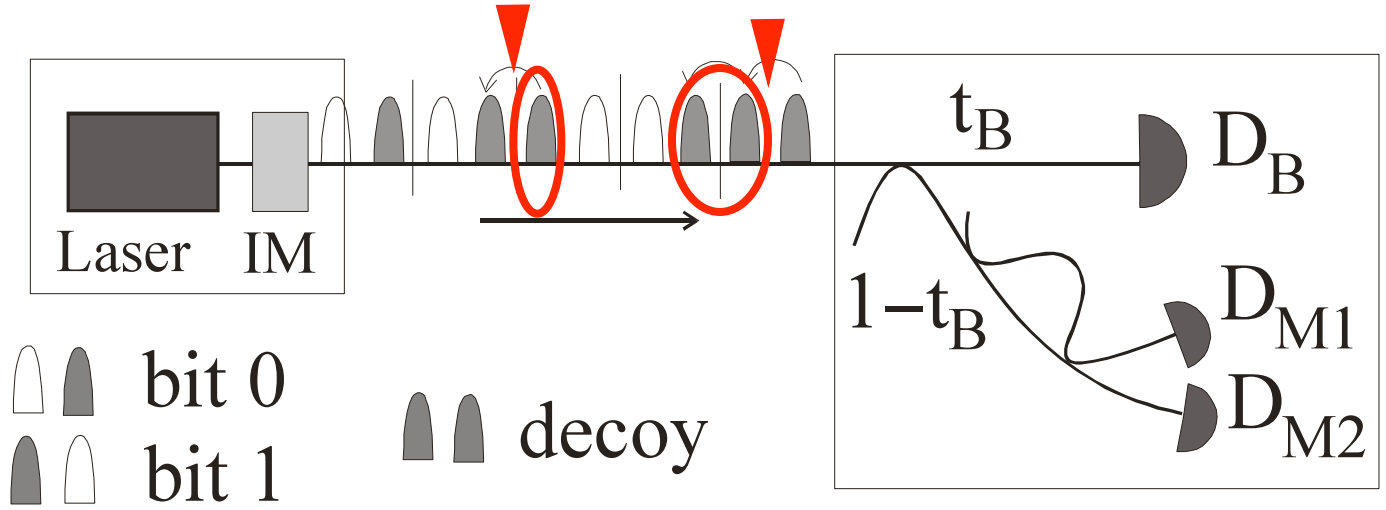
Quantum Key Distribution over Telecom Networks

Hugo Zbinden, N. Walenta, C. Barreiro, P. Eraerds, D.Stucki, N. Gisin,
Group of Applied Physics, University of Geneva, Switzerland
M. Legré and P. Trinkler,
id Quantique, Geneva

- Long-distance high speed QKD
- Commercial QKD and Data Encryption over a single optical fibre using WDM

Coherent one-way (COW) scheme



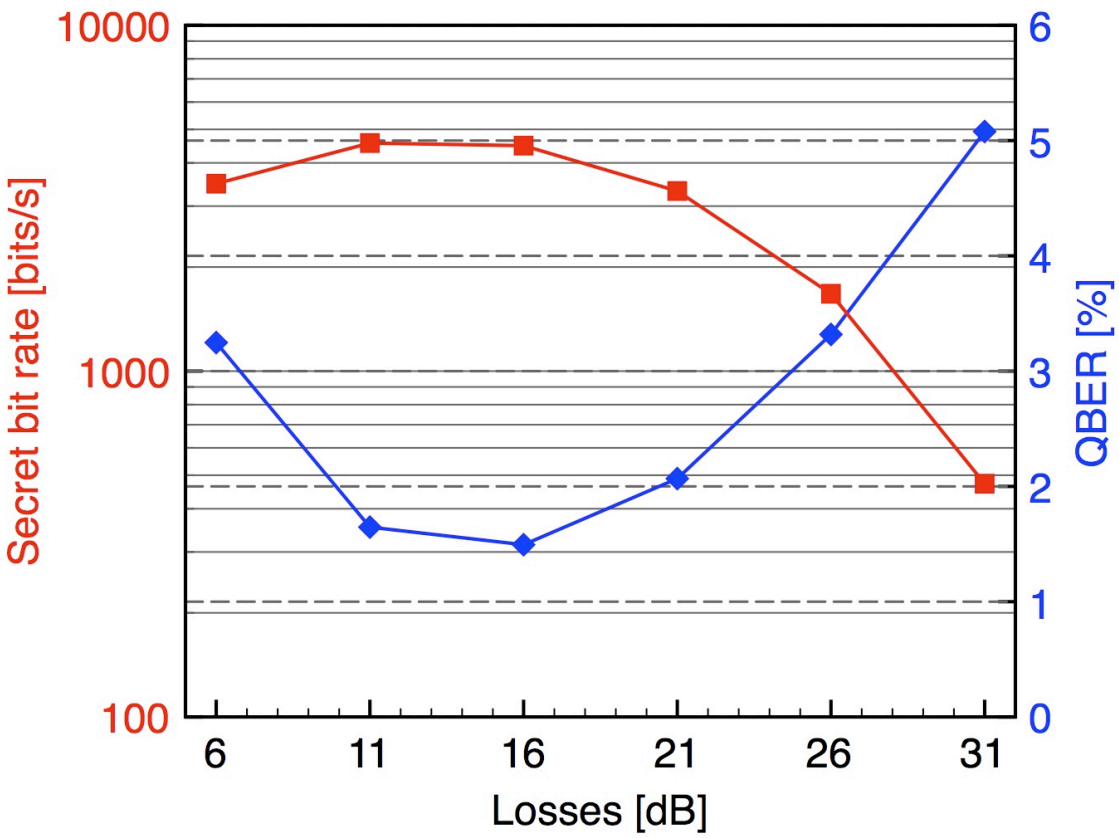
Advantages:

- Simple optical setup, no noise on the data line
- **Security:** check the coherence of successive pulses
Reduced interference visibility does not introduce errors
- Resistant to PNS attacks! ($\mu_{opt} \approx 0.5$)
(Note: Scheme does not work with single photons)

COW implementation (SECOQC)

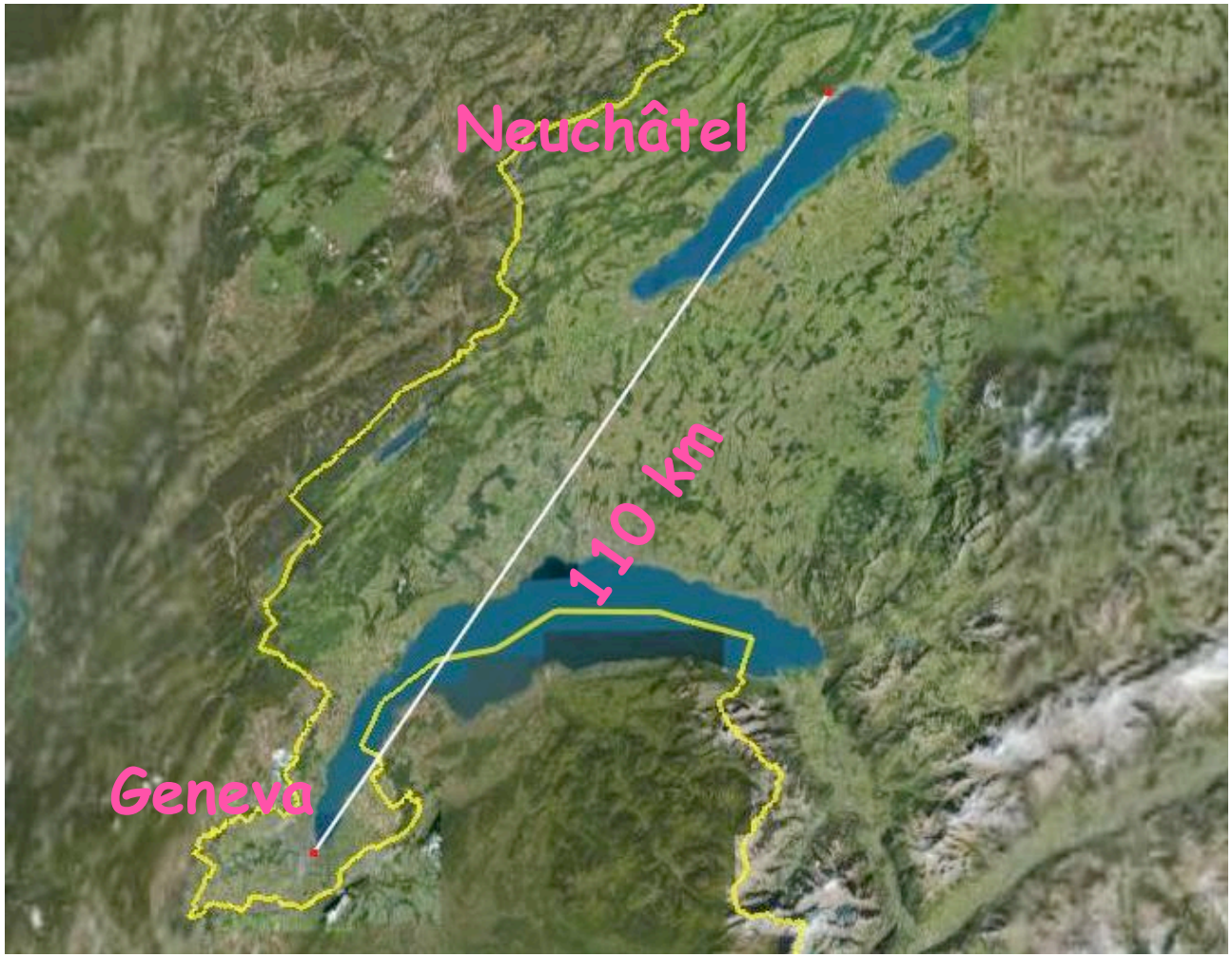
- Completely automated prototypes with integrated PC
- 2.5 GHz Xilinx Virtex II pro FPGA
- 625 MHz pulse rate (312.5 MHz logical)
- Real time distillation (cascade)

COW results (InGaAs lab, 25 km + x dB)



- Detector saturates at short distances
- Range ca. 150 km (0.2 dB/km)

