# *Full Eavesdropping on a practical QKD system*

Qin Liu, Ilja Gerhardt,Vadim Makarov,
Johannes Skaar, Antia Lamas-Linares, Valerio Scarani,
Christian Kurtsiefer

Centre for
Quantum
Technologies

NUS
National University
of Singapore

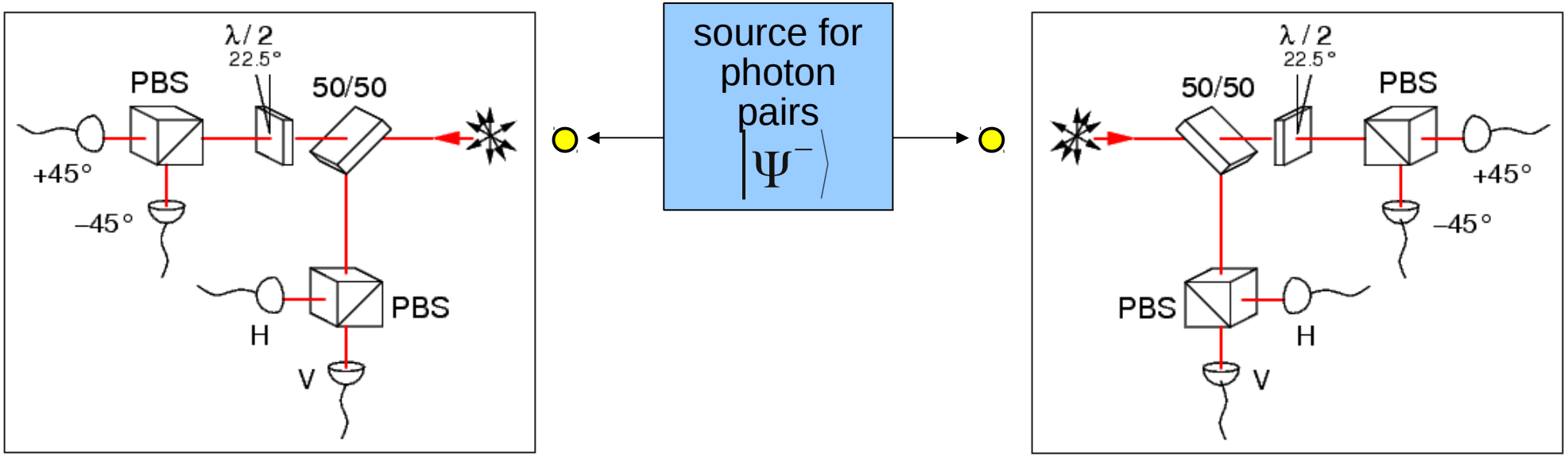
*JTuC2 – CLEO:QUELS , 2. May 2011, Baltimore*

# *Overview*

- Our BB92 QKD implementation
- Photodetector vulnerability
- Practical attack on BBM92 for a fiber channel
- Device-independent protocol and the 'Faking' the violation of a Bell test

# QKD with photon pairs: BBM92

Quantum correlations & measurements on both sides



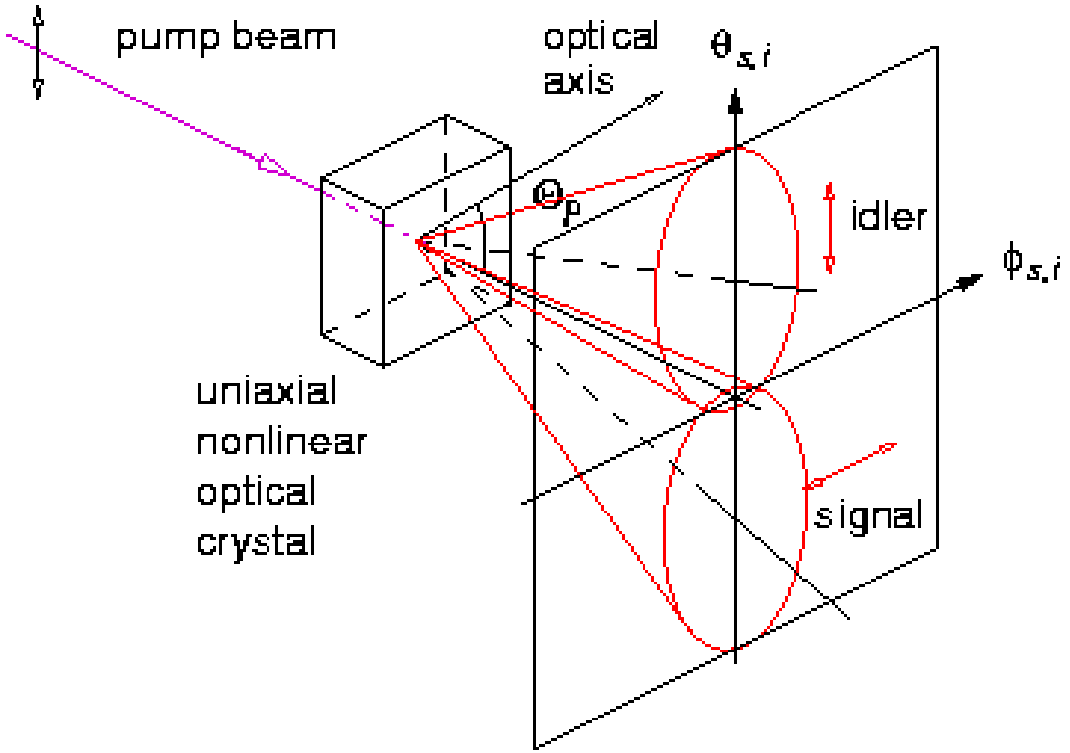

public discussion (sifting, key gen / state estimation)

error correction, privacy amplification

- like BB84, but no trusted random numbers for key
- direct use of quantum randomness for measurement basis

# *Entangled Photon Source*

- Use non-collinear type-II parametric down conversion




two indistinguishable decay paths lead to

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

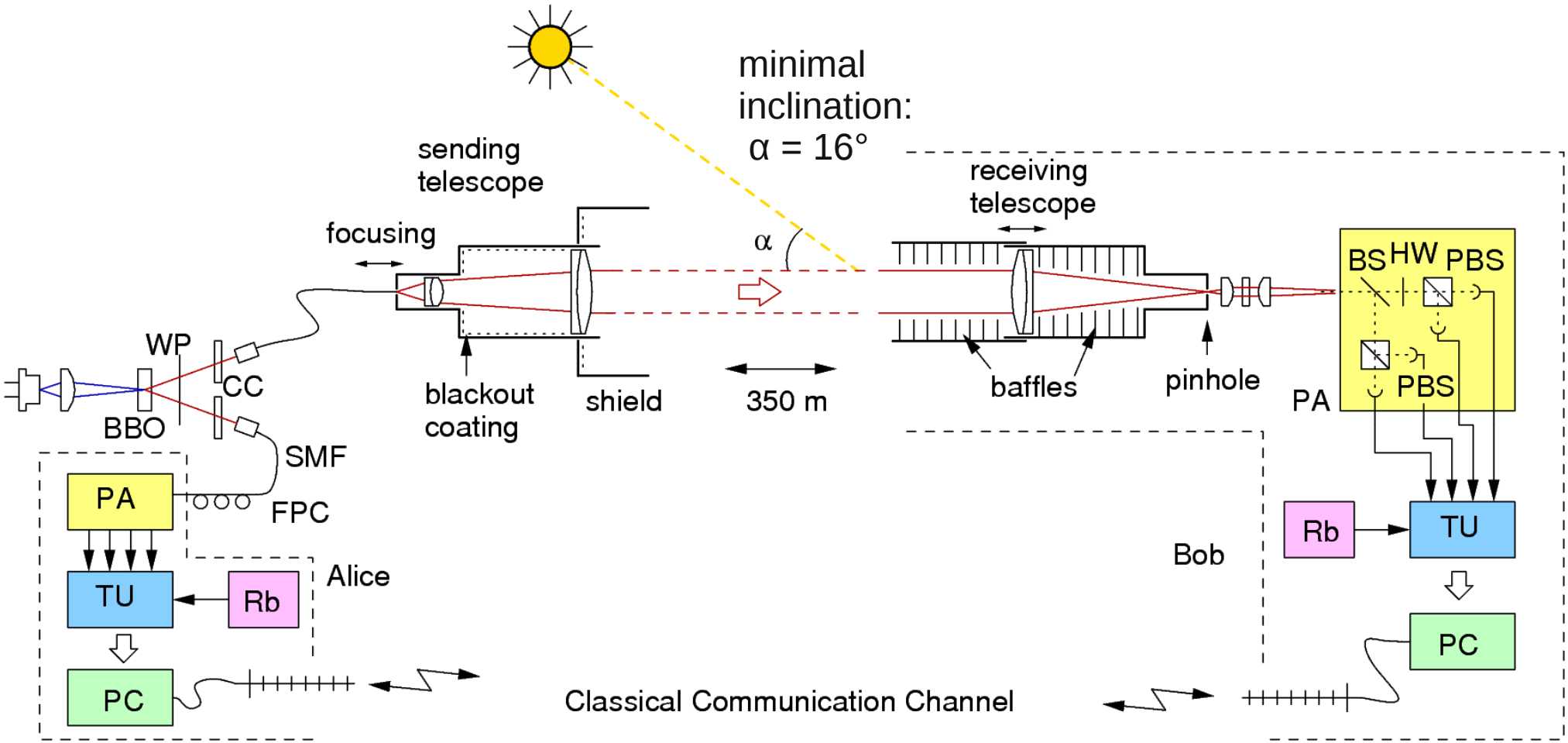
*P.G. Kwiat et al., PRL **75**, 4337 (1995)*

