Lecture at Phys 10 undergraduate seminar, University of Waterloo, September 30, 2014

Quantum cryptography

Image from cover of Physics World, March 1998

Vadim Makarov

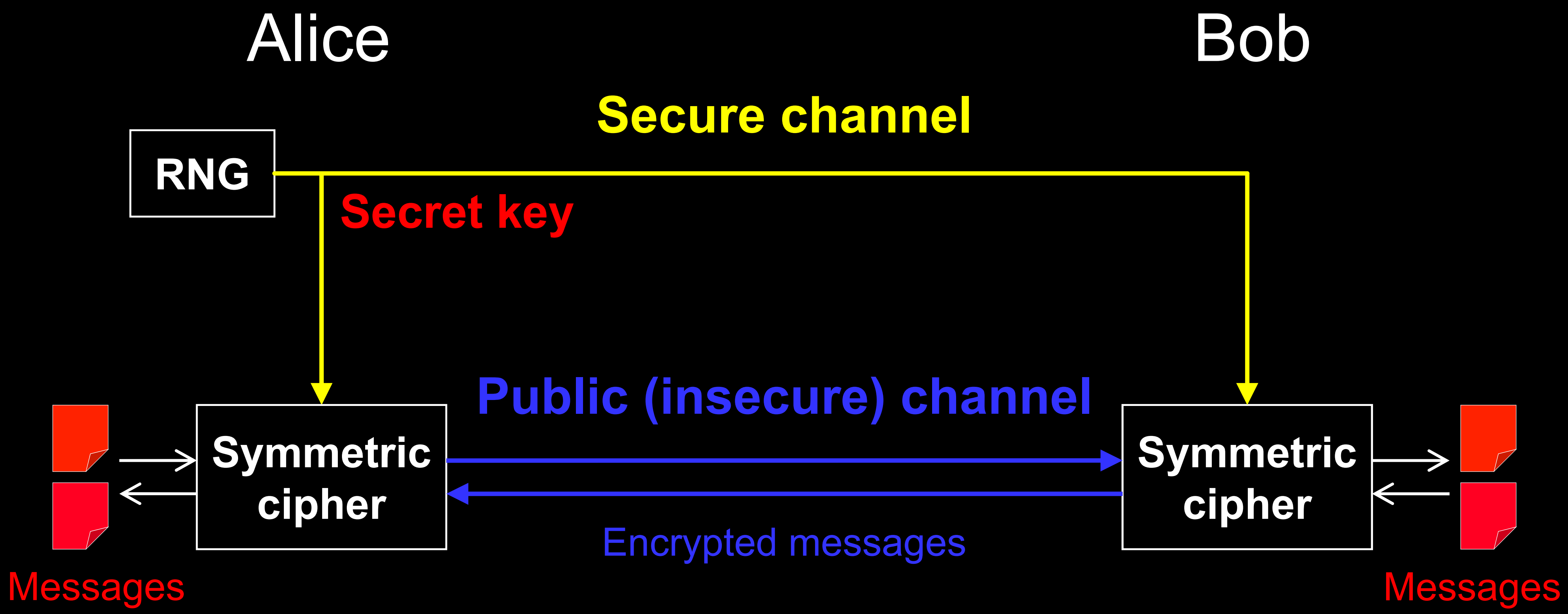
Quantum hacking lab
www.vad1.com/lab

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)

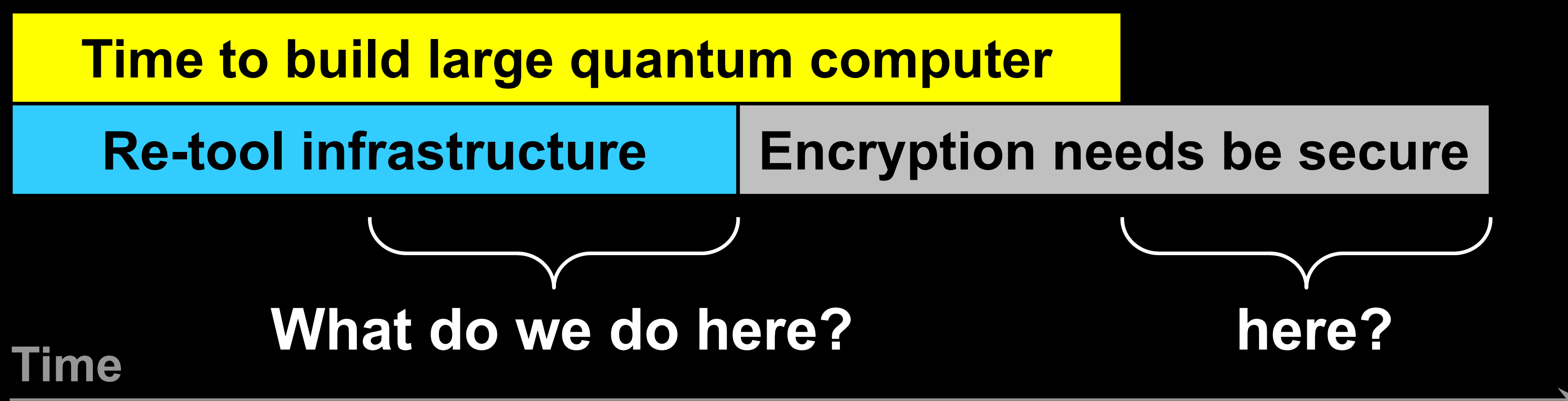
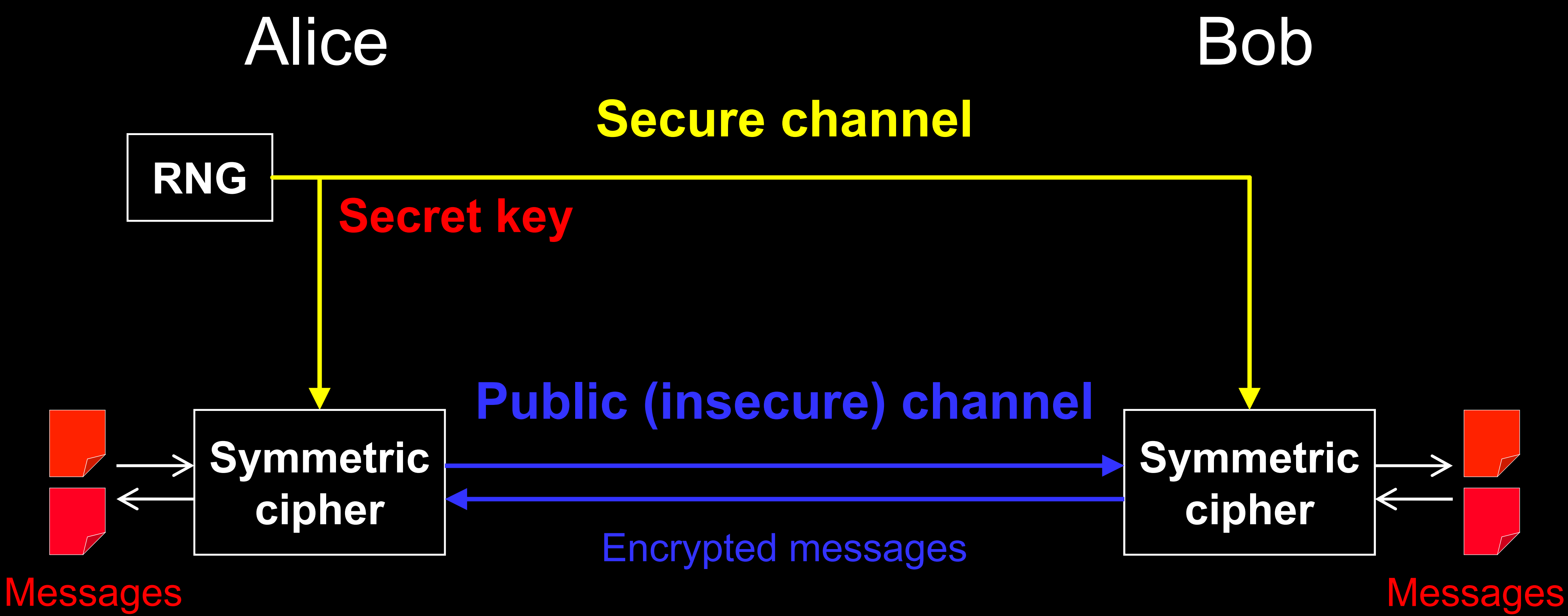


