Implementation of an attack scheme on a practical QKD system

Q. Liu, I. Gerhardt
A. Lamas-Linares, V. Makarov, C. Kurtsiefer

Centre for Quantum Technologies

NUS National University of Singapore

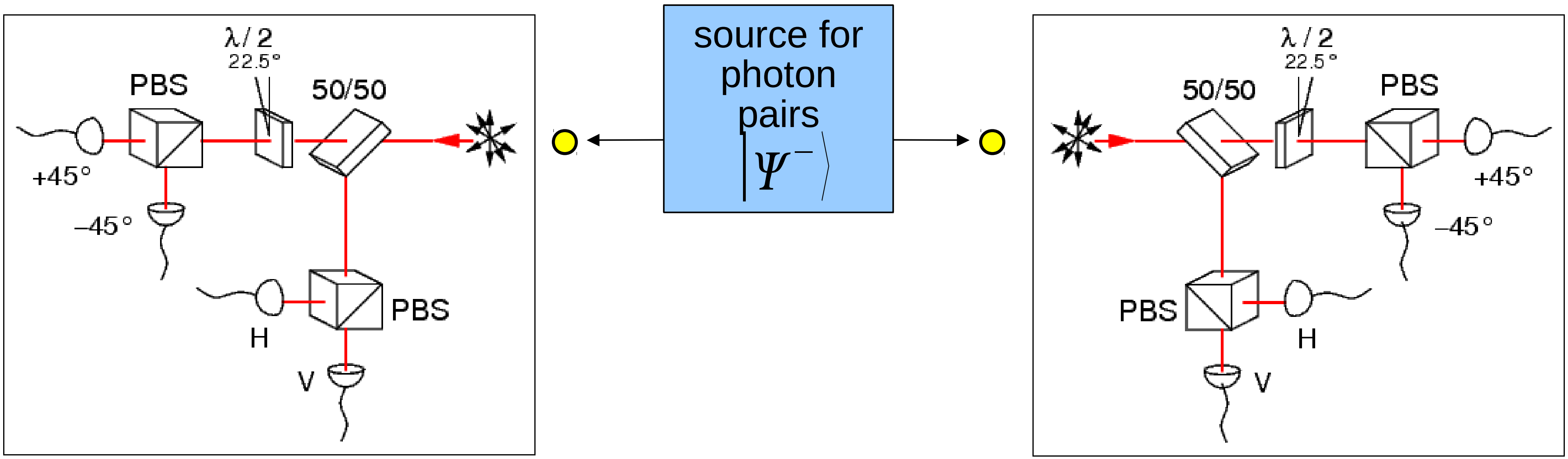
Q56.5 - DPG Tagung Hannover, 12. March 2010

Overview

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

QKD with photon pairs: BBM92

Quantum correlations & measurements on both sides



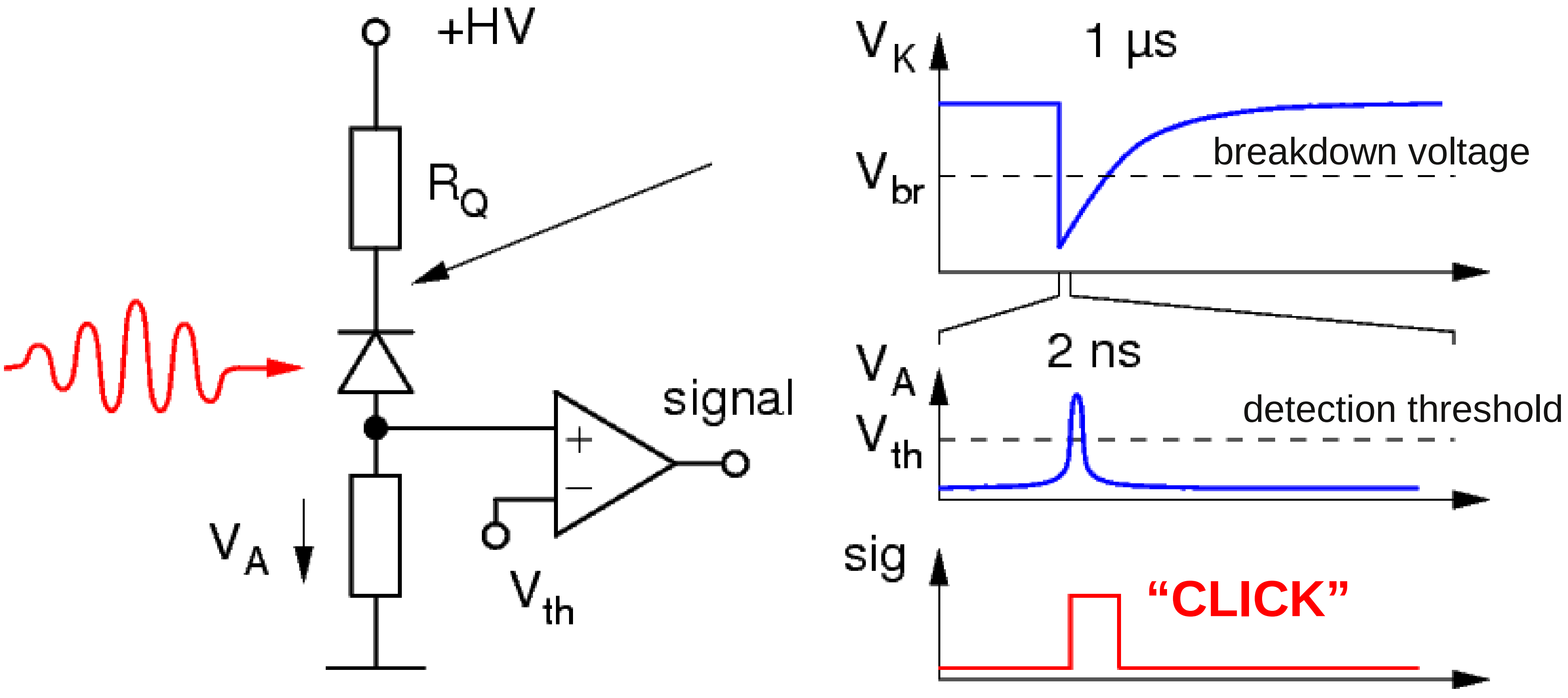
public discussion (sifting, key gen / state estimation)

