Quantum cryptography

Vadim Makarov

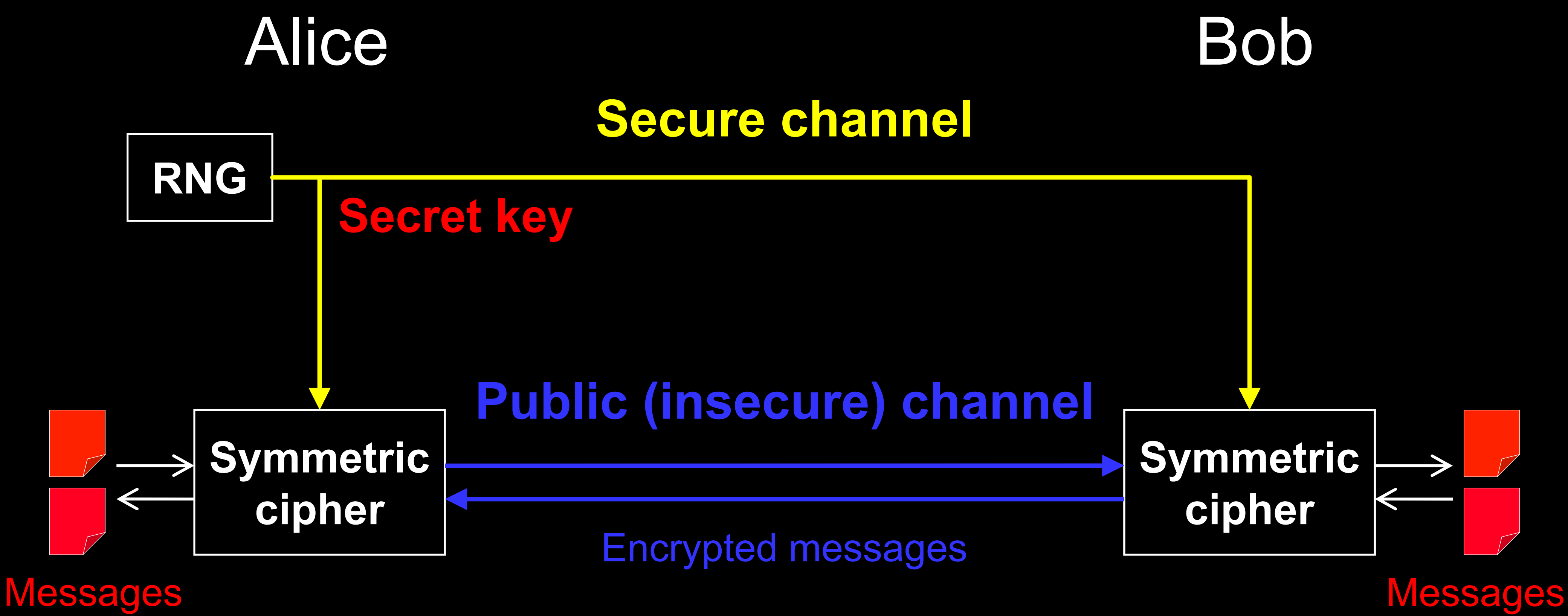
Image from cover of Physics World, March 1998

Quantum hacking lab
www.vad1.com/lab
IQC Institute for Quantum Computing

Communication security you enjoy daily

- Paying by credit card in a supermarket
- Cell phone conversations, SMS
- Email, chat, online calls
- Secure browsing, shopping online
- Cloud storage and communication between your devices
- Software updates on your computer, phone, tablet
- Online banking
- Off-line banking: the *bank* needs to communicate internally
- Electricity, water: the *utility* needs to communicate internally
- Car keys
- Electronic door keys
- Government services (online or off-line)
- Medical records at your doctor, hospital
- Bypassing government surveillance and censorship

Encryption and key distribution



Quantum key distribution transmits secret key by sending quantum states over *open channel.*

Public key cryptography

E.g., RSA (Rivest-Shamir-Adleman)

Elliptic-curve

Based on *hypothesized* one-way functions

- Unexpected advances in classical cryptanalysis
- Shor's factorization algorithm for quantum computer

P. W. Shor, SIAM J. Comput. **26**, 1484 (1997)

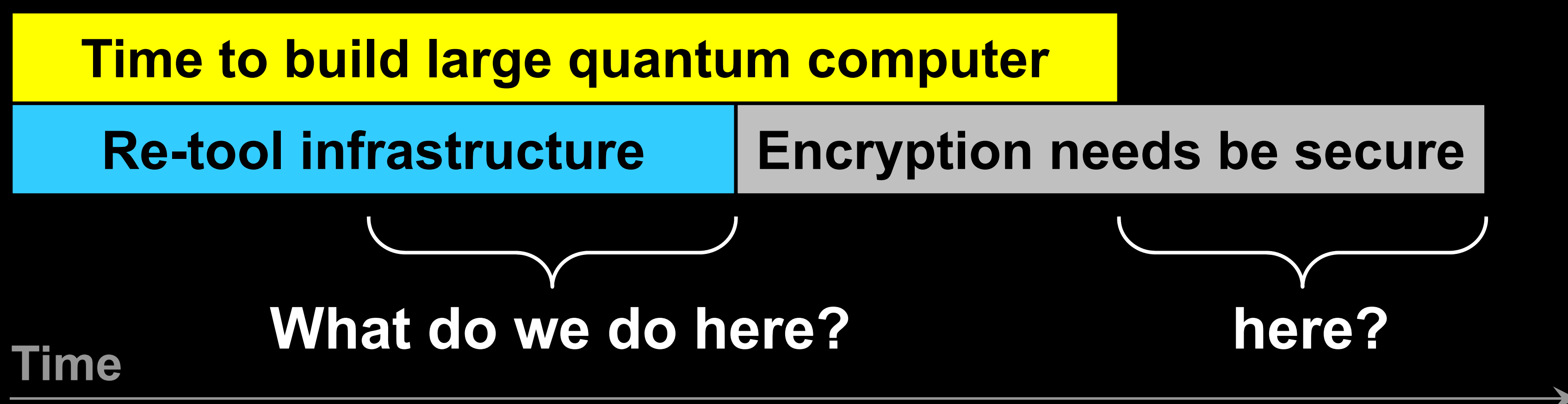
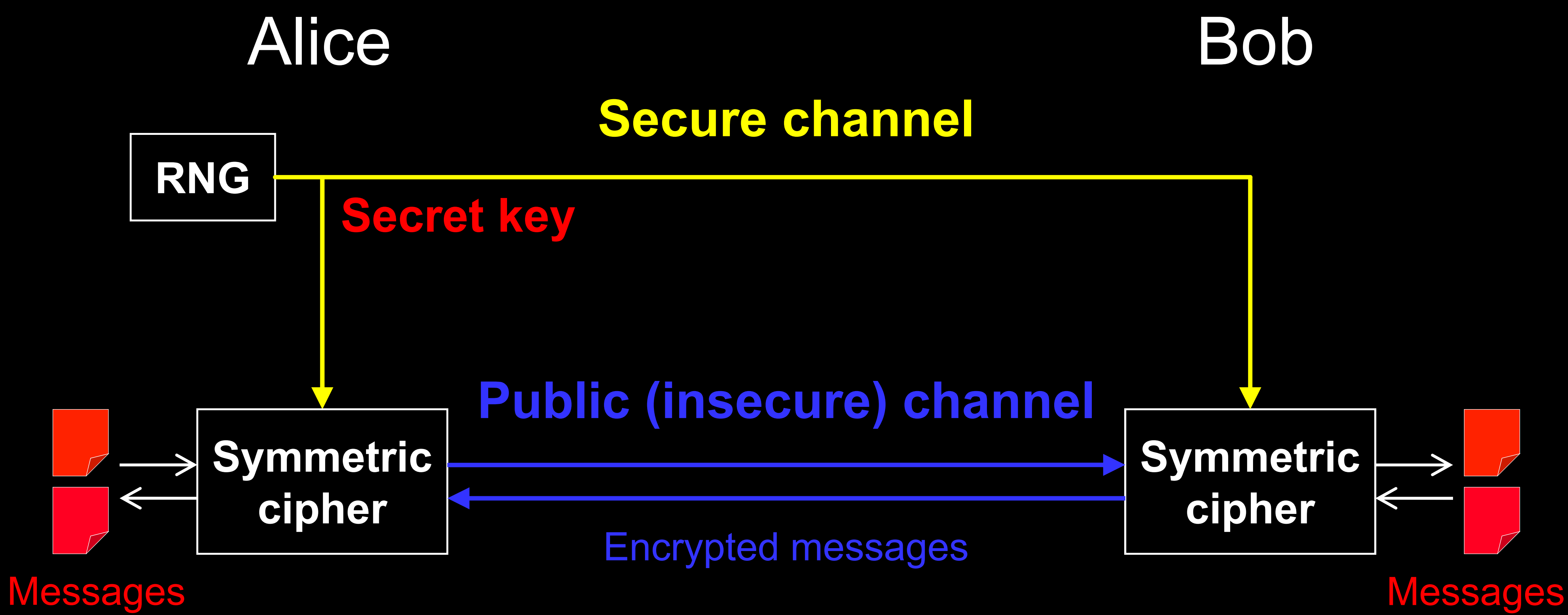


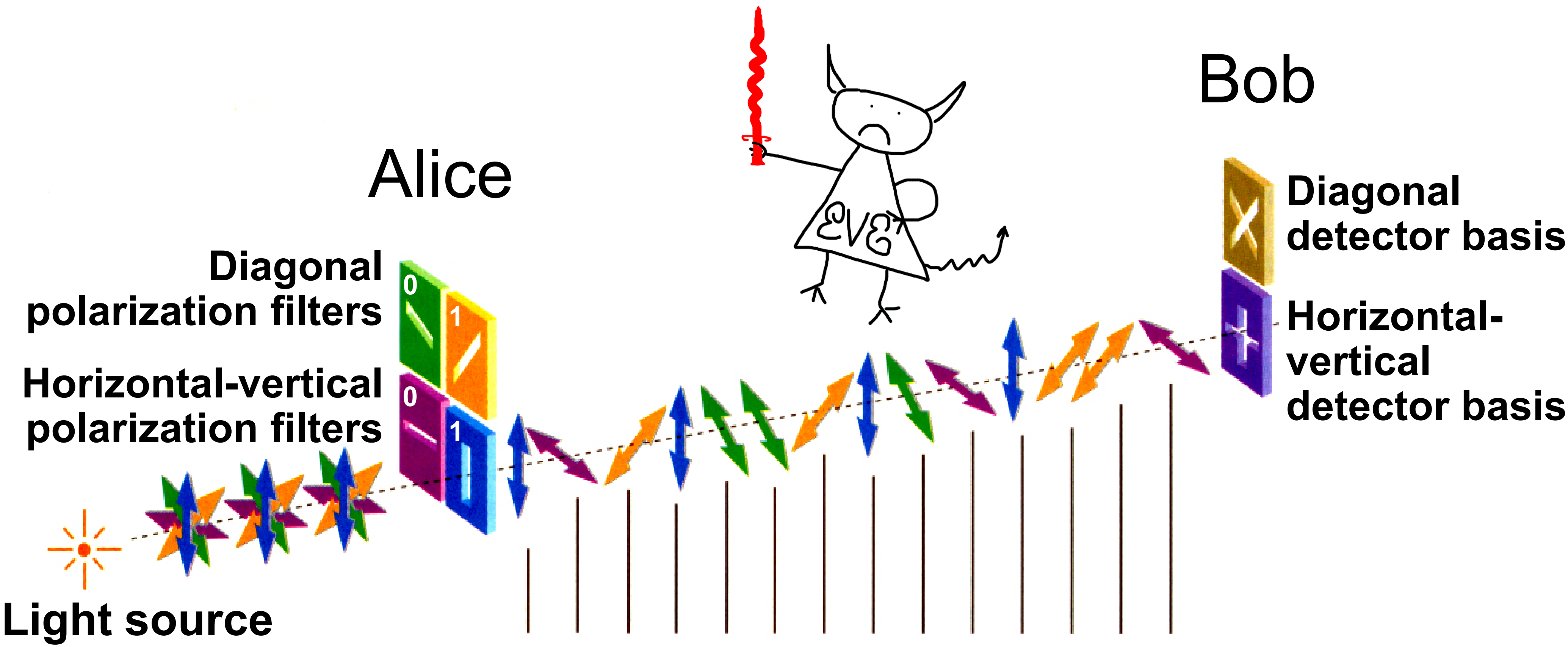
Diagram courtesy M. Mosca

Encryption and key distribution



Quantum key distribution transmits secret key by sending quantum states over *open channel.*

Quantum key distribution (QKD)



Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Bob's detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+
Bob's measurement	1	0	0	1	0	0	1	1	0	0	0	1	0	0
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0

Image reprinted from article: W. Tittel, G. Ribordy & N. Gisin, "Quantum cryptography," Physics World, March 1998

Dealing with errors

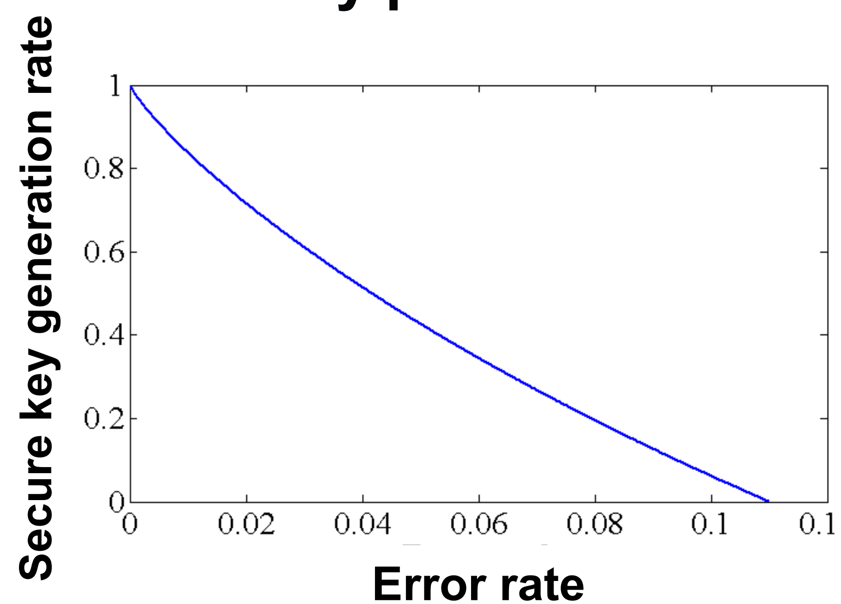
Errors due to imperfections and Eve.
Must assume that all errors are due to Eve!

- **Error correction: standard classical protocols**
- **Privacy amplification:**

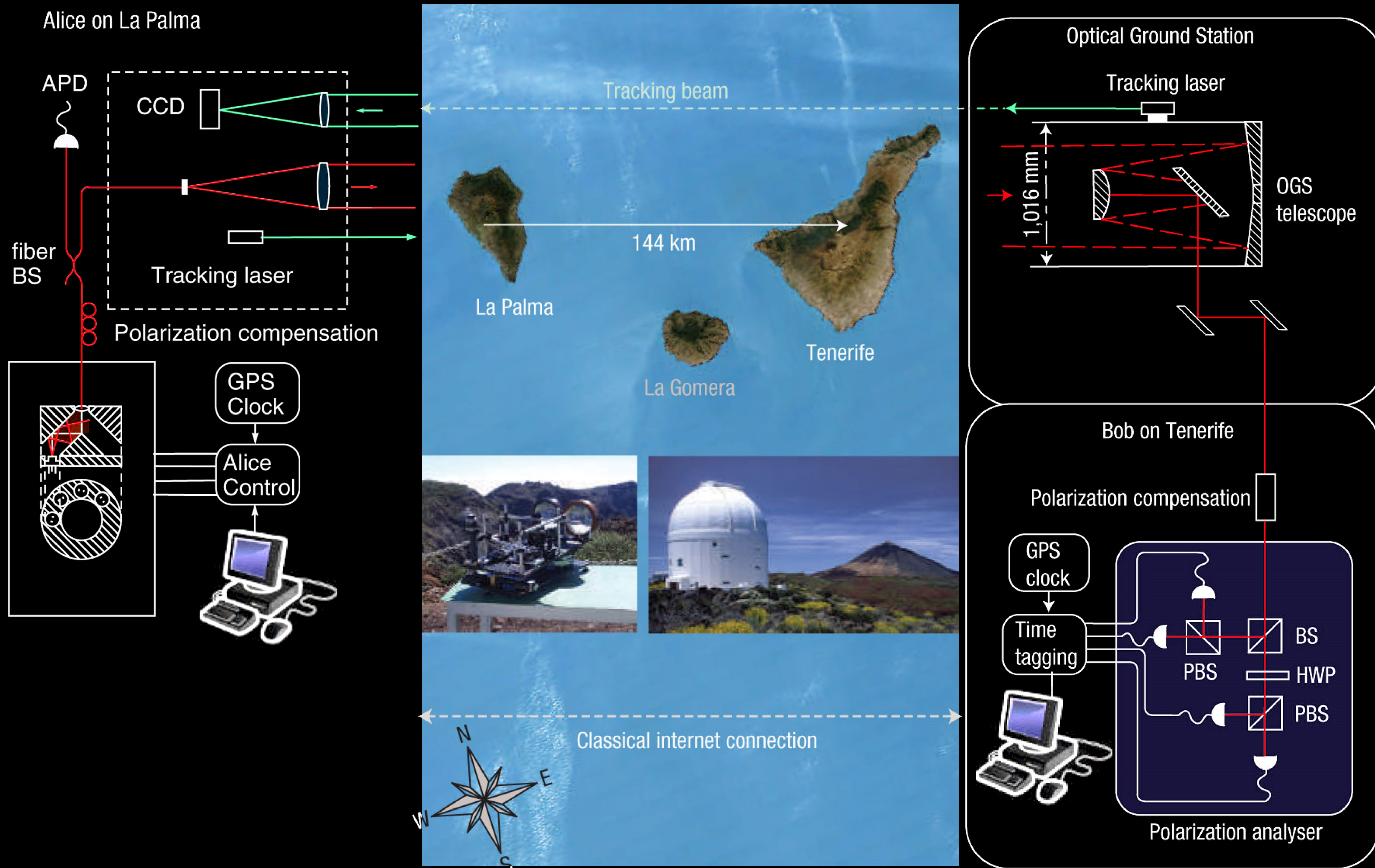
secure key **random matrix** **raw key**

$$\begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Security proof:

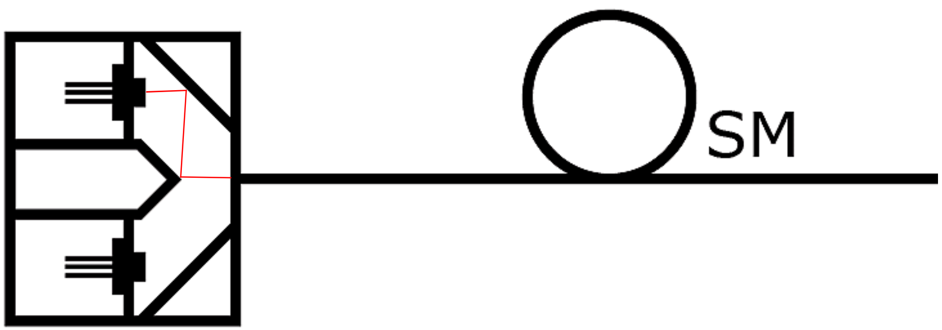


Free-space QKD over 144 km



T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007)

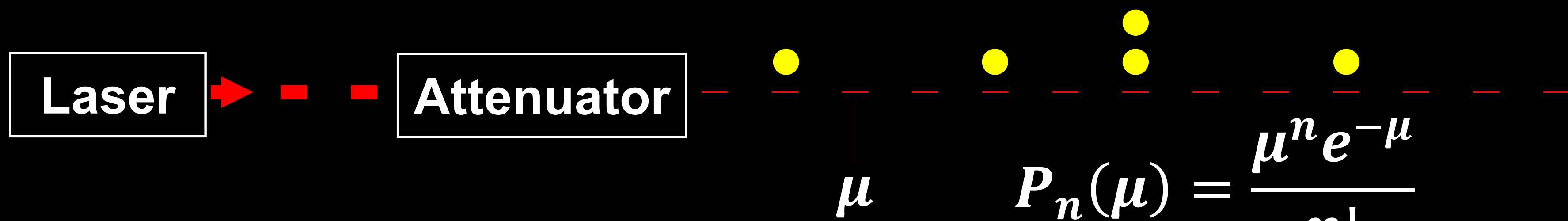
Alice:
Polarized photon source



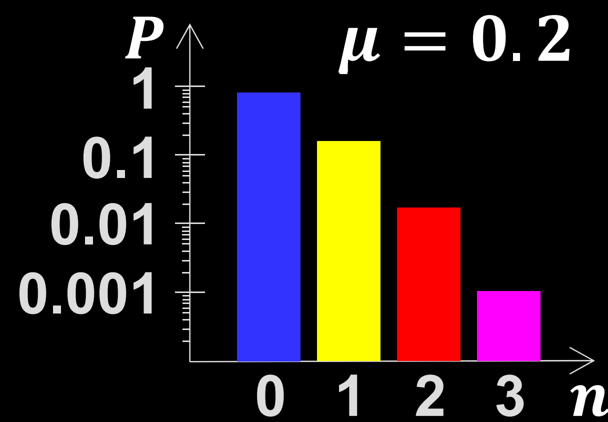
S. Nauerth *et al.,* New J. Phys. **11**, 065001 (2009)

