Tools for Experimental Quantum Cryptography

Quantum Information and Quantum Control Conference, Toronto July 2004

Christian Kurtsiefer

Ludwig−**M**aximilians **U**niversität München

Max-**P**lanck-Institut für **Q**uantenoptik

NUS National University of Singapore

http://xqp.physik.uni−muenchen.de

http://www.quantumlah.org

$$: VDI / BMBF, DFG
EQCSPOT, QuComm (EU)

A*STAR
DSTA

Overview

- a free space implementation of BB84
- a relatively simple single photon source
- tools for implementing the Ekert protocol

Why Free Space Cryptography?

- simple setup!
- try to bridge urban area sites without laying out dedicated fibers
- dream about key exchange with satellites

A free−space QKD implementation

- BB84 protocol with polarisation encoding
- faint pulse source (0.1 photons / pulse)
- small & compact setup
- bridge a useful distance

Previous Art

- C. Bennet, IBM 1992 ~30 cm
- J. Franson, Baltimore ~100m
- R. Hughes, Los Alamos ~ km, now: 10 km

(Fiber−based Systems !)

Technical Challenges

- preparation of single photons
- detection of single photons
- transport

  no amplification possible → low losses

- random numbers

  high rate, high entropy

- background suppression
- synchronisation of Alice / Bob

Weak coherent Pulses

- coherent pulses instead of single photons

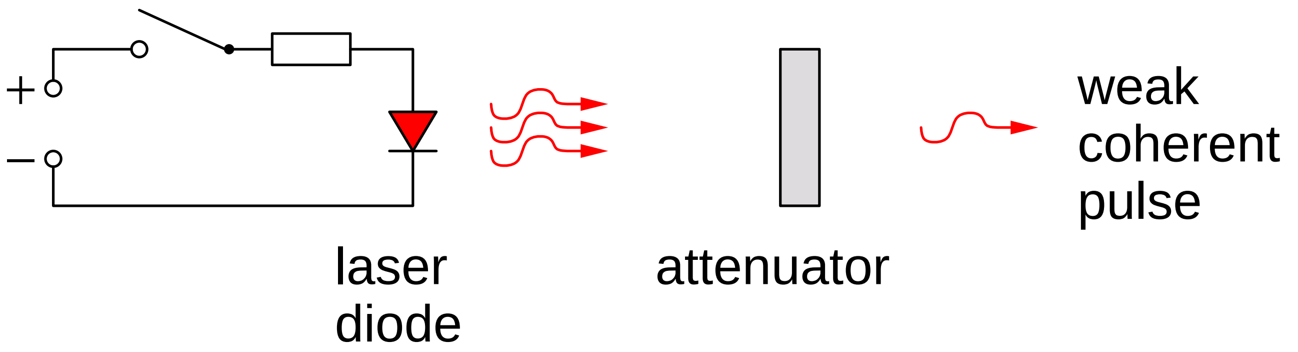
$$p(n) = \frac{\lambda^n}{n!} e^{-\lambda}$$

$\langle n \rangle = 0.1$:

p(0)	= 90.48 %
p(1)	= 9.05 %
p(n>1)	= 0.47 %

+ much simpler to prepare than "true" single photons

laser emit coherent state light fields

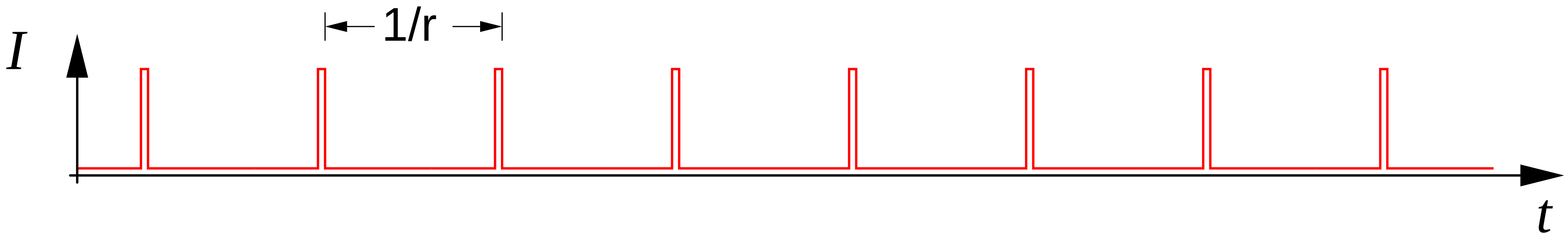


– potentially insecure

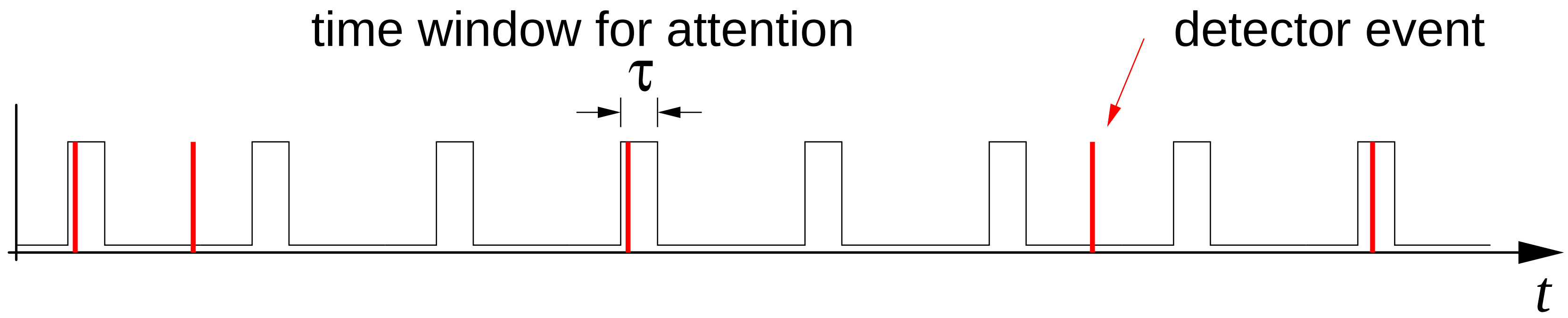
(–) lower signal bandwidth

Timing...

- transmitter:



- receiver:



- background suppression by narrow time windows τ
- clock synchronisation necessary

Practical Estimations

- BB84 raw key rate

$$r = f_0 \times \mu \times \eta_d \div 2 \times T$$

right basis (÷ 2); channel transmission (T); primary send rate (f_0); photons / pulse (μ); detector efficiency (η_d)

- probability for a background event

$$P_D = d \times \tau$$

dark count rate (d); open time window (τ)

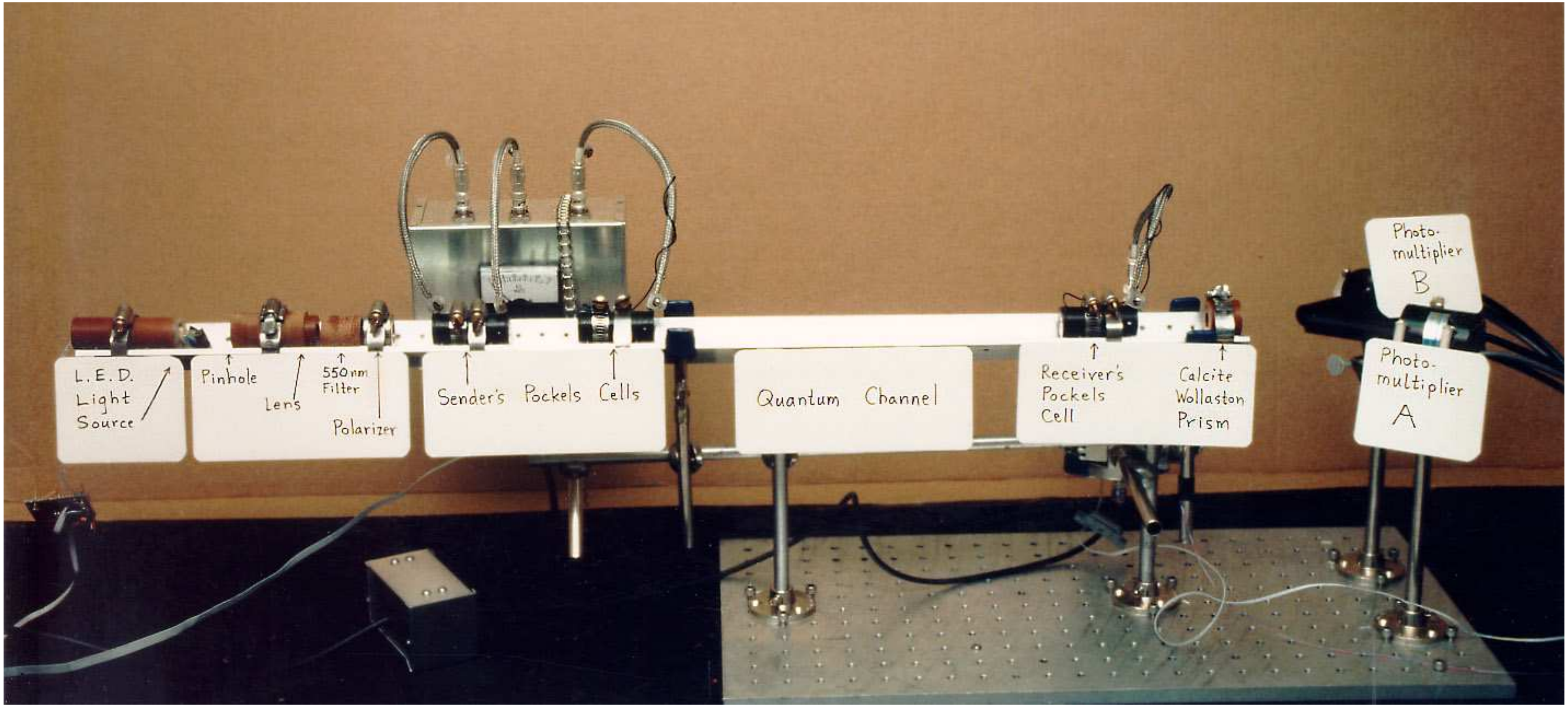
Si:	10^{-7}
InGaAs:	10^{-5}

- detector induced bit error rate

$$QBER = \frac{P_D \times f_0}{r} = \frac{2 \times P_D}{\mu \times \eta_d \times T}$$

Prior Art

Charlie Bennett's Aunt Martha (1984, 1992)

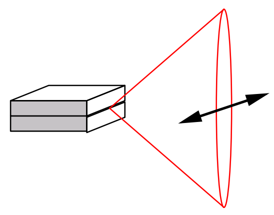


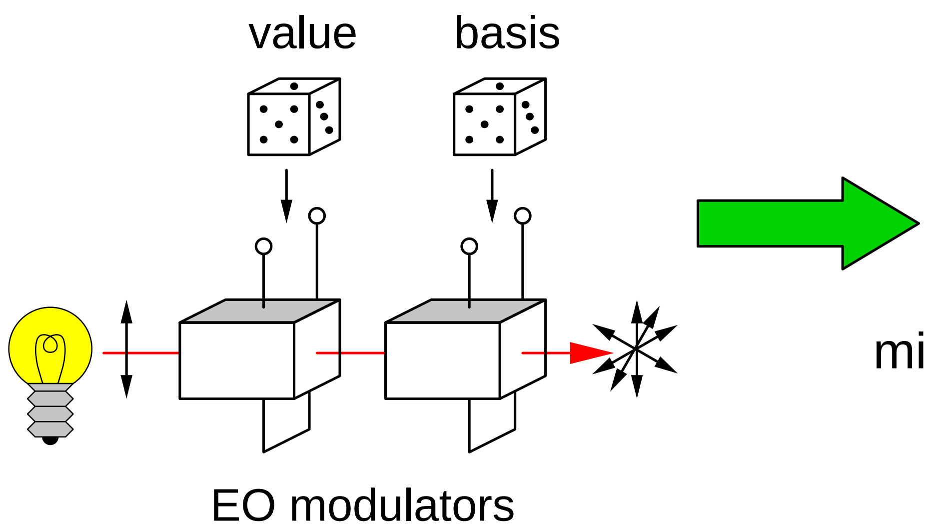
C. Bennett, F. Bessette, G. Brassard, L. Savail and J. Smolin

