Redefining Security

Clavis^{300} Quantum Cryptography Platform

Integrated Quantum Key Distribution & LEA Encryption System

The post-quantum era has begun, where cryptographic methods must be resilient to attacks by a quantum computer. Data with long term sensitivity is at risk of being intercepted now, stored for future use, and decrypted in a few years when multi-purpose quantum computers will be implemented and able to easily break existing public-key cryptography. A solution to this threat is Quantum Key Distribution (QKD), 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 safe against both conventional and future quantum computer-based attacks. It is the cornerstone of a true quantum-safe solution today.

The Clavis^{300} is a complete modular cryptographic solution that performs QKD and LEA encryption as an option. It is ideal for investigating and testing quantum cryptography different network configurations, such as point-to-point or with intermediate relay nodes.

Key Markets

- Telecoms and Network Operators
- Financial Services Companies
- Governments and Defence
- Healthcare Organisations
- Critical Infrastructure
- IP-rich Enterprises

Key Applications

- Quantum Cryptography technology evaluation
- Pilot network deployment
- Demonstrator for Innovation lab
- Long distance key distribution using relay nodes

A Quantum Key Distribution Evaluation Platform

The Clavis^{300} system is designed for testing QKD and LEA encryption, and its integration with existing data communication systems. It comprises both automated and manual operations. The user can therefore experiment various configurations and perform in depth monitoring of its performances before a full deployment.

THE CLAVIS^{300}

The Clavis^{300} generates and distributes keys, providing more than 10kb/s secure key bit generation rate at 10dB link loss. For a standard system, the maximum link loss is 18dB, which corresponds to about 70km in distance, depending on fibre quality. A premium system offers up to 24dB loss (depending on availability). The key refresh rate can be adjusted by an administrator.

As an option, the Clavis^{300} can also be provided with high-speed LEA encryptor blades integrated in the chassis. A single chassis with 6 slots can therefore include both a QKD system and state-of-the-art link encryptors. If needed additional chassis can be paired with the Clavis^{300} to host additional encryption blades. Currently the encryptor is based on Korean LEA (Light Encryption Algorithm) ciphers, and allows 4x10Gbps encryption rate. The encryption processing latency is less than 10 microseconds.

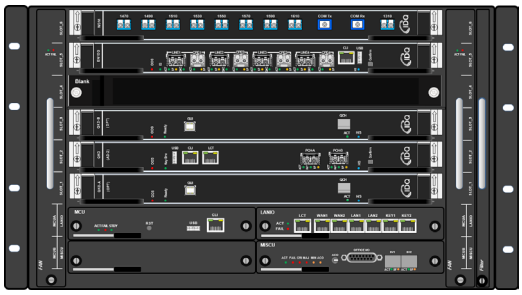

Figure 1: The complete Clavis^{300} platform

MANAGEMENT AND MONITORING FUNCTIONS

The Clavis^{300} is controlled through a Command Line Interface or a Local Craft Terminal with GUI. A TL1-based Equipment Management System (EMS) is also provided for central management and monitoring purposes.

Through these interfaces, users can set-up: the QKD security parameters (such as session key configuration, connected encryptors IP and IDs, key refresh rates etc..); performance indicators (such as thresholds for monitoring alarms on temperature, voltage levels); and network system parameters (such as X.509 certificates, network addresses, masks, gateways etc...).

The system monitors continuously configured parameters and provides alarms and warning information with different severity levels (Minor, Major, Critical) in case thresholds are reached. Users can also monitor in real time the optical alignment and operation failures, acquisition times and lengths of the keys (Raw-Key, Sifted key, Authenticated (Final) Key), key rates, number of key generated and Quantum Bit Error Rate (QBER) through the user interfaces.

Multiple Configurations for Pilot Network Deployment

The Clavis^{300} provides QKD for both point-to-point or relay node configuration for long distance key distribution.

