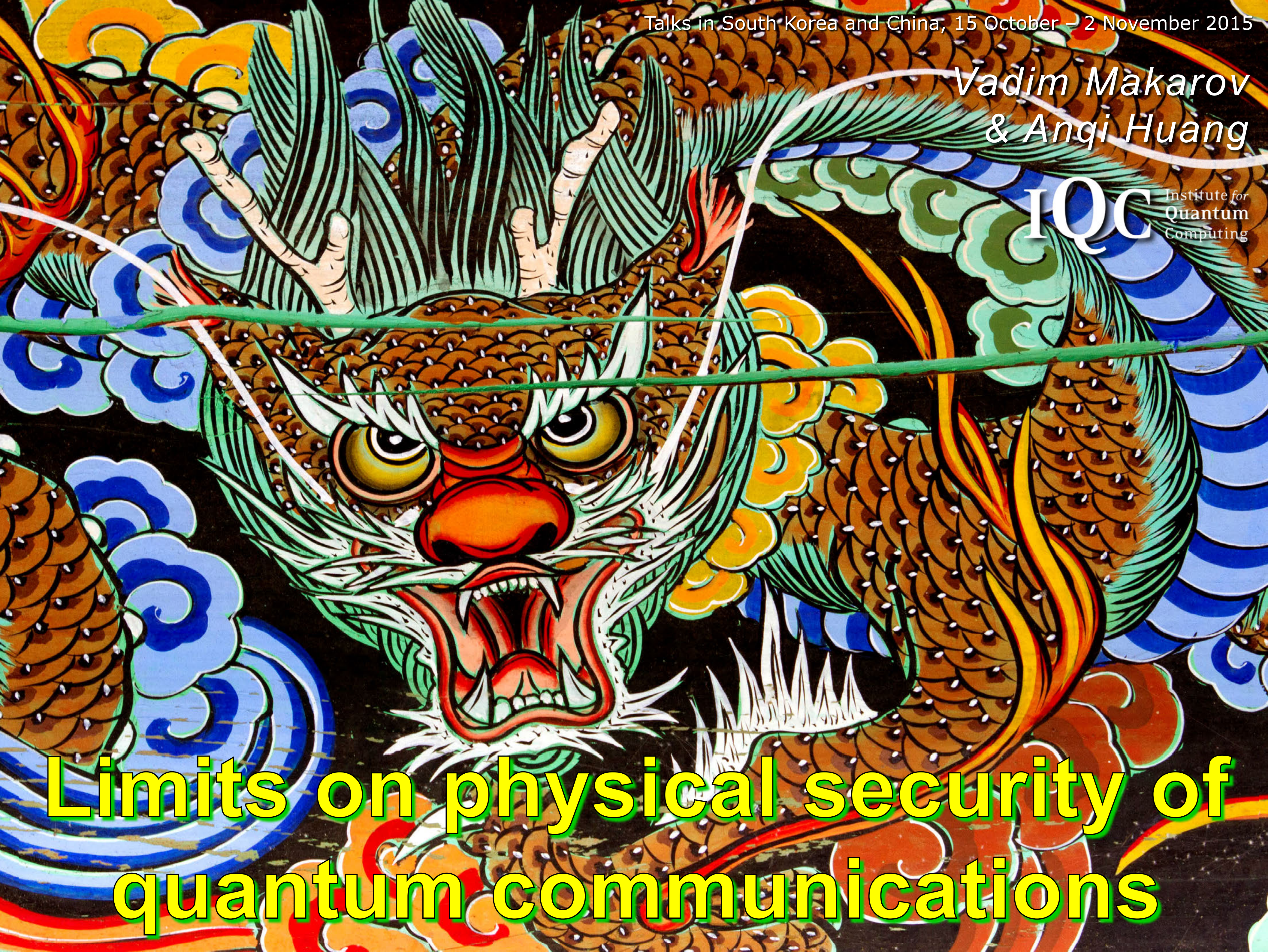

Talks in South Korea and China, 15 October – 2 November 2015
Vadim Makarov
& Anqi Huang
IQC Institute for Quantum Computing
Limits on physical security of quantum communications

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...

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)

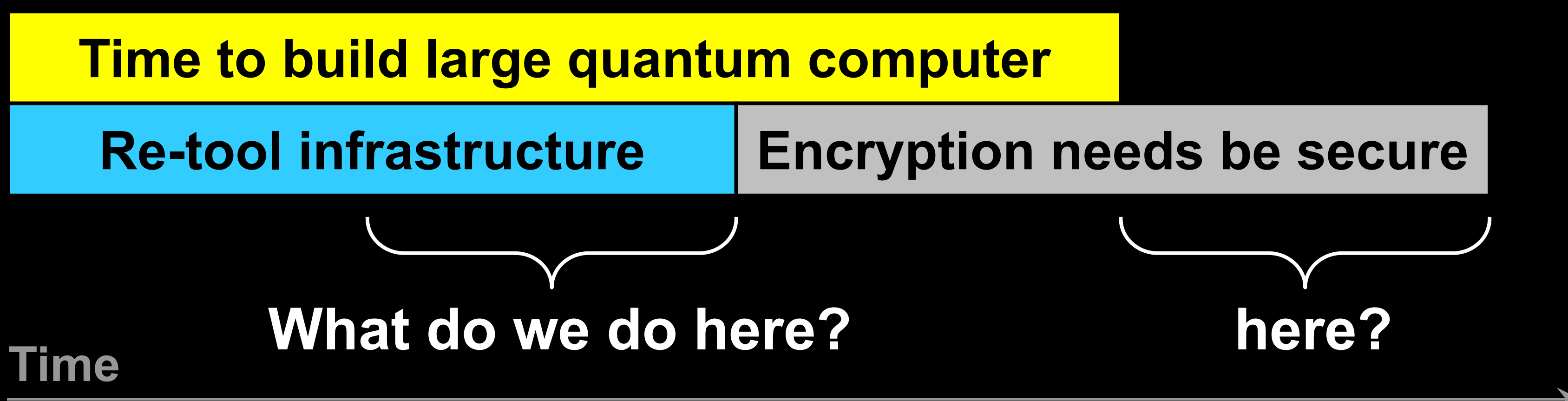


Diagram courtesy M. Mosca

How close is quantum computer?

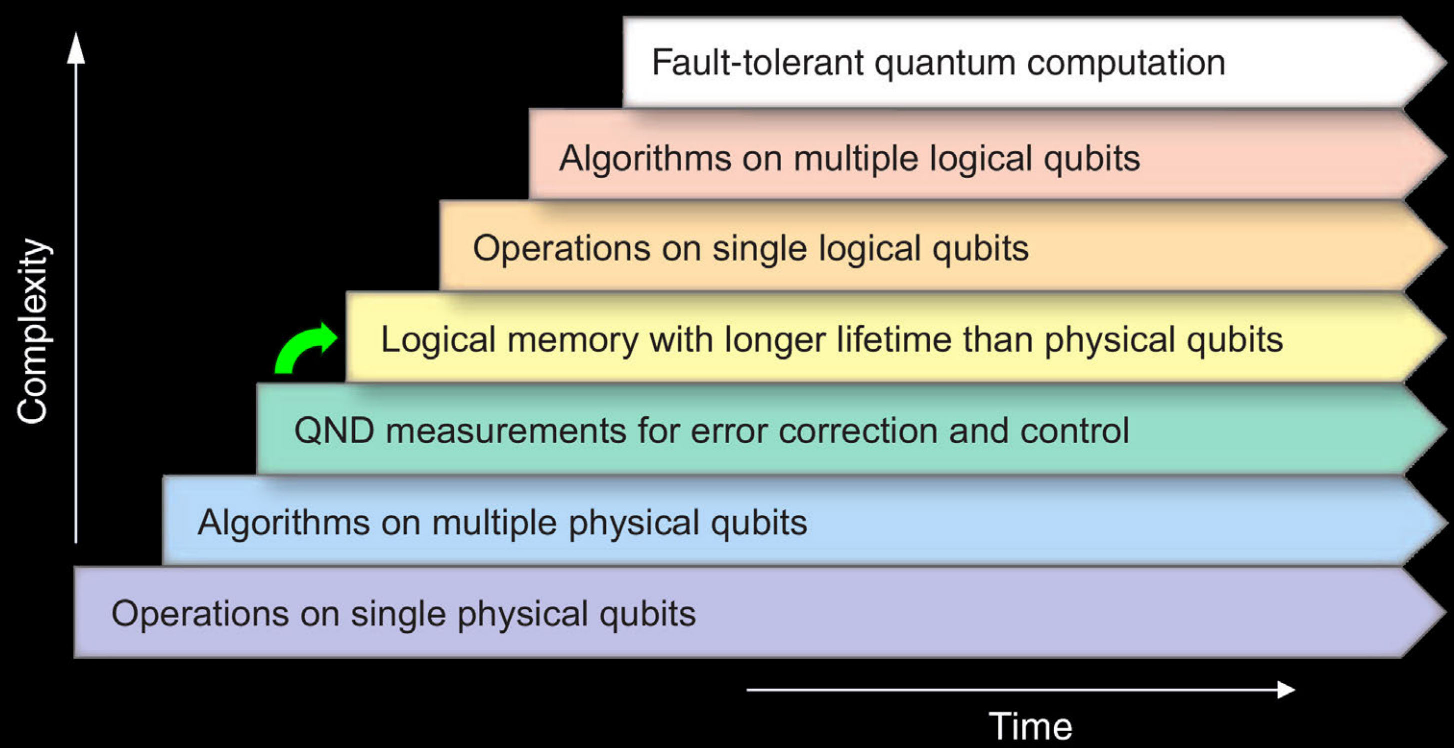


Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third 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, Science **339**, 1169 (2013)

How close is quantum computer?

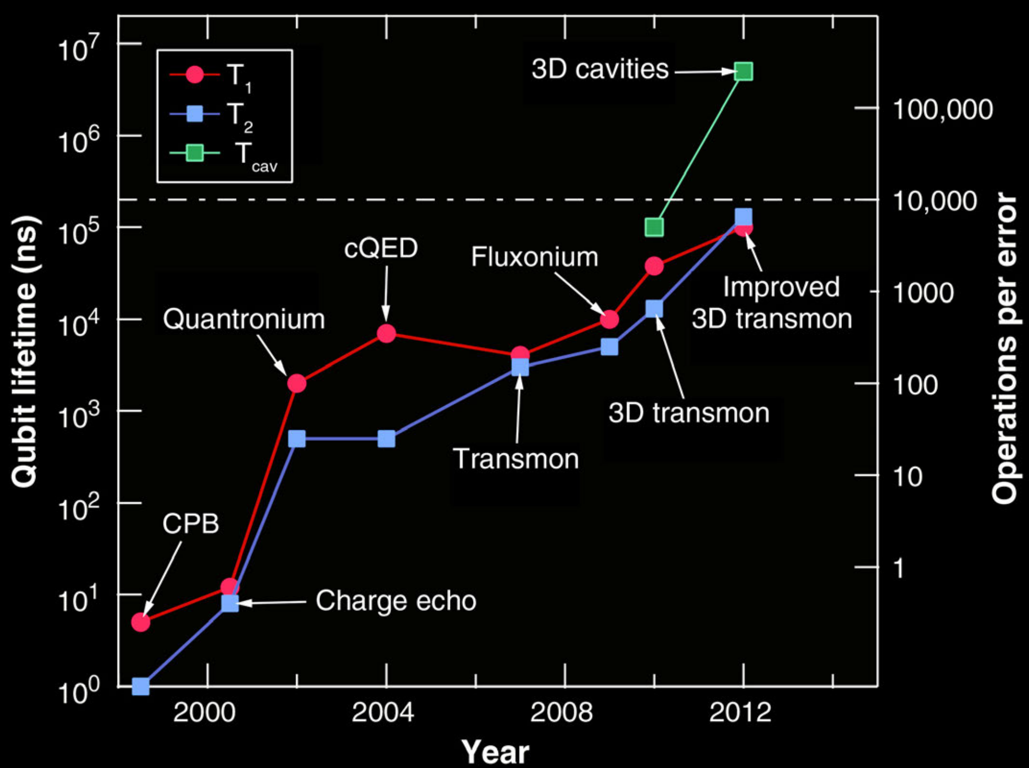


Fig. 3. Examples of the "Moore's law" type of exponential scaling in performance of superconducting qubits during recent years.

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.

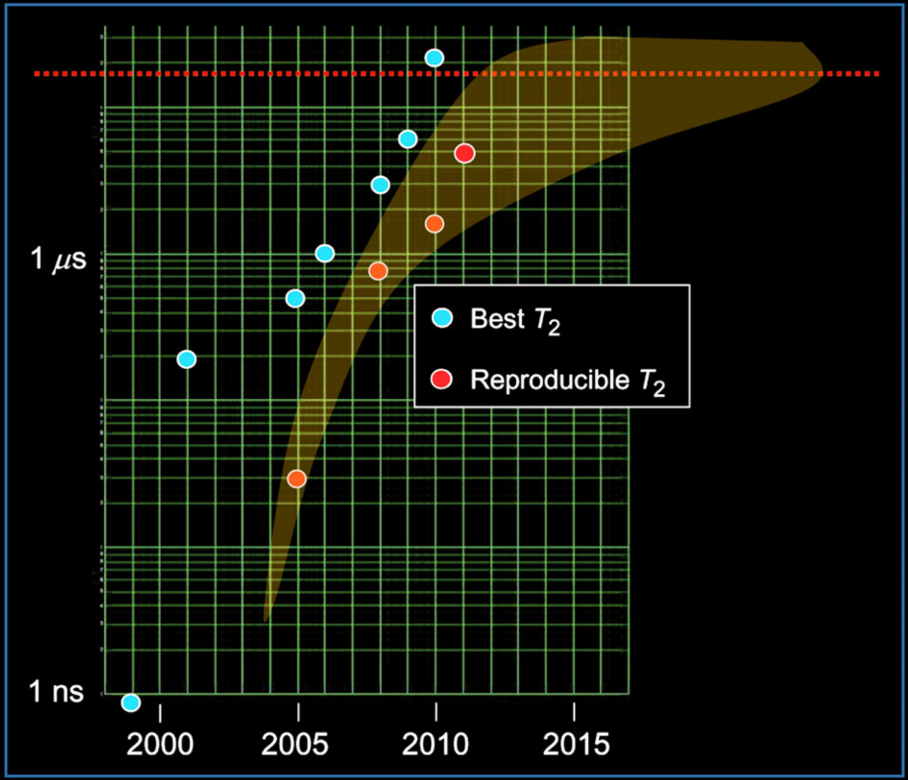


Figure 5

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

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

"post-quantum" cryptography:

- Classical tools deployable without quantum technologies
- Believed/hoped to be secure against quantum computer attacks of the future

quantum cryptography:

- Quantum tools 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

Cryptography Today

In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure, interoperable communications.

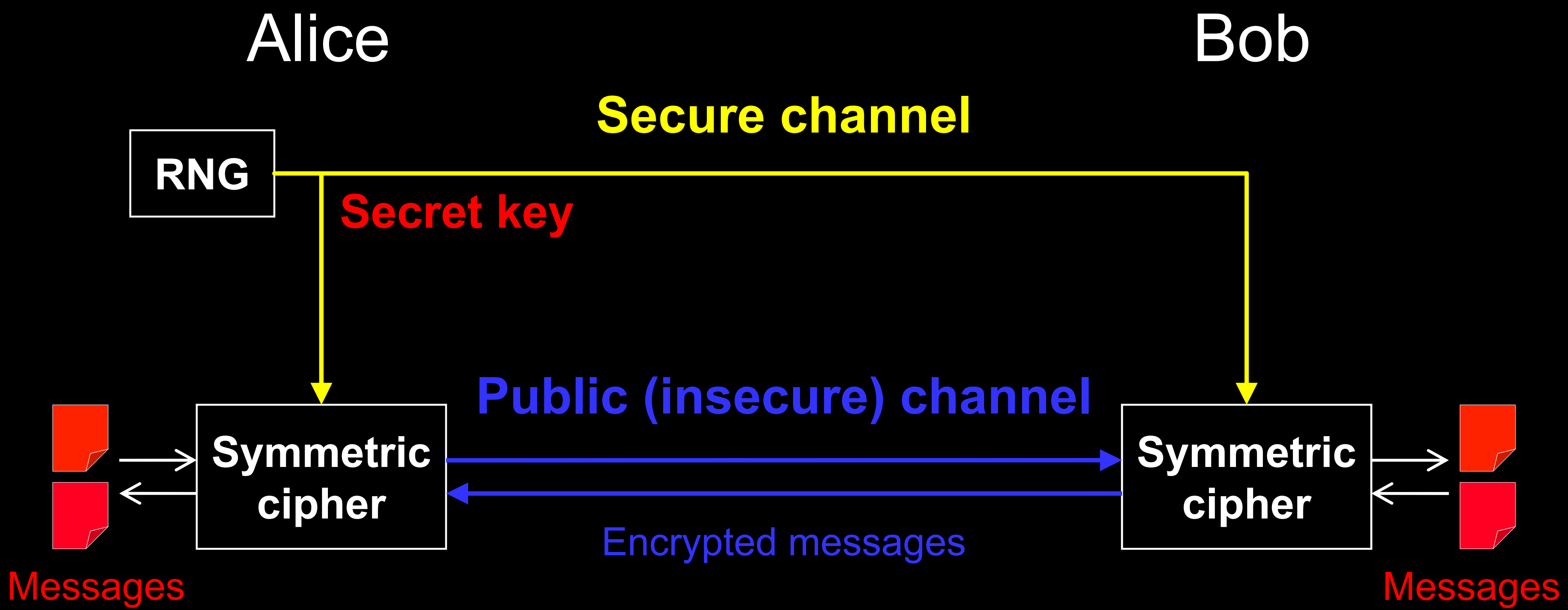
Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.

Background

IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer. We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.

