Long distance and high rate quantum key distribution.

Hugo Zbinden

GAP – Quantum Technologies

UNIVERSITÉ DE GENÈVE

Is the quantum computer a threat for information security?

IBM, 20 qubits

Classical Cryptography

A) Based on Complexity

DES, AES (secret key)

RSA (public key)

Security unproven

One-way functions
Integer factorisation

$$107 \times 53 = x$$
$$5671 = y \times z$$

B) Based on Information Theory

one time pad (Vernam)

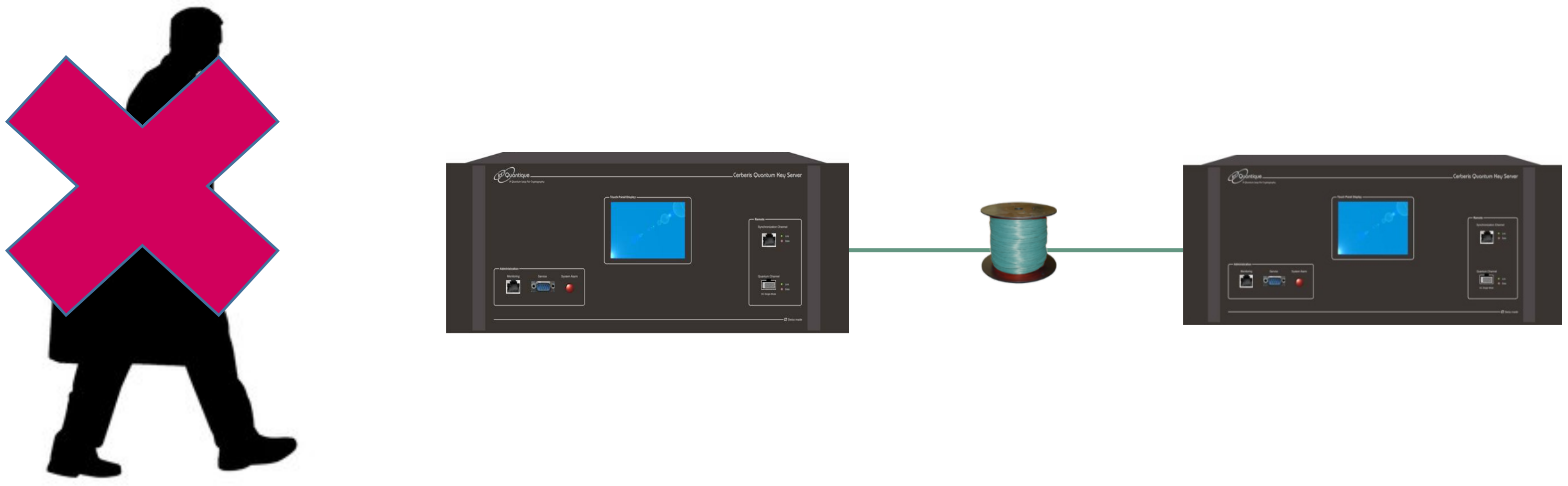
plaintext :	00101001001001110101000110100 1
key:	+10101101101100101010011101010 1
cyphertext:	10000100100101011111011011110 0

security proven

problem: key distribution

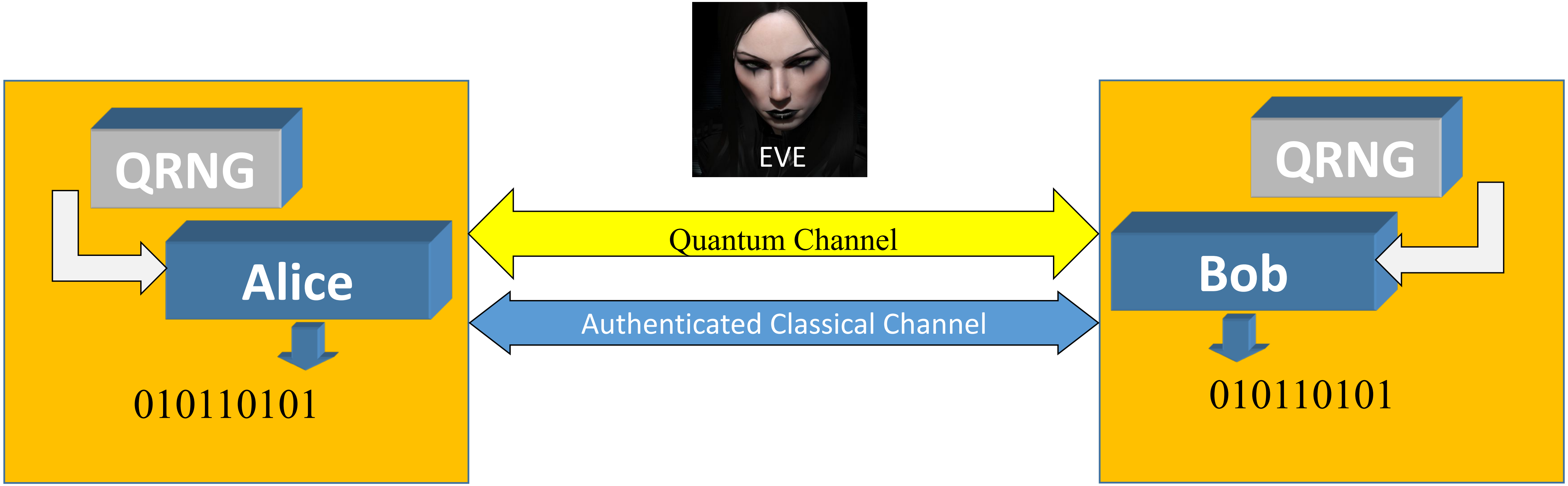
Quantum Key Distribution

- Quantum Crpytography is not a new coding method
- Send key with individual photons (quantum states)
- The eavesdropper may not measure without perturbation (Heisenbergs uncertainty principle)
- Eavesdropping can be detected by Alice and Bob!



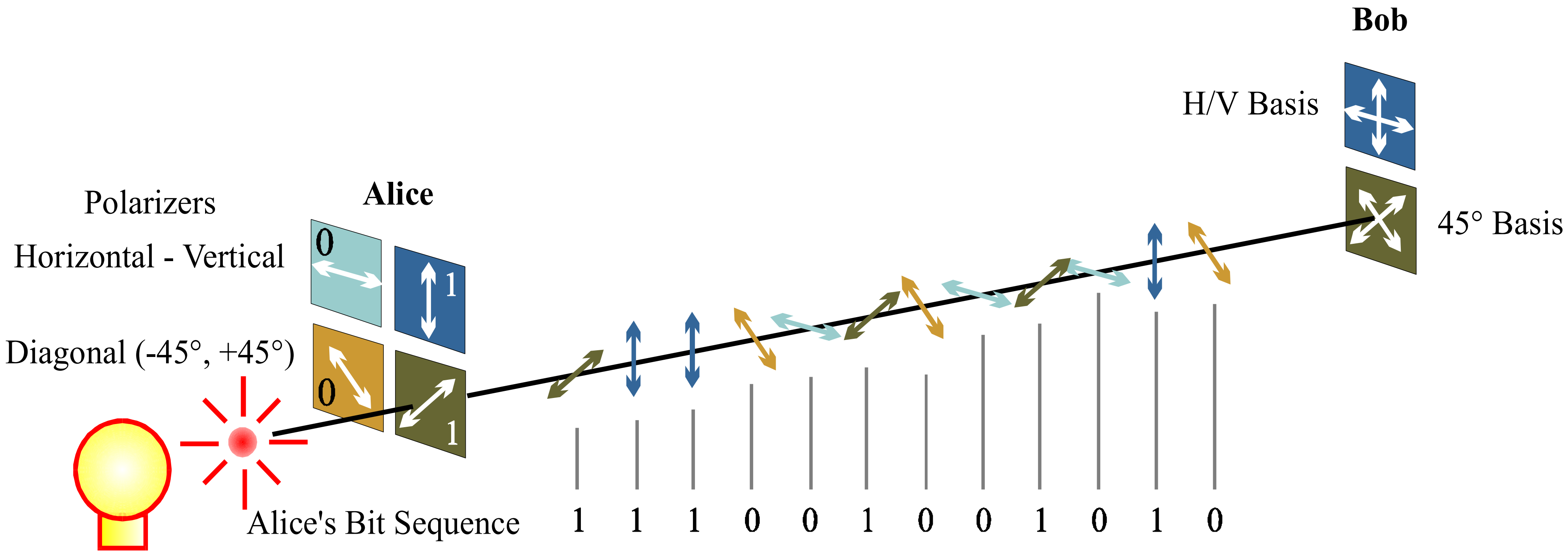
QKD is proven information theoretically secure!

Quantum Key Distribution



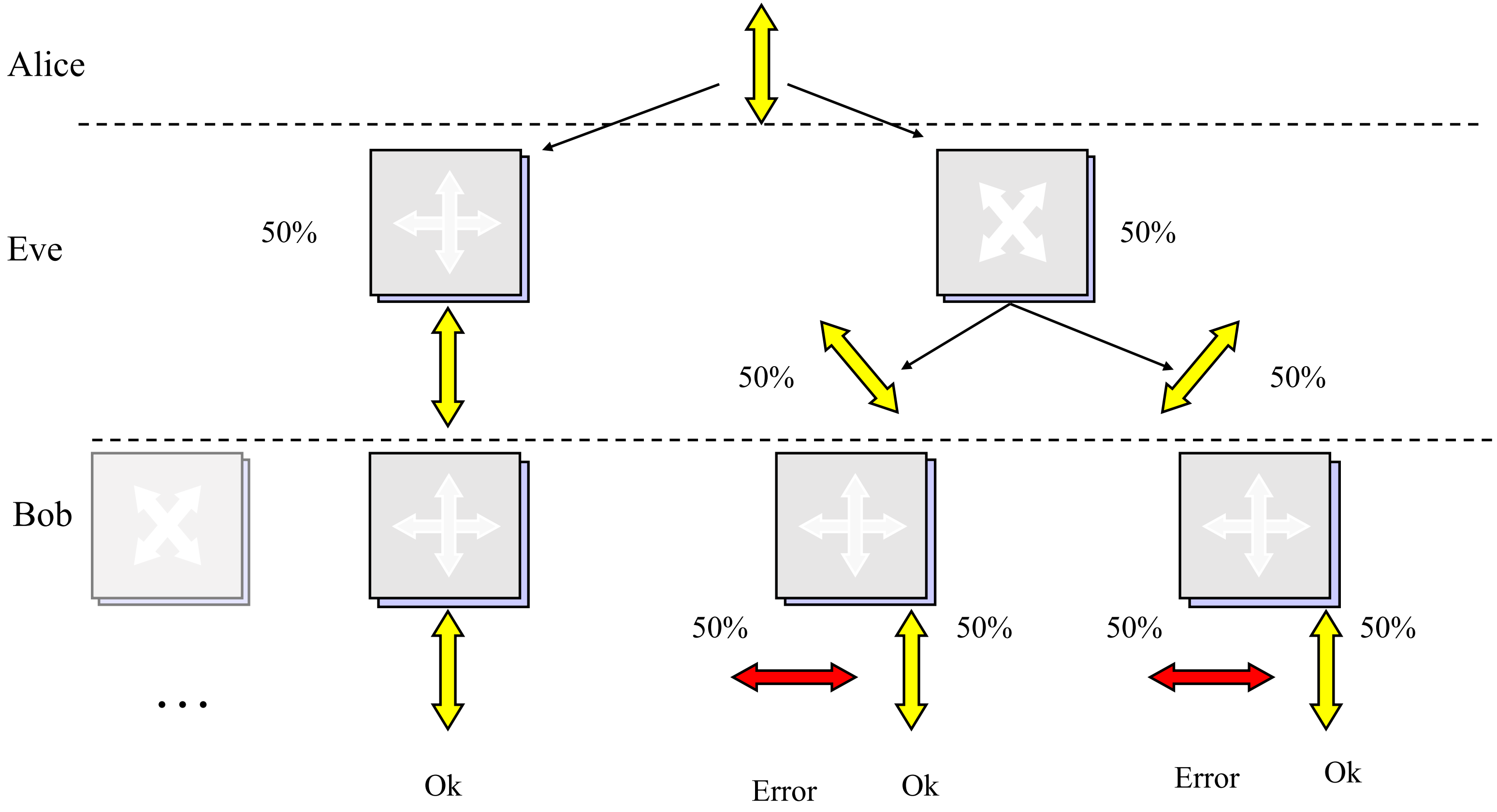
Assumption: secure perimeters for Alice and Bob