NETWORK APPLICATIONS

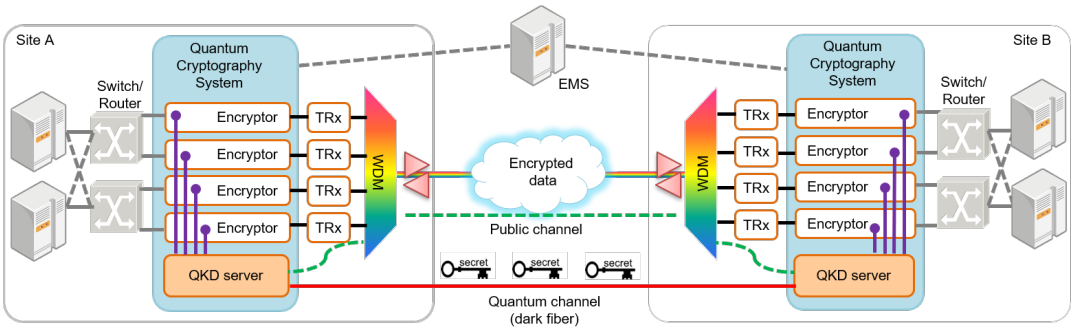

Figure 2: The Clavis^{300} with integrated encryptors in a point-to-point configuraton

The Clavis^{300} systems are inserted in front of the legacy transport system and encrypt/decrypt all traffic data. For better performance (longer distance and higher key rates), a dark fibre link is recommended for the quantum channel. The Clavis^{300} can be used in a point-to-point configuration or as a relay node for long range key distribution, with add/drop functionality.

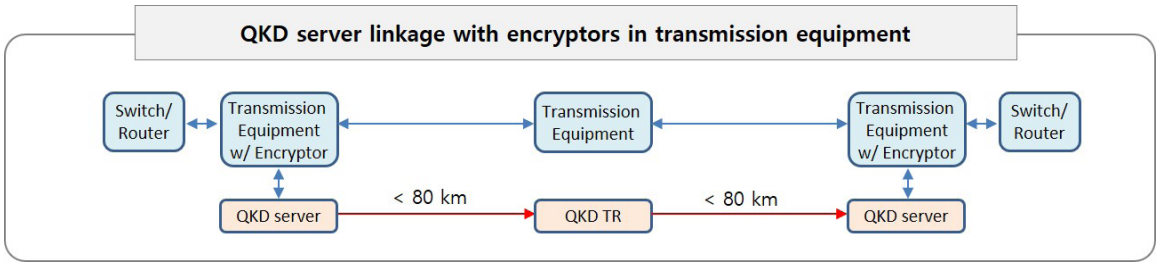

Figure 3: Relay node configuration

MAIN ADVANTAGES

- High-performance key distribution system based on hardware-based key processing (in an FPGA)
- Integrated system with high-speed LEA encryption in same chassis (optional)
- Modular point-to-point key distribution or long-range key distribution with relay nodes
- Highly configurable to access and monitor all parameters manually

Clavis^{300} Quantum Cryptography Platform at a glance

Model	Clavis^{300}
SECURE KEY DISTRIBUTION USING QUANTUM	
Key generation rate	6 kbps @ 12 dB link loss
Maximum range[1]	18 dB (typically 70 km) Up to 24 dB premium (depending on availability)
Typical QBER	<3% @ 10 dB link loss
System clock frequency	125 MHz
Integrated QRNG	1.6 Gbps
Auto-recognition of eavesdropper's attack	✓
Encryption key supply up to 80 encryptors	✓
Secure key supply to encryptors using DTLS	✓
Key relay node with add/drop functionality	✓
SC optical connector for quantum channel	✓
XFP for public channel	✓
PHYSICAL PARAMETERS	
General	Modular system providing high level of scalability and legacy network compatibility
Dimensions	Integrable in a 19'' rack; 6U chassis
Power supply	- 48 VDC (-36 VDC ~- 60 VDC)
Power supply option	Additional 1U AC to DC power supply unit option for 96 ~ 264 VAC
HIGH-SPEED ENCRYPTION (OPTIONAL)	
Bi-directional encryption	4 x 10 Gbps
Algorithm	LEA (Korean standard)
Authentication	GCM (Galois Counter Mode)
Latency	<10 microseconds
MANAGEMENT FUNCTIONS	
CLI and graphical LCT for local access & set	✓
TL1-based EMS server & client for monitoring	✓

[1] Due to polarisation effects, the DR may be restricted for optical links with aerial fibres or cables in rapidly varying environments.

ID Quantique

Rue Eugène-Marziano 25,
1227 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.