Lecture 10 in Quantum communications course, 5 November 2019

Quantum hacking

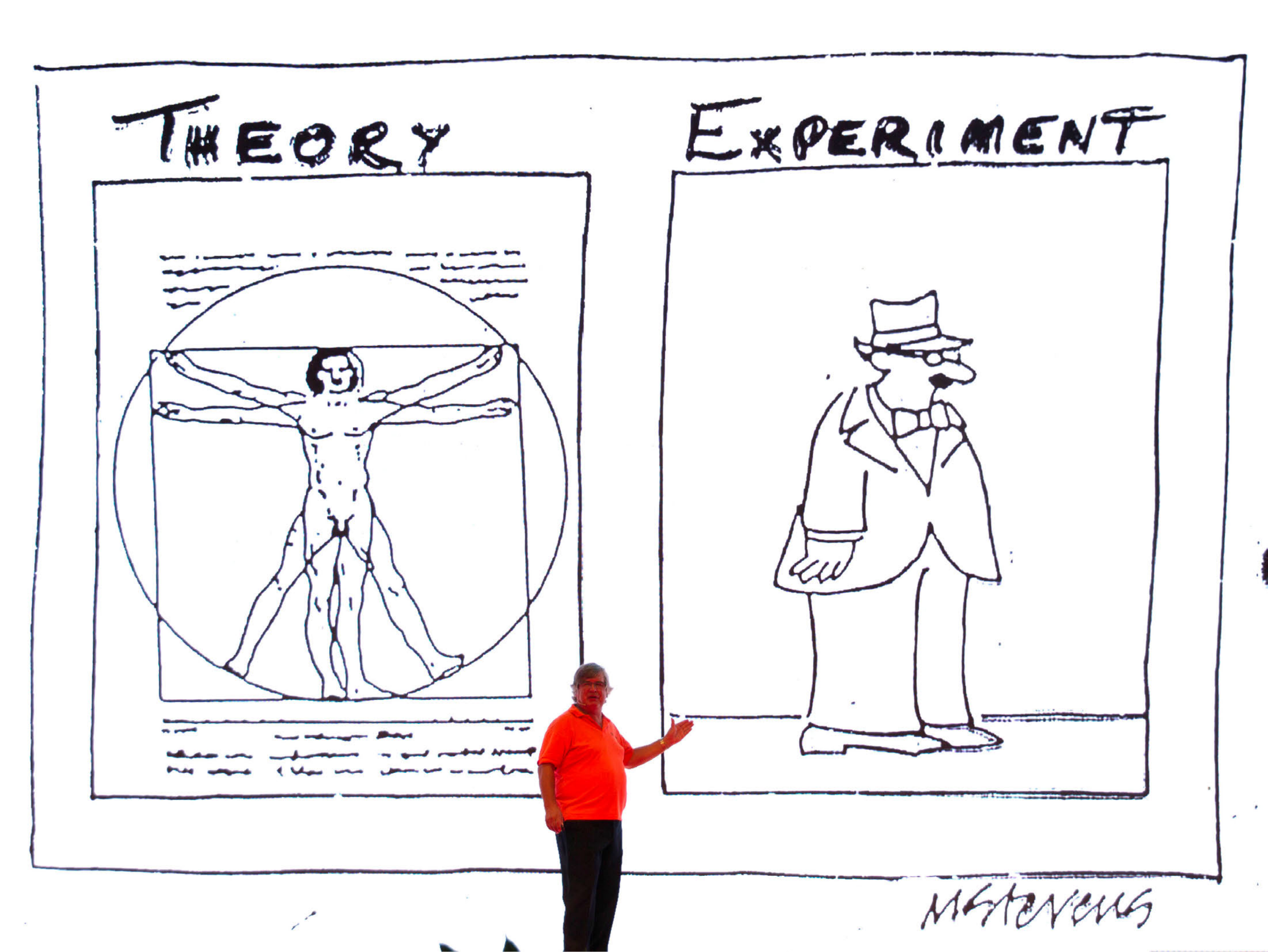
Vadim Makarov

RQC MISIS

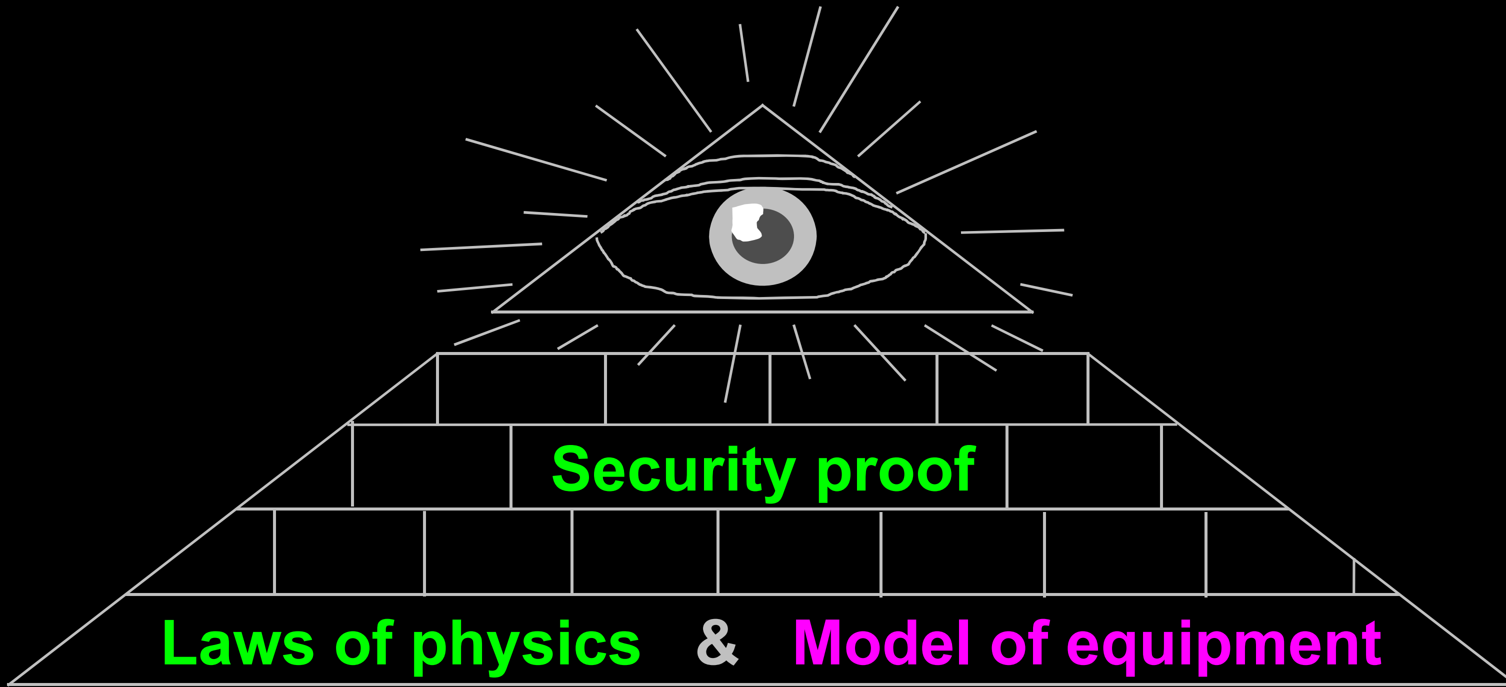
vad1.com/lab

A (very) brief history of cryptography

		Broken?
Monoalphabetic cipher	invented ~50 BC (J. Caesar)	~850 (Al-Kindi)
Nomenclators (code books)	~1400 – ~1800	✓
Polyalphabetic (Vigenère)	1553 – ~1900	1863 (F. W. Kasiski)
…		
One-time pad	invented 1918 (G. Vernam)	**impossible** (C. Shannon 1949)
Polyalphabetic electromechanical (Enigma, Purple, etc.)	1920s – 1970s	✓
…		
DES	1977 – 2005	1998: 56 h (EFF)
Public-key crypto (RSA, elliptic-curve)	1977 –	will be once we have q. computer (P. Shor 1994)
AES	2001 –	?
Quantum cryptography	invented 1984, in development	**impossible***
Public-key crypto (‘quantum-safe’)	in development	?


THEORY
EXPERIMENT
MStevens

Implementation security of quantum communications

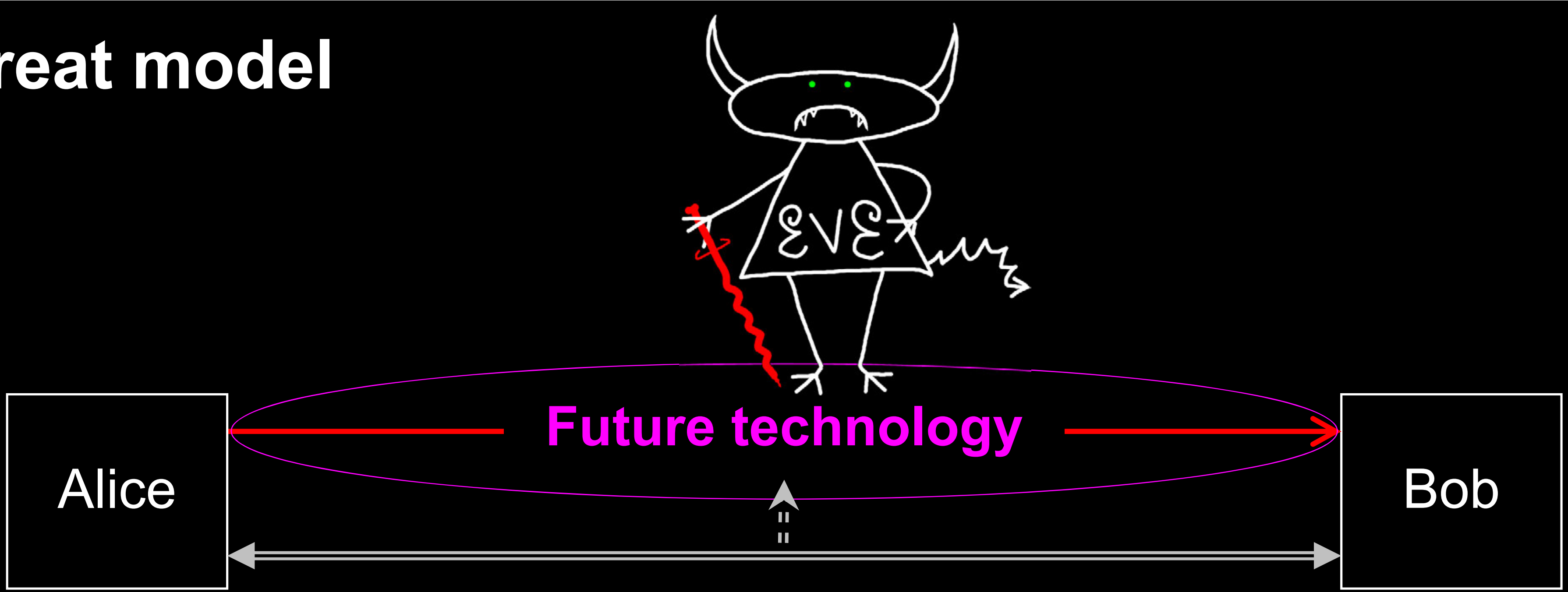


Hack

Integrate imperfection into security model

Formal certification: we need standards and labs ecosystem

Threat model



physically secure,
characteristics known

physically secure,
characteristics known

Kerckhoffs' principle:

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 **9**, 5 (1883)

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

Attack	Target component	Tested system
Distinguishability of decoy states A. Huang *et al.*, Phys. Rev. A **98**, 012330 (2018)	laser in Alice	3 research systems
Intersymbol interference K. Yoshino *et al.*, poster at QCrypt (2016)	intensity modulator in Alice	research system
Laser damage V. Makarov *et al.*, Phys. Rev. A **94**, 030302 (2016); A. Huang *et al.*, poster at QCrypt (2018)	any	5 commercial & 1 research systems
Spatial efficiency mismatch M. Rau *et al.*, IEEE J. Sel. Top. Quantum Electron. **21**, 6600905 (2015); S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015)	receiver optics	2 research systems
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); S. Sajeed *et al.*, Sci. Rep. **7**, 8403 (2017)	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 systems