BB84 protocol (Bennett, Brassard, 1984)



Alice's Bit Sequence	1	1	1	0	0	1	0	0	1	0	1	0
Bob's Bases	+	+	×	×	+	×	+	×	×	+	+	×
Bob's Results	0	1	0	-	0	1	1	1	1	-	1	0
Key	-	1	-	-	0	1	-	-	1	-	1	0

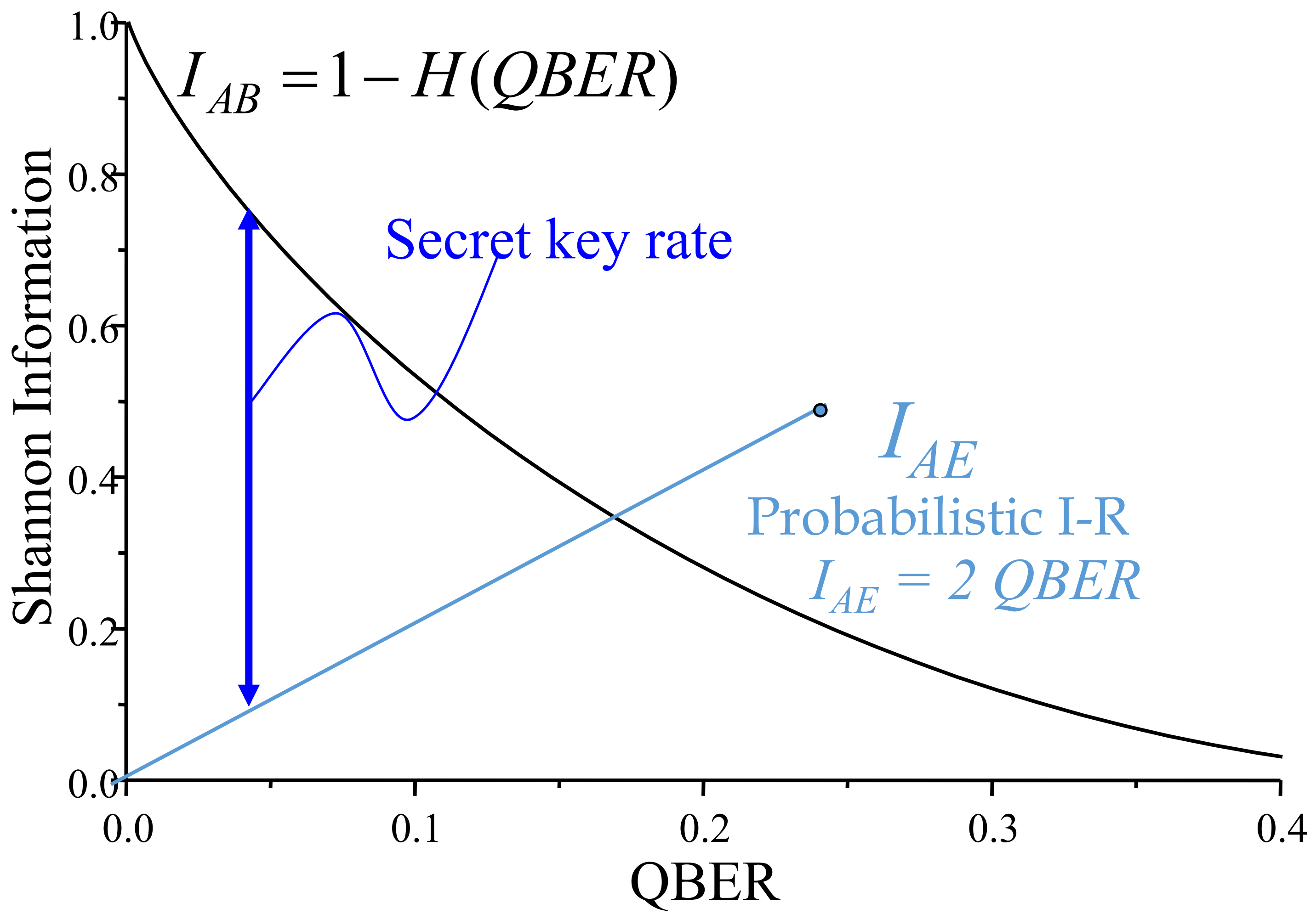
Eavesdropping (intercept-resend)



Error with 25 % probability

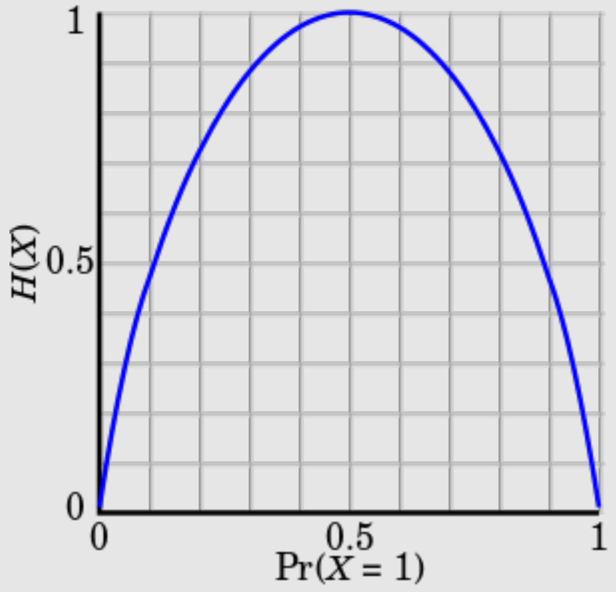
$$I_{AE} = 2\ QBER\ \ (quantum\ bit\ error\ rate)$$

