Status of R&D on Quantum communication and related R&D in Singapore

Christian Kurtsiefer

Updating Quantum Cryptography,
Akihabara Dec 1-2, 2008

Overview

NUS National University of Singapore

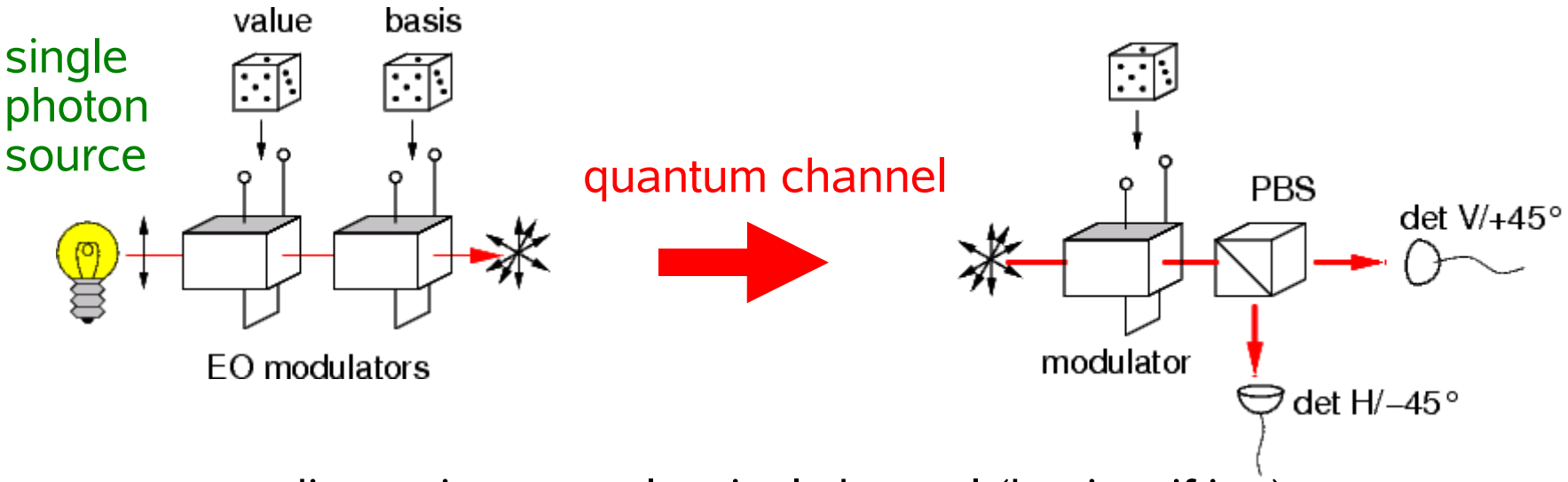
- BBM92 protocol advantages
- Free space transmission channel
- Daylight operation
- An E91 implementation with quantitative knowledge of information leakage
- Physical attack schemes

Related activities in Singapore (not scope of this presentation):

- Valerio Scarani: Finite key length related problems, implications of the device-independent idea on other fields in physics
- B.G. Englert & team: Singapore protocol, reference-frame free QKD schemes
- L.C. Kwek / Simon Benjamin: Concepts on optically networked atoms in cavities

BB84 protocol

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



- uses error fraction to estimate eavesdropper's knowledge

Estimate Eve's knowledge

NUS National University of Singapore

- Raw key with errors: N_r bits
- Quantum bit error ratio (QBER): η
- Number of bits leaked to an eavesdropper N_e

$$N_e = N_r\left(h(\eta)+h(\eta)\right)$$

possible knowledge of an eavesdropper due to measurements

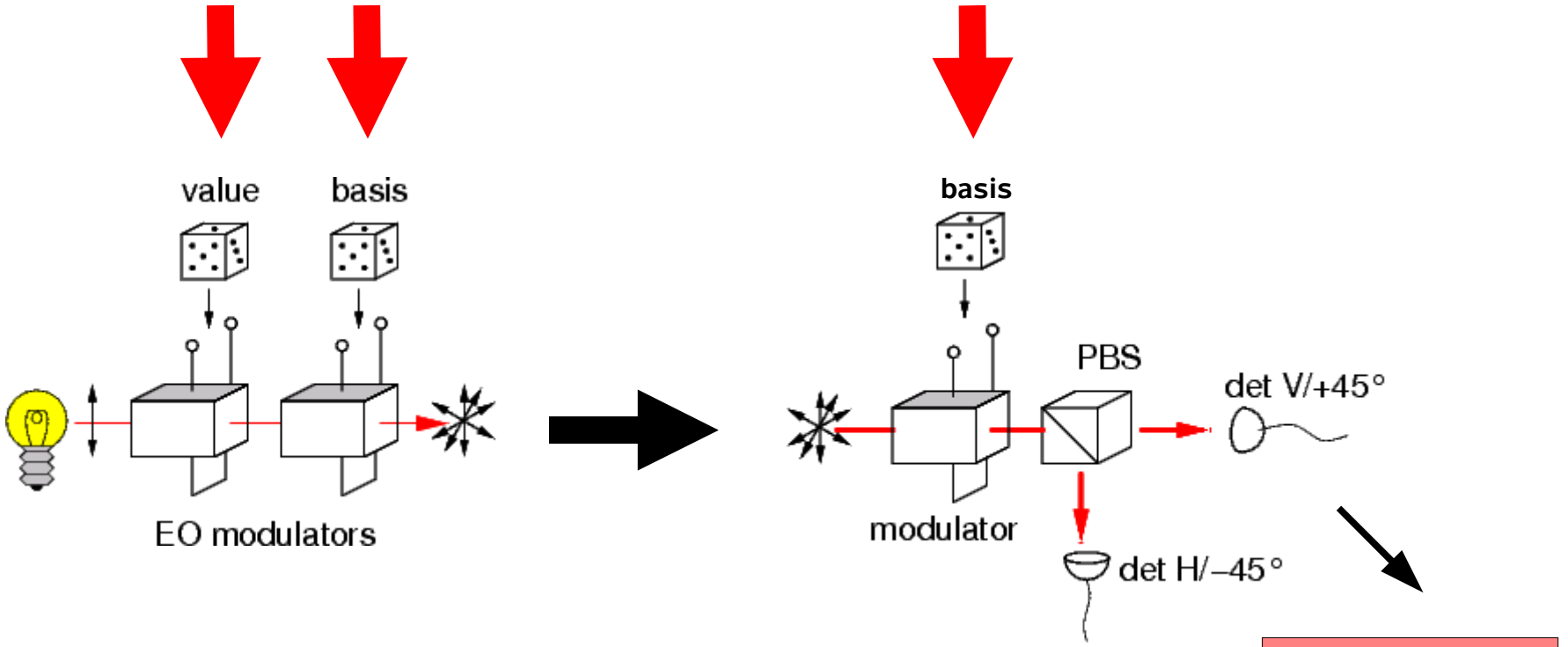
revealed in (optimal) error correction

binary entropy: $h(\eta)=-\eta\log_2\eta-(1-\eta)\log_2(1-\eta)$

for *infinite* key length and (!) single photons

A Prepare & Send problem:

...needs lots* of trusted random numbers!

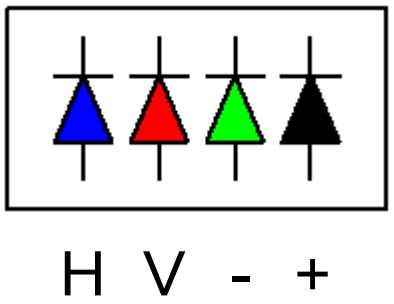


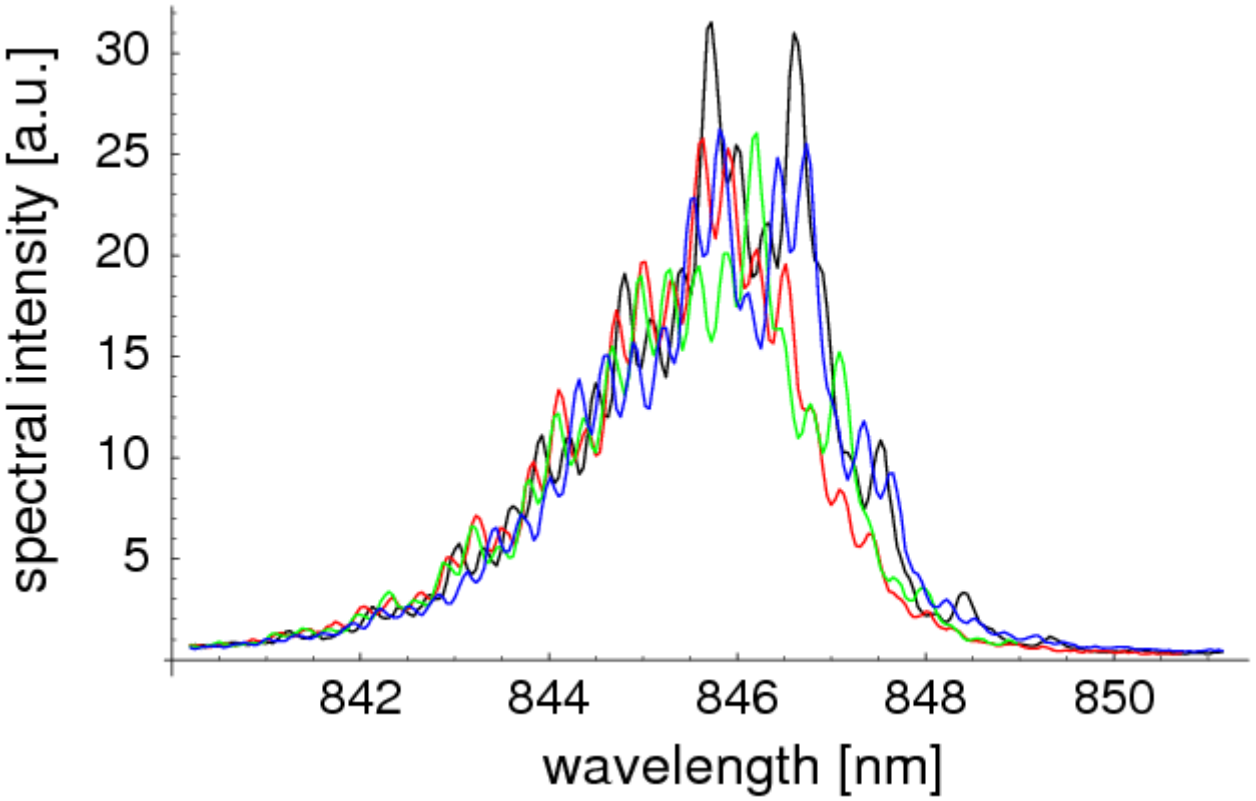
- Do you trust your **random numbers**?

*Mbit/sec for kbit/sec key

BB84: Spectral backdoor

Don't measure polarization, but e.g. color:
The Hilbert Space in your system is larger than it appears

