Optoplex CORPORATION

48500 Kato Road., Fremont, CA 94538
Tel: (510) 490-8320, Fax: (510) 490-8330
info@optoplex.com， www.optoplex.com

Quantum Communication - QKD

1. Introduction

Today, when we talk about quantum communications, it means that a quantum channel is overlaid in the existing classic optical communication networks to securely transmit the key – Quantum Key Distribution (QKD).

In contrast to classical cryptography, quantum key distribution (QKD) and other protocols use quantum mechanics principles to provide an unconditionally secured public-key cryptosystem. These protocols can even detect the presence of an eavesdropper in the system who is attempting to learn the key.

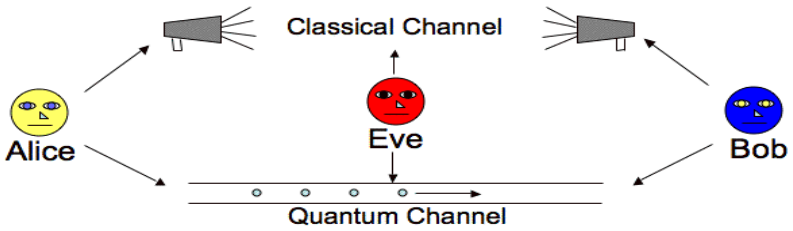

Figure 1.1, Basic QKD Model. Image by Mart

The basic model of QKD consists of two parties, referred to as Alice and Bob, having access to both a quantum communication channel (which is private) that involves sharing a secret key by exchanging quantum particles and a classical communication channel (which is public) that involves basis reconciliation, error correction, and privacy amplification protocols. We assume that an eavesdropper, called Eve, can access both channels.

Now, let's look at the concepts from quantum mechanics that make QKD so useful.

1. Heisenberg's Uncertainty Principle: This principle states that in a quantum system, only one property of a pair of conjugate properties like position and momentum can be known with certainty (a plausible measurement of a particle's position will disturb its speed). Quantum cryptography takes advantage of this by using the polarization of photons (as photons can be exchanged over fiber optic links) on different bases as the conjugate properties.

2. No Cloning Theorem: Indirectly following the last principle states that it is impossible to create identical copies of an unknown quantum state. Due to this, it is possible to find out if someone interrupted the quantum channel during the vital transmission.

Figure 1.2, Fictional representation of entanglement

3. Quantum Entanglement: Regardless of the distance, two quantum particles can entangle. When a particular property is measured in a particle, a correlated state of the property will appear on the other particle. Quantum teleportation uses entanglement for communication via a classical information channel. Entangled states are used as the basis of **Eckert's protocol**, which we will talk about later.

48500 Kato Road., Fremont, CA 94538
Tel: (510) 490-8320, Fax: (510) 490-8330
info@optoplex.com， www.optoplex.com

Quantum Key Distribution (QKD) is a method of secure communication that utilizes the principles of quantum mechanics to generate and distribute cryptographic keys between parties. The fundamental idea behind QKD is to exploit the inherent properties of quantum systems, such as the uncertainty principle and the no-cloning theorem, to establish secure communication channels.

Here's a breakdown of how QKD works:

1. Quantum Properties: QKD relies on the properties of quantum particles, such as photons, to encode information in quantum states. These quantum states can represent the 0s and 1s of classical binary digits (bits).
2. Key Generation: In QKD, two parties, typically referred to as Alice and Bob, exchange a stream of photons encoded with quantum states. These photons are sent over a communication channel, such as an optical fiber or through free space.
3. Quantum Uncertainty: The security of QKD relies on the principles of quantum uncertainty. Any attempt to intercept or measure the quantum states of the photons would disturb their quantum properties, alerting the communicating parties to the presence of an eavesdropper.
4. Measurement: After receiving the encoded photons, Alice and Bob perform measurements on them using compatible quantum measurement devices. These measurements are used to determine the values of the cryptographic key bits.
5. Key Distribution: By comparing a subset of their measurement results over a public channel, Alice and Bob can detect any potential eavesdropping attempts. They discard any bits where discrepancies are found, ensuring the integrity and secrecy of the final cryptographic key.
6. Secure Communication: Once a secure cryptographic key is established, Alice and Bob can use it to encrypt and decrypt their messages using classical encryption algorithms, such as the one-time pad or AES (Advanced Encryption Standard).

QKD offers a theoretically secure method for key distribution, as it relies on the laws of quantum physics to guarantee the security of the exchanged keys. However, practical implementations of QKD must address various challenges, including photon loss, noise, and technical limitations, to achieve real-world security and scalability. Despite these challenges, QKD holds promise for enhancing the security of communication networks, particularly in fields where data privacy and integrity are paramount, such as finance, healthcare, and government communications.

Applications

- Banking and Finance
- Cloud and Data Center
- Government and Defense
- Critical Infrastructure
- Telecommunications
- Healthcare
- Automotive
- IP Protection

2. QKD Schemes

2.1 Photons as Qubits

Photons have quantum properties and can be transmitted through fiber optics and, therefore, can be used to encode the secret key. Let's discuss how photons act as qubits and how we can operate them.

Photons are qubits for their state of polarization. Now, what is polarization? Before that, we must know what a lightwave is? A light wave is an electromagnetic wave where the plane occupied by the electric field is perpendicular to the plane occupied by the magnetic field. And the direction of propagation of the wave is orthogonal to these two planes.

When a light wave is polarized, it oscillates on a single plane. We can use polarizers and wave plates like half-wave plates and quarter-wave plates to polarize light.