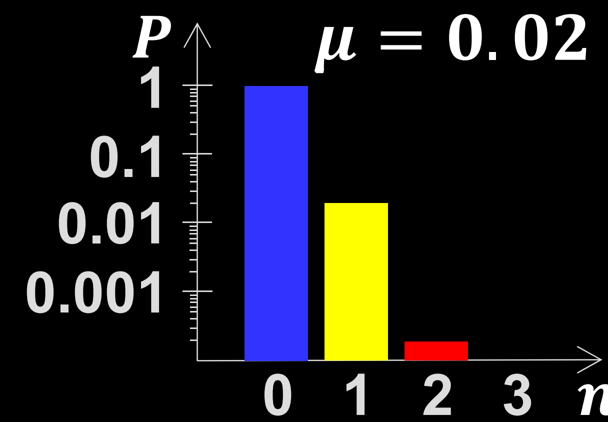
Single-photon sources

Attenuated laser

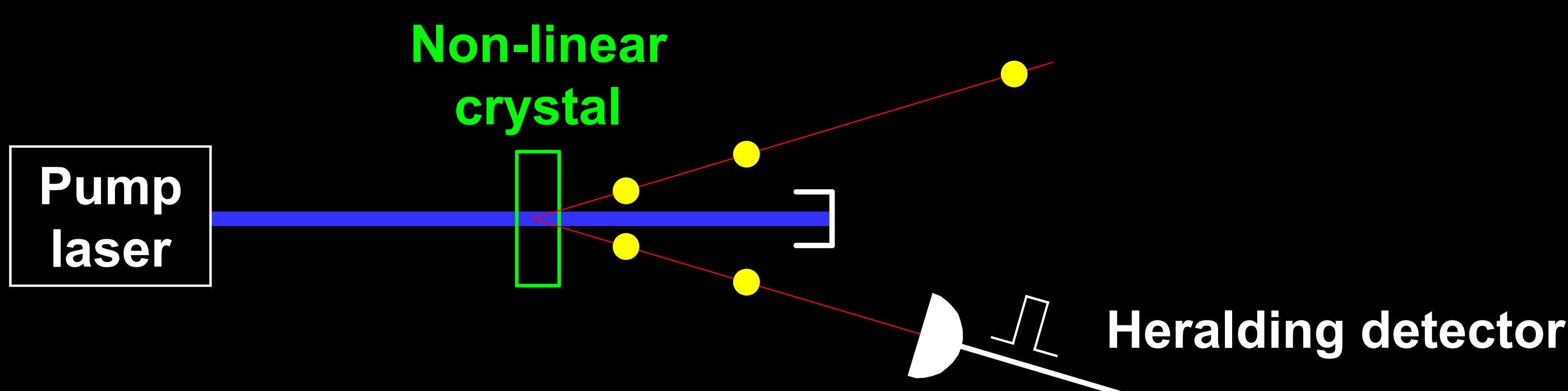


$$P_n(\mu) = \frac{\mu^n e^{-\mu}}{n!}$$

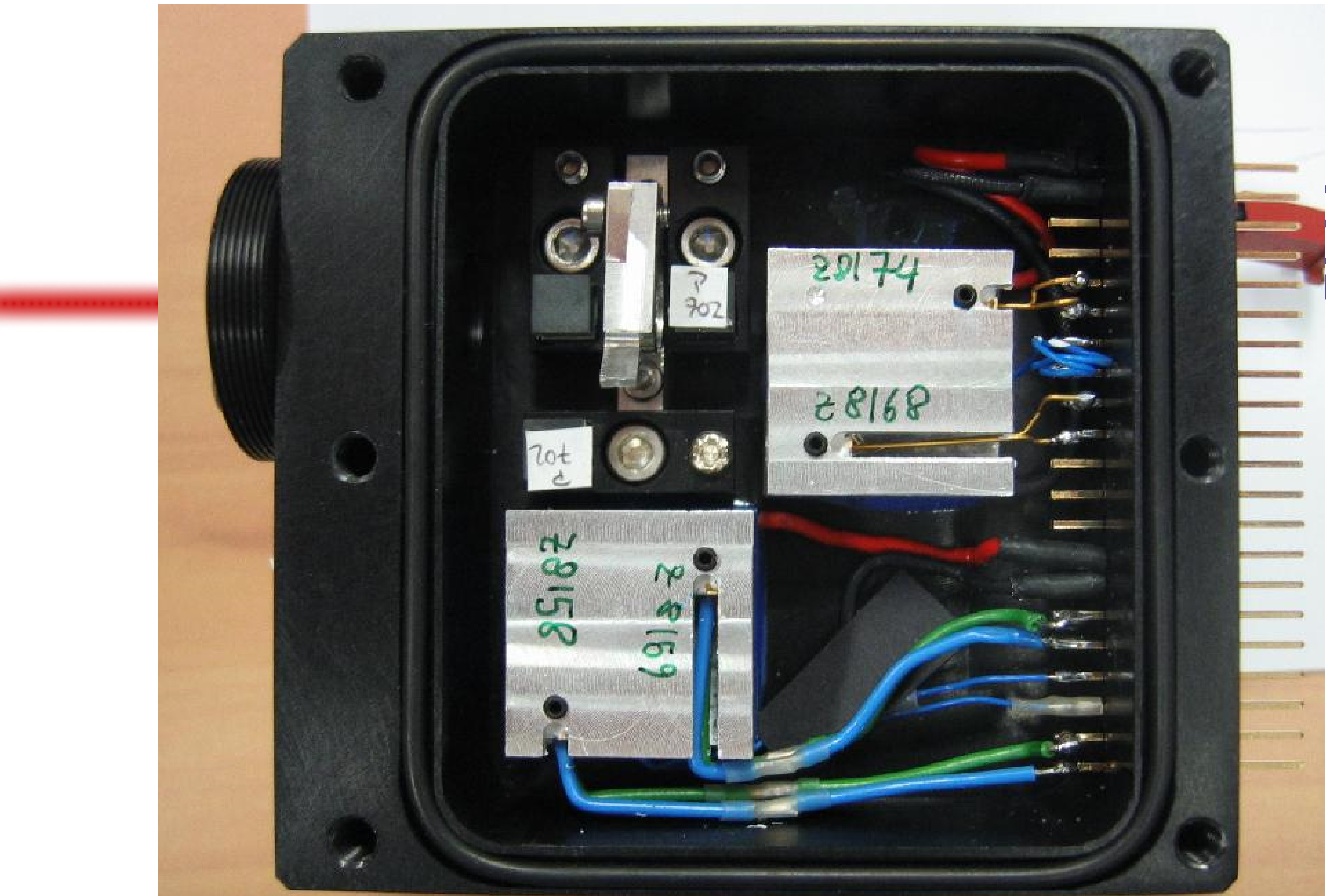




Parametric down-conversion



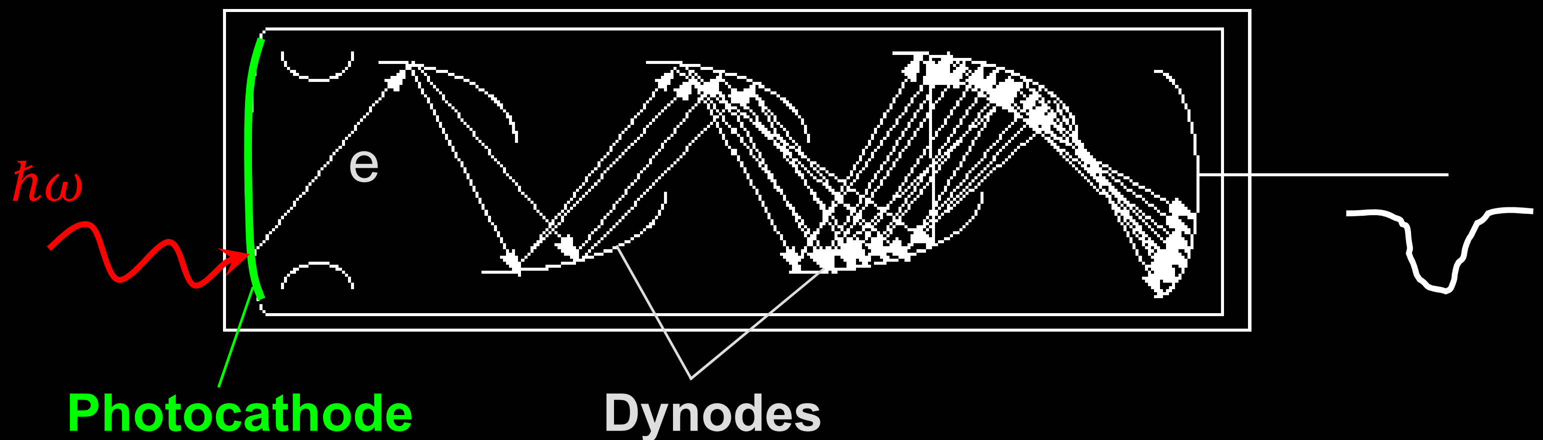
Bob:
Polarization analyzer with single-photon detectors



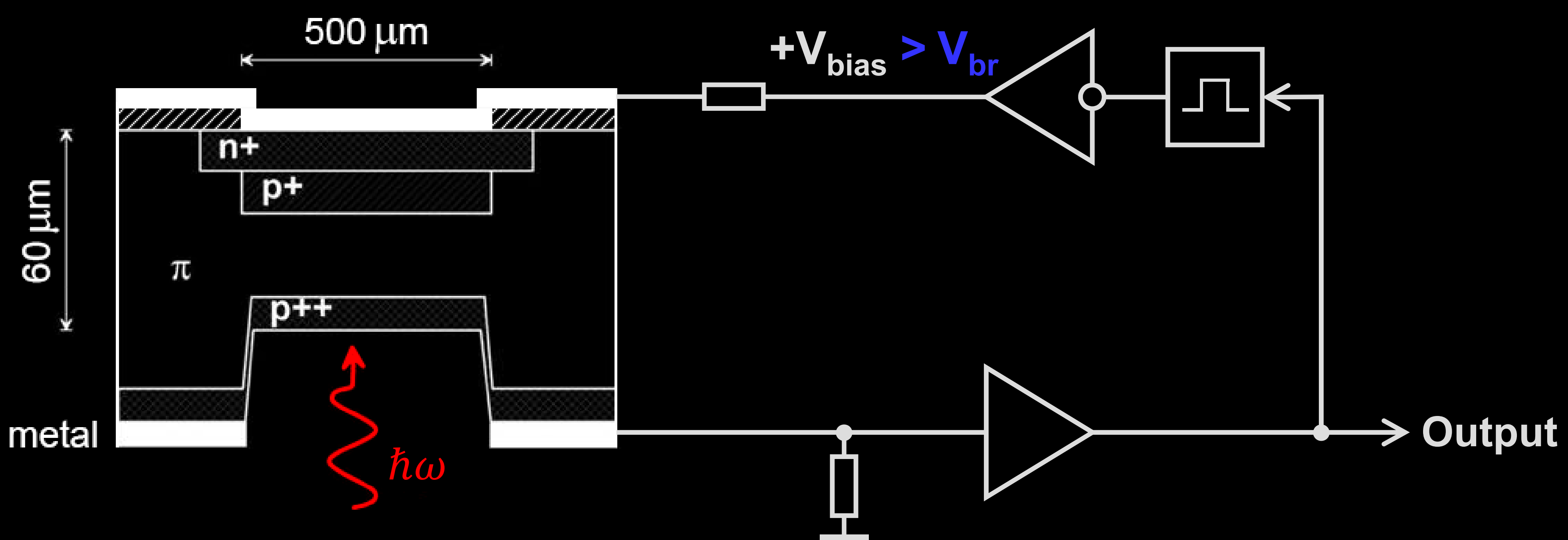
J. G. Rarity, P. C. M. Owens, P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994)

Single-photon detectors

Photomultiplier tube

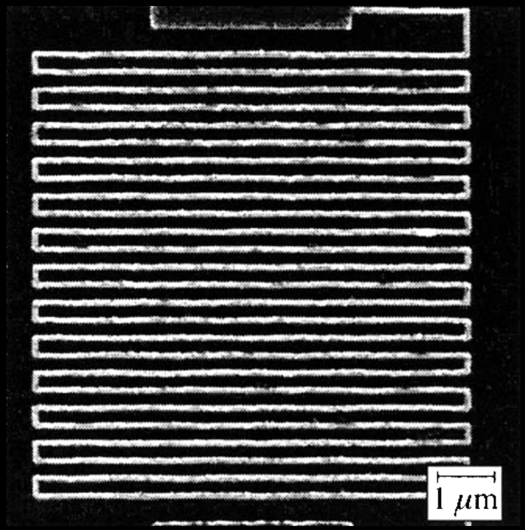


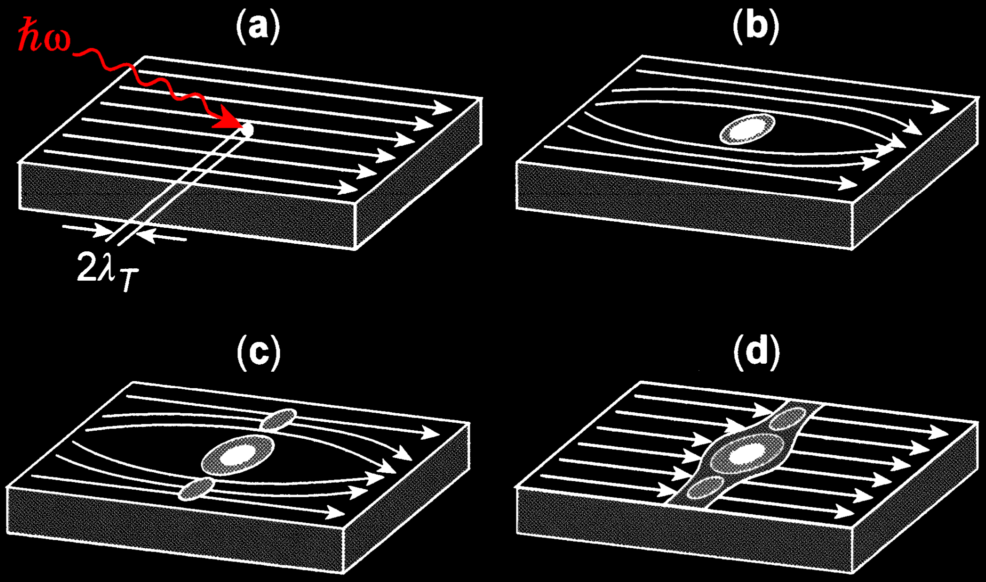
Avalanche photodiode



Single-photon detectors

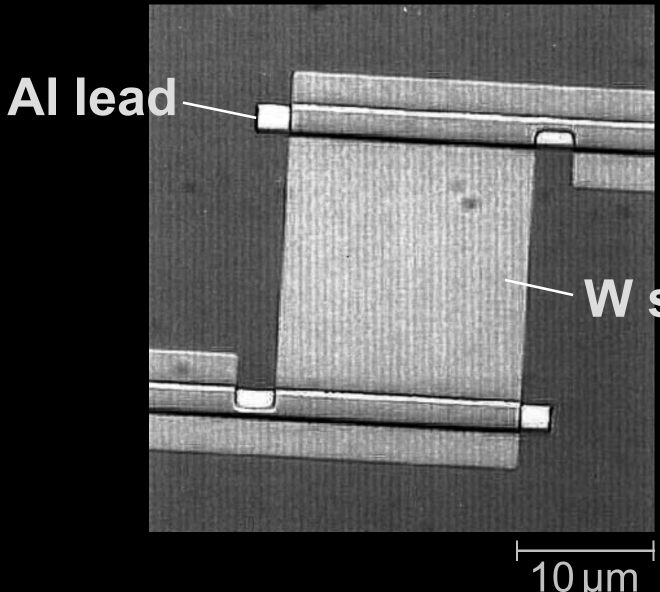
Superconducting nanowire

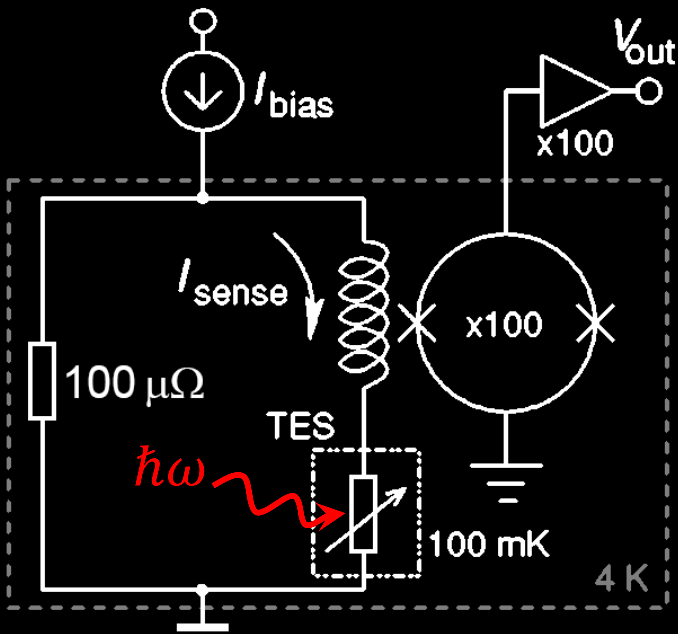




Images reprinted from: R. Sobolewski *et al.*, IEEE Trans. Appl. Supercond. **13**, 1151 (2003)

Transition-edge sensor





Images reprinted from: B. Cabrera *et al.*, Appl. Phys. Lett. **73**, 735 (1998); A.J. Miller *et al.*, Appl. Phys. Lett. **83**, 791 (2003)

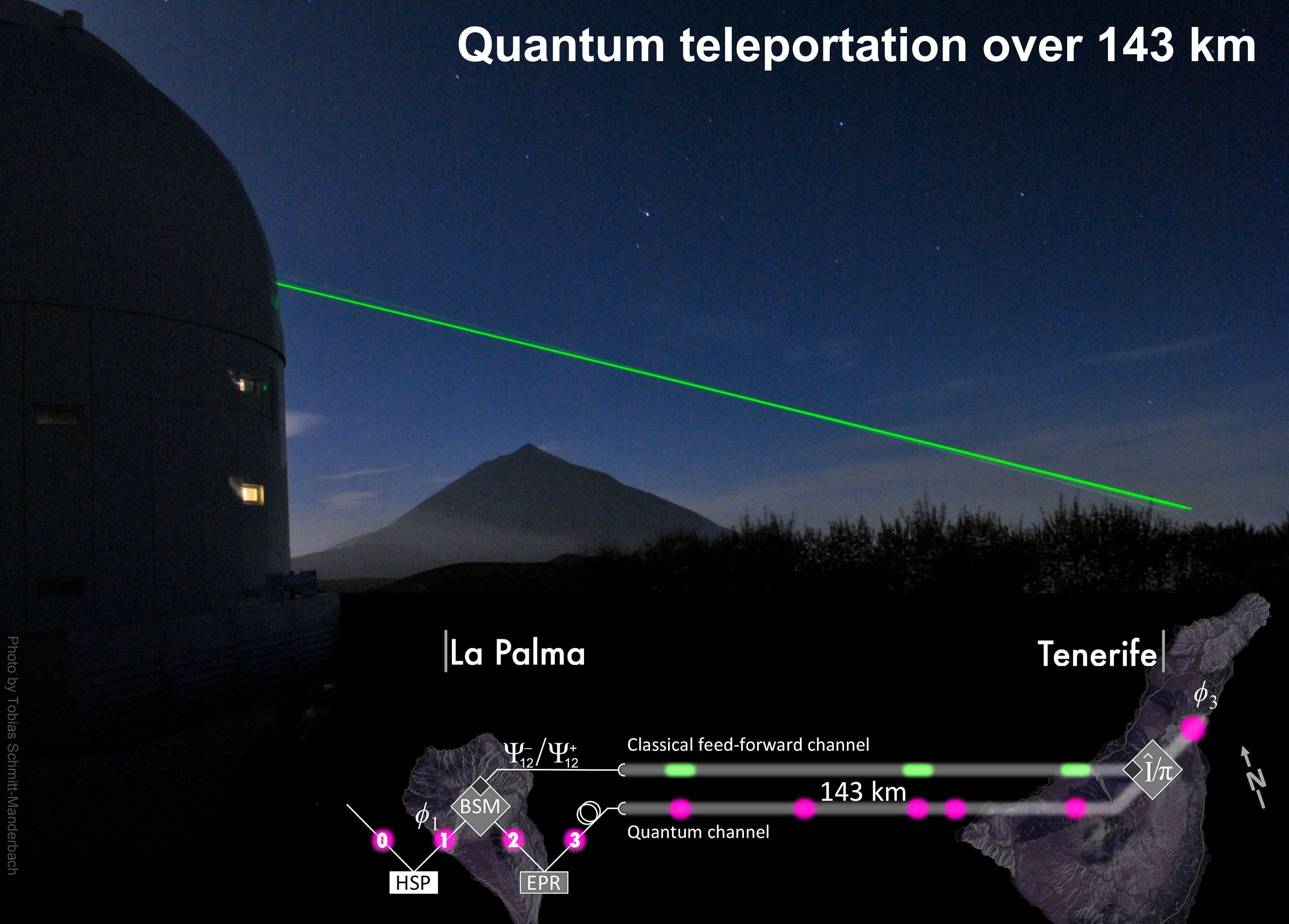
Alice on La Palma

Photo ©IQOQI Vienna

Bob on Tenerife

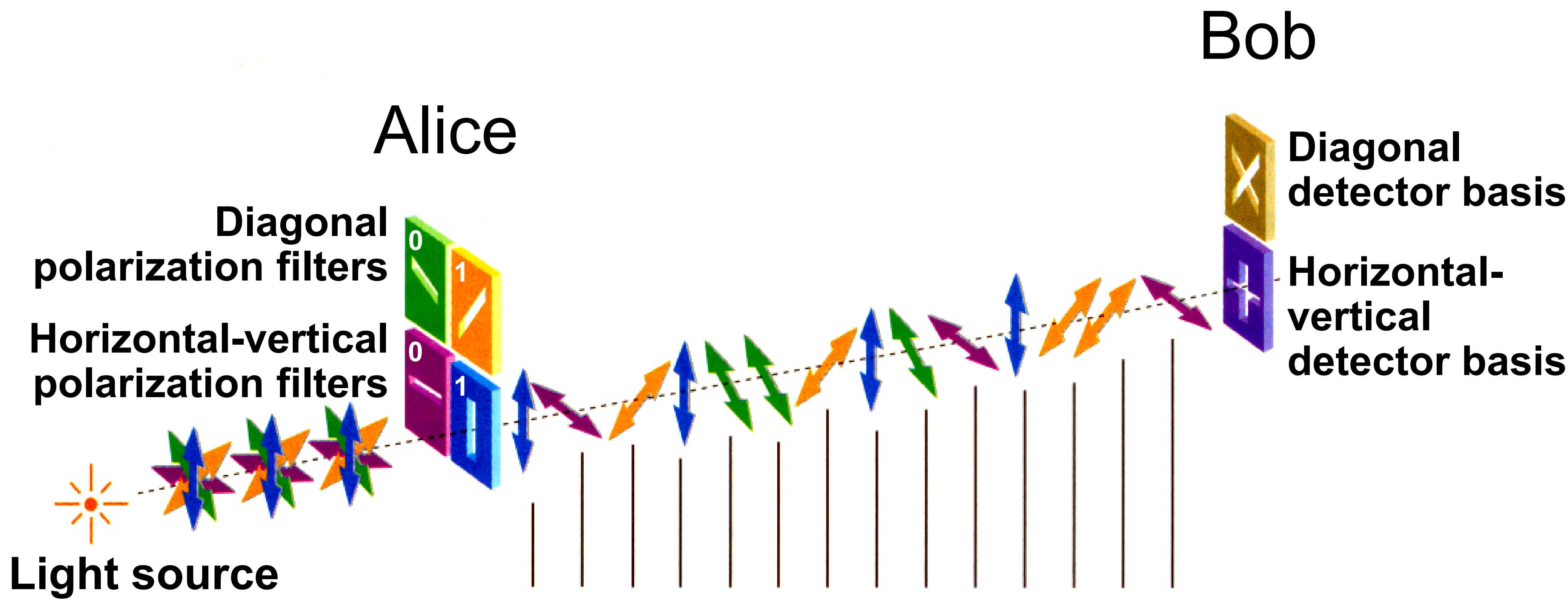
Photo ©IQOQI Vienna

Quantum teleportation over 143 km



X.-S. Ma *et al.*, Nature **489**, 269 (2012)

