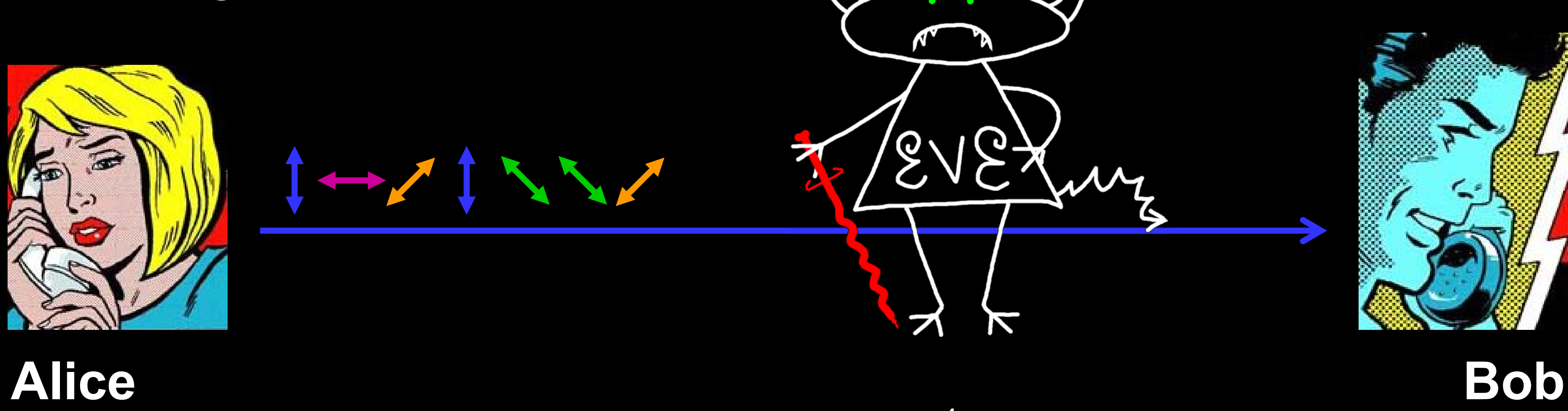
Loopholes in implementations

Vadim Makarov

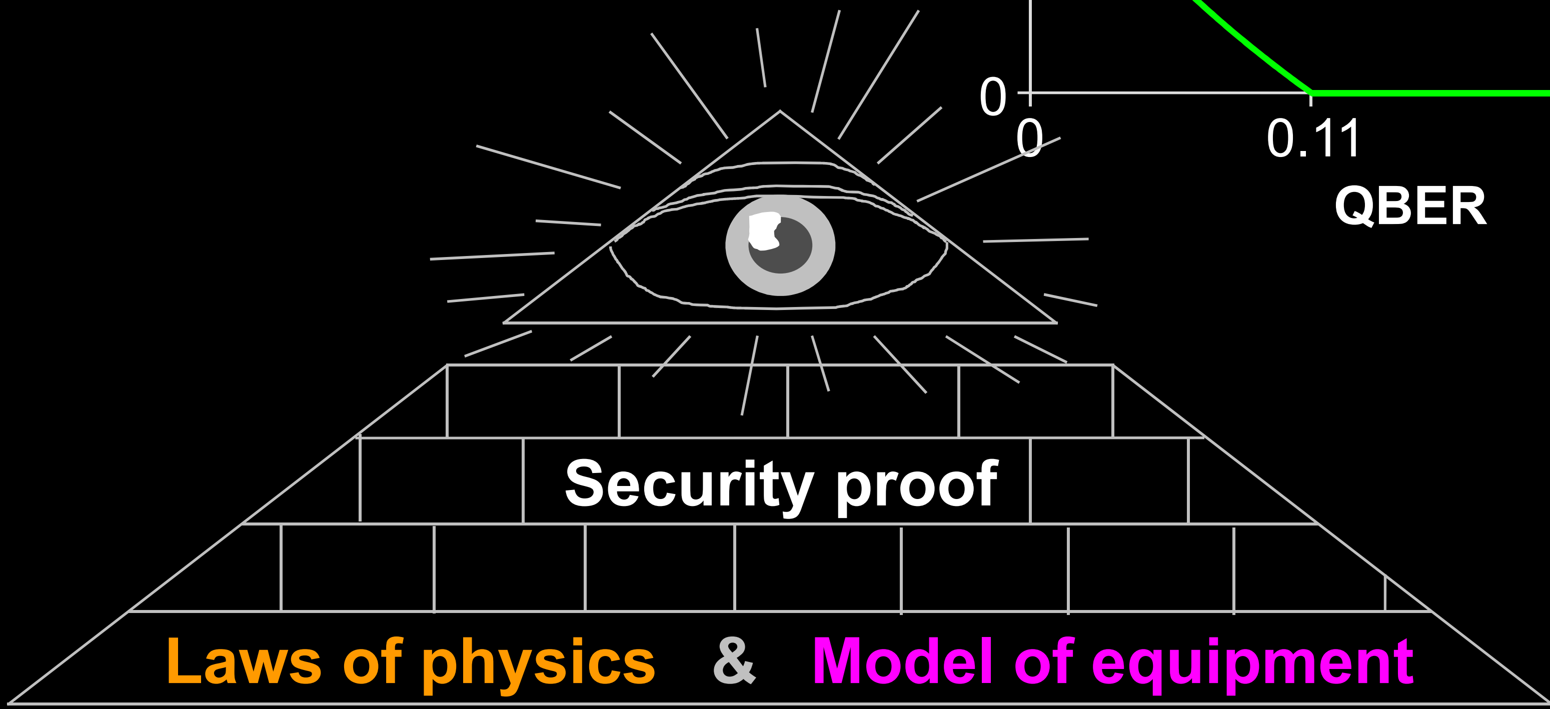
IQC Institute *for* Quantum Computing

Photo ©2010 NTNU Info / Geir Mogen

Security model of QKD



Secret key rate $R = f(\mathrm{QBER})$



Stages of secure technology

Quantum cryptography

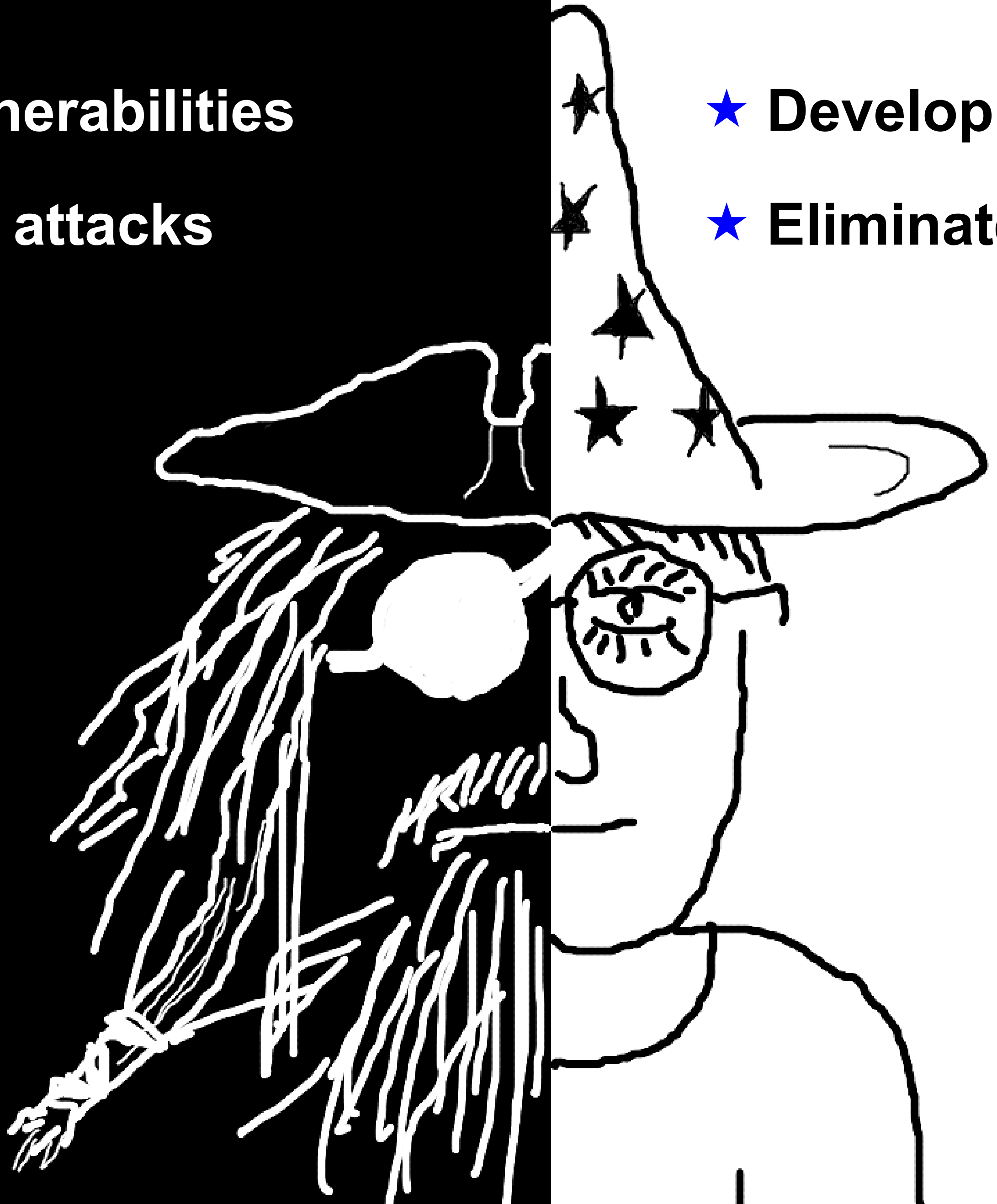
1. Idea / theory / proof-of-the-principle — 1970–1993
2. Initial implementations — 1994–2005
3. Weeding out implementation loopholes — ◄ Now!

   (spectacular failures ⇄ patching)
4. Good for wide use

Quantum hacking

- Discover vulnerabilities
- Demonstrate attacks

- Develop countermeasures
- Eliminate imperfections



Commercial QKD

ID Quantique *Cerberis* system

Classical encryptors:

L2, 2 Gbit/s

L2, 10 Gbit/s

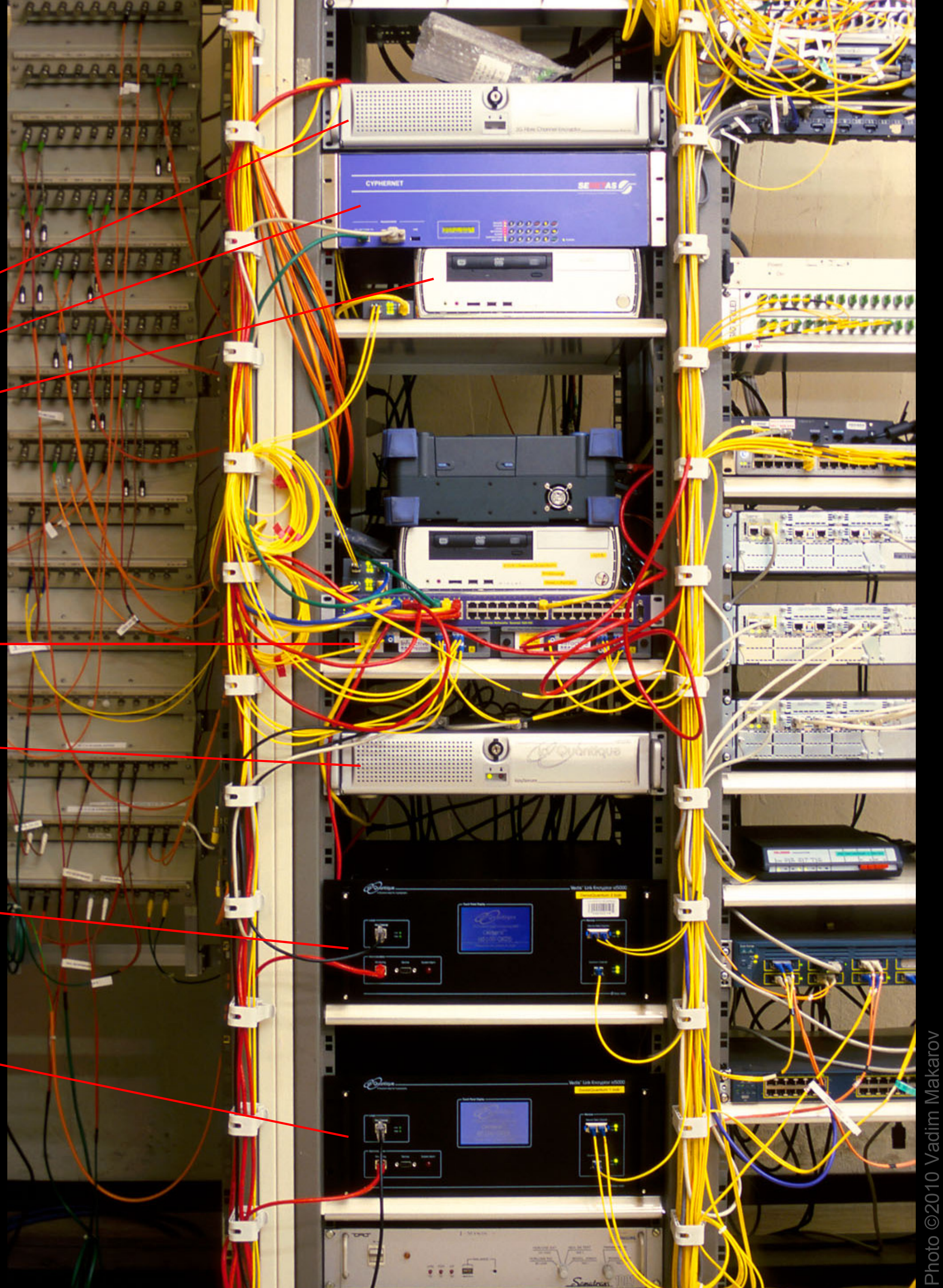
L3 VPN, 100 Mbit/s

WDMs

Key manager

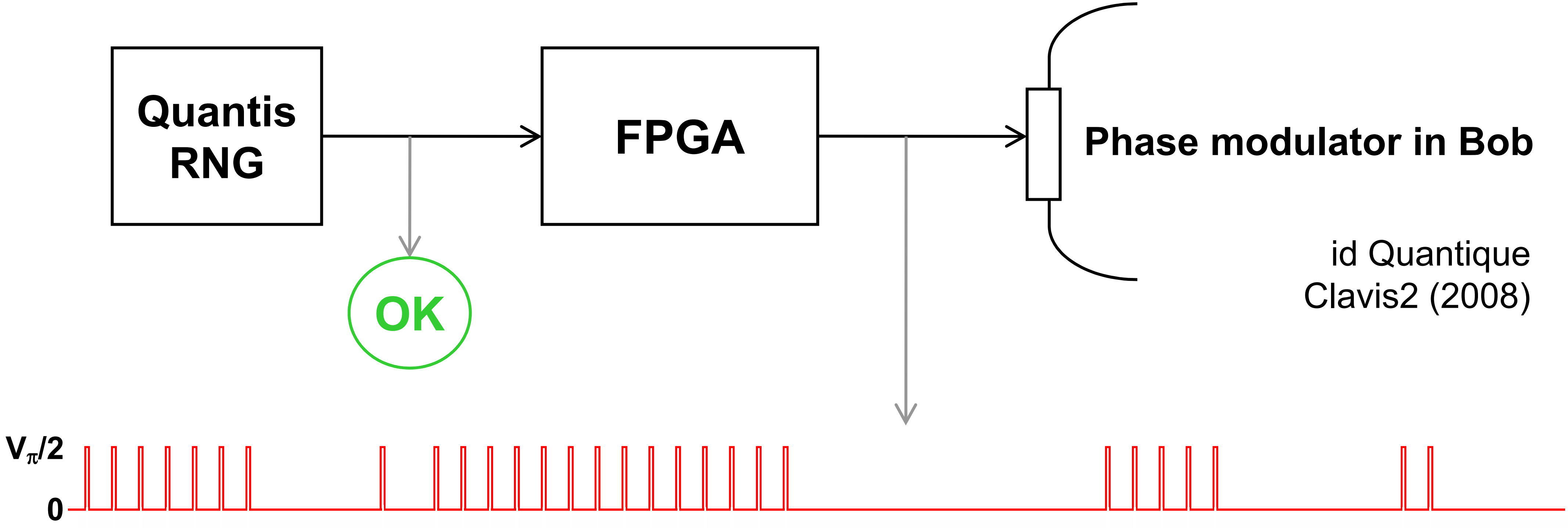
QKD to another node (3 km)

QKD to another node (17 km)

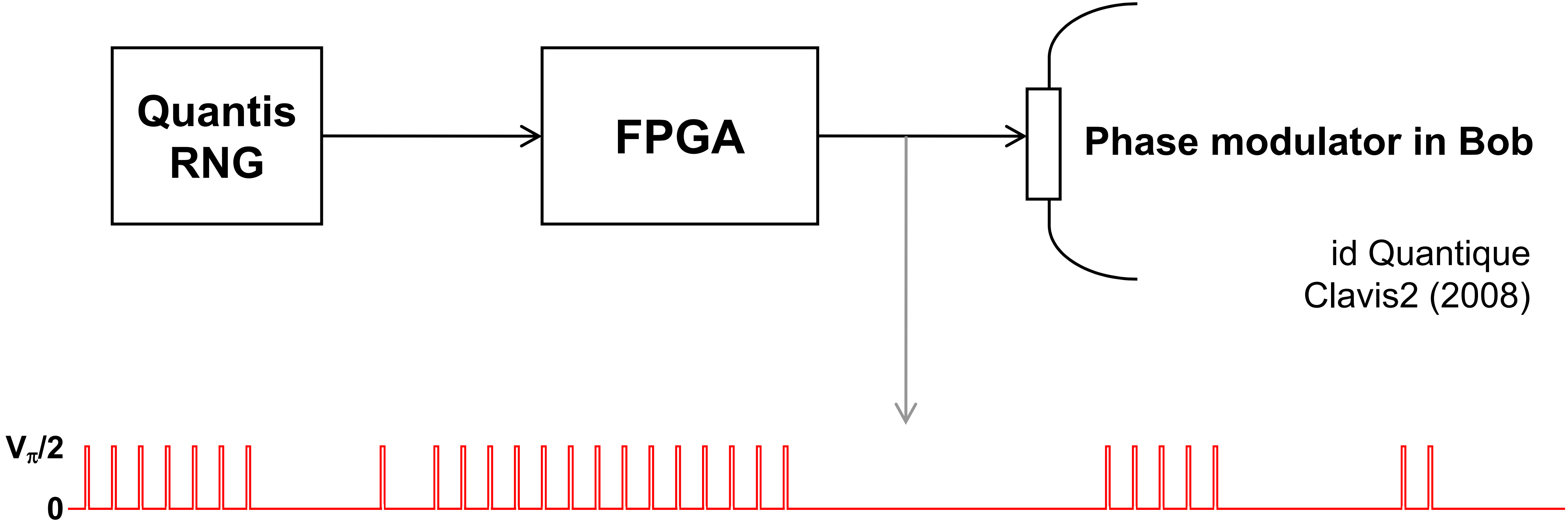


www.swissquantum.com

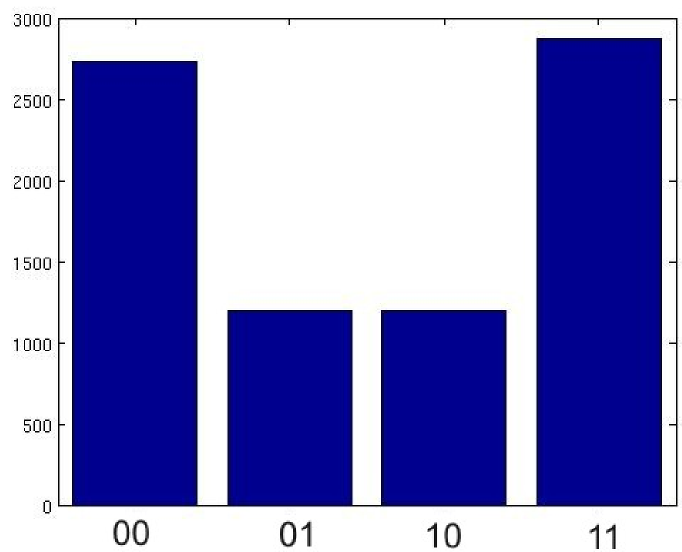
True randomness?



