Aspects of Practical Quantum Key Distribution Schemes

I. Marcikic, A. Ling, D. Gosal, M. Peloso, H. Loh,
V. Scarani, A. Lamas-Linares, C. Kurtsiefer

NUS
National University
of Singapore

6th Int. Conference on Cryptology & Network Security
Singapore, 8.-10. December 2007

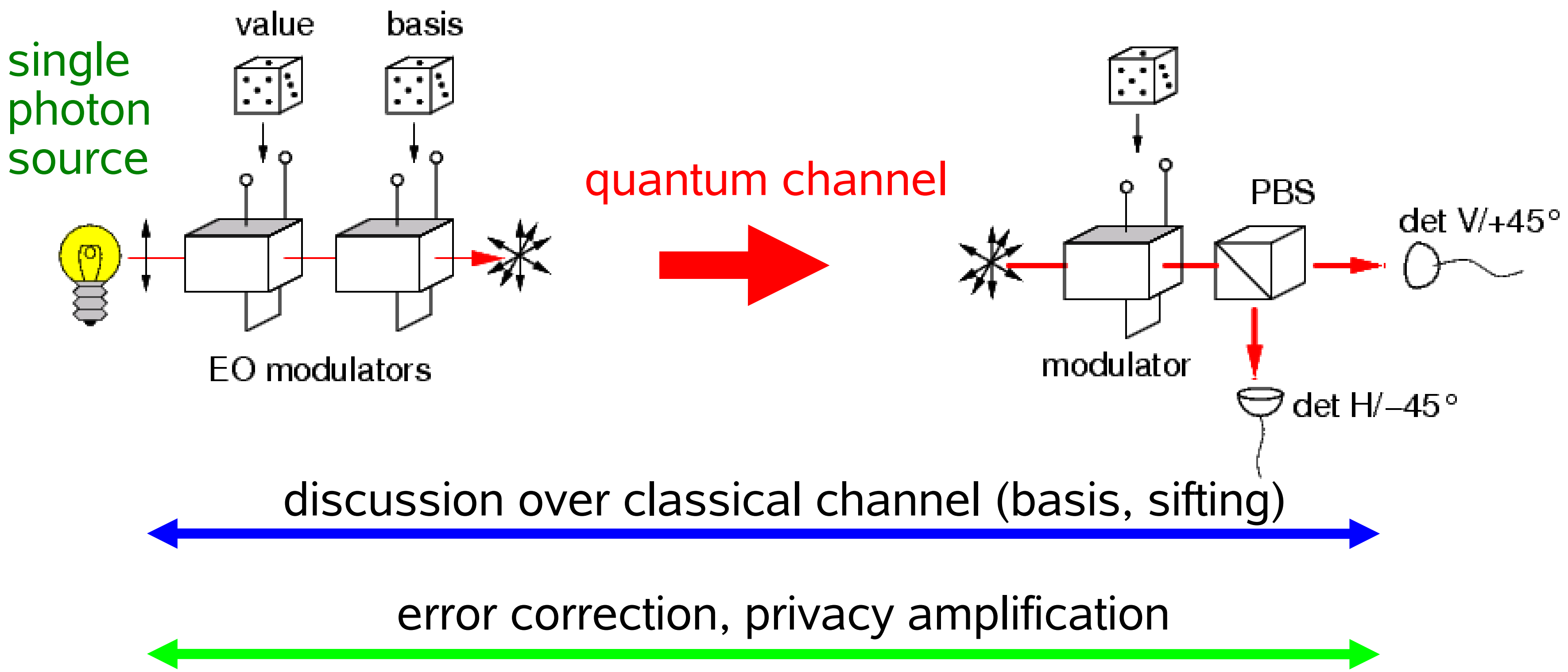
*financial support by DSTA, A*STAR and Ministry of Education*

Overview

- BB84 type prepare & send implementations of QKD
- Free space and optical fiber quantum channels
- Experimental implementation of an entanglement-based QKD scheme
- A possible attack strategy
- Free space QKD during daylight?
- A side channel-tolerant protocol: E91 revisited

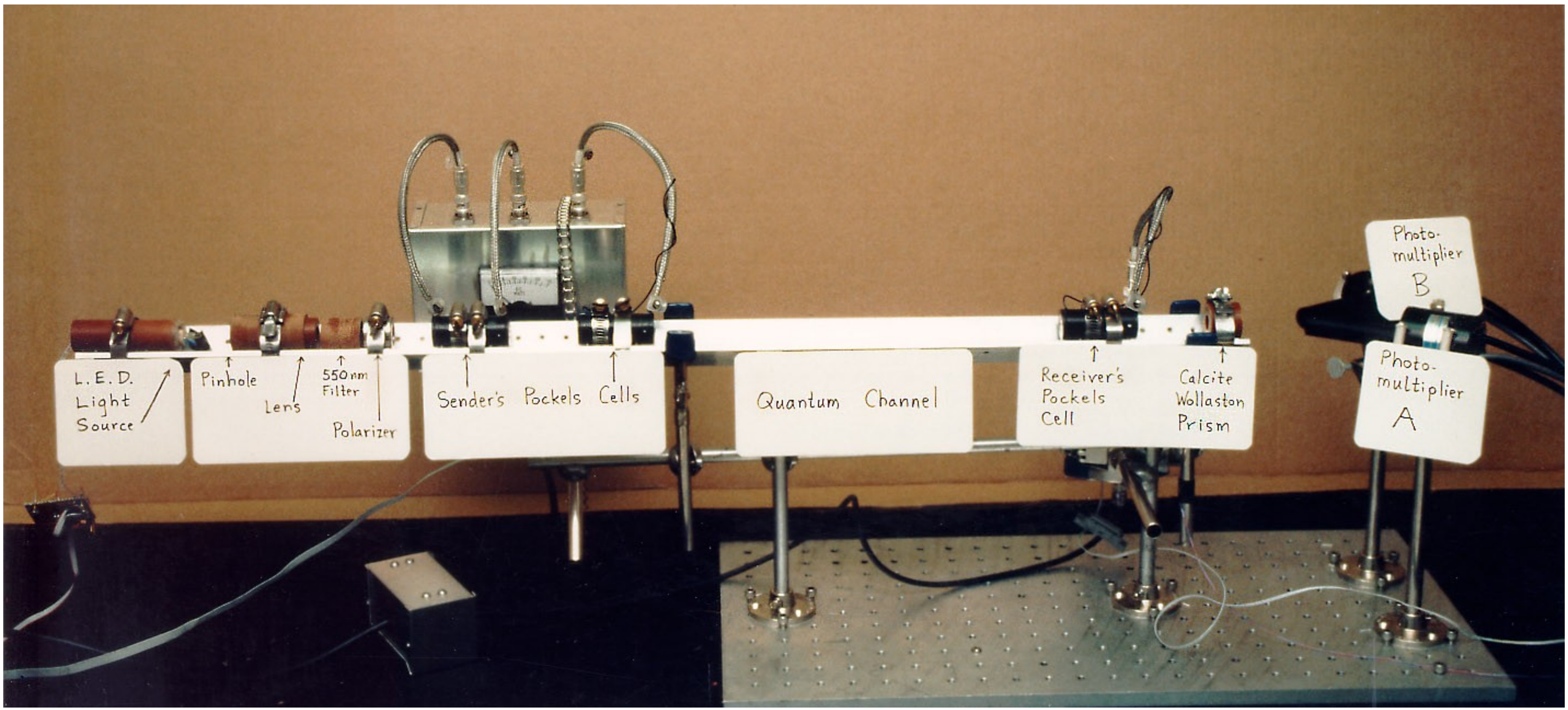
Different protocols I

Prepare & measure protocols (BB84 & friends/derivatives):



- needs lots of trusted random numbers
- knowledge of Hilbert space / good single photon source
- uses error fraction to estimate eavesdropper's knowledge

BB84 original implementation



C. Bennett, F. Bessette, G. Brassard, L. Savail, J. Smolin
*J. Cryptology **5**, 3 (1992)*

BB84 Implementation Hack #1

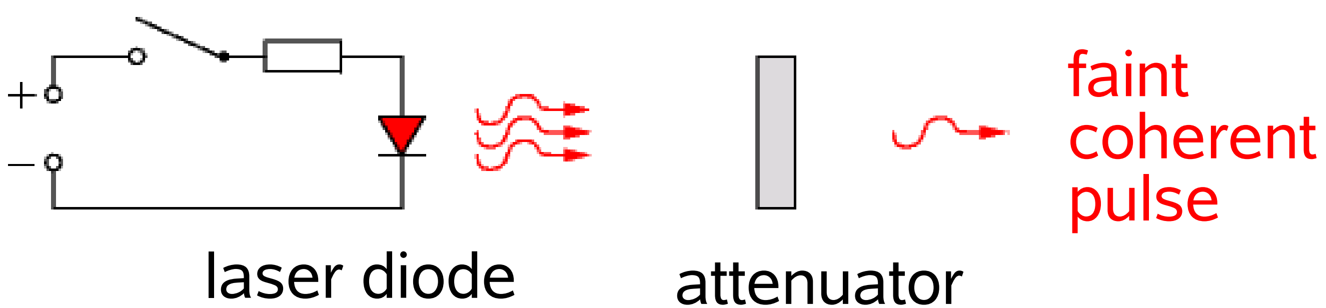
National University of Singapore

- use faint coherent pulses instead of single photons - with Poisson statistics of photon numbers

$$p(n) = \frac{\lambda^n}{n!}\ e^{-\lambda} \qquad \text{for} \qquad \langle n \rangle = 0.1$$

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

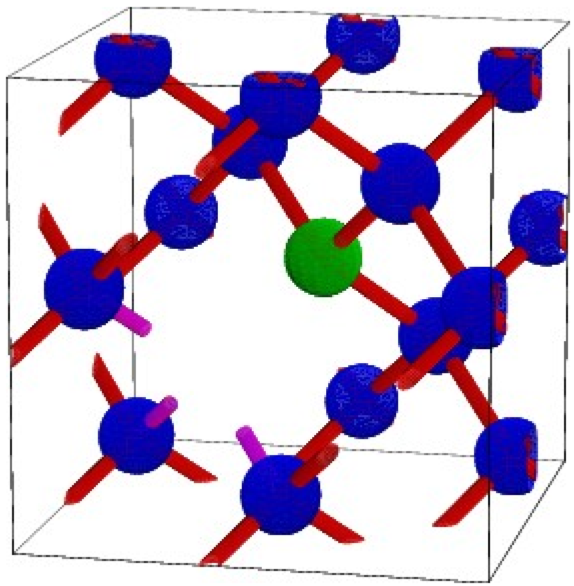
- much simpler to prepare than true single photons:



- potentially insecure: photon number splitting attack
- lower repetition rate

BB84 Hack #1 workarounds

- don't use faint coherent pulses instead of single photons



Physical single photon sources:

- NV centers in diamond

  A. Beveratos et al., Phys. Rev. Lett. ***89*** *187901 (2002)*

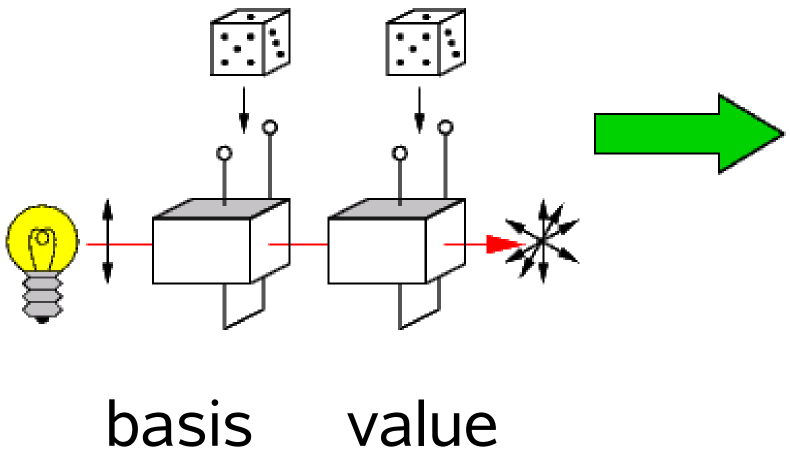
- quantum dots...
- dye molecules...

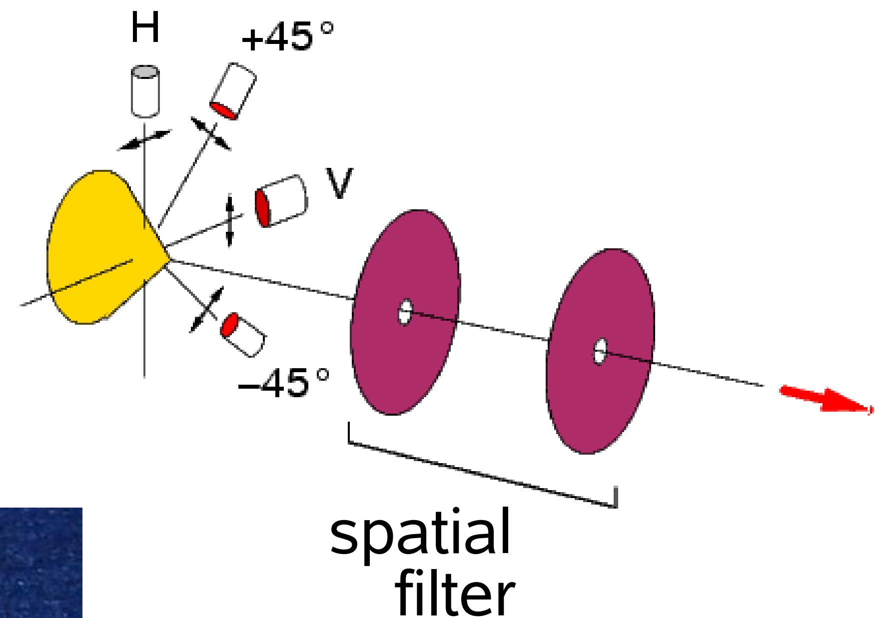
- use decoy states (faint coherent pulses with randomized <n>) to discover photon number splitting attacks

  H.-K. Lo, X. Ma, K. Chen, Phys. Rev. Lett. ***94*** *230504 (2004)*
  T. Schmitt-Manderbach et al., Phys. Rev. Lett. ***98****, 010504 (2007)*

