Lecture 12 in Quantum communications course, 19 November 2019

Detector control attack

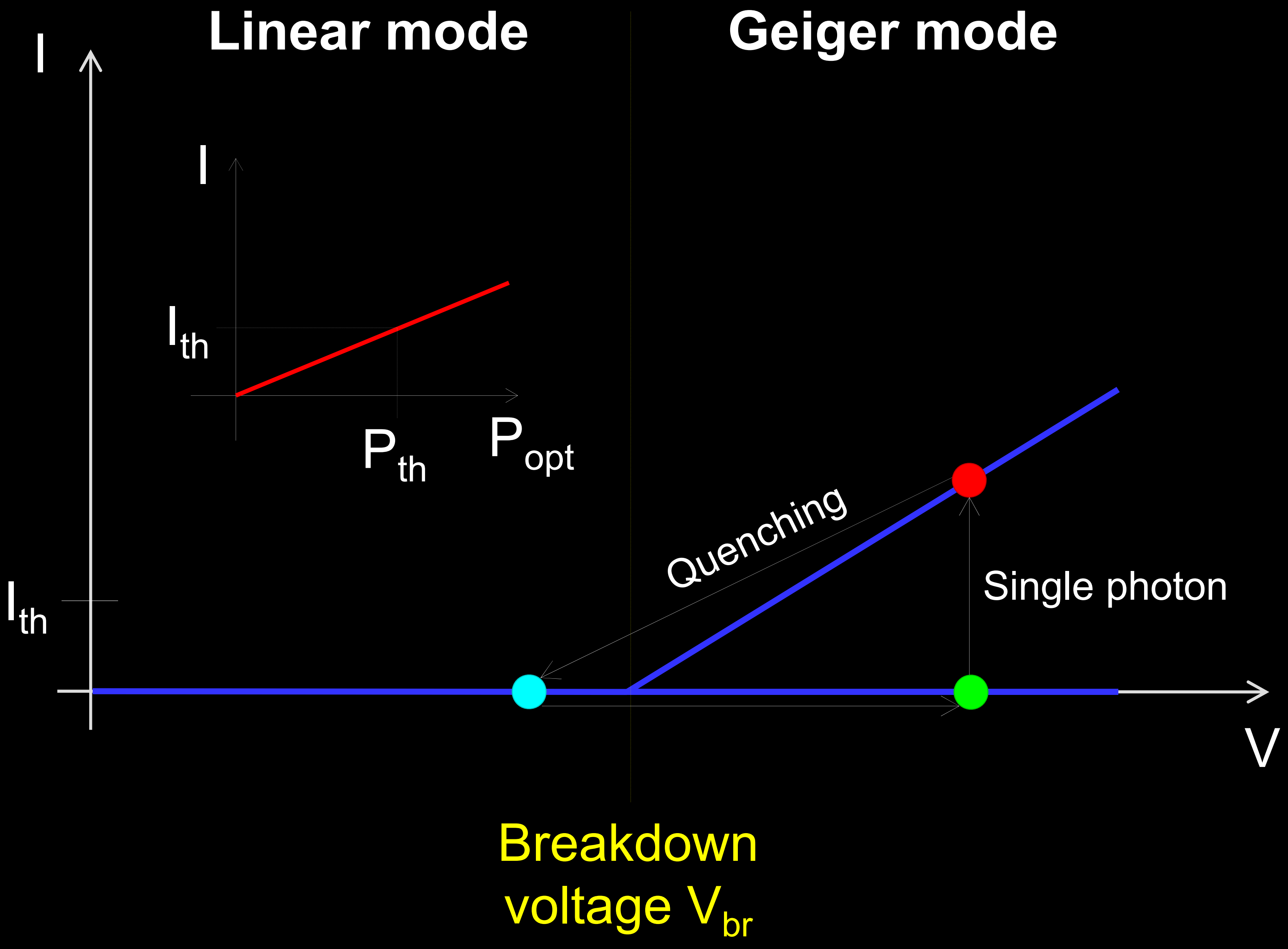
Vadim Makarov

RQC MISIS

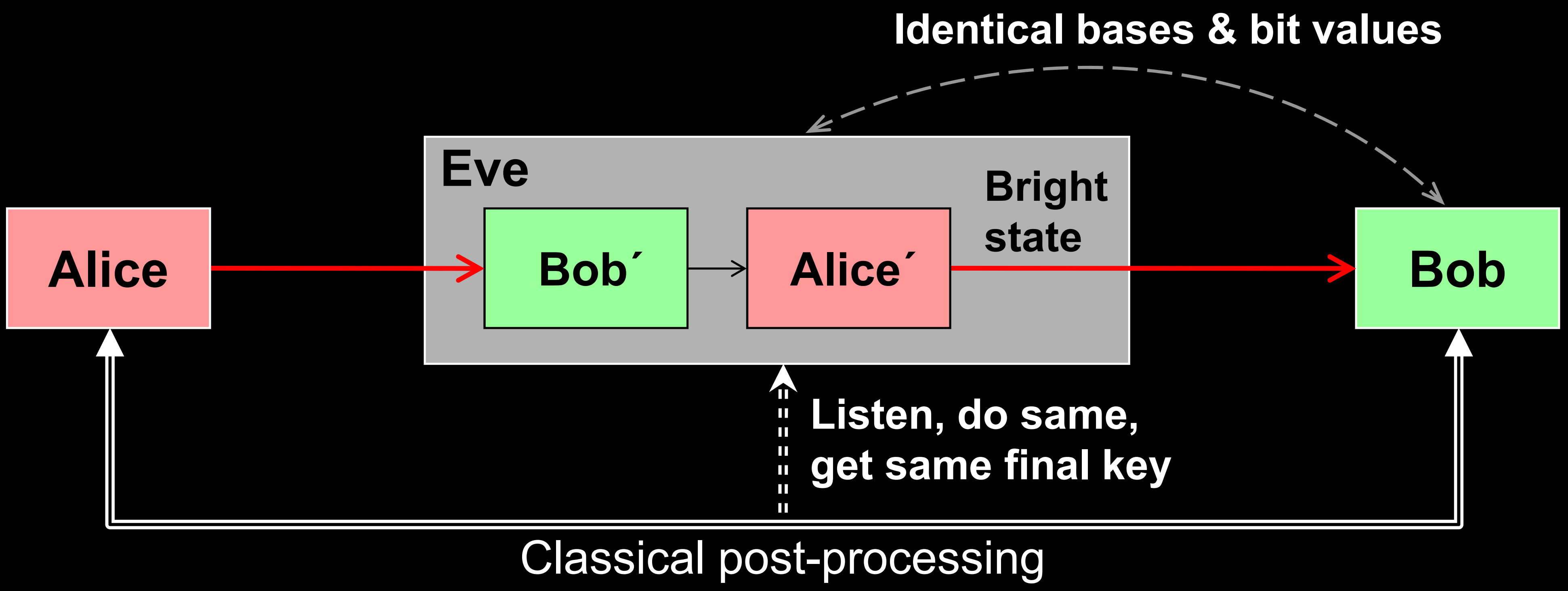
vad1.com/lab

Photo ©2010 NTNU Info / Geir Mogen

Attack example: avalanche photodetectors (APDs)



