Quantum hacking

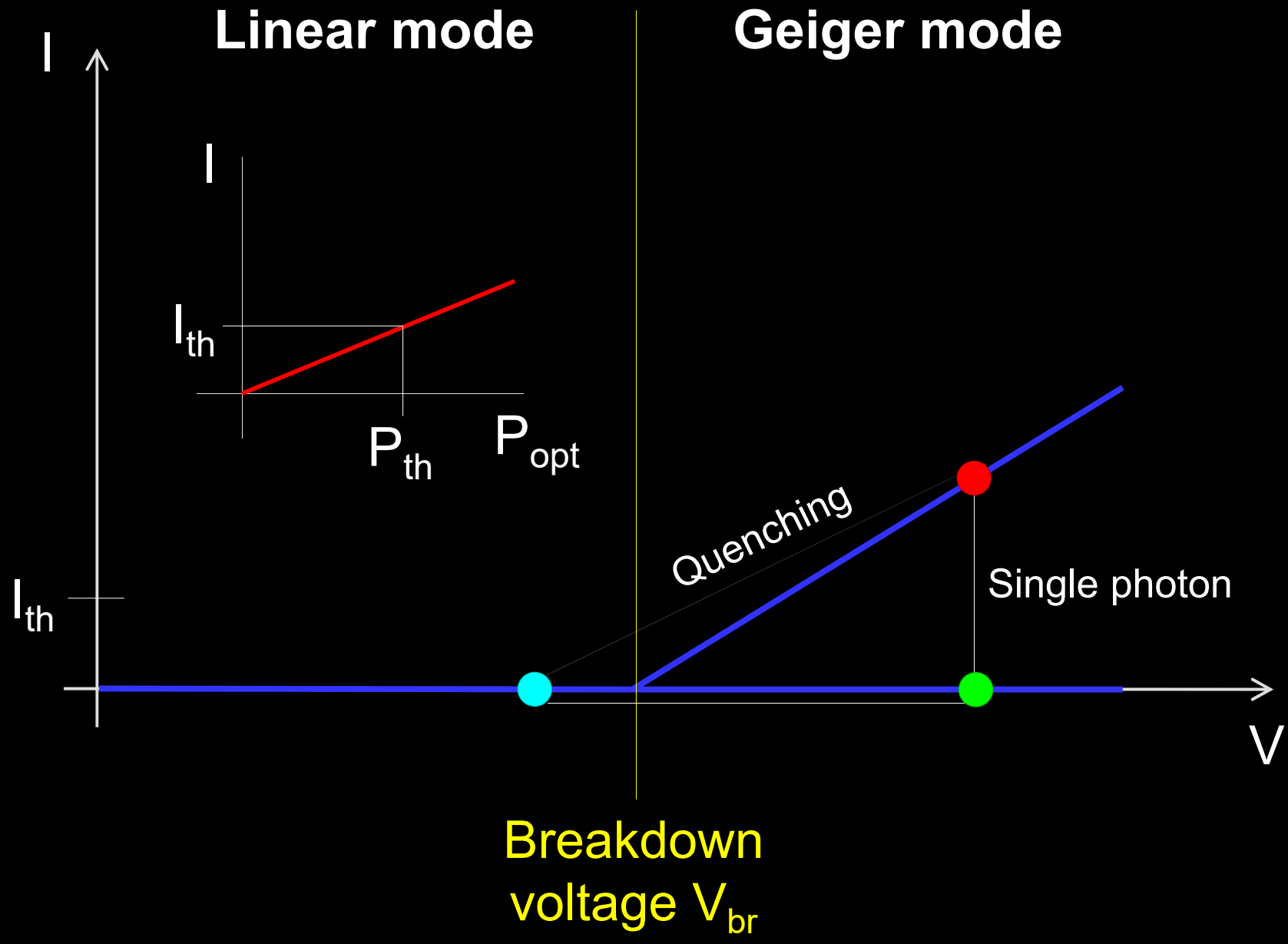
Vadim Makarov

RQC

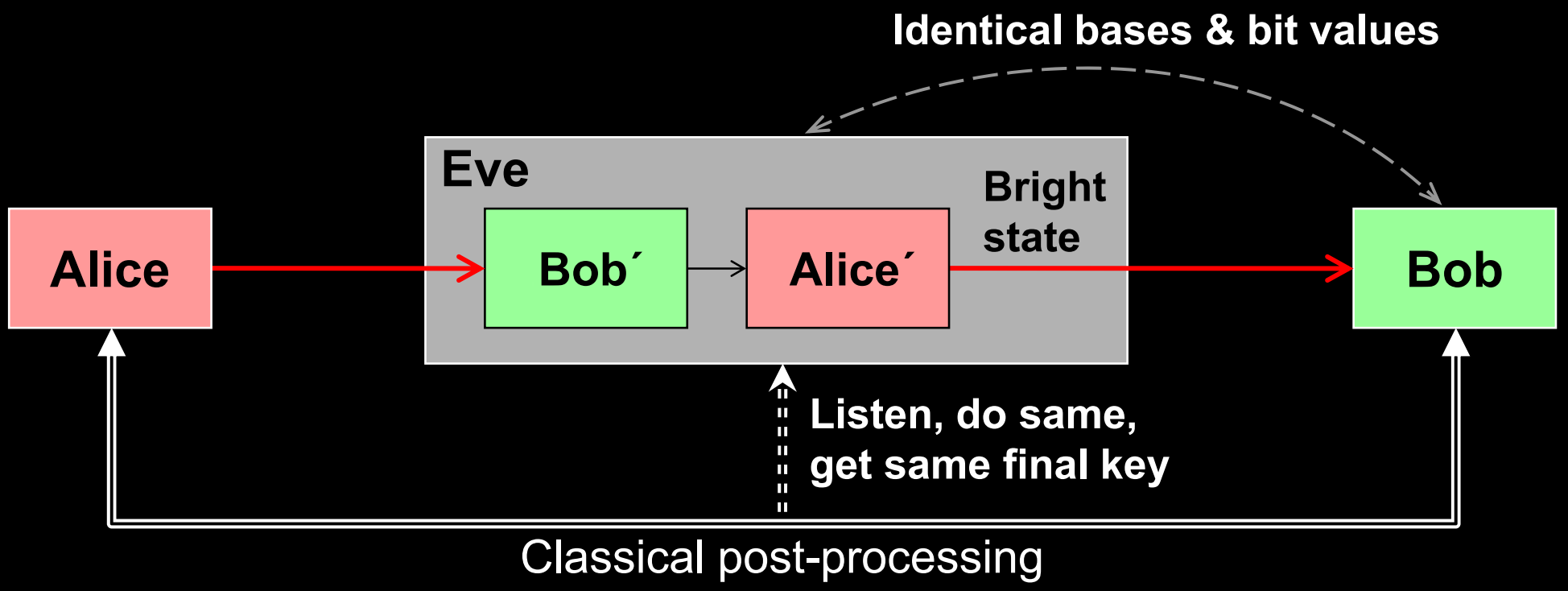
MISIS

vad1.com/lab

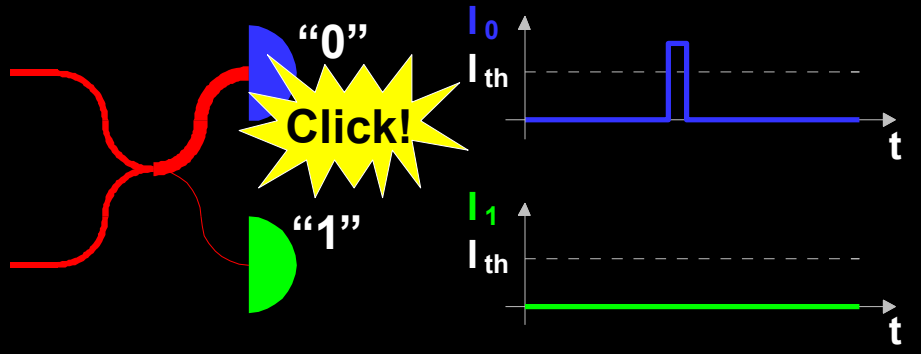
Attack example: avalanche photodetectors (APDs)