Preparation of polarized photons

- Make use of good intrinsic polarization of laser diodes

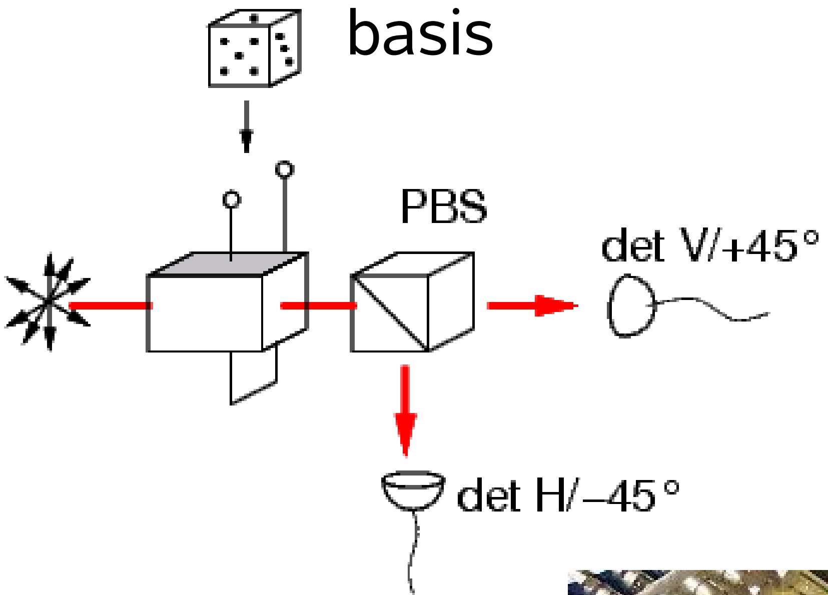


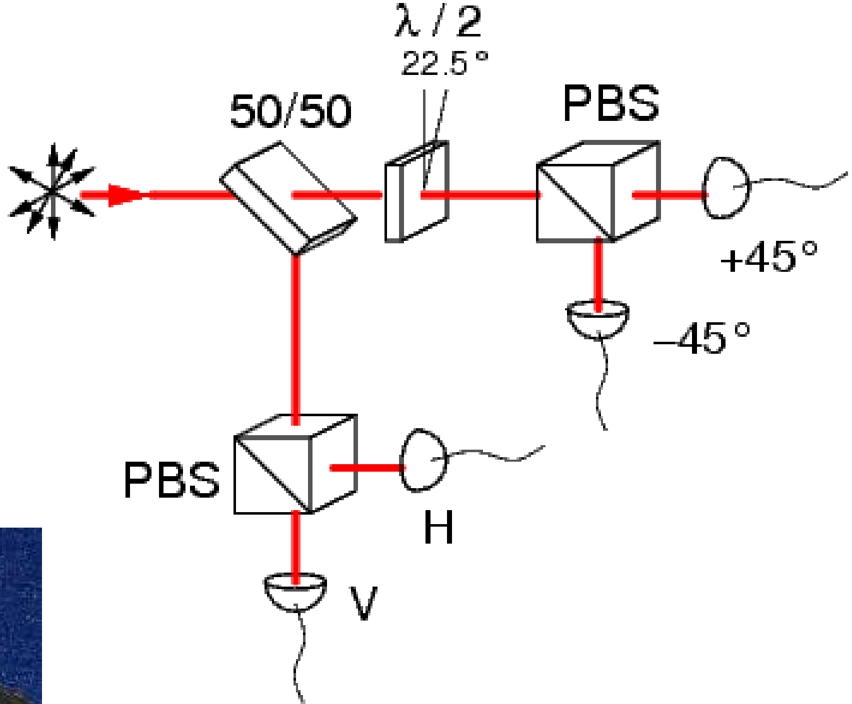


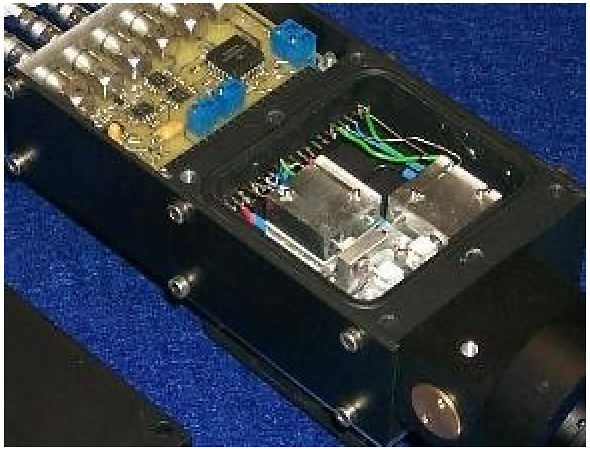
Polarization measurement

- Replace active basis choice by passive choice in a beam splitter

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

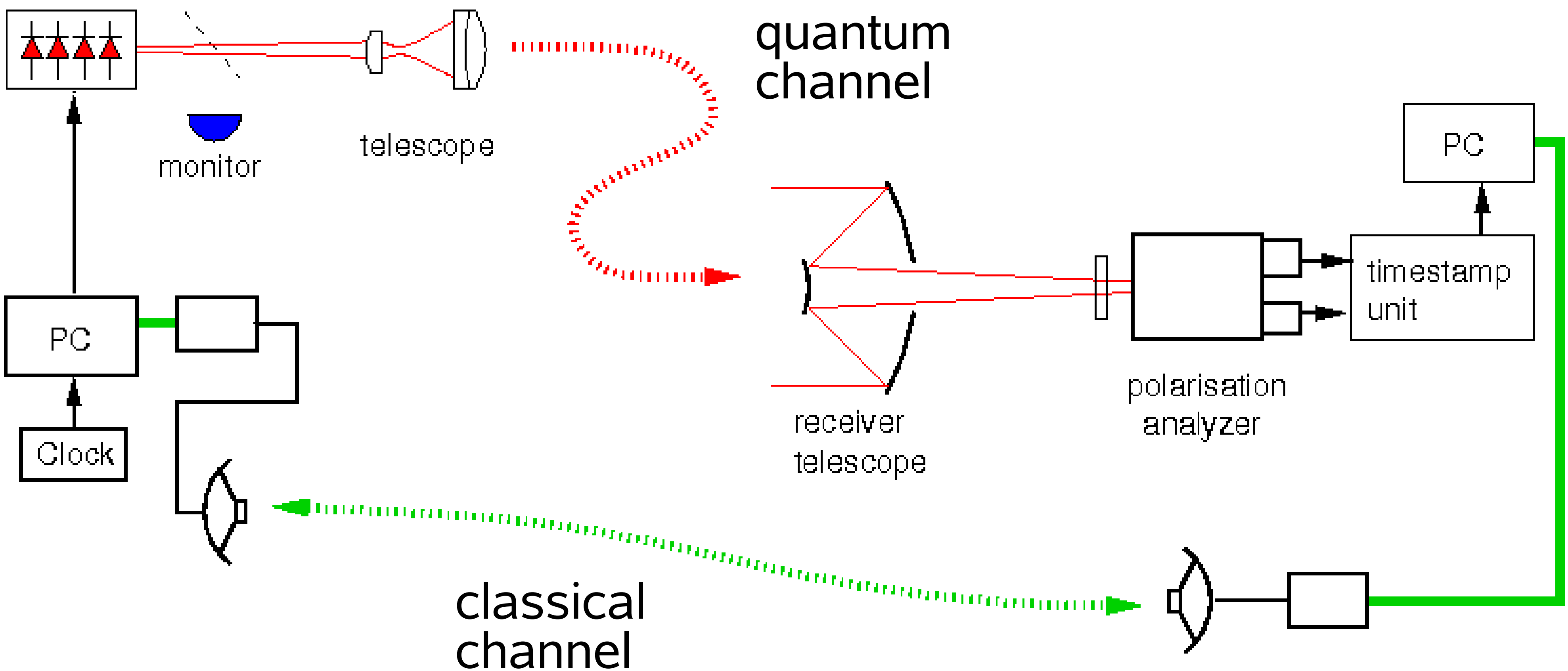




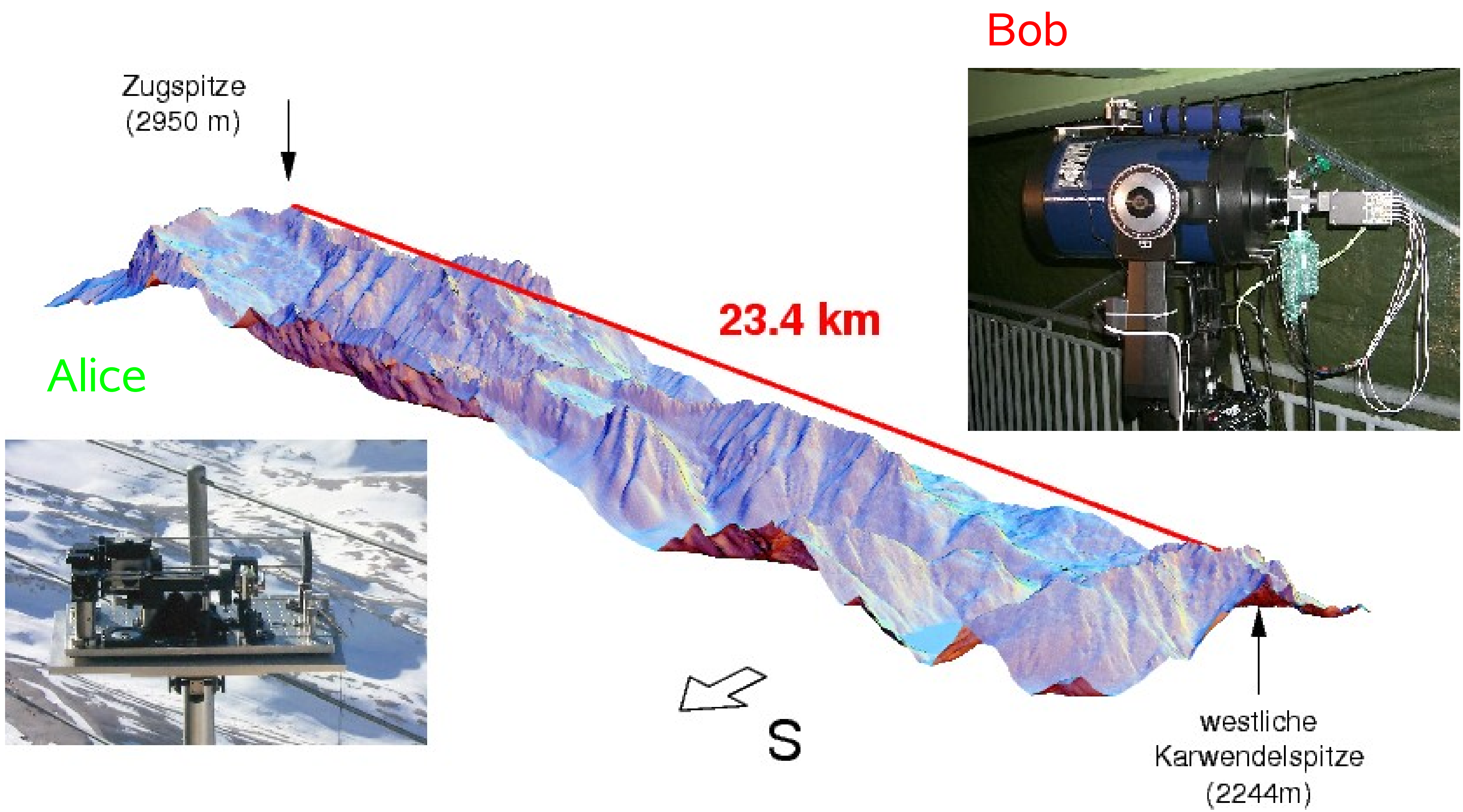


Transport of photons

- Transmission through free space



Bridging distances



*C. K., P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature **419**, 450 (2002)*

Current developments

- Larger distances (up to 144km demonstrated) to test for satellite – earth links

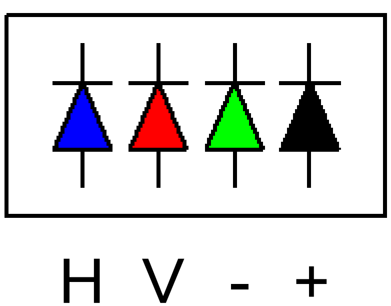
  Munich/Vienna/Bristol:
  T. Schmitt-Manderbach et al., Phys. Rev. Lett. ***98****, 010504 (2007)*

- Larger key rates: VCSEL lasers, detectors with better timing resolution, high clock rates

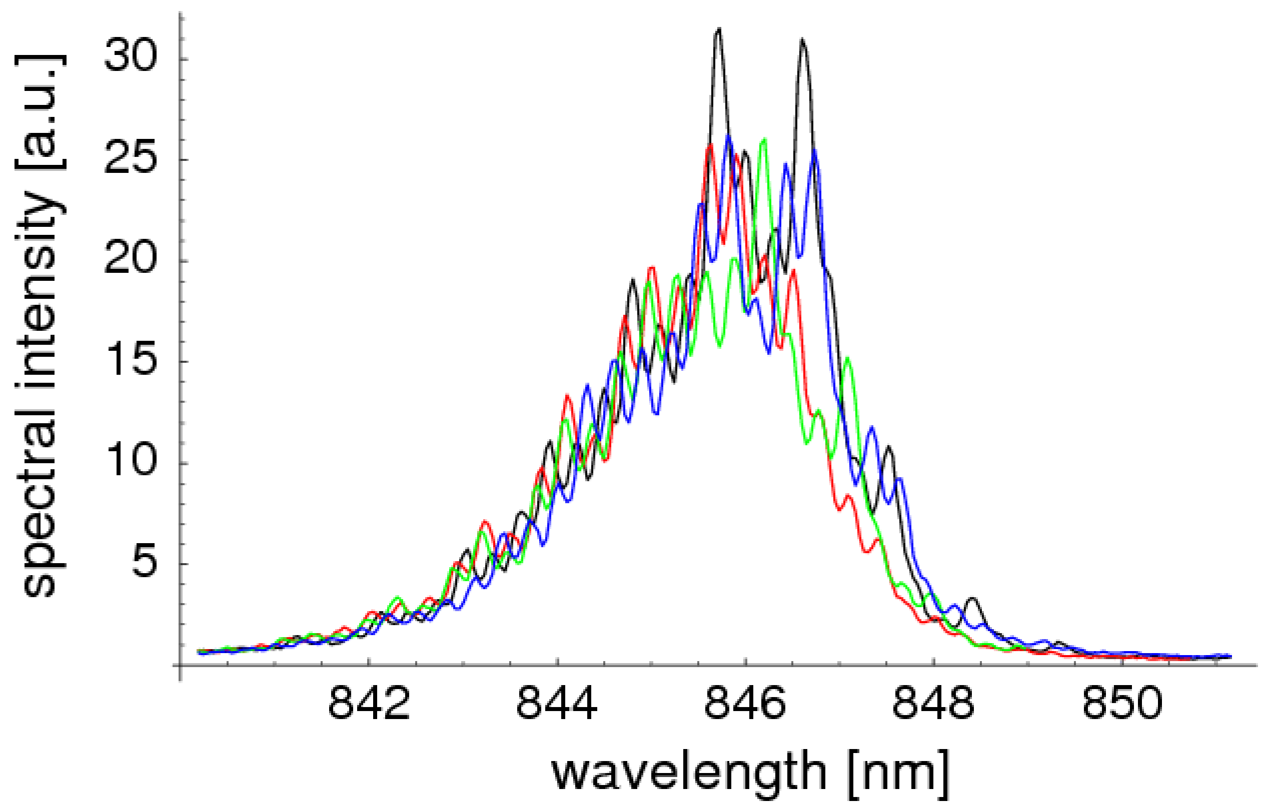
  NIST Gaithersburg:
  J.C. Bienfang et al. Optics Express ***12****, 2011 (2004)*

BB84: Spectral attack

Different “letters” may be distinguishable
Here: By spectral signature from four different laser diodes



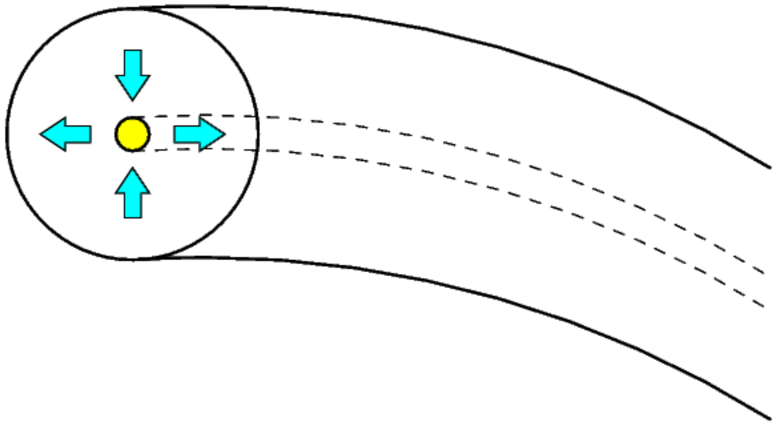
asymptotic average information leakage: <2%



C.K.,P. Zarda, M. Halder, H. Weinfurter (2001)

