A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator

Boris Korzh,
Nino Walenta, Raphael Houlmann, Hugo Zbinden

GAP-Optique
University of Geneva

QCrypt Conference
Waterloo, Canada
August 8th 2013

QSIT Quantum Science and Technology
National Centre of Competence in Research

UNIVERSITÉ DE GENÈVE

FNSNF
SWISS NATIONAL SCIENCE FOUNDATION

Outline

UNIVERSITÉ DE GENÈVE

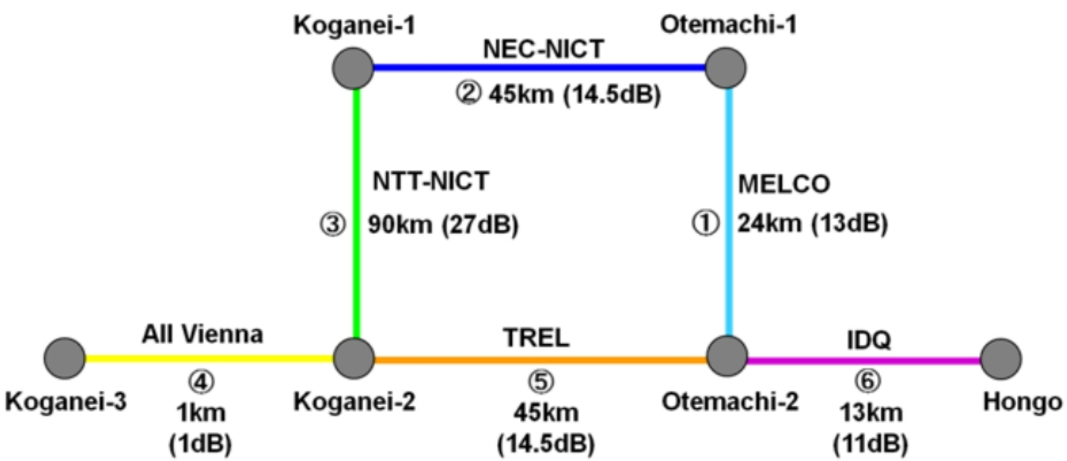
- Motivation
  - Network QKD
  - Possible need for multi-protocol capability
- Protocol overview
- State preparation
- Transmitter performance
  - Characterization
  - QKD
  - Stability
- Conclusion

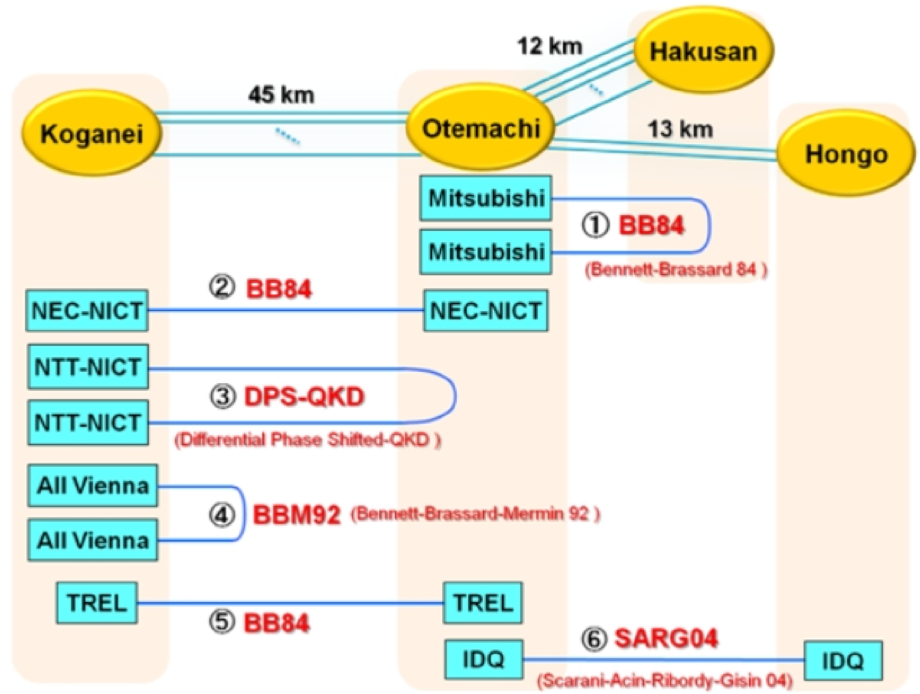
Motivation – Network QKD

UNIVERSITÉ DE GENÈVE

One approach

- Trusted nodes



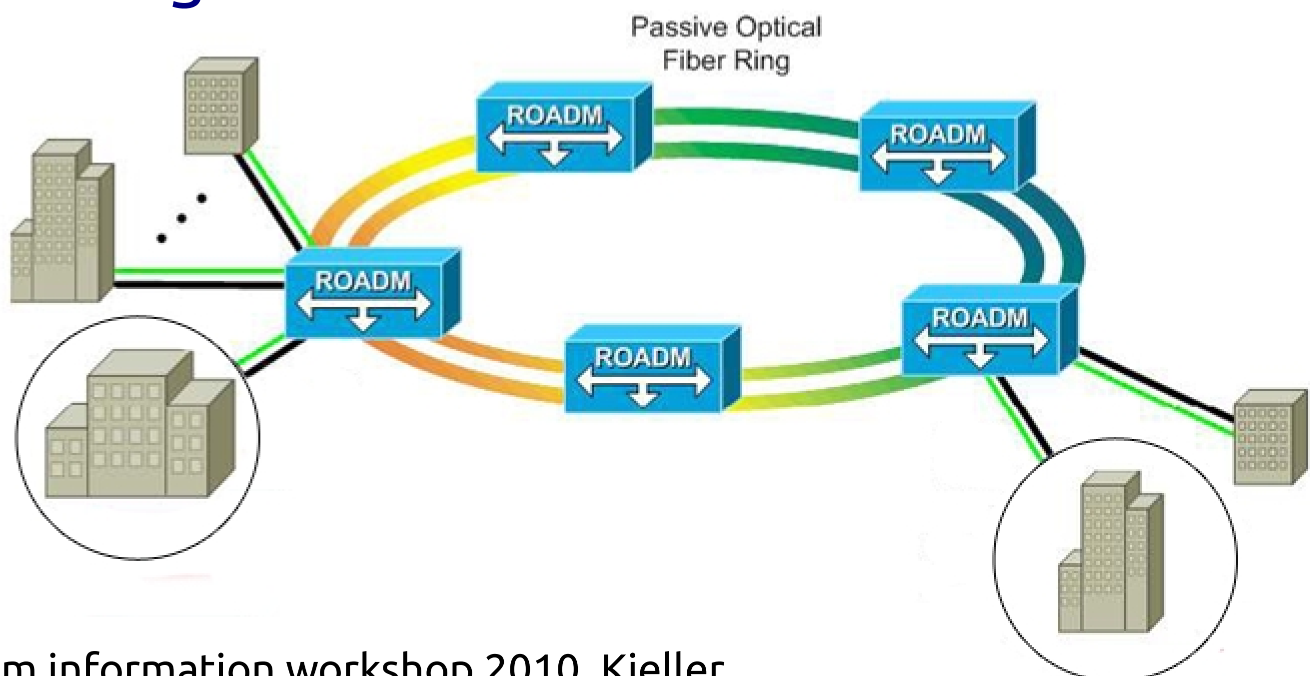


- M. Sasaki et. al., "*Field test of quantum key distribution in the Tokyo QKD network*," Opt. Express 19, 10387–10409 (2011)
- D. Stucki et. al., "*Long-term performance of the SwissQuantum quantum key distribution network in a field environment*," New J. Phys. 13, 123001 (2011)
- M. Peev, et. al., "*The SECOQC quantum key distribution network in Vienna*," New J. Phys. 11, 075001 (2009)

Reconfigurable Networks

UNIVERSITÉ DE GENÈVE

- No need for trusted nodes
- Active optical switching
- Passive optical switching

