

Detector control attack

Vadim Makarov

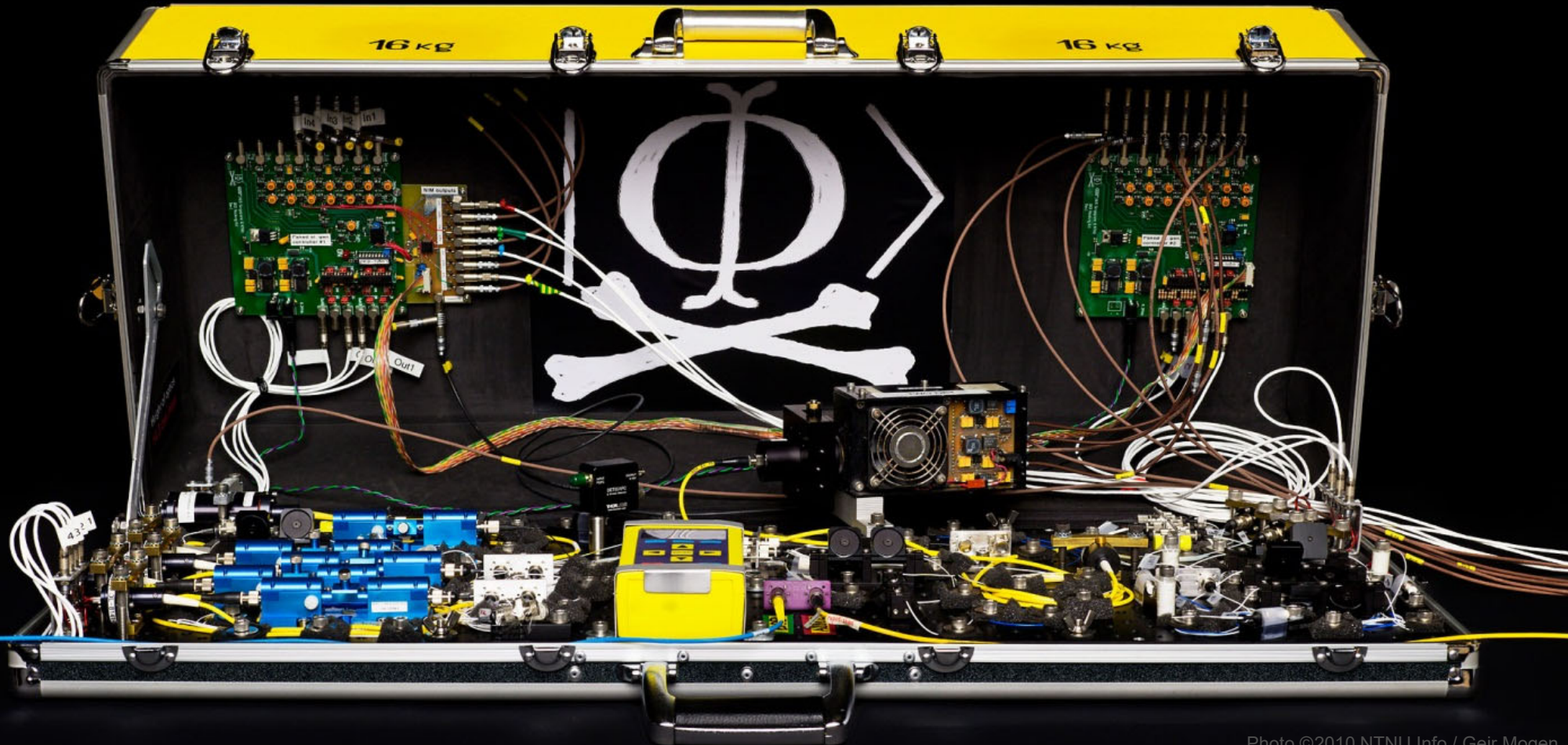


RQC

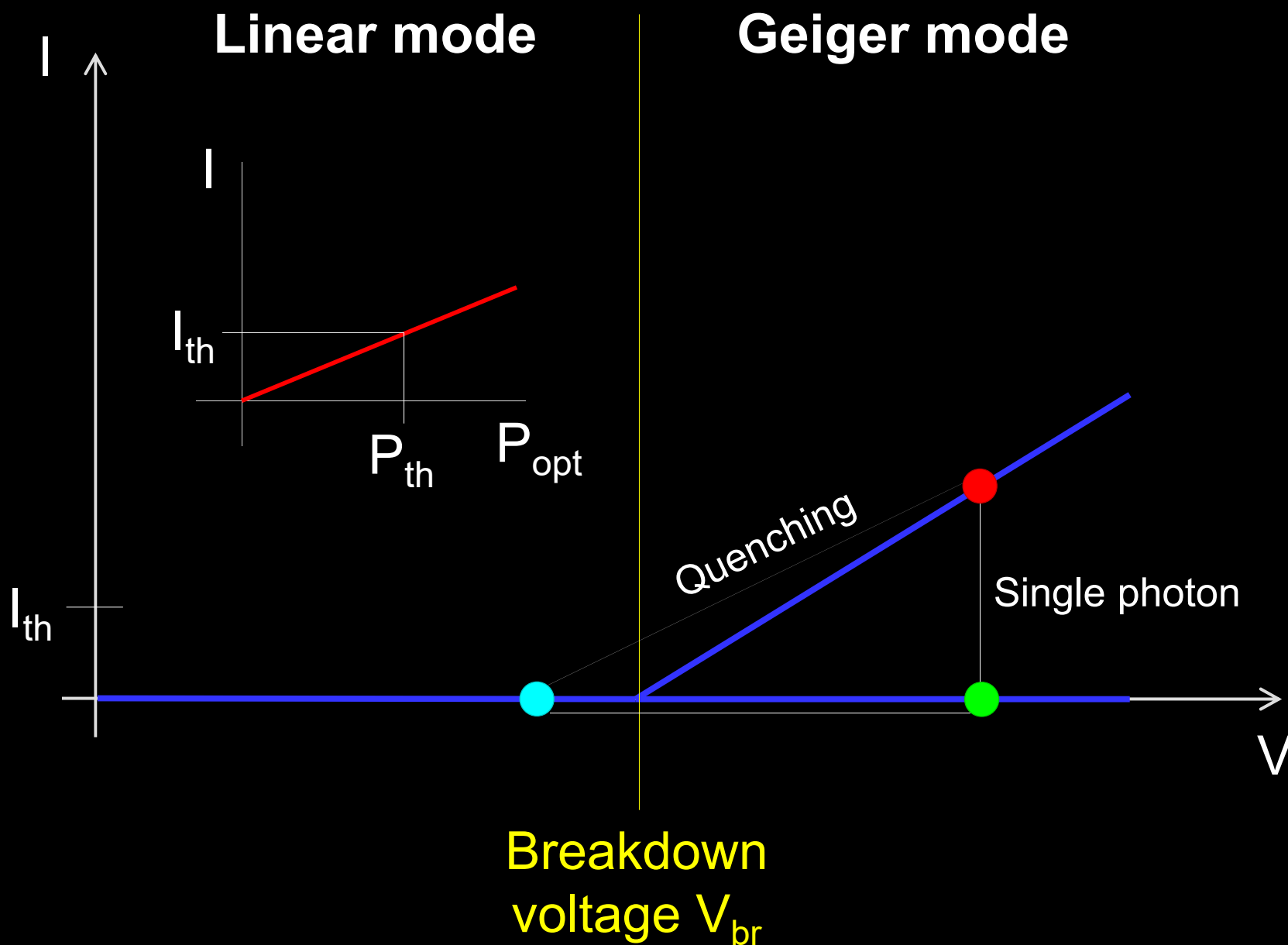


MISIS

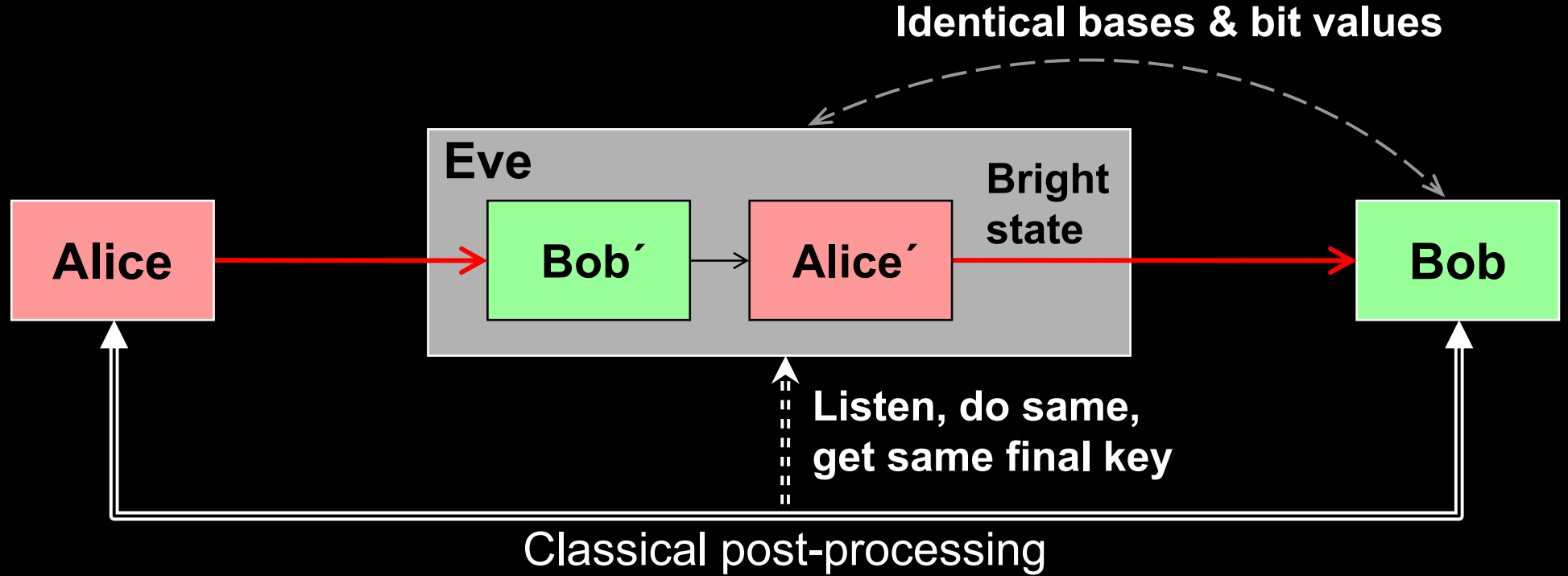