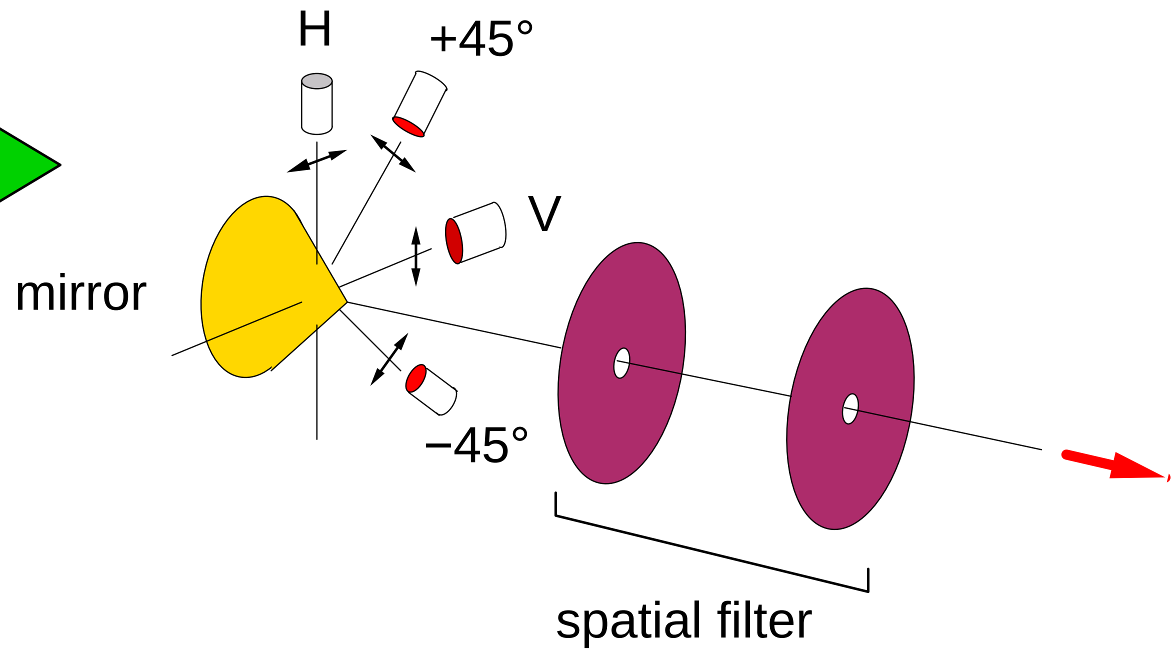
Source miniaturisation

- 4 different sources instead of polarization modulators

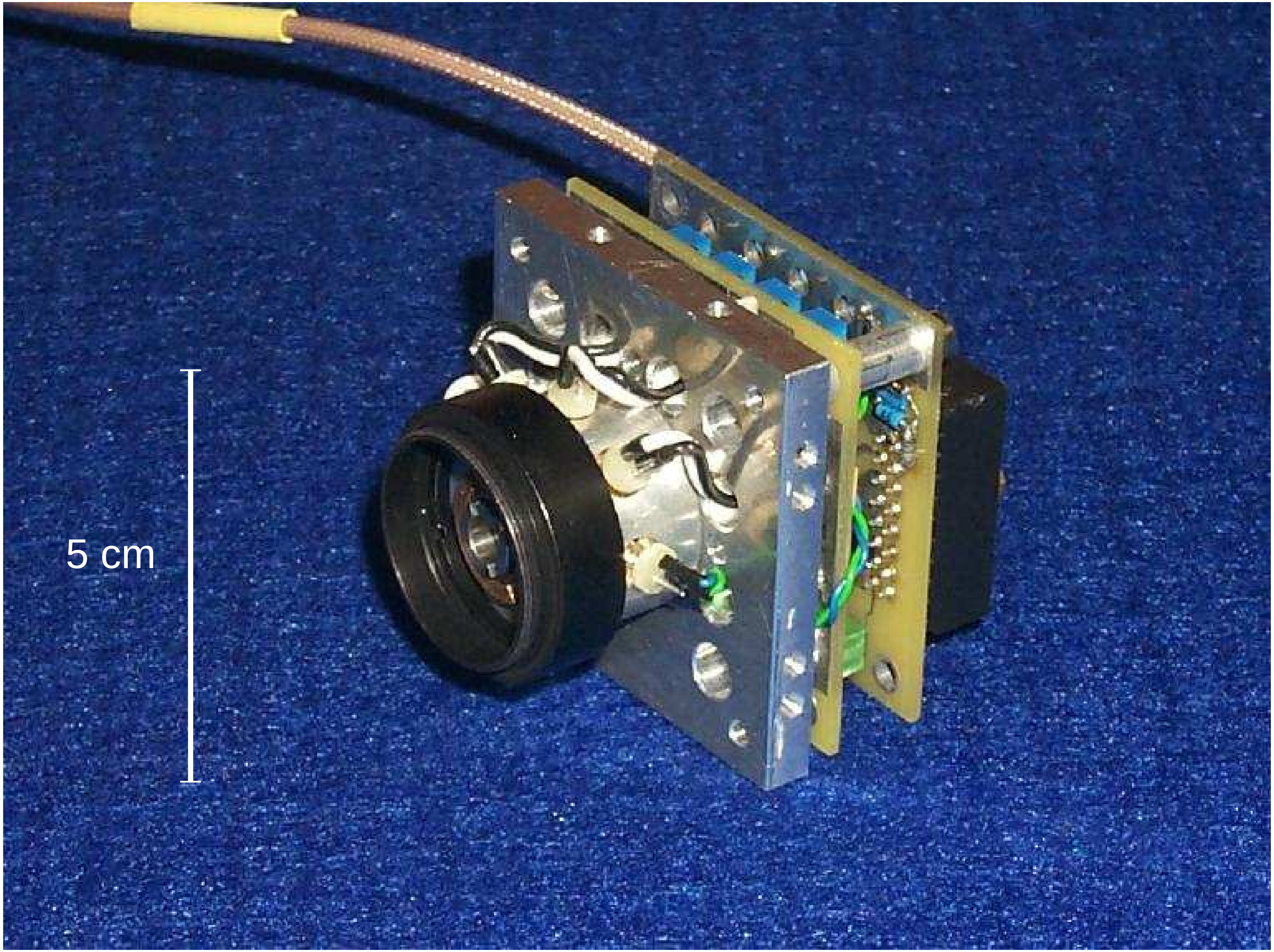
laser diodes : intrinsic
polarization better 1:1000





