OpenQKD
European Quantum Key Distribution Testbed

Florian Fröwis

Helsinki, December 2019

ID Quantique company profile

Founded in 2001

By 4 quantum physicists from the University of Geneva

Geneva, Switzerland
Seoul, South Korea
Bristol, UK
Boston USA

95 employees including ~45 engineers/scientists

Investments in 2018 by SK Telecom & Deutsche Telekom

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

- Quantum-Safe Security
- Quantum Sensing

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

Clients: Governments / Banks / Gaming Industry / Universities / IT Security / O&G / Telecom

Cryptographic Toolbox: Simplified Overview

Symmetric Cryptography
(secret key)

Asymmetric Cryptography
(public key)

Cryptography before and after Quantum Computing

SWISS QUANTUM

OPEN QKD

The hacker’s point of view today…

… and after the
Quantum Computer

IDQ Recommended Path to Quantum Safety

Quantum Random Number Generation (QRNG)

- ✓ **Instantly strengthen your crypto key material**
- ✓ Feed higher quality (Swiss trusted) entropy into key generation servers, HSMs, Linux & crypto applications and connected devices

Crypto agility to move to Post Quantum Crypto

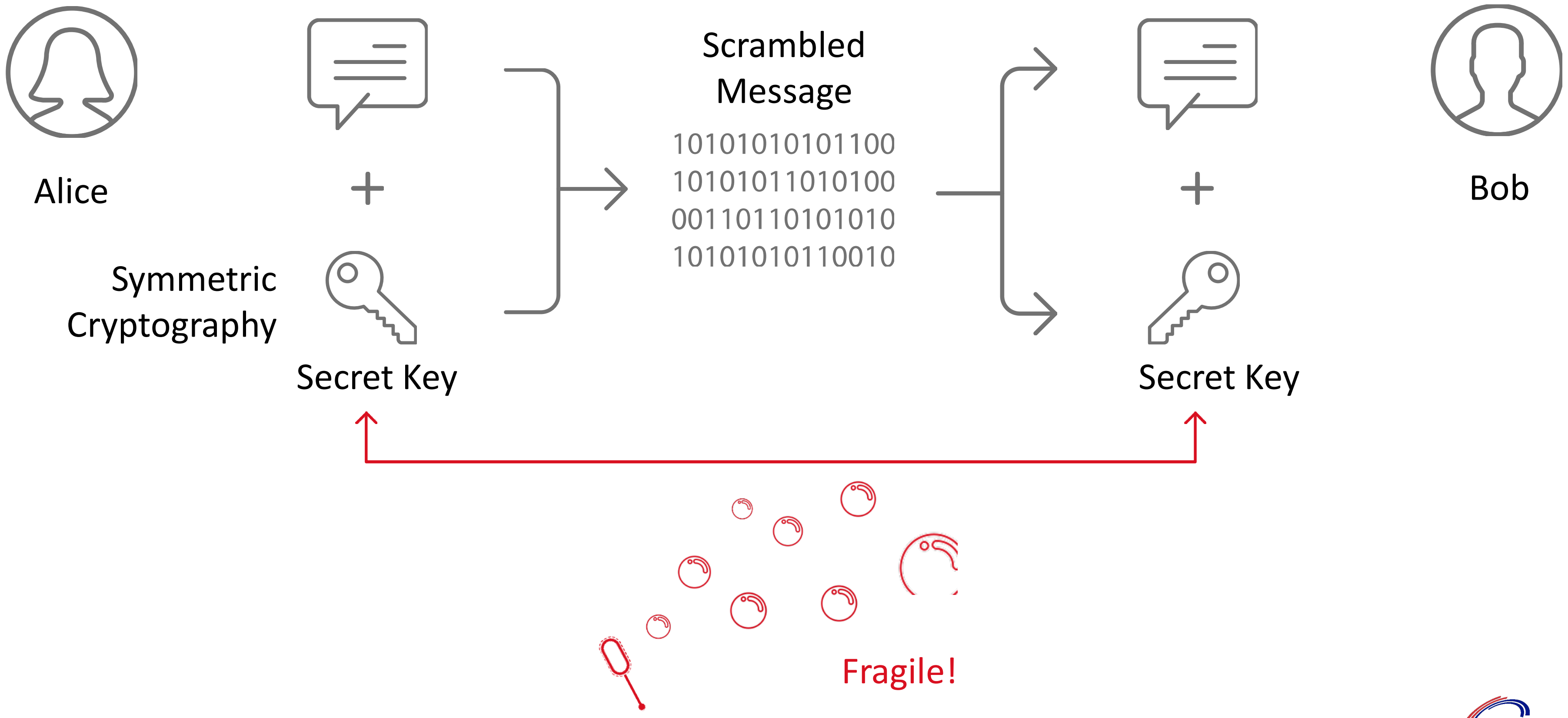
- ✓ Be **crypto-agile** to move to next generation Post Quantum Crypto
- ✓ Be **QKD ready** (ready to upgrade to quantum cryptography)
- ✓ Protect your investments for the next decade and further