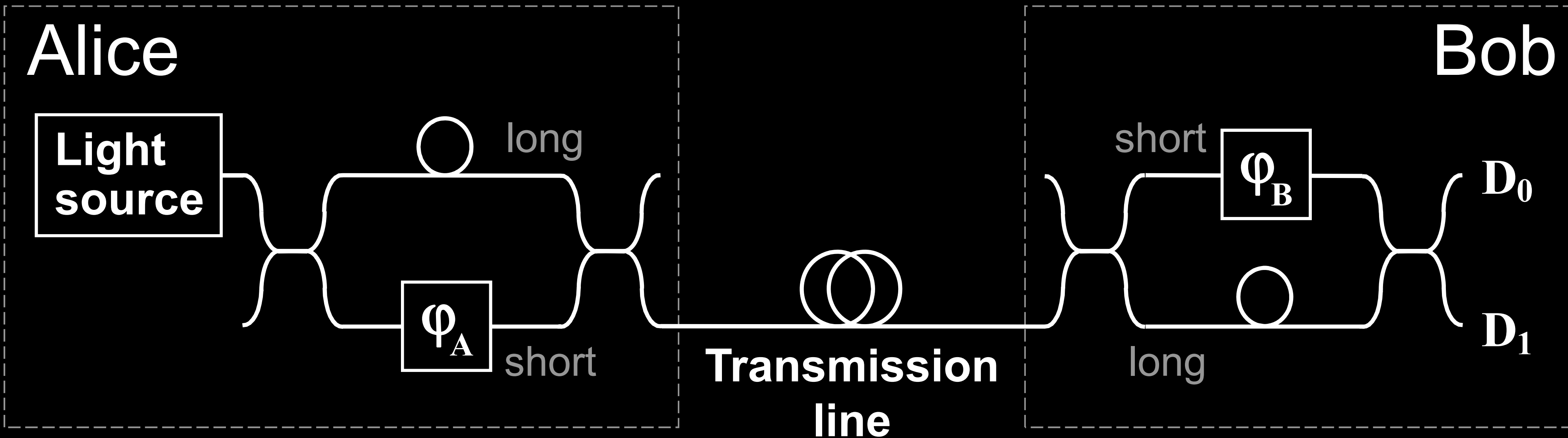
Polarization encoding



Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Bob's detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+
Bob's measurement	1	0	0	1	0	0	1	1	0	0	0	1	0	0
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0

Image reprinted from article: W. Tittel, G. Ribordy & N. Gisin, "Quantum cryptography," Physics World, March 1998

Phase encoding, interferometric QKD channel



$\varphi_A = -45°$ or $+45°$: 0

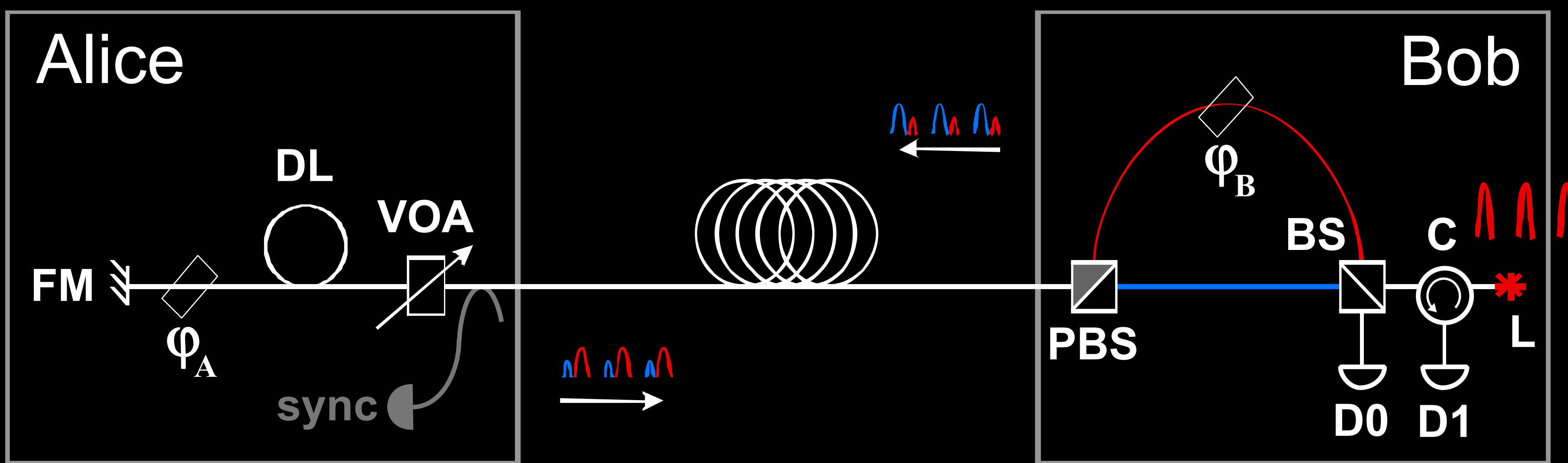
$\varphi_A = +135°$ or $-135°$: 1

Detector bases:

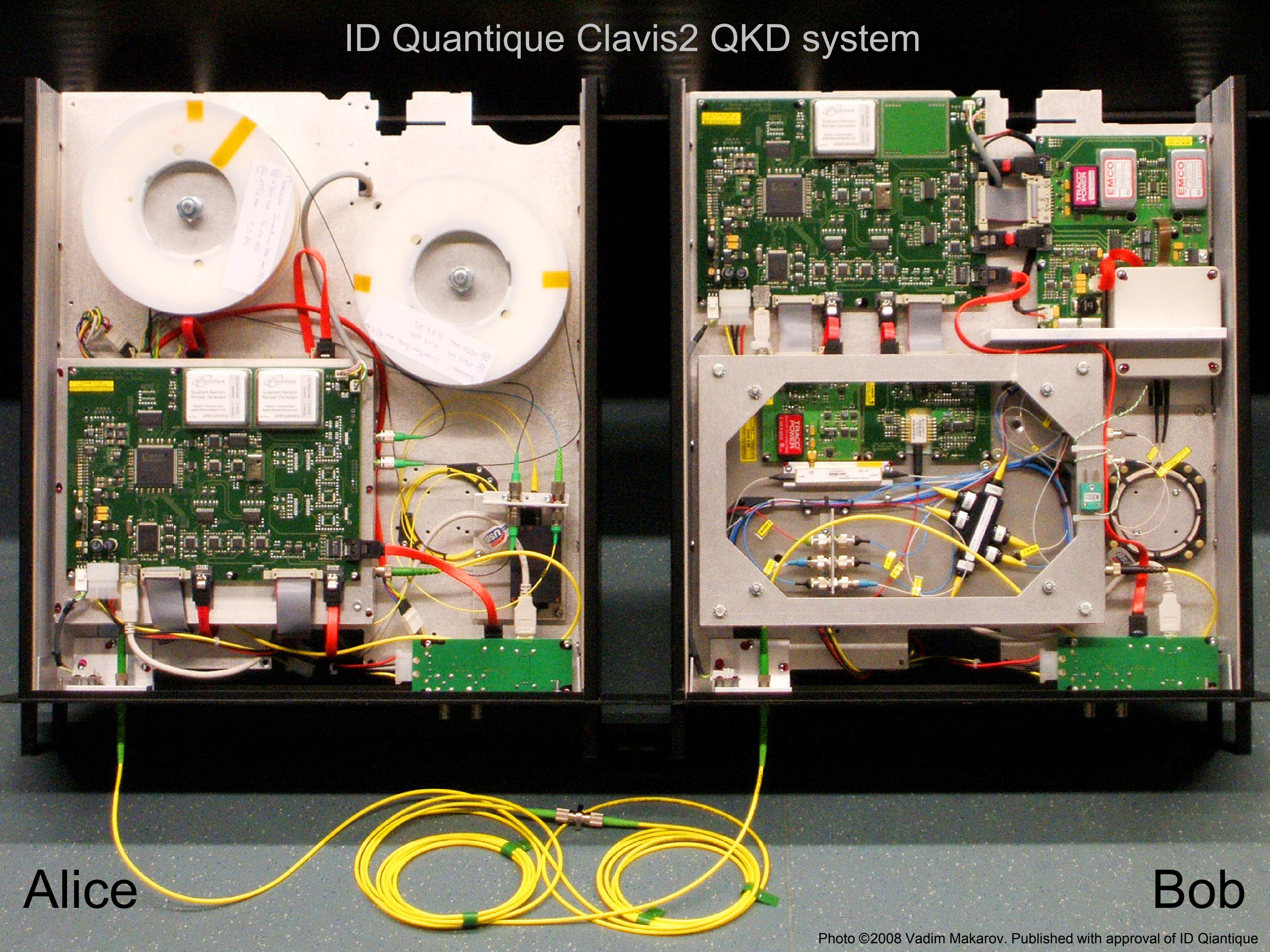
$\varphi_B = -45°$: X

$\varphi_B = +45°$: Z

Plug-and-play scheme



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


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

Commercial QKD

Classical encryptors:

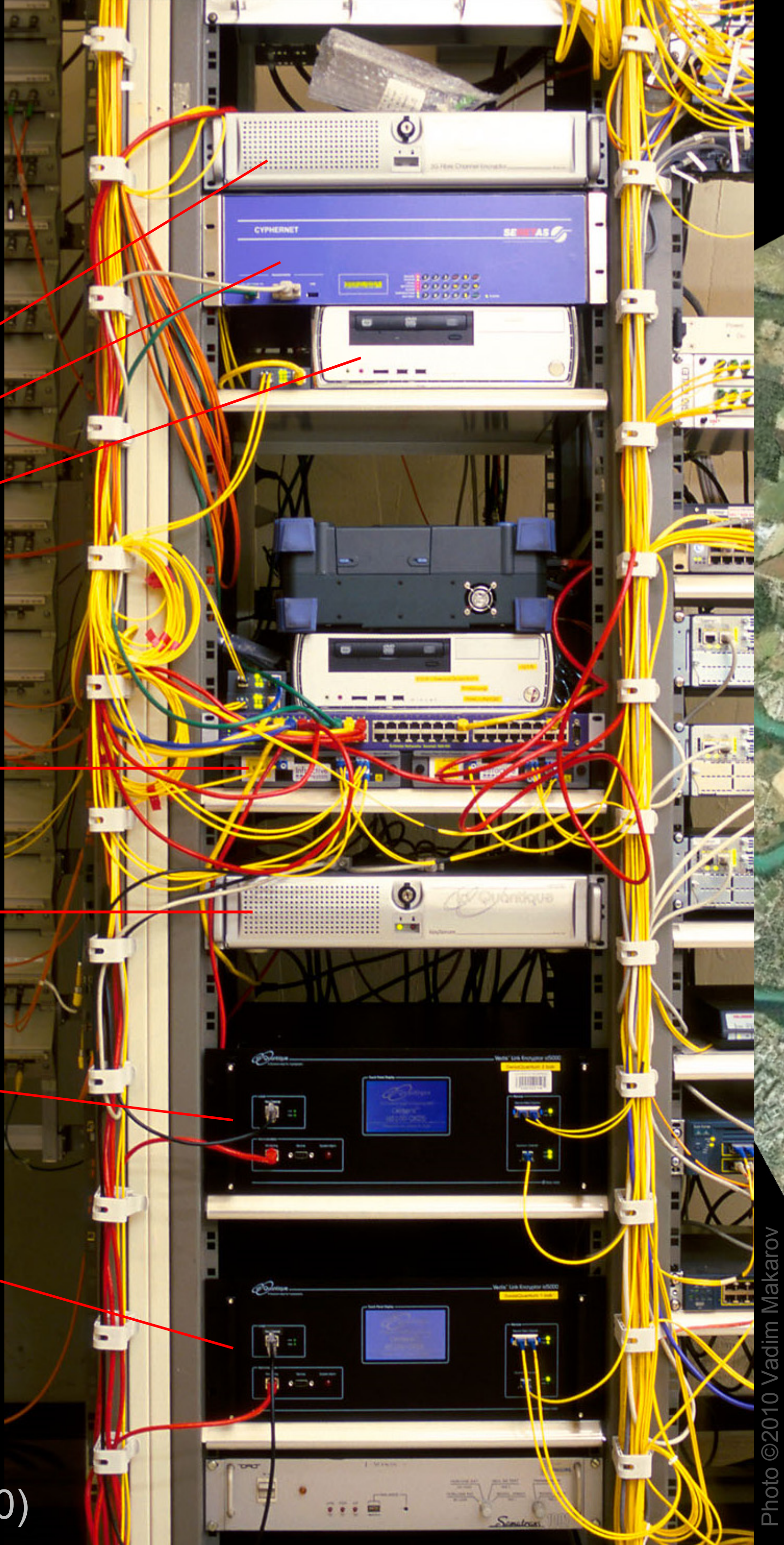
L2, 2 Gbit/s
L2, 10 Gbit/s
L3 VPN, 100 Mbit/s

WDMs

Key manager

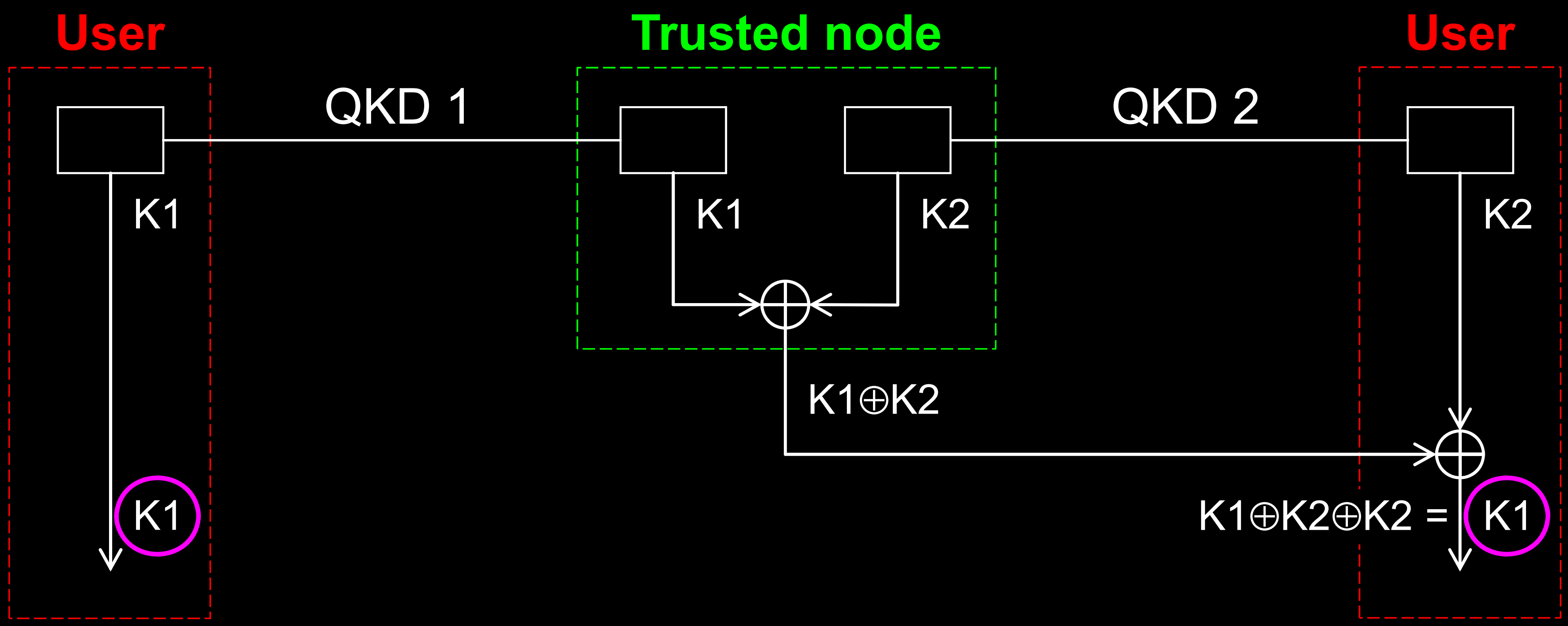
QKD to another node (4 km)

QKD to another node (14 km)

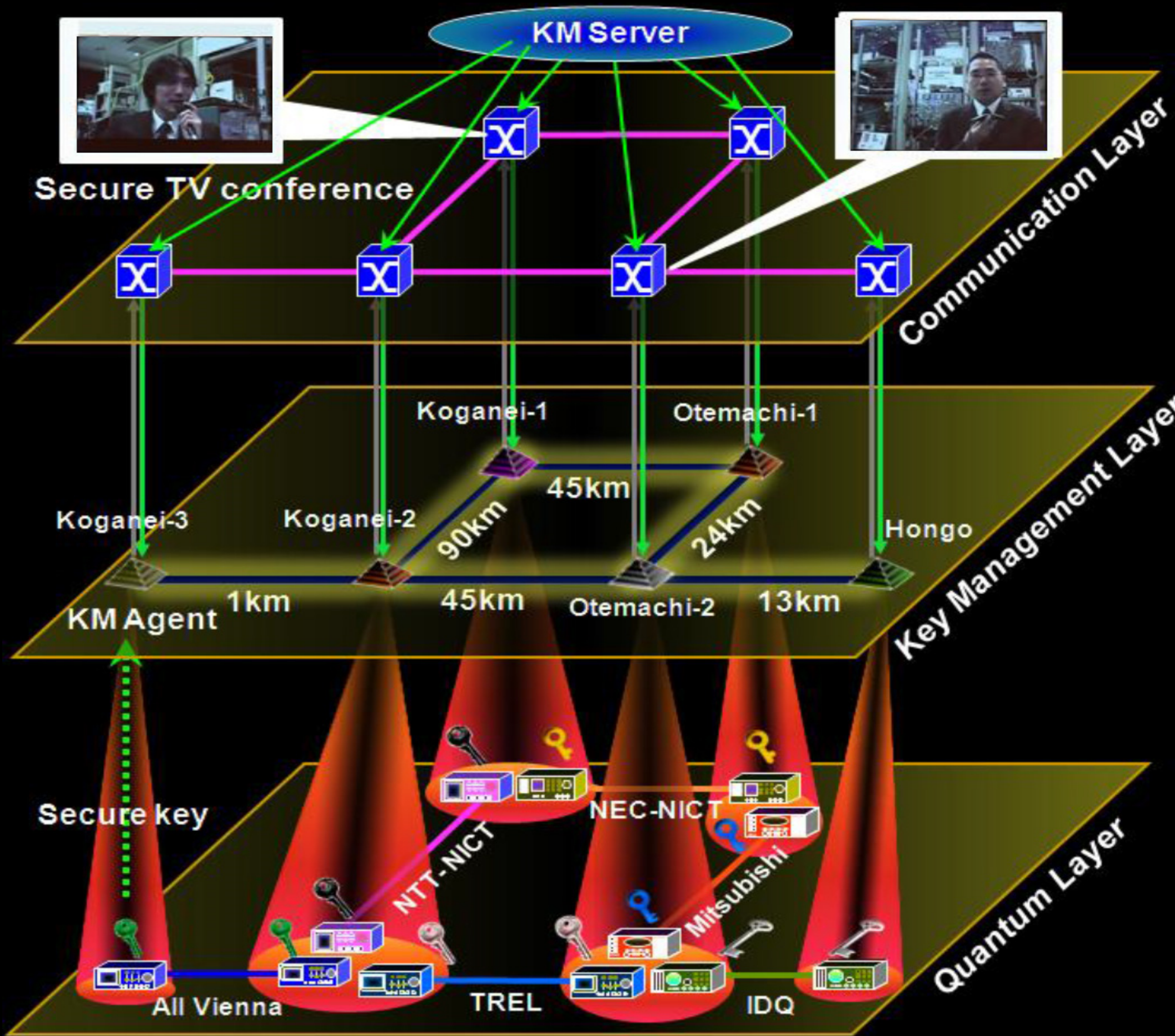


www.swissquantum.com
ID Quantique *Cerberis* system (2010)

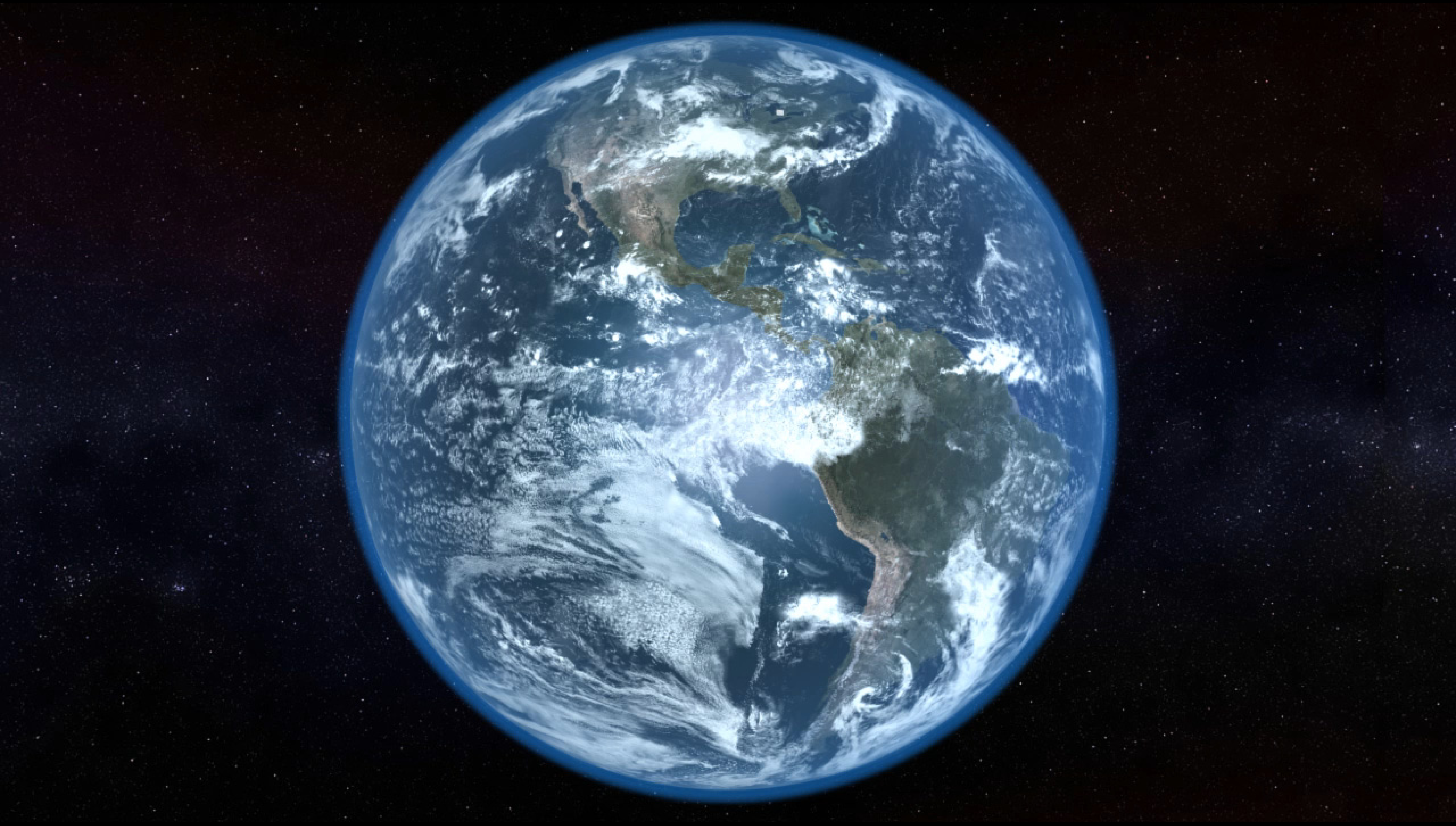
Trusted-node repeater



Trusted-node network



M. Sasaki et al., Opt. Express **19**, 10387 (2011)



Video ©2012 IQC / group of T. Jennewein

Prototype single-photon detector (4-channel)