error correction, privacy amplification

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

Basic photodetector operation

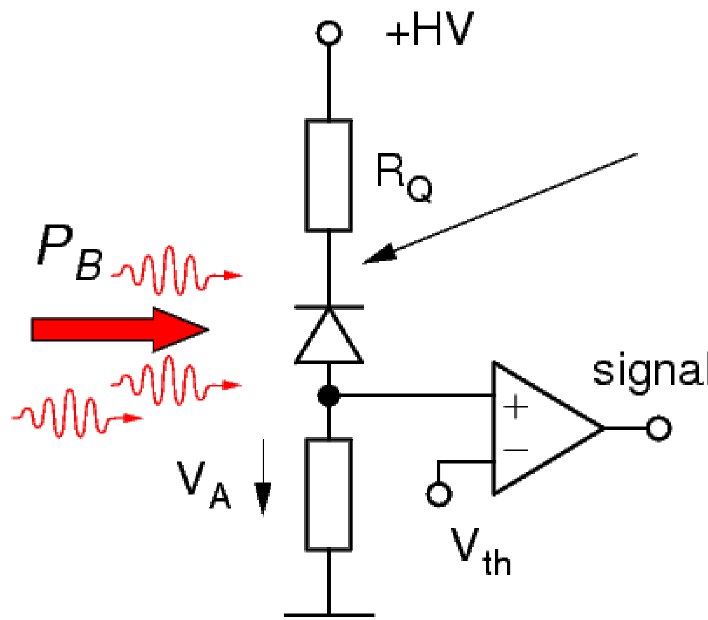
Avalanche photodiodes (APD) are common "single photon" detectors