vad1.com/lab



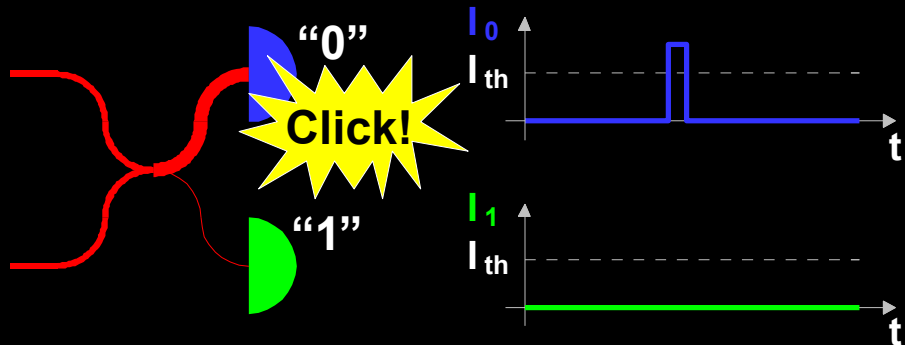
Attack example: avalanche photodetectors (APDs)



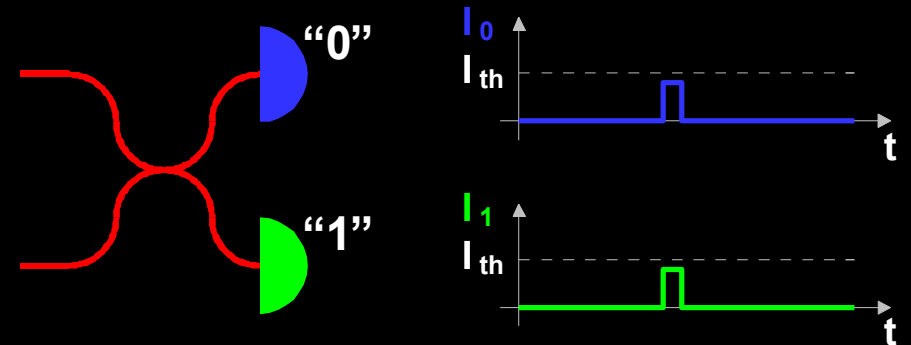
