Lecture at *Hacking at Random*, August 14, 2009

How we eavesdropped 100% of a quantum cryptographic key

Vadim Makarov, Qin Liu,

Ilja Gerhardt, Antía Lamas-Linares, Christian Kurtsiefer

NTNU
Norwegian University of Science and Technology

CQT
Centre for Quantum Technologies, Singapore

Outline

- Introduction to quantum cryptography
- The quantum cryptosystem at CQT
- Problems with photon detectors
- Attack on the real system
- What was a photon? – Perspectives

Quantum cryptography timeline

ca. **1970** Concept (“money physically impossible to counterfeit”)

1984 First key distribution protocol (BB84)

1989 Proof-of-the-principle experiment

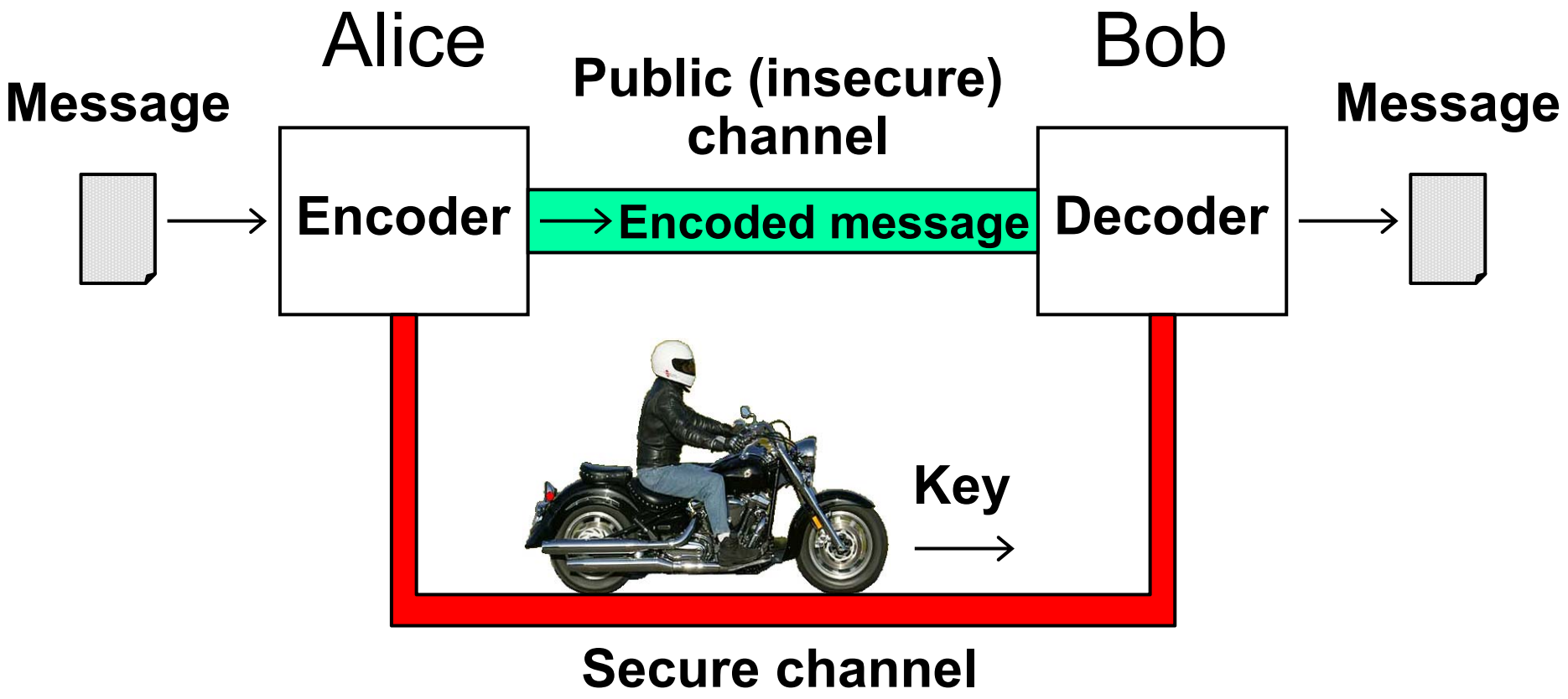
1993 Key transmission over fiber optic link

2004 First commercial offers (20~50 km fiber links)

2007 200 km in fiber, 144 km free-space demonstrated

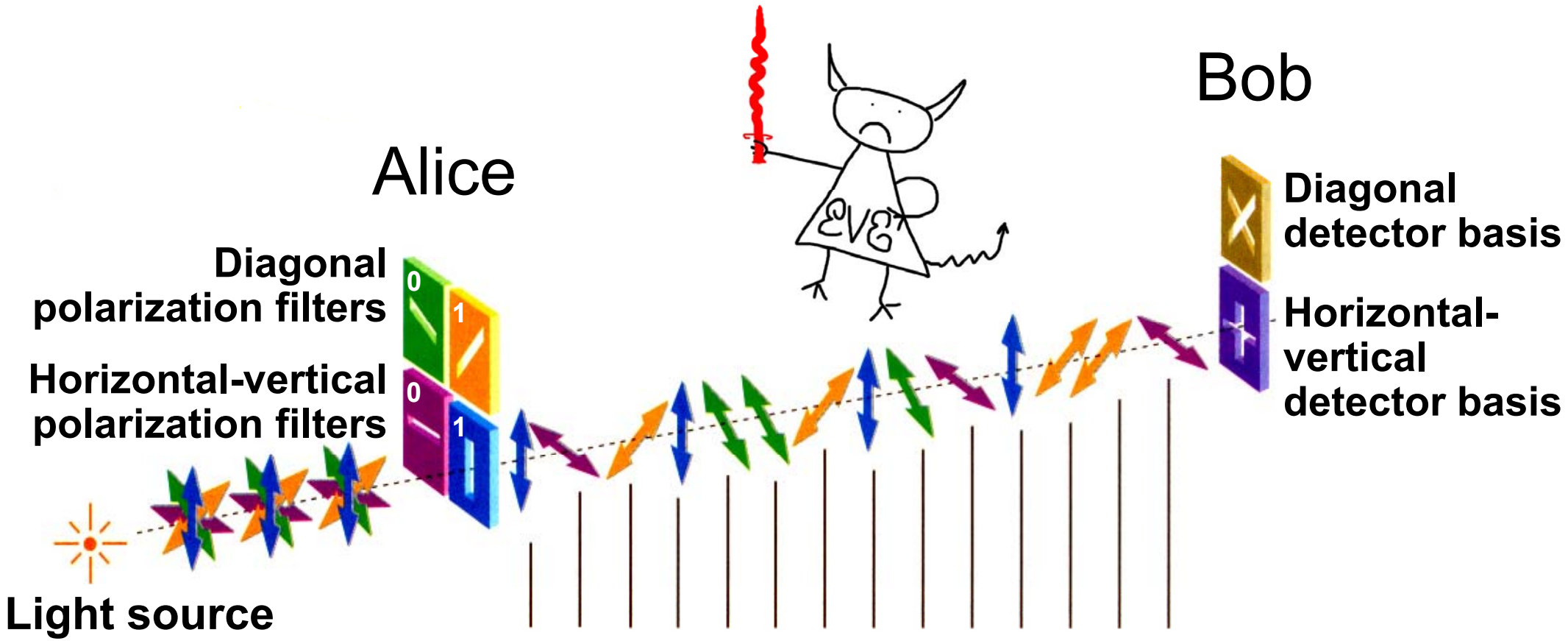
2009 A quantum cryptosystem fully hacked :)

Key distribution



- **Secret key cryptography requires secure channel for key distribution**
- **Quantum cryptography distributes the key by transmitting quantum states in an *open channel***

Quantum key distribution



Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Bob's detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+
Bob's measurement	1	0	0	1	0	0	1	1	0	0	0	1	0	0
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0

Image reprinted from article: W. Tittel, G. Ribordy, and N. Gisin, "Quantum cryptography," Physics World, March 1998

Commercial offers (as of August 2009)

id Quantique

(Switzerland)

SALE
€100,000
(*maybe cheaper)

VPN encryptor (AES)
+
quantum key generator

MagiQ Technologies

(USA)

VPN & quantum key generator

SmartQuantum

(France)

VPN & quantum key generator

Motivation for attack

- How **secure** is quantum key distribution (QKD) **practically**?

To build the first complete working eavesdropping experiment in the world!

- Eve lost the battle against security proofs

but

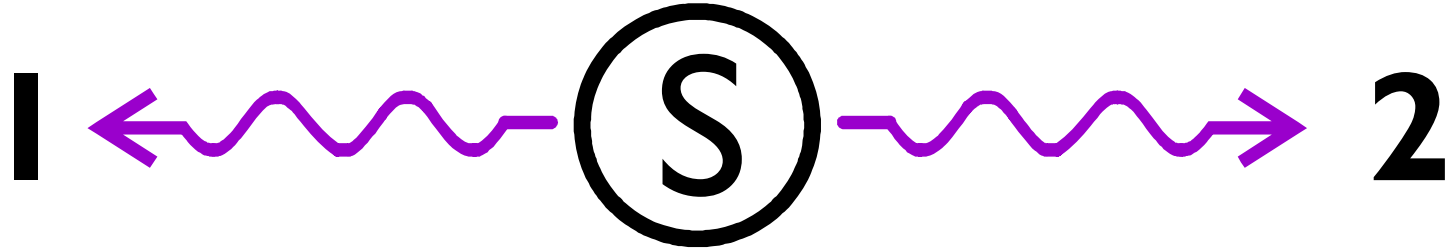
she can **exploit component imperfections**

(e.g., saturation and blinding behavior of passively-quenched APDs)

The system under attack

- QKD system from CQT in Singapore
  - Basically all systems vulnerable
- Entanglement based QKD
  - What is entanglement?
  - How can it be used for QKD?
  - What is Bell's inequality…?

