Lecture 1: A taste of experimental quantum information techniques

Christian Kurtsiefer

Centre for Quantum Technologies

NUS National University of Singapore

Asher Peres International School, Chowder Bay @ Sydney, Nov 2008

A great quote ...

Quantum physics does not happen in Hilbert space -

quantum physics happens in the lab.

Misquoted? Don't know the
exact reference but certainly a view
of Asher Peres I subscribe to

Overview

- Photons as qubits
  - obvious things one can do in quantum information
  - what is commonly understood by a photon?
  - manipulate qubits
  - what really works well: detectors, pair sources
  - what also works: pair (sometimes multi) photon sources
  - Hamilton operators are useful !!

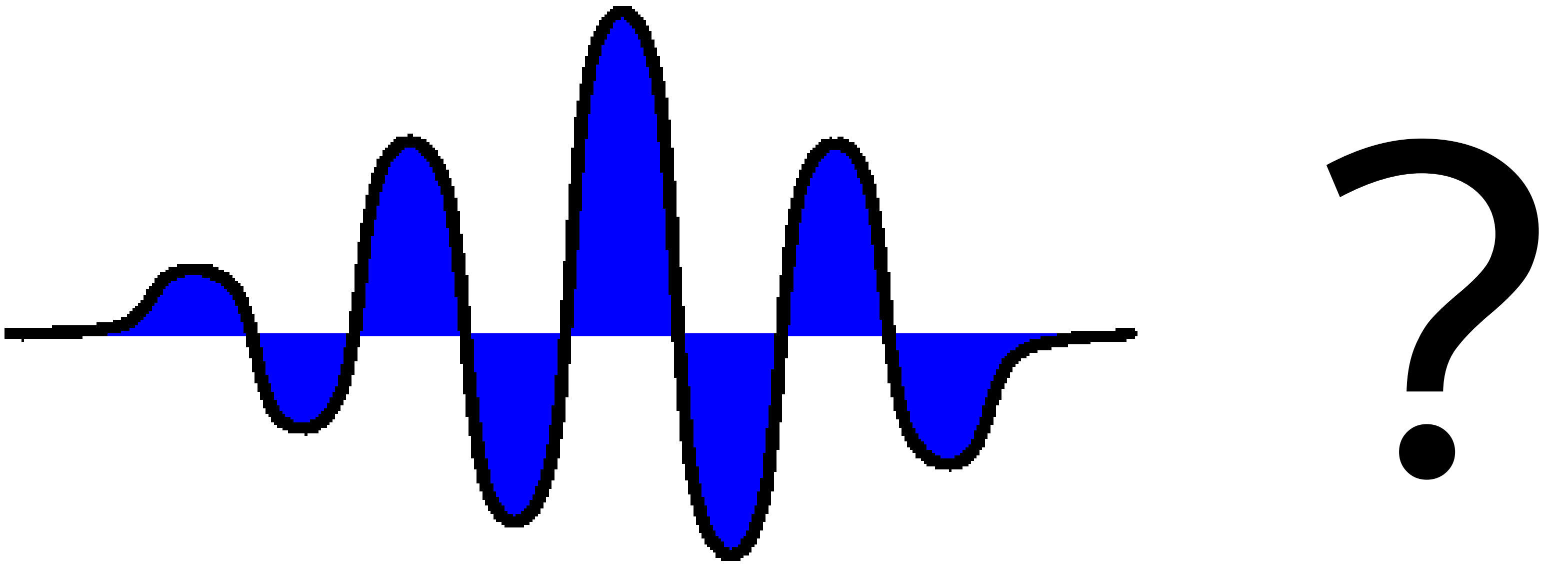
- Quantum key distribution schemes as the usual quantum info suspects
  - basic ideas: BB84
  - Bell inequalities to evaluate knowledge of eavesdropper
  - a practical implementation
  - some dreams and problems

Photons - quantum information

- want distinguishable things representing qubits with possible entanglement in system state:

$$\left|\Psi\right\rangle_{tot} = \sum_i c_i \left|\Psi_{1,i}\right\rangle \otimes \left|\Psi_{2,i}\right\rangle \otimes \left|\Psi_{3,i}\right\rangle \otimes \left|\Psi_{4,i}\right\rangle$$

What is....a photon?



Highly recommended read:
W.E. Lamb: Anti-photon, Appl. Phys. B ***60****, 77 (1995)*

Photons...?

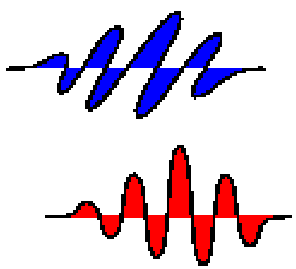
- Definition via detection: photoelectric effect
  localizable in space/time, no energy eigenstates
- Definition via cavity mode excitation
  clean energy eigenstate labelling, very hard to observe
- Definition via spontaneous emission
  localizable in time/origin, well-defined preparation scheme
  “single photon sources” rely on that
- Definition via total energy in ~monochromatic field over hbar

What one can do with photons...

....in quantum information?

- transport light
- encode qubits....without loosing the superposition states

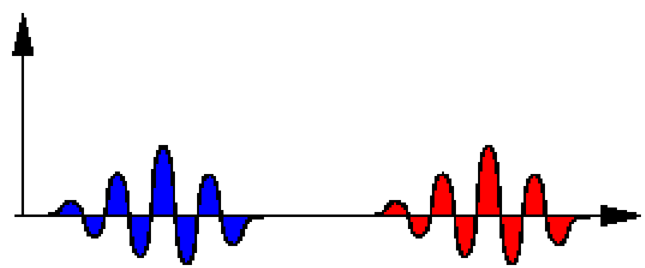
polarization



$|\uparrow\rangle$ H

$|\downarrow\rangle$ V

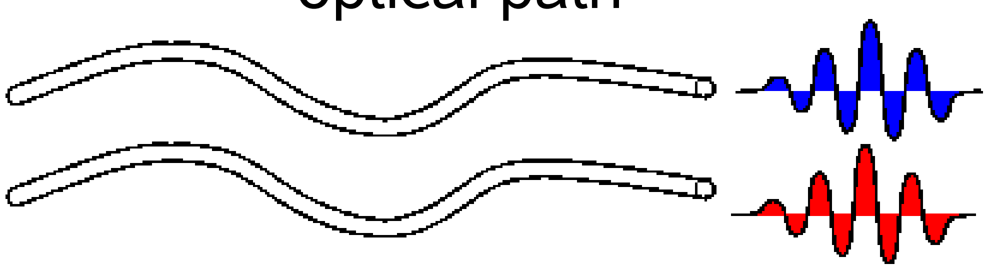
time bin



$|\uparrow\rangle$ early

$|\downarrow\rangle$ late

optical path



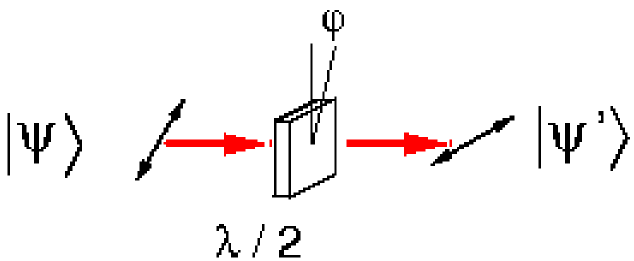
$|\uparrow\rangle$ rail 0

$|\downarrow\rangle$ rail 1

Easy: single qubit operations

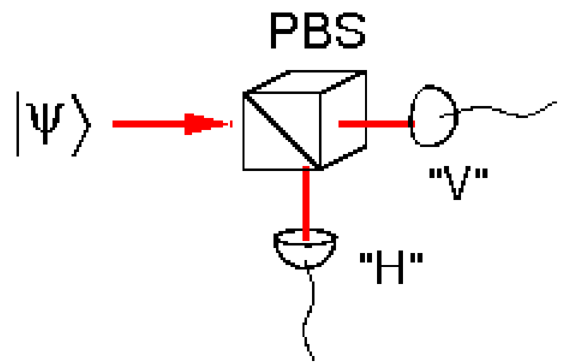
National University of Singapore

- 1-qubit rotation

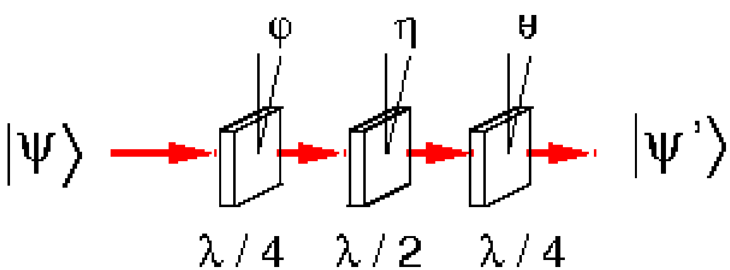


$$|\psi'\rangle = \begin{pmatrix} \cos 2\varphi & -\sin 2\varphi \\ -\sin 2\varphi & -\cos 2\varphi \end{pmatrix} |\psi\rangle$$

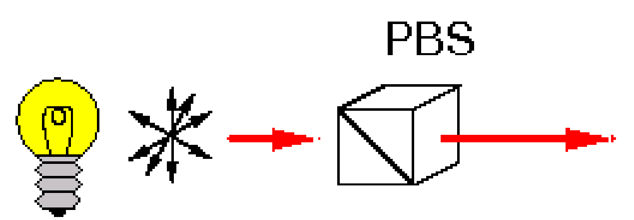
- measurement



- arbitrary 1-qubit operation

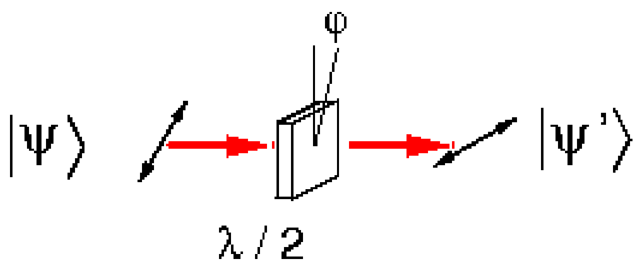


- state preparation



Why are these easy operations?

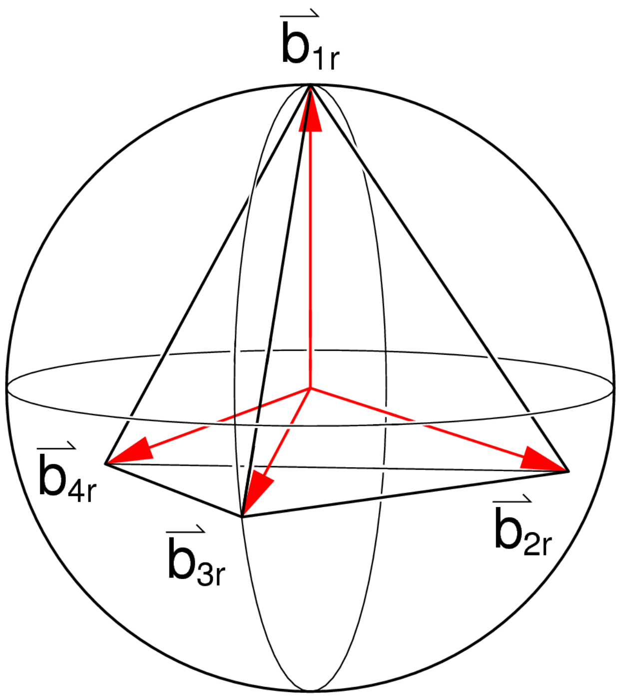
- Inherit all the phase and amplitude manipulation abilities from classical optics / electrodynamics



$$|\psi'\rangle = \begin{pmatrix} \cos 2\varphi & -\sin 2\varphi \\ -\sin 2\varphi & -\cos 2\varphi \end{pmatrix} |\psi\rangle$$

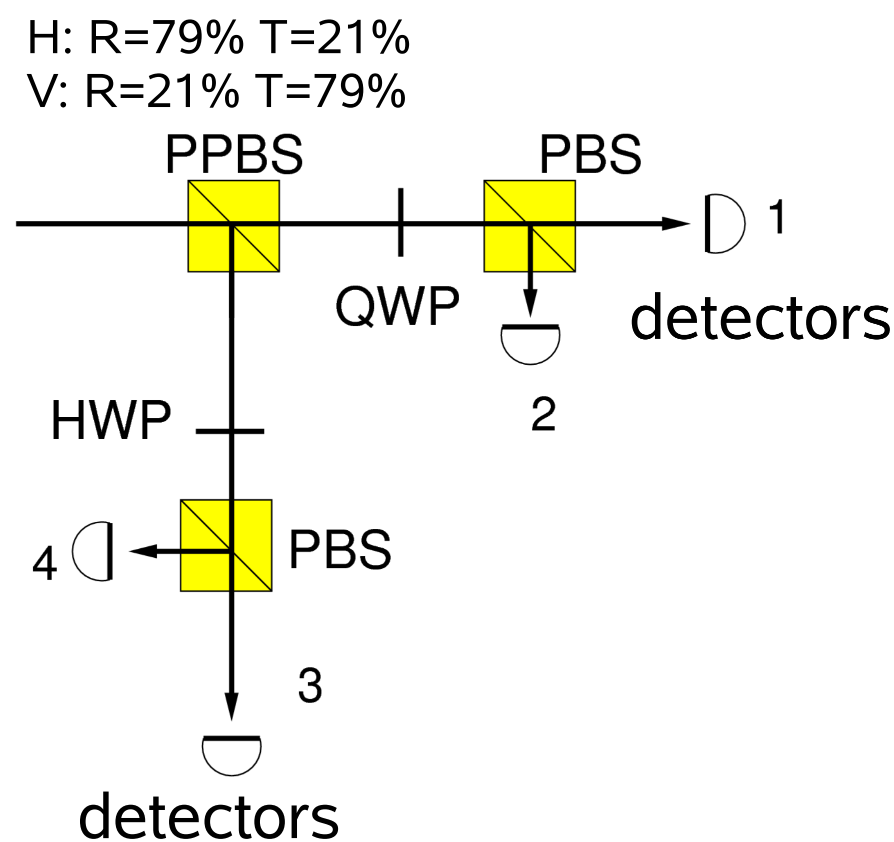
- Birefringent materials, polarization states of light

POVMs in the lab….



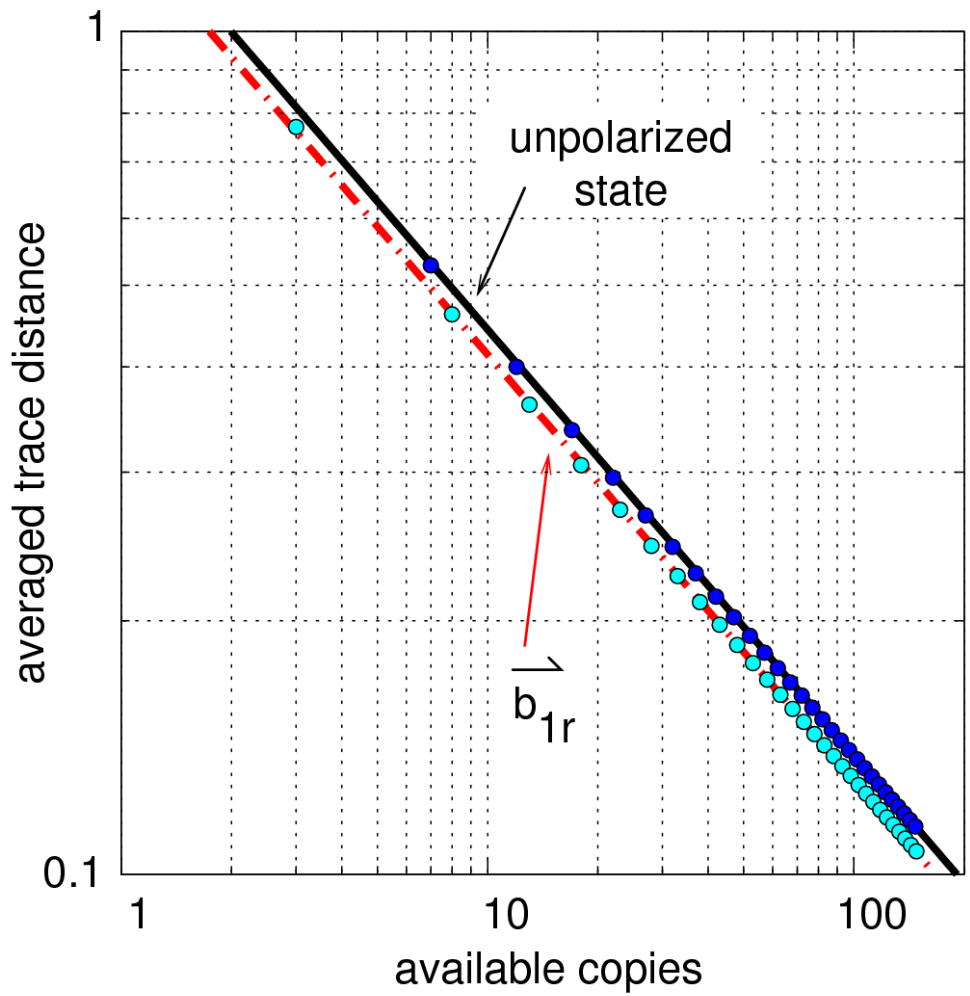
Bloch / Stokes vectors corresponding to an optimal measurement scheme for polarization qubits

optical implementation by embedding in larger Hilbert space



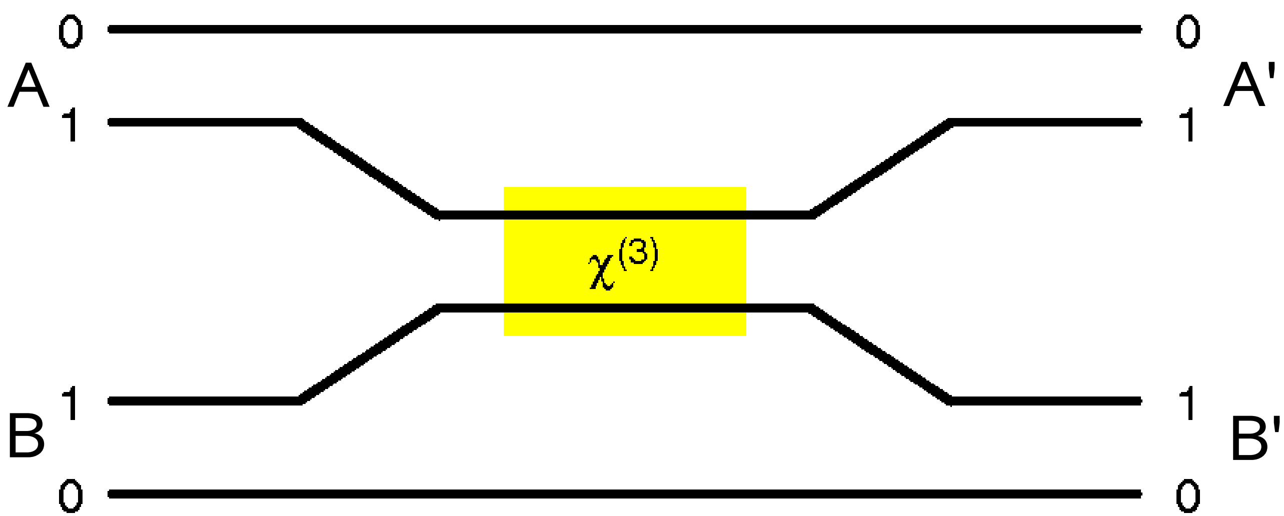
A. Ling et al., J. Mod. Opt. ***53****, 1523 (2006)*

Convergence in an experiment



What is hard?

- universal 2-qubit operations, require large optical nonlinearity



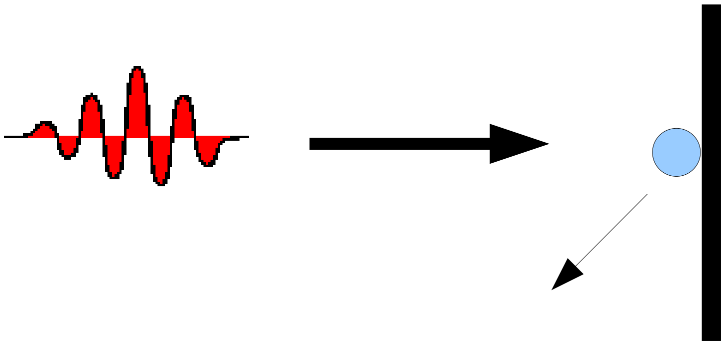
A, B	A', B'
0,0	0,0
0,1	0,1
1,0	1,0
1,1	(1,1) $e^{i\phi}$

- hopeless with typical bulk nonlinearities
- possible with atoms close to resonance:

work by S. Harris & friends in Stanford: atomic clouds
M. Lukin, Harvard: atoms in fibers

Detecting photons

- Use photoelectric effect: Convert electromagnetic field into a charge



metal or
semiconductor
surface

- detect an electron

  becomes an irreversible process in a very short time

Single photon detectors 1

- Photomultiplier
  low-medium quantum efficiency @IR...red, well understood
  can be fast

- Avalanche photodiodes above breakdown
  QE about 20-50% (manufacturer quotes 70%),
  repetition rate ~1MHz

- superconducting detectors
  very high QE (>95% for some), photon number resolving,
  currently slow response rate

- (PIN photodiodes for continuous variables)
  not suitable for single photoelectron counting, high noise at
  low frequencies, up to veryhigh quantum efficiency (>99%)

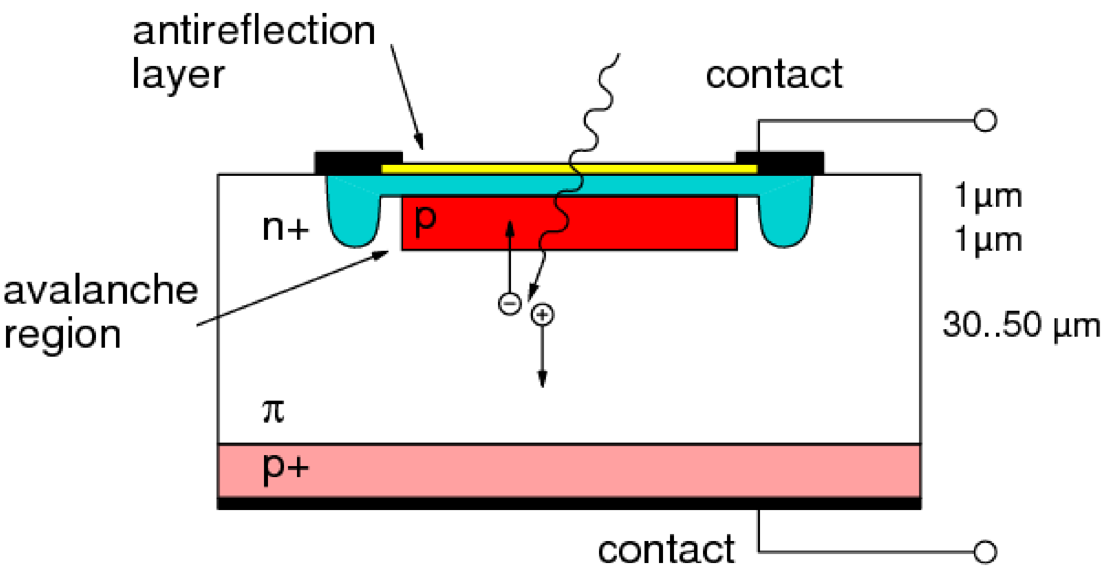
Single photon detectors 2

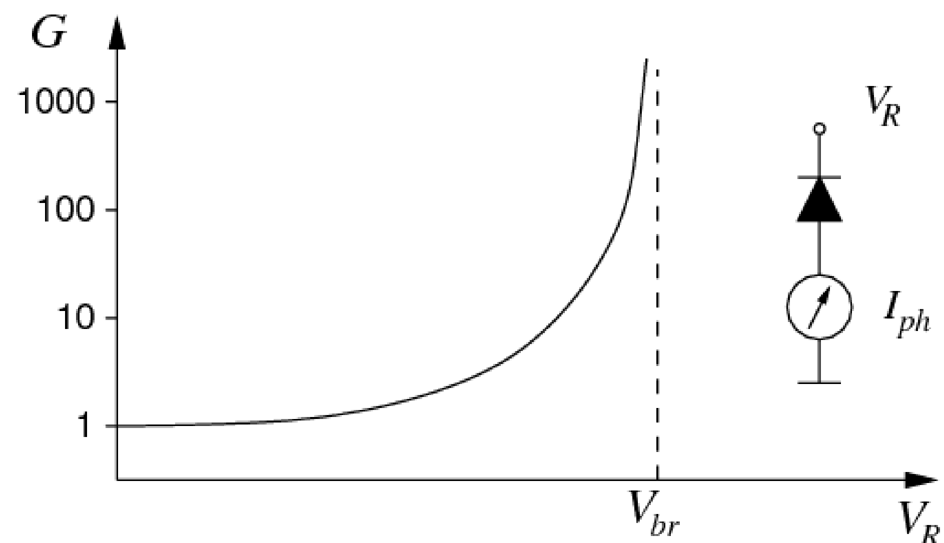
properties:

- quantum efficiency at operational wavelength (0.1..99%)
- timing jitter (30...500 ps)
- dark counts (0...20...100 000 cps)
- dead time (10ns...1us)

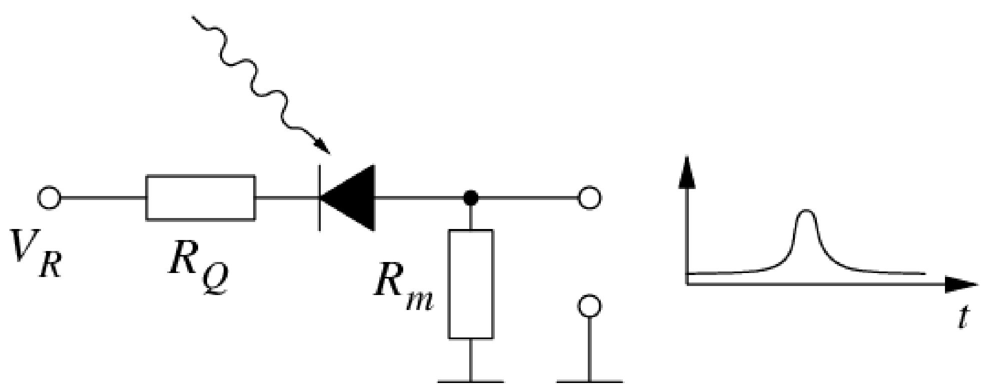
- ugly artefacts: afterpulses, selective blindability
- (intensity-dependent) delays
- gating needs
- temperature requirements (50mK...room temp)

Avalanche photodetector



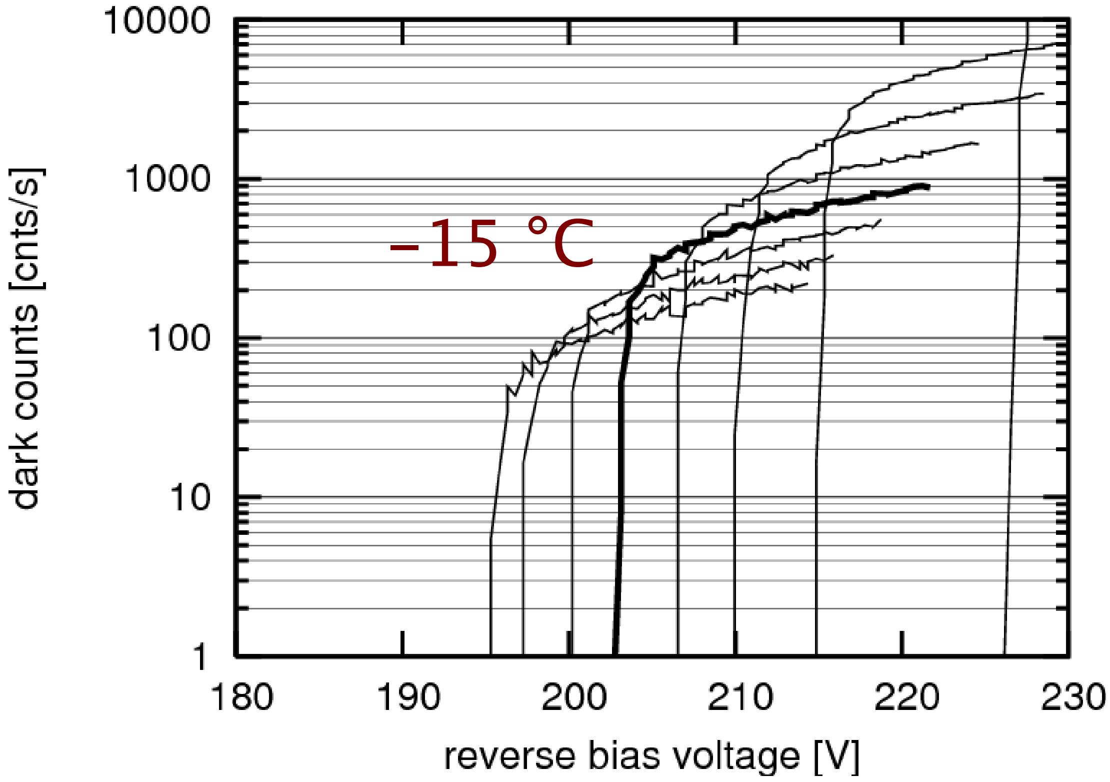


- passive quenching topology:



Detector dark counts

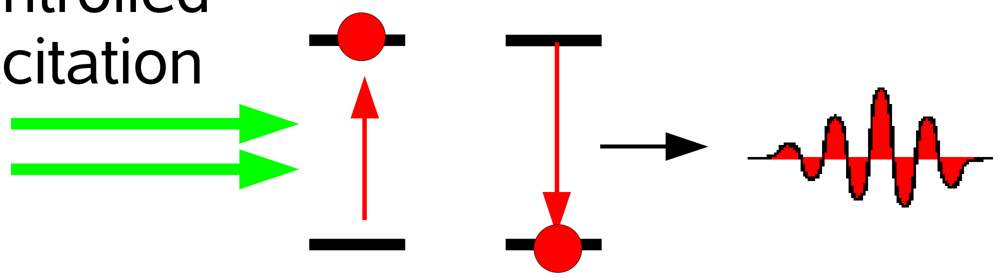
- Lower temperature to limit dark count rate...