Transport through fibers

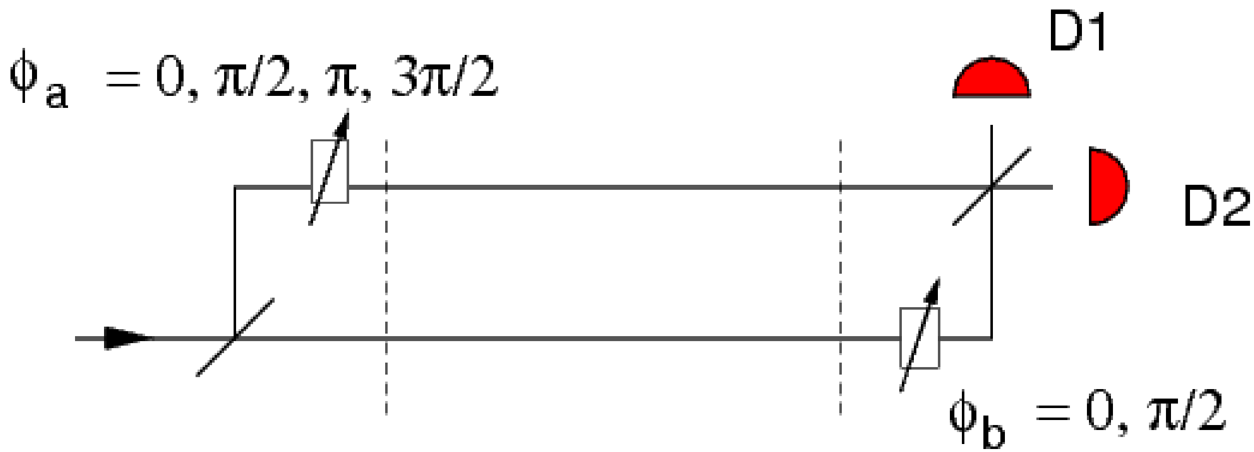
- Very practical: Less susceptible to environment
- Use existing telecom infrastructure
- High optical transmission
  - 800 nm: 2dB/km (T=63% for 1 km) Si detectors
  - 1310nm: 0.2dB/km (T=63% for 10 km)
  - 1550nm: 0.35dB/km (T=44% for 10 km) InGaAs detectors
- Optical birefringence / vector transport



polarization encoding
is more difficult -

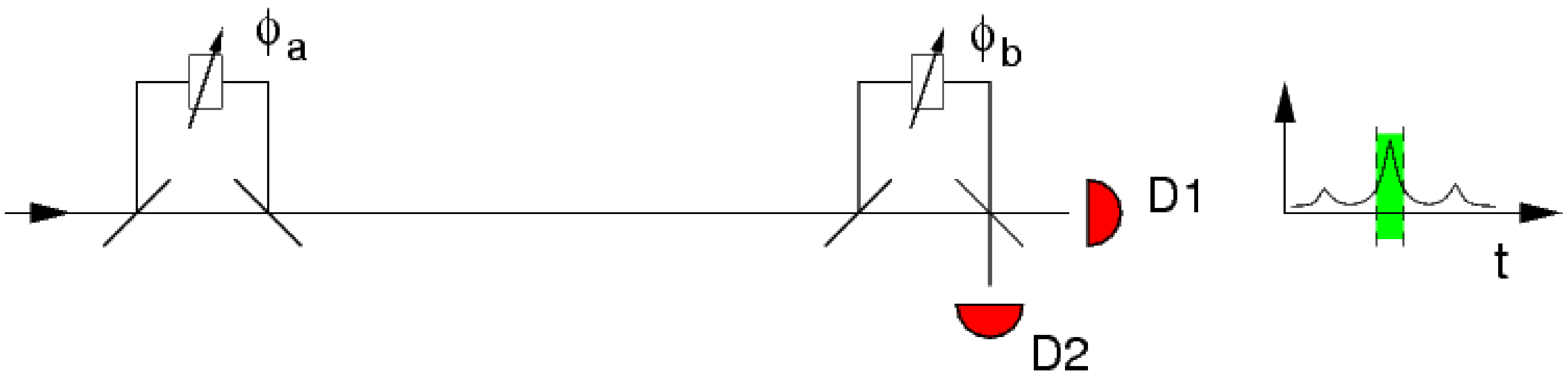
Other encoding techniques

- Encoding qubit in relative phase between two packets



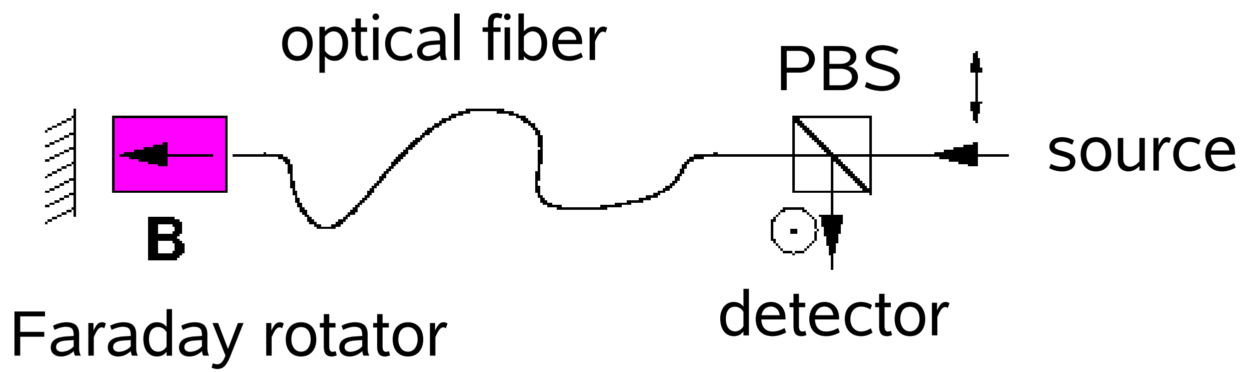
equivalent to polarization encoding

- Replace fiber pair by time structure (early / late)



Birefringence compensation

- Probe fiber birefringence via two passes with Faraday mirror



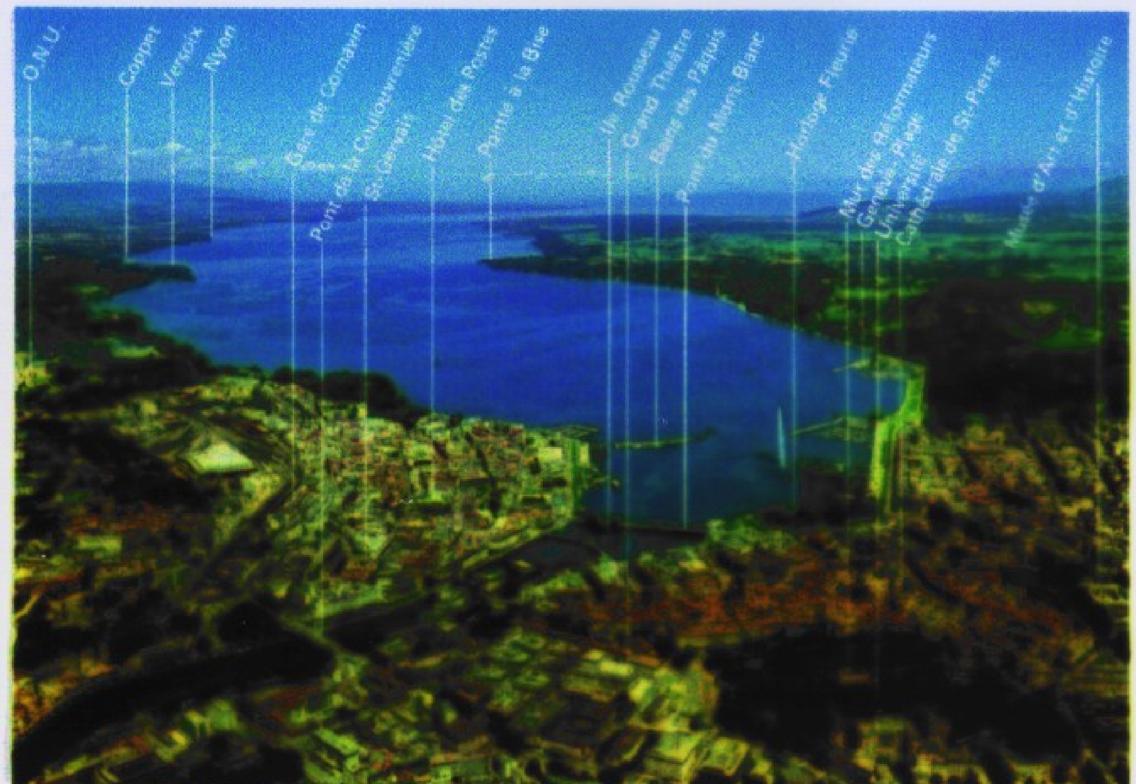
- Basis of "Plug & Play" or autocompensation schemes in commercial QKD systems (id quantique, NEC)
- Bridging ~100 km

N. Gisin & team, GAP optique, Geneva
D. Bethune / W. Risk, IBM Almaden
A. Karlsson, KTH Stockolm
NEC

Geneva lake demonstration

NUS National University of Singapore

The Laboratory



UNIVERSITÉ DE GENÈVE

FACULTÉ DES SCIENCES
SECTION DE PHYSIQUE
GROUPE DE PHYSIQUE APPLIQUÉE

Simple Estimations

NUS National University of Singapore

- BB84 raw key rate:

#photons/pulse

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

channel transmission

primary send rate   detector efficiency

- Probability for a background event:

$$P_D = d \times \tau$$

detector dark count rate   detection time window

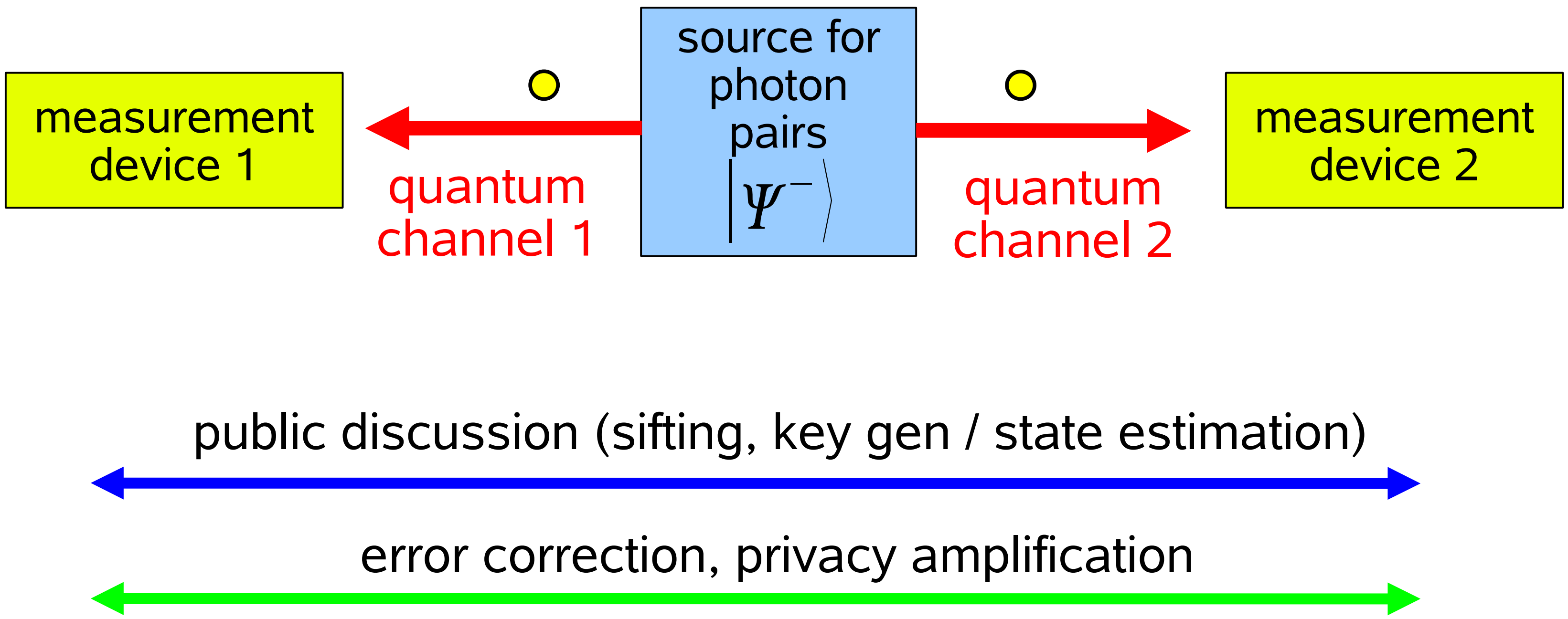
Si: 10^{-7}
InGaAs: 10^{-5}

- detector-induced bit error ratio

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

Different protocols

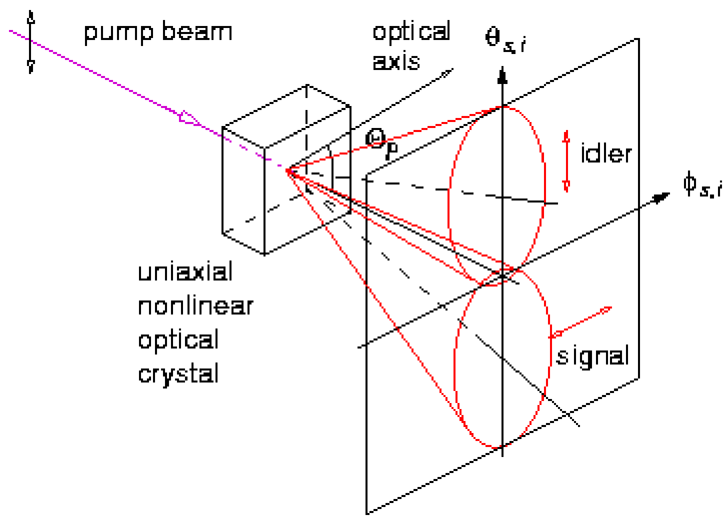
Nonclassical correlation protocols (E91, tomographic protocols)



- no need for trusted random numbers leading to raw key
- knowledge of eavesdropper is derived via a “witness” (knowledge of full state or something more efficient)

Entangled photon resource

- Use non-collinear type-II parametric down conversion



two indistinguishable decay paths lead to

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|HV\rangle - |VH\rangle\right)$$

*P.G. Kwiat et al., PRL **75**, 4337 (1995)*

- Collect pairs into single spatial modes (e.g. optical fibers) for good transmission

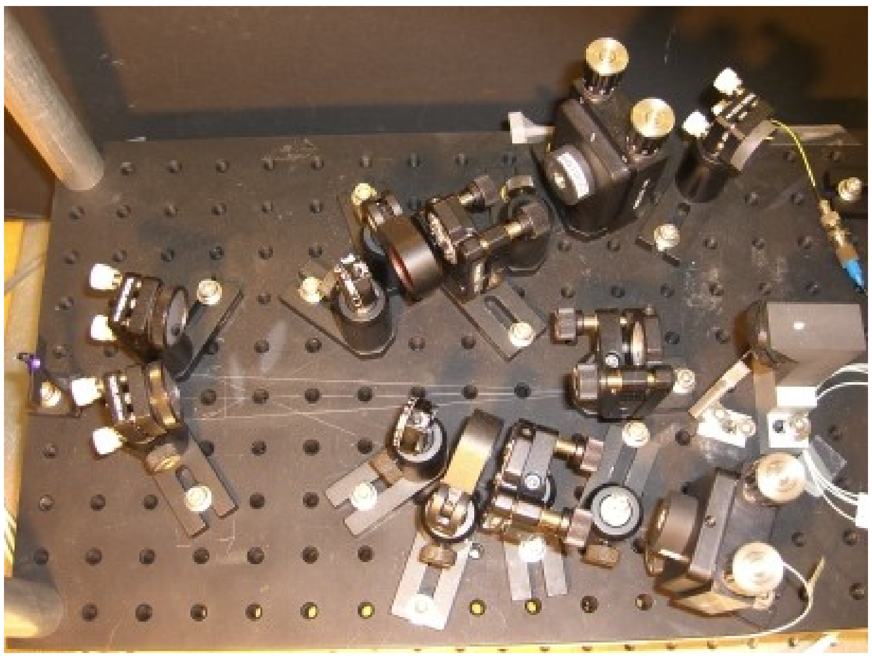
Possible: ~900 polarization-entangled photon pairs per sec and mW pump power (2mm long BBO) for ~97% visibility in 45° basis, ~4 nm bandwidth around 702 nm