Eve attacks: information curves

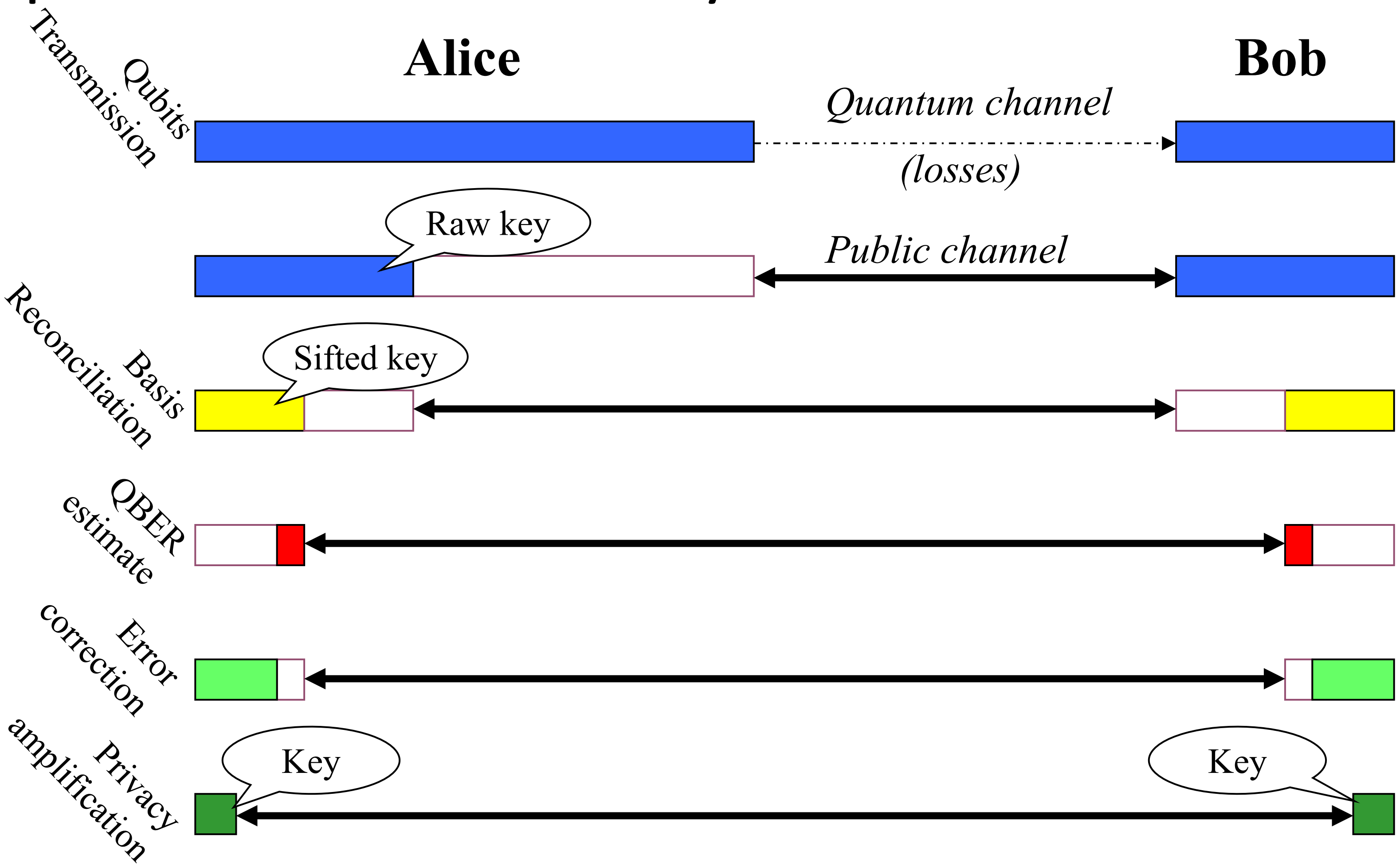


Binary Entropy function

$$H_b(p) = -p \log_2 p - (1-p)\log_2(1-p).$$

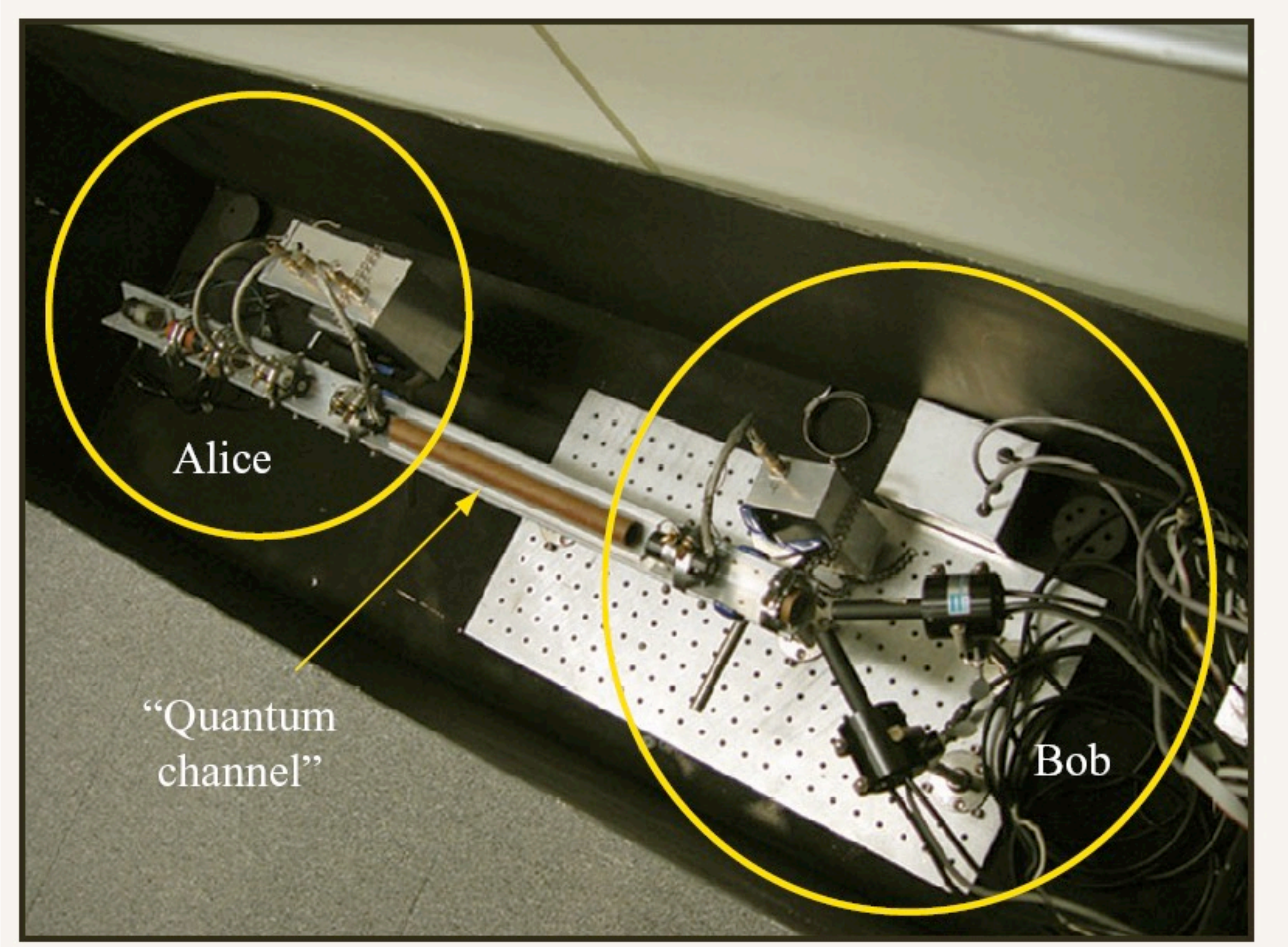


The steps to a secret key



+ Authentication!!!

Smolin and Bennett
IBM 1989



Swiss QCRYPT project (2013)

PHYSICAL REVIEW LETTERS 121, 190502 (2018)

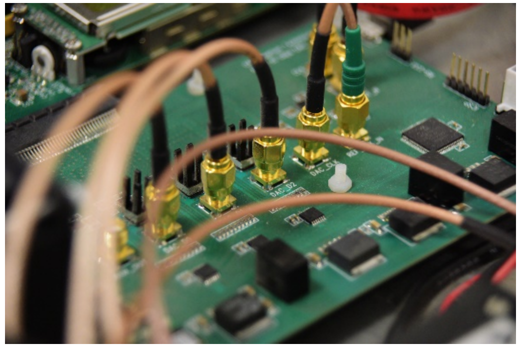
Editors' Suggestion | Featured in Physics

Secure Quantum Key Distribution over 421 km of Optical Fiber

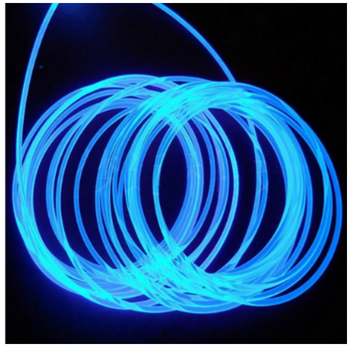
Alberto Boaron,[1,*] Gianluca Boso,[1] Davide Rusca,[1] Cédric Vulliez,[1] Claire Autebert,[1] Misael Caloz,[1] Matthieu Perrenoud,[1] Gaëtan Gras,[1,2] Félix Bussières,[1] Ming-Jun Li,[3] Daniel Nolan,[3] Anthony Martin,[1] and Hugo Zbinden[1]
[1]*Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, 1211 Geneva 4, Switzerland*
[2]*ID Quantique SA, Chemin de la Marbrerie 3, 1227 Carouge, Switzerland*
[3]*Corning Incorporated, Corning, New York 14831, USA*

(Received 10 July 2018; published 5 November 2018)

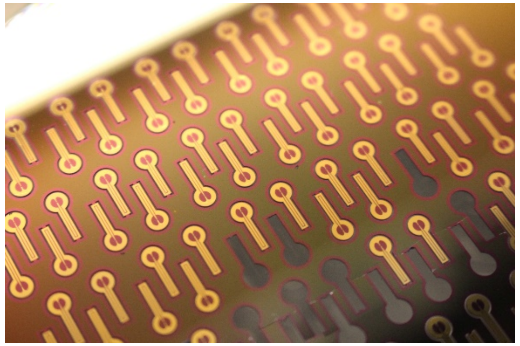
New simple and efficient QKD protocol



2.5 GHz repetition rate transmitter



Ultralow-loss fibers

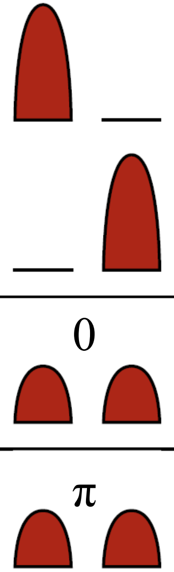


Supeconducting detectors developed in Geneva

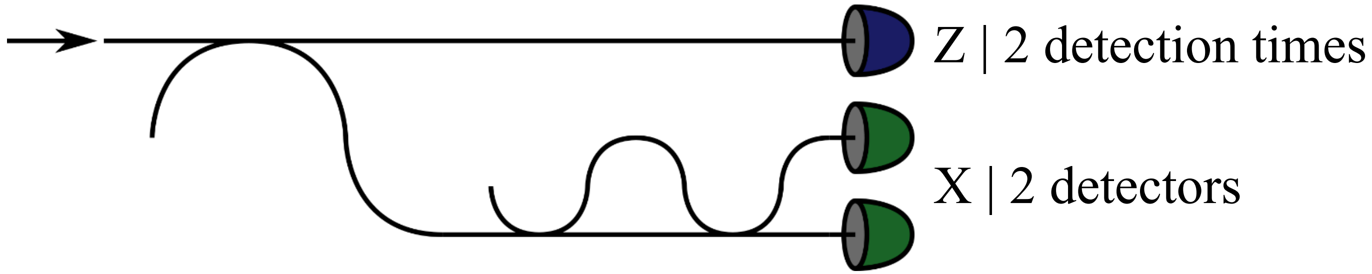
Time-bin encoding BB84

Alice's state preparation

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

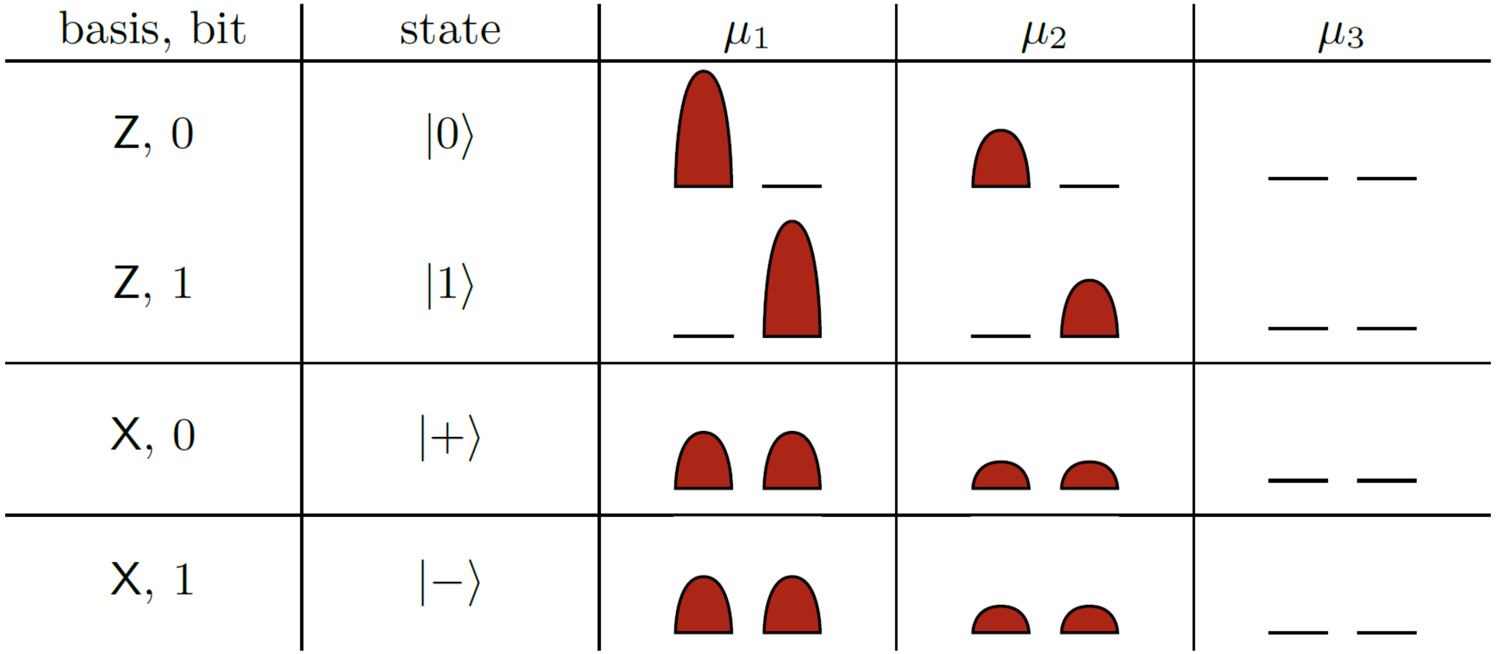


Bob's detection apparatus



a) Protocol

- Time-bin encoding
- Decoy-state method

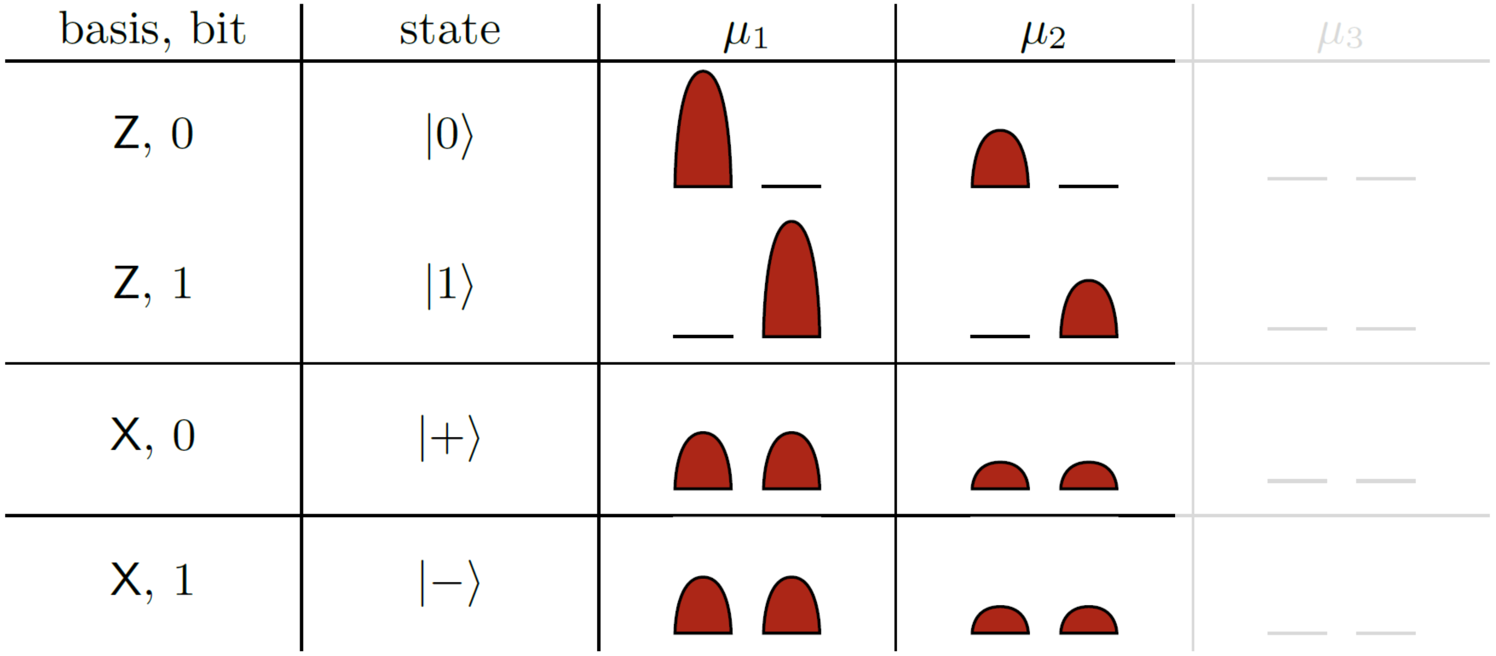


Phys. Rev. A72, 012326 (2005)