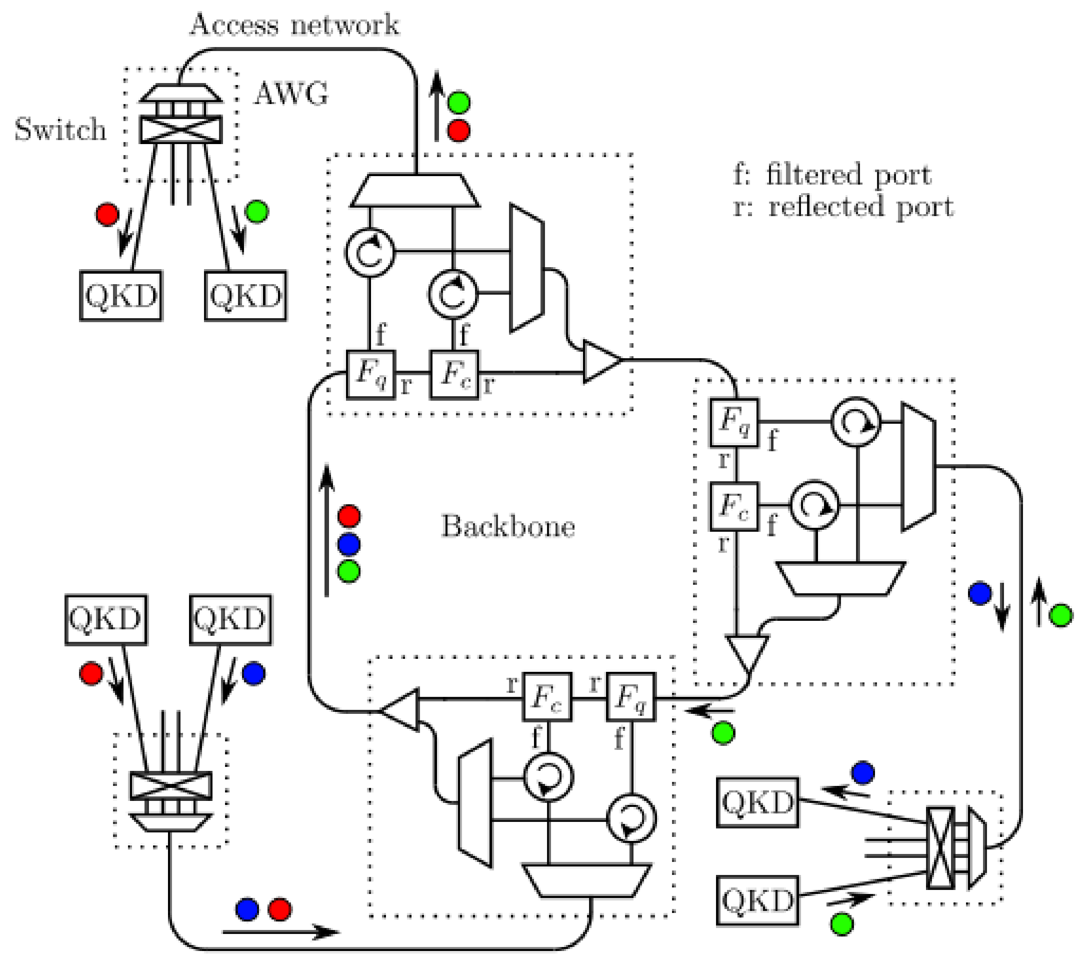


- Vicente Martín – Quantum information workshop 2010, Kjeller
- T. E. Chapuran, et. al., "*Optical networking for quantum key distribution and quantum communications*," New J. Phys. 11, 105001 (2009)
- D. Lancho, J. Martınez-Mateo, D. Elkouss, M. Soto, and V. Martin, "*QKD in standard optical telecommunications networks*," in 1st Int. Conf. on Quantum Communication and Quantum Networking (2010), vol. 36, pp. 142–149

Quantum Metro Network

UNIVERSITÉ DE GENÈVE

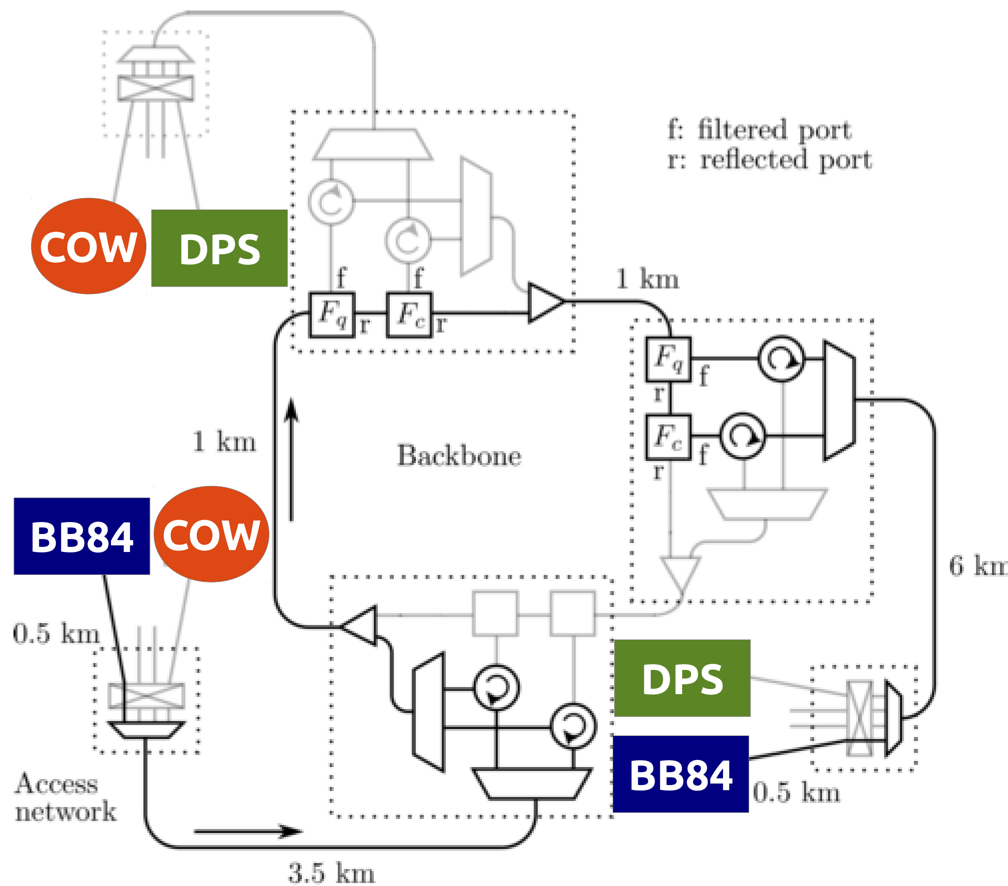
- Wavelength addressable
- All-to-all communication
- Resembles commercial optical networks
  - Core ring
  - Access network



Poster: A. Ciurana, J. Martinez-Mateo, A. Poppe, N. Walenta, H. Zbinden, and V. Martin, "*Quantum Metropolitan Area Network based on Wavelength Division Multiplexing*"

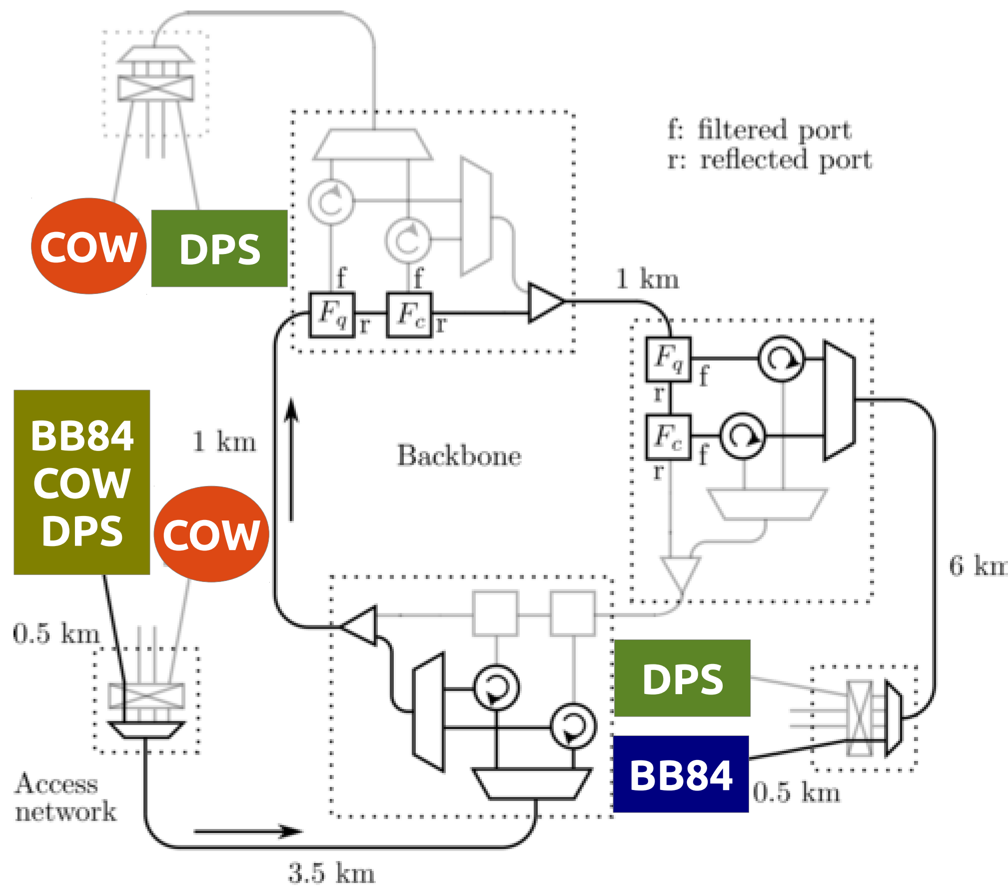
Different protocols?