Photo ©2014 V. Makarov / IQC

End of lecture 1

Quantum hacking

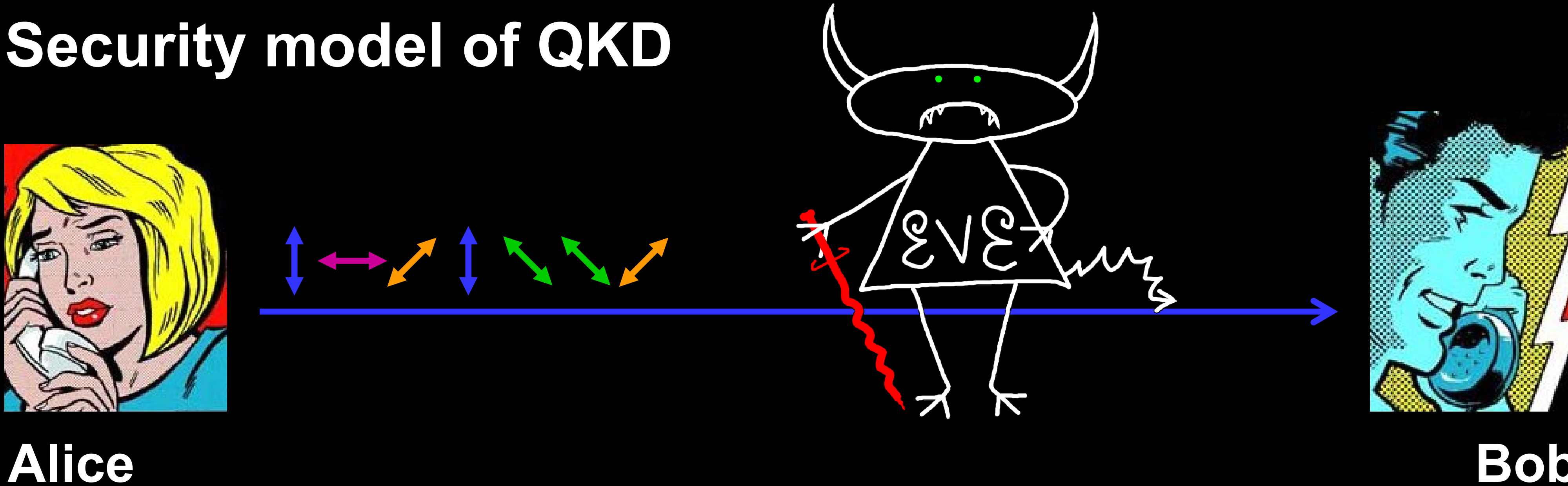
Vadim Makarov

IQC Institute for Quantum Computing

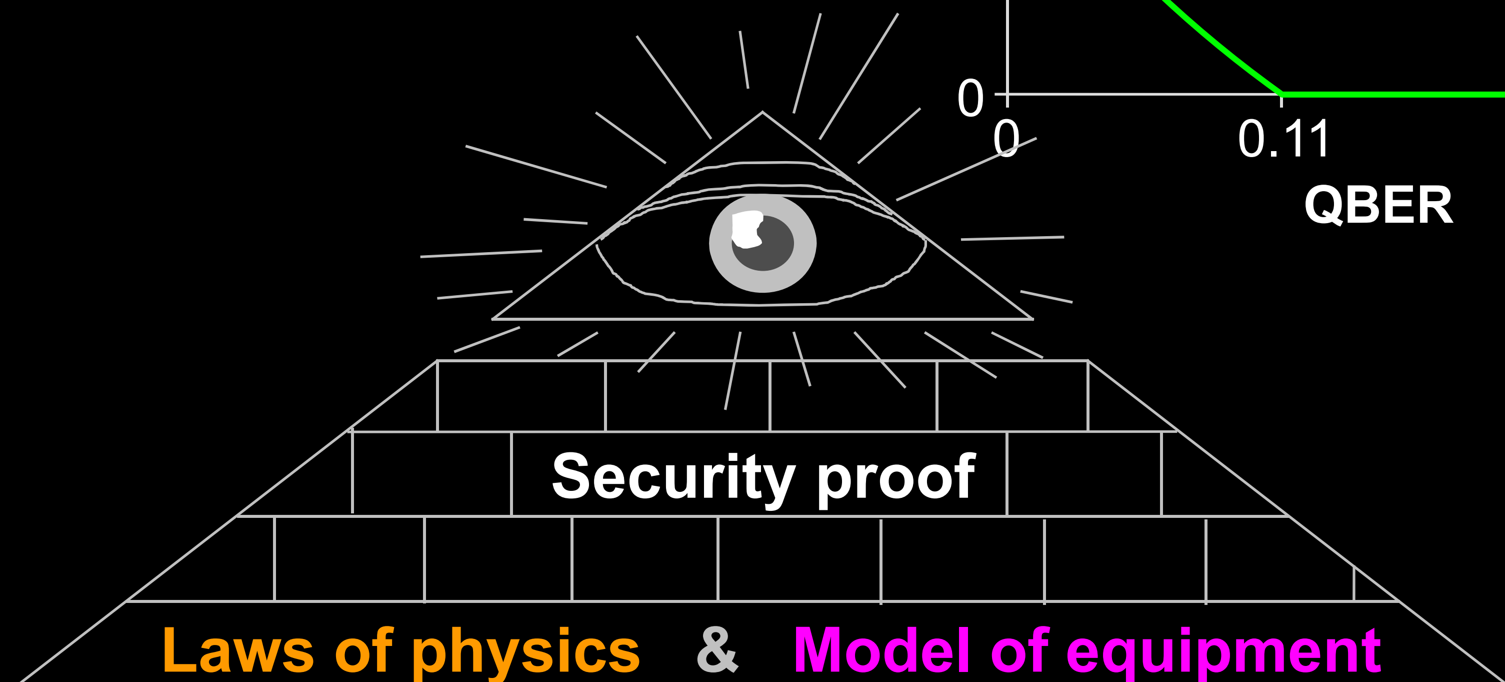
www.vad1.com/lab

Photo ©2010 NTNU Info / Geir Mogen

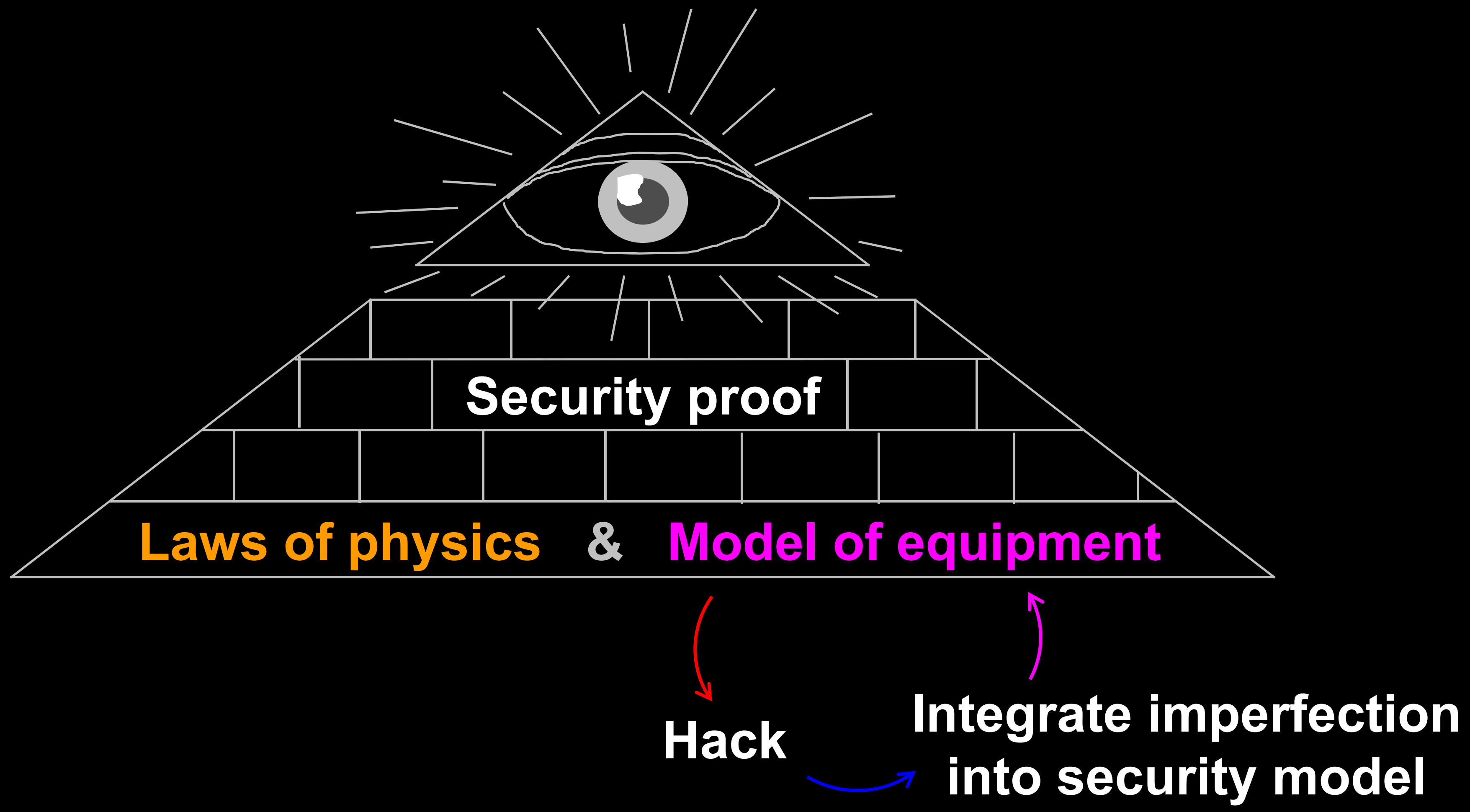
Security model of QKD



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



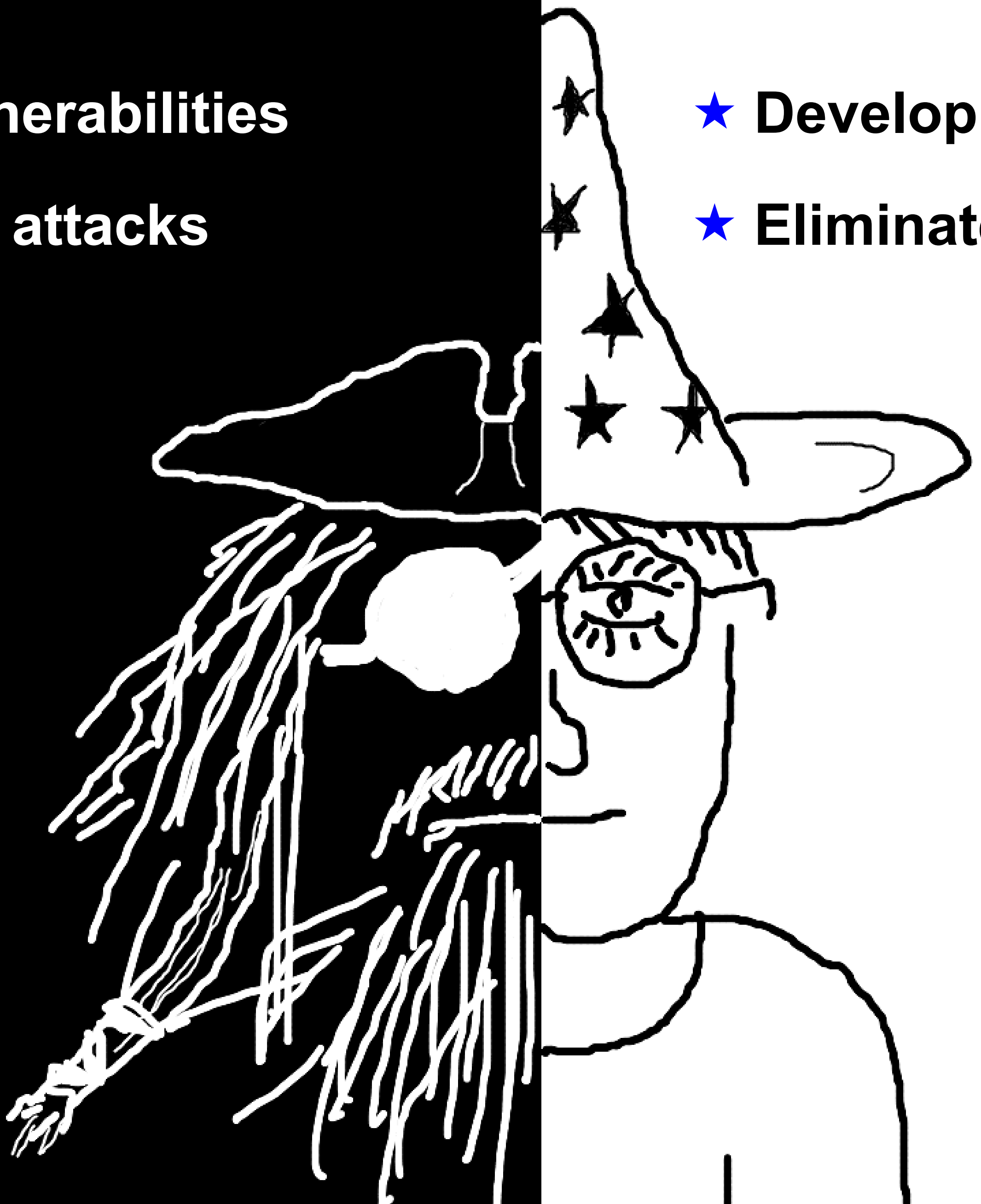
Security model of QKD



Quantum hacking

- Discover vulnerabilities
- Demonstrate attacks

- Develop countermeasures
- Eliminate imperfections




1 2
3 4
5 6
7 8
9 0
* #

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)

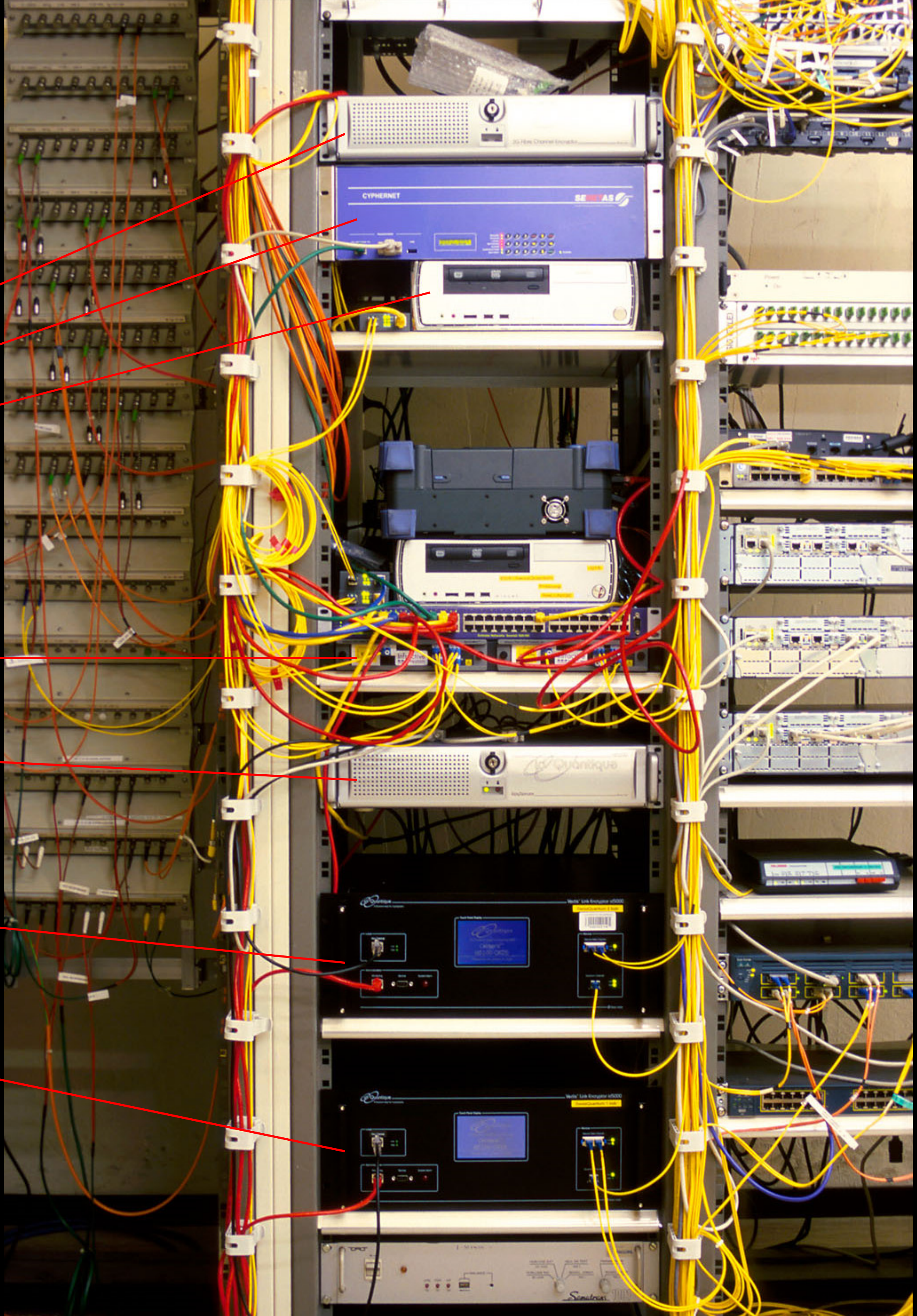
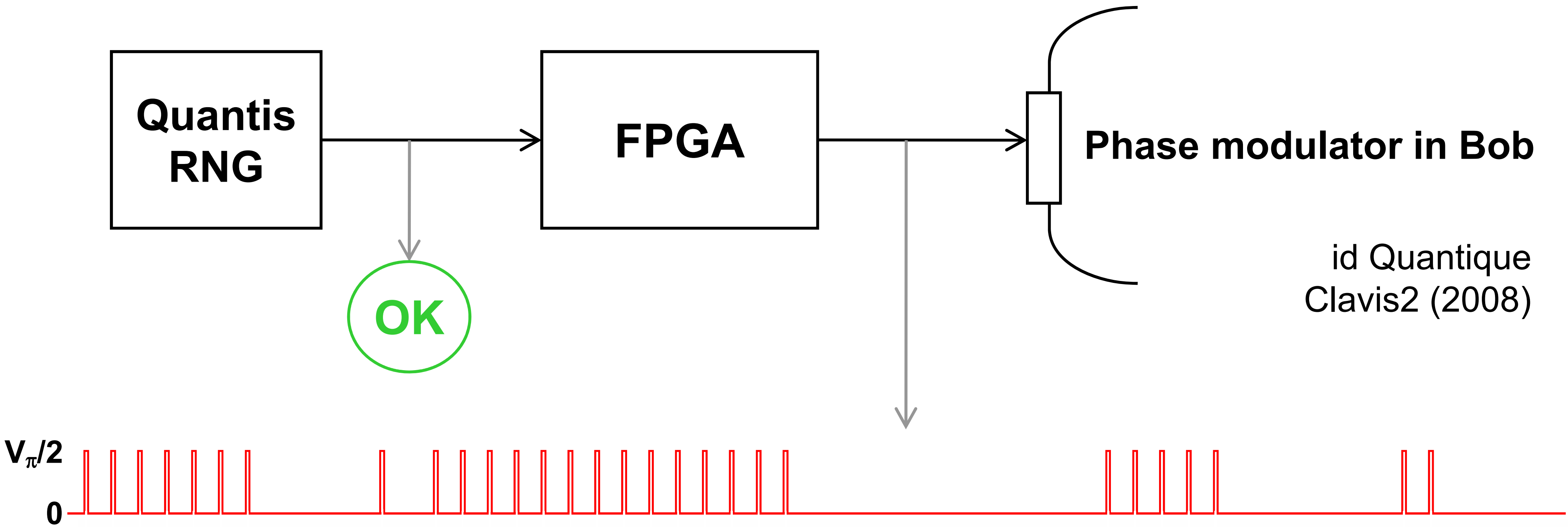


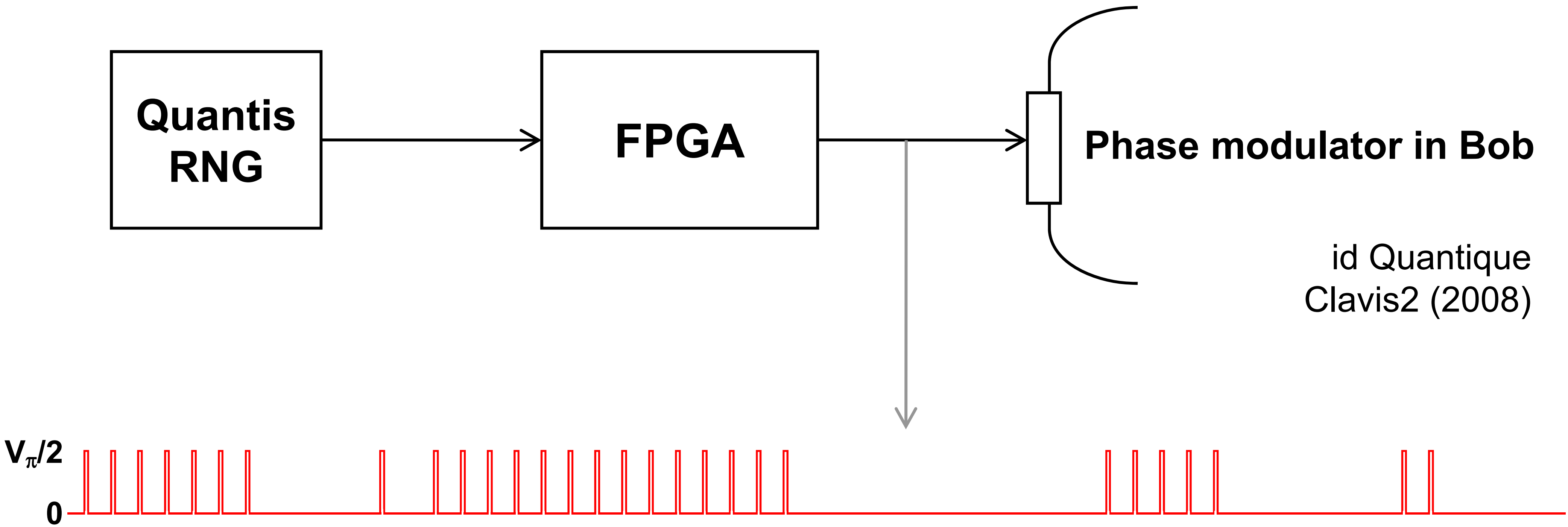
Photo ©2010 Vadim Makarov

www.swissquantum.com

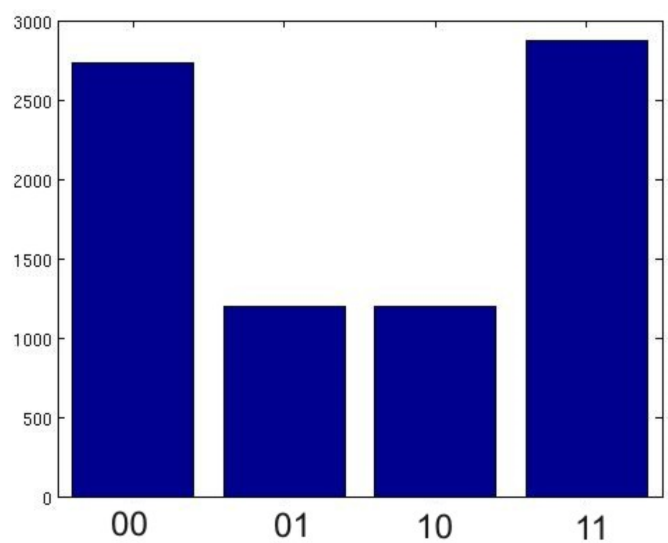
True randomness?



