QUANTUM-SAFE SECURITY

Building a trusted future through quantum technologies

Pejman Panahi
Senior Director, Global Market & Business development

17/03/2021
ID Quantique

Founded in 2001
Geneva, Switzerland
Seoul, South Korea
Boston, USA

100+ employees, including 50 engineers/scientists

By 4 quantum physicists from the University of Geneva

Develops technologies and products based on quantum physics within 2 business units:

- Quantum-Safe Security
- Quantum Sensing

Performs R&D, production, professional services, integration, support

Clients: Governments / Banks / Gaming Industry / Universities / IT Security

Investments in 2018 by SK Telecom & Deutsche Telekom
ID Quantique

The world leader in Quantum Randomness and Quantum-Safe Security

- **2001**: World’s first Quantum Random Number Generator
- **2007**: World’s first real-world QKD implementation to secure Geneva’s elections
- **2016**: IDQ’s third generation of QKD
- **2018**: Launch of the Quantis QRNG chip
- **2019**: SK Telecom apply QKD technology to its 5G network
- **2020**: World’s first 5G smartphone equipped with a QRNG chipset
ID Quantique celebrates its 20 years anniversary
Quantum funding: Public investments

More than a quantum race, the world is building a global ecosystem around quantum technologies.
QUANTUM RANDOM NUMBER GENERATION
Feed your security systems with quantum randomness

The security of any cryptographic system is determined by the security of its keys...

*Which rely on random numbers.*

Getting the foundation right is crucial.

The solution? *Quantum Random Number Generation (QRNG)*

QRNG is the only solution offering provable entropy thanks to the laws of quantum physics which makes it invulnerable to prediction or bias.
The Quantis family

Quantis Chips
IDQ6MC1
IDQ20MC1
IDQ250C2

Quantis Modules
USB 4M
PCIe 4M
PCIe 16M
PCIe 40M
PCIe 240M

Quantis Appliance 2.0
IDQ brings a new level of Quantum enhanced phone security allowing differentiated security solutions for ICT services.

Phone Applications and Services use Security Algorithms

- Pay Services
- Cryptocurrency services
- Identification services
The Quantum decade has begun
Quantis QRNG chip integrated into Vsmart Aris 5G smartphones

- Enhanced security of user data
- Unique differentiation through a much higher level of trust to users
- Basis for new revenue streams especially in combination with e-sim and quantum-secured datacenters

Quantum-enhanced security at your fingertips
QUANTUM KEY DISTRIBUTION
Industries benefiting from QKD

- Government & Defense
- Financial services and Banks
- Telco & MSP
- Healthcare & Pharma
- Datacenter & Cloud
- Critical Infrastructure
Clavis³ QKD Platform

Clavis³

Quantum Key Distribution for academic and research labs

- Open QKD platform for R&D applications
- Interface to external detectors
- Interface to external encryptors
- User interface for technology evaluation and testing
Cerberis³ QKD System

Cerberis³

Quantum Key Distribution for enterprise, government and telco production environments

- Complex network topologies (ring, hub and spoke)
- Interoperability with major Ethernet and OTN encryptors
- Easy integration in any data center
- Centrally monitored solution
- Multiplexing of all channels on single fiber for metropolitan area. DWDM
Clavis\(^{300}\) Quantum Cryptography Platform

**Clavis\(^{300}\)**

Integrated QKD & LEA Encryption System

- 6U 19” chassis
- Key distribution protocol BB84+ decoy
- Transmission loss (typ.): 18db
  (longer range available upon request)
- Secret key rate (typ.): 10 kb/s after 50km
- Point to Point Relay Node configuration
- Embedded high speed LEA L1 encryptor
QUANTUM KEY DISTRIBUTION

Use cases and Applications
Secure data center interconnect

Point-to-Point QKD combined with L1 to L4 encryption

- Hybrid approach
- Generate highly secret keys
- Secure daily backup & database replication
- Assure business continuity and protect against data loss
Integrating QKD with existing encryption solutions

IDQ works with different network encryption solutions which may be upgraded with QKD to be Quantum-safe

Benefits of overlaying QKD:

1. Securing your organization in the post-quantum era
2. Reaching long-term confidentiality and aiding data integrity
3. Improving the TCO & ROI of your incumbent encryption solution
4. Acting as a ‘value-add’, demonstrating your cybersecurity commitments to stakeholders

Supported/PoC Vendors

- SSL VPN
- SSL/TLS
- IP VPN
- IPSec
- MPLS VPN
- Ethernet VPN
- MACSec
- OTN/WDM encryption

Available soon
Secure data center interconnect – OPEN QKD

ADVA FSP3000 (5TCE card) 10 Gbps Encrypted with AES-256

IDQ Cerberis3 - Alice

Primary Datacenter

Quantum Channel & Service Channel

IDQ Cerberis3 - Bob

Backup Datacenter

ADVA FSP3000 (5TCE card)

Standard Interface (ETSI REST API - QKD 0.14)

Standard Interface (ETSI REST API - QKD 0.14)
The Quantum Vault

Principle:

1. Generate keys with QRNG
2. Use Shamir Secret Sharing for distributed safe storage
3. QKD for secure transmission
4. 3 out 5 nodes needed to recover the key

Ultimate security for digital assets custody
QKD on a 5G network

QKD implemented in SK Telecom network in 2019

SKT applied QKD to Sungsoo-Dunsan section of its LTE and 5G network to prevent hacking.

Cryptography based on QKD

Bundang  Ansung  Chengju  Yeongdong  Gimcheon

Sungsoo Core  QKD Trust Repeater*  Dunsan Core  QKD Trust Repeater*  Taepyeong Core

Up to 221 km  Up to 109 km
The two companies will protect major areas of public networks with QKD on a section of up to 2000 km. It will constitute the largest operational QKD network in the world outside of China.

Across a communication network of 48 government organizations, including the Ministry of Employment and Labor, the Ministry of Economy and Finance, the Ministry of Education and local governments.

The National Convergence Network Project will strengthen security and stability, as well as increase the efficiency of the operation and budget of national institutions.

IDQ and SK Broadband selected for the construction of the first nation-wide QKD network in Korea.
QKD on a telecom network

Implementation of UK’s ultra-secure Quantum Network Link

New high-speed link that uses over 125km of standard BT optical fiber between Cambridge and Adastral park.

Worked with BT, Uni York & Uni Cambridge for deployment of system

QKD interfaced with ADVA’s FSP 3000 encryption

Works with Trusted Nodes for distance extension

Uses single fiber multiplexing quantum and data channels

Long distance QKD with Trusted Nodes
ID Quantique

Quantum. Trust enabled for the future

info@idquantique.com | www.idquantique.com

ID Quantique

Founded in 2001

3 Product lines:
1. Quantum Random Number Generation
2. Quantum-Safe Security
3. Quantum Sensing

High-quality engineering
Best-in-class performance
Trust
Operational simplicity