Lecture at ID Quantique 8th winter school on quantum cybersecurity, Les Diablerets, January 16–21, 2016

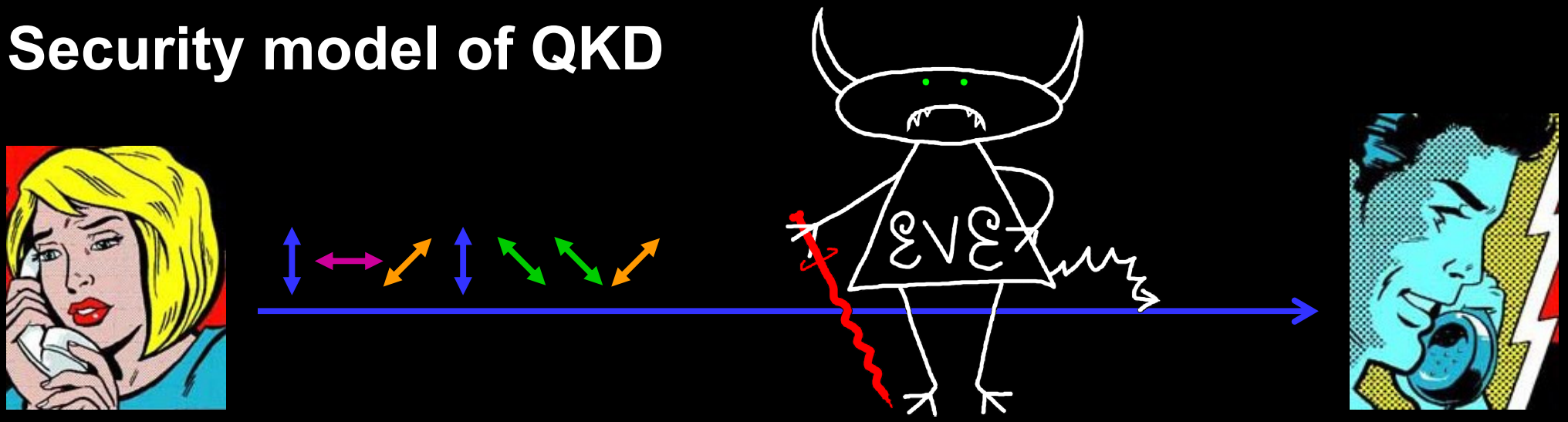
Quantum hacking

Vadim Makarov

IQC Institute *for* Quantum Computing

www.vad1.com/lab

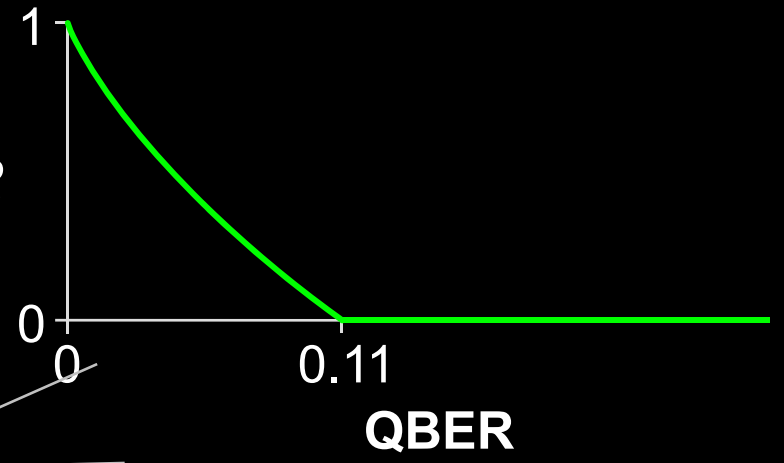
Security model of QKD

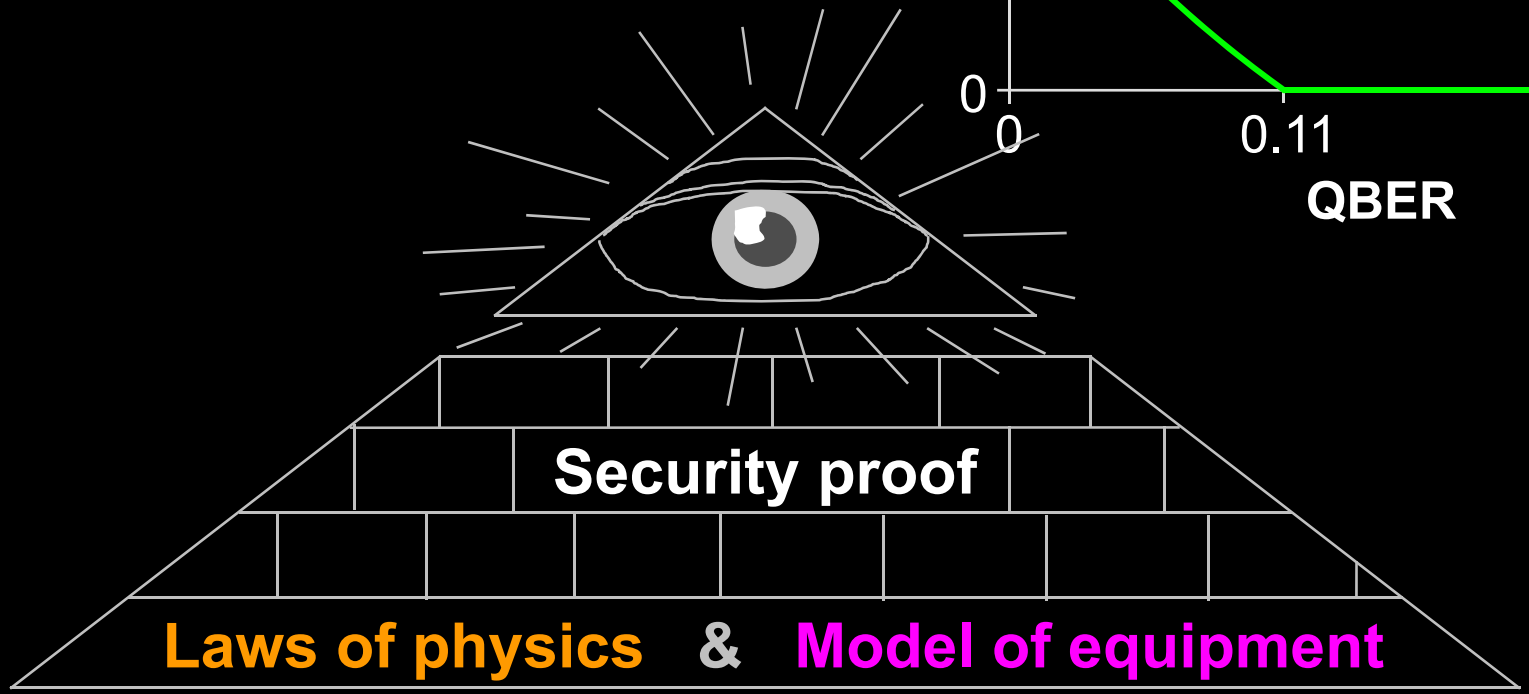


Alice

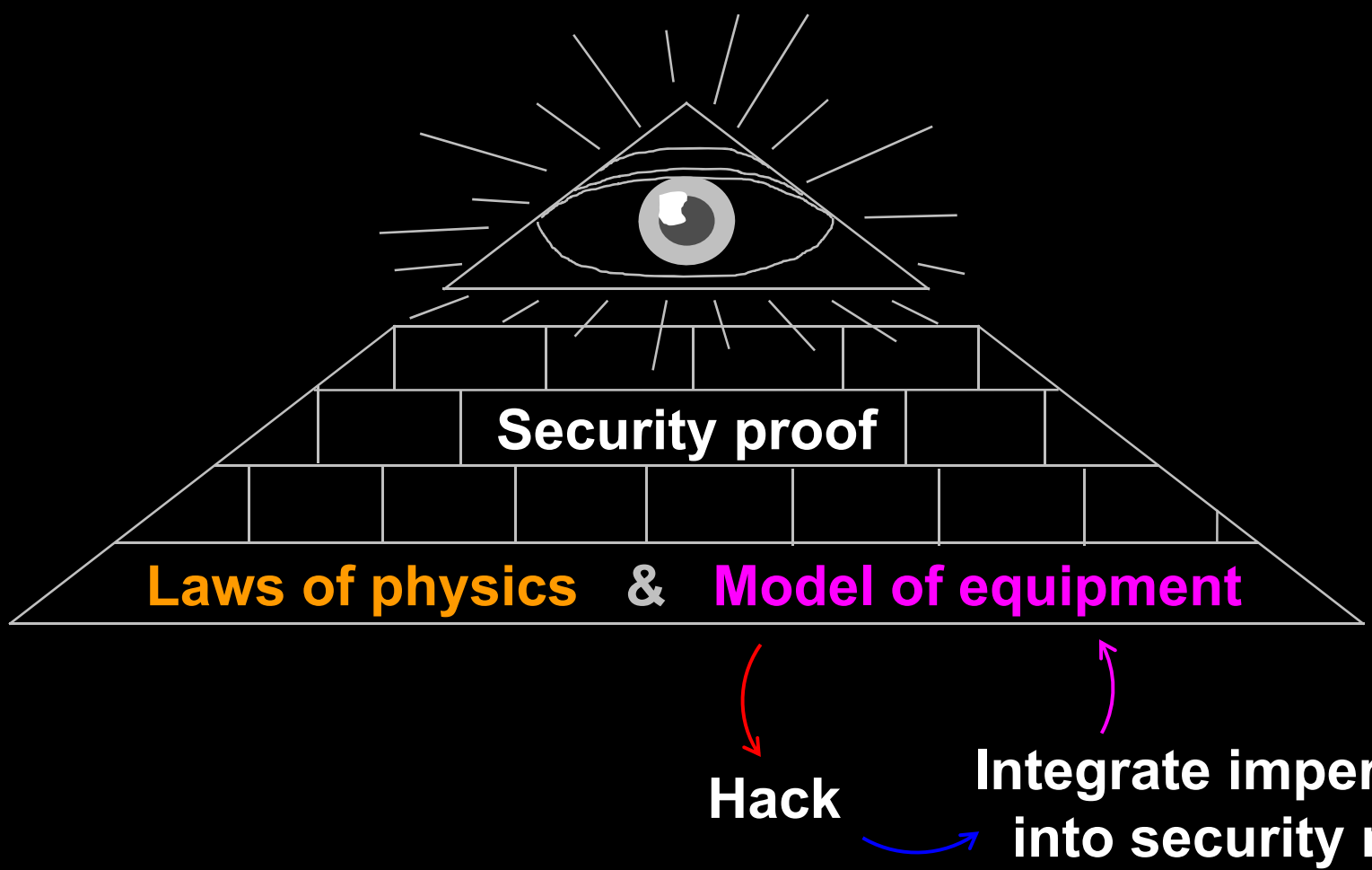
Bob

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





Security model of QKD



Example of vulnerability and countermeasures

Photon-number-splitting attack

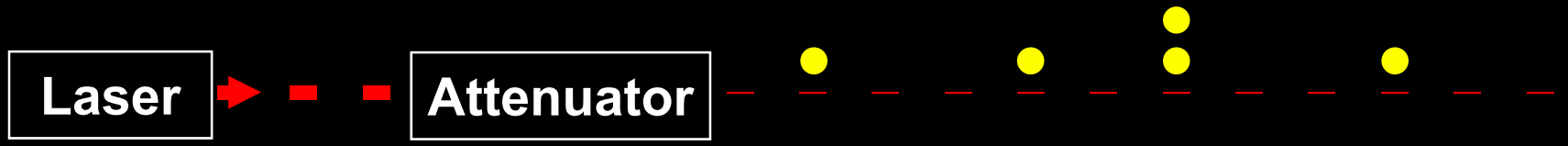
C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992)

G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000)

N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000)

S. Félix, N. Gisin, A. Stefanov, H. Zbinden, J. Mod. Opt. **48**, 2009 (2001)

N. Lütkenhaus, M. Jahma, New J. Phys. **4**, 44 (2002)



★ Decoy-state protocol

W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003)

★ SARG04 protocol

V. Scarani, A. Acín, G. Ribordy, N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004)

★ Distributed-phase-reference protocols

K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002)

K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. A. **68**, 022317 (2003)

N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, V. Scarani, arXiv:quant-ph/0411022v1 (2004)

Attack	Target component	Tested system
Laser damage V. Makarov *et al.,* arXiv:1510.03148	any	ID Quantique, research system
Spatial efficiency mismatch M Rau *et al.,* IEEE J. Quantum Electron. **21**, 6600905 (2015); S. Sajeed *et al.,* Phys. Rev. A **91**, 062301 (2015)	receiver optics	research system
Pulse energy calibration S. Sajeed *et al.,* Phys. Rev. A **91**, 032326 (2015)	classical watchdog detector	ID Quantique
Trojan-horse I. Khan *et al.,* presentation at QCrypt (2014)	phase modulator in Alice	SeQureNet
Trojan-horse N. Jain *et al.,* New J. Phys. **16**, 123030 (2014)	phase modulator in Bob	ID Quantique*
Detector saturation H. Qin, R. Kumar, R. Alleaume, Proc. SPIE 88990N (2013)	homodyne detector	SeQureNet
Shot-noise calibration P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A **87**, 062313 (2013)	classical sync detector	SeQureNet
Wavelength-selected PNS M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A **86**, 032310 (2012)	intensity modulator	(theory)
Multi-wavelength H.-W. Li *et al.,* Phys. Rev. A **84**, 062308 (2011)	beamsplitter	research system
Deadtime H. Weier *et al.,* New J. Phys. **13**, 073024 (2011)	single-photon detector	research system
Channel calibration N. Jain *et al.,* Phys. Rev. Lett. **107**, 110501 (2011)	single-photon detector	ID Quantique
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011)	Faraday mirror	(theory)
Detector control I. Gerhardt *et al.,* Nat. Commun. **2**, 349 (2011); L. Lydersen *et al.,* Nat. Photonics **4**, 686 (2010)	single-photon detector	ID Quantique, MagiQ, research system

* Attack did not break security of the tested system, but may be applicable to a different implementation.

Commercial QKD

ID Quantique *Cerberis* system

Classical encryptors:

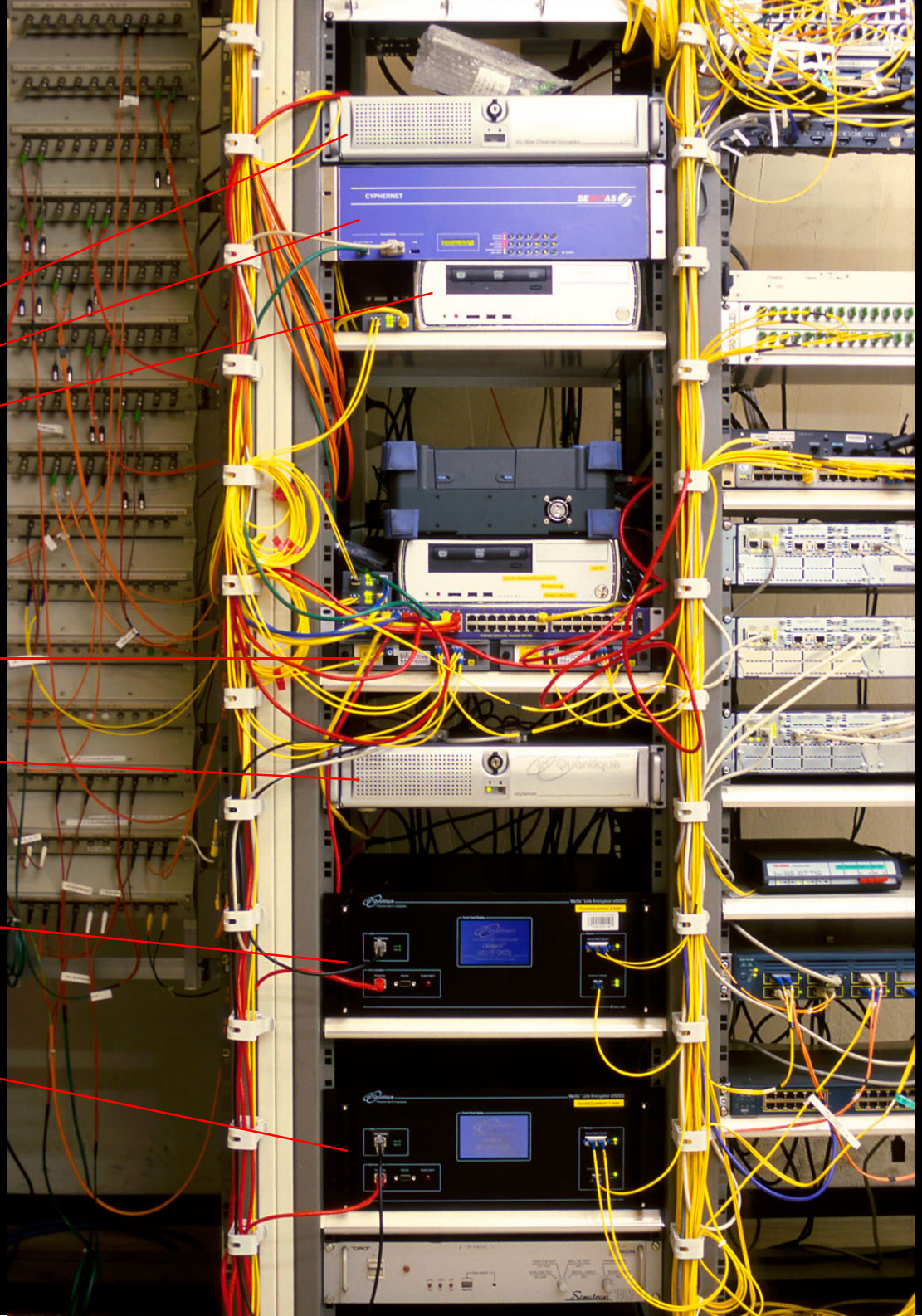
L2, 2 Gbit/s
L2, 10 Gbit/s
L3 VPN, 100 Mbit/s

