Practical Quantum cryptography and possible attacks

Alex Ling, Ilja Gerhardt, Antia Lamas-Linares, Christian Kurtsiefer

24C3 , Berlin

supported by DSTA and Ministry of Education

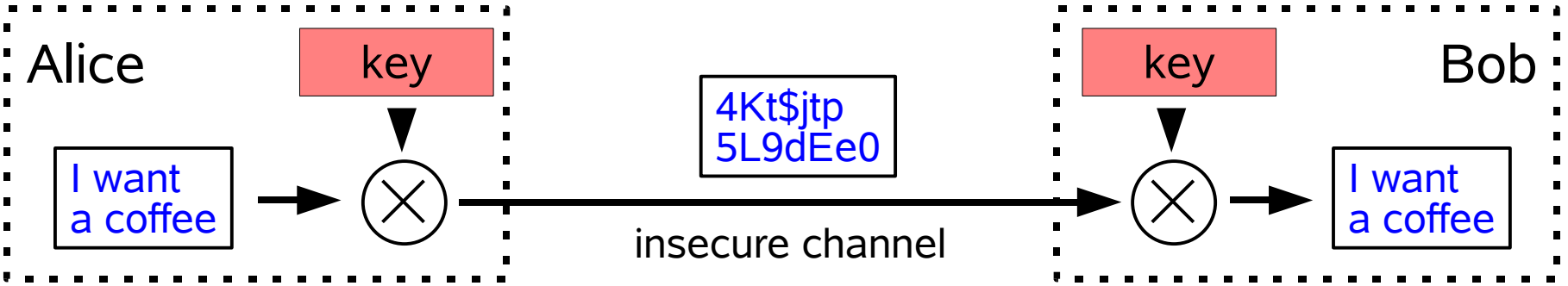
Overview

NUS National University of Singapore

- Cryptography and keys
- What can quantum crypto do?
- BB84 type prepare & send implementations
- Quantum channels
- Entanglement and quantum cryptography
- Timing channel attack
- A side channel-tolerant protocol: E91 revisited

Secure Communication

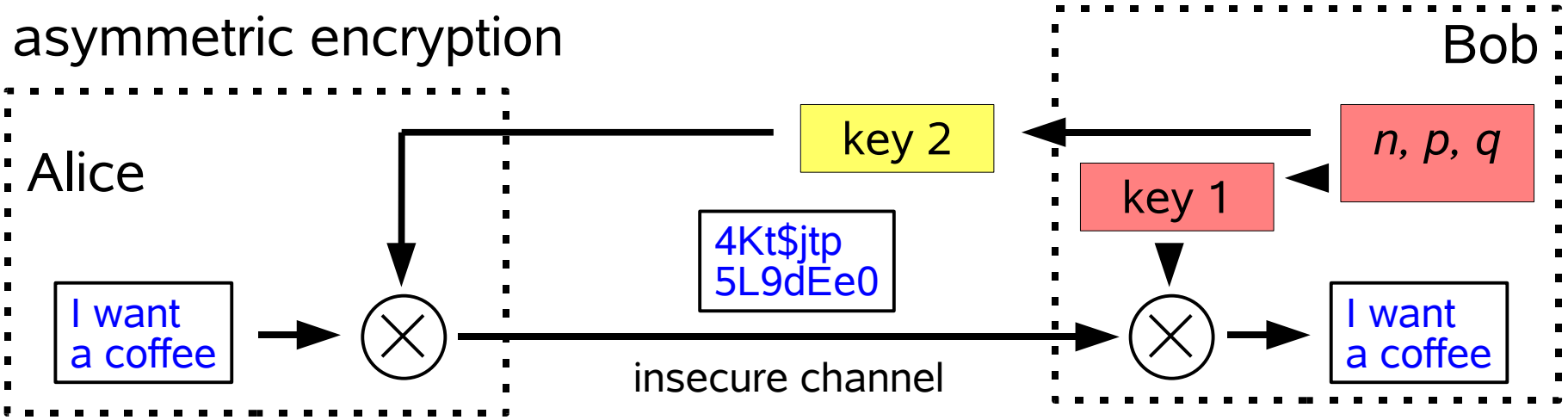
- symmetric encryption



— One time pad / Vernam Cipher: secure for one key bit per bit

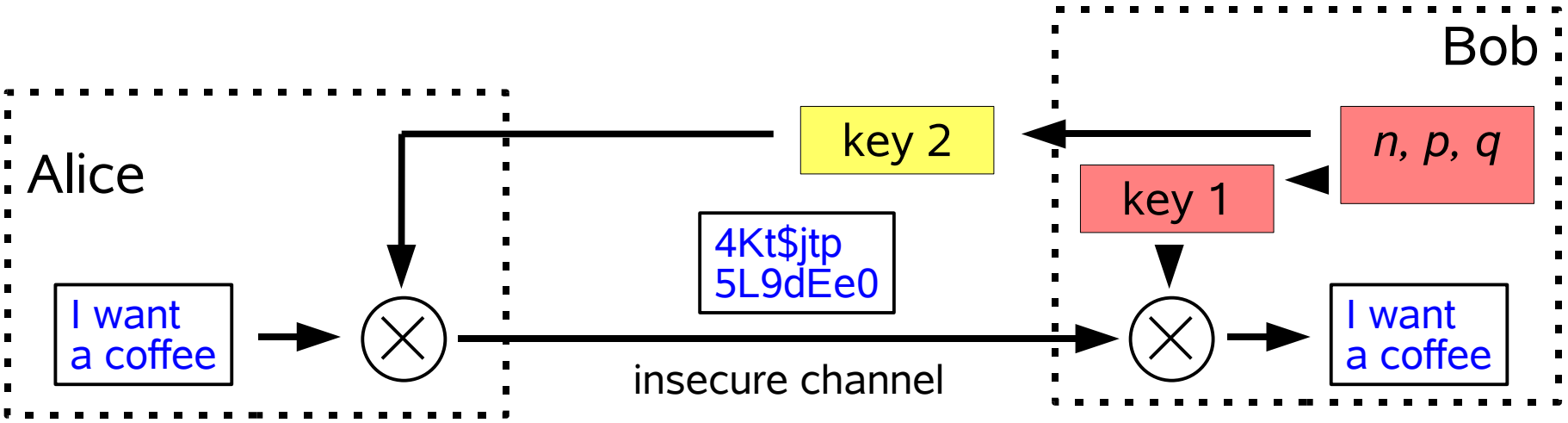
— 3DES, AES & friends: high throughput

- asymmetric encryption



RSA, ellipt. curves: simple, secure **if you can not get key 1 from key 2**

What is wrong with RSA?



....if you can not get key 1 from key 2

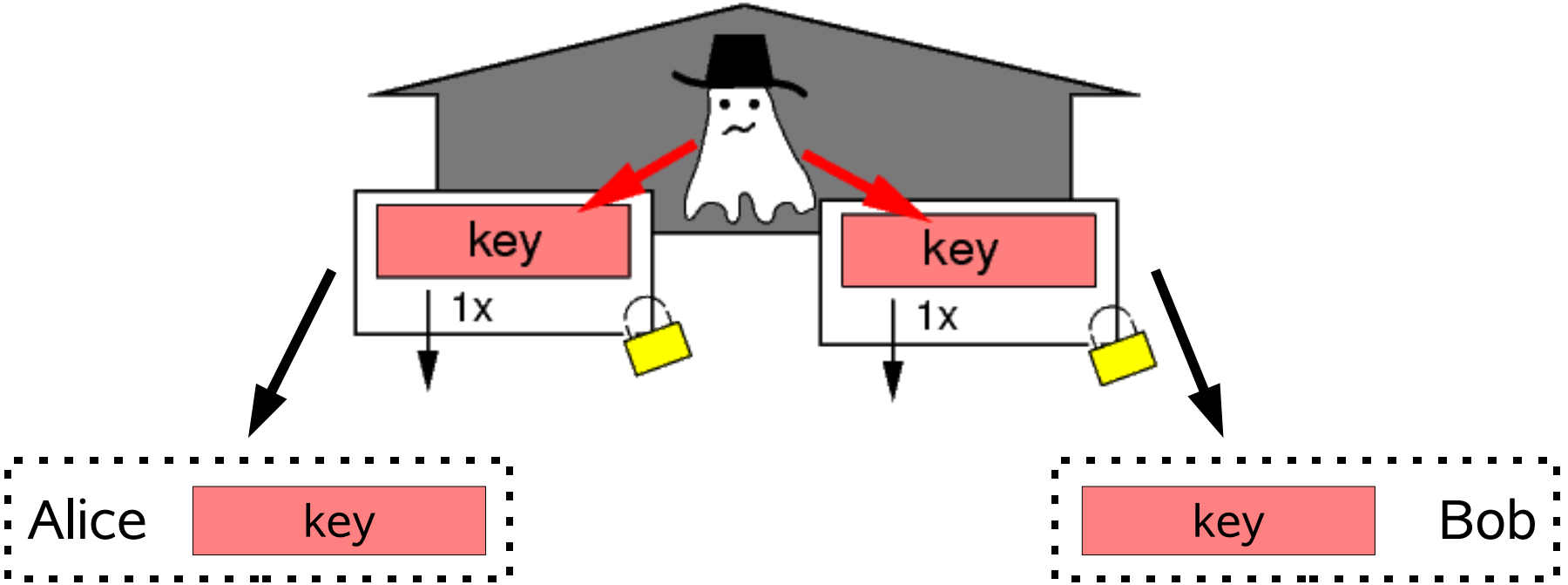
- take dedicated hardware
- find a clever algorithm
- take a quantum computer
- take some time.....

...and you get the key!

Classical Key Distribution

- trusted courier

- tamper-safe devices



Quantum Key Distribution 1

NUS National University of Singapore

- " trusted " courier....

information is carried by physical objects:

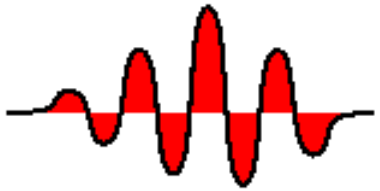
- hole in paper, ink, magnetic domain, electrical charge, dye spot, radio wave, light pulse,...

- classical physics: copying is possible (----> insecure)

Photons carry information

NUS National University of Singapore

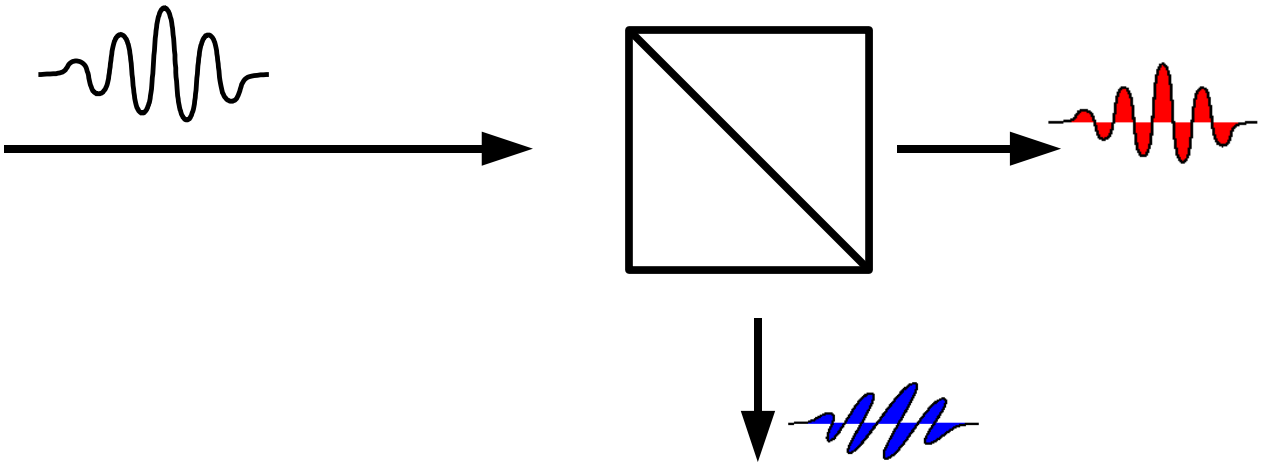
- polarization for 0 and 1:



vertical

horizontal

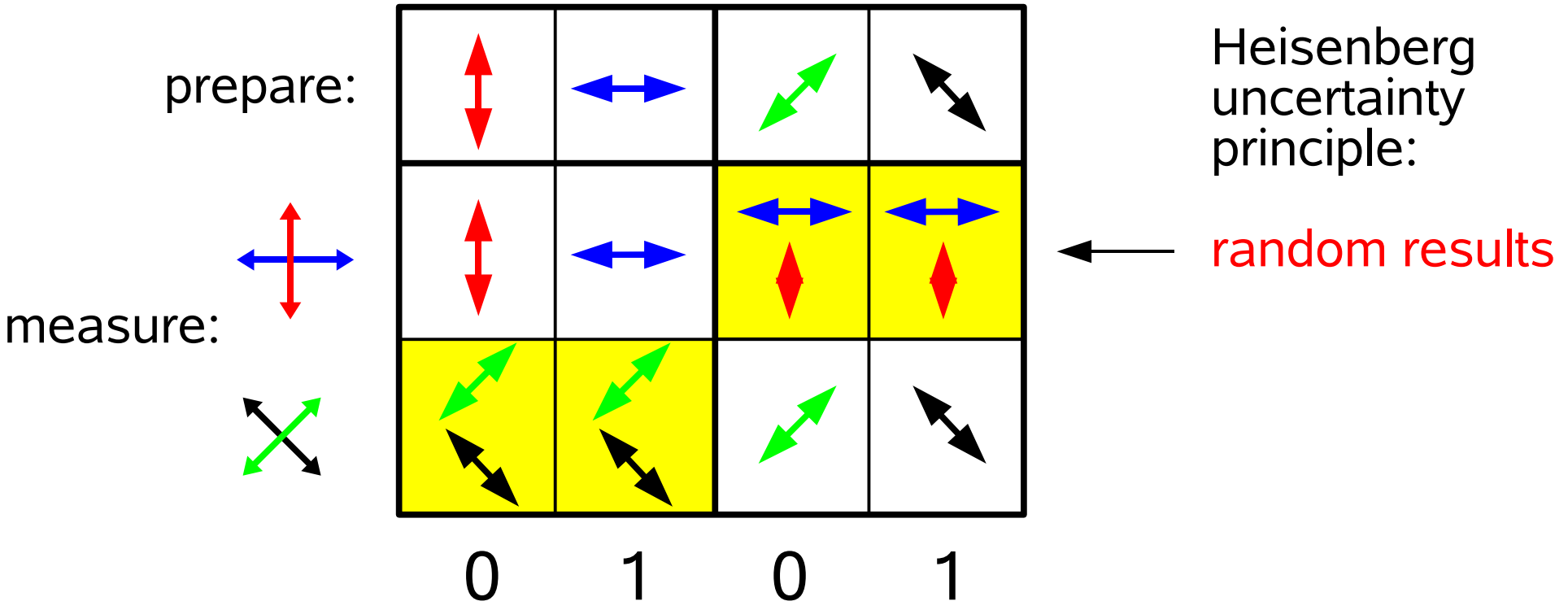
- use polarizing beam splitter to recover 0 or 1:



Quantum mechanics....

- works also with other perpendicular polarizations:

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



Quantum Key Distribution idea

NUS National University of Singapore

- quantum particles as courier....

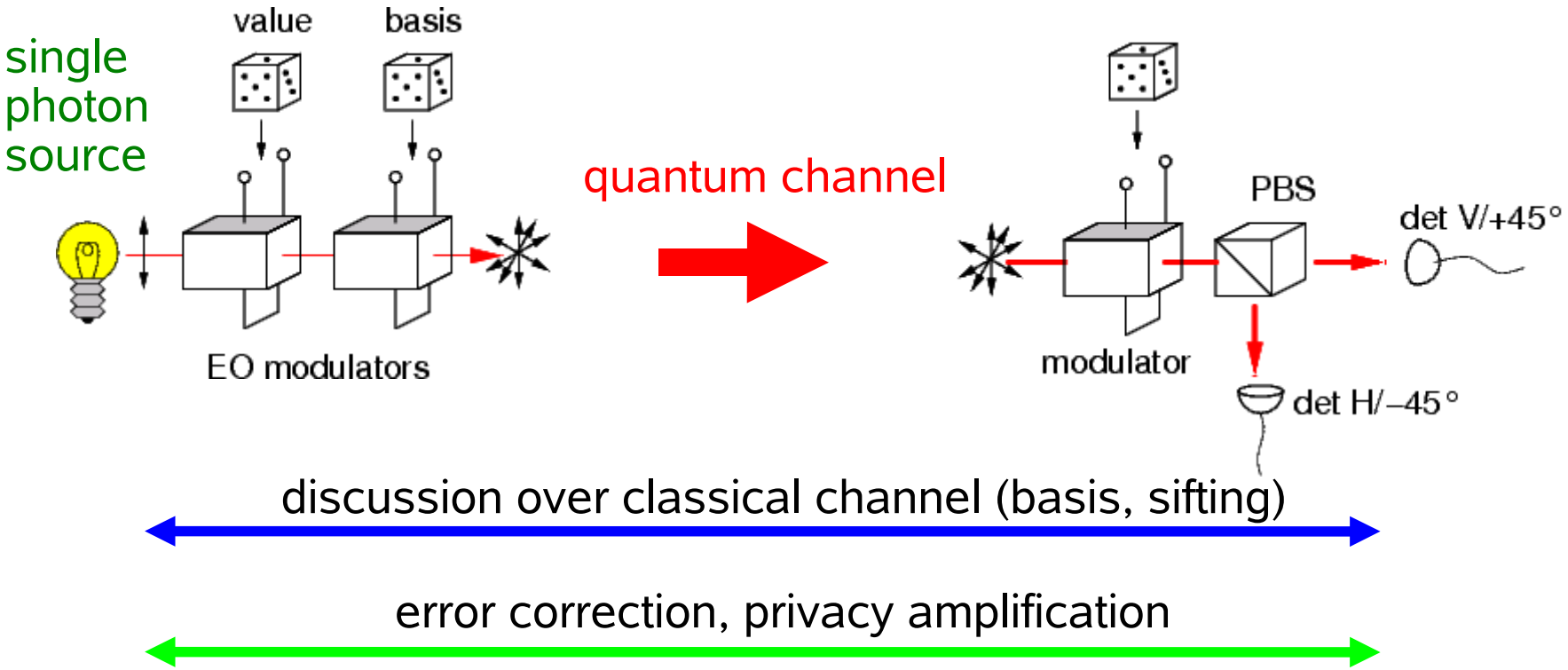
- quantum states cannot be cloned perfectly:

measurements & copying leave traces!