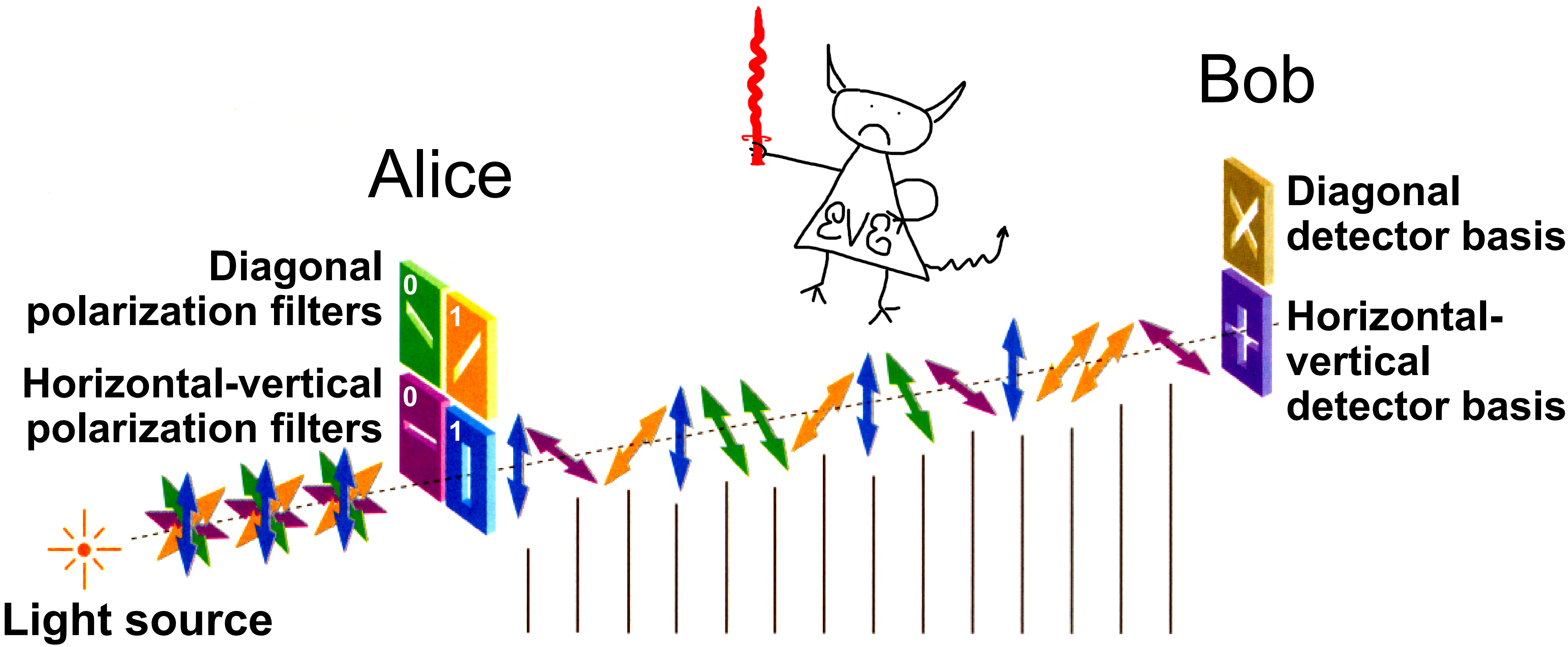
Diagram courtesy M. Mosca

Encryption and key distribution



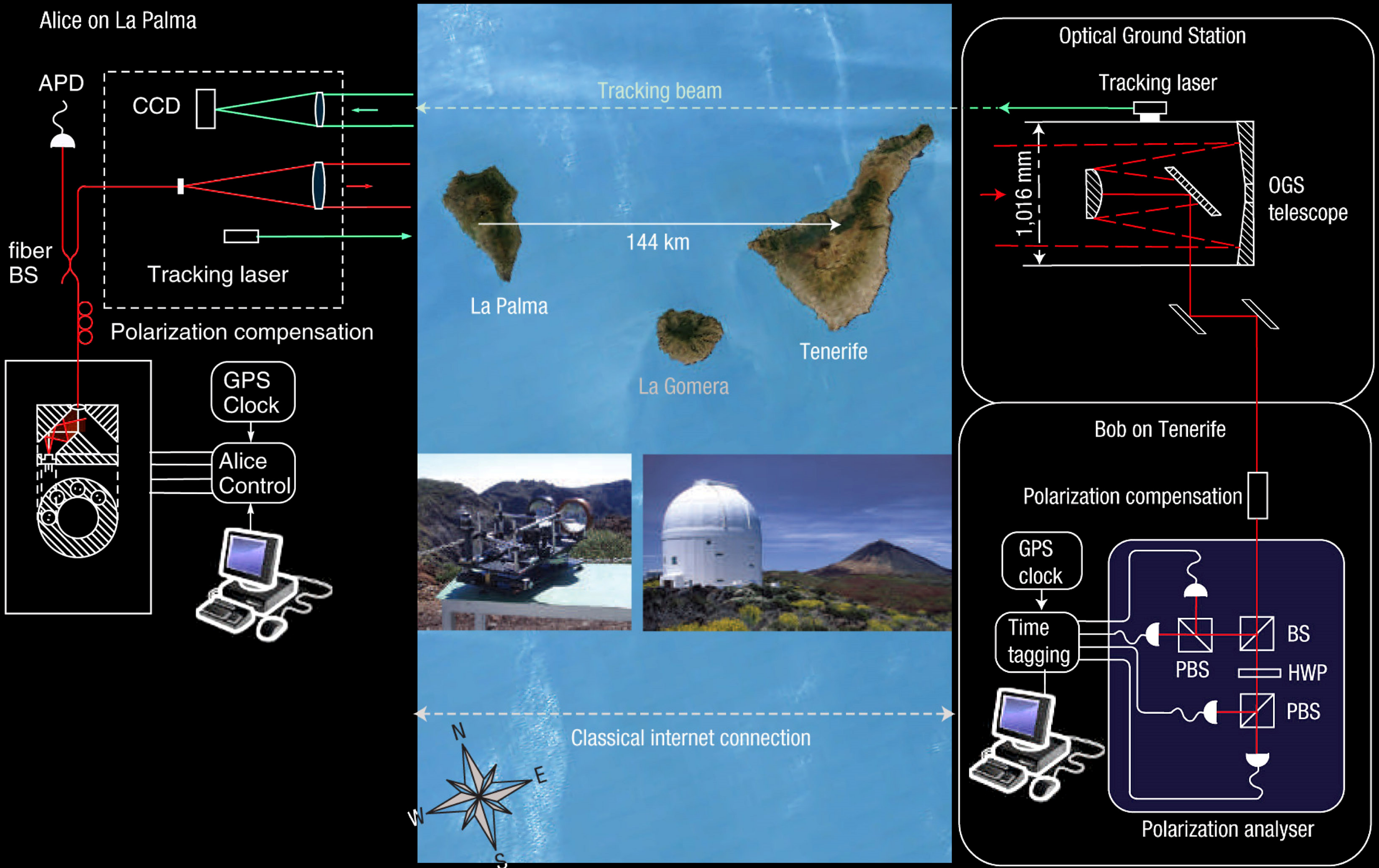
Quantum key distribution transmits secret key by sending quantum states over *open channel.*