There are two types of polarization: **linear** and **elliptical**. We don't need to know about elliptical polarization here. Linear polarization has two states: **rectilinear** and **diagonal**. Again Rectilinear polarization is of two types: **horizontal** and **vertical.** And Diagonal polarization is also of two kinds: **diagonal** and **anti-diagonal.**

It is pretty easy to see that we have a two-level system in photon polarization. Thus, we can use one as |0⟩ and another as |1⟩. The two states of rectilinear polarization, horizontal and vertical, are represented as |H⟩ and |V⟩. The two states of diagonal polarization, diagonal and anti-diagonal, are described as |D⟩ and |A⟩. Now, we can consider |H⟩ and |V⟩ as |0⟩ and |1⟩ on the **Z-axis** and |D⟩ and |A⟩ as |+⟩ and |-⟩ along the **X-axis**.

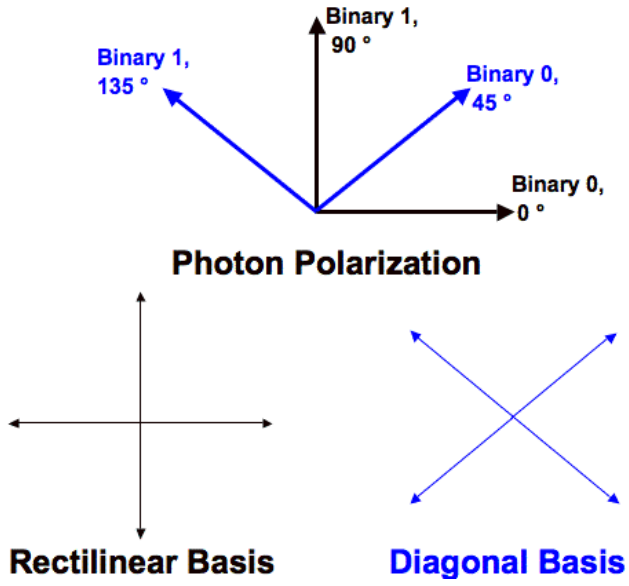

Figure 2.1, Bits are encoded in the polarization state of a photon. Image by Mart Haitjema.

2.2 Major QKD Schemes

There are three major QKS protocols:

1) DV – QKD: Discrete Variable QKD
2) CV – QKD: Continuous Variable QKD
3) DPR – QKD: Distributed Phase Reference QKD

In **DV QKD** protocols, the encoding is done in discrete variables of a quantum state like the polarization of single photons (qubits) with examples being BB84 [a], B92[b], SARG04 protocol [c].

In **CV QKD**, the message is encoded in continuous variables like quadratures of coherent or squeezed states with examples such as Gaussian protocol [d], Discrete modulation protocol [e], CV-B92 protocol [f] etc.

In **DPR QKD**, the phase difference between two successive pulses or the arrival times of the photons are used to encode the key information. In DPR protocols, single photon is not required for encoding, in fact, we use weak coherent pulses (WCP).

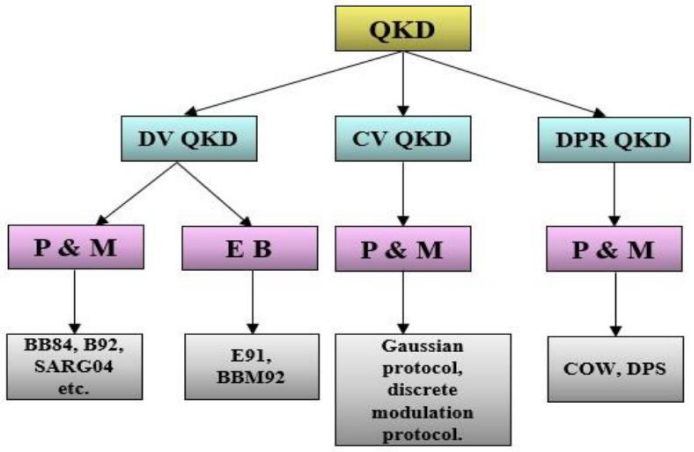

Figure 2.2, QKD Protocols. https://arxiv.org/pdf/2401.00146.pdf

- *P&M: Prepared and Measurement based-QKD protocol;*
- *E B: entanglement based QKD protocol*

References cited in Section-2

a) Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the International Conference on Computers, Systems and Signal Processing, 1984.
b) Charles H Bennett, Gilles Brassard, and N David Mermin. Quantum cryptography without Bell's theorem. Physical Review Letters, 68(5):557, 1992.
c) Valerio Scarani, Antonio Acin, Gr´egoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical Review Letters, 92(5):057901, 2004.
d) [22] Nicolas J Cerf, Marc Levy, and Gilles Van Assche. Quantum distribution of gaussian keys using squeezed states. Physical Review A, 63(5):052311, 2001.
e) [23] Mark Hillery. Quantum cryptography with squeezed states. Physical Review A, 61(2):022309, 2000.
f) [24] S Srikara, Kishore Thapliyal, and Anirban Pathak. Continuous variable B92 quantum key distribution protocol using single photon added and subtracted coherent states. Quantum Information Processing, 19:1–16, 2020.

- In CVQKD, continuous variables (such as optical field quadratures) are used for encoding quantum information.
- DVQKD, on the other hand, uses discrete variables (such as photon polarization or qubits) for key distribution.
- Both approaches have their advantages and applications, and recent progress in CVQKD is narrowing the gap between the two

48500 Kato Road., Fremont, CA 94538
Tel: (510) 490-8320, Fax: (510) 490-8330
info@optoplex.com， www.optoplex.com

3. DV-QKD

A. The BB84 Protocol

In 1984, Charles Bennett and Gilles Brassard published a protocol based on Heisenberg's uncertainty principle. The protocol is named BB84 after the authors' names and the year it was published. It is one of the most prominent quantum protocols. All the other protocols based on HUP are considered variants of BB84.

In the BB84 protocol, Alice can transmit a random secret key to Bob by sending a string of photons with the private key encoded in their polarization. The no-cloning theorem guarantees that Eve cannot measure these photons and transmit them to Bob without disturbing the photon's state in a detectable way.

The above is true, considering no error on the quantum channel. If the track is prone to error, Alice and Bob will not detect Eve's presence all the time.