Example of vulnerability and countermeasures

Photon-number-splitting attack

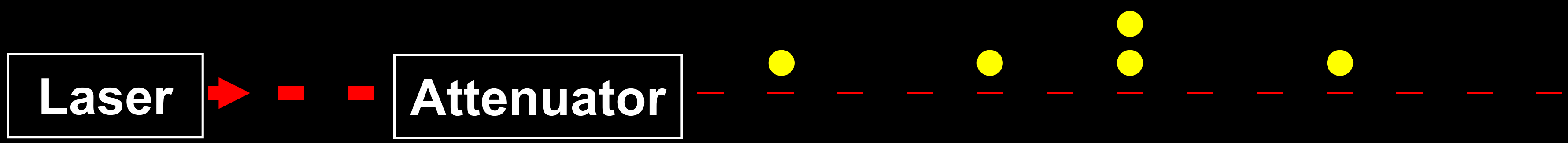
C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992)

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)

Commercial QKD

1st generation (circa 2008)
ID Quantique *Cerberis* system

Classical encryptors:

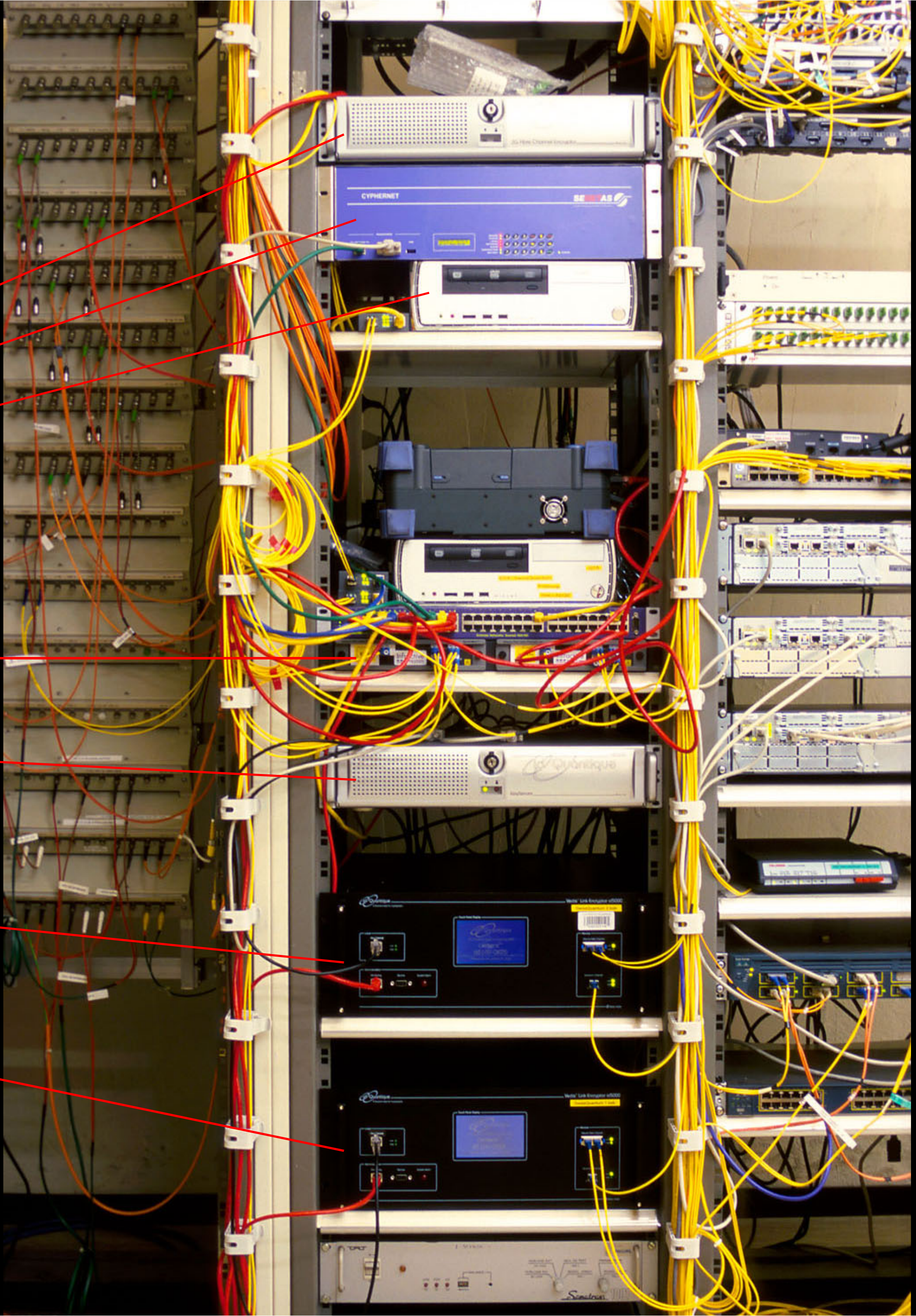
L2, 2 Gbit/s
L2, 10 Gbit/s
L3 VPN, 100 Mbit/s

WDMs

Key manager

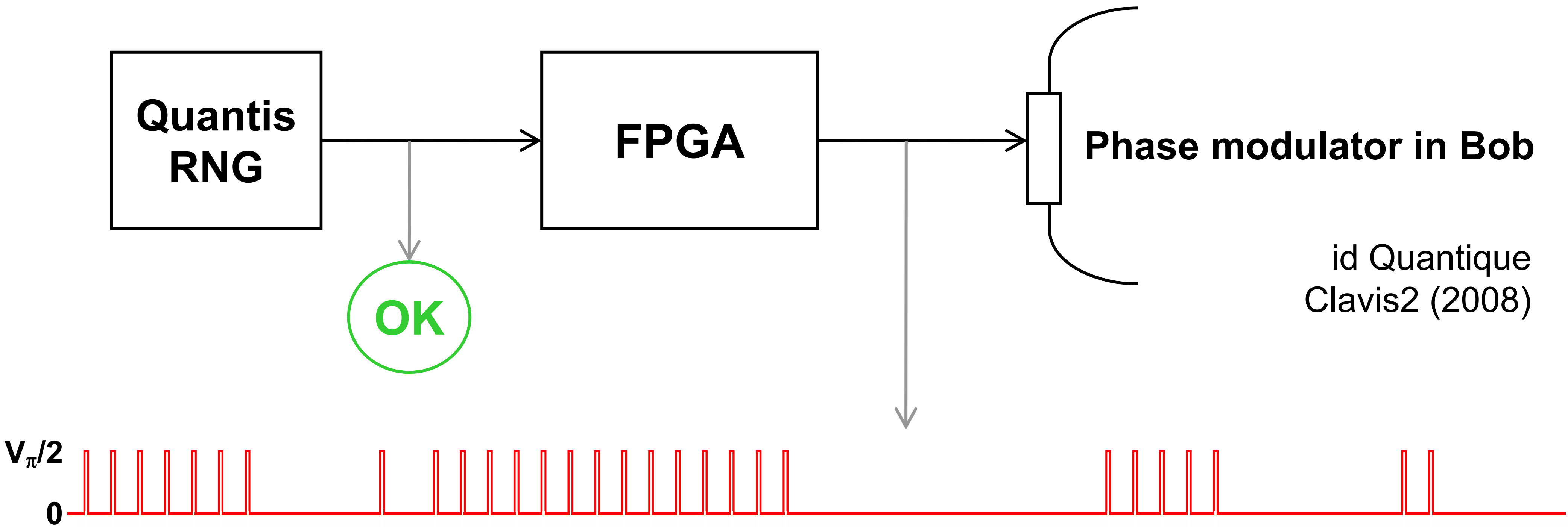
QKD to another node (4 km)

QKD to another node (14 km)

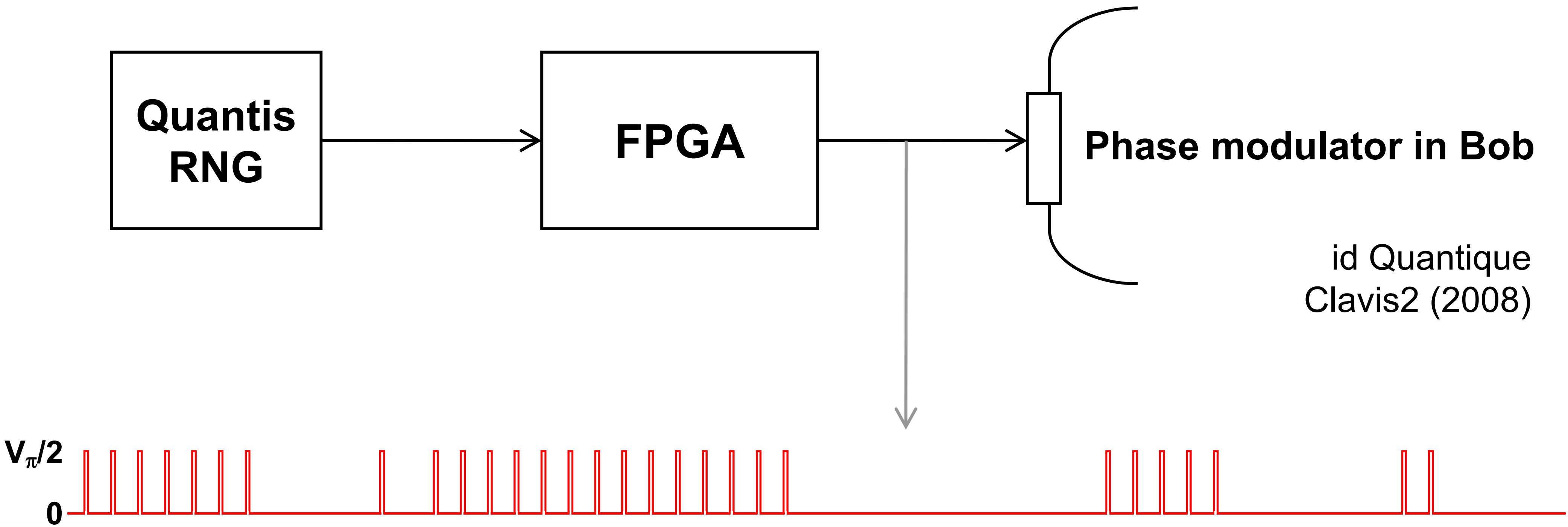


www.swissquantum.com

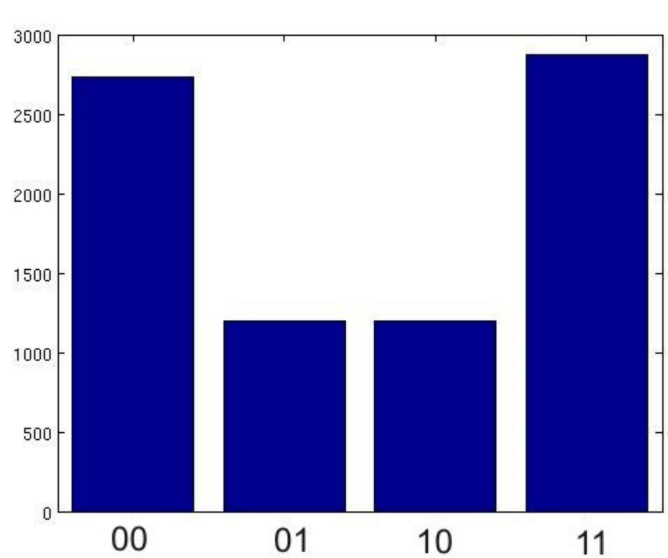
True randomness?