Quantum key distribution (QKD)



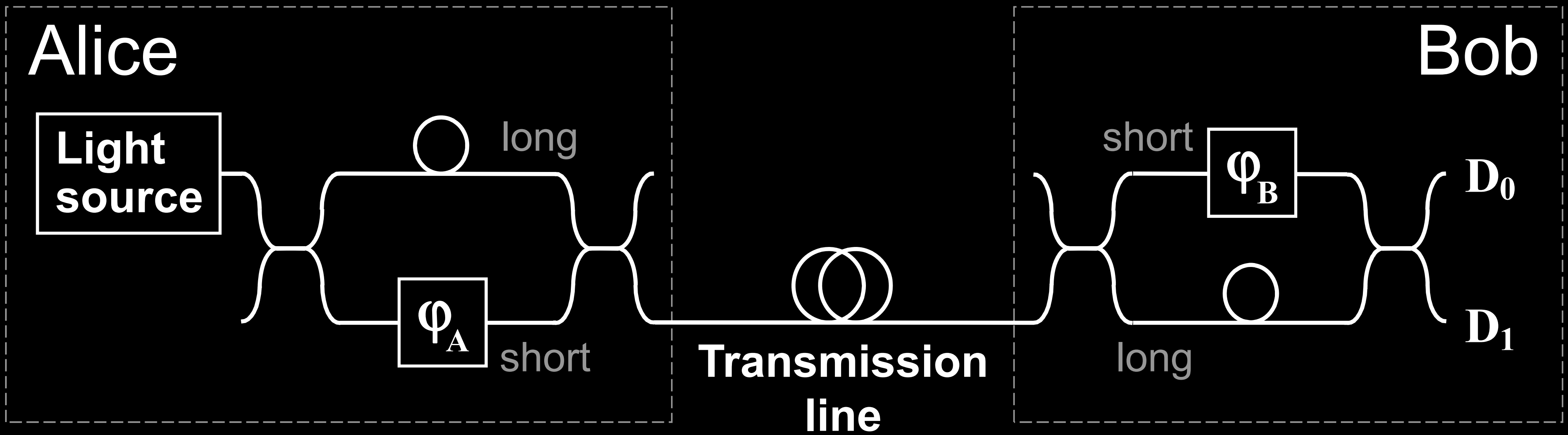
Alice’s bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Bob’s detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+
Bob’s measurement	1	0	0	1	0	0	1	1	0	0	0	1	0	0
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0

Free-space QKD over 144 km



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

Phase encoding, interferometric QKD channel



Detector bases:

φ_A = –45° or +45° : 0

φ_A = +135° or –135° : 1

φ_B = –45° : X

φ_B = +45° : Z

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)

