

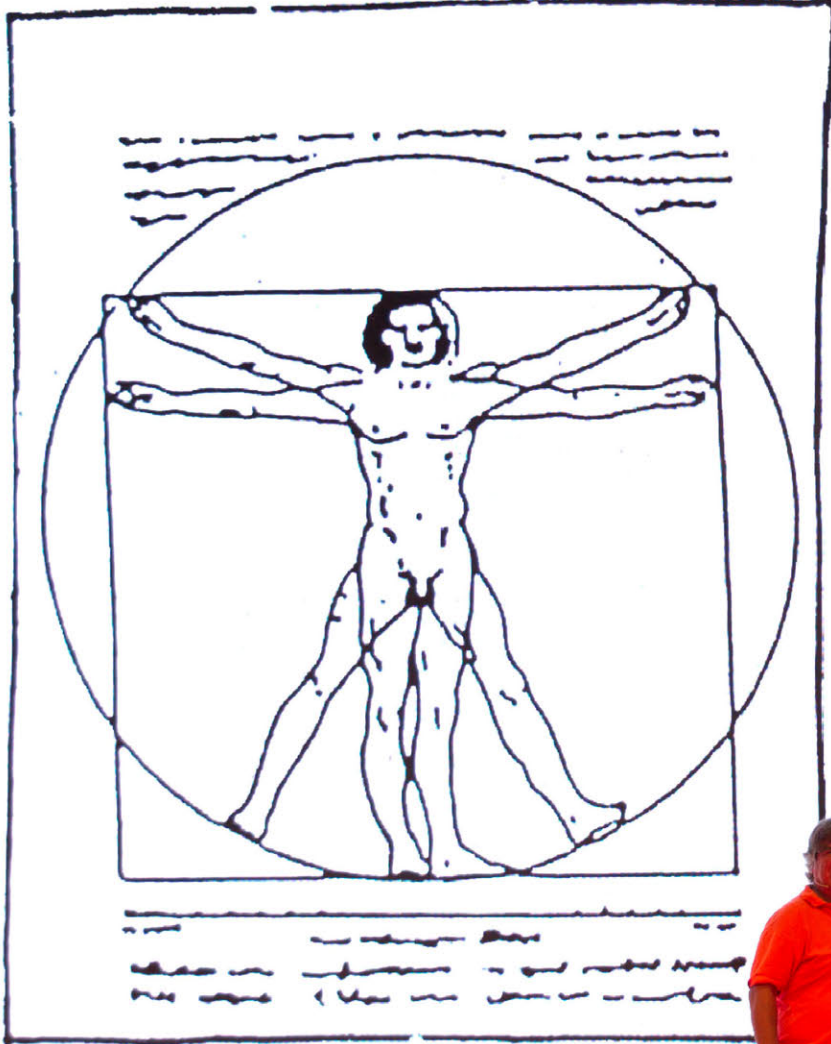
Quantum hacking

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

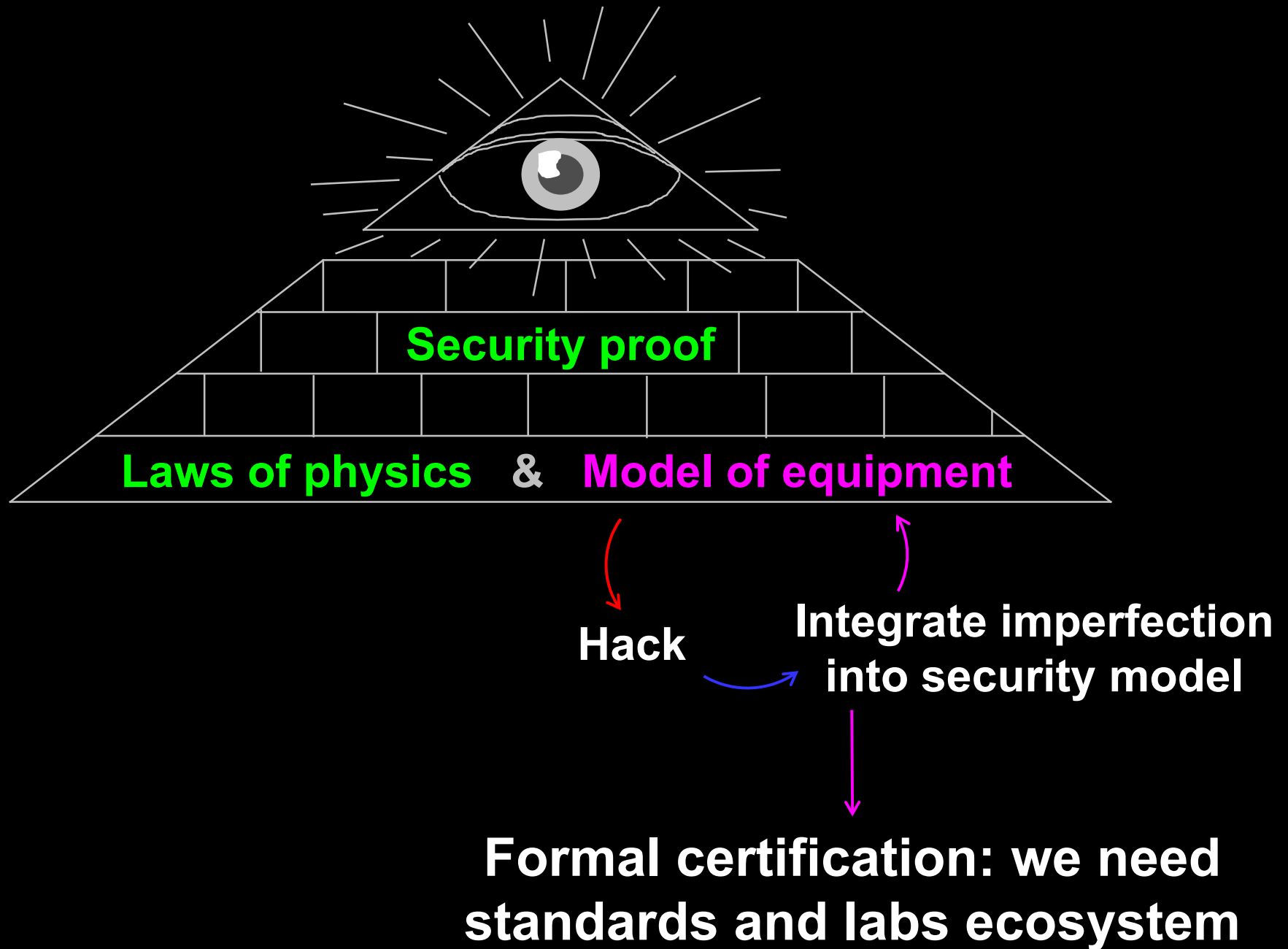


EXPERIMENT

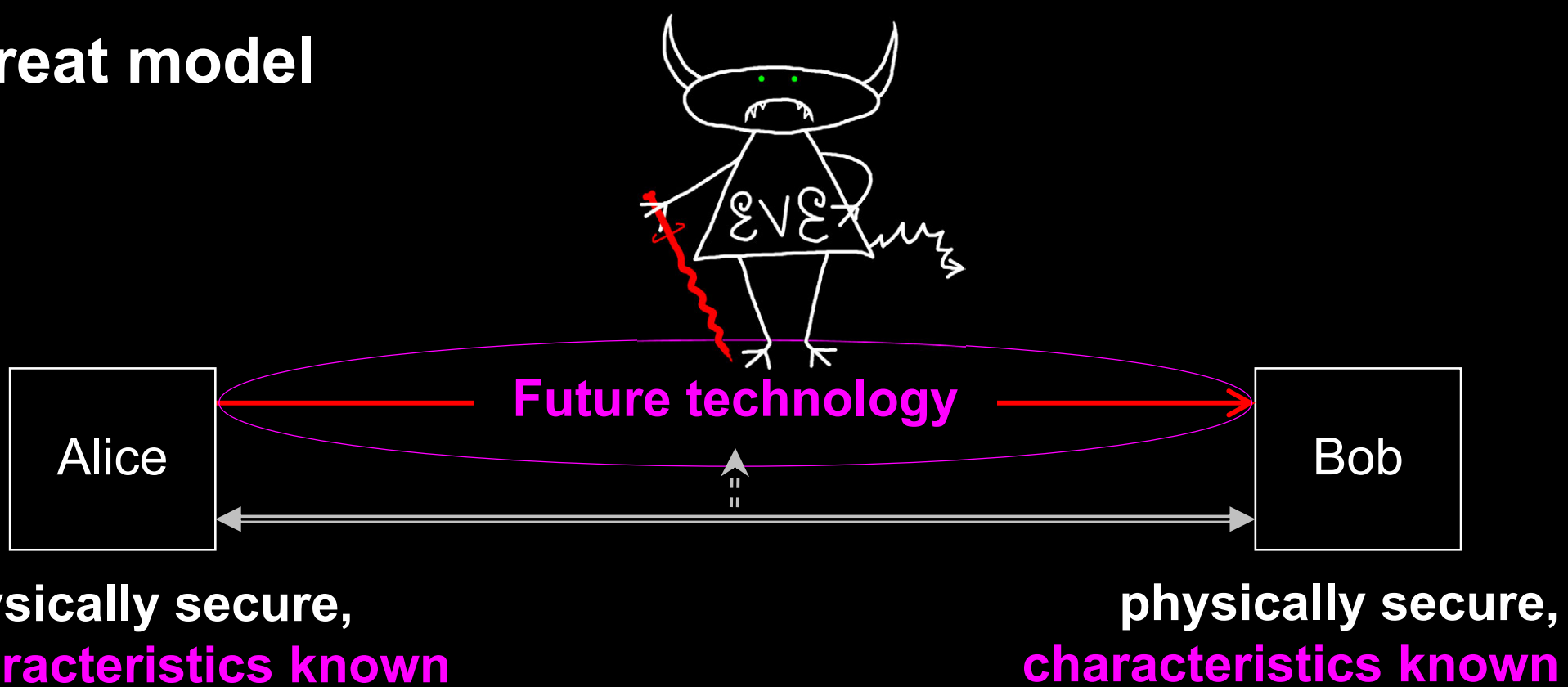


MSTEVENS

Implementation security of quantum communications



Threat model



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

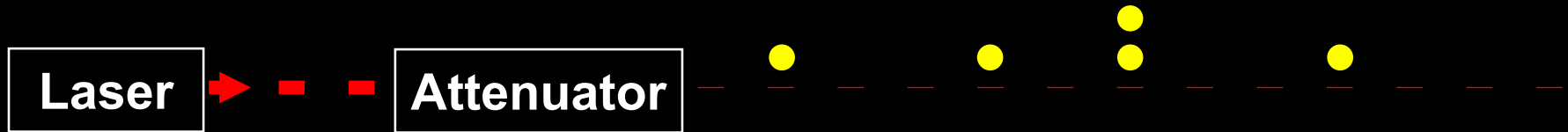
C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992)

