QCoSOne: a Prototype System for Daylight Free-Space Quantum Key Distribution at Telecom Wavelength

Matteo Schiavon

Department of Information Engineering - UniPD
Current: LIP6 - Sorbonne University

14 November 2019

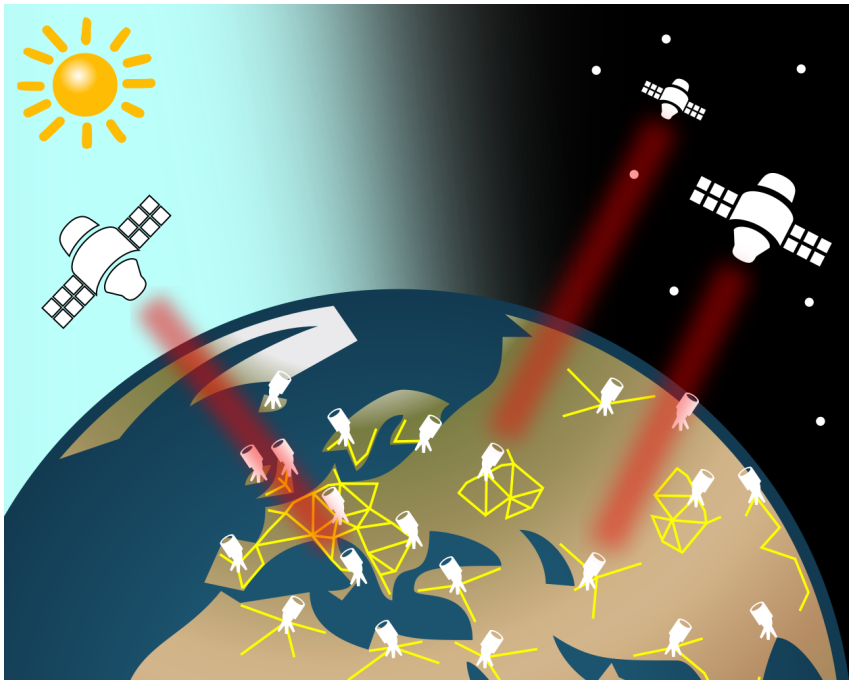
DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

Satellite QKD - Motivations

Current *free-space quantum communication (QC) technology* **cannot compete** with its fiber-based counterpart

BUT

it is a **fundamental component** of a *global-scale QC network*

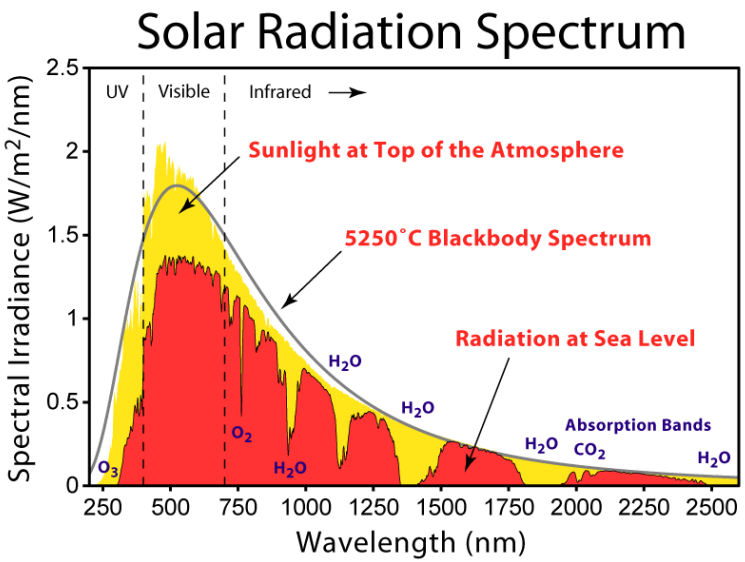


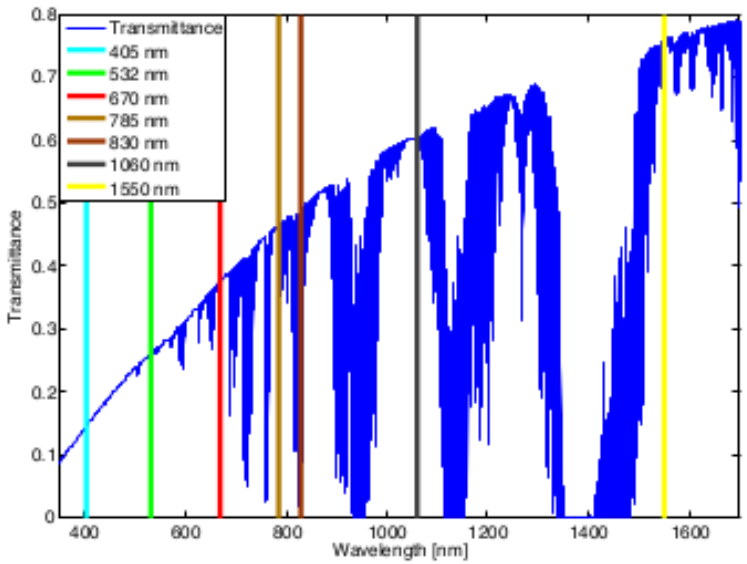
[Credits: F. Vedovato, UNIPD.]

