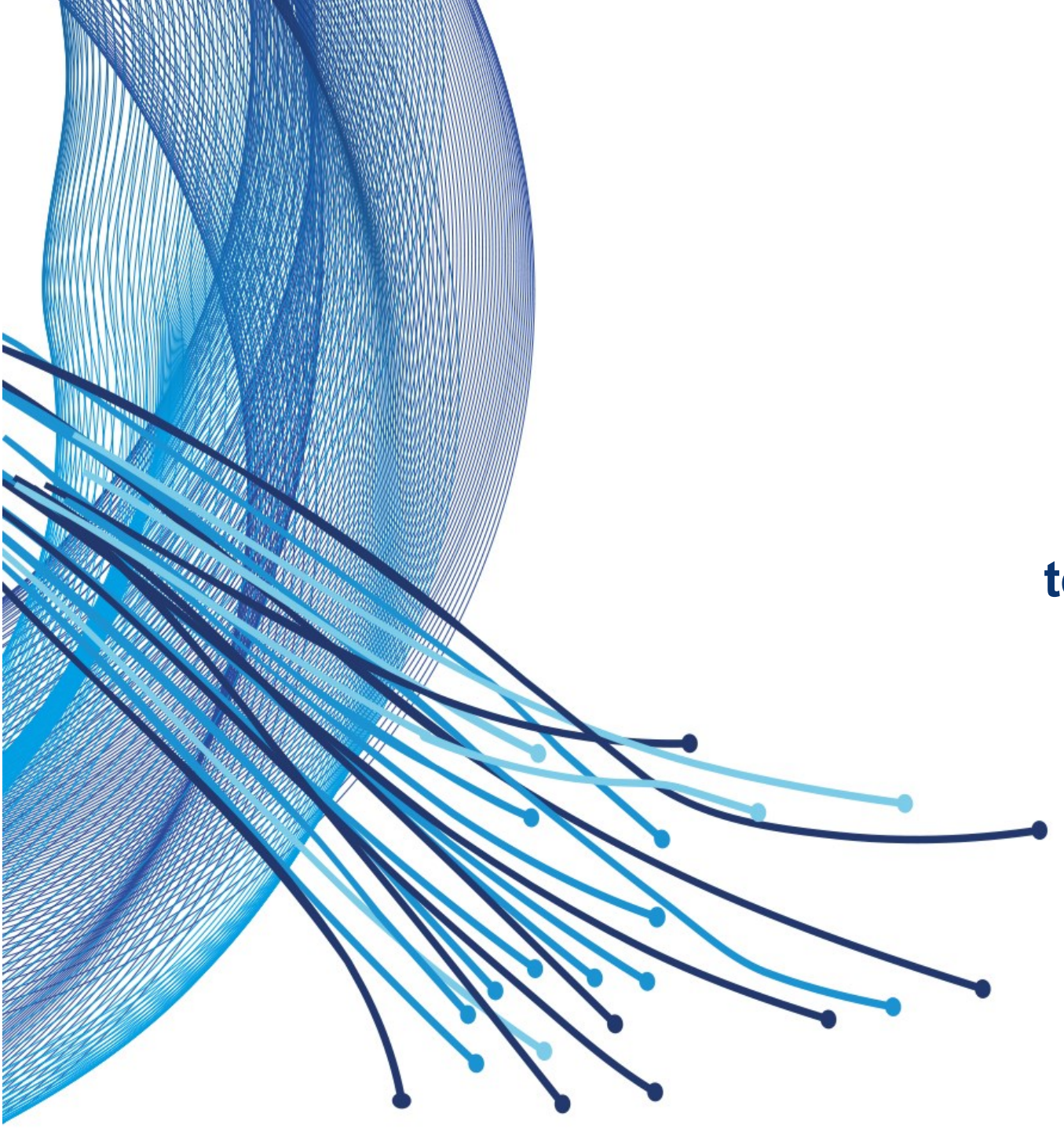


HellasQCI - Quantum Communication Infrastructure for Greece

HellasQCI and EuroQCI, emerging technologies and infrastructures for Quantum Key Distribution (QKD)

Dr. Ilias Papastamatiou, GRNET

HellasQCI Project Coordinator

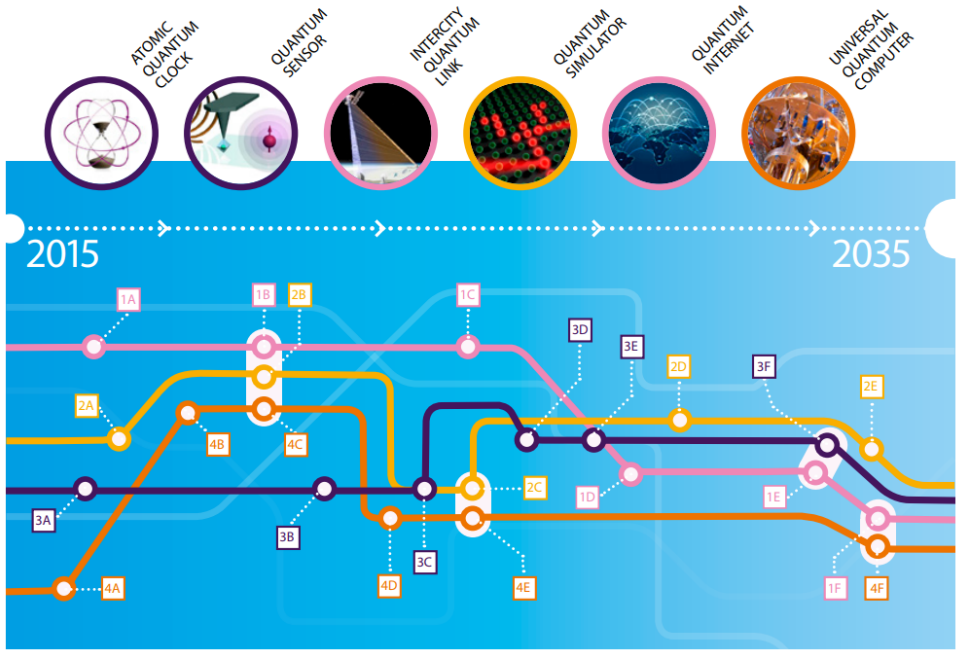
Zenon Mousmoulas, GRNET

HellasQCI Community Coordinator

GRNOG 15 meeting - 25 October 2023

Quantum Technologies

Quantum Technologies Timeline



EU Quantum Manifesto (2016) →
Quantum Flagship, Quantum Internet Alliance, activities in ESA, and European Quantum Communication Infratructure (EuroQCI) initiative.

https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf

	1. Communication	2. Simulators	3. Sensors	4. Computers
0 – 5 years	A Core technology of quantum repeaters B Secure point-to-point quantum links	A Simulator of motion of electrons in materials B New algorithms for quantum simulators and networks	A Quantum sensors for niche applications (incl. gravity and magnetic sensors for health care, geosurvey and security) B More precise atomic clocks for synchronisation of future smart networks, incl. energy grids	A Operation of a logical qubit protected by error correction or topologically B New algorithms for quantum computers C Small quantum processor executing technologically relevant algorithms
5 – 10 years	C Quantum networks between distant cities D Quantum credit cards	C Development and design of new complex materials D Versatile simulator of quantum magnetism and electricity	C Quantum sensors for larger volume applications including automotive, construction D Handheld quantum navigation devices	D Solving chemistry and materials science problems with special purpose quantum computer > 100 physical qubit
> 10 years	E Quantum repeaters with cryptography and eavesdropping detection F Secure Europe-wide internet merging quantum and classical communication	E Simulators of quantum dynamics and chemical reaction mechanisms to support drug design	E Gravity imaging devices based on gravity sensors F Integrate quantum sensors with consumer applications including mobile devices	E Integration of quantum circuit and cryogenic classical control hardware F General purpose quantum computers exceed computational power of classical computers

Different areas on quantum technologies
All areas are interconnected

Security of digital Communications

"This [large-scale quantum computer] would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere."

