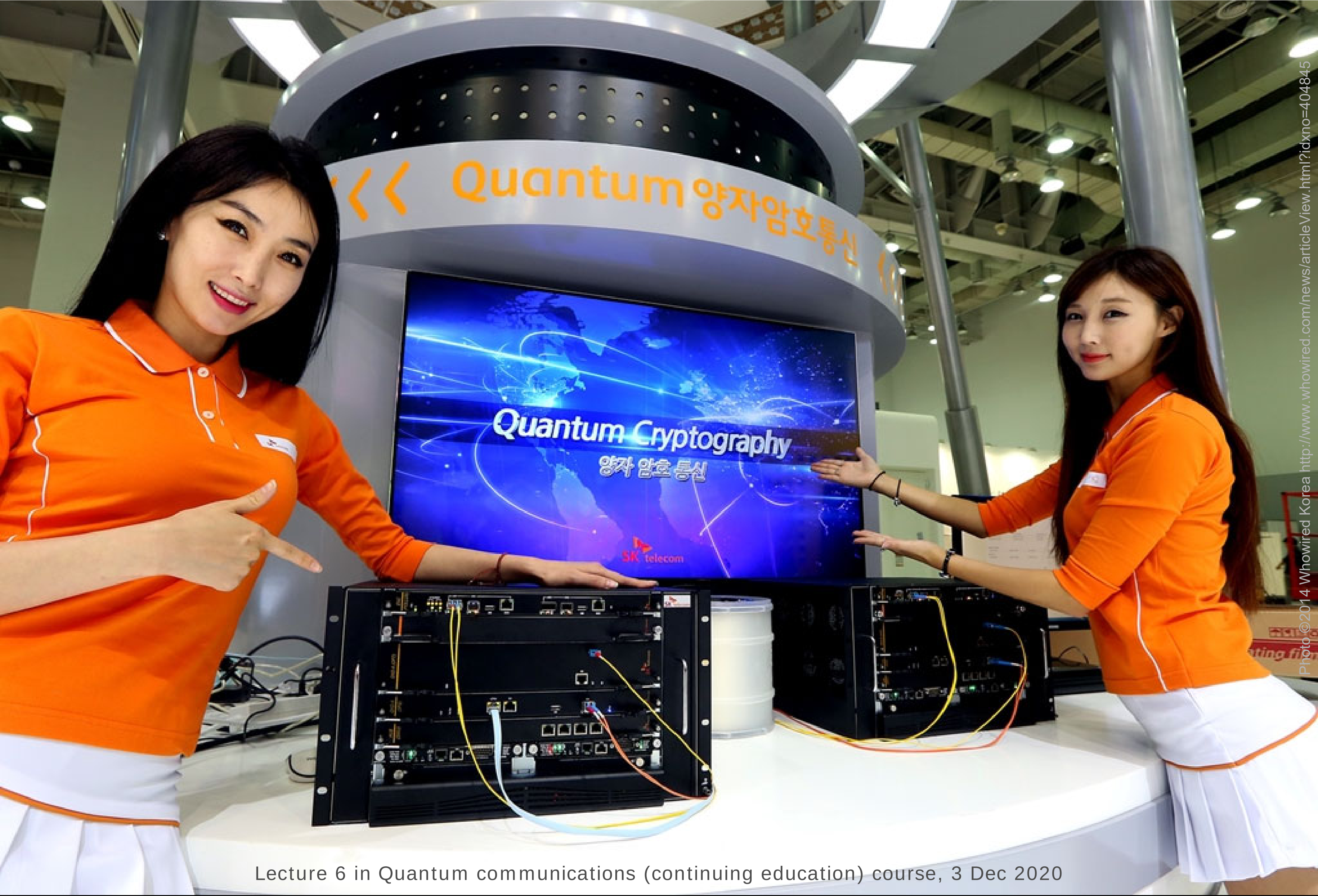
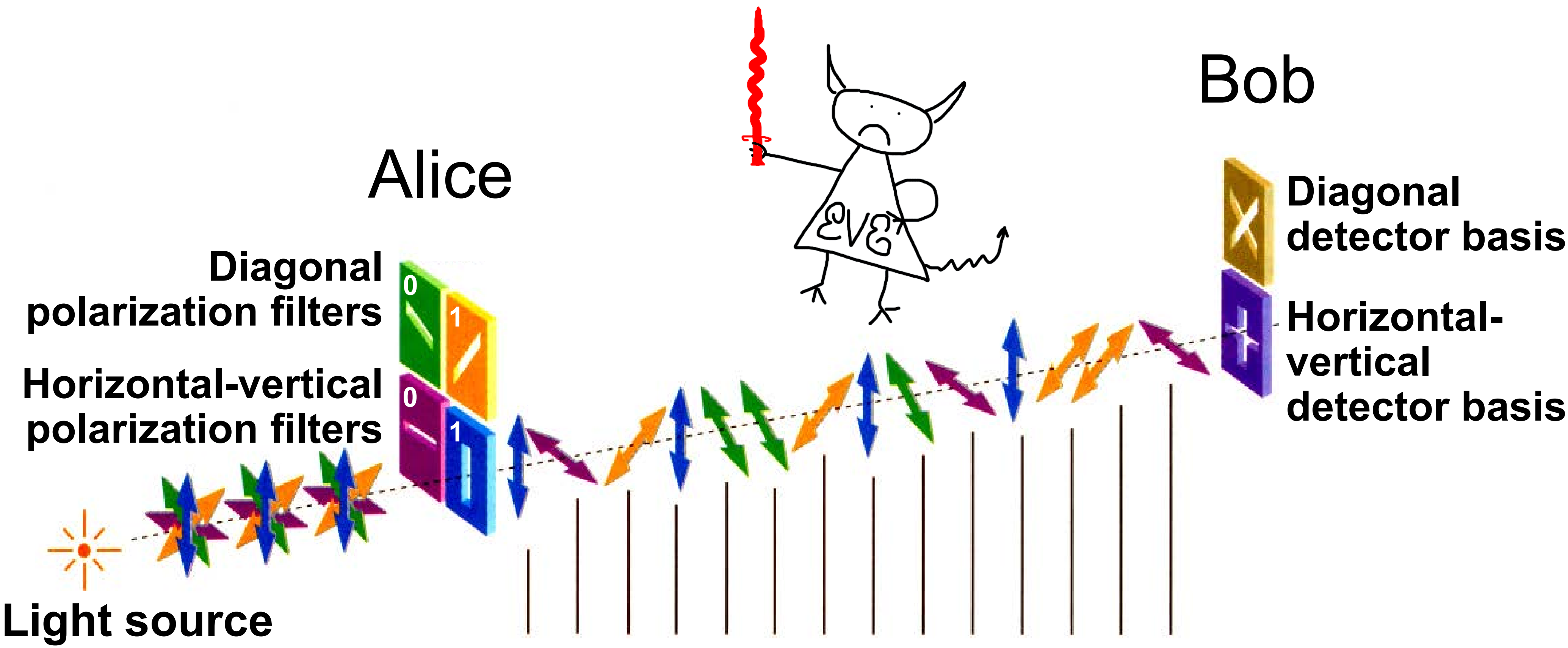


