TeraXion

An indie Semiconductor Company

ARTICLE

Quantum Key Distribution in Optical Communications

Authors: Guillaume Brochu[1], Marc-André Laliberté[2]

1. Scientist, TeraXion
2. Product Line Manager, Optical Communications, TeraXion.

Overcoming QKD Engineering Challenges

Quantum Key Distribution (QKD) in quantum communications is a secure communication method that enables two parties to produce shared secret keys used afterward to encrypt and decrypt messages. Based on the principles of quantum mechanics, the process of measuring a quantum system introduces detectable anomalies, allowing for the detection of an eavesdropper.

As the government, banking, medical, and other regulated industries work through digital transformation, QKD is an important tool in improving secure communications over fiber optic networks by strengthening the classical encryption of internet traffic and other communication channels. Indeed, worldwide massive research and development efforts on quantum computers and their theoretical capacity to break classical encryption algorithms are a real threat to our sensitive data protected by such algorithms, which can be stored at the time of transmission and decrypted later.

Many of the global communications market leaders are investing in research and development for quantum communications systems. Early pioneers approached QKD with a Prepare-and-measure distribution scheme using protocols such as BB84, or its related variants. They are methods of securely communicating a private key from one party to another in a dedicated quantum channel by exploiting the superposition principle using photons [1-5]. Another scheme instead relies on quantum entanglement where one encodes keys in pairs of entangled photons split between both parties (protocols such as E91 or BBM92) [6,7].

Research in QKD and other quantum technologies is quickly ramping up worldwide, and new approaches for QKD are now being considered. These newer systems use protocols such as twin field QKD (TF-QKD) with low noise lasers locked with phase lock loops, or continuous variables QKD (CV-QKD) schemes that typically requires narrow linewidth and low noise lasers [8,9].

QKD with attenuated pulses

Systems based on Prepare-and-measure QKD schemes are the most common in today's practical implementations and, despite recent research still proposing unique system designs, they do share some common basics.

In every schema, Alice sends pulses of polarized photons attenuated to the quasi single-photon level to Bob as Eve, the eavesdropper, tries to intercept it to retrieve information about the secret key. A simplified description of the required optical fiber system for QKD using attenuated pulses is shown in Figure 1.

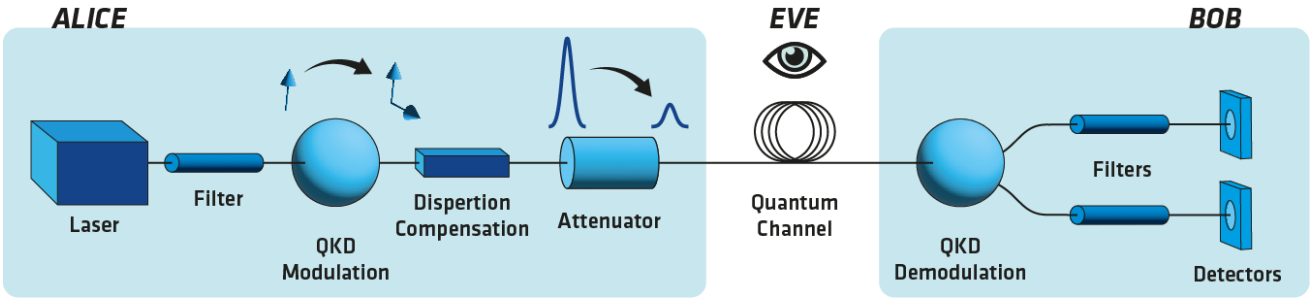

Figure 1. Simplified description of a fiber-based attenuated pulses QKD system.

A single mode laser is modulated to produce a pulse train that is then multiplexed in polarization. The qubits (or quantum bits, the basic unit of quantum information) of the secret key are encoded in the phase and polarization state of the pulses. Before leaving the transmitter box on Alice side, the modulated pulse train is strongly attenuated to bring it to the quasi-single photon level, so if Eve tries to tap some of the pulses, they would not be recoverable by Bob and thus not used to build the secret key. On the receiver side (Bob), the QKD demodulator processes the received signal that is sent to two single photon detectors.

QKD Components Boost Performance

QKD modulation and demodulation typically requires asymmetric Mach-Zehnder interferometers, phase modulators, polarization splitters and combiners, and quantum random number generators. Also, optical components like dispersion compensators and spectral filters are sometimes needed to improve system performance. One should note that the actual QKD protocol and the associated optical sub-systems are more complicated than this simplistic description (Fig.1), used to illustrate the role and importance of optical components, such as dispersion compensators, narrow broadband filters and low noise lasers.

Reducing excess loss is of prime importance on the quantum channel and in the receiver box on the Bob side, as any lost photon must, according to the QKD protocol, be considered as if it was measured by Eve, reducing the transmission rate of usable secure keys.

Chromatic Dispersion Compensation

At the quantum level, chromatic dispersion broadens the statistical distribution of arrival time of the photons at the detectors. If there is too much chromatic dispersion, photons may miss the detection time window, an anomaly that will disrupt the transfer of the secret keys similar to optical loss. Therefore, when increasing fiber span lengths for the quantum channel, the detrimental effect of optical loss and dispersion adds up. A chromatic dispersion compensator is typically needed for distances over 50 km. The dispersion compensator is generally inserted before the attenuator in the transmitter box on the Alice side.