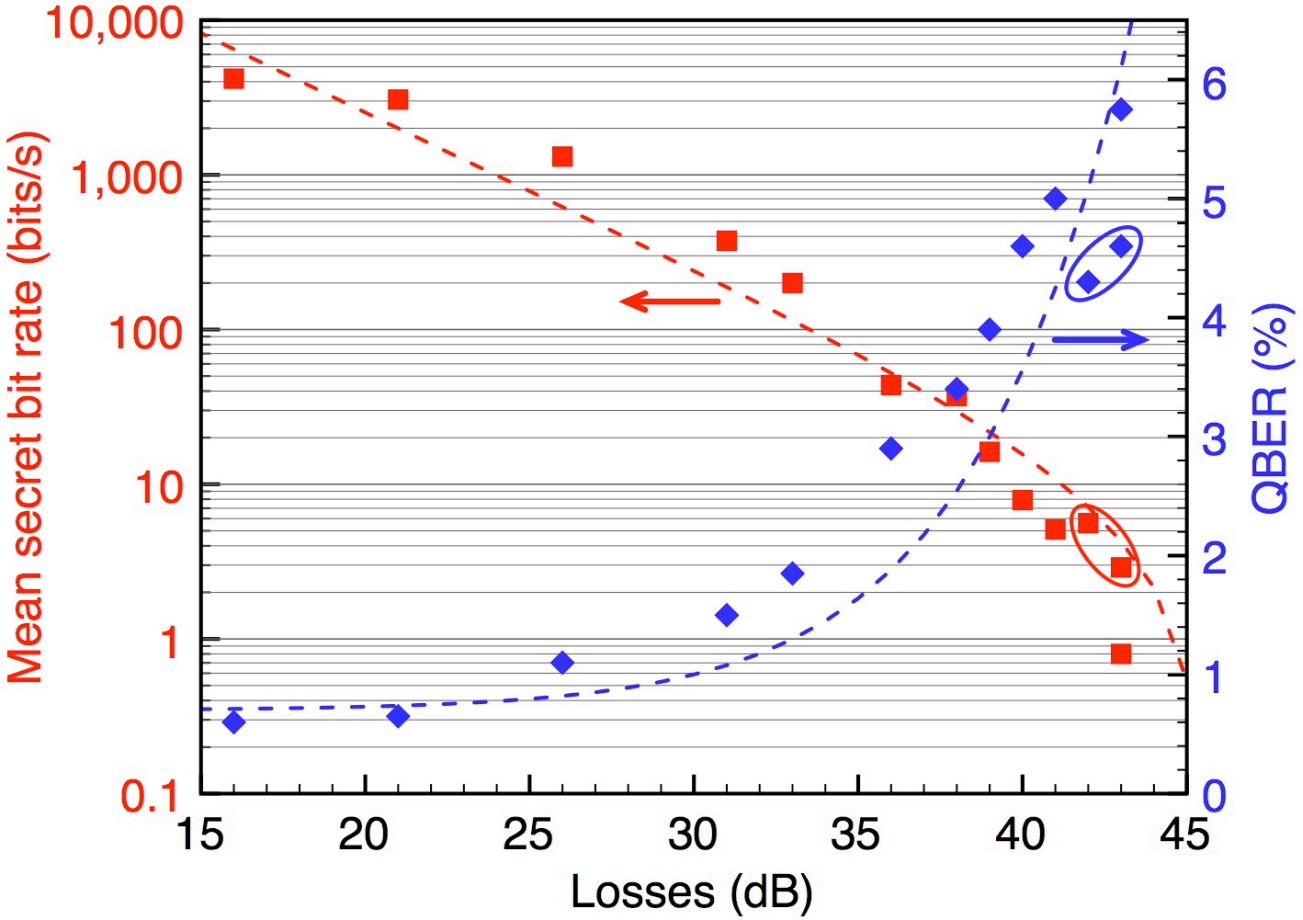
The COW in the Field



2 dark fibers
~150km
43 dB loss
(0.29dB/km)

Opt. Exp. **17** (16), 13326-13334 (2009)