'Making' photons

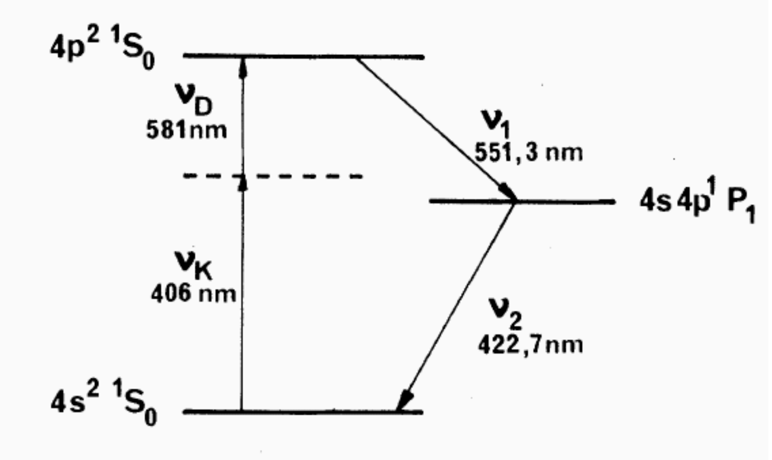
- spontaneous emission from atom-like systems

controlled
excitation



-> James Rabeau

- cascade decays for making pairs

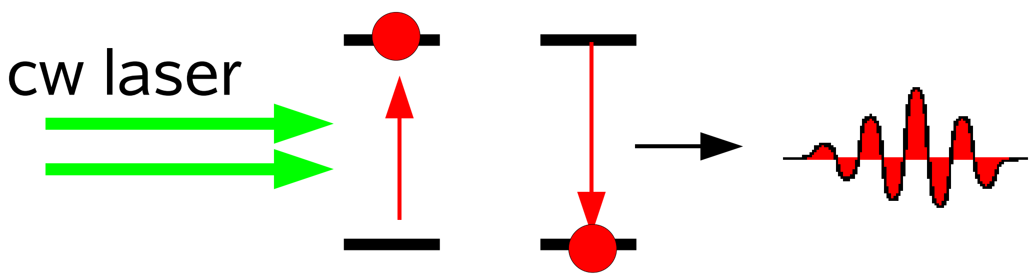


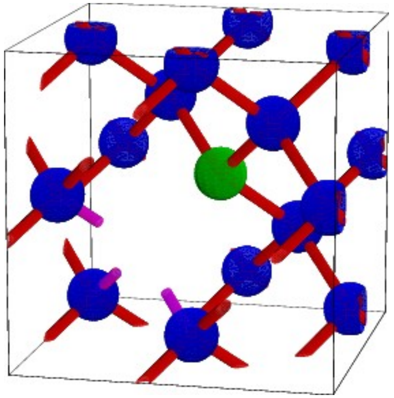
A. Aspect, P. Grangier, P. Roger, Phys. Rev. Lett. ***47,*** *460 (1981)*

- parametric conversion in optical nonlinearities

Single Photon Sources

- making single photons at random times:



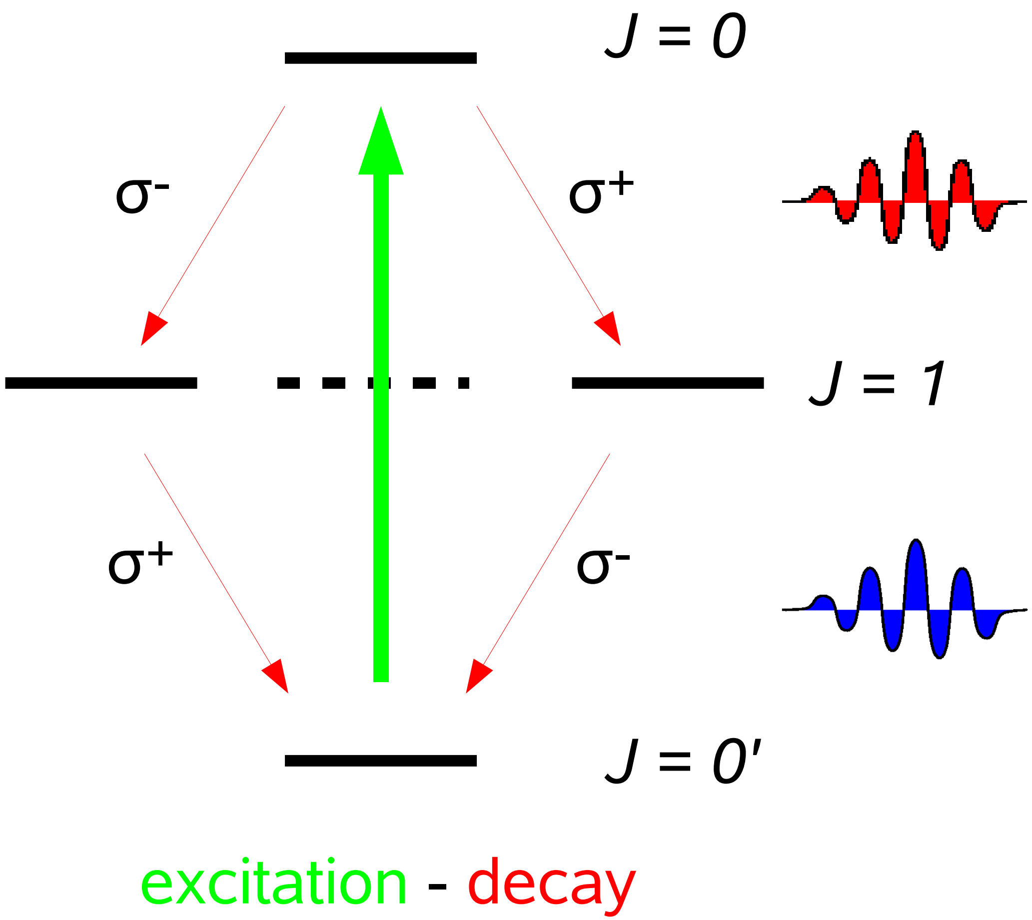


spontaneous emission from
atoms / color centers / quantum dots / single molecules

- making single photons deterministically (and sequences)

  use pulsed excitation,
  cavities to enforce emission in one mode via Purcell effect

Cascade Decays 2



- indistinguishable decay paths

(0,0) – (1,1) – (0',0) and
(0,0) – (1,-1) – (0',0)

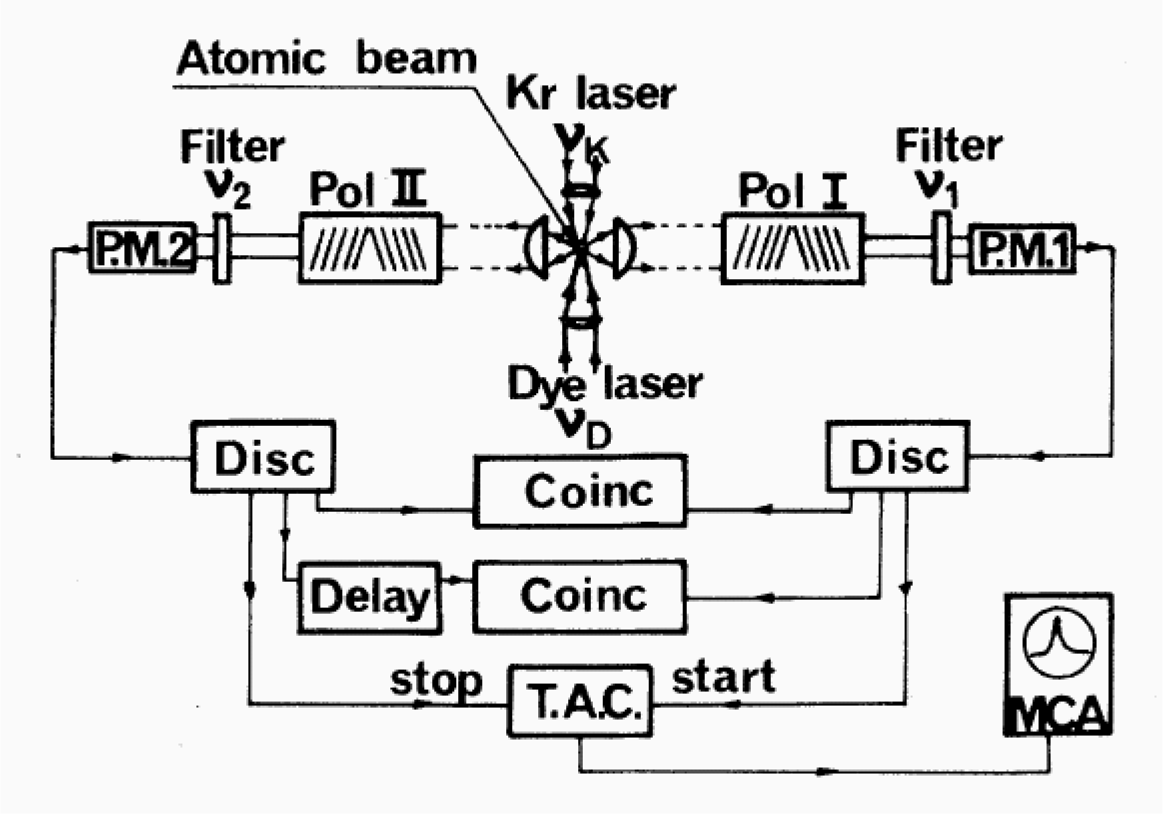
leads to polarization correlation of the photons:

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

singlet Bell state $|\Psi^-\rangle$

A. Aspect, P. Grangier, P. Roger, Phys. Rev. Lett. ***47,*** *460 (1981)*

Atomic Cascade Decays



A. Aspect, P. Grangier, P. Roger, Phys. Rev. Lett. ***47,*** *460 (1981)*

Nonlinear Optical Processes

- Nonlinear optical processes: 3-wave mixing, 4-wave mixing:

  response of a medium:

$$P = \epsilon_0 \left(\chi E + \chi^{(2)} E^2 + \chi^{(3)} E^3 + \ldots \right)$$

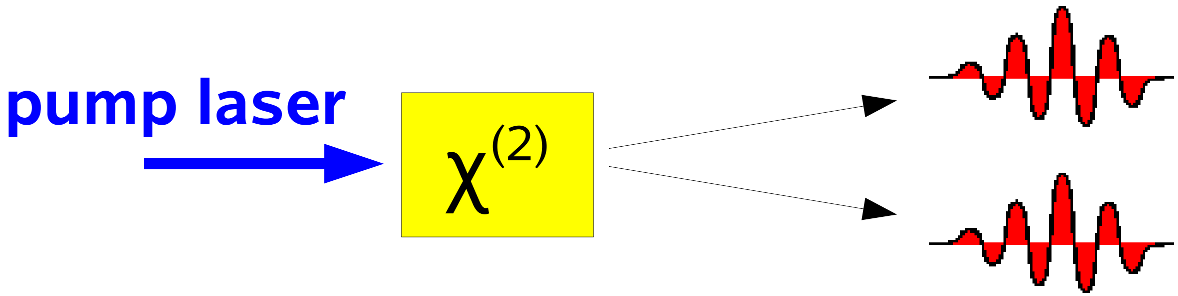
refractive index,
birefringence

second harmonic generation
parametric conversion

Kerr nonlinearity

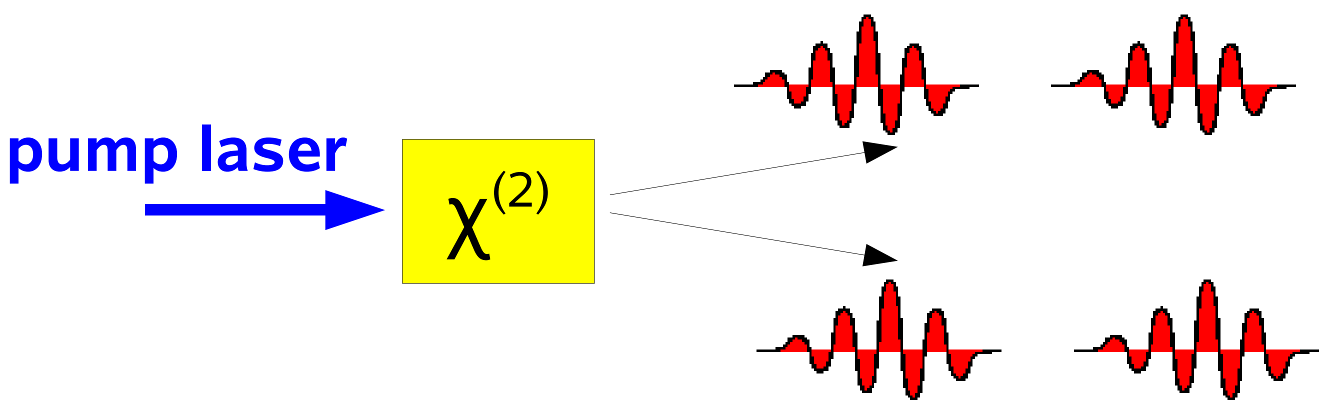
Nonlinear Optical Processes 2

- making sometimes pairs of photons at random/fixed times

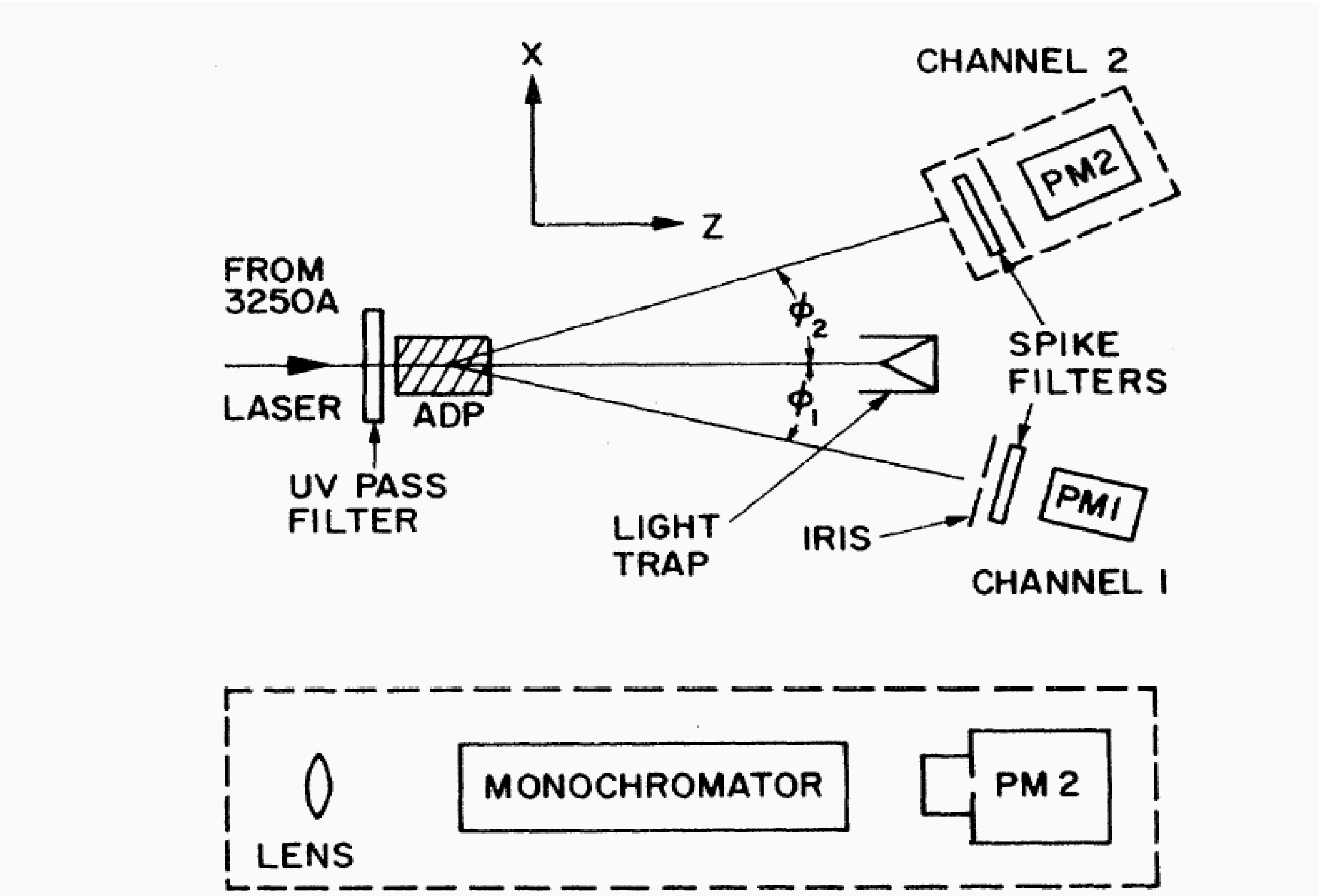


high fidelity maximally entangled photon pair states

- making combinations of 2/4/6.....photon events at fixed times:



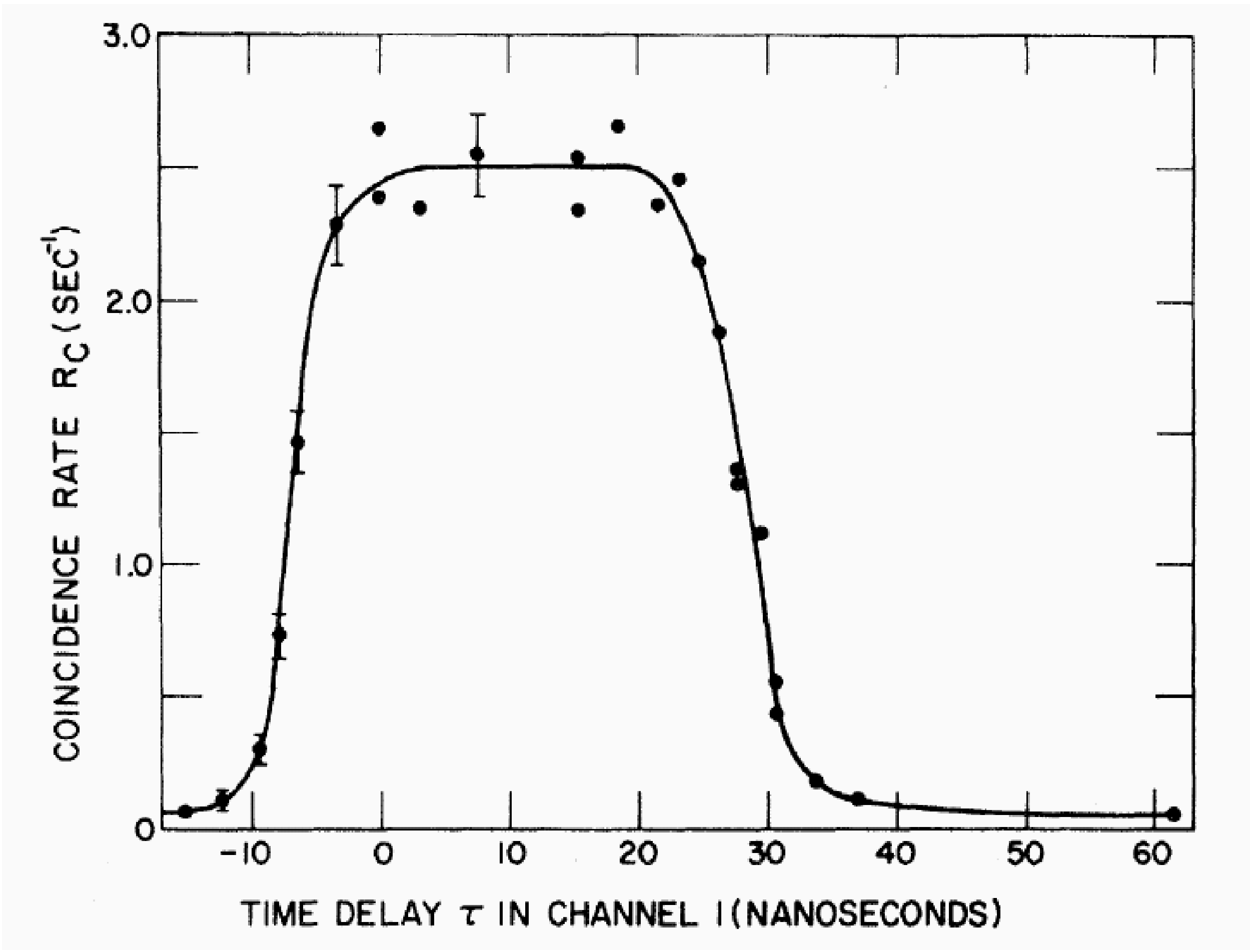
The first (?) PDC pair source



D.C. Burnham, D.L. Weinberg, Phys. Rev. Lett. ***25****, 84 (1970)*

Photon pairs form PDC 2

- correlation between detection times – makes us talk about pairs



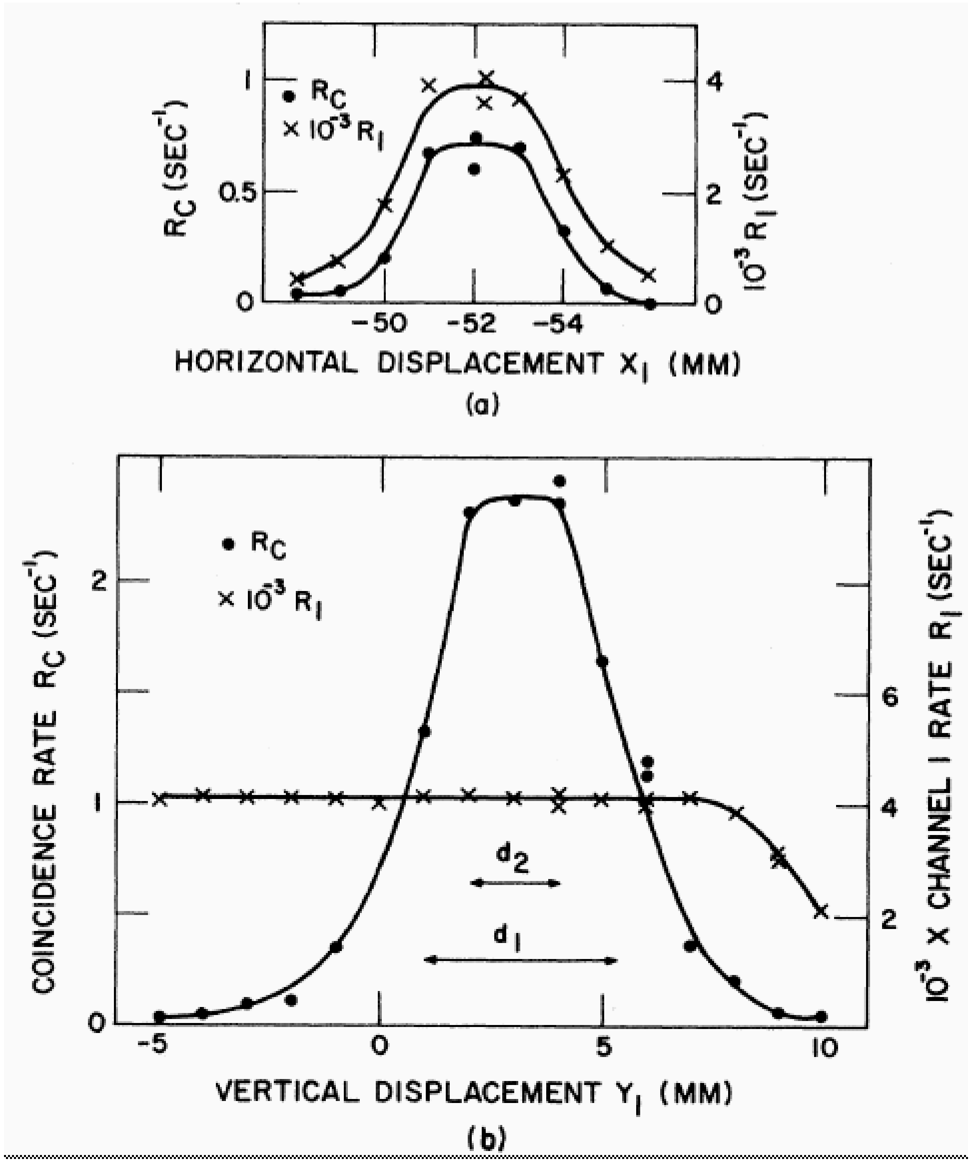
D.C. Burnham, D.L. Weinberg, Phys. Rev. Lett. ***25****, 84 (1970)*

Photon pairs form PDC 3

- 'spatial' correlations:

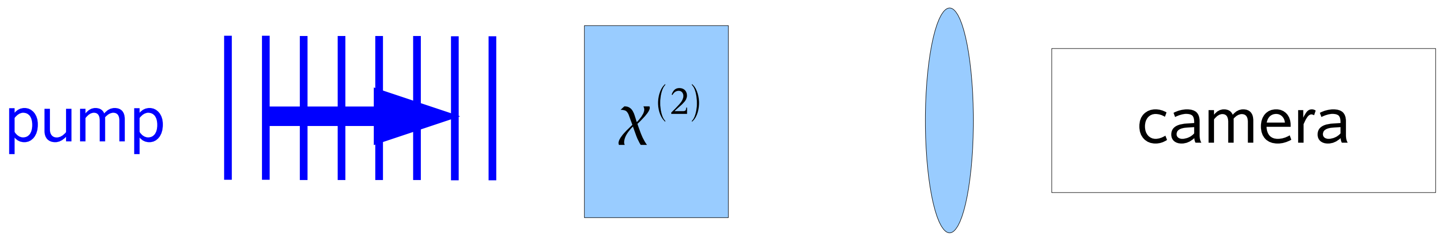
  coincidences show up for particular detector positions

