www.id-3.co.uk

Quantum Key Distribution (QKD)

Continuous Variable QKD for high performance, low cost and fully integrated key distribution.

What is QKD?

Key distribution is the process of exchanging cryptographic keys between two or more parties to allow them to securely share information. Widely used key distribution strategies use mathematics to protect the exchange of keys, but have been vulnerable to weak random numbers, advances in processing power, new attack strategies and the emergence of quantum computers.

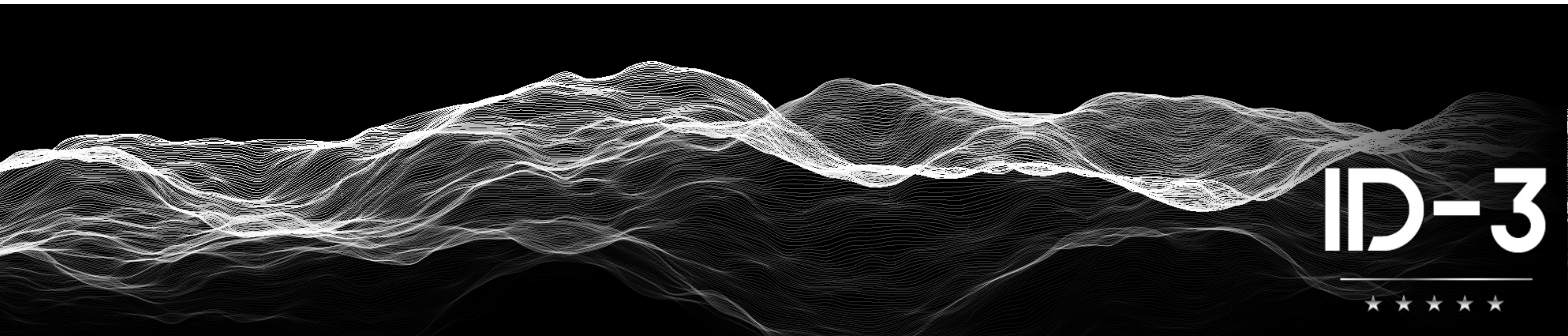
Quantum Key Distribution instead uses physics to share secret keys. Any interception or attempt to compromise the exchange of keys alters the state of the system, which then automatically compensates to ensure continued secure operation. QKD has been proven to be information-theoretic secure, i.e. the protocol cannot be broken even by an adversary with unlimited computing power. No advancements in computing power or crypto-analysis will be able to break the QKD protocol, including quantum computers.

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.
- **Continuous Variable QKD (CV-QKD)** (wave): information can be encoded onto the amplitude and phase quadratures of a bright laser.

	DV-QKD	CV-QKD
Source	Single photons/attenuated laser	Weakly modulated laser
Detector	Single-photon detectors	Homodyne detectors
Protocol	Bennett and Brassard	Silberhorn, Grangier
Information Theoretic Secure?	Yes	Yes



QKD

ID-3 and QuintessenceLabs offers CV-QKD with built-in advantages in terms of cost, form factor, and performance:

- **Performance:** the use of lasers to encode the signal enables high throughputs that are not limited by single-photon generation or detection.
- **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.
- **Reduced Form-Factor:** the ability to use COTS components and integrated functionalities allow for reduced form-factor, power, weight and cost.
- **Free Space QKD:** The homodyne detectors used offer significant robustness to background light sources that negatively affect single-photon systems. CV-QKD systems can operate unimpaired in daylight conditions, without any filtering.

QuintessenceLabs' post-processing implementation includes post-selection, error reconciliation and privacy amplification.

- **Post-selection** is a process that uses exchanged data that is more favorable to the legitimate communicating parties and less favorable to an attacker.
- **Error reconciliation** corrects communication errors in a way that minimizes information flow to an attacker.
- **Privacy amplification** reduces eavesdropper's information to approximately zero.

This post-processing capability delivers on the promise of CV-QKD's high throughput capability, enabling the fastest exchange of secure keys, protected by the laws of physics.

Full Stack Delivery

QKD by itself does not solve the security challenges faced. It needs to be part of an integrated solution generating, sharing and managing encryption keys. QuintessenceLabs' QKD capability is part of a full technology stack including:

- True Quantum Random Number Generator
- Quantum Key Distribution
- Key Management with a hardware root of trust using standards (KMIP)
- Secure replication of quantum keys between key management nodes over a VPN link that is itself secured by quantum keys

Cryptographic Integration	Embeddable key management libraries enforcing security policy. Use of keys for cryptographic purposes
Key Management	Full enterprise key management capability including cryptographic policy management
Encrypted Link Layer	Provides end-to-end, point-to-point encrypted data communications link
Quantum Key Distribution	Continuous Variable QKD, fiber optic and free space
Entropy Source	Quantum Entropy Source delivering full entropy random bits at 1Gbit/s

ID-3