Quantum hacking

Vadim Makarov

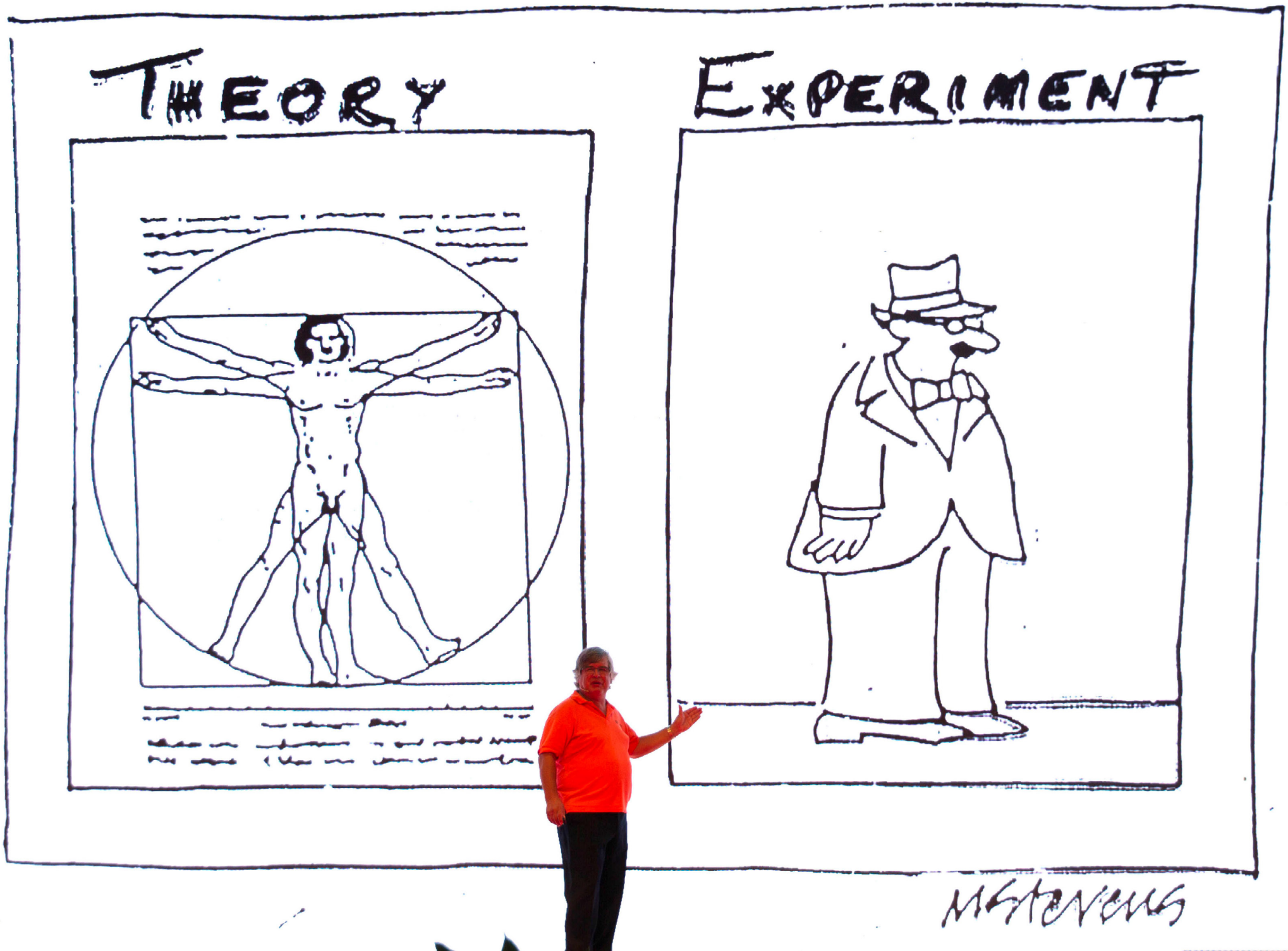
RQC MISIS

vad1.com/lab

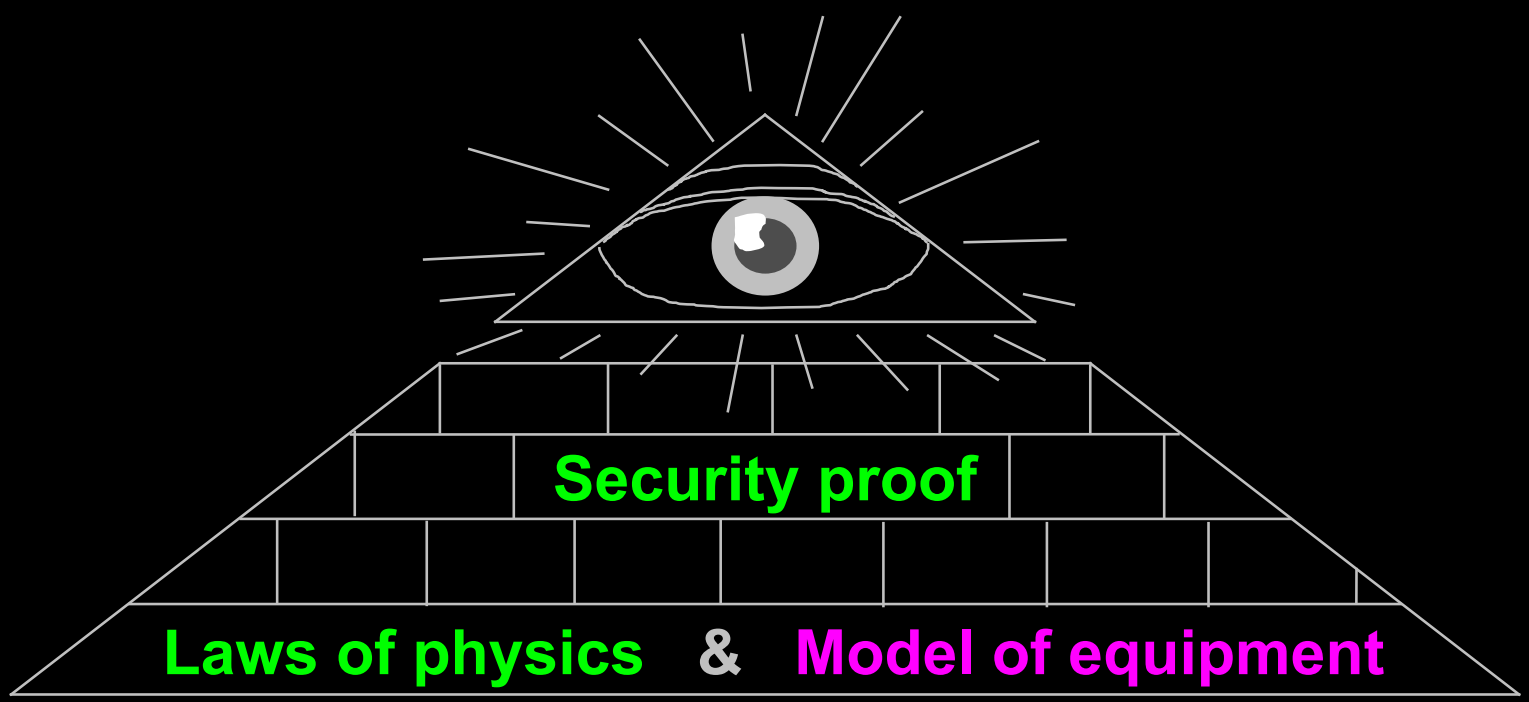
Photo ©2010 NTNU Info / Geir Mogen

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

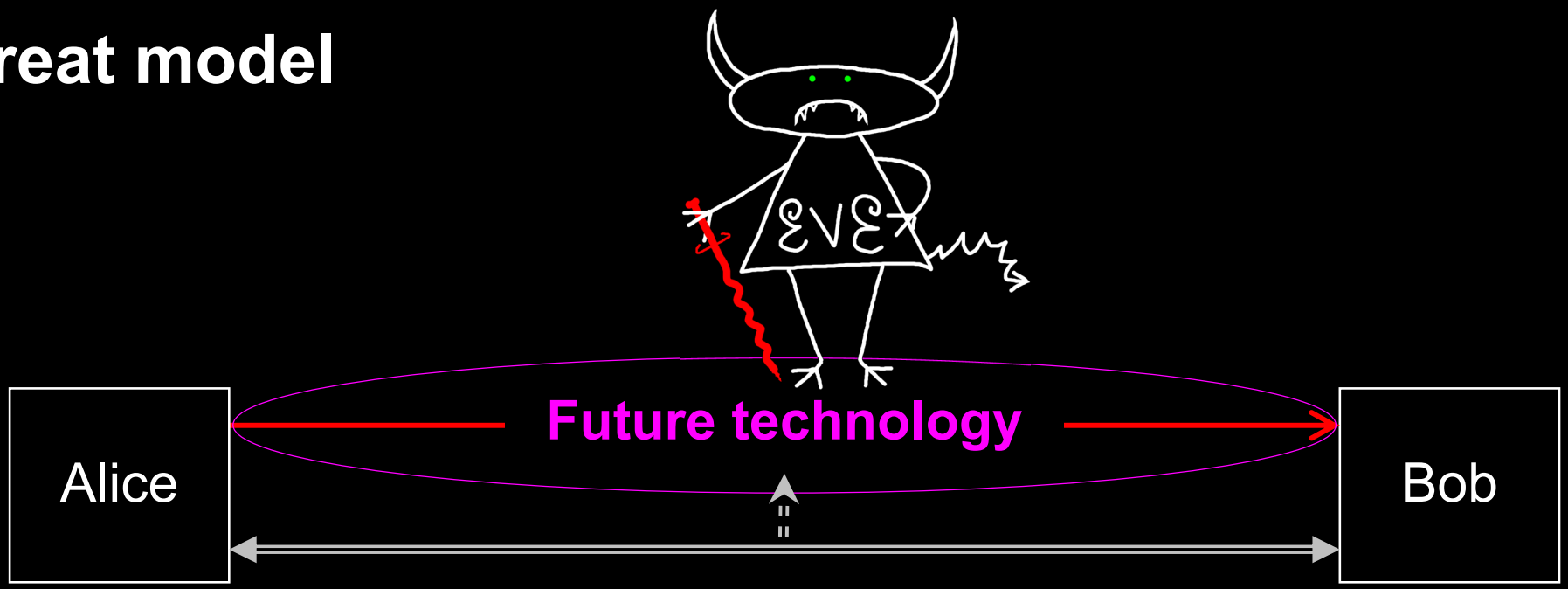


Hack

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
Induced photorefraction P. Ye *et al.,* Phys. Rev. Appl. **19**, 054052 (2023); F.-Y. Lu *et al.,* Optica **10**, 520 (2023); L. Han *et al.,* arXiv:2303.14683	modulators in Alice	7 components, research
Uncertainty of state preparation A. Huang *et al.,* Phys. Rev. Appl. **19**, 014048 (2023)	Alice	2 commercial systems
Laser seeding A. Huang *et al.,* Phys. Rev. Appl. **12**, 064043 (2019); X.-L. Pang et al., Phys. Rev. Appl. **13**, 034008 (2020)	laser in Alice	3 components
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.,* npj Quantum Inf. **4**, 8 (2018); F. Grünenfelder *et al.,* Appl. Phys. Lett. **117**, 144003 (2020)	modulators in Alice	2 research systems
Laser damage V. Makarov *et al.,* Phys. Rev. A **94**, 030302 (2016); A. Huang *et al.,* Phys. Rev. Appl. **13**, 034017 (2020).	any	5 commercial 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	single-photon detector	ID Quantique

