Chapter

Free-Space-Optical Quantum Key Distribution Systems: Challenges and Trends

Josue Aaron Lopez-Leyva, Ariana Talamantes-Alvarez, Miguel A. Ponce-Camacho, Edith Garcia-Cardenas and Eduardo Alvarez-Guzman

Abstract

Nowadays, high security levels are required to transmit critical information for government, private and personal sectors. As a countermeasure, the Quantum Key Distribution systems are the best option in order to protect this information because it provides unconditional security. In addition, increasing the transmission distance is a highlight. Therefore, the Free-Space Optical Quantum Key Distribution systems (FSO-QKD) present an innovative way for sharing secure information between two parties located at ground stations, spacecraft or aircraft. However, these scenarios present several challenges regarding the hardware, protocols and techniques used that must be solved in order to enhance the performance parameters (security level, distance link, final secret key rate, among others) for any QKD system; although, in particular, a high transmission performance is required for both the classical and quantum channels. These issues impose the roadmap and trends in the research, academic and manufacturing sectors around the world.

Keywords: performance parameters, secret key, challenges, trends, Quantum Key Distribution

1. Introduction

Currently, crucial information is shared between two parties located either near or far, in the quantum cryptographic context, the transmitter and receiver side are called Alice and Bob, respectively. Therefore, Alice transmits to Bob important information that requires a high secrecy level based on different kind of cryptography systems against a spy system called Eve. In particular, the most secure systems in the practice and theoretically secure are the Quantum Key Distribution (QKD) systems implemented on fiber optical networks and/or Free Space Optics (FSO) links using both Continuous-Variable (CV) and Discrete-Variable (DV) due to they are based on the physics laws [1]. In general, any QKD system requires on the Alice side different "subsystems" such as optical source, quantum state preparation (QSP), modulation scheme (Mod-Sch) and a Digital Processor & Communication (DP&Comm), among other possible subsystems that can improve the overall performance (**Figure 1**).
In particular, the optical source has some important physical and technical

requirements that affects the security level; these parameters are the linewidth, quantum optical state generated by the source, wavelength stability, among others. The QSP subsystem is probably the most important subsystem because it intends to prepare a true and well-knowledge quantum state that will be used for encoding the key, that is, to ensure the generation and fidelity features of the quantum state, although some QKD systems impose these requirements to an optimum optical source selection. Regarding the DP&Comm subsystem, many classical technologies are used for digital processing (e.g. central processing unit (CPU), graphical processing unit (GPU), field programmable gate array (FPGA)) in order to implement the algorithm for controlling Mod-Sch subsystem and perform a distillation algorithm for each particular protocol used in QKD systems. On the other hand, the DP&Comm also uses classical telecommunication techniques (e.g. Radio frequency, fiber optics link, FSO links, copper transmission lines) based on a classical and public transmission channel. In addition, the Mod-Sch subsystem uses the output signal of the QSP in order to modify some characteristics (e.g. polarization, amplitude, phase, among others) according to the driving output signal of the DP&Comm. After that, the quantum state that carries information is transmitted through a quantum private channel (fiber optics or free space). At the Bob's side, an optical receiver with support of many optical passive devices receives the quantum optical state and, thus, generates an electrical output signal that will be fed to a demodulation scheme (Demod-Sch). In this case, Bob also has a DP&Comm subsystem with the same characteristics and similar tasks in comparison with the used in Alice.

In addition, Quantum State Determination/Performance Parameters (QSP/PP) subsystem is used for: (a) determining the optical quantum state received by Bob based on optical tomography or calculating the density matrix, or, (b) measuring some important performance parameters of the quantum state received, such as amplitude, phase, polarization, among others, without reconstructing the phase representation state or the density matrix. There exist many subsystems that can improve the performance of QKD systems according to specific conditions, however, this chapter only mentions the most important ones based on authors opinion. On the other hand, Eve system also needs different subsystems in order to "listen" the information from Alice and Bob systems. Therefore, in order to reach the secure level imposed by the physical laws, high-end technology is required in each subsystem mentioned concerning hardware (i.e. subsystems mentioned), protocols, novel materials among others highlight topics [2].

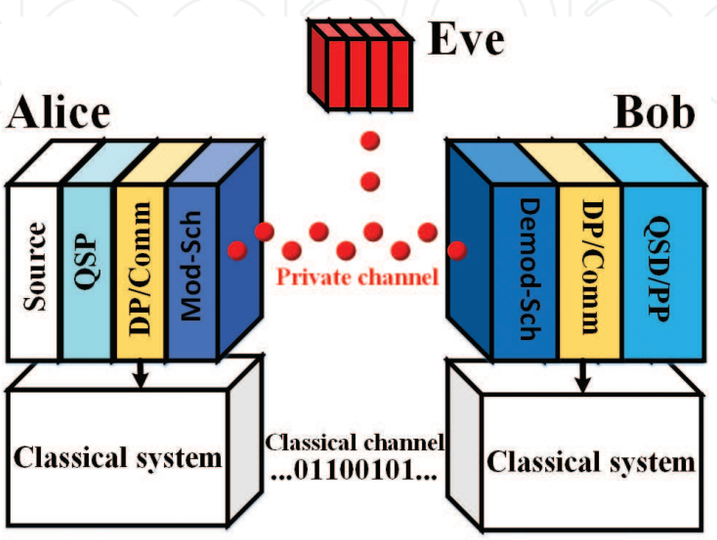

Figure 1.
General block diagram of QKD system emphasizing in the subsystems required for both quantum and classical channel.