1000
1100
10000

Quantum Key Distribution (QKD)

- ✓ **Quantum Cryptography** for secure transmission
- ✓ Provide forward secrecy & anti-eavesdropping of private key exchange/back up
- ✓ Ensure **Information Theoretic Security** for confidentiality to guarantee ownership for the next decade (Post-Quantum era)
- ✓ Use QKD today for backend **IP protection**

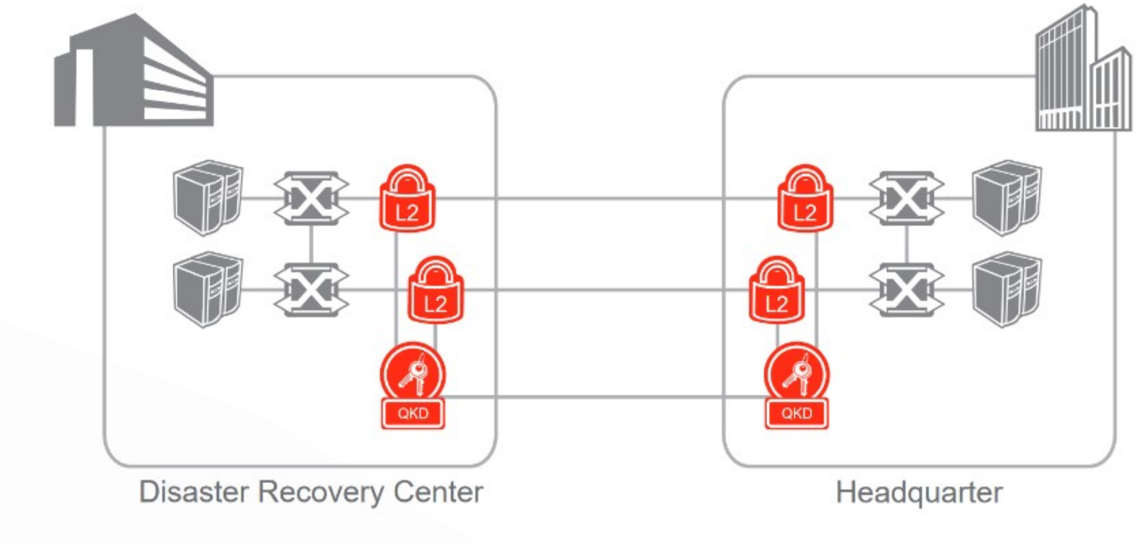
Quantum Key Distribution (QKD): Basic Idea



QKD in Data Center Interconnect

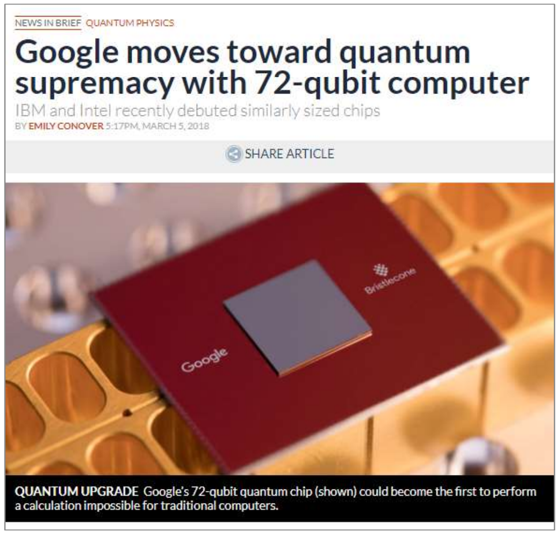
Quantum Cryptography-secured data center link

- Business need
  - Atos (ex Siemens) acted as managed service provider for a leading financial client
  - Needed to secure DC - DC link for critical information



ID Quantique PROPRIETARY

Market Turning Point in 2015-2016



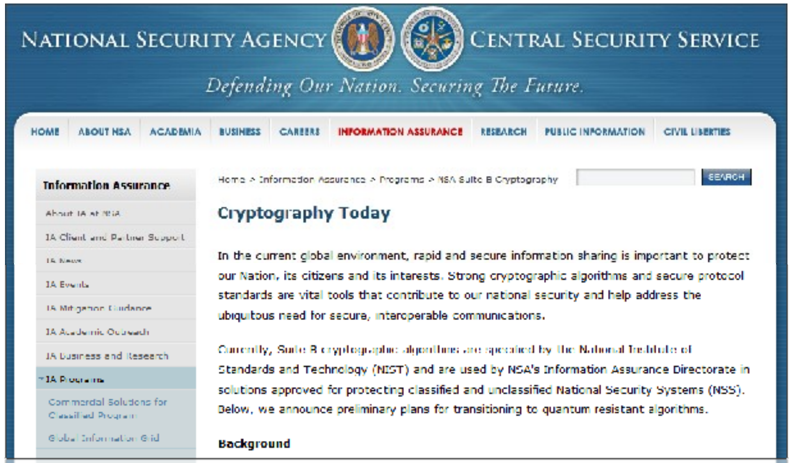
NEWS IN BRIEF QUANTUM PHYSICS

Google moves toward quantum supremacy with 72-qubit computer

IBM and Intel recently debuted similarly sized chips

BY EMILY CONOVER 5:17PM, MARCH 5, 2018

QUANTUM UPGRADE Google's 72-qubit quantum chip (shown) could become the first to perform a calculation impossible for traditional computers.



