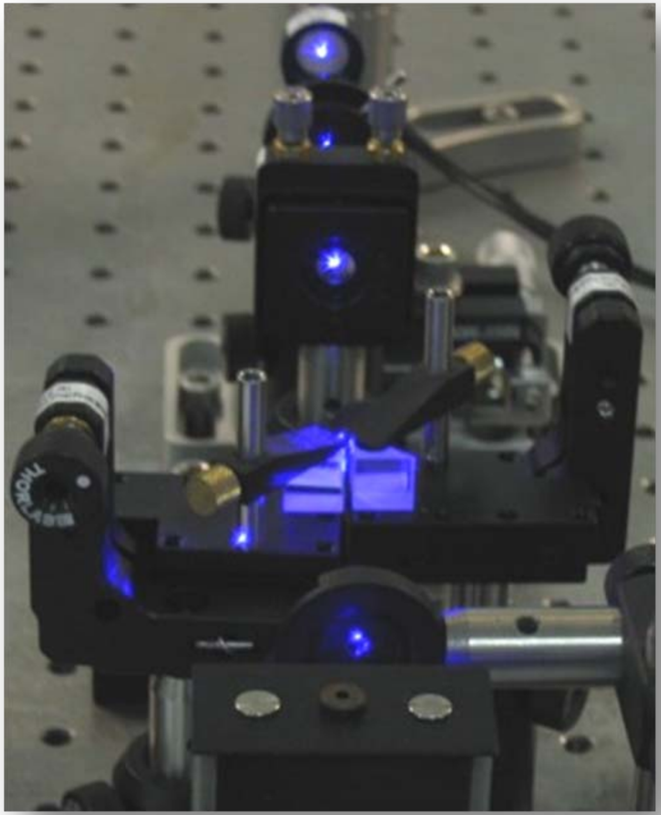
Leopold-Franzens-Universität Innsbruck
Institut für Experimentalphysik
Technikerstrasse 25
http://www.uibk.ac.at

Practical Quantum Key Distribution

Gregor Weihs

Contents

- QKD Protocols
- Implementations of QKD
- Photonic qubit QKD
- Channels
- Example: The Waterloo QKD



Literature

Review articles:

- N. Gisin et al., *Quantum Cryptography,*
  Reviews of Modern Physics **74,** 145 (2002).

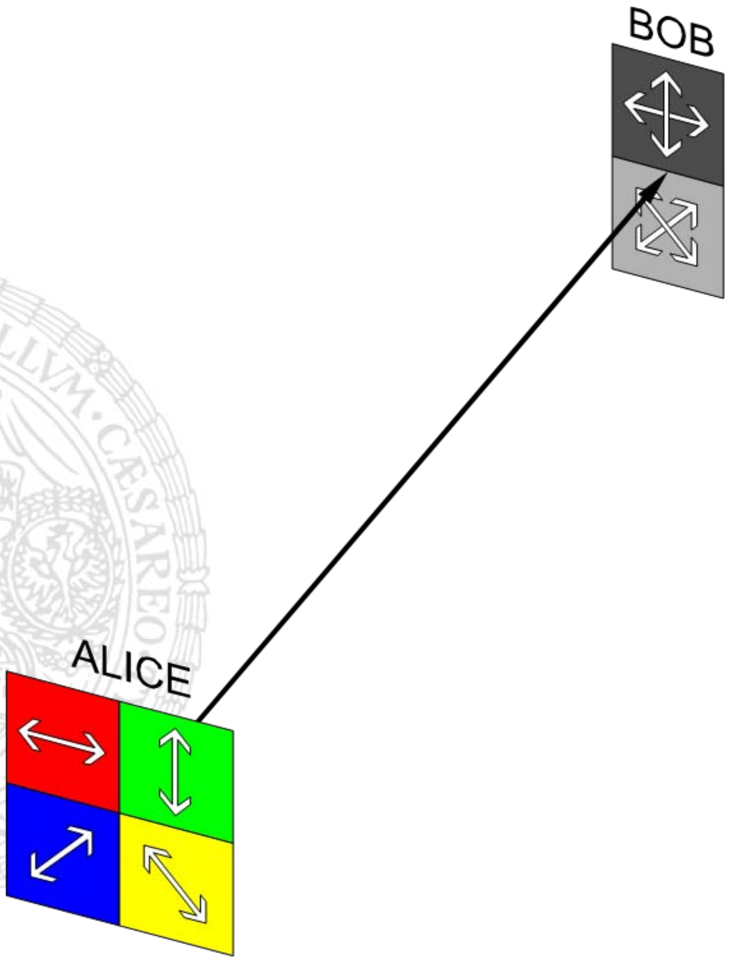
- M. Dusek et al., *Quantum Cryptography,*
  Progress in Optics **49,** 381 (2006).

- V. Scarani et al., *A Framework for Practical Quantum Cryptography,*
  arXiv:0802.4155, to appear in RMP.

Book:

- G. Van Assche, *Quantum Cryptography and Secret-Key Distillation,*
  Cambridge University Press (2006).

BB84



- Alice sends **single photons** with 1-out-of-4 polarizations
- Bob measures in either + or × **basis** and gets one of two results (0, 1) in either case.
- Basis choices are announced after the measurement via **authenticated** public classical channel (internet, broadcast, …)
- Measurement results for agreeing bases are key bits

C. H. Bennett & G. Brassard, *Quantum Cryptography: Public-key distribution and coin tossing* in *Proceedings of IEEE International Conference on Computer Systems and Signal Processing, IEEE,* 175-179 (1984).

The role of security proofs

- Security proofs give a lower bound on the achievable secure key rate as a function of **measurable** parameters
- They tell us how much key has to be sacrificed in privacy amplification in order to eliminate Eve's partial knowledge
- Shor & Preskill, PRL **85,** 441 (2000): through reduction to entanglement purification and quantum error correction the secret key length is lower bounded by a factor of

$$1 - 2h(\mathrm{QBER}) \qquad h(x) = -x \log x - (1-x)\log(1-x)$$

  w.r.t the number of sifted bits, with exponentially small knowledge of the eavesdropper.
- Therefore if QBER < 11%, the secret key length is finite.
- With imperfect error correction we need to use

$$1 - h(\mathrm{QBER}) - h_{\mathrm{EC,leakage}}$$

Noisy Keys

- Raw keys are noisy, because of errors in
  - Channel
  - Equipment (dark counts)
  - Eavesdropper

- (Classical) Error correction can eliminate errors
  - Simple example: Take two blocks of k bits, compare parity, if different, dicscard

Error correction

Alice 01100000 11011101 01111110 00100100 11110100 11011001 10010111 00010101
Bob 01000000 11011101 01111110 00100100 11110100 11011011 10010111 00010101

Alice

0	1	1	0	0	0	0	0	0
1	1	0	1	1	1	0	1	0
0	1	1	1	1	1	1	0	0
0	0	1	0	0	1	0	0	0
1	1	1	1	0	1	0	0	1
1	1	0	1	1	0	0	1	1
1	0	0	1	0	1	1	1	1
0	0	0	1	0	1	0	1	1
0	1	0	0	1	0	0	0	

Bob

0	1	~~0~~	0	0	0	0	0	0
1	1	0	1	1	1	0	1	0
0	1	1	1	1	1	1	0	0
0	0	1	0	0	1	0	0	0
1	1	1	1	0	1	0	0	1
1	1	0	1	1	0	~~1~~	1	0
1	0	0	1	0	1	1	1	1
0	0	0	1	0	1	0	1	1
0	1	1	0	1	0	1	0	

Alice new 10001011 11011110 00110011 11001111 11010110 01010
Bob new 10001011 11011110 00110011 11001111 11010110 01010

Simplified Cascade Error Correction

- Optimized for computational efficiency (vs. information leakage)
- 4 passes
  - Use QBER as determined in previous chunk to choose block size
  - Split key into blocks
    (randomly chosen bit order, different for each pass)
  - Apply BINARY to correct one error in each block (for odd numbers of errors)
    - Calculate parity
    - On disagreeing parity divide block in half
    - Repeat until error found
  - If error is found in later pass, there must have been even number of errors in previous pass' block ➔ go back and correct using BINARY
- Keep track of every bit sent via the public channel

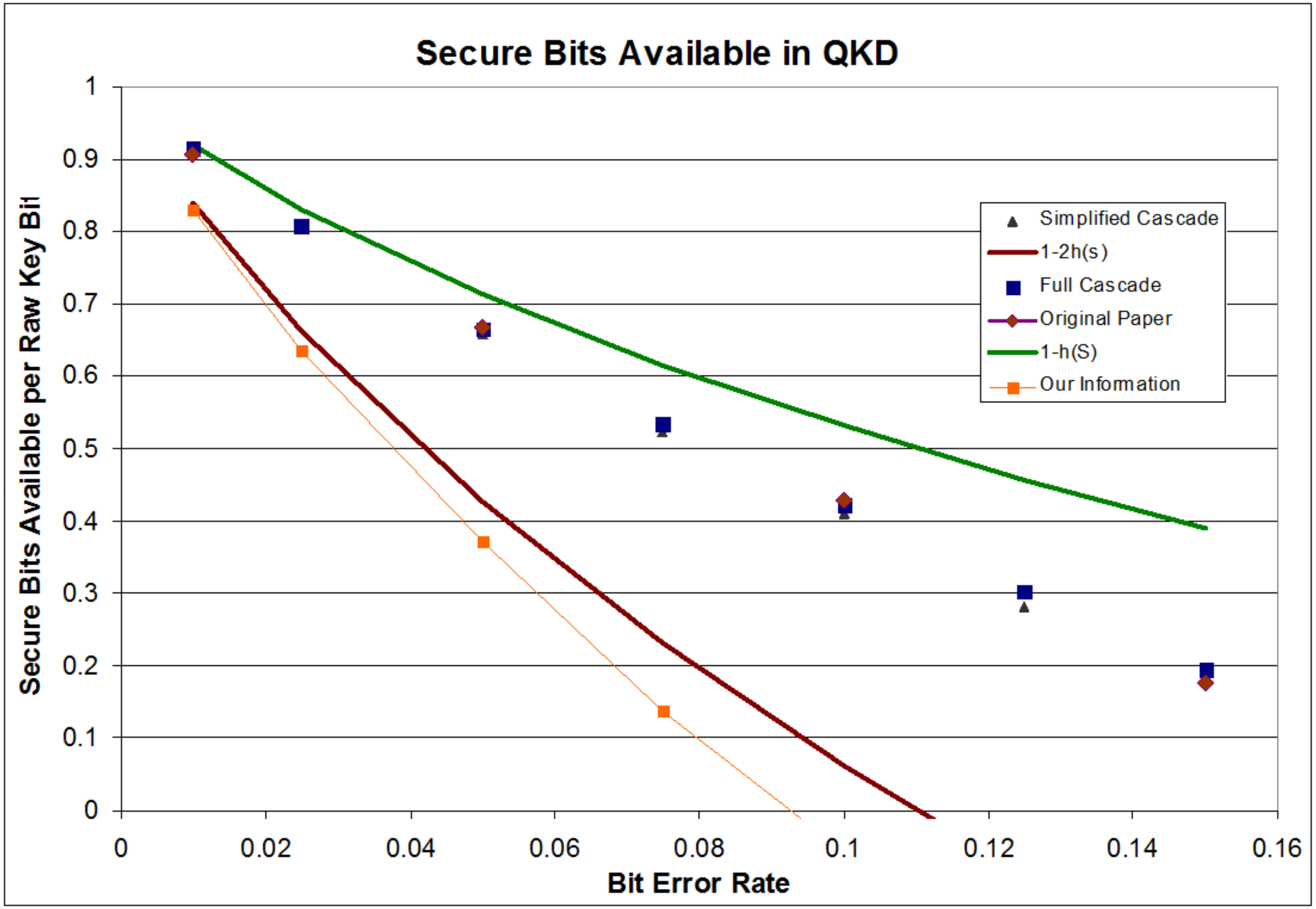
BER	Simplified Cascade	Full Cascade
0.01	0.089	0.085
0.025	0.197	0.1925
0.05	0.341	0.335
0.075	0.477	0.465
0.1	0.589	0.577
0.125	0.717	0.697
0.15	0.817	0.805

G. Brassard and L. Salvail, “Secret-Key Reconciliation by Public Discussion,” Advances in Cryptology – EUROCRYPT ’93, LNCS 765, 410 (1994).

Privacy Amplification

- All the bits revealed during error correction must be discarded
- Any information an eavesdropper could have according to the QBER can be made exponentially small by hashing
- Determine final key length estimate:
  $R = N\,(1 - h_2(\text{QBER})) - \#(\text{bits leaked}) - \#(\text{security bits})$
- Shor-Preskill: $R = N - 2H_2(\text{QBER})$
  Since $\#(\text{bits leaked}) > H_2(\text{QBER})$
  this is always secure
- Calculate $k = (m * (\text{raw key}) + n) \bmod p$
  - m, n are random number generated from a shared seed
  - p is a shared big prime number
- Use the last R bits of k as the key

Privacy Amplification



Classification of QKD Protocols

By source

- Prepare and measure
- Entanglement based

By Modulation

- Discrete
- Continuous
- Distributed phase reference

By implementation

- One-way
- Plug & Play

Modulation

Discrete = Qu**d**its

- Polarization
- Time-bin
- Spatial Mode

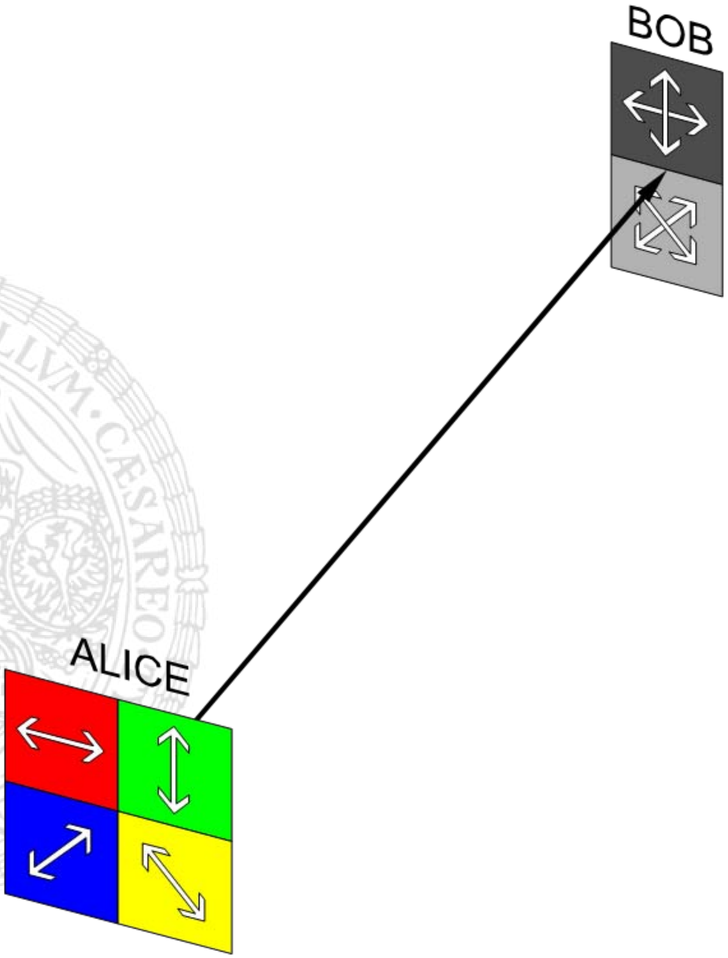
Continuous Variables

- Quadratures of field modes

Distributed Phase Reference

- Differential Phase Shift
- Coherent One-Way

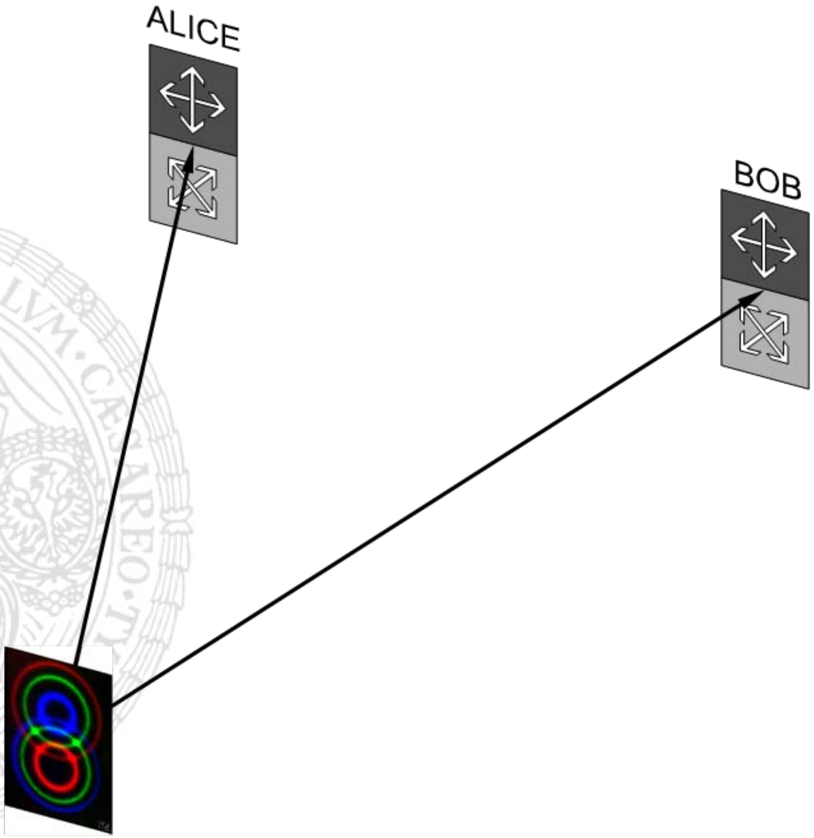
BB84



- Alice sends **single photons** with 1-out-of-4 polarizations
- Bob measures in either + or × **basis** and gets one of two results (0, 1) in either case.
- Basis choices are announced after the measurement via **authenticated** public classical channel (internet, broadcast, …)
- Measurement results for agreeing bases are key bits

C. H. Bennett & G. Brassard, *Quantum Cryptography: Public-key distribution and coin tossing* in *Proceedings of IEEE International Conference on Computer Systems and Signal Processing, IEEE,* 175-179 (1984).