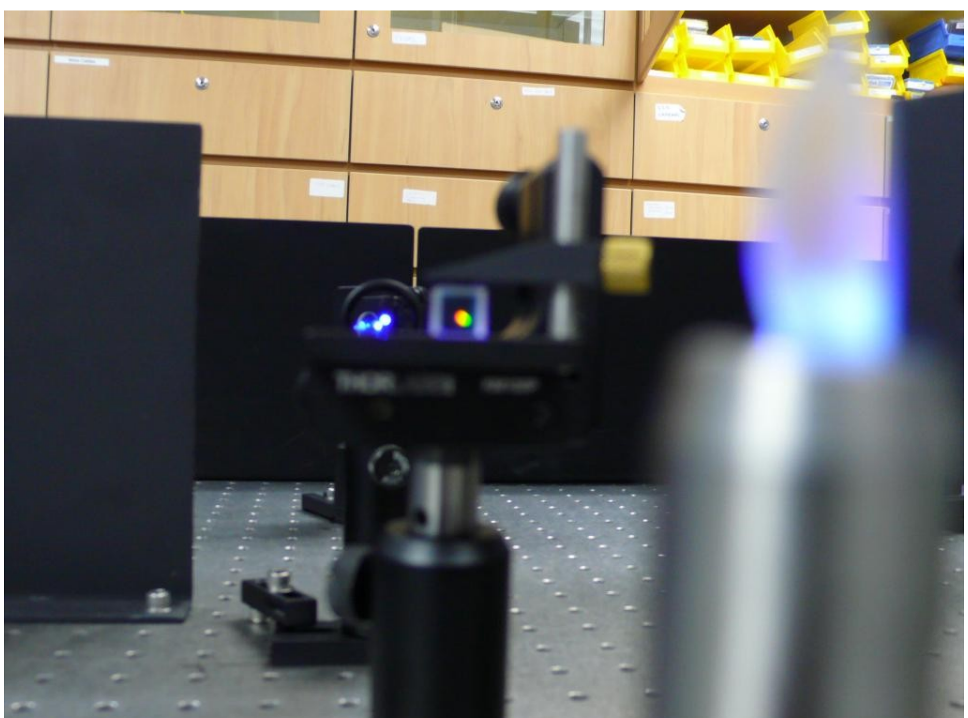
- indicates momentum conservation

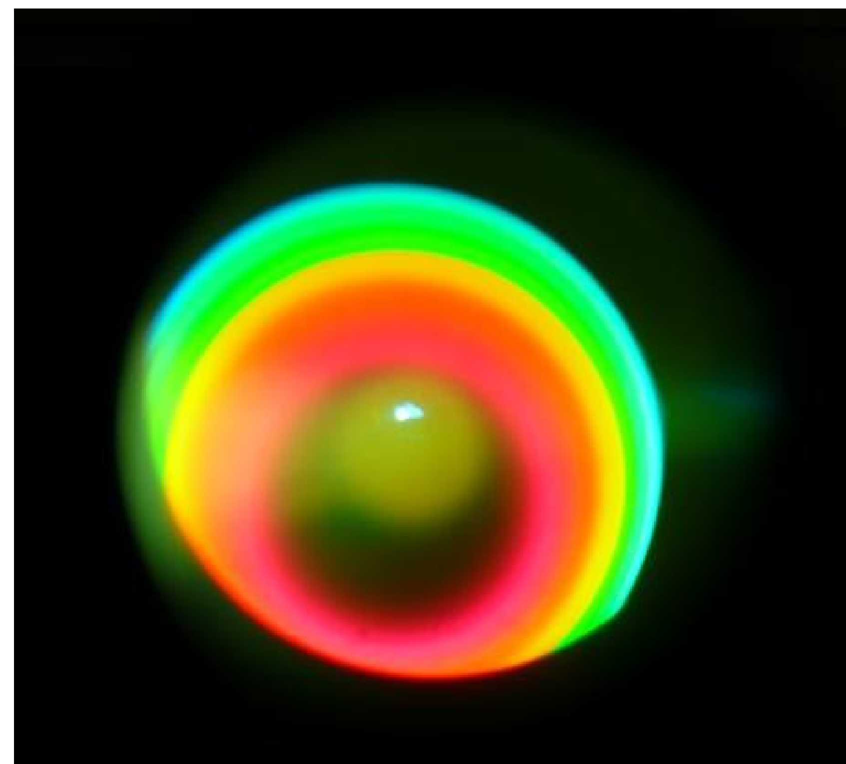


D.C. Burnham, D.L. Weinberg, Phys. Rev. Lett. ***25****, 84 (1970)*

Type-II SPDC fluorescence

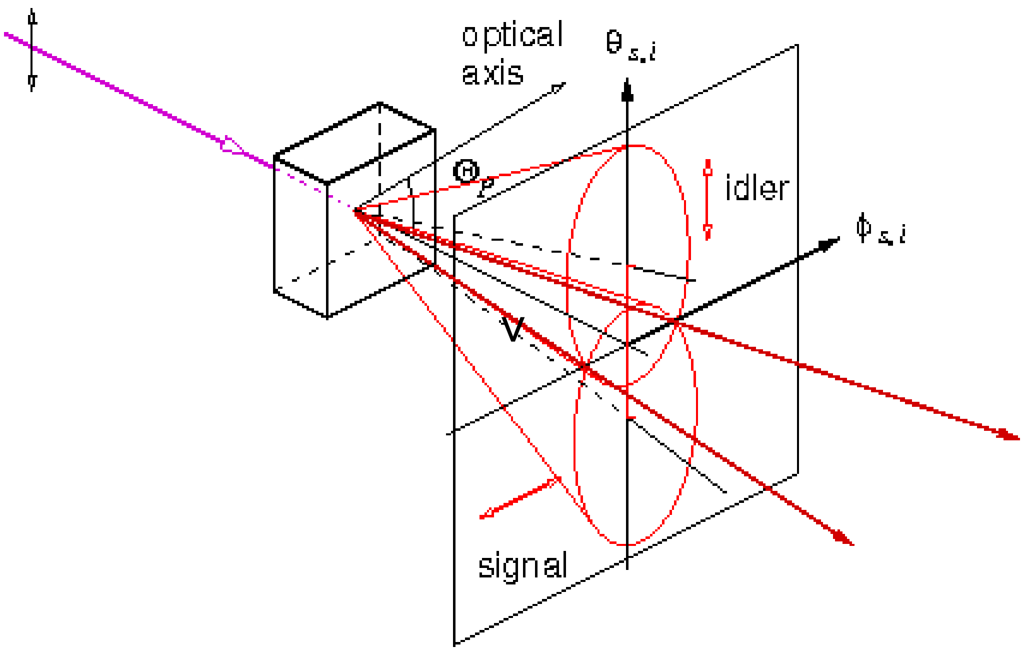






Entangled photon sources

- Use non-collinear type-II parametric down conversion



two indistinguishable decay paths lead to

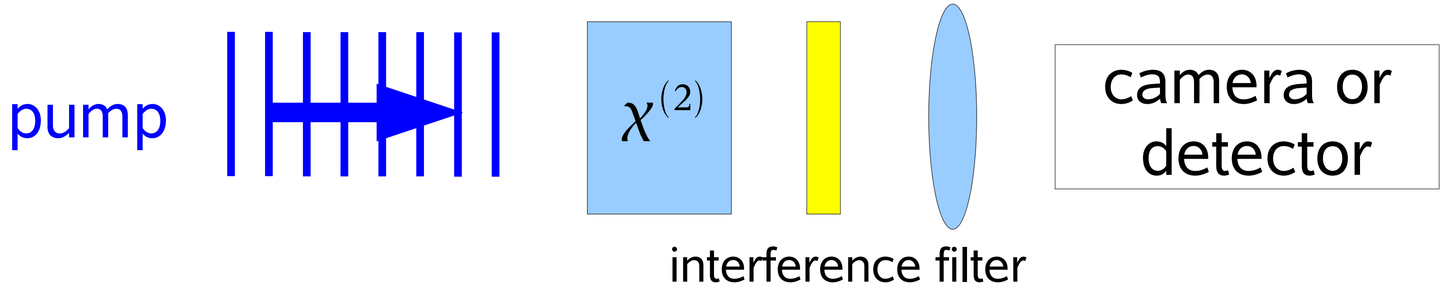
$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|HV\right\rangle - \left|VH\right\rangle\right)$$

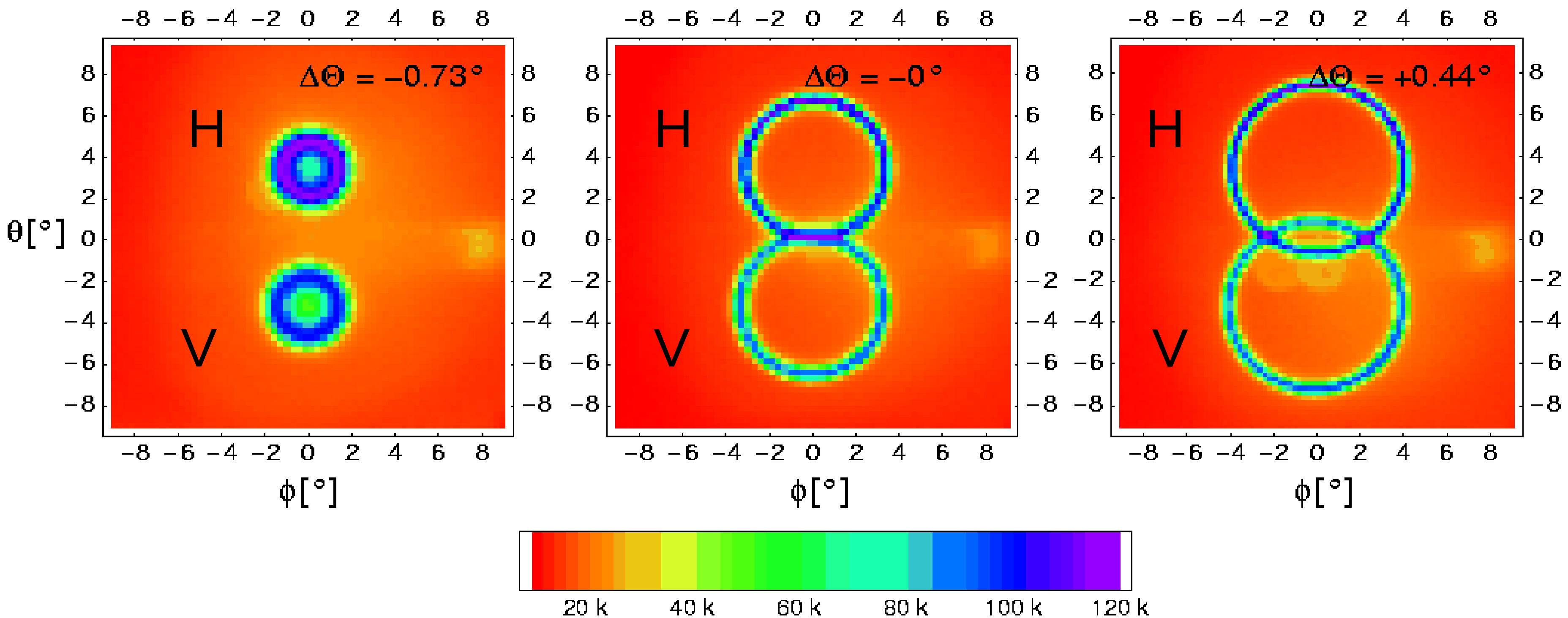
$$= \frac{1}{\sqrt{2}}\left(\left|+-\right\rangle - \left|-+\right\rangle\right)$$

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

Type-II SPDC fluorescence

- Look at a patricular wavelength range





SPDC, quantitatively

- Free electromagnetic field:

$$\hat{H}_F = \frac{\epsilon_0}{2} \int \hat{\vec{E}}^2(\vec{r}) + c^2 \hat{\vec{B}}^2(\vec{r})\, d^3 r$$

- Linear susceptible material

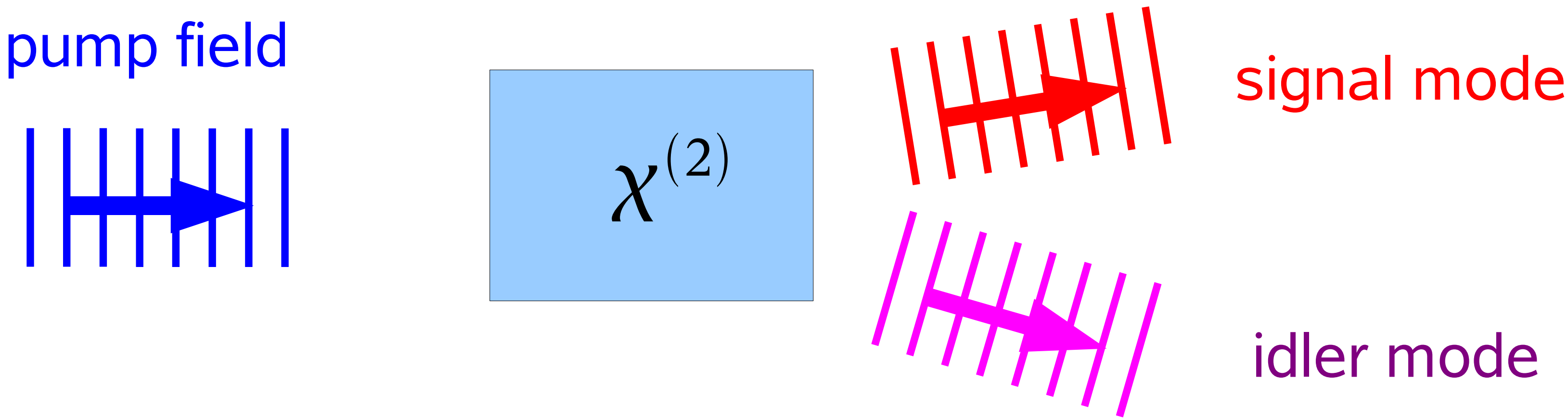
$$\hat{H}_0 = \frac{\epsilon_0}{2} \int \chi \hat{\vec{E}}^2(\vec{r}) + c^2 \hat{\vec{B}}^2(\vec{r})\, d^3 r$$

- With nonlinear material:

$$\hat{H} = \frac{1}{2} \int \hat{\vec{E}} \cdot \hat{\vec{P}}(\vec{r}) + \epsilon_0 c^2 \hat{\vec{B}}^2(\vec{r})\, d^3 r$$

$$= \hat{H}_0 + \frac{\epsilon_0}{2} \int \hat{\vec{E}} \chi^{(2)} : \hat{\vec{E}}^2(\vec{r})\, d^3 r =: \hat{H}_0 + \hat{H}_I$$

Choose fields



- Pump is treated as classical field (non-depleted):

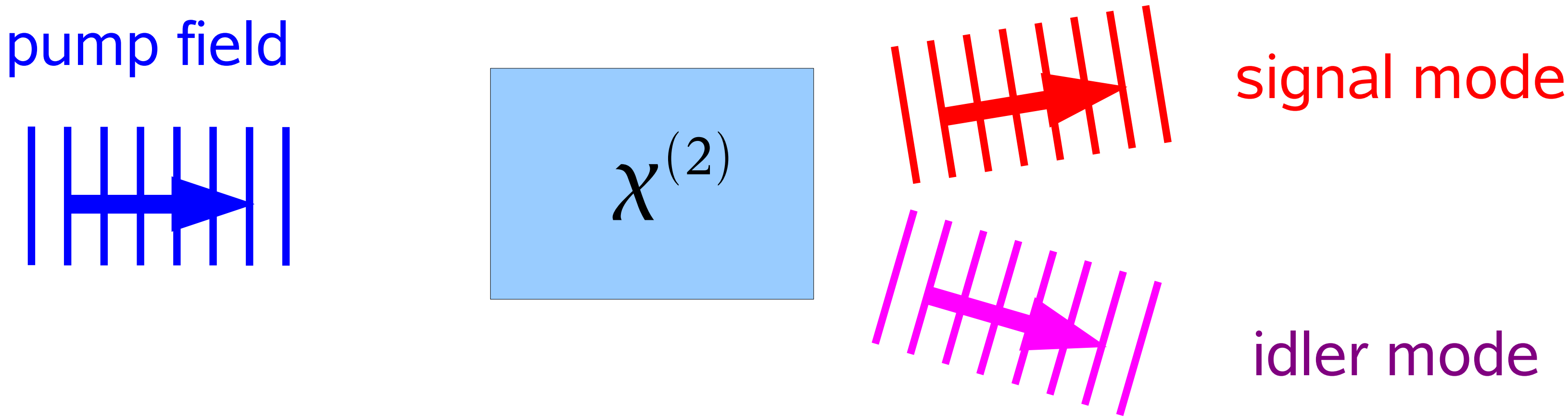
$$\vec{E}_p(\vec{r},t)=E_0\vec{\epsilon}\left[g(\vec{r})e^{i\omega_p t}+g^*(\vec{r})e^{-i\omega_p t}\right]$$

amplitude

mode function

Target modes

NUS
National University of Singapore



- Electrical field operator

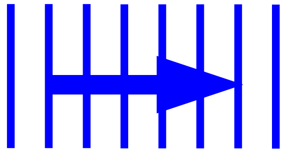
$$\hat{\vec{E}}_{s,i}(\vec{r}) = i\,E_{s,i}\,\vec{\epsilon}\left[g(\vec{r})\,\hat{a}(t) - g^*(\vec{r})\,\hat{a}^+(t)\right]$$

mode function

operator component

normalization

Typical mode functions



- Plane waves:

$$g(\vec{r}) = e^{i\vec{k}\cdot\vec{r}}$$

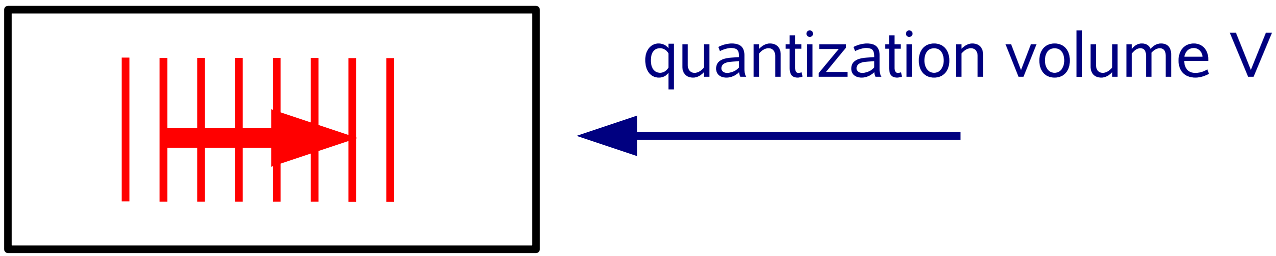
conceptually nice, not really implemented in experiments

- Plane waves with a Gaussian envelope

$$g(\rho, z) = e^{ikz} e^{-\rho^2/w^2}$$

typical laser beams and light that propagates in optical fibers (approx)

Normalize operator...The Works



- Get the magnetic field operator

$$\hat{\vec{B}}_{s,i}(\vec{r},t)=\frac{1}{i\omega}E_{s,i}\left[\nabla\times(\vec{\epsilon}\,g(\vec{r}))\hat{a}(t)+\nabla\times(\vec{\epsilon}\,g^*(\vec{r}))\hat{a}^+(t)\right]$$

- Free field should look like harmonic oscillators:

$$\hat{H}_0=\frac{\epsilon_0}{2}\int_V\left[\hat{\vec{E}}^2(\vec{r})+c^2\hat{\vec{B}}^2(\vec{r})\right]dV=\sum_{modes\ j}\hbar\omega_j(\hat{a}_j^+\hat{a}_j+\frac{1}{2})$$

you need dispersion here: $c^2\vec{k}^2=\omega^2$ for plane waves

you get $E_{s,i}=\sqrt{\dfrac{\hbar\omega_j}{2\epsilon_0 V}}$ for plane waves

Simplify H_I

$$\hat{H}_I = \frac{\epsilon_0}{2} \int \vec{E}_p(\vec{r},t) \chi^{(2)} \hat{\vec{E}}_s(\vec{r},t) \hat{\vec{E}}_i(\vec{r},t) \, d^3 r$$

- eight terms, integral only over mode functions:

$$\hat{H}_I = \sum_{n,m} \frac{\epsilon_0}{2} E_0 E_{s_n} E_{i_m} \left(\vec{\epsilon}_P \chi^{(2)} \vec{\epsilon}_{s_n} \vec{\epsilon}_{i_m} \right) \times$$

constants

$$\left[\left(\int_V g_P(\vec{r}) g_{s_n}(\vec{r}) g_{i_m}(\vec{r}) \, d^3 r \times \right.\right.$$

spatial aspect

$$\left. \hat{a}_{s_n}(t) \hat{a}_{i_m}(t) e^{i \omega_P t} \right)$$

operator character
+ time dependencies

$$\left. + 7 \, more \, terms \right]$$

mode indices

interaction volume

Phase matching

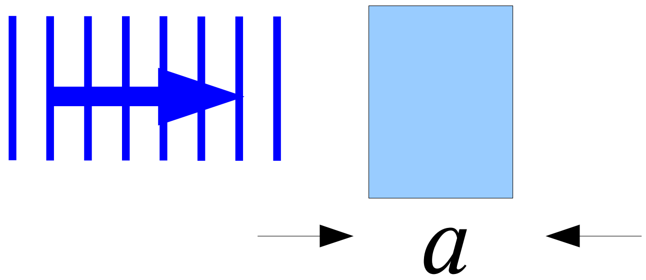
$$S := \int_V g_P(\vec{r})\, g_{s_n}(\vec{r})\, g_{i_m}(\vec{r})\, d^3 r$$

for terms with $\hat{a}_s \hat{a}_i$

- plane waves:

$$S = (2\pi)^3 \delta_{xyz}(k_P + k_s + k_i)$$

- finite size of interaction thickness:



$$S = (2\pi)^2 \delta_{xy}(k_P + k_s + k_i) \times$$
$$a \,\mathrm{sinc}\left[(k_{z,P} + k_{z,s} + k_{z,i})\, a/2\right]$$

Phase matching 2

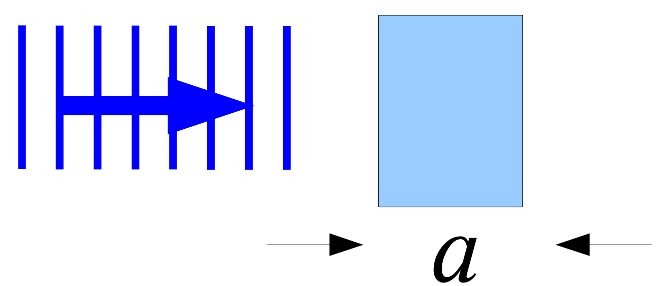
$$S := \int_V g_P(\vec{r})\, g^*_{s_n}(\vec{r})\, g^*_{i_m}(\vec{r})\, d^3 r$$

for terms with $\hat{a}_s^+ \hat{a}_i^+$

- plane waves:

$$S = (2\pi)^3 \delta_{xyz}(k_P - k_s - k_i)$$

- finite size of interaction thickness:



$$S = (2\pi)^2 \delta_{xy}(k_P - k_s - k_i) \times$$
$$a \,\mathrm{sinc}\left[(k_{z,P} - k_{z,s} - k_{z,i})\, a/2 \right]$$

approximate momentum conservation

So now we have...

$$\hat{H}_I = A(\hat{a}_s^+ \hat{a}_i^+ e^{-i\omega_P t} + \hat{a}_s \hat{a}_i e^{+i\omega_P t})$$

......and we know A quantitatively

Where do we go from here on?

- consider asymptotic states (vacuum fields -> pair states)

$$|\Psi_f\rangle = |1_s, 1_i\rangle = \hat{a}_s^+ \hat{a}_i^+ |0\rangle$$

- do Fermi's golden rule for rates from the vacuum $|\Psi_i\rangle = |0\rangle$

...brings energy conservation

Rate details

- for fixed target wave index k_s

mode density
for ki

$$R(k_s) = \frac{2\pi}{\hbar} \left| \langle \Psi_i | \hat{H}_I | \Psi_f \rangle \right|^2 \rho(\Delta E)$$

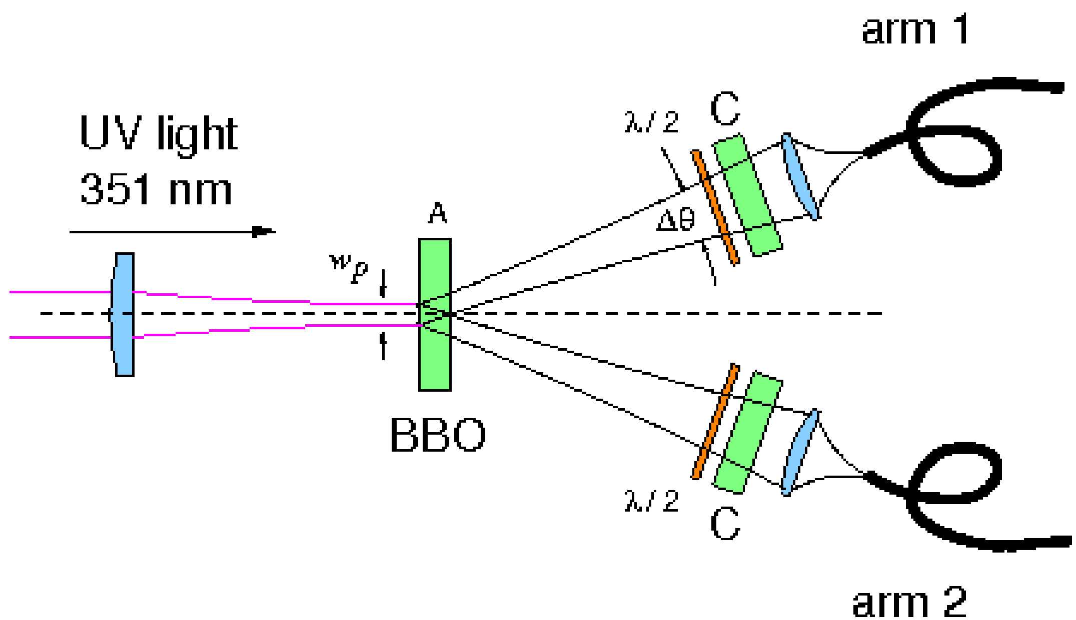
- total rate in all possible ks: (Gaussian beams, collinear modes of waist $w_s = w_i = w_p$):

$$R_T = \frac{4 d^2 a P \omega_P}{9 n_s n_i n_p \epsilon_0 \pi w_P^2 (n_i - n_s) c^2}$$

d: effective nonlinearity
a: crystal thickness
n: refractive indices
P: pump power

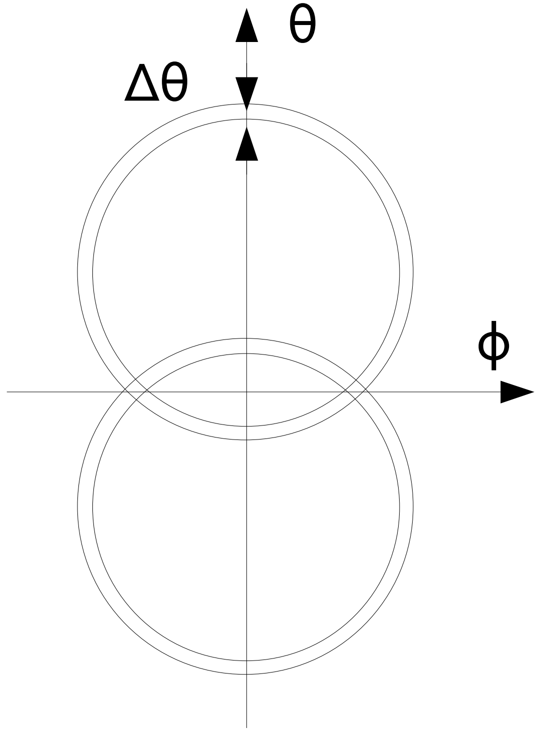
typically ~5000 pairs/sec/mW for 2mm thick BBO in type-II