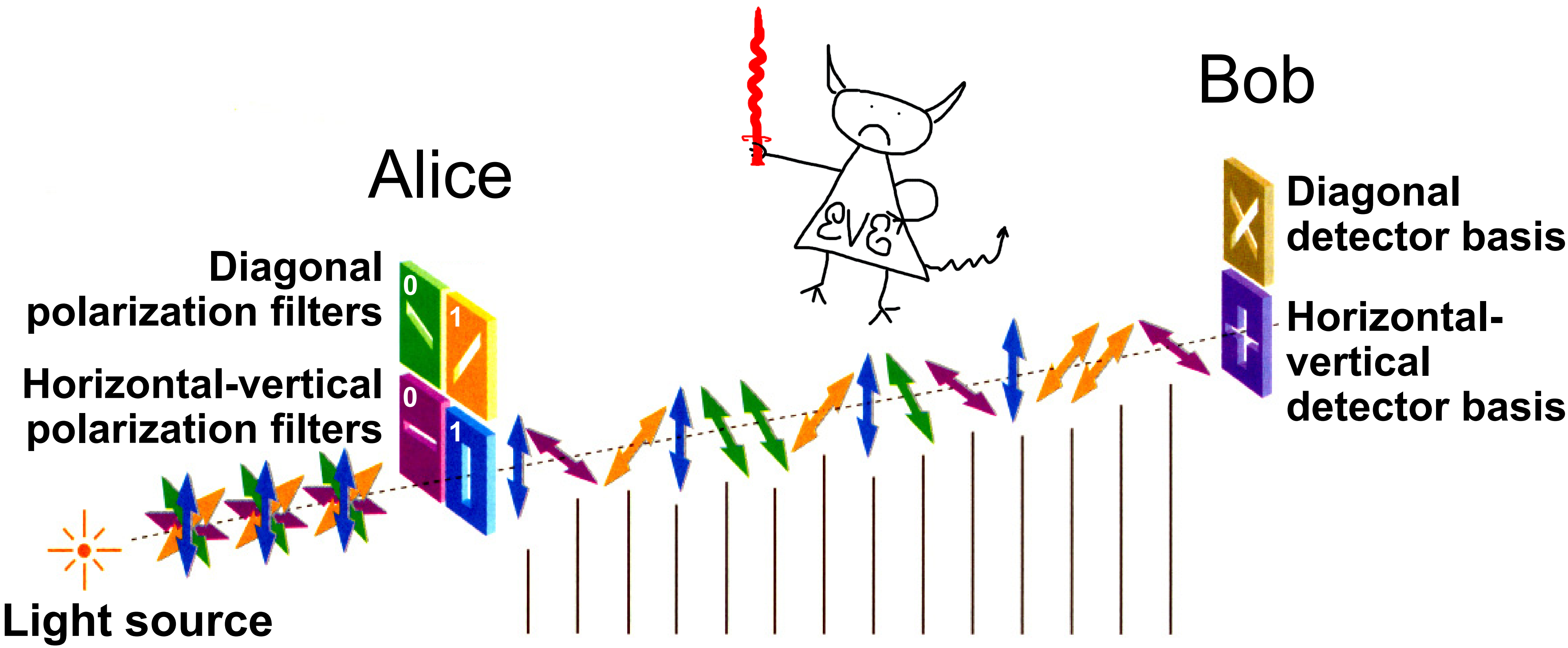
(19 August 2015)

Encryption and key distribution



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

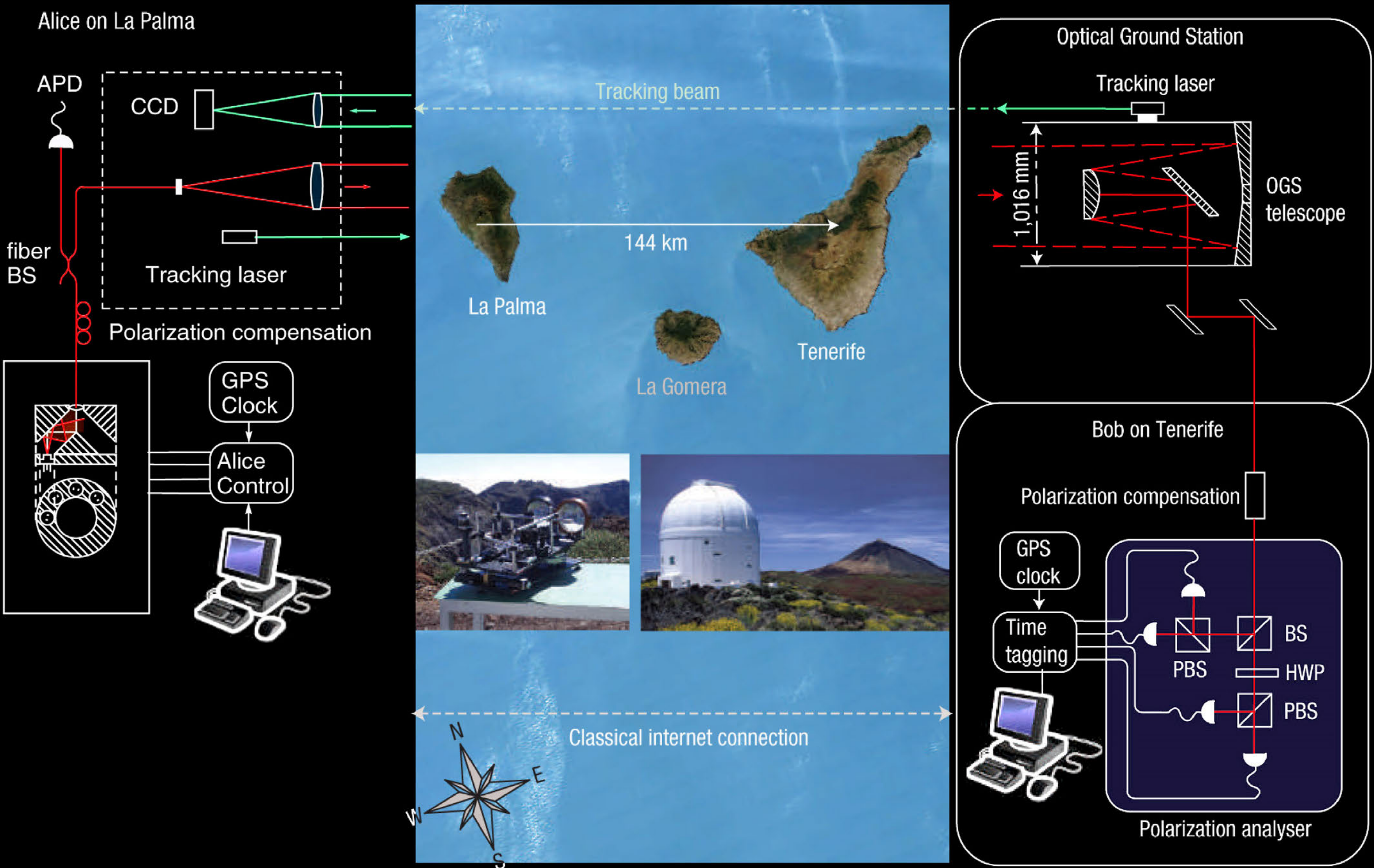
Quantum key distribution (QKD)



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

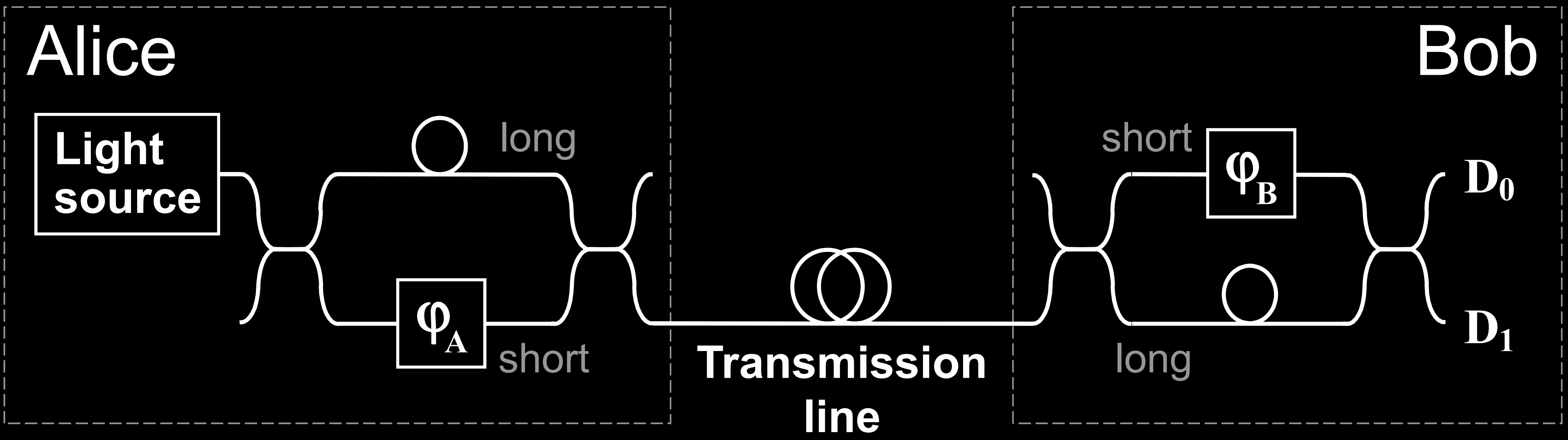
Image reprinted from article: W. Tittel, G. Ribordy & N. Gisin, "Quantum cryptography," Physics World, March 1998

Free-space QKD



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

Phase encoding, interferometric QKD channel



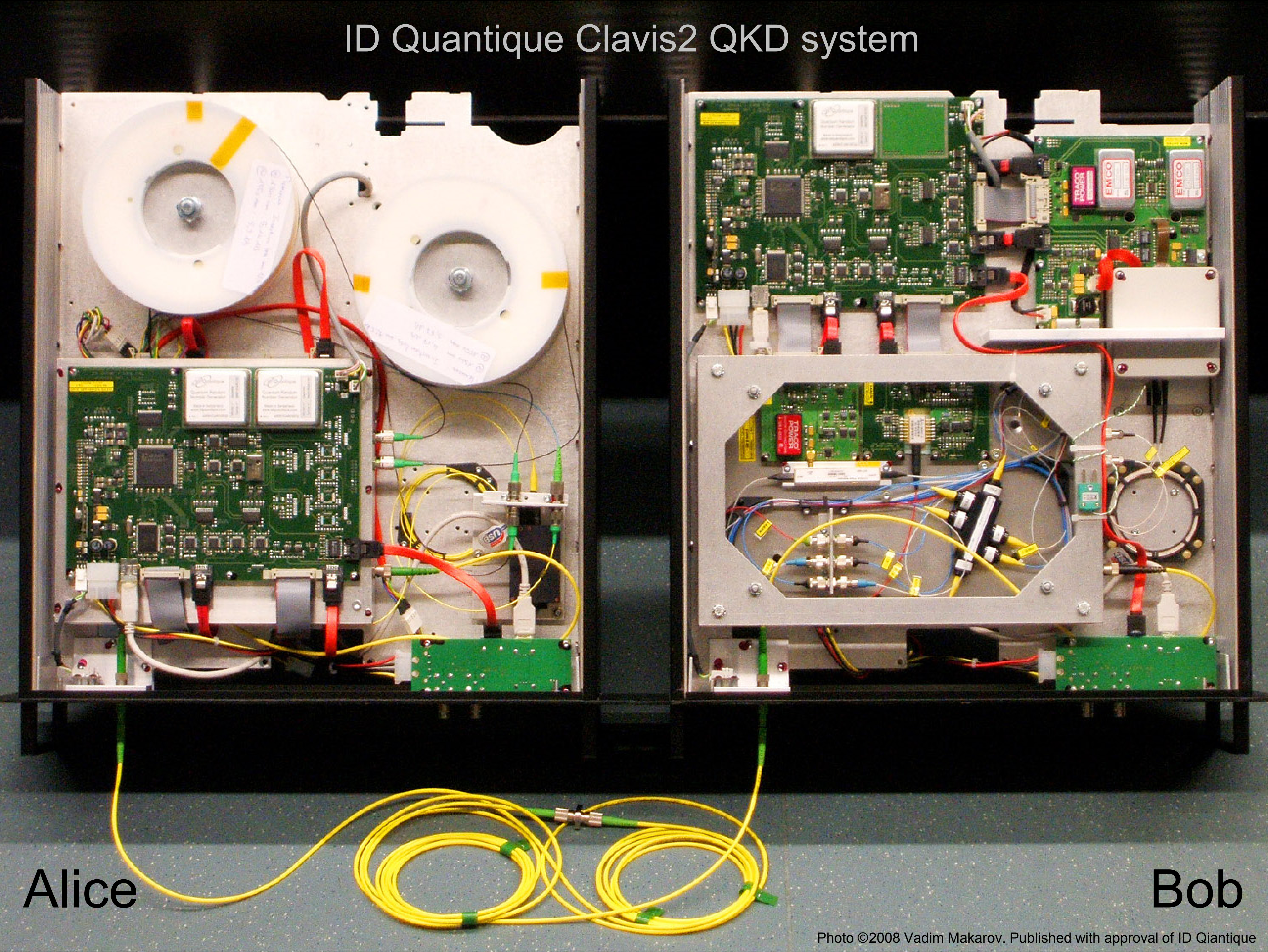
Detection basis:

$\varphi_A =$ 0 or $\pi/2$: 0

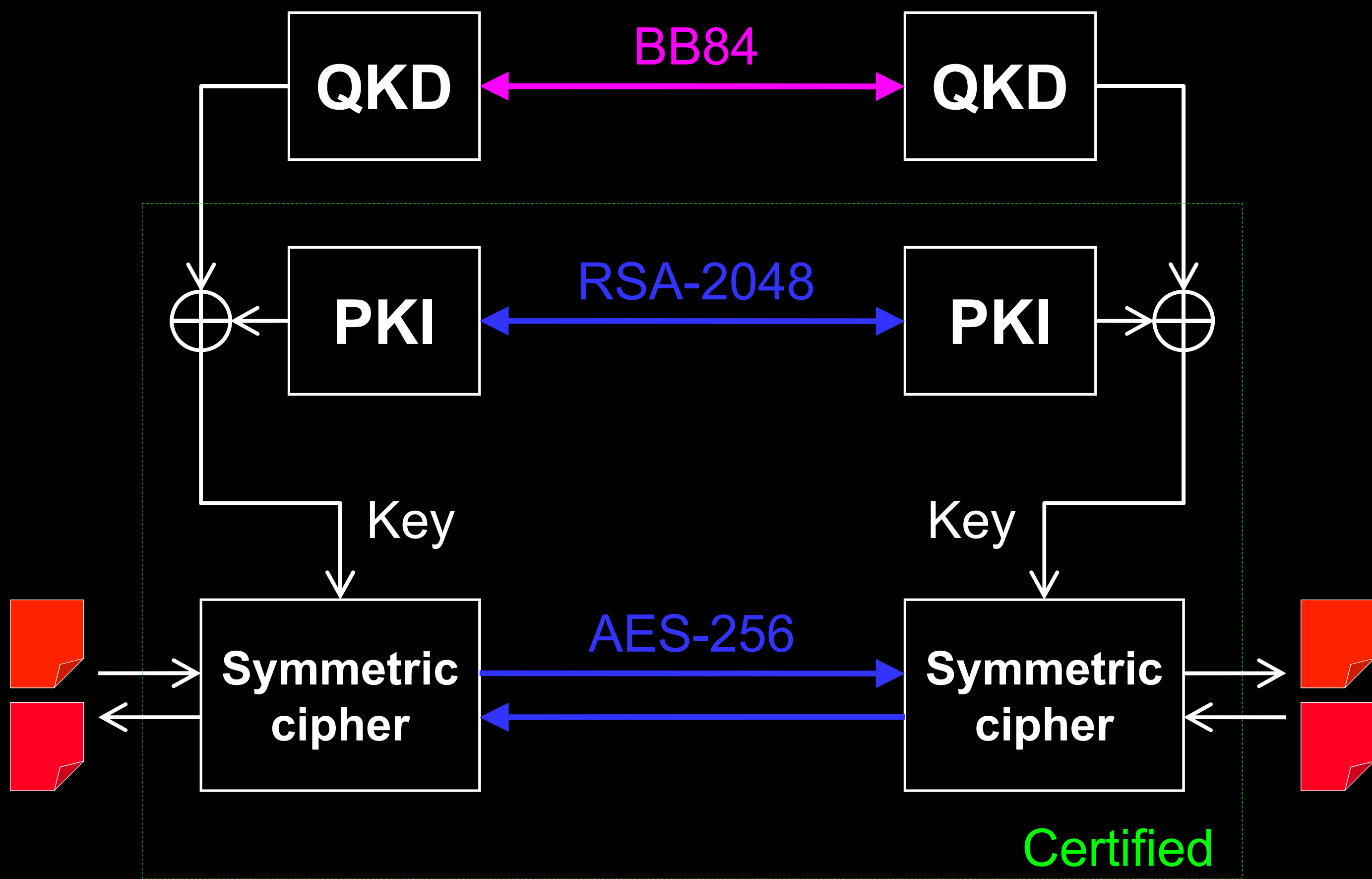
π or $3\pi/2$: 1

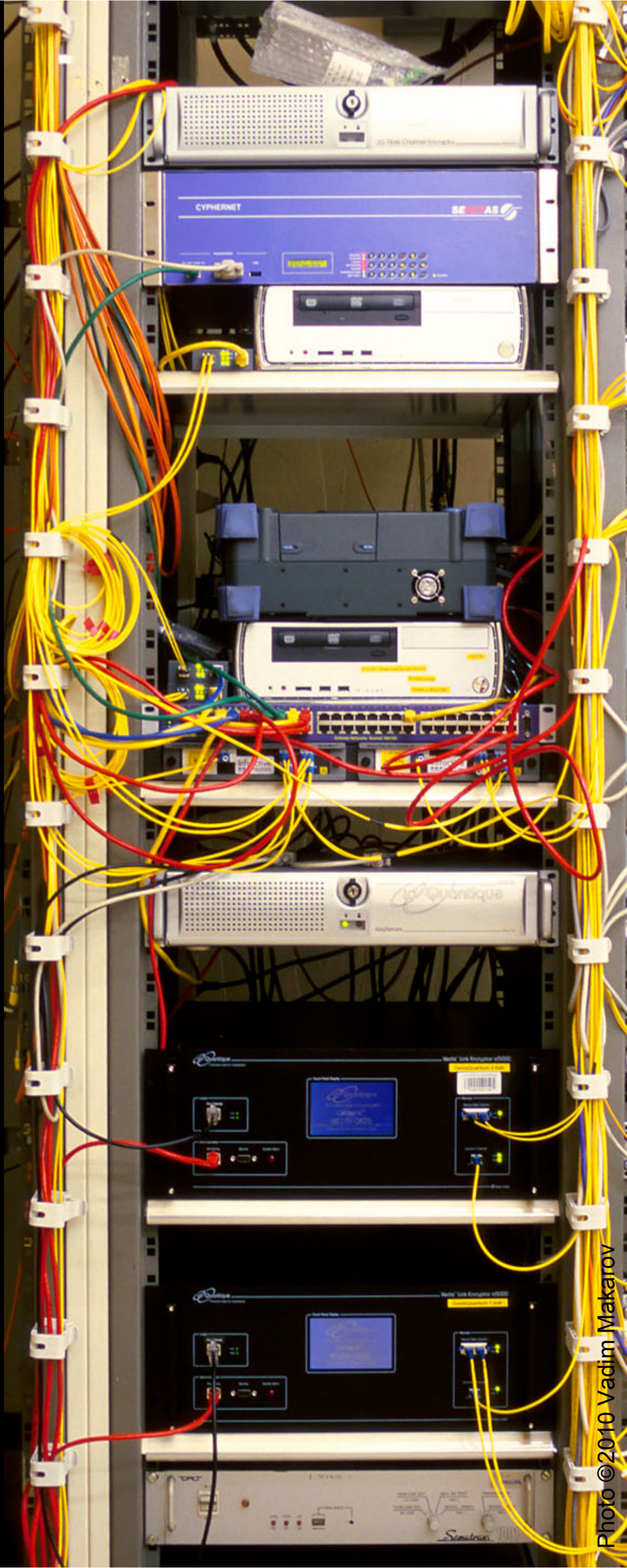
$\varphi_B =$ 0 : X

$\pi/2$: Z


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

Dual key agreement





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

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)