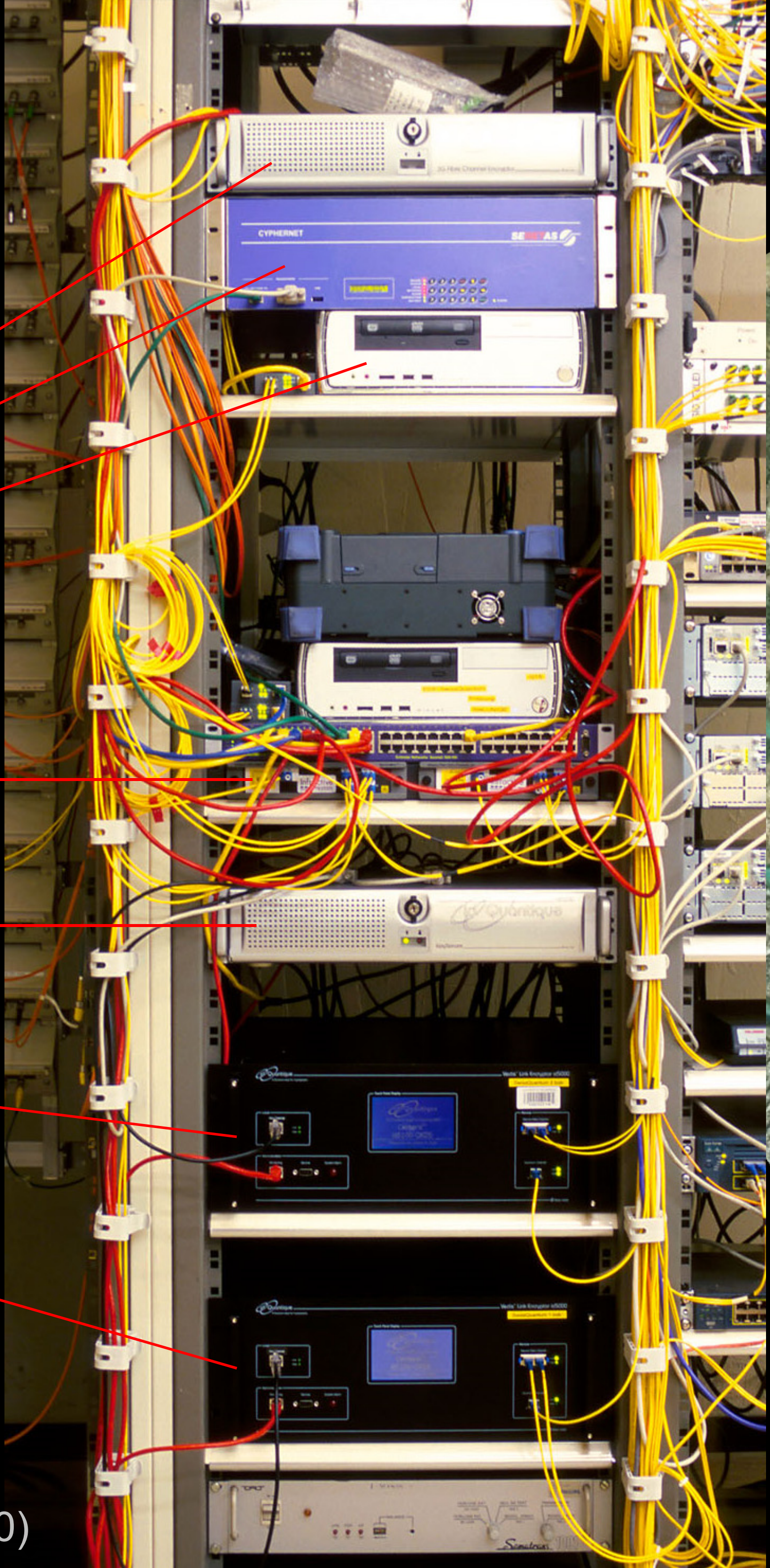
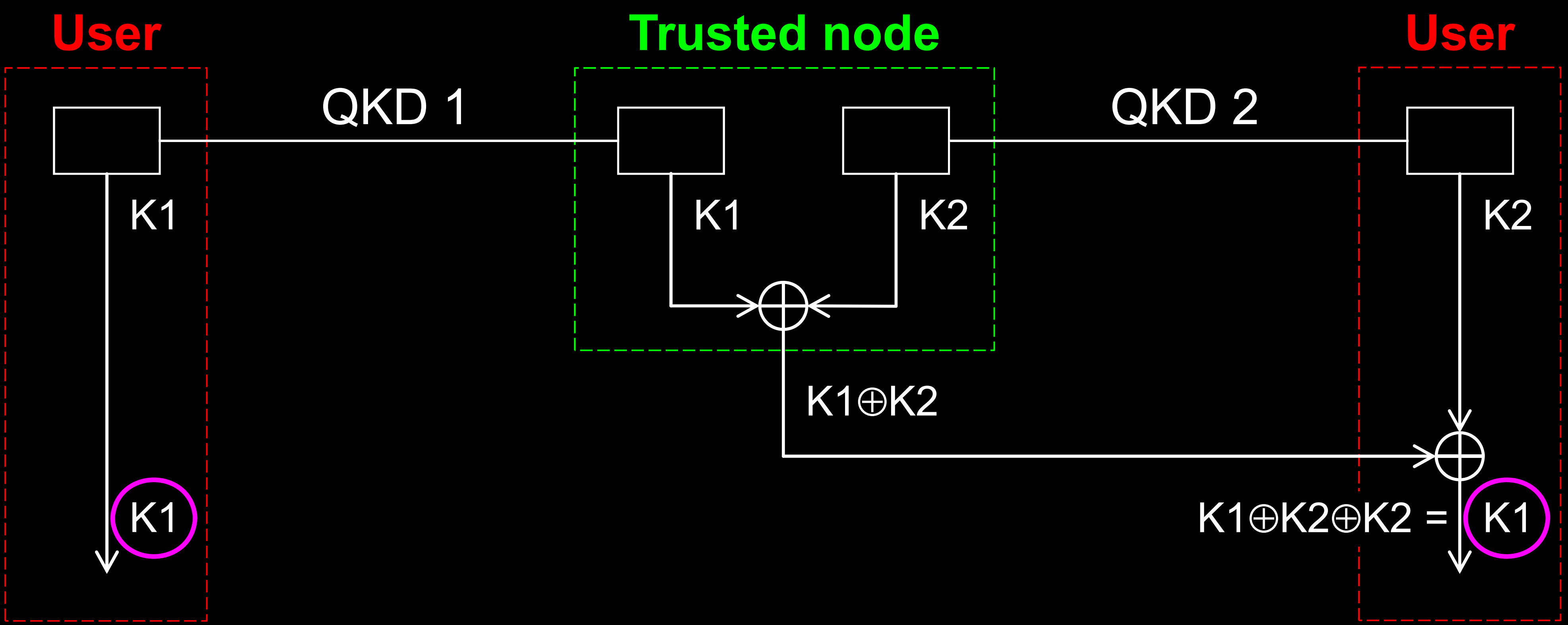