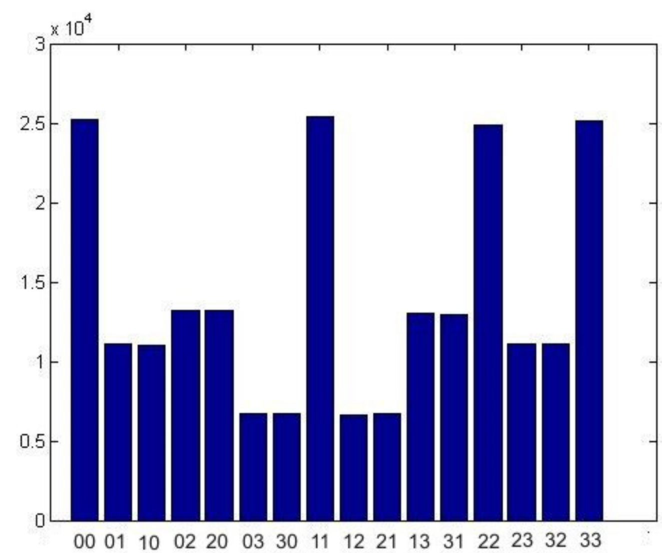
True randomness?



Bob:



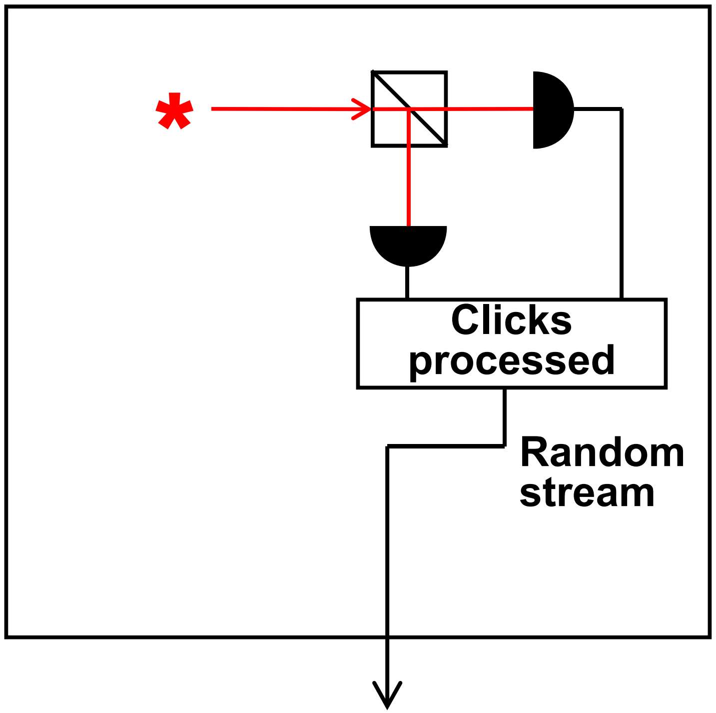
Alice:



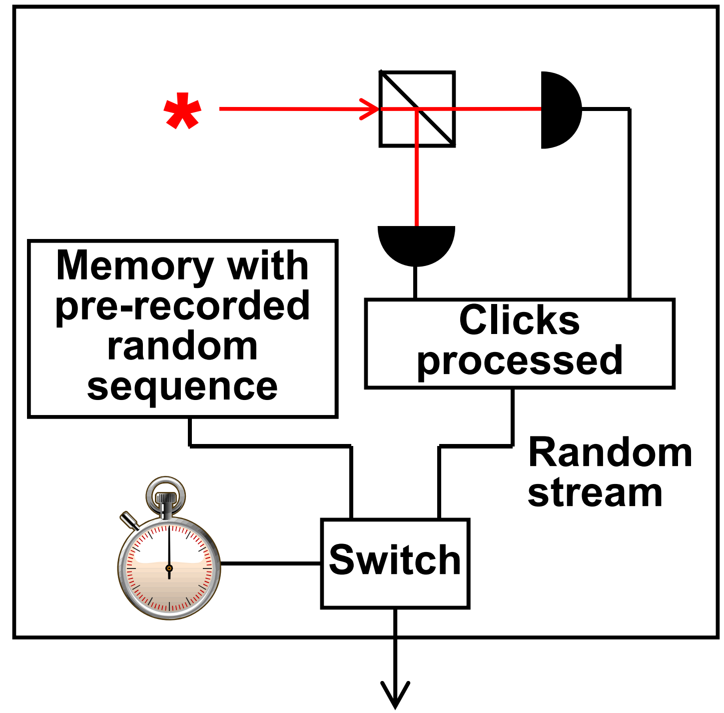
Issue reported patched in 2010

Do we trust the manufacturer?

Quantis RNG

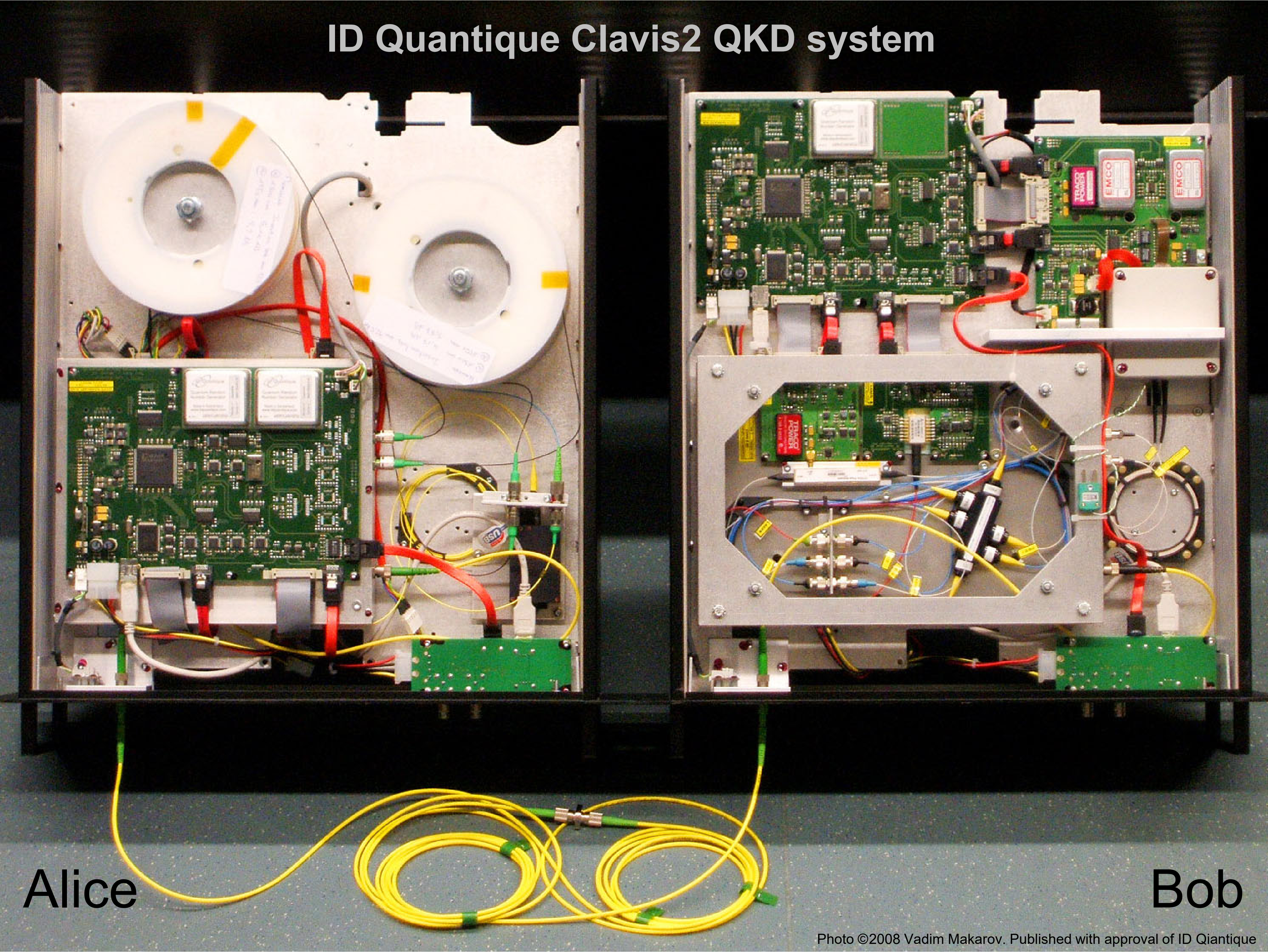


Quantis RNG, Trojan-horsed :)

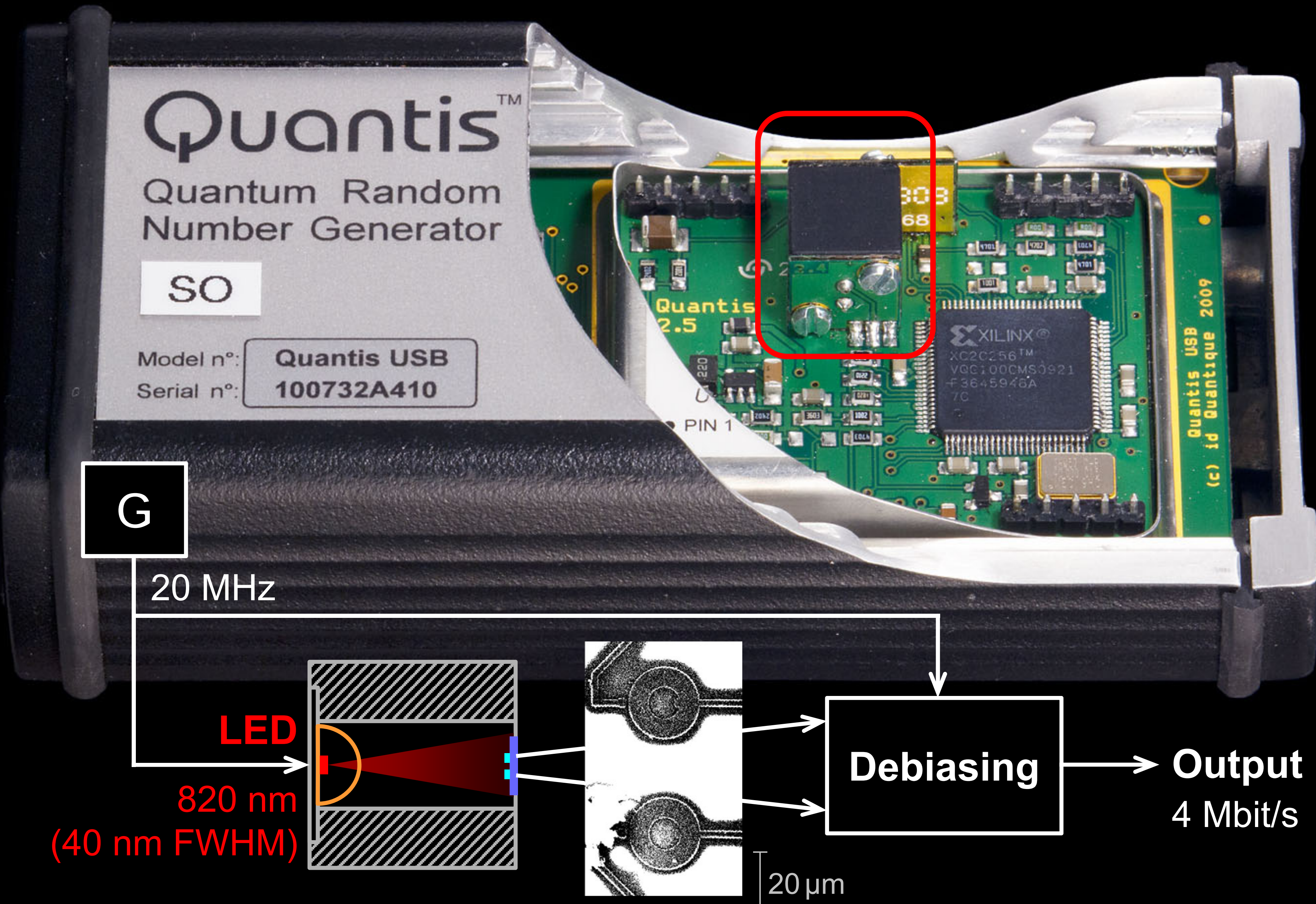


Many components in QKD system can be Trojan-horsed:

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


ID Quantique Clavis2 QKD system
Alice
Bob
EMCO
EMCO
Photo ©2008 Vadim Makarov. Published with approval of ID Qiantique

Quantis RNG: what's inside?



