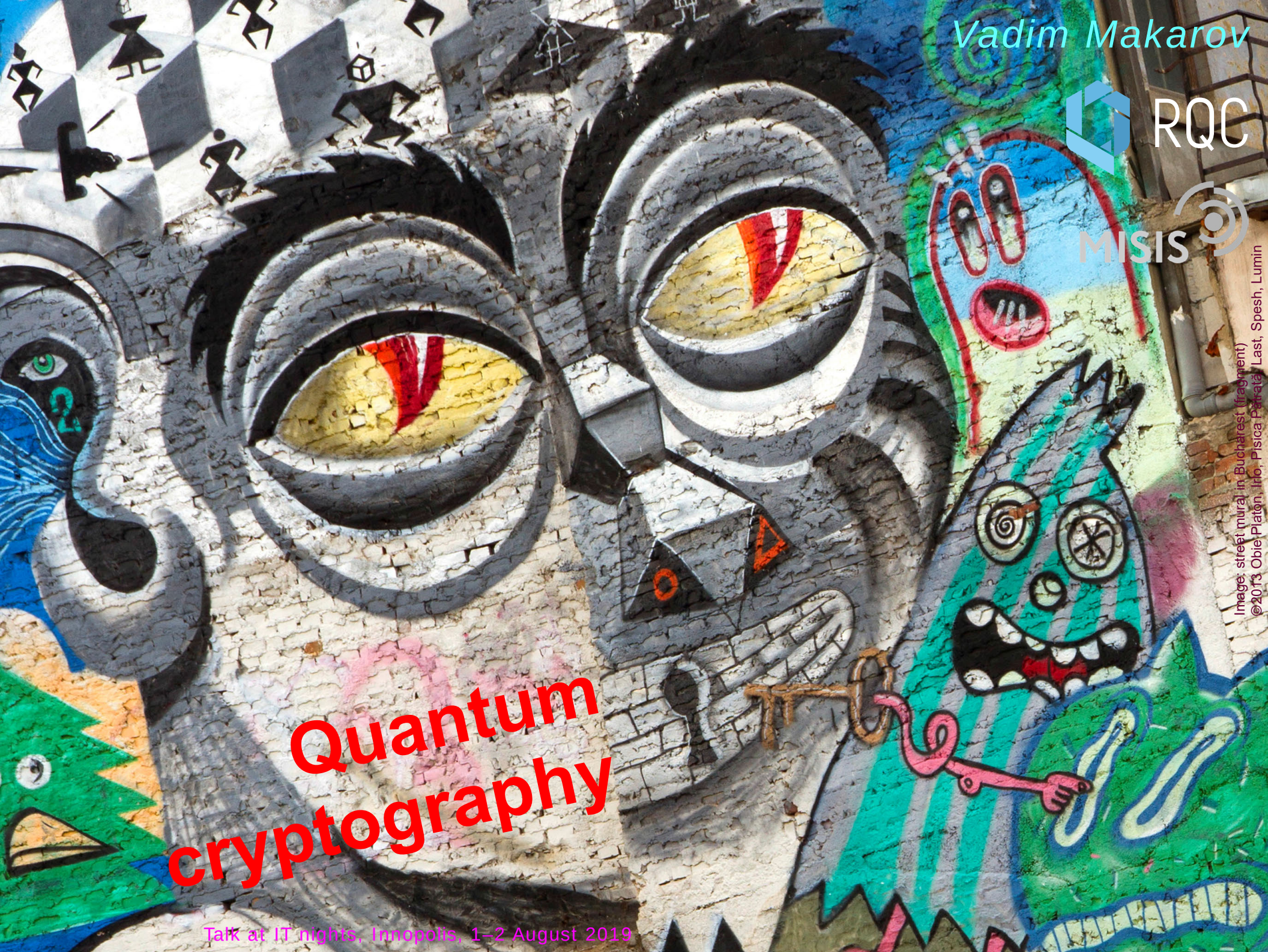


Vadim Makarov

RQC

MISIS

# Quantum cryptography

Talk at IT nights, Innopolis, 1–2 August 2019

Image: street mural in Bucharest (fragment)

# A (very) brief history of cryptography

| | | Broken? |
|---|---|---|
| **Monoalphabetic cipher** | invented ~50 BC (J. Caesar) | ~850 (Al-Kindi) |
| **Nomenclators (code books)** | ~1400 – ~1800 | ✓ |
| **Polyalphabetic (Vigenère)** | 1553 – ~1900 | 1863 (F. W. Kasiski) |
| … | | |
| **Polyalphabetic electromechanical (Enigma, Purple, etc.)** | 1920s – 1970s | ✓ |
| … | | |
| **DES** | 1977 – 2005 | 1998: 56 h (EFF) |
| **Public-key crypto (RSA, elliptic-curve)** | 1977 – | will be once we have q. computer (P. Shor 1994) |
| **AES** | 2001 – | ? |
| **Public-key crypto ('quantum-safe')** | in development | ? |

# Breaking cryptography retroactively


Photo ©2013 AP / Rick Bowmer

# Mosca theorem

*y* (re-tool infrastructure)

*x* (encryption needs be secure)

*z* (time to build large quantum computer)

Time

If $x + y > z$, then worry.

M. Mosca, http://eprint.iacr.org/2015/1075

# A (very) brief history of cryptography

| | | Broken? |
|---|---|---|
| **Monoalphabetic cipher** | invented ~50 BC (J. Caesar) | ~850 (Al-Kindi) |
| **Nomenclators (code books)** | ~1400 – ~1800 | ✓ |
| **Polyalphabetic (Vigenère)** | 1553 – ~1900 | 1863 (F. W. Kasiski) |
| … | | |
| **One-time pad** | invented 1918 (G. Vernam) | **impossible** (C. Shannon 1949) |
| **Polyalphabetic electromechanical (Enigma, Purple, etc.)** | 1920s – 1970s | ✓ |
| … | | |
| **DES** | 1977 – 2005 | 1998: 56 h (EFF) |
| **Public-key crypto (RSA, elliptic-curve)** | 1977 – | will be once we have q. computer (P. Shor 1994) |
| **AES** | 2001 – | ? |
| **Quantum cryptography** | invented 1984, in development | **impossible*** |
| **Public-key crypto ('quantum-safe')** | in development | ? |

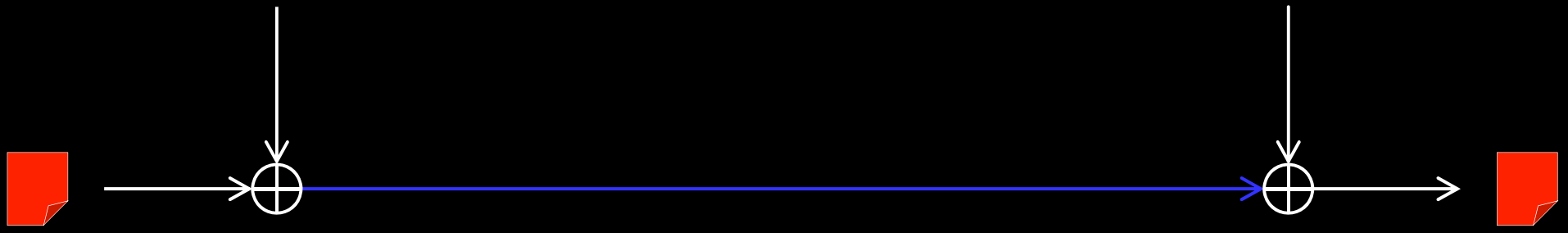
# One-time pad

Alice

Bob

**Random secret key** of same length as message

**Random secret key**



**Message**

**Message**

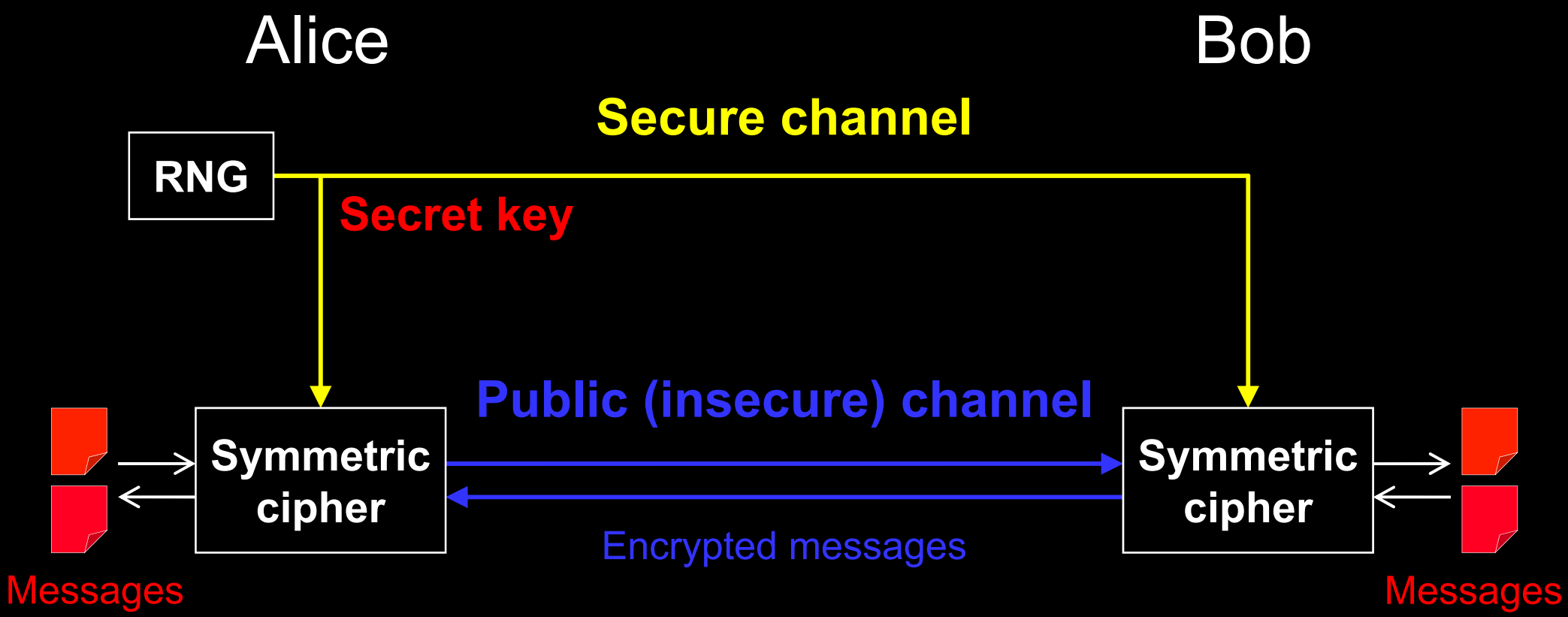
| α | β | α⊕β |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