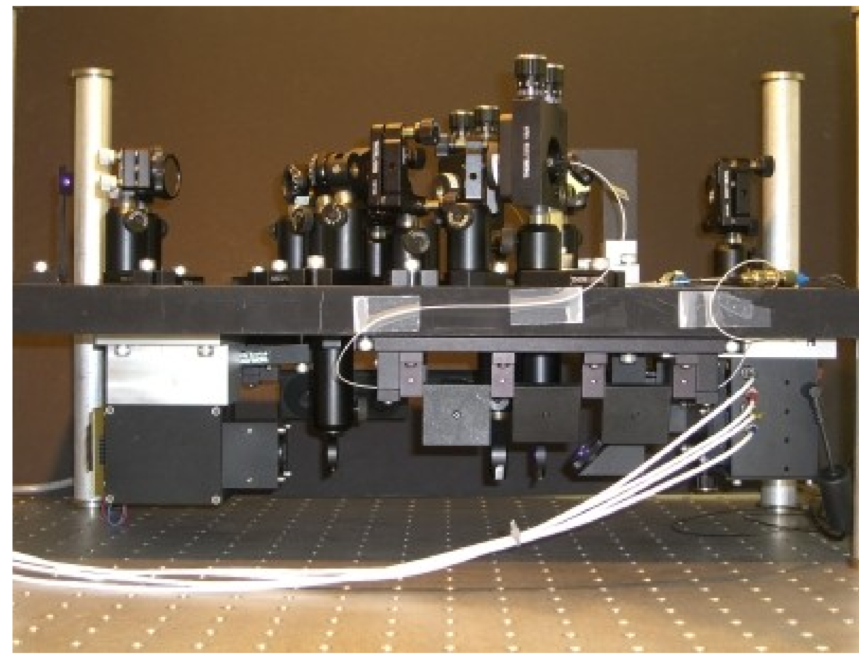
*C.K., M.O., H.W., PRA **64**, 023802 (2001)*

Photon pair source

National University of Singapore

Diode-laser pumped non-collinear type-II PDC in BBO

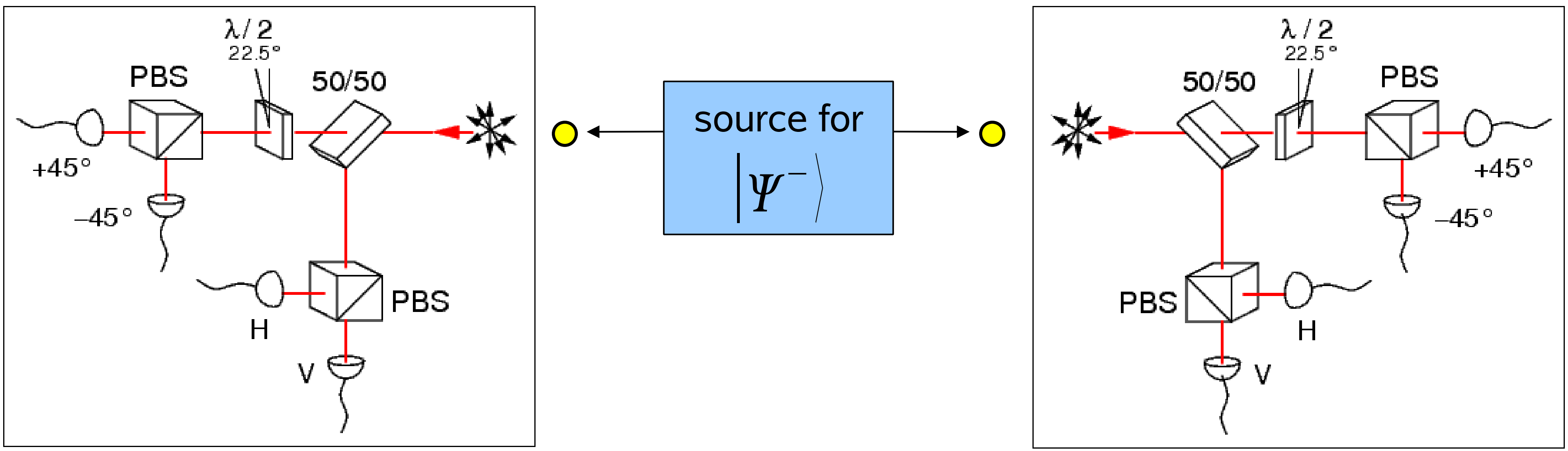




- 24,000 s^{-1} detected pairs from 40 mW pump @ 407nm in single mode fibers, 24 % pair/single ratio (2mm BBO)
- polarization correlation visibility in 45° basis: 92%
- optical bandwidth 6.5 nm FWHM around 810nm / 818 nm
- small footprint, works in outdoor conditions

Our implementation

BB84-type QKD system using polarization-entangled photon pairs

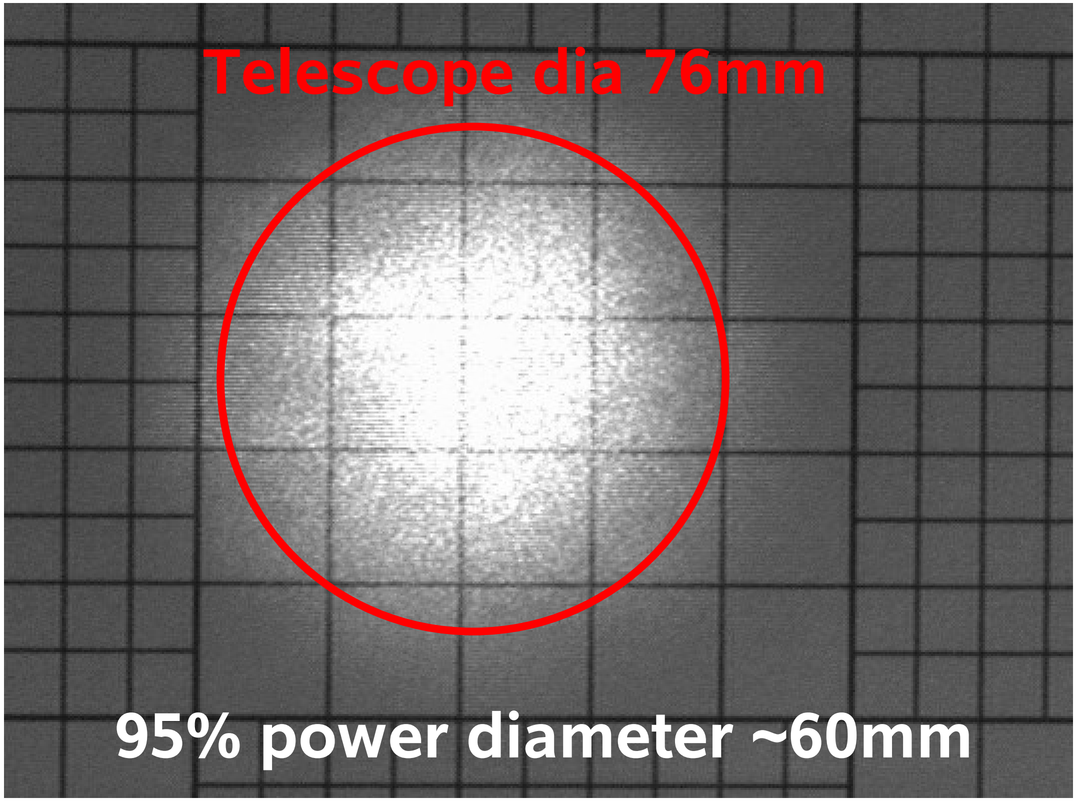


- Perform measurements randomly in H/V or +/- 45deg base on both sides
- Continue with measurement results like in BB84
- No explicit need for a random number generator

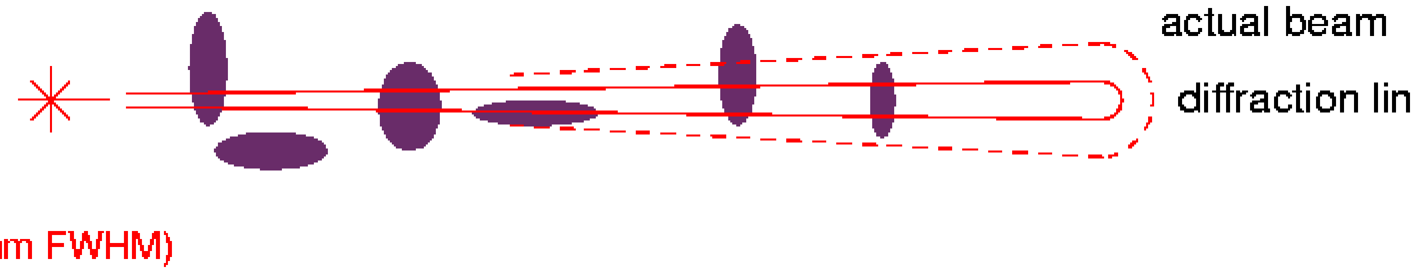
NUS campus test range

Scintillation in atmosphere

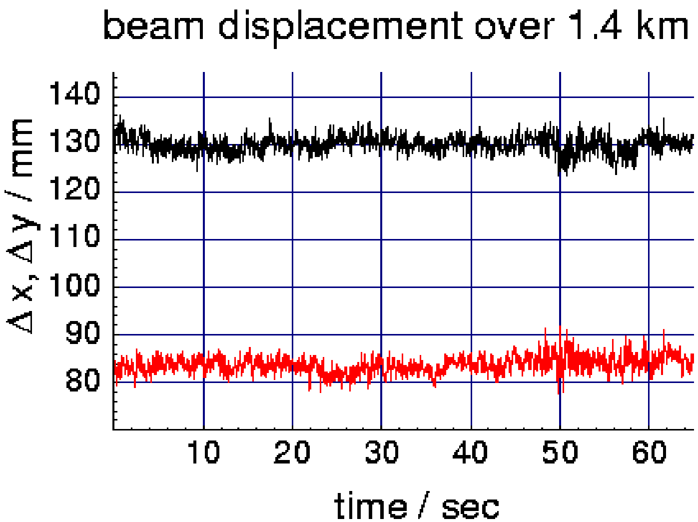
Intensity distribution before the receiver telescope, tested with a bright (500 μW) laser beam @808 nm through the optical system

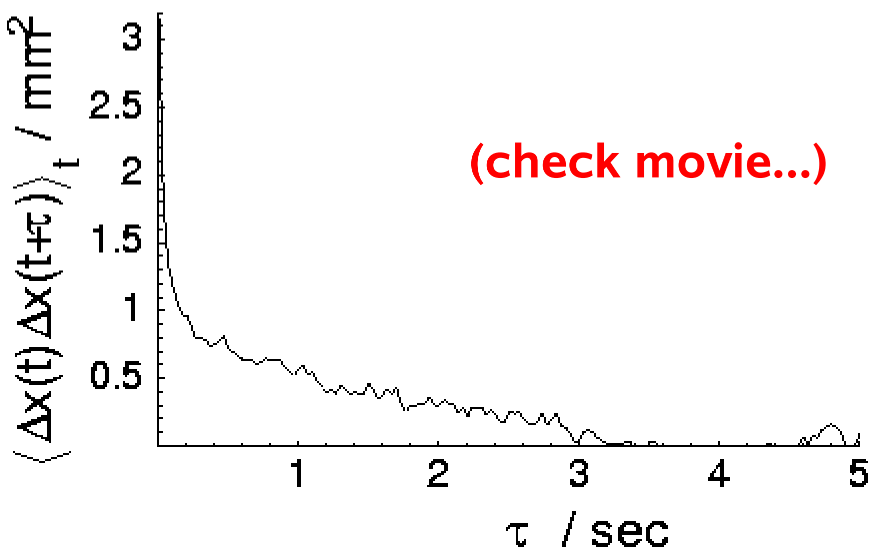


More scintillation



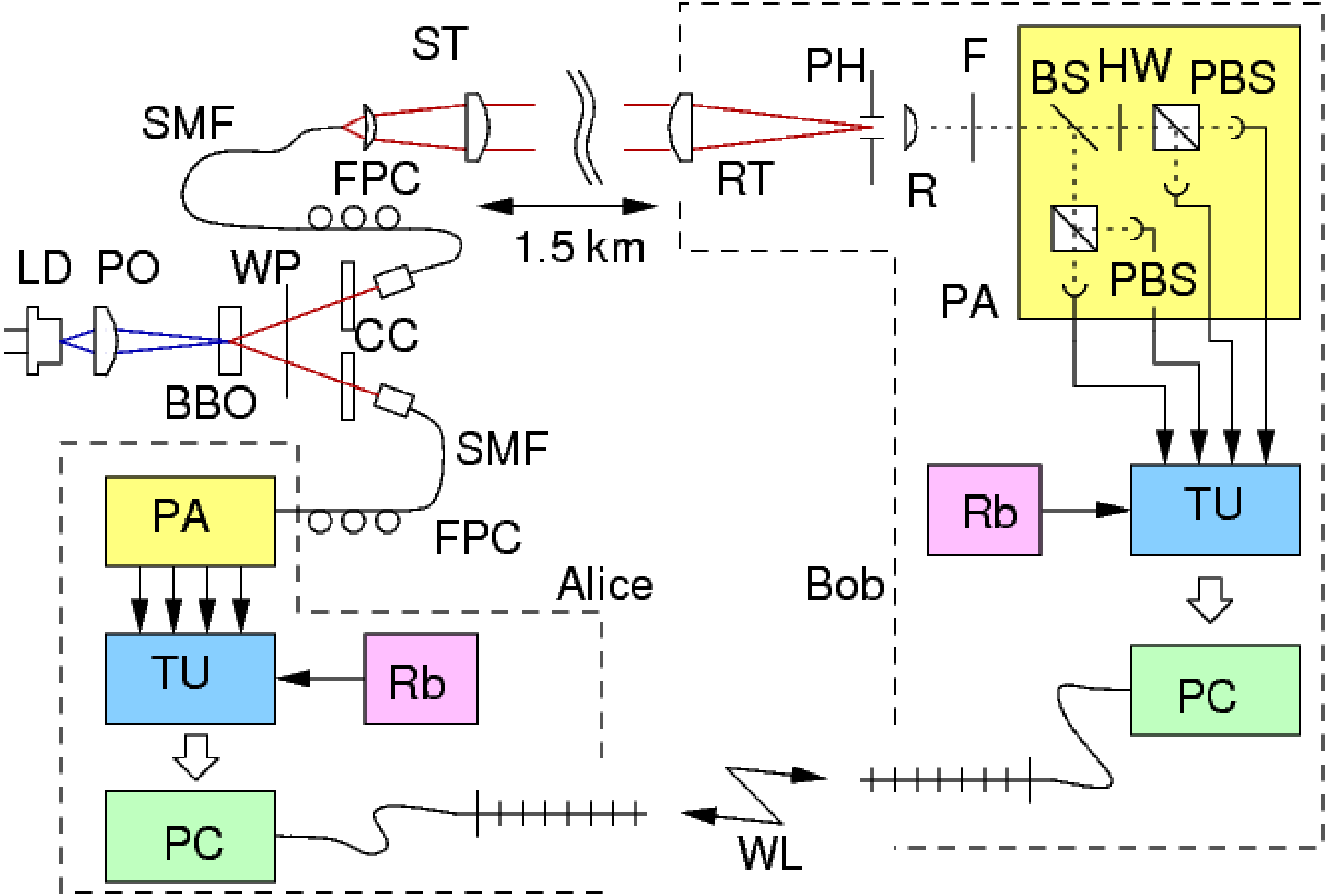
- Beam wandering due to air turbulence seems very low!