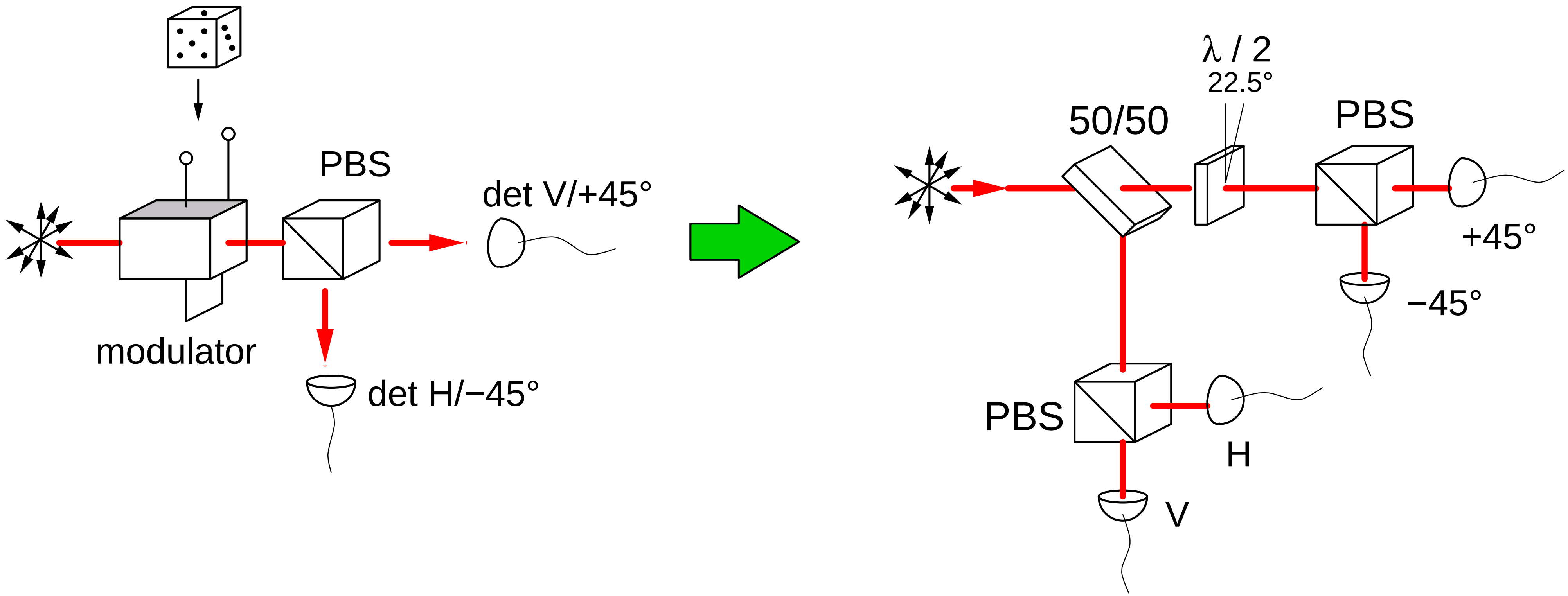


Transmitter module



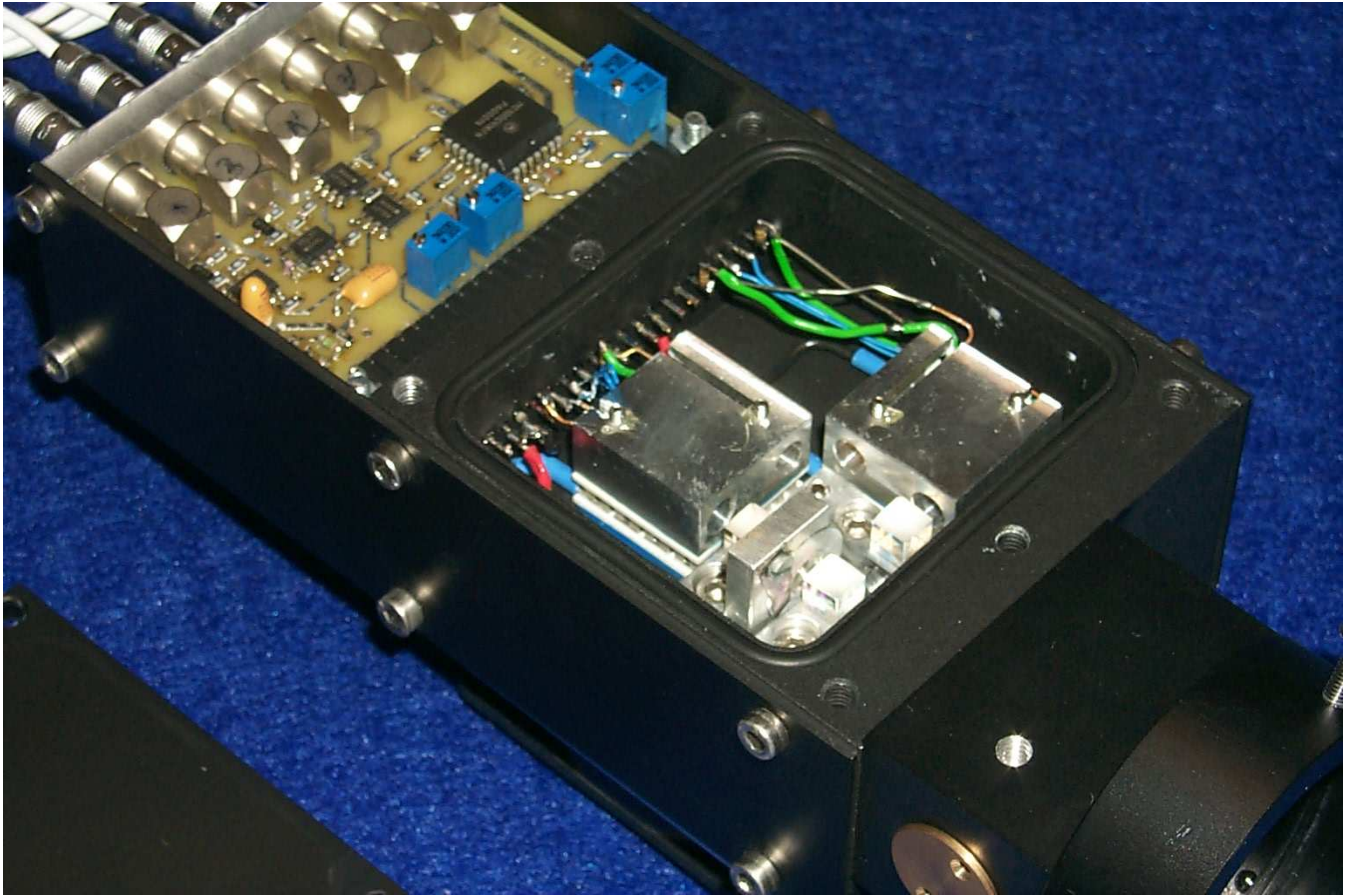
Receiver simplification

- 50/50 beam splitter instead of polarization modulators

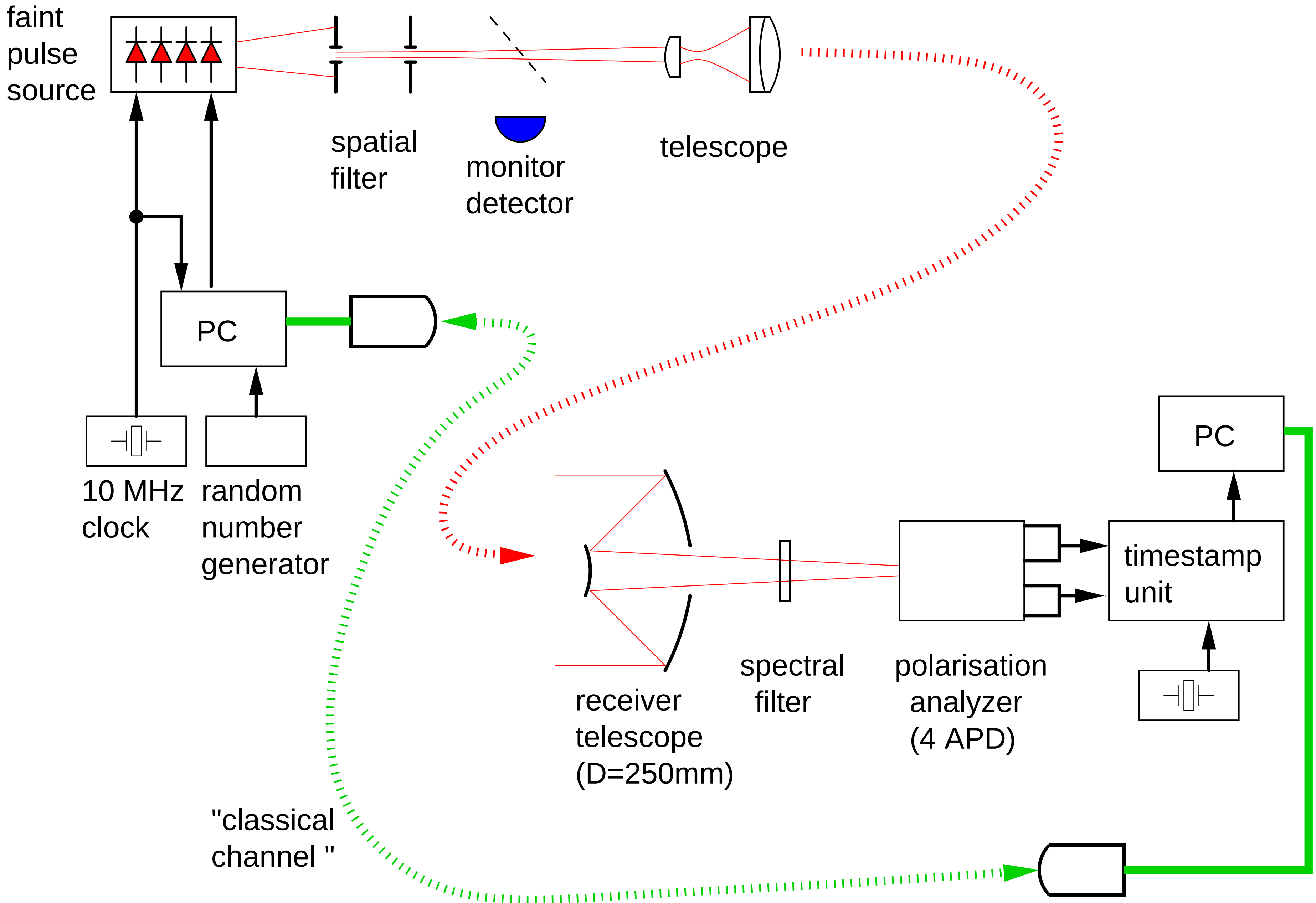


J.G. Rarity, P.C.M. Owens, P.R. Tapster,
J. Mod. Optics **41,** 2345 (1994)

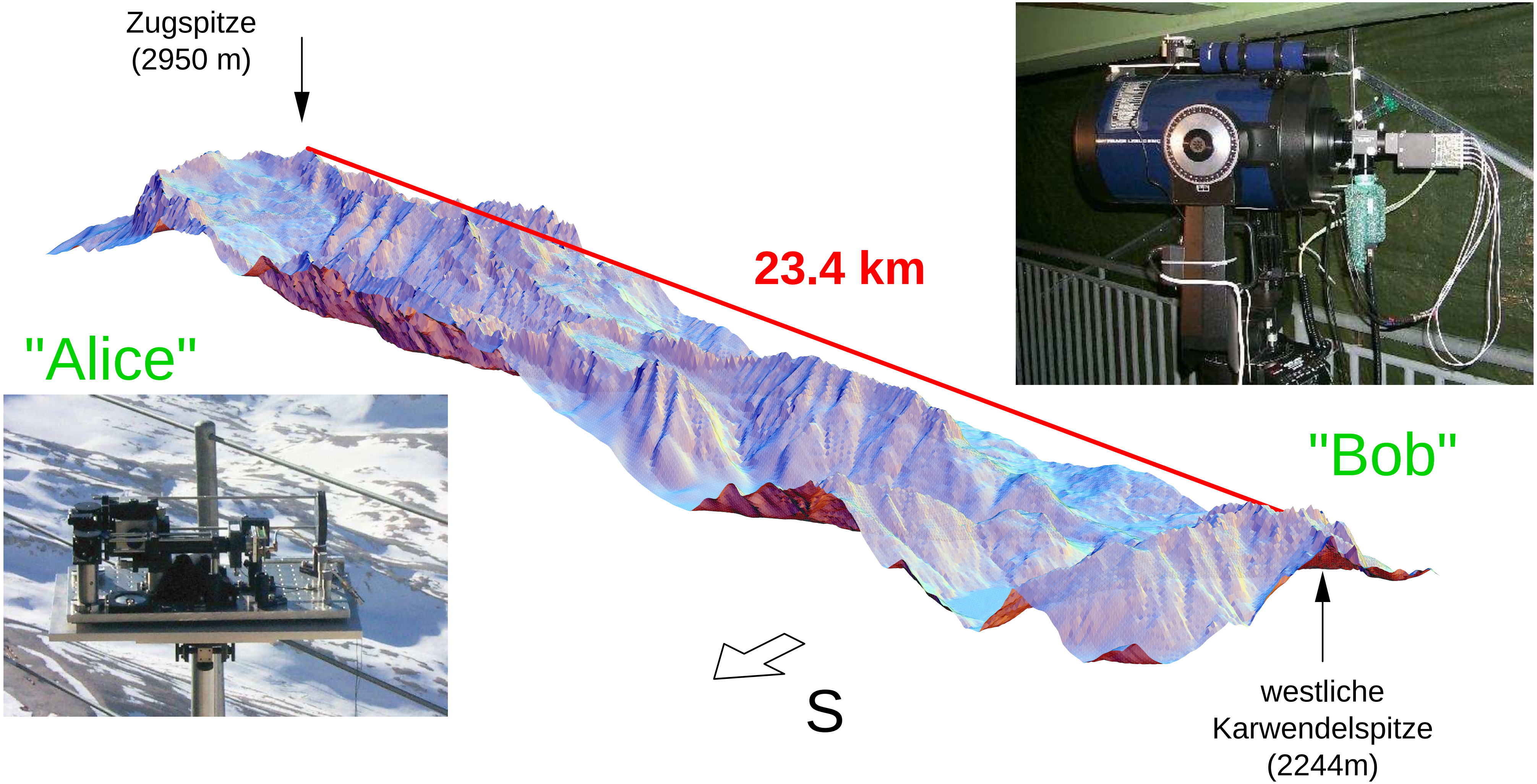
Receiver Module



System Setup

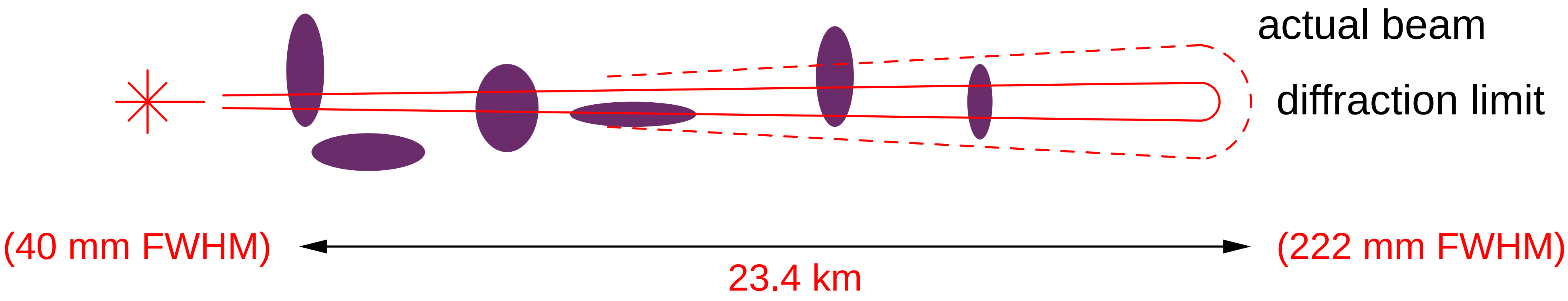


The Trial Site



Why on a mountain top?

- optical path far above ground -- lower turbulence of air

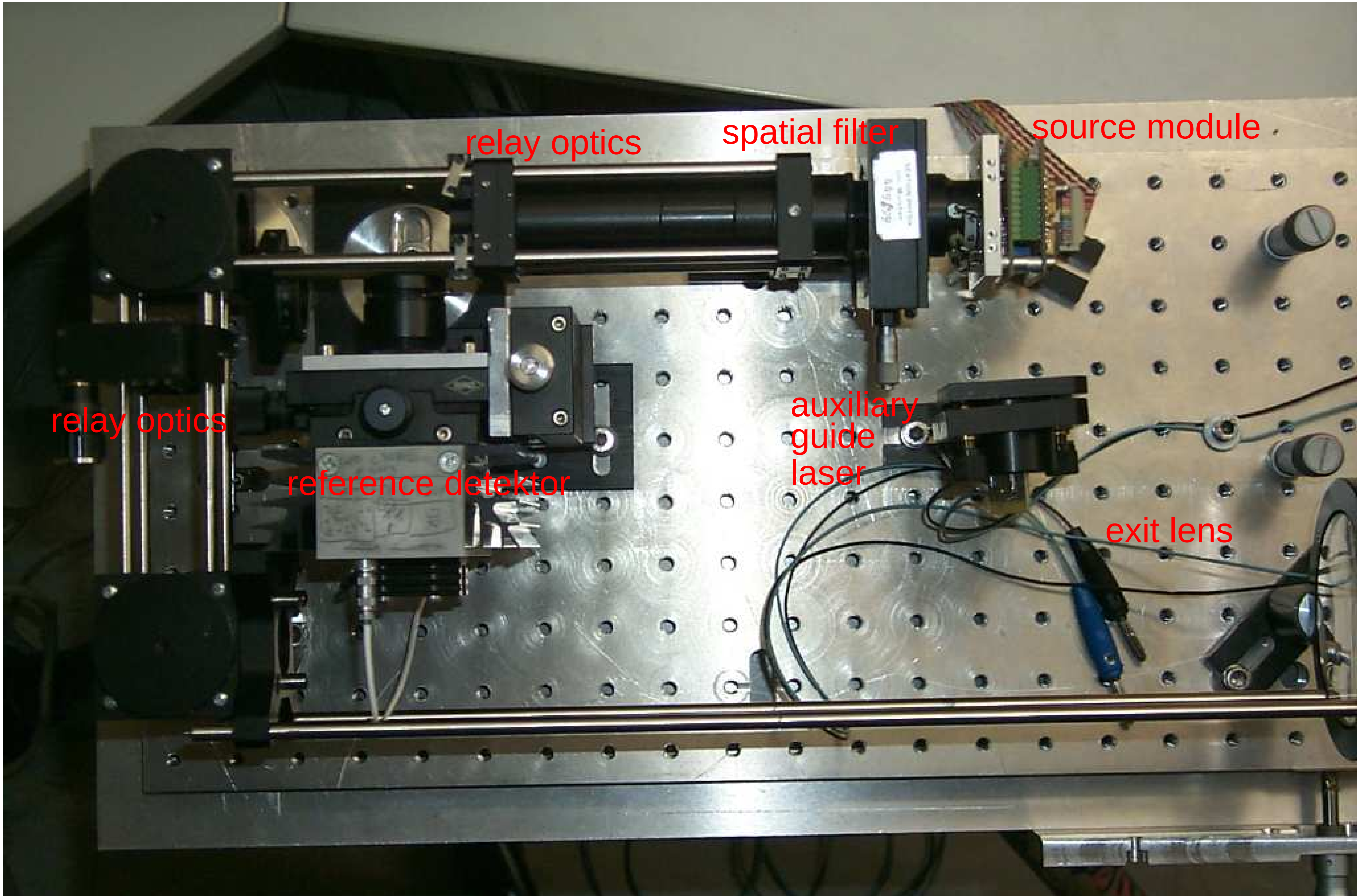


- low absorption (sometimes...)