G. Vernam, U.S. patent 1310719 (filed in 1918, granted 1919)
C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949)

# A (very) brief history of cryptography

| | | Broken? |
|---|---|---|
| **Monoalphabetic cipher** | invented ~50 BC (J. Caesar) | ~850 (Al-Kindi) |
| **Nomenclators (code books)** | ~1400 – ~1800 | ✓ |
| **Polyalphabetic (Vigenère)** | 1553 – ~1900 | 1863 (F. W. Kasiski) |
| … | | |
| **One-time pad** | invented 1918 (G. Vernam) | **impossible** (C. Shannon 1949) |
| **Polyalphabetic electromechanical (Enigma, Purple, etc.)** | 1920s – 1970s | ✓ |
| … | | |
| **DES** | 1977 – 2005 | 1998: 56 h (EFF) |
| **Public-key crypto (RSA, elliptic-curve)** | 1977 – | will be once we have q. computer (P. Shor 1994) |
| **AES** | 2001 – | ? |
| **Quantum cryptography** | invented 1984, in development | **impossible*** |
| **Public-key crypto ('quantum-safe')** | in development | ? |

# Key distribution for encryption




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

# Quantum key distribution (QKD)

Alice

Bob

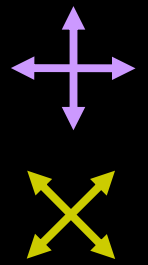
**Prepares photons**

(0), (1)

(0), (1)

**or**  **?**


**Measures photons**



**Eavesdropping introduces errors**

C. H. Bennett, G. Brassard (1984)

# Post-processing in QKD

Alice ⟷ **Classical channel** (e.g., internet) ⟷ Bob

**Raw photon detection data**

↓

**Sifting** (discard bits Bob failed to detect or detected in incompatible basis)

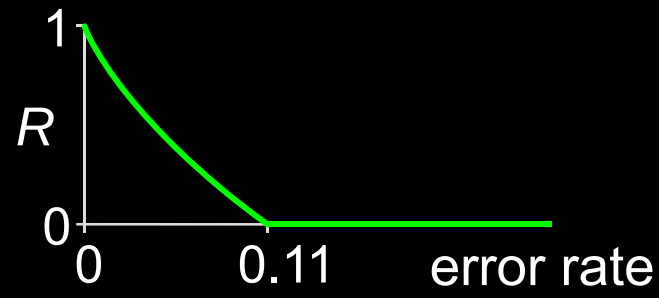
↓

**Error correction**

↓ error rate

**Secret key rate estimation**

↓ $R$




**Privacy amplification** (compress key using a hash function)

↓

**Authentication Alice–Bob** ← 1st time: initial short key, or public-key infrastructure

↓

**Secret key** — small fraction → **Authentication Alice–Bob**

C. H. Bennett *et al.*, J. Cryptology **5**, 3 (1992); N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999)

# 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)

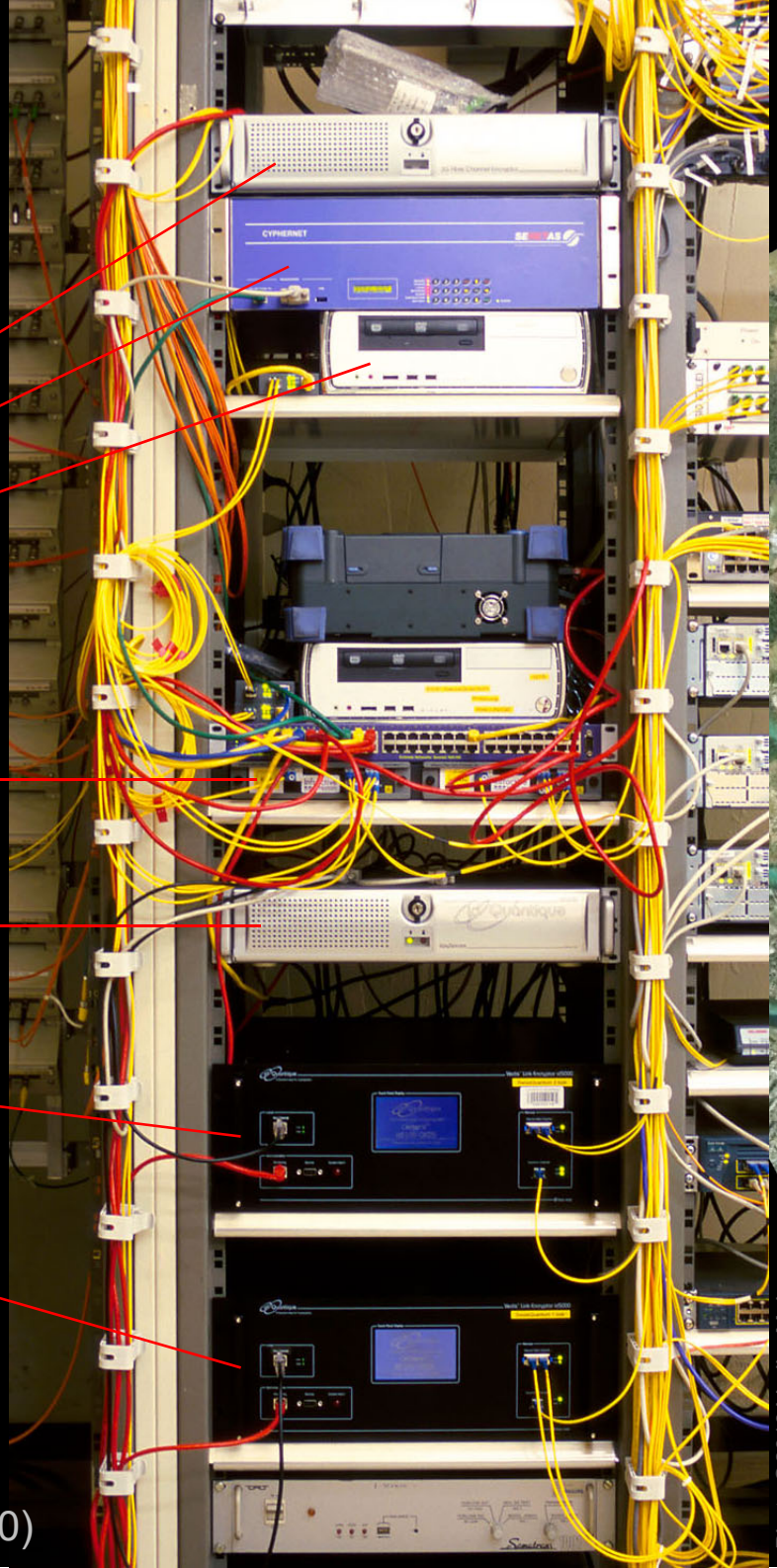
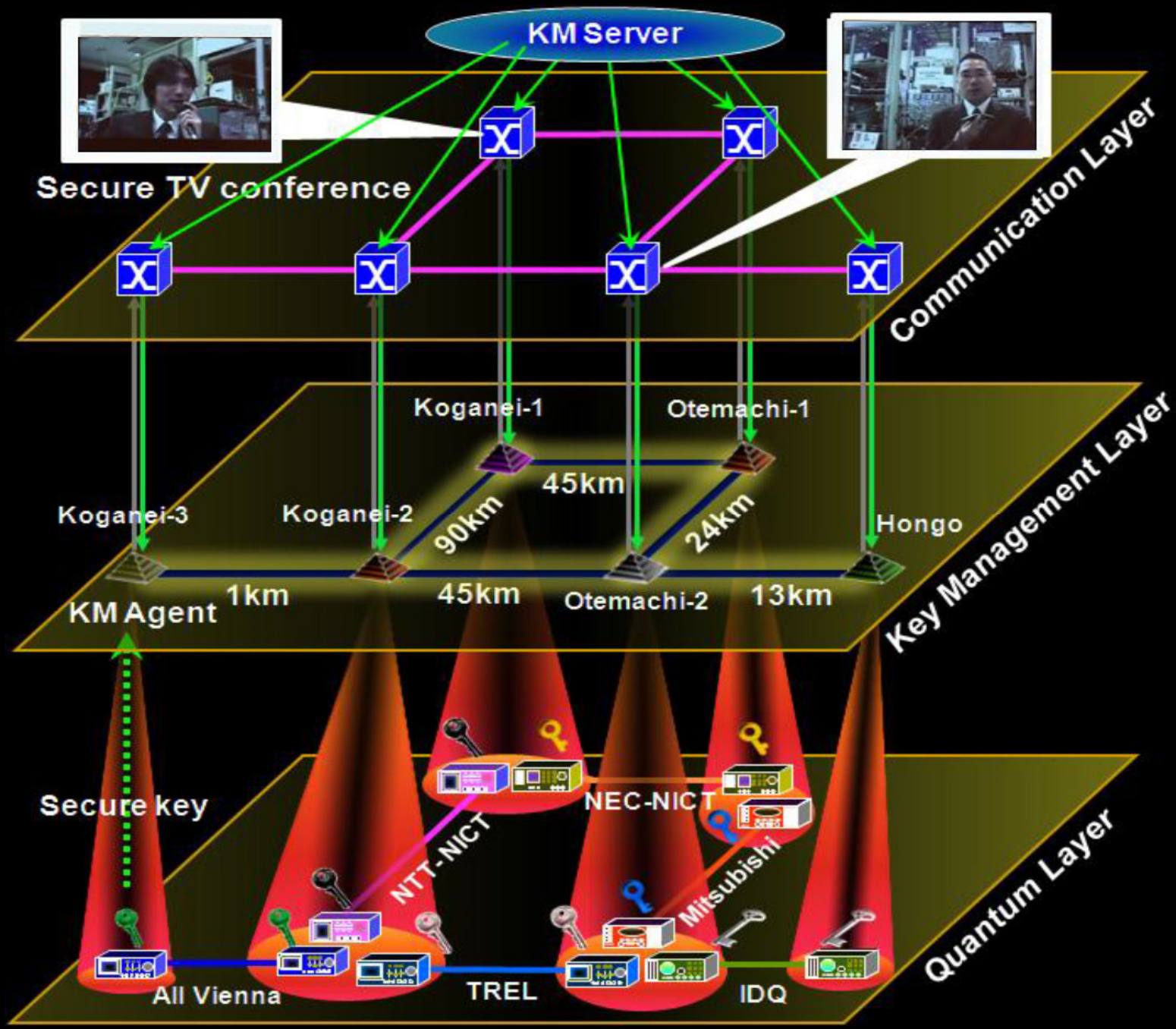



