Quantum Key Distribution is a technology that exploits a fundamental principle of quantum physics - observation causes perturbation - to exchange cryptographic keys over optical fiber networks with absolute security. It is attracting a growing interest in the scientific community. The ID3100/ID3110 Clavis$^2$ Quantum Key Distribution System - clavis is the latin word for key - was developed by id Quantique to serve as a versatile research tool.

The ID3100/ID3110 Clavis$^2$ system uses a proprietary auto-compensating optical platform, which features outstanding stability and interference contrast, guaranteeing a low quantum bit error rate. Secure key exchange becomes possible over distances of tens of kilometers. This optical platform is well documented in scientific publications and has been extensively tested and characterized.

The ID3100/ID3110 Clavis$^2$ system is the most flexible product of its kind on the market. It consists of two stations controlled by one or two external computers.

A comprehensive software suite implements automated hardware operation and complete key distillation. A powerful graphical log file analyzer is supplied to plot the evolution of key parameters and variables, allowing intuitive performance analysis. The software suite also includes a secure chat application using the keys generated by the ID3100/ID3110 Clavis$^2$ system to encrypt communications.

**KEY FEATURES**
- Autocompensating interferometric set-up
- Outstanding stability and contrast
- User-friendly
- Automated operation
- Comprehensive software suite
- Graphical log analysis tool, secure chat
- Flexible and open research platform
- Library for C/C++ programming
- Sync Out signals

**APPLICATIONS**
- Quantum cryptography research
- Pilot network deployment
- Novel protocols implementation
- Education and training
- Demonstration and technology evaluation
OPTICAL PLATFORM

The ID3100/ID3110 Clavis™ quantum key distribution system is based on an autocompensating interferometric set-up, which guarantees outstanding contrast and stability. Trains of light pulses are emitted by a laser and travel from QKDS-B to QKDS-A, where a qubit value is encoded, before they are reflected using a Faraday mirror back to QKDS-B. This two-way approach allows passive compensation for all fluctuations, both in the quantum channel and the interferometer. This technology is patented. The ID3100/ID3110 Clavis™ system also provides electronic synchronization signals to connect and synchronize external components and systems.

Before being reflected, the trains of pulses are stored in a delay line in the QKDS-A station in order to suppress Rayleigh backscattering induced noise. The ID3100 Clavis™ system and ID3110 Clavis™ system are equipped with a delay line of 12 kilometers and 24 kilometers, respectively.

The wavelength of the laser used in the ID3100/ID3110 Clavis™ system is stabilized to a value on the ITU grid. This wavelength is optionally over a range of 2nm.

CONFIGURATIONS

The ID3100/ID3110 Clavis™ stations consist of an optical and electronic platform and must be controlled by an external computer (important note: the computers must be ordered separately from ID Quantique or another supplier). The computers must run under a Linux Ubuntu distribution. The system can be operated in a single- or a double-computer configuration.

In the double-computer configuration, a management (classical) channel is required for system synchronization and key distillation. This classical channel is implemented over a TCP/IP connection over a local area network, the Internet or a dedicated optical fiber.

The computers can provide cryptographic key material to external encryption devices or applications through a dedicated interface.

Single-Computer Configuration

In the single-computer configuration, one computer is used to control both the QKDS-A and QKDS-B stations. Two programs running on the same computer are used to simulate two different devices. Although it does not allow key exchange to different locations, it is useful for testing and calibration purposes.

Double-Computer Configuration

In the double-computer configuration, a different computer is used to control each of the ID3100/ID3110 Clavis™ stations. This configuration allows remote operation of the system, and a management channel (TCP/IP connection) is required.

L – laser
C – circulator
Di – quantum detector
BS – beamsplitter
PBS – polarizing beamsplitter
β – phase modulator
BP – bandpass filter
VOA – optical attenuator
CD – classical detector
DL – delay line
α – phase modulator
FM – Faraday mirror
KEY DISTILLATION
After the raw key material has been exchanged, it is post-processed in order to reduce the information to which an eavesdropper could have access to an arbitrarily low level. In the ID3100/ID3110 Clavis² system, this post-processing is fully implemented and automated in order to allow secure key exchange. It consists of four main steps:
- **Sifting implemented both for BB84 and SARG04**
- **Key distillation**
  - Key reconciliation: Cascade algorithm
  - Privacy amplification: Wegman-Carter Strongly Universal Hashing
- **Authentication - Universal-hashing with One-Time Pad encryption**
- **Key material storage and management**