- Different losses
  - Optimum protocol?
- Different environmental effects
- Commercial systems
  - Rarely the same
  - Patents
- So far systems require dedicated transmitters and receivers



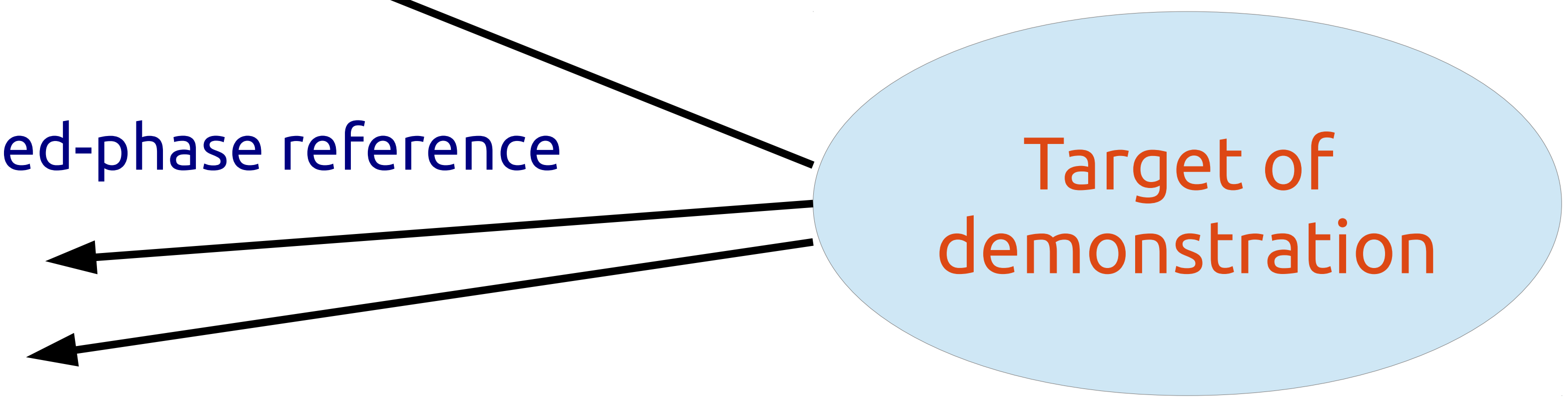
Different protocols?

- All people might want to communicate
- Potential need to move to multi-protocol capability
- Aim
  - Develop a multi-protocol transmitter



Families of Protocols

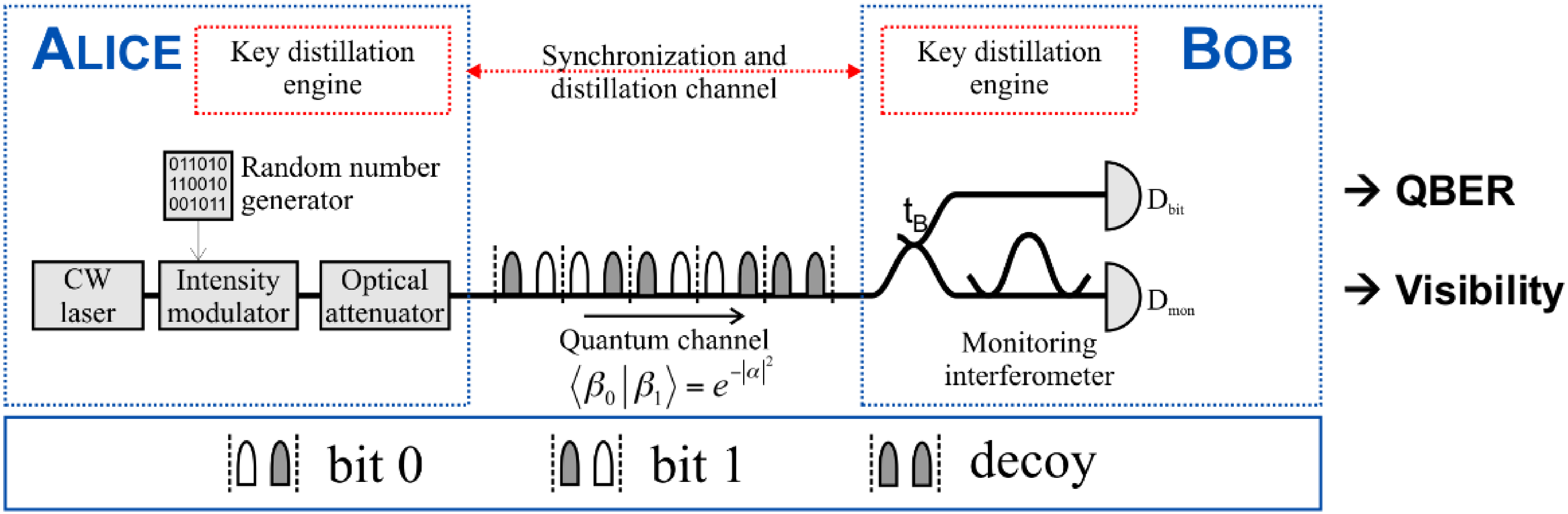
- Discrete variable
  - BB84
  - SARG
  - B92
- Distributed-phase reference
  - COW
  - DPS
- Continuous variable
- Measurement device independent
- Device independent



- V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, “*The security of practical quantum key distribution*,” Rev. Mod. Phys. 81, 1301–1350 (2009)

Coherent one-way

UNIVERSITÉ DE GENÈVE

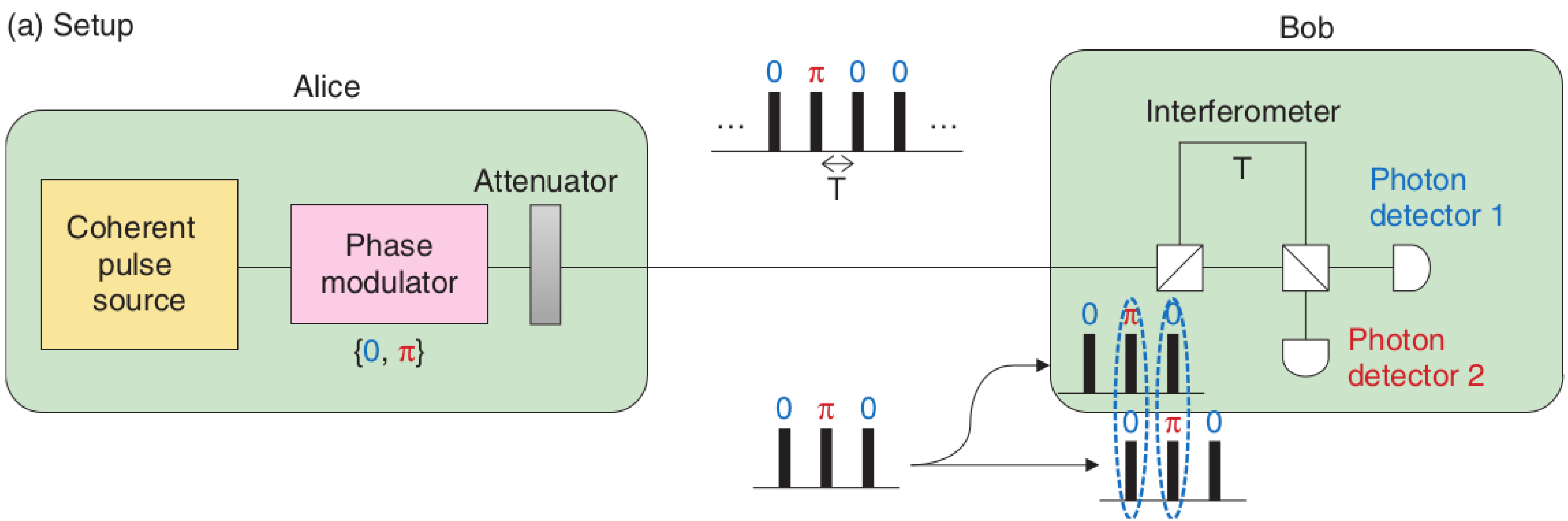


Live demonstration in the industrial exhibit area

- **Real-time post processing**
- **One-time pad encryption or 100 Gbps AES**

- D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "*Fast and simple one-way quantum key distribution*," Appl. Phys. Lett. 87, 194108 (2005)
- C. Branciard, N. Gisin, and V. Scarani, "*Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography*," New J Phys. 10, 013031 (2008)

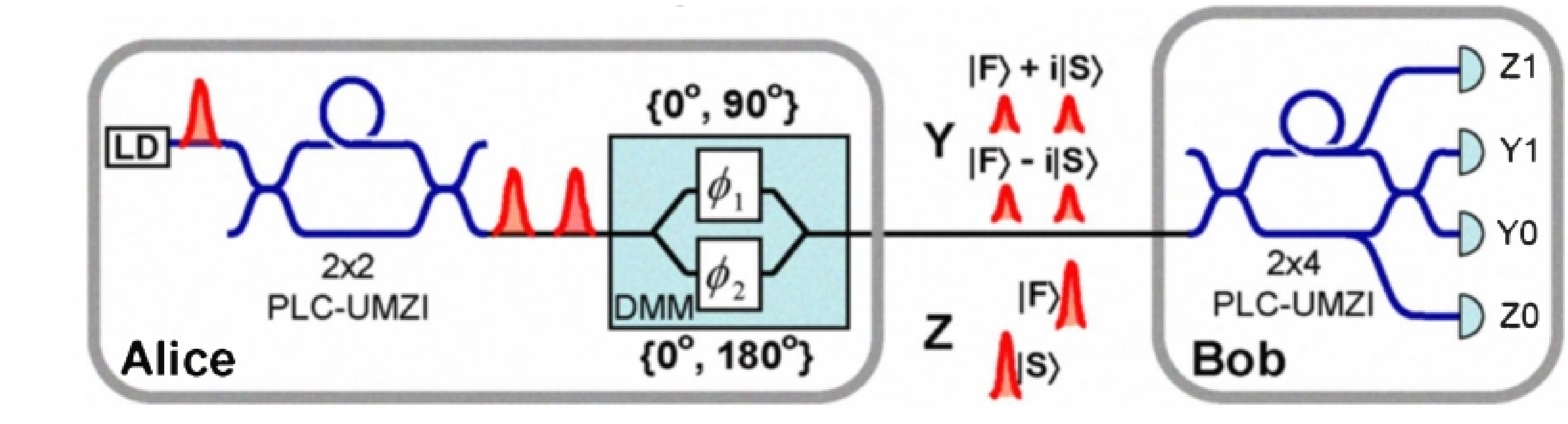
Differential phase shift



- CW laser with pulse carver or mode-locked laser required

- K. Inoue, E. Waks, and Y. Yamamoto, "*Differential phase shift quantum key distribution*," Phys. Rev. Lett. 89, 037902 (2002)
- Yasuhiro Tokura and Toshimori Honjo, "*Differential Phase Shift Quantum Key Distribution (DPS-QKD) Experiments*", NTT Technical review, www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201109fa8.html