WDMs

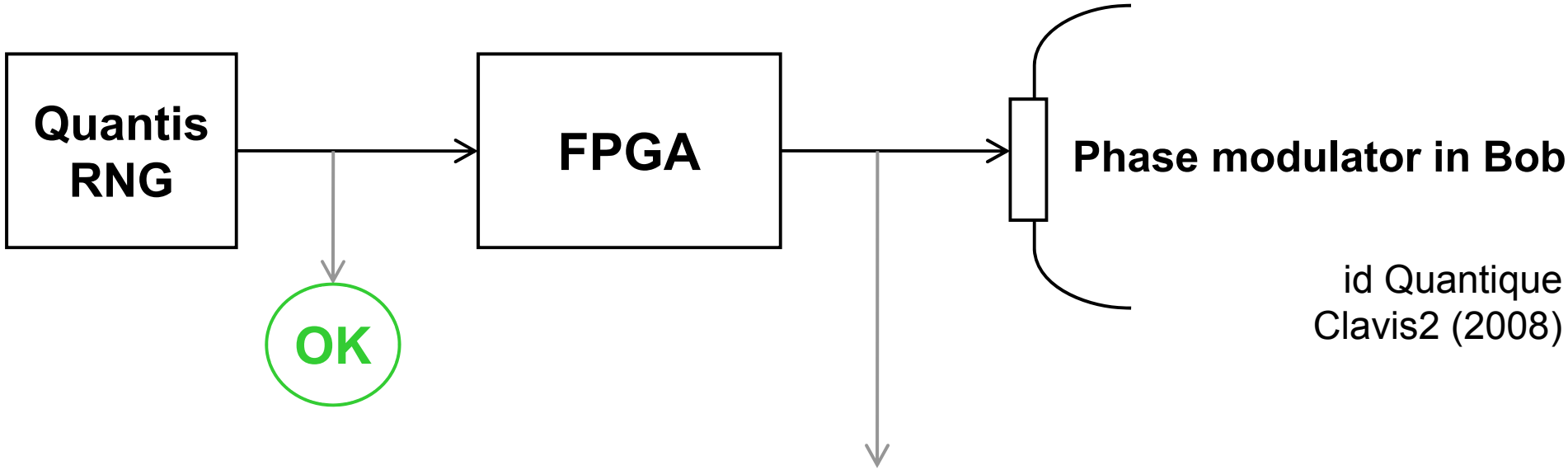
Key manager

QKD to another node (4 km)

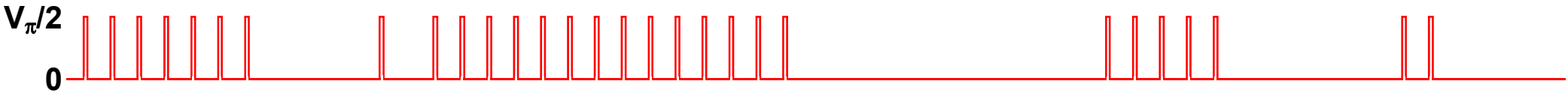
QKD to another node (14 km)



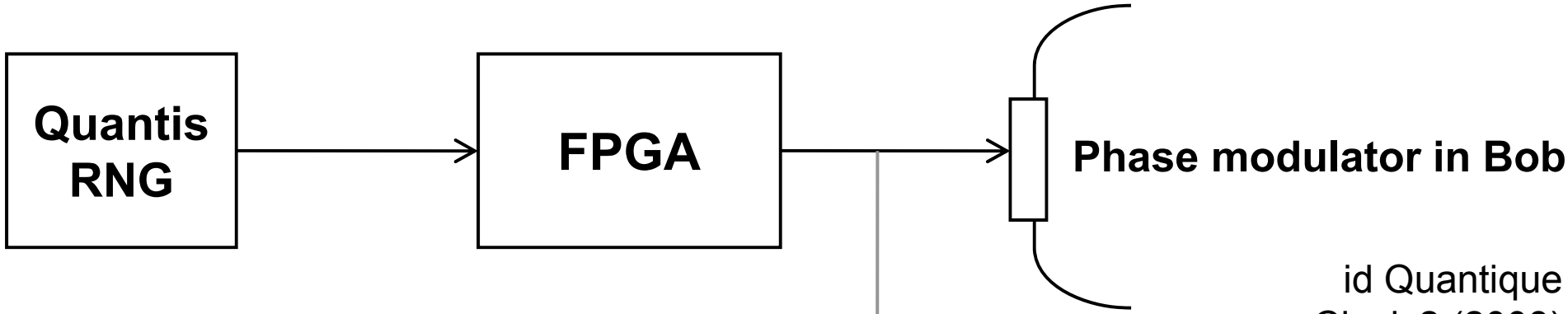
True randomness?



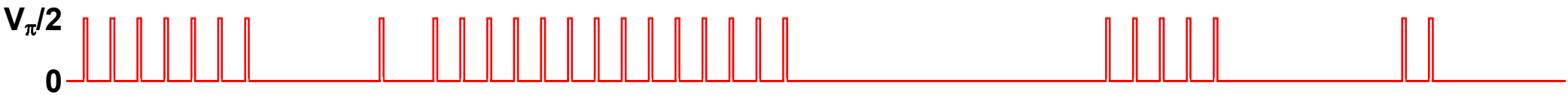
id Quantique
Clavis2 (2008)



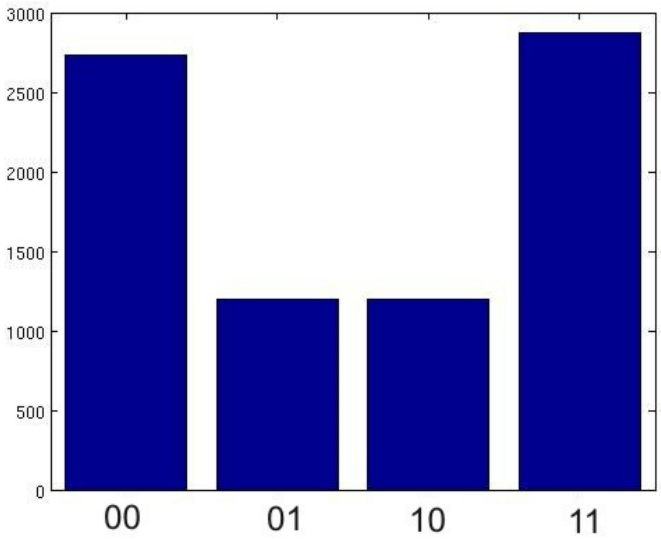
True randomness?



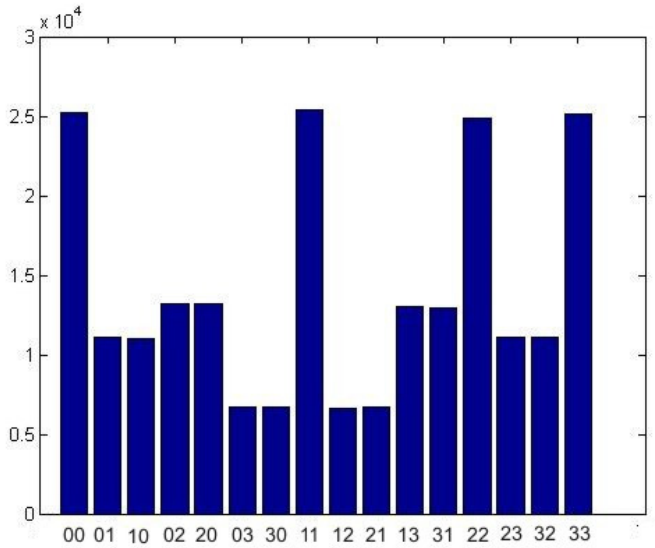
id Quantique
Clavis2 (2008)



Bob:



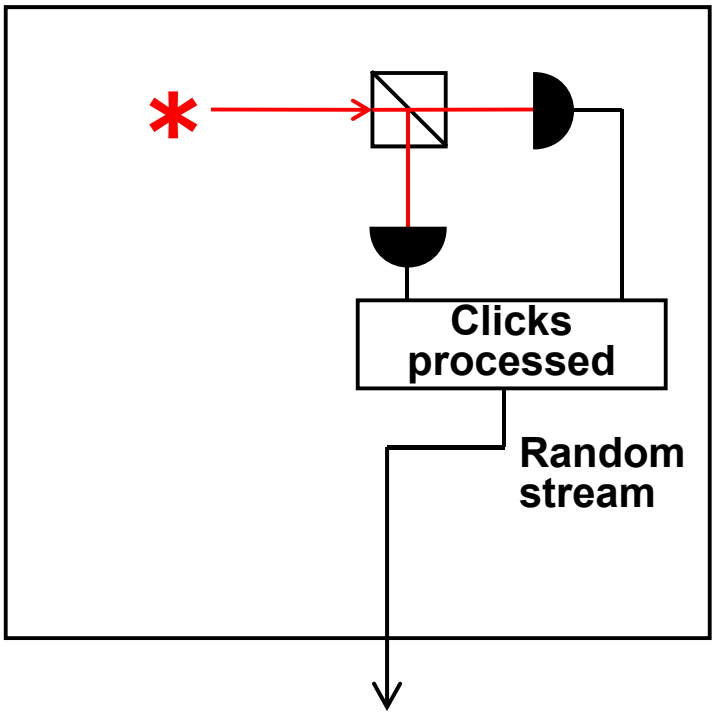
Alice:



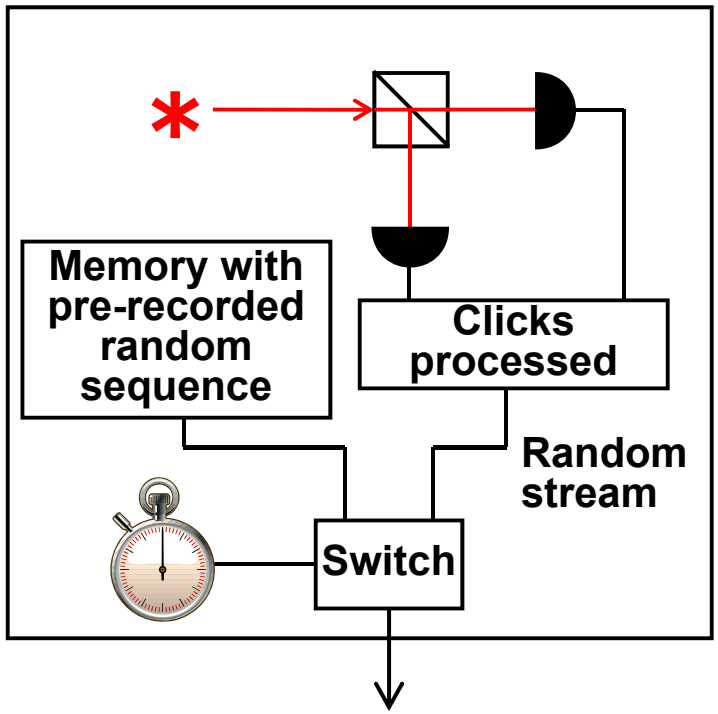
Issue reported patched in 2010

Do we trust the manufacturer?

Quantis RNG



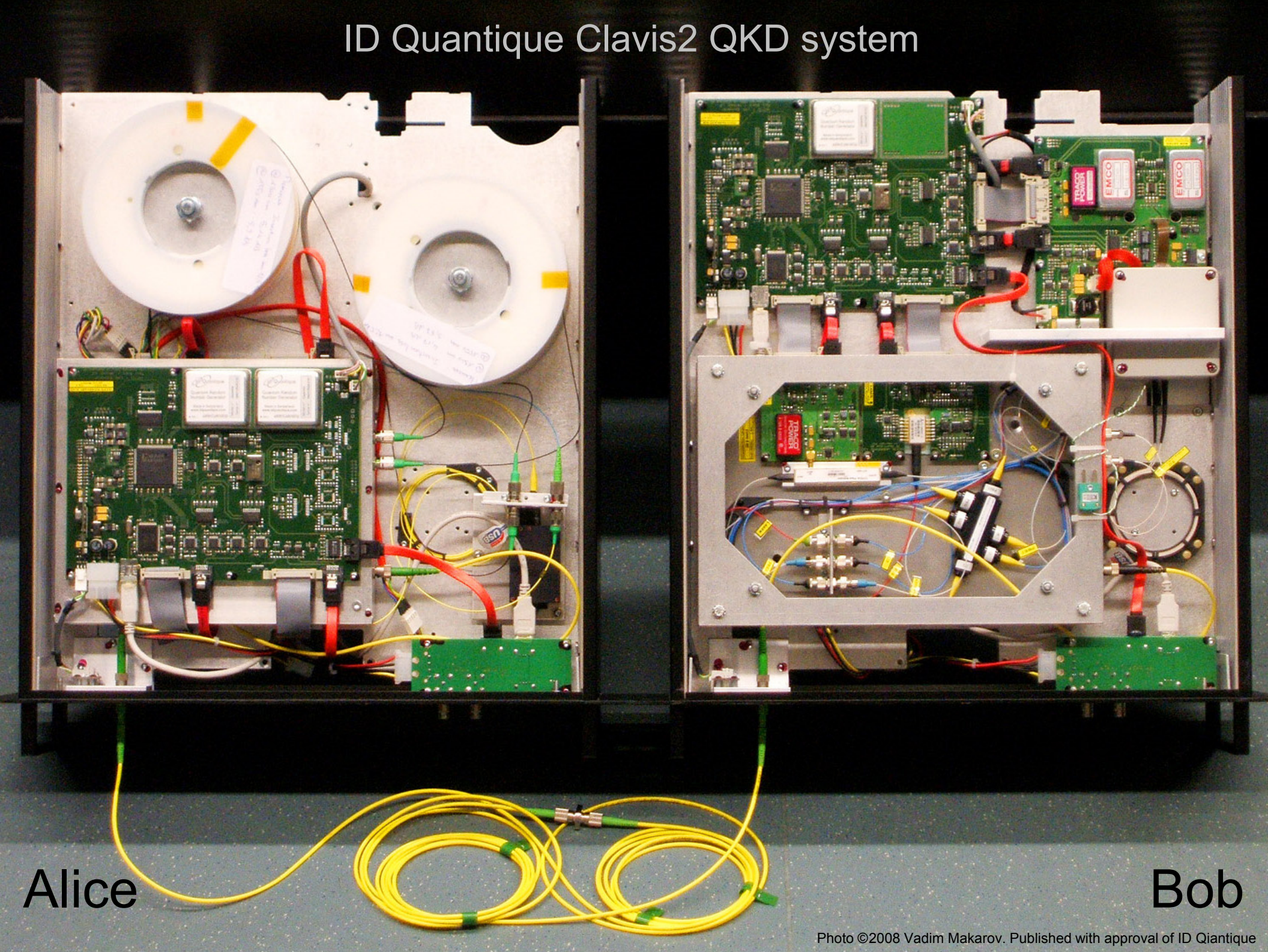
Quantis RNG, Trojan-horsed :)



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

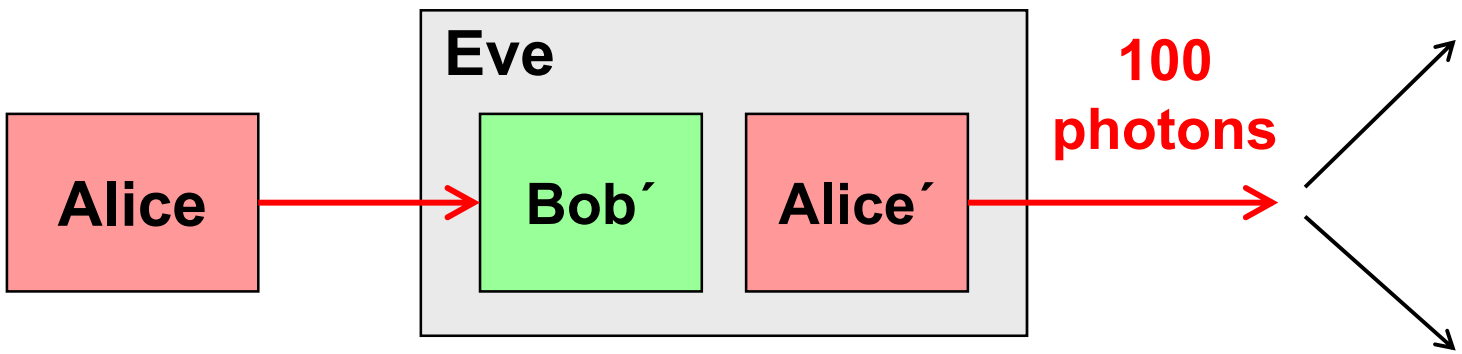


Double clicks

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

Discard them?