Therefore, this chapter explains the state-of-art and actual challenges of each subsystem and devices used in QKD systems for both classical and quantum communications involved in this kind of secure systems. The aforementioned information can help to the reader to visualize and establish a general roadmap of the technologies used in QKD systems in order to focus institutional activities to research, development and innovation to contribute to the scientific and technical sector around the world. This chapter are organized as follows: Sections 2.1, 2.2 and 2.3 show the state-of-art regarding optical sources, optical detector and digital processing systems, respectively. Sections 2.1.1, 2.2.1 and 2.3.1 describe the actual challenges in each particular subsystem and the scientific and technological trends, emphasizing the FSO applications.

2. High-end hardware: challenges and trends

As mentioned above, although QKD systems are unconditionally secure based on laws of quantum mechanics, it is necessary to understand the technological limit of high-end hardware to increase the research, innovation and development activities in order to reach the theoretical performance of a QKD system step by step. In fact, technical limitations and imperfections in the hardware used gives Eve the opportunity to implement some Side-Channel-Attacks (among other attack kinds) based on the non-idealities.

2.1 Optical sources

The most desired optical source for the technical and scientific sector is the single-photon source or on-demand optical source which emit photons at any arbitrary time related to the transmission rate in a deterministic way (not probabilistic), that is, in an ideal case, 100% for emitted a certain photon and 0% for multiple-photons emitted, among others desired features. Thus, many optical sources intend to be a practical single-photon source based on faint laser pulse concept, however, it is not possible to ensure the amount of photons because the probabilistic analysis was made based on the Poisson distribution of the optical signal. On the other hand, there are other type of sources that try the same, but the difference relies in the theory and experiments used in order to generate a single photon. For example: (a) isolated quantum dot systems based on different material such as GaN, CdSe/ZnS, among others. However, these systems are not suitable for C-optical band (i.e. working from ≈340 nm to ≈950 nm) where the conventional telecommunication systems (and QKD systems) work and present a low emission efficiency (from ≈0.02 to ≈0.1) [3, 4]. Although it presents an important feature in single-photon sources, that is the deterministic resolving manner; (b) probabilistic single-photon sources based on Parametric Down-Conversion (PDC) and Four-Wave Mixing implemented in bulk crystals/waveguides and optical fiber, respectively. However, the principal issue is the reduced emission efficiency (from ≈ 0.1 to ≈ 0.85) although they are higher than the systems mentioned in (a). Obviously, this technical option is different compared to the ideal concept of a single-photon source that expects a perfect emission probability for a unique photon; and (c) faint laser is the most useful technique because it relaxes the design and complexity of the implementation of an experiment in both real and laboratory scenarios. This technique presents an emission efficiency of ≈1 and a wide inherent bandwidth suitable for the immersion of QKD systems in the real optical networks [4].

Thus, for all the optical sources mentioned, the efficiency and non-linear optical elements are an important issue for design and manufacturing. It is also important

to remember that the optical sources described have to be suitable for FSO links where a complete QKD system is implemented, that is, the restriction of single-photon is crucial for support the secure aspect inherent in QKD systems, however, the FSO links imposes trade-off that have to be analyzed. For this reason, the faint pulse is the common technique for FSO applications. Until now, the single-photon source information presented has been analyzed based on certain particular characteristics. However, an important aspect is the quantum state of the single photon generated by the optical source, that is, a photon can be generated with a particular quantum state (related to a quasi-probabilistic density functions) such as coherent, Fock, entanglement, among others. In fact, an ideal single-photon deterministic source should be generating a single photon with Fock distribution. On the other hand, an entanglement "single-photon" (probabilistic way) can be used in some short-distance-FSO-QKD systems and laboratory considering a high efficiency channel and finally, a single-photon source with coherent state (faint laser) is the most useful source and distribution used for long distance free space links.

2.1.1 Challenges and trends

In general, the challenges in the actual optical sources are regarding the band telecommunication of the device, inherent bandwidth, emission efficiency and output spatial mode. Therefore, the important advance imposes a clear trend based on efficient optical sources at common telecom wavelengths (i.e. C-band) [5]. Although sources at O-band are available [6]. Basically, the improved performance of the optical sources is based on the use of novel materials, structures and quantum devices that permits the near-ideal quantum state generation [7].