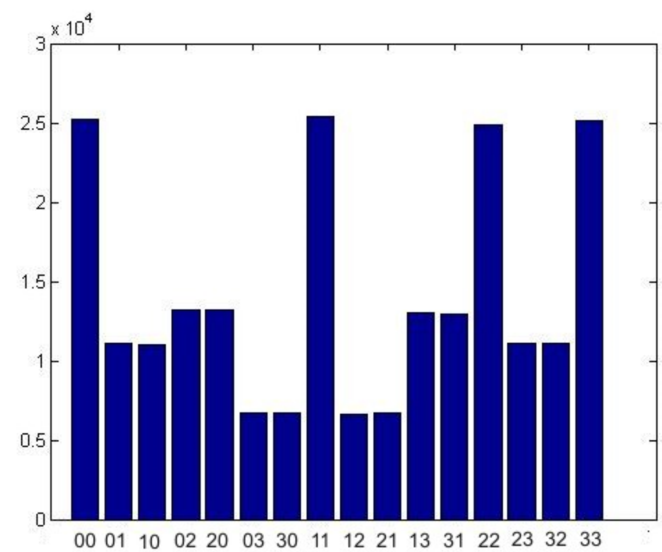
True randomness?



Bob:

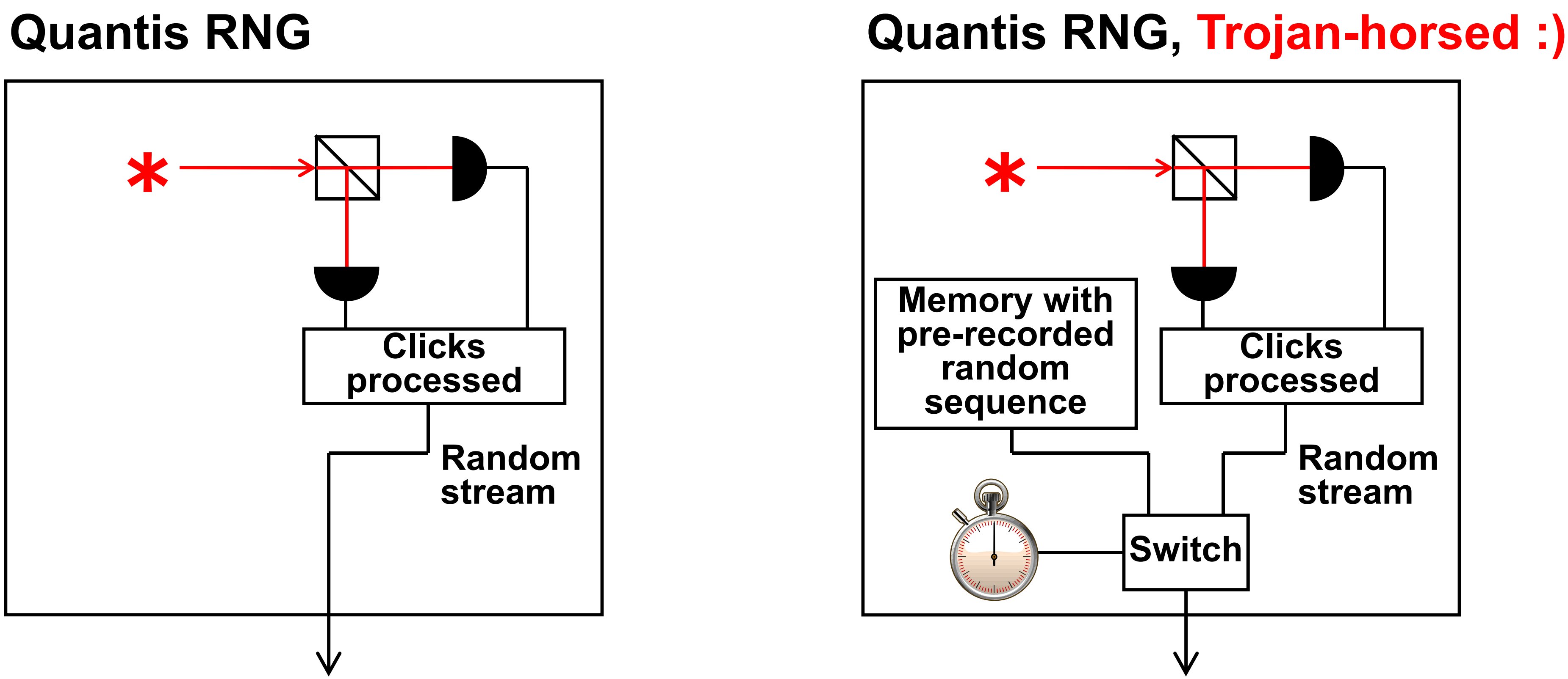


Alice:



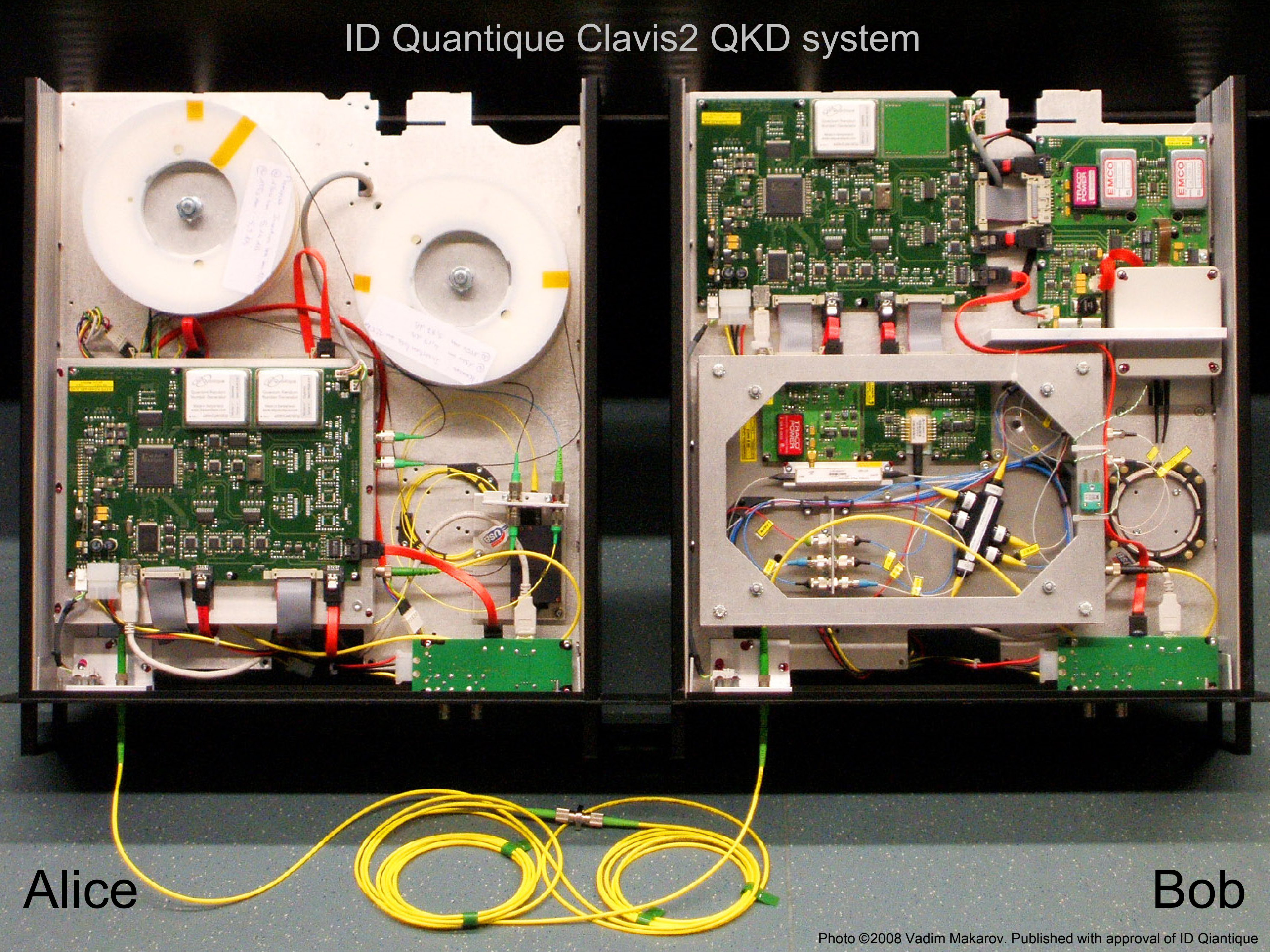
Issue reported patched, as of January 2010

Do we trust the manufacturer?

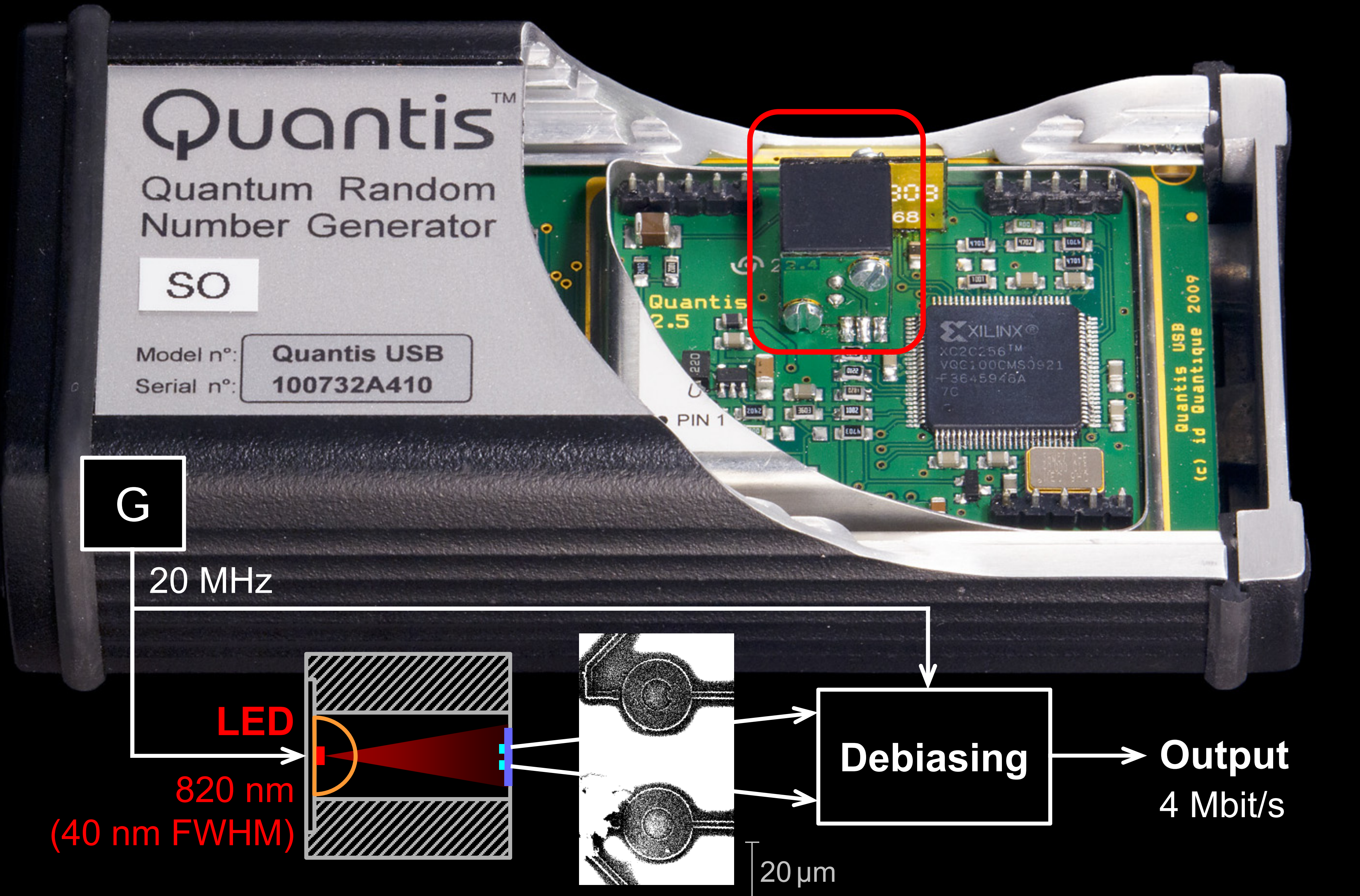


Many components in QKD system can be Trojan-horsed:

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


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

Quantis RNG: what's inside?



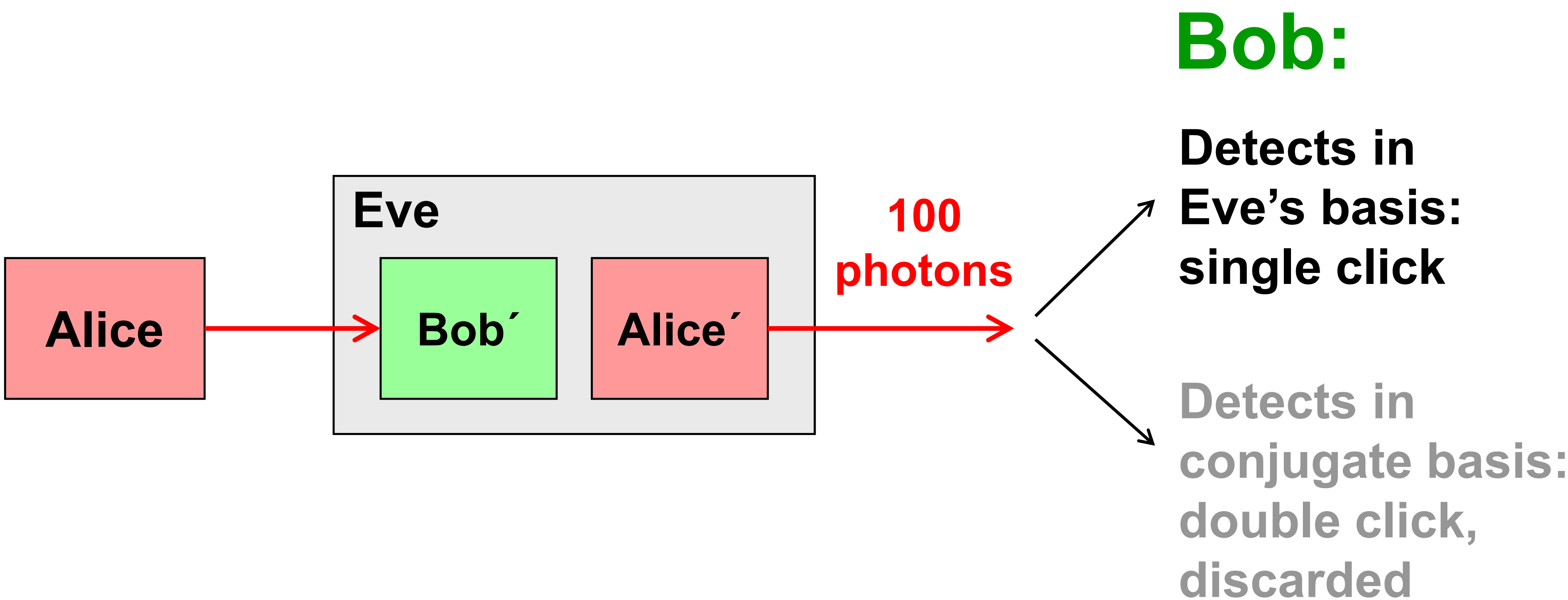
G. Ribordy, O. Guinnard, US patent appl. US 2007/0127718 A1 (filed in 2006)
I. Radchenko *et al.*, unpublished

Double clicks

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

Discard them?

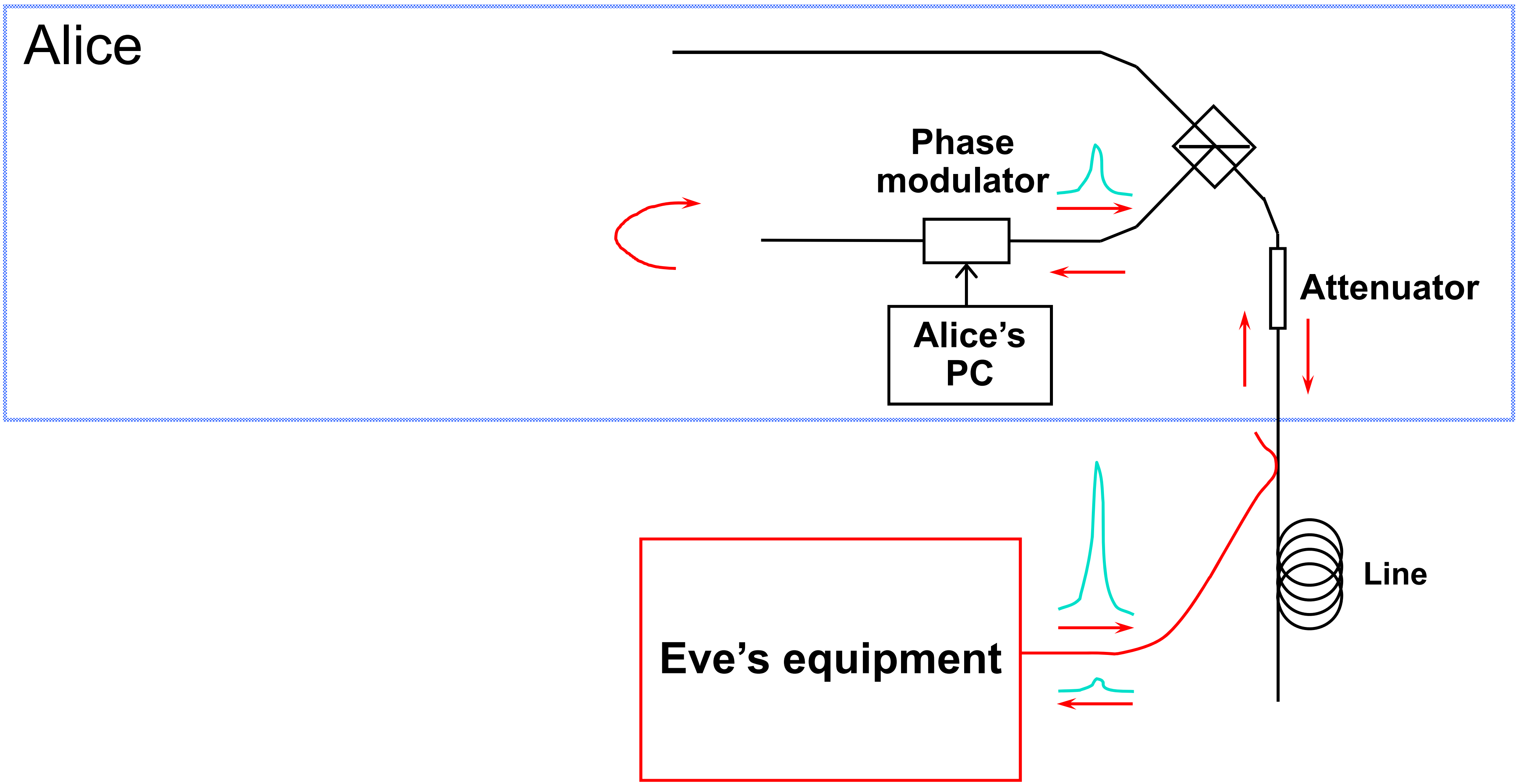
Intercept-resend attack... with a twist:



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

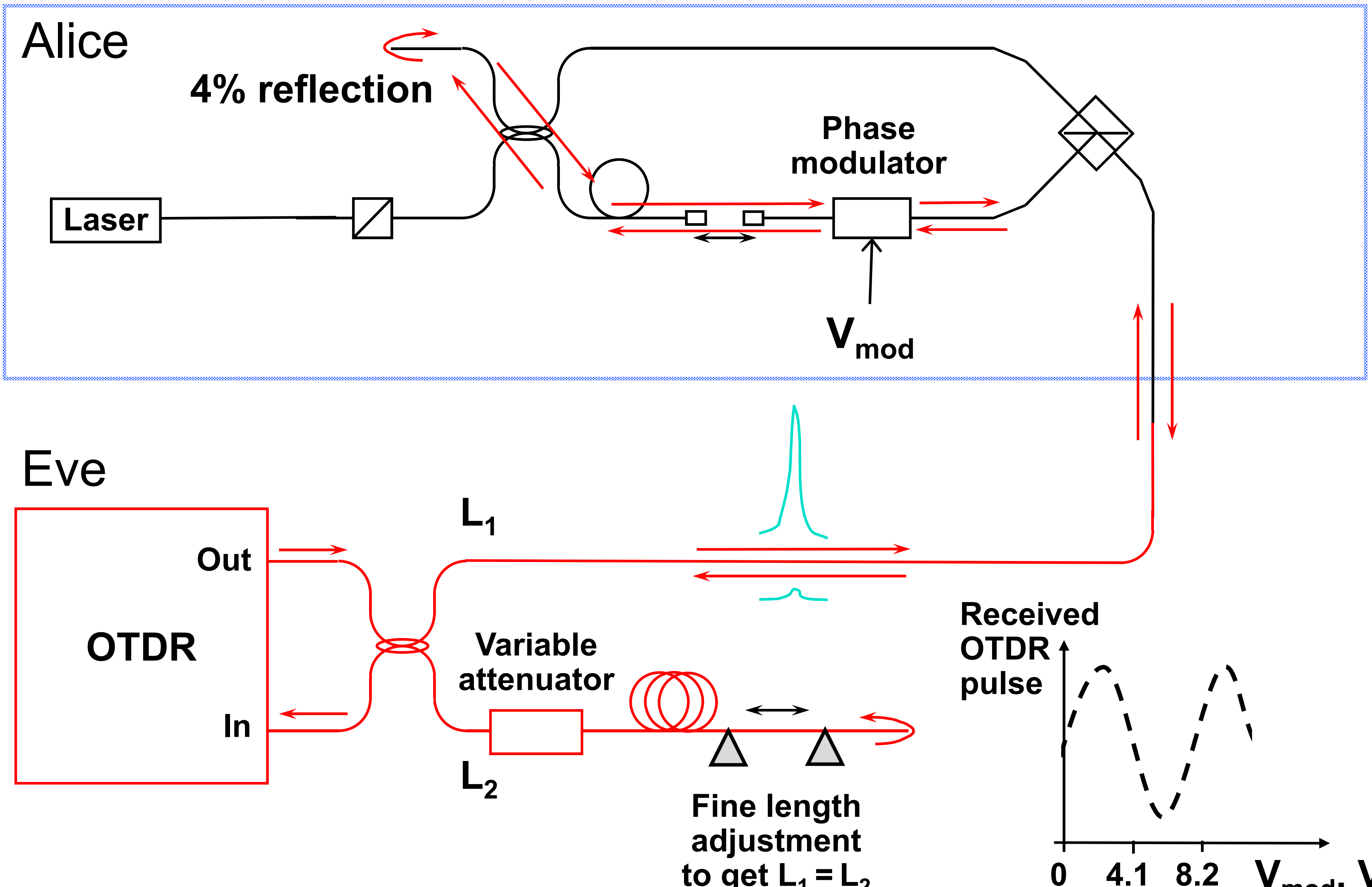
N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999)
T. Tsurumaru & K. Tamaki, Phys. Rev. A **78**, 032302 (2008)