What are the **key requirements** for *free-space QC*?

Satellite QKD - Requirements

1 Full-day functionality





[J.-P. Burgoin *et al.*, NJP 15, 023006 (2013)]

- **700-900 nm band**
  - efficient single photon detectors
  - strong background in daytime
- **1550 nm telecom band**
  - low background and good atmospheric transmittance
  - single photon detectors are either not efficient (InGaAs SPAD) or fiber-based (SNSPD)

Satellite QKD - Requirements

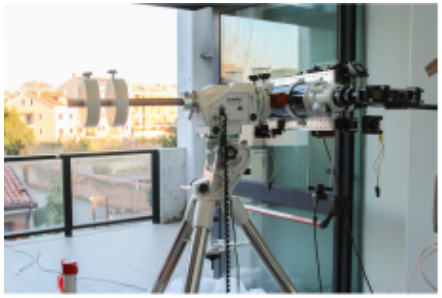
2. **Telecom-technology compatibility and integration**
   - Possibility of using the fast fiber-based components used in classical communication
   - Compatibility with *integrated silicon photonics* (SiPh), which allows to design **fast**, **compact**, **scalable** and **low-power-consuming** devices
3. **Stable free-space link**
   - *Free-space detection system*
     - low sensitivity to atmospheric turbulence
     - side-channel attacks [1]
       background noise (larger FOV)
       low efficiency single-photon detectors at 1550 nm
   - *Fiber-based detection system*
     - spatial filtering
       high efficiency single-photon detectors (SNSPD)
     - very sensitive to atmospheric turbulence

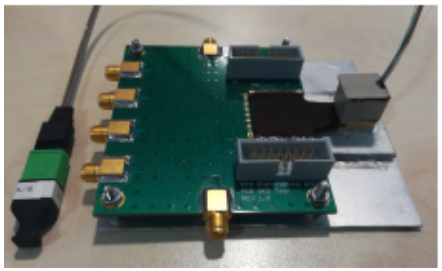
[1] P. Chaiwongkhot, PRA 99, 062315 (2019)

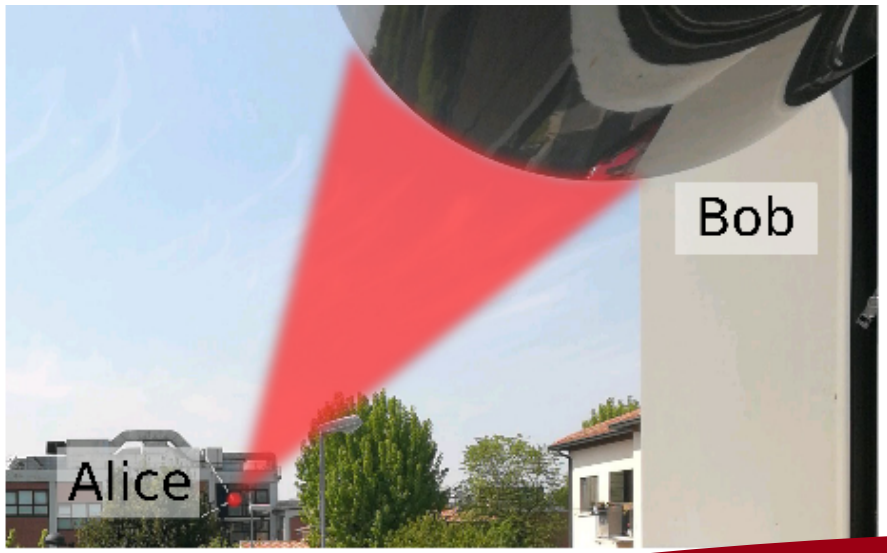
QCoSOne

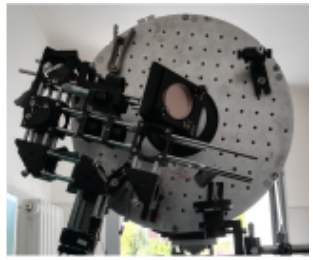
Full-daylight QKD system at 1550 nm developed with the support of the **Italian Space Agency (ASI)**

- Fiber-based **transmitter** with integrated state encoder performing *intensity and polarization modulation* on a *single photonic chip*
- Fiber-based **receiver** using *COTS telecom components* and *SNSPDs*
- **Free-space fiber-to-fiber quantum channel** with correction of turbulence induced low-order beam aberrations