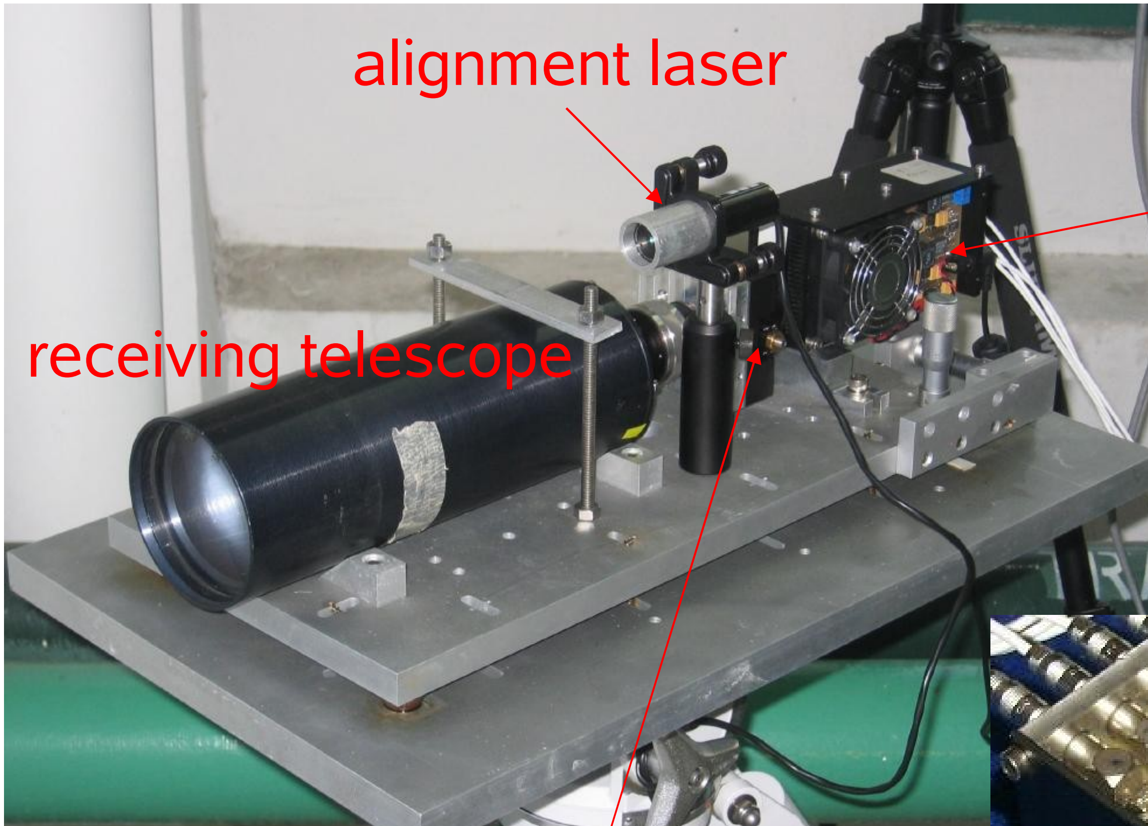


(check movie...)

System setup



Receiver unit

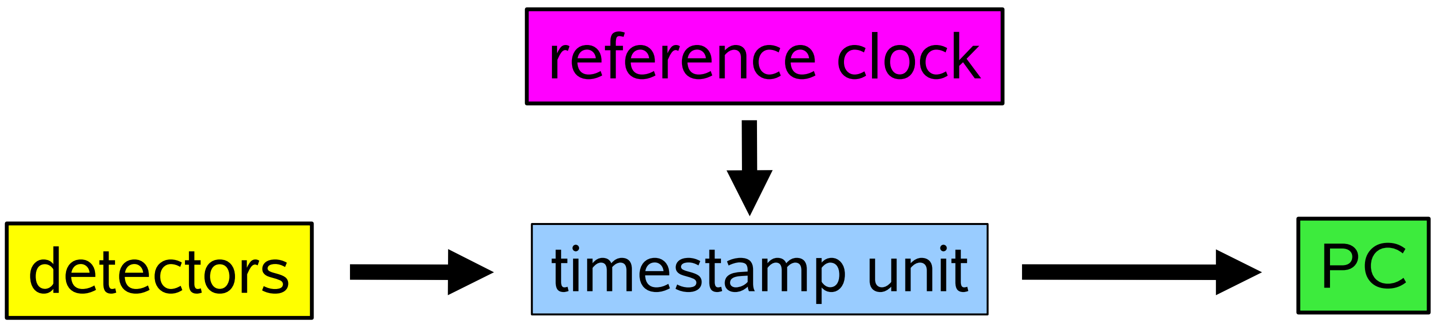


polarization analyzer
passively quenched
Silicon APD
- QE ~50%

~1000s^{-1} dark cnt rate

Coincidence identification I

- Coincidence time is limited by APD jitter (~700 ps)

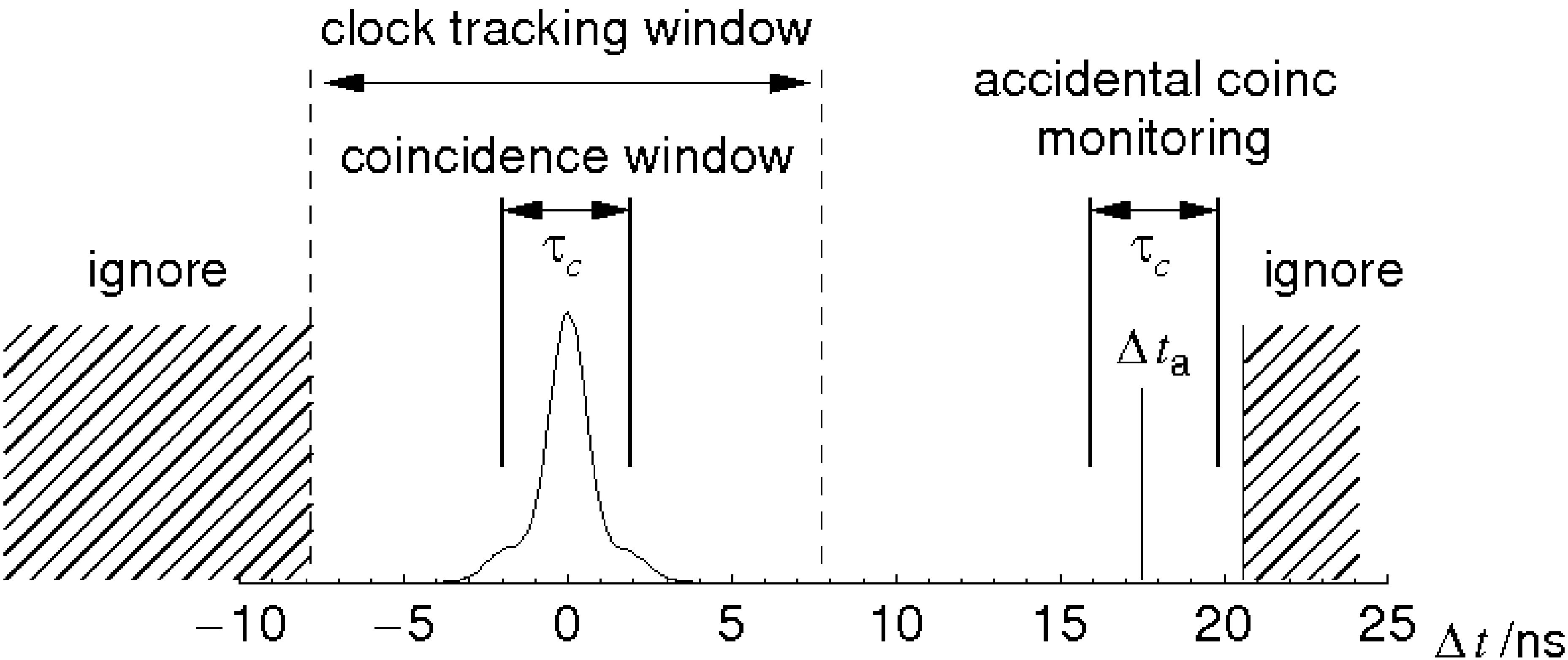


- 125 ps nominal resolution / 500 MHz master clock
- 4 Mevents/sec into host PC via USB interface

- All the rest via software and (efficient) classical communication (15...20 bits per detected event, 13% above Shannon limit by compression)

Coincidence identification II

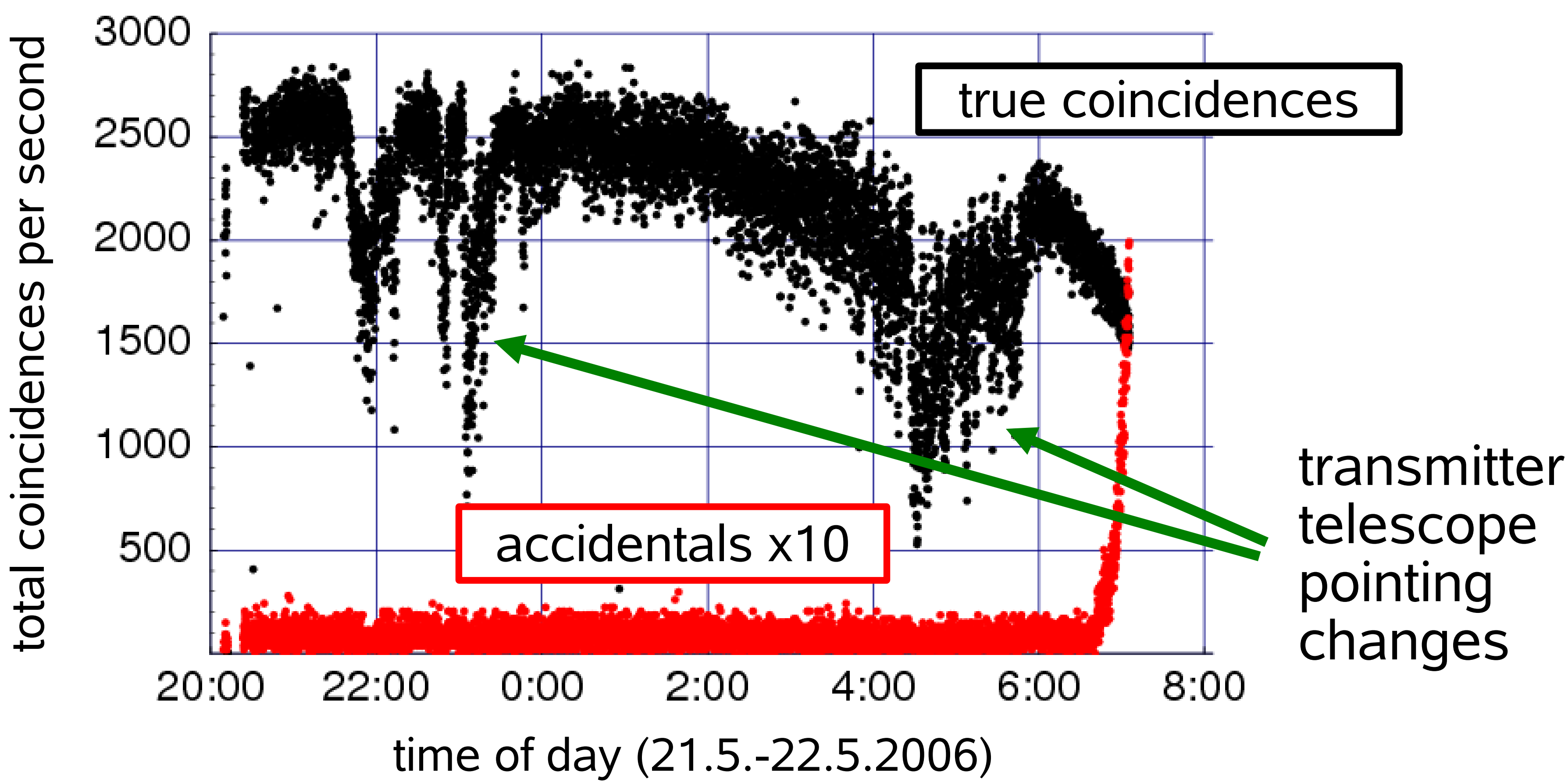
Use time correlation of photon pairs from PDC to identify pairs and to servo clocks



coincidence time: τ_c = 3.75 ns ; measured distribution: 1.4 ns (FWHM)

Experimental results I....

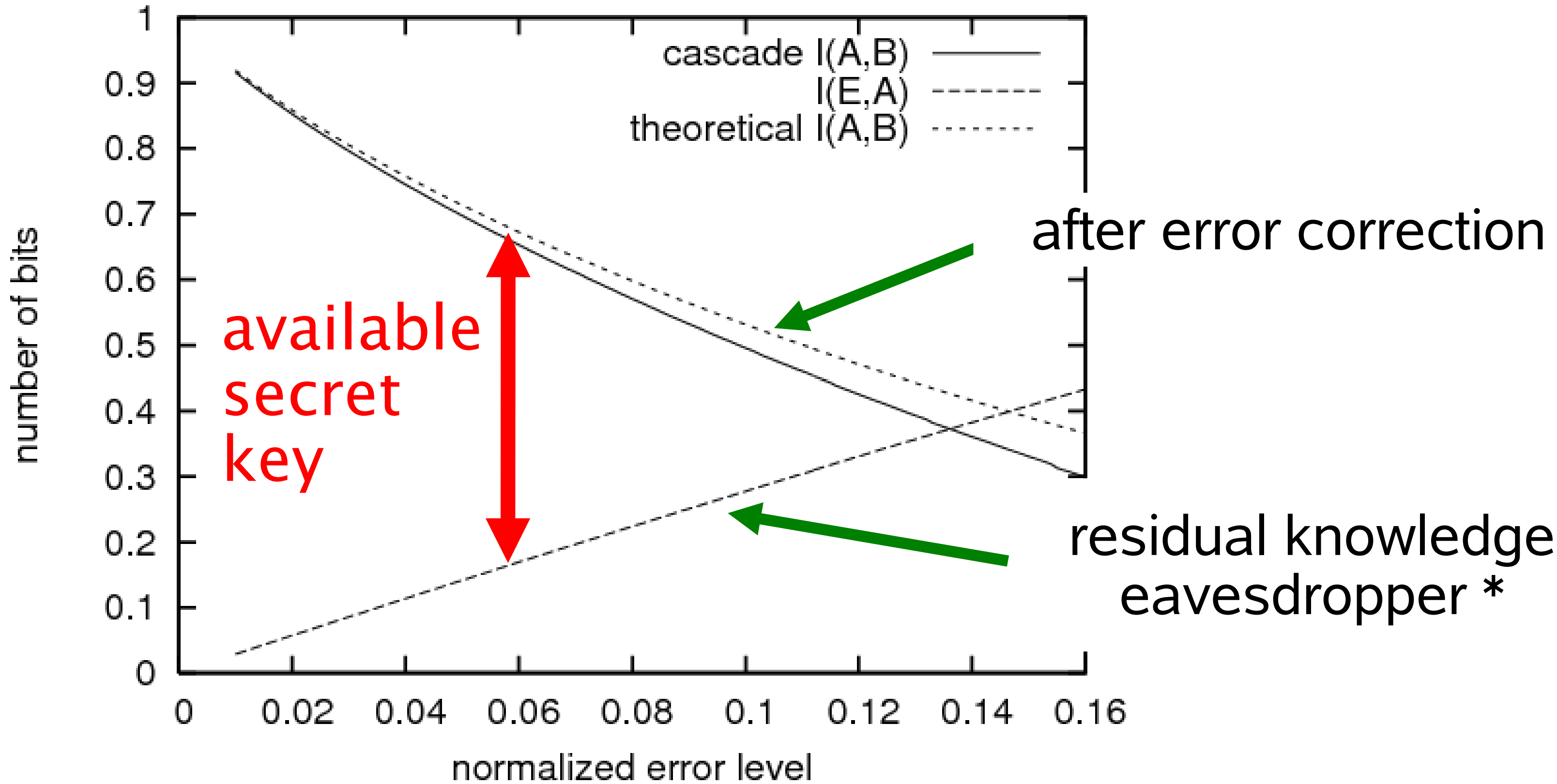
Identified raw coincidences between close and remote receiver