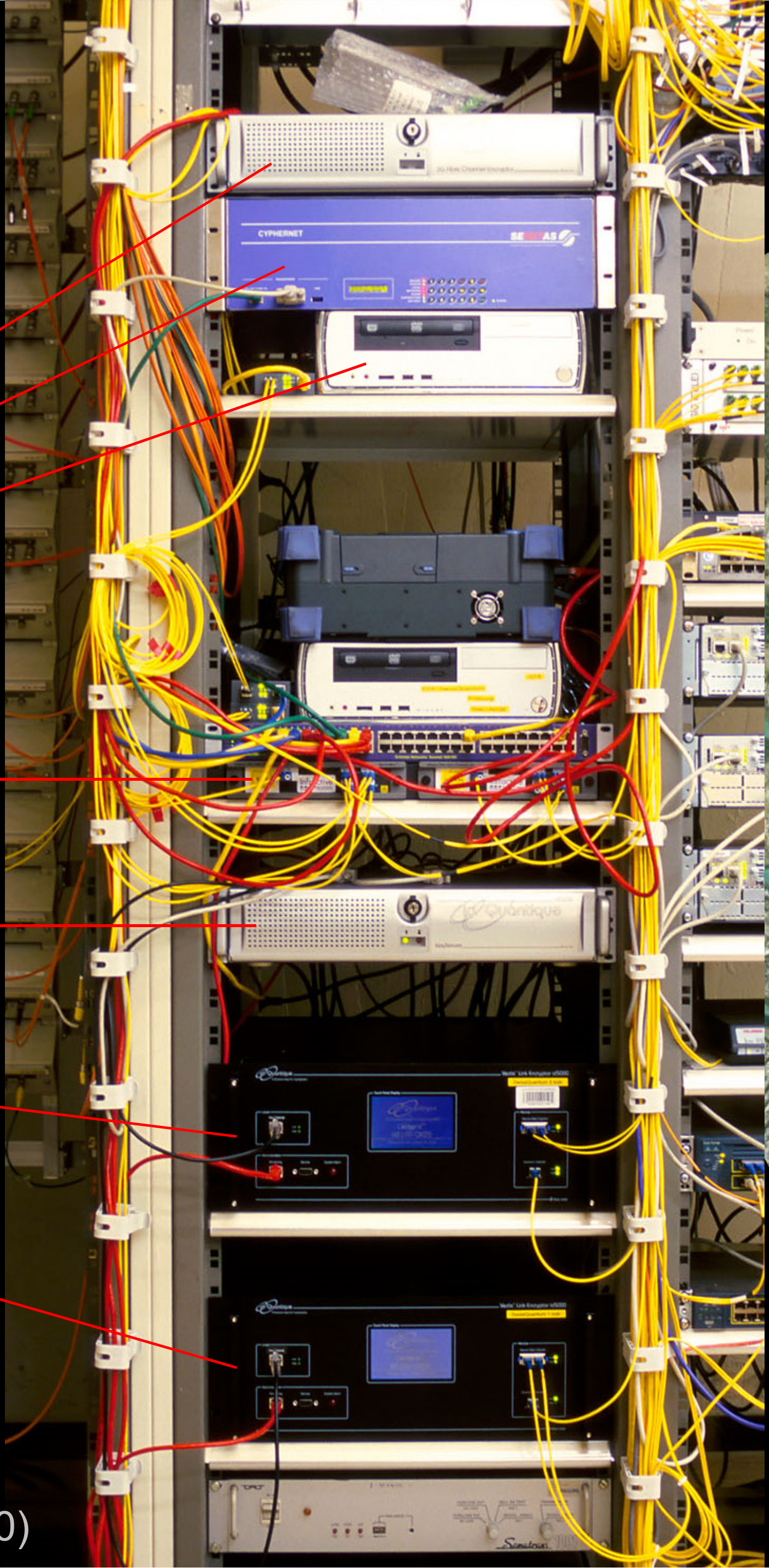
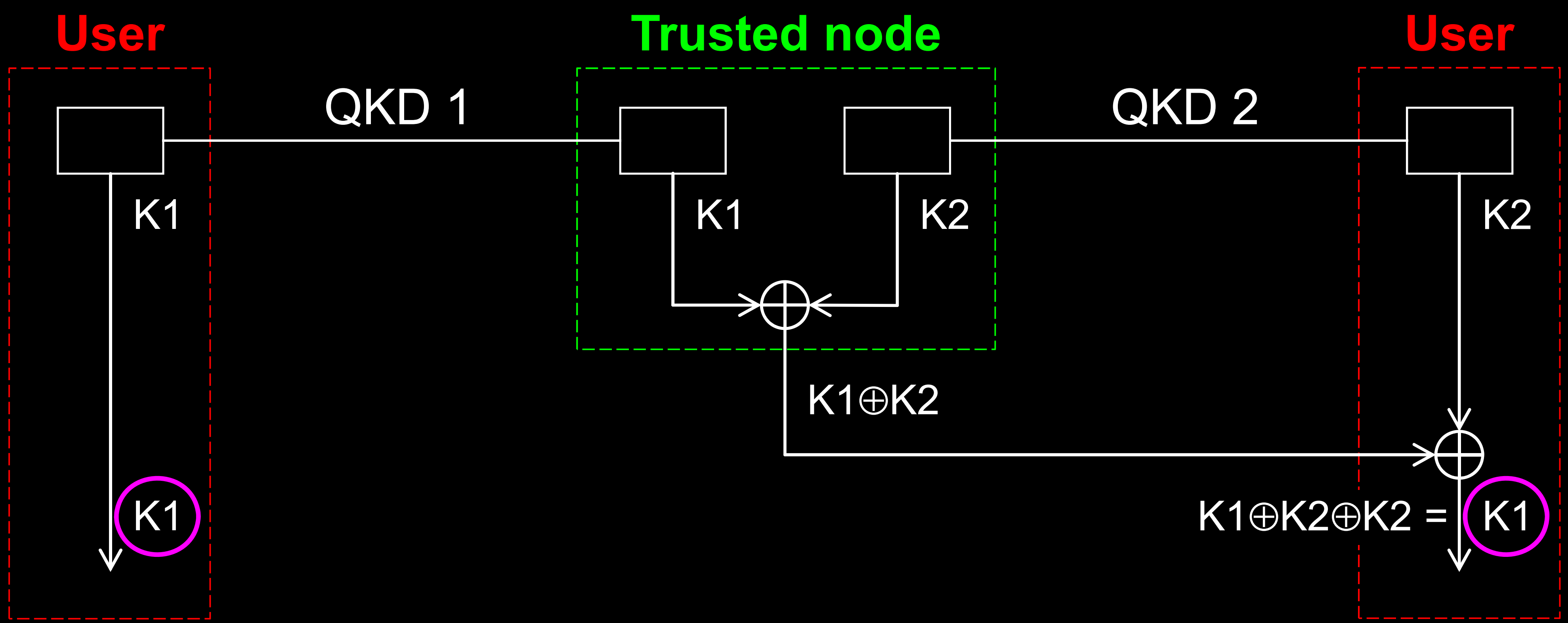


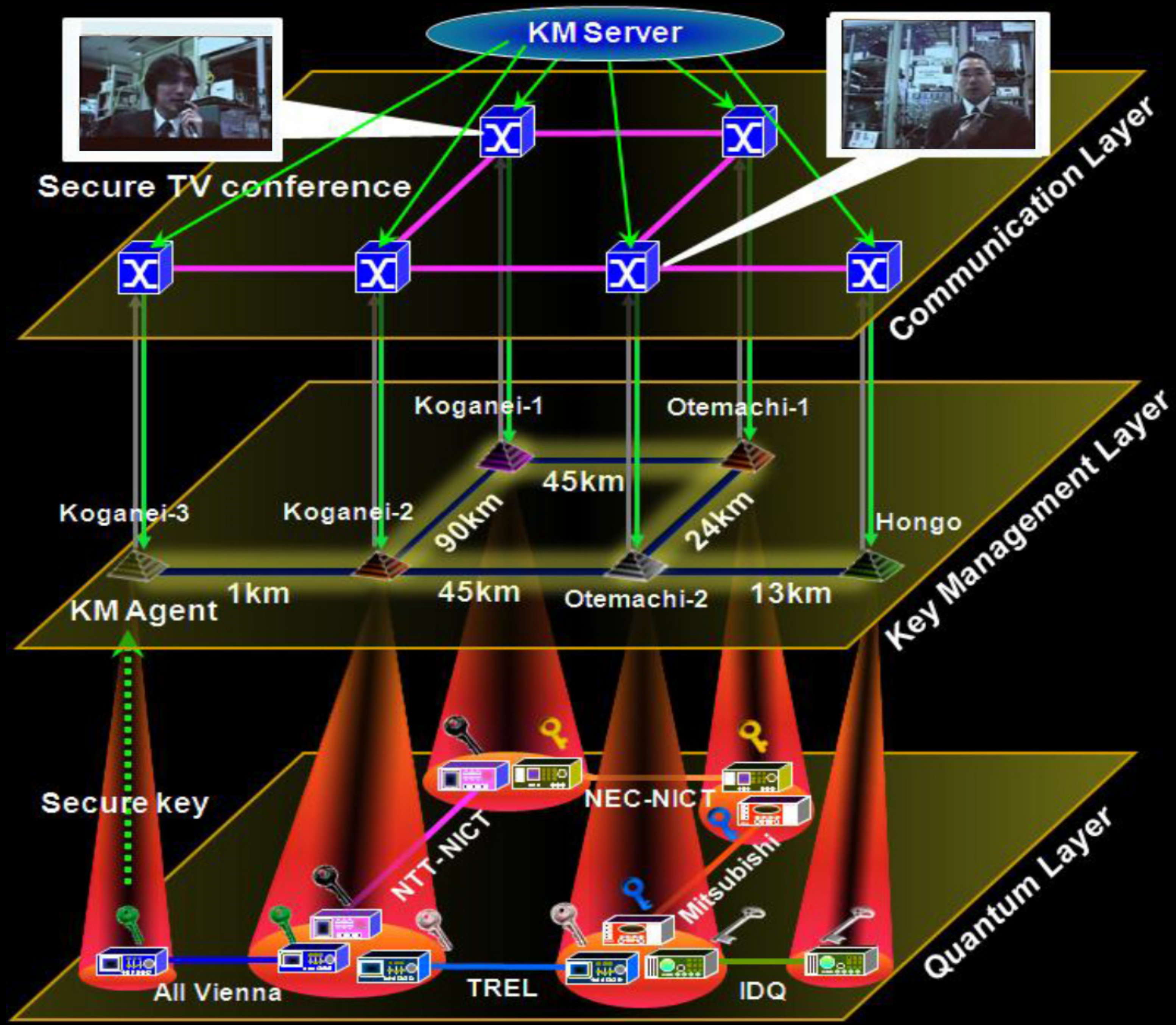
Photo ©2010 Vadim Makarov

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

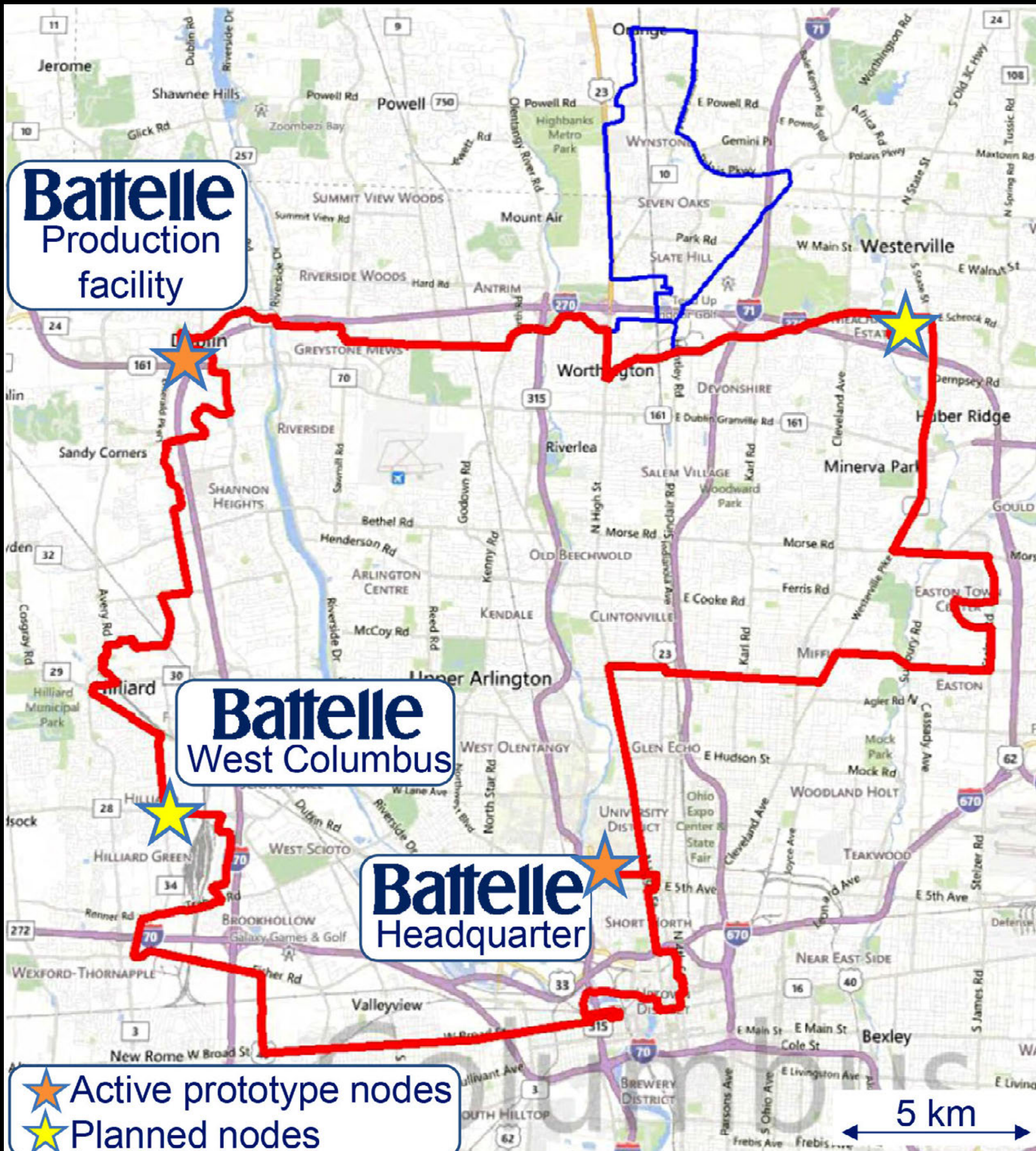
  31 fiber links
- Metropolitan networks

  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:

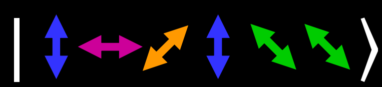
N. Walenta *et al.*, poster at QCrypt 2014

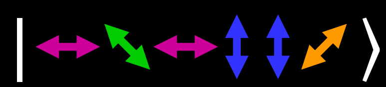
Quantum communication primitives	Advantages over classical primitives:		
	Unconditionally secure?	Less resources?	Other quantum advantages?
Key distribution	●		
Secret sharing	●		
Digital signatures	●	●	
Superdense coding		●	
Fingerprinting		●	
Oblivious transfer	Impossible		●
Bit commitment	Impossible		●
Coin-tossing	●		
Cloud computing	●		
Bell inequality testing			
Teleportation	(no classical equivalent)		
Entanglement swapping			
Random number generators	●		

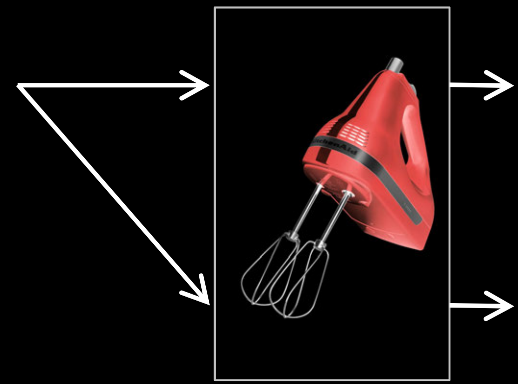
Quantum digital signatures

Alice:

1. Distributes latent signatures

"0" 

"1" 

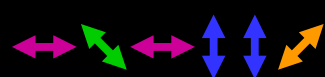


Bob: measures

Charlie: measures

⋮

2. Signs: reveals bit and latent sequence

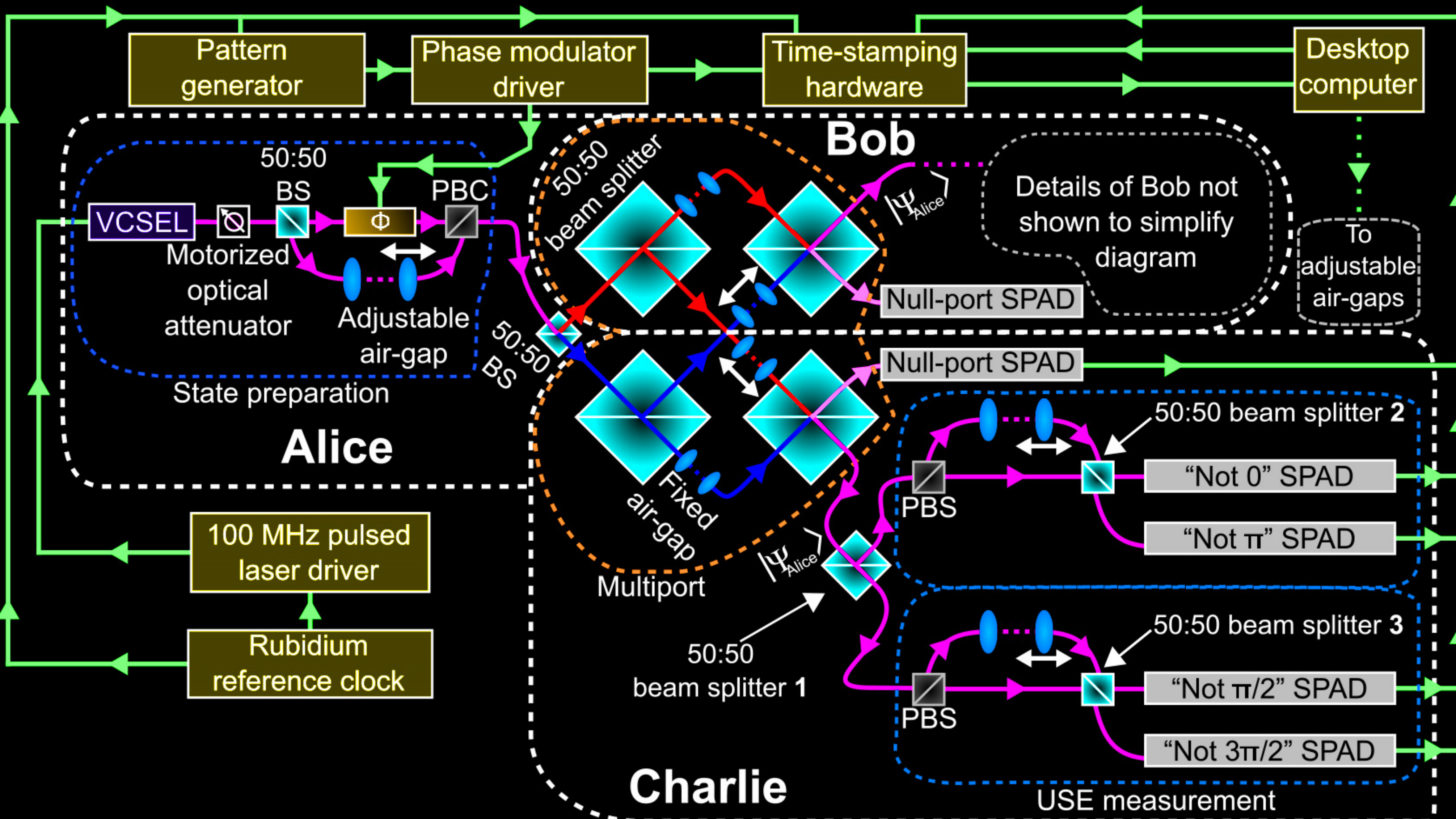
1, 

Bob: verifies measurement results

Charlie: verifies measurement results

R. Collins *et al.*, Phys. Rev. Lett. **113**, 040502 (2014)

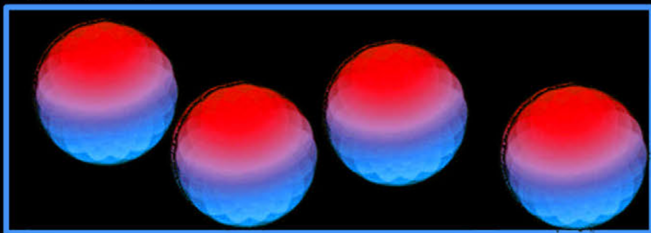
Quantum digital signatures



R. Collins *et al.*, Phys. Rev. Lett. **113**, 040502 (2014)

Blind quantum computing

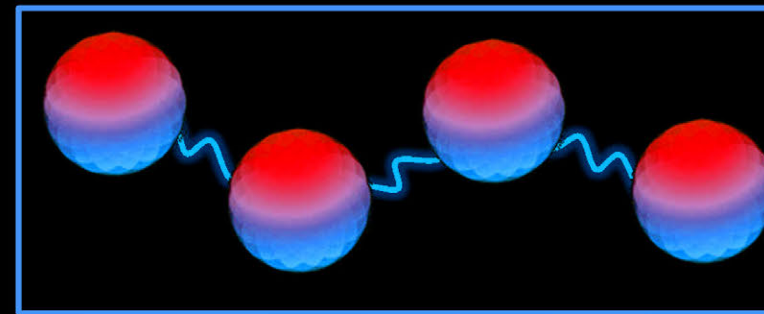
Client



Prepares qubits and sends them to quantum server

„sends single parts of computer“

Quantum Server

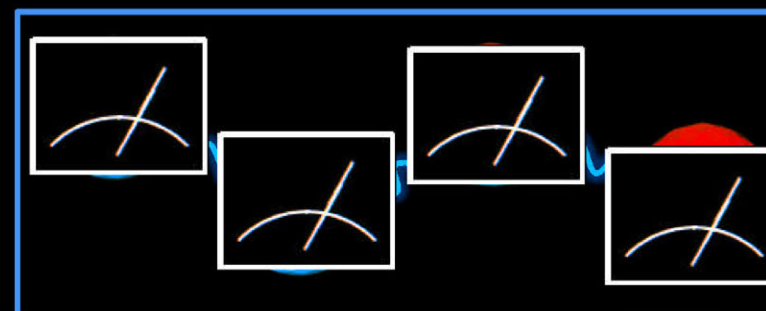


Entangles qubits

„assembles computer“

Computes and sends measurement instructions (adapted to state of the qubits)

