Lecture at ID Quantique 4th winter school on practical quantum cryptography, Les Diablerets, January 22–26, 2012

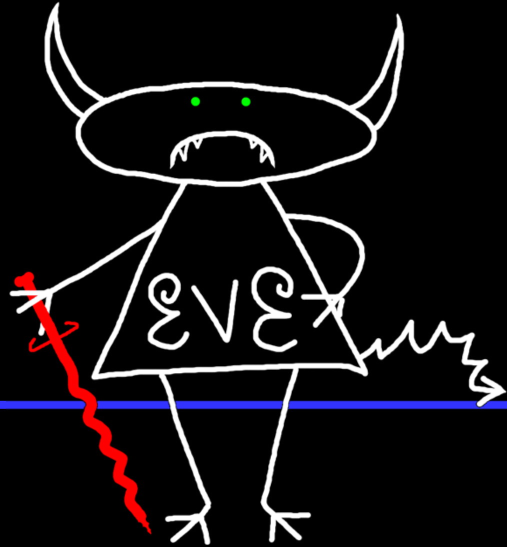
Loopholes in implementations

Vadim Makarov

NTNU
Det skapende universitet

Photo ©2010 NTNU Info / Geir Mogen

Security model of QKD



Alice **Bob**

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

With equipment imperfections:

$$R = f(\text{QBER, additional security parameters})$$

Security is based on the laws of physics and model of equipment

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

Tasks of a quantum hacker

- Discover vulnerabilities
- Demonstrate attacks

- Countermeasures
- Security proofs

Commercial QKD

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)

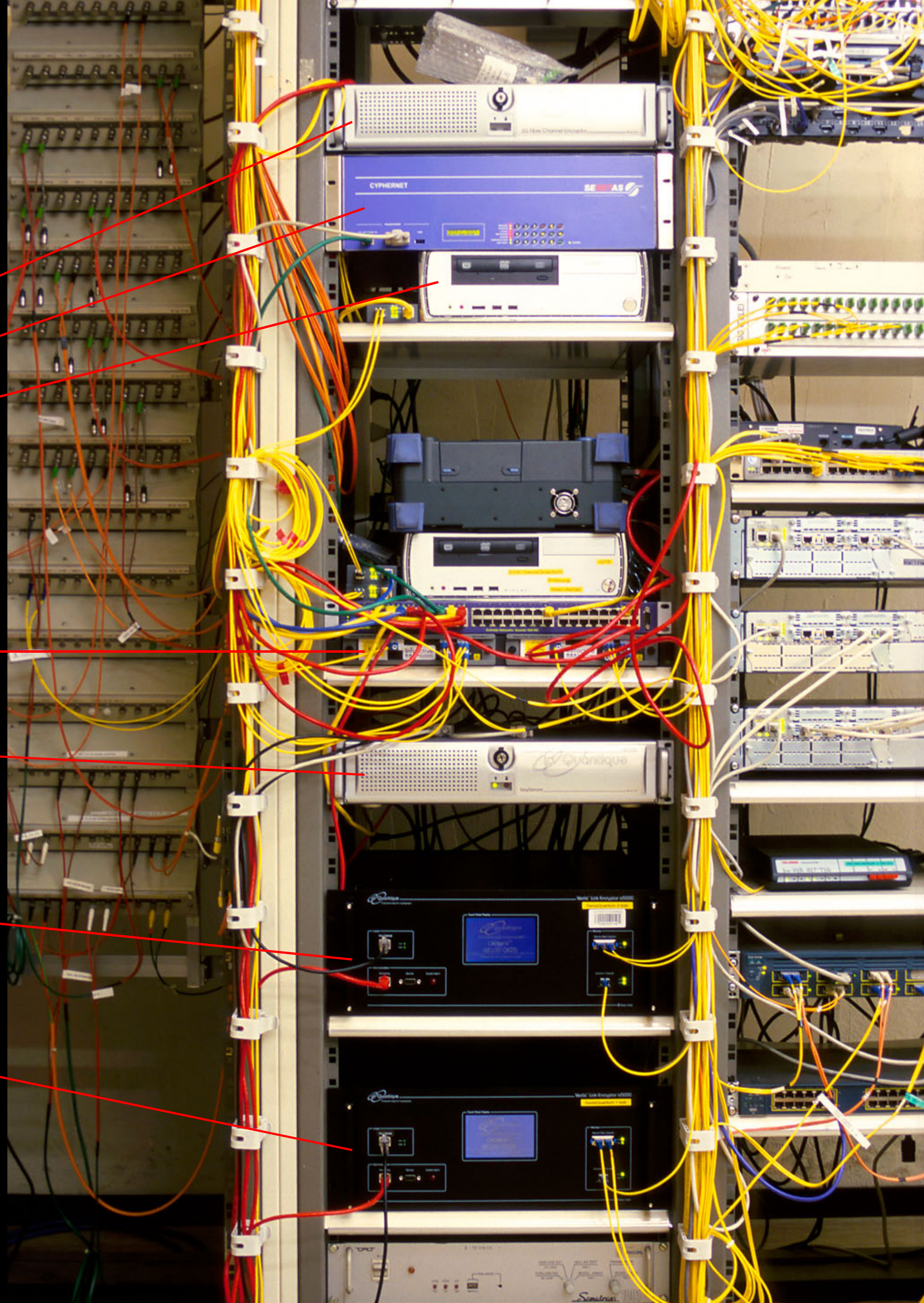
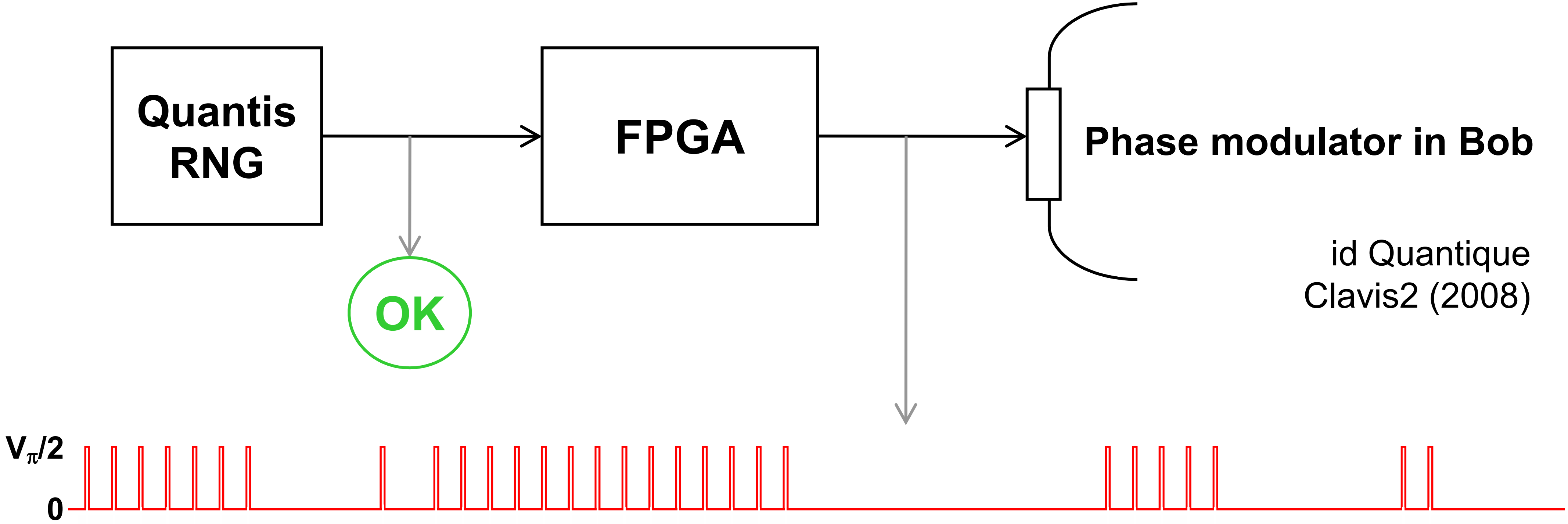
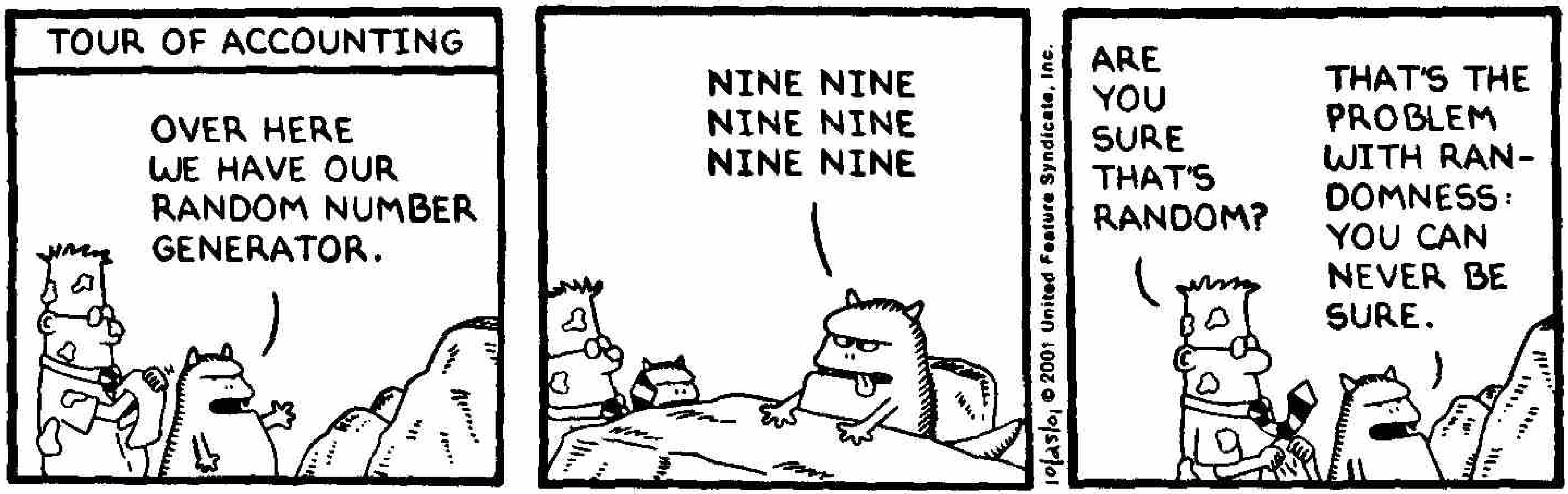


Photo ©2010 Vadim Makarov

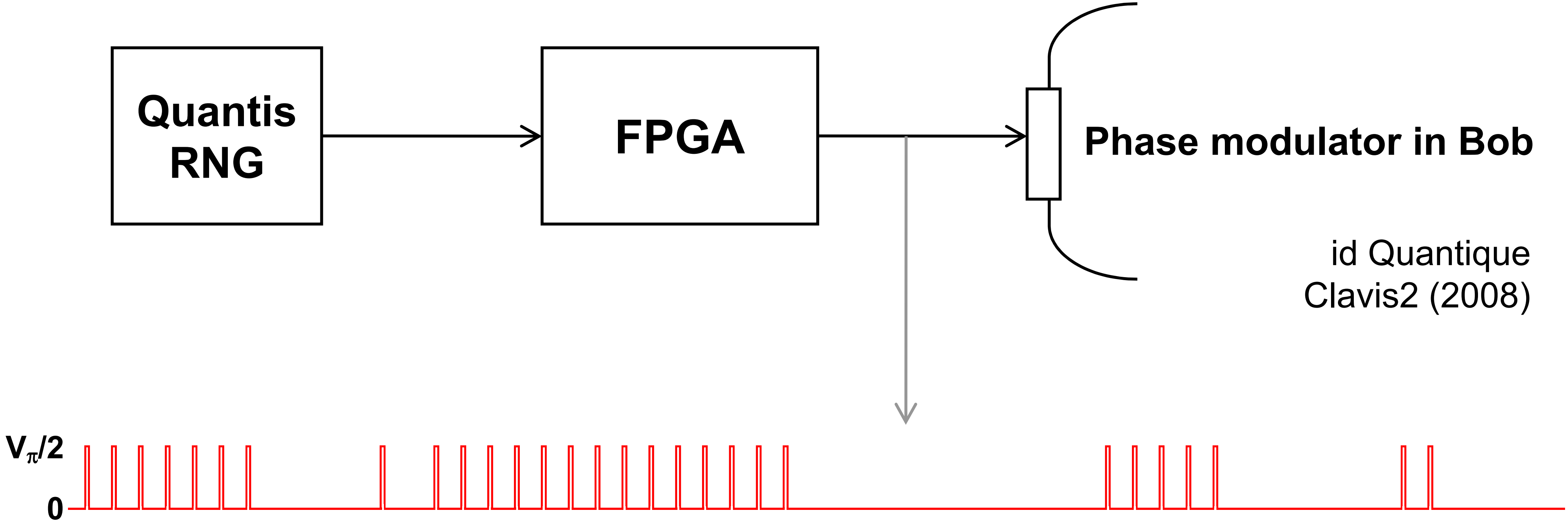
www.swissquantum.com

True randomness?