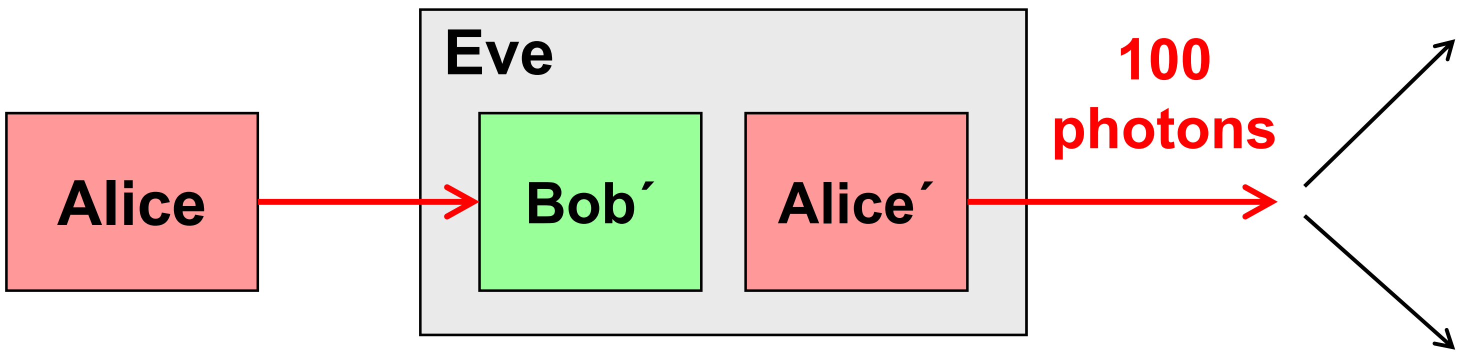
G. Ribordy, O. Guinnard, US patent appl. US 2007/0127718 A1 (filed in 2006)
M. Petrov, I. Radchenko *et al.*, unpublished

Double clicks

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

Discard them?

Intercept-resend attack... with a twist:



Bob:

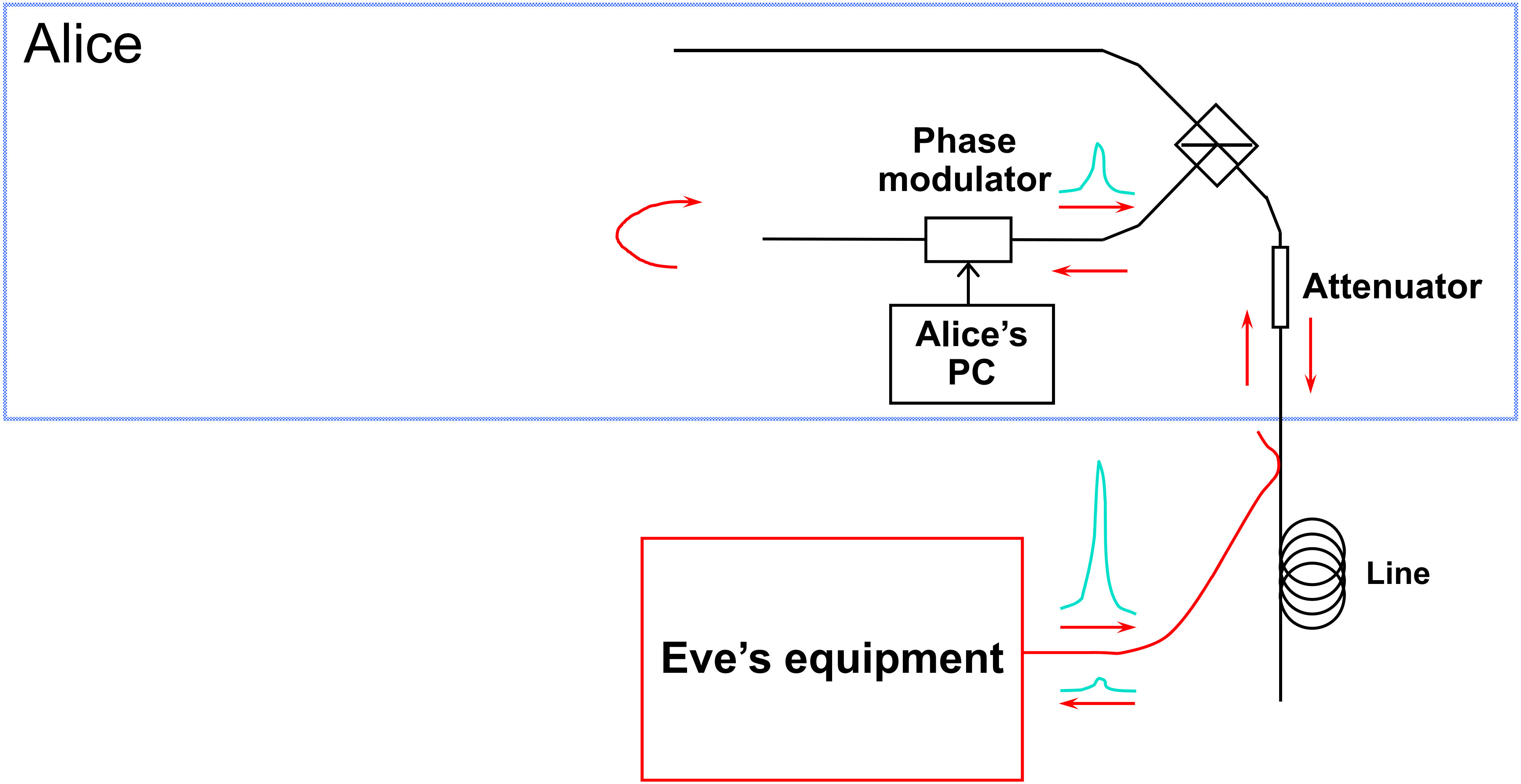
Detects in Eve's basis: single click

Detects in conjugate basis: double click, discarded

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

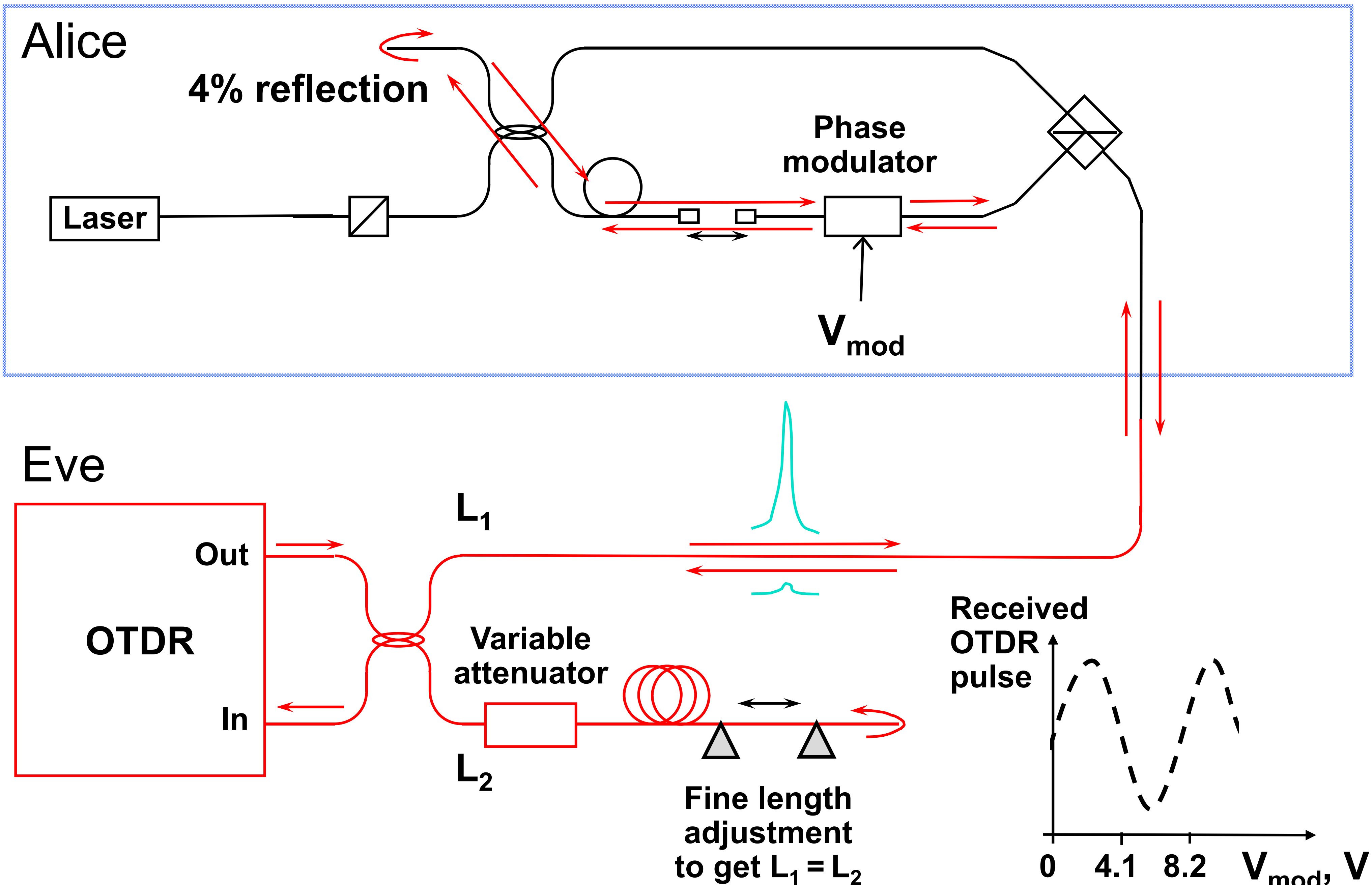
N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999)
T. Tsurumaru & K. Tamaki, Phys. Rev. A **78**, 032302 (2008)

