Progress and challenges in quantum cryptography

Vadim Makarov
IQC Institute for Quantum Computing

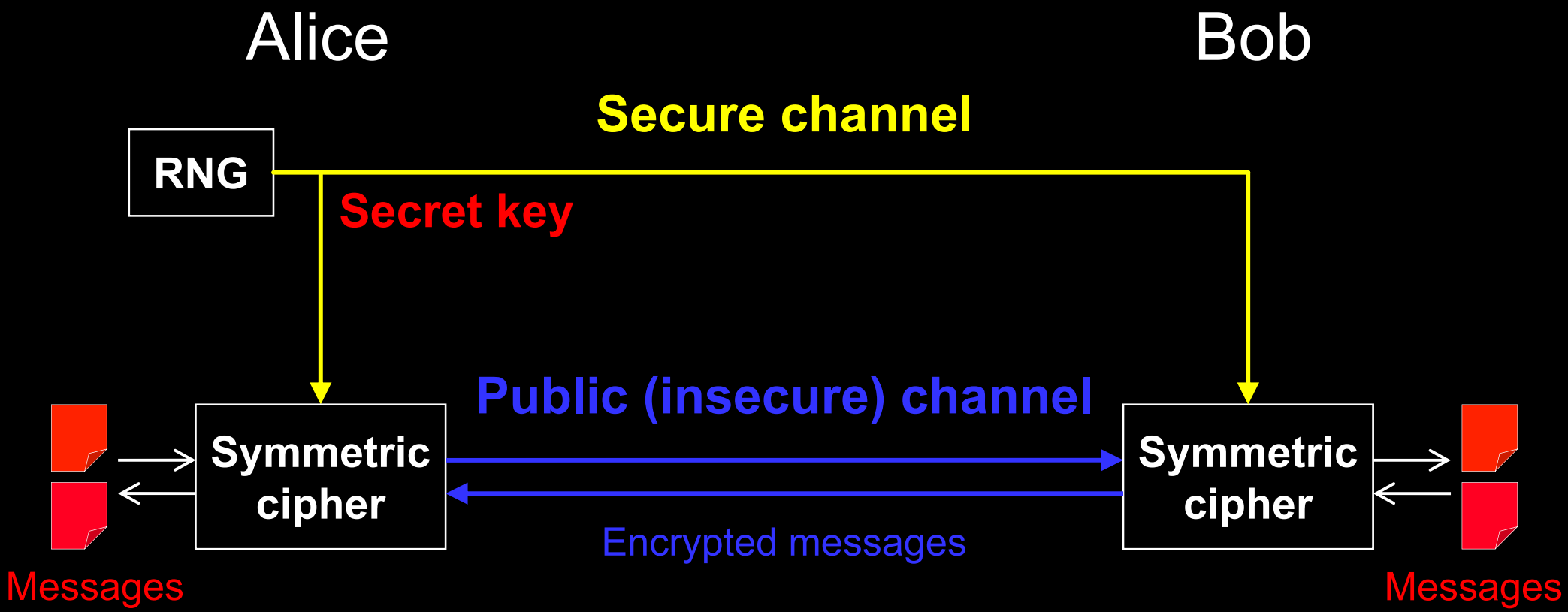
Talk at Telecom ParisTech, Paris, 10 July 2015

Image: street mural in Bucharest (fragment)

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, access control
- Government services (online or off-line)
- Medical records at your doctor, hospital
- Bypassing government surveillance and censorship
- Security cameras, industrial automation, military, spies...

Encryption and key distribution



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)

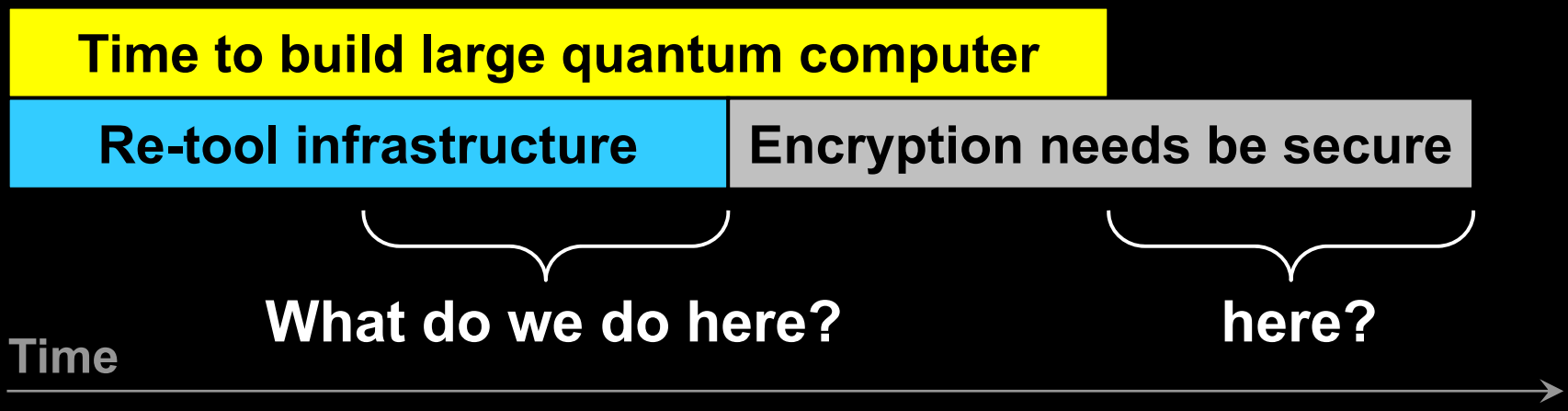


Diagram courtesy M. Mosca

How close is quantum computer?

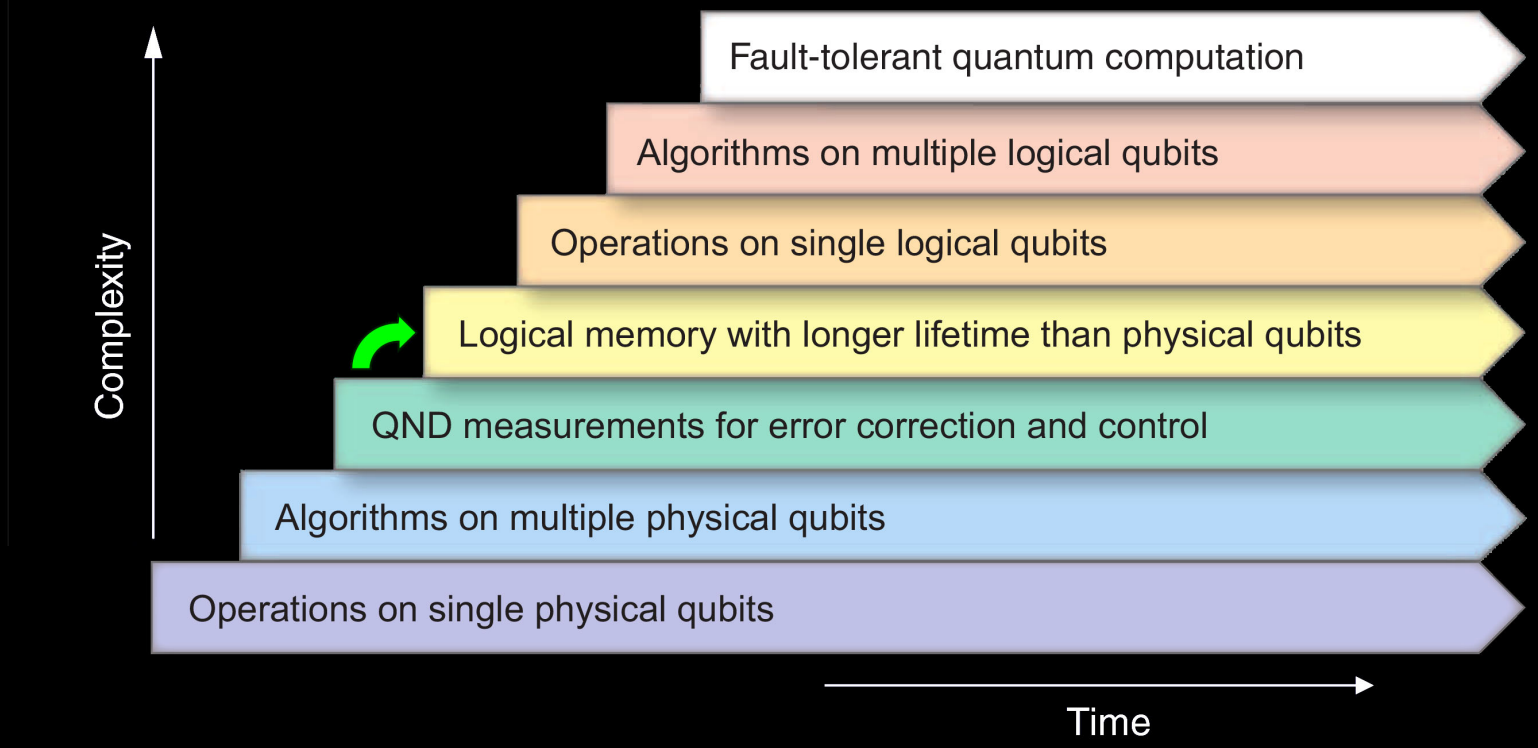


Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they now aim at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit components.

M. H. Devoret, R. J. Schoelkopf, "Superconducting circuits for quantum information: An outlook," Science **339**, 1169 (2013)

How close is quantum computer?

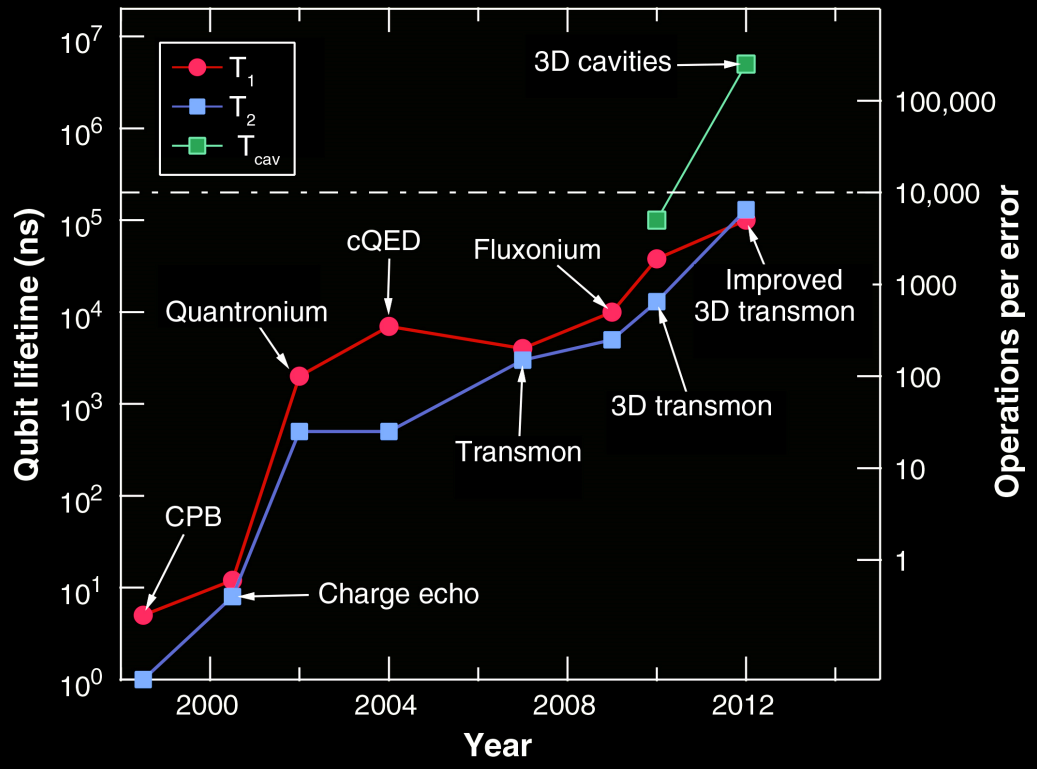


Fig. 3. Examples of the "Moore's law" type of exponential scaling in performance of superconducting qubits during recent years. Improvement of coherence times for the "typical best" results associated with the first versions of major design changes. The blue, red, and green symbols refer to qubit relaxation, qubit decoherence, and cavity lifetimes, respectively. Innovations were introduced to avoid the dominant decoherence channel found in earlier generations. So far an ultimate limit on coherence seems not to have been encountered.