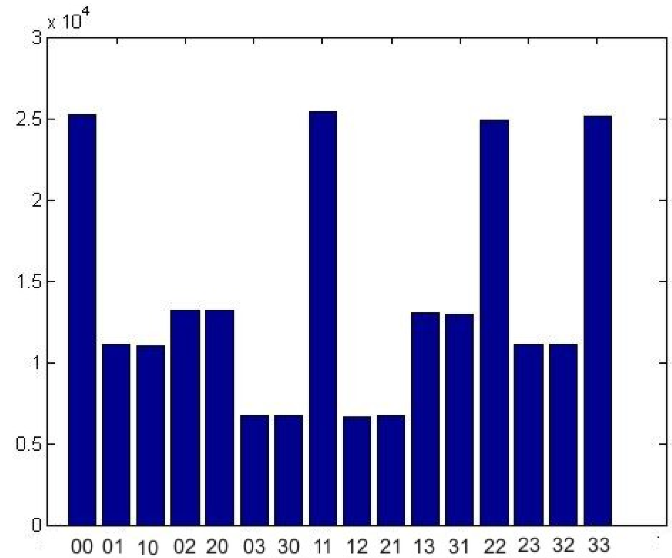
True randomness?



Bob:



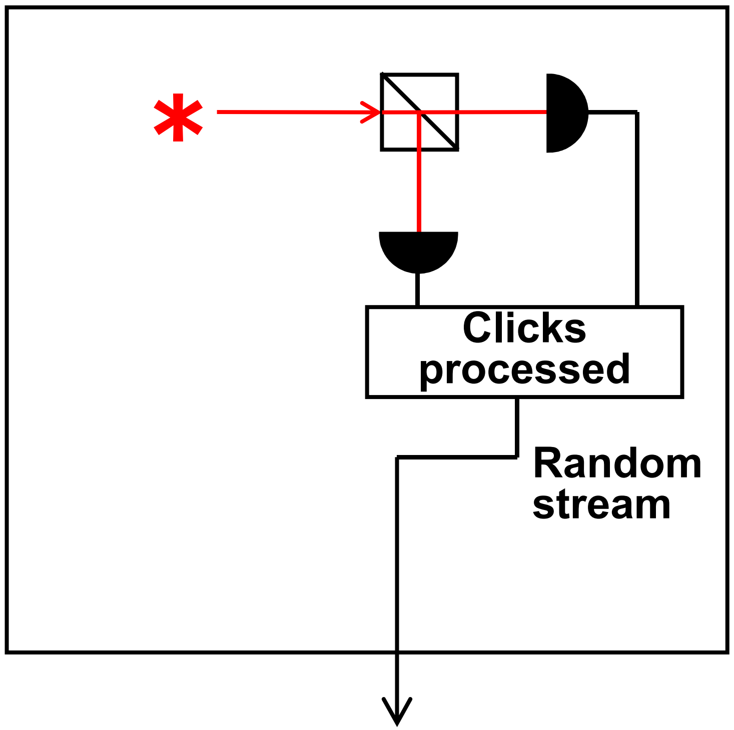
Alice:



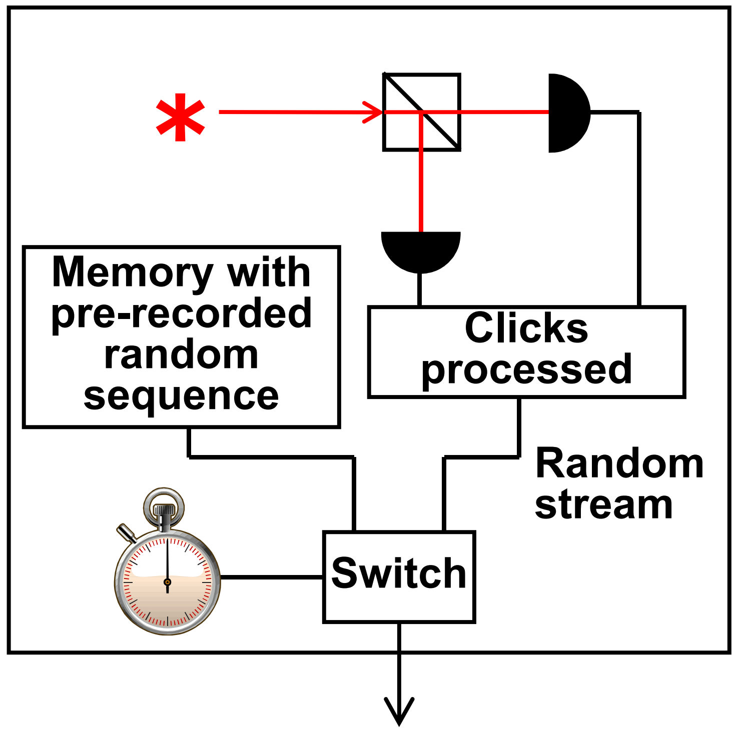
Issue reported patched, as of January 2010

Do we trust the manufacturer?

Quantis RNG



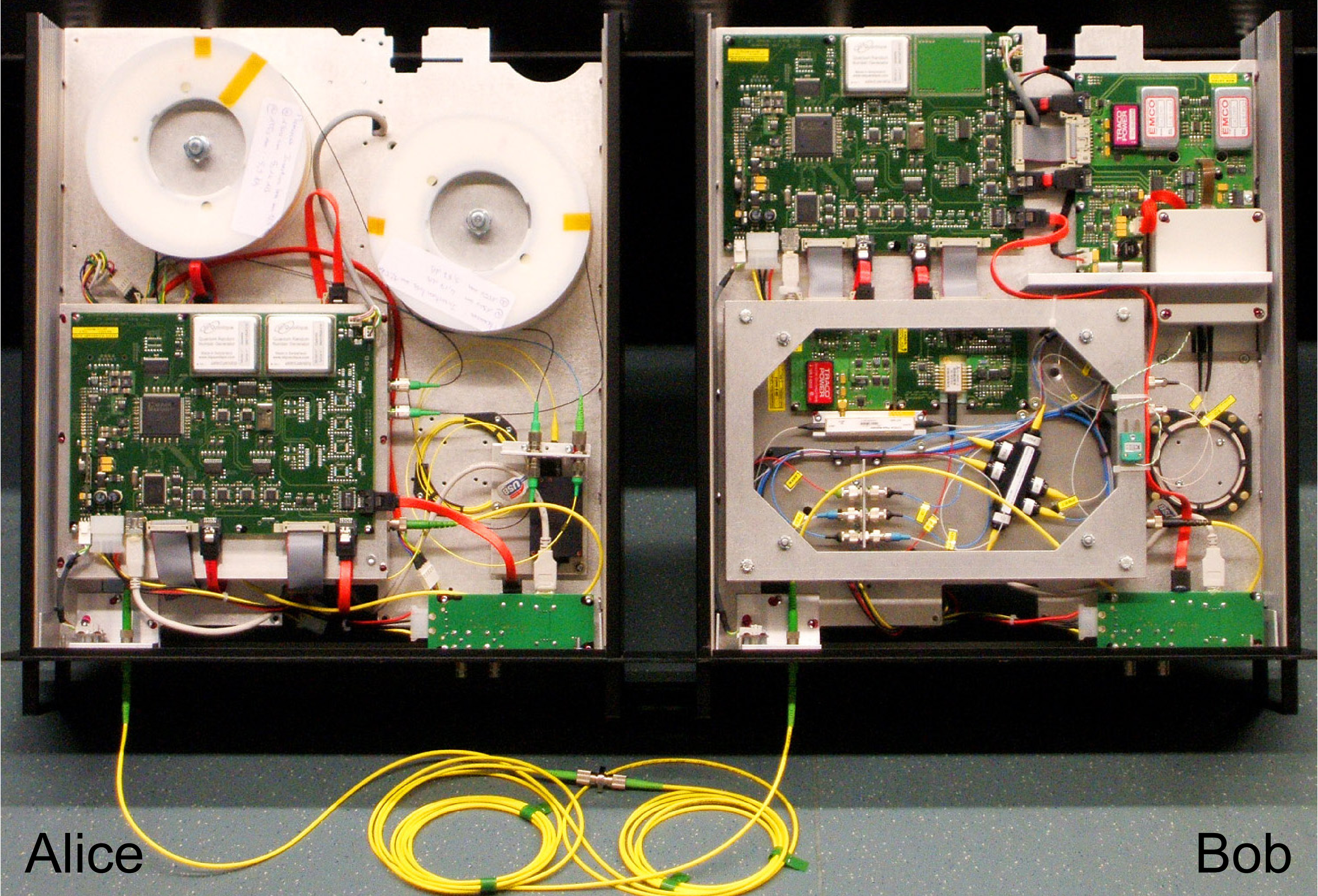
Quantis RNG, Trojan-horsed :)



Many components in QKD system can be Trojan-horsed:

- access to secret information
- electrical power
- way to communicate outside or compromise security

ID Quantique Clavis2 QKD system

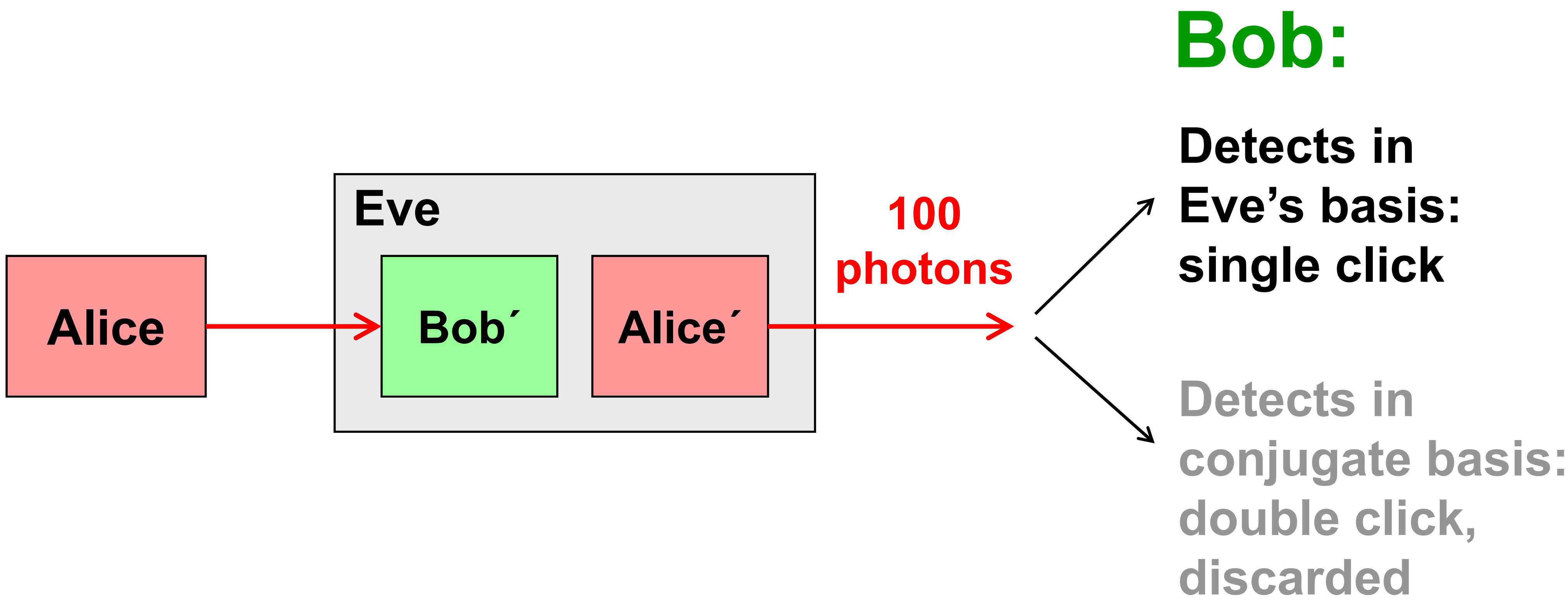


Double clicks

– occur naturally because of detector dark counts, multi-photon pulses...

Discard them?

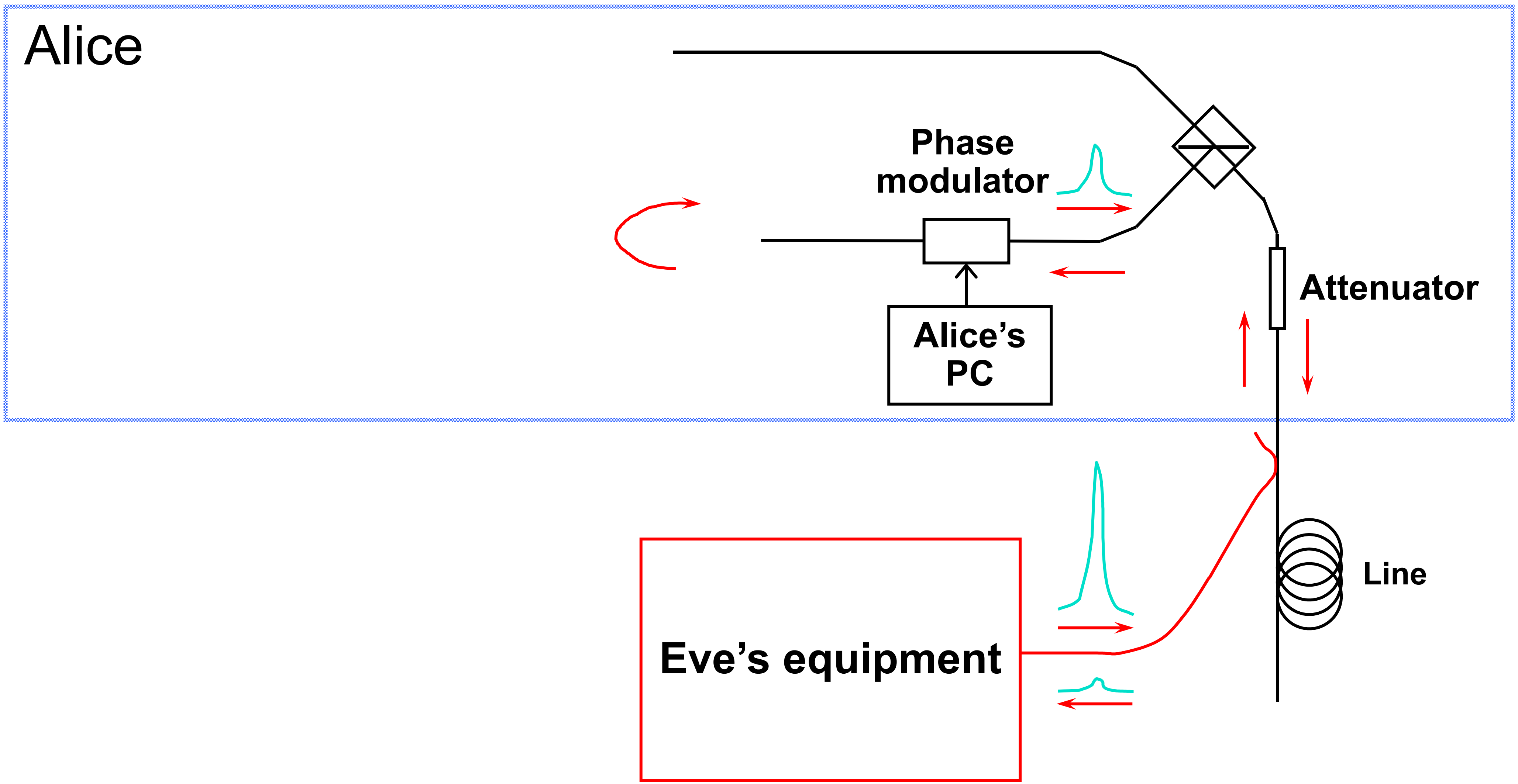
Intercept-resend attack... with a twist:



Proper treatment for double clicks: assign a random bit value.

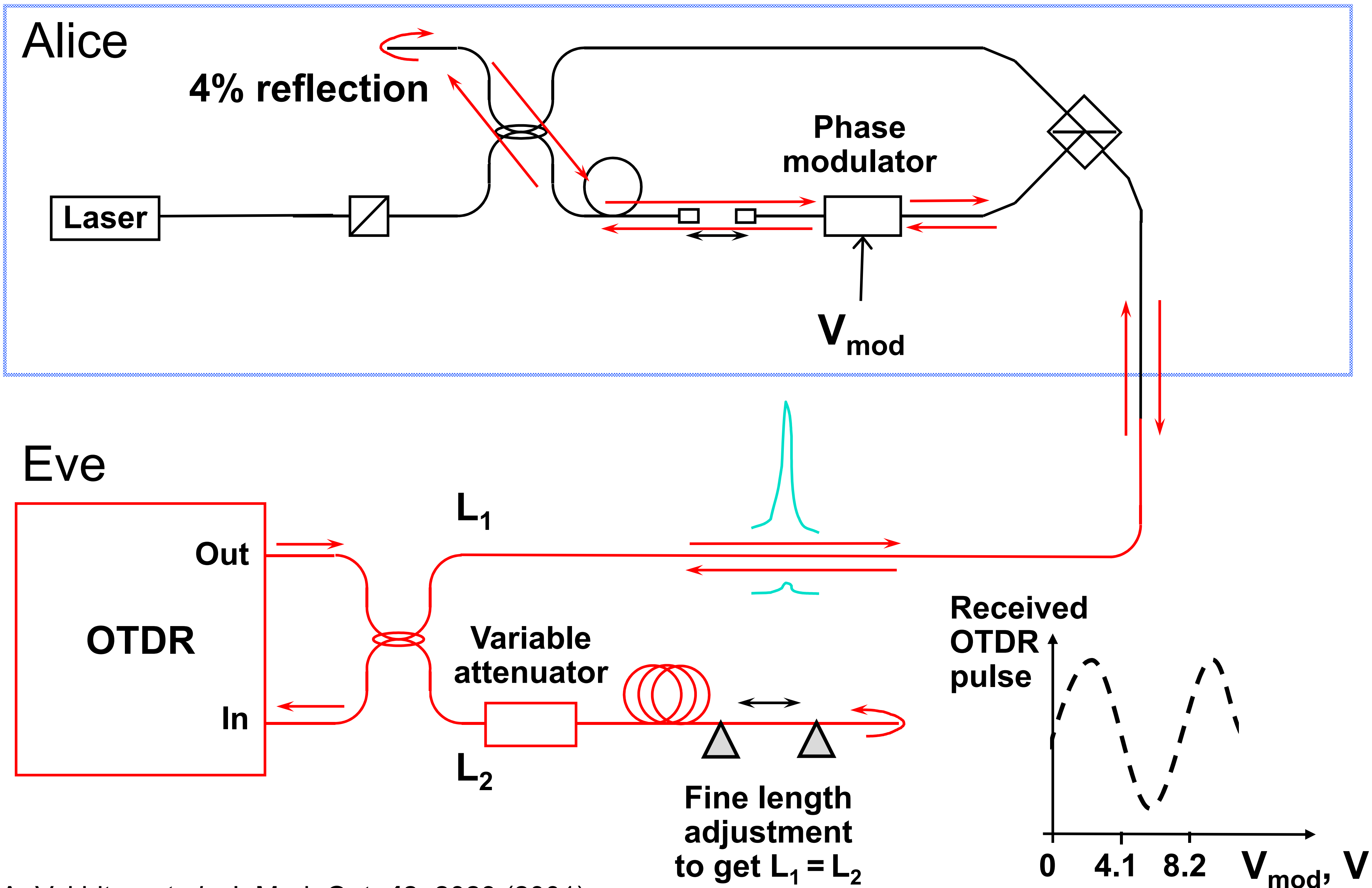
N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999)
T. Tsurumaru & K. Tamaki, Phys. Rev. A **78**, 032302 (2008)