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

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

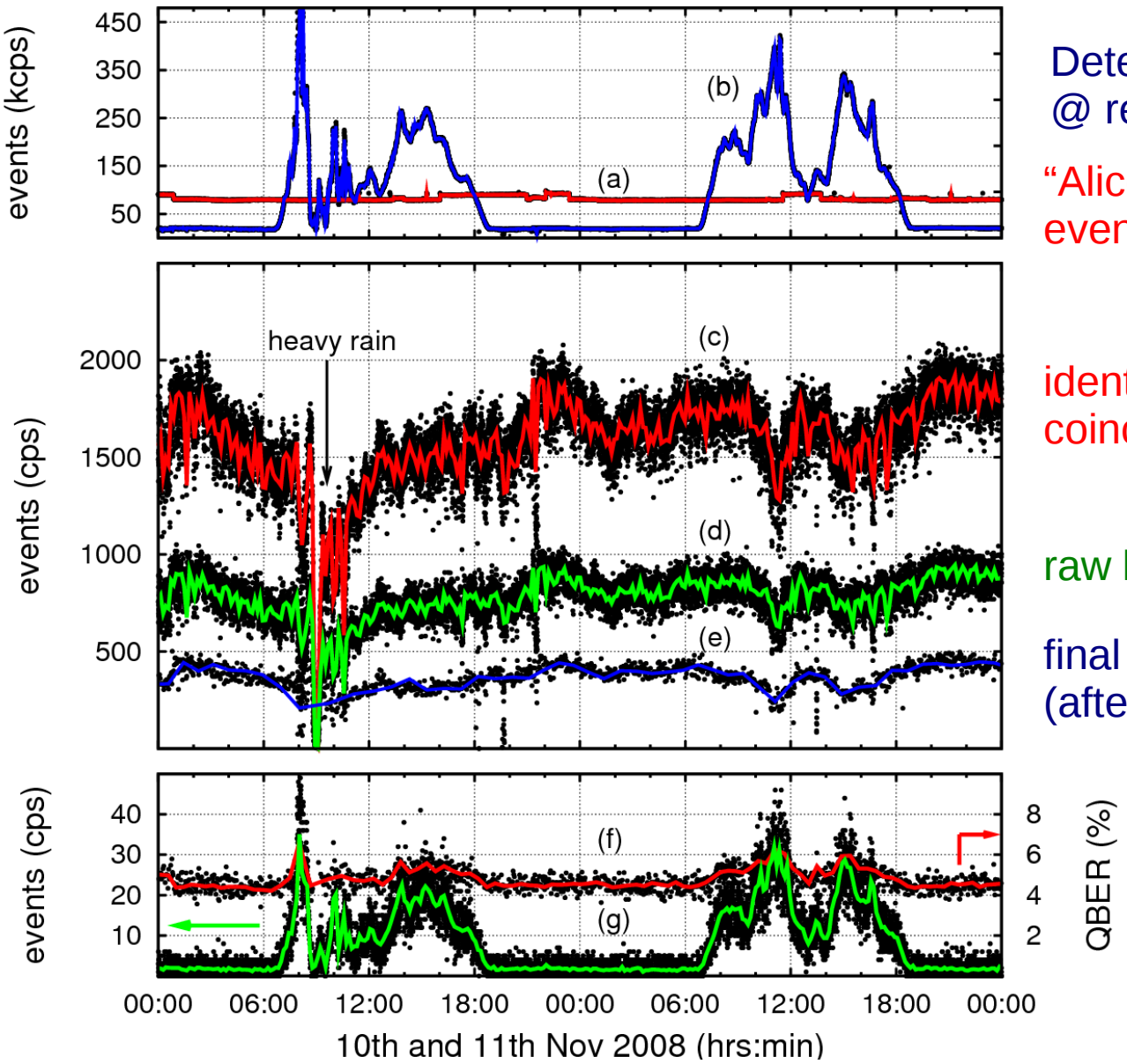
# *Our reference QKD system*

**free space link, works even in daylight**




- polarization encoding, cw pair source, wavelength 810±3nm
  timestamping photoevents

# *Typical performance*




Detector events @ receiver

"Alice" detector events

identified coincidences

raw key

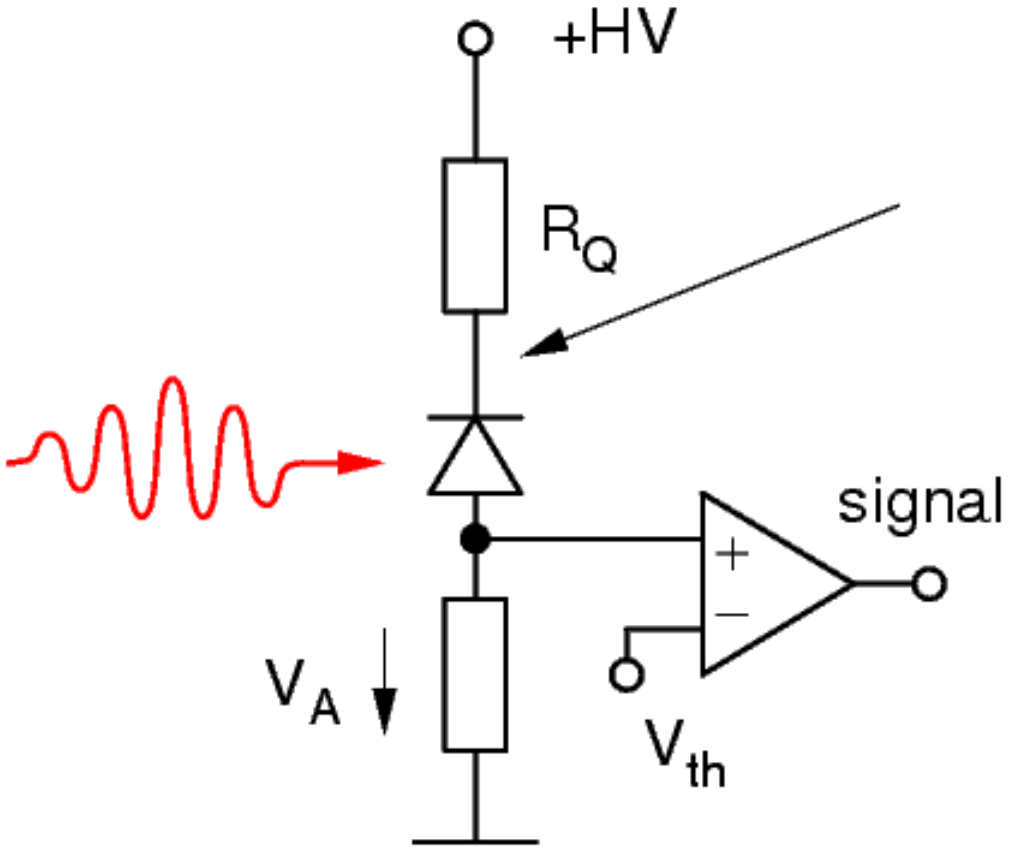
final key (after EC/PA)

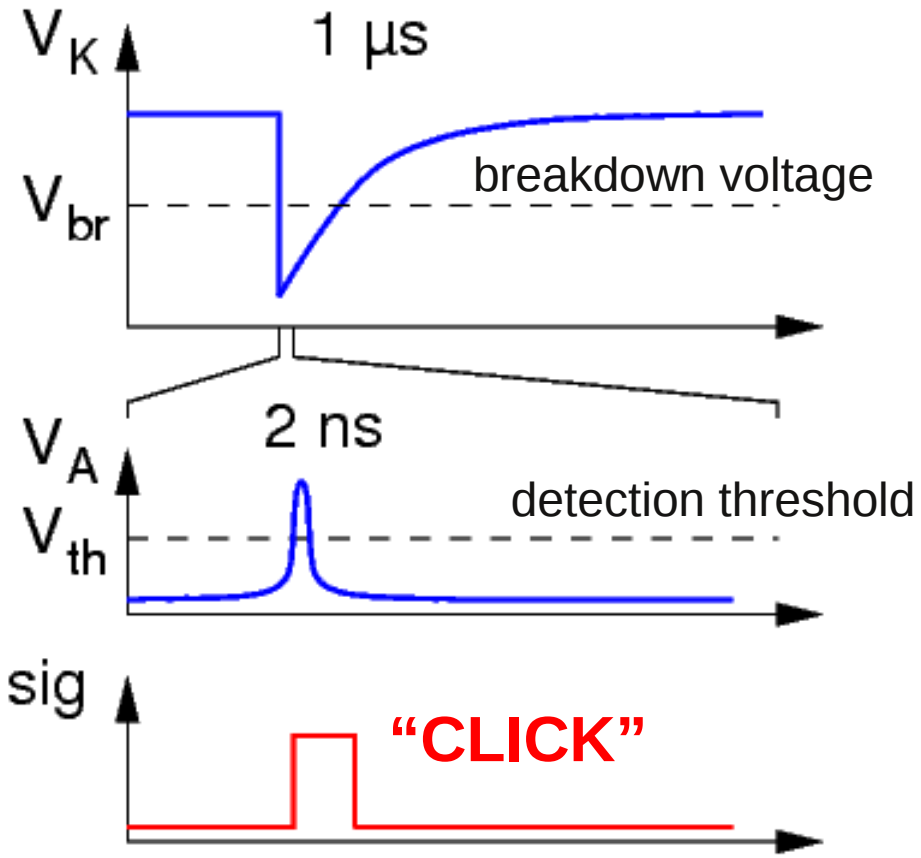
- optical BW: 6.7 nm FWHM
- coincidence time 2 ns
- receiver telescope: 100 μrad
- continuous operation over 4 days