M. H. Devoret, R. J. Schoelkopf, Science **339**, 1169 (2013)

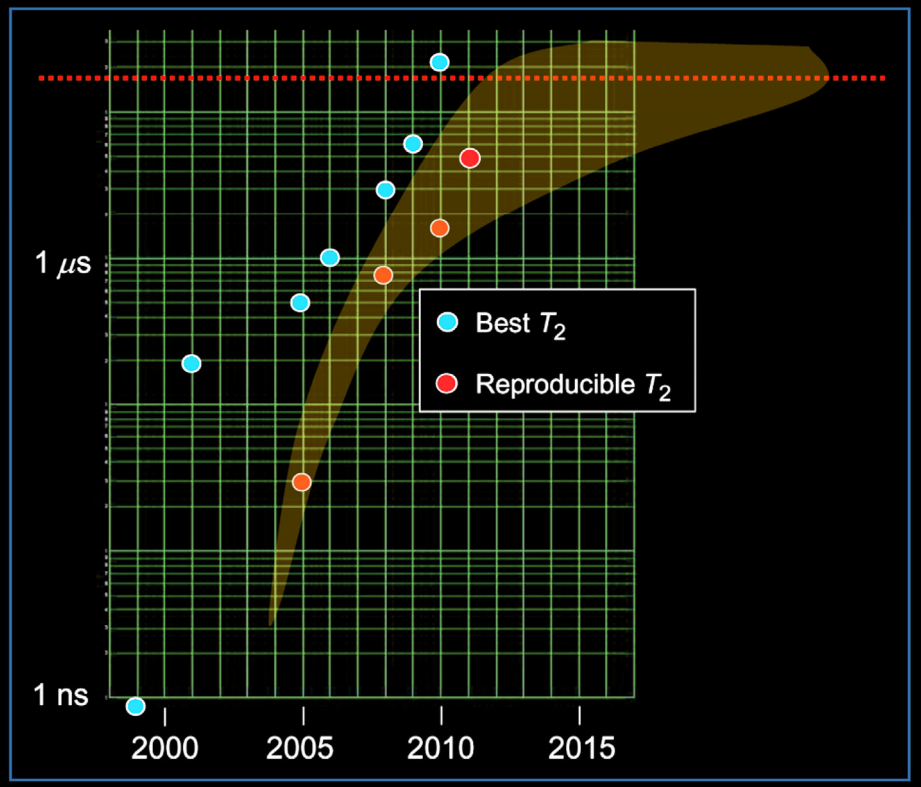


Figure 5

Progress toward reaching long dephasing (T_2) times for superconducting qubits. (Red dashed line) Minimum necessary for fault-tolerant quantum computer, based on a 30-ns two-gate time. (Yellow field) Predicted improvements in T_2.

M. Steffen *et al.*, "Quantum computing: An IBM perspective," IBM J. Res. Dev. **55**, 13 (2011)

Quantum computers capable of catastrophically breaking our public-key cryptography infrastructure are a medium-term threat.

Quantum-safe cryptographic infrastructure

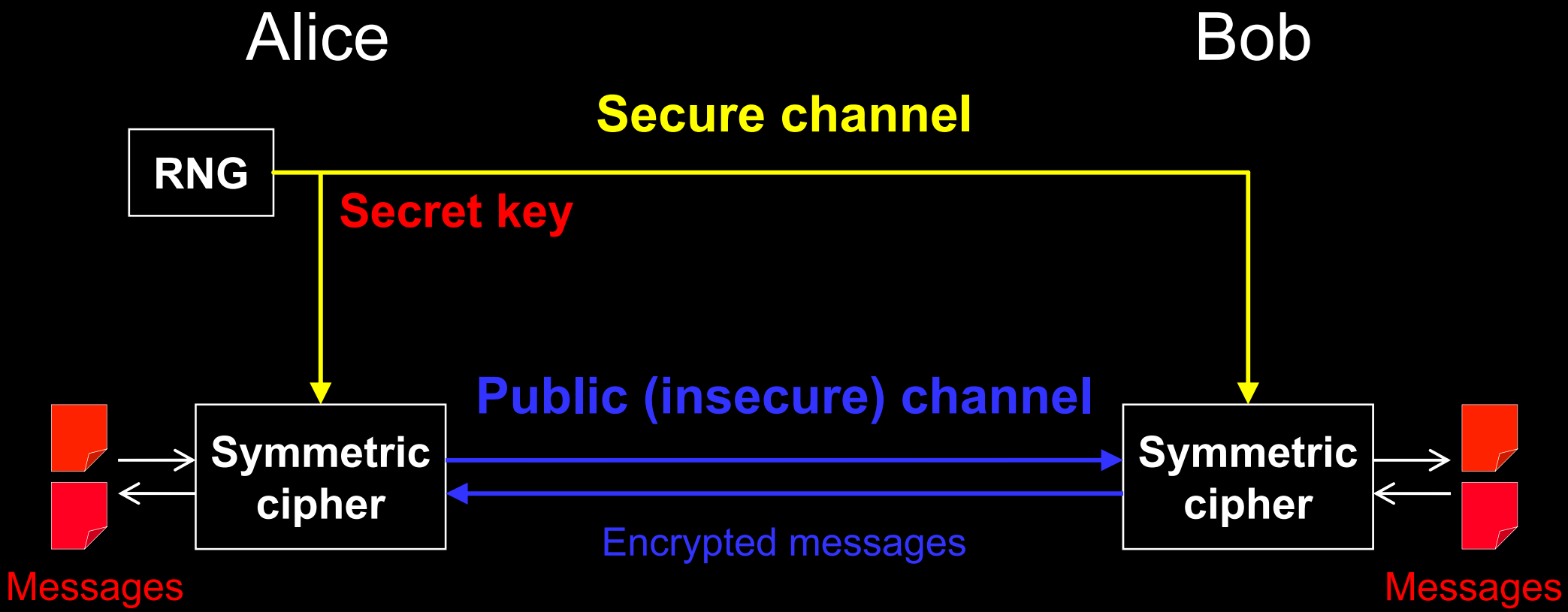
"post-quantum" cryptography + quantum cryptography

- **Classical codes deployable without quantum technologies**
- **Believed/hoped to be secure against quantum computer attacks of the future**
- **Quantum codes requiring some quantum technologies (typically less than a large-scale quantum computer)**
- **Typically no computational assumptions and thus known to be secure against quantum attacks**

Both sets of cryptographic tools can work very well together in quantum-safe cryptographic ecosystem.