Intercept-resend attack... with a twist:



Bob:

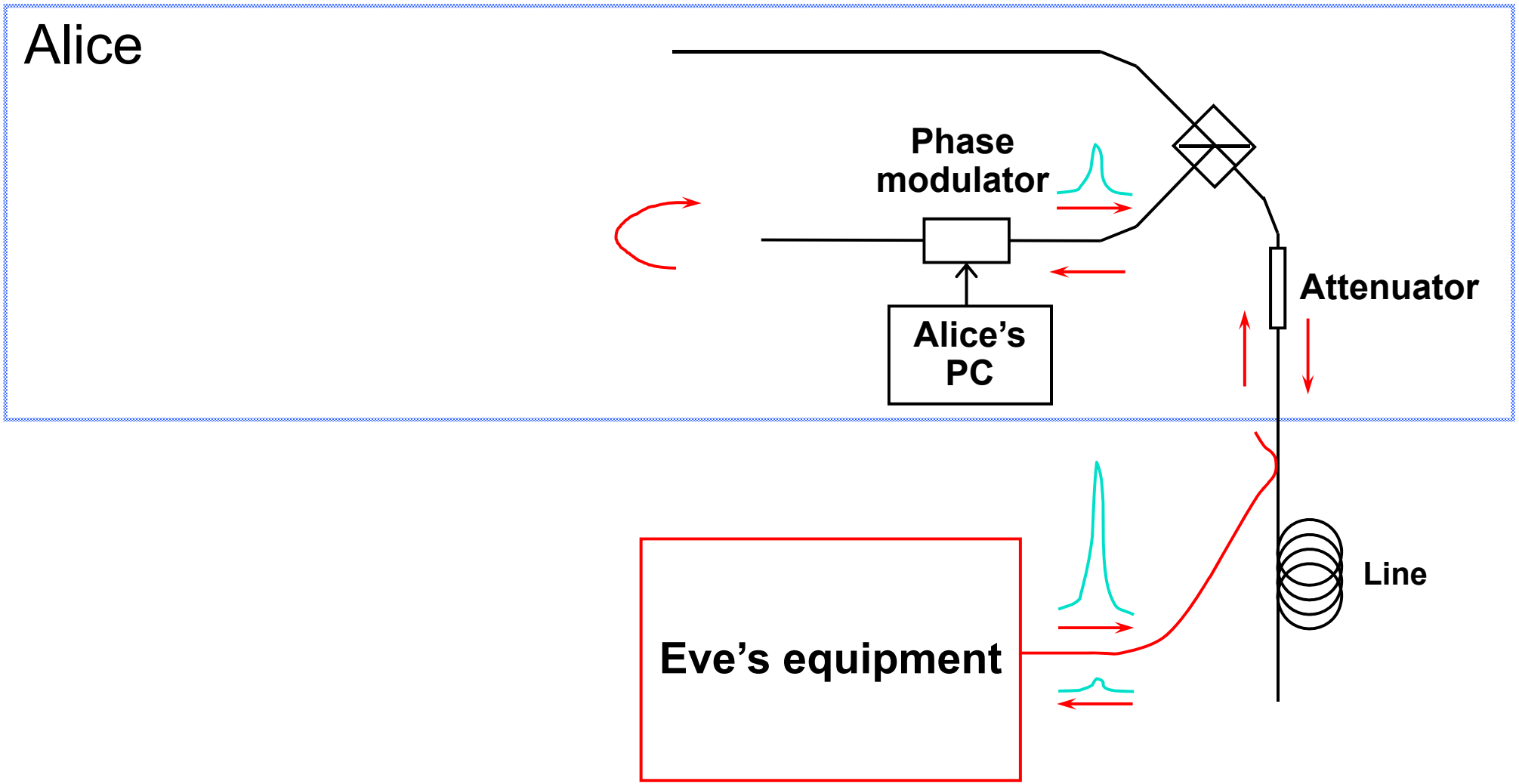
Detects in Eve's basis: single click

Detects in conjugate basis: double click, discarded

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

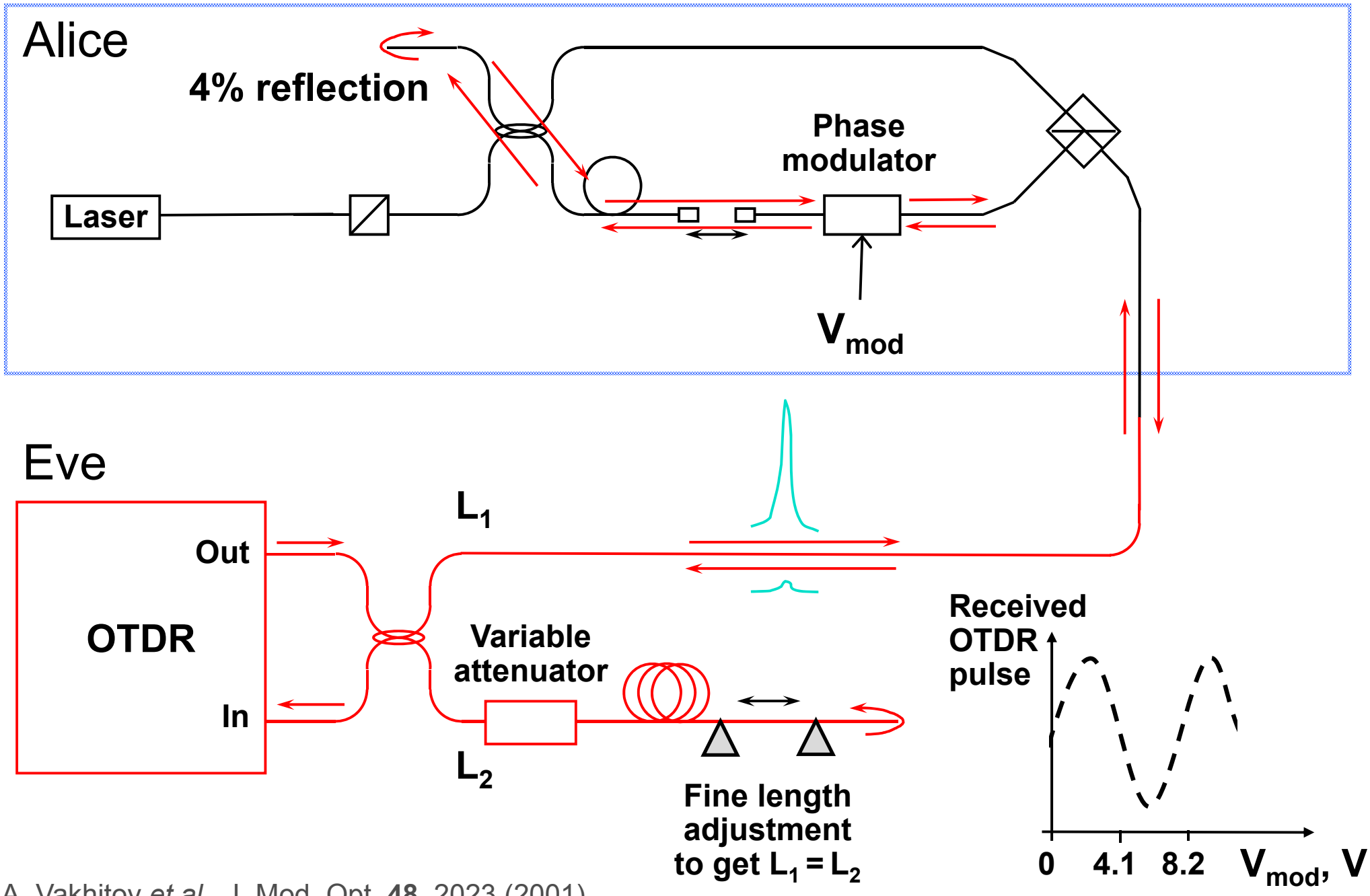
N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999)
T. Tsurumaru & K. Tamaki, Phys. Rev. A **78**, 032302 (2008)

Trojan-horse attack

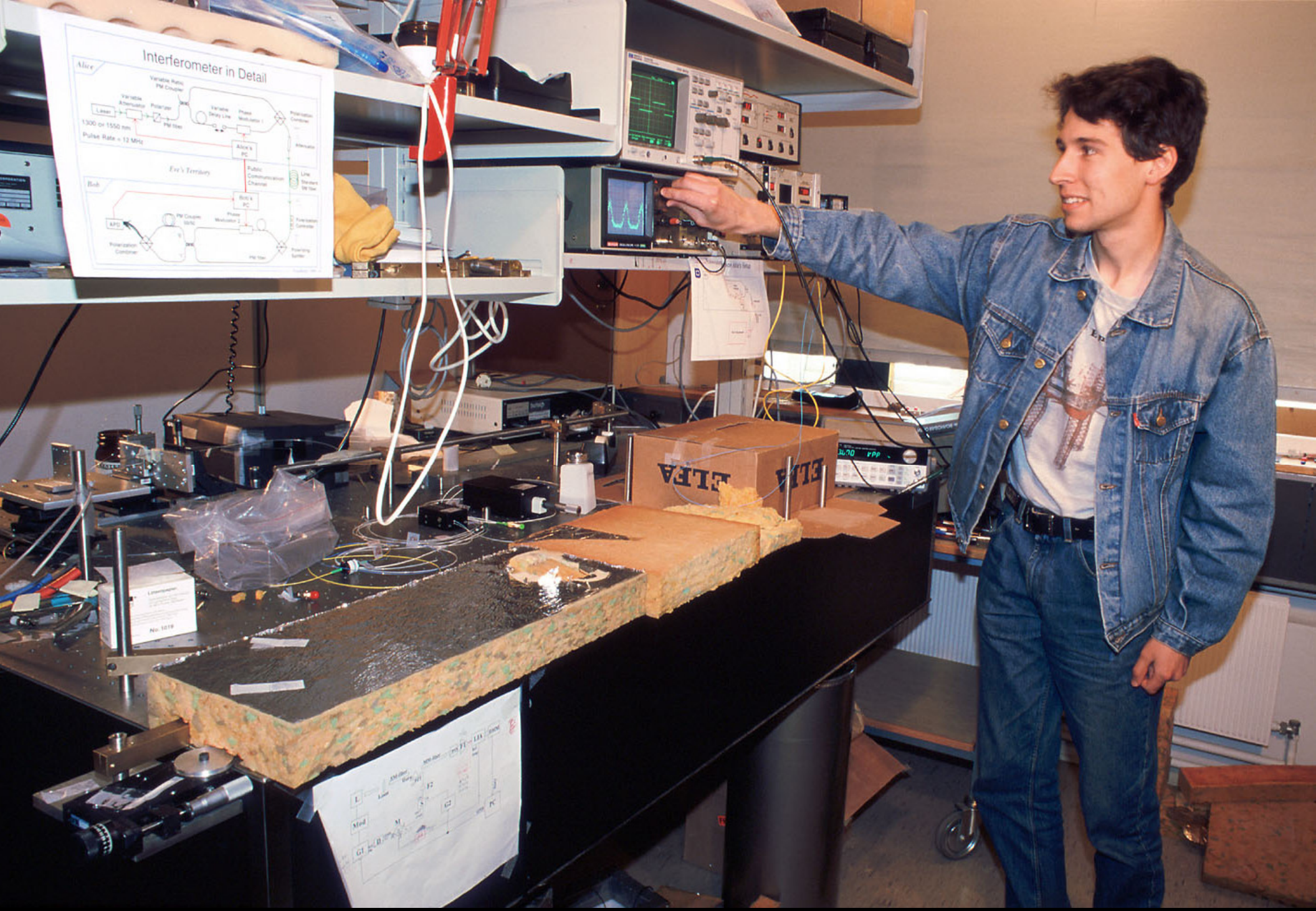


– interrogating Alice's phase modulator with powerful external pulses (can give Eve bit values directly)

Trojan-horse attack experiment

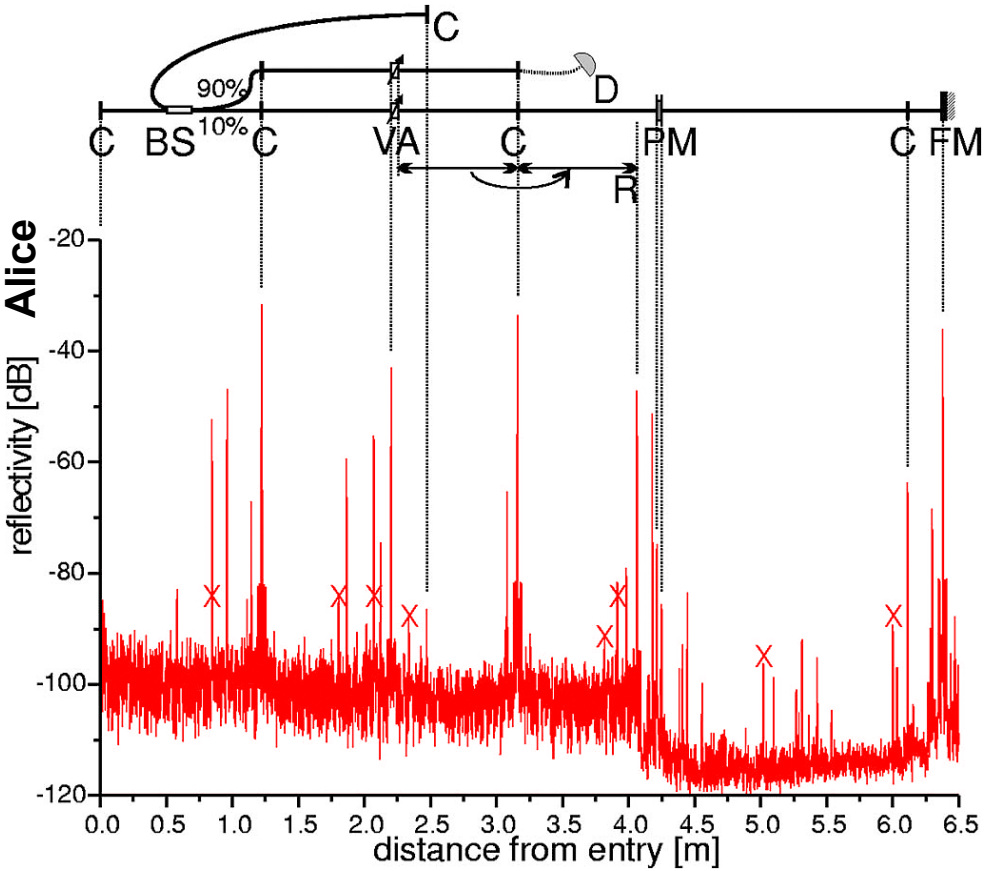


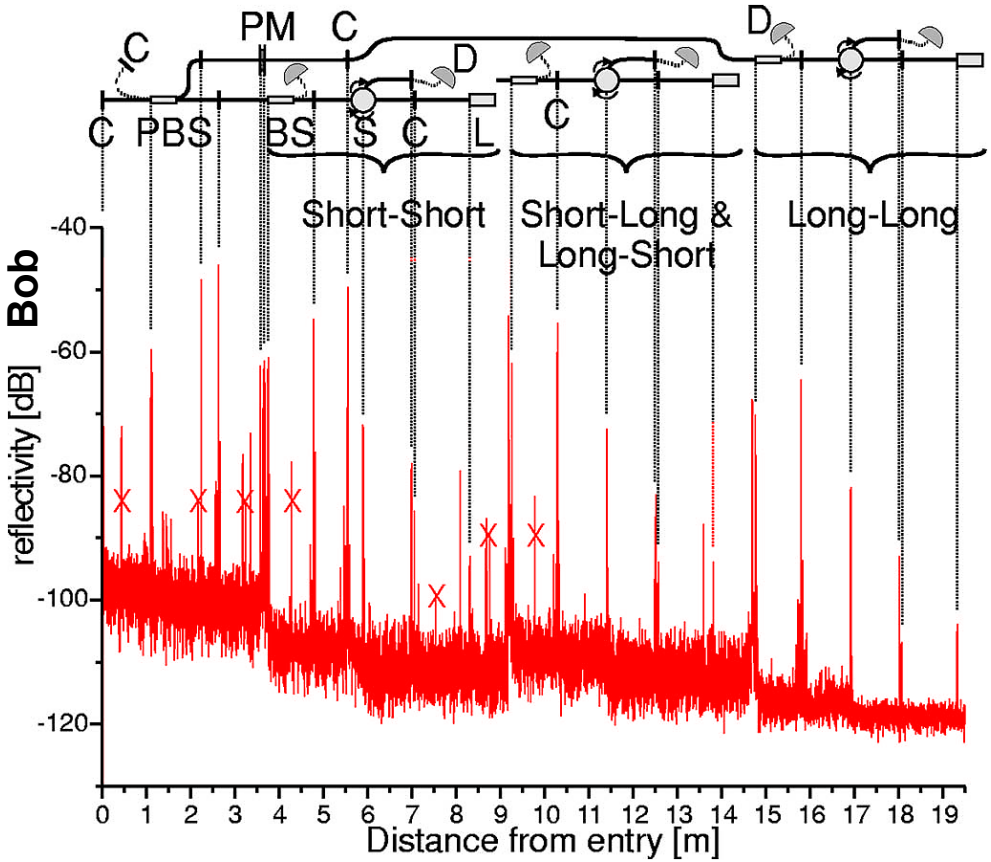
A. Vakhitov *et al.*, J. Mod. Opt. **48**, 2023 (2001)