Faked-state attack in APD linear mode



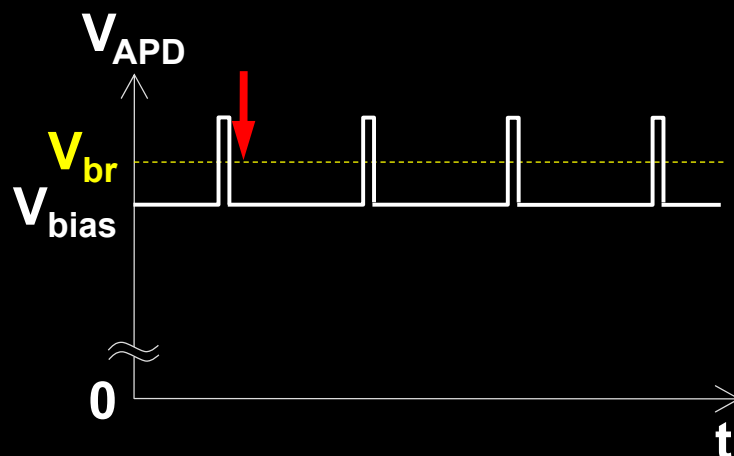
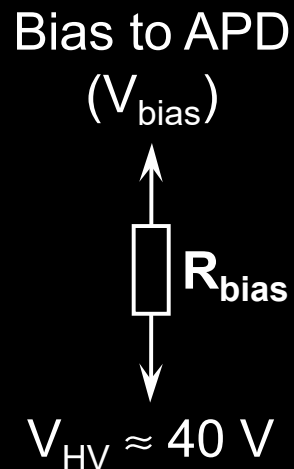
Bob chooses same basis as Eve:



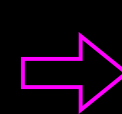
Bob chooses different basis:



Blinding APD with bright light

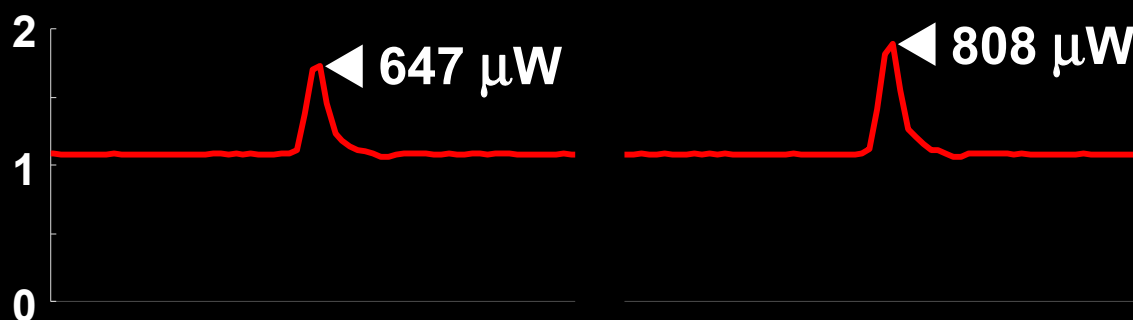


Eve applies CW light

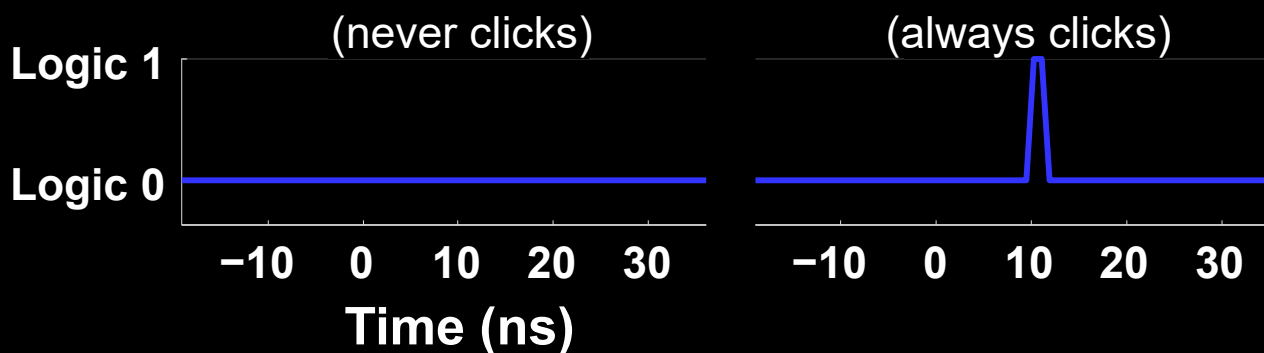


Detector blind!
Zero dark count rate

Input illumination (mW)