2.2 Optical detector

An ideal single-photon detector is useful in QKD systems in order to detect and resolve (determinate) an amount of photons per observation time (related to bit), that is, the detector is enabled to detect a single-photon and determine the exact quantity of a single-photon. However, this definition is based on the assumption of an ideal single-photon source. Obviously, ideal single-photon source and detector permits directly assure specific security levels based on the detection of an Eve system that disturbs the amount of photons transmitted by Alice. However, due to physical characteristics of the materials used on the manufacturing, there are deviations between the idealistic and realistic performance parameters. Thus, many realistic single-photon detectors have the ability of distinguish between zero photons per bit and more than zero photons, but they do not resolve the amount of photon. Based on the above, the most common used single-photon detectors are the non-photon-number-resolving detectors, that is, they have the ability of detecting photon but do not resolving the exact amount of photons. However, there are different modes of operation based on multiple detectors that allow improving the resolving process. Some examples about single-photon detector proposals are: (a) the Photo-Multiplier Tube (PMT) which is a classical single-photon detector that operates from the visible region to the infrared. However, the detection efficiency is considerably reduced, for example, at 500 nm the efficiency is 0.4, while for 1550 nm is 0.02; meaning a major problem for its application in some real optical networks; (b) Single-Photon Avalanche Photodiode (SPAP) category has a wide variety of technical options for detection process, having minimum and maximum efficiencies from 0.40 to 0.74 for 450–780 nm band, respectively (based on Silice). In both cases (i.e. a and b options), the wavelength range is not completely suitable for FSO communications systems, although some beacon systems can use these detectors with previous analysis.

Therefore, SPAP based on InGaAs material is suitable for 1060–1550 nm range with maximum efficiency of ≈0.33 for 1060 nm and ≈0.10 at 1550 nm. Regarding the high-end technology, the superconducting Transition Edge Sensor (TES) is the best option for detecting in FSO-QKD system context based on the detection efficiency-wavelength relationship, that is, efficiency of ≈0.95 at 1556 nm. However, the operation temperature is extremely low, ≈0.1°K, whereas the last mentioned detectors work commonly from 240 to 300°K, although there are some exceptions [4].

2.2.1 Challenges and trends

The principal challenges are related to minimizing the electronic noise and maximizing the gain of the detector maintaining high transmission rates [8, 9]. To do the aforementioned, novel materials and electrical designs are required. In particular, reducing the Noise Equivalent Power (NEP) parameter permits the detection of low optical power with different electrical bandwidth [10]. However, although novel optical detectors have been developed, coherent detection techniques have been helps at Bob side, relaxing the detector selection due to inherent amplification and spectrum filtering of the coherent technique.

2.3 Digital processing systems

The DP&Comm subsystem implemented in conventional QKD systems performs particular basic tasks such as: driver for different devices (e.g. phase and amplitude modulators, true random number generator (TRNG), etc.), quantum key data base, perform the algorithm need to distillation, reconciliation and privacy amplification processes between Alice and Bob. In particular, this algorithm requires access to both quantum and classical channels. Therefore, the DP&Comm requires some important technical specifications so as not to degrade the secure level and secrete key rate of the QKD systems. In particular, Field Programmable Gate Arrays (FPGA) have been used in a real-time QKD systems reaching secret key rate at 17 kb/s in an optical fiber link of 20 Km [11]. It is clear that, the FPGA specifications impact the performance of a QKD systems, therefore, improved synchronization and jitter methods based on high speed and precision devices can reduce the Quantum Bit Error Rate (QBER) and increase the final secret key rate [12].

In addition, the secret key rate has an important relation with the performance of the TRNG subsystems, thus, FPGAs have been used for generation and acquisition of true random digital sequences reaching 1.25 Gb/s [13]. An important issue in DP&Comm subsystems is the ability to adapt and generate countermeasures to maintain or improve the specific performance against external dynamic factors such as atmospheric turbulence in FSO links, resizing and adaptive parameters based on an optimization process [14, 15]. In addition, some QKD systems use a Graphics Processing Unit (GPU) as a DP&Comm (although some considerations have to be analyzed to complete all the task of the DP&Comm) because it provides some important technical features such as parallel computing and processing floating-point information allowing rates of 1.35 Gb/s [16]. The novel standalone modules for particular stages of the protocol used (e.g. sifting, error correction, and privacy amplification modules) also support the performance of QKD systems, which are based on high-end electronic design. These particular technical innovations in specific modules permits reaching secret key rate of ≈13.72 Mb/s [17].

2.3.1 Challenges and trends

Thus, the DP&Comm subsystem depends on the electronic development regarding the high performance related to speed processing and the novel design

of Printed Circuit Board (PCB) used in different subsystems within DP&Comm. Among the devices that need to be improved are high-end converters (Digital-to-Analog-Converter and Analog-to-Digital-Converter), fast output/input ports (e.g. analog and digital) and fast memories. On the other hand, an optimized QKD protocol have to be programmed in DP&Comm subsystems, which includes different algorithms needed in different protocol stages, that is, detecting-correcting errors codes, performing some Hash functions among other used. Therefore, no matter the high-end devices used in the DP&Comm subsystem, the designer should try to reduce the trade-off based on optimized programming.