Entanglement



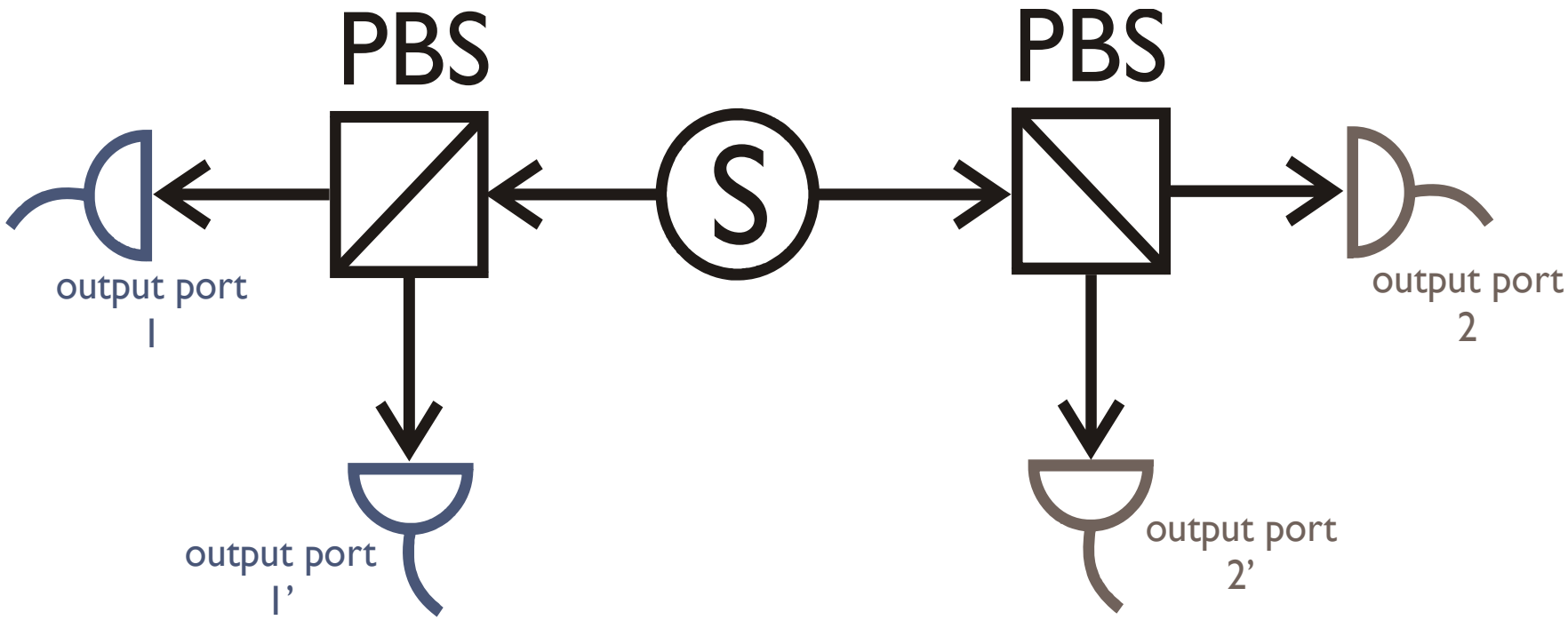
$$|\Psi\rangle^- = \frac{1}{\sqrt{2}}(|\uparrow_1, \rightarrow_2\rangle - |\rightarrow_1, \uparrow_2\rangle)$$

$$= \frac{1}{\sqrt{2}}(|\nearrow_1, \nwarrow_2\rangle - |\nwarrow_1, \nearrow_2\rangle)$$

Entanglement

- "Spooky action at a distance"
  - Einstein, Podolsky and Rosen, 1935
  - John Bell, 1964: How to measure what's going on

Bell state measurement

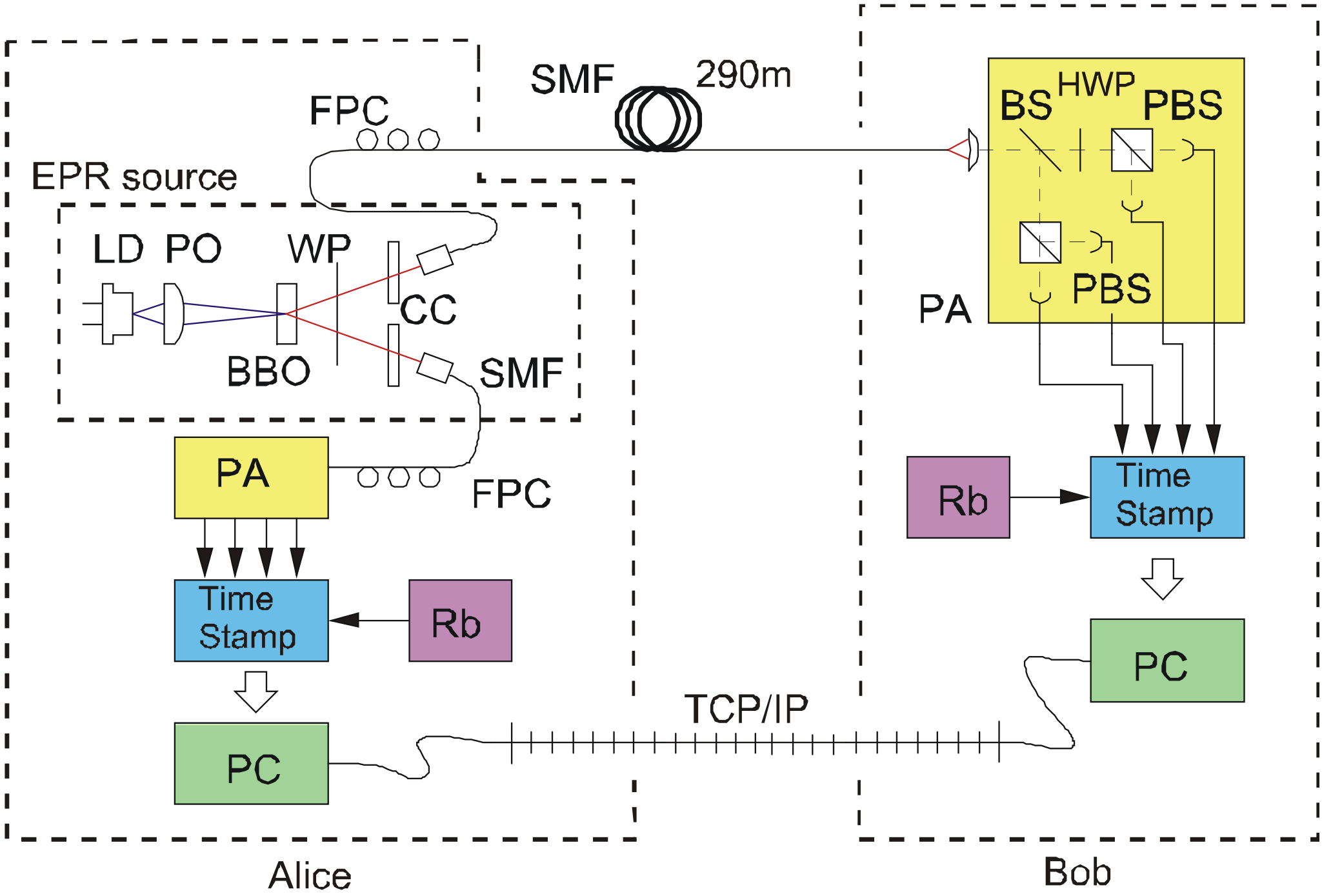


Entanglement-based QKD

- No need for random numbers

- Different photons, different colors?
  - Dimensionality of Hilbert space needs to be known for security, measuring Bell's inequality

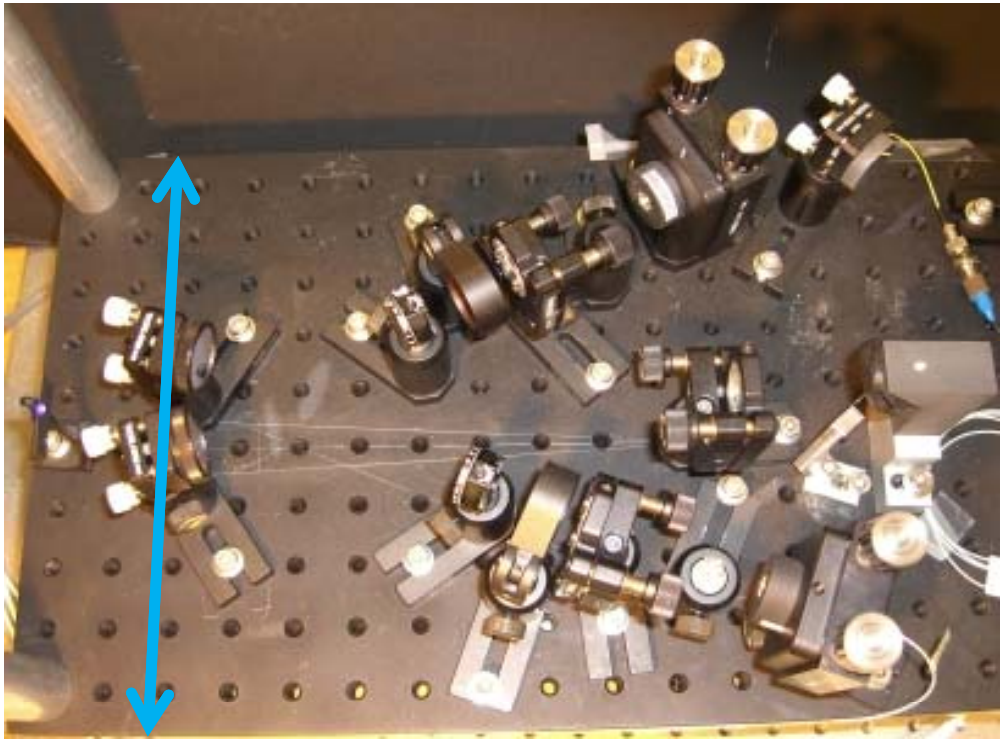
Entanglement-based QKD



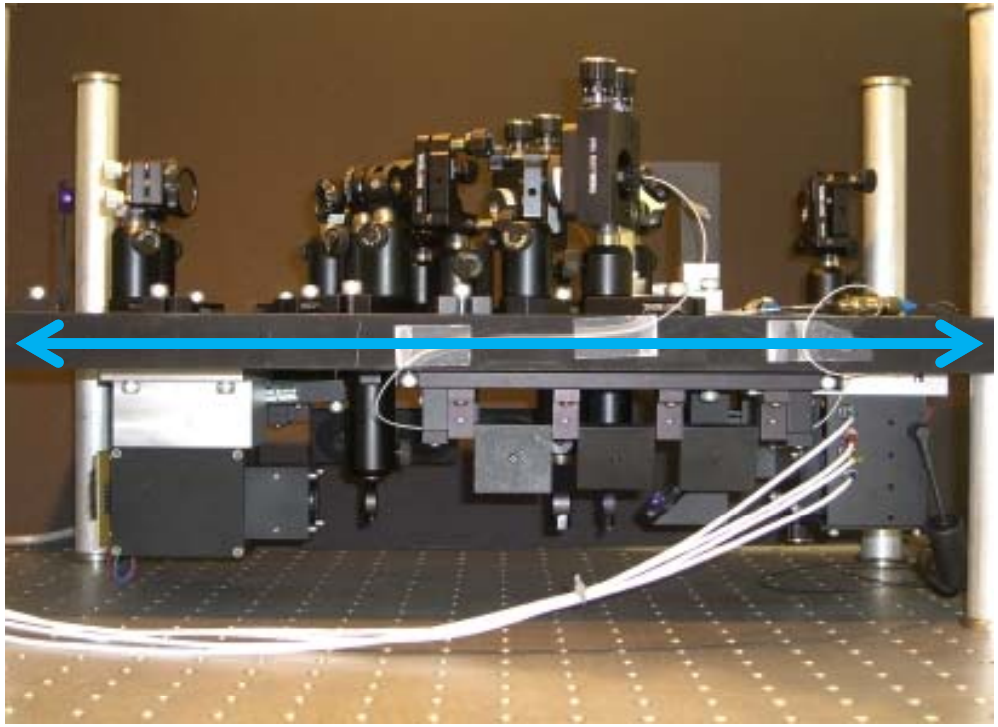
New J. Phys. **11**, 045007 (2009)