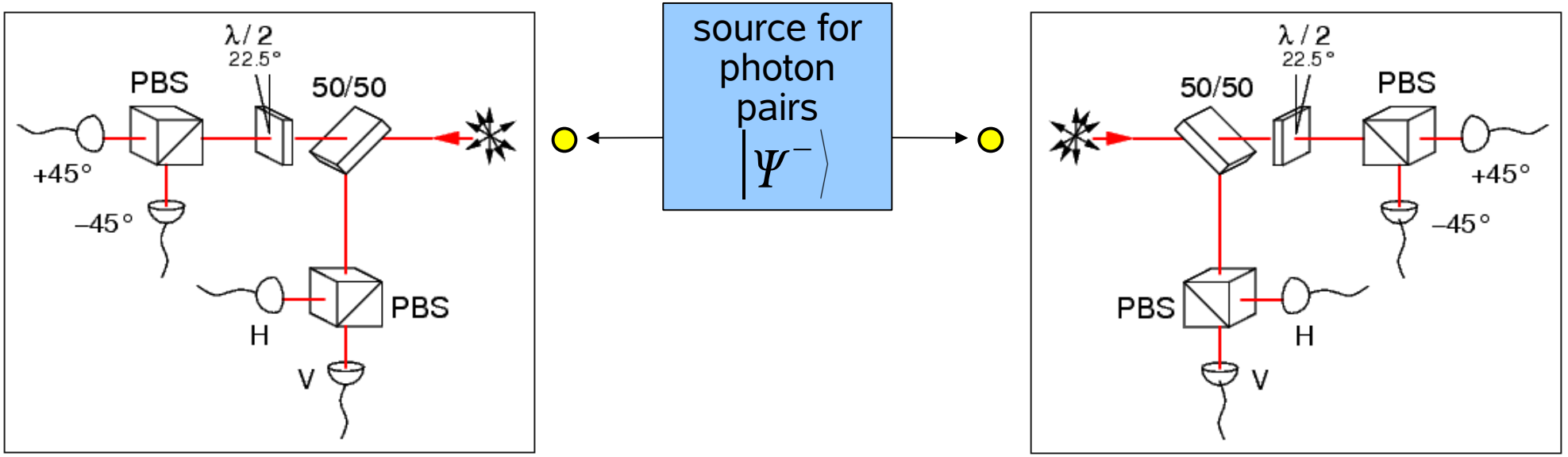




asymptotic
average
information
leakage: <2%

QKD with photon pairs: BBM92

Quantum correlations & measurements on both sides



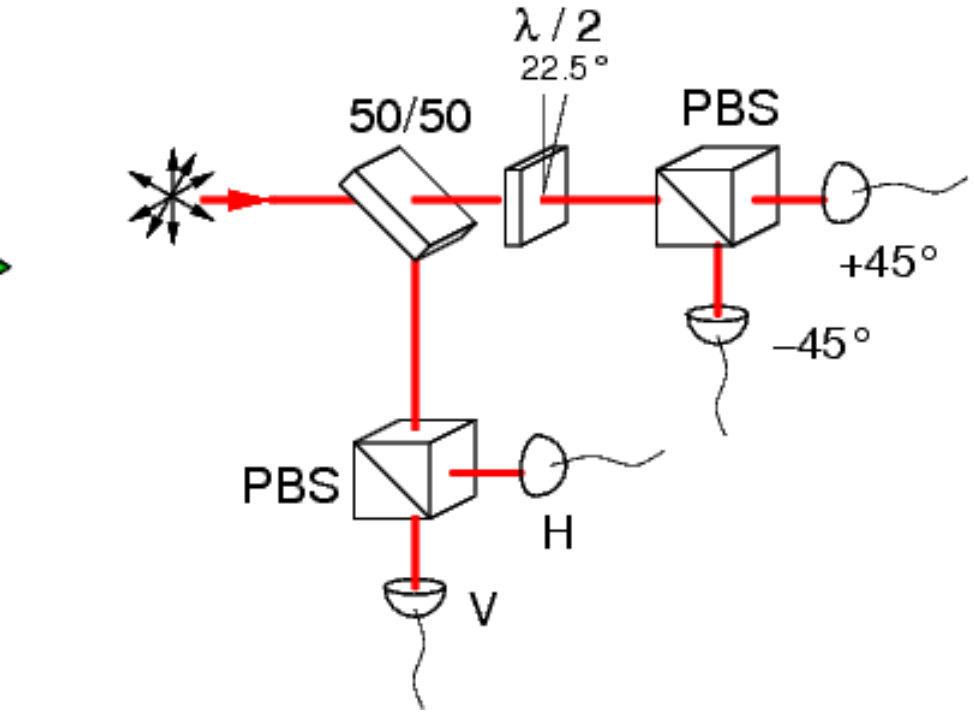
public discussion (sifting, key gen / state estimation)

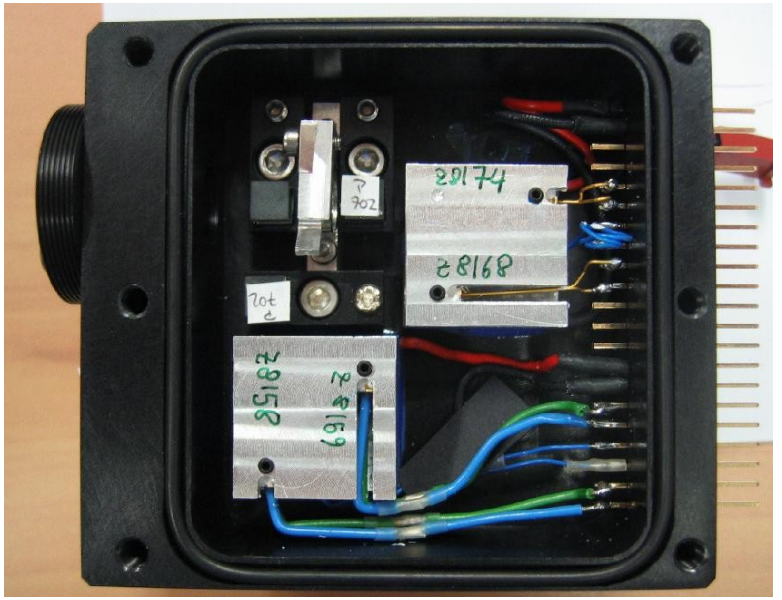
error correction, privacy amplification

- no trusted random numbers for key
- direct use of quantum randomness for measurement basis

Polarization measurement

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

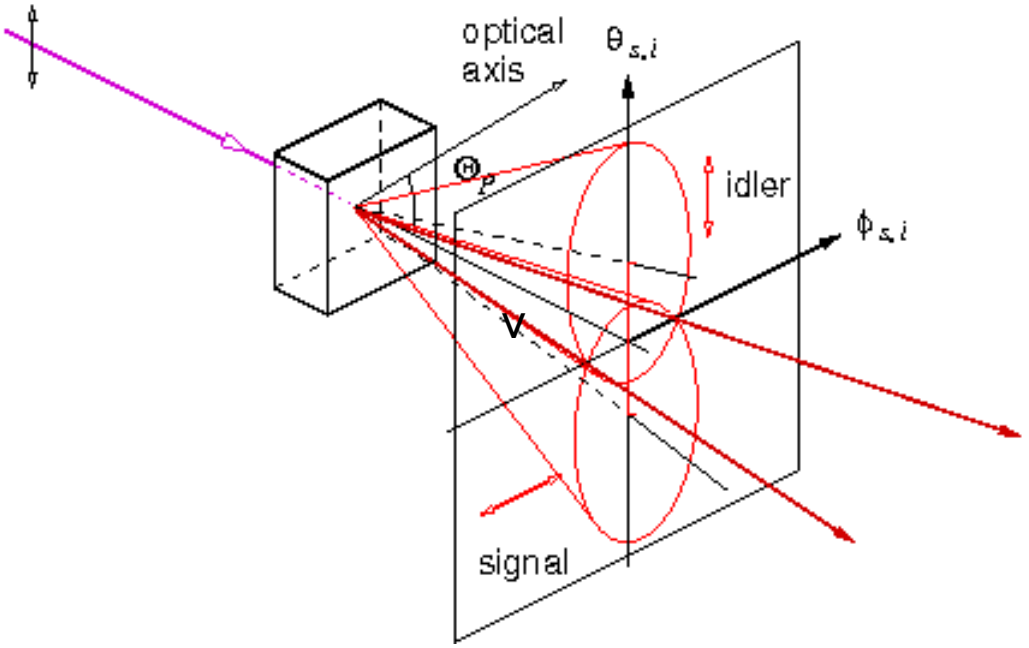




J.G. Rarity, P.C.M. Owens, P.R. Tapster,
J. Mod. Opt. ***41****, 2345 (1994)*

Entangled photon sources

- Use non-collinear type-II parametric down conversion



two indistinguishable decay paths lead to

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

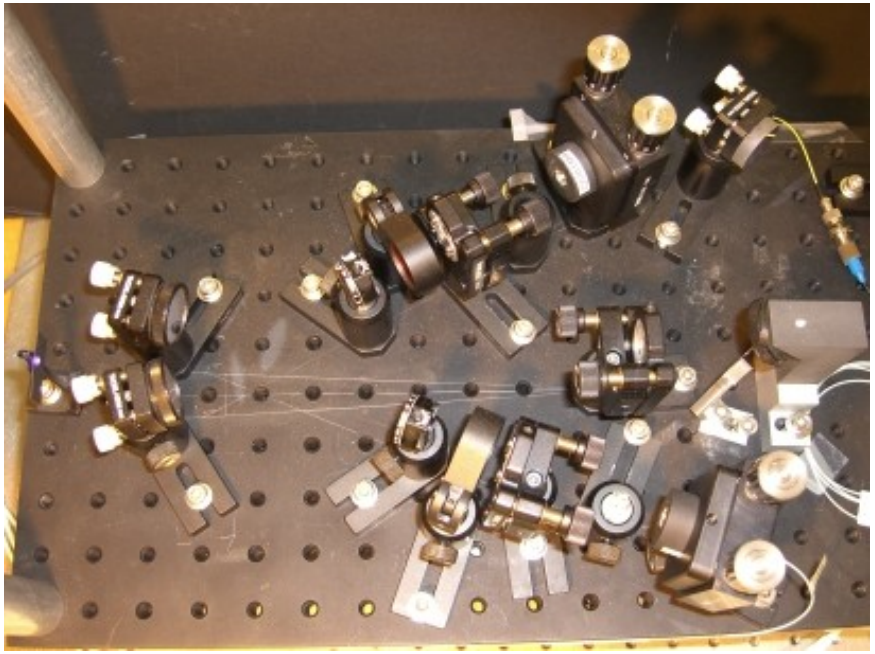
$$= \frac{1}{\sqrt{2}}\left(|+-\rangle - |-+\rangle\right)$$

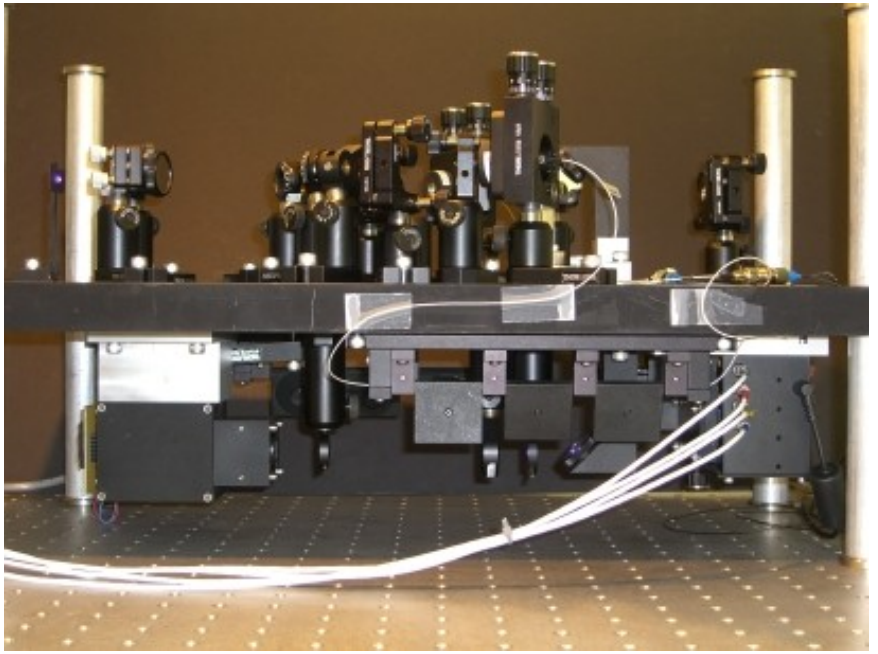
*P.G. Kwiat et al., PRL **75**, 4337 (1995)*

Practical pair source

NUS National University of Singapore

Blue diode-laser as pump source, BBO as nonlinear crystal

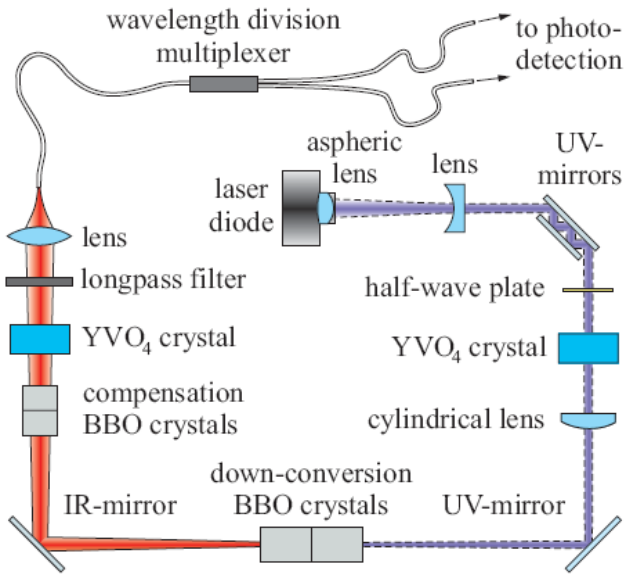




- 24,000 s^{-1} detected pairs from 40 mW pump @ 407nm in single mode fibers at 810/818 nm, 2mm BBO crystal
- polarization correlation visibility in 45° basis: 92%

(Much better pair sources)