Entanglement Based



- Source can be under eavesdroppers control
- Immune to sidechannels

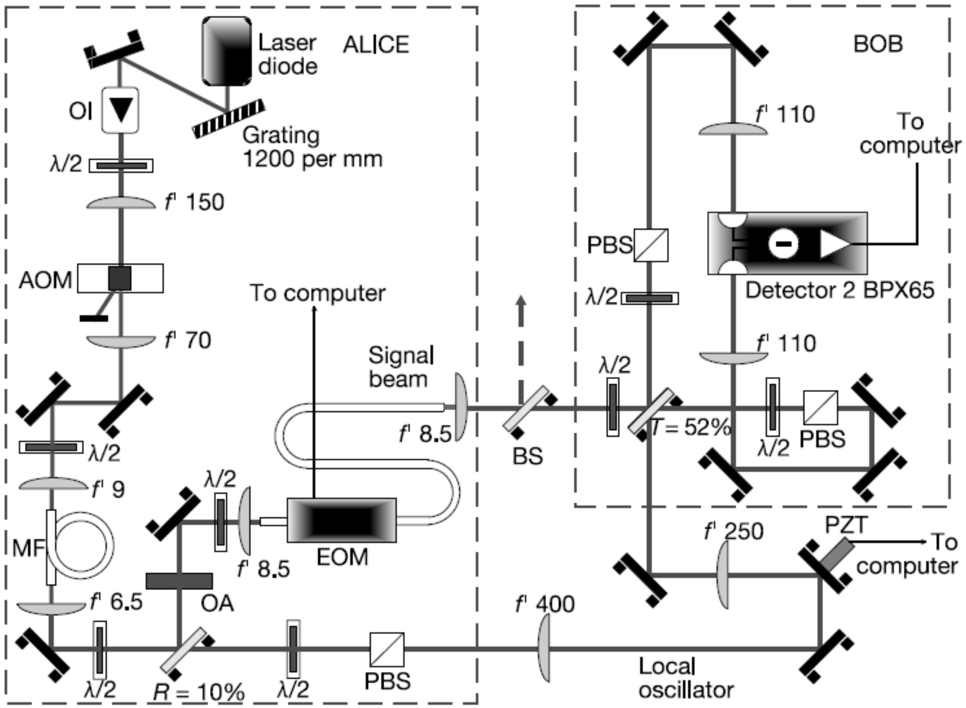
Continuous Variables

- Alice sends coherent states with a random modulation in a given quadrature
- Bob chooses randomly to measure a quadrature using homodyne detection
- Alternative: Squeezed states

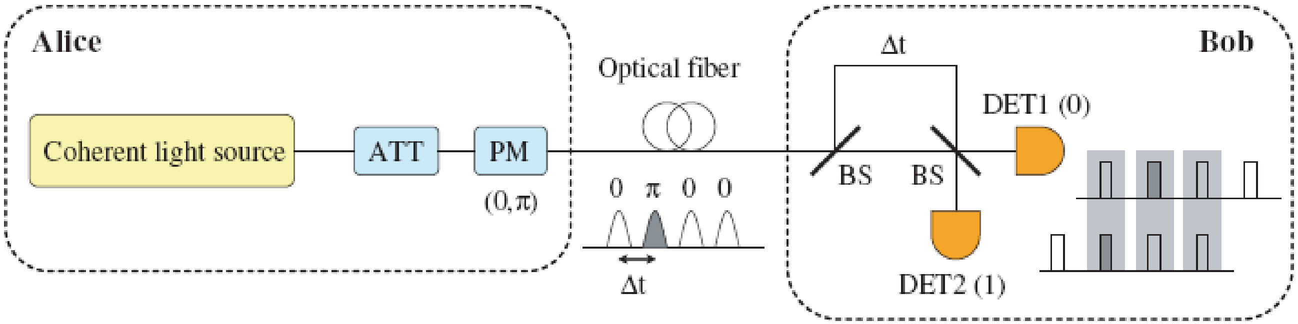
$$\mathbf{E}_\mathbf{k} = i\sqrt{\frac{\hbar\omega_\mathbf{k}}{2\epsilon_0}}\left[\hat{a}_\mathbf{k}\mathbf{u}_\mathbf{k}e^{-i\omega_\mathbf{k}t} - \hat{a}_\mathbf{k}^\dagger\mathbf{u}_\mathbf{k}e^{i\omega_\mathbf{k}t}\right]$$

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle$$

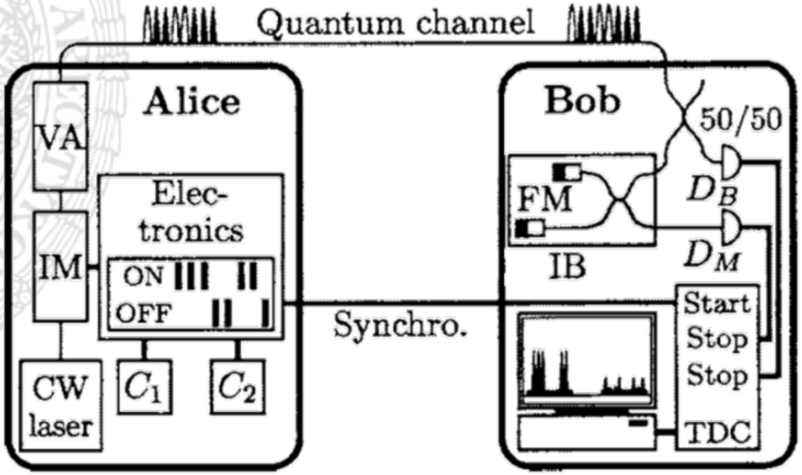
Continuous Variables



Distributed Phase Reference



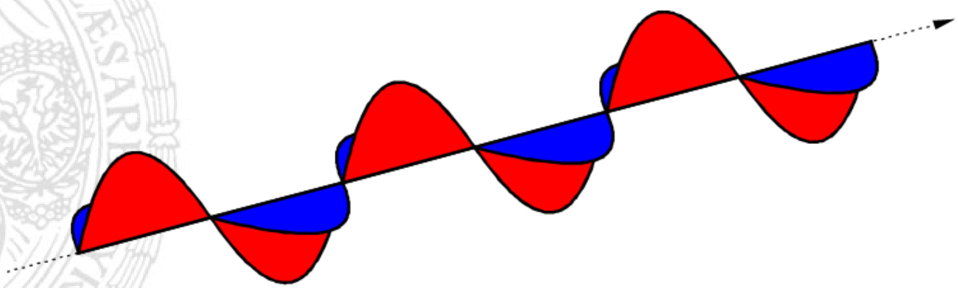
E. Diamanti et al., Opt. Express **14,** 13073-13082 (2006).

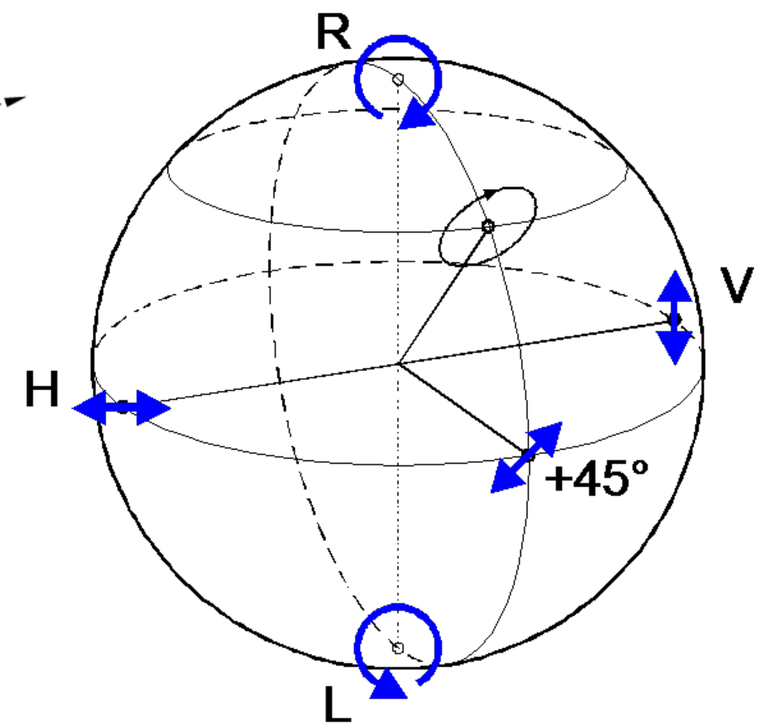


D. Stucki et al., APL **87,** 194108 (2005).

Photon Polarization

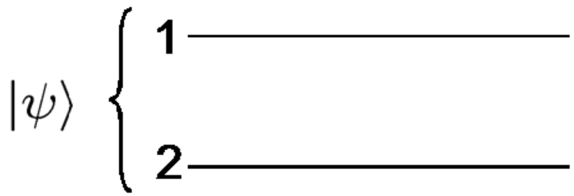
- Every mode has two orthogonal polarizations (directions of the electric field)
- Arbitrary polarization states are superpositions
- Classically, polarization is described on the Poincaré sphere



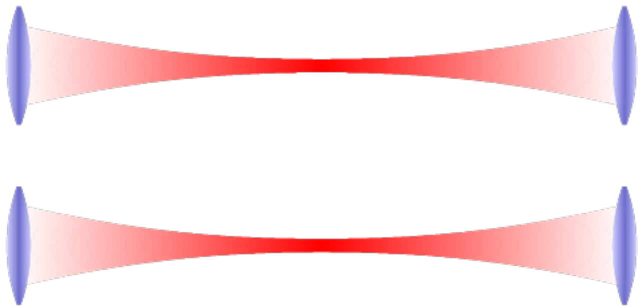


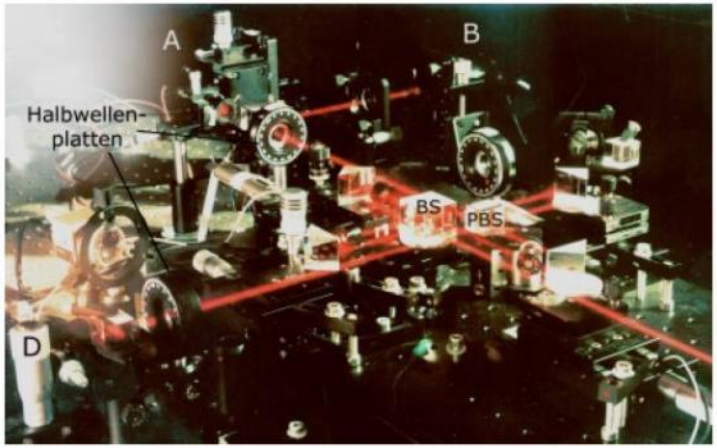
The Dual Rail Qubit

In theory



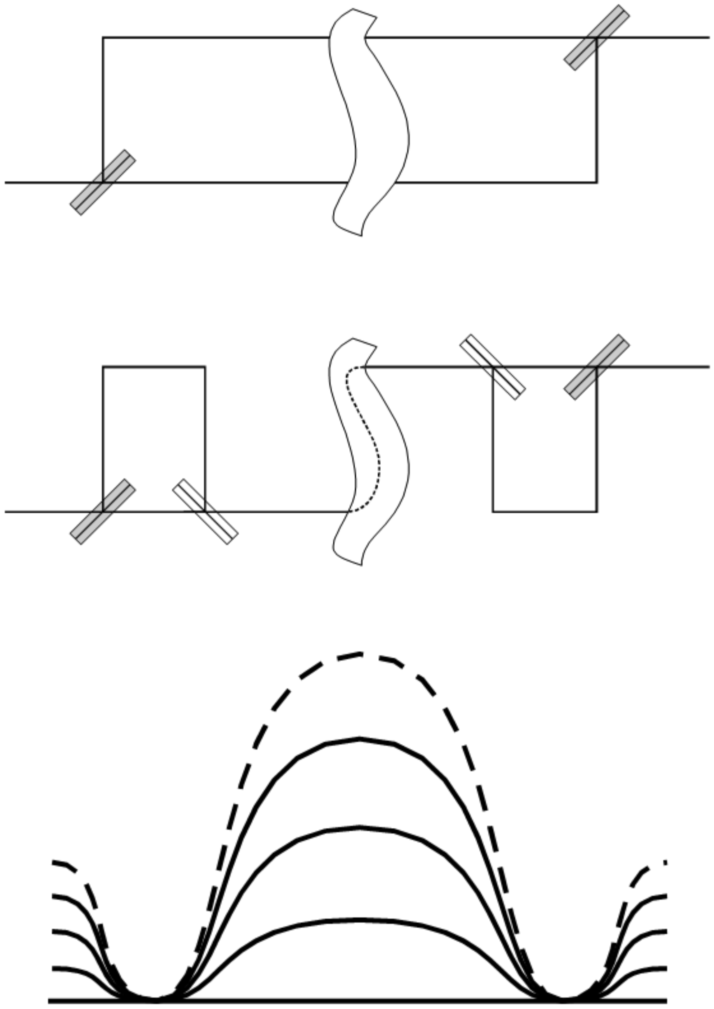
In experiment





The time-bin qubit

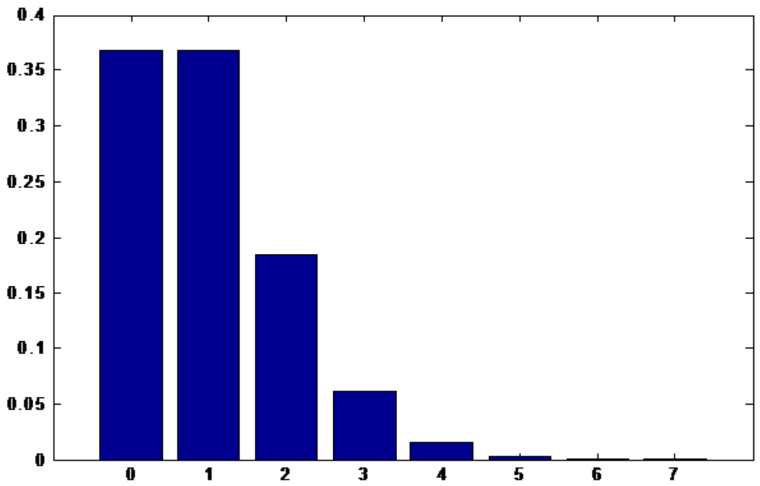
For stability one can multiplex the two rails onto one.



