TOSHIBA

UNIVERSITY OF LEEDS

Twin Field QKD

Experimental repeater-like quantum communications over 600 km of optical fibre with dual-band phase stabilisation

Mirko Pittaluga

Toshiba Europe Ltd.

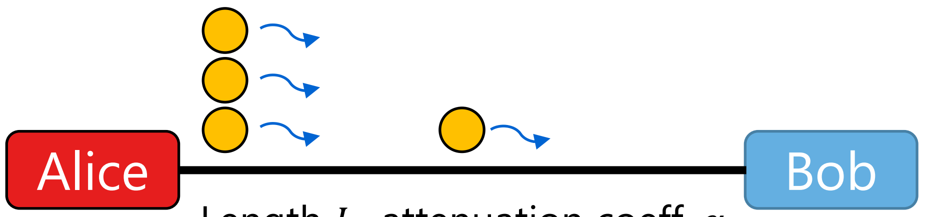
QCrypt 2021
Invited talk
Virtual conference, 26 August 2021

This project has received funding from the European Union's Horizon 2021 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675662

Contents

Limitations of point-to-point QKD

Point-to-point QKD



Length L , attenuation coeff. α

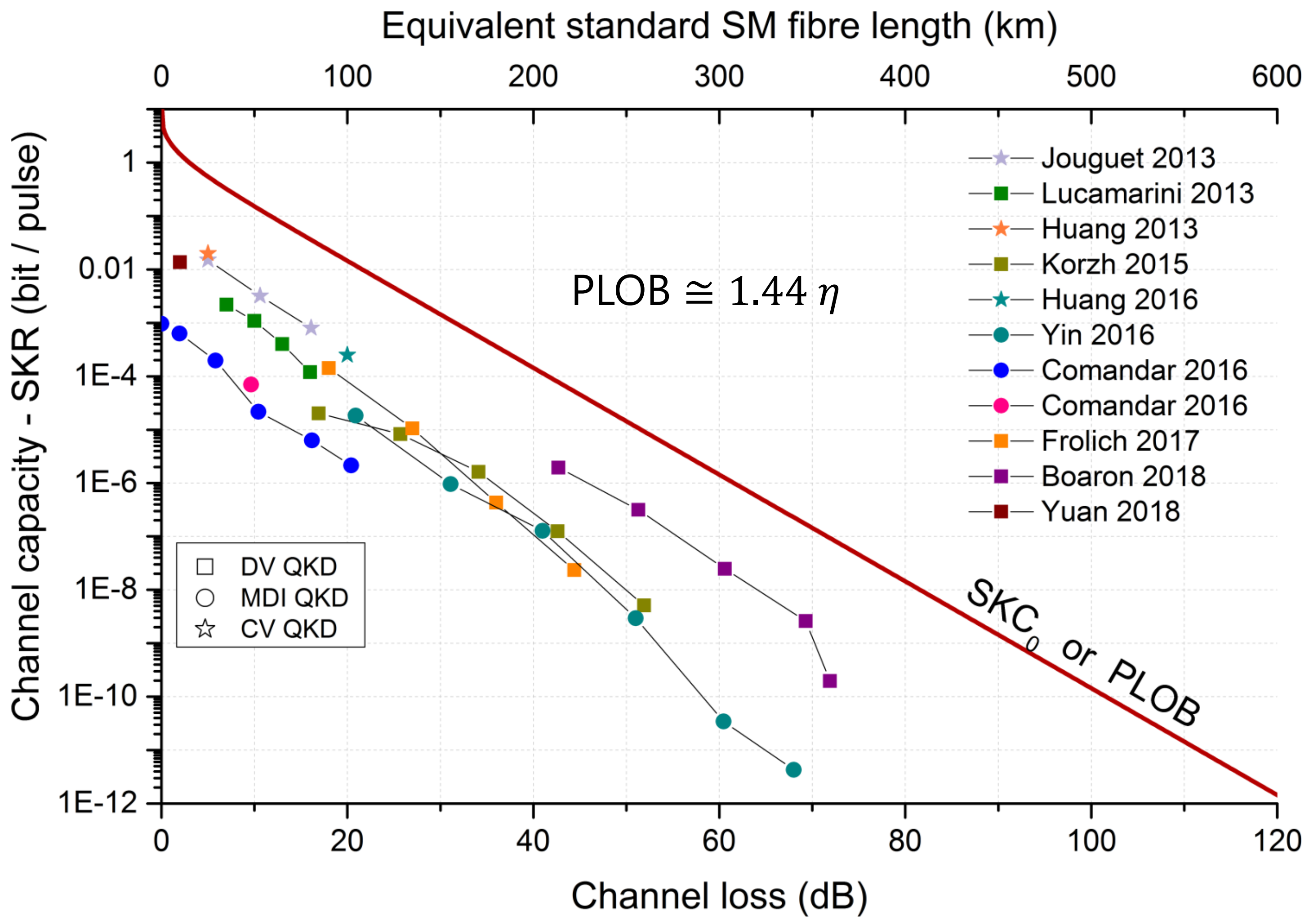
Channel transmission → $\eta = 10^{-\frac{\alpha L}{10}}$

QKD rate $\propto \eta$

Channel loss
+
No-cloning theorem

→

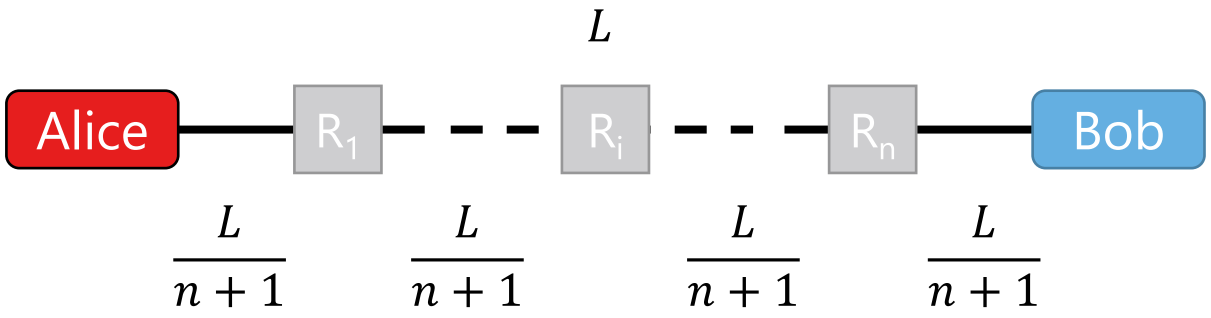
Limit the range of QKD



* Pirandola, *et al.* (2017): Fundamental limits of repeaterless quantum communications. Nat Commun 8, p. 15043.