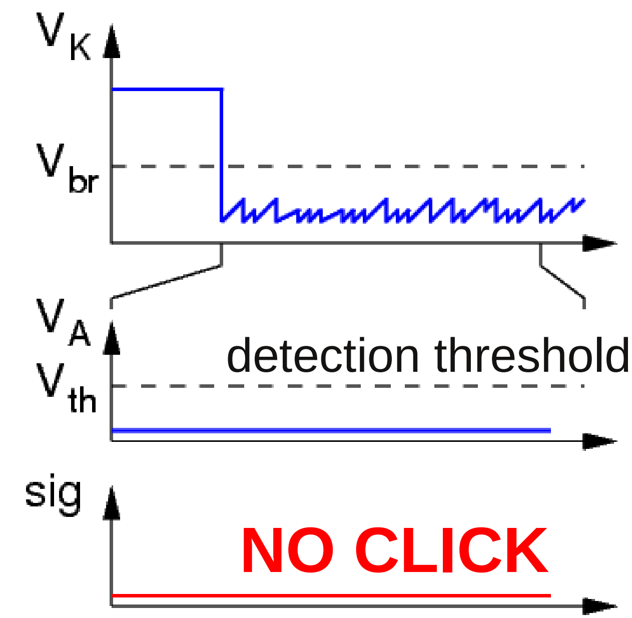


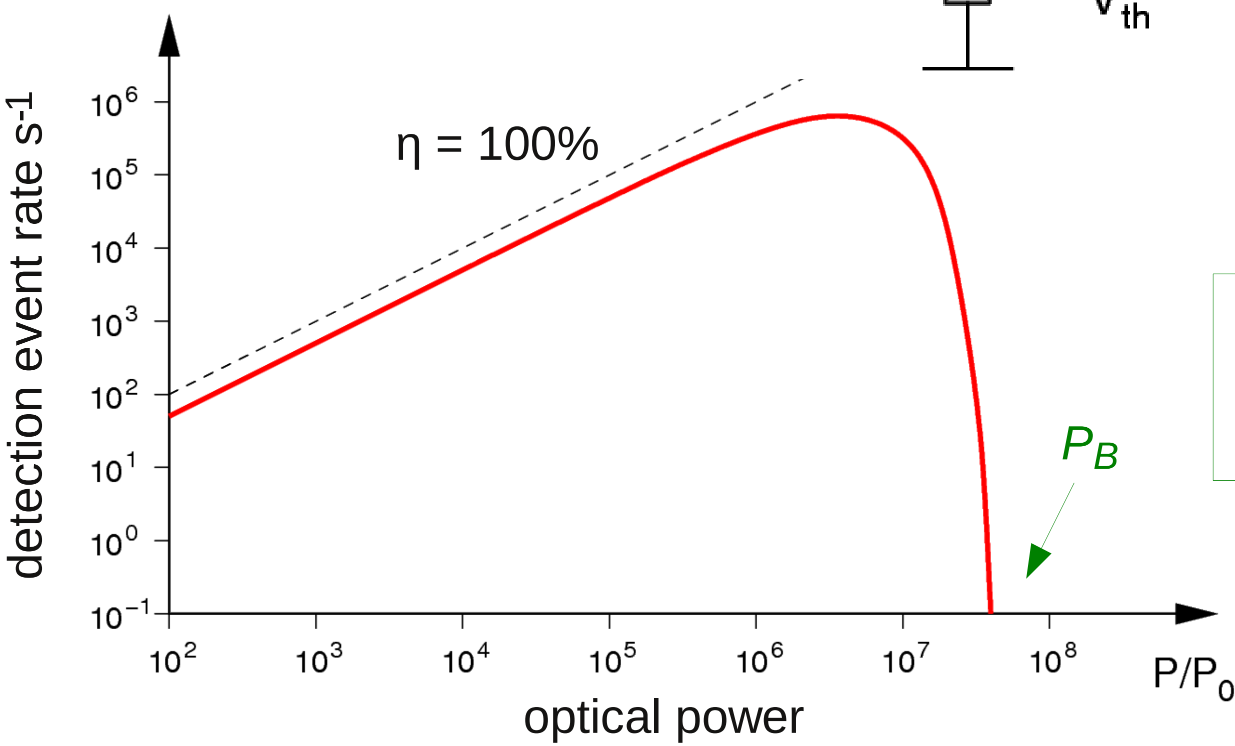
APD detector vulnerability I

Basic Problem:

APD saturate and can be blinded



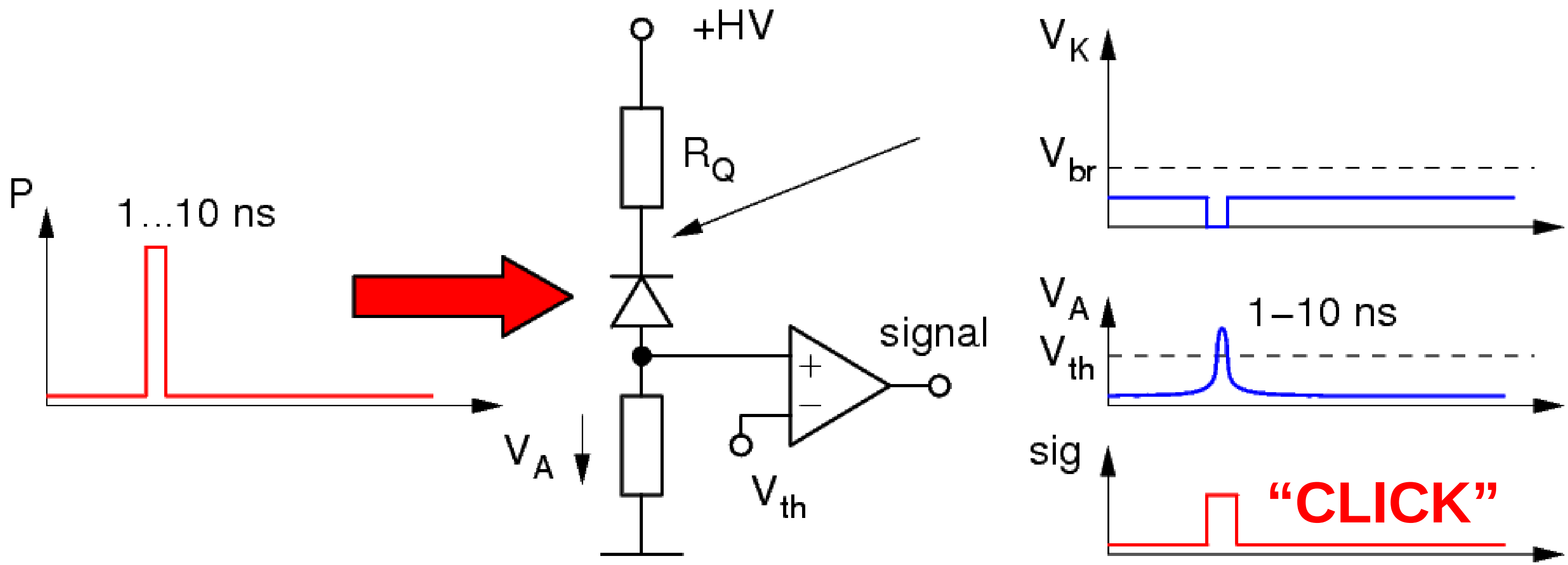




blinding power *P_B*: 1..10 pW
(corresponding to
10^6-10^7 events / sec)

APD vulnerability II

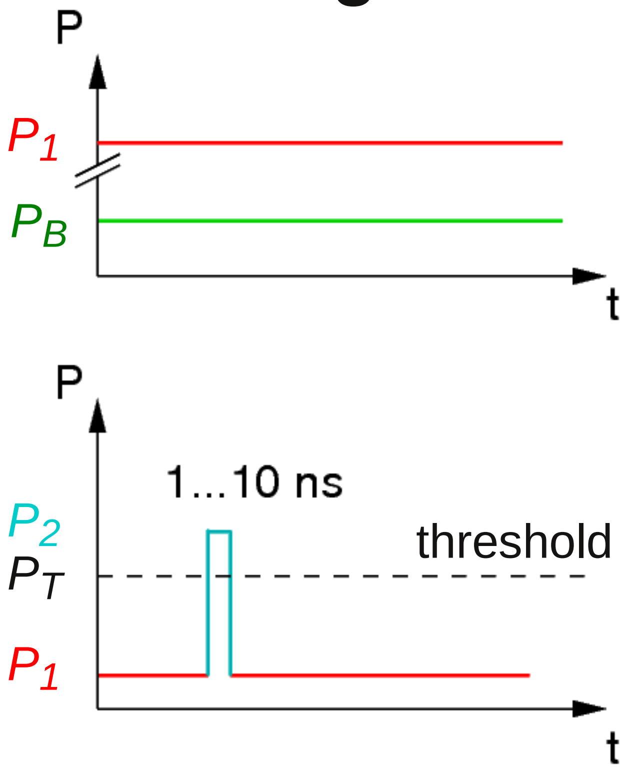
...and forced to give a signal by bright light pulses:



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)

