# QUANTUM CRYPTOGRAPHY - A SURVEY

Arsha PV[1], Maya Mohan[2], and Sruthy Manmadhan[3]
[1]M.Tech First Year Student, [2,3]Assistant Professor
Department of Computer Science and Engineering
NSS College of Engineering, Palakkad
Email: [1]arshaabdulla92@gmail.com, [2]mayajeevan@gmail.com, [3]sruthym.88@gmail.com

***Abstract*—Quantum cryptography is the technique of exploiting the quantum mechanics properties to perform cryptography. The best known example of quantum cryptography is quantum key distribution(QKD) which provides a solution to the key exchange problems. In this paper we analyse the different methods of quantum key distribution and its applications in context of security.**

**Keywords: Quantum cryptography , Quantum key distribution**

## I. INTRODUCTION

Quantum cryptography is a prominent technology where two entities can communicate securely by implementing the sights of quantum physics. The principle of uncertainty could be used for cryptography was first devised by Stephen Wiesner, a physicist in 1969.

The strong point of quantum cryptography is that its security is guaranteed by laws of physics as it is impossible for an unauthorized party to copy an unknown quantum state. Therefore, many protocols for quantum cryptography including quantum key distribution and quantum secret sharing (which extends from two parties in quantum key distribution to more parties) have been proposed. However, four major weaknesses have stood in the way of widespread applications of these protocols, i.e., low coding capacity, low qubit efficiency, short achievable operating distances and low secure key generation rates. On the other hand, there are two major problems: 1) It is very hard and expensive to deal with a lot of quantum data. And 2) Quantum information is fragile (here, it means that it is easy to be broken physically) in nature. In fact, these are also the main reasons why quantum cryptography has not yet been widely used in our daily life.

### A. Quantum Cryptography

*1) Polarization of Photon :* The photon is polarized in one of the bases to represent a bit known as a qubit. A 0 degree polarization of photon in the rectilinear basis or 45 degree in the diagonal basis is used to represent a binary 0. A 90 degree polarization in the rectilinear basis or 135 degree in diagonal basis is used to represent a binary 1 as shown in Fig.1

*2) Representing Information- Qubits and quantum states:* The underlying unit of quantum cryptography is qubit. A bit can be in the state 0 or 1 whereas a qubit can occur in the state $|0>$ or $|1>$. It can also occur in superposition state which is a linear combination of the states $|0>$ and $|1>$.

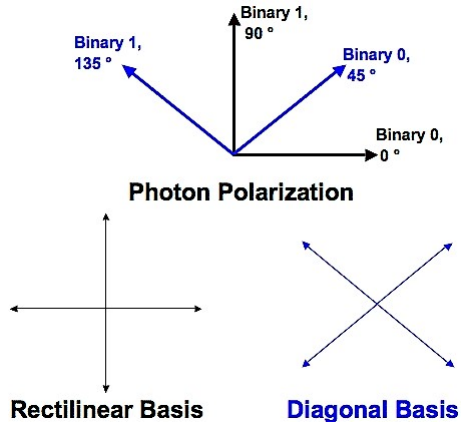


**Fig 1.** Polarization of photons to represent bits

### B. Quantum Key Distribution Protocol

*1) BB84 Protocol :* Bennet and Brassard proposed [1] the quantum key distribution protocol for the first time in 1984 and familiarized as the BB84 protocol depended on Heisenberg Uncertainty principle. The components of BB84 protocol are two bases that are to specify rectilinear (R) and diagonal (D) and four states of polarized photons. A 0 degree polarization of photon in the rectilinear basis or 45 degree in the diagonal basis is used to represent a binary 0. A 90 degree polarization in the rectilinear basis or 135 degree in diagonal basis is used to represent a binary 1.

In QKD, the communicating parties uses two communication channels namely a classical channel and a quantum channel. They transmit polarized single photons i.e. qubits on the quantum channel and the conventional messages on classical channel shown in Fig.2. The following are the steps for secret key which is shared between two users.

