Experimental Quantum Key Distribution: Status and Directions

Gregor Weihs

IQC Institute for Quantum Computing

University of Waterloo

Group

Post-Doc: Christophe Couteau

Graduate Students: Chris Erven
Rolf Horn
Devin Smith

Collaborations

Fabrication: Jayshri Sabarinathan (University of Western Ontario, London)

Materials: Robin Williams (NRC Ottawa)
Glenn Solomon (NIST Gaithersburg)
Chang-Qing Xu (McMaster University, Hamilton)

Funding

Canada Foundation for Innovation
Fondation canadienne pour l'innovation

NSERC
CRSNG

CIAR

ONTARIO PHOTONICS CONSORTIUM

Contents

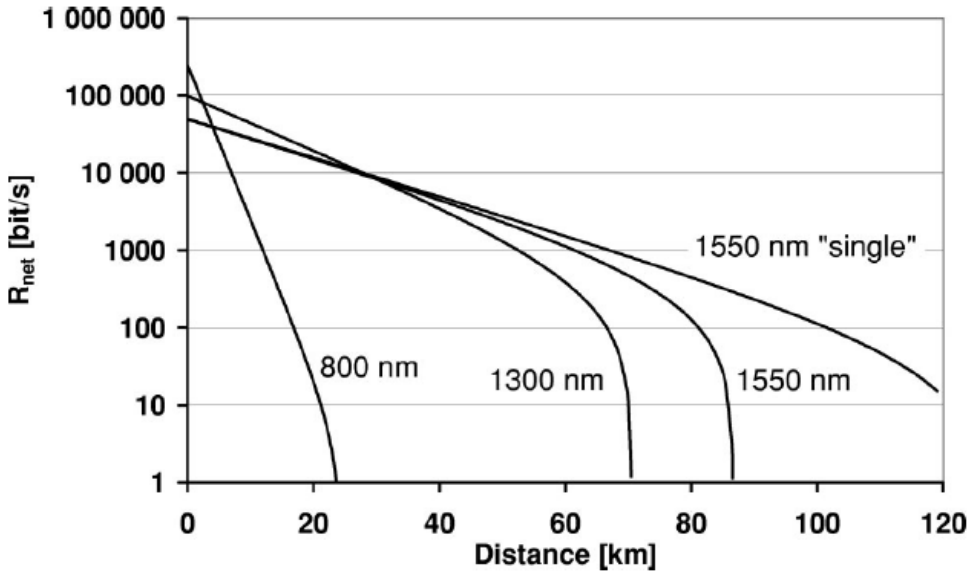
University of Waterloo

- Experimental Challenges
  - Photon Encoding
  - Channels
  - Components
- Complete implementations: Going the distance
  - Fiber
  - Free space
  - Towards satellites…
- The IQC-PI QKD experiment

Towards Long-Haul QKD

University of Waterloo

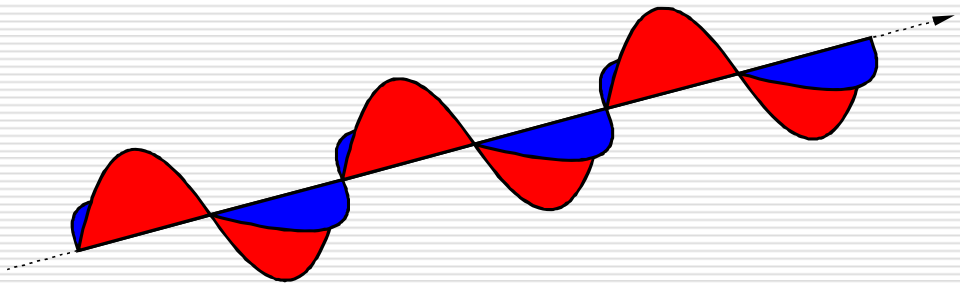
- ***Photons***
  - Polarization
  - Time
  - Path
- Channels
  - Optical Fibers
  - Free-Space (Telescopes)
    ➔ Satellites
- Sources
  - Faint lasers
  - Single photons
- Detectors
  - Si-APDs
  - InGaAs APDs
  - Superconducting

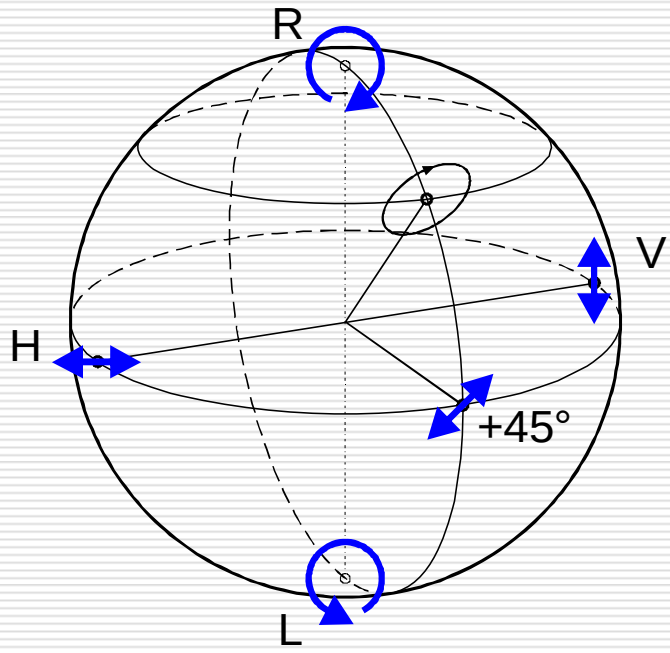


Gisin et al., RMP ***74,*** 145 (2002)

Photon Polarization

- Every mode has two orthogonal polarizations (directions of the electric field)
- Arbitrary polarization states are superpositions
- Classically, polarization is described on the Poincaré sphere

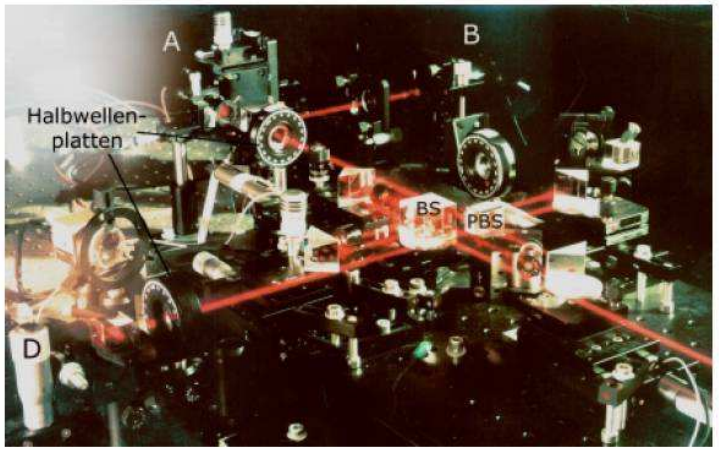




The Dual Rail Qubit

In theory

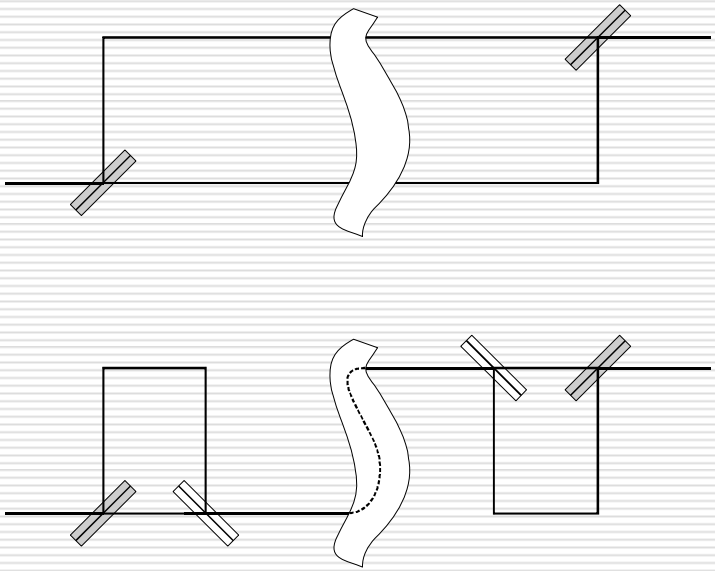
In experiment

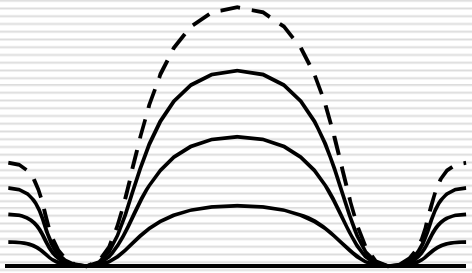


The time-bin qubit

University of Waterloo

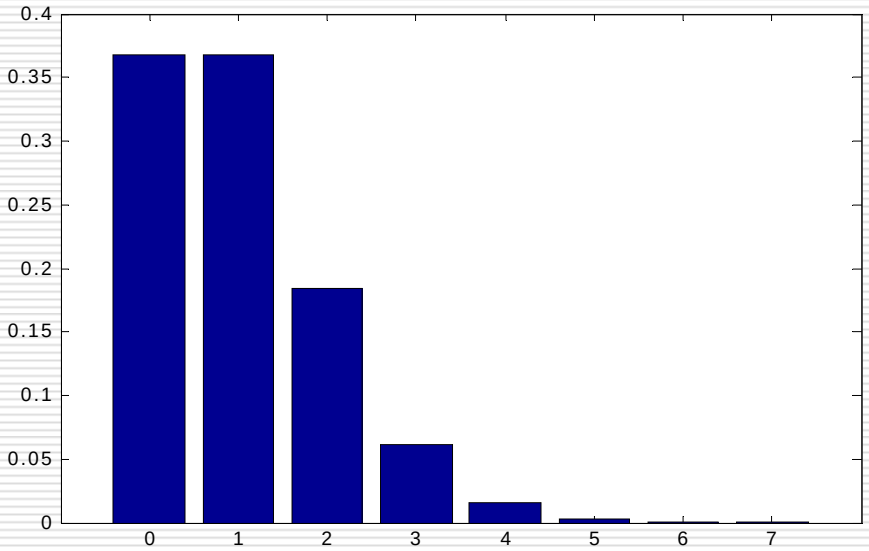
For stability one can multiplex the two rails onto one.