Entanglement-based QKD

- **Pair source:**
  - **Blue photon in, two red photons out**
  - **Strong temporally correlated ☺**
  - **Spectrally broader than dimmed lasers ☹**



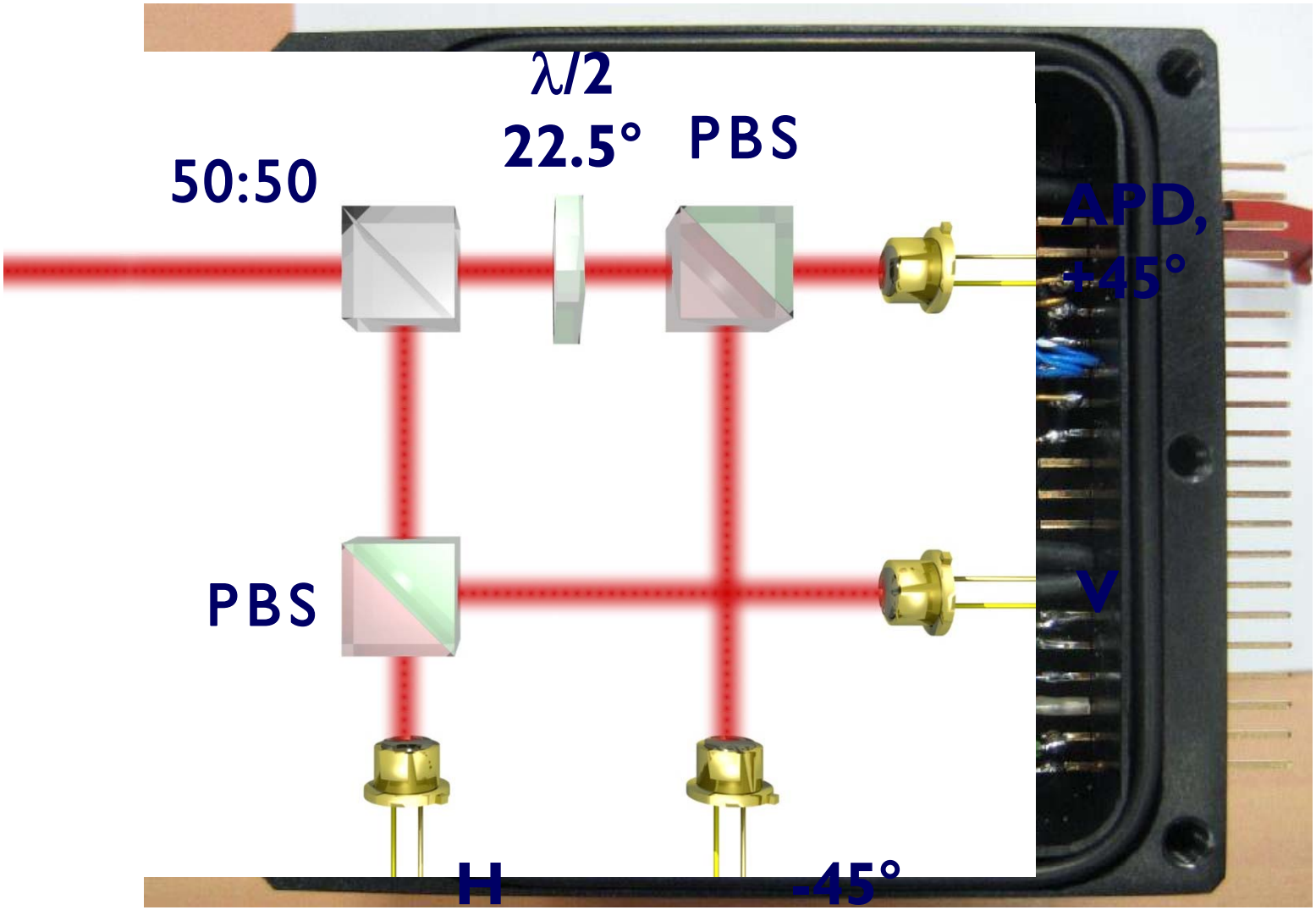
25 cm



50 cm

Detection of photons

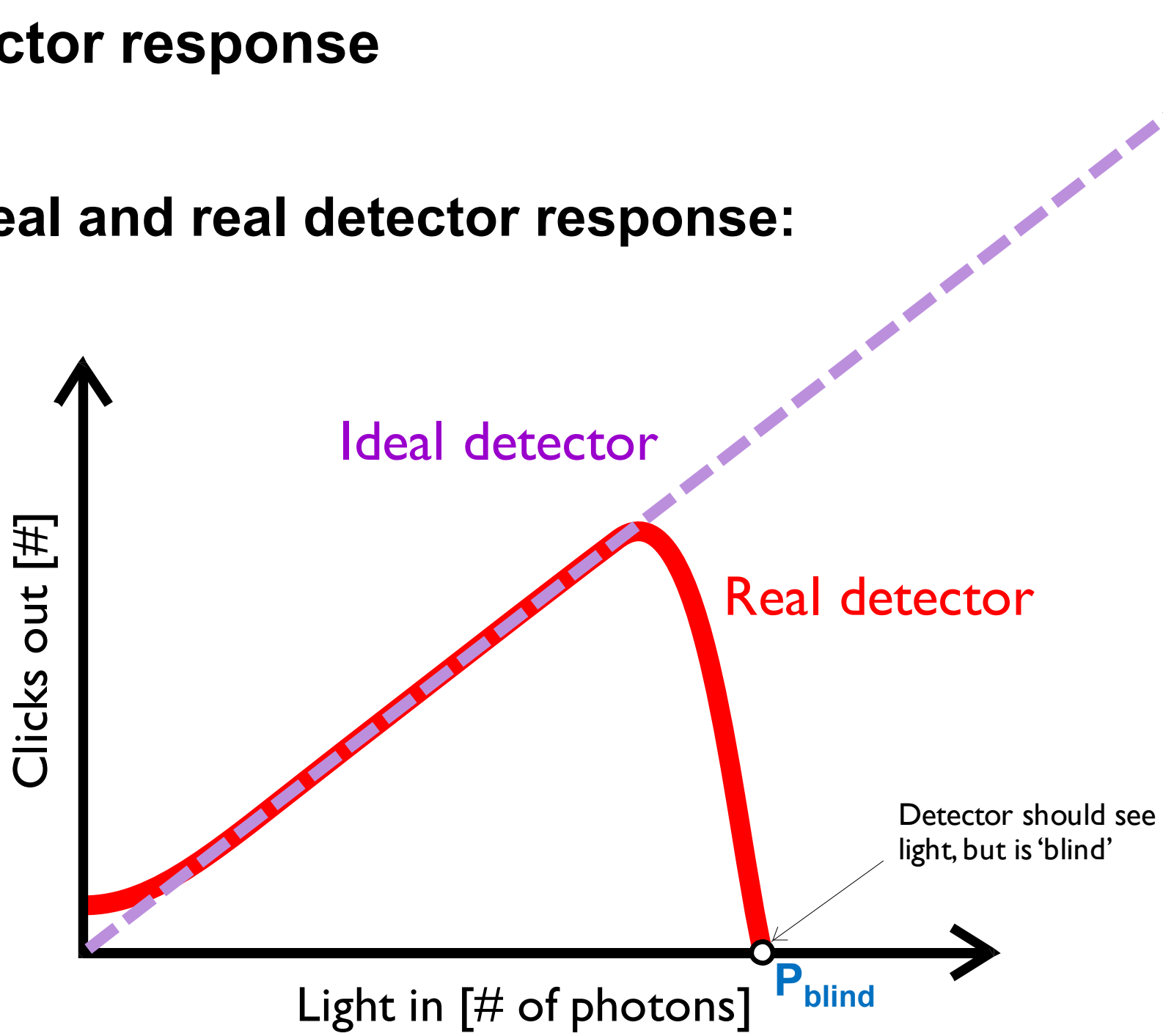
- **Detection: Polarization analyzer**



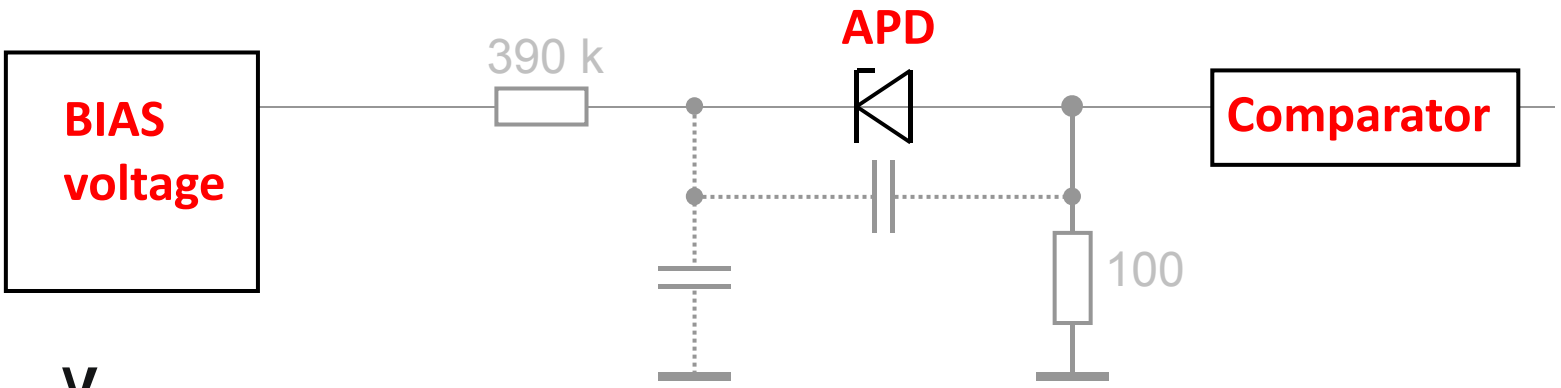
J.G. Rarity et al., J. Mod. Opt. **41**, 2345 (1994)