- BB84 protocol for quantum key transport

BB84 protocol

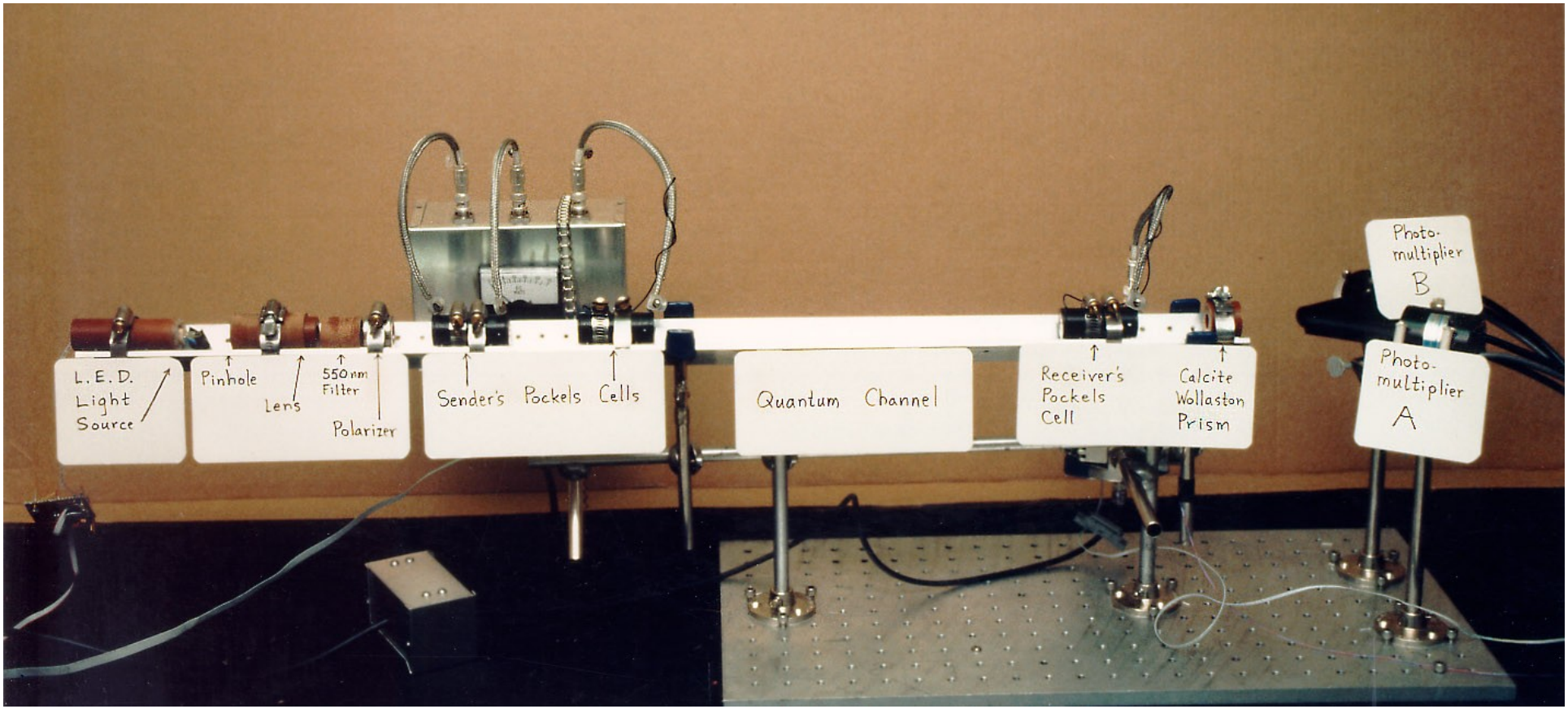
Prepare & measure protocols (BB84 & friends/derivatives):



- uses error fraction to estimate eavesdropper's knowledge

Steampunk BB84

NUS National University of Singapore



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

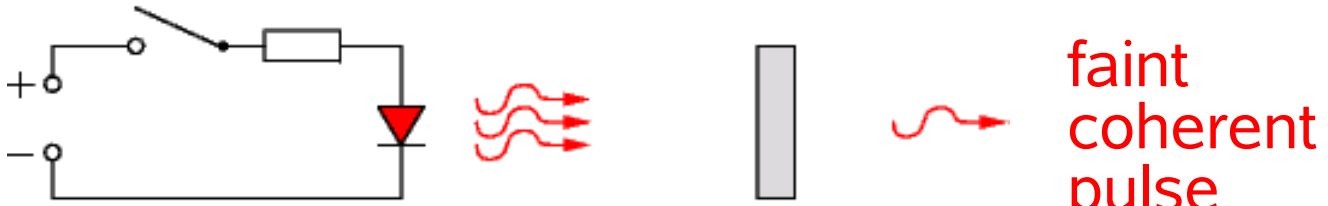
BB84 Implementation Hack #1

- use faint coherent pulses instead of single photons

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

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

- much simpler to prepare than true single photons:

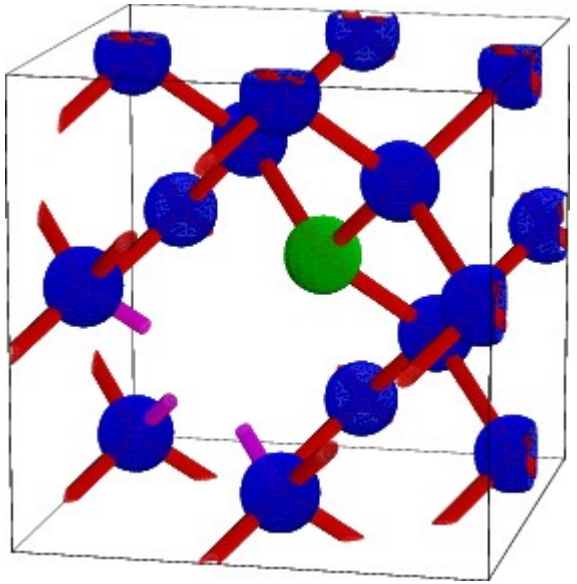


laser diode attenuator

- potentially insecure: photon number splitting attack

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...

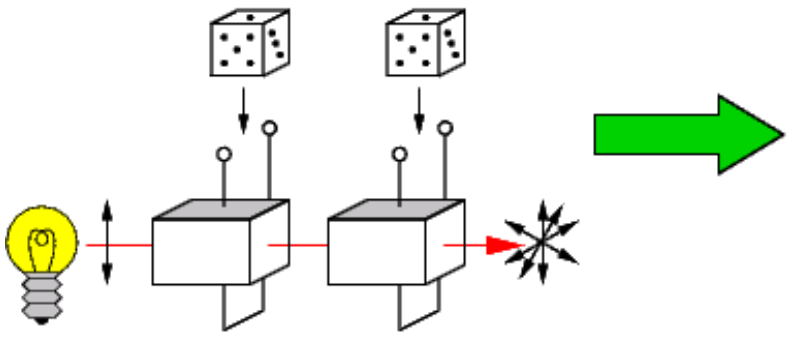
- use decoy states (pulses with randomized <n>) to discover photon number splitting attacks

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

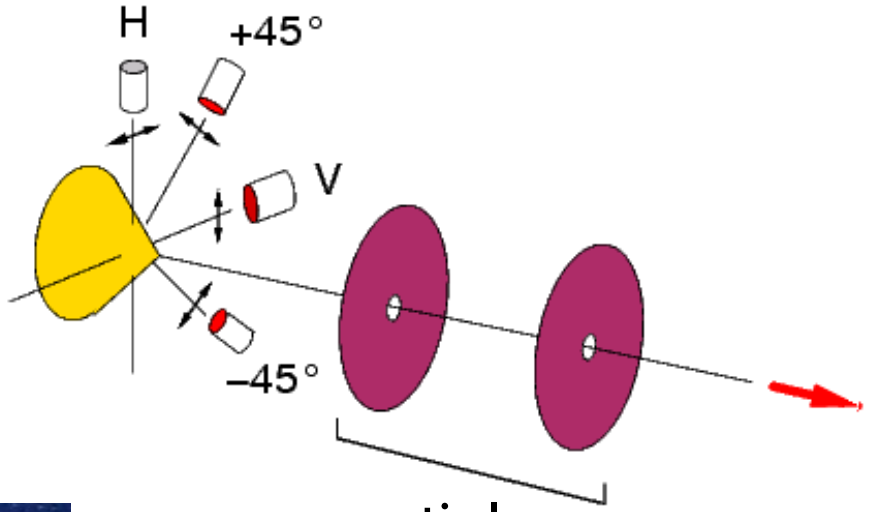
Preparation of polarized photons

NUS National University of Singapore

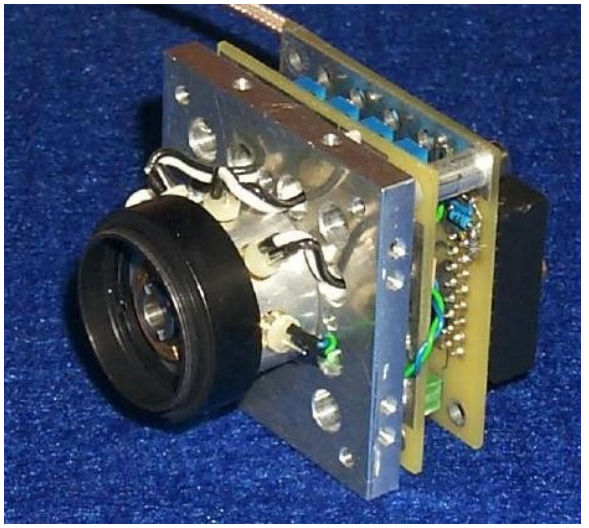
- Make use of good intrinsic polarization of laser diodes



basis value

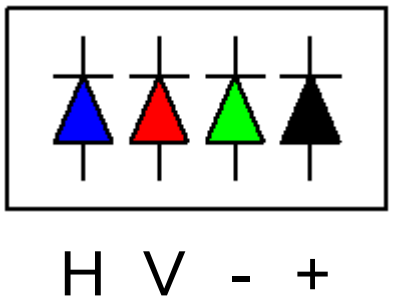


spatial filter

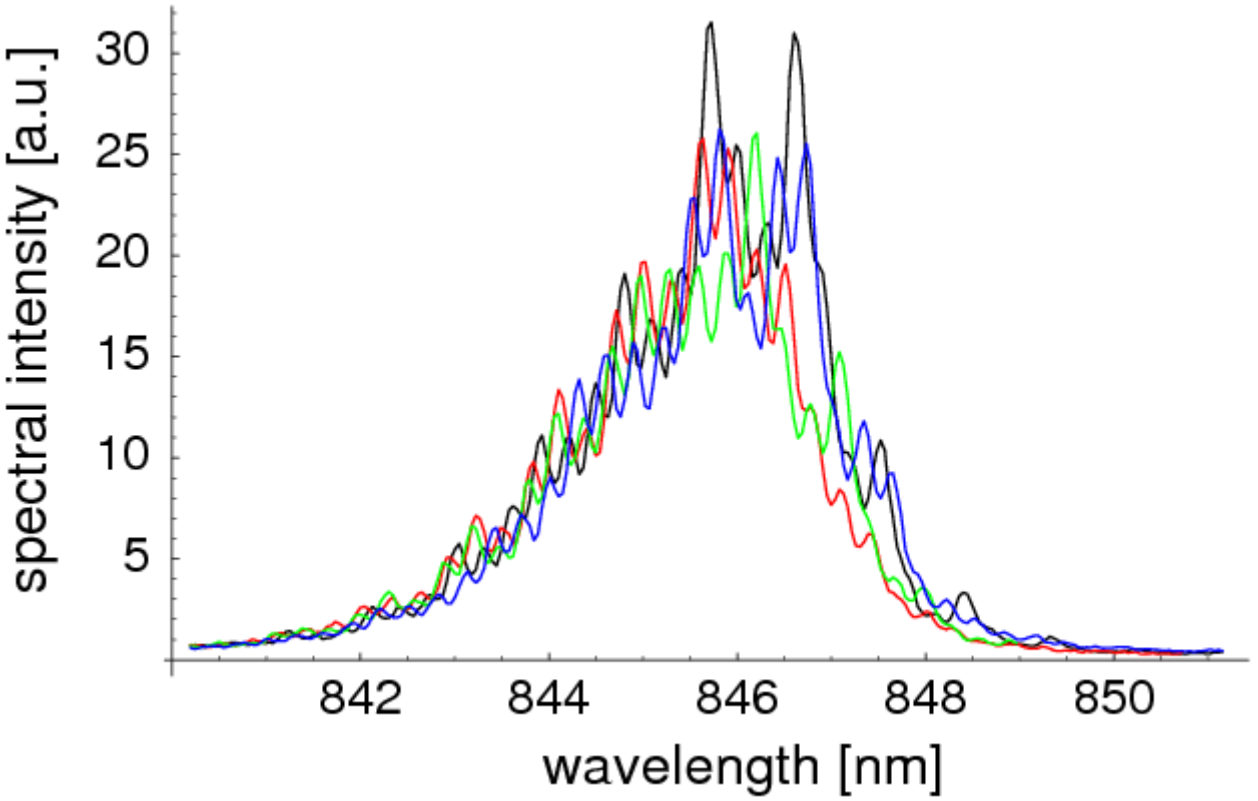


BB84: Spectral attack

Don't measure polarization, but color:



asymptotic average information leakage: <2%

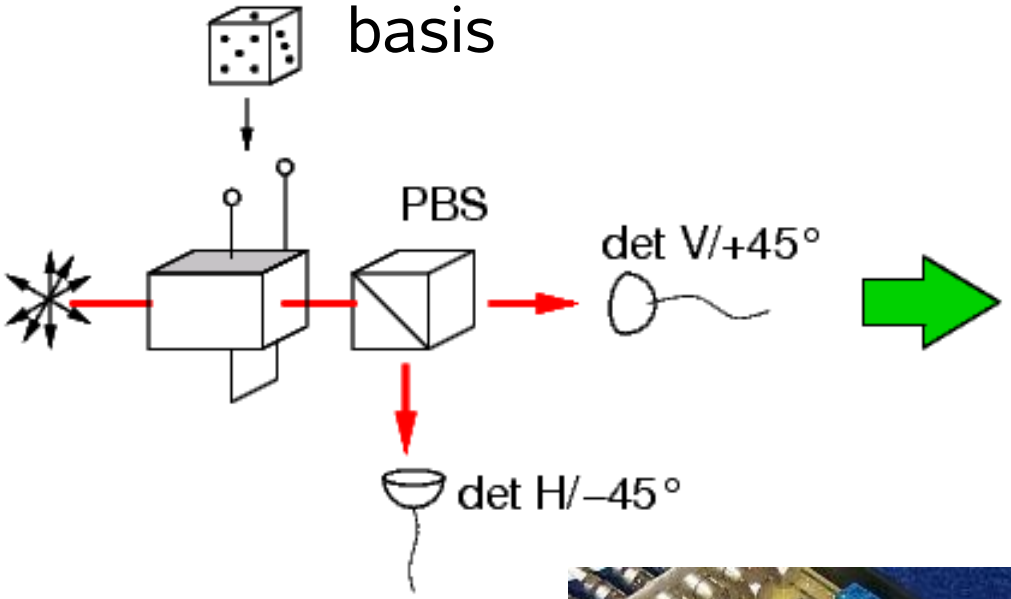


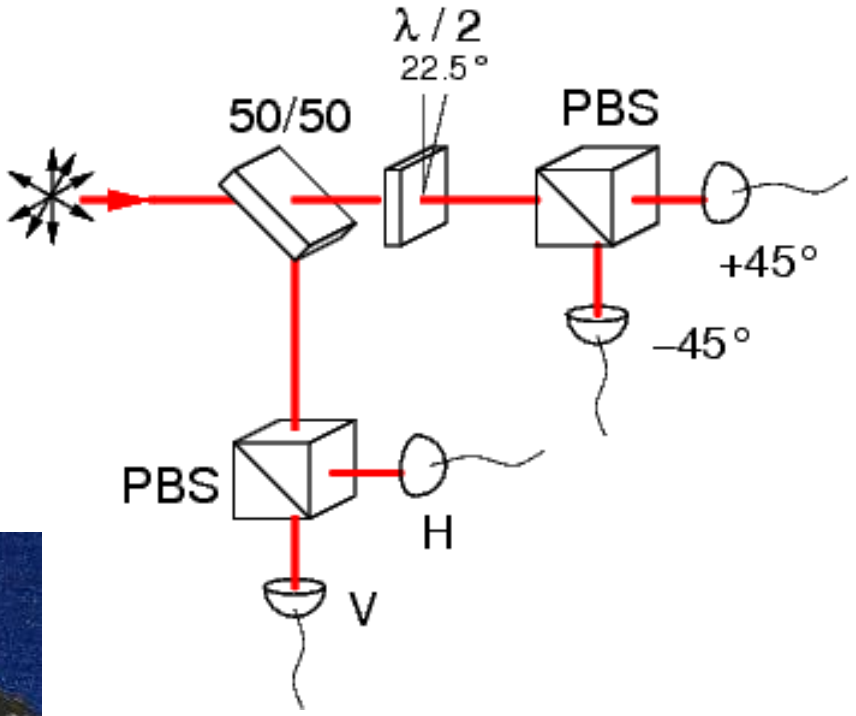
C.K.,P. Zarda, M. Halder, H. Weinfurter (2001)

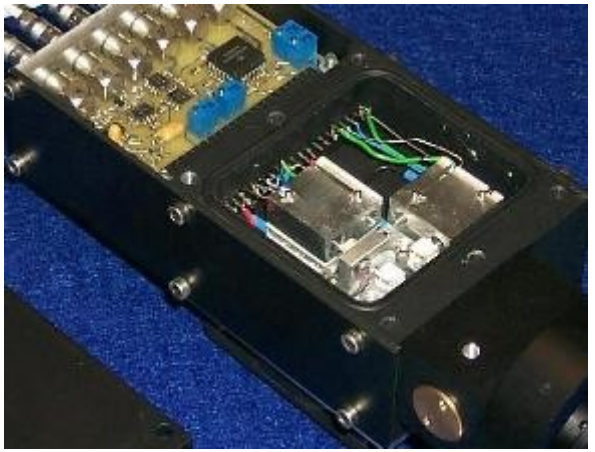
Polarization measurement

- 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)*



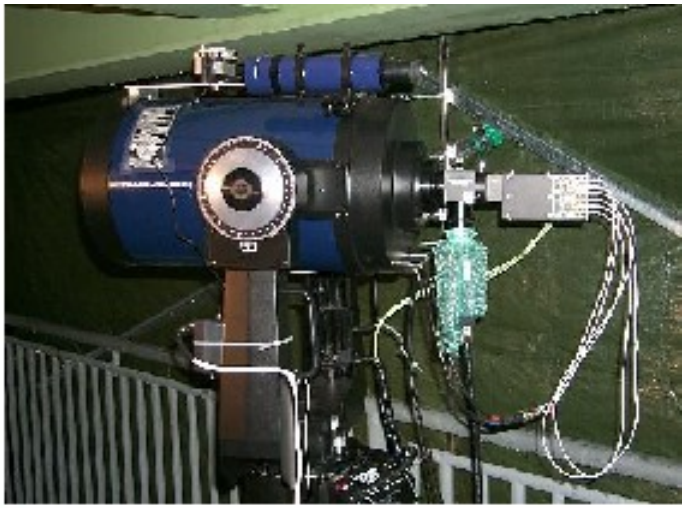




Bridging distances

NUS National University of Singapore

Bob



Zugspitze
(2950 m)

