Secure Quantum Key Distribution over 421 km of Optical Fibre

Alberto Boaron,[1] Gianluca Boso,[1] Davide Rusca,[1] Cédric Vulliez,[1] Claire Autebert,[1] Misael Caloz,[1] Matthieu Perrenoud, Gaëtan Gras,[1] Félix Bussières,[1] Ming-Jun Li,[2] Daniel Nolan,[2] Anthony Martin,[1] and Hugo Zbinden[1]

[1] **Group of Applied Physics**, University of Geneva, Switzerland
[2] **Corning Incorporated**, United States

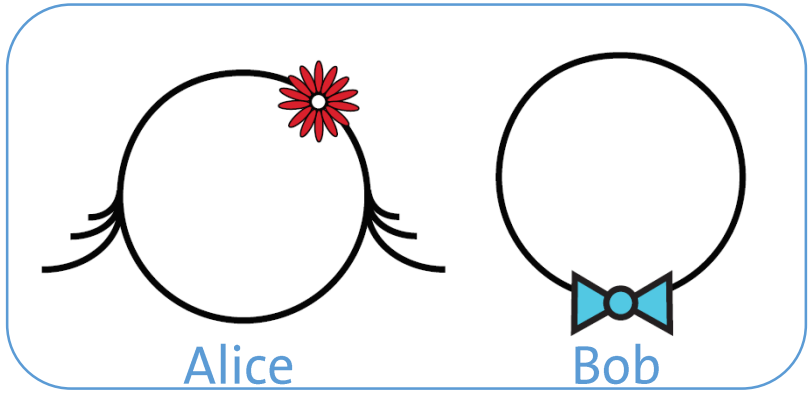
9th GDR IQFA | Montpellier | 15 november 2018

Phys. Rev. Lett. **121**, 190502 (2018)

UNIVERSITÉ DE GENÈVE

What is quantum key distribution ?

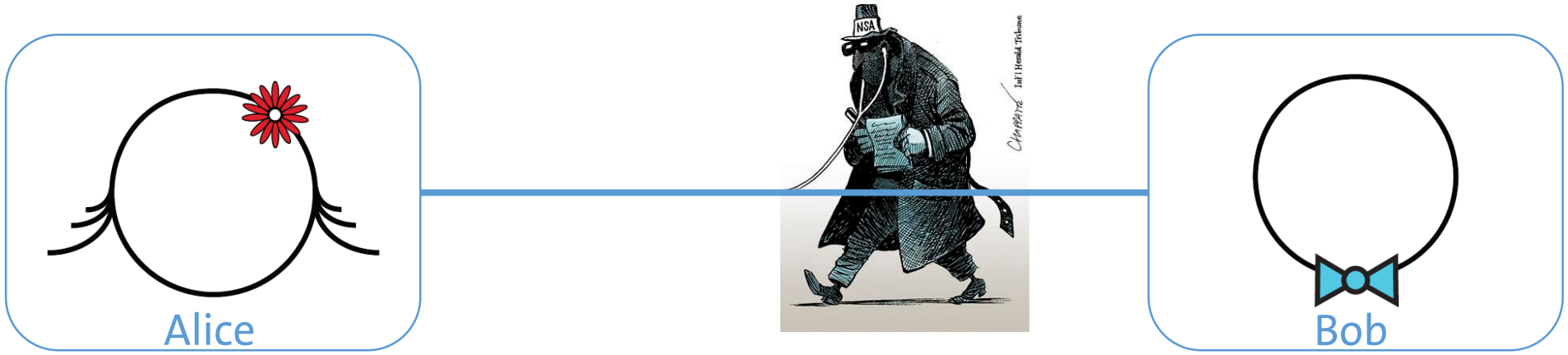
Sharing secrets



Secrets:

- Political, industrial, military
- Privacy, medical, opinions

Sharing secrets (at a distance)



Public-key cryptography is not safe against quantum computers

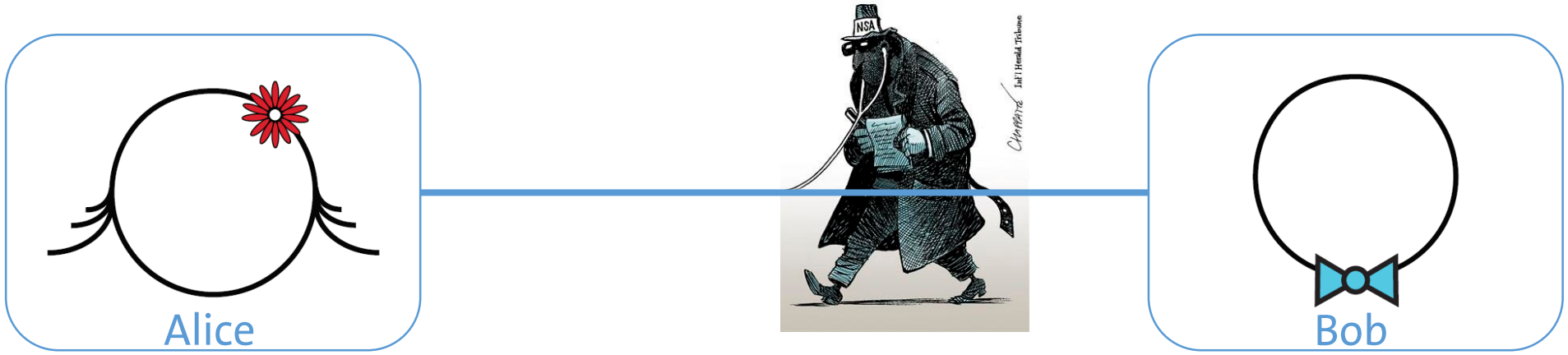
Solution: **symmetric-key cryptography**

One-time-pad

Message	111101111
Key	100000101 $\oplus$ (XOR)
Encrypted message	**011101010**

UNIVERSITÉ DE GENÈVE

Sharing secrets (at a distance)



Public-key cryptography is not safe against quantum computers

Solution: **symmetric-key cryptography**

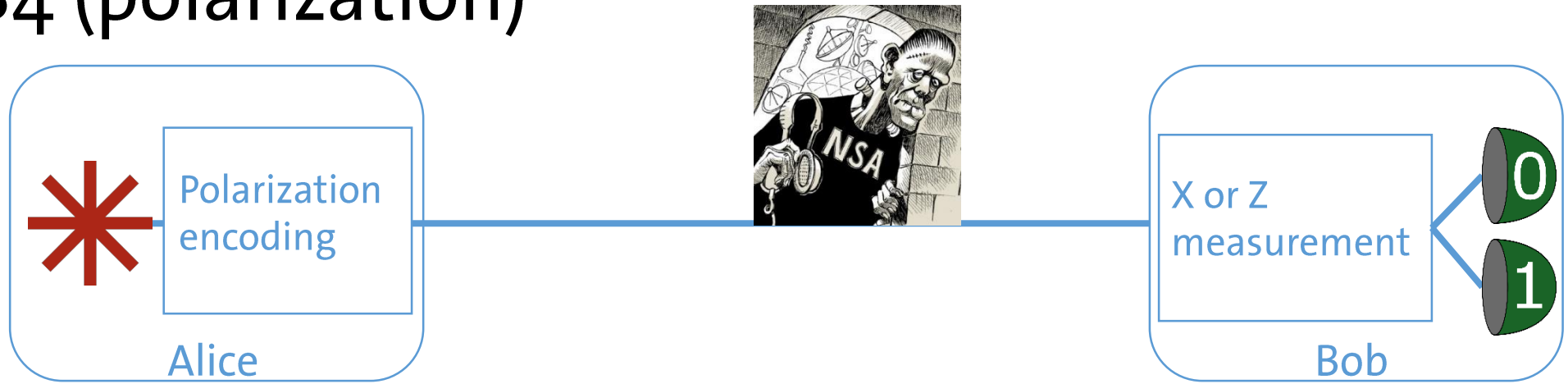
Challenge:
sharing secret key
between two remote users