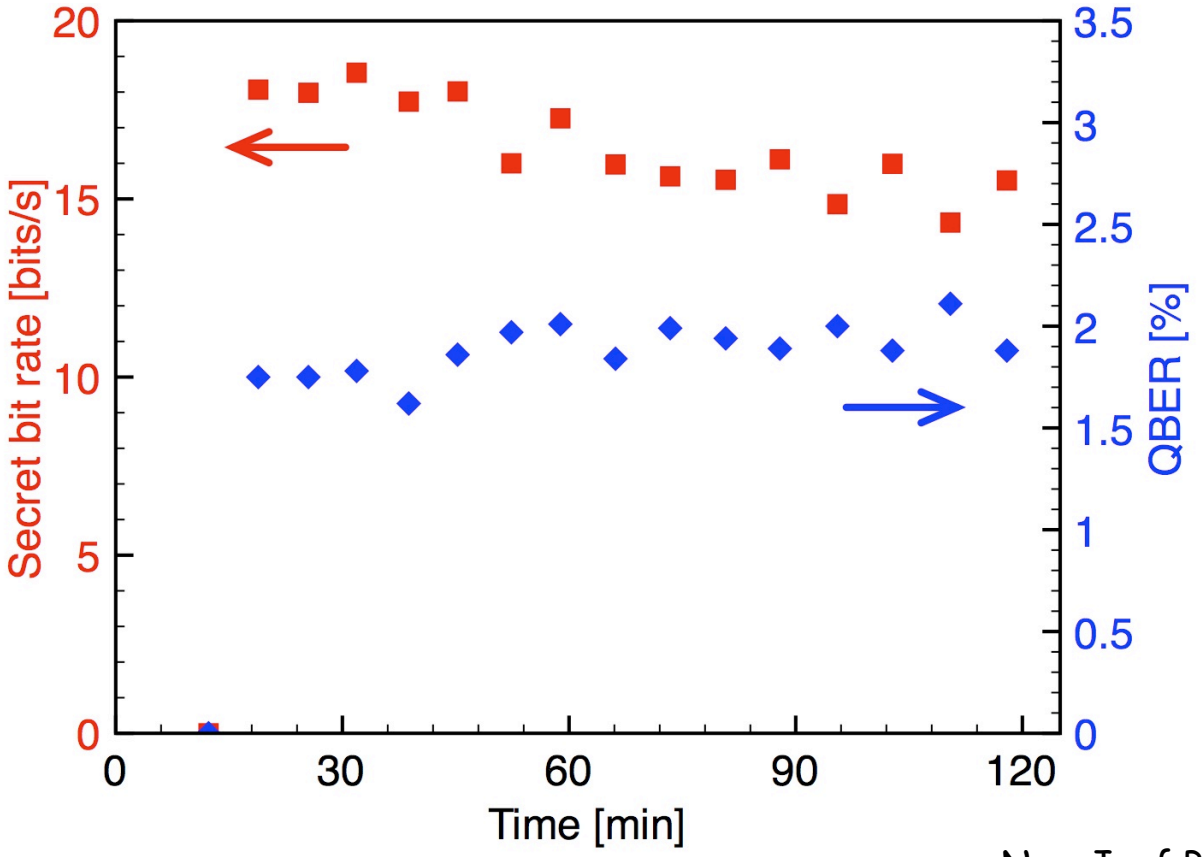
COW results (SSPD, 150 km - x dB)



- SSPDs at 2.7K
- variation of μ to simulate different losses (150 km of fibres)
- more than 2 secret bits/s over 43dB of losses

QKD over 250 km of ULL fibers

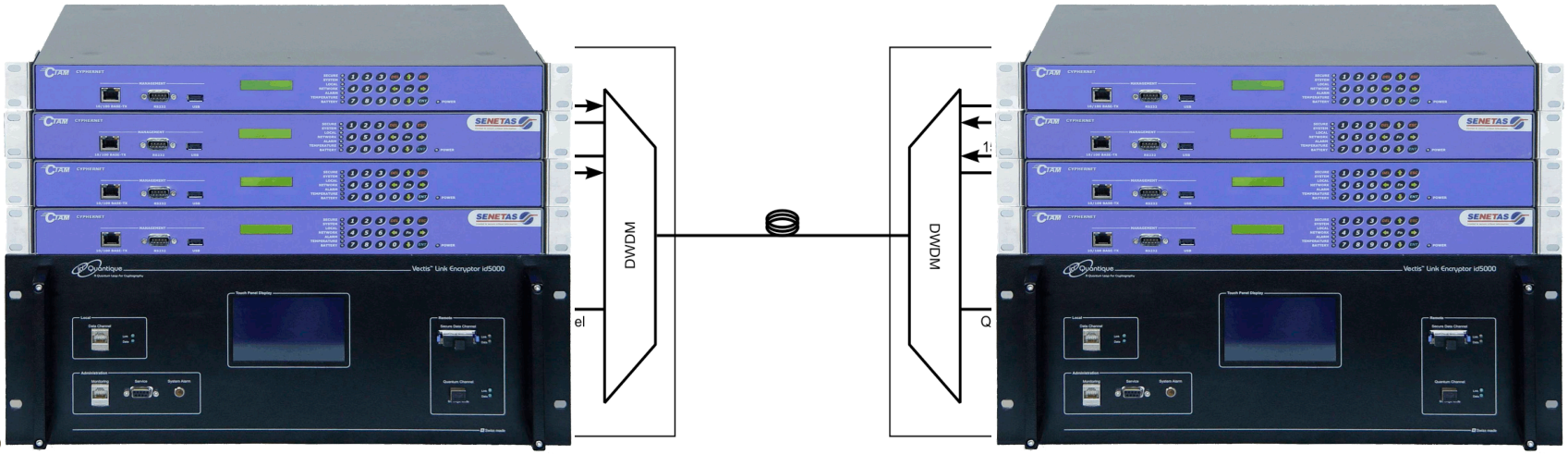
ITU G.652 compliant low loss fiber by Corning Inc.
Attenuation: 0.165 dB/km @ 1550nm