*M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, C.K., NJP **11**, 045007 (2009)*

# *Basic photodetector operation*

**Avalanche photodiodes (APD) are common "single photon" detectors**

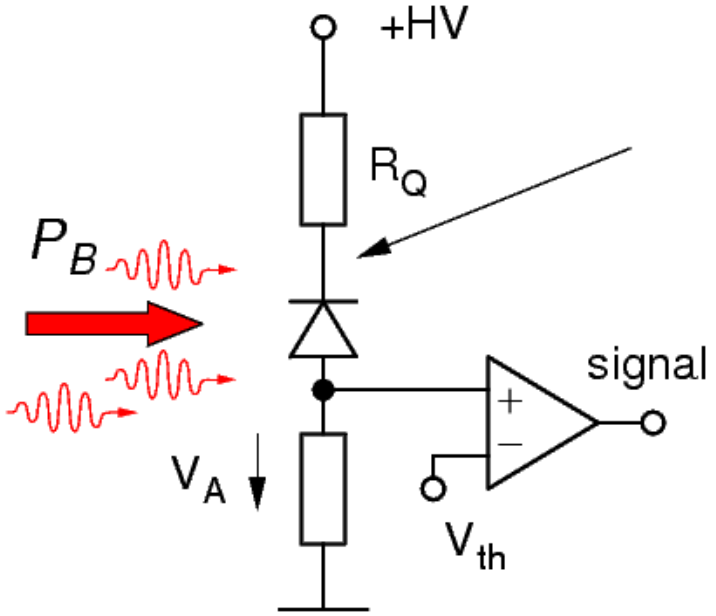


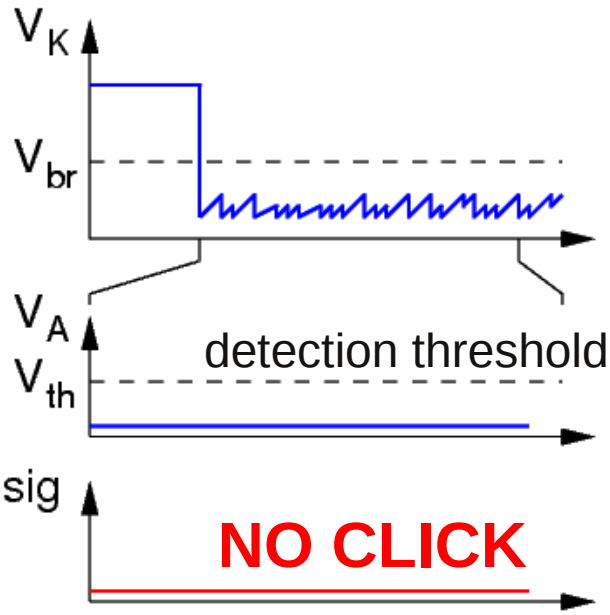



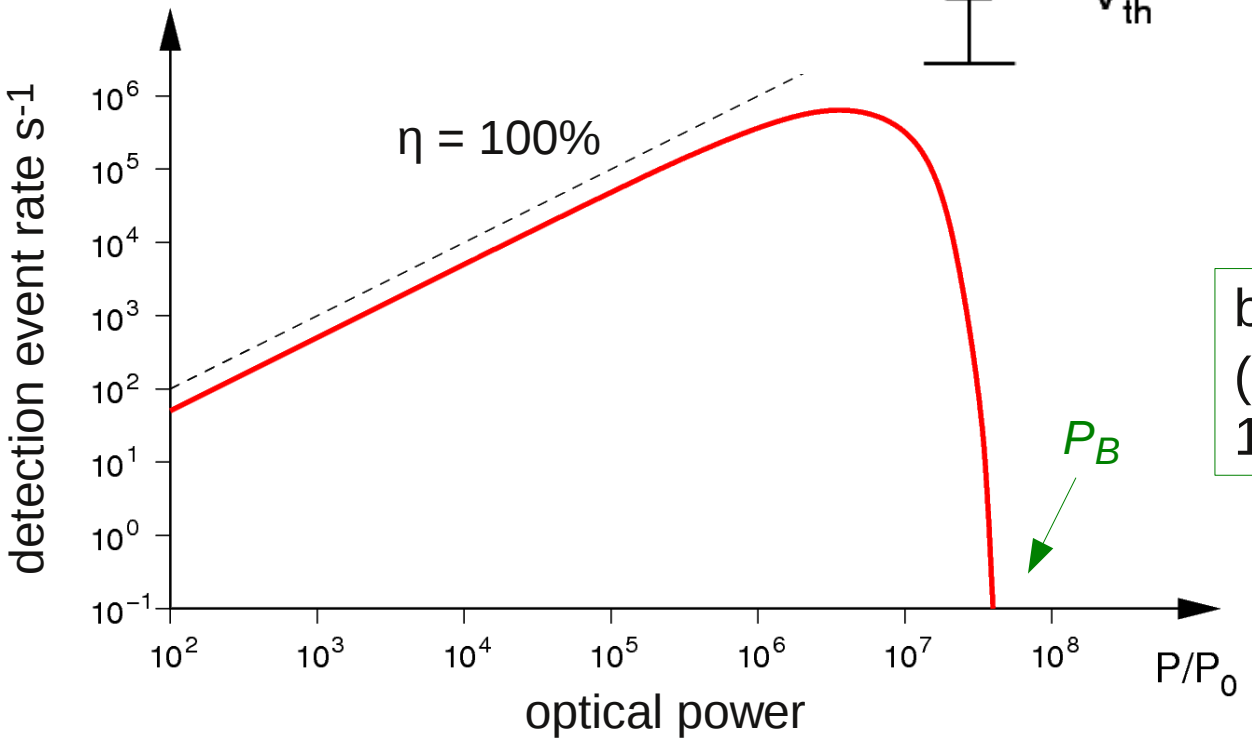
# APD detector vulnerability I

**Basic Problem:**

**APD saturate and can be blinded**



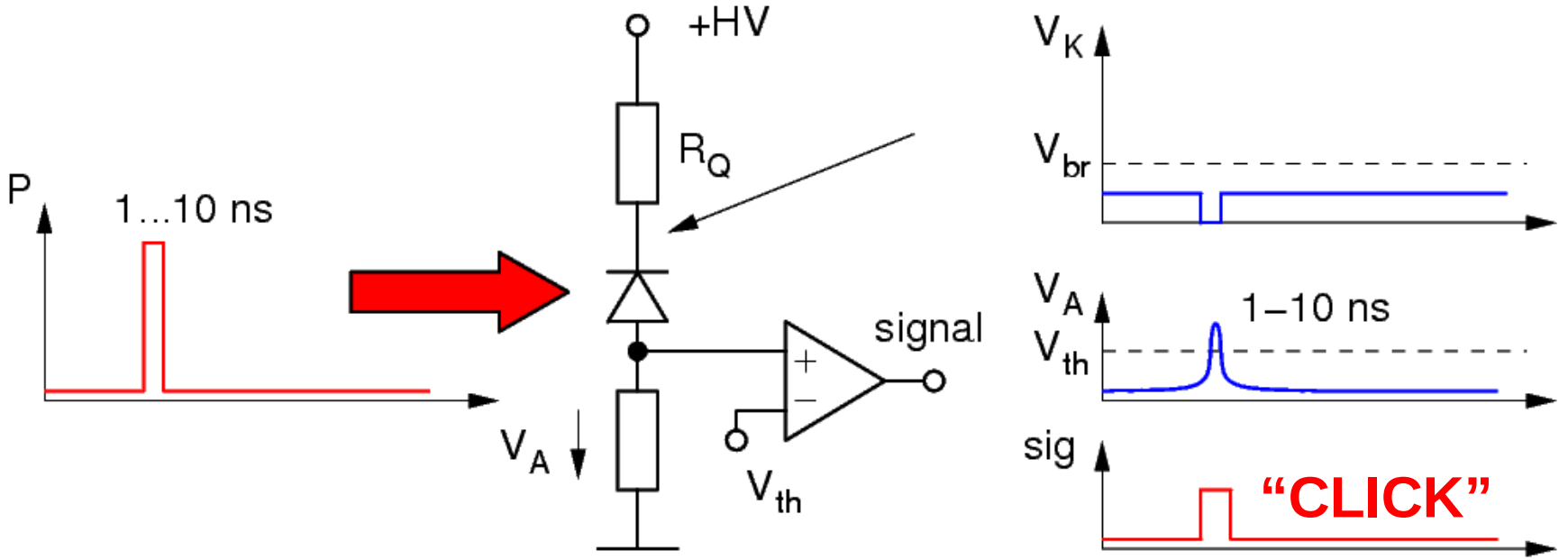




blinding power $P_B$: 1..10 pW
(corresponding to
$10^6$-$10^7$ events / sec)