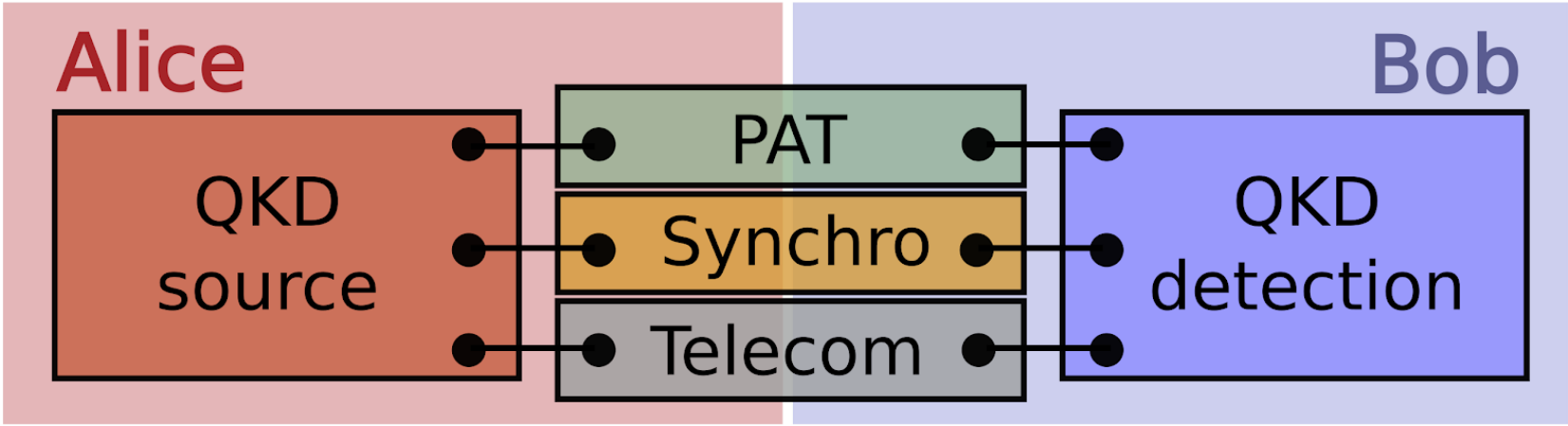








QCoSOne - Modular design



The subsystems are designed to be **as independent as possible**, with a *well-defined interface* between the subsystems.

In principle, it should be possible to *change* one subsystem *without modifying* the rest of the system.

QCoSOne - QKD protocol

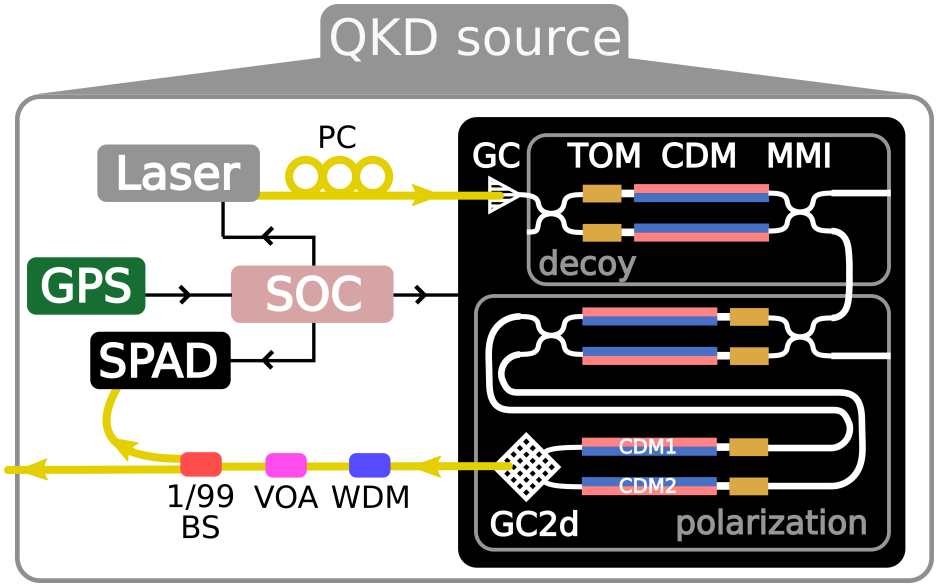
Efficient 3-state 1-decoy BB84 protocol [1]