B. The BB84 Protocol Variants

SSP99 Protocol: The six-state protocol was proposed by Pasquinucci and Gisin in 1999. Instead of two orthogonal bases, it uses six orthogonal bases to encode the bits, which results in a lower escape probability for Eve.

Eckert91 Protocol: Eckert used a single photon source in this protocol that produces entangled photons. One of the photons from each entangled pair goes to Alice and the other one to Bob. Alice and Bob randomly select bases to measure the photons. They will get correlated results for each measurement, where they chose the same basis. After removing the photons measured on different bases, they will have a bit-string binary correlated to each other. Knowing if the entangled states were inversely or directly related, Alice and Bob can convert their key to the shifted key. They can measure a photon (they measured on a different basis) on a third basis, and with that result, they can test Bell's Inequality to check Eve's presence. If the inequality contains, someone may have eavesdropped on the quantum channel.

B92 Protocol: In 1992, Charles Bennett developed a simplified version of the BB84 protocol where only two states are used in encoding bits in photons. Binary 0 is encoded as 0° on a rectilinear basis, and binary 1 as 45° on a diagonal basis. Here the bits themselves dictate the bases Alice must choose to encode them. Bob still selects bases randomly to measure the polarized photons. If he chooses the wrong basis, he will not get any measurement this time.

DV-QKD References

a) Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the International Conference on Computers, Systems and Signal Processing, 1984.
b) [15] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 68(21):3121, 1992.
c) [16] Valerio Scarani, Antonio Acin, Gr´egoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical Review Letters, 92(5):057901, 2004.
d) [17] Artur K Ekert. Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6):661, 1991.

48500 Kato Road., Fremont, CA 94538
Tel: (510) 490-8320, Fax: (510) 490-8330
info@optoplex.com， www.optoplex.com

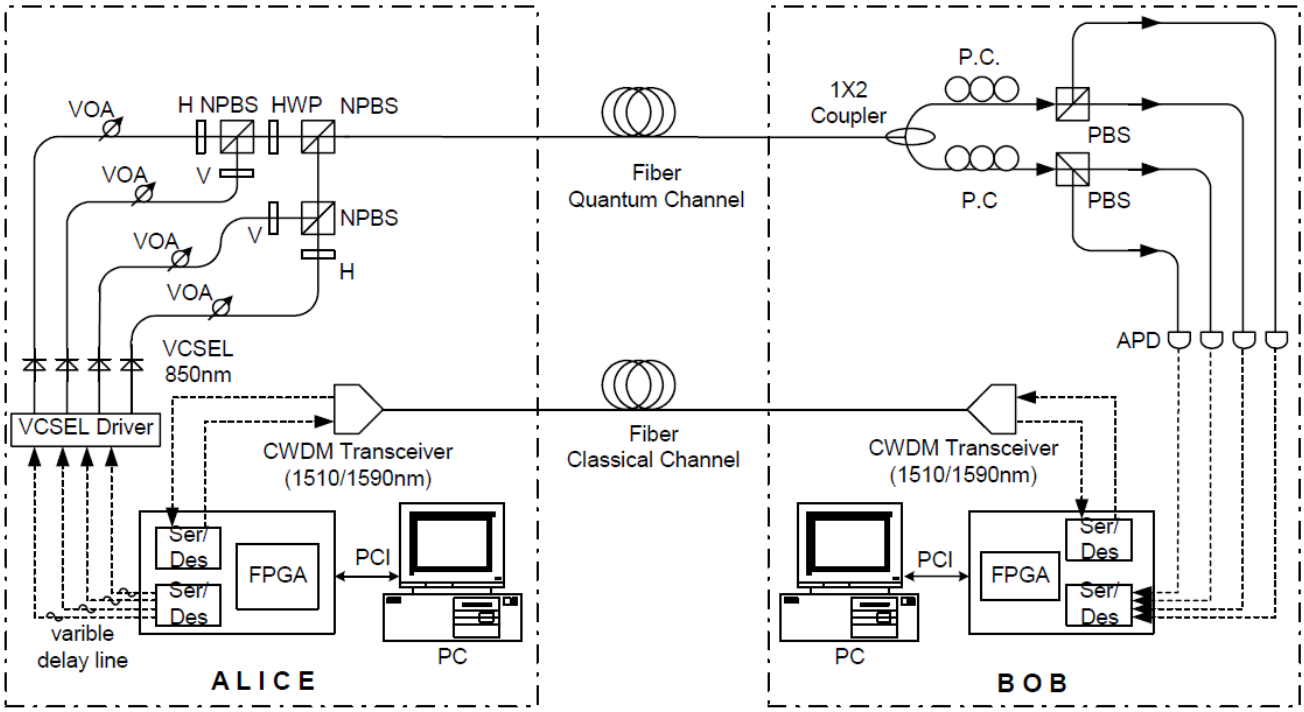

Figure 3.1, Schematic diagram of the BB84 QKD system;

VCSEL: Vertical-Cavity Surface-Emitting Lasers; HWP; Half-wave plate; VOA: Variable Optical Attenuator; NPBS, Non-polarizing Beam Splitter; P.C.: Polarization Controller; FPGA: Custom printed circuit board controlled by a field-programmable gate array; PCI: PCI bus; PBS: Polarizing Beam Splitter; Solid line: Optical fiber; Dotted line: electric cable.

Xiao Tang, etc., Proc. of SPIE Vol. 7092 70920I-1

In a high speed QKD system, the sifted-key rate *R* can be estimated by the following equation if the influence of the APD's dead time is ignored:

$$R = \mu \cdot L_f \cdot L_o \cdot Pd \cdot L_p \cdot \nu$$

Here the mean photon number μ is set to 0.1. *Lf* is the loss in the transmission fiber. *Lo* represents other losses such as bending, coupling and connection losses in the quantum channel. *Pd* is the APD's detection efficiency. *Lp* is the protocol related loss. ν denotes the quantum channel transmission rate. For 4km of 850nm fiber, the sifted-kay rate can be about 1Mbit/s.

