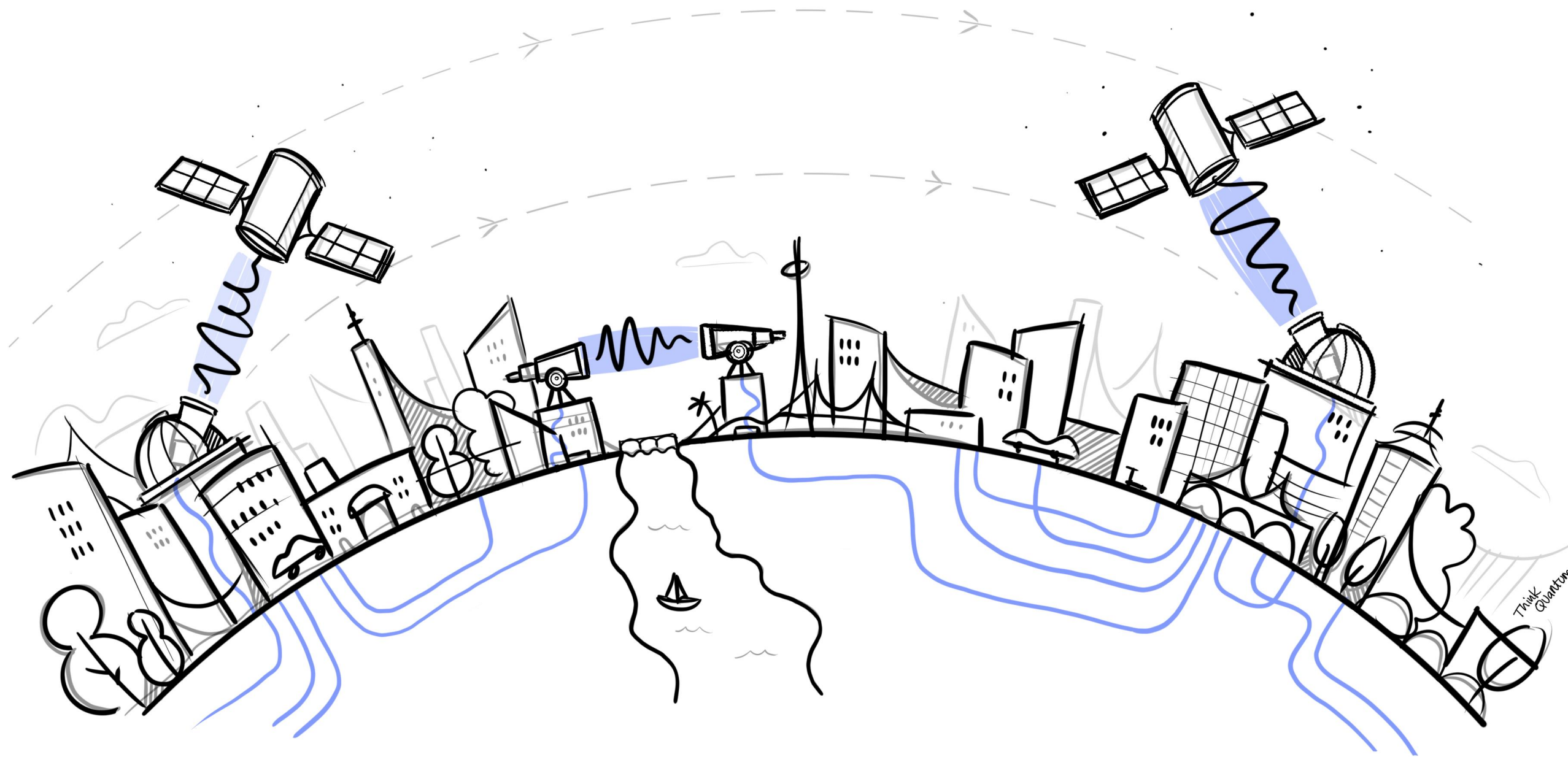# ThinkQUANTUM

OPTICAL AND QUANTUM TECHNOLOGIES FOR CYBER SECURITY

GÉANT Quantum solutions

21 June 2023

Marco Avesani
Co-Founder & Product Developer

ThinkQuantum is a **SPIN-OFF of the UNIVERSITY OF PADUA** offering complete solutions for **cyber security based on quantum technologies**.

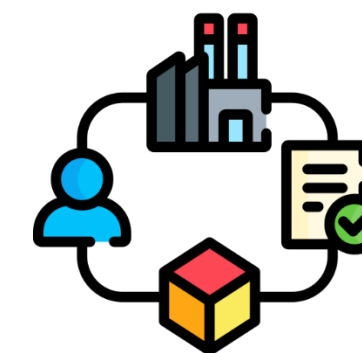**ThinkQuantum** commercializes **QRNG** and **QKD** solutions for **fiber, free-space and satellite** scenarios.

ThinkQuantum covers the **FULL VALUE CHAIN** from design and manufacturing to commissioning of the systems

ThinkQuantum, based in Italy with an Italian shareholders structure is a **fully European company** and offers a **RELIABLE EUROPEAN SUPPLY CHAIN** to those partners active within geopolitical sensitive applications.

A new company with a solid background

ThinkQuantum was founded in 2021 through the **fusion of expertise** from the **university's research group** and the **industrial capabilities of Officina Stellare**.

The **University** group has **more than 20 years of experience** in the field of **quantum information processing and quantum communications** in fibers, free-space and satellites

Officina Stellare is a company **leader** in the design and development of **telescopes** and **optomechanical** systems for **observation**, **laser communication and defense** applications on **ground and space**

Involved in several **ESA & Horizon** projects:
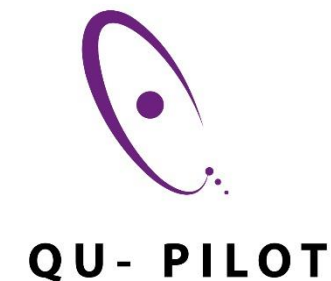
THINKQUANTUM Standard Products

Thike

The Source of True Quantum Randomness by ThinkQuantum

QuKy

The Quantum Key Distribution Platform by ThinkQuantum
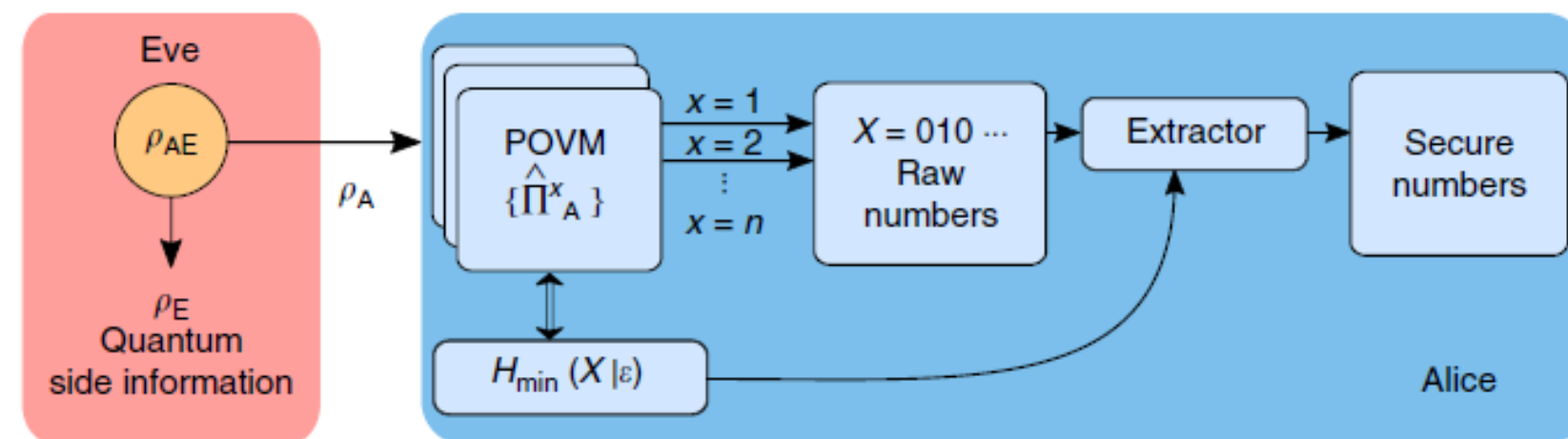
High-speed Source-Device-Independent QRNG

Marco Avesani [1], Davide G. Marangon[1], Giuseppe Vallone [1,2] & Paolo Villoresi [1,2]

☐   Source-device-independent heterodyne-based quantum random number generator at 17   110   2018
Gbps
M Avesani, DG Marangon, G Vallone, P Villoresi
Nature communications 9 (1), 5365

Our **QRNG** exploits a **Source-Device-Independent** protocol, where the source of quantum states can be completely controlled by an attacker. The security proof is valid against **general attacks** in the **finite-size** scenario.

This is the **only Semi-DI QRNG** on the market.

This solution combines **unprecedented security** with **high performances** in a **plug&play** device.
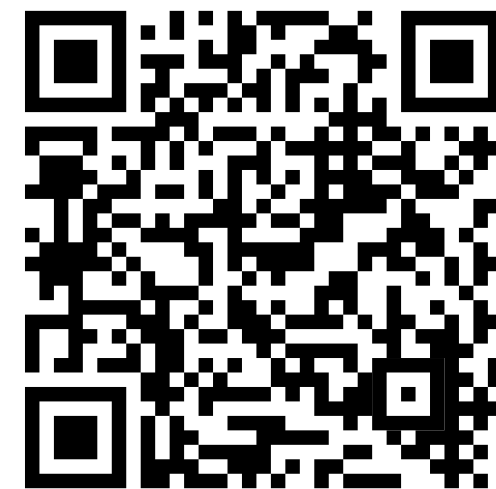
THINKQUANTUM OFFER: QRNG

The Source of True Quantum Randomness by ThinkQuantum

Stand Alone version (Rack and benchtop)

**OEM version
(available for integration into products)**

ThiKe, The Source of True Quantum Randomness by ThinkQuantum, provides the most secure random numbers, based on the Heisenberg's uncertainty principle. At the core of the device, a true random entropy source enables a ultra fast stream of random numbers.

Framework: source-device independent

Internal quantum entropy source: 2 Gbps

Secure random bit rate: 330 Mbps stream already extracted

Interface: RJ45. Socket stream or REST API

Applications: Classical, Quantum & Post-Quantum Crypto, Monte-Carlo simulations…

THINKQUANTUM OFFER: QKD

QuKy

The Quantum Key Distribution Platform by ThinkQuantum

QuKy, is our **stable** and **robust** QKD Platform for **fiber** and **free-space** links. Based on:

- **3-state 1-decoy BB84** protocol secured against general attacks
- **Polarization-based** encoding using the **IPOGNAC**
- Integrates the **QRNG**
- Compatible with ETSI 04, 014, SKIP …
- Compact 2U system

Secret Key Rate: 2.2 kb/s (13 dB) [typ]

Max losses: - Standard 20dB (100km)
                              - Premium 23dB (115km)
                              - with SNSPD 36dB (180km)

QuKy: key features

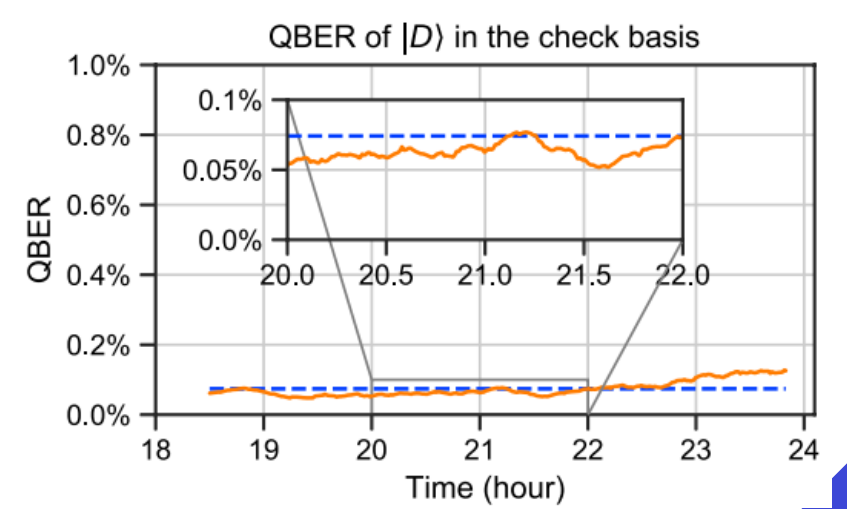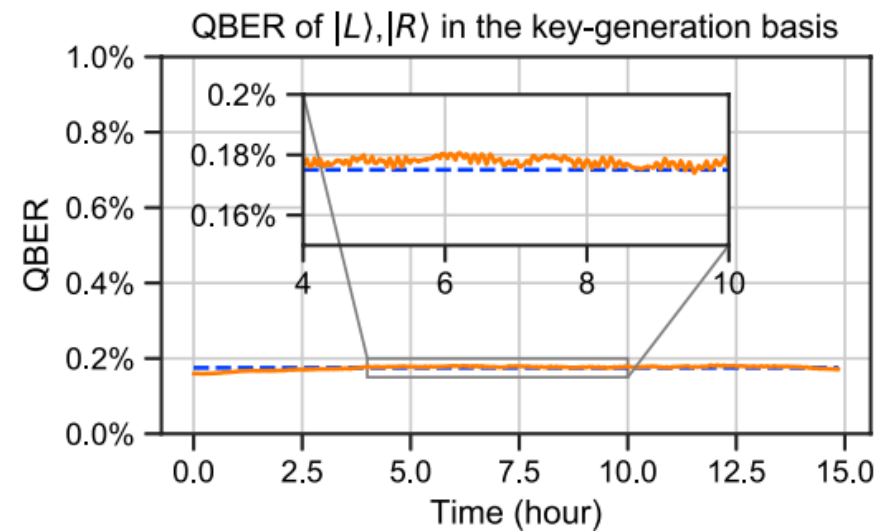|		
🔑	**Key-Rate**	High key generation thanks to the lowest QBER provided by the embedded iPognac (patented solution).
🕐	**Qubit4Sync**	Efficient Qubit-based self-synchronization does not require additional fibers.
🎲	**True QRNG Stream**	QRN2Qubit direct stream (no pseudo-random, no expansion) from embedded QRNG to Qubit Preparation Stage.
⚒️	**Robust & Reliable**	Quick installation, robust and reliable devices coming with hot-swappable power supply system (1+1 redundant).
BB84	**Protocol**	QKD system based on BB84 protocol and polarization encoding.
	Networking	The versatile system enables the modular implementation of complex network topologies. Compatible with ETSI 014, ETSI 004.
	Modularity	Smart system designed to work with either fiber or free-space optical link.
🔄	**Interoperability**	Alice & Bob do not need to be matched: the same device can work with different units.
	Tailored Solution	Flexible design for customized solutions (i.e. SPAD or SNSPD, co-existence of Quantum & Classical on same fiber).
🇪🇺	**EU27**	ThinkQuantum, based in Italy with an Italian shareholder structure, offers a reliable European Supply Chain.