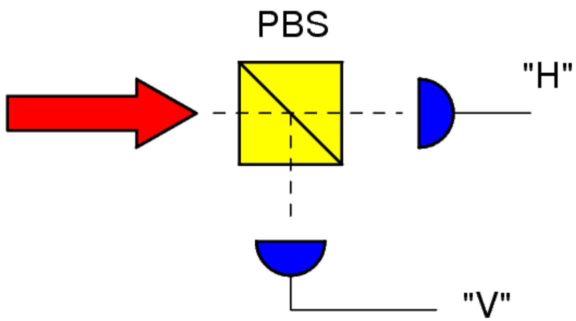
- Detector can be forced to a click at well-defined time

  $P_2 > P_T$ (few mW)

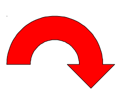
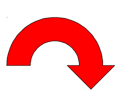
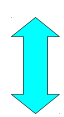
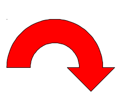
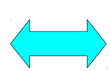
*Fake state attack : Vadim Makarov, NJP **11**, 065003 (2009)*

Hijacking the 'measurement'

- This works with detector pairs as well:



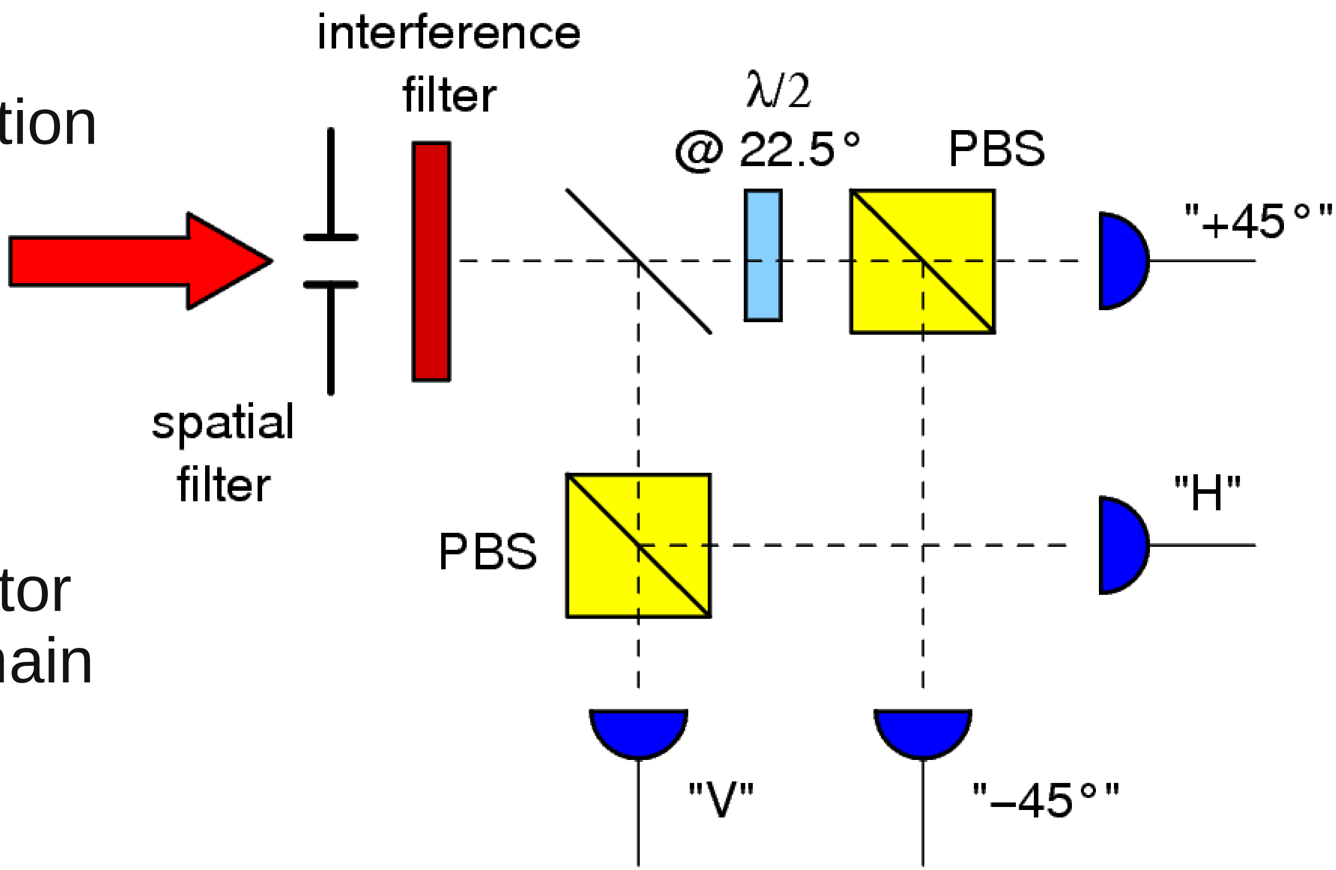
Choose unpolarized / circularly polarized P_1 and different linear polarizations to fake a 'click'

Light:	**“H” detector:**	**“V” detector:**
 >2 P_B	no click	no click
 + 	click	no click
 + 	no click	click

Why stop at two....