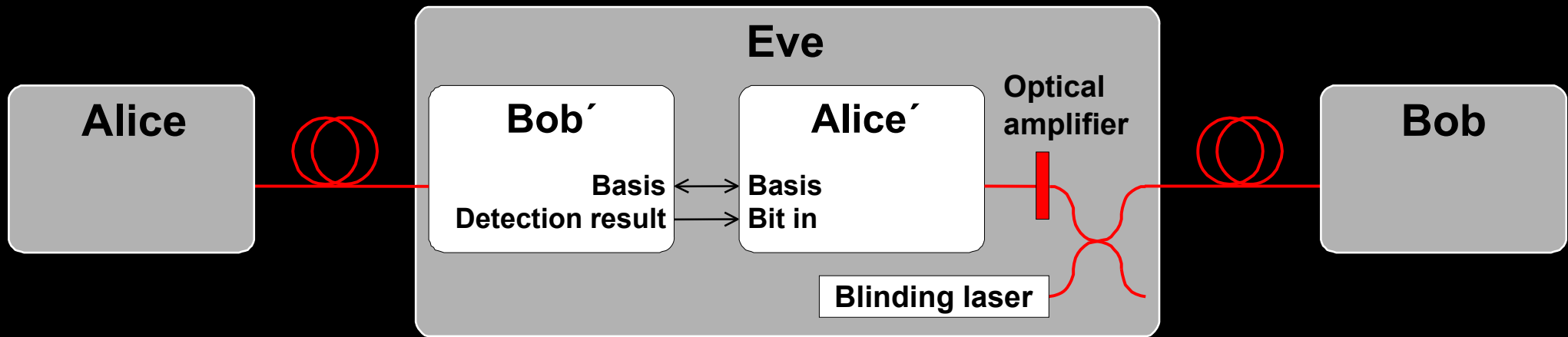


Detector output



ID Quantique
Clavis2

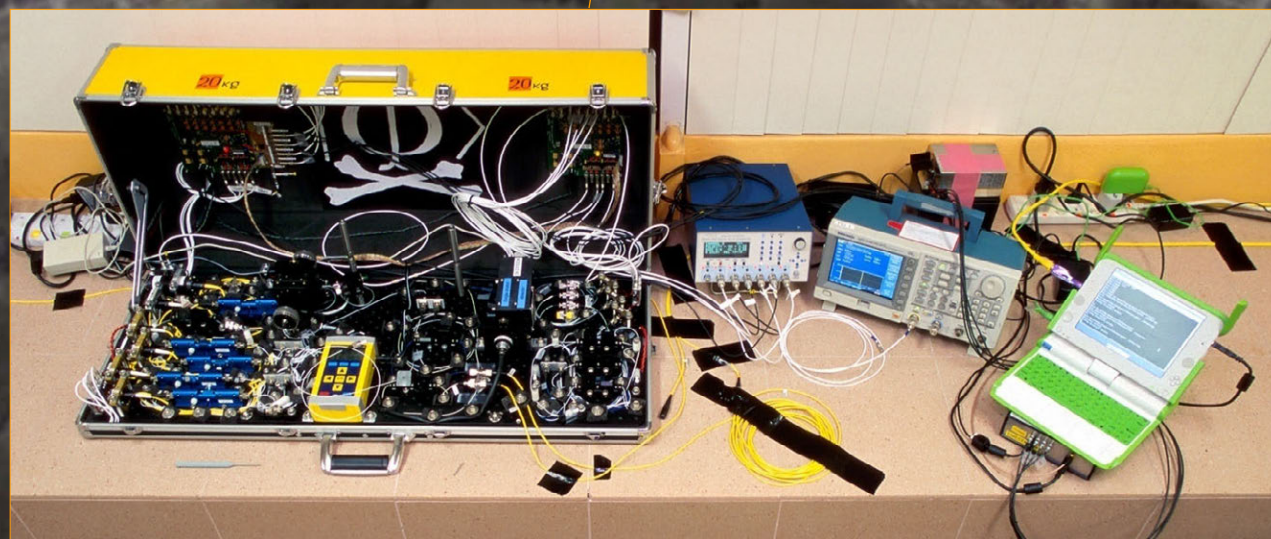
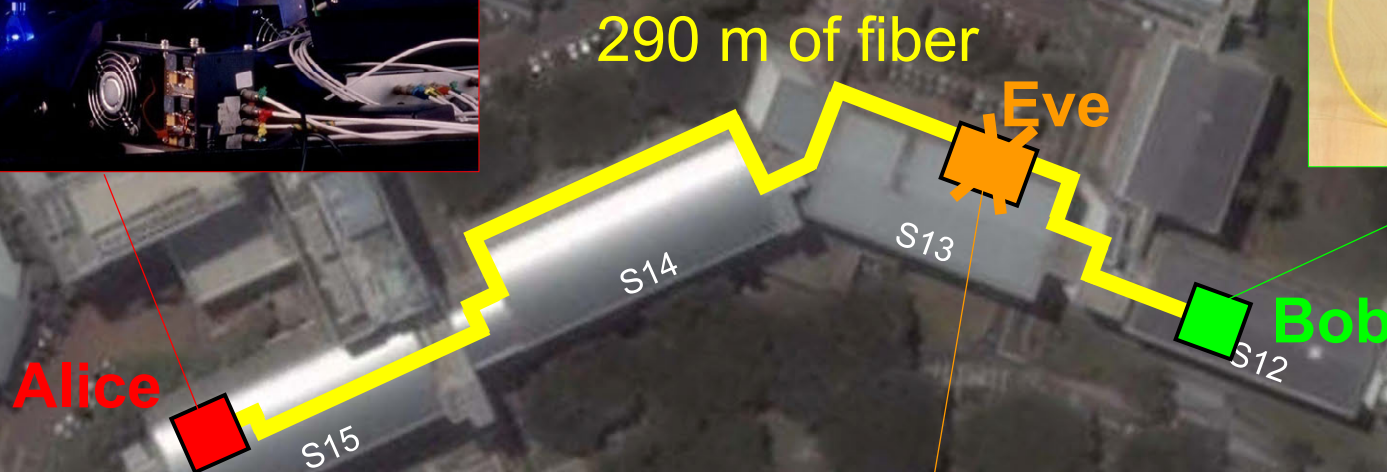
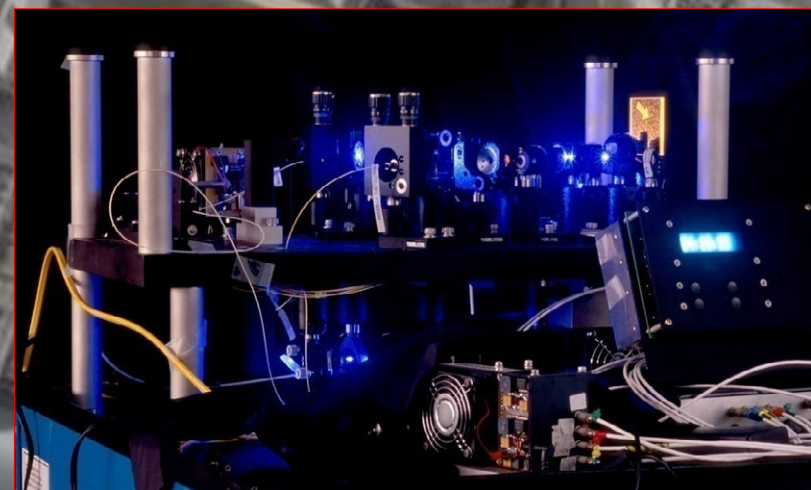
Proposed full eavesdropper