QuKy: key features

🔑	**Key-Rate**	High key generation thanks to the lowest QBER provided by the embedded iPognac (patented solution).
🕐	**Qubit4Sync**	Efficient Qubit-based self-synchronization does not require additional fibers.
🎲	**True QRNG Stream**	QRN2Qubit direct stream (no pseudo-random, no expansion) from embedded QRNG to Qubit Preparation Stage.
⚒️	**Robust & Reliable**	Quick installation, robust and reliable devices coming with hot-swappable power supply system (1+1 redundant).
BB84	**Protocol**	QKD system based on BB84 protocol and polarization encoding.
🕸️	**Networking**	The versatile system enables the modular implementation of complex network topologies. Compatible with ETSI 014, ETSI 004.
🧱	**Modularity**	Smart system designed to work with either fiber or free-space optical link.
🔄	**Interoperability**	Alice & Bob do not need to be matched: the same device can work with different units.
🧍	**Tailored Solution**	Flexible design for customized solutions (i.e. SPAD or SNSPD, co-existence of Quantum & Classical on same fiber).
🇪🇺	**EU27**	ThinkQuantum, based in Italy with an Italian shareholder structure, offers a reliable European Supply Chain.

IPOGNAC polarization encoder
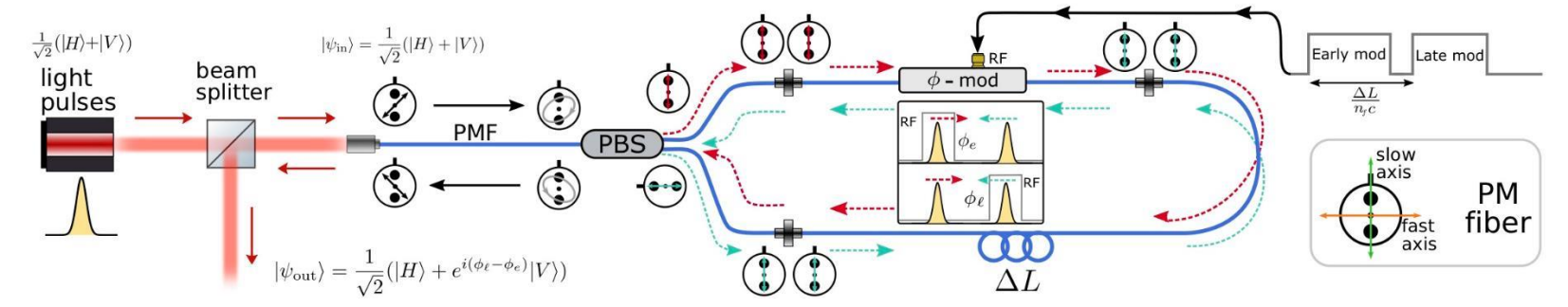
- **Long-term stability**

- High **stability** wrt **thermal** and mechanical fluctuations

- Extremely **low** intrinsic **QBER**

Optics Letters 45, 4706 (2020), patented

QuKy: key features

🔑	**Key-Rate**	High key generation thanks to the lowest QBER provided by the embedded iPognac (patented solution).
🕐	**Qubit4Sync**	Efficient Qubit-based self-synchronization does not require additional fibers.
🎲	**True QRNG Stream**	QRN2Qubit direct stream (no pseudo-random, no expansion) from embedded QRNG to Qubit Preparation Stage.
	Robust & Reliable	Quick installation, robust and reliable devices coming with hot-swappable power supply system (1+1 redundant).
BB84	**Protocol**	QKD system based on BB84 protocol and polarization encoding.
	Networking	The versatile system enables the modular implementation of complex network topologies. Compatible with ETSI 014, ETSI 004.
	Modularity	Smart system designed to work with either fiber or free-space optical link.
🔄	**Interoperability**	Alice & Bob do not need to be matched: the same device can work with different units.
	Tailored Solution	Flexible design for customized solutions (i.e. SPAD or SNSPD, co-existence of Quantum & Classical on same fiber).
🇪🇺	**EU27**	ThinkQuantum, based in Italy with an Italian shareholder structure, offers a reliable European Supply Chain.

Qubit4Sync synchronization
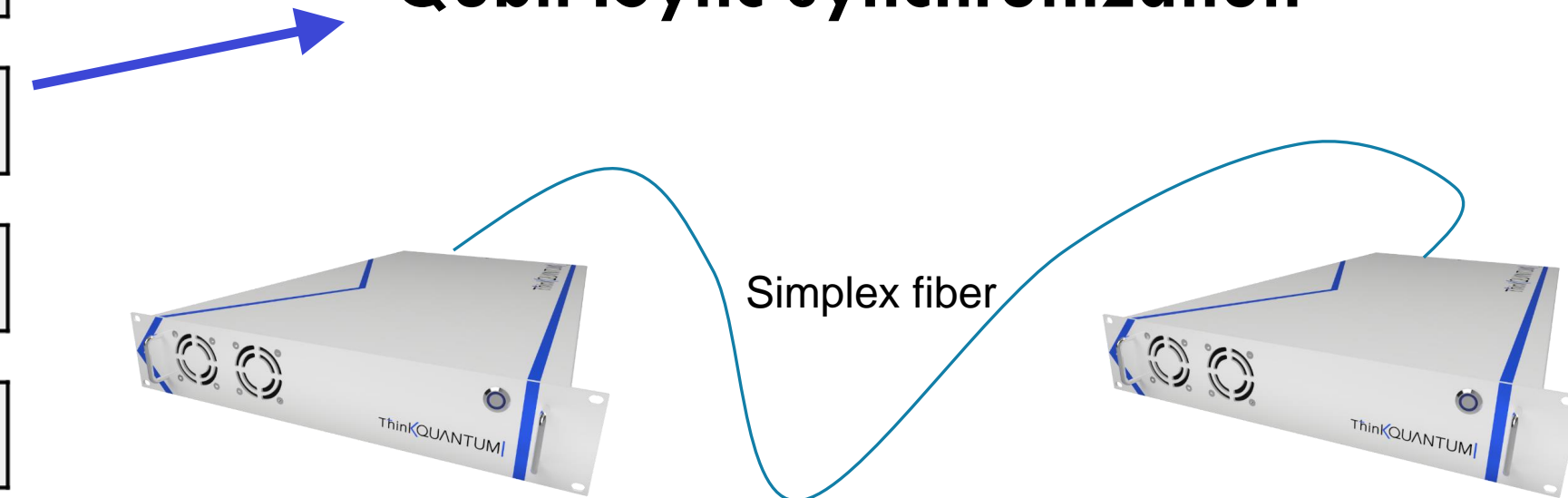
Simplex fiber

- **Synchronization** is performed using directly the **Qubits** via the **Qubit4Sync** protocol
- No need of additional lasers or detectors
- **Only one simplex fiber** is required for the operation.
- Crucial for scenarios with scares fiber availability

QuKy: key features

🔑	**Key-Rate**	High key generation thanks to the lowest QBER provided by the embedded iPognac (patented solution).
🕐	**Qubit4Sync**	Efficient Qubit-based self-synchronization does not require additional fibers.
🎲	**True QRNG Stream**	QRN2Qubit direct stream (no pseudo-random, no expansion) from embedded QRNG to Qubit Preparation Stage.
⚒	**Robust & Reliable**	Quick installation, robust and reliable devices coming with hot-swappable power supply system (1+1 redundant).
BB84	**Protocol**	QKD system based on BB84 protocol and polarization encoding.
⚛	**Networking**	The versatile system enables the modular implementation of complex network topologies. Compatible with ETSI 014, ETSI 004.
🧱	**Modularity**	Smart system designed to work with either fiber or free-space optical link.
🔄	**Interoperability**	Alice & Bob do not need to be matched: the same device can work with different units.
👥	**Tailored Solution**	Flexible design for customized solutions (i.e. SPAD or SNSPD, co-existence of Quantum & Classical on same fiber).
🇪🇺	**EU27**	ThinkQuantum, based in Italy with an Italian shareholder structure, offers a reliable European Supply Chain.

QRN2Qubit

QRNG

QKD

- **Each QKD transmitter contains a QRNG**
- **All the choices by the QKD** transmitter such as **state's and basis** preparation are derived by a fresh random number generated by the **QRNG**
- **No PRNG or expansion involved:**
- Continuous stream of random numbers in real time for the highest security

QuKy: key features

|		
🔑	**Key-Rate**	High key generation thanks to the lowest QBER provided by the embedded iPognac (patented solution).
🕐	**Qubit4Sync**	Efficient Qubit-based self-synchronization does not require additional fibers.
🎲	**True QRNG Stream**	QRN2Qubit direct stream (no pseudo-random, no expansion) from embedded QRNG to Qubit Preparation Stage.
⚒	**Robust & Reliable**	Quick installation, robust and reliable devices coming with hot-swappable power supply system (1+1 redundant).
BB84	**Protocol**	QKD system based on BB84 protocol and polarization encoding.
	Networking	The versatile system enables the modular implementation of complex network topologies. Compatible with ETSI 014, ETSI 004.
	Modularity	Smart system designed to work with either fiber or free-space optical link.
🔄	**Interoperability**	Alice & Bob do not need to be matched: the same device can work with different units.
	Tailored Solution	Flexible design for customized solutions (i.e. SPAD or SNSPD, co-existence of Quantum & Classical on same fiber).
🇪🇺	**EU27**	ThinkQuantum, based in Italy with an Italian shareholder structure, offers a reliable European Supply Chain.

Polarization encoding

Fiber   **Free-space**   **Satellite**
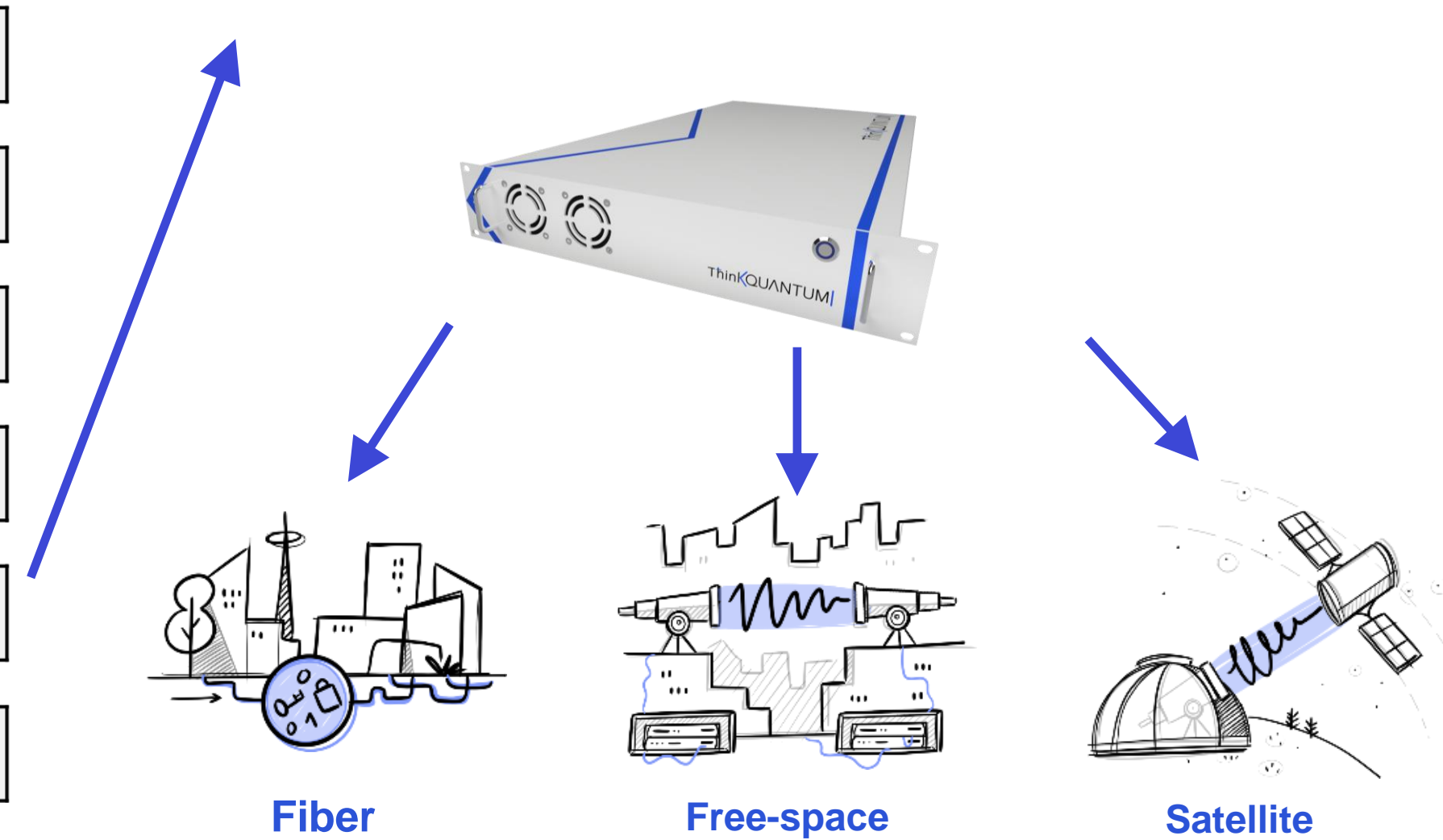
- **Polarization allows to use a single device for multiple different channels**
- **Low QBER**
- **Unmatched Alice and Bob**
- **BB84 is robust and secure against general attacks**

QuKy: key features

🔑	**Key-Rate**	High key generation thanks to the lowest QBER provided by the embedded iPognac (patented solution).
🕐	**Qubit4Sync**	Efficient Qubit-based self-synchronization does not require additional fibers.
🎲	**True QRNG Stream**	QRN2Qubit direct stream (no pseudo-random, no expansion) from embedded QRNG to Qubit Preparation Stage.
⚒️	**Robust & Reliable**	Quick installation, robust and reliable devices coming with hot-swappable power supply system (1+1 redundant).
BB84	**Protocol**	QKD system based on BB84 protocol and polarization encoding.
⚙️	**Networking**	The versatile system enables the modular implementation of complex network topologies. Compatible with ETSI 014, ETSI 004.
🧱	**Modularity**	Smart system designed to work with either fiber or free-space optical link.
🔄	**Interoperability**	Alice & Bob do not need to be matched: the same device can work with different units.
👥	**Tailored Solution**	Flexible design for customized solutions (i.e. SPAD or SNSPD, co-existence of Quantum & Classical on same fiber).
🇪🇺	**EU27**	ThinkQuantum, based in Italy with an Italian shareholder structure, offers a reliable European Supply Chain.