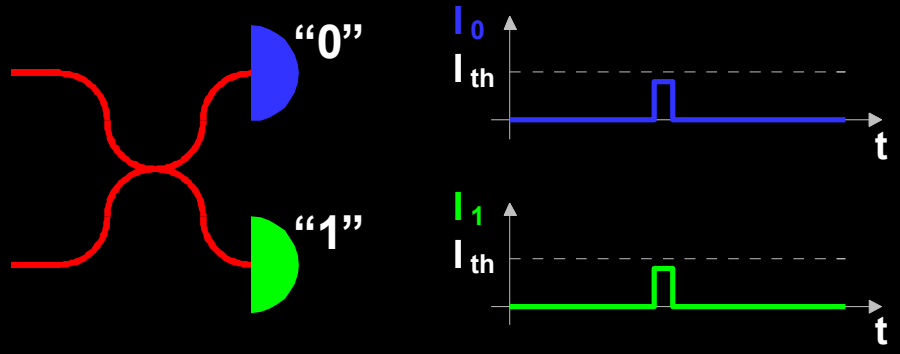
Faked-state attack in APD linear mode



Bob chooses same basis as Eve:

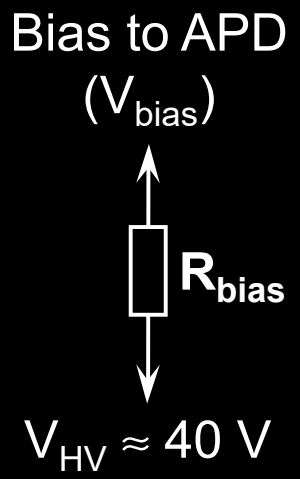


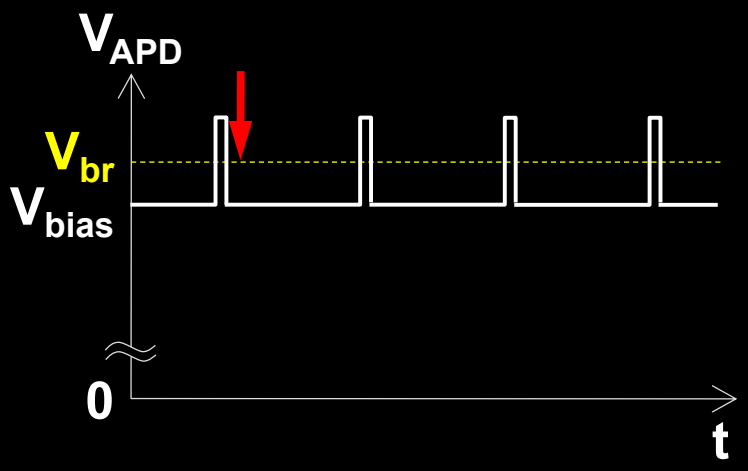
Bob chooses different basis:



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

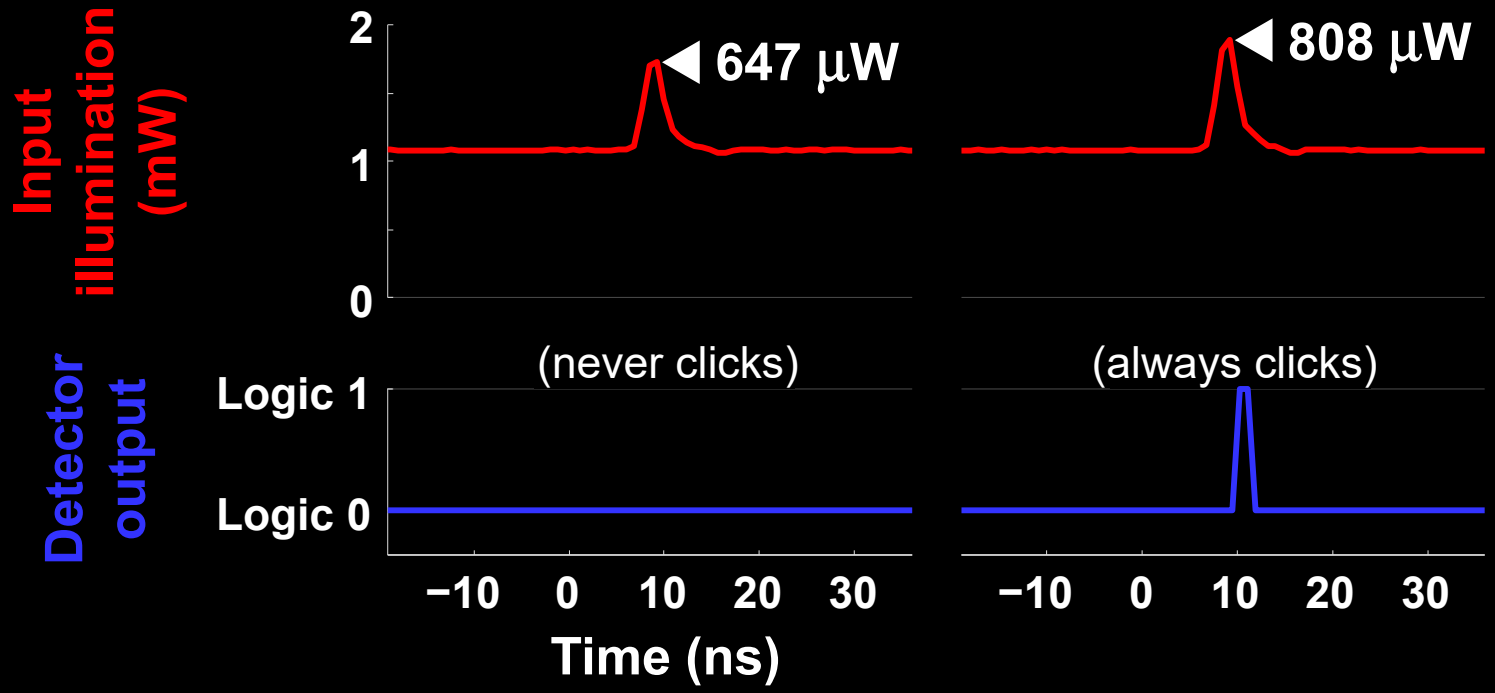
Blinding APD with bright light





Eve applies CW light

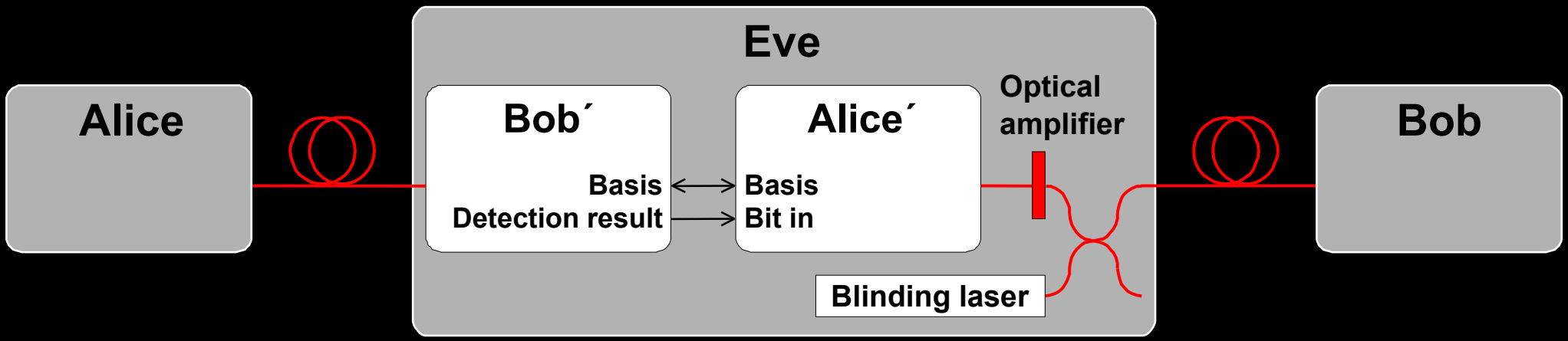
Detector blind!
Zero dark count rate



ID Quantique
Clavis2

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