Lecture 6 in Quantum communications (continuing education) course, 3 Dec 2020

QKD protocol and hacking

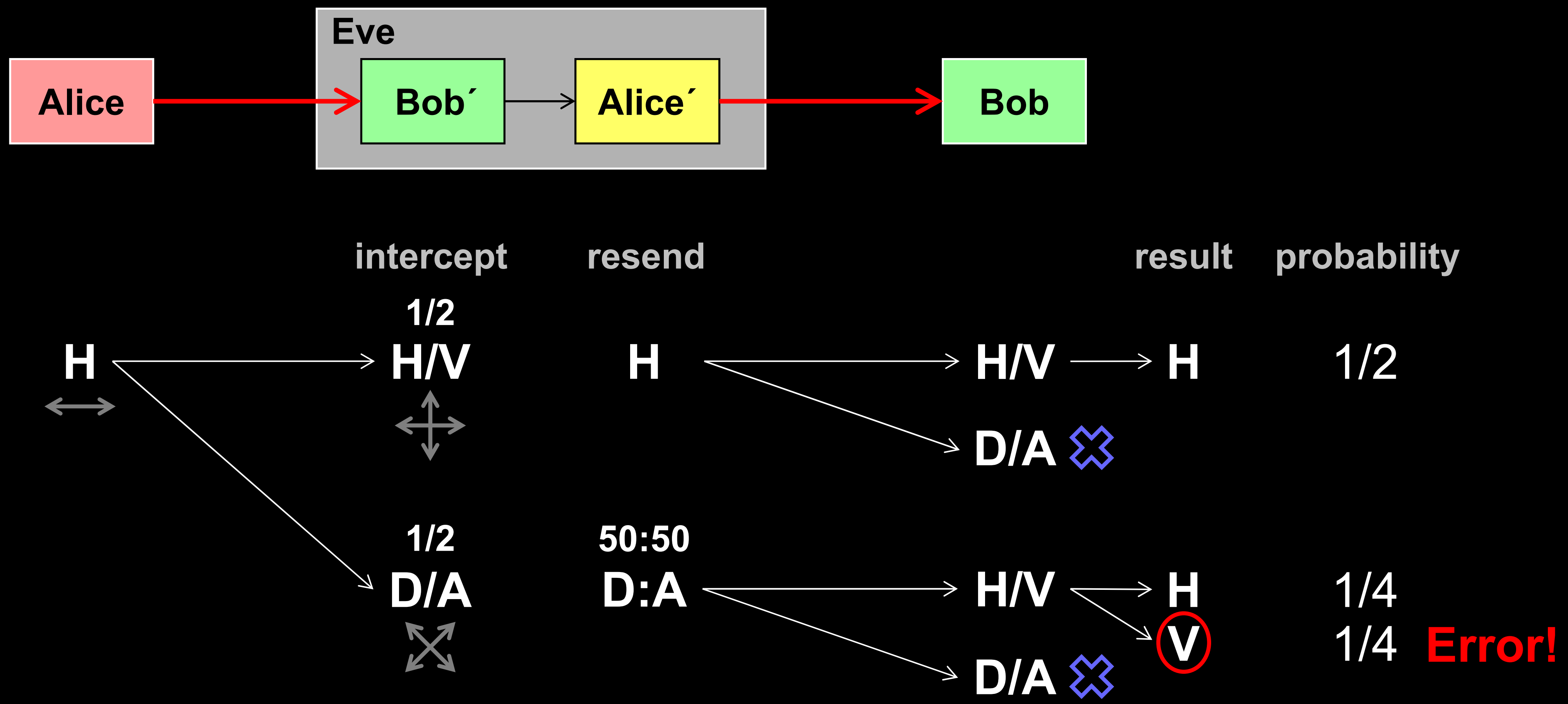
Bennett-Brassard 1984 (BB84) QKD protocol