23.4 km

Alice

S

westliche
Karwendelspitze
(2244m)

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

Latest developments

NUS National University of Singapore

- 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)*

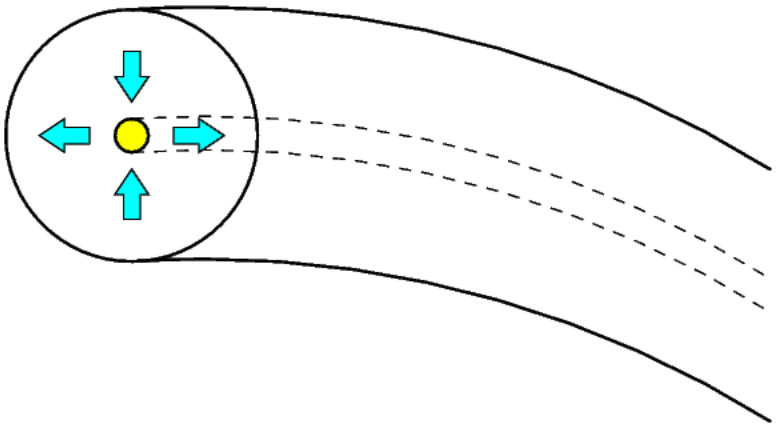
- Larger key rates: VCSEL lasers, detectors with better timing resolution, high clock rate
  ~Mbit/sec key rate (detector limited)

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

Transport through fibers

NUS National University of Singapore

- Very practical: Less susceptible to environment
- 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

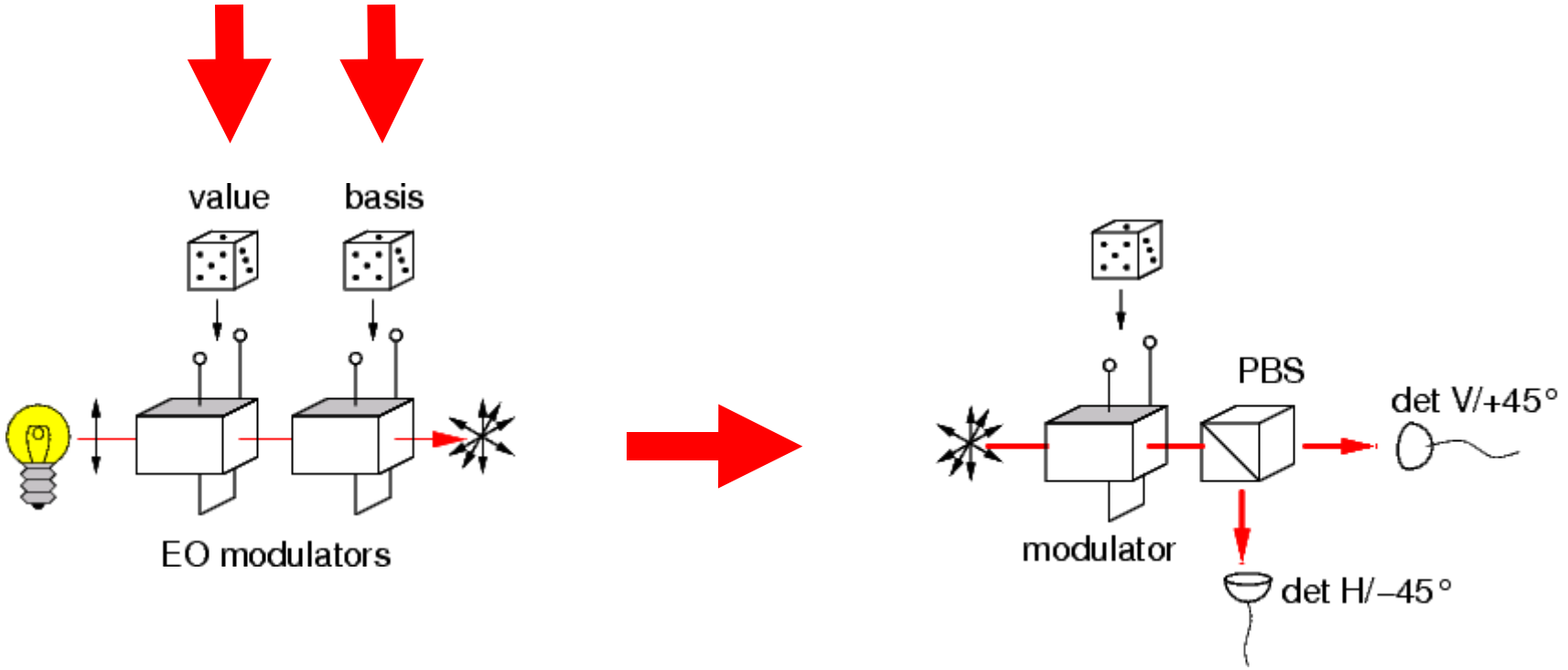


polarization encoding is more difficult.....

- Commercial systems: id quantique, Magiq; NEC, Toshiba

Prepare & Send problem:

...needs lots* of trusted random numbers!



- Do you trust your random numbers?

*Mbit/sec for kbit/sec key

What is a good key?

NUS National University of Singapore

- bad key:

  `000000000000000000000000000000000.....`

- better key:

  `011101010101111010100111010010010 0110.....`

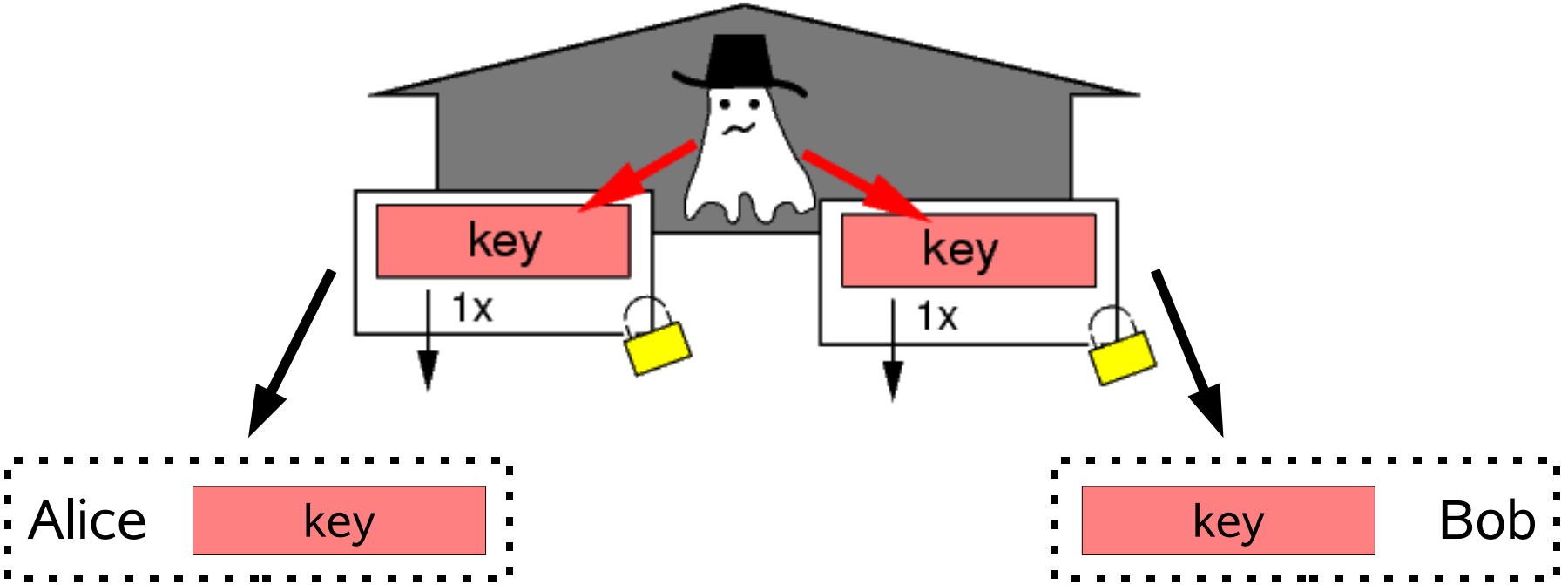
  good keys look like random numbers

  randomness of a bit stream can not be proven mathematically

Quantum Key Distribution 2

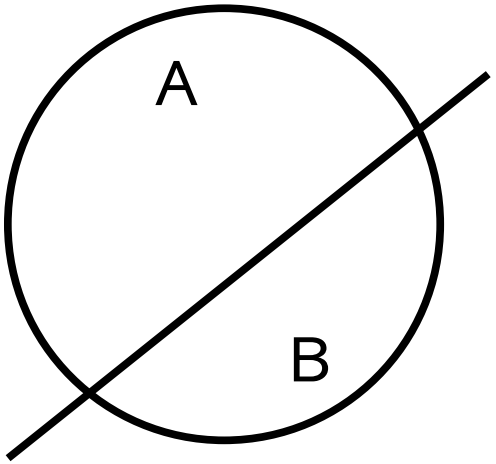
- trustable courier -----> BB84

- tamper-safe devices ?



Entanglement (abstract)

- An entangled system cannot be described as a combination of its parts:

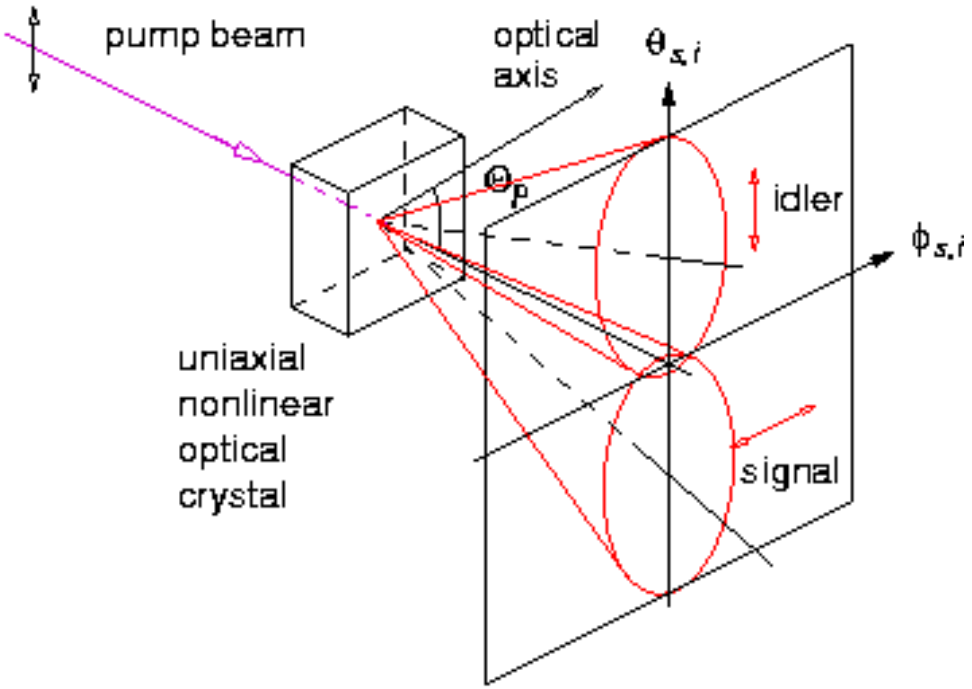


$$|\Psi\rangle_{AB} \neq |\Psi\rangle_A \otimes |\Psi\rangle_B$$

- This is strictly a quantum effect. There is no classical analogon to that.
- A and B can even be separated in space
- You can even do that in practice!!!

Entangled photon resource

- Use non-collinear type-II parametric down conversion



two indistinguishable decay paths lead to

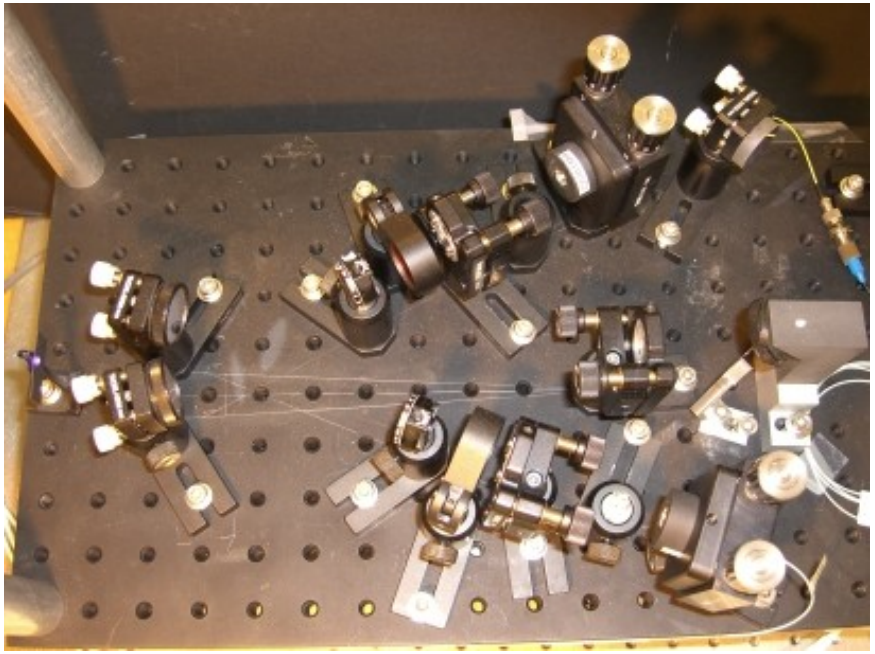
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|HV\rangle - |VH\rangle\right)$$

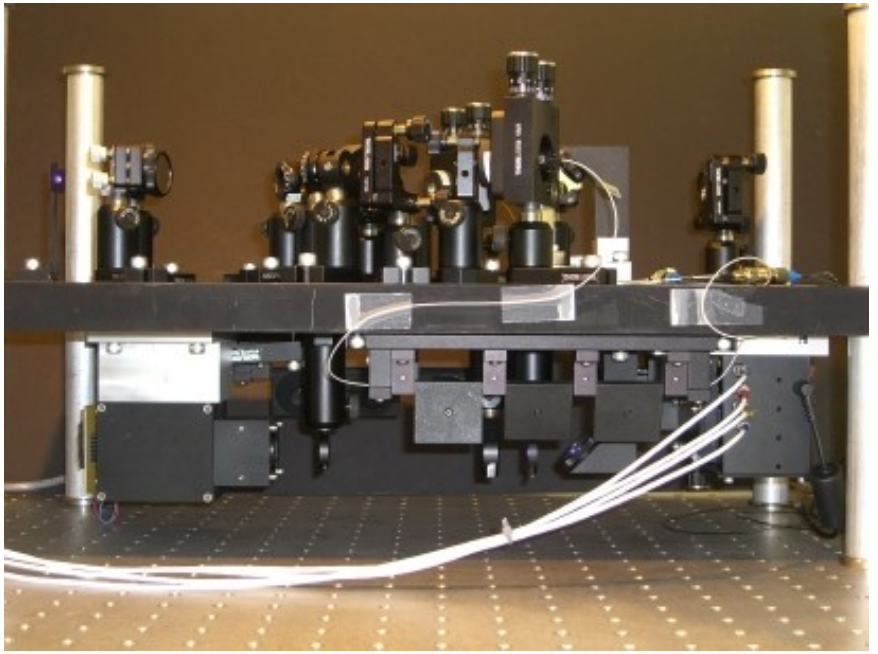
*P.G. Kwiat et al., PRL **75**, 4337 (1995)*

The gadget

NUS National University of Singapore

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

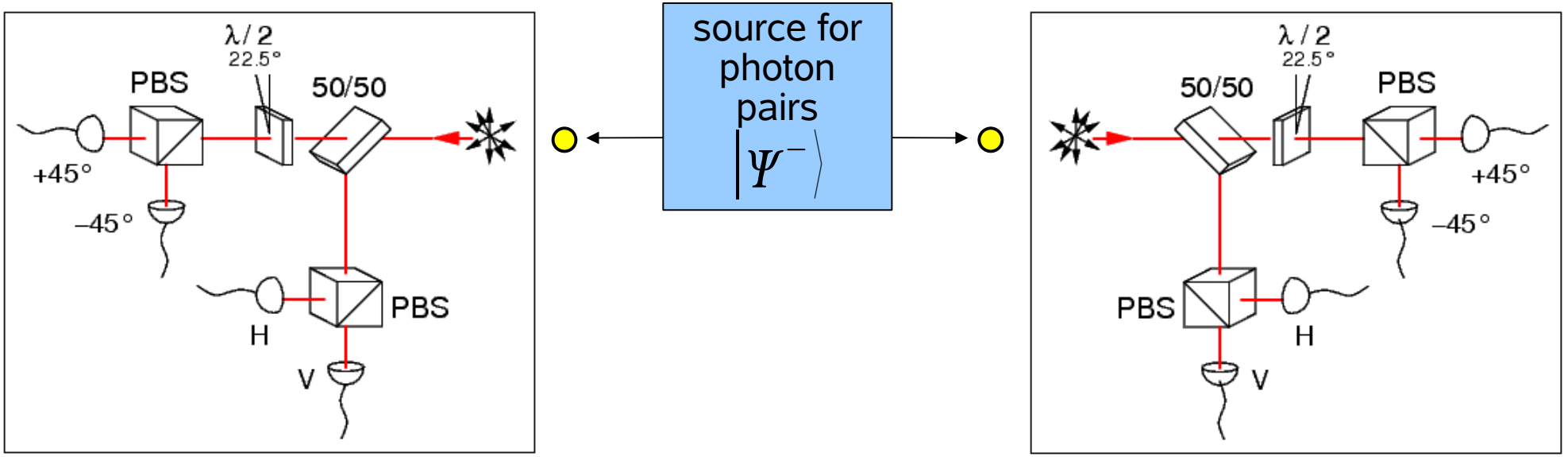




- 24,000 s^{-1} detected pairs from 40 mW pump @ 407nm in single mode fibers at 810/818 nm
- polarization correlation visibility in 45° basis: 92%

BB84 with photon pairs

Quantum correlations & measurements on both sides



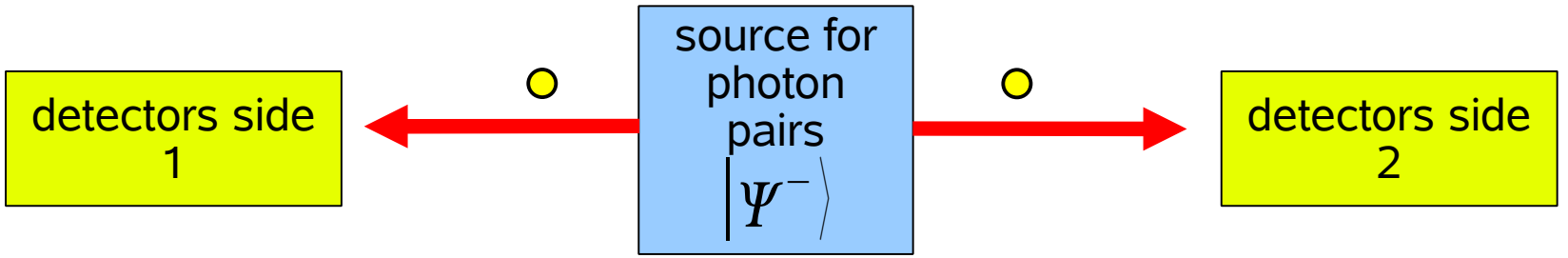
public discussion (sifting, key gen / state estimation)