Trojan-horse attack

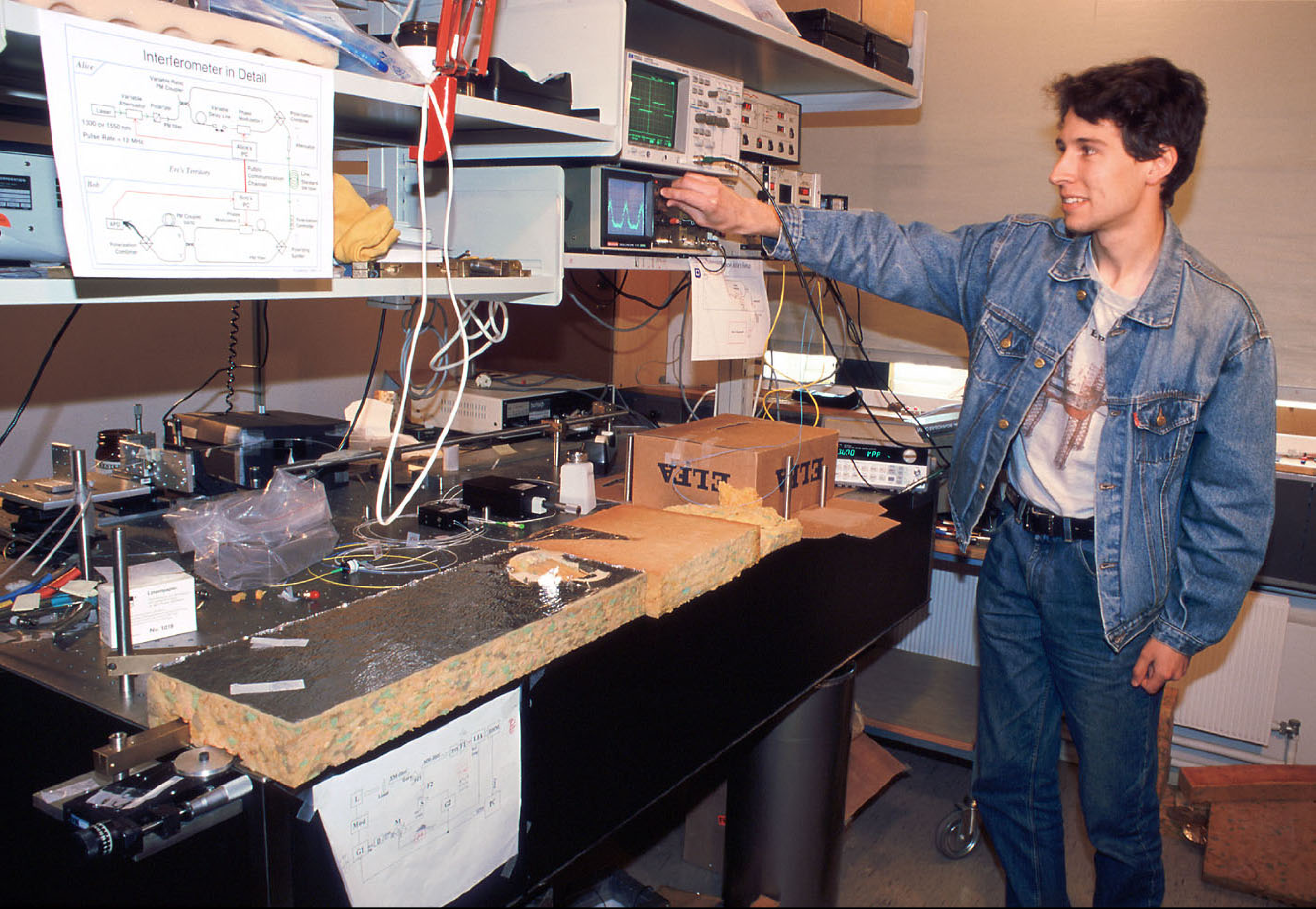


– interrogating Alice's phase modulator with powerful external pulses (can give Eve bit values directly)

Trojan-horse attack experiment

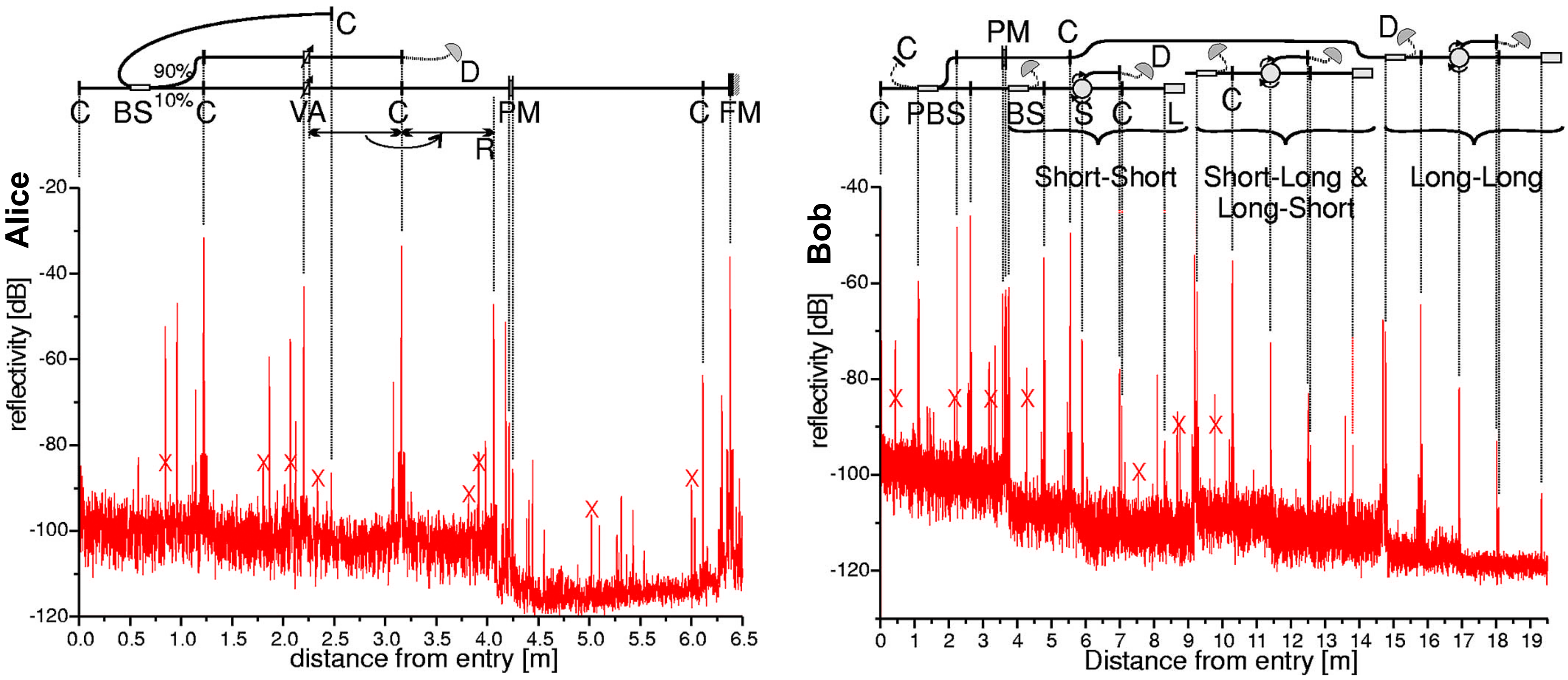


A. Vakhitov *et al.*, J. Mod. Opt. **48**, 2023 (2001)



Artem Vakhitov tunes up Eve’s setup

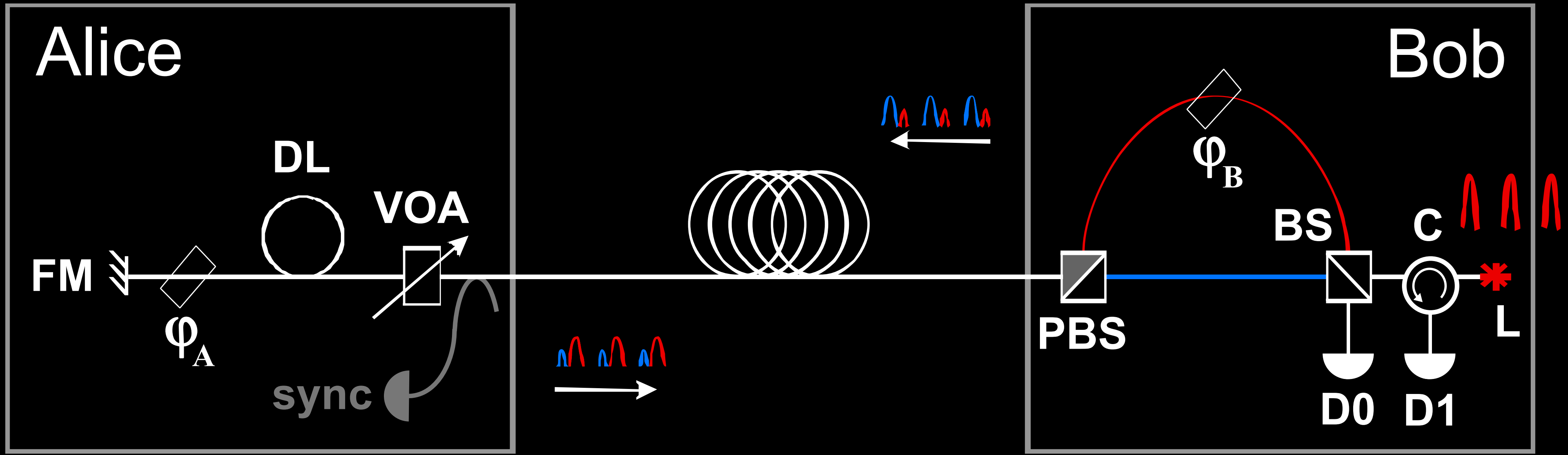
Trojan-horse attack for plug-and-play system



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

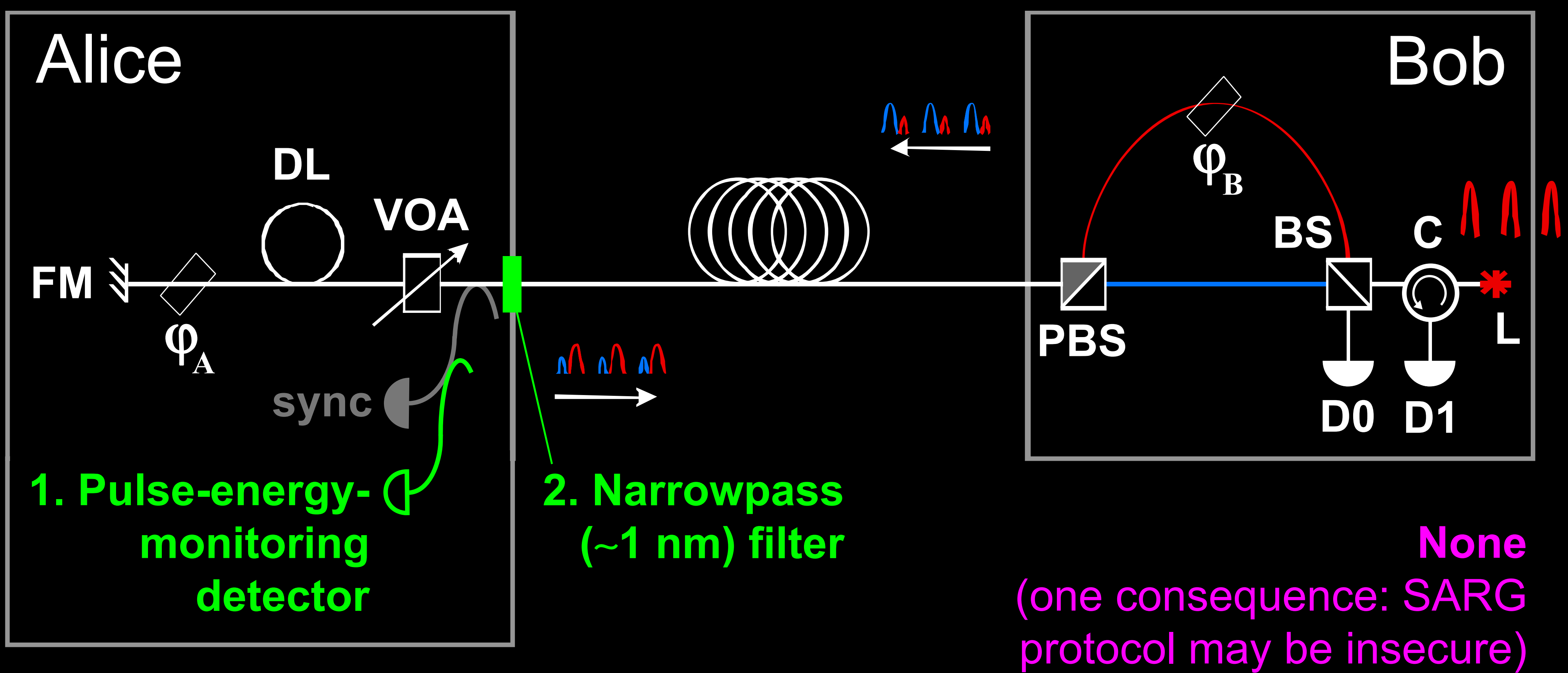
N. Gisin *et al.*, Phys. Rev. A **73**, 022320 (2006)

Countermeasures?