Faked-state attack in APD linear mode



Identical bases & bit values

Eve

Alice

Bob´

Alice´

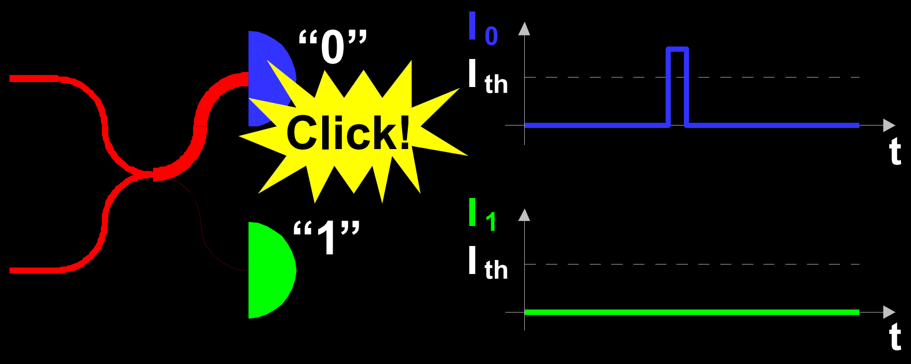
Bright state

Bob

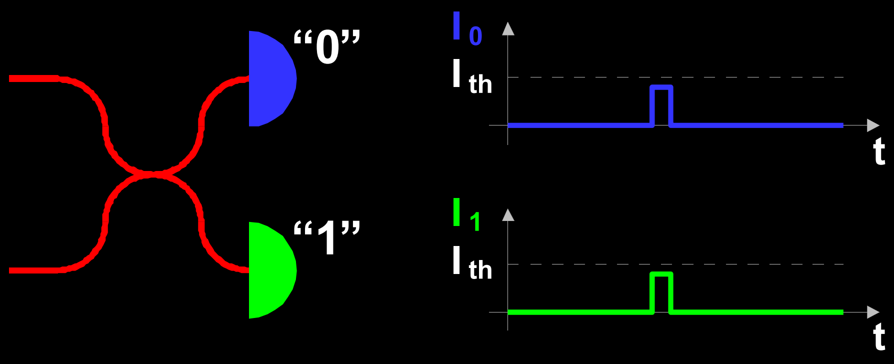
Listen, do same, get same final key

Classical post-processing

Bob chooses same basis as Eve:

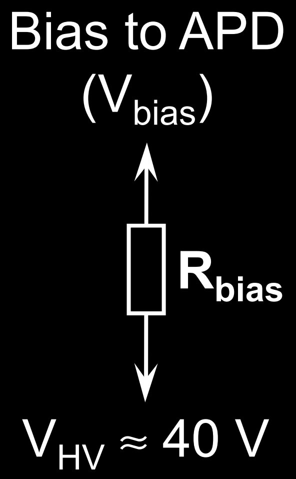


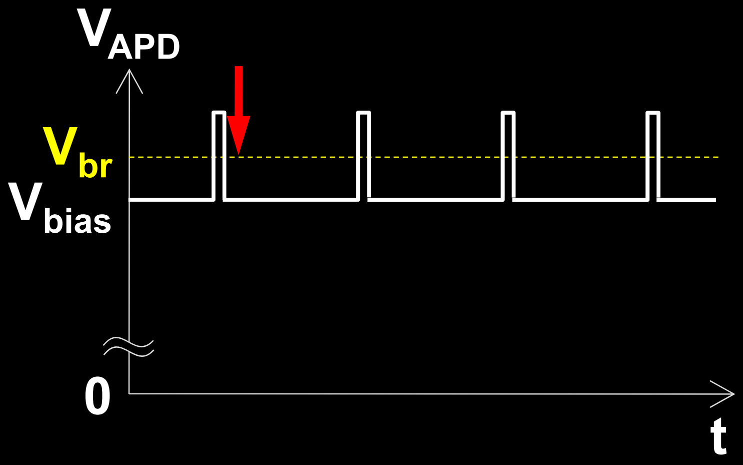
Bob chooses different basis:



L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Nat. Photonics **4**, 686 (2010)

Blinding APD with bright light

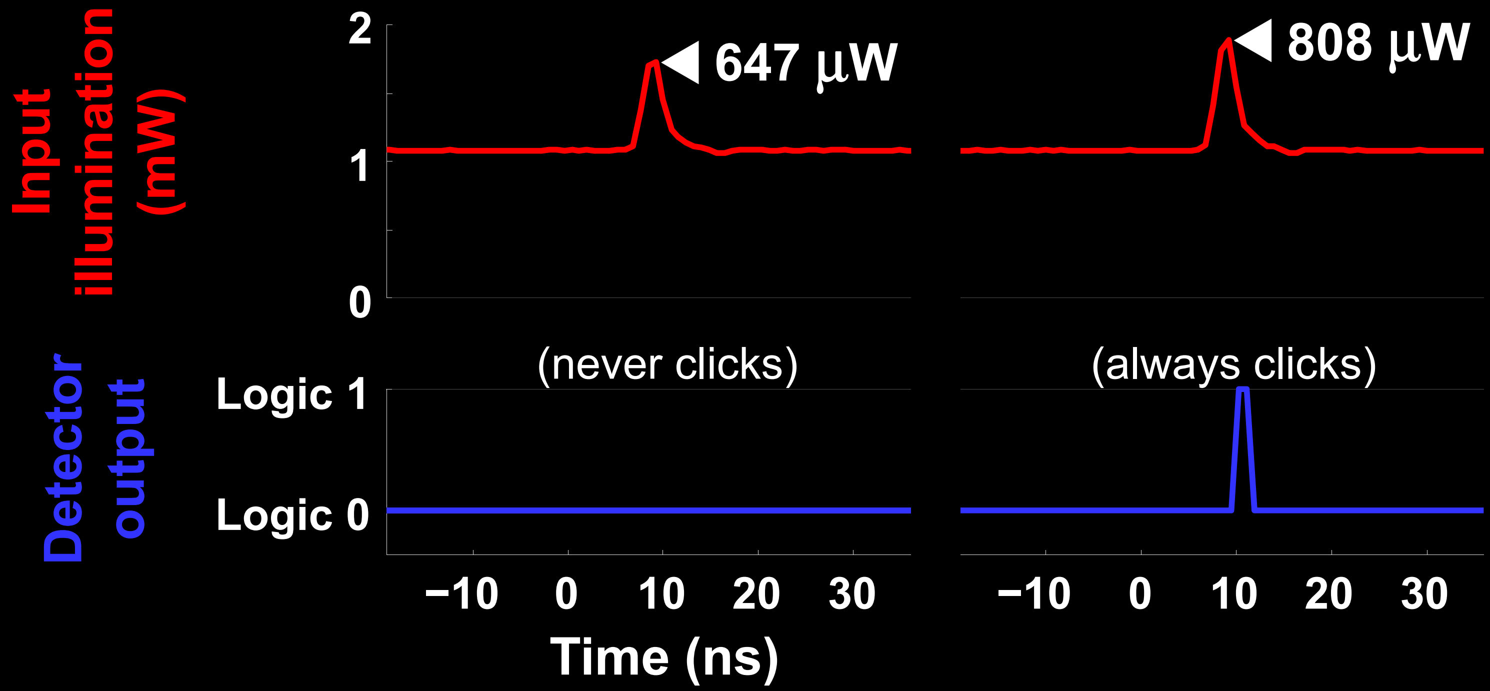




Eve applies CW light

Detector blind!