Extending the range of QKD with quantum repeaters

Quantum repeaters

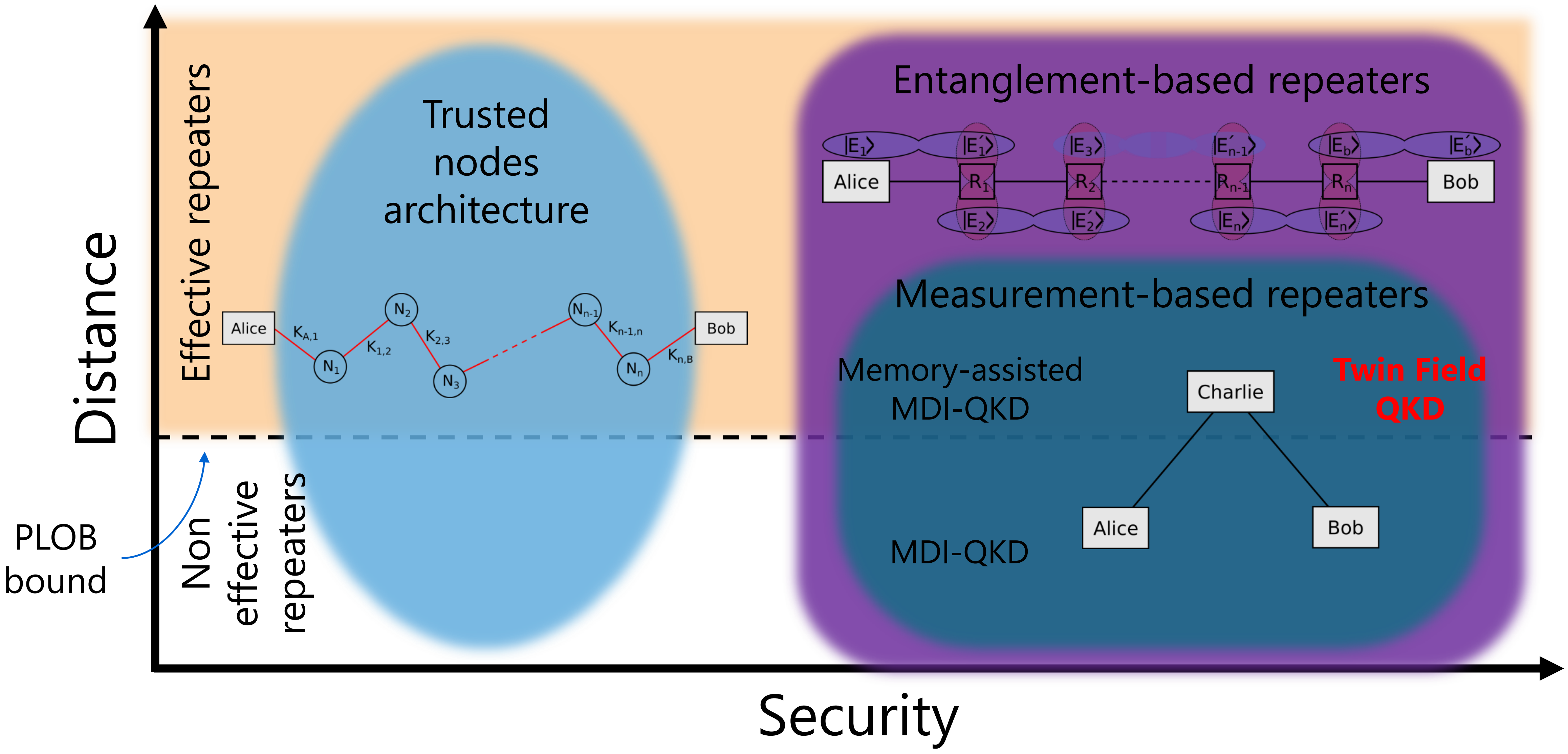


There are several types of quantum repeaters, which can be grouped by their properties

From ref. * : *"In an information-theoretic sense, a quantum repeater [...] is any type of middle node between Alice and Bob that helps their quantum communication by breaking down their original quantum channel in two different quantum channels."*

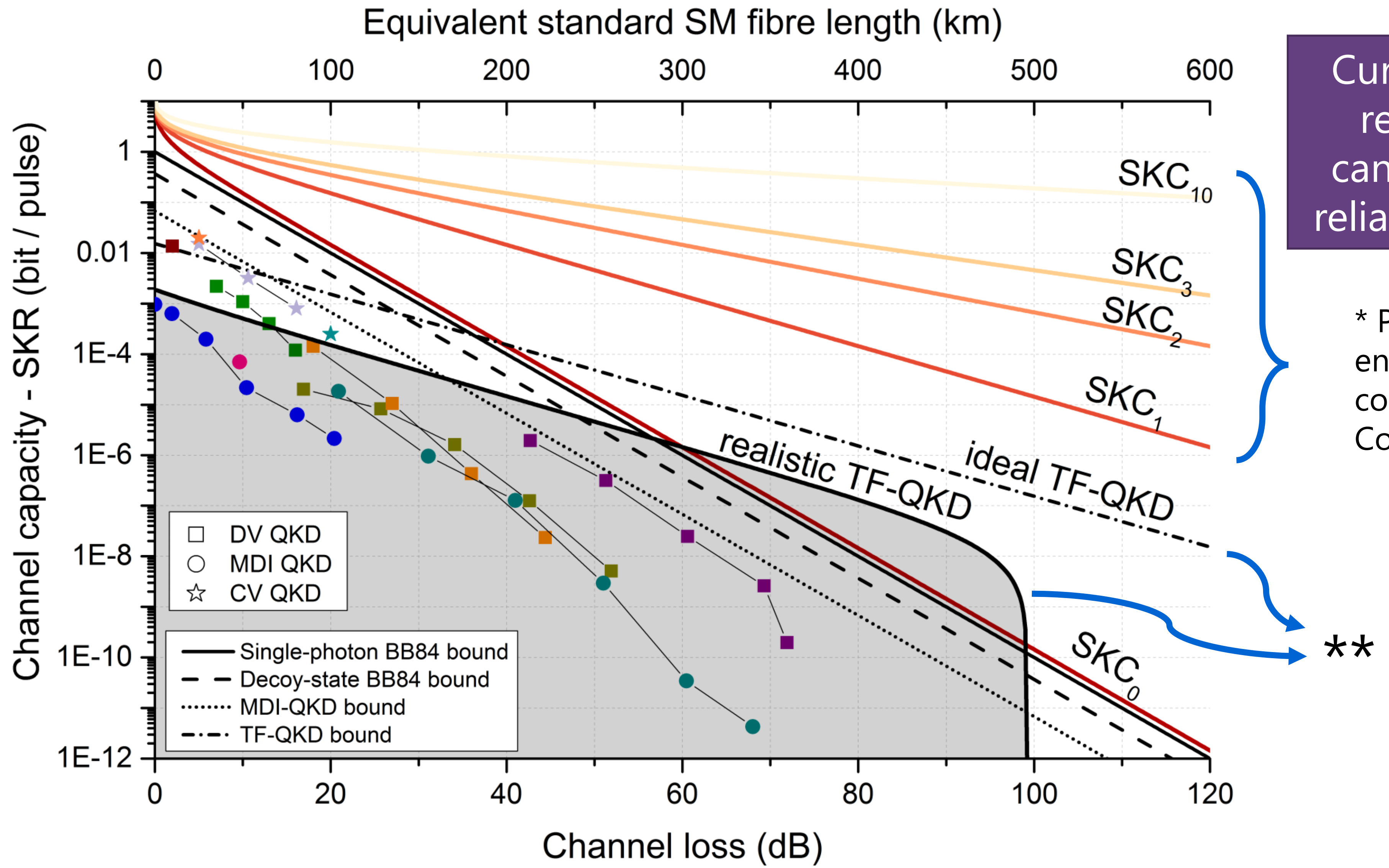
* Pirandola, *et al.* (2020): Advances in quantum cryptography. *Adv. Opt. Photon.* 12 (4), p. 1012

Types of quantum repeaters



* Pirandola, *et al.* (2020): Advances in quantum cryptography. *Adv. Opt. Photon.* 12 (4), p. 1012

Secret Key Rate-to-Loss scaling of repeater assisted QKD



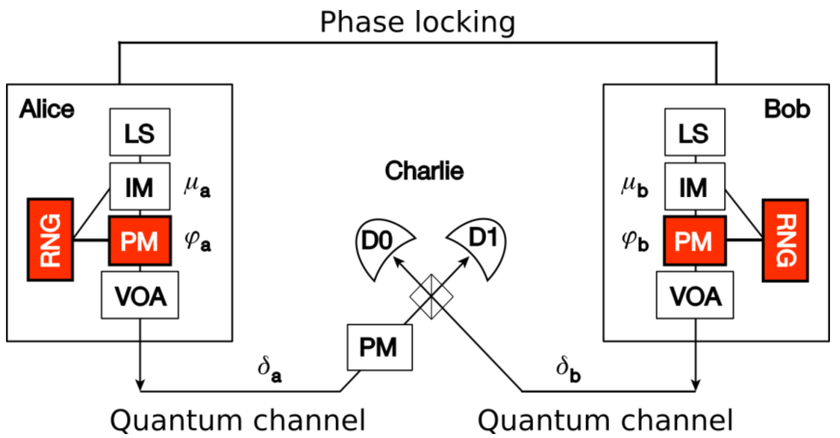
Current multi-nodes quantum repeaters implementations cannot yet support stable and reliable long-distance operation

* Pirandola (2019): End-to-end capacities of a quantum communication network. Commun Phys 2 (1), p. 1023.