Trojan-horse attack

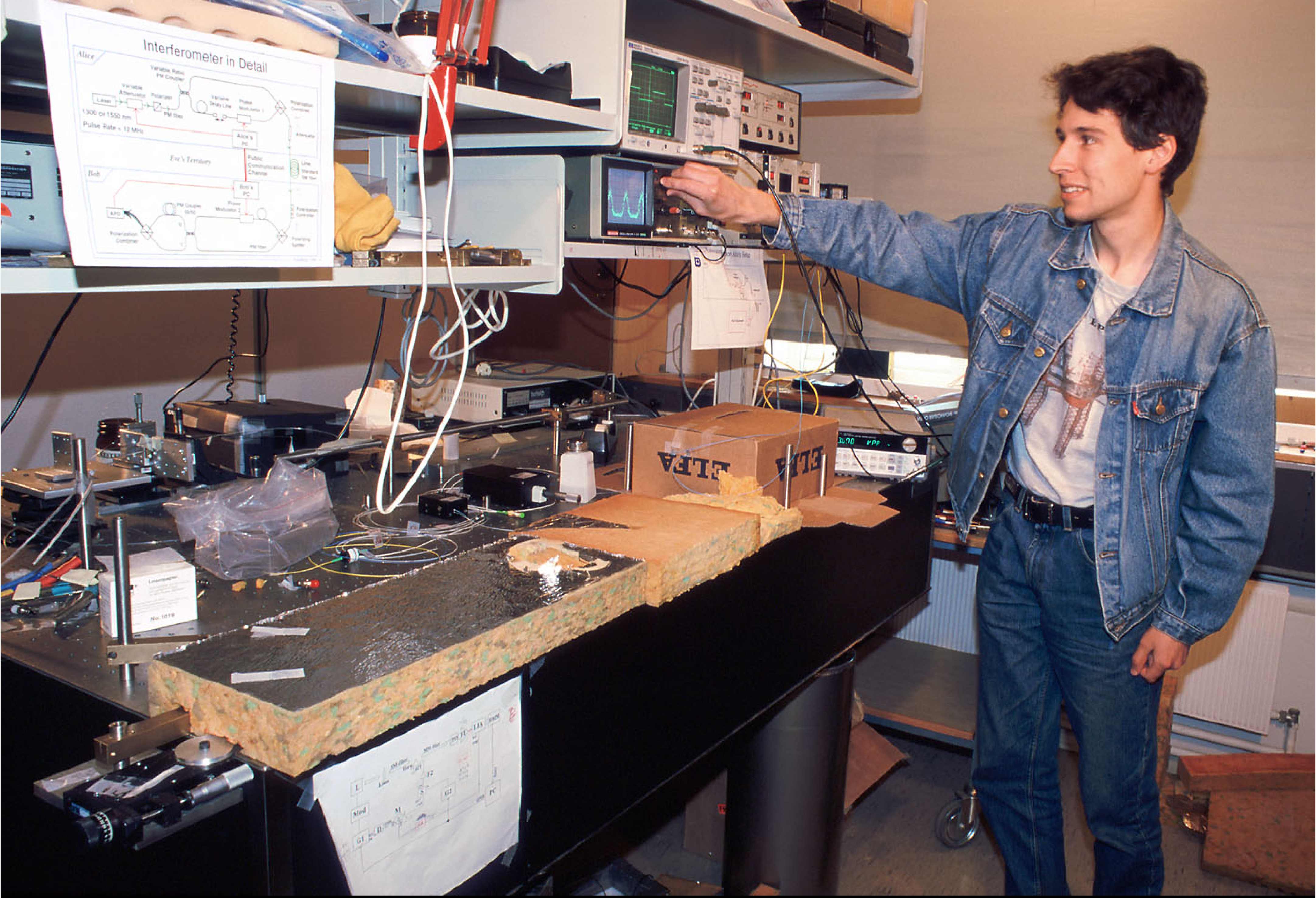


– interrogating Alice's phase modulator with powerful external pulses (can give Eve bit values directly)

Trojan-horse attack experiment

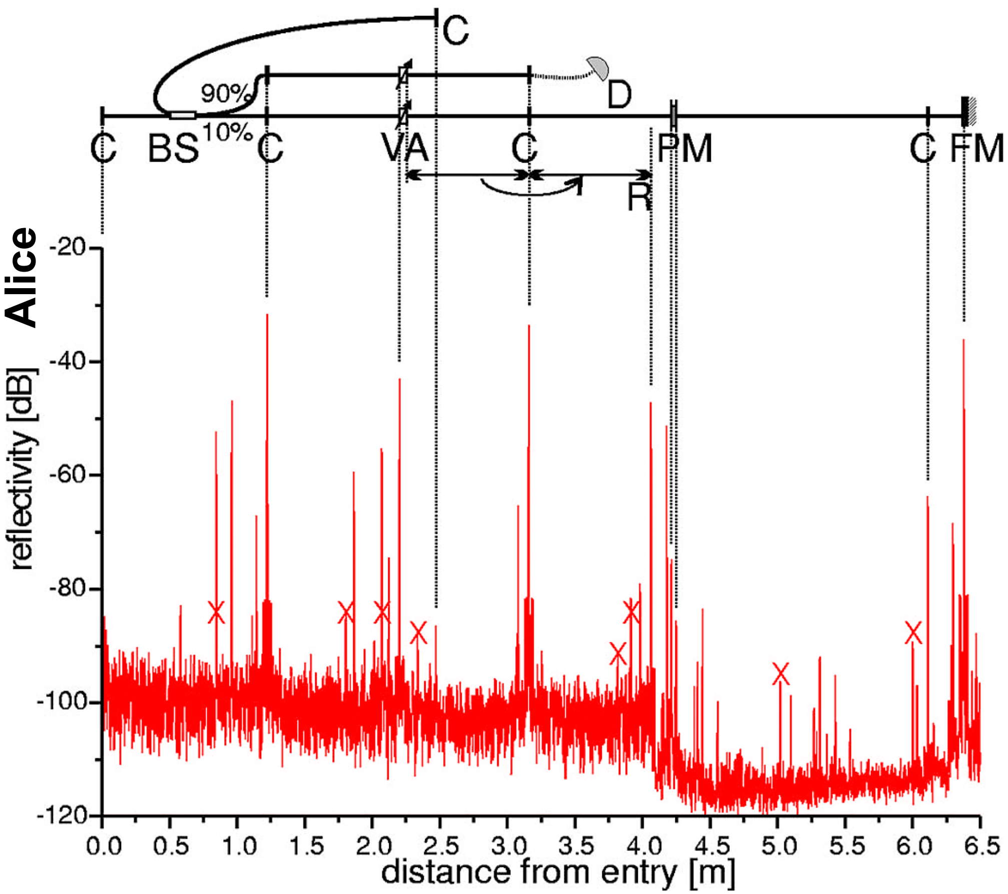


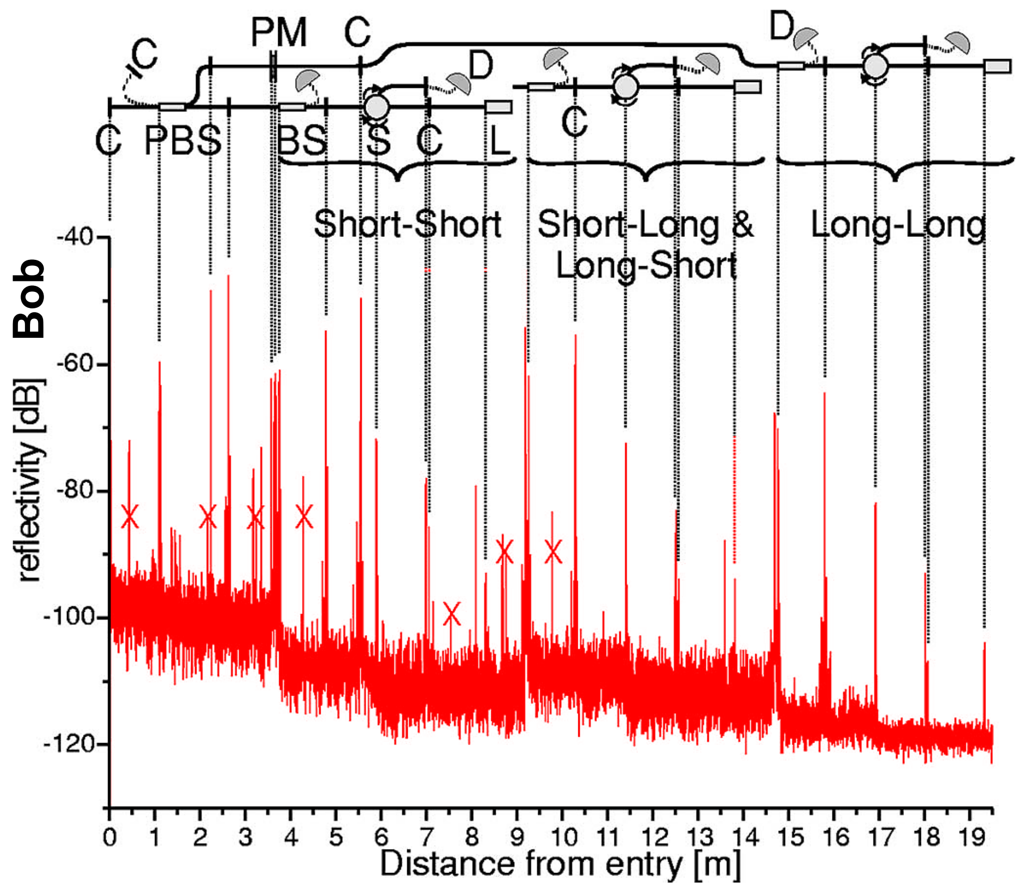
A. Vakhitov *et al.*, J. Mod. Opt. **48**, 2023 (2001)



Artem Vakhitov tunes up Eve's setup

Trojan-horse attack for plug-and-play system

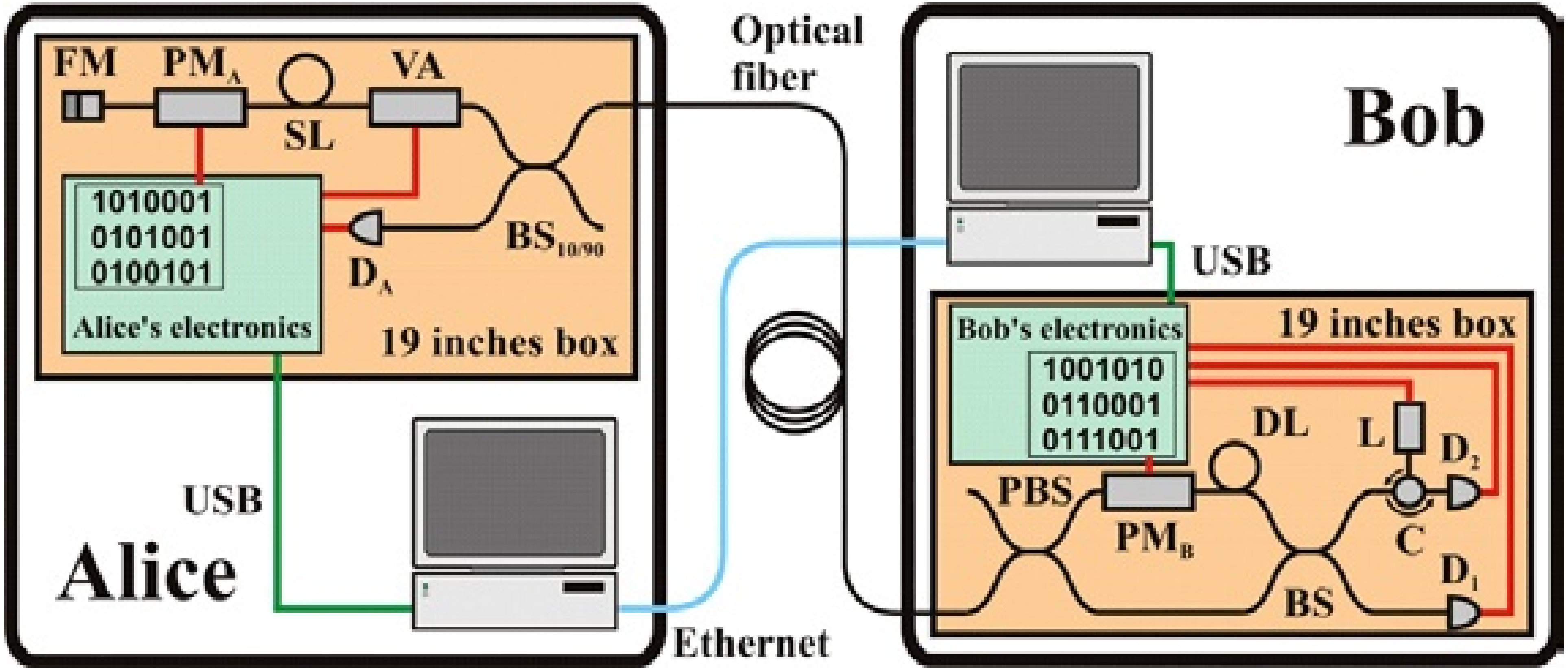




Eve gets back one photon $\rightarrow$ in principle, extracts 100% information

N. Gisin *et al.,* Phys. Rev. A **73**, 022320 (2006)

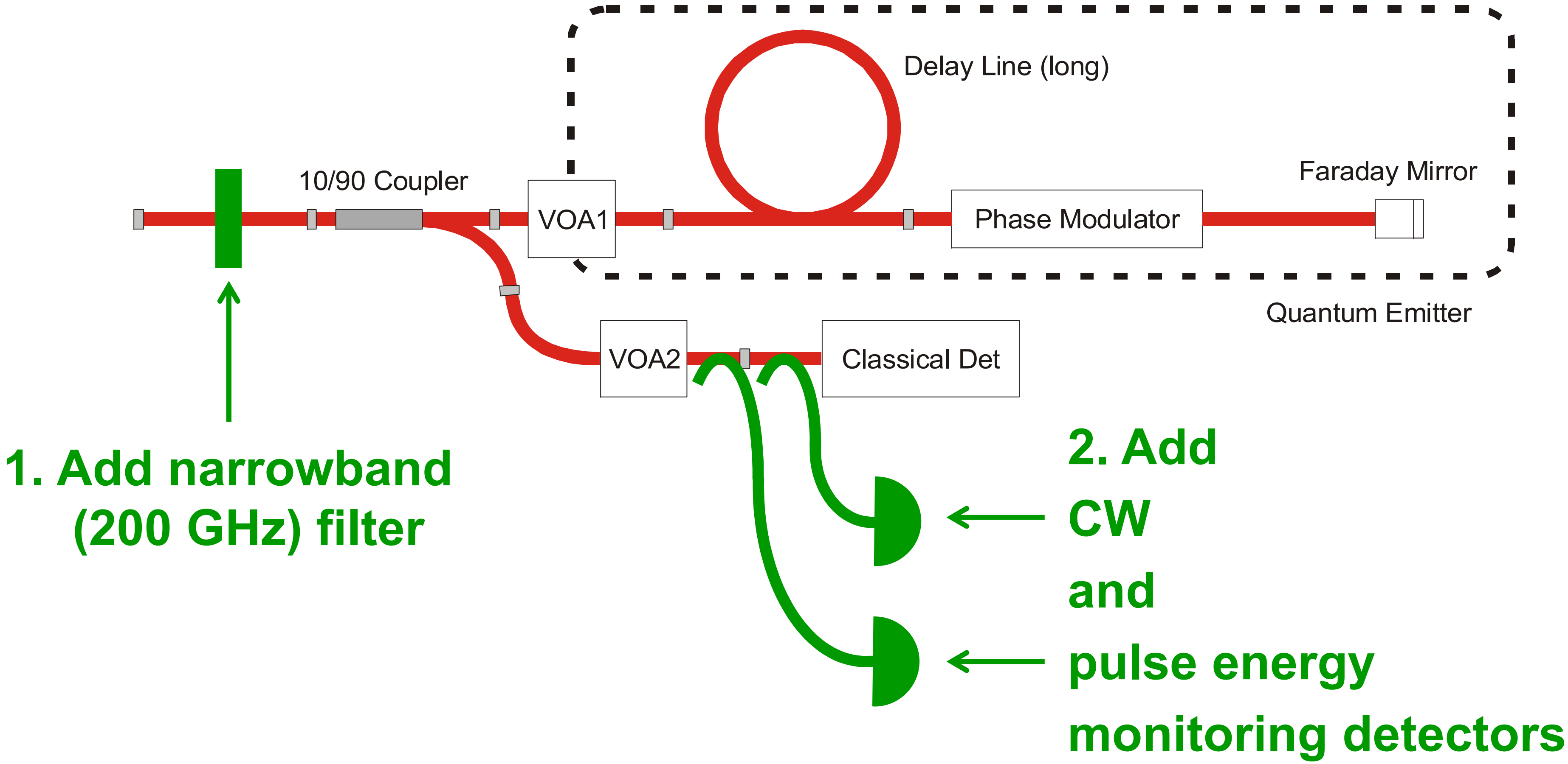
Countermeasures?