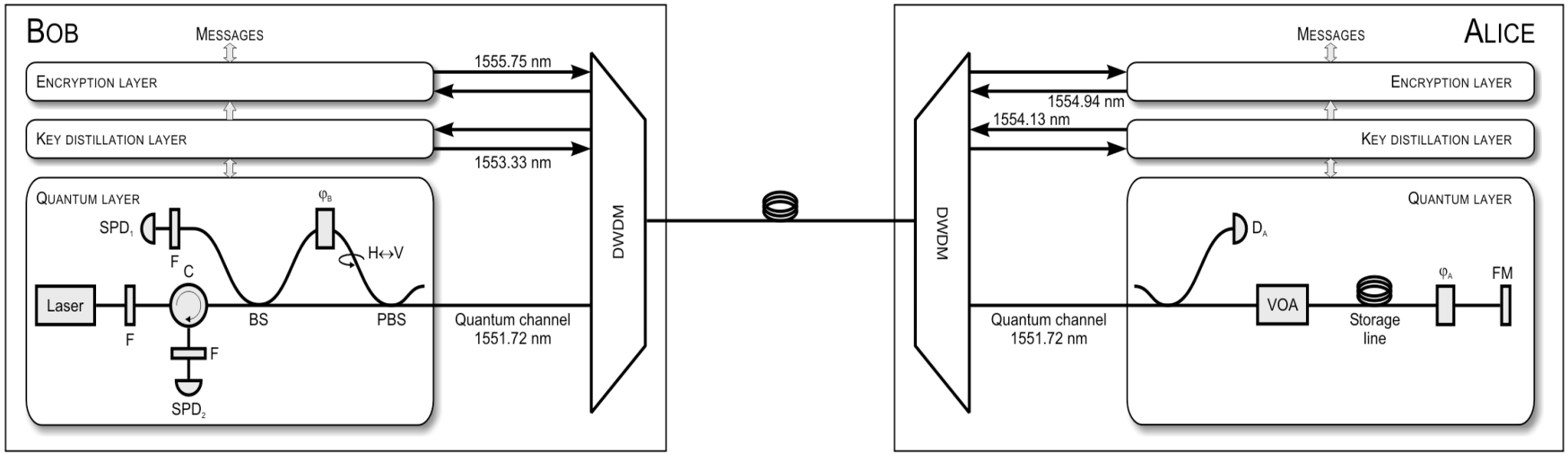


New J. of Phys **11**, 075003 (2009)

Quantum Key Distribution over Telecom Networks

- Goal: Key distribution and high speed data encryption over a single optical fibre
- Commercial QKD (plug & play) and AES-encryptors (256 bits keys, 1 Gbps rate)





$$QBER = QBER_{opt} + QBER_{det} + QBER_{noise/WDM}$$

What are the noise sources?

- Crosstalk of other wavelengths into quantum channel
- Generation of parasitic light at the wavelength of the quantum channel
  - by Raman scattering
  - by Four Wave Mixing (FWM)

Raman Scattering

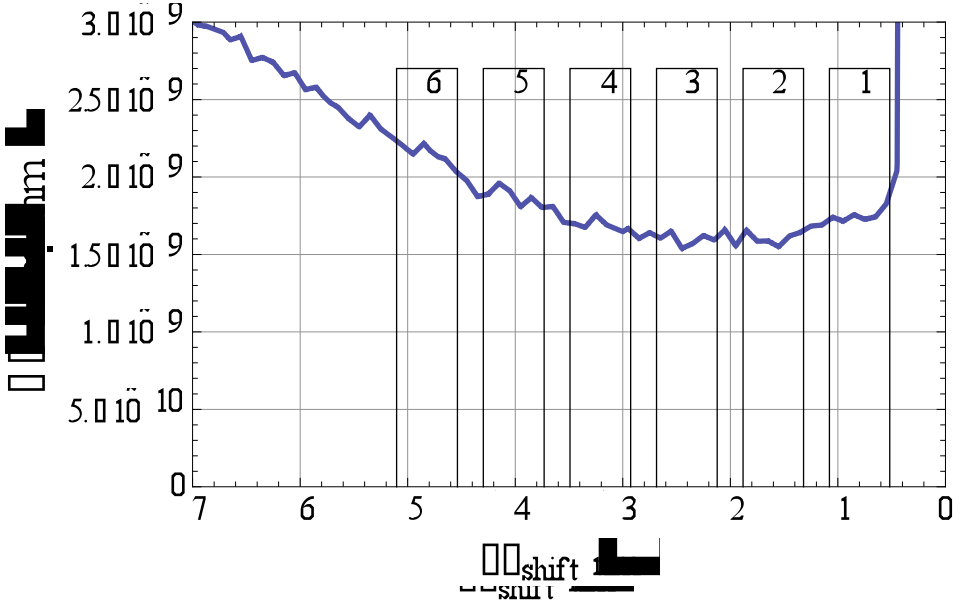
$$P_{forward} = P_{in}\, p(\lambda) L e^{-\alpha L}$$