Photo ©2010 Vadim Makarov

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

# Trusted-node network

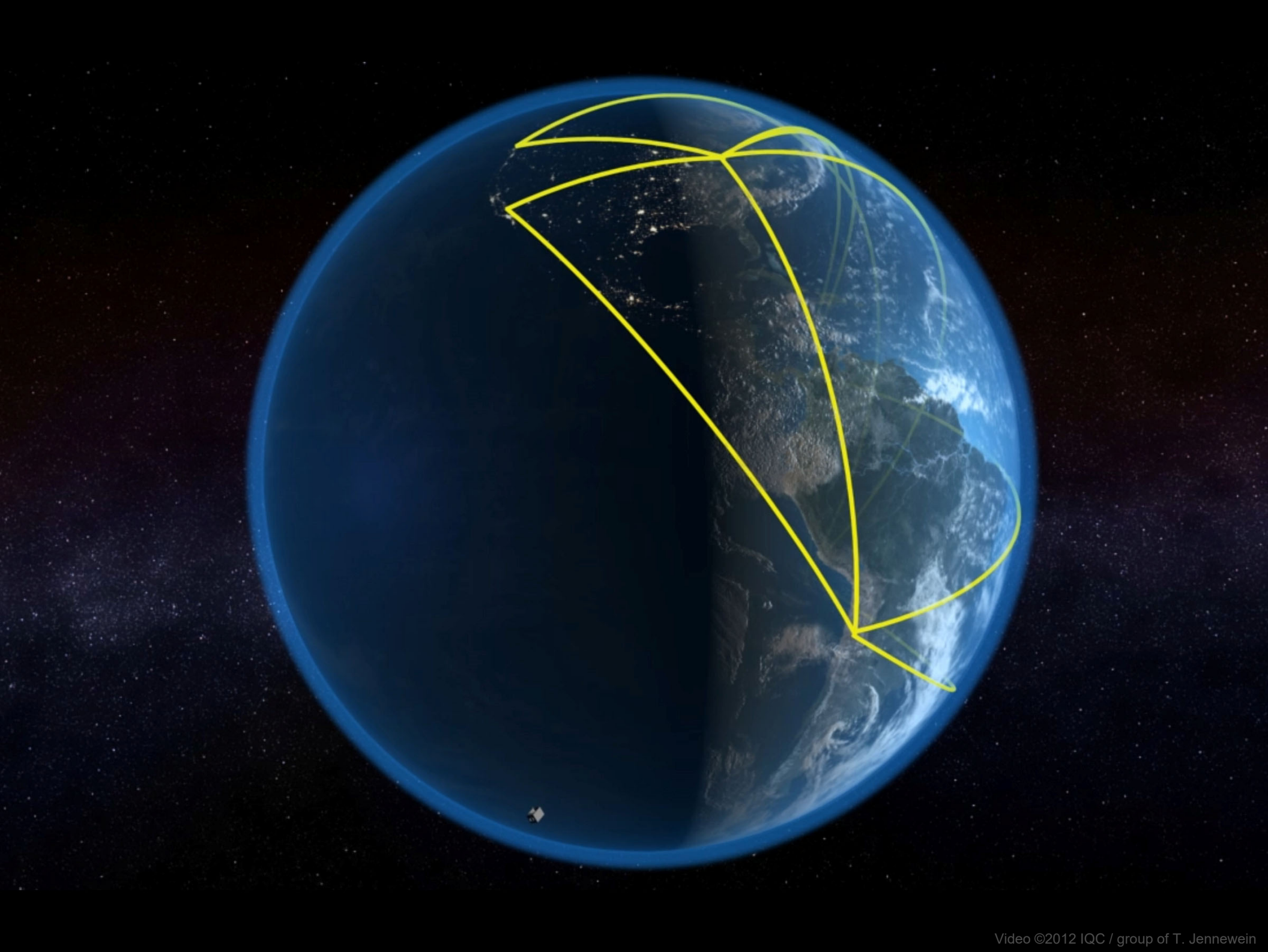



M. Sasaki *et al.*, Opt. Express **19**, 10387 (2011)

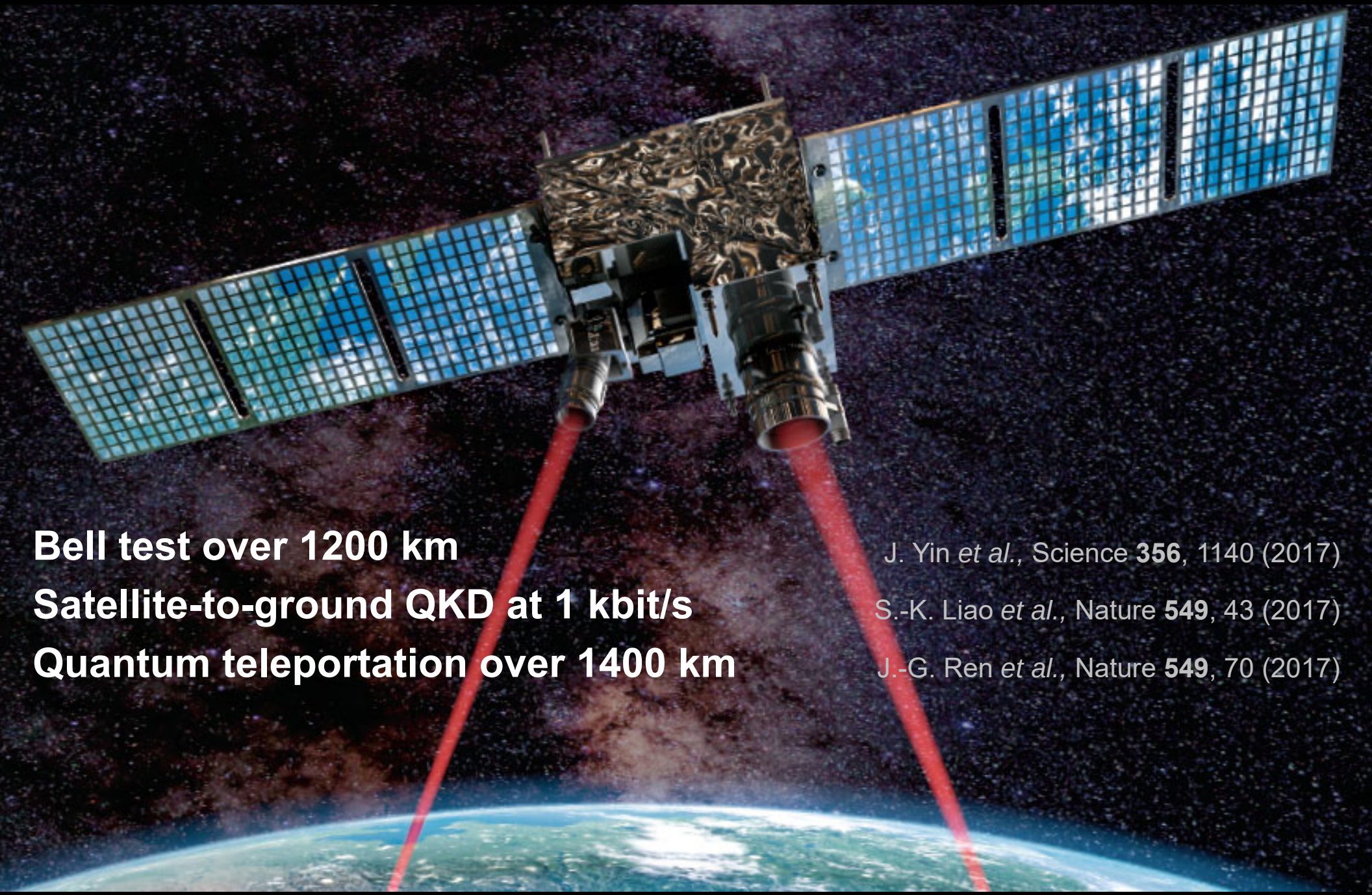



**Shanghai control center of the Chinese quantum key distribution network and satellite**


Global
quantum key distribution
Video ©2012 IQC / group of T. Jennewein



# **Chinese quantum satellite Micius** (launched 2016)



**Bell test over 1200 km**

**Satellite-to-ground QKD at 1 kbit/s**

**Quantum teleportation over 1400 km**

J. Yin *et al.*, Science **356**, 1140 (2017)

S.-K. Liao *et al.*, Nature **549**, 43 (2017)

J.-G. Ren *et al.*, Nature **549**, 70 (2017)