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:

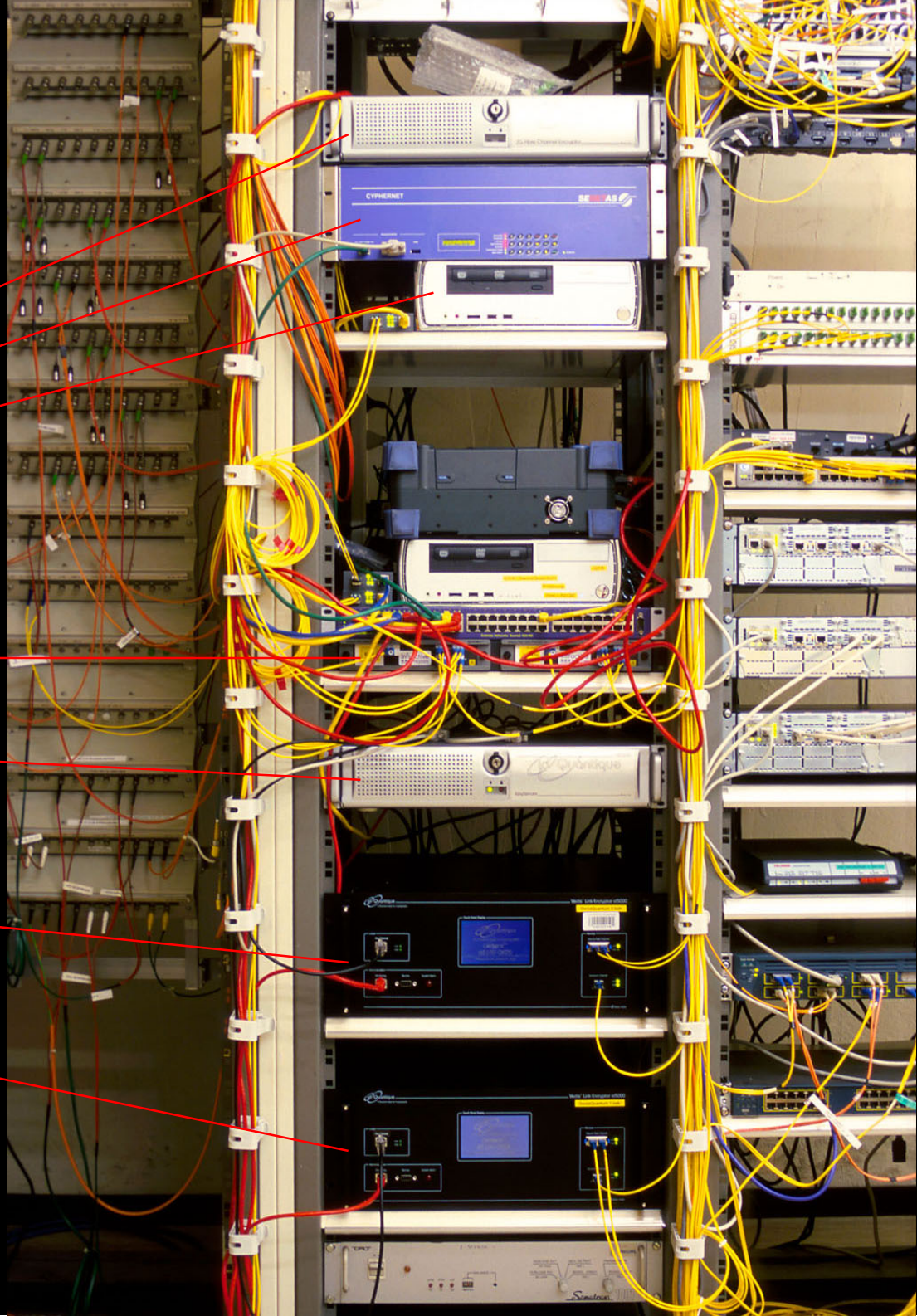
- L2, 2 Gbit/s
- L2, 10 Gbit/s
- L3 VPN, 100 Mbit/s

WDMs

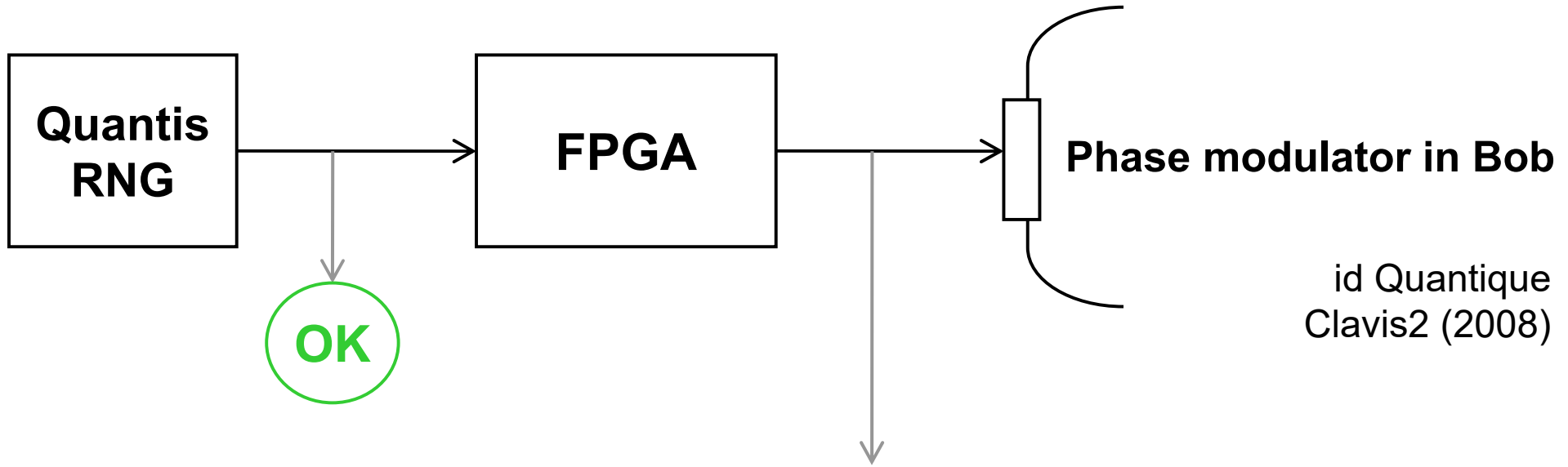
Key manager

QKD to another node (4 km)

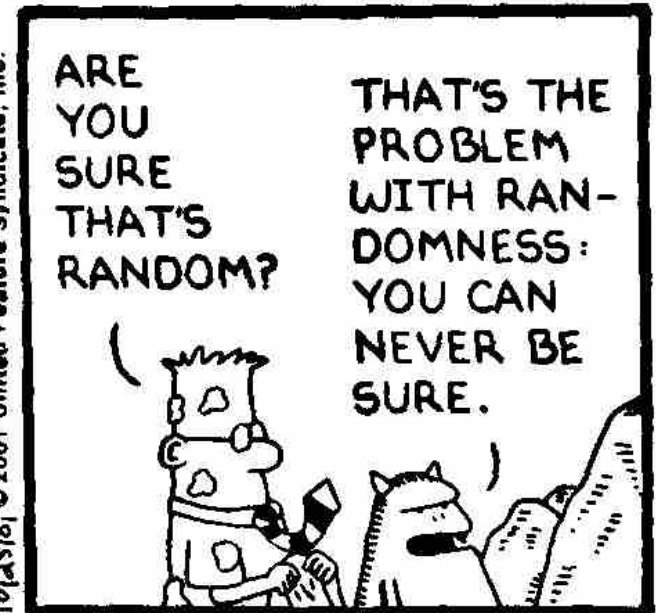
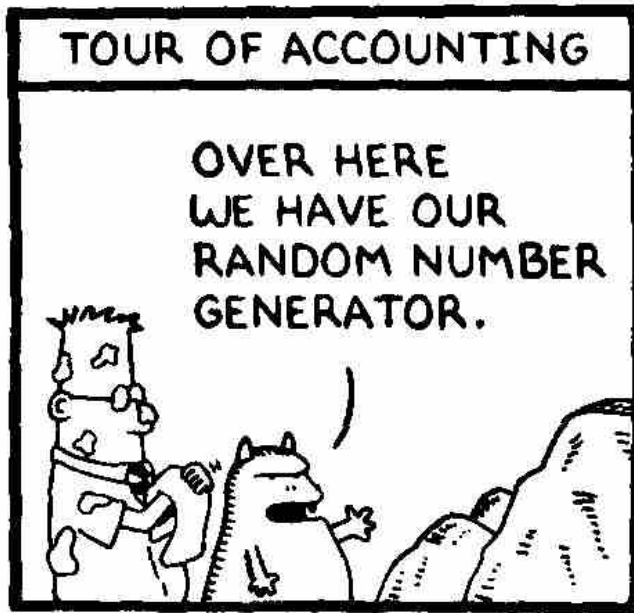
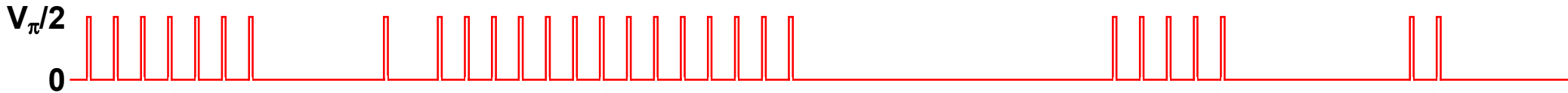
QKD to another node (14 km)



True randomness?