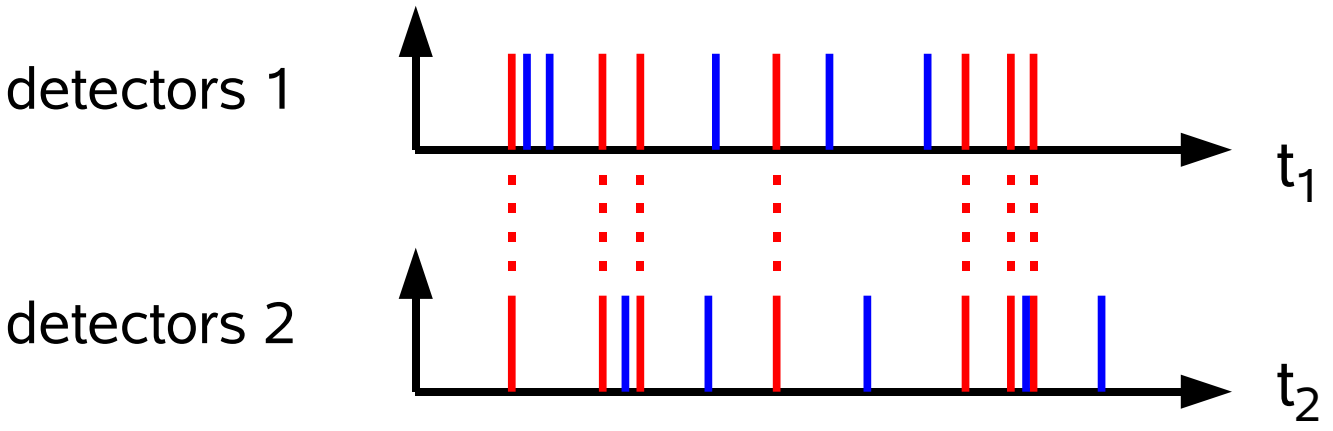
error correction, privacy amplification

- no trusted random numbers for key
- quantum randomness for measurement basis

Coincidence identification I

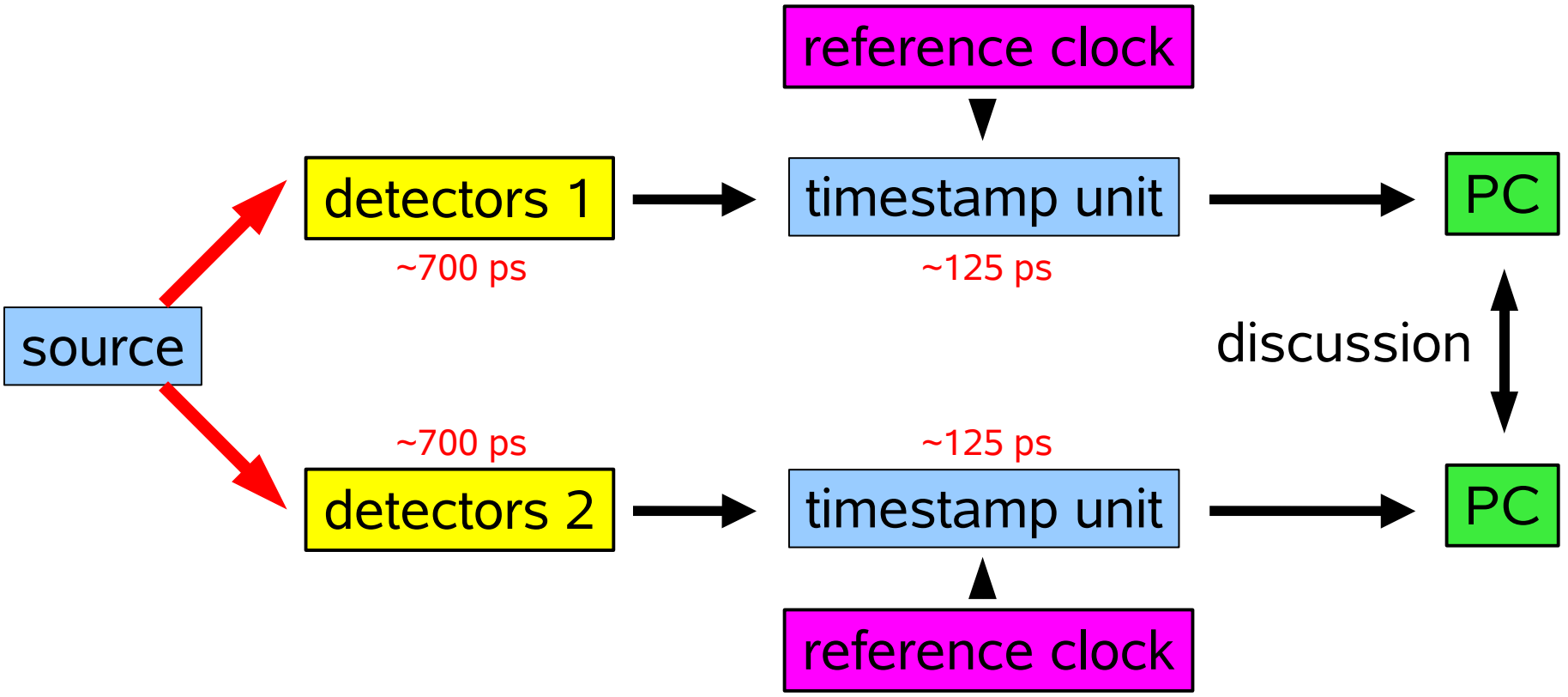
- Photon pairs in PDC are born randomly, but at the same time (within few 100 femtoseconds!)



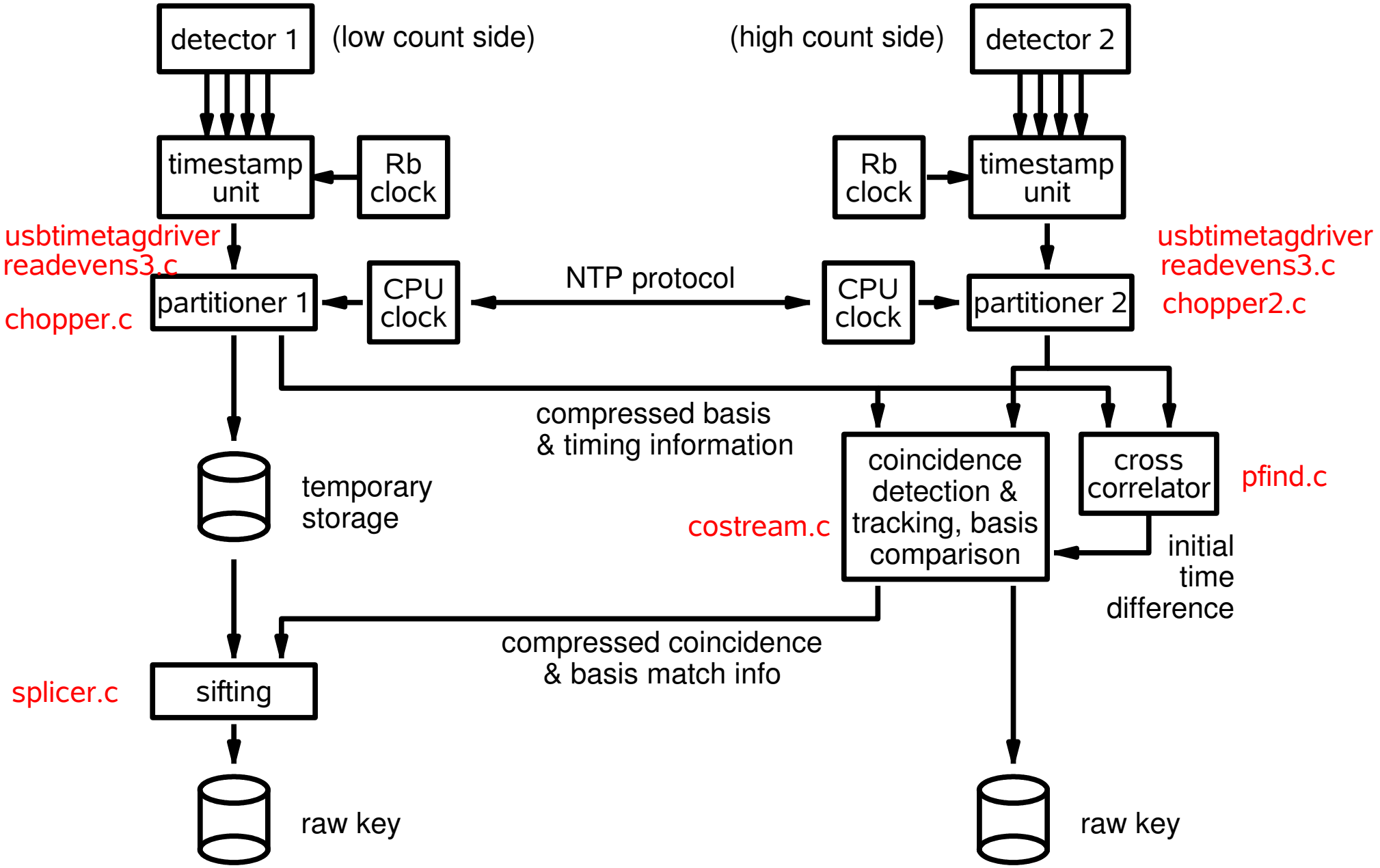


Coincidence identification II

- Photon pairs in PDC are born randomly, but at the same time (within few 100 femtoseconds!)

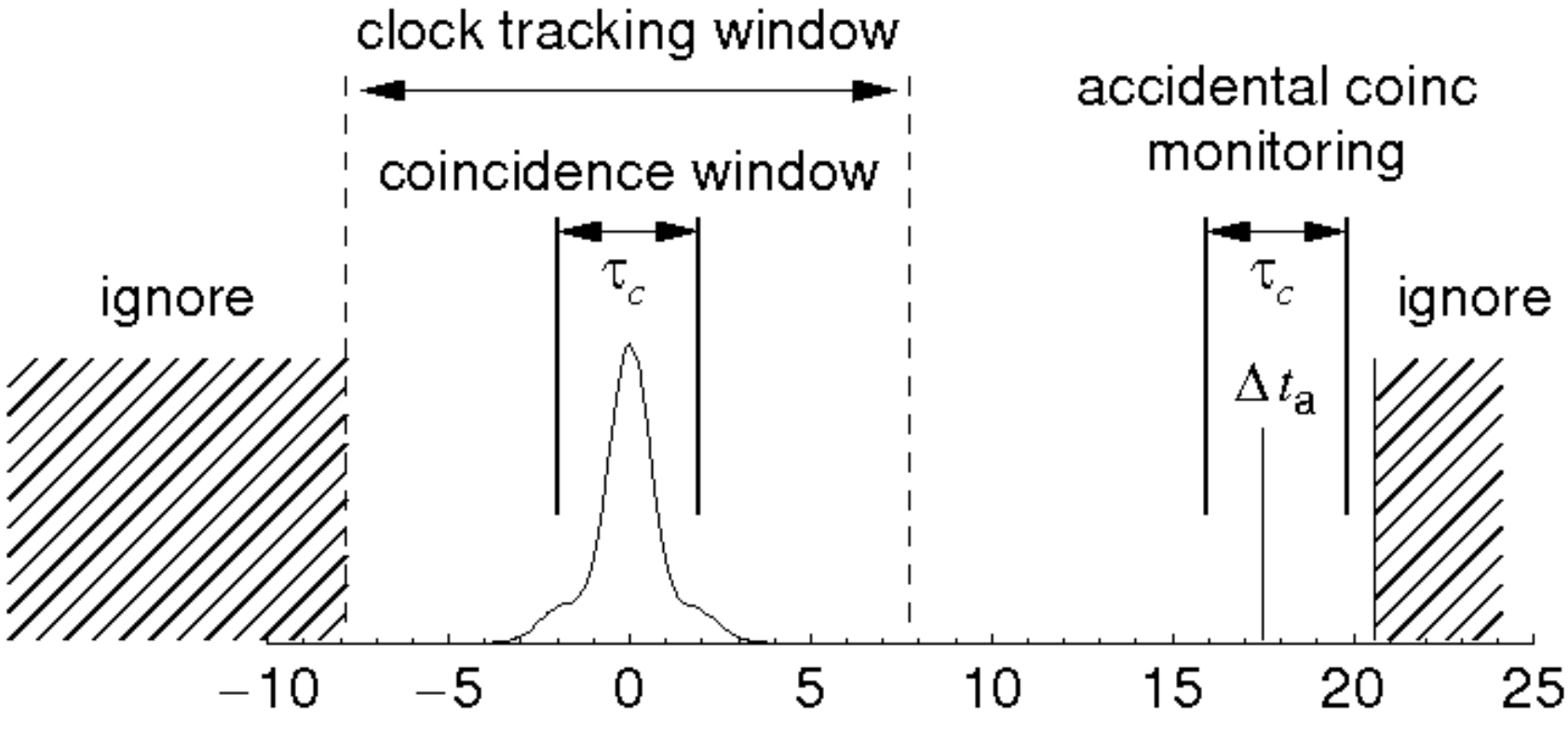


Signal flow


detector 1
(low count side)
(high count side)
detector 2
timestamp unit
Rb clock
Rb clock
timestamp unit
usbtimetagdriver
readevens3.c
chopper.c
partitioner 1
CPU clock
NTP protocol
CPU clock
partitioner 2
usbtimetagdriver
readevens3.c
chopper2.c
compressed basis & timing information
temporary storage
coincidence detection & tracking, basis comparison
costream.c
cross correlator
pfind.c
initial time difference
compressed coincidence & basis match info
splicer.c
sifting
raw key
raw key

Coincidence identification III

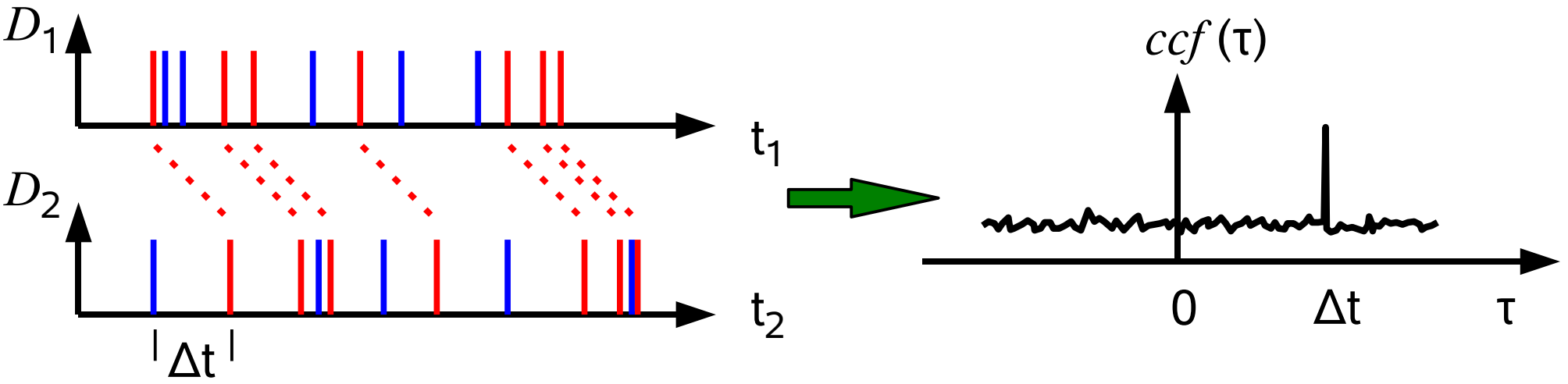
Use time correlation to identify pairs, suppress background, servo clocks



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

Time difference finding

- Find initial time difference between two sides via cross correlation



$$ccf\left[D_1(t), D_2(t)\right](\tau) = \int_{-\infty}^{\infty} D_1(t+\tau)\, D_2(t)\, dt$$

- 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

Error detection / correction

NUS National University of Singapore

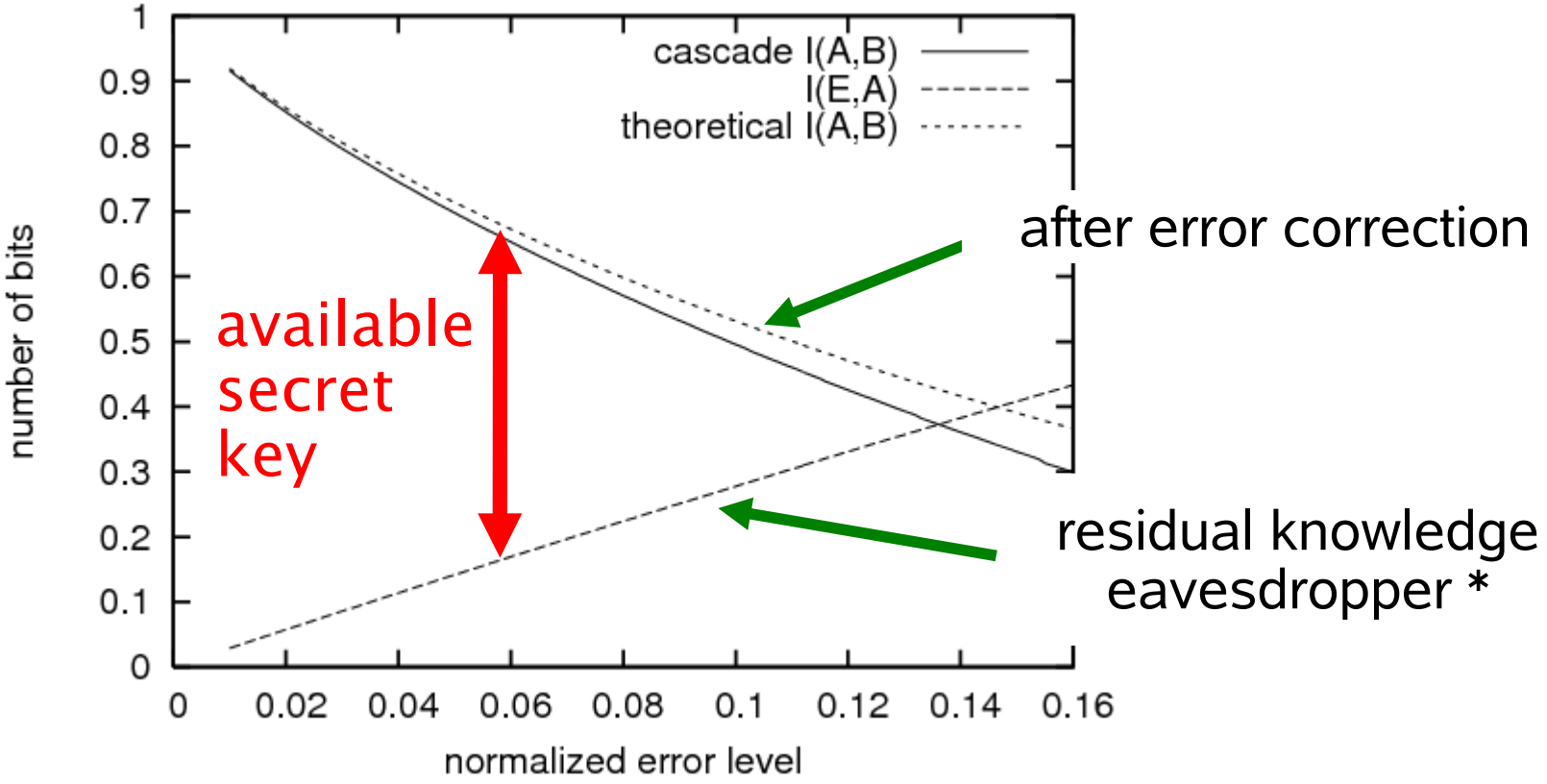
ALICE: **0111 0101 0101 0110 1010 0111 0101 .....**