Colinear down conversion, periodically poled materials



F. Wong et al., MIT

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

P. Trojek, H. Weinfurter, arxiv:0804:3799

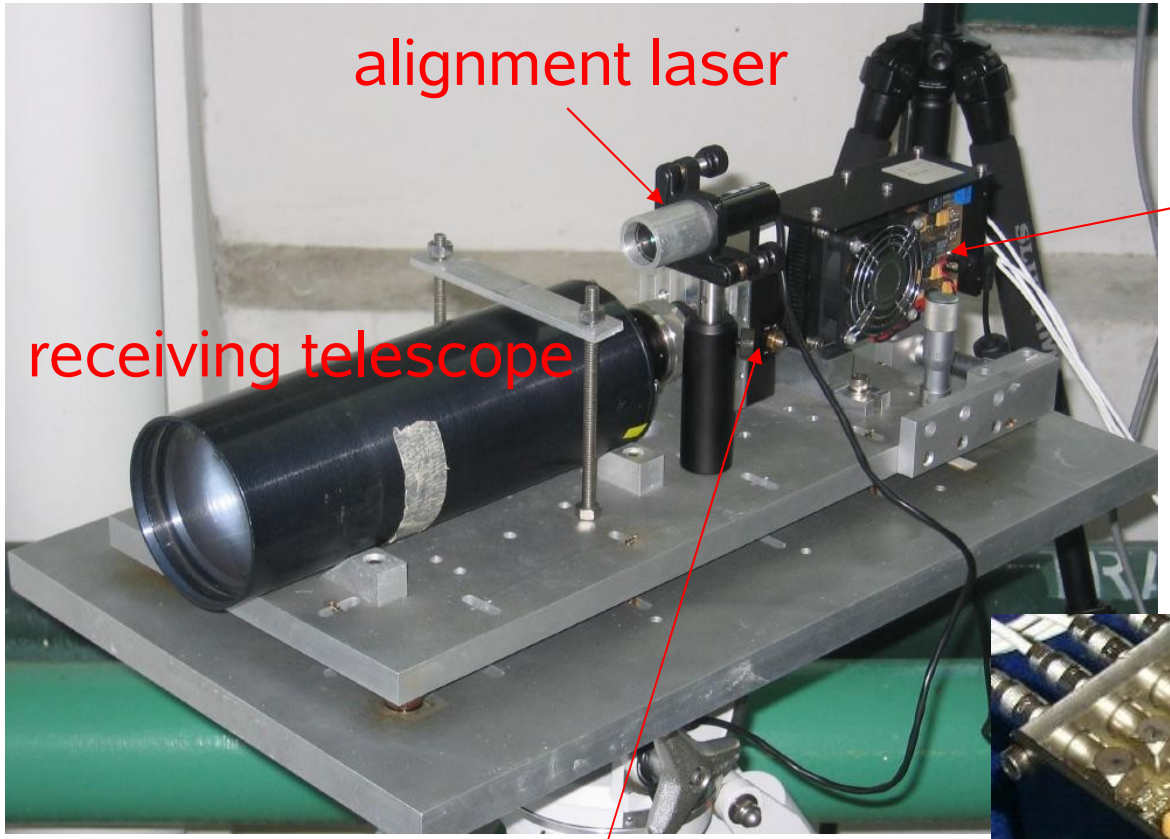
Geneva group: waveguide sources

- Up to 1000 times brighter than non-colinear sources
- Polarization correlation visibility in 45° basis > 99%

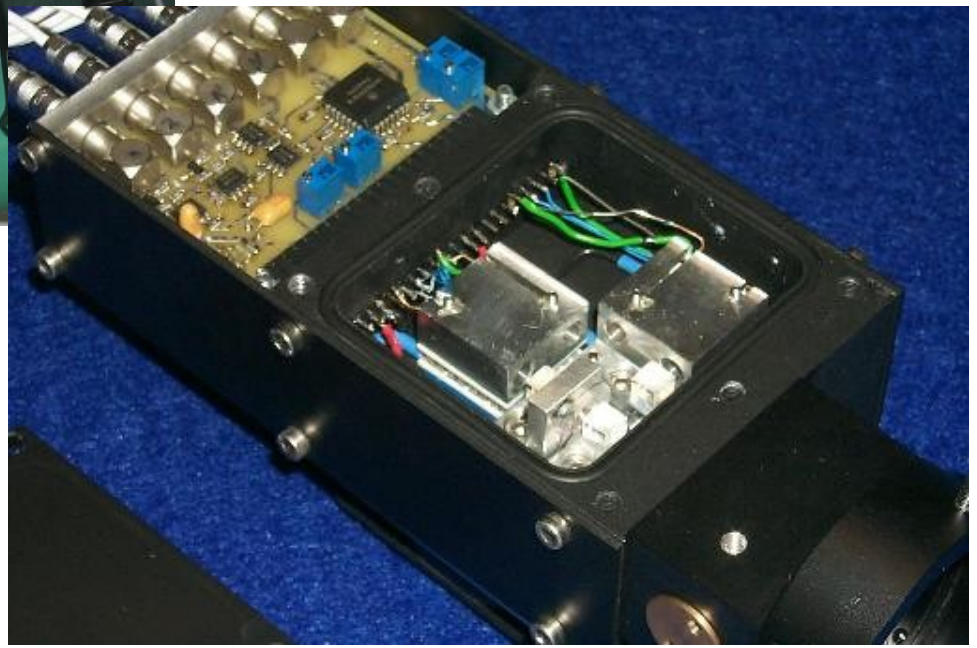
NUS campus test range

NUS National University of Singapore

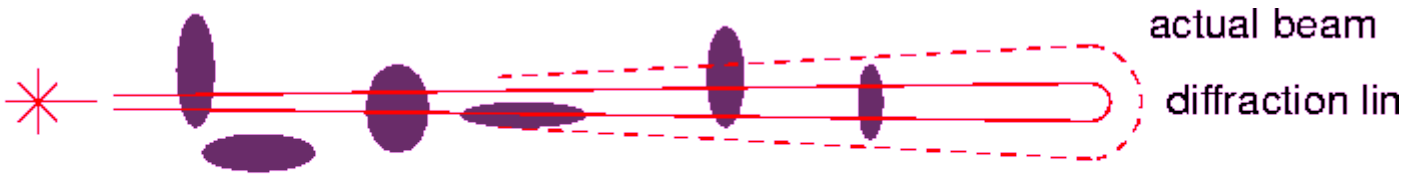
Receiver unit



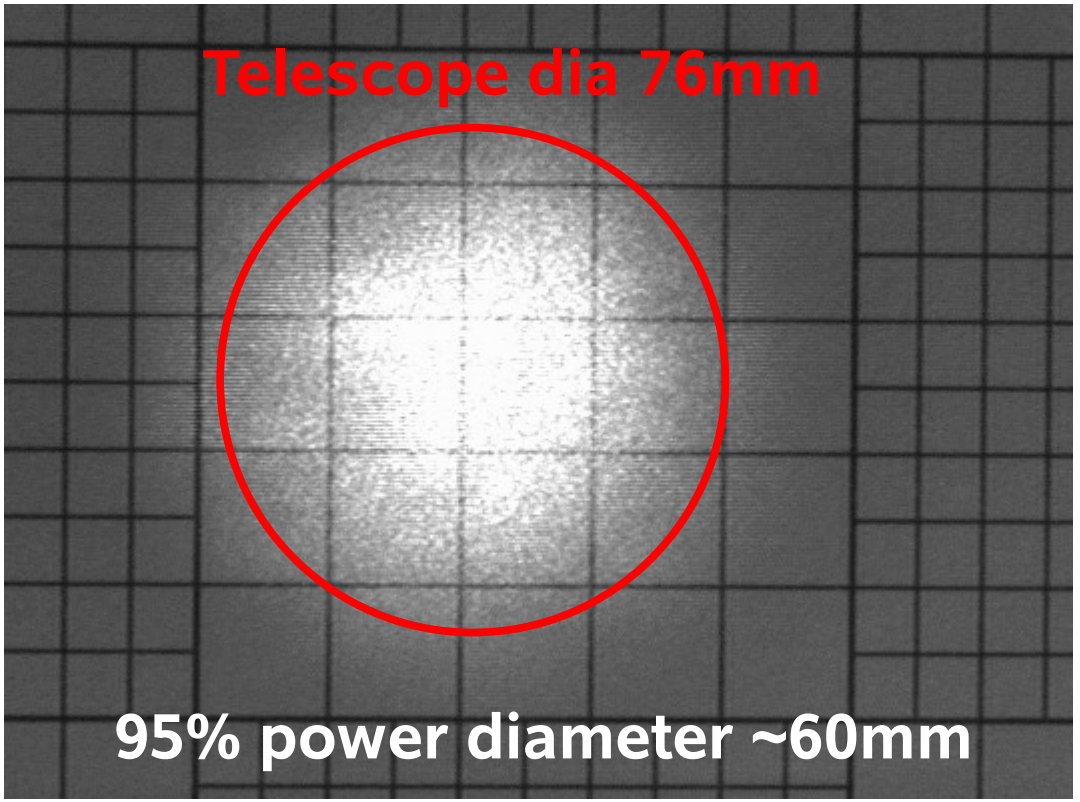
polarization analyzer
passively quenched
Silicon APD
- QE ~50%
~1000s^{-1} dark cnt rate



Scintillation in atmosphere

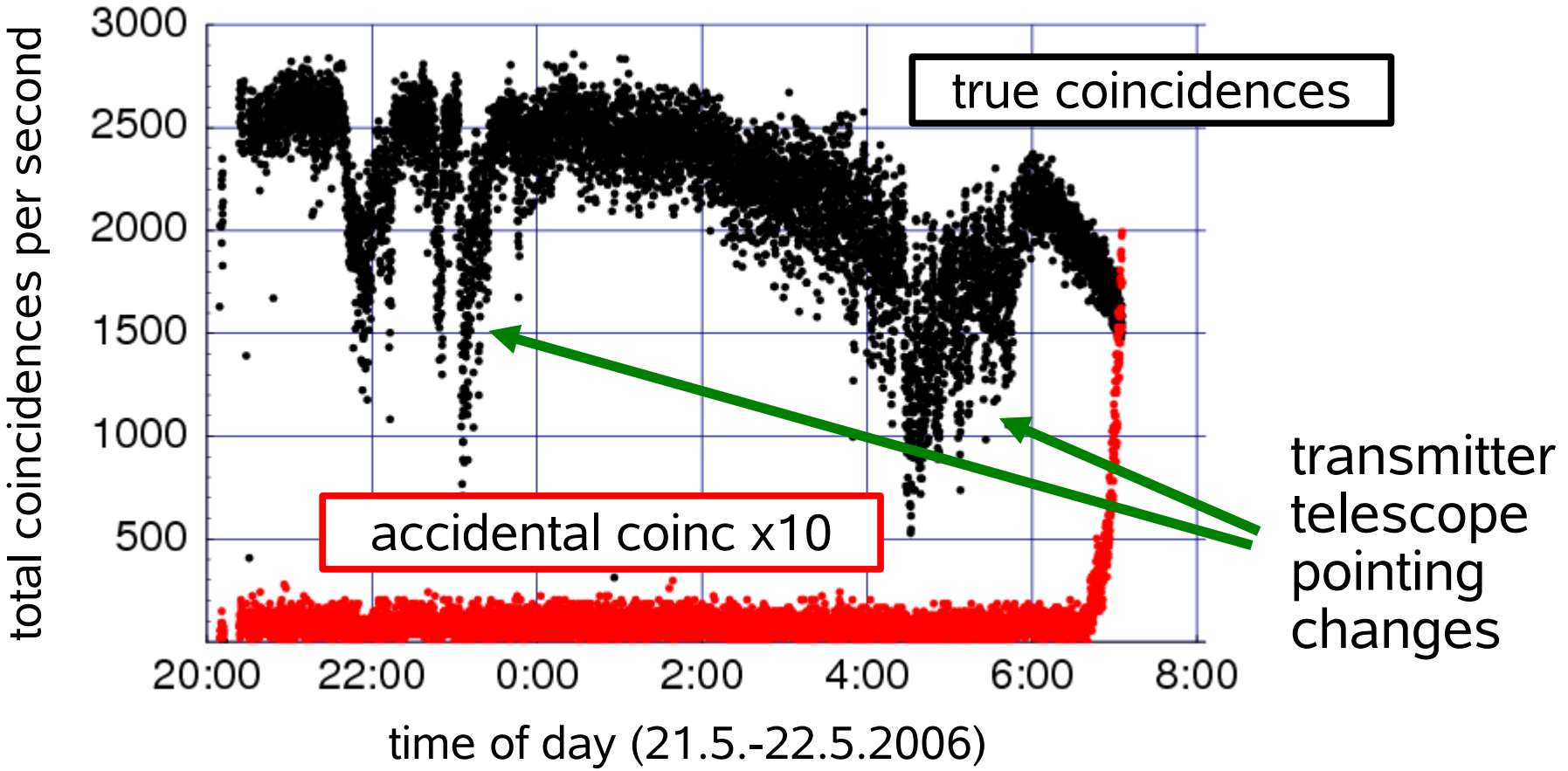


(40 mm FWHM)