Only readily implementable protocol overcoming the PLOB bound (or SKC_0) at high attenuations

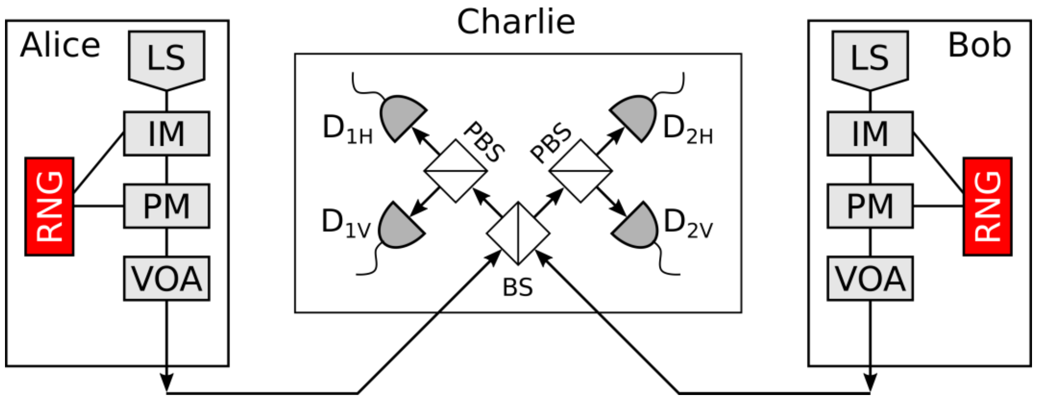
** Lucamarini, *et al.* (2018): Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature 557 (7705), pp. 400–403.

Implementation of the TF-QKD protocol



TF-QKD *

- **Encoding:** information encoded in the phase of the optical fields
- **Type of interference:** 1st order interference (optical field interference)
- **Detection:** Single photon detection
- **Secret Key Rate (SKR)** $\propto \sqrt{\eta}$
- Removes detectors side channels, detection made by an untrusted relay



MDI-QKD **

- **Encoding:** Alice and Bob prepare and send the single photons
- **Type of interference:** 2nd order interference (Hong-Ou-Mandel)
- **Detection:** 2-photons coincidence measurement
- **Secret Key Rate (SKR)** $\propto \eta$
- Removes detectors side channels, detection made by an untrusted relay

* Lucamarini, *et al.* (2018) Nature 557 (7705), pp. 400–403

** Lo, *et al.* (2012) *PRL* 108 (13), p. 130503

Advances in Twin-Field Quantum Key Distribution (TF-QKD)

Theory

- Tamaki, K.; *et al.* (2018): Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. http://arxiv.org/pdf/1805.05511v3.
- Ma, Xi.; *et aL* (2018): Phase-Matching Quantum Key Distribution. In Phys. Rev. X 8 (3), p. 325.
- Wang, X-B; *et al* (2018): Twin-field quantum key distribution with large misalignment error. In Phys. Rev. A 98 (6).
- Lin, J.; *et al.* (2018): Simple security analysis of phase-matching measurement-device-independent quantum key distribution. In Phys. Rev. A 98 (4).
- Cui, C.; *et al.* (2019): Twin-Field Quantum Key Distribution without Phase Postselection. In Phys. Rev. Applied 11 (3), p. 325.
- Curty, M.; *et al.* (2019): Simple security proof of twin-field type quantum key distribution protocol. In npj Quantum Inf 5 (1), p. 64.
- Jiang, C.; *et al.* (2019): Unconditional Security of Sending or Not Sending Twin-Field Quantum Key Distribution with Finite Pulses. In Phys. Rev. Applied 12 (2), p. 24061.
- Yu, Z-W; *et al.* (2019): Sending-or-not-sending twin-field quantum key distribution in practice. In Scientific reports 9 (1), p. 3080.
- Zhou, X-Y; *et al.* (2019): Asymmetric sending or not sending twin-field quantum key distribution in practice. In Phys. Rev. A 99 (6).
- Maeda, K; *et al.* (2019): Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit. In Nature communications 10 (1), p. 3140.
- Lu, F-Y; *et al.* (2019): Improving the performance of twin-field quantum key distribution. In Phys. Rev. A 100 (2).
- Grasselli, F.; *et al.* (2019): Practical decoy-state method for twin-field quantum key distribution. In New J. Phys. 21 (7), p. 73001.
- Xu, H.; *et al.* (2020): Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate. In Phys. Rev. A 101 (4).
- Wang, W.; et al. (2020): Simple method for asymmetric twin-field quantum key distribution. In New J. Phys. 22 (1), p. 13020.
- Wang, R.; et al. (2020): Optimized protocol for twin-field quantum key distribution. In Commun Phys 3 (1), p. 661.
- Jiang, Cong; *et al.* (2020): Zigzag approach to higher key rate of sending-or-not-sending twin field quantum key distribution with finite-key effects. In New J. Phys. 22 (5), p. 53048.
- Currás-Lorenzo, G.; *et al.* (2021): Tight finite-key security for twin-field quantum key distribution. In npj Quantum Inf 7 (1), p. 1301.

Experimental

- Minder, M.; *et al.* (2019): Experimental quantum key distribution beyond the repeaterless secret key capacity. In Nature Photon 13 (5), pp. 334–338.
- Wang, S.; *et al.* (2019): Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System. In Phys. Rev. X 9 (2).
- Liu, Y.; *et al.* (2019): Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending. In Phys. Rev. Lett. 123 (10).
- Zhong, X.; *et al.* (2019): Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution. In Phys. Rev. Lett. 123 (10), p. 100506.
- Fang, X.-T.; *et al.* (2020): Implementation of quantum key distribution surpassing the linear rate-transmittance bound. In Nature Photon 14 (7), pp. 422–425.
- Chen, J.-P.; *et al.* (2020): Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km. In Phys. Rev. Lett. 124 (7), p. 70501.
- Clivati, C.; *et al.* (2020): Coherent phase transfer for real-world twin-field quantum key distribution. Available online at http://arxiv.org/pdf/2012.15199v1.
- Zhong, X.; *et al.* (2021): Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses. In npj Quantum Inf 7 (1), p. 7.
- Pittaluga, M.; *et al.* (2021): 600-km repeater-like quantum communications with dual-band stabilization. In Nat. Photonics 560, p. 7.
- Liu, H.; *et al.* (2021): Field Test of Twin-Field Quantum Key Distribution through Sending-or-Not-Sending over 428 km. In Phys. Rev. Lett. 126 (25).
- Chen, J.-P.; *et al.* (2021): Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. In Nat. Photonics 299, p. 1476.

Reviews *which include TF-QKD*

- Pirandola, S.; *et al.* (2020): Advances in quantum cryptography. In Adv. Opt. Photon. 12 (4), p. 1012.
- Xu, F.; *et al.* (2020): Secure quantum key distribution with realistic devices. In Rev. Mod. Phys. 92 (2), p. 131.

TF-QKD experimental challenges

Experimental challenges for standard QKD implementation

- Single photons (or weak coherent pulses) generation and manipulation
- Quantum channel stabilisation (polarisation, time alignment, etc.)
- Single photons detection

Novel experimental challenges for TF-QKD implementation

Phase noise — $\delta_{ba} = \frac{2\pi}{s}(\Delta\nu L + \nu \Delta L)$

- $\Delta\nu$: Frequency difference between the users' lasers
- ΔL: Optical paths lenght fluctuation