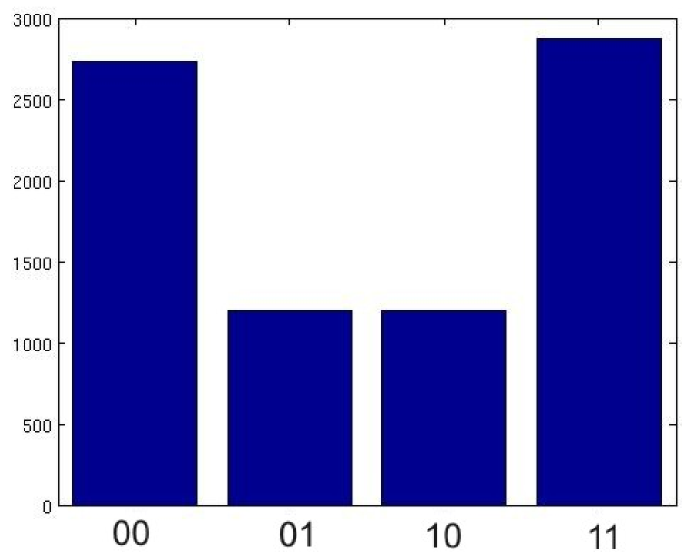




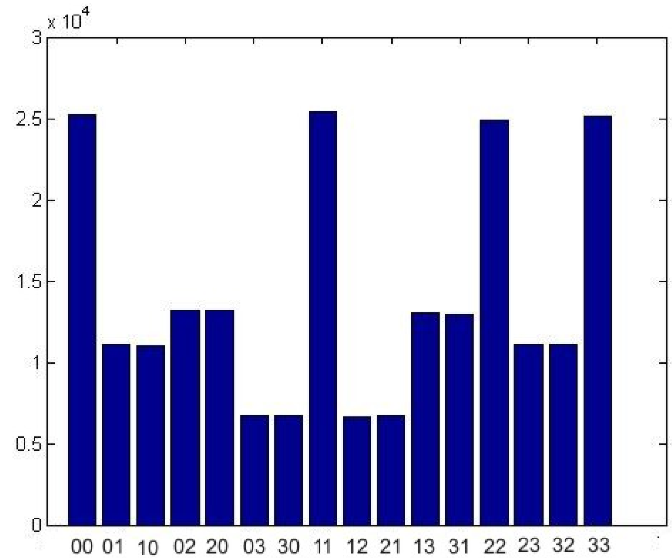
True randomness?



Bob:

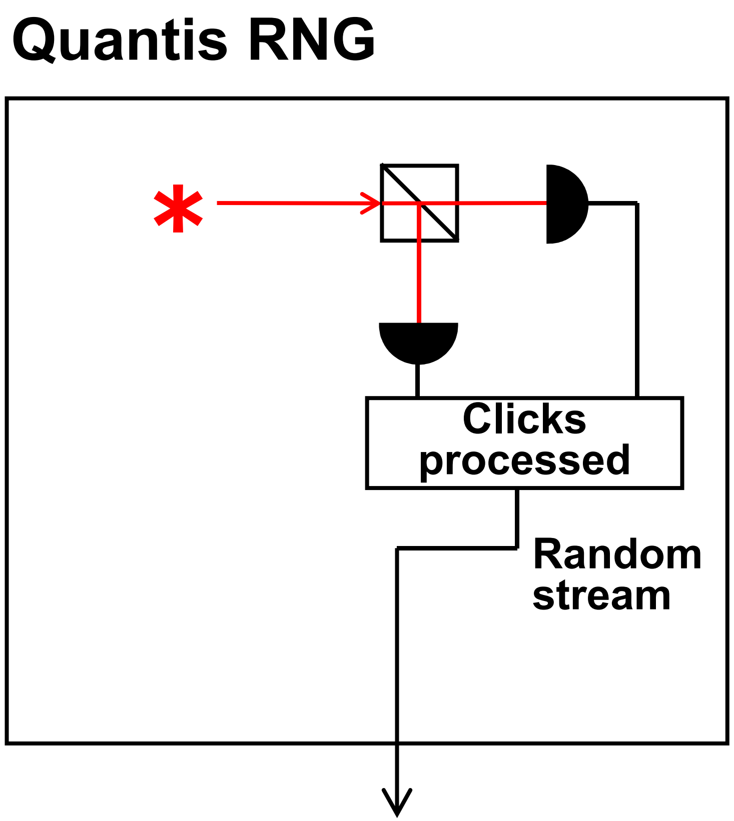


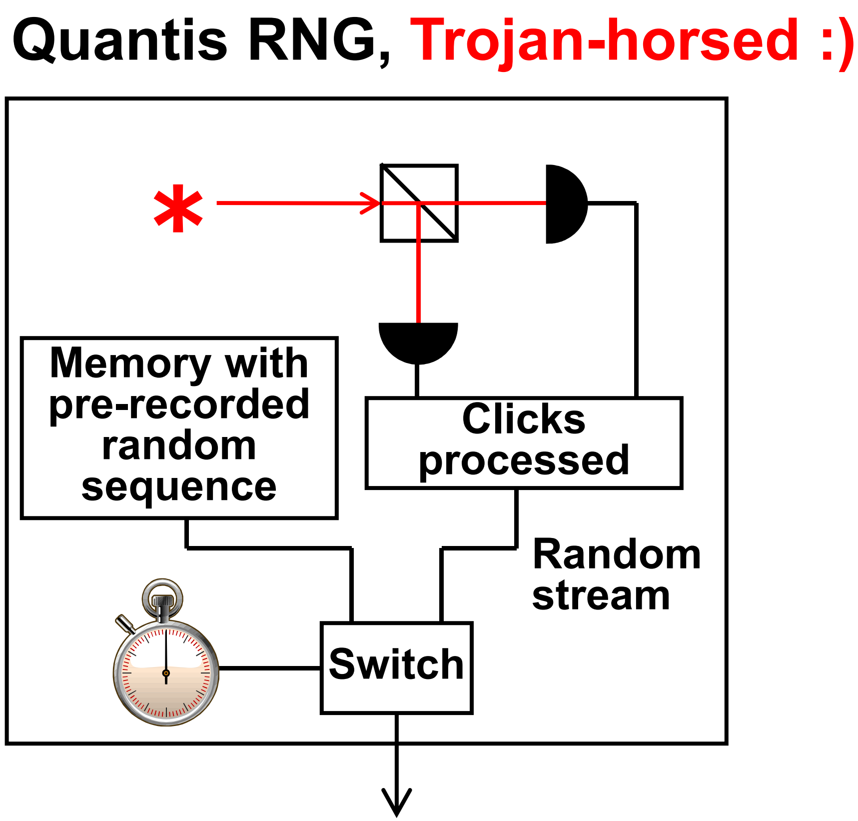
Alice:



Issue reported patched, as of January 2010

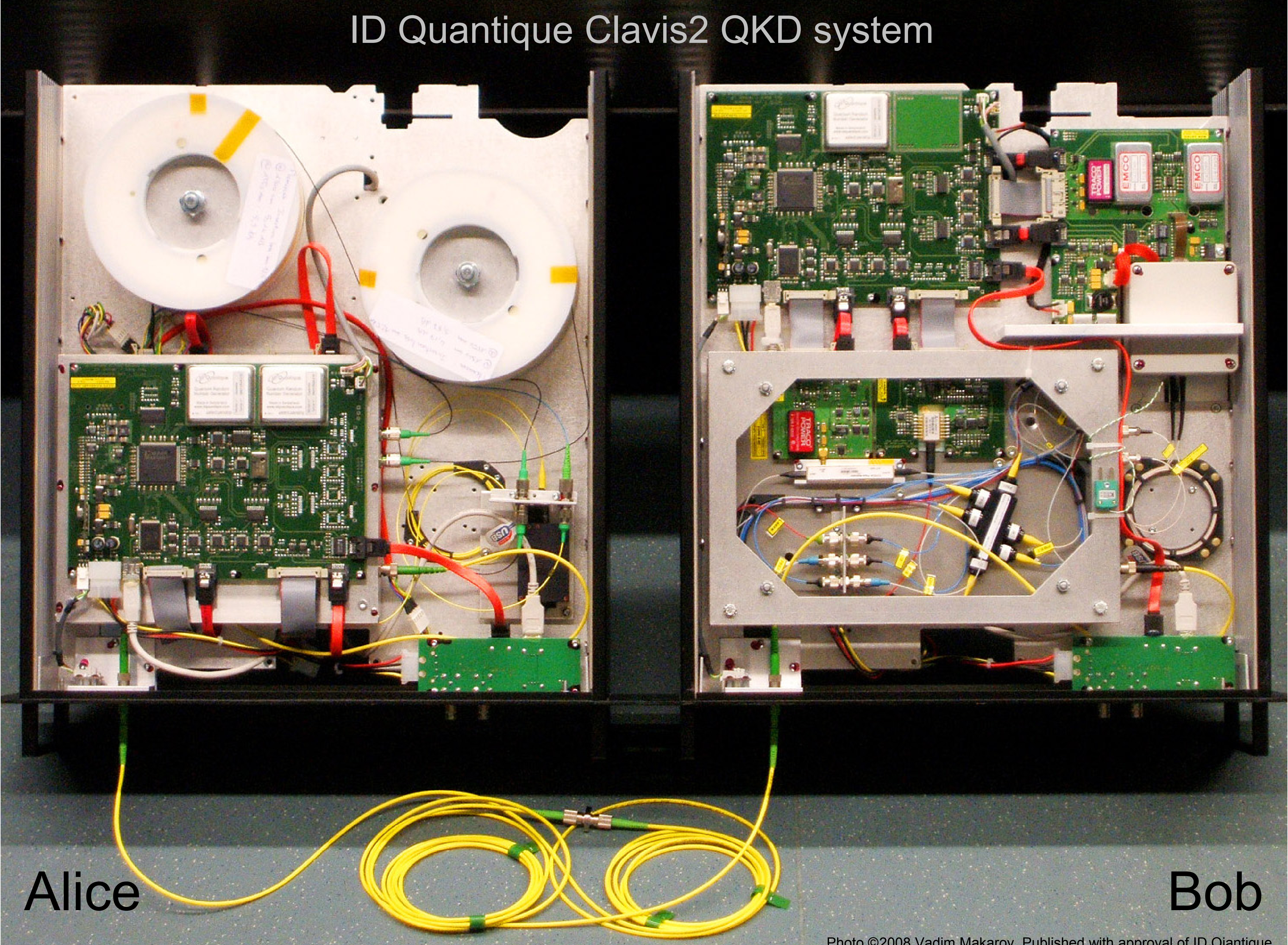
Do we trust the manufacturer?





Many components in QKD system can be Trojan-horsed:

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

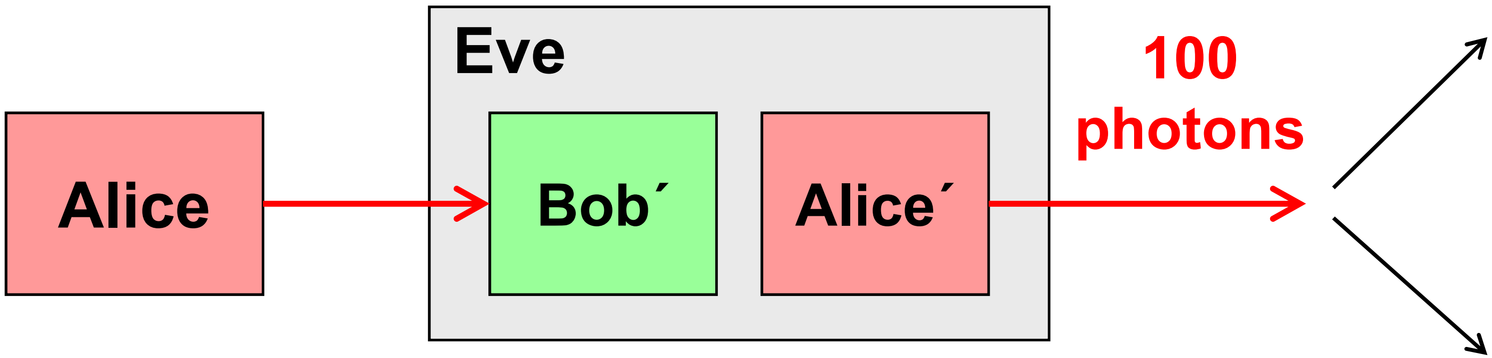

ID Quantique Clavis2 QKD system
TRACO POWER
EMCO
EMCO
TRACO POWER
USB
Alice
Bob
Photo ©2008 Vadim Makarov. Published with approval of ID Qiantique

Double clicks

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

Discard them?