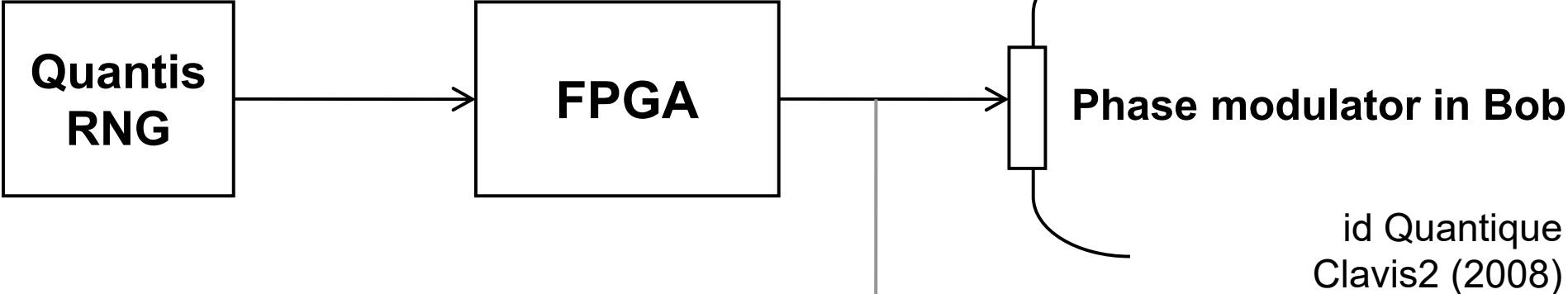


id Quantique
Clavis2 (2008)

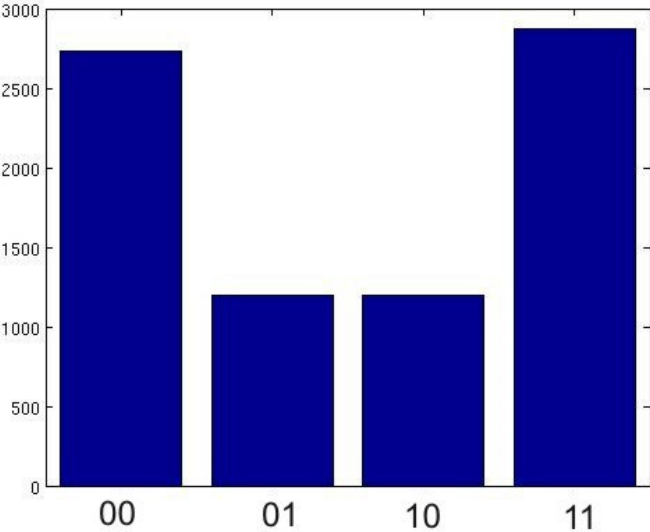


10/25/01 © 2001 United Feature Syndicate, Inc.

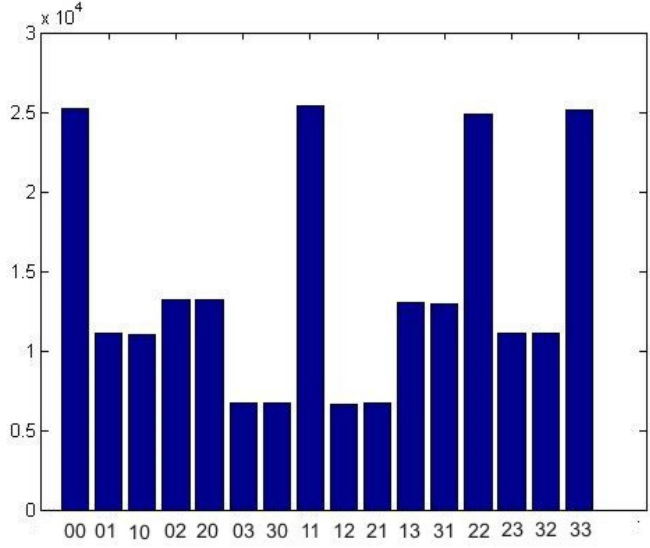
True randomness?



Bob:



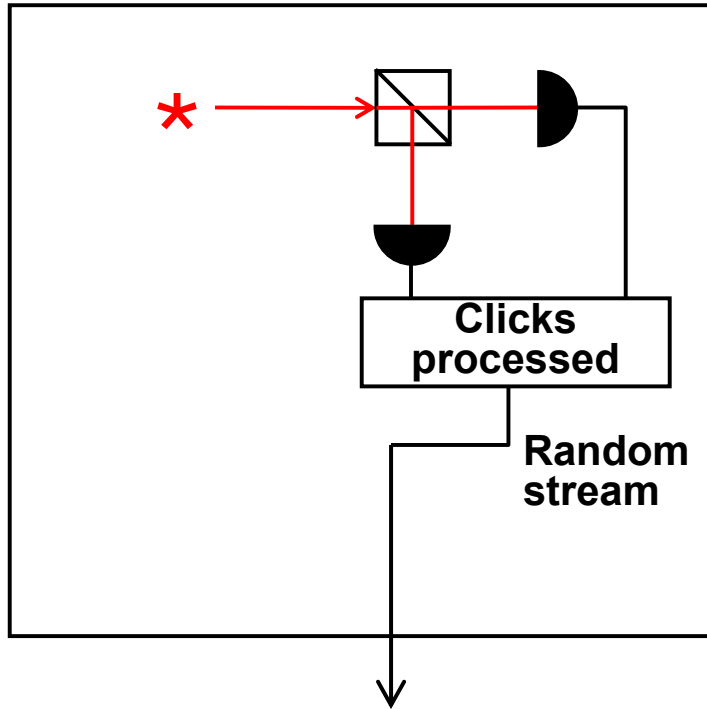
Alice:



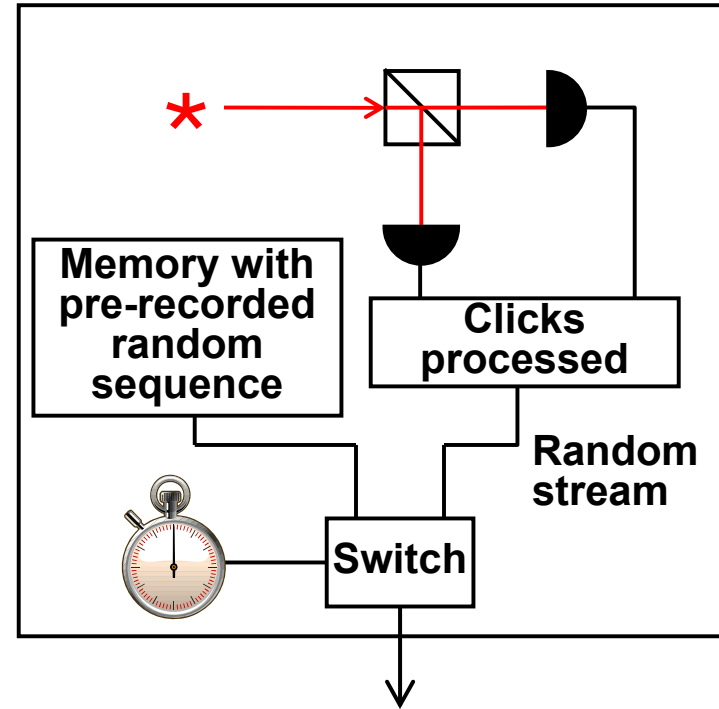
Issue reported patched in 2010

Do we trust the manufacturer?