Detector response

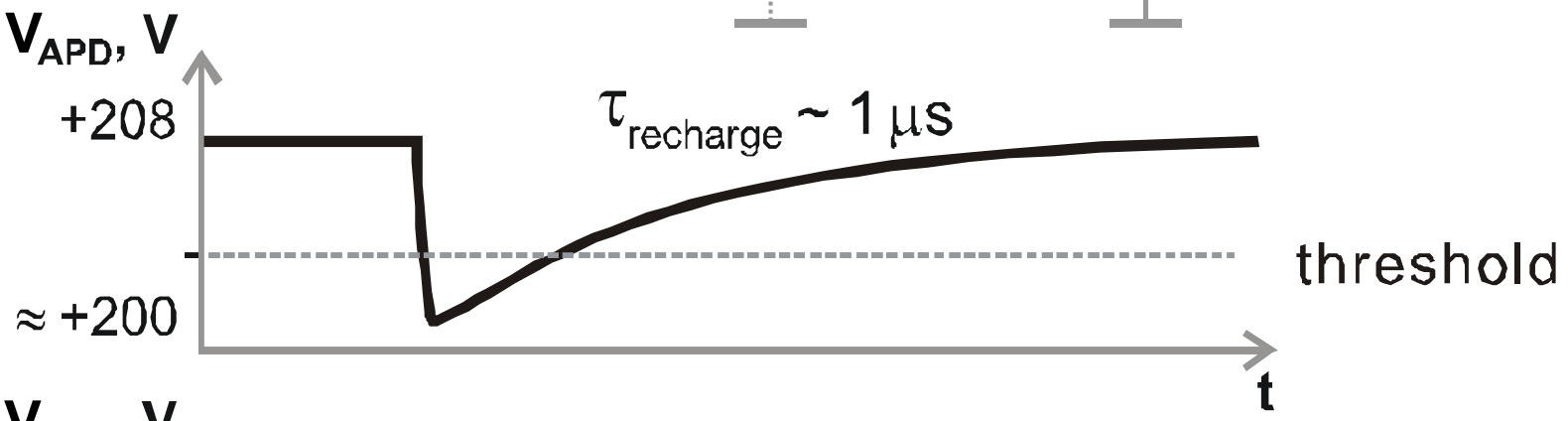
- **Ideal and real detector response:**



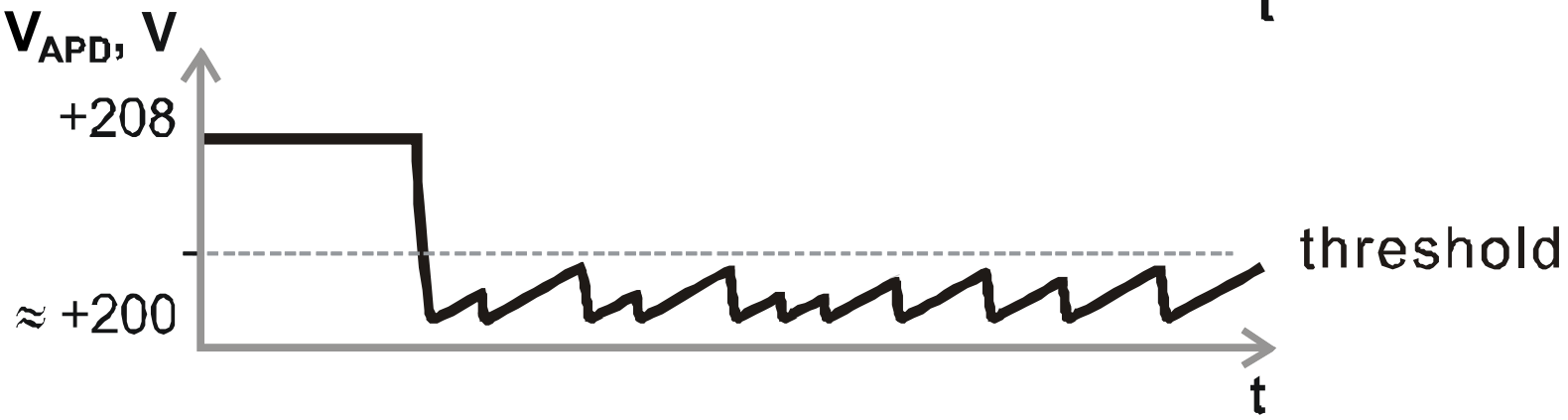
Passively-quenched detector



Single-photon response



Bright illumination

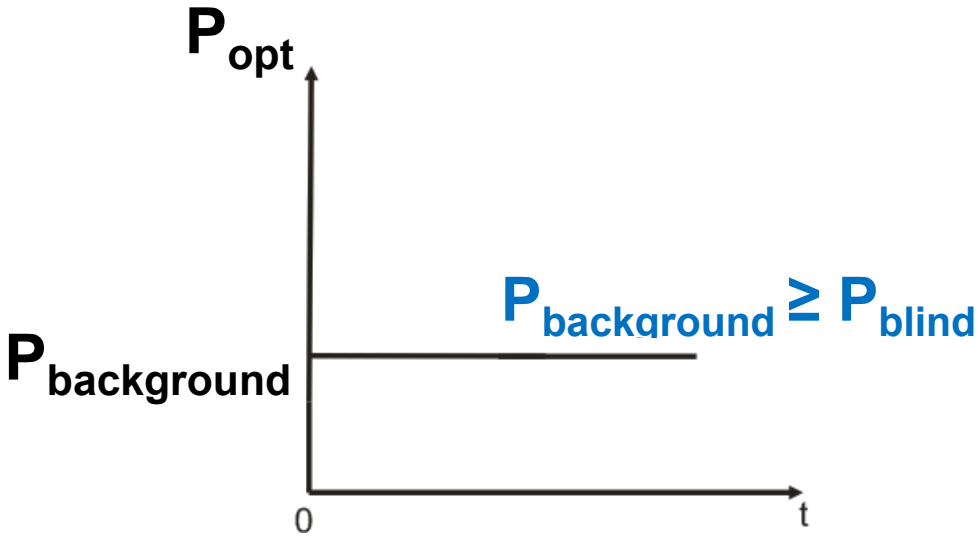


Detector kept below breakdown voltage, now works in classical mode!

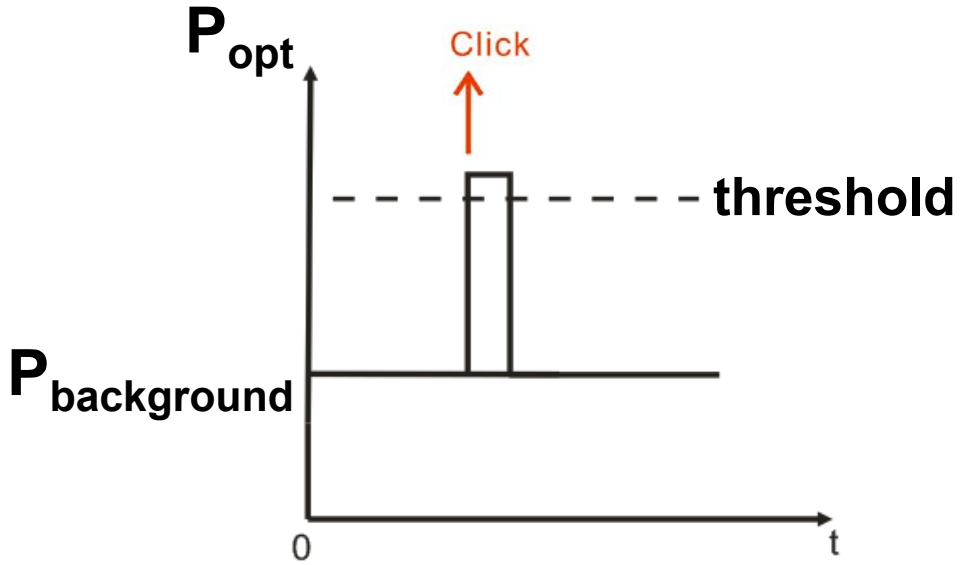
→ Detector is blind (”0”) to single photons