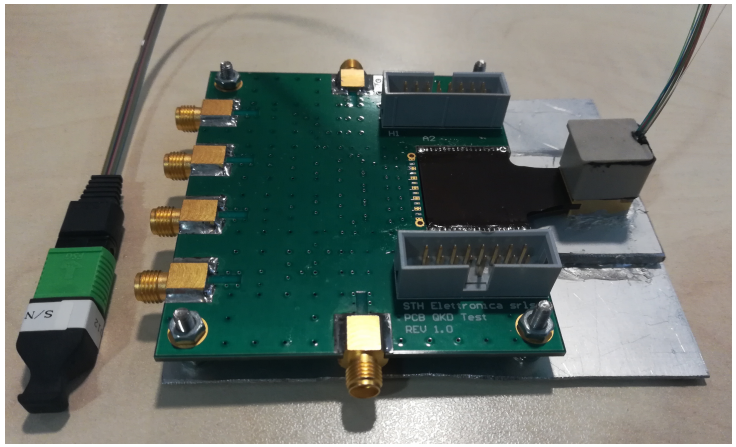
- **Alice - state preparation**
  1. **Basis (b_A) random choice**: $Z = \{|R\rangle, |L\rangle\}$ basis with p_A^Z, $X = \{|+\rangle, |-\rangle\}$ basis with $p_A^X = 1 - p_A^Z$.
  2. **State (s) random choice**: if $b = Z$, s is $|R\rangle$ or $|L\rangle$ with probability $1/2$; if $b = X$, $s = |+\rangle$.
  3. **Pulse intensity μ choice**: μ_1 with probability p_{μ_1} and μ_2 with $p_{\mu_2} = 1 - p_{\mu_1}$.

  In general, $\mu_1^X \neq \mu_1^Z$ and $\mu_2^X \neq \mu_2^Z$ [2].
- **Bob - measurement** on basis $b_B = Z$ with probability $p_B^Z = p_A^Z$ and on basis $b_B = X$ with $p_B^X = p_A^X$.
- **Sifting**
  - Alice reveals *for each pulse* the intensity μ and the encoding basis b_A.
  - Bob reveals the positions where $b_A \neq b_B$ and they both discard them.
- Separate **parameter estimation** on pulses with intensity μ_1 and μ_2.
- **Error correction** and **privacy amplification** to extract the *secure key*.

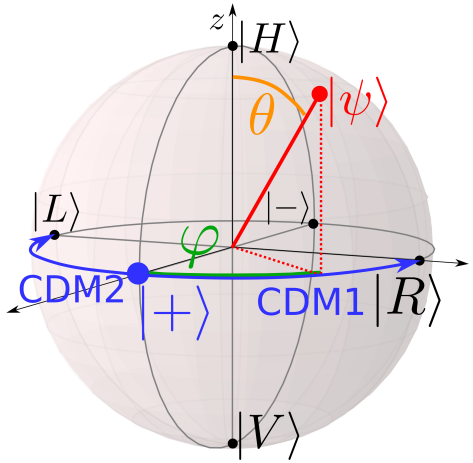
[1] Rusca *et al.*, Appl. Phys. Lett. 112, 171104 (2018)
[2] Yu *et al.*, PRA 93, 032307 (2016)