One-time-pad

Message	111101111
Key	100000101 $\oplus$ (XOR)
Encrypted message	**011101010**

UNIVERSITÉ DE GENÈVE

BB84 (polarization)



Encoding

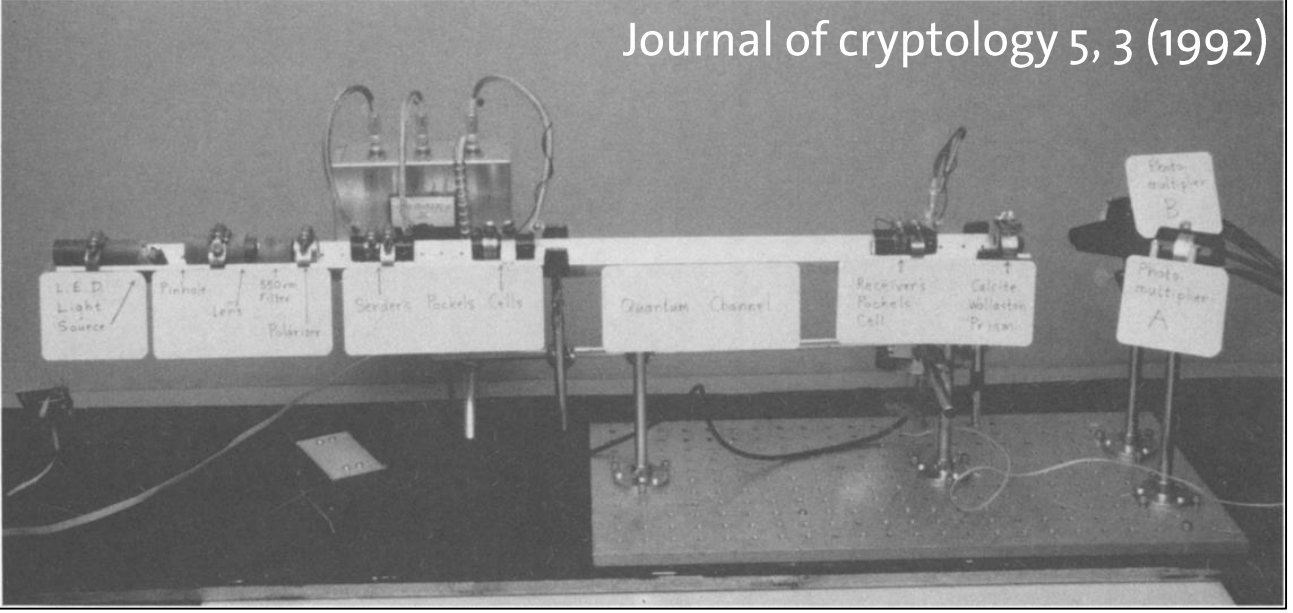
	pol	bit	basis
↔	H	0	Z
↕	V	1	Z
⤢	D	0	X
⤡	A	1	X

Measurement

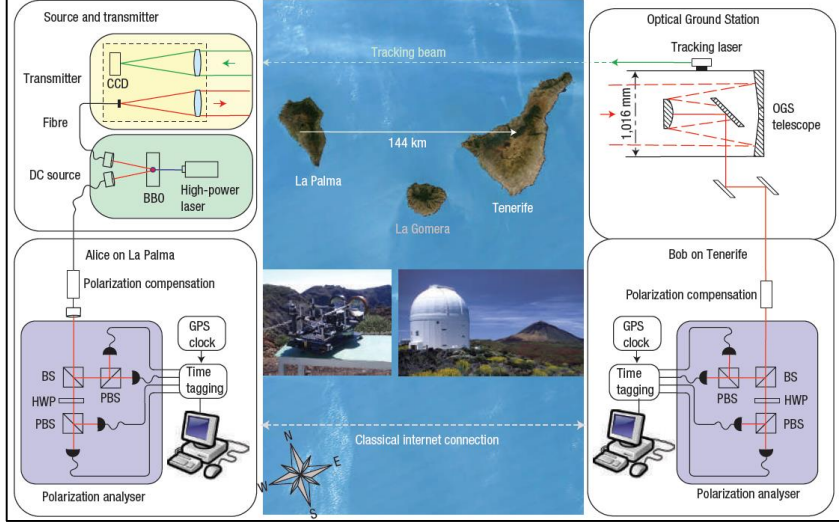
✢	H-V	Z
⤫	D-A	X

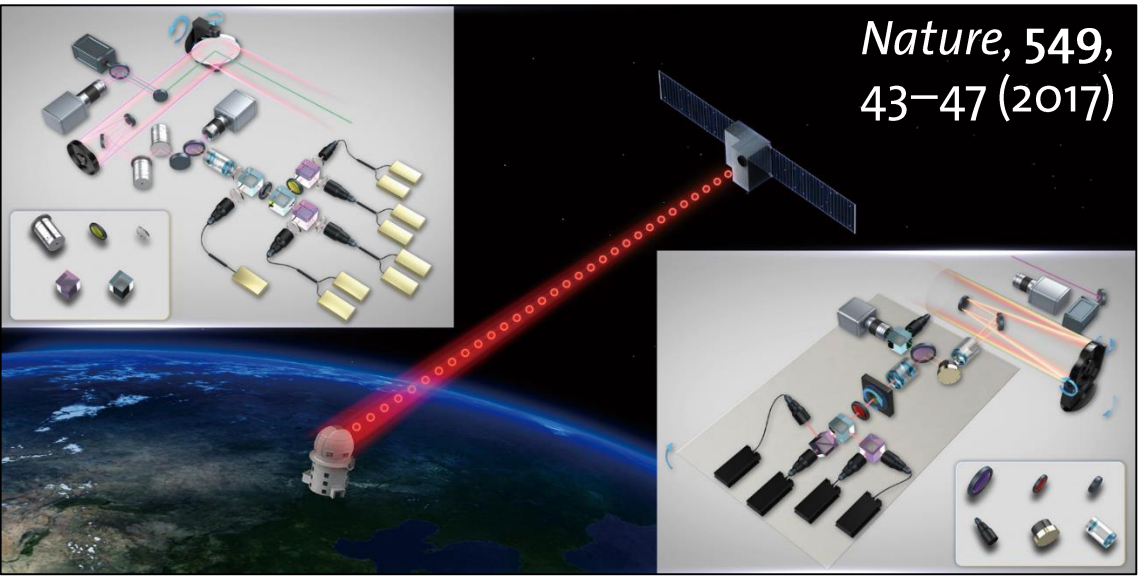
Quantum Bit Error Rate (QBER)
Secret key rate