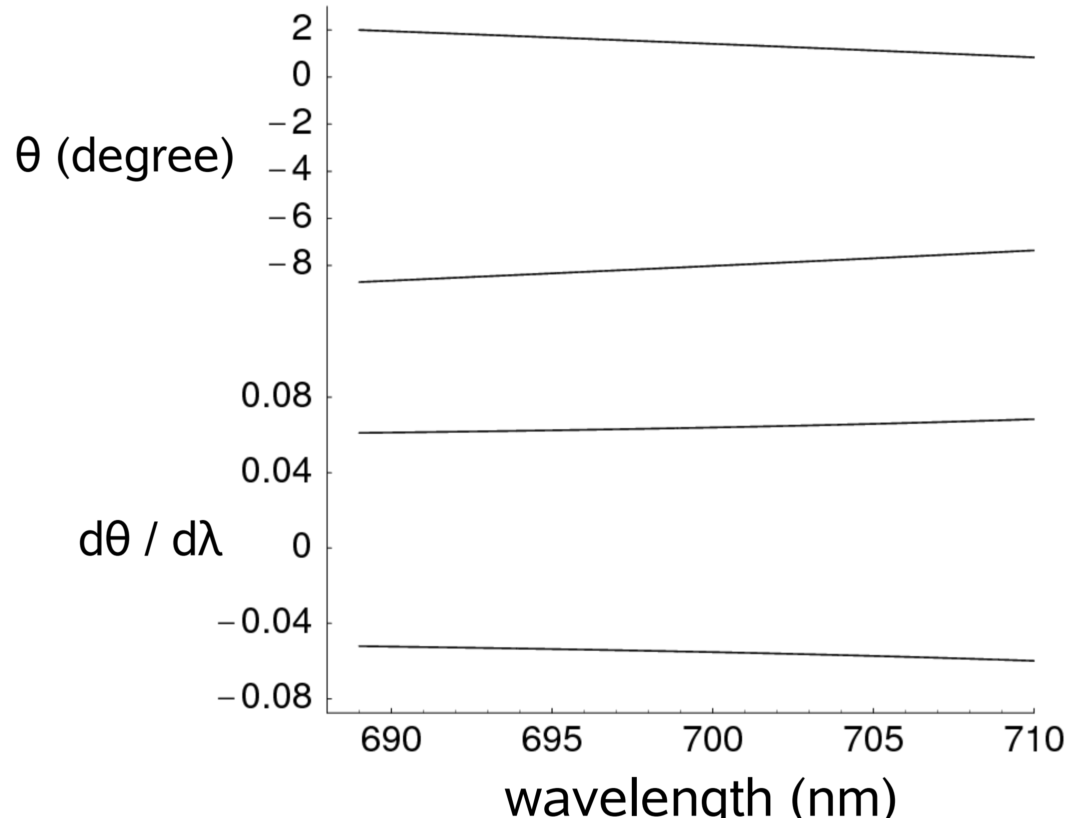
An efficient pair source



- Choose a target wavelengh which is suitable for detectors
- couple target modes in single mode optical fibers
- Remove residual distinguishability between photons due to birefringence

Match angular dispersion

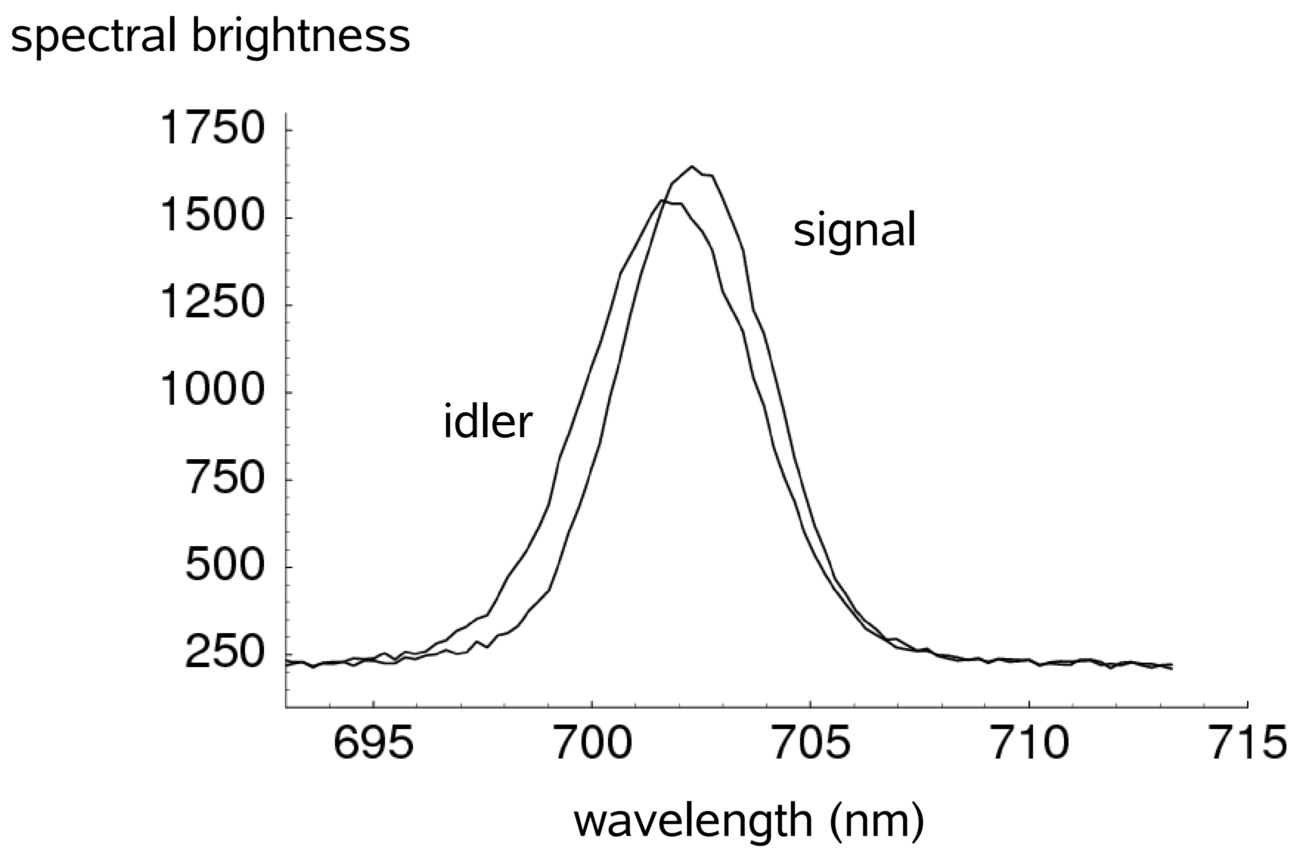




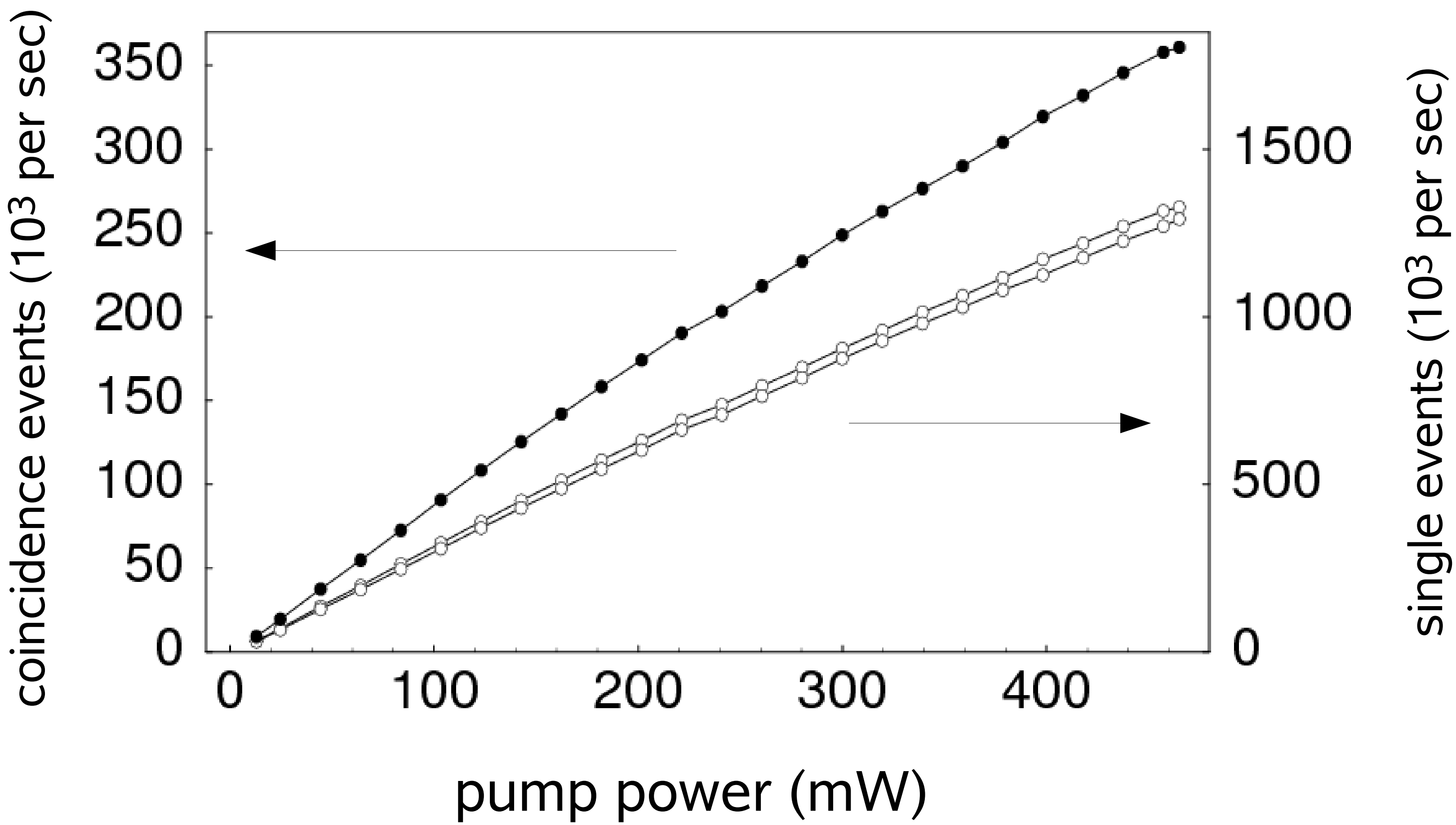
- Choose an optical bandwidth $\Delta\lambda$
- Choose collection angle of fiber modes to $\Delta\theta = \Delta\lambda\, d\theta/d\lambda$
- Restrict pump mode to collection region

C. K., M. Oberparleiter, and H. Weinfurter, Phys. Rev. A ***64****, 010102(R) (2001)*

Spectral distribution

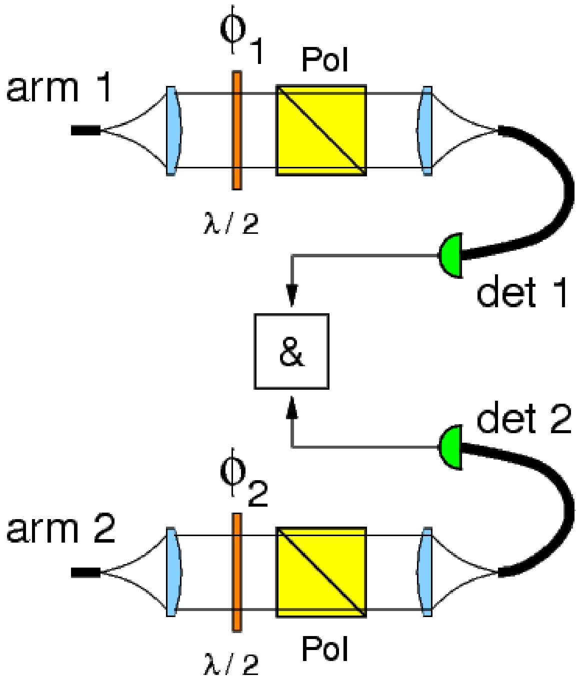


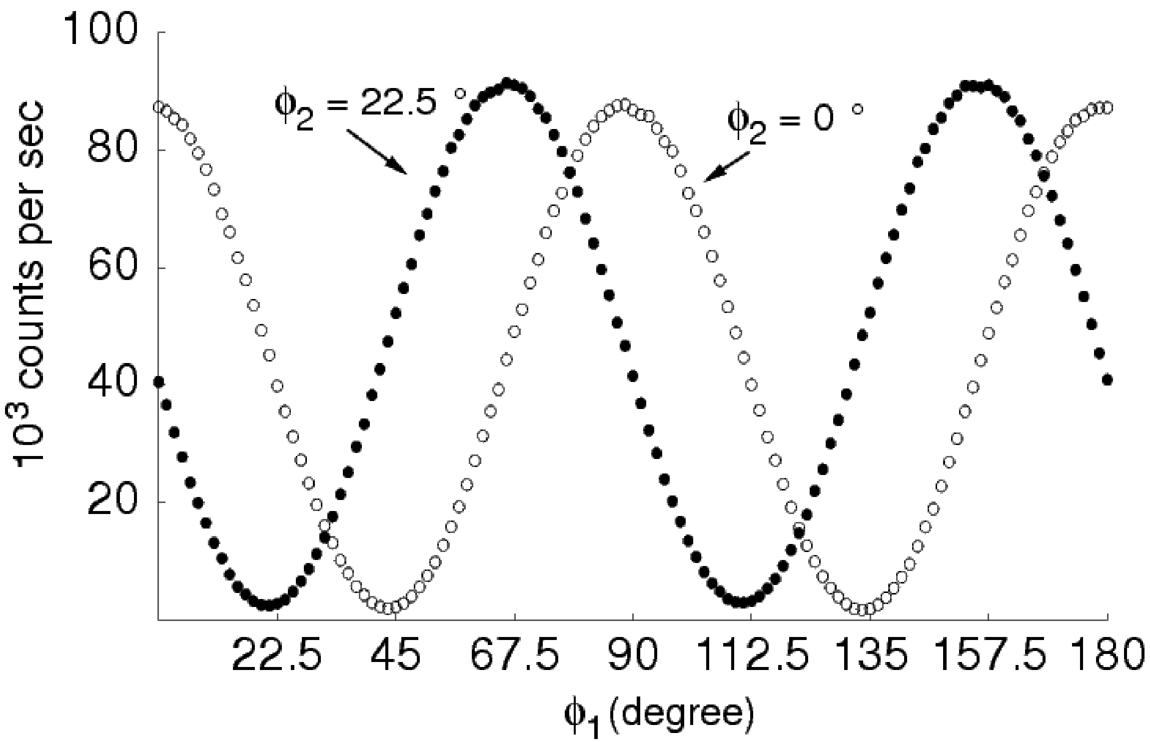
Pair and single rates



- high brightness by mode matching, observed pair/single ratio: 28%

Entanglement Quality

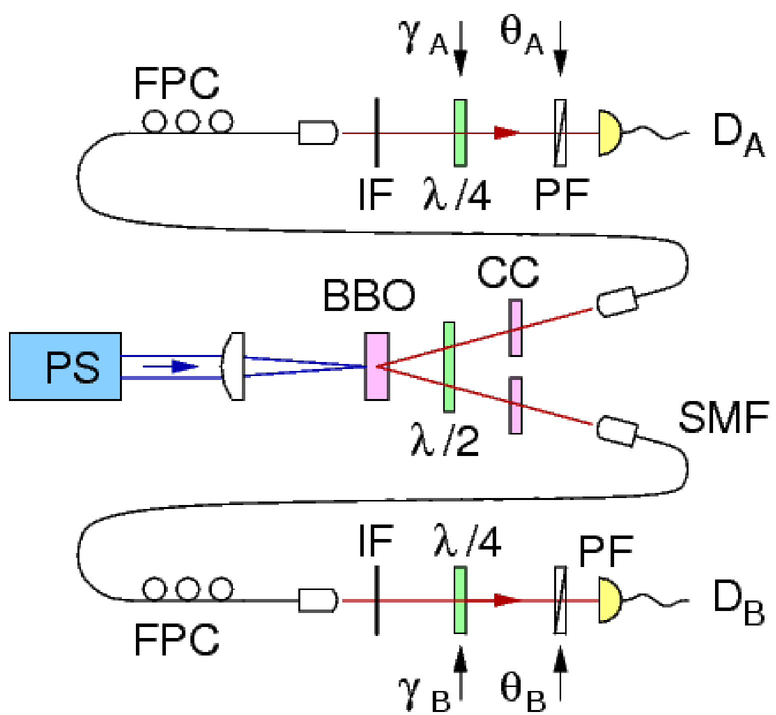


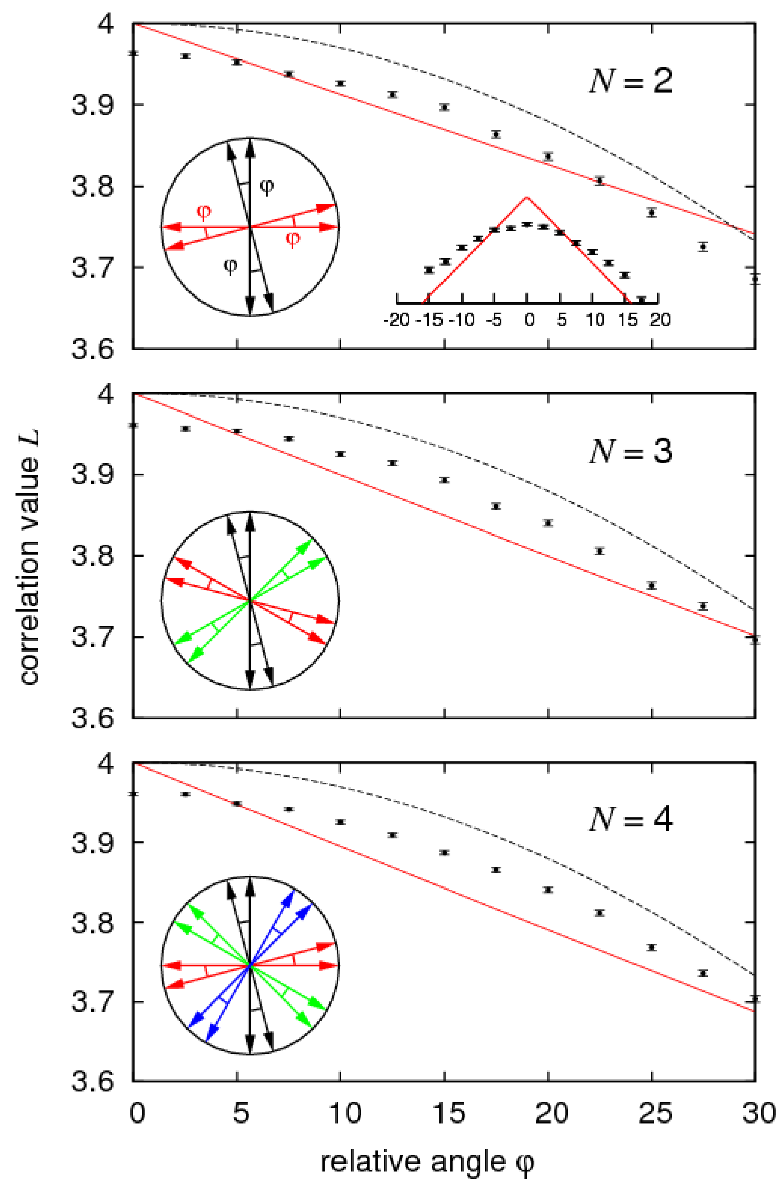


- Visibility of polarization correlations:
  HV: 98.2%, ±45deg: 96.3%
- Violation of a CHSH-type Bell inequality:
  S=2.6989±0034 (204 σ in 1sec/point)

Other experimental tests

- Visibility of Polarization correlation >99% in all bases
- Leggett-type inequalities for (nonlocal) hidden variable models

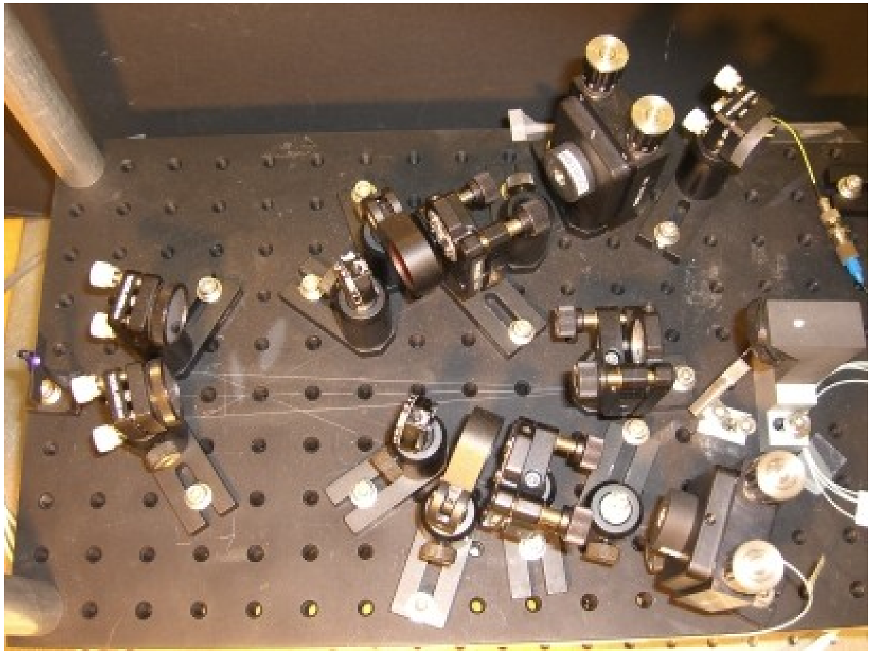


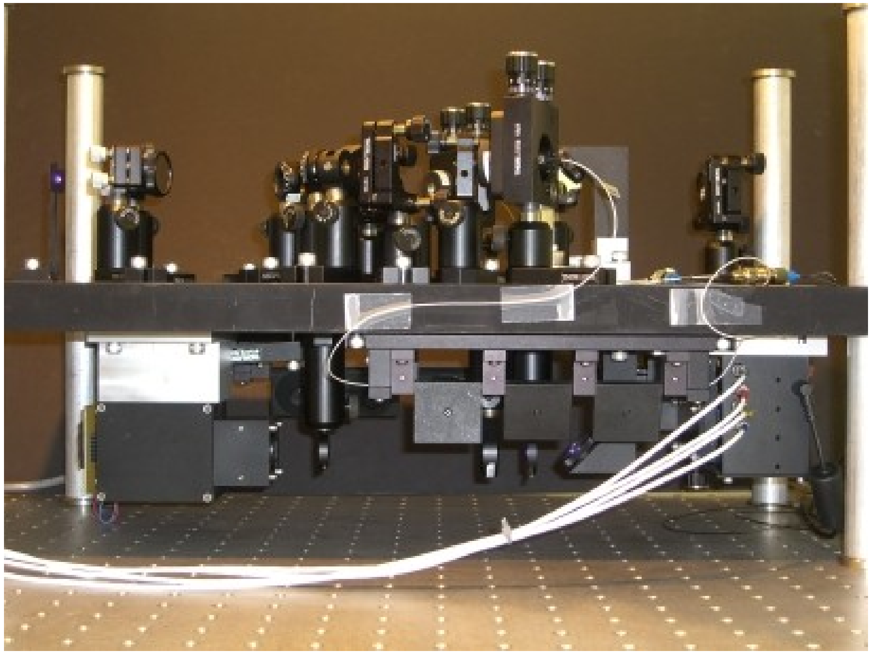


C. Branciard, A. Ling, N. Gisin, C.K., A. Lamas-Linares, V. Scarani, PRL ***99****, 210407 (2007)*

Practical pair source

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

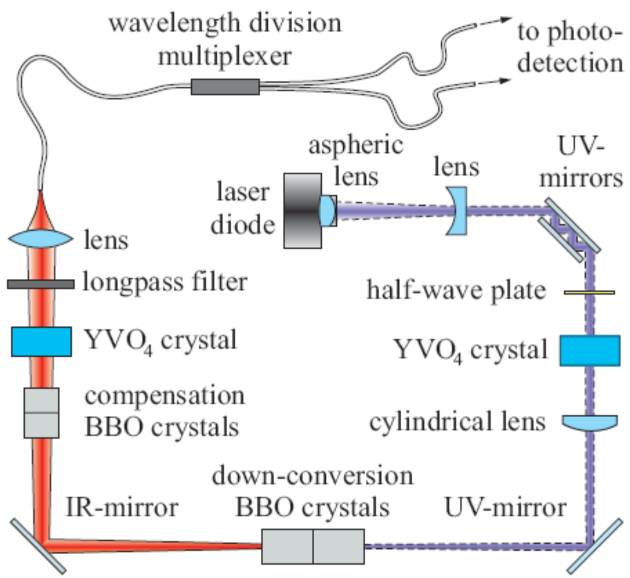




- 24,000 s^{-1} detected pairs from 40 mW pump @ 407nm in single mode fibers at 810/818 nm, 2mm BBO crystal
- polarization correlation visibility in 45° basis: 92%

Much better implementations

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%

Summary

- Make single qubits and qubit pairs
- Manipulate and transport photonc qubits
- Fundamental tests of quantum mechanics

  test Bell-type inequalities & friends

- Quantum communication

  quantum cryptography

Time for Coffee.....

Thank you !

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

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

Lecture 2: Aspects of Quantum Cryptography

Christian Kurtsiefer

Centre for Quantum Technologies

NUS National University of Singapore

Asher Peres International School, Chowder Bay @ Sydney, Nov 2008

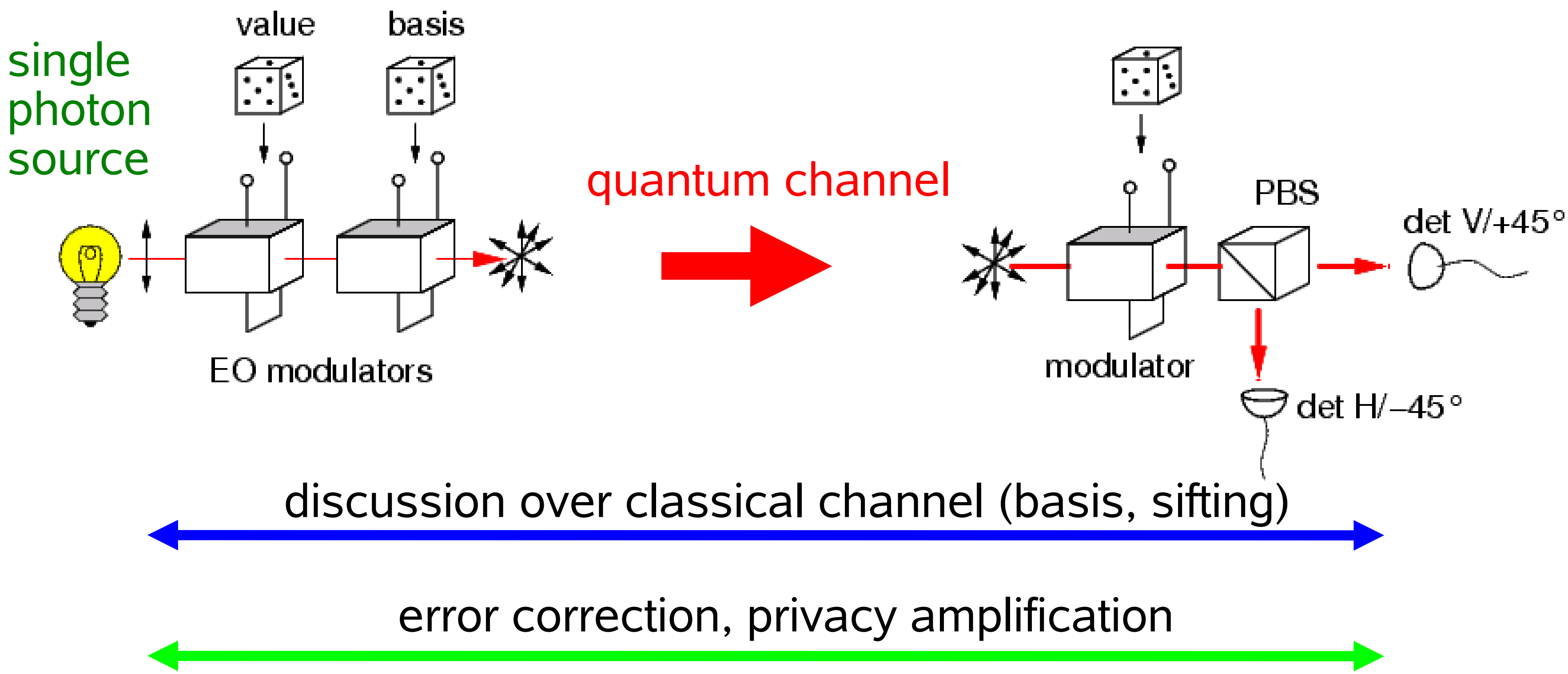
Quantum 'cryptography'

- better: quantum key distributoion
- even better: quantum key growing

- BB84 protocol
- Ekert protocol
- Device independent key distribution

BB84 protocol

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

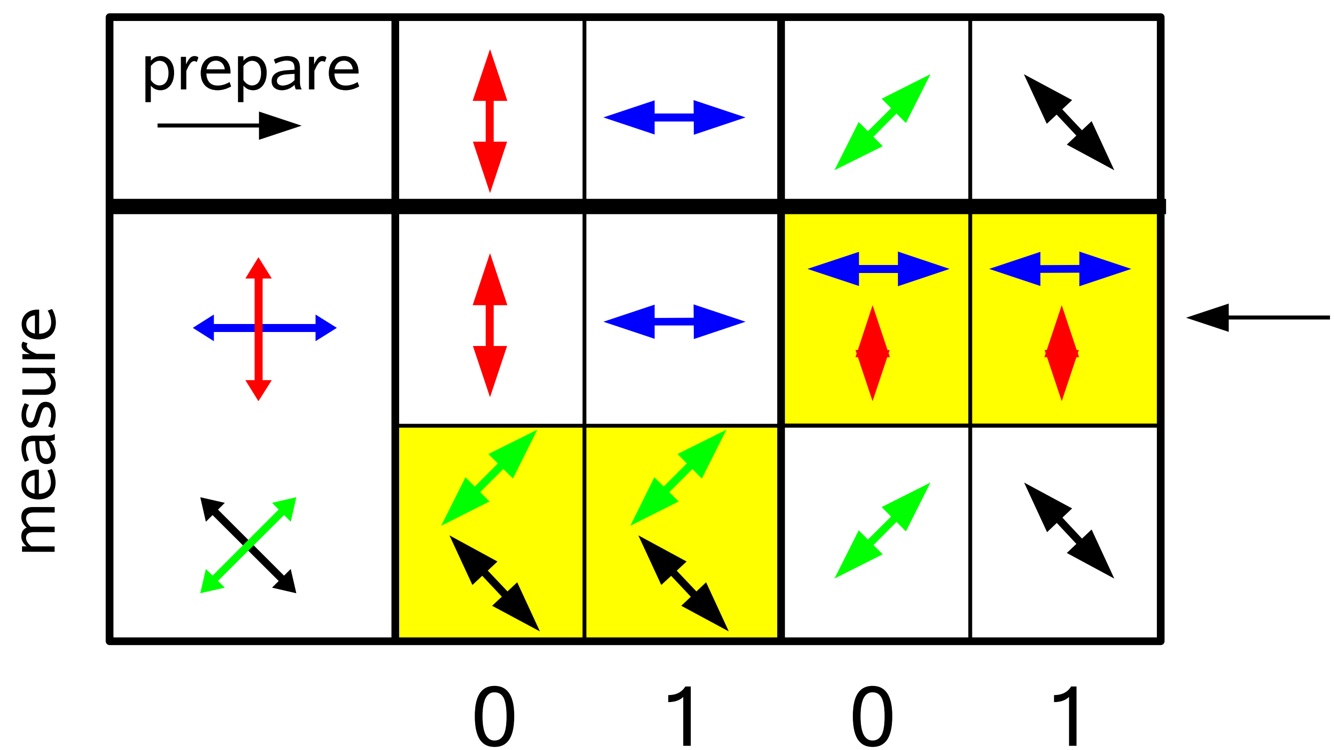


- uses error fraction to estimate eavesdropper's knowledge

Encoding information....

