Redefining Security

Cerberis XGR QKD Platform

Quantum Key Distribution designed for Academia & Research Institutes

Safety of current encryption methods, and especially of the key exchange mechanisms based on asymmetric cryptography, is a major concern today. While high-value sensitive data is already at risk, the arrival of quantum computers will render arithmetic asymmetric key exchanges unsafe: encrypted data can be stored now and easily decrypted later. Governments or enterprises, which must protect data for five to ten years or more, need to move to new crypto solutions now.

As a leading cyber security solution provider, IDQ has developed Quantum Key Distribution (QKD) systems that generate and distribute cryptographic keys across a provably secure communication network, to safely encrypt or authenticate data. In contrast to conventional key distribution algorithms, QKD is the only known cryptographic technique which provides proven secrecy of encryption keys, as well as long-term data confidentiality and integrity.

Cerberis XGR is ID Quantique's 4th generation of QKD and is especially designed to meet the needs of academia and research institutes. The study of QKD has acquired a new sense of urgency: it is simply not possible to wait until the arrival of quantum computers to design and test suitable cryptographic methods.

Key Applications

- Quantum cryptography research
- Point-to-point and Trusted Node evaluation system
- Education and training
- Demonstration and technology evaluation

Key Benefits

- Open QKD platform for R&D applications
- Embedded KMS for key distribution
- Interface to external encryptors
- User interface for technology evaluation and testing

Cerberis XGR QKD Platform

A Quantum Key Distribution Research Platform

The Cerberis XGR was designed as a research platform, with both automated and manual operations. The user can therefore experiment with different parameters and study various setups. IDQ's QKD products for academia & research institutes are well documented in scientific publications and have been extensively tested and characterized.

THE CERBERIS XGR

The Cerberis XGR Quantum Key Distribution Platform was developed by ID Quantique to serve as a versatile research tool for both academic and technology evaluation labs. The user can therefore experiment different parameter set-up and configurations, in both automated and manual modes.

The Cerberis XGR platform comprises two stations: the transmitter unit, Cerberis XGR-A (ALICE) and the receiver unit, Cerberis XGR-B (BOB).

The Cerberis XGR-A and Cerberis XGR-B units are linked by the quantum channel, used for the key transmission. In addition, a Service Channel is used for synchronization between the two units. Both channels are made of optical fiber strands, connected to the units with SFP transceivers and a single UPC connector for the quantum channel. Furthermore, the service channel can be reduced to a single fiber strand with SFP transceivers supporting bidirectional transmissions.

Secure key exchange is possible over fibers with a maximum loss of 12 dB to 18 dB (typ. up to one hundred kilometers), as well as over a single core using WDM. The optical platform is well documented in scientific publications and has been extensively tested and characterized.

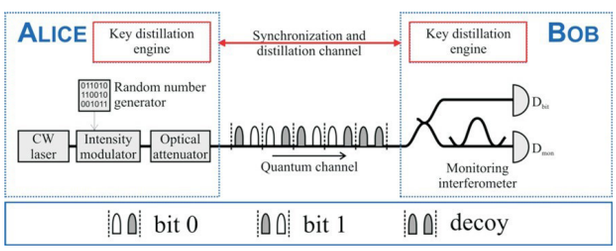
The Cerberis XGR also integrates a Key Management System (KMS) that manages key requests and key transfers between QKD optical systems and external encryptors. Key distribution to encryptors or any key consumer is performed over secured QKD ETSI REST API or proprietary interfaces developed in partnership with major vendors.

Cerberis XGR systems can be used in any network configurations including point-to-point, relay for longer distances, ring or star topologies.

A comprehensive software suite implements automated hardware operation and complete key distillation. The IDQ4P protocol of the Cerberis XGR can stream out the RAW Keys before the QKD post processing is applied (esp. the error correction). Those keys correspond on Bob side to the detection values and on Alice side to the Qbits that were sent for those specific detections. With the RAW Keys the user can compare the two streams and verify the QBER of the system.