Intercept-resend attack... with a twist:



Bob:

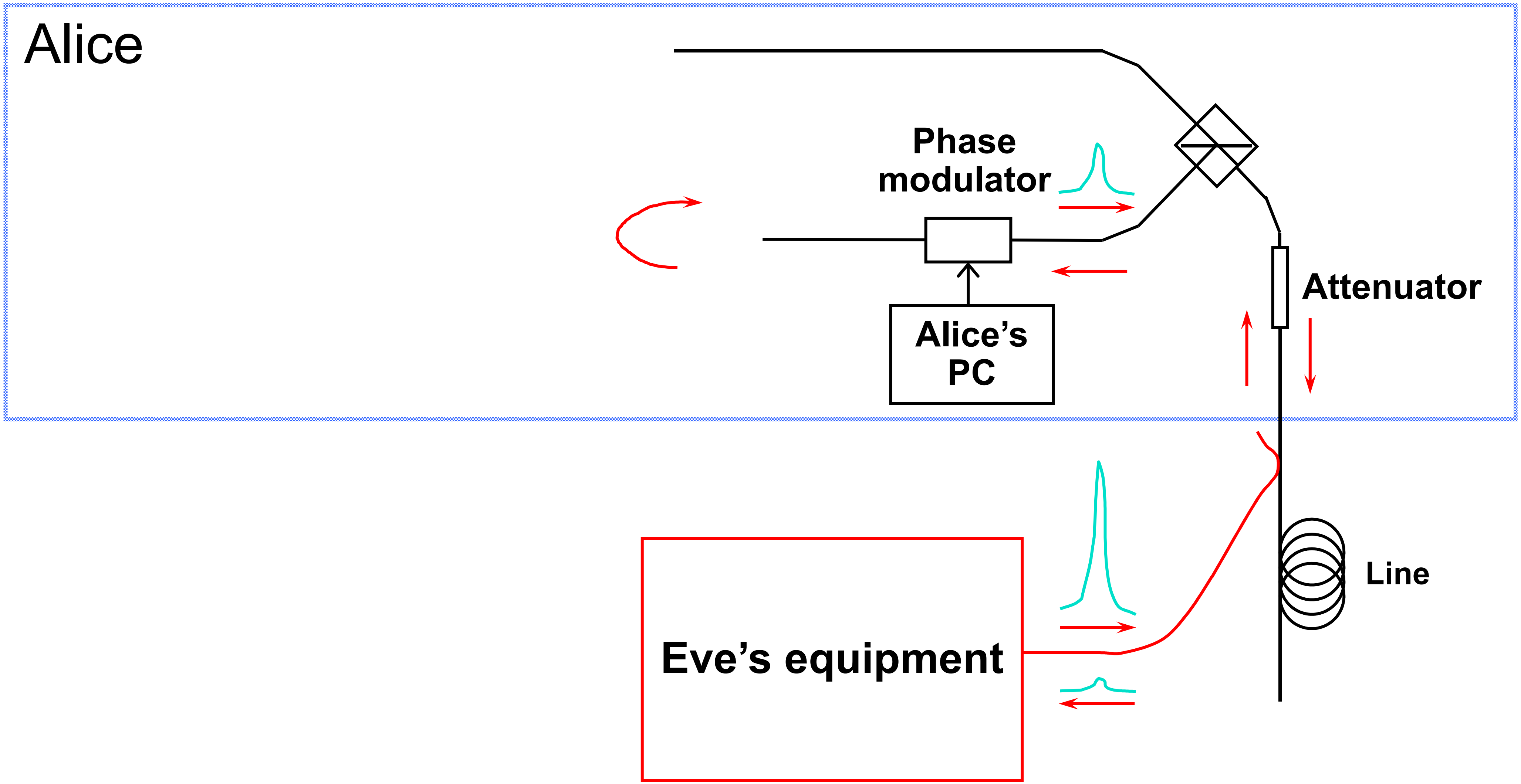
Detects in Eve's basis: single click

Detects in conjugate basis: double click, discarded

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

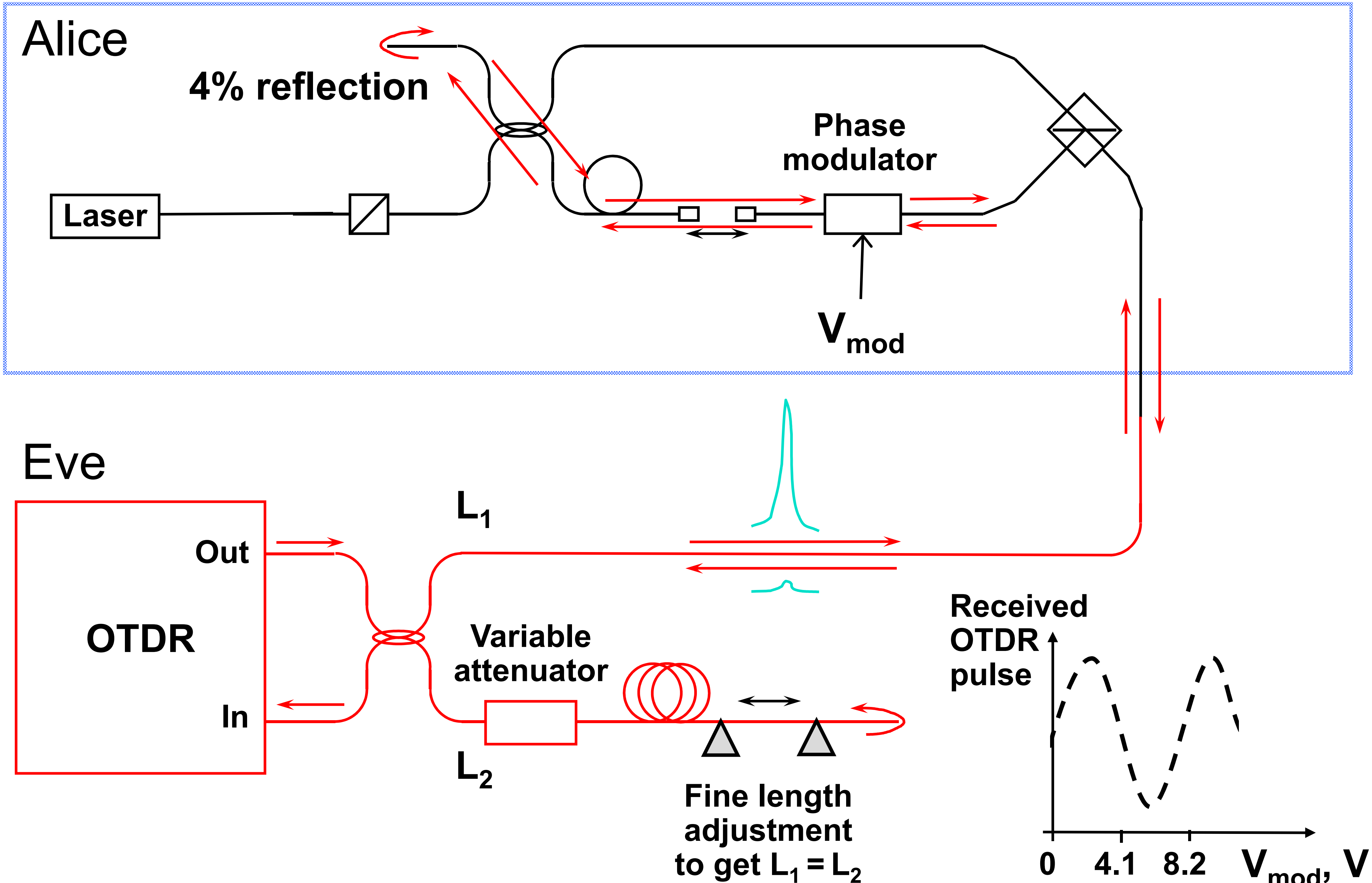
N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999)
T. Tsurumaru & K. Tamaki, Phys. Rev. A **78**, 032302 (2008)

Trojan-horse attack



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

Trojan-horse attack experiment



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

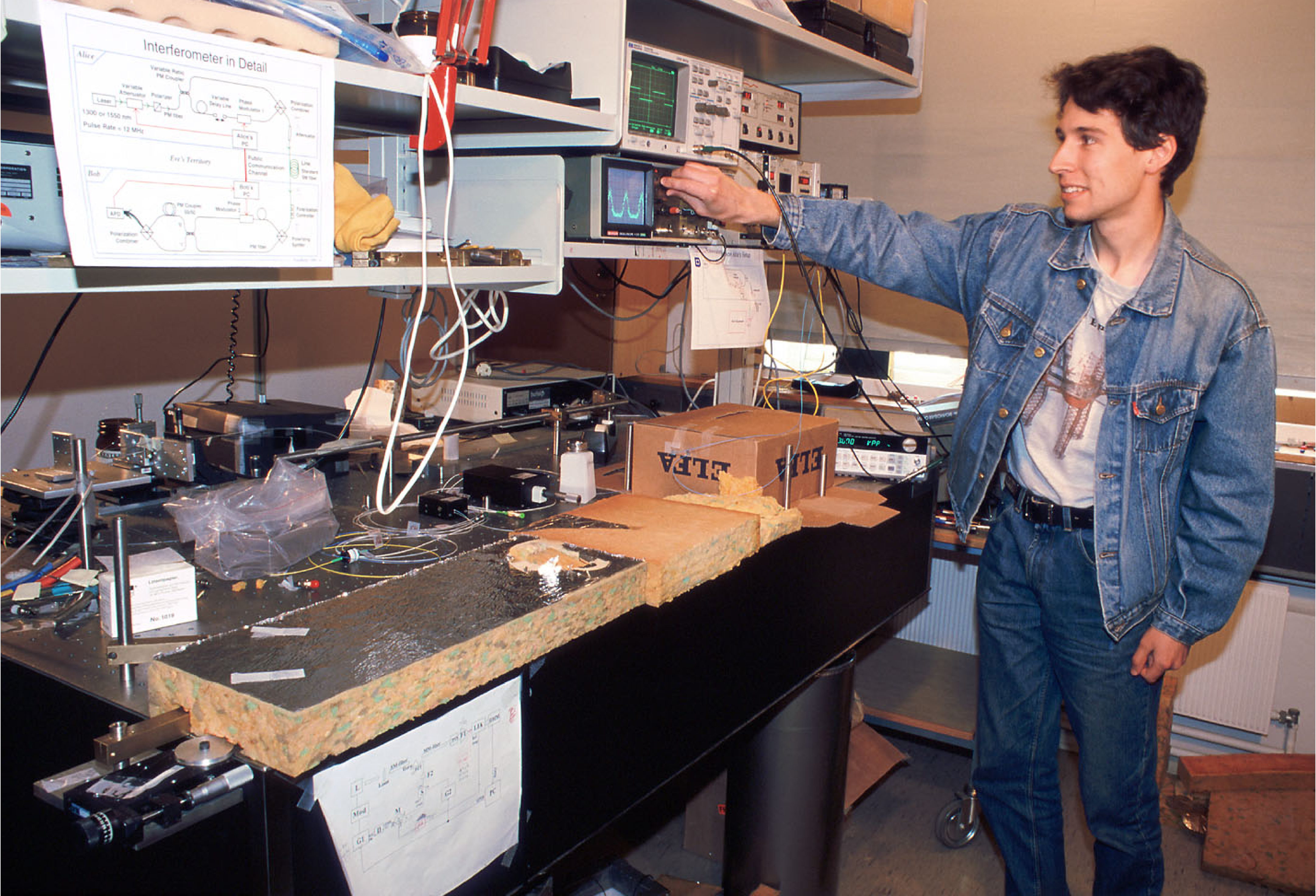
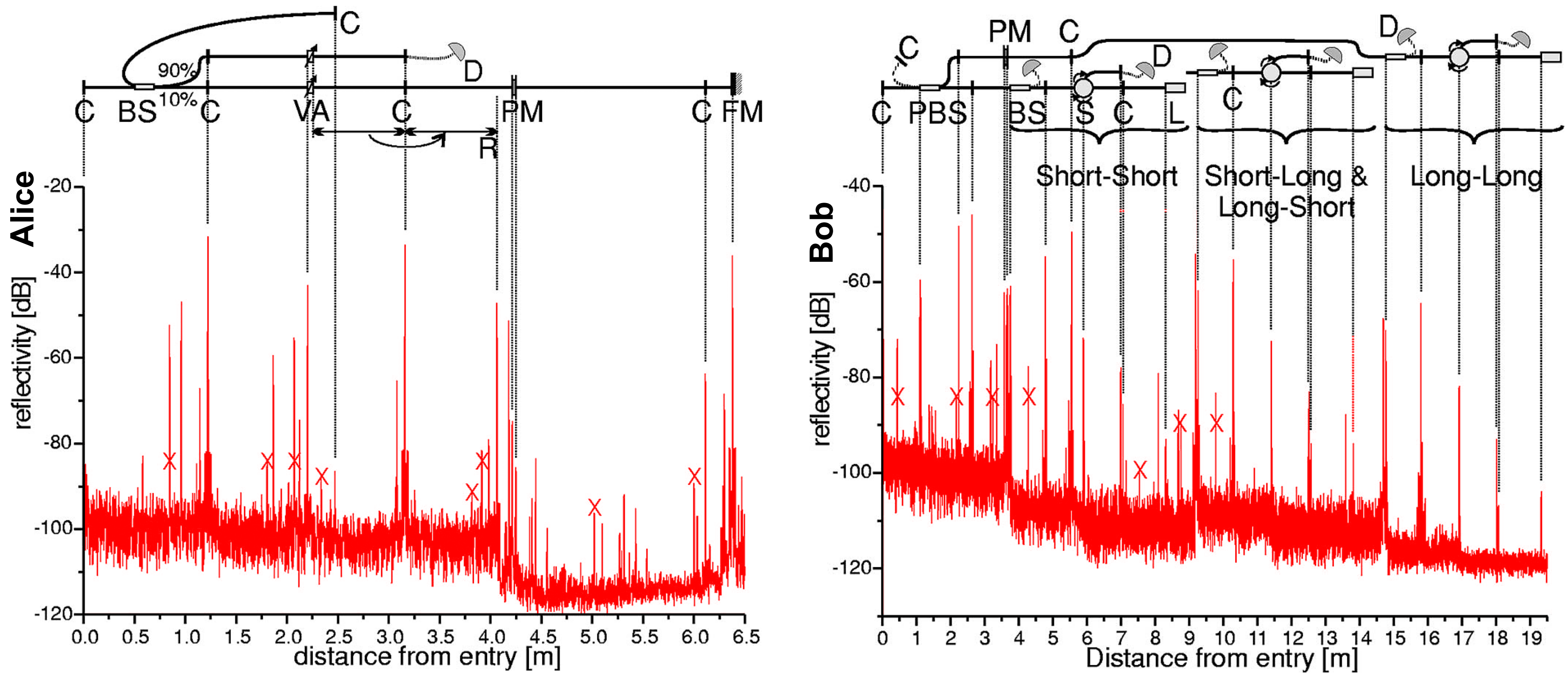