UNIVERSITÉ DE GENÈVE

a) Protocol

- Time-bin encoding
- Decoy-state method



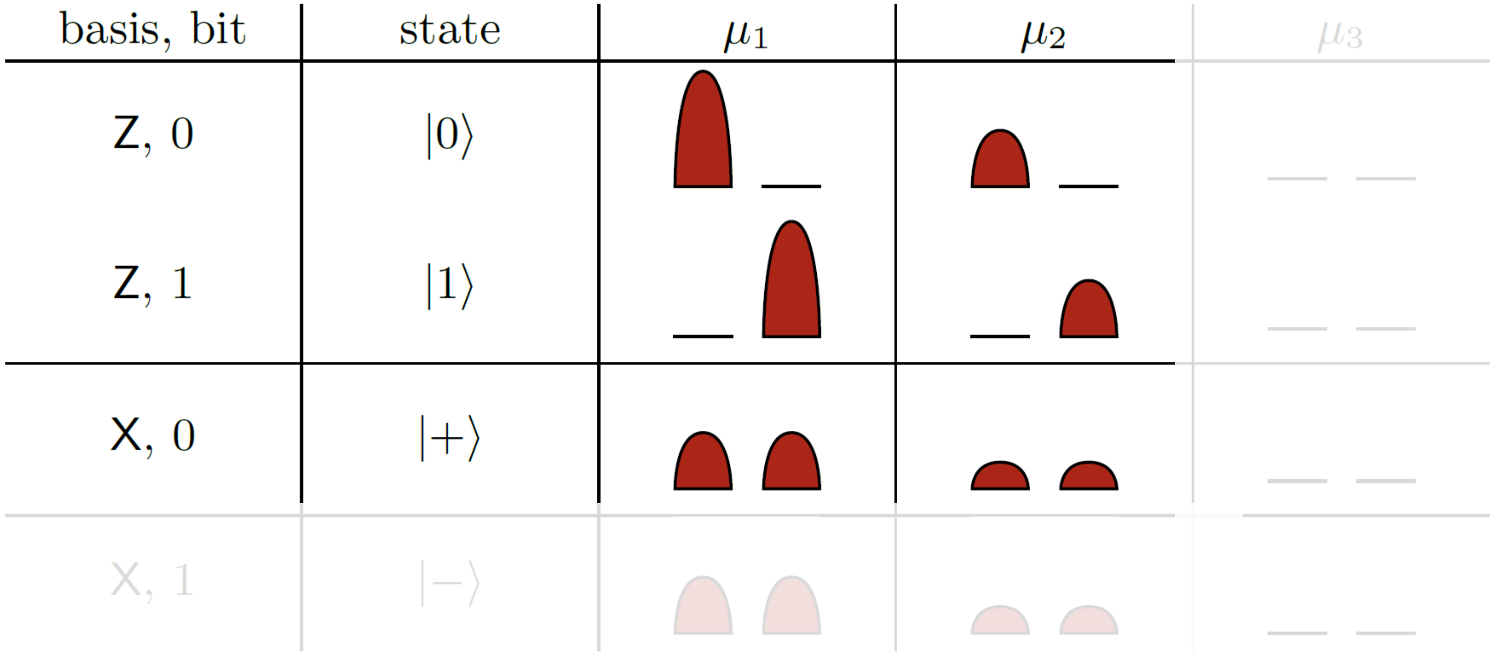
Finite key analysis:
For limited block size, using only two different average energies is advantageous!

$\varepsilon = 10^{-9}$

UNIVERSITÉ DE GENÈVE

a) Protocol

- Time-bin encoding
- Decoy-state method



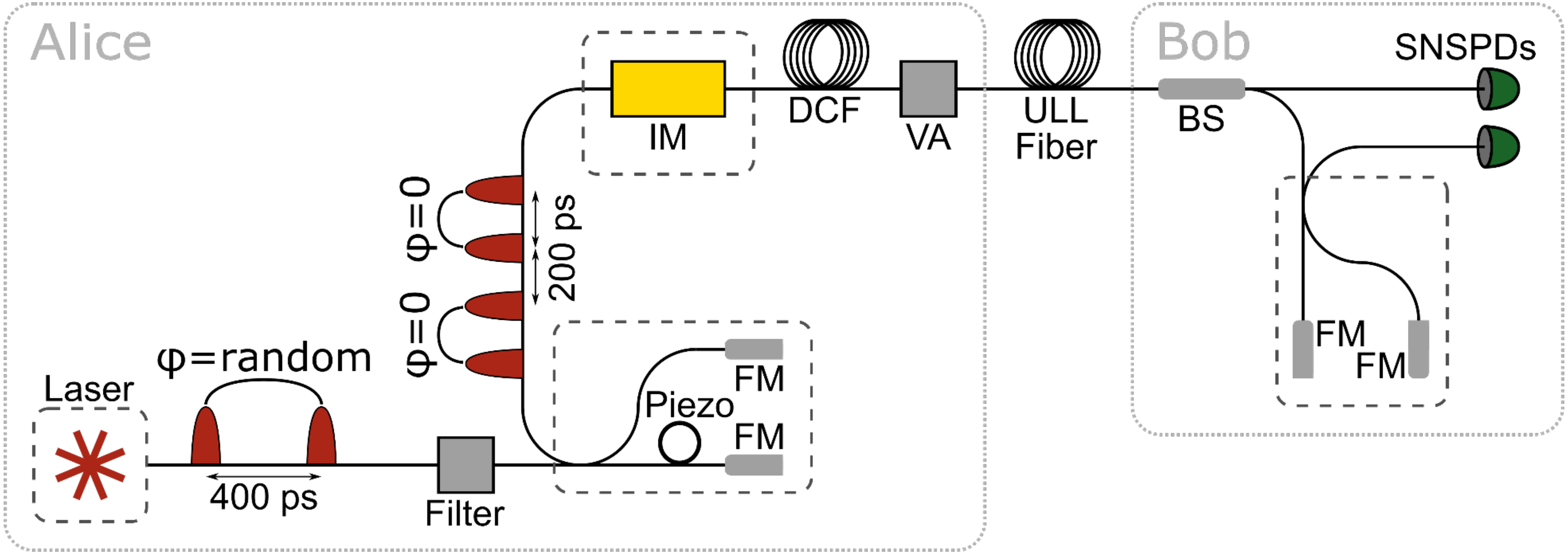
4 states, 4 outcomes $\rightarrow$ 3 states, 3 outcomes
Phys. Rev. A 74, 042342 (2006)

$\mu_1 \approx 0.5$

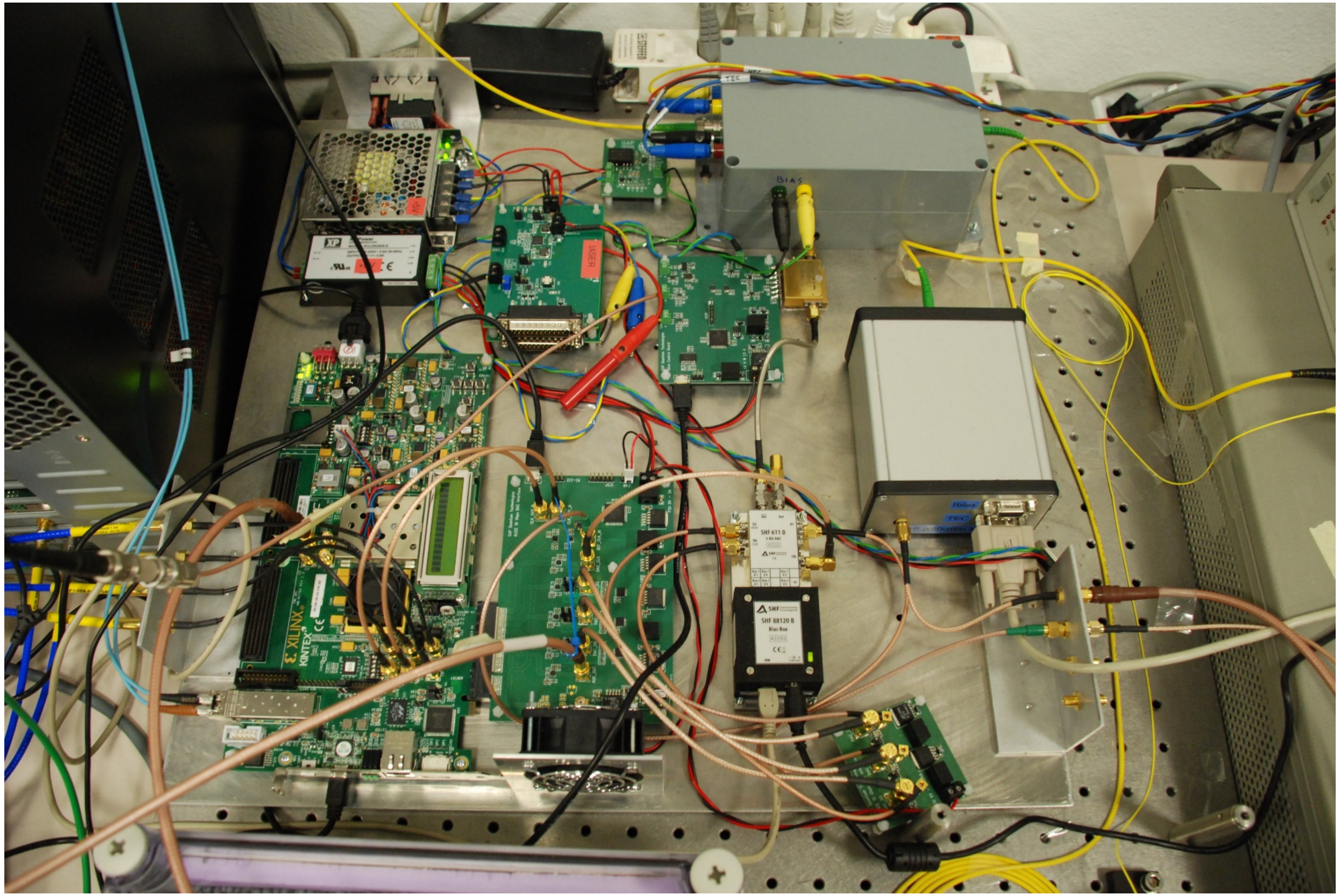
Rusca et. al, Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol, Phys. Rev. A 98, 052336 (2018)