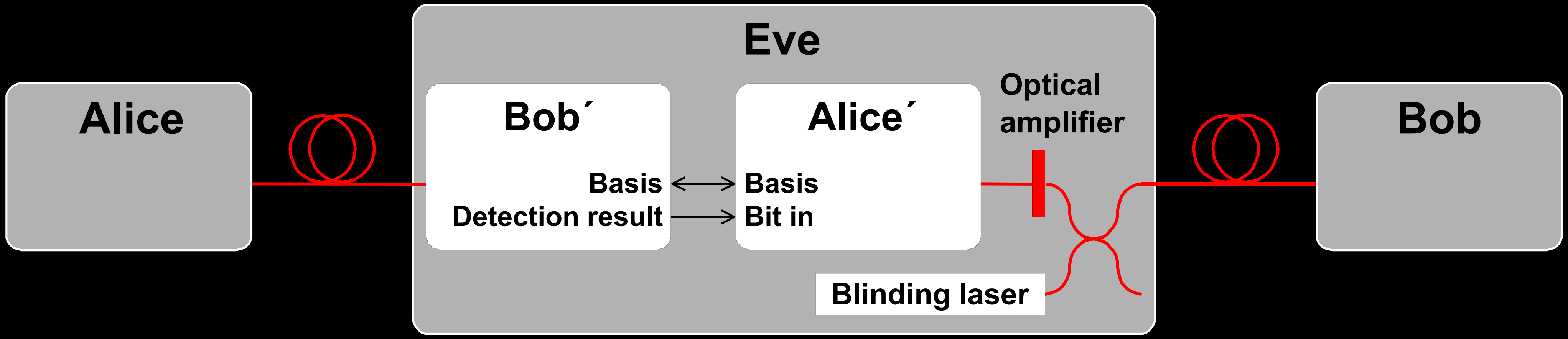
Zero dark count rate



ID Quantique Clavis2

L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Nat. Photonics **4**, 686 (2010)

Proposed full eavesdropper



Note: Intercept-resend always breaks QKD security

M. Curty, M. Lewenstein, N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004)

Eavesdropping 100% key on installed QKD line

on campus of the National University of Singapore, July 4–5, 2009

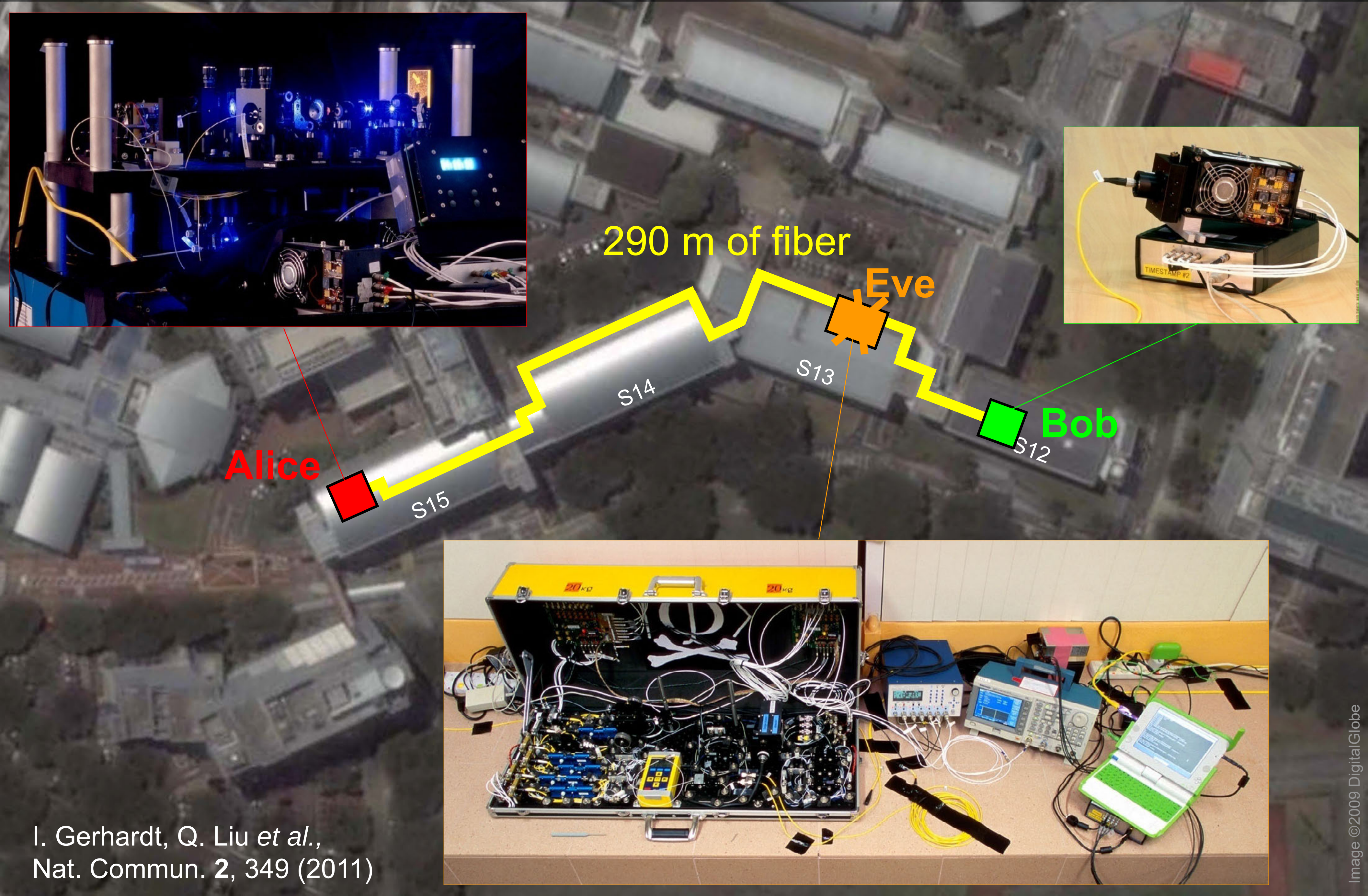
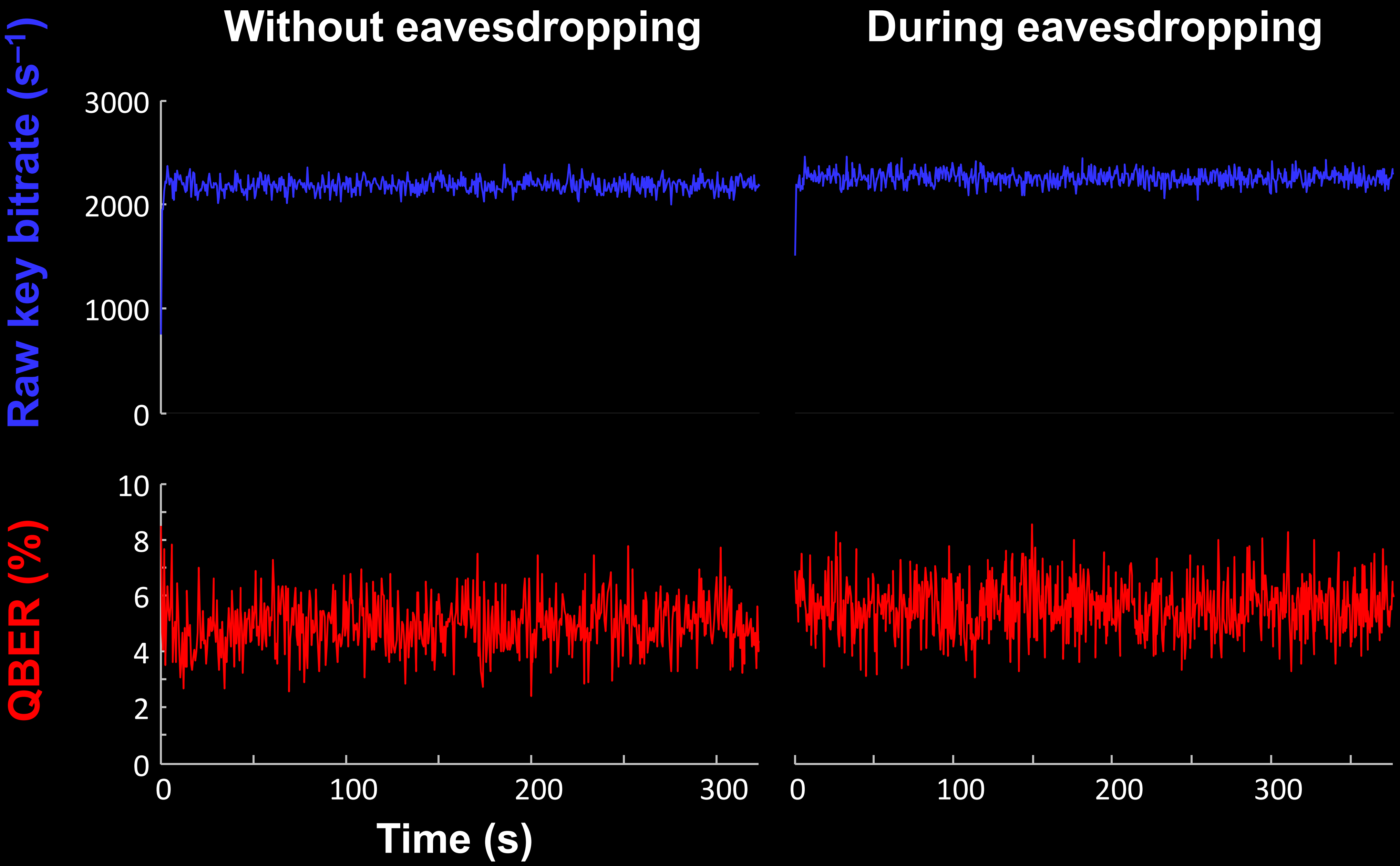