1) The sender makes random bits in sequence manner and chooses random bases. He/she represents bits using polarized photons and sends the photons to receiver through the quantum channel.
2) The receiver measures each of them by choosing one of the two bases.
3) If the receiver selects the same basis as of sender's, then he/she will share the same binary information with sender, otherwise, with a different basis.
4) The receiver communicates this through the classical channel and sender tells receiver for which qubit he/she chose the same basis as he/she.

5) Both the parties will delete the bits which are of different bases and the other bits are the key known as sifted key

| Quantum Transmission | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alice's Random bits | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |
| Alice's random sending bases | D | R | D | R | R | R | R | R | D | D | R | D | D | D | R |
| Photons Alice sends | / | \| | \ | – | \| | \| | – | – | \ | / | \| | \ | / | / | \| |
| Random Bases as received by Bob | R | D | D | R | R | D | D | R | D | R | D | D | D | D | R |
| Bits as received by Bob | 1 | | 1 | | 1 | 0 | 0 | 0 | | 1 | 1 | 1 | | 0 | 1 |
| Public Discussion | | | | | | | | | | | | | | | |
| Bob reports bases of received bits | R | | D | | R | D | D | R | | R | D | D | | D | R |
| Alice says which bases were correct | | | OK | | OK | | | OK | | | | OK | | OK | OK |
| Shared information | | | 1 | | 1 | | | 0 | | | | 1 | | 0 | 1 |
| Bob reveals some bits at random | | | | | 1 | | | | | | | | | 0 | |
| Alice confirms it | | | | | OK | | | | | | | | | OK | |
| Sifted Key | | | 1 | | | | | 0 | | | | 1 | | | 1 |

**Fig 2.** BB84 Protocol [2]

## II. RELATED WORKS

This section describes five proposed frameworks which discussed important challenges in practical QKD.

### *A. Differential Phase-Shift Quantum Key Distribution Systems*

Differential phase-shift (DPS) QKD is another QKD scheme [3] proposed about two decades after BB84, which has an unique structure different from BB84, featuring simplicity and practicality.

*1) Configuration and Operation:* A transmitter (Alice) sends a highly attenuated coherent pulse train that is randomly phase-modulated by $(0,\pi)$ for each pulse.The transmitted signal power is so small that the average photon number per pulse is less than one, e.g., 0.2. A receiver (Bob) receives the transmitted signal with a one-pulse delay Mach-Zehnder interferometer. In the interferometer, adjacent pulses interfere with each other, as illustrated in Fig. 3, and photons are detected according to the phase difference between the interfering pulses such that detector 1 (or 2) clicks for a phase difference of 0 (or $\pi$). Here, photon detection occurs rarely and randomly because of the small number of photons in the pulse train. After signal transmission, Bob tells Alice the photon detection time through a classical channel. With this time information and her phase modulation data, Alice knows which detector clicked at Bob. Then, Alice and Bob obtain identical bit strings, provided that detector1 (or2) is assigned to bit0 (or1), which can be a secret key.The configuration of DFS-QKD is shown in Fig.3.

The features of this protocol are simplicity and high key creation efficiency. The traditional QKD protocol BB84 includes a basis selection procedure, and basis-mismatched photons are discarded. On the other hand, the DPS protocol needs no such process and all detected photons contribute to key bits, resulting in a higher key creation efficiency. The fact that there is no need for the basis selection is also beneficial in terms of receiver complexity and detectors dark count errors. Practical BB84 systems usually employ a combination of a beam splitter (BS)and two sets of measurement apparatus for the basis selection, where

