High-speed QKD:
removing the roadblocks for integration and utilisation in real-world networks

Qcrypt, University of Maryland, 2023

Rebecka Sax

Quantum Technologies Group of Hugo Zbinden

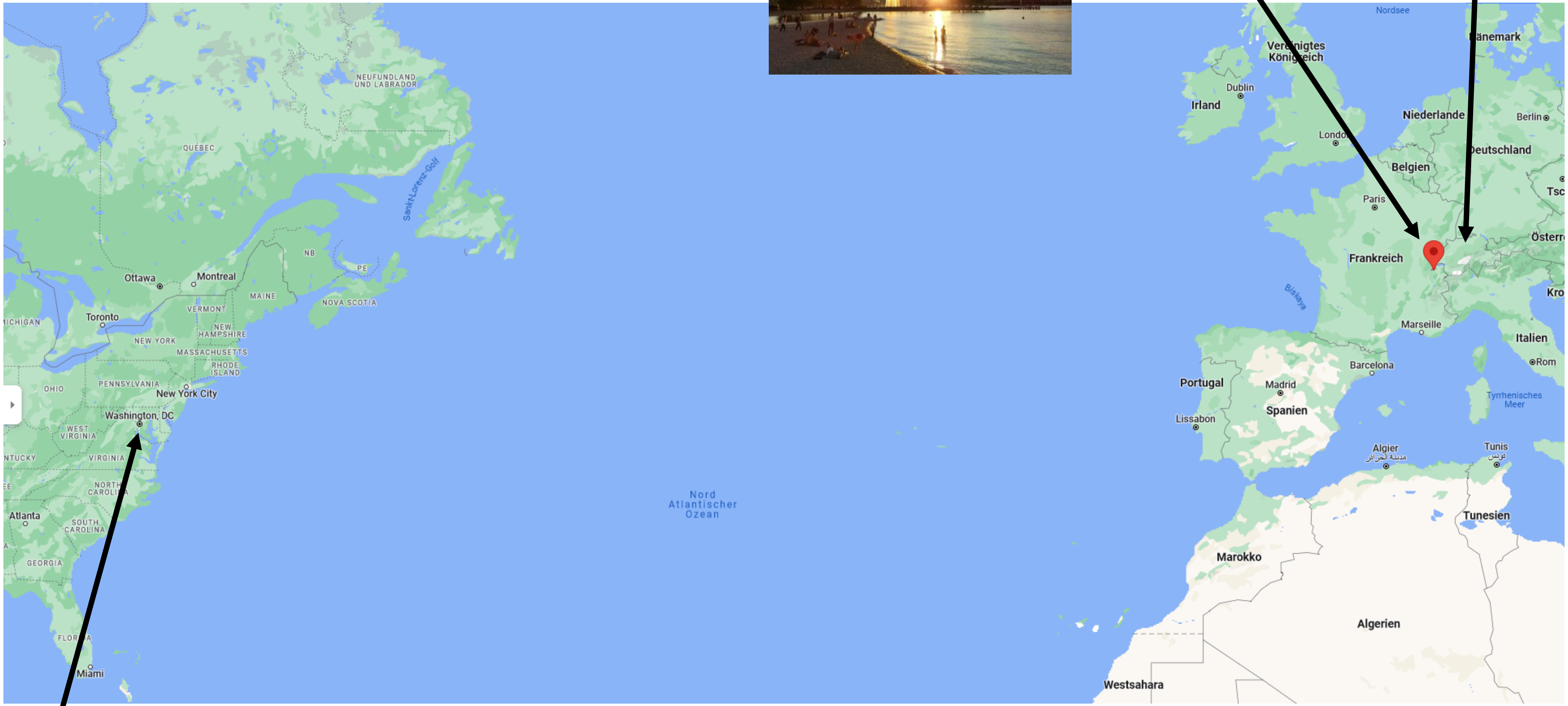
@ University of Geneva, Switzerland

UNIVERSITÉ DE GENÈVE

FACULTÉ DES SCIENCES

Geneva

Switzerland



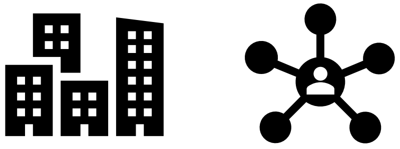
Google Maps

Qcrypt

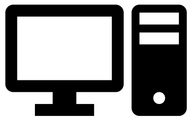
Deployment of QKD in real-world networks

Identifying the roadblocks

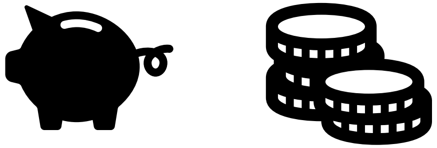
- Smooth fusion with existing fibre-optic networks
  - Combining quantum and classical channels in one fibre



- High-speed systems for high secret key rate production



- Low cost, mass-produced, scalable, practical
  - Integrated photonic circuits



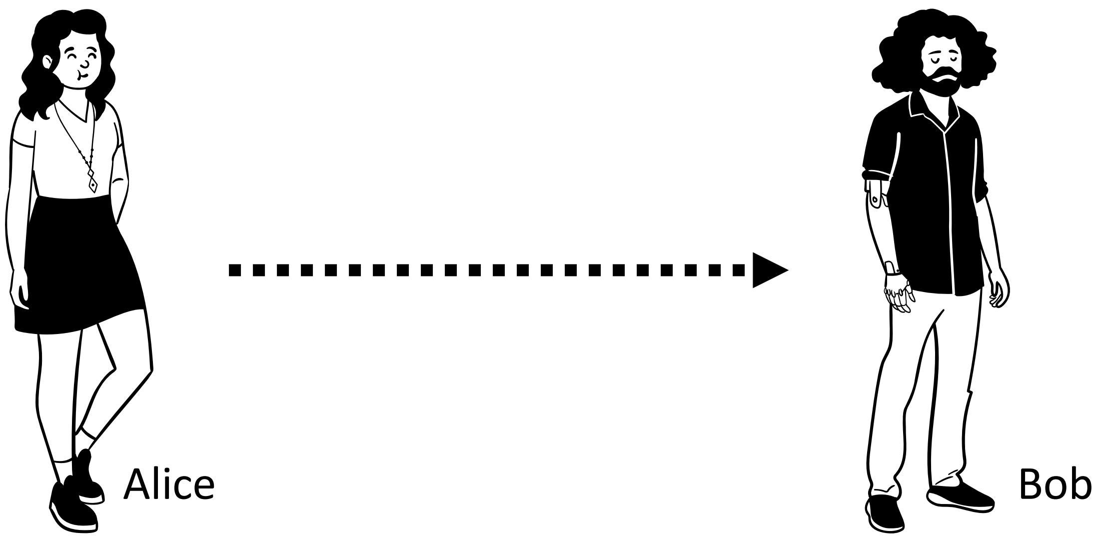
Outline

I. QKD protocol: 3-state time-bin BB84 with 1 decoy state

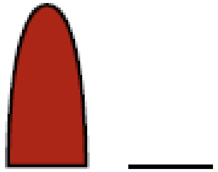
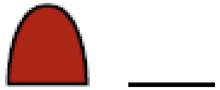
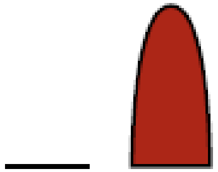
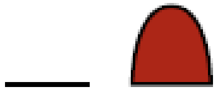
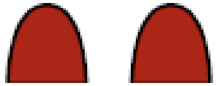
II. QKD in network environment

III. QKD with high secret key rates

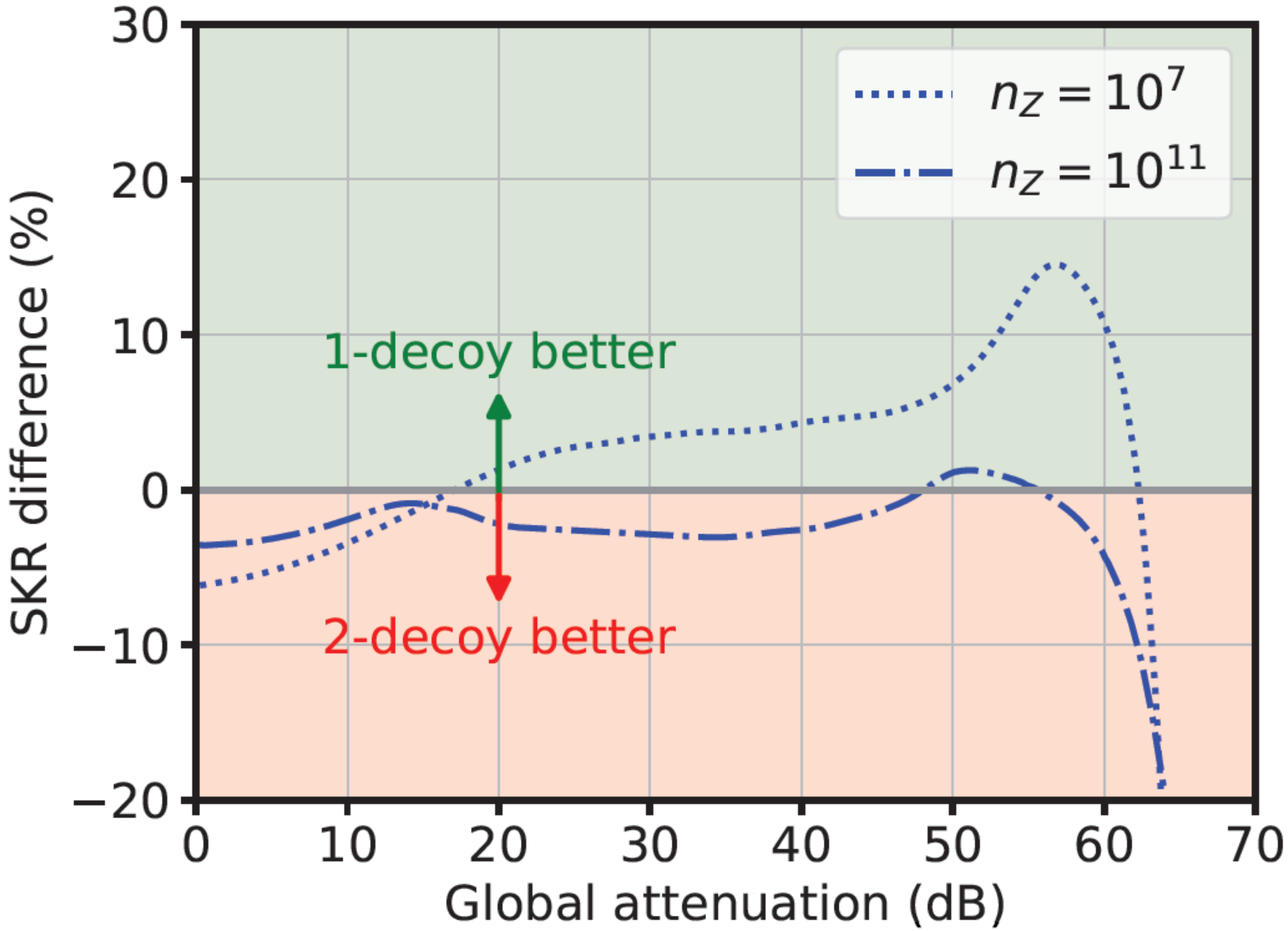
IV. High-speed integrated QKD



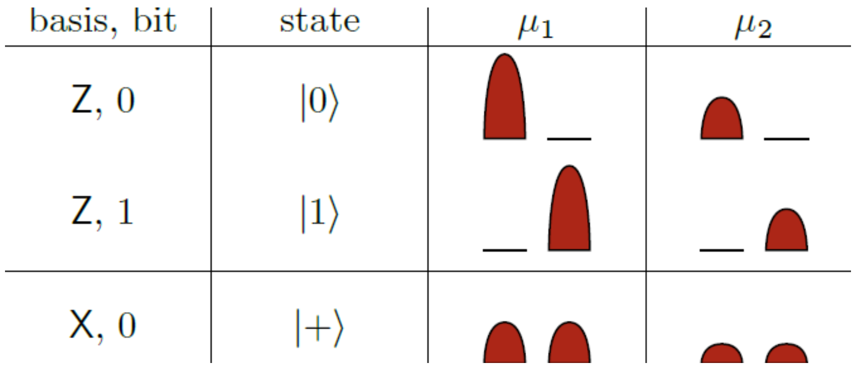
I. 3-state time-bin BB84 with 1 decoy state

basis, bit	state	μ_1	μ_2
Z, 0	$\|0\rangle$		
Z, 1	$\|1\rangle$		
X, 0	$\|+\rangle$		