D. Stucki *et al.*, New J. Phys. **4**, 41 (2002)

Countermeasures for plug-and-play system

Alice:



Bob: none

(one consequence: SARG protocol may be insecure)

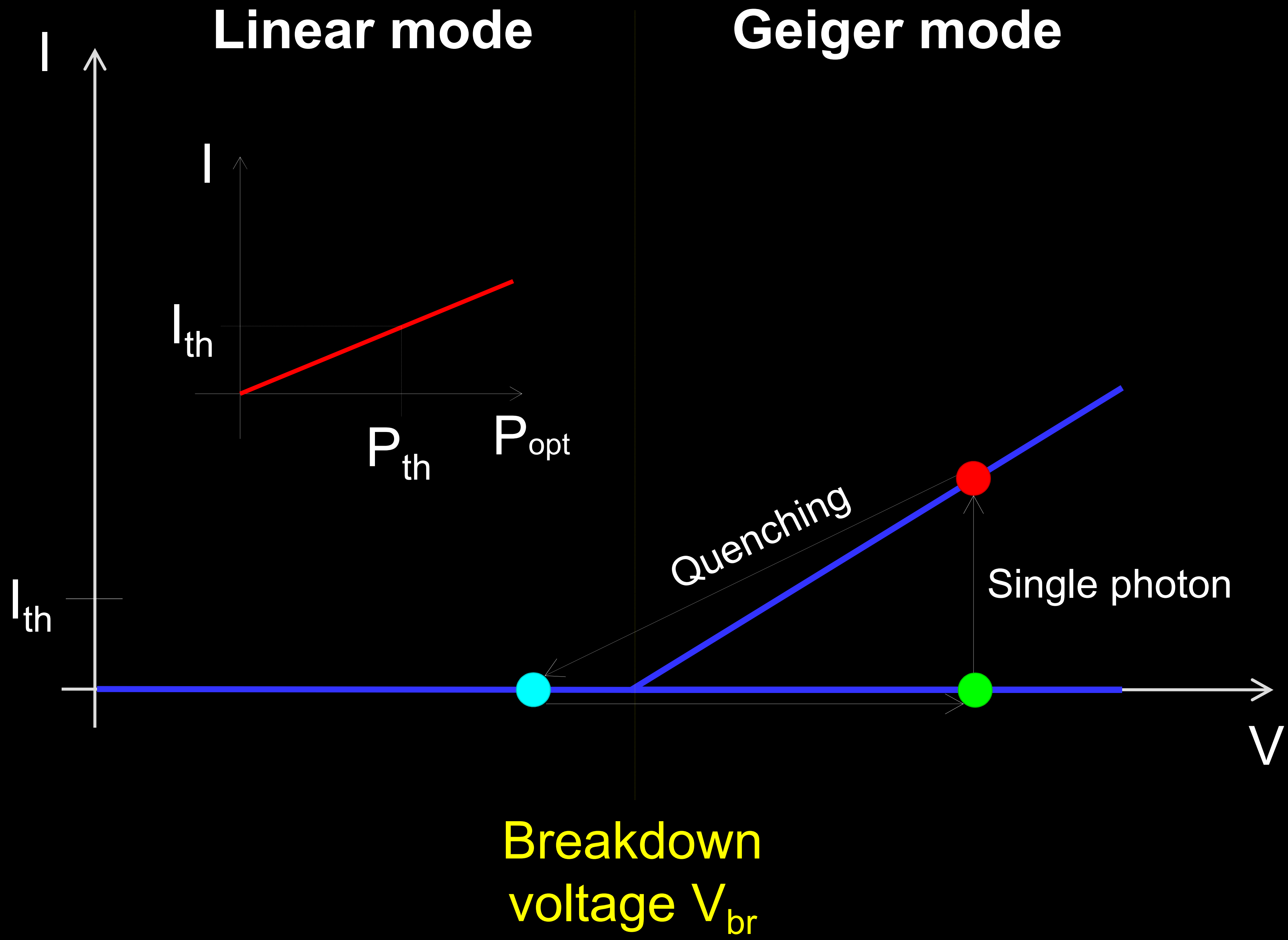
Attack	Target component	Tested system	Demonstrated eavesdr. (% key)?	Keeps full key rate?
Phase-remapping	phase modulator	ID Quantique	**no** (full inf.-th.)	**yes** (@ transm. $\ll 1$)
F. Xu, B. Qi, H.-K. Lo, New J. Phys. **12**, 113026 (2010)				
Faraday-mirror	Faraday mirror	(theory)	(full inf.-th.)	**yes** (@ transm. $\ll 1$)
S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011)				
Channel calibration	detector	ID Quantique	**no** (full inf.-th.)	**yes**
N. Jain *et al.*, Phys. Rev. Lett. **107**, 110501 (2011)				
Detector control	detector	ID Quantique, MagiQ Tech.	**no** (**100%**)	**yes**
L. Lydersen *et al.*, Nat. Photonics **4**, 686 (2010)				
Detector control	detector	research syst.	**yes** (**100%**)	**yes**
I. Gerhardt *et al.*, Nat. Commun. **2**, 349 (2011)				
Deadtime	detector	research syst.	**yes** (**98.8%**)	**no, 1/4**
H. Weier *et al.*, New J. Phys. **13**, 073024 (2011)				
Multi-wavelength	beamsplitter	research syst.	**yes** ($\lesssim$**100%**)	**yes**
H.-W. Li *et al.*, Phys. Rev. A **84**, 062308 (2011)				

Attack	Target component	Tested system	Demonstrated eavesdr. (% key)?	Keeps full key rate?
Phase-remapping F. Xu, B. Qi, H.-K. Lo, New J. Phys. **12**, 113026 (2010)	phase modulator	ID Quantique	no (full inf.-th.)	yes (@ transmit. $\ll 1$)
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011)	Faraday mirror	(theory)	(full inf.-th.)	yes (@ transm. $\ll 1$)
Channel calibration N. Jain *et al.,* Phys. Rev. Lett. **107**, 110501 (2011)	detector	ID Quantique	no (full inf.-th.)	yes
Detector control L. Lydersen *et al.,* Nat. Photonics **4**, 686 (2010)	detector	ID Quantique, MagiQ Tech.	no (100%)	yes
Detector control I. Gerhardt *et al.,* Nat. Commun. **2**, 349 (2011)	detector	research syst.	yes (100%)	yes
Deadtime H. Weier *et al.,* New J. Phys. **13**, 073024 (2011)	detector	research syst.	yes (98.8%)	no [illegible]4
Multi-wavelength H.-W. Li *et al.,* Phys. Rev. A **84**, 062308 (2011)	beamsplitter	research syst.	yes ($<\sim$100%)	yes

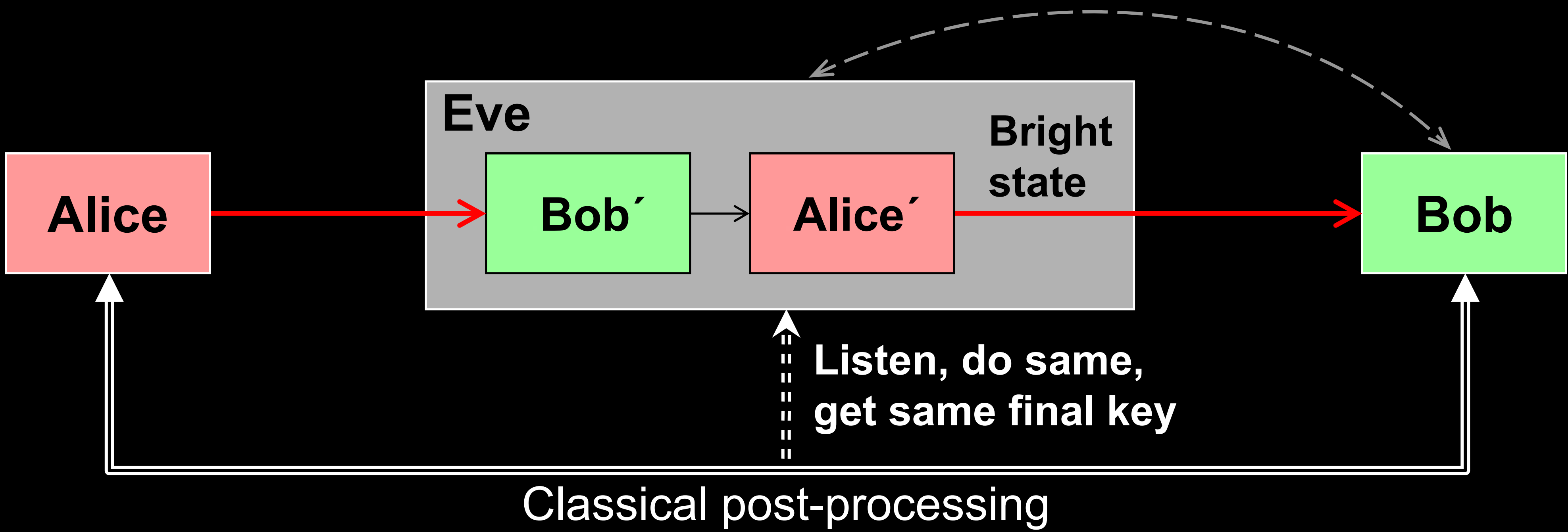
Every attack
breaks QKD security!

Attack	Target component	Tested system	Demonstrated eavesdr. (% key)?	Keeps full key rate?
Phase-remapping F. Xu, B. Qi, H.-K. Lo, New J. Phys. **12**, 113026 (2010)	phase modulator	ID Quantique	no (full inf.-th.)	yes (@ transm. $\ll 1$)
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011)	Faraday mirror	(theory)	(full inf.-th.)	yes (@ transm. $\ll 1$)
Channel calibration N. Jain *et al.*, Phys. Rev. Lett. **107**, 110501 (2011)	detector	ID Quantique	no (full inf.-th.)	yes
Detector control L. Lydersen *et al.*, Nat. Photonics **4**, 686 (2010)	detector	ID Quantique, MagiQ Tech.	no (100%)	yes
Detector control I. Gerhardt *et al.*, Nat. Commun. **2**, 349 (2011)	detector	research syst.	yes (100%)	yes
Deadtime H. Weier *et al.*, New J. Phys. **13**, 073024 (2011)	detector	research syst.	yes (98.8%)	no, 1/4
Multi-wavelength H.-W. Li *et al.*, Phys. Rev. A **84**, 062308 (2011)	beamsplitter	research syst.	yes ($\lesssim$100%)	yes

Attack example: avalanche photodetectors (APDs)

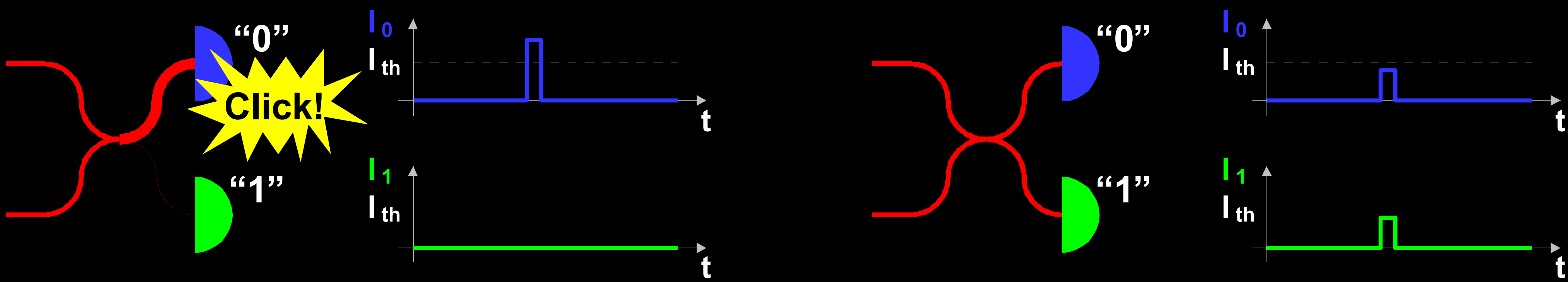


Faked-state attack in APD linear mode



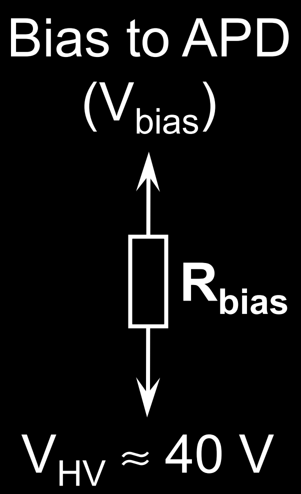
Bob chooses same basis as Eve:

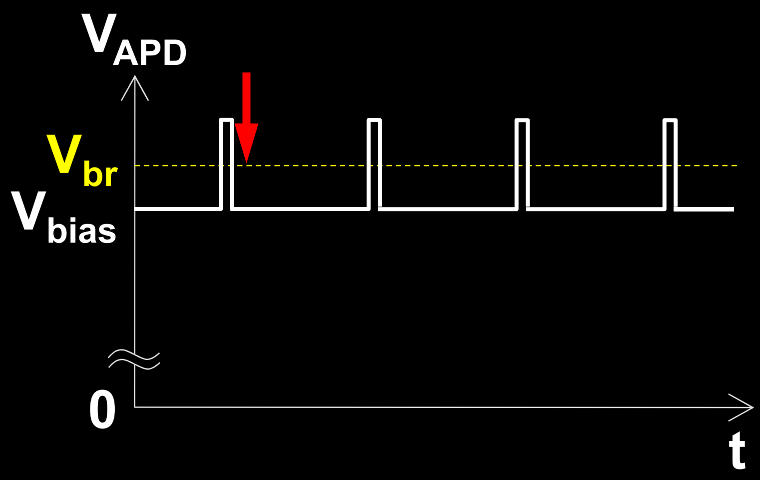
Bob chooses different basis:



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

Blinding APD with bright light

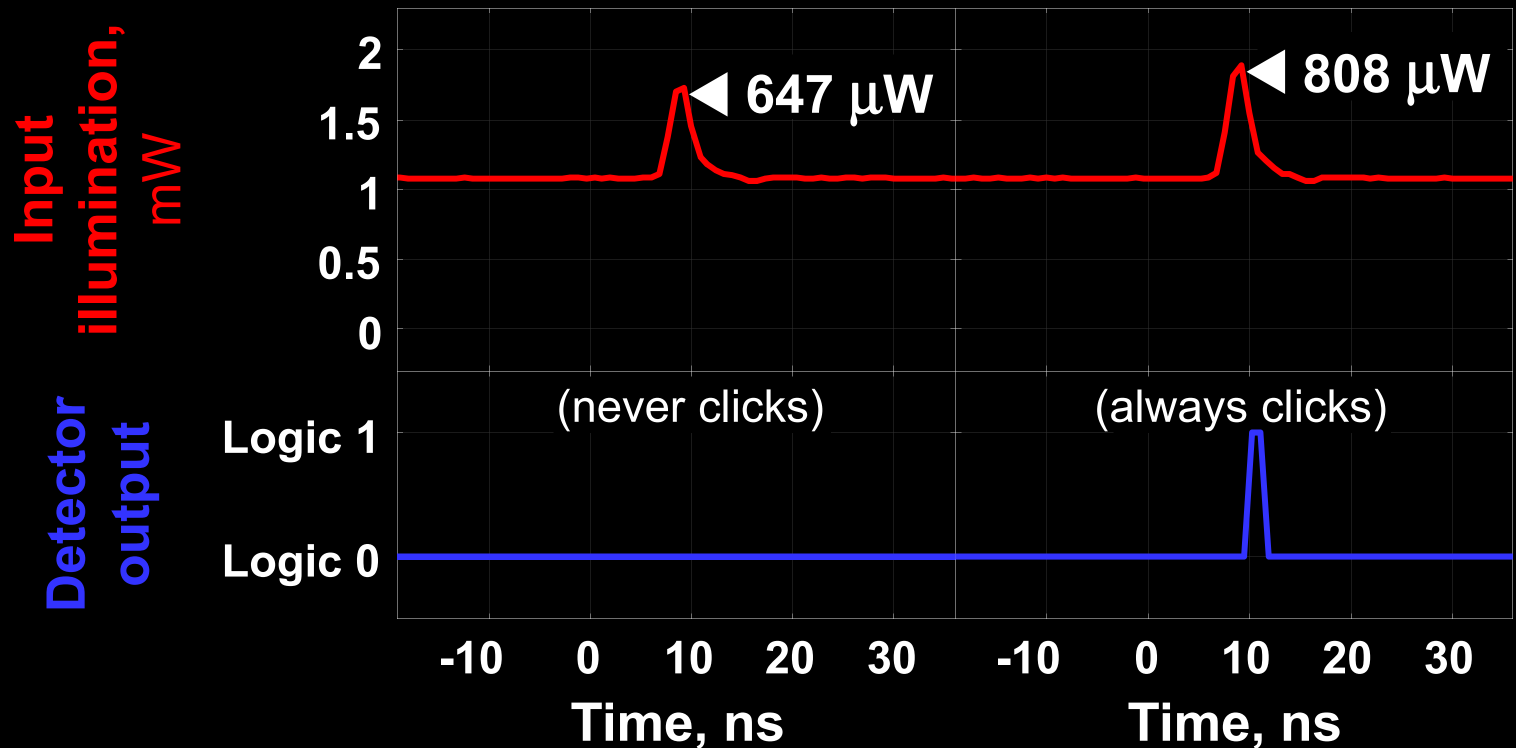




Eve applies CW light

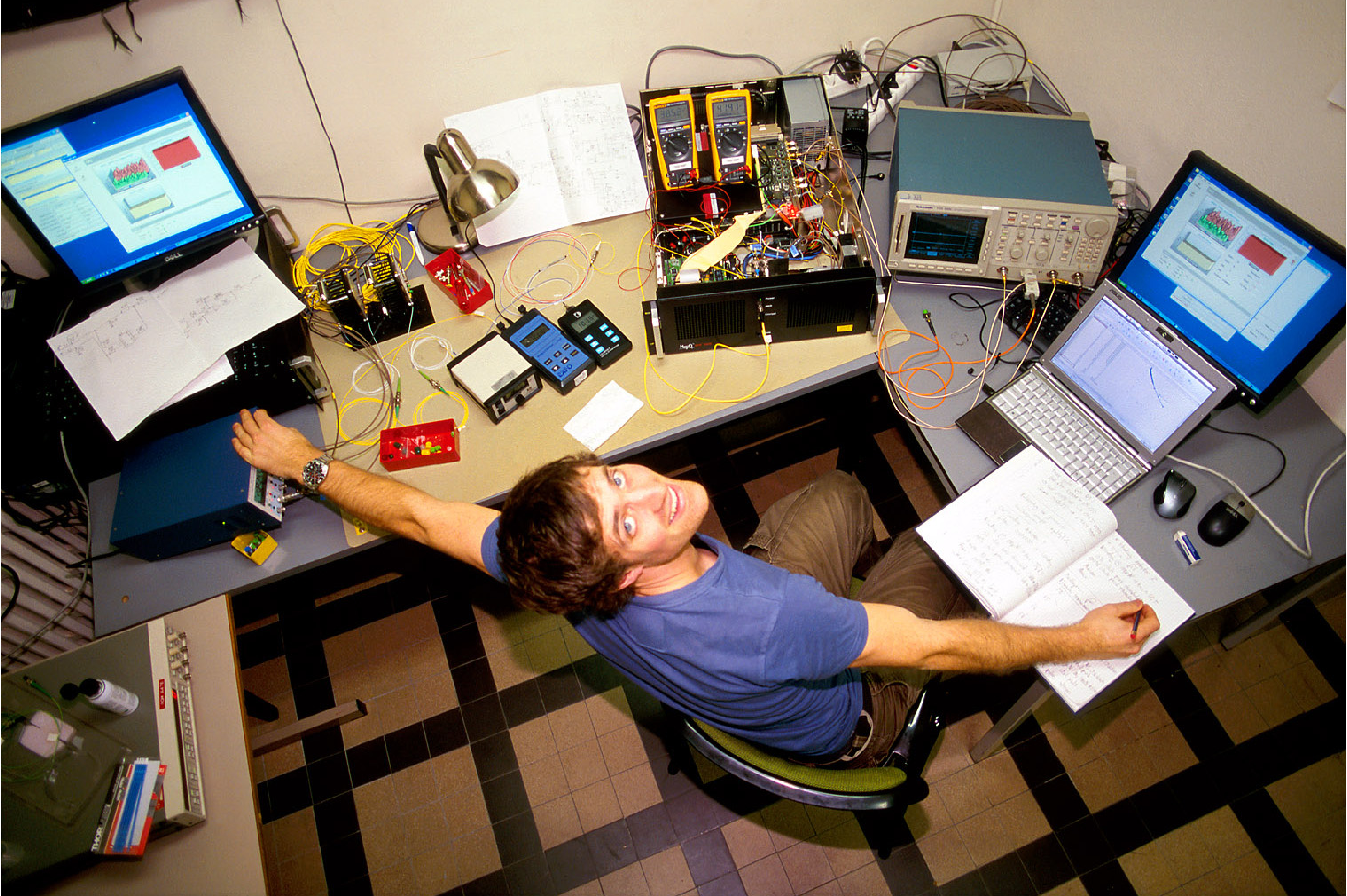
Detector blind!