# Certification of cryptographic tools

Government

National security agency

Legal requirements

Approval

Accredited lab


System

Certificate

Engineering documentation

IDQ

Manufacturer

Sale

Customer

# Certification of cryptographic tools

Government

National security agency

Legal requirements

Approval

Accredited lab

Russia: optional for commercial uses

System


Certificate

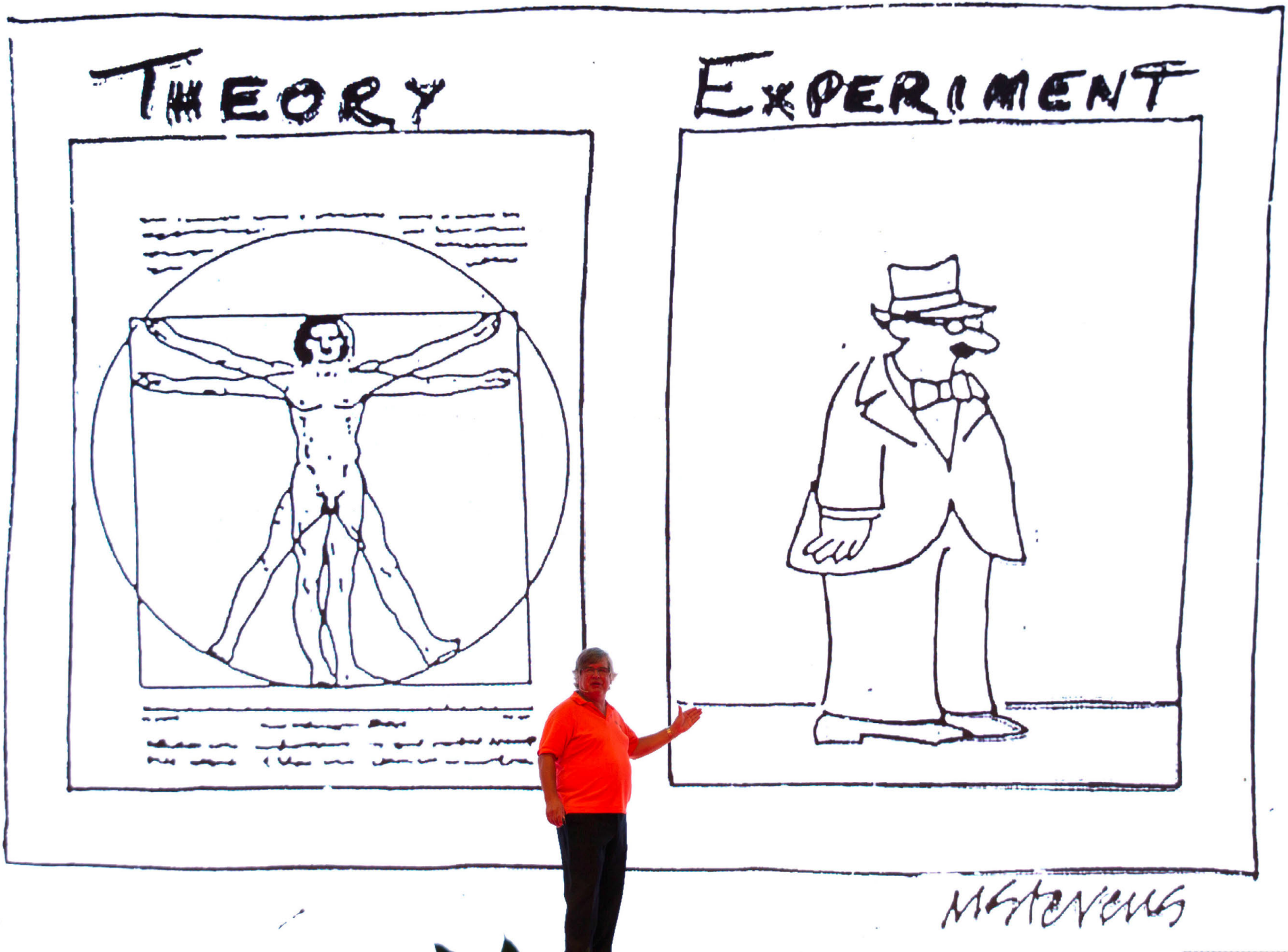
Engineering documentation

IDQ

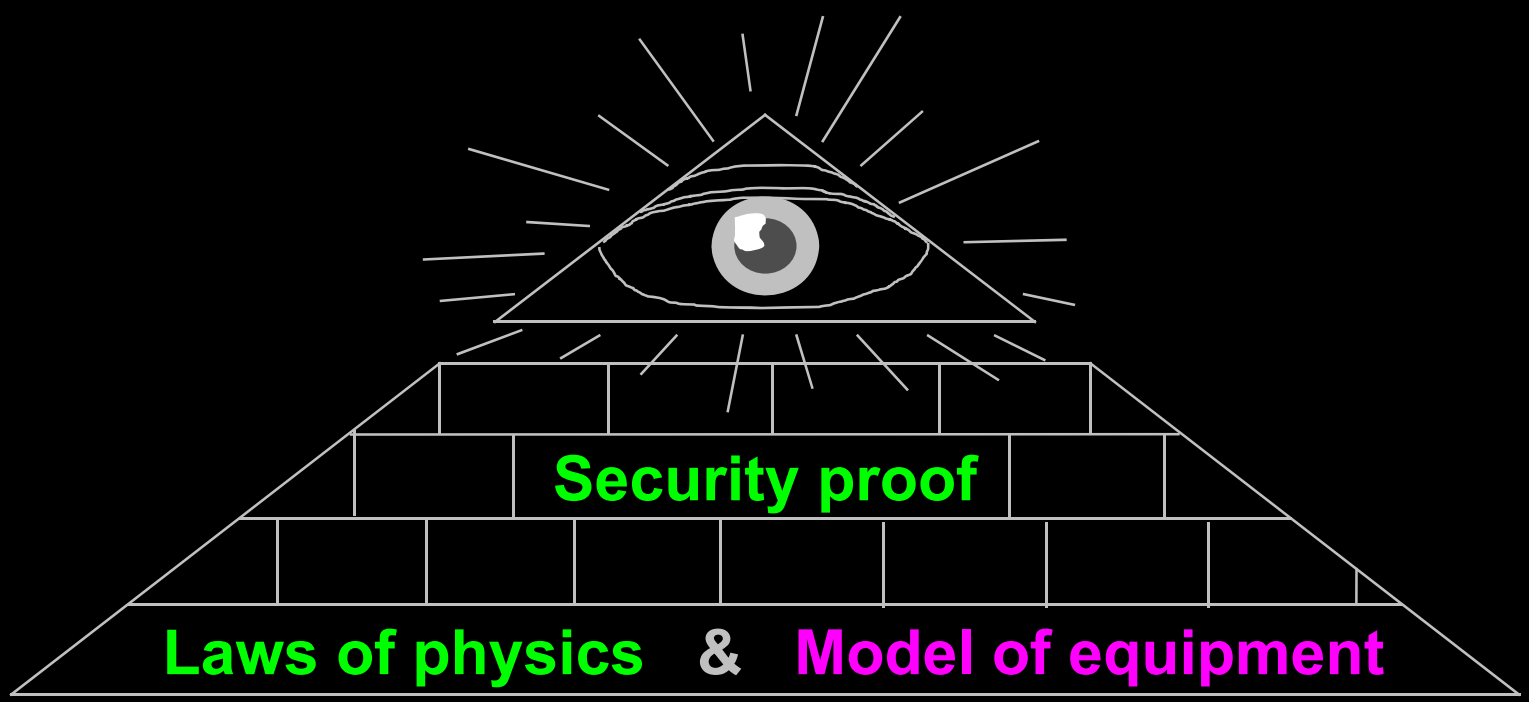
Manufacturer

Sale

Customer


THEORY
EXPERIMENT
M STEVENS

# Implementation security of quantum communications

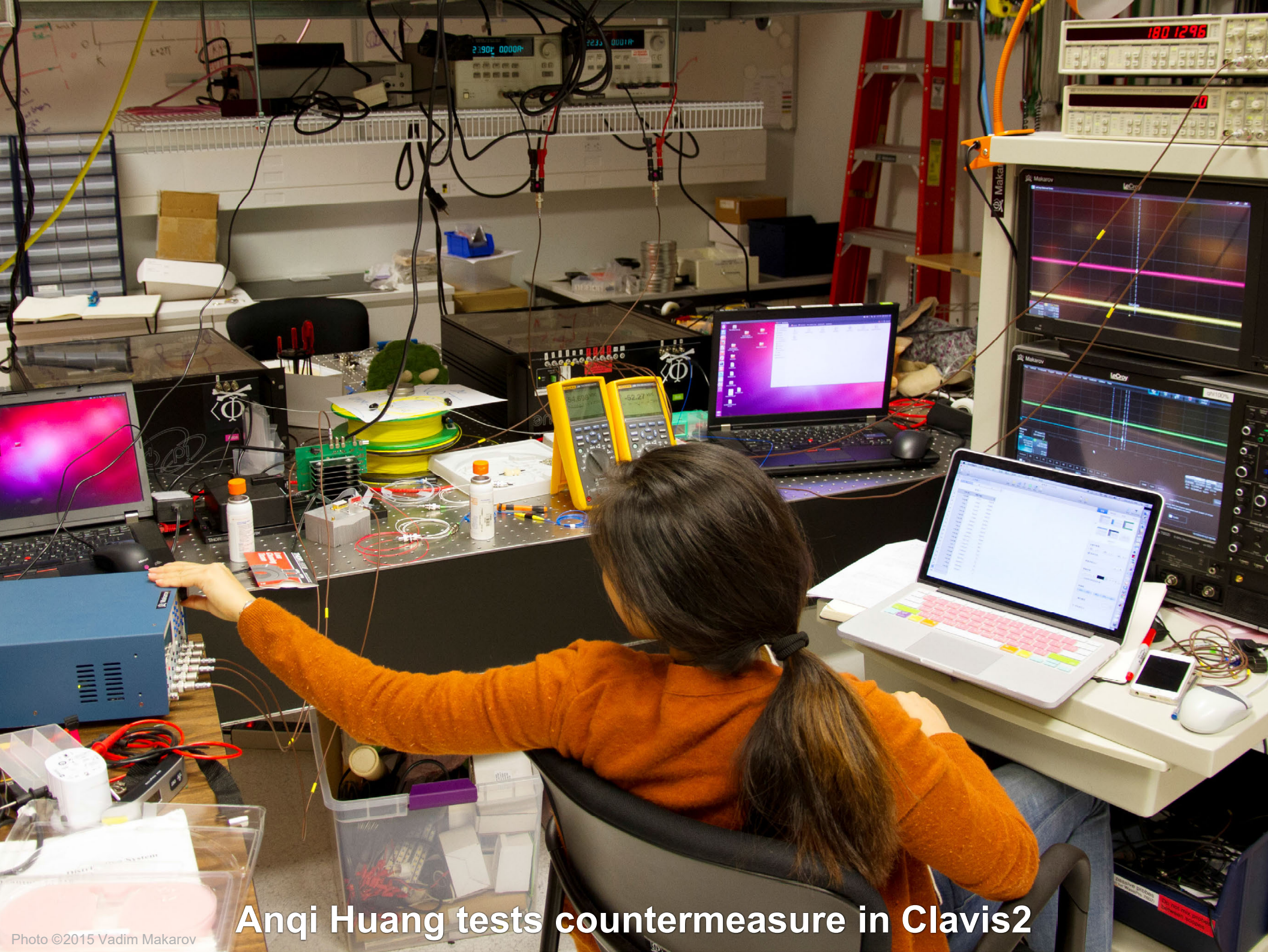



Hack

Integrate imperfection into security model

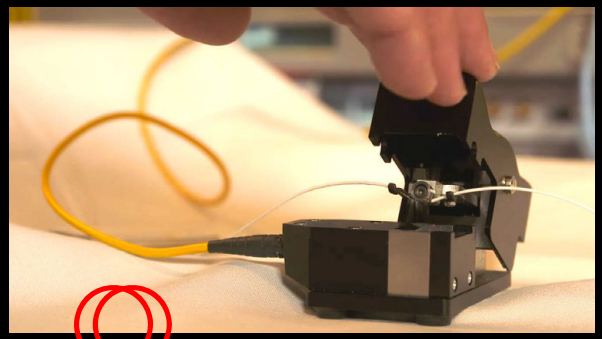
**Formal certification: we need standards and labs ecosystem**

| Attack | Target component | Tested system |
|---|---|---|
| **Distinguishability of decoy states**<br>A. Huang *et al.,* Phys. Rev. A **98**, 012330 (2018) | laser in Alice | 3 research systems |
| **Intersymbol interference**<br>K. Yoshino *et al.,* poster at QCrypt (2016) | intensity modulator in Alice | research system |
| **Laser damage**<br>V. Makarov *et al.,* Phys. Rev. A **94**, 030302 (2016); A. Huang *et al.,* poster at QCrypt (2018) | any | 5 commercial &<br>1 research systems |
| **Spatial efficiency mismatch**<br>M. Rau *et al.,* IEEE J. Sel. Top. Quantum Electron. **21**, 6600905 (2015); S. Sajeed *et al.,* Phys. Rev. A **91**, 062301 (2015) | receiver optics | 2 research systems |
| **Pulse energy calibration**<br>S. Sajeed *et al.,* Phys. Rev. A **91**, 032326 (2015) | classical watchdog detector | ID Quantique |
| **Trojan-horse**<br>I. Khan *et al.,* presentation at QCrypt (2014) | phase modulator in Alice | SeQureNet |
| **Trojan-horse**<br>N. Jain *et al.,* New J. Phys. **16**, 123030 (2014); S. Sajeed *et al.,* Sci. Rep. **7**, 8403 (2017) | phase modulator in Bob | ID Quantique |
| **Detector saturation**<br>H. Qin, R. Kumar, R. Alleaume, Proc. SPIE 88990N (2013) | homodyne detector | SeQureNet |
| **Shot-noise calibration**<br>P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A **87**, 062313 (2013) | classical sync detector | SeQureNet |
| **Wavelength-selected PNS**<br>M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A **86**, 032310 (2012) | intensity modulator | (theory) |
| **Multi-wavelength**<br>H.-W. Li *et al.,* Phys. Rev. A **84**, 062308 (2011) | beamsplitter | research system |
| **Deadtime**<br>H. Weier *et al.,* New J. Phys. **13**, 073024 (2011) | single-photon detector | research system |
| **Channel calibration**<br>N. Jain *et al.,* Phys. Rev. Lett. **107**, 110501 (2011) | single-photon detector | ID Quantique |
| **Faraday-mirror**<br>S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011) | Faraday mirror | (theory) |
| **Detector control**<br>I. Gerhardt *et al.,* Nat. Commun. **2**, 349 (2011); L. Lydersen *et al.,* Nat. Photonics **4**, 686 (2010) | single-photon detector | ID Quantique, MagiQ,<br>research systems |