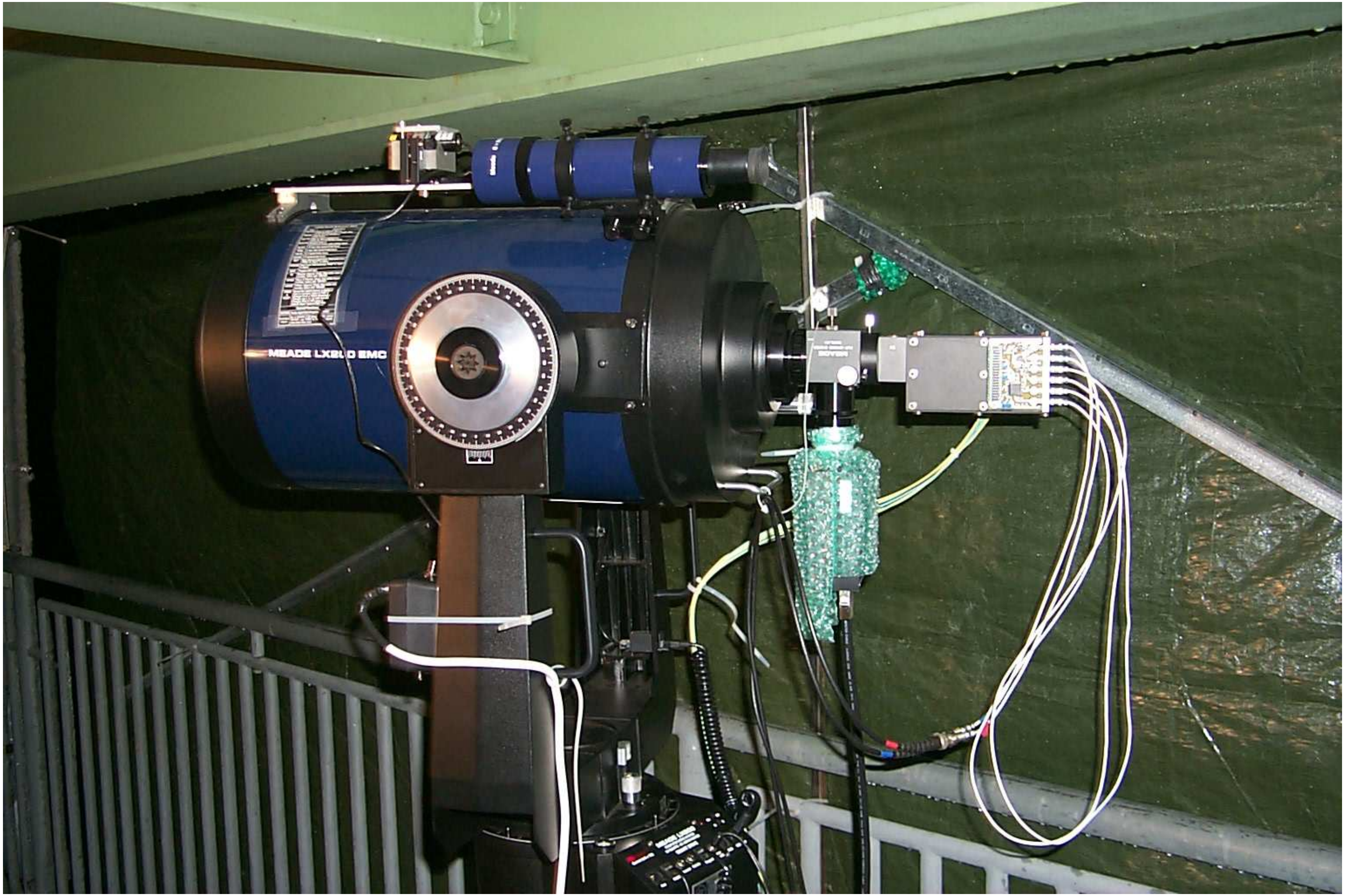
- low background light

Transmitter

Transmitter Unit 2

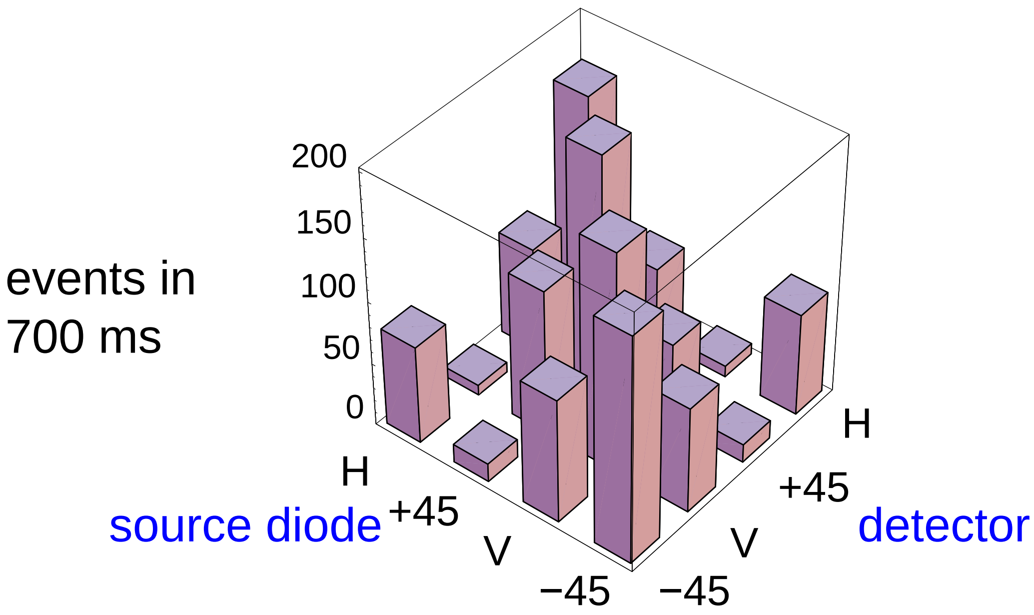


Receiver telescope & polarisation analyzer



Experimental Results

- polarisation transfer from Alice to Bob:



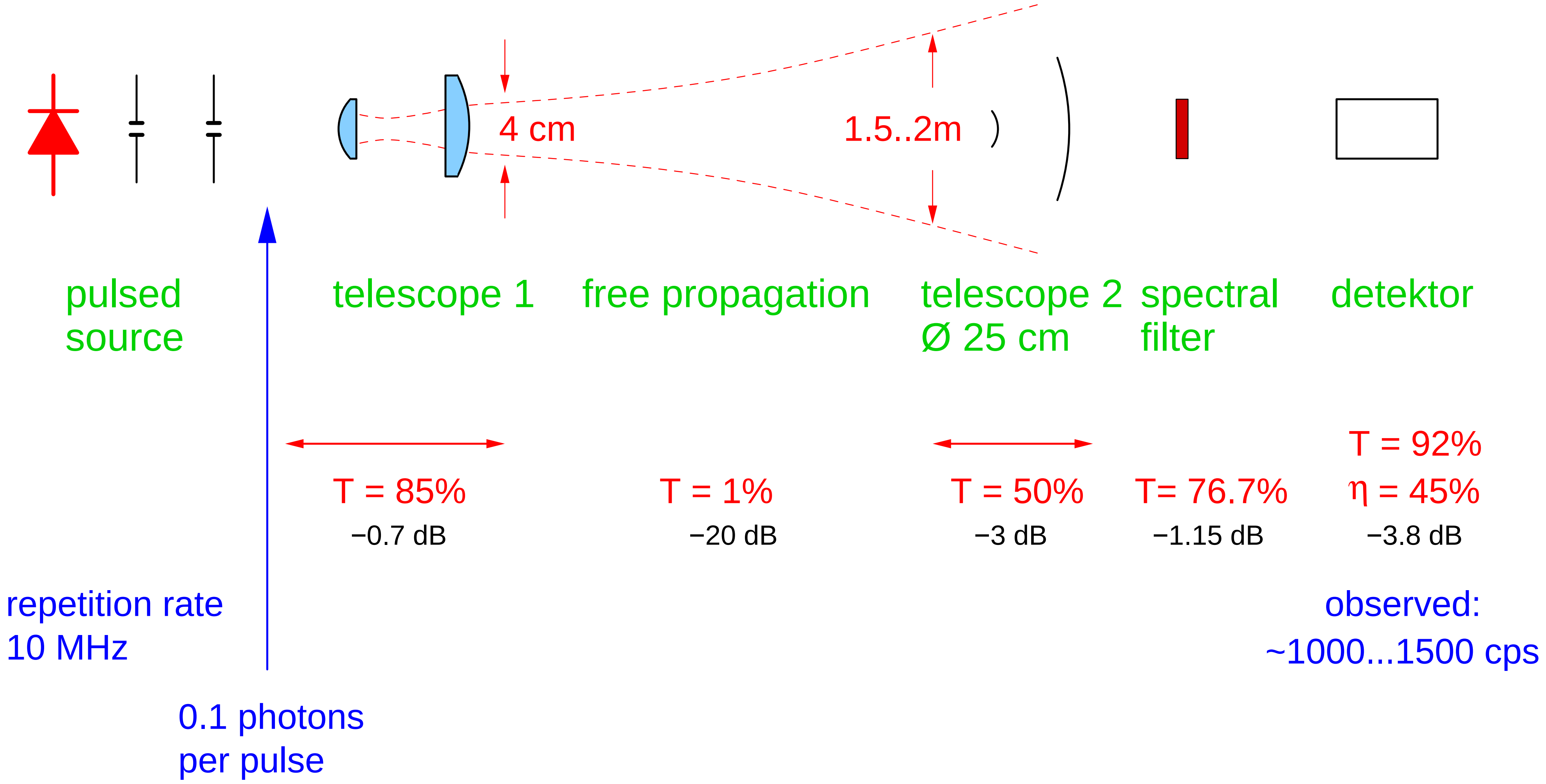
23.4 km through air

detection time window

τ = 1.4 ns

run	<n>	background	raw key rate (same base)	QBER	(from background)
#1	0.18	5578 s^{-1}	1490 s^{-1}	4.54 %	(2.6%)
#2	0.096	4510 s^{-1}	1365 s^{-1}	5.05 %	(2.3%)
#3	0.081	4360 s^{-1}	1162 s^{-1}	5.38 %	(2.6%)

Loss budget


4 cm
1.5..2m
pulsed
source
telescope 1
free propagation
telescope 2
Ø 25 cm
spectral
filter
detektor
T = 92%
T = 85%
−0.7 dB
T = 1%
−20 dB
T = 50%
−3 dB
T= 76.7%
−1.15 dB
η = 45%
−3.8 dB
repetition rate
10 MHz
observed:
~1000...1500 cps
0.1 photons
per pulse

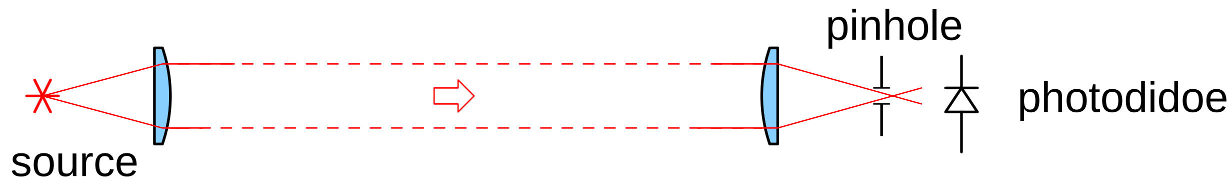
Current Technological Limits

- photodetectors
  - timing jitter: ~500 ps
  - dark count rate: ~50–50k s^{-1}
  - repetition rate: ~10^6 s^{-1}
- transmission of thr optical channel: 30–40 dB
- random number source: 20 – 100 Mbit/s