Image ©2009 DigitalGlobe

I. Gerhardt, Q. Liu *et al.*,
Nat. Commun. **2**, 349 (2011)

Eve does not affect QKD performance



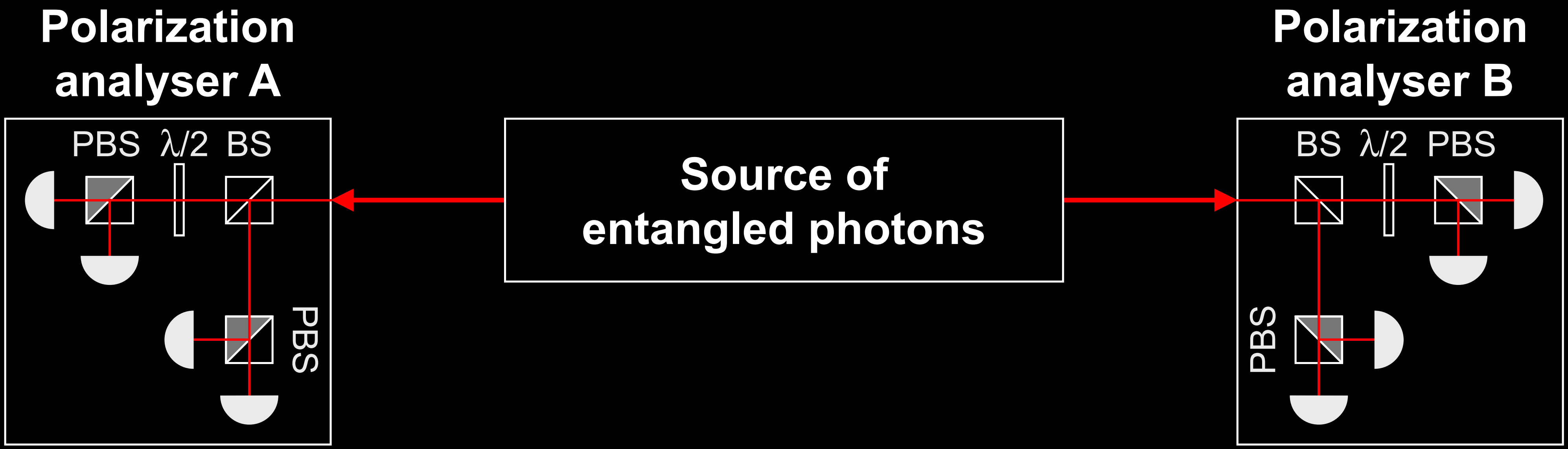
I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, V. Makarov, Nat. Commun. **2**, 349 (2011)