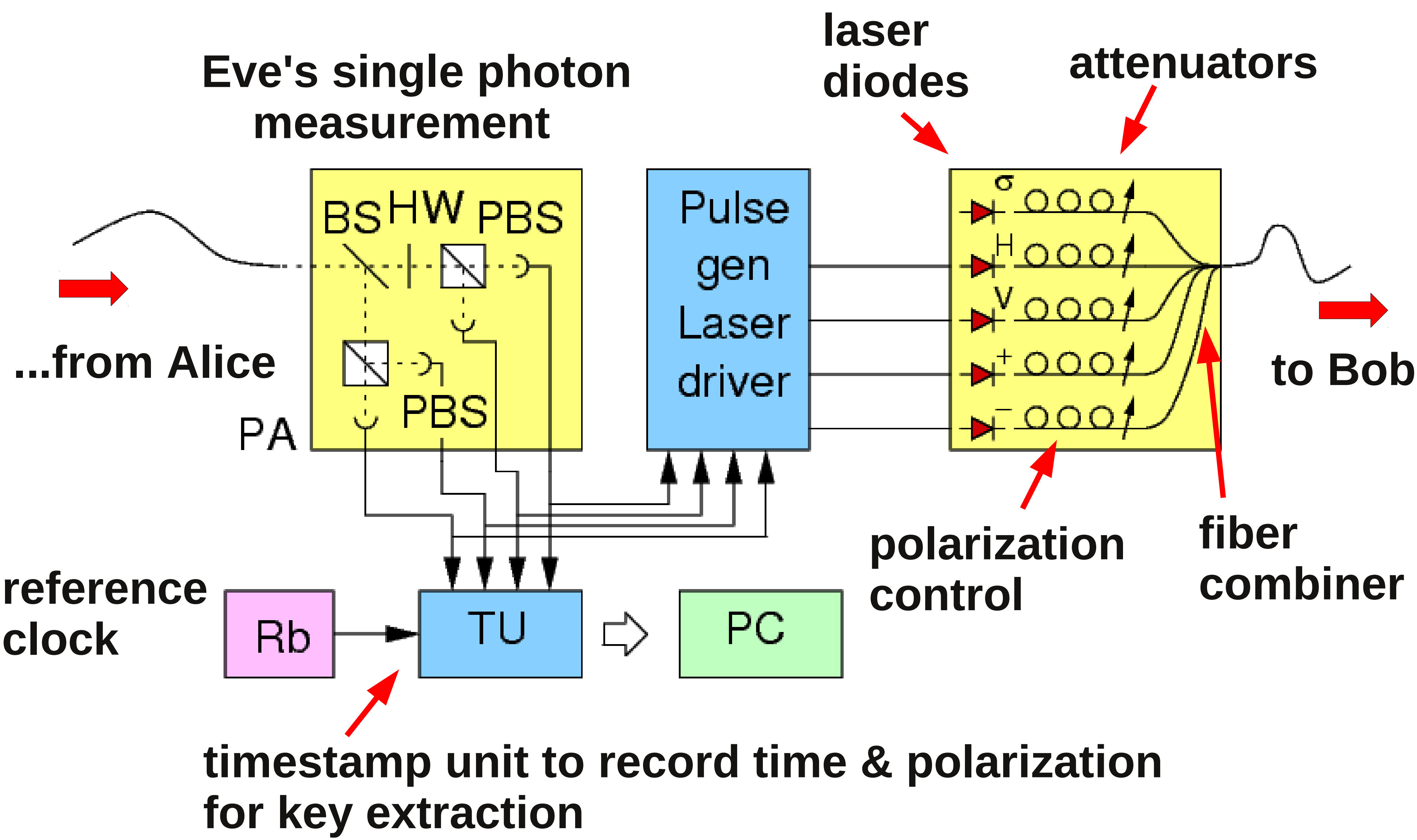
Control of a passive base choice QKD detector:

- Choose σ+ polarization for blinding



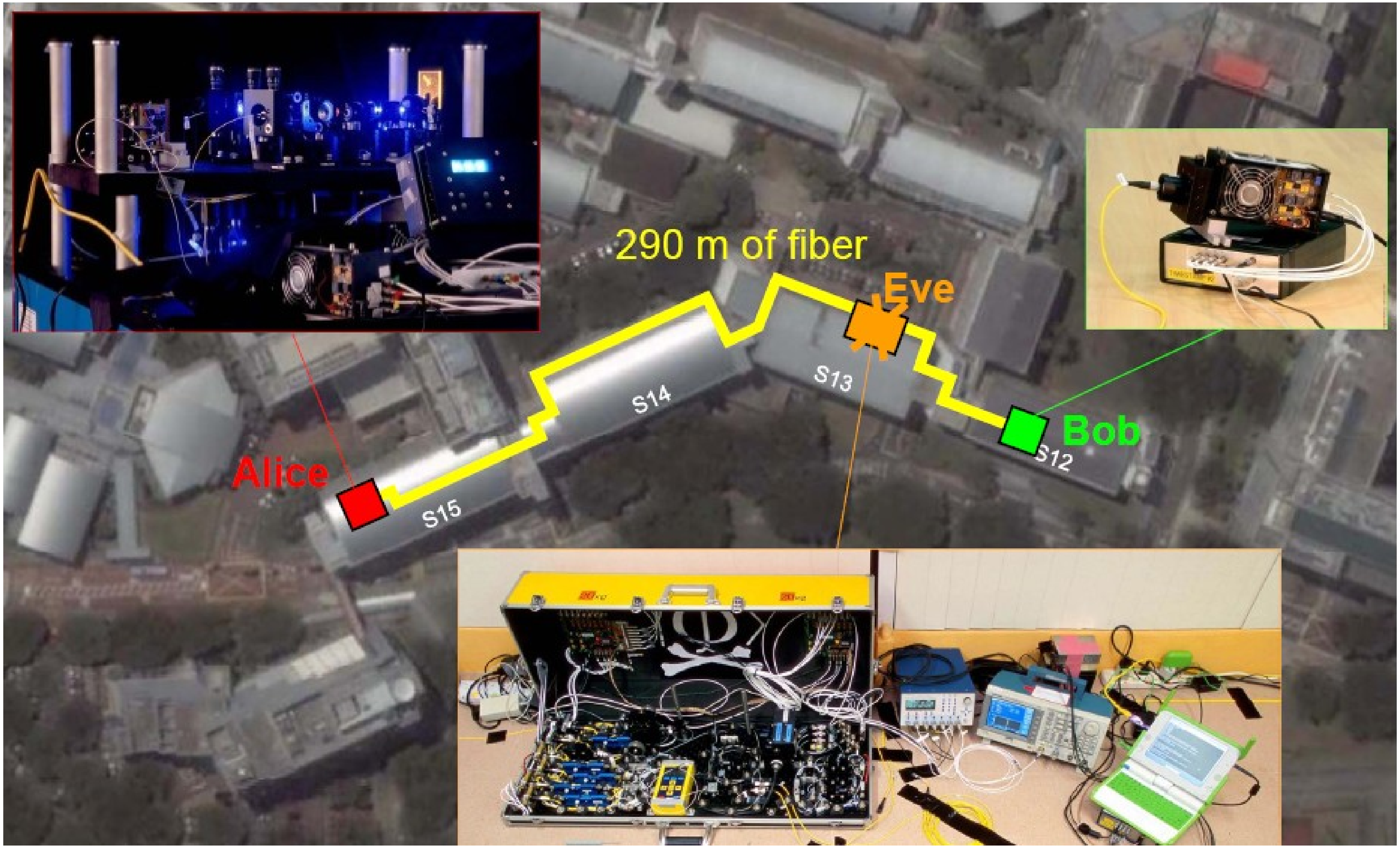
- Choose power for each fake pulse such that one detector fires, the others remain below threshold
- Eve now has complete control over this detection scheme....