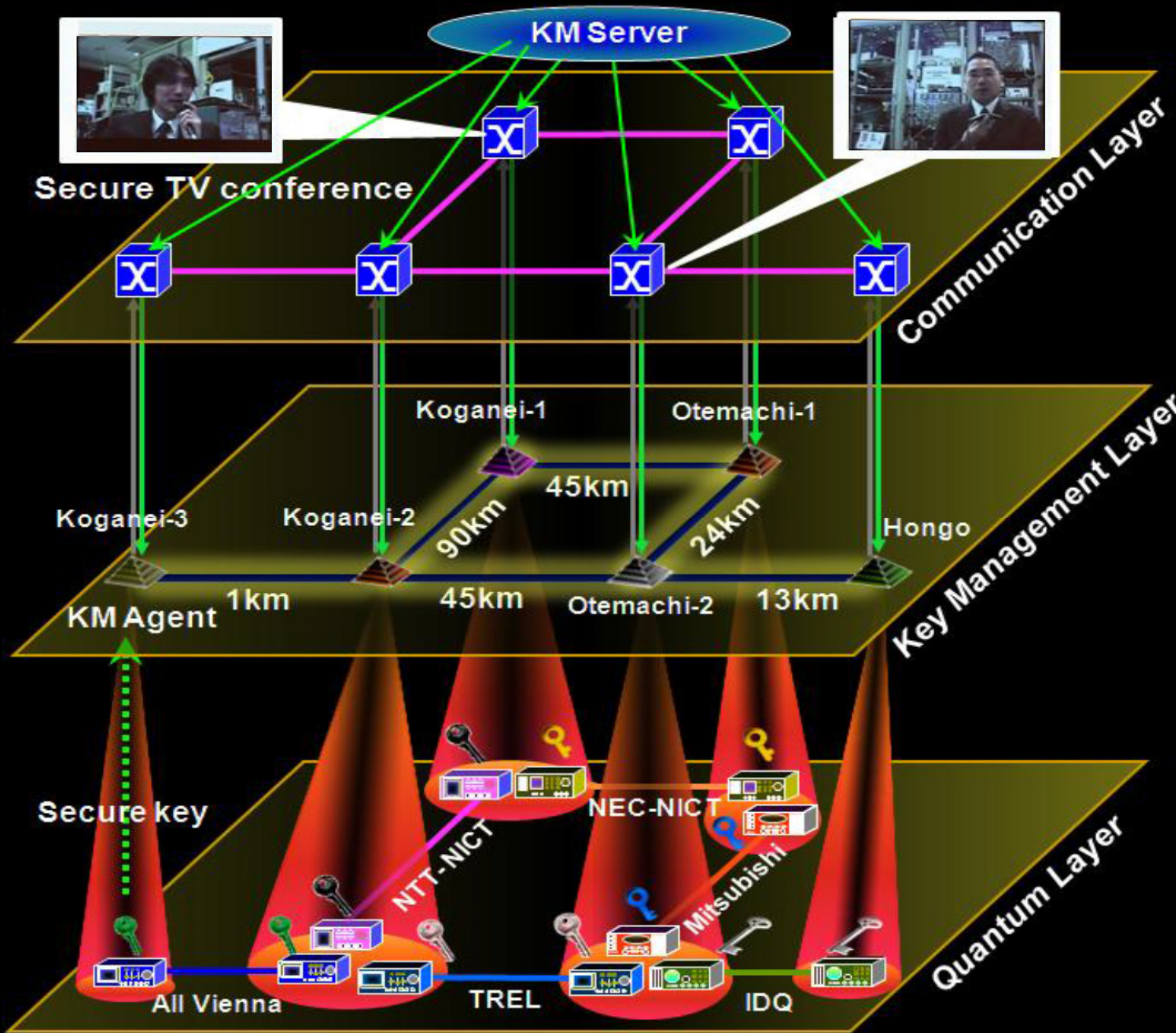
Photo ©2010 Vadim Makarov

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

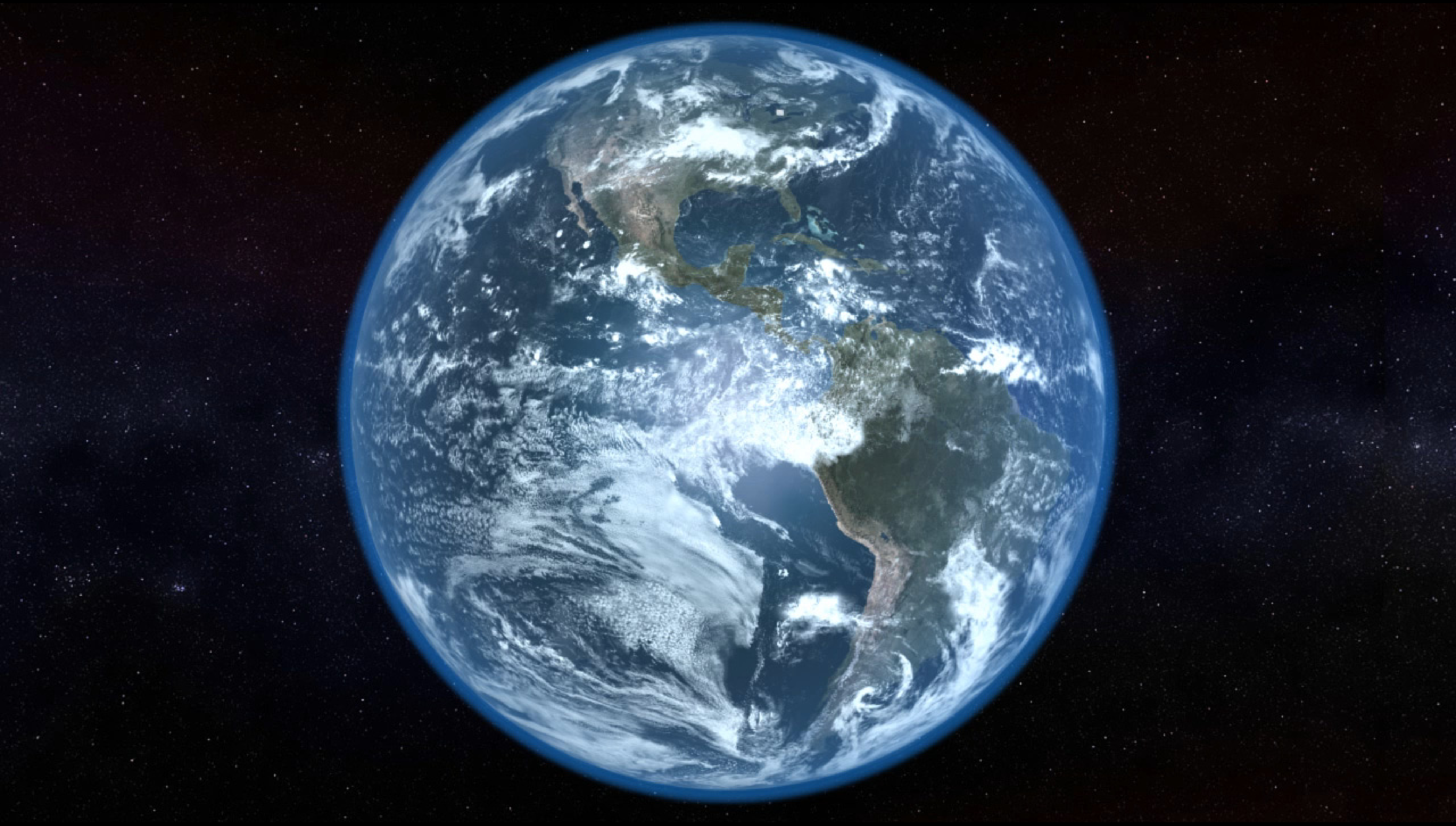
Trusted-node repeater



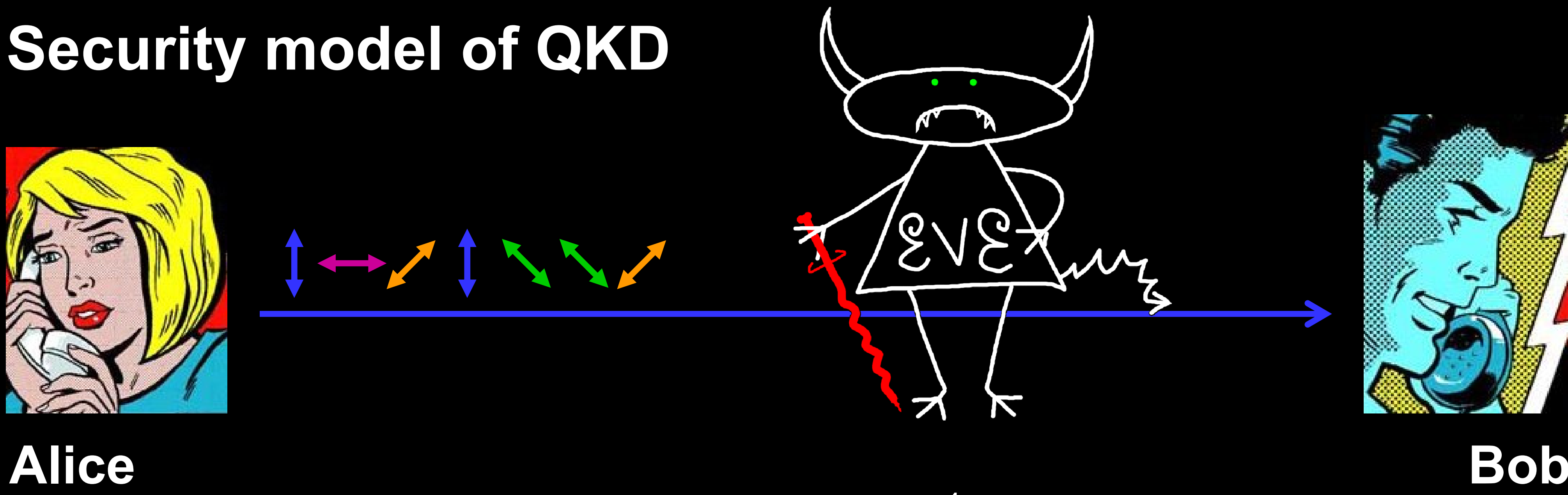
Trusted-node network



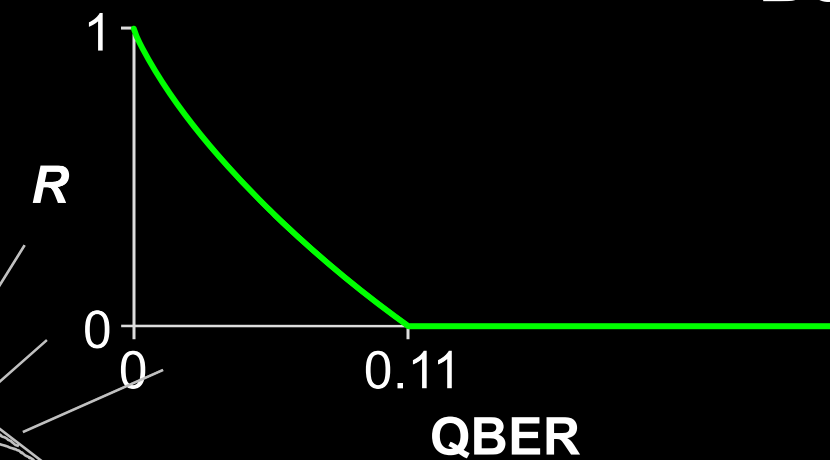
M. Sasaki et al., Opt. Express **19**, 10387 (2011)