Time-phase BB84

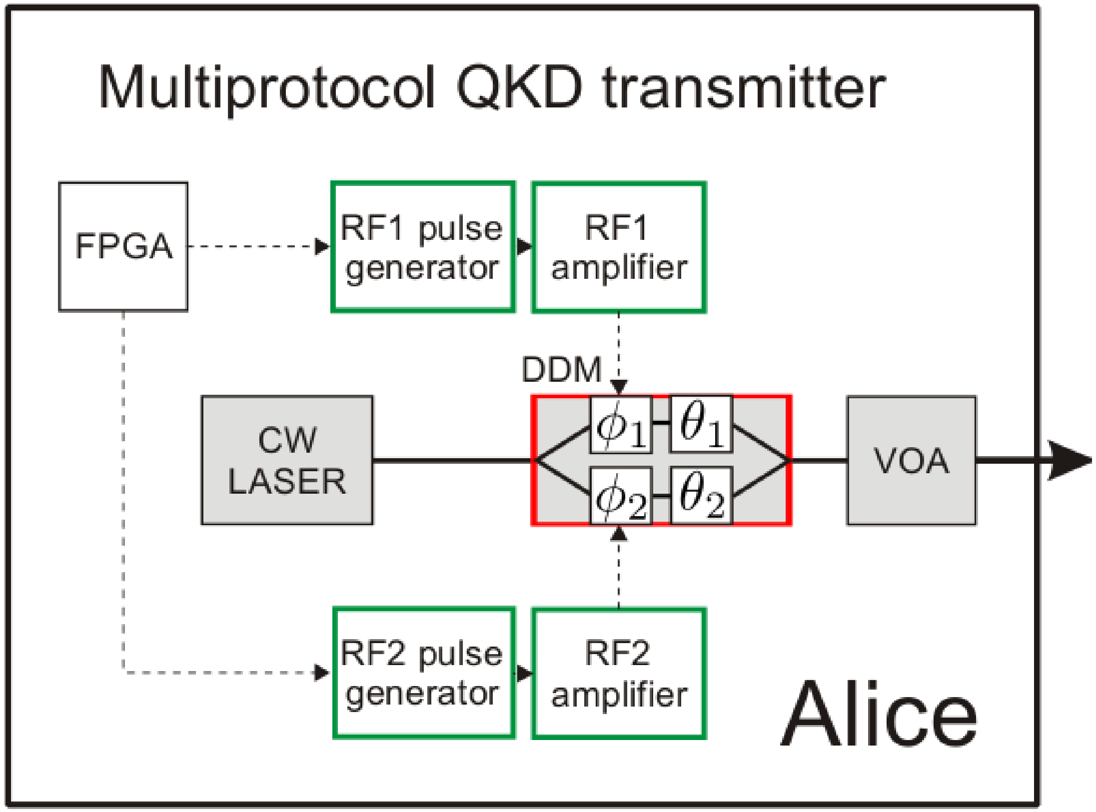


- Requires matched interferometers at Alice and Bob
- Inherently phase randomized

- K. Yoshino, et. al., "*Dual-mode time-bin coding for quantum key distribution using dual-drive Mach-Zehnder modulator*," in 33rd European Conference and Exhibition of Optical Communication (ECOC, 2007), pp. 1–2 (2007)
- K. Yoshino, et. al. "*High-speed wavelength-division multiplexing quantum key distribution system*," Opt. Lett. 37, 223–225 (2012)
- A. Tomita, et. al., "*High speed quantum key distribution system*," Opt. Fiber Technol. 16, 55 – 62 (2010)

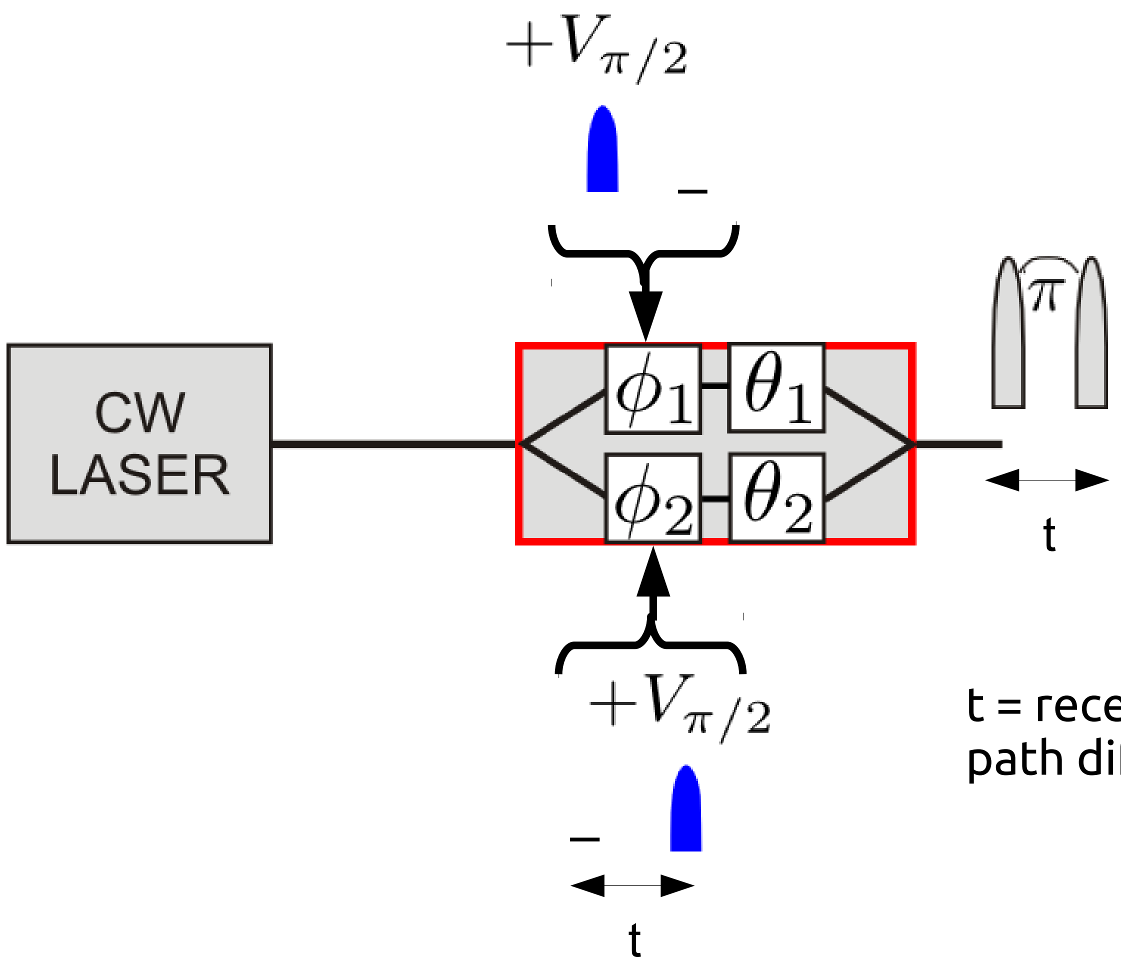
New transmitter

- Simplified version
- 1 Electo-optic modulator
  - Phase and intensity control
- No interferometer at Alice