Sources

- Attenuated lasers:
  poissonian statistics

$$p(n,\mu) = \frac{\mu^n}{n!} e^{-\mu}$$

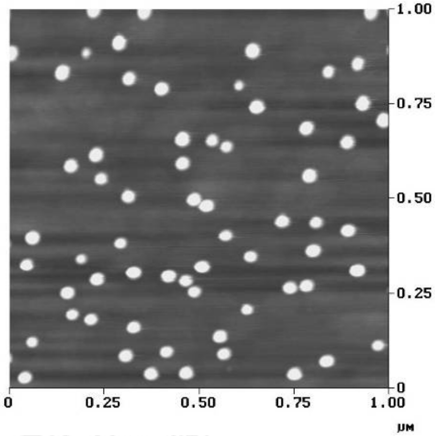


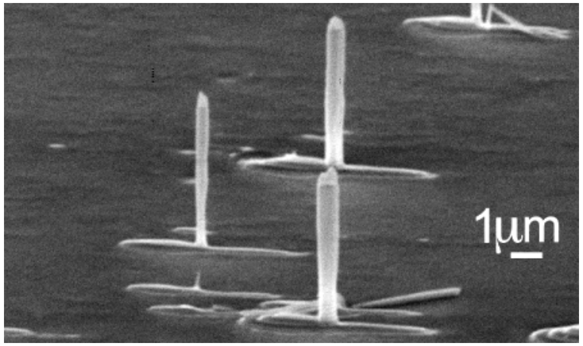
- In order to optimize the secure key rate μ has to be set to a value that scales with *t*, the transmission of the channel

$$\mu_{\text{opt}} \approx t\eta \frac{1 - h(\text{QBER}) - h(2\,\text{QBER})}{1 - h(2\,\text{QBER})}$$

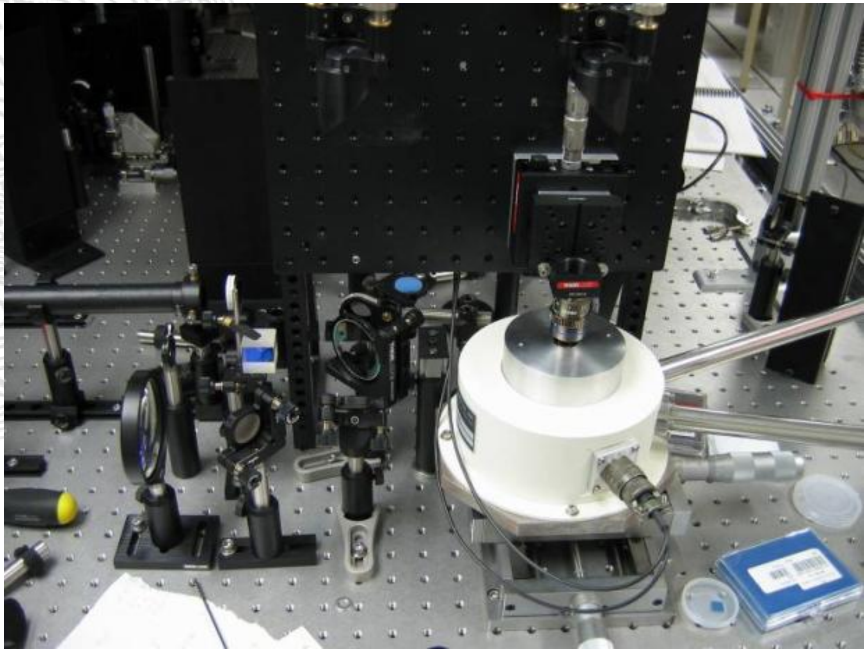
$$K \approx R \frac{1}{2} \mu_{\text{opt}} \left[1 - h(\text{QBER}) - h(2\,\text{QBER})\right]$$

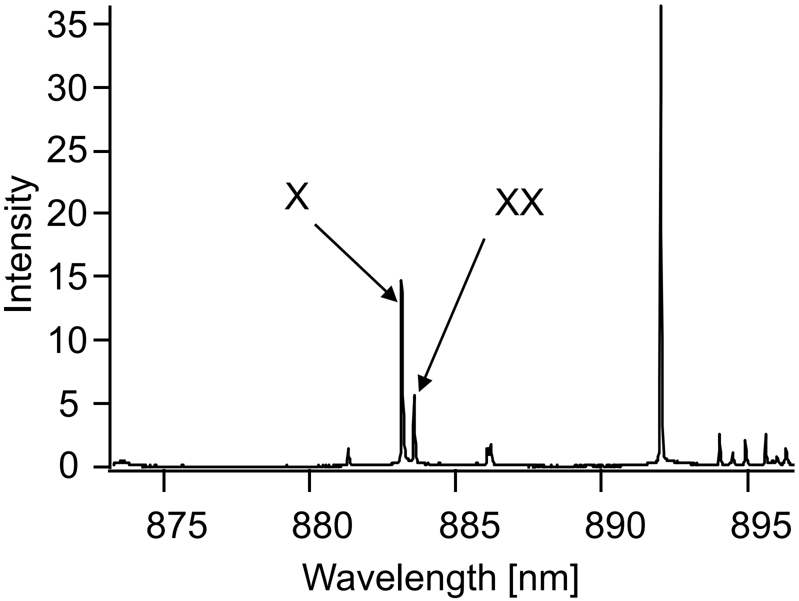
Single Photon



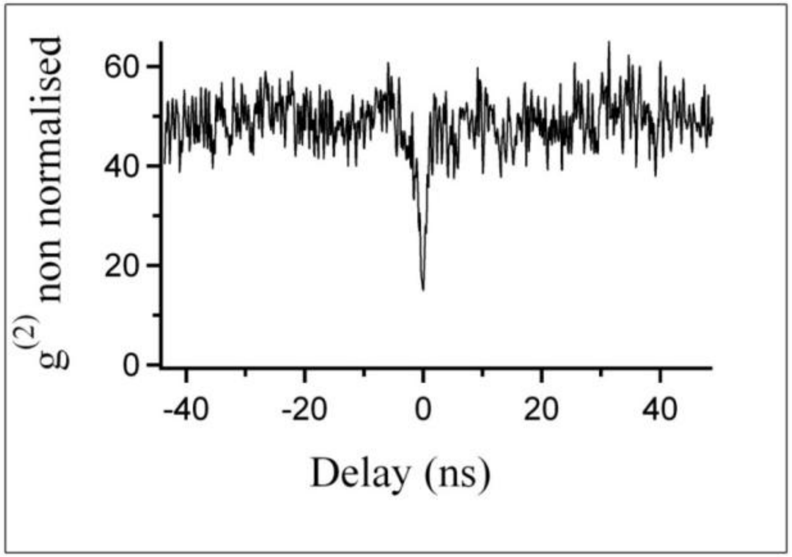


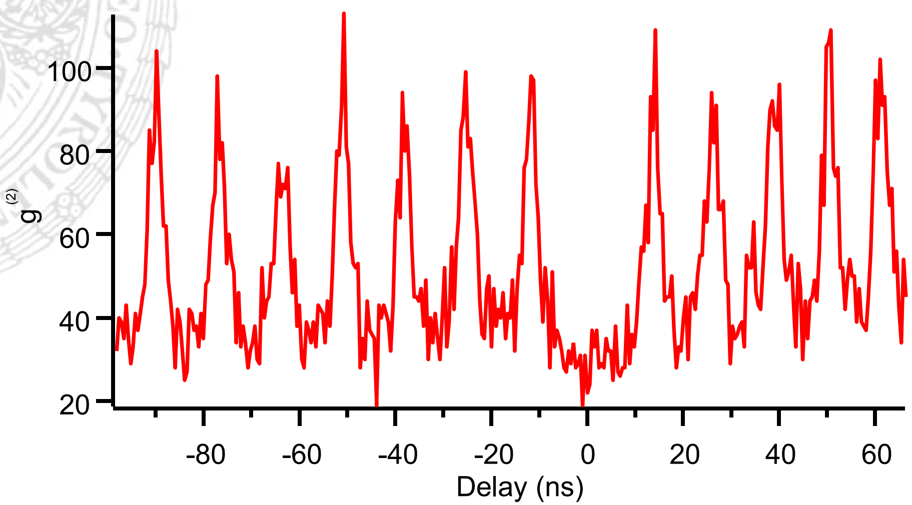
$$K \approx R\,[1 - 2h(\mathrm{QBER})]$$





Single Photons





Second Order Degree of Coherence

Measured by Hanbury Brown – Twiss Interferometry

$$g^{(2)}(\tau) = \frac{\langle I(t)I(t+\tau)\rangle}{\langle I(t)\rangle\langle I(t+\tau)\rangle}$$

CW

Two-photon suppression limited by detector resolution and finite re-excitation probability

Pulsed

Two-photon suppression only limited other background (filter performance)

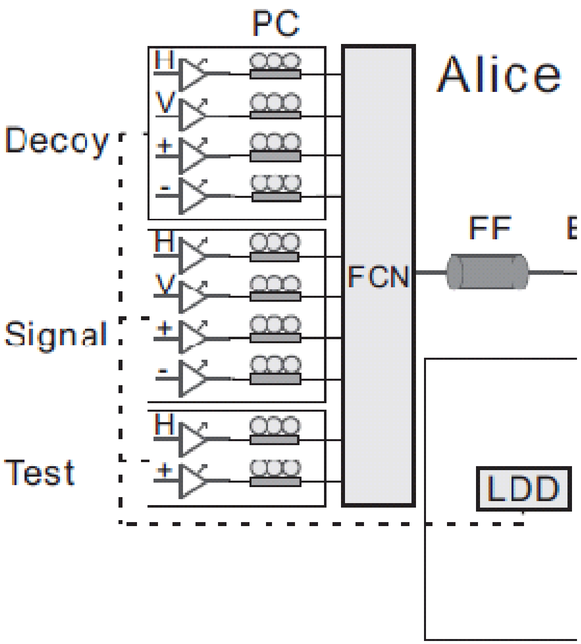
Decoy States

- Alice randomly chooses from a few (e.g. 3) different mean photon numbers

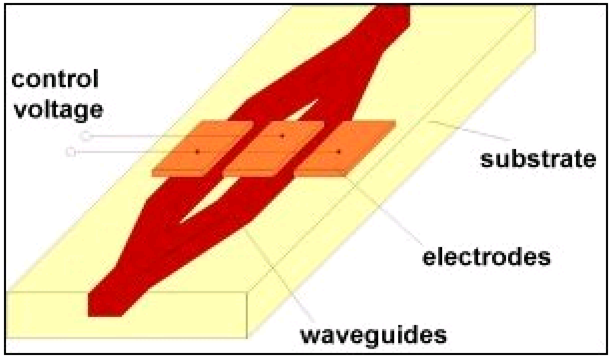
$$\mu_{\text{opt}} \approx \frac{1}{2}\left[1 - \frac{h(\text{QBER})}{1 - h(\text{QBER})}\right] \qquad K \approx R\frac{1}{2}\mu_{\text{opt}}\left[1 - 2h(\text{QBER})\right]$$

Modulation

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



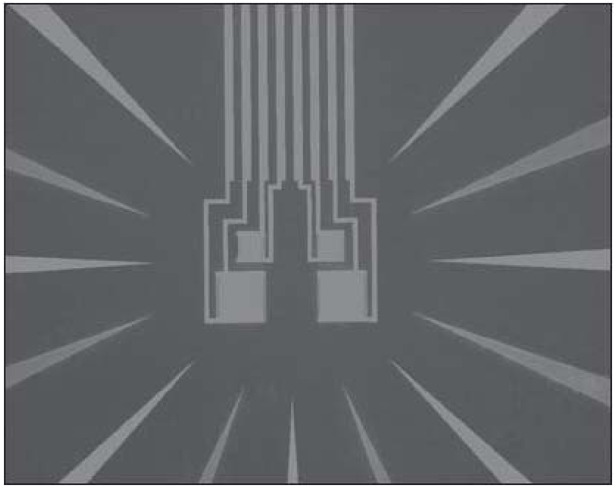
- Modulate laser
  - Polarization
  - Phase (commercially up to 40 GHz)
  - Amplitude for decoy



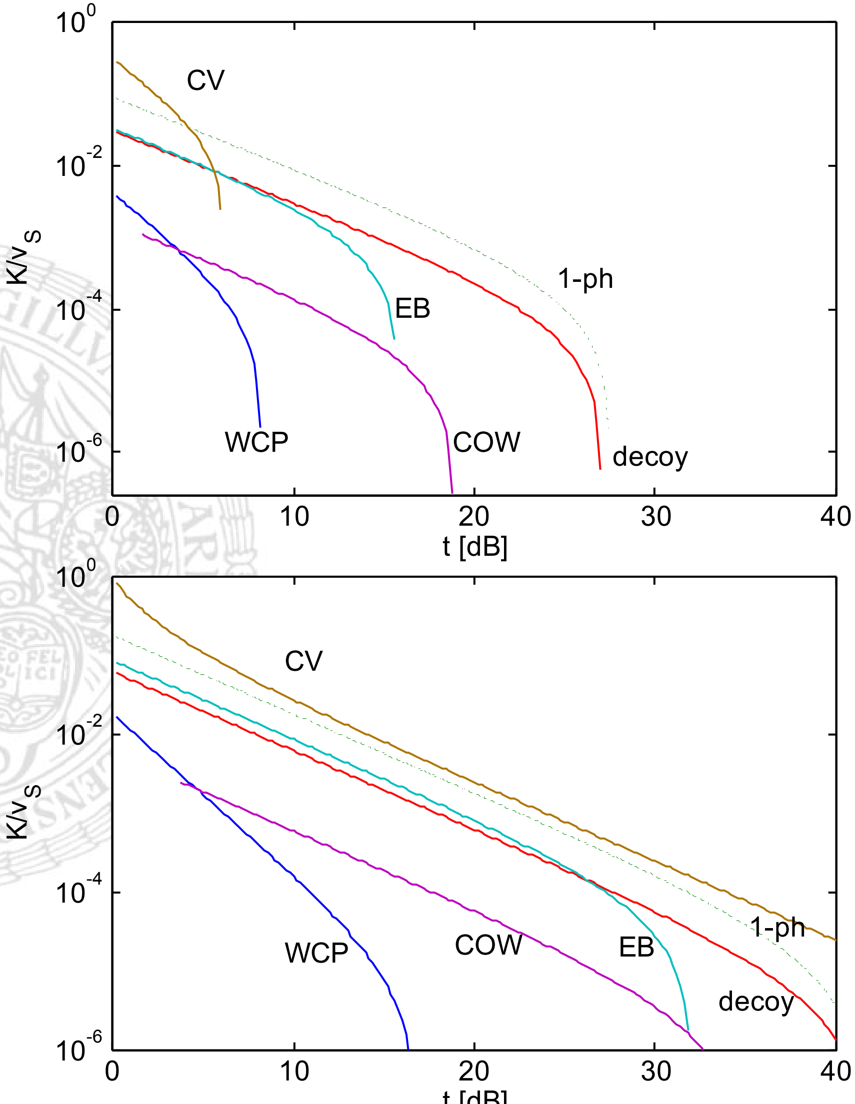
Some Facts About Detectors

- 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



Performance comparison



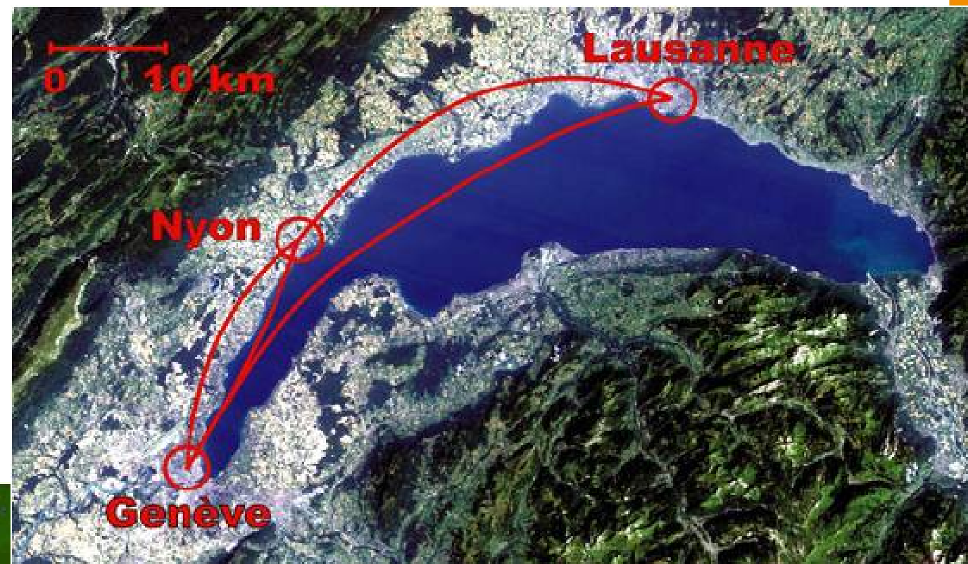
V. Scarani et al., arXiv:0802.4155

CV	Continuous Variables
WCP	Weak Coherent Pulses
COW	Coherent One-Way
EB	Entanglement Based
decoy	Decoy States
1-ph	Single Photon Source