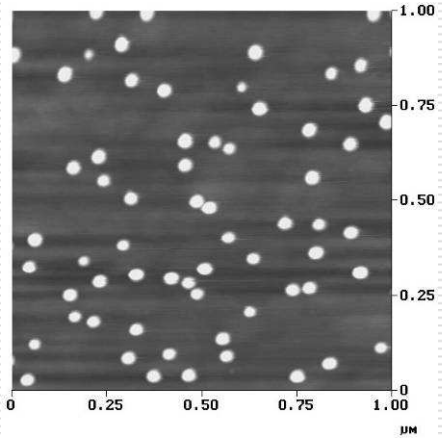


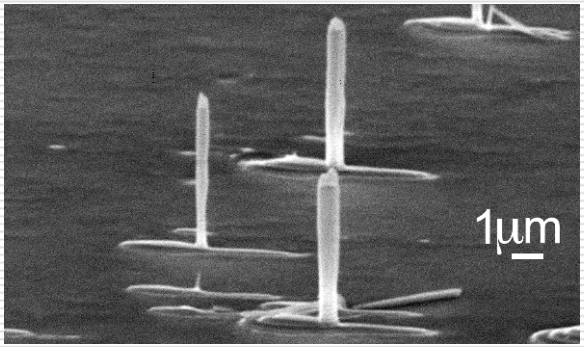
Sources

- Attenuated lasers: poissonian statistics



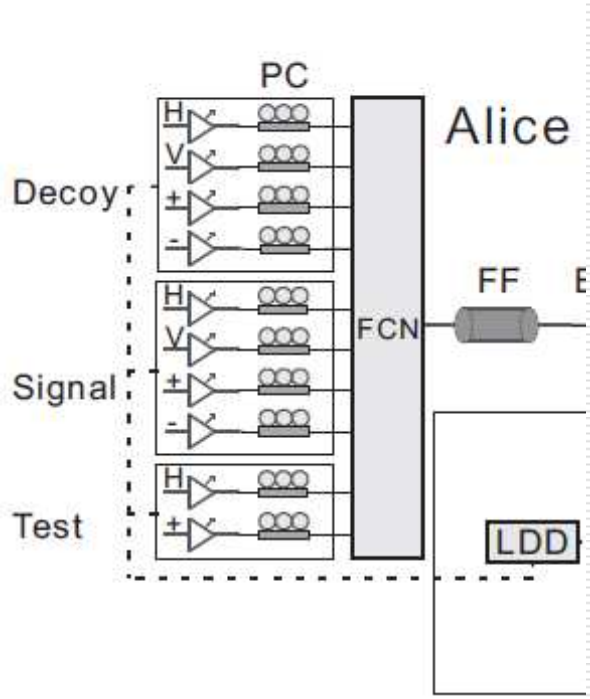
- Single photons: quantum dots, single mocecules, color centers in diamond, trapped atoms



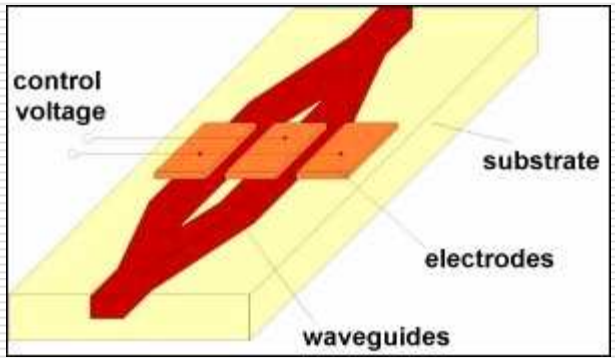


Modulation

- Combine multiple lasers and pulse them individually
  - Beware of side channels!



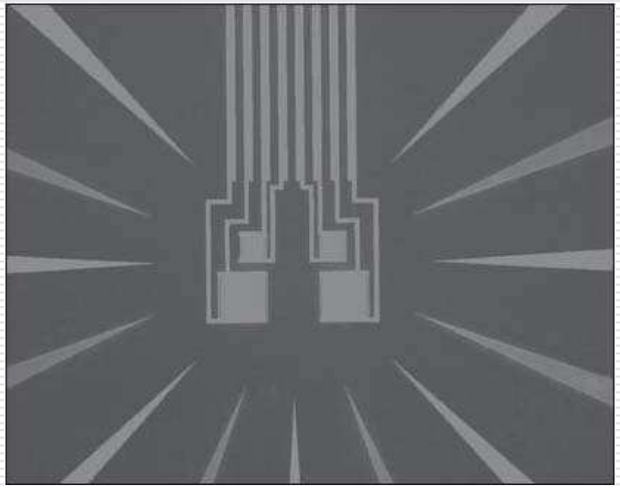
- Modulate laser
  - Polarization
  - Phase (commercially up to 40 GHz)
  - Amplitude for decoy



Some Facts About Detectors

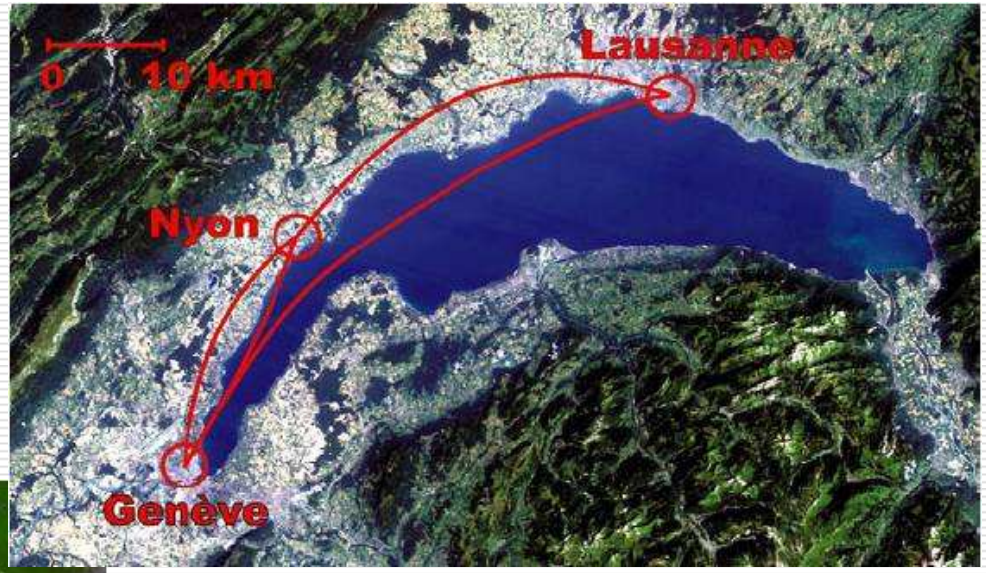
- Detection efficiency = Quantum efficiency * Amplification efficiency
- For red / very near infrared light about 70%, ~10 /s noise
- Most common:
  Single Photon Avalanche Diode (SPAD)

- For telecommunication wavelengths (1550 nm): InGaAs APDs have <15% efficiency, some 10000 /s noise counts
- Alternative detectors
  - Visible Light Photon Counter
  - Superconducting Transition Edge Detector



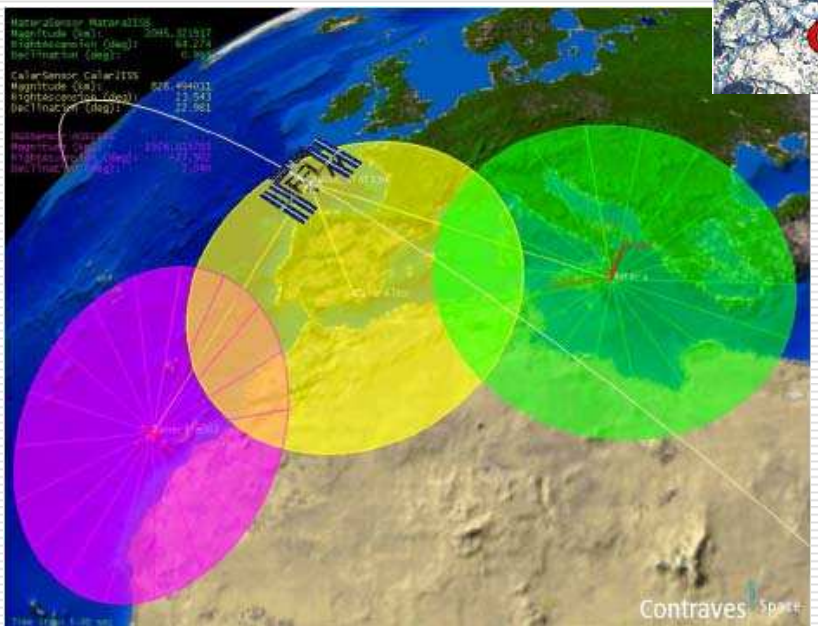
Channels

- Guide light in single-mode optical fibers



GAP-Optique, U. Geneva

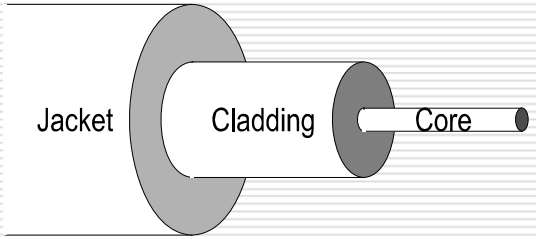
Pfennigbauer et al., JON ***4,*** 549 (2005)

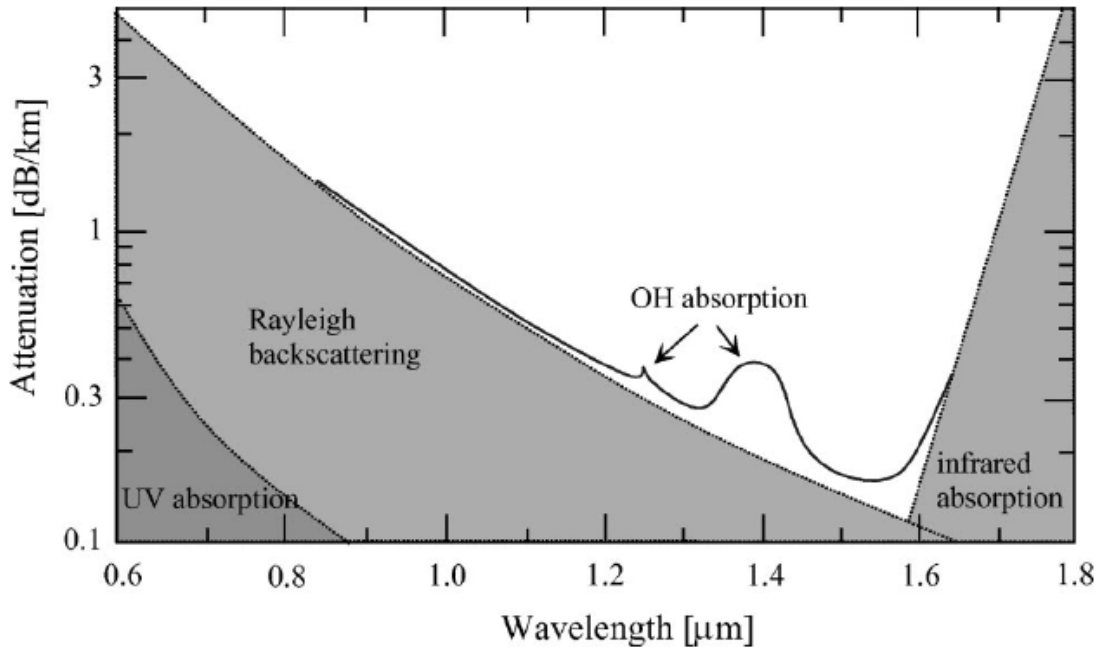


- Broadcast photons from a satellite using telescopes

Optical Fibers

- Fused silica core guides light
- Attenuation by Rayleigh scattering
- Minimum @1550 nm: 0.17 dB/km = 4%/km loss
- Installed fiber typically has 0.3 dB/km
- Polarization
  - Birefringence needs to be compensated
  - Depolarization due to different group velocities (~√L)