Faking violation of Bell inequality

CHSH inequality: $|S = E_{AB} + E_{A'B} + E_{AB'} - E_{A'B'}| \leq 2$

$$E \in [-1, 1]$$

Entangled photons: $|S| \leq 2\sqrt{2}$



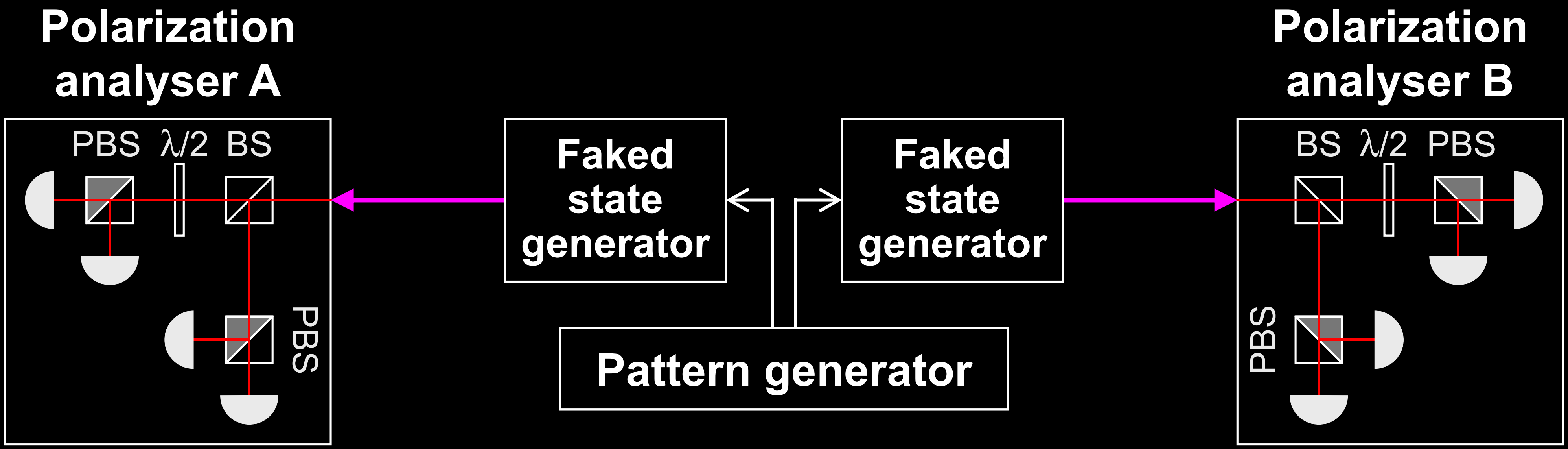
I. Gerhardt, Q. Liu *et al.*, Phys. Rev. Lett. **107**, 170404 (2011); S. Sajeed, N. Sultana *et al.*, arXiv:1902.03197

Faking violation of Bell inequality

CHSH inequality: $|S = E_{AB} + E_{A'B} + E_{AB'} - E_{A'B'}| \leq 2$

$$E \in [-1, 1]$$

Entangled photons: $|S| \leq 2\sqrt{2}$



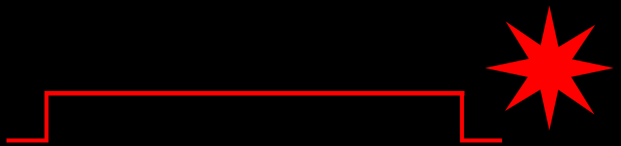
Passive basis choice: $|S| \leq 4$, click probability $= 100\%$

Active basis choice: $|S| \leq 4\ (2\sqrt{2})$, click probability $= 50\%\ (82.8\%)$

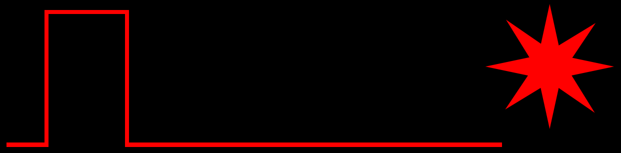
I. Gerhardt, Q. Liu *et al.*, Phys. Rev. Lett. **107**, 170404 (2011); S. Sajeed, N. Sultana *et al.*, arXiv:1902.03197

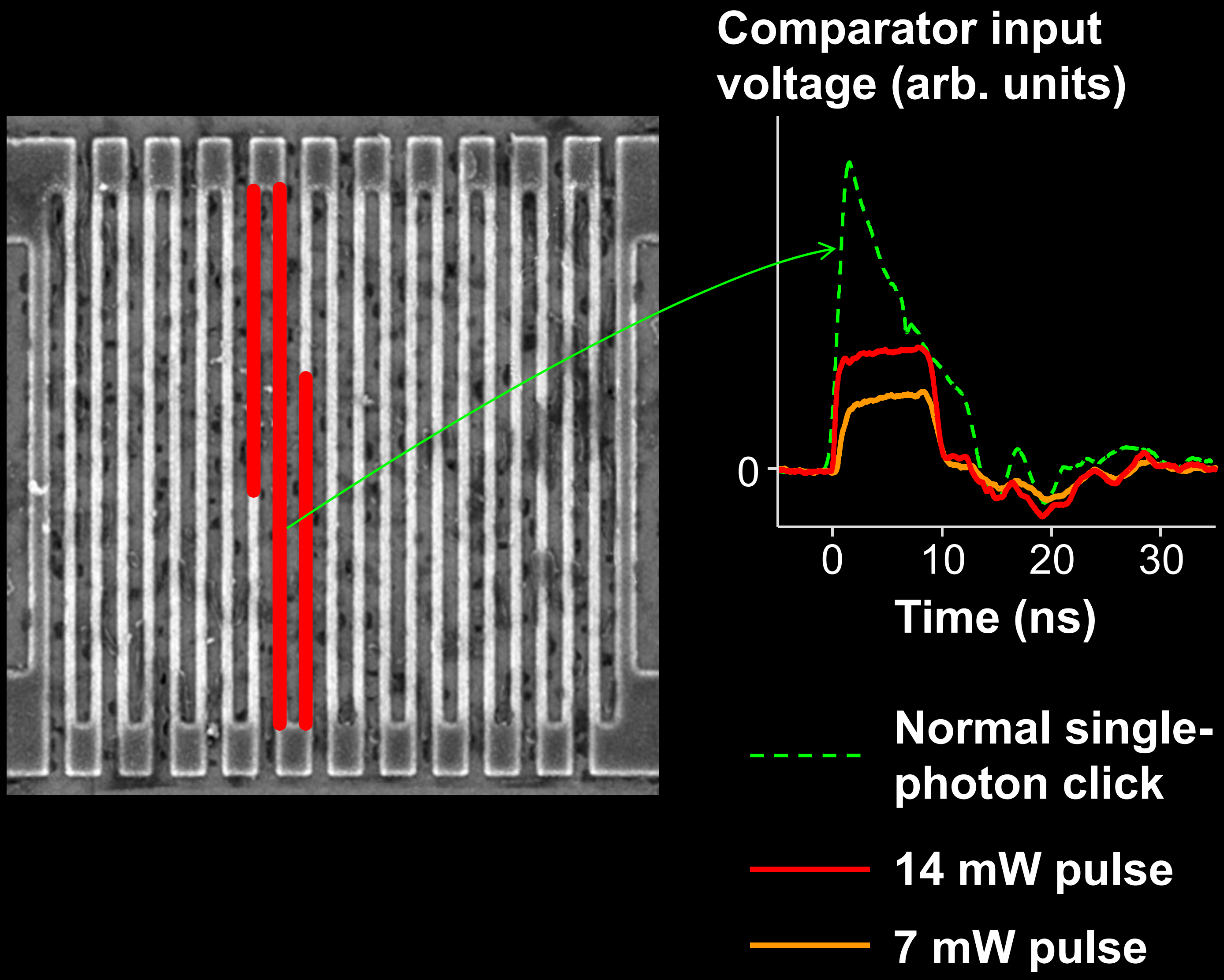
Controlling superconducting nanowire single-photon detectors