Eve's intercept-resend kit

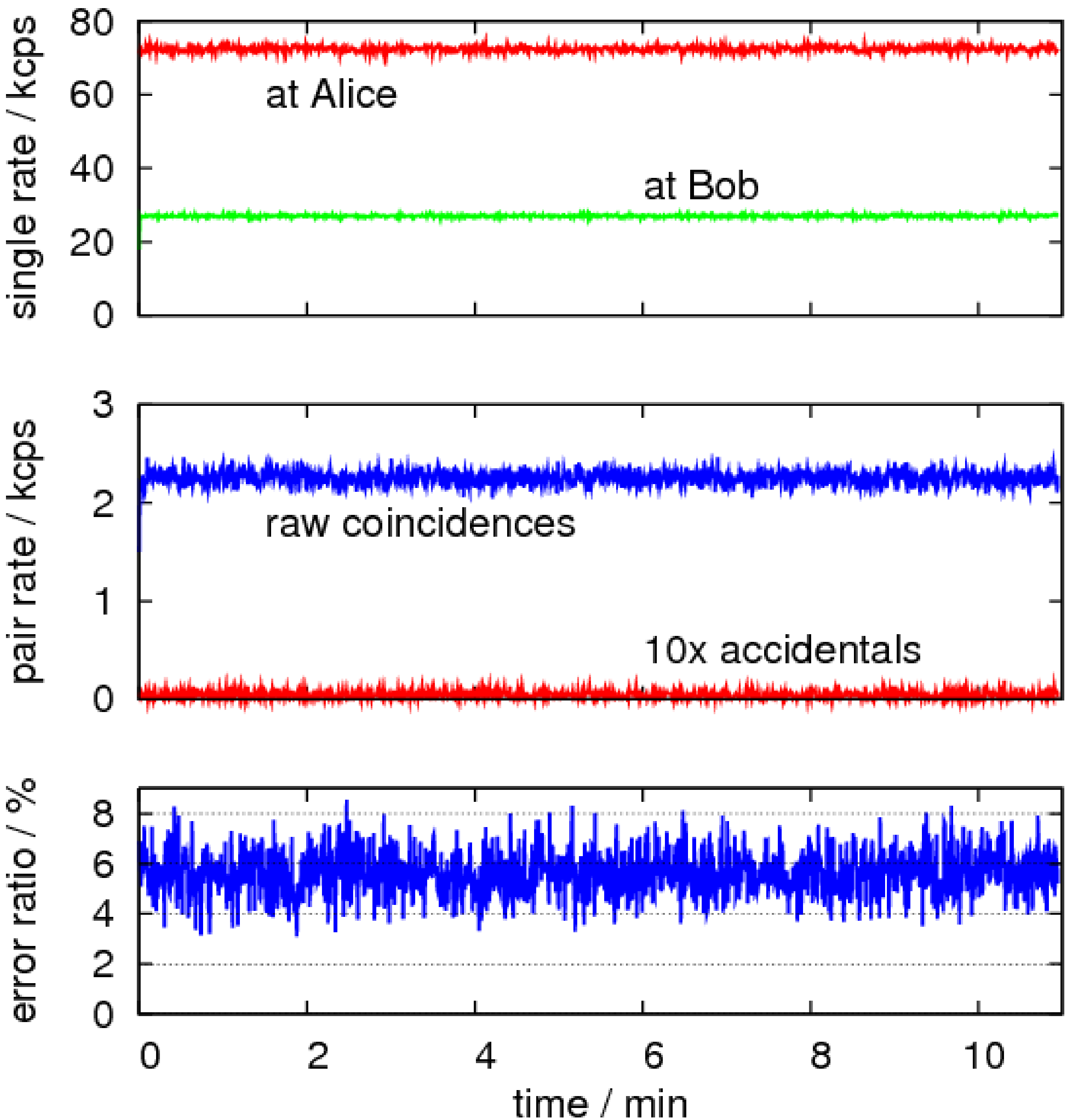


Layout of the plot

"Realistic" fiber link across the Science faculty @ NUS



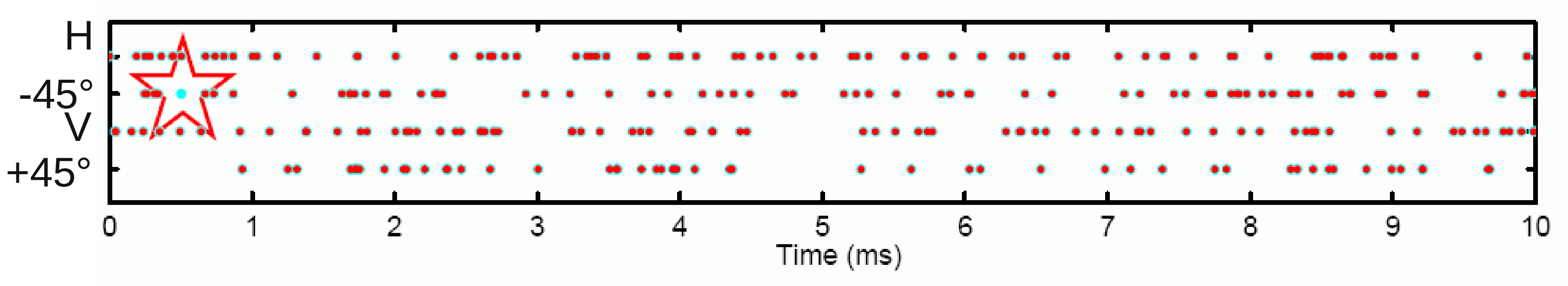
Results for Alice & Bob



- 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