Trojan-horse attack

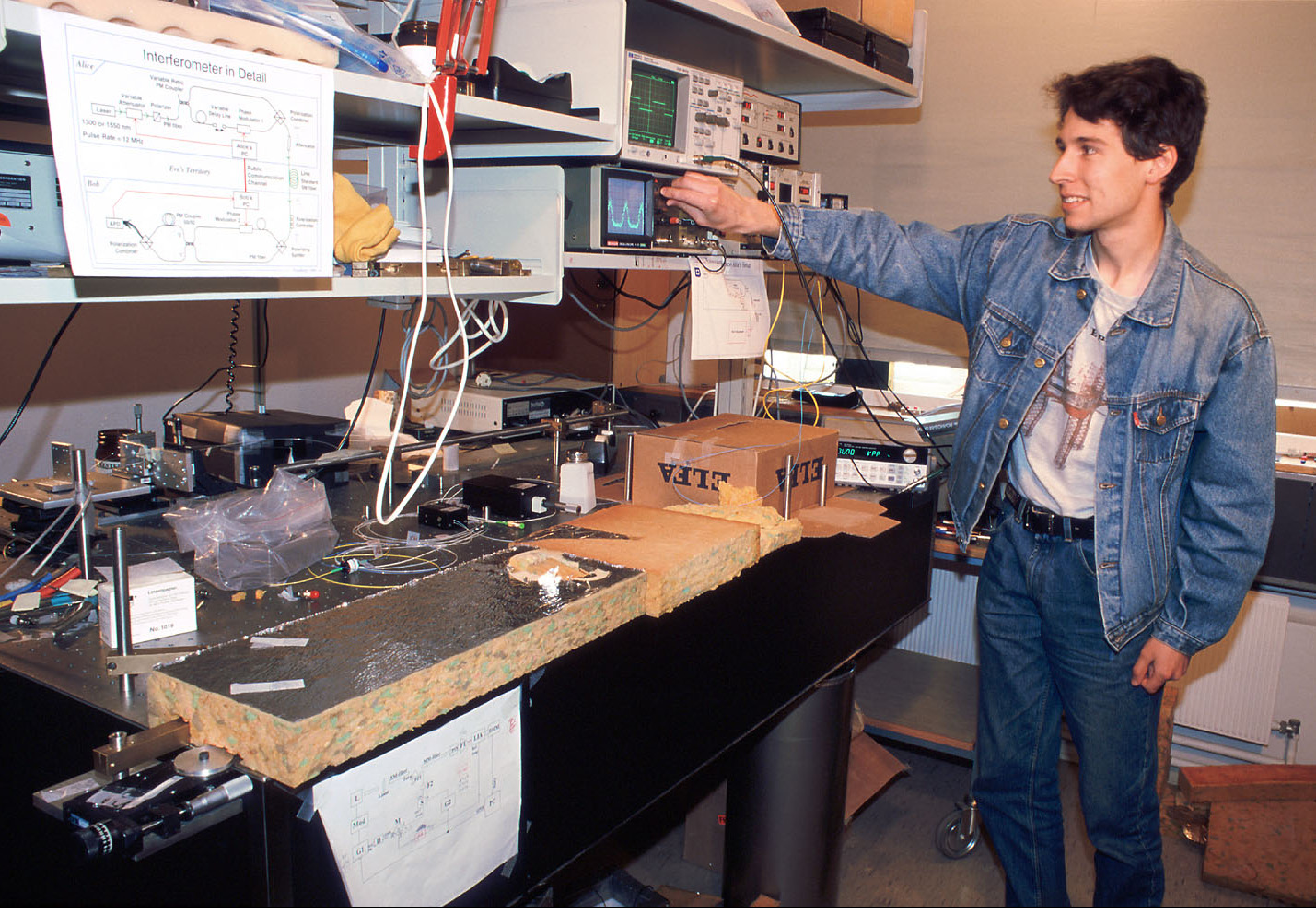


– interrogating Alice's phase modulator with powerful external pulses (can give Eve bit values directly)

Trojan-horse attack experiment

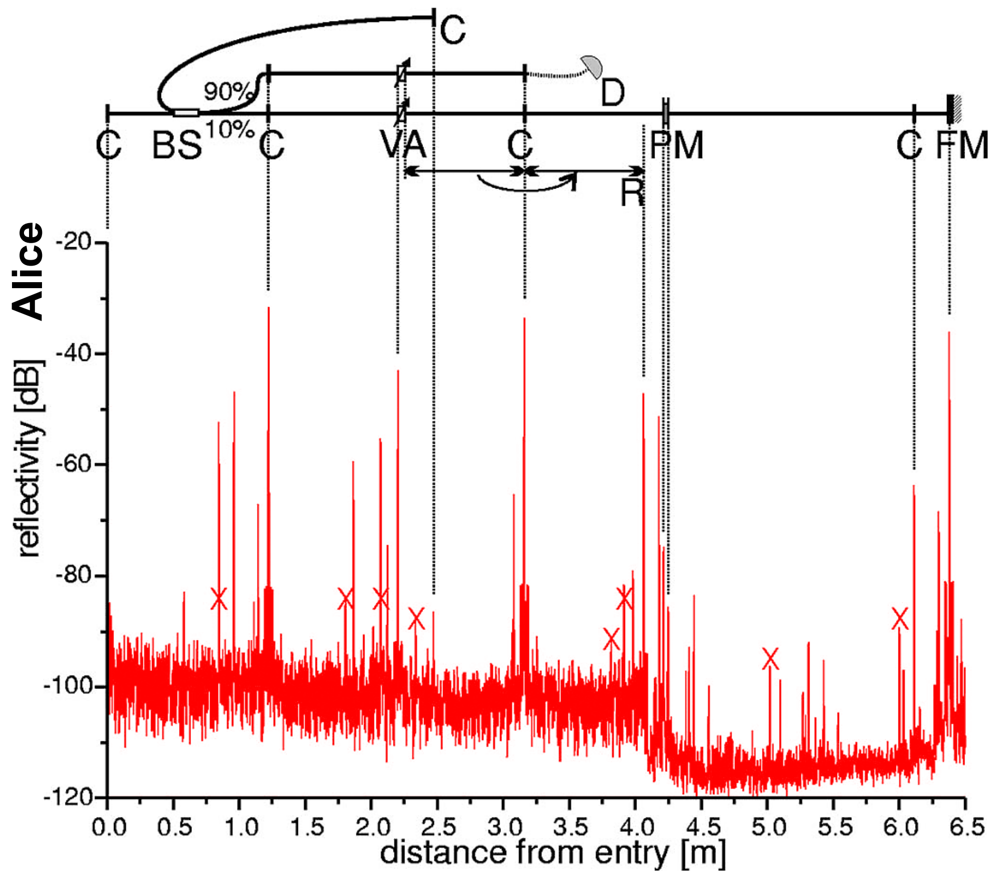


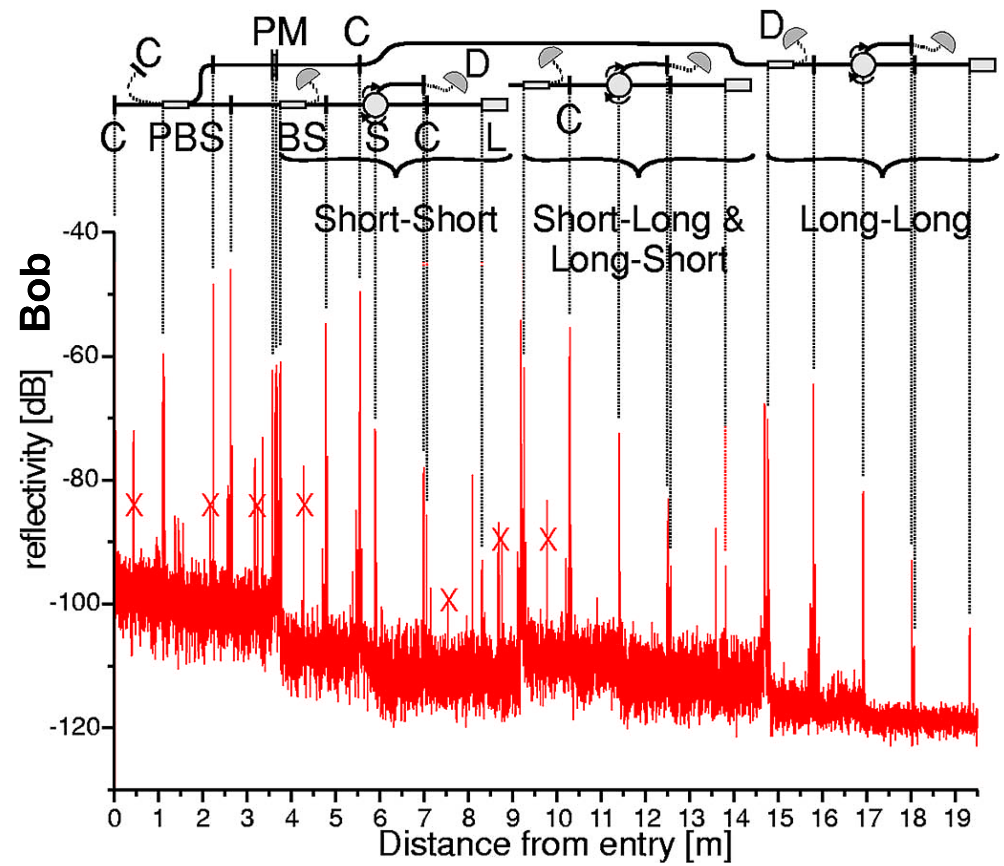
A. Vakhitov *et al.*, J. Mod. Opt. **48**, 2023 (2001)



Artem Vakhitov tunes up Eve’s setup

Trojan-horse attack for plug-and-play system

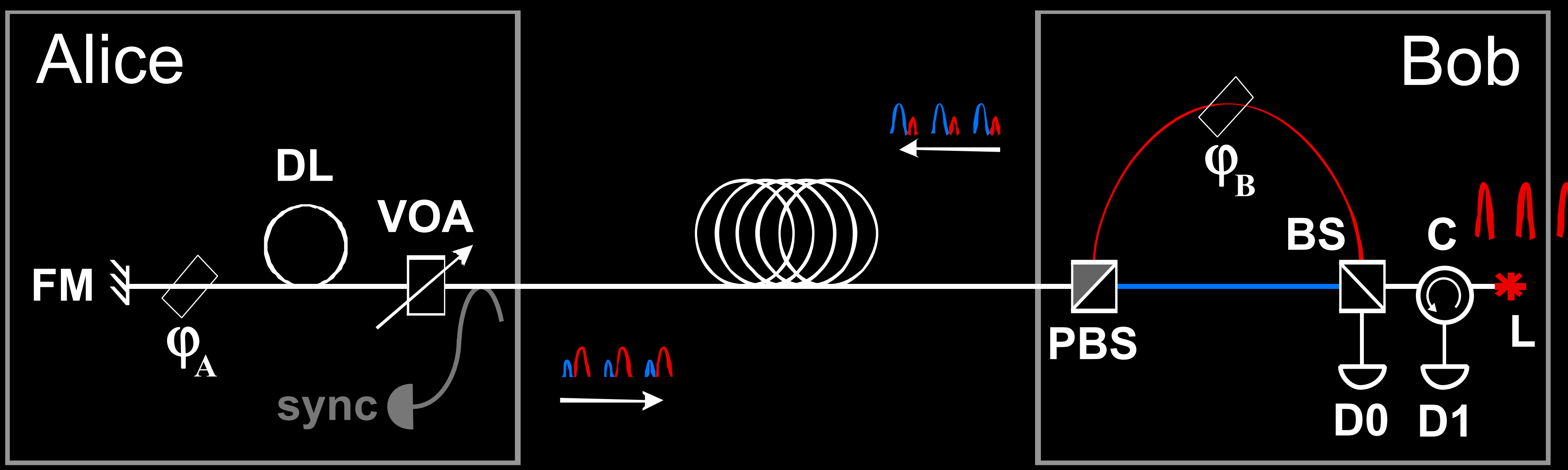




Eve gets back one photon $\rightarrow$ in principle, extracts 100% information

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

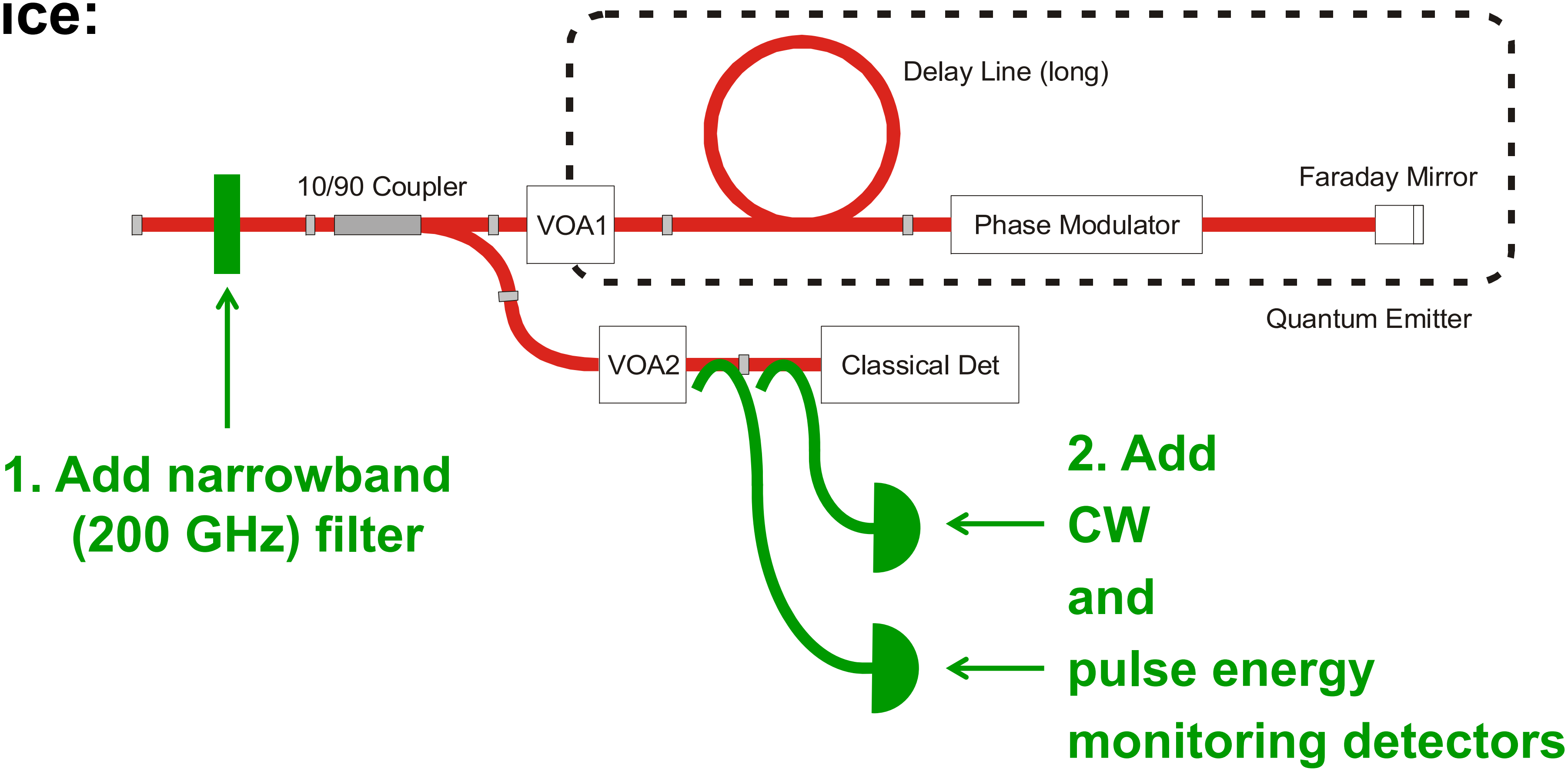
Countermeasures?



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

Countermeasures for plug-and-play system

Alice:



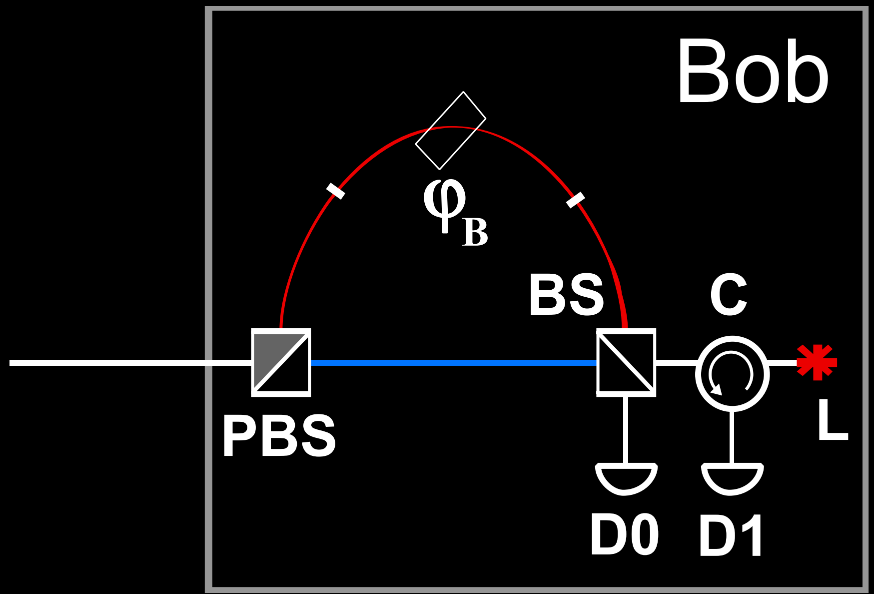
S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, L. Monat, M. Legré, V. Makarov, *unpublished*

Bob: none

(one consequence: SARG protocol may be insecure)

N. Jain, E. Anisimova, I. Khan, V. Makarov, Ch. Marquardt, G. Leuchs, arXiv:1406.5813

Trojan-horse attack on Bob



N. Jain, E. Anisimova, I. Khan, V. Makarov, Ch. Marquardt, G. Leuchs, arXiv:1406.5813

Example of vulnerability and countermeasures

Photon-number-splitting attack

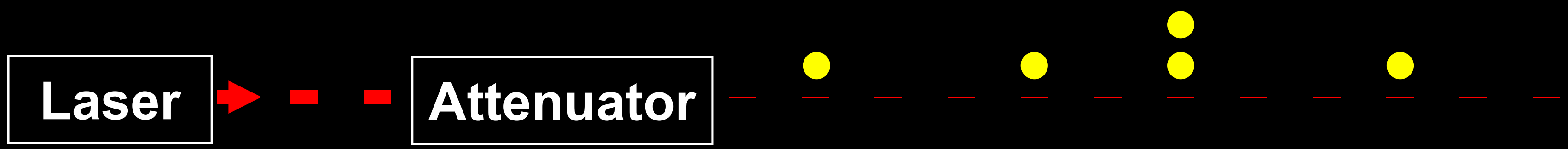
C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992)

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)

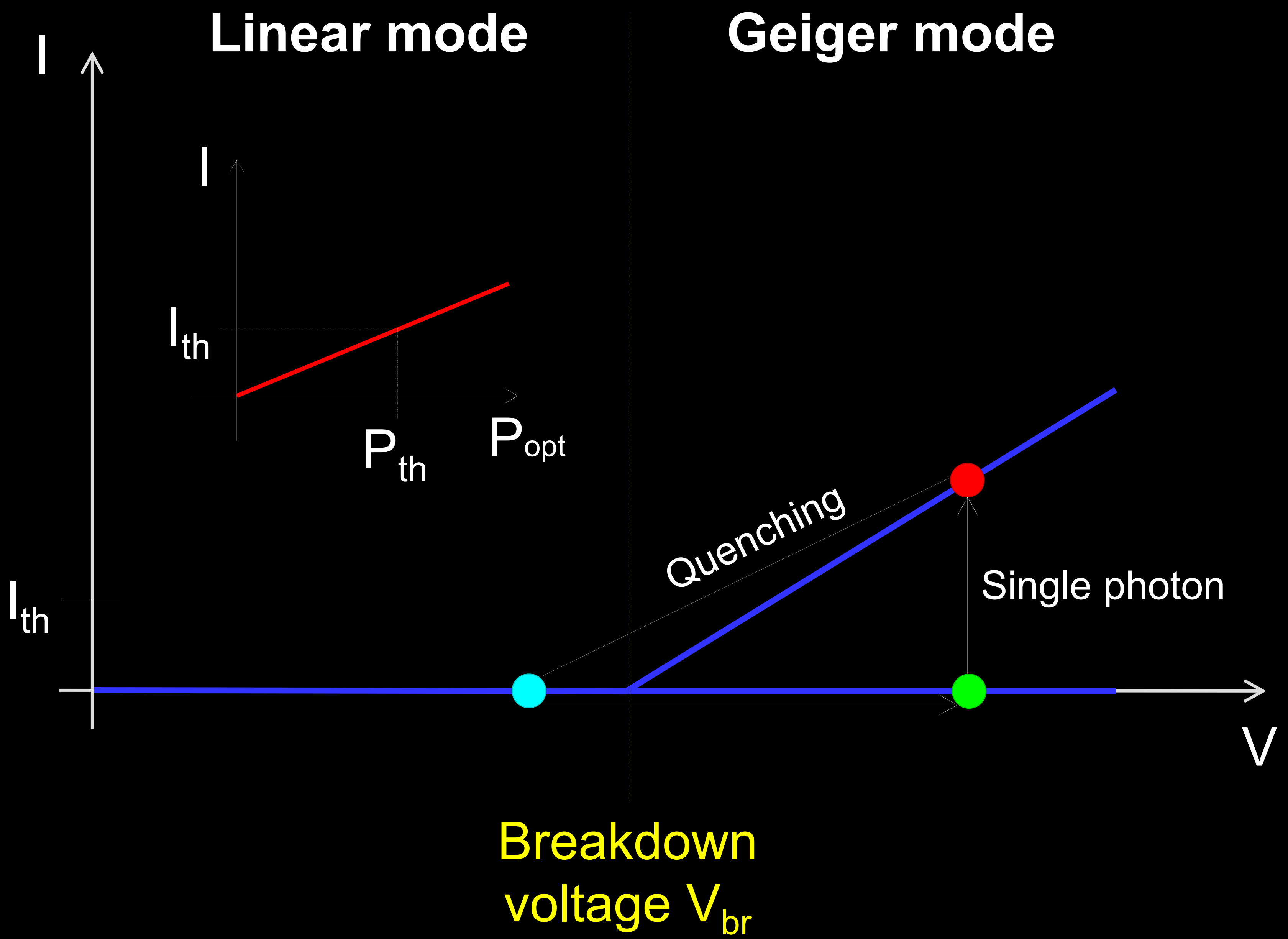
K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. A. **68**, 022317 (2003)