1. Blind (latch)



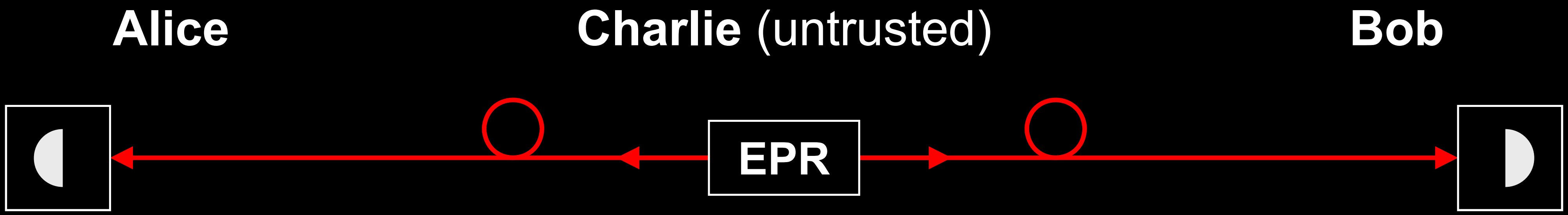
2. Control



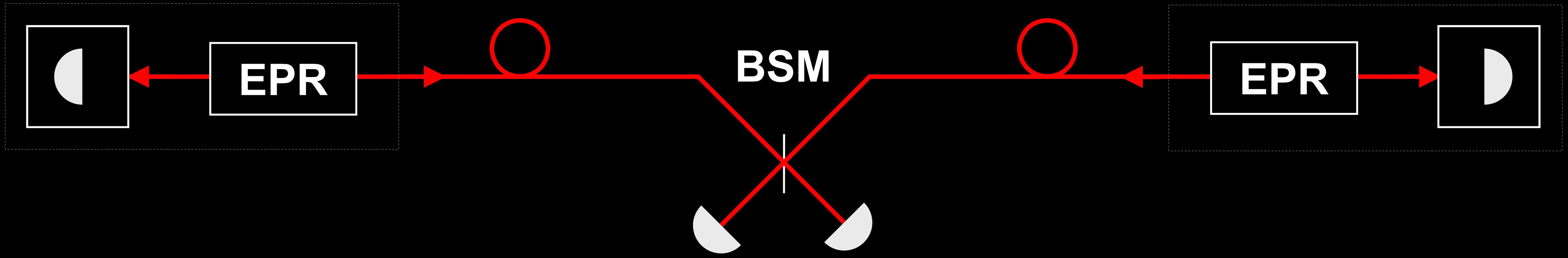

Comparator input voltage (arb. units)
0
0
10
20
30
Time (ns)
Normal single-photon click
14 mW pulse
7 mW pulse

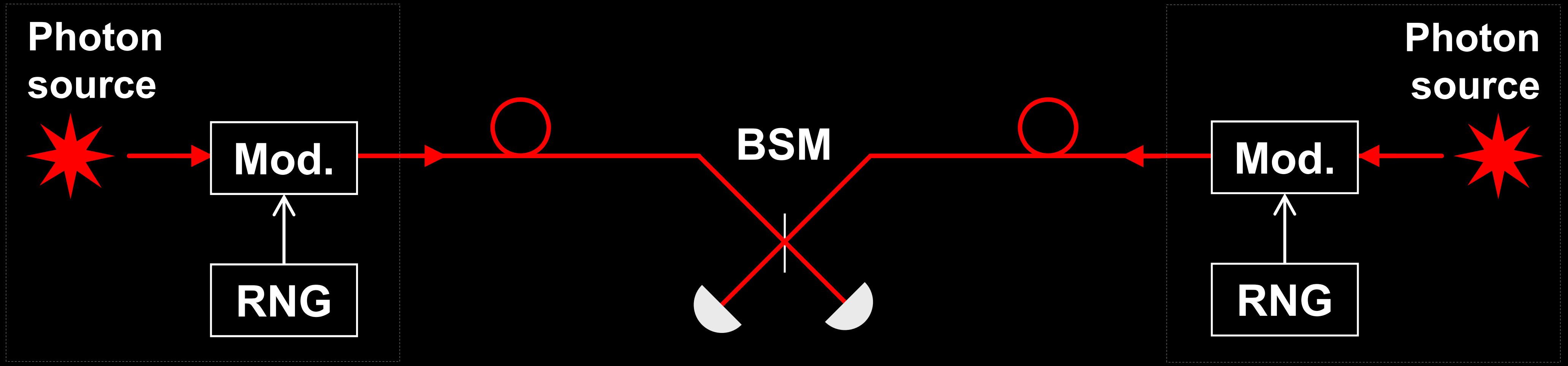
L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, V. Makarov, New J. Phys. **13**, 113042 (2011)
M. G. Tanner, V. Makarov, R. H. Hadfield, Opt. Express **22**, 6734 (2014)

Countermeasures to detector attacks?



A. Ekert, Phys. Rev. Lett. **67**, 661 (1991); C. Bennett *et al.*, Phys. Rev. Lett. **68**, 557 (1992)

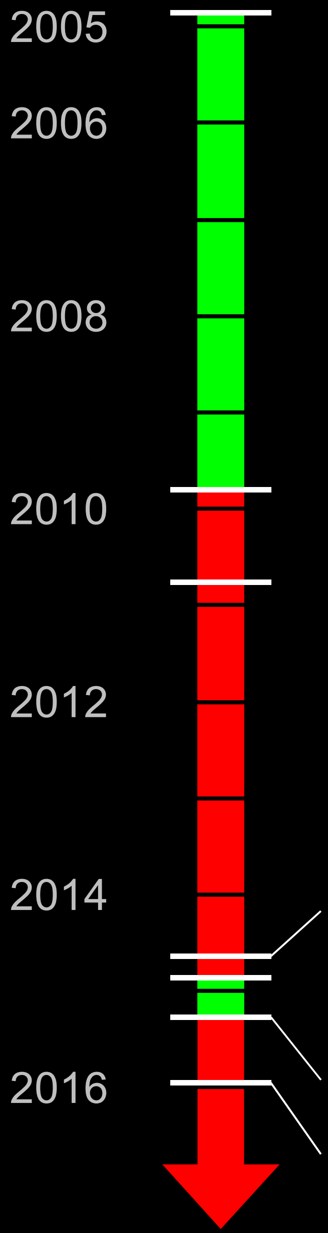




Measurement-device-independent QKD

H.-K. Lo, M. Curty, B. Qi, Phys. Rev. Lett. **108**, 130503 (2012)