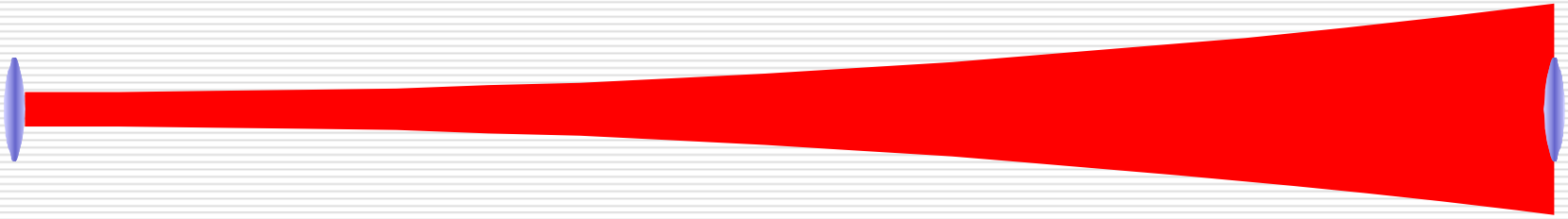




Gisin et al., RMP ***74,*** 145 (2002)

Free-Space Optical Links

University of Waterloo



- Send photons through air in "beam"
- Diffraction causes beam to spread ($\sim L^2$)
- Turbulence causes beam wander
  - ➔ Can be incorporated as additional diffraction
- Scattering causes exponential attenuation

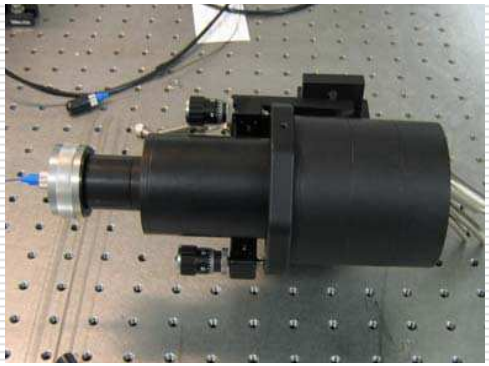
$$A = \frac{L^2(\theta_T^2 + \theta_{atm}^2)}{D_R^2} 10^{\frac{A_{atm}}{10}}$$

Telescopes

G. Bianco: *The Matera Laser Ranging Observatory System*

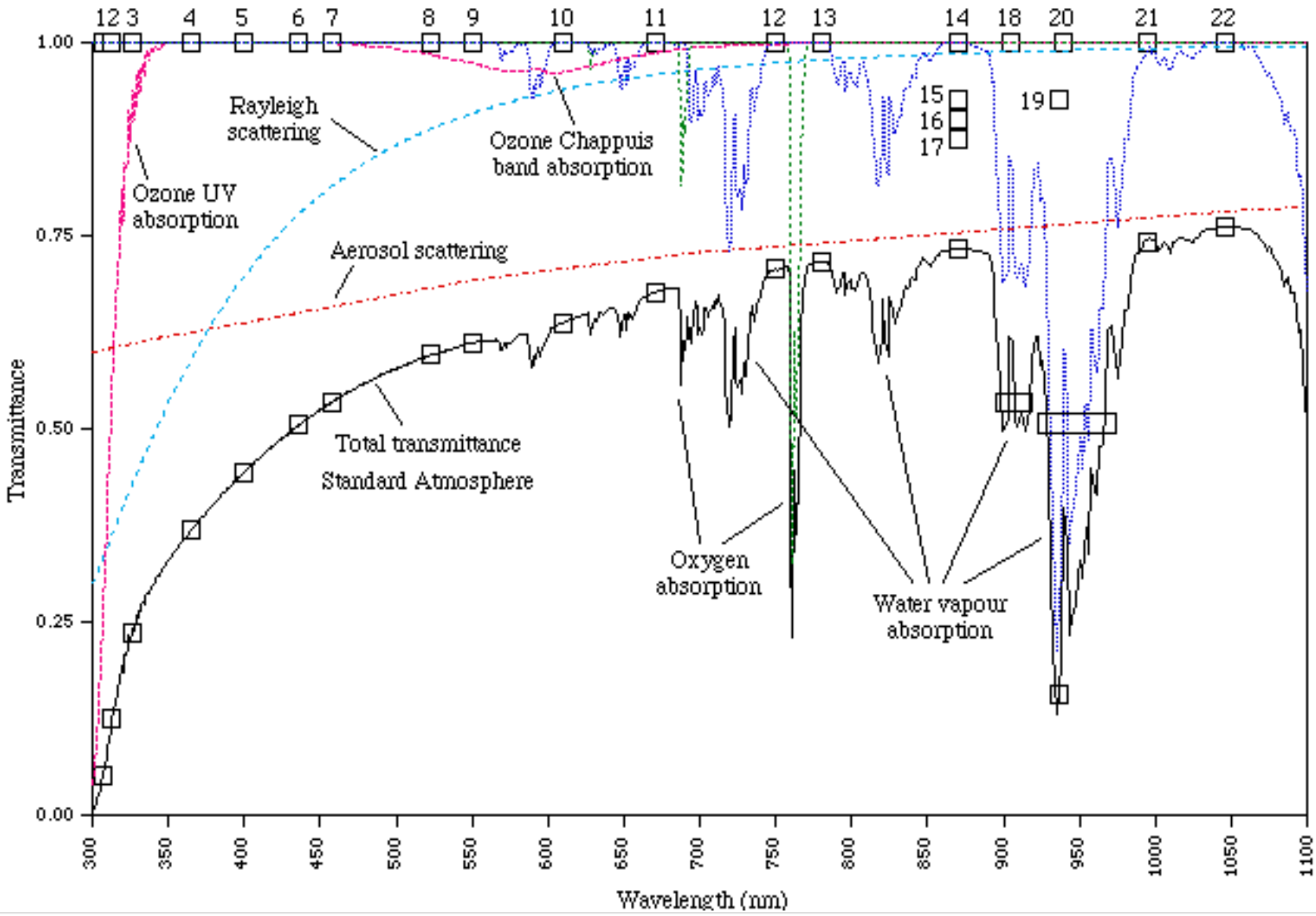
The MLRO telescope

Padova, 21-22 december 2000



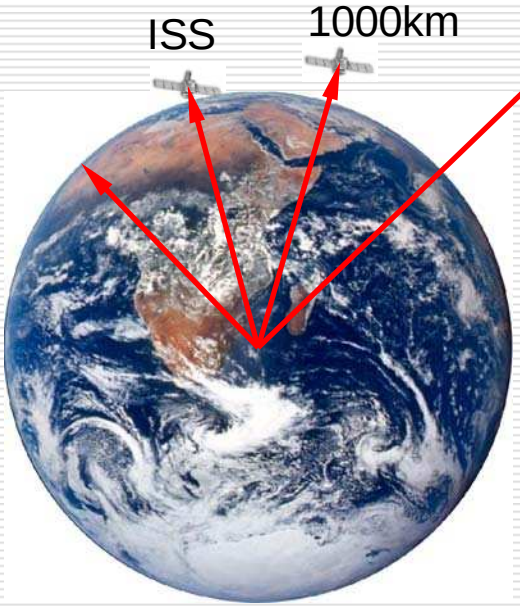
- Diffraction angle ~(wavelength/diameter)
- Need stable pointing
- For satellites: tracking

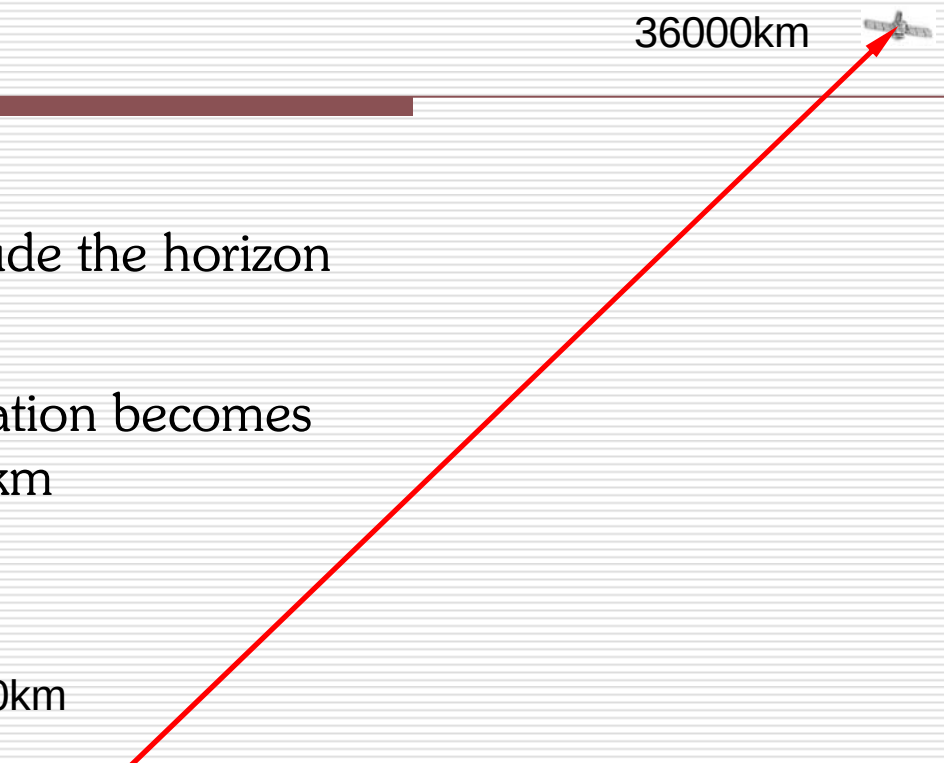
Atmosphere


12 3 4 5 6 7 8 9 10 11 12 13 14 18 20 21 22
1.00
0.75
0.50
0.25
0.00
Transmittance
Rayleigh scattering
Ozone Chappuis band absorption
15
16
17
19
Ozone UV absorption
Aerosol scattering
Total transmittance
Standard Atmosphere
Oxygen absorption
Water vapour absorption
300 350 400 450 500 550 600 650 700 750 800 850 900 950 1000 1050 1100
Wavelength (nm)