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

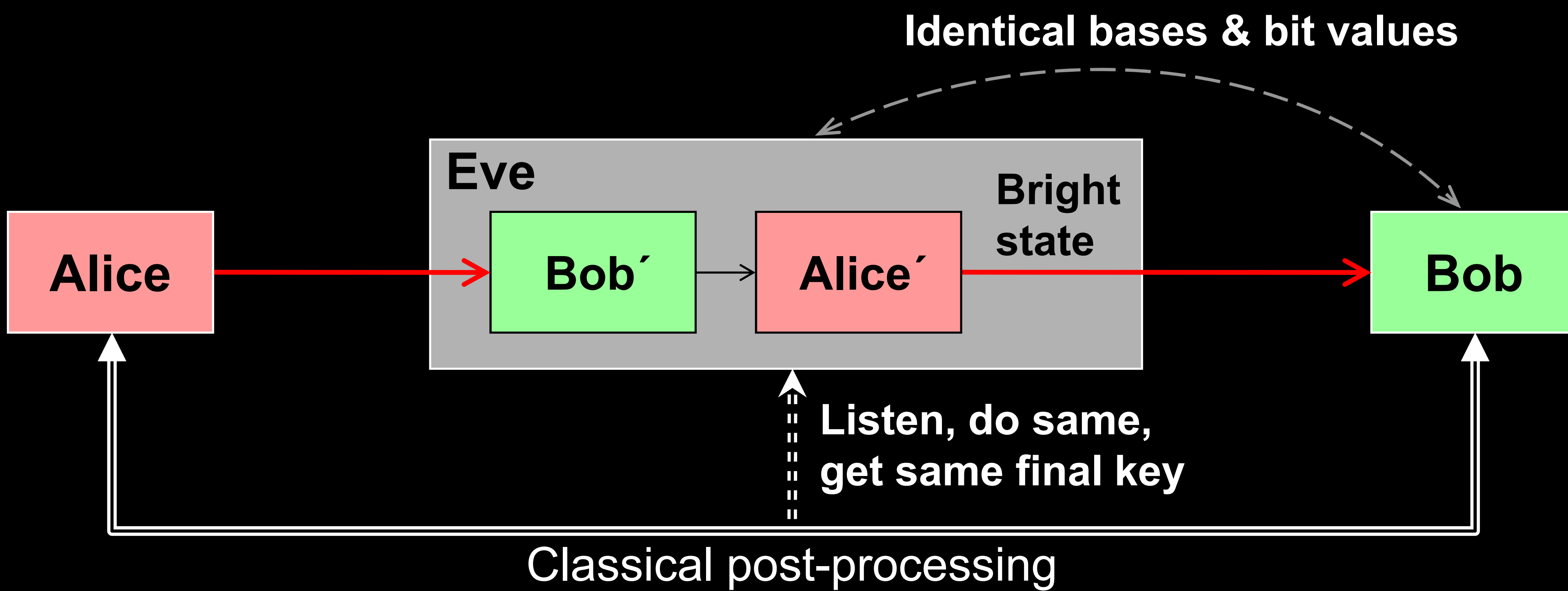
Attack	Target component	Tested system
Detector saturation H. Qin, R. Kumar, R. Alleaume, presentation at QCrypt (2013)	homodyne detector	SeQureNet
Shot-noise calibration P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A **87**, 062313 (2013)	sync detector	SeQureNet
Wavelength-selected PNS M.-S. 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 syst.
Deadtime H. Weier *et al.*, New J. Phys. **13**, 073024 (2011)	single-photon detector	research syst.
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)
Phase-remapping F. Xu, B. Qi, H.-K. Lo, New J. Phys. **12**, 113026 (2010)	phase modulator	ID Quantique
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 syst.
Time-shift	single-photon detector	ID Quantique

Attack	Target component	Tested system
Detector saturation H. Qin, R. Kumar, R. Alleaume, presentation at QCrypt (2013)	homodyne detector	SeQureNet
Shot-noise calibration P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A **87**, 062313 (2013)	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 syst.
Deadtime H. Weier *et al.*, New J. Phys. **13**, 073024 (2011)	single-photon detector	research syst.
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)
Phase-remapping F. Xu, B. Qi, H.-K. Lo, New J. Phys. **12**, 113026 (2010)	phase modulator	ID Quantique
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 syst.
Time-shift	single-photon detector	ID Quantique

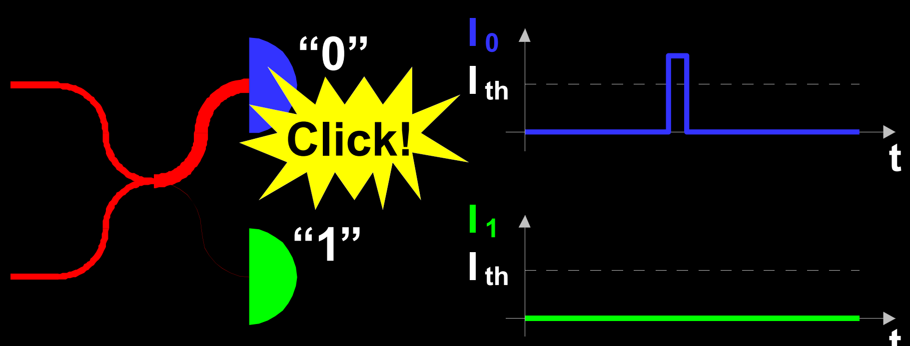
Attack example: avalanche photodetectors (APDs)



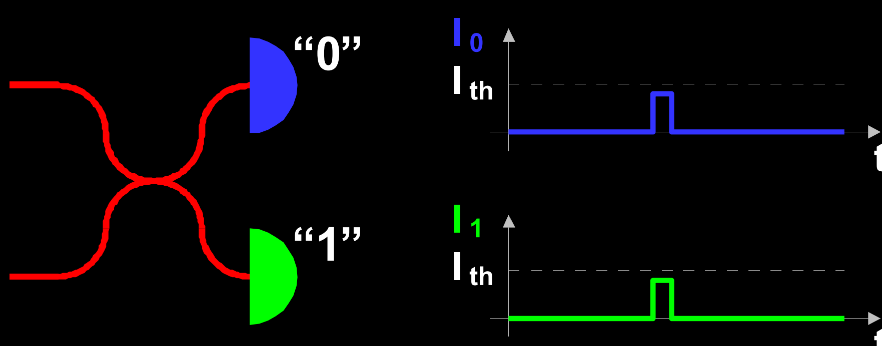
Faked-state attack in APD linear mode



Bob chooses same basis as Eve:

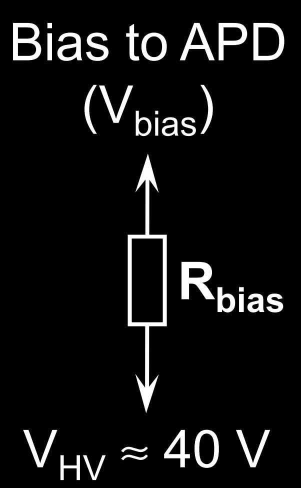


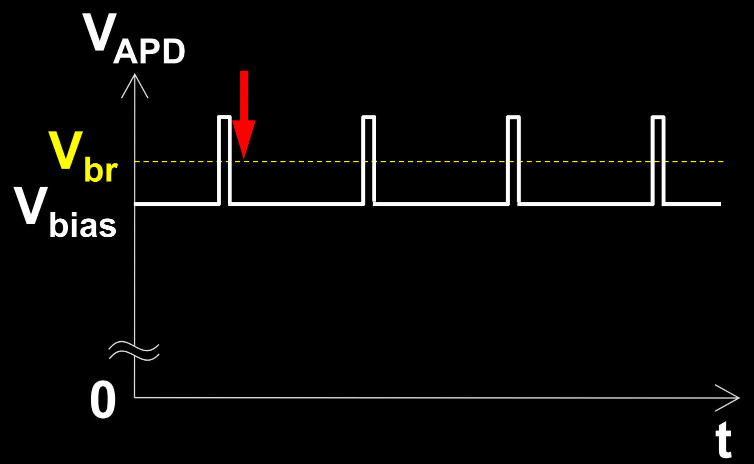
Bob chooses different basis:



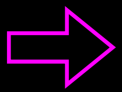
L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Nat. Photonics **4**, 686 (2010)

Blinding APD with bright light



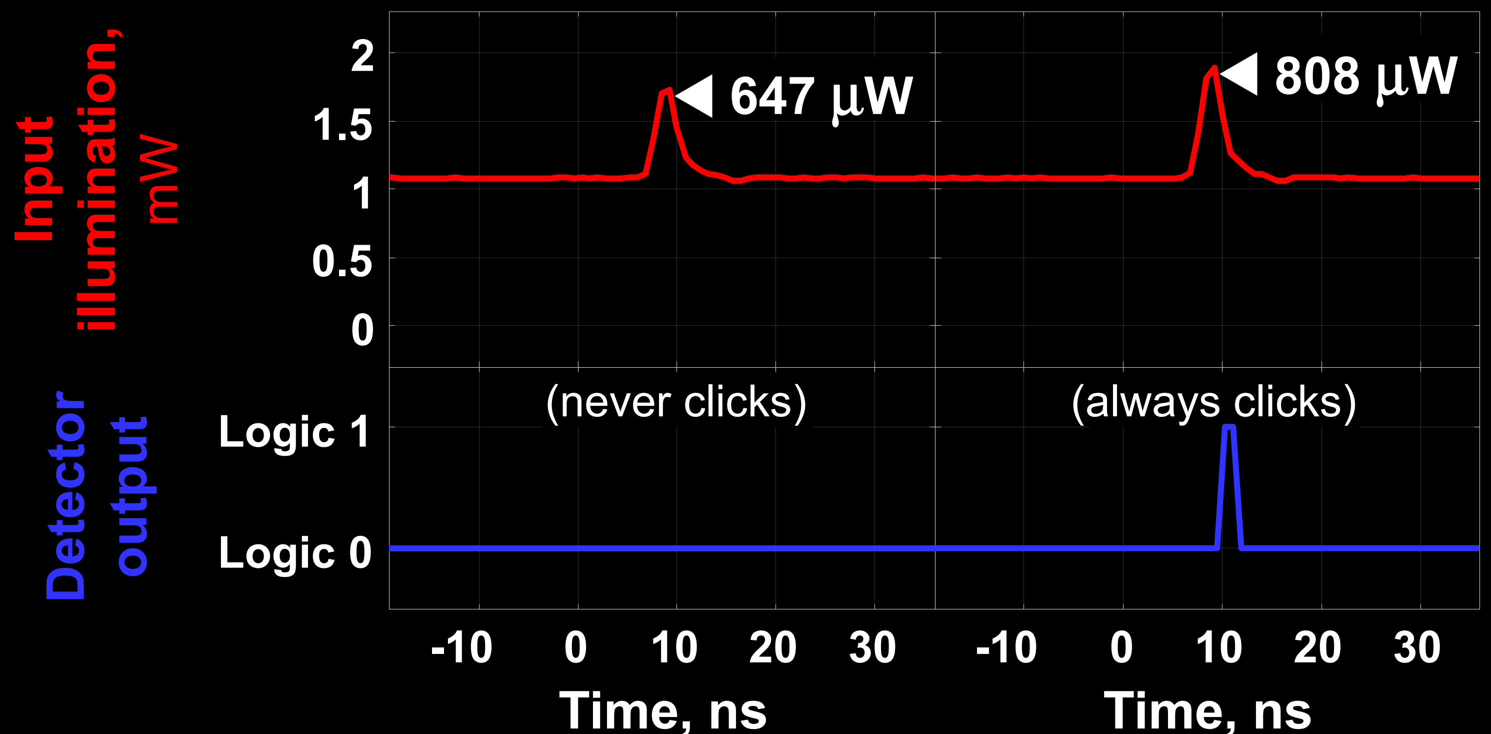


Eve applies CW light



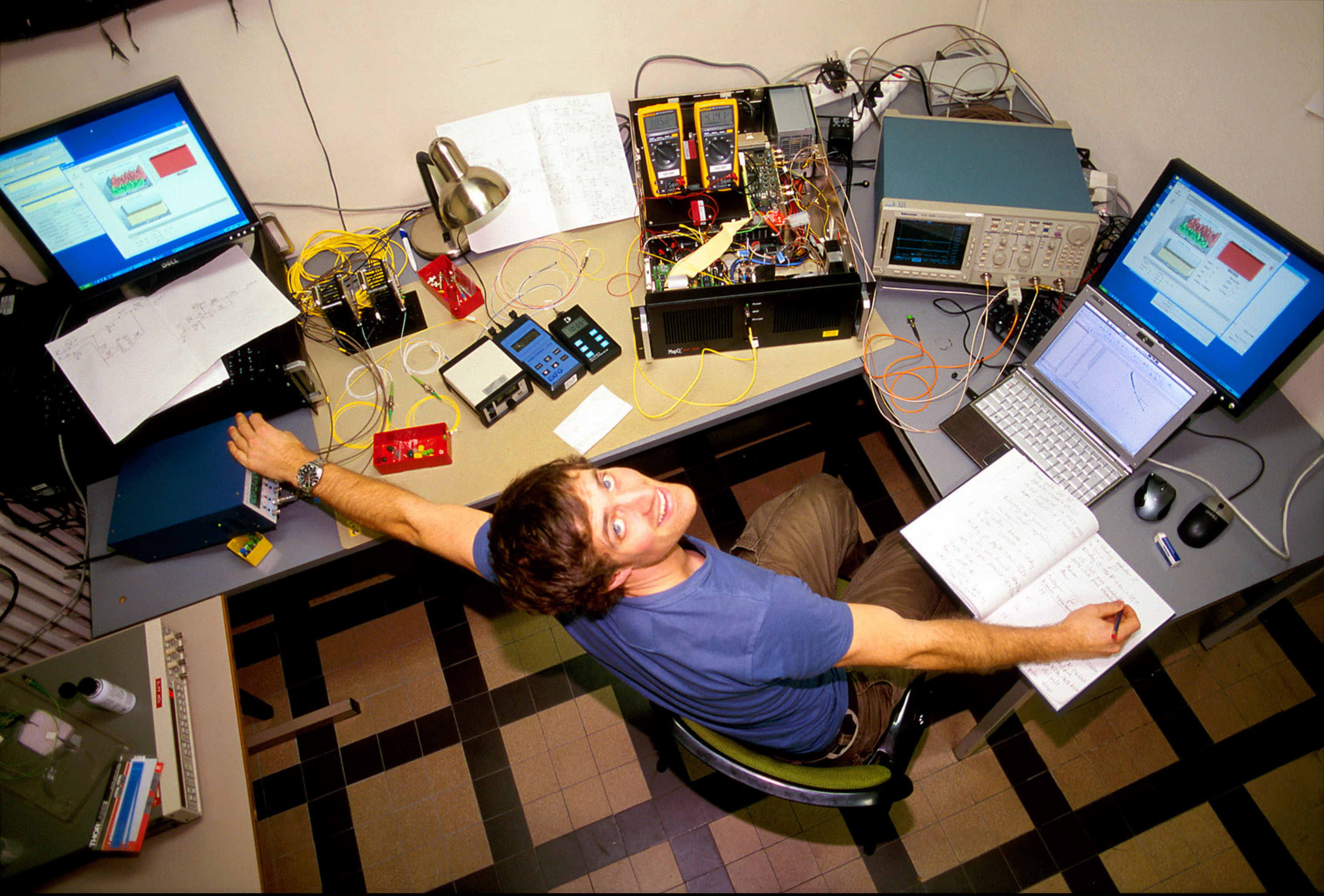
Detector blind!