QCoSOne - QKD source

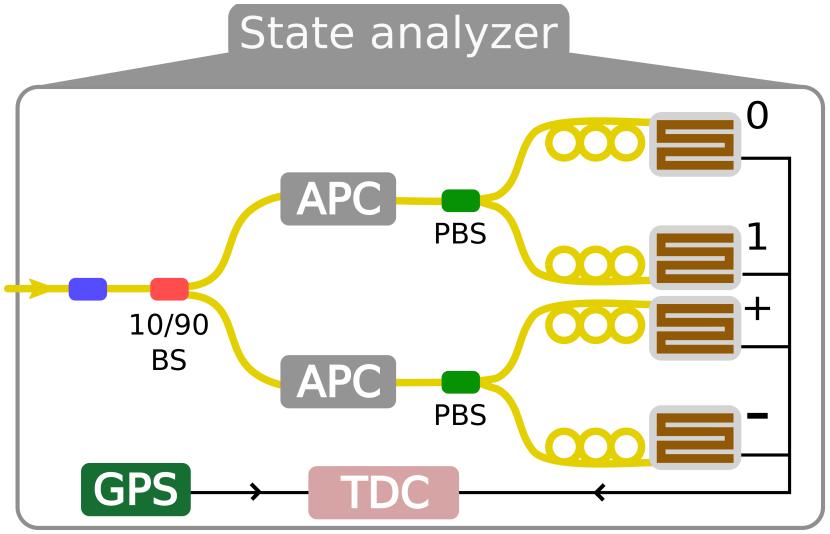


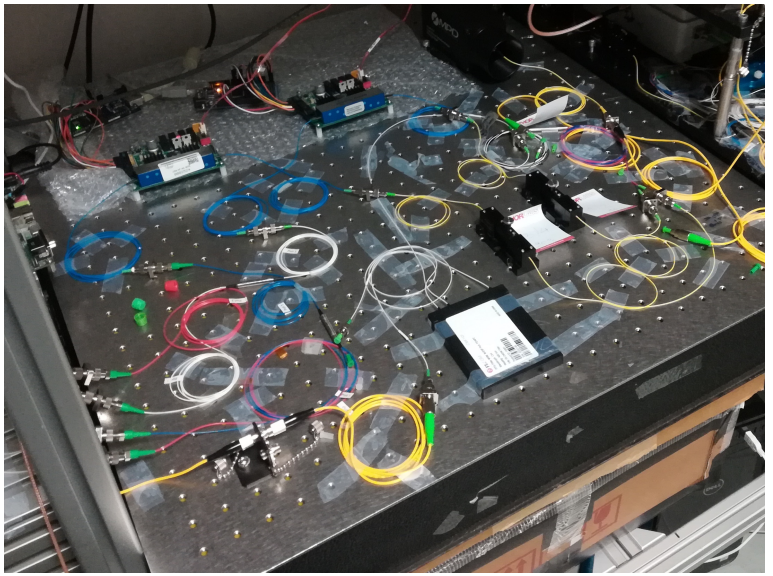


- Output interface: SMF
- *Pulsed DFB laser* at $\lambda = 1550\,\mathrm{nm}$ and repetition rate $50\,\mathrm{MHz}$
- PIC with **thermal** (DC) and **carrier-depletion modulators** (RF) on the Si-waveguide
- **InGaAs/InP gated SPAD** to monitor the intensity level μ



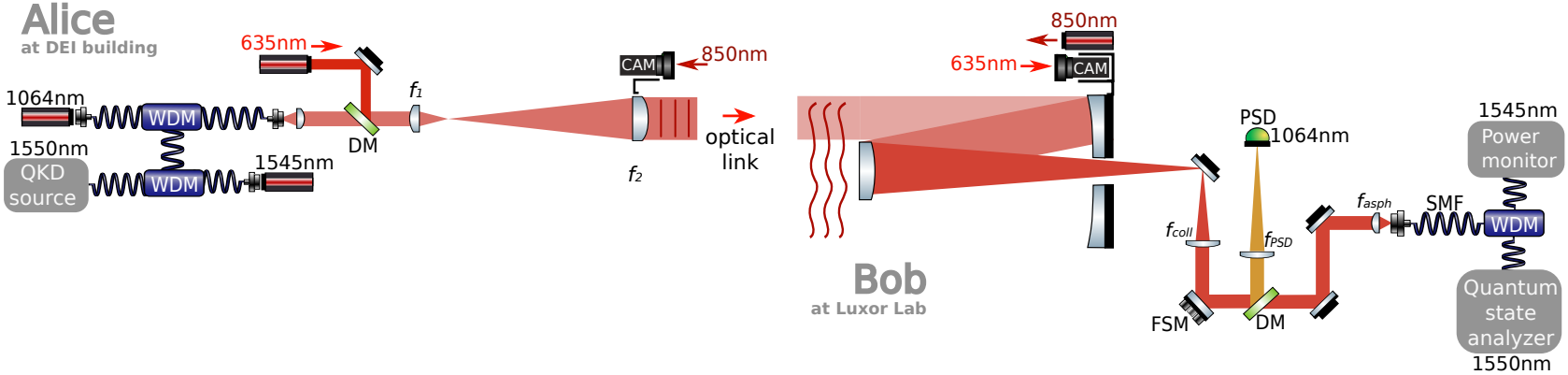
QCoSOne - QKD detection





- Input interface: **SMF** (40 m long)
- **State analyzer setup**: *COTS elements* (fiber BS, PBS, polarization controllers and DWDM) and *4 SNSPDs*
- *Measurement basis* set by two automatic polarization controllers (APCs) on the calibration phase
- Detection and GPS PPS recorded on a time-to-digital converted (TDC)

QCoSOne - PAT system



- Input & output interfaces: SMF
- Galileian **transmitter** of aperture 120 mm and Dall-Kirkham **receiver** of aperture 315 mm
- Correction of **angle-of-arrival fluctuations** using the feedback signal provided by a 1064 nm beacon laser acquired by a *position-sensitive-detector* (PSD)
- **1545 nm beacon** to monitor coupling efficiency in real time

