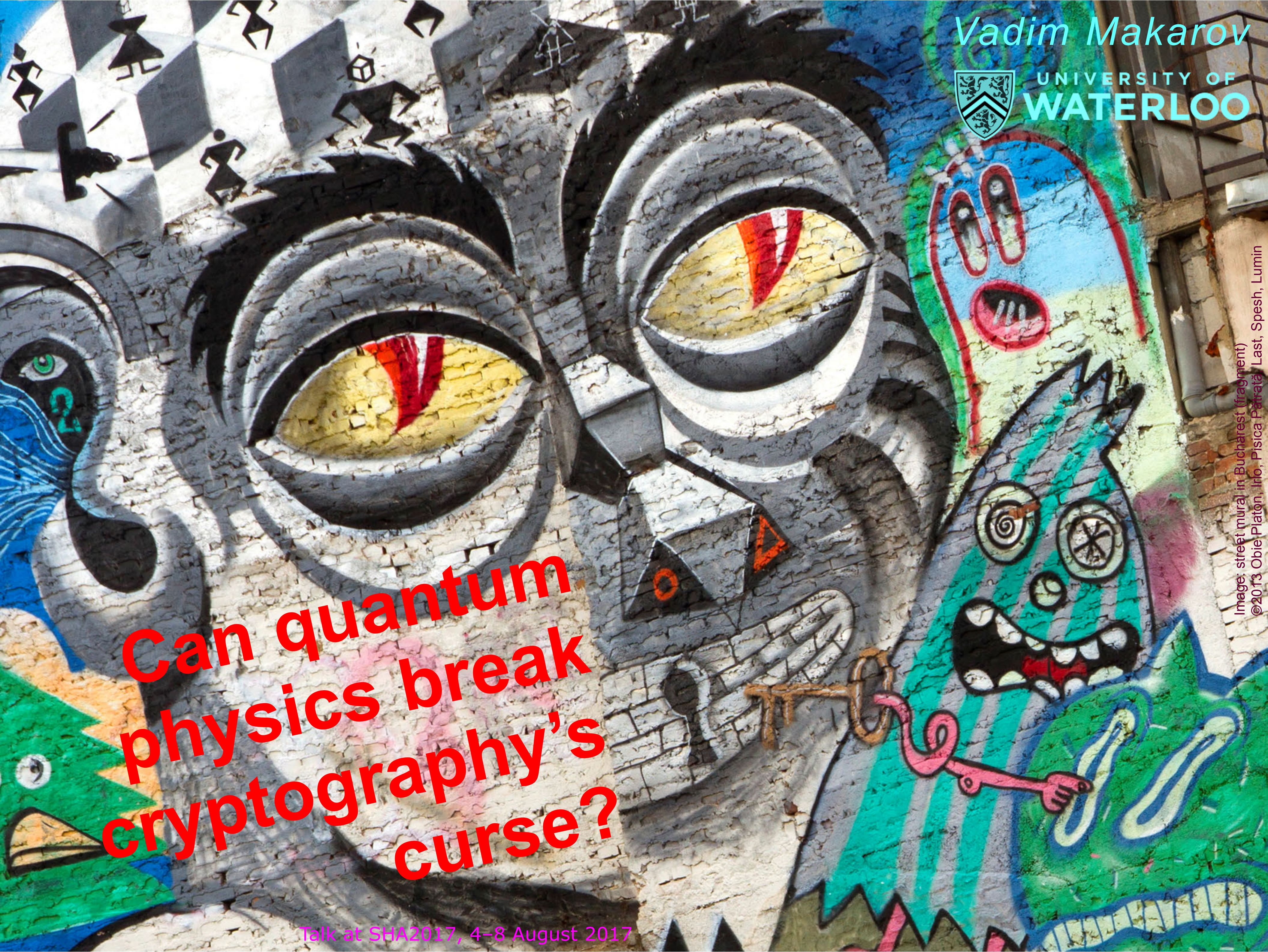
Vadim Makarov
UNIVERSITY OF WATERLOO



Can quantum physics break cryptography's curse?

Image: street mural in Bucharest (fragment)

Talk at SHA2017, 4–8 August 2017

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

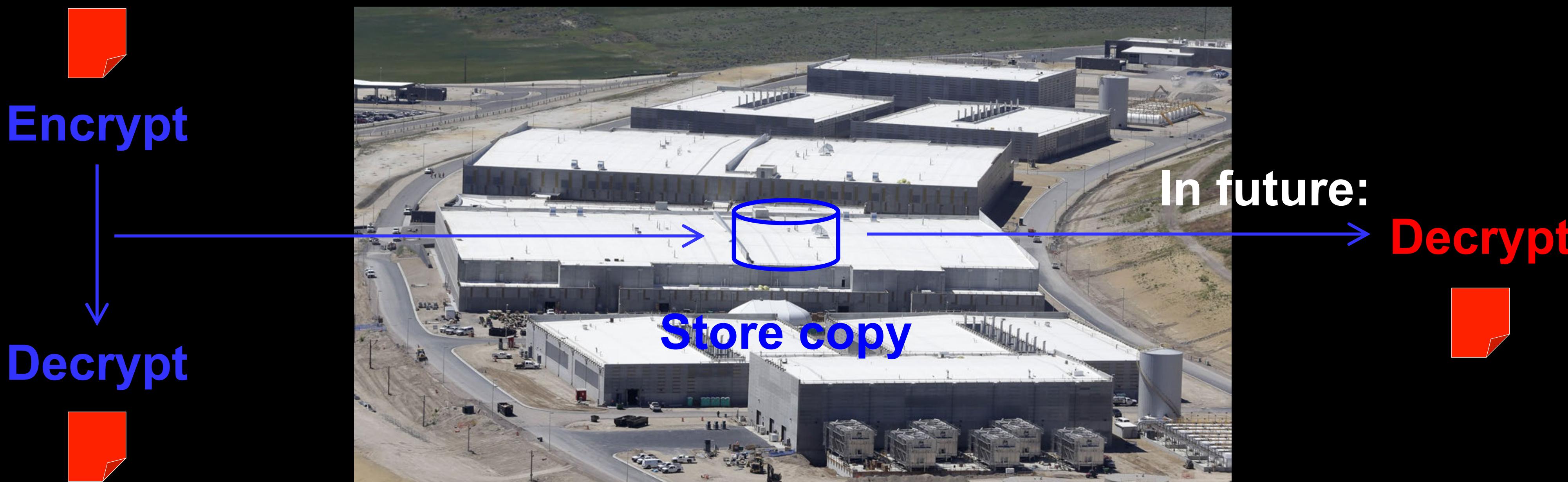
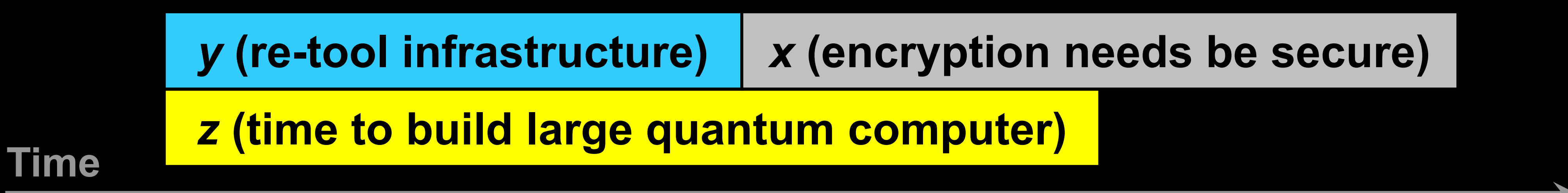


Photo ©2013 AP / Rick Bowmer

Mosca theorem



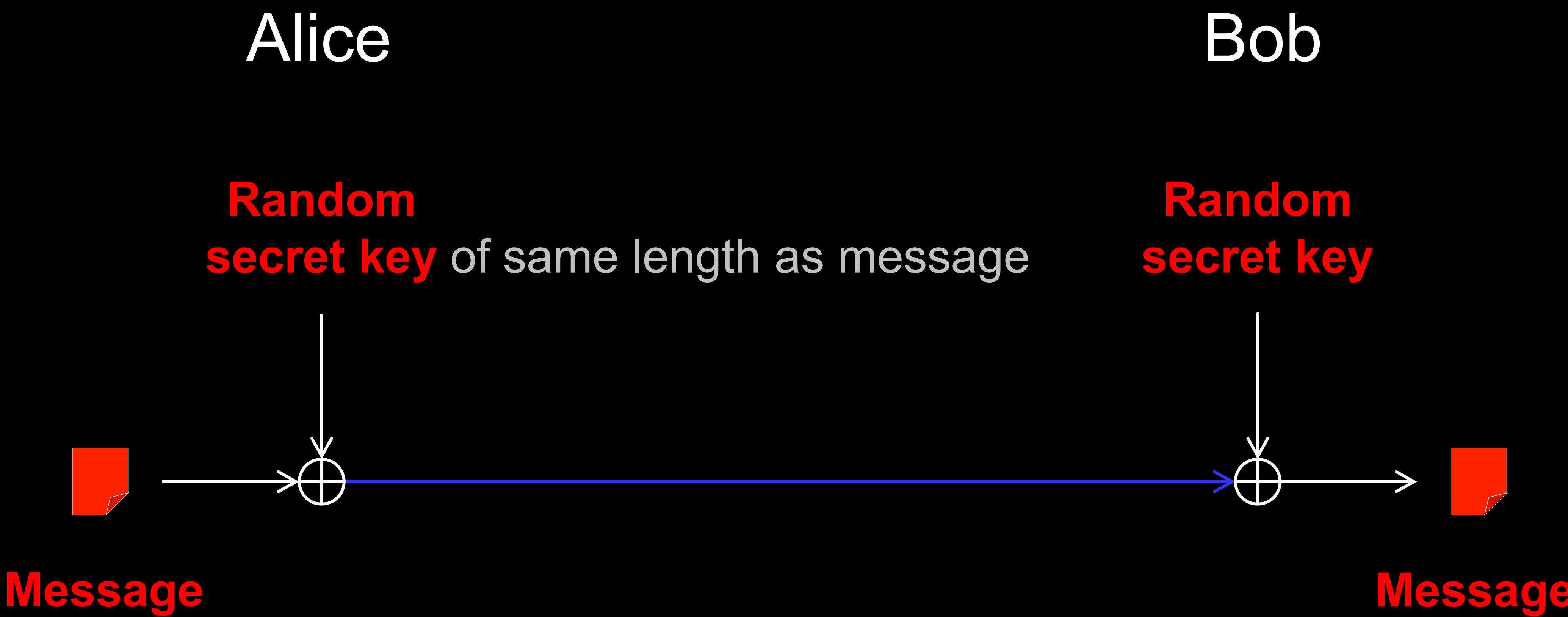
If $x + y > z$, then worry.

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



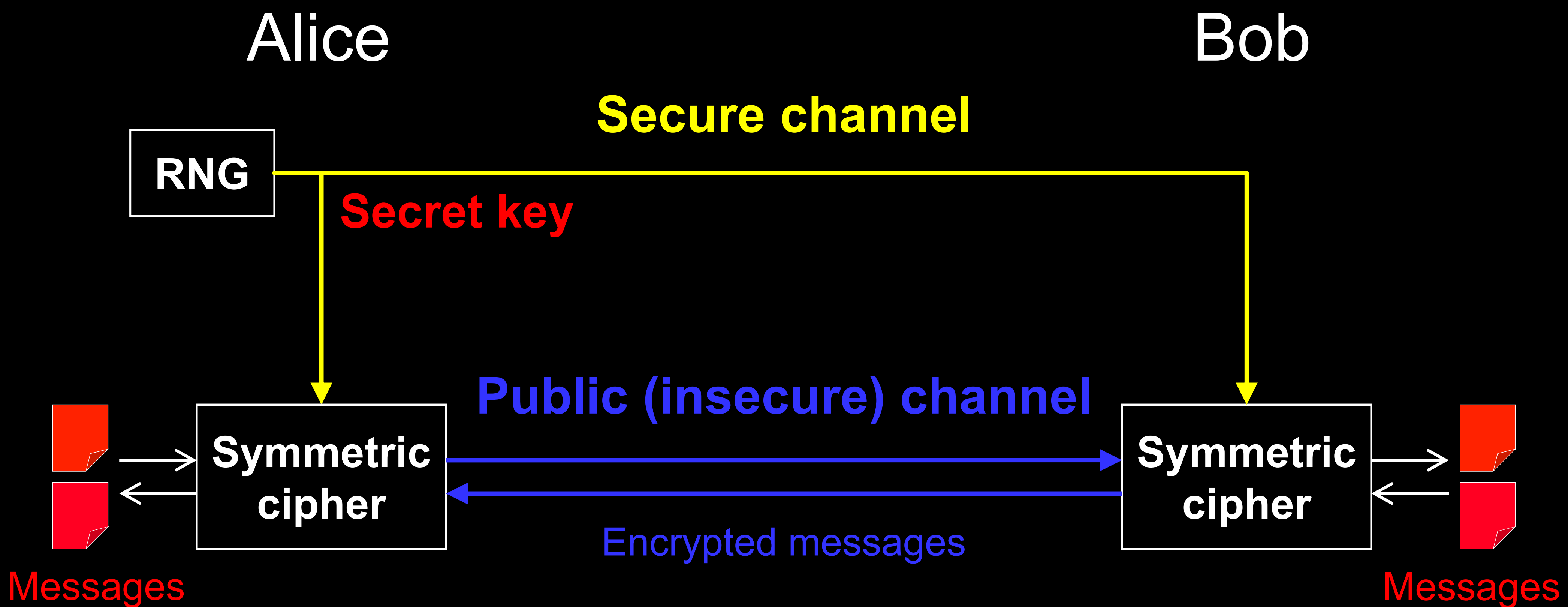
α	β	α⊕β
0	0	0
0	1	1
1	0	1
1	1	0

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	?