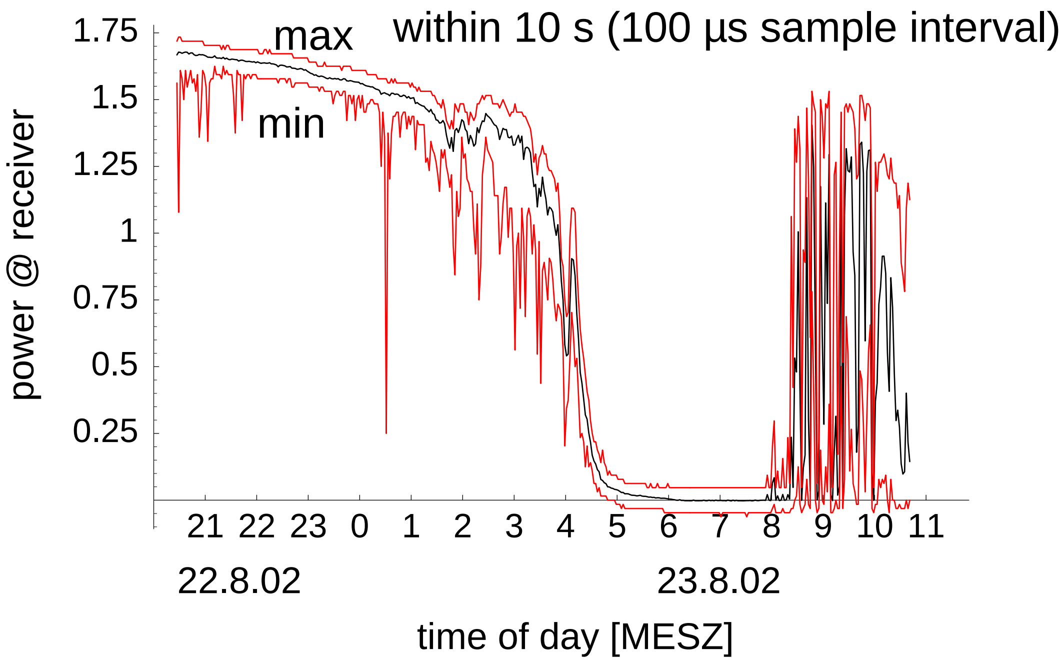
Urban Area Link

Transmission Fluctuations in an Urban Link

- Theresienstraße/Amalienstraße (ca. 500 m)

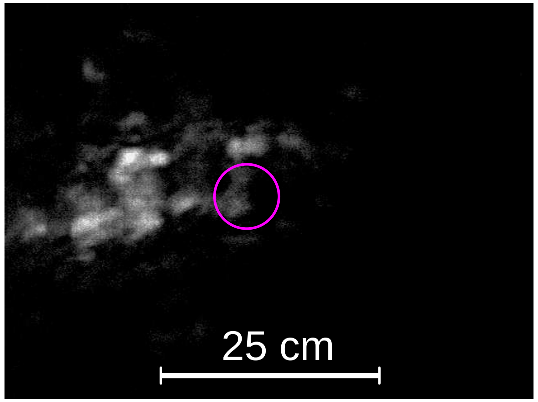


- power fluctuations

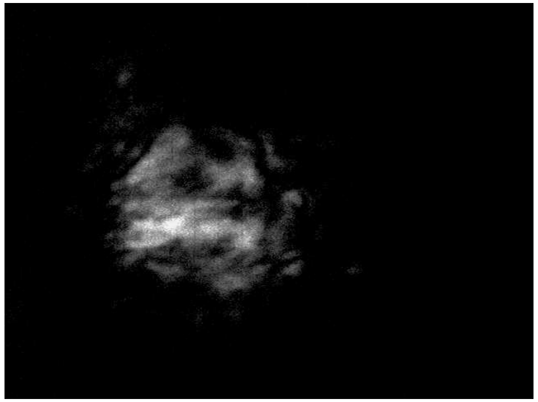


Effects of turbulence

- intensity distribution vs. time

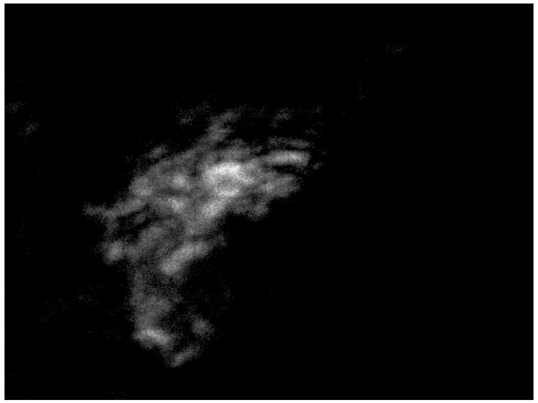


0 ms



100 ms

200 ms

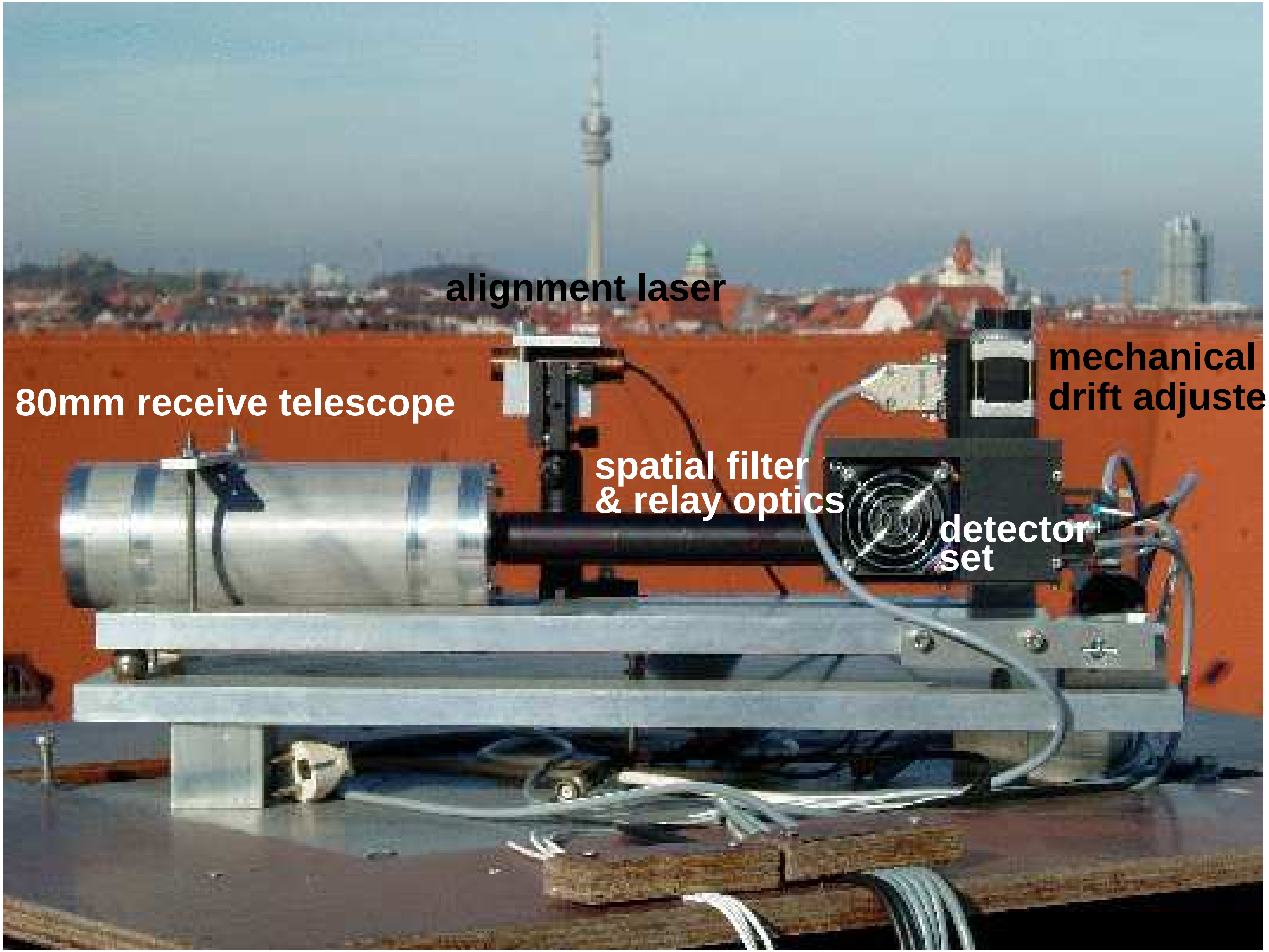


300 ms

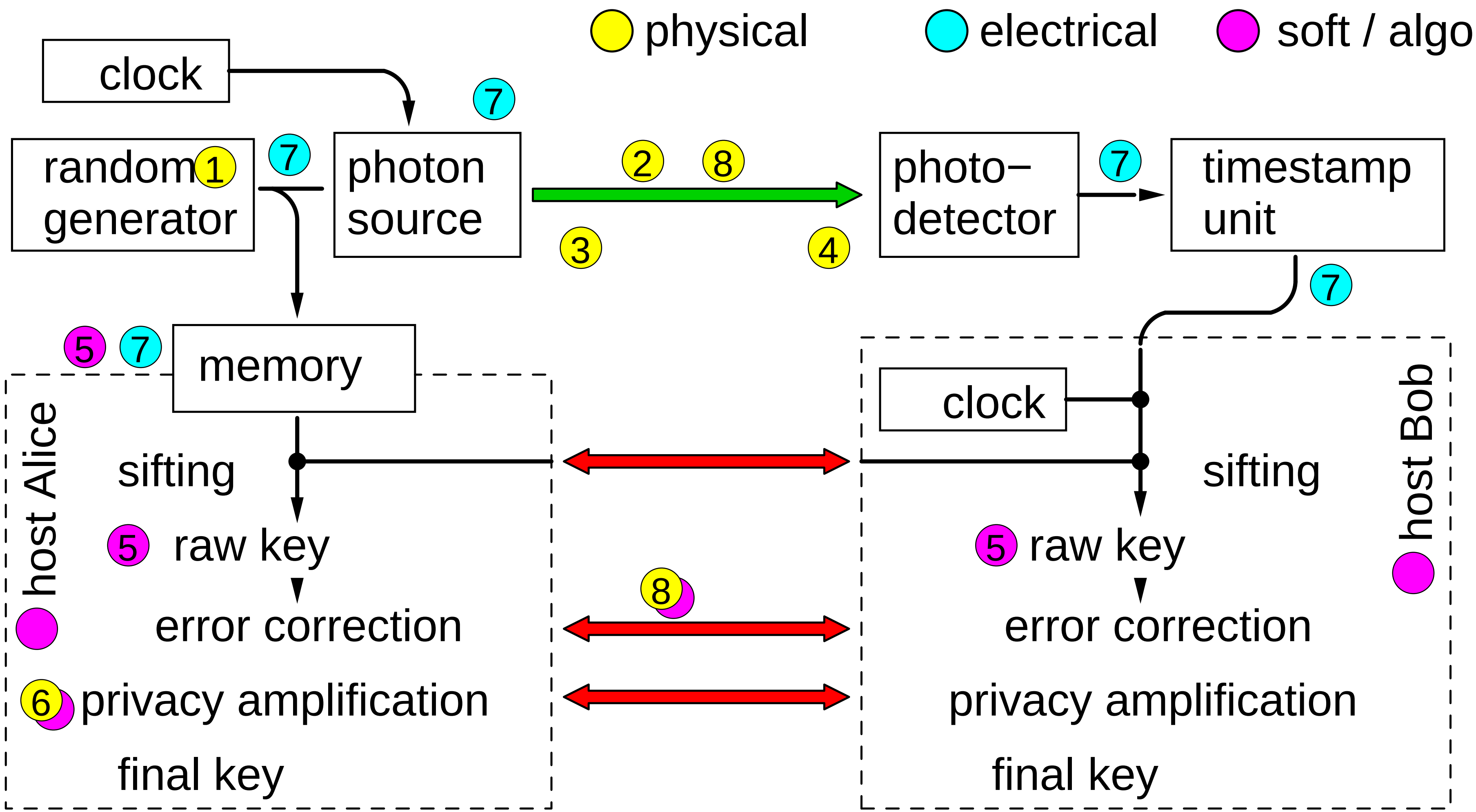
400 ms

(d ~ 9 km
downtown Munich
10–20m over ground)