(with interference filter 5nm FWHM, 50% peak transmission)

Error detection / correction

correct for errors, estimate knowledge of an eavesdropper



* depends on the attack model (individual attack);
for *infinite* key length

Privacy amplification

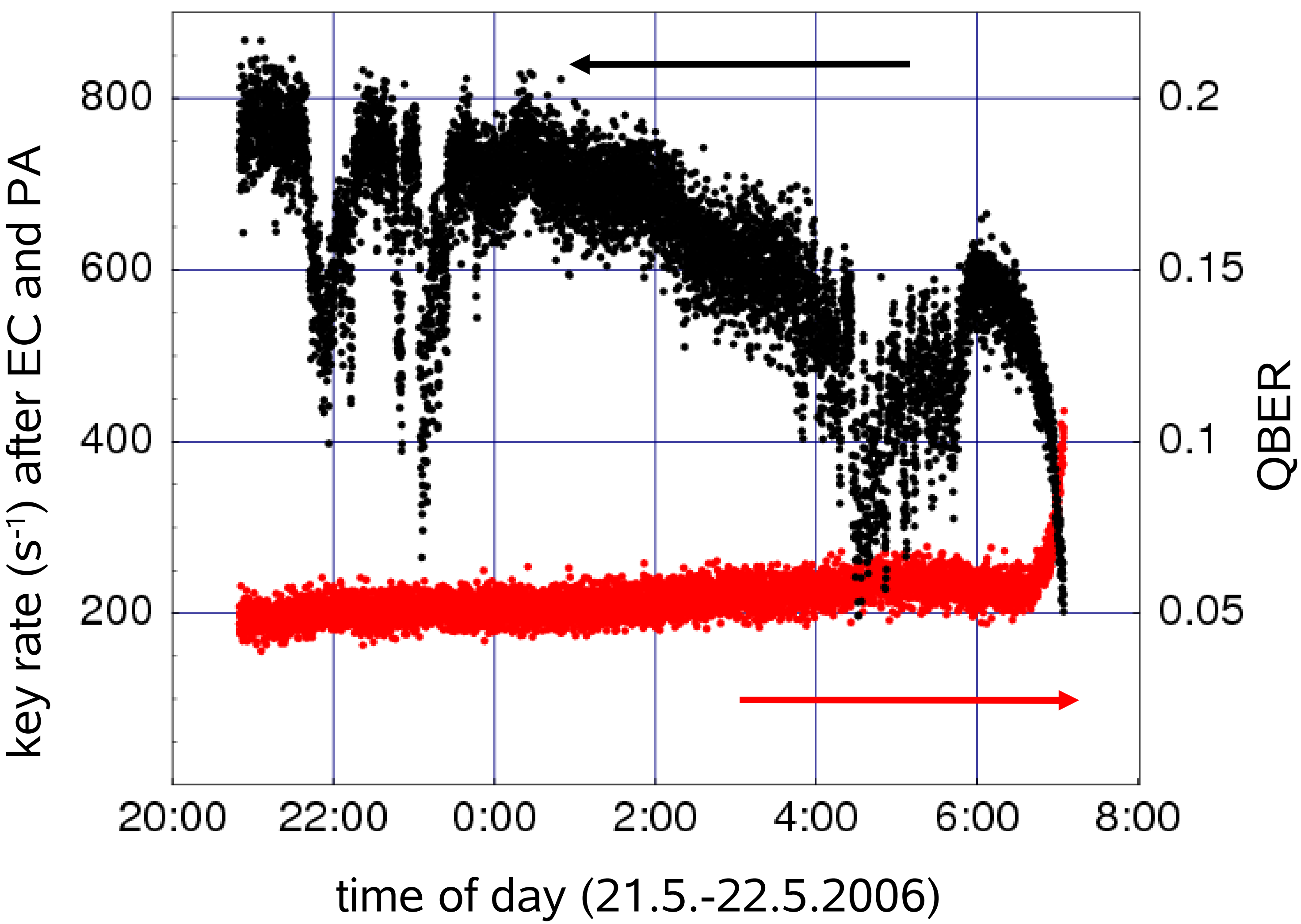
- compress raw key to a size corresponding to the information advantage vs. Eve..

final key	=	random matrix	x	key w/o errors

- All information leakage to Eve (attacks + error correction) has to be considered

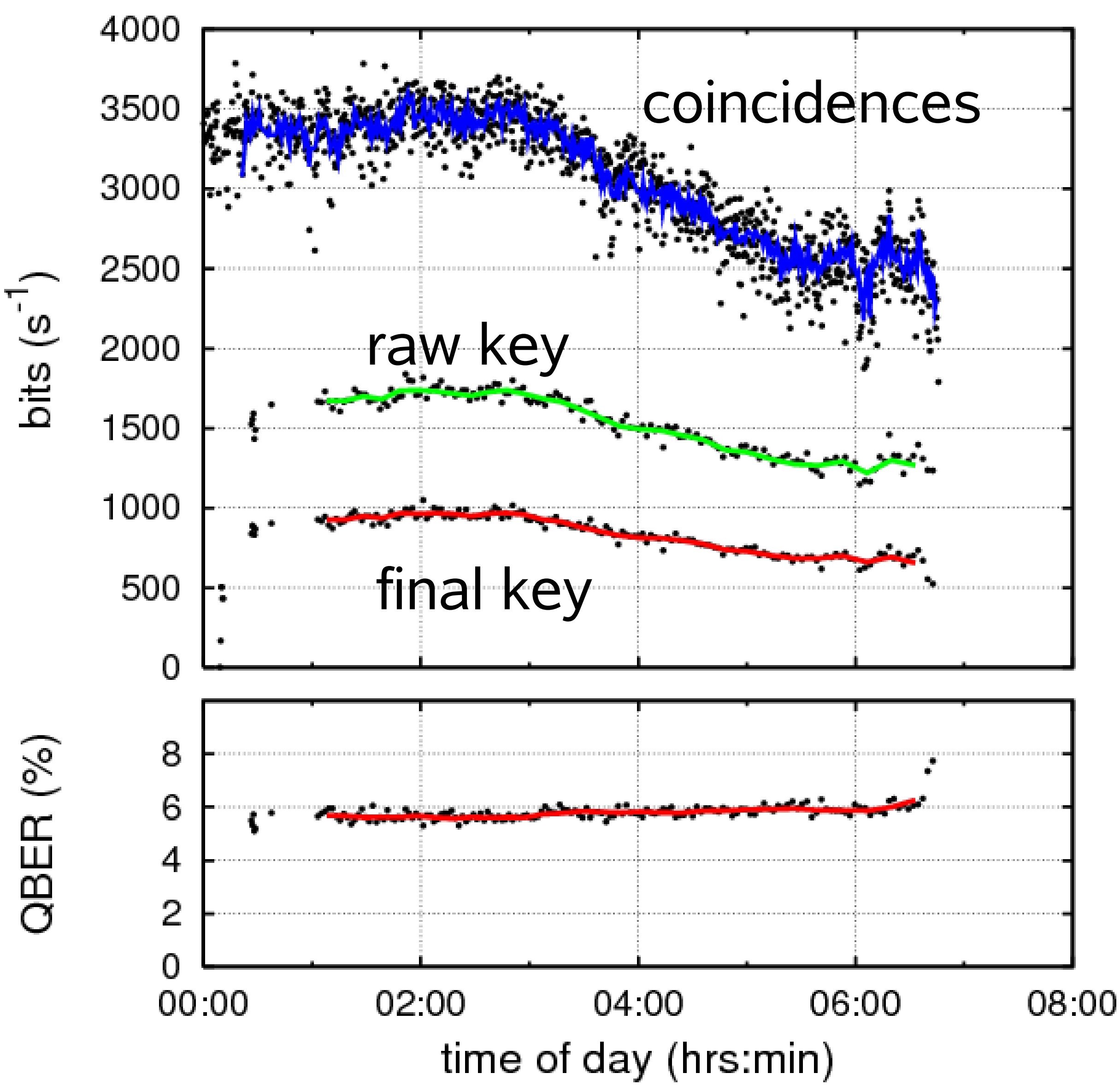
Tricky: finite key length may make privacy amplification more difficult – ~10^7 to 10^{10} bits

....and after The Works:



- CASCADE error correction with ~6000 bit packets
- assume incoherent attack strategy for privacy amplification
- average efficiency of EC/PA: >57%
- average final key rate: 650 bits/sec
- residual error rate ~10^{-6}

Without interference filters



(data taken 1.6.2006)

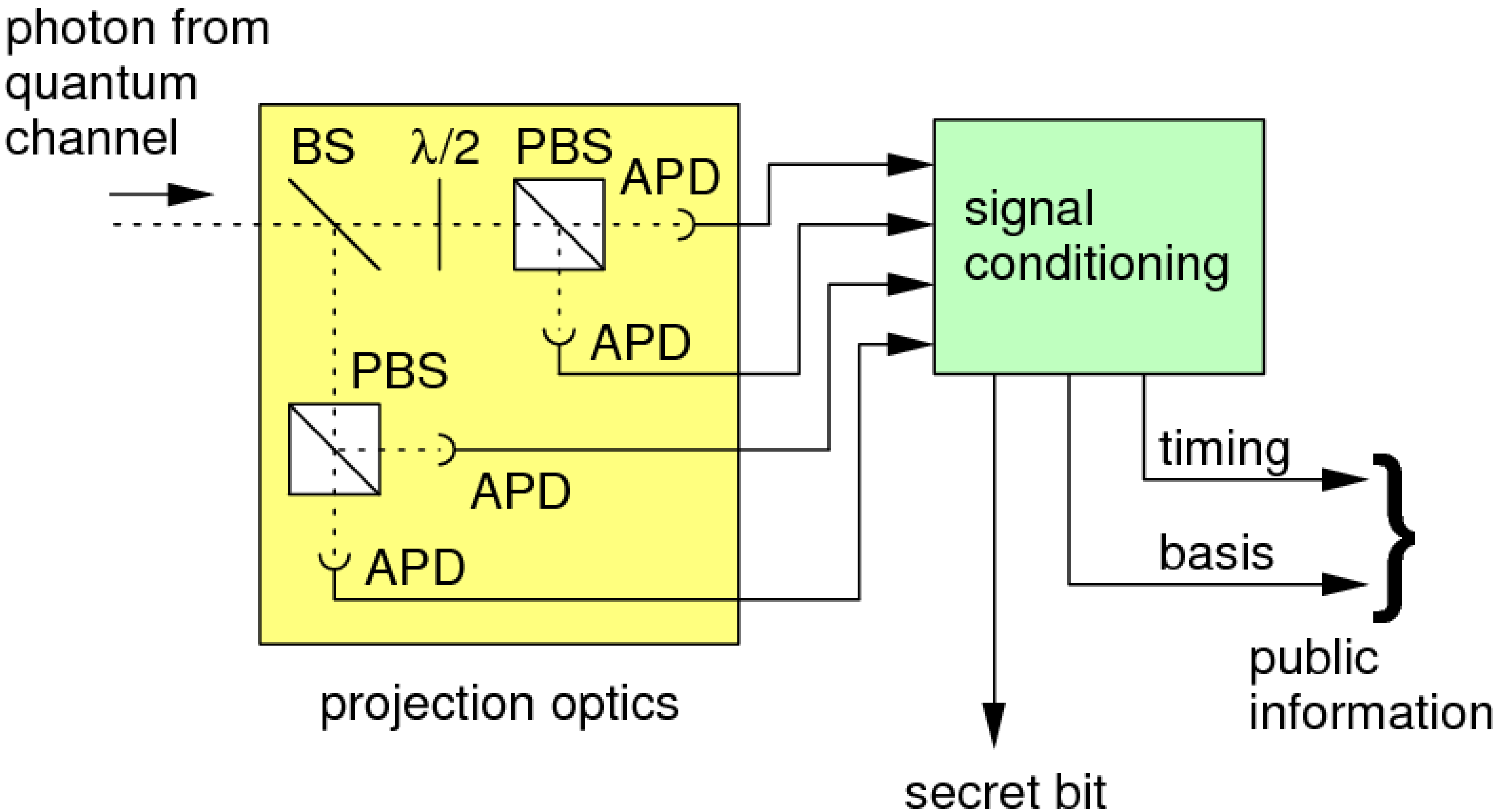
- use a RG780 long pass filter to suppress visible light
- average final key rate 850 bits/sec

(link loss 8.3 dB)

Why we think this is nice

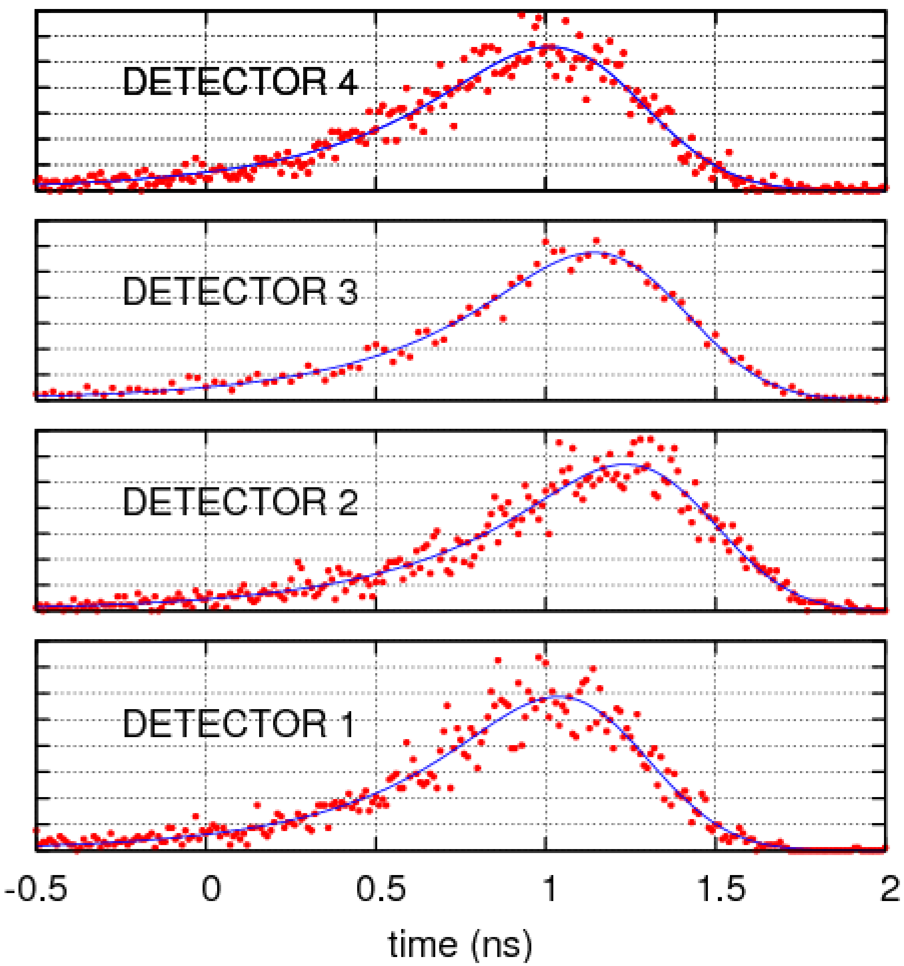
- Only passive components (no switches); technical complexity similar to faint pulse QKD implementations
- No external random numbers are needed
- No hardware sync channel needed besides the classical ethernet link
- Lean sifting communication (~15…20 bits per event)
- Reasonably compact, possible to install in ad-hoc situations
- Runs reliably hands-off and produces continuously key