→ Detector will click (”1”) if classical pulse above comparator threshold

Control intensity diagrams



No click



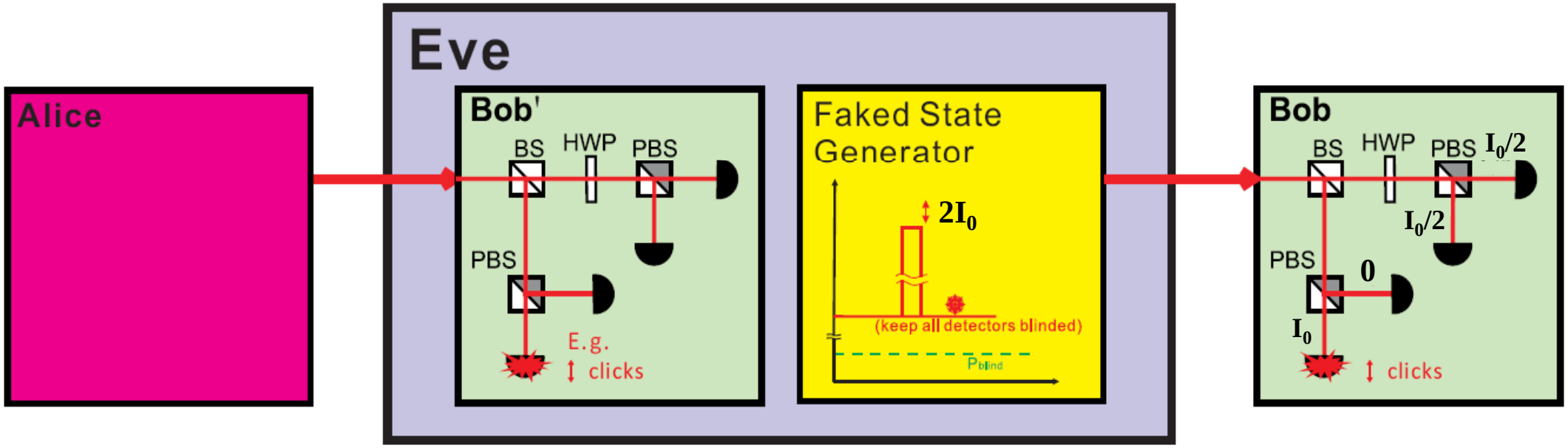
Single click

Faked state

Intercept-resend (faked-state) attack

Eve forces her detection result onto Bob by sending

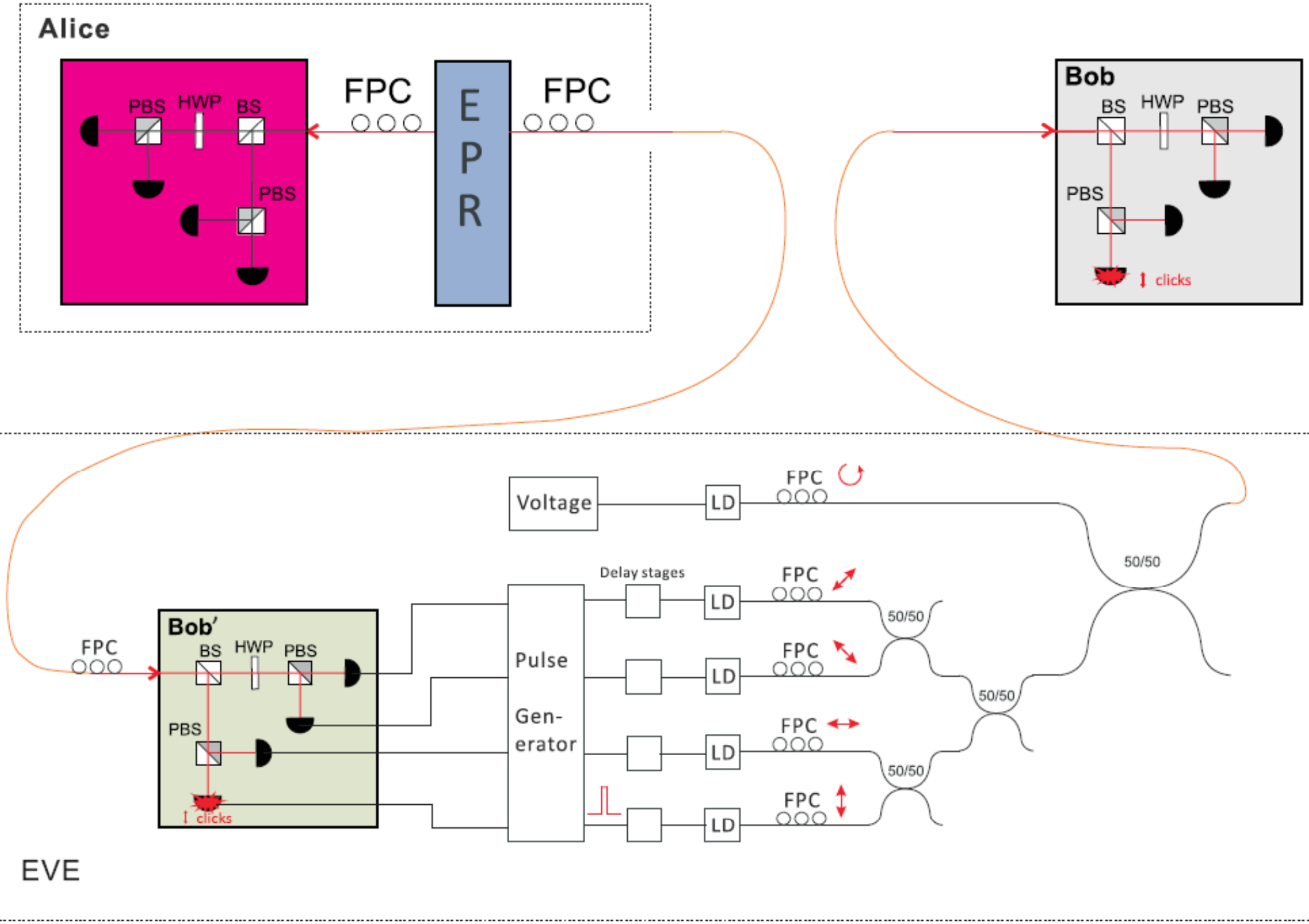
- Background light to keep all detectors blinded (circular polarization)
- Faked-state above intensity threshold to make target detector click (linear polarization)



In conjugate basis, faked-state is split in half, below threshold (no click)

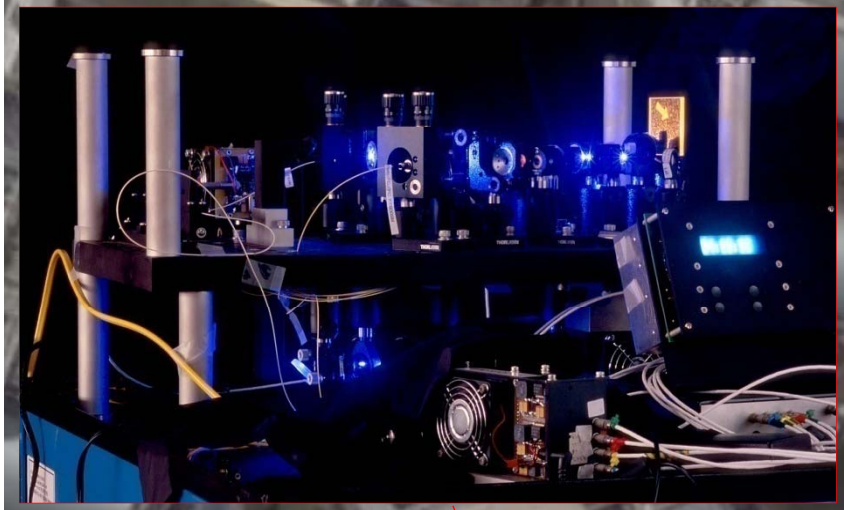
arXiv:0809.3408

QKD under attack



Eavesdropping on installed QKD line

on campus of the National University of Singapore



290 m of fiber

Eve

Alice

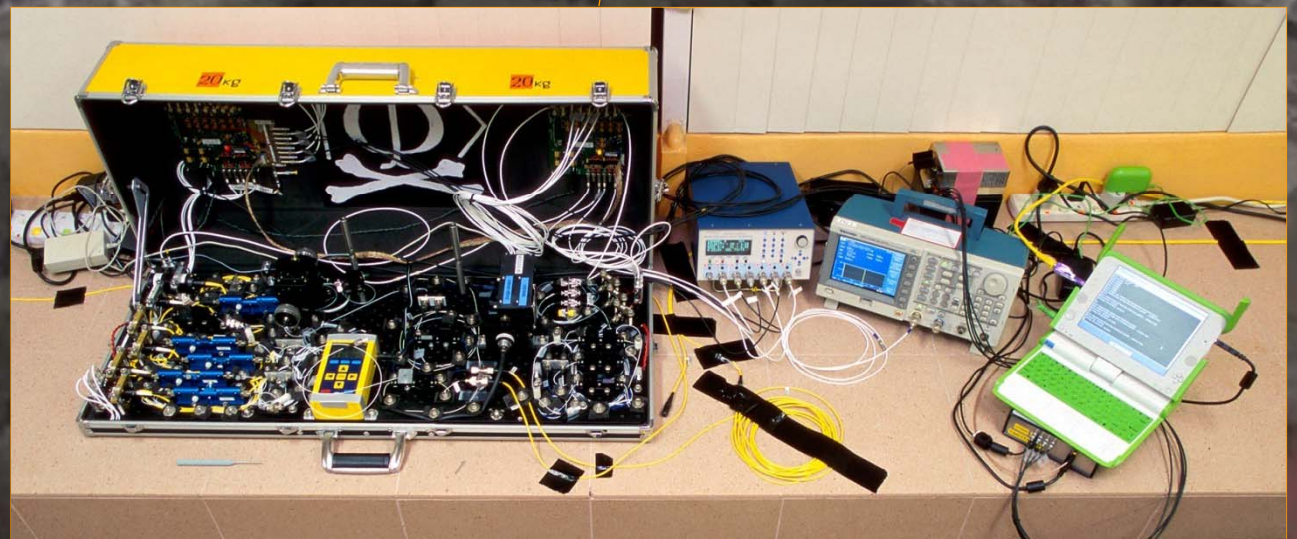
Bob

S15

S14

S13

S12



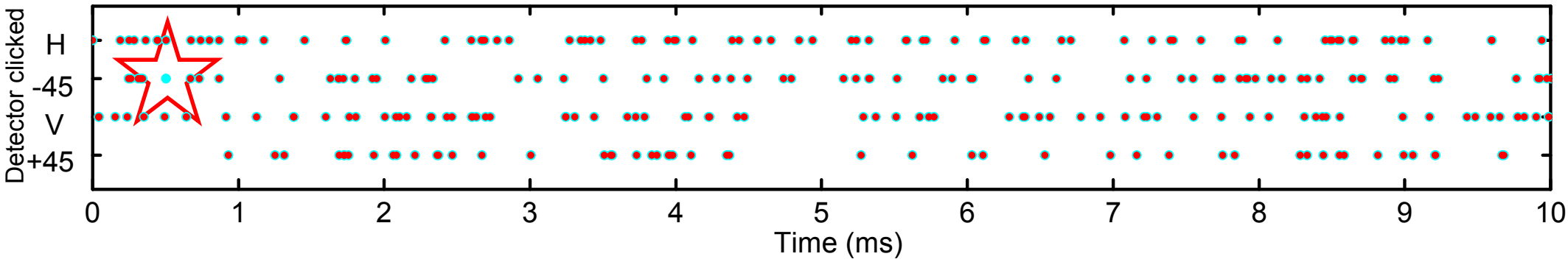
Satellite image ©Google

Eve, installed and running

+ recording all classical communication Alice–Bob (Wireshark)

Does Eve really have 100% key information?

Clicks in Eve and Bob:



✓ **Good correlation**

✗ **More clicks in Eve doesn't matter**

- Eve forcing a click in Bob: ≈97% probability
- Eve has 100% information of the wiretapped line, because Bob has to reveal which clicks were received

What about a ‘workaround’?

- Sure... there will be a workaround
  - BUT:
  - No universal security measure, like a ‘quantum state’!