# *APD vulnerability II*

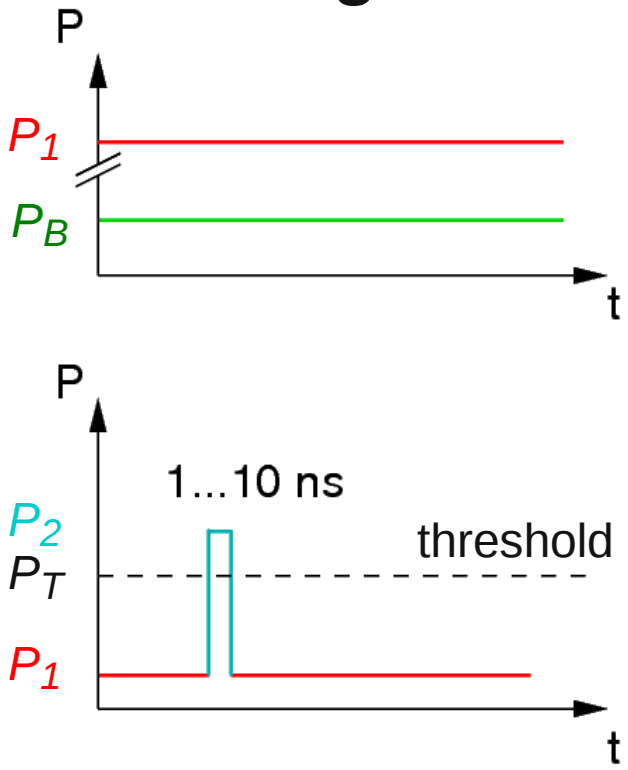
**...and forced to give a signal by bright light pulses:**




Avalanche diode operates in PIN / normal amplification regime

# *Hijacking one detector...*

**Combined to attack scheme by sending 'fake states' of classical light:**




- Detector is quiet

  blinding level $P_1 > P_B$ (few pW)

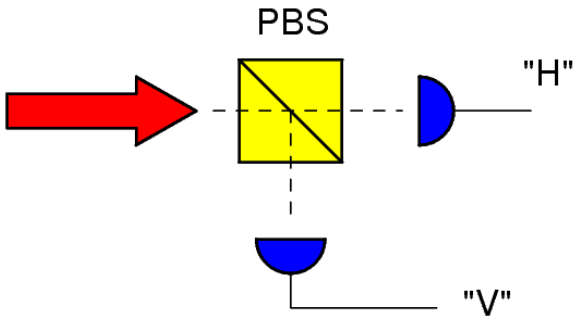
- Detector can be forced to a click at well-defined time

  $P_2 > P_T$ (few mW)

*Fake state attack : Vadim Makarov, NJP **11**, 065003 (2009)*

# *Hijacking the 'measurement'*

- This works with detector pairs as well:



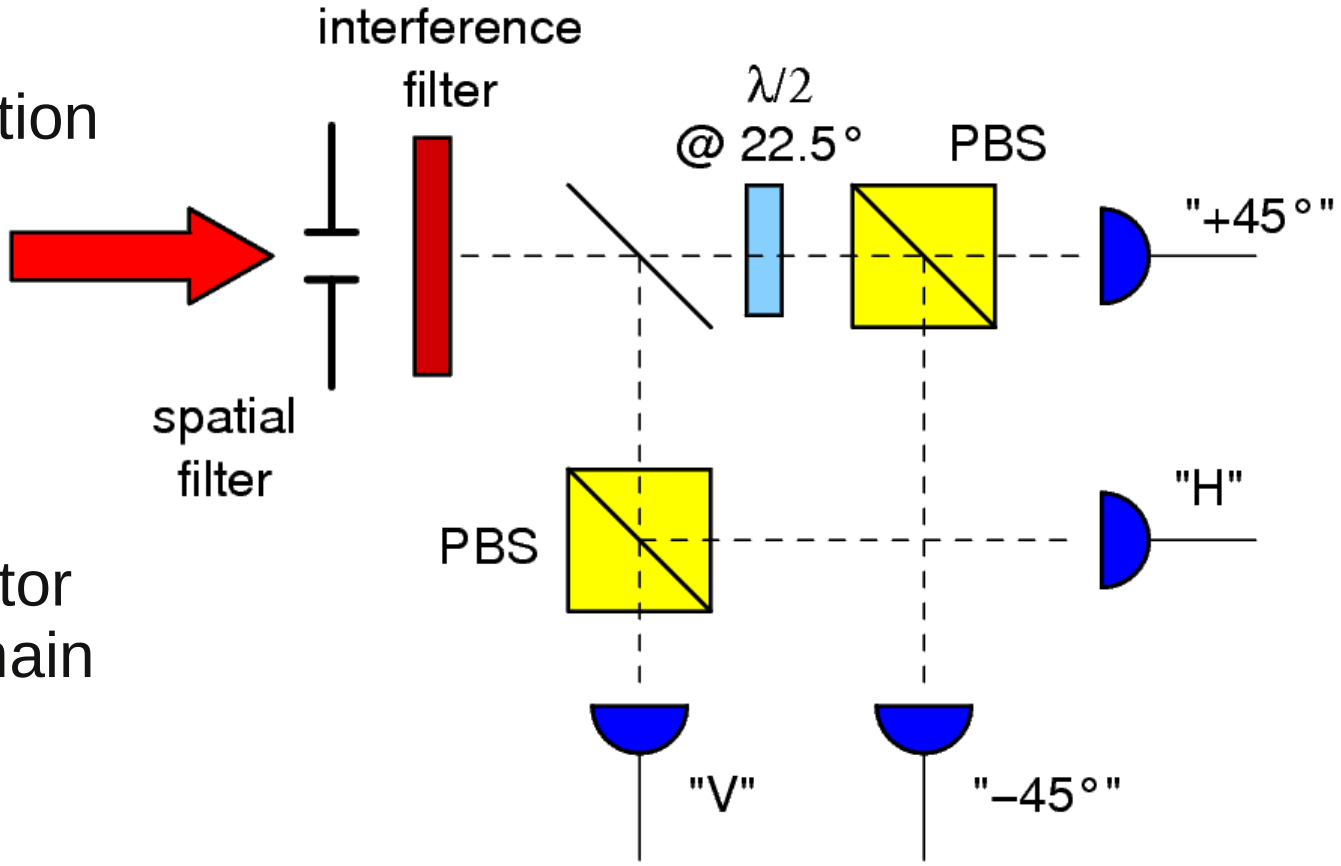

Choose unpolarized / circularly polarized $P_1$ and different linear polarizations to fake a 'click'

| **Light:** | **“H” detector:** | **“V” detector:** |
|---|---|---|
| >2 $P_B$ | no click | no click |
| + ↕ | click | no click |
| + ↔ | no click | click |

# *Why stop at two....*

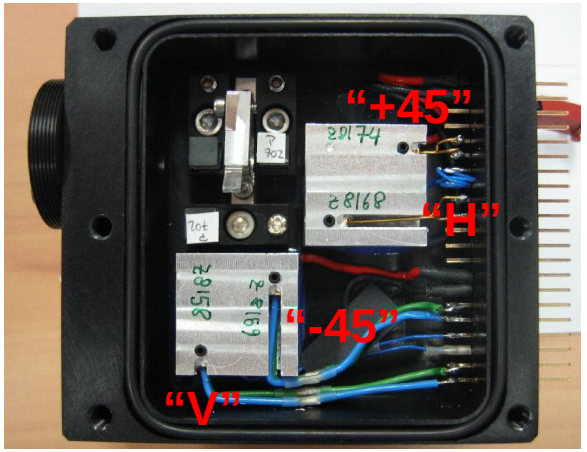
## Control of a passive base choice QKD detector:

- Choose σ+ polarization for blinding
- Choose power for each fake pulse such that one detector fires, the others remain below threshold
- Eve now has complete control over this detection scheme....



# *Four detector attack*

"faked state"