Quantis RNG



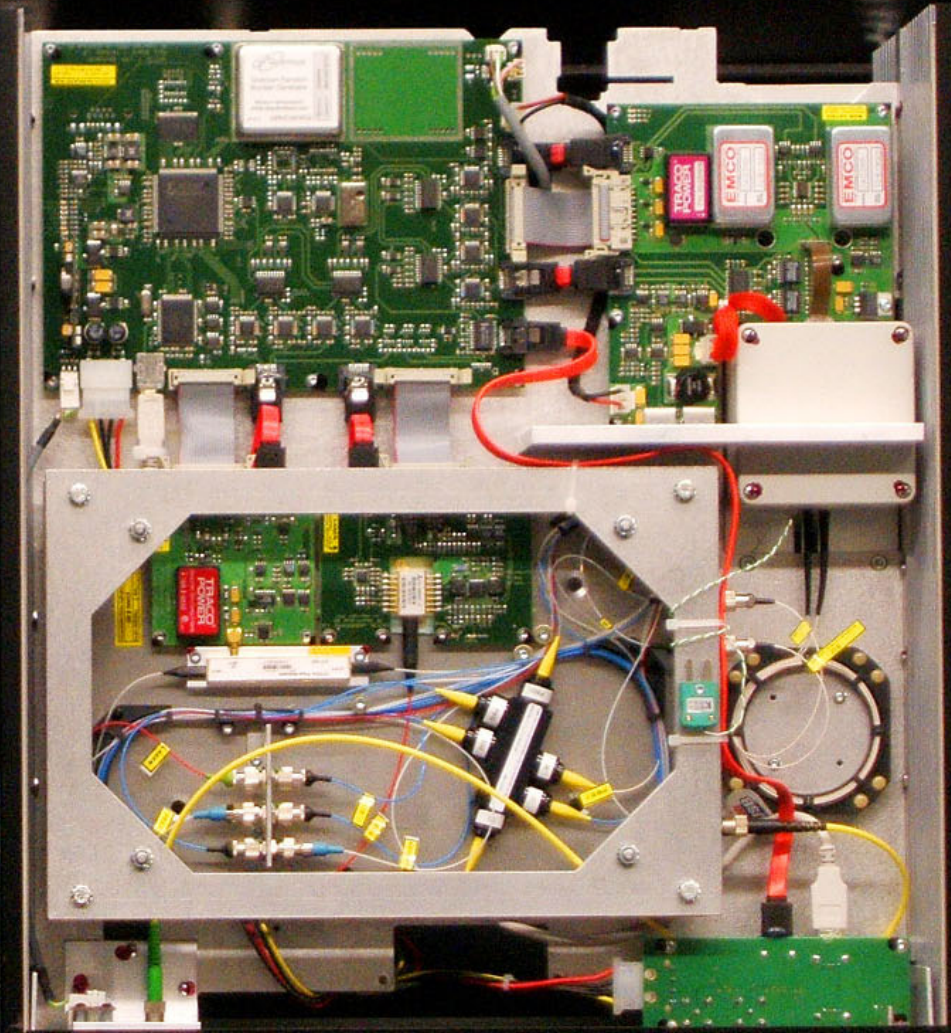
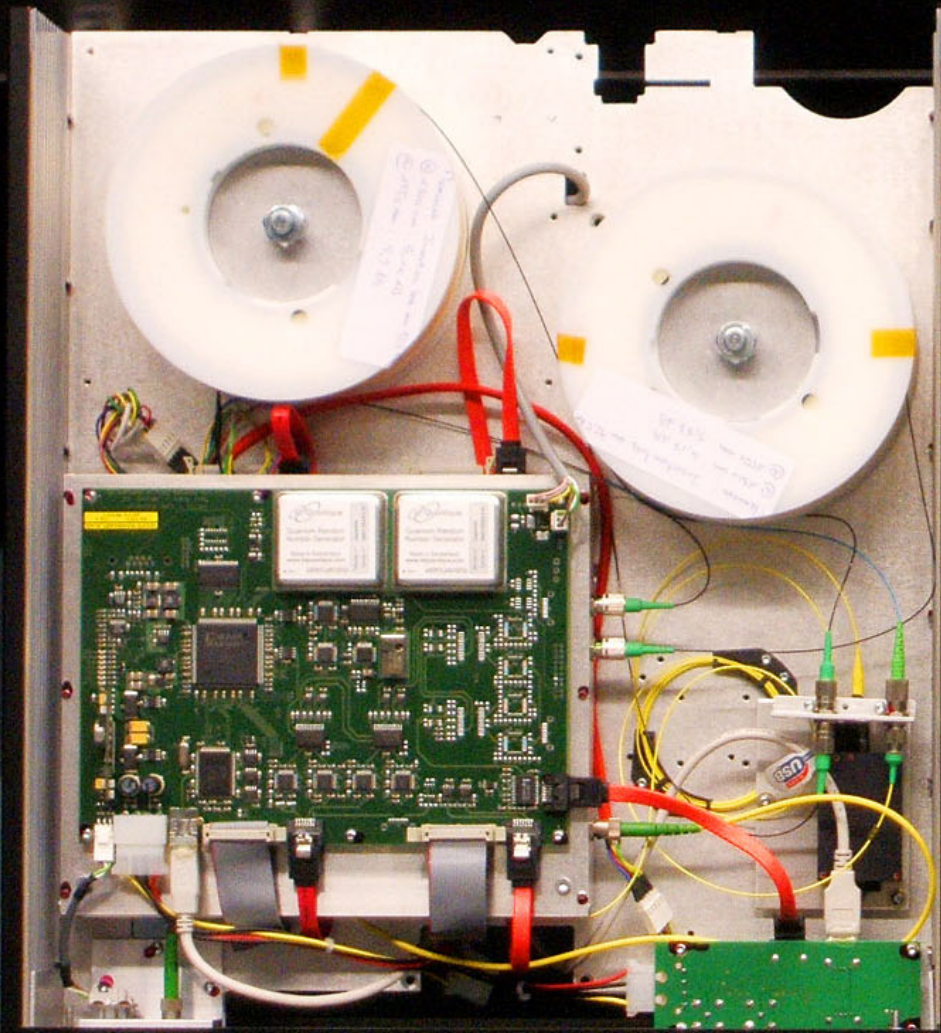
Quantis RNG, Trojan-horsed :)



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

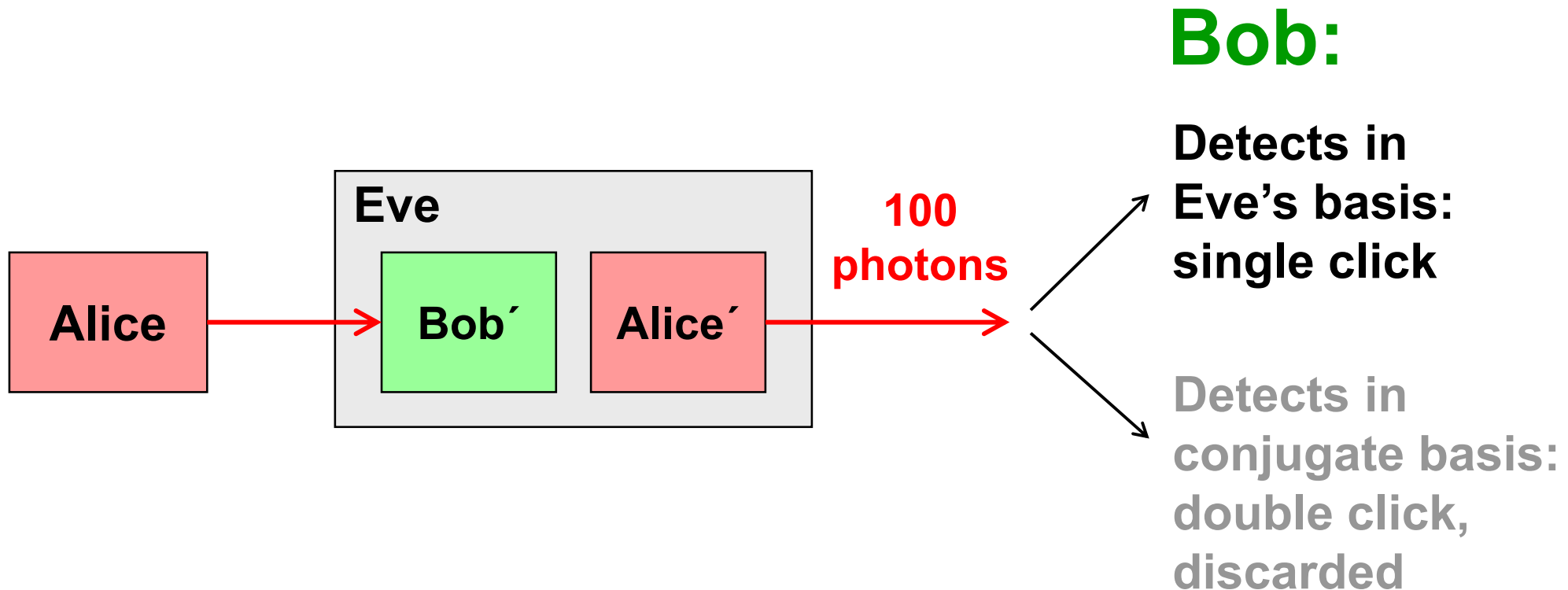
Bob

Double clicks

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

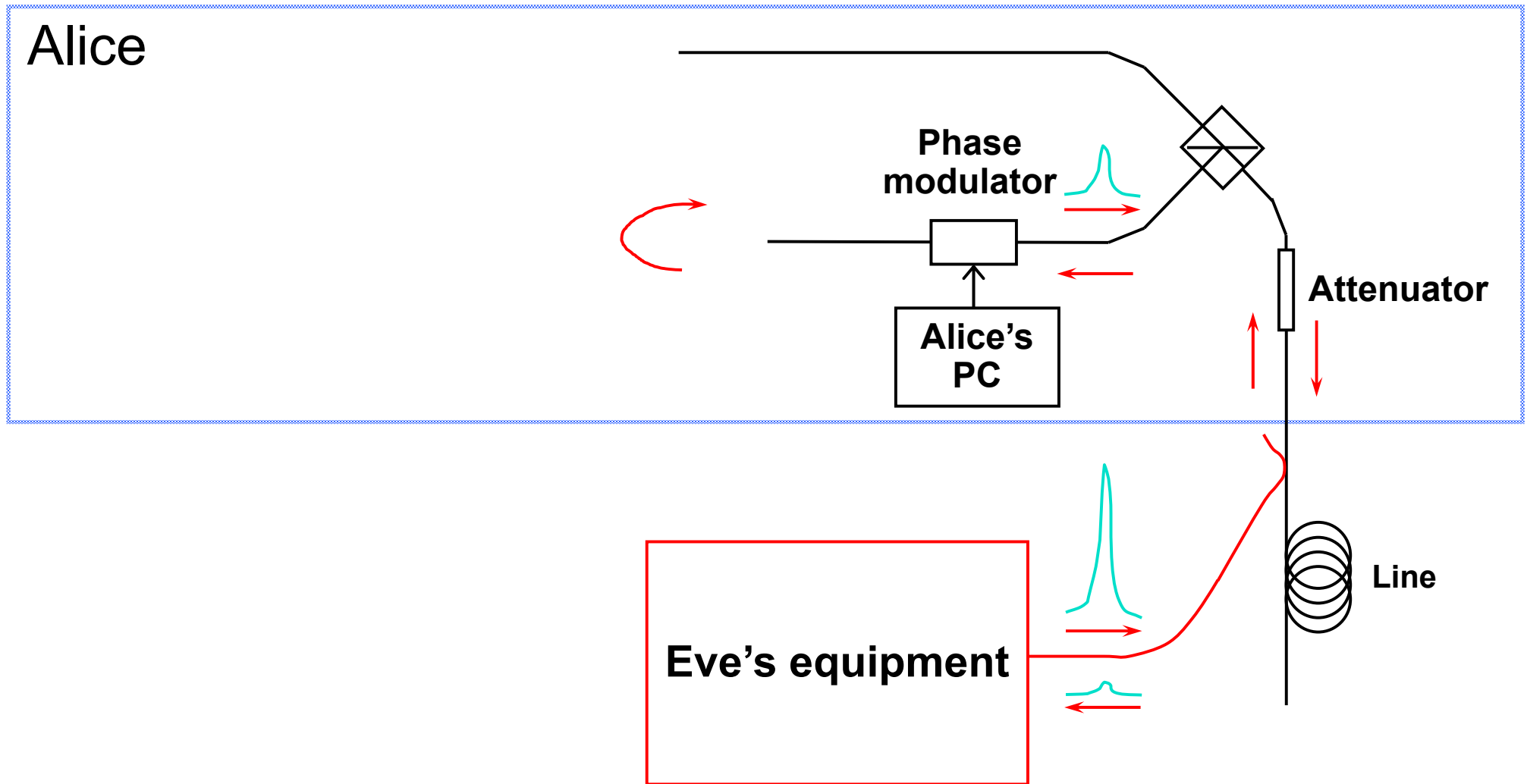
Discard them?