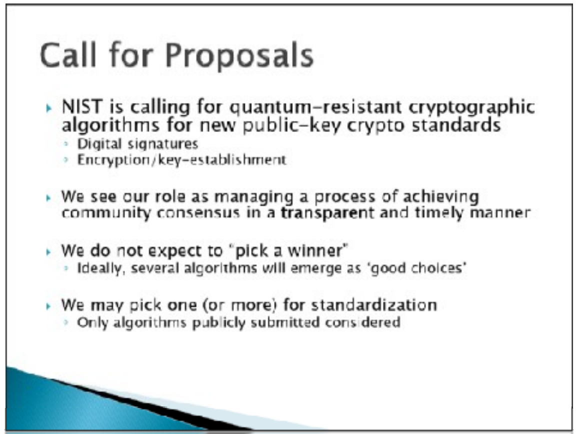
Cryptography Today

In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure, interoperable communications.

Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.

Background

"We announce preliminary plans for transitioning to quantum resistant algorithms to provide security against a potential quantum computer" - Aug. 2015



Call for Proposals

- NIST is calling for quantum-resistant cryptographic algorithms for new public-key crypto standards
  - Digital signatures
  - Encryption/key-establishment
- We see our role as managing a process of achieving community consensus in a transparent and timely manner
- We do not expect to "pick a winner"
  - Ideally, several algorithms will emerge as 'good choices'
- We may pick one (or more) for standardization
  - Only algorithms publicly submitted considered

China and CAS Quantum Network

SWISS QUANTUM

National Quantum Secure Communication Backbone Network (Phase I, 2018~2020)