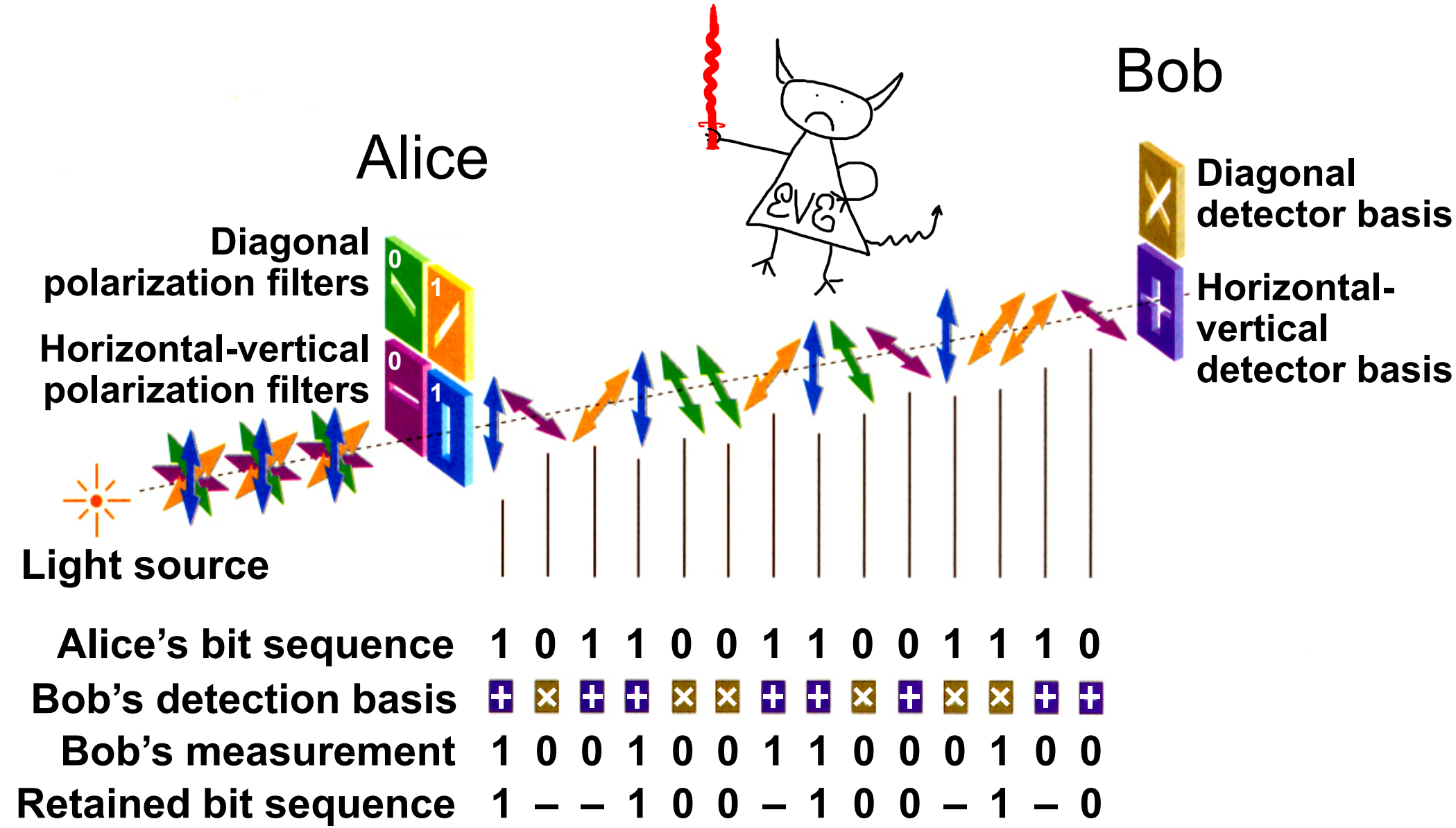
Slide courtesy M. Mosca

Encryption and key distribution



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

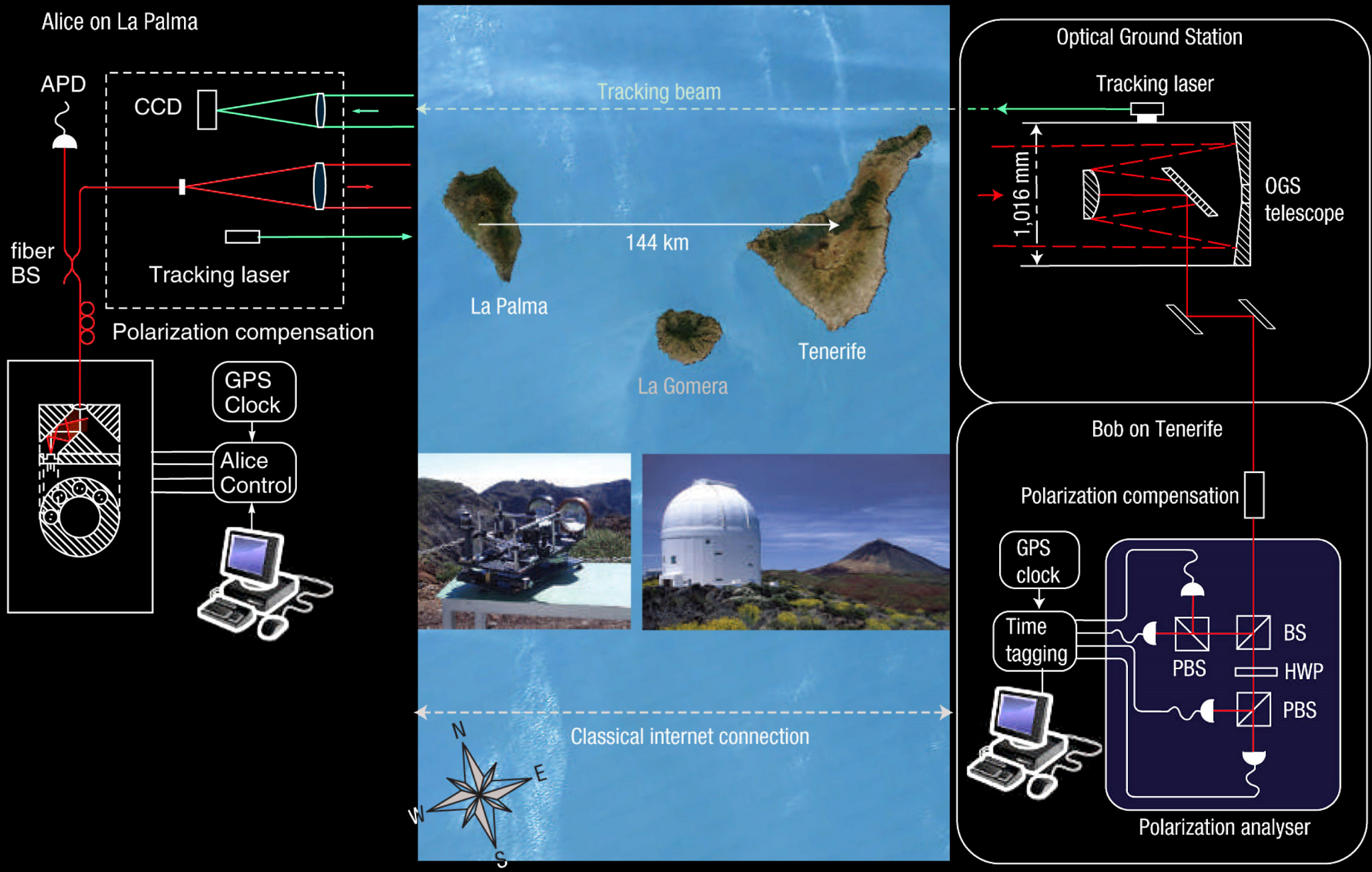
Quantum key distribution (QKD)



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

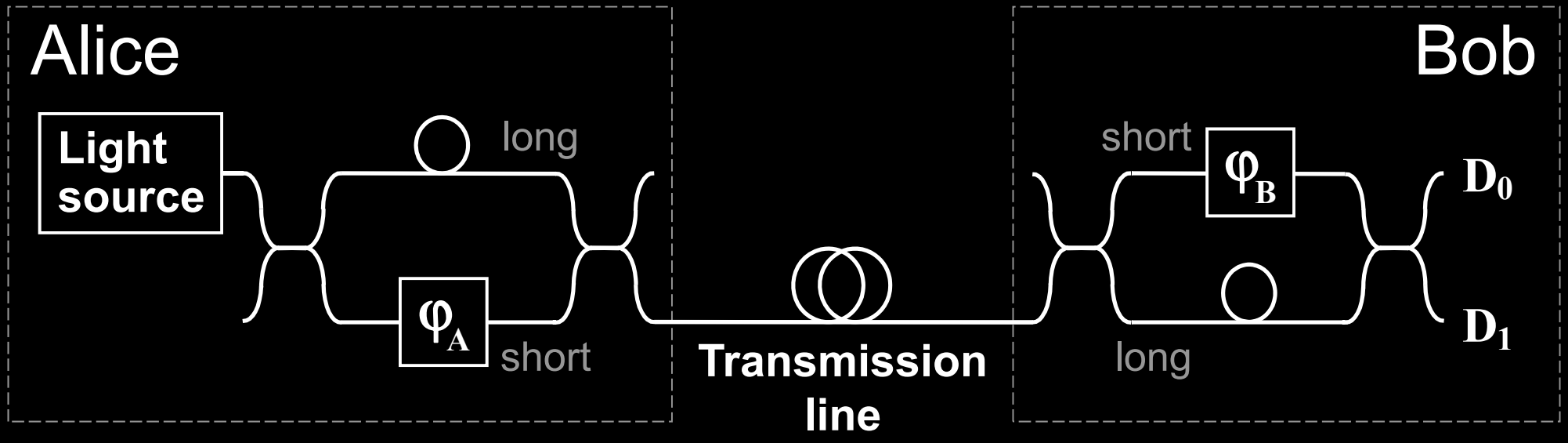
Image reprinted from article: W. Tittel, G. Ribordy & N. Gisin, "Quantum cryptography," Physics World, March 1998

Free-space QKD over 144 km



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

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

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)

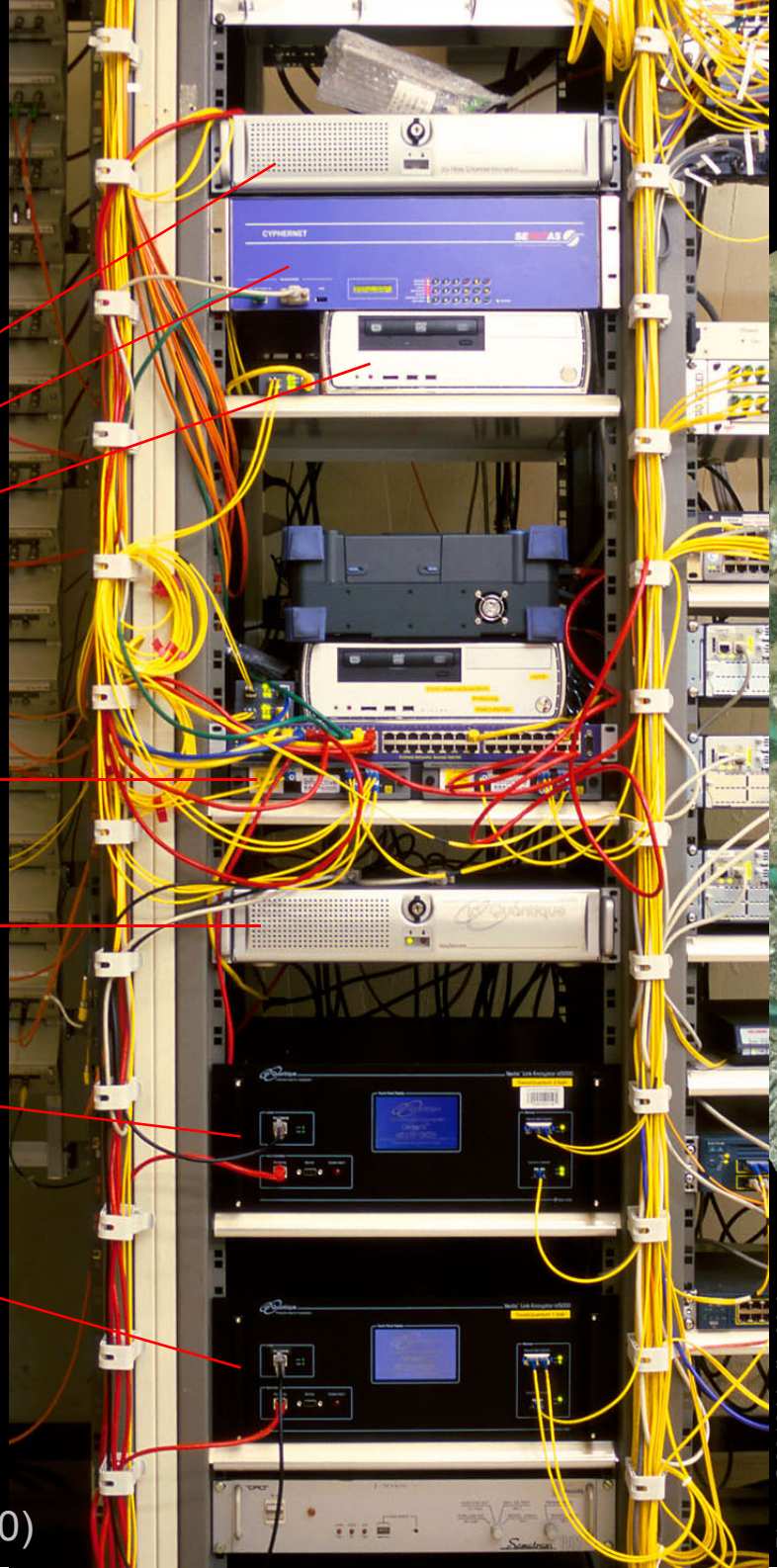
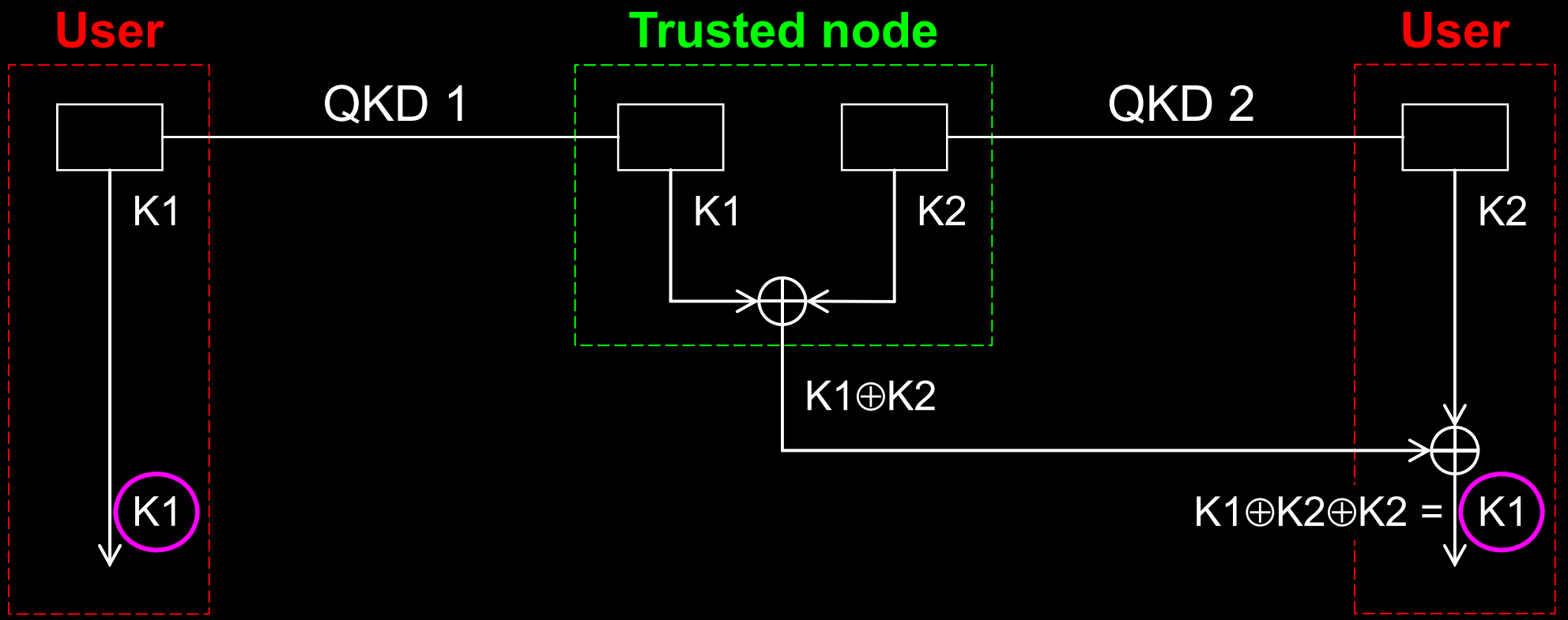