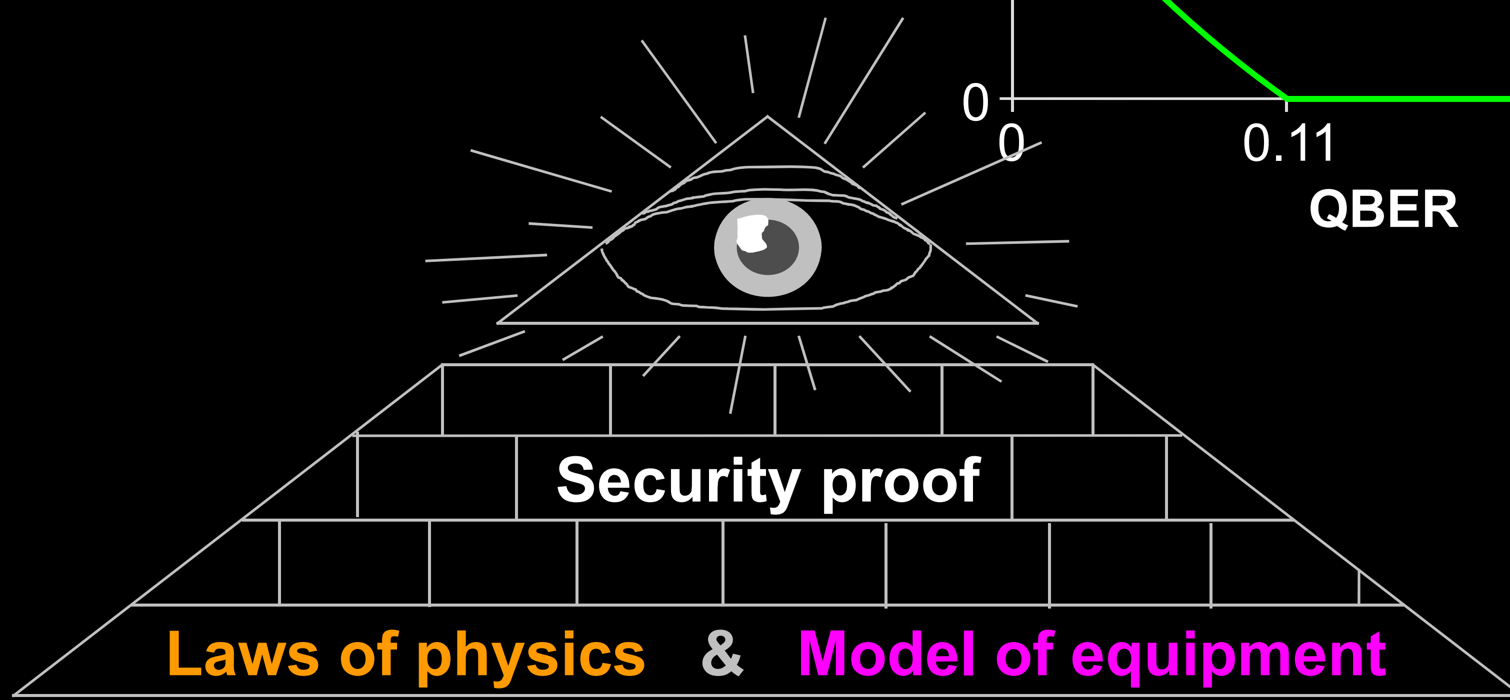


Security model of QKD

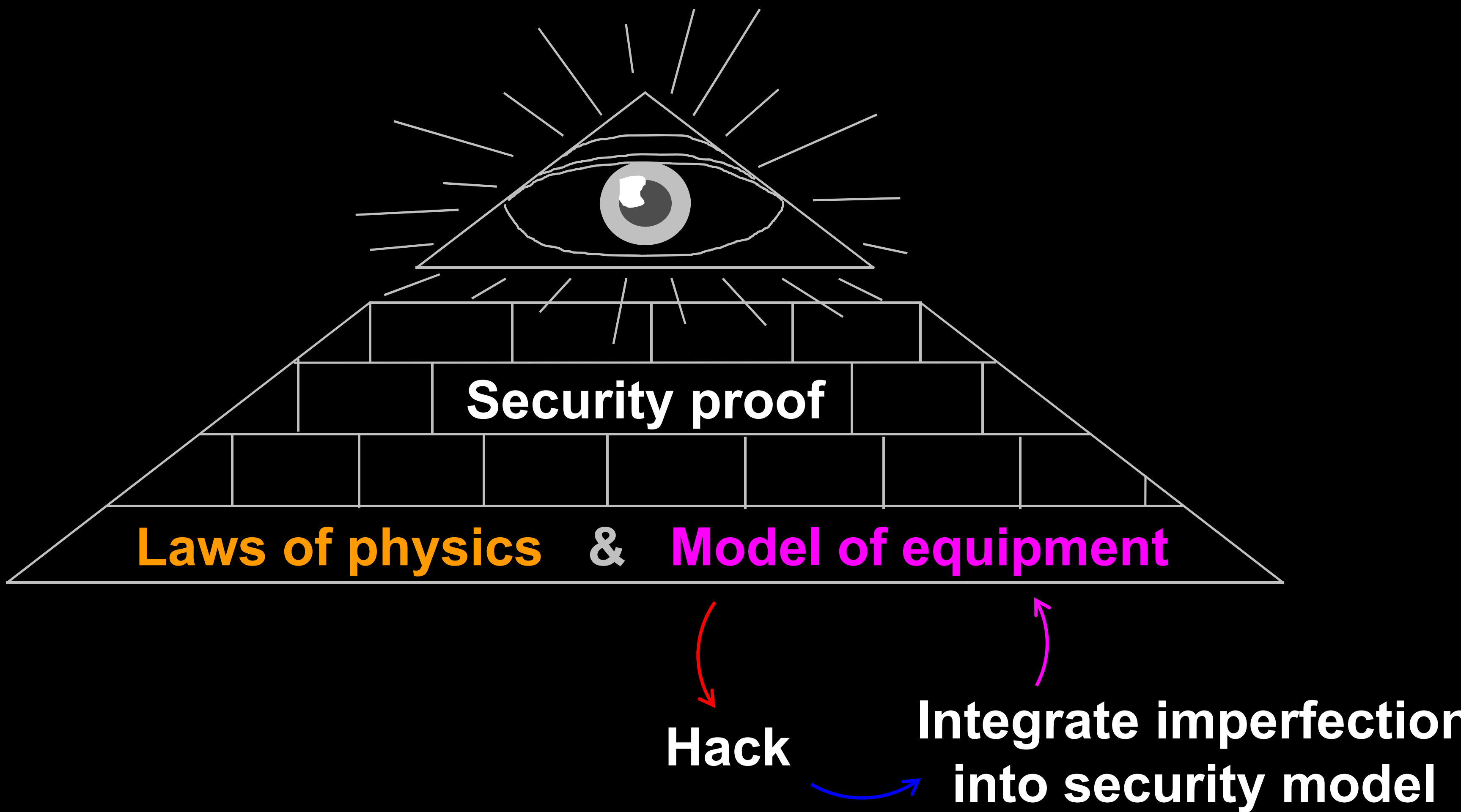


Secret key rate $R = f(\mathrm{QBER})$





Security model of QKD



Example of vulnerability and countermeasures

Photon-number-splitting attack

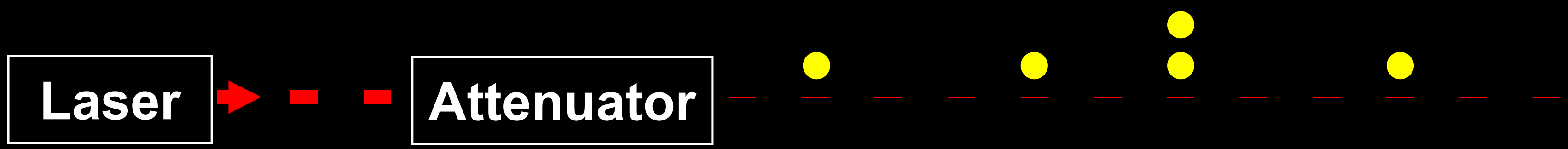
C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992)

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)