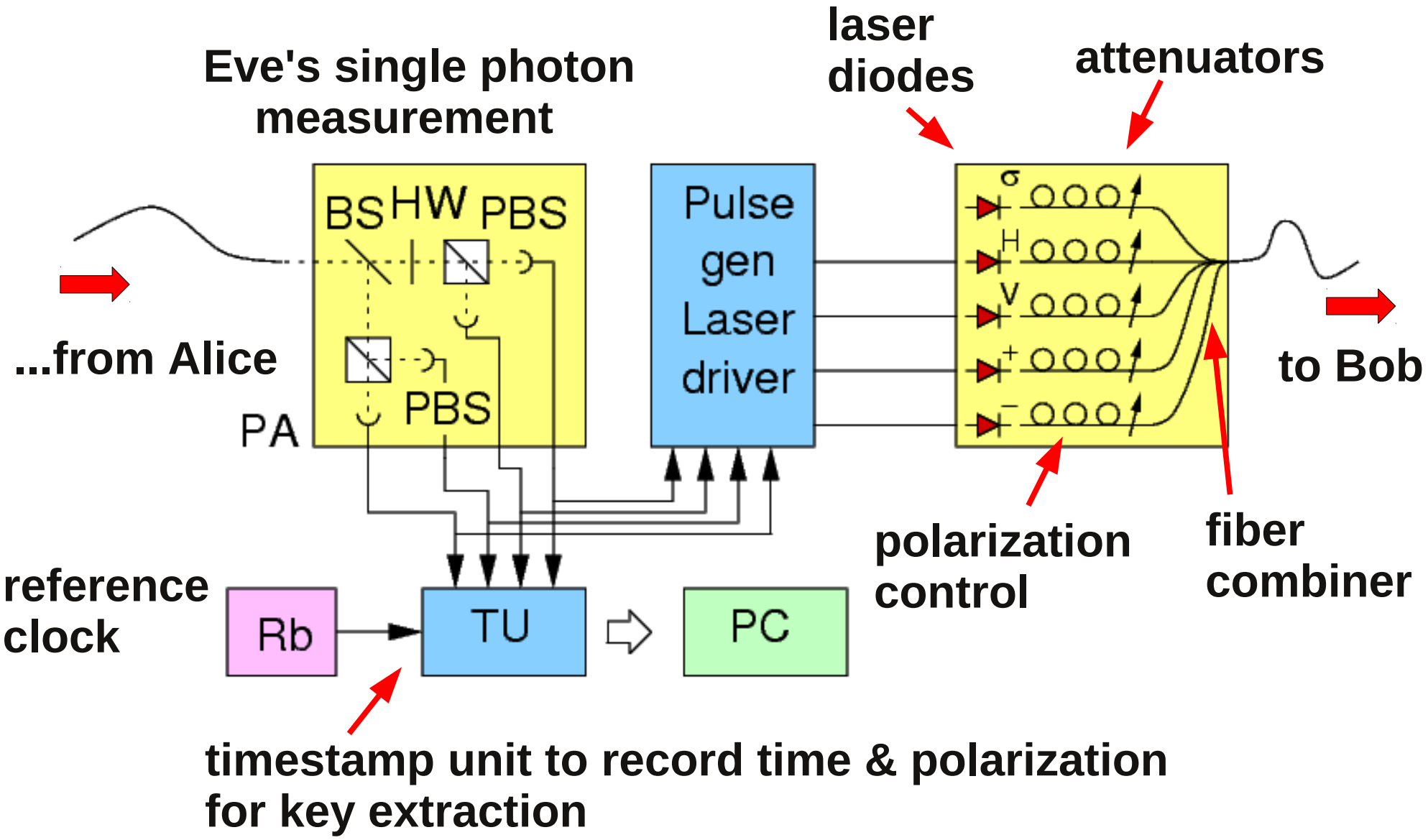



our polarization detector

| Light: | "H" | "V" | "+45" | "-45" |
|---|---|---|---|---|
| >4 $P_B$ | no click | no click | no click | no click |
| + ↕ | click | no click | no click | no click |
| + ⤢ | no click | no click | click | no click |

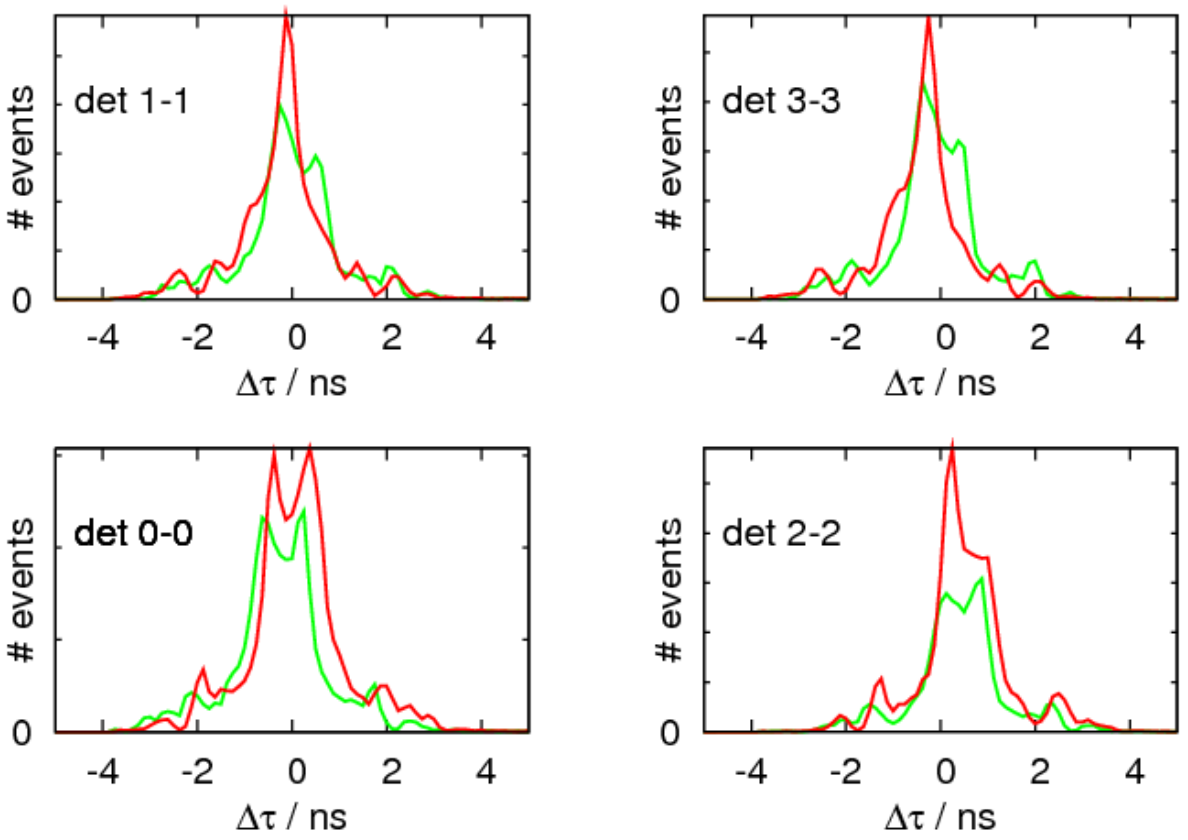
- Choose pulse amplitudes above +45 threshold, but below H/V threshold -- ideally 1- √2/2 margin for $P_2$

# *Eve's intercept-resend kit*



# *Eve's insertion timing*

## Coincidence timing histograms of a working system



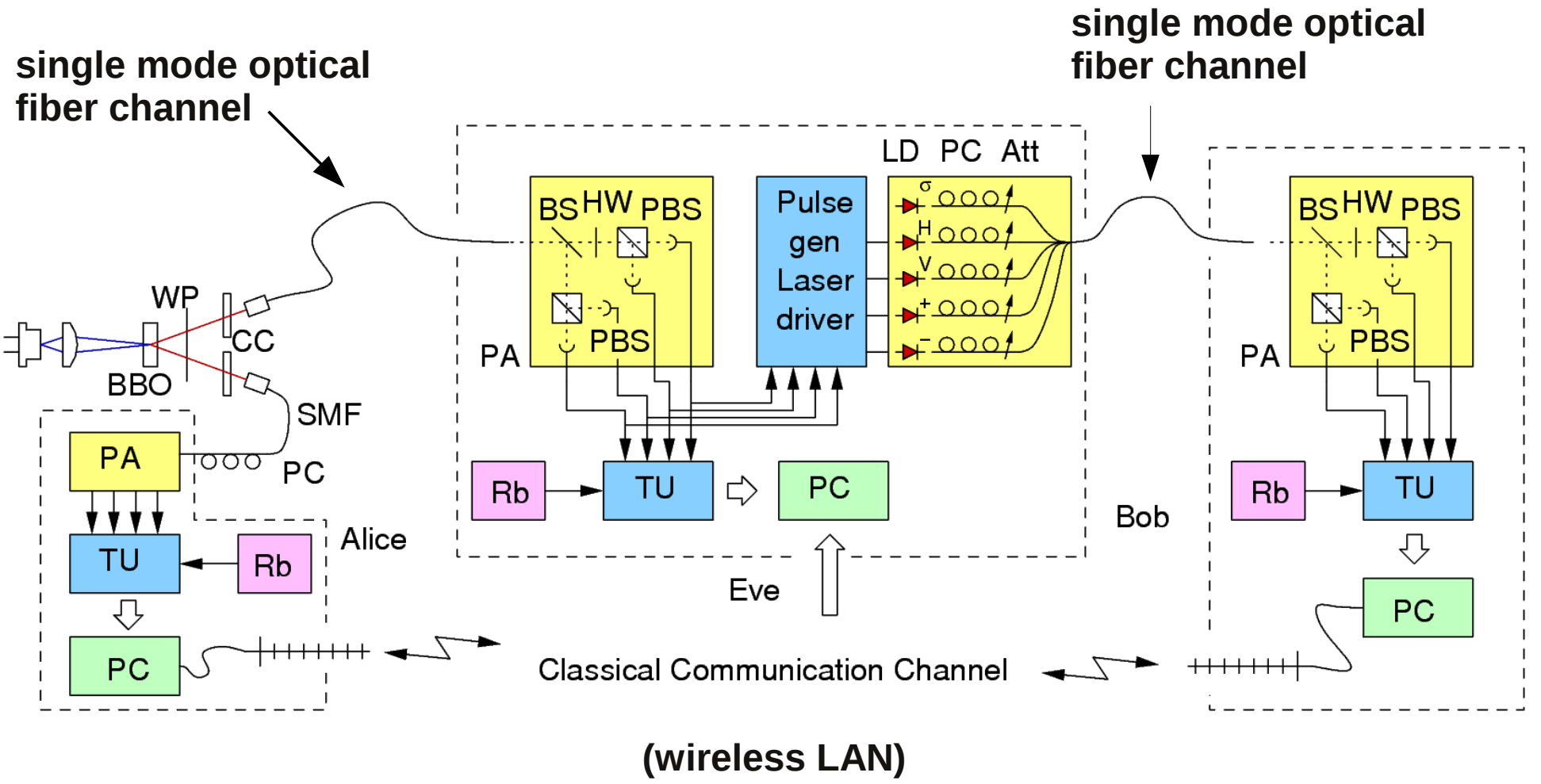

**without Eve intercept**

**with Eve intercept**

No resolvable influence on detector signal timing (<100 ps jitter)