Proposed full eavesdropper

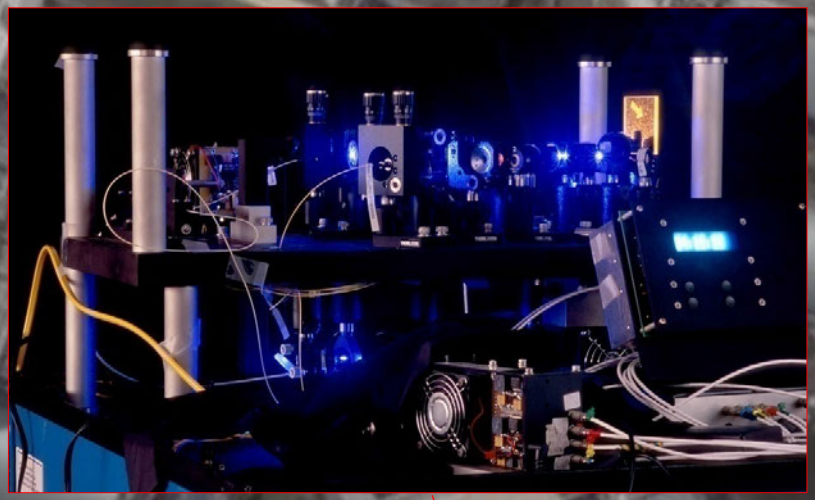


Note: Intercept-resend always breaks QKD security

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



290 m of fiber

Eve

Alice

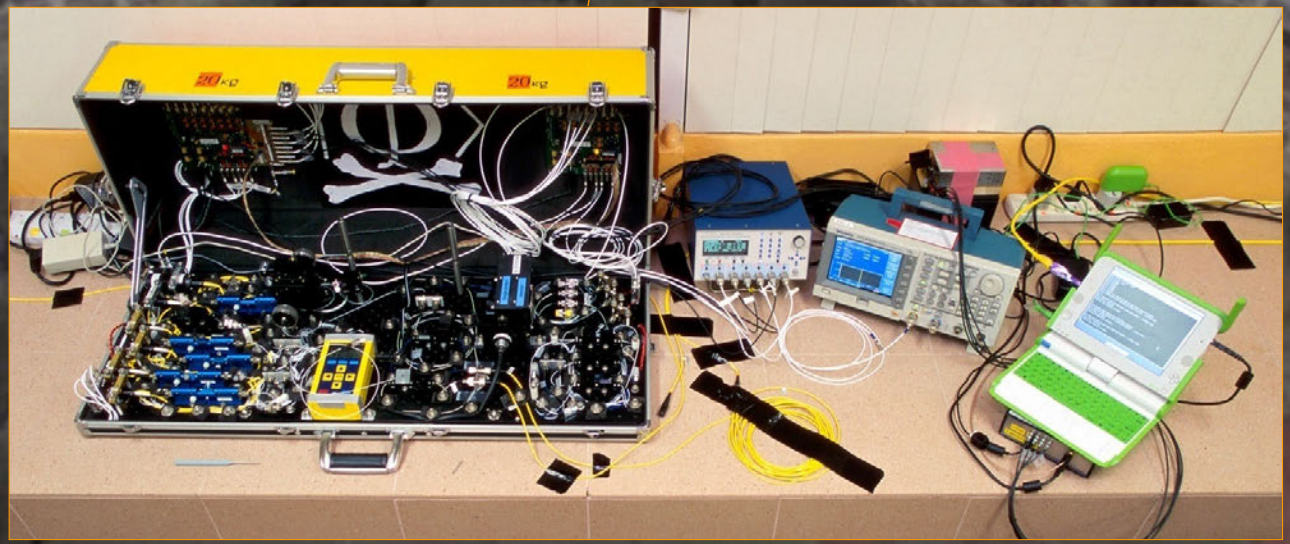
Bob

S15

S14