„sends computer program“



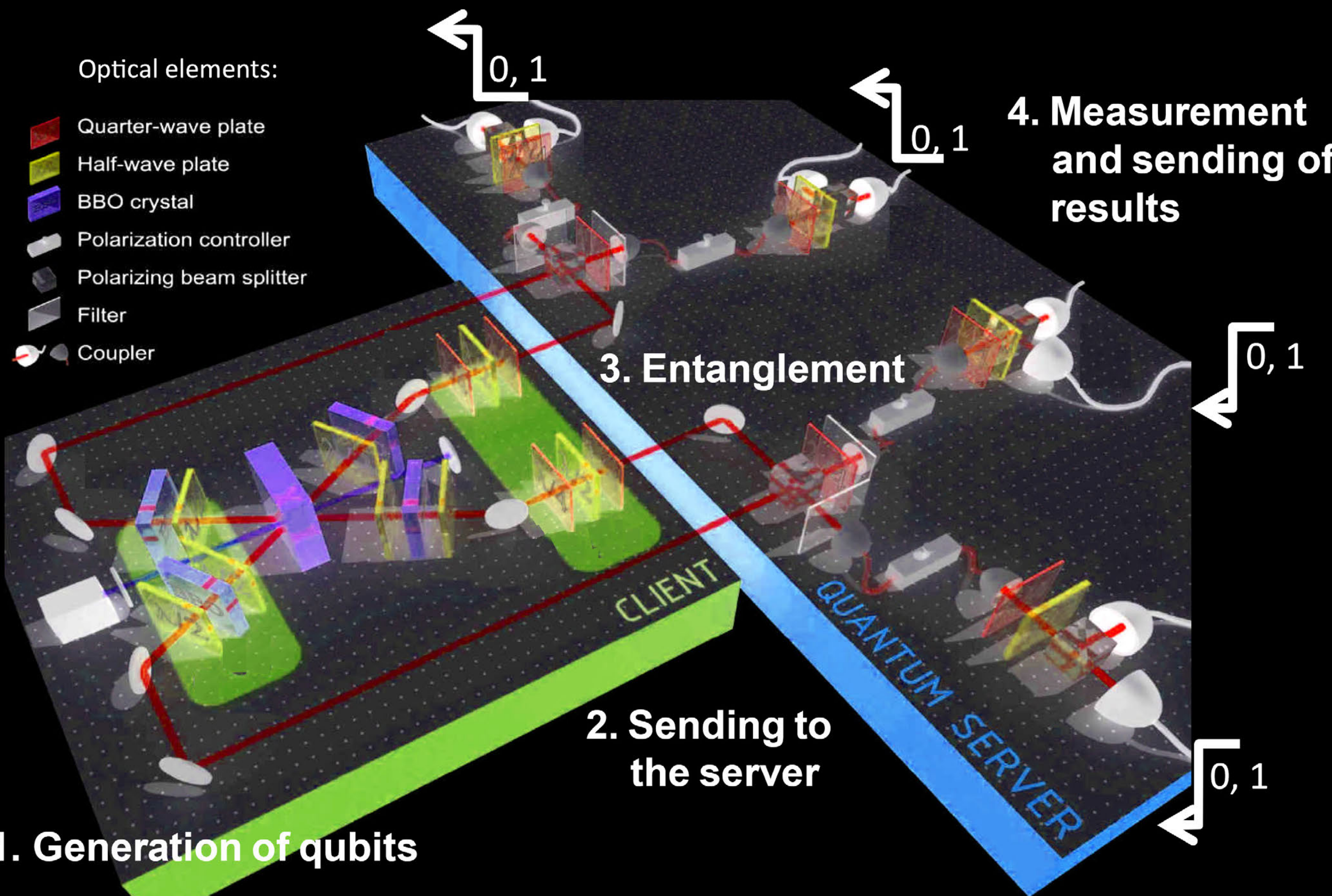
Qubits are unknown, instructions seem like random operations

„computes, but does not know computer“

Client can interpret and use the results

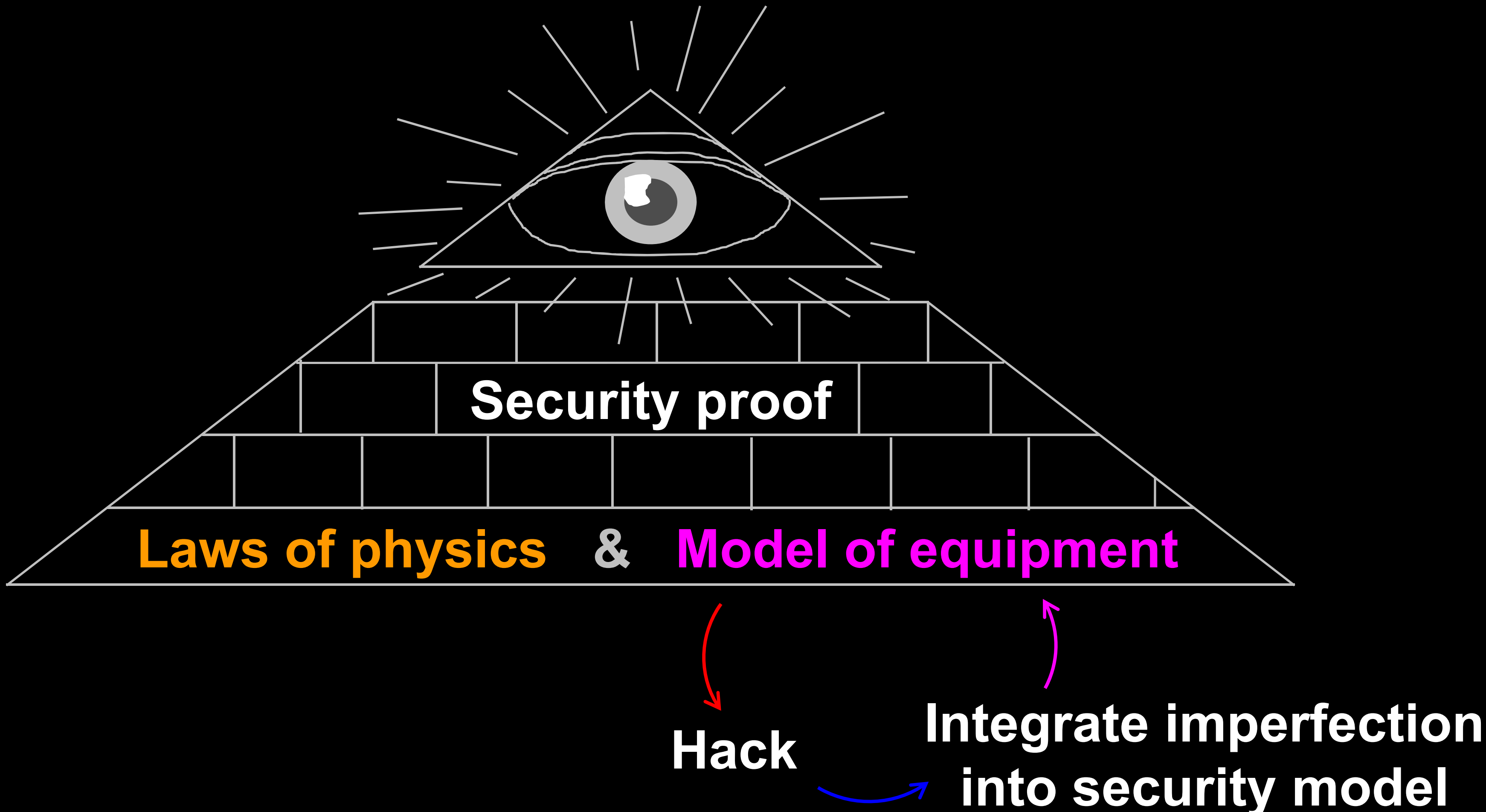
Slide courtesy S. Barz

Blind quantum computing



S. Barz *et al.*, Science **335**, 303 (2012)

Security model of QKD



Attack	Target component	Tested system
Laser damage V. Makarov *et al.,* arXiv:1510.03148	any	ID Quantique, research 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

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

Example of vulnerability and countermeasures

Photon-number-splitting attack

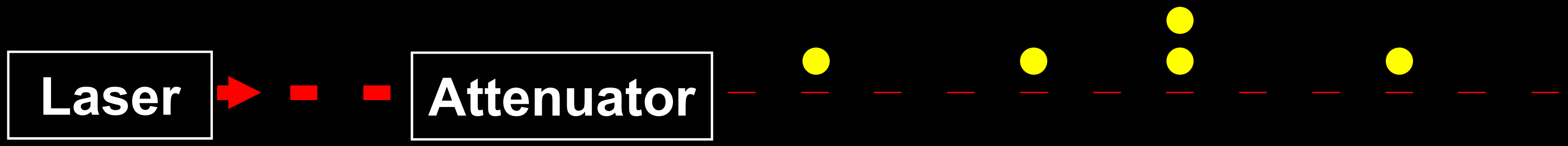
C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992)

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)

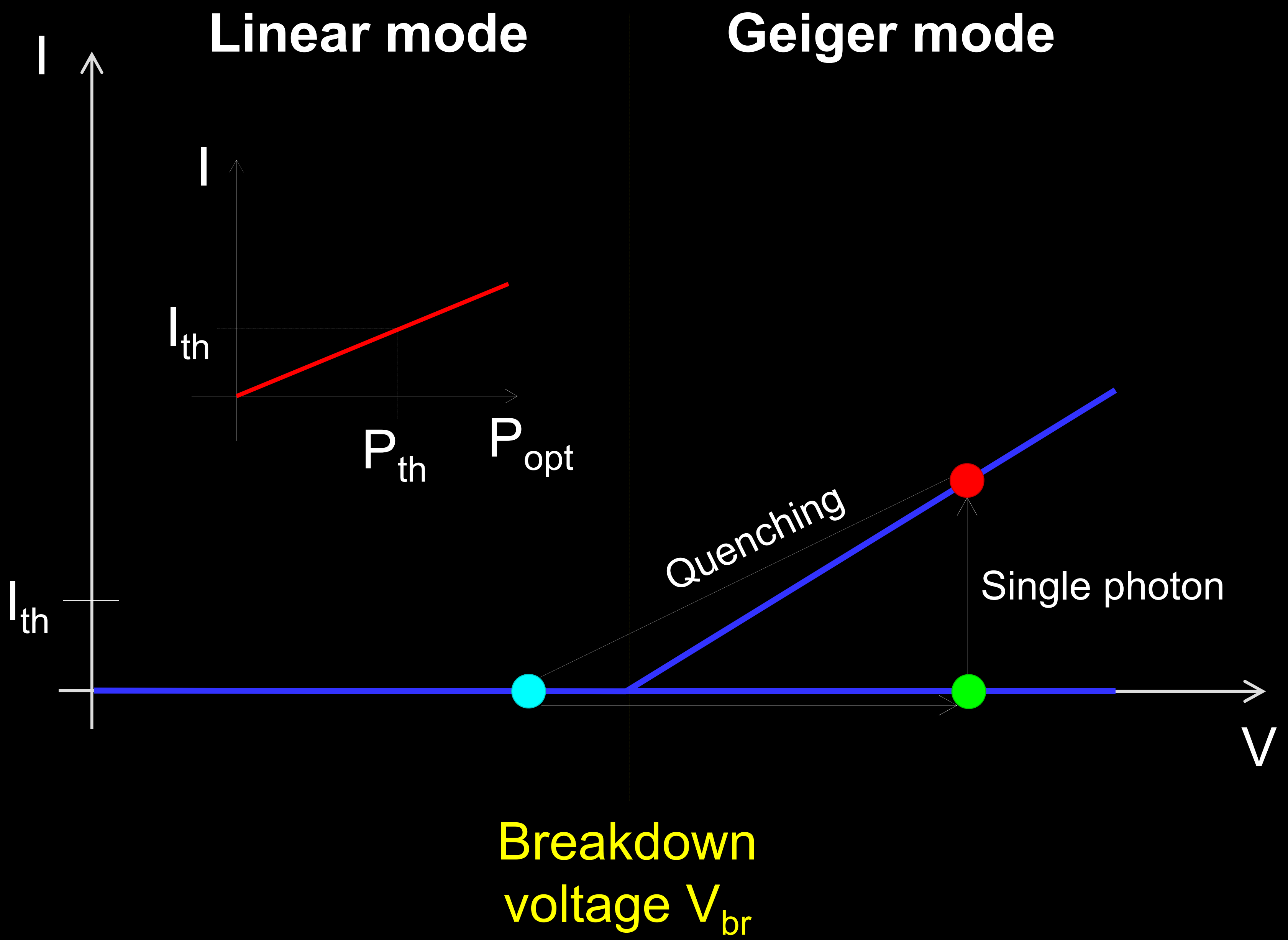
★ Distributed-phase-reference protocols

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

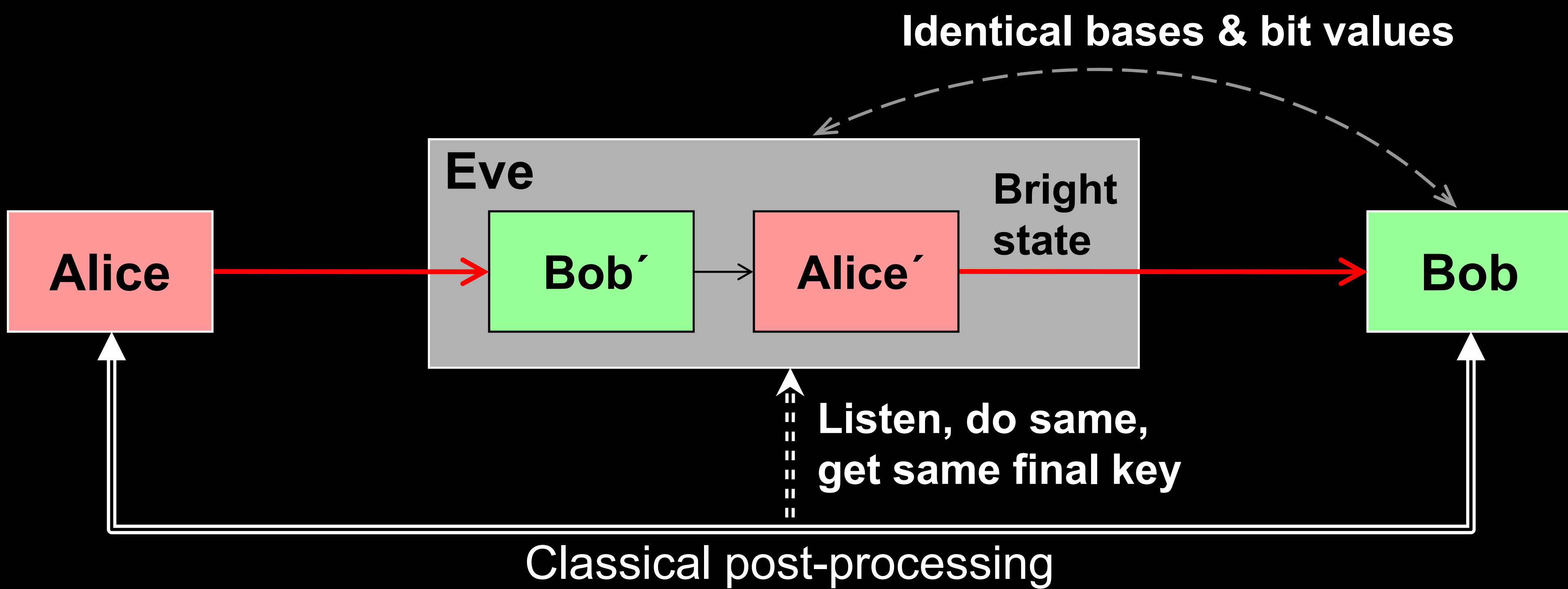
K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. A. **68**, 022317 (2003)

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

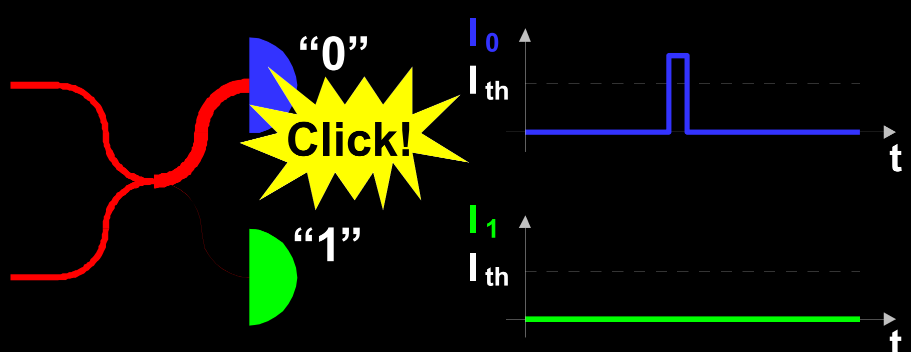
Attack example: avalanche photodetectors (APDs)



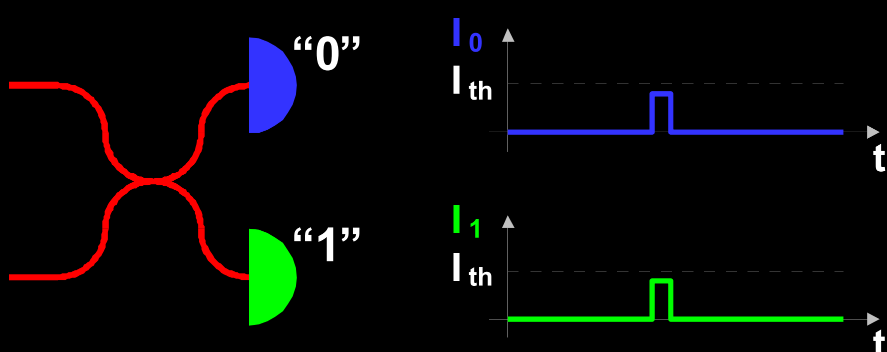
Faked-state attack in APD linear mode



Bob chooses same basis as Eve:

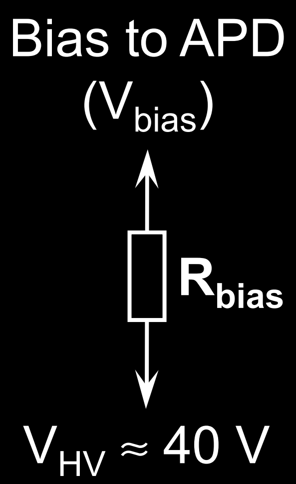


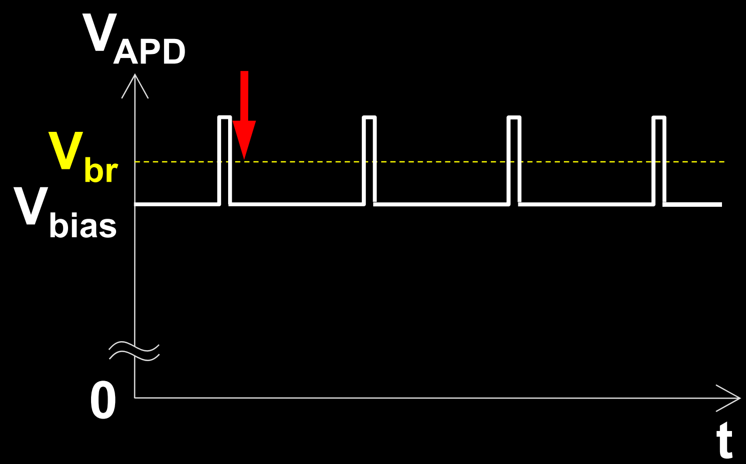
Bob chooses different basis:



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

Blinding APD with bright light

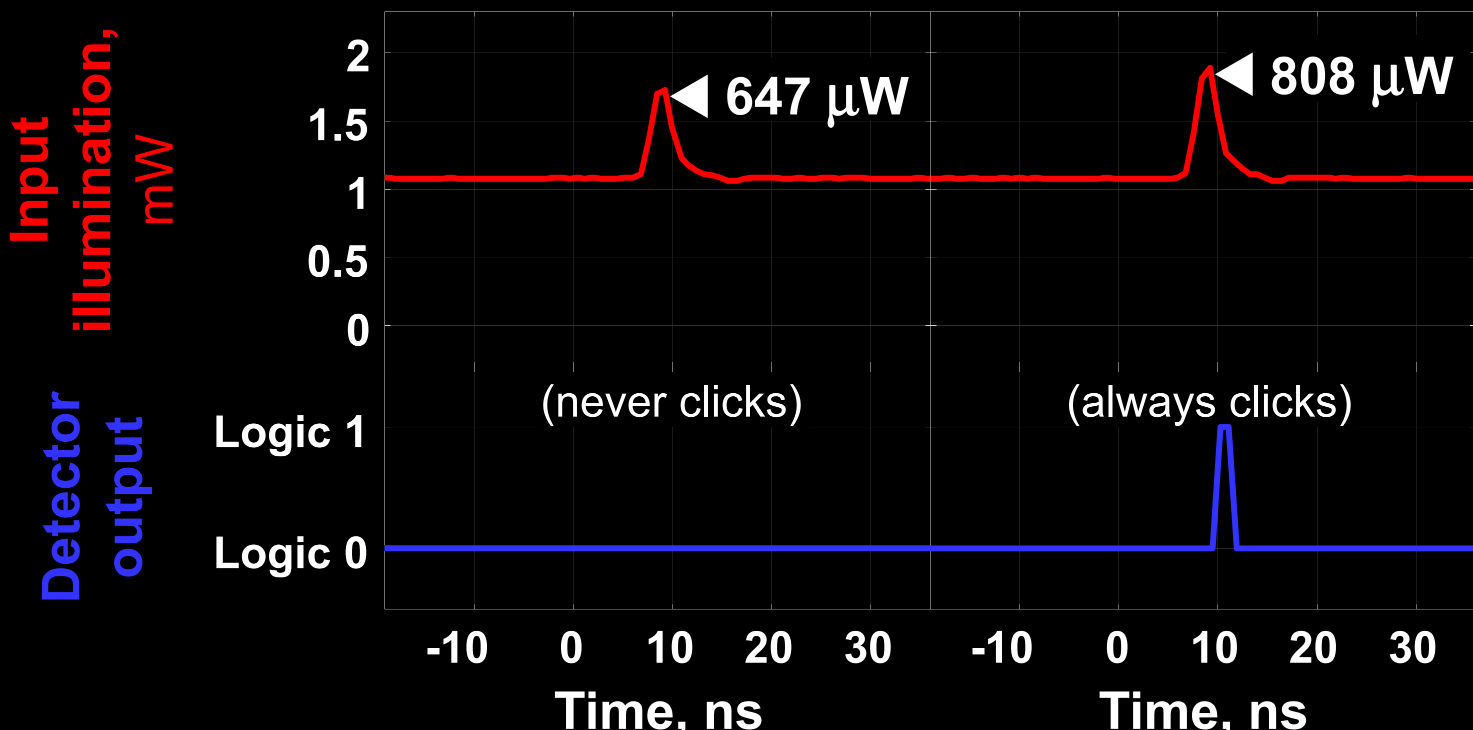




Eve applies CW light

Detector blind!

Zero dark count rate



ID Quantique Clavis2

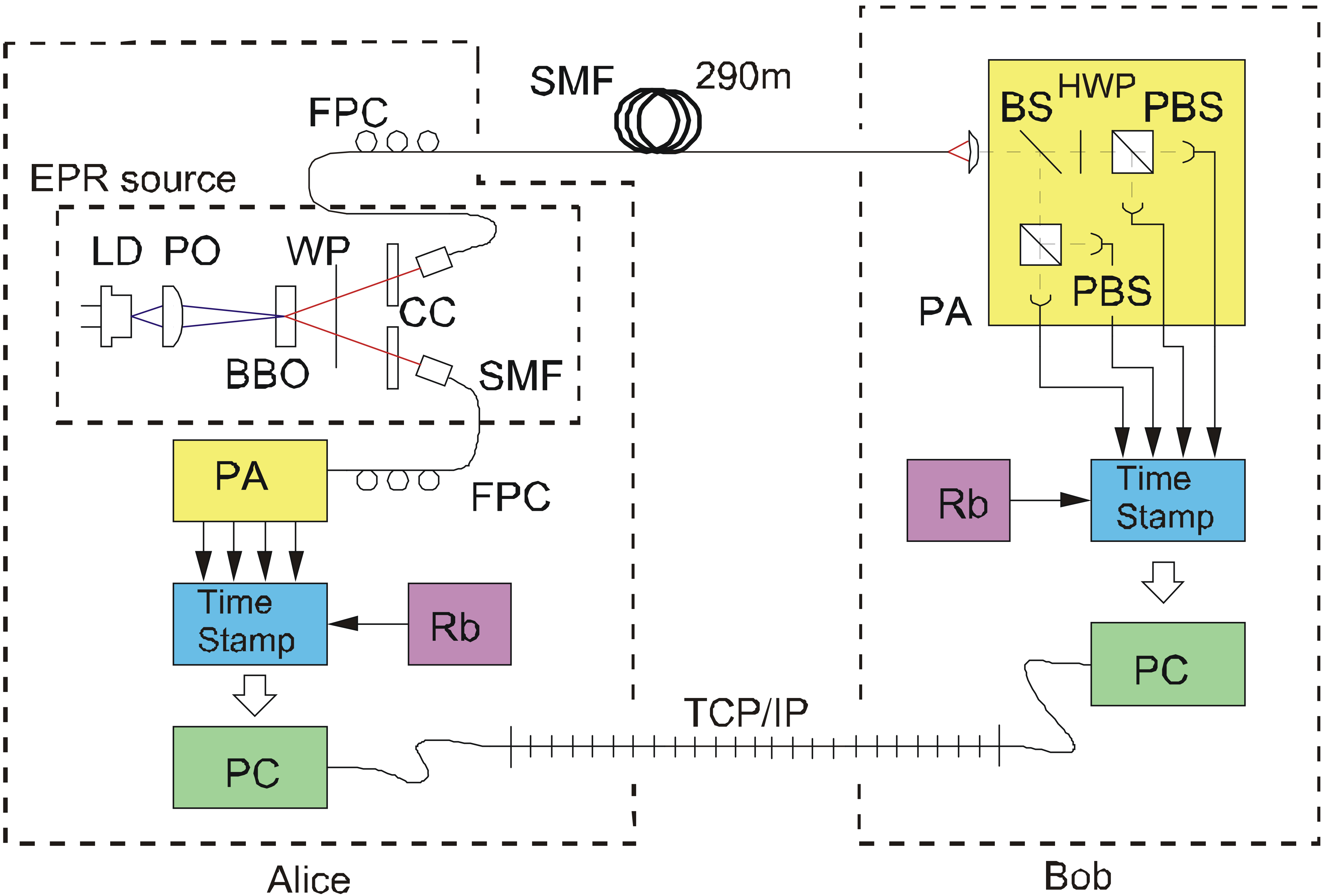
L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Nat. Photonics **4**, 686 (2010)

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)

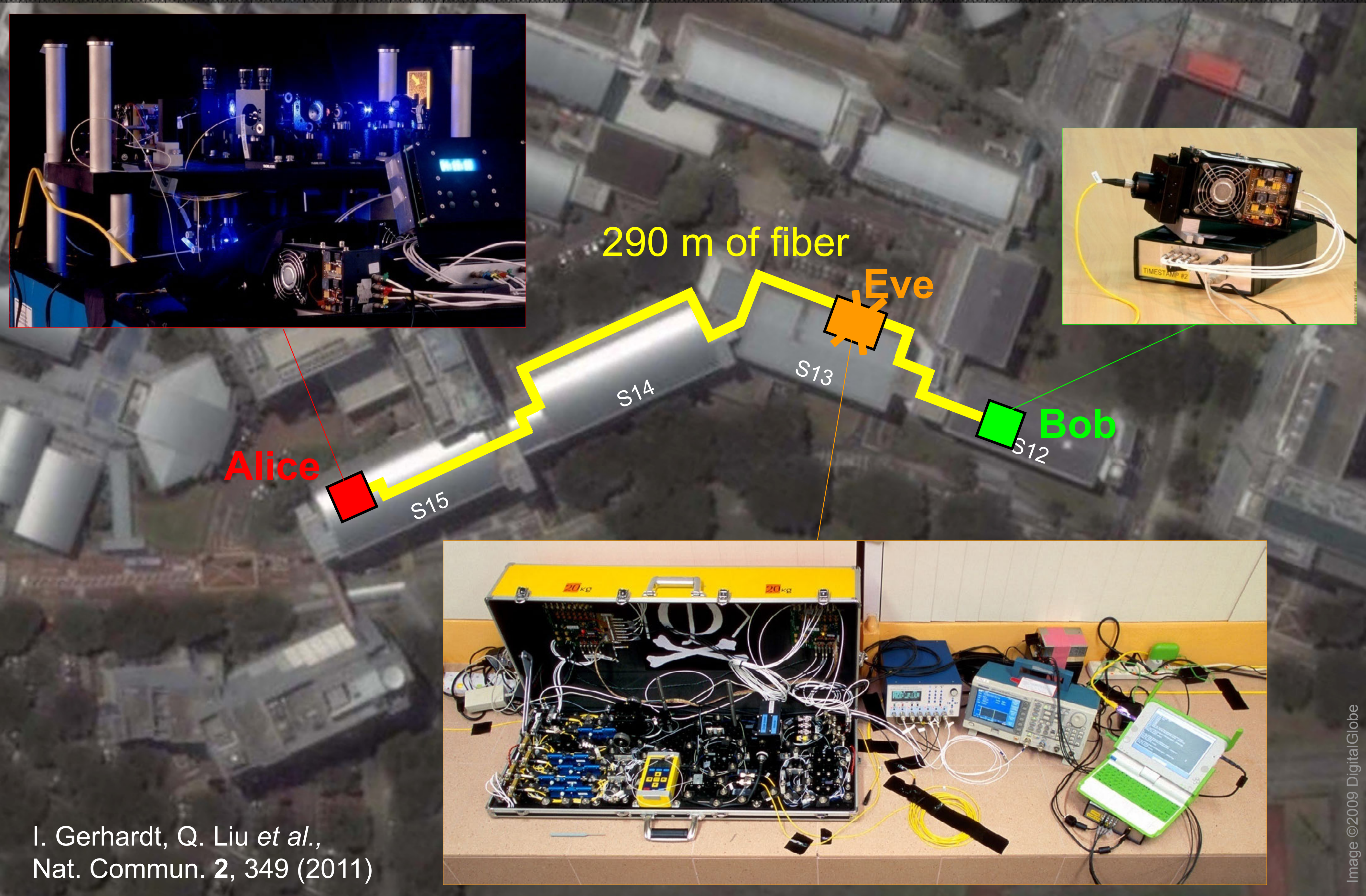
Entanglement-based QKD



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

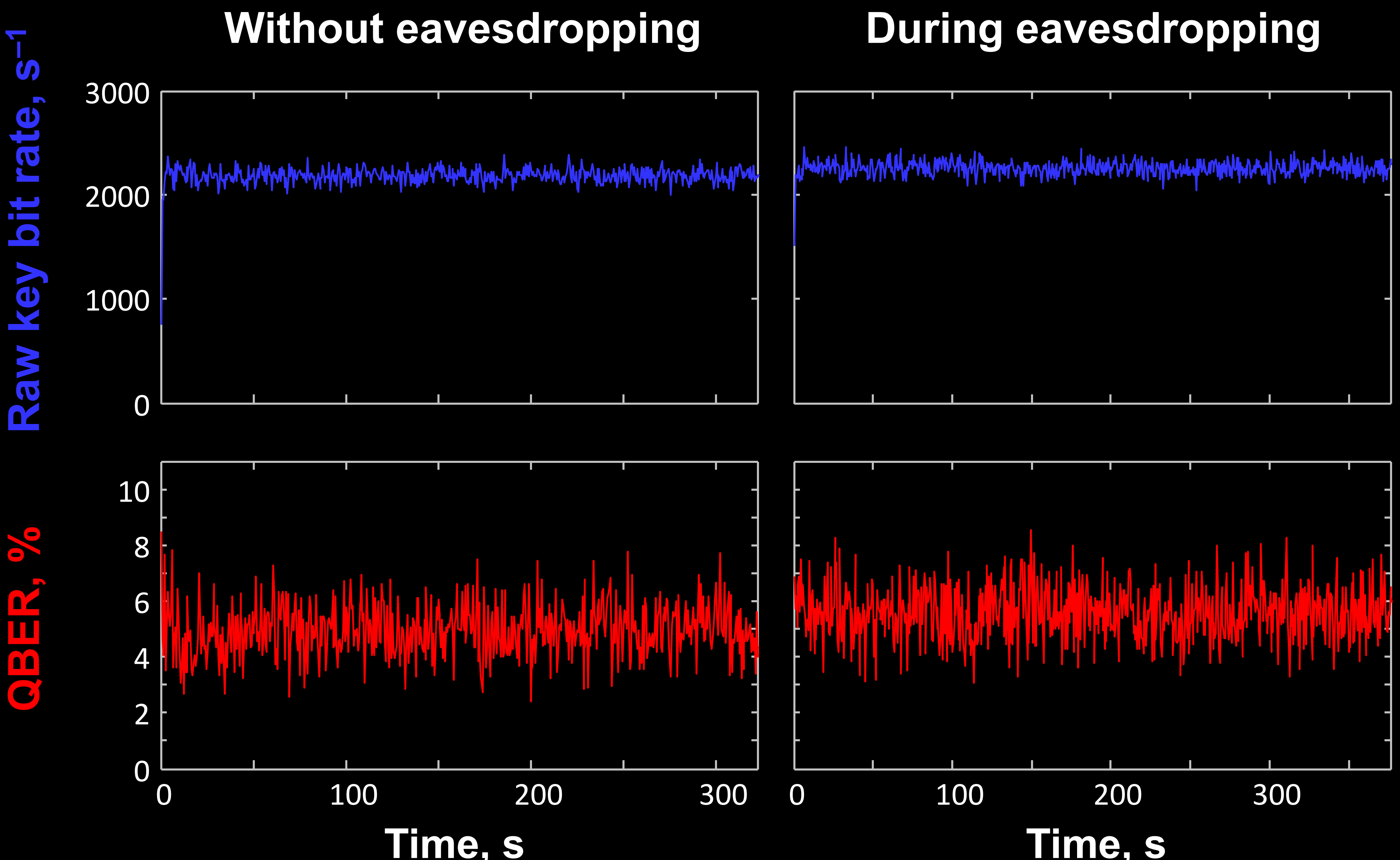
Eavesdropping 100% key on installed QKD line

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



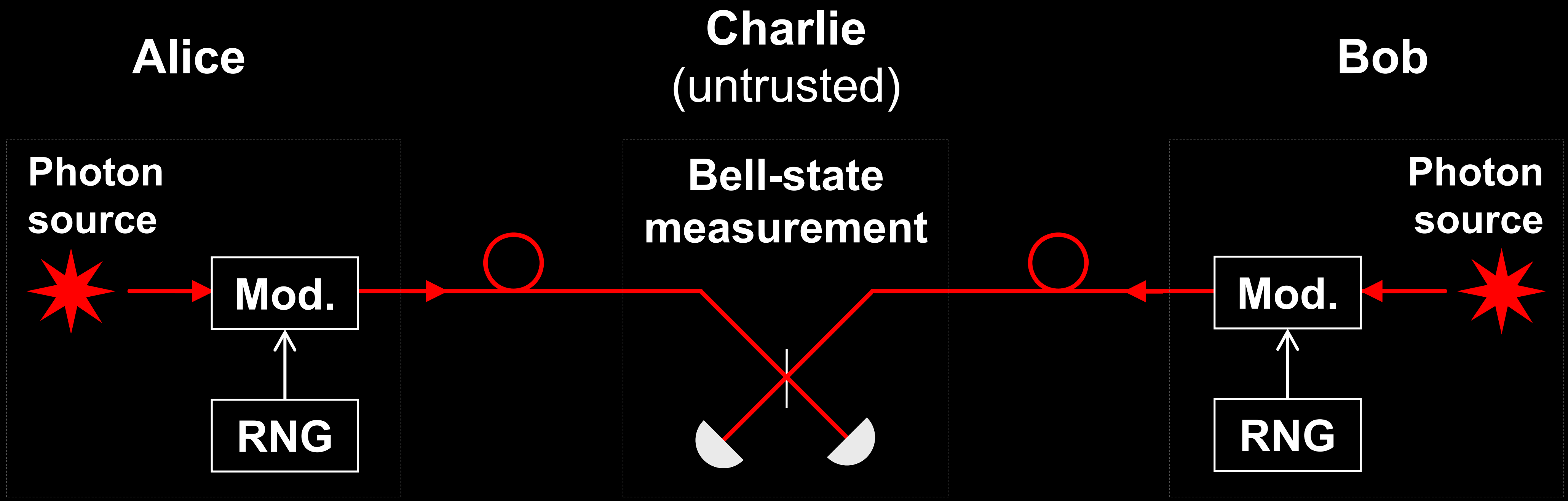
I. Gerhardt, Q. Liu *et al.*,
Nat. Commun. **2**, 349 (2011)