Note: Intercept-resend always breaks QKD security

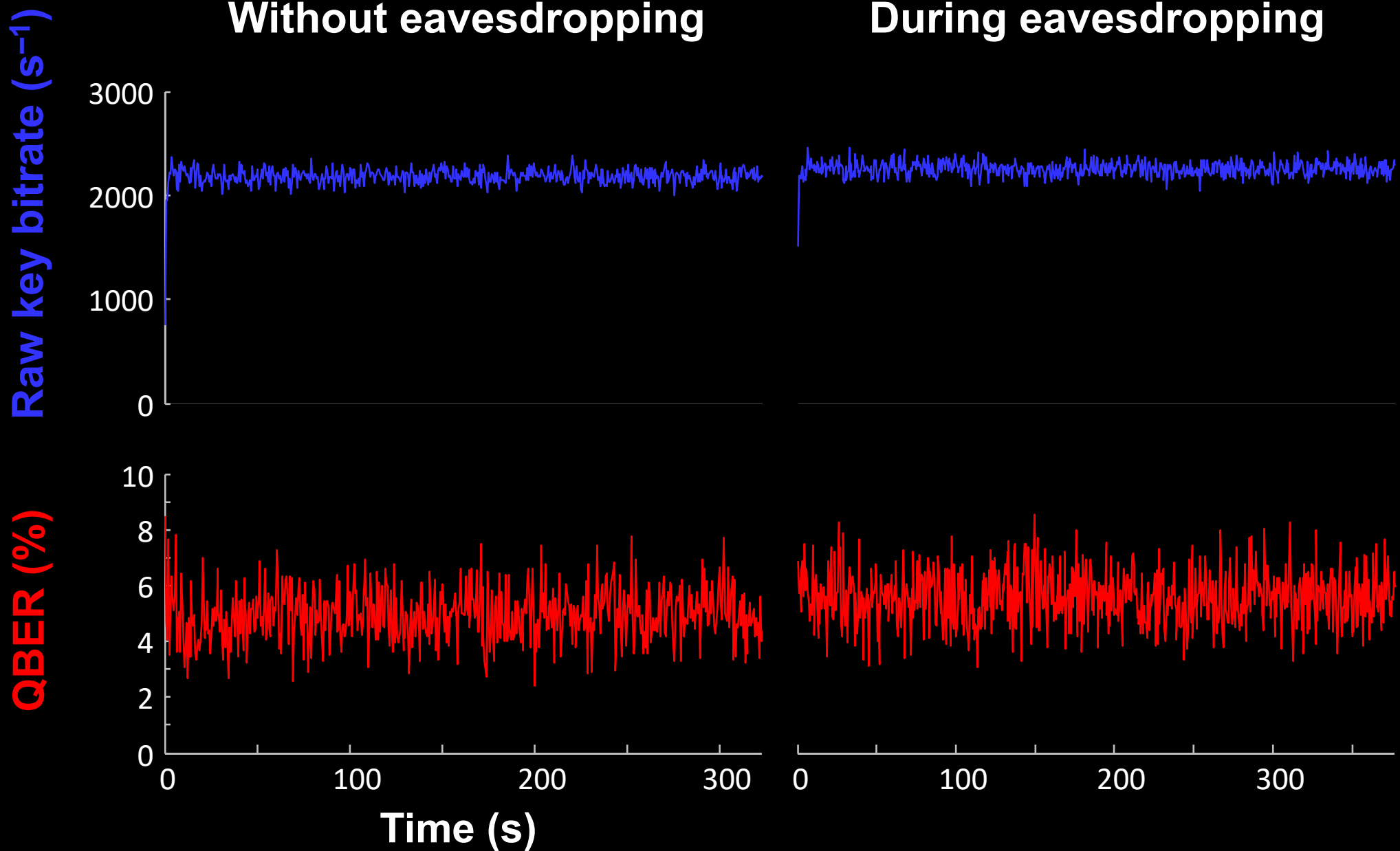
Eavesdropping 100% key on installed QKD line