NIST.IR.8105

National Institute of Standards and Technology USA

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Quantum Communications

Post-Quantum Cryptography – PQC

NIST selected one public-key encryption algorithm

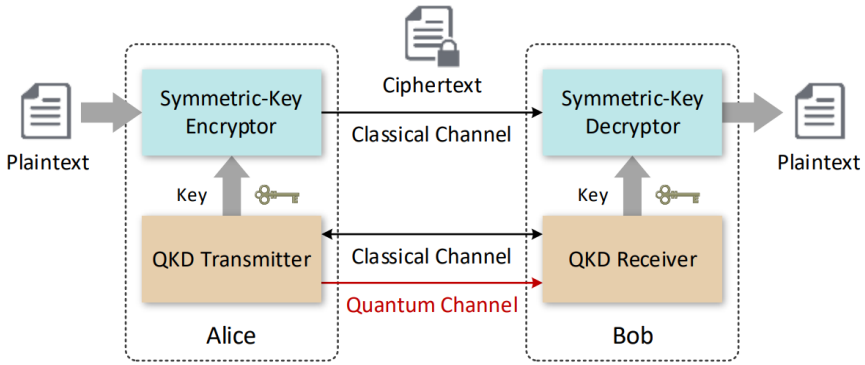
Might be vulnerable to future algorithms

Quantum Key Distribution - QKD

Unconditional security

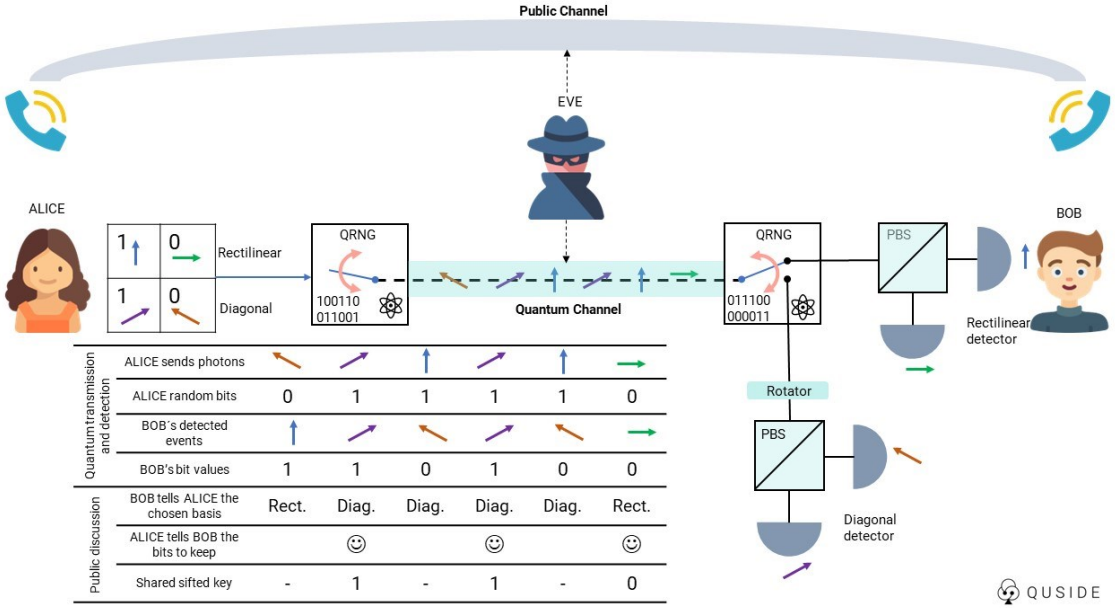
Composable with unconditionally secure authentication or encryption algorithms

Future-proof



QKD Protocol - BB84

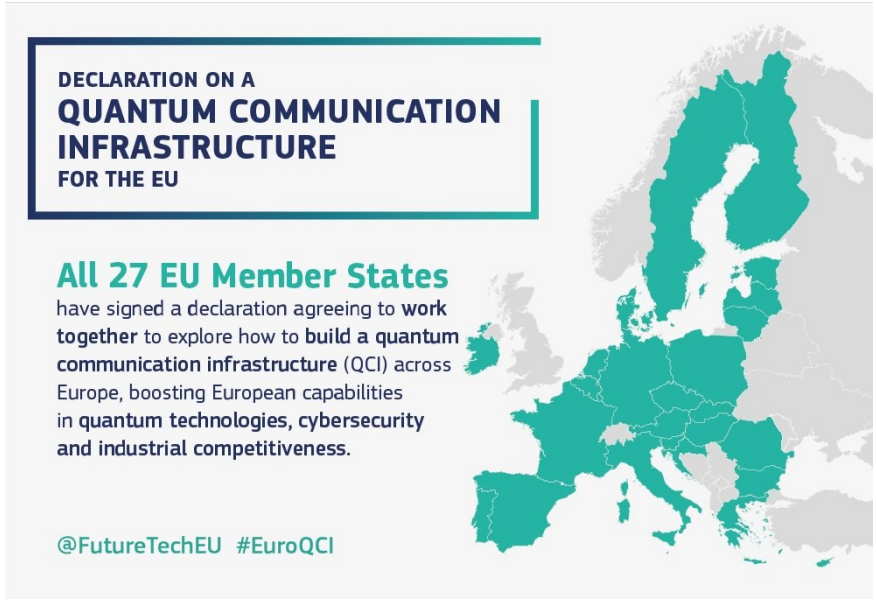
- ✓ Proposed by Charles Bennett and Gilles Brassard in 1984 → one of the earliest protocols for **quantum cryptography** and remains one of the fundamental protocols used in this field.
- ✓ The sender sends a series of quantum bits (qubits) to the receiver → polarized photons.
- ✓ The sender randomly chooses one of two possible polarizations for each qubit.
- ✓ The receiver also randomly chooses a polarization for each qubit upon reception.
- ✓ The sender and receiver exchange information about their chosen polarizations for each qubit without revealing the qubits themselves.
- ✓ They publicly disclose a small subset of their sequences to check for any intervention from an external eavesdropper.
- ✓ Once the security of the connection is confirmed, the two parties use the remaining qubits to create a shared secret key.



In the **BB84 protocol with decoy states**, additional states are introduced during the transmission of qubits → These decoy states are used as a security measure to detect eavesdropping and enhance the security of the QKD process

EuroQCI

EuroQCI



The aim is for EuroQCI to be **operational by 2027**

Since **June 2019**, all 27 EU Member States have signed the **EuroQCI Declaration**, signaling their commitment to establish the EuroQCI

The participating countries are working with the **European Commission** and the **European Space Agency** to design and deploy the EuroQCI

The aim of the EuroQCI is to safeguard **sensitive data** and **critical infrastructures**, providing an additional security layer based on **quantum physics**

Building the EuroQCI will boost Europe's capabilities in **quantum technologies**, **cybersecurity** and **industrial competitiveness**.