Encryption and key distribution

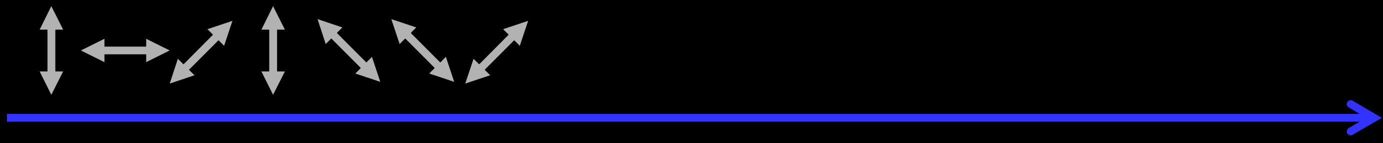


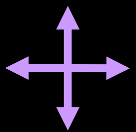
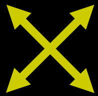
Quantum key distribution transmits secret key by sending quantum states over *open channel.*

Quantum key distribution (QKD)

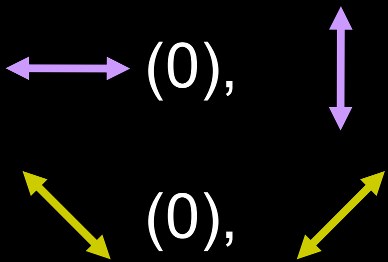
Alice

Bob



 or  ?

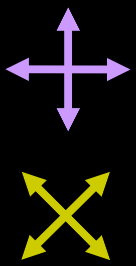
Prepares photons



(0), (1)

(0), (1)

Measures photons



Eavesdropping introduces errors

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

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)

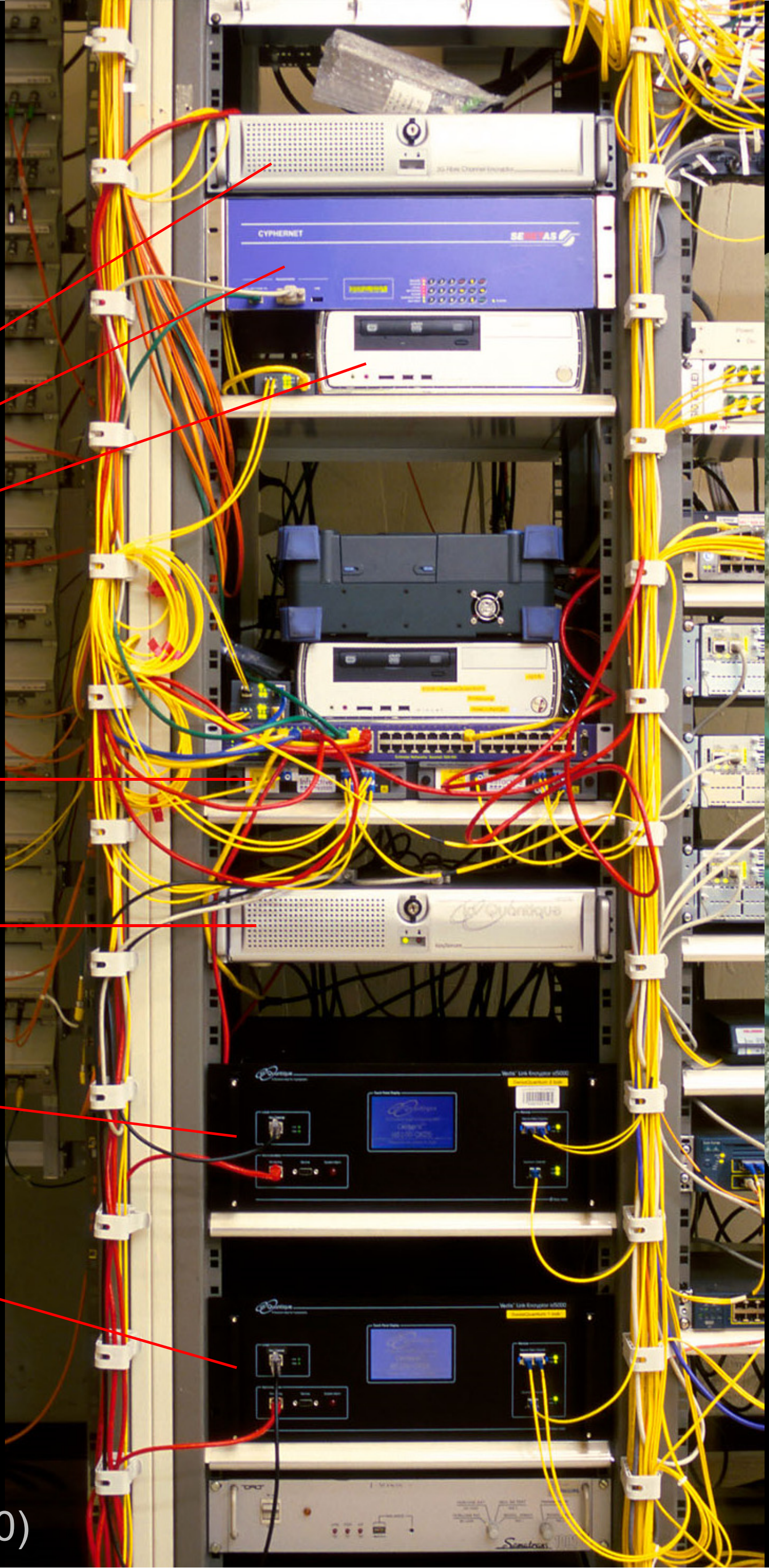
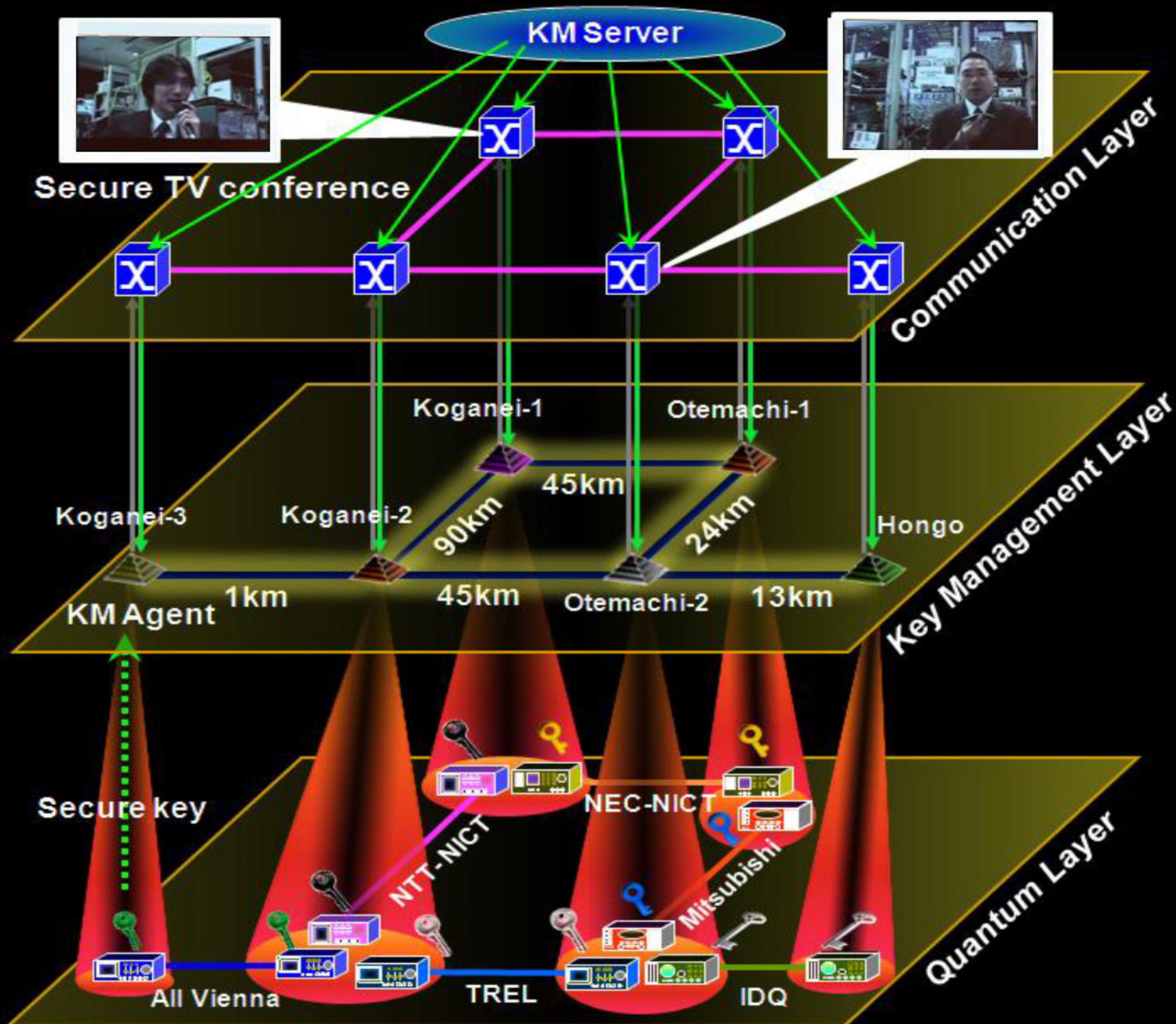


Photo ©2010 Vadim Makarov

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

Trusted-node network



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

Quantum Backbone

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

  31 fiber links
- Metropolitan networks

  Existing: Hefei, Jinan

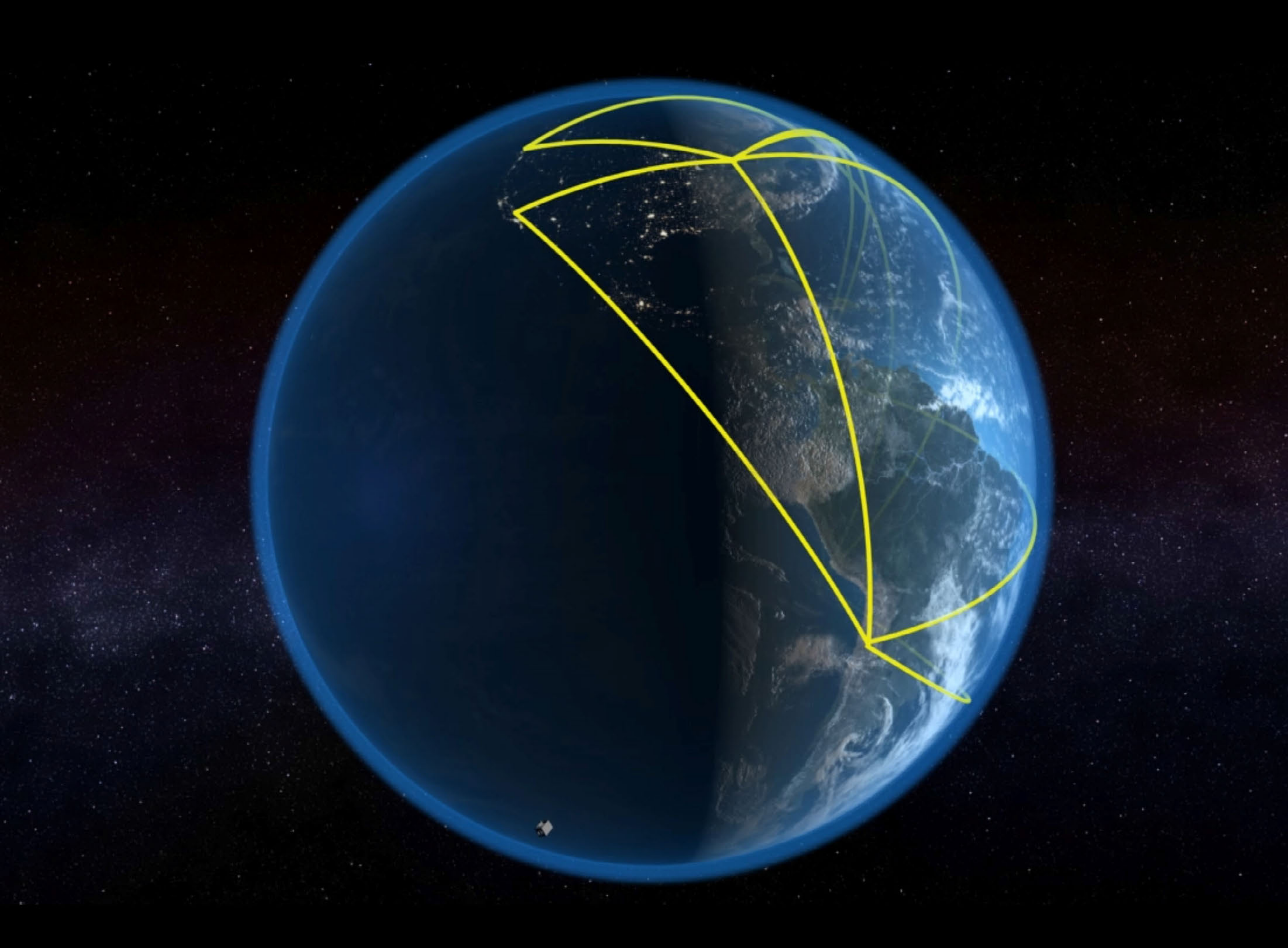
  New: Beijing, Shanghai
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC

Q. Zhang, talk at QCrypt 2014

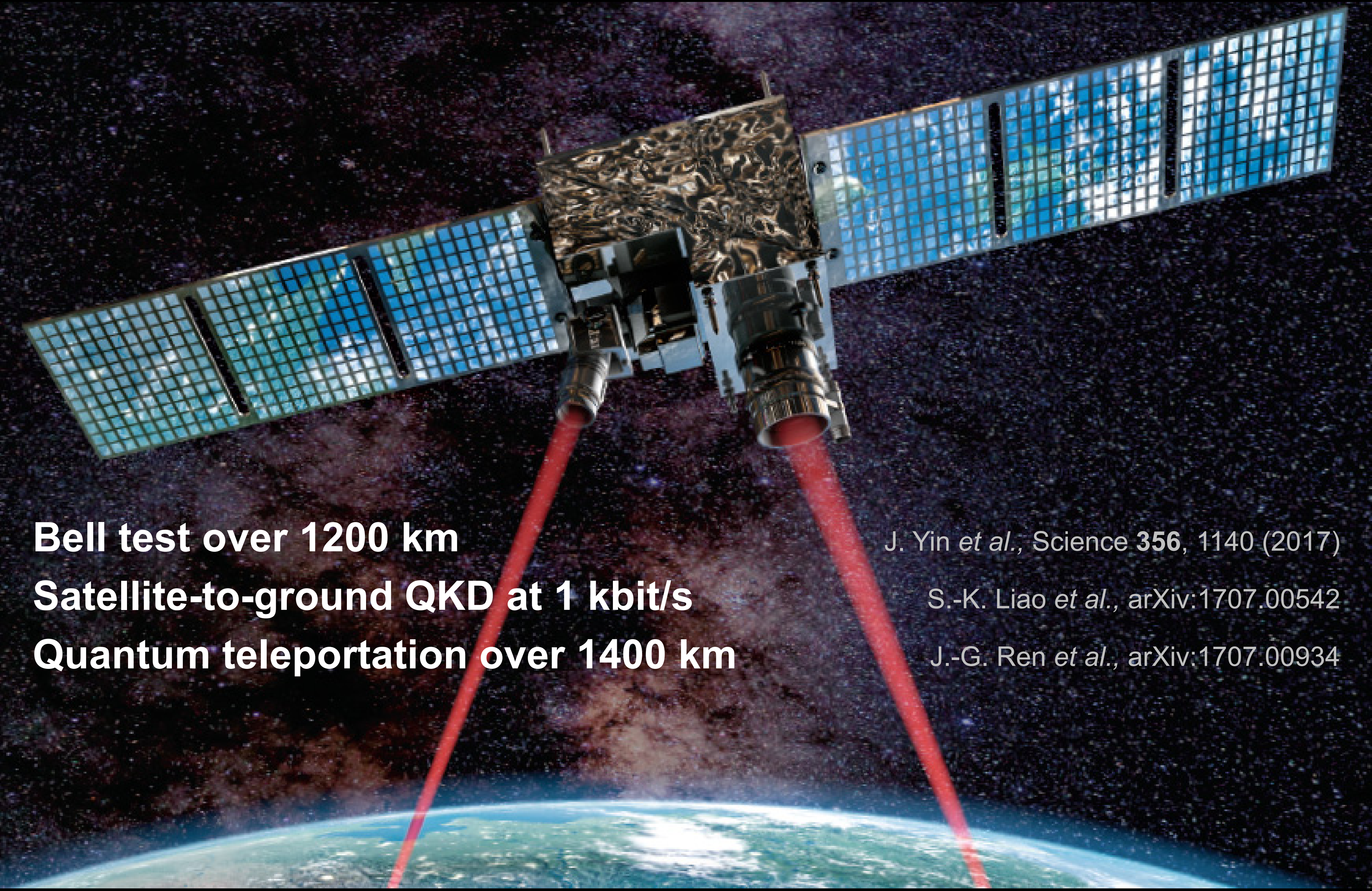
Shanghai control center of the Chinese quantum key distribution network and satellite

Global quantum key distribution

Video ©2012 IQC / group of T. Jennewein



Chinese quantum satellite (launched 2016)

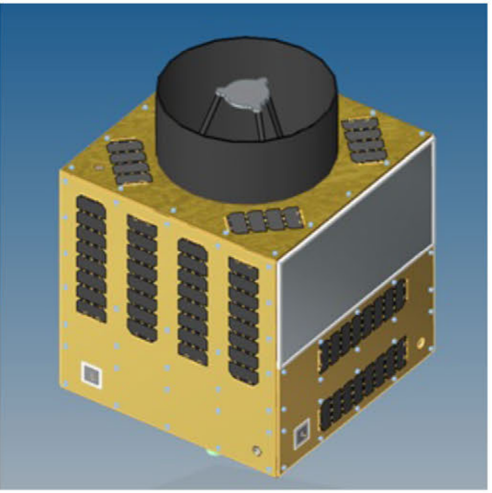


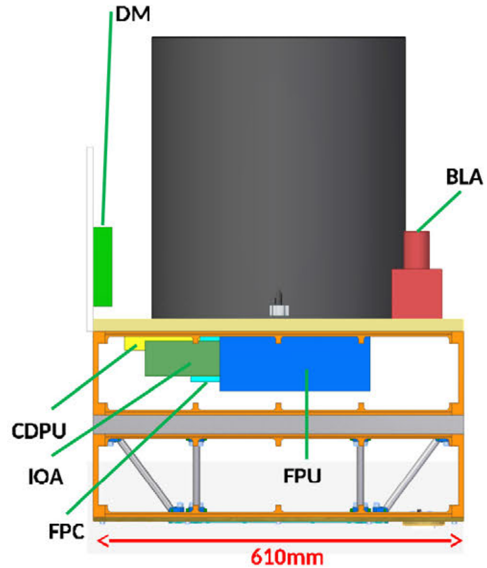
Bell test over 1200 km — J. Yin *et al.*, Science **356**, 1140 (2017)

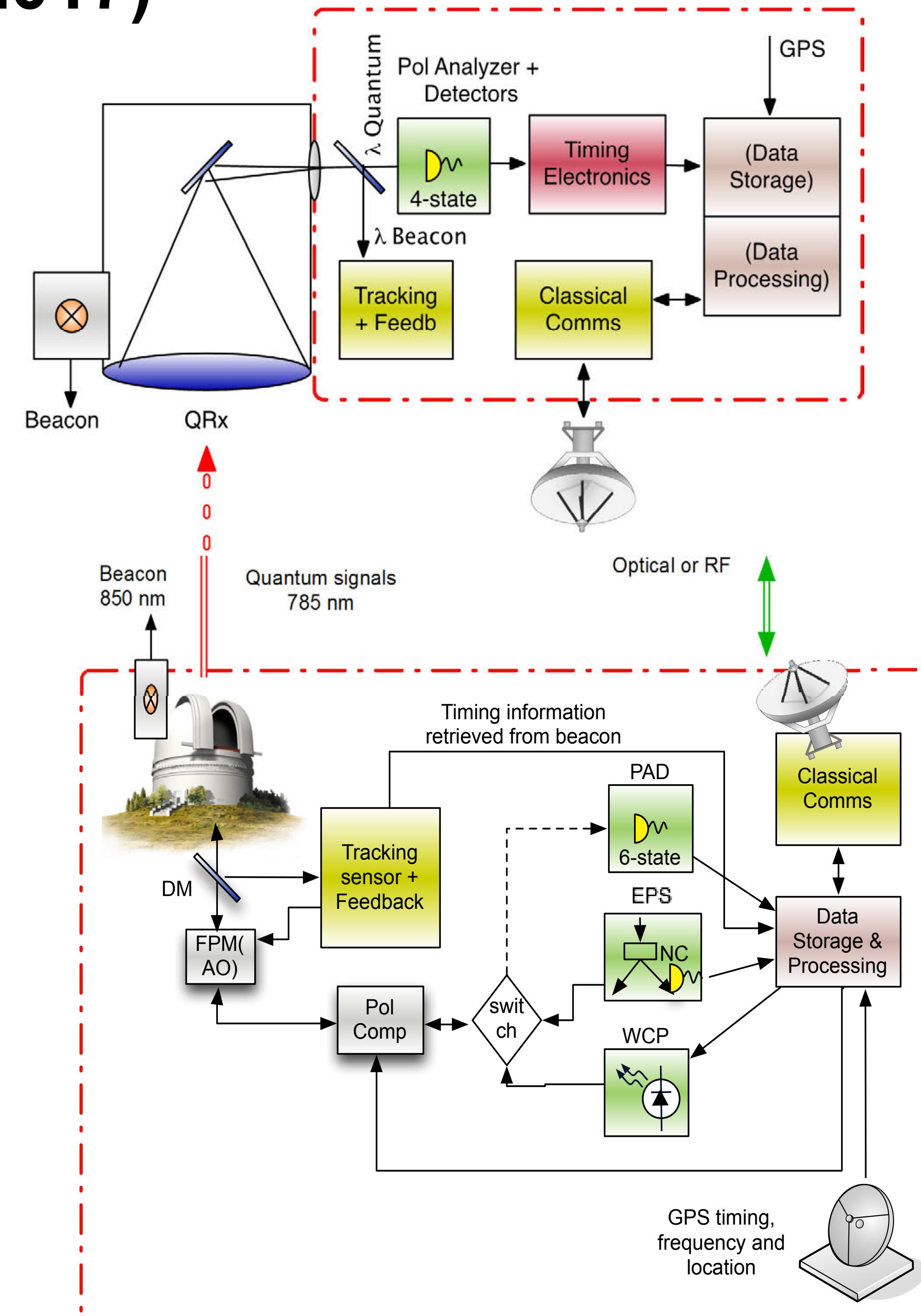
Satellite-to-ground QKD at 1 kbit/s — S.-K. Liao *et al.*, arXiv:1707.00542

Quantum teleportation over 1400 km — J.-G. Ren *et al.*, arXiv:1707.00934

QEYSSat (funded in April 2017)