Satellites

- From 1000 km altitude the horizon is 3000 km away
- Atmospheric attenuation becomes negligible above 10km





- LEO satellites move fast
- Can only be "seen" from a ground stations for a small fraction of the orbit
- Diffraction loss becomes very severe for geostationary satellites

Early Experimental QKD

University of Waterloo

- 1989 Bennett *et al.*, J. Cryptolog. ***5,*** 3 (1992)
  30cm faint laser pulses
- 1993 Muller *et al.*, Europhys. Lett. ***23,*** 383 (1993)
  Polarization in fiber
- 1994 Townsend, Electron. Lett. ***30,*** 809 (1994)
  10 km fiber, phase
- 1996 Muller *et al.*, Appl. Phys. Lett. ***70,*** 793 (1997)
  Plug & play system
- 1999 Jennewein *et al.*, Phys. Rev. Lett. ***84,*** 4729 (2000)
  Entanglement based QKD (360m)
  1999 Tittel *et al.* Phys. Rev. Lett. ***84,*** 4737 (2000)
  Energy-time entanglement in fiber

The plug & play system (67km demo)

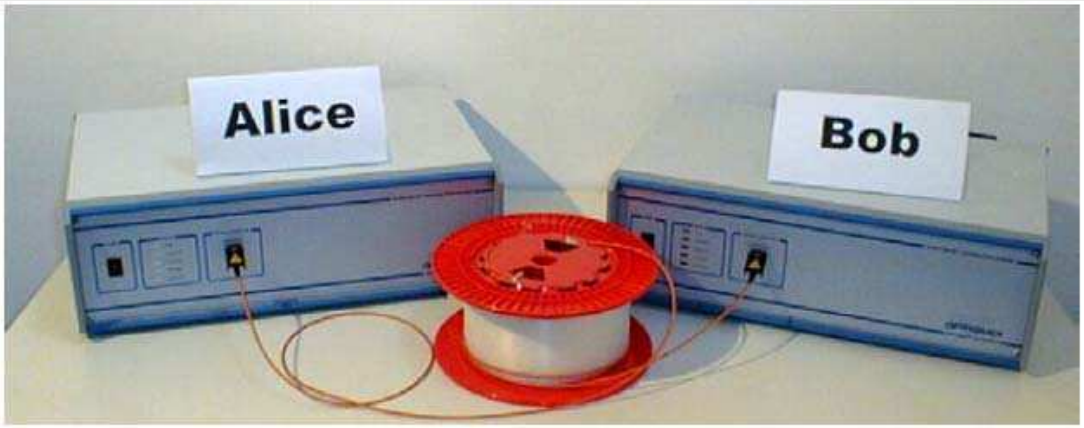


Figure 1. Picture of the p&p system.

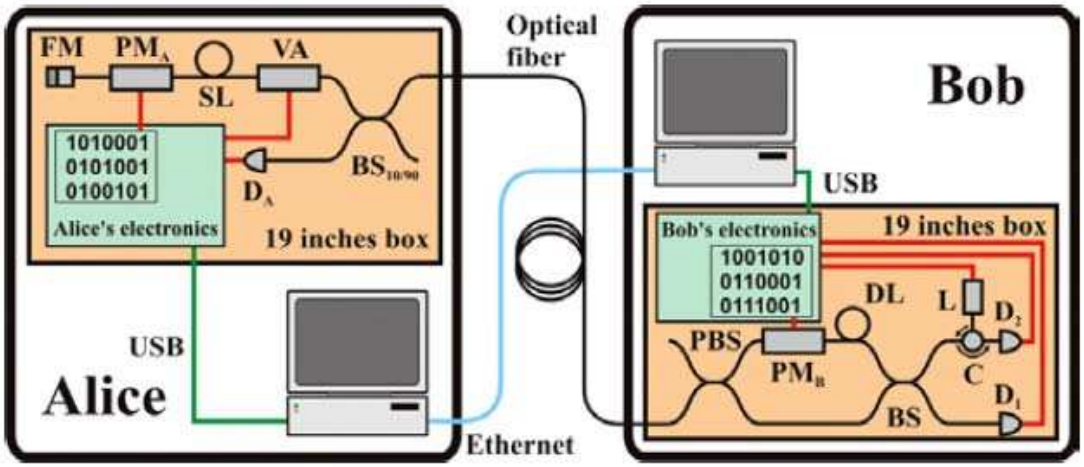
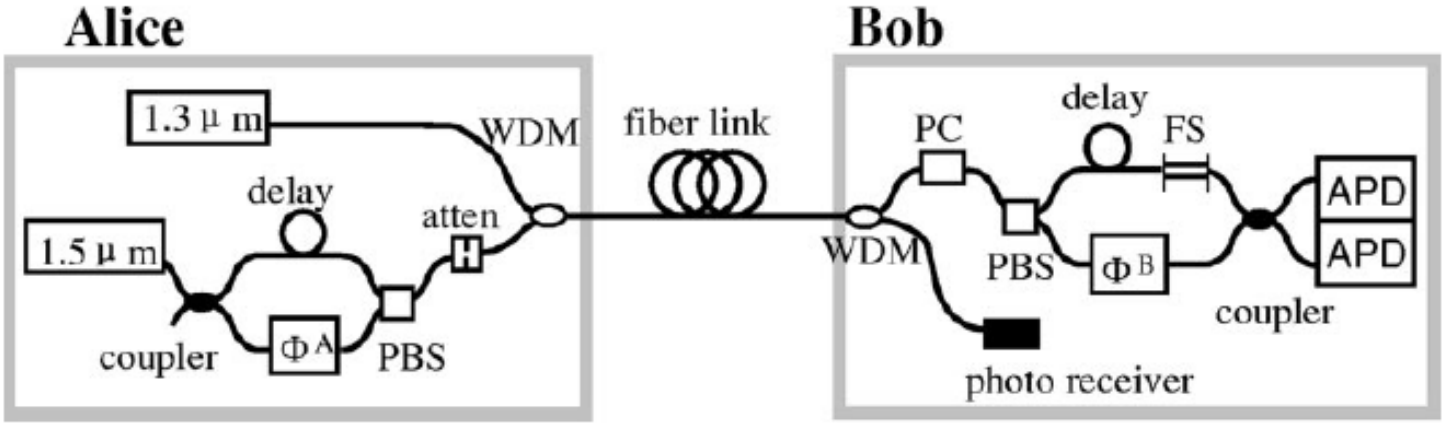


Figure 2. Schematic of the p&p prototype.

Stucki, et al., NJP ***4,*** 41 (2002).

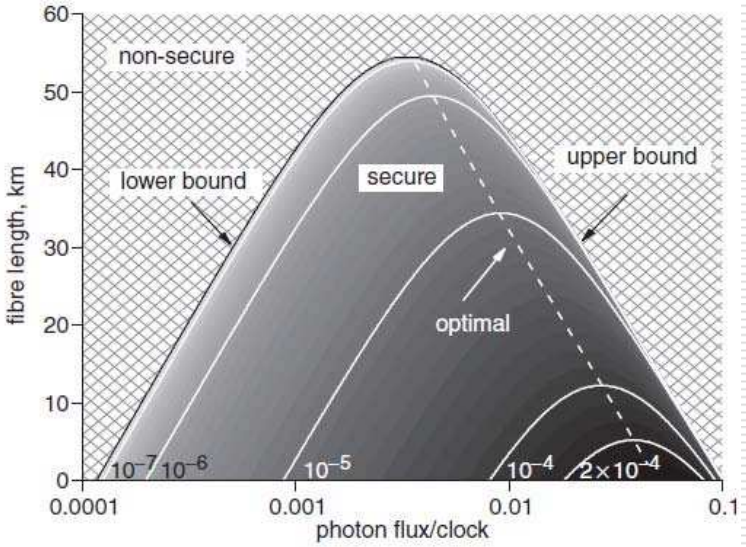
- Uses phase encoding
- Eliminates polarization correction by Faraday mirror
- Need to send "strong" pulse from Bob to Alice for coding

Increasing the distance

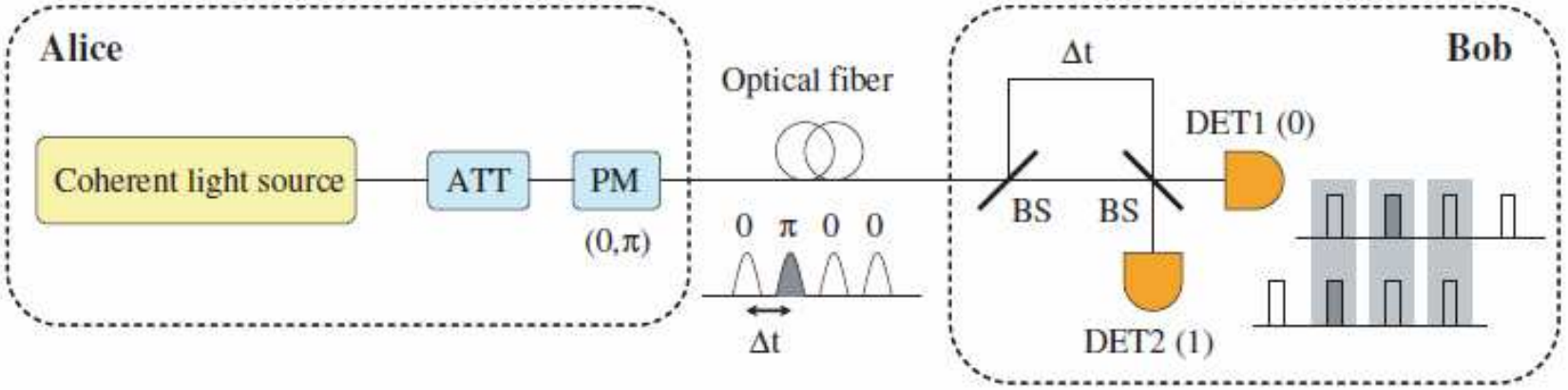


Gobby et al., Appl. Phys. Lett. ***84,*** 3762 (2004).
Gobby et al., Electron. Lett. ***40,*** 1603 (2005).