EuroQCI Space and Terrestrial Segments

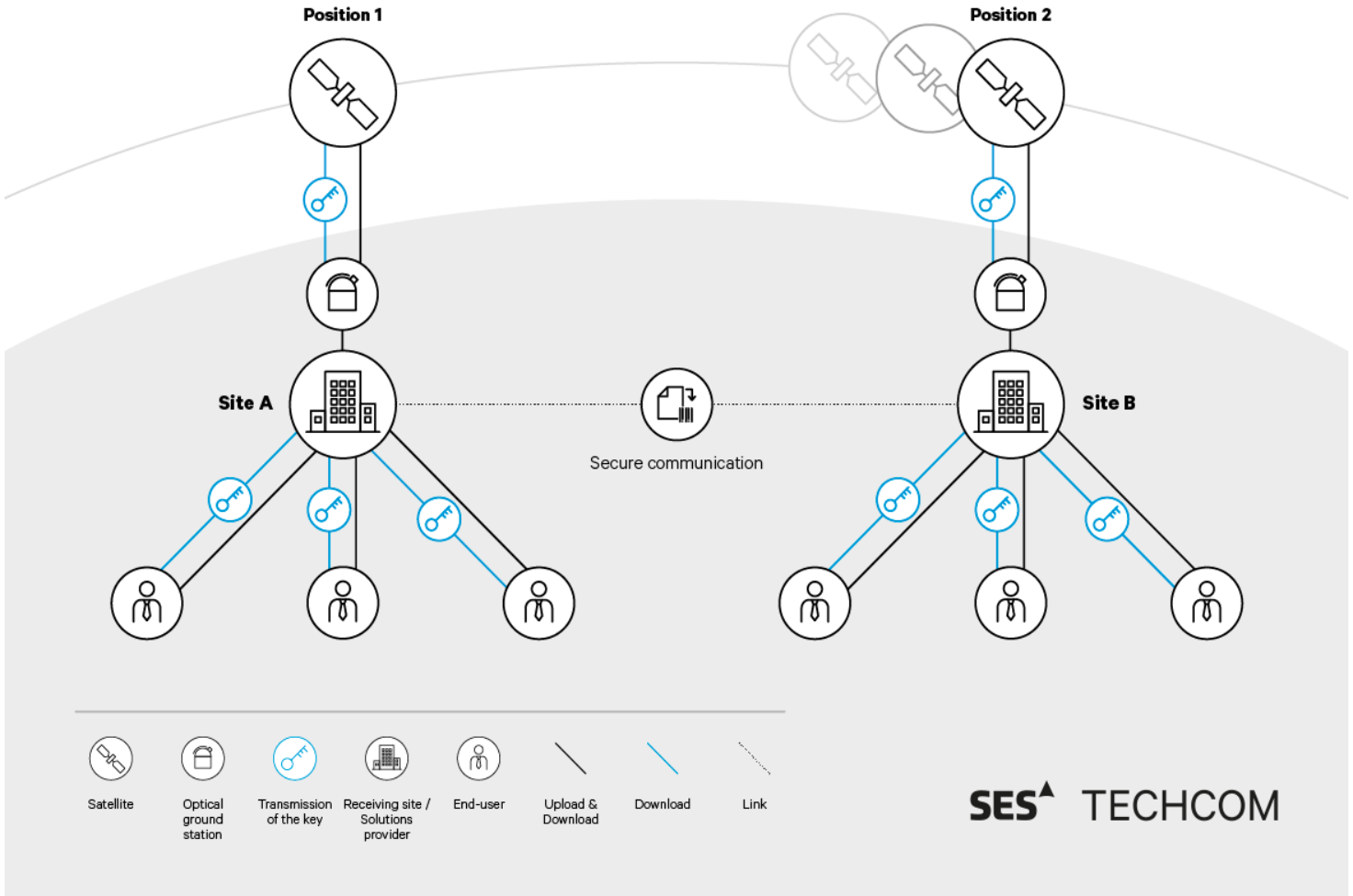
Space segment

implemented by **ESA**
EAGLE-1 Satellite is being built by SES/ESA

Terrestrial segment

implemented by the **Member States** and the support of **PETRUS project.**

Both under the supervision of the **European Commission**



Operational EuroQCI → Interoperable and reliable Space and Terrestrial Segments

EuroQCI Space and Terrestrial Segments

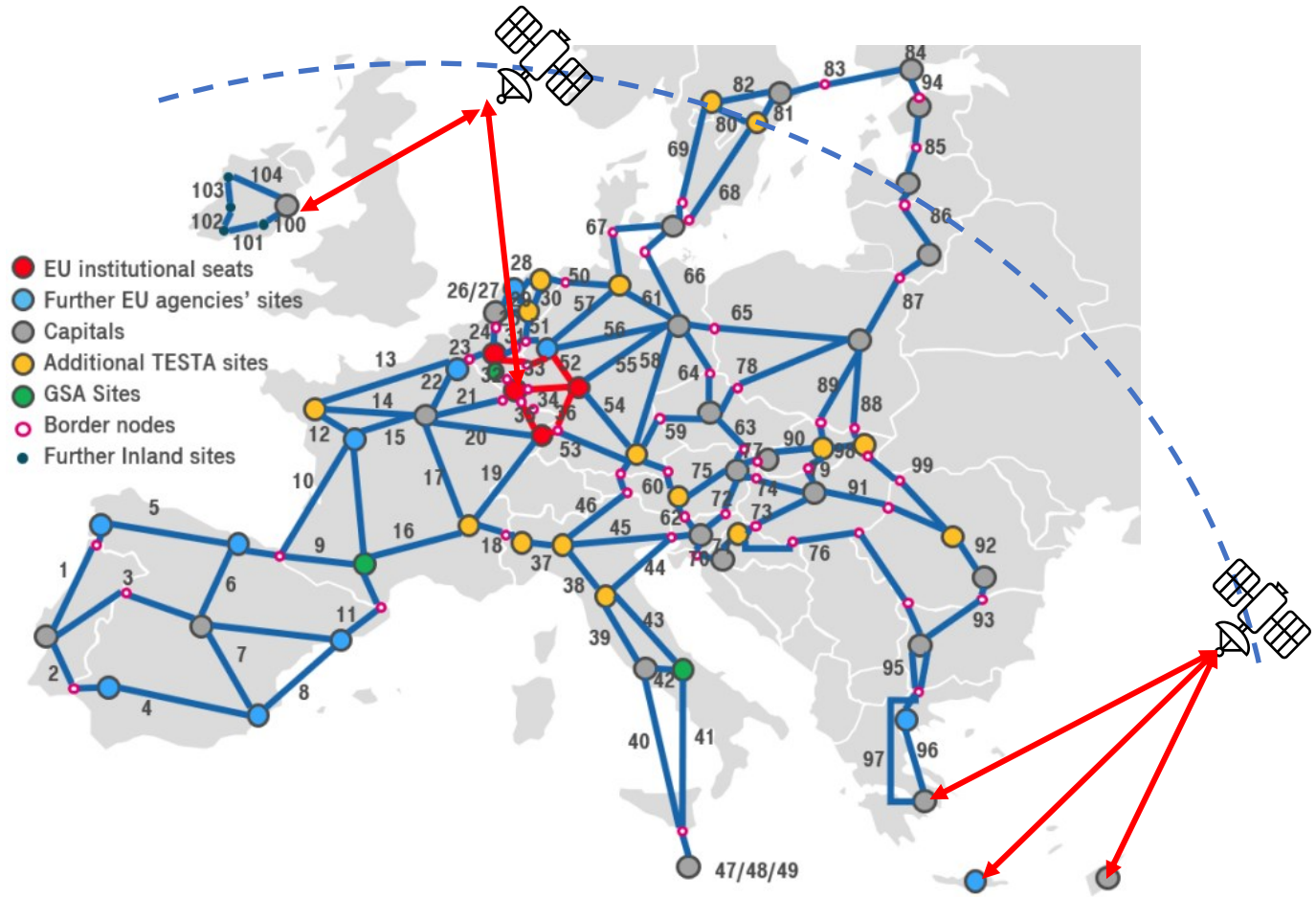
Terrestrial segment

Federation of national terrestrial QCI networks with cross-border connectivity → Total length of fibers 44,000 km