Timing channel attack I

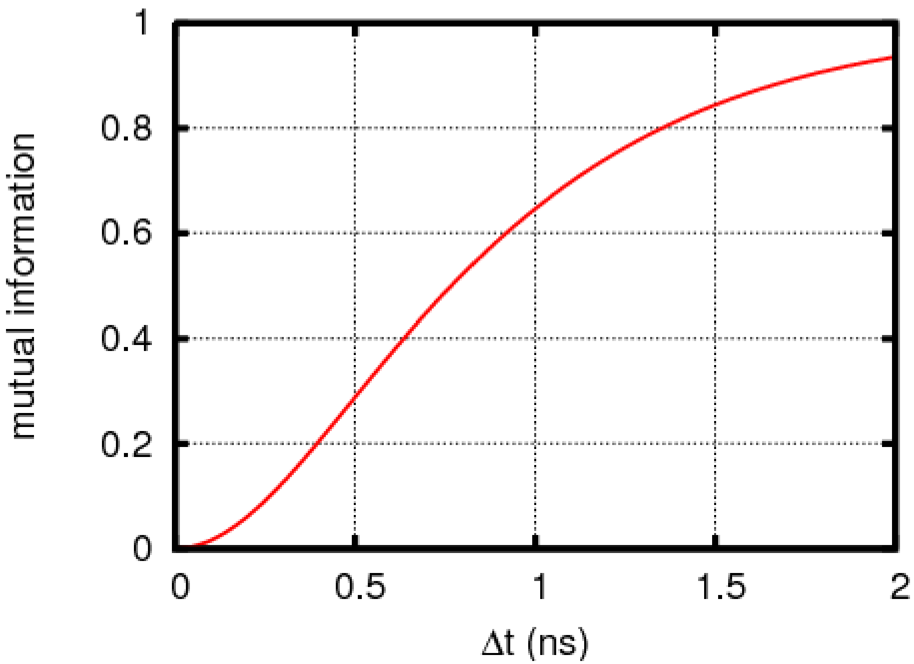


Timing channel attack II

Classical timing information carries fingerprint of detectors:



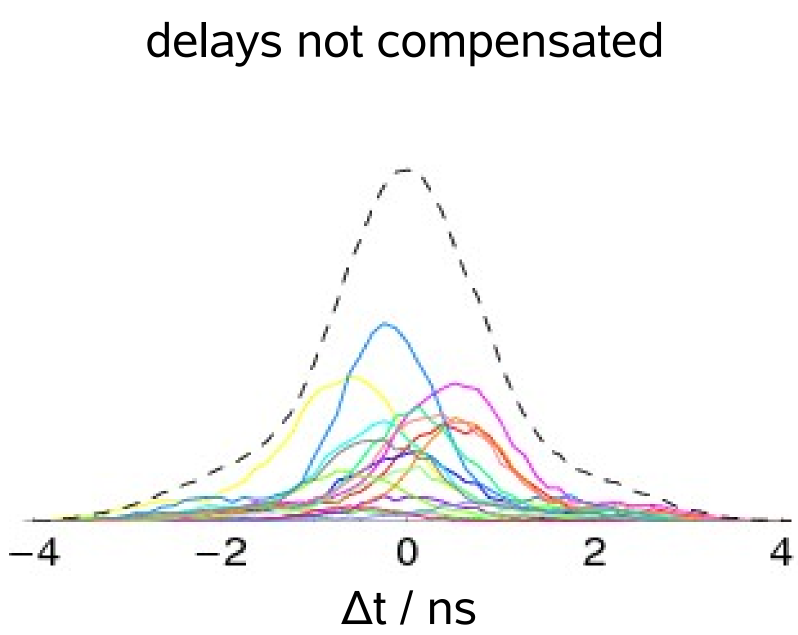
small detector imbalances may tell Eve a lot!

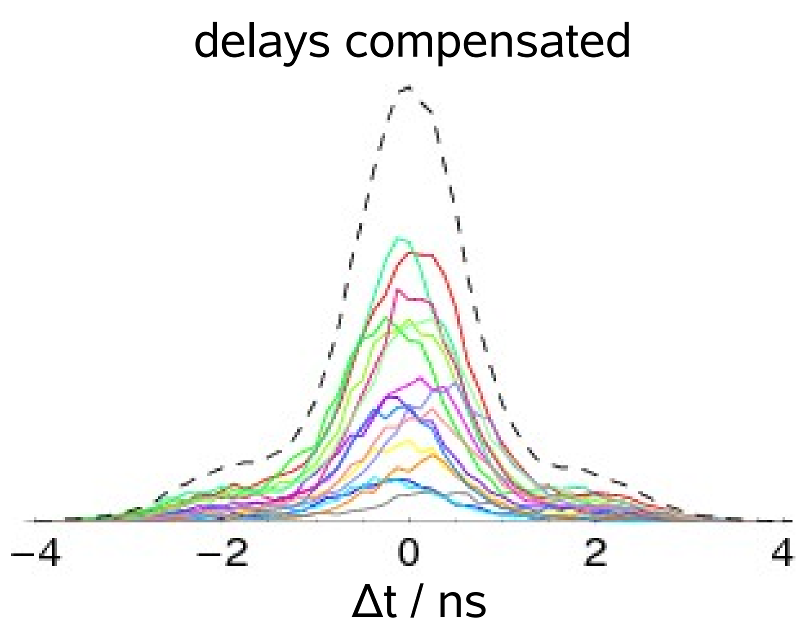


A. Lamas-Linares, C.K. quant-ph/0704.3297

Timing ch attack – The Cure

- Make sure no detail timing information is revealed.....





- Alternative cures (costly for background):
  - coarser quantized timing information
  - add timing noise

Challenges for daylight QKD

- Daylight irradiation ~ 10^2 W sr^{-1} m^{-2} μm^{-1} at 800 nm

  For $\Omega = 10^{-8}$ sr, $A = 0.005 m^2$, $\Delta\lambda = 5$ nm:
  10^8 photons/sec or 0.1 event per ns time window

  Detectable rate with standard Si APD: 10^6 s^{-1}

- narrow band filter: 0.5..1nm — factor 5..10
  (on the way: 1nm source)
  reduce background brightness: — factor 10 or more

- other approaches (need very narrowband spectra)

  atomic filters (~10 MHz) — *X. Shan et al, APL **89**, 191121 (2006)*

  Fraunhofer lines (~ 1.2 Å) — *J. Bienfang & friends @ NIST Gaithersburg*

More daylight QKD

- Current status:

  - Receiver can handle 4×10^6 s^{-1} event rate using USB transfer
  - system starts reliably and generates key with ~5% QBER under “moderate daylight conditions”, i.e., overcast skies, and/or early evening over short distances (30m)

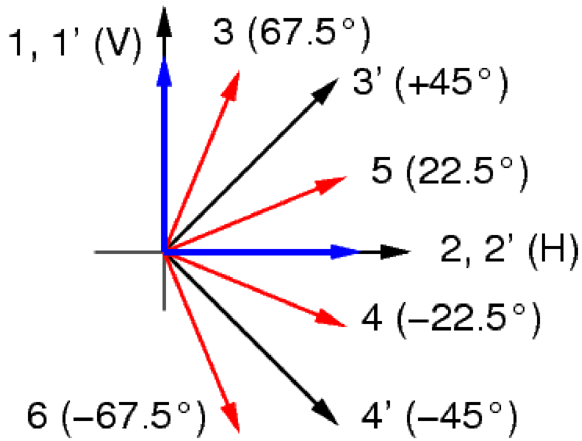
  - longer distance trials ongoing....

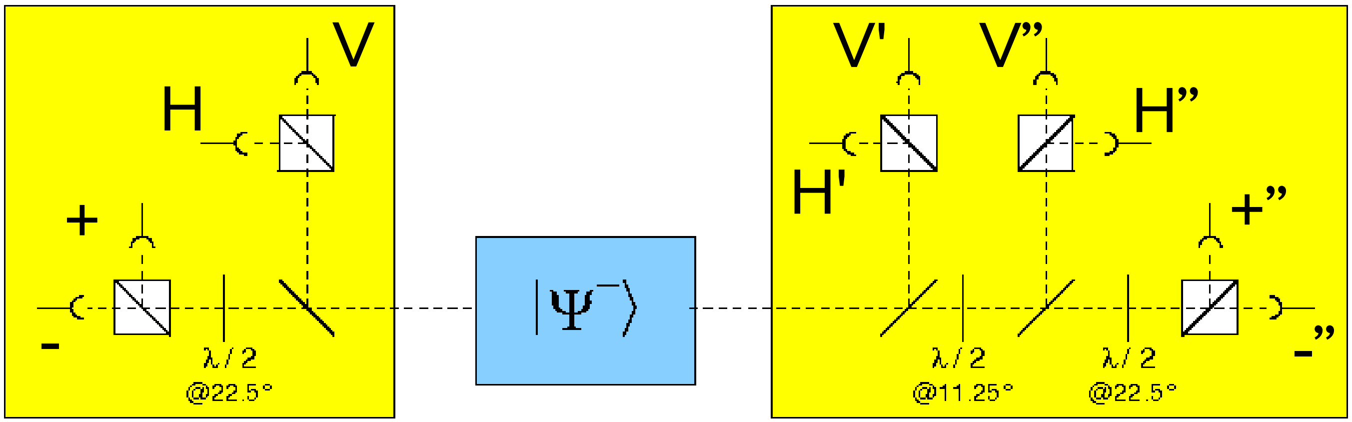
- Uglier in daylight:

  - Initial alignment of telescopes
  - more scintillation

Smart plugging of side channels

Modified E91protocol
(side-channel independent, towards *“device-independent”*)





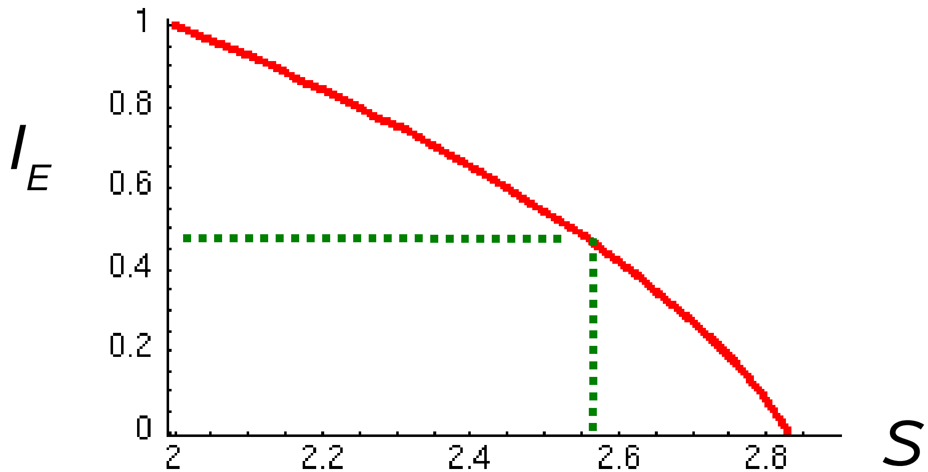
- {H,V; H',V'} coincidences → key generation
- {H,V,+,-;H”,V”,+”,-”} coincidences → CHSH Bell test
- low QBER with existing simple source

A. Acin, N. Brunner, N. Gisin,S. Massar, S. Pironio, V. Scarani, PRL 98, 230501 (2007)

Indoor results

test run over 6853 seconds with short free-space link (1.3m):

total identified coincidences: N_c = 41×10^6 pairs
total collected raw key: N_k = 11×10^6 bits
error ratio: QBER = 1.97%
Bell violation over all events: S = 2.569+/-0.001

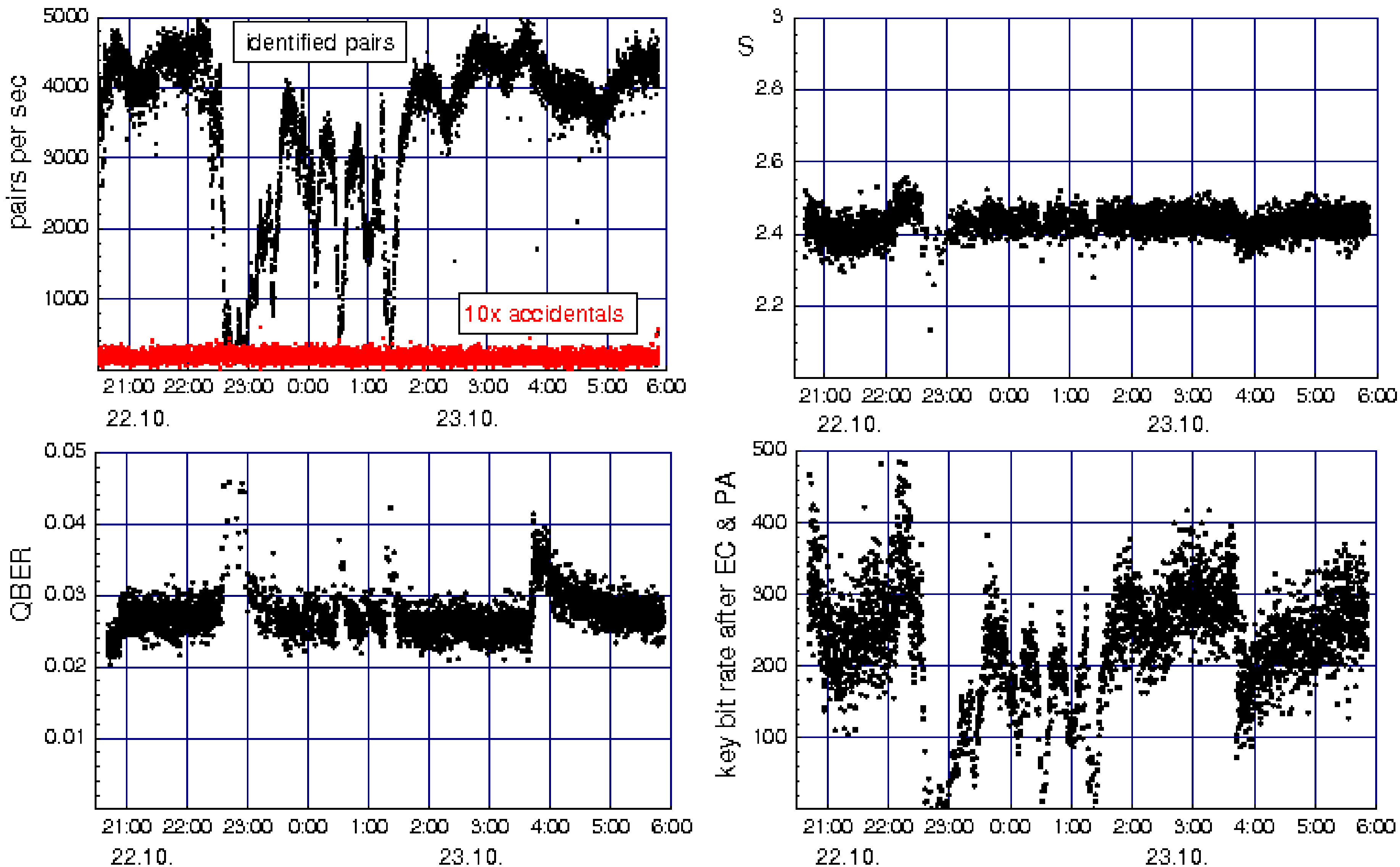


Holevo information of Eve: I_E = 46.7%
key-contributing pairs: 27.4%
asymmetry: $N_0/(N_0+N_1)$ = 0.49
QBER distribution on 0/1 bits: 1:1.67

Field results (1.4km range)

NUS National University of Singapore

- typical data run (with tropical rainfall inbetween)



Ongoing developments

- Availability of much stronger entangled photon pair sources based on PPKTP converters

  T. Jennewein et al., Opt. Express ***15,*** *15277 (2007)*

- Influence of finite-length key on privacy amplificaton

  V. Scarani, R. Renner, work in progress

Time for Coffee.....