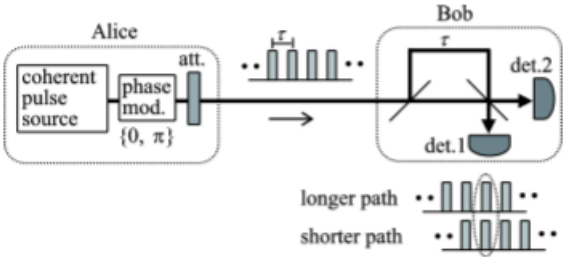


**Fig 3.** Configuration of DPS-QKD [3]

four photon detectors are used. On the other hand, the DPS protocol uses one measurement apparatus with two detectors, i.e., a simpler receiver configuration. In addition, the smaller number of detectors causes lower dark counts, resulting in a larger number of secure key bits after error correction and privacy amplification. Using sequential pulses, each of which can contribute to a key bit, is another feature. The time domain is efficiently utilized, resulting in a high key creation speed in practice. Robustness against photon-number splitting attacks, even when using weak coherent light, is another advantage of the DPS protocol.

*2) Security issues:*

- **Beam Splitting Attack:** The typical and simplest eavesdropping against QKD that uses coherent light is a beam splitting attack. Eve replaces the transmission line by a loss less one, splits and stores Alice's signal with a fraction corresponding to the original transmission loss, and measures the split signal after Bob's detection time is disclosed. This strategy does not change Bob's receiving signal and cannot be noticed at all.
  However, the amount of information leaked to Eve through this eavesdropping is limited because of the small photon number in DPS signals.In measuring the split and stored signal, Eve attempts to identify the phase difference between two neighboring pulses from which Bob detected a photon and created a key bit. Here, the corresponding pulses include $2r\mu$ photons on an average, where $\mu$ is the mean photon number sent from Alice per pulse and r is the beam-splitting ratio that is equal to the original transmission loss. Thus, the information rate leaked to Eve through the beam split attack is $2r\mu$, which is small for a small mean photon number $\mu$ and can be excluded from the key bits by privacy amplification.
- **Photon Number Splitting Attack :** Photon number splitting (PNS) attacks are known to be serious eaves dropping against BB84 using weak coherent light. In order to prevent this eavesdropping, a decoy method is usually employed in practical BB84 systems, making the key creation process complicated. The DPS protocol, on the other hand, is robust against PNS attacks [4]. In PNS attacks, Eve probes the photon number included in a transmitted signal, and picks up and measures an extra photon when more than two photons are included. Unfortunately for Eve, the phase information of a DPS signal collapses when the photon number is probed,

and, as a result, bit errors are induced at Bob. Thus, PNS attacks are readily revealed in DPS-QKD systems. This is one of the advantages of the DPS protocol compared with the original BB84 protocol.

- **Side-Channel Attack :** Recent QKD studies focus on side-channel attacks, which take advantage of imperfections in actual devices used in practical QKD systems. Such an attack was also proposed against a DPS-QKD system equipped with superconducting single photon detectors (SSPDs). Utilizing the operation characteristics of a SSPD, Eve arbitrarily manipulates the SSPD click by injecting bright blinding light. She can then obtain the complete key bit information by an intercept-resend attack using bright light as a fake signal. A countermeasure against this bright illumination attack has also been proposed. However,this eaves dropping can be noticed by monitoring the light power received by Bob. Based on, the injection light power should be greater than 30 dBm for Eve to perform the bright light illumination attack, which can be easily monitored by a handy optical power meter.

### *B. Safeguarding Quantum Key Distribution Through Detection Randomization*

A countermeasure scheme aiming on closing the back-door opened by the Single photo detector(SPD) regarding its susceptibility to external manipulation by bright light is proposed in [5]. This scheme used to render the detection apparatus of a quantum key distribution system immune to the main classes of hacking attacks in which the eavesdropper explores the back-door opened by the single-photon detectors. The countermeasure is based on the creation of modes that are not deterministically accessible to the eavesdropper. The use of beam splitters and extra single-photon detectors at the receiver station passively creates randomized spatial modes that erase any knowledge the eavesdropper might have gained when using bright-light faked states. The scheme is based on fundamental randomization of input modes to the detection apparatus inside Bobs station, thus not deterministically accessible to the Eve.