- ....works also with other perpendicular polarizations.....

- ....but you need correct measurement basis:



Heisenberg uncertainty principle:

random results

Error detection / correction

```
ALICE: 0111 0101 0101 0110 1010 0111 0101 .....

BOB:   0110 0101 0111 1110 1010 0111 0101 .....
```

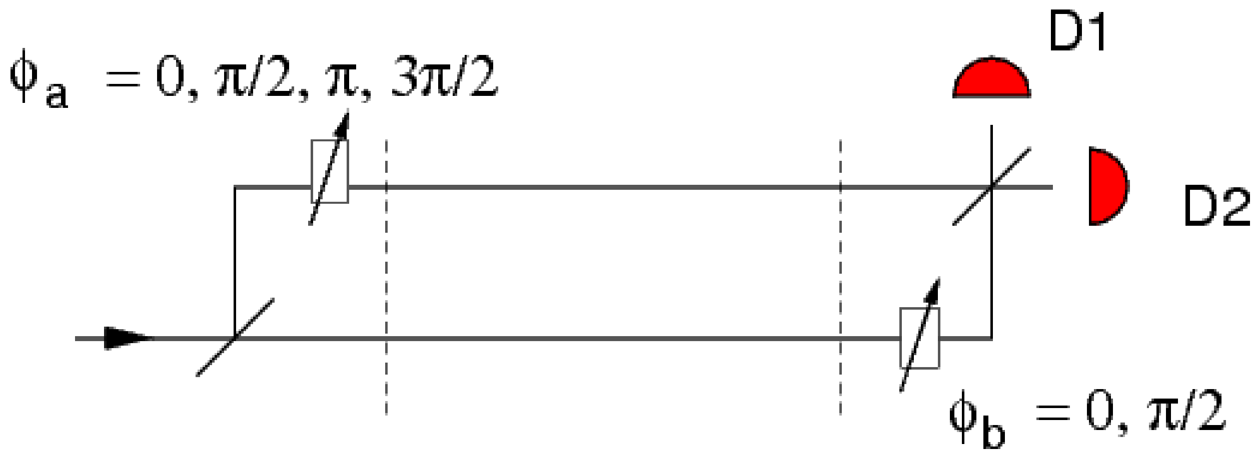
- Some errors are due to imperfect devices, detectors, background light etc.
- Some errors indicate an **eavesdropping attempt**
- Correct errors by discussing parity bits over blocks openly:

```
A->B:  p=1  p=0  p=0  p=0  p=0  p=1  p=0  .....

B->A:  ERR  OK   ERR  ERR  OK   OK   OK   .....
```

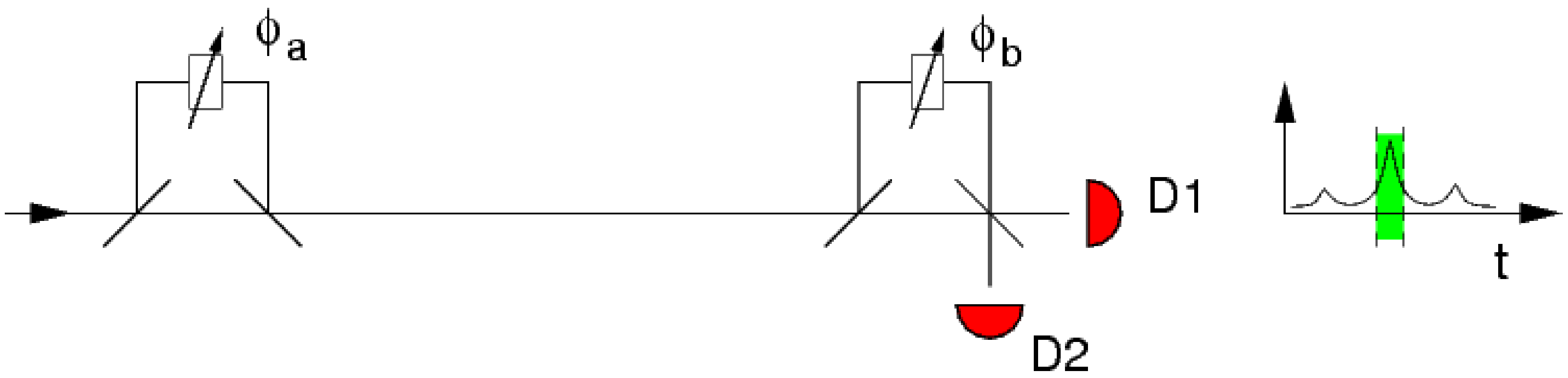
Other encoding techniques

- Encoding qubit in relative phase between two packets



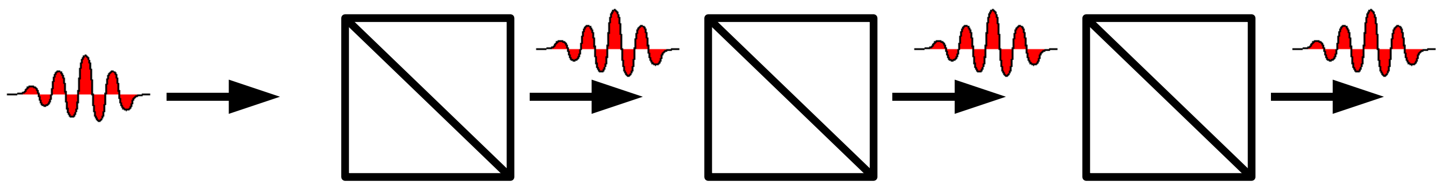
equivalent to polarization encoding

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

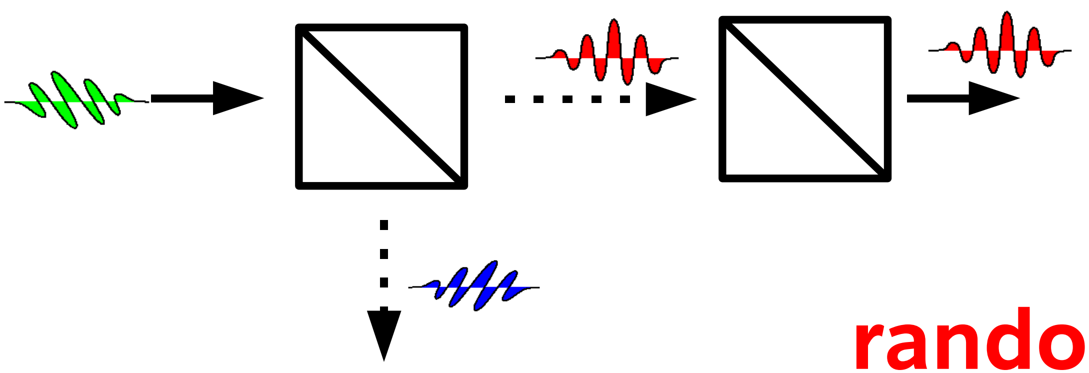


Consecutive measurements

- same basis: always same outcome



- different bases



random outcome at first PBS

Estimate Eve's knowledge

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

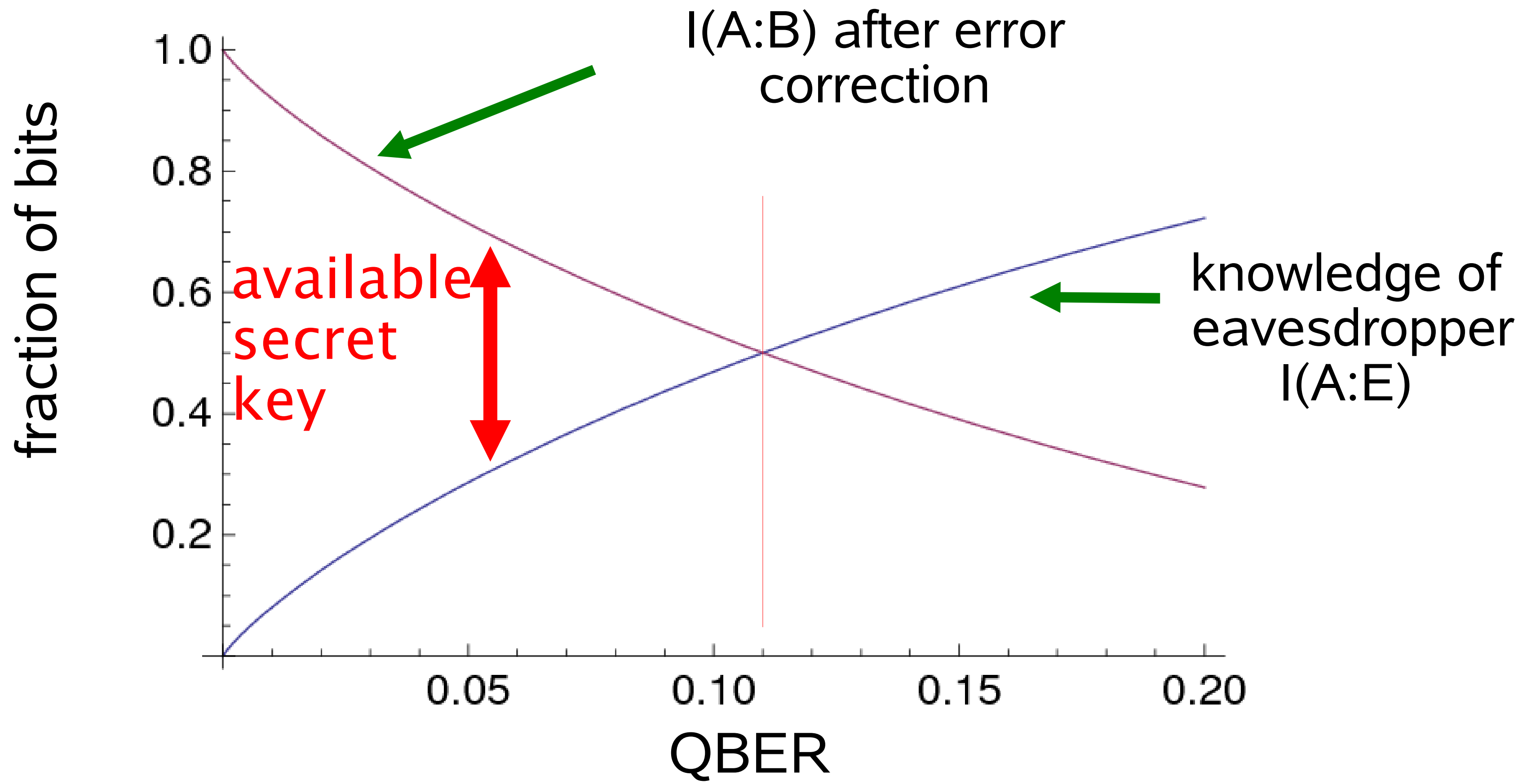
$$N_e = N_r \left(h(\eta) + h(\eta) \right)$$

possible knowledge of an eavesdropper due to measurements

revealed in (optimal) error correction

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

Estimate Eve's knowledge



* depends on the attack model (individual attack);
for *infinite* key length and (!) single photons

Privacy amplification

NUS National University of Singapore

- compress raw key to the information advantage vs. Eve..

$$\underbrace{\begin{bmatrix}0\\1\\0\\1\end{bmatrix}}_{\text{final key}} = \underbrace{\begin{pmatrix}0&1&0&1&1&1\\1&0&1&1&0&0\\0&1&1&0&1&1\\1&0&1&1&0&1\end{pmatrix}}_{\text{hash matrix}} \times \underbrace{\begin{bmatrix}1\\0\\1\\1\\1\\0\end{bmatrix}}_{\text{raw key, no errors}}$$

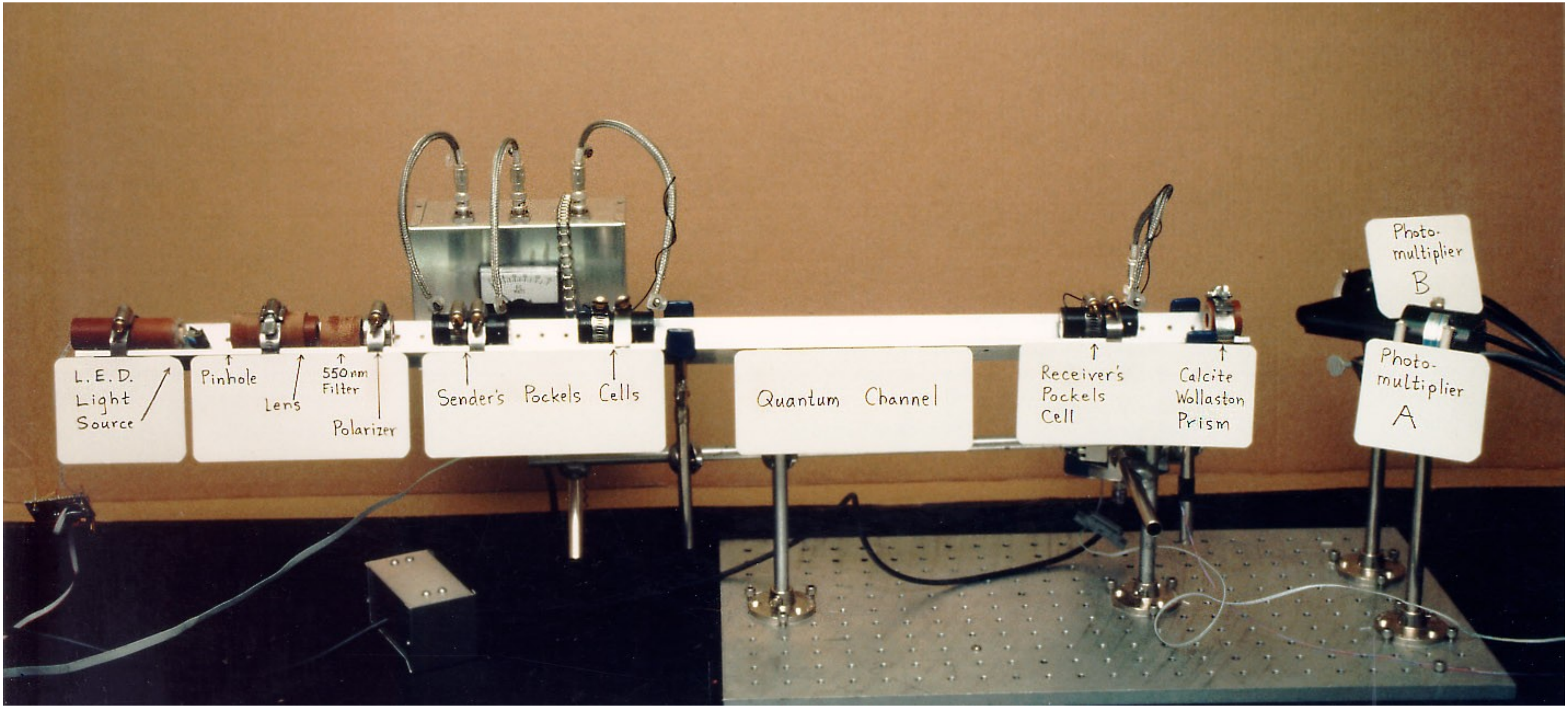
Eve may know this

- All information leakaged 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

BB84 original implementation

NUS
National University of Singapore



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

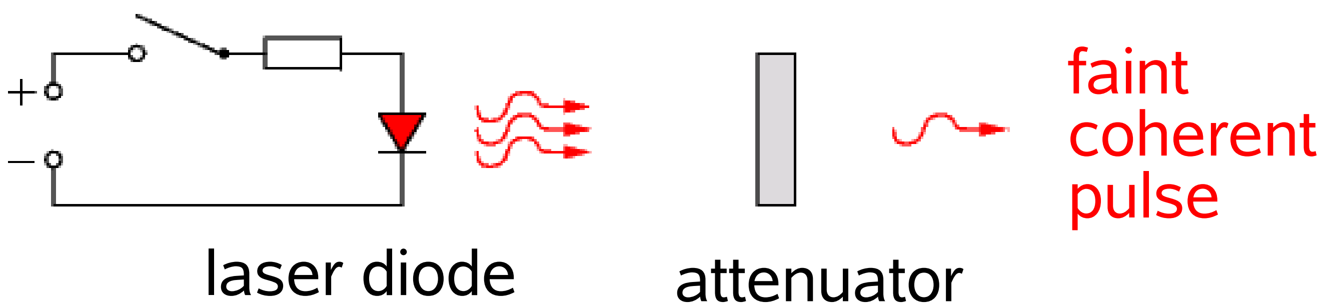
Imperfect 'single photons'

- use faint coherent pulses instead of single photons

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

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

- much simpler to prepare than true single photons:

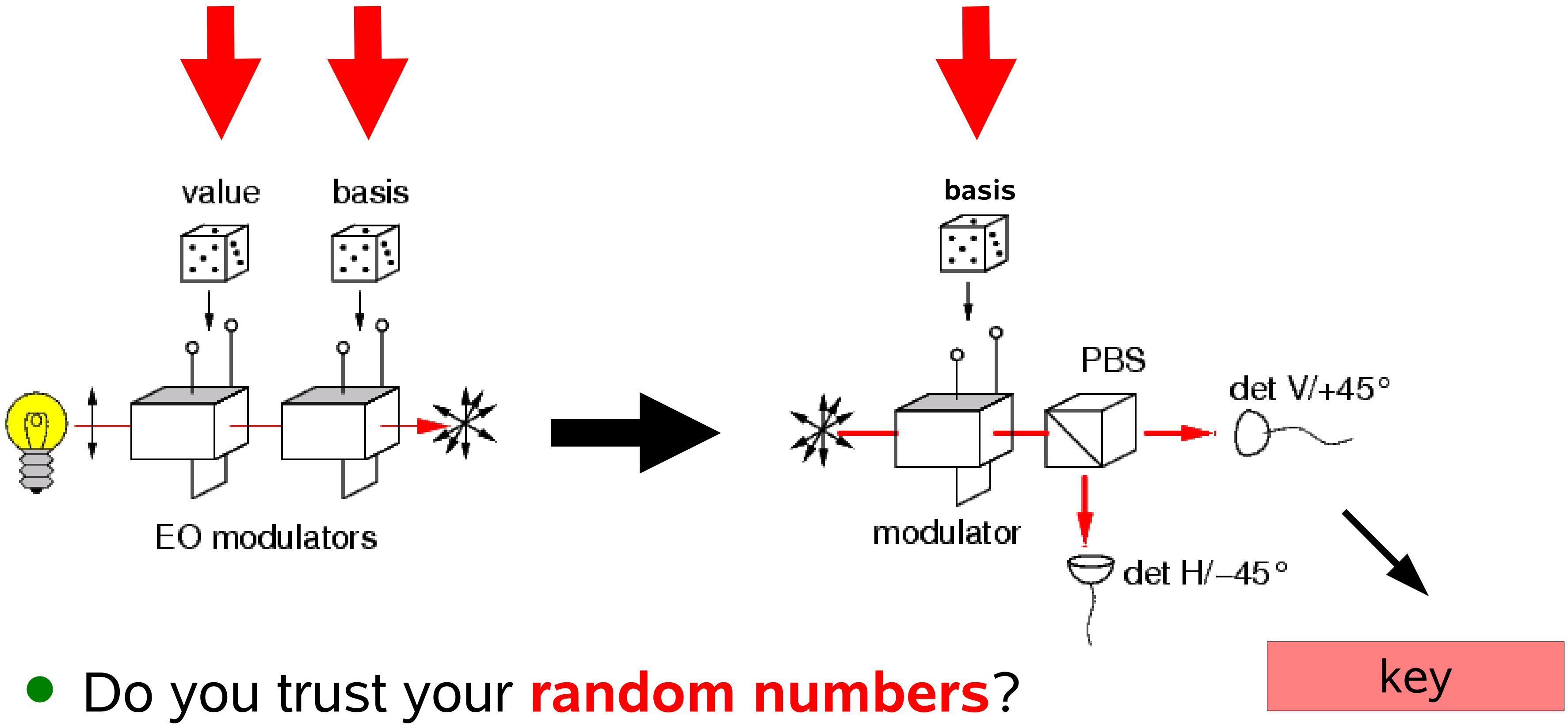


- potentially insecure: photon number splitting attack
---> decoy state protocol

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

A Prepare & Send problem:

...needs lots* of trusted random numbers!

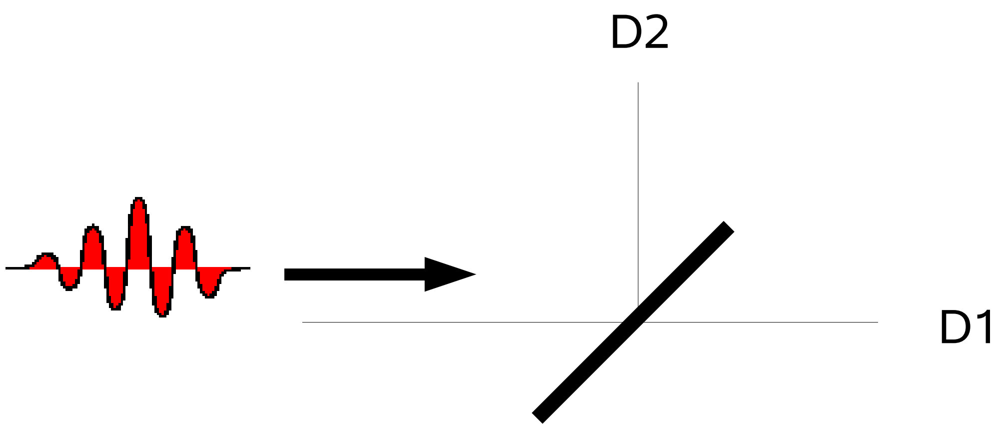


- Do you trust your **random numbers**?