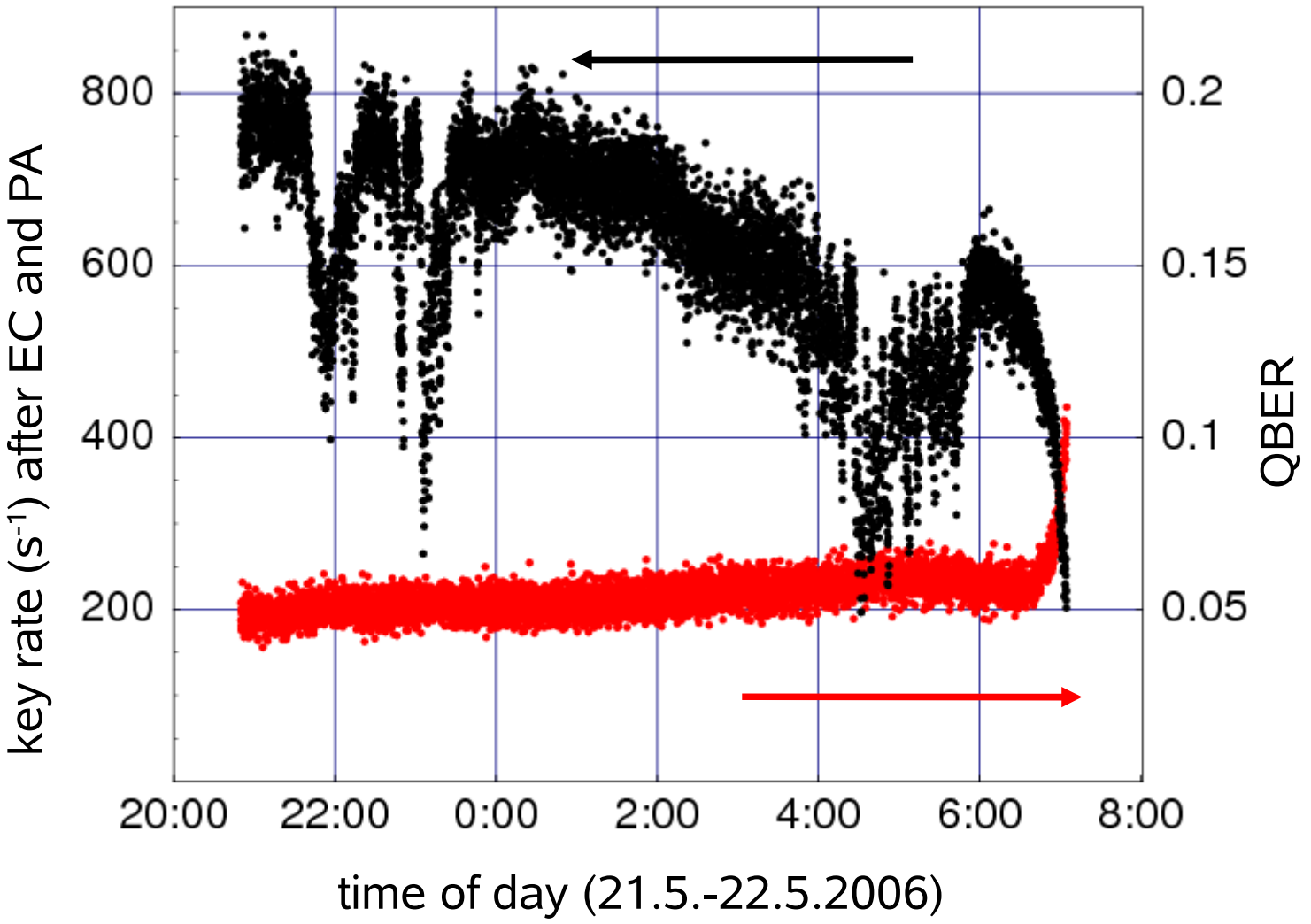
Experimental results I....

Identified raw coincidences between close and remote receiver



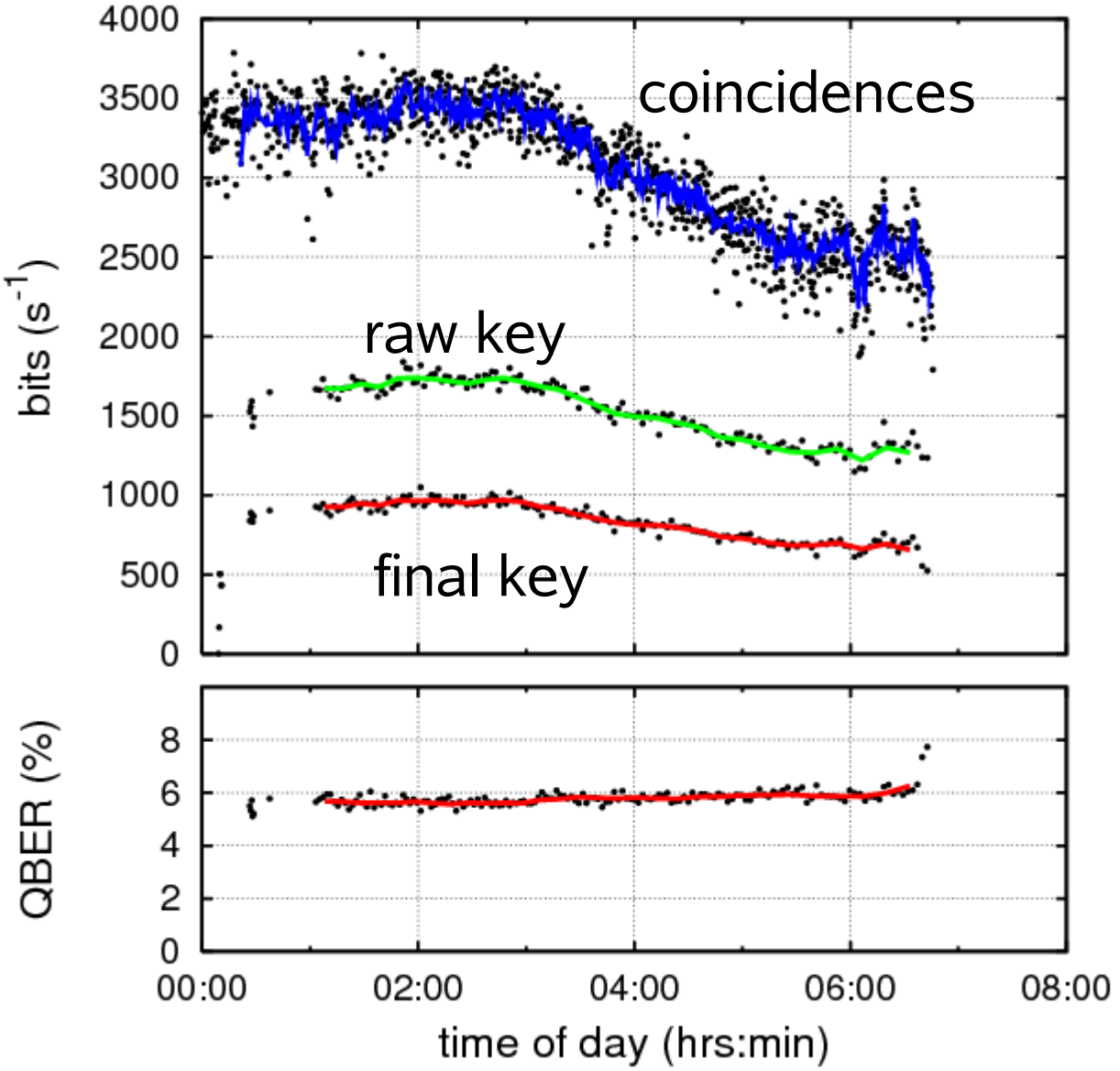
(with interference filter 5nm FWHM, 50% peak transmission)

....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

No interference filter



(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)

Daylight also can?

NUS National University of Singapore

Background light issues

NUS National University of Singapore

- Previous work: Los Alamos

  Faint coherent pulses: R. Hughes et al., J. Mod. Opt. ***47****, 549 (2000)*

- detectors may die

- detector saturation: dead time $\tau_d \approx 1\mu s$ for passive quenching

  loss of useful signal $$r' = r \frac{1}{1 + r\tau_d}$$

- accidental coincidences increase QBER:

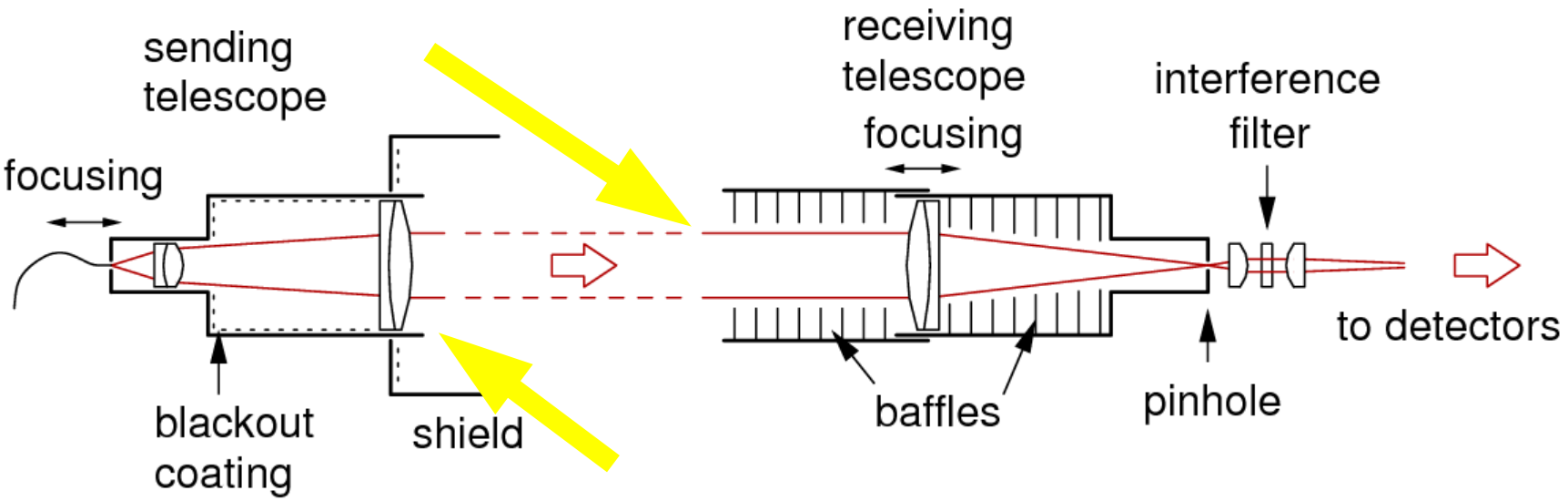
$$q_t = \frac{1}{r'_a + r'_s}\left(q_i r'_s + \frac{1}{2} r'_a\right)$$