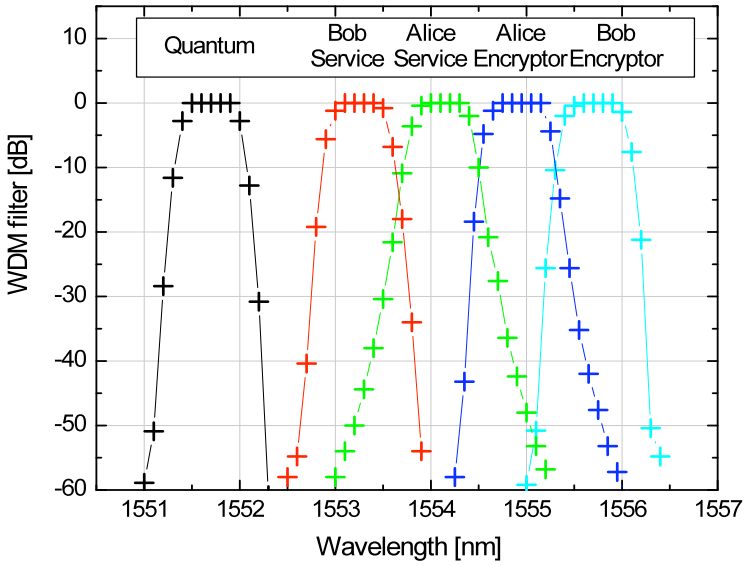
$$P_{backward} = P_{in}\, p(\lambda) \frac{1 - e^{-2\alpha L}}{2\alpha}$$

$$P_{forward} = P_{out}\, p(\lambda) L$$

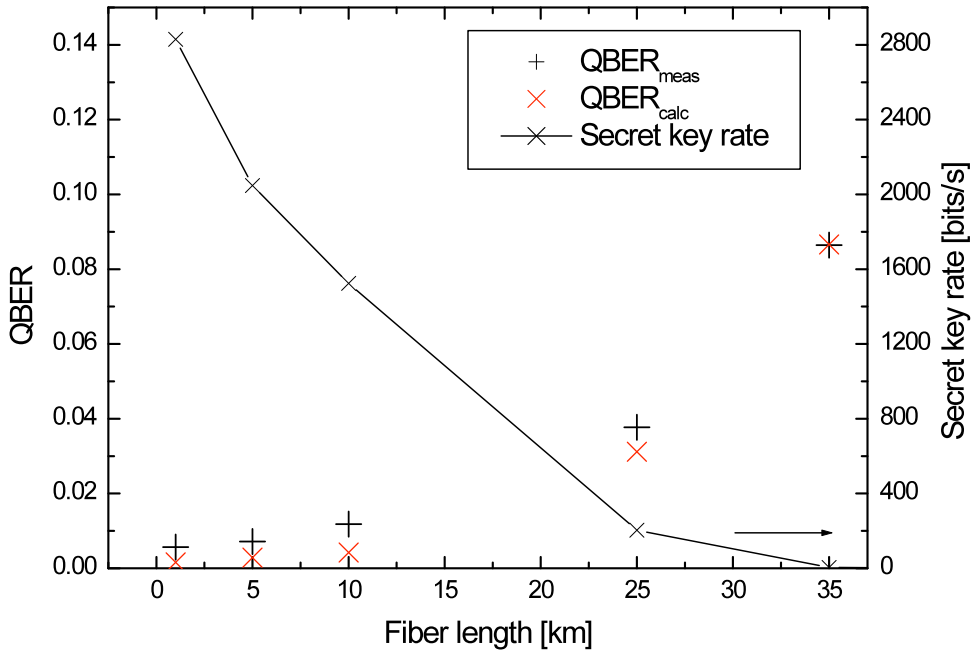
$$P_{backward} = P_{out}\, p(\lambda) \frac{e^{\alpha L} - e^{-\alpha L}}{2\alpha}$$