Platform	**Parameter**	**Set #1**	**Set #2**
	μ mean intensity	(opt.)	(opt.)
	V visibility: P&M	0.99	0.99
	V visibility: EB	0.96	0.99
BB84,	t_B transmission in Bob's device	1	1
COW	η det. efficiency	0.1	0.2
	p_d dark counts	10^{-5}	10^{-6}
	ε (COW) bit error	0.03	0.01
	ζ (EB) coherent 4 photons 0 0	0	0
	leak EC code	1.2	1
	$v = v_A + 1$ variance	(opt.)	(opt.)
	ε optical noise	0.005	0.001
CV	η det. efficiency	0.6	0.85
	v_{el} electronic noise	0.01	0
	β EC code	0.9	0.9

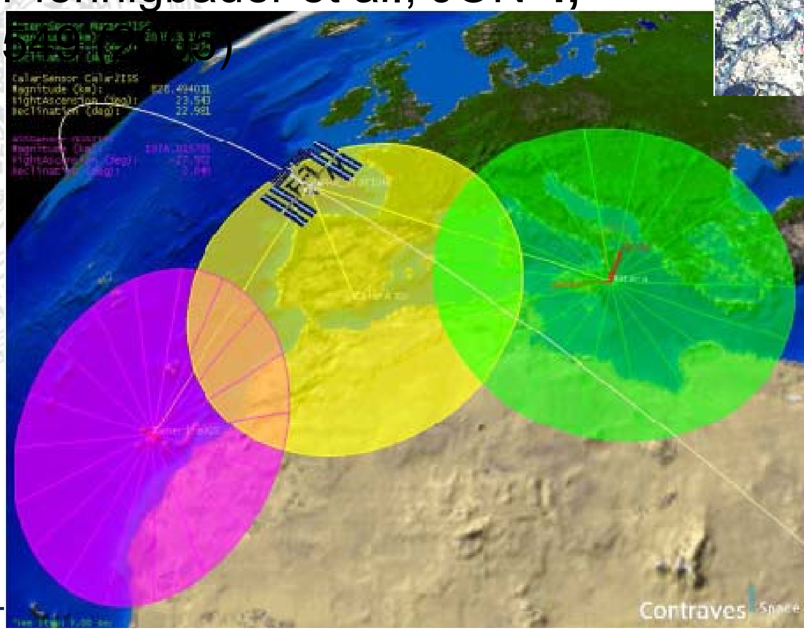
Channels

- Guide light in single-mode optical fibers



GAP-Optique, U. Geneva

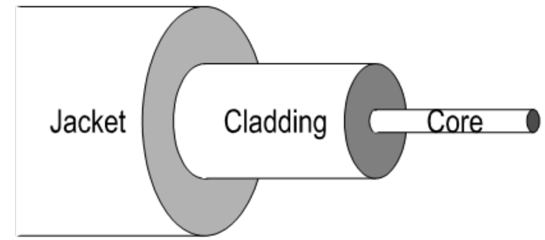
Pfennigbauer et al., JON **4**,

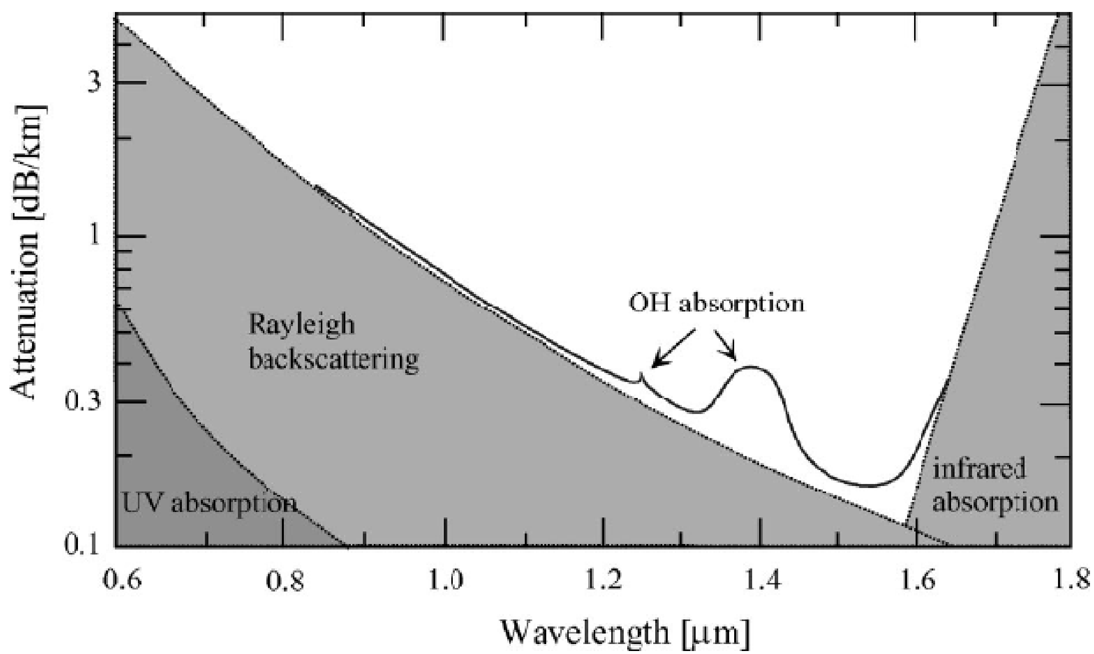


- Broadcast photons from a satellite using telescopes

Optical Fibers

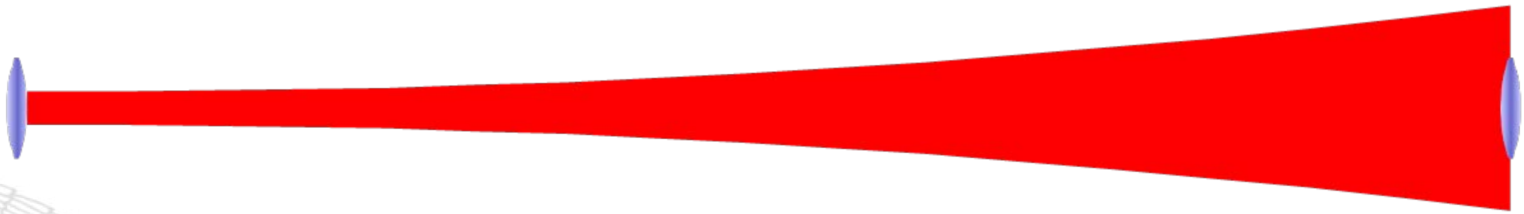
- Fused silica core guides light
- Attenuation by Rayleigh scattering
- Minimum @1550 nm: 0.17 dB/km = 4%/km loss
- Installed fiber typically has 0.3 dB/km
- Polarization
  - Birefringence needs to be compensated
  - Depolarization due to different group velocities (~√L)





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

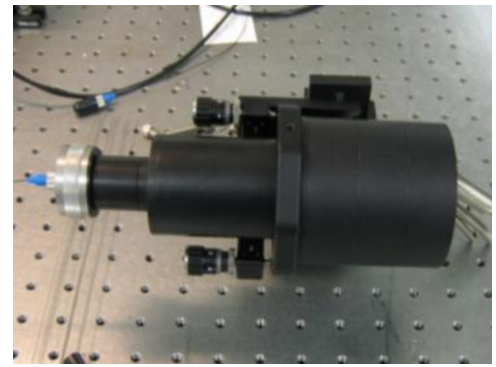
Free-Space Optical Links



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

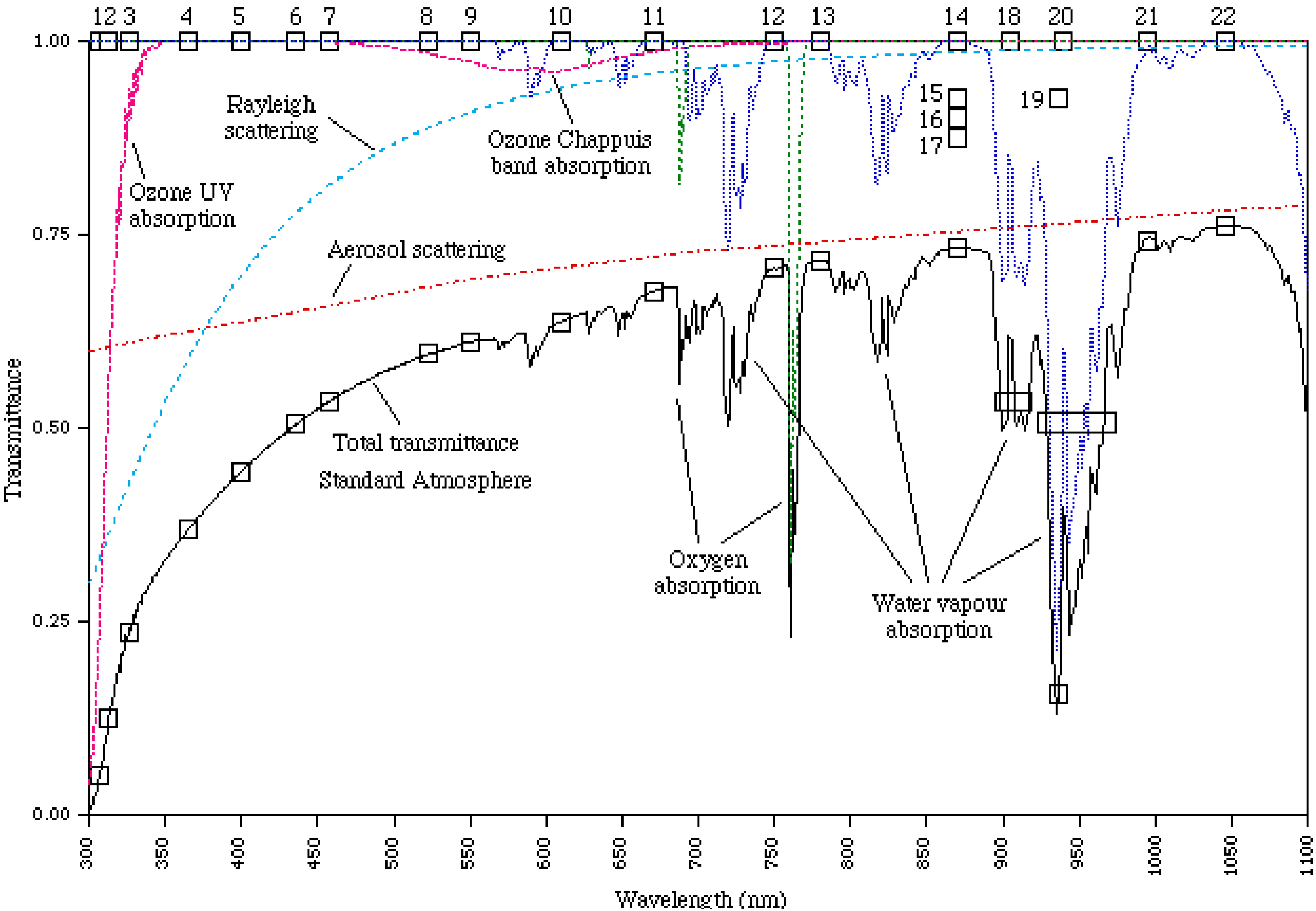
$$A = \frac{L^2(\theta_T^2 + \theta_{\mathrm{atm}}^2)}{D_R^2} 10^{\frac{A_{\mathrm{atm}}}{10}}$$

Telescopes



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

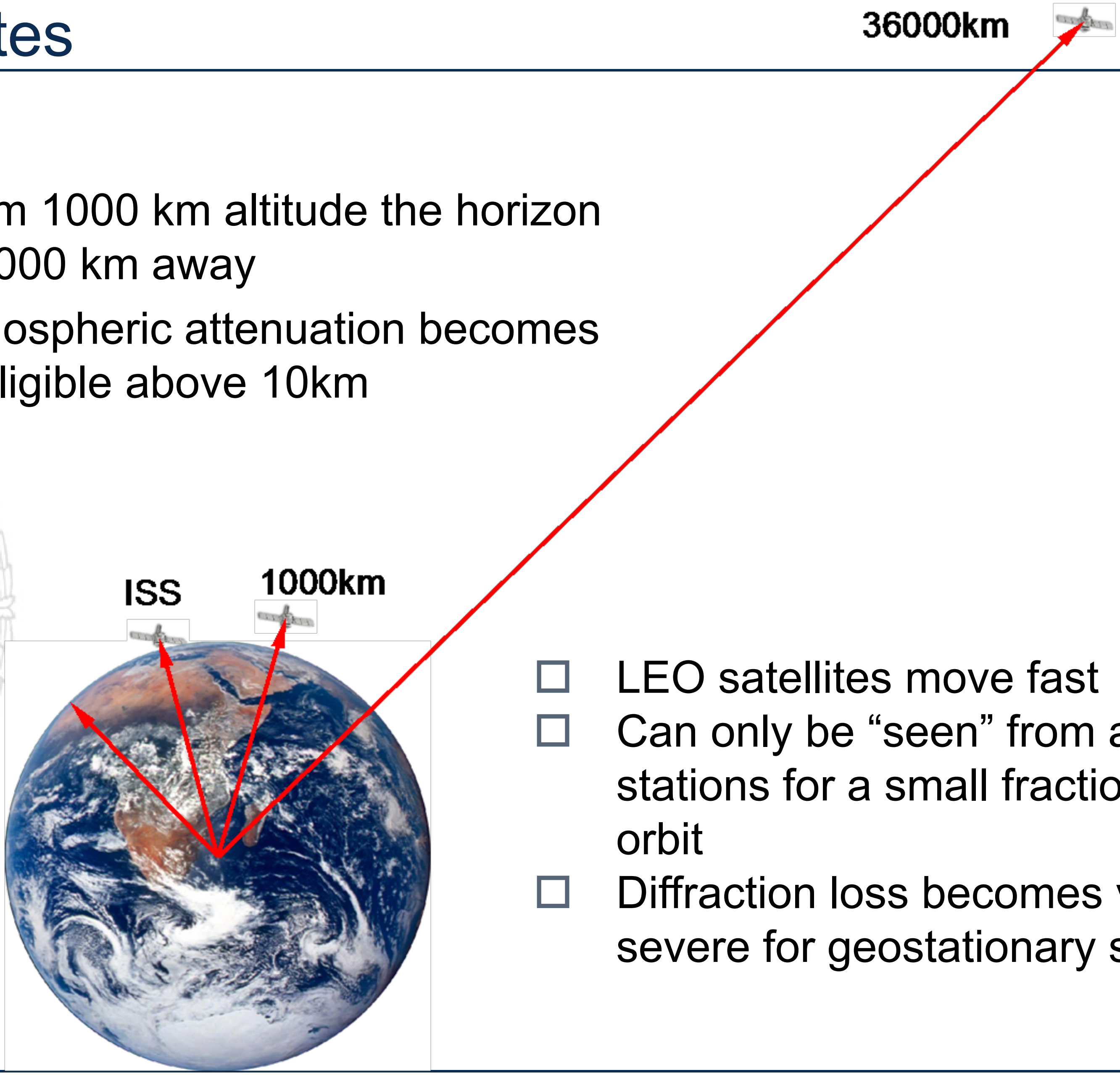
Atmosphere



Rayleigh scattering
Ozone UV absorption
Ozone Chappuis band absorption
Aerosol scattering
Total transmittance
Standard Atmosphere
Oxygen absorption
Water vapour absorption
Transmittance
Wavelength (nm)
1.00
0.75
0.50
0.25
0.00
300
350
400
450
500
550
600
650
700
750
800
850
900
950
1000
1050
1100

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

- 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)

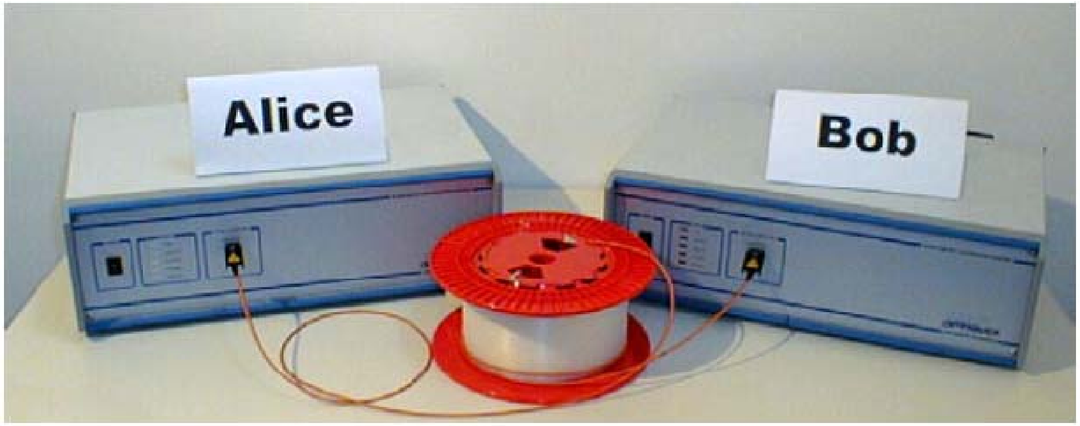


Figure 1. Picture of the p&p system.