Coverage area

Total Distance: ~ 11000 km

Backbone network: ~ 8000 km

City access network: ~ 3000 km

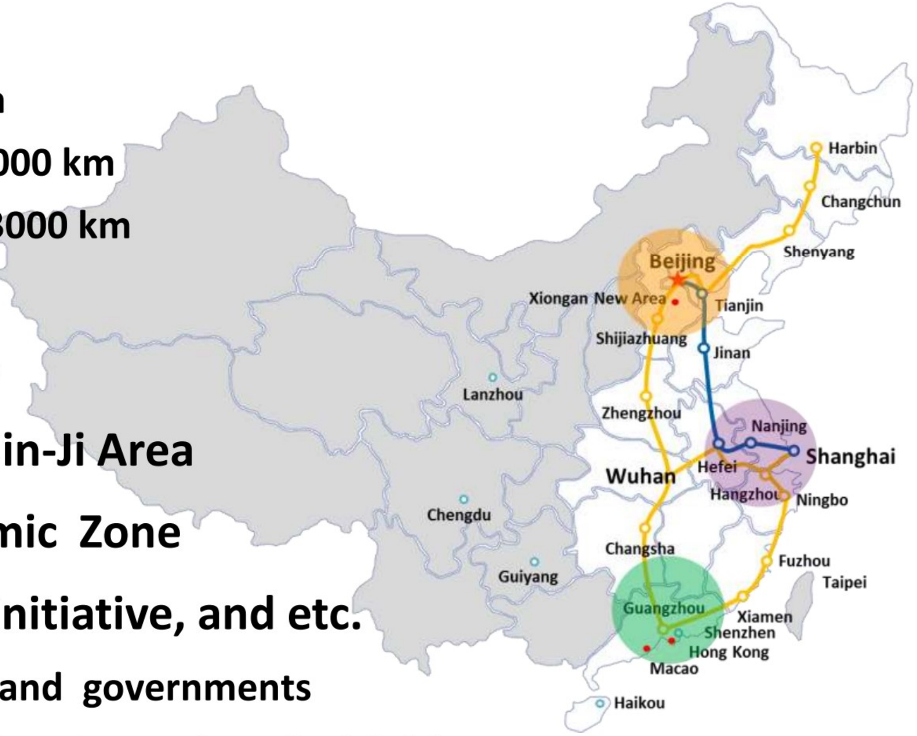
Main function

Serve for national strategy

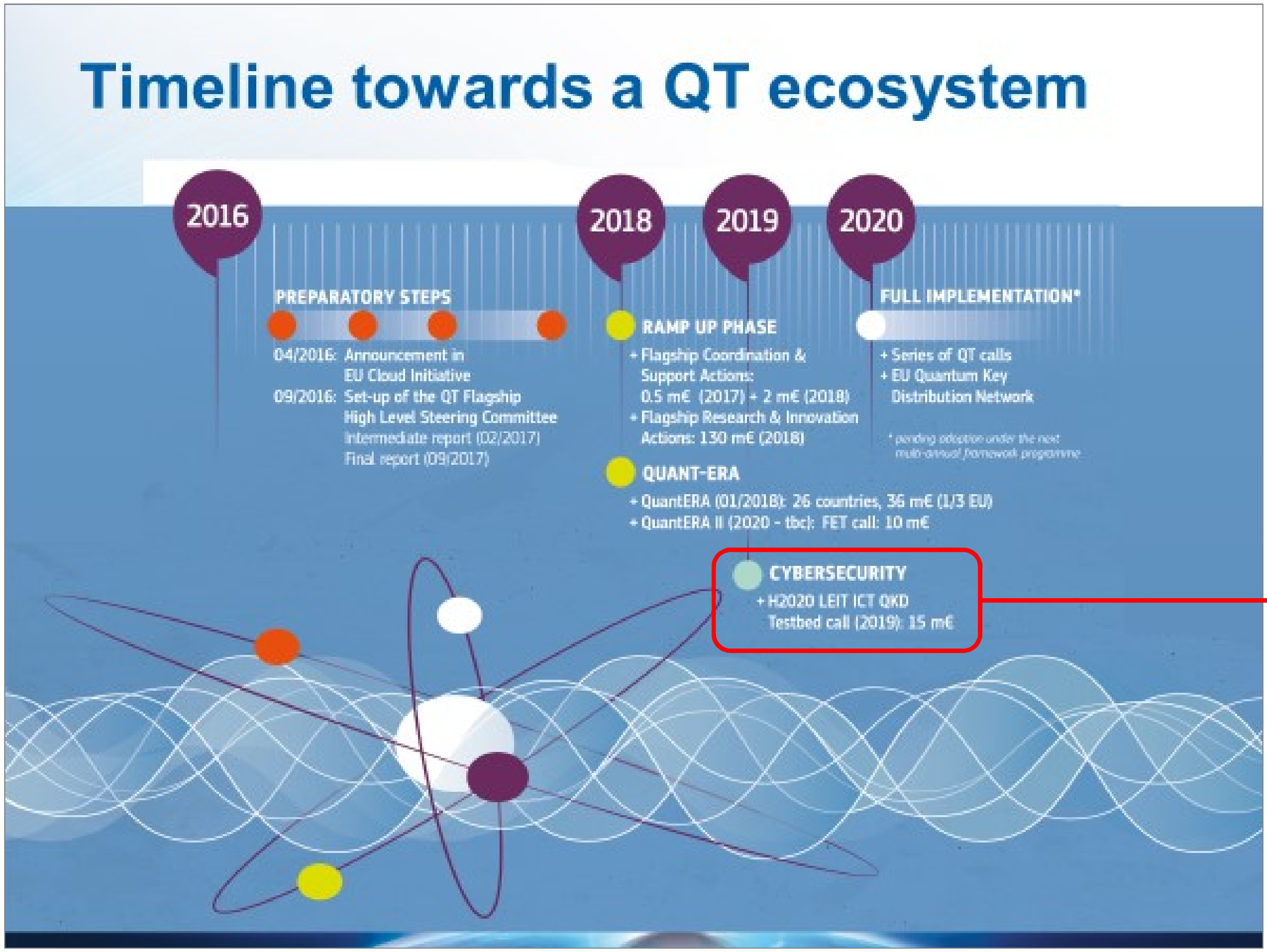
- Integration in Jing-Jin-Ji Area
- The Yangtze Economic Zone
- The Belt and Road Initiative, and etc.

Serve for financial sectors and governments

Explorer applications in education and medical fields



QT Vision in Europe



Timeline towards a QT ecosystem

2016

PREPARATORY STEPS

04/2016: Announcement in EU Cloud Initiative

09/2016: Set-up of the QT Flagship High Level Steering Committee
Intermediate report (02/2017)
Final report (09/2017)

2018

RAMP UP PHASE

- Flagship Coordination & Support Actions: 0.5 m€ (2017) + 2 m€ (2018)
- Flagship Research & Innovation Actions: 130 m€ (2018)

QUANT-ERA

- QuantERA (01/2018): 26 countries, 36 m€ (1/3 EU)
- QuantERA II (2020 - tbc): FET call: 10 m€

2019

CYBERSECURITY

- H2020 LEIT ICT QKD Testbed call (2019): 15 m€

2020

FULL IMPLEMENTATION*

- Series of QT calls
- EU Quantum Key Distribution Network

* pending adoption under the next multi-annual framework programme

Quantum Flagship (qt.eu)
1B€ for Quantum Technologies
(2018-2027)