Phase locking of distant sources

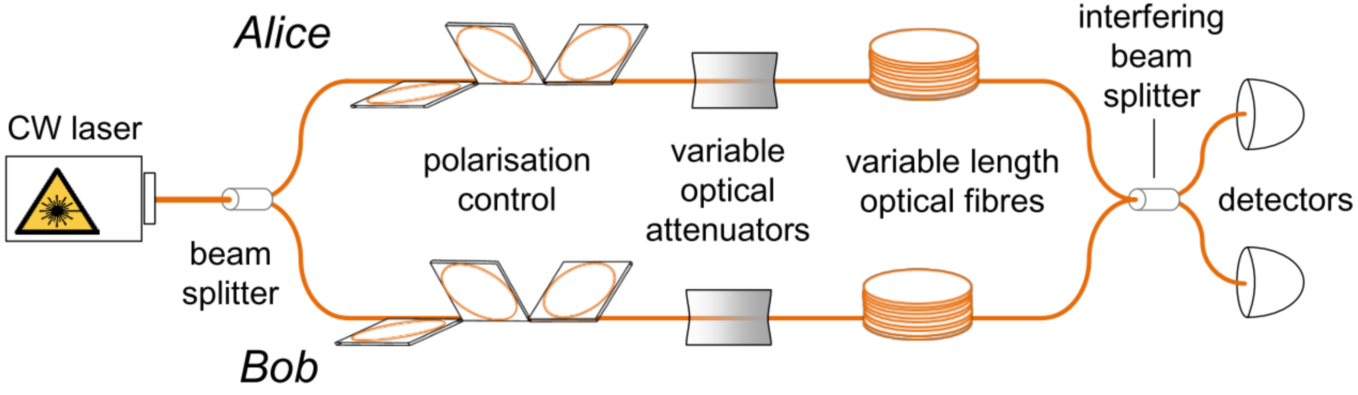
- Optical Injection Locking
- Optical Phase Locked Loop

Phase stabilisation of the quantum channel (sub-wavelength level)

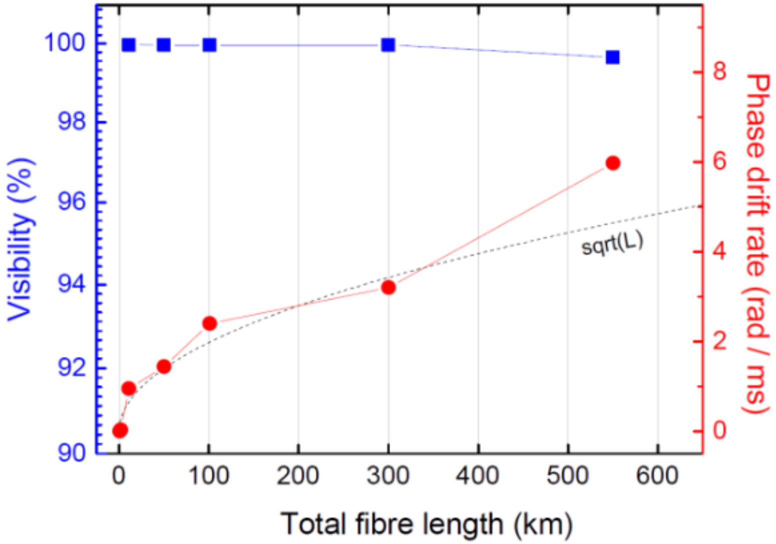
- Passive stabilization
- Active stabilization
  - in post-processing
  - in real time

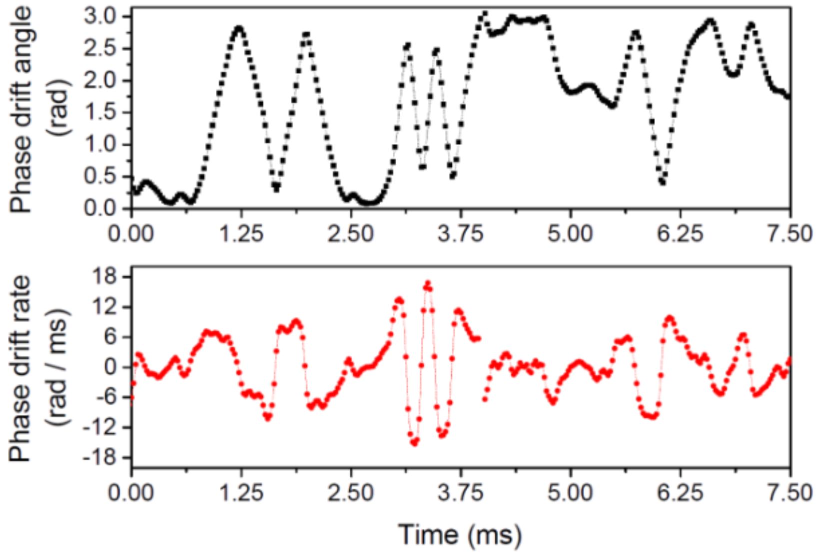
Phase noise introduced by optical fibres

Mach-Zehnder interferometer



Scaling of phase noise with interferometer size





* M. Lucamarini, *et al.* (2018): Nature 557 (7705), pp. 400–403

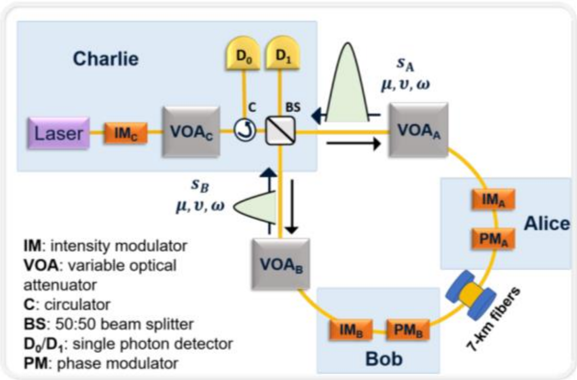
Removing phase noise introduced by optical fibres in TF-QKD

Remove phase noise introduced by optical fibres

Passive compensation

Active compensation

Sagnac loop experimental configuration

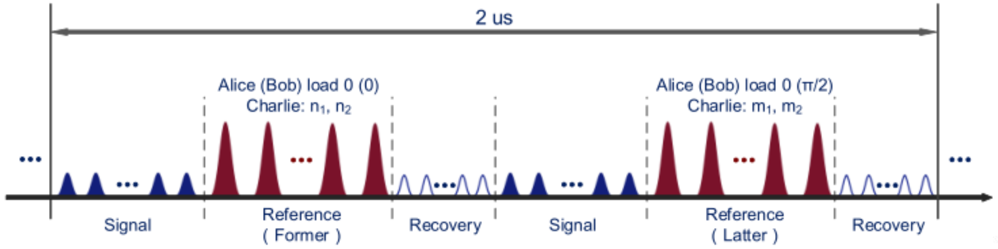


- X. Zhong, *et al.* (2019) *Phys. Rev. Lett.* 123 (10), p. 100506
- X. Zhong, *et al.* (2021) *npj Quantum Inf* 7 (1), p. 7

QCrypt 2021 – poster #132

Noise compensation in post-processing

Reference **time multiplexed** with signal

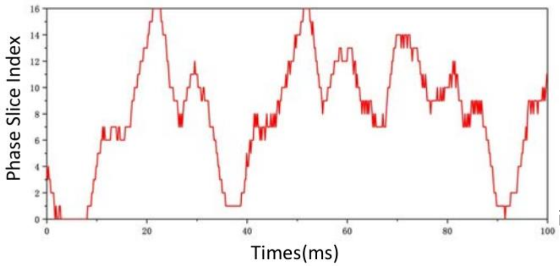


- X.-T. Fang, *et al.* (2020) *Nat Photonics* 14 (7), pp. 422–425
- J.-P. Chen, *et al.* (2020) *Phys. Rev. Lett.* 124 (7), p. 70501
- H. Liu, *et al.* (2021) *Phys. Rev. Lett.* 126 (25), p. 250502
- J.-P. Chen, *et al.* (2021) *Nat Photonics* 15 (8), pp. 570-575

Active noise cancellation

Reference **time multiplexed** or **wavelength multiplexed** with signal

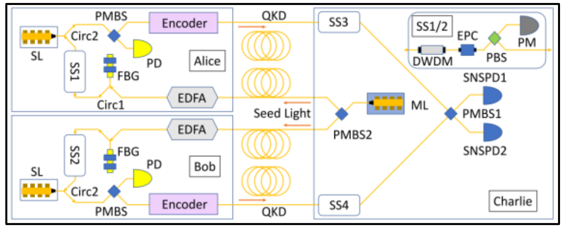
- S. Wang, *et al.* (2019) *Phys. Rev. X* 9 (2)
- M. Minder, *et al* (2019) *Nat Photonics* 13 (5), pp. 334–338