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



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

Eve does not affect QKD performance

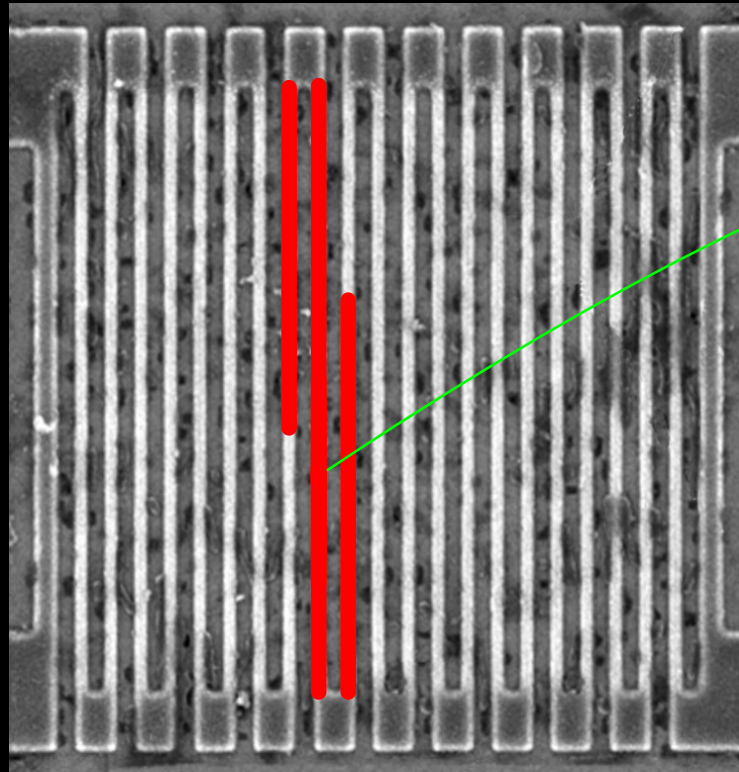


Controlling superconducting nanowire single-photon detectors

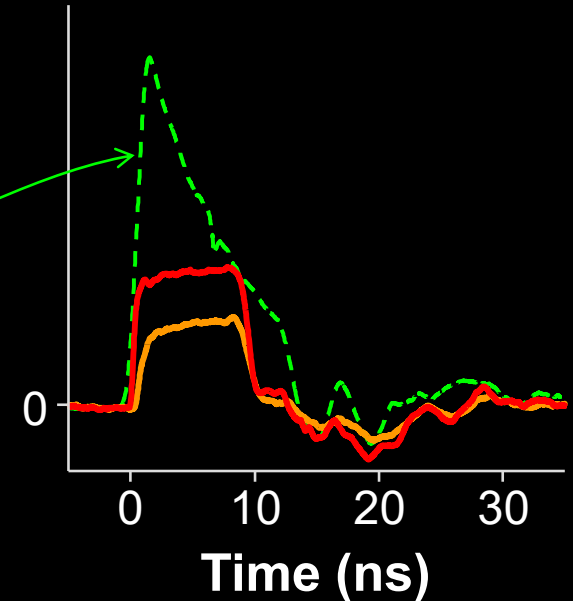
1. Blind (latch)