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

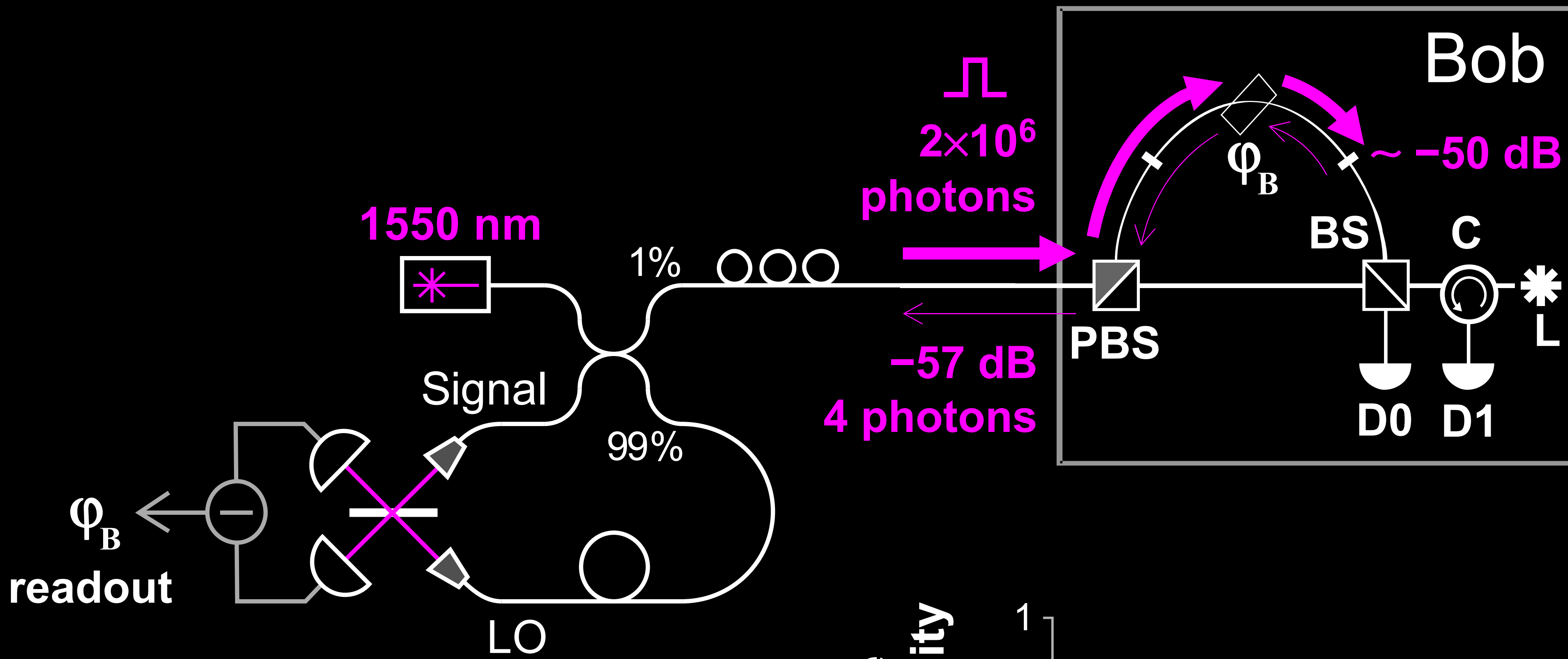
Countermeasures for plug-and-play system