Networking, KMS & Encryptors

- **Compatible with star and ring topologies**
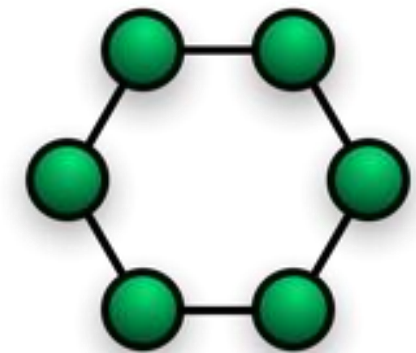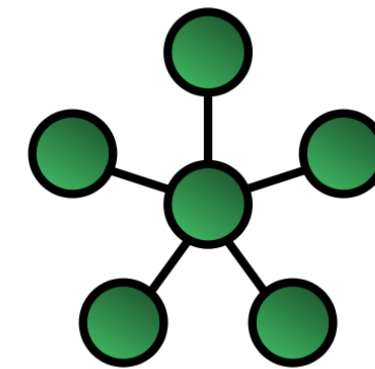
- **KMS integrated into the devices. Compatible with interoperable QKD operation**

- **Compatible with ETSI 04, ETSI 014, SKIP (other on request)**

- **System compatible and tested with encryptors from different vendors such as ADVA, Rohde & Schwarz, CISCO, Thales… always open to new partners**

QuKy: key features

🔑	**Key-Rate**	High key generation thanks to the lowest QBER provided by the embedded iPognac (patented solution).
🕐	**Qubit4Sync**	Efficient Qubit-based self-synchronization does not require additional fibers.
🎲	**True QRNG Stream**	QRN2Qubit direct stream (no pseudo-random, no expansion) from embedded QRNG to Qubit Preparation Stage.
⚒	**Robust & Reliable**	Quick installation, robust and reliable devices coming with hot-swappable power supply system (1+1 redundant).
BB84	**Protocol**	QKD system based on BB84 protocol and polarization encoding.
⚛	**Networking**	The versatile system enables the modular implementation of complex network topologies. Compatible with ETSI 014, ETSI 004.
🧱	**Modularity**	Smart system designed to work with either fiber or free-space optical link.
🔄	**Interoperability**	Alice & Bob do not need to be matched: the same device can work with different units.
👥	**Tailored Solution**	Flexible design for customized solutions (i.e. SPAD or SNSPD, co-existence of Quantum & Classical on same fiber).
🇪🇺	**EU27**	ThinkQuantum, based in Italy with an Italian shareholder structure, offers a reliable European Supply Chain.

Interoperability & Wavelength diversity

- **The systems work in the O or C band, 1ch of DWDM grid selectable by the user**

- **Alice and Bob don't need to be "optically matched" and can work in an interoperable way**

- **Bob is broadband and can work with transmitters with different wavelengths**

- **Useful for complex or reconfigurable network topologies**

QuKy stability

An important aspect of **QKD** systems from the point of view of an **end user** or **network operator is stability**

Installation at a **client facility,** used in **production over a dark fiber** to secure a critical infrastructure in Italy.

QKD used together with layer-2 **encryptors** from **ADVA.**

QKD system running for **7 months**
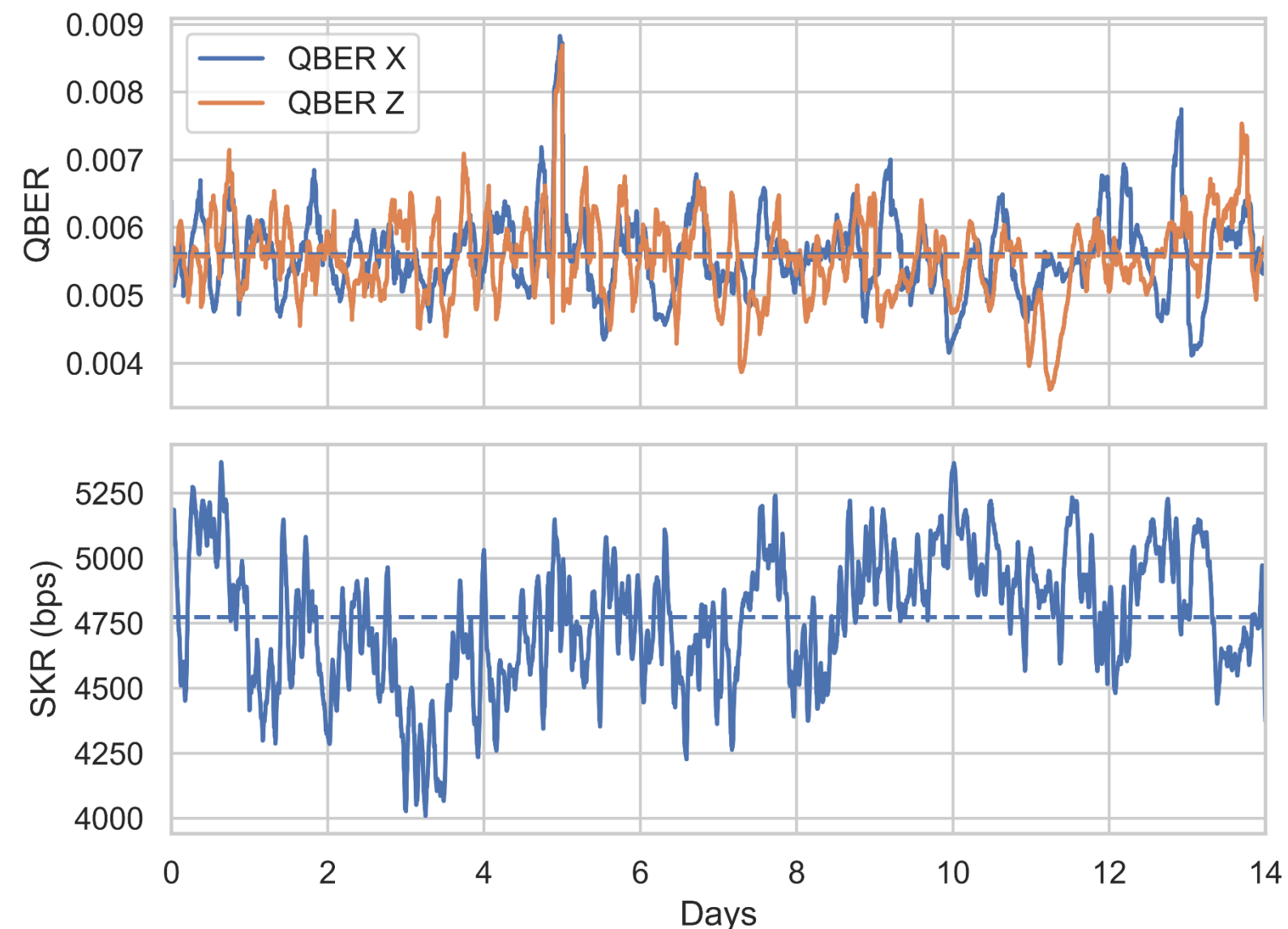
Stable Secret Key rate: 4,7kbps

Stable and Low QBER in both bases 0.58%

Challenges in developing Quantum Networks

Need to develop a quantum infrastructure compatible with the current classical telecom network. Several points to explore:

- **Dark fibers are limited and expensive: QKD should coexist** together with classical communication **on the same fibers**

- **Cannot rely on a single type of channel: fiber, free-space and satellite** links will be required. Need to develop intermodal operation

- **Multiple protocols, encodings and spectral channels will be used.** Study their compatibility and integration in the network

- **Optimization of the network:** a full quantum network can offer more than point-to-point. Can optimize the topology to deploy less devices or increase the rate
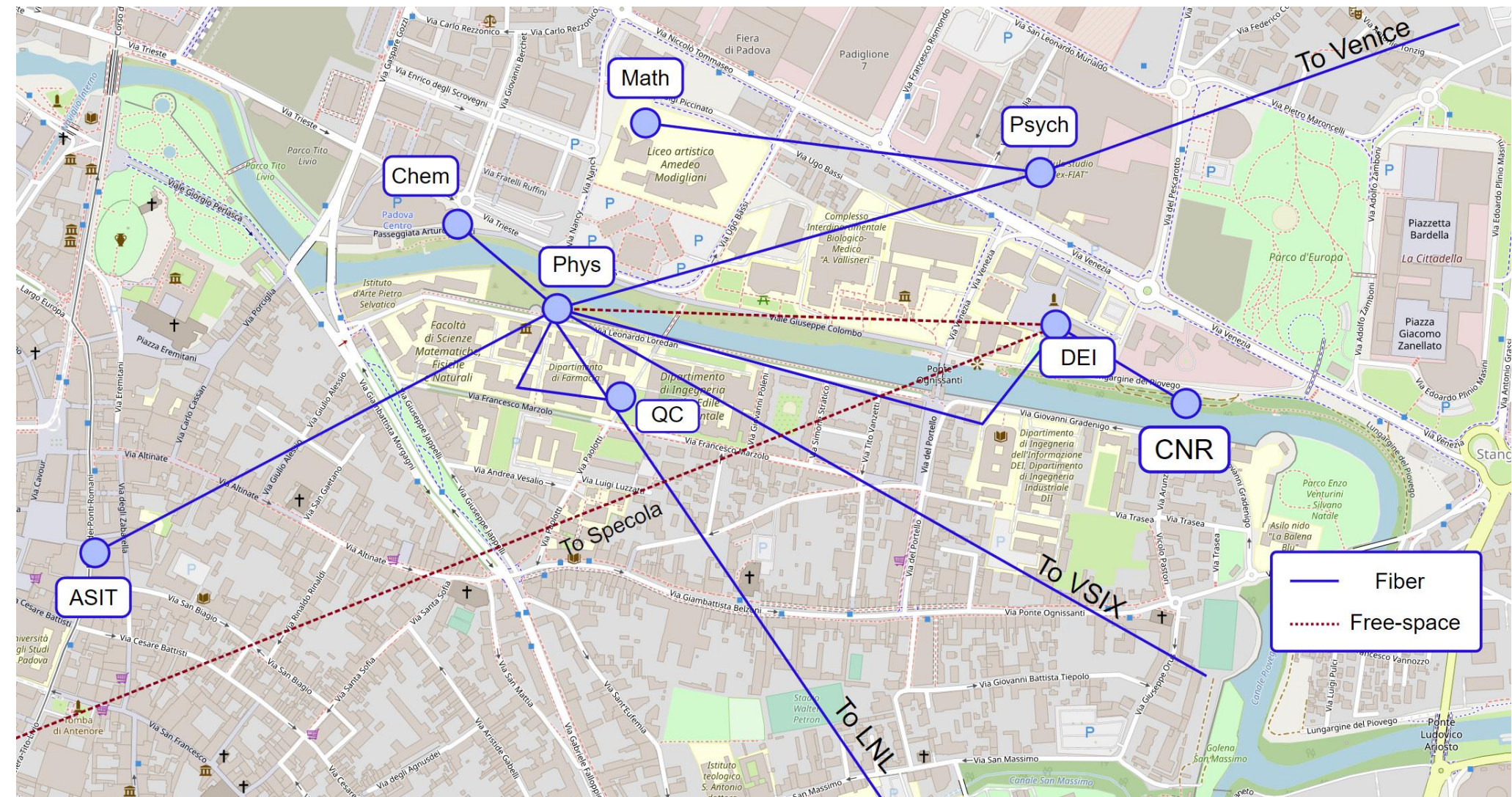
A quantum network in Padova

A Quantum Network which connects several departments of the University, together with other research institutions such as CNR, INFN and private companies.

The **network** is composed by **8 nodes** (11 soon) in the **city** and beyond.

- **Fiber** based links with both **dark and grey fibers**
- **Free-space horizontal** links
- One node (DEI) is equipped with **40-cm telescope** for both **horizontal** and **satellite** links

A quantum network in Padova

A Quantum Network which connects several departments of the University, together with other research institutions such as CNR, INFN and private companies.

The **network** is composed by **8 nodes** (11 soon) in the **city** and beyond.