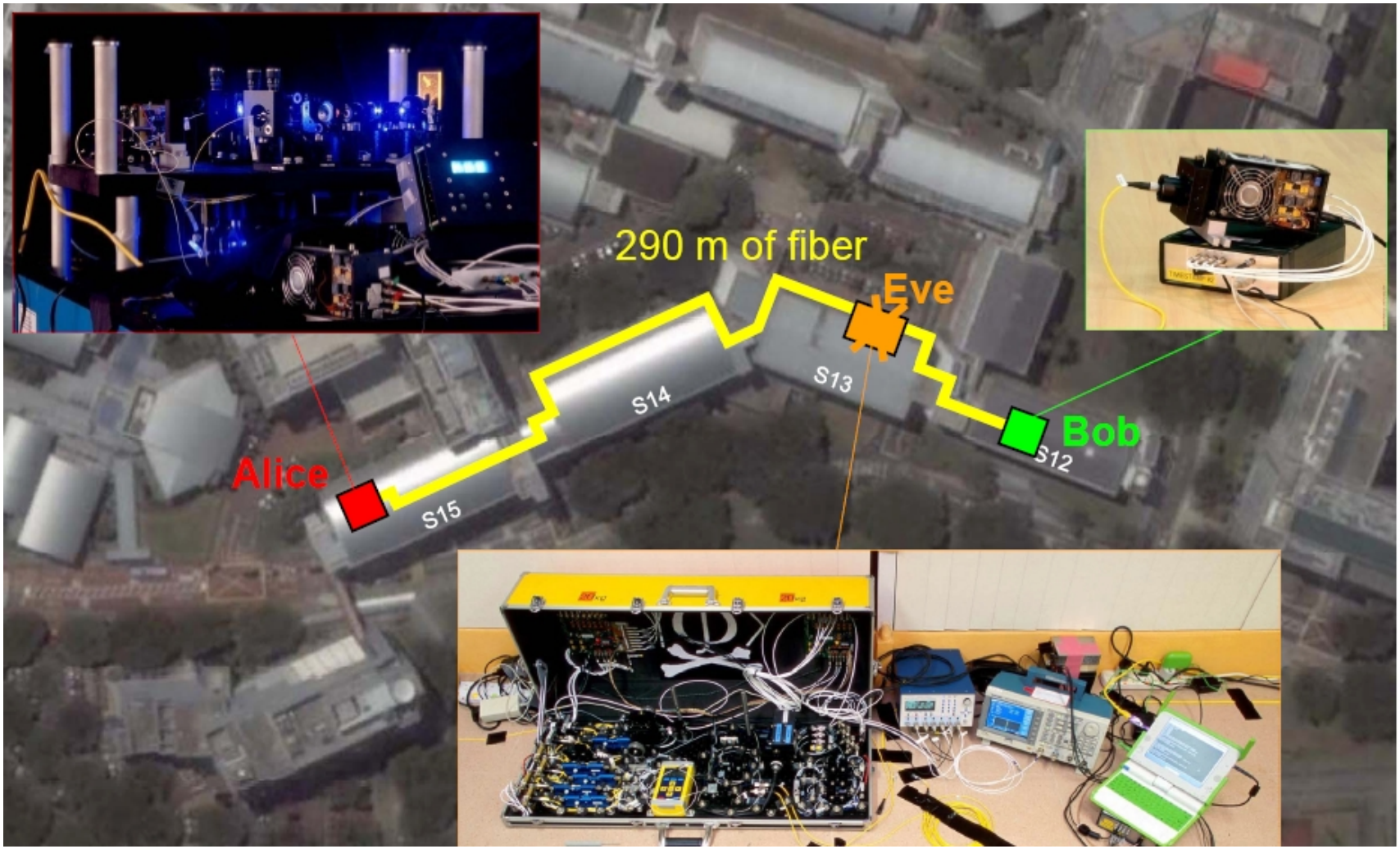
Insertion delay ~10 nsec

# *Full intercept/resent scheme*

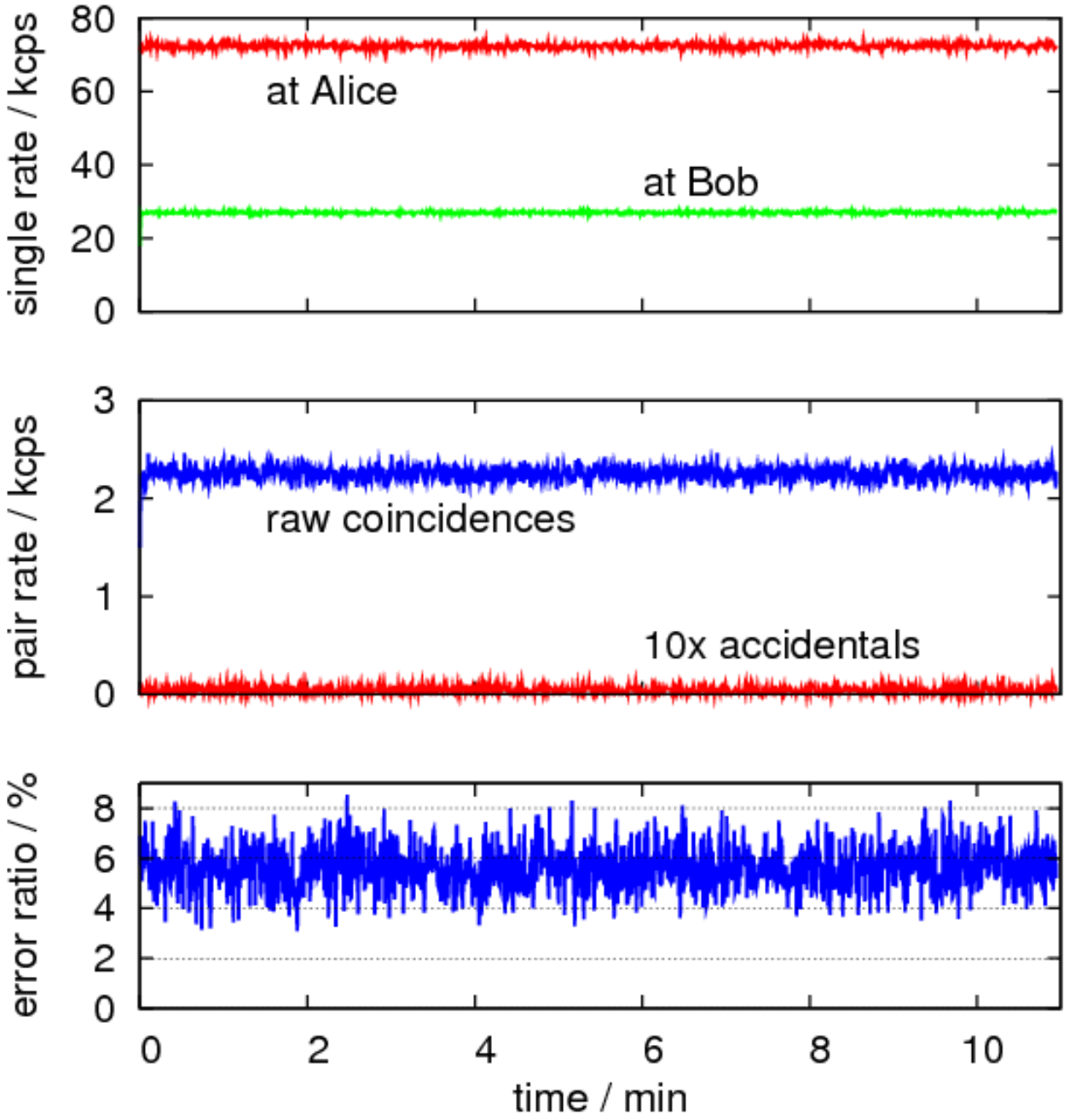


# *Layout of the plot*

“Realistic” fiber link across the Science faculty @ NUS



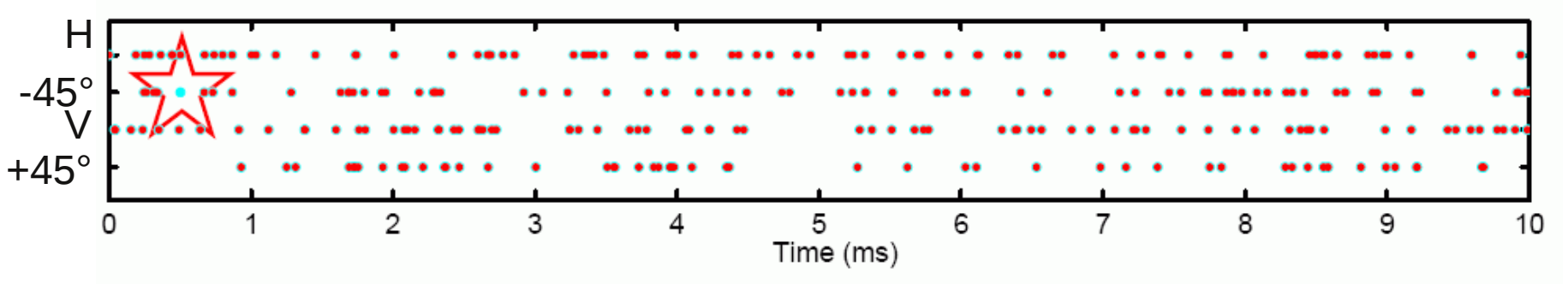
# *Results for Alice & Bob*




- reasonable photo detection rates on both sides (includes transmission loss)
- reasonable pair rate and raw key rate around 1.1 kcps
- no spurious pulses
- reasonable error ratio for this source allows to extract 500 bits/sec key after PA / EC

# *Attack Results I*

**A real-time display of events between Eve and Bob:**




- About 97%-99% of Eve clicks are transferred to Bob
- Eve can identify successful detections by Bob from timing information (classical channel intercept)
- Eve knows correctly identified pairs due to losses (classical channel intercept)
- Eve knows all detector outcomes of Bob