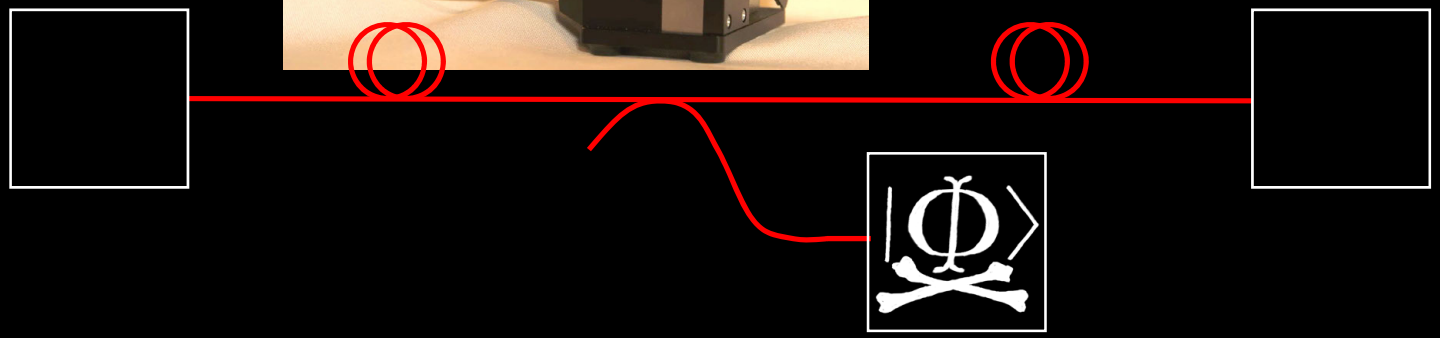


Anqi Huang tests countermeasure in Clavis2

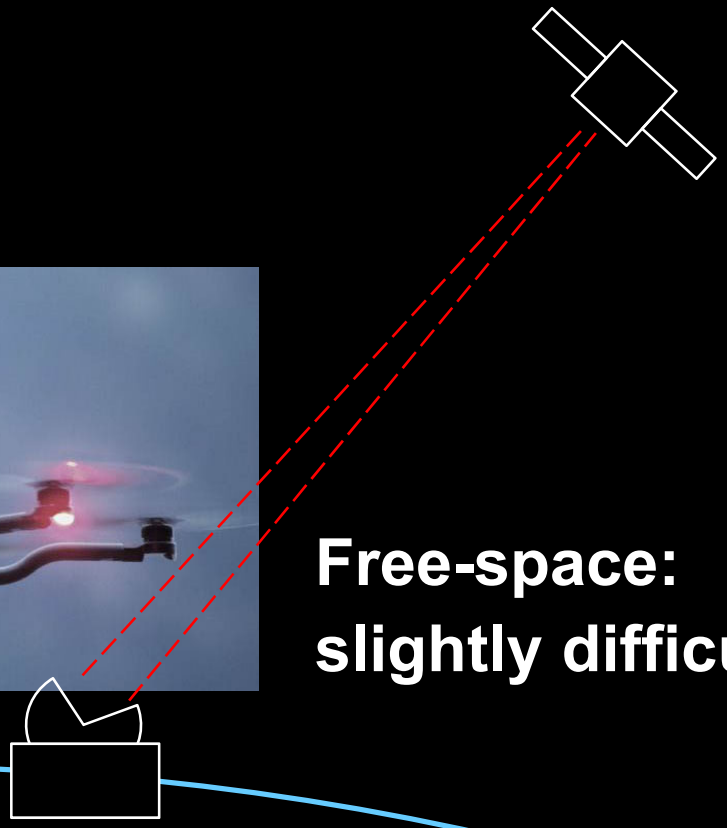
# Attacks require realtime physical access to channel