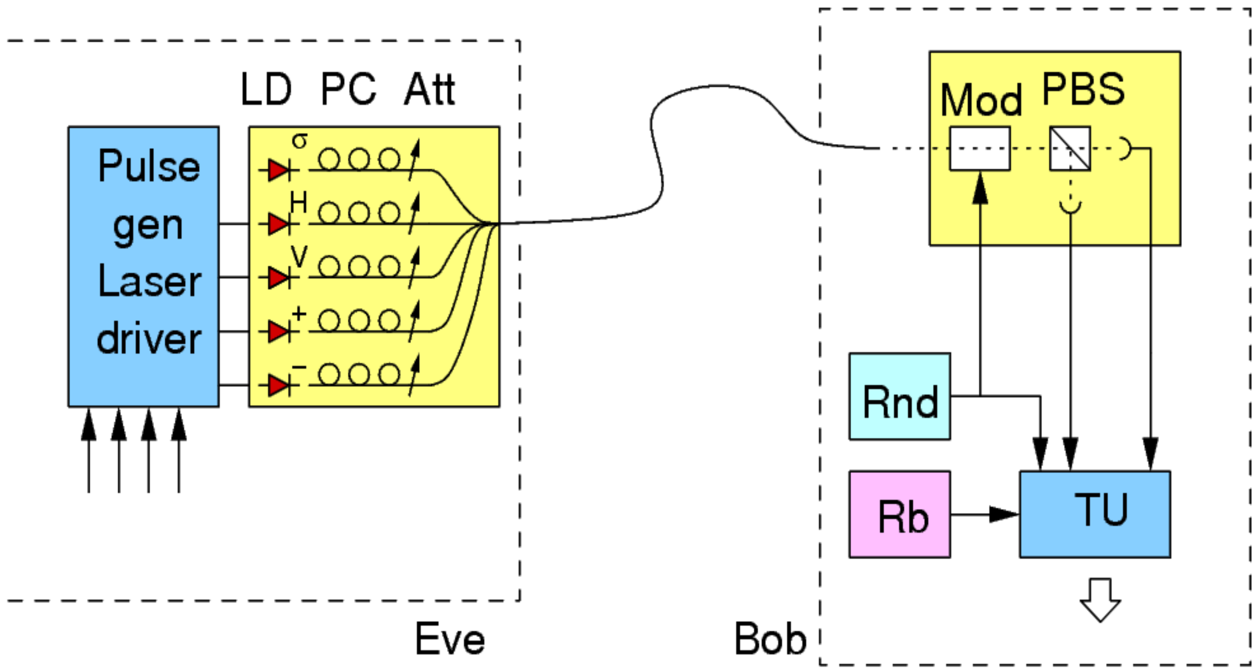
Attack Results II

- 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

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)

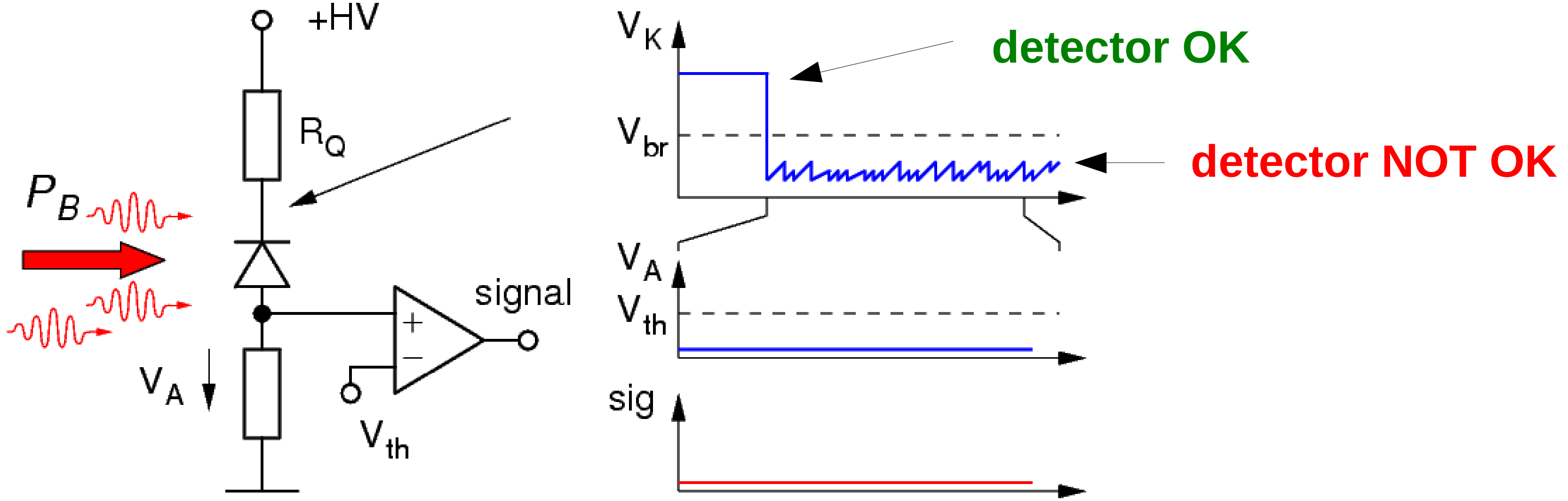
Can this be fixed ?