- **Fiber** based links with both **dark and grey fibers**
- **Free-space horizontal** links
- One node (DEI) is equipped with **40-cm telescope** for both **horizontal** and **satellite** links
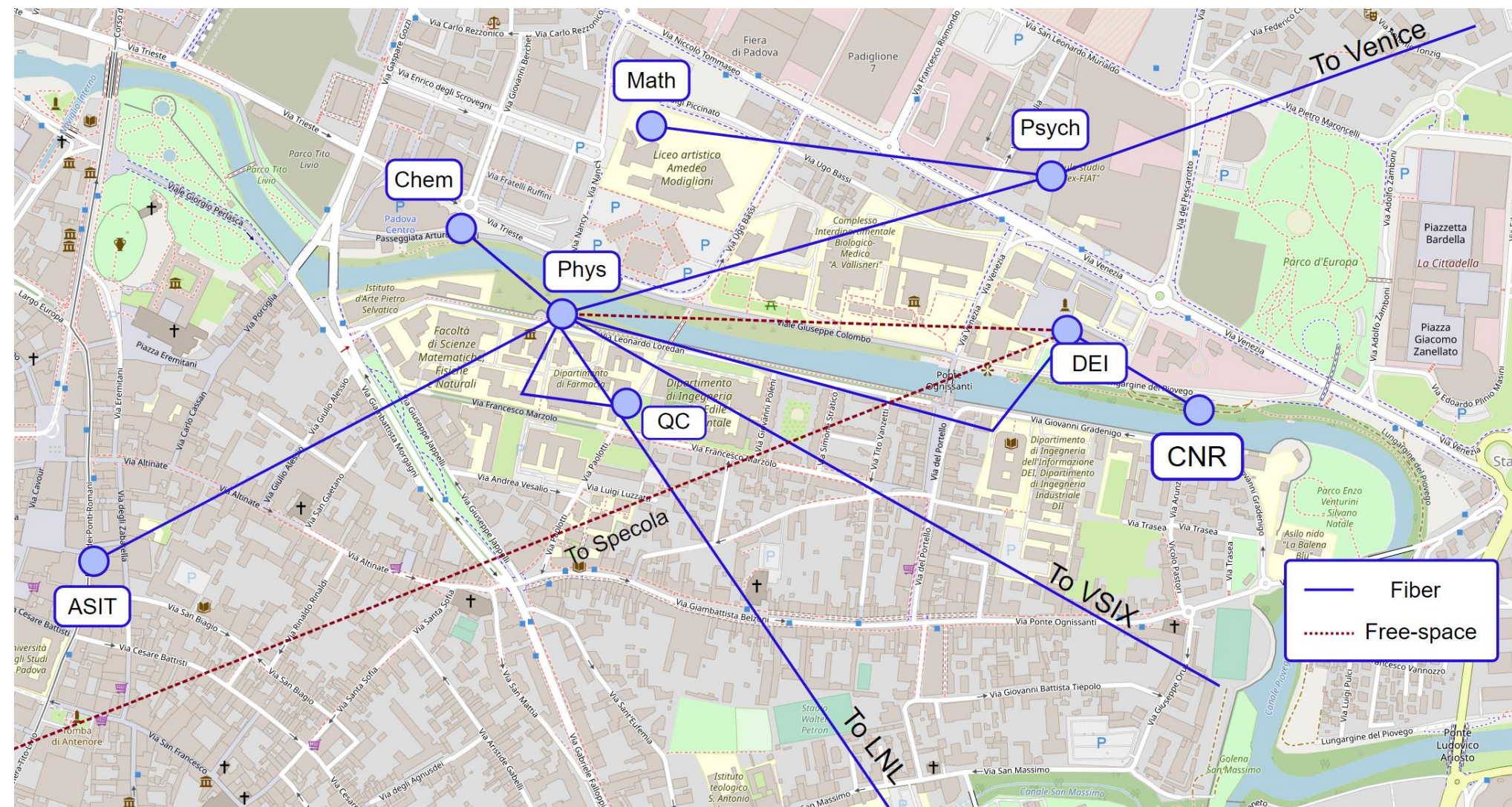

The **network has a dual use:**
- Test on a **real and deployed infrastructure new protocols and implementations** to address the previous points
- **Fixed and long term installations** to provide a **service**
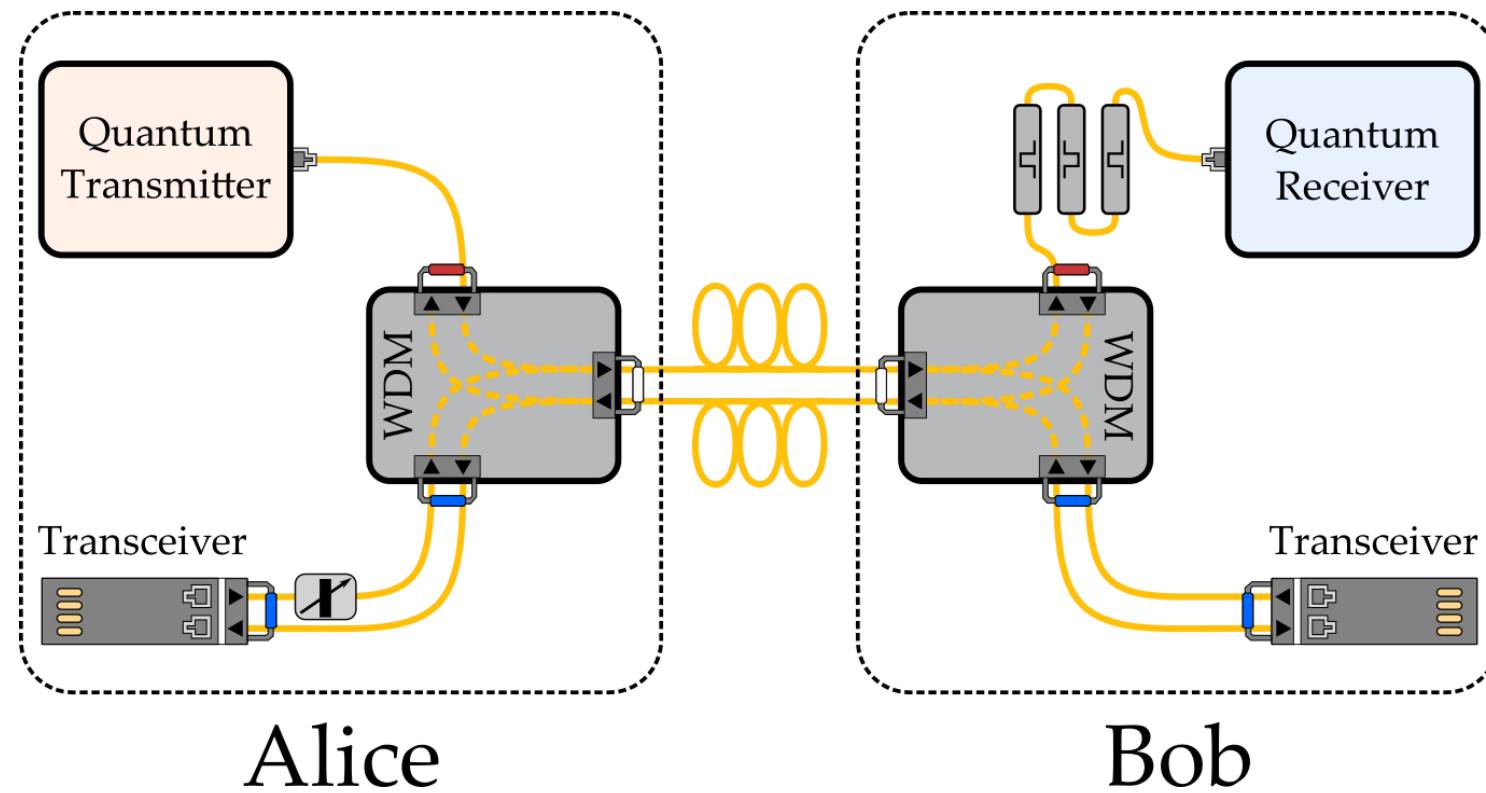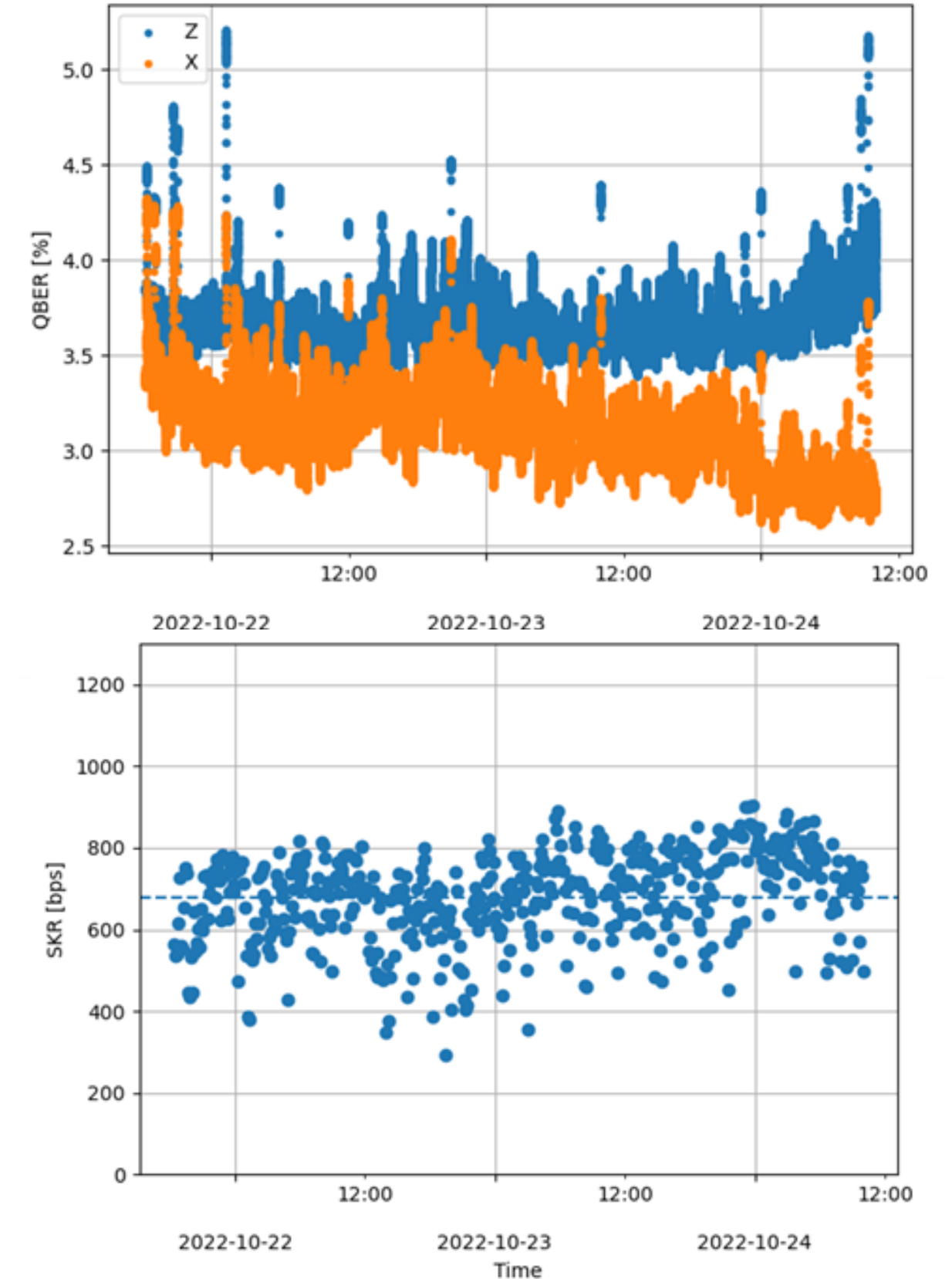
Classical and quantum coexistence
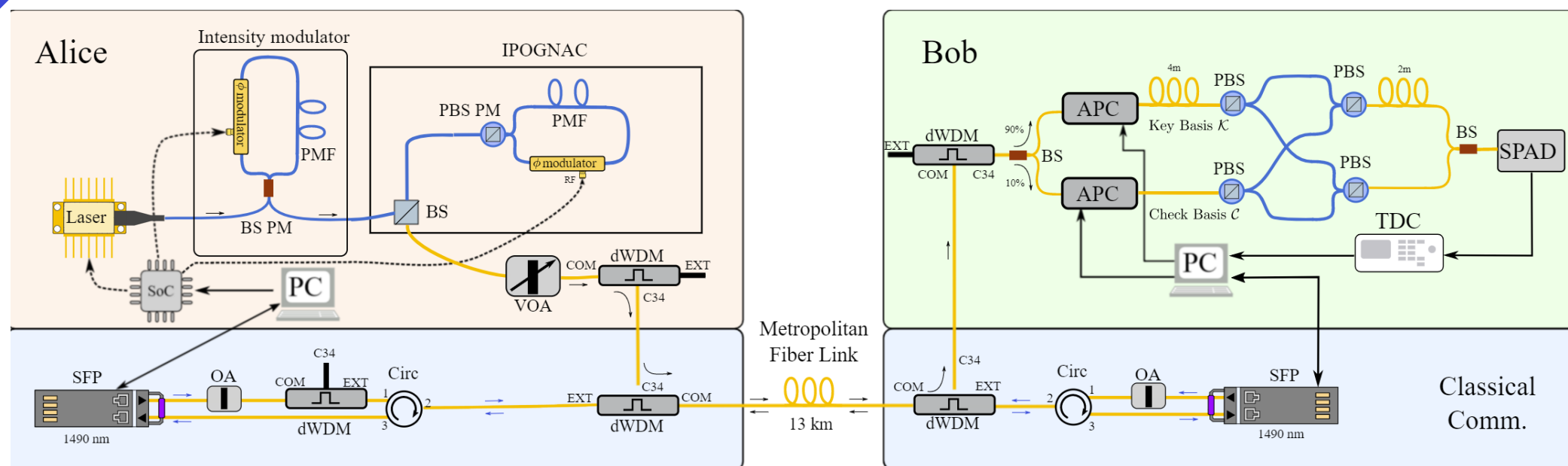
- **Coexistence of QKD and classical** communication over a **single fiber**
- **Quantum @ 1550nm (CH34 DWDM)**
- **1GBps** COTS SFP @ **1490nm**
- **13 km @6,7db** over metropolitan fibers
- **1,7kbps** of average SKR in 24h

