IDQ

SWISS QUANTUM

Redefining Security

Cerberis³ QKD System

State-of-the-art Quantum Key Distribution

Companies have a growing need to exchange data over multiple networks, and to provide information-based services or applications for partners and clients in order to uphold a competitive position. Maintaining the confidentiality, integrity and availability of data without impacting network performance is a pre-requisite for today's information technology systems. However, optical fibre links and other data transport infrastructures constitute a potentially dangerous vulnerability in the IT infrastructure of an organisation. Mission critical data must be protected through encryption when travelling outside the secure perimeter of the company.

Simultaneously, in the next decade or so, the massive processing power of quantum computers will render much of the current encryption unsafe – and specifically the public key cryptography used for key exchange. The threat today is that hackers, ranging from powerful states to criminals, can already download data in transit, and then decrypt it offline – either by brute force attacks today, or by using known algorithms on a quantum computer tomorrow. This means that governments or enterprises, which must protect some classifications of data for over five or even ten years, have a limited time frame to move to quantum-safe crypto solutions. In order to ensure continued confidentiality, they need to deploy such quantum-safe solutions already today.

Key Markets

- Telecom and Networks Operators
- Financial Services Companies
- Governments and Defence
- Healthcare Organisations
- Critical Infrastructure
- IP-rich Enterprises

Key Benefits

- Provably secure key distribution
- Long-term data security
- Truly random key generation
- Fully automated key exchange with continuous key renewal
- Set & forget functioning
- Interoperability with network encryption provider

Cerberis³ QKD System

Quantum-Safe Security for today's applications

The Cerberis³ takes QKD to the next level: seamless integration with telecom and IT networks. It is designed as a network appliance, with monitoring and control abilities.

QUANTUM KEY DISTRIBUTION AND QUANTUM COMPUTING

Quantum Key Distribution (QKD) is a technology that exploits a principle of quantum physics – observation causes perturbation – to exchange cryptographic keys over optical fibre networks with provable security.

The principle of QKD is quite straightforward. According to quantum physics, the mere fact of observing a quantum object perturbs it in an irreparable way. Therefore, if one encodes the value of a digital bit on a single quantum object, a qubit, its interception will necessarily translate into a perturbation. This perturbation causes errors in the sequence of bits exchanged by the sender and recipient. By checking for the presence of such errors, the two parties can verify whether an eavesdropper was able to gain information on their key. QKD is used to generate two identical secure keys on the two ends of the channel. A Quantum Random Number Generator (QRNG) embedded in the QKD system guarantees that keys are produced in an absolute random way. Once the key exchange is validated, the keys can be used to encrypt data.

QKD – Also known as quantum cryptography – is the only known cryptographic technique, which can ensure quantum-safe security today. With QKD, encrypted messages will remain confidential against the power of a quantum computer. The design and realisation of a multipurpose quantum computer, which will be able to break existing public-key cryptography, remains a challenge. However, recent progress in this field means that governments, standards bodies and industries are starting to mandate quantum-safe encryption methods. The era of post-quantum cryptography, where cryptographic methods will have to be resilient to quantum computer, has already begun.

TECHNOLOGY

At the core, as explained above, QKD is a point-to-point technology. The two servers must be linked by a quantum channel, which transmits the necessary qubits. The quantum channel is preferably a dark optical fibre, in order to maximise the transmission distance[1]. It can also be multiplexed with other data channels on the same fibre, with restricted distance. Thanks to the modular structure of the Cerberis³ QKD, several systems can be aggregated in various ways, to provide a variety of network architectures. These architectures comprise:

> QKD backbones with a number of linked servers, known as Trusted Nodes. This linear structure provides long-distance key distribution.

> QKD rings, which offer redundancy in case of a failure of a single link.

> Point-to-multipoint structures, such as a star configuration, linking a central hub to several outlying nodes.

In most practical applications, the Cerberis³ QKD System autonomously generates, manages and distributes the secret keys to one or more encryption appliances. ID Quantique can provide its own Centauris high-speed Ethernet encryptor. QKD-ready encryption is being enabled by other major companies, notably leading OTN vendors. The standardisation of the interface between QKD systems and link encryptors is currently under way at the European Telecommunication Standardisation Institute (ETSI).

In practice, QKD is often combined with conventional key distribution techniques, such as RSA or ECC, to generate a dual key agreement. The resulting key is as secure as the strongest of the two original keys. Importantly, dual key agreement retains the existing certifications of the conventional system.

ID Quantique's Cerberis³ QKD System, combined with IDQ's Centauris high-speed Ethernet encryptors, guarantees long-term protection of data into the quantum era, when the massive processing power of quantum computers will break today's public key exchange mechanisms.

[1] For longer distances, and especially communication to satellites, free space optical communication is currently investigated. However, the Cerberis³ QKD System is dedicated to optical fibre communication.

Cerberis³ QKD System

Modularity is the key

The Cerberis³ is the first commercial QKD system, designed with a modular structure. It can accommodate a variety of network architectures. A single Advanced Telecommunication Computing Architecture (ATCA) chassis houses one or several Cerberis QKD Blades, and a Quantum Node Controller (QNC), for management & control.