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

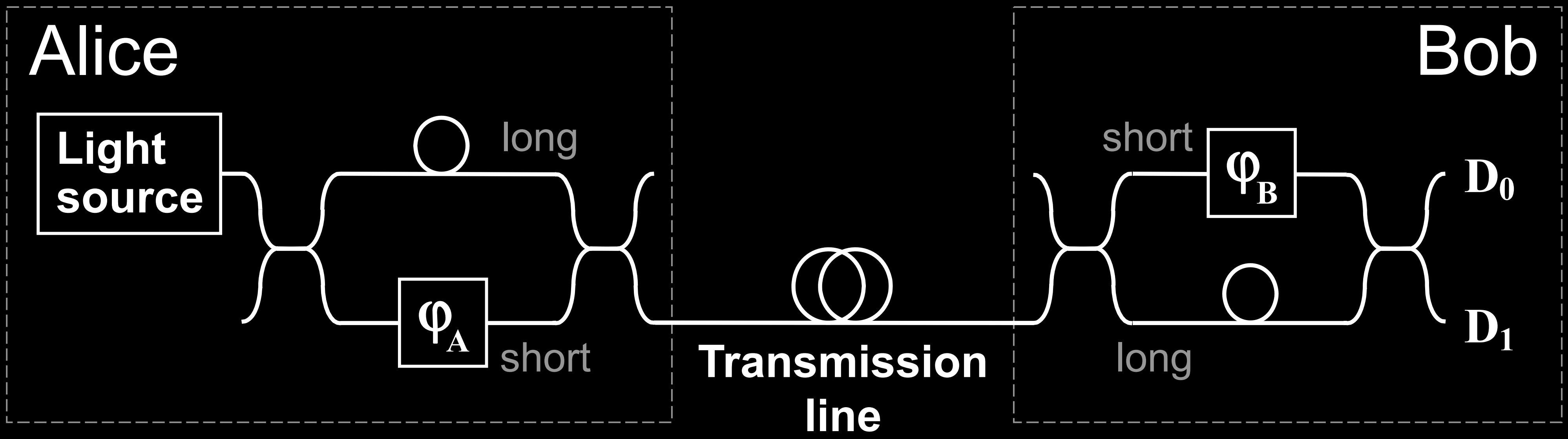
Image reprinted from article: W. Tittel, G. Ribordy & N. Gisin, "Quantum cryptography," Physics World, March 1998

Intercept-resend attack



C. H. Bennett, G. Brassard, in *Proc. Intl. Conf. on Computers, Systems, and Signal Processing (Bangalore, India)*, p. 175 (1984)

Phase (time-bin) encoding, interferometric QKD channel



Detection basis:

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

π or $3\pi/2$: 1

$\varphi_B =$ 0 : X

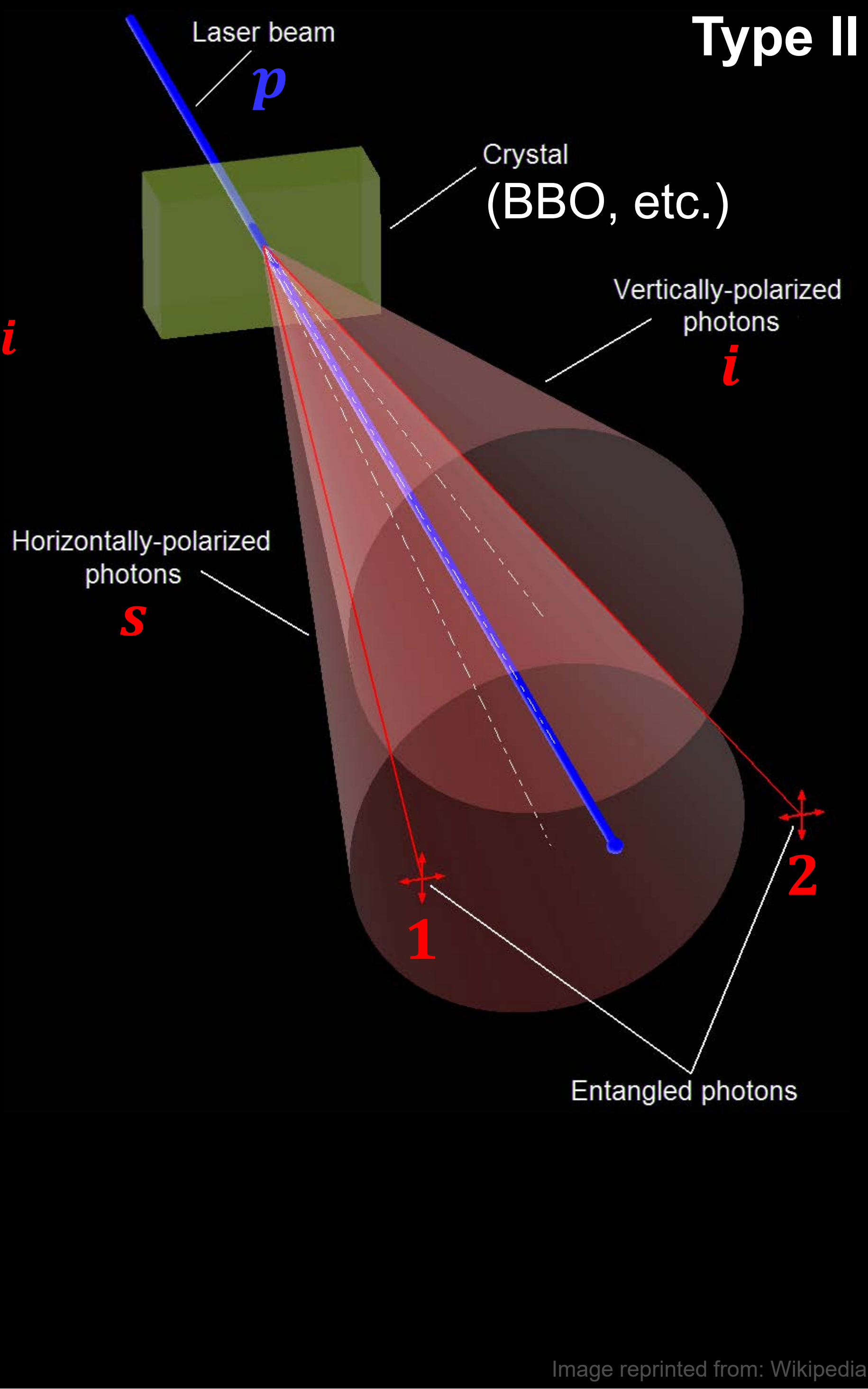
$\pi/2$: Z

Spontaneous parametric down-conversion

Energy conservation: $\omega_p = \omega_s + \omega_i$

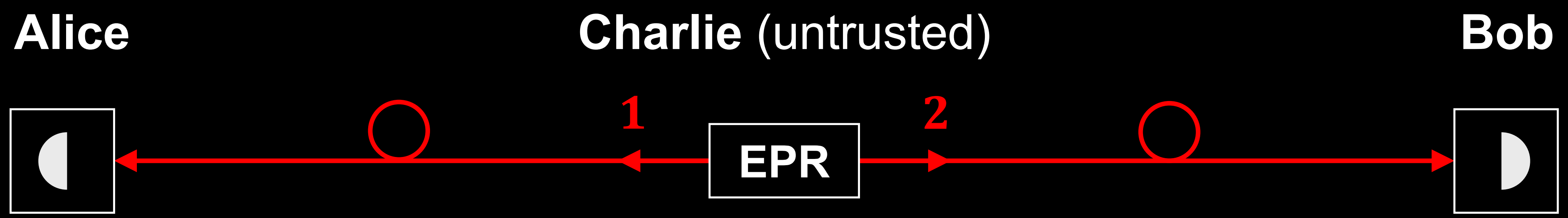
Momentum conservation: $\vec{k}_p = \vec{k}_s + \vec{k}_i$

$$|\psi\rangle = (|H_1, V_2\rangle + |V_1, H_2\rangle)/\sqrt{2}$$
$$= (|D_1, A_2\rangle + |A_1, D_2\rangle)/\sqrt{2}$$