*1) Spatial Modes Randomization :* A practical scheme using BSs and additional SPDs is proposed to avoid the direct control of the detectors by the Eve. Fig.4 shows a sketch of Bob's apparatus employed in a BB84 based QKD system with the countermeasure implemented.

For each received qubit, Bob chooses the measurement basis at his HWP and sends it to a PBS. Each output spatial mode of the PBS is randomly divided in two modes by each BS according to Equation (3) [5]

$$|1,0>_{in1,in2} \rightarrow \sqrt{\tau}\,|1,0>_{out1,out2} + j\sqrt{1-\tau}\,|0,1>_{out1,out2} \quad (1)$$

where the indices in and out represent the two input and two output modes of the BS. When the splitting ratio $\tau$ is 0.5, the photon has the same probability of emerging at one or other output mode. Each output spatial mode is delivered to a SPD. When under regular operation, whenever Bob's basis is correctly chosen, detector A or B may click for a certain

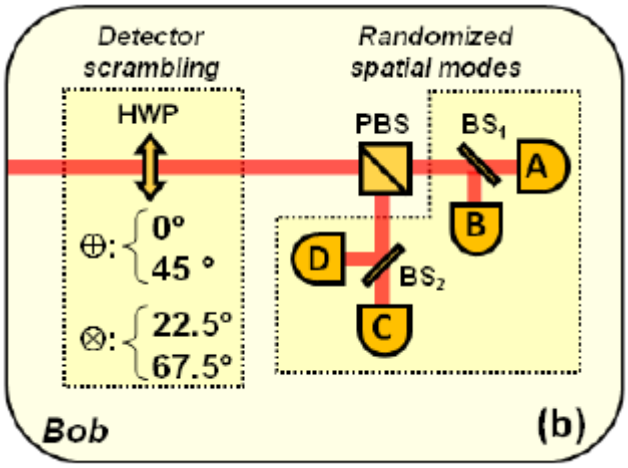


**Fig 4.** Countermeasure scheme with randomized spatial modes [5]

state (say, horizontal SOP); or detector C or D may click if the corresponding orthogonal state is received (vertical SOP). Due to the low average number of photons per optical pulse sent by Alice($\mu$), and the channel attenuation, the probability of both A and B, or C and D, detectors clicking together (coincident counts) is low. The counter-measure aims on avoiding the control of the SPDs by the Eve, what is accomplished through the randomization of the spatial modes by the two BSs. It is thus essential for the scheme to work that the splitting ratio of the BS cannot be manipulated by the Eve. The use of four standard SPDs behind the two BSs passively creates random spatial modes that are not deterministically accessible to the Eve. Thus the Eve has no access on the inner working of the devices and cannot deterministically manipulate the splitting ratio of the BS.

*2) Detector Scrambling :* Detector Scrambling is the the detector-scrambling countermeasure against detection efficiency mismatch-based attacks. This setup emulates the time-shift attack [6].

### *C. Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems*

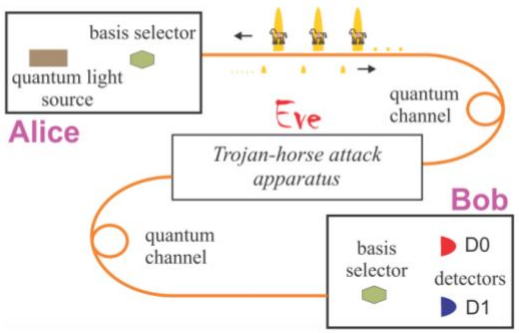


**Fig 5.** Scheme of a Trojan-hoarse attack [8]

Eve attacks Alice by sending a bright pulse from the quantum channel into the system and analyzing the back-reflected pulses

