UNIQORN QUANTUM KEY DISTRIBUTION ENGINES FOR SECURE 5G-AND-BEYOND COMMUNICATIONS

G. Giannoulis, **National Technical University of Athens**
F. Setaki, **COSMOTE Mobile Telecommunications S.A**

INFOCOM Athens, 06.11.2020
https://www.infocomworld.gr

Affordable Quantum Communication for Everyone: Revolutionizing the Ecosystem from Fabrication to Application

UNIQORN
Affordable Quantum Communication for Everyone

Call: H2020-FETFLAG-2018-03 (QComm.), RIA

Project nº: 820474

Countries: AT (Coord.), DE, DK, NL, IL, EL, IT, UK, BE

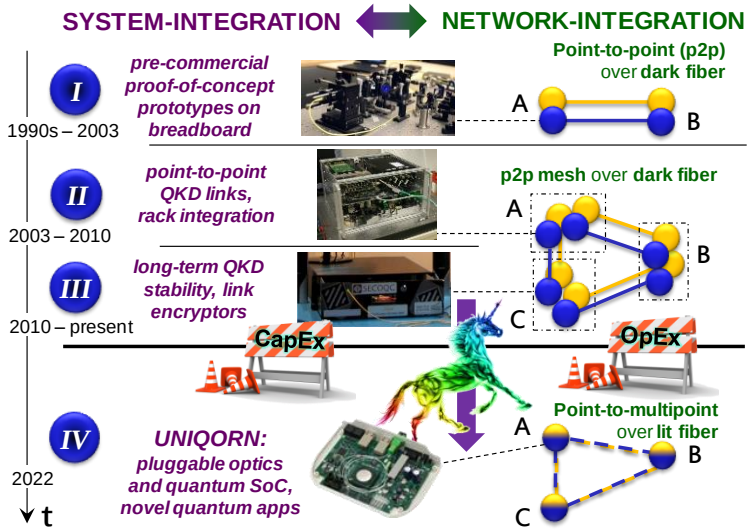
Partners: 17 (with 8 Univ., 3 RTO, 3 SME, 3 Lrg.Ent.)

Funding: 10 M€ over duration of 36M

Focus: Ubiquitous Quantum Communication

- ✓ Quantum-enhanced communication protocols:
  information-theoretically secure key exchange, quantum random number generation and
  secure multiparty computation

- ✓ High technological readiness at the device level:
  Achieve cost-effectiveness through integrated, deployable quantum-photonic solutions



Security Threats in 5G

Physical Network Infrastructure vulnerable to Hacking attacks

5G infrastructure for ultra-dense deployment

- Fiber-connected RU/RRH nodes will be hosted in street furniture (e.g. lampposts), and can be accessible practically from everyone
- Physical layer infrastructure of DU/CU nodes can be accessible in a multi-operator environment

Optical Fiber Hacking

- A simple optical cable tapping equipment can be used to penetrate optical fiber network

Public Key Infrastructure vulnerable to Quantum Attack

Quantum Computer can solve certain mathematical problems exponentially faster than classical computers

- Any cryptosytem based on mathematical complexities (RSA, DSA, DH)
- Any security protocol from the above public key ciphers
- Any products or security systems based on these protocols

