

QUANTUM SAFE SECURITY

CLAVIS³

新型量子密钥分发安全性 研究型操作平台

QKD量子保密通信是一种利用量子物理的基本原理来实现确保光纤网络保密信息交换的绝对安全技术

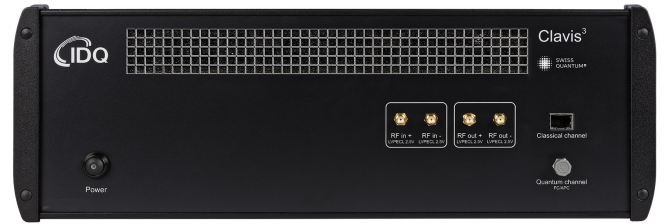


Figure 1: The Clavis³ receiver

QKD是完整加密系统的一个组成部分；包含：密码生成、密码更换和加密来确保量子密码的安全性；比如：密文将被严格保密以防量子计算机黑客的攻击；即使是对一台多功能的并能打破公共秘密体系的量子计算机而言仍然是一项艰巨的挑战；在这一领域的最新发展满足了量子密码安全性更高的要求；量子密码的时代已经开始了，其加密技术必须要配有量子计算机

因此QKD的研究也面临着紧迫性，因为无法等待用量子计算机来测试合适的加密方法的设计

这套Clavis3系统的名字取自拉丁文，由瑞士ID Quantique公司开发用于学术研究和工业应用上

这套Clavis3系统是作为一个研究平台而设计，可以自动或手动操作；用户可以根据不同的试验要求做参数设置；另外还有Clavis3接收器、Clavis3 B,可以使用外部的单光子探测器，这些可以由ID Quantique或用户自己来选择

可以实现在上百公里距离范围内的安全密码交换，即使是标准的WDM电信网络我们的这套光学平台已在多种学术刊物上转载并被广泛关注

全面的软件包可实现自动化硬件操作及密码蒸馏，提供的密码由Clavis3的不同加密系统，包含：ID Quantique公司提供的可以达到100 Gb/s layer 2 encryption的Centauris, CN8000 encryptor

上海沃埃得贸易有限公司

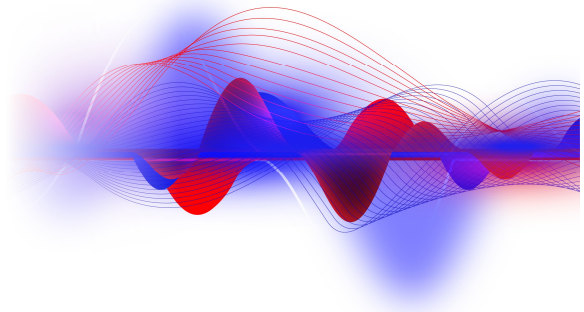
<http://www.worldwide-china.com>

上海市共和新路3699号共和国际A1707

电话：+86 21 66621556/7/8/9

邮箱：sales@worldwide-china.com





主要特点

快速生成密码, 1.25 GHz发射脉冲重复率
 由外部探测器可实现最大便捷性
 基于硬件关键处理(在一个FPGA), 可以提高密码分发率
 用户友好操作界面

手动和自动操作
 设计作为研究平台, 可以实现访问, 修改的可能性各种参数
 同步信号
 可以集成Centauris加密器, 获得一个完整的高速加密系统

主要应用

量子密码学的研究
 试验网络部署
 教育和培训
 用户友好操作界面来演示和技术评估

最佳方案

Clavis3密钥分发系统是基于Coherent-One-Way (COW) 协议, 是IDQ公司的专利产品。
 协议方案介绍见下图2流程图

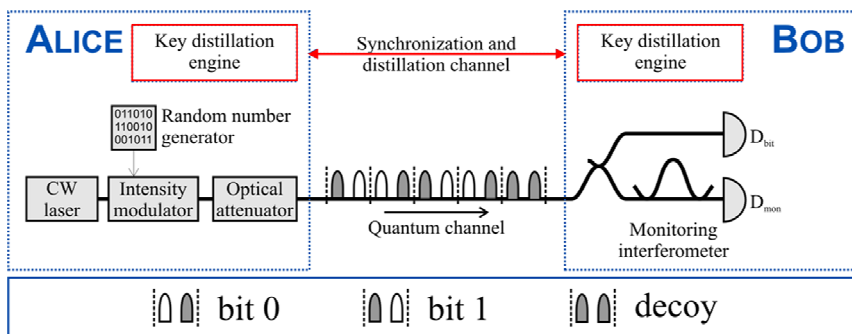
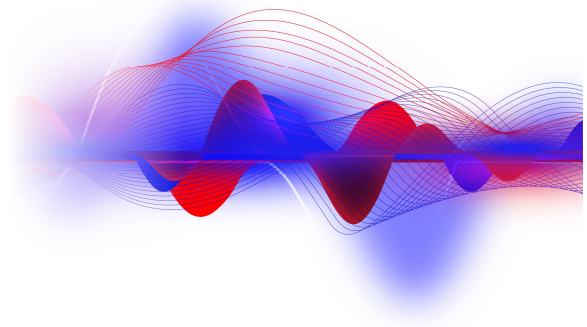