Eve does not affect QKD performance



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

Countermeasure to detector attacks



Measurement-device-independent QKD

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

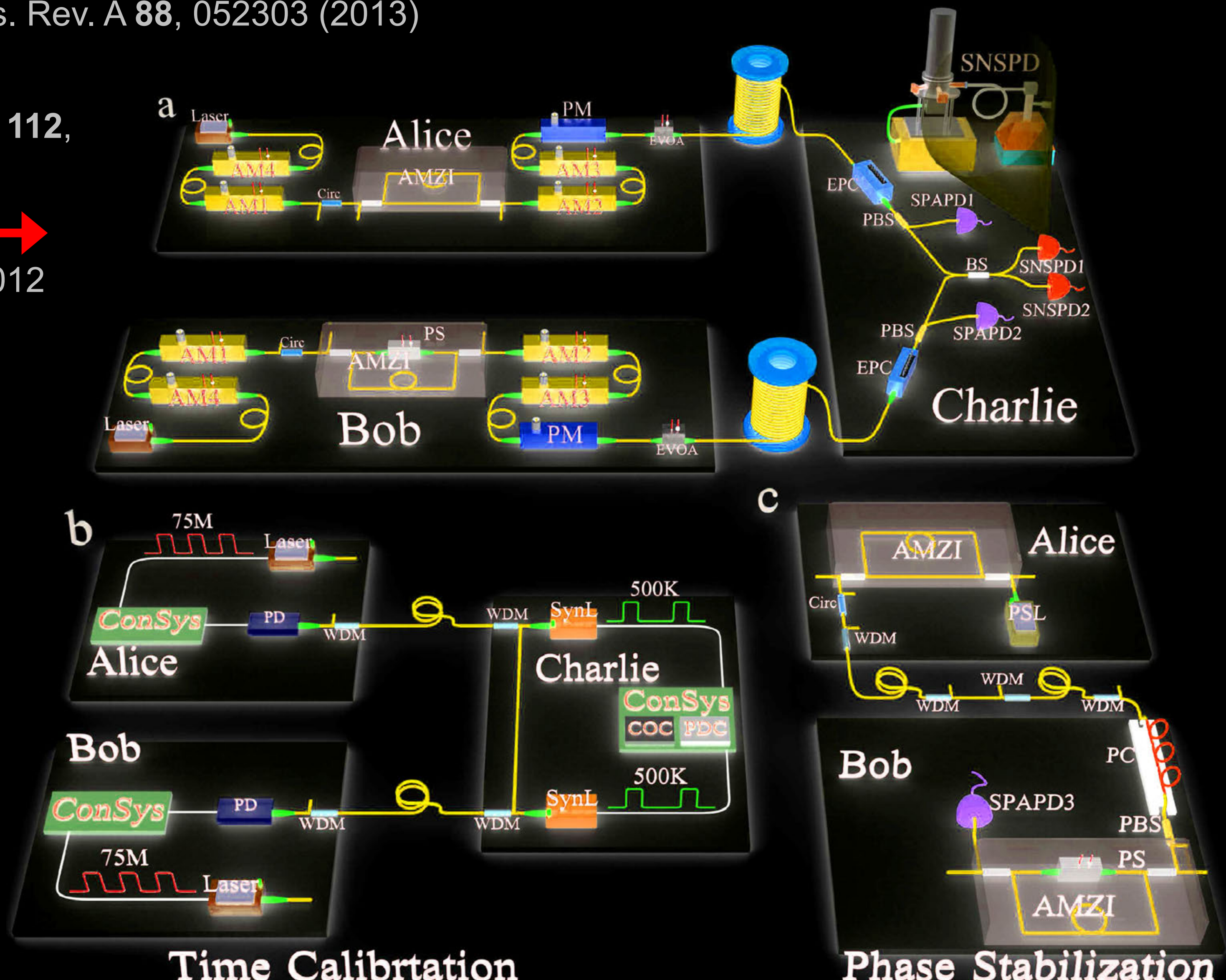
Measurement-device-independent QKD: experiments

Calgary, 28 km
A. Rubenok *et al.,* arXiv:1204.0738v2

Rio de Janeiro, 17 km
T. Ferreira da Silva *et al.,* Phys. Rev. A **88**, 052303 (2013)

Toronto, 10 km
Z. Tang *et al.,* Phys. Rev. Lett. **112**, 190503 (2014)

Hefei, 200 km
Y.-L. Tang *et al.,* arXiv:1407.8012



Industrial countermeasure (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**

2014-08-27 — **Lim *et al.* preprint about the countermeasure arXiv:1408.6398**

2014-11-18 — ★ **Implementation of countermeasure delivered by company to our lab (firmware update for Clavis2)**

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

A. Huang *et al.*, unpublished; presented at QCrypt 2015

Testing random-gate-removal countermeasure against detector blinding attack

(unpublished)

Anqi Huang
Quantum Hacking Lab

2015-10-26

Introduction: timeline

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

2014-08-27 — Lim *et al.* preprint about the countermeasure arXiv:1408.6398

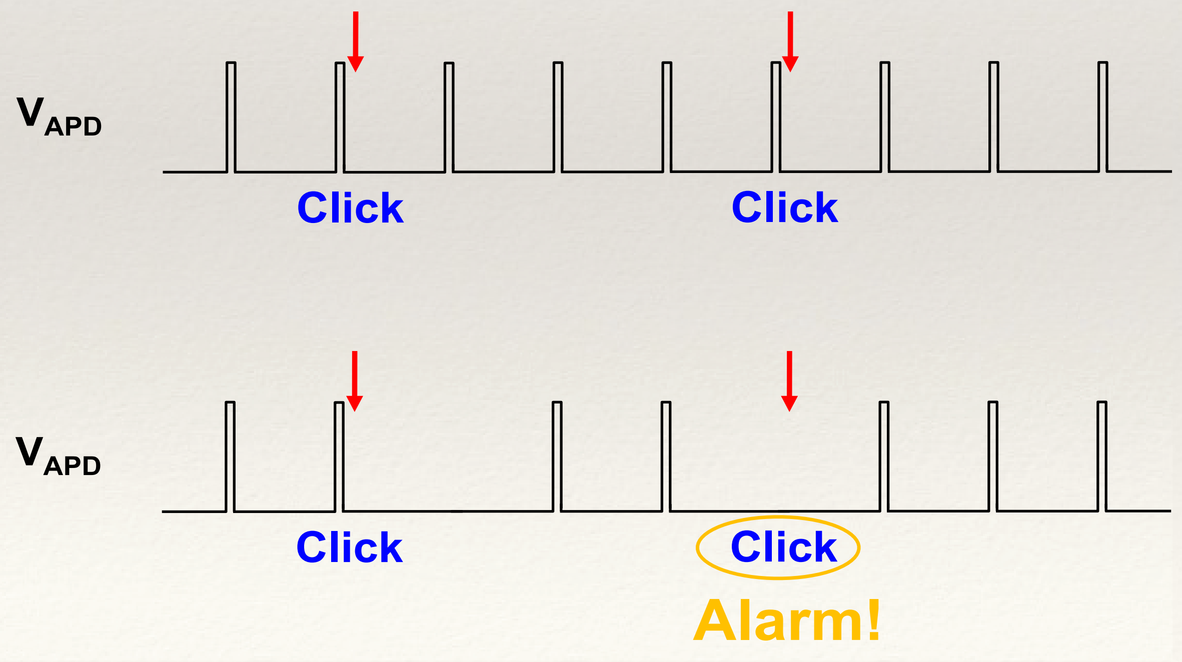
2014-11-18 — ★ Implementation of countermeasure delivered by company to our lab (firmware update for Clavis2)

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

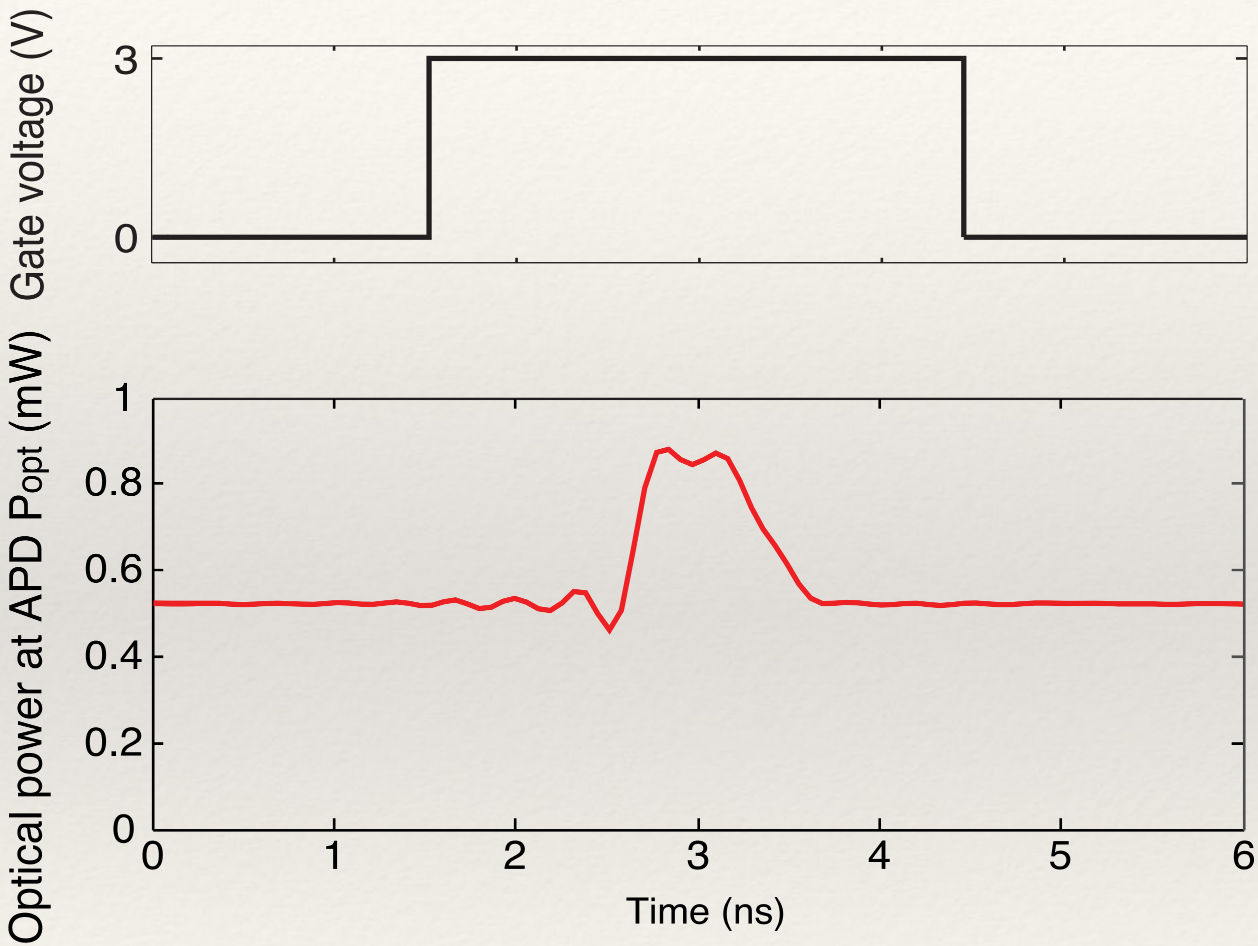
Introduction: random-gate-removal countermeasure

- Goal: introduce an information gap between Eve and Bob
- Implementation:

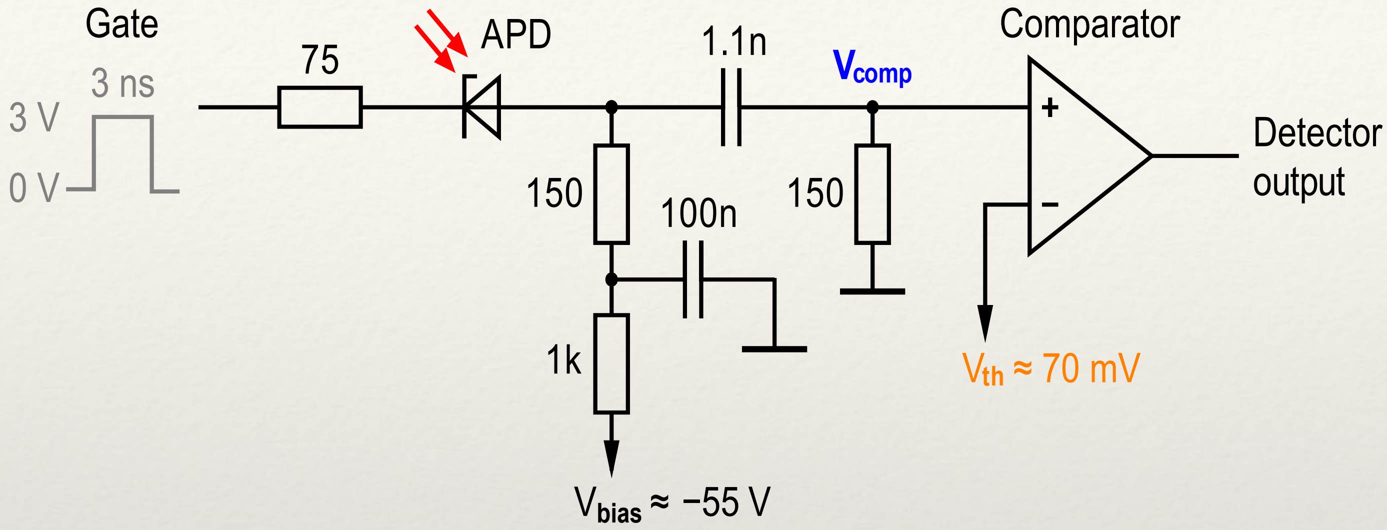
The gate is suppressed randomly with 2% probability (zero efficiency)

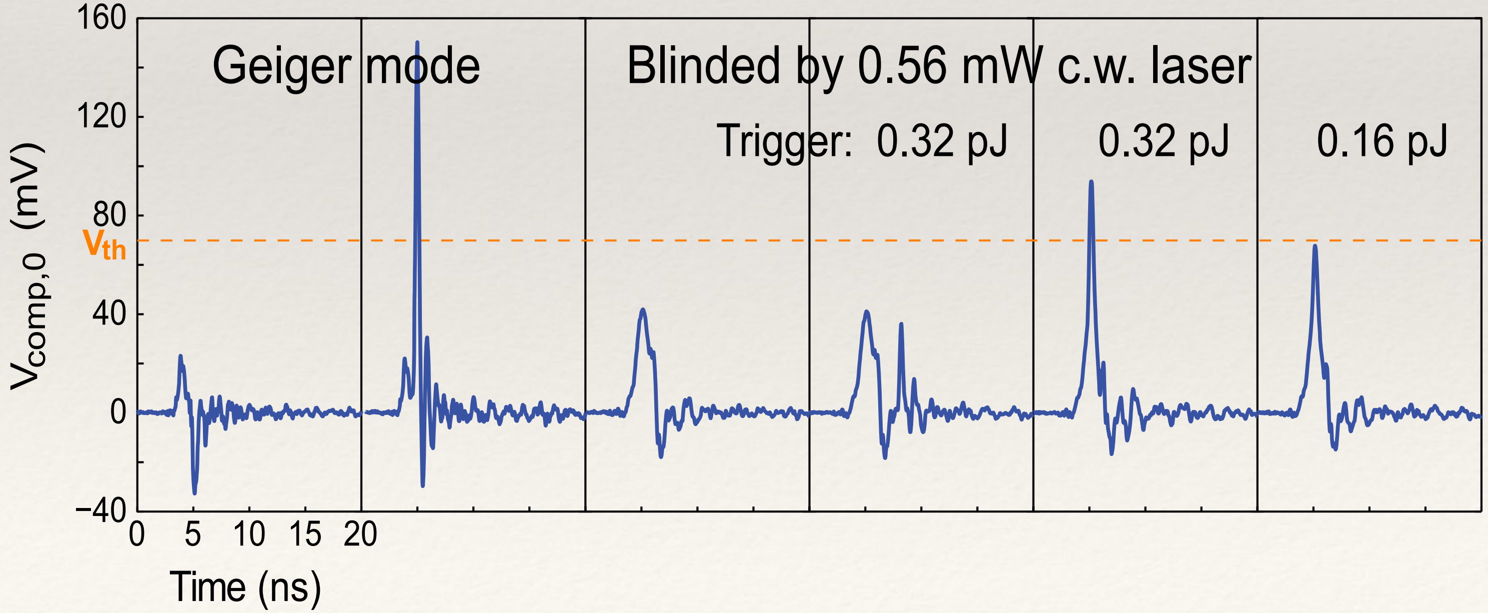


Hack the countermeasure

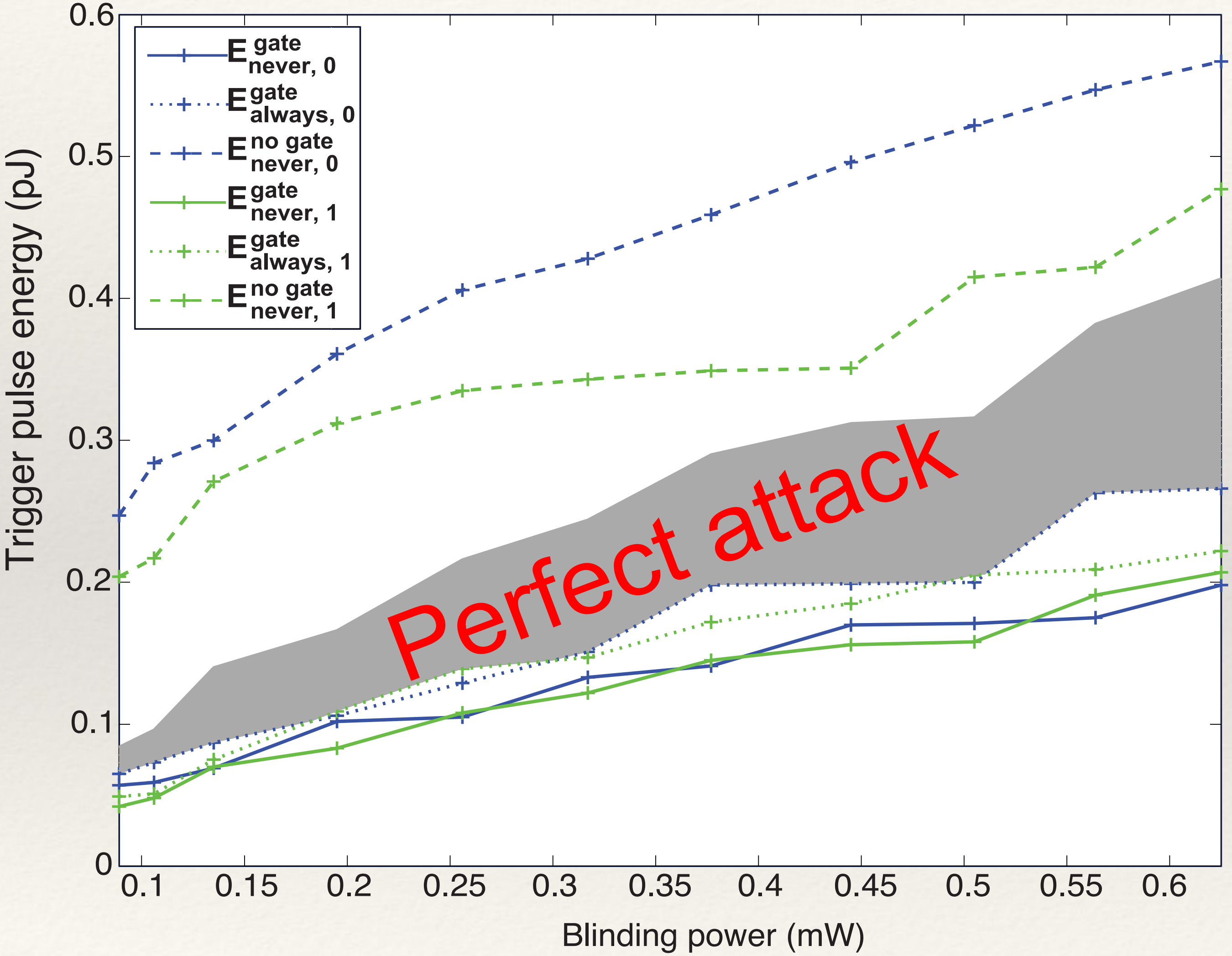


Hack the countermeasure





Hack the countermeasure



Thresholds:

If energy of trigger pulse $E \leq E^{gate}_{never,\ i}$

detectors never click when the gate is applied.