*Mbit/sec for kbit/sec key

Quantum Random numbers

- use beam splitters and single (post-selected) photons



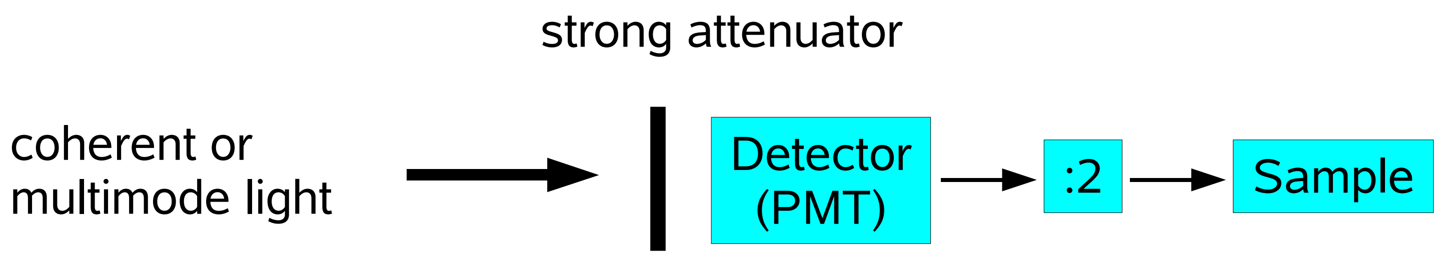
J.G. Rarity et al., J. Mod. Opt. 41, 2345 (1994)

T. Jennewein et al., Rev. Sci. Inst. 71, 1675 (2000)

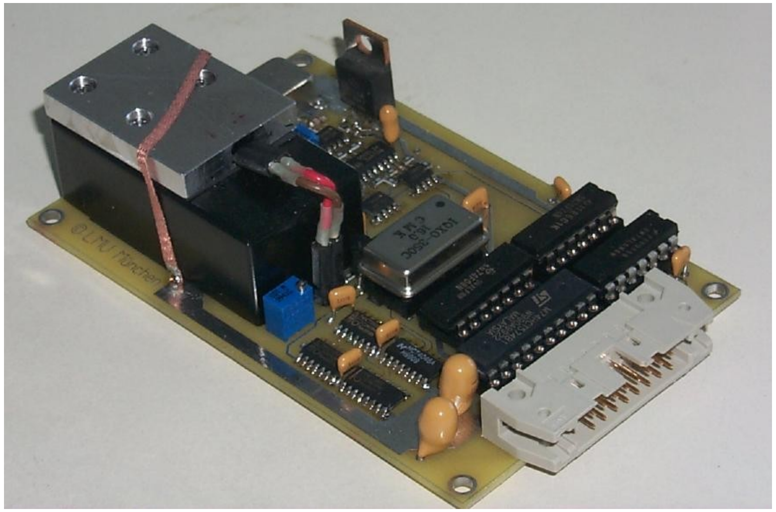
- need to remove bias, two detectors

Quantum RNG II

- extract Poissonian photon statistics

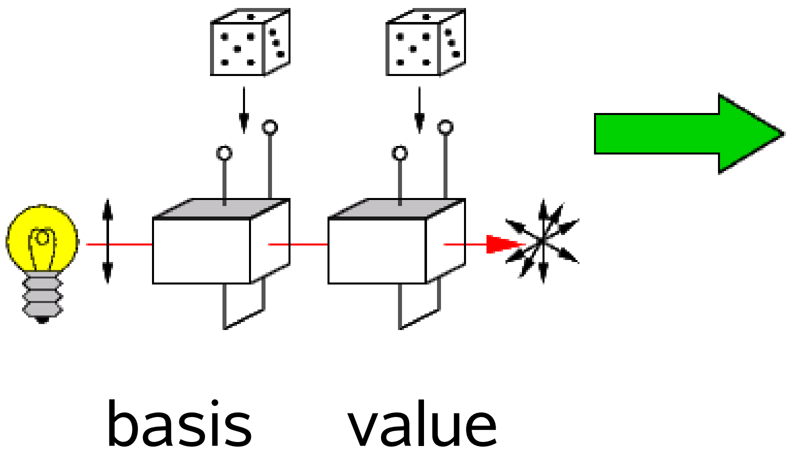


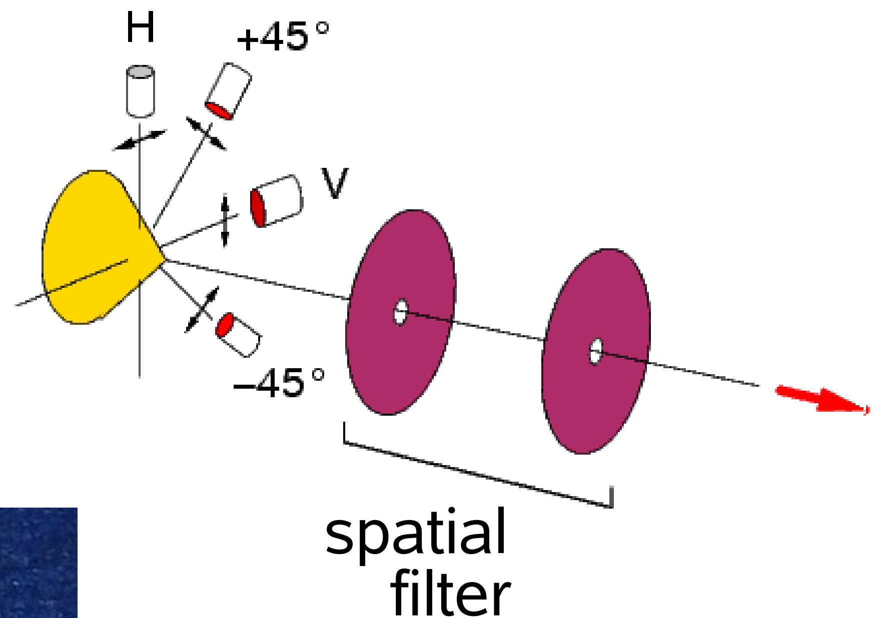
- 20 Mbit/s

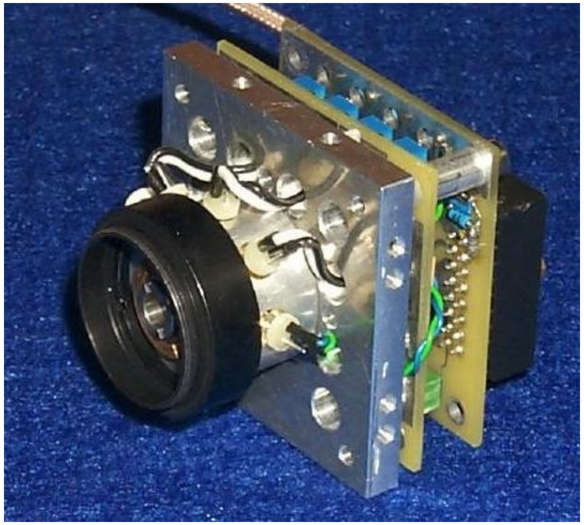


Preparation of polarized photons

- Make use of good intrinsic polarization of laser diodes

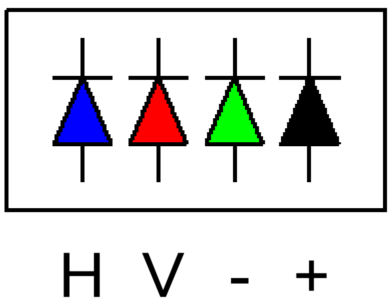


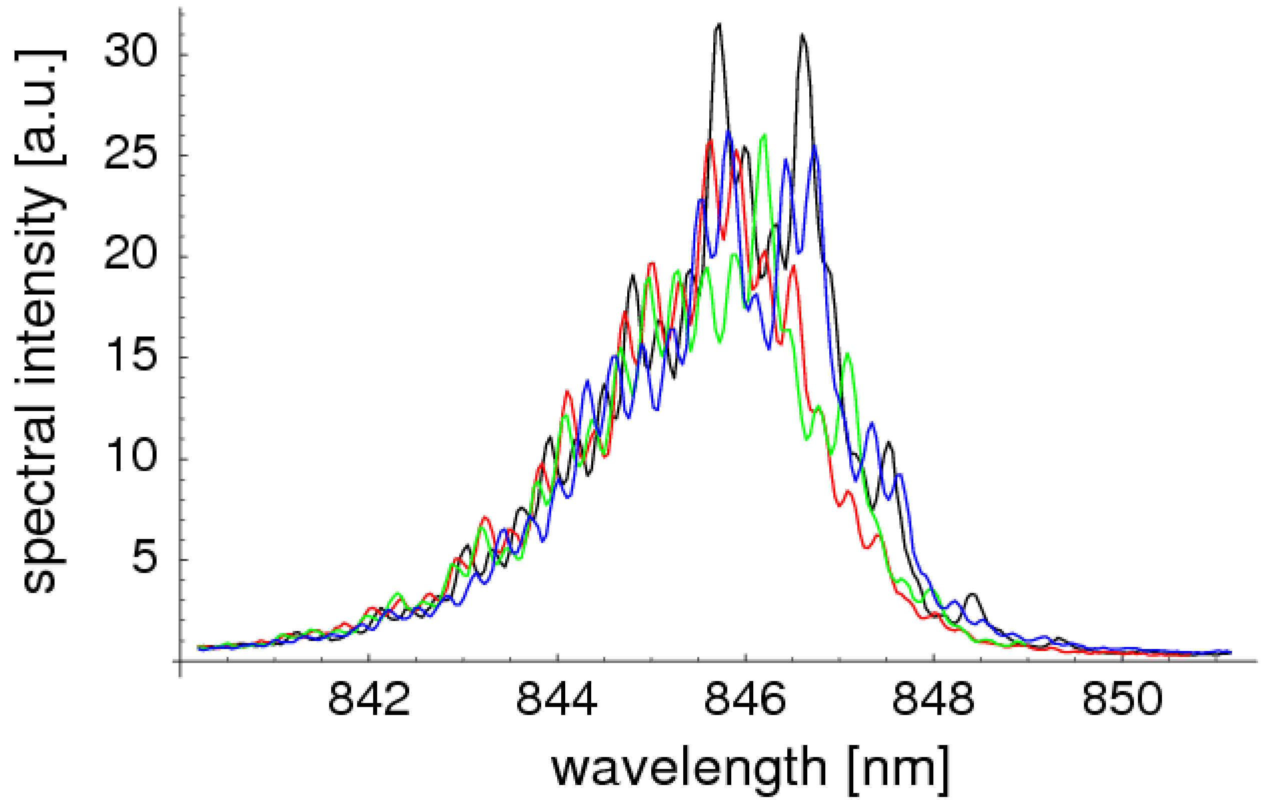




BB84: Spectral attack

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



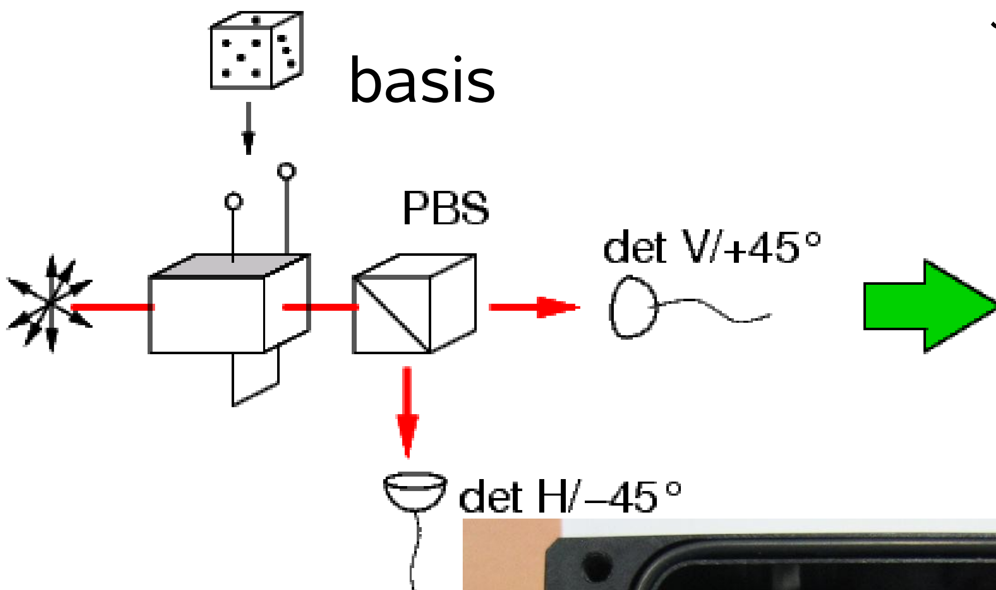


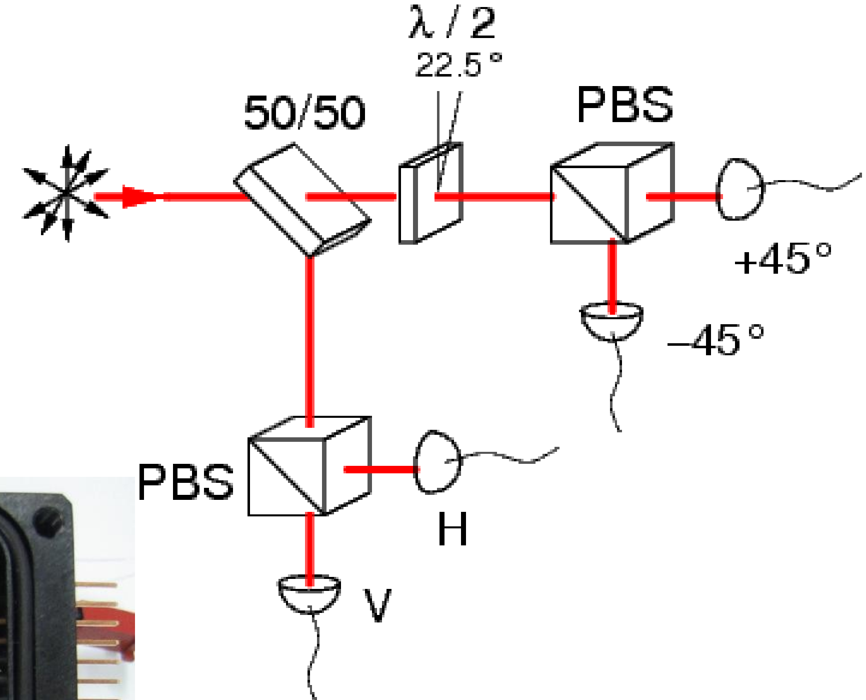
asymptotic
average
information
leakage: <2%

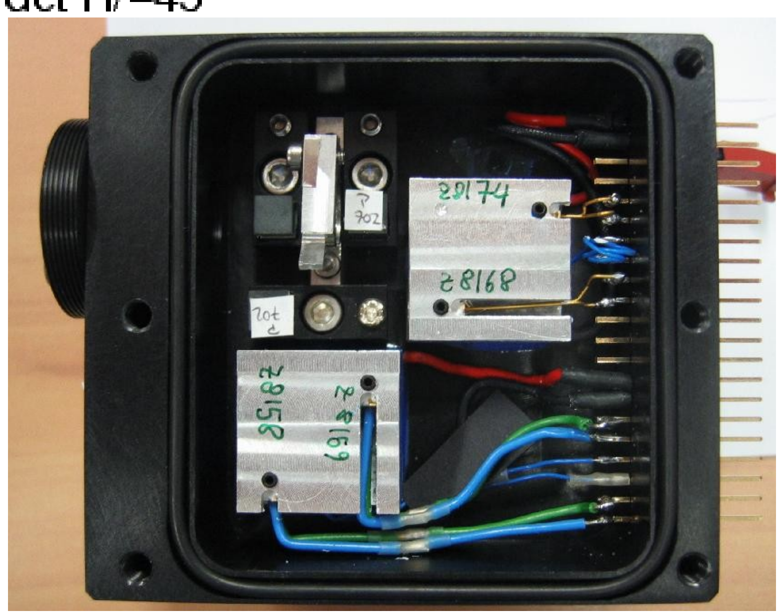
Polarization measurement

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

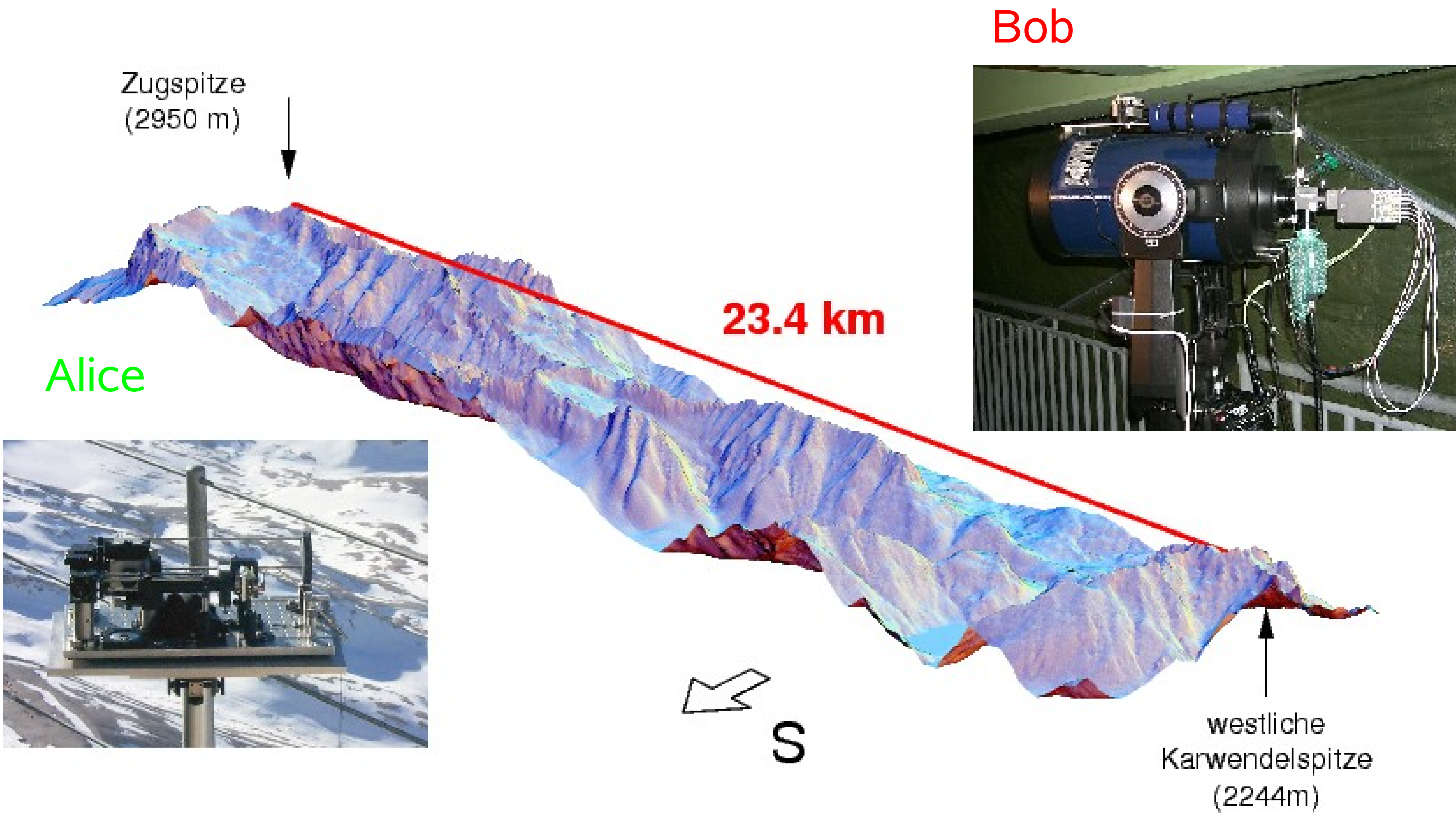
J.G. Rarity, P.C.M. Owens, P.R. Tapster, J. Mod. Opt. ***41****, 2345 (1994)*







Bridging distances

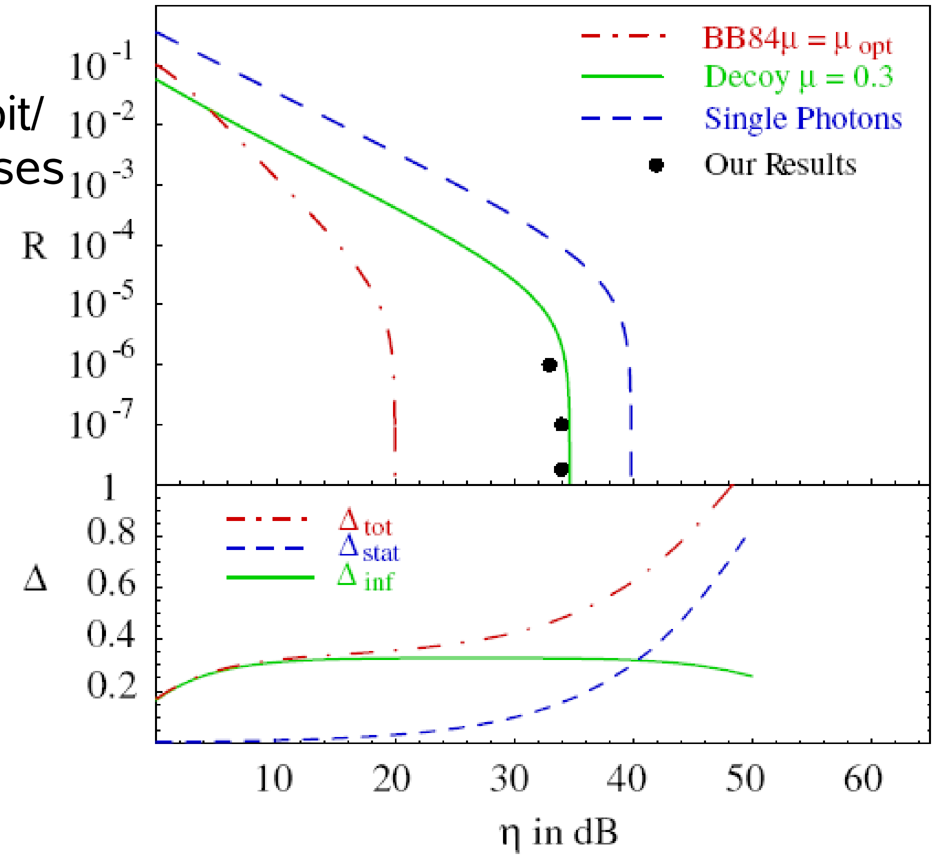


C. K., P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature ***419****, 450 (2002)*

Even further....

- use decoy states to reveal an eavesdropping attempt in a high loss regime

secure bit/ sent pulses

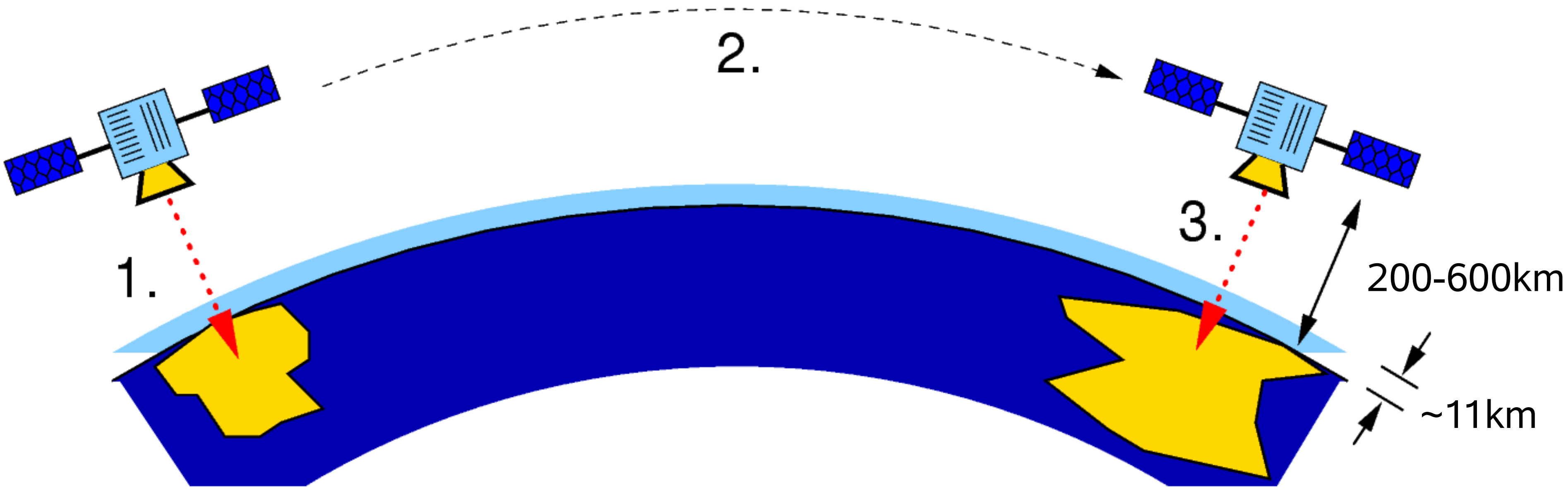


optical loss

T. Schmitt-Manderbach et al., Phys. Rev. Lett. ***98****, 010504 (2007)*

Go Global

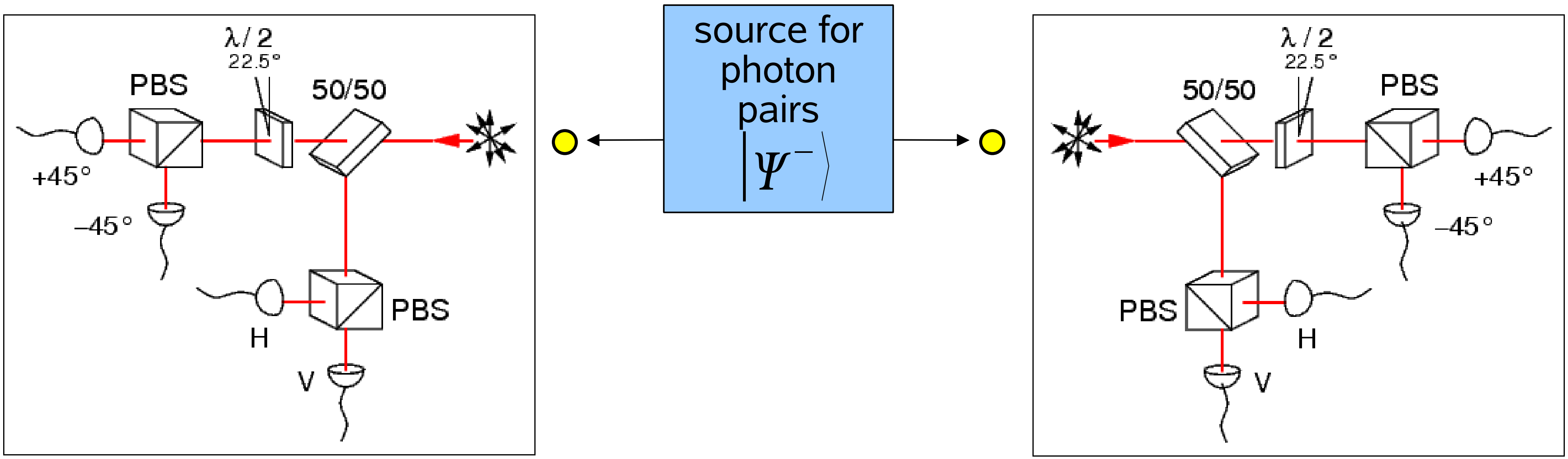
- Use satellites as trusted relays between distant locations



- .....but why should you trust it?

QKD with photon pairs: BBM92

Quantum correlations & measurements on both sides



public discussion (sifting, key gen / state estimation)

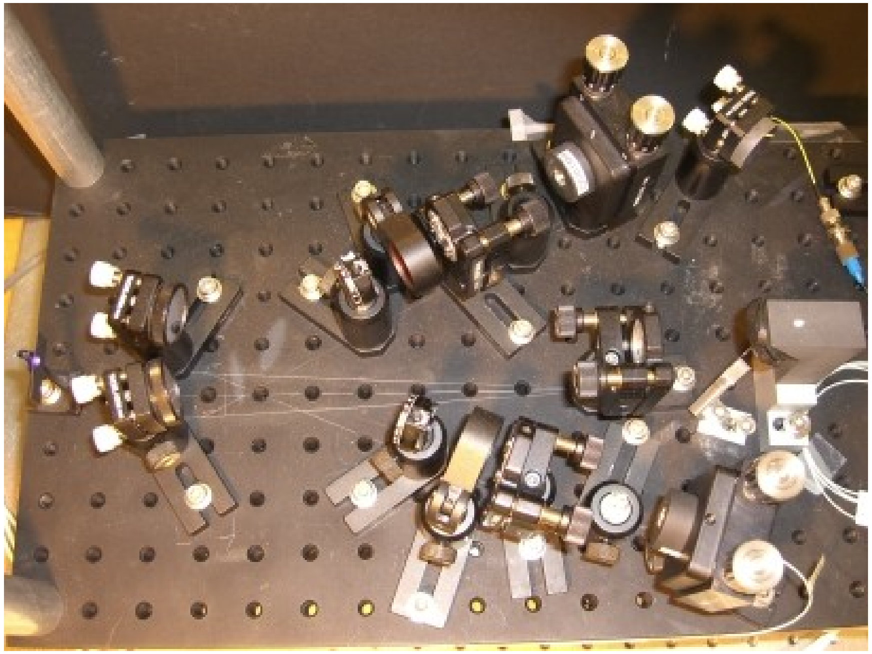
error correction, privacy amplification

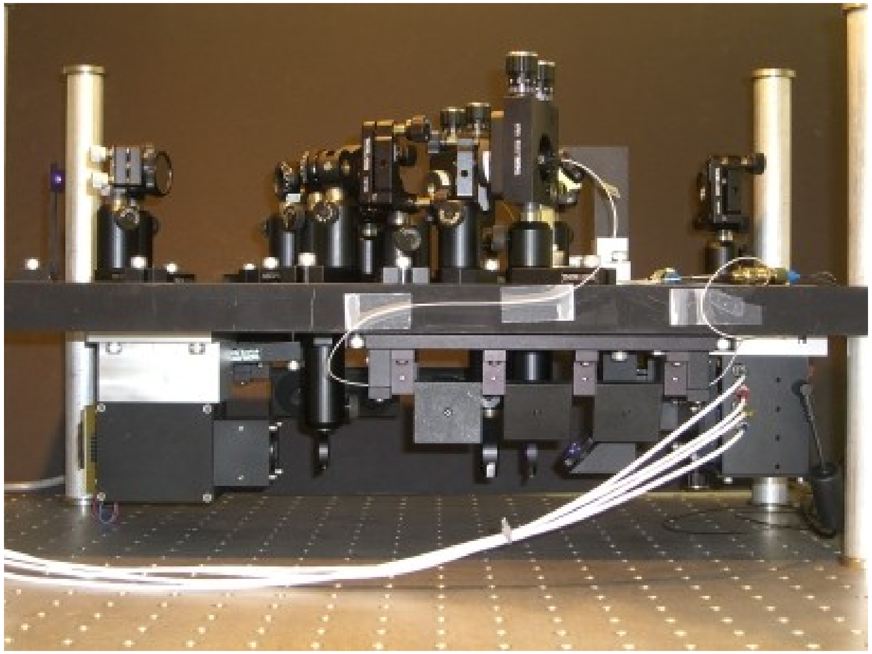
- no trusted random numbers for key
- direct use of quantum randomness for measurement basis