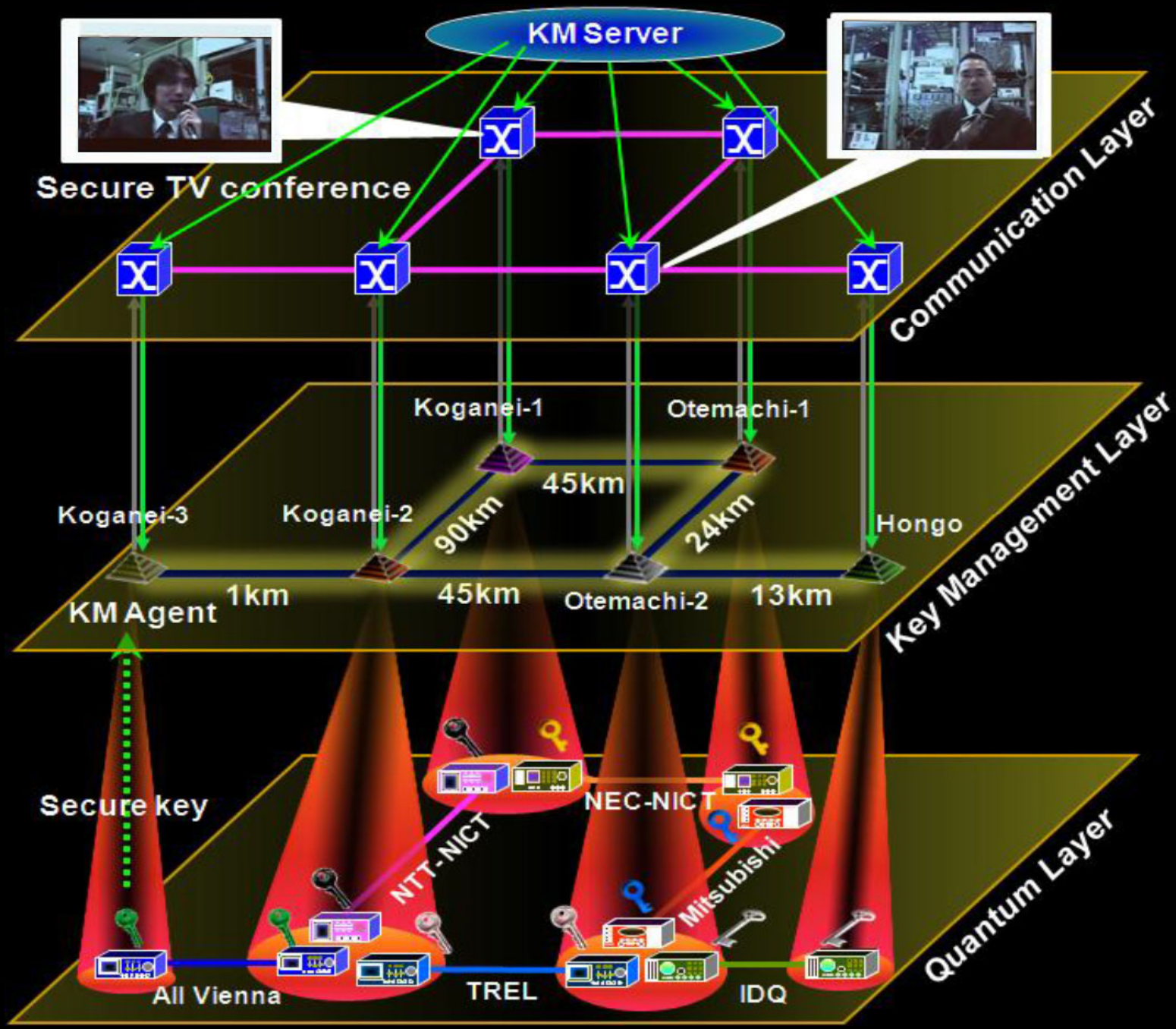
Photo ©2010 Vadim Makarov

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

Trusted-node repeater



Trusted-node network



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

Quantum Backbone

- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes

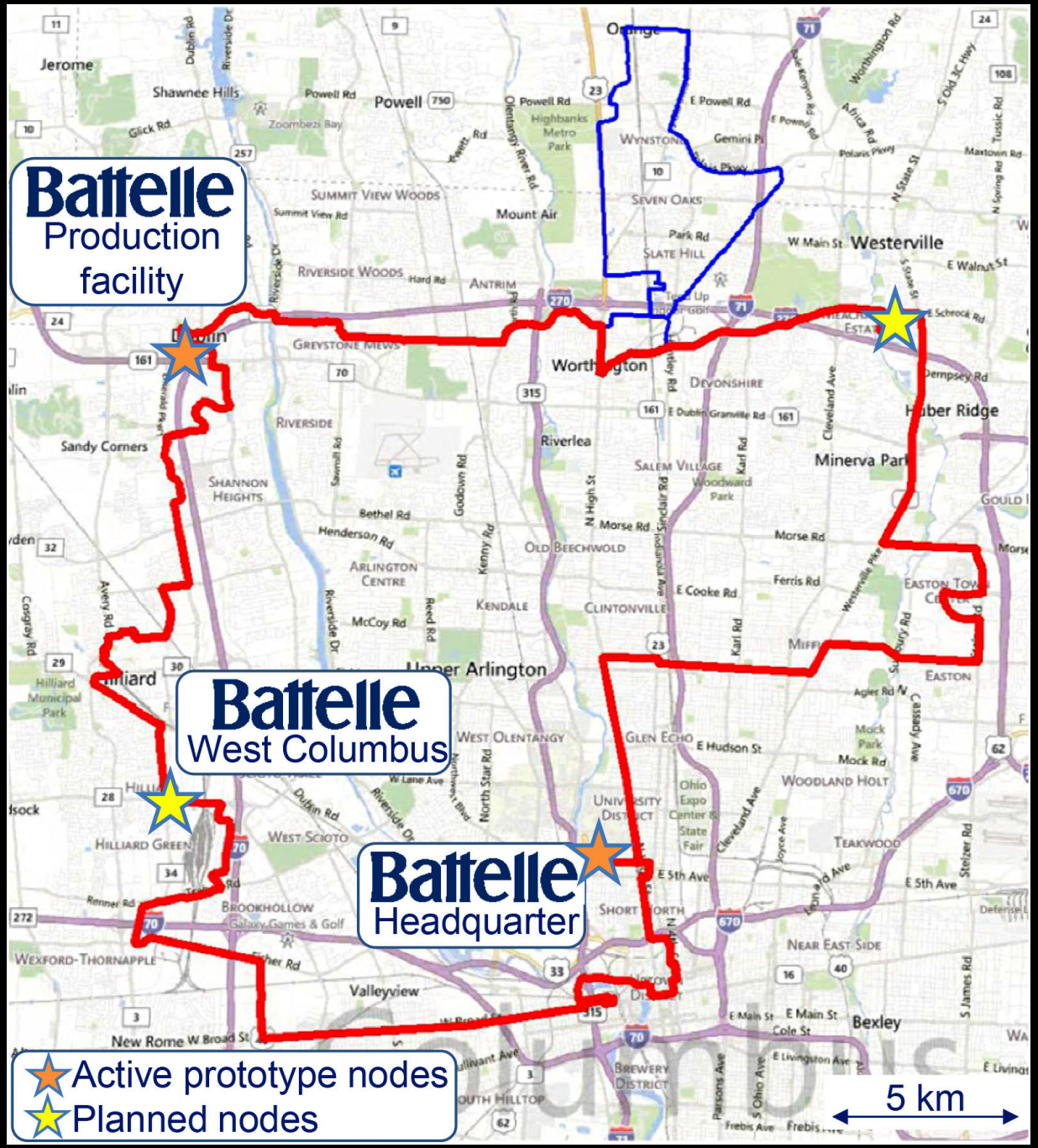
  31 fiber links
- Metropolitan networks

  Existing: Hefei, Jinan

  New: Beijing, Shanghai
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC

Q. Zhang, talk at QCrypt 2014

The Battelle quantum network

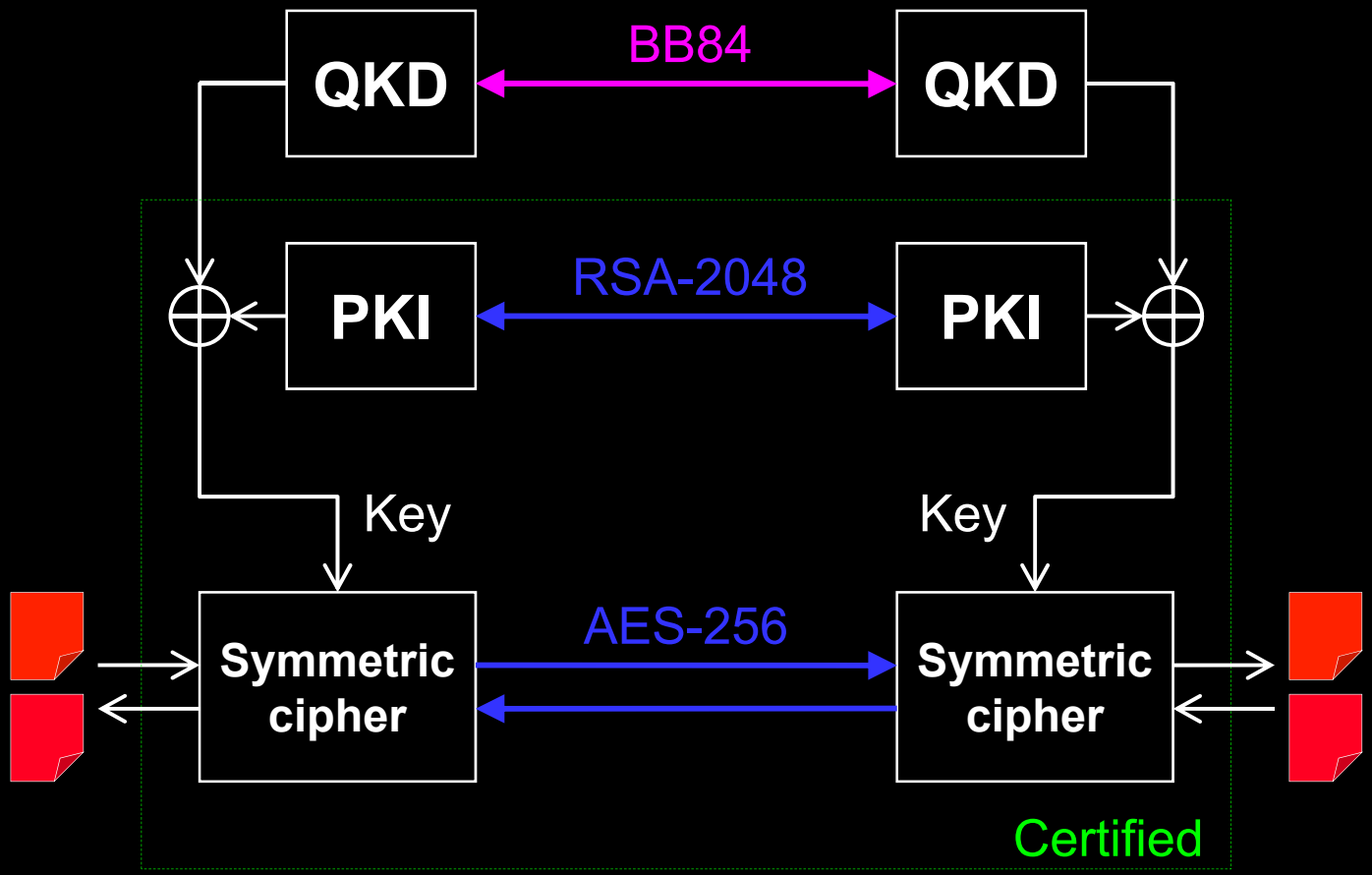


Plans:

N. Walenta *et al.*, poster at QCrypt 2014

Video ©2012 IQC / group of T. Jennewein

Dual key agreement



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

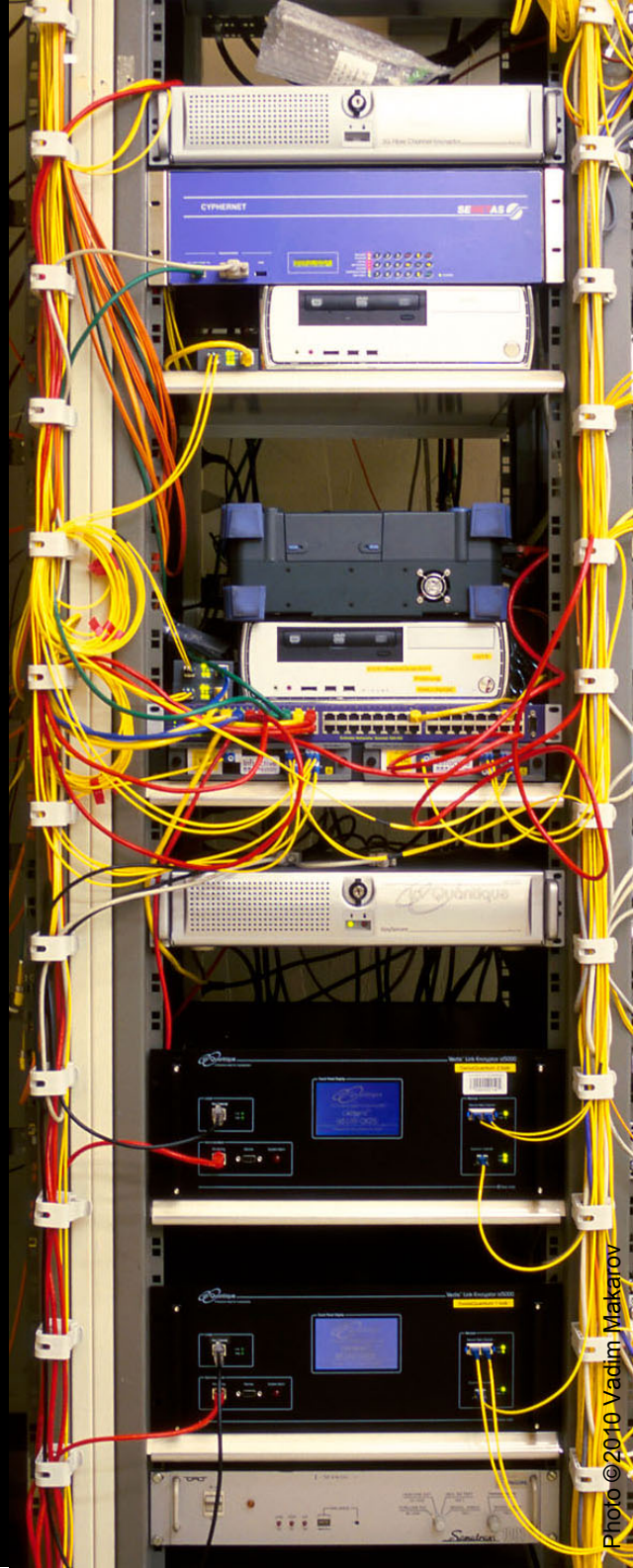


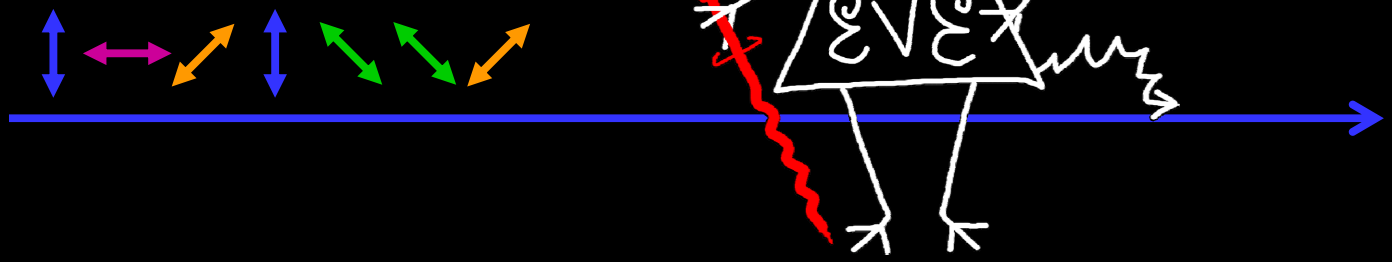
Photo © 2010 Vadim Makarov

Cryptography: classical vs. quantum

	Unproven mathematical assumptions	Laws of physics
Based on...		
Convenient to implement?	**Yes**	**No**
Forward secure?	**No**	**Yes**
Authenticate via PKI?	**Yes**	**Yes**
Loopholes in implementations?	**Yes**	**Yes**
Exploitable retroactively?	Sometimes	**No***

* Single exception: A. Lamas-Linares & C. Kurtsiefer, Opt. Express **15**, 9388 (2007)