S13

S12

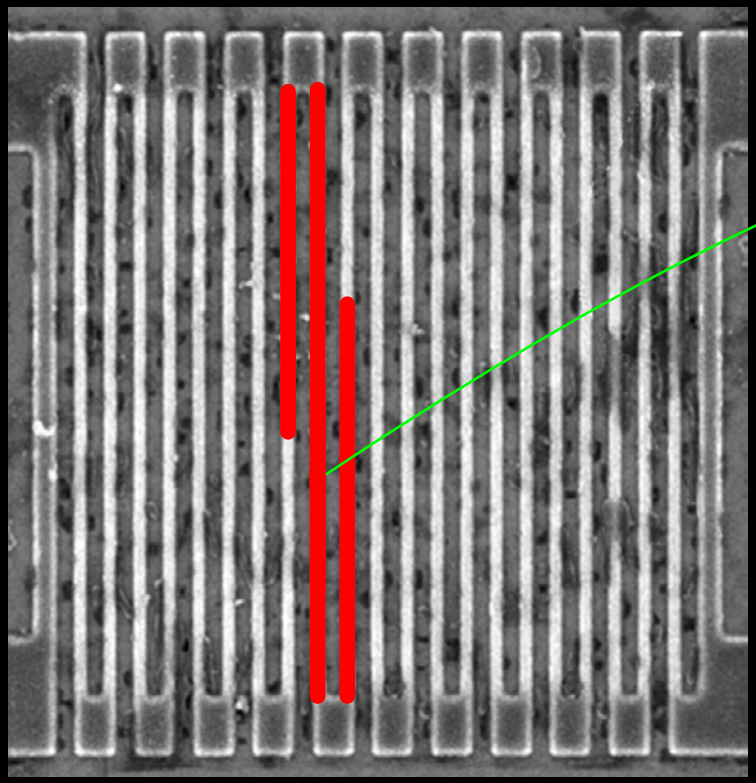


I. Gerhardt, Q. Liu *et al.*,
Nat. Commun. **2**, 349 (2011)

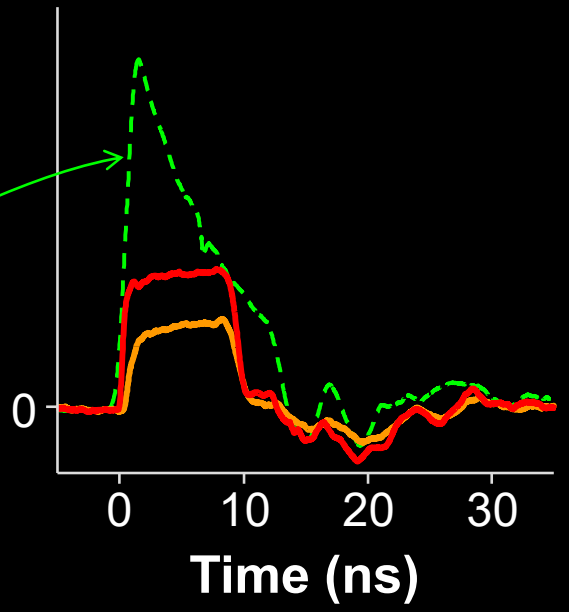
Controlling superconducting nanowire single-photon detectors

1. Blind (latch)

2. Control



Comparator input voltage (arb. units)