MAIN APPLICATIONS

The Cerberis³ QKD System offers quantum-safe key distribution for:

> Point-to-point data center interconnections

> Metropolitan backbone optical networks

> Multipoint architectures

It is also a building block for extended quantum backbones (in conjunction with Trusted Node technology).

SYSTEM DESCRIPTION

The Cerberis³ QKD System is a modular QKD system, which comprises the following components:

> An ATCA chassis, where various ATCA format blades will be inserted. One chassis is needed at each QKD node;

> One or several QKD Blades, either a transmitter (Alice) or a receiver (Bob), which distribute the keys over the quantum channel;

> A Quantum Node Controller (QNC) distributes the keys to the link encryptors or to various key user entities in the node. For QKD backbones, the QNC is also used as a Trusted Node Controller, which allows keys to be forwarded securely over the full backbone;

> A switch for network connection

The Cerberis³ QKD System can accommodate different key distribution architectures and topologies, including: backbone for long-distance key distribution with trusted nodes; ring for redundant local distribution, star for distribution from a central location to local branches. The size of the ATCA chassis at each quantum node can be adapted to the needs, to deliver the required functionalities.

The Cerberis³ is the latest generation of QKD systems at IDQ, based on 16 years of experience in the development and commercialisation of quantum-based products.

SELECTED USE CASES

Financial Services: 10G encryption with QKD for disaster recovery

Since 2010 IDQ's quantum cryptography has been deployed on the data center interconnect of a leading Swiss bank. The solution comprises IDQ's Cerberis QKD servers, which provide quantum-safe encryption keys into redundant 10G Ethernet encryption devices provided by Safenet-Gemalto. The QKD solution was implemented to protect long-term sensitive client data.

Government Central Bank: Quantum Safe links for MAN

In 2017 a Central Bank tested and validated the use of IDQ's QKD on its production link, integrated with 100G encryption system. The bank validated deployment of the system to protect the critical data passing between the different bank offices in the Metro Area Network. In 2018 the first link went live, with an additional 3 links planned for 2019.

Geneva Government: Securing the DCI with QKD

In 2007 the Canton of Geneva deployed the world's first QKD system on its data center interconnect link, to protect the integrity of the federal votes between its main data center and the vote counting center. In 2017 the decade-long use of the first commercial QKD system made another world record.

Cerberis[3] QKD System at a glance

Model	Cerberis[3]
KEY FEATURES	
High speed key generation	1.25 GHz pulse repetition rate
High speed hardware-based key processing, to distill the secret keys	✓
Key distribution protocol (see Note below)	COW
Key security parameter[1]	$\varepsilon_{QKD} = 4.\ 10^{-9}$
Maximum transmission loss (typ.)	12 dB Standard
Maximum length of quantum channel (typ.)	50 km
Secret key rate (typ.)	3 kb/s after 50 km
PHYSICAL PARAMETERS	
ATCA Chassis	6 slots available
Small footprint for QKD Blade	2-slot ATCA blade
Dimensions[2]	Integrable into 19'' rack; 6U height; 13'' depth
Weight for one node[3]	25 kg
Operating conditions	
Temperature	10 to 30°C
Max relative humidity (@30°C)	80% (non condensing)
Non-operating conditions	
Temperature	-10 to +60°C
Max relative humidity (@40°C)	90% (non condensing)

[1] The key security parameter characterises quantitatively the quality of the distributed keys. Technically, it is defined as the probability that the key distillation process went wrong, with either an error or at least one bit of the key leaked to the eavesdropper. It is normally calculated over a large block size, to allow an efficient distillation process. 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 for example: https://doi.org/10.1088/1367-2630/16/1/013047

[2-3] For a typical installation with the ATCA chassis, the QNC and one QKD blade.

Note: The COW protocol

The Cerberis[3] is based on the Coherent One-Way (COW) protocol, designed in collaboration between the University of Geneva and IDQ.

The protocol is designed with the following key requirements in mind:

• Simplicity of the optical engine: COW only uses a restricted number of standard telecom grade optical components. The receiver is entirely passive, and the transmitter comprises a single active amplitude modulator. This ensures a high reliability of the optical system, as well as a clear path to lower costs of manufacturing.

• Ease of integration into standard optical networks: the quantum channel (over which keys are transported) is a standard optical link. It does not require any specific adaptation (such as polarisation control). The Blades are connected at each end of the channel, and only need synchronisation to distribute keys.

• Stability: the parameter used for key transmission is the time of detection (0's or 1's differ by their relative timing). Small changes in the optical link (which may modify the polarisation or phase of the qubits in other protocols) have no influence on the transmission. The translates into a high stability, low bit error rate, and high reliability of the system.

These features represent significant advantages for real-world applications of QKD in terms of installation, maintenance, and total cost-of-ownership.

ID Quantique

Chemin de la Marbrerie 3,
1227 Carouge/Geneva Switzerland

T +41 22 301 83 71
F +41 22 301 83 79
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 organisations globally.

IDQ also commercialises 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.