Zero dark count rate



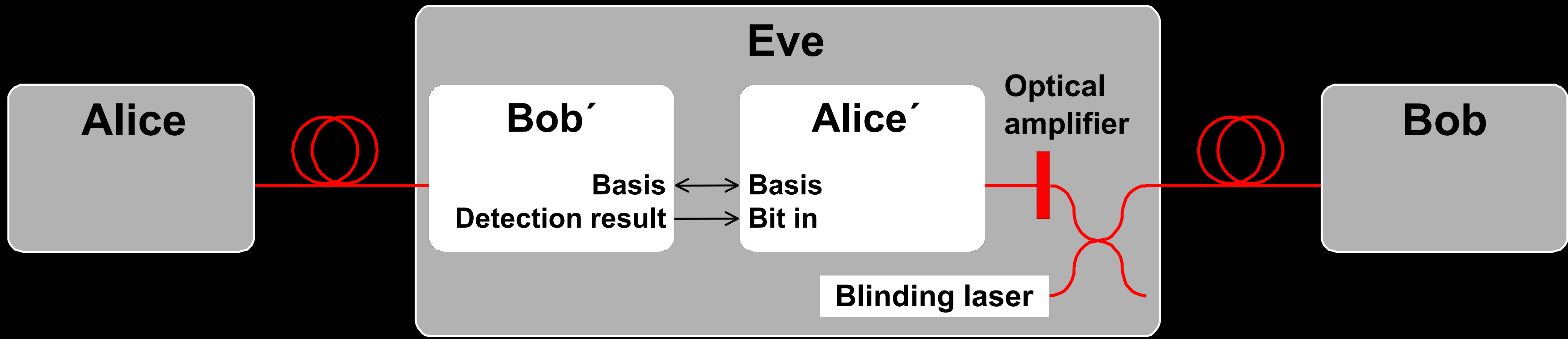
ID Quantique Clavis2

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



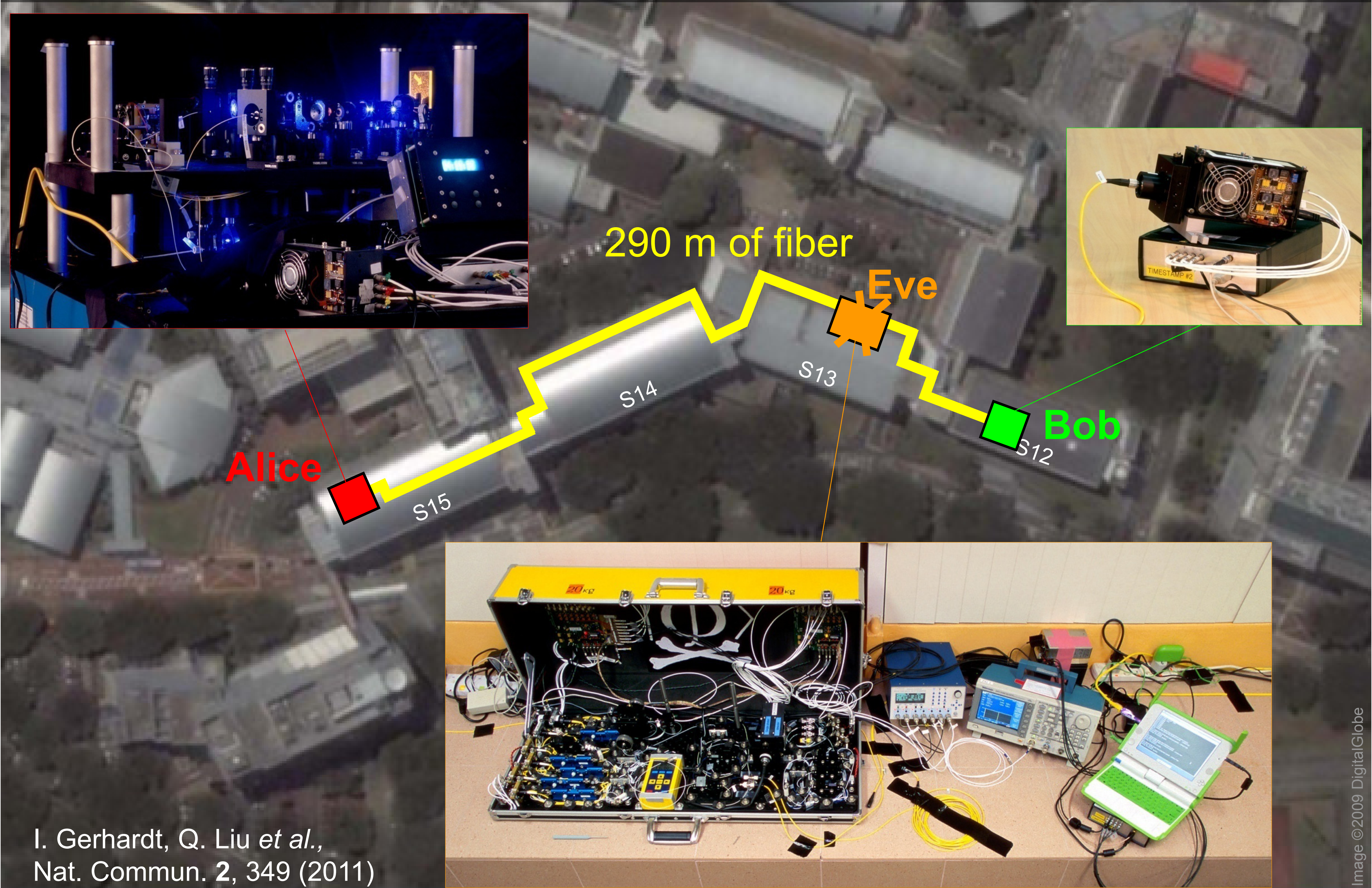
Lars Lydersen testing MagiQ Technologies QPN 5505

Proposed full eavesdropper



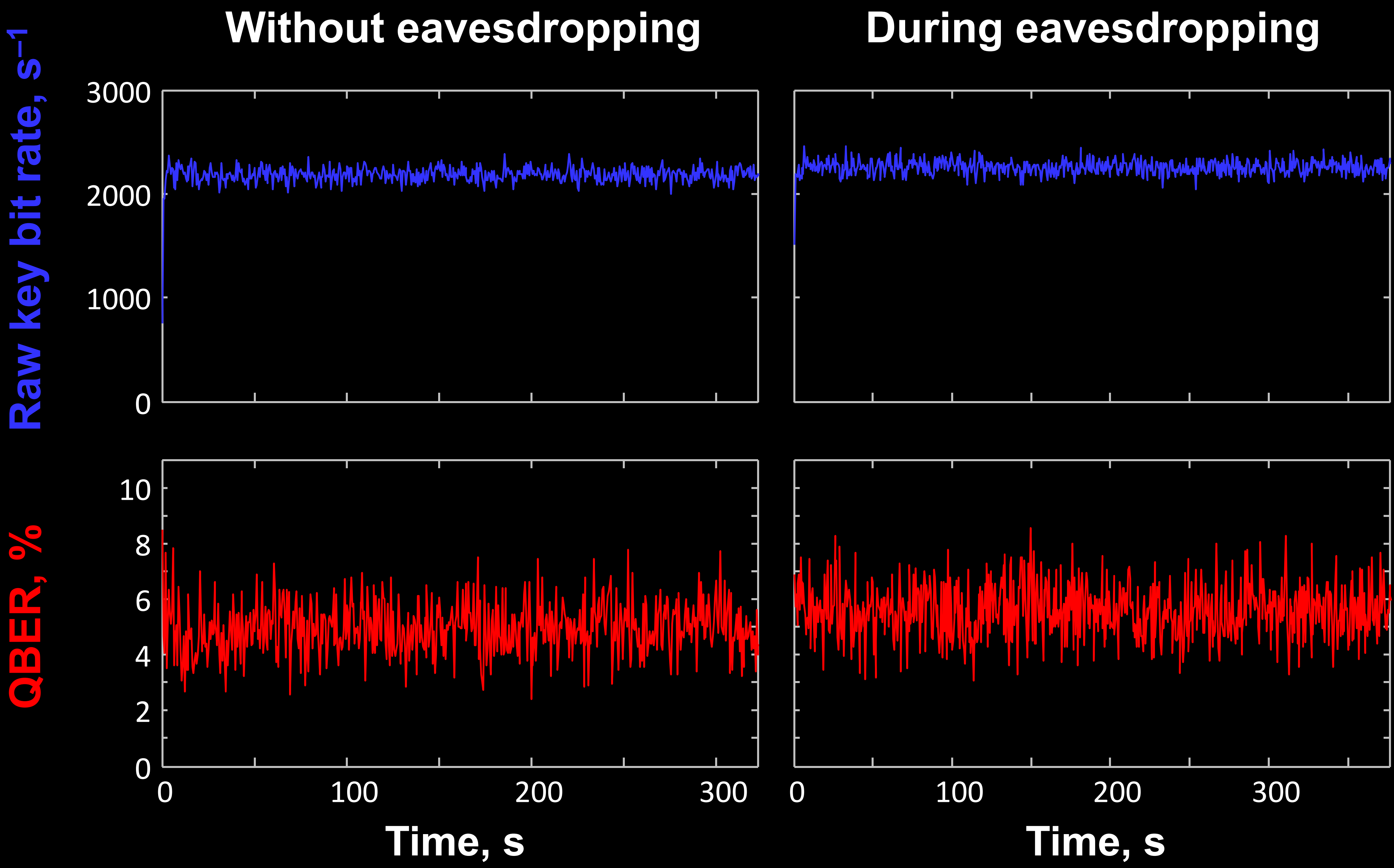
Eavesdropping 100% key on installed QKD line

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



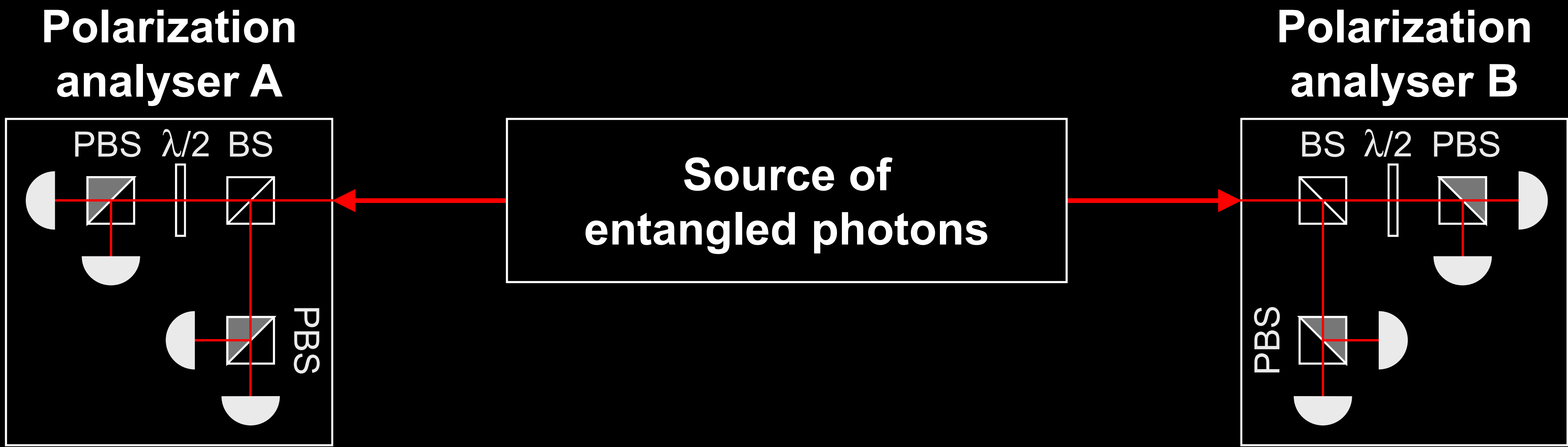
I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, V. Makarov, Nat. Commun. **2**, 349 (2011)

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



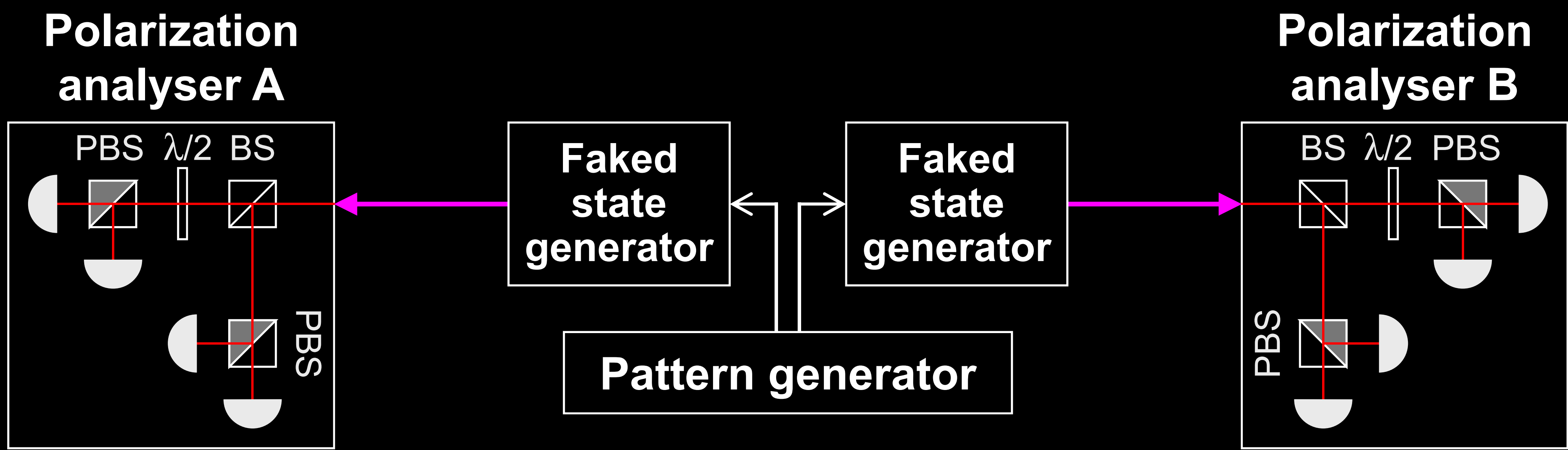
I. Gerhardt, Q. Liu *et al.*, Phys. Rev. Lett. **107**, 170404 (2011)

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

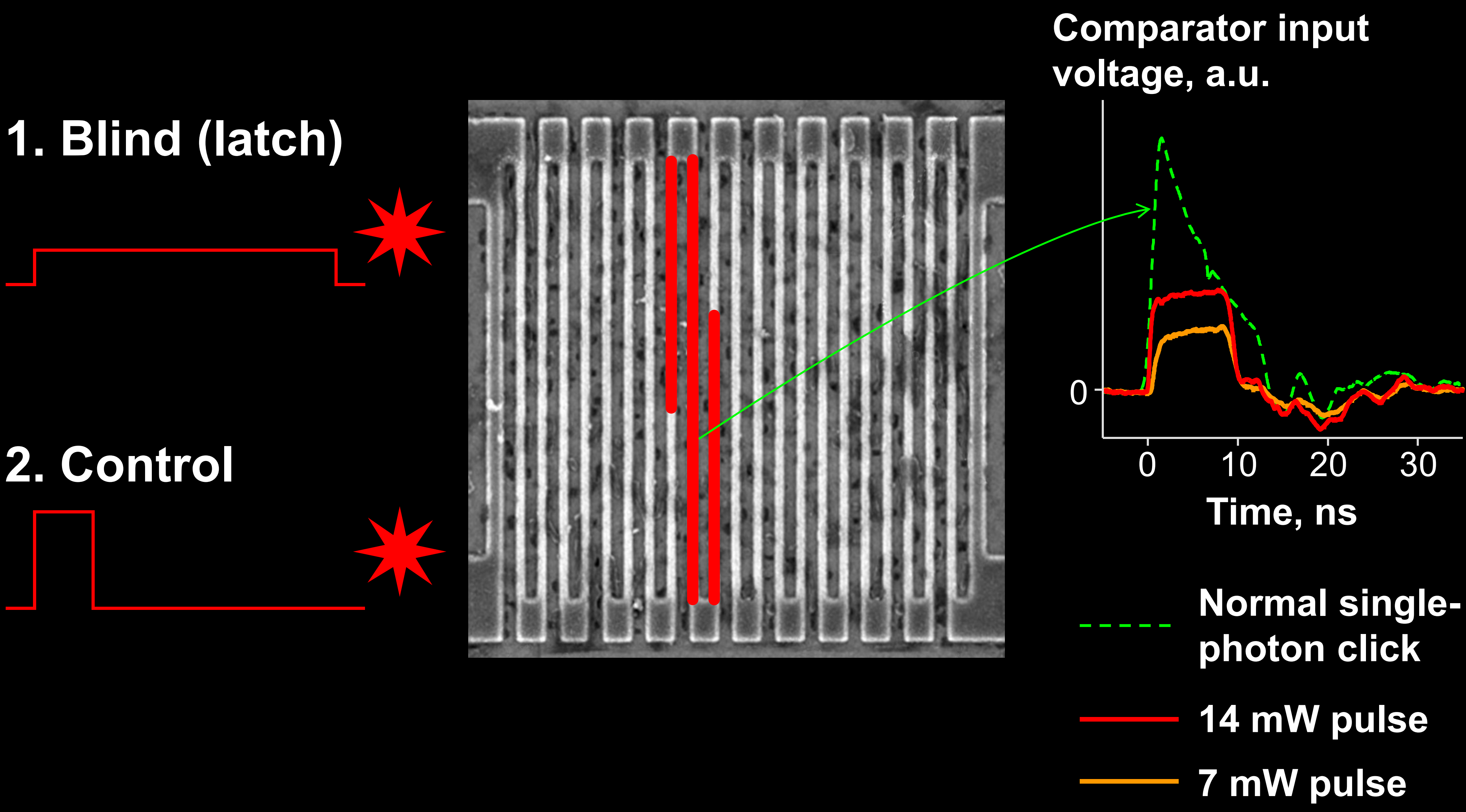


Passive basis choice: $|S| \leq 4$, click probability $= 100\%$

Active basis choice: $|S| \leq 4$, click probability $= 50\%$

I. Gerhardt, Q. Liu *et al.*, Phys. Rev. Lett. **107**, 170404 (2011)

Controlling superconducting nanowire single-photon detectors



L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, V. Makarov, New J. Phys. **13**, 113042 (2011)

Countermeasures to detector attacks?