Dual-drive modulator

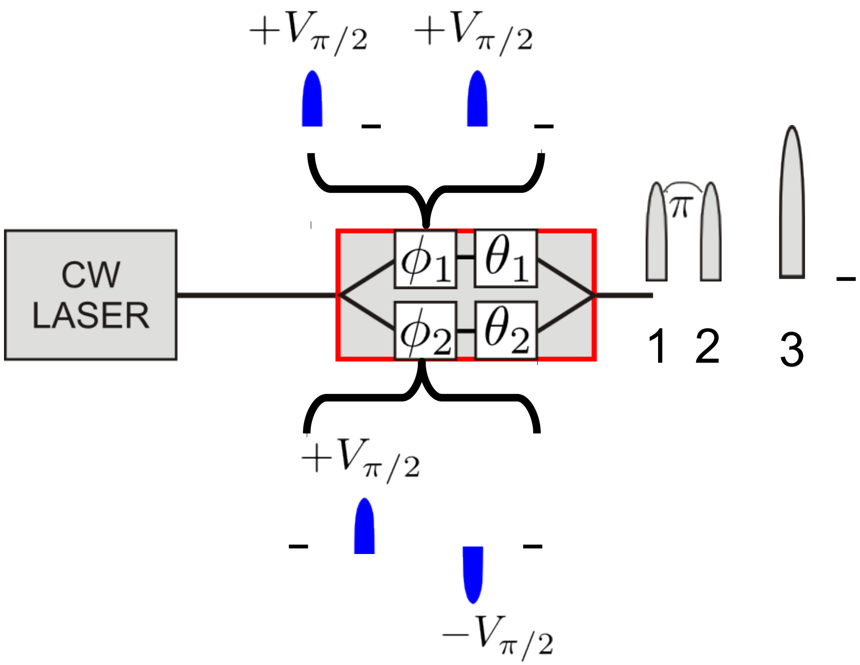
UNIVERSITÉ DE GENÈVE

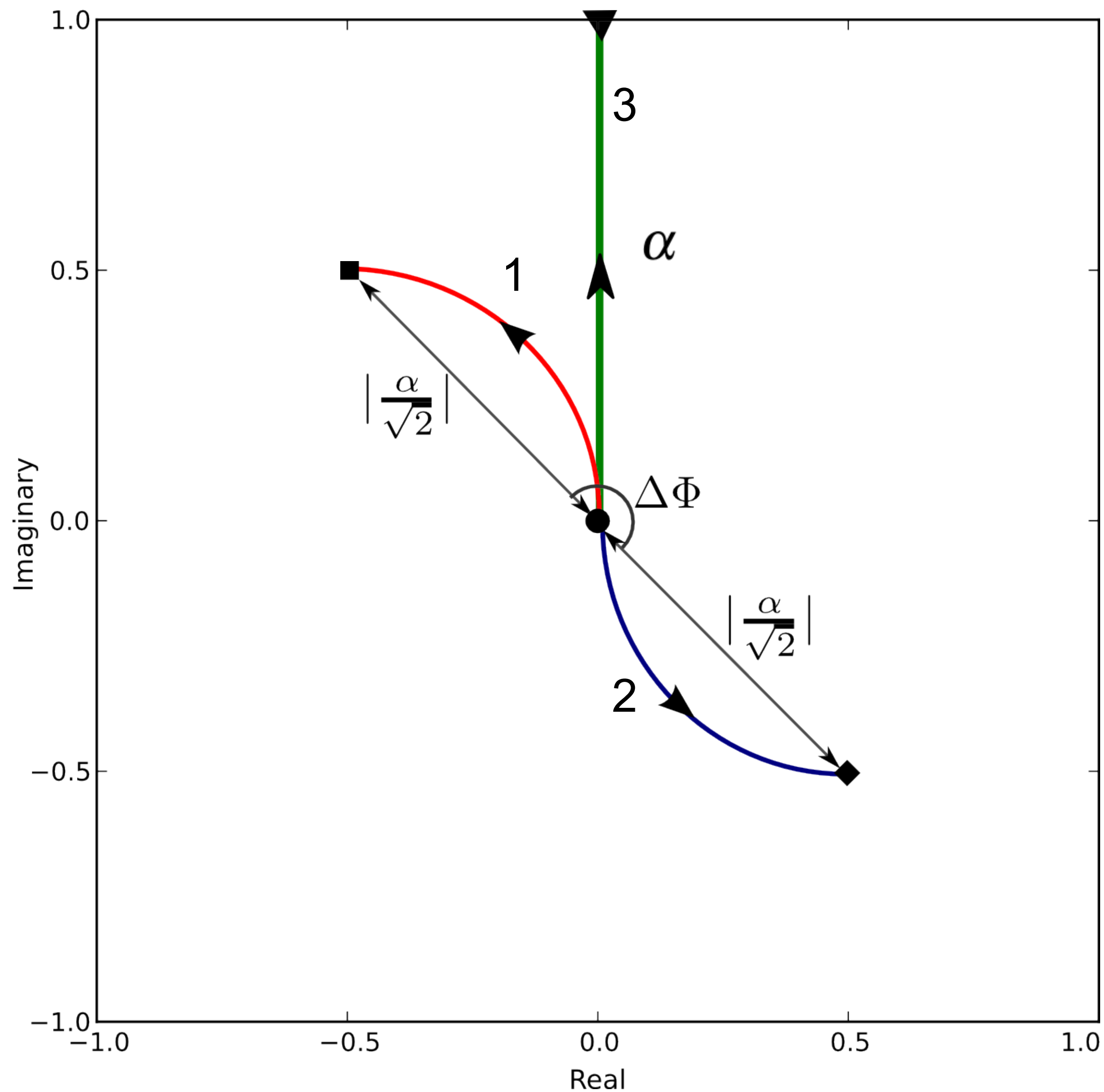


t = receiver interferometer path difference

$$|\alpha\rangle \rightarrow = e^{i\left(\frac{\theta_1+\theta_2+\phi_1+\phi_2}{2}\right)} \cdot \cos\left(\frac{\theta_1-\theta_2+\phi_1-\phi_2}{2}\right)|\alpha\rangle$$