I. 3-state time-bin BB84 with 1 decoy state

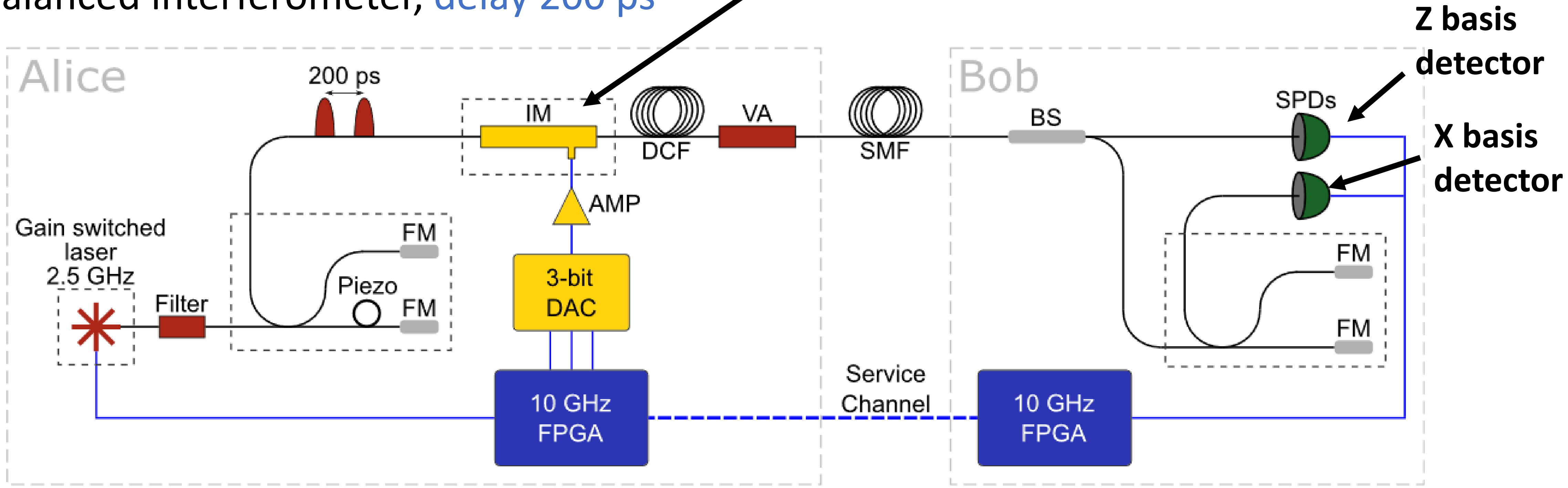


Rusca, D. et al. 'Finite-key analysis for the 1-decoy state QKD protocol', Appl. Phys. Lett. 23 (2018)



Experimental setup

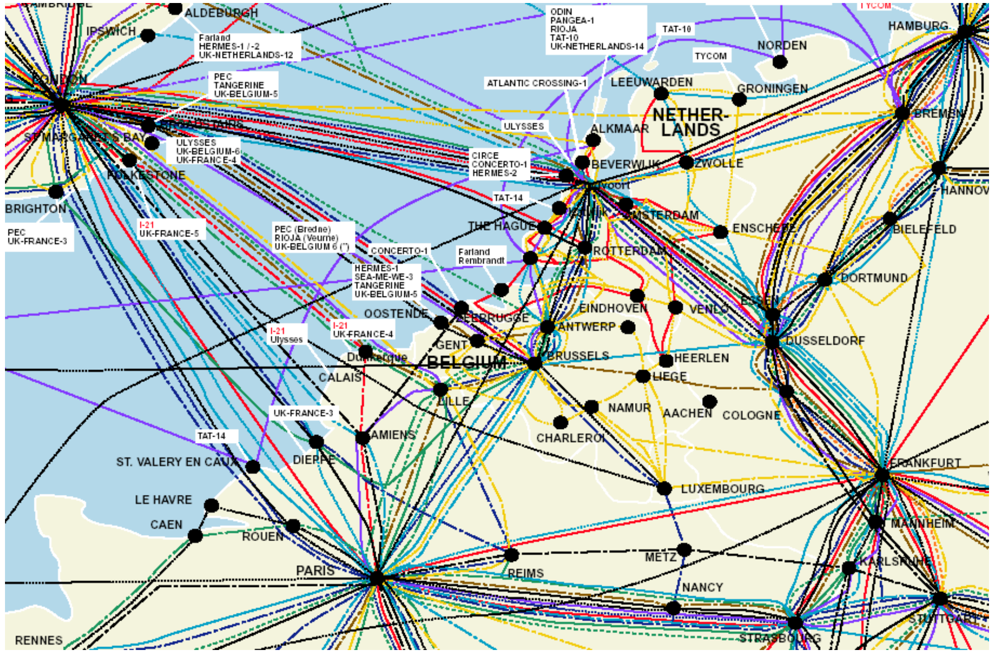
- Gain-switched phase-randomised pulses at 2.5 GHz and 1550 nm are generated
- Unbalanced interferometer, delay 200 ps



Boaron, A. et al. 'Simple 2.5 GHz time-bin quantum key distribution', Appl. Phys. Lett. 23, (2018)

II. QKD in network environment

Motivations



J. Rutherford, *‘The Territoriality of Pan-European Telecommunications Backbone Networks’*

- Wide-spread fibre-optics communications network

- Expensive to rent/maintain/place a dark fibre

- Merge quantum communication channels with existing classical communication channels

Network integration of QKD system

- Combining quantum and classical channels:

  Wavelength division multiplexing (WDM)

- Propagation loss in
  C-band: ~ 0.2 dB/km
  O-band: ~ 0.3 dB/km

- Classical channels most often in C-band (1550 nm)

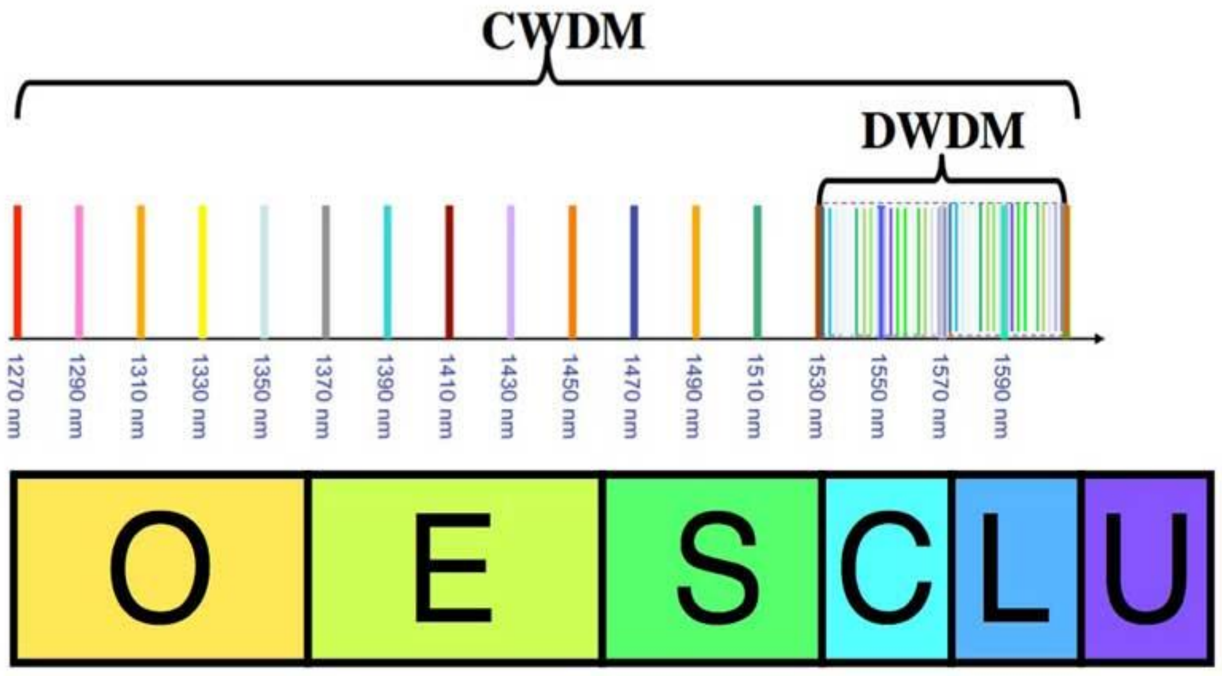


Image: The Fibre Optic Association

Network integration of QKD system

- Combining quantum and classical channels:
  Wavelength division multiplexing (WDM)

- Propagation loss in
  C-band: ~ 0.2 dB/km
  O-band: ~ 0.3 dB/km

- Classical channels most often in C-band (1550 nm)

Channel	Classical	Quantum
Average Power	>1 mW	1 nW

Obstacles in presence of classical channel

- Imperfect isolation
  - Proper filtering using coarse-WDM

- Scattering: Brioullin
  - Separation b/w channels of two DWDM channels

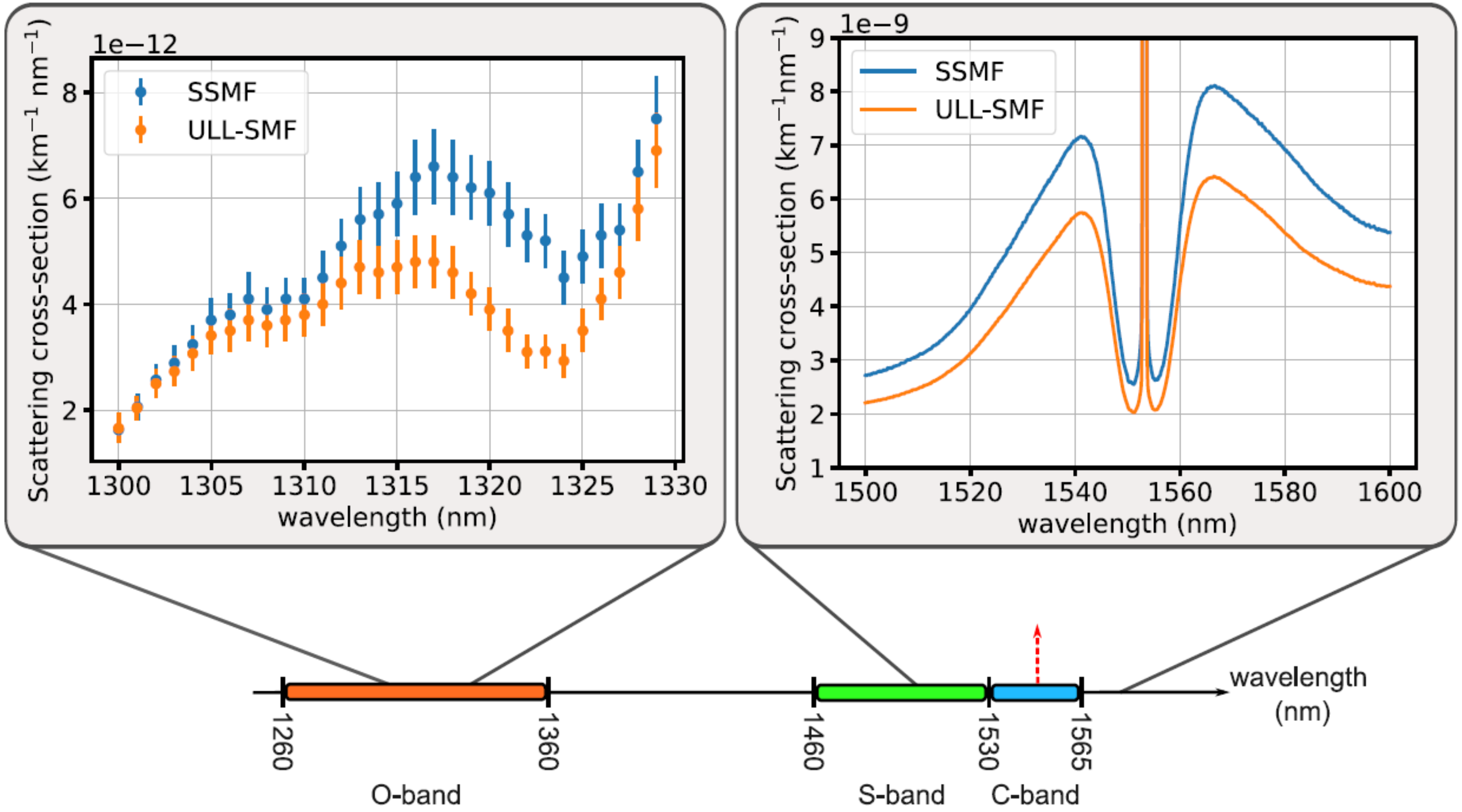
- Scattering: Raman
  - Main contribution to noise!