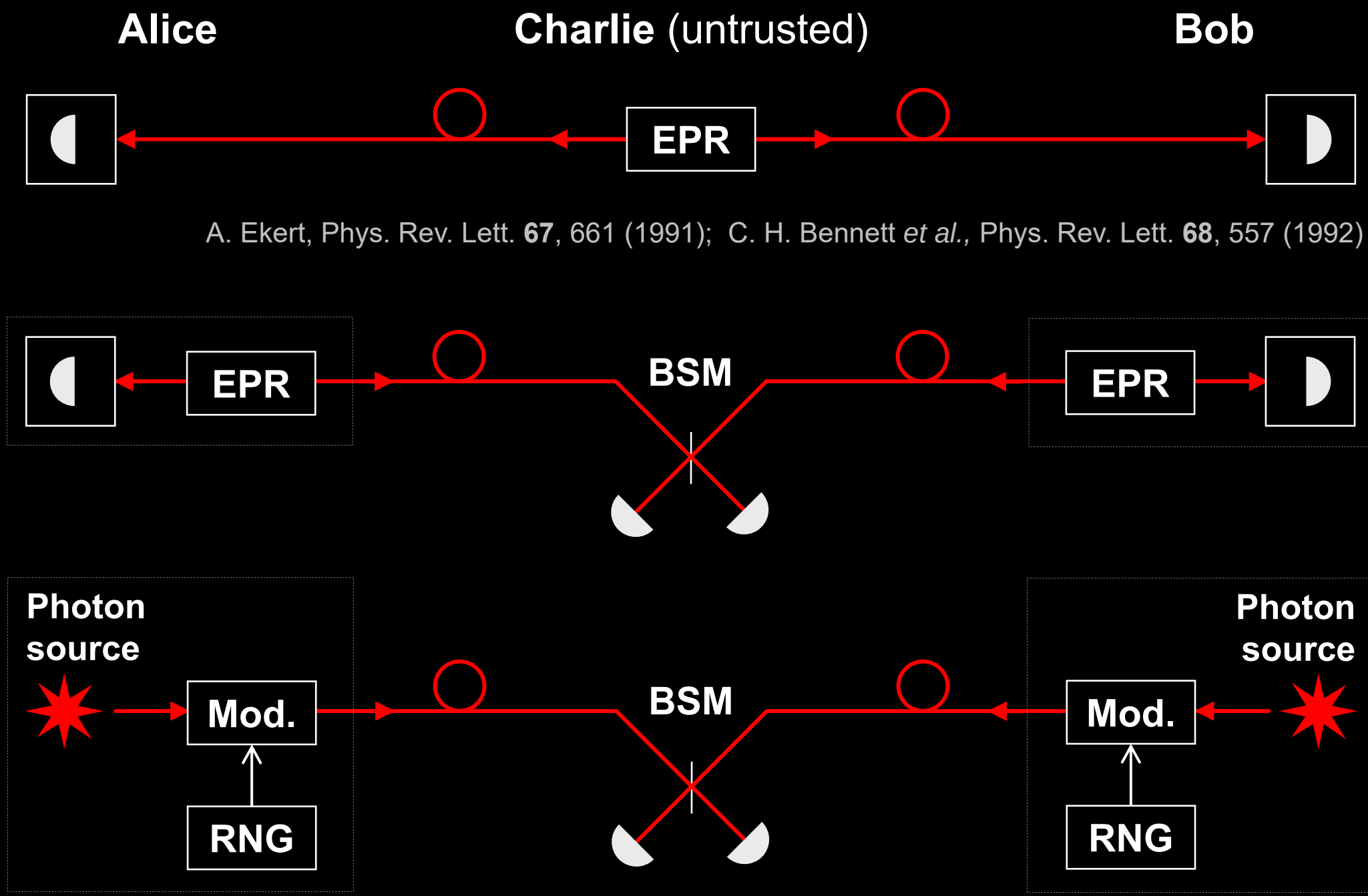
Normal single-photon click

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. H. 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)