Photo ©2000 Vadim Makarov

Artem Vakhitov tunes up Eve’s setup

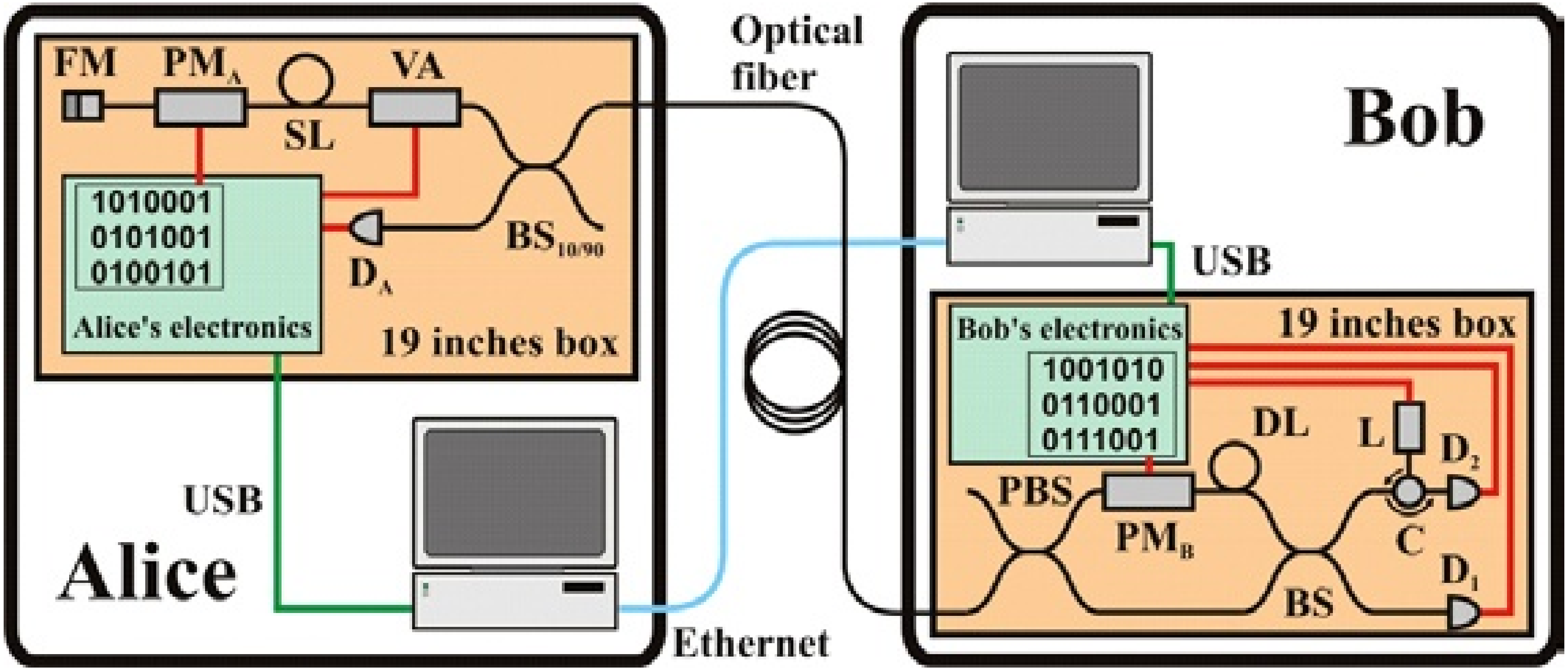
Trojan-horse attack for plug-and-play system



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

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

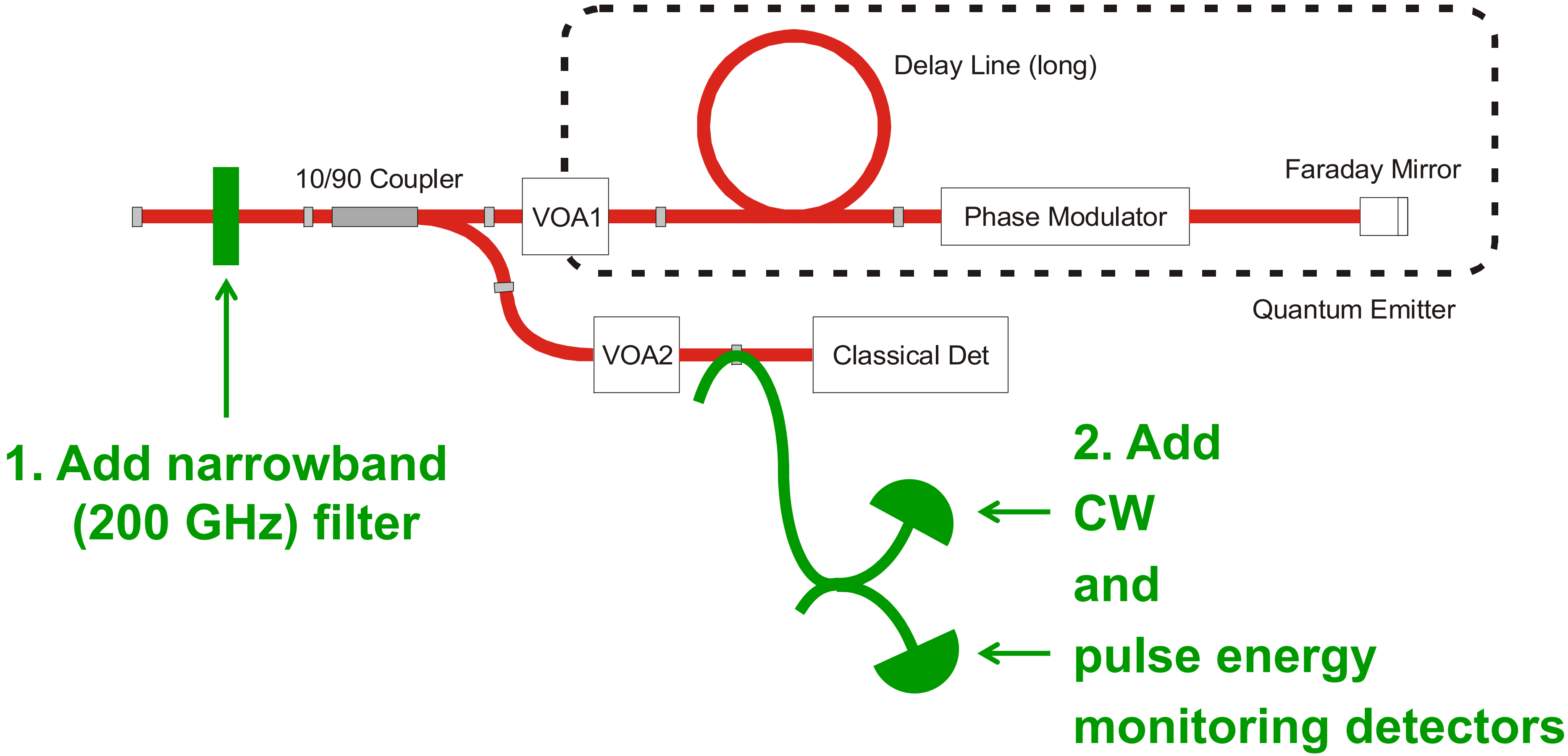
Countermeasures?



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)

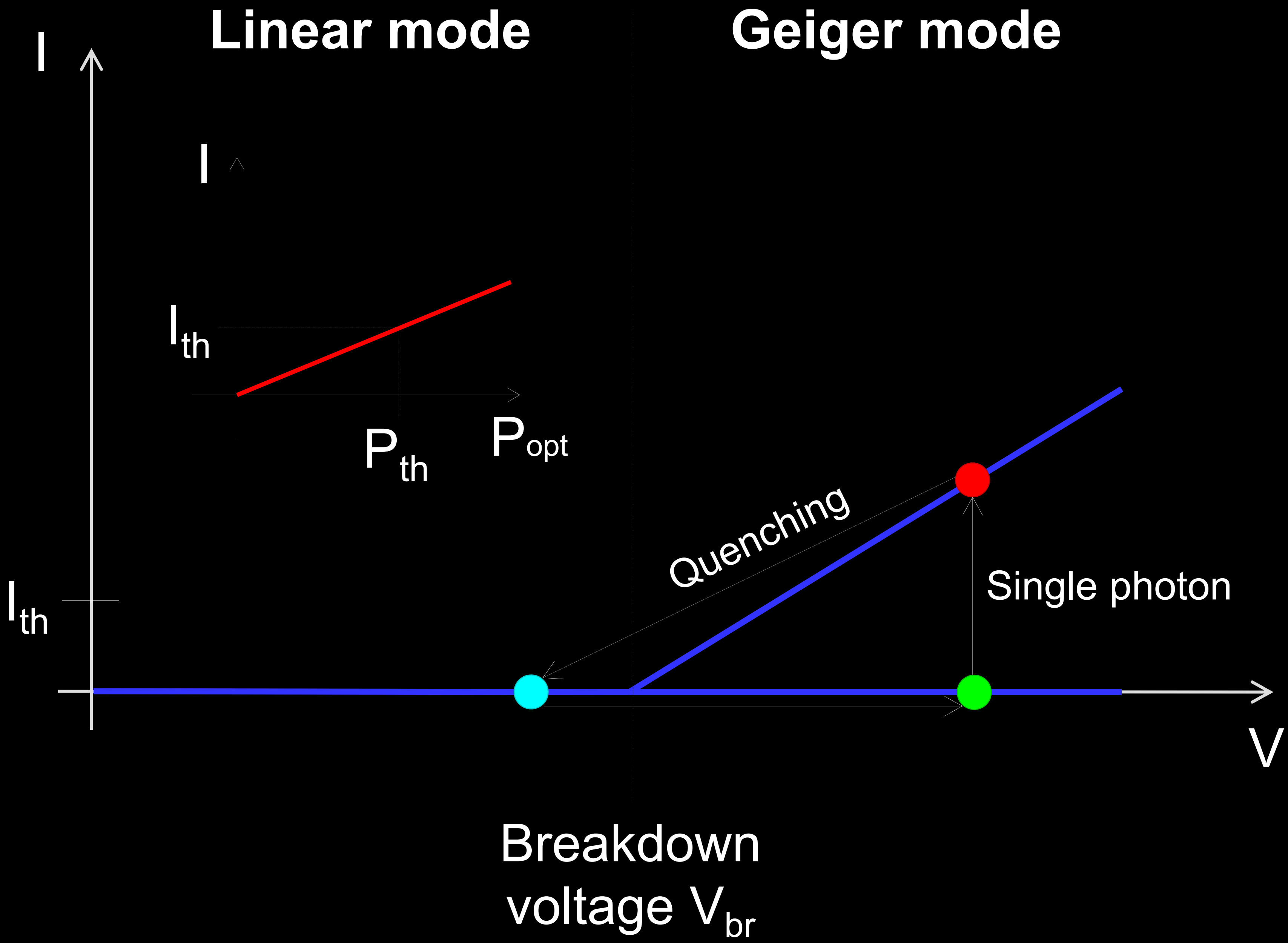
Attack	Target component	Tested system	Demonstrated eavesdr. (% key)?	Keeps full key rate?
Time-shift Y. Zhao *et al.*, Phys. Rev. A **78**, 042333 (2008)	detector	ID Quantique	**no** (fraction)	**no**
Phase-remapping F. Xu, B. Qi, H.-K. Lo, New J. Phys. **12**, 113026 (2010)	phase modulator	ID Quantique	**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**

Attack	Target component	Tested system	Demonstrated eavesdr. (% key)?	Keeps full key rate?
Time-shift Y. Zhao *et al.*, Phys. Rev. A **78**, 042333 (2008)	detector	ID Quantique	no (fraction)	[illegible]
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