Raman scattering

3 orders of magnitude higher Raman scattering in C-band than O-band

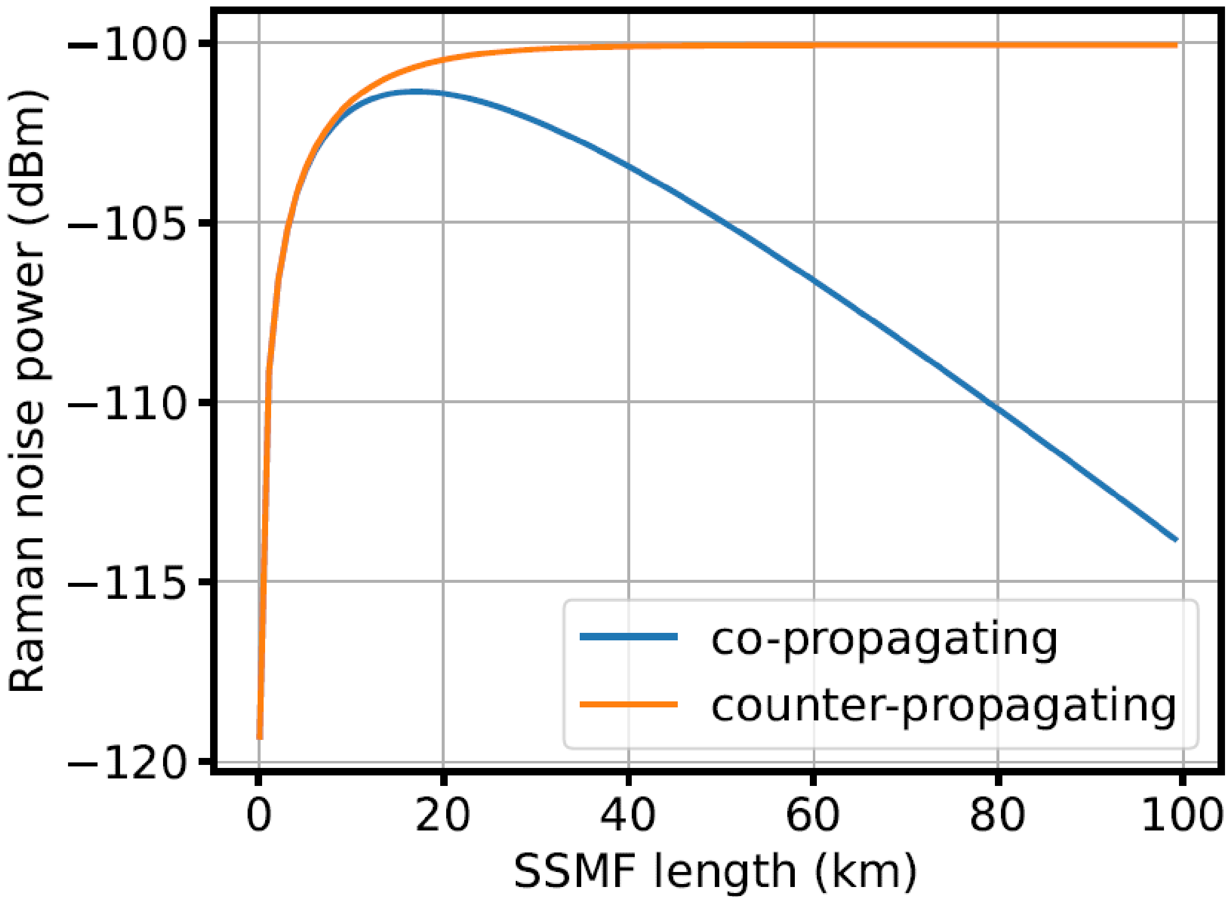
QC in O-band

QC in C-band



PhD Thesis, Fadri Grünenfelder, 'Performance, Security and Network Integration of Simplified BB84 Quantum Key Distribution'

Co- and counter-propagation



Raman scattering is isotropic!

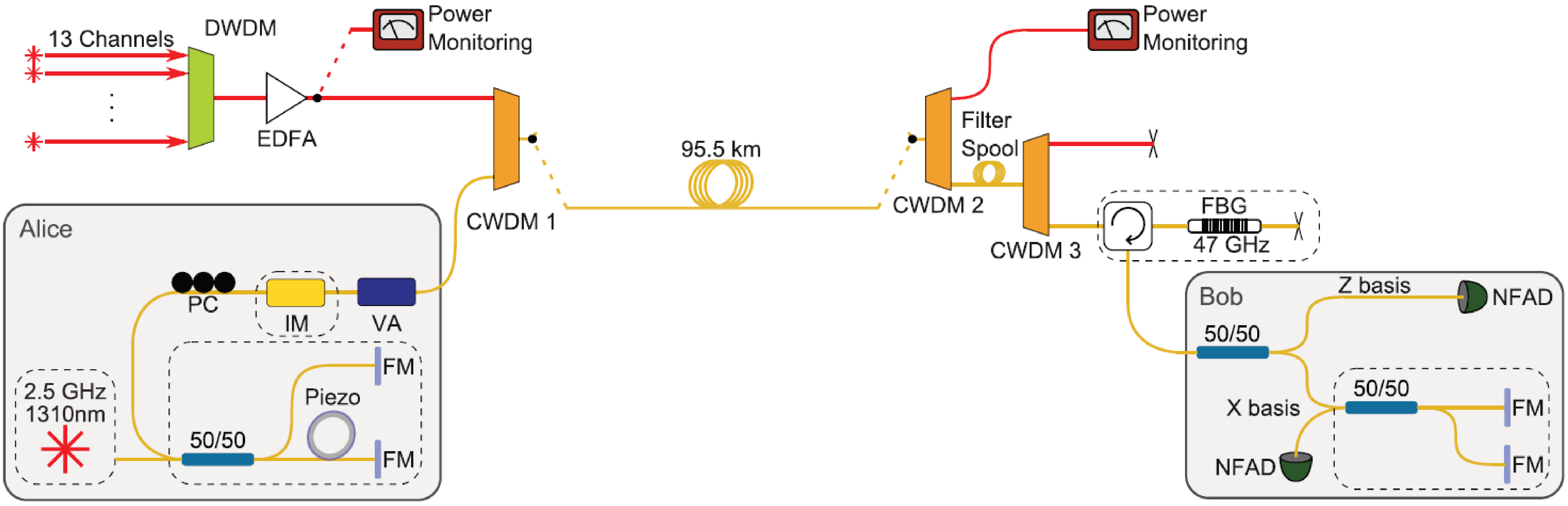
Fixed classical power

PhD Thesis, Fadri Grünenfelder, 'Performance, Security and Network Integration of Simplified BB84 Quantum Key Distribution'

WDM time-bin QKD

- Classical channel in C-band (1550 nm)
- Quantum channel in O-band (1310 nm)
- Co-propagating scheme

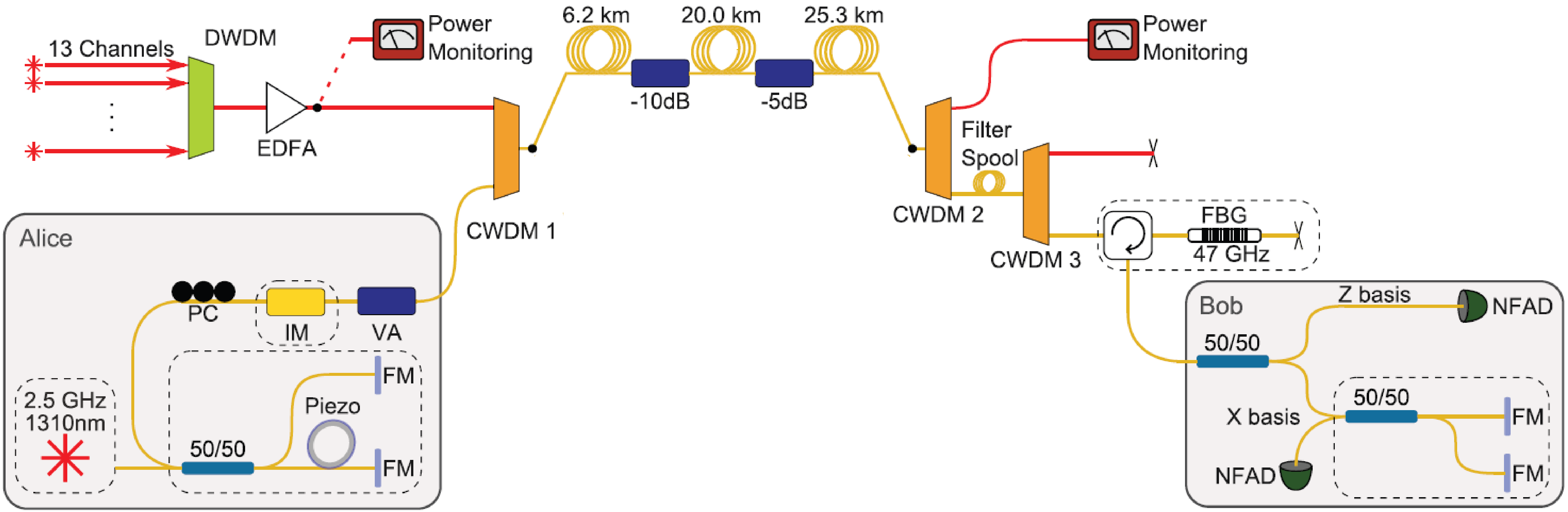
Experimental setup: WDM time-bin QKD
Long-distance link



Grünenfelder, F. *et al. 'The limits of multiplexing quantum and classical channels: Case study of a 2.5 GHz discrete variable quantum key distribution system' Appl. Phys. Lett.* 20 (2021)