UNIVERSITÉ DE GENÈVE

Simple Setup (with a single intensity modulator)



b) all fibre, high repetition rate source



Alice and Bob are FPGA controlled:

- Synchronization
  real-time adjustement of:
  - interferometer phase
  - detector timing

- Generate random bits
  QRNG + expansion

- High-speed integrated intensity
  modulator: 5 GHz

- Sifting
- Error correction
- Privacy amplification
- Authentication

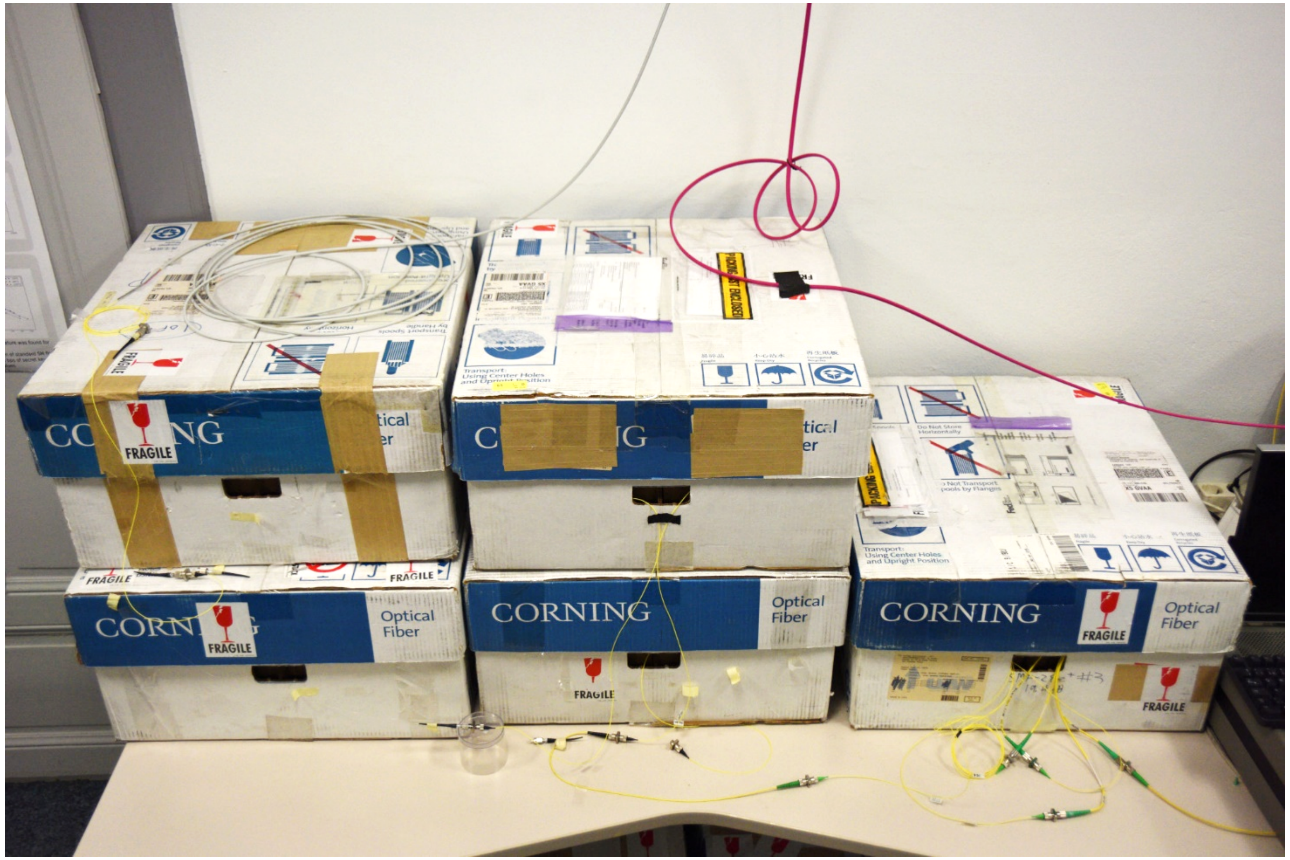
UNIVERSITÉ
DE GENÈVE

c) 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

CORNING

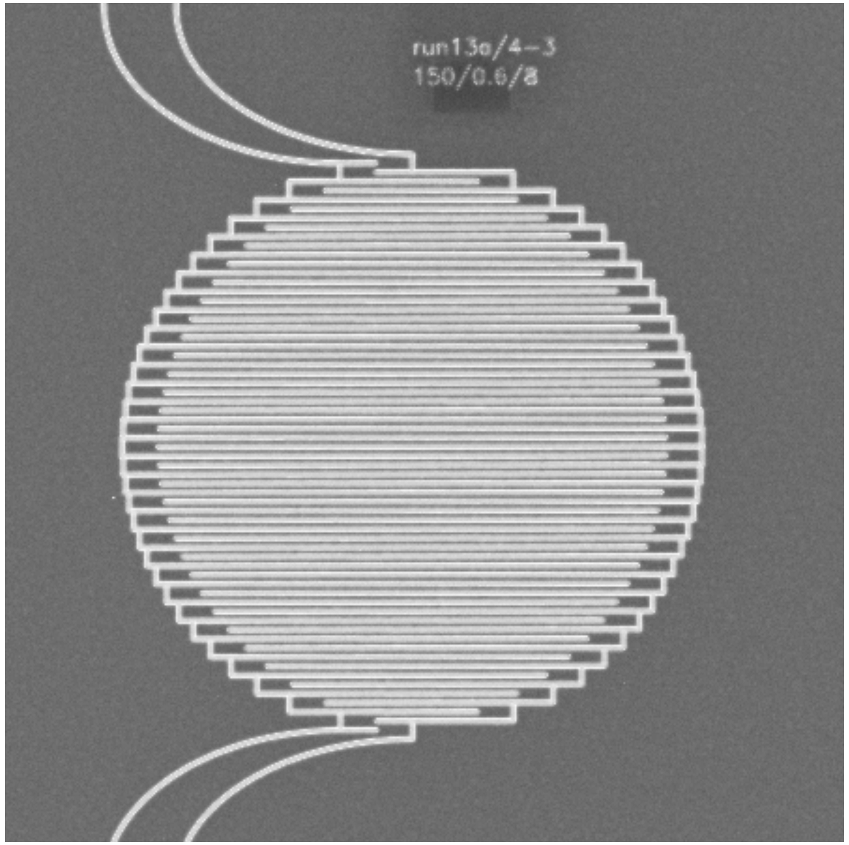


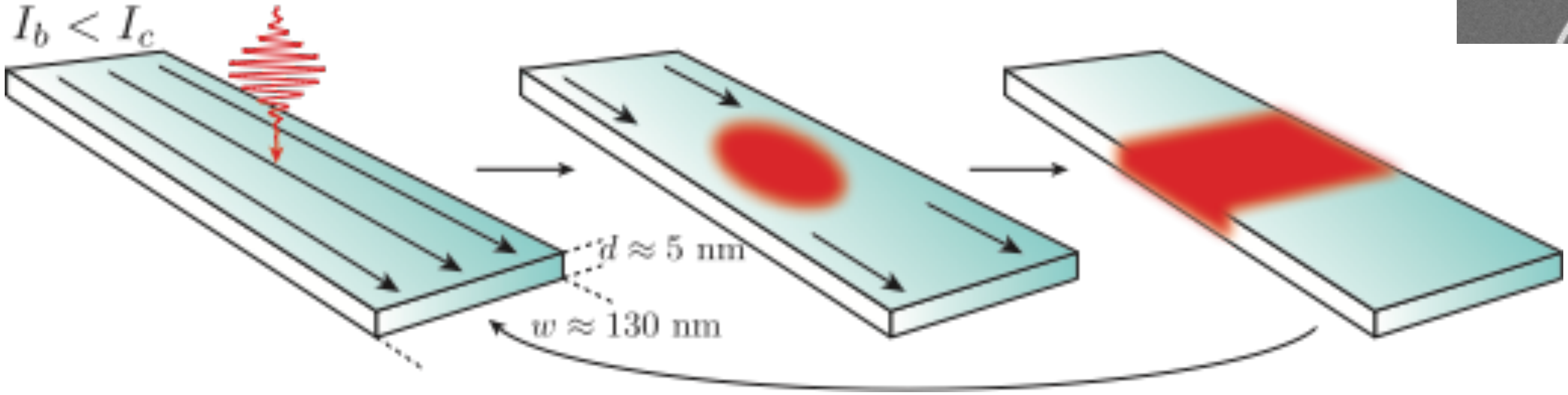
d) detectors

Superconducting nanowire single-photon detectors

Amorphous molybdenum silicide

Temperature: 0.8 K

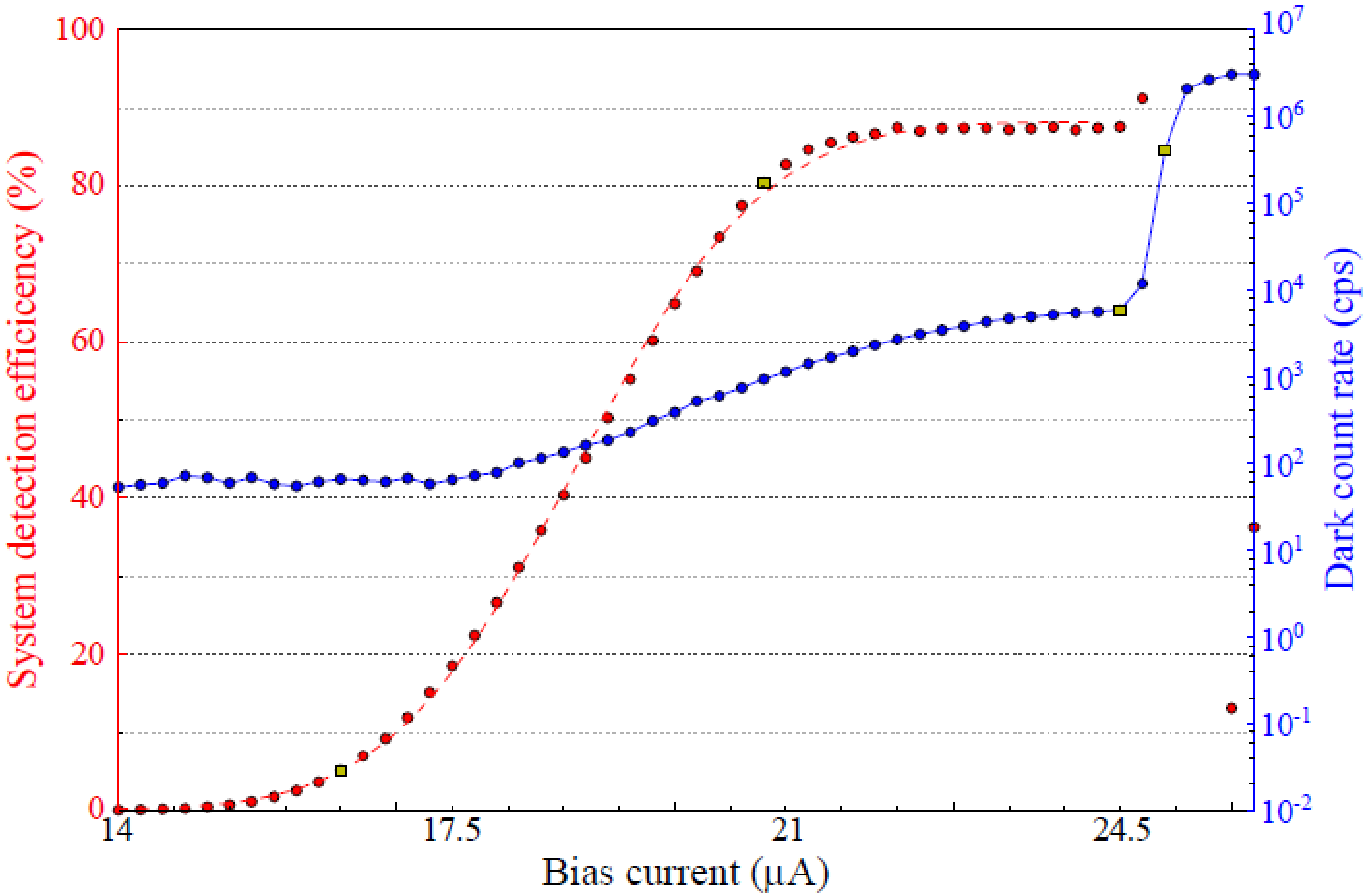




Appl. Phys. Lett. **112**, 061103 (2018)