State preparation

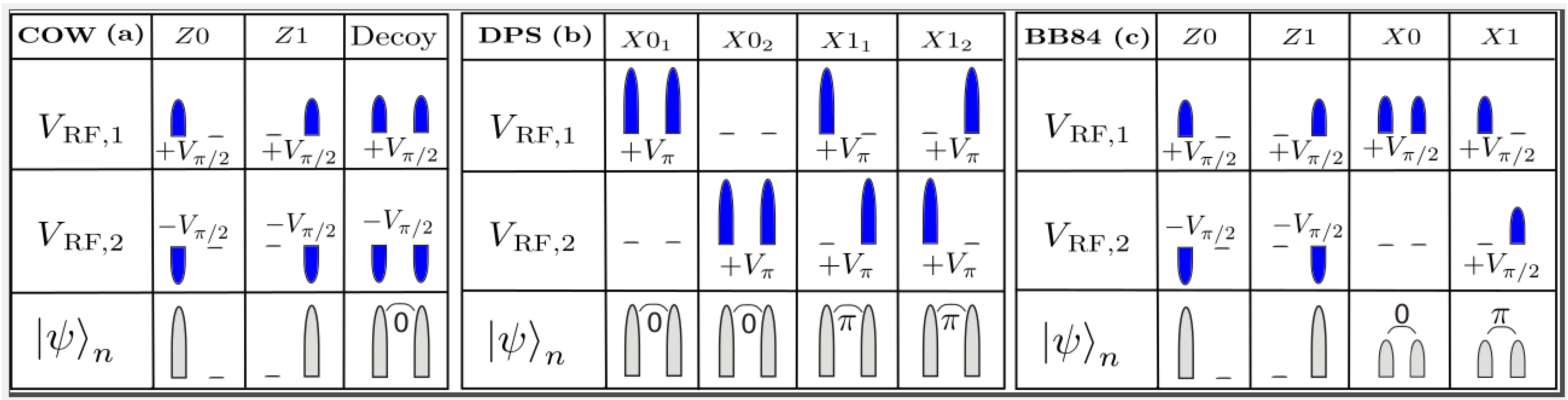




$$Re[\psi] = \frac{1}{2}\left[\cos\phi_1 - \cos\phi_2\right]$$

$$Im[\psi] = \frac{1}{2}\left[\sin\phi_1 - \sin\phi_2\right].$$

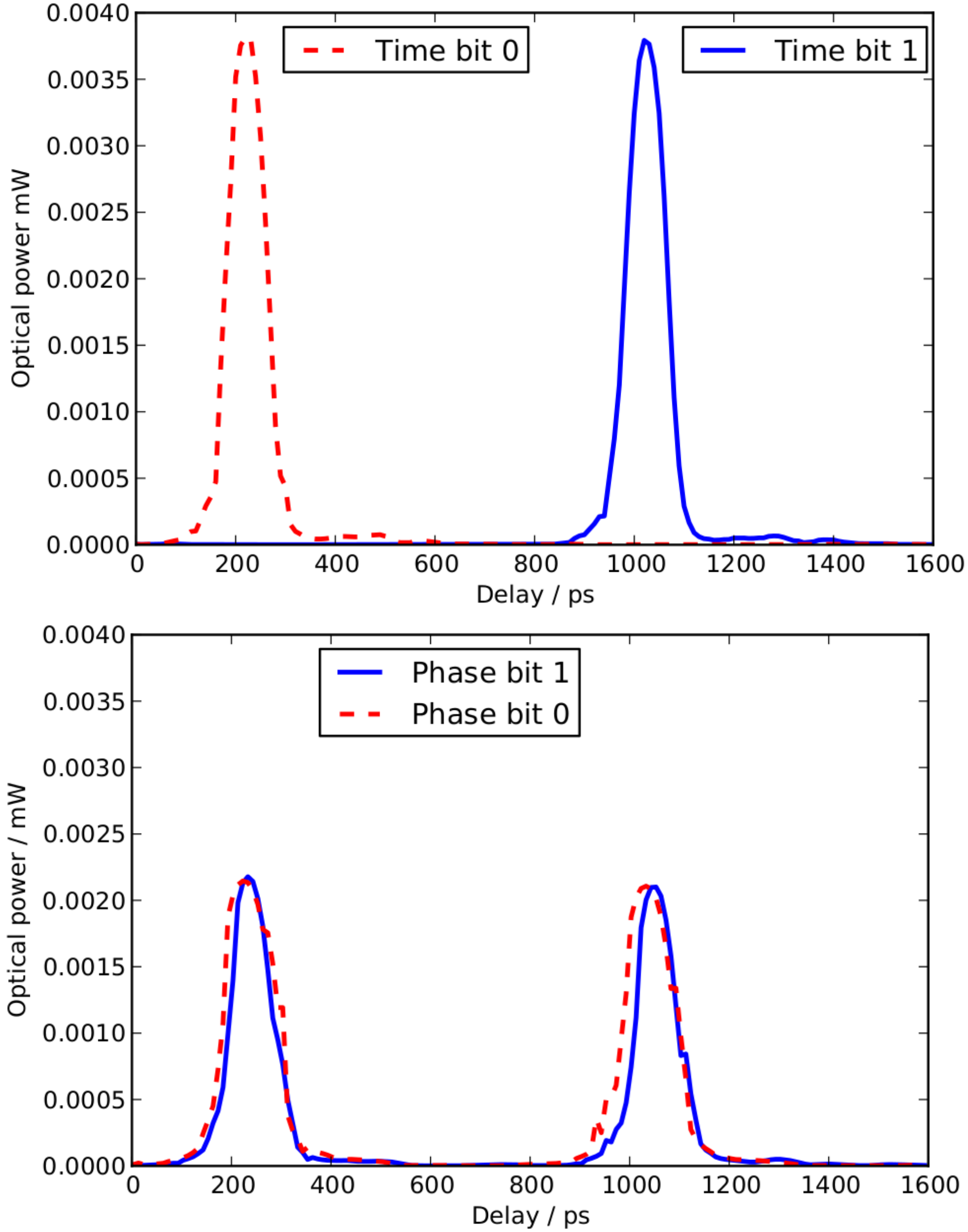
Coding scheme



- All states necessary can be produced

Pulse shape

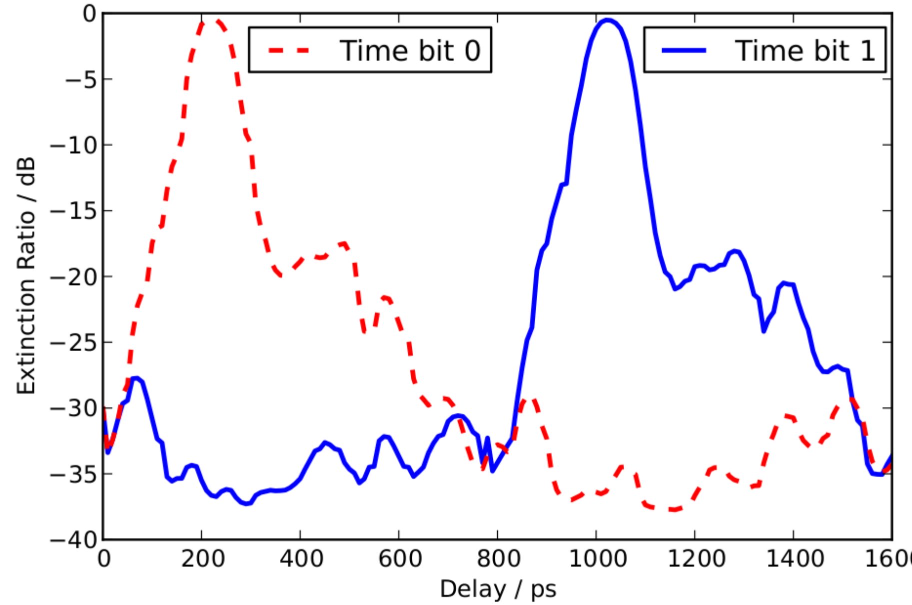
- Pulses after the dual-drive modulator
- 90 ps (fwhm)
- Linear scale

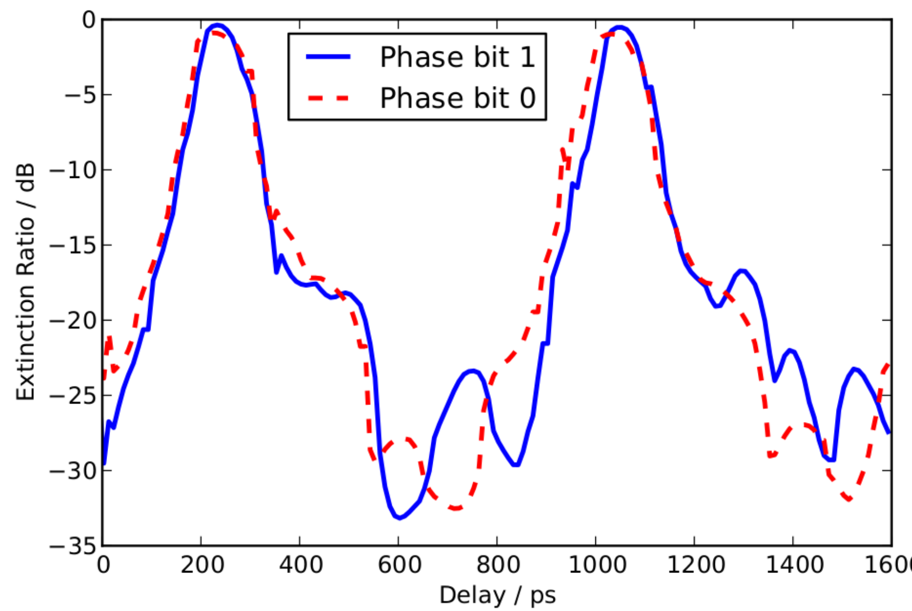


Pulse shape

UNIVERSITÉ DE GENÈVE

- Extinction ratio
  - >27 dB
  - Less than 0.2% QBER in time basis
- Logarithmic scale

