Redefining Security

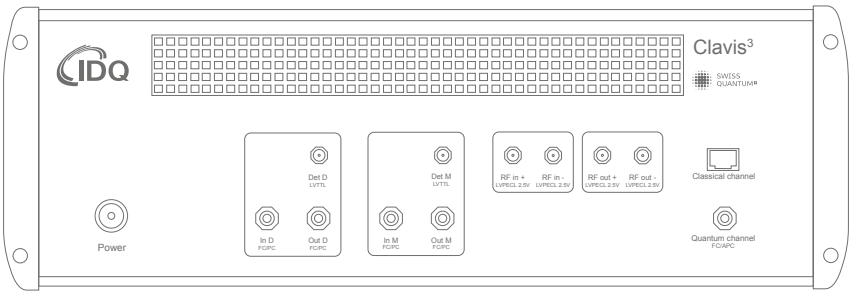
Clavis³ QKD Platform

Quantum Key Distribution for R&D applications

Quantum Key Distribution (QKD) is a technology that exploits a fundamental principle of quantum physics – observation causes perturbation – to exchange cryptographic keys over optical fibre networks with provable security.

QKD is one element in a complete cryptographic system. It includes both key exchange and encryption, which can ensure quantum-safe security, i.e. a guarantee that encrypted messages will remain confidential against the power of a quantum computer. Although the design and realisation of a multi-purpose quantum computer, which will be able to break existing public-key cryptography, remains a challenge, progress in this field is driving demand for quantum-safe encryption methods. The era of post-quantum cryptography has begun, where cryptographic methods must be resilient to a quantum computer

The study of QKD has therefore acquired a new sense of urgency: it is simply not possible to wait until the arrival of the quantum computer to design and test suitable cryptographic methods.



Key Applications

- Quantum Cryptography Research
- Pilot Network Deployment
- Education and Training
- Demonstration and Technology Evaluation

Key Benefits

- Open QKD platform for R&D applications
- High-speed key generation and distribution up to 100 km
- Option for external detectors
- Coherent One-Way (COW) Protocol

A Quantum Key Distribution Research Platform

The Clavis³ was designed as a research platform, with both automated and manual operations. The user can therefore experiment with different parameters and study various setups. The optical platform is well documented in scientific publications and has been extensively tested and characterised.

THE CLAVIS³

The Clavis³ Quantum Key Distribution Platform – clavis is the Latin word for key – was developed by ID Quantique to serve as a versatile research tool for both academic and industrial applications.

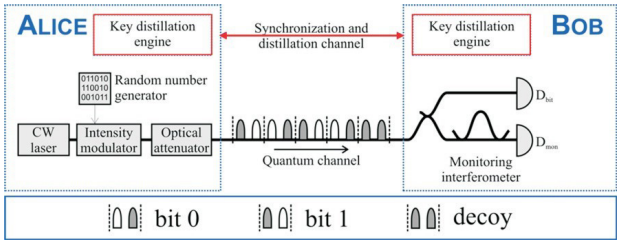
The Clavis³ was designed as a research platform, with both automated and manual operations. The user can therefore experiment with different parameters and study various setups. In addition, the Clavis³ receiver, the Clavis3-B, can use external single-photon detectors, which can be provided either by ID Quantique, or by the end-user himself.

Secure key exchange is possible over distances of up to one hundred kilometers, as well as over standard telecom networks with WDM. The optical platform is well documented in scientific publications and has been extensively tested and characterised.

A comprehensive software suite implements automated hardware operation and complete key distillation. The secret keys provided by Clavis³ can be fed in various encryption systems.

OPTICAL SCHEME

The Clavis³ quantum key distribution platform is based on the Coherent One-Way (COW), protocol, patented by IDQ.



The COW optical scheme

The transmitter, Clavis3-A (ALICE) contains a laser, which emits a CW beam. The beam is subsequently modulated, to provide coherent optical pulses, with bit patterns corresponding to zeros and ones. The pulses are then attenuated to reach single photon levels. These pulses travel from the transmitter, Clavis3-A, over the quantum channel, to the receiver, Clavis3-B, where they are detected. In the receiver, some of the pulses reach the detector D_{bit}, where they generate the key, and some of the pulses go through the monitoring interferometer and reach detector D_{mon}. They are used to monitor eavesdropping.

The Clavis³ stations provide electronic synchronisation signals to connect and synchronise external components and systems. The wavelength of the laser used in the Clavis³ platform is stabilised to a value on the ITU grid.

KEY DISTILLATION

After the raw key material has been exchanged, it is post-processed in order to correct errors and reduce the information to which an eavesdropper could have access to an arbitrarily low level. In the Clavis³ platform, this post-processing is fully implemented and automated in order to allow secure key exchange. It consists of five main steps:

Sifting: sifting removes the bits, which cannot be used in the key itself (for example when decoy sequences are sent).