UNIVERSITÉ DE GENÈVE

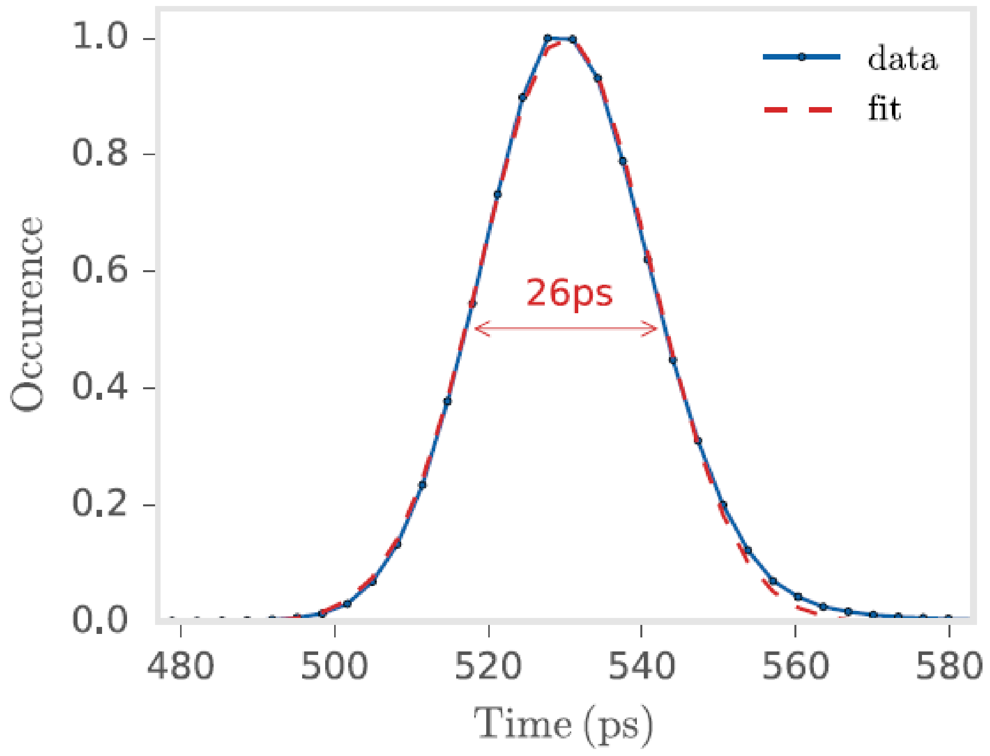
Performance of our SNSPD

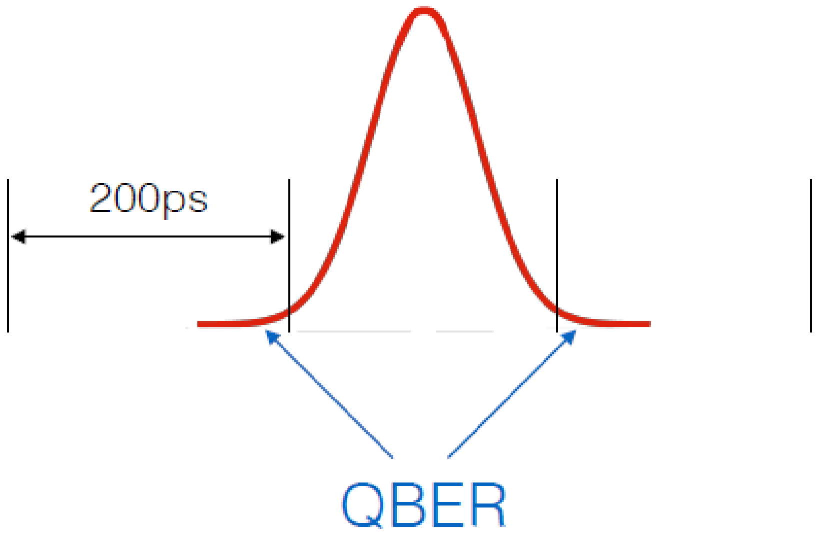


UNIVERSITÉ DE GENÈVE

Detector contributions to QBER

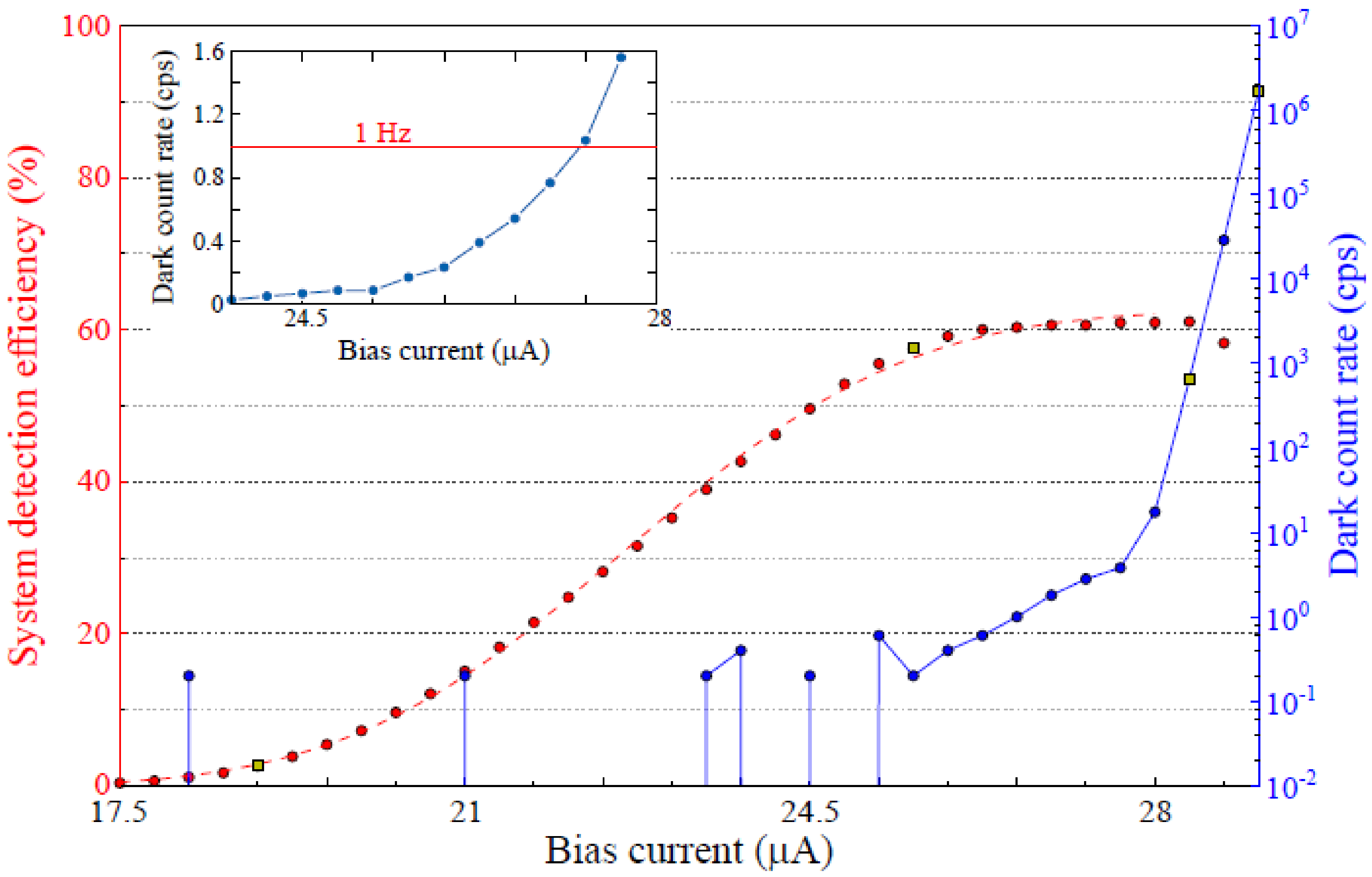
- Timing jitter
- darkcounts





UNIVERSITÉ DE GENÈVE

Dark counts: dominated by black-body radiation

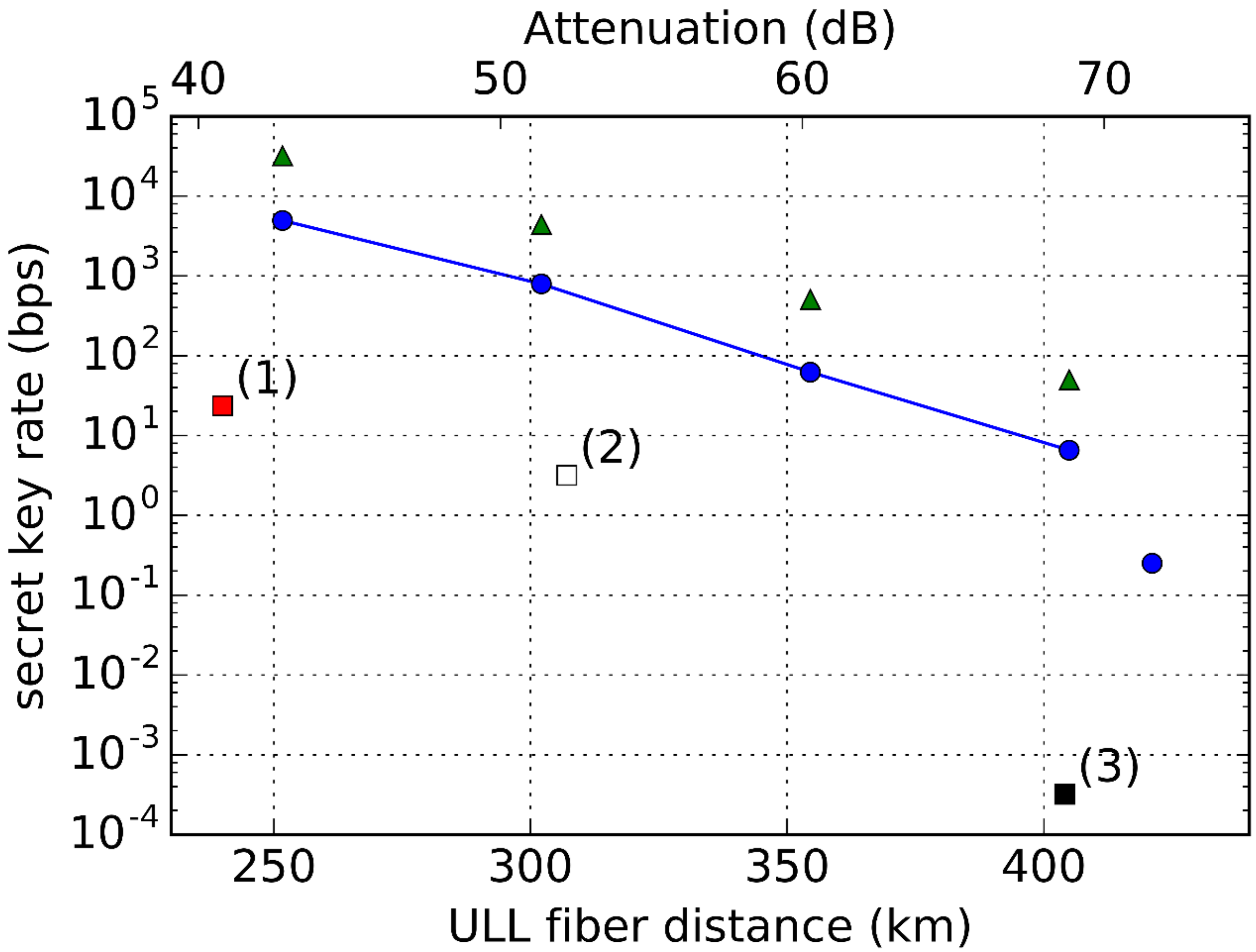


- No filtering
- +Fiber spool (cold)
- + WDM filter

- < 1 cts/s
- ~50% efficiency

UNIVERSITÉ DE GENÈVE

Results: SKR vs distance



Ideal system

- BB84 with decoy state
- 2.5 GHz repetition rate
- No detector noise
- 100% detection efficiency
- Same block size than exp. points