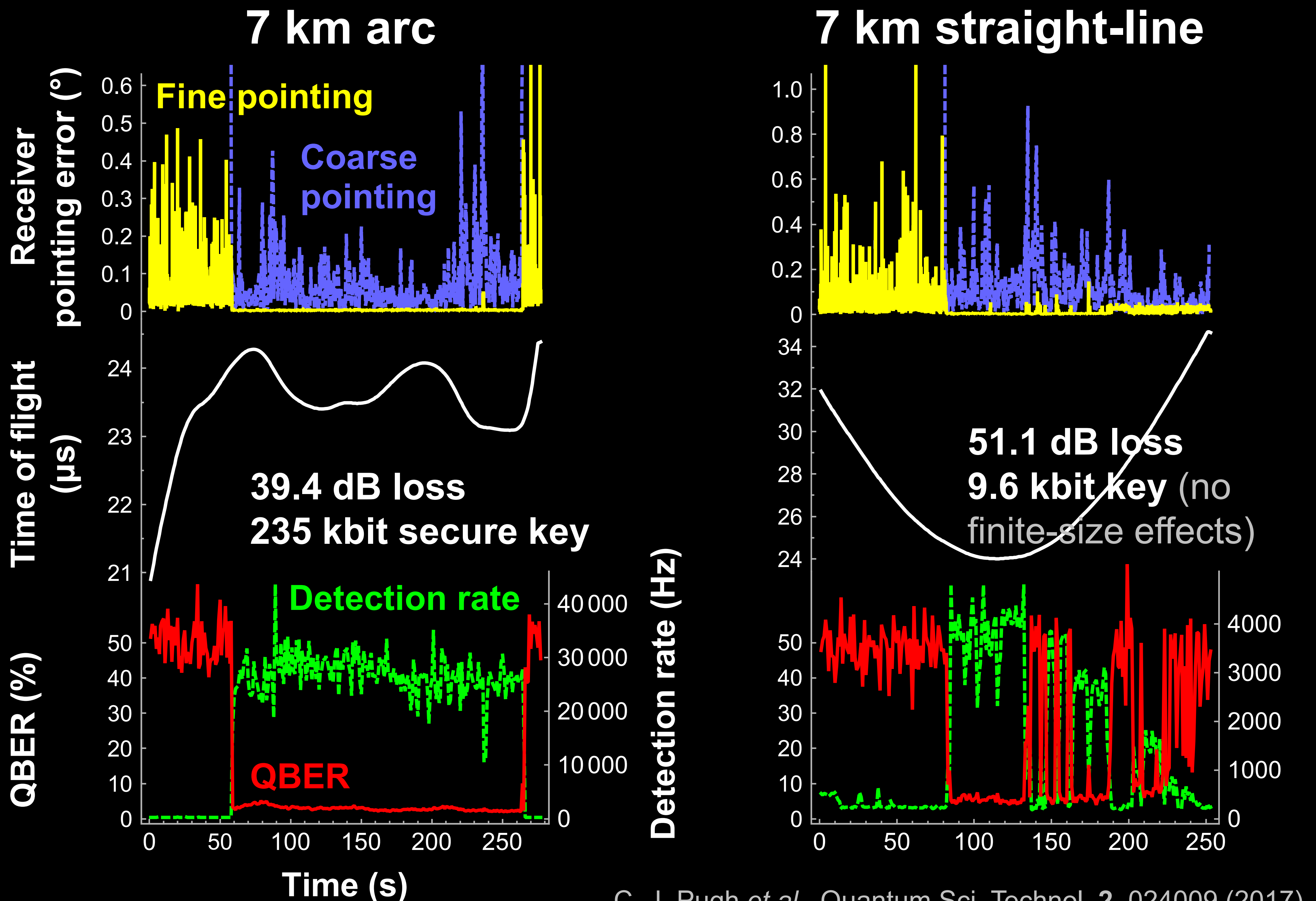
Airborne QKD demonstration

Airborne QKD demonstration

Airborne QKD demonstration

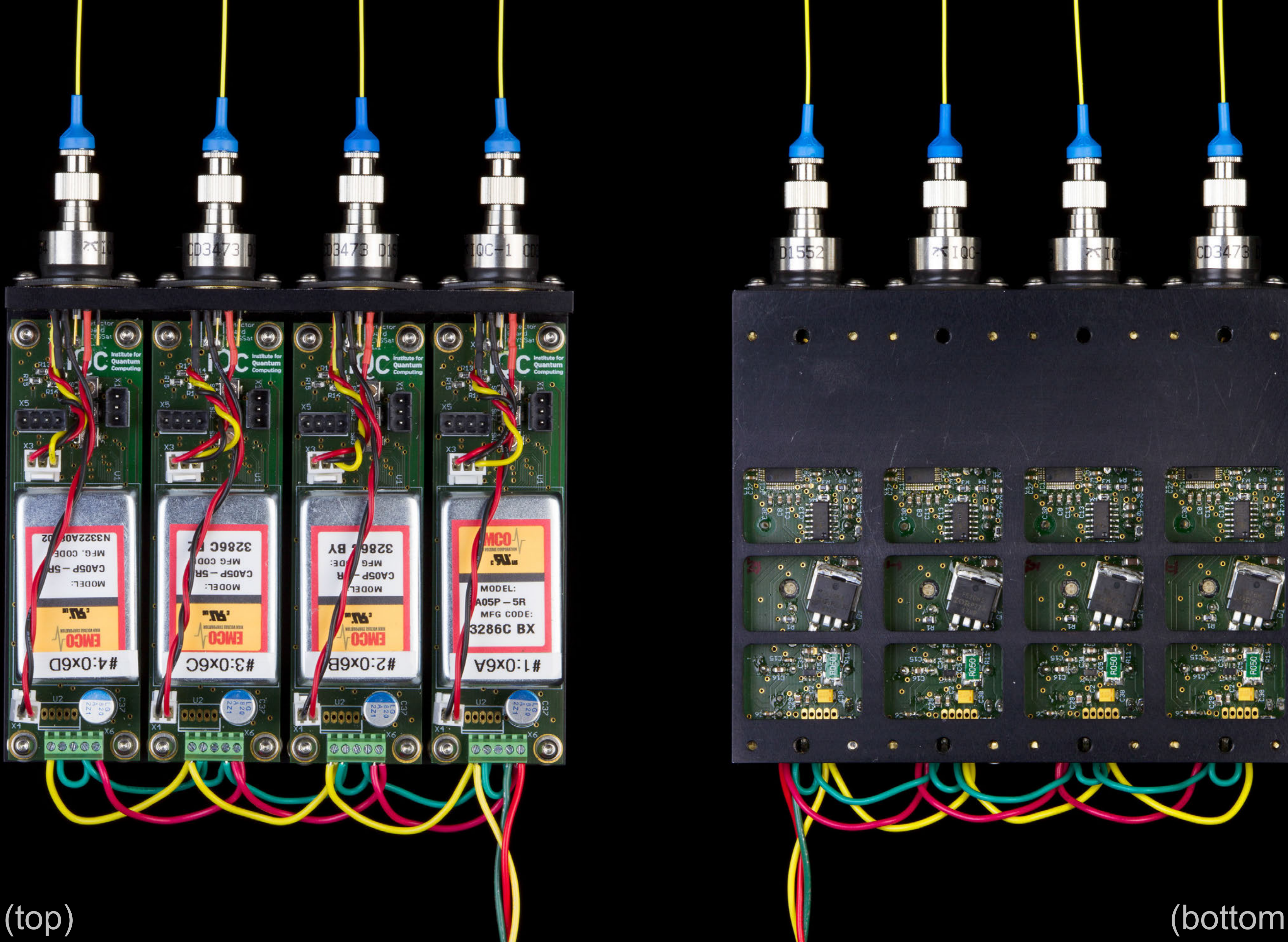
C. J. Pugh *et al.*, Quantum Sci. Technol. **2**, 024009 (2017)

Airborne QKD demonstration



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

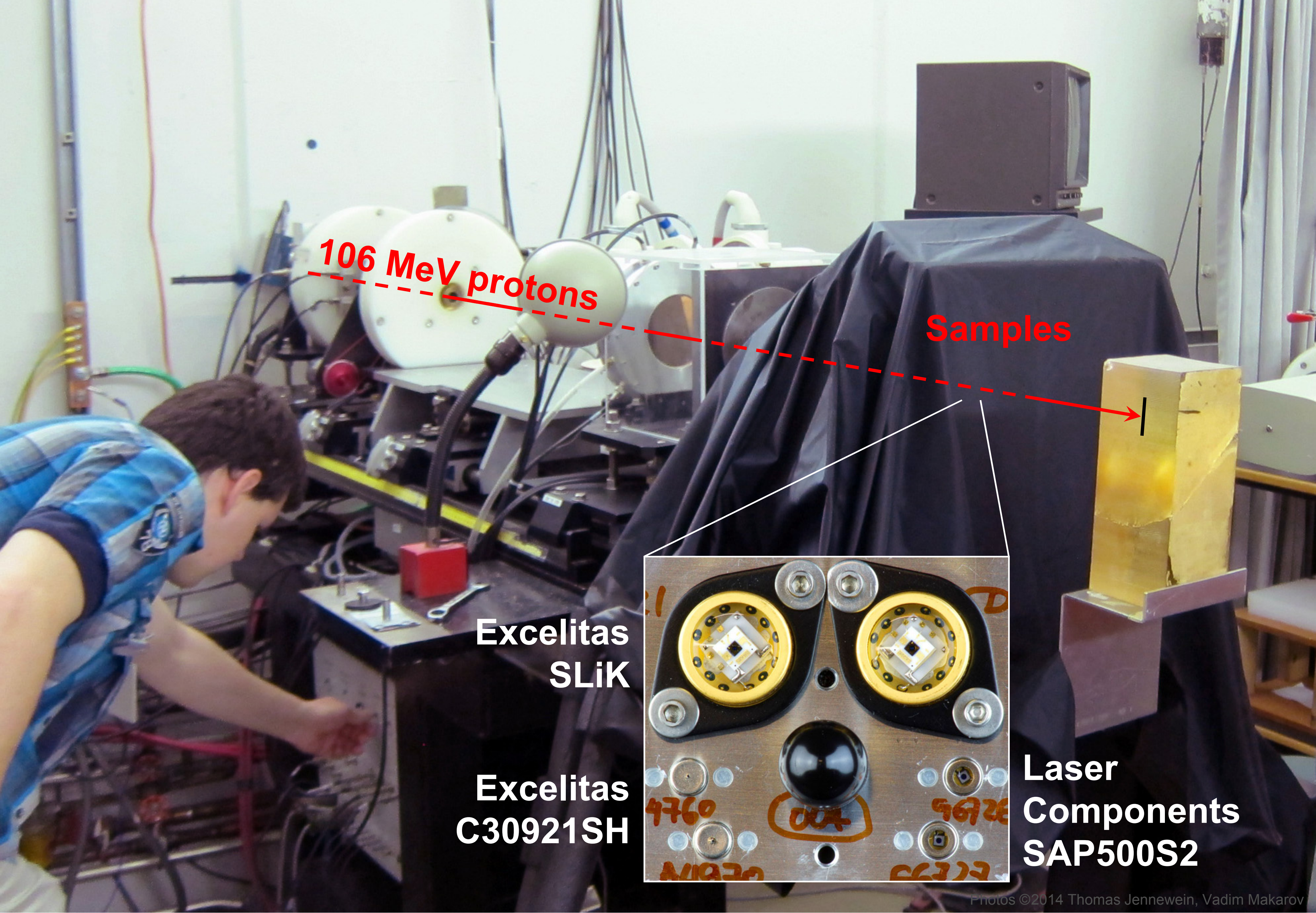
Prototype single-photon detector (4-channel)



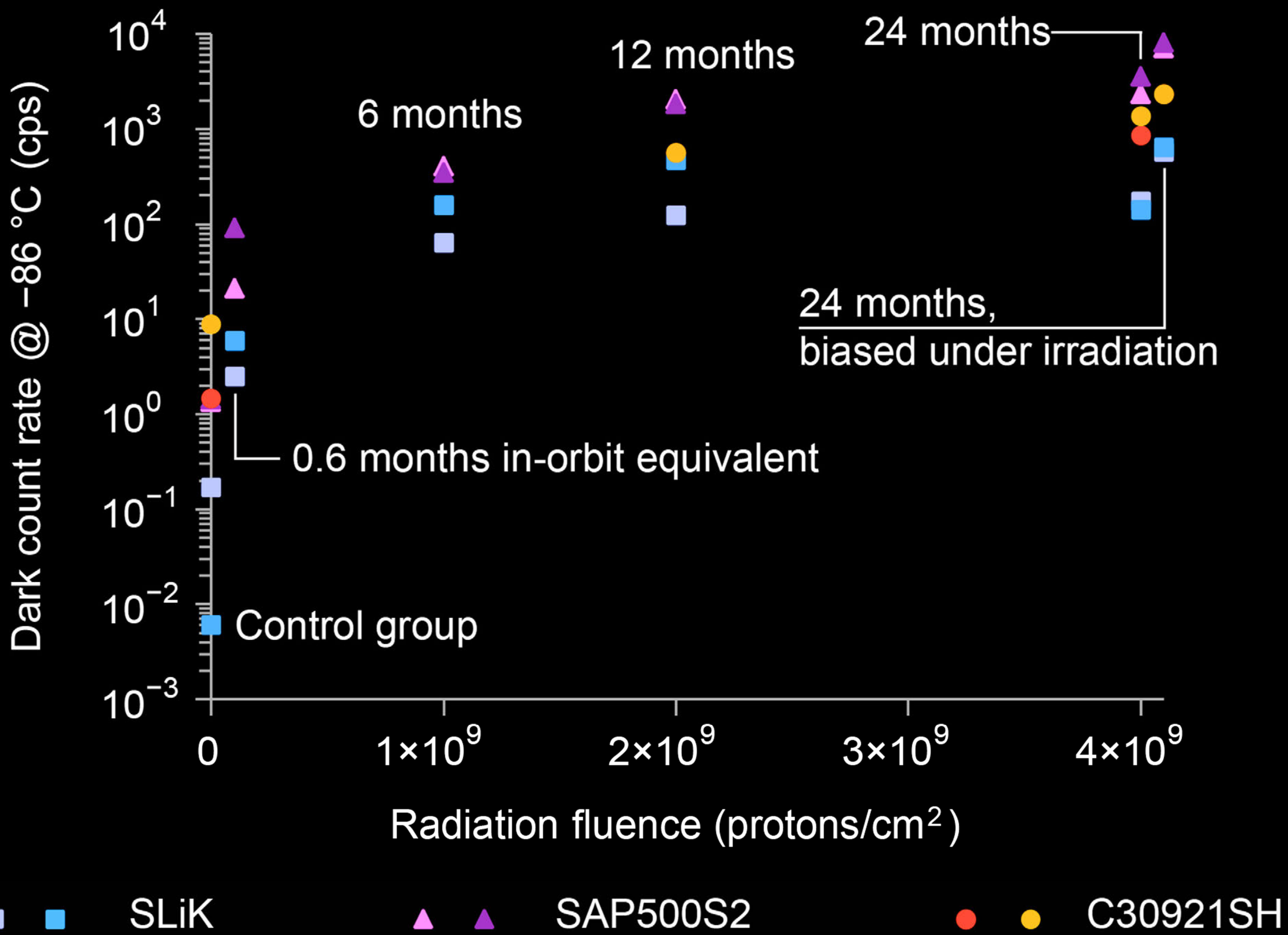
(top)