Countermeasures to detector attacks

- ID Quantique: software-only, randomly varying detector sensitivity

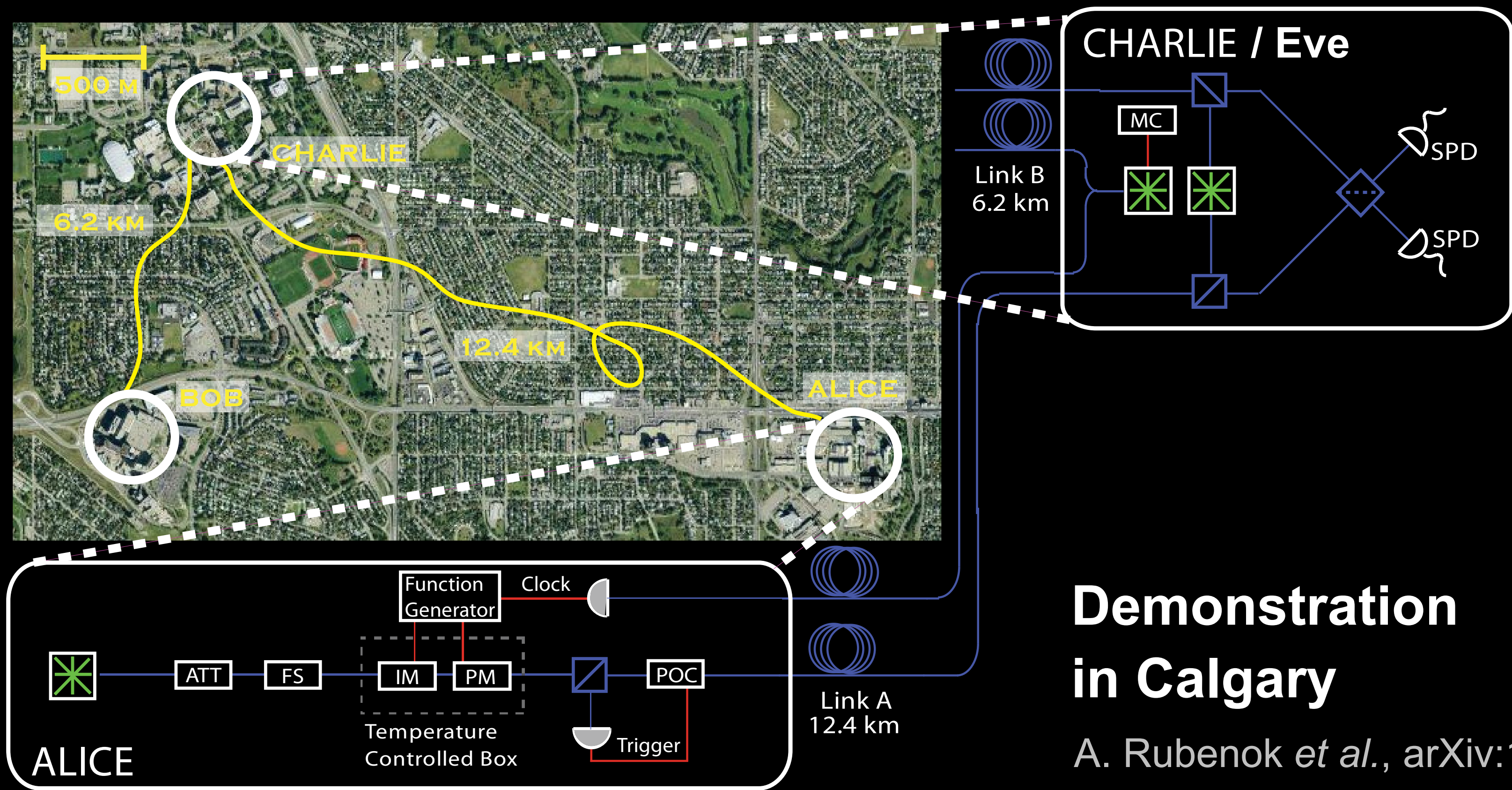
  M. Legre, G. Robordy, intl. patent appl. WO 2012/046135 A2 (filed in 2010)

- Toshiba Cambridge: monitoring extra electrical parameters in detector

  Z. L. Yuan, J. F. Dynes, A. J. Shields, Appl. Phys. Lett. **98**, 231104 (2011)

- U. of Toronto: entirely new scheme and protocol

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



Demonstration in Calgary

A. Rubenok *et al.*, arXiv:1204.0738

Responsible disclosure is important

2009

Example: hacking commercial systems

ID Quantique got a detailed vulnerability report

- **reaction: requested time, developed a patch**

2010

MagiQ Technologies got a detailed vulnerability report

- **reaction: informed us that QPN 5505 is discontinued**

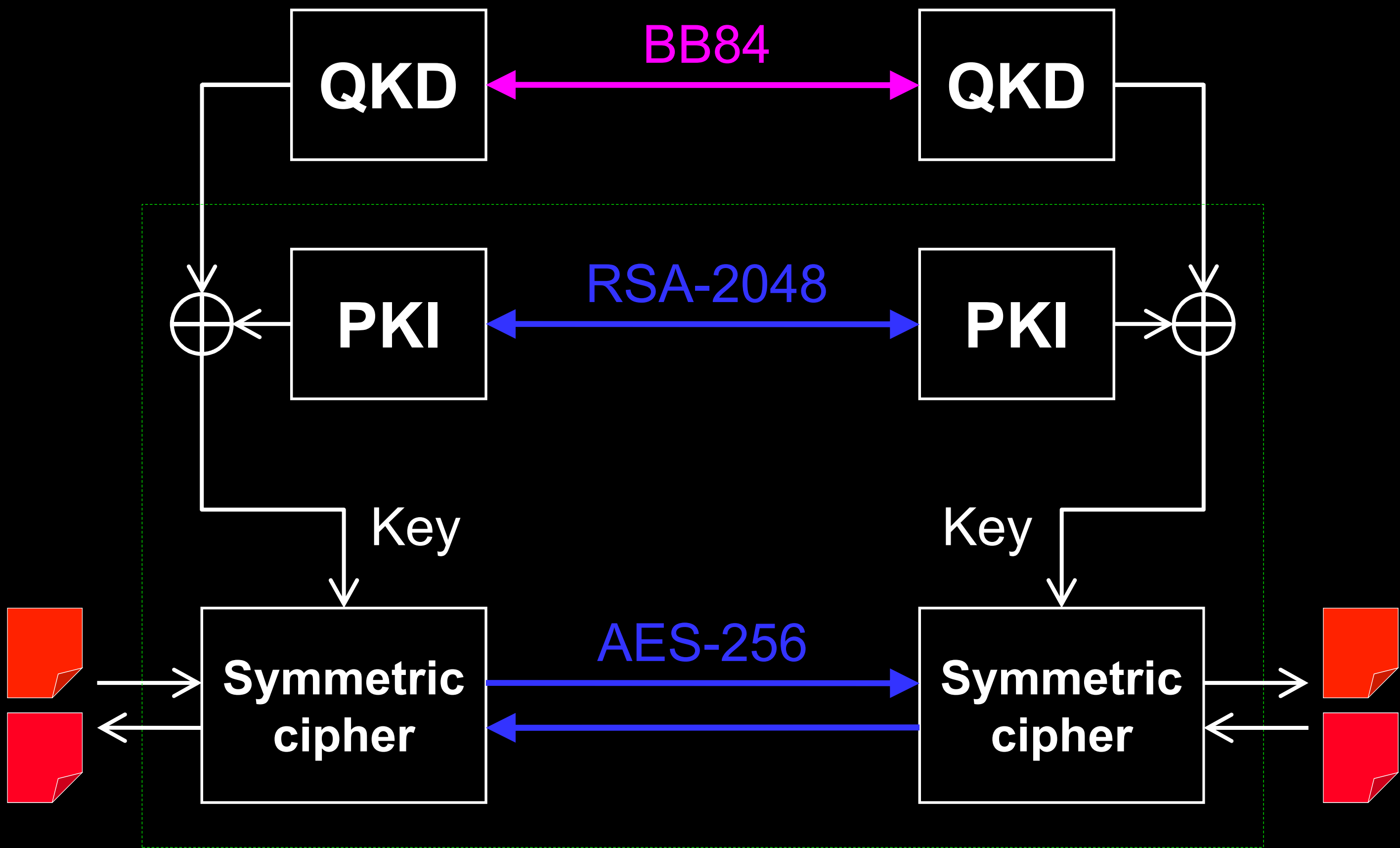
Results presented orally at a scientific conference

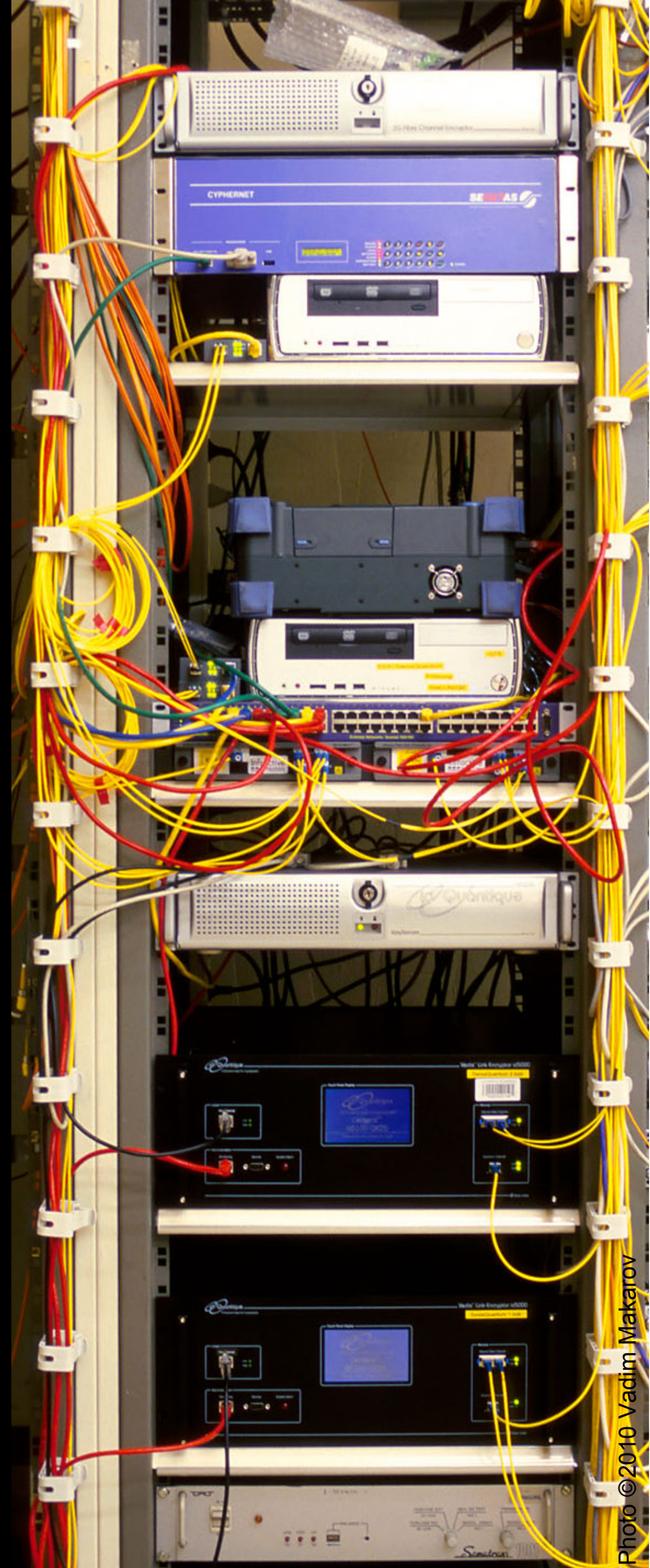
Public disclosure in a journal paper

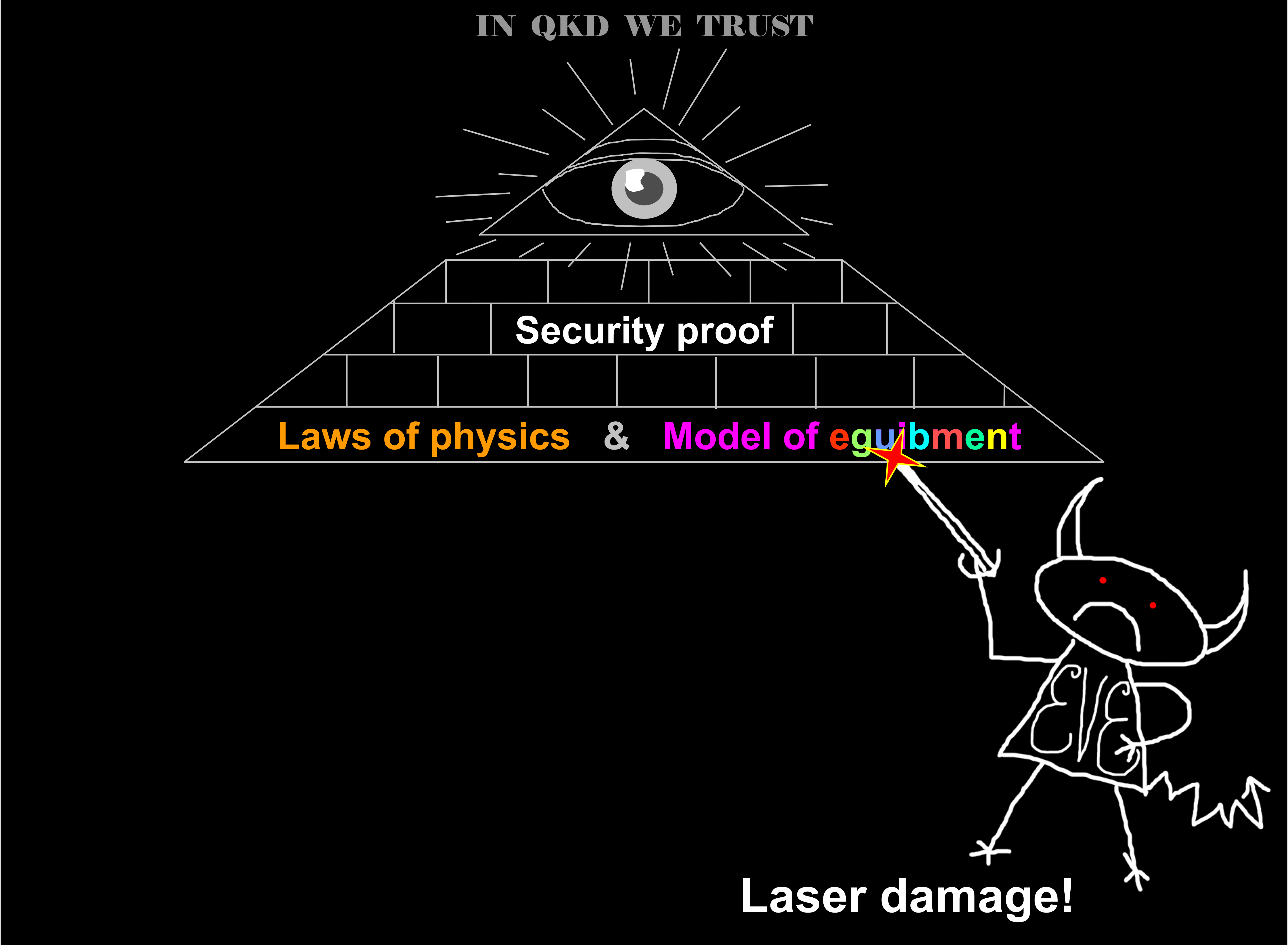
L. Lydersen *et al.*, Nat. Photonics **4**, 686 (2010)

Can we eavesdrop on commercial systems?

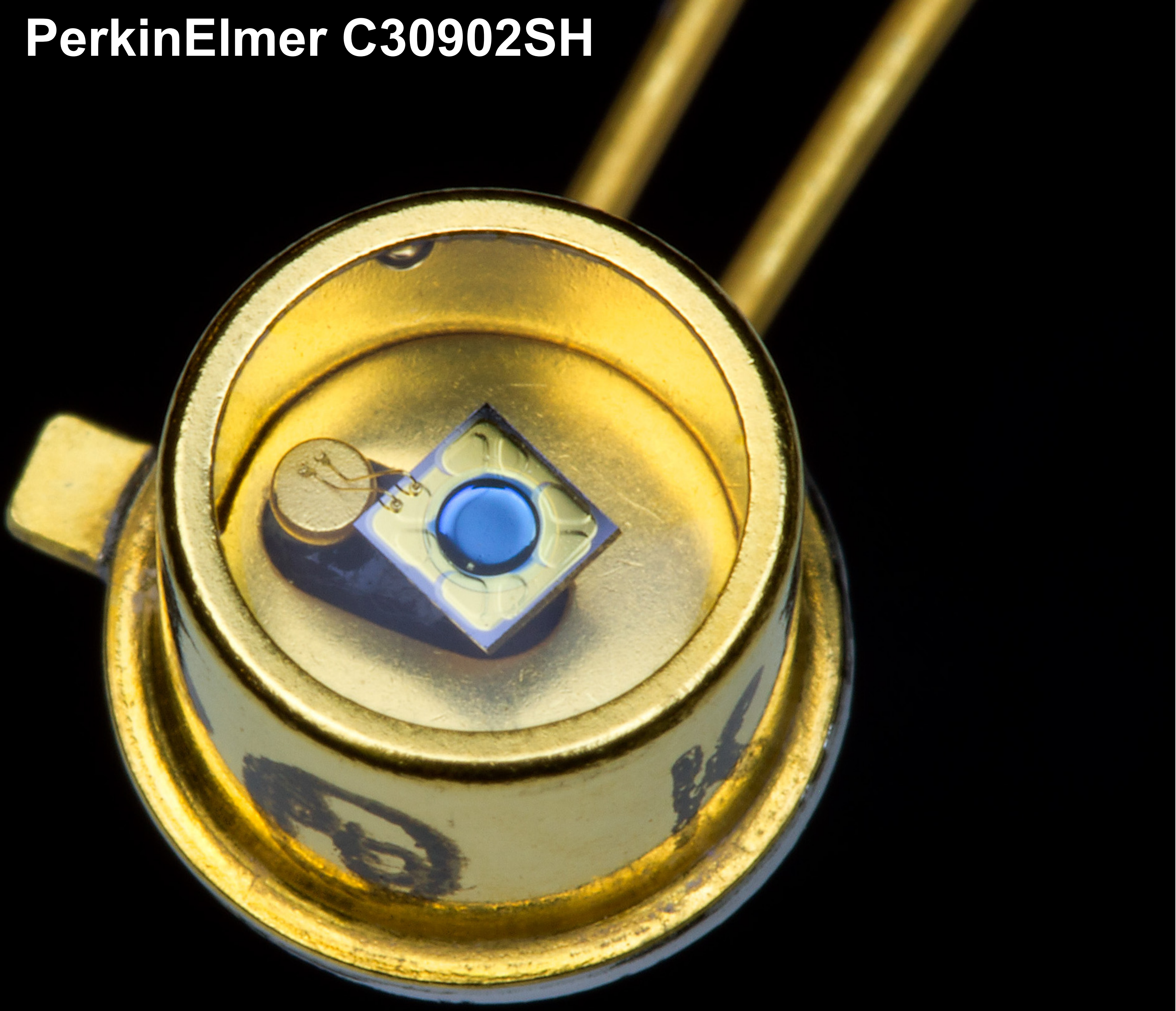
ID Quantique's Cerberis:
Dual key agreement



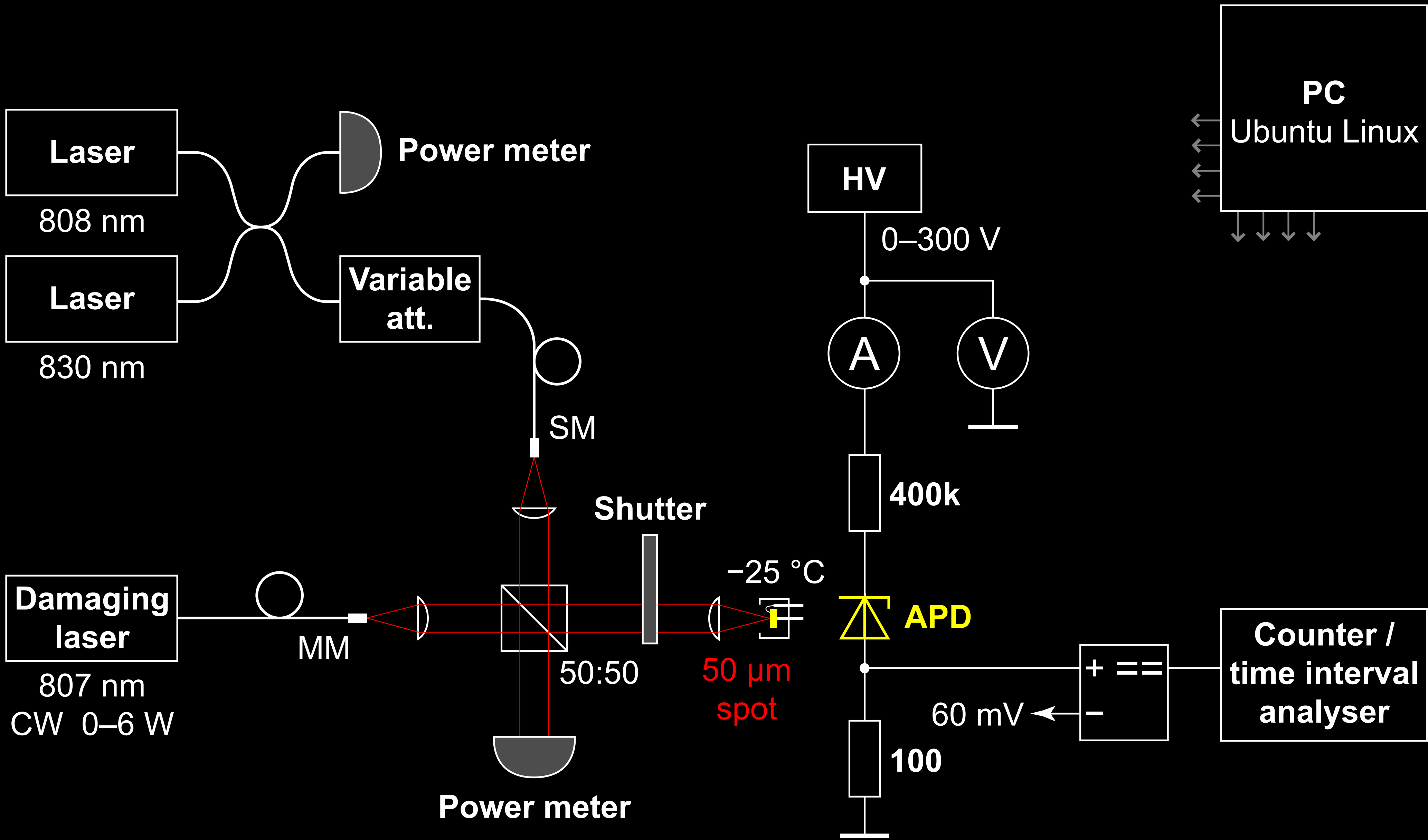



IN QKD WE TRUST
Security proof
Laws of physics & Model of eguibment
EVE
Laser damage!