Experimental setup: WDM time-bin QKD

Realistic link



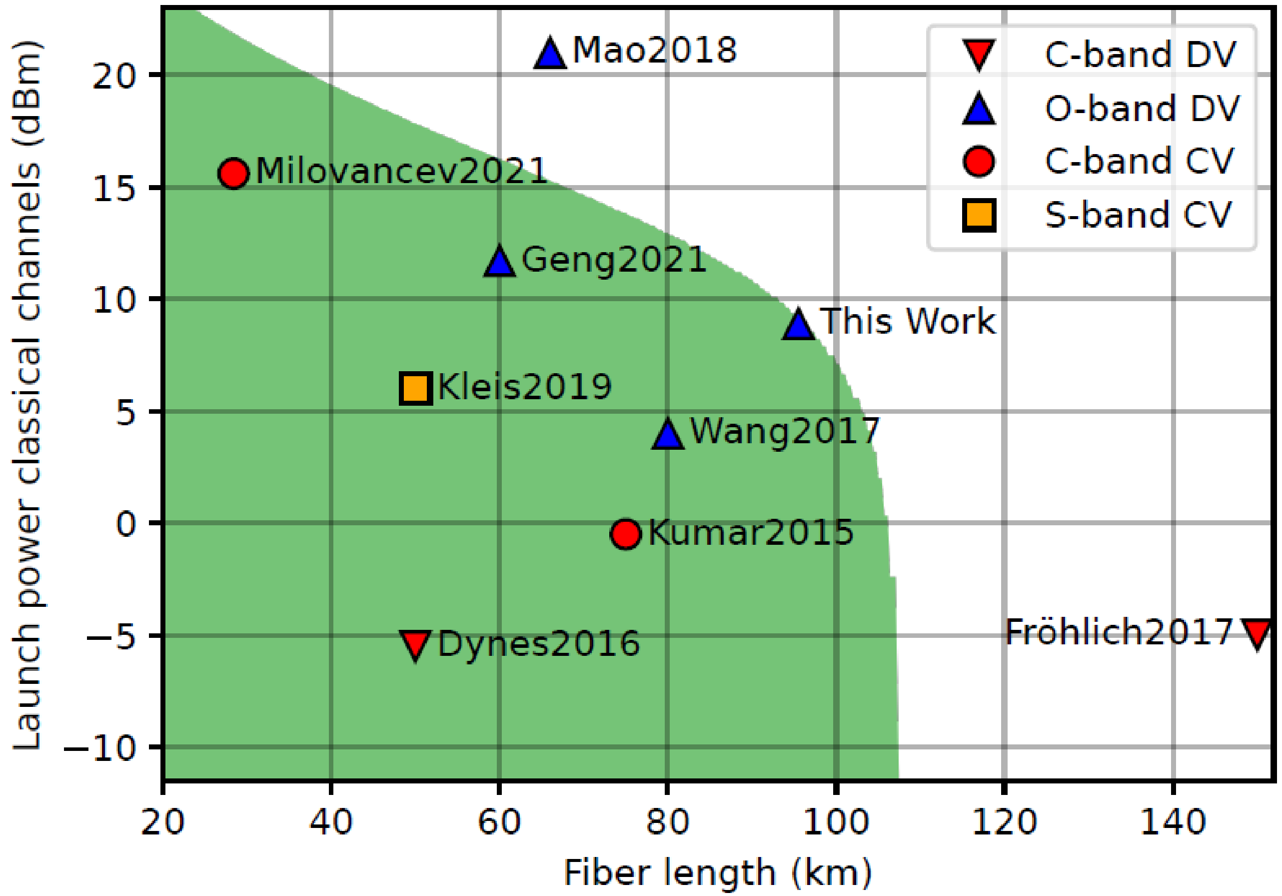
Grünenfelder, F. et al. 'The limits of multiplexing quantum and classical channels: Case study of a 2.5 GHz discrete variable quantum key distribution system' Appl. Phys. Lett. 20 (2021)

Results

Distance (km)	Extra loss (dB)	Classical power sent (dBm)	Classical power received (dBm)	Secret key rate (bps)
95.5	0	8.9	-12.1	42
51.5	15.0	16.7	-11.8	172

Grünenfelder, F. *et al. 'The limits of multiplexing quantum and classical channels: Case study of a 2.5 GHz discrete variable quantum key distribution system' Appl. Phys. Lett.* 20 (2021)

Comparisons



- DV systems with quantum channel in the O-band best for medium distance and high classical power

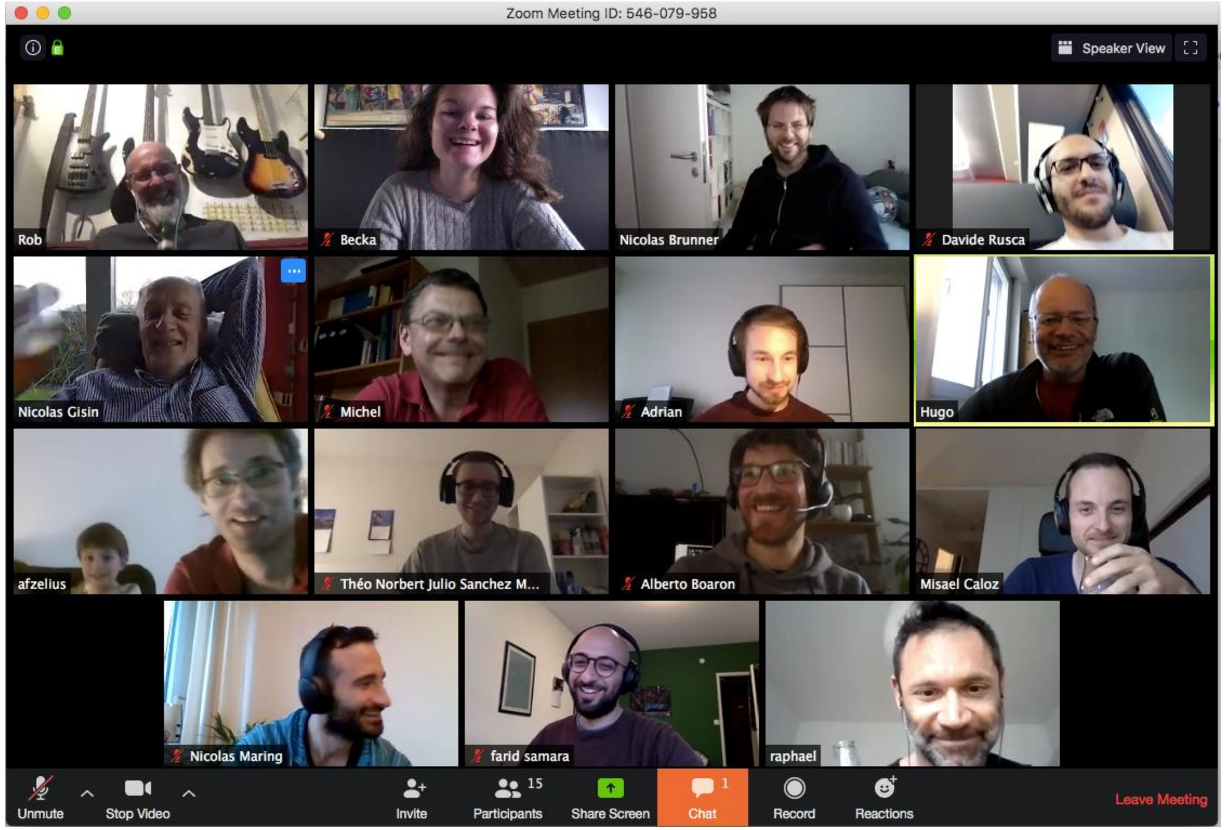
III. High secret key rate QKD

In collab. with:

IDQ

HSLU Hochschule Luzern

Motivations



- Encrypted video-conf.*: 6 Mbps
- How high SKRs can our system acheive?

*: US Federal Communications Commission

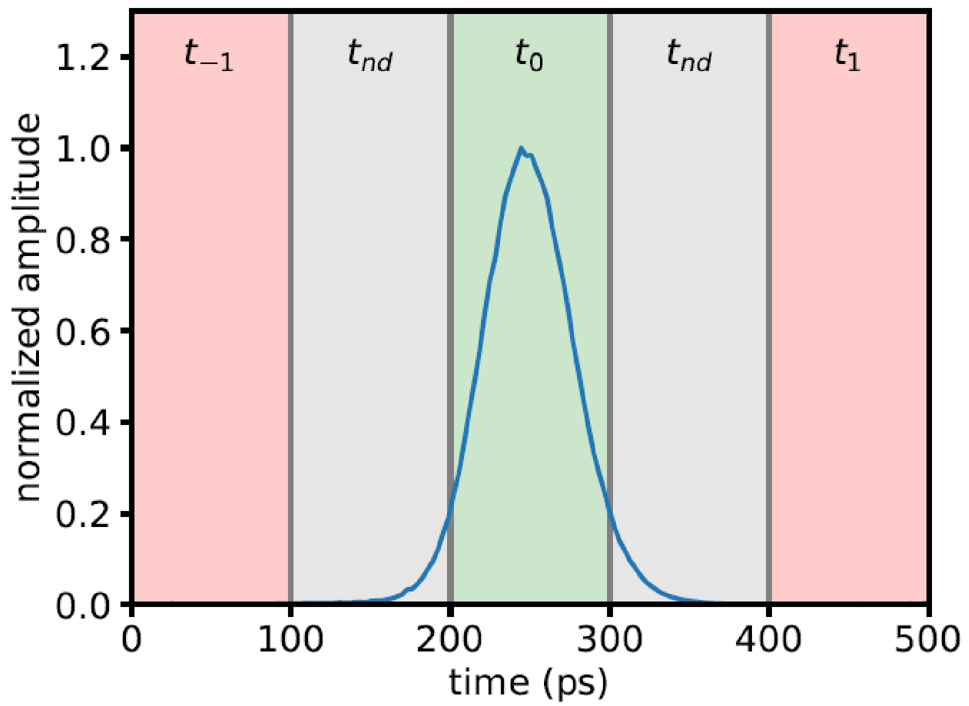
High secret key rate QKD

- Necessary conditions to perform a high-rate secret key exchange:

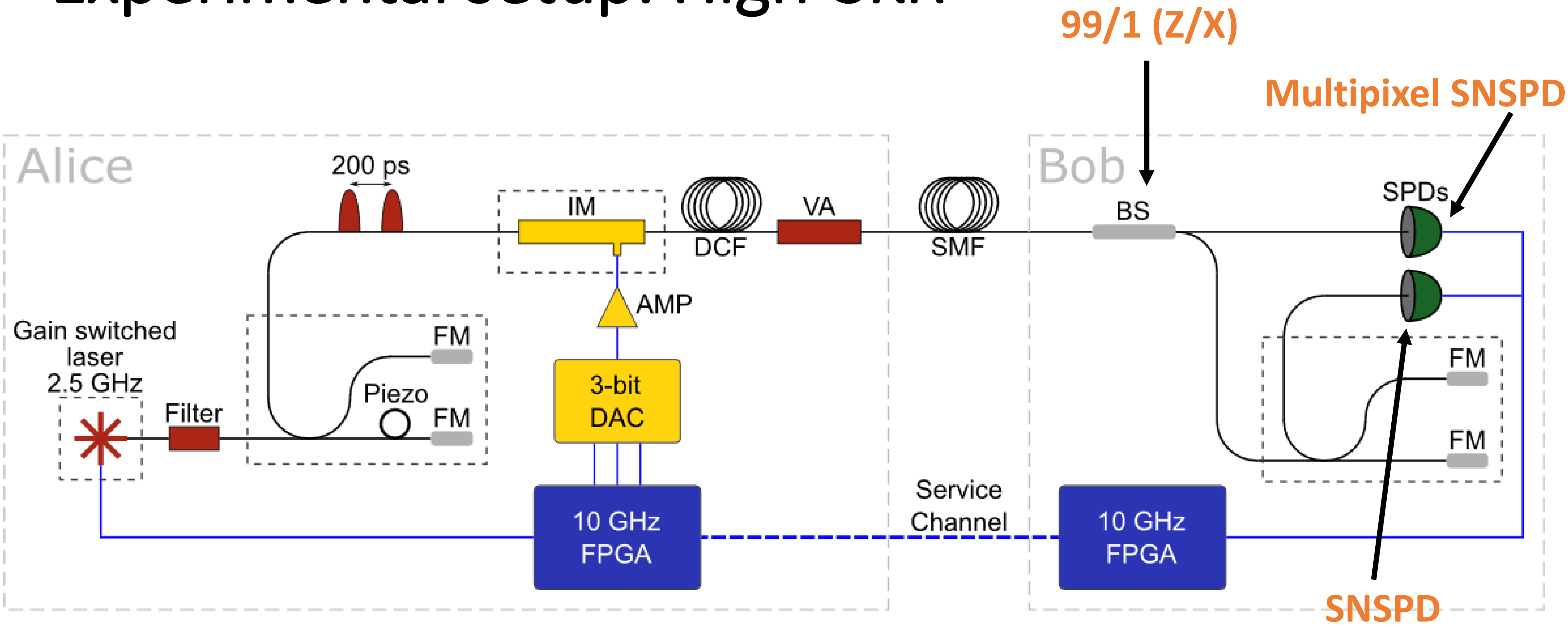
  1. Detector with low timing jitter and high efficiency at ultra-high count rates