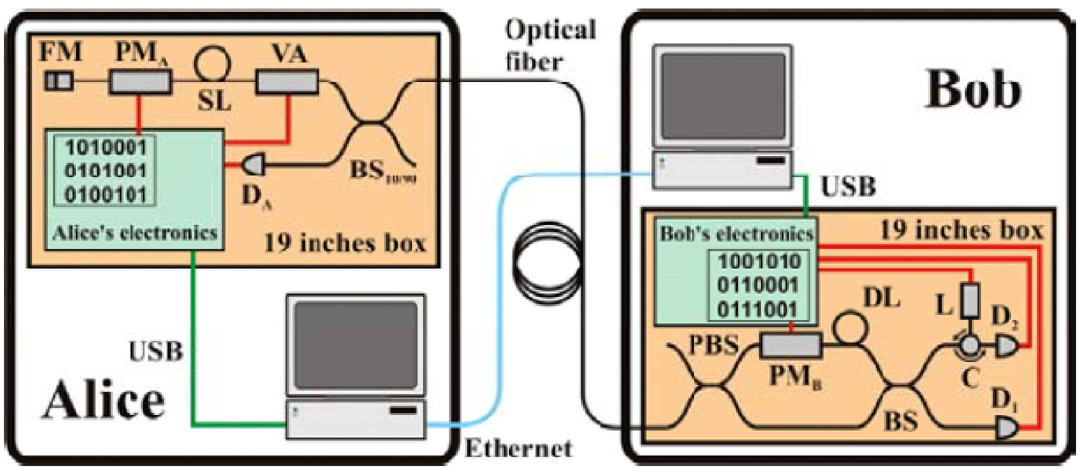
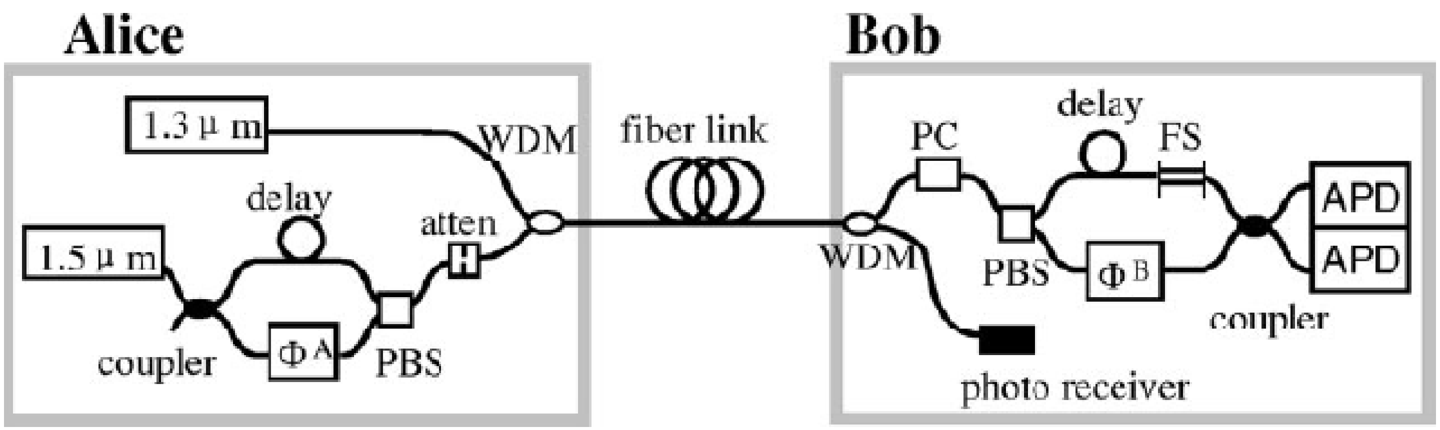


Figure 2. Schematic of the p&p prototype.

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

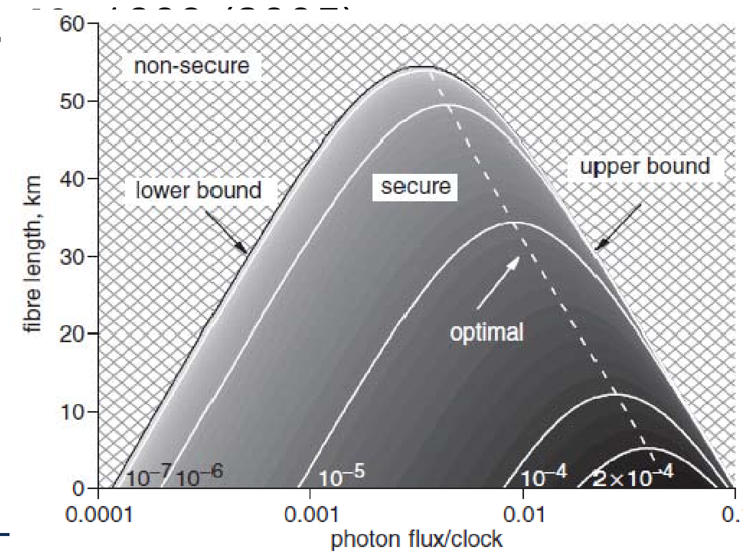
Increasing the distance



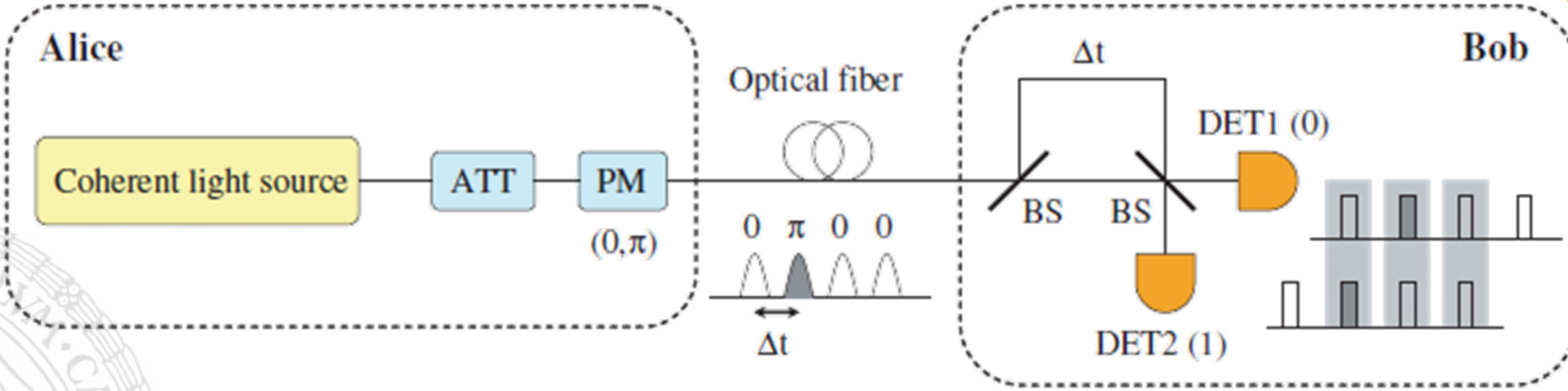
Gobby et al., Appl. Phys. Lett. **84,** 3762 (2004).

Gobby et al., Electron. Lett.

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



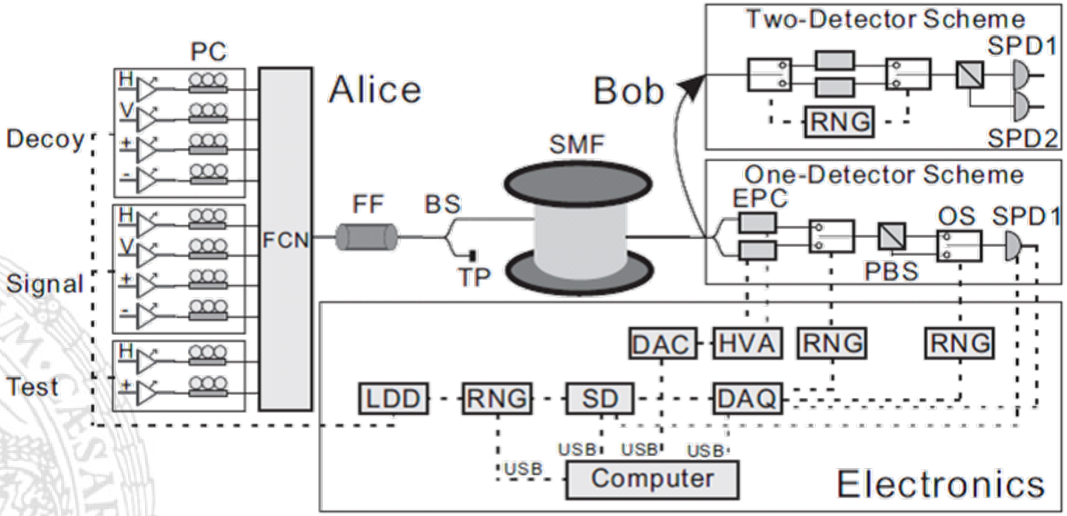
Differential Phase Shift Keying QKD



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

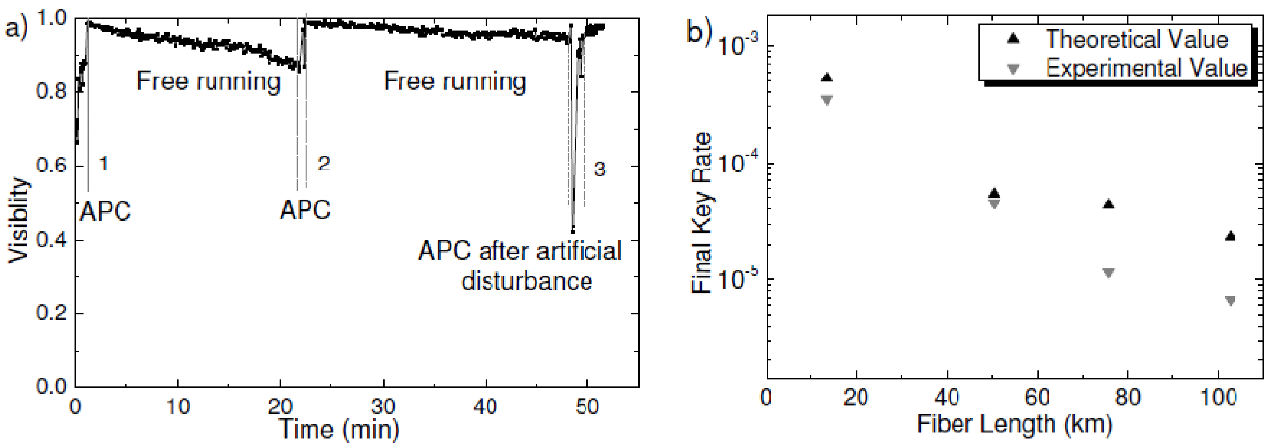
- Better use of clock period
- Achieved 1 GHz clock rate
- Using up-conversion single photon detectors
- @100 km 166 bits/s secure (?)

Polarization in Fiber

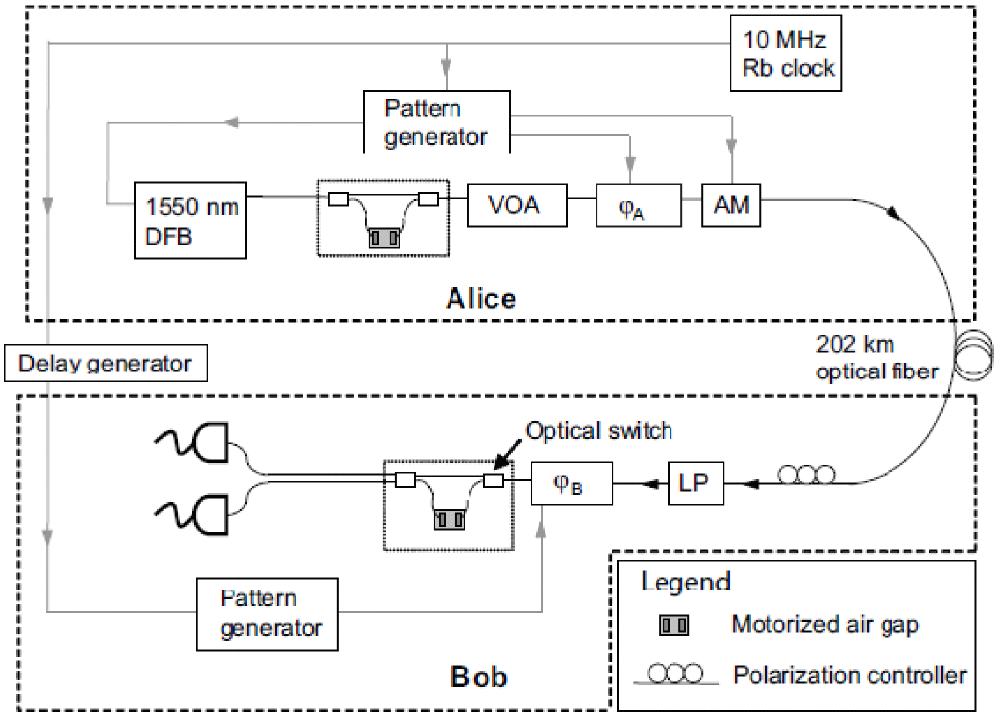


Peng et al., quant-ph/0607129 (2006)