Thank you !

http://qoptics.quantumlah.org/lah/

Time difference finding I

- Obtain discrete cross correlation function via

$$ccf(\tau) = F^{-1}\left[F\left[f_a\right] \cdot F\left[f_b\right]\right]$$

with two discrete pairs of folded detector functions

$$f_{a,b}(k) = \sum_i \delta_{k,\left(t_i^{(a,b)}/\Delta t\right) mod N}$$

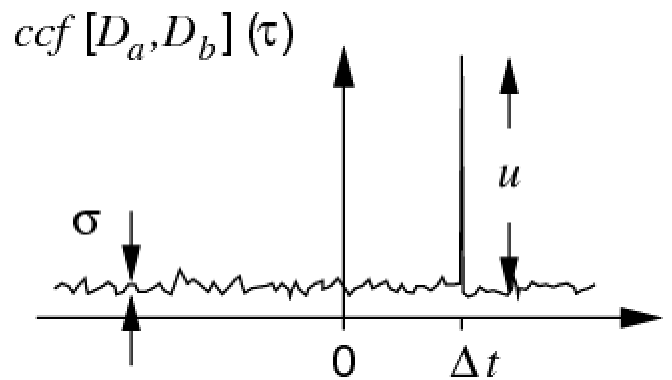
for $N=2^{17}$ and

- combine peak positions in ccf for different Dt to get the coarse and fine value of the final time difference

$$\Delta t = 2\mathrm{ns}, 2048\mathrm{ns}$$

Time difference finding II

- Sea of uncorrelated photodetection events leads to noisy background of ccf:



- Need large enough SNR (u/sigma) to identify time difference with sufficient statistical confidence:

epsilon	0.1	0.05	0.01	0.005	0.001	0.0001
n=16 bit	4.67	4.81	5.12	5.25	5.54	5.93
n=17 bit	4.81	4.94	5.25	5.37	5.65	6.04
n=18 bit	4.94	5.08	5.38	5.50	5.78	6.15
n=19 bit	5.08	5.21	5.50	5.62	5.89	6.26

Time difference finding III

- typical operating conditions:

$$r_1 = 80000\, s^{-1}$$
$$r_2 = 4000\, s^{-1}$$
$$\Delta t = 2\text{ns} \;\; / \;\; 2048\text{ns}$$

we obtain within 2.5 seconds a SNR>8 at $N=2^{17}$.

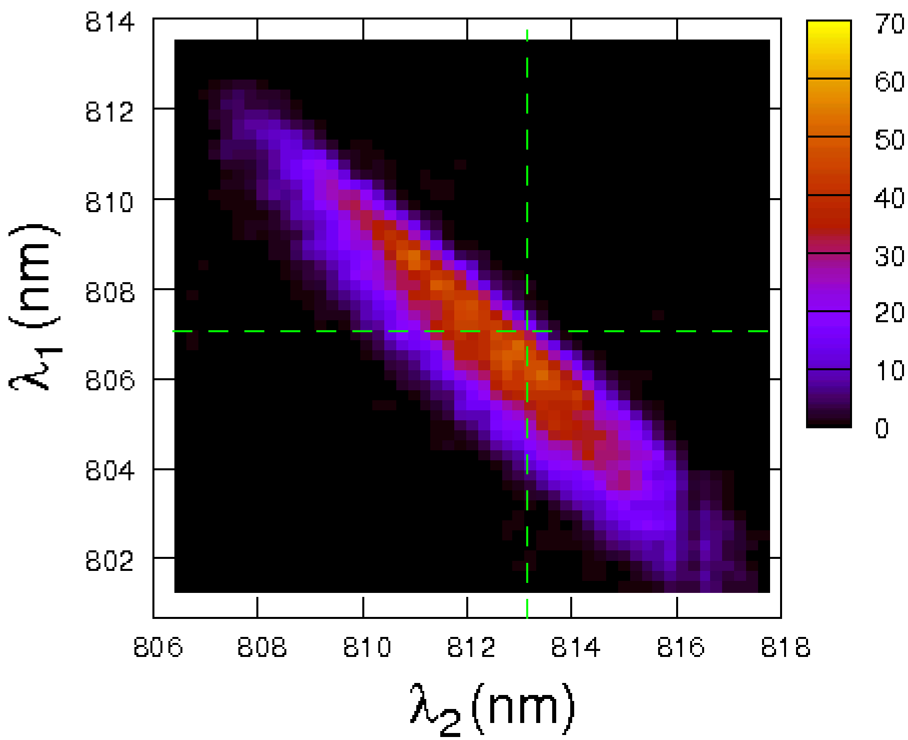
results vary, depending on overlap between sampled events

Conclusion: Periode finding works with very little numerical effort!

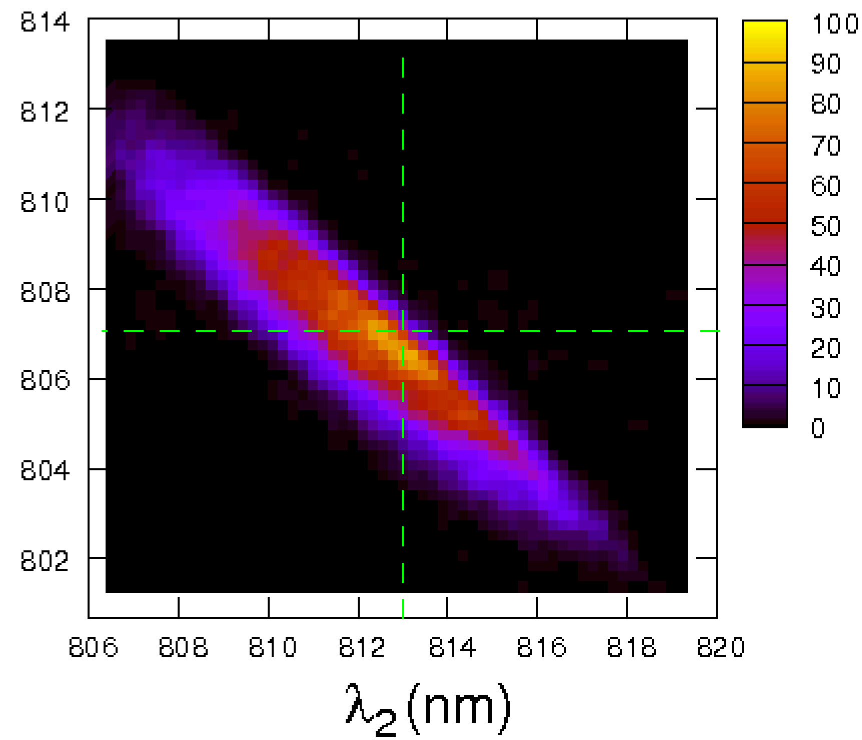
Limits of (this) pair source

- Spectral distinguishability of decay paths:

HV coincidences



VH coincidences



- Spectral width of pump around 0.7 nm (blame blue laser diode)

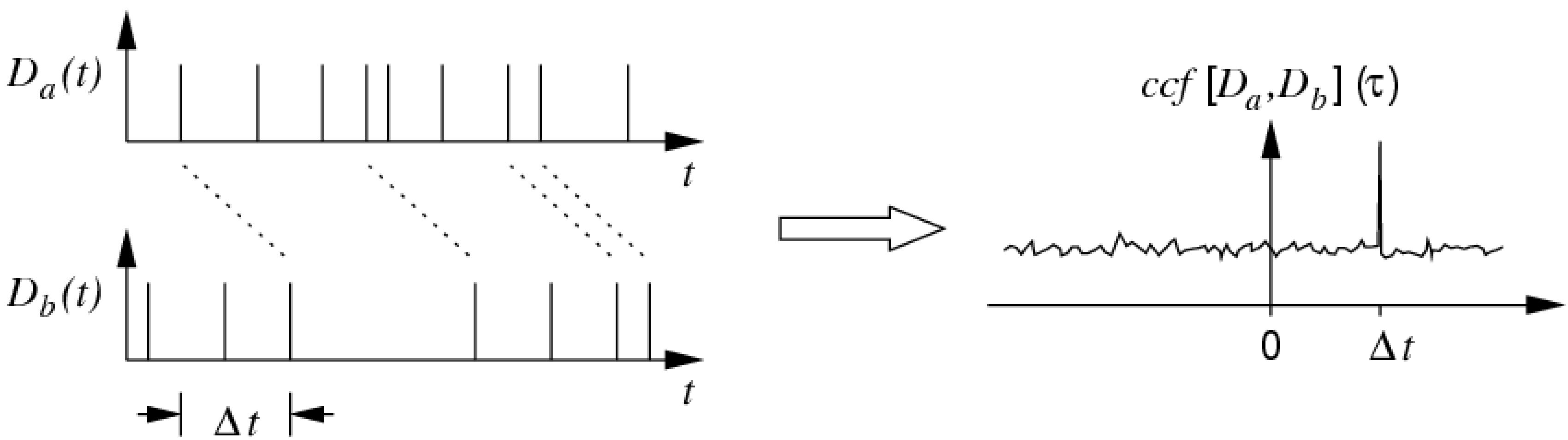
The Quantum Channel

- Use **free space optical** link:
  + simple polarization qubits
  + no cable infrastructure needed (mobile)
  + use Silicon photodetectors with
    higher QE (50%), lower background (10^{-7} ns^{-1})
    at the same time with “unselected” devices
    detectors can be always on
  - absorption in atmosphere (rain, birds)
  - propagation variation in air (scintillation)
  - HUGE background in daylight

- Alternatives: **optical fibers**
  + almost no background
  + existing telecom infrastructure
  + high availability of fiber
  - worse single photon detectors @ 1300nm

Synchronization

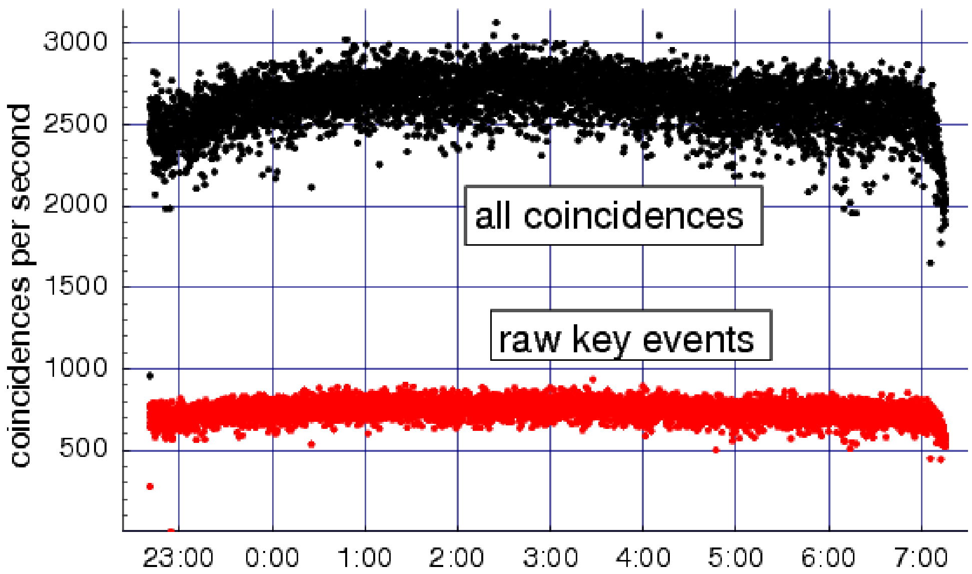
- Find initial time difference between two sides via cross correlation of detector event timings:

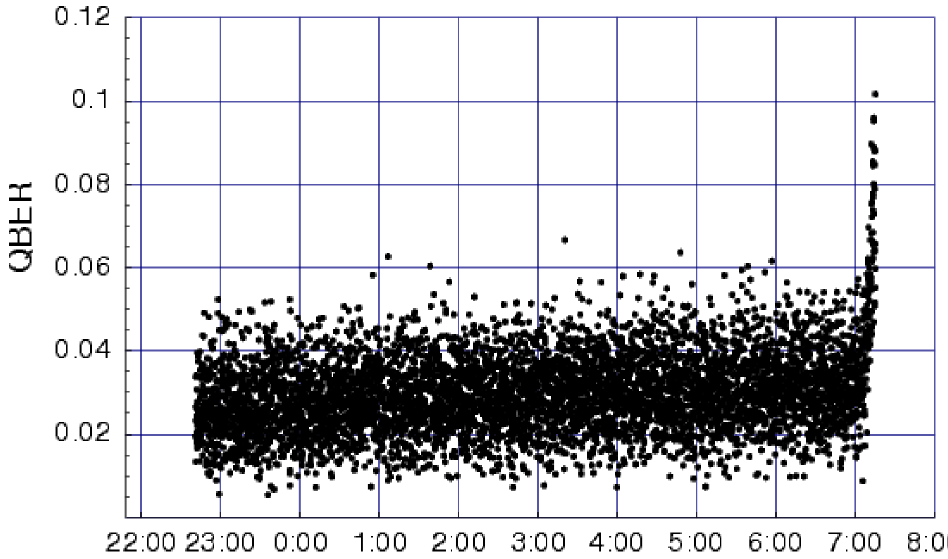


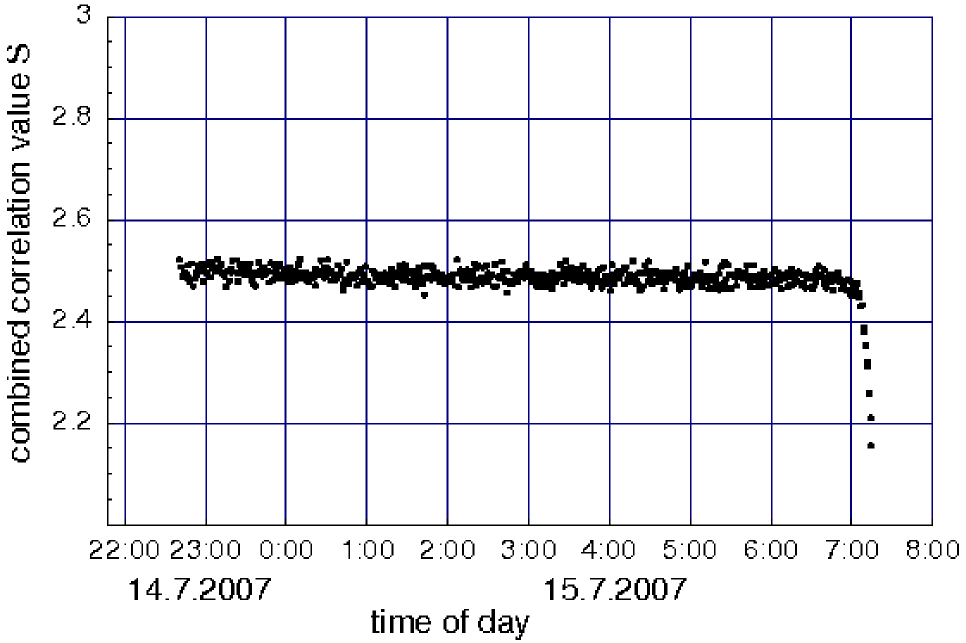
$$ccf\left[D_a(t),D_b(t)\right](\tau)=\int_{-\infty}^{\infty} D_a(t)\,D_b(t+\tau)\,dt$$

- Use clocks with low (10^{-9}) frequency difference over ~1s
- Tiered cross correlation technique for reasonable numerical effort to capture Δt ~500 msec with 2 ns resolution

No rain.....







- raw key rate: 610 bit/sec
  operation: 10h24'
  S=2.485±0.0005
  final key after EC/PA: 5.1E6 bits
- next: daylight operation, other protocols, finite key length.....