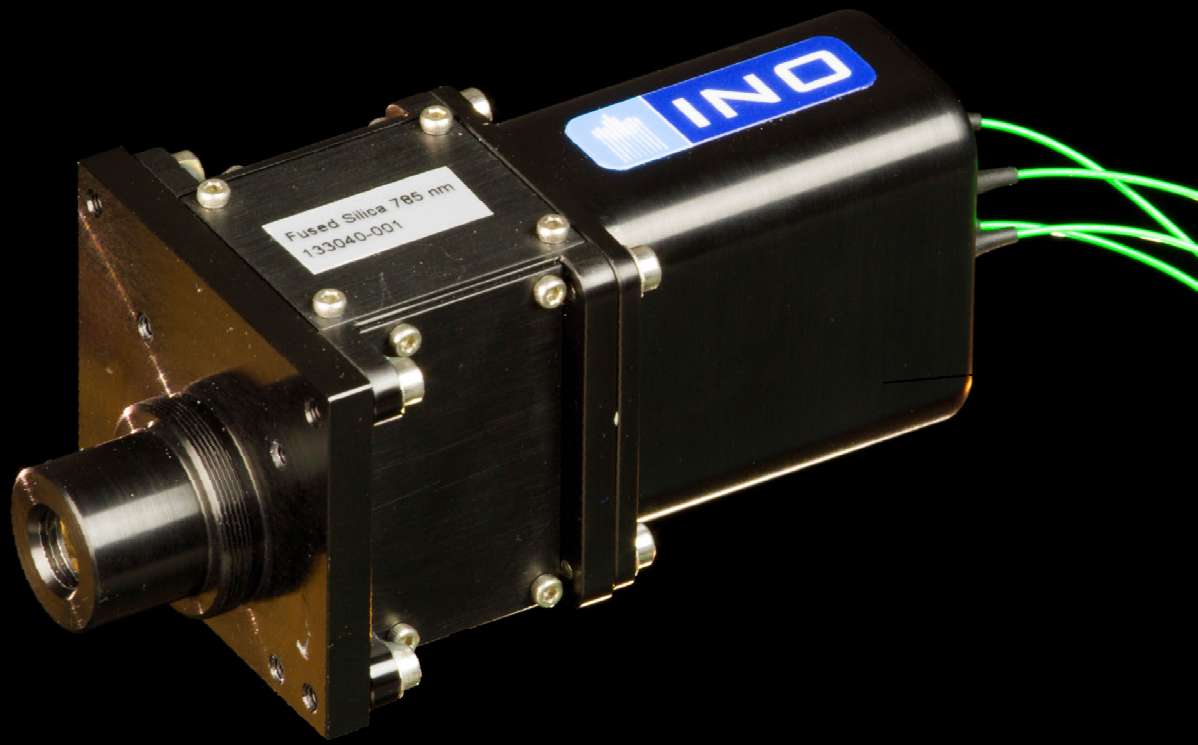
Fiber: easy



Free-space:
slightly difficult

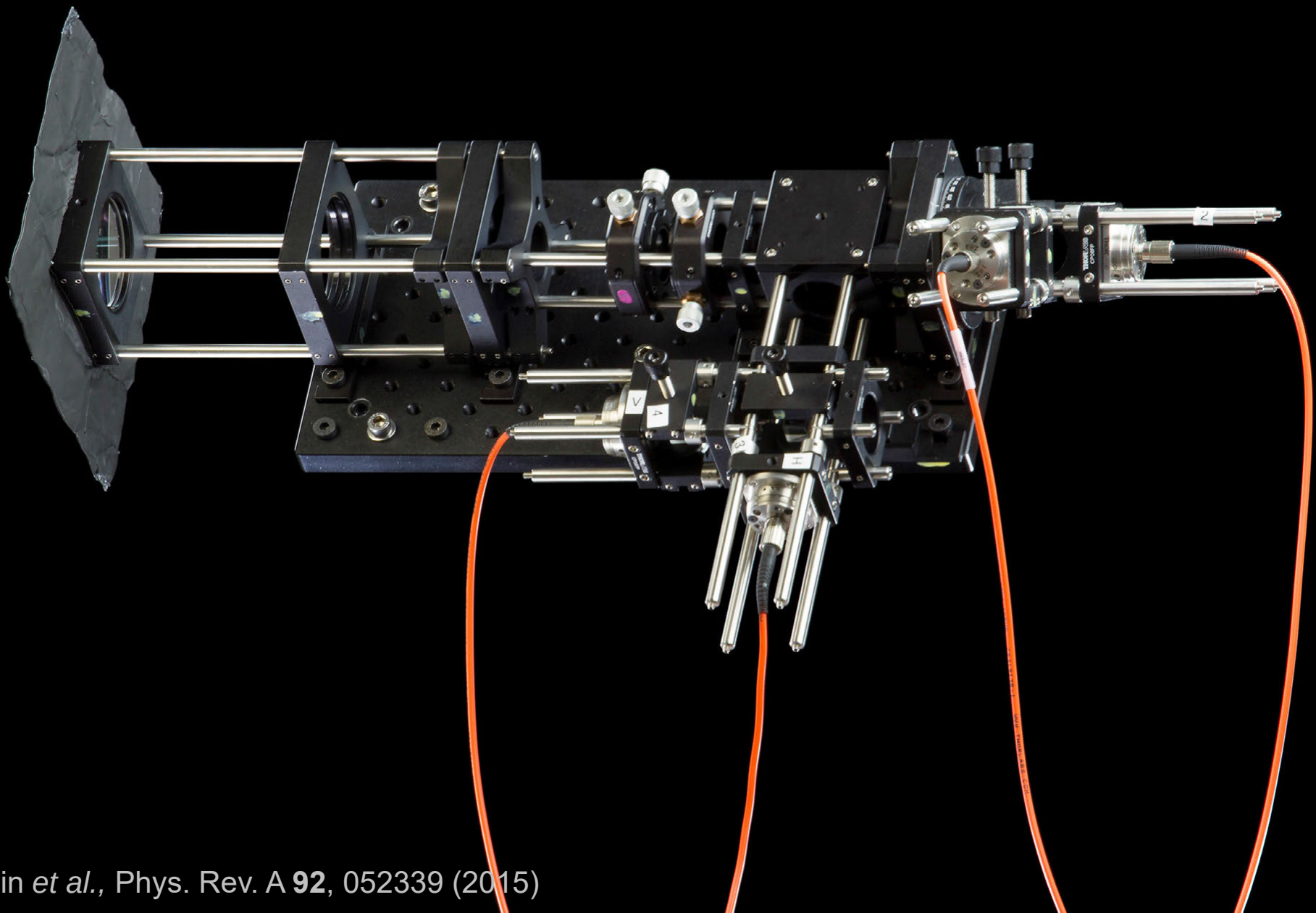


# Polarization receiver for satellite



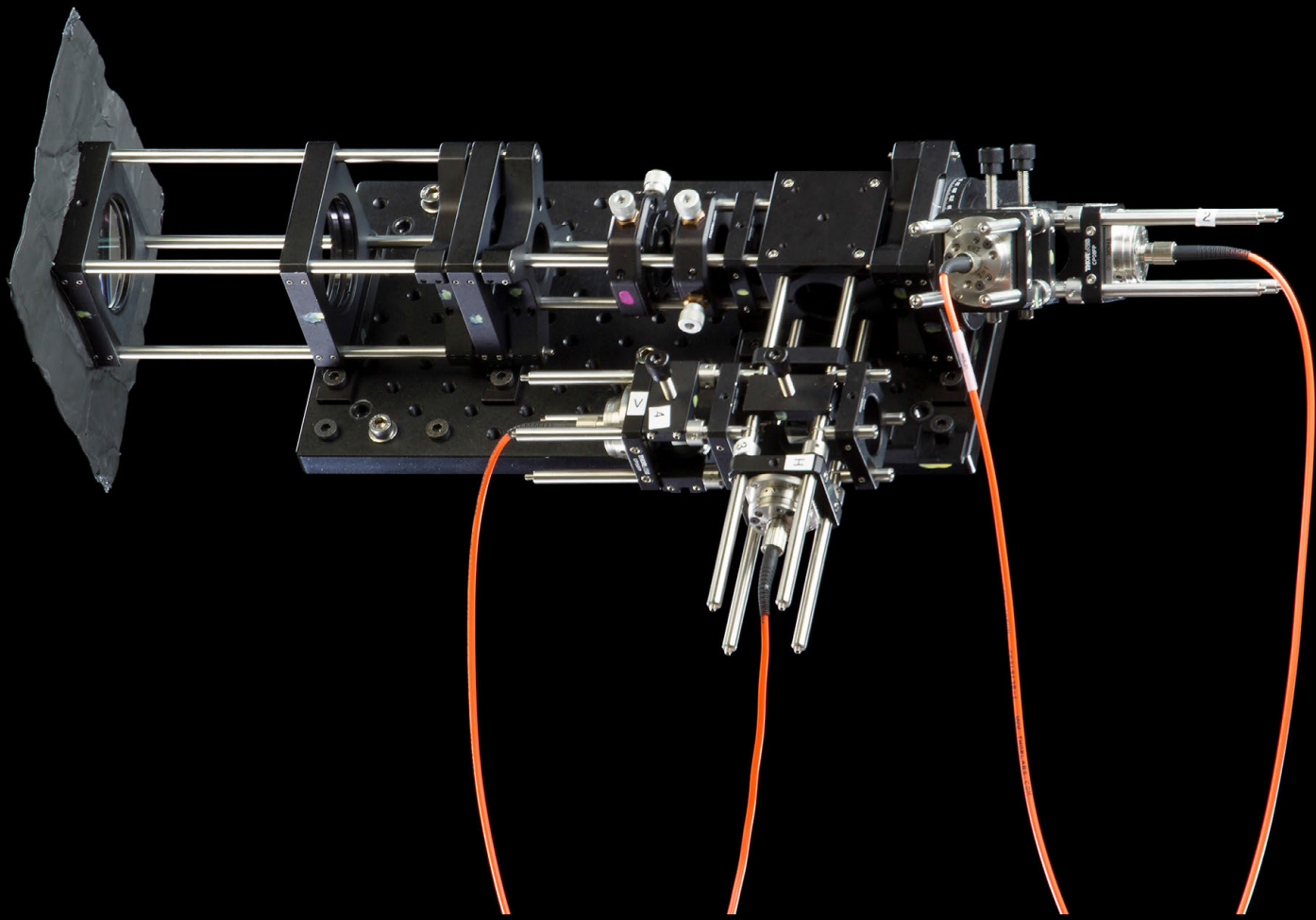

C. J. Pugh *et al.*, Quantum Sci. Technol. **2**, 024009 (2017)

# Polarization analyzer



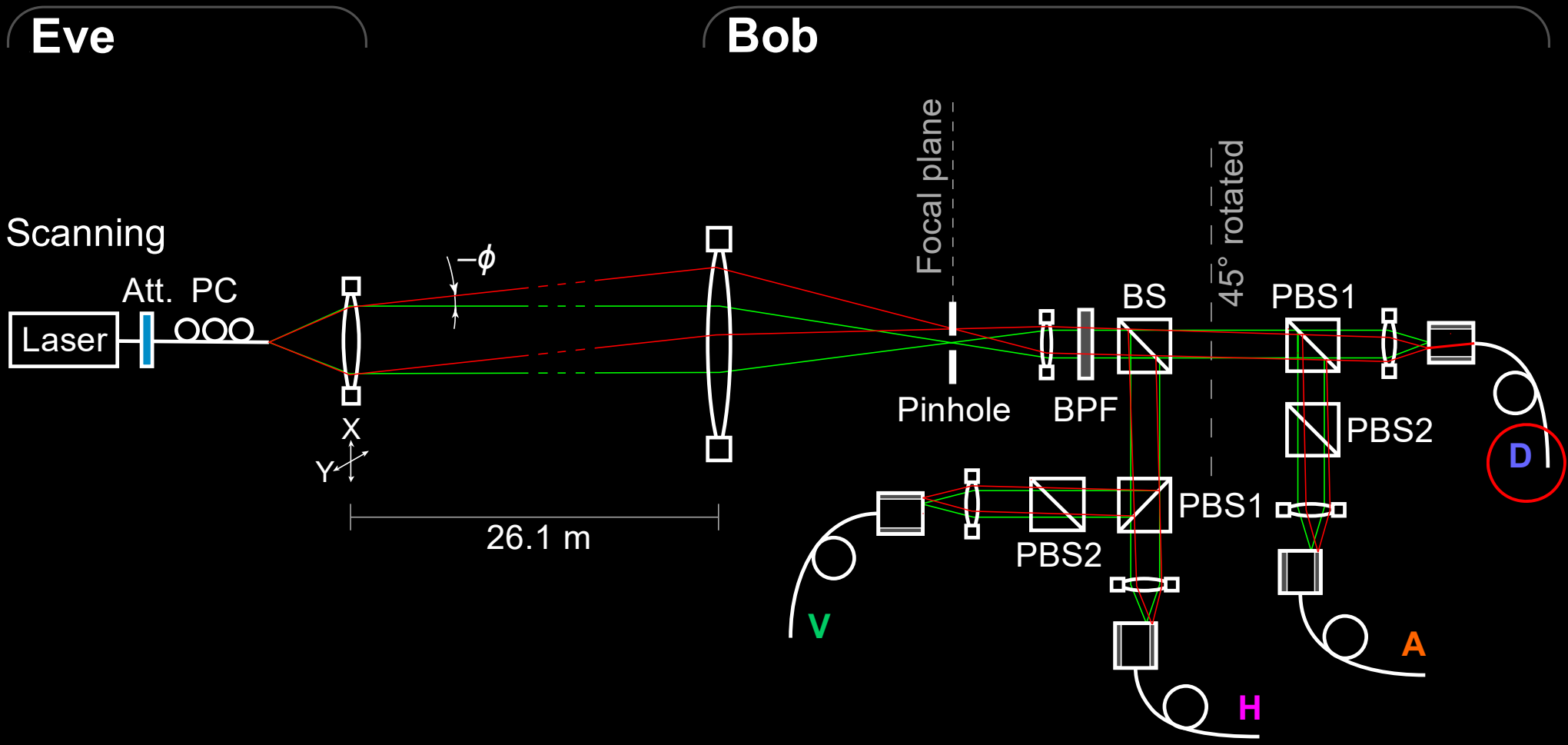
J.-P. Bourgoin *et al.*, Phys. Rev. A **92**, 052339 (2015)

# Polarization analyzer



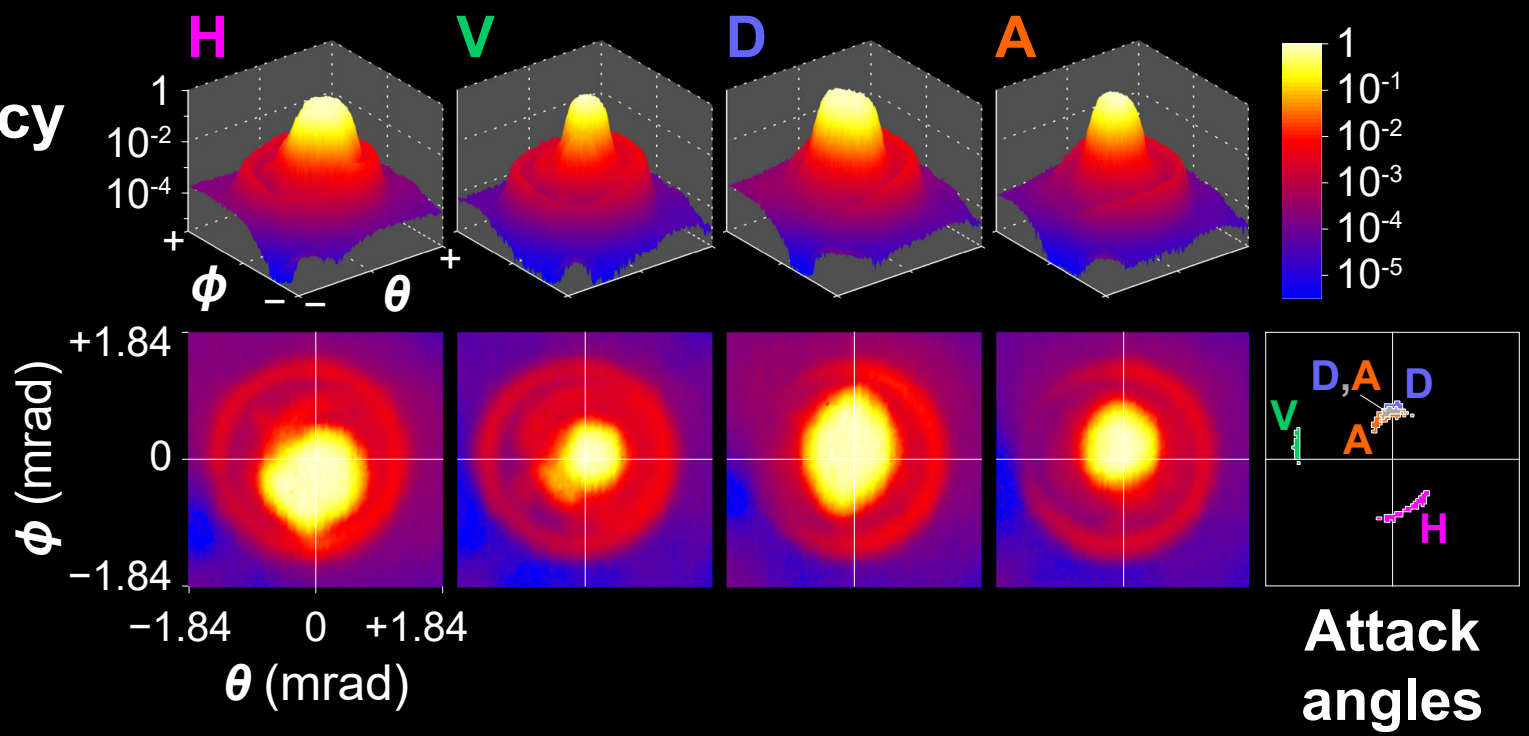
J.-P. Bourgoin *et al.*, Phys. Rev. A **92**, 052339 (2015)