Figure 2: The COW optical scheme (see test for details)

发射器, Clavis3-A (ALICE) 包含一个激光发射连续波光束。
 随后调制光束, 提供一致的光脉冲, 二进制模式相应的0和1。
 然后脉冲衰减达到单光子中位数。这些脉冲从发射器Clavis3A量子信道到被探测的接收器Clavis3 B
 接收器, 一些脉冲到达产生密码的D bit探测器, 和而且一些脉冲穿过监测干涉仪和到达探测器D mon
 这些都是用于监视窃听

Clavis 3工作站提供电子同步信号连接和同步外部组件和系统。运用在Clavis3系统中的激光波长稳定在ITU网格值。



主要信息

参数

Dimensions (L x W x H) :	424 x 402 x 144 mm
19" Rack compatible ² ,	space required: 4U
Weight (QKDS-A)	10kg
Weight (QKDS-B)	10kg
Operating conditions:	
Temperature	10 to 30°C
Max relative humidity (@30°C)	80%
Non-operating conditions:	
Temperature	-10 to +60°C
Max relative humidity ³ ,(@40°C)	90%

推荐电脑配置

Ethernet connexion

RAM: 4GB

Hard Disk: a minimum of 100MB of free space for software suite installation, additional space is needed when running the applications

Processor: minimum Intel Core Duo

技术规格

硬件

Optical platform;

Proprietary digital signal generation and data acquisition electronics;

Random number generation: one Quantis QRNG⁴ OEM component in each station.

Power supply: 100-240 VAC @ 50/60 Hz

External computers (sold separately)

输入输出接口

Optical connectors (front panel):

Quantum channel

Connector type: FC/APC

Optical fiber type: SMF-28

Service channel:

Two SFP modules, with LC/APC connectors (for two-fiber configuration)

Or one bidirectional SFP module (for single-fiber configuration)

Computer interface (back panel): Ethernet

控制面板

Power LED indicator (red: on);

Quantum Link LED indicator (green: quantum channel active);

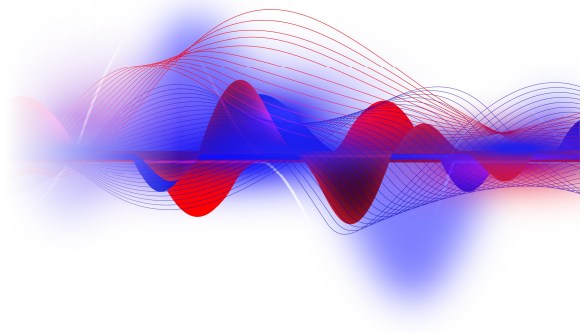
Data LED indicator (green: raw key exchange in progress).

Quantum Link LED indicator

² A tray is necessary

³ Non condensing

⁴ The random number generation rate is 4 Mb/s, which will be expanded to 1.25 GHz



密钥交换特征

Maximum transmission loss acceptable (typ.):	12 dB Standard
	18 dB Premium
	>18 dB Extra (upon availability)
Maximum length of quantum channel (typ.)	>100 km
Secret key rate ⁵ (typ.):	> 3 kb/s after 50 km
Sifting and Key Distillation: Hardware-based, fully automated sifting and key distillation	

标准选项

External detectors
 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 power meter
 High-speed encryptors (Centauris - more information on www.idquantique.com)

相关产品

单光子探测器（外部探测器配置）

ID210	InGaAs/InP gated photon detector with the lowest noise
ID230	InGaAs/InP free-running photon detector with the lowest noise
ID280	Supraconductor photon detector (need cooling at + 2.3 °K, not provided)

随机数发送器

Quantis — Quantum random number generators

网络加密

Centauris — High-speed layer 2 encryptors

订单信息

Clavis³ Quantum key distribution system

知识产权备注

This product is protected by US Patents No. US 7929690B2 and US 8995650B2. Other patents pending.