UNIVERSITÉ DE GENÈVE



PRL 98, 010504 (2007)





nature photonics LETTERS
PUBLISHED ONLINE: 9 FEBRUARY 2015 | DOI: 10.1038/NPHOTON.2014.327

Provably secure and practical quantum key distribution over 307 km of optical fibre

Boris Korzh[1]*, Charles Ci Wen Lim[1]*, Raphael Houlmann[1], Nicolas Gisin[1], Ming Jun Li[2], Daniel Nolan[2], Bruno Sanguinetti[1], Rob Thew[1] and Hugo Zbinden[1]

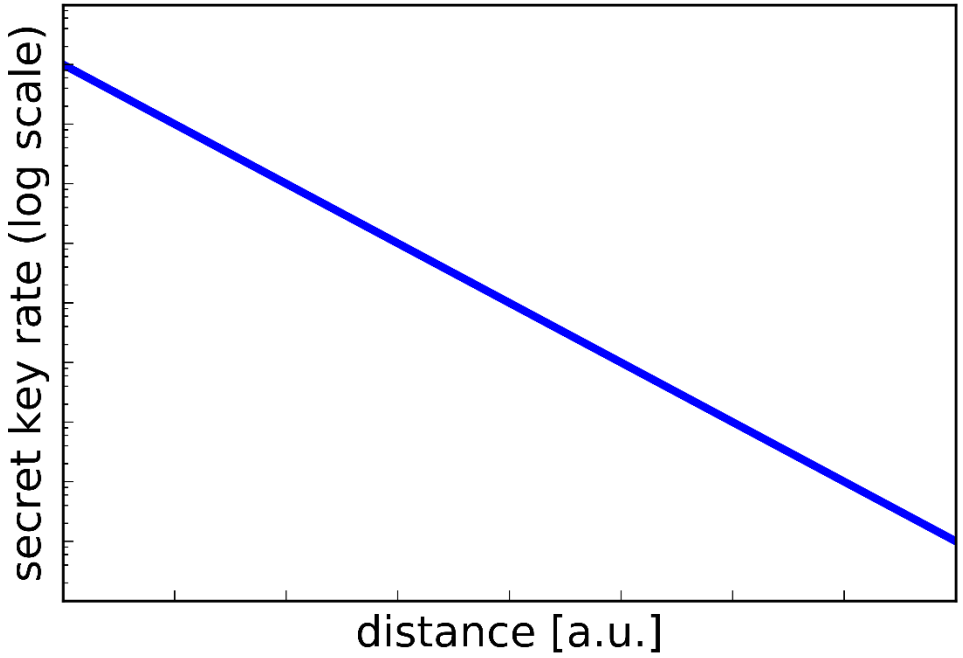
PRL **117**, 190501 (2016) PHYSICAL REVIEW LETTERS week ending 4 NOVEMBER 2016

Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber

Hua-Lei Yin,[1,2] Teng-Yun Chen,[1,2] Zong-Wen Yu,[3,4] Hui Liu,[1,2] Li-Xing You,[5] Yi-Heng Zhou,[2,3] Si-Jing Chen,[5] Yingqiu Mao,[1,2] Ming-Qi Huang,[1,2] Wei-Jun Zhang,[5] Hao Chen,[6] Ming Jun Li,[6] Daniel Nolan,[6] Fei Zhou,[7] Xiao Jiang,[1,2] Zhen Wang,[5] Qiang Zhang,[1,2,7,*] Xiang-Bin Wang,[2,3,7,†] and Jian-Wei Pan[1,2,‡]

What does limit the transmission distance ?

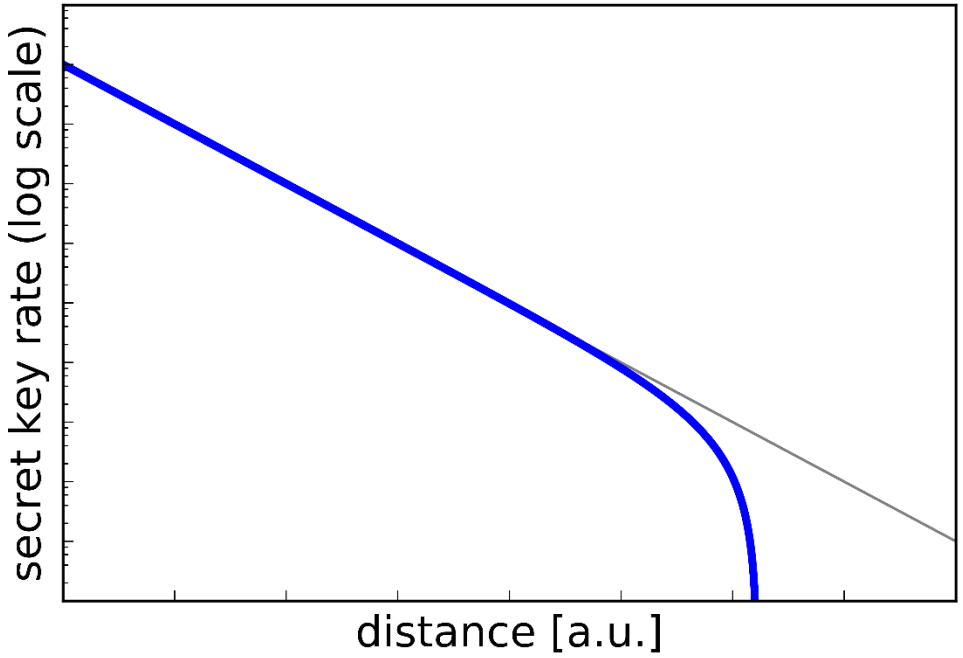
- Fiber attenuation (0.2 dB/km for standard single-mode fibre)



UNIVERSITÉ DE GENÈVE

What does limit the transmission distance ?