If $E \geq E^{gate}_{always,\ i}$

detectors always click when the gate is applied.

If $E \leq E^{no\ gate}_{never,\ i}$

detectors never click when the gate is not applied.

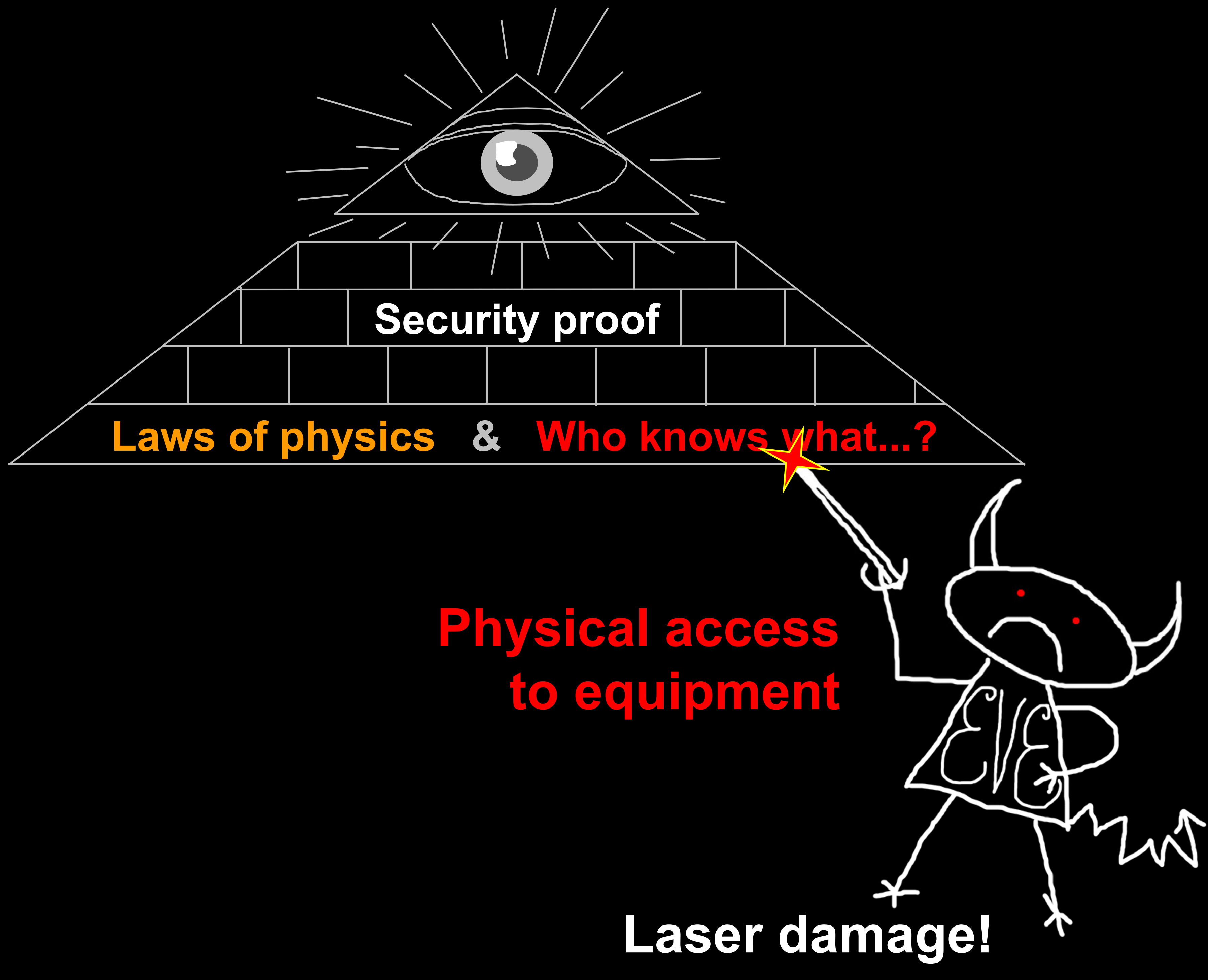
Click thresholds versus c.w. blinding power. Shaded area shows the range of trigger pulse energies of the attack.

Conclusion

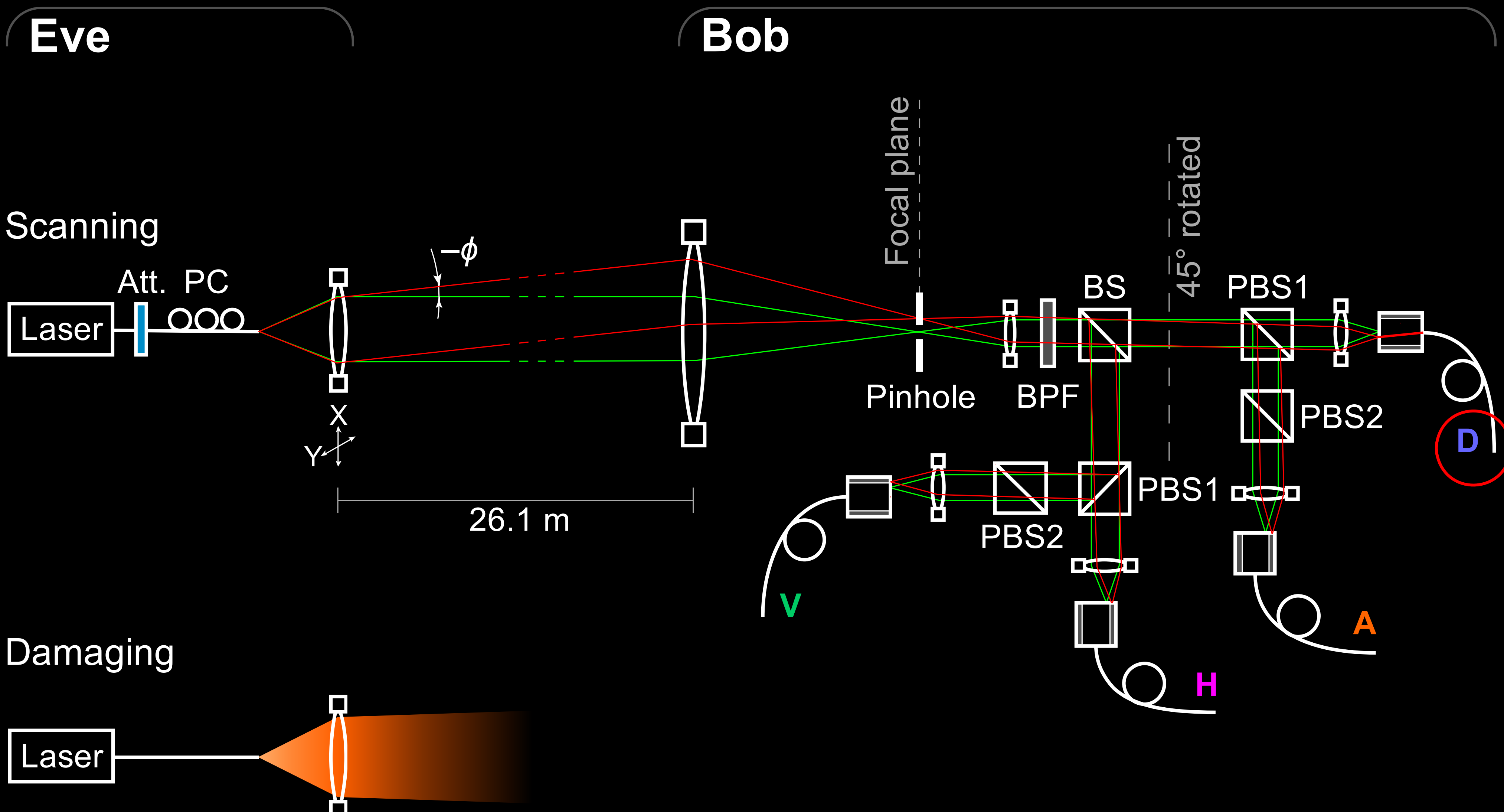
Countermeasure doesn’t work!


IDQ
little
helper
Alice
KING SIZE

Limits on physical security

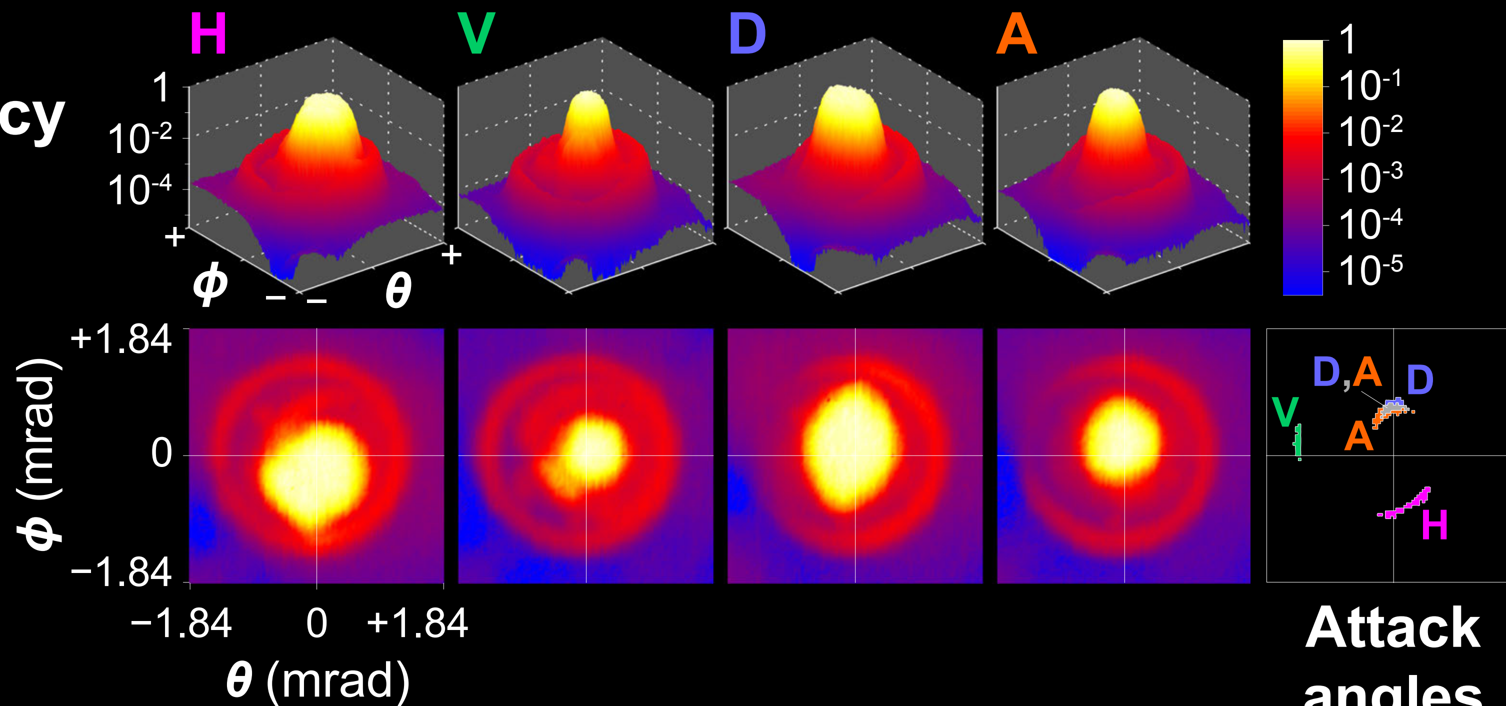


Efficiency mismatch in QKD receiver



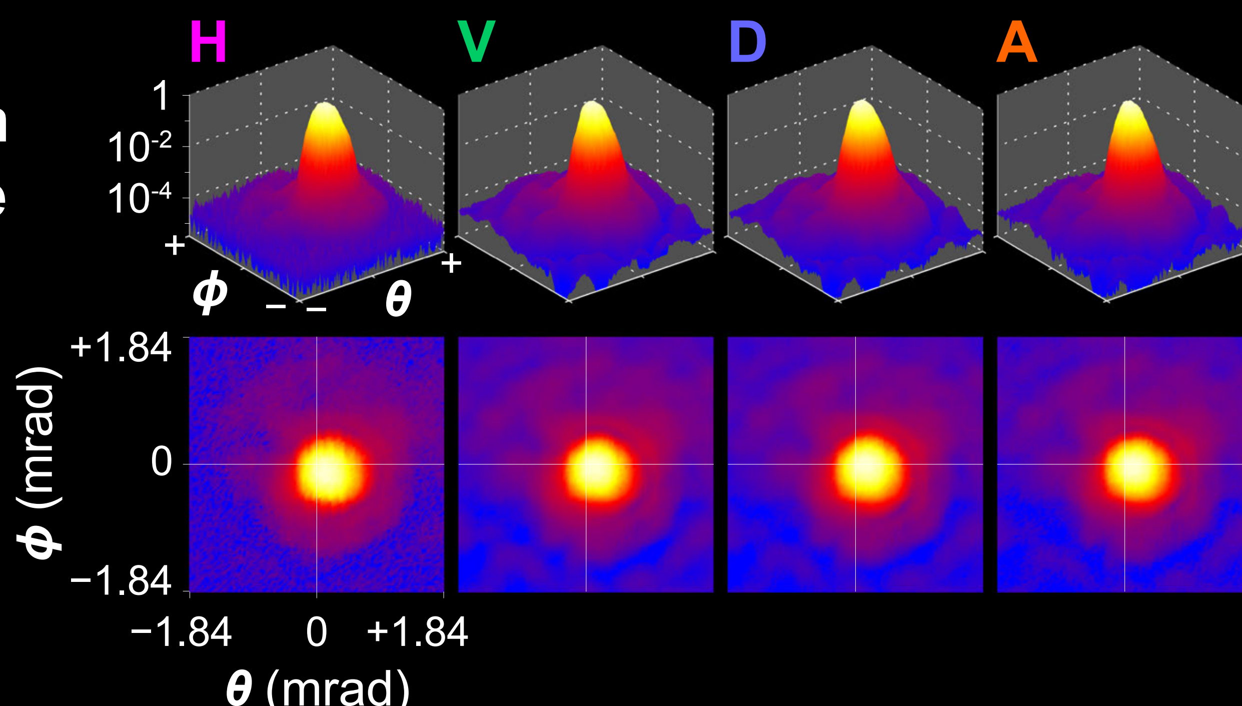
S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015)
V. Makarov *et al.*, arXiv:1510.03148