- Up to 122 km QBER is under 11% for photon flux = 0.1 /pulse
- Up to 50km unconditionally secure



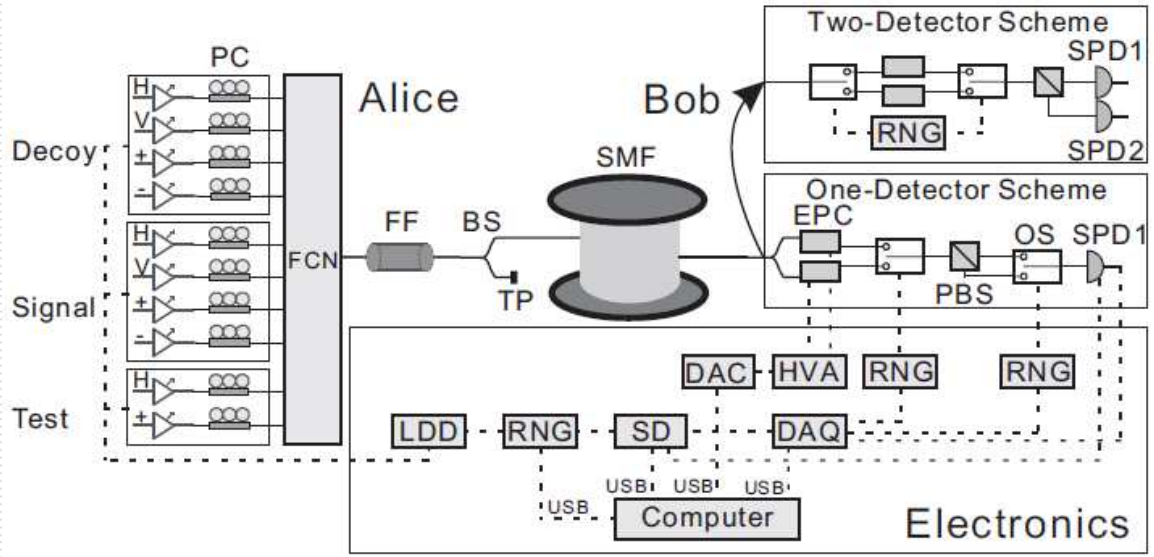
Differential Phase Shift Keying QKD



Takasue et al., NJP ***7,*** 232 (2005).
Diamanti et al., quant-ph/0608110.

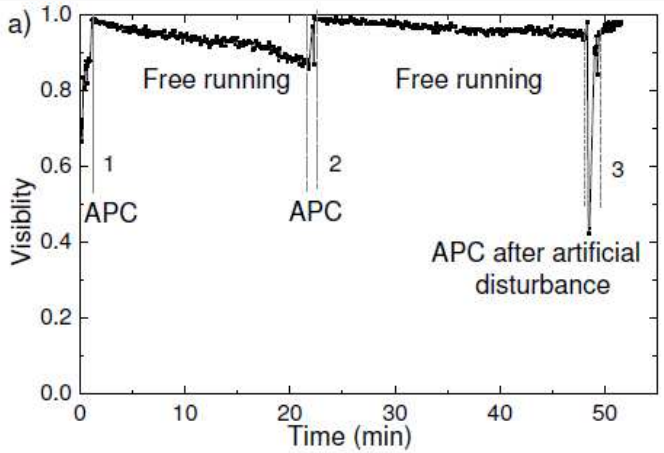
- Better use of clock period
- Achieved 1 GHz clock rate
- Using up-conversion single photon detectors
- @100 km 166 bits/s secure (?)

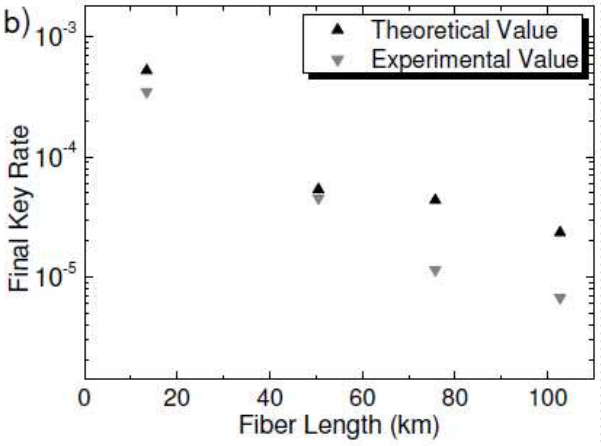
Polarization in Fiber



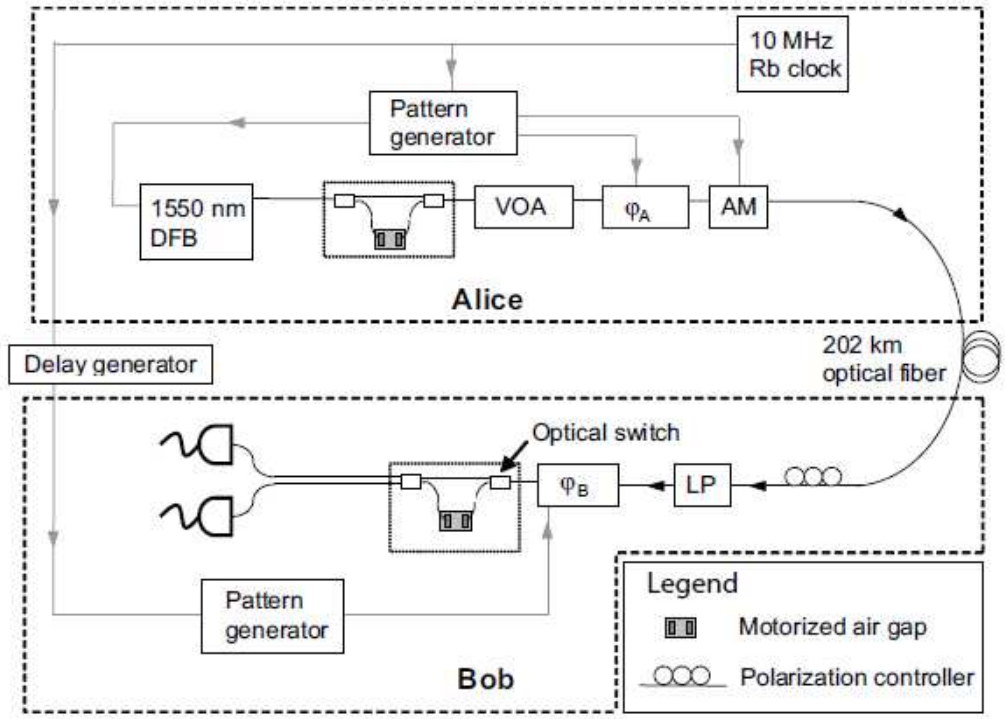
Peng et al., quant-ph/0607129 (2006)

- With decoy states achieved 103 km





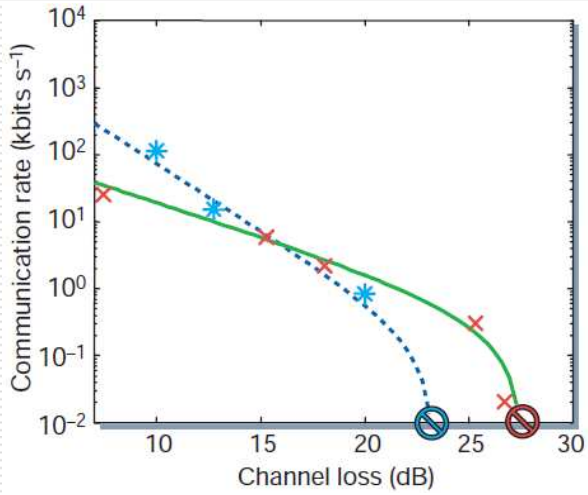
With (Almost) Noise-Free Detectors



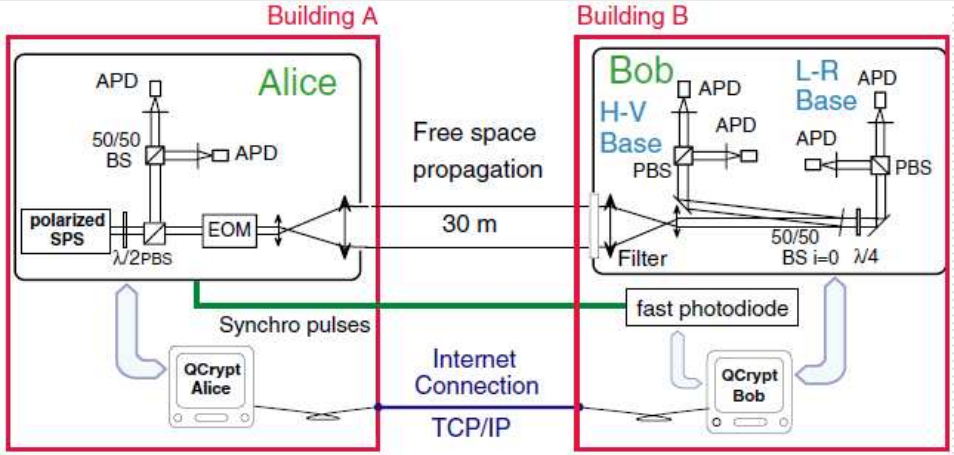
- Superconducting Transition Edge Sensors
  - Virtually zero noise
  - Poor timing ➔ slow clock cycle
- With decoy states achieved unconditionally secure key over 107 km

Rosenberg et al., Appl. Phys. Lett. ***88***, 021108 (2006).
Rosenberg et al., quant-ph/0607186

With Single Photons



Waks et al., Nature ***420,*** 762 (2002)