OPTICAL SCHEME

The Cerberis XGR Quantum Key Distribution platform is based on the Coherent One-Way (COW) protocol, patented by IDQ.



The COW optical scheme

The transmitter, Cerberis XGR-A 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, Cerberis XGR-A, over the quantum channel, to the receiver, Cerberis XGR-B, where they are detected. In the receiver, some of the pulses reach the detector Dbit, where they generate the key, and some of the pulses go through the monitoring interferometer and reach detector Dmon. They are used to monitor eavesdropping.

The wavelength of the laser used in the Cerberis XGR platform is stabilized to a value on the ITU grid.

Cerberis XGR QKD Platform

Full real-time monitoring

Full monitoring tools that keep track in real time of the status and performance of the system in order to have the earliest warning of failures.

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 Cerberis XGR platform, this post-processing is fully implemented and automated 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.

SOFTWARE SUITE

Graphical User Interface for configuration, parameter set-up and monitoring

The Cerberis XGR Cockpit is a graphical interface desktop application that can be used to control and operate the Cerberis XGR platform. It provides access to some hardware parameters and allows the user to visualize processes ranging from system calibration to secure key exchange.

The QMS Web Application is also provided to configure links between QKD and encryptors, to monitor the Cerberis XGR systems and manage the Cerberis XGR Firmwares.

IDQ4P Communication Protocol for key streaming and key management

The IDQ4P Communication Protocol is the proprietary communication protocol used for key transmission and management of the Cerberis XGR platform. Users can write customized programs accessing the system to perform the tasks required by quantum key distribution. The protocol defines a key channel for the streaming of indexed keys and management/control channels for startup/shutdown, SW/FW updates, system notifications including events and alerts.

QNET WebAPI for automated management and monitoring

The QNET REST WebAPI used by the GUI can also be used directly to configure and monitor the Cerberis XGR.

WHY CERBERIS XGR?

- Research platform with GUI for visualization of parameters and QKD processes
- Access to QKD parameters, keys and RAW keys via API
- Manual & Automated operation
- Advanced Key Management System (KMS)
- Full real-time monitoring and management system (QMS)
- Key delivery to external encryptors

Cerberis XGR QKD Platform at a glance

Model	Cerberis XGR
GENERAL INFORMATION	
Parameters	
Dimensions	19'' rackmount chassis; 22.4'' deep
Dimensions without front & back handles, and mounting kit (L x W x H)	610 x 428 x 43.6 mm
Weight (QKDS-A)	13.5 kg
Weight (QKDS-B)	13.5 kg
Operating conditions:	
Temperature	10 to 35 °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	8 GB
Hard Disk	A minimum of 100 MB of free space for software suite installation and operation
Processor	CPU quad-core
TECHNICAL SPECIFICATIONS	
Hardware	
Optical platform	✓
Proprietary digital signal generation and data acquisition electronics	✓
Random number generation	2 QRNG chips (IDQ20MC1) per station
Power supply	100-240 V~ / 50/60 Hz / 5-2.5 A
Interfaces and Inputs/Outputs	
Optical connectors (front panel):	
Quantum channel Connector type: Optical fiber type:	 SC/UPC SMF-28
Service channel Two SFP modules, with LC/UPC connectors (for two-fiber configuration) Or one bidirectional SFP module (for single-fiber configuration)	
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

Applicable Standards:

FCC: 47 CFR, Part 15 (Class A)

Industry Canada: ICES-003, Issue 7 (Class A)

CE Safety: IEC 62638-1:2018, IEC 60825-1:2014

CE EMC: EN 55032:2015+A11:2020 (Class A)
EN 55035:2017+A11:2020

RoHS: 2015/863/EU

ID Quantique

Chemin de la Marbrerie 3,
1227 Carouge/Geneva Switzerland

T +41 22 301 83 71
F +41 22 321 12 52
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.