Quintessence Labs

WHITE PAPER

Quantum Key Distribution Systems Compared

Author(s):
Andrew Lance
John Leiseboer
Thomas Symul

Table of Contents

1. Document Scope

This document describes some of the key differences between Discrete Variable QKD and Continuous Variable QKD (CV-QKD) followed by a discussion of the technology pathway for CV-QKD.

2. Introduction

Quantum physics offers an information-theoretical secure method for distributing cryptographic key material. Quantum Key Distribution (QKD) enables two remote parties, “Alice” and “Bob,” who are connected by a quantum channel such as a passive optical link to securely generate secret key material. Alice transmits random information encoded onto quantum states of light to Bob, who measures the received quantum states using detectors. Following this step, Alice and Bob apply a series of algorithms on their data to extract a cryptographically secure key. It has been proven that QKD is information-theoretical secure, meaning that any eavesdropping attempt is either guaranteed unsuccessful, or detected, in which case Alice and Bob will not use their freshly generated keys.

3. Two types of Quantum Key Distribution: Discrete Variable & Continuous Variable

In general, there are two different (but complementary) approaches to QKD to generate the secret key material. Analogous to the particle-wave duality of light, these two approaches either put the emphasis on the corpuscular or wave aspect of the quantum carrier of information to provide the security.

The first approach is Discrete Variable QKD (DV-QKD), in which the particle nature of light is emphasised to achieve secure key distribution. For example, information is encoded on the physical properties of single-photon, such as their polarisation state, by the transmitter. Single-photon resolving detectors are used to measure the received quantum states.

The second approach is Continuous Variable QKD (CV-QKD), in which the wave nature of light is emphasised to achieve secure key distribution. In this second approach, information is encoded onto the amplitude and phase quadratures of a bright coherent laser by the transmitter, and the receiver measures the quadratures of light using balanced homodyne detectors.

DV-QKD was originally conceived in 1984 by Bennett and Brassard,[1] and shown to be information-theoretically secure by Lo and Chau in 1999.[2] Currently there are several research groups and a few companies around the world working on DV-QKD technologies and implementations.

Although CV-QKD is a much younger technology, it now achieves similar performance and security levels as DV-QKD technologies. CV-QKD, however, offers a significantly superior pathway forward in terms of cost, form factor, and performance, at the cost of a more complex data processing.

CV-QKD was conceived in the early 2000s.[3] Two independent protocols were proposed in 2002 by Silberhorn et al.[4] and in 2003 by Grangier et al.[5] Both protocols utilized coherent state lasers, and also enabled, in principle, the generation of secret key material over arbitrary long distances in ideal operating conditions. Several research groups and at least one company are developing CV-QKD technologies.

Importantly, CV-QKD was proven to be information-theoretically secure in 2009,[6] putting it on par with DV-QKD in terms of security.

[1] C.H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, December 1984, pp 175-179.

[2] H.-K. Lo and H. F. Chau Science 283, 2050 (1999).

[3] T. C. Ralph, Phys. Rev. A 61, 010303(R) 2000. M. Hillery, Phys. Rev. A 61, 022309 2000. D. Reid, e-print quant-ph/9909030.

[4] Ch. Silberhorn, T. C. Ralph, N. Lutkenhaus, and G. Leuchs, Phys. Rev. Lett. 89, 167901 (2002).

[5] F. Grosshans et al., Nature (London) 421, 238 (2003).

[6] R. Renner and J. I. Cirac, Phys. Rev. Lett. 102, 110504 (2009). A. Leverrier and P. Grangier, Phys. Rev. Lett. 102, 180504 (2009).

4. Secret Key Rates: Protocols and Assumptions

The secret key rate is affected by the following factors:

i. The information rate between Alice and Bob in units of:
   a. Quantum states/second (system architecture dependent)
   b. Error corrected bits/Quantum states (protocol dependent)

ii. Finite key effects

iii. For DV-QKD, quantum bit error rate (QBER); for CV-QKD, channel loss and excess noise

All things being equal, the secret key rate will be most influenced by the information rate (error-corrected raw key rate) between Alice and Bob. In this aspect, discrete and continuous variable approaches differ, in that for single-photons, most are lost during transmission, but each photon contains a good amount of information, whilst all continuous quantum states are detected, but each contain very little information.

Moreover, the secret key rate of any QKD protocol can be optimised by considering specific security assumptions for a given implementation. When comparing QKD key rates for different implementations, it is vitally important to understand and account for all differences in security assumptions.

5. Physical Architecture Comparison

In contrast to DV-QKD, CV-QKD is neither limited by single-photon generation nor single-photon detection techniques. Rather, CV-QKD can be implemented by modulating the amplitude and phase quadratures of a shot-noise-limited coherent laser and using shot-noise limited homodyne detectors.[7]

CV-QKD offers the advantage of high total detection efficiencies by using homodyne detectors with high quantum efficiency photodiodes. Furthermore, CV-QKD systems are compatible with current telecommunication technologies, such as modern telecommunication encoding, transmission techniques, and detection techniques. In fact, CV-QKD systems can be fully built using “off-the-shelf” coherent optical telecommunication hardware.

The main technology differences between DV-QKD and CV-QKD protocols are summarized in this table:

	DV-QKD	**CV-QKD**
Source	Single photons/attenuated coherent laser	Weakly modulated coherent laser
Detector	Single-photon detectors	Homodyne detectors

Table content is further explained below.

5.1 DV-QKD Single-Photon Sources

It is both difficult and resource-intensive to produce a true single-photon source; e.g., single-photon pairs produced via a parametric down conversion process. Alternatively, single-photon sources can be approximated using an attenuated laser.