48500 Kato Road., Fremont, CA 94538
Tel: (510) 490-8320, Fax: (510) 490-8330
info@optoplex.com， www.optoplex.com

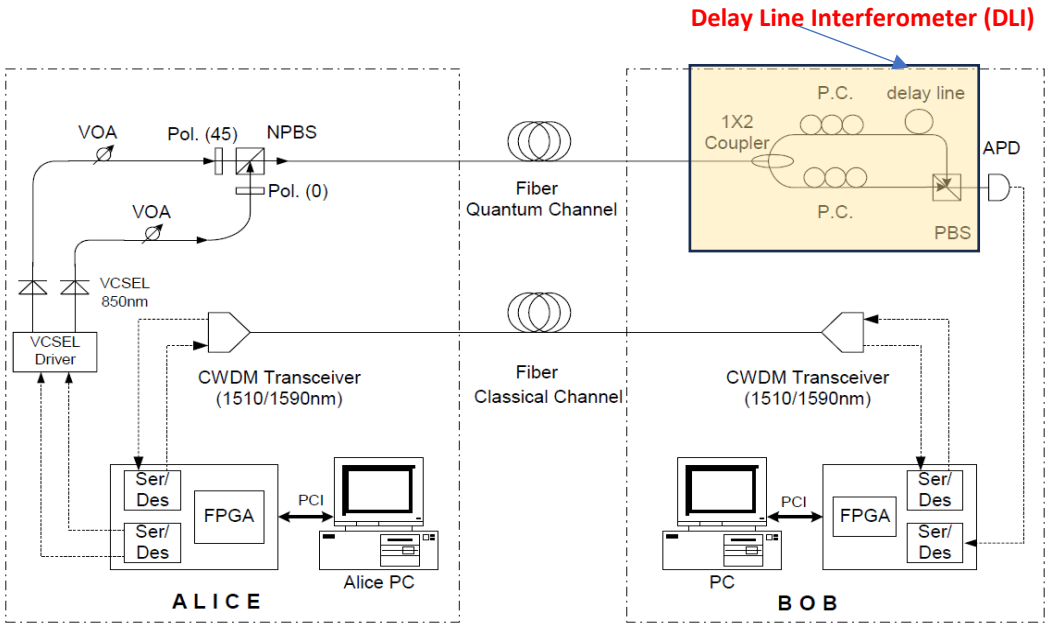

Figure 3.2, Schematic diagram of our B92 DTBS-QKD system;

VCSEL: Vertical-Cavity Surface-Emitting Lasers; Pol.: Polarizer;
VOA: Variable Optical Attenuator; NPBS, Non-polarizing Beam Splitter; P.C.: Polarization Controller; FPGA: Custom printed circuit board controlled by a field-programmable gate array; PCI: PCI bus; PBS: Polarizing Beam Splitter; Solid line: Optical fiber; Dotted line: electric cable.
Xiao Tang, etc., Proc. of SPIE Vol. 7092 70920I-1

Polarization based discrete variables quantum key distribution via conjugated homodyne detection

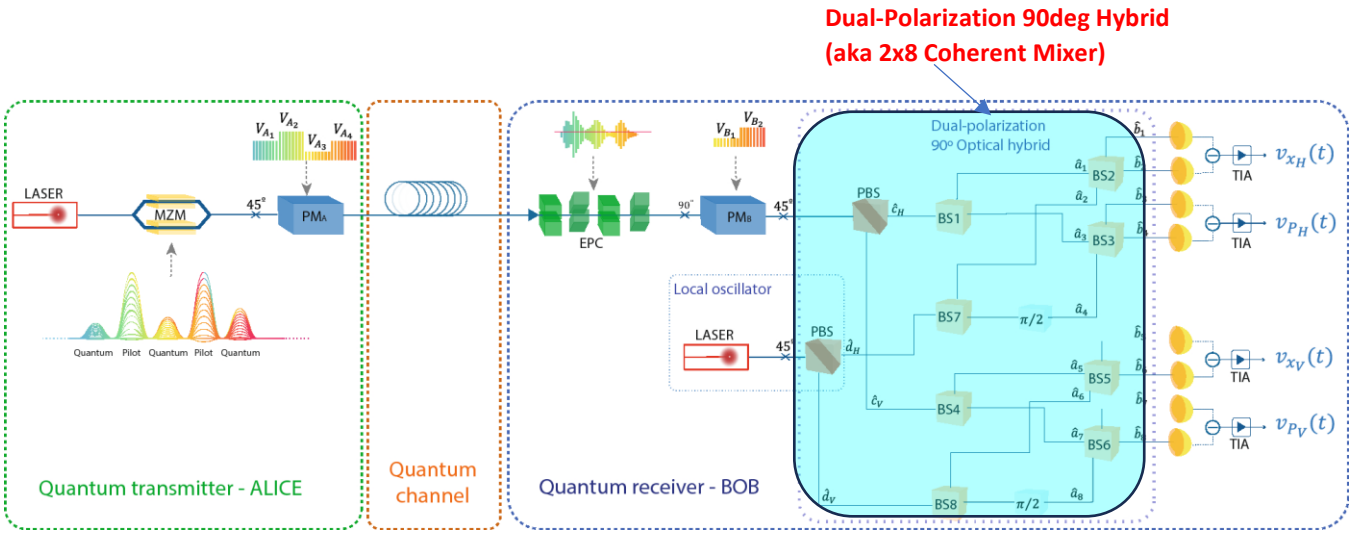

Figure 3.3, Schematic representation of the discrete variable quantum key distribution (DV-QKD) system based on polarization diversity coherent detection. [MZM] denotes the Mach–Zehender amplitude modulator, [PM_A] and [PM_B] the phase-modulators of Alice and Bob, respectively, [EPC] the electronic polarization controller, [PBS] the polarization beam-splitters, [BS] the beam-splitters, and [TIA] the trans-impedance amplifiers.