P. G. Kwiat *et al.*, Phys. Rev. Lett. **75**, 4337 (1995)

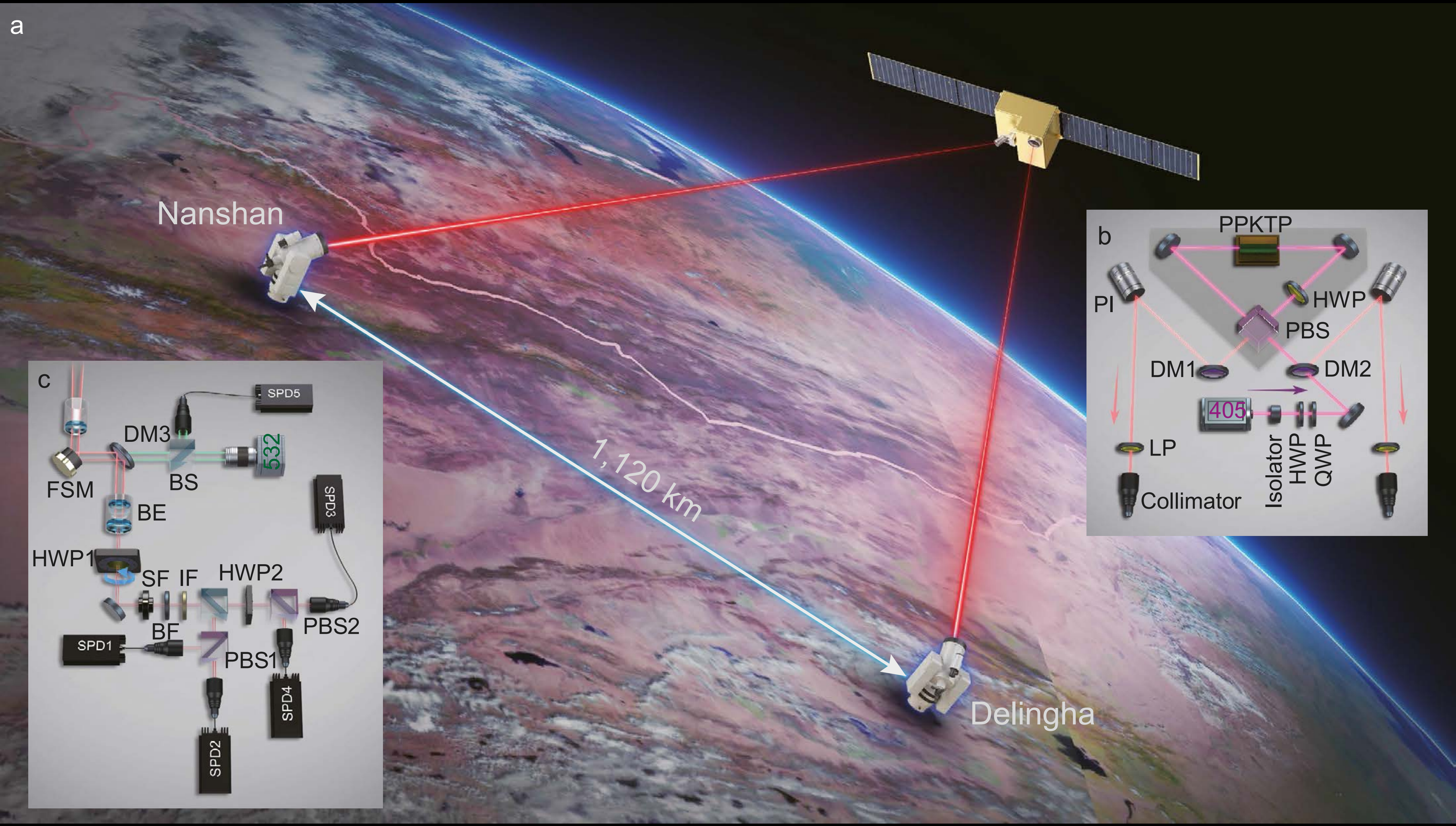
Entangled-pair QKD



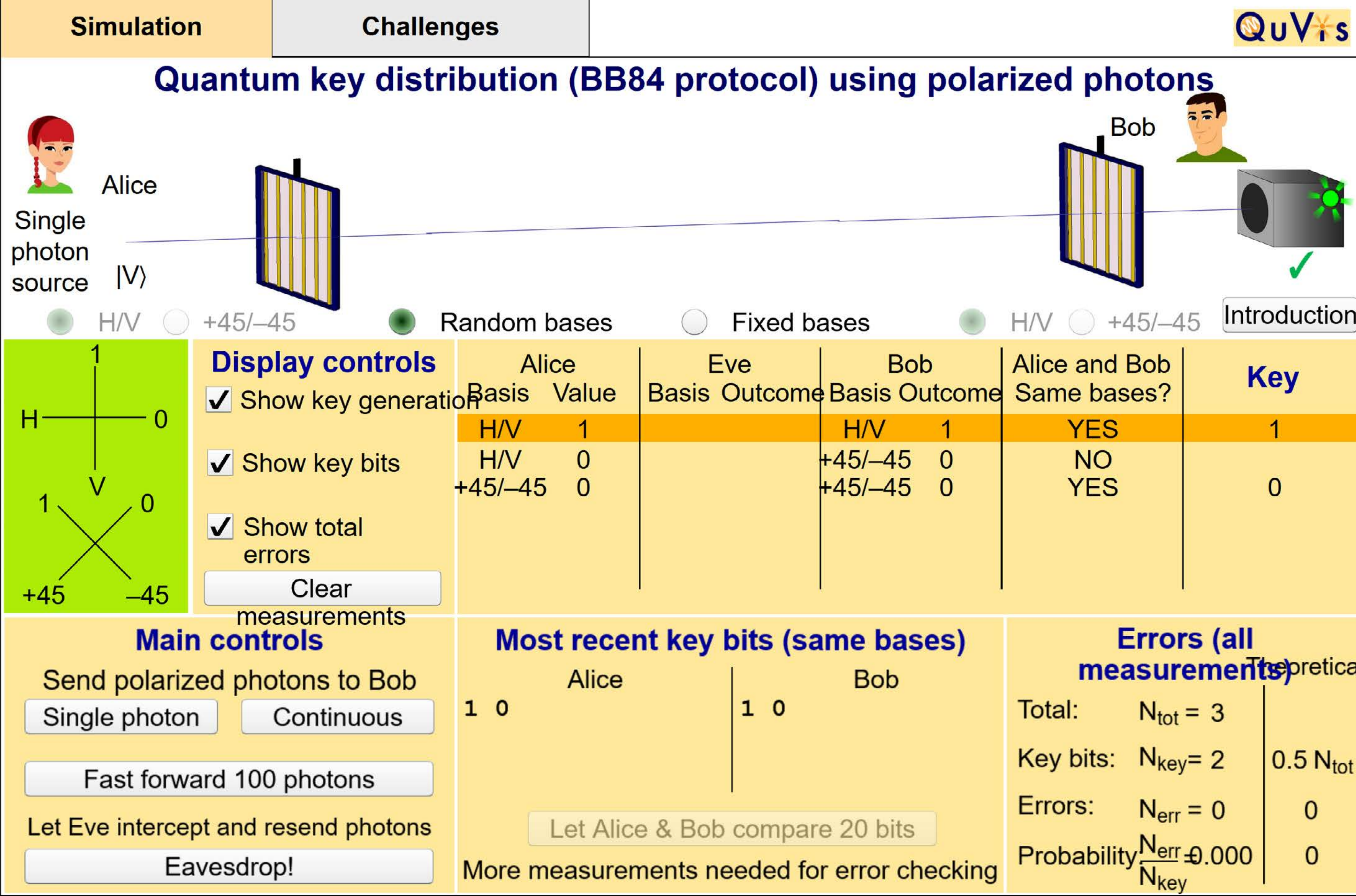
$$|\psi\rangle = (|H_1, V_2\rangle + |V_1, H_2\rangle)/\sqrt{2}$$
$$= (|D_1, A_2\rangle + |A_1, D_2\rangle)/\sqrt{2}$$

A. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
C. H. Bennett, G. Brassard, N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992)

Entangled-pair QKD over 1120 km



J. Yin *et al.*, Nature **582**, 501 (2020)



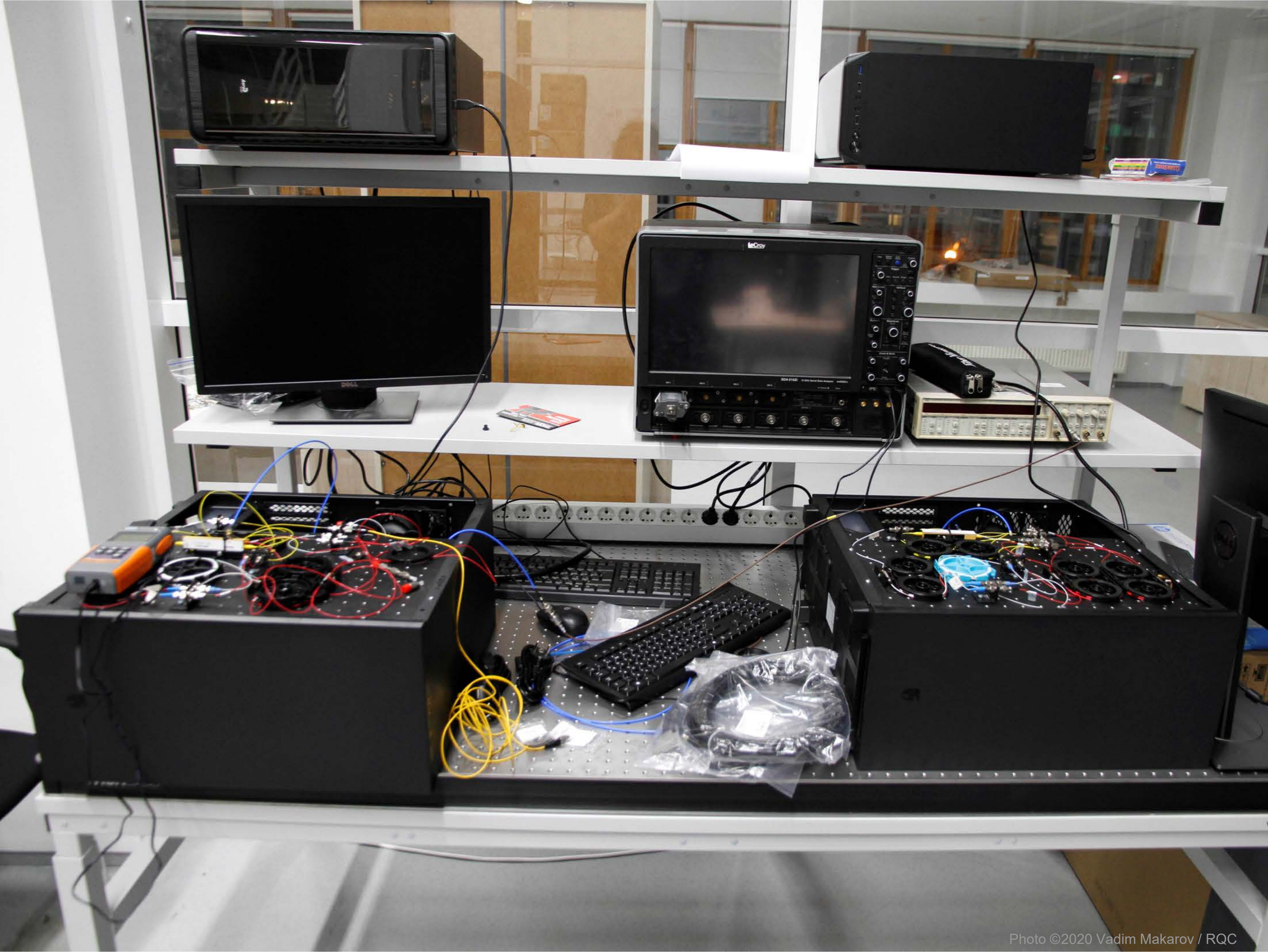
https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/BB84_photons/BB84_photons.html