Space segment

Distribution of quantum-secured encryption keys on a European scale
Ideal for EU island countries

Alternative route in critical events



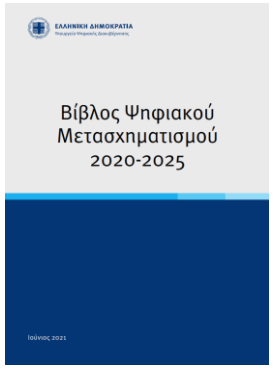
Jean-François Buggenhout "EU Quantum Technologies Flagship and the quantum internet"
ENISA TELECOM SECURITY FORUM, 29 June 2022

Operational **EuroQCI** → **Interoperable** and **reliable** Space and Terrestrial Segments

EuroQCI Greece

The **Ministry of Digital Governance** signed on behalf of **Greece** the EuroQCI Declaration

EuroQCI is part of the **Digital Transformation Strategy of Greece** (2020-2025)



GRNET was appointed (October 2021) by the Ministry of Digital Governance to participate to the **EuroQCI** and be responsible for the **DEP-CEF national proposals** coordination and submission

According to **Laws 4623/2019** Art. 58 **Law 4727/2019** Art. 87 **GRNET** "has the central role of **coordinator of all digital infrastructures** for Education and Research" and "constitutes **the national representative of the research and technological community** in the research infrastructures of the EU"

DEP TOPIC -2 : HellasQCI Project

EDU
- NKUA (BEN)
- FORTH (BEN)
- NCSRD (BEN)
- AUTH (BEN)
- NOA (BEN)
- ICCS (AP)

GOV
- MinDigital (BEN)
- NIS (LoS)
- Army (LoS)
- Police (LoS)

HellasQCI Consortium
GRNET (COO)

IND
- Motor Oil (BEN)
- Cosmote (BEN)
- Space Hellas (BEN)
- Qubitech (BEN)

National QCI Partnerships
Luxembourg (AP)
Ireland (AP)
Austria (LoS)
Bulgaria (LoS)
Cyprus (LoS)
Poland (LoS)
Malta (LoS)

HellasQCI Budget: 9.997.545 €	
EU funding rate at 50%	
EU Funding: 4.998.772,50 € National Funding: 4.998.772,50 € Around 6M € for equipment and fibers	Project Started: 1 January 2023 Project Ends: 30 June 2025

DEP 2 - Results	
Excellent score	Ranked in **the 2nd cluster** based on rating (out of 7) along with **Germany**'s, **Finland's** and **Ireland's** National QCI proposals.

HellasQCI National Quantum Backbone

1

O1: Build the National Quantum Networks as part of the EuroQCI

- 3 national test-sites: Athens, Thessaloniki, Crete
- HellasQCI provides terrestrial links to OGS
- 3 OGS will be connected to the backbone network
- 500km length of fiber links will be deployed
- More than 12 perm. QKD nodes will be installed

8

O8: Quantum Satellite Connectivity

- Builds on Helmos, Holomontas and Skinakas OGSs
- All telescopes part of ESA ARTES Scylight, Hydron and SAGA programmes
- Connect to QKD satellites for connecting our test-sites and also connect with the rest of the EU

HellasQCI Powerful Metropolitan Testbeds

O2: Develop and Deploy advanced quantum systems and networking technologies

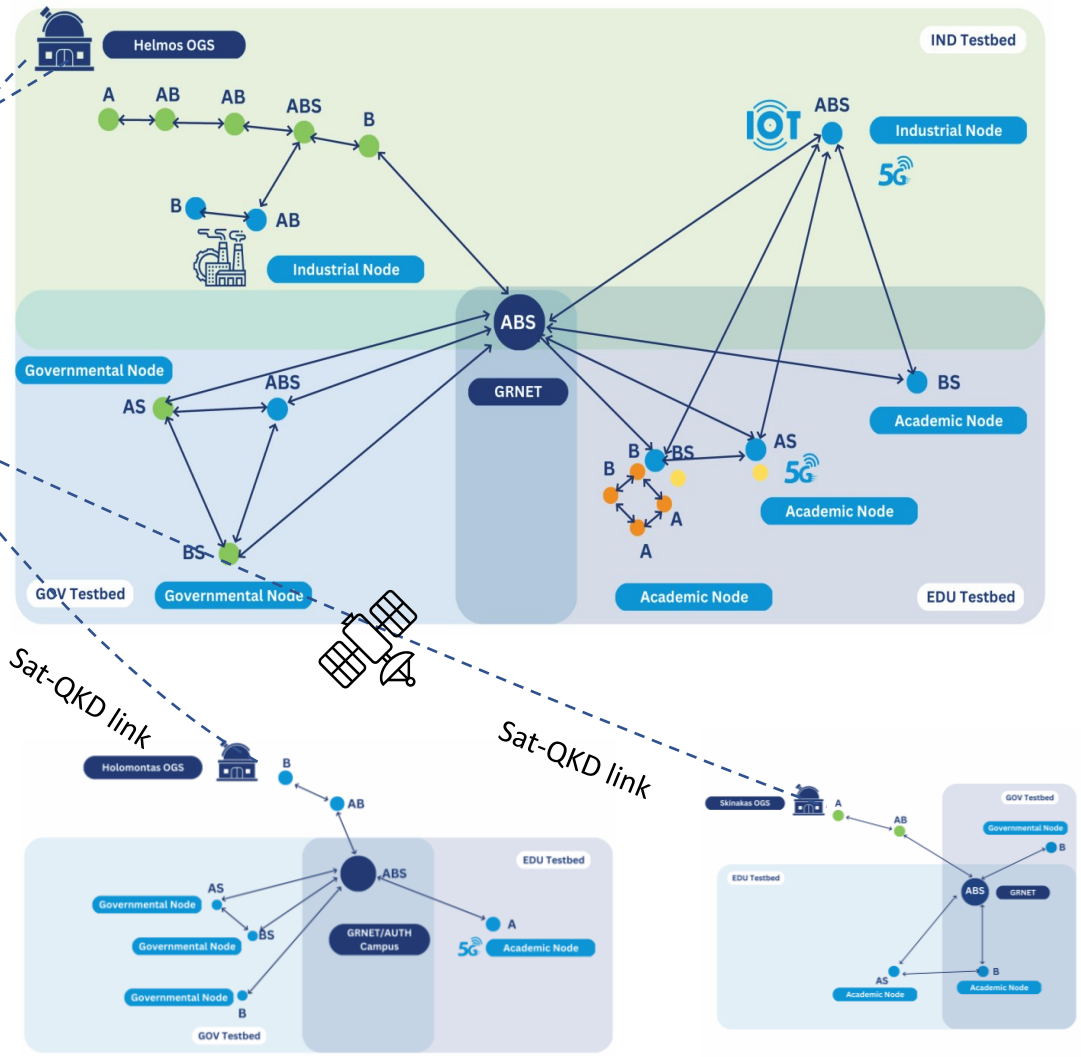
- **QKD technologies**
  - ✓DV-QKD technology (Most mature solution)
  - ✓Single photon detectors and sources (entanglement)