Results in long distance TF-QKD: lab and field trial experiments

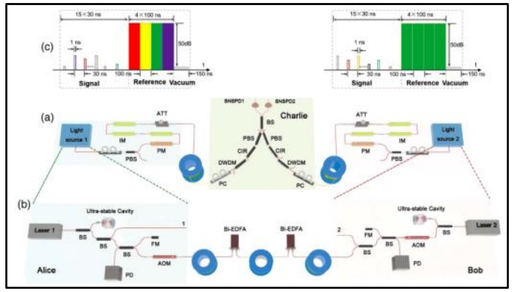
Lab-based TF-QKD over 502 km

X.-T. Fang, *et al.* (2020)
Nat Photon 14 (7), pp. 422–425



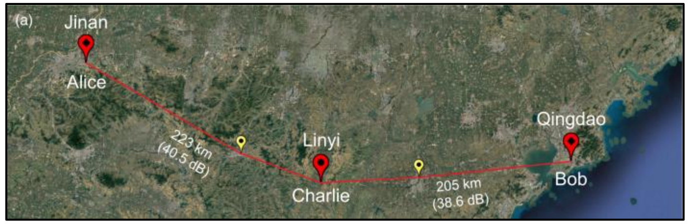
Lab-based TF-QKD over 509 km

J.-P. Chen, *et al.* (2020)
Phys. Rev. Lett. 124 (7), p. 70501



Field trial TF-QKD over 428 km

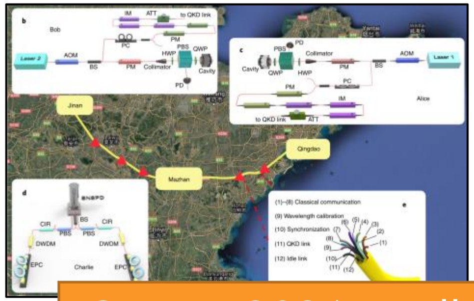
H. Liu, *et al.* (2021) *Phys. Rev. Lett.* 126 (25), p. 250502



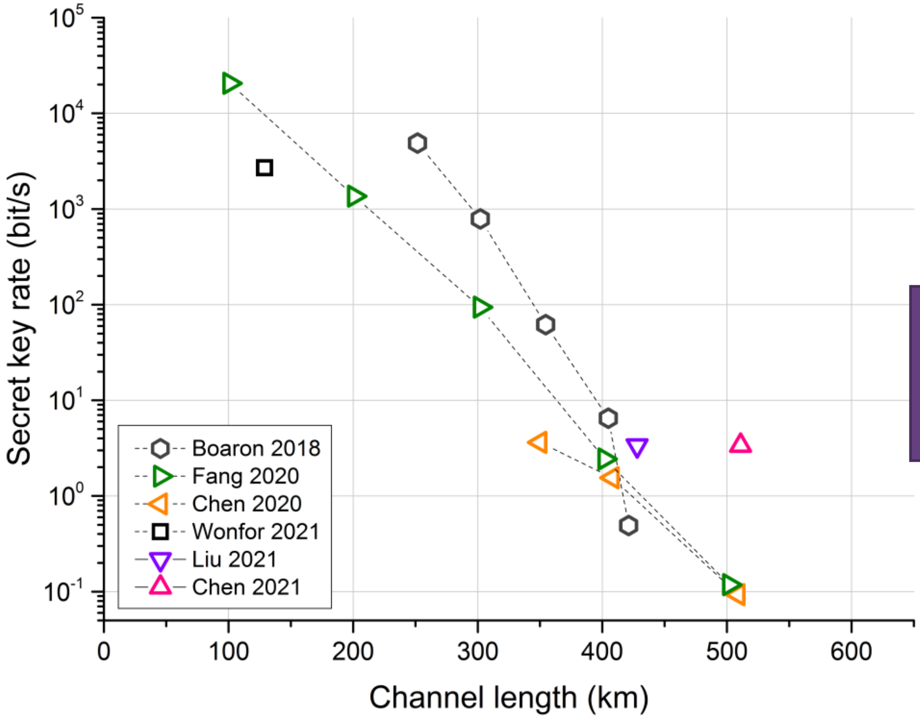
Field trail TF-QKD over 511 km

430 km installed fibre + 81 km in lab

J.-P. Chen, *et al.* (2021) *Nat Photonics* 15 (8), pp. 570-575



Qcrypt 2021 – talk 27/08 @ 14:30



Considerably extended the range of QKD!

...and the distance for field-trial implementations!

Common aspects:

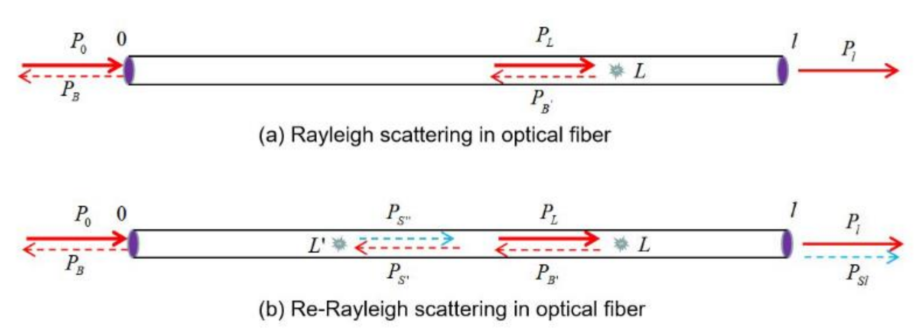
- Phase stabilization done in post-processing
- Reference signals time-multiplexed with the encoded pulses

Stabilization method drawbacks:

- Time multiplexing reduces the protocol clock rate (reducing the maximum achievable SKR)
- Bright stabilization signal at the same wavelength of the encoded signal introduces Rayleigh noise (which limits the maximum achievable distance)

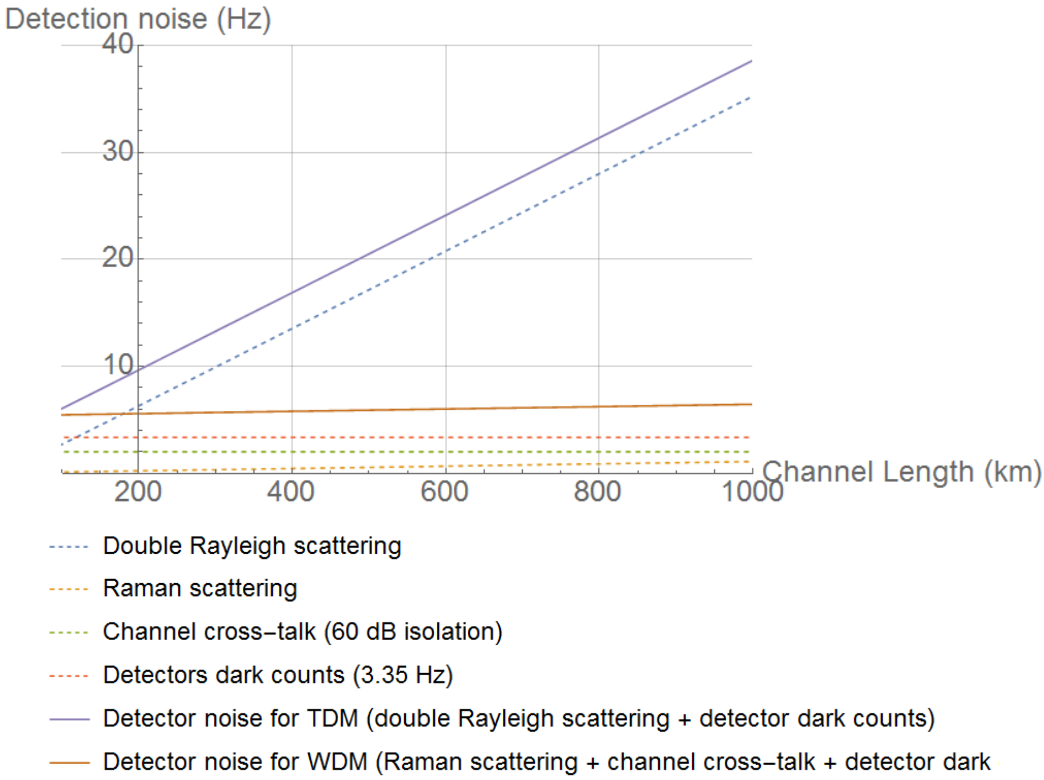
Double Rayleigh scattering – limiting factor for long distance TF-QKD