to know the bases selections during the operation of the QKD protocol. Thus information is carried by the back-reflected pulses coming out of Alice. Such Trojan-horse attacks [7] can breach the security of the QKD system, if appropriate safeguards are not installed, they can be fooled by the Eve. According to the rule of thumb, Eve must avoid disturbing the legitimate quantum signals traveling from Alice to Bob as much as possible since she is interested in knowing only the basis settings. Fig.5 shows the scheme of a Trojan-horse attack. Only the most relevant components are shown in Alice and Bob for the sake of clarity. The back-reflections that carry information of the applied bases are measured by Eve, for instance using state discrimination methods, as and when they return to the attack apparatus. If Eve could indeed do this entire operation without alerting Alice and Bob, she could break the security of any prepare-and-measure protocol (including both discrete and continuous variable protocols). However,as mentioned before, such vulnerability has been known for some time. Two common practical measures to prevent or catch Trojan-horse attacks [8] in action are to add an isolator or install a watchdog detector, respectively, at the entrance of the Alice subsystem. While an ideal isolator would passively torpedo any Trojan-horse attack by a complete extinction of Eve's pulses, no matter how bright dispatched into Alice, an ideal watchdog or monitoring detector would actively raise an alarm whenever any unknown or non-designated optical signals arrive into Alice.

*1) Back-reflections and Eve's Photon Budget :* In a Trojan-horse attack, Eve's light goes back and forth through the attacked subsystem. Moreover, atleast one of the onward Trojan-horse pulse or the back-reflected pulse must probe or pass through the basis selector(phase modulator)[9]. The onward and reverse paths decide the insertion loss, and together with the back-reflection level, determine the total attenuation suffered by Eve's pulse in the double pass. With the knowledge of these values,Eve can estimate the number of photons to expect on average ($\mu$Eve), in the back-reflected pulse of interest as it travels to her on the quantum channel.

We assume the attack wavelength to be $\lambda \sim 1550$ nm, a binary basis choice, and that $\mu$Eve $\approx$4 suffices for accurately knowing the probed choice of the basis. Eves Trojan-horse pulse needs to have roughly 4*10$\bigwedge$ 6. Photons for accurately knowing the probed choice of the basis. So that the back-reflected pulse of interest would carry the necessary four photons on average. Total attenuation suffered by Eves light can be calculated as R+ IL$\approx$60dB. Where R is reflectivity and IL is insertion loss. To protect the system against Trojan-horse attacks, Alice also uses an isolator providing an isolation of $\geq$ 50 dB at $\lambda \sim 1550$ nm. Eves photon budget needs to be raised by at least five orders of magnitude($>$4). Such powerful pulses easily detectable.

### *D. Quantum Photonic Network: Concept, Basic Tools, and Future Issues*

In a new network paradigm, various QKD schemes, physical layer cryptography, algorithmic cryptography and optical/quantum communications are integrated in an inter-operable manner, depending on user needs and allowed costs. Such a paradigm unifying quantum communication and cryptography with conventional optical communication and cryptography may be referred to as quantum photonic network [10]. This emerging platform is to integrate QKD for the highest security, quantum communication for power-minimum maximum-capacity communications, and a new scheme of physical layer cryptography which merges the merits of these two to realize the secrecy capacity with the provable security into a network, so that the whole network can provide best solutions for various kinds of use cases.

*1) Quantum Photonic Network:* Photonic network is an emerging infrastructure of optical communications. Its structure is depicted in Fig.6