SFP receivers: -28dBm





Experimental Results



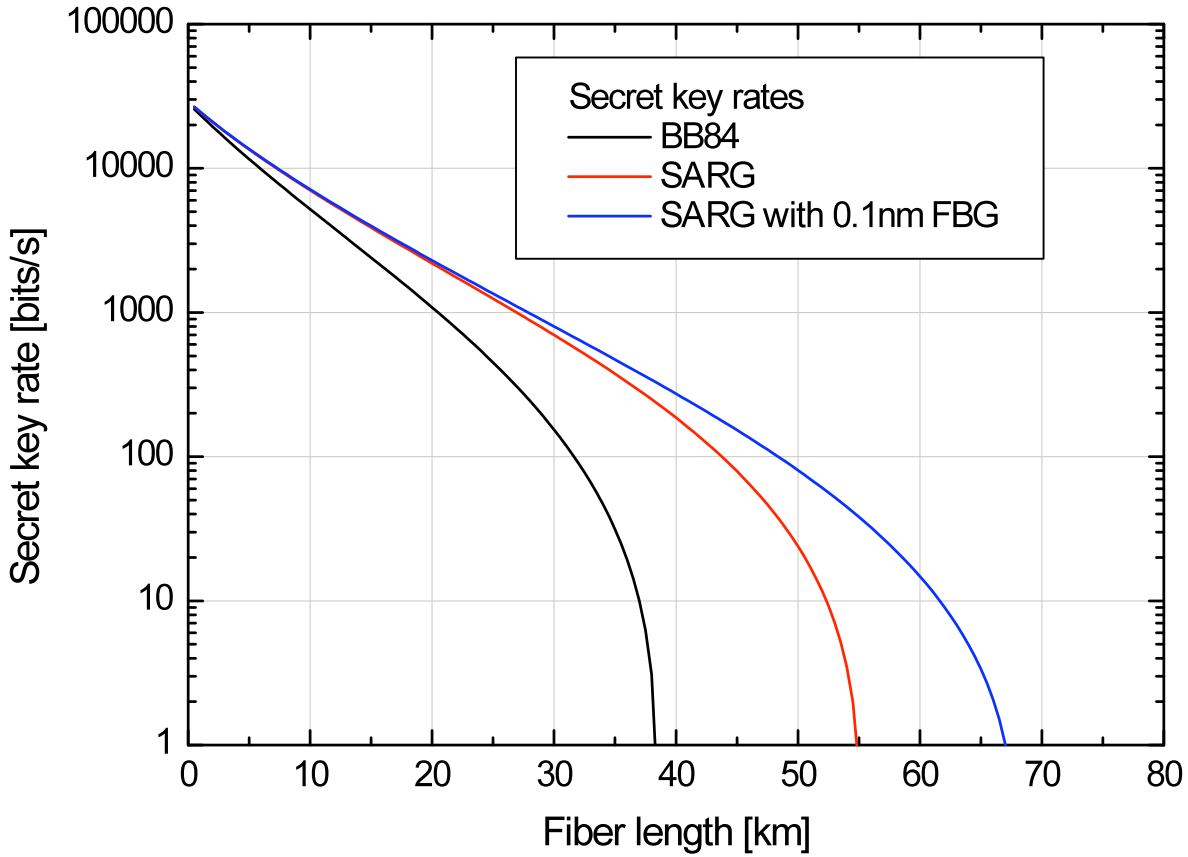
How can we increase the range?

$$S \propto \mu(L), e^{-\alpha L}$$

$$N \propto \Delta\lambda, e^{\alpha L}$$

BB84: $\mu=t$ SARG: $\mu=t^{1/2}$

Additional filter (FBG) : $\Delta\lambda$=0.8 nm $\rightarrow\Delta\lambda$=0.1 nm