Three Quantum Network domains

- Governmental (GOV)
- Industrial (IND)
- Research and Innovation (EDU)

Advanced QKD technologies

- Dynamic QKD for optimal resource allocation, resilience and flexible networking
- Co-existence of Quantum and Classical Channels
- Enhanced PUF encryption schemes



HellasQCI 16 Multidisciplinary Use cases

3

O3: Advanced use cases in different application scenarios

- 16 use cases
- 7 National Security and Governmental nodes connected + long-distance testing
- 6 Critical infrastructures, health sector and ICT industry nodes connected
- 6 Research and Innovation nodes connected
- Entanglement distribution network 4 receivers – 2 nodes

National Security

Use Case 1 — QKD for National Security
Use Case 2 — Enhanced QKD resilience for National Security Links
Use Case 3 — Satellite QKD connectivity for remote National Security Nodes
Use case 16 — HellasQCI space and terrestrial segments

Public Health

Use Case 4 — Secure communications for Public Safety applications
Use Case 5 — Quantum Secure technologies for cloud Health Applications
Use Case 6 — Secure transmission of medical imaging data for Public Hospitals

Industry | Critical Infrastructures

Use Case 8 — Quantum cryptography to secure communication links of critical infrastructures
Use Case 9 — ICT sector | Secure storage in cloud data centres
Use case 10 — ICT sector | QKD over 5G
Use case 11 — ICT sector |Next Generation Quantum Secured FTTH services
Use case 15 — Preparation of a quantum encrypted software application
Use Case 7 — QKD for secure connectivity to supercomputing infrastructure

Research

Use case 12 — Preparing for the quantum internet
Use Case 13 — Advanced quantum network controls
Use case 14 — PUF-based hybrid authentication for switched QKD

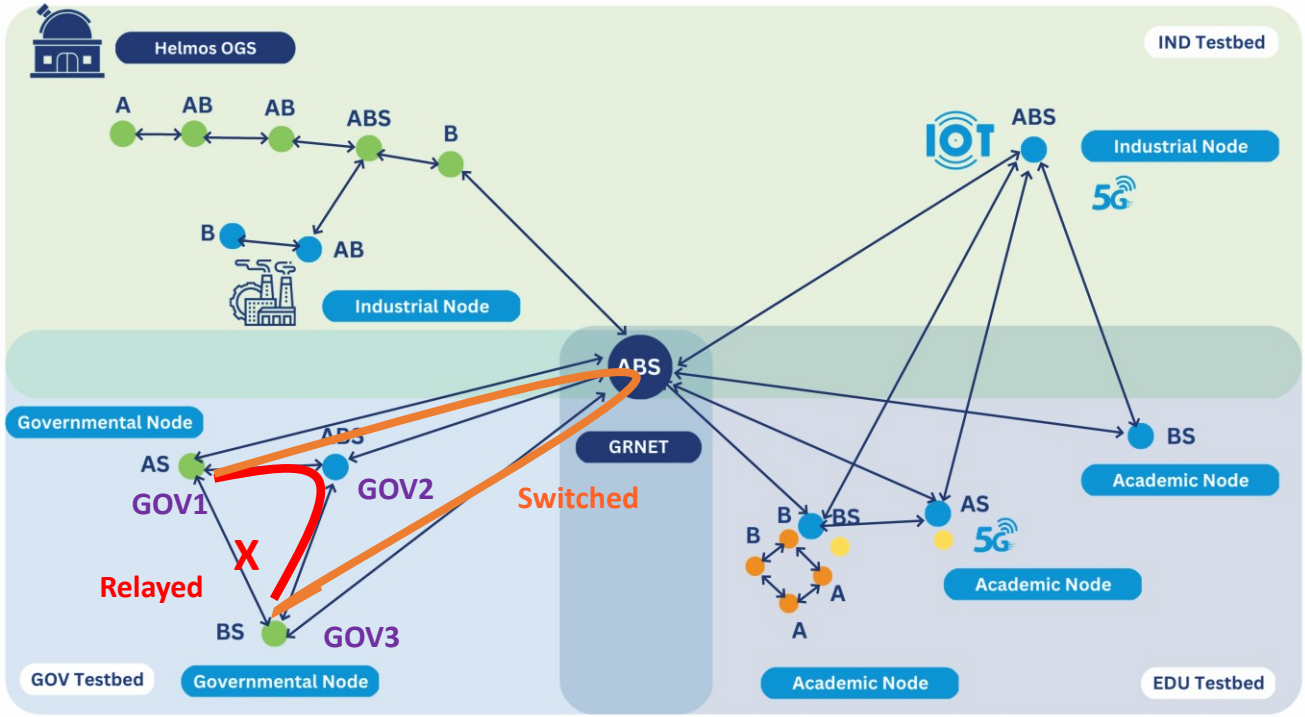
Use Case – Enhanced QKD resilience for National Security Links