Zero dark count rate



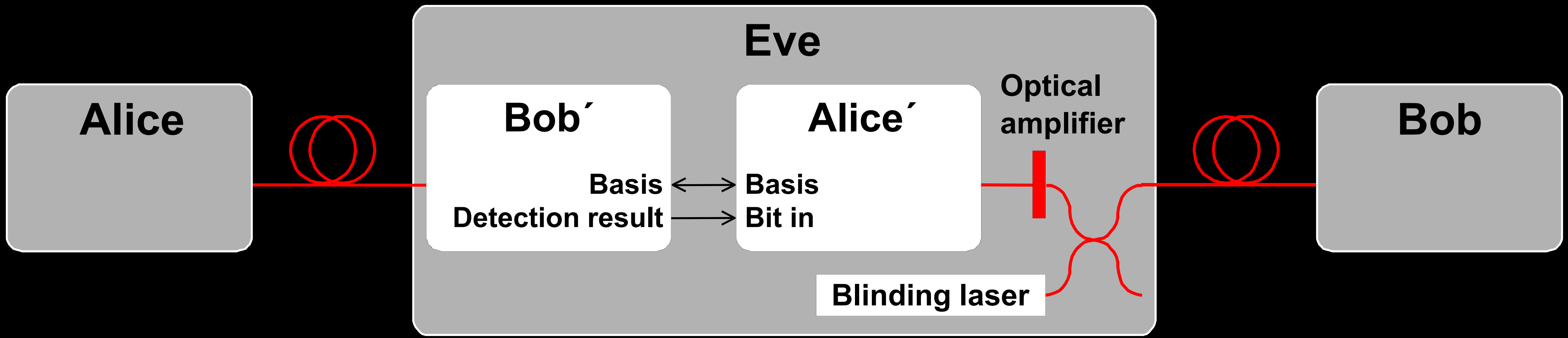
ID Quantique Clavis2

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



Lars Lydersen testing MagiQ Technologies QPN 5505

Proposed full eavesdropper

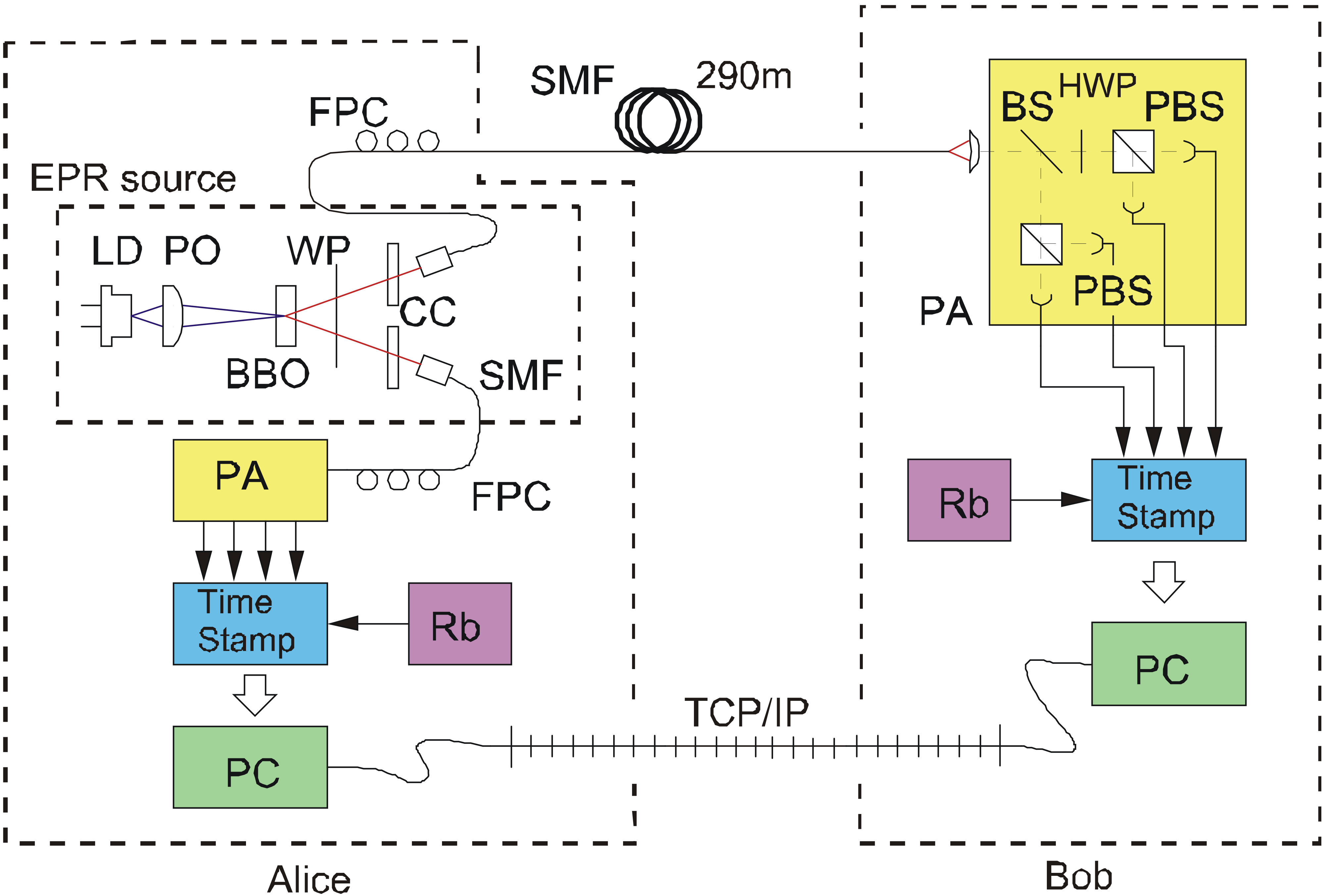


Eavesdropping 100% key on installed QKD line

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

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

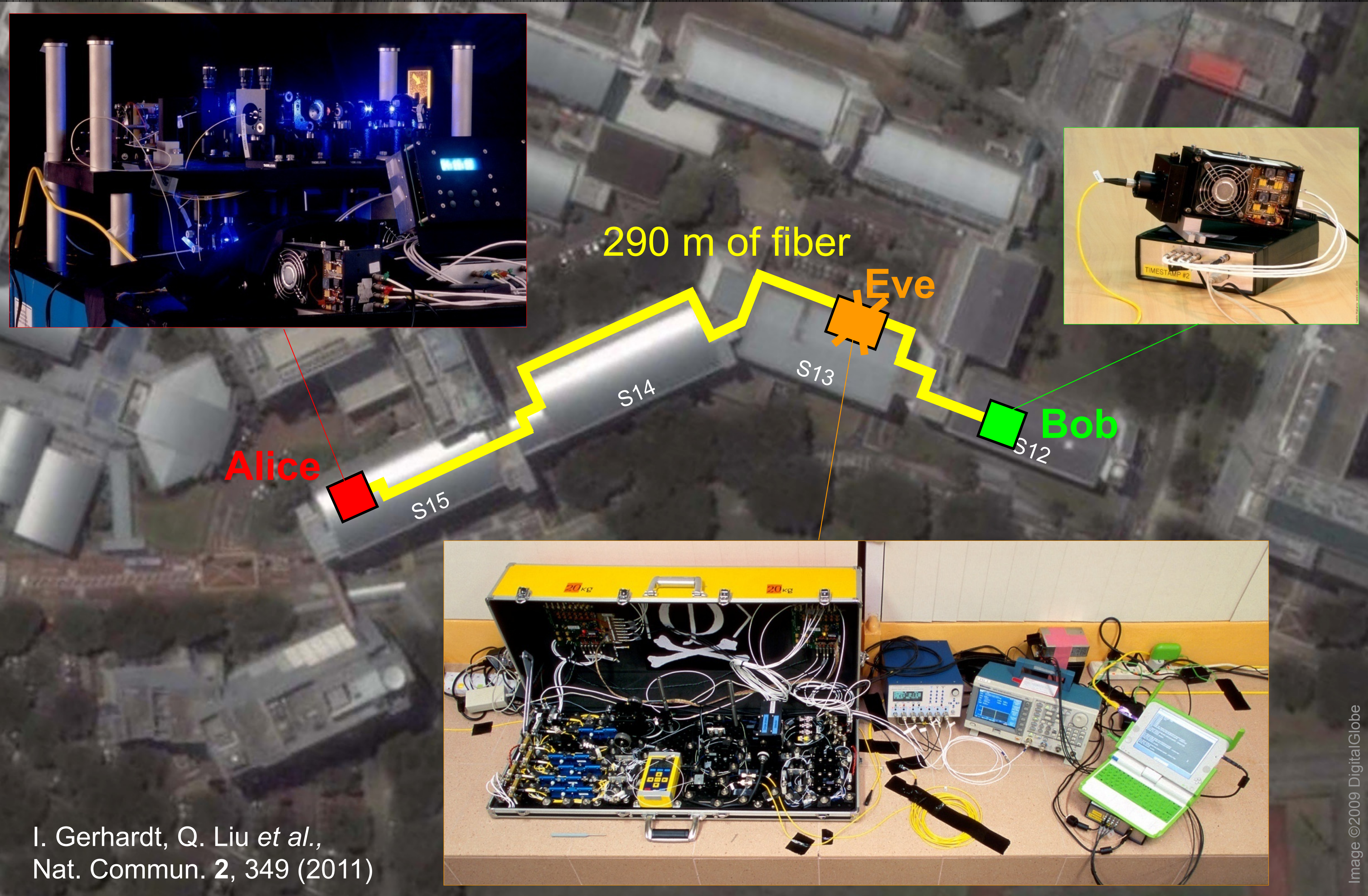
Entanglement-based QKD



M. P. Peloso *et al.*, New J. Phys. **11**, 045007 (2009)

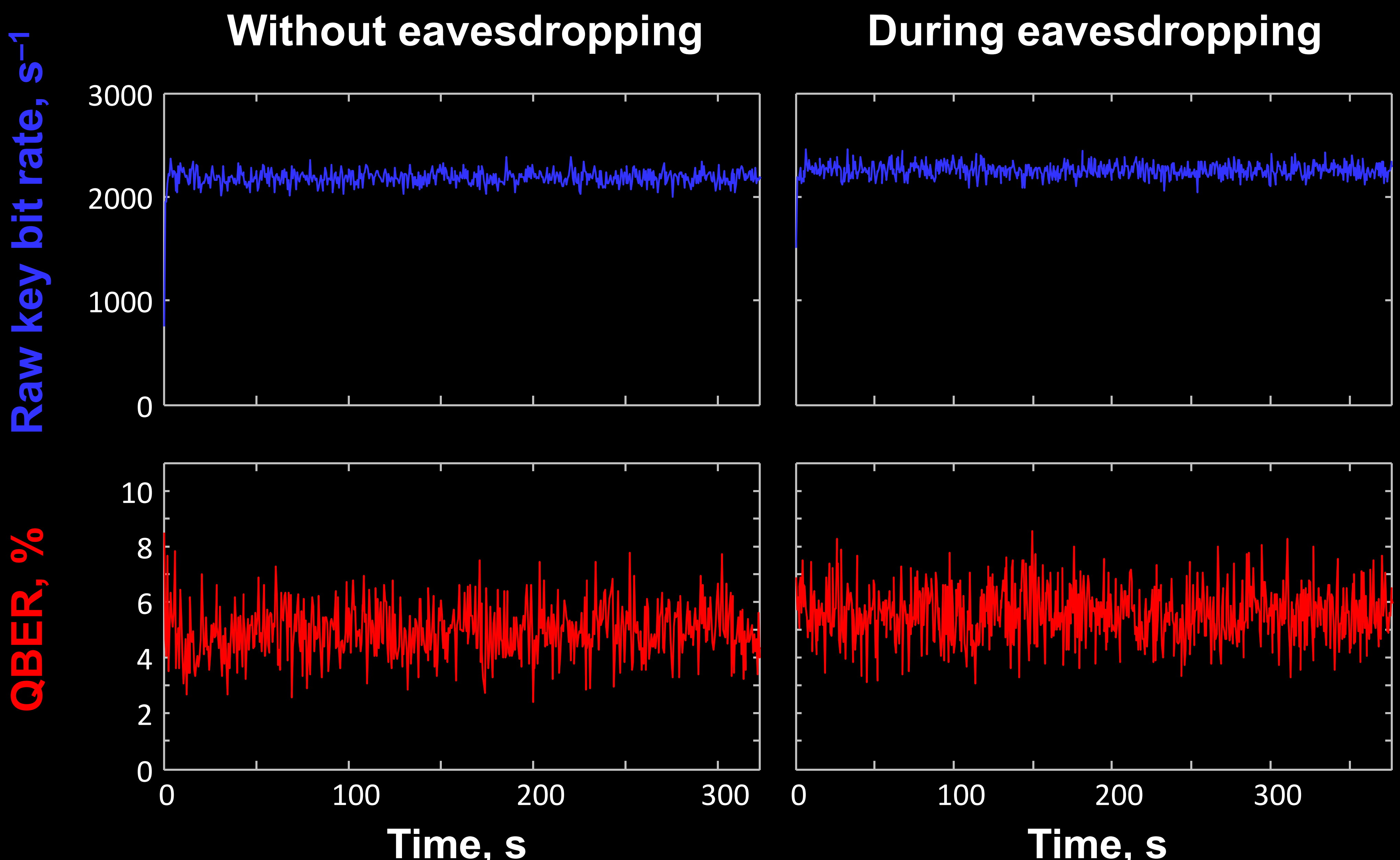
Eavesdropping 100% key on installed QKD line

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



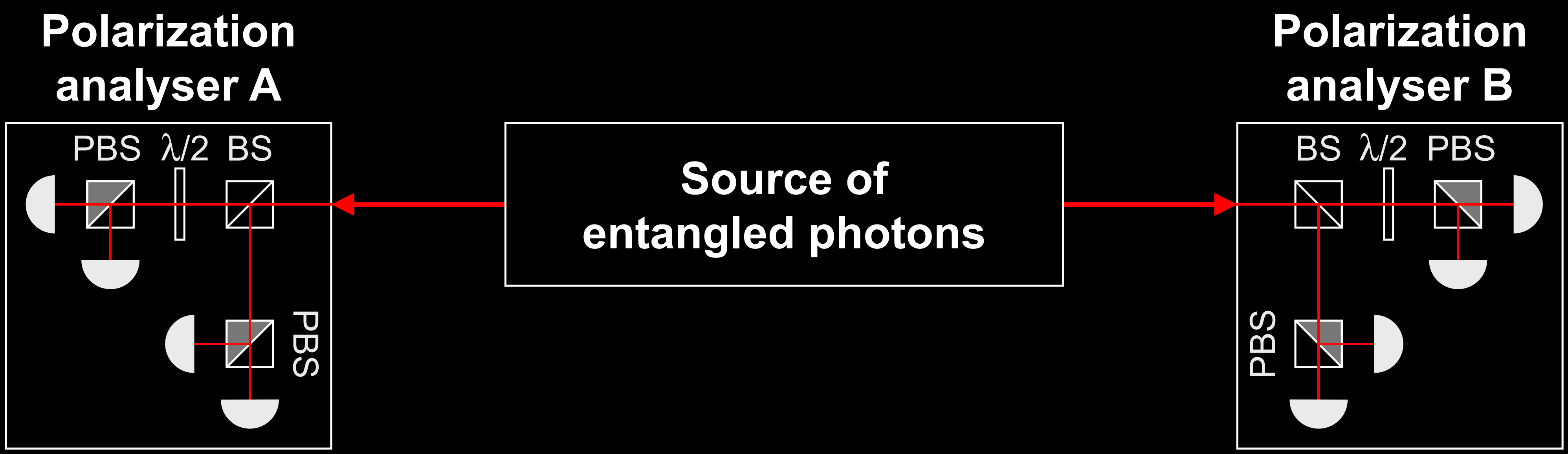
I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, V. Makarov, Nat. Commun. **2**, 349 (2011)

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



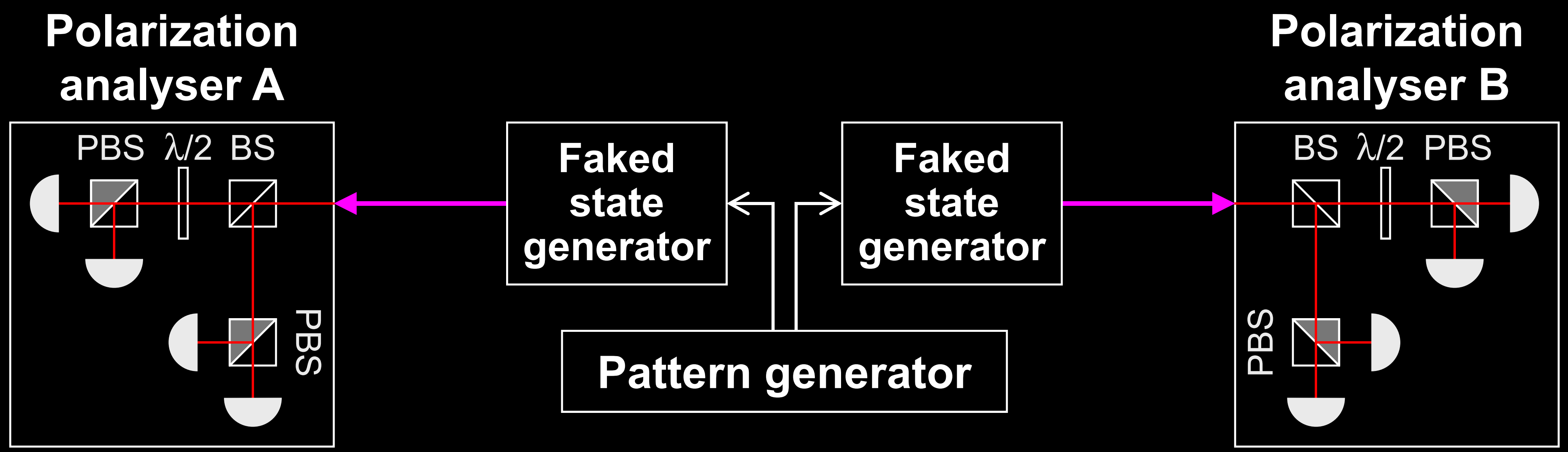
I. Gerhardt, Q. Liu *et al.*, Phys. Rev. Lett. **107**, 170404 (2011); N. Sultana, V. Makarov, *unpublished*

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

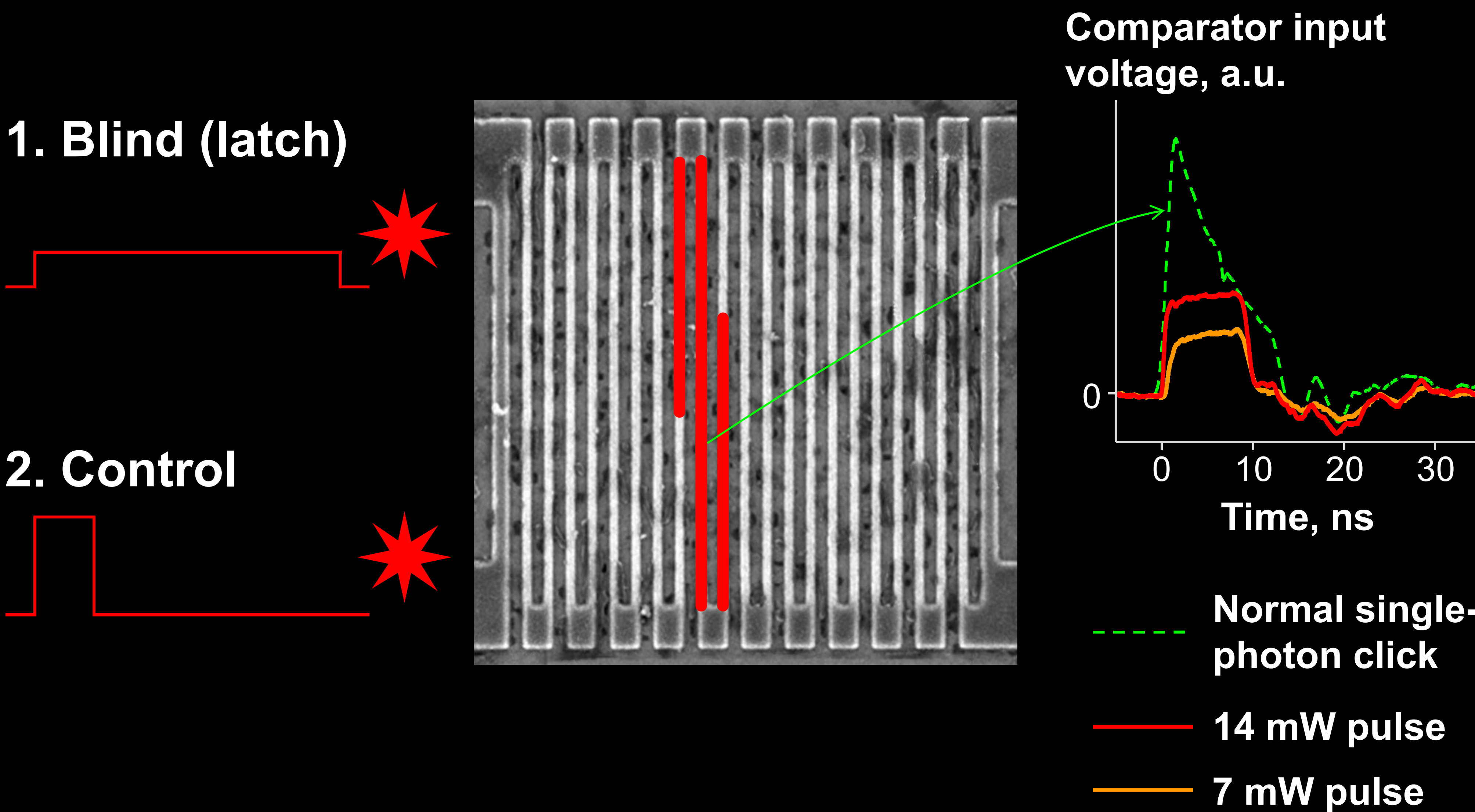


Passive basis choice: $|S| \leq 4$, click probability $= 100\%$

Active basis choice: $|S| \leq 2\sqrt{2}\ (4)$, click probability $= 66.7\%\ (50\%)$

I. Gerhardt, Q. Liu *et al.*, Phys. Rev. Lett. **107**, 170404 (2011); N. Sultana, V. Makarov, *unpublished*

Controlling superconducting nanowire single-photon detectors



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

Band-aid

- **Software patch to randomly vary detector sensitivity**

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

- **Monitoring extra electrical parameters in detector**

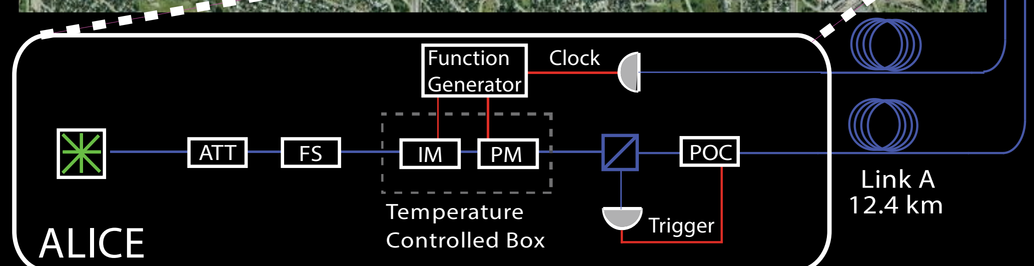
  Z. L. Yuan, J. F. Dynes, A. J. Shields, Appl. Phys. Lett. **98**, 231104 (2011)

  ...

Integrated into security model

- **Measurement-device-independent QKD**

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



Demonstration in Calgary

A. Rubenok *et al.*, arXiv:1204.0738v2

2009

Responsible disclosure is important

Example: hacking commercial systems

2010

ID Quantique got a detailed vulnerability report

- **reaction: requested time, developed a patch**

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

MagiQ Technologies got a detailed vulnerability report

- **reaction: informed us that QPN 5505 is discontinued**

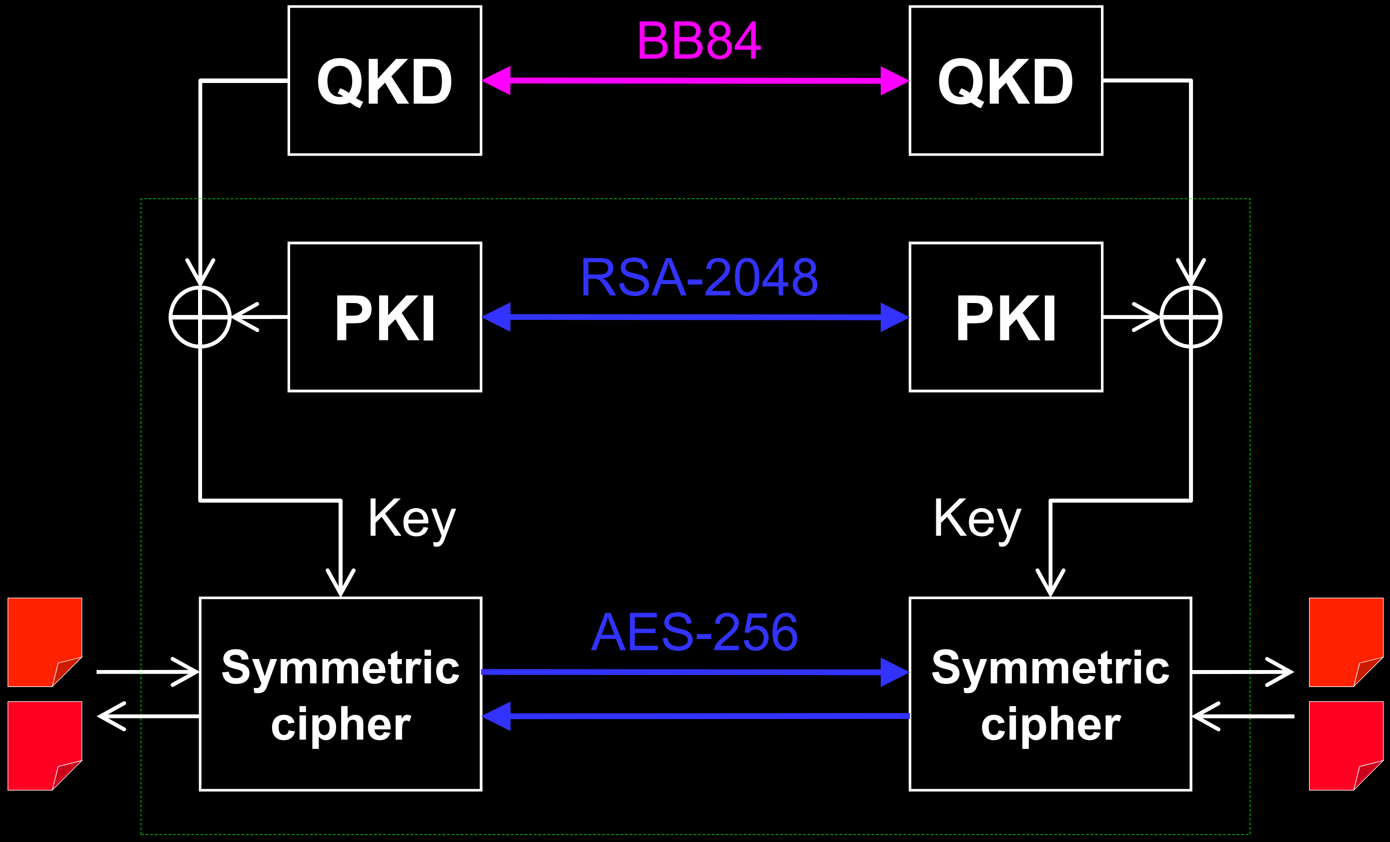
Results presented orally at a scientific conference

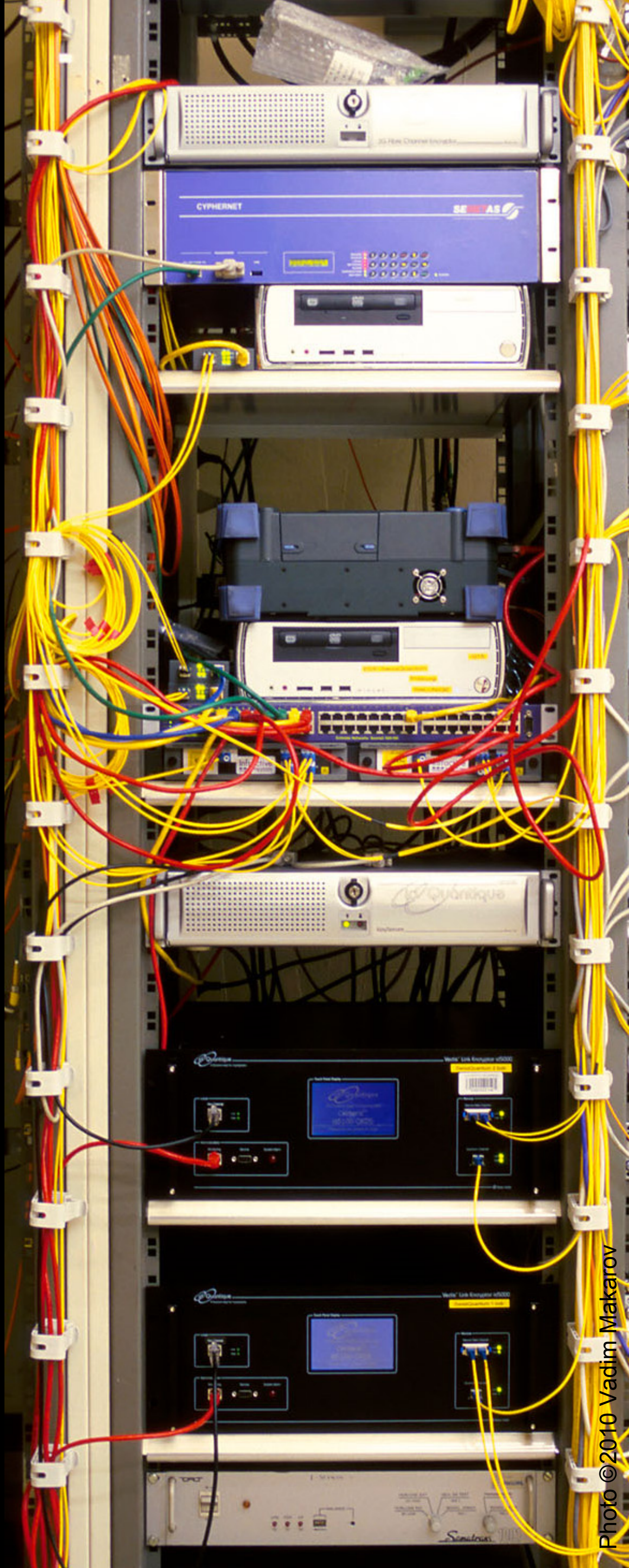
Public disclosure in a journal paper

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

Can we eavesdrop on commercial systems?

ID Quantique's Cerberis:
Dual key agreement





Some other topics in experimental quantum cryptography...

- Continuous-variable QKD
- Differential-phase-shift-keying protocols
- Quantum repeaters
- Device-independent QKD

Quantum cryptography is a viable complement to aging classical cryptography methods

Quantum cryptography has implementation imperfections, too, and the research community handles this problem successfully

$|\Phi\rangle$

www.vad1.com/lab