SOFTWARE SUITE
- **QKD Menu Application**
The QKD Menu application can be used to control and operate the ID3100/ID3110 Clavis² system. It provides access to all hardware parameters and allows the user to perform tasks ranging from system calibration to secure key exchange. The QKDMenu application is used to control both the QKDS-A and QKDS-B stations.
- **QKD Sequence Application**
The QKD Sequence application is a fully automated quantum key distribution program. It controls the ID3100/ID3110 Clavis² system and sequentially performs the tasks required for quantum key distribution (hardware monitoring, system synchronization, interferometric contrast measurement, raw key production and key distillation). This application stores the cryptographic key material produced in a key store, which can be accessed by other applications and external devices.
- **QKD Log Analyzer Tool**
The QKD Log Analyzer Tool is a program allowing the user to parse log files produced by the ID3100/ID3110 Clavis² system and to graphically display key parameters and variables in order to analyze their temporal evolution. The tool runs on any operating system (SUN Java Virtual Machine 1.6 or newer required). It can be used on the computers controlling the system or, alternatively, it can also be run on a third computer where a log file has been imported for off-line performance analysis.
- **QKD Device Access Library**
The QKD Device Access Library is a library of functions that can be used to program the ID3100/ID3110 Clavis² system in C/C++. It allows users to write customized programs accessing the system to perform the tasks required by quantum key distribution. The library includes functions ranging from low-level primitives allowing the user to read or set a particular hardware parameter, to high-level procedures for complete quantum key distribution. The library includes more than 50 functions, some of which are specific to one of the stations of the ID3100/ID3110 Clavis² system (QKDS-A or QKDS-B), while others apply to both. A comprehensive and detailed reference guide, as well as examples of source code, are provided.
- **QKD Secure Chat Tool**
The QKD Secure Chat Tool is a messaging application allowing the exchange of encrypted messages between computers connected to the stations of the ID3100/ID3110 Clavis² system. Encryption can be performed using the One-Time Pad and AES algorithms or can be disabled. The latter option is useful for data interception demonstrations. The encryption keys are exchanged using QKD and are retrieved from the ID3100/ID3110 Clavis² system.
ID Quantique
Geneva / Switzerland
T +41 22 301 83 71
F +41 22 301 83 79
info@idquantique.com
www.idquantique.com

Best-in-Class Performance

QUANTUM KEY DISTRIBUTION

GENERAL INFORMATION

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Min</th>
<th>Typical</th>
<th>Max</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions (L x W x H)</td>
<td>466 x 428 x 177 mm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rack mountable, space required</td>
<td>4U</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weight (QKDS-A)</td>
<td>16 kg</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weight (QKDS-B)</td>
<td>16 kg</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating temperature</td>
<td>10 °C</td>
<td>30 °C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relative humidity 1</td>
<td>0 %</td>
<td>80 %</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-operating temperature</td>
<td>-10 °C</td>
<td>60 °C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relative humidity 2</td>
<td></td>
<td>90 %</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1 operating @ 30°C
2 non-operating @ 40°C

RECOMMENDED COMPUTER SPECIFICATIONS

- USB 2.0 ports (one and two for single- and double-computer configurations respectively)
- RAM: 1GB
- Hard Disk: a minimum of 100MB of free space for software suite installation, additional space is needed when running the applications
- Linux Ubuntu distribution (supplied)

ORDERING INFORMATION

ID3100 Clavis2 quantum key distribution system, with delay line of 12 kilometers
ID3110 Clavis2 quantum key distribution system, with delay line of 24 kilometers

INTELLECTUAL PROPERTY NOTICE

This product is protected by US Patent No. 6,438,234. Other patents pending.

TECHNICAL SPECIFICATIONS

- **Hardware**
  - Optical platform: autocompensating interferometric set-up
  - Proprietary digital signal generation and data acquisition electronics
  - Random number generation: Quantis quantum RNG
  - QKDS-A: 2 x Quantis OEM components
  - QKDS-B: 1 x Quantis OEM components
  - Power supply: redundant, auto-sensing, 100-240 VAC @ 50/60 Hz
  - External computers (sold separately)

- **Interfaces and Inputs/Outputs**
  - Optical connector (front panel): quantum channel
    - Connector type: F3000/APC (compatible LC/APC)
  - Computer interface (front panel): USB 2.0 port
  - Output Sync Signal Connectors (front panel)
    - Connector type: BNC
  - QKDS-A: classical detector and phase modulator
  - QKDS-B: laser trigger and phase modulator
  - Power supply (rear panel): redundant

- **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)

- **Key Exchange**
  - Maximum transmission range: > 50 km
  - Secret key rate (ID3100 Clavis2): > 500 bps over 25 km
  - Secret key rate (ID3110 Clavis2): > 1000 bps over 25 km

- **Sifting and Key Distillation**
  - Fully automated sifting and key distillation
  - Sifting for BB84 and SARG04 both supported

- **Options**
  - Warranty extension (after first year)
  - Services (installation, training, on-site and remote support)
  - Computers with Linux OS and Clavis2 software suite installed
  - Optical fiber spools (various lengths available)
  - Optical powermeter
  - High-speed encryptors (Centauris - more information on www.idquantique.com)

Disclaimer
The information and specification set forth in this document are subject to change at any time by ID Quantique without prior notice. Copyright © 2014 ID Quantique SA - All rights reserved - clavis2 v2014 09 10 - Specifications as of July 2014