Intercept-resend attack... **with a twist:**



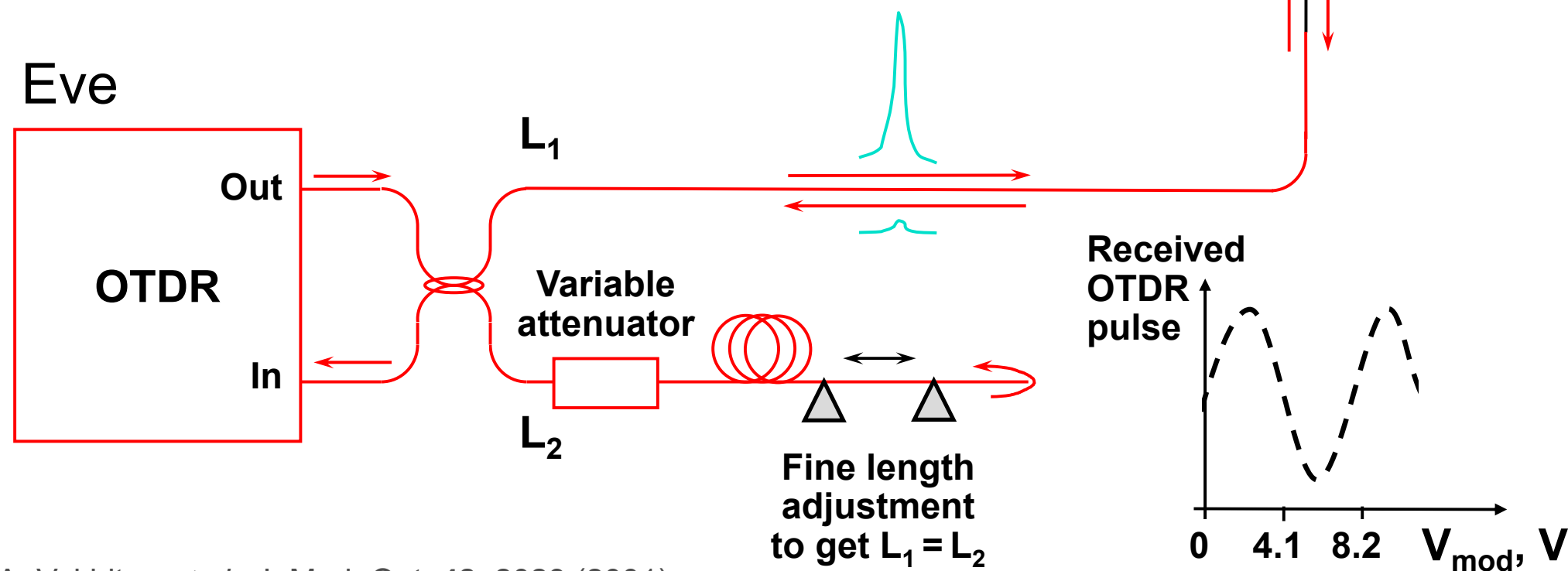
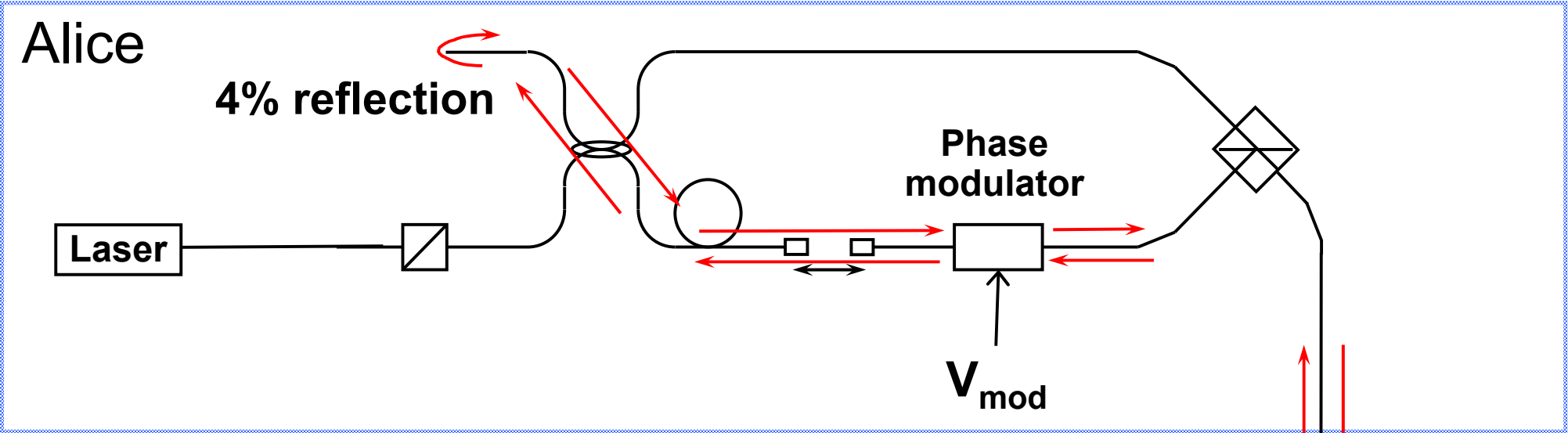
Proper treatment for double clicks: assign a random bit value.

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)