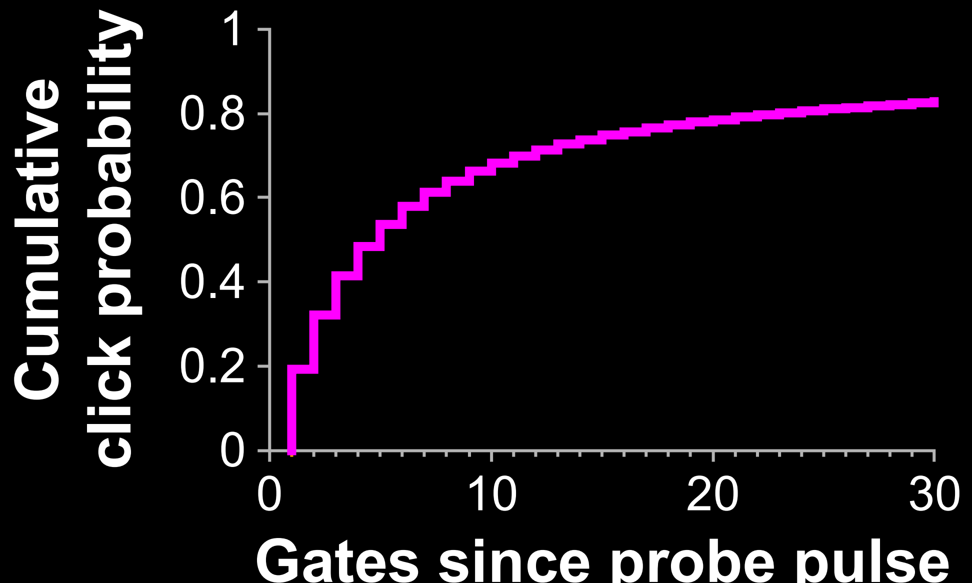


S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

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

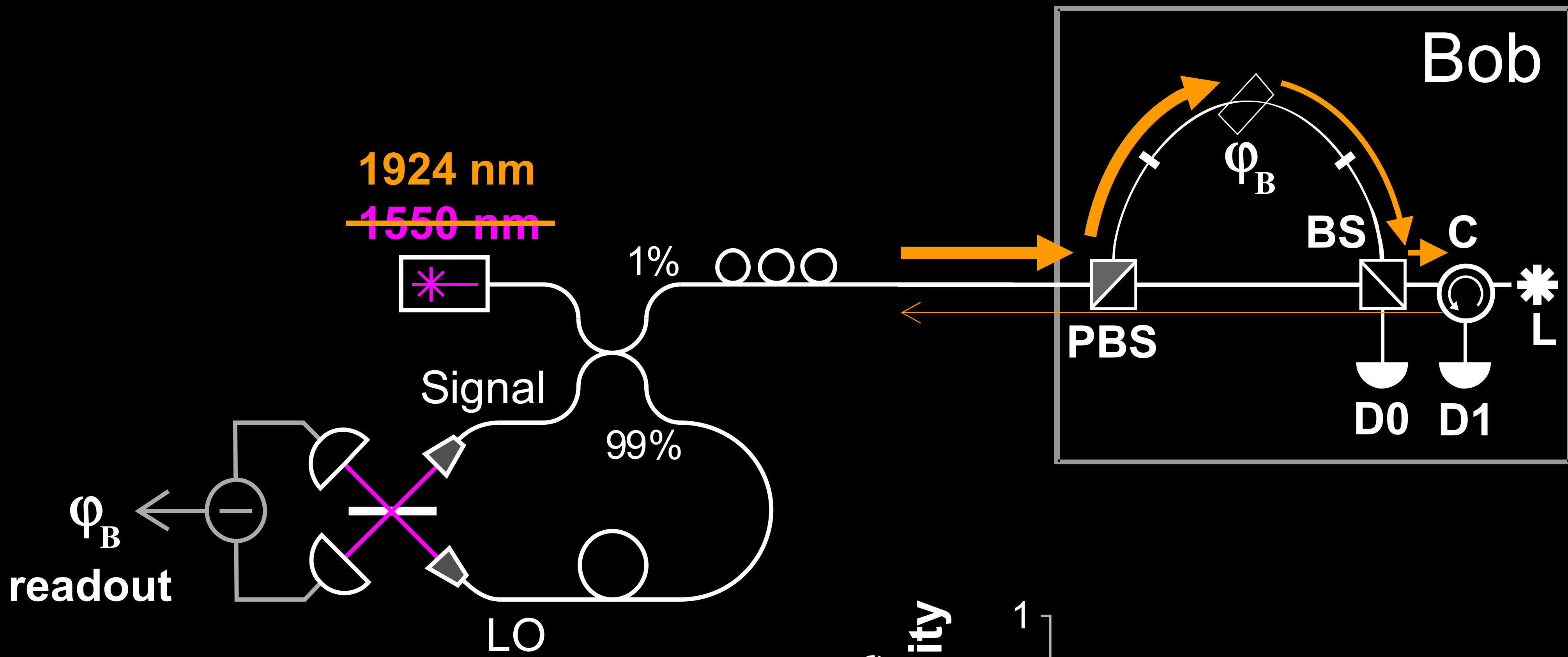
Trojan-horse attack on Bob

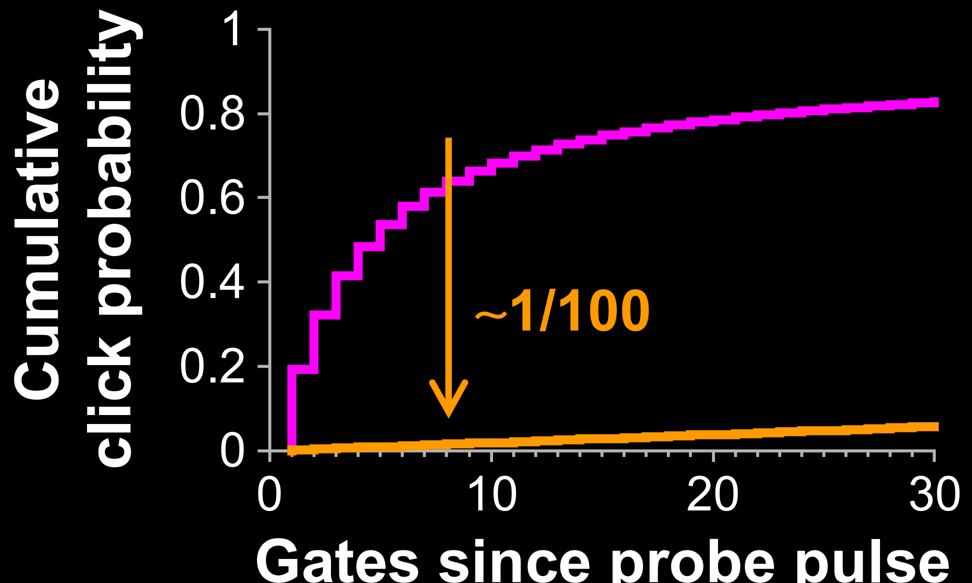




N. Jain *et al.*, New J. Phys. **16**, 123030 (2014)

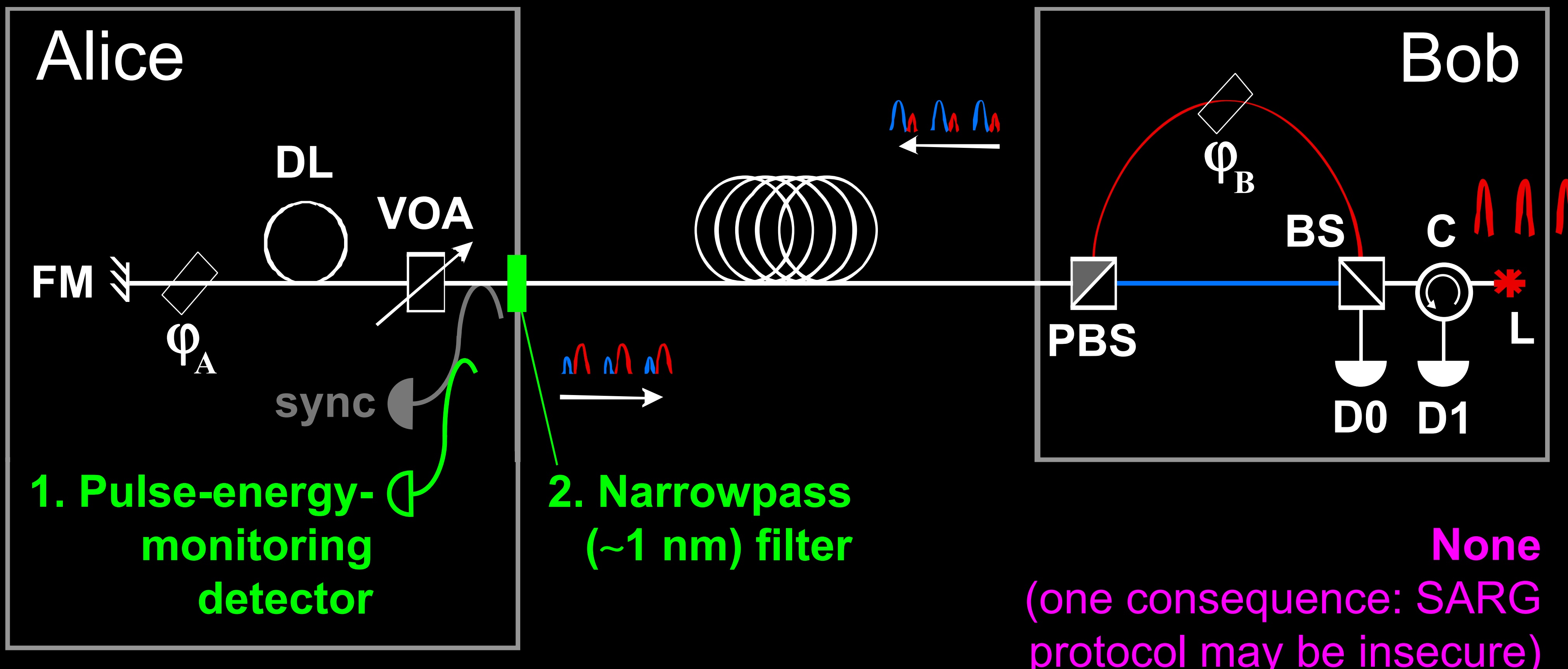
Trojan-horse attack on Bob





S. Sajeed *et al.*, Sci. Rep. **7**, 8403 (2017)

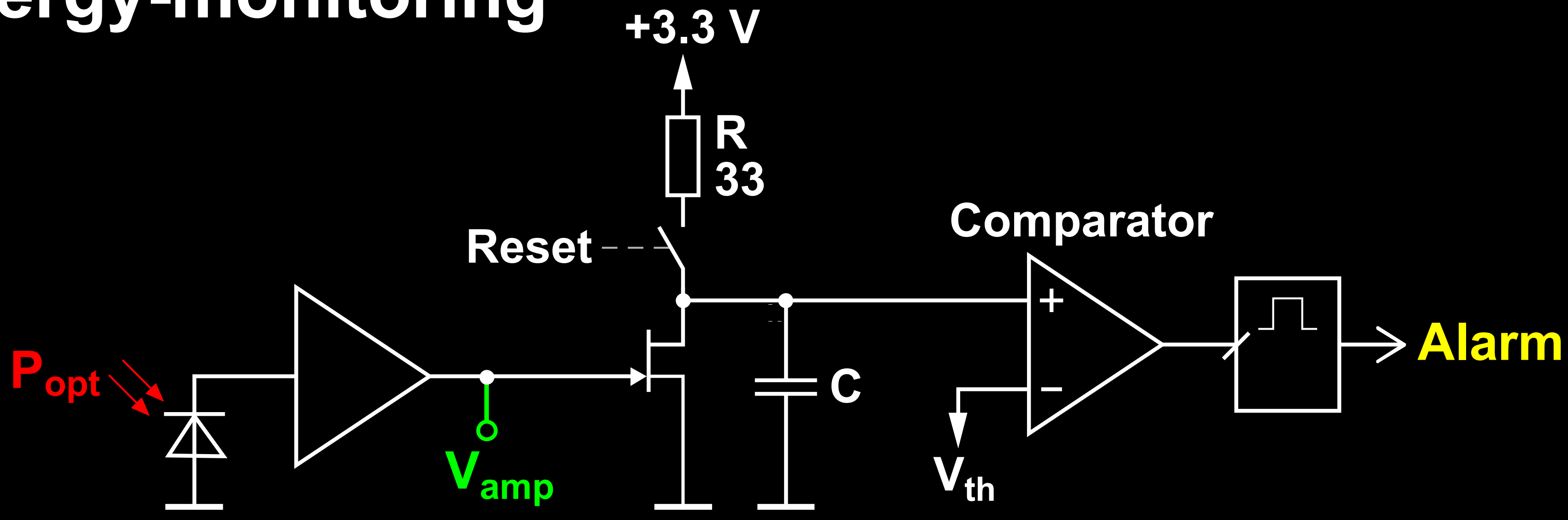
Countermeasures for plug-and-play system