Reducing background

- use good spatial, spectral and temporal filtering

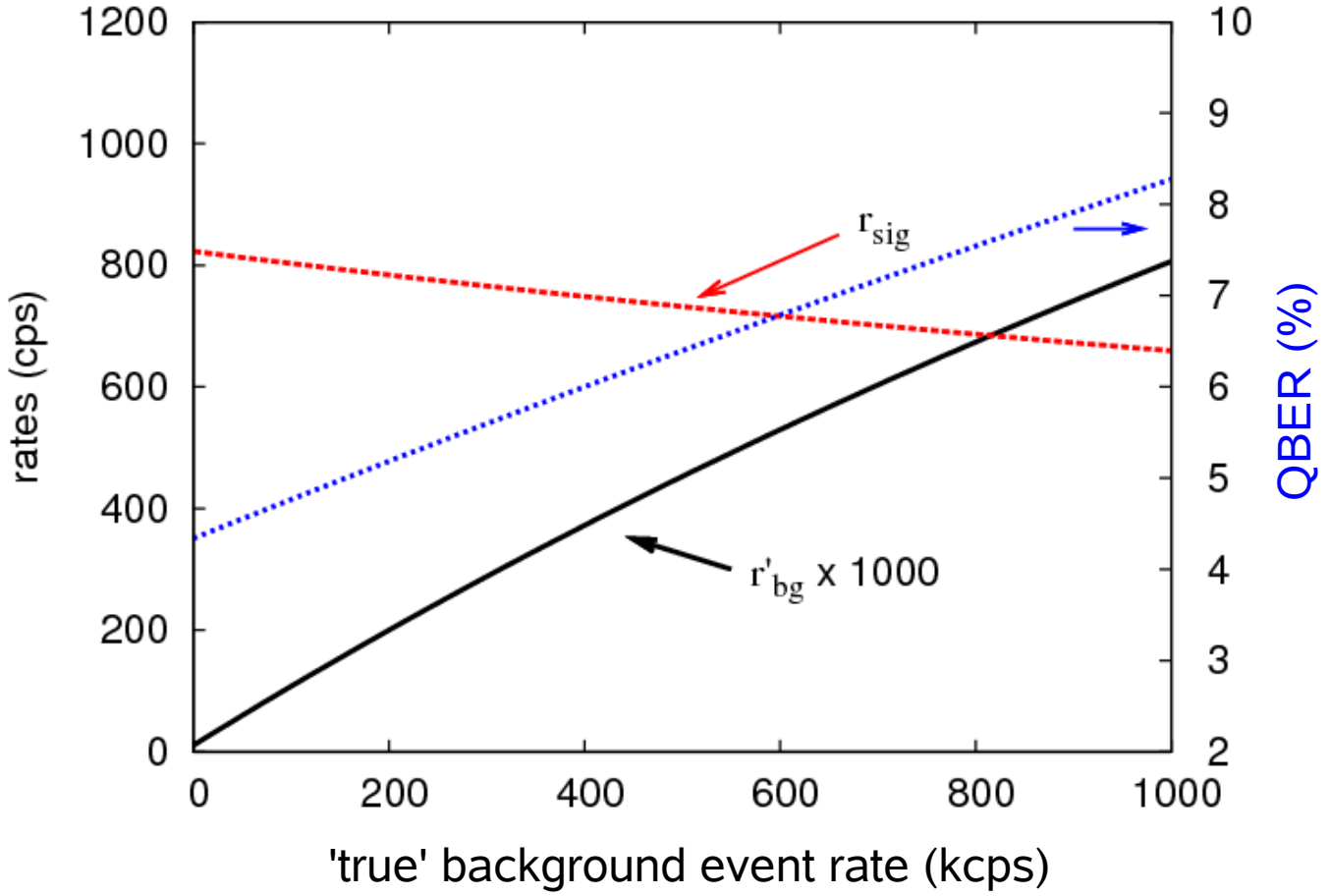
  spatial: 100 µrad acceptance angle
  spectral: 6.7 nm wide interference filter

- avoid excessive scattering in optical path



Realistic numbers

- intrinsic QBER: 4.3%, coincidence time τc = 2 ns, detector τd = 1 μs



- background does not kill the QBER
- detector saturation is limiting us!

Setup on a 350m stretch...

NUS National University of Singapore

transmitter:

Experimental results

NUS National University of Singapore

total detection rate at receiver (cps)

total 'local' detector rate at source (cps)

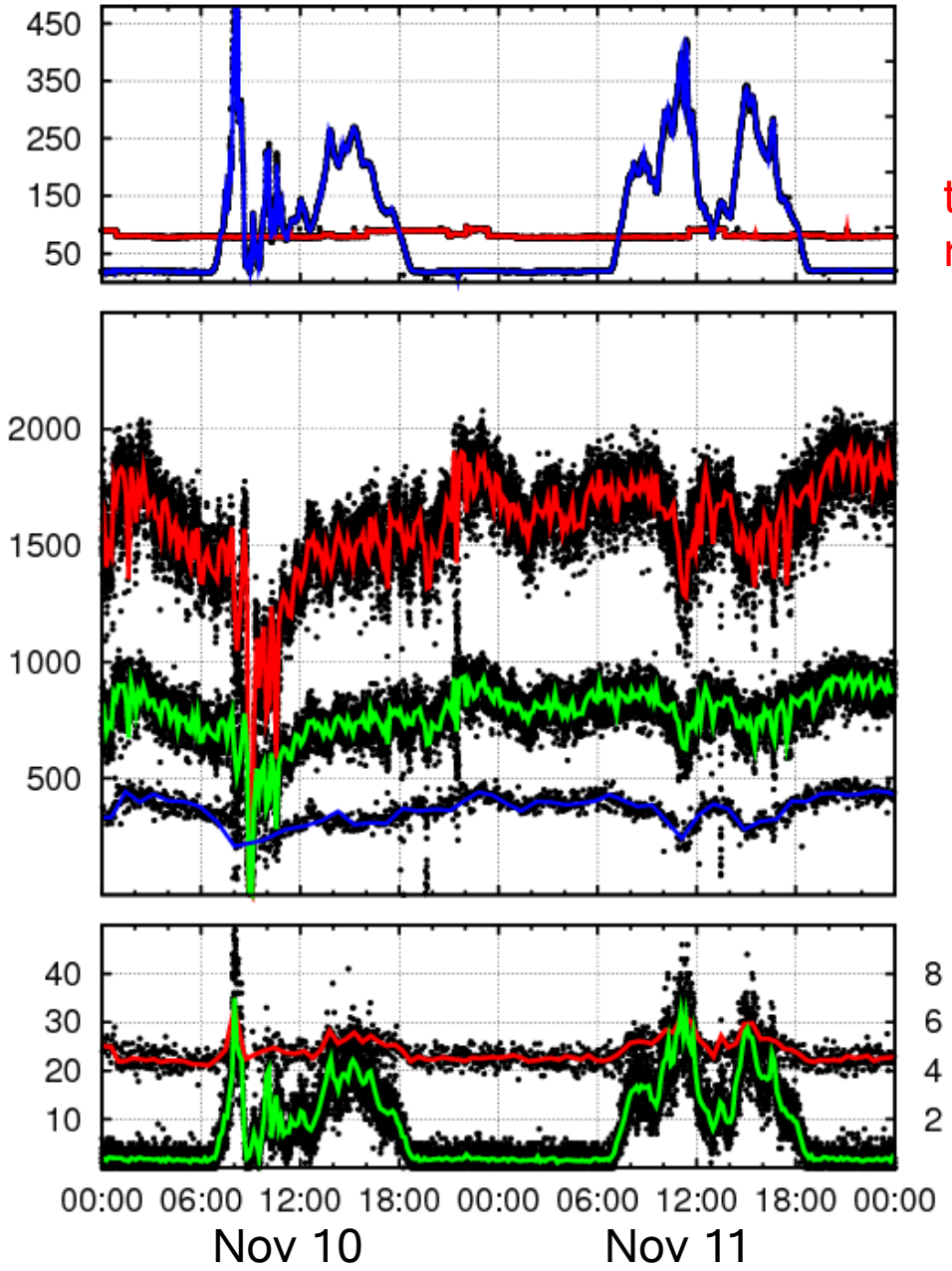
coincidences (cps)

raw key rate (s^{-1})

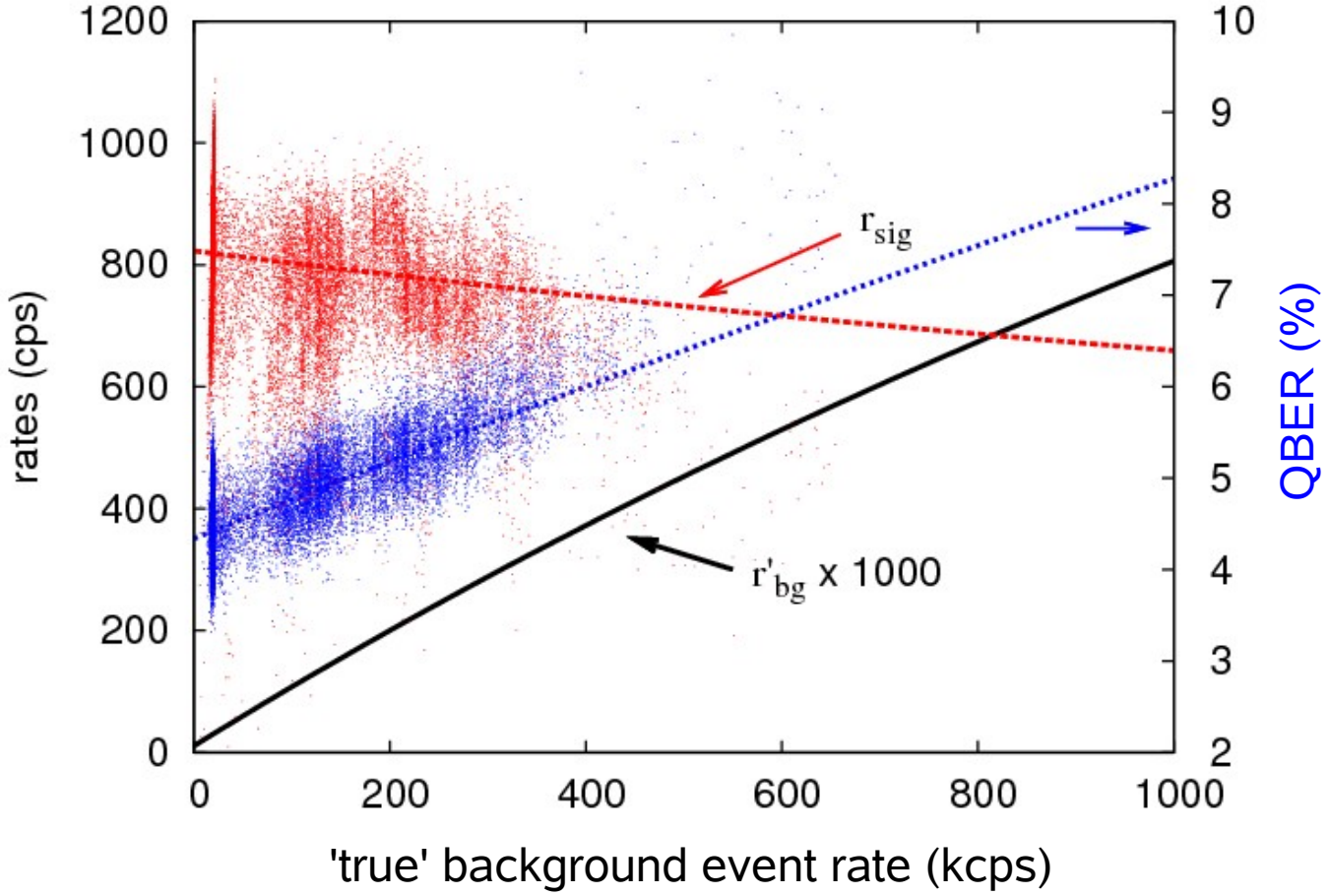
key rate after error correction (s^{-1})

accidental coincidence rate r_a (cps)

QBER (%)



Extract background influence

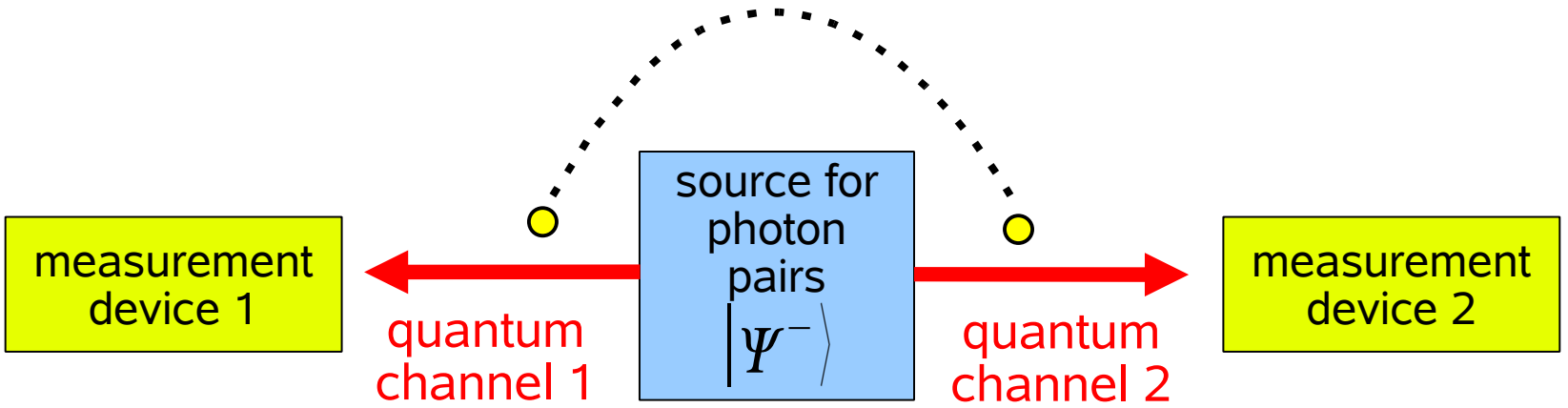


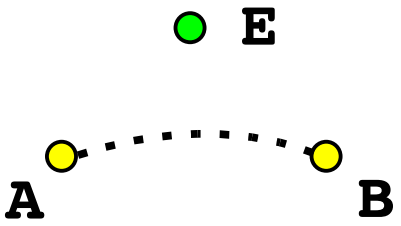
- continuous key generation over free-space link in daytime:

Can, lah!