In addition, Commercial Off-The-Shelf (COTS) devices have been used for QKD-FSO systems using an optimized protocol to not degrade the security level and secret key rate [18]. **Figures 2** and 3 show the Alice and Bob set-up, respectively. Both systems use COTS devices in a Local Area Network (LNA). In particular, Alice set up (**Figure 2**) consists of an optical source in order to generate a LO and a data signal (the way to divide the optical signal is not graphically clear expressed, but 1X2 fiber splitters were used), the LO signal will be sent to Bob separately in order to perform a self-homodyne detection. In addition, a minimum optical signal is used for the TRNG to generate two random digital sequences (RSA1 and RSA2). These sequences are used by a COTS device that uses a DB-RN in order to drive the PM and perform the quantum protocol using both classical and quantum channels. The PC and PBS are used in order to maintain and ensure a vertical SOP in the incoming PM signal because in order to avoid a residual amplitude modulation. Since the optical source is non-polarized and it has an optical fiber output, a PC is used as the first element for polarization controlling, but because Alice and Bob have to be implemented in free space, a PBS was added in order to ensure the SOP. However, the PC can be deleted if an optical source with free space coupling and linear vertical polarization is used. Thus, residual amplitude modulation can affect the overall performance of the QKD systems. Next, phase modulation is used to encrypt the information and a half-wave plate to produce a linear SOP at 45 degrees needed for Bob set-up. Because the optical source generates a coherent state, an attenuator is used to produce a weak coherent state emulating a long distance free-space link. Before the optical signal is transmitted through the free space channel, a BS and PD are used for monitoring the optical power corresponding to the weak coherent state.

At the Bob side (**Figure 3**), a free space optical hybrid (π-hybrid) based on BS, PBS and BHDs is used in order to measure simultaneously both quadrature components of the weak coherent stated received. Mirrors and attenuators are used in order to calibrate the optical power received in each photodetector (implemented in each BHDs) due to the different optical paths. In particular, a quarter-wave plate

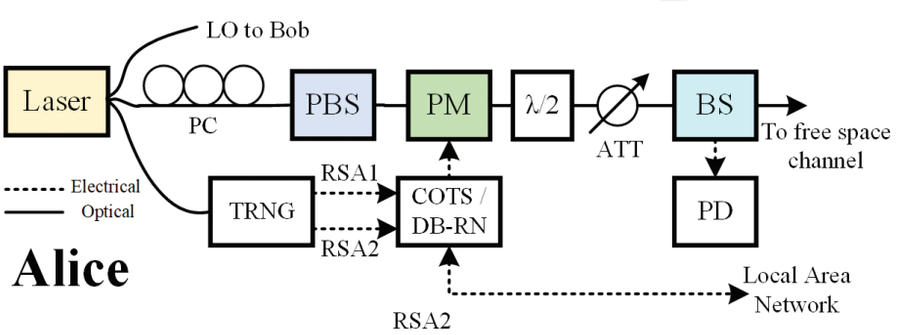

Figure 2.
Alice set-up. PBS, polarized beam splitter; TRNG, true random number generator; PM, phase modulator; DB-RN, database-random number; BS, beam splitter; ATT, attenuator; PD, photodetector; RSA, random sequence in Alice; PC, polarization controller; λ/2, half-wave plate; LO, local oscillator. Own figure and presented in [18].

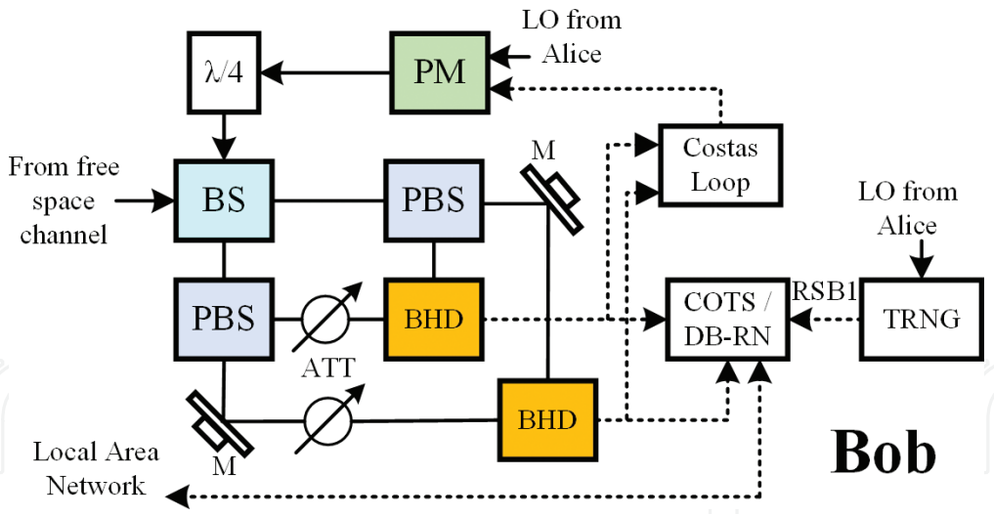

Figure 3.
Bob set-up. M, mirror; BHD, balanced homodyne detector; λ/4, quarter-wave plate; RSB, random sequence in bob. Own figure and presented in [18].