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**	**.....**

Estimate Eve's knowledge

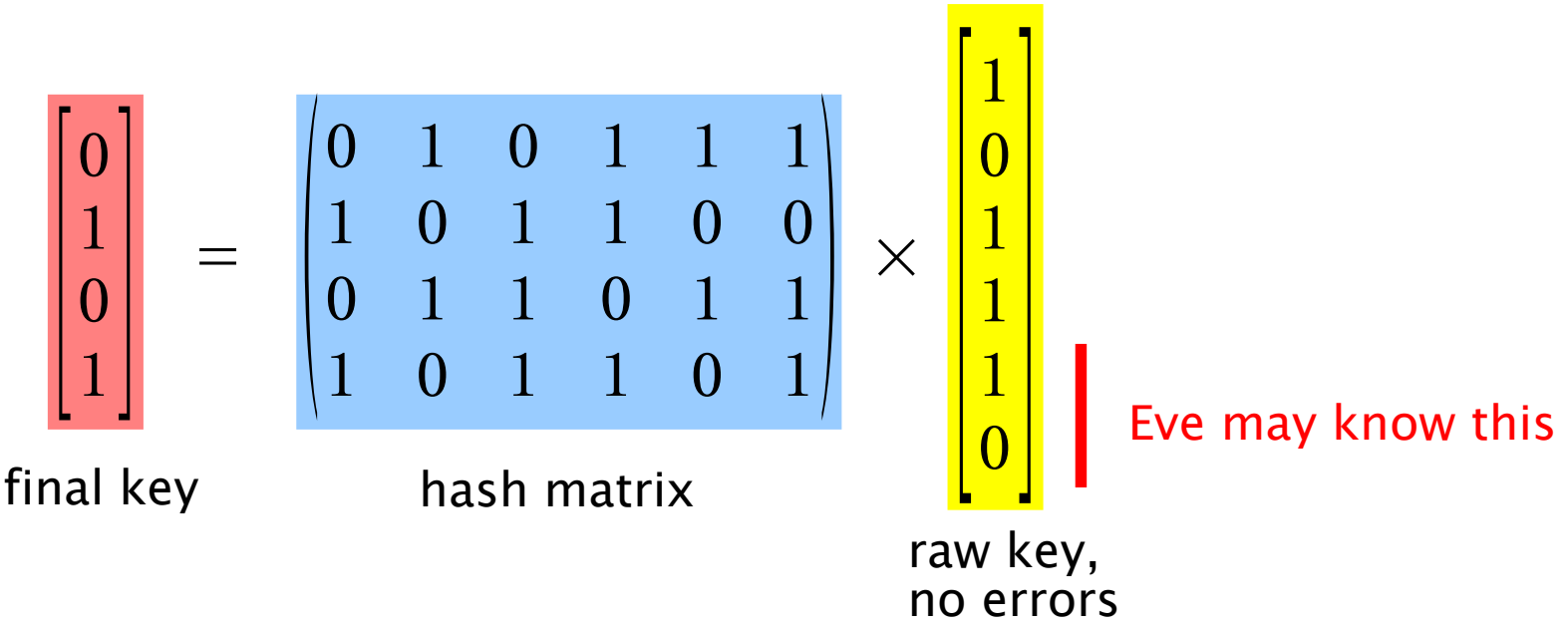


* depends on the attack model (individual attack); for *infinite* key length

Privacy amplification

NUS National University of Singapore

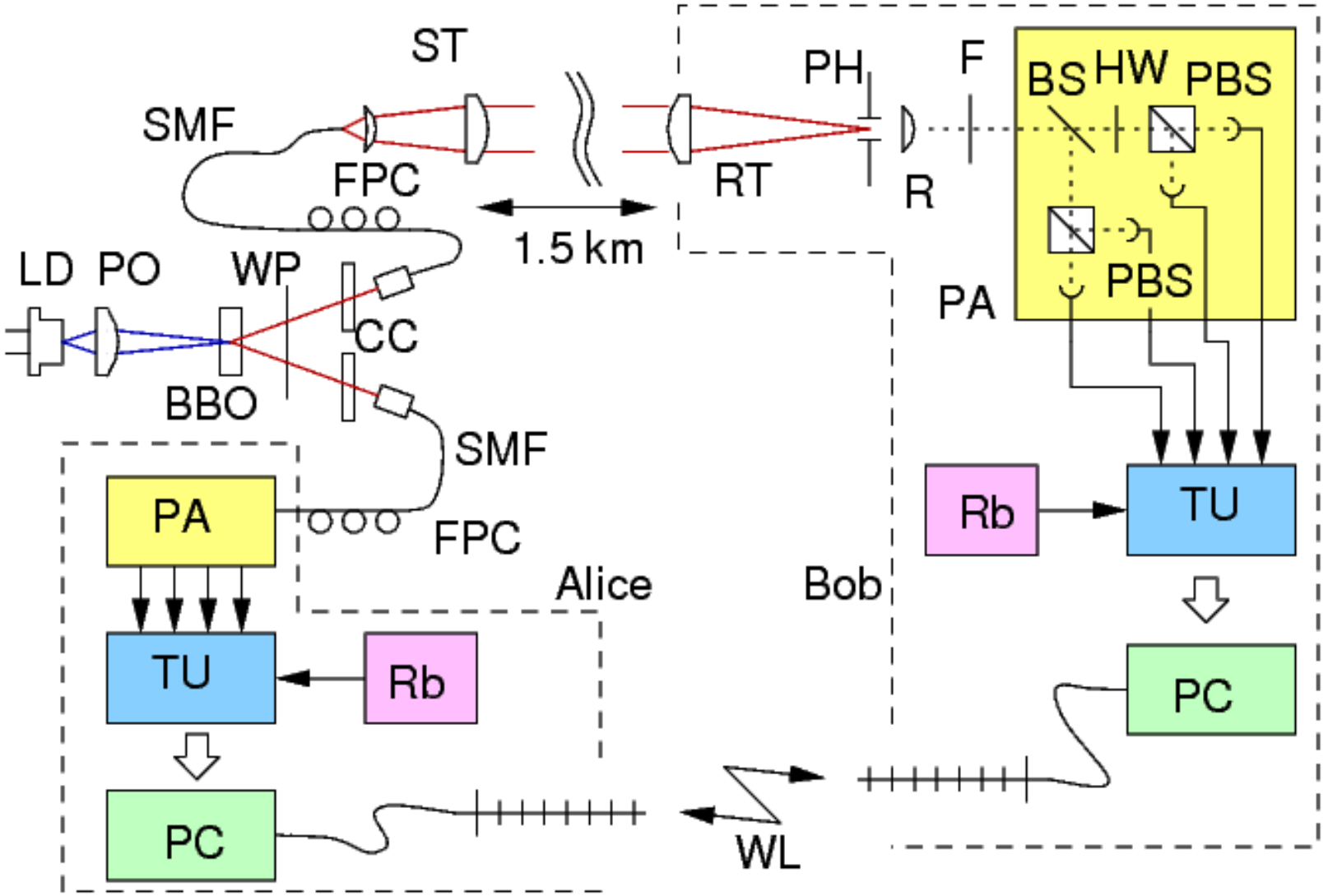
- compress raw key to the information advantage vs. Eve..



- 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

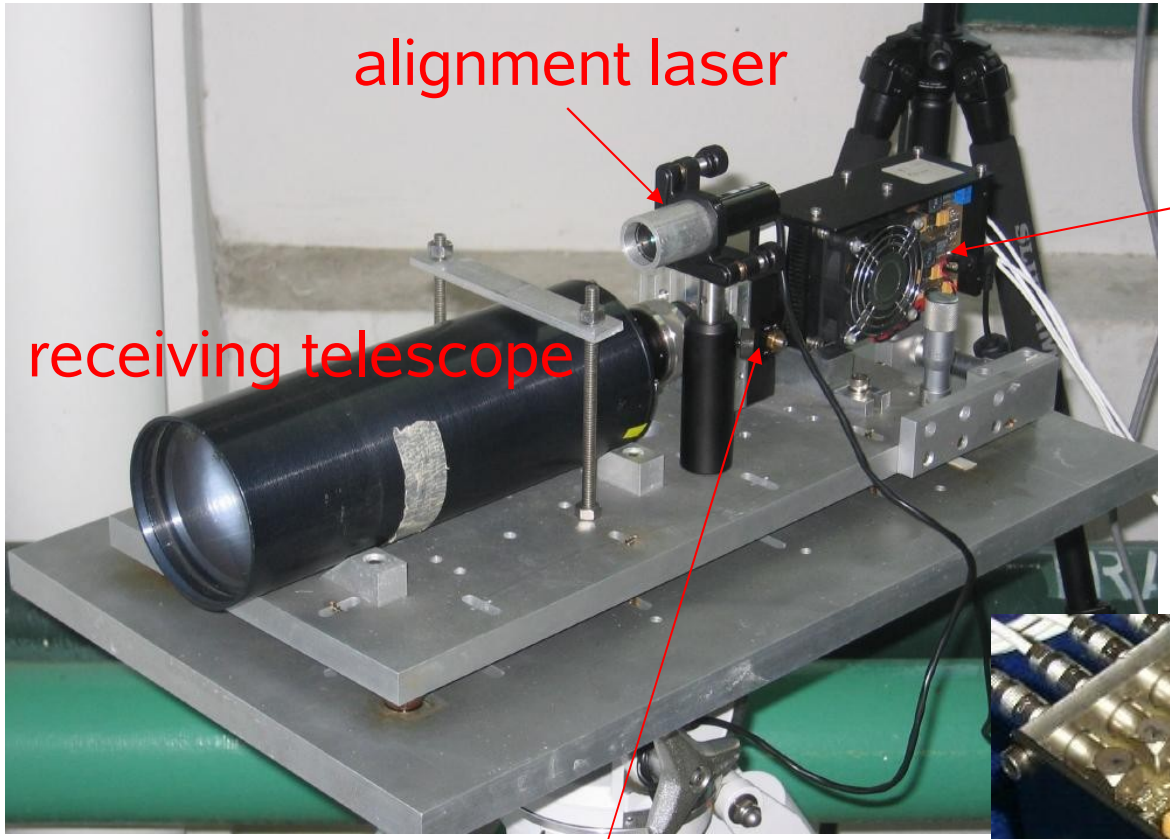
System setup



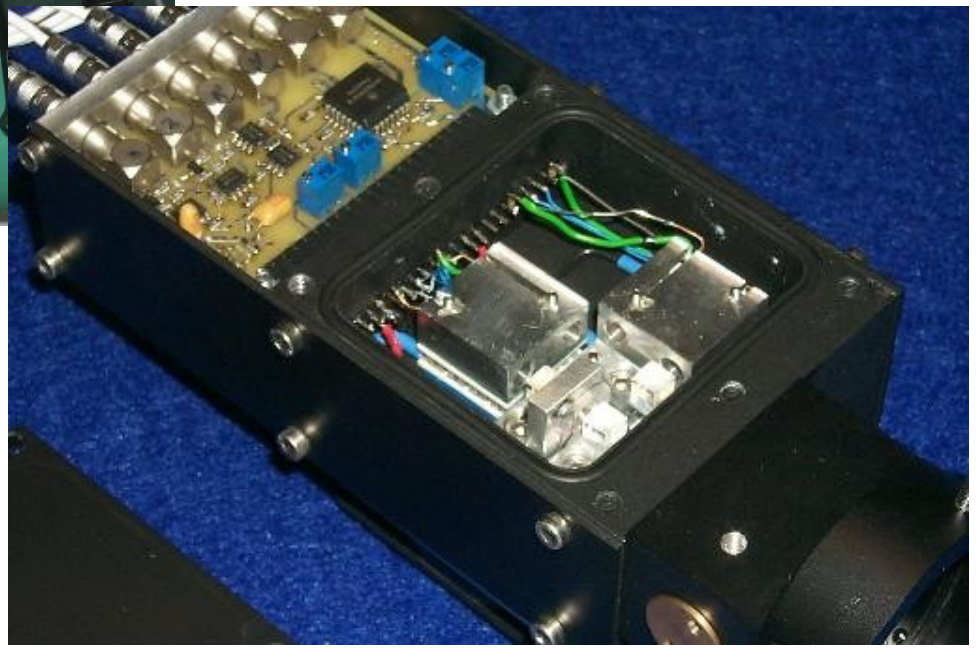
NUS campus test range

NUS National University of Singapore

Receiver unit



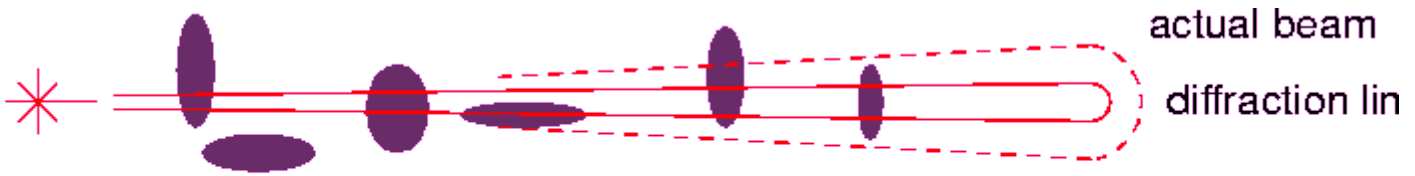
polarization analyzer
passively quenched
Silicon APD
- QE ~50%
~1000s^{-1} dark cnt rate



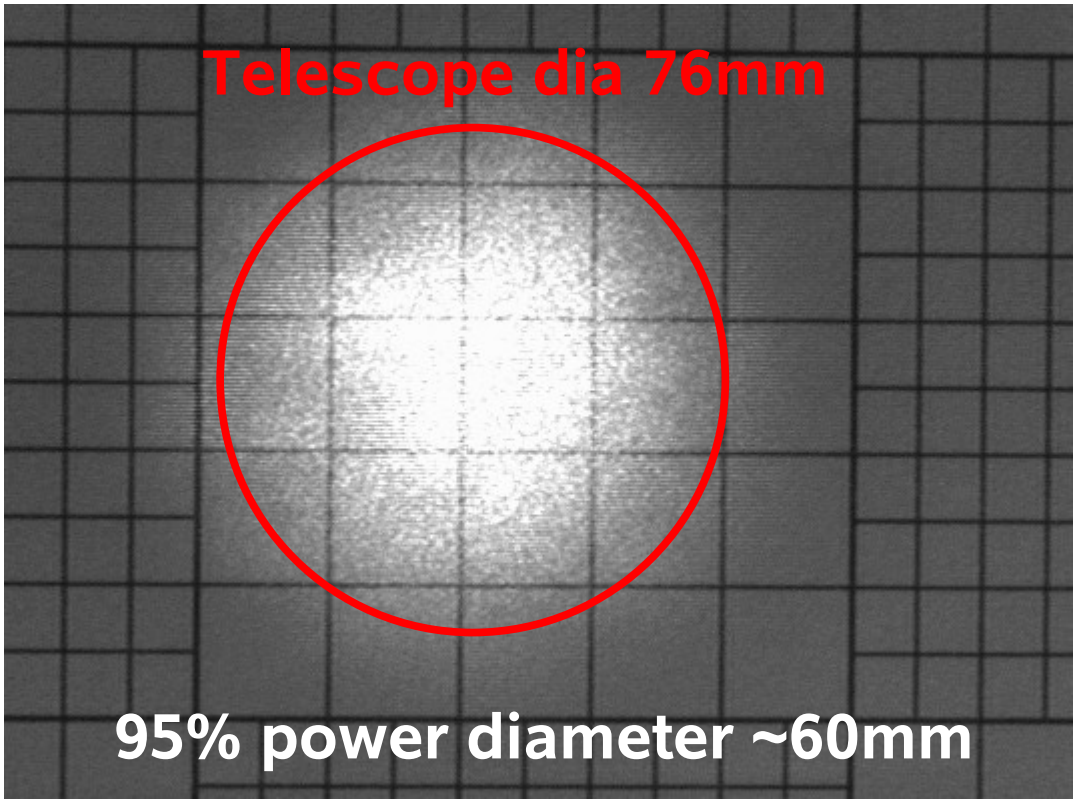
spatial filter (150 μrad)

visit exhibit @ .....

