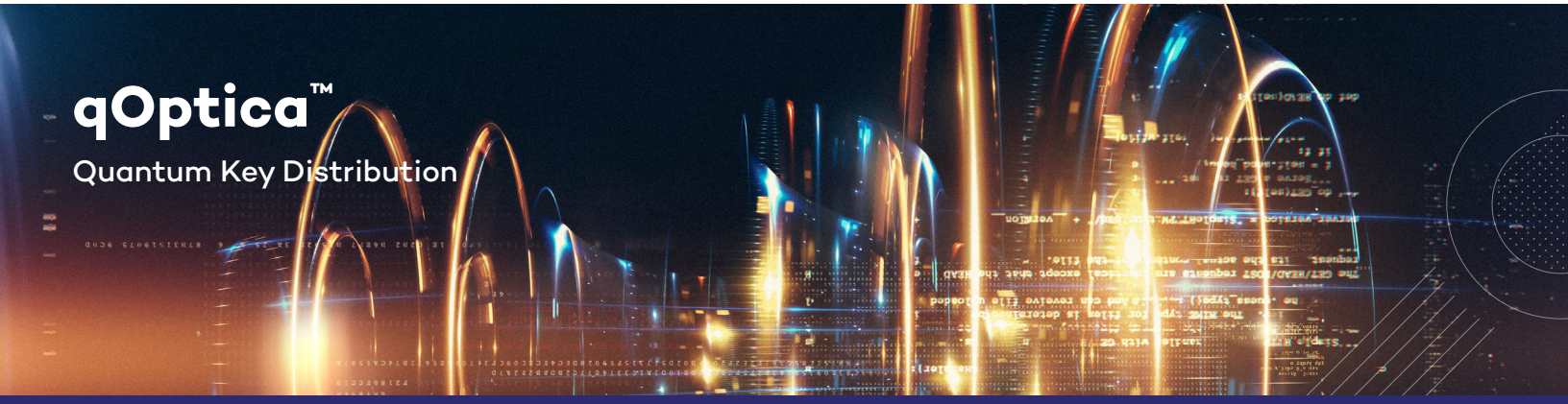
Quintessence Labs



qOptica™

Quantum Key Distribution

A significant step towards providing a quantum safe crypto environment

Fast exchange of secure keys, protected by the laws of physics

Continuous Variable QKD fiber optic and free space

QKD Overview

Quantum Key Distribution (QKD) is a point-to-point protocol that uses specialised hardware to share secret keys over an optical link (fibre or free-space). Secrecy of the keys is guaranteed by the laws of quantum physics—the system continuously estimates the maximum amount of information that could have been obtained by an eavesdropper, and only outputs keys when it can exploit an information advantage.

Types of QKD

There are two main approaches to QKD that leverage, respectively, the particle or wave characteristics of the quantum information carrier.

- Discrete Variable QKD (DV-QKD) (particle): information can be encoded on the physical properties of single-photons, and measured with single-photon detectors.
- Continuous Variable QKD (CV-QKD) (wave): information can be encoded onto the amplitude and phase quadratures of a coherent laser, and measured with coherent detectors.

	DV-QKD	CV-QKD
Source	Single photons/attenuated laser	Weakly modulated laser
Detector	Single-photon detectors	Coherent detectors
Theoretic Secure	Yes	Yes

qOptica Benefits

QuintessenceLabs offers CV-QKD technology with built-in advantages in terms of cost, form factor, and performance:

- **Performance:** The use of coherent signal encoding enables high throughputs that are not limited by single-photon generation or detection. Moreover it allows for daylight operation over free space optical links.
- **Cost:** Compatibility with current telecommunication technologies, such as telecommunication encoding, transmission and detection techniques, as well as the ability to use standard fiber connections, allow for cost effective systems.

Quantum Safe Architecture

QKD by itself does not solve the quantum security challenges faced. It needs to be part of an integrated solution generating, sharing and managing encryption keys.

QuintessenceLabs' quantum safe crypto solutions are a part of a full technology stack including:

- **True Quantum Random Number Generator**
- **Quantum Key Distribution**
- **Post quantum crypto-agile key management with hardware root of trust and quantum entropy**
- **Secure replication of quantum keys between key management nodes over a VPN link that is itself secured by quantum keys**

SPECIFICATIONS

qOptica™

Quantum Key Distribution

CV-QKD System Description	• Coherent state CV-QKD system • Gaussian modulation • Dual homodyne detection
Security Options	• Finite size effects • Epsilon security parameter • Collective or individual attacks
System Performance	• Raw key rate - 15×10^6 symbols/second sustained • Max optical quantum channel loss -10 dB (maximum) • Max distance: 40 km over standard commercial fibre • Indicative final key rates under individual attack assumption:

Distance	AES256 keys per second	Key rate (Kb/sec)
5 km / 3 miles	960	240
10 km / 6 miles	776	194
20 km / 12 miles	400	100
30 km / 18 miles	112	28
40 km / 25 miles	16	4.3

• Indicative final key rates under collective attack assumption:

Distance	AES256 keys per second	Key rate (Kb/sec)
5 km / 3 miles	480	120
10 km / 6 miles	336	84
20 km / 12 miles	132	33
30 km / 18 miles	56	14
40 km / 25 miles	7	1.9

Dimensions: These are for each station. *Two stations are required: **transmit and receive**.*	• Height – 6 RU (26.67 cm or 10.5 inches) (excluding UPS) • Width – standard telecoms 48.26 cm (19-inch) rack mount • Length – 120 cm (47.24 inches)
Power Requirements	• ~1kW per Alice and Bob subsystems
Data Interface Requirements	• 1 x RJ45 Gb/sec ethernet connection for management traffic • 1 x SMF28 optical fibre from Alice to Bob (QKD channel) • 1 x SMF28 optical fibre from Alice to Bob (Classical communication channel)
Power Interface Requirements	• 15 Amp mains power to UPS
User Interface	• GUI for controlling system • QLabs proprietary interface for key provisioning • ETSI interface for key provisioning

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: 5098-01