M. Avesani et al, Journal of Lightwave Technology 40 (6), 1658 - 1663 (2022)
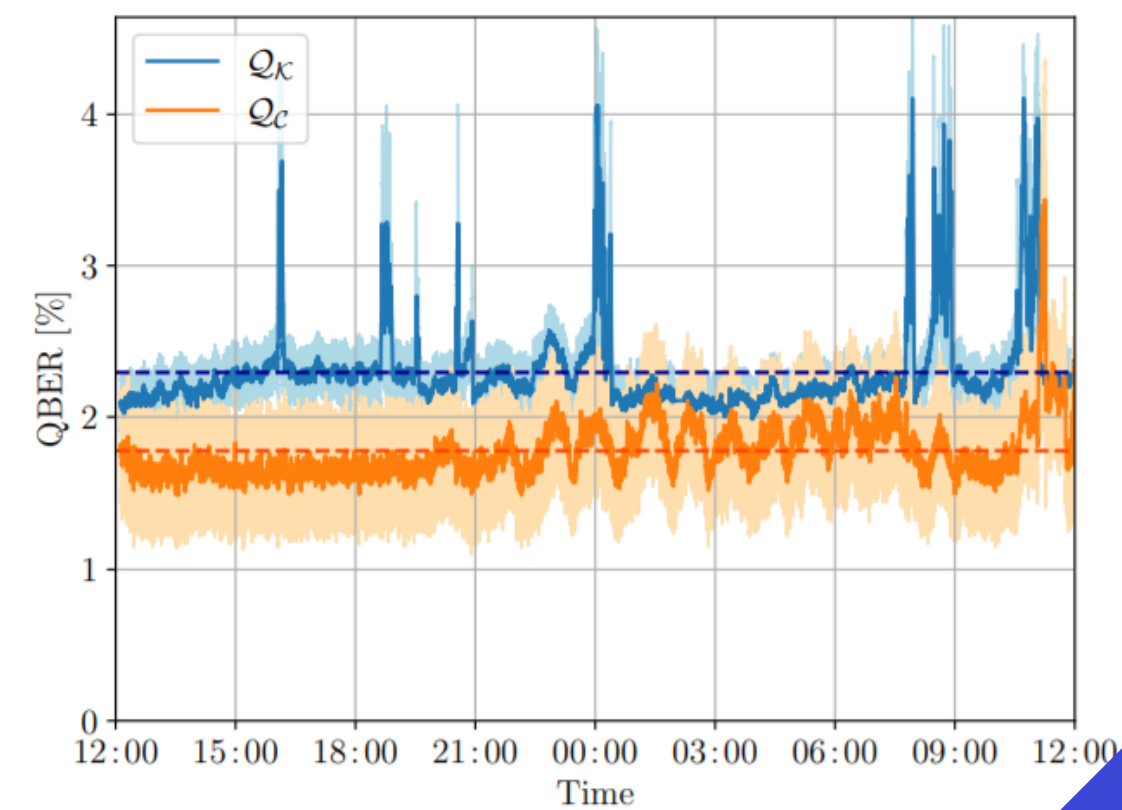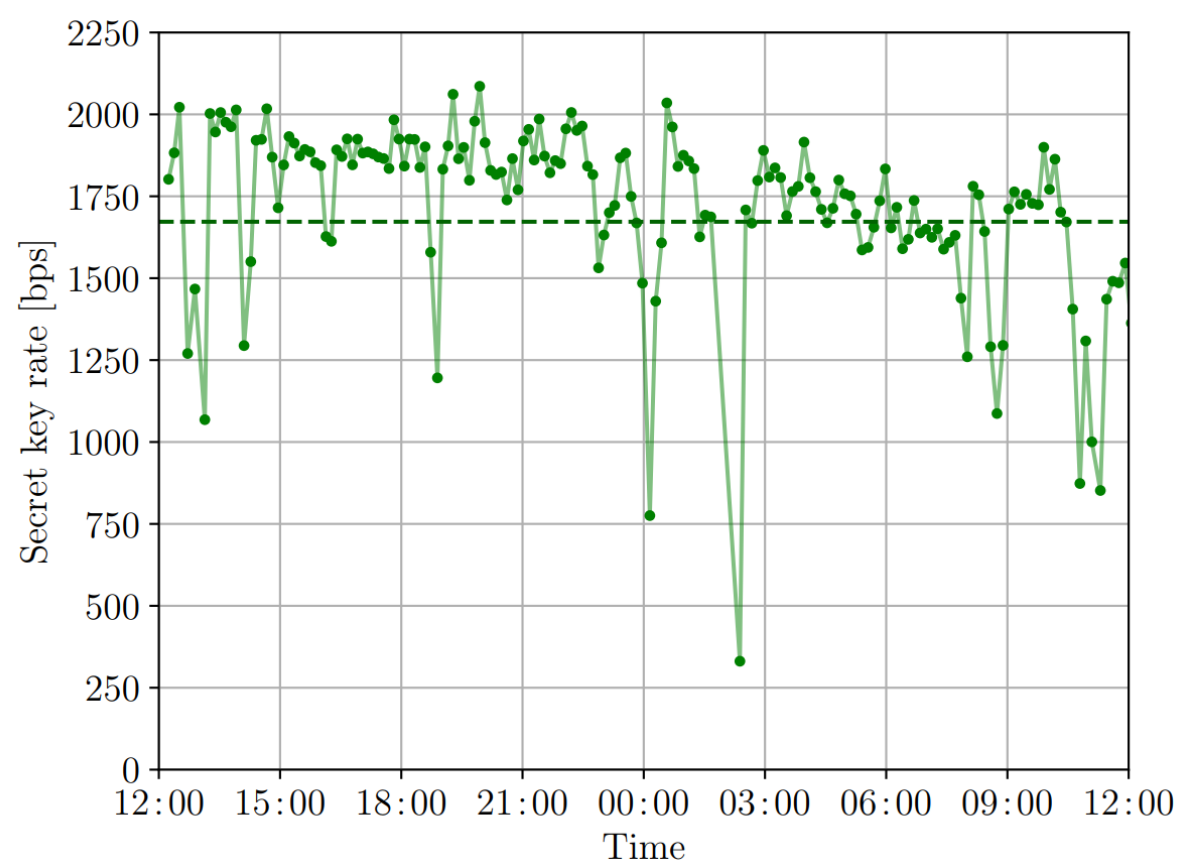
Classical and quantum coexistence

- **Deployed a stable link between ASIT and VSIX**
- Routing classical traffic from University network
- COTS 1310/1550 mux-demux, COTS DWDM filters
- **10GBps COTS XFP @ 1310nm**
- 13 km @6,7db over metropolitan fibers
- 3 day long of data
- **SKR 680 bps on average**

Classical and quantum coexistence with reversed wavelengths

1310 nm

Alice Quantum

Classic 10G

1550 nm

WDM

Channel

WDM

1310 nm

Bob Quantum

Classic 10G
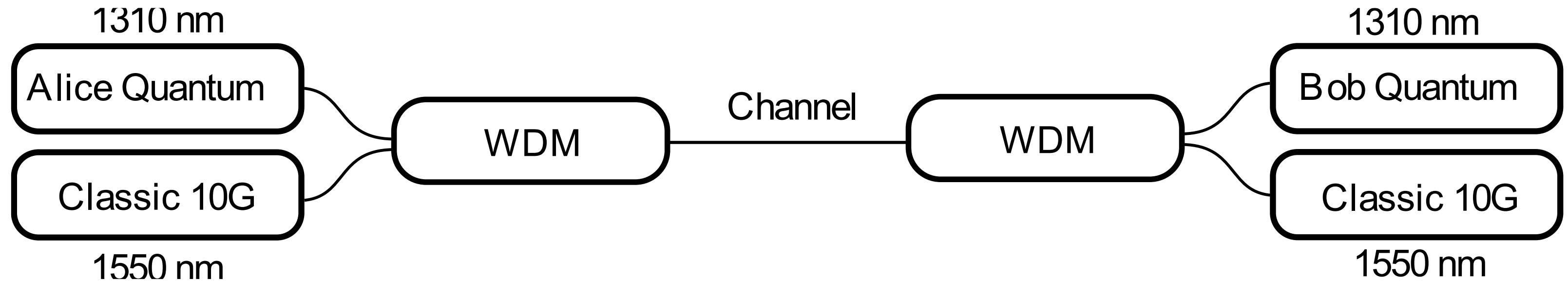
1550 nm

- **Developed a QKD system working in the O band (1310nm)**
- **Deployed a stable link between ASIT and VSIX**
- Developed to test the coexistence with dWDM transport system in the C band
- Routing classical traffic from GARR network
- **10GBps COTS SFP+ @ 1550nm**
- One entire week of data acquisition
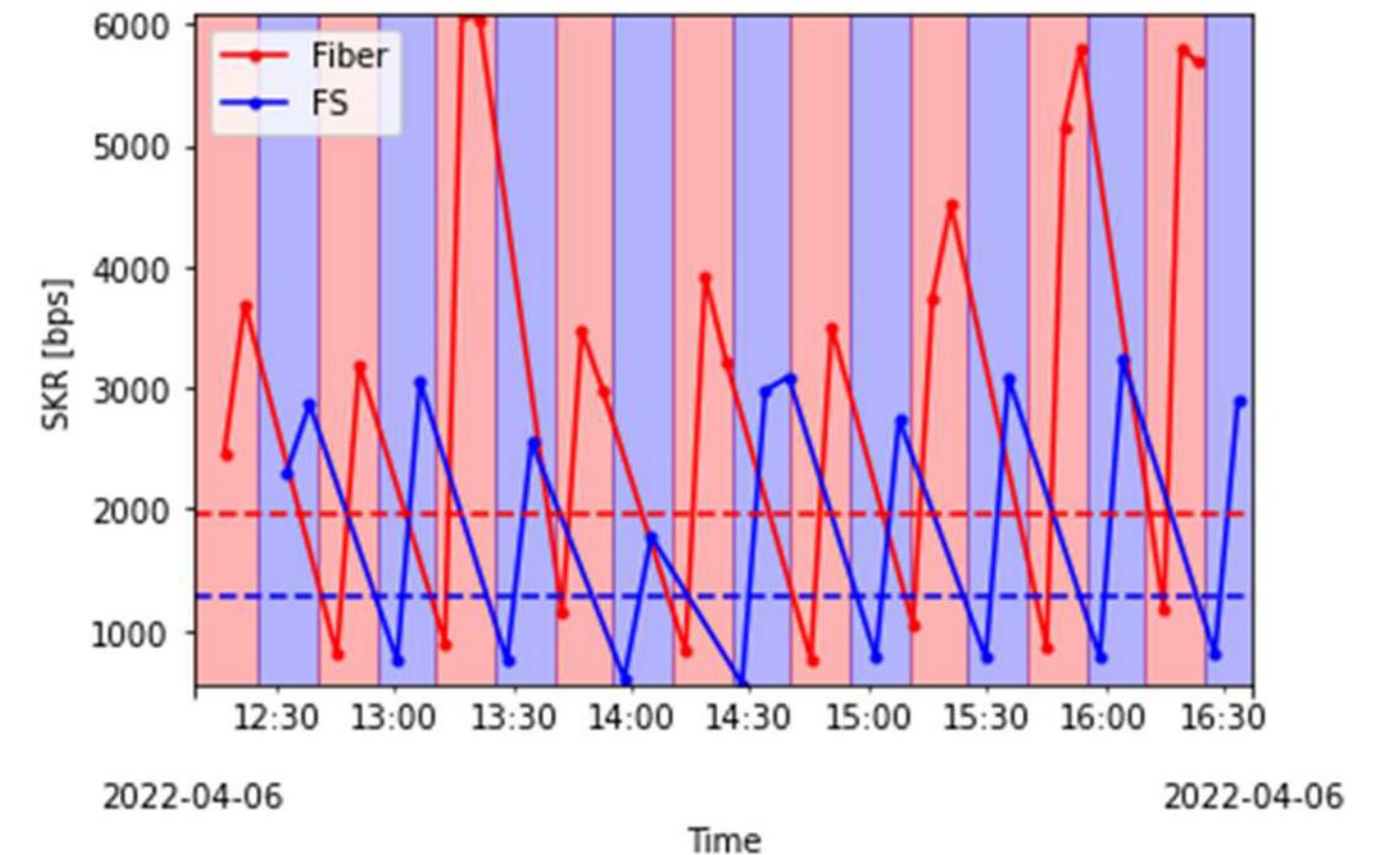- **SKR 480 bps on average**