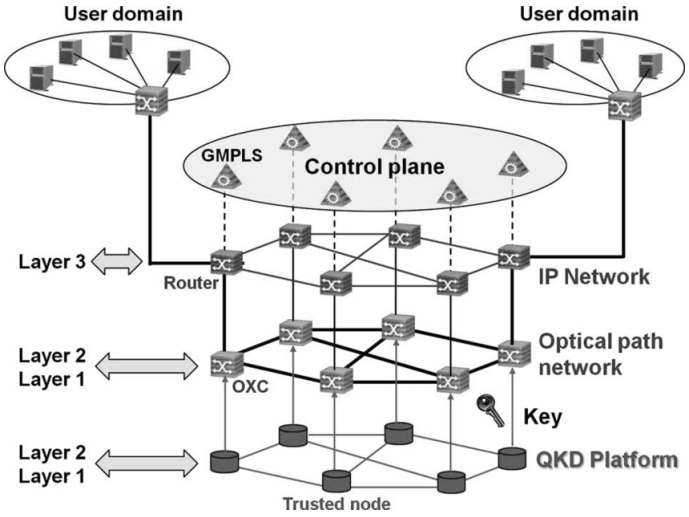


**Fig 6.** Quantum photonic network [10]

The optical path network is at the physical layer (Layer 1), and is made as transparent as possible based on all optical processing nodes (photonic nodes), instead of conventional nodes of electrical processing. It is to utilize broadband of optical fields and to resolve the speed limit and heating of electrical devices. Actually broadband optical transmission is realized by wavelength division multiplexing (WDM) in a fiber. Networking and routing are carried out by all optical processing with wavelength switching, which is performed by the optical cross-connects (OXCs). The OXCs are directly connected to IP routers at the network layer (Layer3) to setup a desired opticalpath. Routing,signaling,and link management at Layer 3 are supported by the generalized multi-protocol label switching in the control plane, which is implemented in out-of-band channels in optical fibers or sometimes over a dedicated control network.

Networking and extending the range of QKD must rely on the key relay via the trusted nodes at present. Security of the nodes should be protected classically. This means that there must be the same security loop holes in a QKD network as a classical one. In spite of this fact, the trusted-node-based QKD network is worth being developed as a practical network solution. One of new values added by QKD is the inter connectivity of cryptosystems, thanks to the simplest encryption/decryption by XOR operation between a plain/cipher text and a key. This point should be contrasted to conventional algorithmic schemes. Their high-end

solutions are specifically designed organization by organization, and their specification are usually not disclosed. This makes it very hard to interconnect the systems of different organizations in a seamless secure link. The QKD network can solve this problem if the keys and their identification could be properly managed in the trusted nodes.

*2) QKD and Related Technology :*

- **Entanglement QKD:** The entanglement based QKD [11] schemes require no random number sources because random selection of bases can be automatically done in a passive manner in the measurement process. This allows one a simpler implementation. The scheme is also less susceptible to side-channel attacks.
- **Efficient Photon Source:** The distance and key rate of the entanglement-QKD are still poorer than one-way QKD like BB84. For improving the key rate, more efficient photon sources are desired. for this a photon source based on type-II parametric down conversion with a group-velocity matched periodically poled KTiOPO4 (GVM-PPKTP) for the telecom bands [12].

### *E. Principles of 4 Level CV-QKD*

QKD uses a principle from quantum mechanics, namely the uncertainty principle, to avoid eavesdropping in a communication channel. If eavesdropping is detected, the key is discarded and a new key is sent at a different time. Once a secure key has been shared by the sender and receiver, an absolutely secure cipher transmission becomes possible by using a one-time pad scheme. In a QKD system, the sender transmits the key information to a legitimate receiver by encoding it on a single photon with orthogonal polarization or phases of a weak coherent light [13]. In CV-QKD [14], the information is encoded in the quadrature amplitude of a weak light.

Fig.7 shows a standard QPSK constellation used in digital coherent optical transmission. In this scheme, each I and Q component simultaneously has 1 bit of data, resulting in 2 bits/symbol. The first QKD method (BB84) uses two sets of orthogonal polarization states, namely the rectilinear mode (+) and the diagonal mode (⊗) as shown in Figure 7. The polarization orthogonality in each mode is assigned 0 or 1. For example, when a sender transmits bit 0 or 1 with a vertical or horizontal polarization state in the rectilinear mode, no data are simultaneously sent in the diagonal mode and vice versa.

This situation corresponds to 1 bit/symbol fitting one photon/bit. Note here that when an eavesdropper detects rectilinear data in a diagonal mode, she cannot obtain correct information because the same amplitude is inevitably detected. This concept can be transformed into orthogonal I and Q axes (modes) as shown in Fig.7. This method is called CV-QKD[15], in which the constellation is rotated 45 deg. from a conventional QPSK signal.