Scintillation in atmosphere

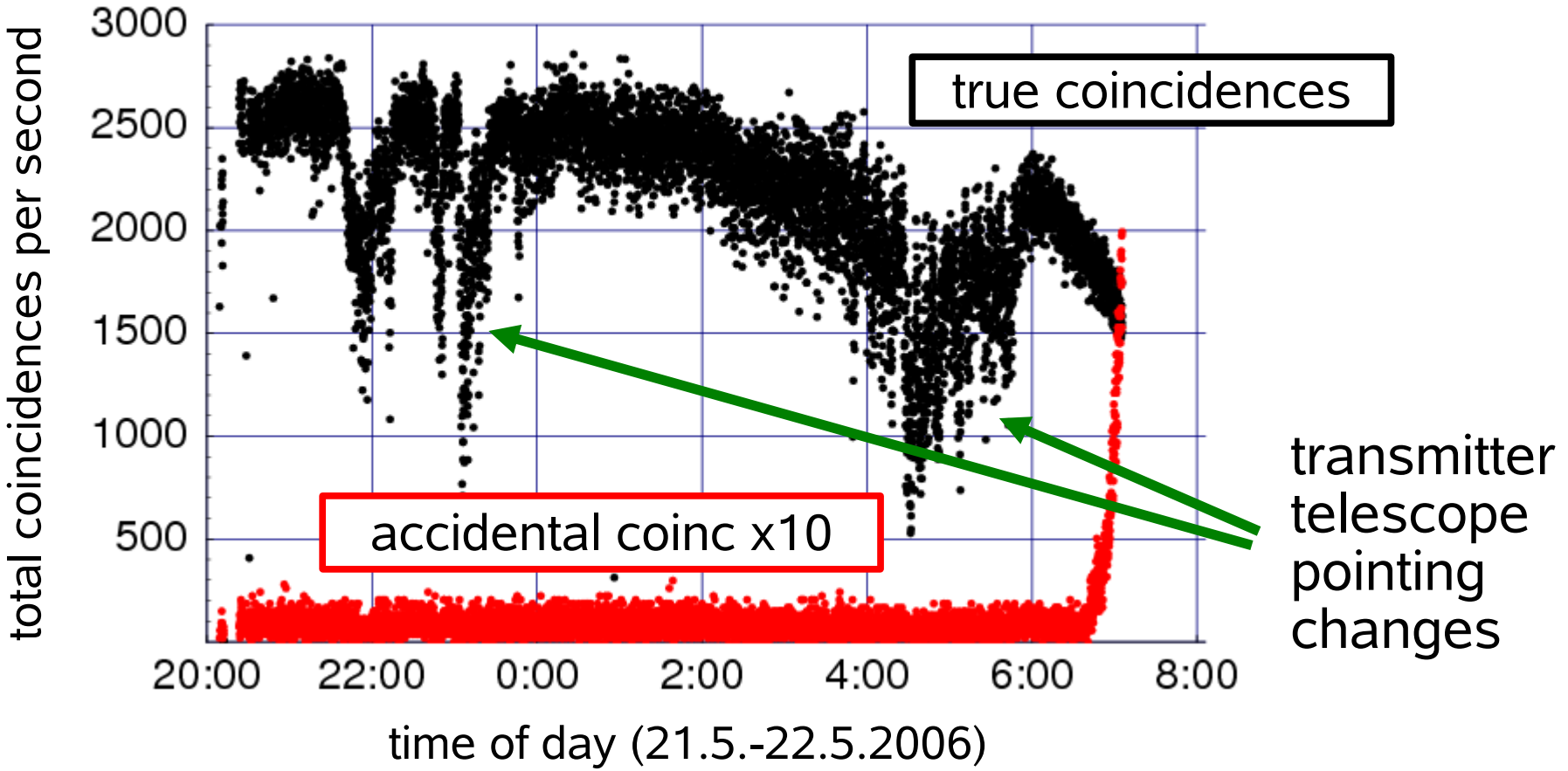


(40 mm FWHM)



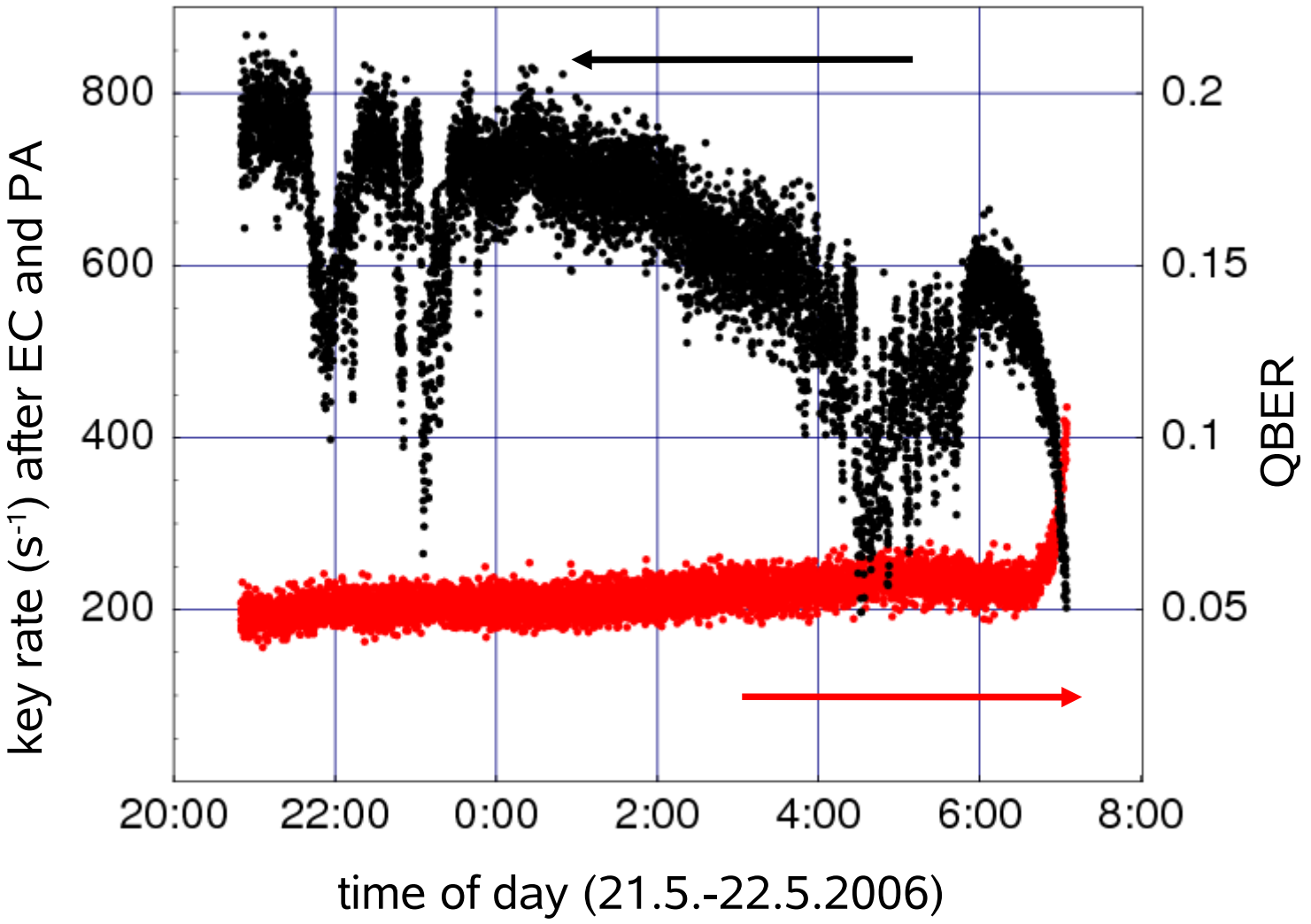
Experimental results I....

Identified raw coincidences between close and remote receiver



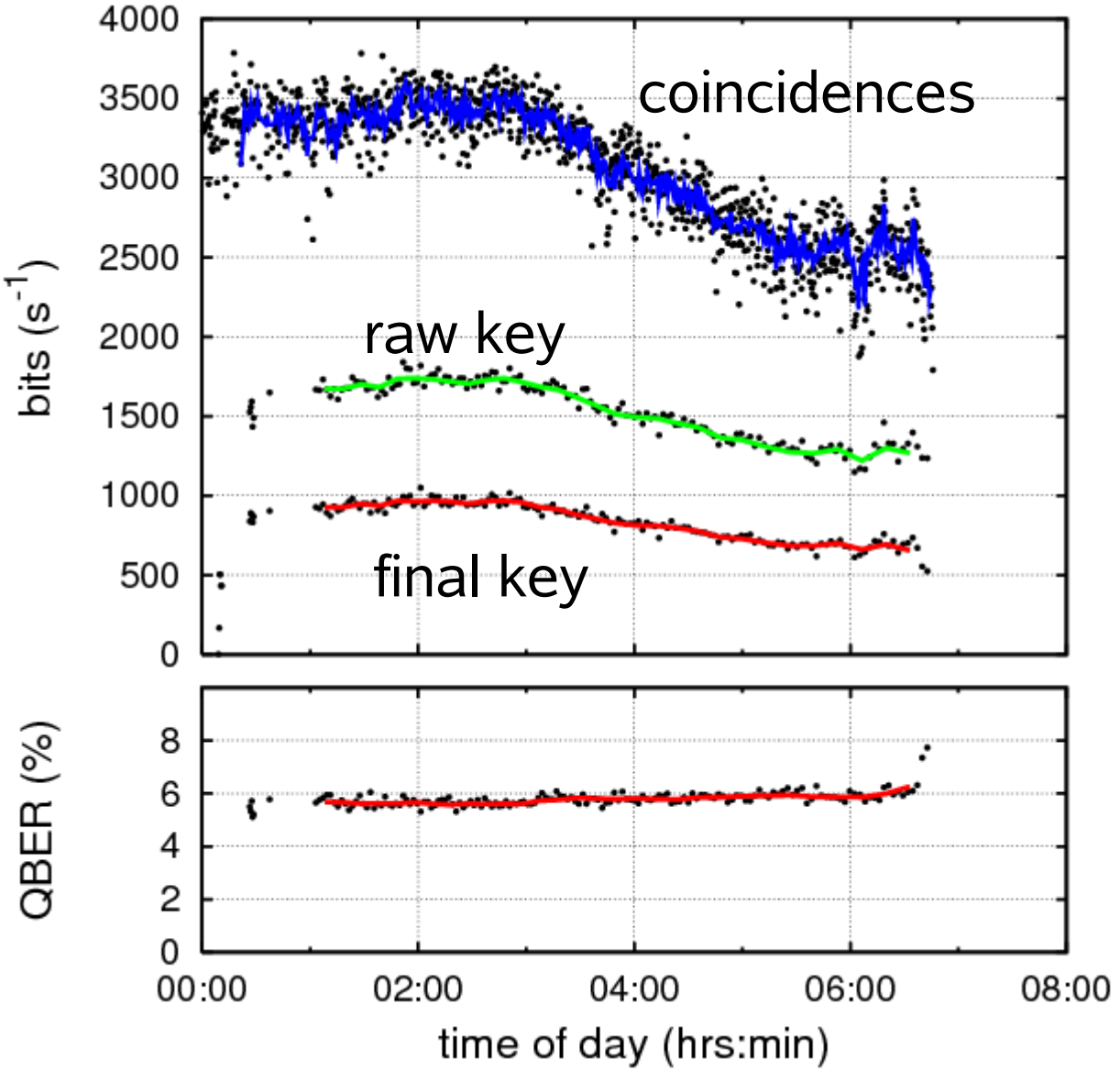
(with interference filter 5nm FWHM, 50% peak transmission)

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

Another run at night....



(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

NUS National University of Singapore

- Only passive components (no switches); technical complexity similar to CD a player
- No random numbers needed
- software-only synchronisation
- Lean sifting (~15...20 bits per event)
- Compact, install for ad-hoc situations
- Runs reliably hands-off, produces continuously key

visit exhibit/workshop @ level C staircase 29.12. 16:00

Is it now really secure ?

NUS National University of Singapore

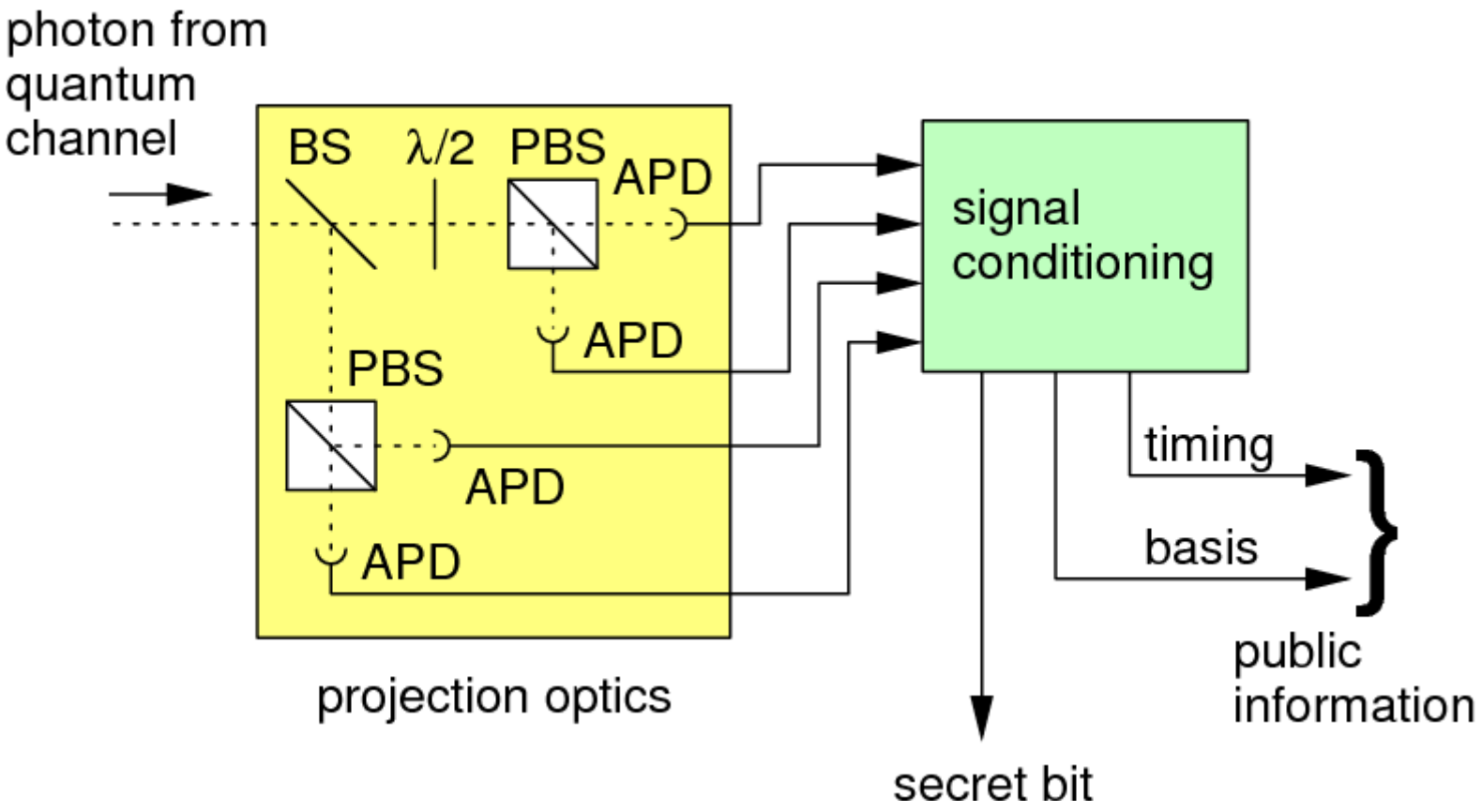
- No spectral fingerprint in transmitters
- No untrusted random number sources
- Software implementation bugs are probably always around

  Invitation: Look and software, try to find the holes

  details, code, description, (too little) documentation
  under http://qoptics.quantumlah.org/cryptoplay/

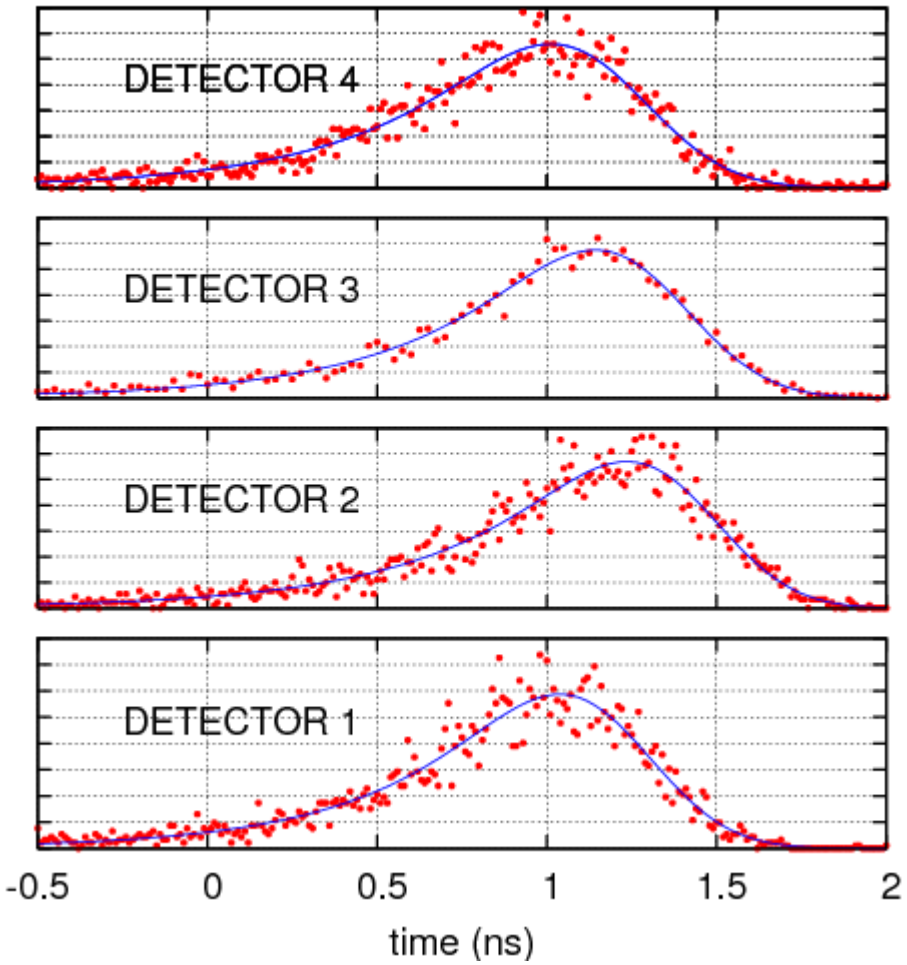
- Hmmm....there is a lot of timing information exchanged

Timing channel attack I

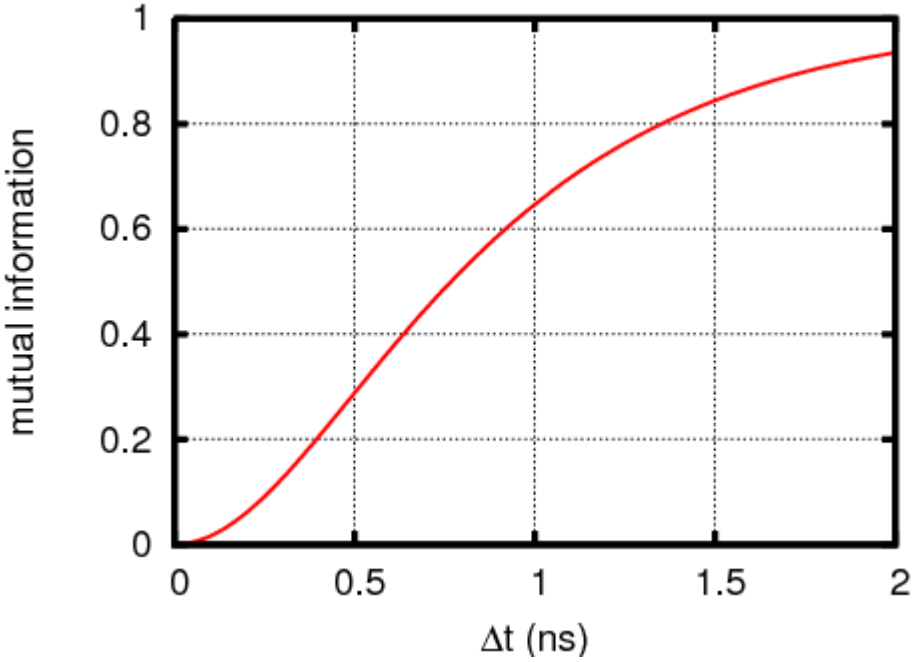


Timing channel attack II

Classical timing information carries fingerprint of detectors:



small detector imbalances may tell Eve a lot!