Attack	Target component	Tested system
H. Weier *et al.,* New J. Phys. **13**, 073024 (2011)		
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
Phase-remapping F. Xu, B. Qi, H.-K. Lo, New J. Phys. **12**, 113026 (2010)	phase modulator in Alice	ID Quantique
Time-shift Y. Zhao *et al.,* Phys. Rev. A **78**, 042333 (2008)	single-photon detector	ID Quantique
Efficiency mismatch V. Makarov, A. Anisimov, J. Skaar, Phys. Rev. A **74**, 022313 (2006)	single-photon detector	2 components
Avalanche backflash C. Kurtsiefer *et al.,* J. Mod. Opt. **48**, 2039 (2001); A. Meda et al., Light Sci. Appl. 6, e16261 (2017); P. Pinheiro *et al.,* Opt. Express 26, 21020 (2018);	single-photon detector	3 components, research
Photon-number splitting C. Bennett *et al.,* J. Cryptology **5**, 3 (1992); G. Brassard *et al.,* Phys. Rev. Lett. **85**, 1330 (2000)	laser in Alice	(theory)

Example of vulnerability and countermeasures

Photon-number-splitting attack

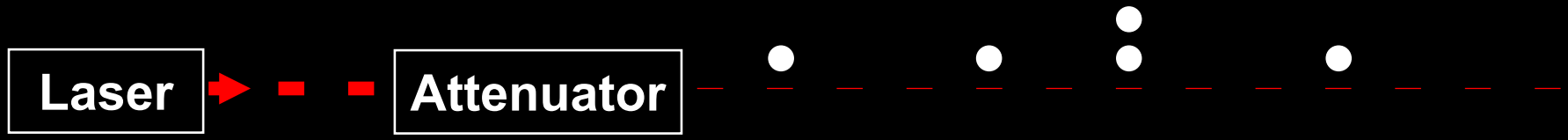
C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992)

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)

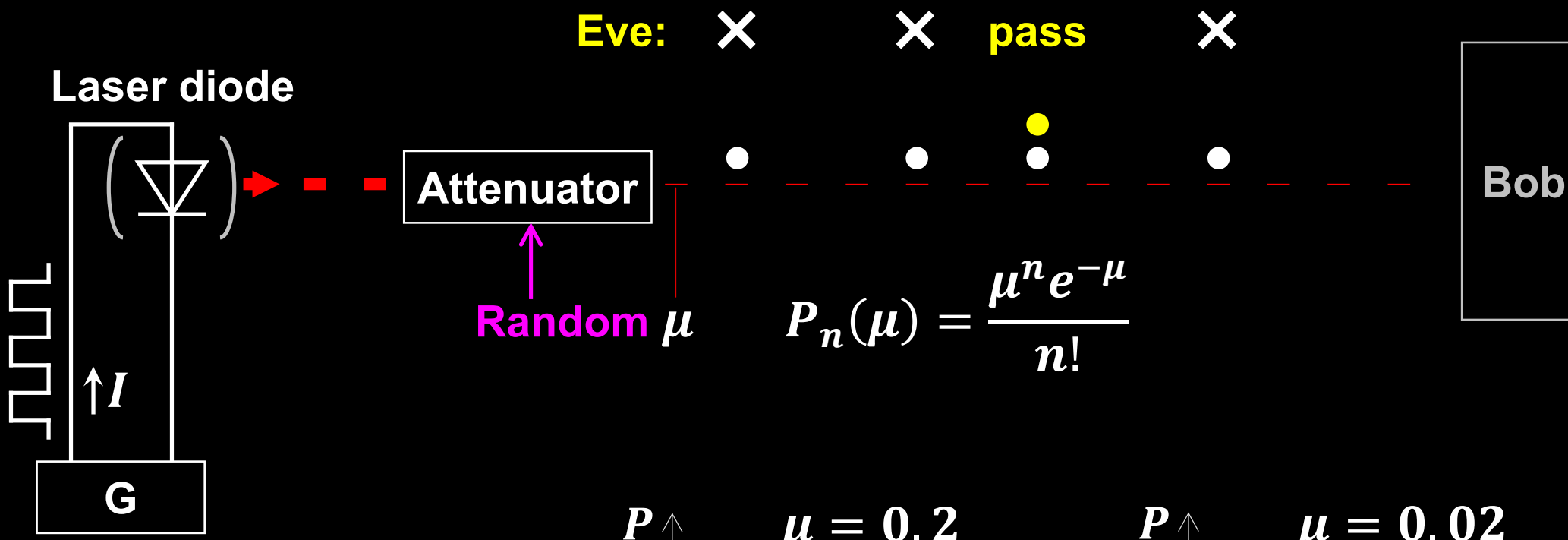
★ Distributed-phase-reference protocols

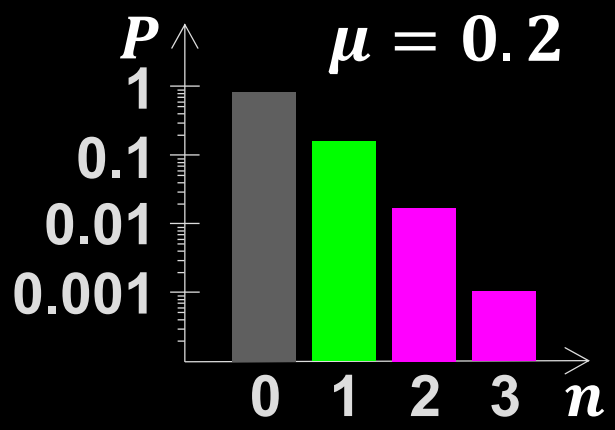
K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002)

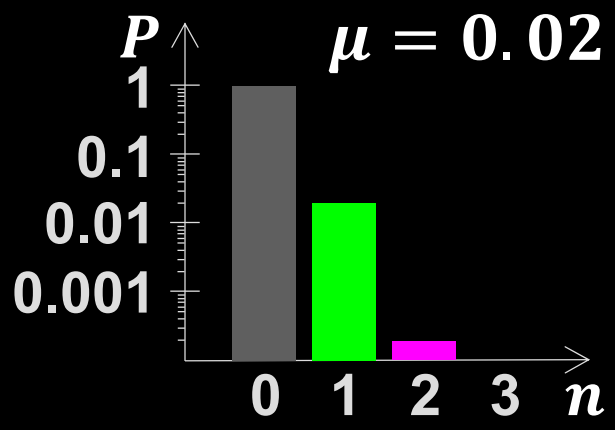
K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. A. **68**, 022317 (2003)

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

Decoy-state protocol







Eve: blocks less

blocks more

S. J. van Enk, C. A. Fuchs, arXiv:quant-ph/0111157; W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003)

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)