Key objective

demonstrate resilience in DDoS attacks using the switched QKD operation

Implementation

Demonstrate the plethora of scenarios for interconnecting the GOV nodes



Space segment Use Cases

Key objectives

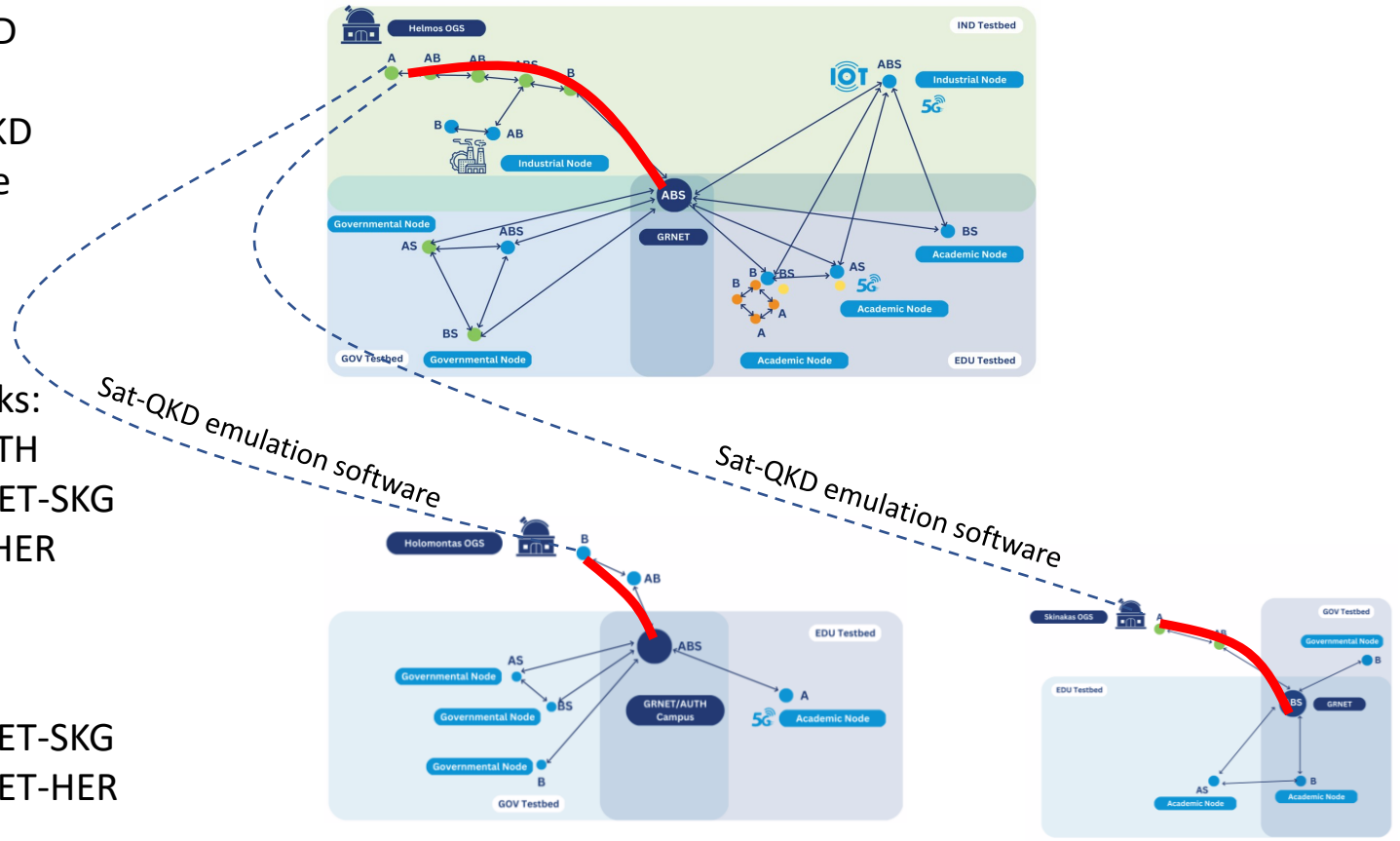
- Demonstrate relayed QKD connectivity with OGS
- Emulate Inter-testbed QKD connectivity with suitable software

Relayed QKD links

- Establish relayed QKD links:
- OGS Helmos to GRNET-ATH
- OGS Holomontas to GRNET-SKG
- OGS Skinakas to GRNET-HER

Sat-QKD links

- Emulate a sat-QKD links
- from GRNET-ATH to GRNET-SKG
- from GRNET-ATH to GRNET-HER

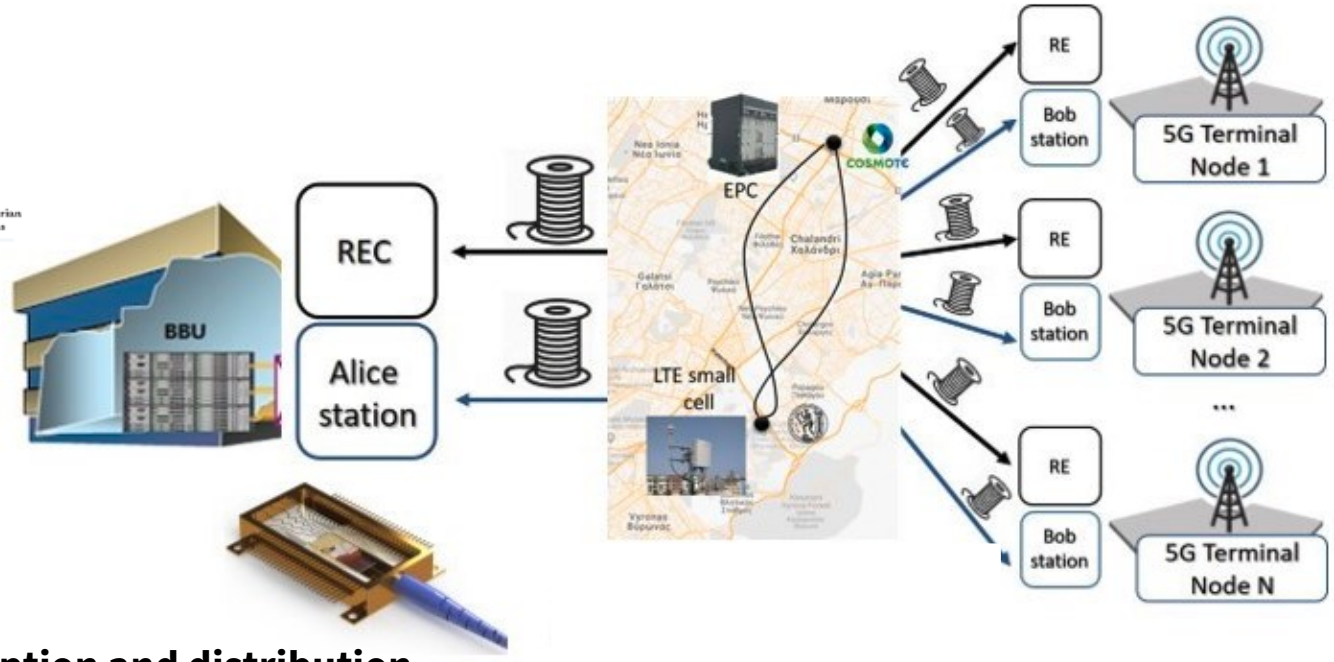


Research and Industrial Use Cases

- Industrial and Academic partners have demonstrated novel technologies for QKD
- HellasQCI offers a field testbed as the sandpit to further develop the technologies

