Redefining Security

Clavis 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, ID Quantique (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 applicable to data in-transit and guarantying long-term data confidentiality and integrity of such data.

The XGR Series is IDQ's 4th generation of telecommunication-grade 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 and network integration research
- Grey box security testing
- Education and training
- Demonstration and technology evaluation

Key Benefits

- Access to internal data and modifiable parameters
- Option to use external detectors
- Interoperability through standardised interfaces for experimental networks
- Automated turn-key solution and user-friendly full stack SW for quick start

Clavis XGR QKD System

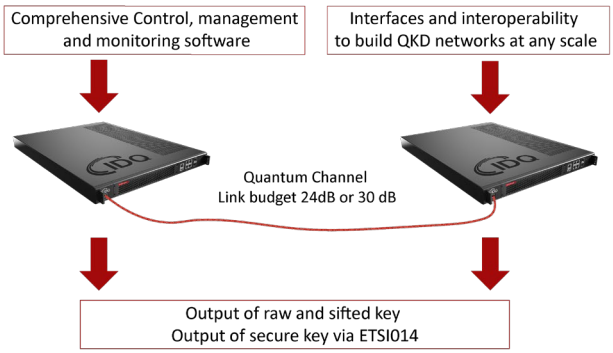
A Quantum Key Distribution Research Platform

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.

XGR basic functionality

The Clavis XGR is based on the Clavis XG, which is a QKD system intended for production use. The hardware and the basic functionality are identical. The product is a standalone system and it only requires a standard computer for management, control and monitoring.

The Clavis XGR combines the best out of two worlds: a highly industrialized system operating at telecommunication wavelength and an automated system with additional research features, which are herein described.



QKD protocol

A standard BB84 decoy state QKD protocol is implemented in the Clavis XGR including four-state preparation and measurement modules, respectively. The physical encoding is done in time-bin. This means that one degree of freedom is the time of arrival of the photon (early/late), and the second one is the phase relation between them, see figure below.

BB84 optical schema

Test and research features

Access to parameters and raw data

Designed for both research or testing and training activities, the Clavis XGR allows the user to access and manipulate certain key parameters of the protocol and the system configuration or implementation:

- Random number generator usage
- Qubit preparation
- Built-in single photon detectors
- System alignment and self-testing
- Post-processing of the raw data

Measurement results and raw data are exportable at several stages:

- Raw key
- Sifted key
- Key after error correction
- Secure key (i.e., the final key)

The Clavis XGR can be operated with external detectors. This illustration shows a Clavis XGR transmitter connected to three ID Qubes.

Operation with external detectors (NEW!)

The Clavis XGR now can be used with external detectors to replace the internal single-photon detectors (SPDs). This opens a plethora of research options in various directions:

- More control and more accessible parameters of the SPDs
- Better performance with high-end detectors like superconducting nanowire single-photon detectors (SNSPDs)
- Test your own detector for QKD applications

The Clavis XGR is designed to be compatible with all near-infrared single-photon detectors from IDQ (see page 4 for details).

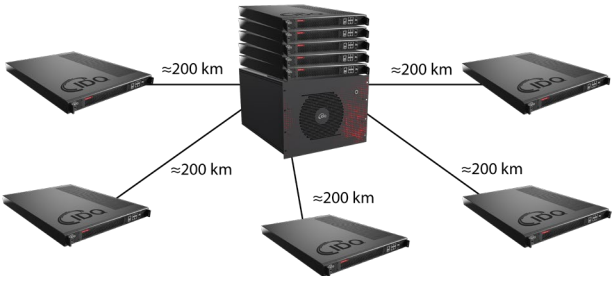
External detector options

The Clavis XGR can be optionally operated with external single-photon detectors. The choice of the detectors unlocks various research and education directions. They range from testing QKD from a security point of view, to researching QKD on an optical and protocol level, to integrating QKD in optical transport networks.

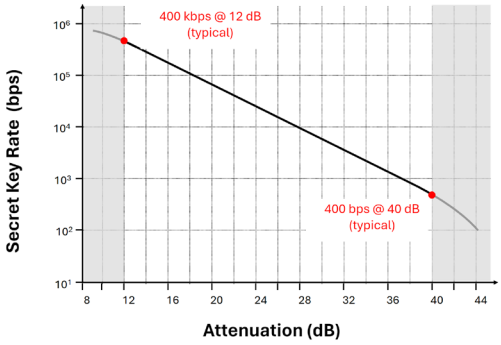
Long distance performance with SNSPDs

SNSPDs are the very best in single-photon detection, combining incredibly high detection efficiency, low dark count rates, unparalleled timing precision, and fast recovery times.

IDQ has developed polarization insensitive SNSPDs specifically optimized for QKD performance with the Clavis XGR.



A single ID281 or ID281 Pro system can embed SNSPD detectors to serve up to 5 Clavis XGR receiver modules in parallel, allowing to build a star topology with five links over typically 200 km each, for example. The ID281 Pro is a rack-mounted solution. The central node in this example is only 23U high, including the compressor and vacuum pump (not shown in the figure).



Unprecedented QKD performance: 400 kb/s secret key rate at 12 dB (typically) and at least 40 dB dynamical range can be achieved with the ID281 used as external detectors.

ID Qube and ID230

Semiconductor-based detectors are compact, affordable and easy-to-operate. The ID Qube Series of SPD's gives the researcher access to an even broader parameter set, and it allows for extended grey box testing of IDQ's BB84 implementation. The ID230 is ideally suited for research on extended QKD performance with SPAD-based SPDs.

External detector recommendations for various use cases




Use case	ID281 CO	ID281 Pro	ID230	ID Qube
QKD security testing and evaluation				x
High-performance QKD research	x	x	x	
Network and OTN integration research		x	x	
Academic courses and training	x			x

Clavis XGR QKD System at a glance

Model	Clavis XGR
KEY FEATURES USING BUILT-IN DETECTORS	
Maximum length of quantum channel (typ. @ 0.2 dB/km)	120 km (@ 24 dB, optional 150 km @ 30 dB)
Secret key rate	Typical 14'000 AES-256 Keys per hour @ 24 dB
Protocol	BB84 with decoy state
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 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	14 kg
Temperature range	Operating +5 to +40°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
External detectors	
Interfaces	Electrical interface: 3 x SMA connectors / optical interface: 3 x FC/UPC connectors
Supported detectors[3]	ID Qube, ID 230, ID281, ID281 Pro
Secret Key Rate using ID281 QKD detectors (typical)[4]	400 kb/s @ 12 dB
Dynamical Range using ID281 with spiral detectors (minimal)[4]	40 dB

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
[3] Support for other detectors on request.
[4] Check with the ID Quantique whether your ID281 fulfils the requirements.

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