Mariana F. Ramos, Armando N. Pinto & Nuno A. Silva, Nature – Scientific Reports, 12 April 2022,

48500 Kato Road., Fremont, CA 94538
Tel: (510) 490-8320, Fax: (510) 490-8330
info@optoplex.com， www.optoplex.com

4. CV-QKD

Continuous-Variable QKD (CV-QKD), one of the major QKD schemes, focuses on continuous-variable systems and offers several advantages:

1. **Coherent States**: CV-QKD protocols are based on **coherent states**, which are continuous quantum variables. These states can be generated using commercial lasers and detected using homodyne detectors, making them compatible with existing telecom infrastructure.
2. **High Key Rates**: Unlike some discrete-variable QKD protocols, CV-QKD can achieve **high key rates** over metropolitan distances. This makes it suitable for practical applications in real-world scenarios.
3. **Room Temperature Operation**: The use of standard telecom components allows CV-QKD systems to operate at **room temperature**, simplifying their implementation.

Here's a brief overview of CV-QKD:

- **Principle**: CV-QKD relies on the continuous properties of quantum states, such as the quadrature amplitudes of coherent states. These continuous variables are modulated and transmitted over a quantum channel.
- **Security**: The security of CV-QKD protocols is analyzed against various attacks, including channel noise, detector imperfections, and eavesdropping. Rigorous security proofs ensure that the keys exchanged remain secure.
- **System Structure**: CV-QKD systems consist of key modules, transmitters, receivers, and classical communication channels. These components work together to establish secure keys.
- **Advancements**: Ongoing research focuses on digital techniques, system-on-chip implementations, and point-to-multipoint systems. These advancements aim to enhance the practicality and scalability of CV-QKD.

In summary, CV-QKD is rapidly transitioning from lab demonstrations to real-world implementations, promising secure communication channels based on the fascinating principles of quantum mechanics[1].

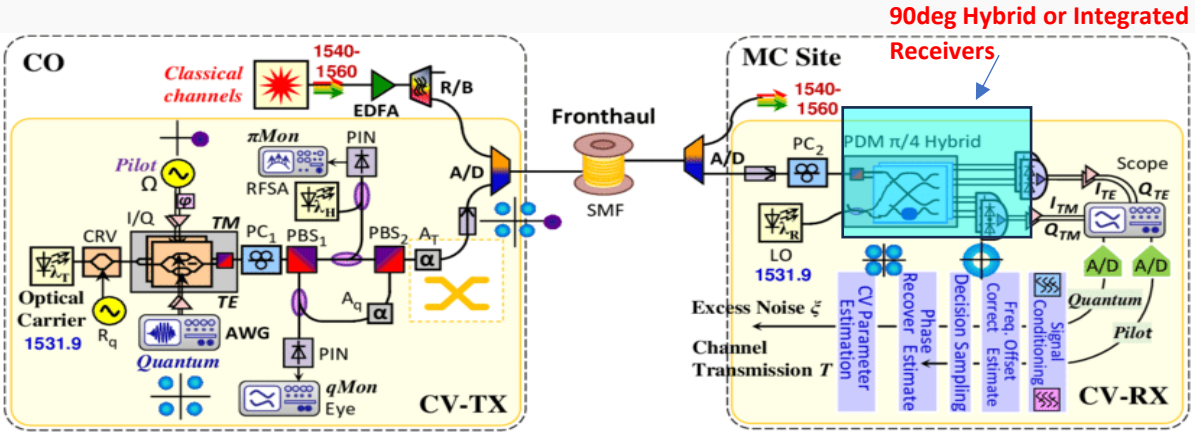

Figure 4.1, A typical CV-QKD system

Dinka Milovančev, etc., Journal of Lightwave Technology (Volume: 39, Issue: 11, June 2021)

48500 Kato Road., Fremont, CA 94538
Tel: (510) 490-8320, Fax: (510) 490-8330
info@optoplex.com， www.optoplex.com

A typical optical configuration of CV-QKS system is shown in Figure 4.2 below, in which a 90deg optical hybrid or 90deg hybrid integrated receiver is used in the receiving side.

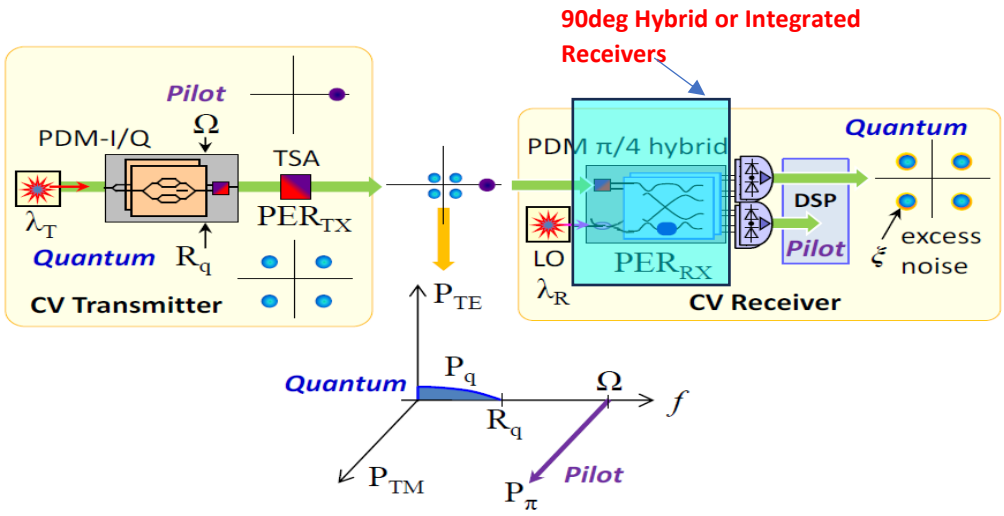

Figure 4.2, Optical setup in a typical CV-QKD system

Dinka Milovančev, etc., Journal of Lightwave Technology (Volume: 39, Issue: 11, June 2021)

A more complicated CV-QKS system in which a polarization-diversified 90deg hybrid (aka 2x8 coherent mixer) is used, as shown in Figure 4.3 below.