In addition, the photon number is reduced to one, where the size of the red circles is determined by an uncertainty principle with the photon number and the phase. When we deal with a single-photon-level signal, all the symbols are so close together

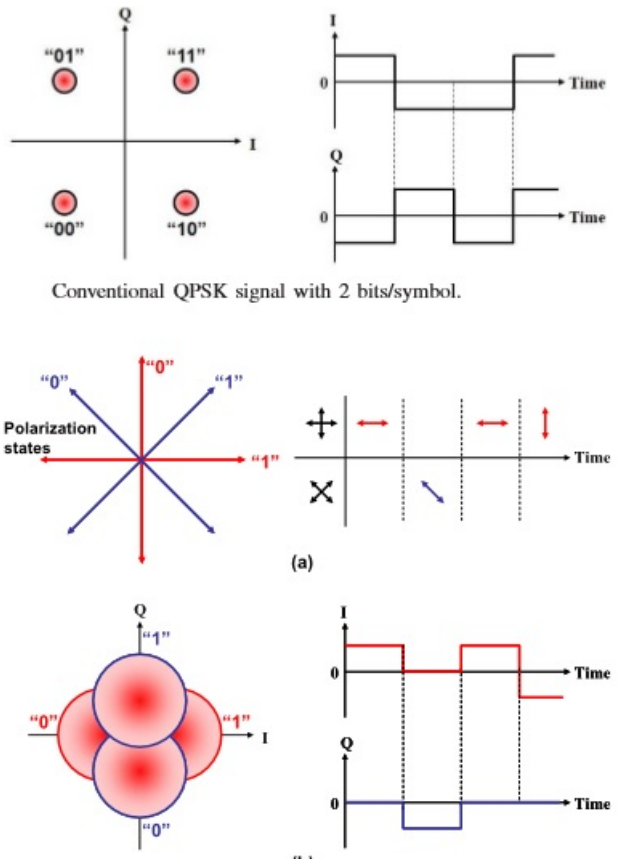


**Fig 7.** CV-QKD [15]

near the zero point that the error probability increases greatly in both modes, which makes it difficult for eavesdroppers to find the correct data. The sender transmits bits 1 and 0 at 0 and 180 deg. in the I mode and bits 1 and 0 at 90 and 270 deg.in the Q mode,respectively. When the key is transmitted in only the I mode, it is easy to determine whether the key is 0 or 1 by employing homodyne detection with a local oscillator (LO) signal, which is in-phase with the I mode. However, if we send a photon in the orthogonal Q mode, the detection result is randomly 0 or 1 with a probability of 1/2.

## III. DISCUSSIONS AND FINDINGS

Differential phase shift (DPS) QKD is a one kind of QKD scheme which has a unique structure different from BB84, featuring simplicity ,practicality and Robustness against photon number splitting attacks.DPS-QKD uses randomly phase modulated pulse train for transmission. Detection randomization scheme demonstrate a method to avoiding the control of SPDs through the randomization of spacial modes by the two BSs .So Eve cannot access on inner working of the user's devices. The main drawbacks of this scheme against quantum hacking are the increase in the number of detectors when compared to the traditional setup for the BB84 protocol.

Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems describes how the wavelength dependence of optical devices frequently used in practical fiber optical QKD systems that can make the system more vulnerable to Trojan-horse attacks.Isolator and Watchdog Detector Protect the