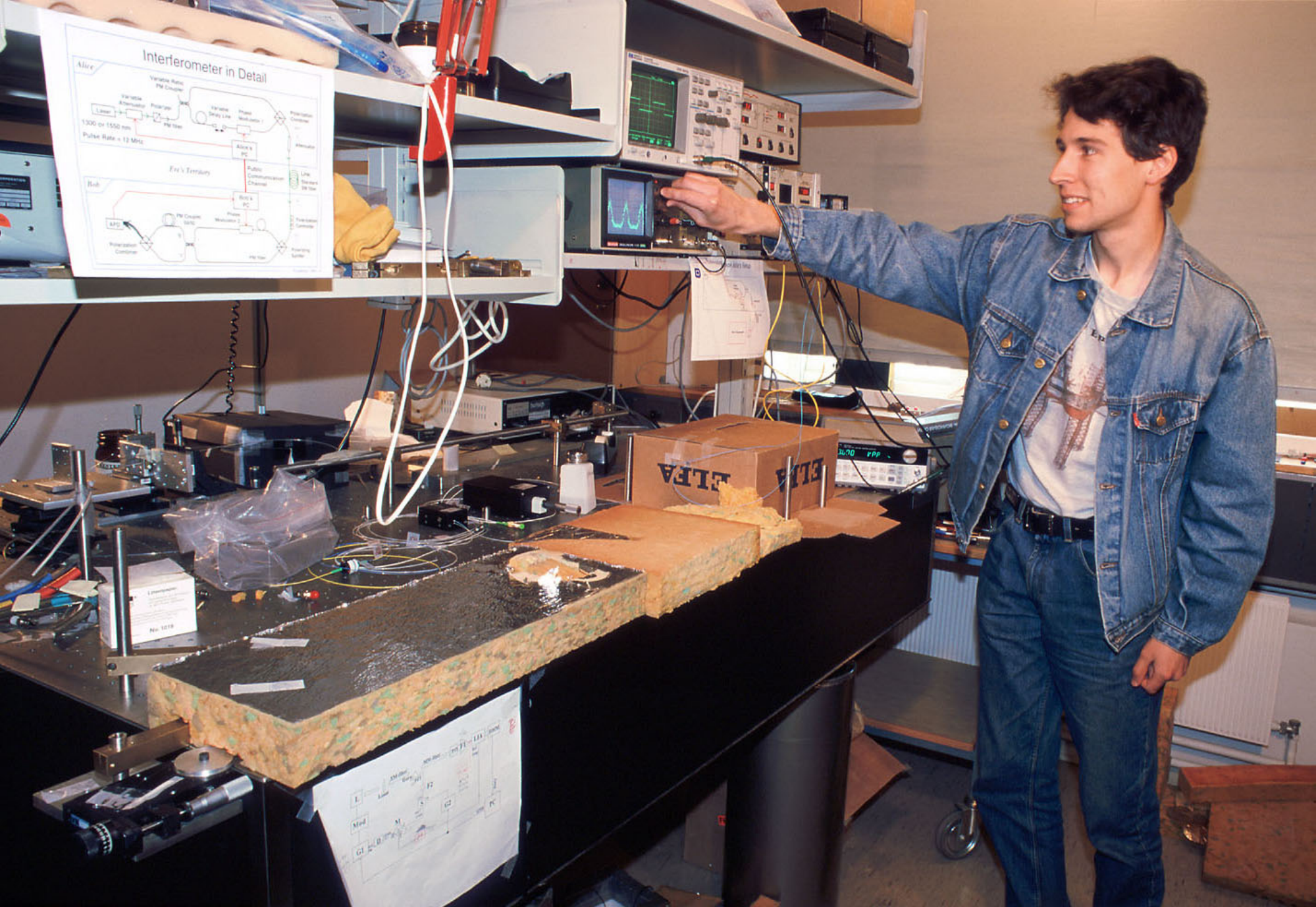
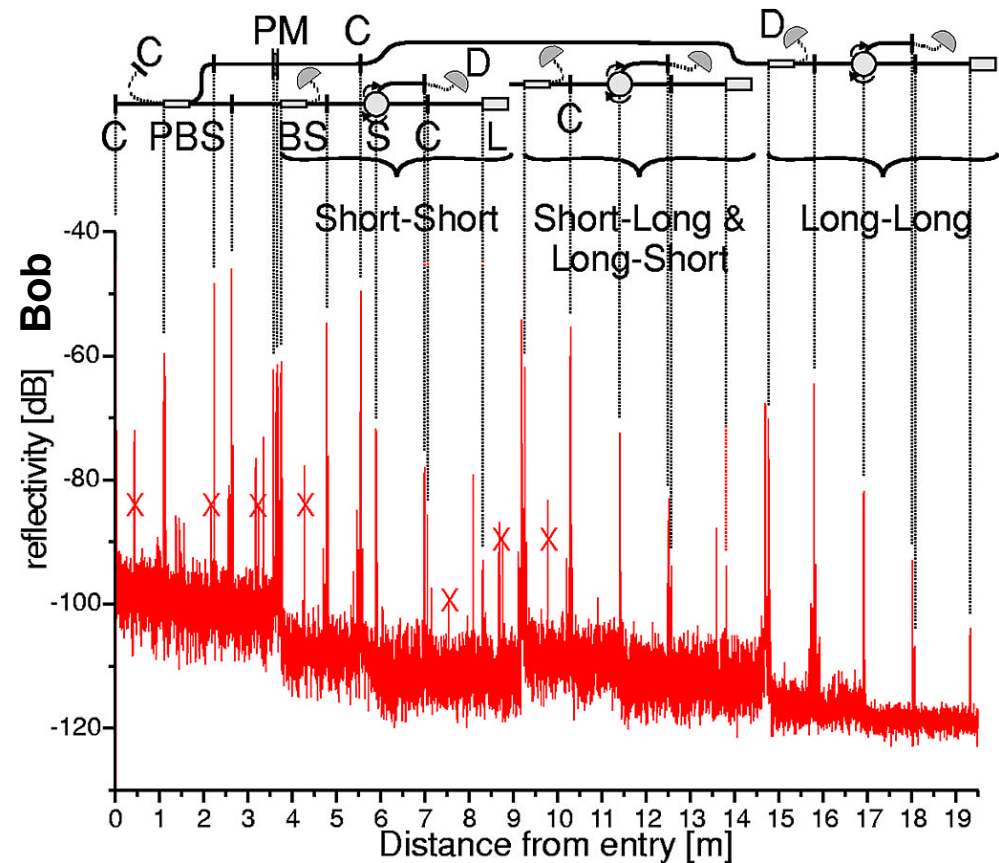
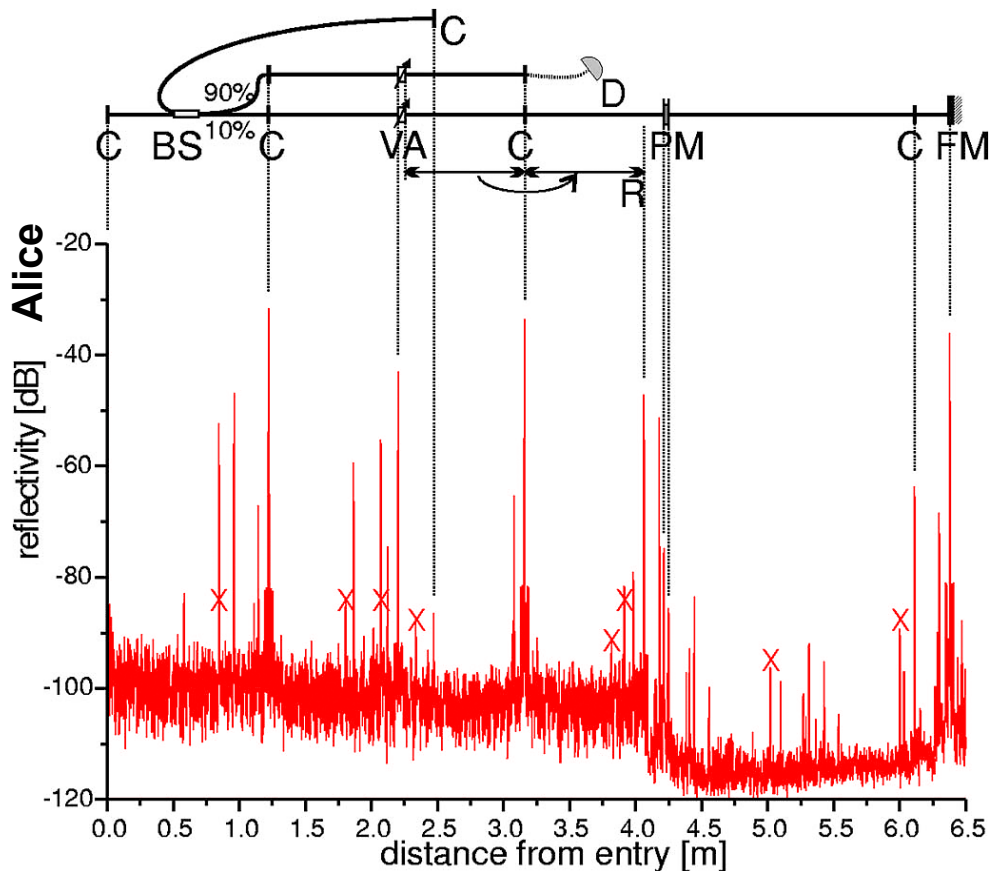