Artem Vakhitov tunes up Eve's setup

Trojan-horse attack for plug-and-play system

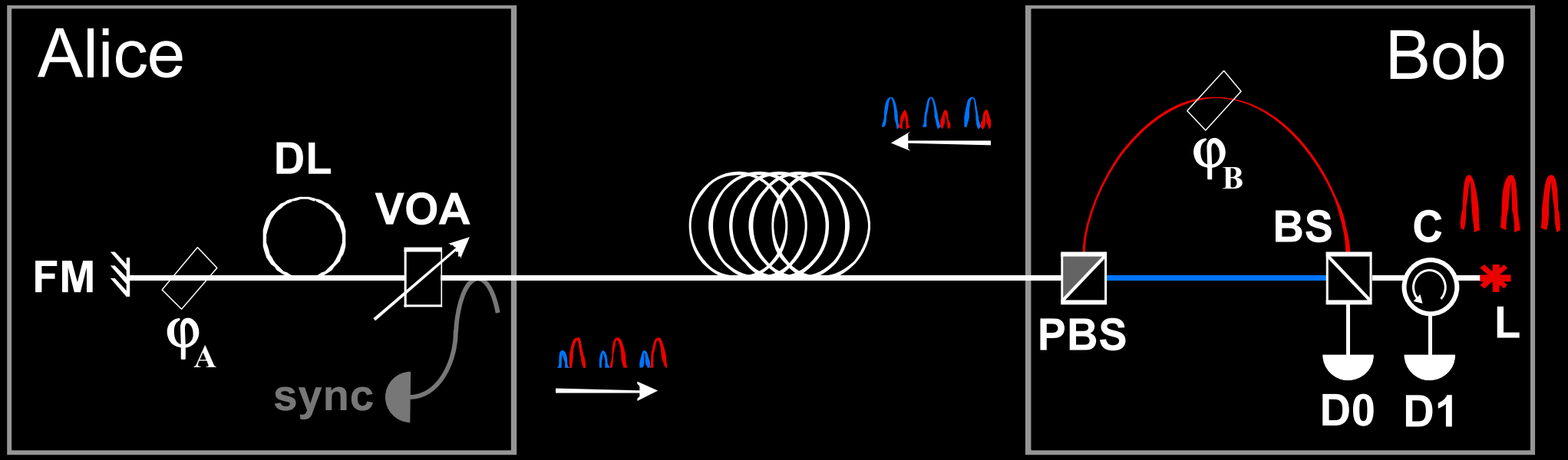




Eve gets back one photon → in principle, extracts 100% information

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

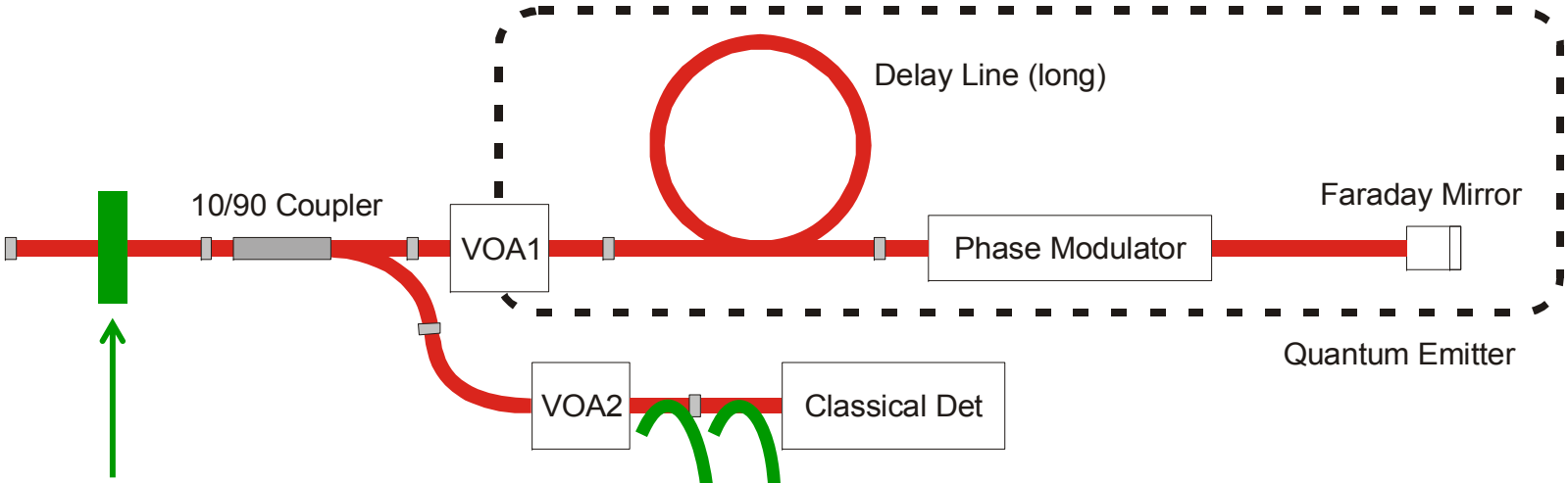
Countermeasures?



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

Countermeasures for plug-and-play system

Alice:



1. Add narrowband (~1 nm) filter

2. Add CW and pulse energy monitoring detectors

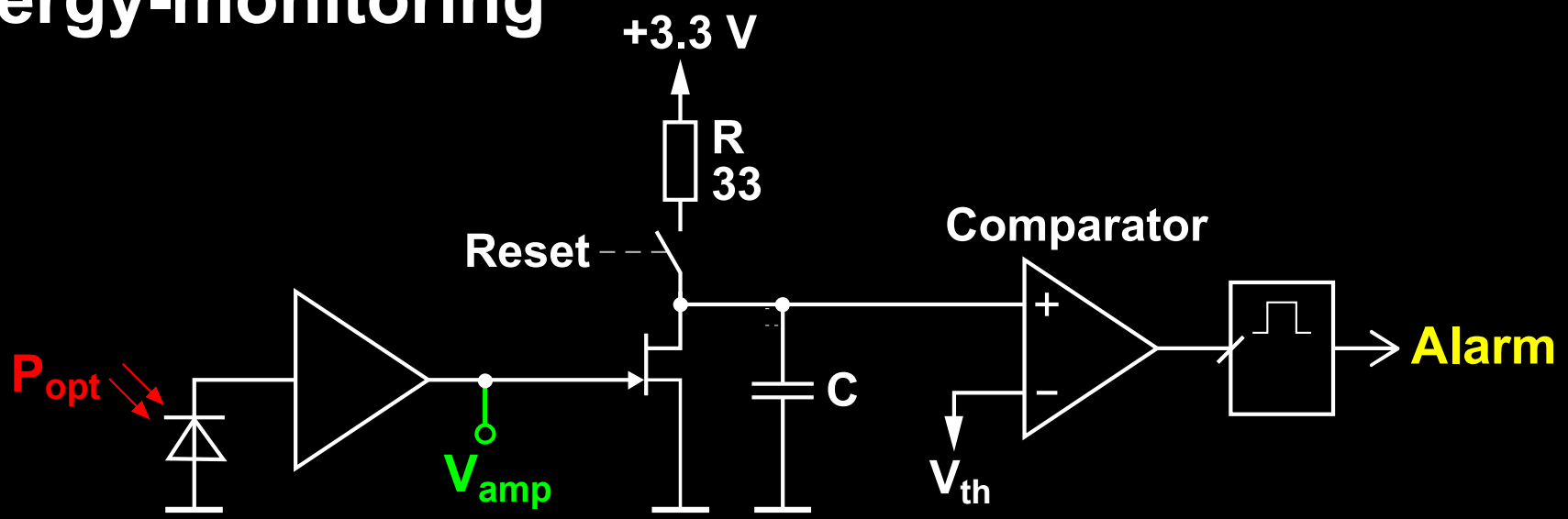
S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

Bob: none

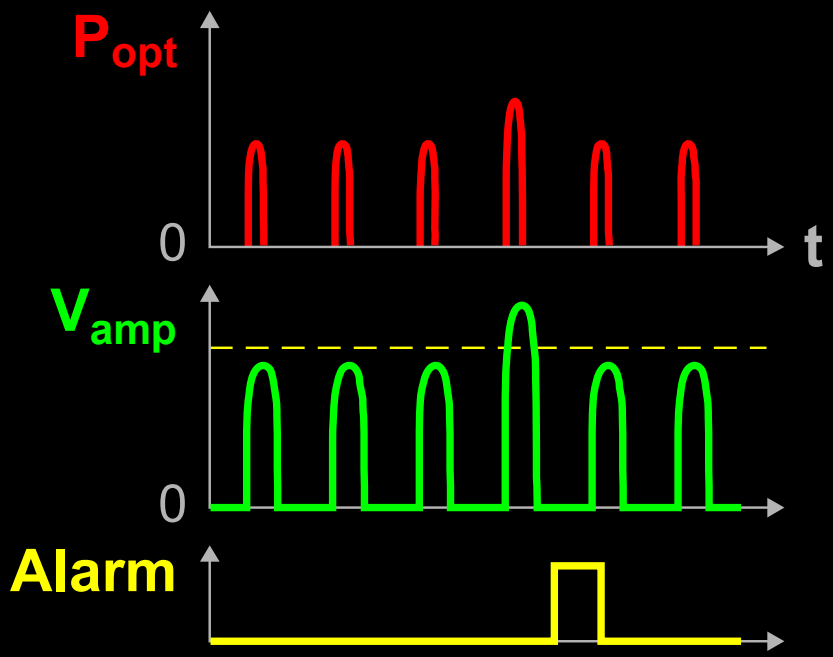
(one consequence: SARG protocol may be insecure)

N. Jain *et al.*, New J. Phys. **16**, 123030 (2014)

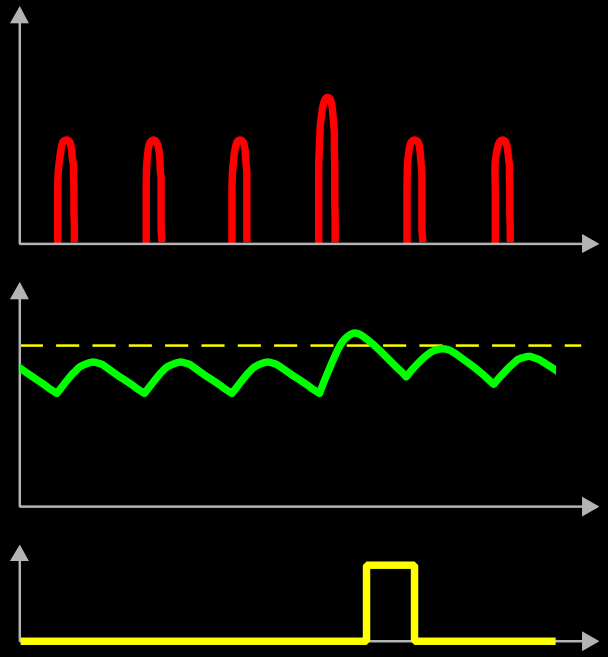
Pulse-energy-monitoring detector



Theory:

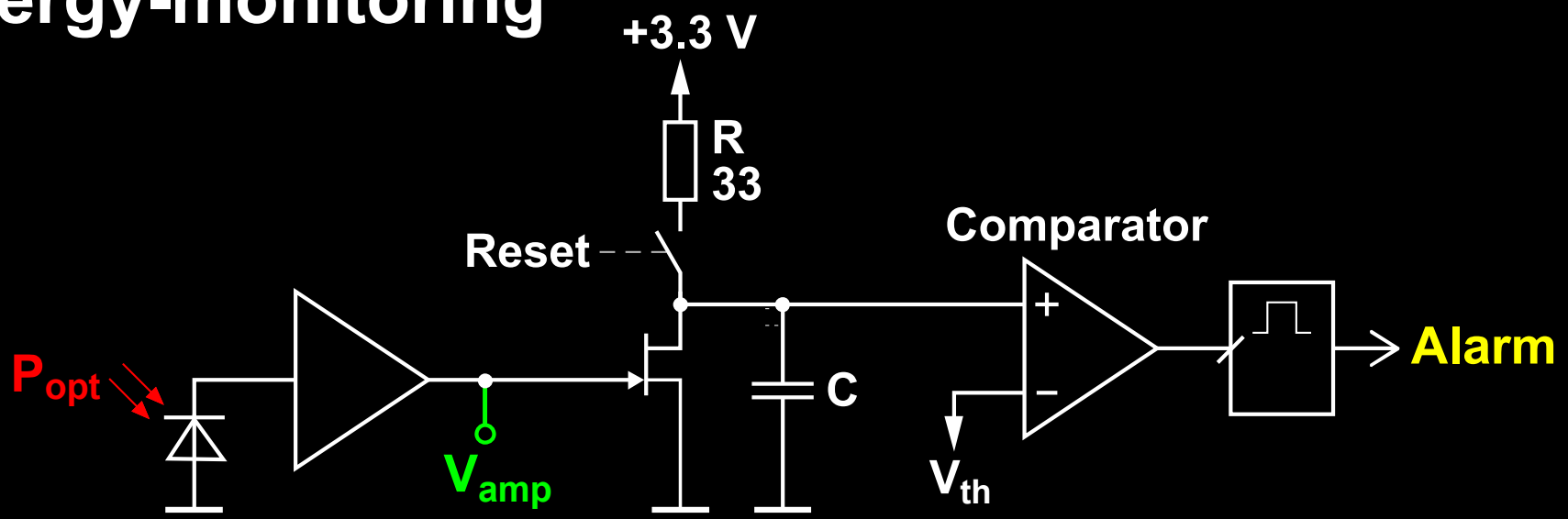


Implementation:

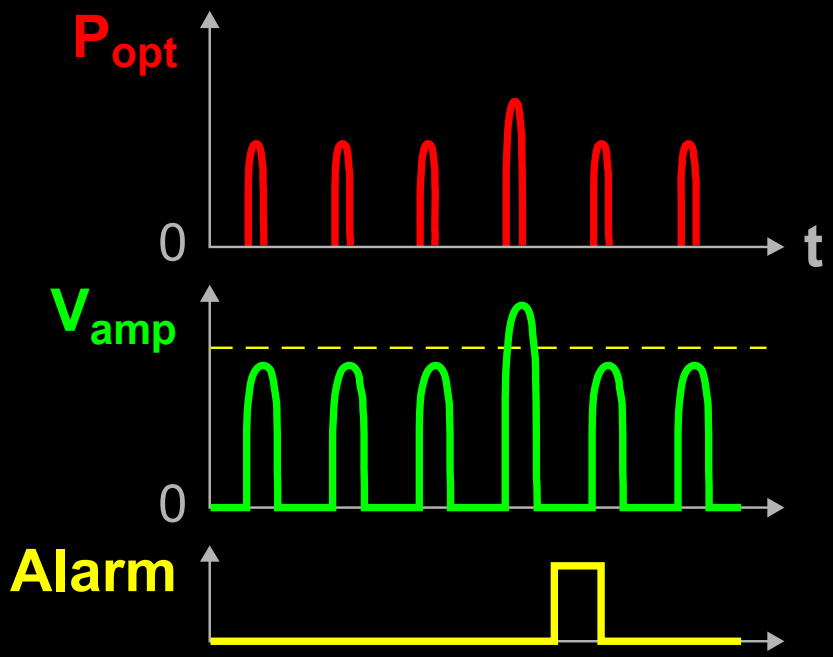


S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

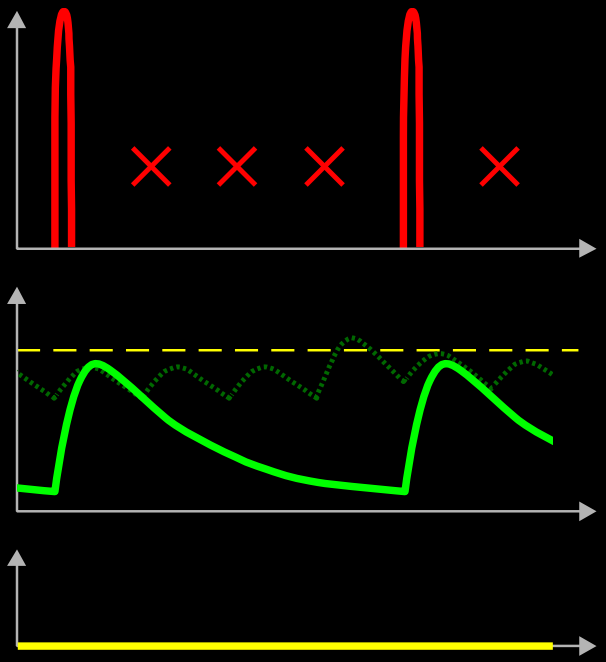
Pulse-energy-monitoring detector



Theory:

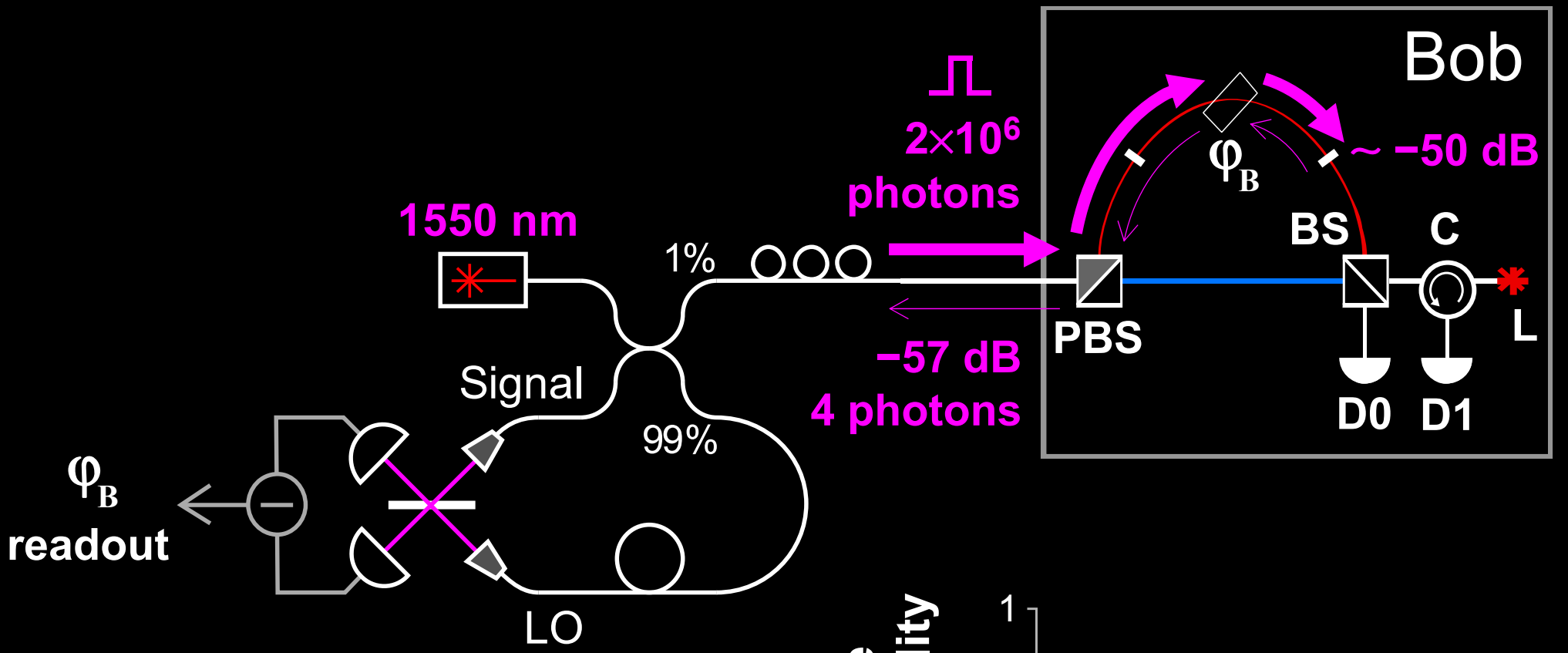


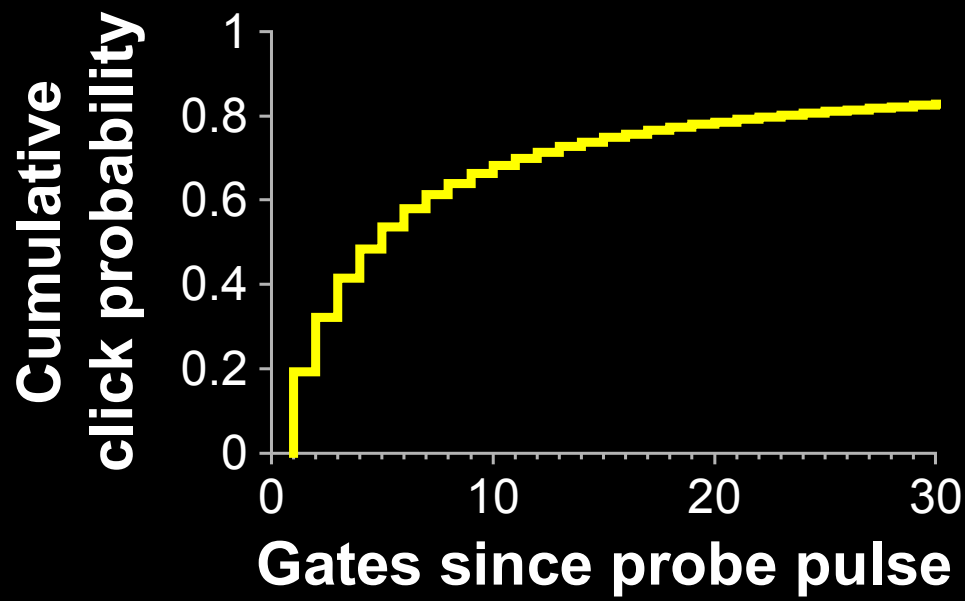
Attack:



S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

Trojan-horse attack on Bob

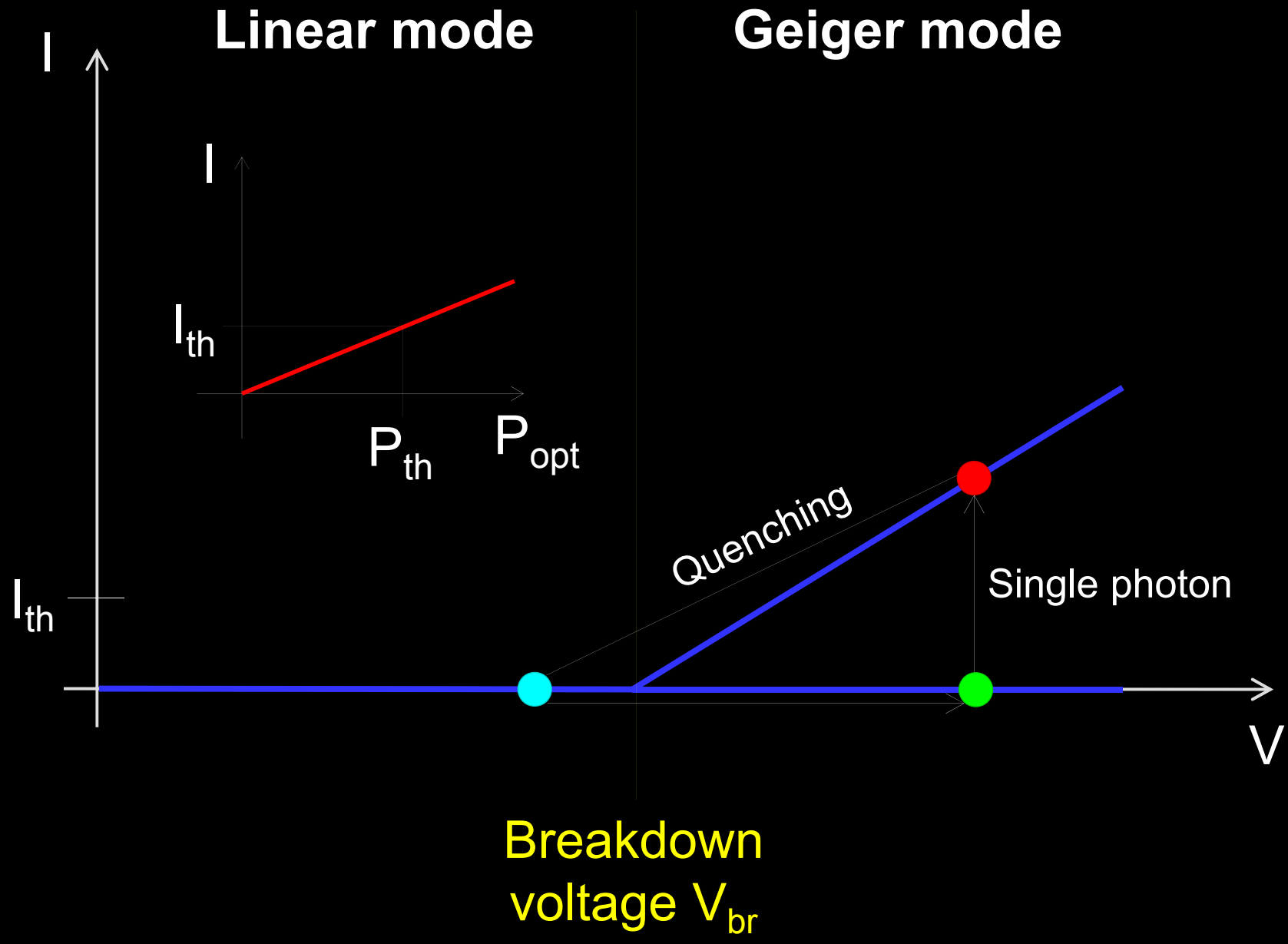




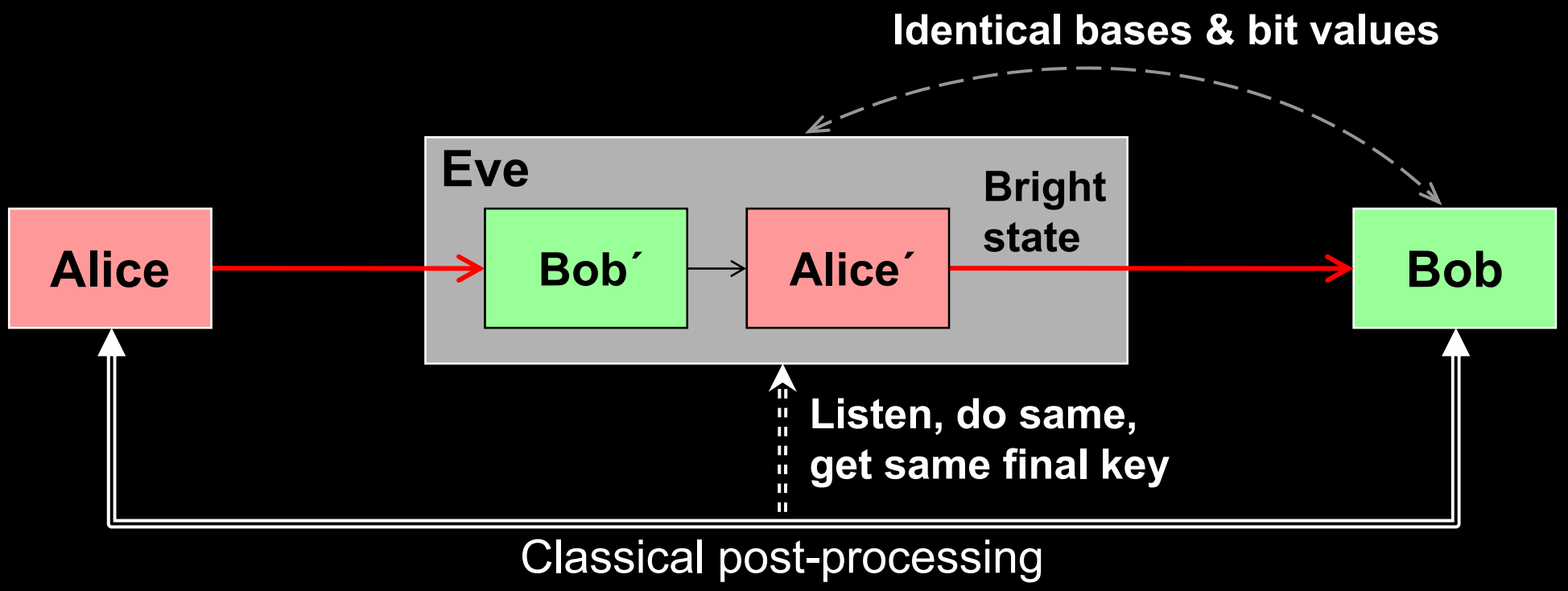
N. Jain *et al.*, New J. Phys. **16**, 123030 (2014)

End of lecture 1

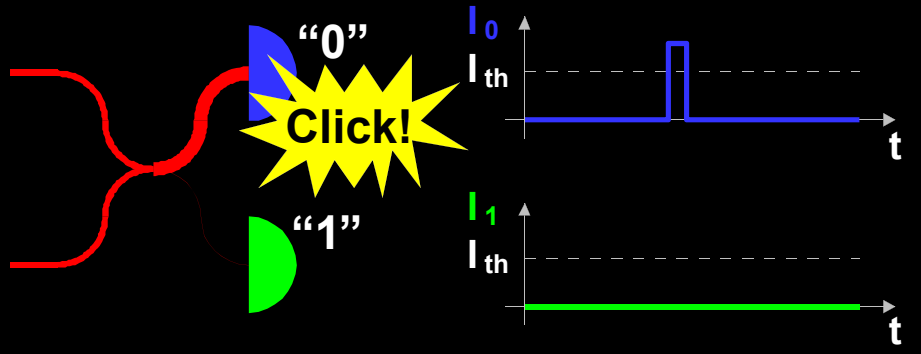
Attack example: avalanche photodetectors (APDs)



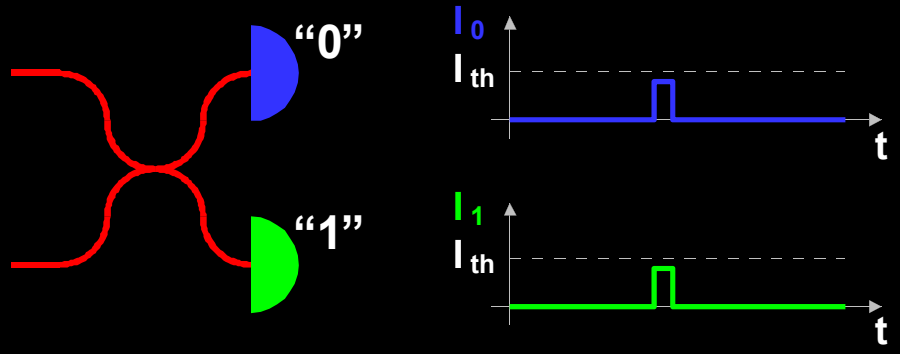
Faked-state attack in APD linear mode



Bob chooses same basis as Eve:

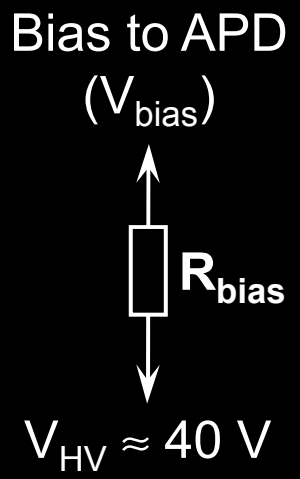


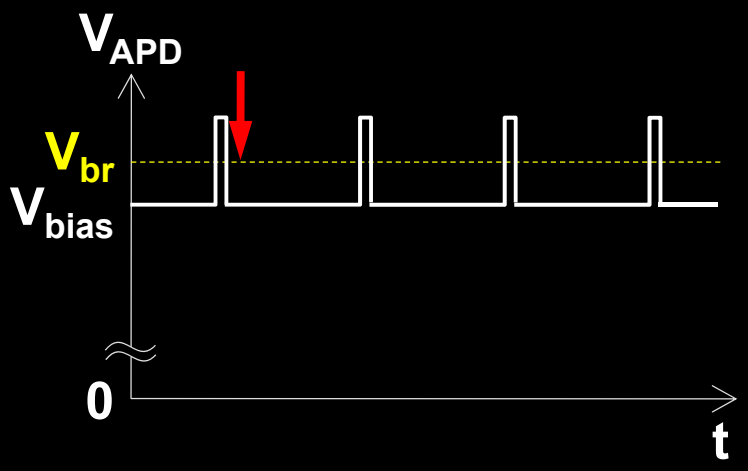
Bob chooses different basis:



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

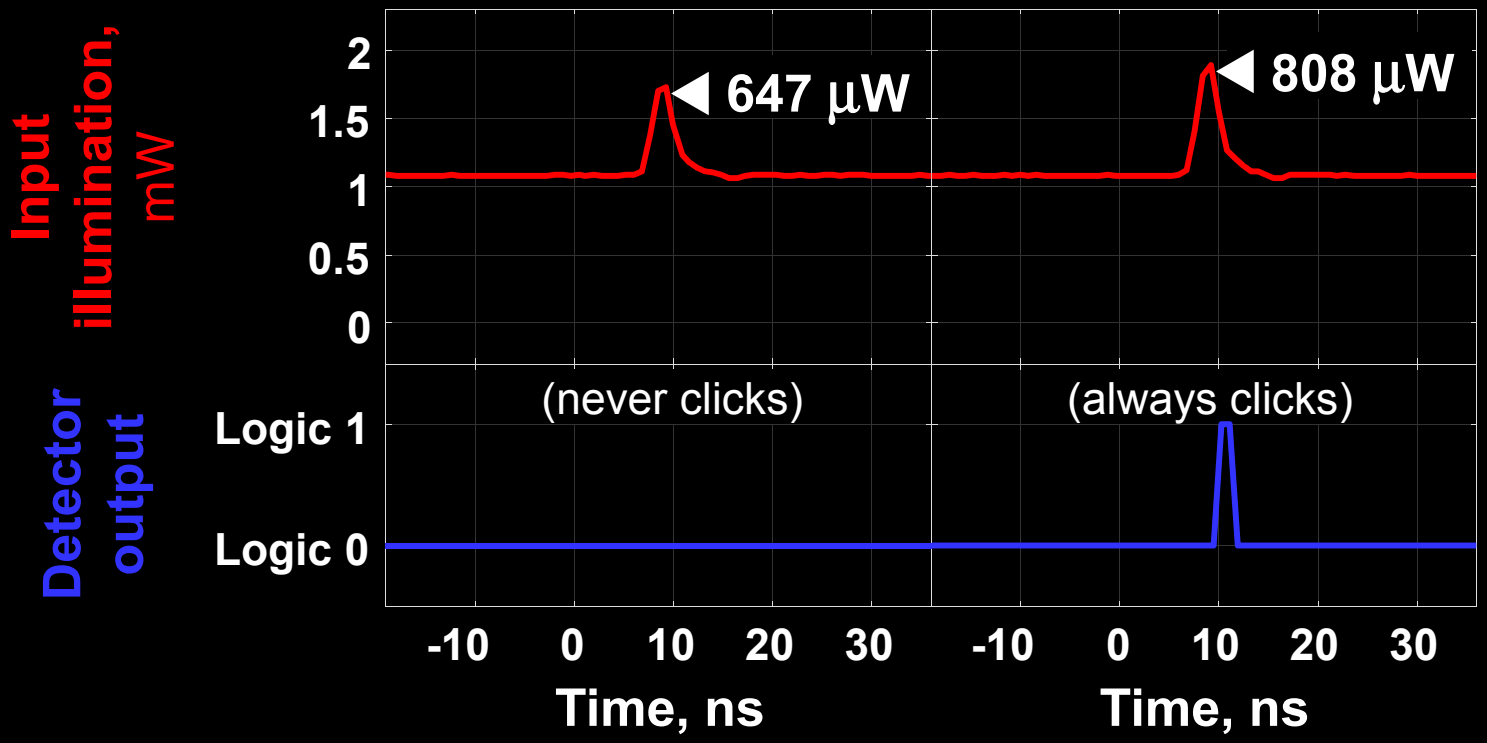
Blinding APD with bright light





Eve applies CW light

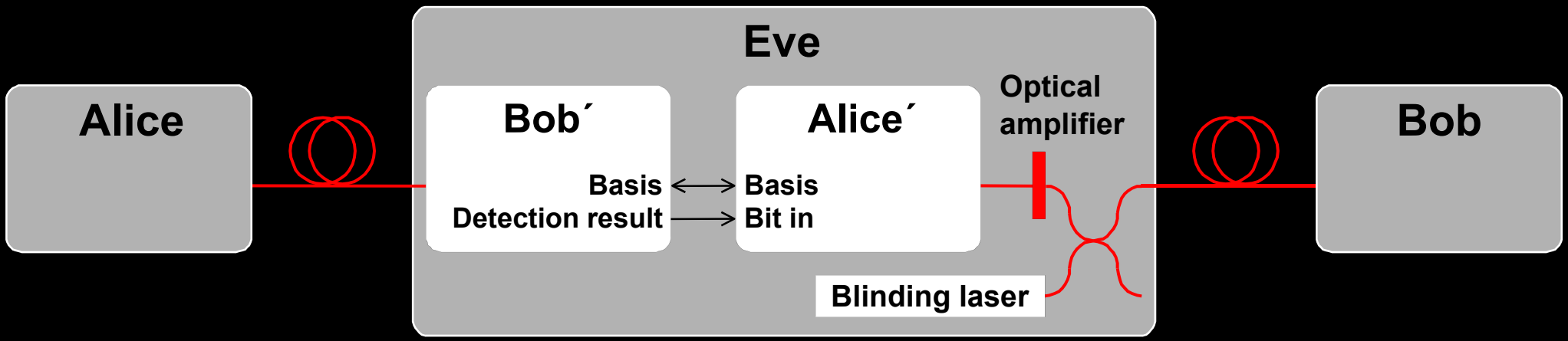
Detector blind!
Zero dark count rate



ID Quantique Clavis2

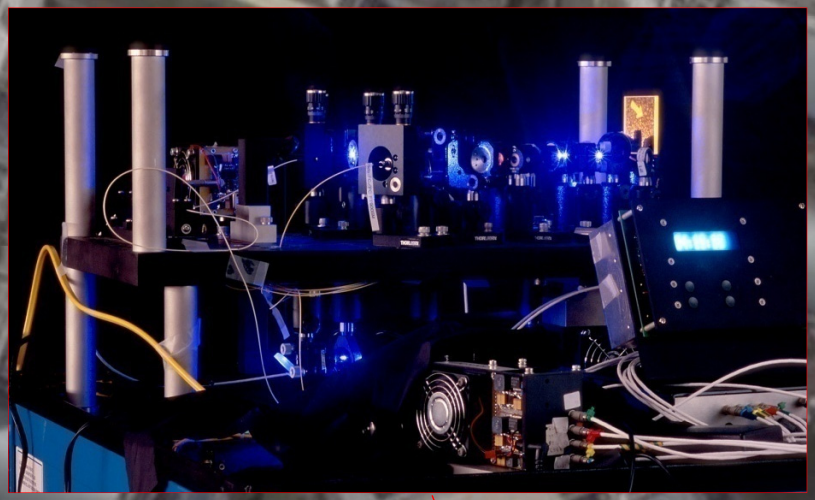
L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Nat. Photonics **4**, 686 (2010)

Proposed full eavesdropper



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

S12

S13

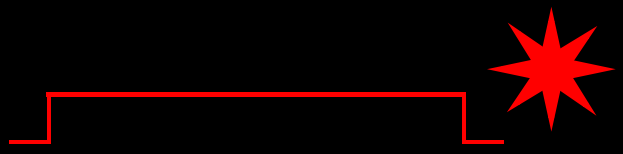
S14

S15

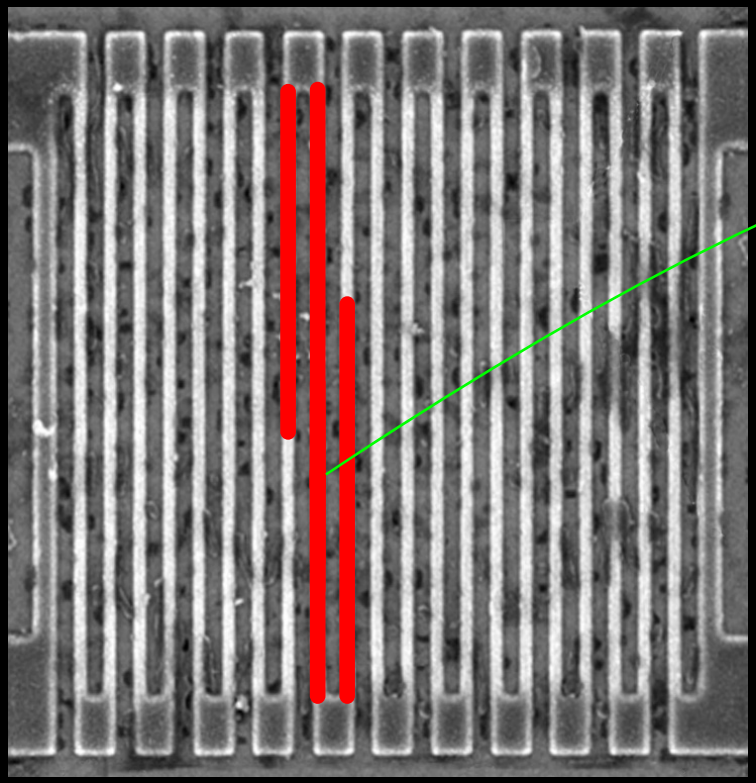
I. Gerhardt, Q. Liu *et al.*,
Nat. Commun. **2**, 349 (2011)

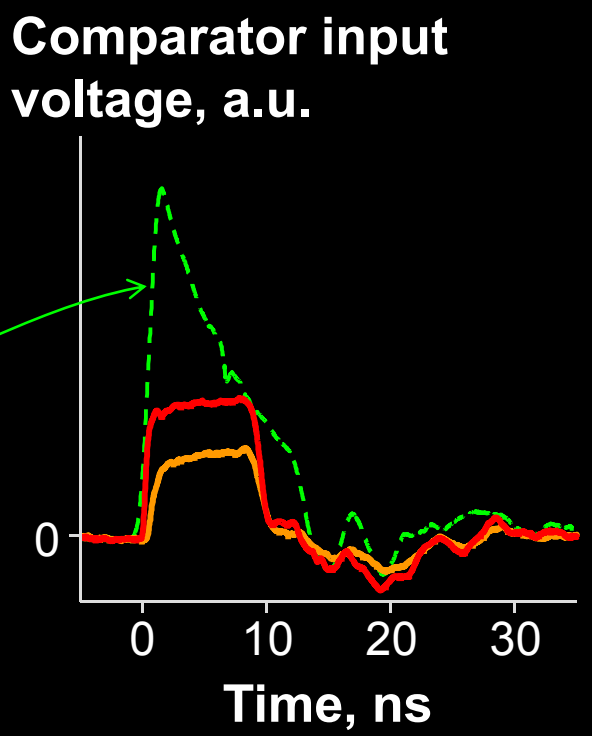
Controlling superconducting nanowire single-photon detectors

1. Blind (latch)



2. Control

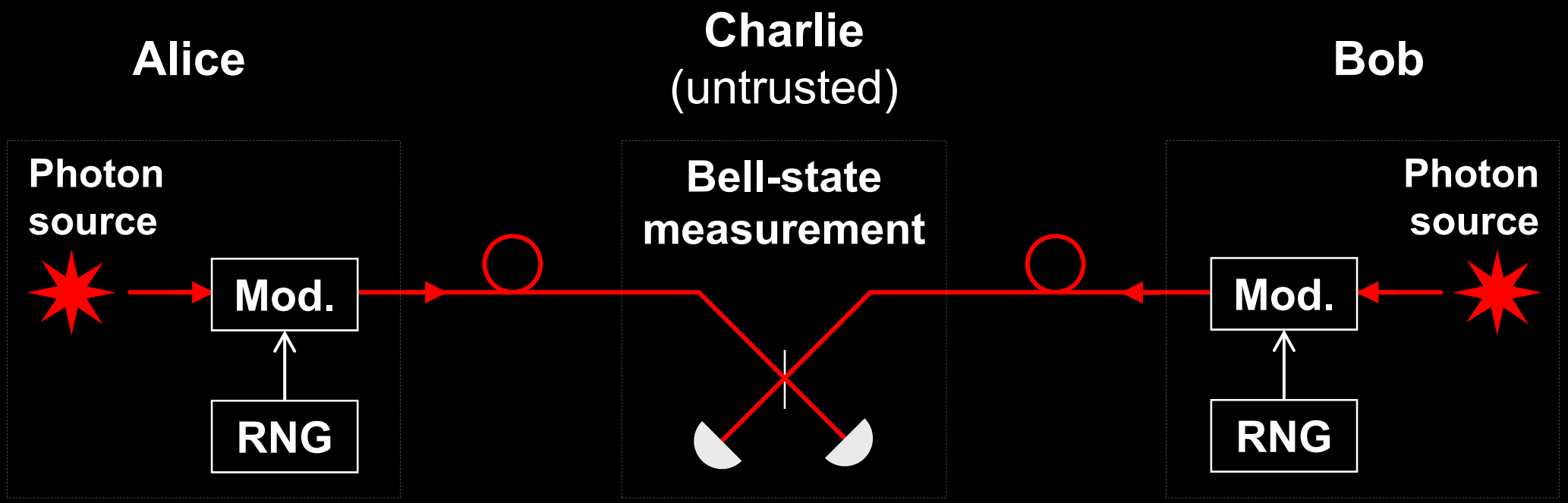




L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, V. Makarov, New J. Phys. **13**, 113042 (2011)
M. G. Tanner, V. Makarov, R. H. Hadfield, arXiv:1305.5989

Countermeasures to detector attacks?

Perfect countermeasure to detector attacks



Measurement-device-independent QKD

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

Industrial countermeasure (ID Quantique)

2004-11-10 — **First commercial Clavis1 system is shipped to a customer**

2009-10-22 — **Report about detector blinding attack sent to IDQ**

2010-10-08 — **IDQ applies for a patent on randomization of detector efficiency as a countermeasure**

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

2014-08-27

2014-11-18 — ★ **Implementation of countermeasure delivered by IDQ to our lab (firmware update for Clavis2)**

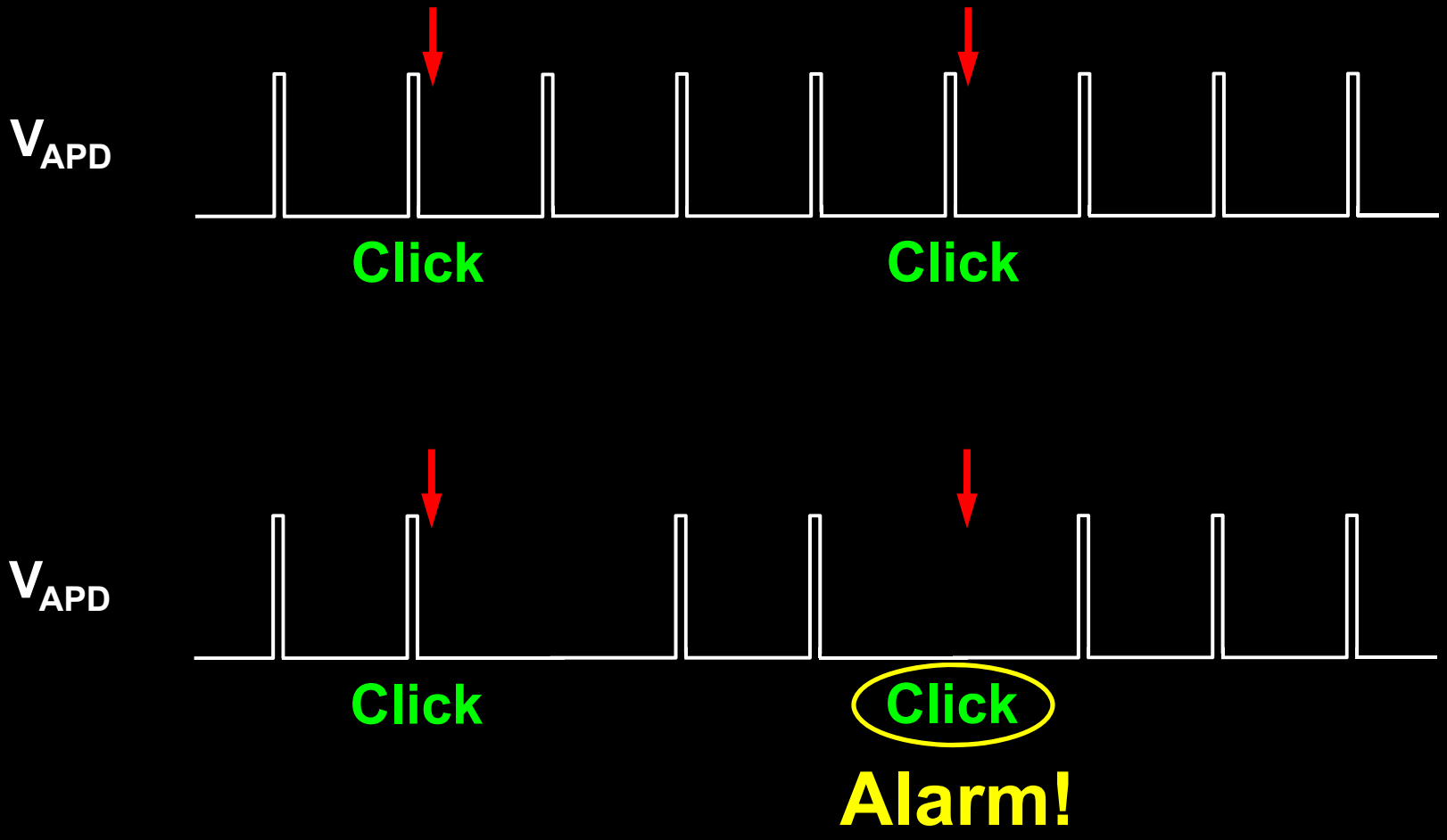
2015-04-17

2015-12-21 — **Testing report sent to IDQ proposing a modified attack that works**