……

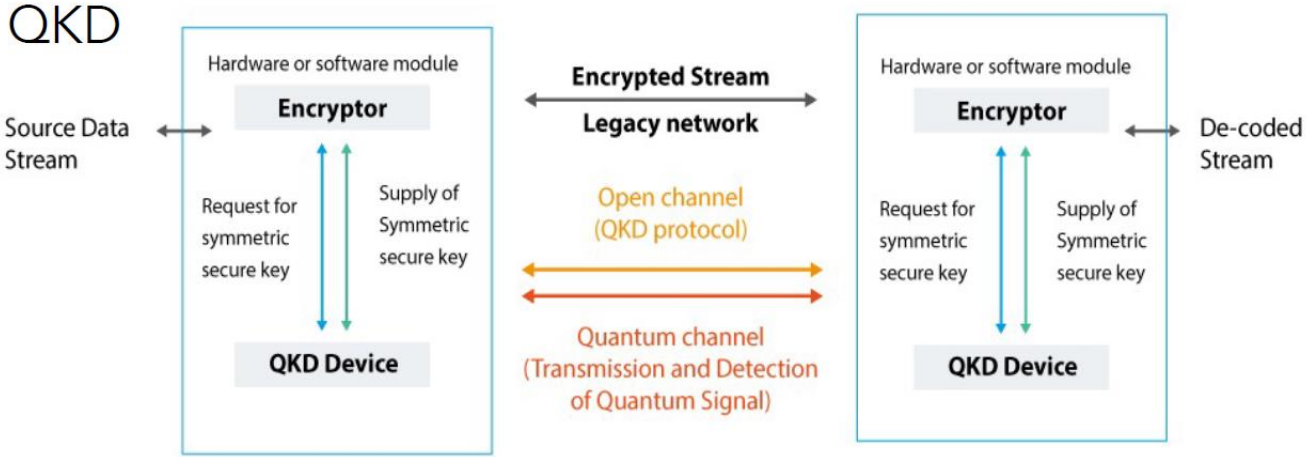
Symmetric key ciphers like AES are believed to be Quantum-Safe

Quantum Key Distribution

How to securely distribute symmetric keys between distant parties without relying on insecure legacy public key algorithms?

QKD answers this question:

- Quantum cryptography solves the problem of key distribution by allowing the exchange of a key between two remote parties with absolute security guaranteed by the fundamental Laws of Physics
- QKD is a technology that uses Quantum Physics to secure the distribution of symmetric encryption keys
- These symmetric keys can then be used securely with conventional cryptographic algorithms



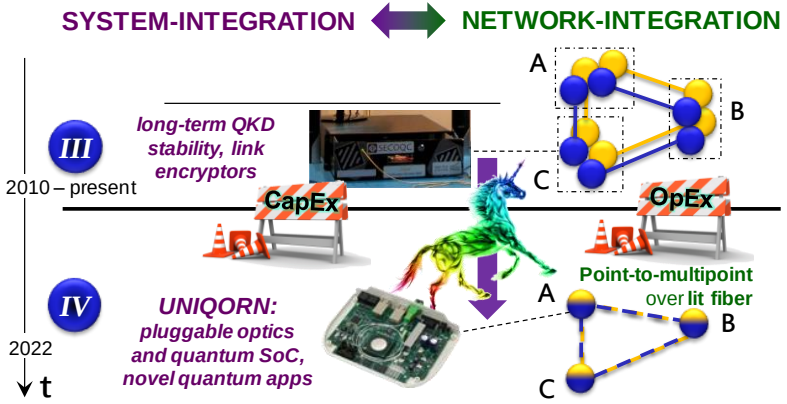
Drivers: The challenges for QKD going practical

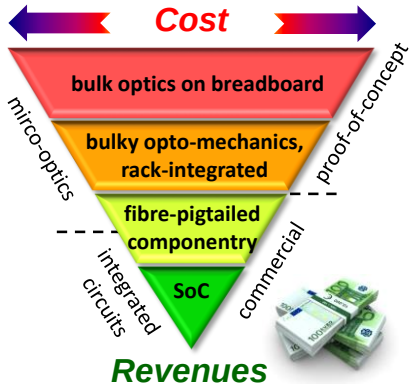
ICT infrastructure will not change to accommodate quantum network functions.

Need to merge the striking benefits of quantum technology with highly advanced telecom technologies (“co-existence”)

Powerful quantum applications need powerful yet cost-effective components

The Second Quantum Revolution is only possible when it follows a success story such as that of microelectronics, which led to the Information Age.