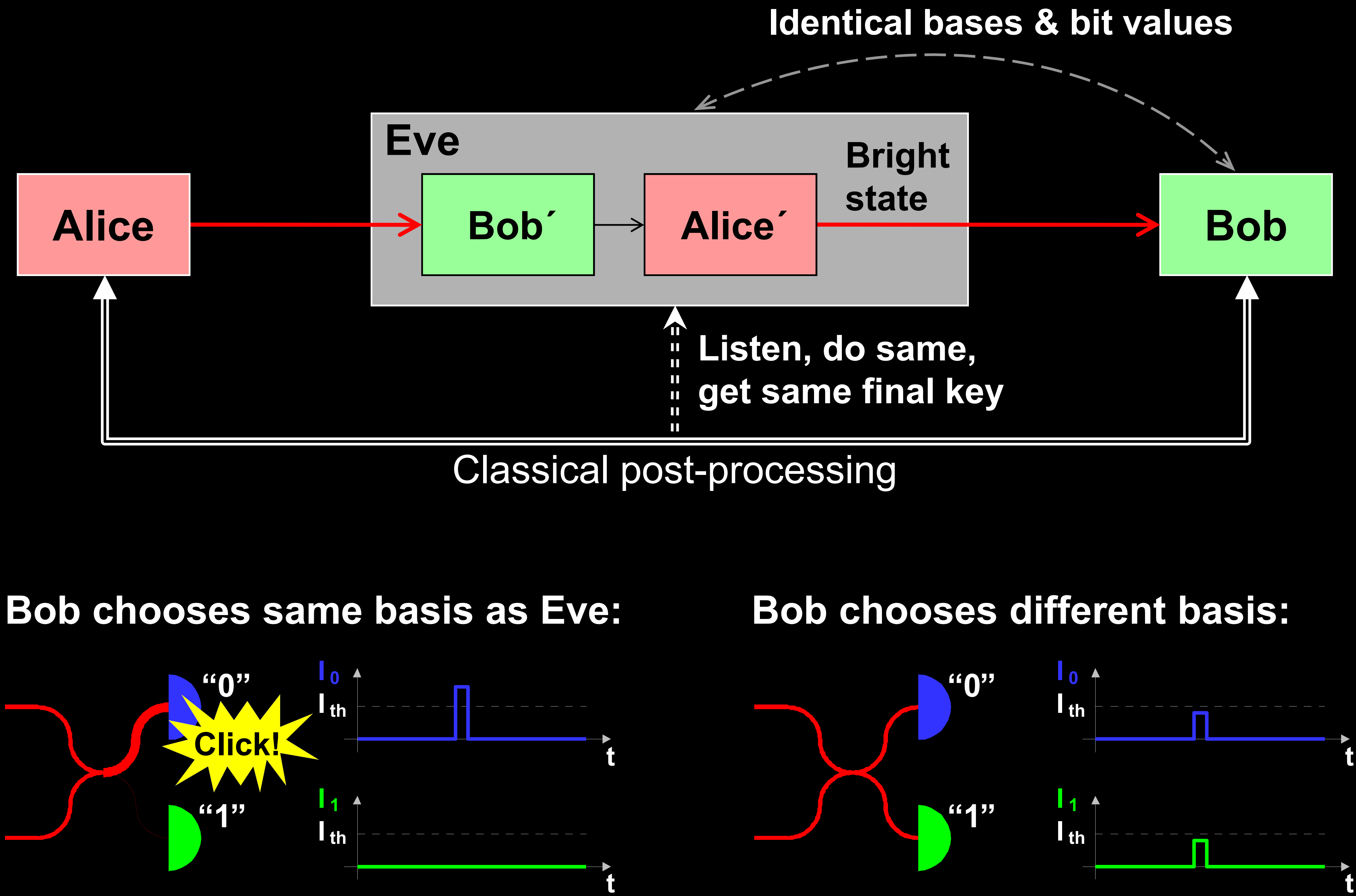
Every attack
breaks QKD security!

Attack	Target component	Tested system	Demonstrated eavesdr. (% key)?	Keeps full key rate?
Time-shift Y. Zhao *et al.*, Phys. Rev. A **78**, 042333 (2008)	detector	ID Quantique	**no** (fraction)	**no**
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**

How avalanche photodiodes (APDs) work



Faked-state attack in APD linear mode



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

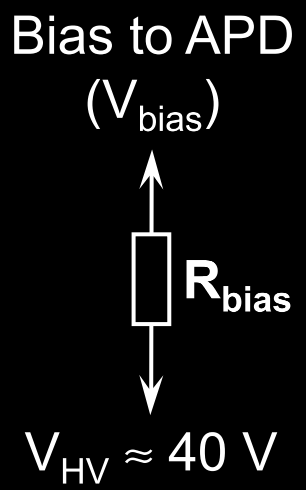
Launching bright pulse after the gate...

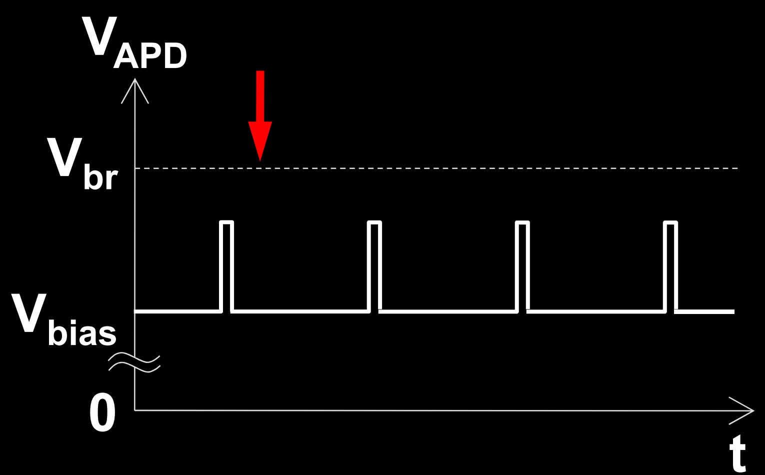
afterpulses,
increased QBER

▼ bright
▼ < 120 photons

C. Wiechers *et al.*, New J. Phys. **13**, 013043 (2011)
L. Lydersen *et al.*, Phys. Rev. A **84**, 032320 (2011)

Add CW light...

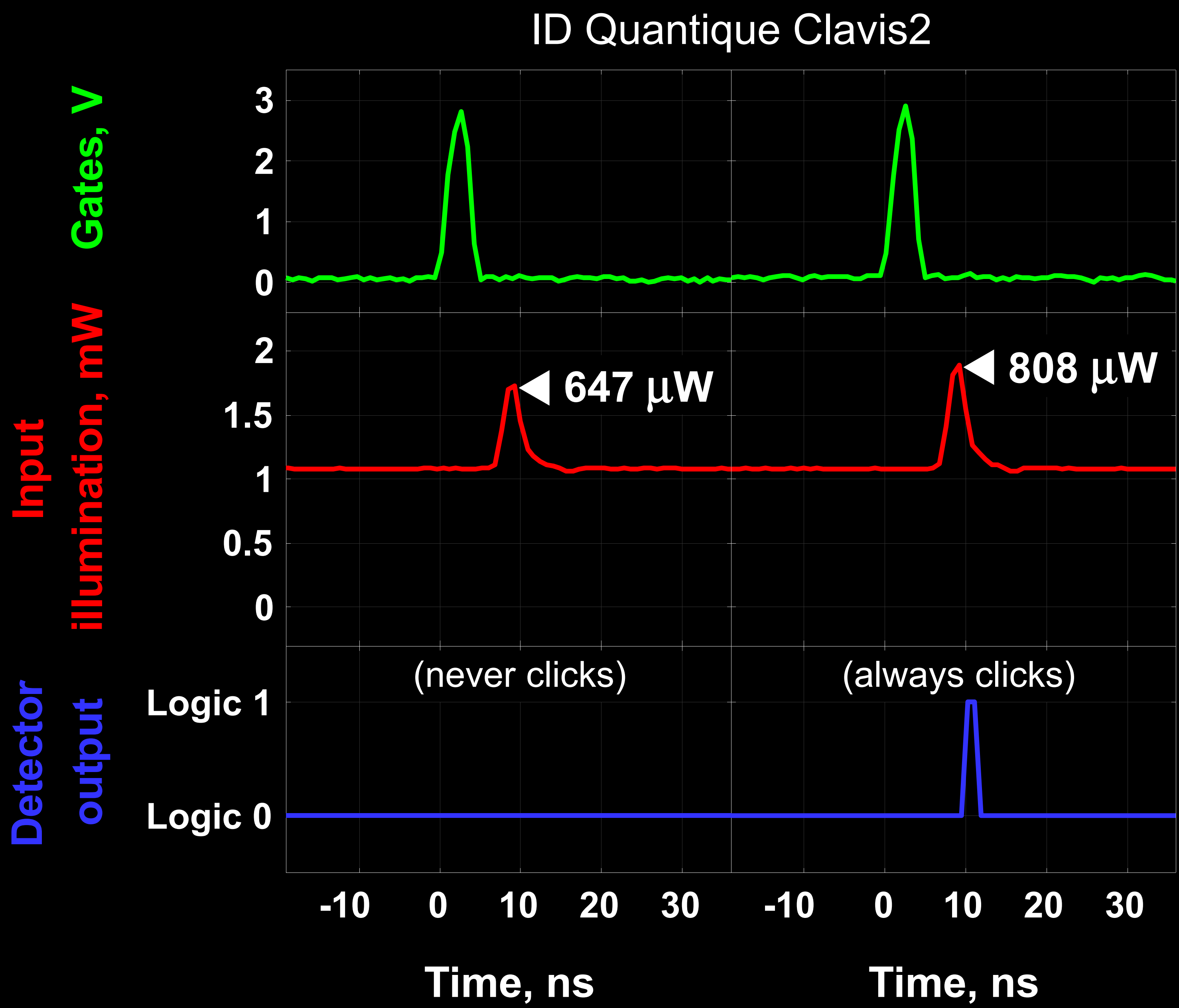




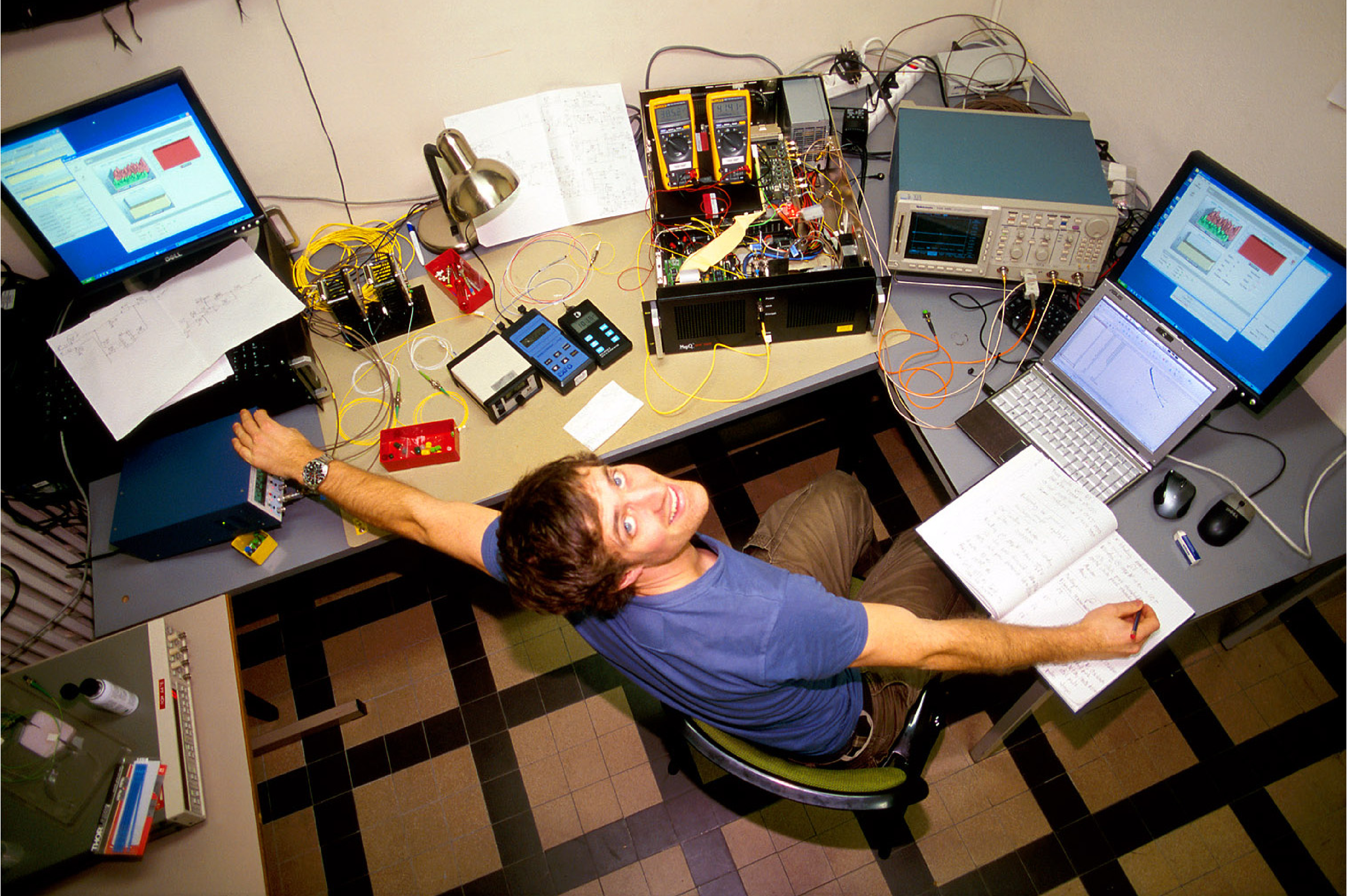
Detector blind!
Zero dark count rate

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

Full detector control

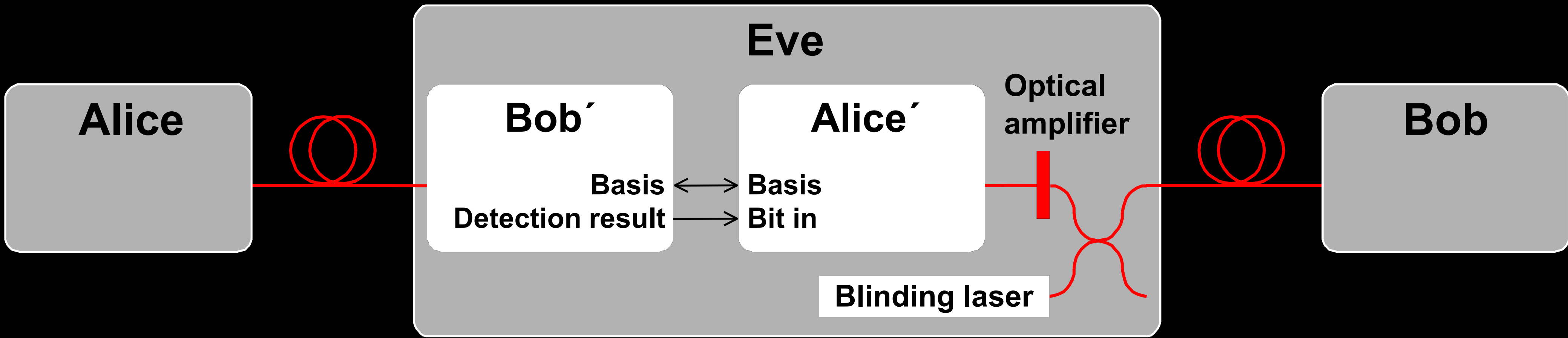


L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Nat. Photonics **4**, 686 (2010)