Countermeasure for existing systems (ID Quantique)



First commercial Clavis1 system is shipped to a customer

🗡 Report about detector blinding attack sent to IDQ

IDQ applies for a patent on randomization of detector efficiency as a countermeasure

Lim *et al.* upload a preprint about countermeasure arXiv:1408.6398

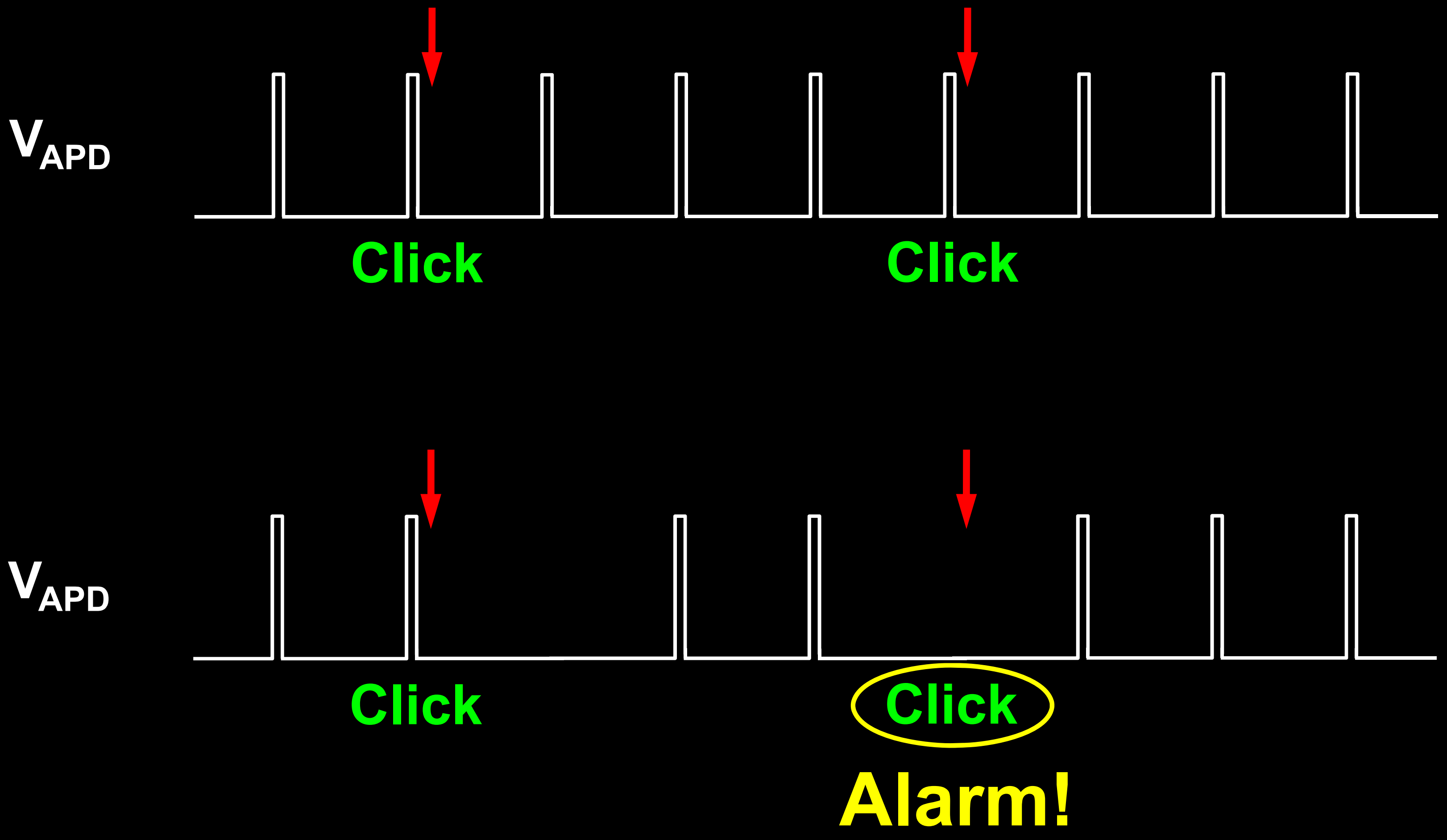
★ Implementation of countermeasure delivered by IDQ to our lab (firmware update for Clavis2)

🗡 Testing report sent to IDQ proposing a modified attack that works

🗡 Testing report sent to IDQ showing full implementation of countermeasure to be unreliable

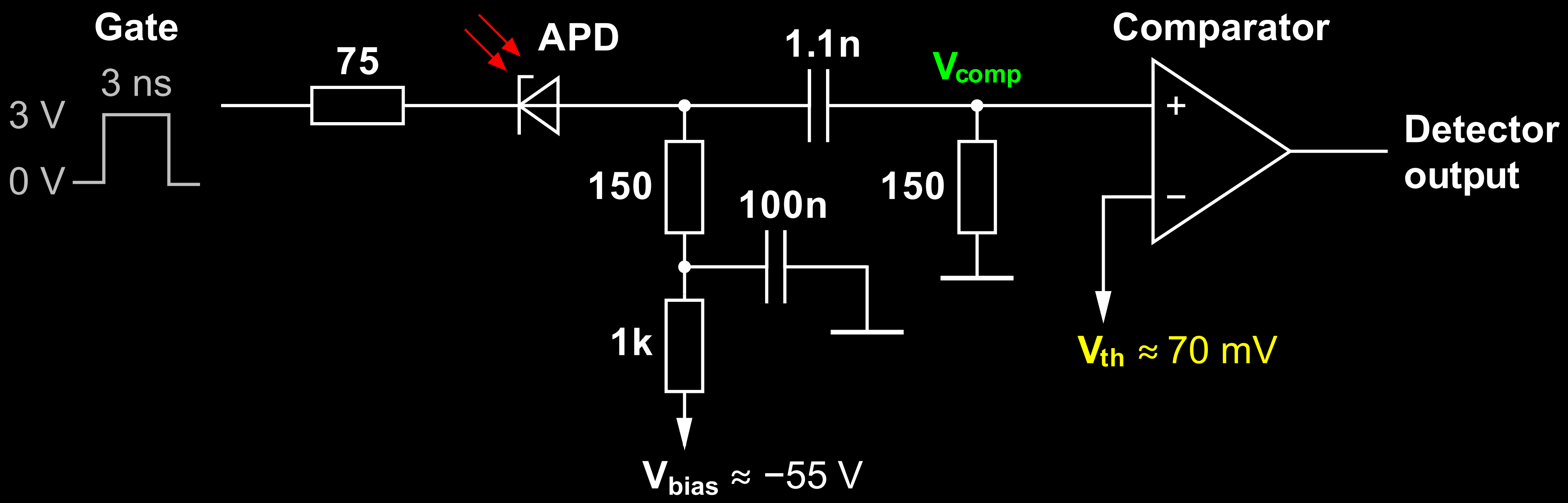
A. Huang *et al.*, IEEE J. Quantum Electron. **52**, 8000211 (2016)