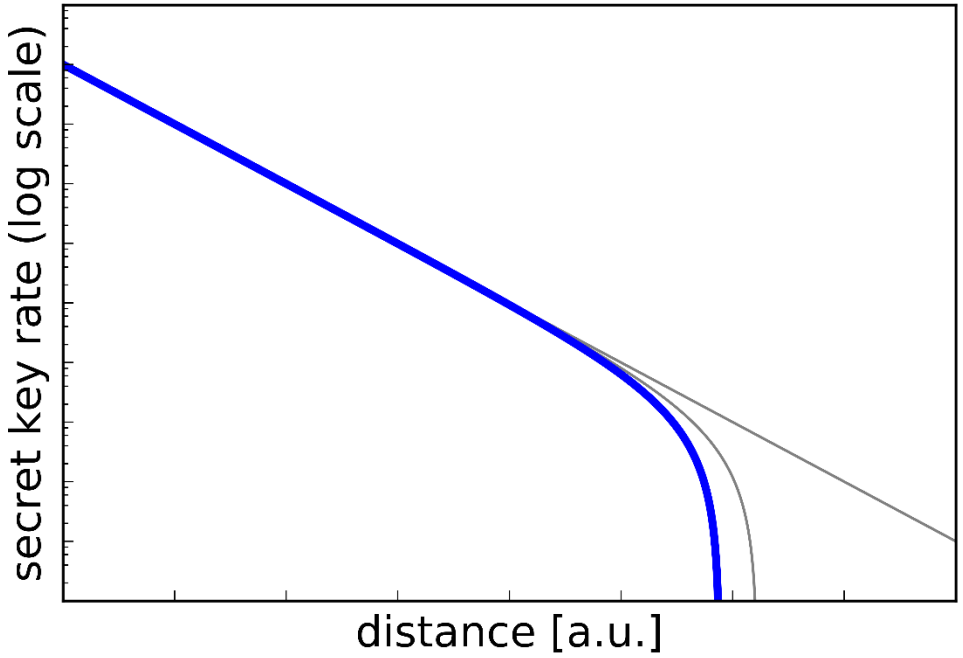
- Fiber attenuation (0.2 dB/km for standard single-mode fibre)
- Dark count rate of the detectors



UNIVERSITÉ DE GENÈVE

What does limit the transmission distance ?

- Fiber attenuation (0.2 dB/km for standard single-mode fibre)
- Dark count rate of the detectors
- Finite-size effects (acquisition time)



UNIVERSITÉ DE GENÈVE

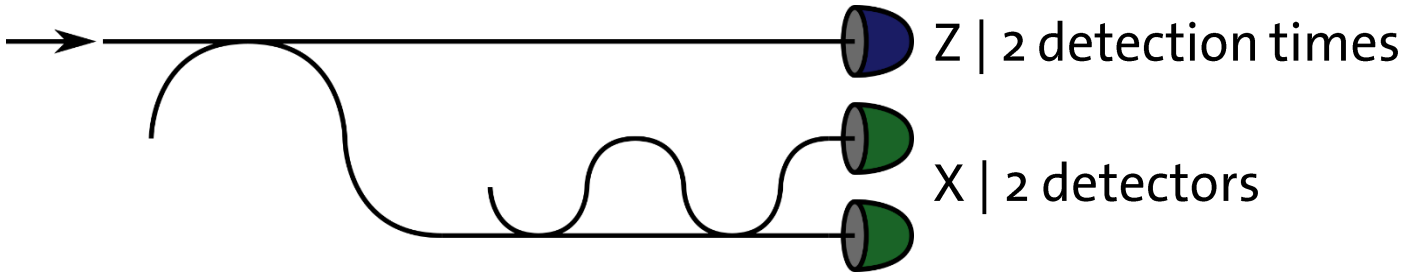
Implementing a quantum key distribution system

Time-bin encoding

Alice's state preparation

Z, 0	$\lvert 0\rangle$	
Z, 1	$\lvert 1\rangle$	
X, 0	$\lvert +\rangle$	0
X, 1	$\lvert -\rangle$	π

Bob's detection apparatus



Protocol

- Time-bin encoding
- Decoy-state method

basis, bit	state	μ_1	μ_2	μ_3
Z, 0	$\|0\rangle$			
Z, 1	$\|1\rangle$			
X, 0	$\|+\rangle$			
X, 1	$\|-\rangle$			

Protocol

- Time-bin encoding
- Decoy-state method

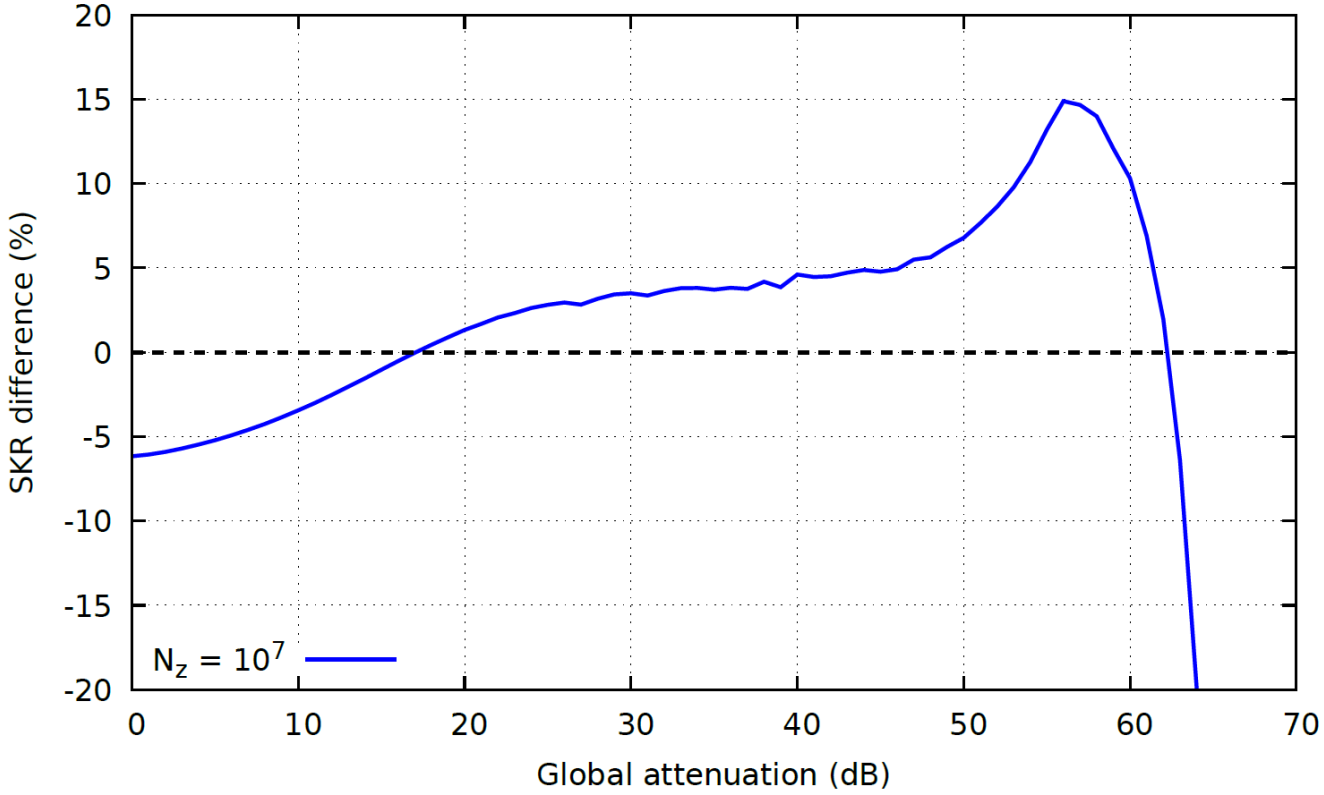
basis, bit	state	μ_1	μ_2	μ_3
Z, 0	$\|0\rangle$			
Z, 1	$\|1\rangle$			
X, 0	$\|+\rangle$			
X, 1	$\|-\rangle$			

Phys. Rev. A72, 012326 (2005)

UNIVERSITÉ DE GENÈVE

1-decoy versus 2-decoy

1-decoy (i.e. two levels in total) is more efficient for most experimental settings !