Double Rayleigh scattering



Limits to ~500 km the maximum distance for time multiplexed stabilisation

Comparison Rayleigh / Raman scattering



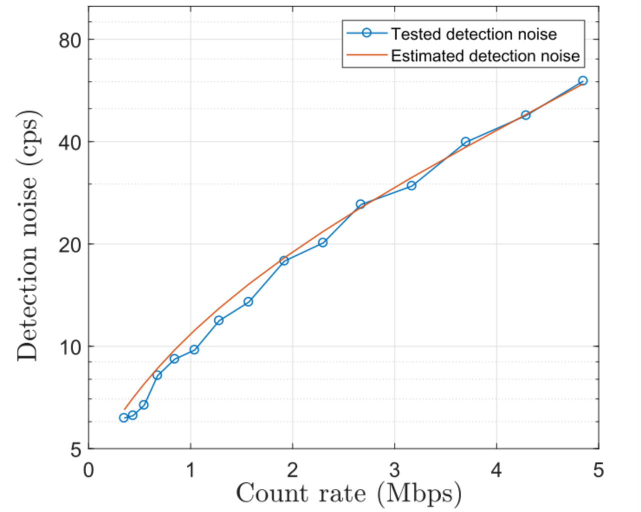


FIG. 6. Detection noise caused by double Rayleigh backscattering for different count rates in 250-km standard optical fiber. The blue circles show the experimental results and the orange curve shows the theoretical estimation results.

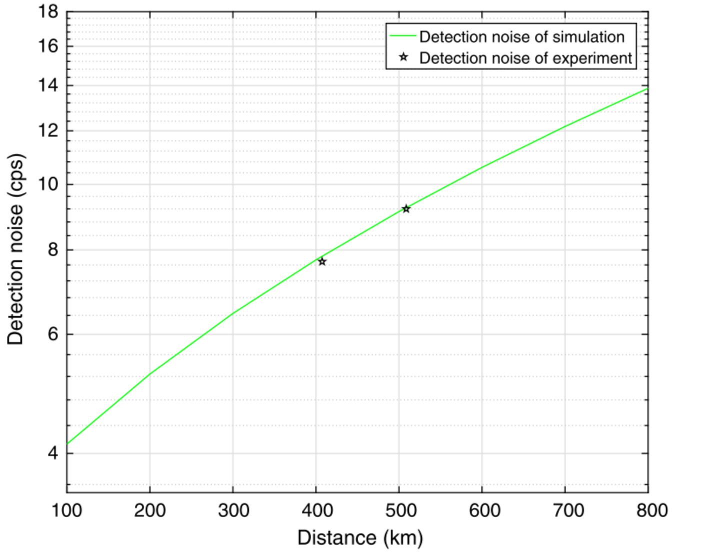
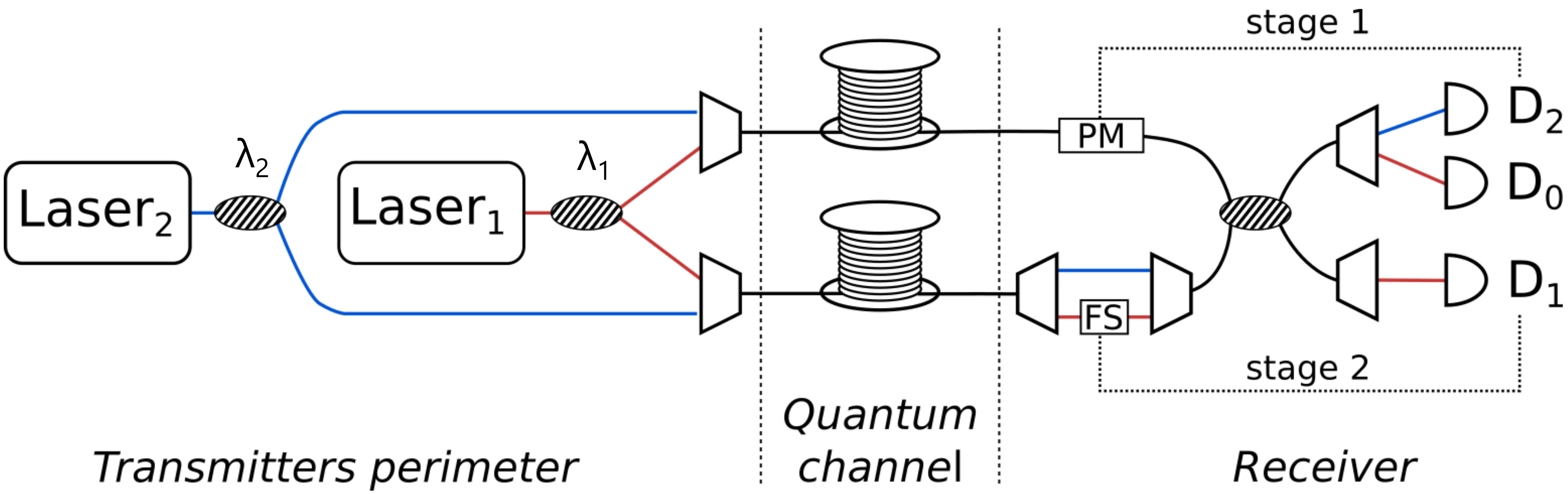


FIG. 2. Theoretical and experimental noise rates with different fiber lengths. Alice and Bob are assumed to emit at the working intensity, with 2 MHz reference counts detected. The green curve