(bottom)

Proton irradiation facility at TRIUMF (Vancouver)

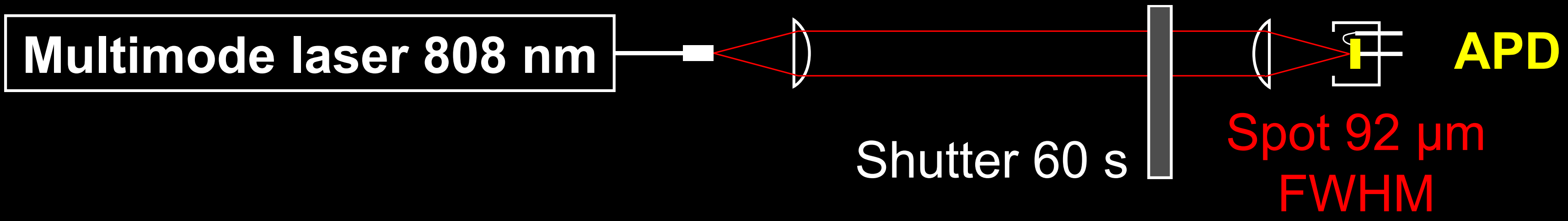


Radiation testing of Si avalanche photodiodes (APDs)



E. Anisimova *et al.*, EPJ Quantum Technol. **4**, 10 (2017)

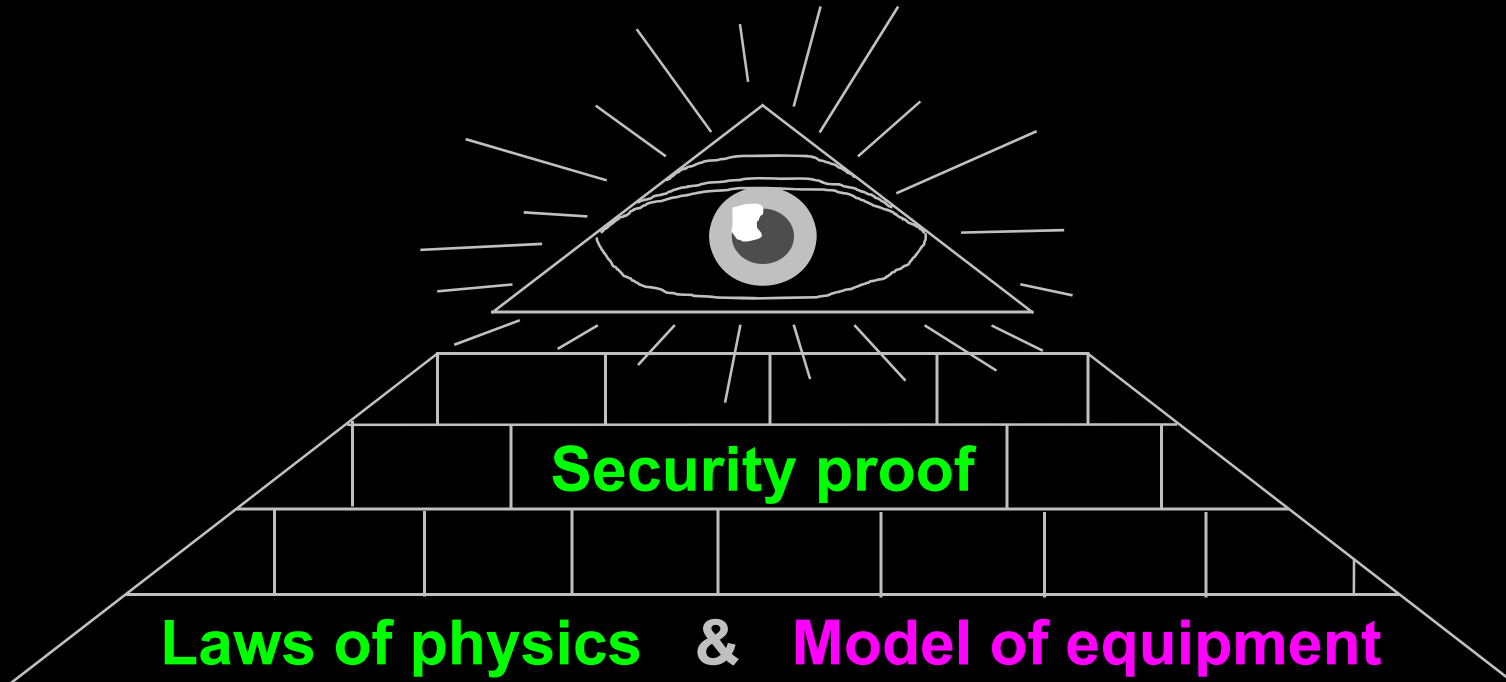
Mitigation: laser annealing



Sample ID	106 MeV proton fluence (cm^{-2})	Equivalent time in 600 km polar orbit (months)	Thermal annealing procedure	Dark count rate at −80 °C			Annealing power (W)
				Before (Hz)	Lowest after (Hz)	Highest reduction factor	
C30902SH-1	10^9	6	None	347	2.3	150	0.8
C30902SH-2	10^9	6	None	363	2.64	137	1.5
SLiK-1	10^8	0.6	2 h @ +100 °C	6.71	0.16	41.7	1.4
SLiK-2	10^8	0.6	2 h @ +100 °C	2.19	0.42	5.3	0.8
SLiK-3	4×10^9	24	4 h @ +80 °C, 2 h @ +100 °C	43.1	2.09	21	1.4
SLiK-4	10^9	6	None	192	8.3	23	1.0
SLiK-5	4×10^9	24 (with bias voltage applied)	3 h @ +80 °C, 2 h @ +100 °C	447	58	7.7	1.0
SAP500S2-1	4×10^9	24	4 h @ +80 °C, 2 h @ +100 °C	1579	2.08	758	1.4
SAP500S2-2	10^8	0.6	2 h @ +100 °C	213	1.66	128	1.6

J. G. Lim *et al.*, EPJ Quantum Technol. **4**, 11 (2017)

Implementation security of quantum communications



Hack

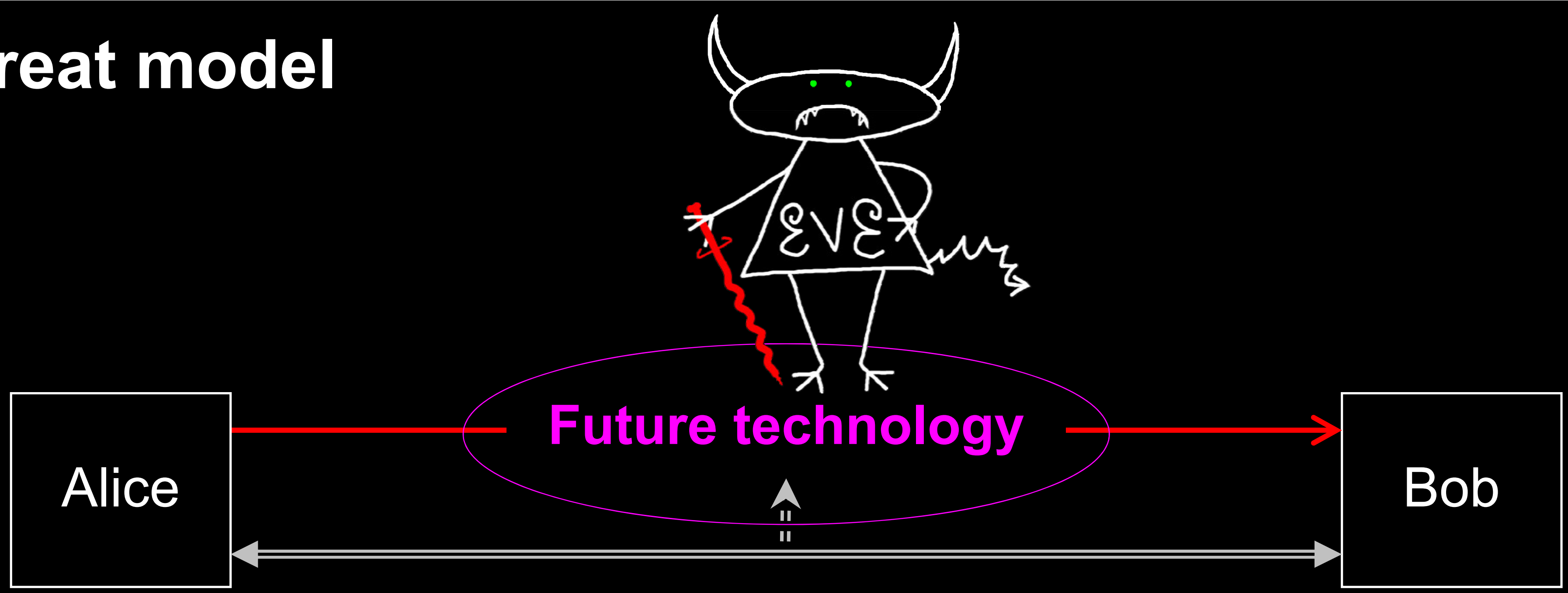
Integrate imperfection into security model

Formal certification: we need standards and labs ecosystem

ETSI
World Class Standards

T. Länger, G. Lenhart, New J. Phys. **11**, 055051 (2009)

Threat model



physically secure,
characteristics known

physically secure,
characteristics known

Kerckhoffs' principle:

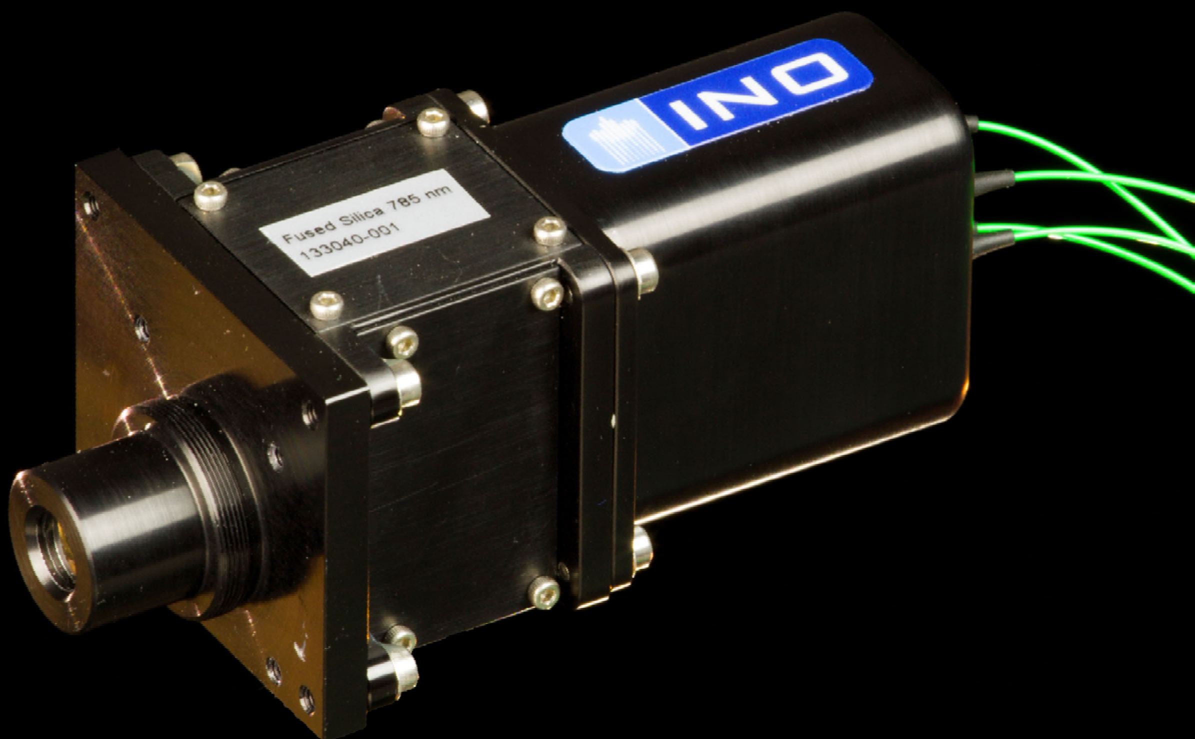
Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi

A. Kerckhoffs, J. des Sciences Militaires **9**, 5 (1883)

Everything about the system that is not explicitly secret is known to the enemy

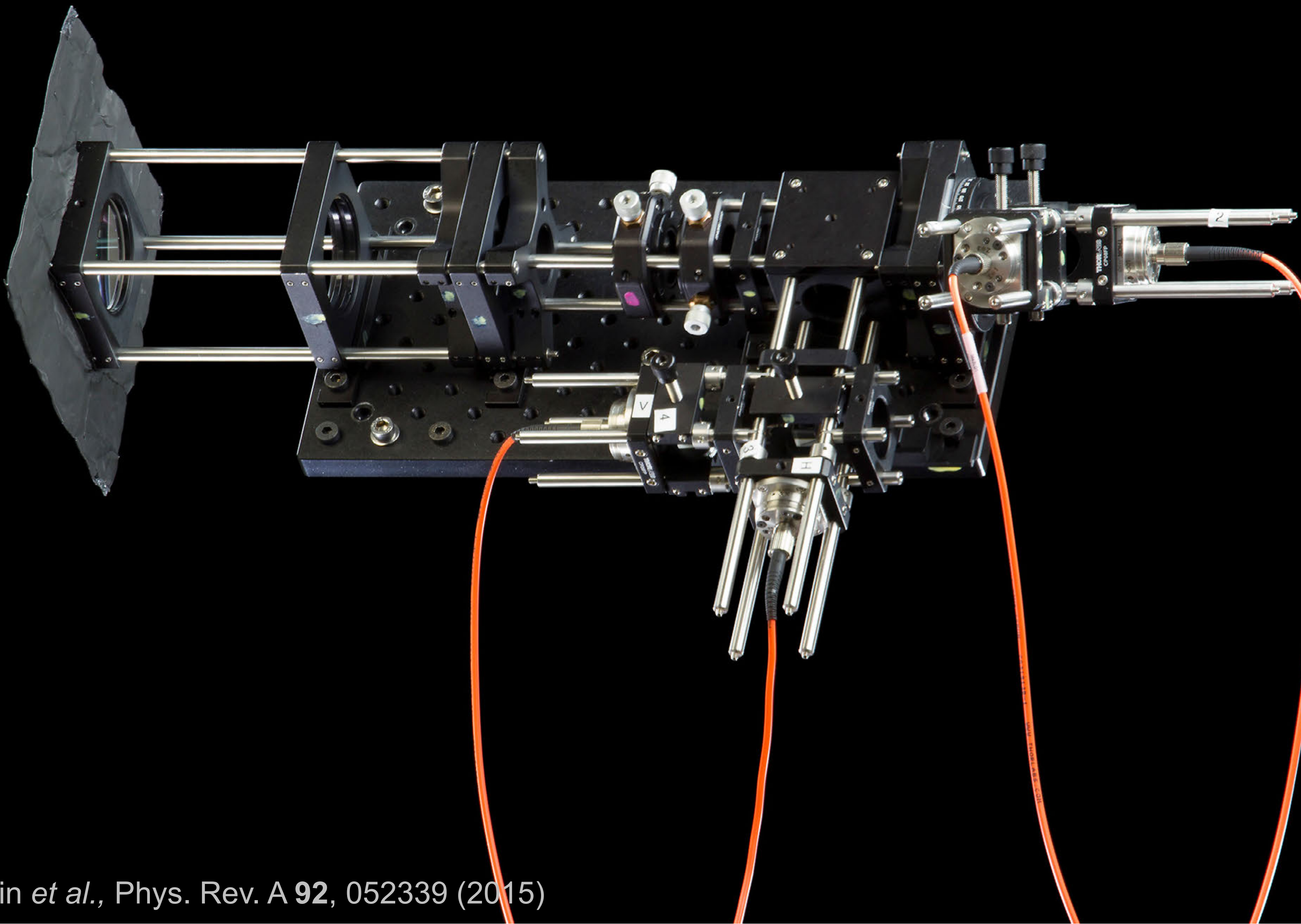
Attack	Target component	Tested system
Intersymbol interference K. Yoshino *et al.,* poster at QCrypt (2016)	intensity modulator in Alice	research system
Laser damage V. Makarov *et al.,* Phys. Rev. A **94**, 030302 (2016)	any	ID Quantique, research system
Spatial efficiency mismatch M. Rau *et al.,* 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); S. Sajeed *et al.,* arXiv:1704.07749	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

Polarization receiver for satellite



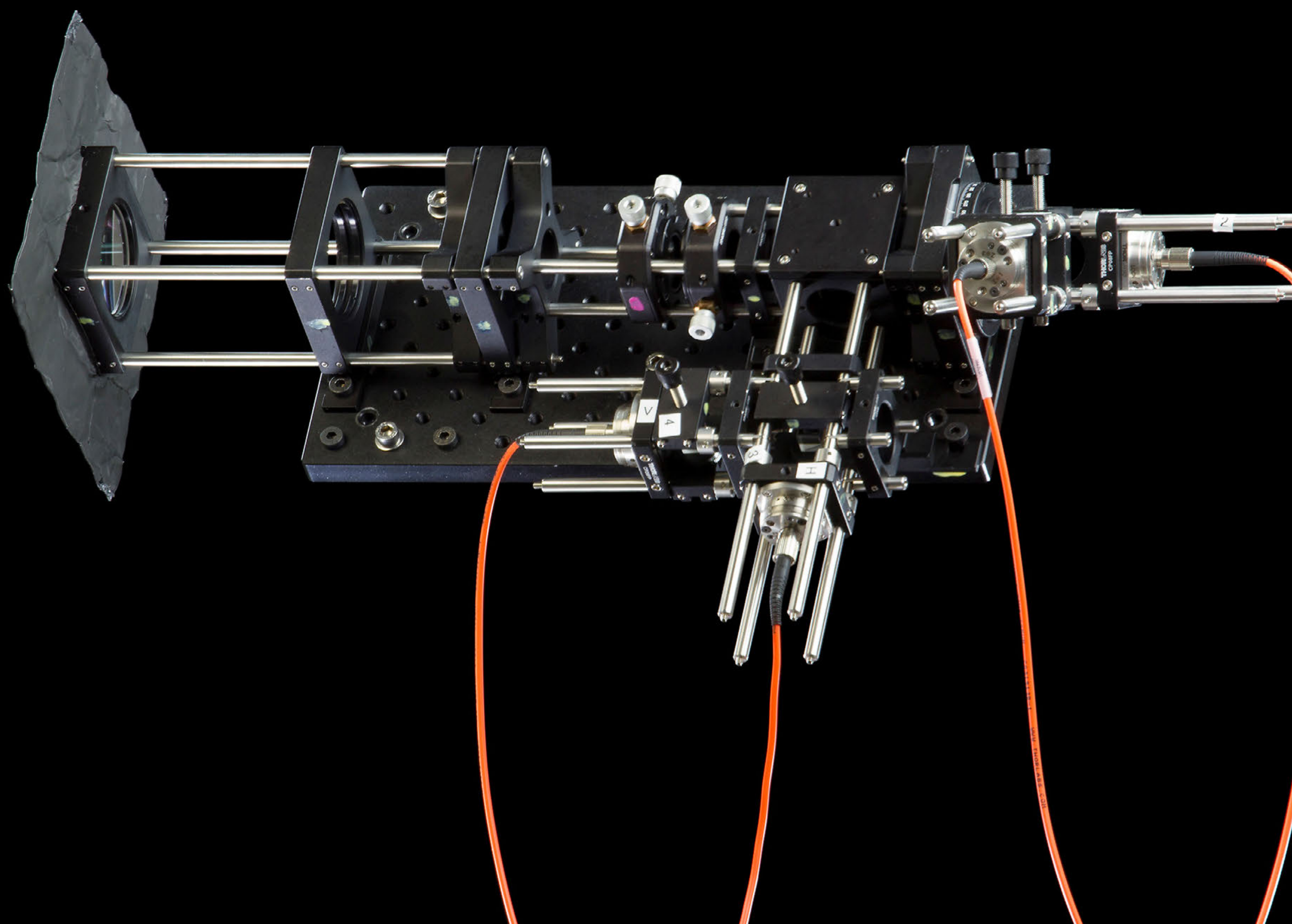
C. J. Pugh *et al.,* Quantum Sci. Technol. **2**, 024009 (2017)

Polarization analyzer



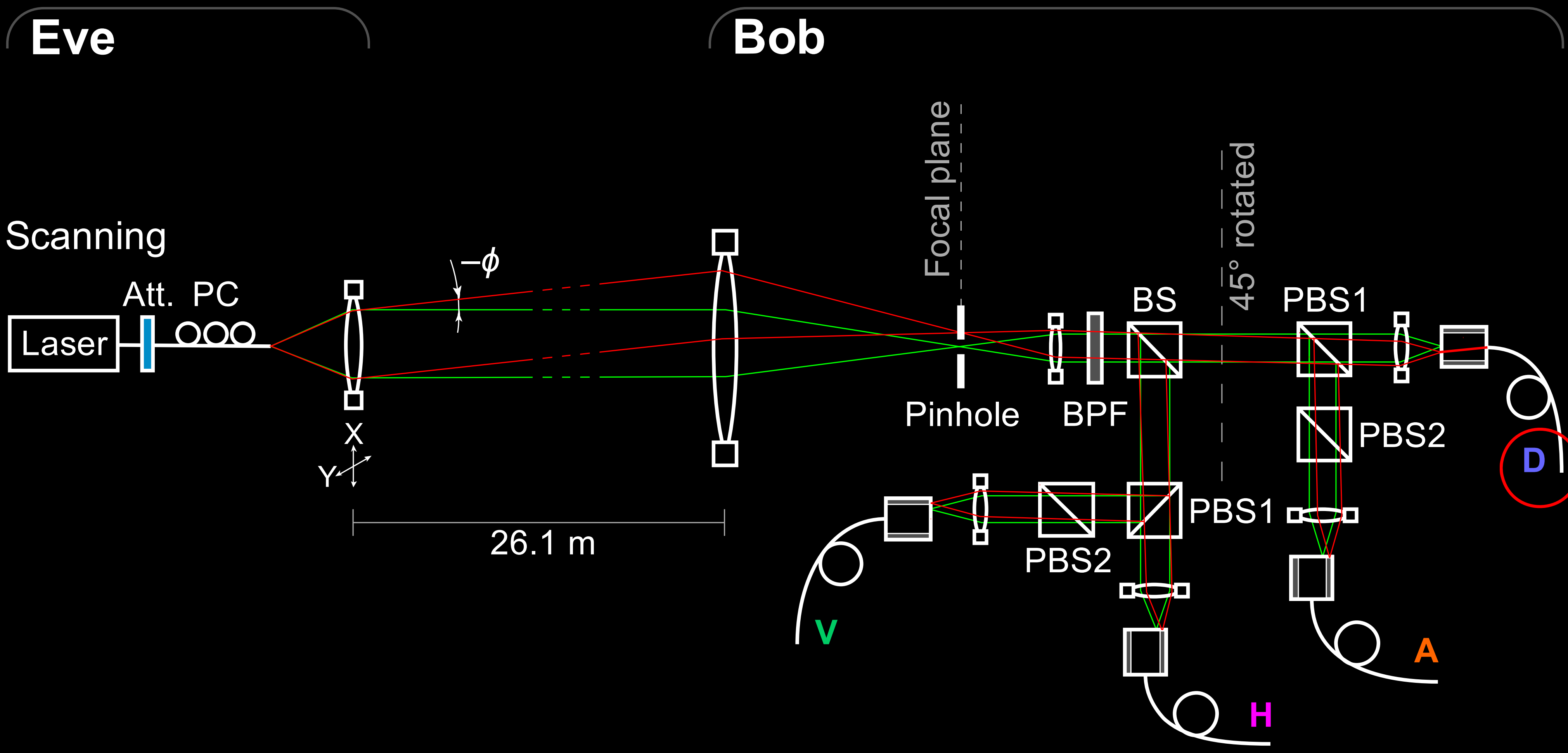
J.-P. Bourgoin *et al.,* Phys. Rev. A **92**, 052339 (2015)