  2. High-rate sifting and readout electronics

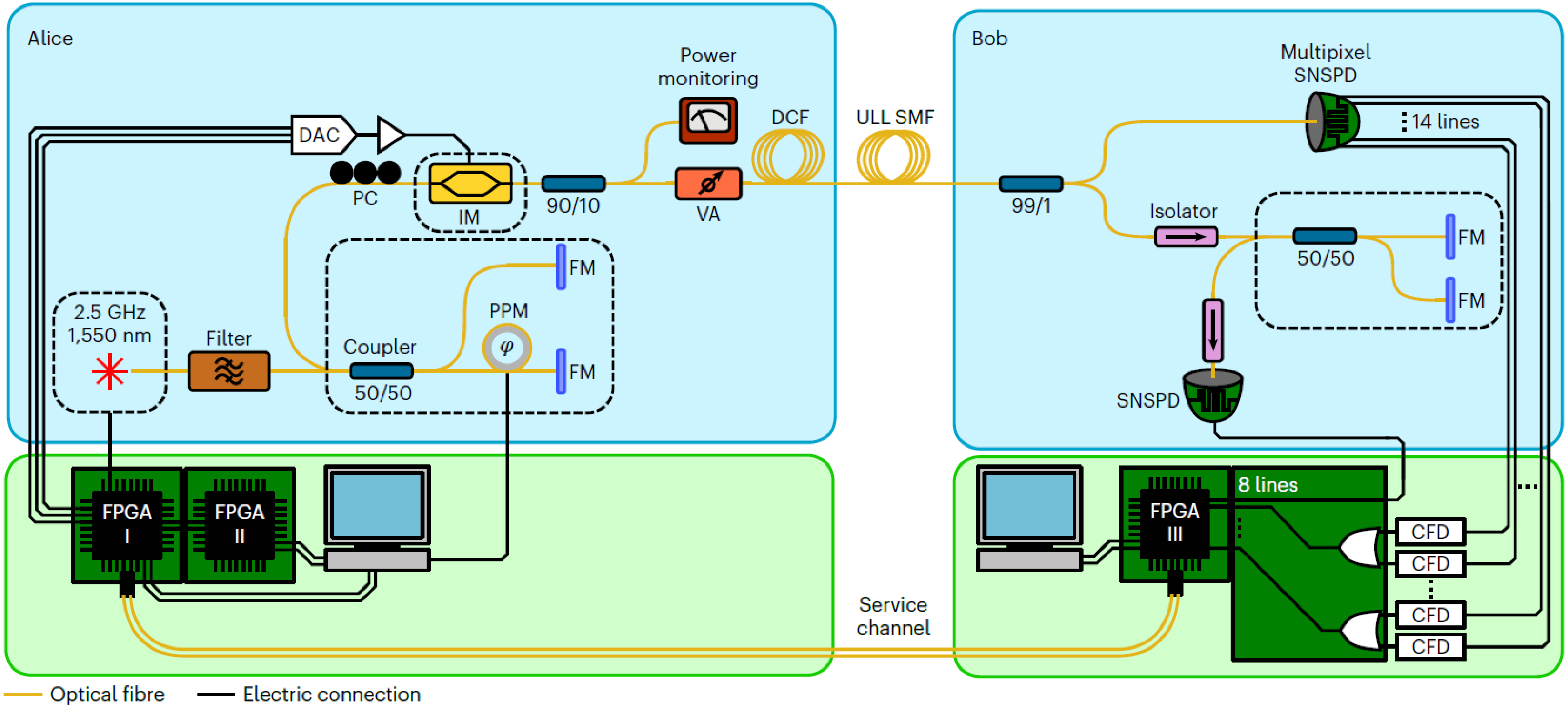
  3. Fast post-processing as well as the real-time privacy amplification



Experimental setup: High-SKR



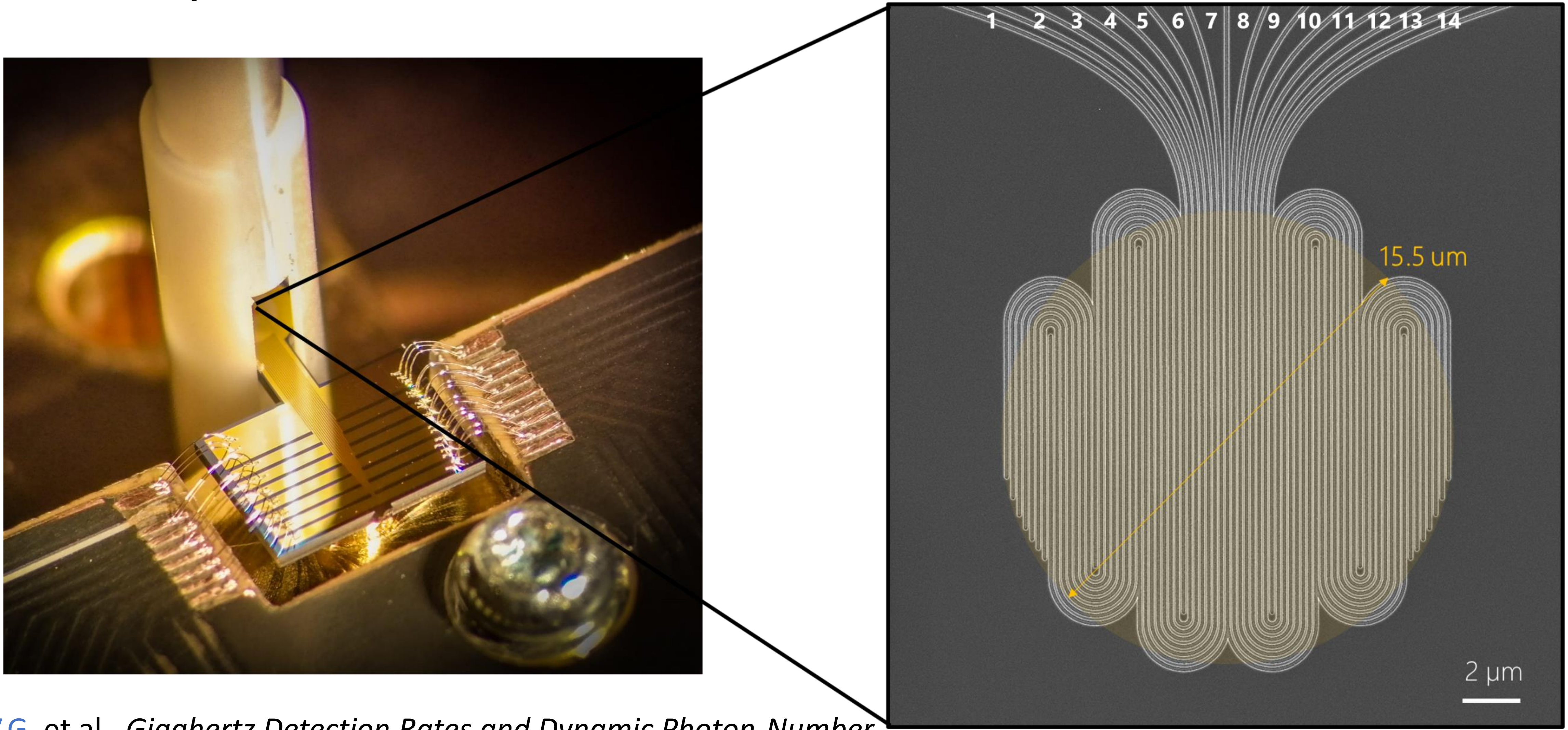
Experimental setup: High-SKR



Grünenfelder, F. et al. 'Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems', Nat. Photon. 17, 422–426 (2023)

Talk: Giovanni Resta, Friday!

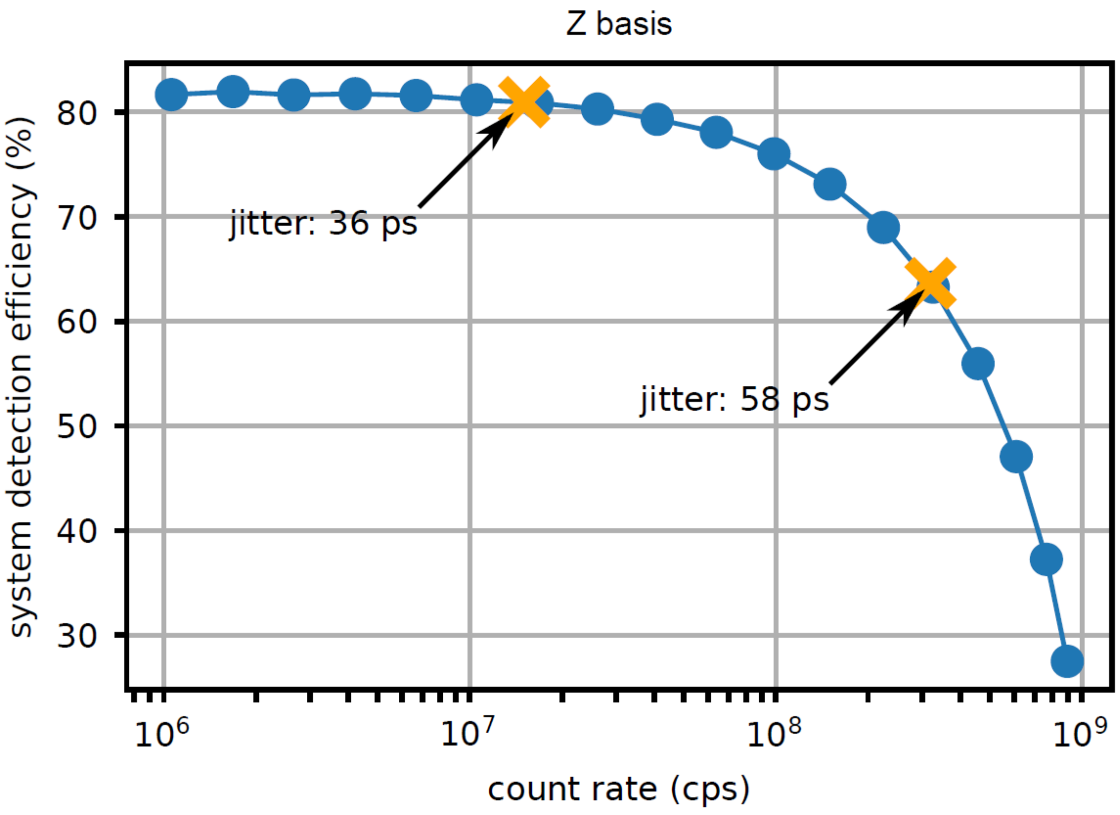
Multipixel SNSPD

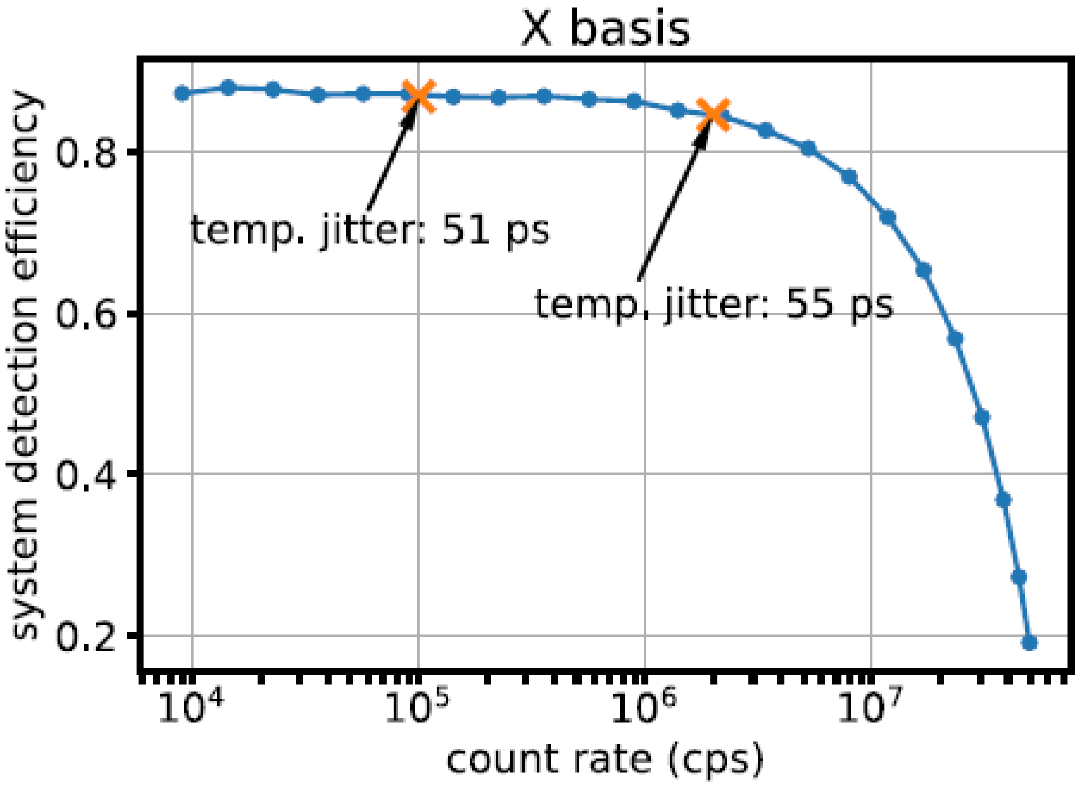


Resta, V.G. et al., *Gigahertz Detection Rates and Dynamic Photon-Number Resolution with Superconducting Nanowire Arrays, Nano Lett.* 2023