Portable optical systems
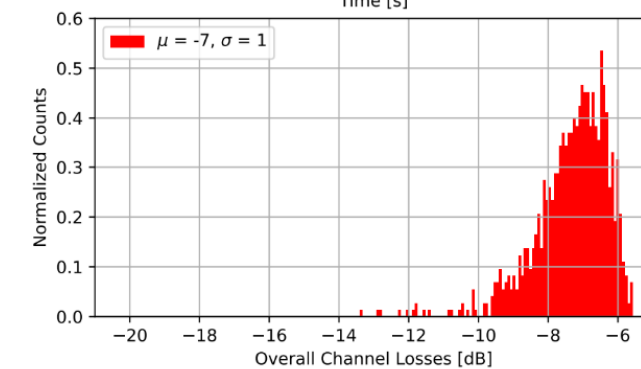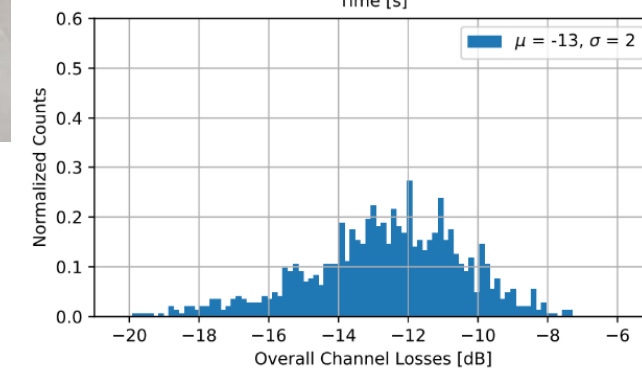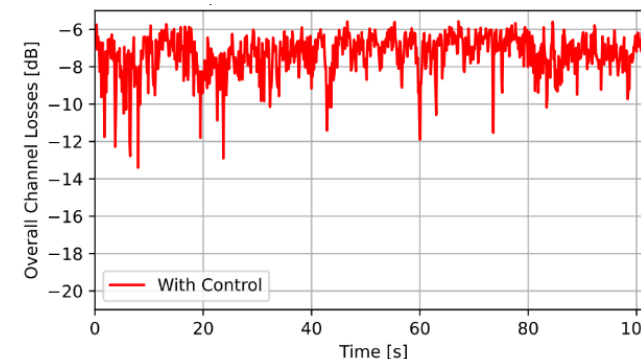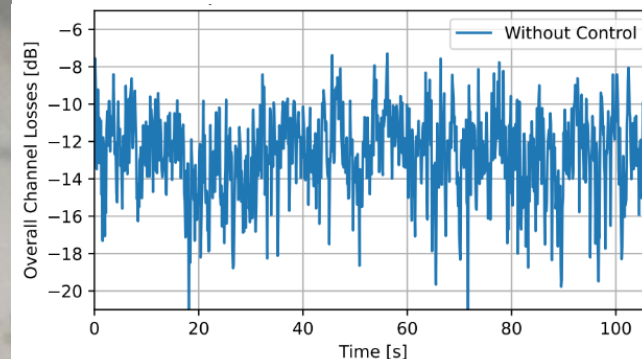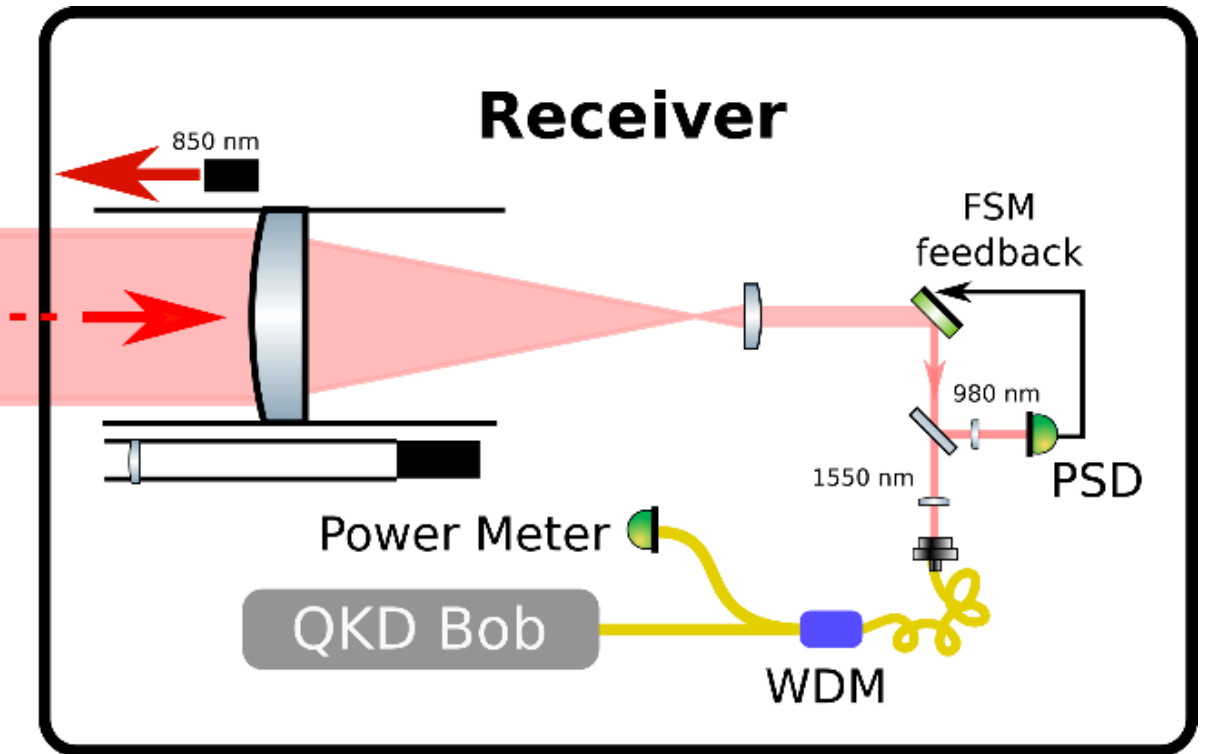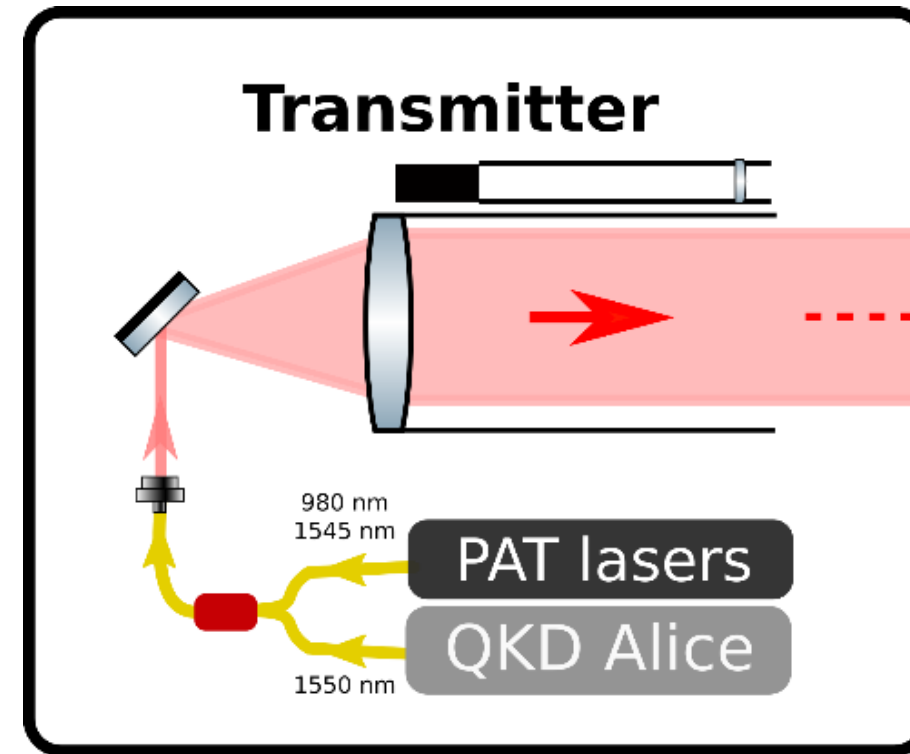
- **Couple into single mode fibers**

- **Compatible with both research and commercial QKD systems**

- **Suitable for distance up to few km**

- **Tested on a 600m-long urban link**
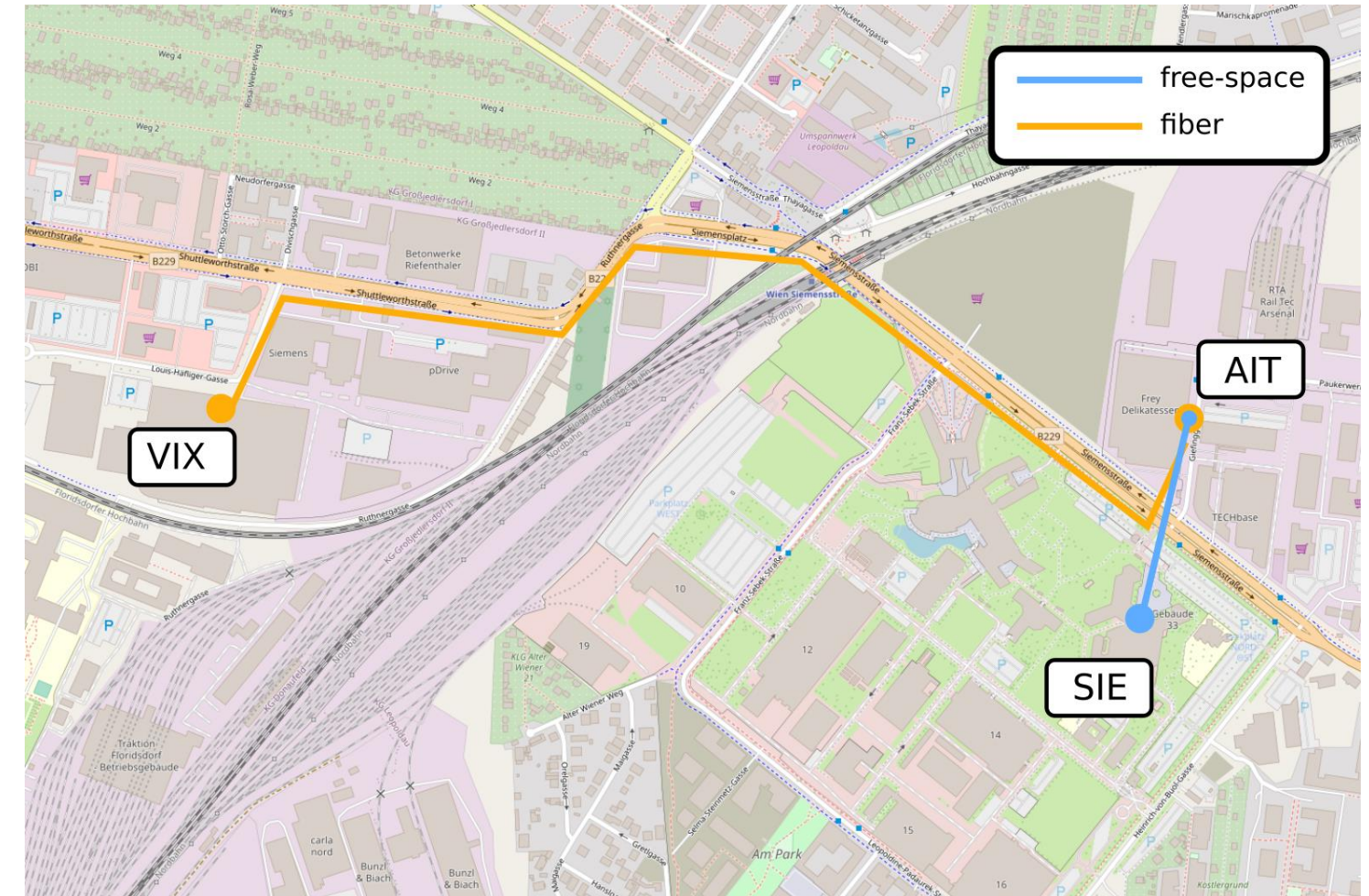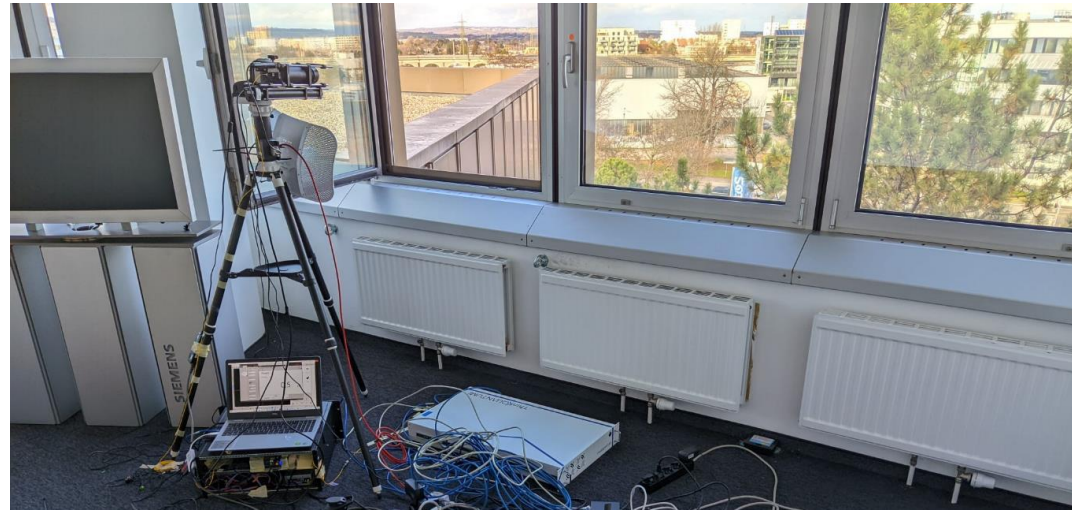
CEQUAM UC OPENQKD
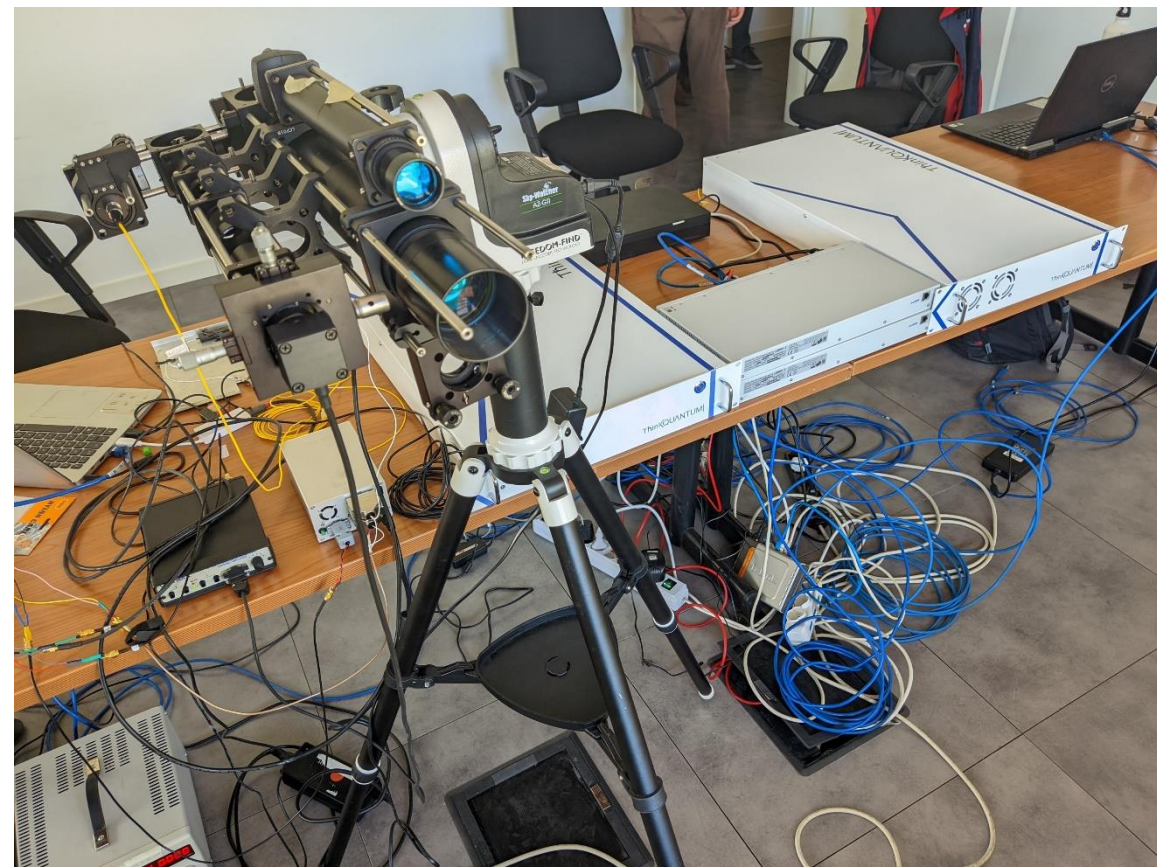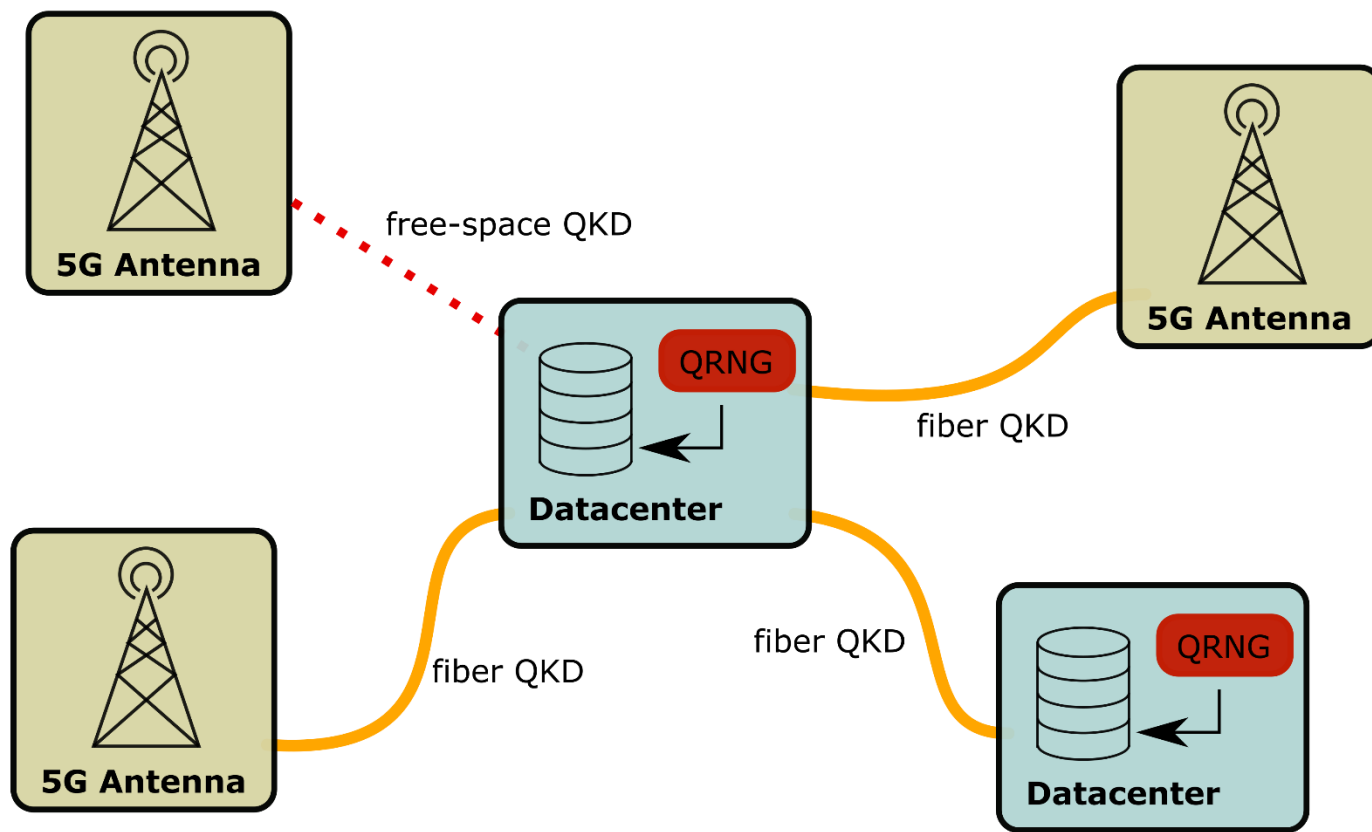
Current and average SKR for Fiber and Free Space systems