Urban Receiver Setup



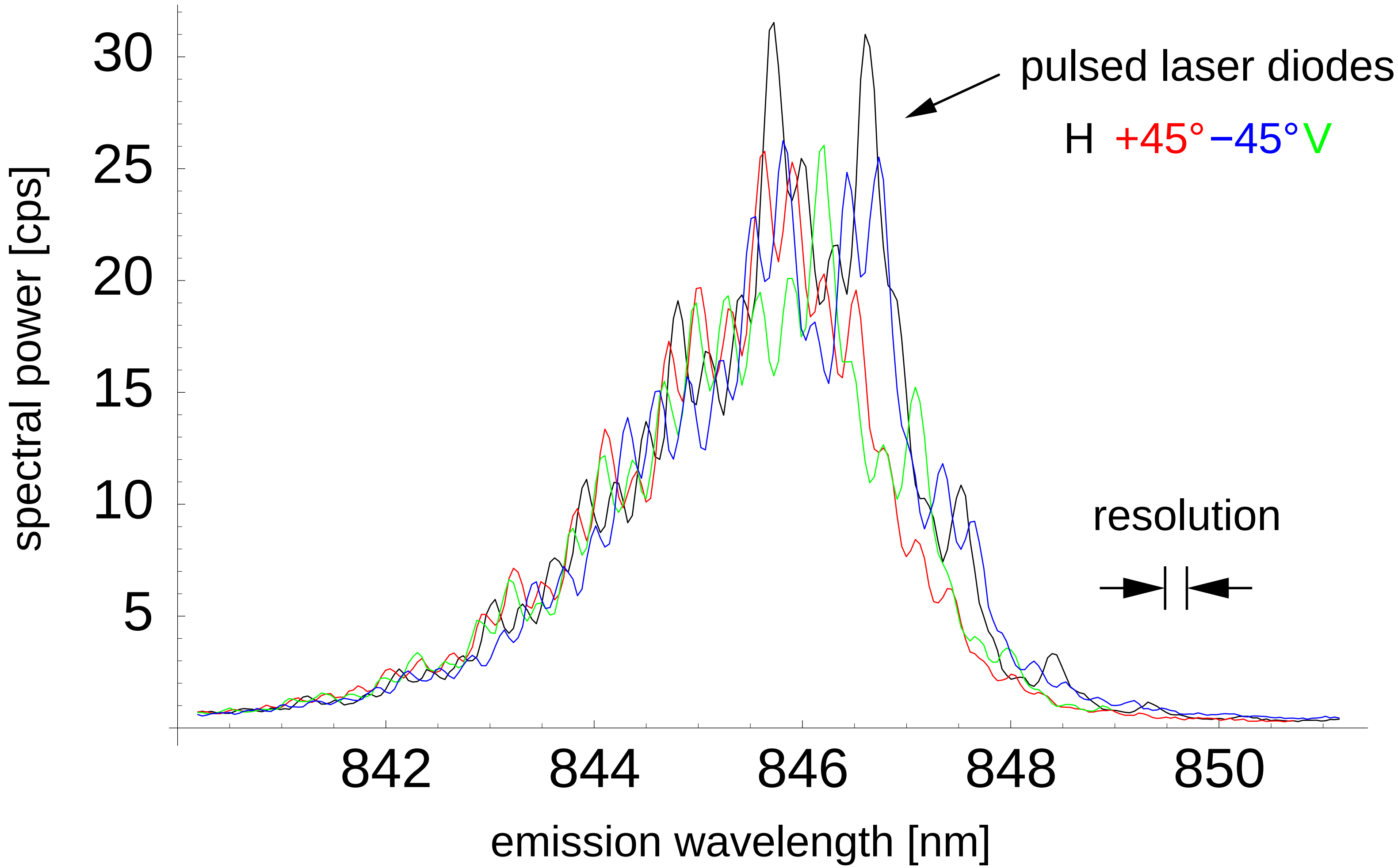
Practical attack schemes



1: bad random numbers / backdoor
2: no single photons
3: side channels
4: optical intercept of detectors

5: vagabonding raw key
6: too optimistic assumptions on eavesdroppers' knowledge
7: electrical eavesdropping
8: DoS

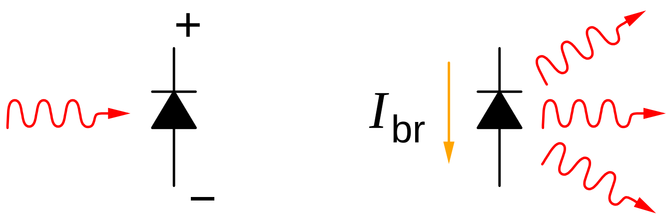
Spectral Indistinguishability of Laser Diodes



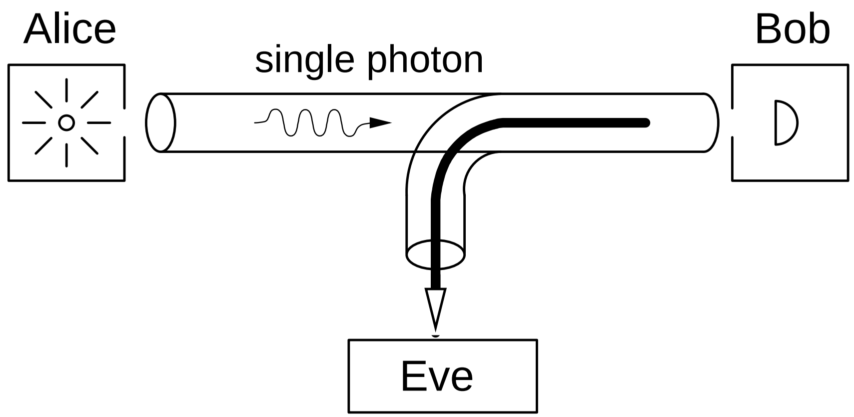
free running laser diodes indistinguishable through their wavelength

APD breakdown flash − an eavesdropping backdoor?

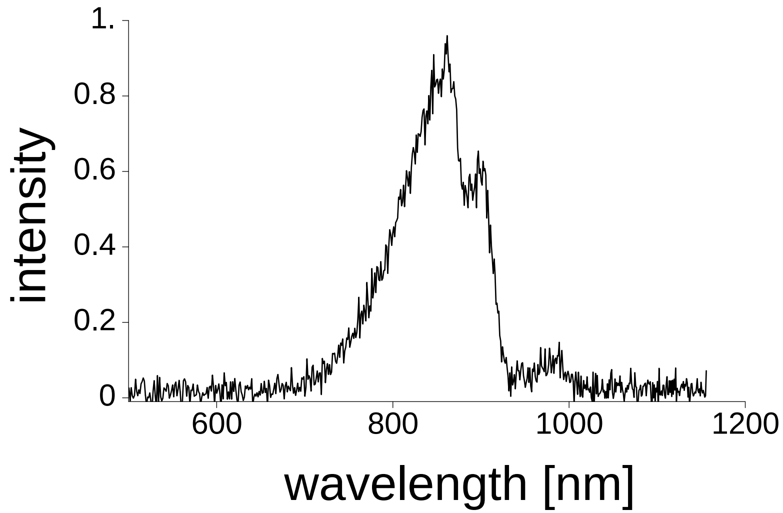
- when an APD undergoes an avalanche, light is emitted:



- possible eavesdropping attack:



- spectral distribution of breakdown light of Si APD



- measured emission:
  ~40 photons /sr for Si APD in usual operation mode

- no problem with spectral & spatial filtering

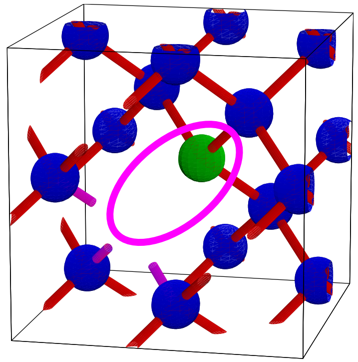
A typical DoS attack....

Overview

- a free space implementation of BB84
- a relatively simple single photon source
- tools for implementing the Ekert protocol

Fluorescence from color centers in solids

- NV centers in diamond



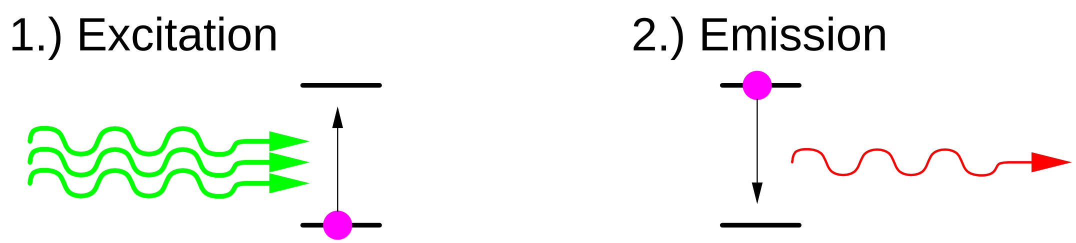
...similar to atoms

...are stable

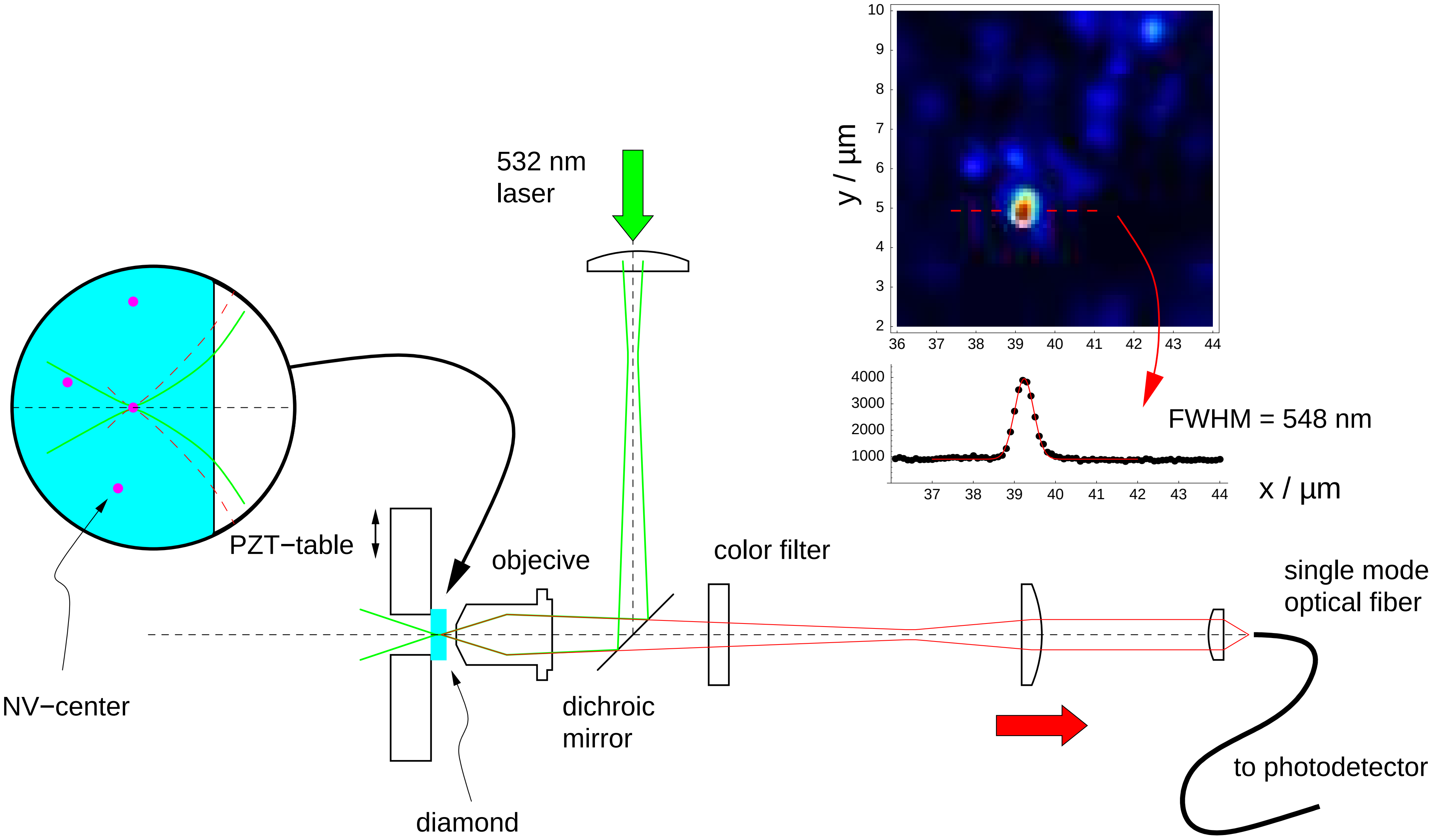
...exhibit radiative decay probability ~1