UNIQORN
Affordable Quantum Communication for Everyone

QKD over 5G
QKD for FTTH



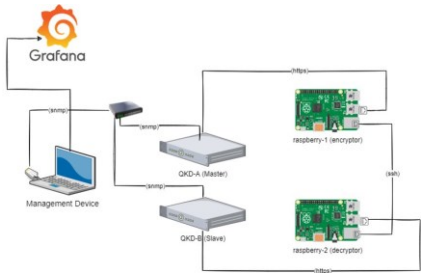
Quantum key encryption and distribution

SPACE

HELLENIC REPUBLIC
National and Kapodistrian University of Athens

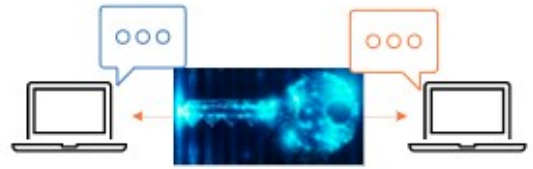
QGOV

OPEN QKD



quantum-safe messaging and communication application

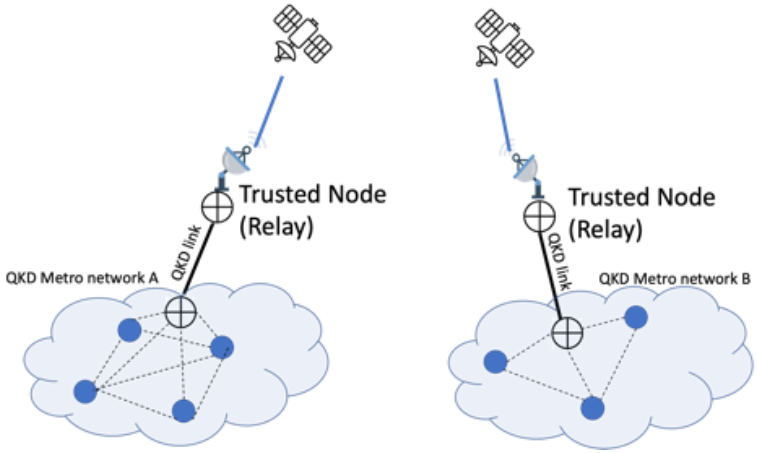
UBITECH quantum technologies



Research and Industrial Use Cases

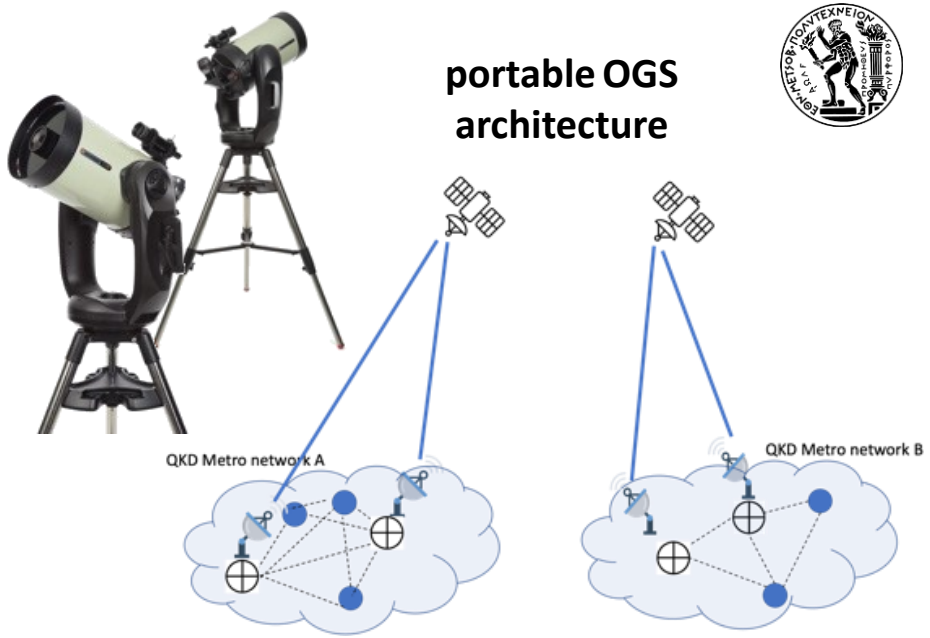
- HellasQCI will experiment with **FSO** and **portable OGS** to address the need for higher key rates
- Remove requirement to transform an observatory-OGS into a trusted node → the trusted node becomes an OGS

Large OGS architecture



- ✓ *Portable telescope provided by NOA: CPC DELUXE 1100HD*
- ✓ *FSO link 28 cm Telescope (Rx)*

portable OGS architecture

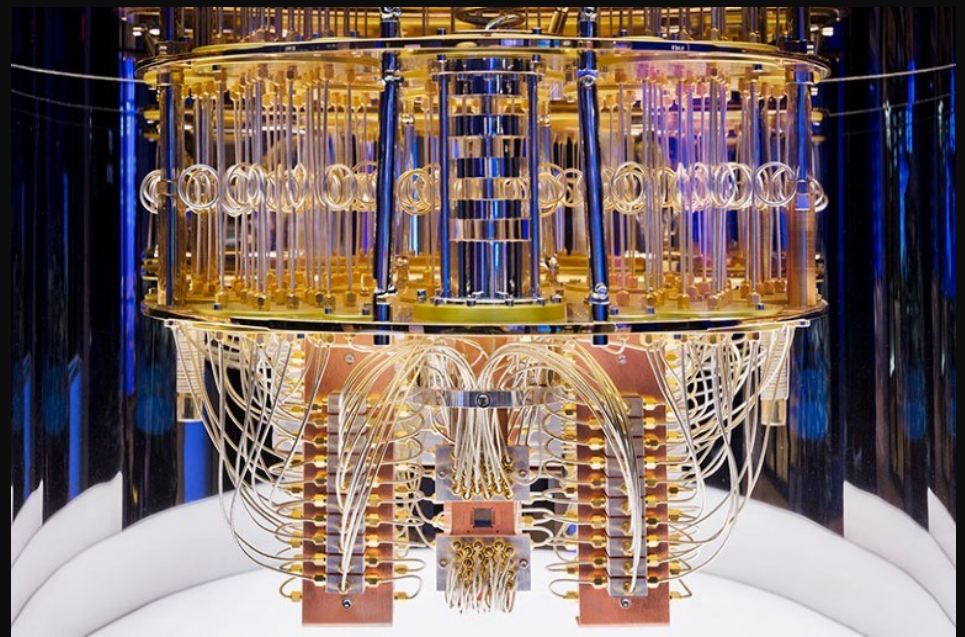


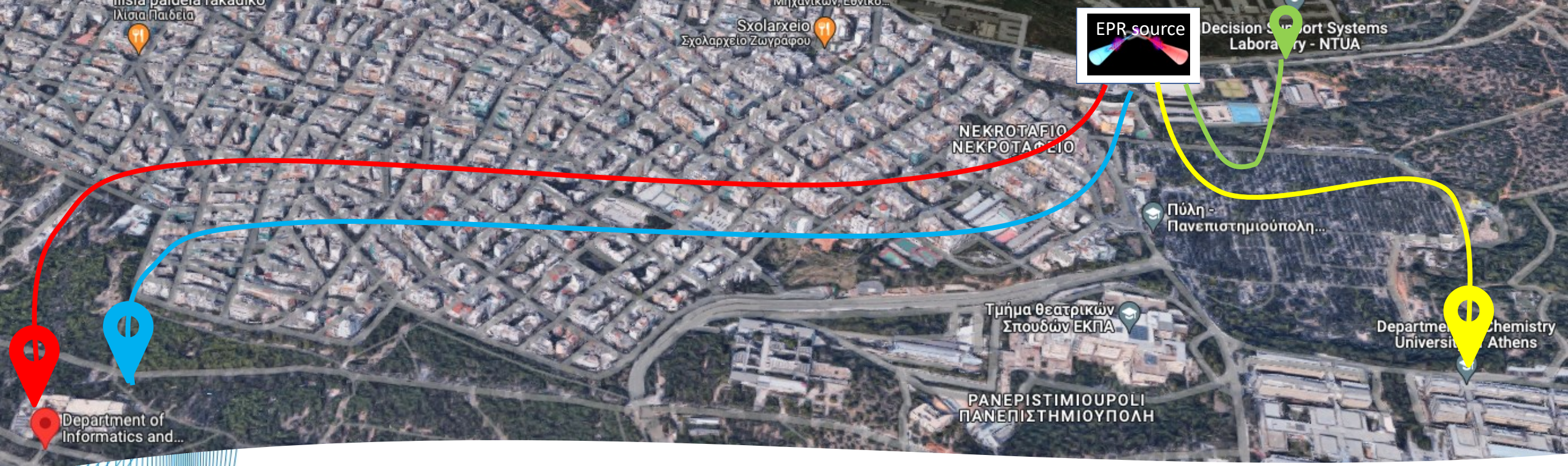
MOH refinery encryption requirements and application

- Sub use case 1: Feed external QKD to existing networking devices to achieve strong SSL/TLS encryption over optical fiber interconnections.
- Sub use case 2: In-line pair of QKD Equipment supporting SSL/TLS protocols to undertake E2E encryption over optical fiber interconnections.