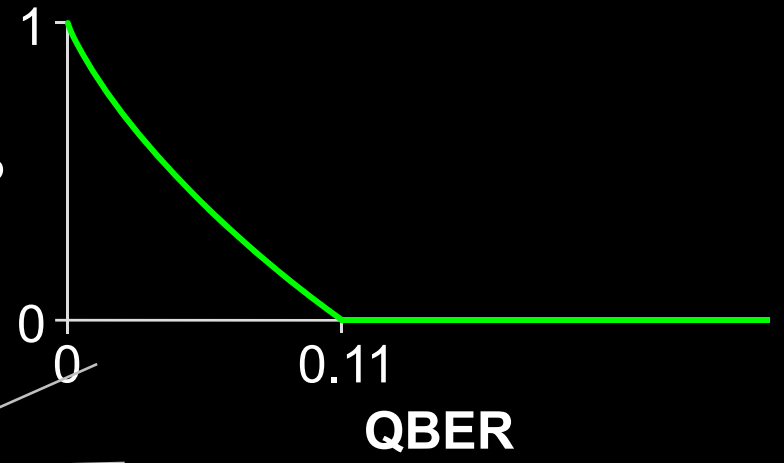
Security model of QKD

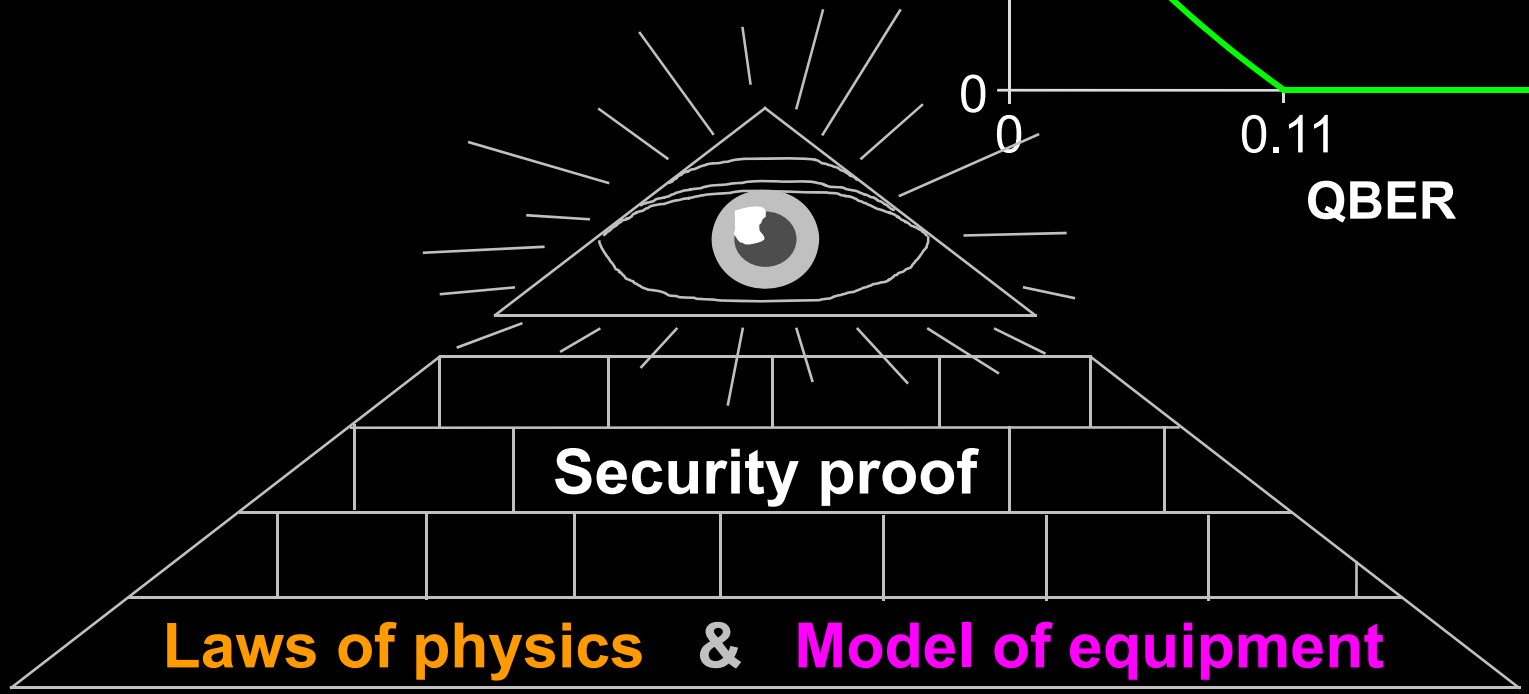


Alice

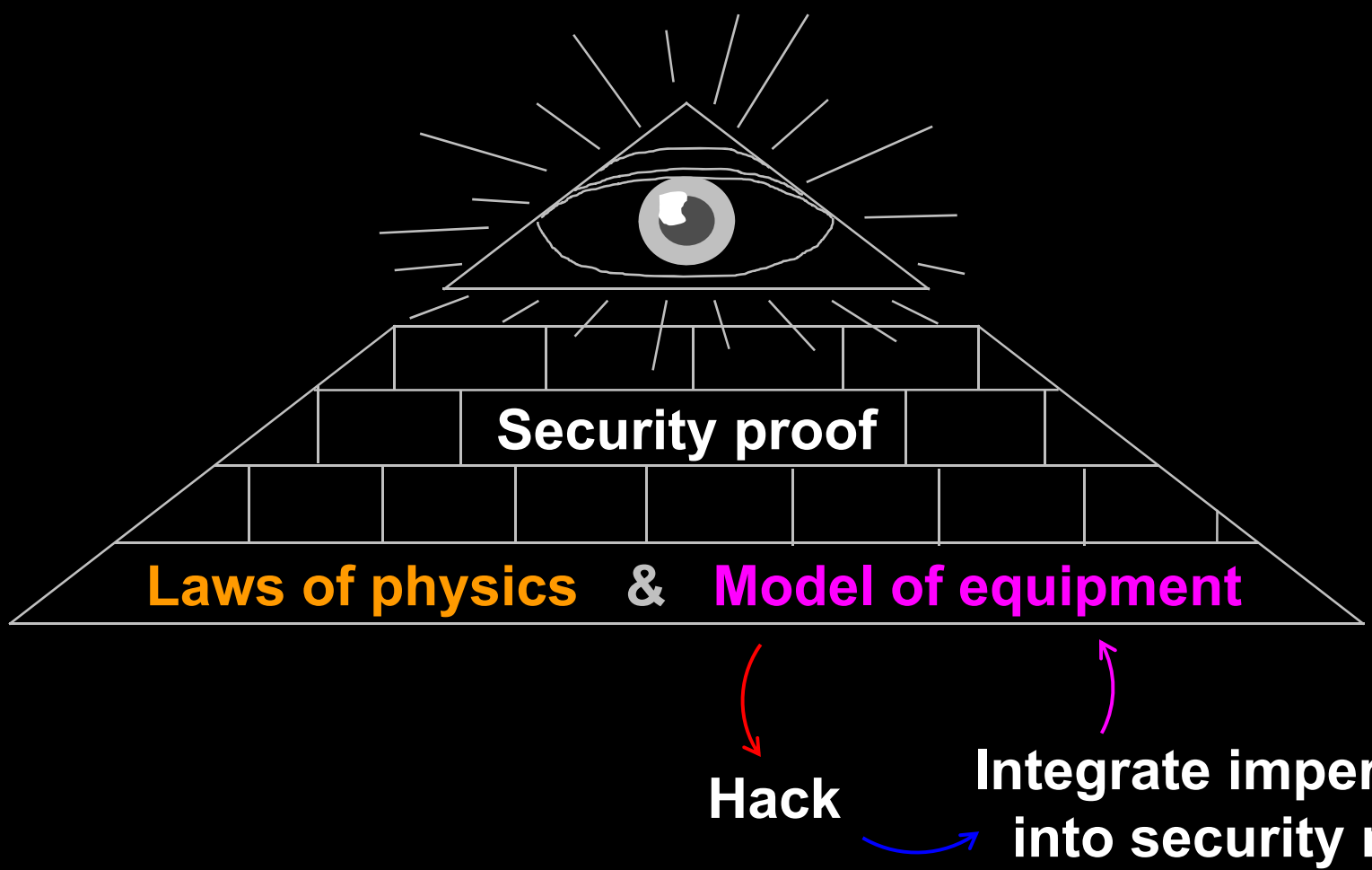
Bob

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





Security model of QKD



Attack	Target component	Tested system
Spatial efficiency mismatch M Rau *et al.,* IEEE J. Quantum Electron. **21**, 6600905 (2015); S. Sajeed *et al.,* Phys. Rev. A **91**, 062301 (2015)	receiver optics	research system
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)	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 system
Phase-remapping F. Xu, B. Qi, H.-K. Lo, New J. Phys. **12**, 113026 (2010)	phase modulator in Alice	ID Quantique*

* Attack did not break security of the tested system, but may be applicable to a different implementation.

Example 1: academic

Photon-number-splitting attack

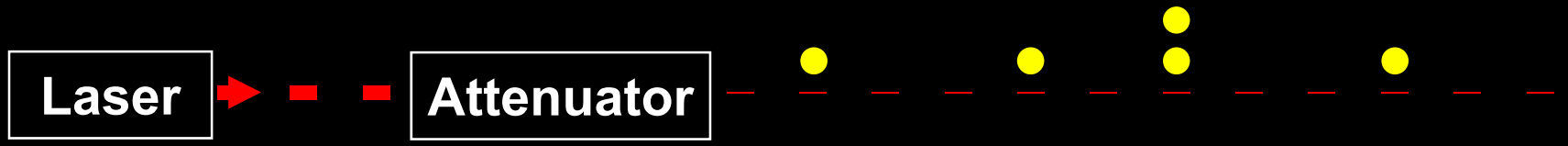
C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992)

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)

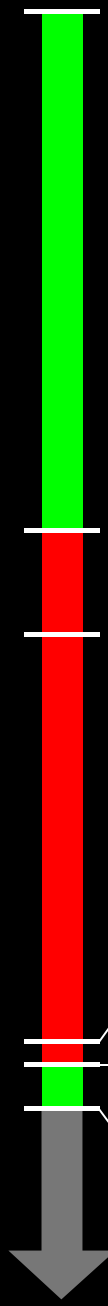
★ Distributed-phase-reference protocols

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)

Example 2: industrial (ID Quantique)



2004-11-10 — First commercial Clavis1 system is shipped to a customer

2009-10-22 — Report about detector blinding attack sent to company

2010-10-08 — Company applies for a patent on randomization of detector efficiency as a countermeasure

Lim *et al.* preprint about the countermeasure arXiv:1408.6398

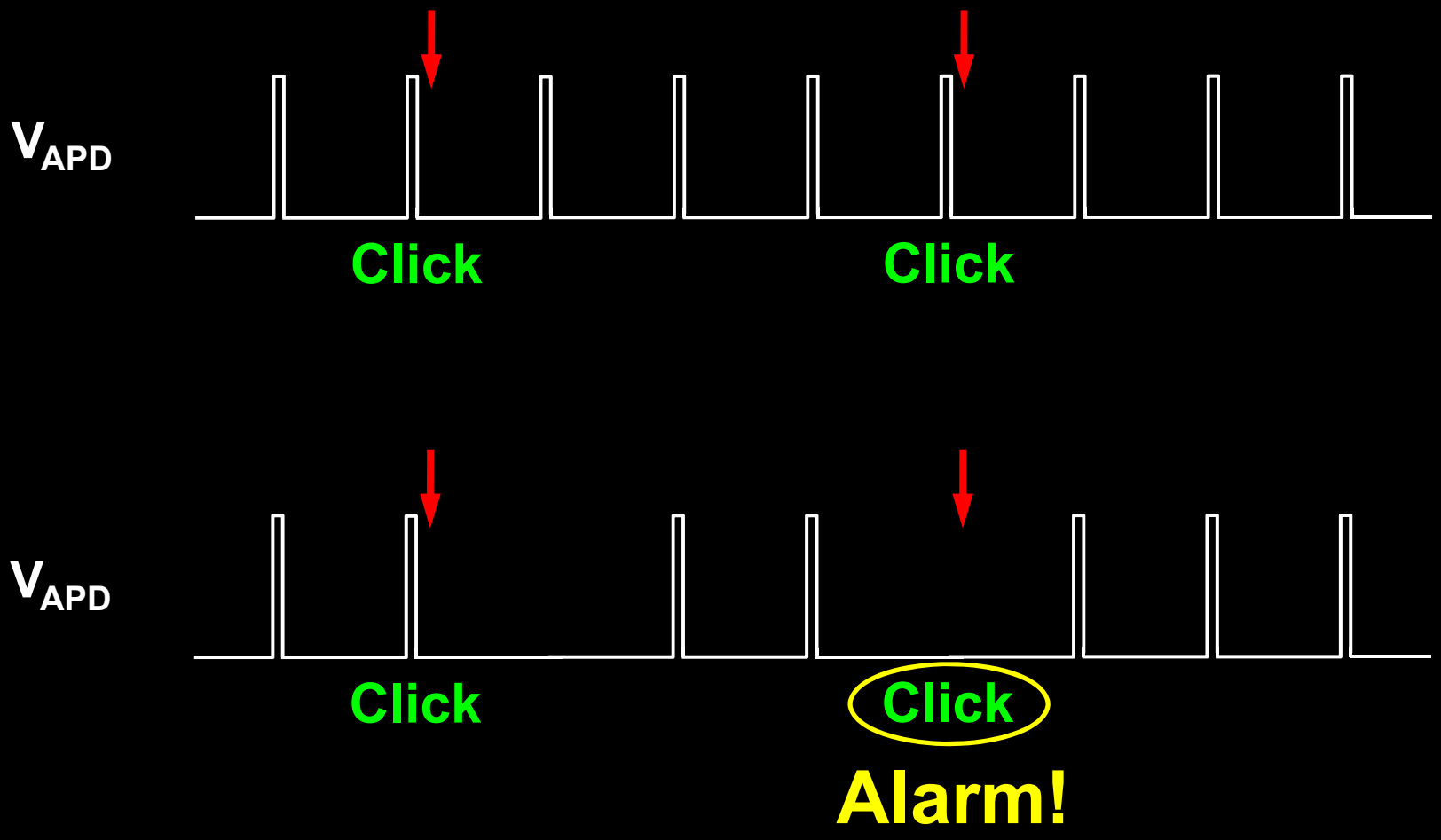
2014-08-27 — ★ Implementation of countermeasure delivered by company to our lab (firmware update for Clavis2)

2014-11-18

2015-04-17 — ? Countermeasure testing report sent to company

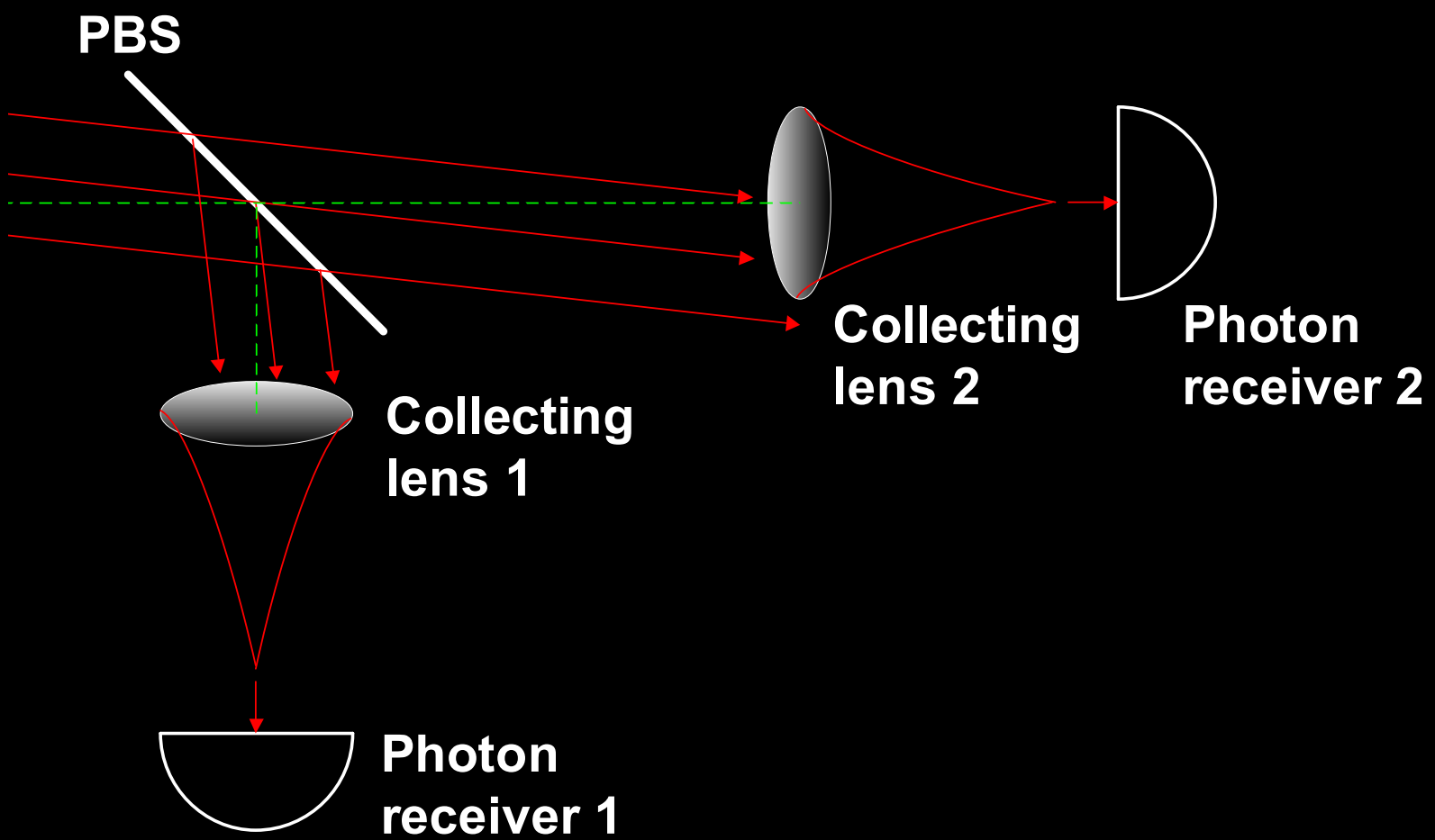
A. Huang *et al.*, unpublished

Randomly varying detector sensitivity
(ID Quantique)



