwong, and Yi Zhao. "Quantum cryptography." *Encyclopedia of Complexity and Systems Science* (2009): 7265-7289.

## Author Profile

**Pranav Verma** received his M. Tech. degree in Computer Science and Engineering with specialization in Information and Network Security from Nirma University, India. His area of interest includes Network and Data Security, Cryptography, MANET, Security protocols for wireless networks etc.

**Ritika Lohiya** received her M. Tech. degree in Computer Science and Engineering with specialization in Information and Network Security from Nirma University, India. Her area of interest includes Cryptography, Intrusion Detection System, Cyber Forensics, Face Recognition etc.

**Table 1:** A comparison of various protocols proposed in Quantum Cryptography

| *Sr. No* | *Year* | *Name of Protocol* | *Principles* | *Applications* |
|---|---|---|---|---|
| 1 | 1984 | BB84 | Heisenberg Uncertainty Principles | Photon Polarization state is used in this protocol, there are four such stated defined in it. |
| 2 | 1991 | E91 | Quantum Entanglement | Entangled pairs of photons were used in place of polarization. |
| 3 | 1992 | BB92 | Heisenberg Uncertainty Principles | Made only two states compulsory instead of four polarization states. |
| 4 | 1999 | SSP | Heisenberg Uncertainty Principles | It has 6 states: ±x, ±y, ±z on the Poincare sphere, as there were only four in BB84. |
| 5 | 2003 | DPS | Quantum Entanglement | It is simple in configuration, has efficient time domain use and it shows robustness against Photon Number Splitting attack. |
| 6 | 2004 | SARG04 | Heisenberg Uncertainty Principles | It becomes more robust if attenuated laser pulses are used instead of single photon sources. It provide more security than BB84 against of Photon Number Splitting attack. |
| 7 | 2004 | COW | Quantum Entanglement | Able to work when there are high bit rates of weak coherent pulses. This can reduce PNS attack. |
| 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 |
| 9 | 2012 | S09 | Public private key cryptography | Hard to implement as there are many exchange cycles of qubits among users. It can distribute keys among n number of systems and one key message distribution centre. As no classical channel are used do it is secure fro Man-In-The-Middle attacks. |
| 10 | 2013 | S13 | Heisenberg Uncertainty Principles | Uses random seed. it has zero information loss. Differs only in the classical procedure, as compared to BB84.No need of hardware upgrade for implementation. |