Polarization analyzer



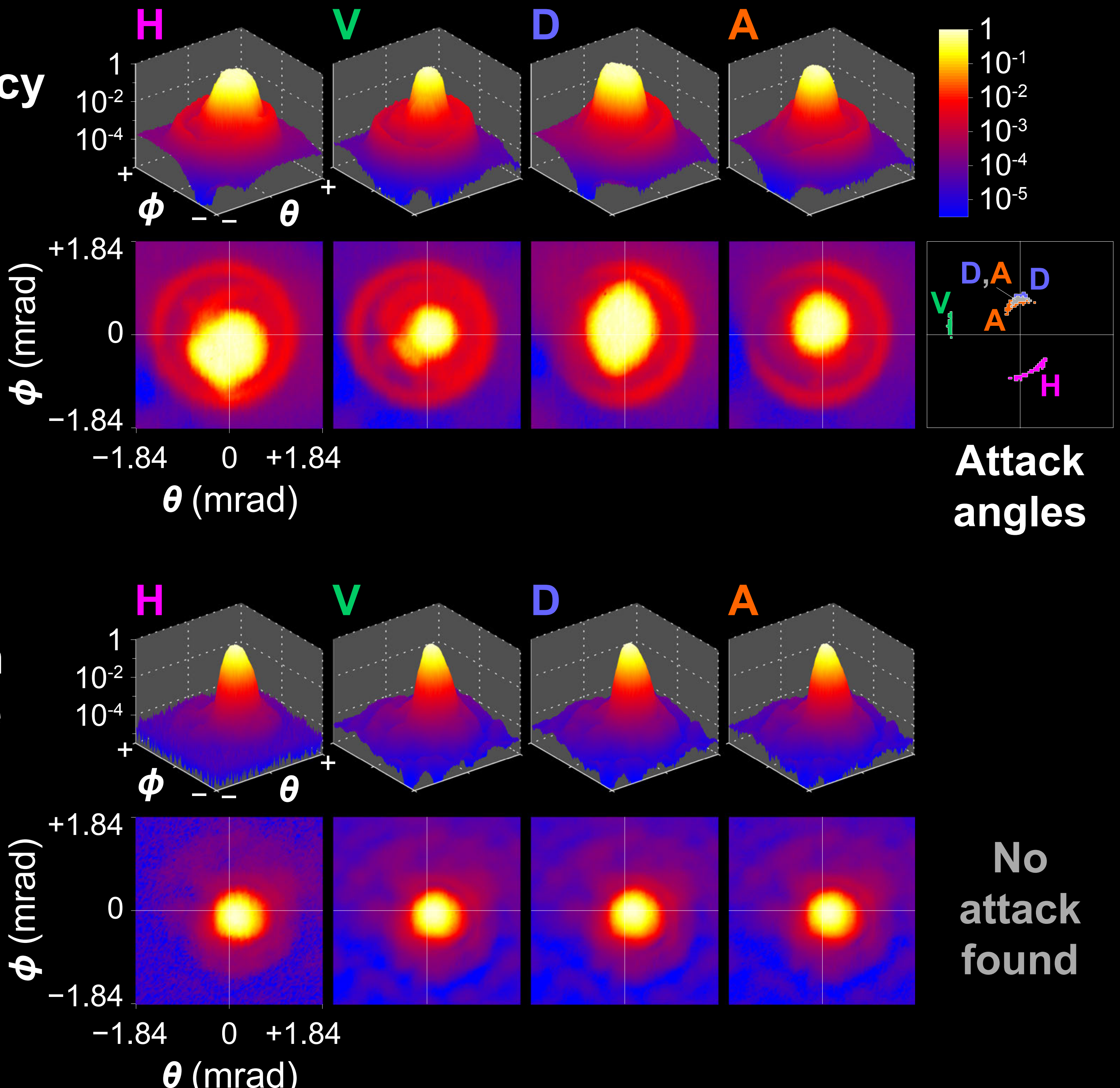
J.-P. Bourgoin *et al.*, Phys. Rev. A **92**, 052339 (2015)