is used to change the SOP of the LO, that is, the LO needs a circular SOP in order to allow simultaneous measurements. Therefore, the complete Bob scheme is based on coherent detection technique, where an opto-electronic Costal loop permits the improvement of the complete performance reducing the phase noise due to different optical paths. Particularly, a COTS device and TRNG (it generates other random digital sequence, RSB1) are used in a similar way as Alice in order to perform the quantum protocol. The quantum transmitter-receiver shows an experimental average Quantum Bit Error Rate (QBER) of 30% using auto-homodyne detection with 0.25 photons per bit in locking phase mode. The final secret key rate measurements were 20 and 40 Kbps for minimum and maximum throughput in the LAN. Finally, although common elements (i.e. passive and active optical elements) are used in **Figures 2** and **3**, the important aspect is the uses of COTS devices in QKD systems that allow relaxing some design parameters maintain adequate performance parameters as mentioned (e.g. QBER, final secret key rate).

3. QKD protocols: challenges and trends

The research on the protocols used for the distribution of the cryptographic key based on the principles of quantum mechanics had a great boom in the last 10 years. In general, the QKD protocols describe the particular tasks or steps (i.e. algorithm) needed in order to generate a final quantum secret key rate. Although the QKD protocols are programmed in a DP&Comm subsystem, they require all the subsystems. In particular, the protocols and their performance depend on the statistical information (discrete and continuous variables, DV and CV, respectively) regarding the quantum state used.

The BB84 protocol is the first protocol proposed to guarantee unconditional security (because it is based on orthogonal states) when transmitting the cryptographic key that gives access to the information of a message. It has been considered as the ideal protocol, at least in theory, since it is based on the transmission of the quantum state of a single photon to represent a bit of information and provide immediate information through the characteristics of the received signal, about a possible attack by a spy [19]. In addition, if we add that the key is used in a single occasion (One Time Pad) it provides better protection in case that at some point an intruder manages to obtain the key. Next, B92 protocol was proposed based on BB84 protocol.

While BB84 protocol uses 4 orthogonal states, B92 only uses 2 non-orthogonal states. Therefore, the different quantum states (i.e. orthogonal and non-orthogonal) used in BB84 and B92 protocols impose a trade-off regarding the final secret key rate generated by Alice, Bob and the attacks performed by Eve [20]. Since the BB84 protocol is extremely vulnerable to Photon Number Splitting attacks, the SARG04 protocol was proposed, which uses 4 non-orthogonal quantum states; however, the final secret key rate is also affected [21]. Additionally, there exists the E91 protocol based on Einstein, Podolsky and Rosen (EPR) paradox that uses entangled quantum states generated either by Alice, Bob or a trusted third party [22]. Later, the BBM92 protocol was proposed which implies EPR pairs, that is, entangled photon pairs. This protocol can be described as the BB84-EPR protocol [23]. Until now, the protocols mentioned are based on State of Polarization (SOP), DV framework and general stages such as: raw key exchange, key sifting and privacy amplification, that is, all the protocols have the same stages in order to generate the final quantum key. On the other hand, QKD protocols based on CV variables are also suitable, such as COW protocol (Coherent One-Way), which is based on an amplitude encoded sequence of weak coherent pulse with the same phase for each particular time slot. In particular, different time slots have several optical pulses (related to an optical power average) and, occasionally, decoy sequences are sent in order to hinder the eavesdropped process [24]. Due to the different quantum states and encoding scheme used, this protocol is so-called distributed-phase-reference (DPR), in fact, there are many protocols in the same category such as the differential-phase-shift (DPS), which uses different phases but the amplitude remains constant. Therefore, interferometric techniques are required in the receiver [25]. All the DPR protocols perform joint measurements on subsequent signals. Actually, GG02 protocol is present in many commercial equipment. In general, this protocol is based on random distributions of coherent or squeezed states and modulates either the phase or amplitude of a quantum state and uses coherent detection in Bob's side [26]. Finally, each protocol mentioned has a particular security principle, be it the Heisenberg uncertainty or quantum entanglement. Although there exist novel protocols that change the security principle in order to improve the performance of particular QKD systems.

3.1 Challenges and trends

The challenges present in the QKD protocols are related with the performance parameters of the QKD systems. In particular, although each protocol uses different security principle and quantum states, the important issues are increasing the security level, secret key rate and distance link between Alice and Bob in presence of Eve system. In fact, while a particular protocol presents a high security level and particular secret key rate for short distance links, other protocol presents the same security level and secret key rate for long distance links. However, as was mentioned, a QKD protocol requires the other subsystems, thus, a hypothetically complicated protocol imposes a strict and detailed design, that is, the experimental set-up is not simple. Therefore, the tendency of the protocols refers to proposing novel QKD protocols that allow to easily implement them in optical commercial networks, while the performance parameters remain constant or improved. In addition, a high dimension protocol is proposed in order to increase the photon information capacity when the photon rate is restrained. This protocol is based on entangled photon pairs that allow information to be transmitted using an extremely large alphabet [27].