Photo ©2000 Vadim Makarov

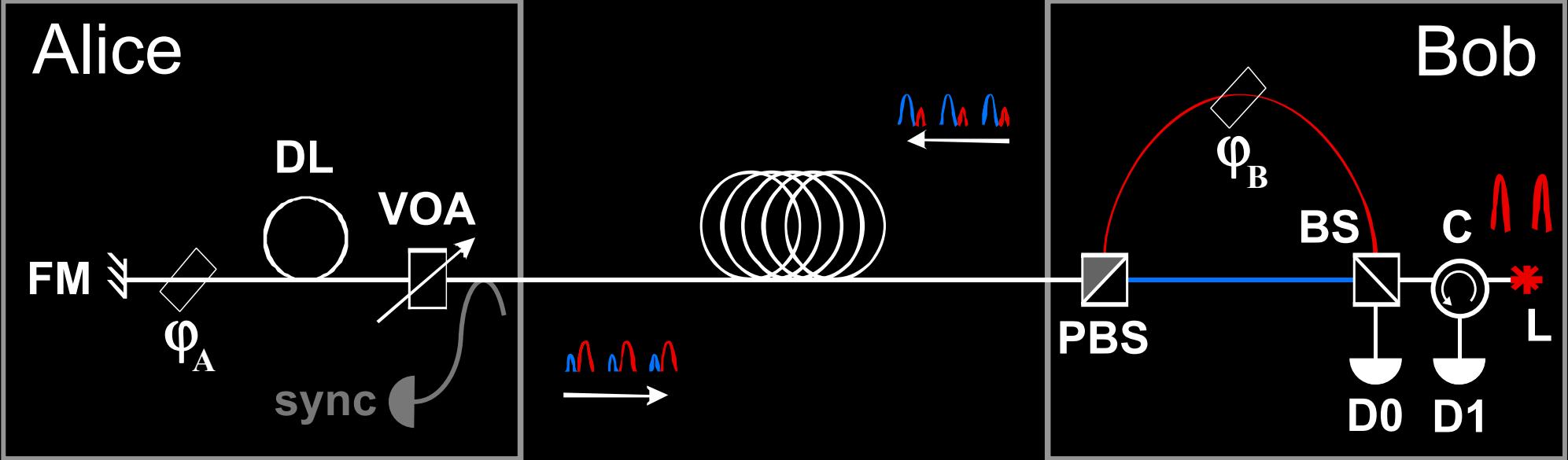
Artem Vakhitov tunes up Eve's setup

Trojan-horse attack for plug-and-play system

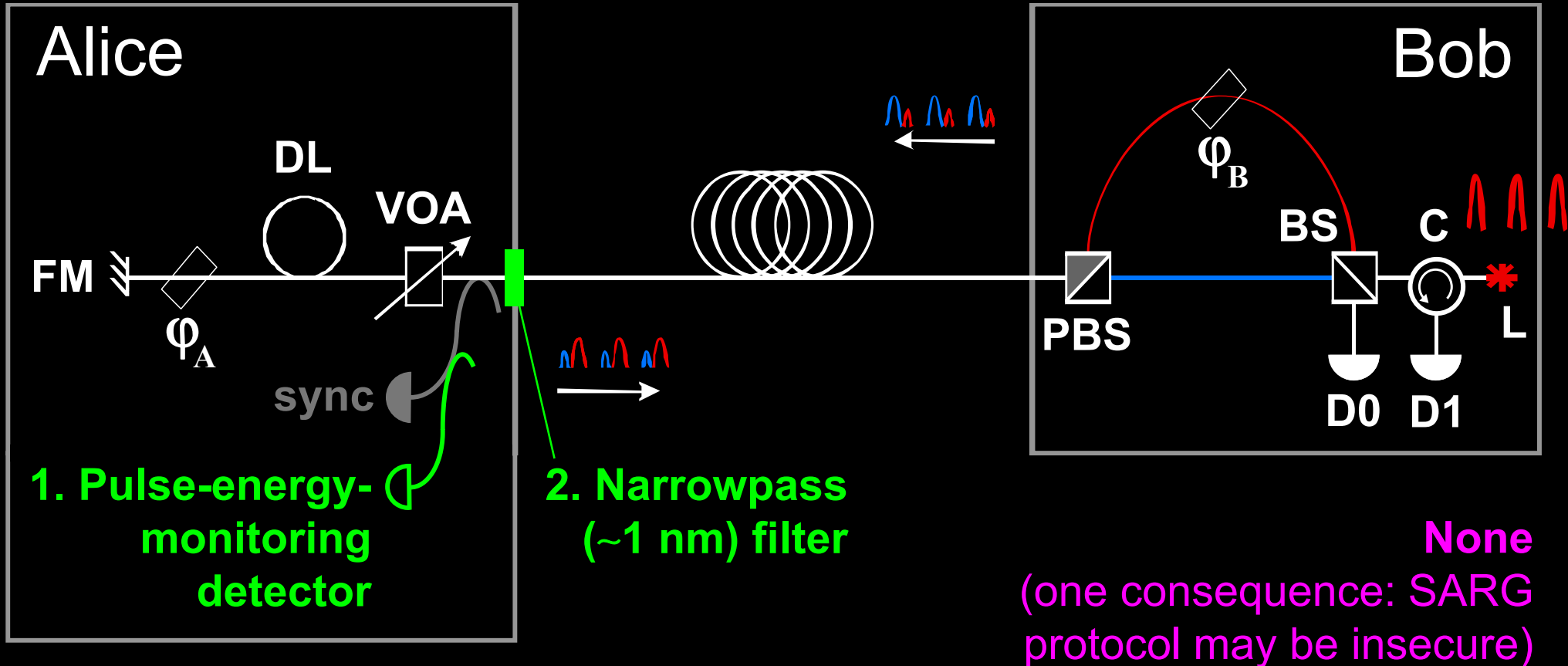


Eve gets back one photon → in principle, extracts 100% information

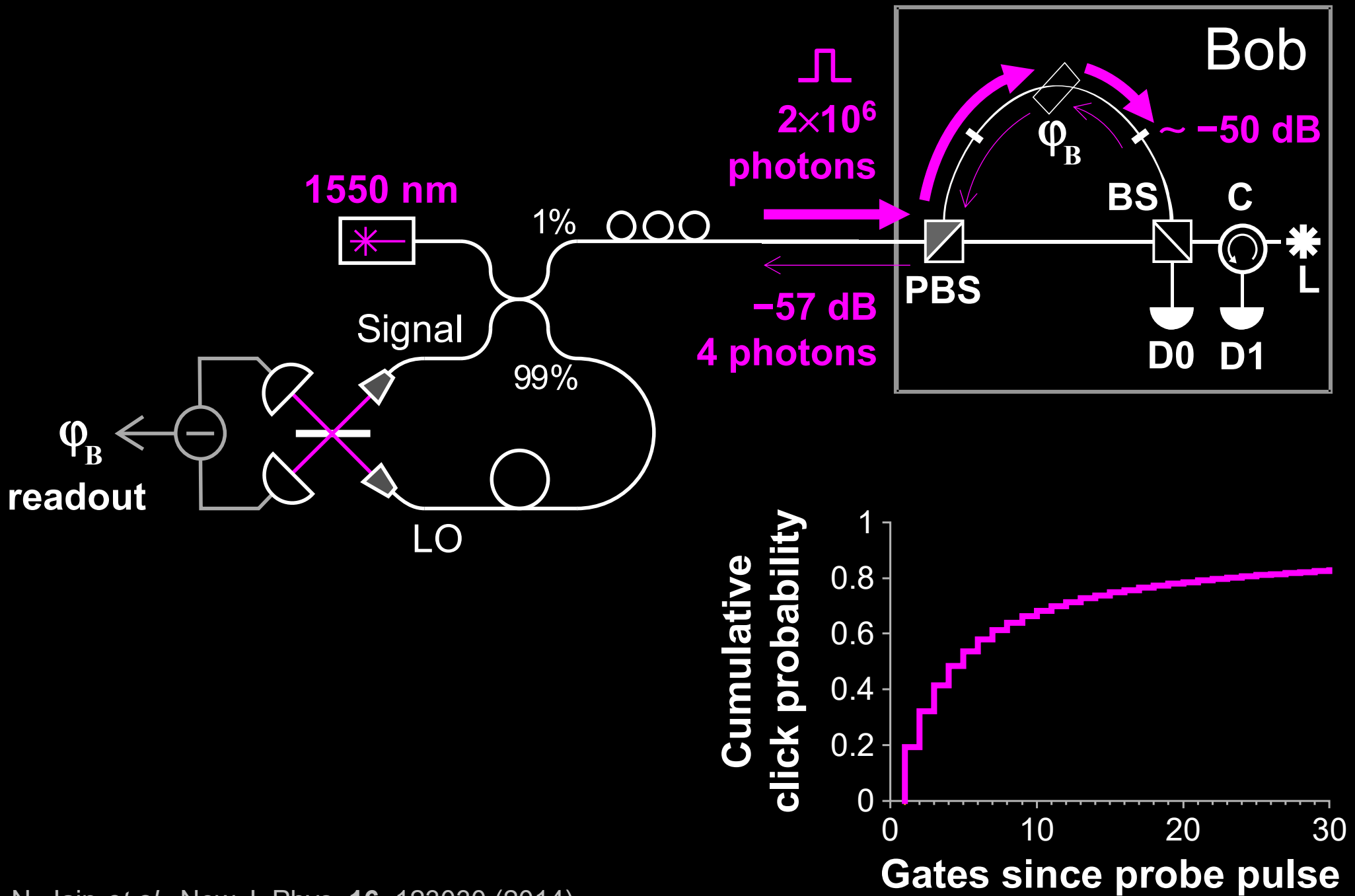
Countermeasures?



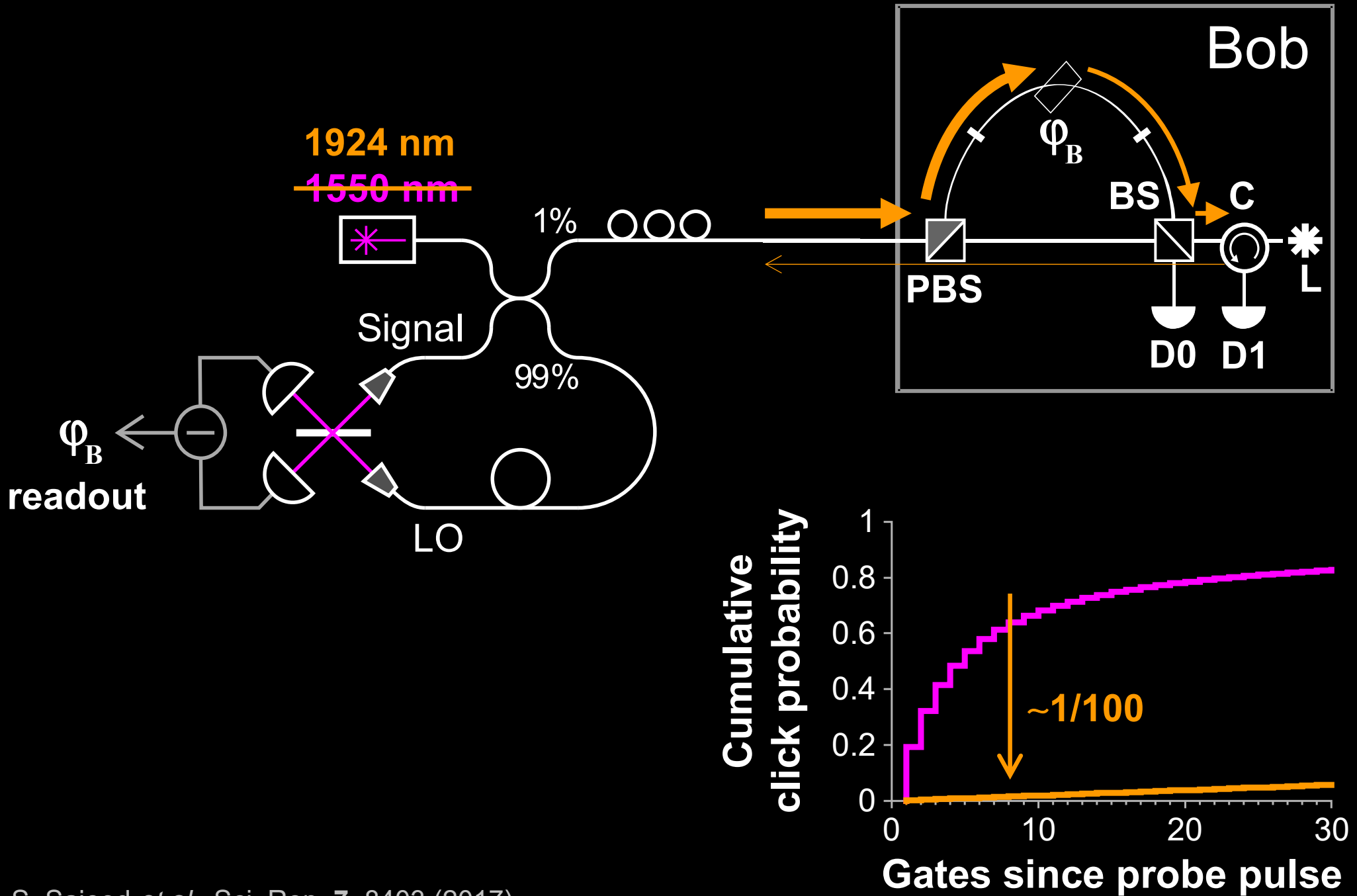
Countermeasures for plug-and-play system