- Usecase with **TIM** to **secure 5G antennas**

- **Free-space and fiber links**

- **Single bob for different Alices time access with switch**

- **Stable performance: 2kbps fiber, 1kbps free space**

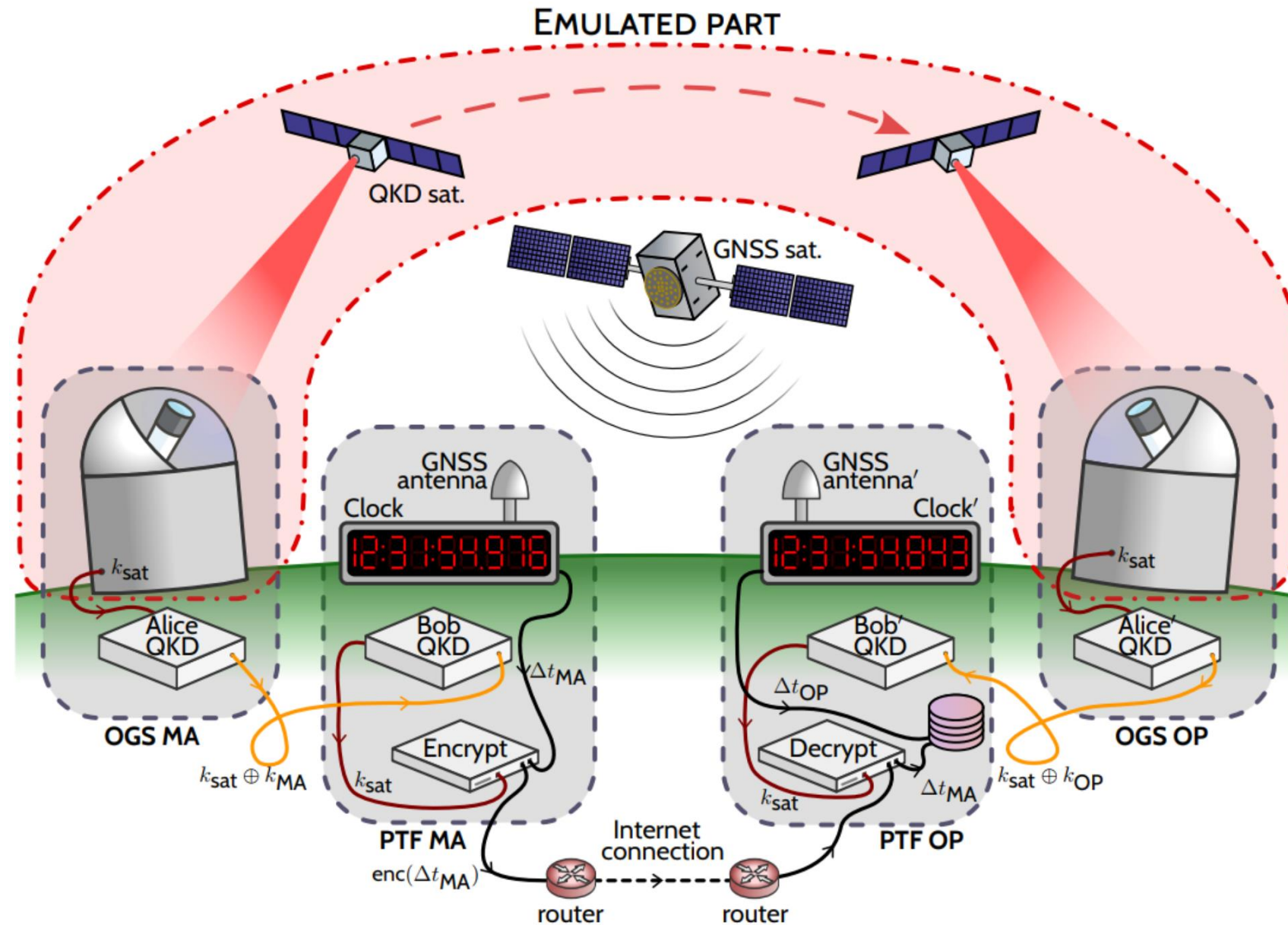- **Integration with ADVA encryptors**
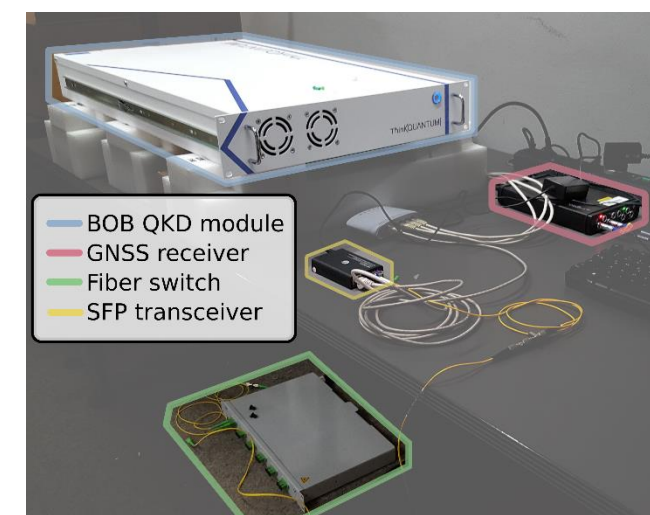
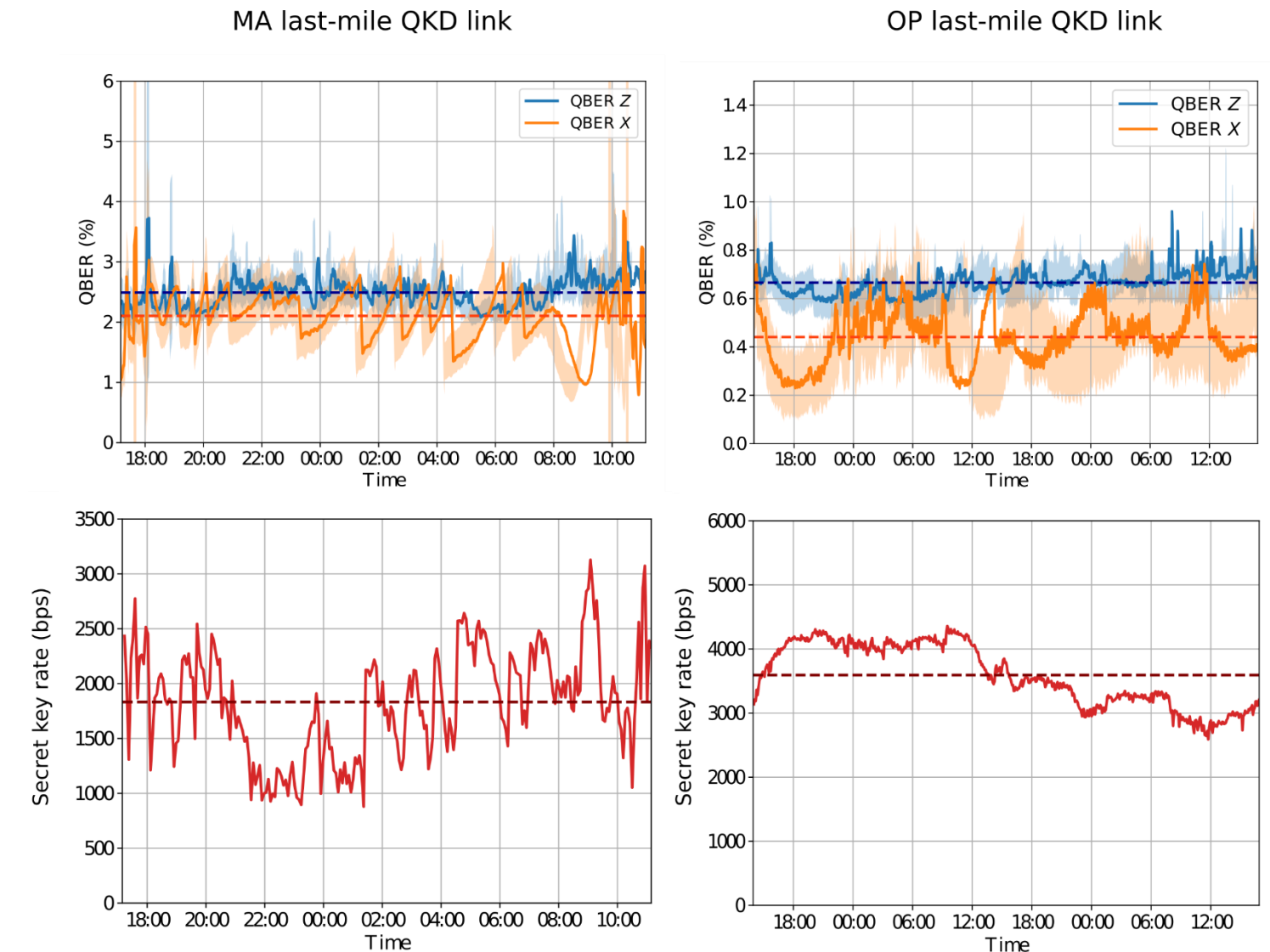# TKQ in action

SIE

VIX

AIT

- ThinkQuantum devices also in the **Vienna testbed** along a **230m free-space link + 4 km fiber link**
- We realized the experiment also **UNDER RAIN**, obtaining an average SKR around 600 bit/s
- In Vienna we also integrate two **encryptors by ADVA** and realized an encrypted video call