Now, each QKD protocol has been theoretically described, however, free space and atmospheric channels impose important trade-off that determines the suitable protocol. In particular, BB84 protocol has been optimized for FSO links affected by atmospheric turbulence improving the secret key rate up to over 20% [28].

However, BB84 protocol remains unchanged while other subsystems are modified. In fact, many QKD protocols have been implemented in FSO links in order to demonstrate their performance under particular conditions.

4. Techniques and structure in QKD: challenges and trends

The techniques and structures used in QKD context involve the different set-ups, operation rules and devices that perform a particular protocol. Therefore, the first step is choosing the quantum protocol and next, the general structure can be proposed and implemented. In particular, the structure consists of optical source, optical detector, digital processing unit (the challenges and trends that have already been mentioned) among other specific devices connected together in order to perform a complete QKD system. On the other hand, the techniques are the novel operational rules in order to enhance the complete performance of the QKD system. Each protocol mentioned was proofed, first, using a particular technique and structure, these can be can be found and analyzed in the references listed. However, many improves to each protocol have been proposed for QKD systems implemented in FSO.

For example, the atmospheric turbulence is an important problem for QKD systems based on FSO links. In order to mitigate the degraded performance of the secret key rate for QKD systems based on BB84 protocol, an optimization technique was proposed based on an adaptive optical power transmission considering the random irradiance fluctuation [28]. In the same context, a novel encoder technique was proposed for the classical channel in QKD-FSO systems based on adaptively encoder gain according to atmospheric turbulence levels [29], The results show that the secret key rate remains constant for a region of turbulence levels and imposes the need of a high-end DP&Comm subsystem in order to extend the operating region. In addition, many structures and techniques used in conventional classical optical communication systems have been adapted to QKD-FSO systems. In particular, Multi-Input-Multi-Output (MIMO) and Wavelength Division Multiplexing (WDM) are suitable options used in order to increase the capacity of free space channel based on Orthogonal Angular Momentum (OAM) modulation [30]. Among the structures and techniques necessary to implement a QKD-FSO system are the subsystems used in order to pointing, acquisition and tracking the two parties (Alice and Bob, represented by satellites and ground stations). In this case, pointing systems used in satellites have reached from 0.6 μrad to 3 μrad pointing capability [31, 32].

4.1 Challenges and trends

In general, the structures and techniques allow to improve the performance of a QKD-FSO system. Therefore, the design of techniques and high-end structures allows to support in a better way the actual QKD system proposals. In fact, the principal challenges are related with the optimization and improving of the secondary subsystems of a QKD-FSO systems (i.e. secondary subsystems are not mentioned in detail in this chapter, such as telescope, mechanical structures, access multiplexing techniques, among others). Finally, the QKD-FSO system trends related with the structures and techniques are: maximize the channel capacity, increase the distance link and secret key rate, increase the power consumption efficiency in order to support long-time missions, improve the thermal control and isolation, among others.

In addition, novel encoding technique for classical channel has been proposed in order to increase the secret key rate at QKD-FSO links. **Figure 4** shows a diagram proposed based on an adaptive LDPC (Low-Density Parity-Check Codes) encoder in order to countermeasure the effect caused by the dynamical atmospheric turbulence [29].

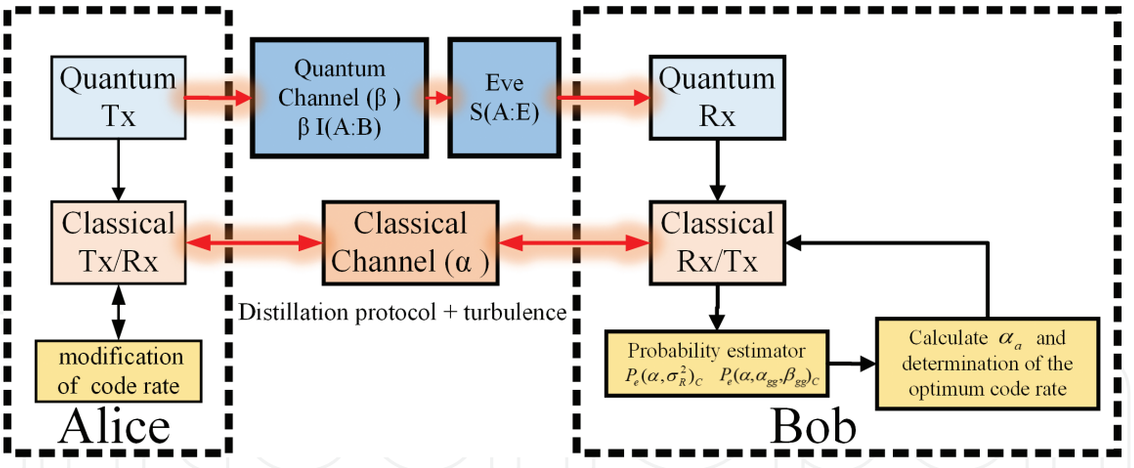

Figure 4.
Block diagram of the simulation-experimental set-up of the QKD system proposed with dynamical encoder for different atmospheric turbulence levels. Own figure and presented in [29].