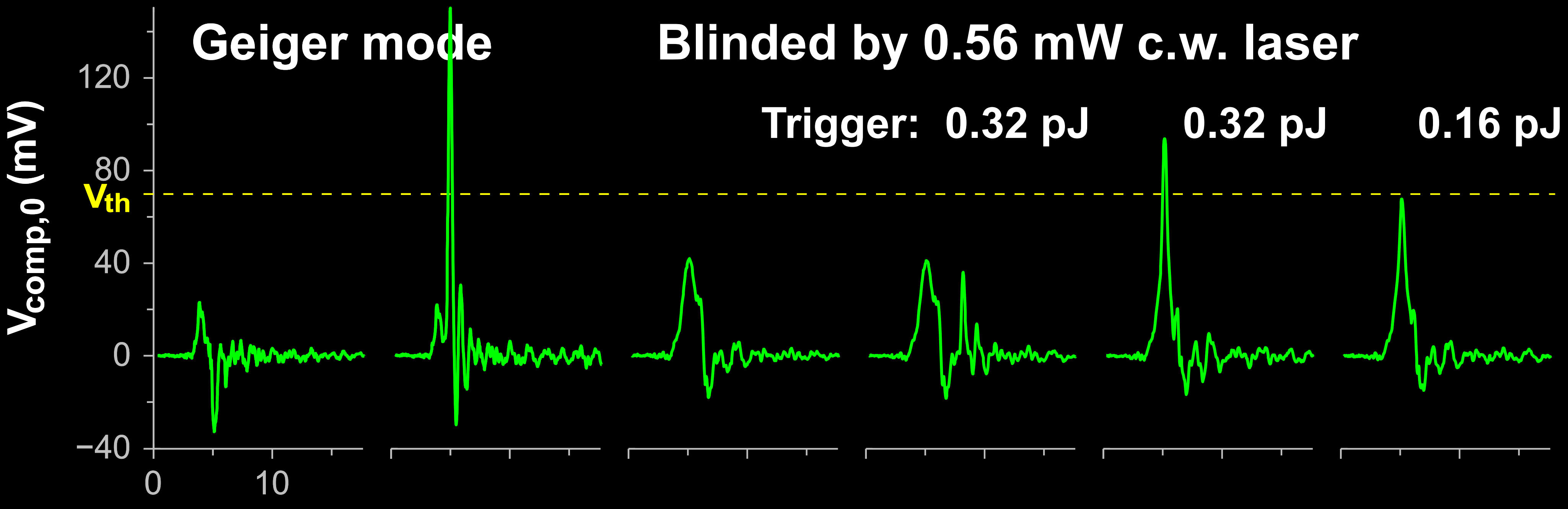
Randomly varying detector efficiency



M. Legre, G. Robordy, Intl. patent appl. WO 2012/046135 A2 (filed in 2010)

Oscillograms at comparator input





A. Huang *et al.*, IEEE J. Quantum Electron. **52**, 8000211 (2016)

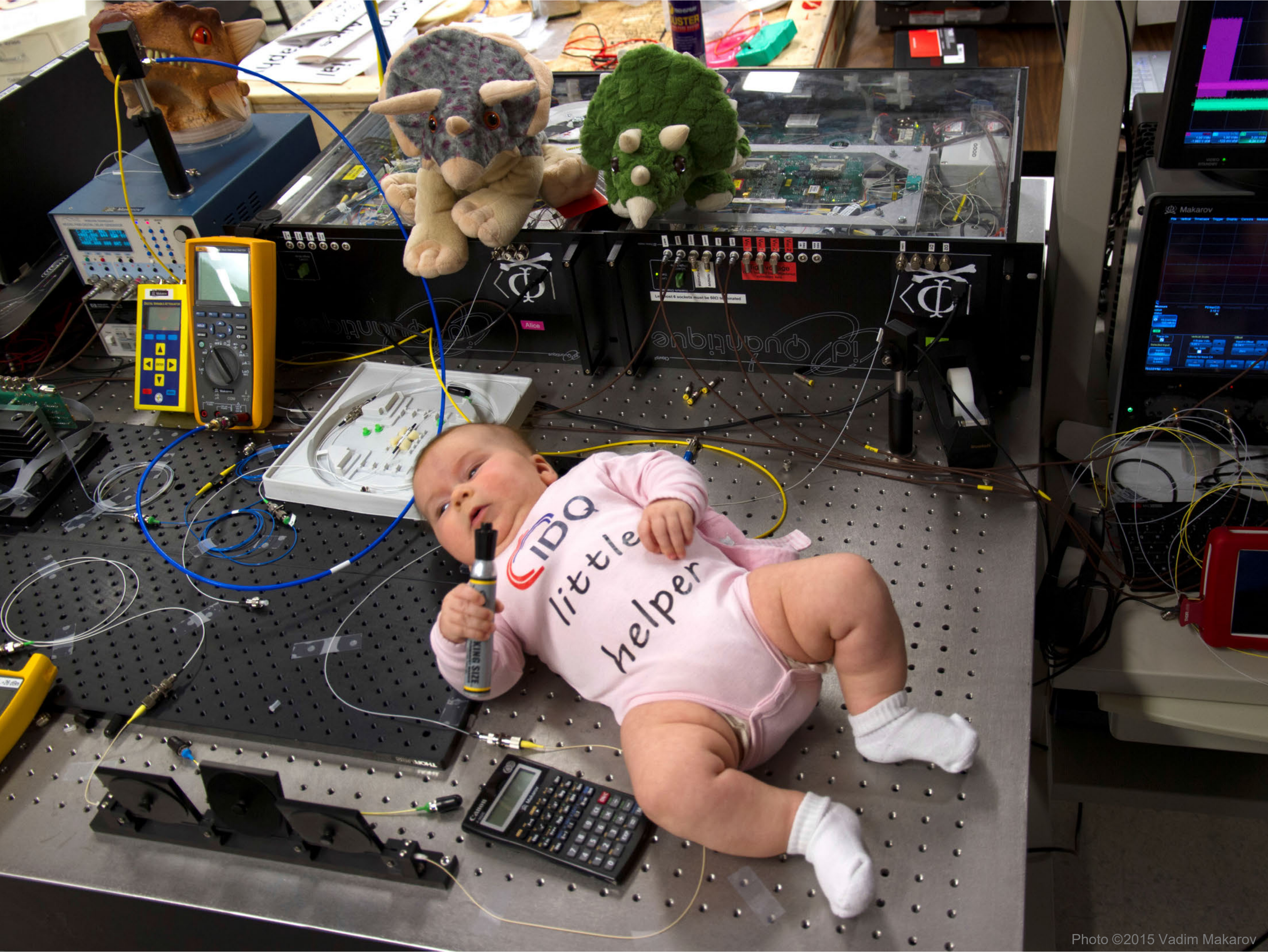


Photo ©2015 Vadim Makarov