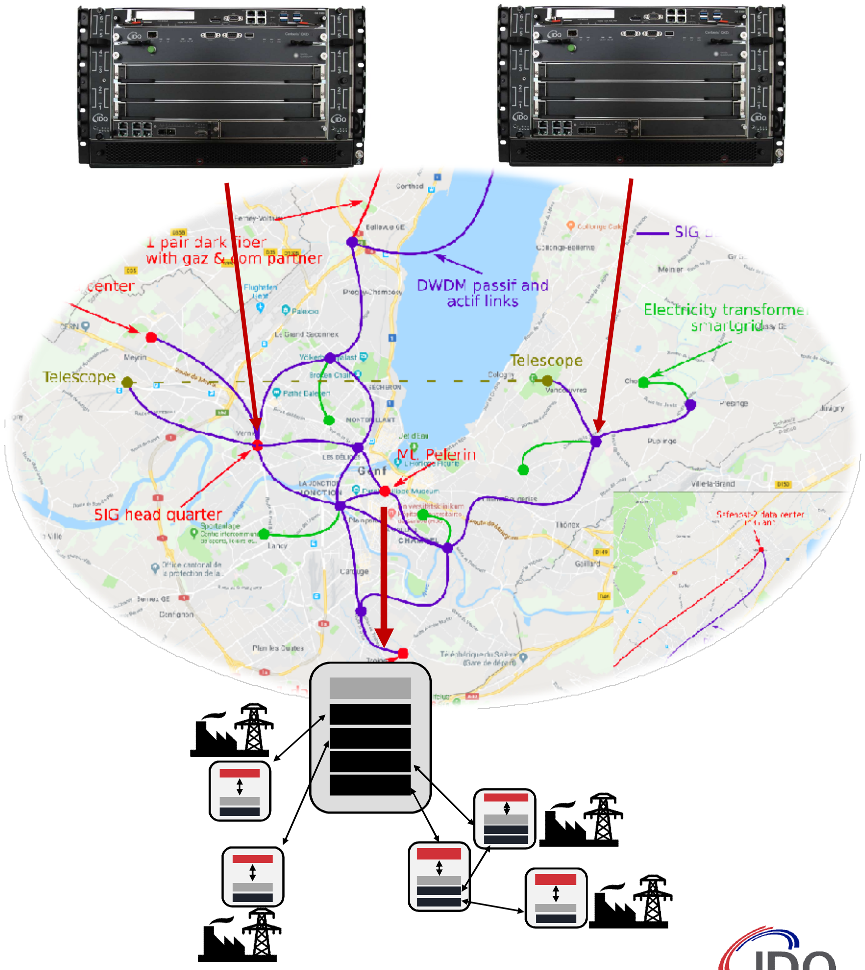
Testbed – 15M€ - 2019-2022

Scope of OpenQKD

SWISS QUANTUM

OPEN KD

- System development
- Network integration
- Use case testing and evaluation
- Further objectives
  - Innovation for European QC ecosystem
  - Collaboration and open source solutions
  - Prepare pan-European quantum communication infrastructure



ID Quantique PROPRIETARY

IDQ

Improvements on system level

Fibre-based: high TRL

- Cost of ownership I:
  - Smaller
  - Cheaper components (integrated photonics)
  - "Plug and play"
- Increase of distance from ≈50km to ≈150km
- Increase rate from kb/s to Mb/s
- Device independent

Free-space: low TRL

- Proof of concept

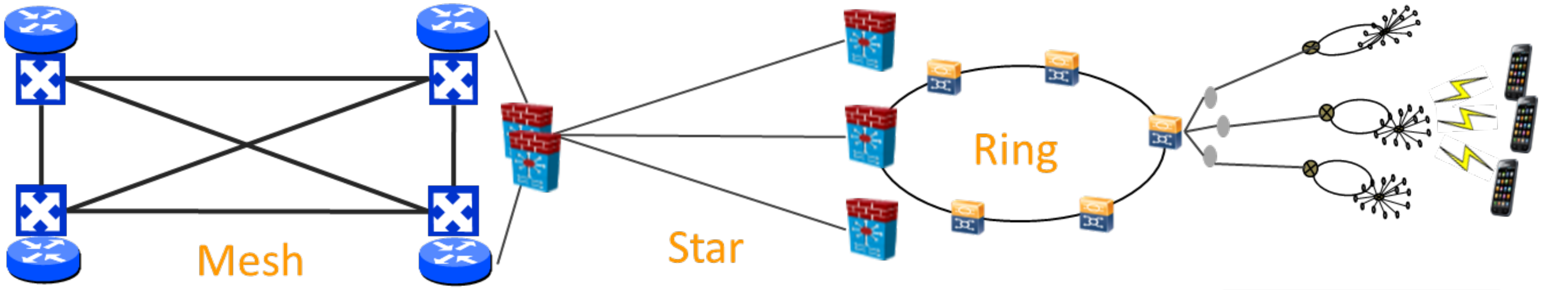
Cerberis 3: COW protocol,
ATCA chassis

Quantum Access Network (Short-Range)