Here, $I(A{:}B)$ is the mutual information that Alice and Bob shared, and the maximum information shared for Alice and Eve is $S(A{:}E)$. In this case, β_{gg} is the reconciliation efficiency. In other hand, α is the classical channel efficiency that is based on the encoder capacity (related to the amount the erroneous bits that are detected and corrected). In this scenario, the dynamical atmospheric turbulence is represented by Rayleigh or Gamma-Gamma (GG) density probability functions, $P_e(\alpha,\sigma_R^2)_c$ and $P_e(\alpha,\alpha_{gg},\beta_{gg})_c$, respectively, where σ_R^2 represents the Rytov variance related with the atmospheric turbulence, α_{gg} and β_{gg} are the effective numbers of large-scale and small-scale for GG function, respectively. Basically, Alice and Bob monitored the dynamical atmospheric turbulence calculating the error probabilities and modifying LDPC encoder capacity used by them.

5. Conclusions

The proper understanding of the high-end hardware, protocols, techniques and schemes used in FSO-QKD systems allow to improve the performance parameters such as secret key rate, distance link, security level, among others. In particular, although there are wide suitable options for the subsystems required for FSO-QKD systems, it is necessary that the high-end subsystems are more accessible and compact in order to increase their uses in traditional optical networks.

Acknowledgements

Many thanks to CETYS University for the administrative and technical support in the development of diverse projects related to the subject mentioned in this chapter. In addition, thanks to the Center of Innovation and Design (CEID) of Baja California for the important discussion on improving quality of the chapter.

DOI: http://dx.doi.org/10.5772/intechopen.81032

Author details

Josue Aaron Lopez-Leyva[1*], Ariana Talamantes-Alvarez[1], Miguel A. Ponce-Camacho[1], Edith Garcia-Cardenas[2] and Eduardo Alvarez-Guzman[3]

1 CETYS University, Baja California, Mexico

2 IBERO University, Baja California, Mexico

3 Autonomous University of Baja California, Baja California, Mexico

*Address all correspondence to: josue.lopez@cetys.mx

References

[1] Qu Z, Djordjevic IB. High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing. Optics Express. 2017;**25**:7919-7928. DOI: 10.1364/OE.25.007919

[2] Diamanti E, Lo H-K, Qi B, Yuan Z. Practical challenges in quantum key distribution. npj Quantum Information. 2016;**2**:1-12. DOI: 10.1038/npjqi.2016.25

[3] Schlehahn A, Fischbach S, Schmidt R, Kaganskiy A, Strittmatter A, Rodt S, et al. A stand-alone fiber-coupled single-photon source. Scientific Reports. 2018;**8**:1-7. DOI: 10.1038/s41598-017-19049-4

[4] Eisaman MD, Fan J, Migdall A, Polyakov SV. Invited review article: Single-photon sources and detectors. Review of Scientific Instruments. 2011;**82**:1-26. DOI: 10.1063/1.3610677

[5] Haffouz S, Zeuner KD, Dalacu D, Poole PJ, Lapointe J, Poitras D, et al. Bright single InAsP quantum dots at telecom wavelengths in position-controlled InP nanowires: The role of the photonic waveguide. Nano Letters. 2018;**18**:3047-3052. DOI: 10.1021/acs.nanolett.8b00550

[6] Dusanowski L, Holewa P, Maryński A, Musiał A, Heuser T, Srocka N, et al. Triggered high-purity telecom-wavelength single-photon generation from p-shell-driven InGaAs/GaAs quantum dot. Optics Express. 2017;**25**:31122-31129. DOI: 10.1364/OE.25.031122

[7] Heindel T, Rodt S, Reitzenstein S. Single-photon sources based on deterministic quantum-dot microlenses. In: Michler P, editor. Quantum Dots for Quantum Information Technologies. Springer; 2017. pp. 199-228. DOI: 10.1007/978-3-319-56378-7

[8] Abdulwahid OS, Sexton J, Kostakis I, Ian K, Missous M. Physical modelling and experimental characterisation of InAlAs/InGaAs avalanche photodiode for 10 Gb/s data rates and higher. IET Optoelectronics. 2018;**12**:5-10. DOI: 10.1049/iet-opt.2017.0068

[9] Tossoun B, Stephens R, Wang Y, Addamane S, Balakrishnan G, Holmes A, et al. High-speed InP-based p-i-n photodiodes with InGaAs/GaAsSb type-II quantum wells. Photonics Technology Letters. 2018;**30**:399-402. DOI: 10.1109/LPT.2018.2793663

[10] Jiang X, Itzler M, O'Donnell K, Entwistle M, Owens M, Slomkowski K, et al. InP-based single-photon detectors and Geiger-mode APD arrays for quantum communications applications. Journal of Selected Topics in Quantum Electronics. 2015;**21**:3800112. DOI: 10.1109/JSTQE.2014.2358685