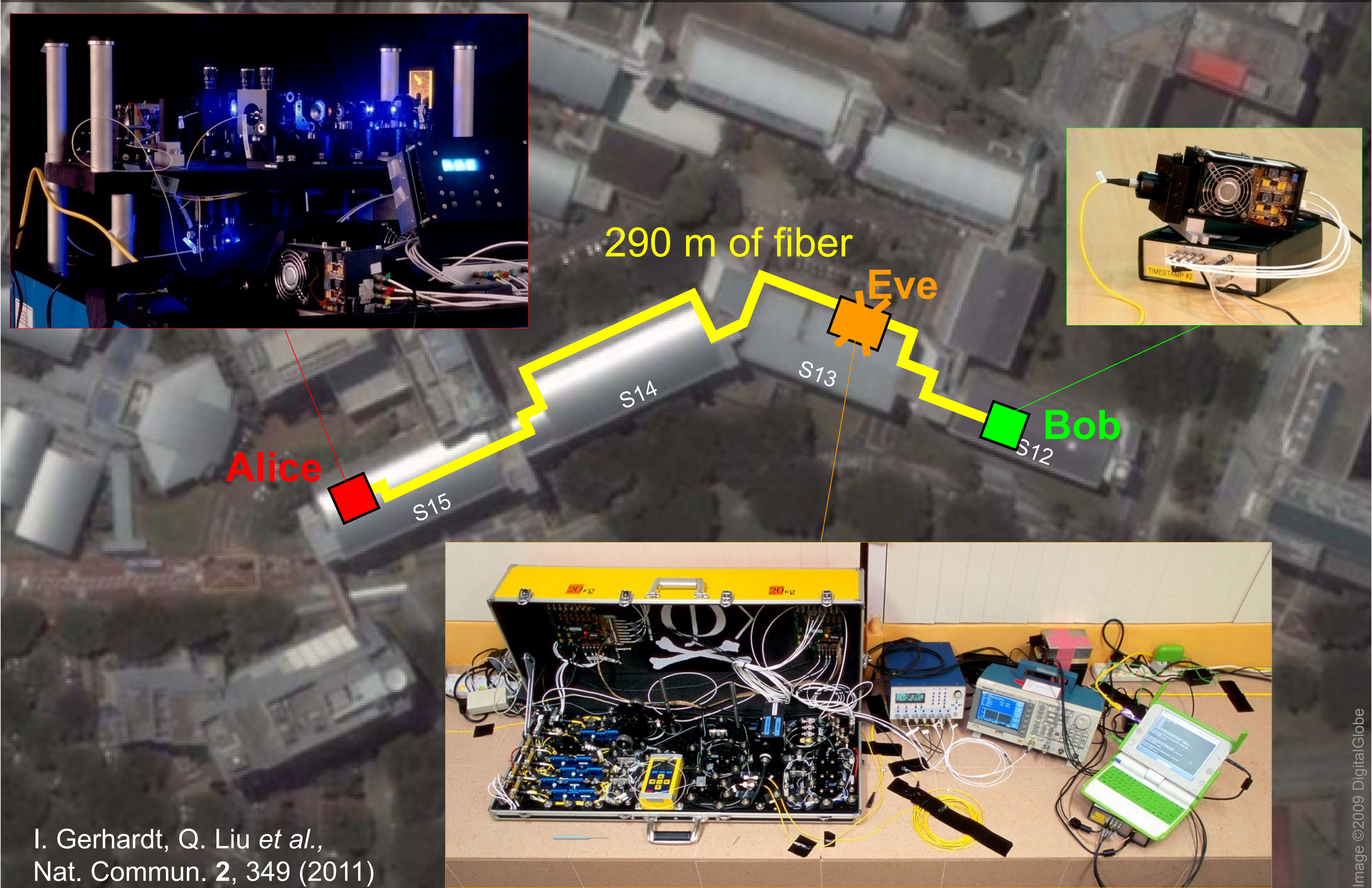
Lars Lydersen testing MagiQ Technologies QPN 5505

Proposed full eavesdropper



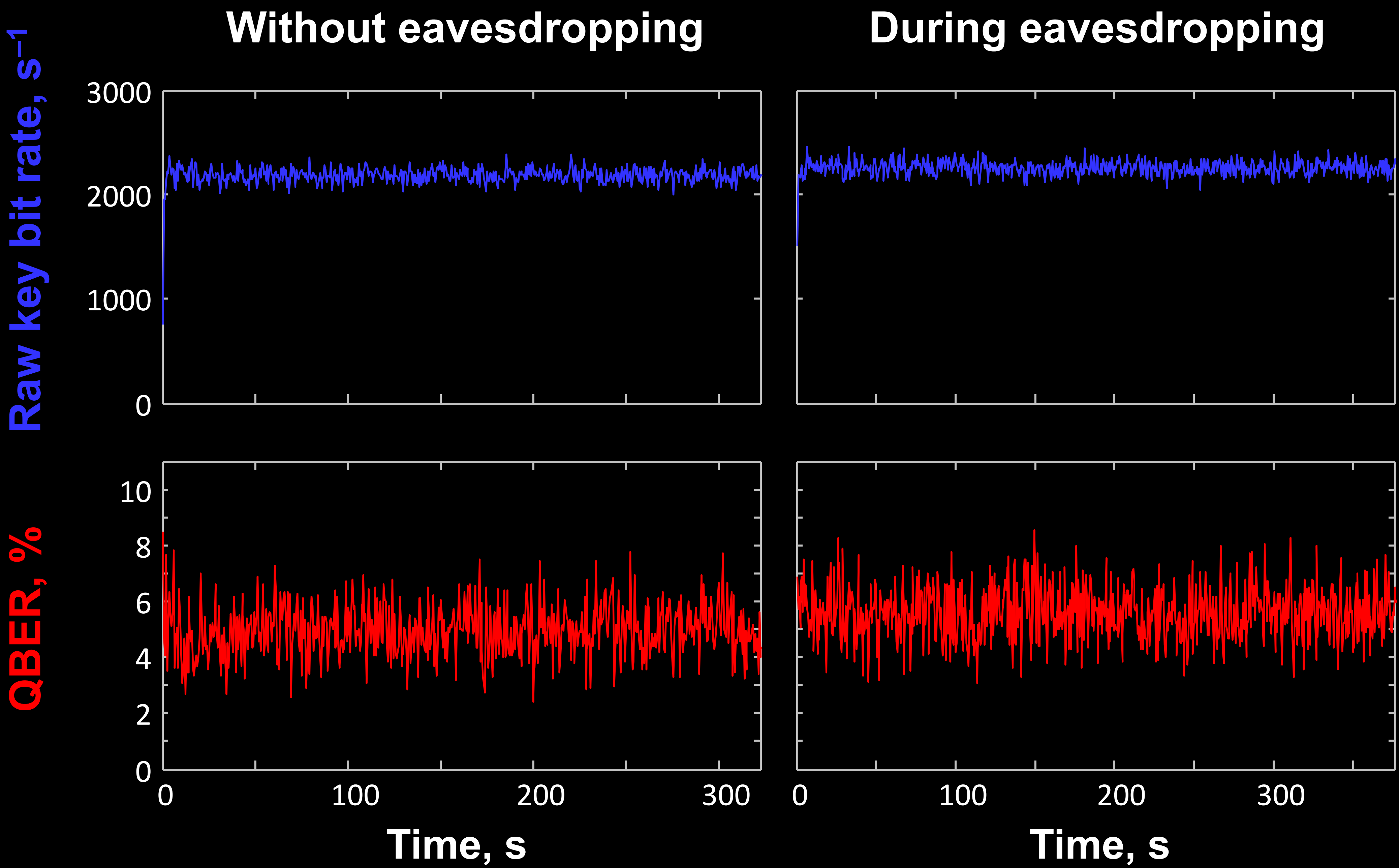
Eavesdropping 100% key on installed QKD line

on campus of the National University of Singapore, July 4-5, 2009



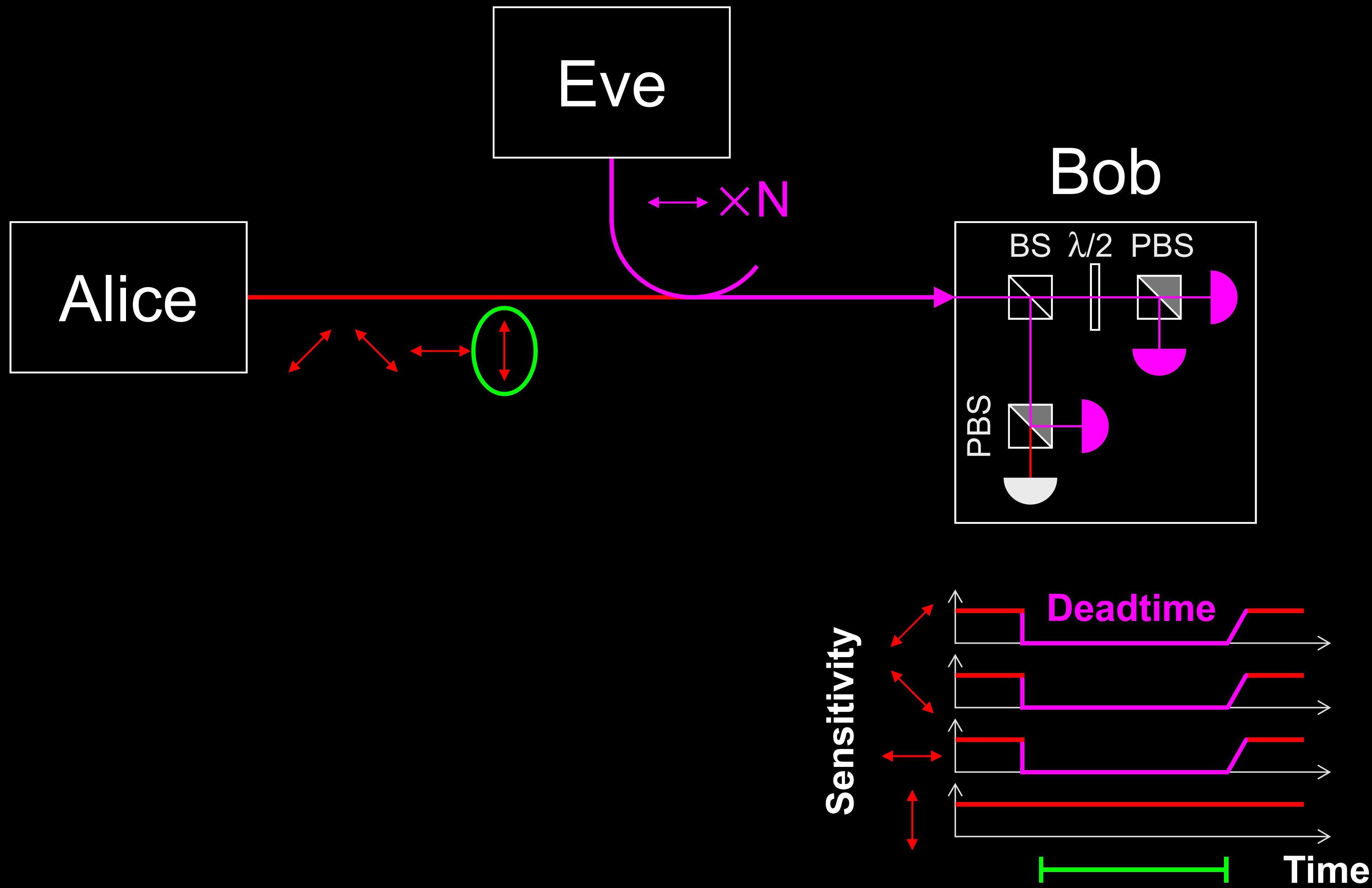
I. Gerhardt, Q. Liu *et al.*,
Nat. Commun. **2**, 349 (2011)