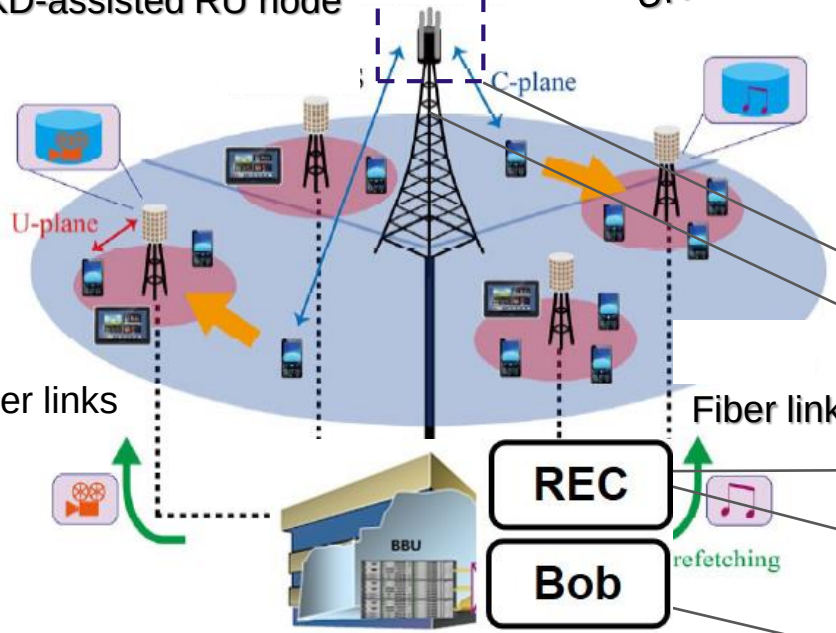




The promise of UNIQORN

Quantum-to-the-Radio for Secure 5G terminal nodes

QKD-assisted RU node

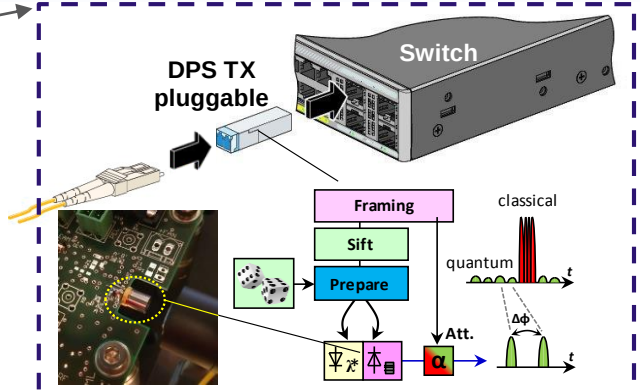


Fiber links

Fiber links

AES-256 encryption engines

UNIQORN Quantum PIC



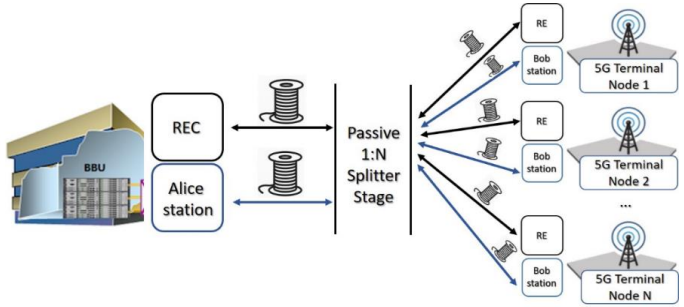
Lightweight Quantum Pluggable delivering the keys to the radio node

Fiber links for Quantum Channel interconnecting Alice/Bob sites and implementing RU/DU/CU communication

Centralized Bob stations hosting complex quantum equipment (e.g. SPADs) at centralized node

QKD integration in 5G environments

Design and Integration studies

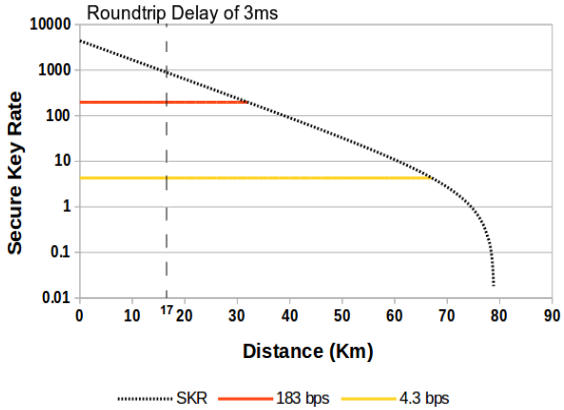


System parameters

- Latency budget
- Attack surface (depending on AES-256 key rotation times)
- Physical layer implementation using dark fibers and shared infrastructure