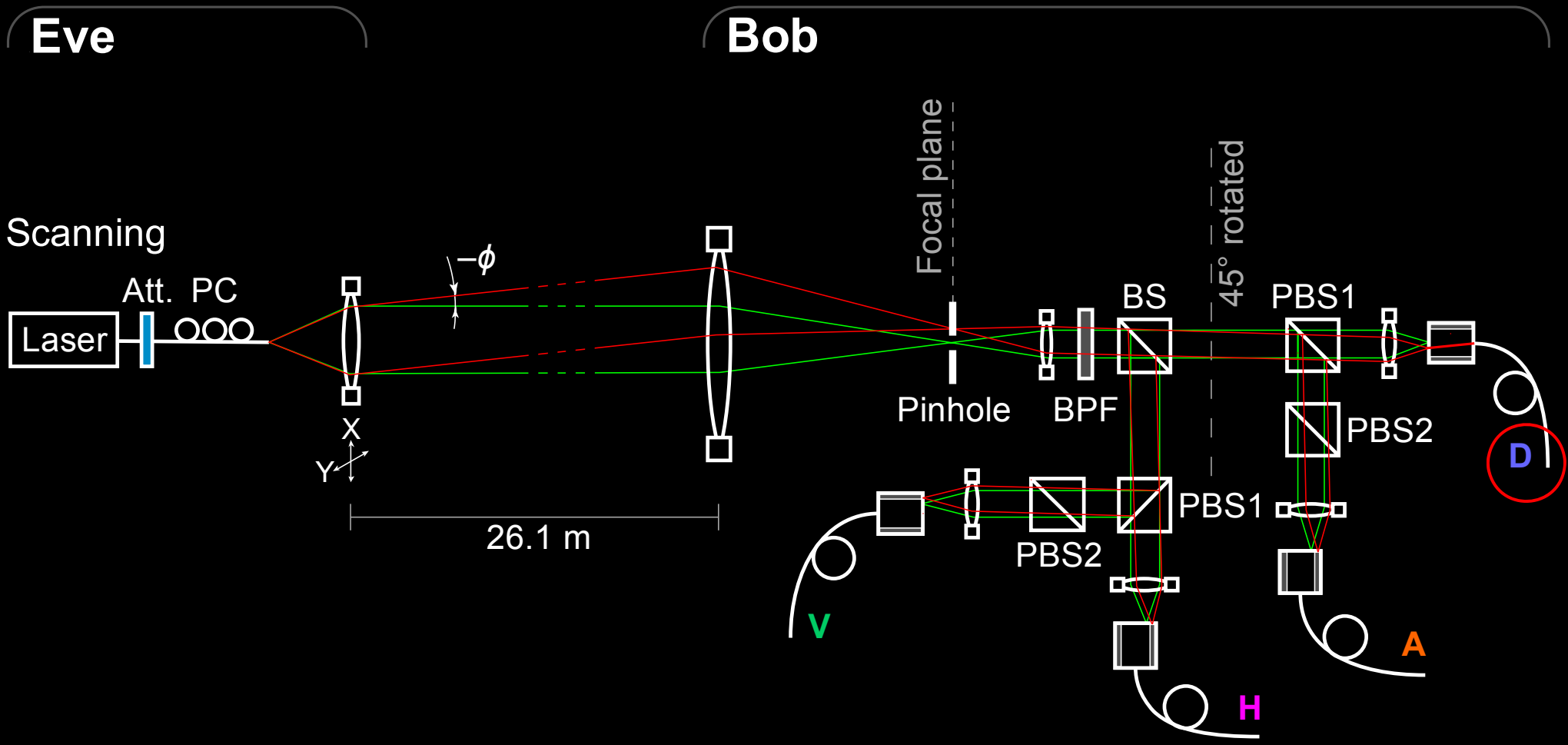
C. C. W. Lim *et al.*, arXiv:1408.6398
M. Legre, G. Robordy, Intl. patent appl. WO 2012/046135 A2 (filed in 2010)

Example 3: academic. Efficiency mismatch



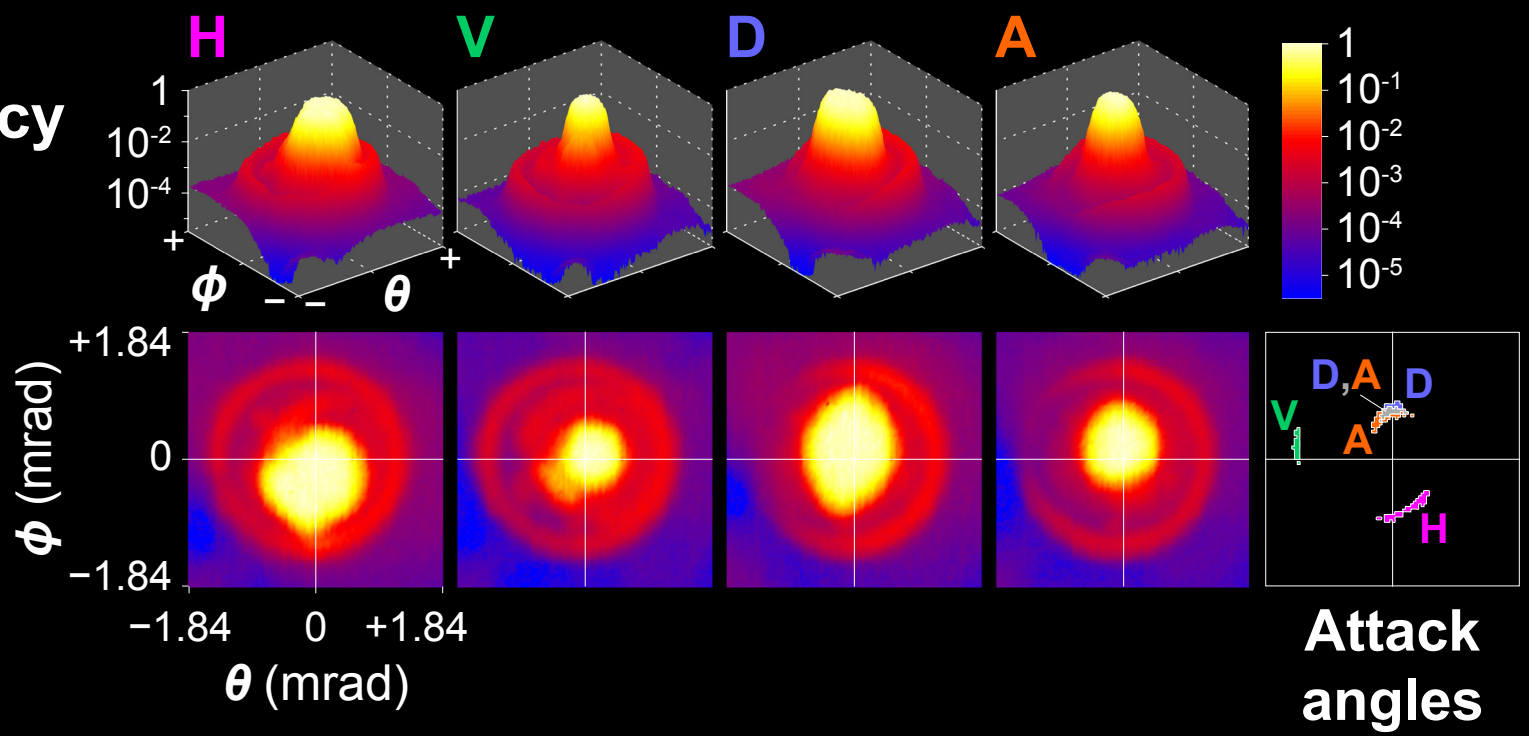
C.-H. F. fung *et al.,* Quantum Inf. Comput. **9**, 0131 (2009)

Efficiency mismatch in QKD receiver



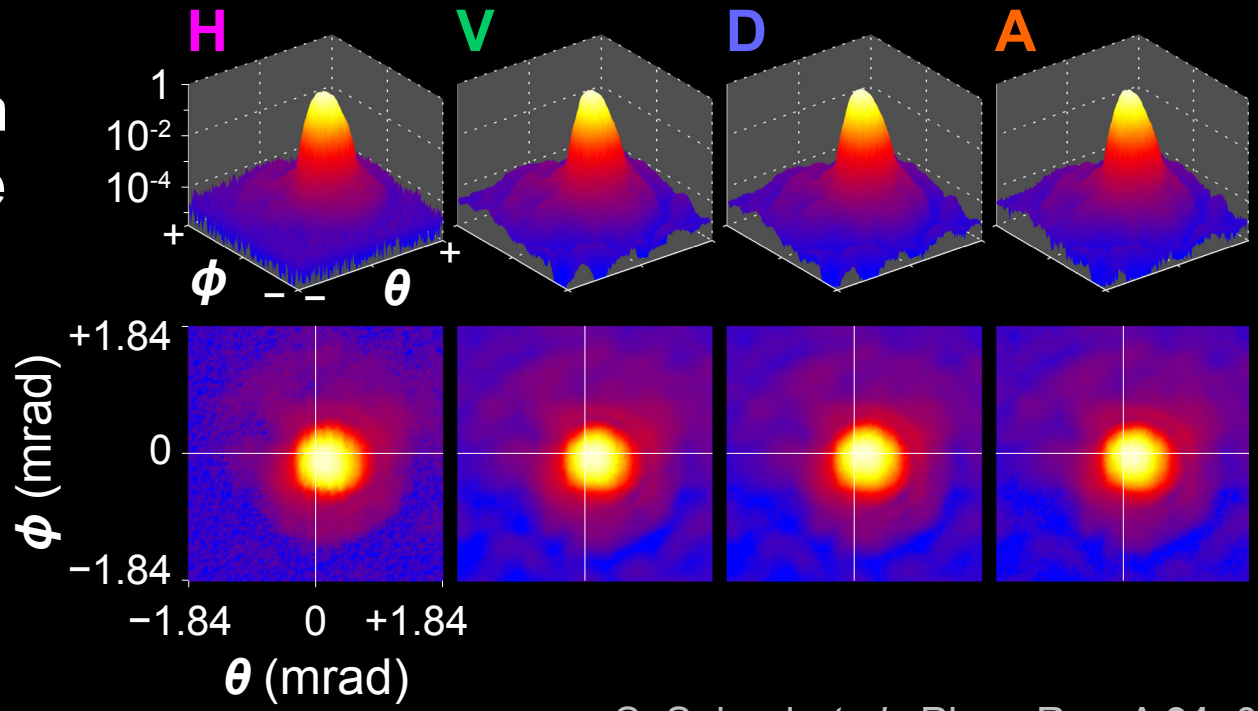
S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015).