# *Attack Results II*

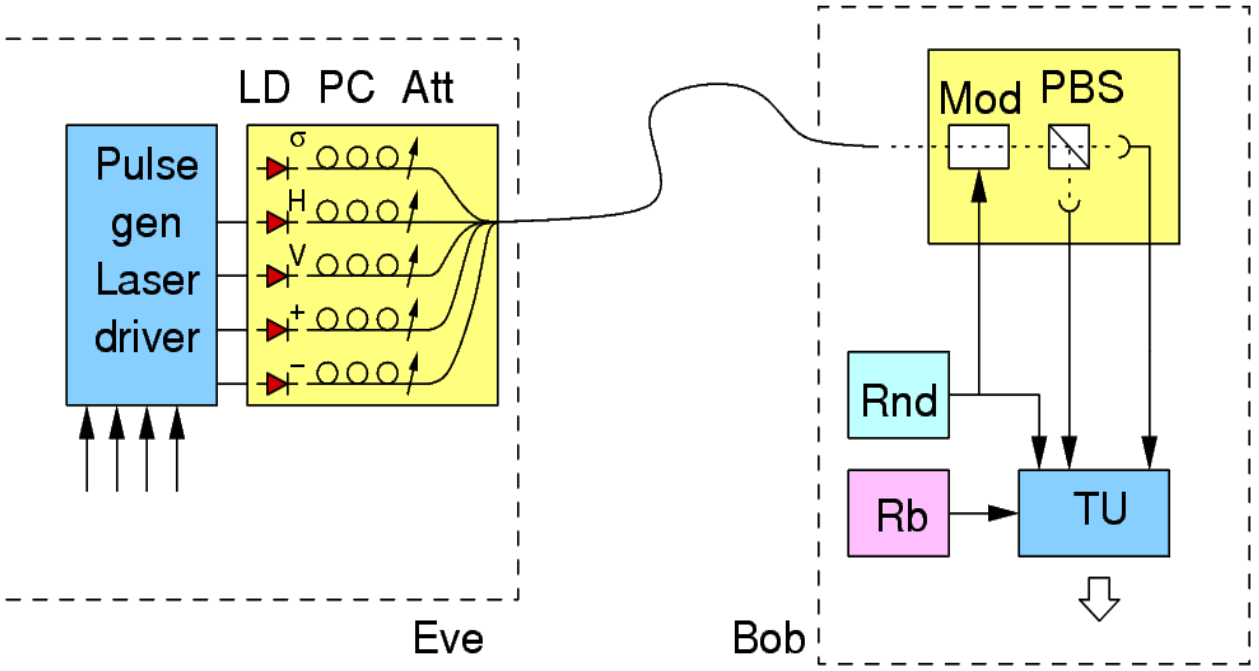
- Correlation between Eve and Bob's result (the hijacked receiver) is 100%

| | | | |
|---|---|---|---|
| 630,106 | 0 | 0 | 0 |
| 0 | 841,072 | 0 | 0 |
| 0 | 0 | 1,116,070 | 0 |
| 0 | 0 | 0 | 1,026,603 |

- Eve has Bob's complete raw key
- By eavesdropping the classical communication in error correction/privacy amplification, Eve can reconstruct the secret key

*I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, V. Makarov, arxiv:1011.0105*

# *Does active base choice help?*

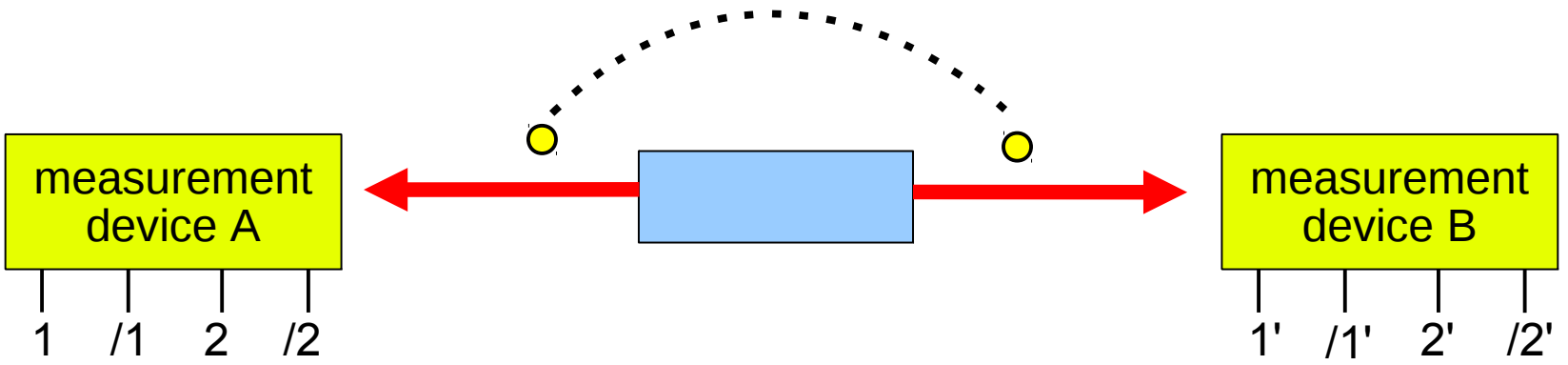



- Correlation between Eve's command and Bob results is 100%
- Bob's probability of getting Eve's base choice correct is 50%

  Presence of Eve looks like 50% loss (no big help)

# *Do other protocols help?*

## Device-independent / Ekert-91 protocol idea




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:

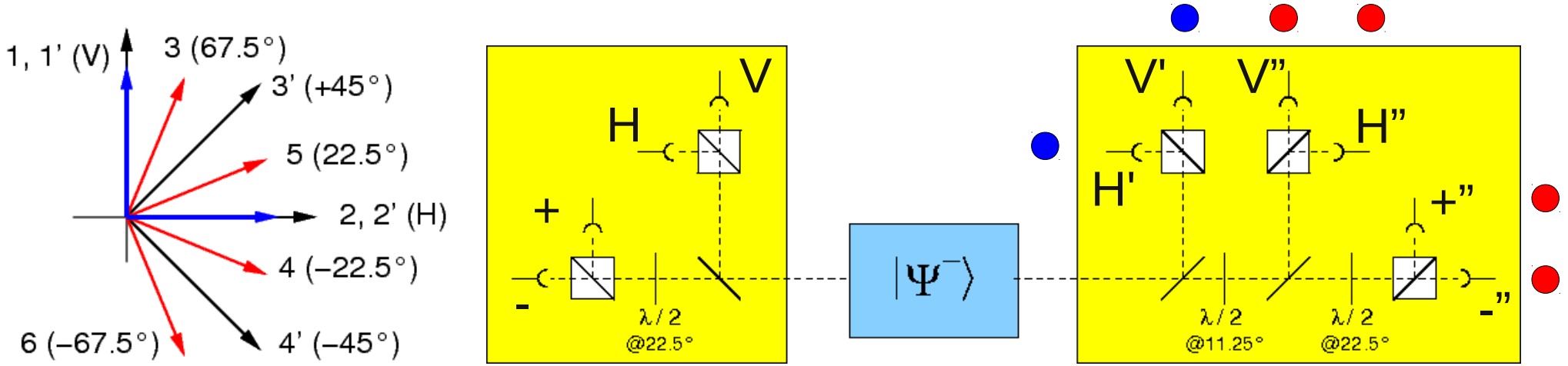
$$I_E(S) = h\left(1 + \frac{\sqrt{S^2/4 - 1}}{2}\right)$$

- 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)*

# *Implementation (partial?)*

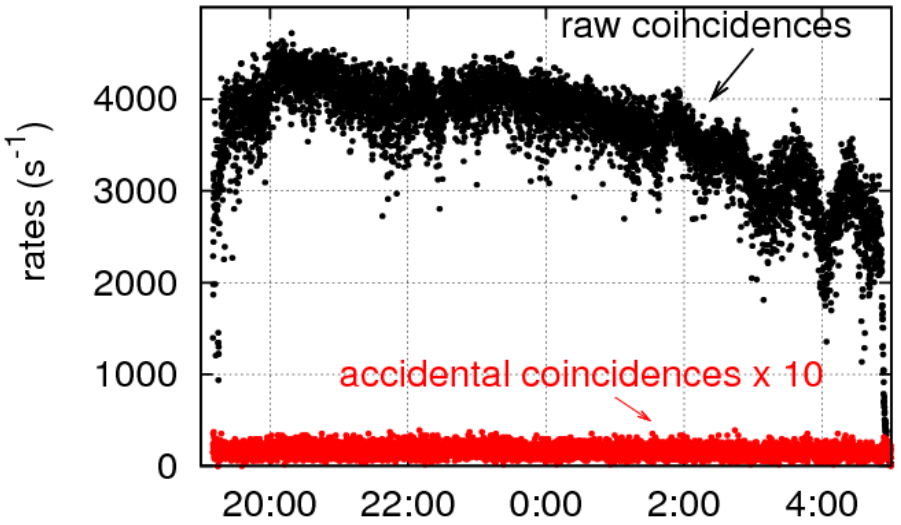
- use almost same kit:

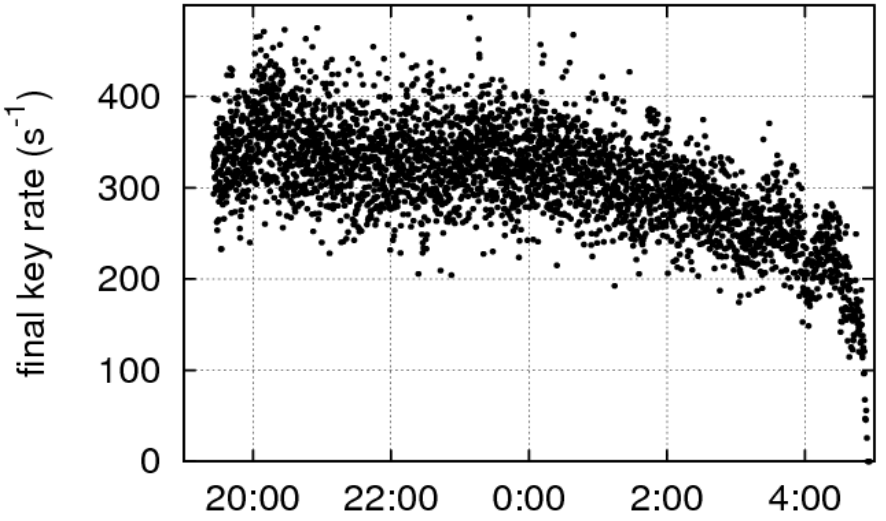


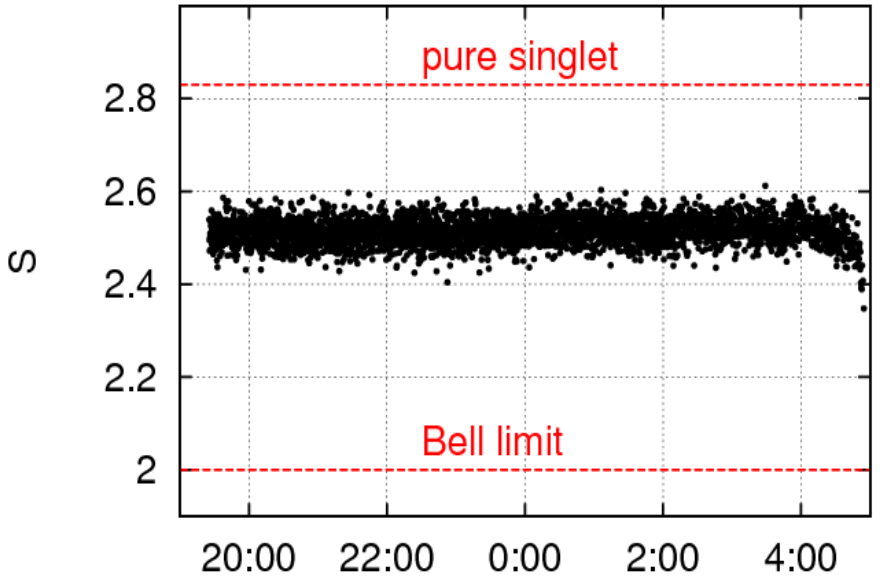

- {H,V; H',V'} coincidences → key generation
- {H,V,+,-;H",V",+",-"} coincidences → CHSH Bell test
- low QBER with existing simple source

# Practical E91 Key Generation

## Key generation results:



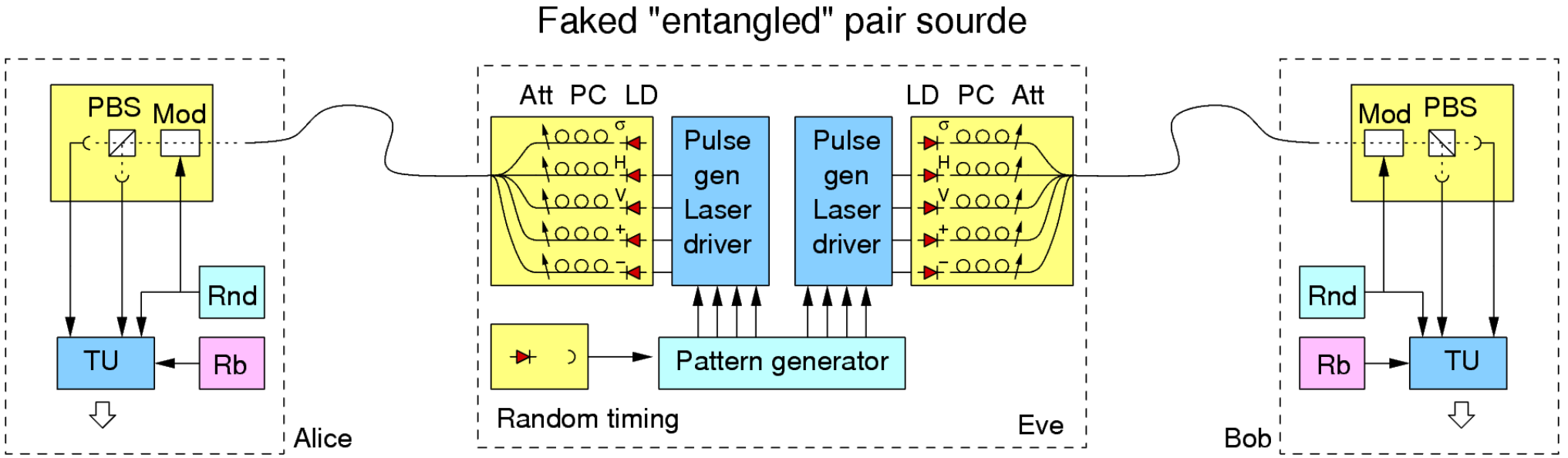




- continuous operation at night
  final key after EC/PA: $10^7$ bits

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

# *Faking Violation of a Bell ineq*

## (core part of device-independent QKD protocol)




- Alice & Bob will see “programmed” correlations in 25% of the cases (base match on both sides), rest nothing
- Alice and Bob cannot distinguish from lossy line....
- We programmed (and found)  CHSH results from S = -4 .... 4 with active choice

# *What is going on??*

## How can device-independent break down?

- Losses in CHSH are removed by post-selecting pair observations using a fair sampling assumption
- Current pair sources (η = 70%) and detectors (η = 50% for non-cryogenic ones)
- Eve hides behind losses of transmission line. Best guess: optical fiber and ideal (η = 100%) detectors, active base choice: At 0.2dB/km@1550nm, $T$ = 25% for *dist* = 30 km
- Only very short distances possible with current detectors

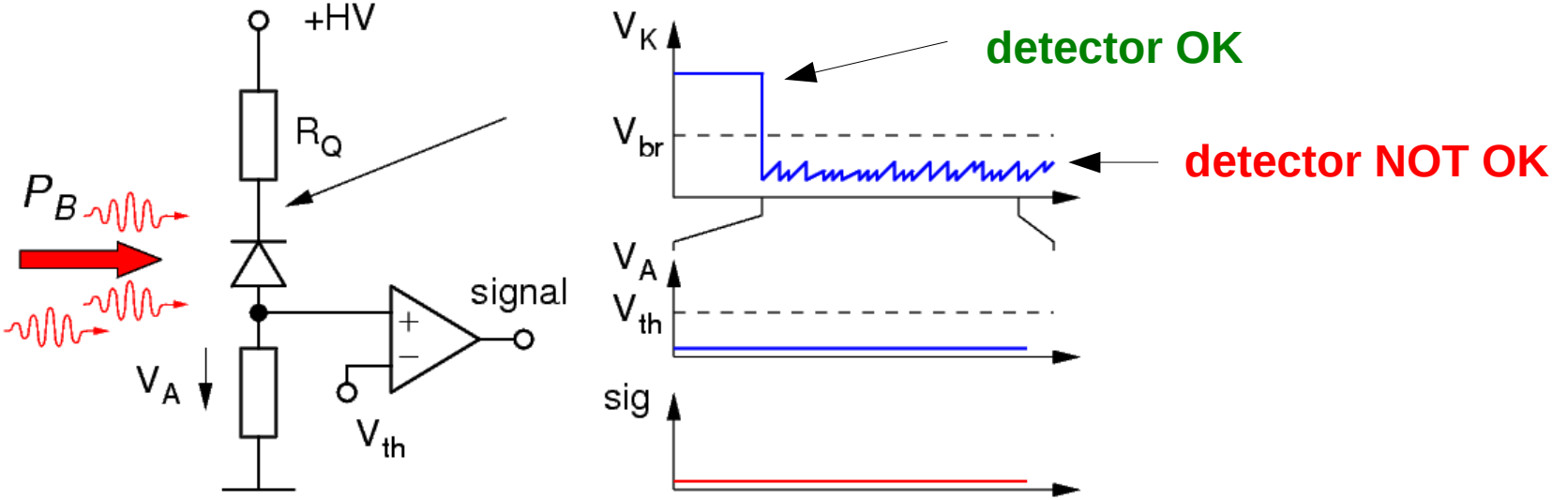
# *Can this be fixed ?*

**Yes, of course.**

- Monitor total intensity with a separate, non-saturable photodetector (PIN diode)

  Blinding power and bright pulses are much brighter than usual photon signal

- Monitor the state of APD's by looking at their voltage, asserting 'detector readiness'



# *Is this a "good" fix....?*

## ...of a "Bad Implementation" ??

- Are there detectors / detector concepts which are not susceptible to such or similar attacks?
- Do we have other practical attacks?
- Will all practical implementations always be potentially bad implementations of a theoretically secure protocol?
- Let's leave Hilbert space and have independent challenge/assessments of security claims
- What do we offer in comparison to classical key exchange devices like tamper-safe devices? Is QKD just an elegant version of such a device?

*Valerio Scarani, C.K., arxiv:0906.4547*

# *Thank You!*

**Team members NTNU Trondheim**
Vadim Makarov
Qin Liu
Johannes Skaar

**Team members CQT Singapore**
Ilja Gerhardt
Antia Lamas-Linares
Valerio Scarani
C.K.

**Group:**
http://www.qolah.org

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