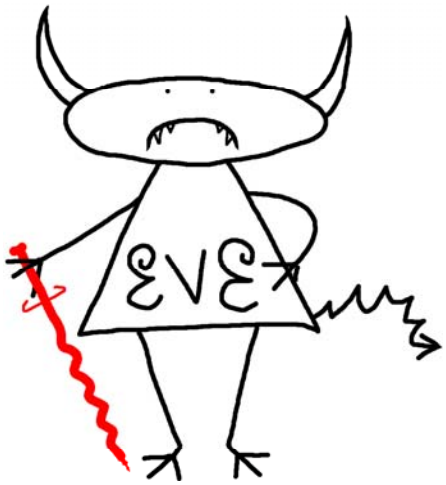
Generating arbitrary quantum states

- Eve is able to fake an EPR source
  - Also interesting for other experiments
- The laws of physics:
  - Quantum correlations:
  - No eavesdropper??
- Applicable to schemes which expect single photons

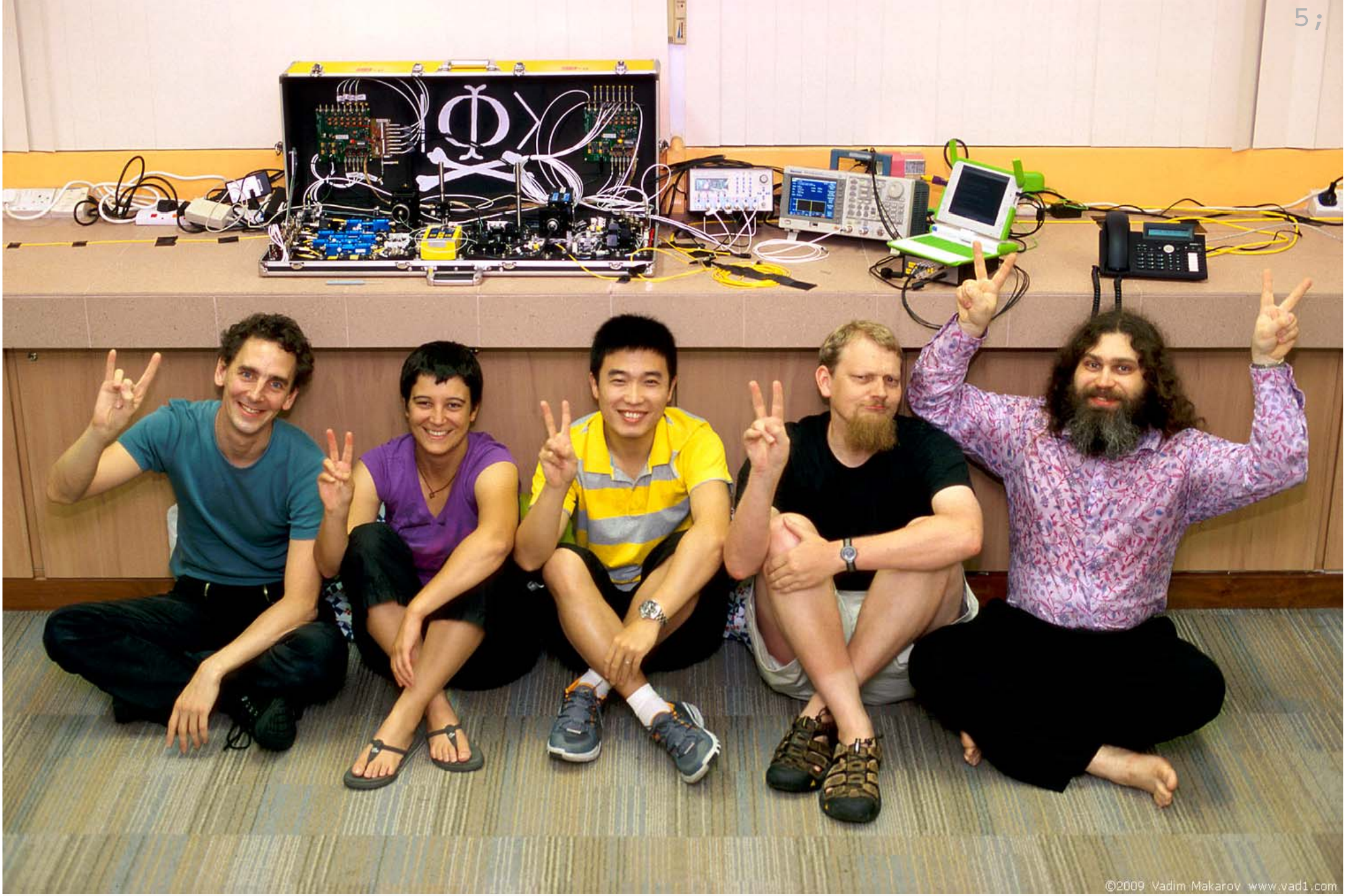
Questions and perspectives:

- What is a photon?
  - A photon is a single click on a detector… (Anton Zeilinger)
  - well....
- You cannot delegate security!
  - Don’t trust ‘security’ in a black box, even if it’s expensive or called ‘quantum’

Our attack



- First experimental implementation
- Eve has 100% key information
- Demonstrated eavesdropping under realistic conditions (290 m fiber run via 4 buildings)



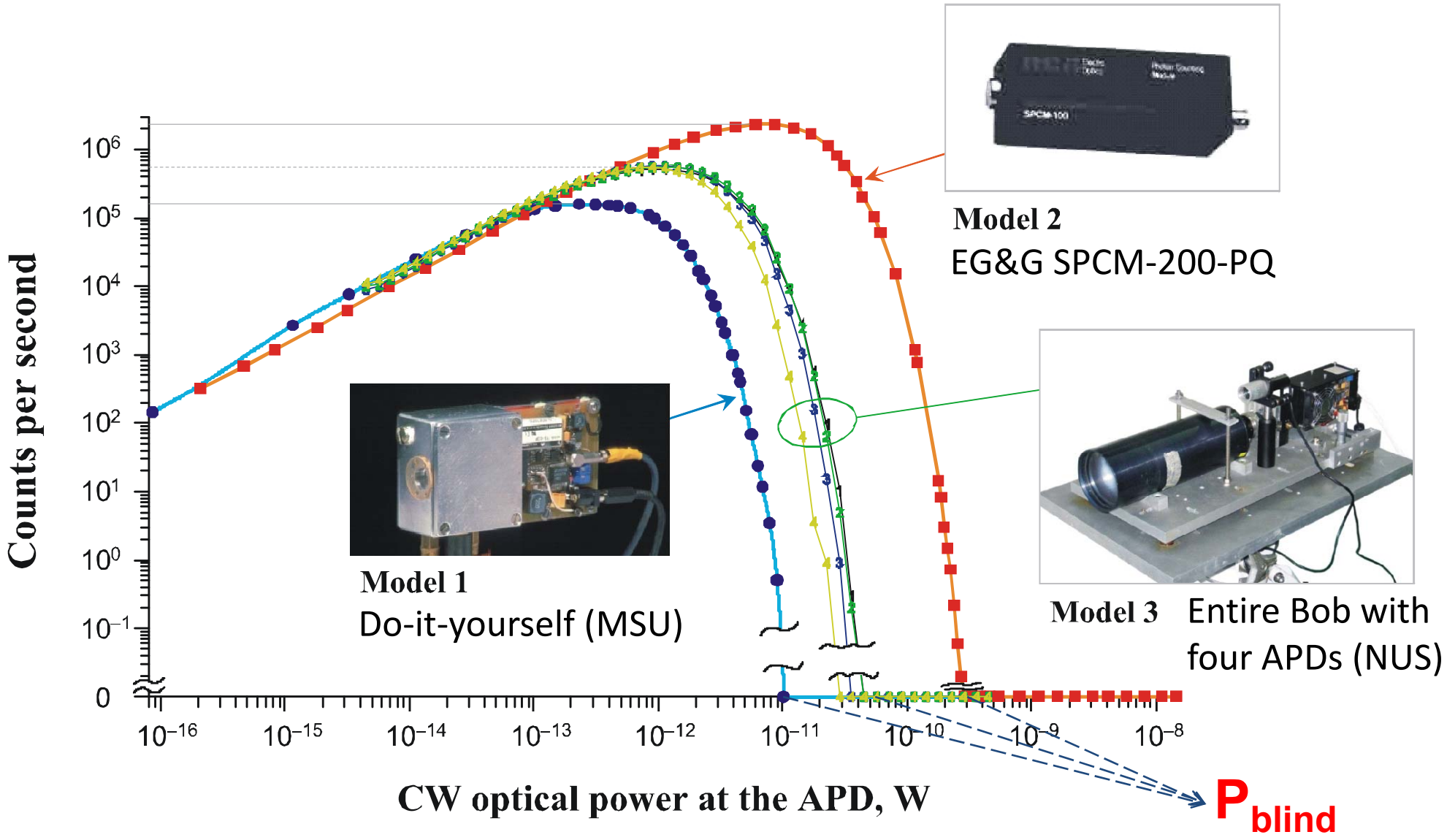
Thank you.

www.iet.ntnu.no/groups/optics/qcr
www.quantumlah.org

More technical details about the attack

that we didn’t have time to show in the talk

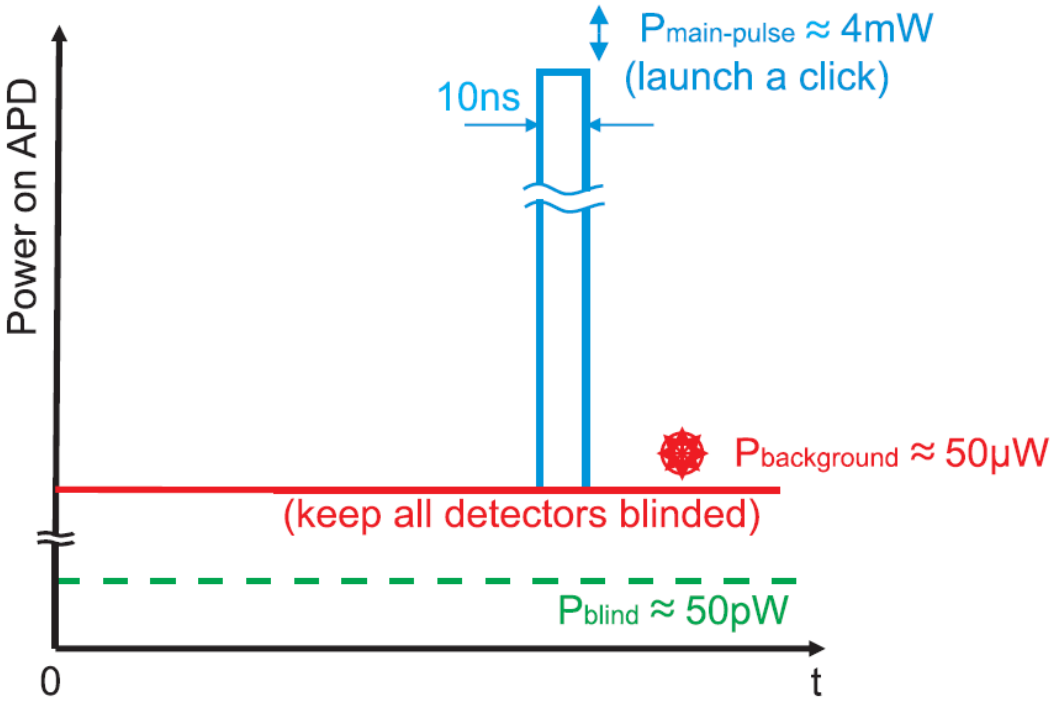
Eve can exploit blinding of APD under bright illumination... and make a single photon detector work as a classical detector!