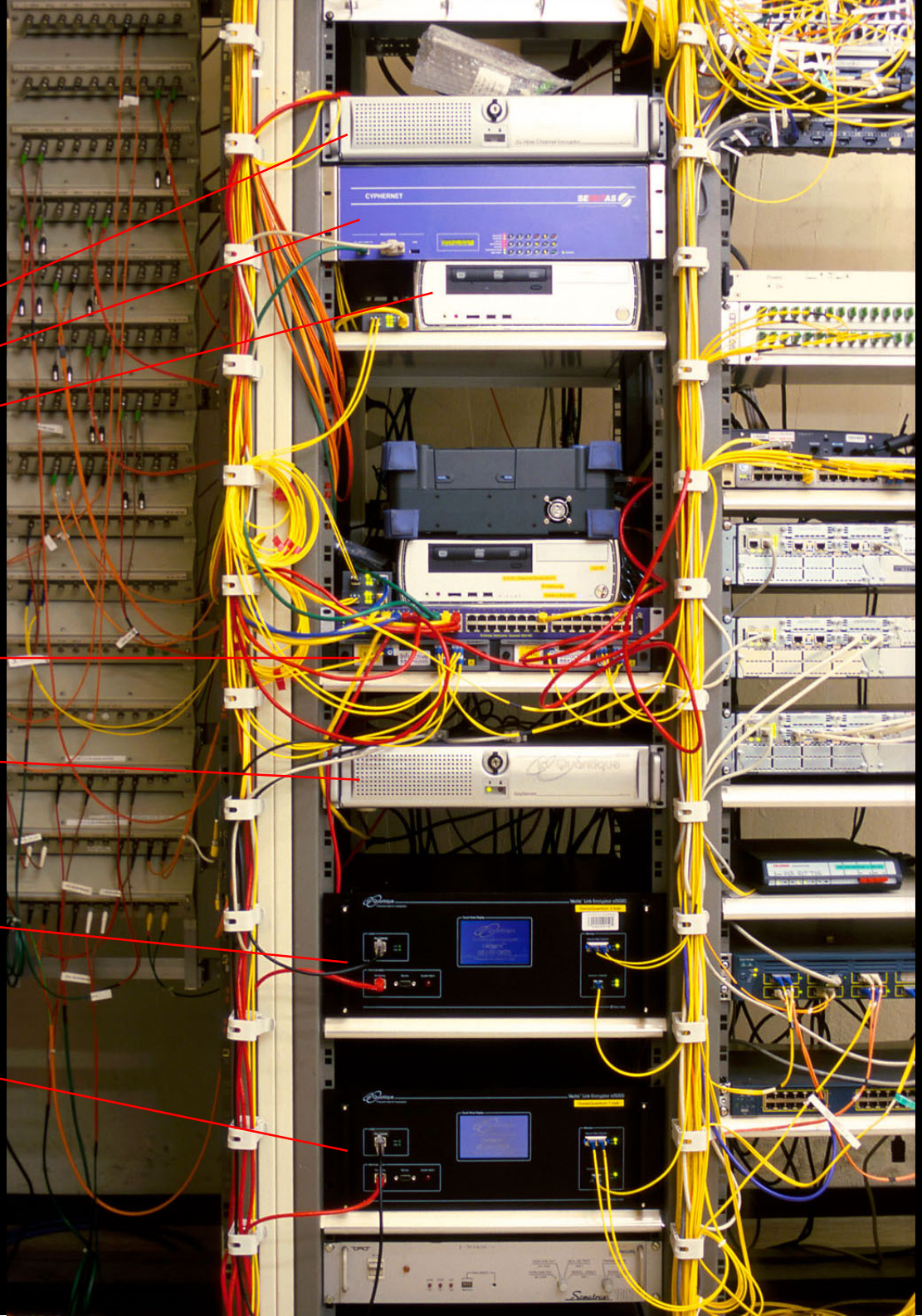
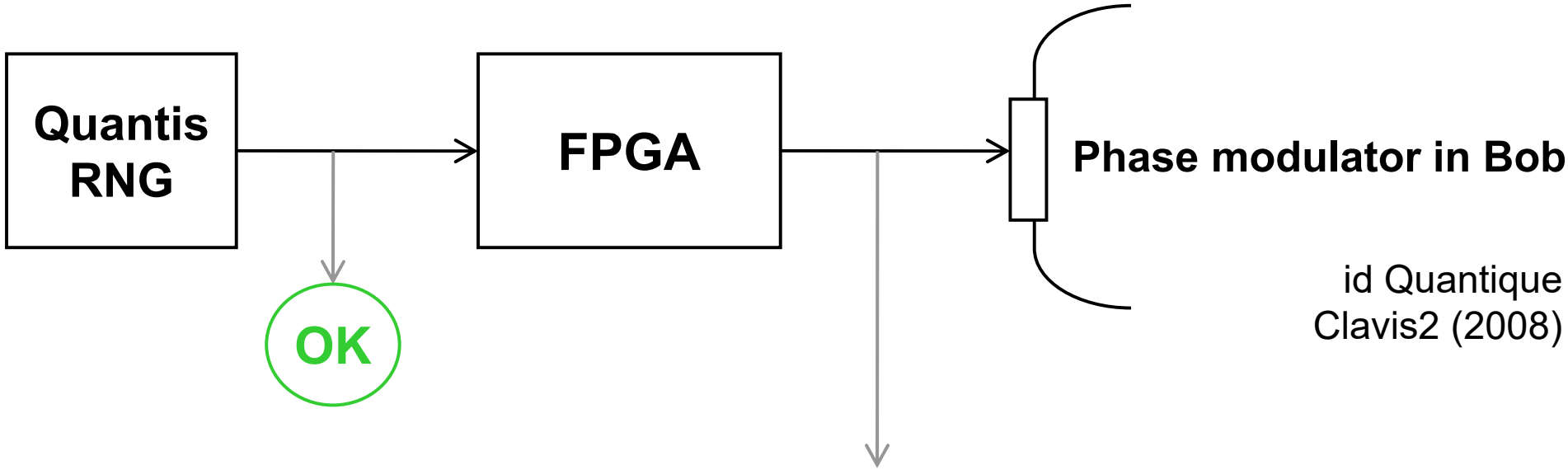
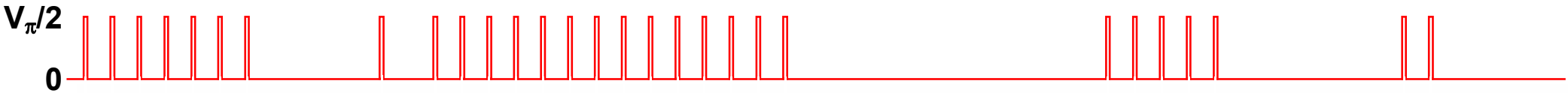


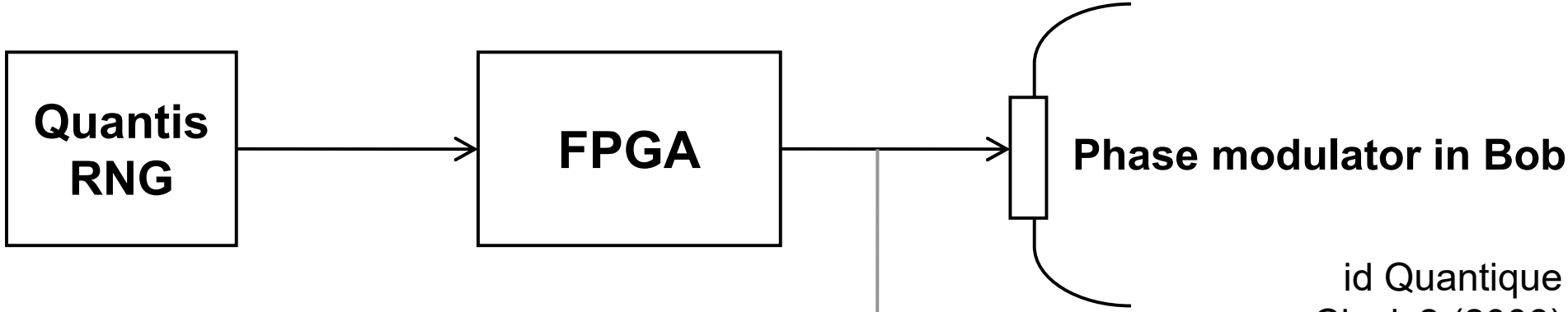
Photo ©2010 Vadim Makarov

True randomness?

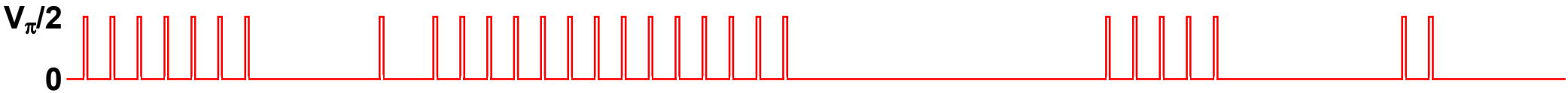




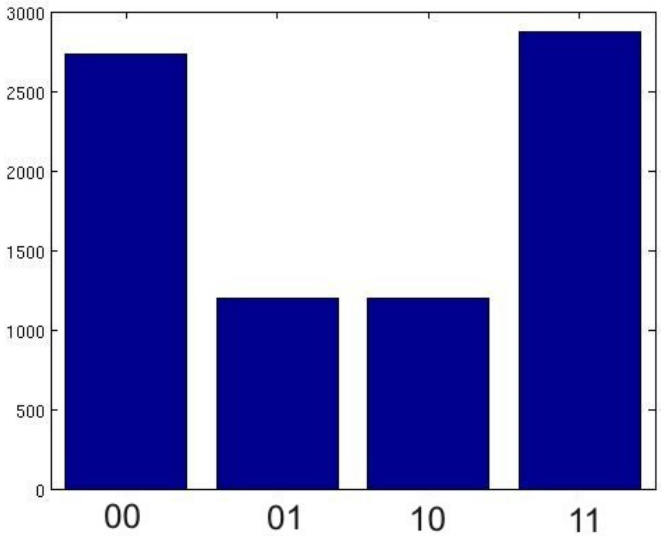
True randomness?



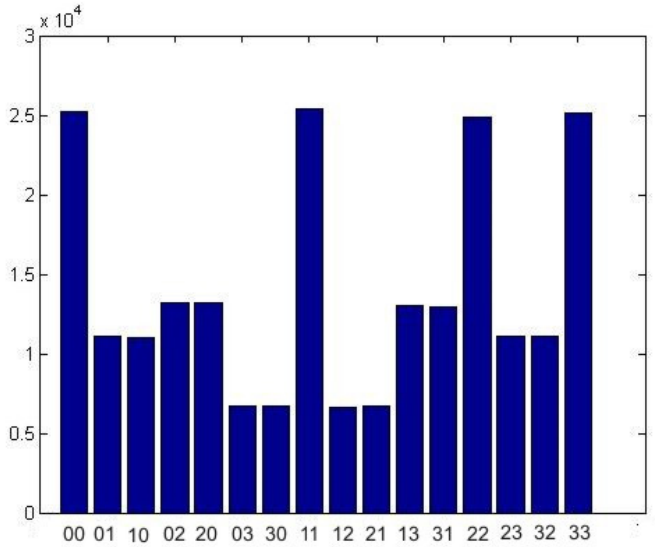
id Quantique
Clavis2 (2008)



Bob:



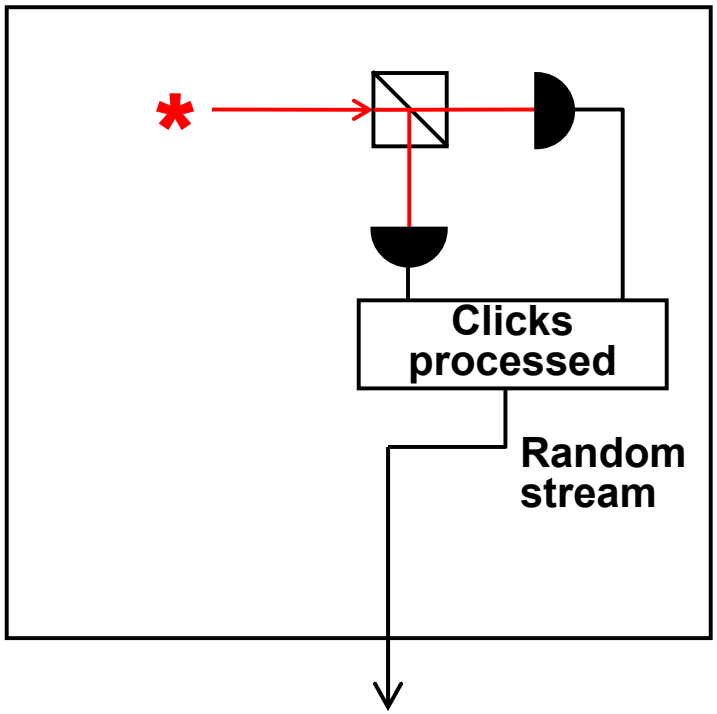
Alice:



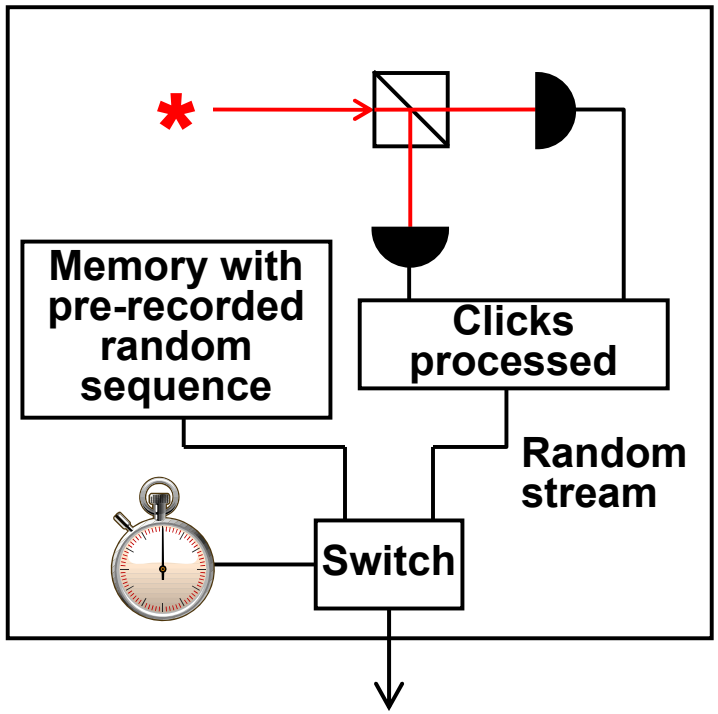
Issue reported patched in 2010

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

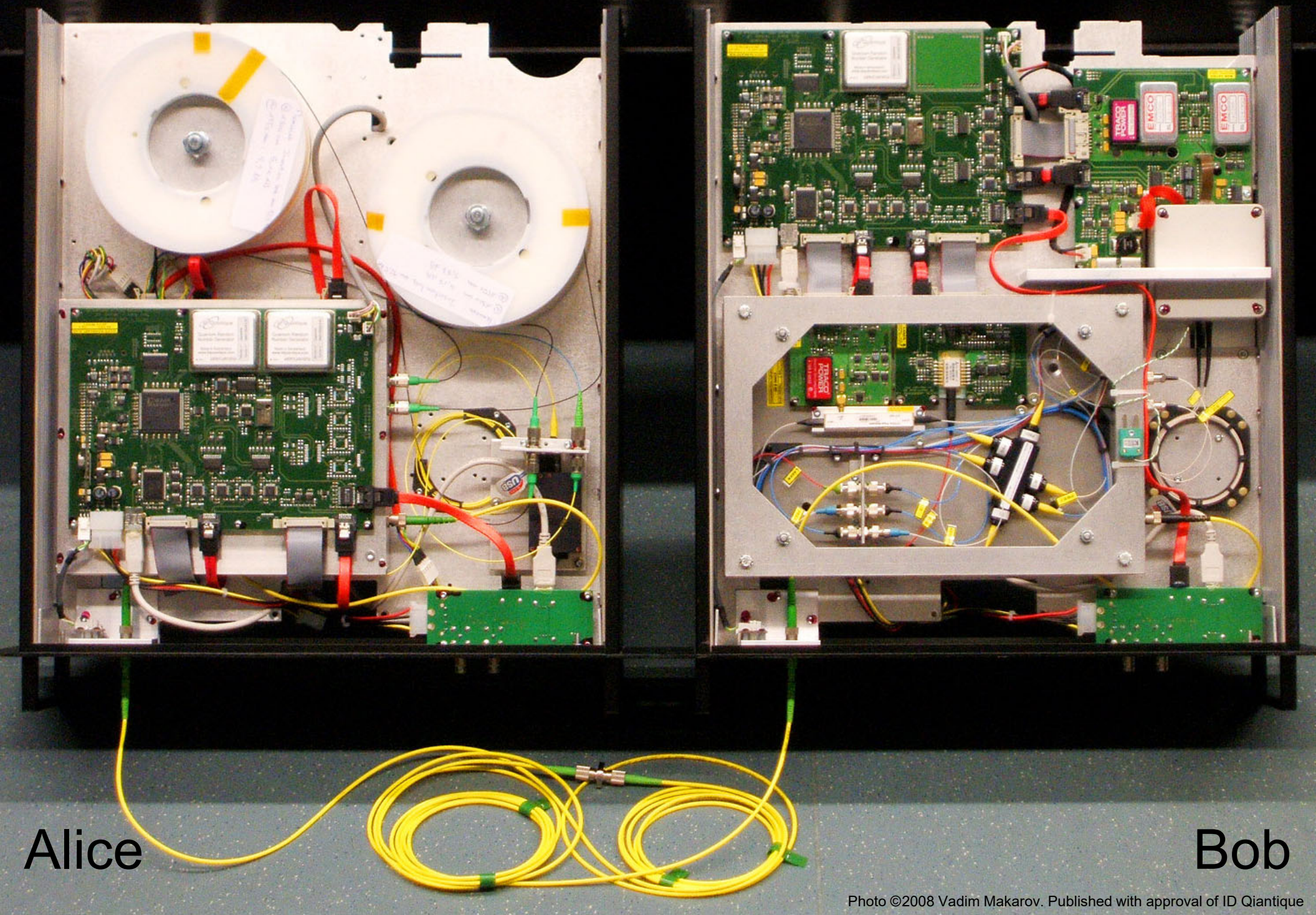


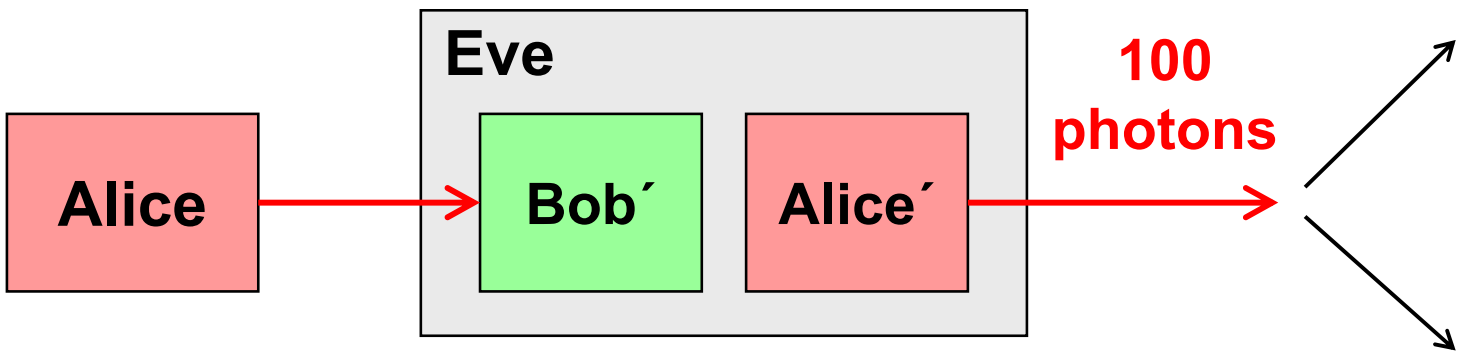
Photo ©2008 Vadim Makarov. Published with approval of ID Qiantique

Double clicks

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

Discard them?

Intercept-resend attack... with a twist:



Bob:

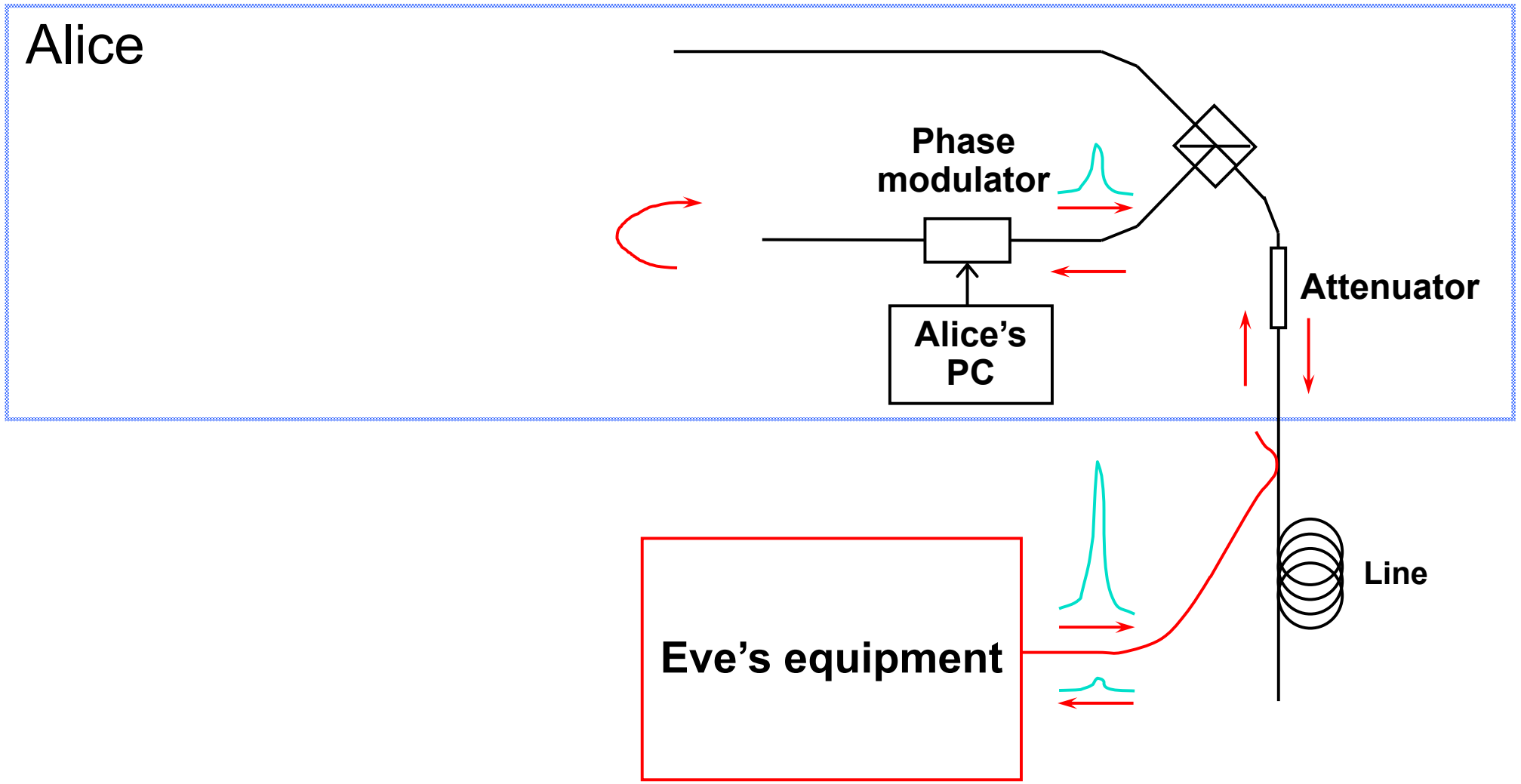
Detects in Eve's basis: single click

Detects in conjugate basis: double click, discarded

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

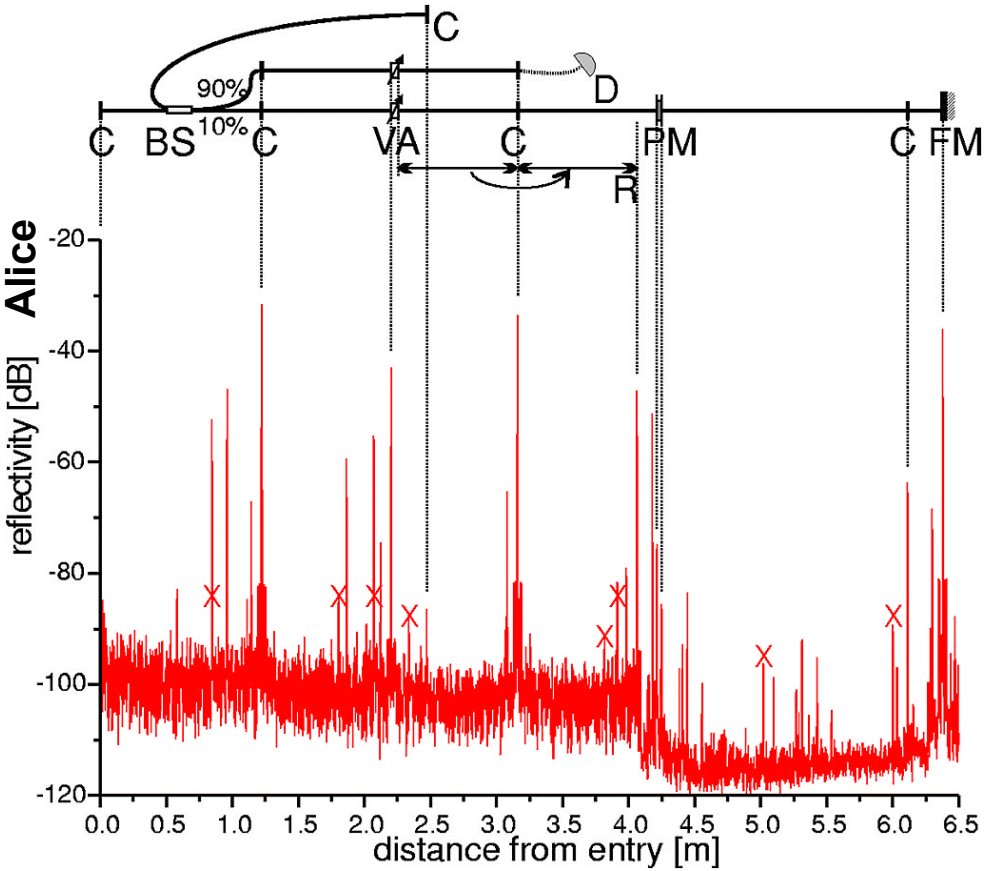
N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999)
T. Tsurumaru & K. Tamaki, Phys. Rev. A **78**, 032302 (2008)