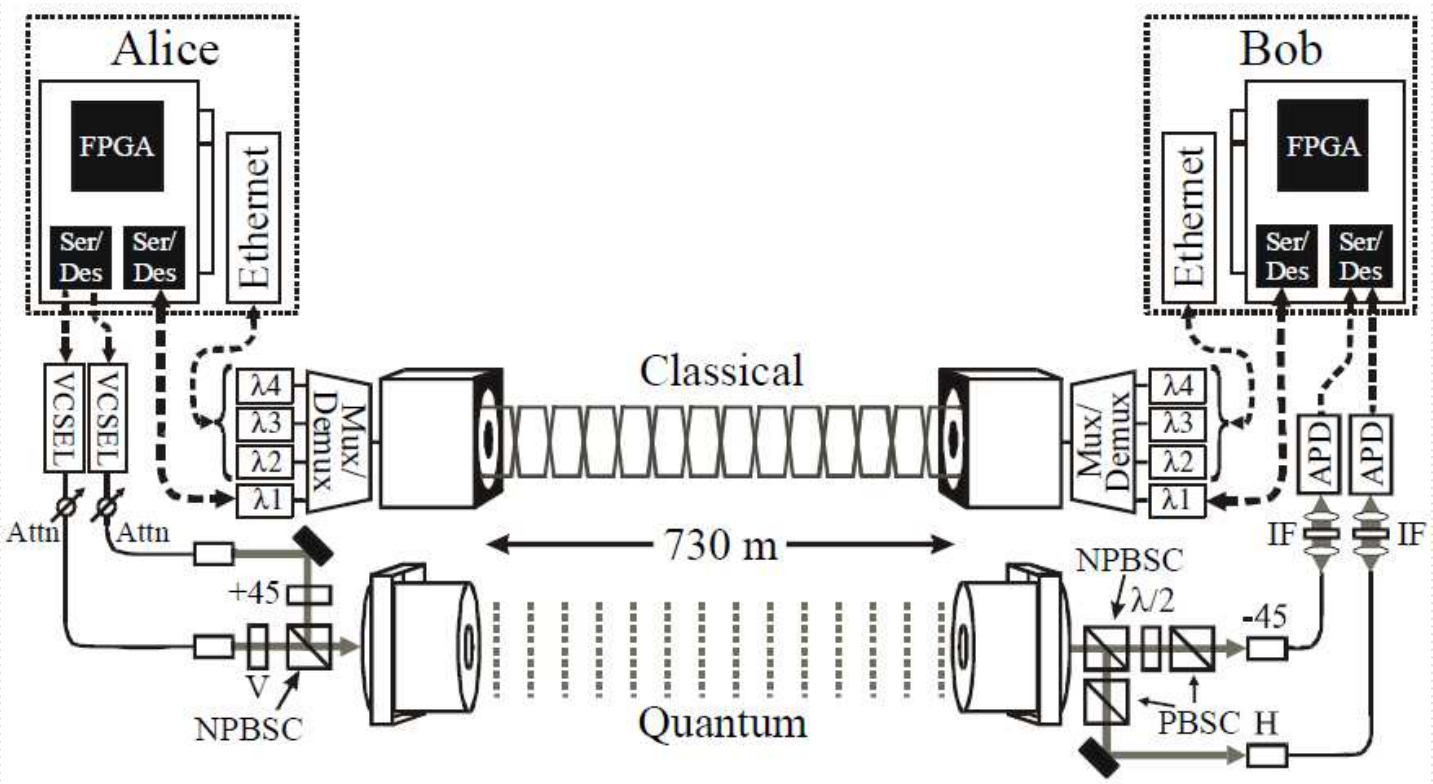
Alleaume et al., NJP ***6,*** 92 (2004)

- Single photons: unconditional security without decoy states
- Waks et al.: InAs quantum dots
- Alleaume et al.: Color centers in diamond

High Data-Rate Free-Space QKD

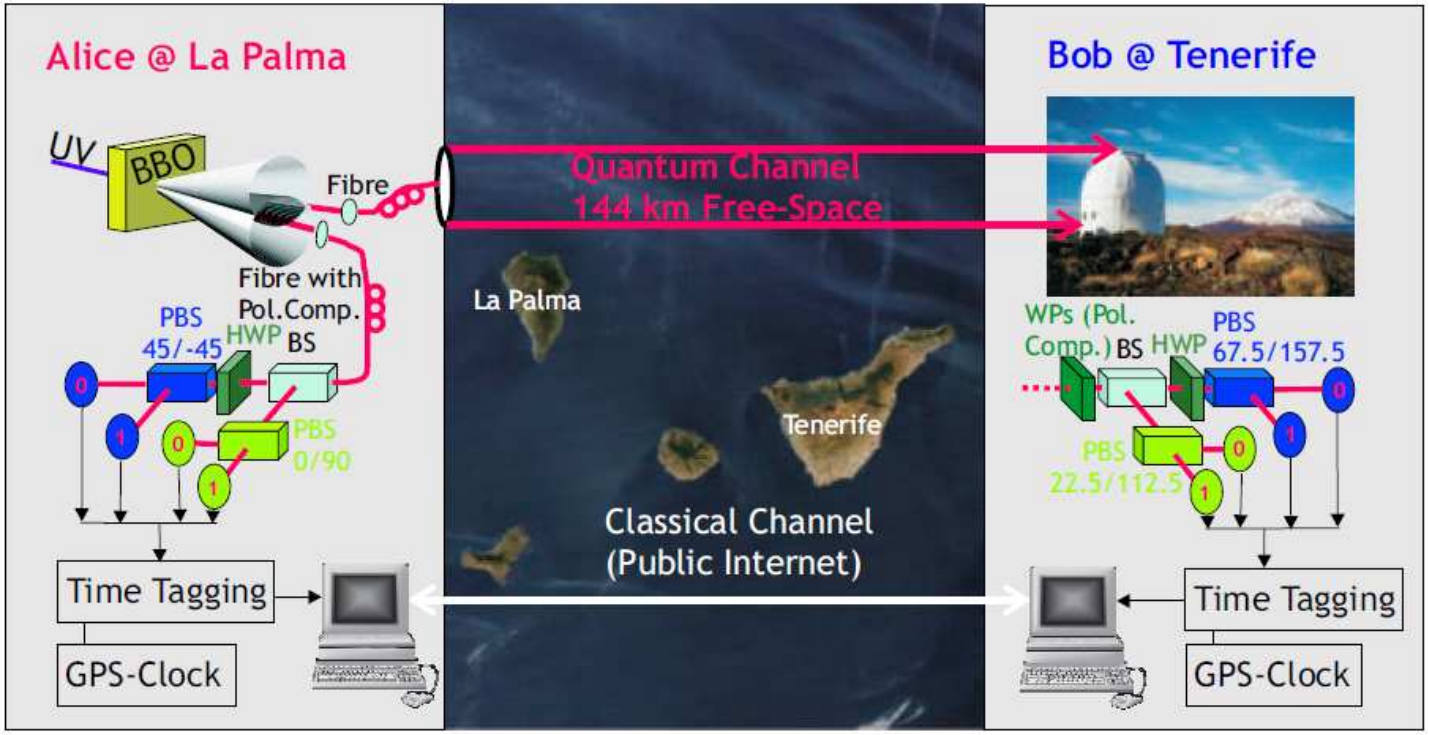
- 690 kbit/s at 0.15 photons/pulse at Alice

Bienfang et al., Opt. Express ***12,*** 2011 (2004)



Free-Space Long Distance

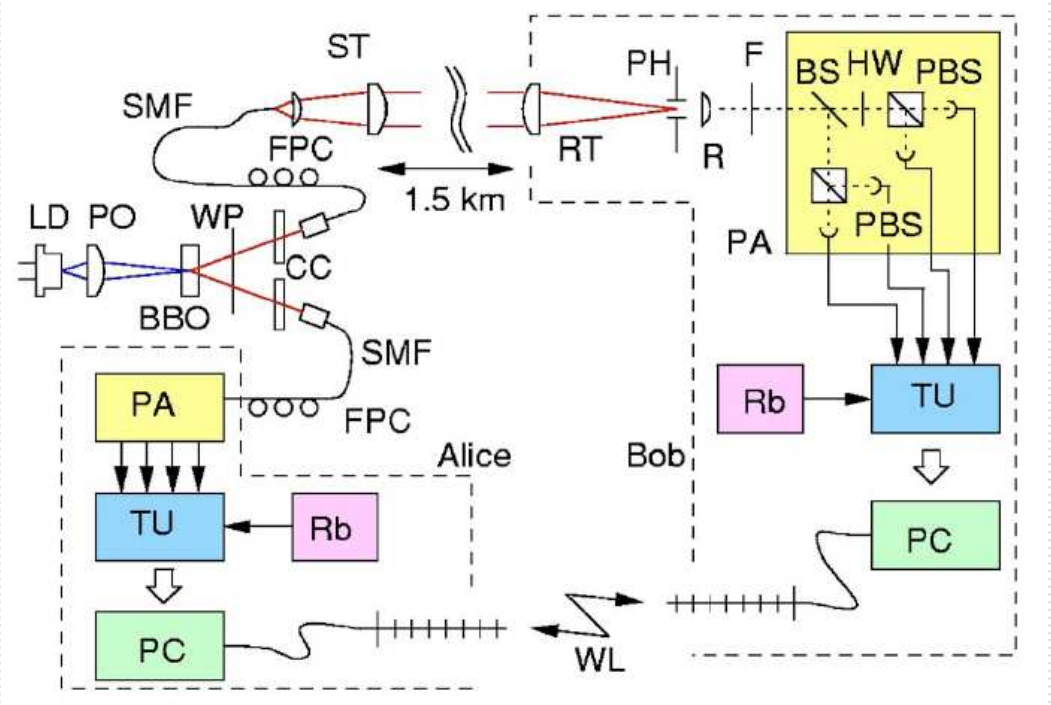
Ursin et al., quant-ph/0607182



- Entanglement-based with source at Alice's
- 1m receiver telescope
- Typical loss -30 dB
- ~30 raw key bits/s