Detector efficiency without pinhole



Attack angles

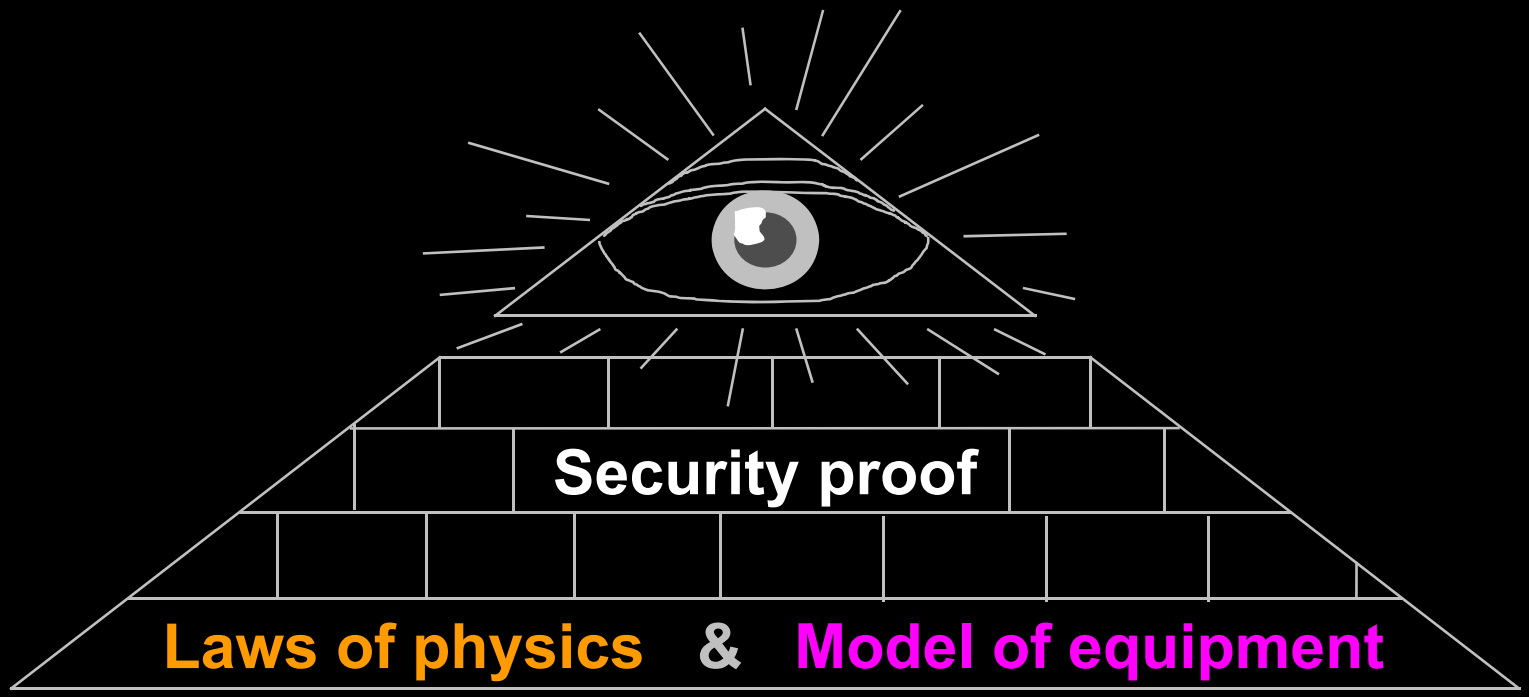
...and with 25 μm diameter pinhole



No attack found

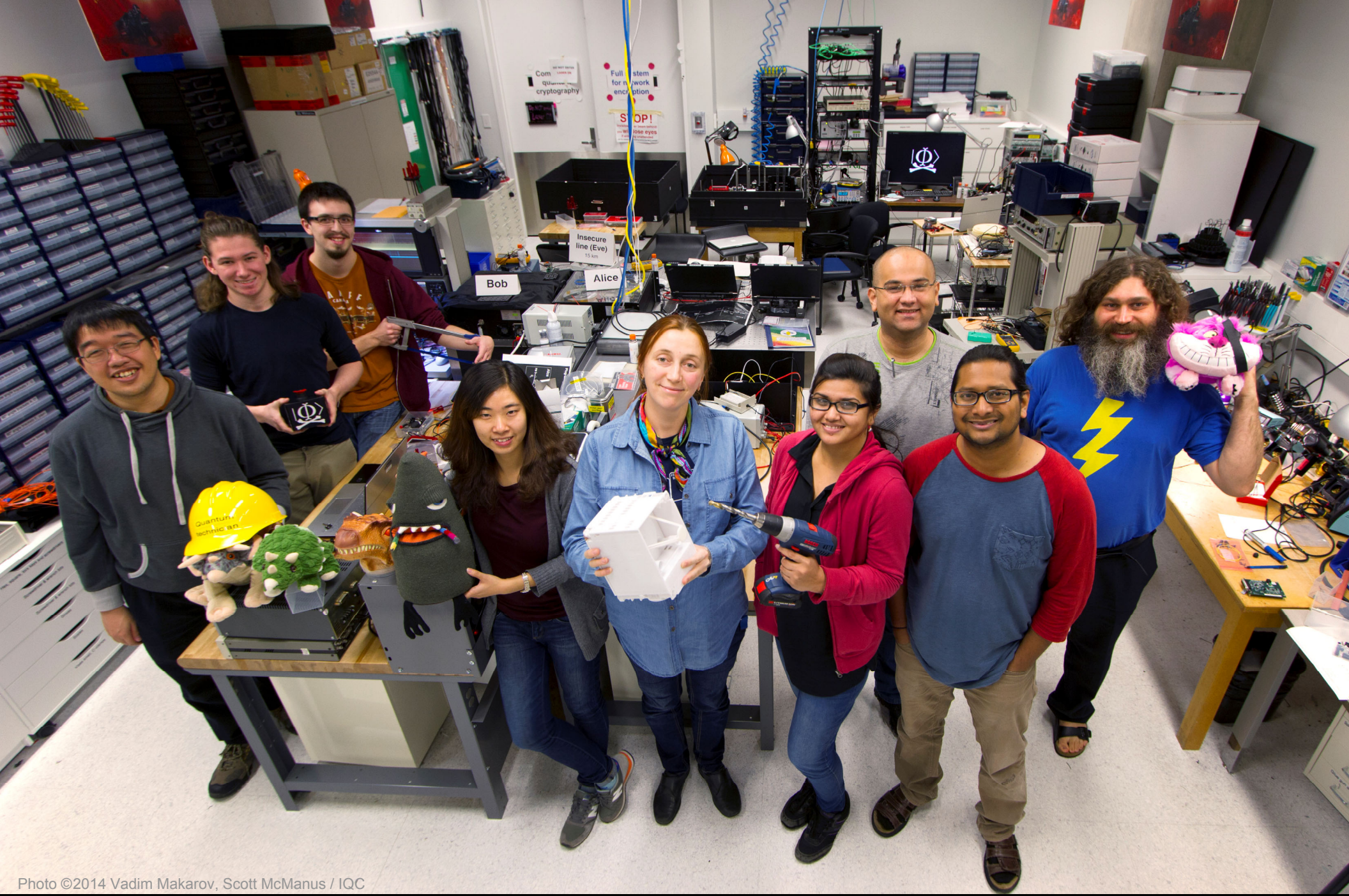
S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015).

Security model of QKD



Hack

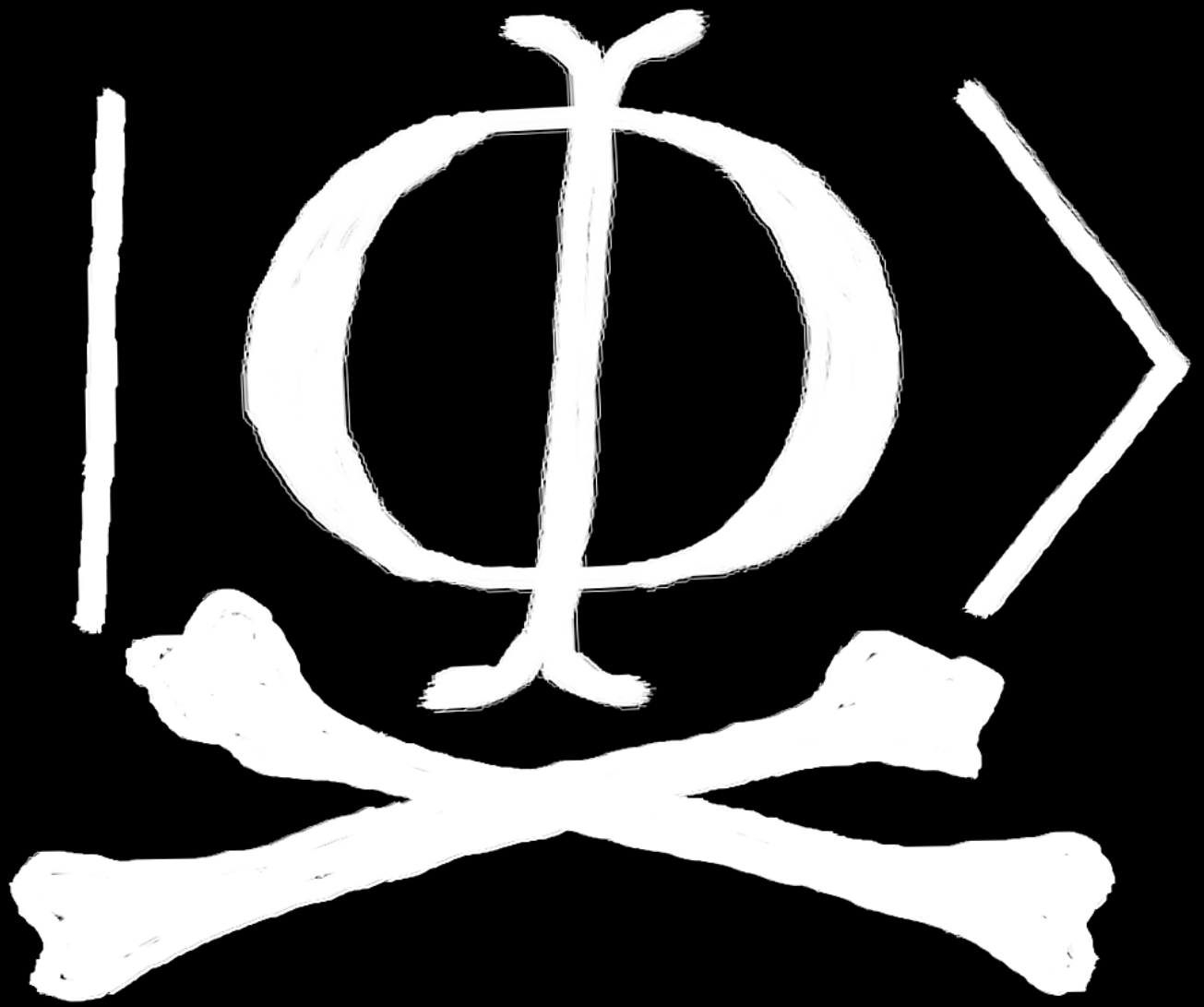
Integrate imperfection into security model



IQC Institute for Quantum Computing

Quantum hacking lab

www.vad1.com/lab



IQC Institute for Quantum Computing

Quantum hacking lab

www.vad1.com/lab