Key reconciliation: key reconciliation relies on the Low Density Parity Code (LDPC) algorithm to remove errors; it is also used to estimate the bit error rate.

Privacy Amplification: PA uses the Wegman-Carter Strongly Universal Hashing to reduce the information, which may have leaked to an eavesdropper, to any chosen level. The set of Universal Hashing functions is constituted of Toeplitz matrices.

Authentication: authentication of the two stations is done through IT-secure polynomial Universal-Hashing with One-Time Pad encryption.

Key material storage and management: the final keys are stored and can be later accessed for verification, key usage and further analysis.

Clavis^3 QKD Platform

Faster Key Processing

All key distillation steps are hardware-based, implemented in an FPGA inside the platform, for enhanced speed and reliability.

CONFIGURATIONS

The Clavis^3 platform comprises two stations, the transmitter unit, Clavis3-A and the receiver unit, Clavis3-B. Each station consists of an optical and electronic platform, which must be controlled by an external computer, which is linked to the station through an Ethernet connector.

The Clavis 3-A and Clavis 3-B units are linked by the quantum channel, used for the key transmission. In addition, they need a Service Channel, used for synchronisation between the two units The service channel is made of a couple of optical fibre strands, connected to the units with SFP transceivers with LC/APC connectors. The two fibre strands can be reduced to a single one with SFP transceivers supporting bidirectional transmissions.

SOFTWARE SUITE

Cockpit GUI

The Clavis^3 Cockpit is a graphical interface that can be used to control and operate the Clavis^3 platform. It provides access to some hardware parameters and allows the user to visualise processes ranging from system calibration to secure key exchange. The Clavis^3 Cockpit GUI is used to control both the QKDS-A and QKDS-B stations.

IDQ4P Communication Protocol

The IDQ4P Communication Protocol is the proprietary communication protocol used to control and monitor the Clavis^3 platform. Users can write customised programs accessing the system to perform the tasks required by quantum key distribution. The protocol includes functions ranging from low-level primitives allowing the user to read or set a particular hardware parameter, to high-level procedures for complete quantum key distribution. A comprehensive and detailed reference manual is provided.

Why Clavis^3 QKD Platform?

- High speed key generation, with 1.25 GHz pulse repetition rate at the transmitter
- Possibility to have external detectors for maximum flexibility
- Hardware-based key processing (in an FPGA), to allow high key distribution rate
- High ease of use
- Manual & automated operation
- Designed as a research platform, with access to, and possibility to modify, several parameters
- *Synch Out* signals

Clavis³ QKD Platform at a glance

Model	Clavis³
GENERAL INFORMATION	
Parameters	
Dimensions (L x W x H)	424 x 402 x 144 mm
19'' Rack compatible	Space required: 4U
Weight (QKDS-A)	10 kg
Weight (QKDS-B)	10 kg
Operating conditions:	
Temperature	20 to 30 °C
Max relative humidity (@ 30 °C)	80%
Non-operating conditions:	
Temperature	-10 to +60 °C
Max relative humidity (@ 40 °C)	90%
Recommended computer specifications	
Ethernet connexion	✓
RAM	4 GB
Hard Disk	A minimum of 100 MB of free space for software suite installation, additional space is needed when running the applications
Processor	Minimum Intel Core Duo
TECHNICAL SPECIFICATIONS	
Hardware	
Optical platform	✓
Proprietary digital signal generation and data acquisition electronics	✓
Random number generation	One Quantis QRNG OEM component in each station
Power supply	100-240 VAC @ 50/60 Hz
External computers	Sold separately
Interfaces and Inputs/Outputs	
Optical connectors (front panel):	
Quantum channel Connector type: Optical fibre type:	 FC/APC SMF-28
Service channel Two SFP modules, with LC/APC connectors (for two-fibre configuration) Or one bidirectional SFP module (for single-fibre configuration)	
Computer interface (back panel):	Ethernet
Front Panel Indicators	
Power LED indicator (red: on)	
Quantum Link LED indicator (green: quantum channel active)	
Data LED indicator (green: raw key exchange in progress)	
Quantum Link LED indicator	
Key Exchange Characteristics	
Maximum transmission loss acceptable (typ.)	12 dB Standard
	18 dB Premium
	>18 dB Extra (upon availability)
Maximum length of quantum channel (typ.)	>100 km
Secret key rate (typ.)	>3 kb/s after 50 km
Sifting and Key Distillation	Fully automated

ID Quantique

Chemin de la Marbrerie 3,
1227 Carouge/Geneva Switzerland

T +41 22 301 83 71
F +41 22 301 83 79
E info@idquantique.com

www.idquantique.com

ID Quantique (IDQ) is the world leader in quantum-safe security solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services to the financial industry, enterprises and government organisations globally.

IDQ also commercialises a quantum random number generator, which is the reference in the gaming and security industries.

Additionally, IDQ is a leading provider of optical instrumentation products; most notably photon counters and related electronics. The company's innovative photonic solutions are used in both commercial and research applications.