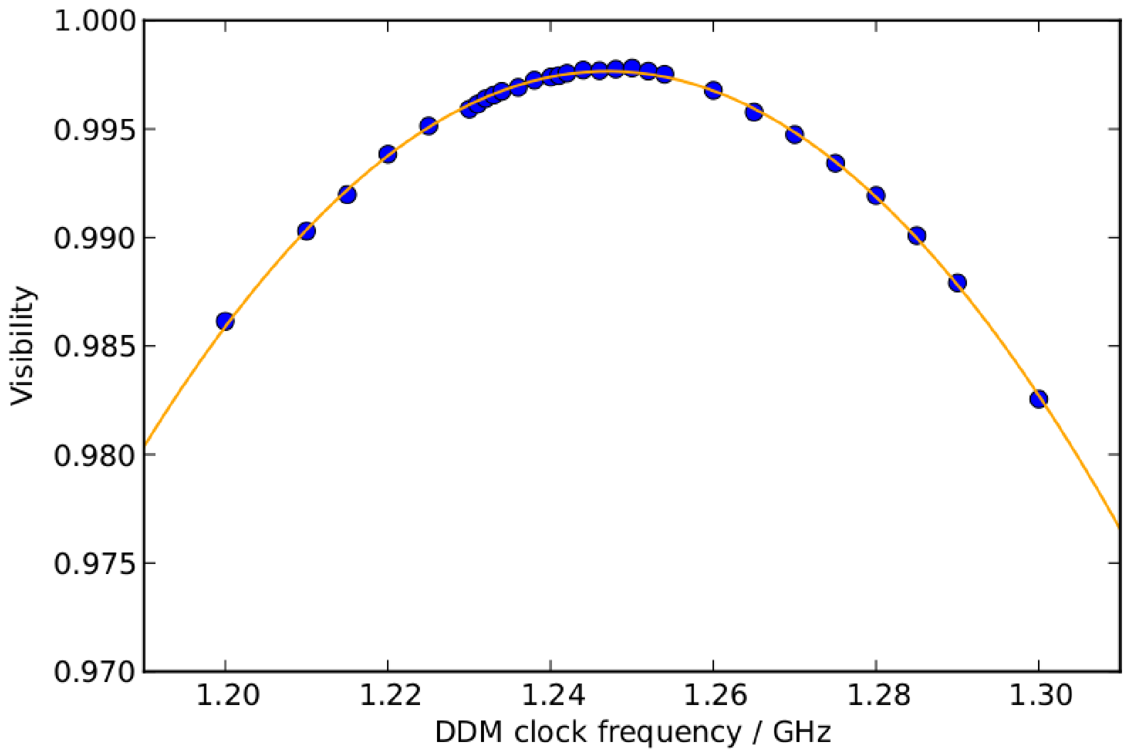




Clock frequency optimization

UNIVERSITÉ DE GENÈVE

- 20 MHz clock accuracy corresponds to
  - 0.01% QBER

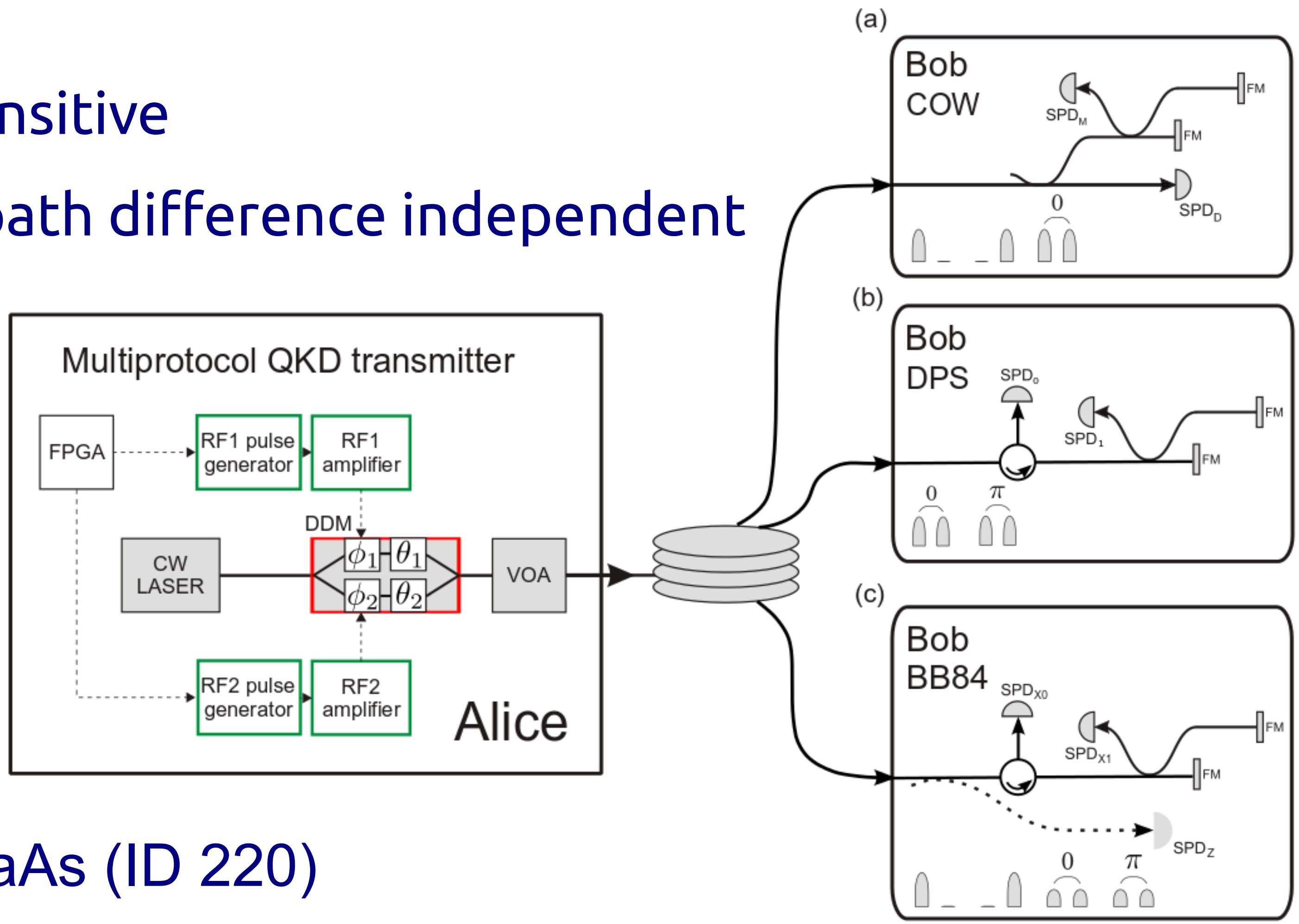


Multi-protocol test platform

UNIVERSITÉ DE GENÈVE

Specifications

- Polarization insensitive
- Interferometer path difference independent



Detectors

- Free running InGaAs (ID 220)

- T. Lunghi, C. Barreiro, O. Guinnard, R. Houlmann, X. Jiang, M. A. Itzler, and H. Zbinden,“*Free-running single-photon detection based on a negative feedback InGaAs APD*,” J. Mod. Opt. 59, 1481–1488 (2012)

QKD engine

UNIVERSITÉ DE GENÈVE

Sifting	Timing and base information
Error estimation	Direct comparison or sampling
Error correction	LDPC forward error correction
Error verification	Universal hashing
Privacy amplification	Toeplitz hashing
Authentication	Polynomial hashing

- 1.25 GHz
- FPGA distillation engine

- Block length 10^6
- Most tasks are protocol independent

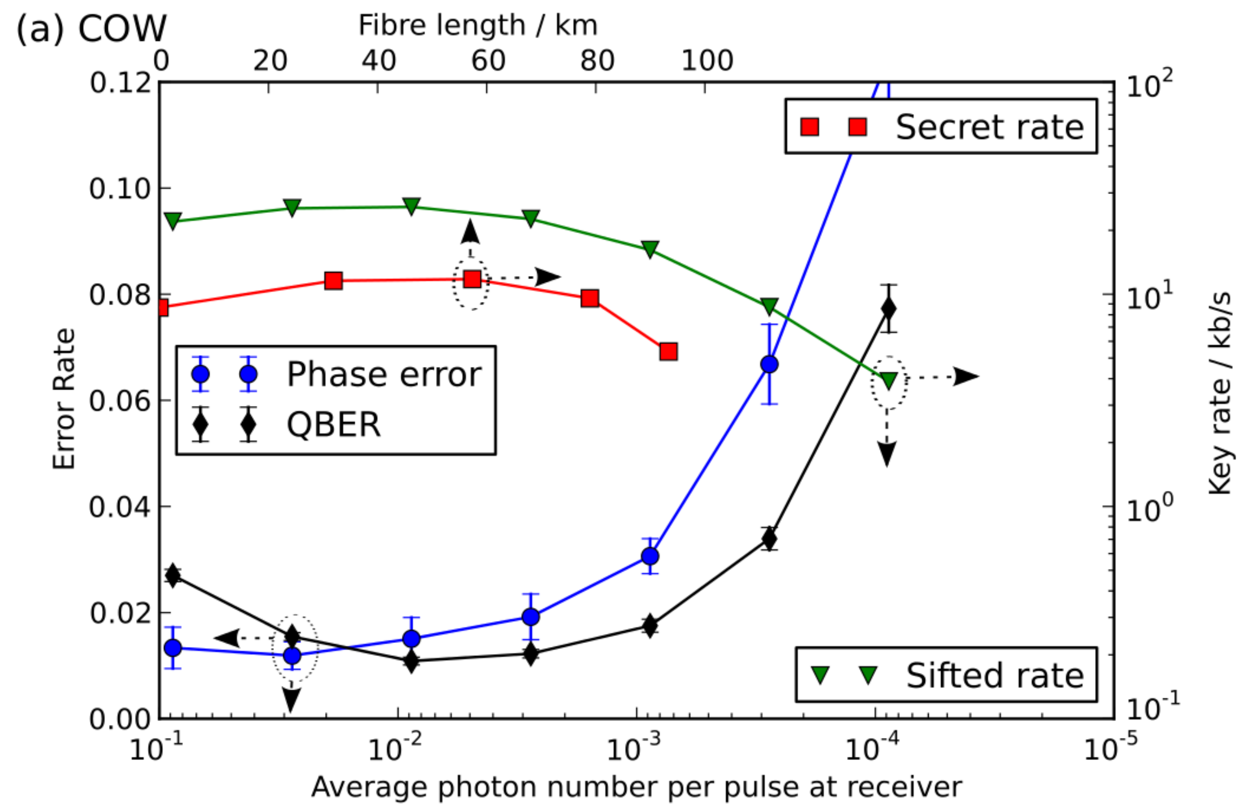
Poster: Nino Walenta, et. al. "*Continuous coherent-one way QKD and data encryption at up to 100 Gbits/s*", Industrial exhibit area, QCrypt 2013.

COW performance

UNIVERSITÉ DE GENÈVE

With dark counts

- QBER < 1.5%
- Phase error < 2%



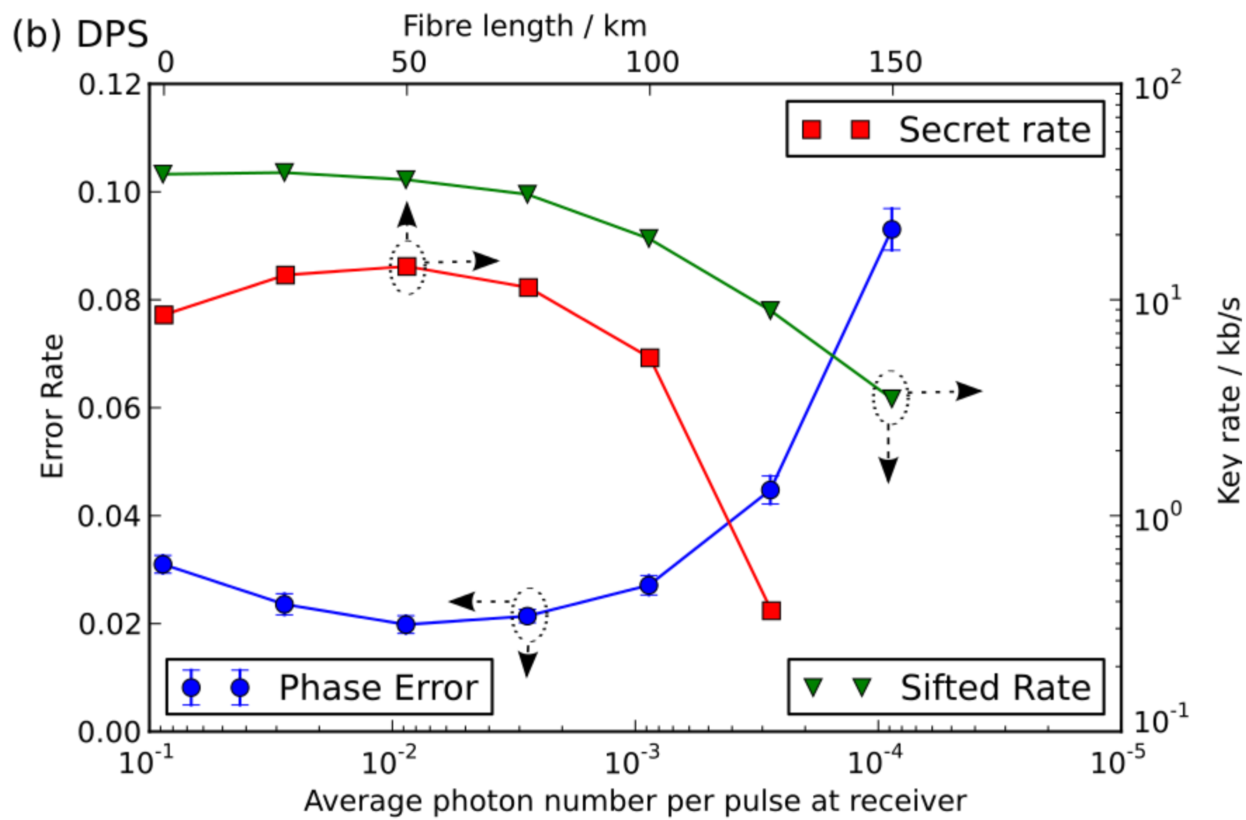
- C. Branciard, N. Gisin, and V. Scarani, "*Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography*," New J Phys. 10, 013031 (2008)
- M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "*Tight finite-key analysis for quantum cryptography*," Nature Commun. 3 (2012)