J.-P. Chen, *et al.* (2020) *Phys. Rev. Lett.* 124 (7), p. 70501

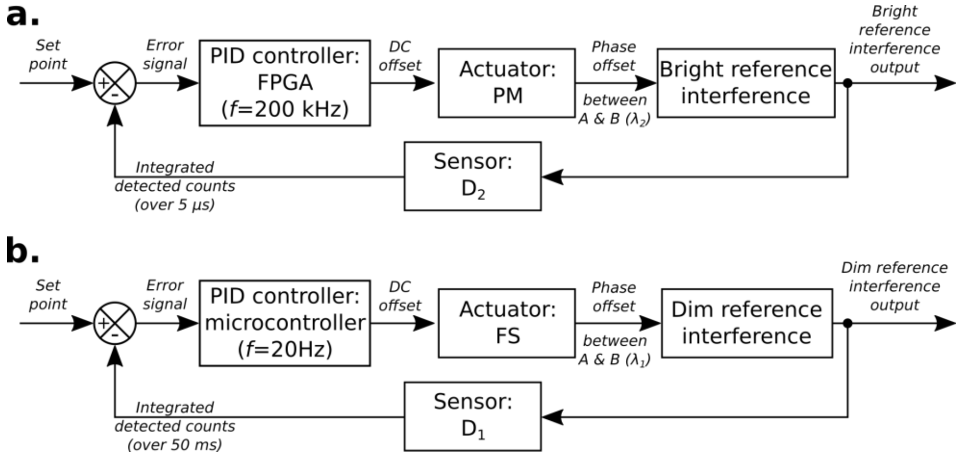
Dual-band phase stabilisation



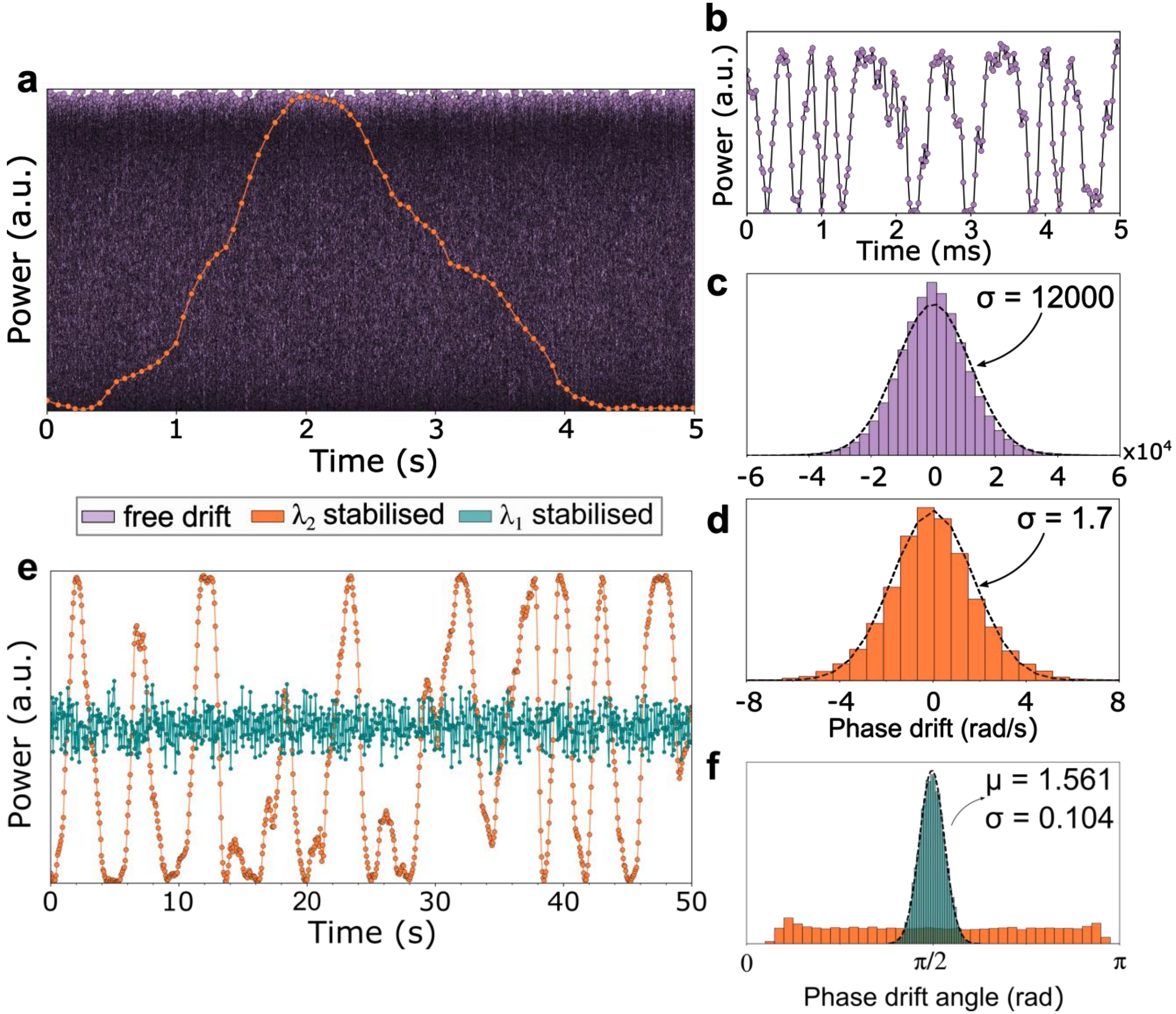
	Wavelength	Intensity	Modulation	Function
Reference wavelength	λ_2	High	None	Stage-1- phase compensation
Signal wavelength	λ_1	Low	Intensity & phase	Stage-2 phase compensation & key generation

Dual-band feedback scheme and characterization

Block schemes of the feedback loops



Stabilisation results for 600 km channel



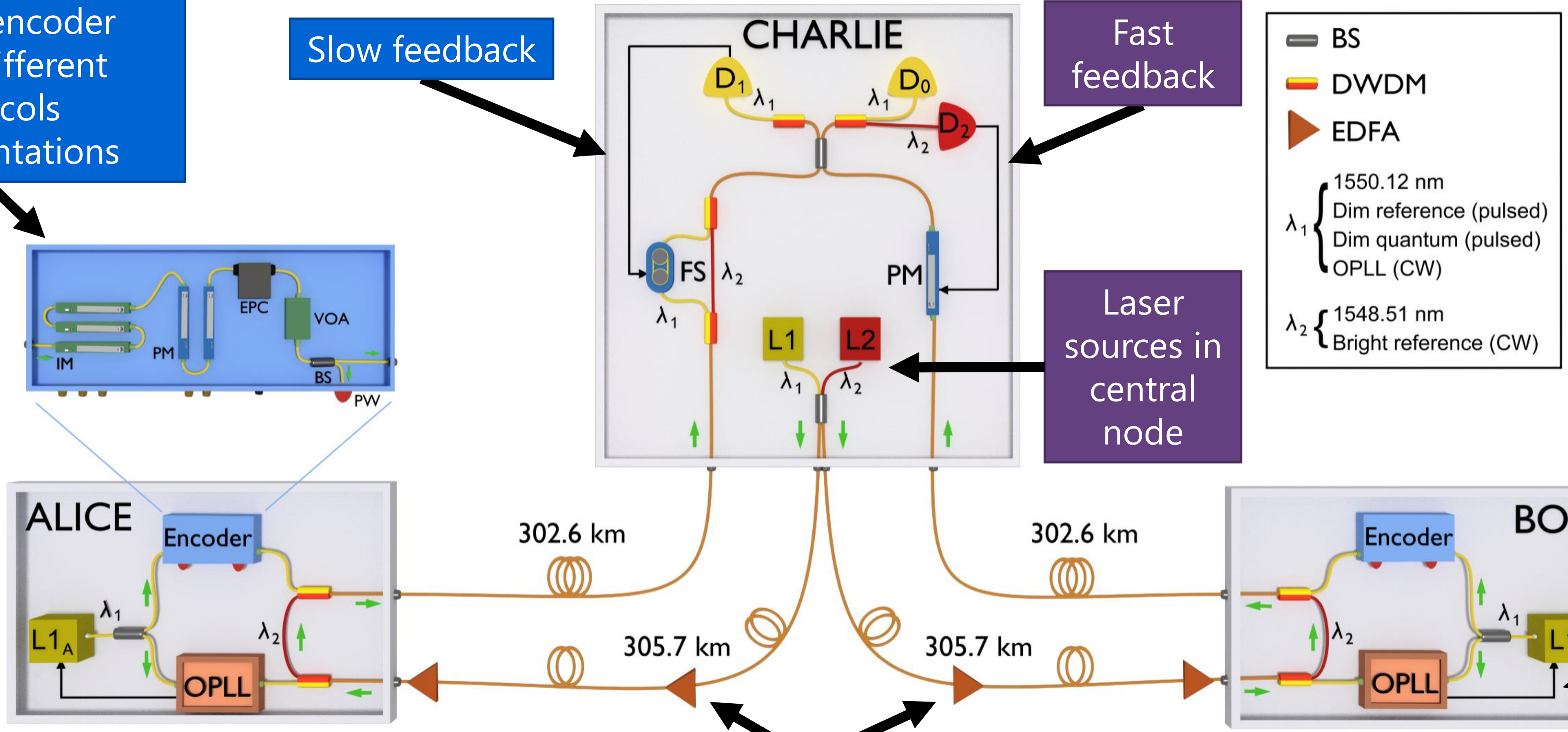
M. Pittaluga, *et al.* (2021) *Nat Photonics* 15 (7), pp. 530-535

Dual-band phase stabilisation applied to a TF-QKD setup

Flexible encoder allows different protocols implementations

Slow feedback

Fast feedback



Laser sources in central node

λ_1 regenerated through OPLL

Distributed optical signals amplified with EDFAs

Key elements:

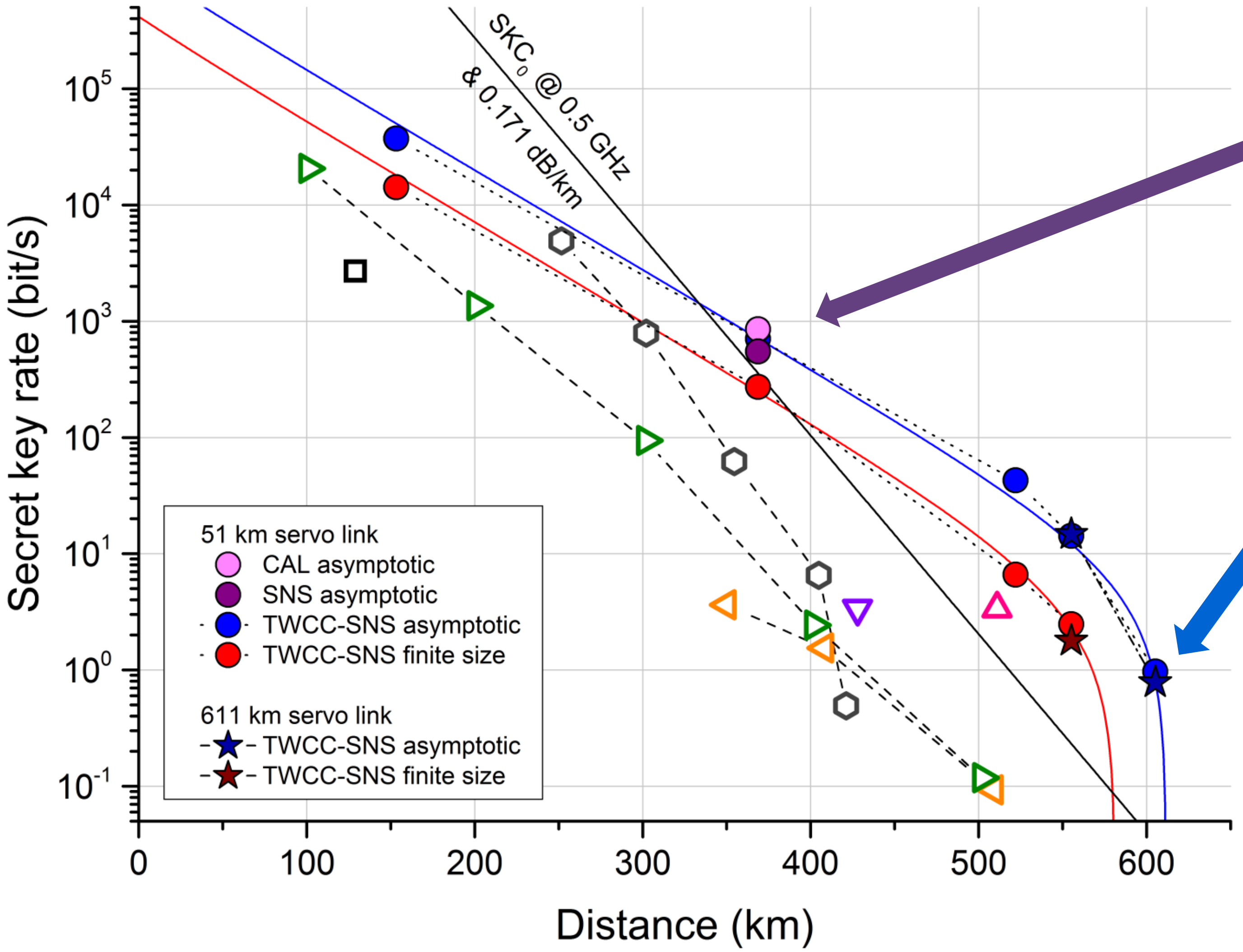
- Two wavelengths travelling through the communication channel;
- Two feedback system (coarse and fine) to compensate for the phase drift.

Advantages:

- Protocol clock rate not affected by stabilization signals;
- Elastic optical scattering occurring along the channel not hindering the protocol execution

M. Pittaluga, *et al.* (2021) *Nat Photonics* 15 (7), pp. 530-535

Results of TF-QKD beyond 600 km



Different protocols tested

Longest distance and highest loss ever achieved for fibre based QKD:

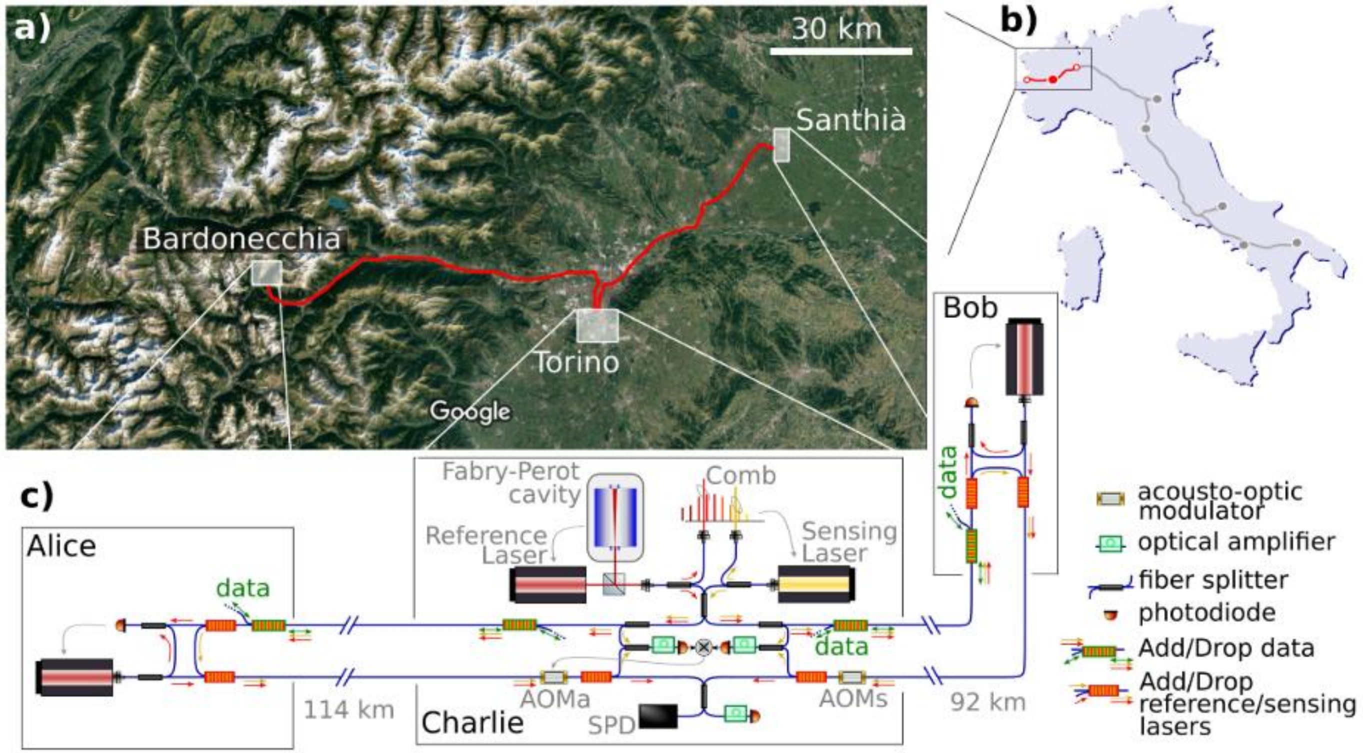
> 600 km
> 100 dB

Feasibility of dual-band stabilisation technique for real world operations?

M. Pittaluga, *et al.* (2021) *Nat Photonics* 15 (7), pp. 530-535

Italian TF-QKD-ready field trial

Coherent dual-band stabilisation system in deployed fibres



- 206 km of installed fibres
- 65 dB of channel attenuation

Qcrypt 2021 – poster #96

European fibre based network for Time-Frequency dissemination

Phase fluctuations massively reduced

F. Rhiele, Nat Photonics 2017

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

TOSHIBA

C. Clivati, *et al.* (2020) arXiv:2012.15199v1

Phase sensitive quantum communications

Phase-sensitive quantum communications

Absolute phase encoding useful beyond QKD

Class of quantum communications tasks where the Qbit state is encoded in the absolute phase of the optical field transmitted

Absolute phase -> very delicate physical property

Classical amplification of the signal -> not possible

Quantum secret sharing

Quantum fingerprinting

Phase-based quantum internet

Longer-baseline telescopes

Quantum key distribution (**Twin Field QKD**, Side channel free QKD)

...

Conclusions

- Measurement-based **1-node quantum repeaters** allowed to overcome the SKC_0 bound

- Demonstrated for the first time QKD **>100 dB loss** and **>600 km of fibre**

- Introduced and demonstrated the feasibility of the dual-band phase stabilisation technique. This technique could be a future resource for phase-based quantum communications

- Proved feasibility of dual-band stabilisation in real world applications in collaboration with INRIM

The team behind this work:

Mariella Minder

Marco Lucamarini

Mirko Sanzaro

Robert I. Woodward

Zhiliang Yuan

Andrew J. Shields

P.S.: we are hiring!

See:
https://www.toshiba.eu/pages/eu/Cambridge-Research-Laboratory/join-us

Thanks for your attention! Any questions?