[11] Zhang H-F, Wang J, Cui K, Luo C-L, Lin S-Z, Zhou L, et al. A real-time QKD system based on FPGA. Journal of Lightwave Technology. 2012;**30**:3226-3234. DOI: 10.1109/JLT.2012.2217394

[12] Shen Q, Liao S, Liu S, Wang J, Liu W, Peng C, et al. An FPGA-based TDC for free space quantum key distribution. Transactions on Nuclear Science. 2013;**60**:3570-3577. DOI: 10.1109/TNS.2013.2280169

[13] Martin A, Sanguinetti B, Wen Lim CC, Houlmann R, Zbinden H. Quantum random number generation for 1.25-GHz quantum key distribution systems. Journal of Lightwave Technology. 2015;**33**:2855-2859. DOI: 10.1109/JLT.2015.2416914

[14] Yang S-S, Bai Z-L, Wang X-Y, Li Y-M. FPGA-based implementation of size-adaptive privacy amplification in quantum key distribution. Photonics

Journal. 2017;**9**:1-8. DOI: 10.1109/JPHOT.2017.2761807

[15] Yan Z, Meyer-Scott E, Bourgoin J-P, Higgins B-L, Gigov N, Mac Donald A, et al. Novel high-speed polarization source for decoy-state BB84 quantum key distribution over free space and satellite links. Lightwave Technology. 2013;**31**:1399-1408. DOI: 10.1109/JLT.2013.2249040

[16] Wang X, Zhang Y, Yu S, Guo H. High-speed implementation of length-compatible privacy amplification in continuous-variable quantum key distribution. Photonics Journal. 2018;**10**:1-9. DOI: 10.1109/JPHOT.2018.2824316

[17] Yuan Z, Plews A, Takahashi R, Doi K, Tam W, Sharpe A, et al. 10-Mb/s quantum key distribution. Journal of Lightwave Technology. 2018;**36**:3427-3433. DOI: 10.1109/JLT.2018.2843136

[18] Lopez-Leyva JA, Ruiz-Higuera J, Arvizu-Mondragon A, Santos-Aguilar J, Ramos-Garcia R, Ponce-Camacho M. High performance quantum key distribution prototype system using a commercial off-the-shelf solution: Experimental and emulation demonstrations. Optica Applicata. 2017;**XLVII**:411-419. DOI: 10.5277/oa170307

[19] Bennet CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science. 2014;**560**:7-11. DOI: 10.1016/j.tcs.2014.05.025

[20] Bennett CH. Quantum cryptography using any two non-orthogonal states. Physical Review Letters. 1992;**68**:3121-3124. DOI: 10.1103/PhysRevLett.68.3121

[21] Scarani V, Acín A, Ribordy G, Gisin N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical Review Letters. 2004;**92**:057901. DOI: 10.1103/PhysRevLett.92.057901

[22] Artur E. Quantum cryptography based on Bell's theorem. Physical Review Letters. 1991;**67**:661-663. DOI: 10.1103/PhysRevLett.67.661

[23] Bennett CH, Brassard G, Mermin ND. Quantum cryptography without Bell's theorem. Physical Review Letters. 1992;**68**:557-559. DOI: 10.1103/PhysRevLett.68.557

[24] Stucki D, Brunner N, Gisin N, Scarani V, Zbinden H. Fast and simple one-way quantum key distribution. Applied Physics Letters. 2005;**87**:194108. DOI: 10.1063/1.2126792

[25] Inoue K, Waks E, Yamamoto Y. Differential-phase-shift quantum key distribution using coherent light. Physical Review A. 2003;**68**:022317. DOI: 10.1103/PhysRevA.68.022317

[26] Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Physical Review Letters. 2002;**88**:057902. DOI: 10.1103/PhysRevLett.88.057902

[27] Bechmann-Pasquinucci H, Tittel W. Quantum cryptography using larger alphabets. Physical Review A. 2000;**61**:062308. DOI: 10.1103/PhysRevA.61.062308

[28] Sun X, Djordjevic IB, Neifeld MA. Secret key rates and optimization of BB84 and decoy state protocols over time-varying free-space optical channels. Photonics Journal. 2016;**8**:7904713. DOI: 10.1109/JPHOT.2016.2570000

[29] Lopez-Leyva JA, Arvizu-Mondragon A, Santos-Aguilar J, Ramos-Garcia R. Improved performance of the cryptographic key distillation protocol of an FSO/CV-QKD system on

a turbulent channel using an adaptive LDPC encoder. Revista Mexicana de Fisica. 2017;**63**:268-274

[30] Cvijetic M, Takashima Y. Beyond 1Mb/s free-space optical quantum key distribution. In: Proceedings of the IEEE International Conference on Transparent Optical Networks (ICTON'14). Graz, Austria: IEEE; 6-10 July 2014. pp. 1-4

[31] Yin J et al. Satellite-based entanglement distribution over 1200 kilometers. Science. 2017;**356**:1140-1144. DOI: 10.1126/science.aan3211

[32] Oi DKL et al. Cube Sat quantum communications mission. EPJ Quantum Technology. 2017;**4**:1-20. DOI: I 10.1140/epjqt/s40507-017-0060-1