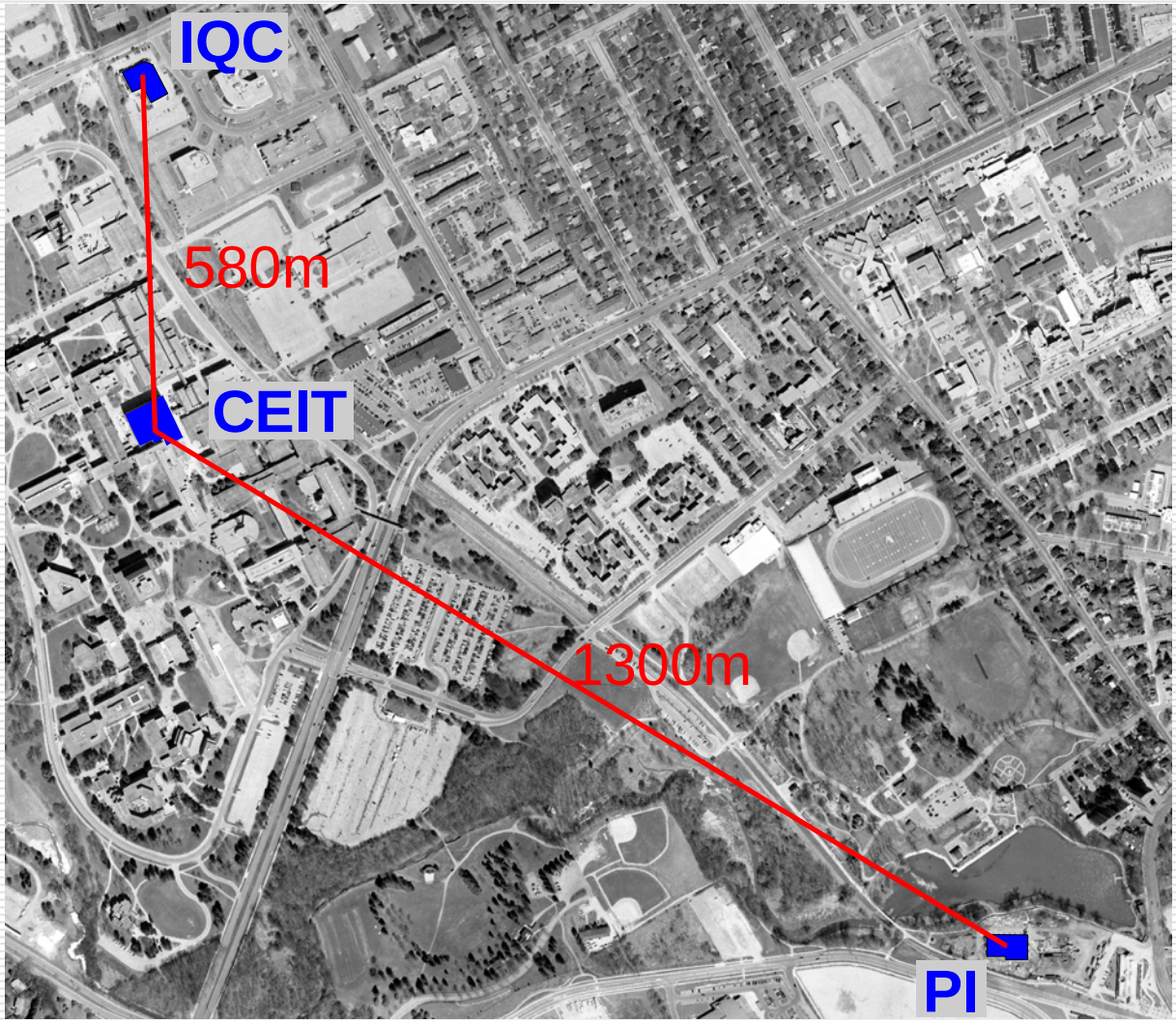
Entanglement based FS QKD

- Dedicated real time entanglement based QKD system
- 630 bits/s *final* key

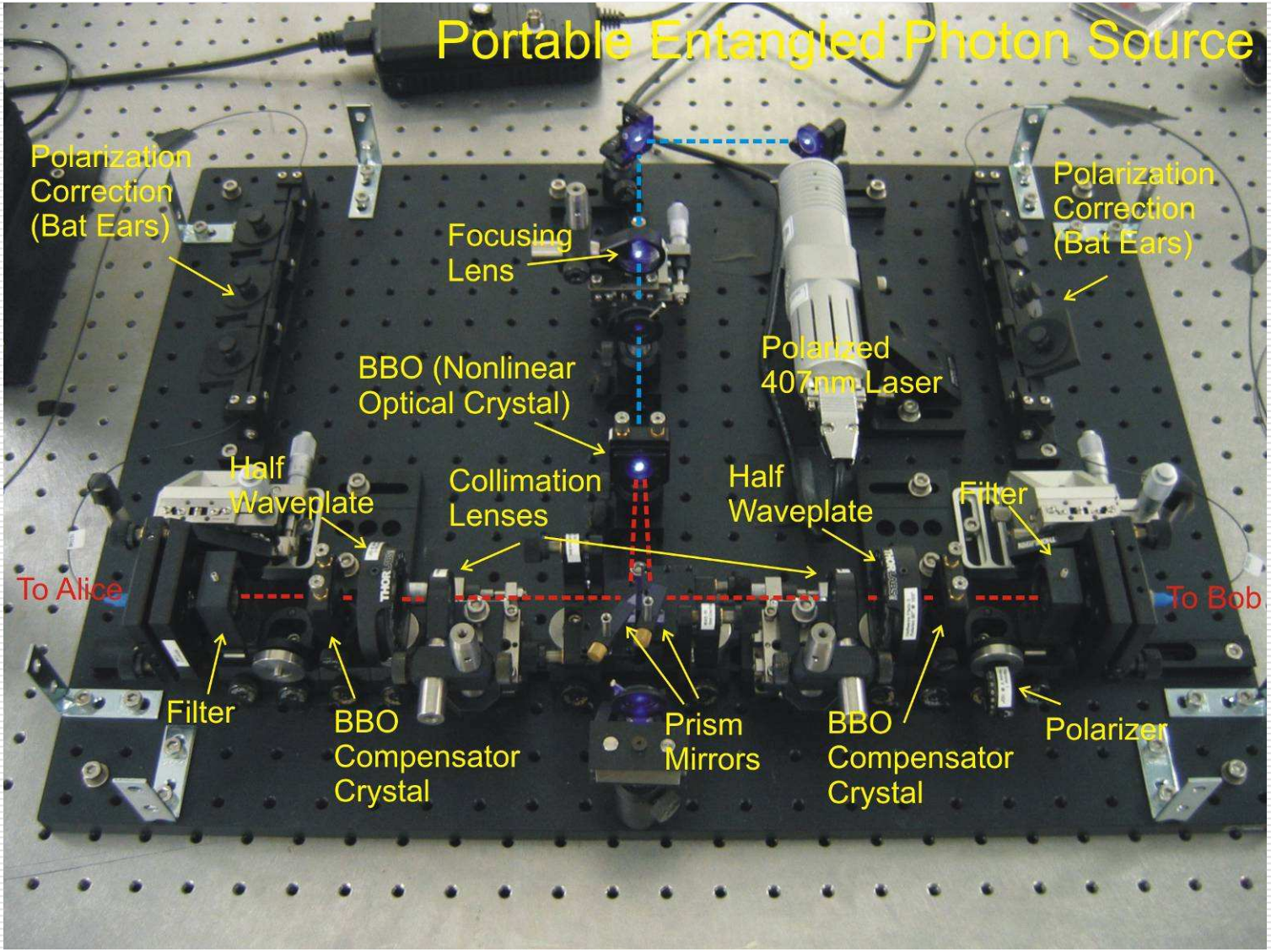


Marcikic et al., Appl. Phys. Lett. ***89,*** 101122 (2006)

Free-space QKD



QKD Source


Portable Entangled Photon Source
Polarization Correction (Bat Ears)
Focusing Lens
Polarization Correction (Bat Ears)
BBO (Nonlinear Optical Crystal)
Polarized 407nm Laser
Half Waveplate
Collimation Lenses
Half Waveplate
Filter
To Alice
To Bob
Filter
BBO Compensator Crystal
Prism Mirrors
BBO Compensator Crystal
Polarizer

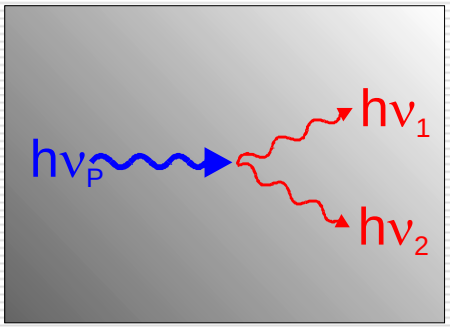
Parametric down-conversion

Nonlinear Polarization $P_i = \chi_{ij}^{(1)} E_j + \chi_{ijk}^{(2)} E_j E_k + \chi_{ijkl}^{(3)} E_j E_k E_l + \ldots$

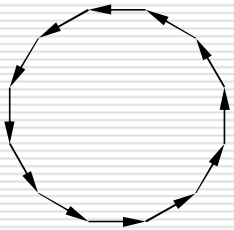
Energy conservation

Crystal-momentum conservation = Phase matching

$$\omega_p = \omega_1 + \omega_2, \qquad \mathbf{k}_p = \mathbf{k}_1 + \mathbf{k}_2$$



No Phase-Matching



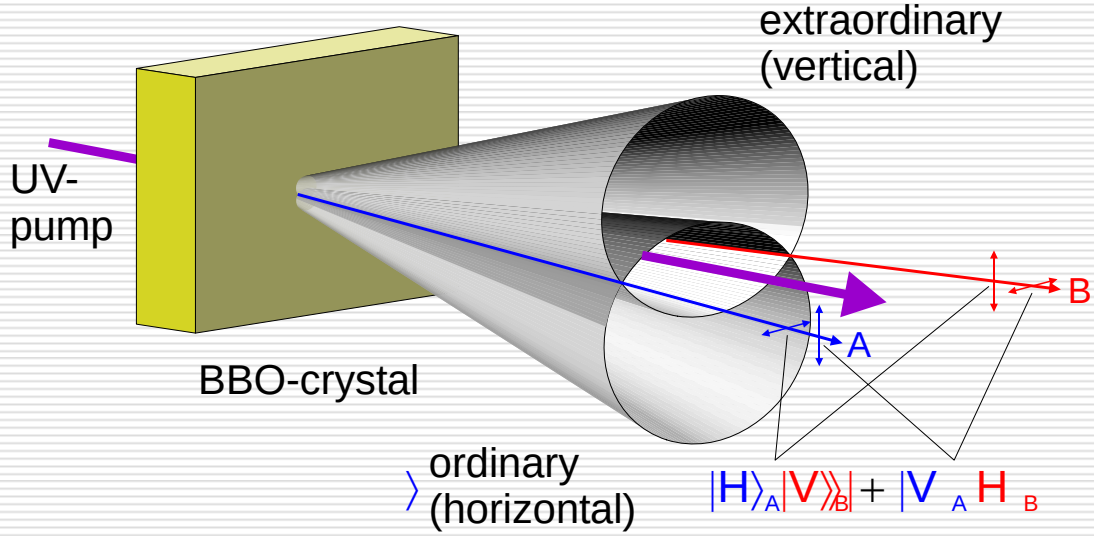
Perfect Phase-Matching

University of Waterloo

Type-I Parametric Down-conversion

by Guido Czeija, Gregor Weihs and Alipasha Vaziri
Quantum Experiments and Foundational Physics
Prof. Anton Zeilinger
Institut für Experimentalphysik
University of Vienna