NB. Scale of x-axes!

Detectors

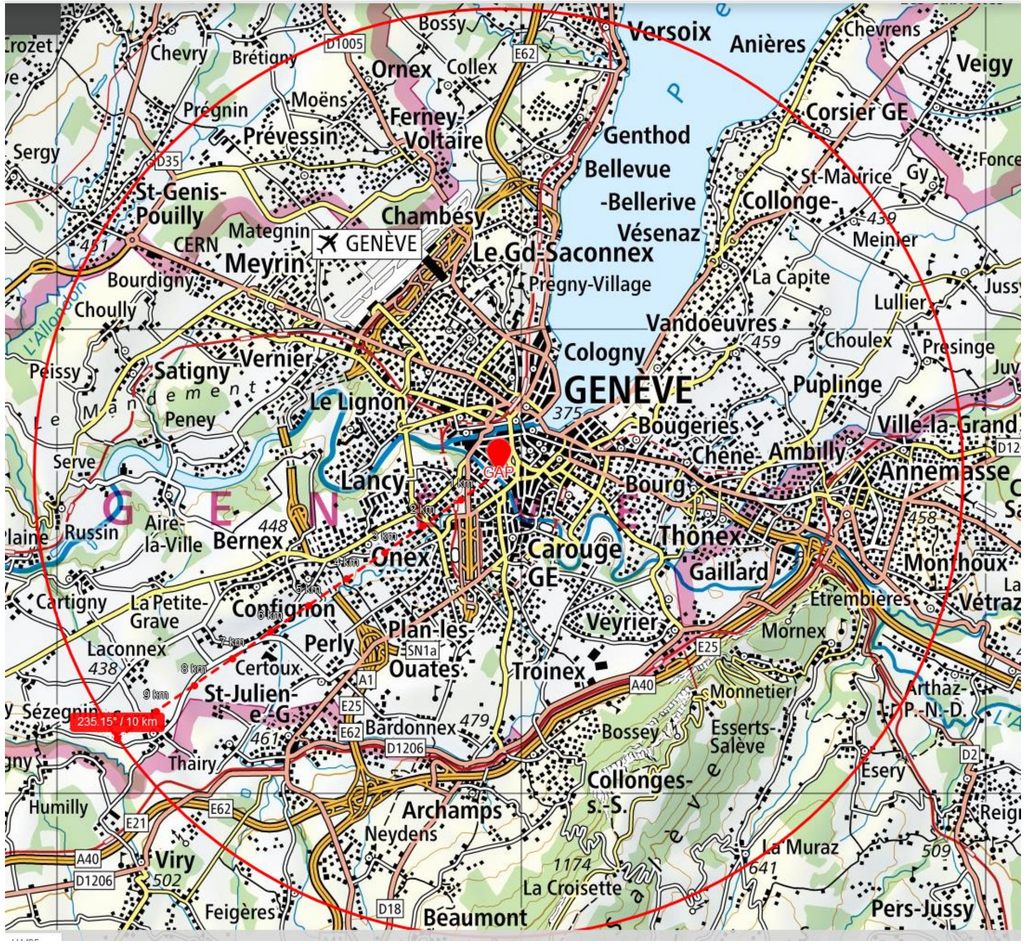




Grünenfelder, F. et al. *'Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems', Nat. Photon. 17, 422–426 (2023)*

Results

Distance (km) (ULL-SMF)	Sifted key rate (Mbps)	$QBER_Z$ (%)	Phi_Z (%)	Secret key rate (Mbps)
102.4	7.8	0.3	1.0	3.0
10.0	159.4	0.4	0.8	63.6



Grünenfelder, F. et al., Nat. Photon. 17, 422–426 (2023)

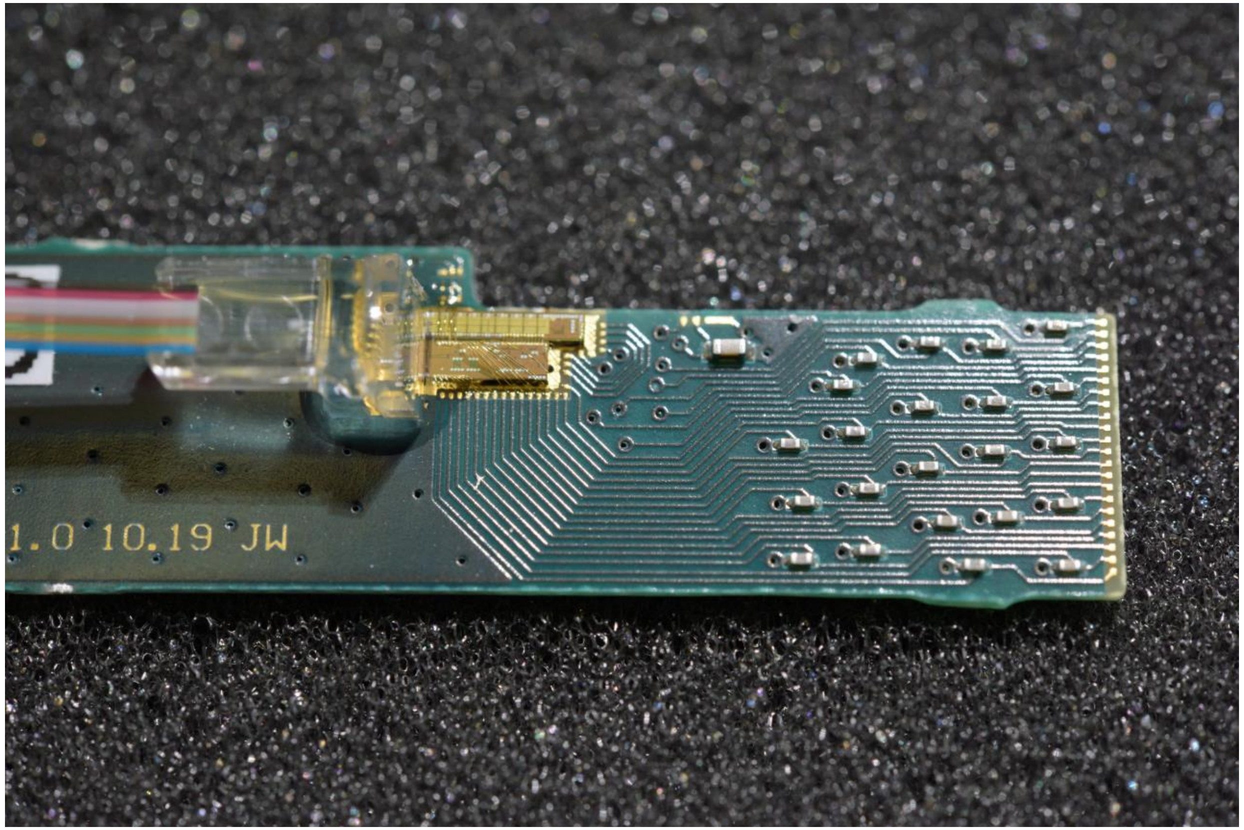
Li, W. et al. Nat. Photon. 17, 416–421 (2023)

IV. High-speed integrated QKD

In collab. with: POLITECNICO MILANO 1863, IDQ, sicoya, CNR IFN Istituto di Fotonica e Nanotecnologie

Integrated photonics

Image: Transmitter



Advantages:

low cost,

small footprint,

mass production,

reliable,

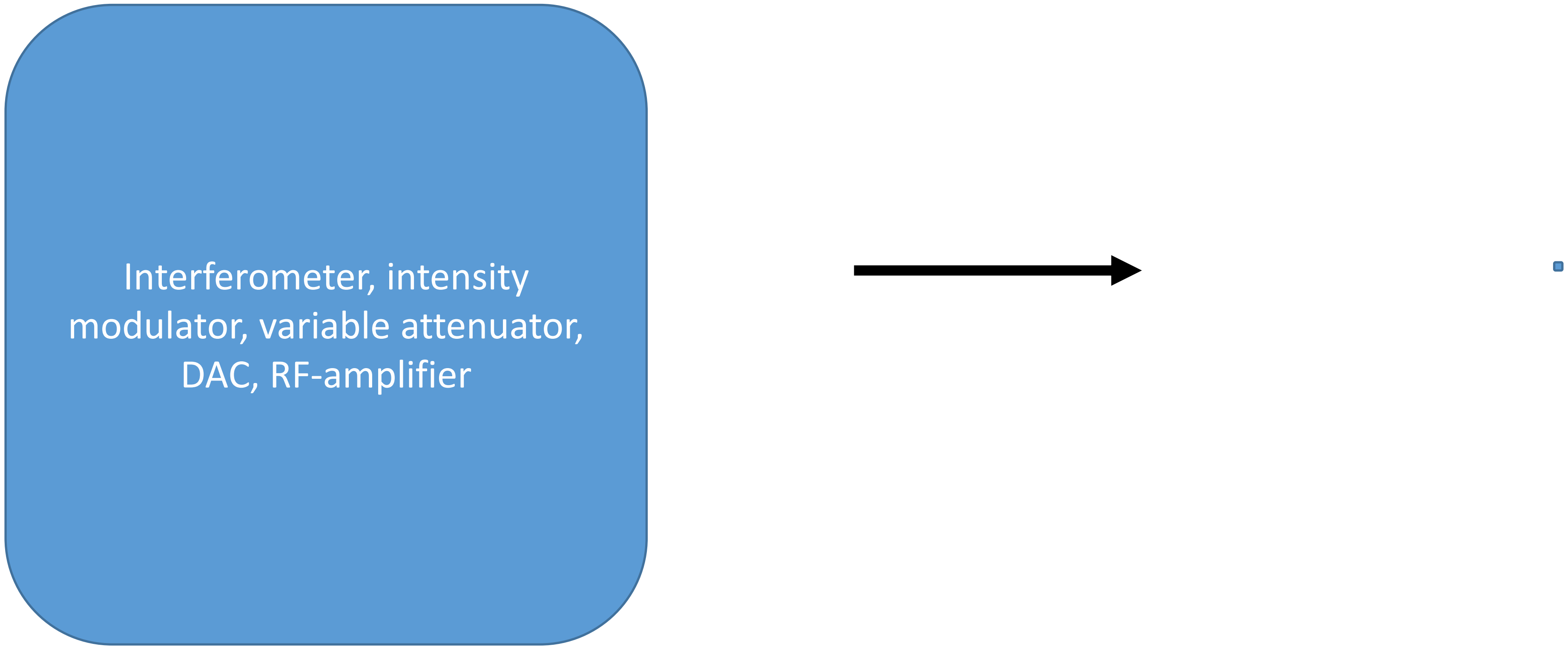
low power consumption,

…

Transmitter – Alice

Fiber-based transmitter

Integrated transmitter



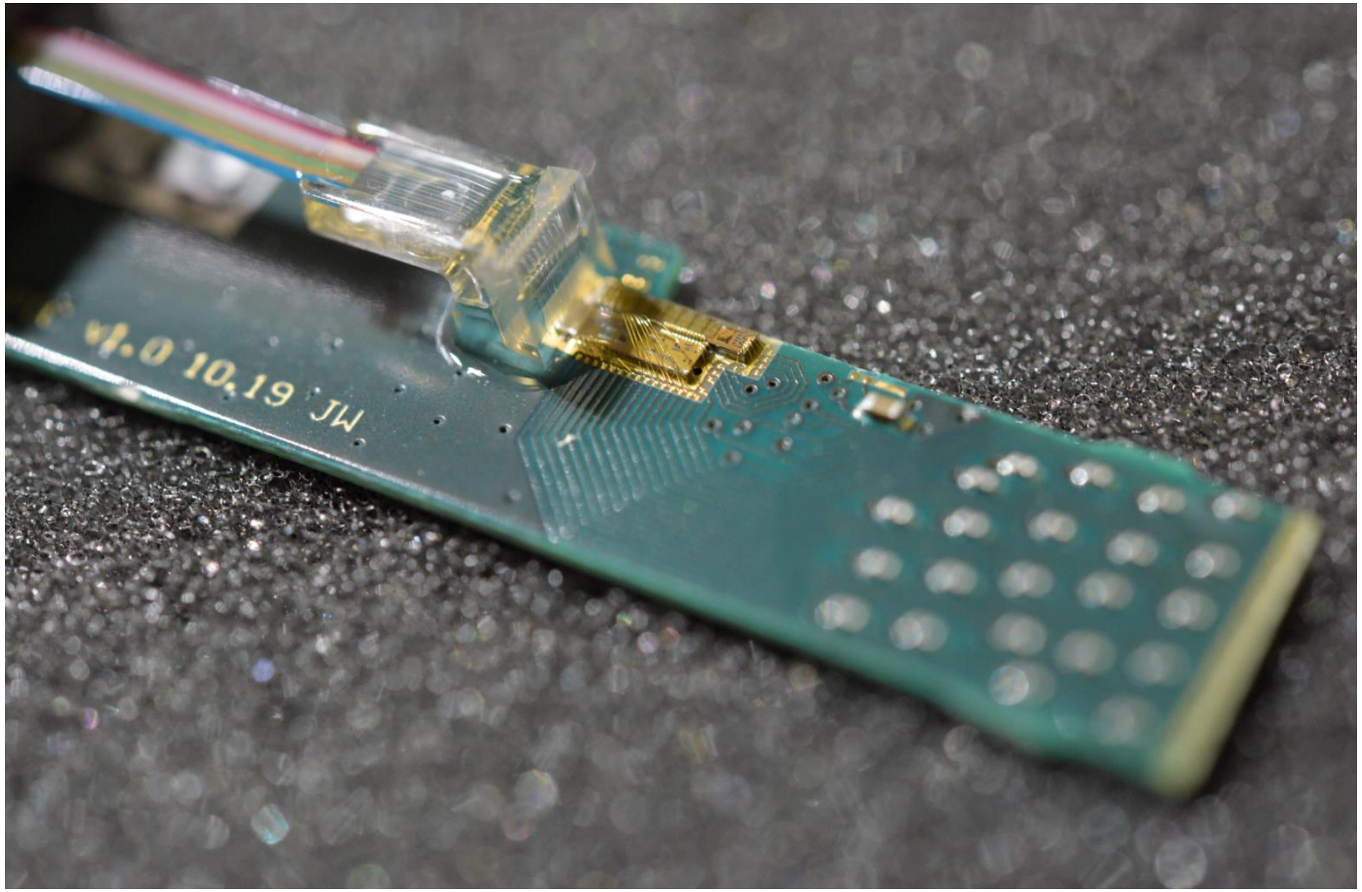
Transmitter – Alice

- Based on silicon photonics
- Footprint: 1.1 mm x 4.5 mm

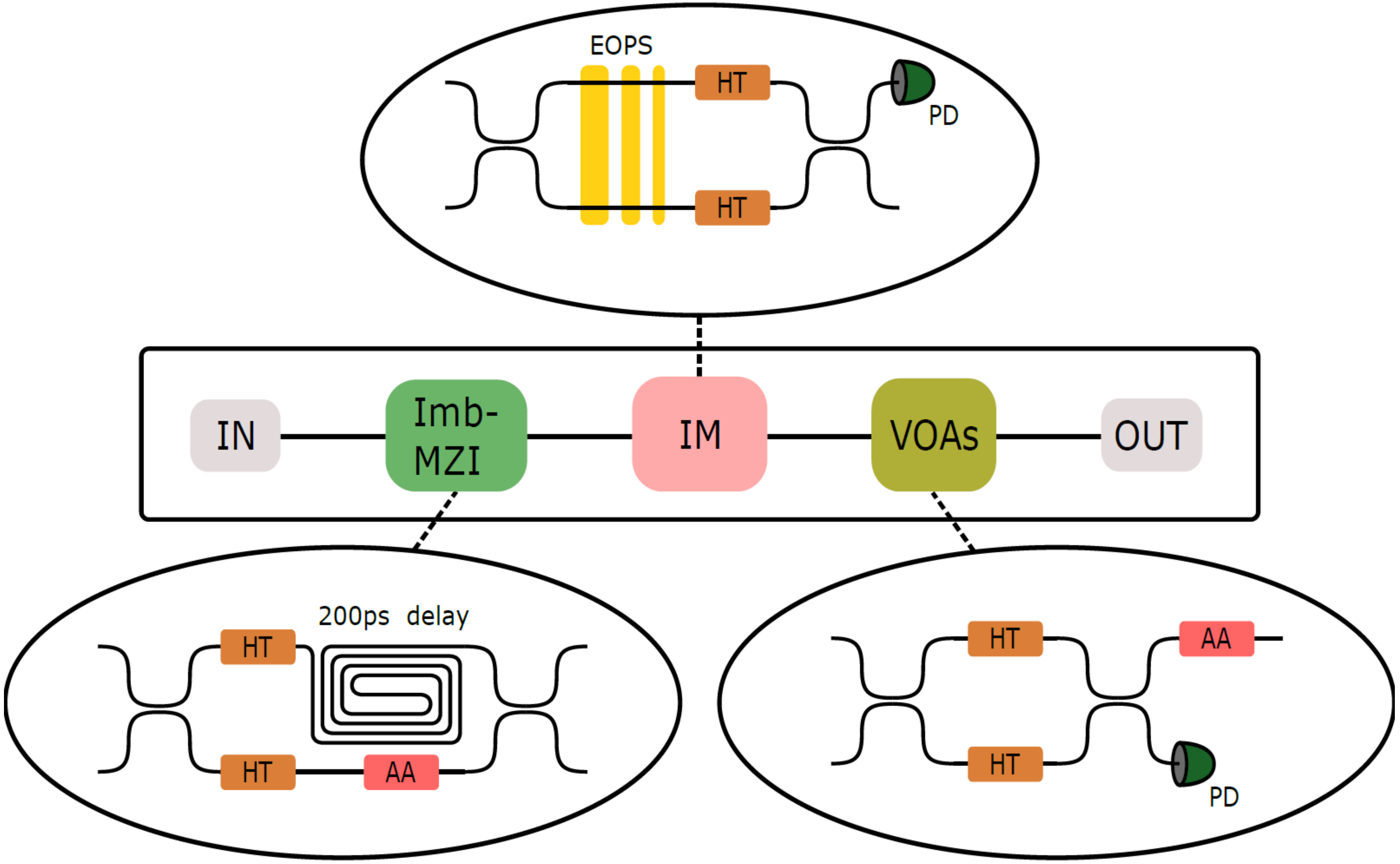
Platform choice

Pros: Small footprint, PIC and EIC, fast modulation

Cons: Cannot integrate laser

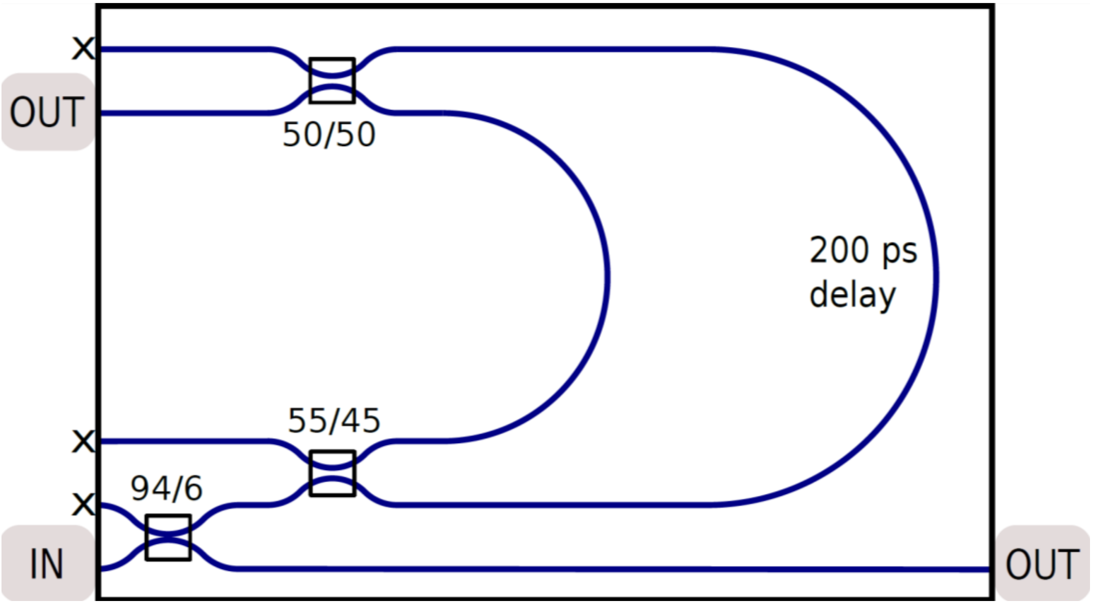


Transmitter – Alice

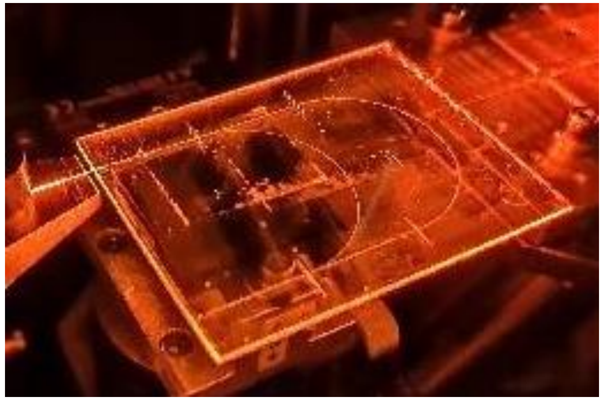


Receiver - Bob

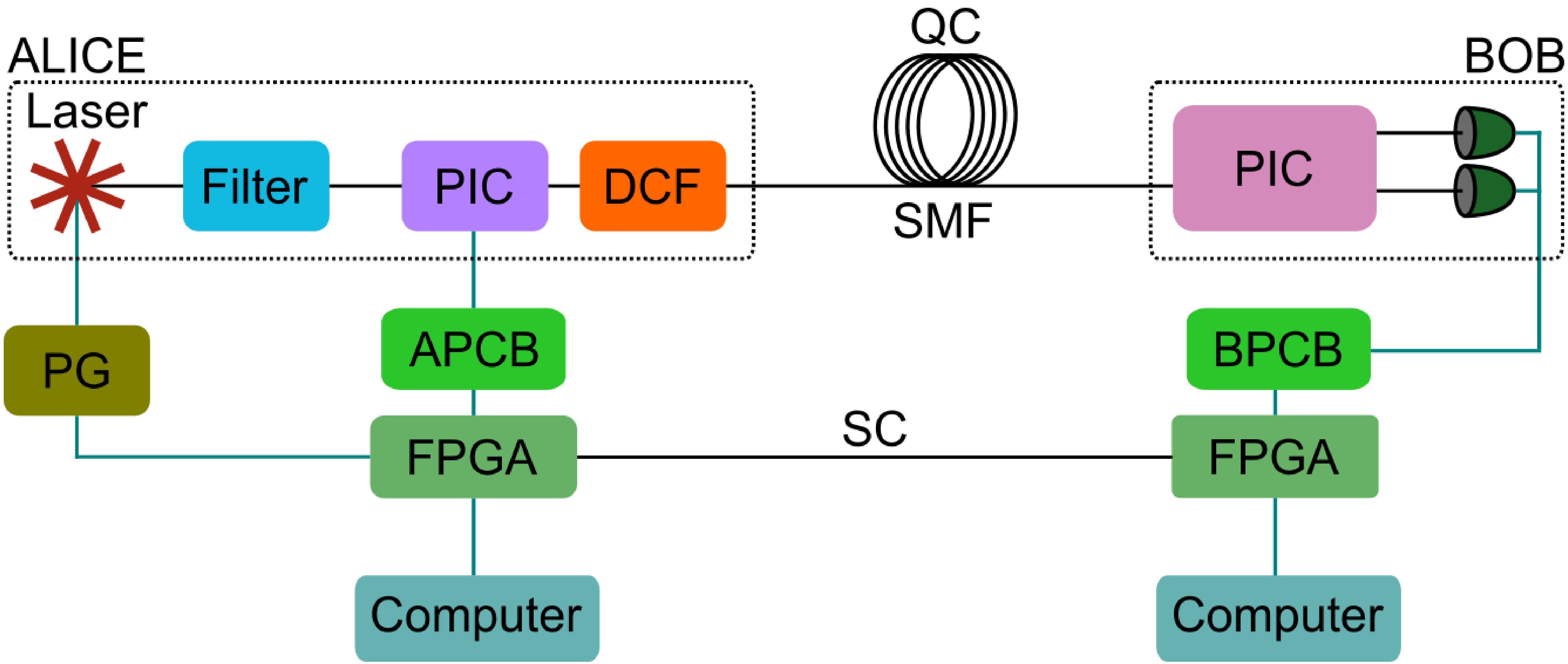
- Based on silica
- Fabricated at CNR – IFN, Milano (R. Osellame) using femtosecond laser micromachining technique



Platform choice
Pros: Low loss (3 dB), polarization insensitive
Cons: Cannot integrate detector,
«large» footprint (8 cm x 6 cm)



Full experimental setup: Integrated QKD



Sax, R. et al. ‘High-speed integrated QKD system’ Photon. Res. 11, 1007-1014 (2023)