D. Zavitsanos, et al., On the QKD Integration in Converged Fiber/Wireless Topologies for Secured, Low-Latency 5G/B5G Fronthaul. Applied Sciences, 10(15), 5193. (2020)

Proof-of-concept validation for P2P and P2MP



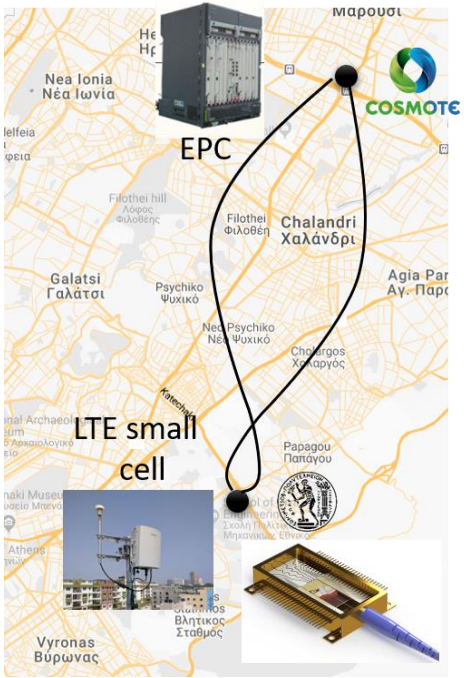
- Symmetric encryption with fast key rotation times (down to 1.4s) allowing for ultra-low attack success probabilities of less than 2^{-60}
- Successful operation for both P2P and P2MP topologies
- Ultra-low roundtrip latency performance of less than 3ms

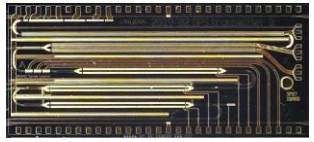
Proof-of-concept experiments in Athens

DPS-QKD
Bob station

AUSTRIAN INSTITUTE OF TECHNOLOGY

DV-Bob station





InP-based DPS
Transmitter

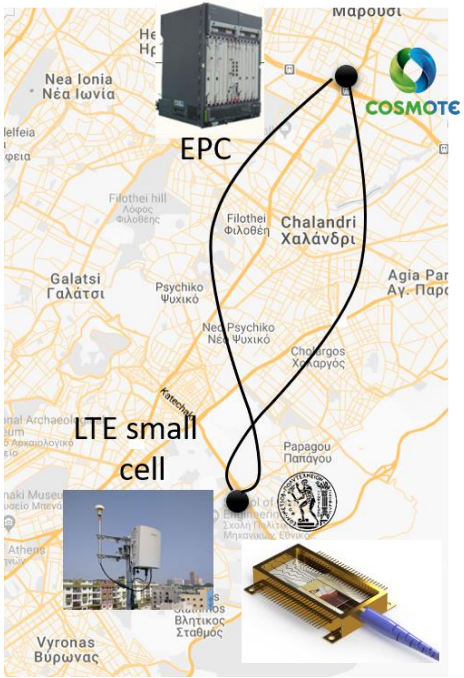
DPS-QKD
Alice station

The goal of the experiments

- Demonstrate the integration of UNIQORN DV-engines in support of key generation and delivery over the deployed fiber link interconnecting COSMOTE and ICCS/NTUA premises
- Demonstrate the potential of using shared fiber links carrying both the mobile transport layer as well the quantum keys
- Investigate system integration scenarios for both P2P and P2MP optical distribution networks

Deployment plan

DPS-QKD
Bob station



DPS-QKD
Alice station

Where we are now

- Successful interconnection of EPC and small cell through standard SFPs operating at 1550nm
- Experimental verification of P2P and P2MP optical layer implementation based on available power budget from 1.55μm SFPs

Next phase activities

- Exploring the single fiber transport for realizing bi-directional traffic between EPC and small cell
- Measuring the noise photons over the installed infrastructure using InGaAs SPAD units
- Integration of UNIQORN DV-engines providing quantum keys

Thank you!

UNIQORN
Affordable Quantum Communication for Everyone

QUANTUM Communication

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 820474.

QUANTUM FLAGSHIP