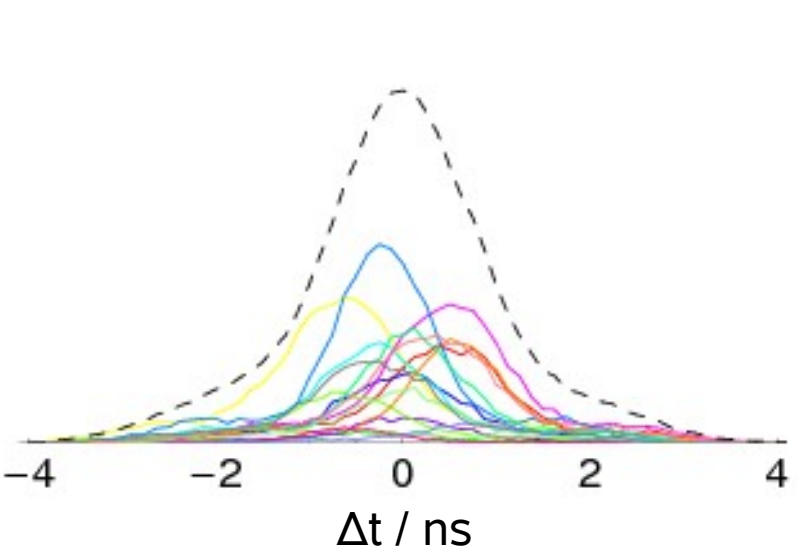


A. Lamas-Linares, C.K. quant-ph/0704.3297

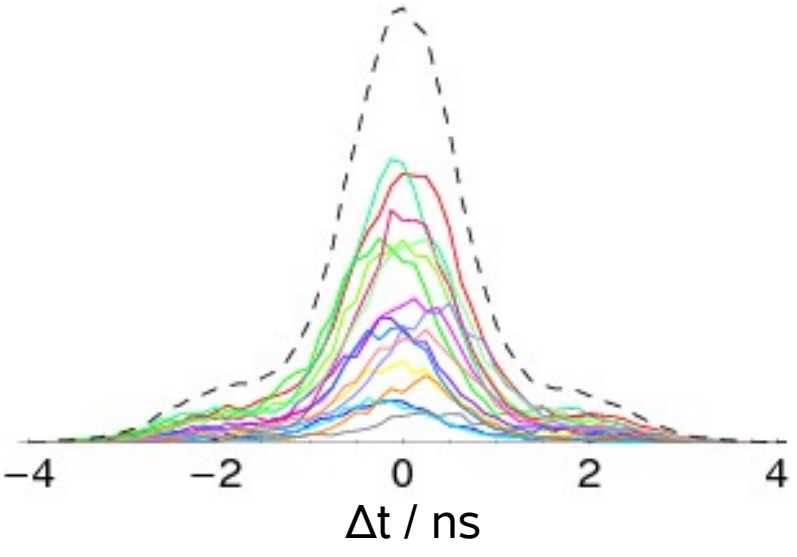
Timing ch attack – The Cure

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

delays not compensated



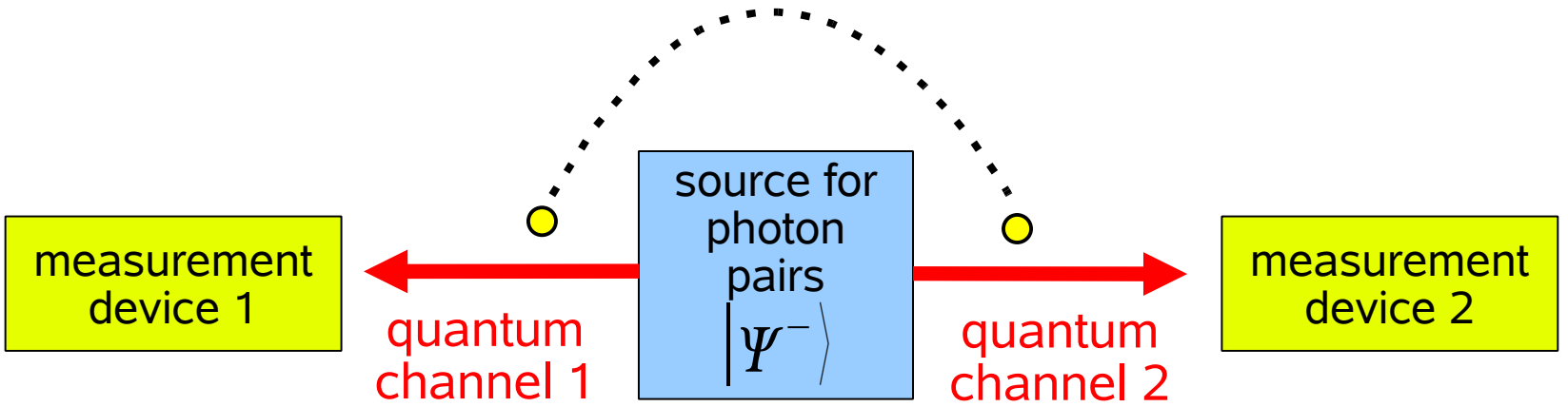
delays compensated

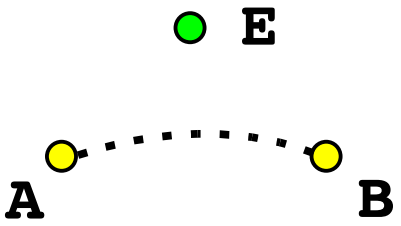


- Alternative cures (costly for background):
  - coarser quantized timing information
  - add timing noise

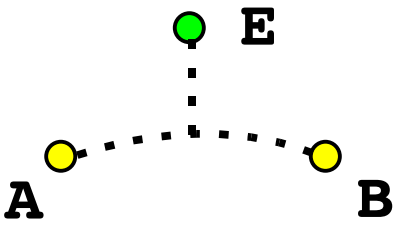
Entanglement based protocols

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



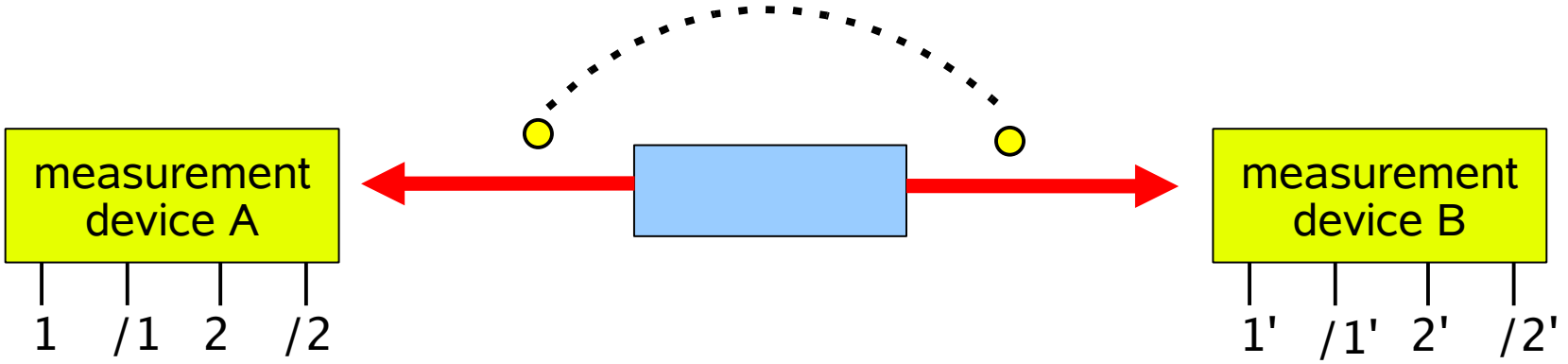


maximal entanglement
between **A** and **B**



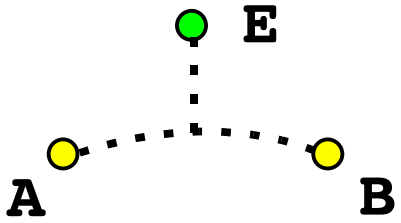
reduced entanglement
between **A** and **B**

Bell inequality I



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

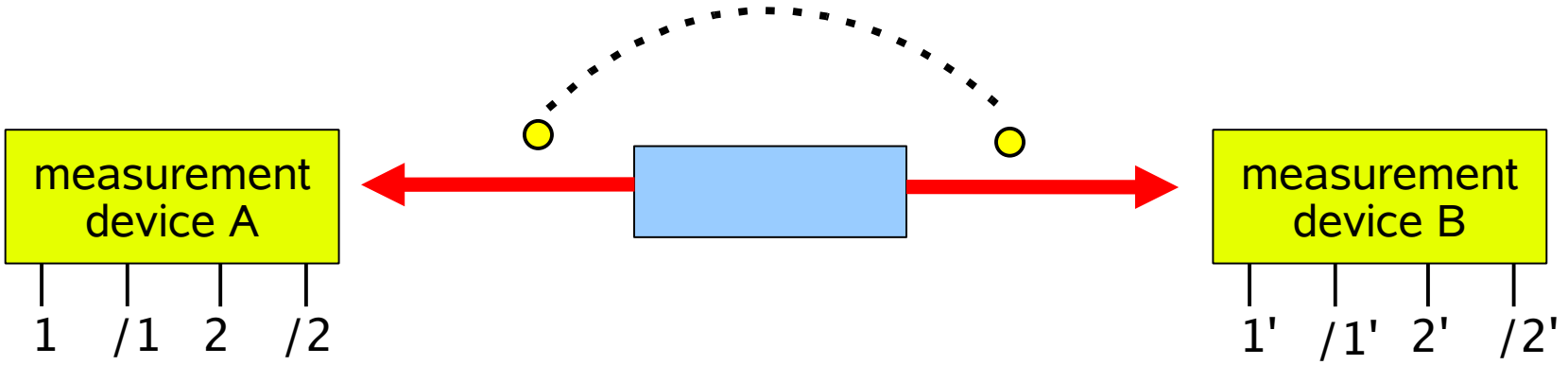
combined correlation function: $$S := E(1,1')+E(1,2')+E(2,1')-E(2,2')$$



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

$$|S| \leq 2$$

Bell inequality II



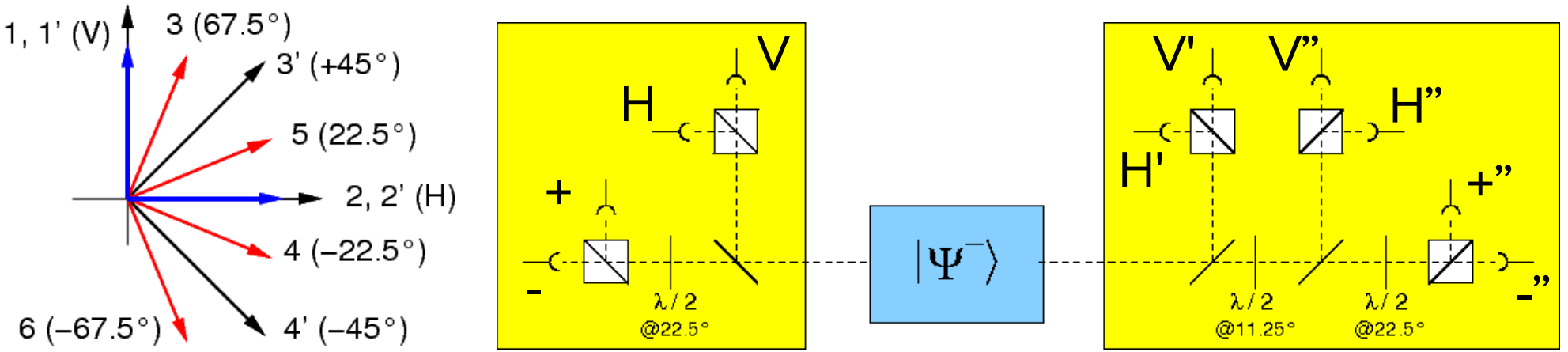
For proper settings 1, 2, 1', 2' and state $|\Psi^-\rangle$: $S = \pm 2\sqrt{2}$

- Estimate quantitatively the knowledge of Eve of raw key between A and B from S, and use part of the measurements to generate a key by measurement
- Assume “fair sampling” between key measurement and Bell test
- No fingerprint problems of photons due to sude channels

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

E91 Implementation

- use almost same kit:



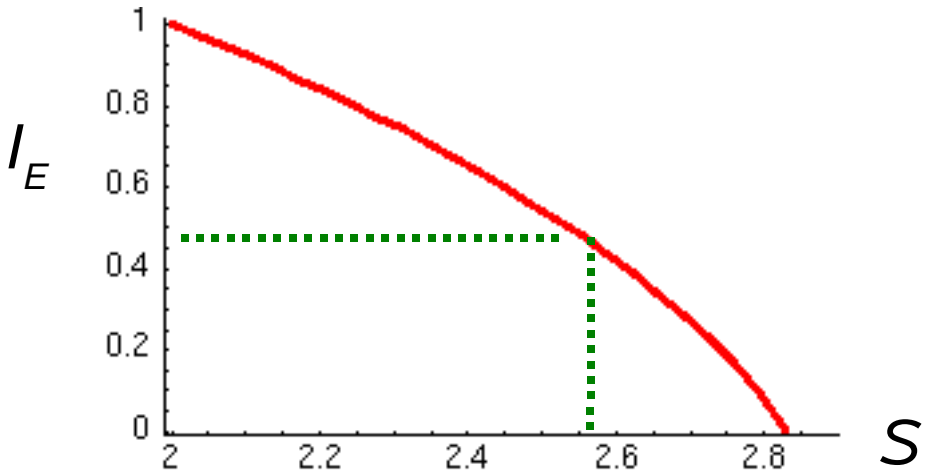
- {H,V; H',V'} coincidences → key generation
- {H,V,+,-;H",V",+",-"} coincidences → CHSH Bell test
- low QBER with existing simple source

Indoor results

NUS National University of Singapore

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

total identified coincidences:	N_c = 41x10^6 pairs
total collected raw key:	N_k = 11x10^6 bits
error ratio:	QBER = 1.97%
Bell violation over all events:	S = 2.569+/-0.001

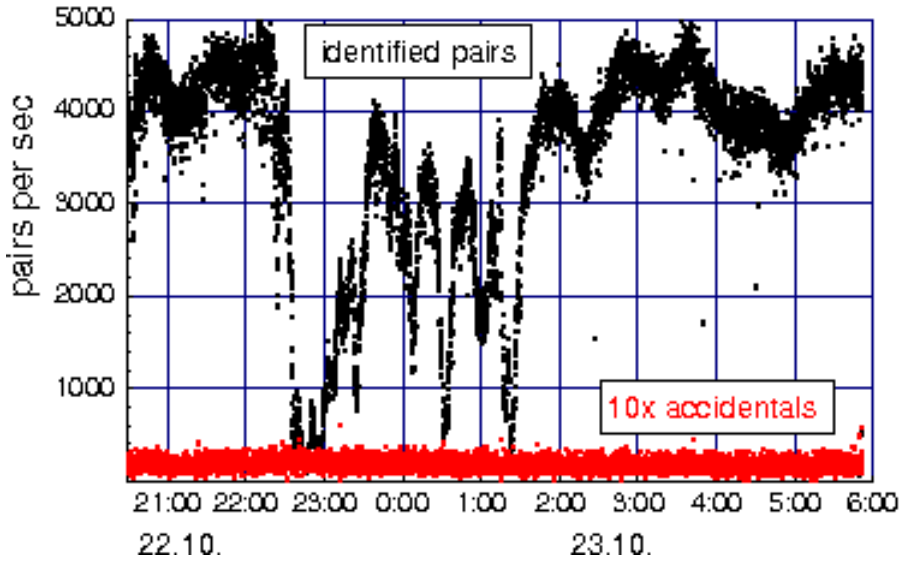


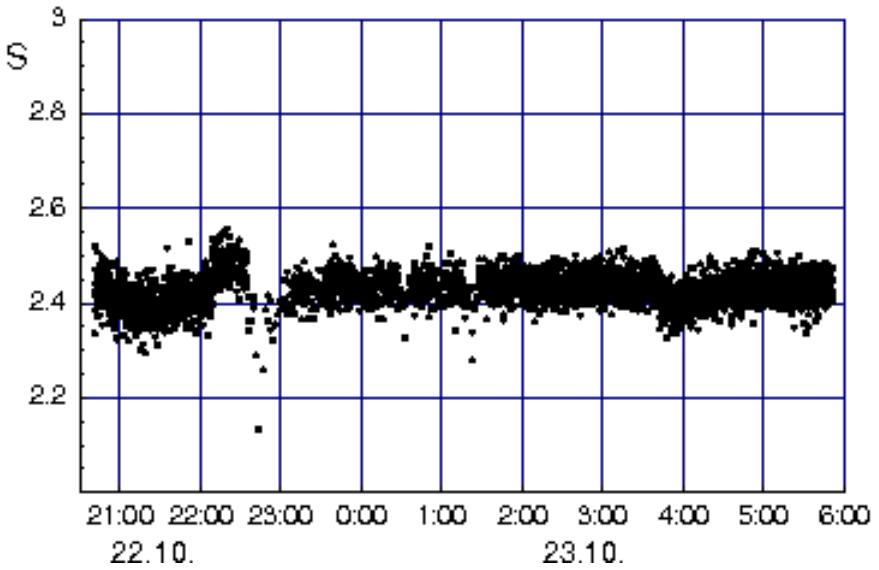
Holevo information of Eve:	I_E = 46.7%
key-contributing pairs:	27.4%
asymmetry:	$N_0/(N_0+N_1)$ = 0.49
QBER distribution on 0/1 bits:	1:1.67

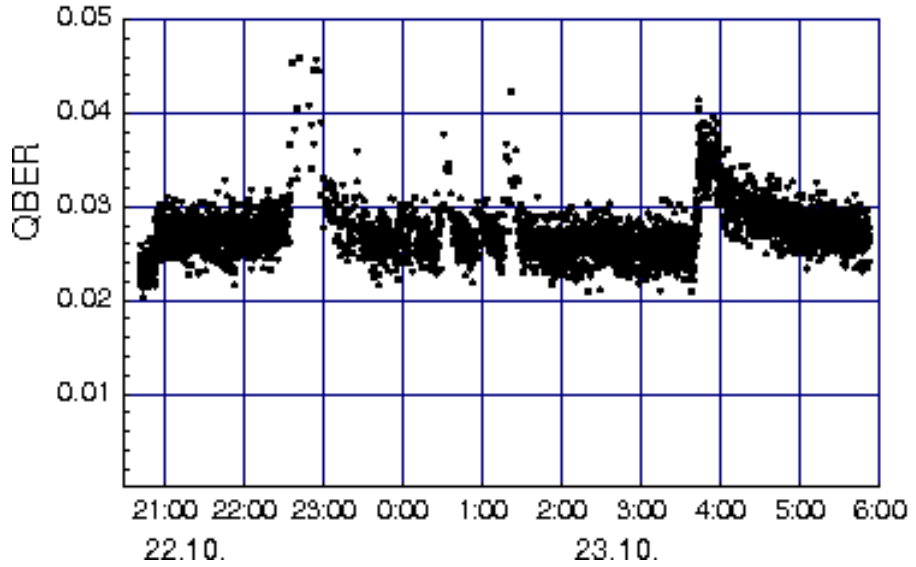
Field results (1.4km range)

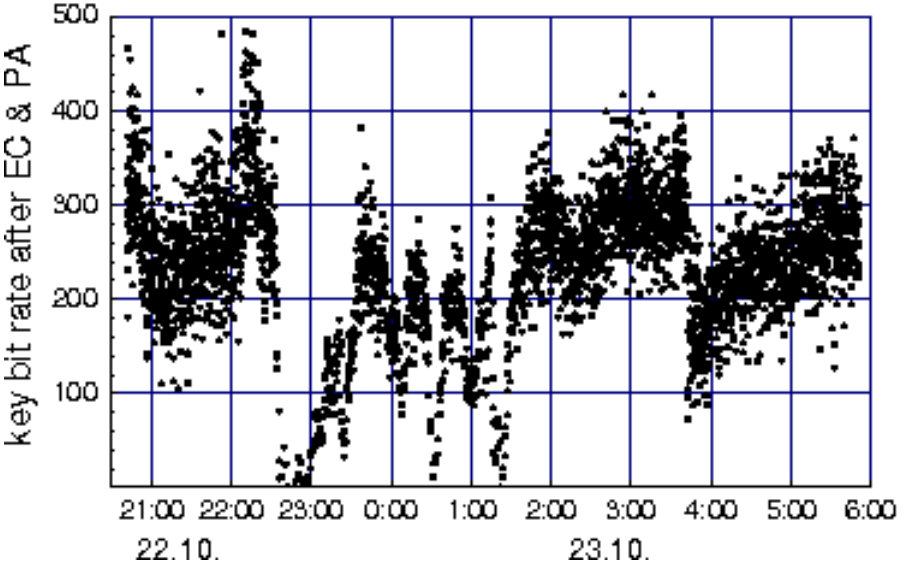
NUS National University of Singapore

- typical data run (with tropical rainfall inbetween)









Ongoing developments

NUS National University of Singapore

- 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.....