Eve does not affect QKD performance



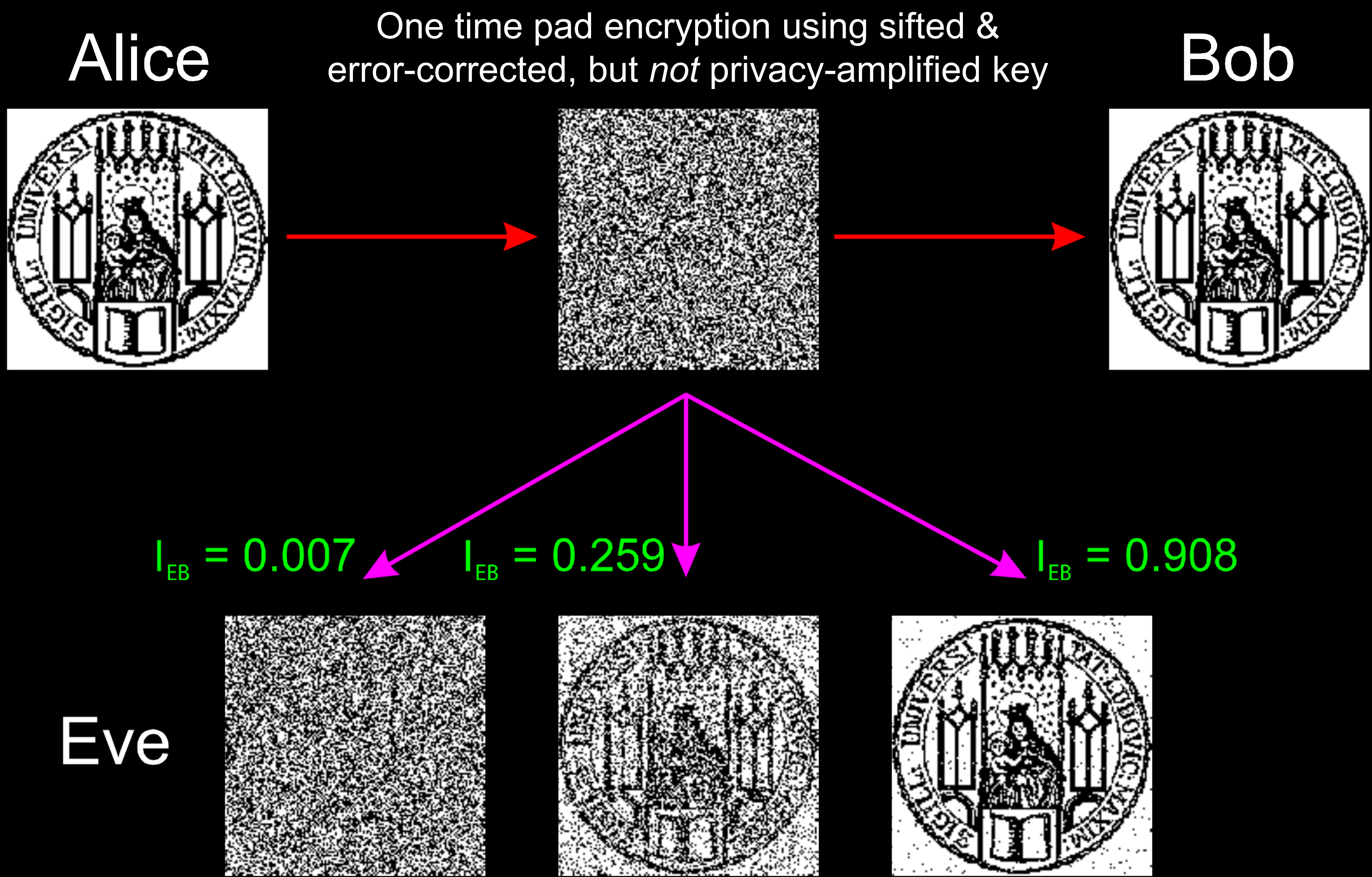
I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, V. Makarov, Nat. Commun. **2**, 349 (2011)

Detector deadtime attack



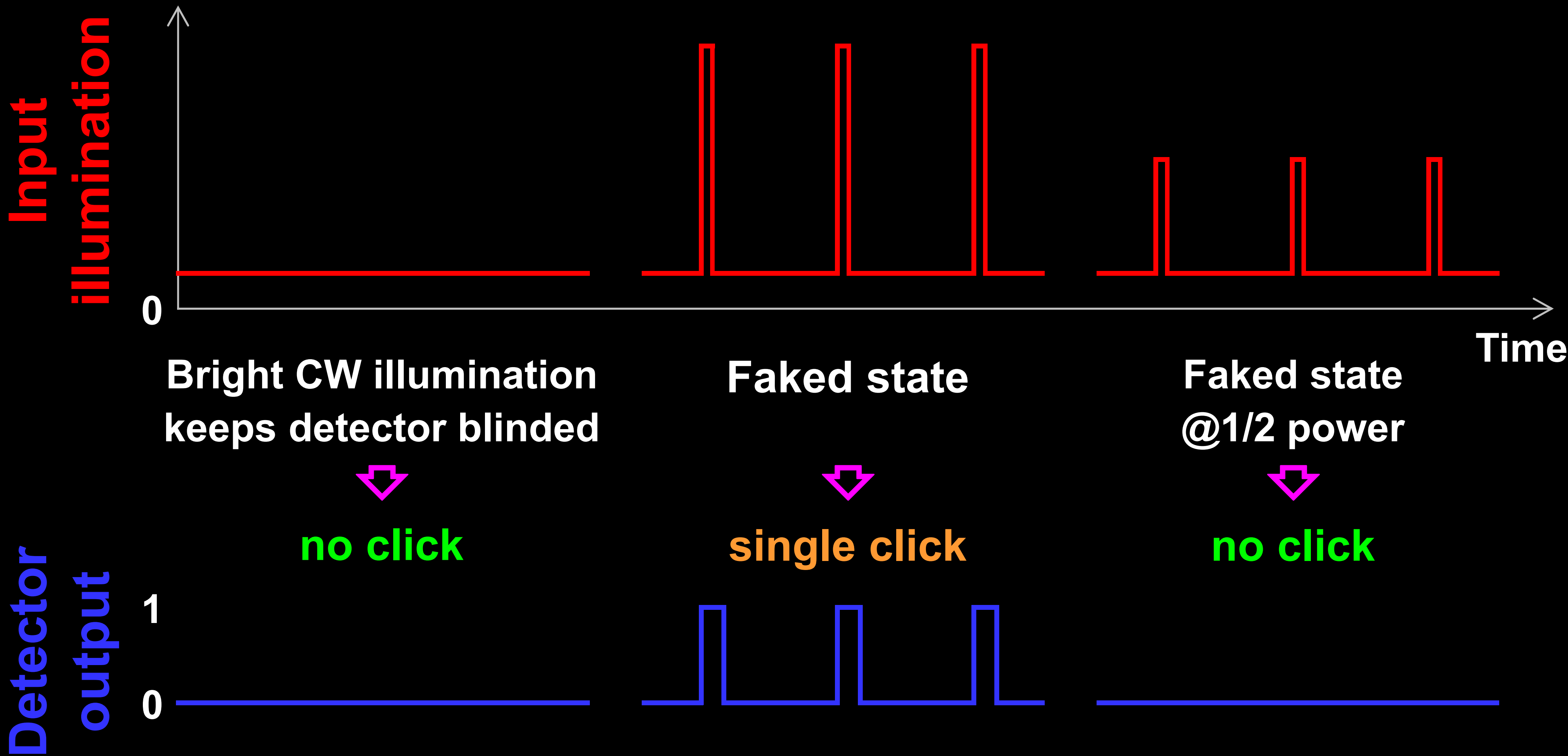
H. Weier *et al.*, “Quantum eavesdropping without interception: An attack exploiting the dead time of single photon detectors,” New J. Phys. **13**, 073024 (2011)

Eavesdropping < 100% key



H. Weier *et al.*, "Quantum eavesdropping without interception: An attack exploiting the dead time of single photon detectors," New J. Phys. **13**, 073024 (2011)

Detector control demo. Now I am blind, now I click...

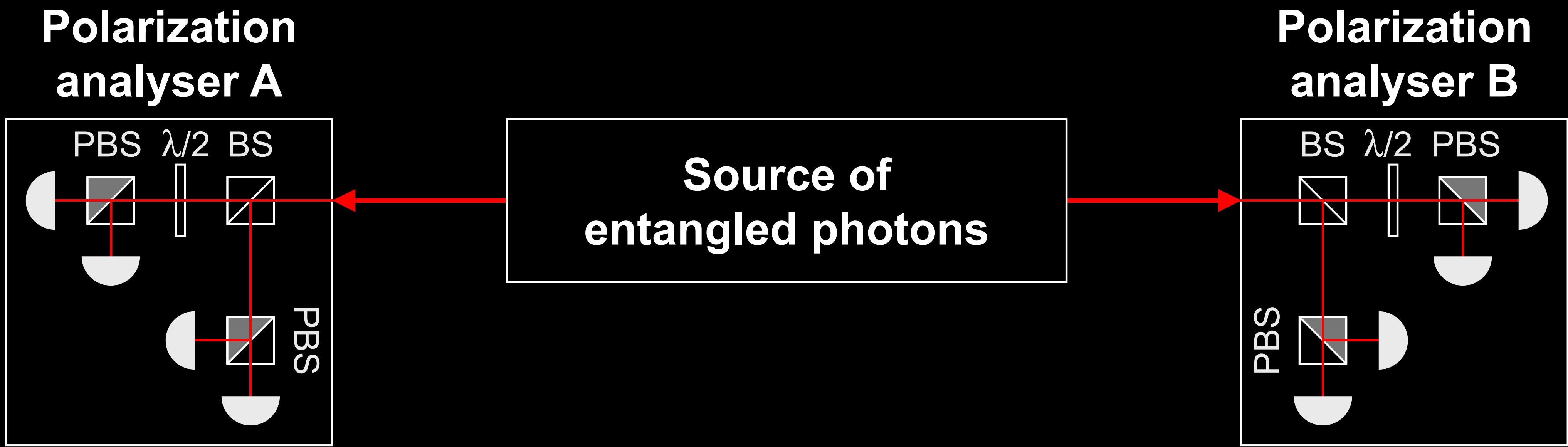


Faking violation of Bell inequality

CHSH inequality: $|S = E_{AB} + E_{A'B} + E_{AB'} - E_{A'B'}| \leq 2$

$$E \in [-1, 1]$$

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



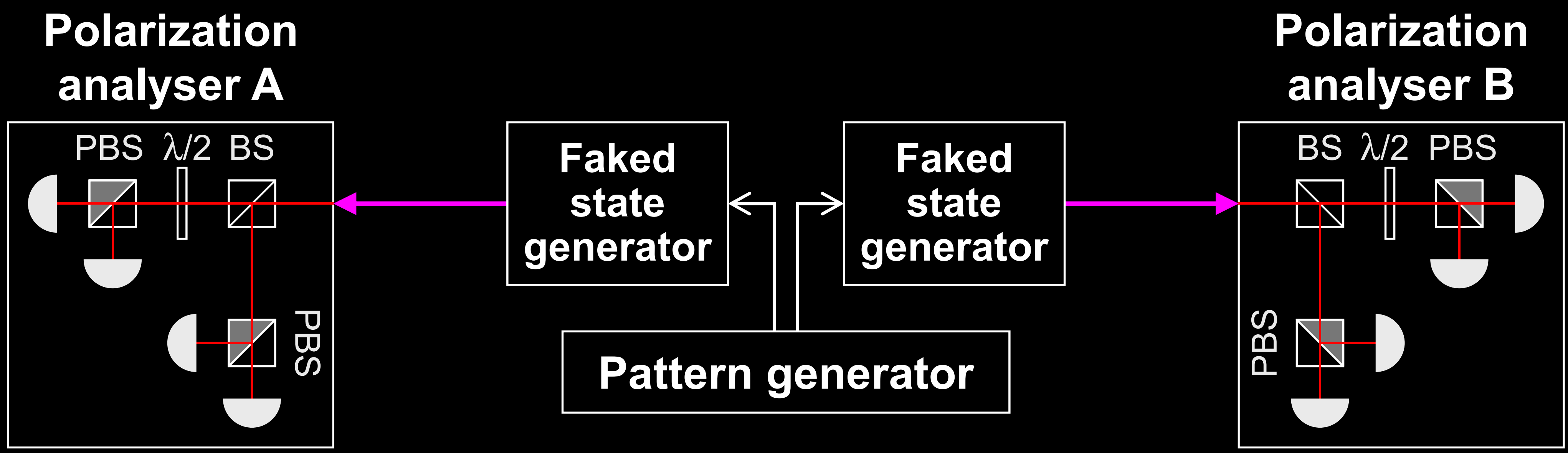
I. Gerhardt, Q. Liu *et al.*, Phys. Rev. Lett. **107**, 170404 (2011)