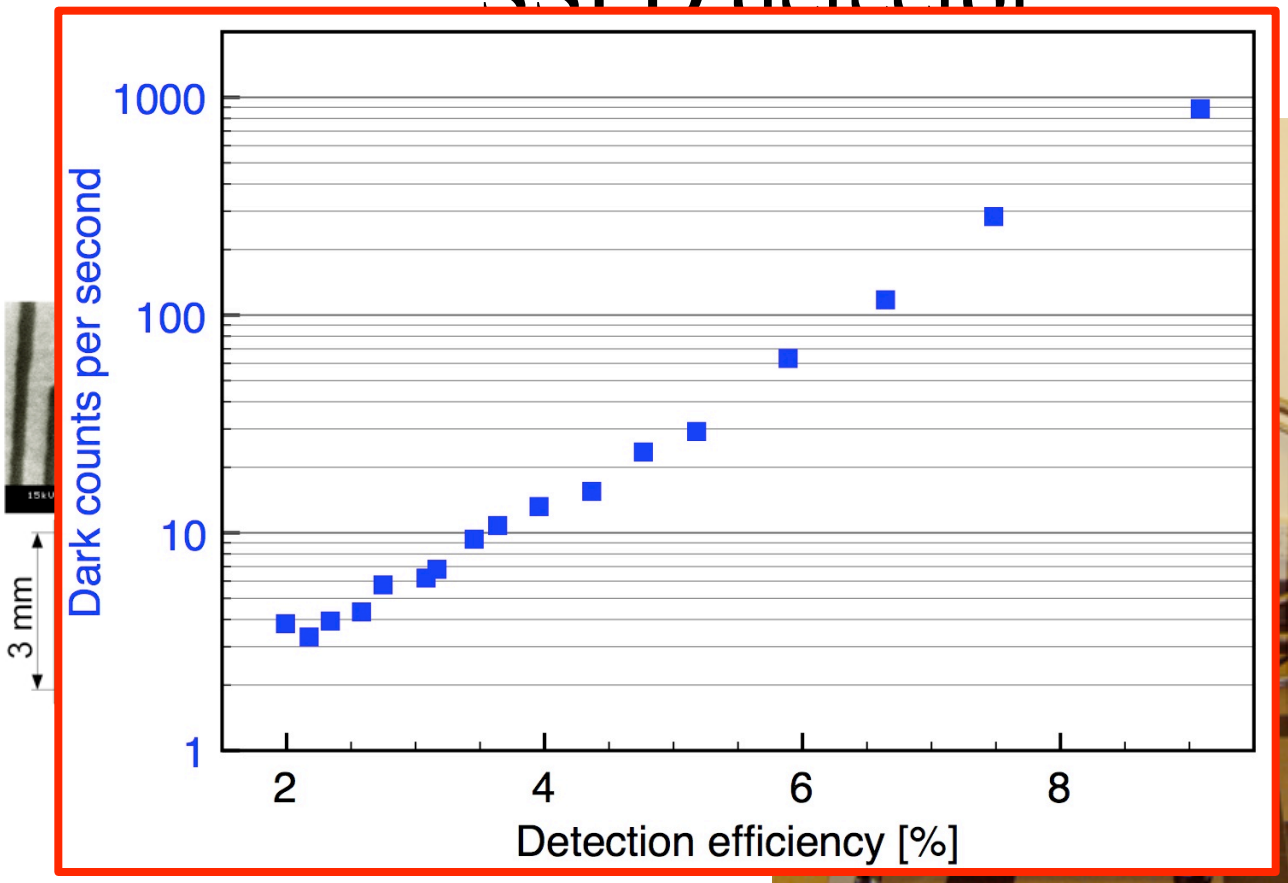
Conclusions

Limits of QKD

- Standard fibre and InGaAs detectors: 150 km
- With ULL fibre and SSPD detector: 250 km
- Key exchange and high speed encryption (1Gbps) using a single dark fibre: 60 km

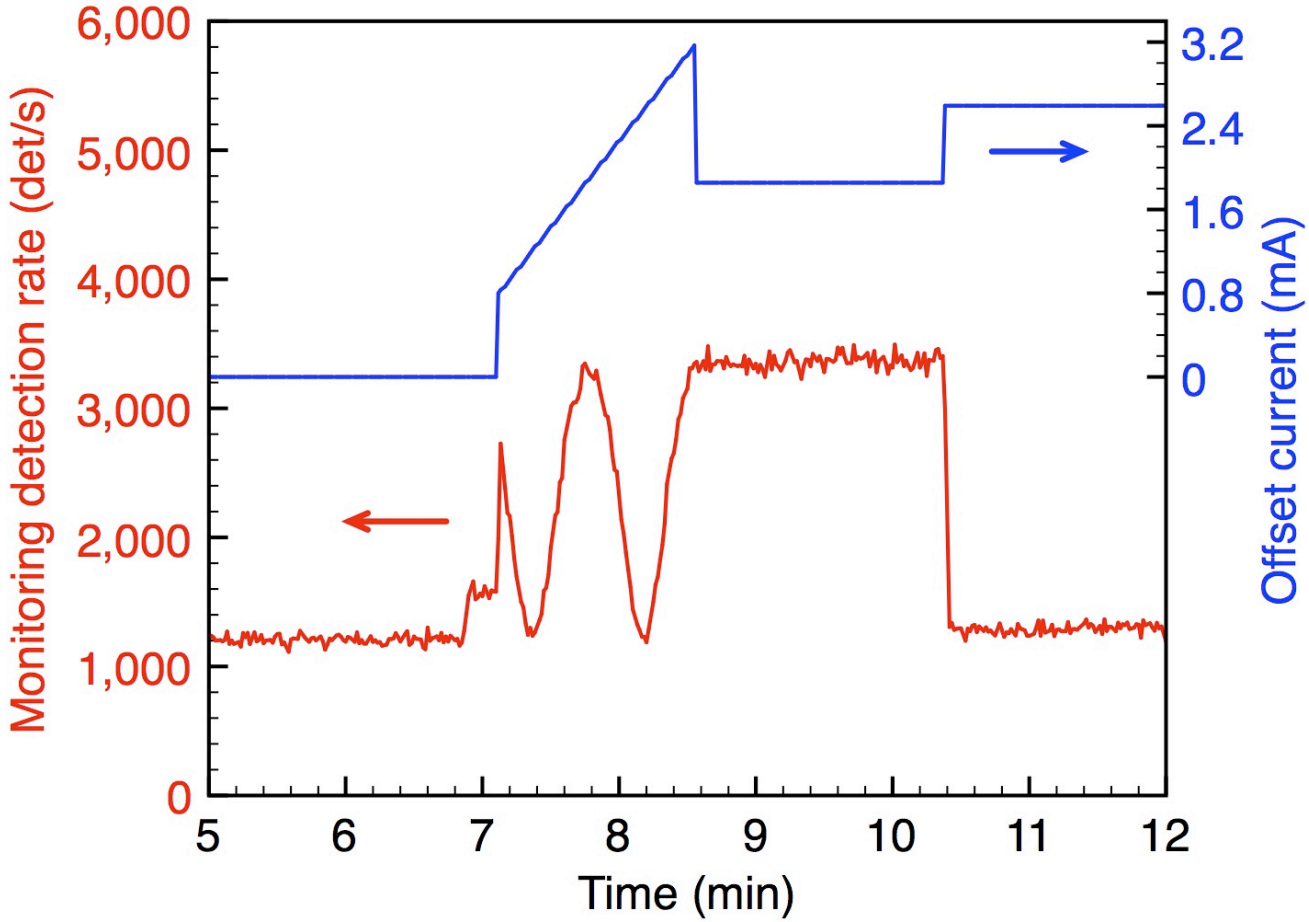
- Acknowledgments:
  Swisscom, University of Neuchâtel, Corning, NCCR quantum photonics, SINPHONIA

SSPD detector



- superconducting single photon detectors (SSPD) based on meandered NbN nano-wires
- cryogen-free, closed cycle, cryostat system
- temperature 2.5-2.8K

Monitoring



- Visibility larger than 95%
- InGaAs detector with 25km + 10dB