Efficiency mismatch in polarization analyzer



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

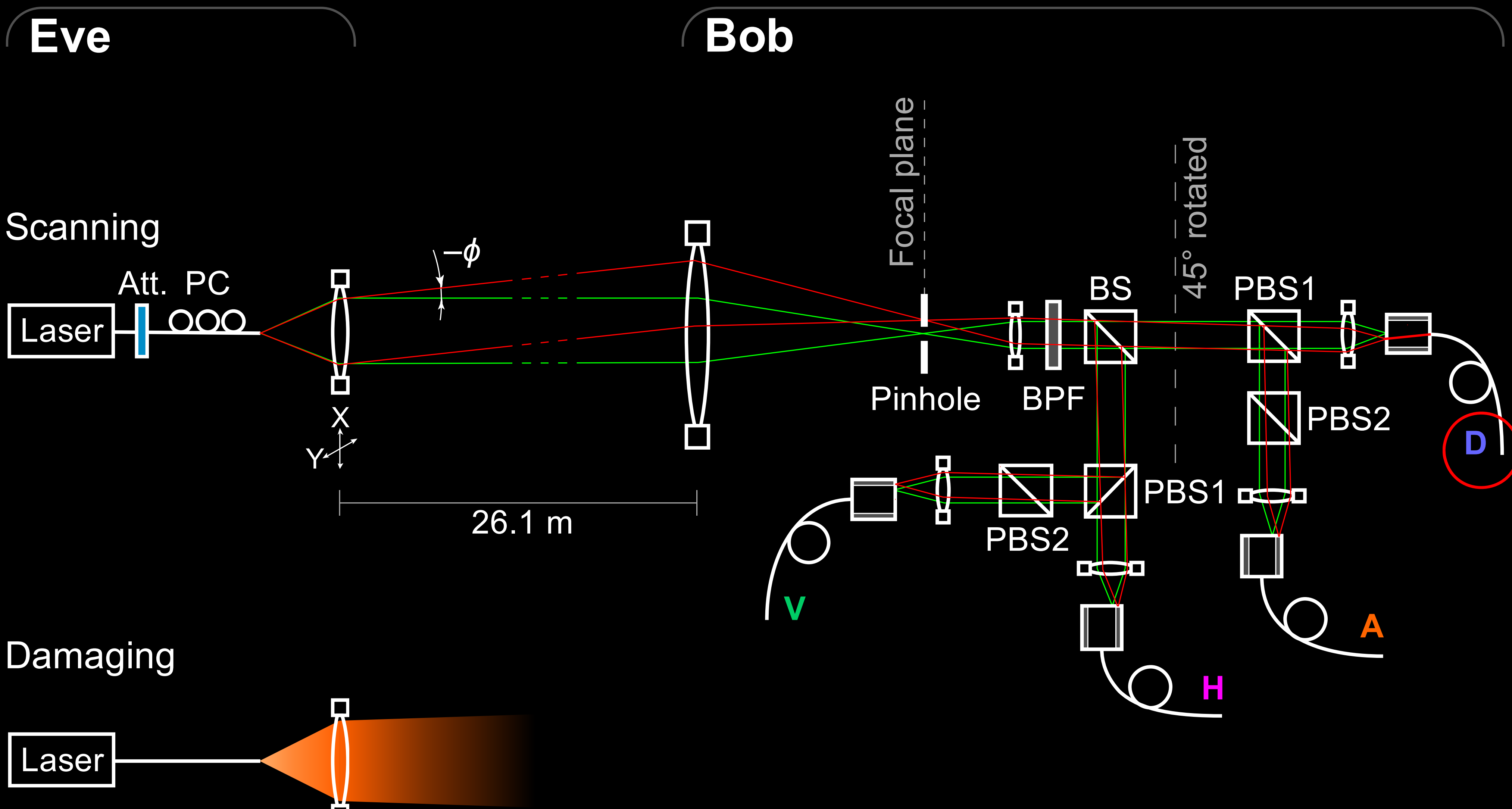
Detector efficiency without pinhole



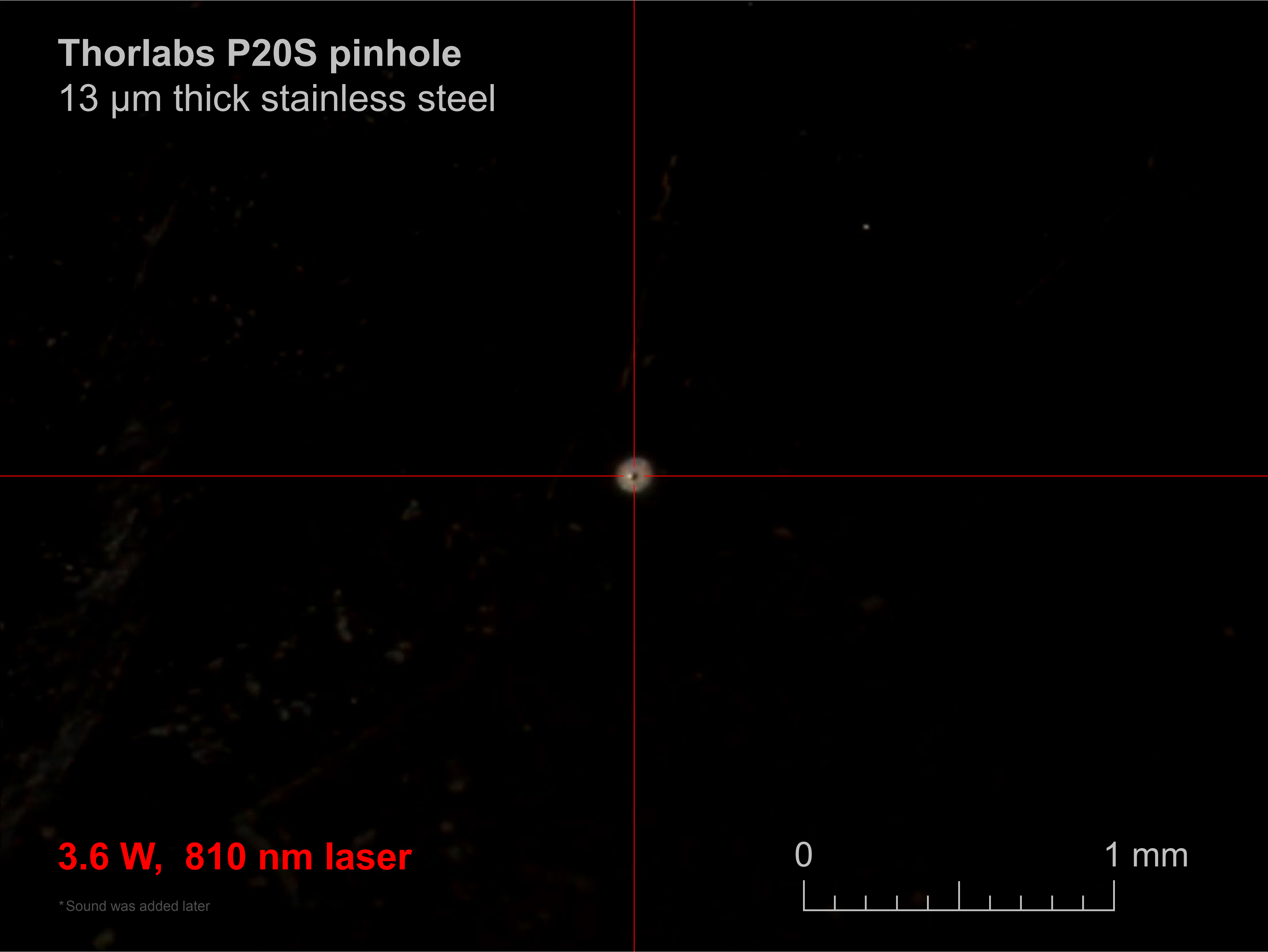
...and with 25 µm diameter pinhole

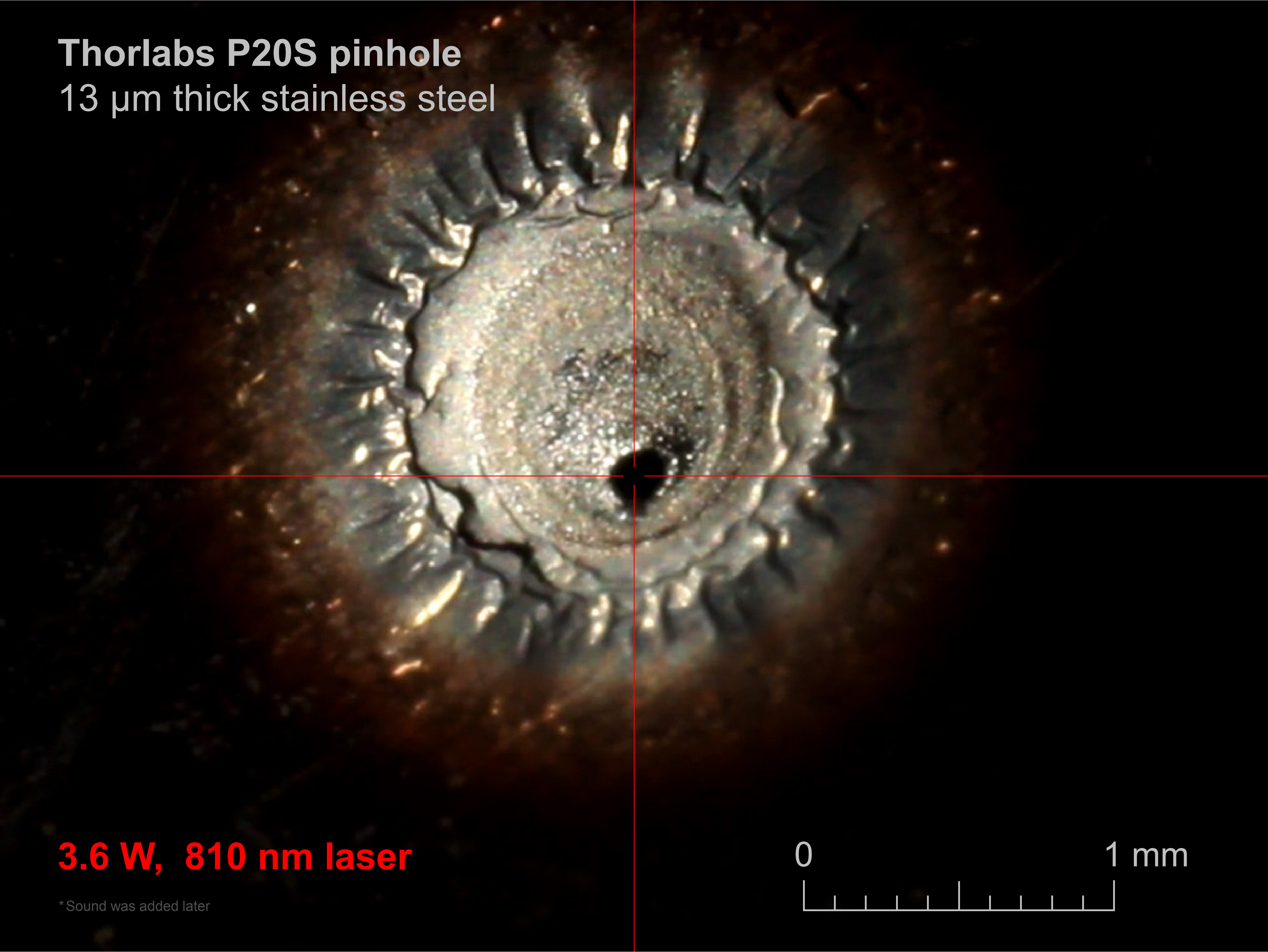
S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015)

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 (informal) of industrial systems

NDA, full access to engineering documentation

Team of experts :) ►

Stage I: Initial analysis of documentation

Stage II: Lab testing / follow-up

Goal: Identify all known potential vulnerabilities in optics and electronics

Example of initial analysis report (stage I)

TABLE I: **Summary of potential security issues in [redacted] system.**

Potential security issue	C	Q	Target component	Brief description	Requirements for complete analysis	Lab testing needed?	Risk evaluation
[redacted]	CX	Q1–5,7	[redacted]	[redacted]	Complete circuit diagram of	Yes	High
[redacted]	CX	Q1–3	[redacted]	See Ref. 3.	Complete circuit diagram of	Yes	High
[redacted]	CX	Q1,2	[redacted]	See Ref. 4.	Complete circuit diagram of	Yes	High
[redacted]	C0	Q2,3	[redacted]	Manufacturer needs to implement [redacted]	Known issue. The manufacturer should patch it.	No	High
[redacted]	CX	Q3–5,7	[redacted]	[redacted]	Known issue. The manufacturer should [redacted]	No	Medium
[redacted]	CX	Q1	[redacted]	[redacted]	Model numbers of all optical components; complete receiver for testing.	Yes	High
[redacted]	CX	Q1–5	[redacted]	[redacted]	Complete circuit diagram of [redacted] settings of	Yes	Insufficient information
[redacted]	CX	Q1–3	[redacted]	[redacted]	Algorithm of [redacted]	Yes	Low
[redacted]	CX	Q1,2	[redacted]	See Ref. 13.	Model numbers of [redacted]	Yes	Medium
[redacted]	CX	Q4,5	[redacted]	[redacted]	Full system algorithms; complete system if decided to test.	Maybe	Low
[redacted]	CX	Q1,3–5	[redacted]	Eve can [redacted]	Algorithm for [redacted]	Maybe	Low

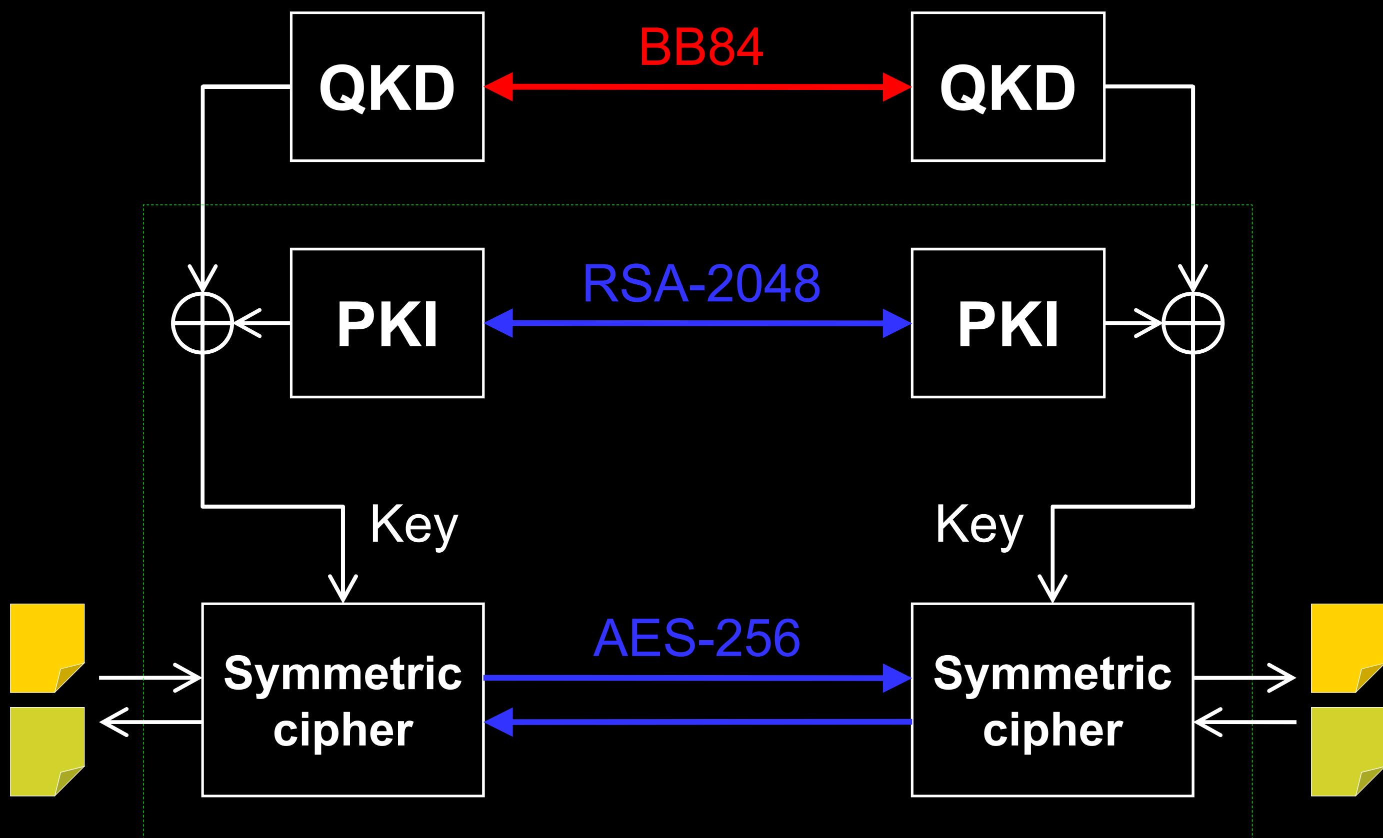
Security audit	System	Stage I	Stage II
IDQ	 Clavis3	2016	ongoing
国盾量子 QuantumCTek	(undisclosed)	2016	ongoing
Univ. Calgary / W. Tittel	MDI-QKD prototype	2017	

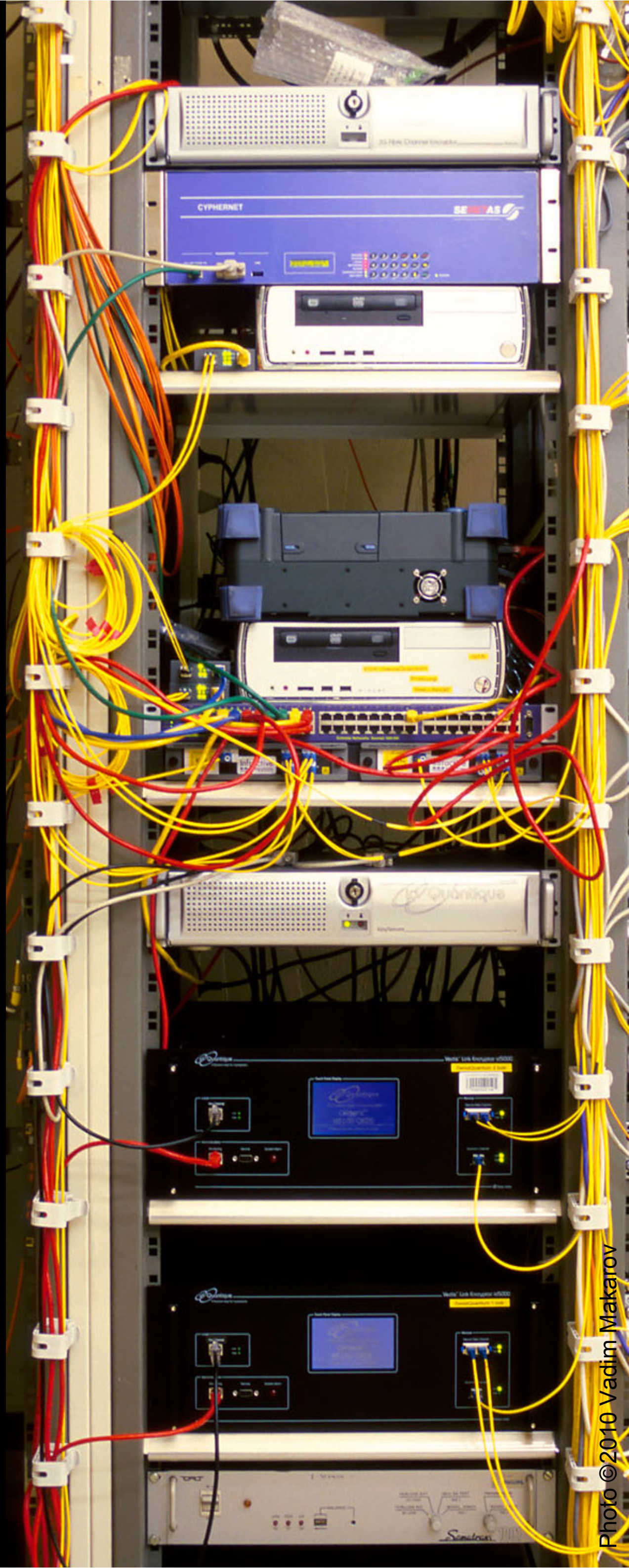
Stepping stone to international security standards

ETSI

Industry standards group in QKD. Open for anyone!

Dual key agreement





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

Credits

Labs of

Thomas Jennewein,

Norbert Lütkenhaus,

Vadim Makarov

UNIVERSITY OF WATERLOO

Quantum hacking lab

vad1.com/lab

Winter school on quantum cybersecurity

Next: 20–26 January 2018
Les Diablerets, Switzerland

2 days (executive track) +
4 days (technical track, with 3 labs)

Overview talks + quantum technologies, including QKD.
Lecturers change, in 2017 were: M. Afzelius, J. P. Aumasson, A. Ekert, M. Legré, V. Makarov, C. Marquardt, M. Mosca, S. Popescu, R. Renner, G. Ribordy, C. William, H. Zbinden.
20 students

€3200 full board (€1800 executive track only)
nice, includes a brief skiing lesson, etc.

Organised by IDQ

QKD summer school

Next: August 2018 (TBC)
Europe or Canada (TBC)

5 days of lectures

Mix of classical and quantum crypto.
Lecturers: D. Jao, T. Jennewein, N. Lütkenhaus, V. Makarov, M. Mosca, R. Renner, D. Stinson.
60 students

$600 including housing
no frills!

Org. by IQC Institute for Quantum Computing