- 19" 6U chassis
- Maximum transmission loss (typ.): 12dB (Premium 18dB upon availability)
- Secret key rate (typ.): 3 kb/s after 50 km

Modern communication networks

Backbone | Core | Access



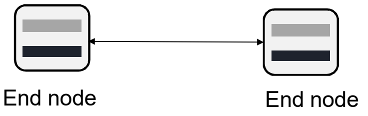
SK telecom

Quantum Key Distribution

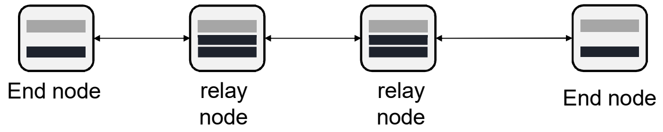
5G standard security & QRNG

Examples of QKD network topologies

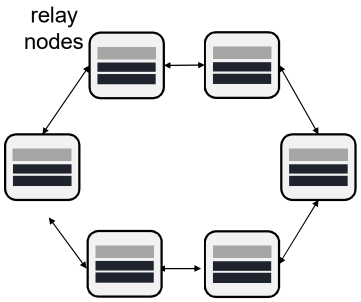
Point to point



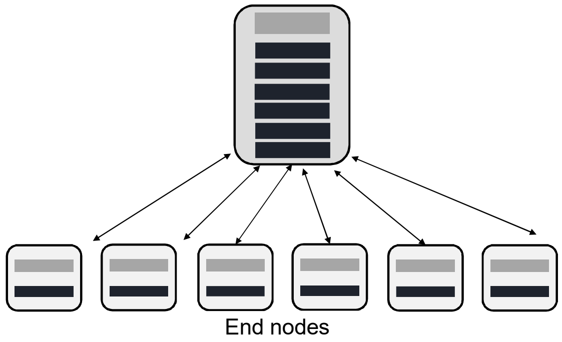
Point to point (with relay for long distance)



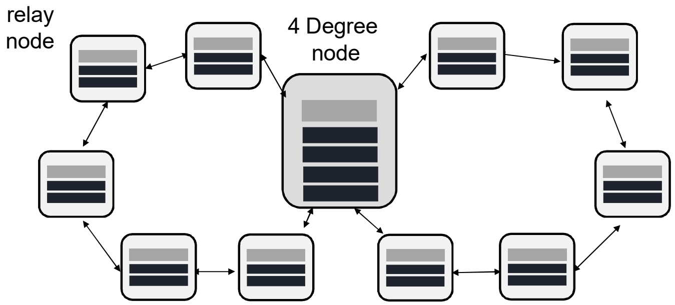
Ring network



Hub and spoke



2-Ring network



■ Optical blade (Alice or Bob)- 2U

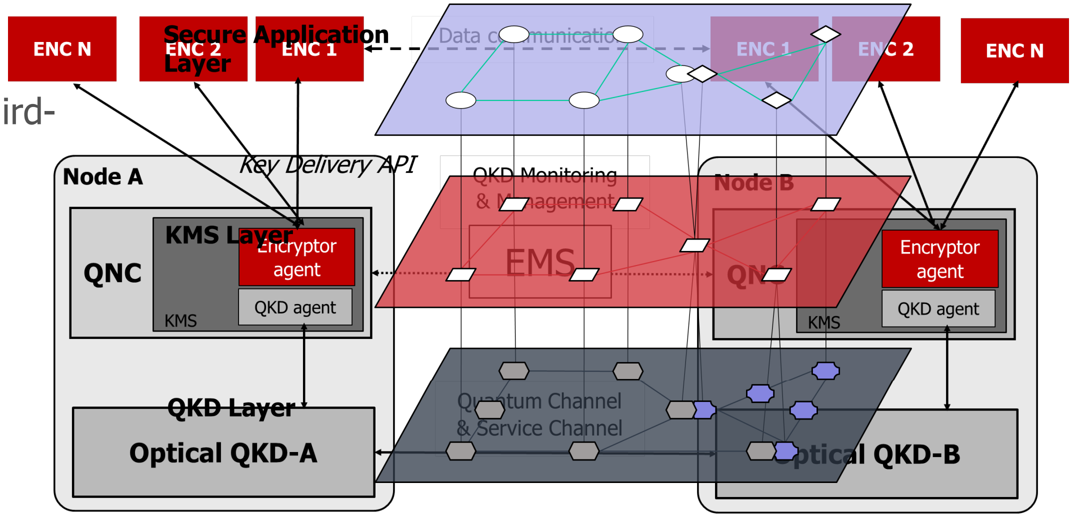
▒ KMS blade -1U

⟷ Quantum channel (dark fiber or wavelength in O-band)
KMS Channel (logical mux possible)
Service channel (C-band)

▢ QKD location (node), One KMS per node.
May host several 6U-chassis depending on degree (number of optical blades)