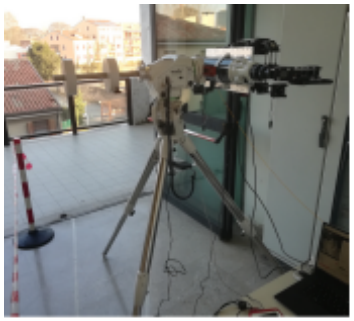
QCoSOne - Other subsystems

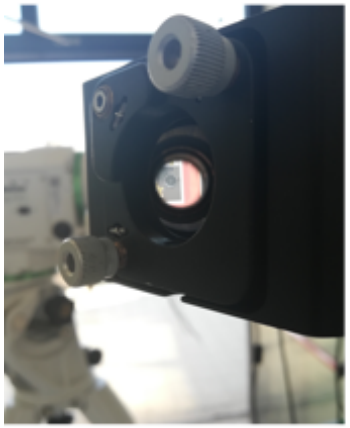
- **Synchronization**
  - Rough synchronization (better than $300\,\mathrm{ns}$) through *GPS*
  - Fine synchronization by measuring the *difference between the expected and measured time of arrivals* of photons at Bob's side (**Qubit4Sync**) [1]
- **Telecom**
  - **Classical communication**, **post-processing** and **key extraction** using a modified version of the *AIT QKD R10 software* [2]
- **Randomness** to the *QKD source* is provided by a source-device-independent QRNG [3]

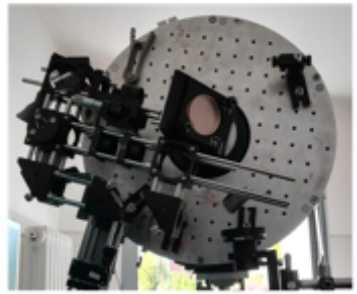
[1] L. Calderaro *et al.*, arXiv:1909.12050v1 (2019)
[2] https://sqt.ait.ac.at/software/projects/qkd
[3] M. Avesani *et al.*, Nat. Commun. 9, 5365 (2018)