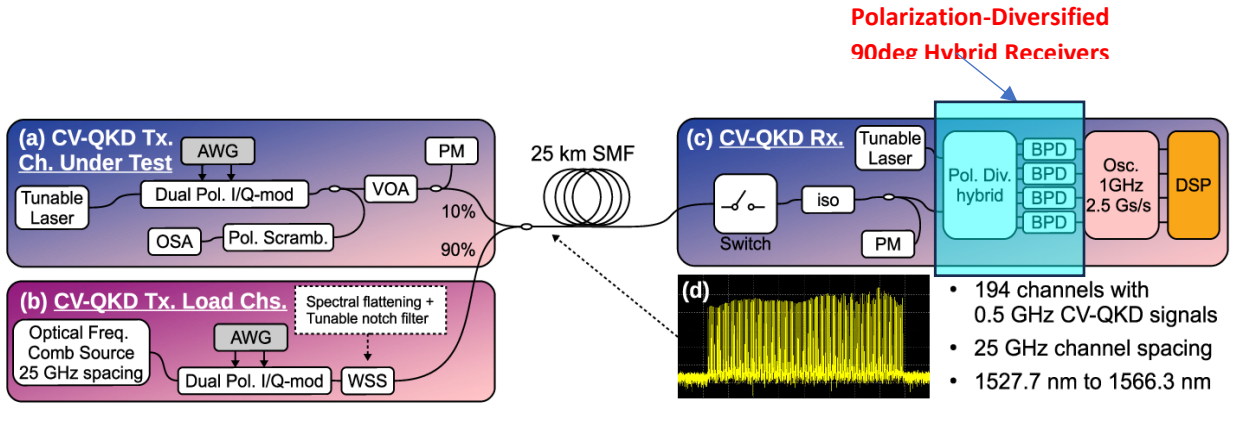

Figure 4.3, Experimental setup showing (a) the CV-QKD channel under test based generating 0.5 GHz four-state (QPSK) CV-QKD channels. (b) The transmitter for generating 193 load channels with a tunable notch filter to remove the load channel at the channel under test. (c) The CV-QKD receiver with a switch that is synchronized to the oscilloscope trigger to measure the shot-noise and CV-QKD signal in the same trace. (d) The measured spectra of the 194 transmitted CV-QKD channels

T. Eriksson, R. Luís, etc., Journal of Lightwave… 15 April 2020

References for CV-QKD

a) Timothy C Ralph. Continuous variable quantum cryptography. Physical Review A, 61(1):010303, 1999.
b) *Y. Zhang etc.,* Continuous-variable quantum key distribution system: past, present, and Future, *arXiv:2310.04831v3 [quant-ph] 17 Feb 2024*

Optoplex CORPORATION
48500 Kato Road., Fremont, CA 94538
Tel: (510) 490-8320, Fax: (510) 490-8330
info@optoplex.com， www.optoplex.com

5. DPR QKD

With the present available technology, a DPR scheme is considered to be one of the most practical QKD solutions. Compared to other QKD schemes, DPR QKD protocols have relatively easy-to-implement experimental setups and high communication efficiency. DPR QKD protocols are mainly divided into two protocols namely:

- differential phase shift (DPS) QKD and
- coherent one-way (COW) QKD.

DPS protocol was first introduced in 2002 [a] and COW protocol [b] was introduced in 2005 and since then we have seen several advances with respect to their experimental implementations for various distances. A detailed analysis of the major advancements in the distances of DPR QKD will be discussed during the later part of this article.

In DPS QKD, the encoding is done in the form of the phase difference between two consecutive coherent pulses and the mean number of photons should be ($\mu = |\alpha|^2 = 0.2$), while

in COW QKD, the encoding is done by combining vacuum and coherent pulse with mean photon number ($\mu = |\alpha|^2 = 0.5$).

Both of the protocols are robust with respect to photon number splitting (PNS) attack and polarization sensitivity. In case of DPS QKD, the minimum number of detectors required is 2 whereas for COW QKD implementation, 3 detectors are required (one for data line and the other two are for monitoring line).

(PNS: Photon number splitting; WCP: weak coherent pulse (WCP)

Important Parameters

DT: Detector Dead Time

DR: Disclose Rate

CR: Compression Rate

Table 5.1, Comparison of COW and DPS

S No.	Properties	COW	DPS
1	Encoding	Combining vacuum and coherent pulse	Phase difference between consecutive coherent pulse
2	Source	WCP	WCP
3	μ	0.5	0.2
4	PNS attack effect	No	No
5	No of detectors	3	2
6	Phase	Constant	Modulated
7	Intensity	Modulated	Constant
8	Polarization	Insensitive	Insensitive

https://arxiv.org/pdf/2401.00146.pdf

5.1 DPS QKD

The DPS QKD protocol was proposed in 2002 by Inoue et al. *[a]*. In this protocol, Alice creates a weak coherent pulse (WCP) whose average photon number is 0.2 and randomly modulates the phase either by 0 or π using a phase modulator. She sends these modulated pulses to Bob using an optical fiber. At the receiver's side, Bob passes the received pulses to a 1 bit delay Mach Zehnder interferometer. The outputs of the Mach Zehnder interferometer are measured either by single photon detectors (SPDs) or superconducting nanowire single photon detectors (SNSPDs). The two consecutive pulses interfere with each other in the Mach Zehnder interferometer with the detection from either of the two detectors having information of the phase difference between the two consecutive pulses. In *Fig. 5.1*, click on DM1 (DM2) means phase difference 0 (π) between the two successive pulses. The steps involved in the DPS QKD protocol are as follows:

1) Alice sends a random sequence of phase-modulated (0, π) attenuated pulses to Bob, with each pulse having an average photon number less than one.
2) Bob uses photon detectors and a 1 bit delay Mach Zehnder interferometer to measure the phase difference between two consecutive pulses and records the information of detector clicks as well as time of arrival of photons.
3) Bob publicly informs Alice about the times when either of the detectors clicked.
4) With the timing information about Bob's detectors clicks, Alice obtains 'which detector clicks' information at Bob's side.
5) Key bits 0 and 1 are respectively assigned if the phase difference between two successive pulses are 0 or π.
6) Alice and Bob perform error correction and privacy amplification on the sifted key to obtain the secret key.