Results: InGaAs/InP detectors

Distance	Raw key rate (kbps)	$QBER_Z$ (%)	Phi_Z (%)	Secret key rate (kbps)
150 km	18.0	3.6	2.1	2.9
150 km	23.0	3.2	2.1	7.2

← *Boaron, A. et al. 'Simple 2.5 GHz time-bin quantum key distribution', Appl. Phys. Lett. 23, (2018)*

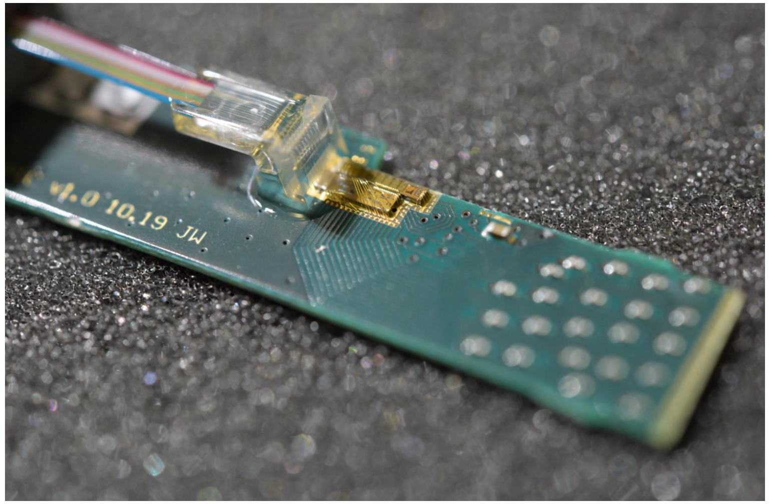
QBER = quantum bit error rate

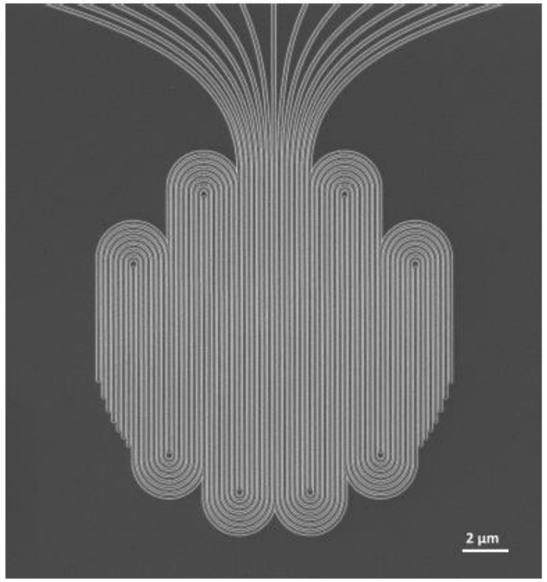
Phi_Z = phase error rate

Sax, R. et al. 'High-speed integrated QKD system' Photon. Res. 11, 1007-1014 (2023)

Conclusion

- QC in O-band and CC in C-band: possible key generation in a high-loss link
- Record high-SKR QKD at metropolitian and longer distances
- Integrated QKD at long distances with competetive SKRs and low QBERs

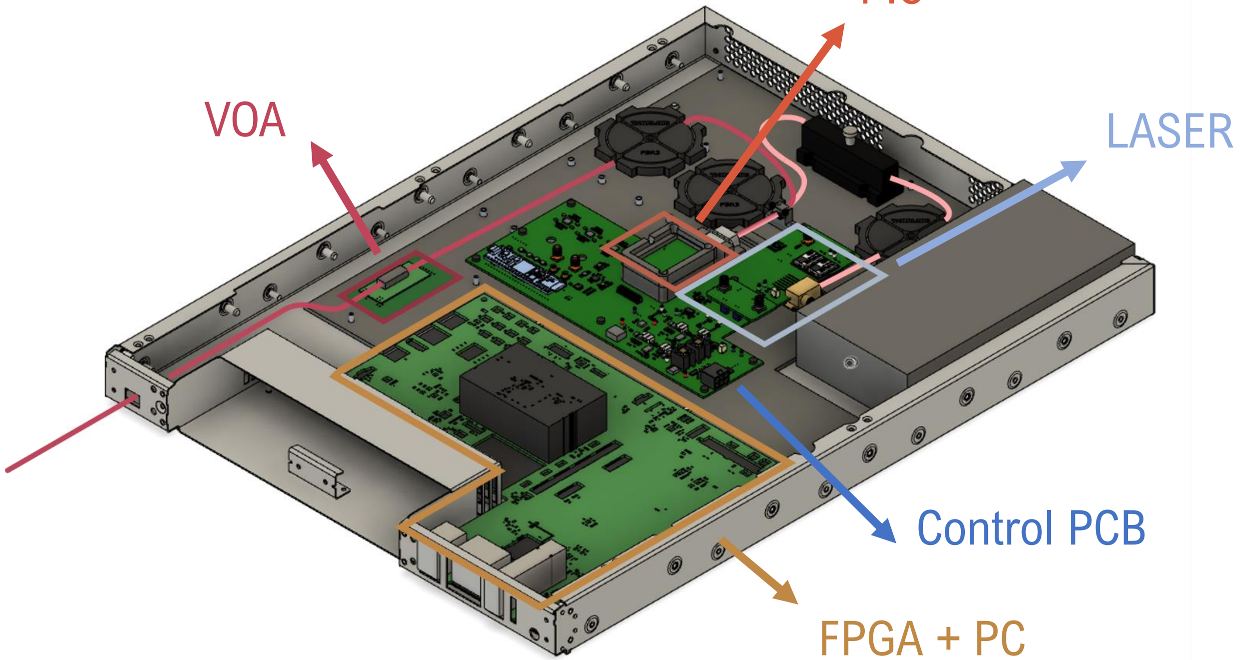




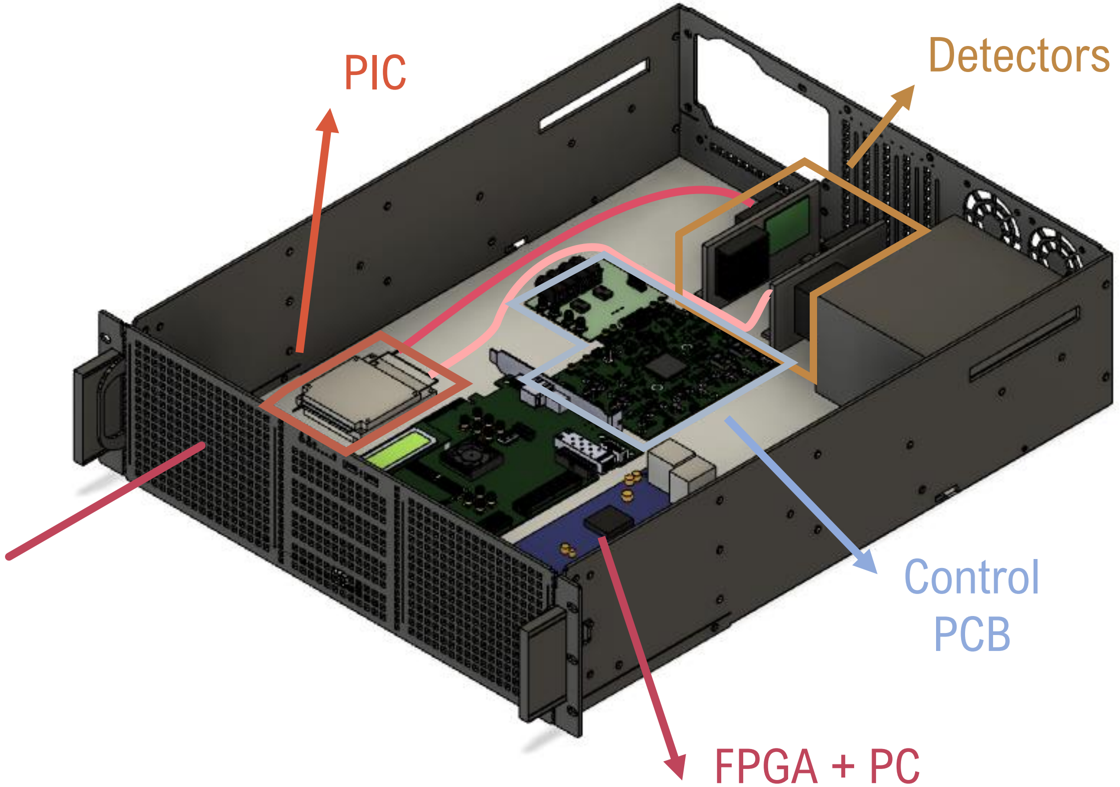
Ongoing work

- Integrated QKD: practical prototype!

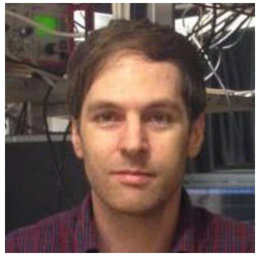
Alice



Bob



On behalf of the Quantum Technologies group and IDQ partners in Geneva:



+ Sylvain El-Khoury

Thank you for your attention!