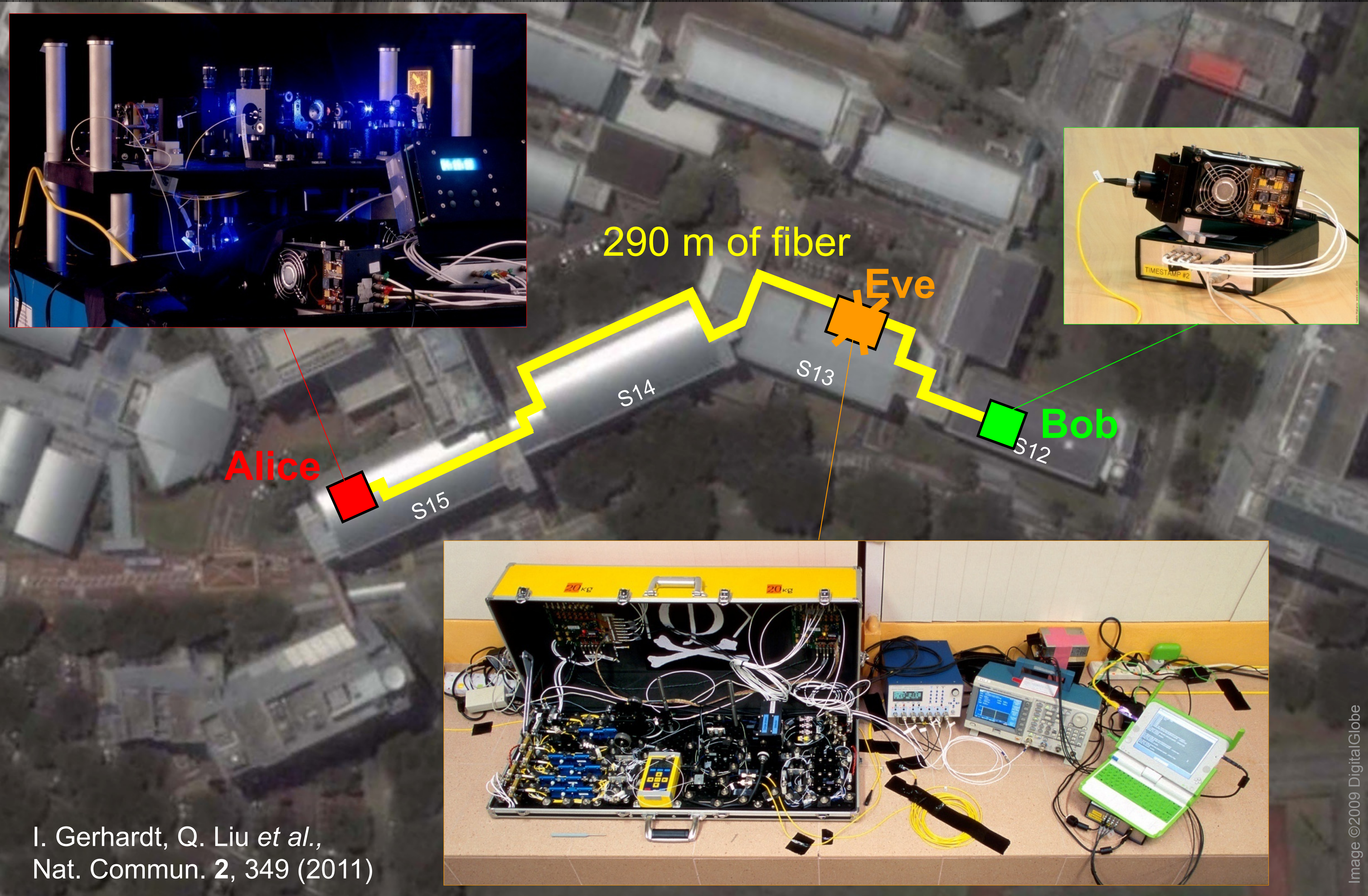
K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. A. **68**, 022317 (2003)

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

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)

2009

Responsible disclosure is important

Example: hacking commercial systems

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)