# Efficiency mismatch in polarization analyzer



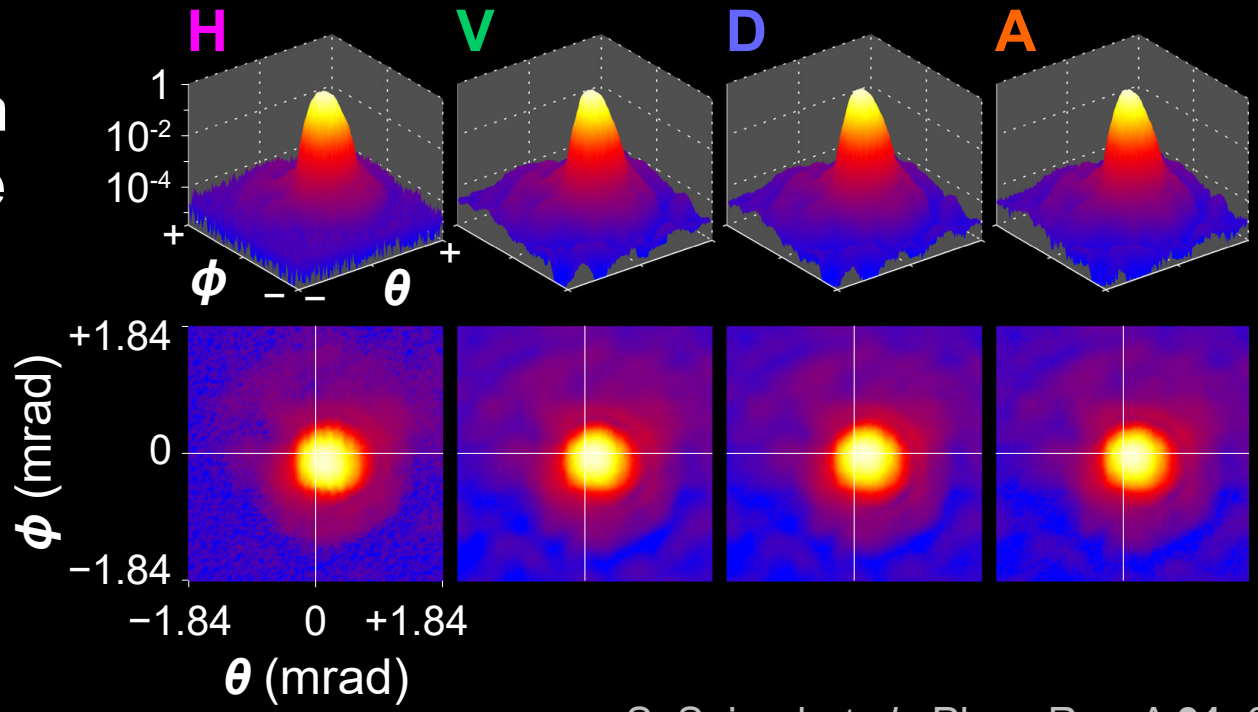

S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015)