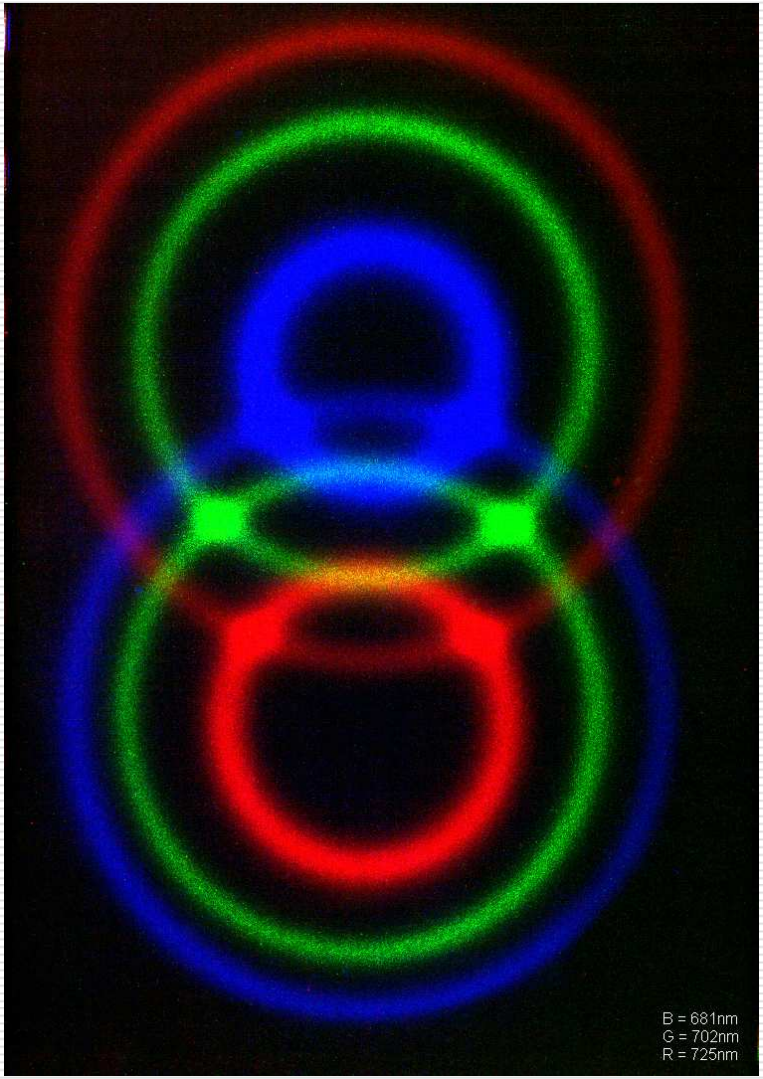
Polarization entanglement



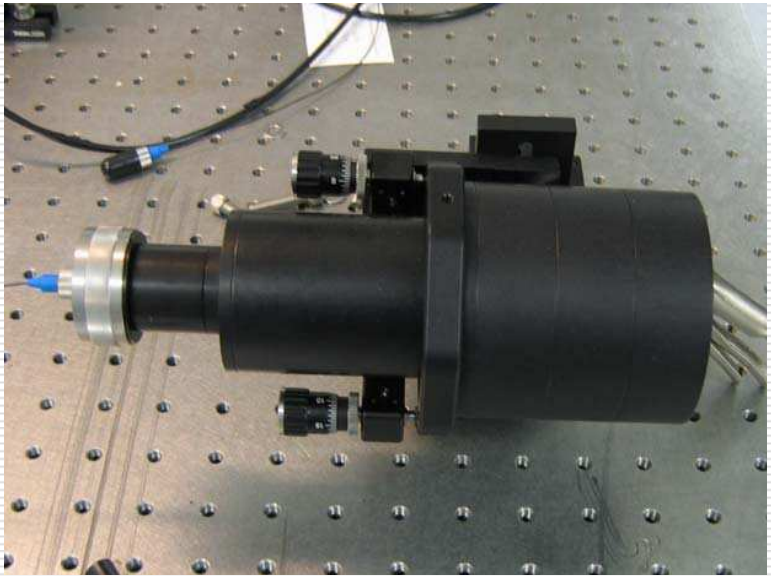
- Kwiat et al. PRL ***75,*** 4337 (1995)
- Compensation necessary
- Shorter crystals yield higher useful count rates! [Lee et al. PRA ***70,*** 043818 (2004)]

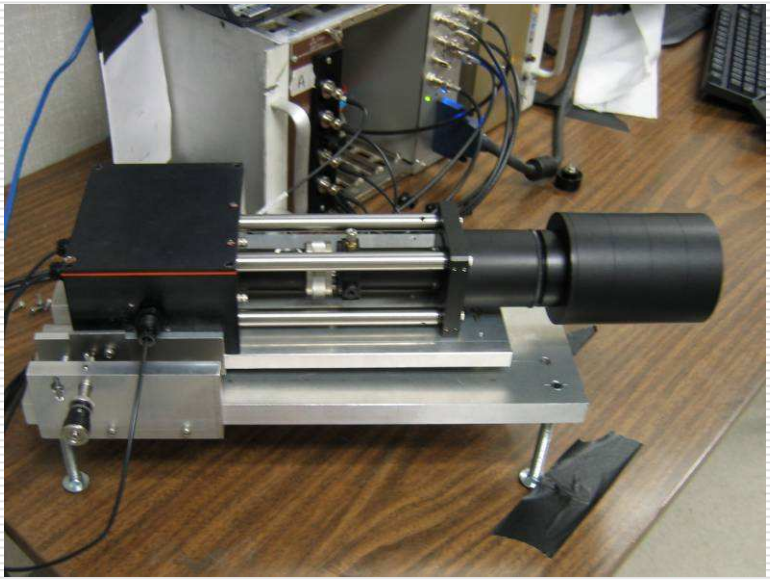
Entangled photon pairs

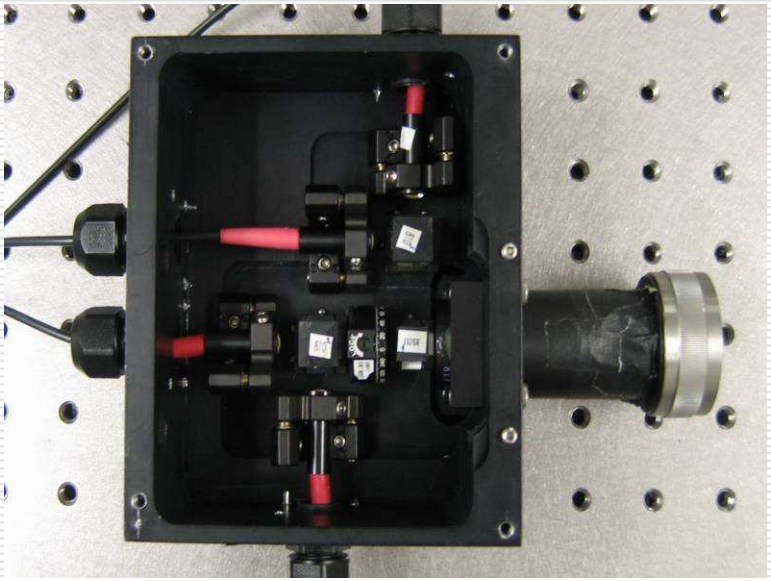
University of Waterloo



Transmission & Detection

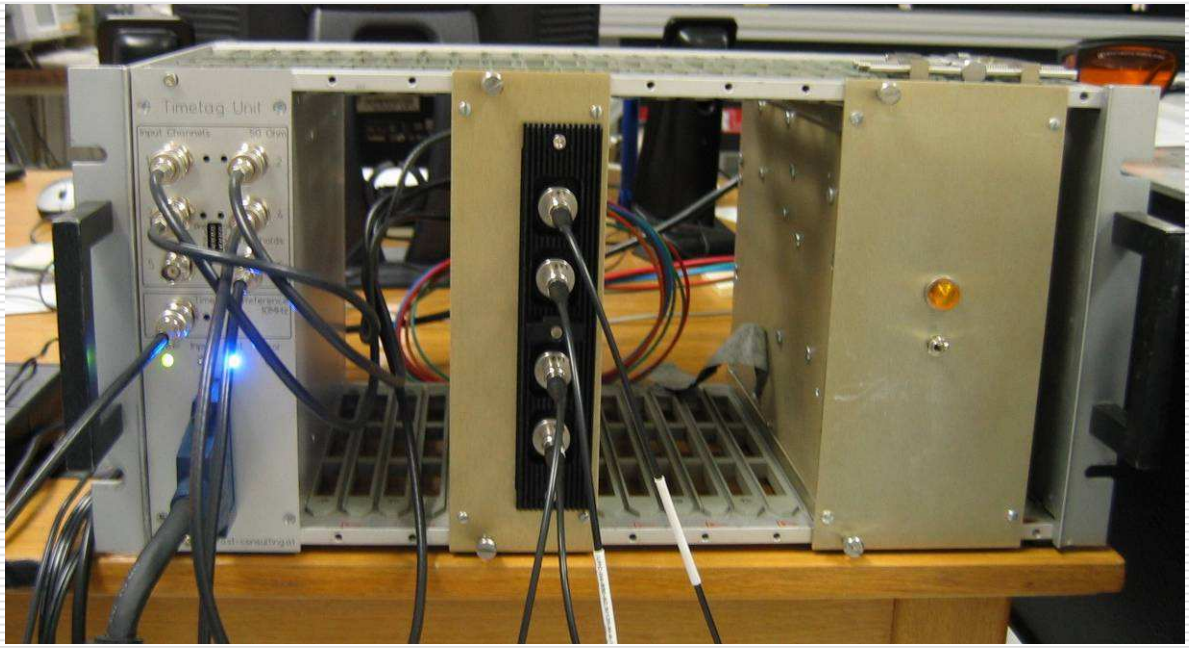






Detection - Electronics

- SPCM
- FPGA time tagging (~156.25ps)
- GPS based synchronization + correlation



Preliminary Results & Outlook

University of Waterloo

- Raw key rate via one link in lab: 5000 /s
- Raw QBER: ~4%

- Improve spatial and wavelength filtering for daylight operation
- Implement brighter source
- Automate alignment

Directions in Experimental QKD

University of Waterloo

Fiber

- Increase clock rates
- Better detectors ➔ increase distances
- Networks

Free-space

- Implement automatic alignment and tracking
- Create light-weight entanglement sources for satellites