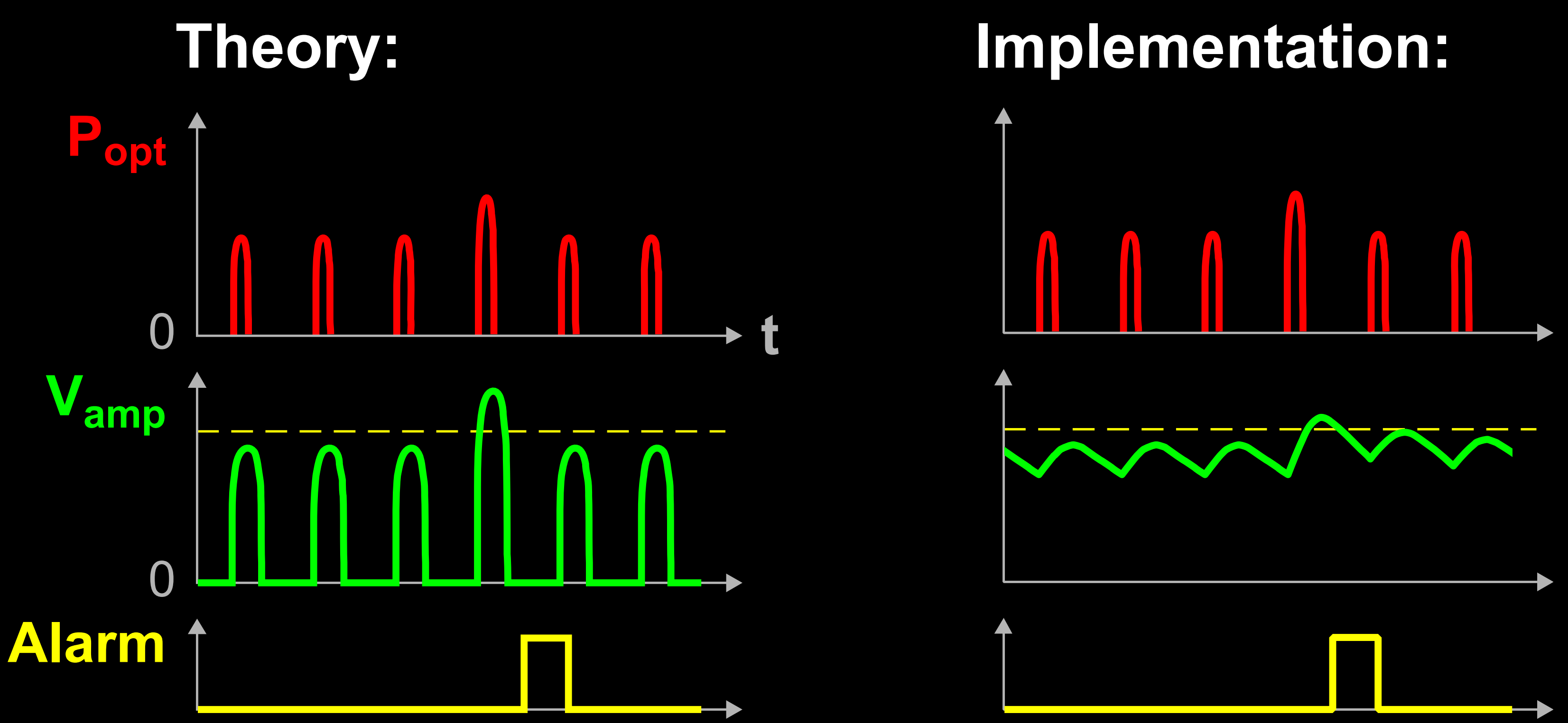


S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

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

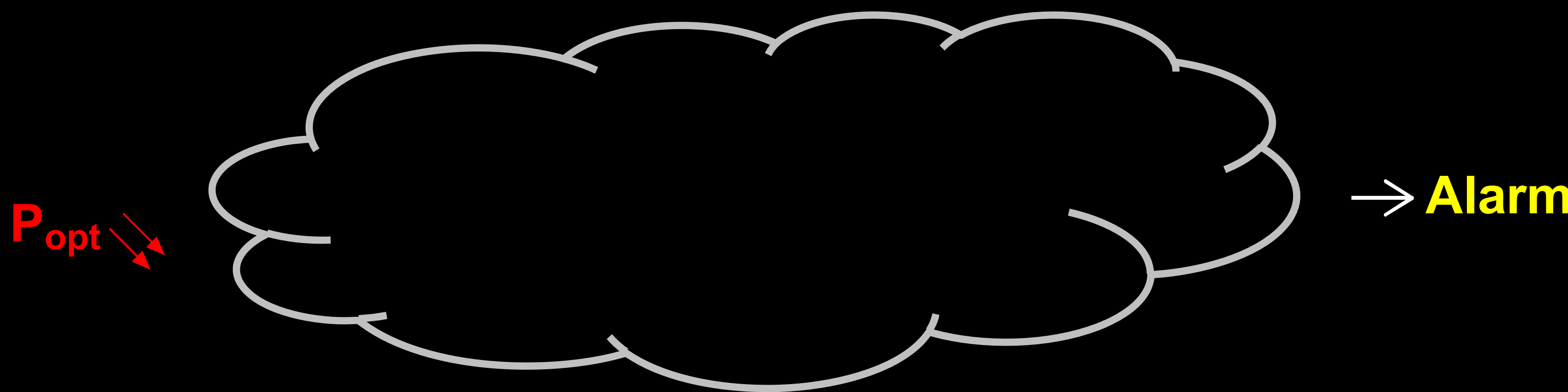
Pulse-energy-monitoring detector



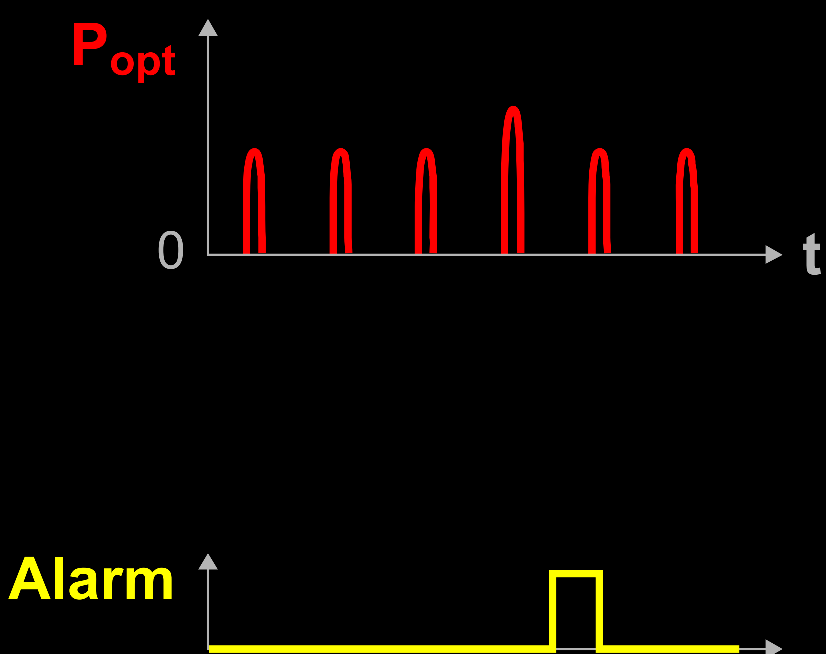


S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

Pulse-energy-monitoring detector

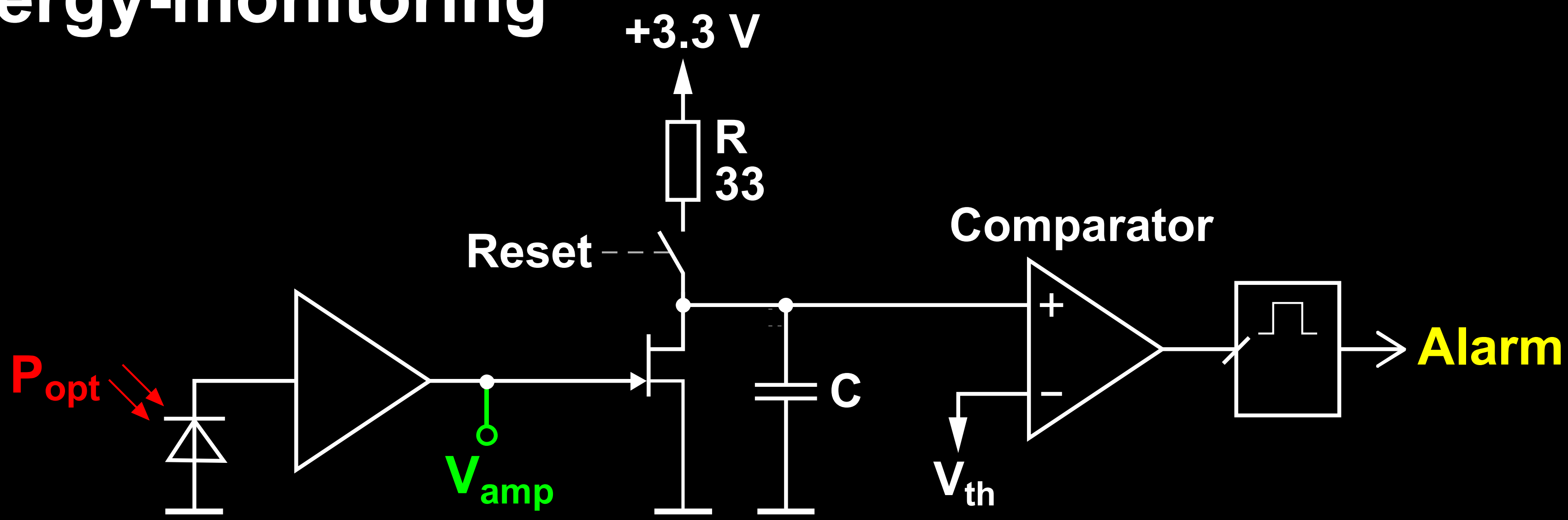


“Certification standard” (internal by ID Quantique):



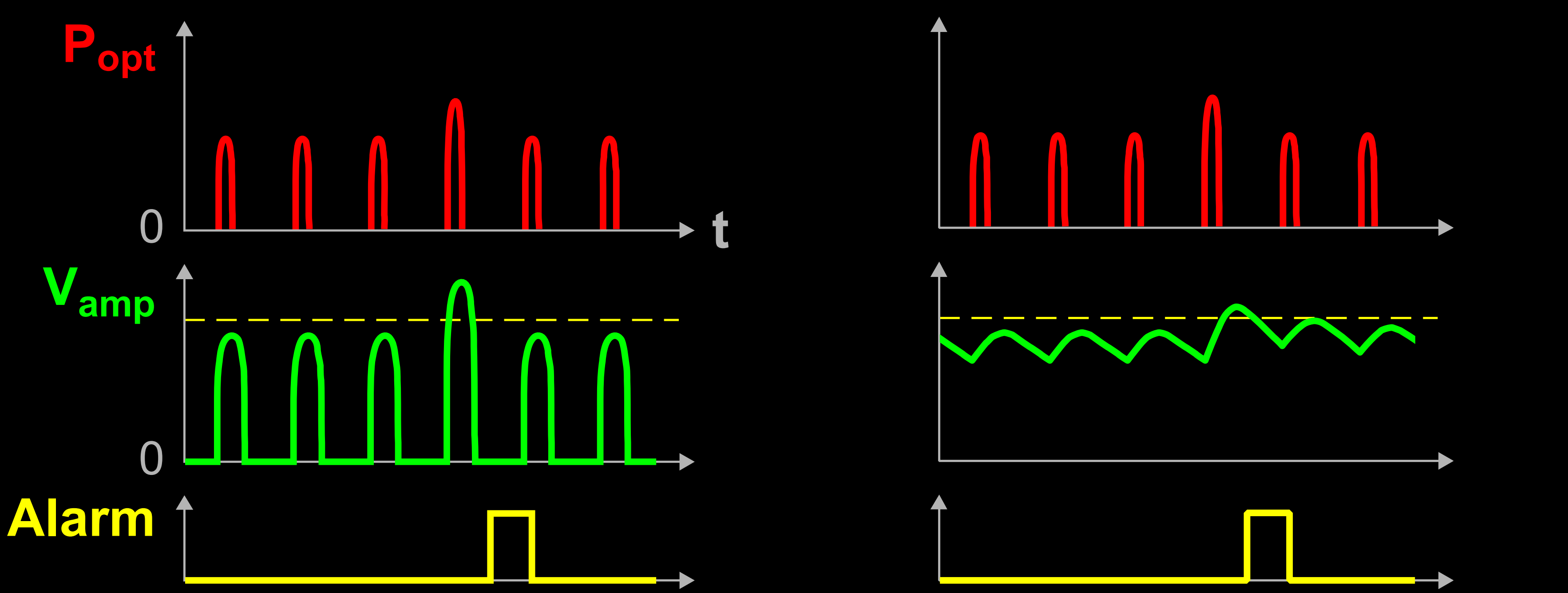
S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

Pulse-energy-monitoring detector



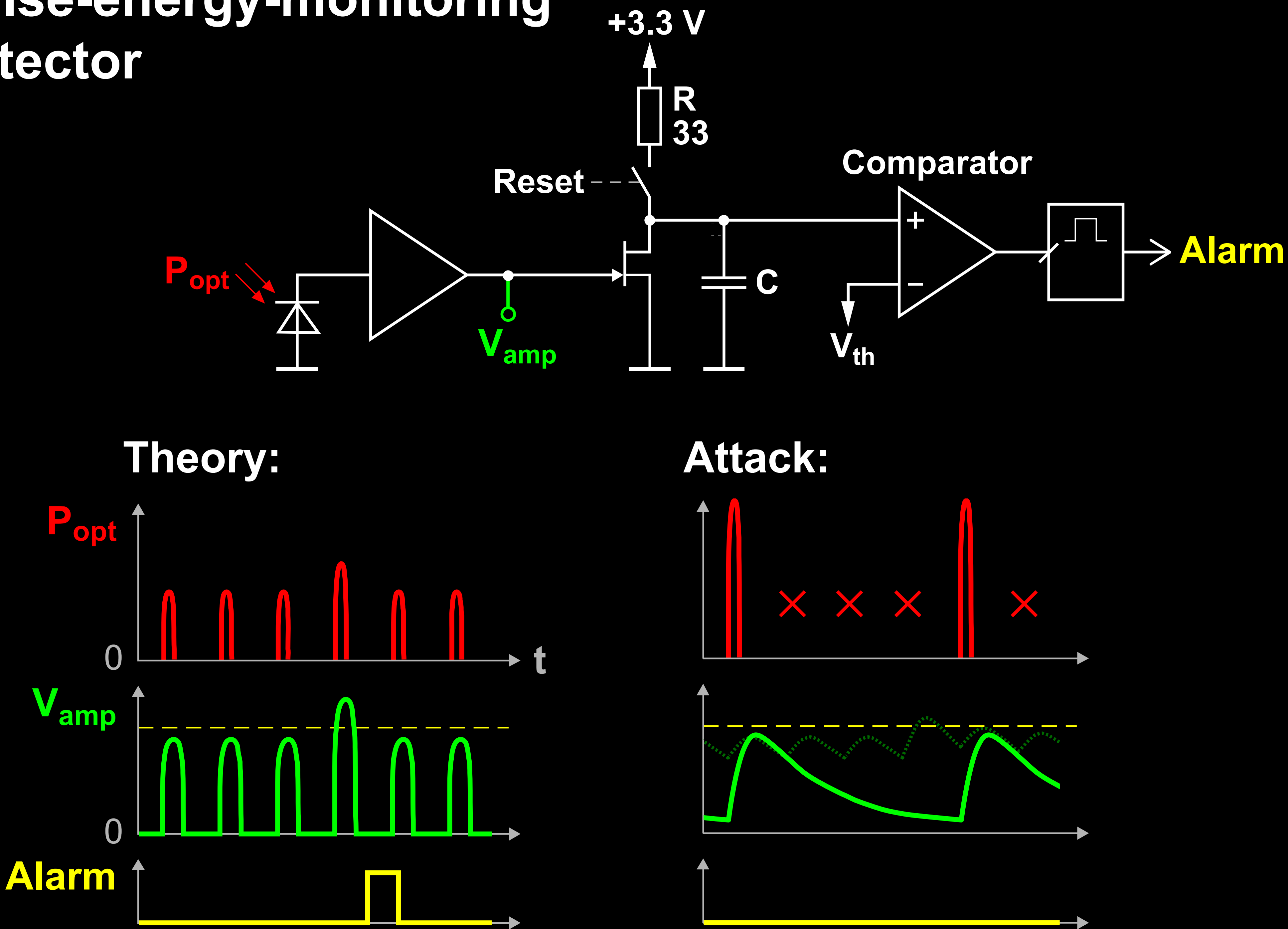
Theory:

Implementation:



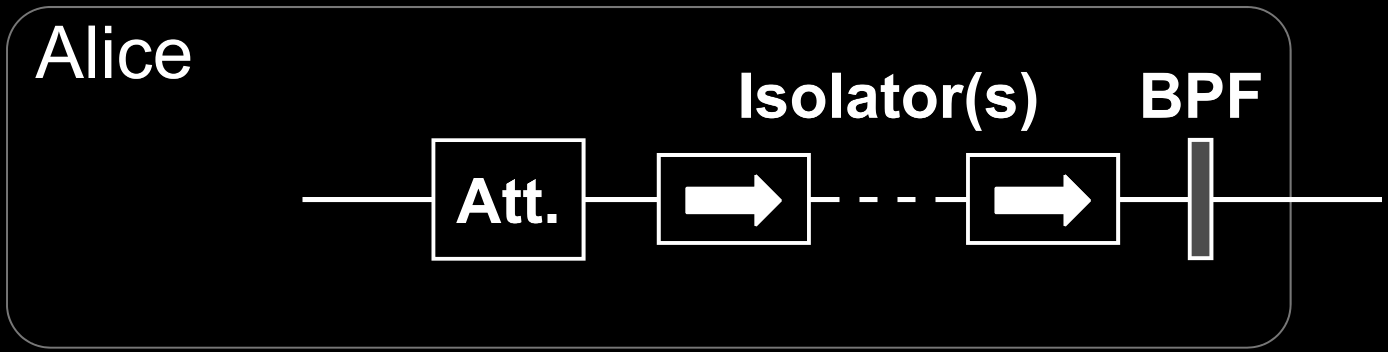
S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

Pulse-energy-monitoring detector



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

Draft security standard @ ETSI: Trojan-horse in one-way system



M. Lucamarini *et al.*, Phys. Rev. X **5**, 031030 (2015)

Winter school on quantum cybersecurity

Annual. Next: 25–31 January 2020
Les Diablerets, Switzerland

2 days (executive track) +
4 days (technical track, with 4 labs)

Overview talks + quantum technologies, including QKD

Lecturers in 2019: J. Baloo, C. Bennett, G. Brassard, E. Diamanti, R. Floeter, N. Gisin, J. Hart, B. Huttner, E. Hodges, V. Makarov, M. Mosca, S. Popescu, R. Renner, F. Ruess, G. Ribordy, V. Scarani, D. Stucki, C. Williams

30 students, first-come, sells out

€3200 / €1600 executive track only

Winter sports in breaks

Organised by IDQ

www.idquantique.com/winter-school-switzerland-25-31-january-2020

2016

2018

International school on quantum technology

Annual. Next: 1–7 March 2020
Roza Khutor, Russia

4 days of lectures and skiing, poster session

Tutorials on quantum sensing, computing, metrology, QKD

Lecturers in 2019: A. Akimov, V. Balykin, M. Chekhova, V. Eliseev, A. Fedyanin, A. Korolkov, L. Krivitsky, V. Makarov, A. Odinokov, O. Snigirev, S. Straupe, A. Urivsky, S. Vyatchanin, F. Zhelezko

100 students, competitive admission

€200

4 h of pro skiing instruction

Organised by Центр Квантовых Технологий

qutes.org

2019