The device that will be installed in Motor Oil refinery must comply with technical (ATEX) specifications:
Degree of protection: IP65
Ex-Protection: II3G Ex ec IIC (T3 gc)
Temperature range: -20C - +40C

HellasQCI will pave the way towards the Quantum Internet in Greece





World-class Entanglement distribution in Greece

- ✓ Two experimental active entanglement distribution stations will be permanently installed in two universities in Athens
- ✓ HellasQCI will implement a state-of-the-art active entanglement distribution network using **cryogenic single photon detectors in NKUA** and **entanglement sources in ICCS/NTUA**

HellasQCI - EuroQCI synergies

O4: Cooperation with EuroQCI PETRUS and other NatQCIs projects to build robust, interoperable and secure QKD systems and networks

- GRNET/MinDig made **7 partnerships** with Austria, Luxembourg, Bulgaria, Cyprus, Malta, Poland and Ireland National QCI proposals
- GRNET is partner to **Lux4QCI** and **IrelandQCI** National QCI projects and vice-versa
- GRNET is partner to **PETRUS EuroQCI project** that coordinates the National QCIs and participates in the Quantum Strategy Group of **GEANT** and its project GN5-1

O5: National Stakeholder Engagement

- Establishment of the **HellasQCI community** from all national stakeholders that can benefit and support the HellasQCI networks, gather expertise and share knowhow on QCI and QKD
- Ensure better participation into the **EuroQCI** and leverage new end-users for the expansion of the HellasQCI networks
- https://hellasqci.eu/community-repository/

HellasQCI Trainings & Standards

O6: Provide a training environment for technical, research and end-users staff

- 5 Training workshop events
- Summer schools for MsC/PhD students
- Integration of HellasQCI training material in MSc and undergraduate courses
- Online training platform

O7: Provide a secure architecture compatible with EU QKD Standards and Certifications

1st HellasQCI 4-day Training event in Athens September 2023

The event had two different thematic axes:
Workshop on Quantum Key Distribution (QKD) Systems

Workshop on Cybersecurity with QKD Systems and Post-Quantum Cryptography (PQC)

Welcoming remarks by the new Secretary General of Telecommunications and Posts, Prof. Konstantinos Karantzalos

HellasQCI 4-Day Training Event: Assessment Report

Updates - Procurements

Fibers ~ €1.8M

- 27 links have been procured: 3 long-distance and 24 metropolitan ones (around 500km) → 21 links for the GOV sector and 6 links for the EDU.

Quantum equipment ~€3M

- 2 x EPPS - entangled photon sources
- 16 x SNSPDs -superconducting nanowire single-photon detectors
- 9 x Mature DV-QKD systems
- 2 x EU DV-QKD systems

Upcoming procurements

low-loss optical switches, encryptors (and quantum equipment)

PoC | HellasQCI - NOKIA

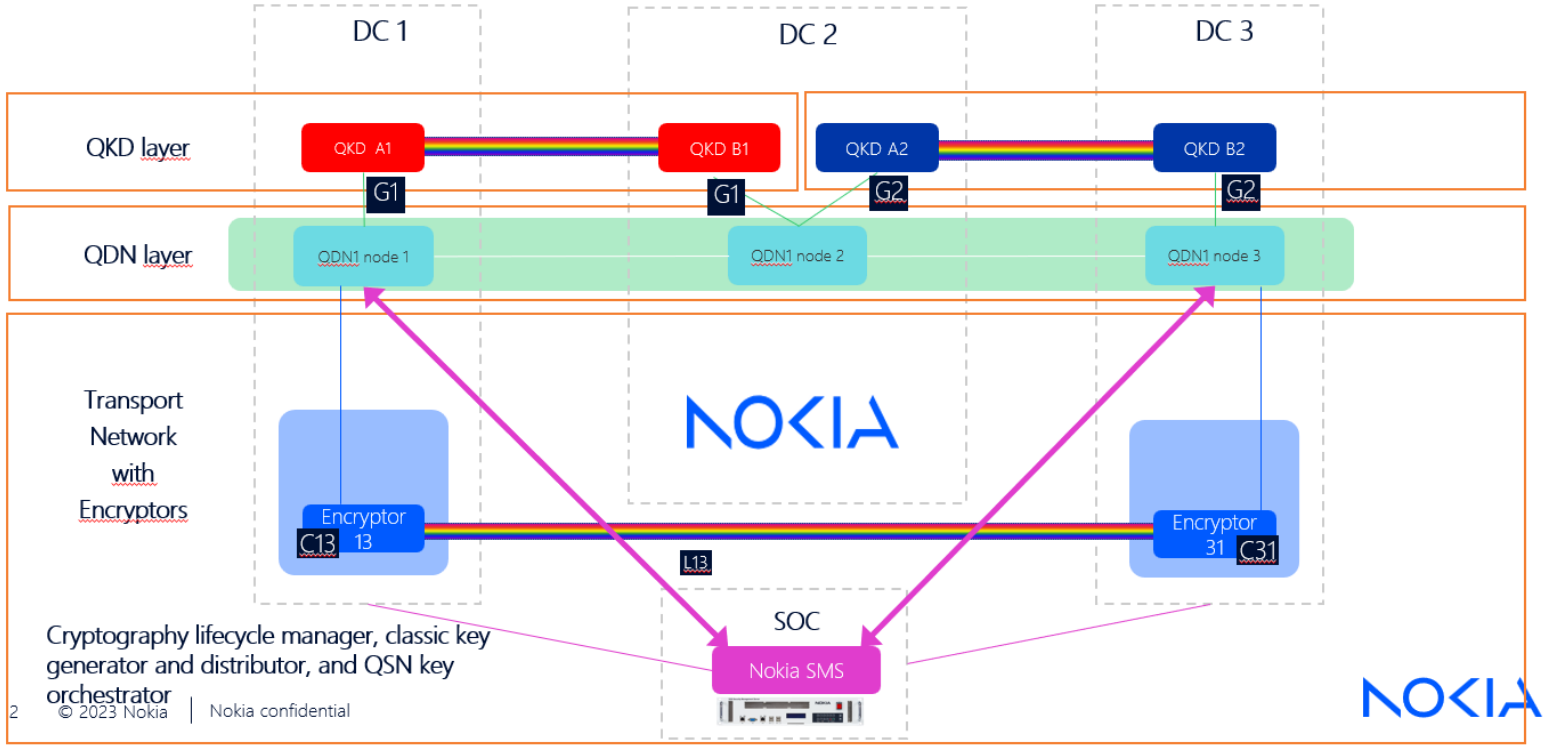
Key objectives

- Explore the monitoring tools and control software for the QKD and move towards operational QKD solutions

Implementation

- Demonstrate the integrated control software in operation with the GRNET classical optical network and the deployed QKD network (OTN-SEC)

Quantum Delivery Network (QDN)



Nokia Secure Management Server-SMS → orchestrator between the quantum channel and the classical optical channel

Thank you

Dr. Ilias Papastamatiou

ipapastamatiou@admin.grnet.gr

HellasQCI - Quantum Communication Infrastructure for Greece

HellasQCI.eu

Co-funded by the European Union

EuroQCI

This project is co-funded by the European Union
under the Digital Europe Program grant agreement No. 101091504.