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

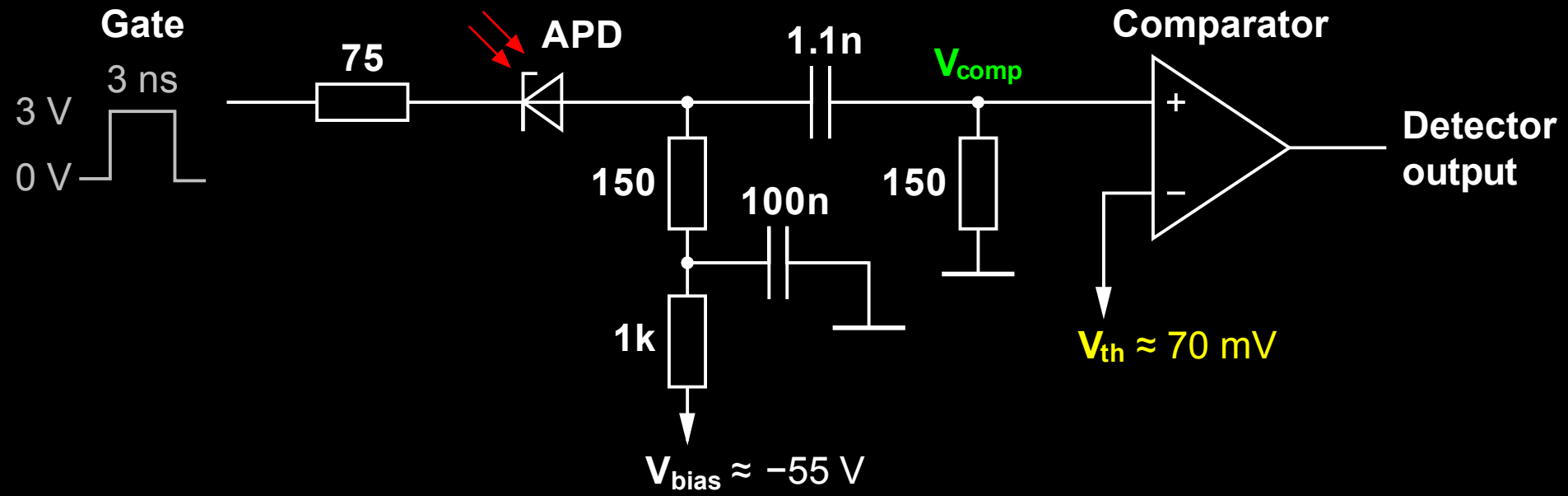
A. Huang *et al.*, arXiv:1601.00993

Randomly varying detector efficiency



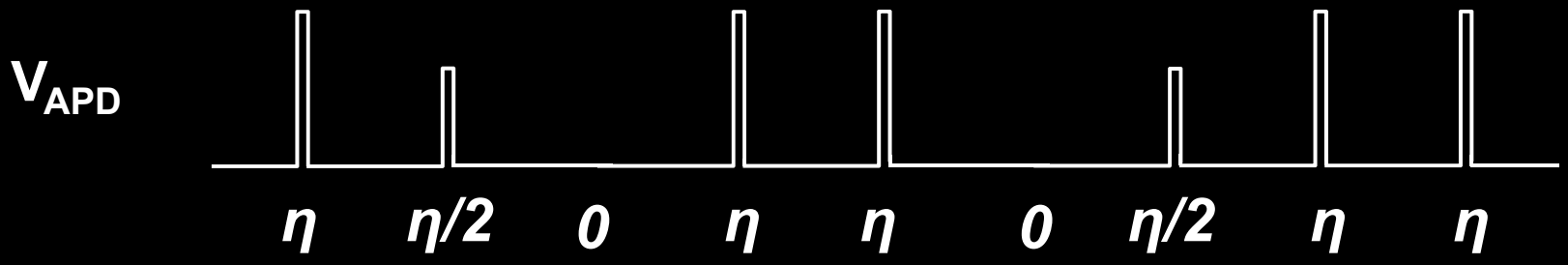
M. Legre, G. Robordy, Intl. patent appl. WO 2012/046135 A2 (filed in 2010)

Oscillograms at comparator input

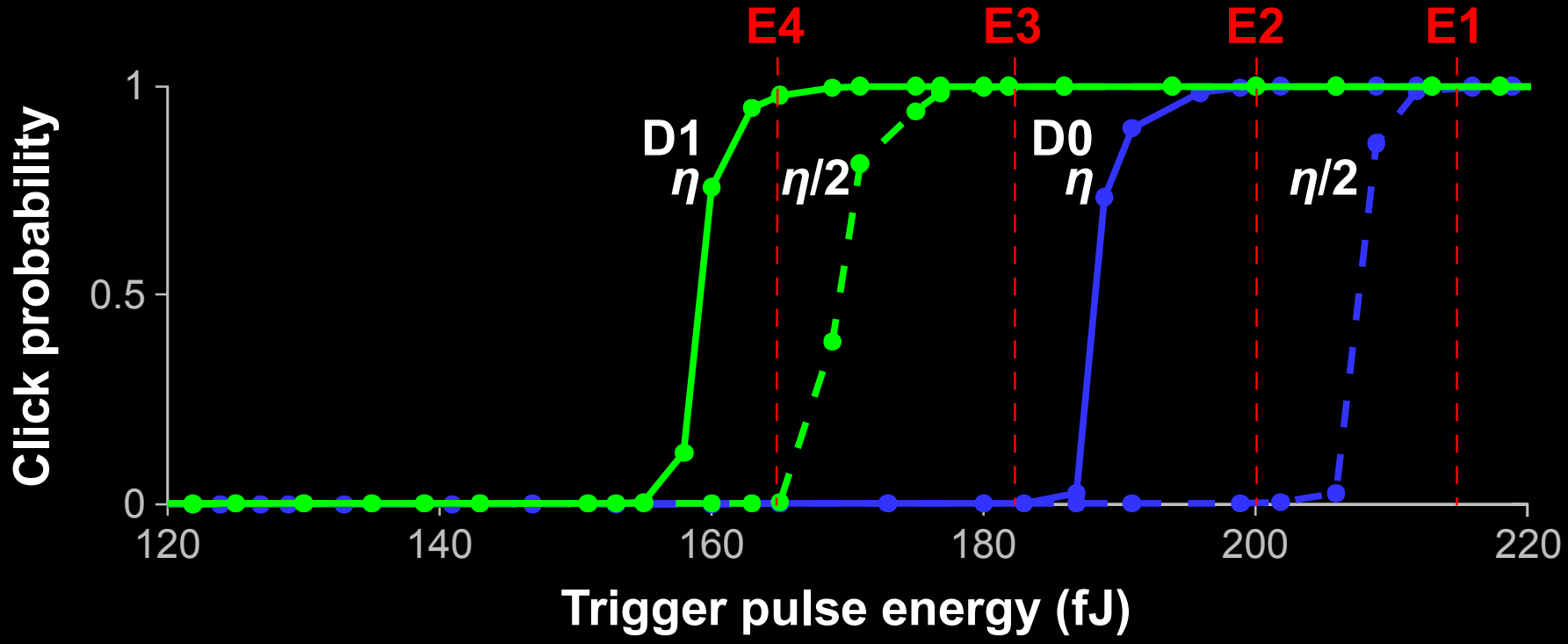


A. Huang *et al.*, arXiv:1601.00993

Full two-efficiency-level countermeasure



C. C. W. Lim *et al.*, IEEE J. Sel. Top. Quantum Electron. **21**, 6601305 (2015)
M. Legre, G. Robordy, Intl. patent appl. WO 2012/046135 A2 (filed in 2010)



A. Huang *et al.*, arXiv:1601.00993

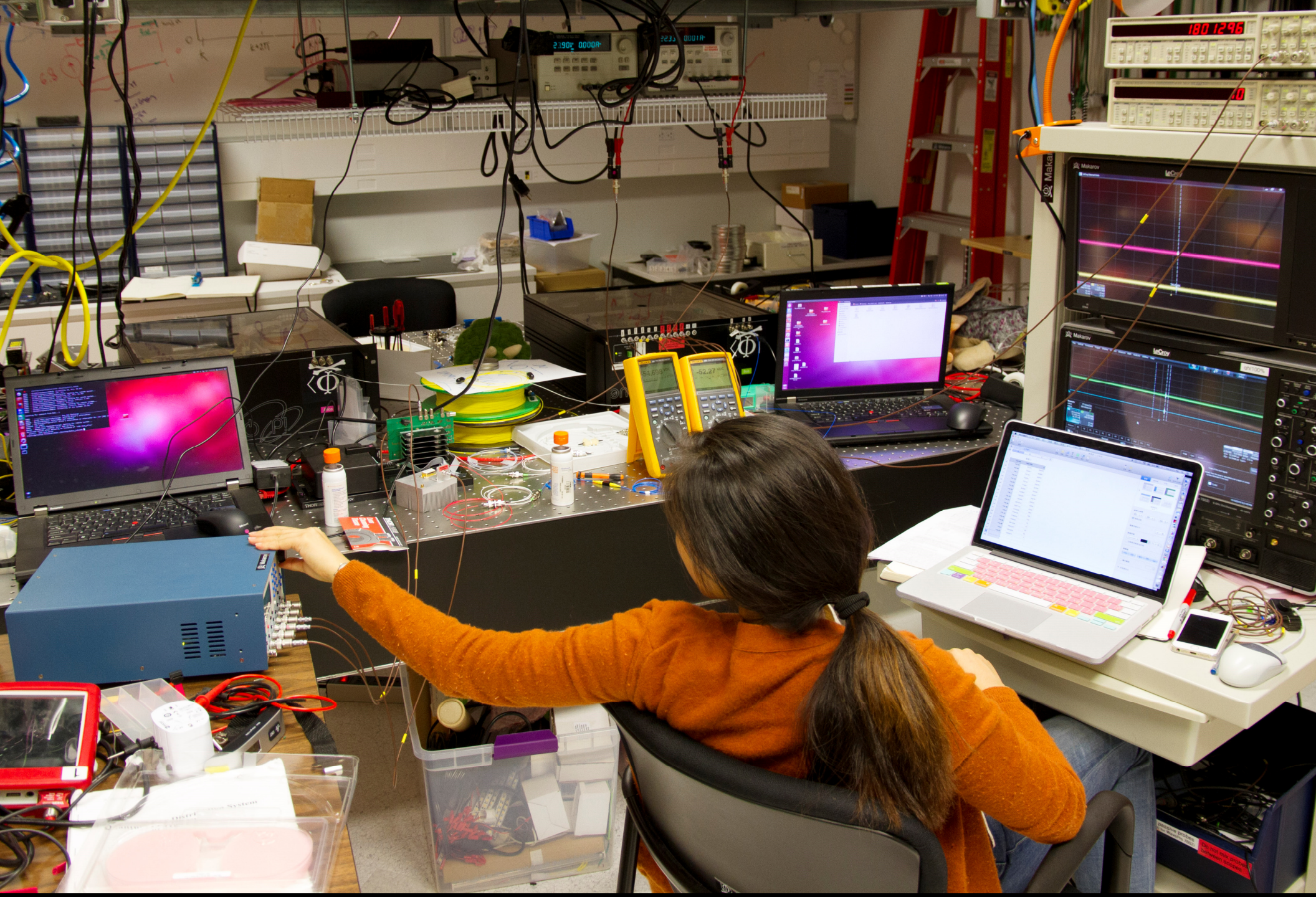
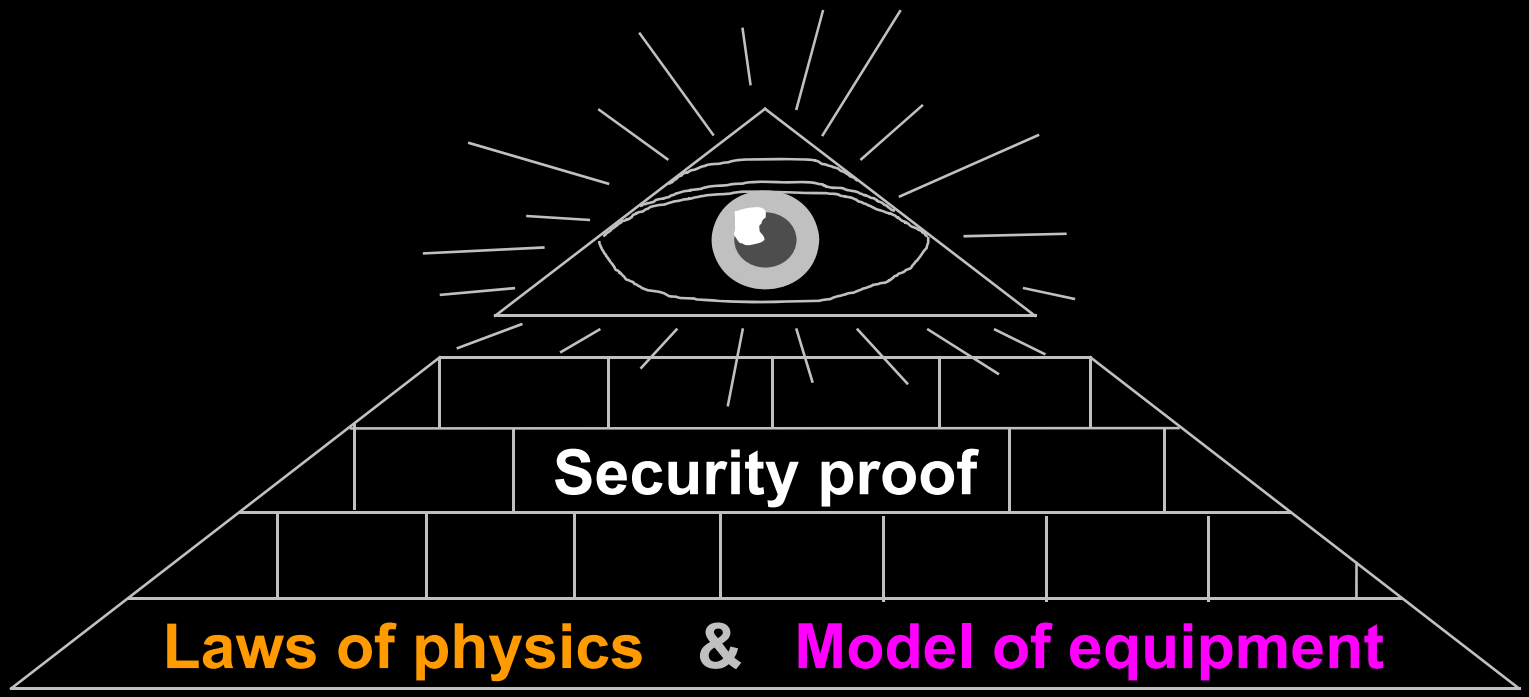