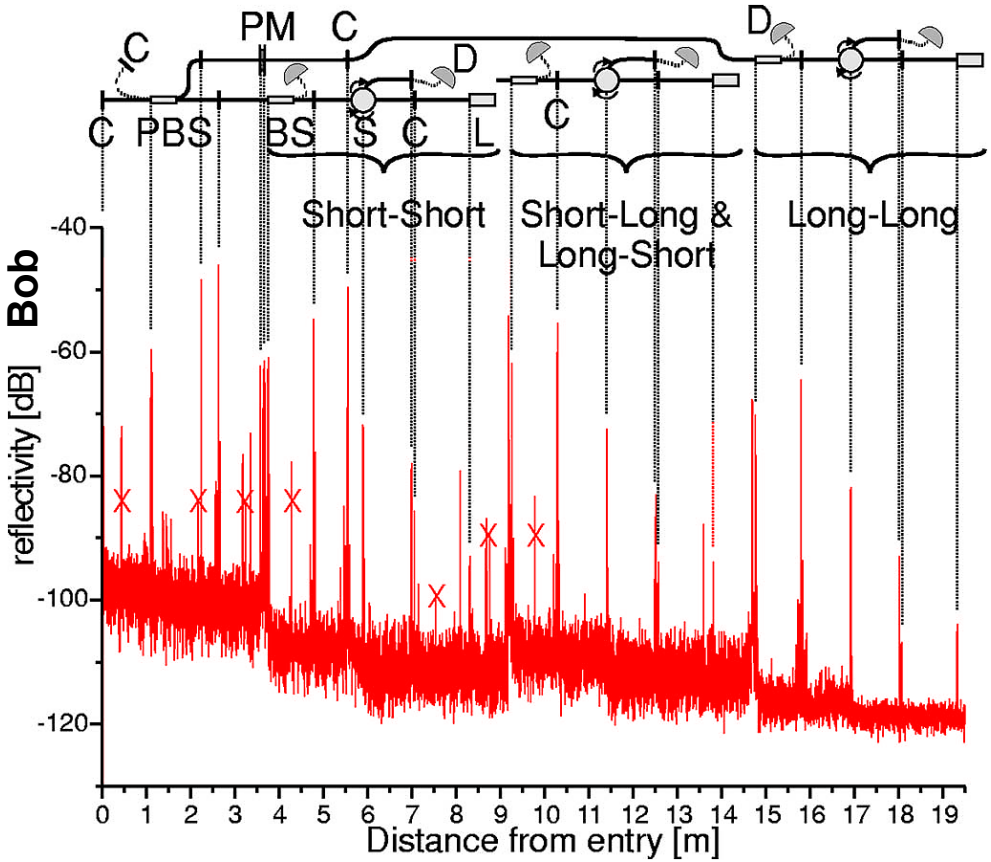
Trojan-horse attack



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

Trojan-horse attack for plug-and-play system

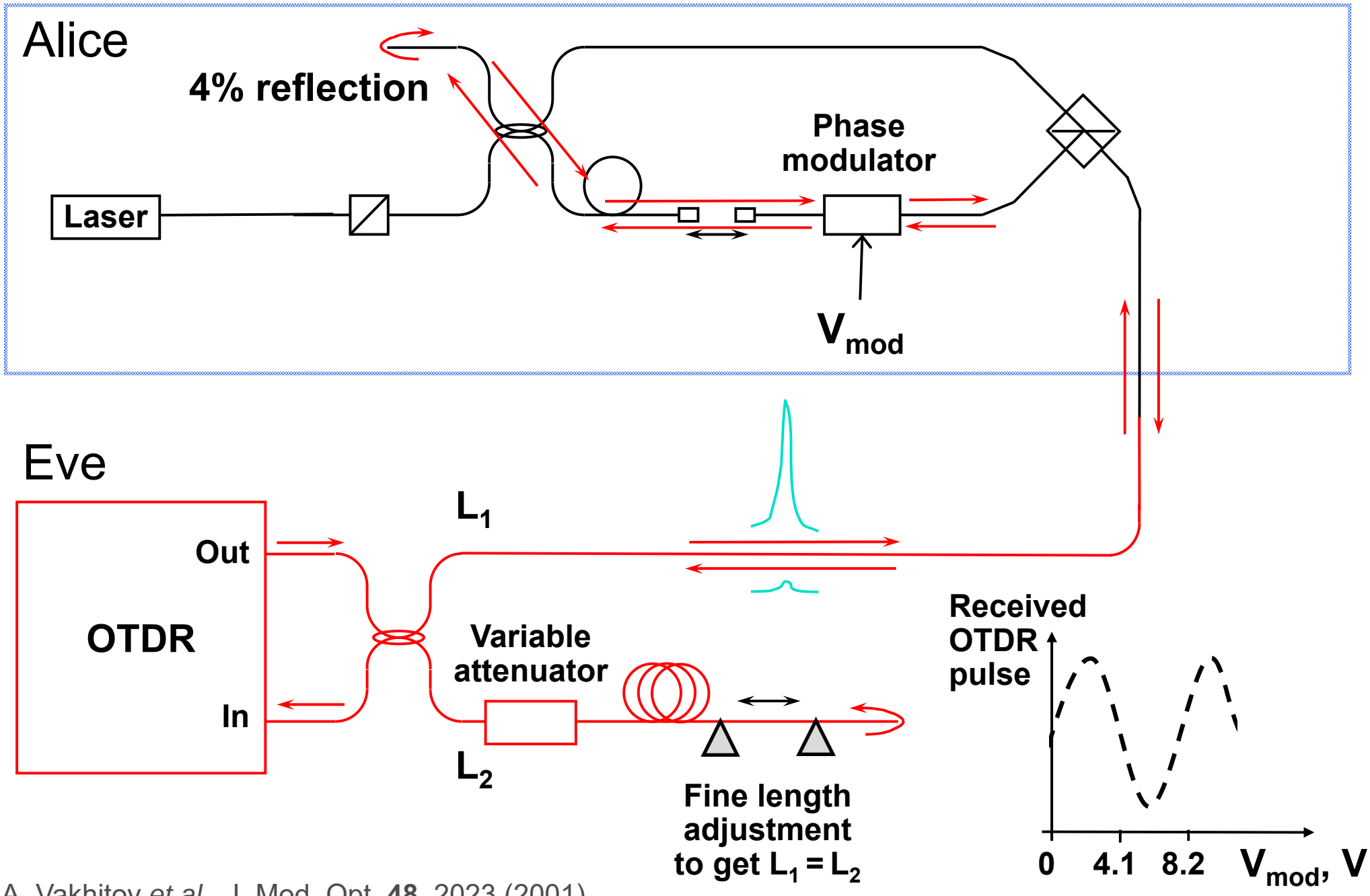




Eve gets back one photon → in principle, extracts 100% information

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

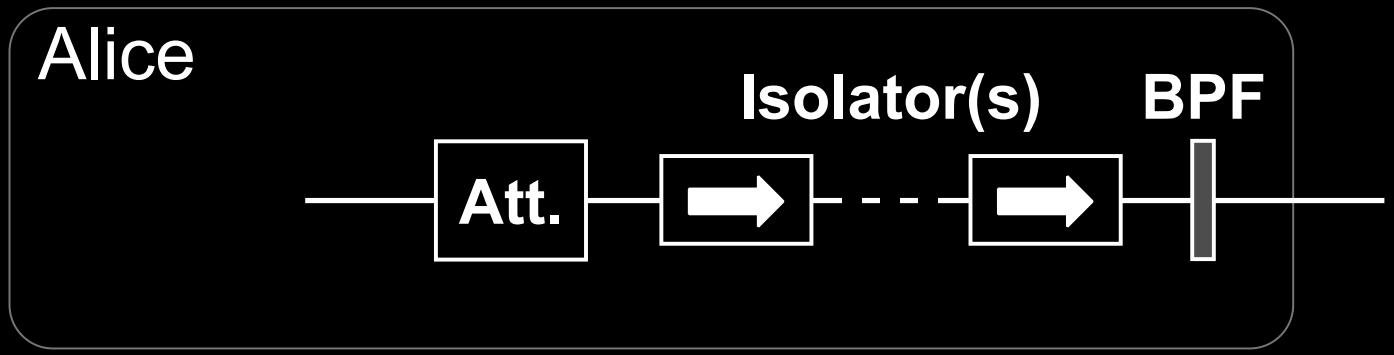
Trojan-horse attack experiment



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

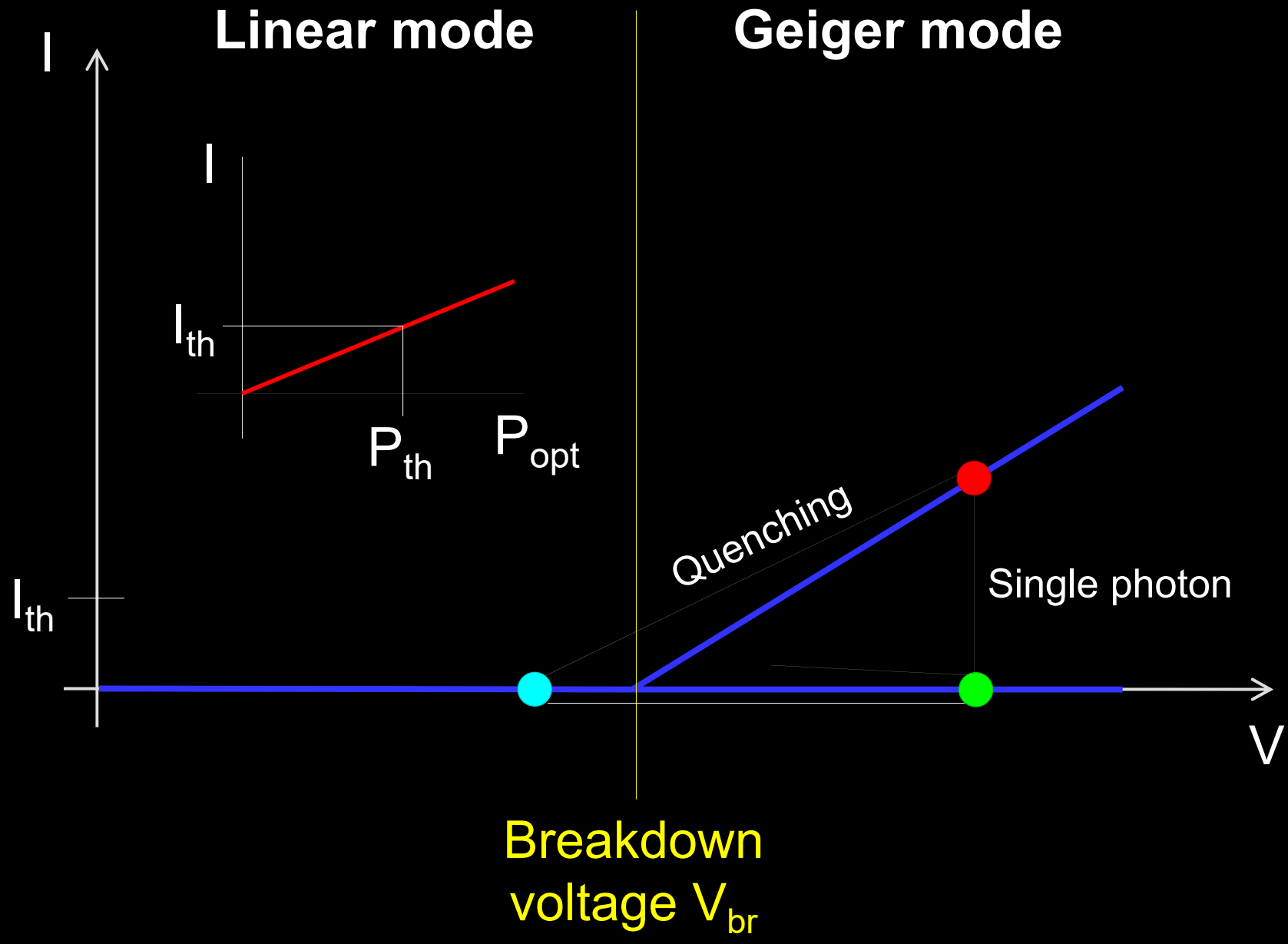
Countermeasures to Trojan-horse attack?

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

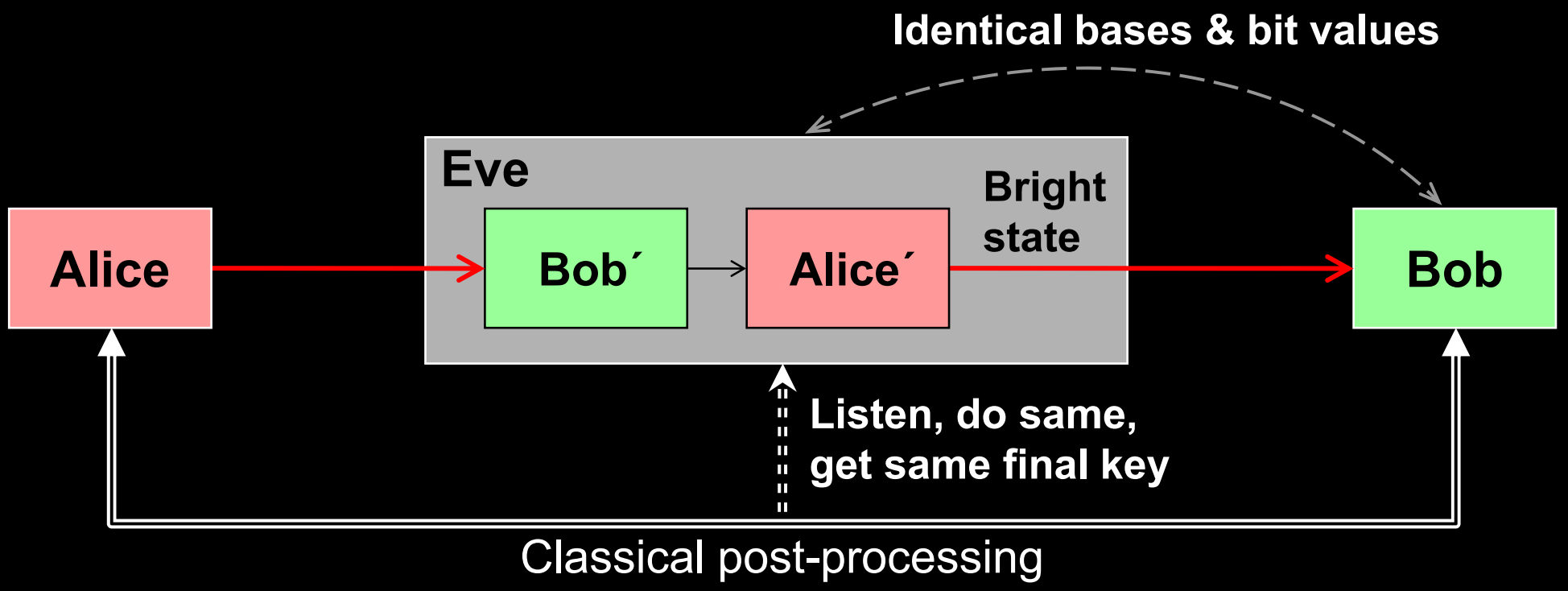


M. Lucamarini *et al.*, Phys. Rev. X **5**, 031030 (2015)

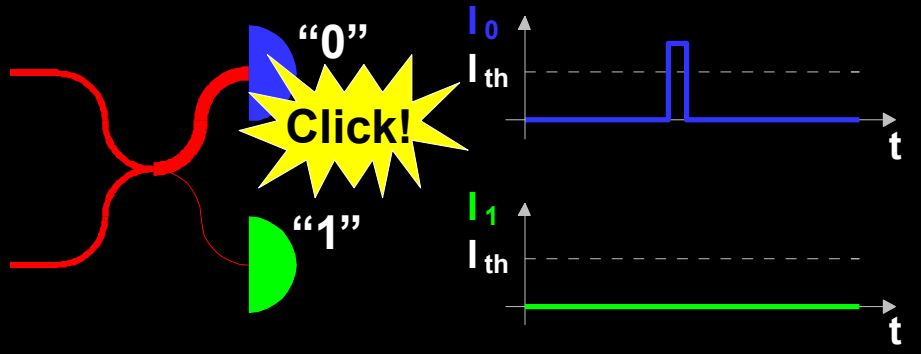
Attack example: avalanche photodetectors (APDs)