(1) **BB84**, Fröhlich et al., Optica **4**, 163 (2017), (2) **COW**, Korzh et al., Nat. Phot. **9**, 163 (2015)

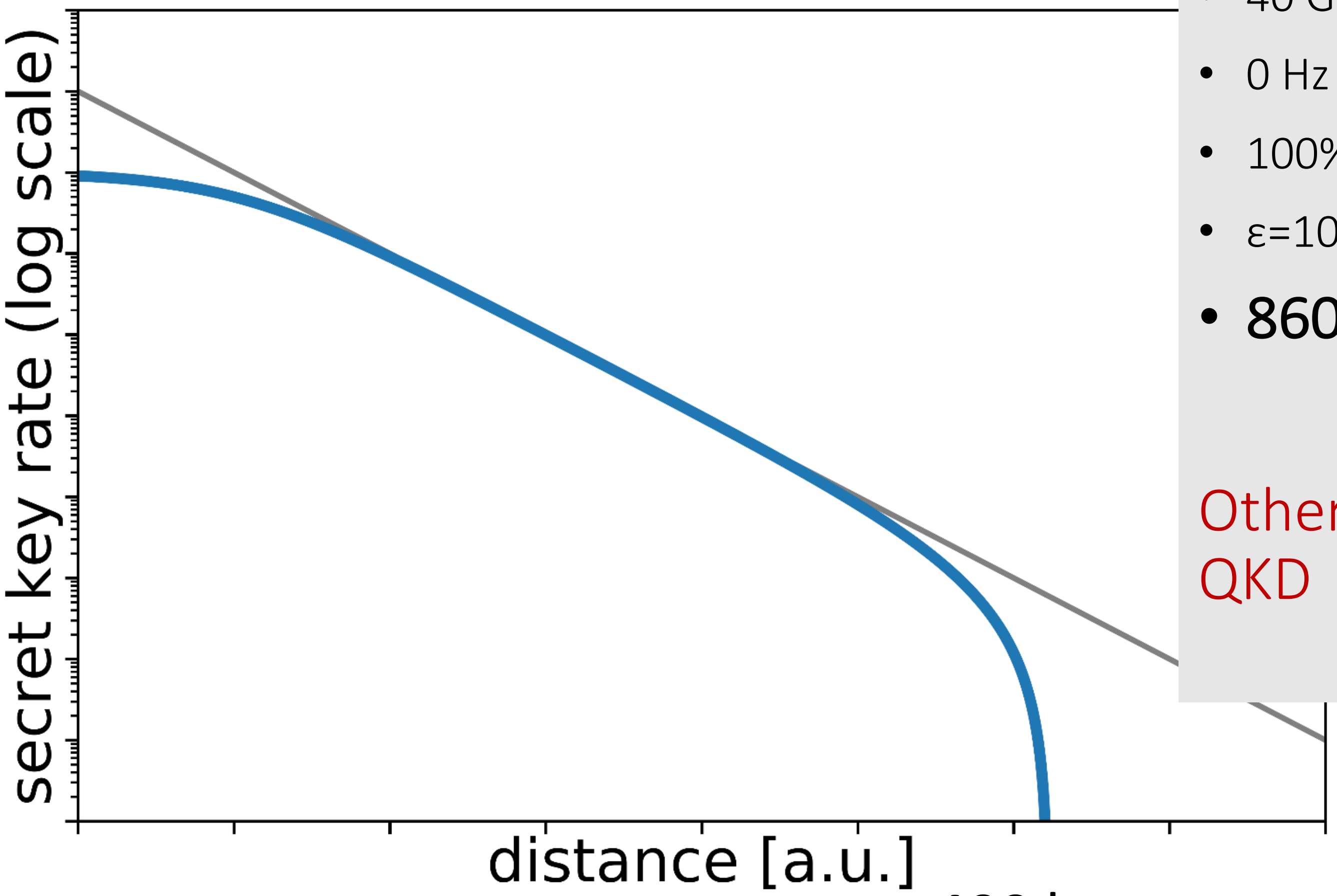
(3) **MDI**, Yin et al. Phys. Rev. Lett. **117**, 190501 (2016)

Secret Key rate vs distance

Dmax = f(dcr, block size)

10 Mbit/s

≈ $1/t_{dead}$



400 km

- **1 day acquisition time**
- BB84 with decoy state
- 40 GHz repetition rate
- 0 Hz dark counts
- 100% detection efficiency
- $\varepsilon=10^{-9}$
- **8600 bits/24h @ 600km**

Other approach: twin-field QKD

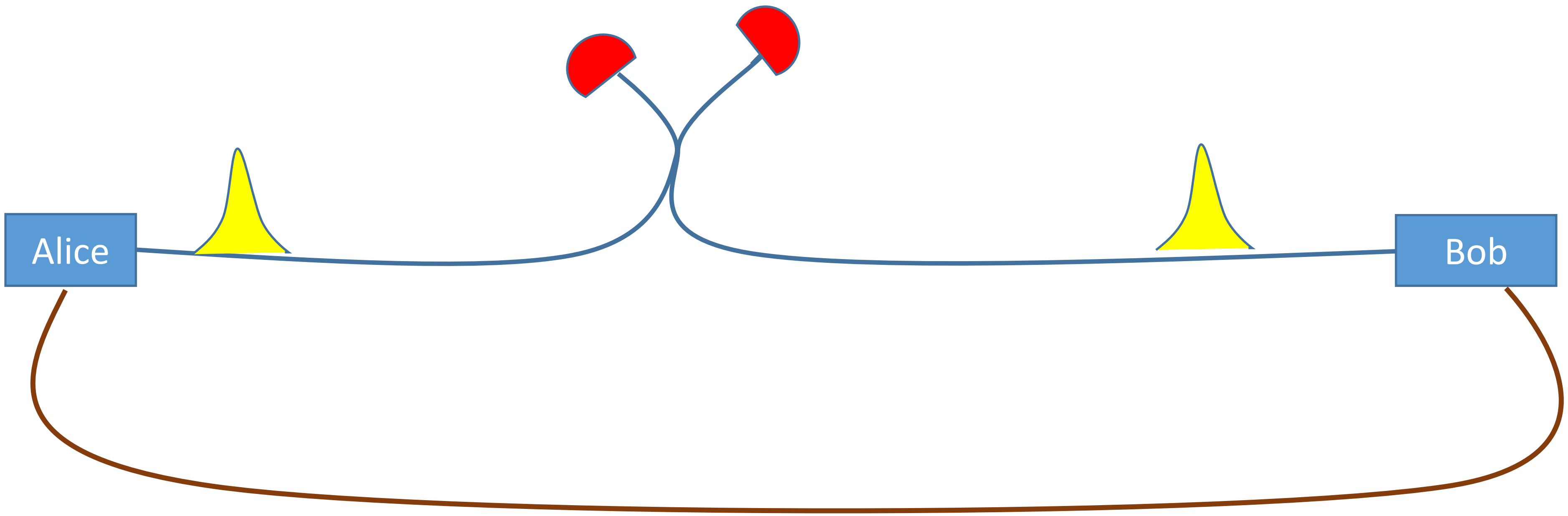
UNIVERSITÉ DE GENÈVE

Twin field QKD

In fact, it's a huge interferometer!

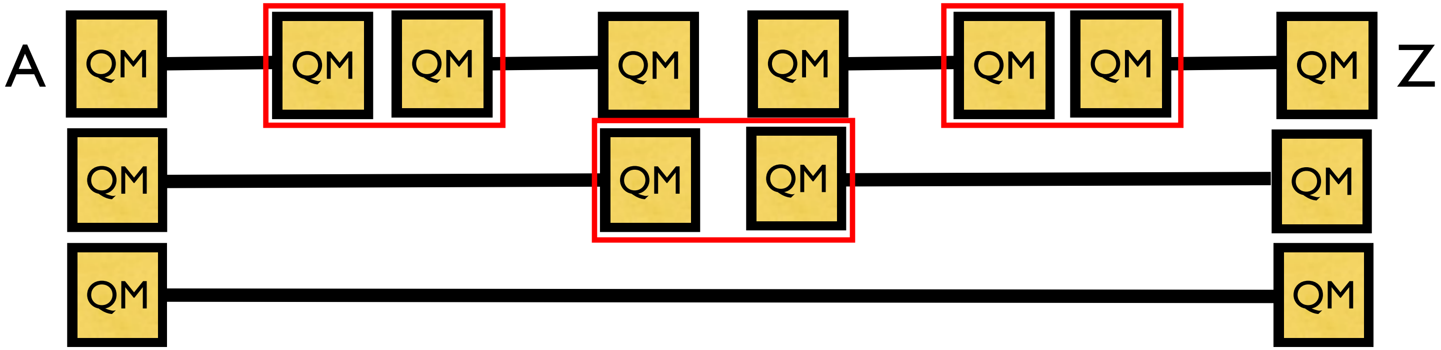
- Stabilisation!
- Synchronisation!