Network integration

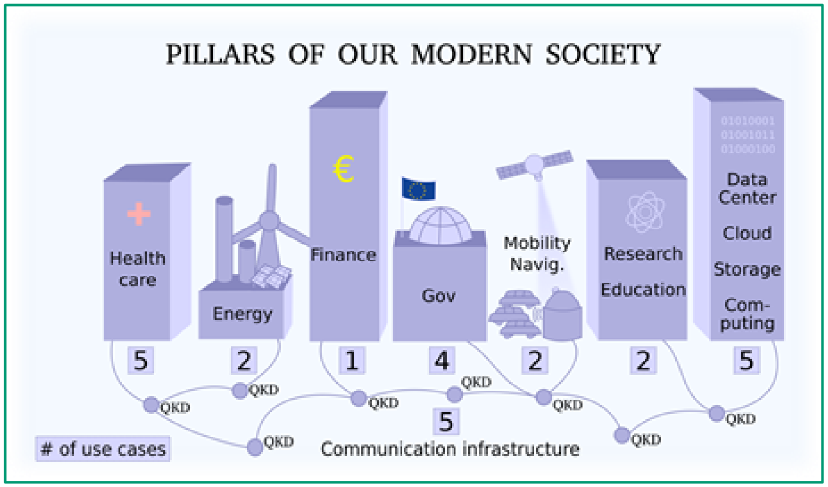
- Total cost of ownership II:
  - Multiplexing of QKD signals on fibres with third-party traffic
- Interoperability
  - Between QKD and encryptors
  - Between QKD links from different vendors
- →Standards
- Key management system → SDN
- 5G (network slicing, …)
- Different network topologies



Use cases

Operation of use-cases deriving from Secure Societies needs

- Demonstration of more than 30 use-cases for QKD featuring:
  - realistic operating environments
  - end-user applications and support



Range of use-cases:

- Secure and digital societies
  - Inter/Intra datacenter comm., e-Government, High-Performance computing, financial services, authentication and space applications, integration with post-quantum cryptography
- Healthcare
  - Secure cloud storage services and securing patient data in transit
- Critical infrastructure
  - QKD for telecom networks, 5G infrastructure and securing smart grids

Open Calls!!!

Use case example

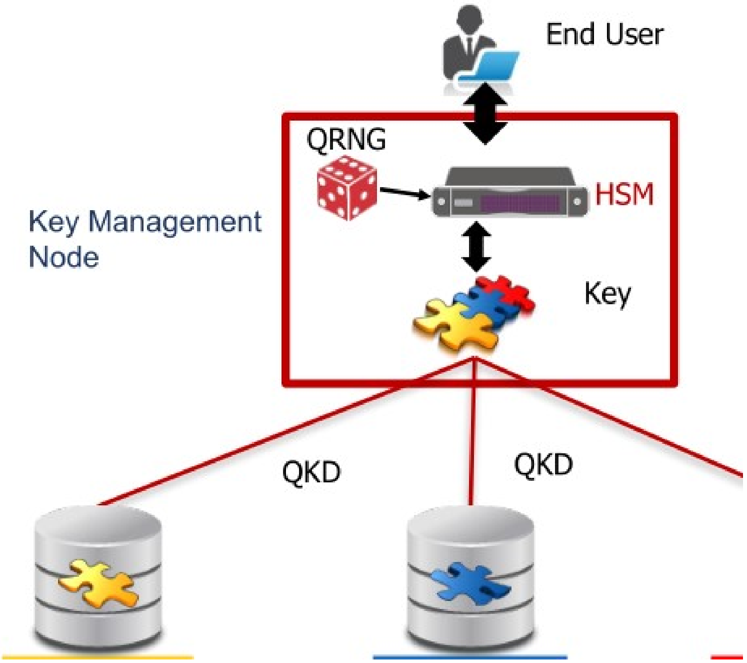
Quantum Vault (deployed in Geneva)

- End User wants to securely store a cryptographic asset: protecting against failures and attacks

- Key enabling technology
  - Quantum Random Number Generation (QRNG) to guarantee a perfectly random and unpredictable key
  - Shamir Secret Sharing Protocol for secure backup without duplication of the asset; protecting against single point of failure
  - Quantum Key Distribution (QKD) to distribute key elements

- Implementation partner: Mt Pelerin ("blockchain bank")

- Role of IDQ
  - Co-development of use case
  - Provision of QRNG and QKD systems
  - Consulting and technical support



OPENQKD eco system

SWISS QUANTUM

OPEN KD

- QKD suppliers

IDQ FROM VISION TO TECHNOLOGY TOSHIBA

- QKD R&D partners

MAX PLANCK INSTITUTE for the science of light

NOKIA Bell Labs ÖAW ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN LMU LUDWIG-MAXIMILIANS UNIVERSITÄT MÜNCHEN UNIVERSITÉ DE GENÈVE DTU