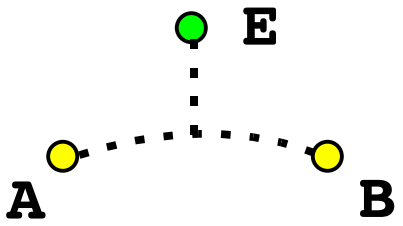
Entanglement based protocols

Find eavesdropper not via errors, but via testing entanglement:
Ekert91 – type and tomographic protocols



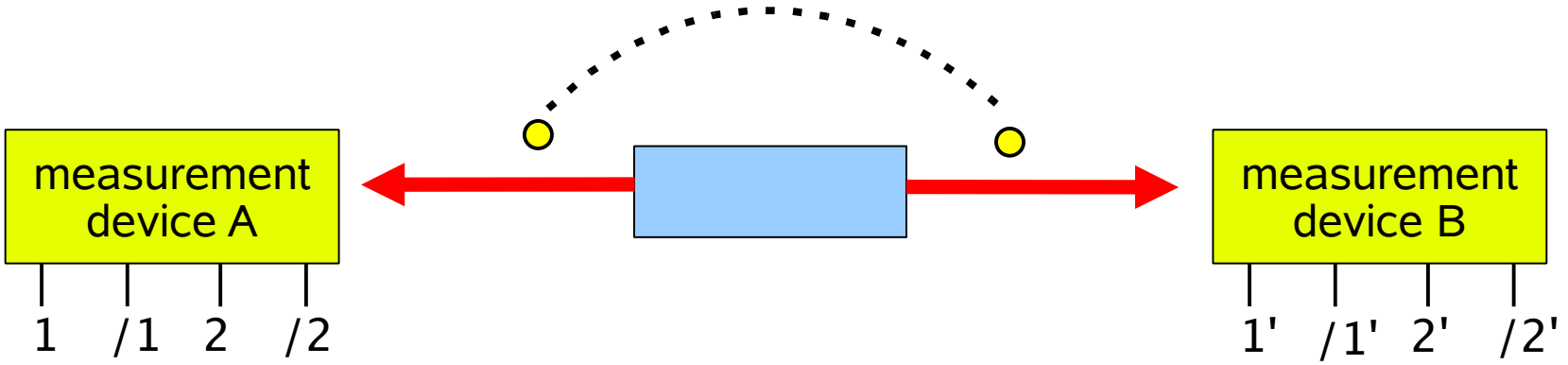


maximal entanglement
between **A** and **B**



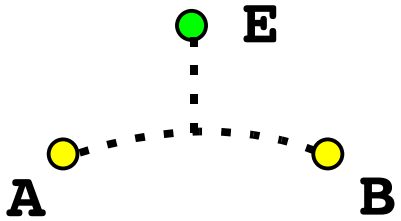
reduced entanglement
between **A** and **B**

Bell inequality I



Correlation between setting i, j: $$E(i,j) := \frac{n(i,j)+n(\bar{i},\bar{j})-n(i,\bar{j})-n(\bar{i},j)}{n(i,j)+n(\bar{i},\bar{j})+n(i,\bar{j})+n(\bar{i},j)}$$

combined correlation function: $$S := E(1,1')+E(1,2')+E(2,1')-E(2,2')$$

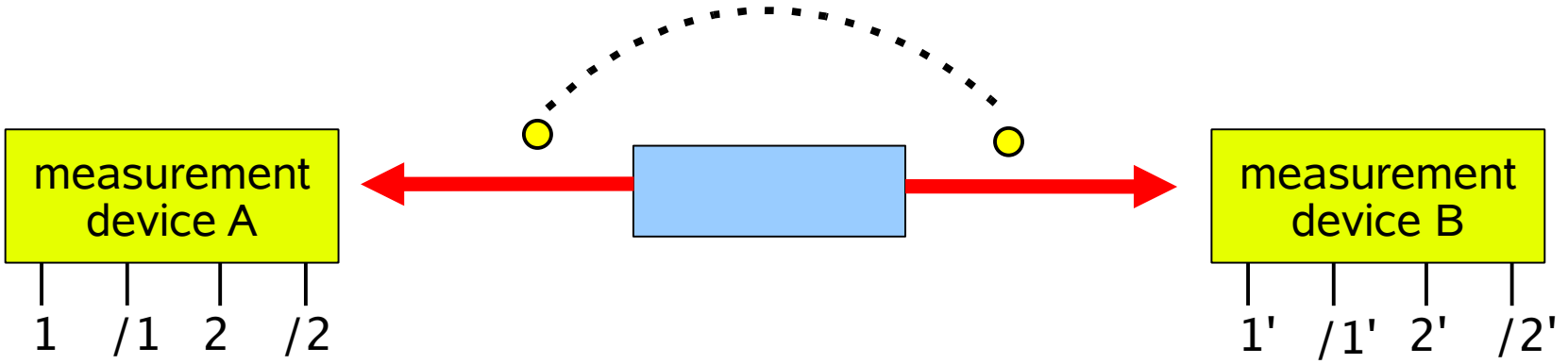


If there is a local hidden parameter λ
(= knowledge of **E**) governing the measurement outcomes of **A** and **B**, then:

$$|S| \leq 2$$

To some extent: T. Jennewein et al., Phys. Rev. Lett. ***84****, 4729 (2000)*

Bell inequality II



For proper settings 1, 2, 1', 2' and state $|\Psi^-\rangle$: $S = \pm 2\sqrt{2}$

- Estimate quantitatively the knowledge of Eve of raw key between A and B from S:

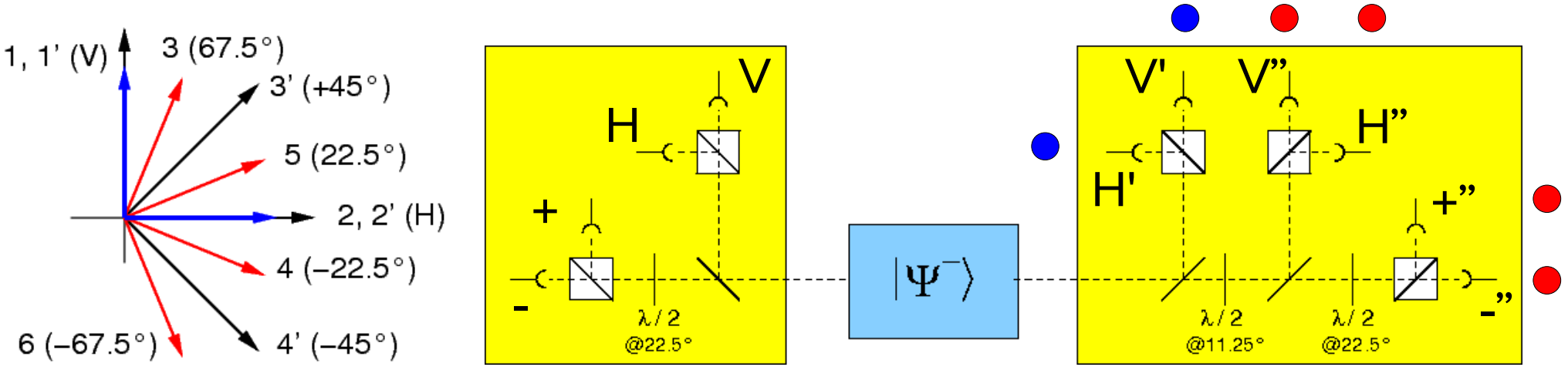
$$I_E(S) = h\left(1 + \frac{\sqrt{S^2/4 - 1}}{2}\right)$$

- Assume “fair sampling” between key measurement and Bell test
- No fingerprint problems of photons due to side channels

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

E91 Implementation

- use almost same kit:



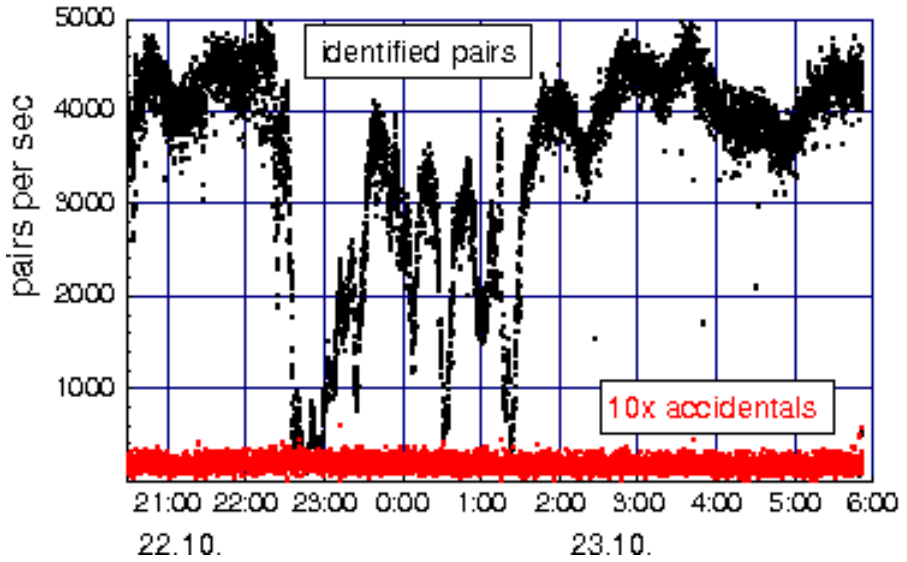
- {H,V; H',V'} coincidences → key generation
- {H,V,+,-;H",V",+",-"} coincidences → CHSH Bell test
- low QBER with existing simple source

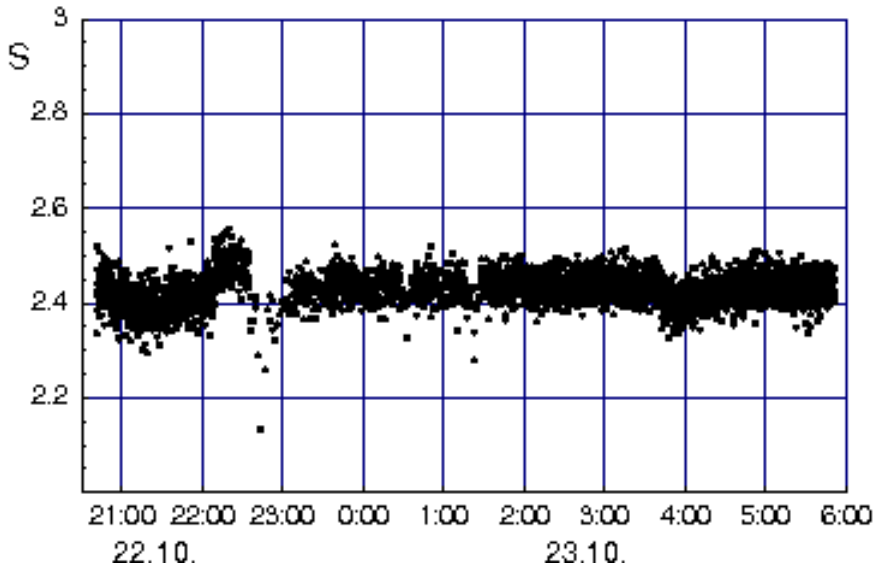
*A. Ling, M. Peloso, I. Marcikic, A. Lamas-Linares, V. Scarani, C.K., Phys. Rev. A **78**, 020301(2008)*

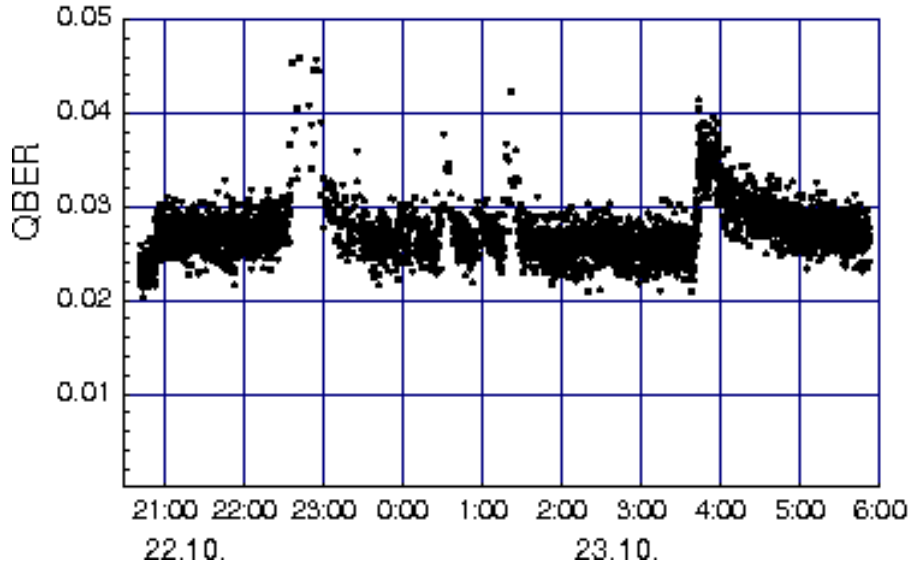
Field results (1.4km range)