A. Grubner et al., Science **276**, 2012 (1997)

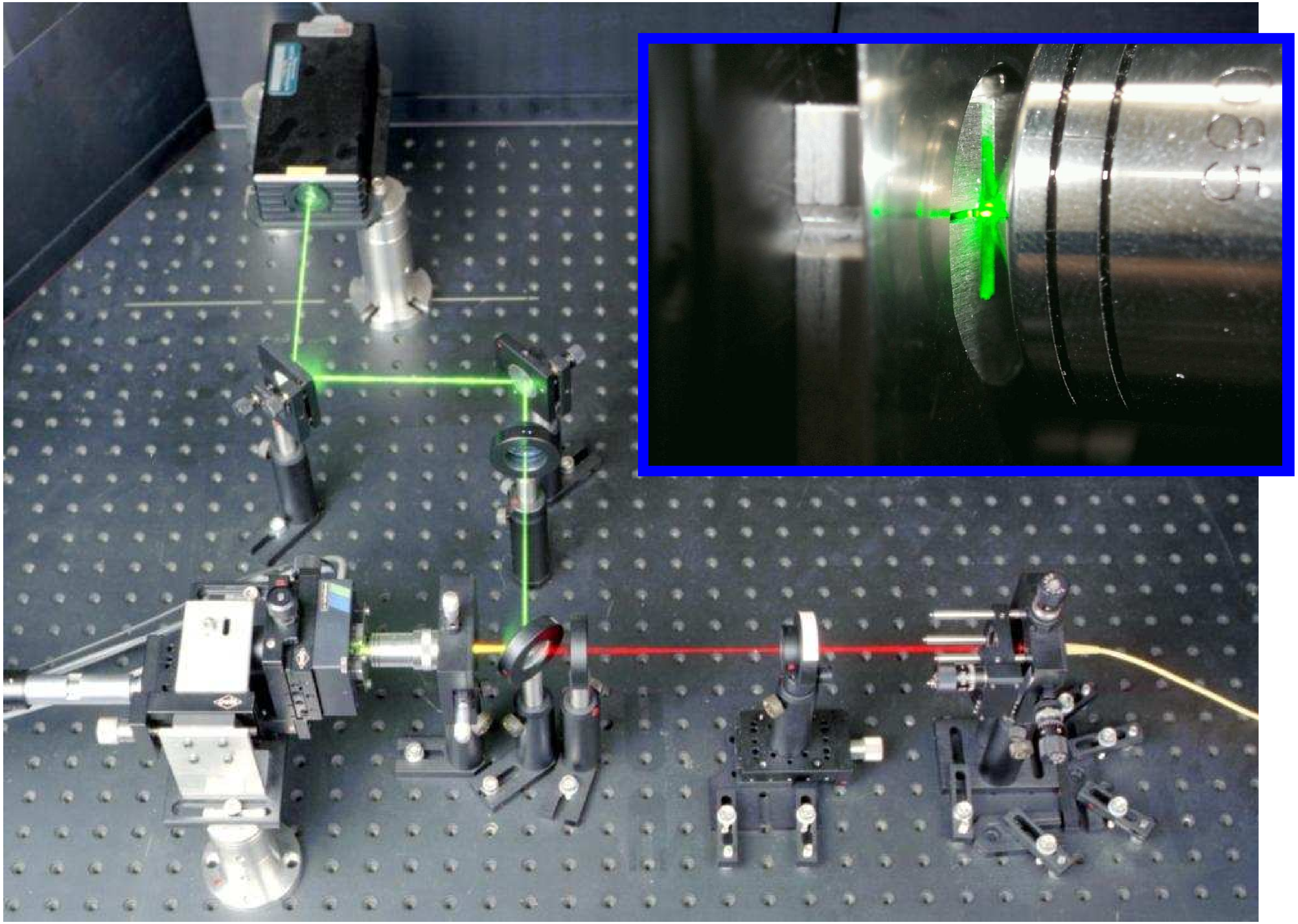
- Use these centers to create single photons:



Confocal Microscope

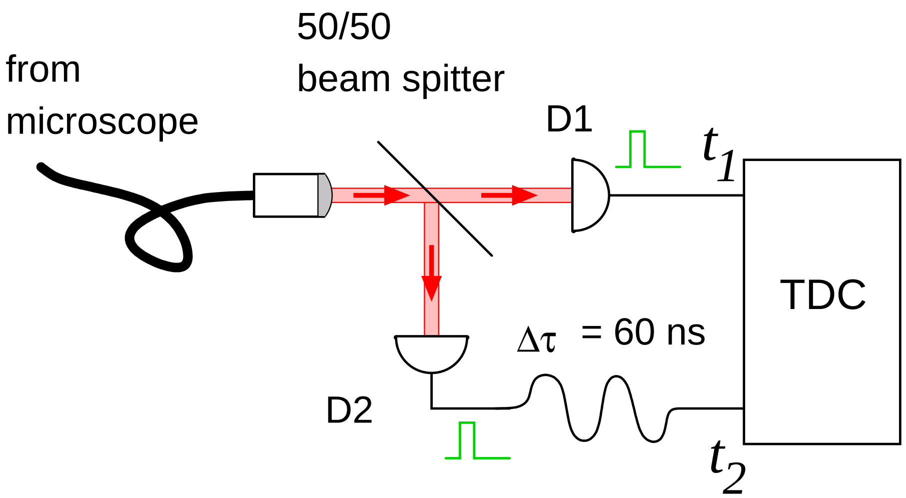


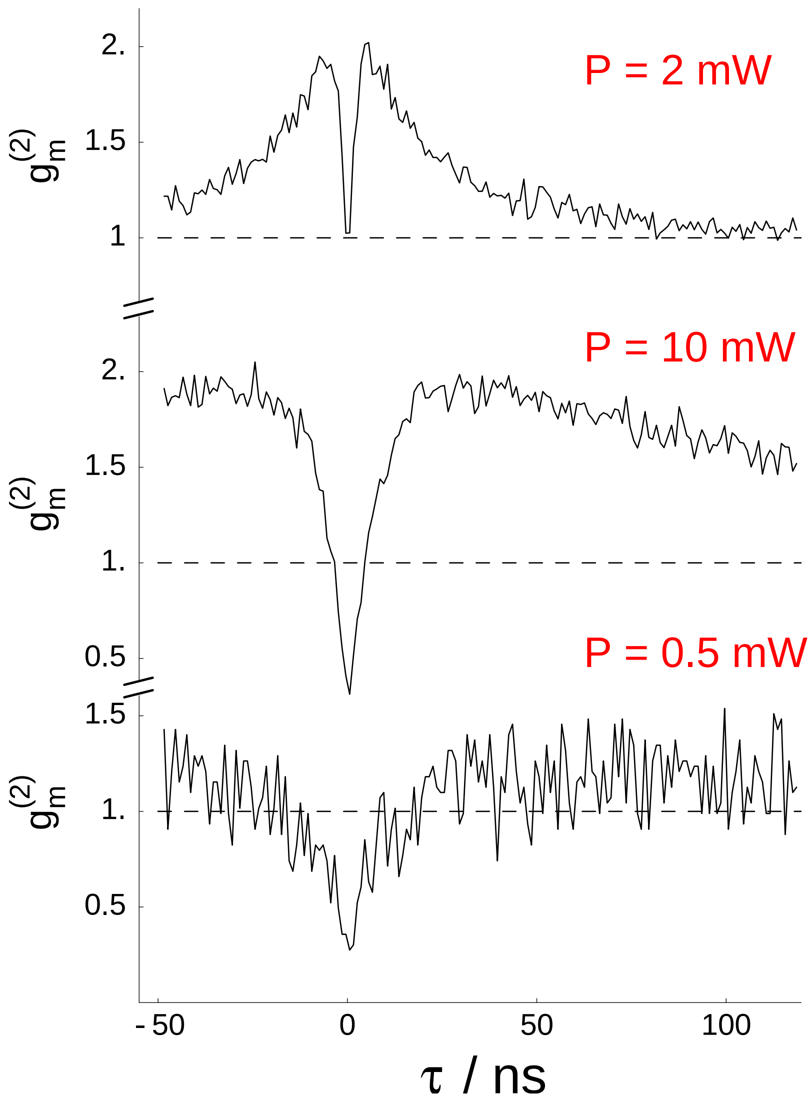
Experimental Setup



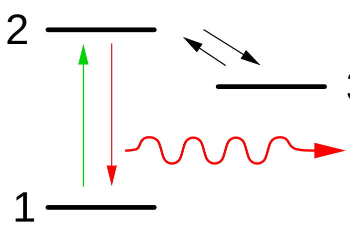
Intensity correlation function

- Observation of the photon statistics





- model:

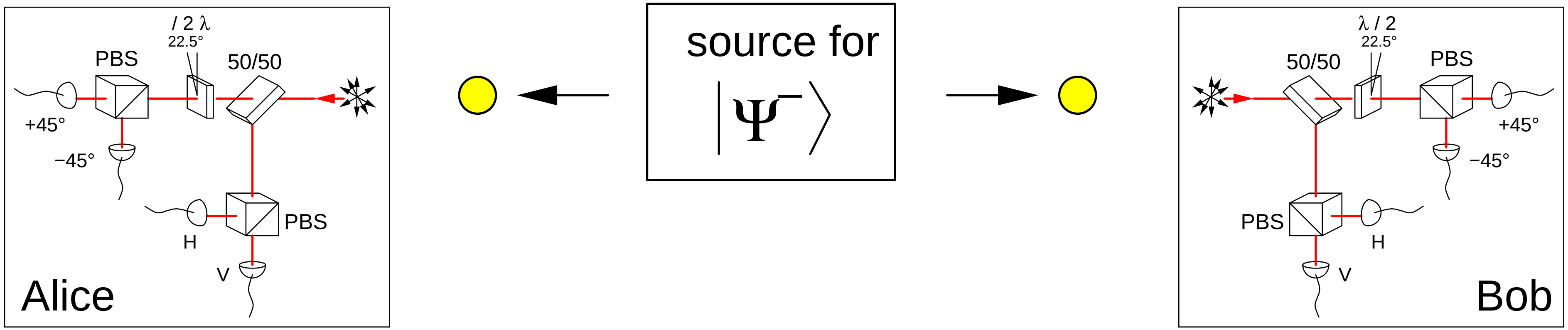


$$g^{(2)}(\tau) = 1 + c_2\, e^{-\tau/\tau_2} + c_3\, e^{-\tau/\tau_3}$$

Overview

- a free space implementation of BB84
- a relatively simple single photon source
- tools for implementing the Ekert protocol

EPR / Ekert Protocoll



- for every detection:

Alice:

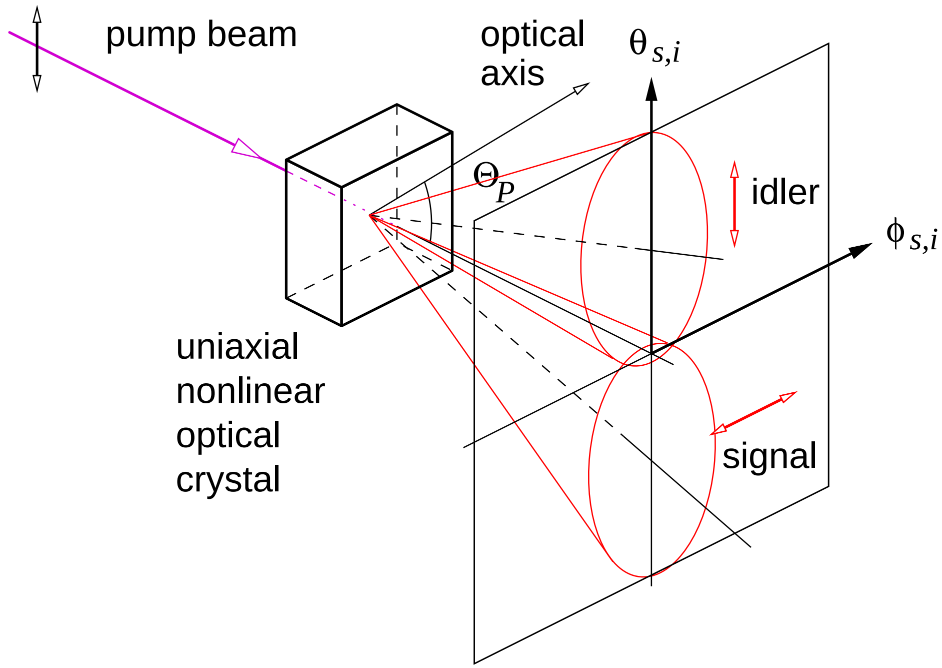
Polar.	b1	w
V	0	0
H	0	1
−45°	1	0
+45°	1	1

Bob:

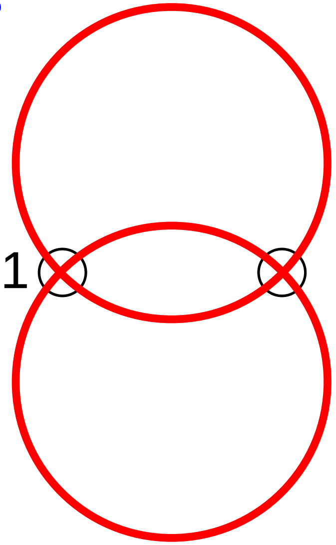
Polar.	b2	e
V	0	1
H	0	0
−45°	1	1
+45°	1	0

- continue like in BB84
- additional eavesdropping tests (check Bell inequalities)
- no external random number source!