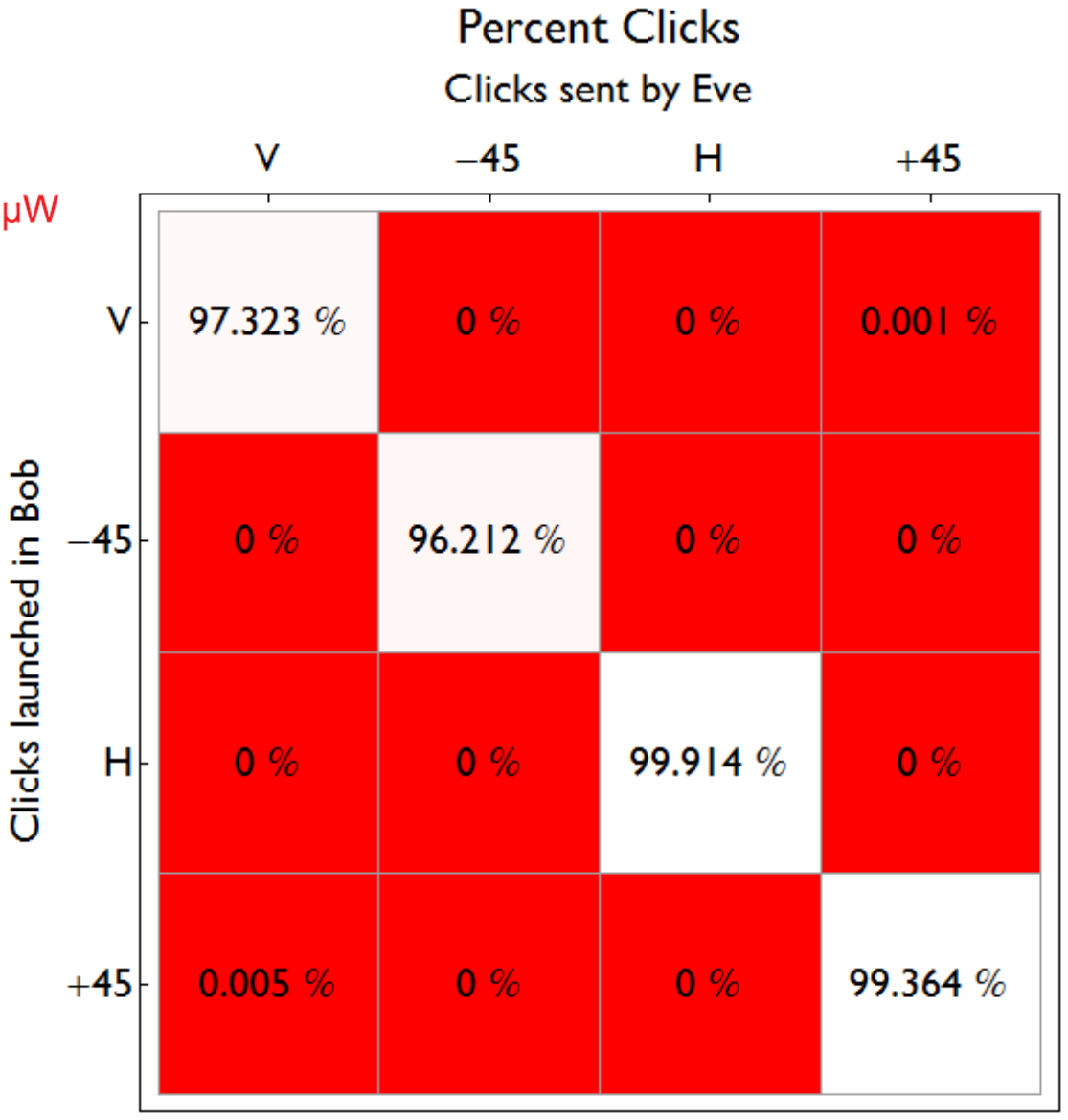


Above P_{blind}, detector totally blind to single photons, dark counts, afterpulses

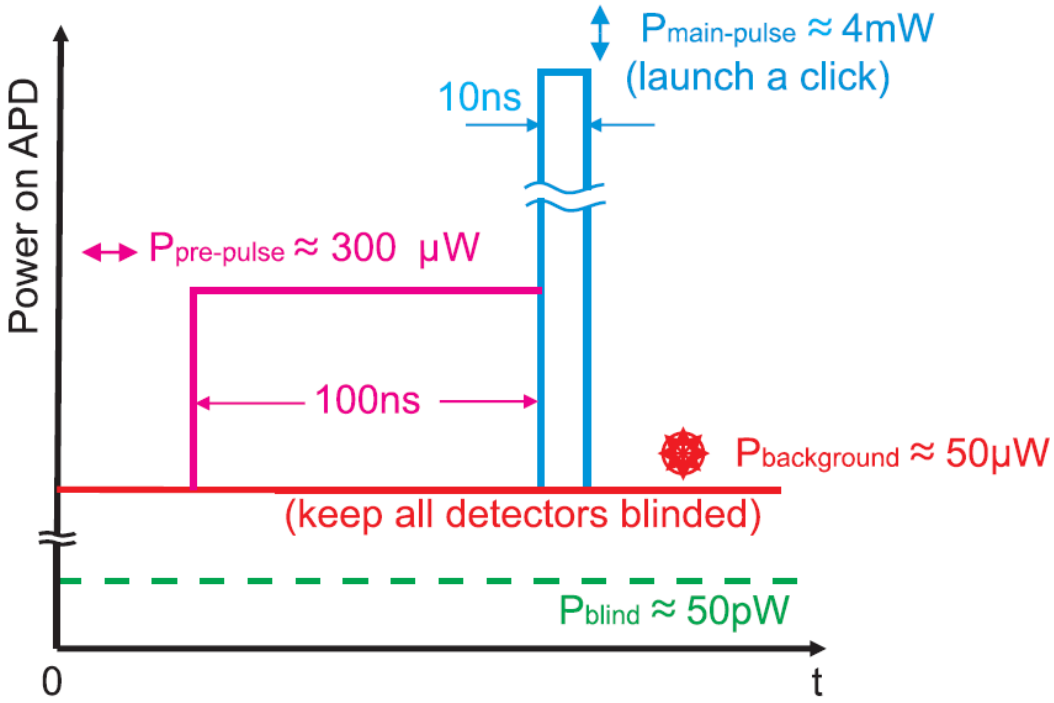
New J. Phys. **11**, 065003 (2009)