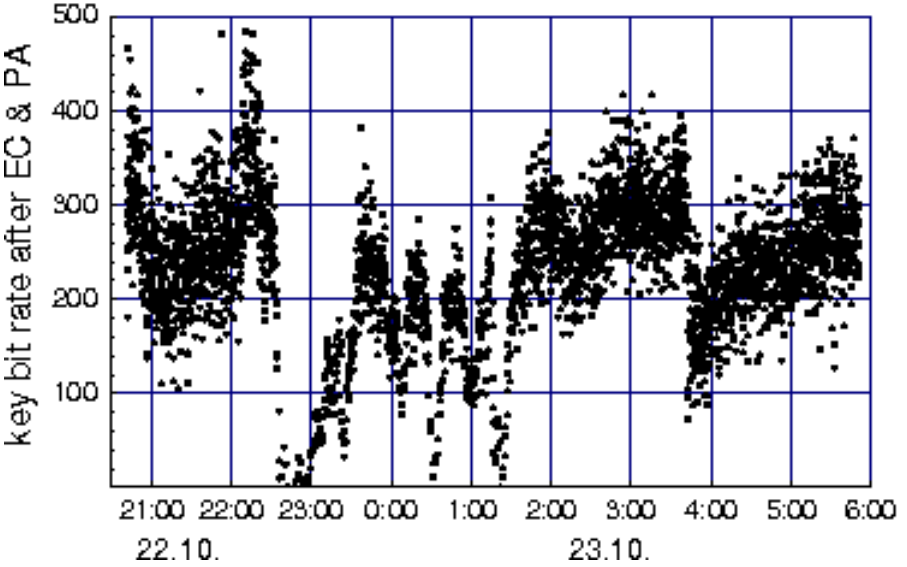
NUS National University of Singapore

- typical data run (with tropical rainfall inbetween)

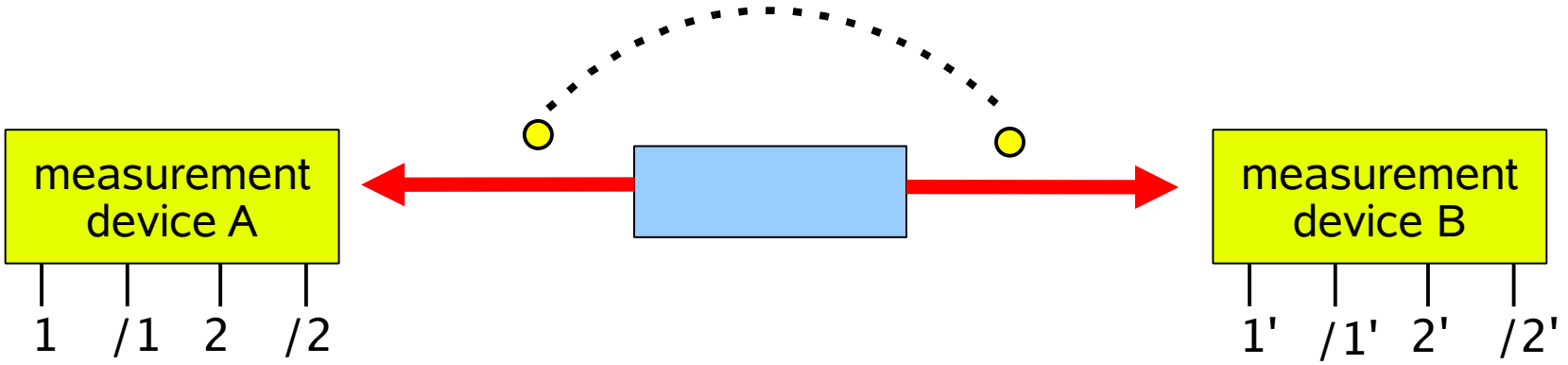








Device-independent QKD?



- For non-lossy detectors and a measurement basis decision at "free will" of the observers:

  No assumptions on devices and source is necessary to get an upper bound for eavesdropping!

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

Compare technical specs?

NUS National University of Singapore

- 'clockless' QKD scheme, uses timestamping only with resolution nominally 125 ps (efficient sifting)
- Photodetection rates ~1 M cps (detectors), up to 6 Mcps for electronics
- synchronization entirely software based (no specific HW channel)
- no dedicated classical channel (wireless or other TCP link will do)
- form factors: Reaching consumer grade complexity?

Lean setup

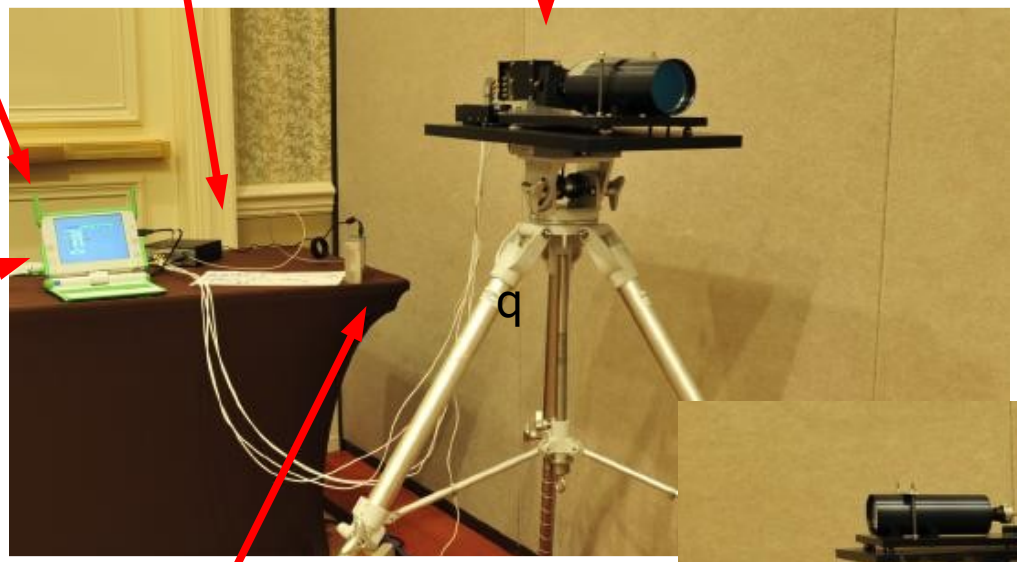
NUS National University of Singapore

classical channel WiFi

timestamp unit 10 W

receiver 15 W

- Demos at 24C3, Berlin 2007, Black Hat / DEFCON16, 2008

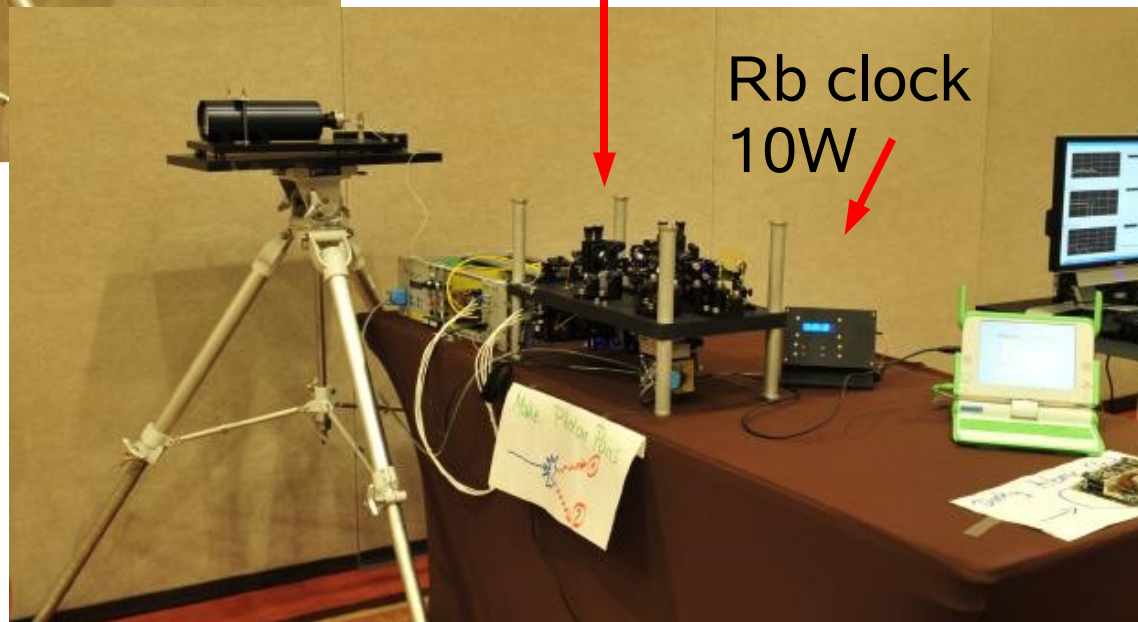


PC (olpc) 2 W

Rb clock 8 W (ebay, $200)

pair source ~15W
detectors 15W

Rb clock 10W



Field usage, open source

NUS National University of Singapore

PDC pair source & sender

- System gets simpler and more robust, low power consumption (<65W)