QCoSOne field test

145-m urban link in Padova

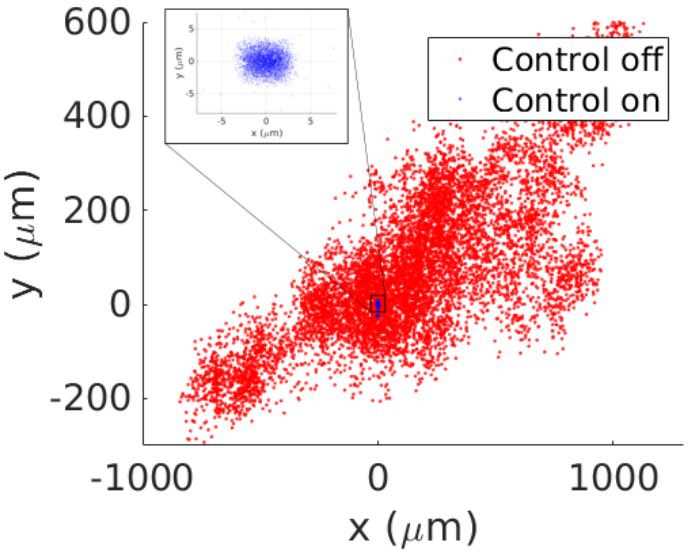


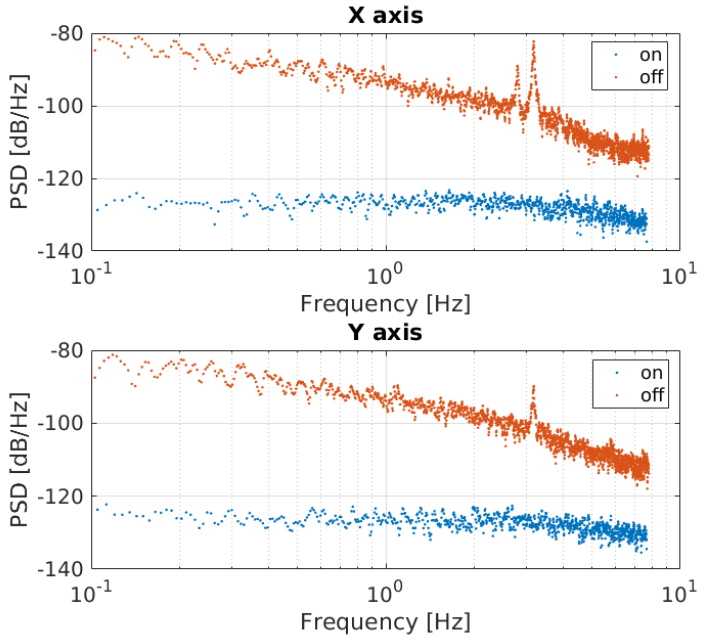


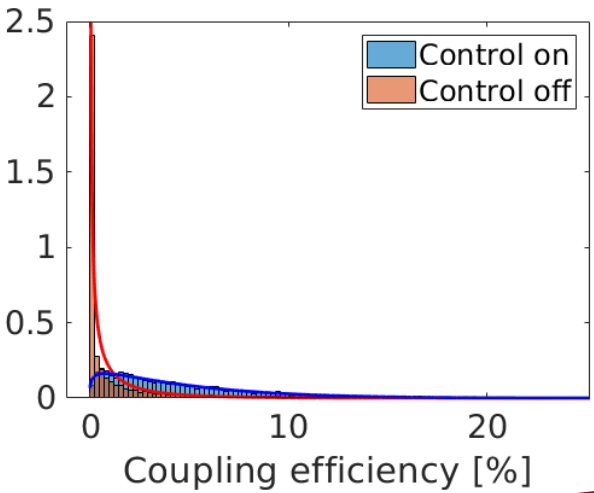


Results: PAT subsystem - worst case perfromance

April 18, 2019 - h 9:15



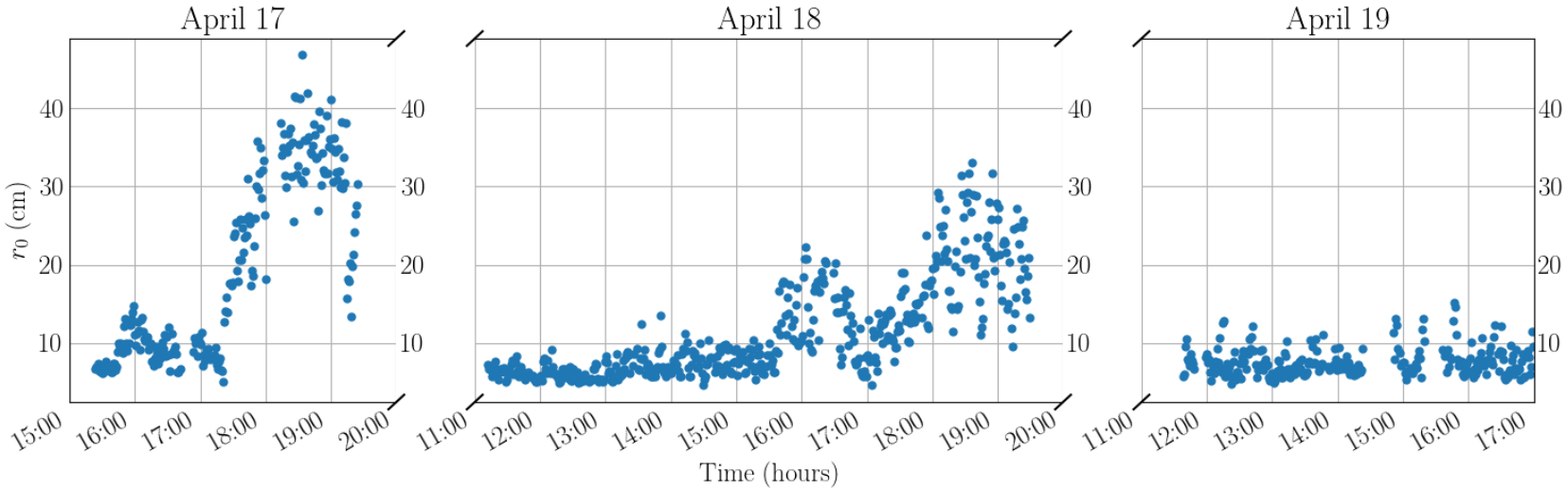




	σ_x	σ_y	μ_η	σ_η
ON	1.4 μm	1.7 μm	4.8 %	4.2 %
OFF	426 μm	177 μm	1.3 %	2.7 %

$$r_0 = 4.7\,\mathrm{cm}$$
$$D/r_0 = 2.6$$

Results: the quantum channel




11:30


12:00


13:00

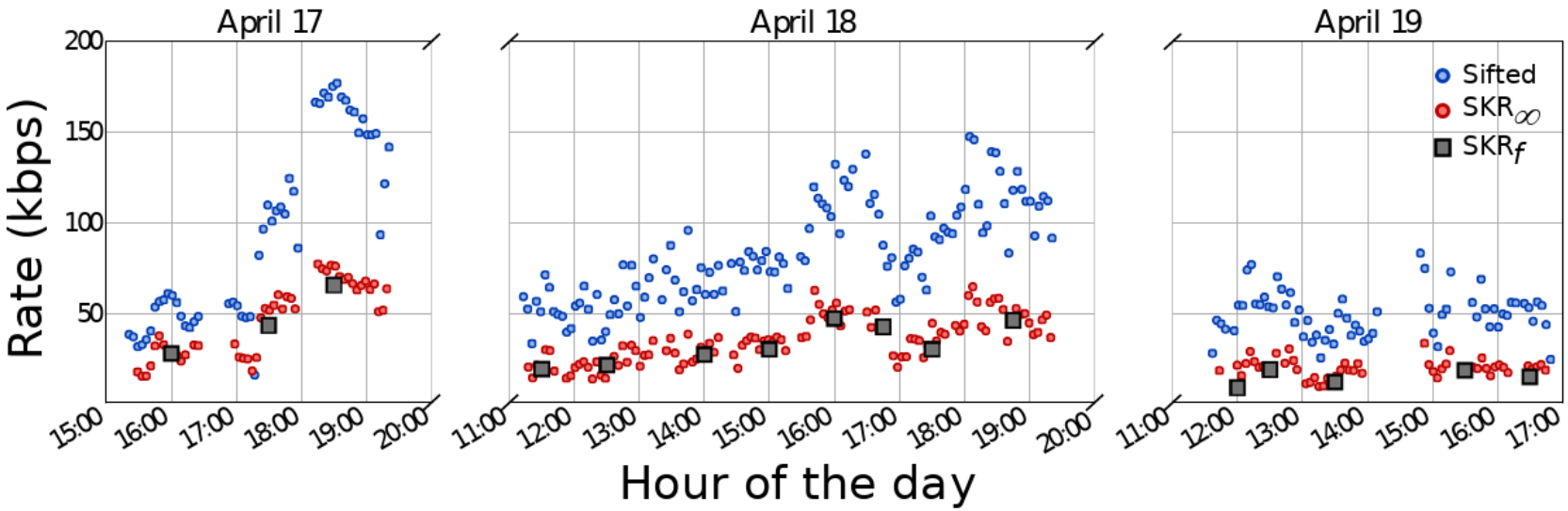

14:30

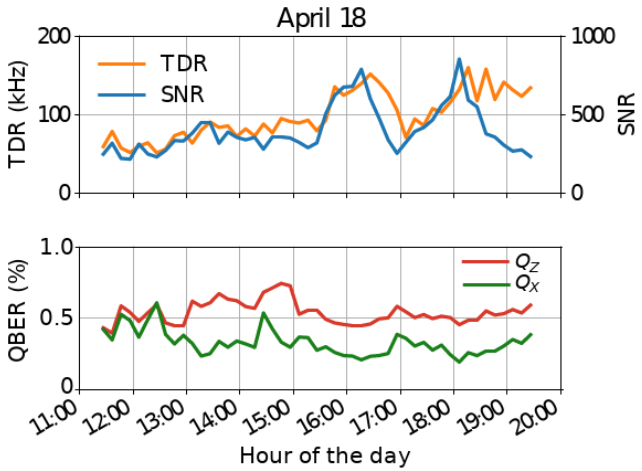

16:30


19:30

- Sunny spring days.
- *Weak turbulence*: D/r_0 from 0.25 (*late afternoon*) to 2.6 (during the *day*)
- **Sunset** at **20:00**.

Results: QKD





- **Total attenuation $\sim$ 22 dB** (SMF coupling $\sim$ 12 dB, optics and fibers $\sim$ 10 dB)
- **Extremely low QBER $\sim$ 0.5 %** in both bases, with no active polarization stabilization
- **Finite-key rate SKR$_f$** up to $\sim$ 70 kbps

Conclusions . . .

- Successful realization of **daylight QKD at 1550 nm**
  - *strong background rejection* by exploiting different filters:
    - **temporal** (synchronization)
    - **spatial mode** (fiber-based detector)
    - **spectral mode** (IF and DWDM)
  - **integrated chip encoder**
    - intensity and polarisation modulators **on the same chip**
    - compact and portable transmitter suitable as optical payload for **satellite QKD**
  - compatible with **current telecom technology and infrastructure**

