Redefining Security

Cerberis XGR QKD System

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. High-value sensitive data is already at risk. Indeed, the arrival of quantum computers renders 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.

The Cerberis XGR is part of IDQ's 4th generation of QKD and is an extension of the XG Series (for production environments) which aims to meet the needs of academia, research institutes and innovation labs.

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-friendly interface for technology evaluation and testing

Cerberis XGR QKD System

A Quantum Key Distribution Research Platform

The XGR Series 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 System 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-ups and configurations, in both automated and manual modes.

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

The XGR-A and XGR-B units are linked by the quantum channel, used for the key transmission. In addition, a Service Channel is used for synchronization and processing 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 and can be multiplexed with other data channels.

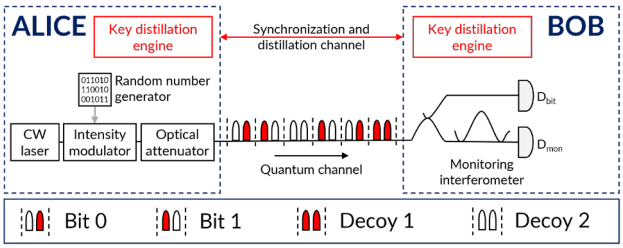
Secure key exchange is possible over fibers with a maximum loss of 12 dB to 18 dB (typ. up to ninety kilometers), as well as over a single core using WDM. The optical platform is well documented in scientific publications and has been extensively tested and characterized.

The Cerberis XGR also integrates IDQ Clarion KX Quantum Key Management System (Q-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 the secured QKD ETSI REST API or proprietary interfaces developed in partnership with major vendors.

A comprehensive software suite implements automated hardware operation and complete key distillation. The Cerberis XGR provides access to raw key material's sample and the sifted Keys before the QKD post processing is applied (esp. the error correction). Those sifted 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 sifted Keys the user can compare the two streams and verify the QBER of the system.

OPTICAL SCHEMA

The Cerberis XGR uses the Coherent One-Way (COW) protocol, patented by IDQ.



COW optical schema

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 system is stabilized to a value on the ITU grid.

Cerberis XGR QKD System

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 first sifted to remove all undetected pulses and all unusable detections. Then, 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 XGR systems, this process 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 Winnow 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 QMS Web application is a graphical interface application that can be used to control and operate the XGR systems. It provides access to some hardware parameters and allows the user to visualize processes ranging from system calibration to secure key exchange. It also allows to configure links between QKD and encryptors, to monitor the XGR systems and manage the XGR Devices' Firmwares.

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 XGR Devices.

WHY THE CERBERIS XGR?

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

Cerberis XGR QKD System at a glance

Model	Cerberis XGR
KEY FEATURES USING BUILT-IN DETECTORS	
Maximum length of quantum channel (typ. @ 0.2 dB/km)	60 km (@ 12 dB, optional 80/90 km @ 16/18 dB)
Secret key rate	Typical 14'000 AES-256 Keys per hour @ 18 dB Typical 28'000 AES-256 Keys per hour @ 12 dB
Protocol	Coherent One-Way (COW)
Key generation source	IDQ QRNG chip
Quantum channel	1 dedicated fiber (Optional WDM: O-Band in a single core)
Service Channel	1 TX/RX DWDM channel (C-Band)
Optical engine	Intrinsically polarization independent
Key processing	High speed hardware-based
Key security parameter[1]	$\varepsilon_{QKD} = 4.\ 10^{-9}$
Pulse repetition rate	1.25 GHz
ENVIRONMENTAL AND PHYSICAL PARAMETERS (per device)	
Form factor	1U, 19'' rackmount chassis
Dimensions (without front & back handles, and mounting kit)	W 428 mm x L 610 mm x H 43.6 mm
Interfaces	• Full Status LEDs available on the front panel • 2x Duplex Fiber SFP (Service Channel, KMS-O) • 1x Simplex Fiber (Quantum Channel) • 4x 1Gb Ethernet ports (Keys / Encryptors, KMS, Mgt, Aux) • 1x RS-232 (Console) • 1x USB 2.0
Power supply	1+1 Redundant hot-swappable power supply Each 300 W, 100-240 VAC, 47-63 Hz, 5-2.5 A or 36-72 VDC (optional)
Weight	13.5 kg
Temperature range	Operating +5 to +35°C Non-operating -10 to +60°C
Relative humidity range	Operating 5% to 85% RH, non-condensing Non-operating 5% to 90% RH, non-condensing
MANAGEMENT AND MONITORING	
Alerting functions & continuous monitoring[2]	XG Series can be administrated, configured and monitored via multiples interfaces (QNET REST Web API, QNET CLI Tools, QMS Web Application, SNMP, Syslog)
Raw data and key extraction	
Interface for accessing QKD parameters and raw data	QNET CLI Tools

Applicable standards	**FCC:** 47 CFR, Part 15 (Class A) **Industry Canada:** ICES-003, Issue 7 (Class A) **RoHS:** 2015/863/EU **NIST:** ESV IID SP 800-90B (IDQ QRNG chip)	**CE Safety:** IEC 62638-1:2018, IEC 60825-1:2014 **CE EMC:** EN 55032:2015+A11:2020 (Class A) EN 55035:2017+A11:2020

[1] With the above value, the probability that an eavesdropper knows at least one bit of a 256-bits AES key is about 10^{-12}. See this example.
[2] Provided separately

ID QUANTIQUE SA
Rue Eugène-Marziano 25
1227 Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 83 79
info@idquantique.com
www.idquantique.com