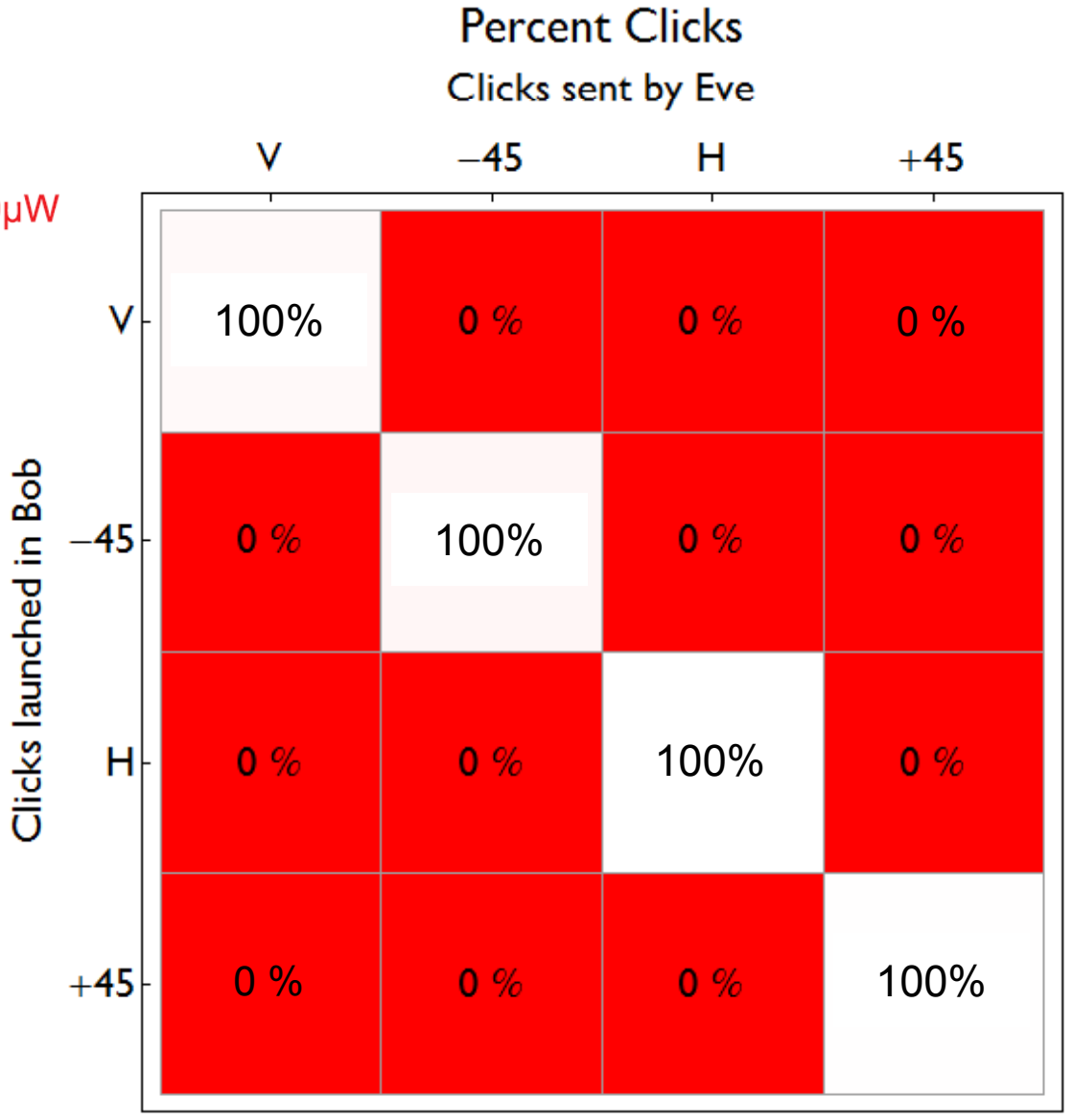
Bob control efficiency



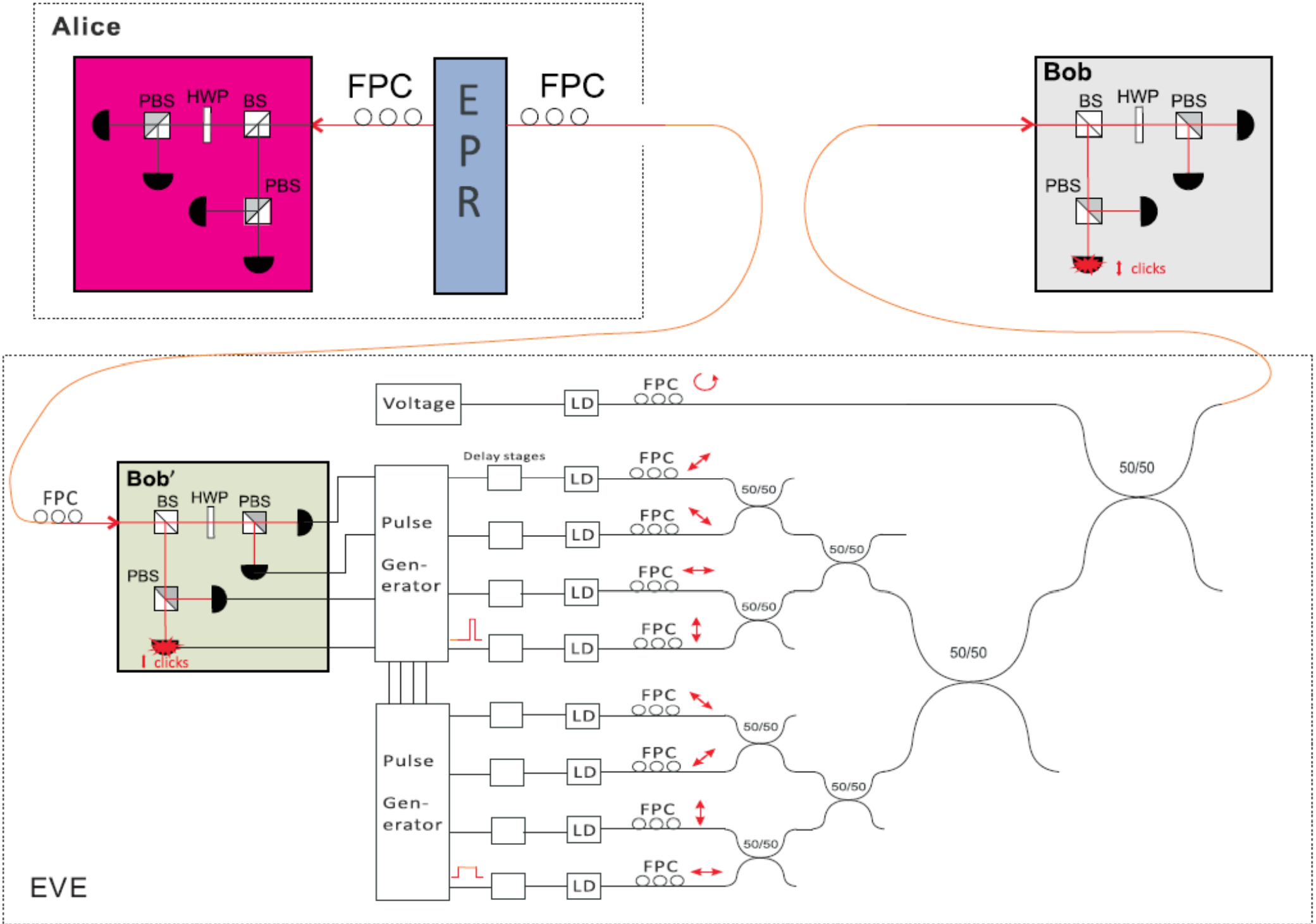


Improved control intensity diagram



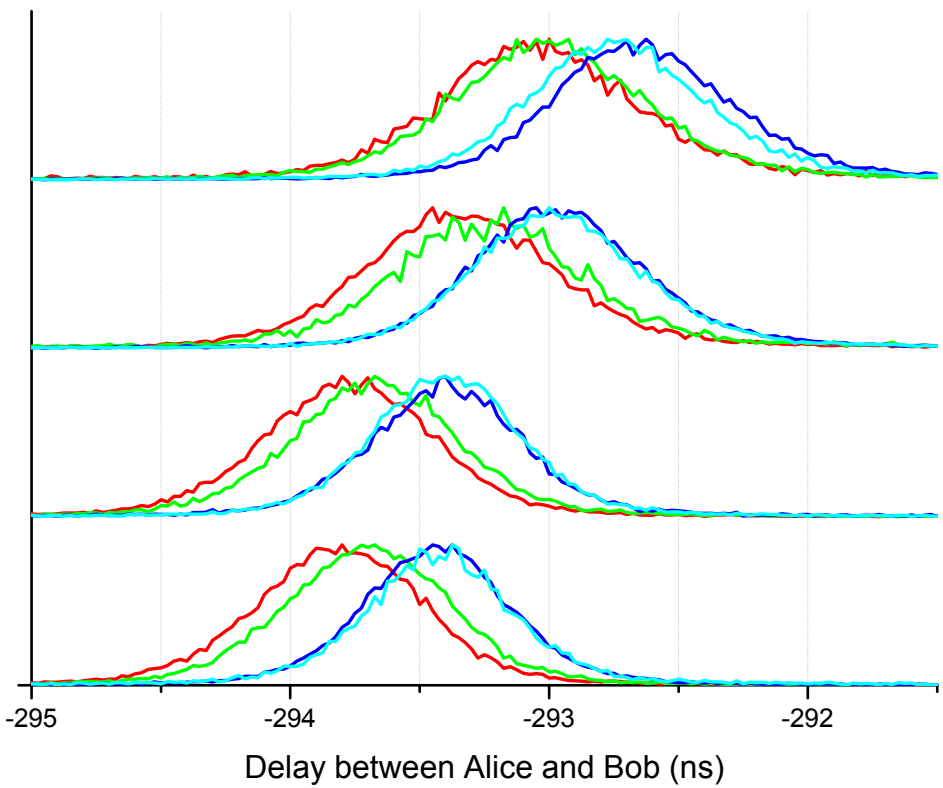


Final Eve's scheme

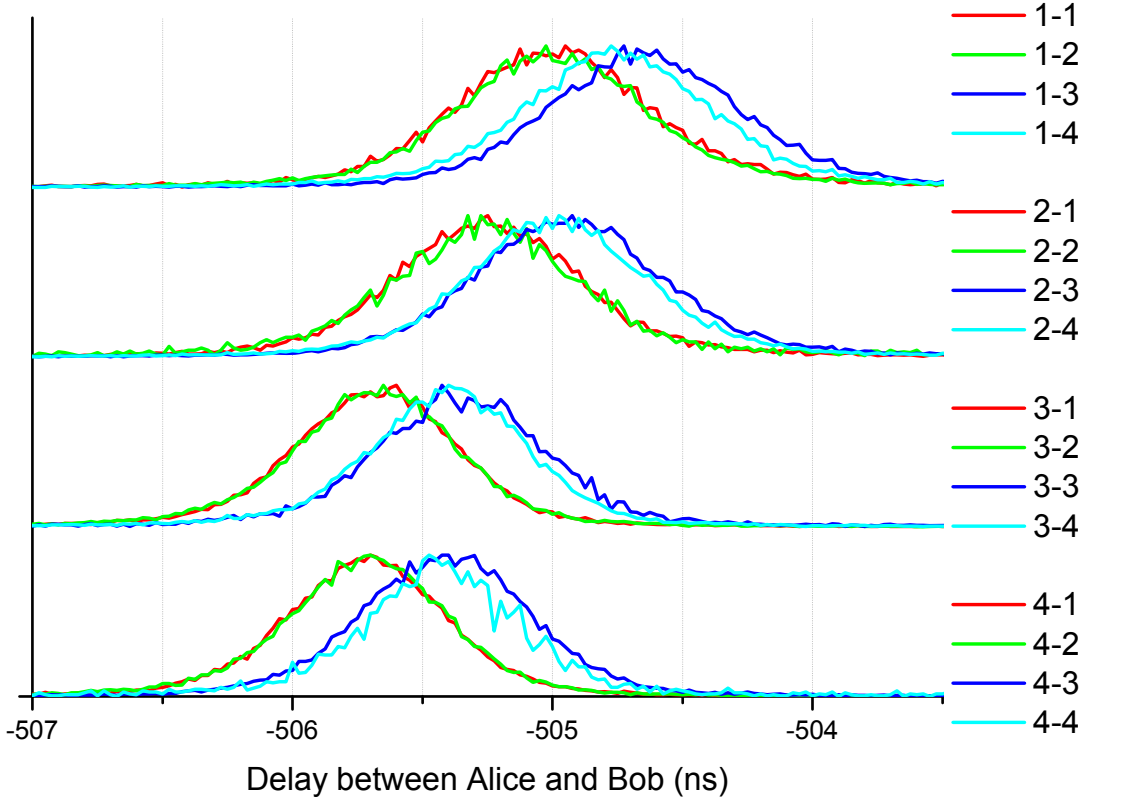


Timing performance

Normal QKD without Eve



After Eve's delay stages adjusted



$FWHM_{avg.}$ = 761 ps

$FWHM_{avg.}$ = 779 ps

Compare the average FWHM of 16 combinations:

→ After Eve inserted, the FWHMs is practically unchanged

Attack also works via free-space link