. . . and future perspectives

- **Possible improvements**
  - Increase **system clock rate** (GHz is the current state of the art)
  - Improve **SMF coupling efficiency** by using **adaptive optics**
- **Further tests**
  - different link configurations and **longer distances** (preliminary tests of the PAT system over 10 *km* in Matera)
- Use the optical link to test **different quantum devices**
  - **POOGNAC**, a fiber-based DV-QKD source characterized by *great intrinsic stability* [1]
  - **CV-QKD** on a real atmospheric channel
  - . . .

[1] C. Agnesi *et al.*, Opt. Lett. 44, 2398 (2019)

The authors

[M. Avesani *et al.*, arXiv:1907.10039 (2019)]

- **QuantumFuture research group (DEI-UniPD)**
  M. Avesani, L. Calderaro, MS*, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, F. Vedovato, G. Vallone, P. Villoresi
  * *Current affiliation:* LIP6 - Sorbonne University
- **InPhoTec - Integrated Photonics Technologies Foundation (Pisa)**
  M. Chiesa, A. Nottola, D. Rotta
- **PNTLab - Consorzio Nazionale Interuniversitario per le Telecomunicazioni (Pisa)**
  M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello
- **Instituto TeCIP - Scuola Superiore Sant'Anna (Pisa)**
  G. Contestabile
- **Matera Laser Ranging Observatory, Italian Space Agency (Matera)**
  D. Dequal, G. Bianco
- **Telecommunication and Navigation Division, Italian Space Agency (Rome)**
  C. Facchinetti, A. Tuozzi

Thank you for the attention!