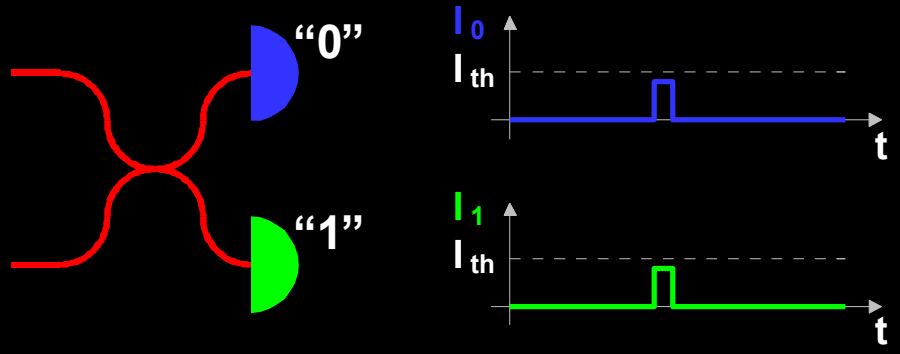
Faked-state attack in APD linear mode



Bob chooses same basis as Eve:

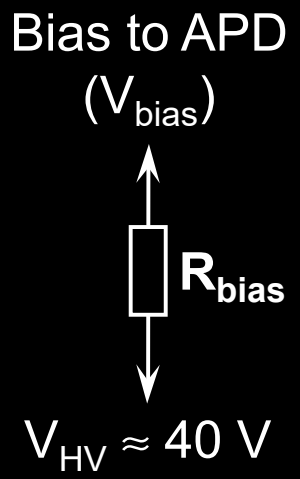


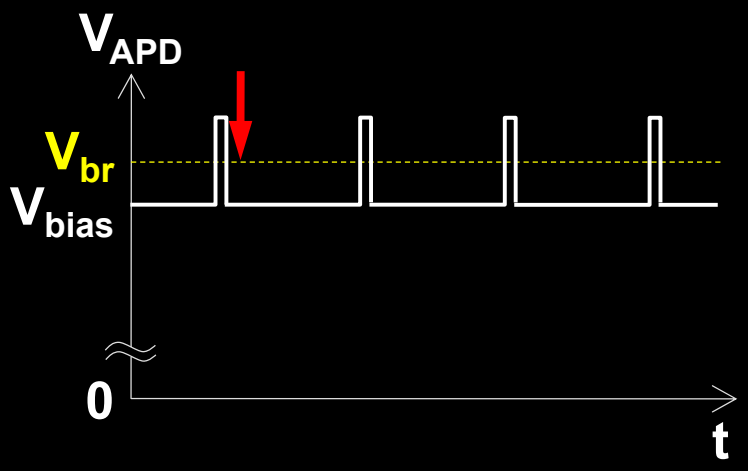
Bob chooses different basis:



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

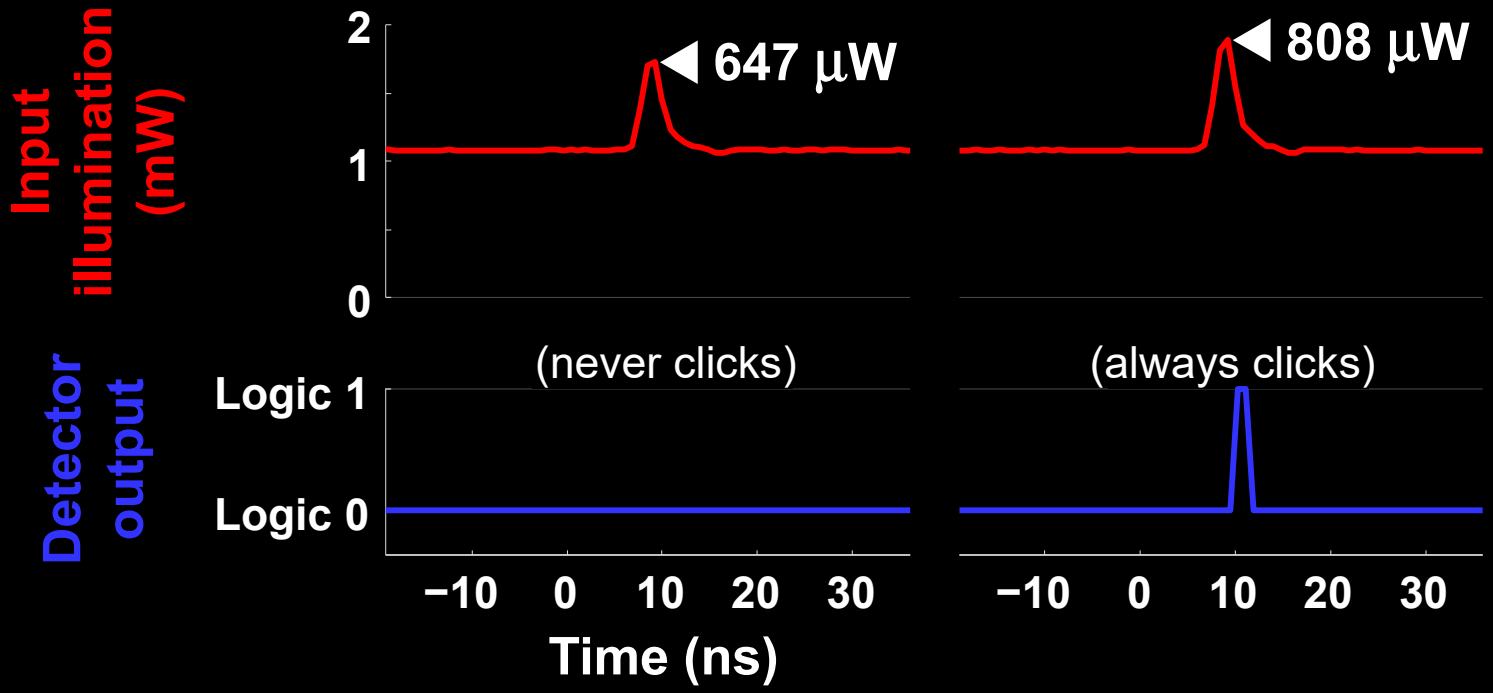
Blinding APD with bright light





Eve applies CW light

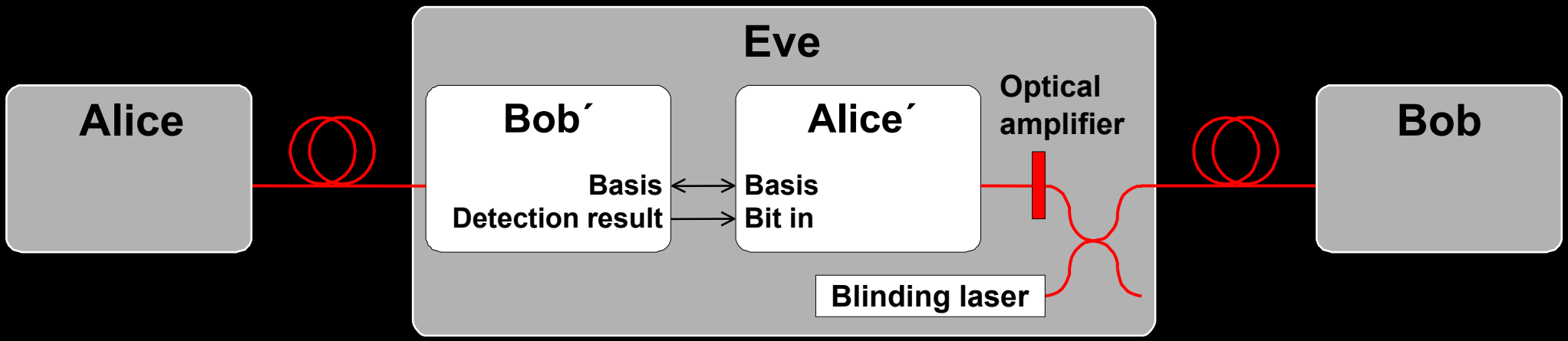
Detector blind!
Zero dark count rate



ID Quantique
Clavis2

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

Proposed full eavesdropper

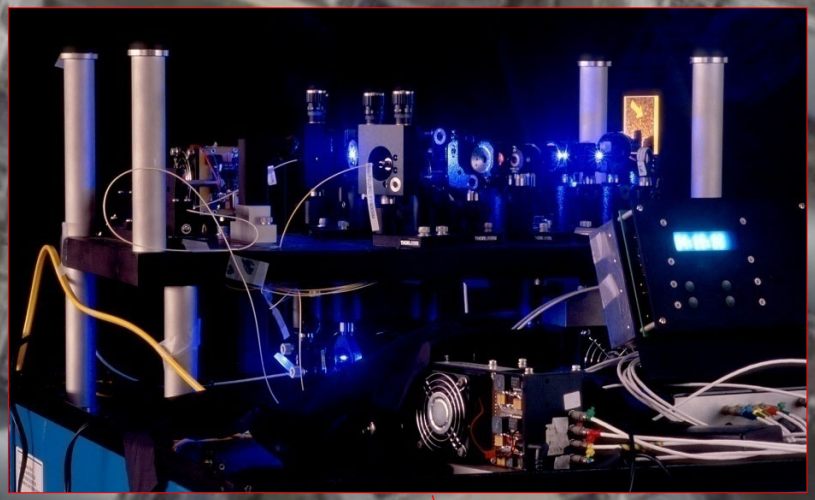


Note: Intercept-resend always breaks QKD security

M. Curty, M. Lewenstein, N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004)

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

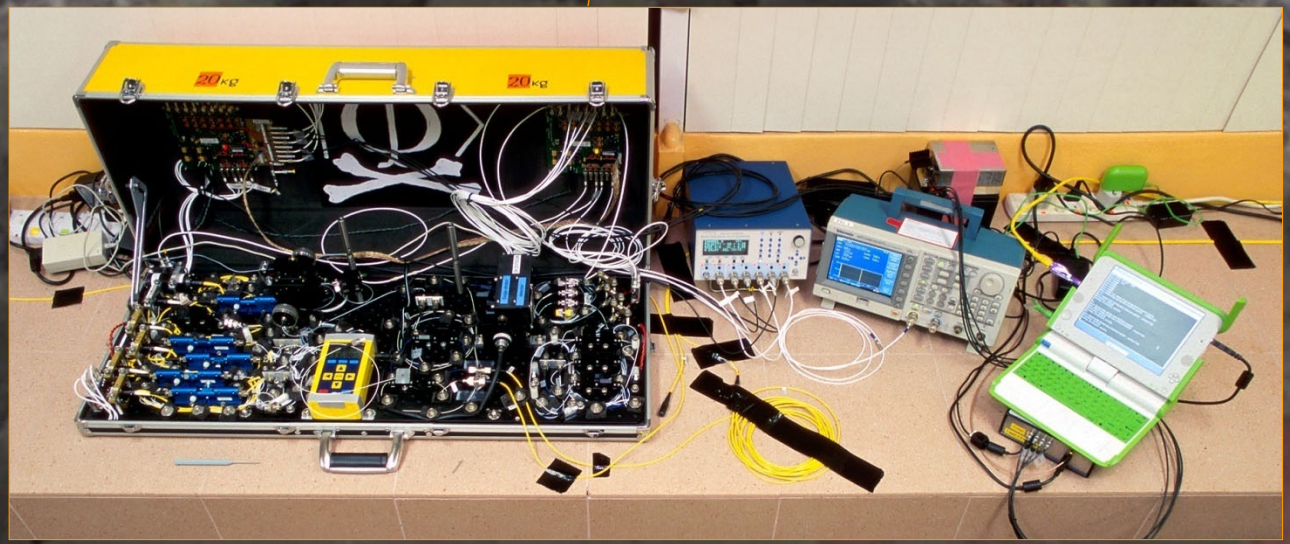
Bob

S15

S14

S13

S12

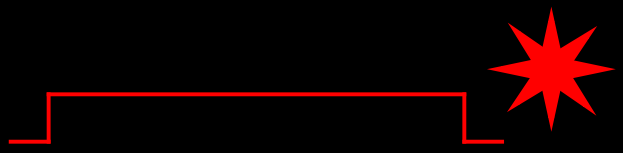


I. Gerhardt, Q. Liu *et al.*,
Nat. Commun. **2**, 349 (2011)

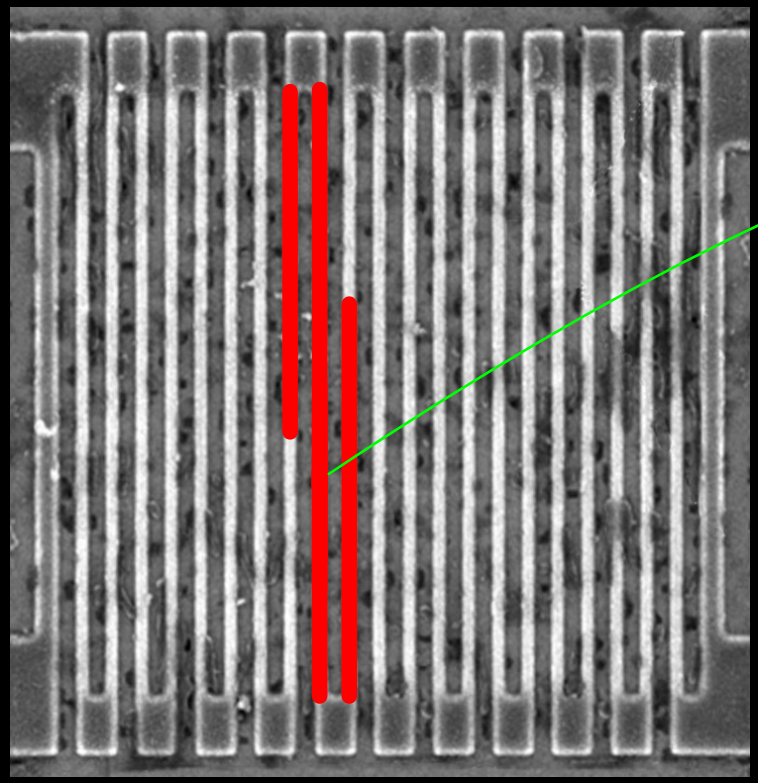
Image ©2009 DigitalGlobe

Controlling superconducting nanowire single-photon detectors

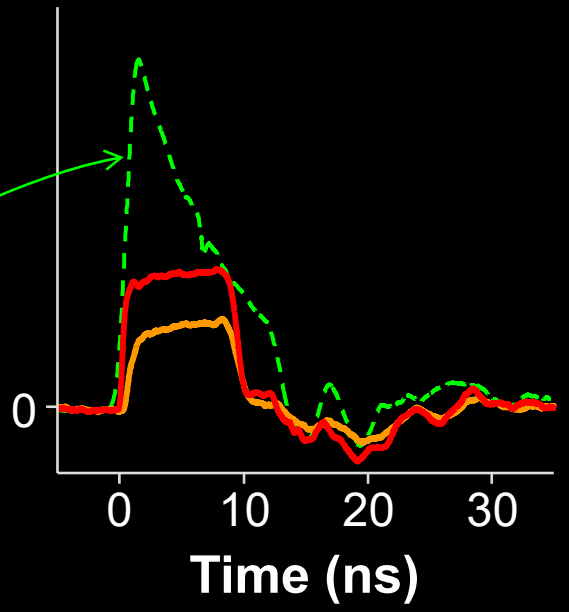
1. Blind (latch)



2. Control



Comparator input voltage (arb. units)



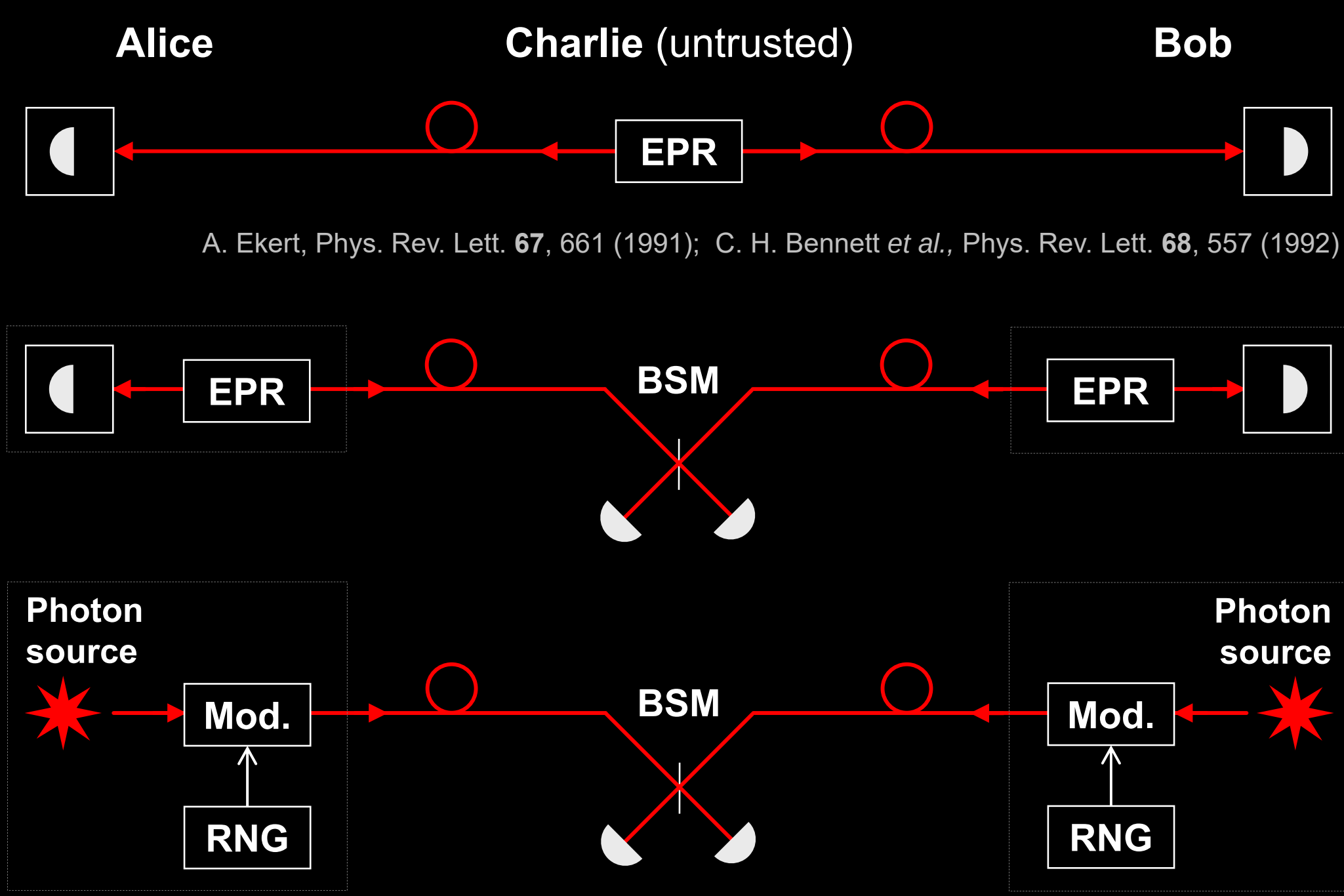
Normal single-photon click

14 mW pulse

7 mW pulse

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, Opt. Express **22**, 6734 (2014)

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)