- With decoy states achieved 103 km



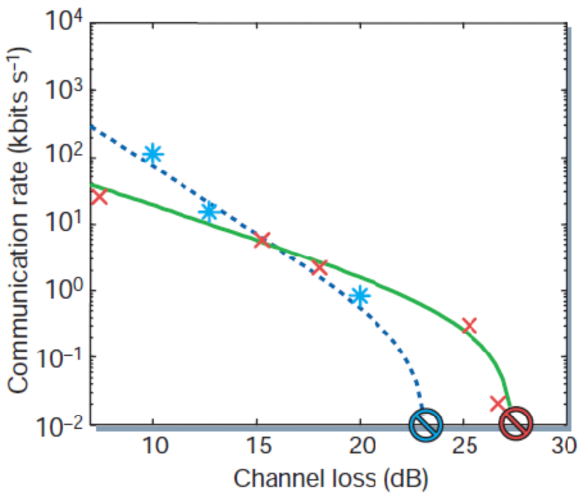
With (Almost) Noise-Free Detectors



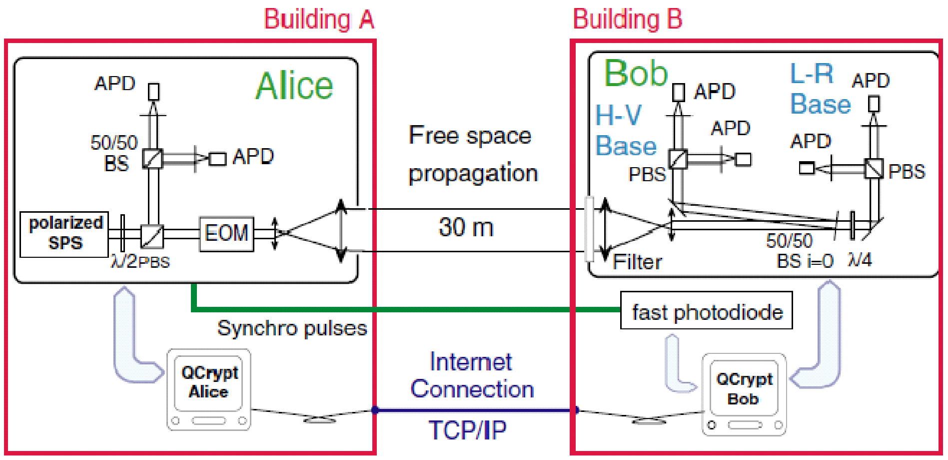
- Superconducting Transition Edge Sensors
  - Virtually zero noise
  - Poor timing ➔ slow clock cycle
- With decoy states achieved unconditionally secure key over 107 km

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)



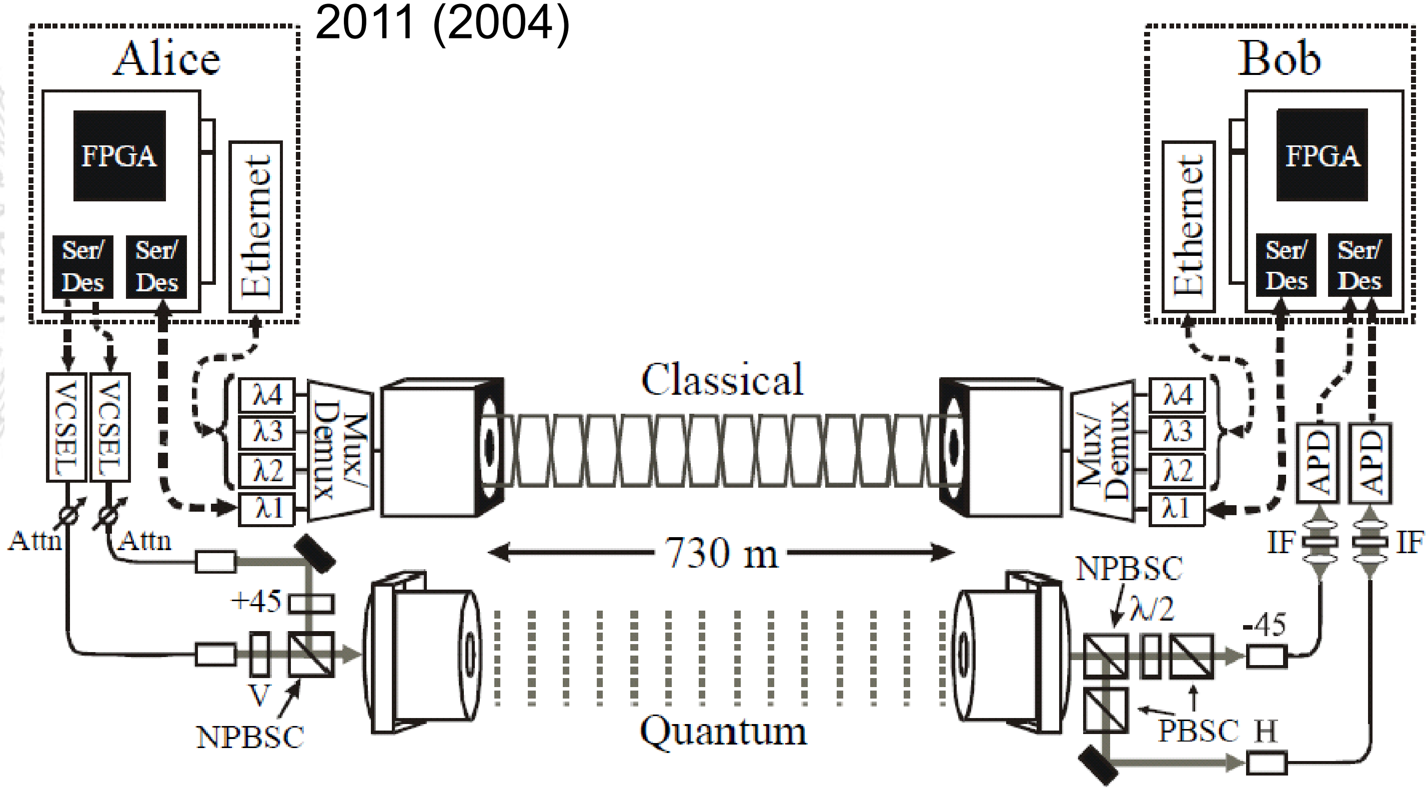
Alleaume et al., NJP **6,** 92 (2004)

- 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

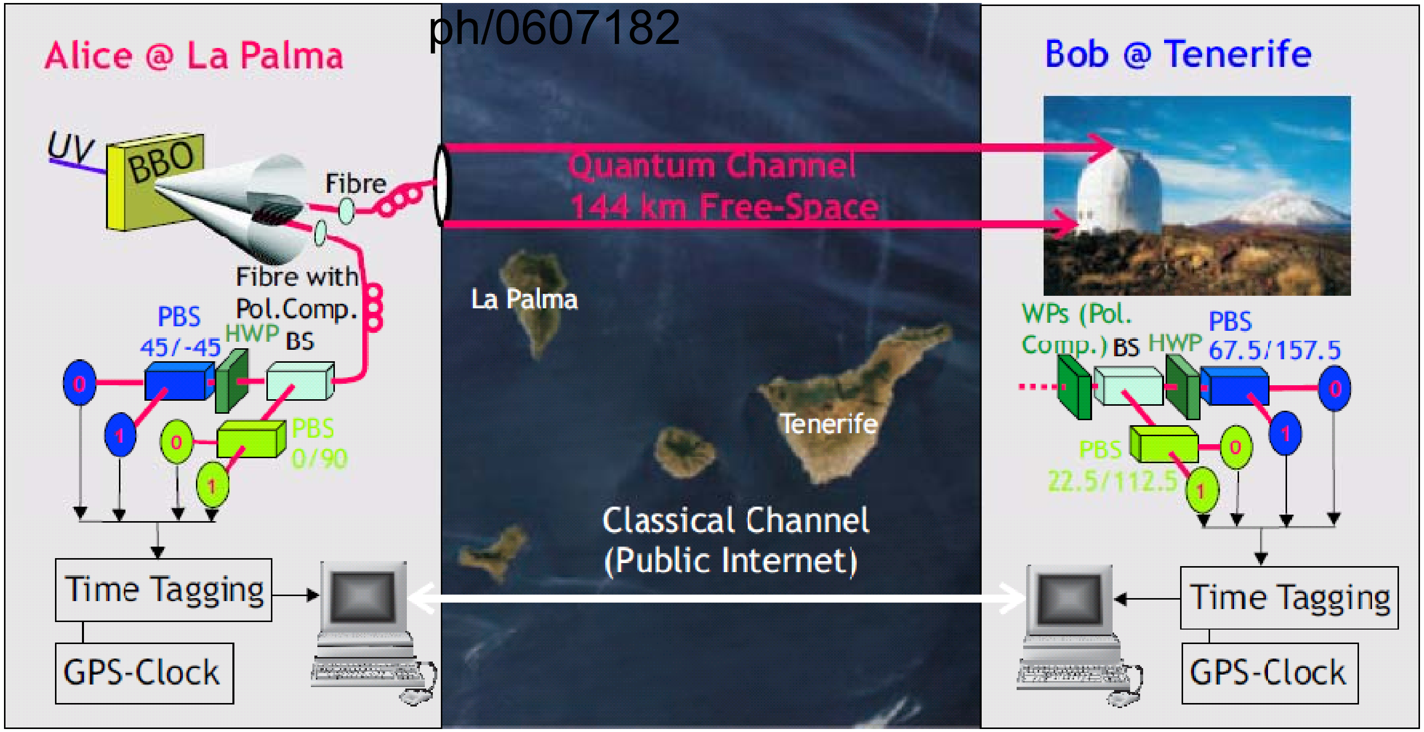
- 690 kbit/s at 0.15 photons/pulse at Alice

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



Free-Space Long Distance

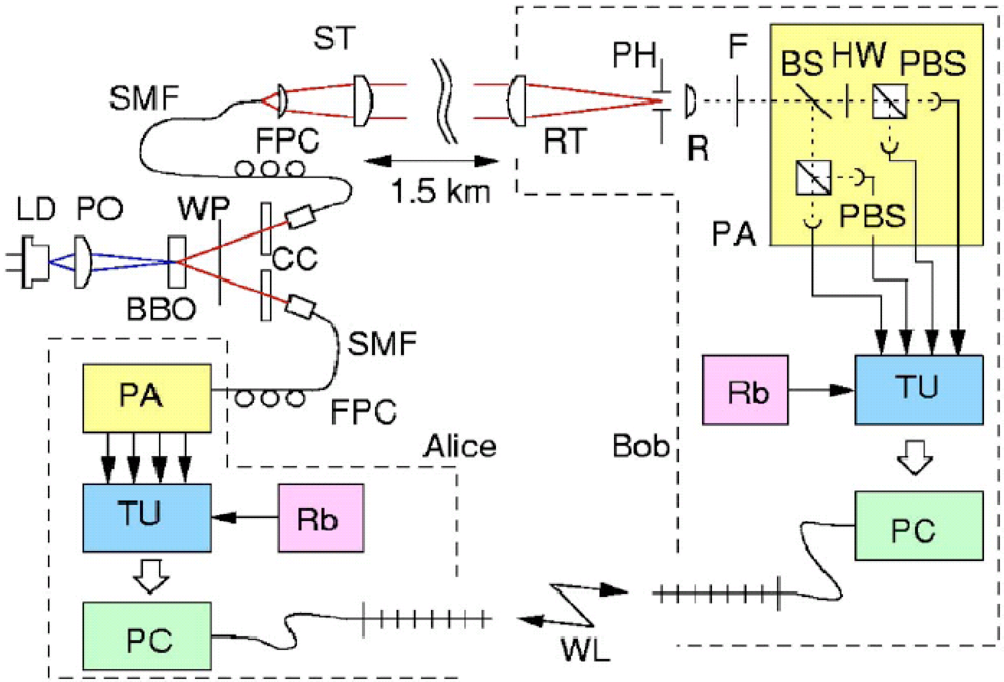
Ursin et al., quant-ph/0607182



- 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)

IQC

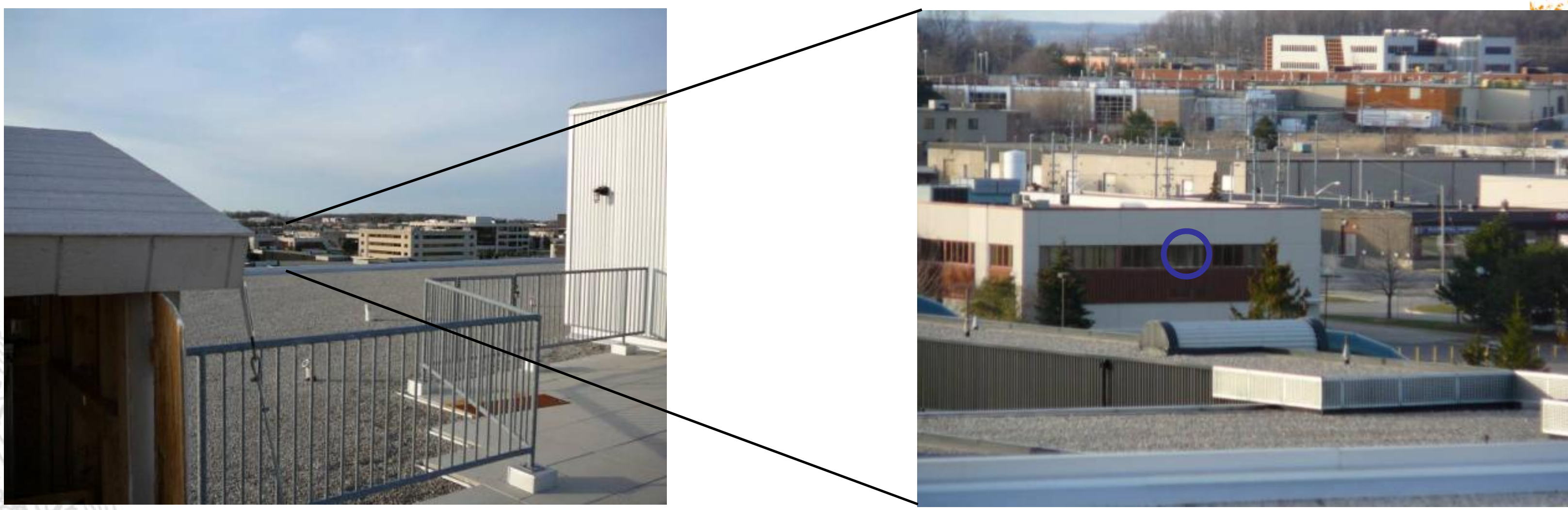
CEIT

PI

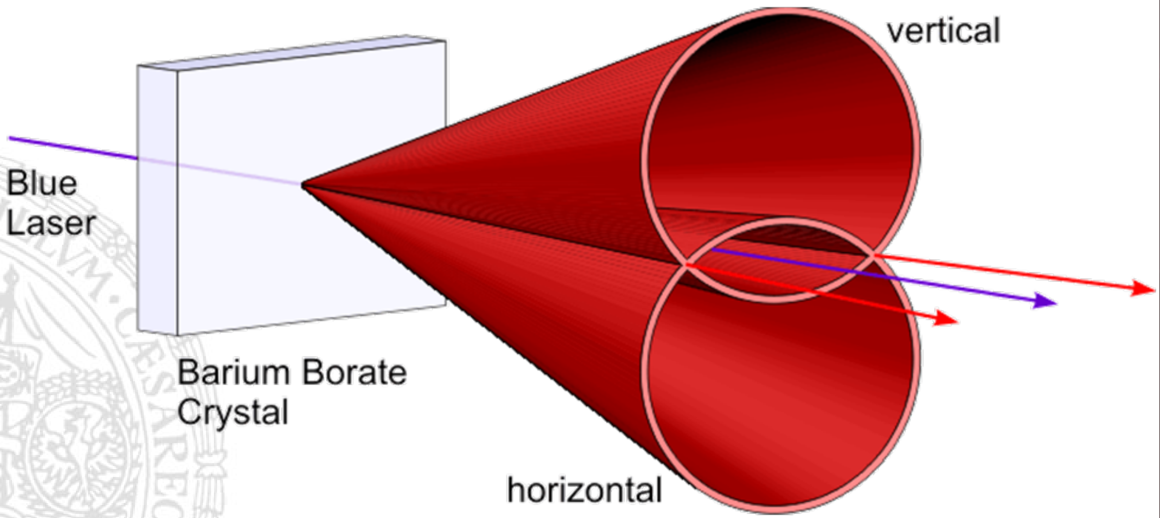
The IQC-Perimeter Institute QKD Experiment