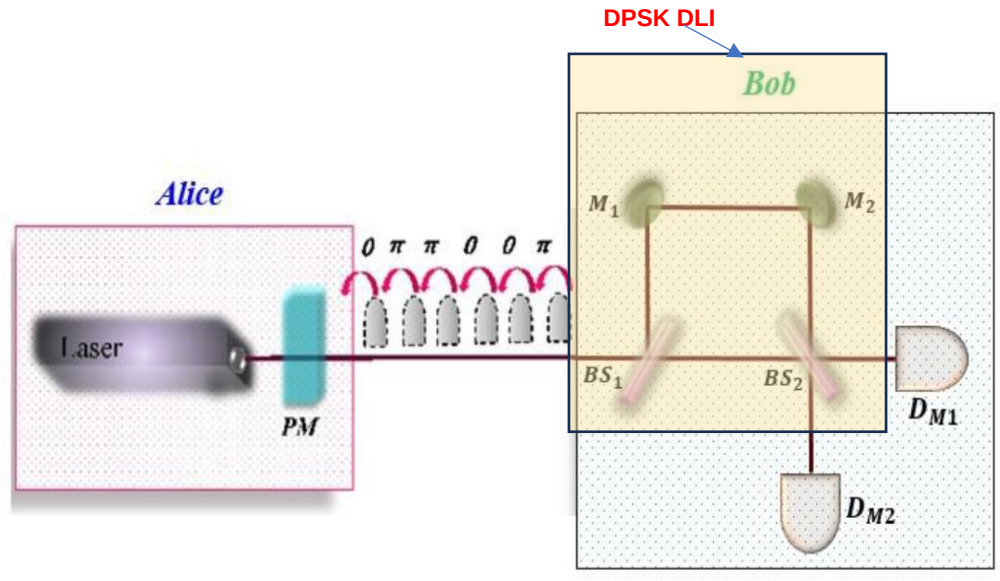

Figure 5.1, Illustration of DPS protocol. PM: phase modulator, BS1, BS2 are beamsplitters and M1, M2 are mirrors. Ref: https://arxiv.org/pdf/2401.00146.pdf

48500 Kato Road., Fremont, CA 94538
Tel: (510) 490-8320, Fax: (510) 490-8330
info@optoplex.com， www.optoplex.com

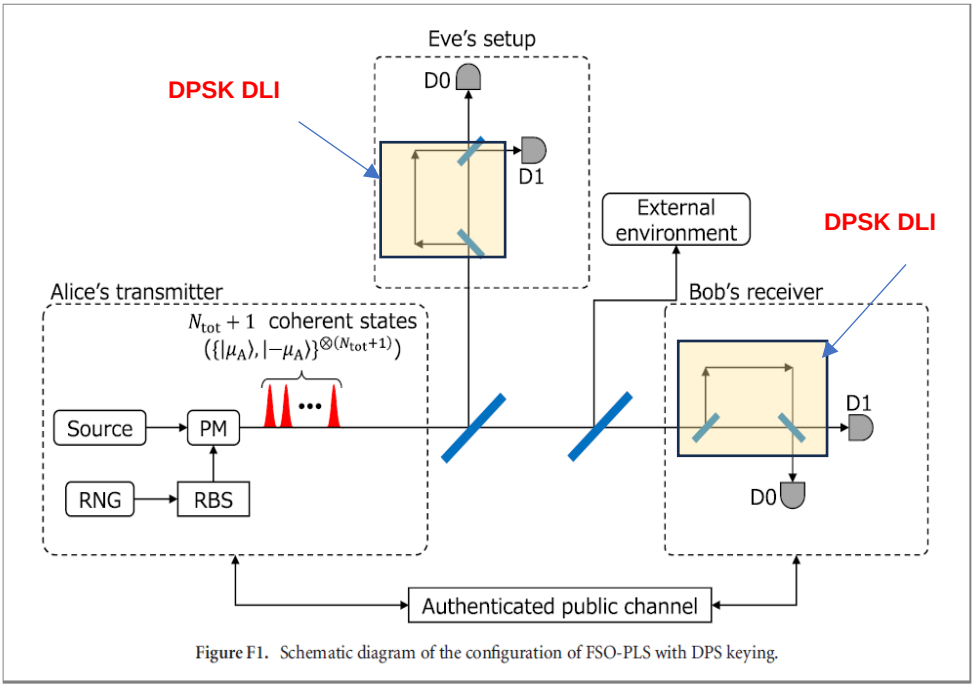

Figure 5.2, A schematic of DSP QKD protocol

Hiroyuki Endo et al 2022 New J. Phys. 24 025008

5.2 COW QKD

In COW QKD protocol, the encoding of a bit is done using a pair of empty and nonempty pulse. It was first introduced by Stuki et al. [b, c] and the steps involved in the protocol are as follows:

1. Alice prepares a sequence of pulses **|0⟩ |α⟩** (empty, non-empty), **|α⟩ |0⟩** (non-empty, empty) and **|α⟩ |α⟩** (non-empty, non-empty) ($|\alpha|^2 < 1$) corresponding to logical bit 1, 0 and decoy respectively using attenuated light source and intensity modulator with each logical bit having probability $(1-f)/2$ with the decoy occurring with probability f. Alice sends these pulse sequence to Bob via high quality optical fiber.