Additionally, the photon number distributions of both sources obey Poissonian statistics, which leads to a security risk that is due to the non-zero probability of generating two photons per pulse. In this case, it has been shown that the security of QKD protocols can be compromised over long transmission distances in the case where Eve uses sophisticated photon-number splitting attacks.[8] It was shown in 2005, however, that the security of DV-QKD protocols that use weak coherent state pulses could be improved by using decoy state protocols.[9]

[7] S. L. Braunstein and P. Loock. Rev. Mod. Phys. 77 513 (2005).
[8] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. 85 1330, (2000).
[9] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94 230504, (2005).

5.2 DV-QKD Single-Photon Detectors

In practice, the secret key rates of DV-QKD protocols are inherently limited by the detection of single-photons.[10] Typically, single-photons or weak coherent pulses are detected using photon detectors such as avalanche photodiodes or superconducting photodetectors. Four main factors limit the rate of these single-photon detectors:

a. Finite quantum detection efficiency
b. Electronic noise (or dark noise)
c. Timing resolution (jitter)
d. The detector recovery time (known as detector dead time)

In addition, single-photon detectors can be expensive, bulky and may sometimes require cooling (via liquid nitrogen or liquid helium) to achieve peak performance.

Steady technological advancement has allowed DV-QKD to achieve secret key rate transmission over distances up to 240 km at a rate of a few hundred of bits per seconds.

5.3 CV-QKD Weakly Modulated Coherent Laser

The amplitude and phase quadratures of the light can be detected using off-the-shelf balanced homodyne detectors, which can have a shot-noise to electronic dark-noise clearance exceeding 10 dB for a bandwidth exceeding 3 GHz. It is anticipated that these detector bandwidths could be readily extended up to 10 GHz.

5.4 Basis Switching

In DV-QKD protocols it is required that Bob randomly switch measurement basis. However, counter intuitively, with CV-QKD protocols it is not only possible to simultaneously encode information onto both the amplitude and phase quadratures of the coherent laser, but also to simultaneously measure both the amplitude and phase quadratures of the light. This so-called "no-switching" protocol[11] not only vastly simplifies the implementation of CV-QKD protocols, but also enables higher secret key transmission rates.

6. Technology Pathway for CV-QKD

The technology pathway for CV-QKD exploits the three advantages of the CV-QKD technology:

a. High raw key rates
b. Reduced form factor
c. Reduced cost

6.1 High Key Rates

High key rates are achievable using off-the-shelf telecommunications components, including shot noise limited lasers, modulators, and balanced detectors.

CV-QKD is DWDM compatible, thus supporting multiple channels to achieve high key rates, as well as supporting more flexible deployments:

a. Multiple users on a single optical channel
b. Different topologies
c. Coexistence with existing telecom architecture

6.2 Reduced Form-Factor

It is relatively simple to integrate CV-QKD optics functionality to reduce form-factor, power, weight and cost. Discrete COTS components already exist for all required functionality. In some cases, some integrated functionality is also already available as COTS components. As all the individual components already exist, there is negligible risk in developing highly integrated CV-QKD transmitter and receiver components.

[10] N.Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74 145, (2002).

[11] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul. T. C. Ralph and P. K. Lam, Phys. Rev. Lett. 93 170504, (2004).

For reduction of form factors, CV-QKD can leverage the advancements made by the coherent optical communications community in areas of VLSI technology. These integration technologies range from well understood platforms of Indium Phosphide (InP), planar light wave circuits (PLC), and more recently, Silicon photonics.

(Non-QKD) subsystems manufactured using InP and PLC have been deployed in space.

6.3 Free Space QKD

CV-QKD offers several advantages over DV-QKD in free space applications. CV-QKD systems do not require single-photon detectors, which are sensitive to background light sources. In contrast, CV-QKD systems use a homodyne detector that requires a local oscillator to detect the transmitted signal. A homodyne detector system using a local oscillator offers significant robustness to background light sources that otherwise affect single-photon systems. The local oscillator acts as a spatial and spectral filter such that only photons with the same frequency and in the same optical mode as the local oscillator laser are detected using the homodyne detector. As such, homodyne detectors can be operated unimpaired in daylight conditions, without any of the filtering (i.e., spatial filters, spectral filters, etc.) required for single-photon detectors.

Furthermore, in CV-QKD systems, Alice typically multiplexes the local oscillator laser with the signal laser so that the two lasers co-propagate in the same spatial mode to Bob. This technique offers several additional advantages. Firstly, by using the local oscillator as the timing reference, the system can be made to be robust against timing jitter caused by atmospheric fluctuations. Secondly, provided the detector is sufficiently large, the system is robust against spatial beam jitter, as both beams jitter spatially in an identical fashion due to the common spatial mode. In this case, adaptive optics may help to prevent optical losses due to beam jitter. Finally, the use of adaptive optics may enable the correction of wave front distortions due to propagation through the atmosphere. In both aforementioned cases, a secondary "guide" laser would not be required.

7. Additional Information

For more information on this topic please contact QuintessenceLabs by emailing **info@quintessencelabs.com** or visit **quintessencelabs.com**.

Quintessence Labs

AUSTRALIA
Unit 11, 18 Brindabella Circuit
Brindabella Business Park
Canberra Airport ACT 2609
+61 2 6260 4922

UNITED STATES
175 Bernal Road
Suite 220
San Jose CA 95119
+1 650 870 9920

www.quintessencelabs.com

Document ID: 3676