Narrow Broadband Filters

In addition to loss and dispersion, non-linear scattering of photons from the adjacent regular channel, for example, when the quantum channel is in the same fiber as the dense wavelength-division multiplexing (DWDM) traffic at higher optical power, as well as other noise sources like the spontaneous emission from the laser, can cause false detections on the single photon detectors. As rejection of typical DWDM demultiplexers is often not sufficient, high-rejection, narrowband, low-loss filters may be required just before the single photon detectors or elsewhere in the optical setup.

TeraXion solutions for QKD

Over the years, TeraXion has developed several qualified products and technologies that could address current and future challenges of QKD systems manufacturers:

Low-loss dispersion compensators

TeraXion's ClearSpectrum™ DCML addresses chromatic dispersion with full C-band coverage to improve QKD signals over long distances. With an insertion loss lower than 3 dB for distances up to 200km with a single module, these compensators also prevent intrachannel and interchannel nonlinear impairments and have negligible latency.

Narrow bandpass filters

TFN and static filters advanced optical filtering solutions reduce the detrimental effect of non-linear scattering and other sources of optical noise in the QKD system. QKD using attenuated pulses typically requires passband filters with high spectral isolation and a bandwidth of about 2-20 GHz that is determined by the pulse repetition rate. Depending on the required bandwidth and other application challenges, a frequency-tunable or an athermal package could be used to boost filter performance and stabilize its center wavelength. This is particularly critical when encoding quantum information in the frequency sidebands of an attenuated coherent state.

Ultranarrow bandpass filters

With bandwidth from 50 MHz to 500 MHz, TeraXion's UNF filters are well-suited to QKD systems using entangled photons source. For example, they can be used to optimize bandwidth following the spontaneous parametric down-conversion process (SPDC).

Low noise lasers

Optical sensing components like TeraXion's PureSpectrum™ lasers offer precision feedback monitoring, ultra-low-noise performance (linewidth down to 20 kHz), and superior wavelength stability.

Off-the-shelf components help reduce demonstration costs and advance the systems to the point of commercialization. TeraXion looks to partner with system manufacturers to evolve the technology together. TeraXion's family of quantum communications components support the advancement of quantum technologies, from R&D to full commercialization.

Whether using single-photon sources, attenuated pulses, entangled photons, CV-QKD, twin field QKD, or a novel approach, our engineers are happy to discuss your system challenges.

Bibliography

[1] YUAN, Z. L., DIXON, A. R., DYNES, J. F., et al. Gigahertz quantum key distribution with InGaAs avalanche photodiodes. Applied Physics Letters, 2008, vol. 92, no 20, p. 201104 https://doi.org/10.1063/1.2931070

[2] ERAERDS P., WALENTA N., LEGRÉ M., et al. Quantum key distribution and 1 Gbps data encryption over a single fibre. New Journal of Physics, 2010, vol. 12, no 6, p. 063027 https://doi.org/10.1088/1367-2630/12/6/063027

[3] BOARON A., BOSO G., RUSCA D., et al. Secure quantum key distribution over 421 km of optical fiber. Physical review letters, 2018, vol. 121, no 19, p. 190502 https://doi.org/10.1103/PhysRevLett.121.190502

[4] MLEJNEK, Michal, KALITEEVSKIY, Nikolay A., et NOLAN, Daniel A. Modeling high quantum bit rate QKD systems over optical fiber. In : Quantum Technologies 2018. SPIE, 2018. p. 122-131 https://doi.org/10.1117/12.2306875

[5] CHEN, Yu-Ao, ZHANG, Qiang, CHEN, Teng-Yun, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature, 2021, vol. 589, no 7841, p. 214-219 https://doi.org/10.1038/s41586-020-03093-8

[6] TITTEL W., Brendel J., Zbinden H., and Gisin N. Quantum Cryptography Using Entangled Photons in Energy-Time Bell States. Physical Review Letters, 2000, vol. 84, pp. 4737 https://doi.org/10.1103/PhysRevLett.84.4737

[7] KAISER Florian, ISSAUTIER, Amandine, NGAH, Lutfi A., et al. A versatile source of polarization entangled photons for quantum network applications. Laser Physics Letters, 2013, vol. 10, no 4, p. 045202.CV-QKD https://doi.org/10.1088/1612-2011/10/4/045202

[8] PITTALUGA, Mirko, MINDER, Mariella, LUCAMARINI, Marco, et al.600-km repeater-like quantum communications with dual-band stabilization. Nature Photonics, 2021, vol. 15, no 7, p. 530-535. https://doi.org/10.1038/s41566-021-00811-0

[9] HUANG, Duan, HUANG, Peng, LIN, Dakai, et al. High-speed continuous-variable quantum key distribution without sending a local oscillator. Optics letters, 2015, vol. 40, no 16, p. 3695-3698 https://doi.org/10.1364/OL.40.003695

TeraXion
An indie Semiconductor Company

teraxion.com

2716 rue Einstein
Québec City, Québec, CANADA G1P 4S8
+1 (877) 658-8372 / ultrafast@teraxion.com