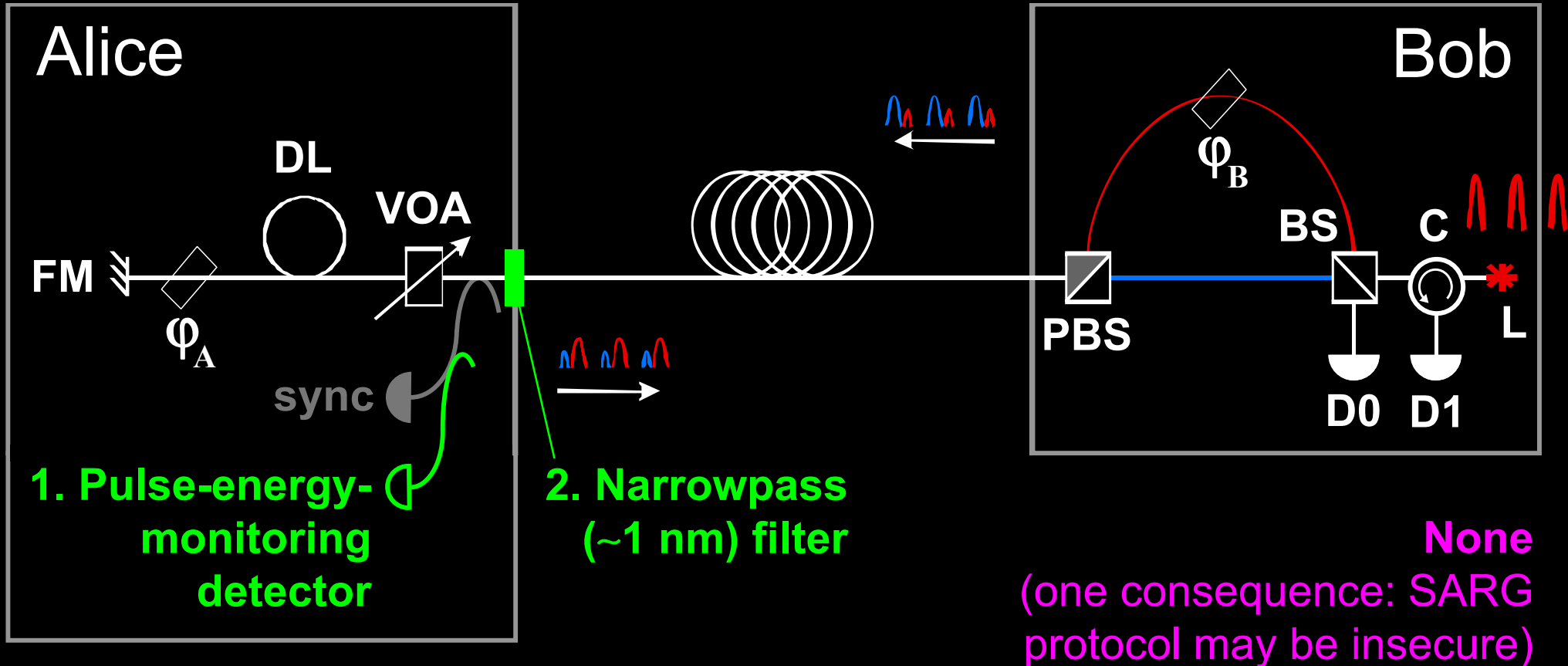
Trojan-horse attack on Bob



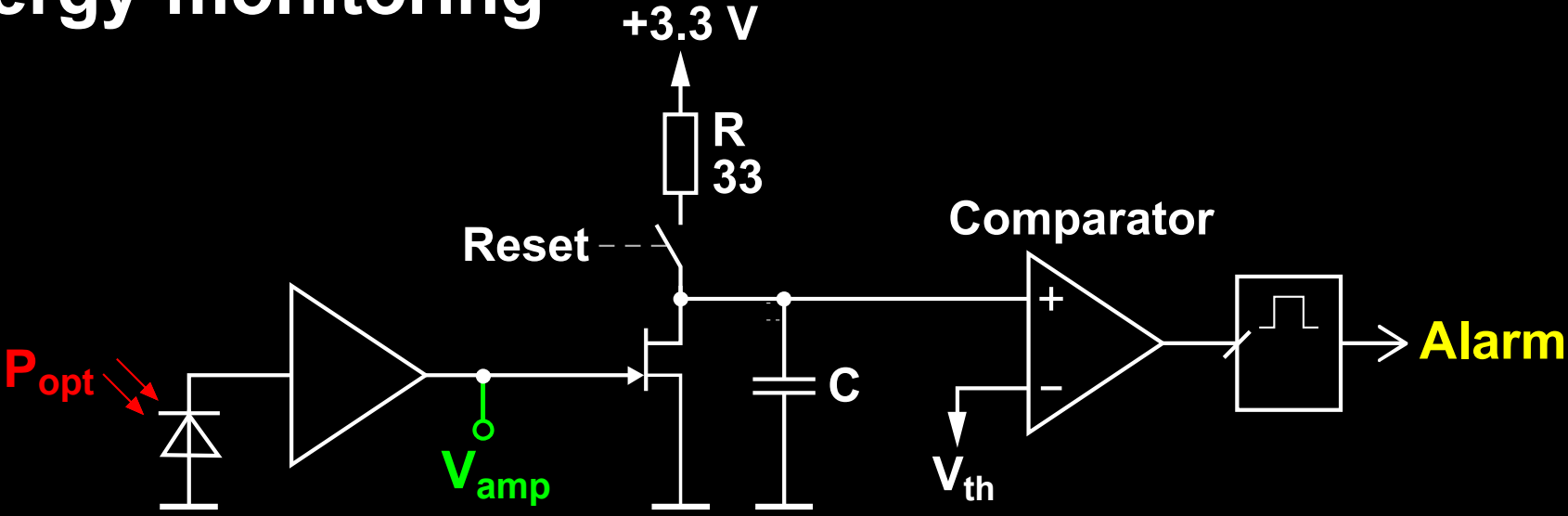
Trojan-horse attack on Bob



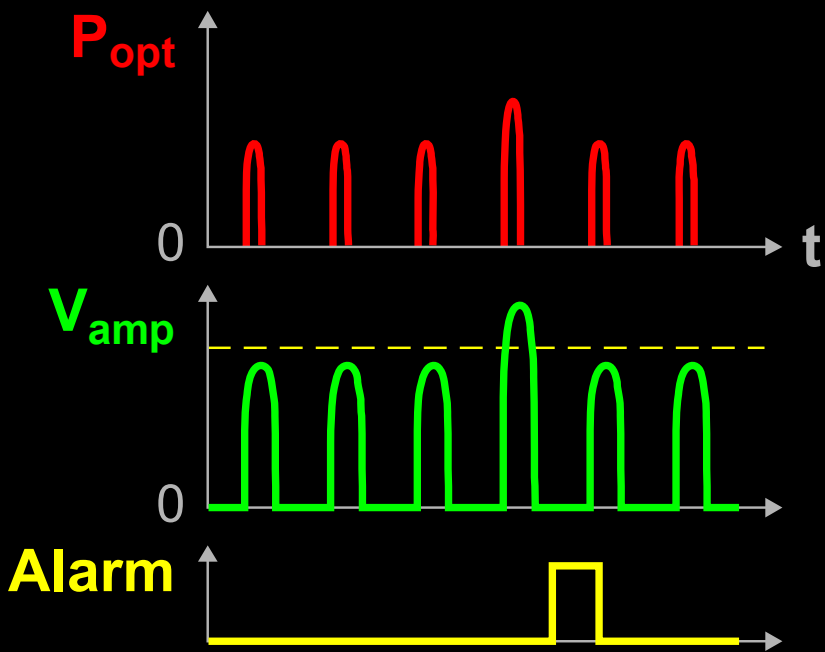
Countermeasures for plug-and-play system



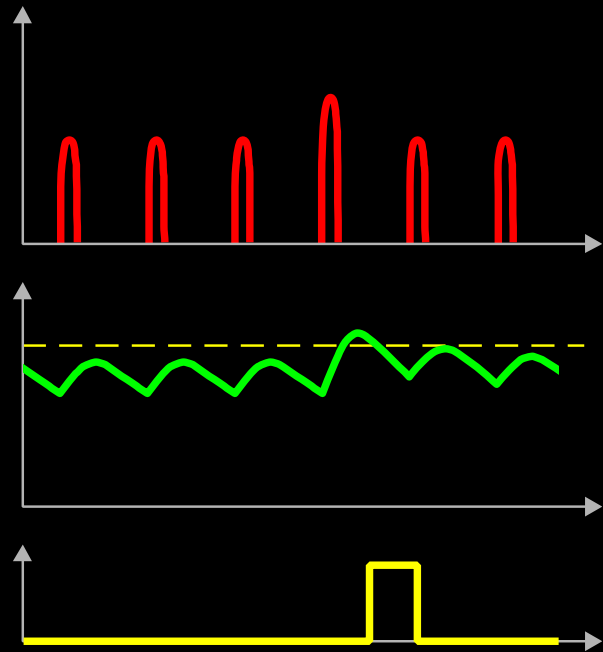
Pulse-energy-monitoring detector



Theory:



Implementation:



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