Photo ©2015 Vadim Makarov

Anqi Huang tests countermeasure in Clavis2

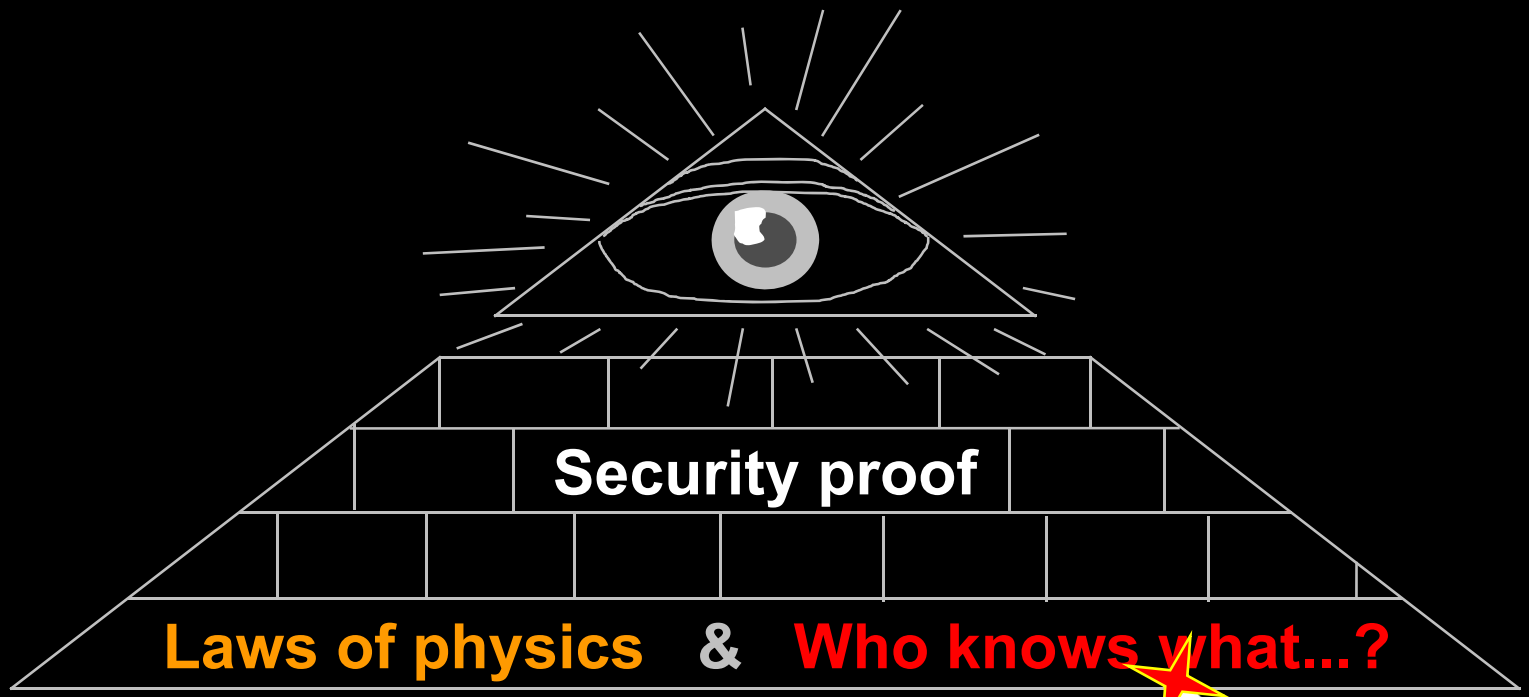
Security model of QKD



Hack

Integrate imperfection into security model

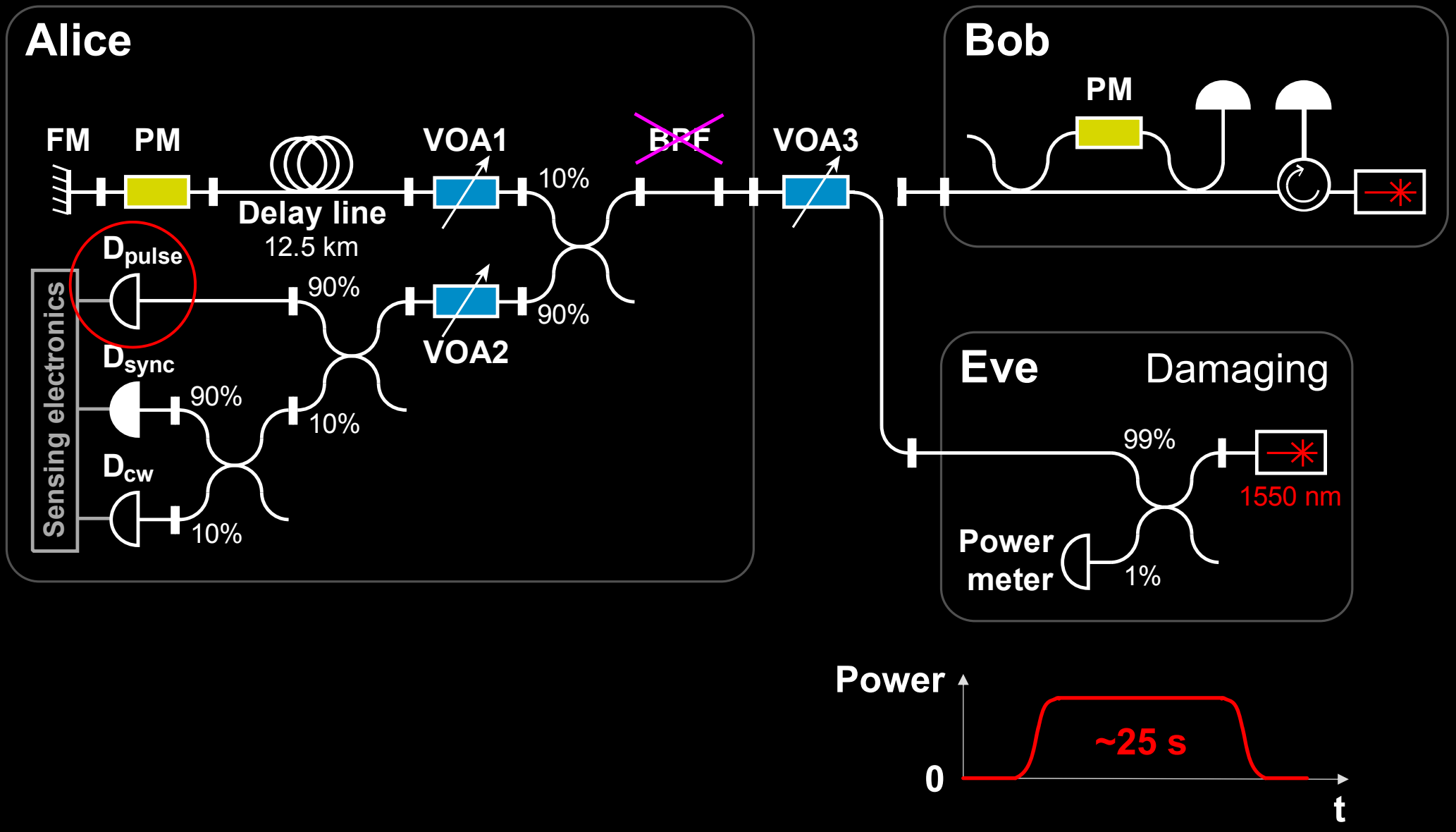
Limits on physical security



Physical access to equipment

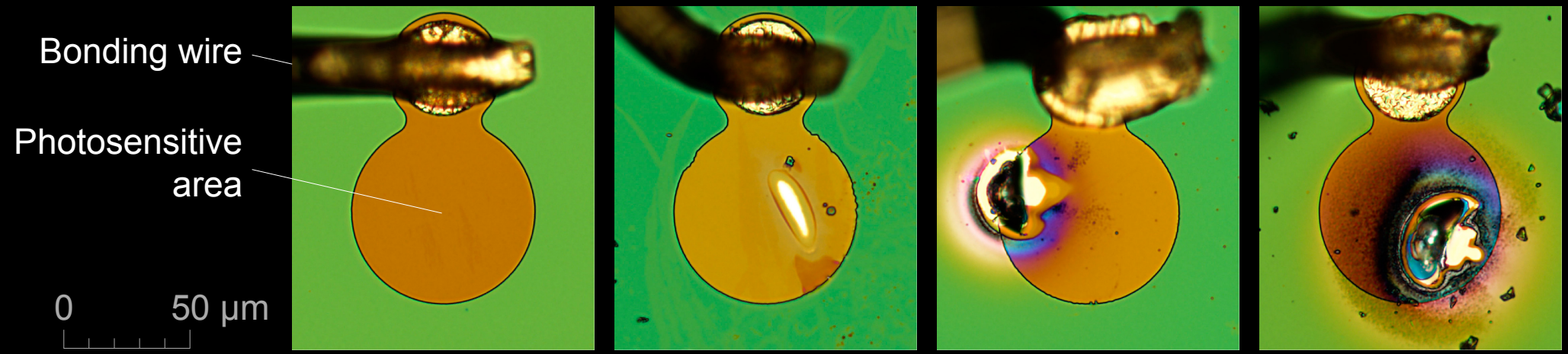
Laser damage!

Laser damage in commercial QKD system Clavis2



V. Makarov *et al.*, arXiv:1510.03148

InGaAs p-i-n photodiode D_{pulse} (JDSU EPM 605LL)



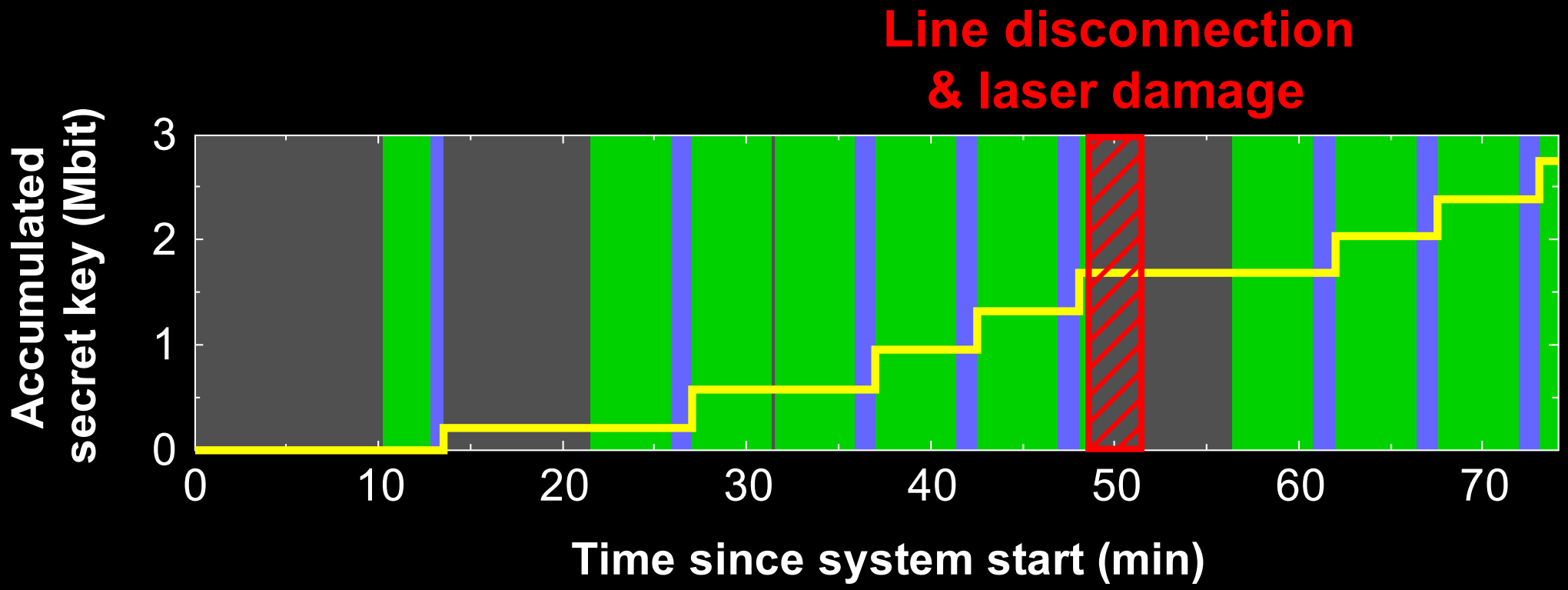
Damaging power at Alice's entrance (W)	**none**	**1.0**	**1.5**	**1.7**
Loss of photo-sensitivity (dB)	**undamaged**	**1.6**	**5.5**	**completely lost photosensitivity**

↑

Reproducible (repeated with 3 samples)

V. Makarov *et al.*, arXiv:1510.03148

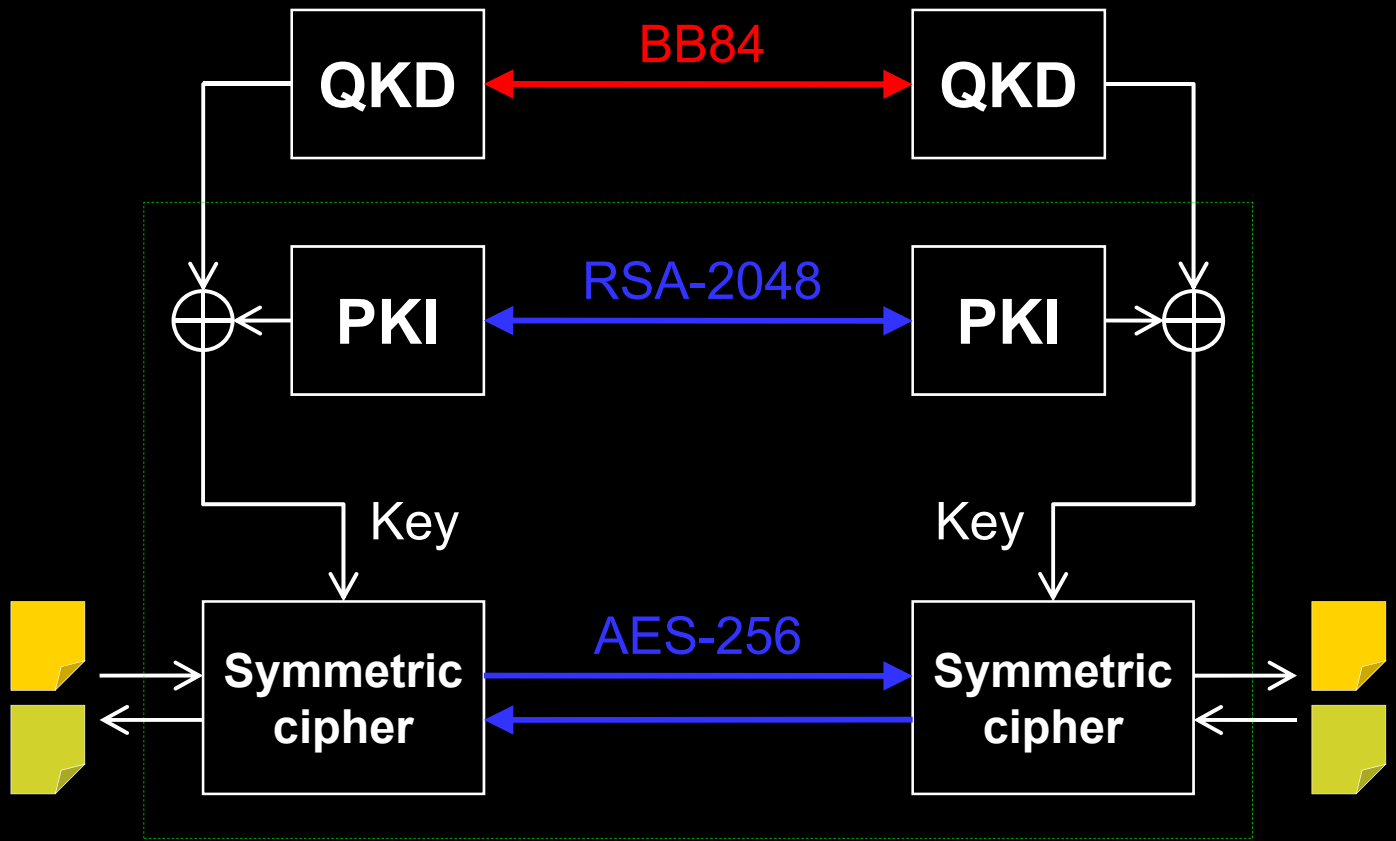
QKD system log



V. Makarov *et al.*, arXiv:1510.03148

Can we eavesdrop on commercial systems?

ID Quantique's Cerberis:
Dual key agreement



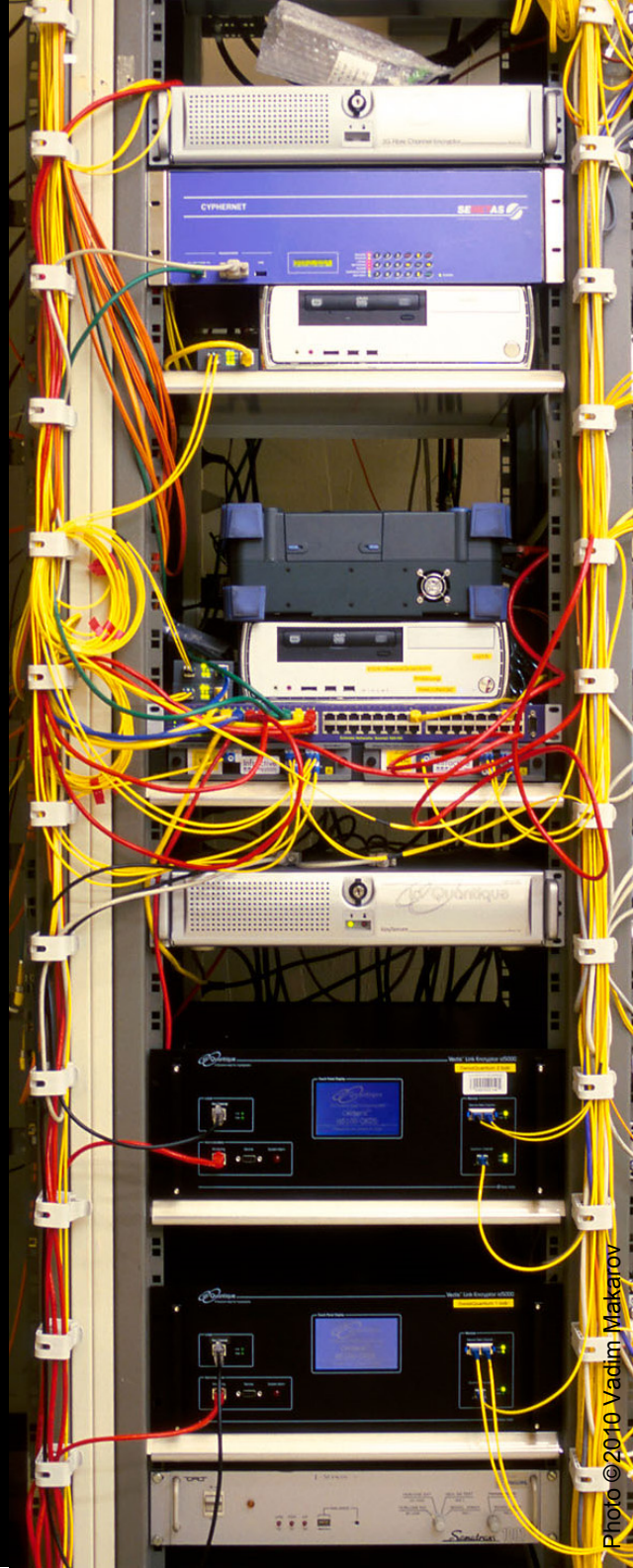
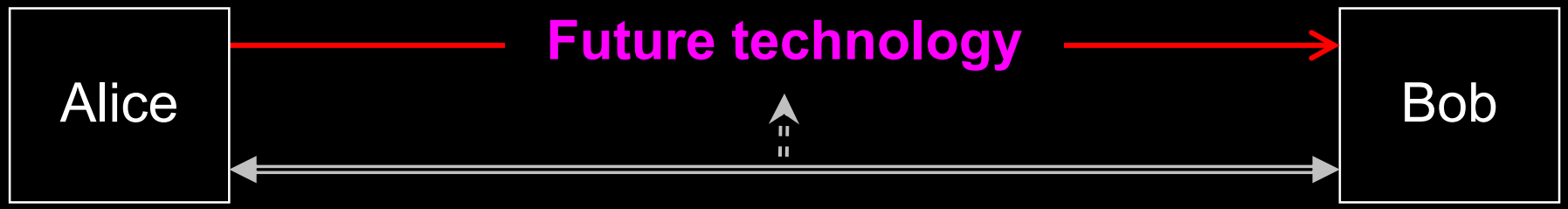


Photo © 2010 Vadim Makarov

Kerckhoffs' principle



characteristics known **characteristics known**

Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi

A. Kerckhoffs, J. des Sciences Militaires **IX**, 5 (1883)

Everything about the system that is not explicitly secret is known to the enemy

Eavesdropping in real life?

Alice → **Future technology** → Bob

characteristics known — Many papers — **characteristics known**

Alice → **Today's technology (modeled)** → Bob

characteristics measured — Many papers — **characteristics measured**

Alice → **Implemented** → Bob

characteristics measured — **characteristics measured**

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

Alice → **Implemented** → Bob

no access — Not yet :) — **no access**