Si APD PerkinElmer C30902SH

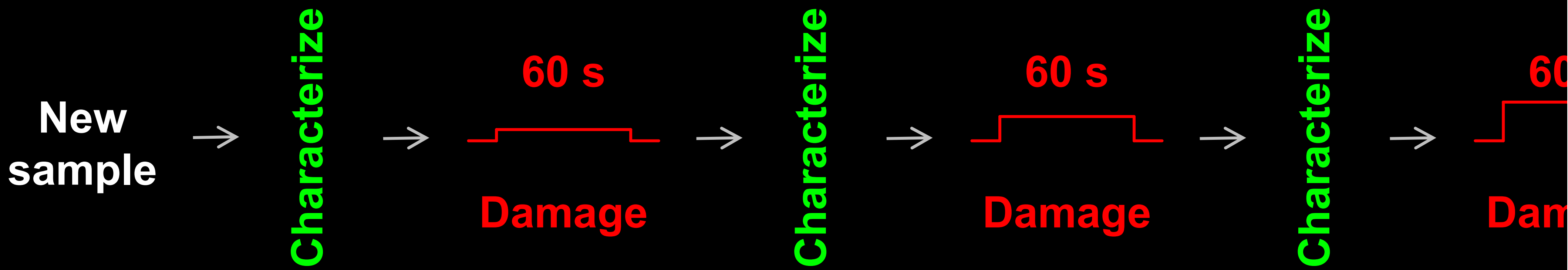


Damage and characterization setup

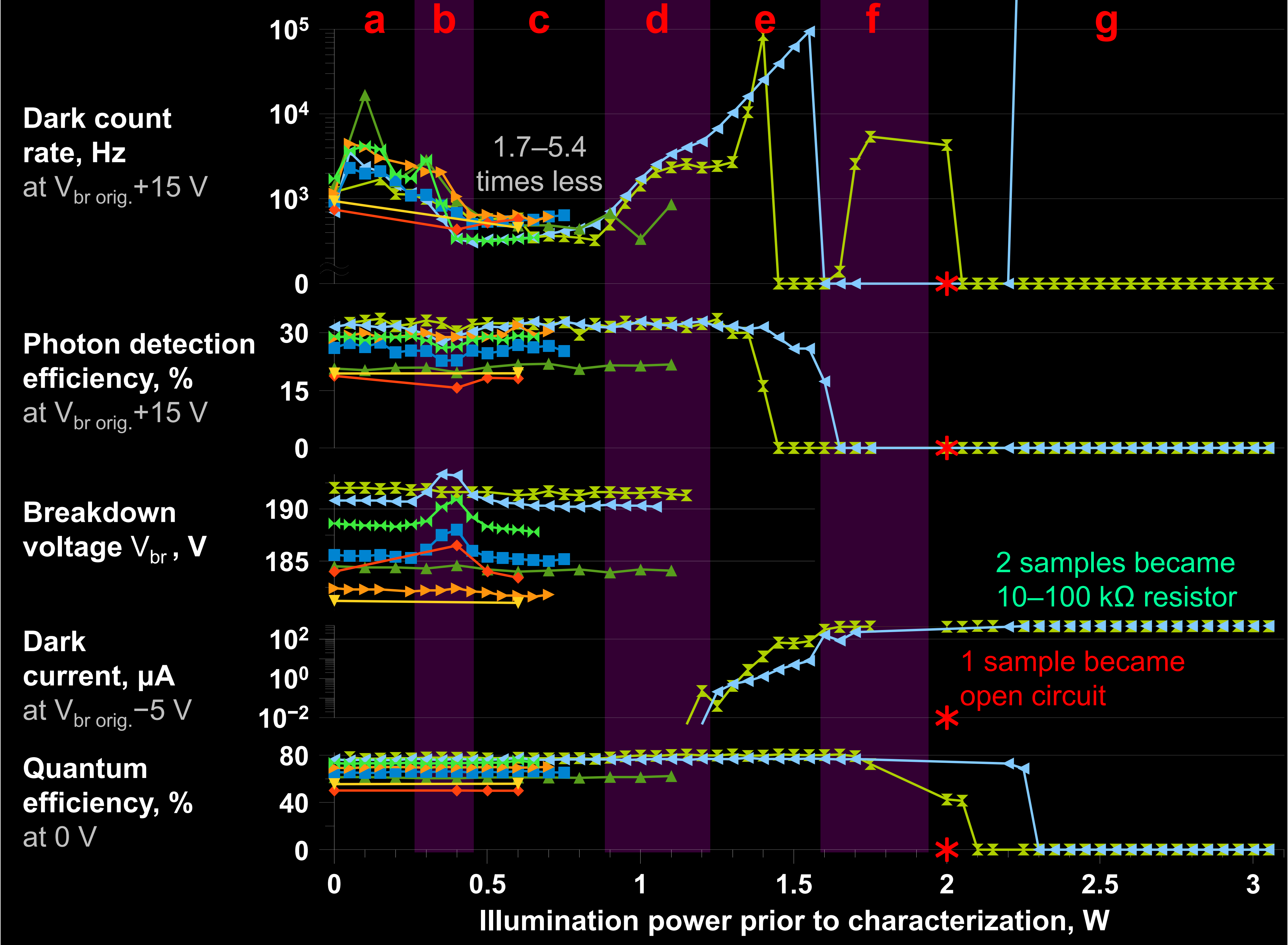


A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, V. Makarov, *unpublished*

Test sequence

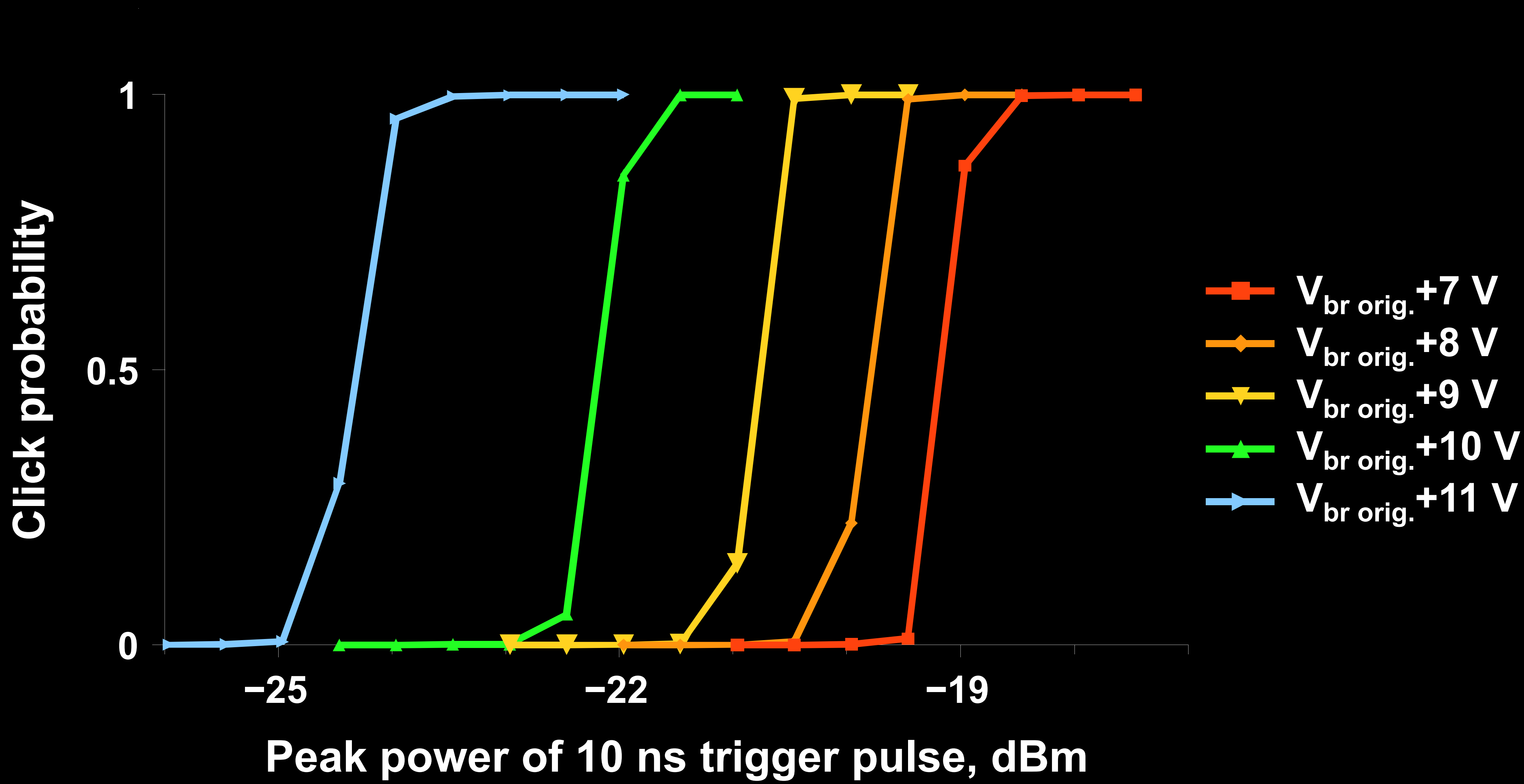


A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, V. Makarov, *unpublished*

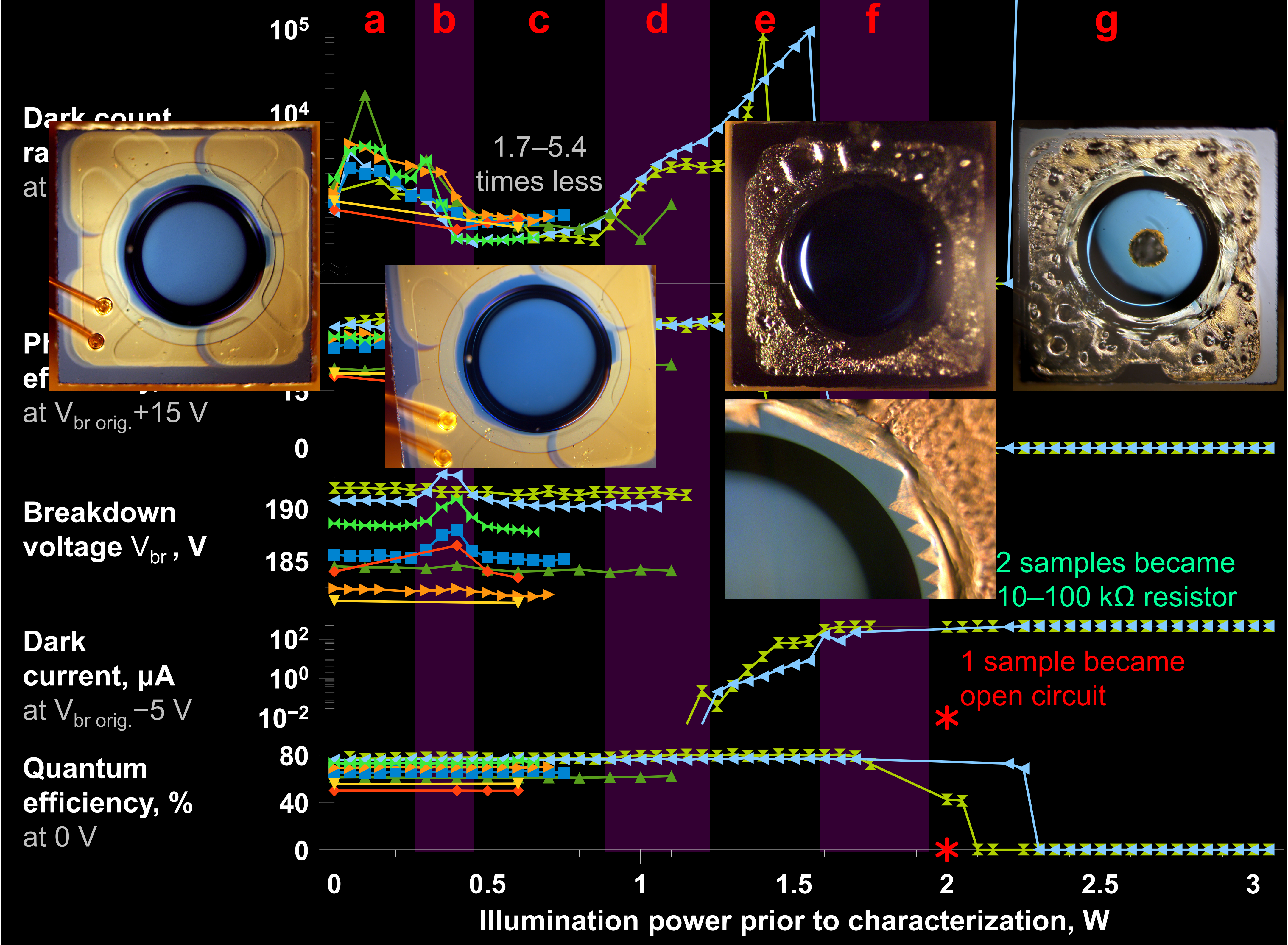


a
b
c
d
e
f
g
Dark count rate, Hz
at V br orig. +15 V
1.7–5.4 times less
Photon detection efficiency, %
at V br orig. +15 V
Breakdown voltage V br , V
2 samples became 10–100 kΩ resistor
Dark current, μA
at V br orig. −5 V
1 sample became open circuit
Quantum efficiency, %
at 0 V
Illumination power prior to characterization, W