2. Bob receives the pulse sequence and measures the time of arrival of 90% photons on his detector D_B for the generation of sifted key while the rest 10% of photons are measured on the monitoring line for security purpose (refer to *Fig. 5.3*).

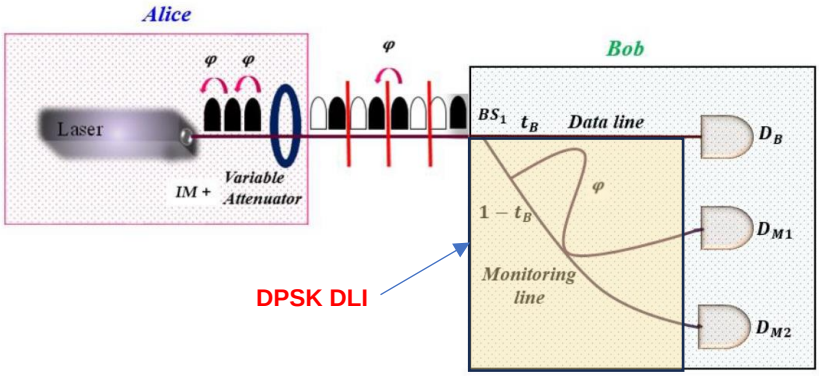

Figure 5.3, Illustration of COW protocol. IM: intensity modulator, BS1: beamsplitter
Ref: https://arxiv.org/pdf/2401.00146.pdf

48500 Kato Road., Fremont, CA 94538
Tel: (510) 490-8320, Fax: (510) 490-8330
info@optoplex.com， www.optoplex.com

3. Bob randomly checks the coherence between the non-empty pulses using the detector D_{M1} and D_{M2} in the monitoring line. Basically, the monitoring line is a Mach Zehnder interferometer arranged in such a manner that detector D_{M1} will click if there is no disturbance by Eve (refer *Fig.5.3*). Alice and Bob abort the protocol if the number of detections at D_{M2} is more than the threshold level.

4. Alice and Bob generate a shifted key from the pulses received from the data line. The shifted key undergoes through error correction and privacy amplification to get the private key which can be used for encryption and decryption.

DPR-QKD References

a) *Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. Differential phase shift quantum key distribution. Physical Review Letters, 89(3):037902, 2002*
b) *Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden. Fast and simple one-way quantum key distribution. Applied Physics Letters, 87(19):194108, 2005.*
c) *Damien Stucki, Claudio Barreiro, Sylvain Fasel, Jean-Daniel Gautier, Olivier Gay, Nicolas Gisin, Rob Thew, Yann Thoma, Patrick Trinkler, Fabien Vannel, et al. Continuous high speed coherent one-way quantum key distribution. Optics Express, 17(16):13326–13334, 2009.*

6. Optical Networks

Networks are commonly divided into three categories,

- local area networks (LAN);
- metropolitan area networks (MAN) and
- wide area networks (WAN).

The **LAN**, sometimes referred to as a campus area network, is a short distance network (usually <5 km) typically using a star/hub topology. For this type of network, mass produced hardware is deployed since low-cost is a significant consideration. Usually use 850nm optics:

- low-cost vertical cavity surface emitting lasers (VCSELs), and
- silicon-based avalanche photodiodes (APDs) , jitter response is ~100s ps
- QKD system clock rate can be >1Gbps
- A key rate of more than 1 Mbit/s over 4 km of standard telecom fiber achievable

MANs are geographically larger than LANs and usually cover a city area (<50 km). MANs are usually based on a ring or mesh network topology implemented with Wavelength Division Multiplexing (WDM) technology. Usually using 1310nm. In some cases, using 1550nm, or a combination of 1310 and 1550nm.

A **WAN**, sometimes called a core network or long-haul network, covers a broad area linking metropolitan areas and crossing national boundaries (e.g., several hundred km or longer). This type of network usually uses a mesh network topology and Dense WDM (DWDM) technology. Long distance and high throughput are the main requirements for this kind of network. Usually using 1550nm.

In general, the cost of the optics used in long-haul or WAN is much higher than that used in MAN and LAN. The LAN's is cheapest one.

48500 Kato Road., Fremont, CA 94538
Tel: (510) 490-8320, Fax: (510) 490-8330
info@optoplex.com， www.optoplex.com

7. Optoplex's Products used in QKD

Optoplex is leading technology and market leader with cutting-edge products for optical communications. It was the first company to introduce optical phase demodulators, such as DPSK, DQPSK, QPSK (90deg Hybrid) and DP-QPSK (aka polarization-diversified 90deg hybrids), and their integrations with balanced receivers for high-speed optical communications.

Optoplex's optical phase demodulators are based on athermal design of miniature free-space optics micro-inteferometer platforms (either Michaelson or Mach-Zehnder) with optical contact. The products feature high-performace (such as low insertion loss, polarization-independent, precisely matched optical skews) and excellent environmental stability. They have been employed globally in terrestrial, subsea and aerospace optical communication networks.

Recently, Optoplex has engineering-tailored those products for quantum communications – QKD. These products include

DPSK Optical Phase Demodulators (Delay Line-Interferometer, DLI)

- Mach-Zehnder DLI with Fixed FSR (delay): FSR = 1.0GHz, 1.25GHz, 2.5GHz, ….
- Variable Delay Line: 400ps ~ 1ns
- Custom-design available.

90deg Optical Hybrid Product Line

(free-space optics based, fiber-pigtail packaged)

- 90deg Optical Hybrids
- Phase-Tunable 90deg Optical Hybrids
- Polarization-Diversified 90deg Optical Hybrids (aka DP-QPSK Coherent Mixer)
- 90deg Optical Hybrid integrated with Balanced Receivers.
- Other related products

Visit Optoplex' website at: https://www.optoplex.com/ or check out at Optoplex's online catalogue at https://www.optoplex.com/download/Optoplex%20Product%20Catalogue_2022.pdf for more detail information. Contact Optoplex at sales@optoplex.com.