DPS performance

UNIVERSITÉ DE GENÈVE

With dark counts

- Phase error 2% (min)



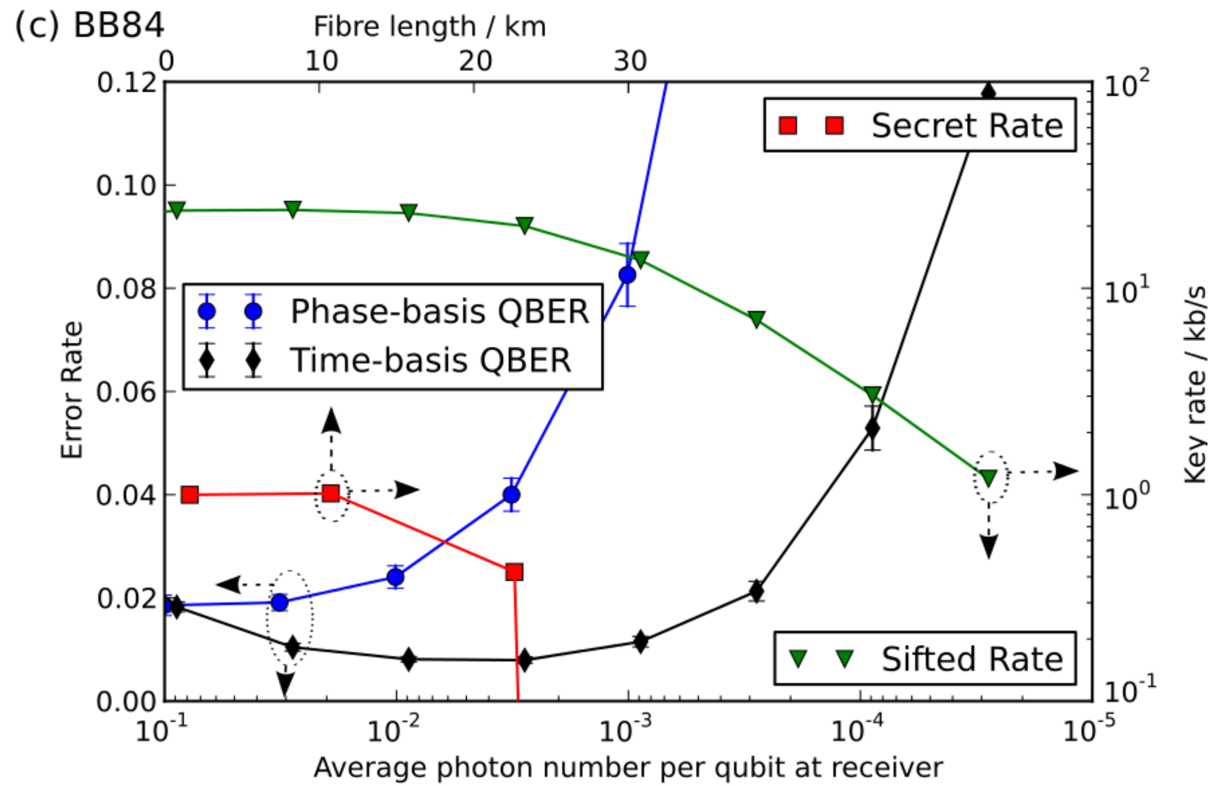
- E. Waks, H. Takesue, and Y. Yamamoto, "*Security of differential-phase-shift quantum key distribution against individual attacks*," Phys. Rev. A 73, 012344 (2006)

BB84 Performance

UNIVERSITÉ DE GENÈVE

With dark counts

- QBER < 1%
- Phase error < 2%



- H.-K. Lo and J. Preskill, "*Security of quantum key distribution using weak coherent states with nonrandom phases*," Quantum Info. Comput. 7, 431–458 (2007)

Optical QBER

UNIVERSITÉ DE GENÈVE

Measure of transmitter performance

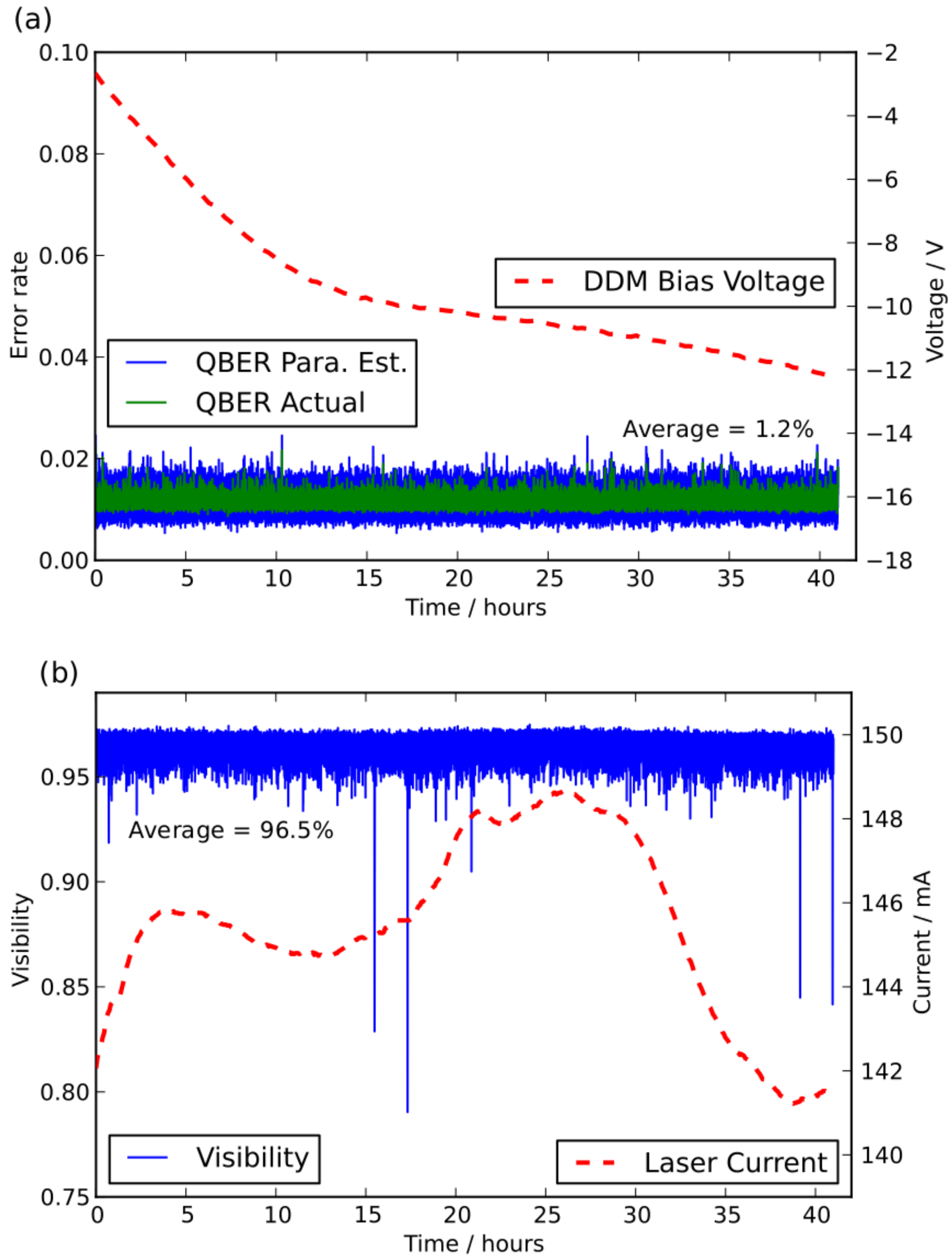
- Subtracting dark counts

Protocol	Phase basis $QBER_{opt}$	Time basis $QBER_{opt}$
DPS	$1.83 \pm 0.19\%$	N/A
COW	$0.92 \pm 0.41\%$	$0.89 \pm 0.08\%$
BB84	$1.51 \pm 0.16\%$	$0.58 \pm 0.06\%$

System stability

Automatic tracking of QBER and Visibility

- Modulator bias voltage
- Laser current



Conclusion

UNIVERSITÉ DE GENÈVE

- Demonstrated multi-protocol transmitter
  - No interferometer
  - 1.25 GHz (flexible)
    - Crucial for addressing different receivers
  - Easily stabilized
  - Performance comparable to protocol dedicated transmitters
- Further development
  - Decoy state preparation
  - Phase randomization
  - Full integration with high speed QKD platform

Thank you

Nino Walenta
Raphael Houlmann
Olivier Guinnard
Charles Ci Wen Lim
Hugo Zbinden

Antonio Ruiz-Alba

arXiv:1306.5940 [quant-ph]

To be published in Optics Express

QSIT Quantum Science and Technology
National Centre of Competence in Research

UNIVERSITÉ DE GENÈVE

IDQ FROM VISION TO TECHNOLOGY

nano-tera.ch
swiss scientific initiative in health / security / environment systems

FNSNF
SWISS NATIONAL SCIENCE FOUNDATION