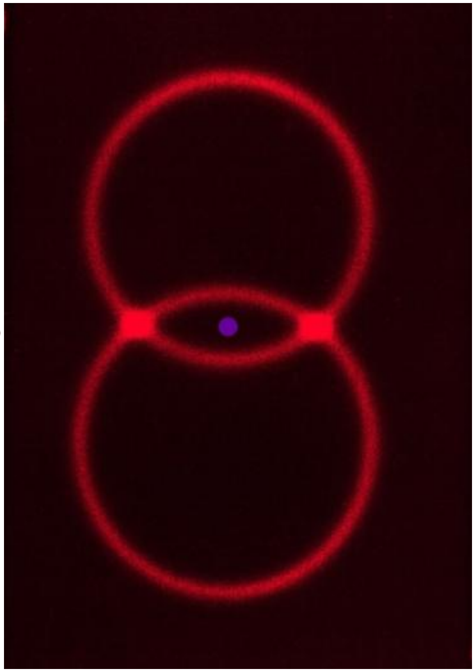
http://maps.google.com/maps/ms?msa=0&msid=
103964276287441386699.00000113448f5481181e2

Views



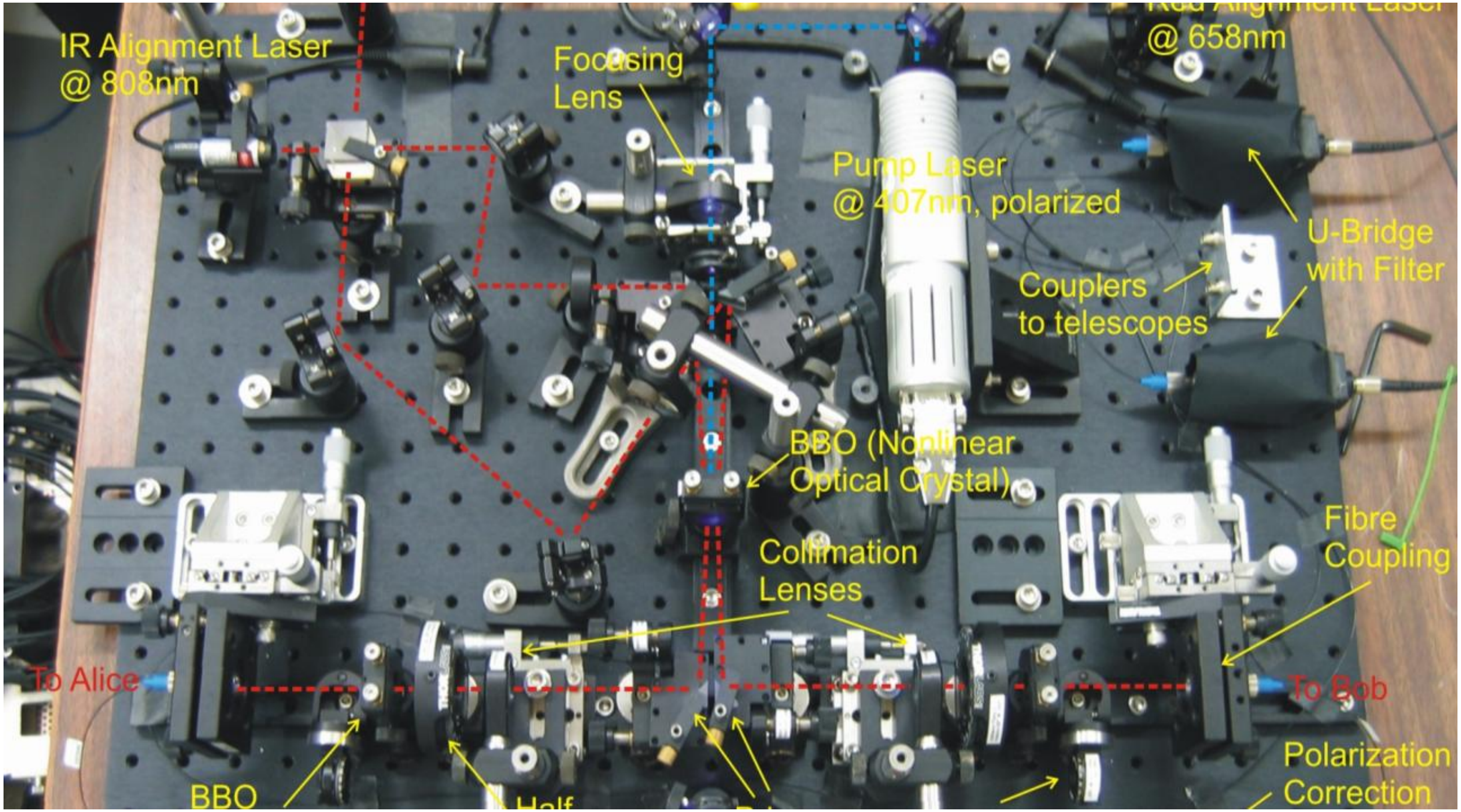
Entangled Photon Pairs





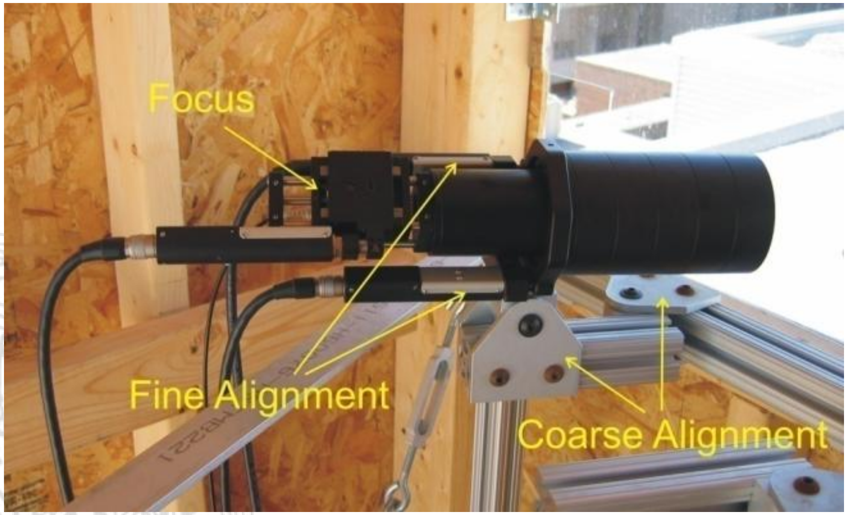
$$|\Psi\rangle = \frac{1}{2}\left(|H\rangle_1 |V\rangle_2 + |V\rangle_1 |H\rangle_2\right)$$

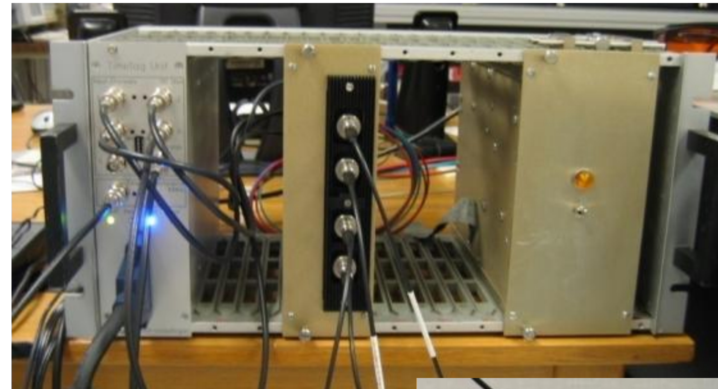
- Parametric down-conversion:
  blue photon converts into pair of red photons
- Polarization entangled photon pairs via special geometry