- Recent feasability experiment: 500 km



Quantum repeater

Create remote entanglement independently for each link. Extend by swapping



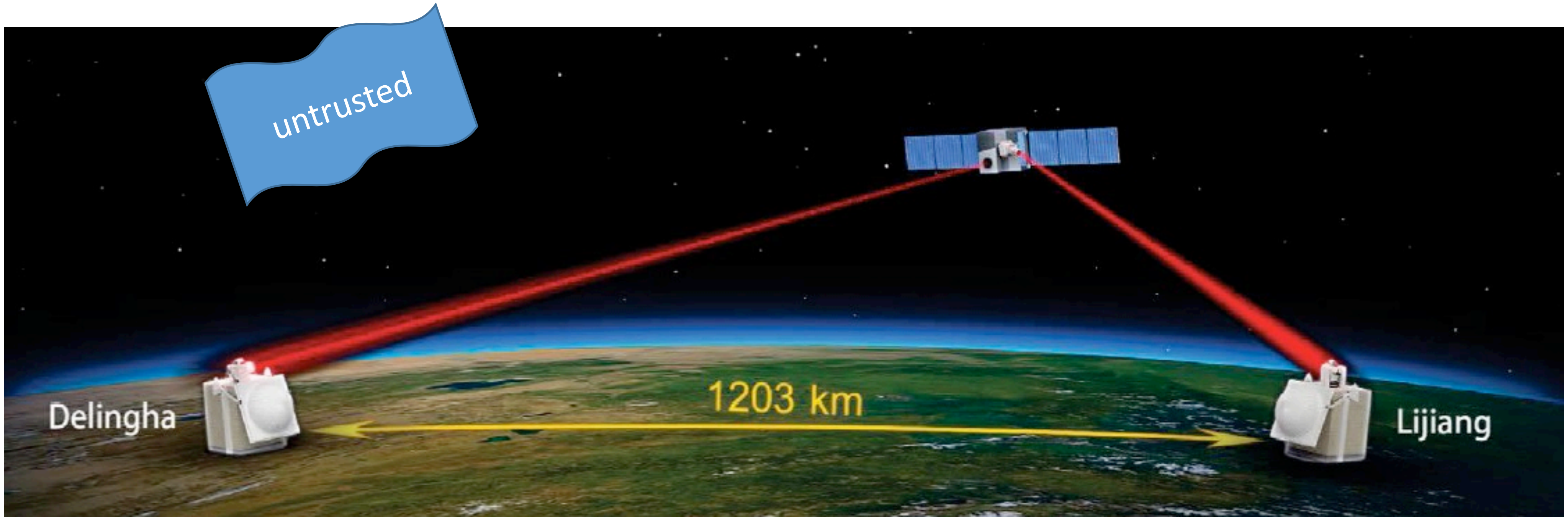
Direct transmission $T \sim \left(\frac{1}{\eta_t}\right)^n$

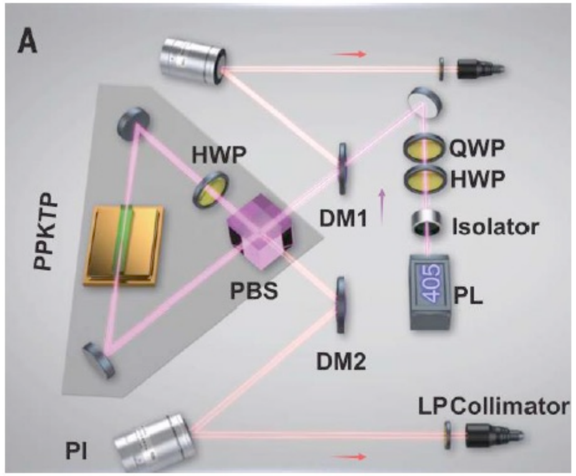
Repeater $T \sim \frac{1}{\eta_t}$

Requires heralded entanglement creation, storage and swapping of entanglement

Talk de Mikael Afzelius demain!


Science
AAAS
QUANTUM OPTICS
Satellite-based entanglement distribution over 1200 kilometers
Juan Yin,[1,2] Yuan Cao,[1,2] Yu-Huai Li,[1,2] Sheng-Kai Liao,[1,2] Liang Zhang,[2,3] Ji-Gang Ren,[1,2] Wen-Qi Cai,[1,2] Wei-Yue Liu,[1,2] Bo Li,[1,2] Hui Dai,[1,2] Guang-Bing Li,[1,2] Qi-Ming Lu,[1,2] Yun-Hong Gong,[1,2] Yu Xu,[1,2] Shuang-Lin Li,[1,2] Feng-Zhi Li,[1,2] Ya-Yun Yin,[1,2] Zi-Qing Jiang,[3] Ming Li,[3] Jian-Jun Jia,[3] Ge Ren,[4] Dong He,[4] Yi-Lin Zhou,[5] Xiao-Xiang Zhang,[6] Na Wang,[7] Xiang Chang,[8] Zhen-Cai Zhu,[5] Nai-Le Liu,[1,2] Yu-Ao Chen,[1,2] Chao-Yang Lu,[1,2] Rong Shu,[2,3] Cheng-Zhi Peng,[1,2*] Jian-Yu Wang,[2,3*] Jian-Wei Pan[1,2*]
http://science.sciencemag.org/content/356/6343/1140





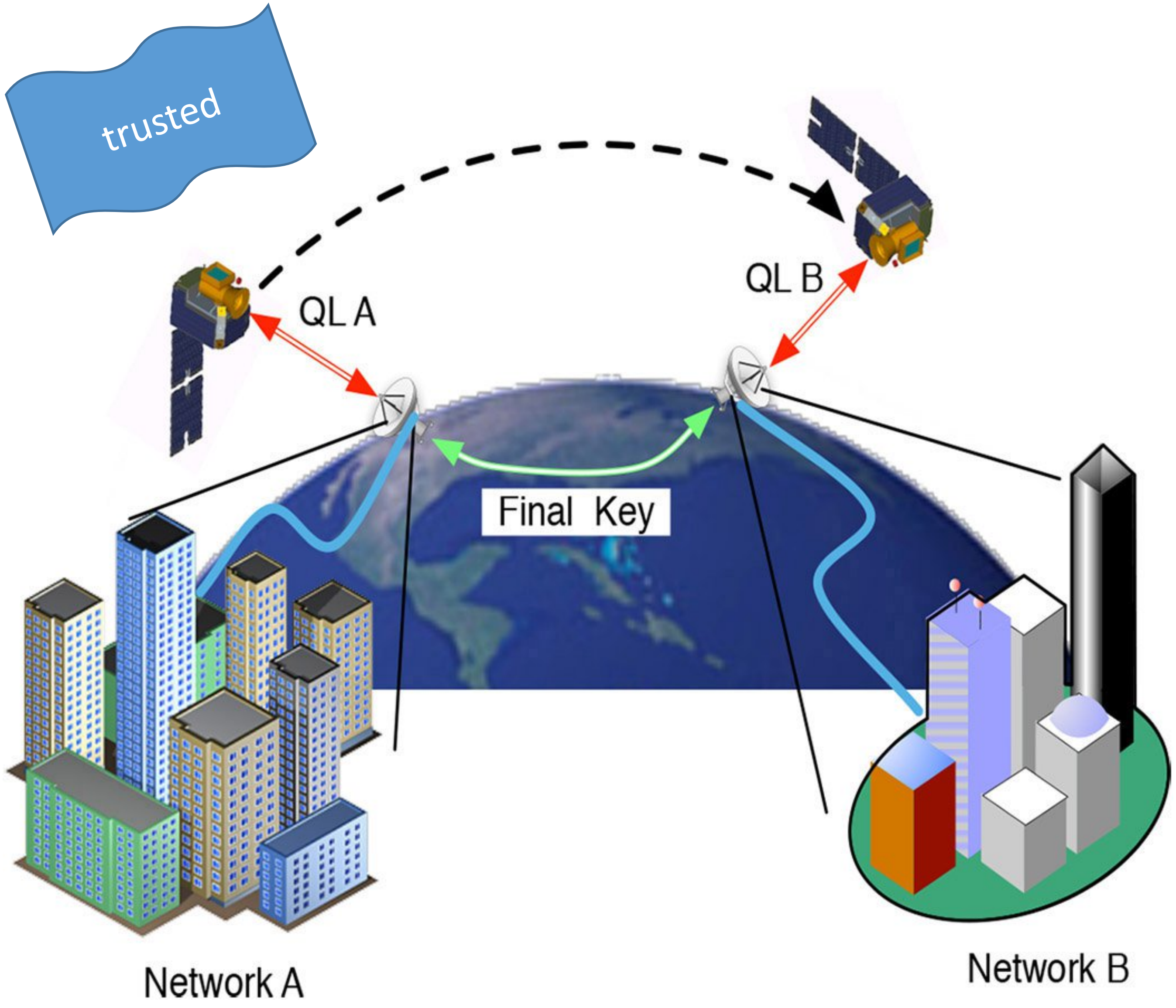
SPDC source: 810 nm
6 MHz pair generation rate

Total loss: ~65dB
Average coincidence count rate: 1Hz
275s coverage time
S=2.37 ± 0.09

Finite key analysis: Impossible to extract a key with small ε

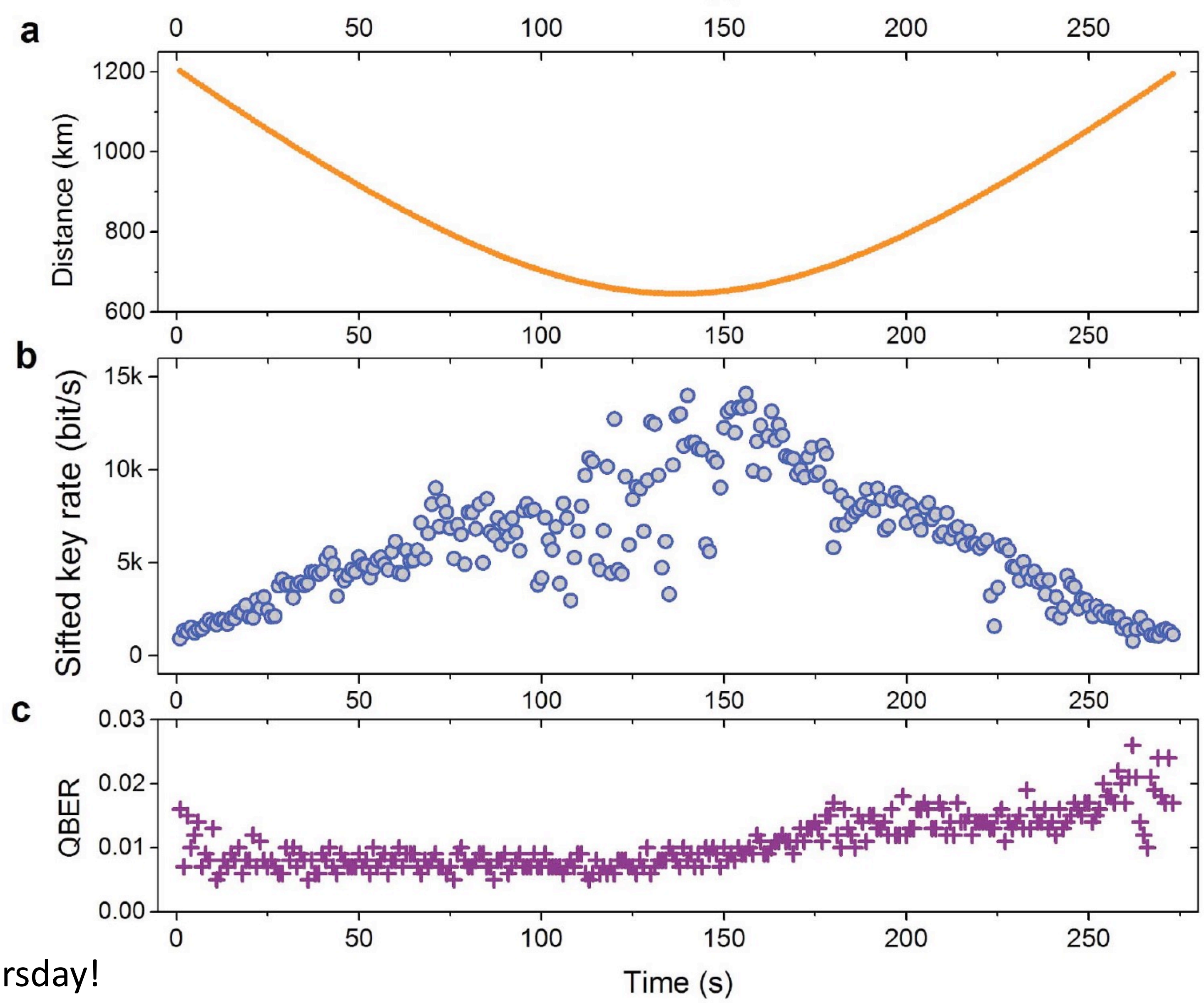
UNIVERSITÉ DE GENÈVE

Satellite to ground QKD



- just one downlink with decoy-state faint laser pulses (polarisation BB84)

Results



1-10 kb/s
during 250s per passage

Thursday!

UNIVERSITÉ
DE GENÈVE

Conclusions

- QKD over 400 - 500 km
- Bit rates over 10Mbit/s @ < 50km

Outlook:

- Make it smaller, make it cheaper (integrated optics)
- Integrate it in telecom network
- Find many applications!