Detector efficiency without pinhole



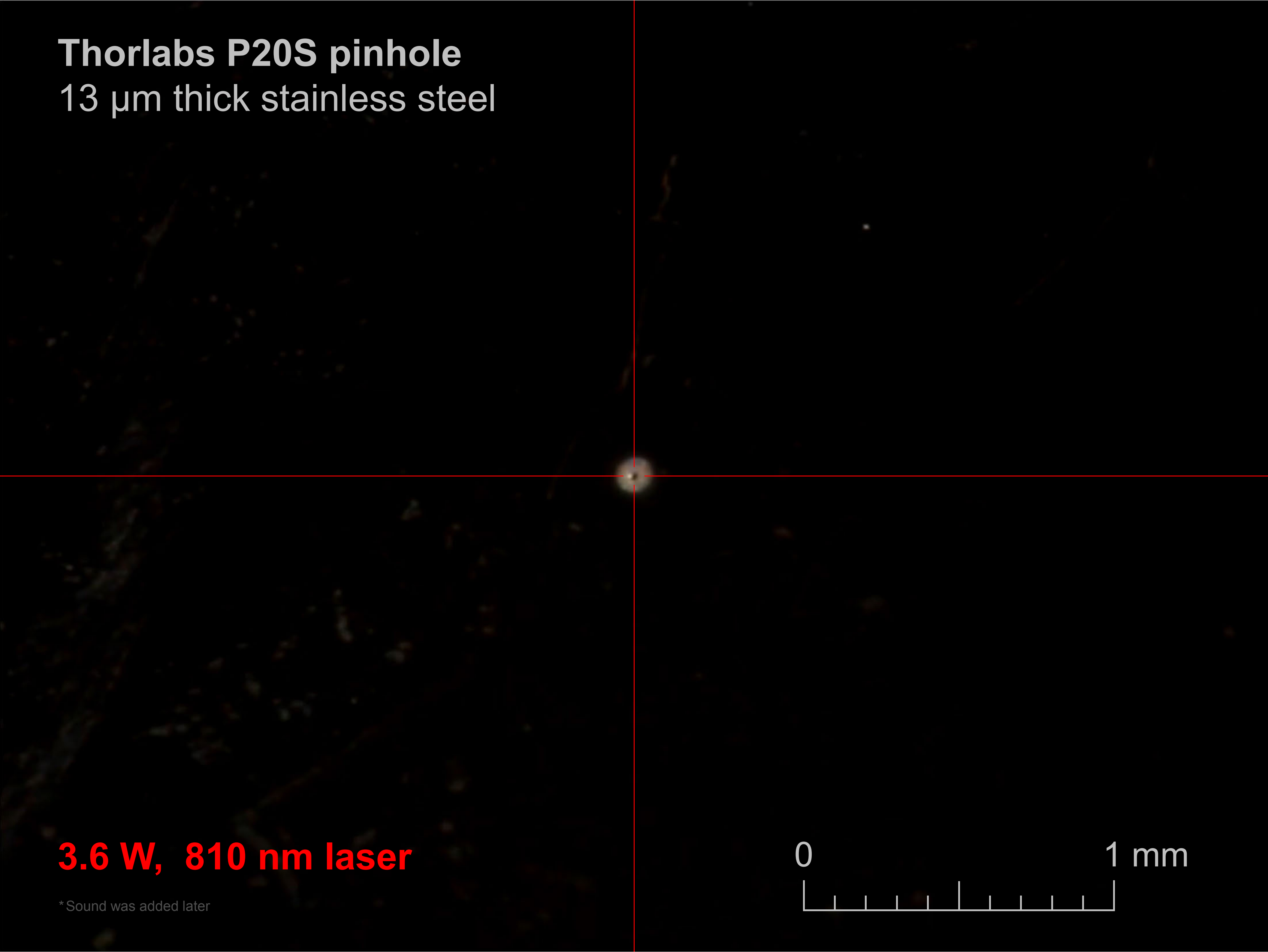
Attack angles

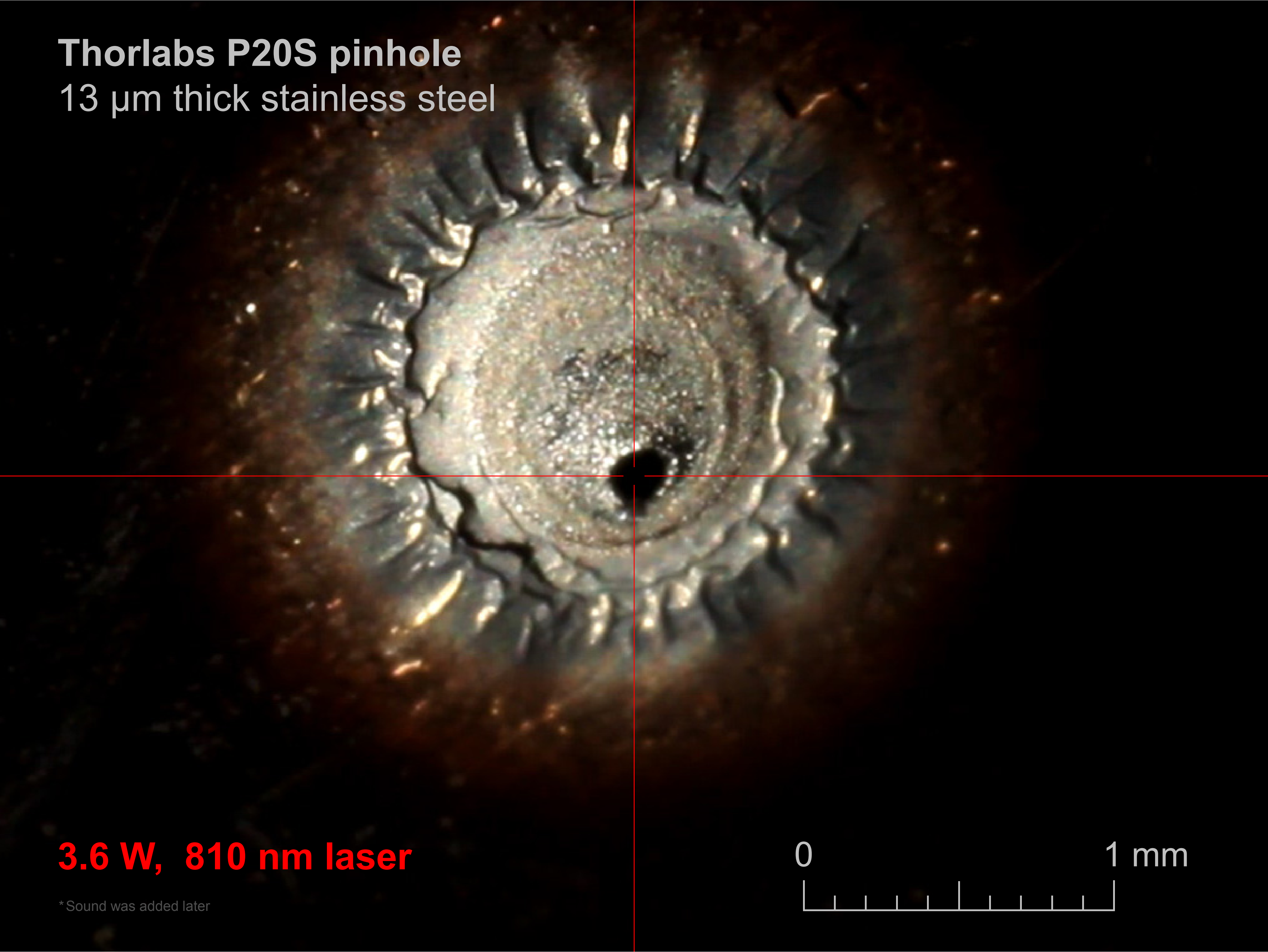
...and with 25 μm diameter pinhole



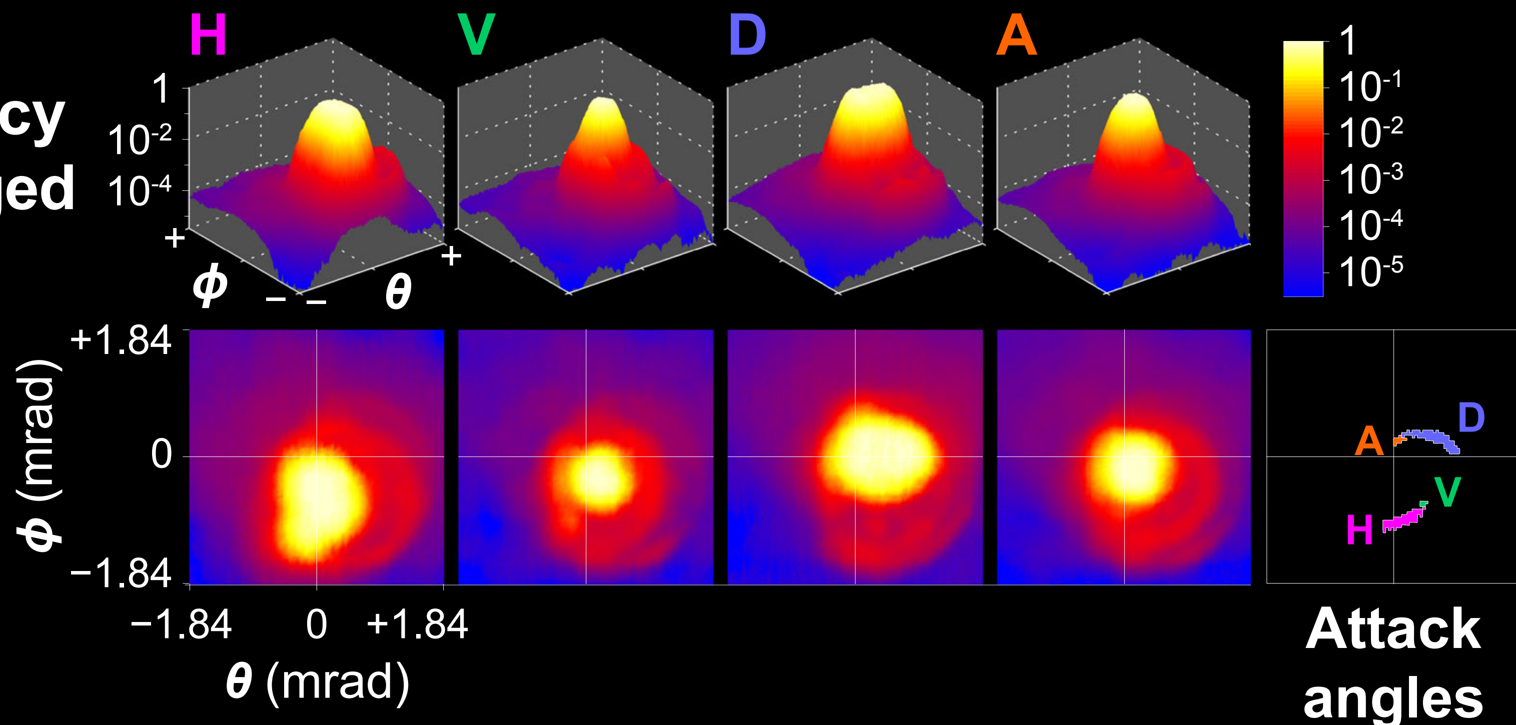
No attack found

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

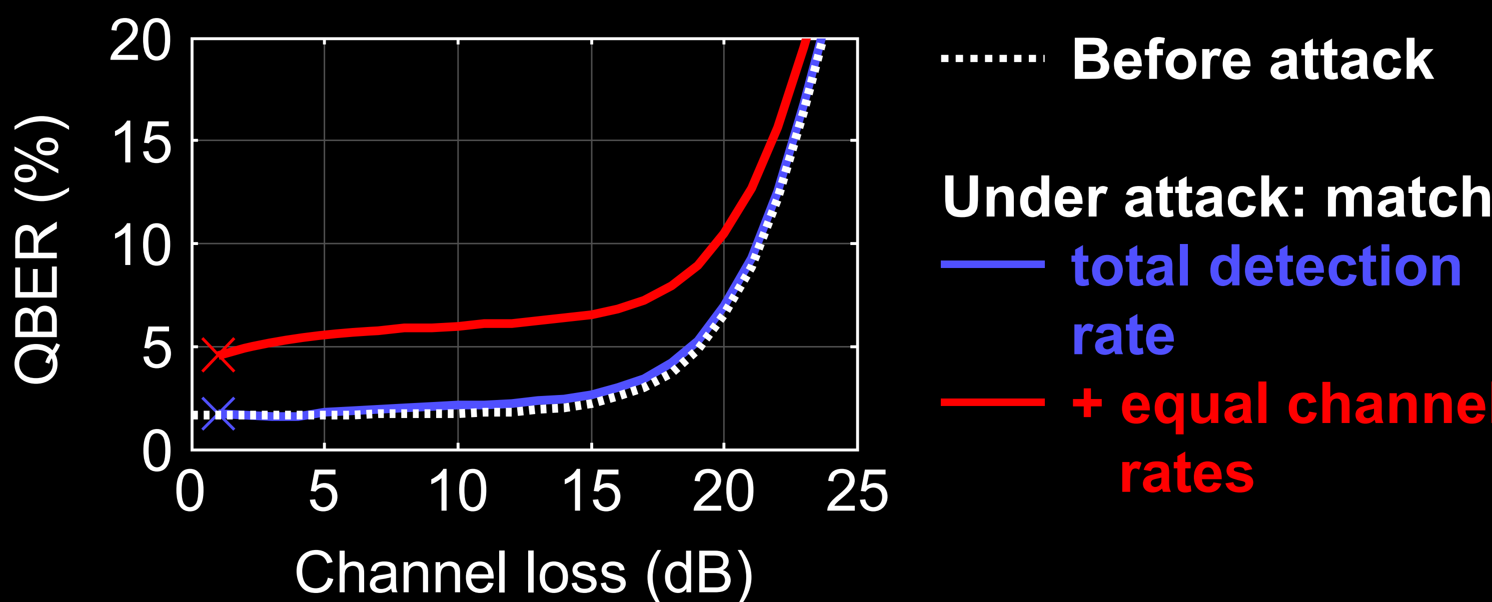

Thorlabs P20S pinhole
13 µm thick stainless steel
3.6 W, 810 nm laser
* Sound was added later
0
1 mm


Thorlabs P20S pinhole
13 µm thick stainless steel
3.6 W, 810 nm laser
*Sound was added later
0
1 mm

Detector efficiency with laser-damaged pinhole

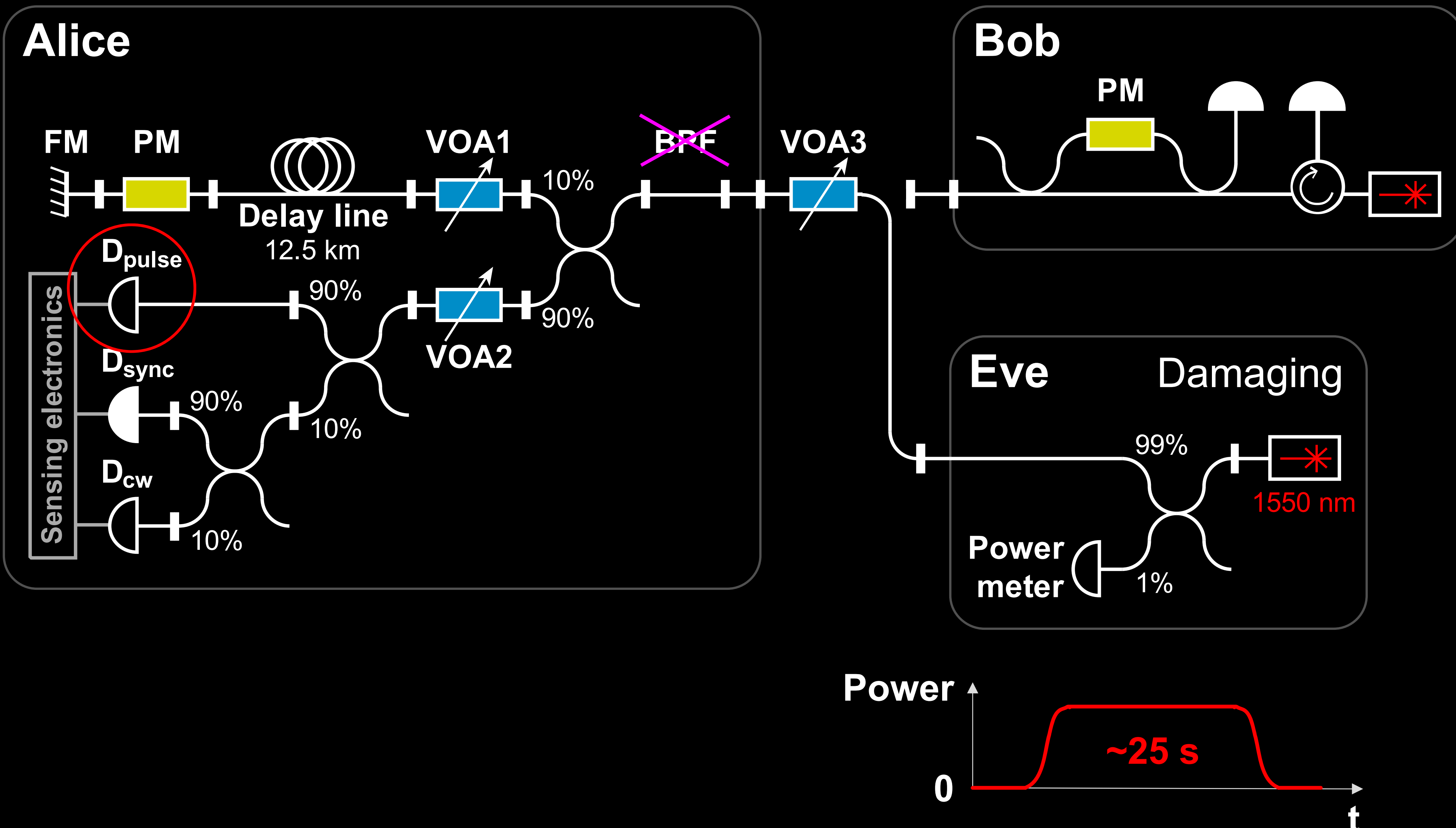


Attack performance



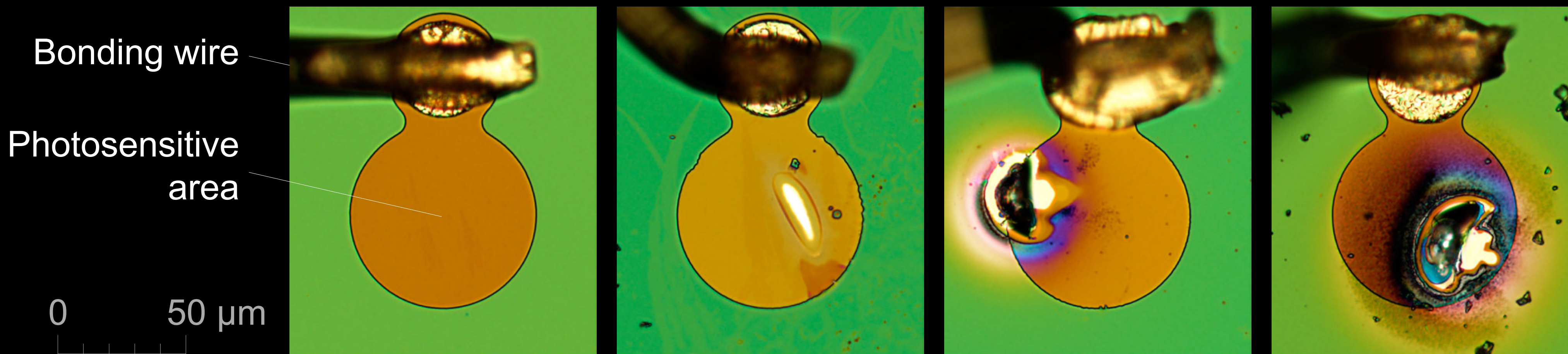
V. Makarov *et al.*, arXiv:1510.03148

Laser damage in commercial QKD system Clavis2



V. Makarov *et al.*, arXiv:1510.03148

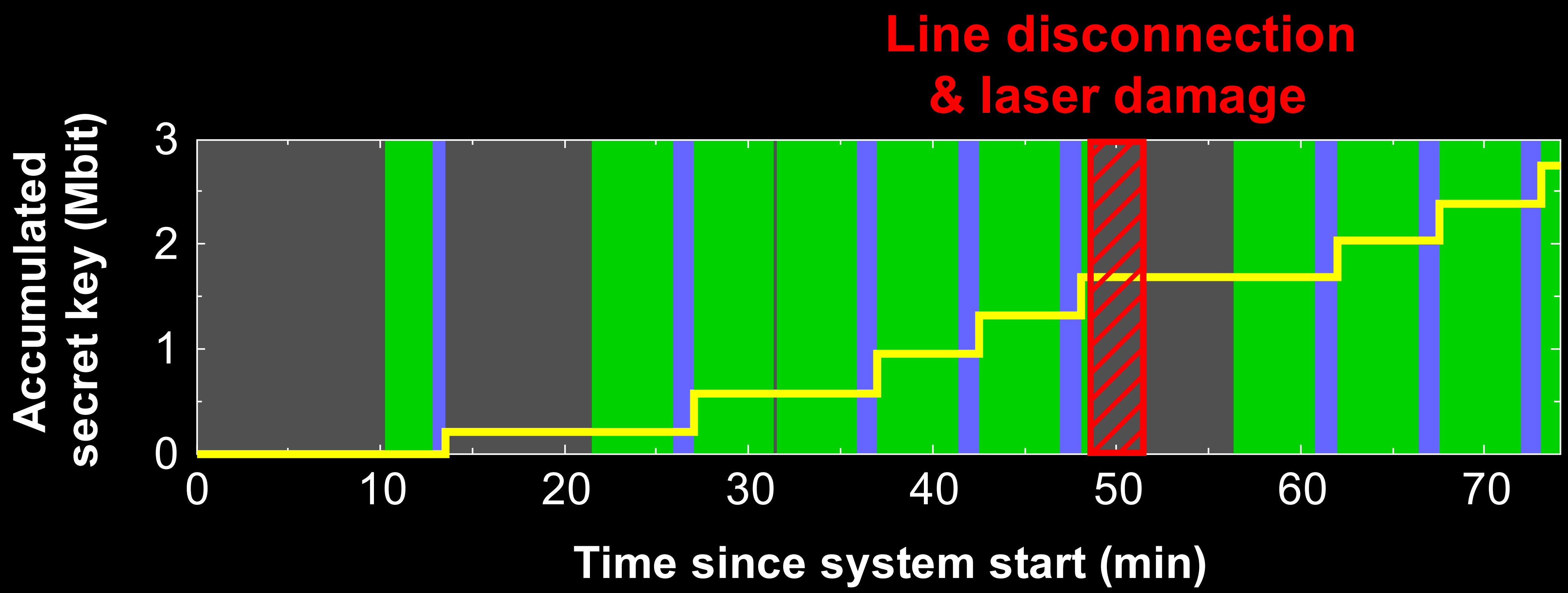
InGaAs p-i-n photodiode D_{pulse} (JDSU EPM 605LL)



Damaging power at Alice's entrance (W)	**none**	**1.0**	**1.5**	**1.7**
Loss of photo-sensitivity (dB)	**undamaged**	**1.6**	**5.5**	**completely lost photosensitivity**

V. Makarov *et al.*, arXiv:1510.03148

QKD system log



System service & recalibration routines

Qubit exchange

Classical post-processing

V. Makarov *et al.*, arXiv:1510.03148

Credits

Institute for Quantum Computing

Shihan Sajeed
Sarah Kaiser
Anqi Huang
Poompong Chaiwongkhot
Jean-Philippe Bourgoin
Carter Minshull
Thomas Jennewein
Norbert Lütkenhaus
Vadim Makarov

POLYTECHNIQUE MONTRÉAL

Mathieu Gagné
Raman Kashyap

IDQ

Mathilde Soucarros
Matthieu Legré

IQC Institute *for* Quantum Computing

Quantum hacking lab

www.vad1.com/lab

IQC Institute *for* Quantum Computing

Quantum hacking lab

www.vad1.com/lab