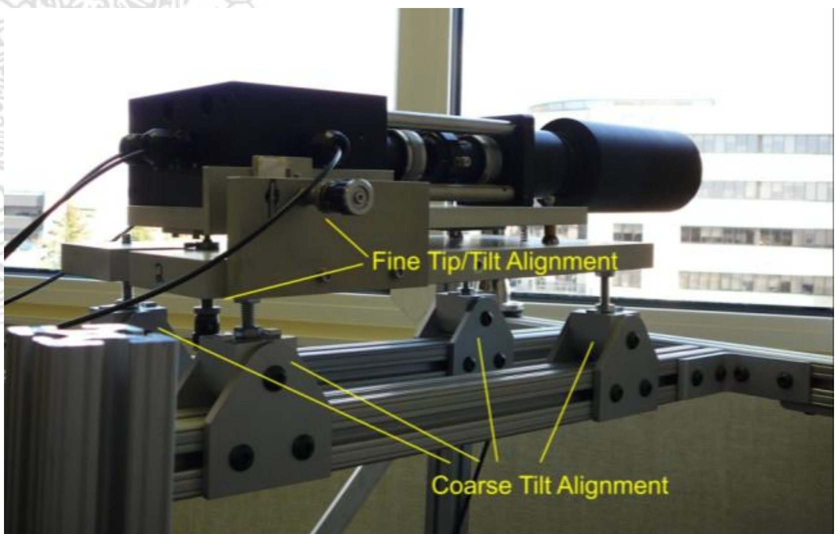


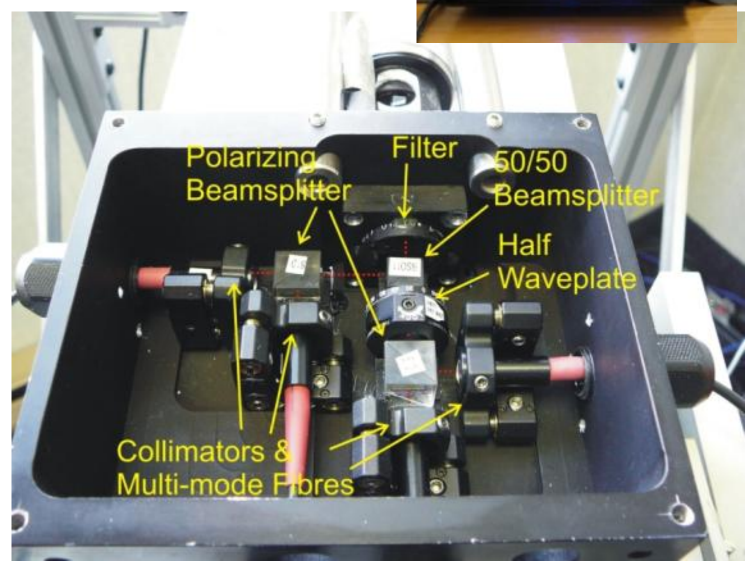
Entangled Photon Pair Source

Send / Receive Equipment

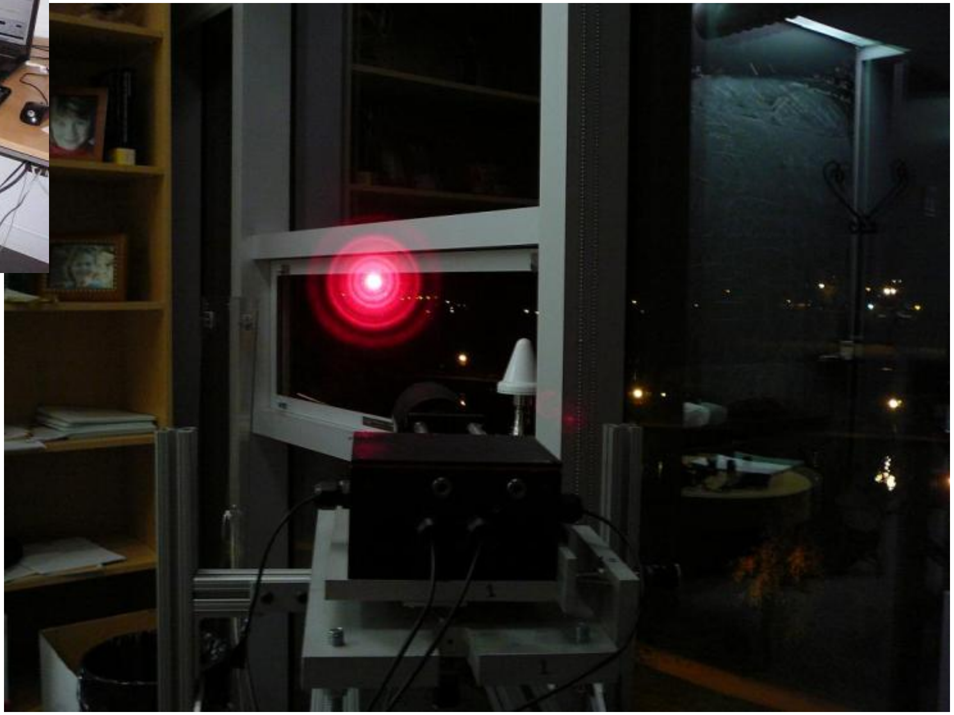




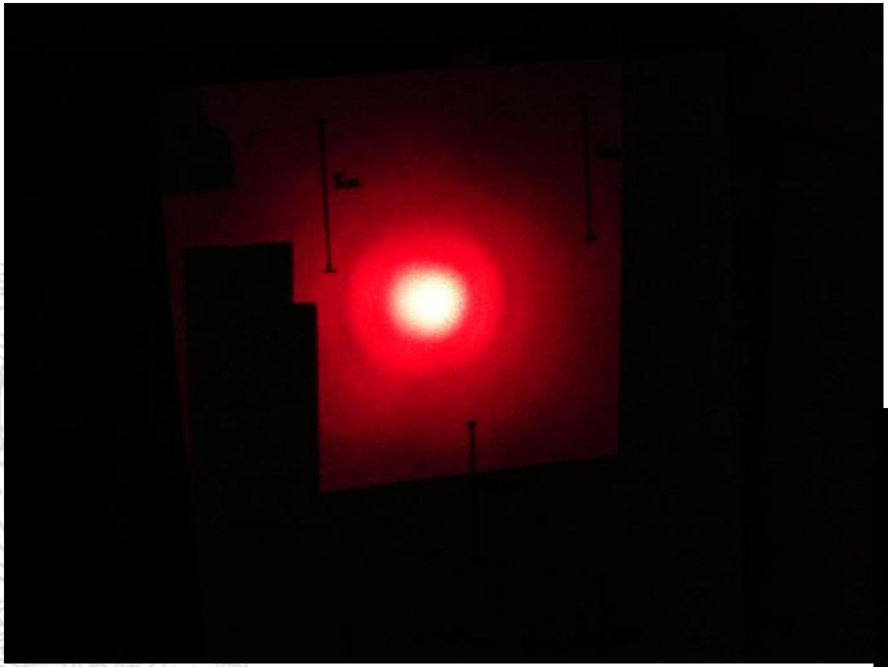


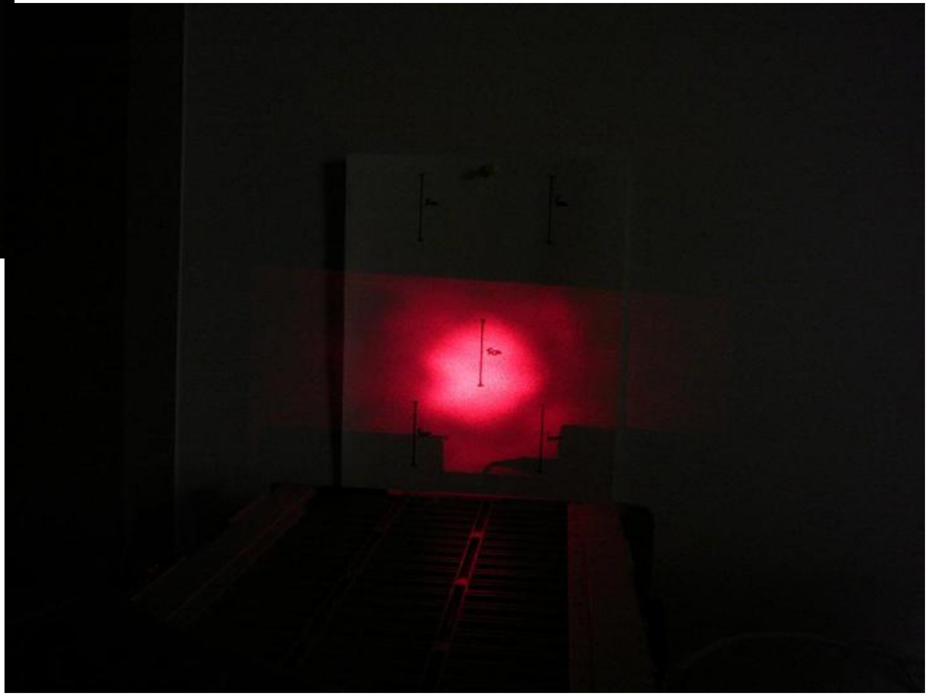


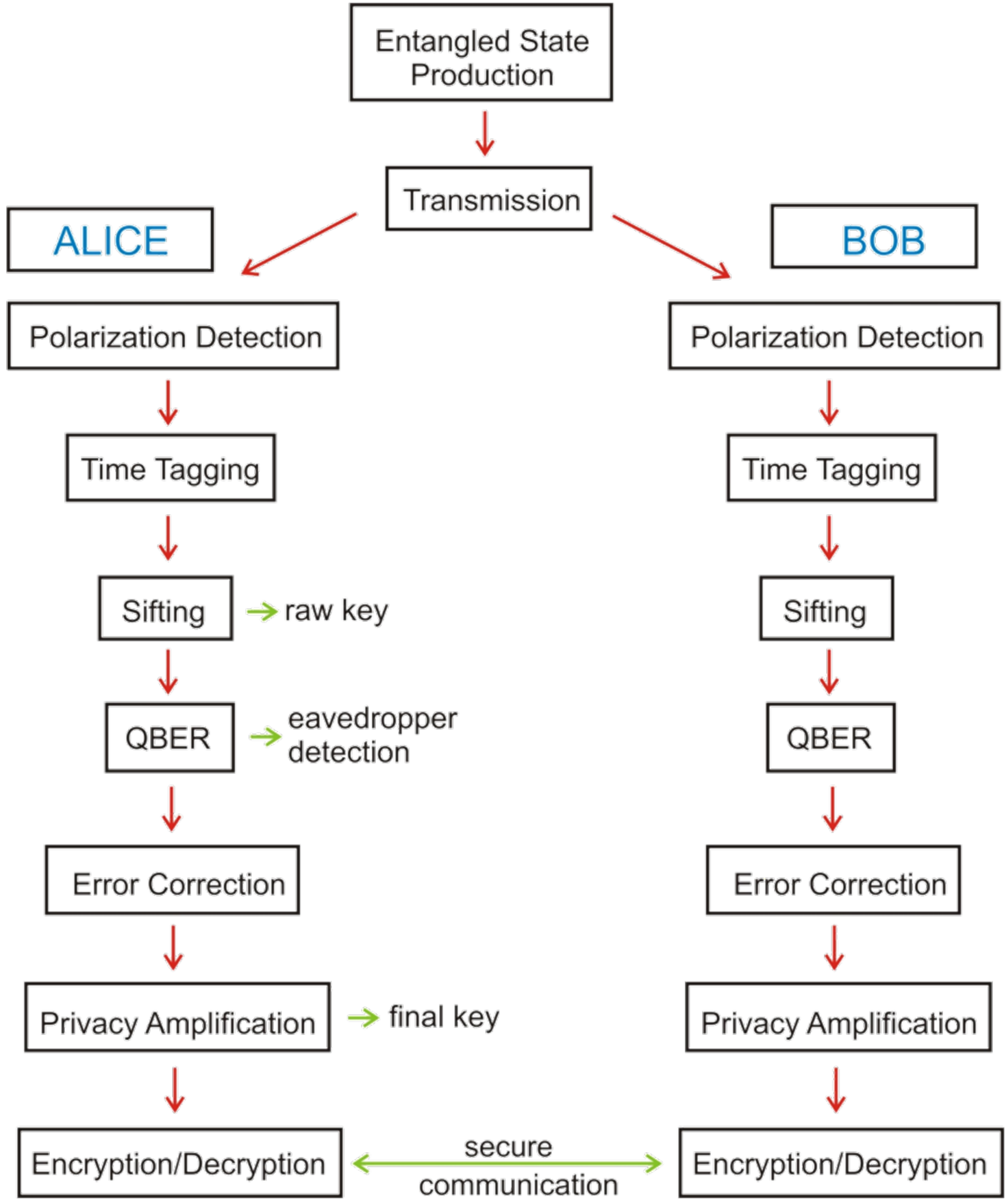
Bob @ Perimeter Institute



Alignment Spots

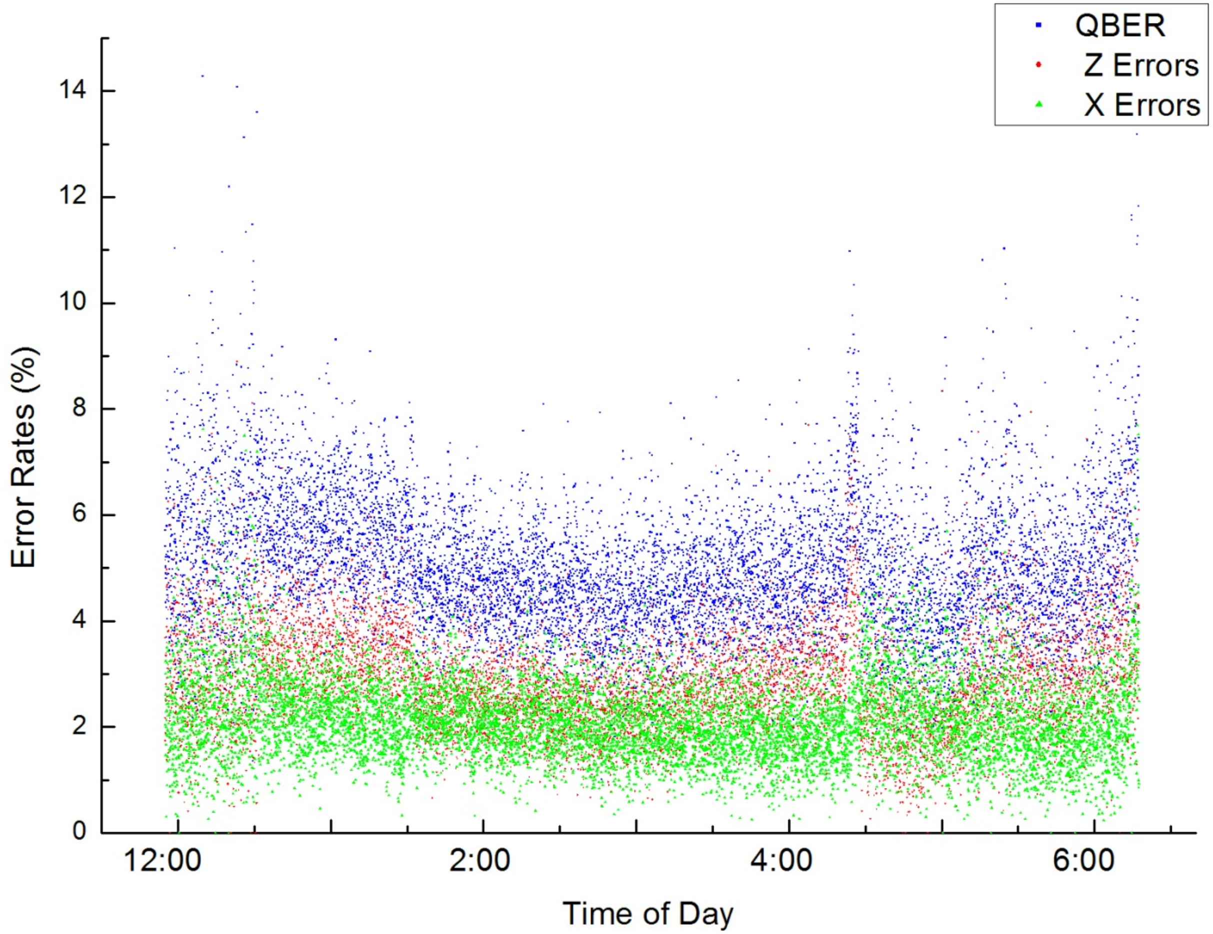






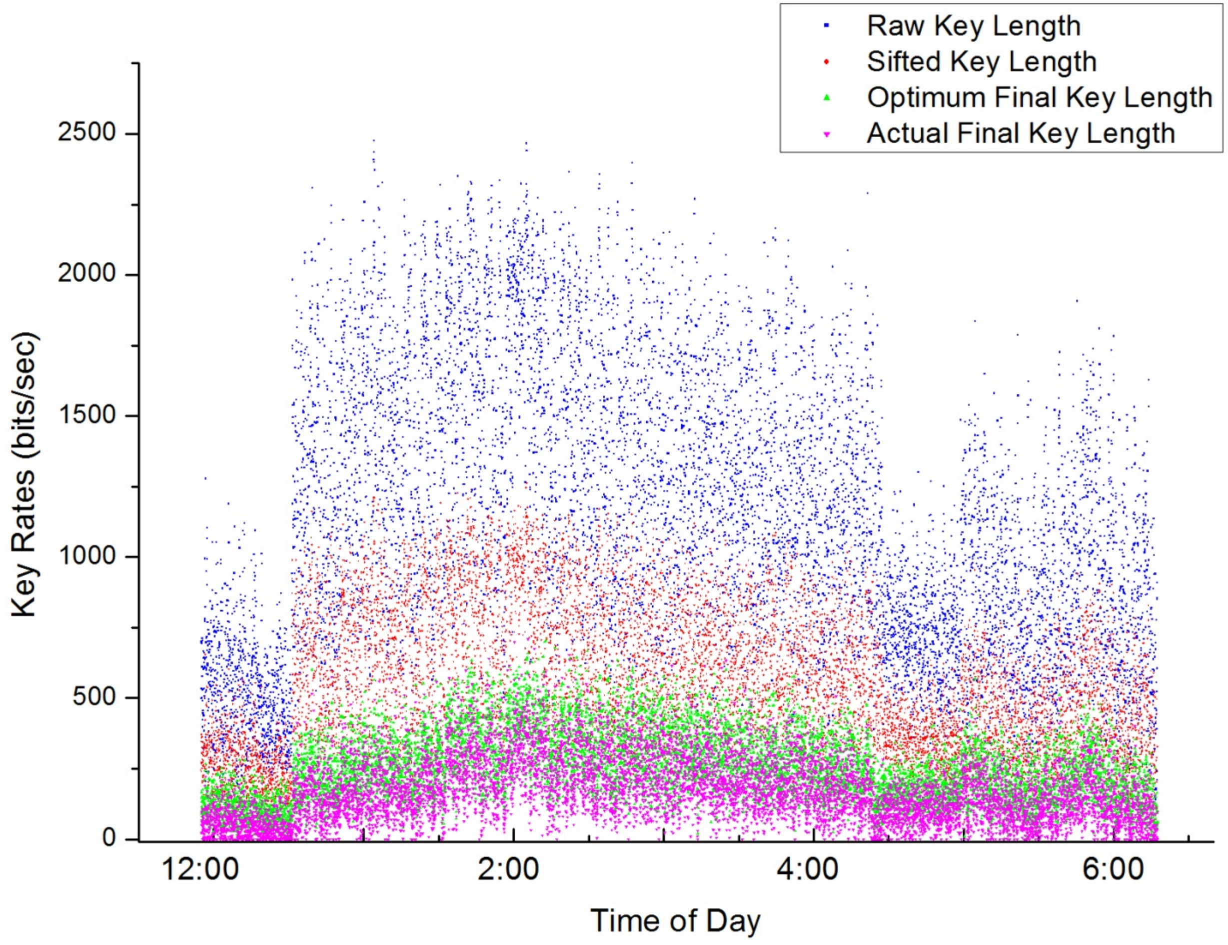
universität innsbruck

QBER

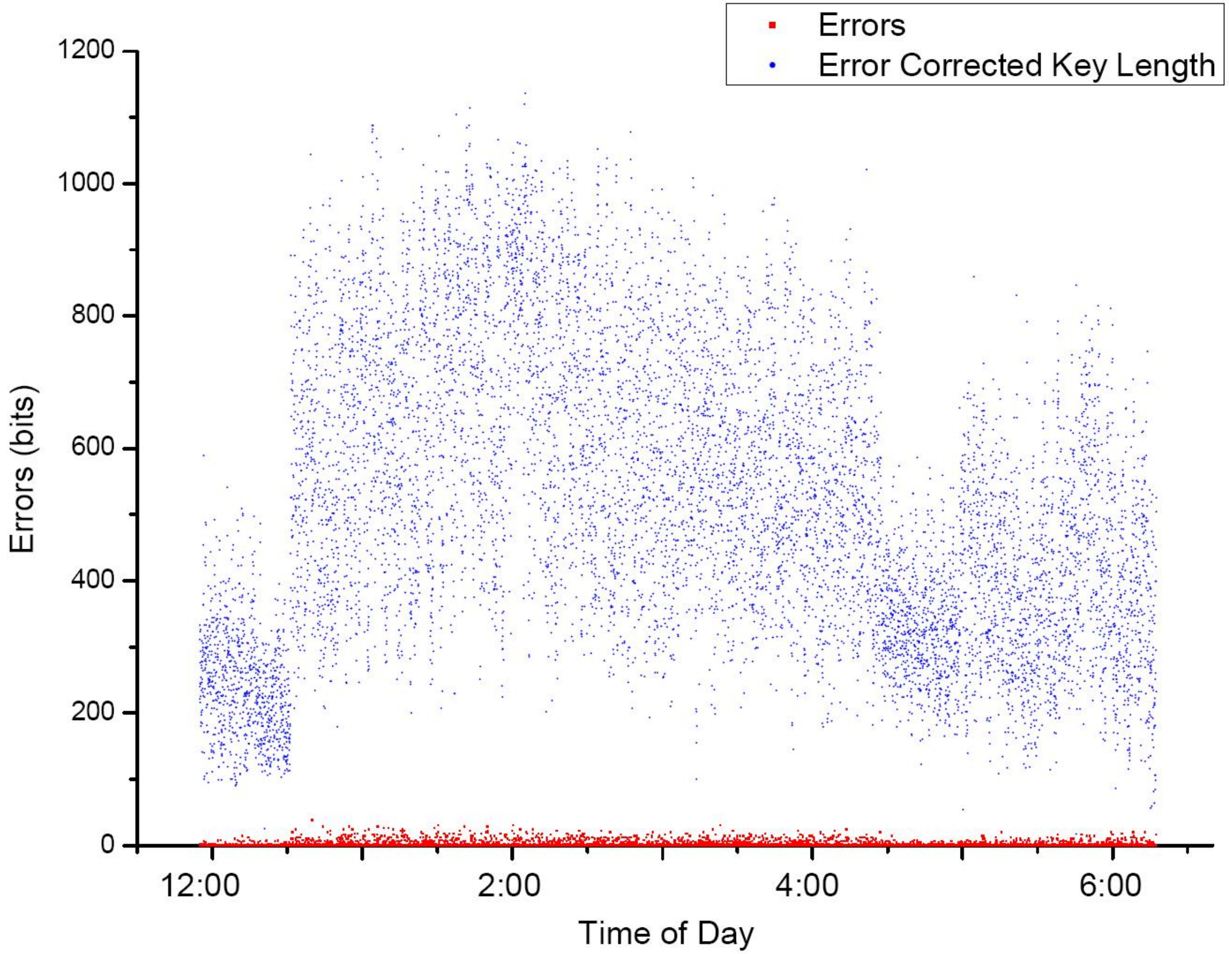


QBER
Z Errors
X Errors
Error Rates (%)
0
2
4
6
8
10
12
14
12:00
2:00
4:00
6:00
Time of Day

Key Rate


Raw Key Length
Sifted Key Length
Optimum Final Key Length
Actual Final Key Length
Key Rates (bits/sec)
0
500
1000
1500
2000
2500
12:00
2:00
4:00
6:00
Time of Day

Corrected Key



Statistics

		Alice				
		H	V	+	-	
Bob	H	39,497	1,218,454	393,100	355,074	2,006,125
	V	1,300,749	112,793	682,595	854,848	2,950,985
	+	680,032	878,628	51,217	1,262,143	2,872,020
	-	548,695	955,146	1,374,648	63,261	2,977,750
		2,604,973	3,165,021	2,501,560	2,535,326	

- Raw key rate = 565 bits/sec
- Sifted key rate = 284 bits/sec
- Optimum final secret key rate = 124 bits/sec
- Actual final secret key rate = 85 bits/sec
- QBER = 4.92%
- Total key of 1,612,239 bits > 1.5MB generated
- Visibilities: H/V = 88.6%, +/- = 91.7%
- Residual error rate = 1.92 e-003 errors/bit