2010

MagiQ Technologies got a detailed vulnerability report

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

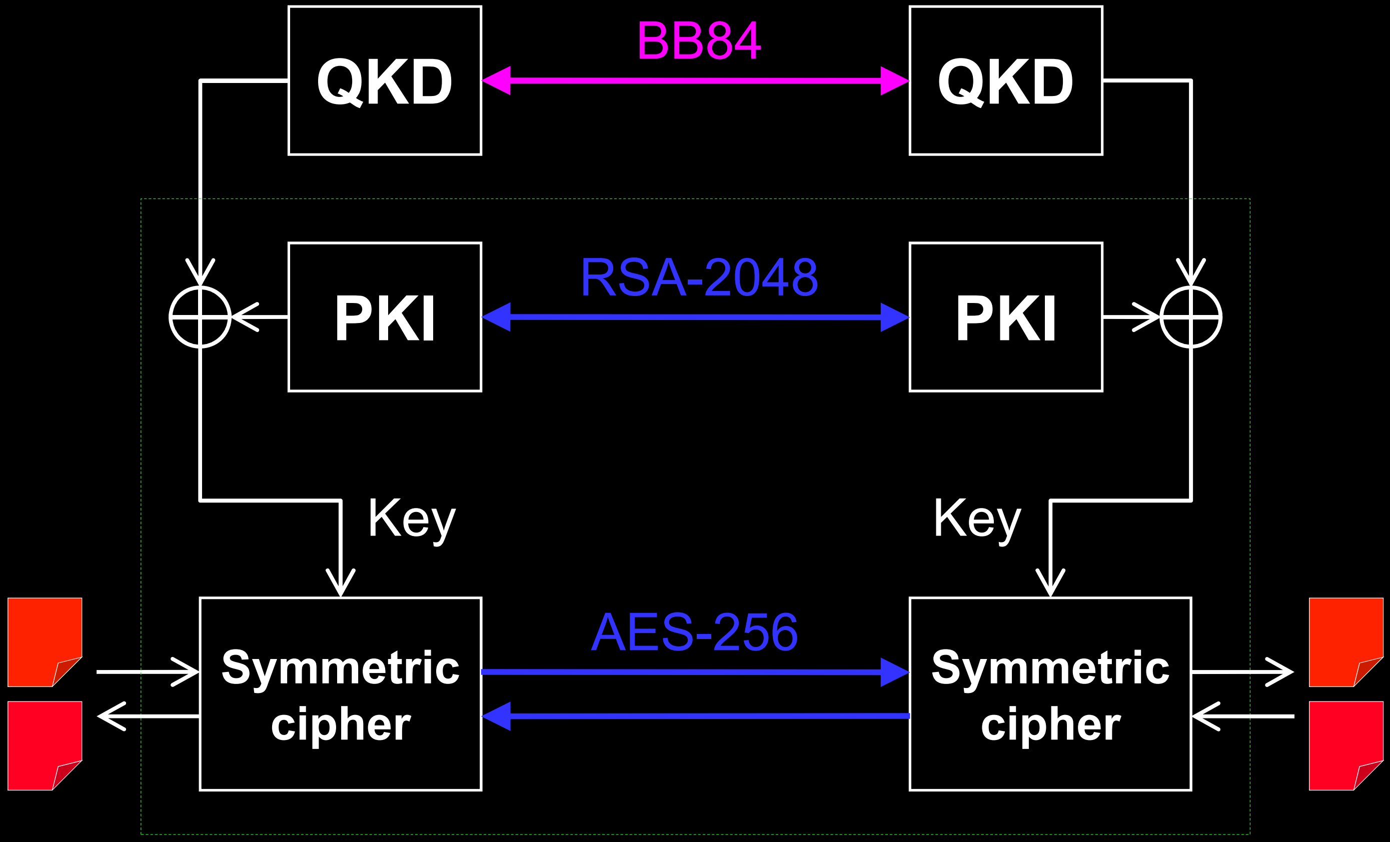
Results presented orally at a scientific conference

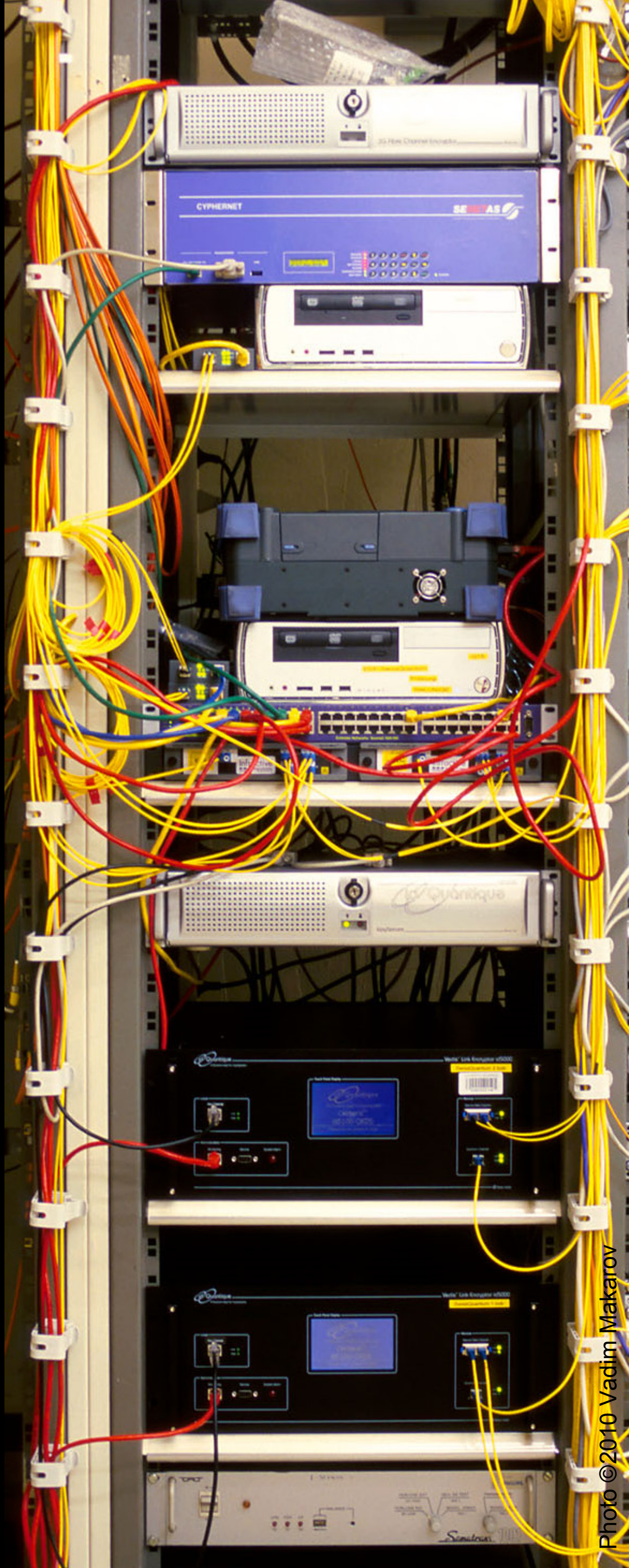
Public disclosure in a journal paper

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

Can we eavesdrop on commercial systems?

ID Quantique's Cerberis:
Dual key agreement





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

www.vad1.com/lab