F. Vedovato et al., Proc. SPIE Int. Soc. Opt.Eng. 12446, 124460Q (2023)
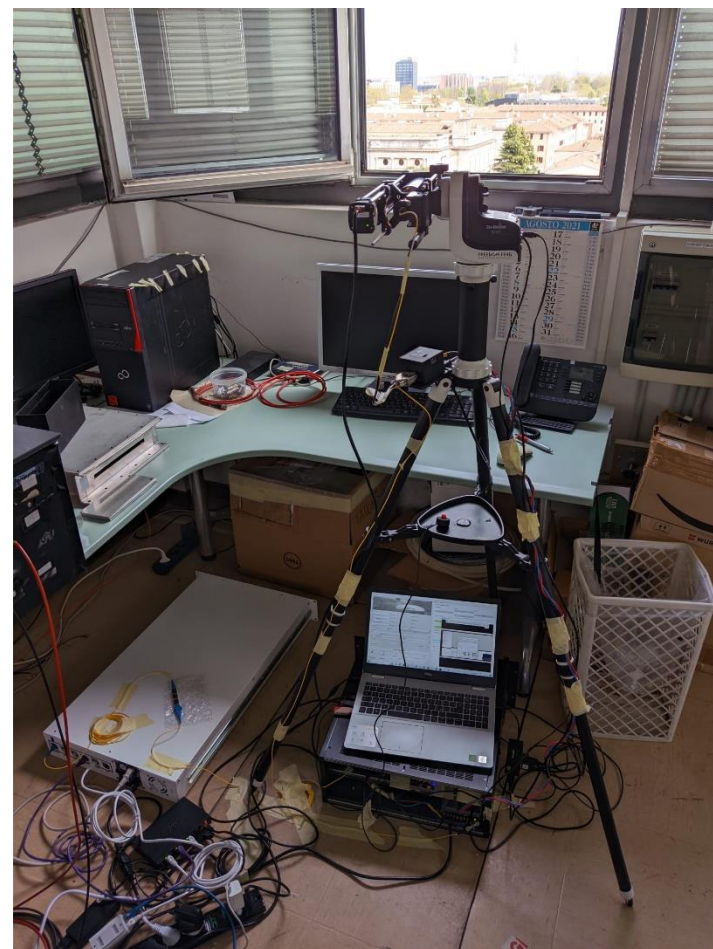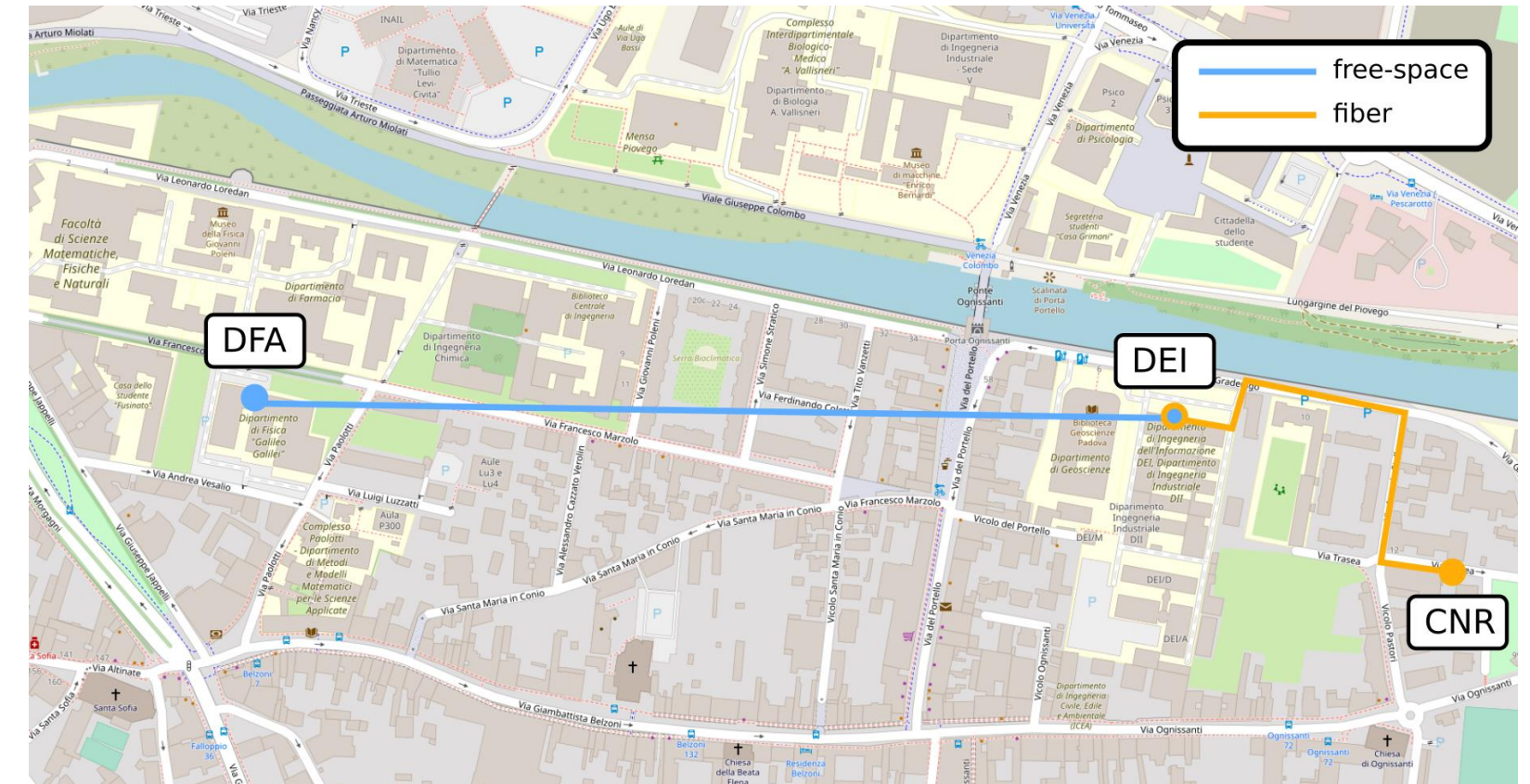
TKQ in action

EMULATED PART

- Two pairs of devices: one pair in Matera, one at DLR in Munich.
- Securing the last mile, from the telescope to the GNSS stations
- **XOR of the keys with the emulated satellite.**
- **Encryption between Matera and DLR with layer-2 over layer-3**
- **Rohde & Schwarz encryptors**

MA last-mile QKD link

OP last-mile QKD link

- BOB QKD module
- GNSS receiver
- Fiber switch
- SFP transceiver

F. Picciariello et al. (2023),
https://doi.org/10.48550/arXiv.2305.01554

TKQ in action

OPEN QKD
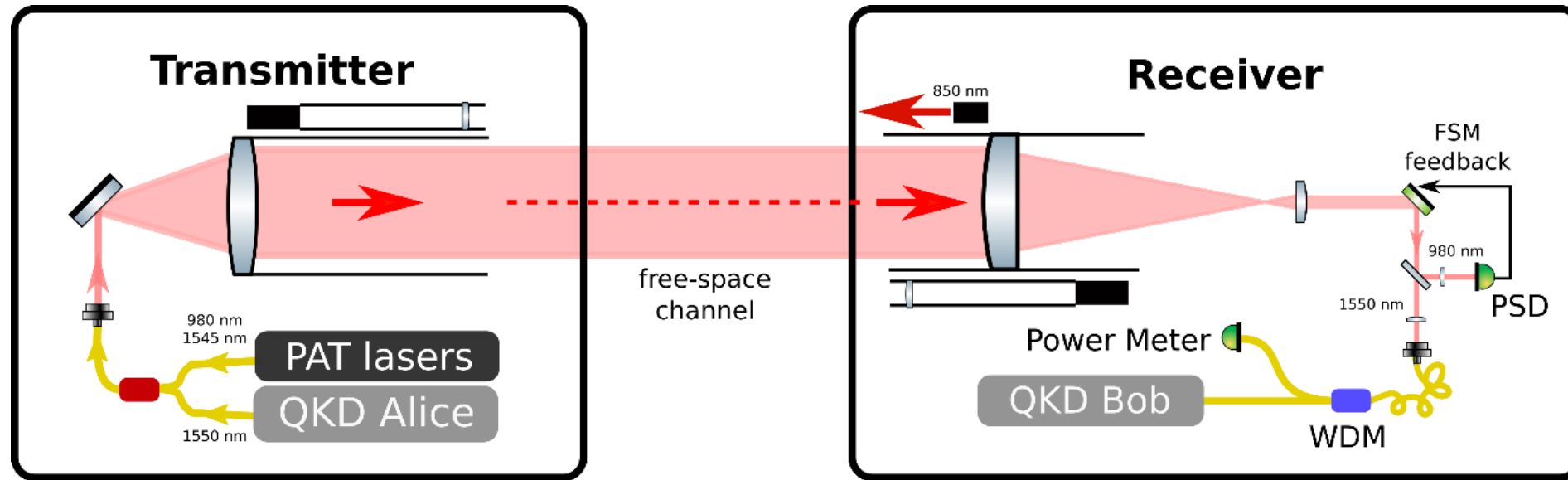
- **Intermodal operation in Padua: test of the interface between the satellite and the terrestrial infrastructure**
- **Full daylight operation**
- **600m free-space link + 500m fiber link**
- **SKR of 4kbps on free space and fiber**

F. Vedovato et al., Proc. SPIE Int. Soc. Opt.Eng. 12446, 124460Q (2023)

Multi transmitter to single receiver over different channels

Star network configurations can reduce the number of QKD devices required to share keys

- 3 nodes, same links

- Two Alice, one at DFA (UNIPD) one at CNR (ThinkQuantum)

- One Bob (ThinkQuantum) at DEI connected to both Alices

- Programmable optical switch to time multiplex access to Bob

- 4 hours in daylight operation

- SKR: 840 bps for fiber, 190 for free-space

- Key manager handles two node operation
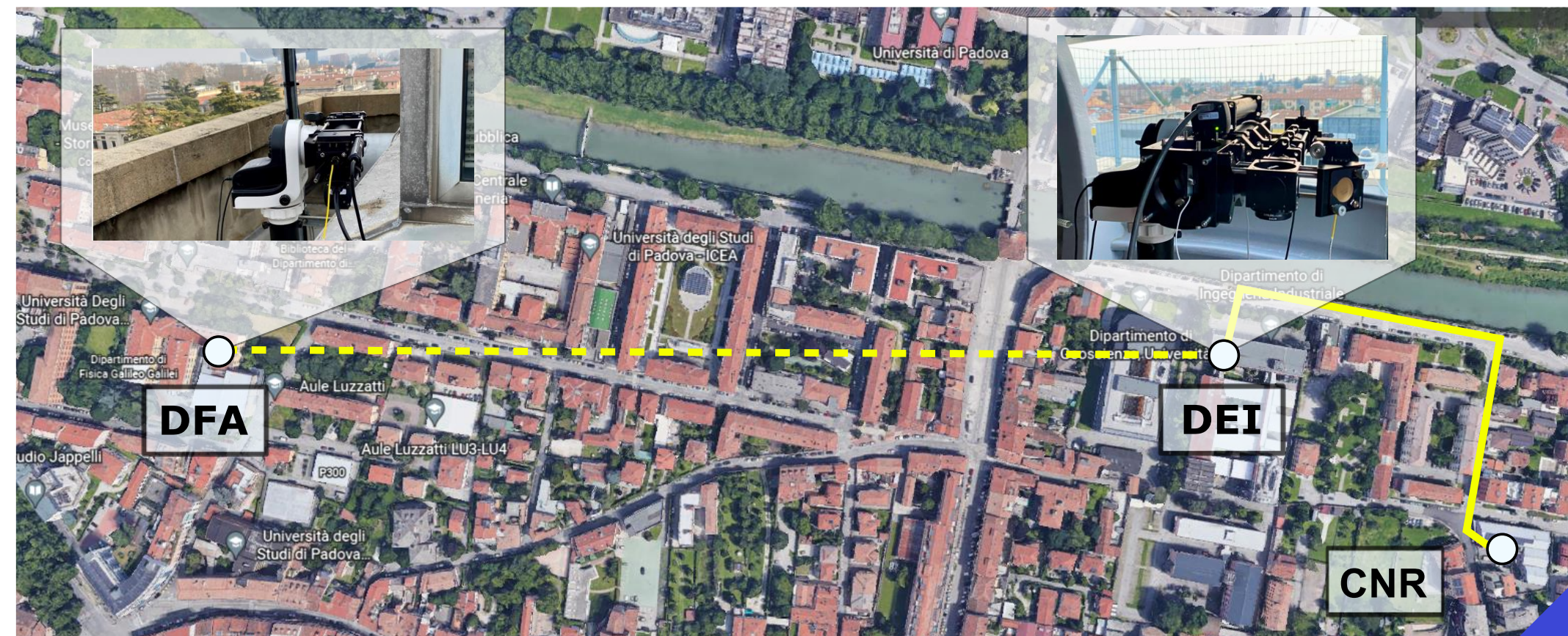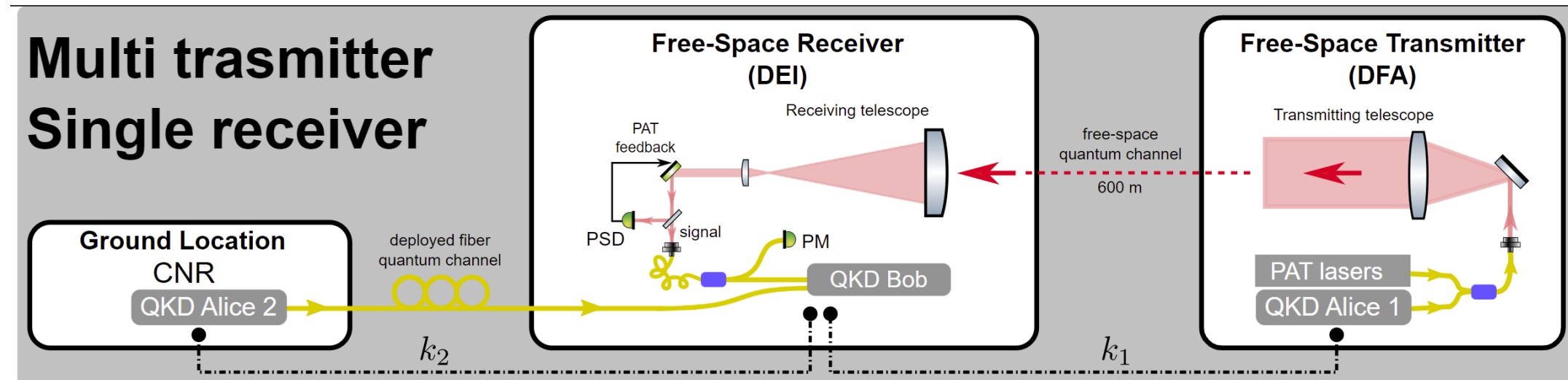
ThinkQuantum Contacts

WEBSITE

www.thinkquantum.com

info@thinkquantum.com

CERTIFIED E-MAIL

thinkquantum@legalmail.it

LEGAL ENTITY

Thinkquantum Srl

Via della Tecnica 85,

36030 Sarcedo (VI) – Italy

INNOVATION LABS

Via Trasea 7,

35131 Padova - Italy