AIT AUSTRIAN IN iXblue PHOTONICS ICFO cnrs TU Delft

- QKD network developers

INSTITUT POLYTECHNIQUE DE PARIS 800 1222-2022 ANNI UNIVERSITÀ DEGLI STUDI DI PADOVA POLITÉCNICA

- Suppliers of network encryption

ROHDE&SCHWARZ fragmentiX® QUANTUM SAFE STORAGE SOLUTIONS THALES ADVA™

- Fiber infrastructure operators

UNIVERSITY OF CAMBRIDGE SIG PSNC

citycom we c the v imdea instituto madrileño de estudios avanzados

- Telecom operators

T BT Telefonica orange™

- Aerospace and satellite industry

DLR ThalesAlenia Space

- Standardisation institutes

DIN NPL National Physical Laboratory QMI Quantum Metrology Institute

- Early adopters

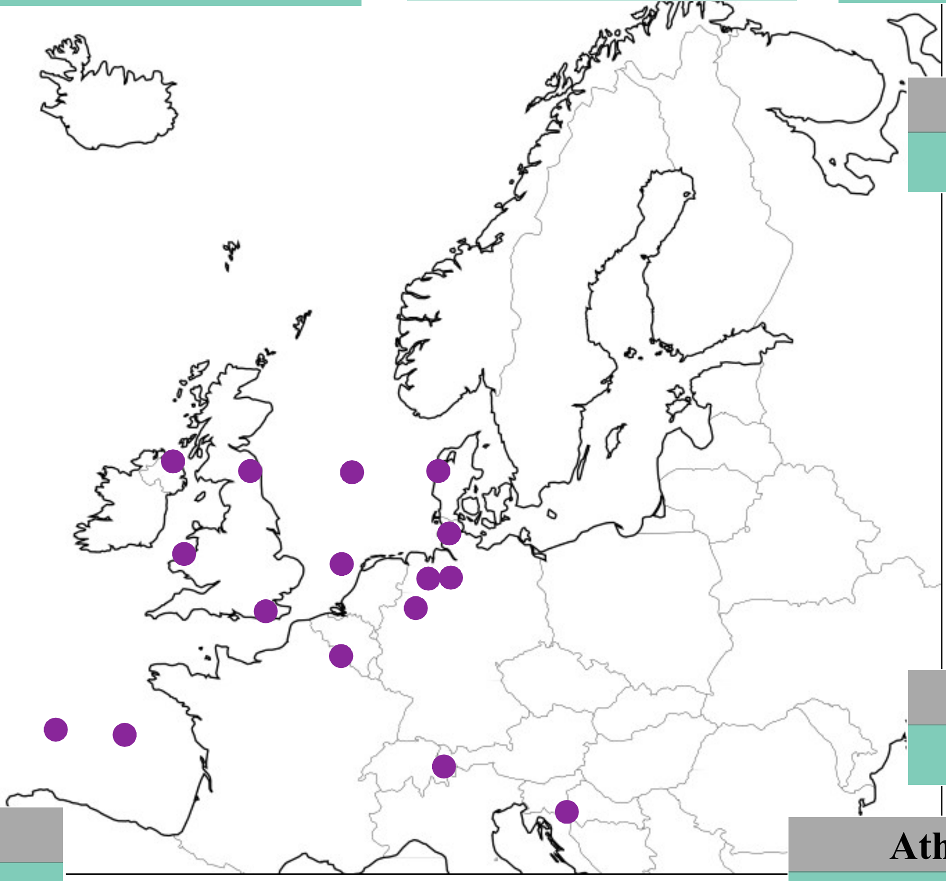
Medical University of Graz Mt Pelerin

VSB TECHNICAL UNIVERSITY OF OSTRAVA Mellanox® TECHNOLOGIES

IDQ

ID Quantique PROPRIETARY

16 OPENQKD test sites



Madrid ES
Telecom

Berlin DE
Telecom

Posnan PL
Governement

Vienna AT
Government

Delft NL
MDI QKD

Cambridge UK
Data Centers

Paris FR
Academic network

Geneva CH
Smart Grid

Oberpfaffenhofen DE
Satellite QKD

Barcelona ES
Video Com

Bratislava CZ
Government

Ostrava CZ
High Perf. Comp.

Graz AT
Healthcare

Padua IT
Free-space QKD

Matera IT
Satellite QKD

Athens GR
Data Com

OPENQKD Metadata

Call:H2020-SU-ICT-2018-3, Innovation action
Topic: SU-ICT-04-2019 Quantum Key Distribution testbed
Grant Agreement No.: 857156

Estimated project cost: **~18M**
Requested EU Contribution: **~15M**

Start Date: **02 September 2019**
Duration: **36 months**

13 EU and associated countries: AT, BA CZ, DK, FR, DE, IL, IT, NL, PL, ES, CH and UK

Coordination:
AIT Austrian Institute of Technology

Partners: **38**

Let’s stay entangled …

Send an email to alice@openqkd.eu or bob@openqkd.eu

Follow us https://twitter.com/openqkd | @openqkd

Connect with us www.linkedin.com/in/openqkd | OPENQKD Project

Find information https://openqkd.eu/

For more information
http://www.idquantique.com/