NUS National University of Singapore

Thank you !

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

code & data:

http://qoptics.quantumlah.org/cryptoplay/

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

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

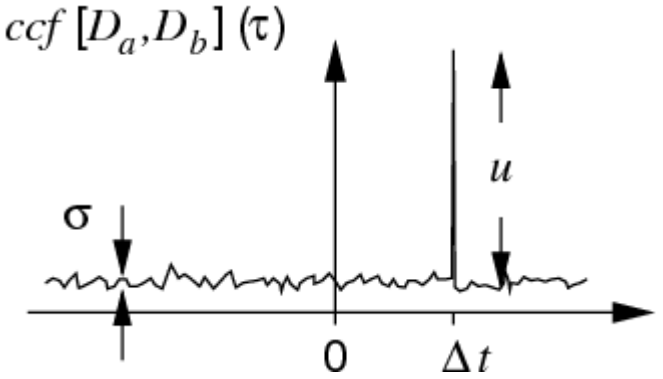
for $N=2^{17}$ and

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

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

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:

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

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

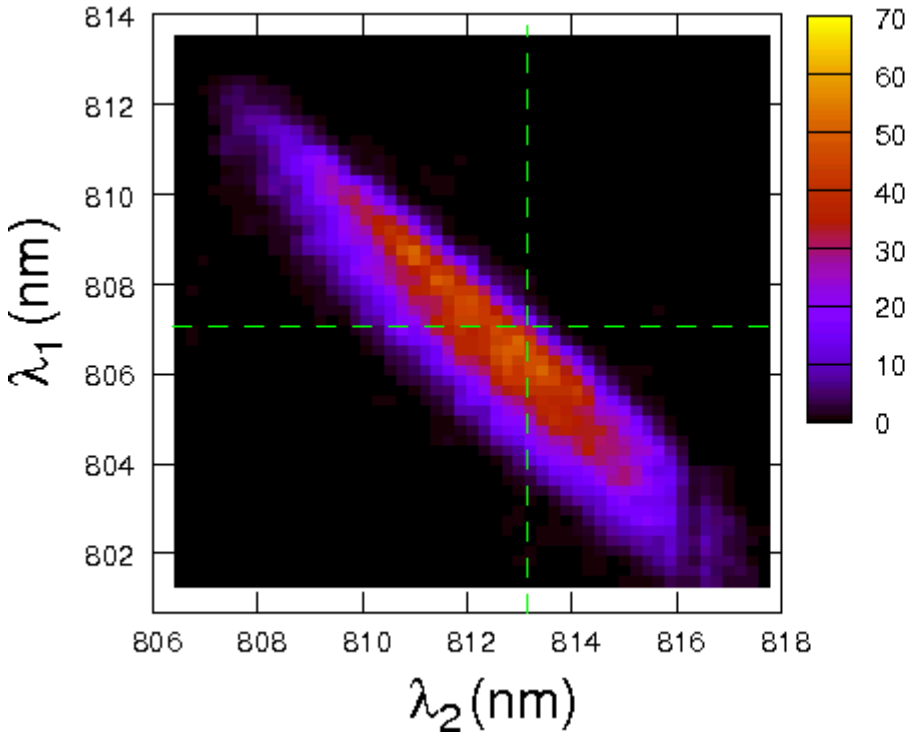
results vary, depending on overlap between sampled events

Conclusion: Periode finding works with very little numerical effort!

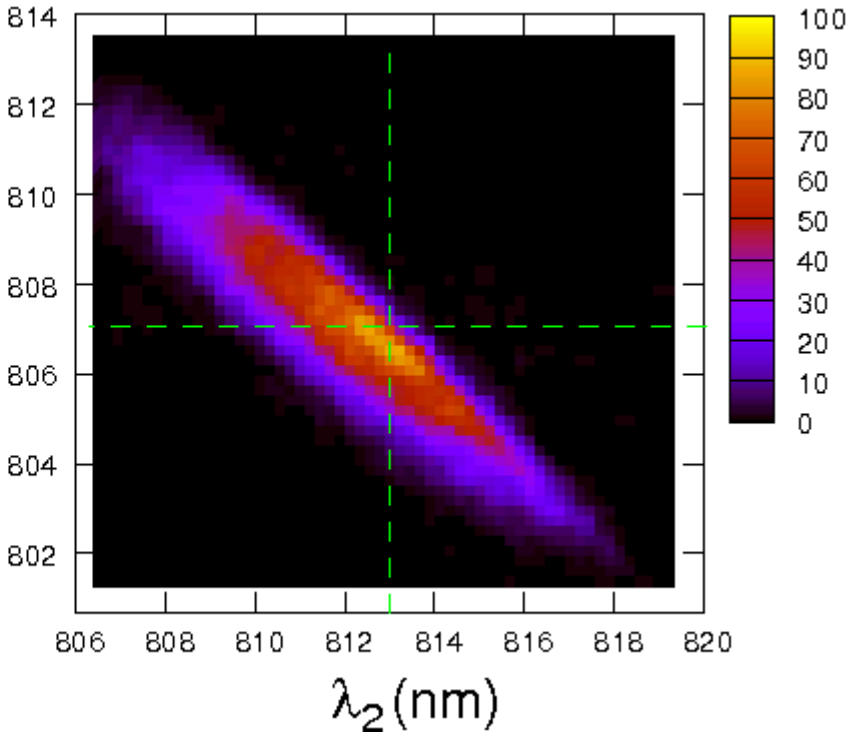
Limits of (this) pair source

- Spectral distinguishability of decay paths:

HV coincidences



VH coincidences



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

The Quantum Channel

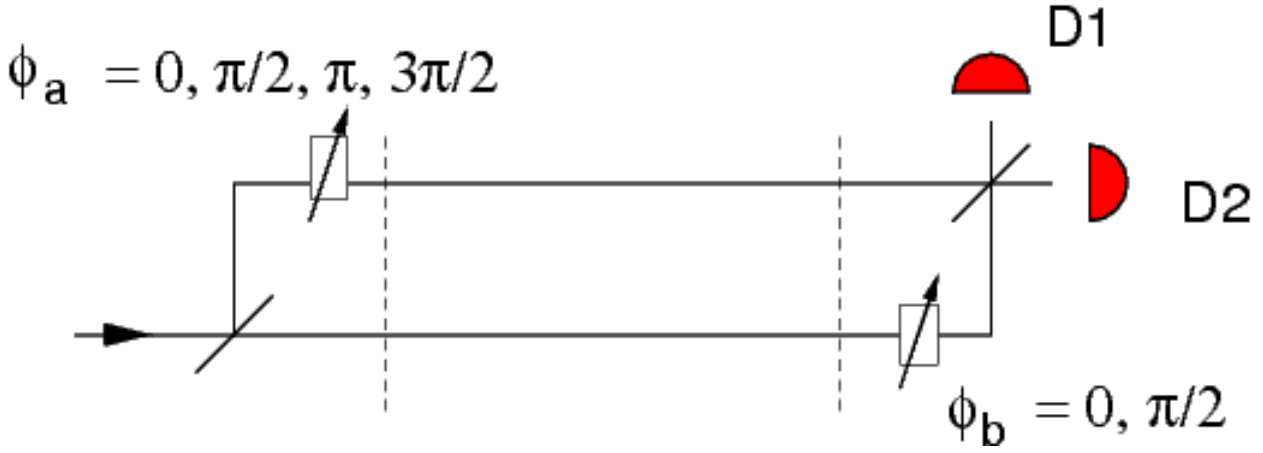
NUS National University of Singapore

- 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

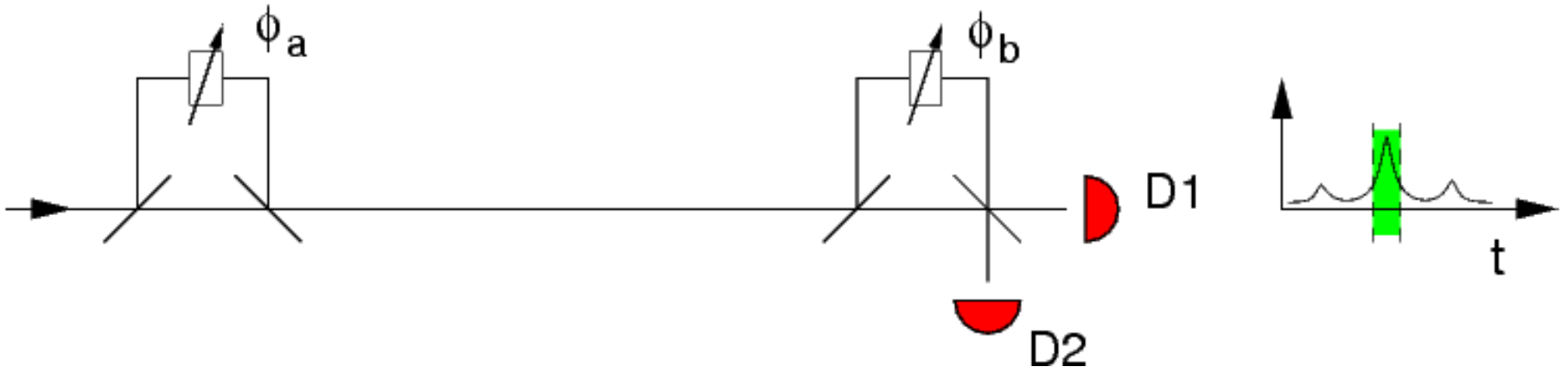
Other encoding techniques

- Encoding qubit in relative phase between two packets



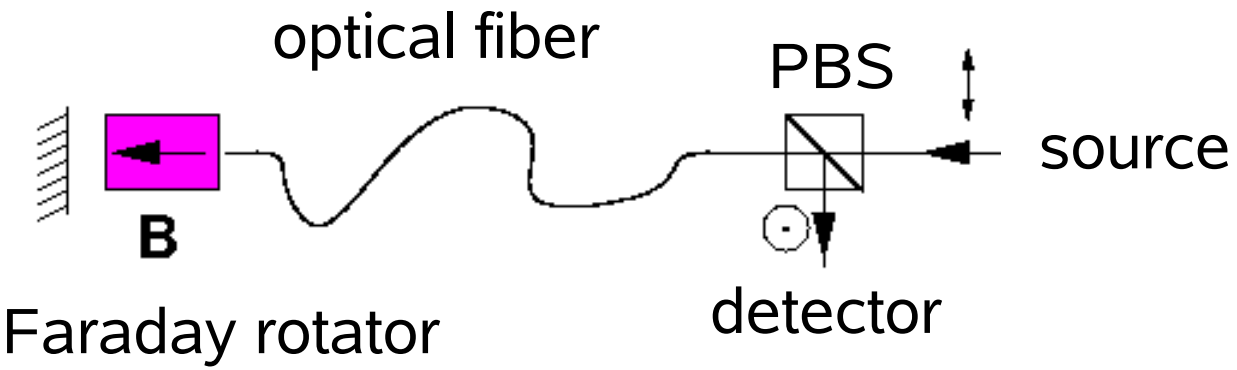
equivalent to polarization encoding

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



Birefringence compensation

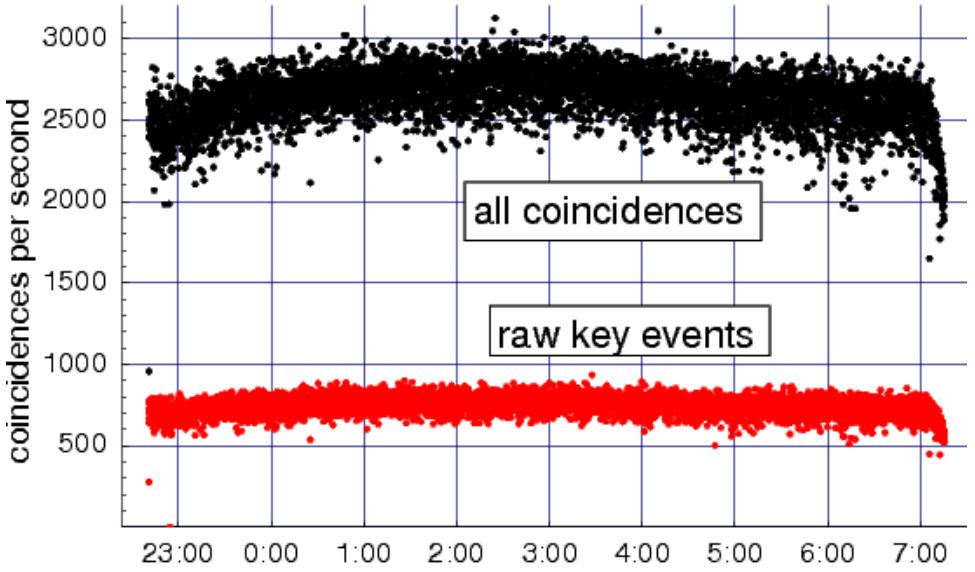
- Probe fiber birefringence via two passes with Faraday mirror

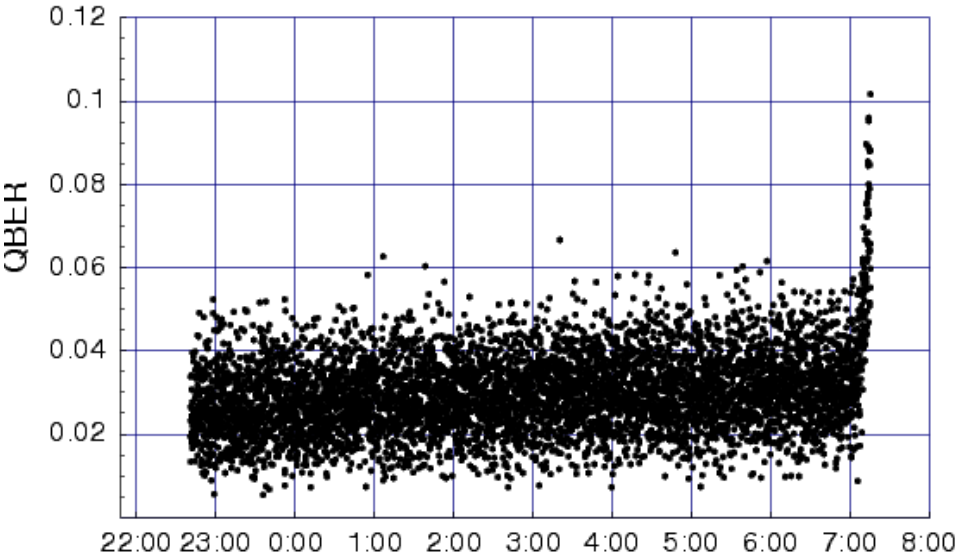


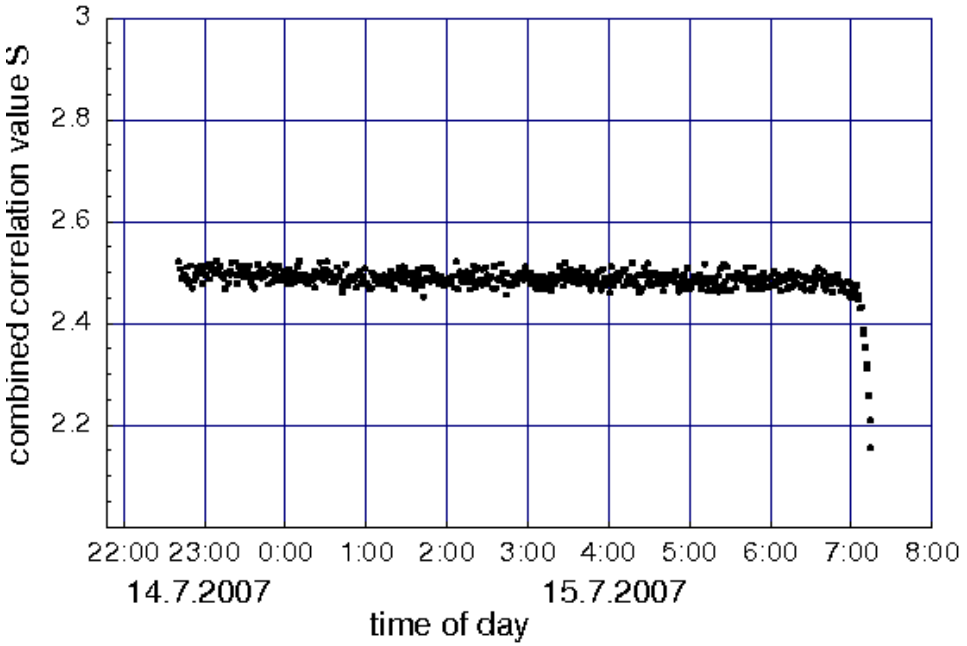
- Basis of “Plug & Play” or autocompensation schemes in commercial QKD systems (id quantique, NEC)
- Bridging ~100 km

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

E91 protocol, 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.....

Rate & Error Estimations

- BB84 raw key rate:

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

#photons/pulse; 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

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

Challenges for daylight QKD

NUS National University of Singapore

- 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*

Entanglement

NUS National University of Singapore

- Two things A, B can be in a well defined joint state, but each thing itself is in an undefined state.
- The two things can even be far apart, and remain still in the same state. The entanglement holds.
- Example: A and B can be in H or V, but the pair can be in a state

$$\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|H_A V_B\right\rangle - \left|V_A H_B\right\rangle\right)$$

- Neither A nor B is in H or V, but A is always orthogonal to B