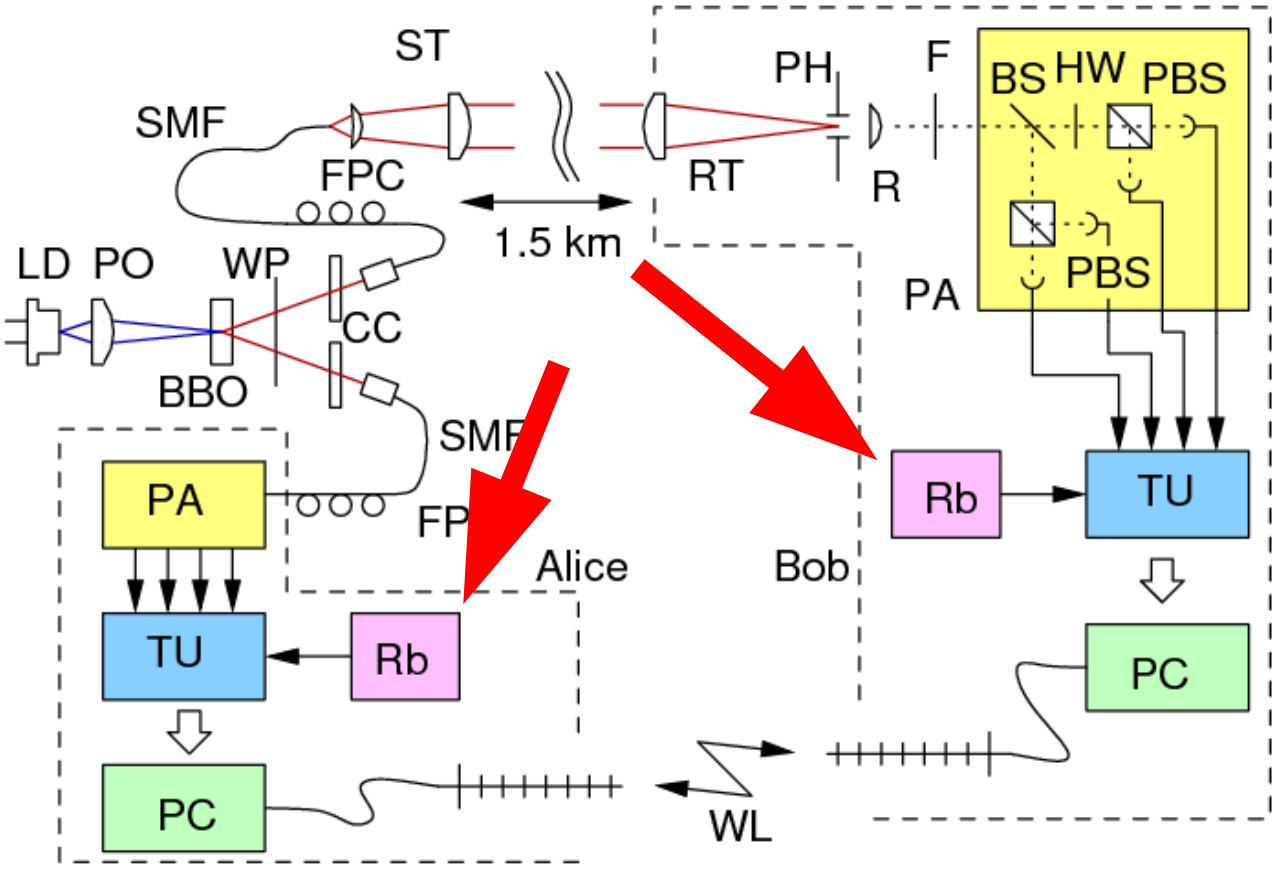
receiving side

- Software is open source (GPLv2): http://code.google.com/p/qcrypto

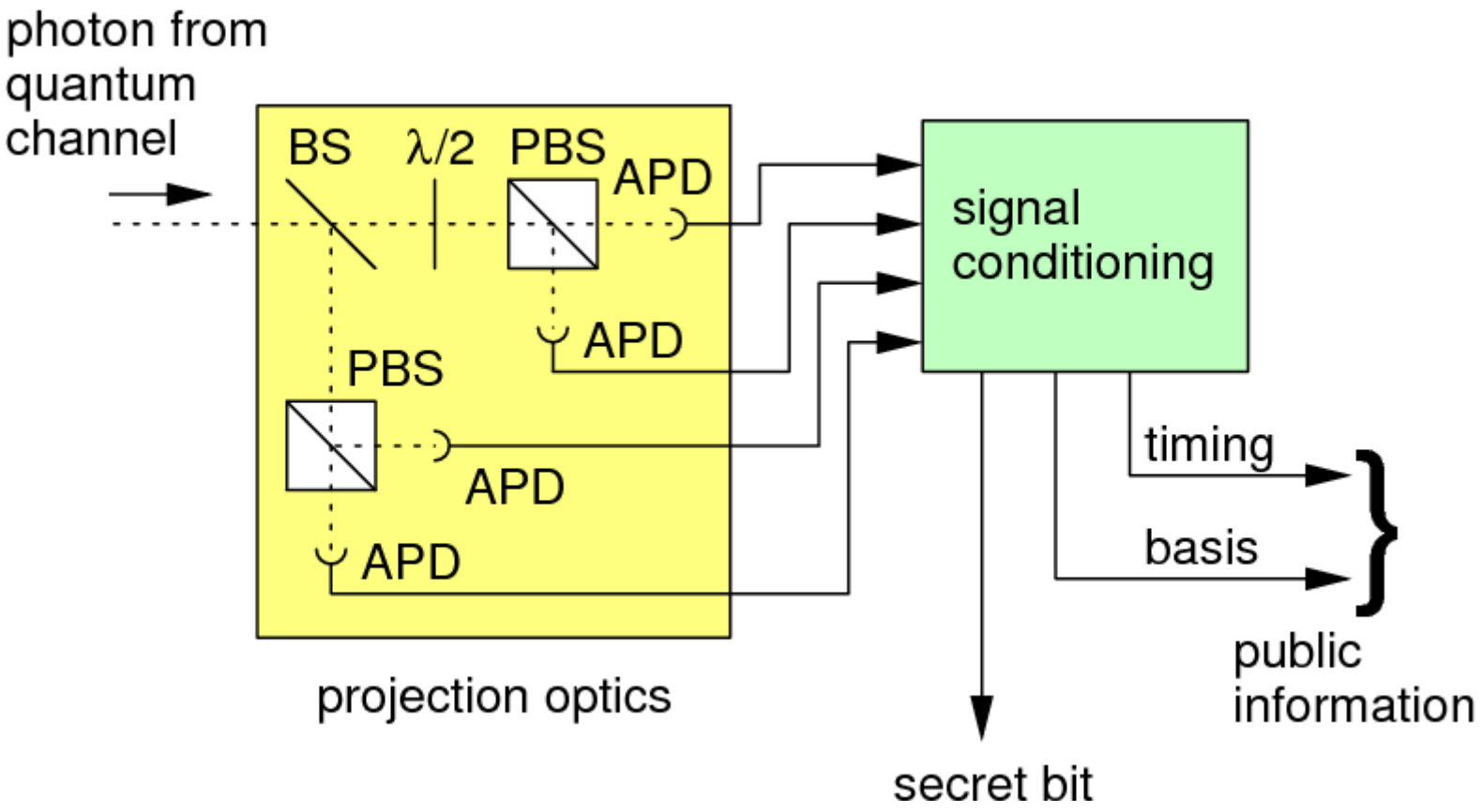
  Open hardware under way

On the more technical side....

- remove need for good reference clocks, we can initialize and maintain coincidence identification with standard crystal oscillators with $\Delta f / f \approx 10^{-4}$

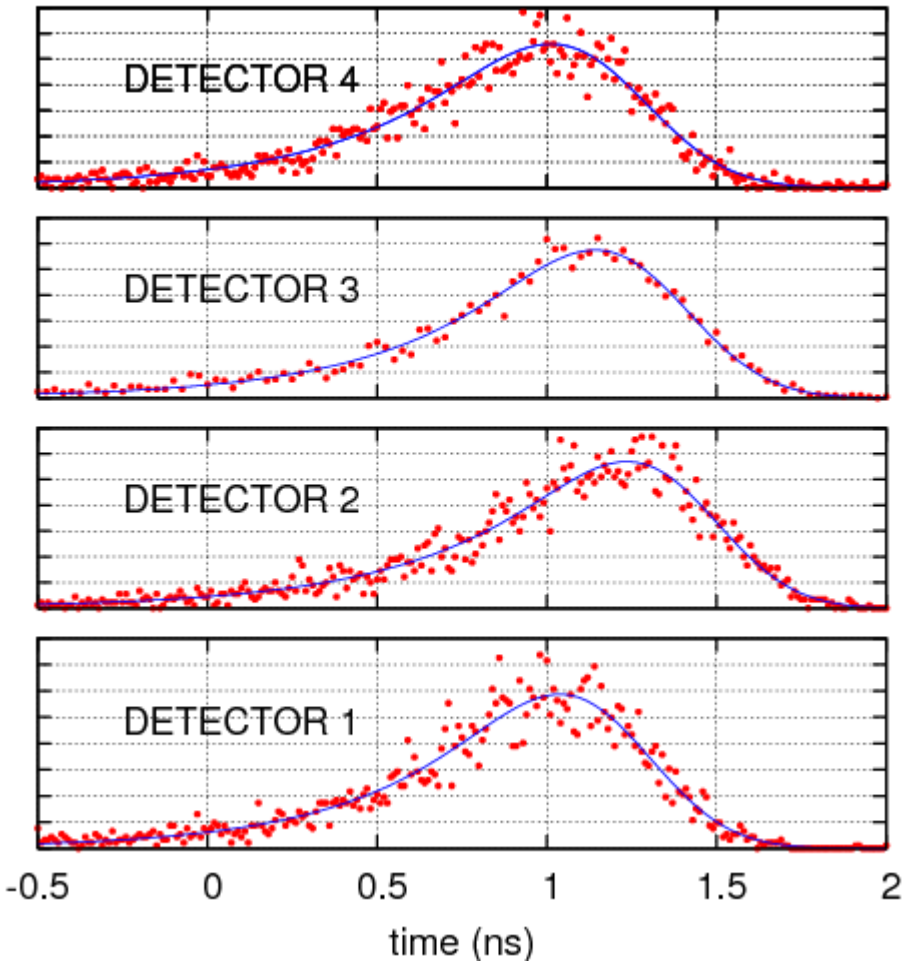


Timing channel attack I

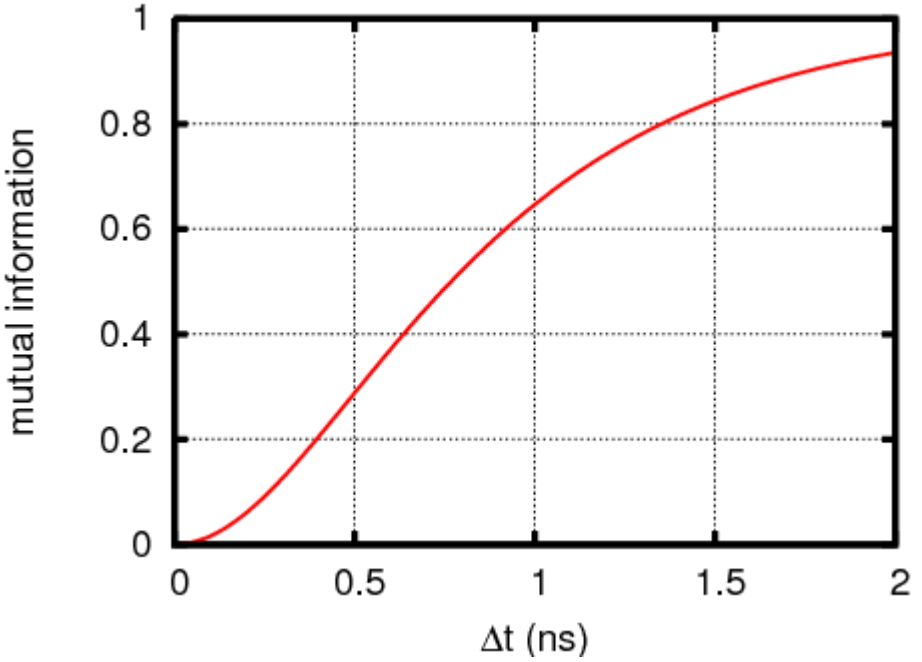


Timing channel attack II

Classical timing information carries fingerprint of detectors:



small detector imbalances may tell Eve a lot!

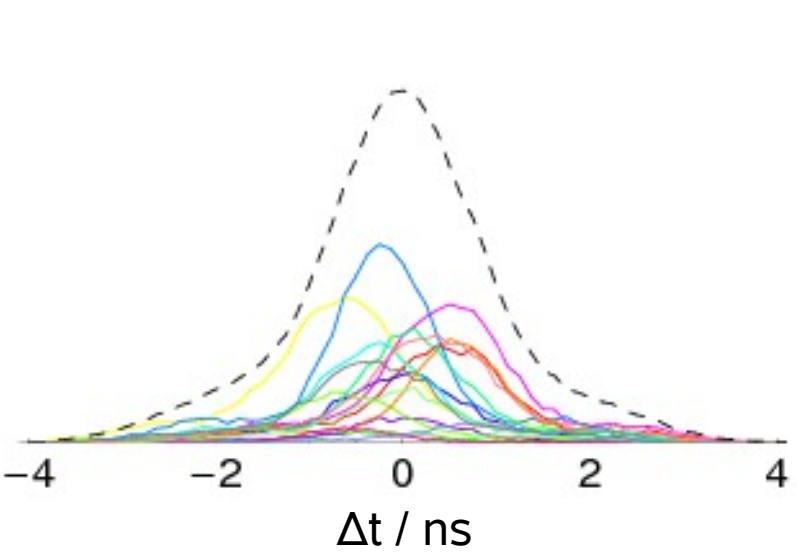


ALL, CK, Optics Express ***15****, 9388 (2007)*

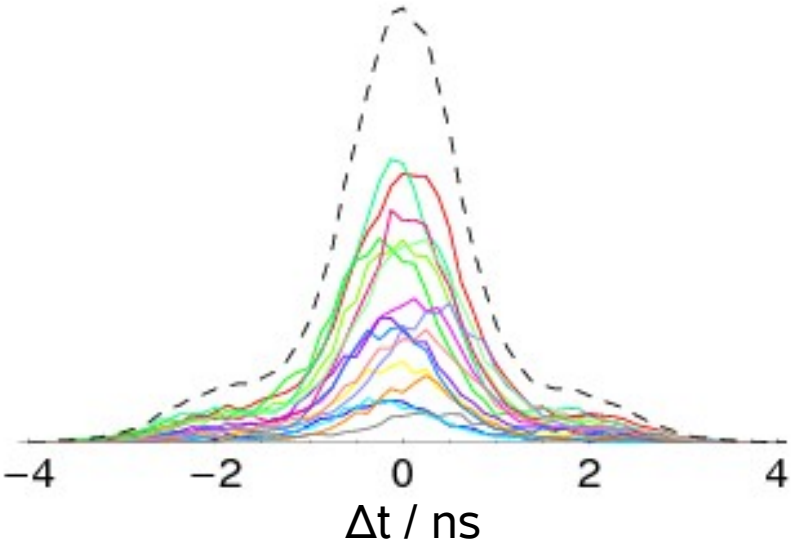
Timing ch attack III

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

delays not compensated



delays compensated



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

Nastier attacks:
V. Makarov
Trondheim
H.K. Lo, Toronto

Time for Coffee.....

NUS National University of Singapore

Thank you !

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

CQT Graduate program:
http://cqtphd.quantumlah.org