**Detector efficiency without pinhole**




**Attack angles**

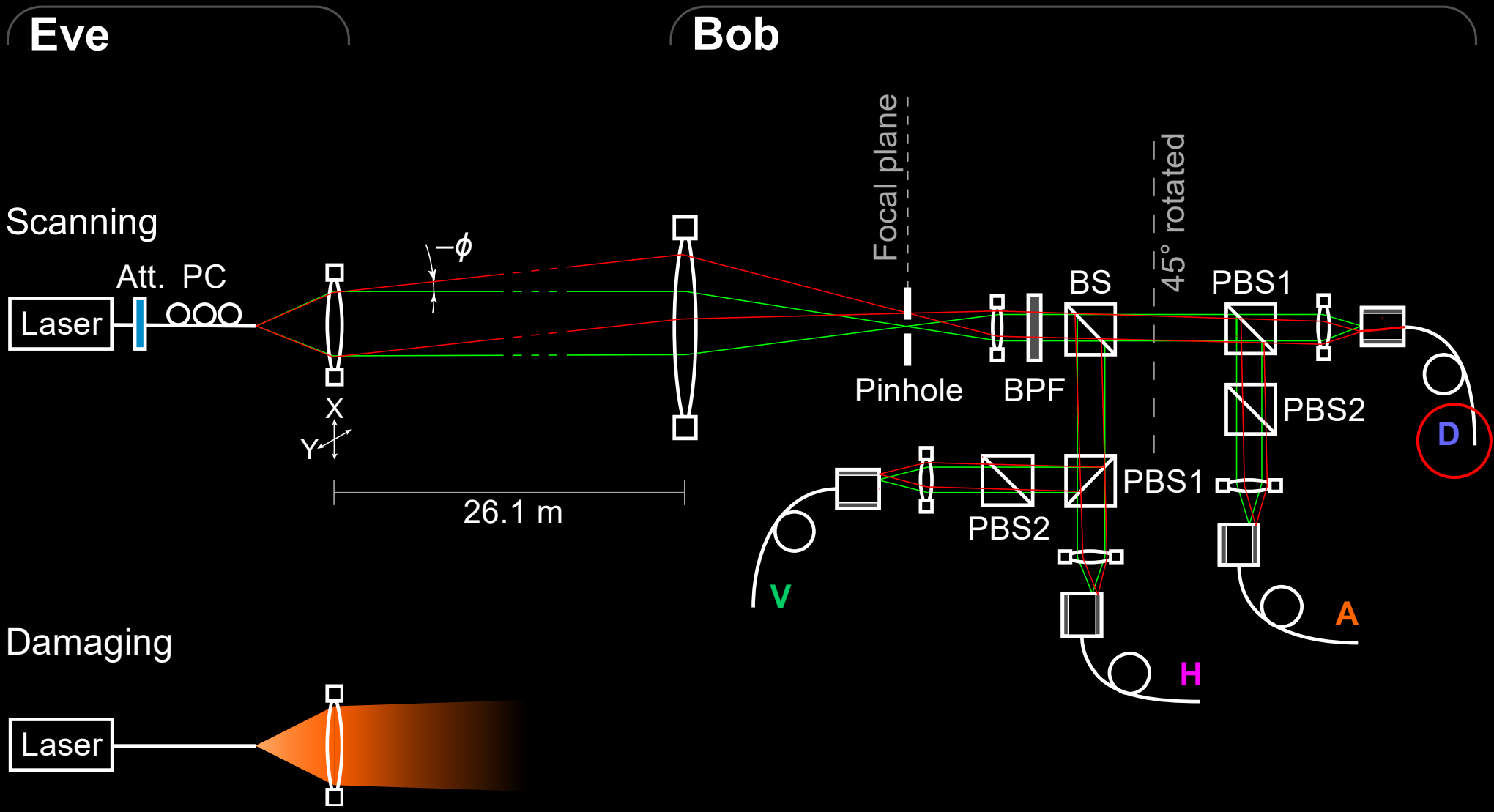
**...and with 25 μm diameter pinhole**



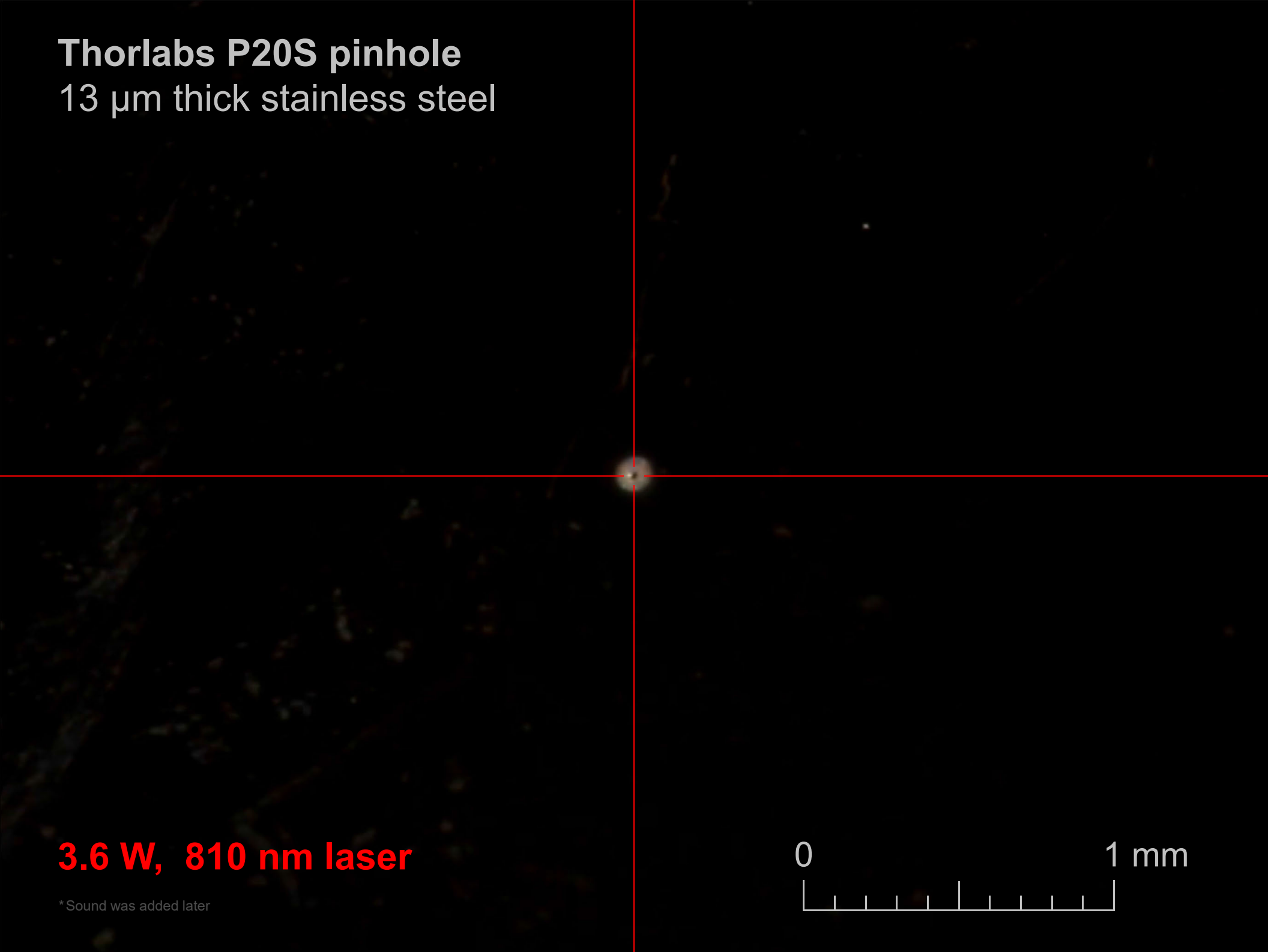

**No attack found**

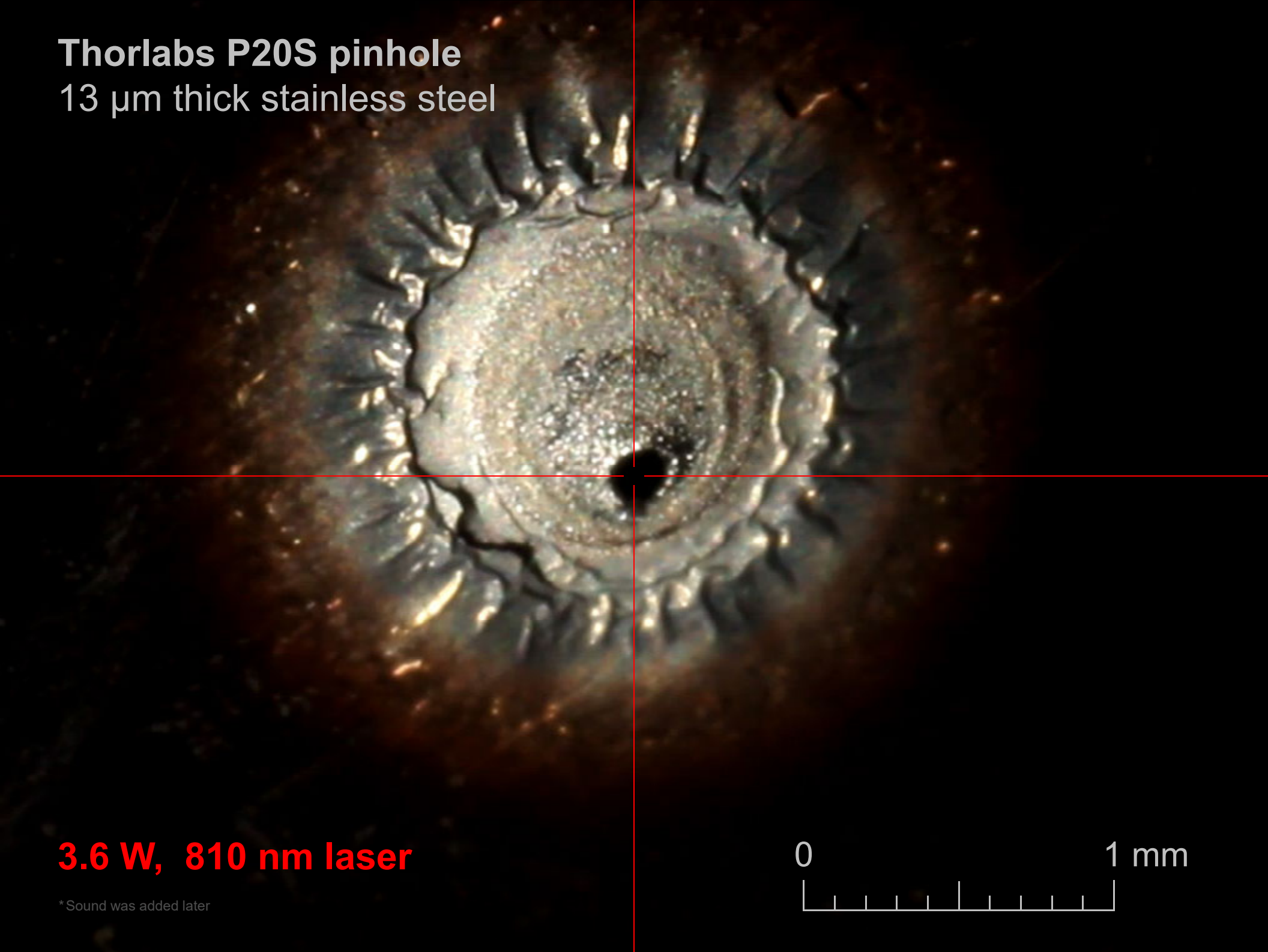
S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015)

# Counter-attack




V. Makarov *et al.*, Phys. Rev. A **94**, 030302 (2016)


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

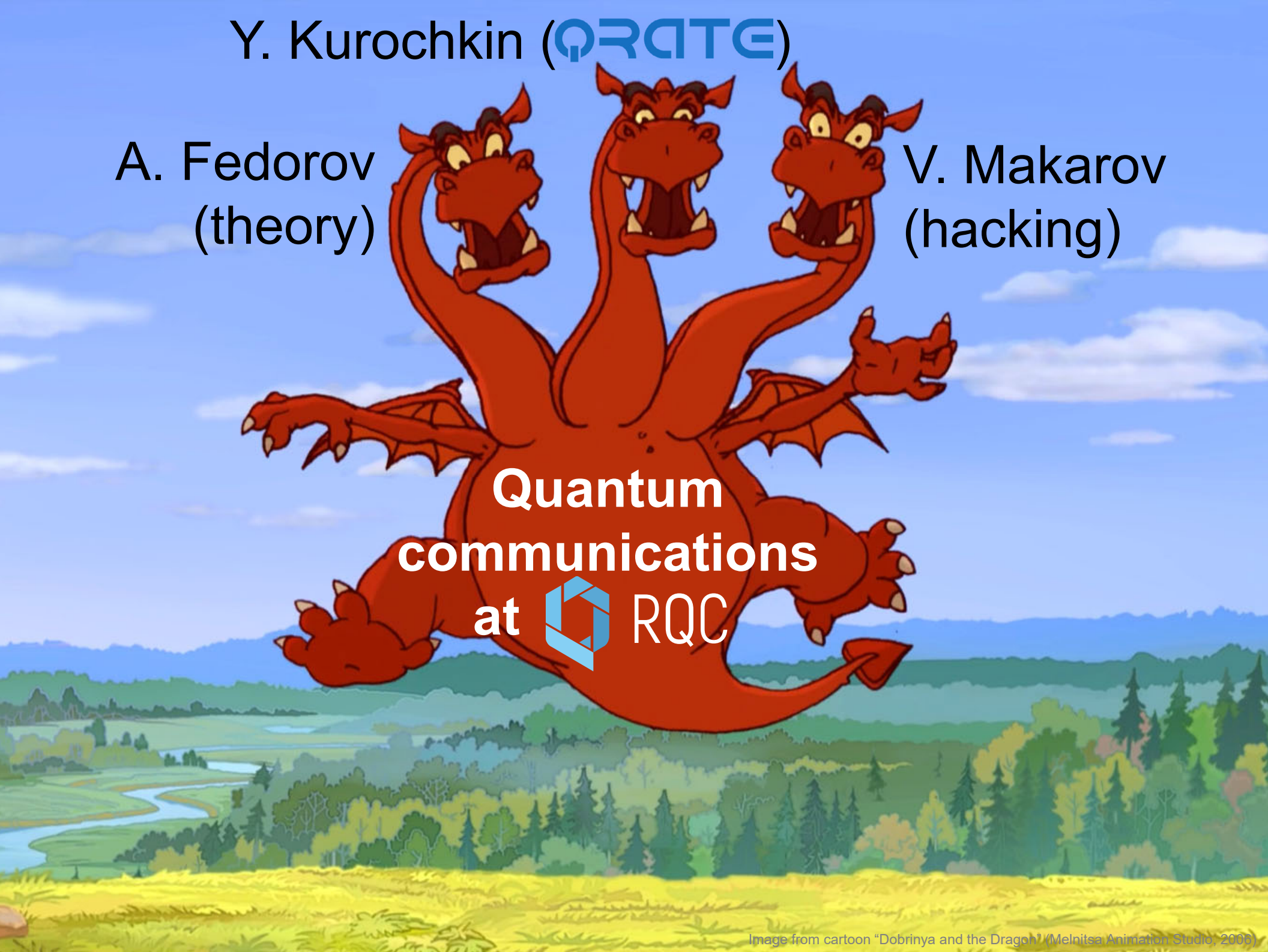
| Security audit | System | Report | Tests |
|---|---|---|---|
| IDQ |  Clavis3 | 2016 | –2018 incomplete |
| 国盾量子 QuantumCTek | 40 MHz system | 2016, 2018–19 | ongoing |
| ITMO UNIVERSITY (ООО Квантовые коммуникации) | Subcarrier scheme (A. Gleim) | 2018 | ongoing |
| QRATE | New 1 GHz system | (2019) | to do |

S. Sajeed *et al.*, unpublished

**International certification standards are being developed**

ETSI Industry standards group in QKD

ISO


Y. Kurochkin (QRATE)
A. Fedorov (theory)
V. Makarov (hacking)
Quantum communications at RQC
Image from cartoon “Dobrinya and the Dragon” (Melnitsa Animation Studio, 2006)

# Winter school on quantum cybersecurity

**Annual. Next: 25–31 January 2020**
**Les Diablerets, Switzerland**

**2 days (executive track) +**
**4 days (technical track, with 4 labs)**

**Overview talks + quantum technologies, including QKD**

Lecturers in 2019: J. Baloo, C. Bennett, G. Brassard, E. Diamanti, R. Floeter, N. Gisin, J. Hart, B. Huttner, E. Hodges, V. Makarov, M. Mosca, S. Popescu, R. Renner, F. Ruess, G. Ribordy, V. Scarani, D. Stucki, C. Williams

**30 students,** first-come, sells out

**€3200** / €1600 executive track only

**Winter sports in breaks**

**Organised by** IDQ

**www.idquantique.com/winter-school-2018**

2016

2018

# International school on quantum technology

**Annual. Next: early March 2020**
**Roza Khutor, Russia**

**4 days of lectures and skiing, poster session**

**Tutorials on quantum sensing, computing, metrology, QKD**

Lecturers in 2019: A. Akimov, V. Balykin, M. Chekhova, V. Eliseev, A. Fedyanin, A. Korolkov, L. Krivitsky, V. Makarov, A. Odinokov, O. Snigirev, S. Straupe, A. Urivsky, S. Vyatchanin, F. Zhelezko

**100 students,** competitive admission

**€80 academic / €300 other (TBC)**

**4 h of pro skiing instruction**

**Organised by** Центр Квантовых Технологий

**qutes.org**

2019