Type−II Parametric Down Conversion



- energy & momentum conservation:
  2 cones

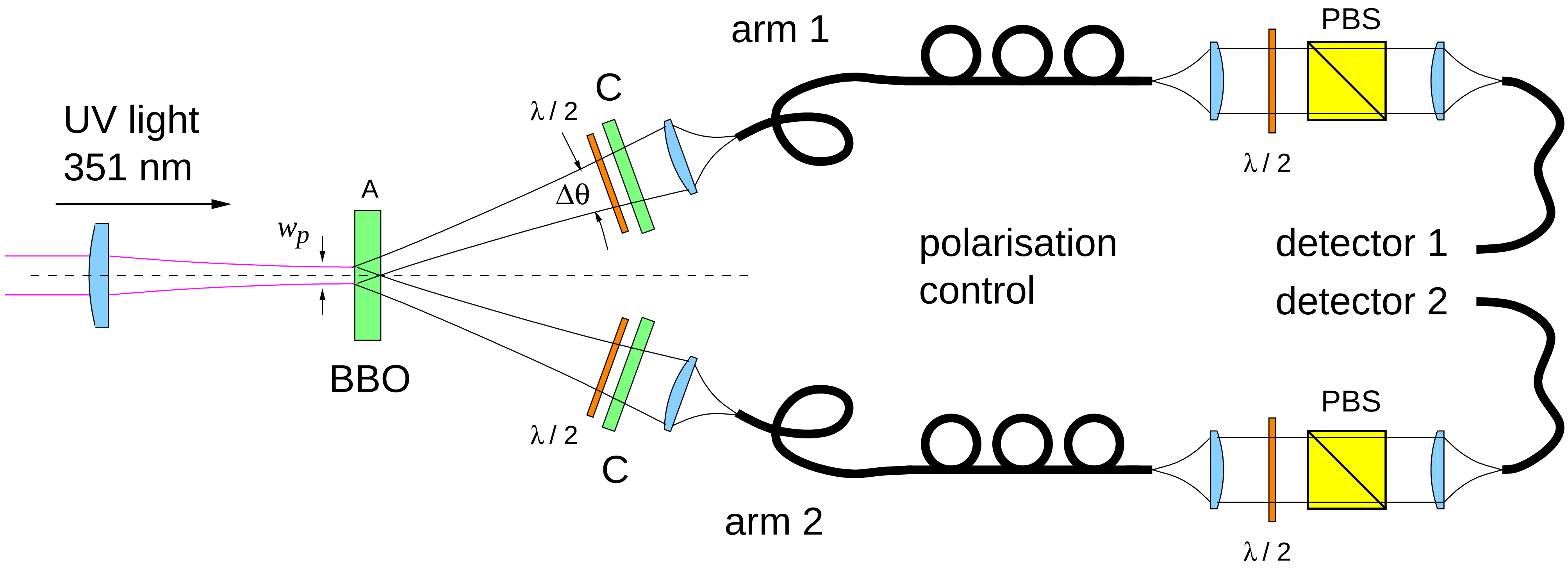


- indistinguishability of photons leads to a
  polarisation−entangled photon pairs along directions 1 & 2

P. Kwiat et al., Phys. Rev. Lett. **75** , 4337 (1995).

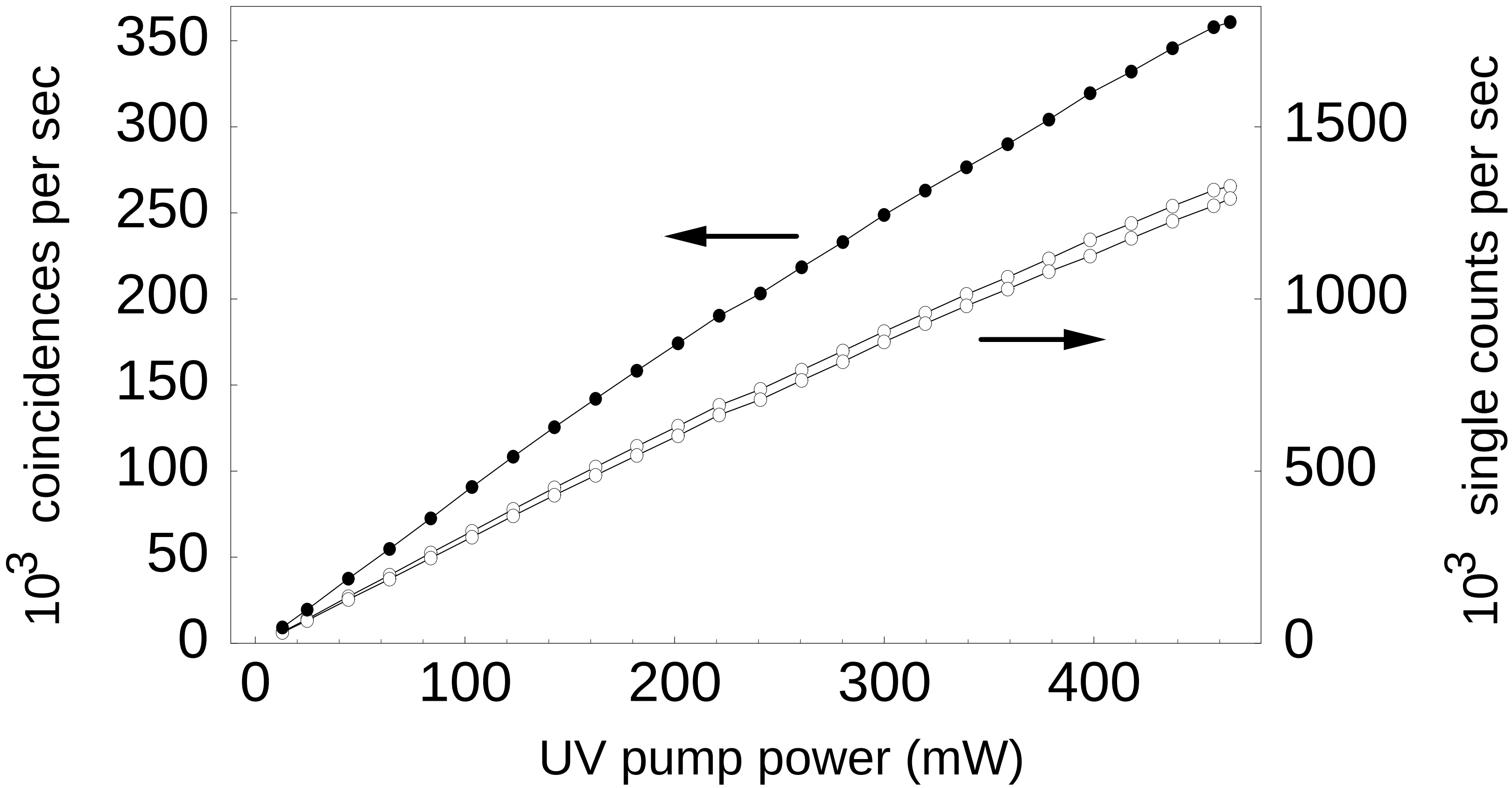
$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|HV\rangle + e^{i\zeta} |VH\rangle \right)$$

Experimental Setup I



- targeted bandwidth: 4 nm FWHM
- acceptance angle: 0.22 deg FWHM
- conversion diameter in the crystal: w = 82 µm FWHM
- no interference filter

Count Rates vs. Pump Power

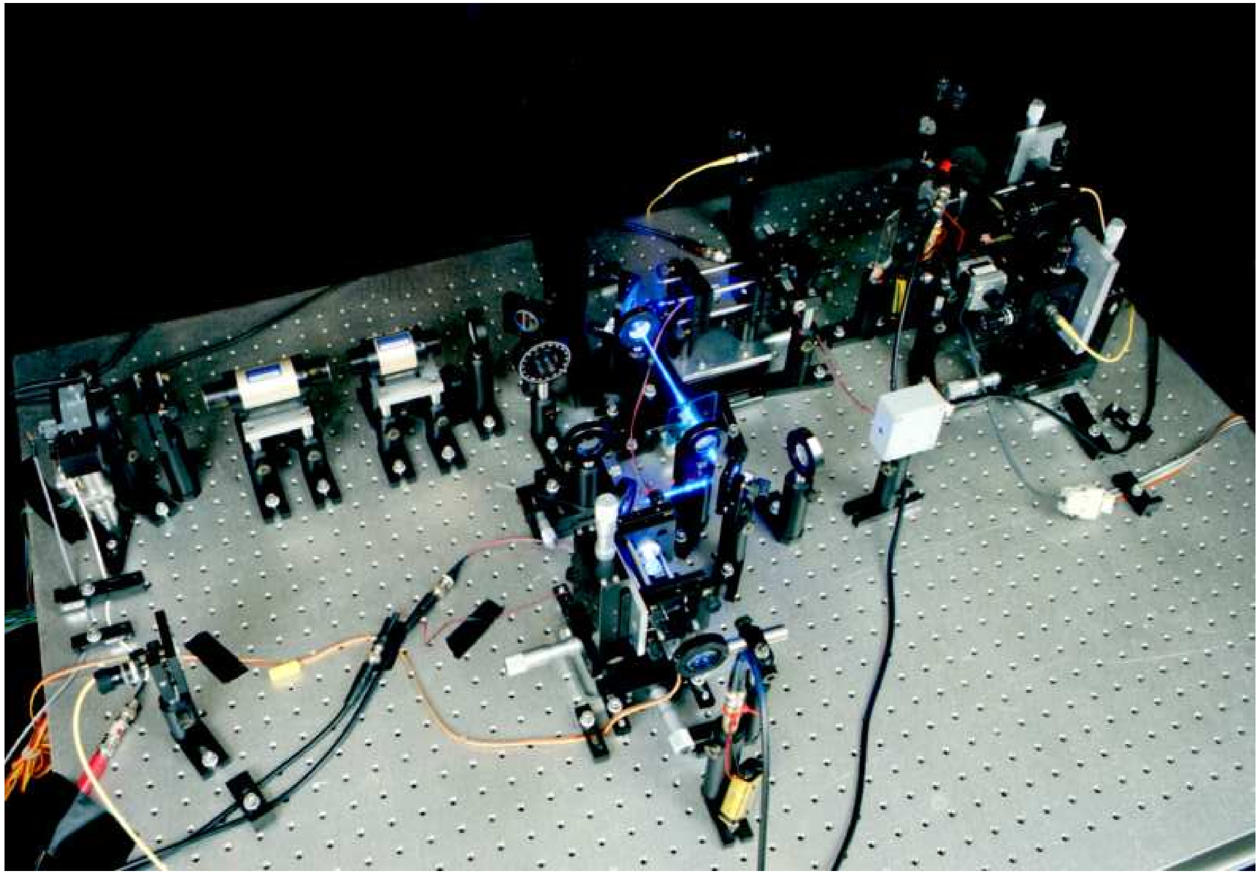


- Identifying correlated photon pairs (τ_C = 6.8 ns)

  coincidence count rate: **360 800 cps** from a 2 mm thick BBO crystal

  coincidence /single ratio: **28.6 %** (Si APD, actively quenchend)

Diode Laser Based Photon Pair Source



- coincidence rate:
  10 000 cps

- high entanglement:

  S = 2.63±0.0074 (85 σ)

  in 5 sec integration time per point

J. Volz, Ch. Kurtsiefer, H. Weinfurter
Appl. Phys. Lett. 79, 869 (2001)

Experimental Activities in Singapore.....

- understand / compensate atmospheric transmission fluctuations
- establish a free−space link (banks, gov orgs, cell phone base stations?)
- experimentally implement new entanglement−based QKD protocols (with D. Kaszlikowski, B.G. Englert, LC. Kwek et al.)
- improve singlet pair sources

Summary

- BB84−type quantum key distribution systems became technology
- simple single photon sources still subject of research
- Ekert protocol QKD systems / pair sources under development

Next steps

- operation under ambient light conditions
- implement new protocols
- urban area quantum key distribution
- think about satellite links?

People here & there

- Munich group

Free Space Optics
- Matthäus Halder
- Patrick Zarda
- Henning Weier
- Tobias Schmitt−Manderbach

Single Photons
- Sonja Mayer
- Chunlang Wang

Entangled pairs
- Markus Oberparleiter
- Jürgen Volz
- Christian Schmidt
- Pavel Trojek

New Protocols
- Oliver Schulz
- Ruprecht Steinhübl

Christian Kurtsiefer **Harald Weinfurter**

- collaborations

Qinetiq
- Paul R. Tapster
- Phil M. Gorman
- John G. Rarity

- Singapore group

Experimental
- Foo Pei Yih
- Darwin Gosal
- Tey Meng Khoon
- Alexander Ling
- Ivan Marcikic
- Antia Lamas−Linares
- Ch. K.

Theory
- Ajay Gopinathan
- Dagomir Kaszlikowski
- B.G. Englert
- Kwek Leong Chuan
- Artur Ekert
- Oh Choo Hiap