D. Rusca et al., *The 1-decoy state protocol: the best choice for practical QKD*, Appl. Phys. Lett. 112, 171104 (2018)

UNIVERSITÉ DE GENÈVE

Protocol

- Time-bin encoding
- Decoy-state method

basis, bit	state	μ_1	μ_2	μ_3
Z, 0	$\|0\rangle$			
Z, 1	$\|1\rangle$			
X, 0	$\|+\rangle$			
X, 1	$\|-\rangle$			

Protocol

- Time-bin encoding
- Decoy-state method

basis, bit	state	μ_1	μ_2	μ_3
Z, 0	$\|0\rangle$			
Z, 1	$\|1\rangle$			
X, 0	$\|+\rangle$			
X, 1	$\|-\rangle$			

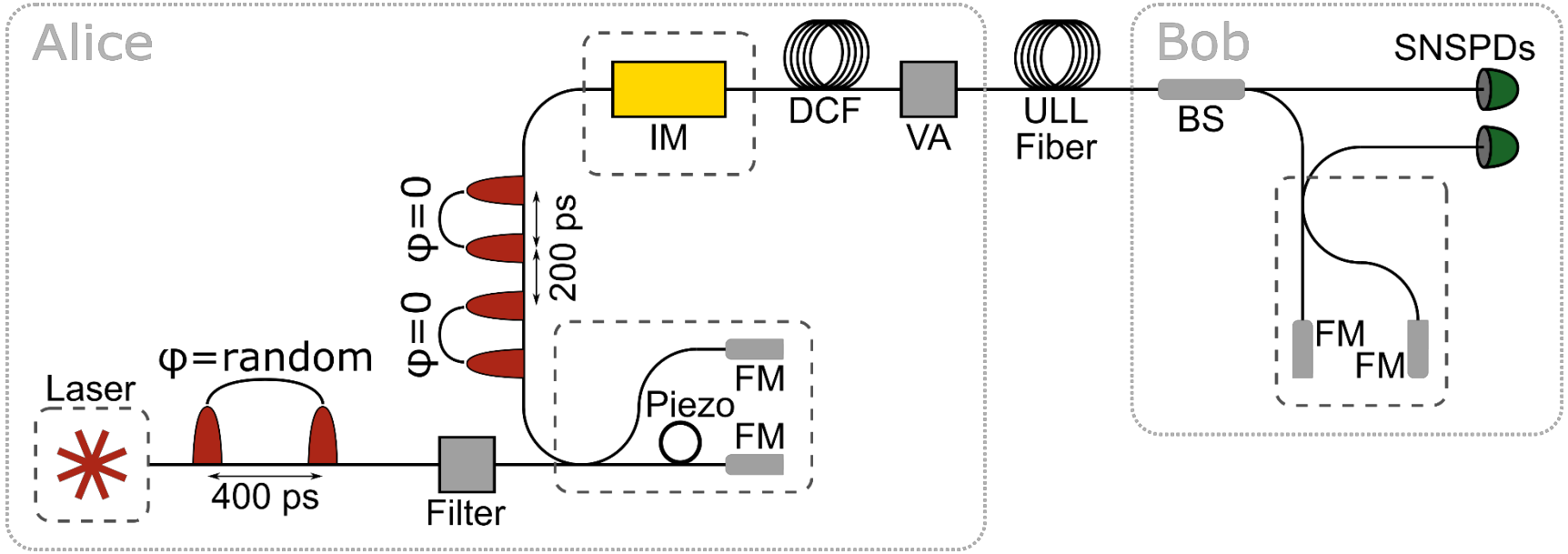
Phys. Rev. A 74, 042342 (2006)

UNIVERSITÉ DE GENÈVE

Protocol

- Time-bin encoding
- Decoy-state method

basis, bit	state	μ_1	μ_2	μ_3
Z, 0	$\|0\rangle$			
Z, 1	$\|1\rangle$			
X, 0	$\|+\rangle$			
X, 1	$\|-\rangle$			

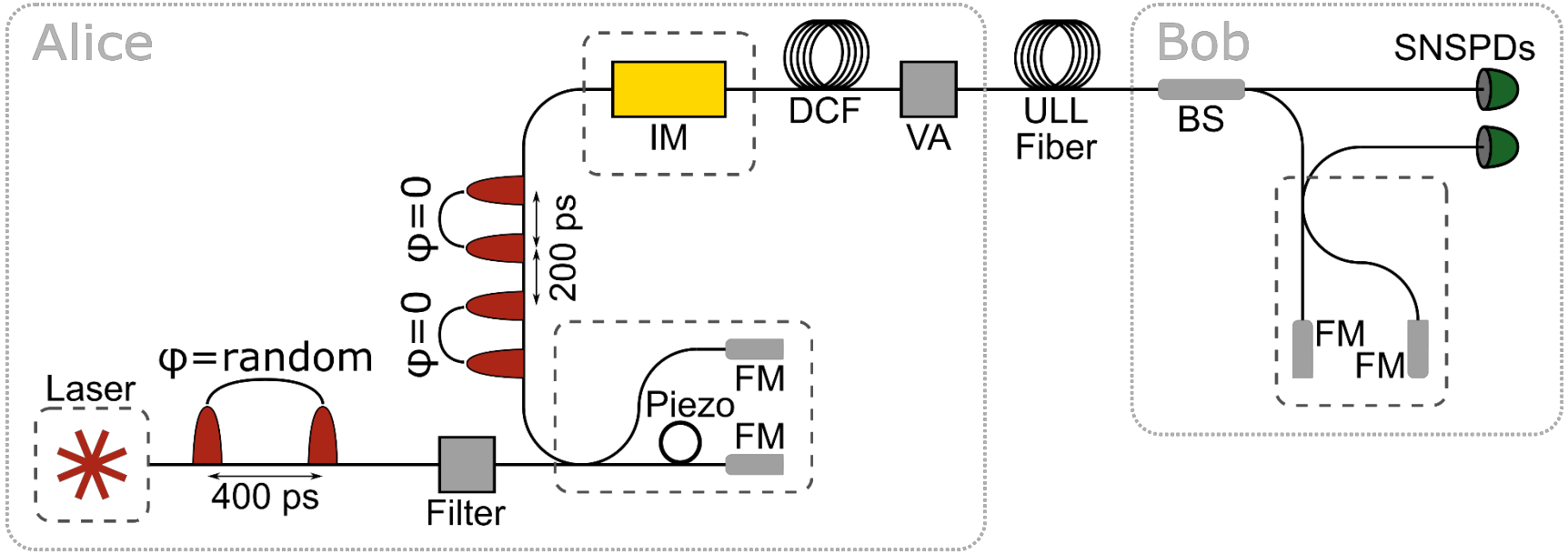


UNIVERSITÉ DE GENÈVE

Protocol

- Time-bin encoding
- Decoy-state method

basis, bit	state	μ_1	μ_2	μ_3
Z, 0	$\|0\rangle$			
Z, 1	$\|1\rangle$			
X, 0	$\|+\rangle$			
X, 1	$\|-\rangle$			