2. Control



Comparator input
voltage (arb. units)

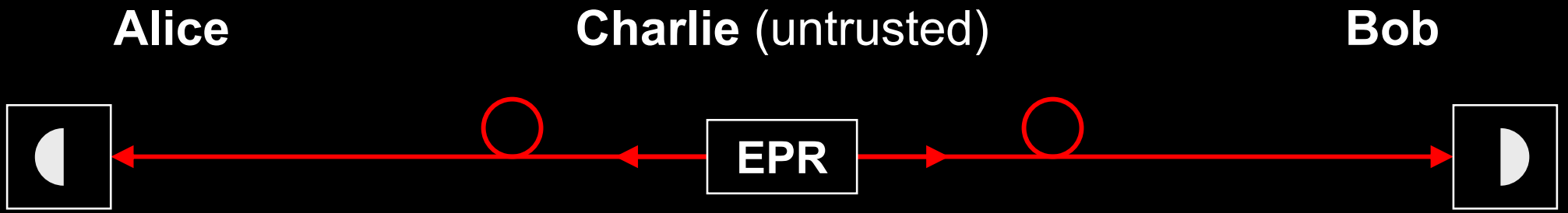


Normal single-photon click

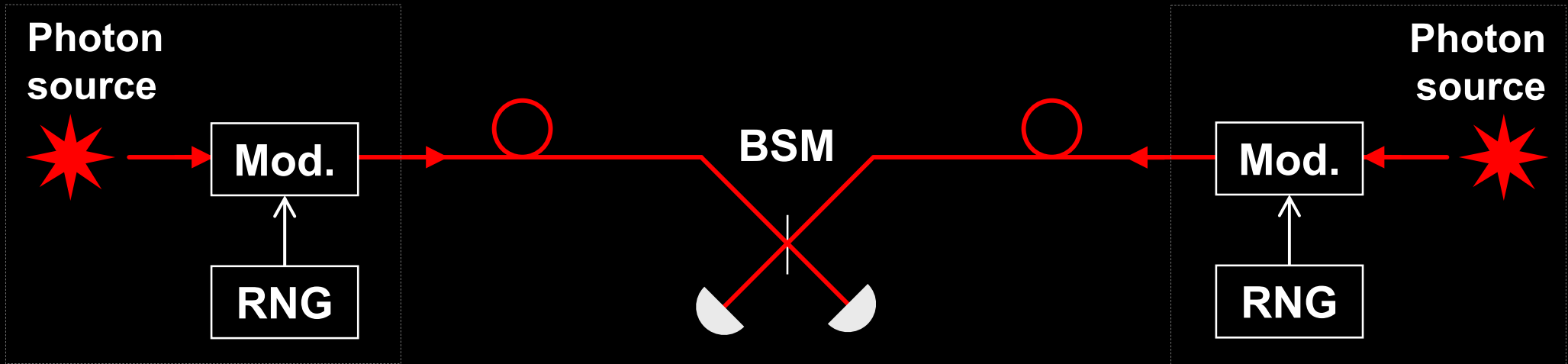
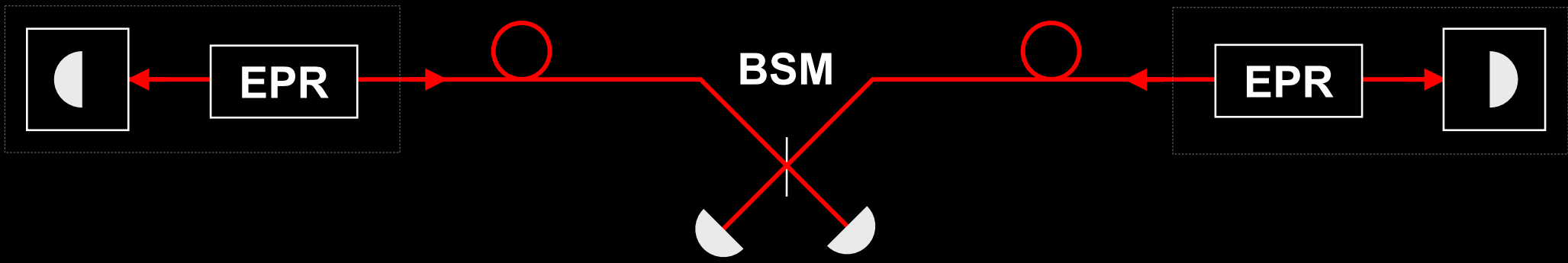
14 mW pulse

7 mW pulse

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)