Practical pair source

NUS National University of Singapore

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



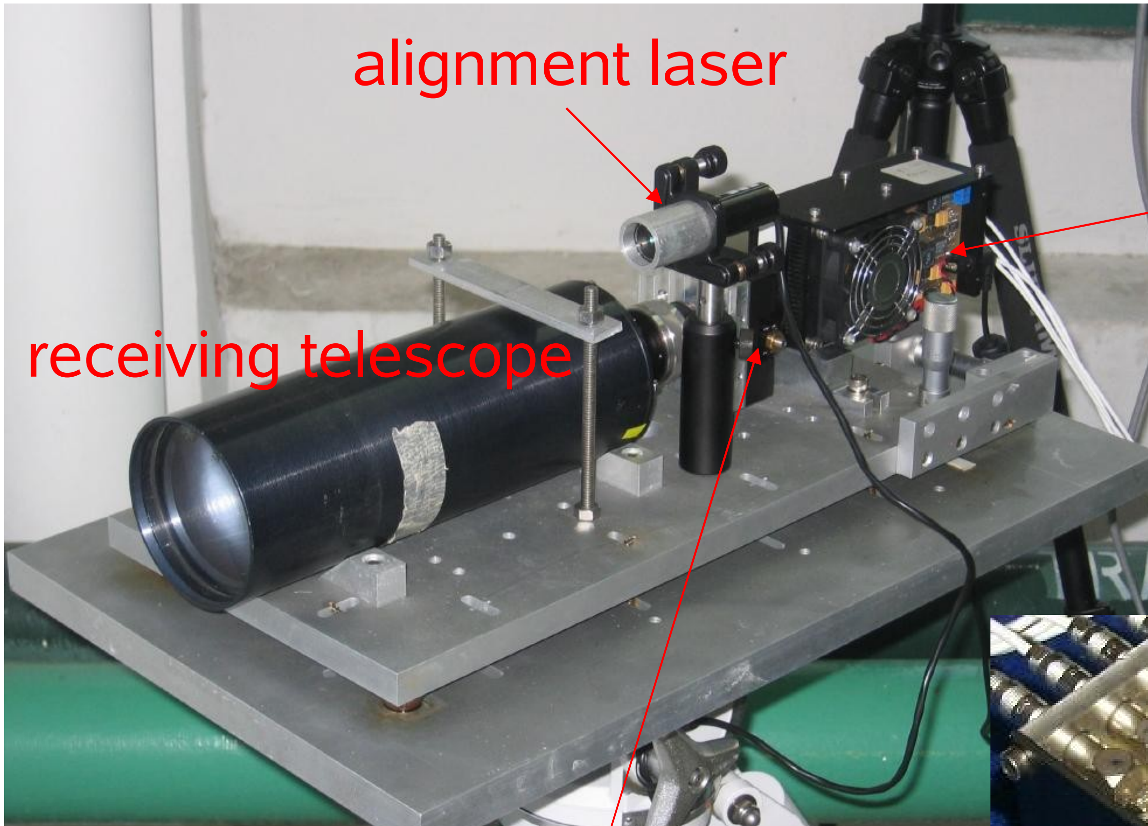


- 24,000 s^{-1} detected pairs from 40 mW pump @ 407nm in single mode fibers at 810/818 nm, 2mm BBO crystal
- polarization correlation visibility in 45° basis: 92%

NUS campus test range

Receiver unit

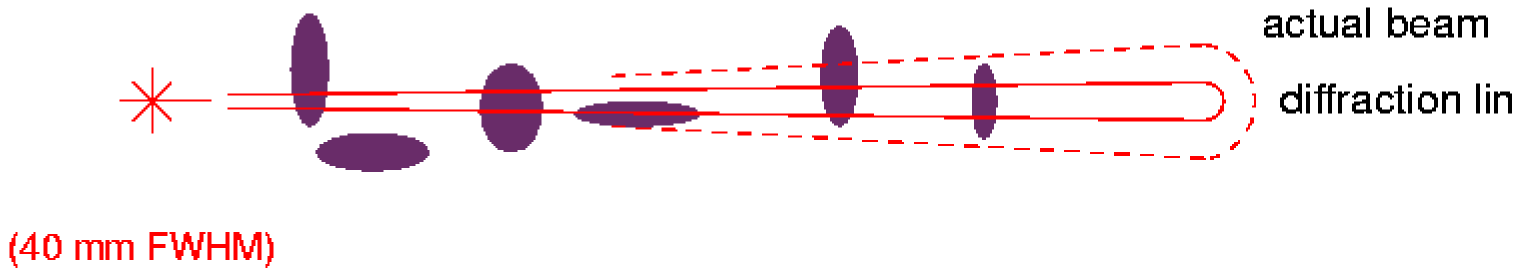
NUS
National University of Singapore

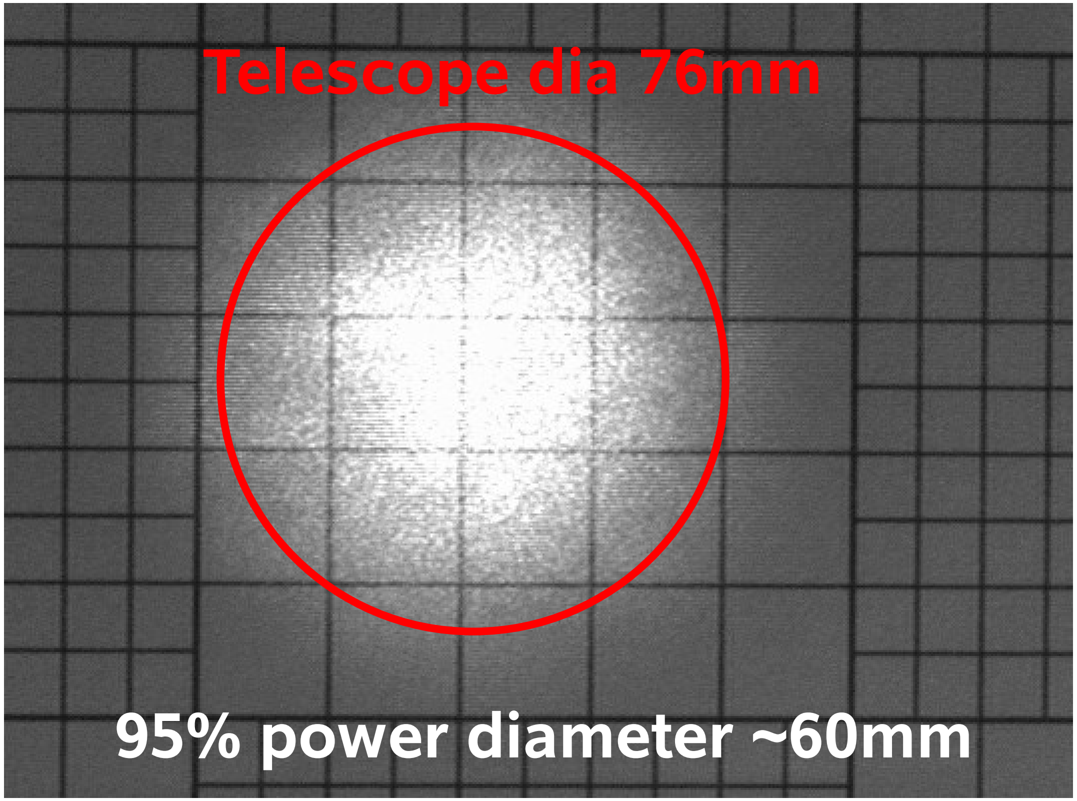


spatial filter (150 μrad)

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

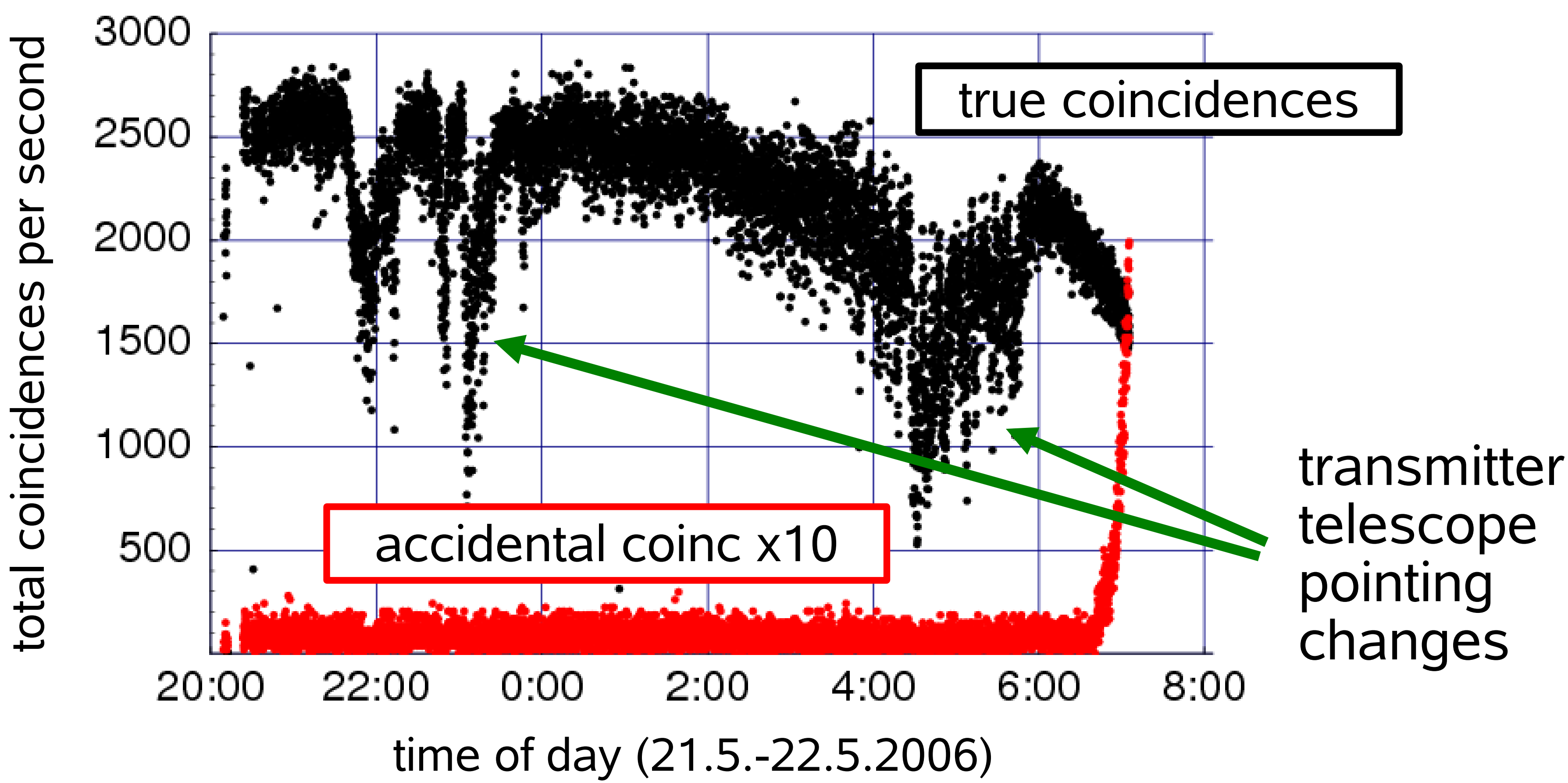
Scintillation in atmosphere





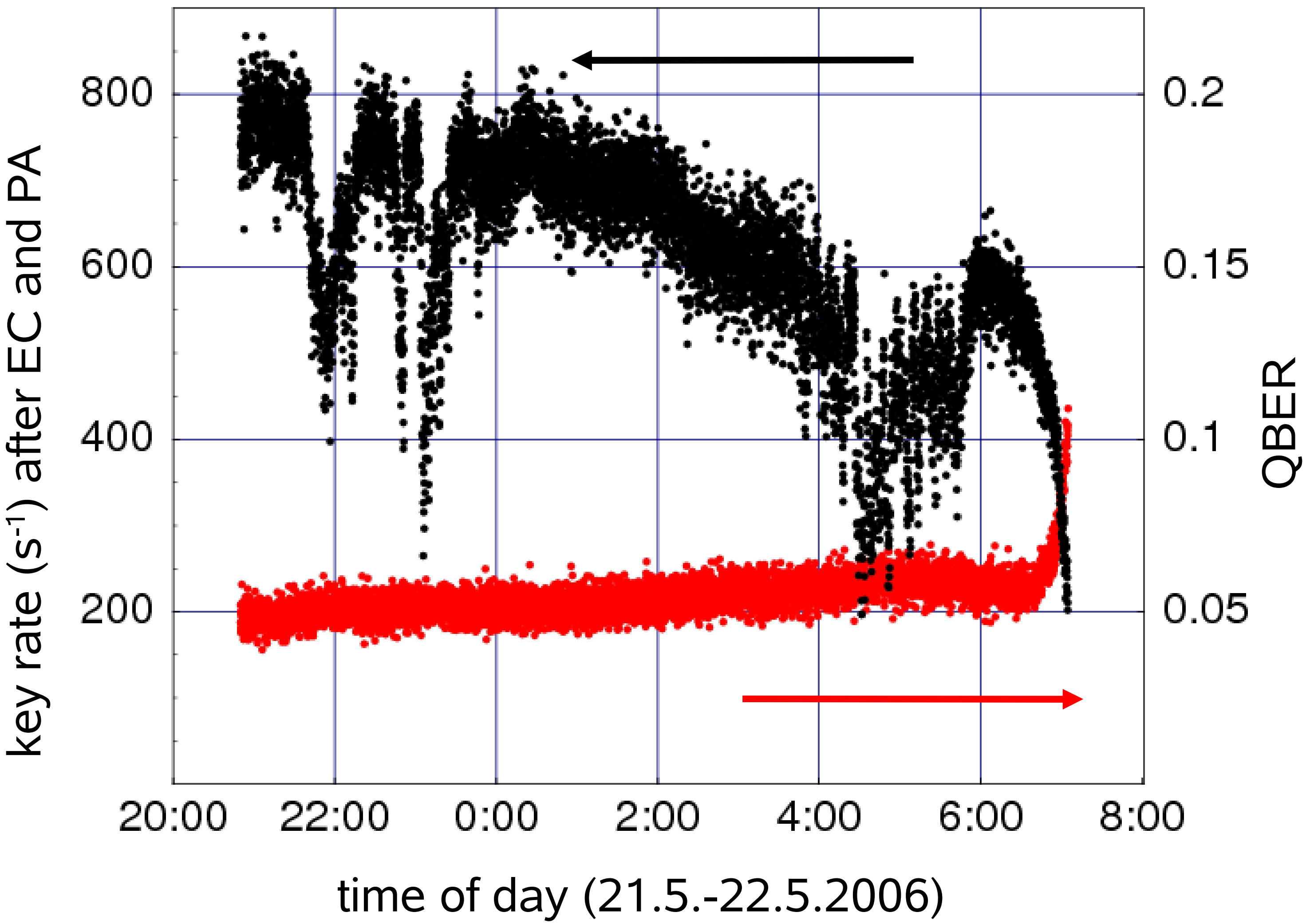
Experimental results I....

Identified raw coincidences between close and remote receiver



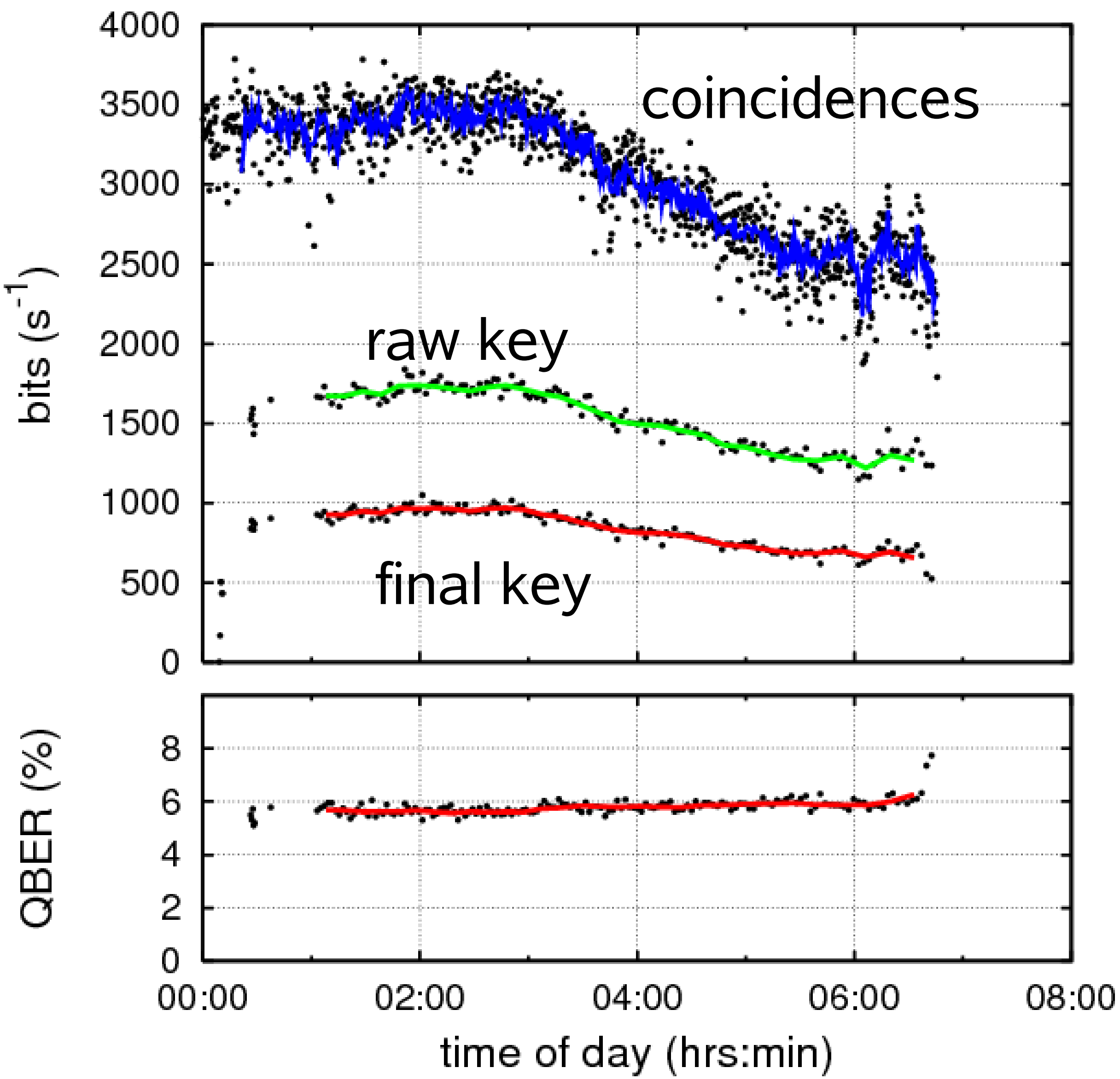
(with interference filter 5nm FWHM, 50% peak transmission)

....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
- residual error rate ~10^{-6} due to a stupid error

No interference filter



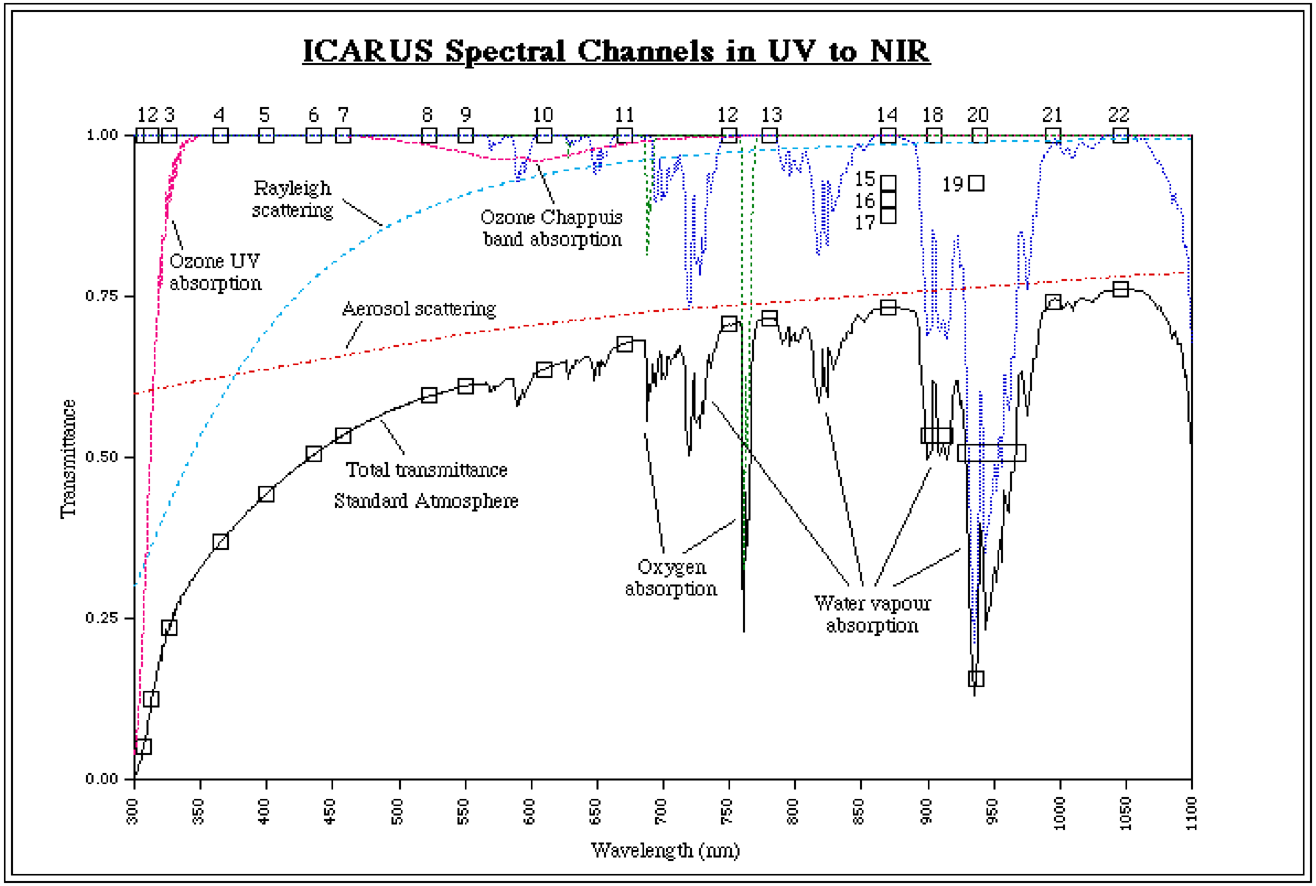
(data taken 1.6.2006)

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

(link loss 8.3 dB)

Atmospheric absorption

- representative vertical atmoshpere layer (corresponds to ~11 km air on ground)

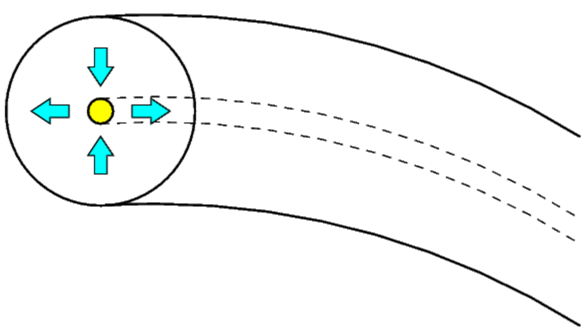


Optical fibers as 'channel'

- Use existing telecom infrastructure
- independent of environment
- high transmission:

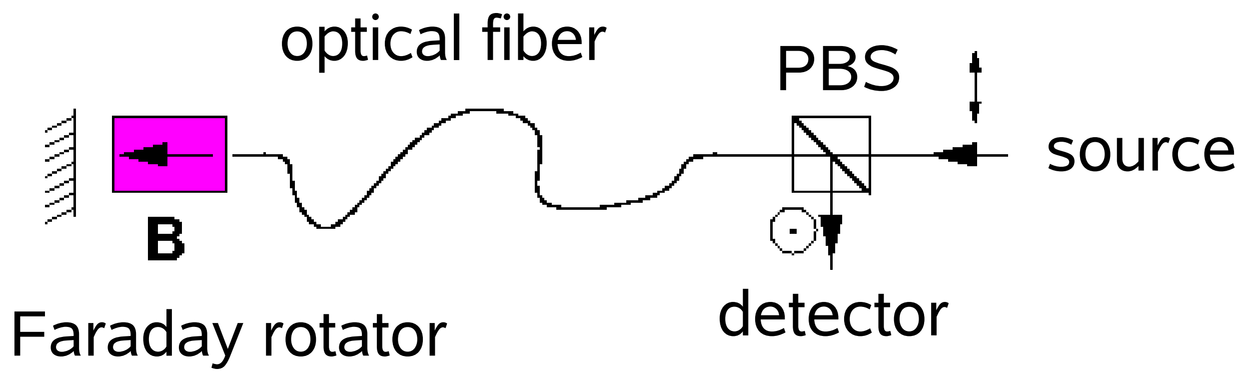
800nm:	2dB/km	(T=63% in 1km)
1310nm:	0.2dB/km	(T=63% in 10km)
1550nm:	0.35dB/km	(T=44% in 10km)

- stress birefringence and geometric phases are time dependent:



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

Compare figures of merit

- 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

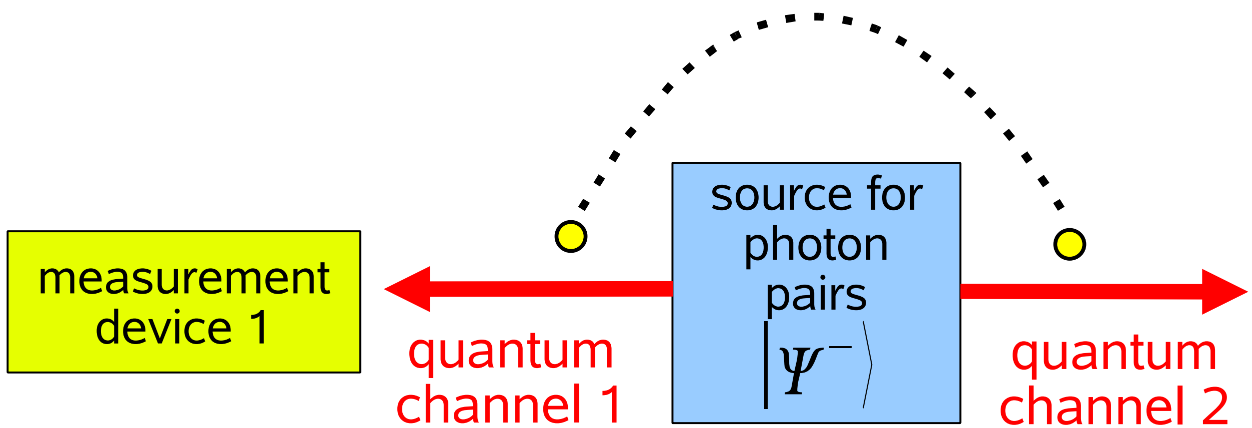
Si: 10^{-7}
InGaAs: 10^{-5}

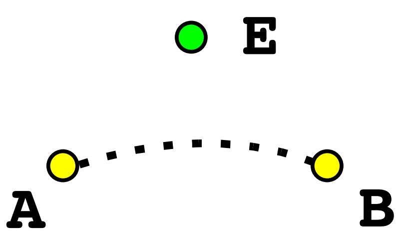
- detector-induced bit error ratio

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

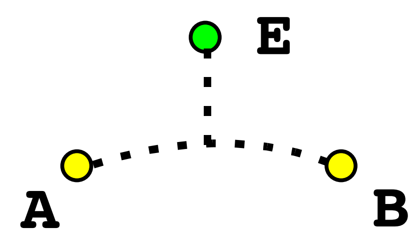
Entanglement based protocols

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



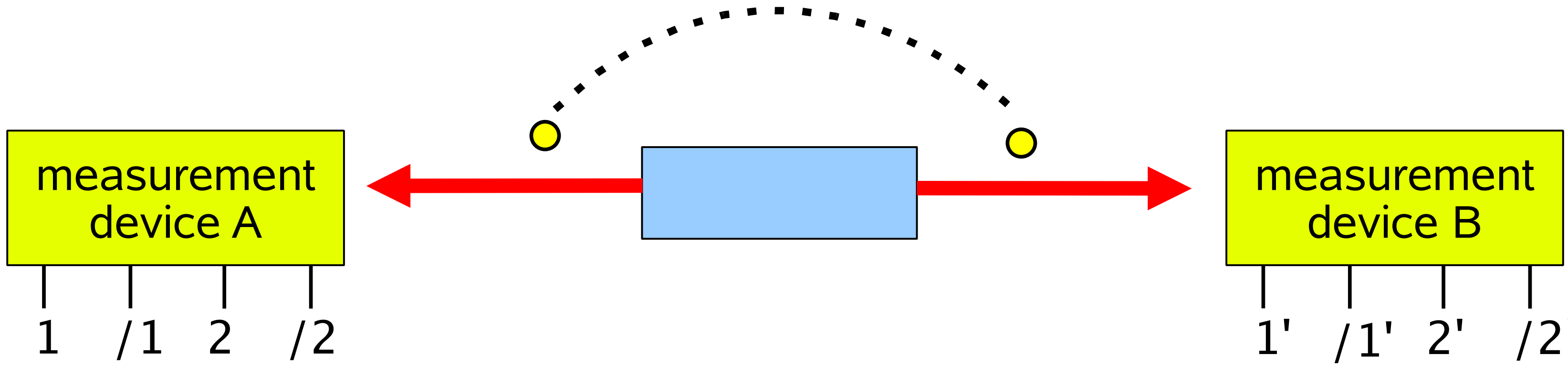


maximal entanglement between **A** and **B**



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

Bell inequality I

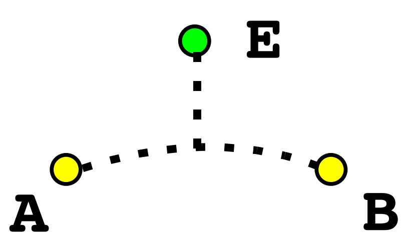


Correlation between setting i, j:

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

combined correlation function:

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

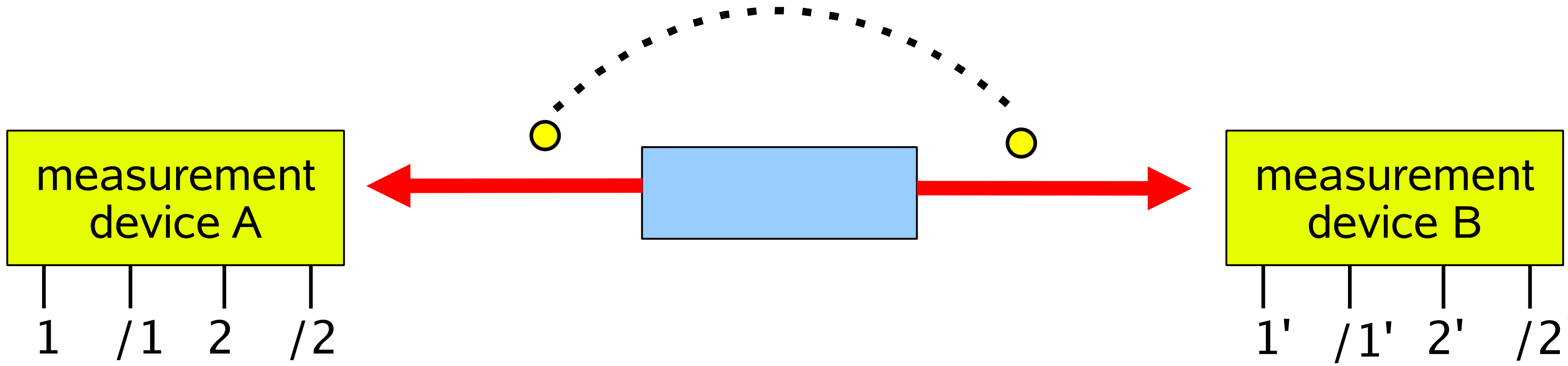


If there is a local hidden parameter λ (= knowledge of **E**) governing the measurement outcomes of **A** and **B**, then:

$$|S| \leq 2$$

Bell inequality II

NUS National University of Singapore



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:

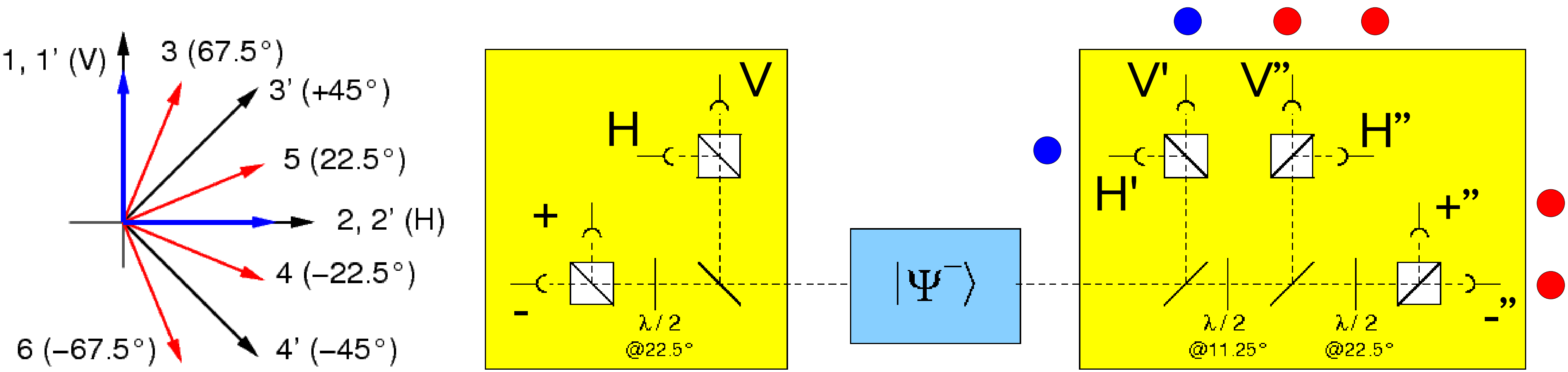
$$I_E(S) = h\left(1 + \frac{\sqrt{S^2/4 - 1}}{2}\right)$$

- 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

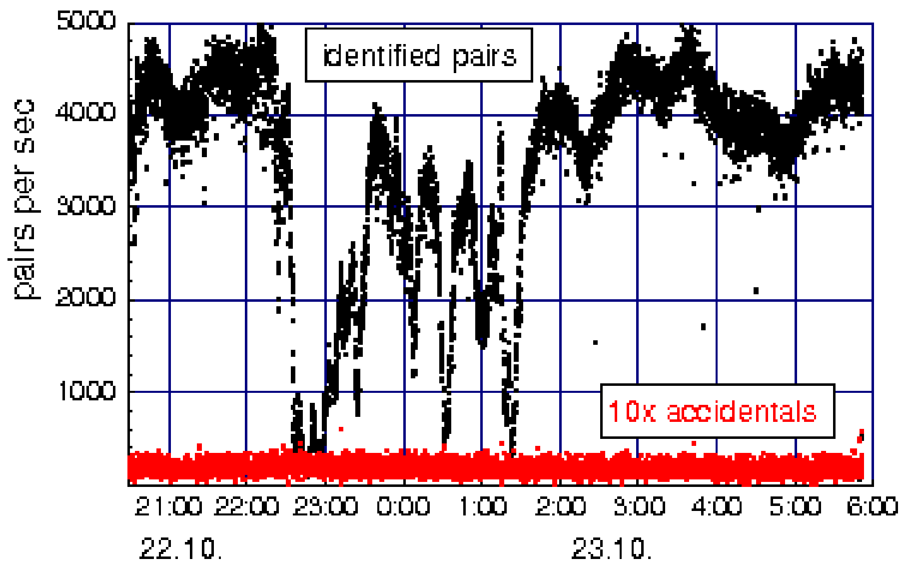
- use almost same kit:

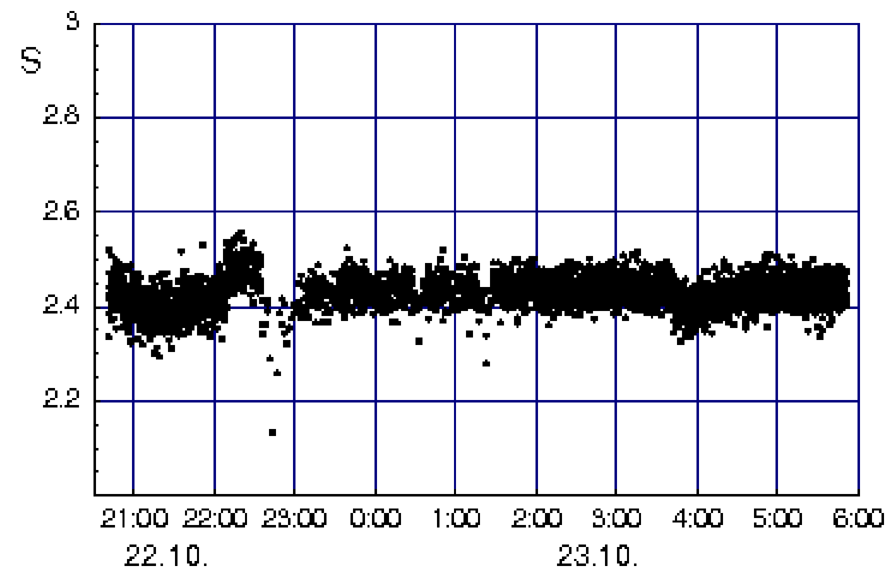


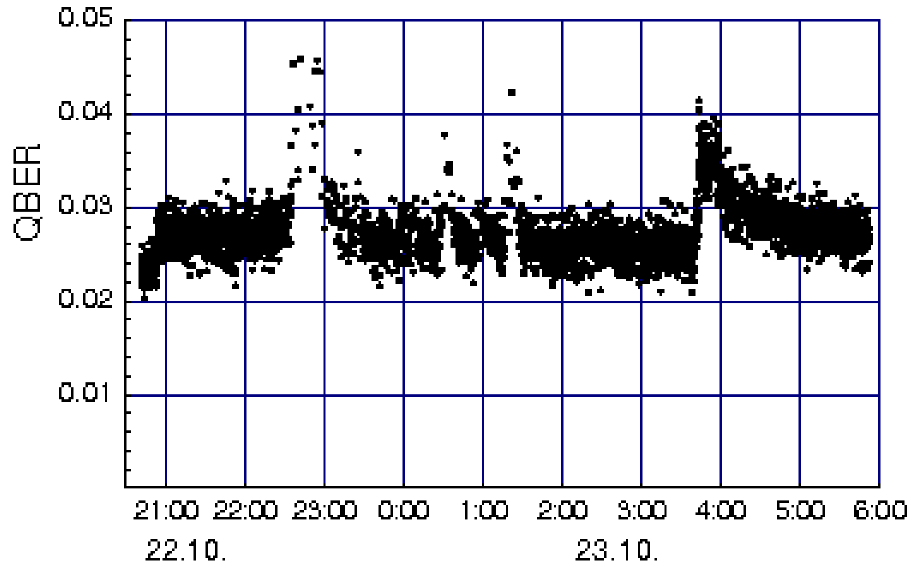
- {H,V; H',V'} coincidences → key generation
- {H,V,+,-;H",V",+",-"} coincidences → CHSH Bell test
- low QBER with existing simple source

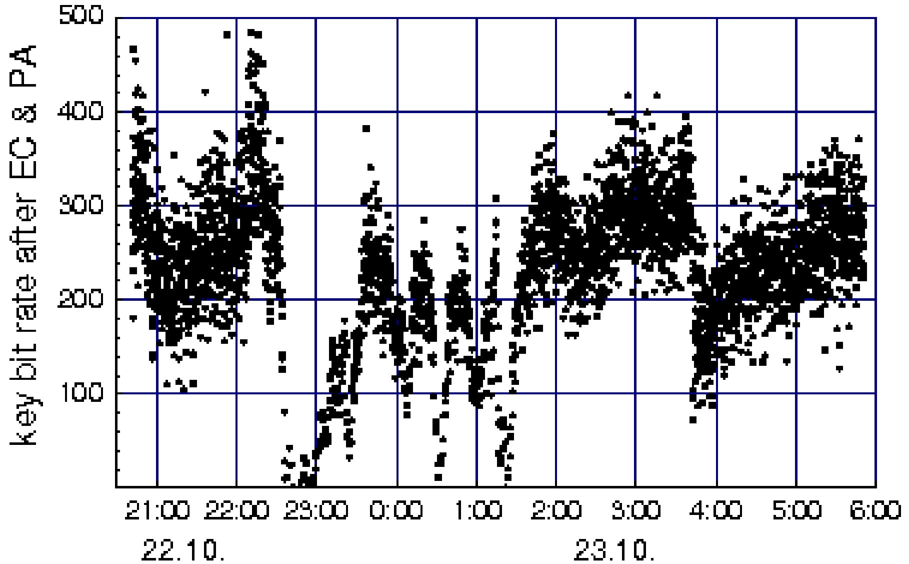
Field results (1.4km range)

- typical data run (with tropical rainfall inbetween)

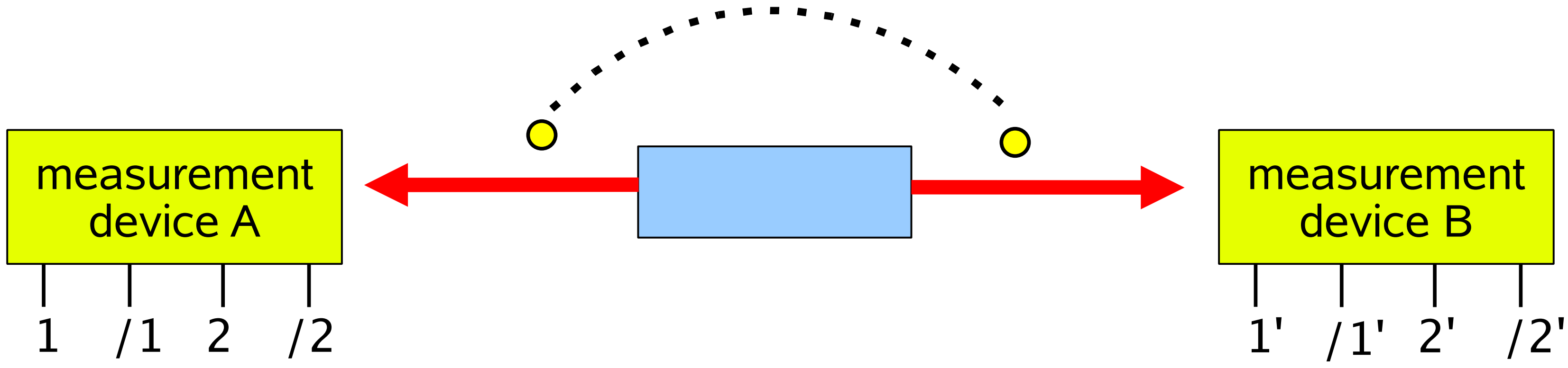








Device-independent QKD?



- 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)

Field usage...

PDC pair source & sender

- Open source: http://code.google.com/p/qcrypto
- 24C3, Berlin 2007, Black Hat / DEFCON16, 2008

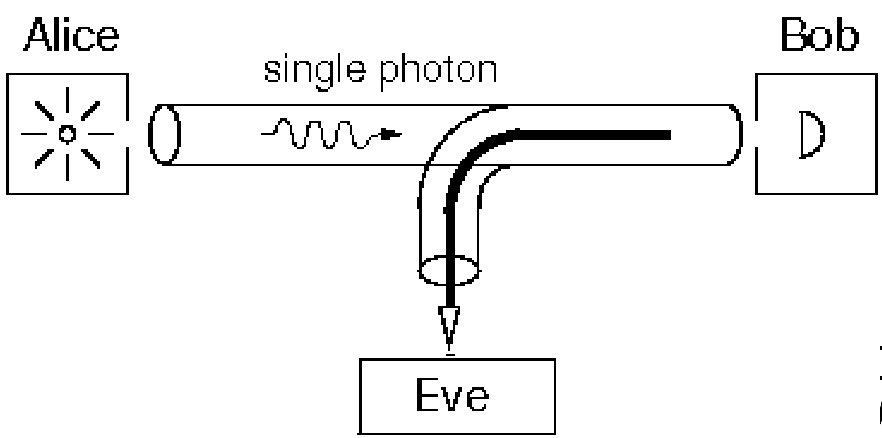
- System gets simpler and more robust

receiving side

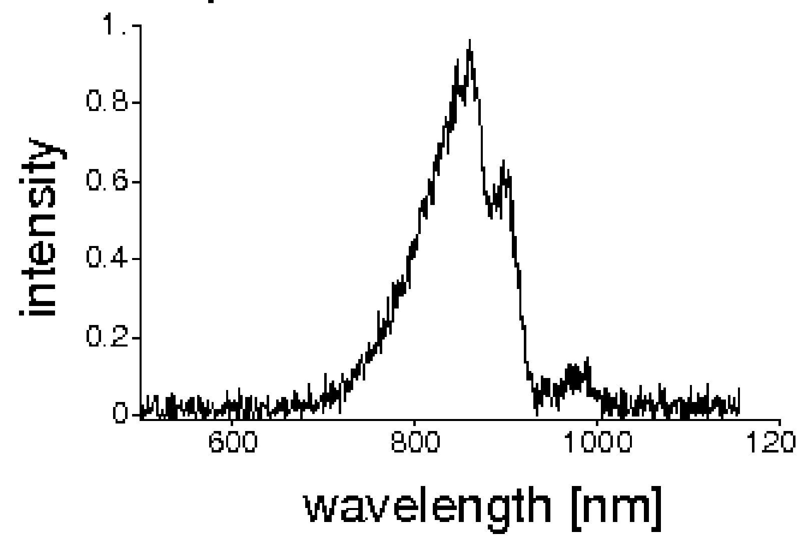
Detector breakdown signature

- detection scenario

- attack scenario



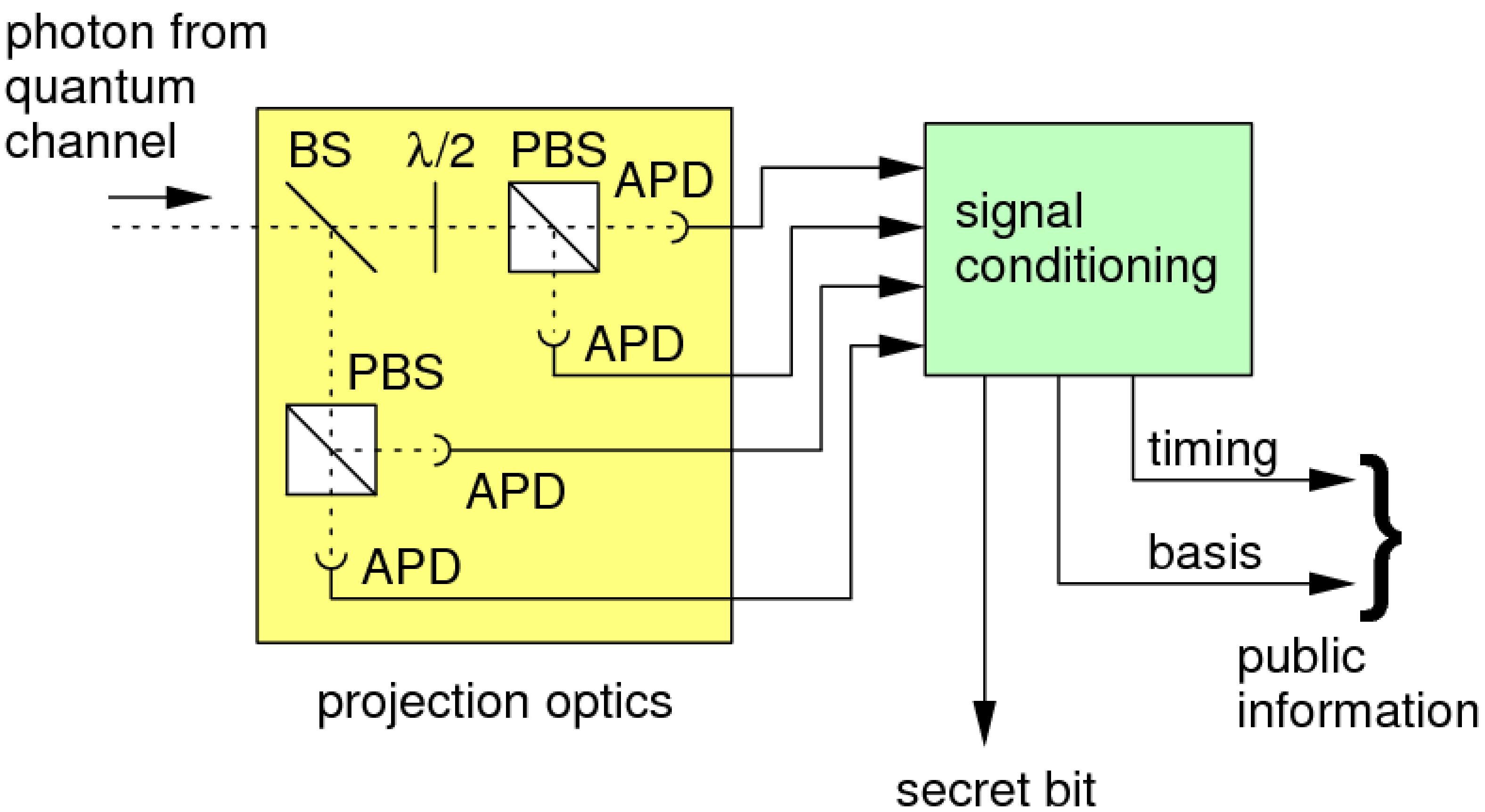
- hot carrier recombination spectrum



- approx 40 photons/sr in Si APD

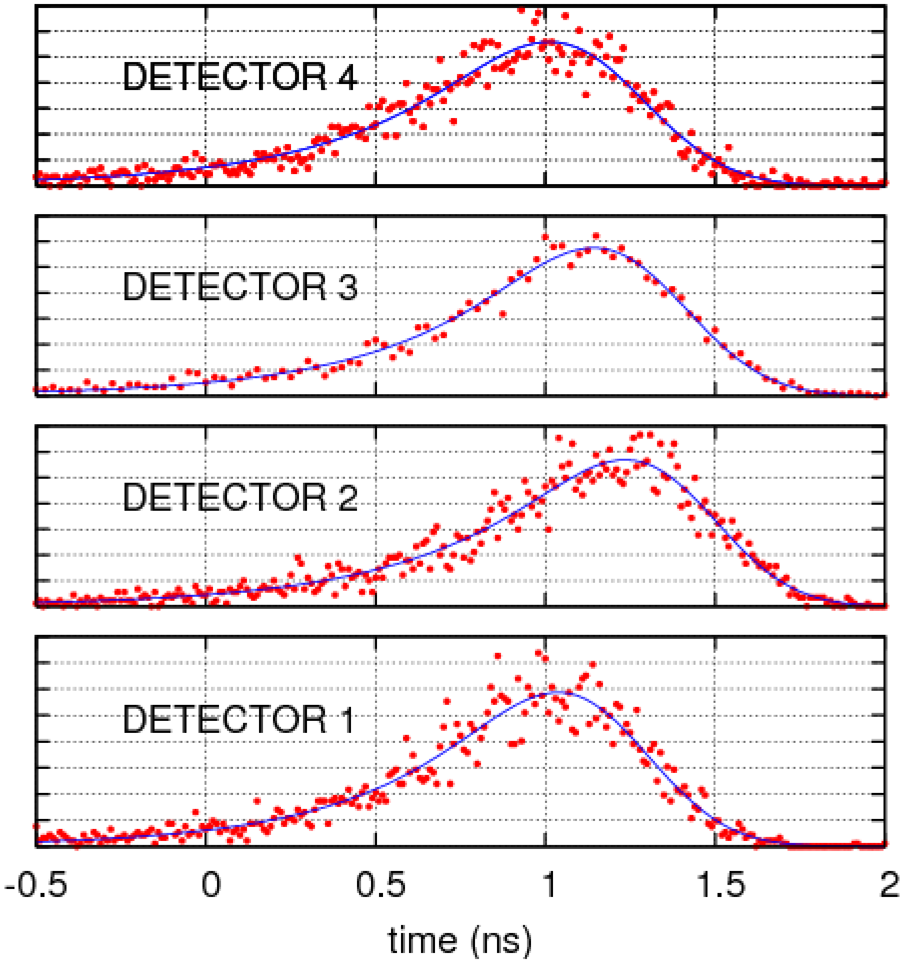
.K.,P. Zarda, M. Halder, H. Weinfurter,
. Mod. Opt. 48, 2039 (2001)

Timing channel attack I

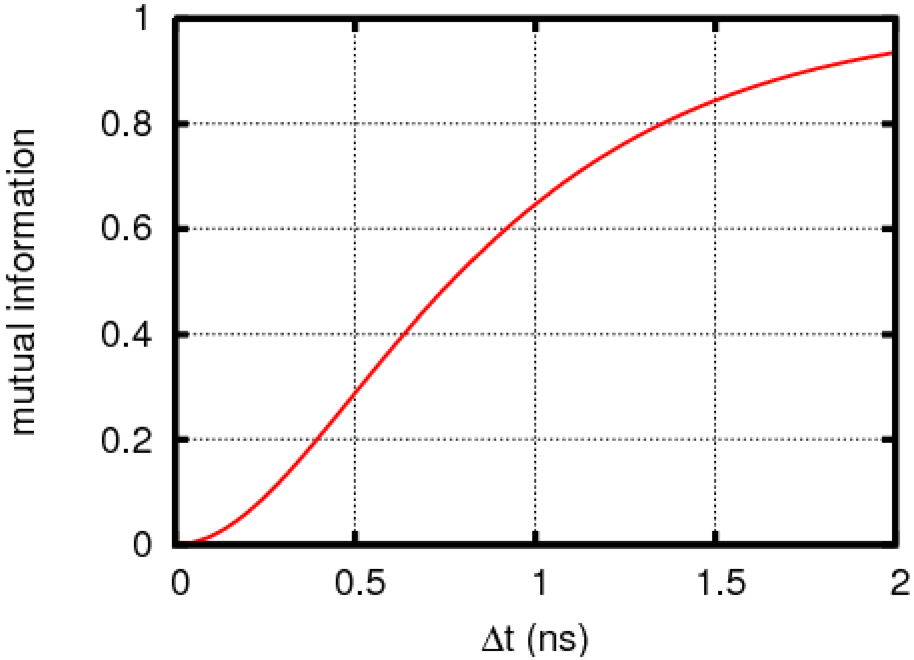


Timing channel attack II

Classical timing information carries fingerprint of detectors:



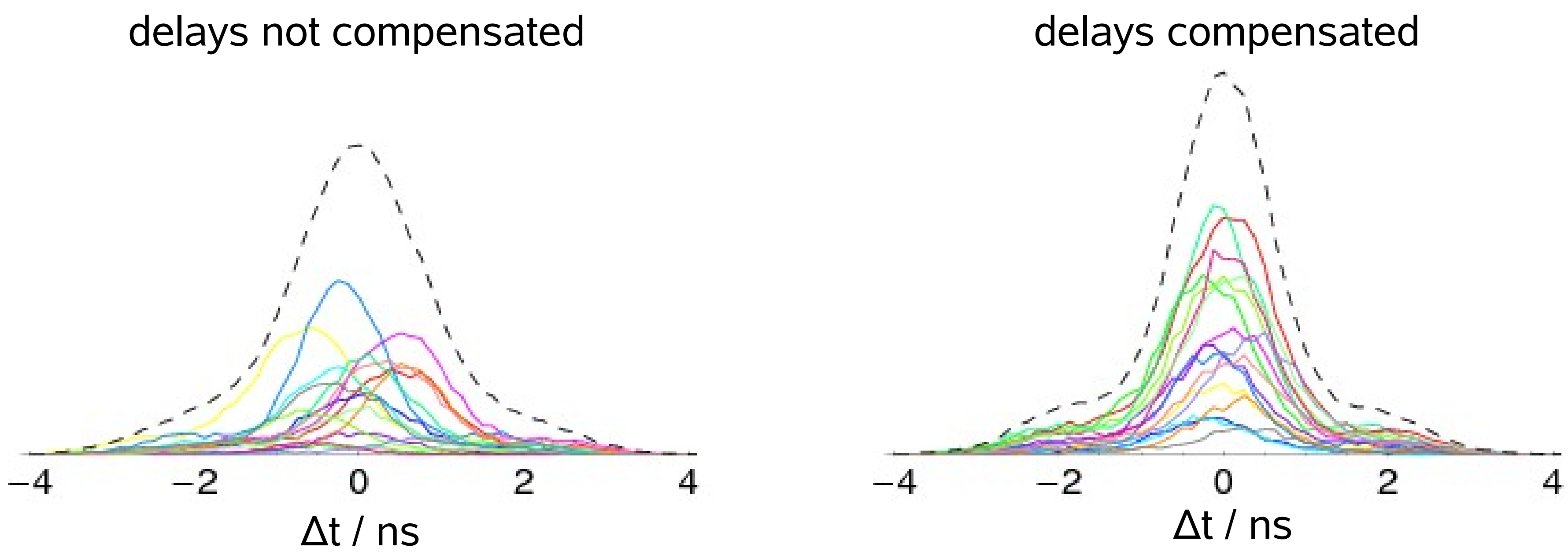
small detector imbalances may tell Eve a lot!



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

Timing ch attack – The Cure

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



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

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

Time for Coffee.....

Thank you !

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

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