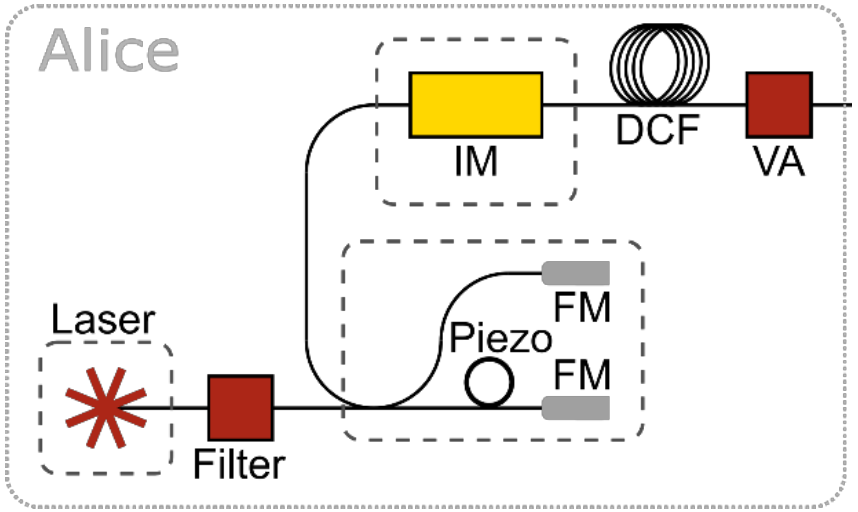
4 states, 4 outcomes
↓
3 states, 3 outcomes

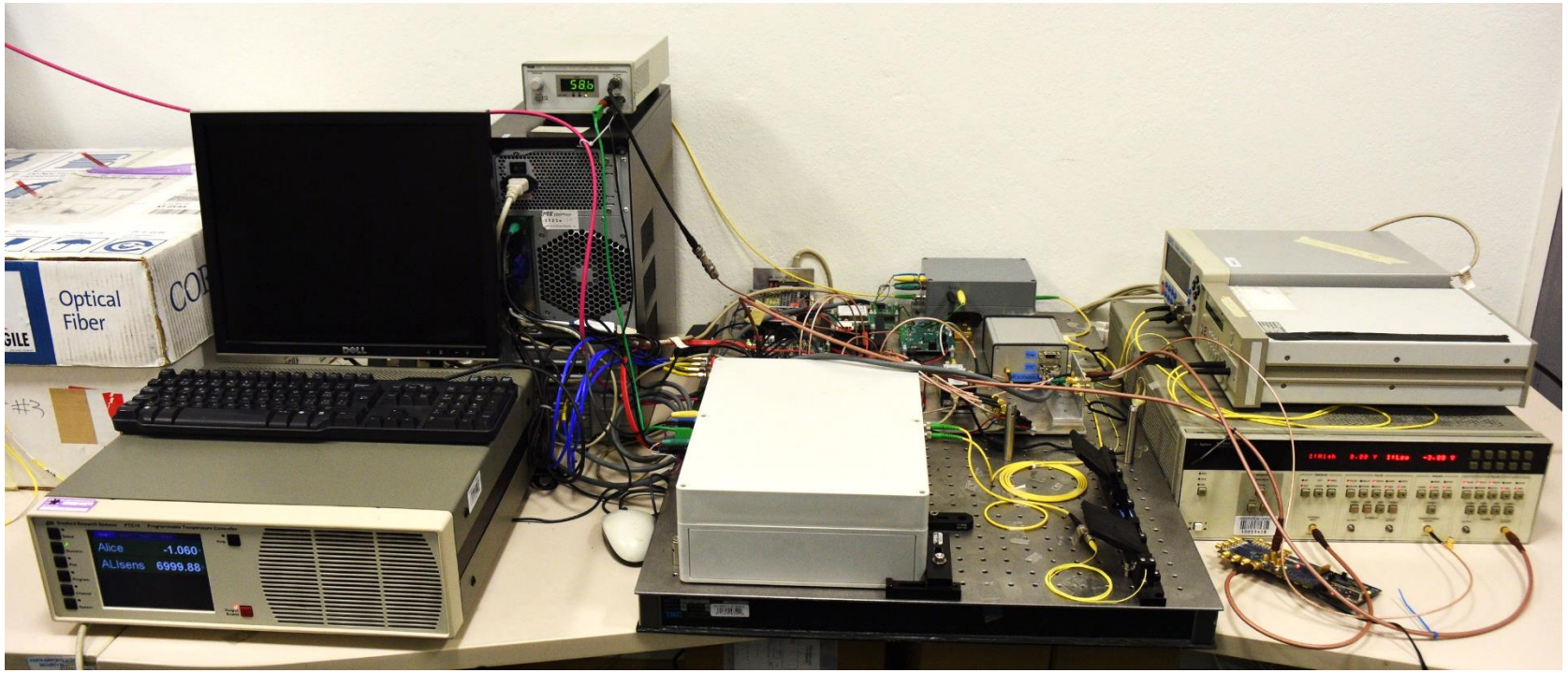
Security proof available on the ArXiv | 1808.08259 (to appear in Phys. Rev. A)

UNIVERSITÉ DE GENÈVE

1. all fibred high repetition rate source

- Phase-randomized DFB laser:
  - Repetition rate: 2.5 GHz
  - Pulse duration: 30 ps
- High-speed integrated intensity modulator: 5 GHz





→ requires dispersion compensation fibre: -140 ps/nm/km

(standard single-mode fibre dispersion: 17 ps/nm/km)