Yes, of course.

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

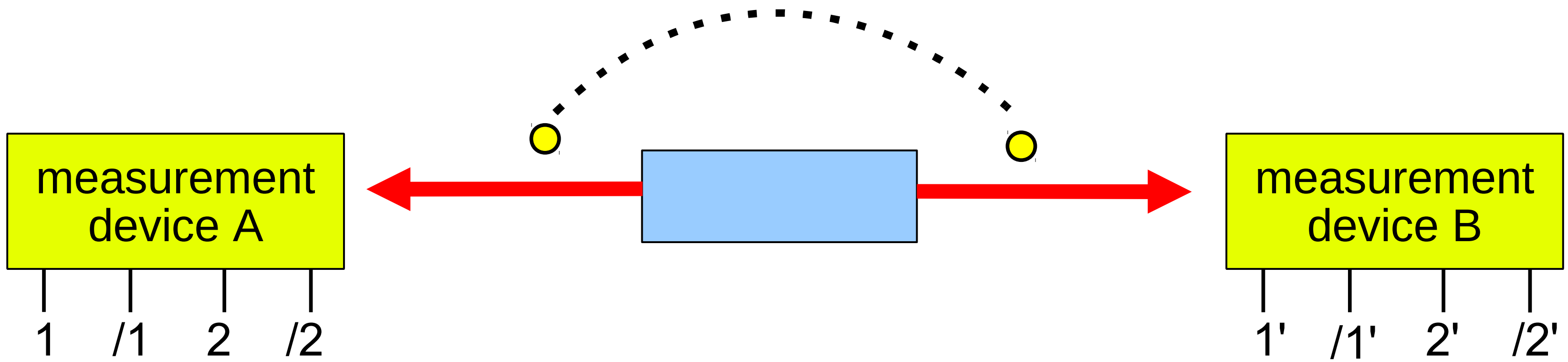
  Blinding power and bright pulses are much brighter than usual photon signal

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



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:

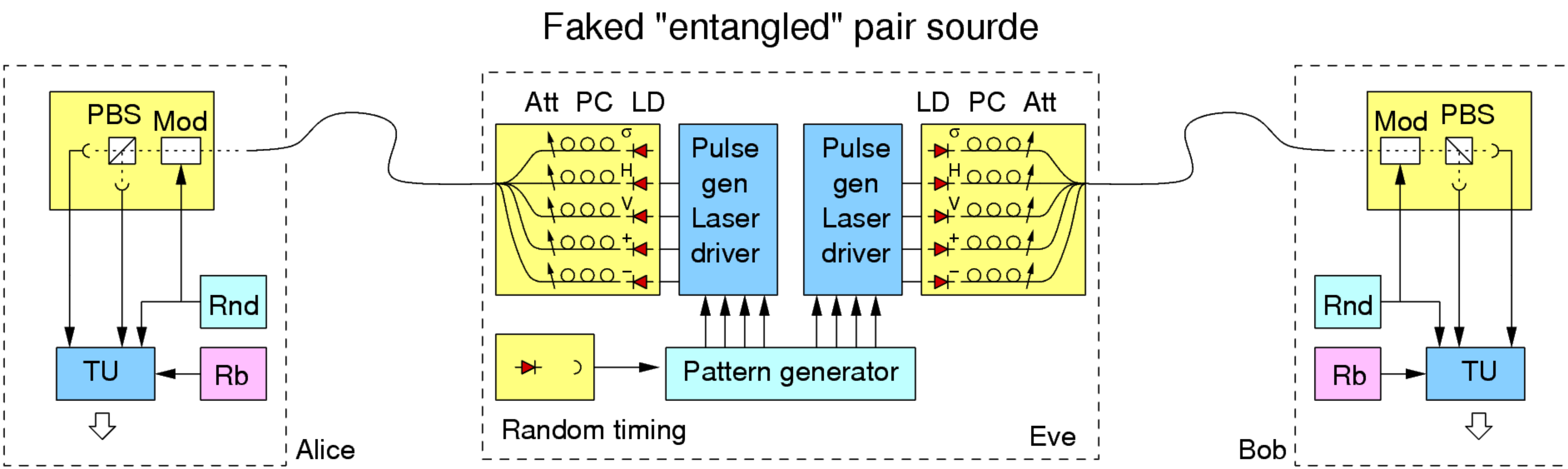
$$I_E(S)=h\left(1+\frac{\sqrt{S^2/4-1}}{2}\right)$$

- 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)

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.
  At 0.2dB/km@1550nm, T = 25% for *dist* = 30 km

- Only very short distances possible with current detectors

Thank You!

Team members NTNU Trondheim
Vadim Makarov
Qin Liu

Team members CQT Singapore
Ilja Gerhardt
Matt Peloso
Caleb Ho
Antia Lamas-Linares
C.K.

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

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

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