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



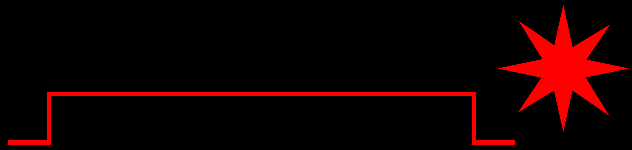
Passive basis choice: $|S| \leq 4$, click probability = 100%

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

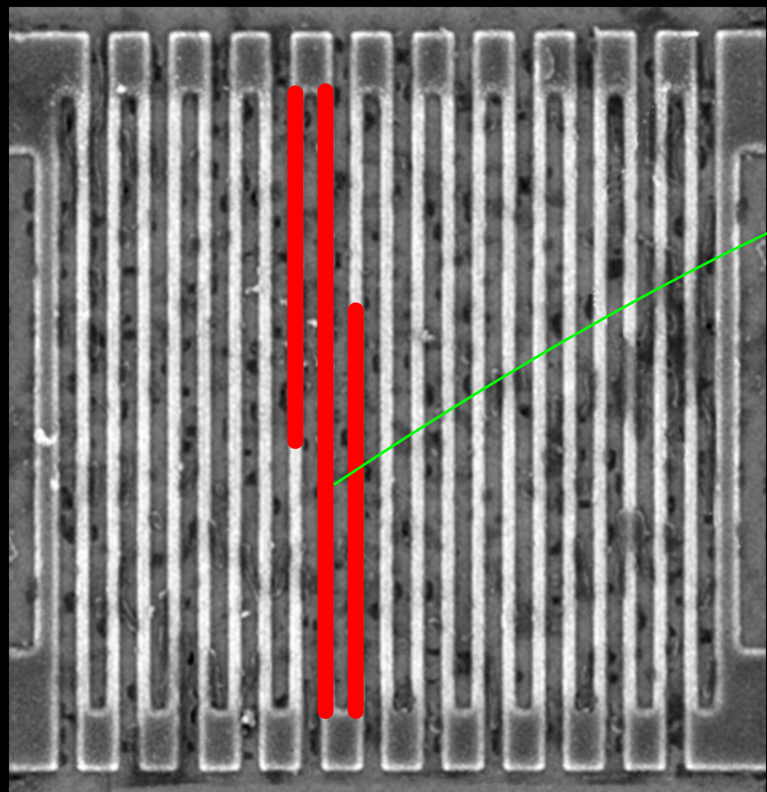
I. Gerhardt, Q. Liu *et al.*, Phys. Rev. Lett. **107**, 170404 (2011)

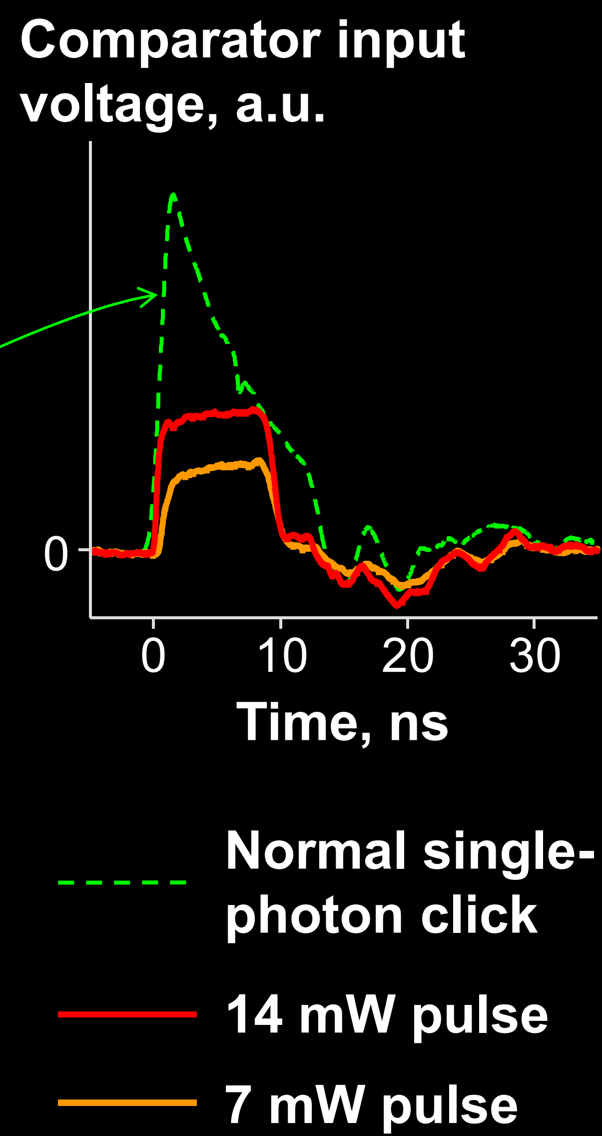
Controlling superconducting nanowire single-photon detectors

1. Blind (latch)



2. Control





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

Responsible disclosure is important

2009

Example: hacking commercial systems

- ID Quantique got a detailed vulnerability report
  - reaction: requested time, developed a patch

2010

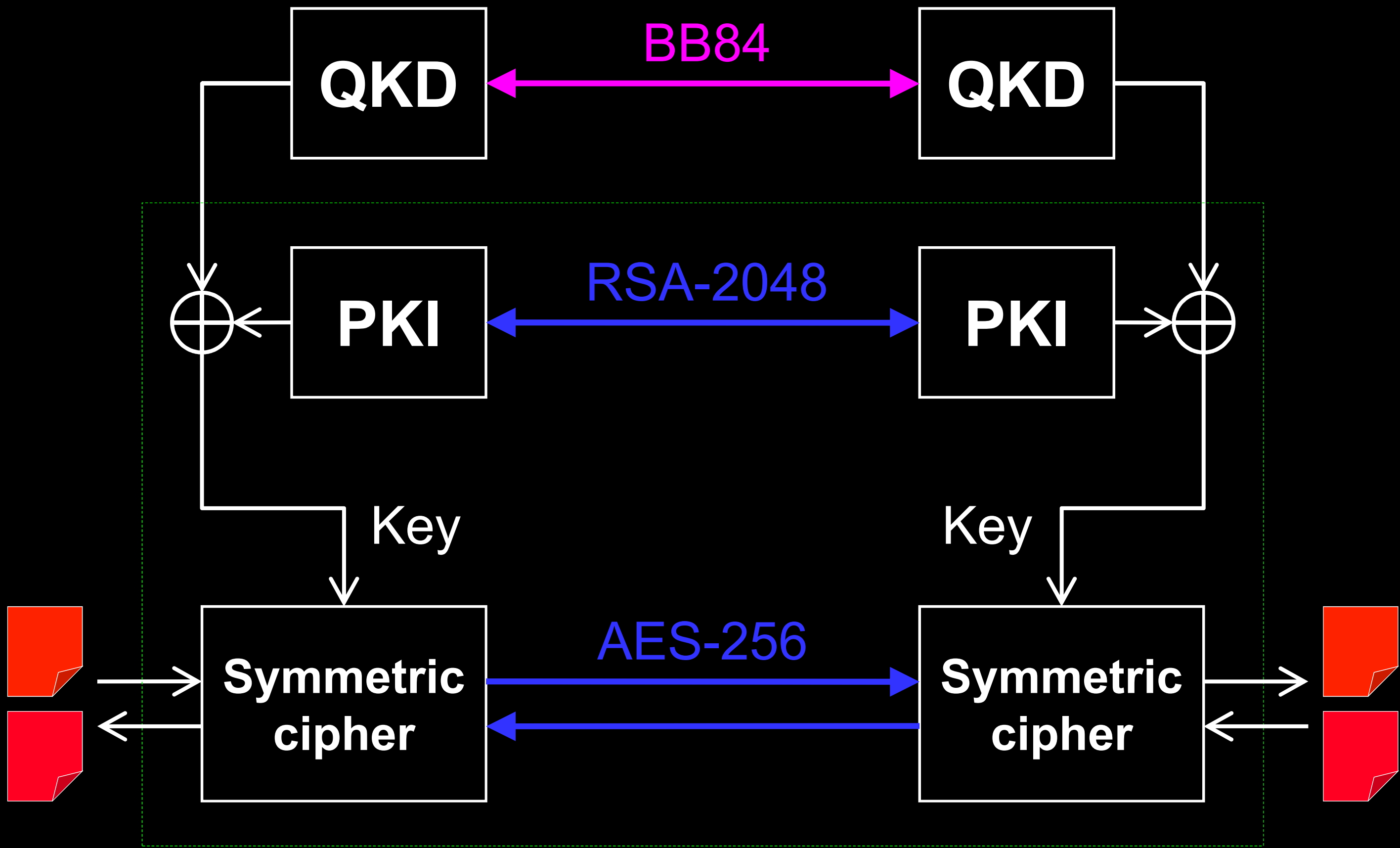
- MagiQ Technologies got a detailed vulnerability report
  - reaction: informed us that QPN 5505 is discontinued
- Results presented orally at a scientific conference
- Public disclosure in a journal paper

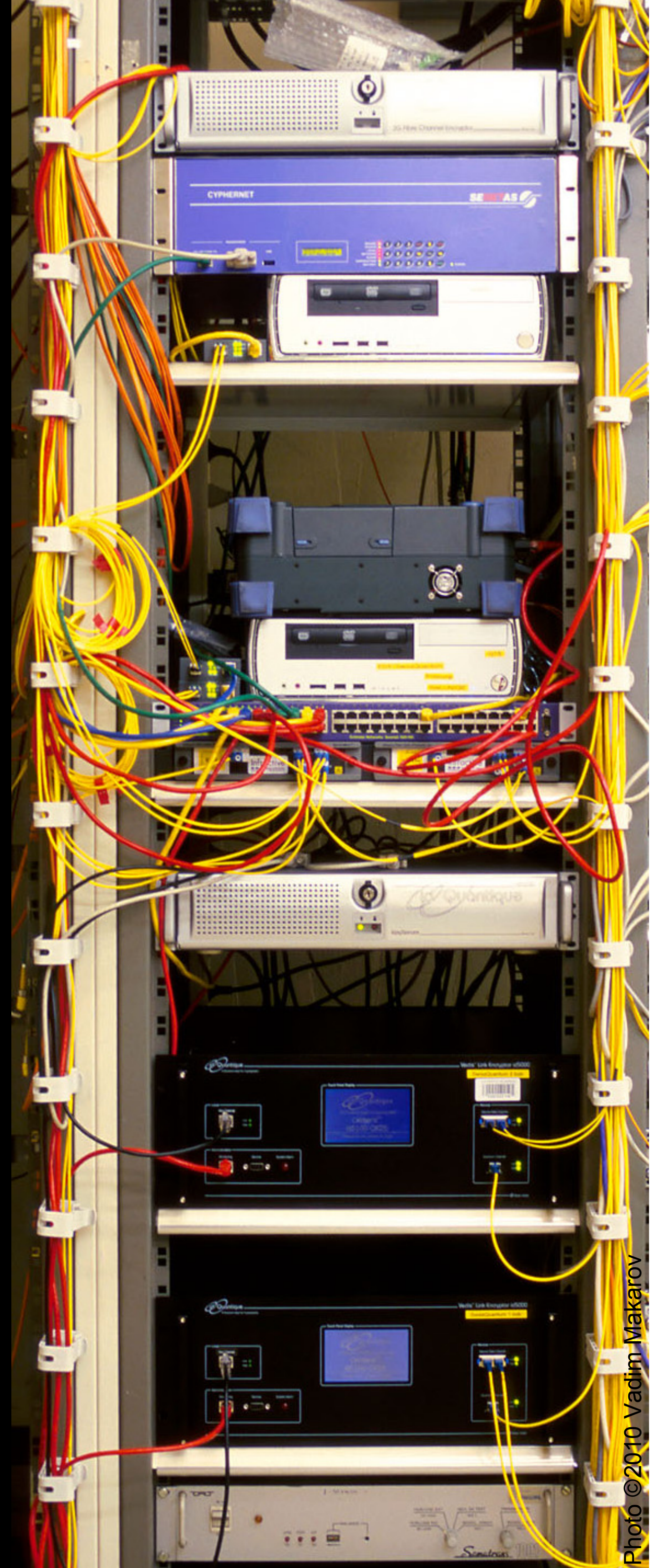
L. Lydersen *et al.*, Nat. Photonics **4**, 686 (2010)

Can we eavesdrop on commercial systems?

ID Quantique's Cerberis:

Dual key agreement





Countermeasures

Kill the hacker

- Illegal
- Does not solve the problem

Countermeasures

"Quick and intuitive" patches

- "Deterministic detection or exclusion (of attack)"

Z. L. Yuan, J. F. Dynes, A. J. Shields, Appl. Phys. Lett. **99**, 196102 (2011).

- Lead away from provable security model of QKD
- Can often be defeated by hacking advances

L. Lydersen, V. Makarov, J. Skaar, Appl. Phys. Lett. **99**, 196101 (2011)
L. Lydersen *et al.*, Phys. Rev. A **84**, 032320 (2011)

Integrate imperfection into security proof

- May require deep modification of protocol, hardware, and security proof

Ø. Marøy *et al.*, Phys. Rev. A **82**, 032337 (2010)
L. Lydersen *et al.*, Phys. Rev. A **83**, 032306 (2011)

H.-K. Lo, M. Curty, B. Qi, arXiv:1109.1473
S. L. Braunstein, S. Pirandola, arXiv:1109.2330

$|\Phi\rangle$