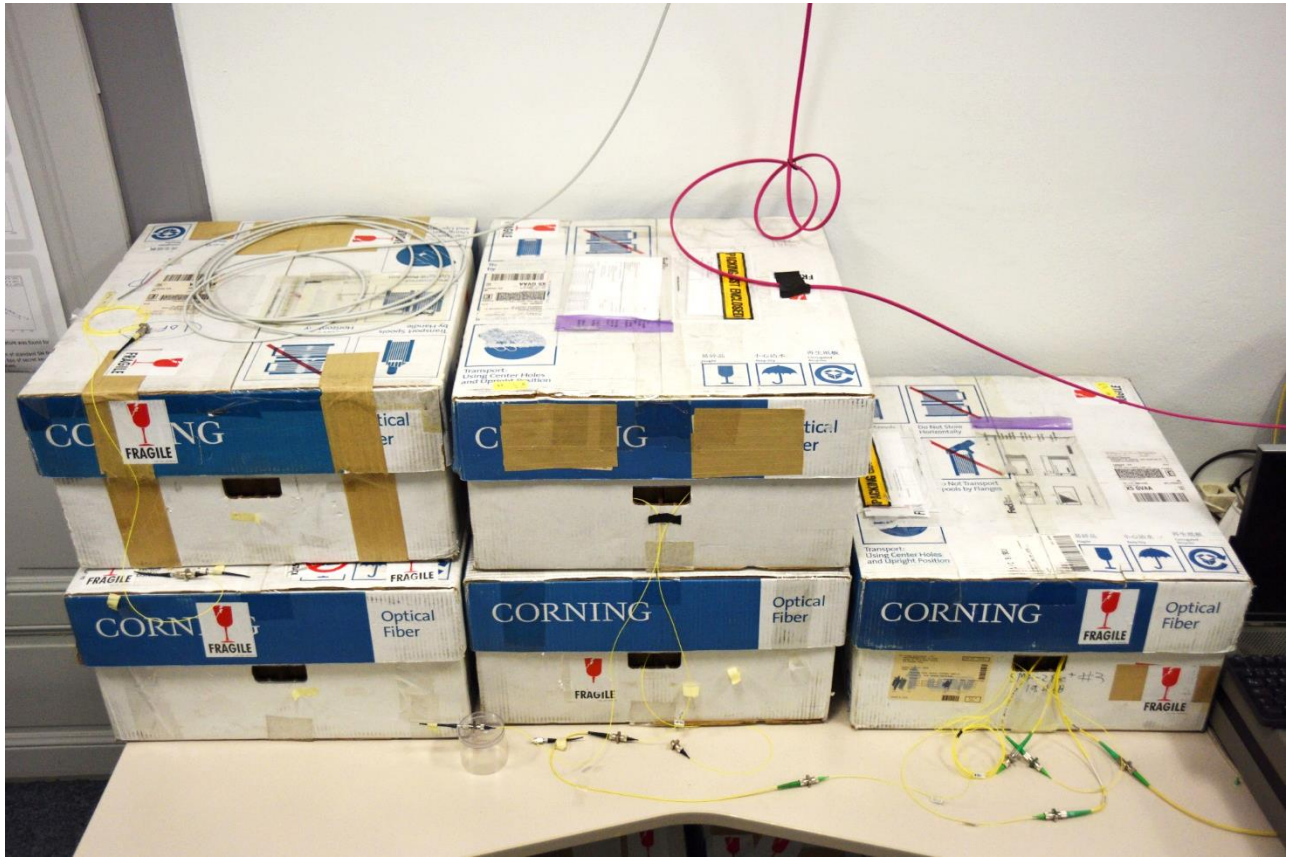
CORNING

UNIVERSITÉ DE GENÈVE

2. quantum channel: ultra low-loss fibres

Corning ULL-28® ultralow-loss fibre: 0.16 dB/km

Attenuation including connectors and splices: 0.17 dB/km



UNIVERSITÉ DE GENÈVE

3. detectors

Superconducting nanowire single-photon detectors

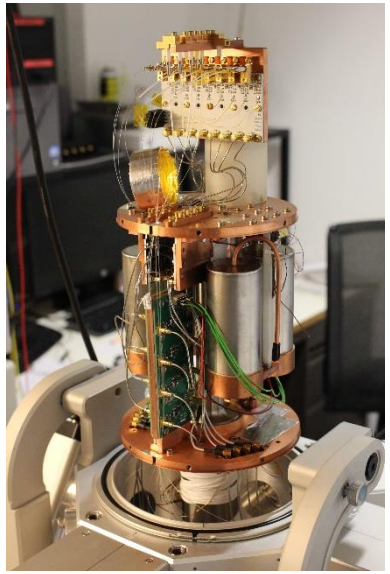
Amorphous molybdenum silicide

Temperature: 0.8 K

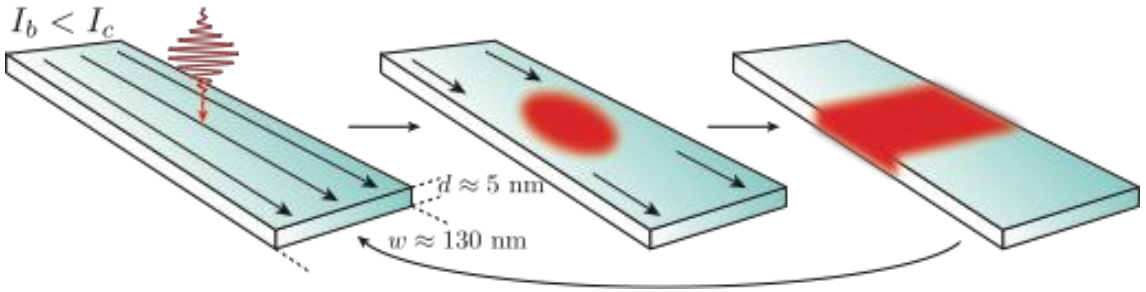
Dark counts: < 0.3 count/s

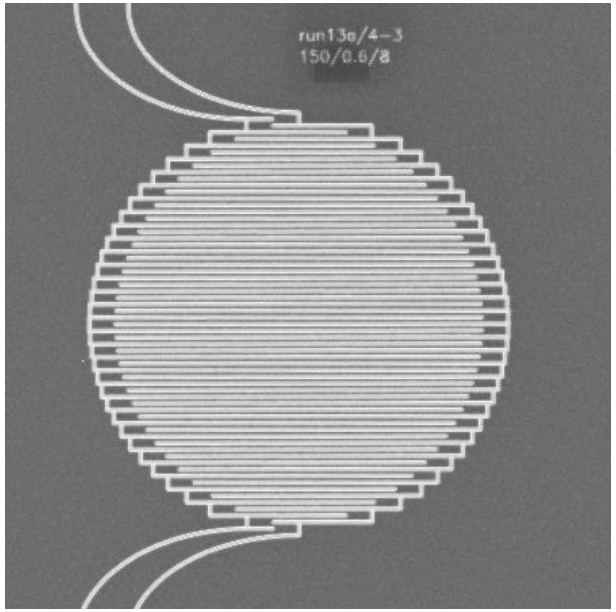
Efficiency: 50% (at low dark counts rates)

