Redefining Security

XGR Series – 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. 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 XGR Series is ID Quantique'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.

Cerberis XGR

Clavis XGR

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

XGR Series – QKD Platform

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 XGR SERIES

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

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

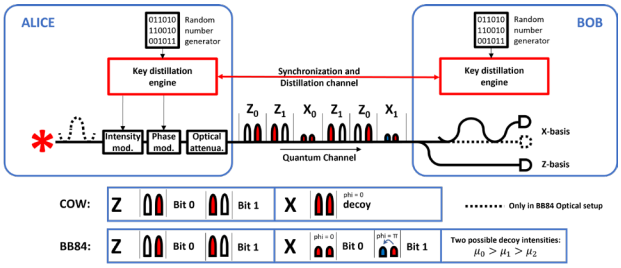
The XGR-A and XGR-B units are linked by the quantum channel, used for the key transmission. In addition, a Service Channel is used for synchronization and processing between the two units. Both channels are made of optical fiber strands, connected to the units with SFP transceivers and a single UPC connector 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) for a Cerberis XGR pair or 24 dB (typ. up to one hundred fifty kilometers) for a Clavis XGR pair, 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 XGR Series 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 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 IDQ4P protocol of the XGR Series can stream out the sifted 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 sifted Keys the user can compare the two streams and verify the QBER of the system.

OPTICAL SCHEMA



COW/BB84 optical schema

The Cerberis XGR uses the Coherent One-Way (COW) protocol, patented by IDQ. The transmitter, XGR-A, contains a laser, which emits a CW beam. The beam is subsequently modulated in intensity, 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, XGR-A, over the quantum channel, to the receiver, XGR-B, where they are detected. In the receiver, some of the pulses reach the detector Z-axis, where they generate the key, and some of the pulses go through the monitoring interferometer and reach detector X-basis. They are used to monitor eavesdropping. The major differences with the BB84 scheme are that the COW protocol does not use an interferometer on Alice's side, does not apply phase modulation and requires only one detector for the X-basis.

Clavis XGR uses the BB84 optical scheme. The transmitter, XGR-A, contains a pulsed laser. The beam is subsequently modulated in intensity and phase, to provide 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, XGR-A, over the quantum channel, to the receiver, XGR-B, where they are detected. Bits 0 and 1 are either on the detector Z-basis for intensity modulation and detectors X-basis for phase modulation. Eavesdropping monitoring is using information from both set of bases.

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

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 platform, 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 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 XGR Series' QMS Web application is a graphical interface application that can be used to control and operate the XGR platform. 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.

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 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 XGR Devices.

WHY THE XGR SERIES?

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

XGR Series – QKD Platform at a glance

Model	Cerberis XGR[1]	Clavis XGR[2]
GENERAL INFORMATION		
Parameters		
Dimensions	1U, 19'' rackmount chassis	
Dimensions without front & back handles, and mounting kit	W 428 mm x L 610 mm x H 43.6 mm	
Weight	13.5 kg	14 kg
Power supply	100-240 V~ / 50/60 Hz / 5-2.5 A	
QKD protocol	COW	BB84
Inputs/Outputs		
Quantum channel Connector type: Optical fiber type:	 SC/UPC SMF-28	
Service channel	Or one bidirectional SFP module (for single-fiber configuration) (OPTIONAL) Two SFP modules, with LC/UPC connectors (for two-fiber configuration)	
RECOMMENDED COMPUTER SPECIFICATIONS (TO RUN IDQ SOFTWARE SUITE)		
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	

[1] Detailed Technical and Environmental specifications can be found in the Cerberis XG brochure.
[2] Detailed Technical and Environmental specifications can be found in the Clavis XG brochure.

ID Quantique

Rue Eugène-Marziano 25
1227 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 organizations globally.

IDQ also commercializes 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.