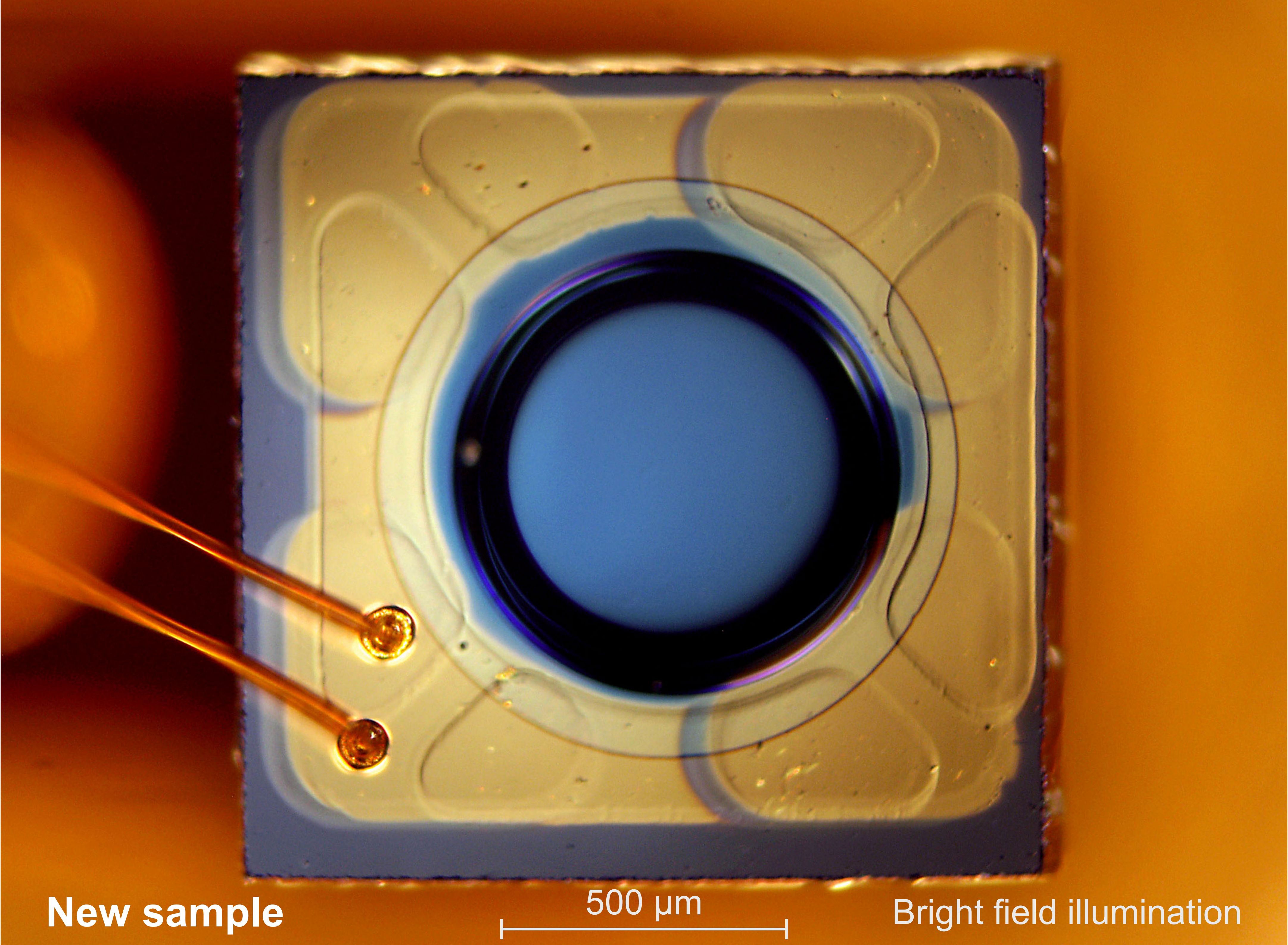
Region f: control a zombie

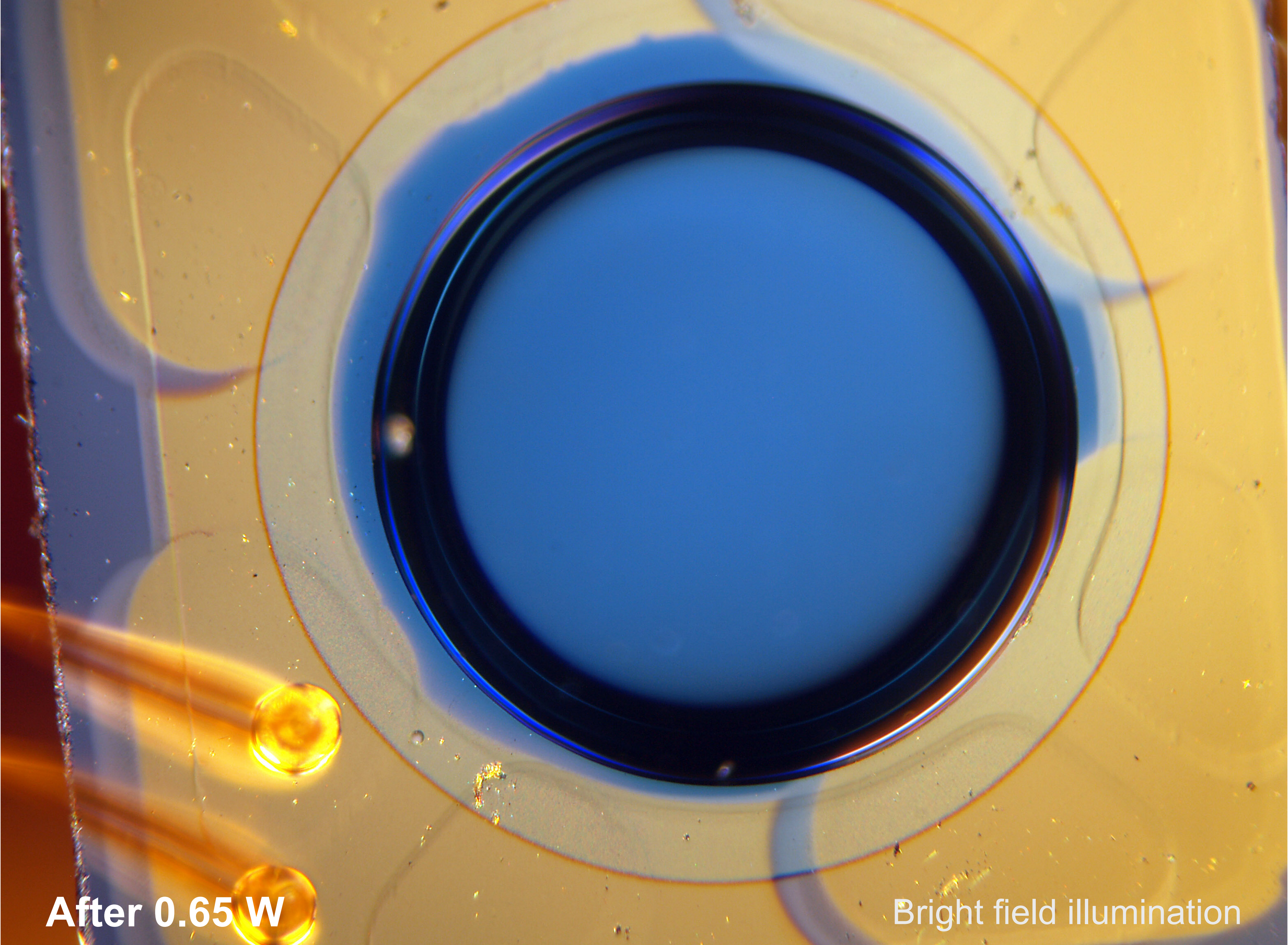


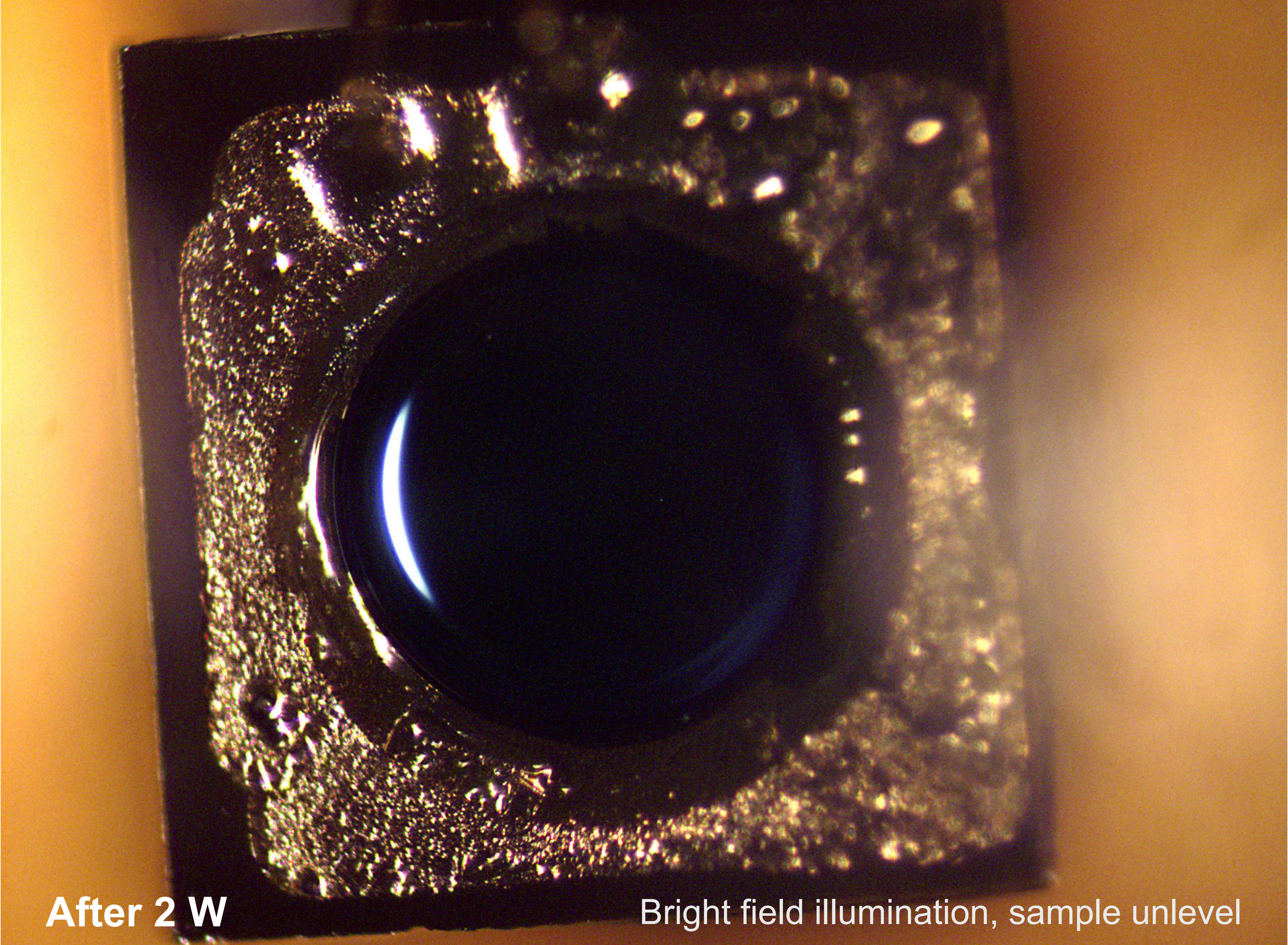
A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, V. Makarov, *unpublished*

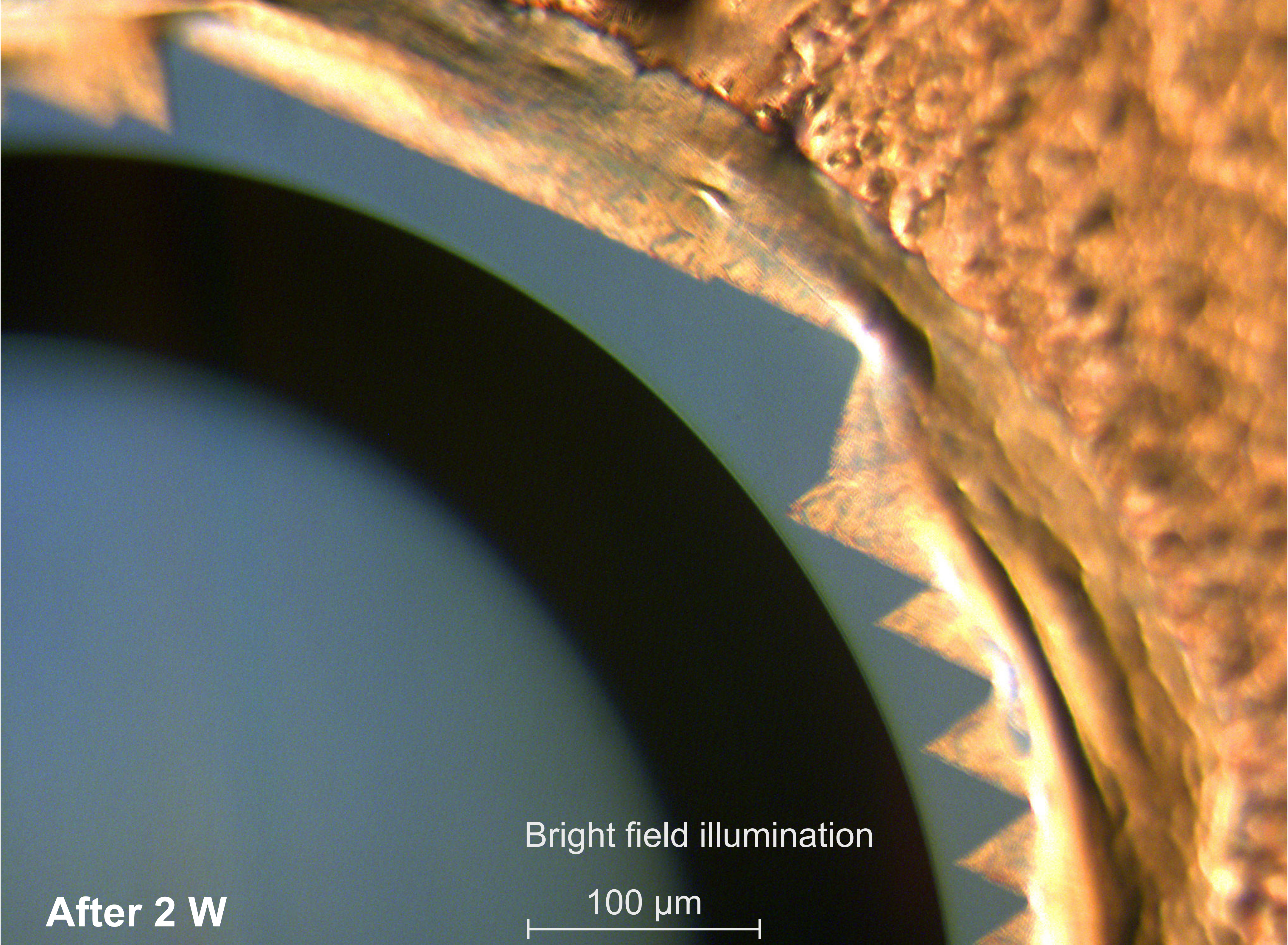


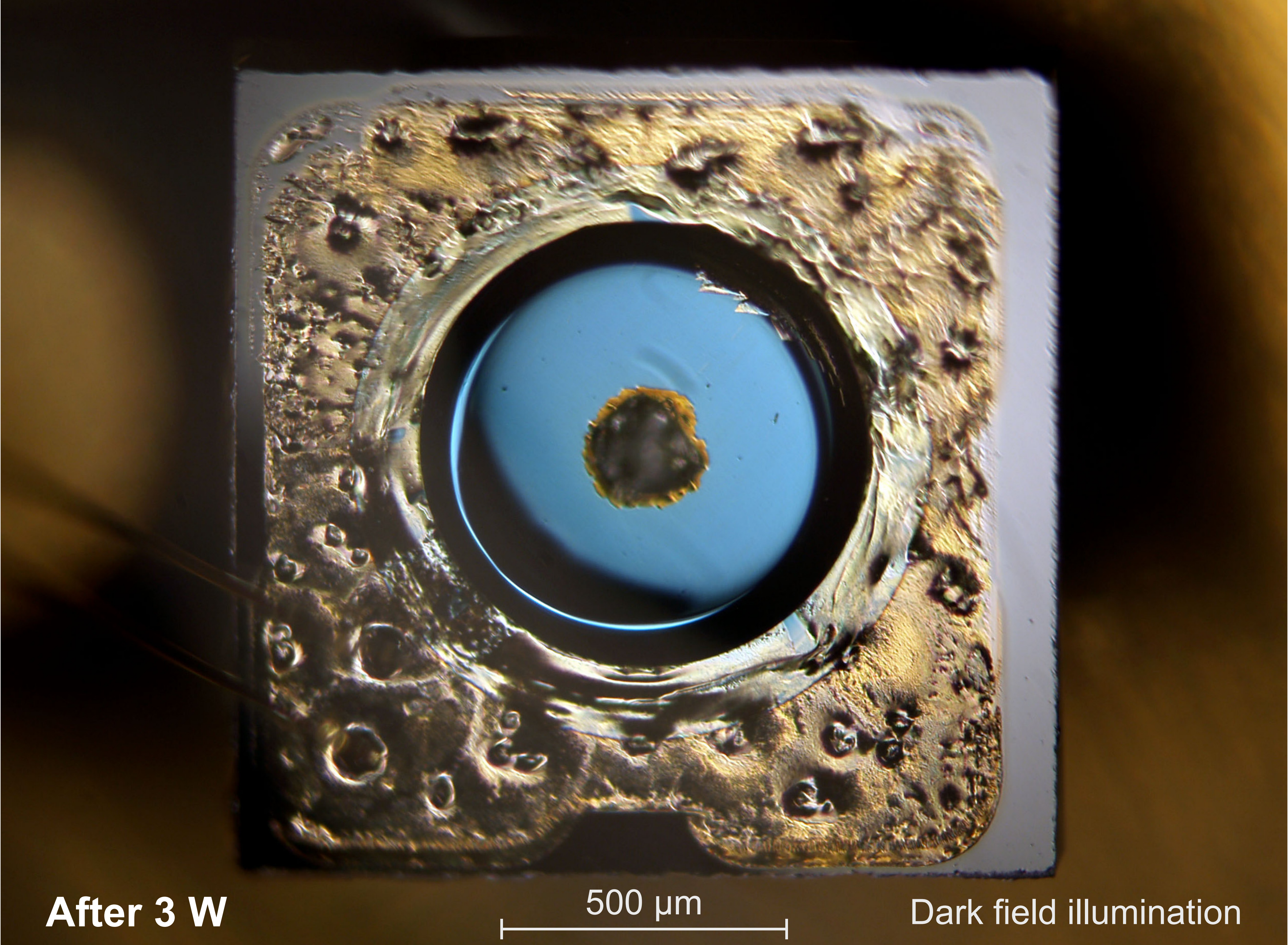
a
b
c
d
e
f
g
Dark count
ra
at
1.7–5.4
times less
Ph
ef
at V br orig. +15 V
0
Breakdown
voltage V br , V
190
185
2 samples became
10–100 kΩ resistor
Dark
current, μA
at V br orig. −5 V
1 sample became
open circuit
Quantum
efficiency, %
at 0 V
80
40
0
0
0.5
1
1.5
2
2.5
3
Illumination power prior to characterization, W


New sample
500 µm
Bright field illumination


After 0.65 W
Bright field illumination

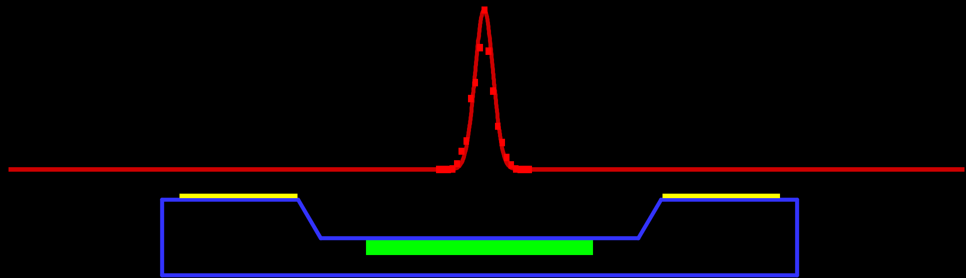

After 2 W
Bright field illumination, sample unlevel


Bright field illumination
100 µm
After 2 W

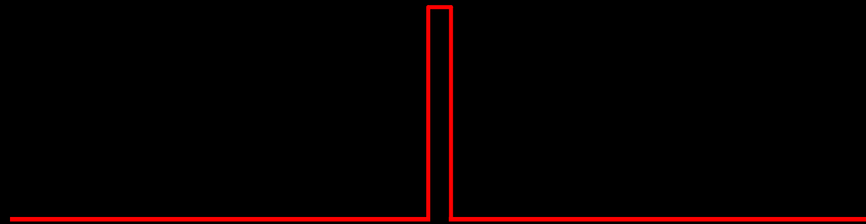

After 3 W
500 µm
Dark field illumination

Reduction of dark count rate vs. illumination profile

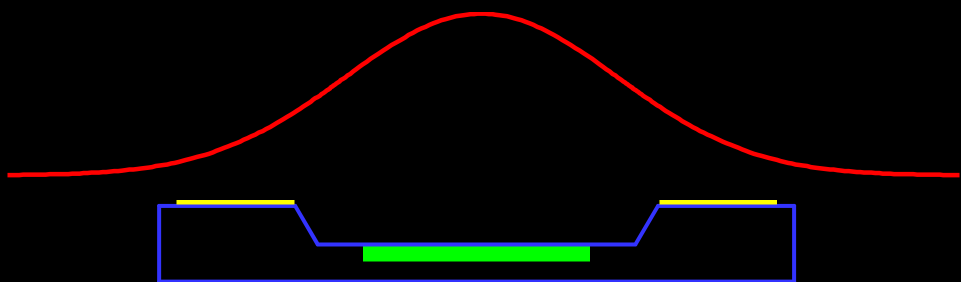
Spatial



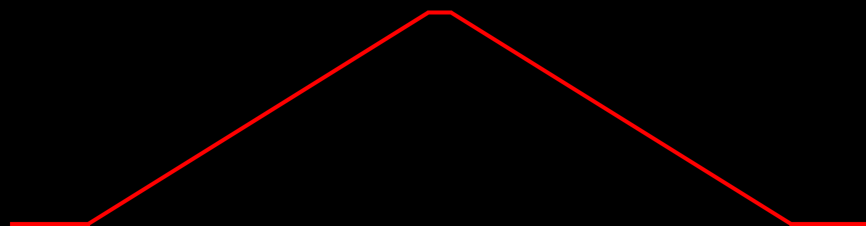
Temporal



7 samples: DC / 1.7–5.4



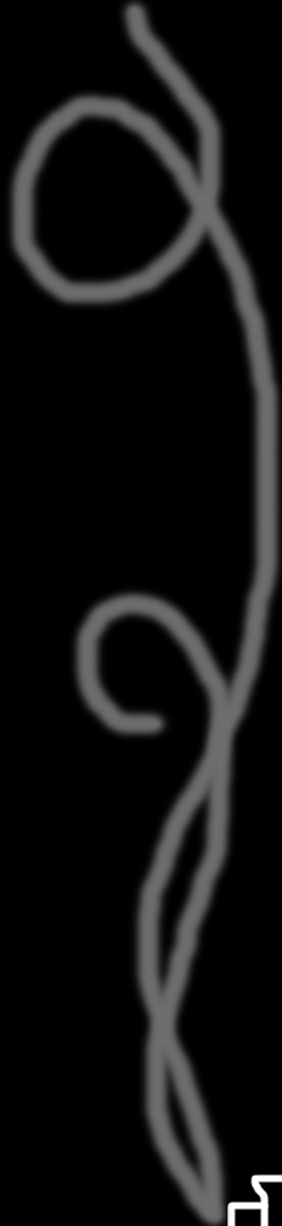
1 sample: DC / 4.2



1 sample: DC / 2.5

Localized annealing? R. H. Haitz, J. Appl. Phys. **36**, 3123 (1965)

Laser damage summary



- Demonstrated controlled laser damage to a component of QKD scheme. New mode of attack!
- PerkinElmer C30902SH Si APD:
  - Changed V_{br} and photon detection efficiency
  - Reduced dark count rate by a factor of 1.7–5.4, in all 9 samples (patent pending)
  - Permanently blind, bright-pulse control
  - Permanently blind to all light
- Future studies should test other QKD components


Qrypt 2013
CONFERENCE ON QUANTUM CRYPTOGRAPHY
2013.qcrypt.net
August 5-9
Waterloo, Canada

IQC Institute *for* Quantum Computing

Quantum hacking lab

www.vad1.com/lab