TABLE I
COMPARISON

| Papper | Method | Advantages | Limitations |
|---|---|---|---|
| [3] | DSP-QKD | simplicity, high key creation efficiency, Robustness against photon-number splitting attacks. | Vulnerable to sequential attacks. |
| [5] | SPD | Eve cannot access on inner working of the user's devices. | Requires more number of detectors. |
| [8] | Isolator and Watchdog Detector | Protect the system against Trojan horse attacks. | sensitive to photon's intensity. |
| [10] | QPN | Highest security power-minimum maximum-capacity communications. | high implementation cost. |
| [15] | CV-QKD | Delivering key with a high degree of security. | complex state of polarization. |

system against Trojan horse attacks. Quantum Photonic network provide a platform to integrate QKD for the highest security and quantum communication for power-minimum maximum-capacity communications. High implementation cost is the main disadvantage of this system. CV-QKD is a new QKD method . It transforms Orthogonal polarization states concept into orthogonal I and Q axes (modes). The transmission of key information using two orthogonal modes with an uncertainty relationship makes it possible to deliver a key with a high degree of security.

Quantum cryptographic security cannot be breached by any hackers so we can apply this technology in several fields for transmitting highly confidential data such as military and Ultra secure voting application. QKD provide a hope for the future communication network with highest security.

## IV. CONCLUSION

Quantum cryptography renders a cryptographic solution which is imperishable as it fortifies prime secrecy that is applied to quantum public key distribution. It is a prominent technology wherein two entities can communicate securely with the sights of quantum physics. In classical cryptography, bits are used to encode information where as quantum cryptography uses photons or quantum particles and photon's polarization properties used to encode the information. Once detected photon cannot back to its original polarized state So Quantum crytographic security does not hampered by hackers. The attacks against QKD can be nullify with proper and efficient counter measurement like DSP-QKD, CV QKD and Spatial mode randomization . Quantum photonic network is an emerging technology for high security communication.

## REFERENCES


[1] Bennett, C.H. and G. Brassard, 2014, " Quantum Cryptography: Public key distribution and coin tossing ", Theoretical Computer Science, Elseiver, vol. 560, pp.7-11.

[2] Ms. V. Padmavathi, et al., 2016, "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey ", *IEEE 6th International Conference on Advanced Computing*.

[3] Kyo Inoue, 2015, "Differential Phase-Shift Quantum Key Distribution Systems", *IEEE J. Quantum Electron*, vol. 21, no. 3.

[4] K. Inoue and T. Honjo, 2005, " Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack," Phys. Rev. A , vol. 71, no. 4, pp. 042305-1-042305-4.

[5] Thiago Ferreira da Silva, et al., 2015, " Safeguarding Quantum Key Distribution Through Detection Randomization ", *IEEE J. Quantum Electron*, Vol.17, No.1.

[6] Y. Zhao et al., 2008, " Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, p. 042333.

[7] N. Gisin et al., 2006, " Trojan-horse attacks on quantum-key-distribution systems ", *Phys.Rev.A,* vol.73,no.2, p. 022320.

[8] Nitin Jain, et al., 2015, " Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems ", *IEEE J. Quantum Electron*, vol. 21, no. 3.

[9] N.Jain, et al., " Trojan-horse attacks threaten the security of practical quantum cryptography," arXiv: 1406.5813, to be published.

[10] Mikio Fujiwara, et al., 2015, "Quantum Photonic Network: Concept, Basic Tools, and Future Issues", *IEEE J. Quantum Electron*, vol. 21, no. 3.

[11] K. Kitayama, et al., 2011, "Security in photonic networks: Potential threats and security enhancement," *J. Lightw. Technol.*, vol. 29, no. 21, pp. 3210-3222.

[12] R.-B. Jin et al., 2013, "Widely tunable single photon source with high purity at telecom wavelength," *Opt. Exp.*, vol. 21, no. 9, pp. 10659-10666.

[13] C. H. Bennett, 1992, " Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121.

[14] S. Lorenz, et al., 2004, " Continuous-variable quantum key distribution using polarization encoding and post selection," *Appl. Phys. B, Lasers Opt.*, vol. 79, no. 3, pp. 273-277.

[15] Masataka Nakazawa, 2017, " QAM Quantum Noise Stream Cipher Transmission Over 100 km With Continuous Variable Quantum Key Distribution ", *IEEE J. Quantum Electron*, vol. 53, no. 4.