Timing jitter: 30 ps



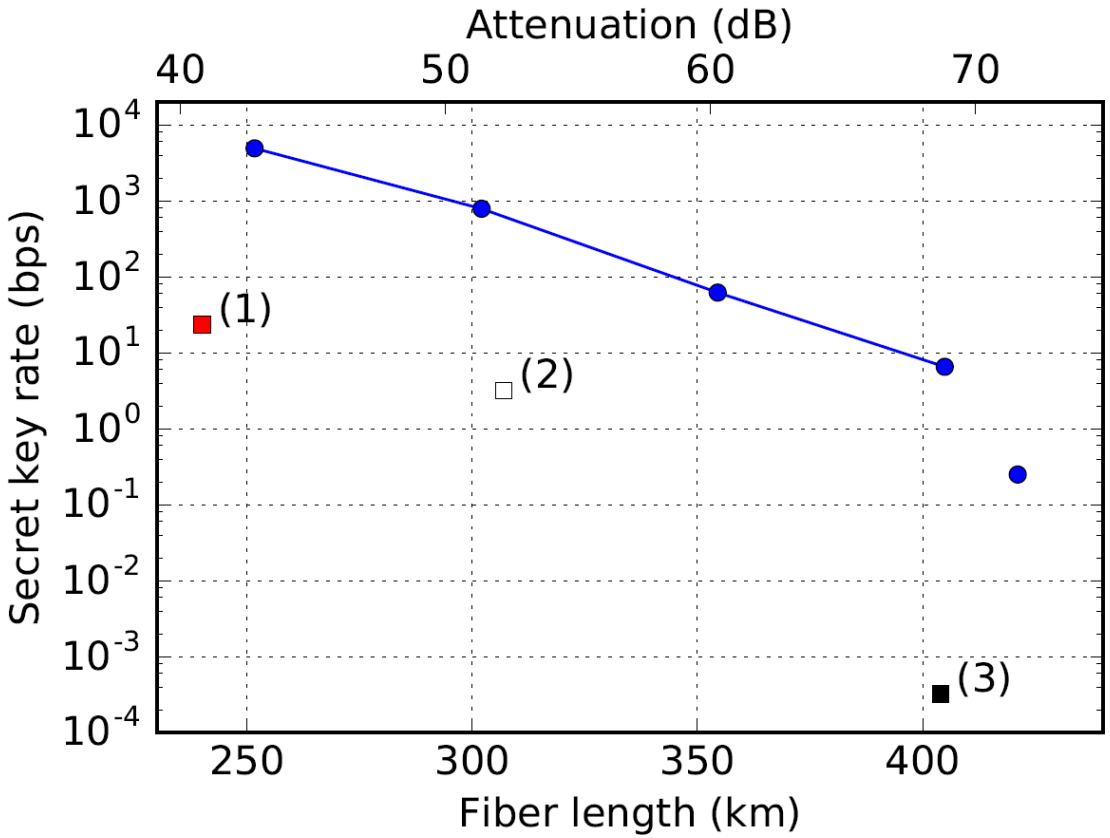
Appl. Phys. Lett. **112**, 061103 (2018)





UNIVERSITÉ DE GENÈVE

Secret key rate vs distance



421 km | 71.9 dB

24.2 h overall acquisition time

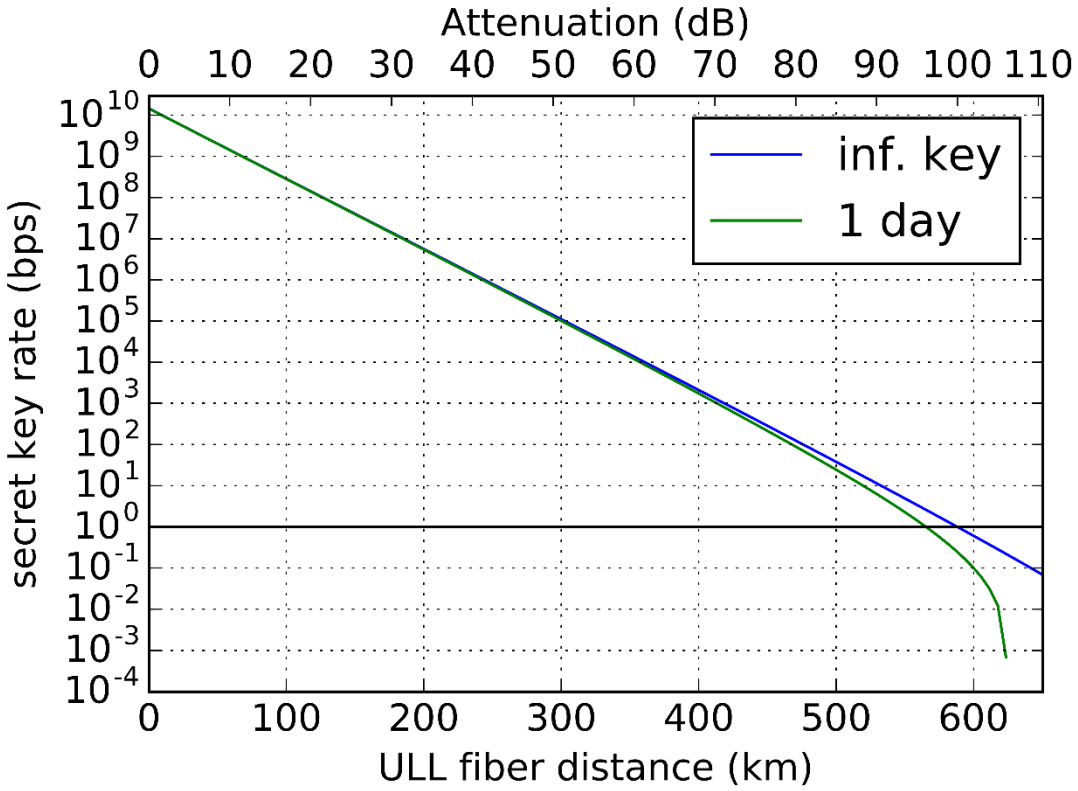
12.7 h of data used

length (km)	attn (dB)	μ_1	μ_2	block size	block time (h)	QBER Z (%)	ϕ_Z (%)	RKR (bps)	SKR (bps)
251.7	42.7	0.49	0.18	$8.2 \cdot 10^6$	0.20	0.5	2.2	$12 \cdot 10^3$	$4.9 \cdot 10^3$
302.1	51.3	0.48	0.18	$8.2 \cdot 10^6$	1.17	0.4	3.7	$1.9 \cdot 10^3$	$0.79 \cdot 10^3$
354.5	60.6	0.35	0.15	$6.2 \cdot 10^6$	14.8	0.7	1.8	117	62
404.9	69.3	0.35	0.15	$4.1 \cdot 10^5$	6.67	1.0	4.3	17	6.5
421.1	71.9	0.30	0.13	$2.0 \cdot 10^5$	24.2 (12.7*)	2.1	12.8	2.3 (4.5*)	0.25 (0.49*)

UNIVERSITÉ DE GENÈVE

Ultimate limit

- BB84 with decoy state
- 40 GHz repetition rate
- 0 Hz dark counts
- 100% detection efficiency
- 1 day acquisition time



UNIVERSITÉ DE GENÈVE

Conclusion

A simplified BB84 protocol

A system mainly based on of-the-shelf components

- A QKD transmitter based on commercially available components combined with some in-house-made electronics
- Commercially available ultra low-loss fibres
- In-house-made SNSPDs (but almost commercially available)

Transmission of secret keys over 421 km of optical fibre

Thank you for you attention !

Quantum technologies group | leader: Hugo Zbinden

UNIVERSITÉ DE GENÈVE