THORLABS

Discovery

EDU-QCRY1
EDU-QCRY1/M
Quantum Cryptography Demonstration Kit

Manual


LeCroy
DELL

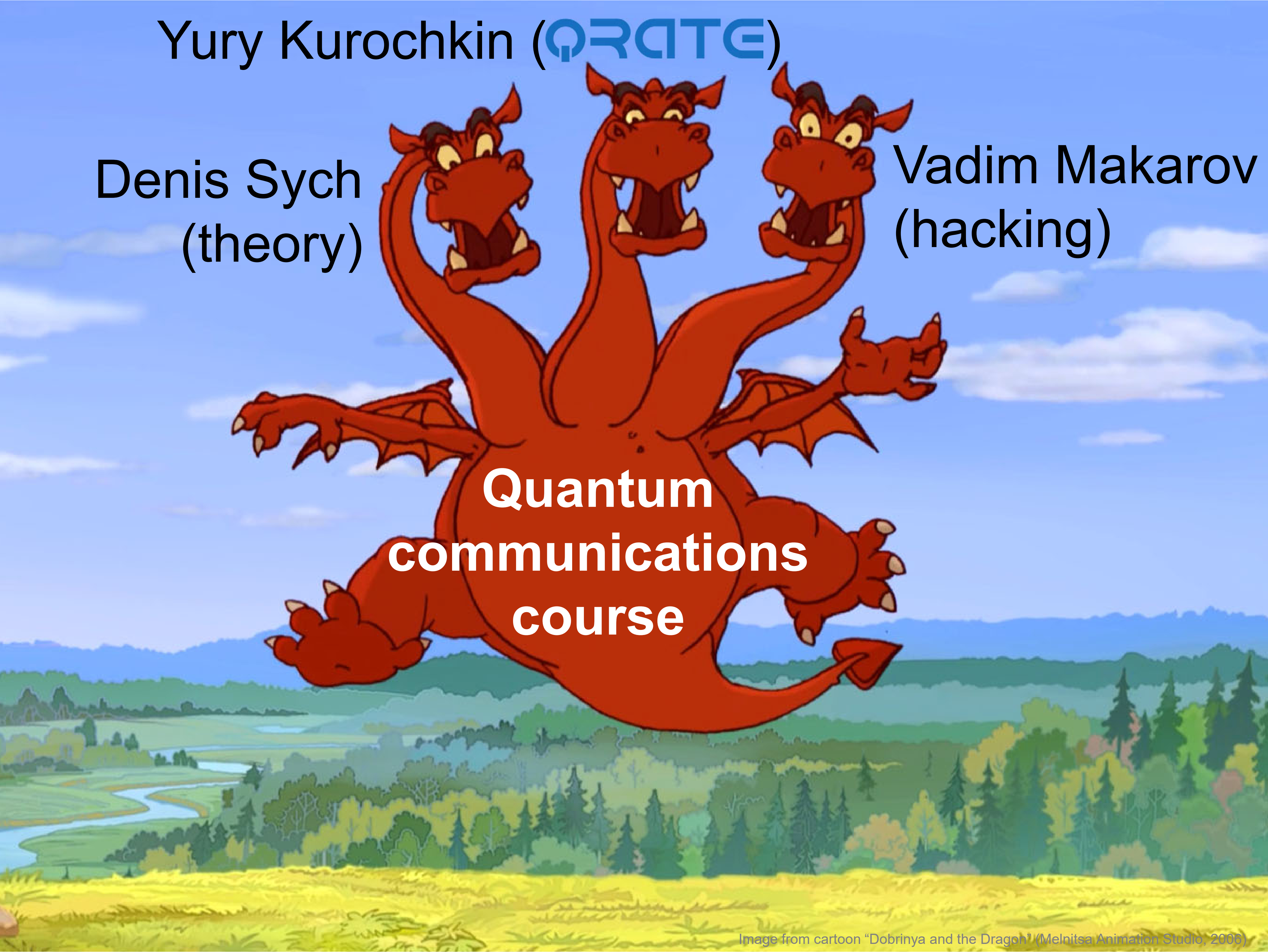
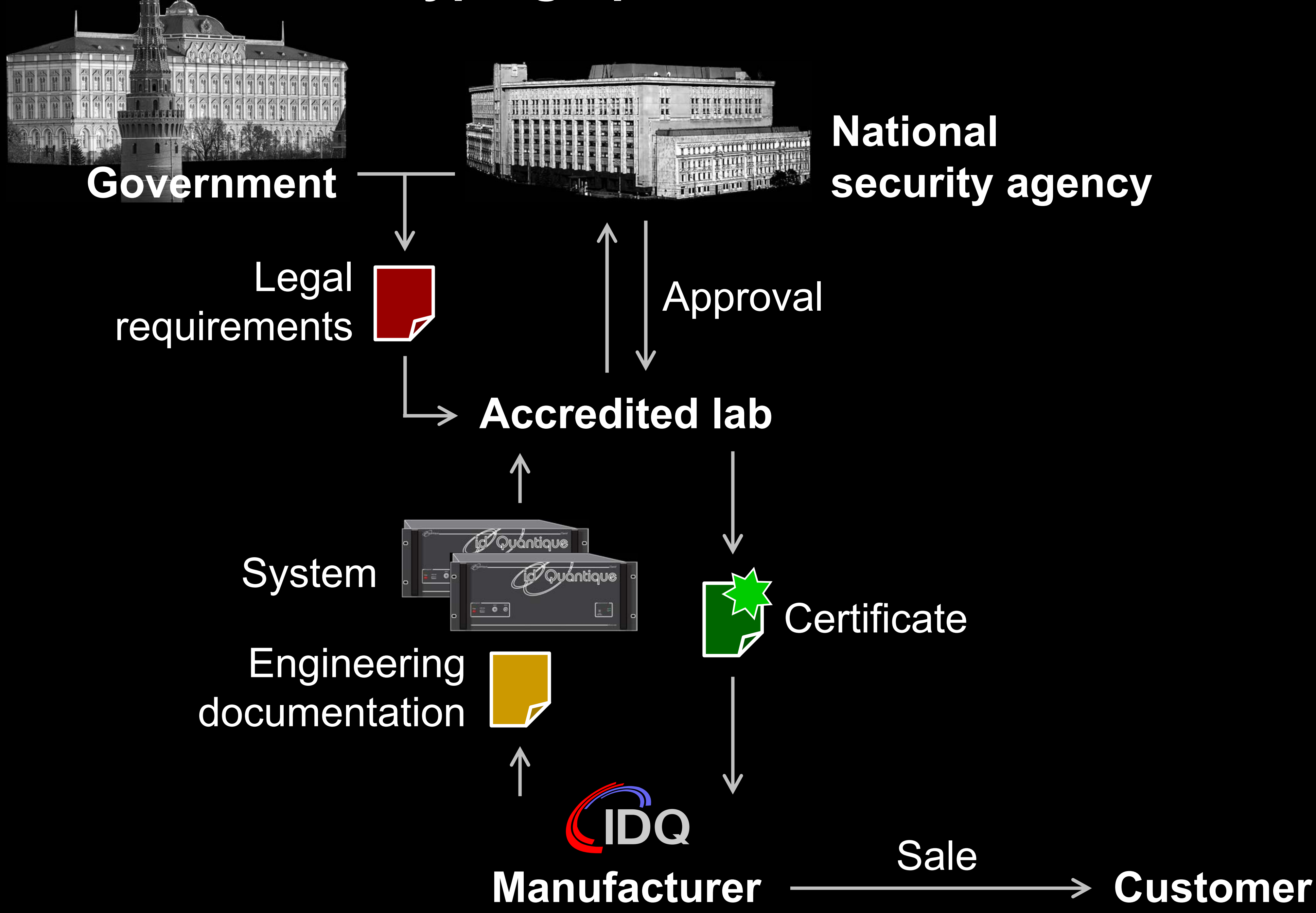
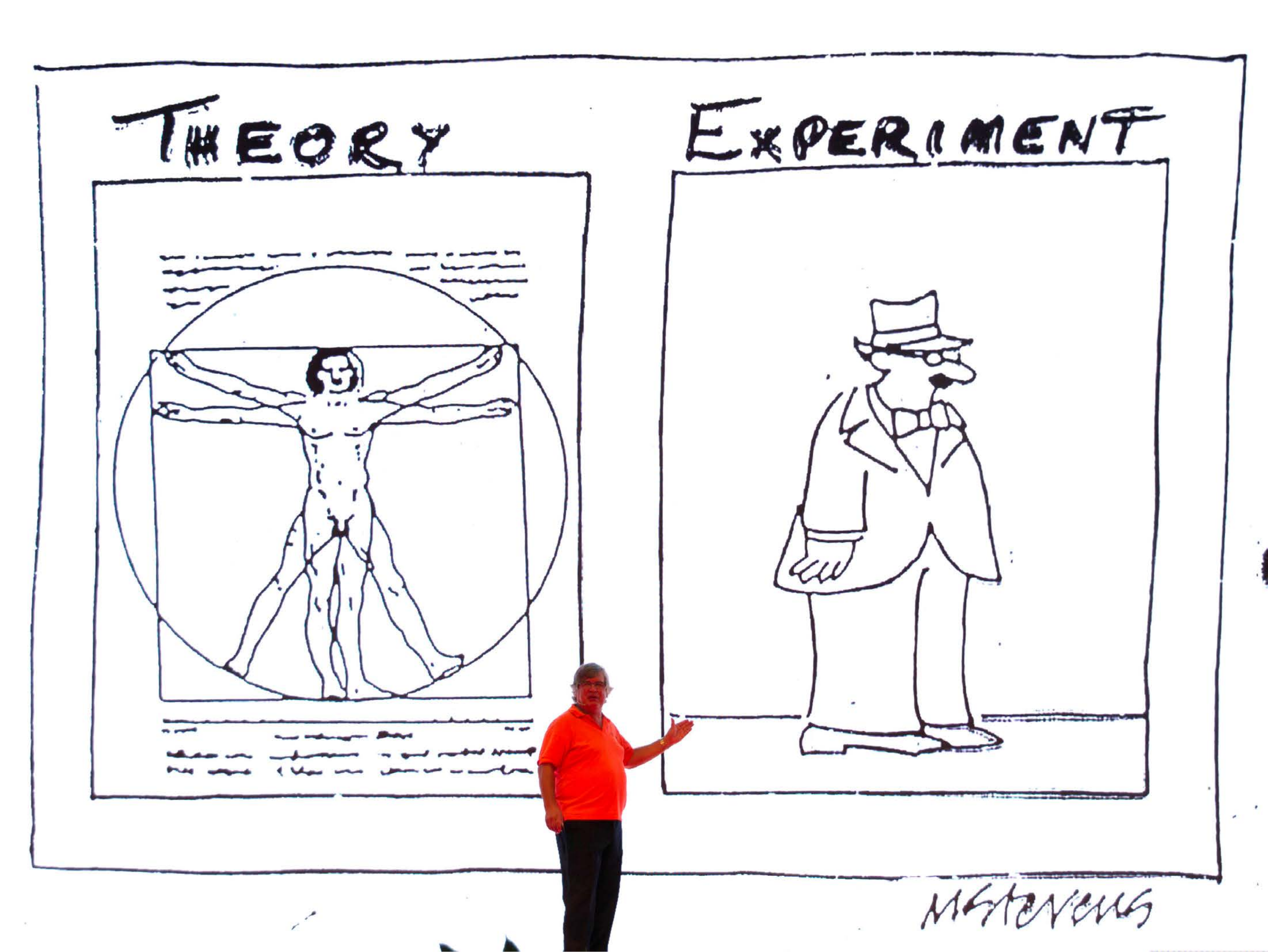


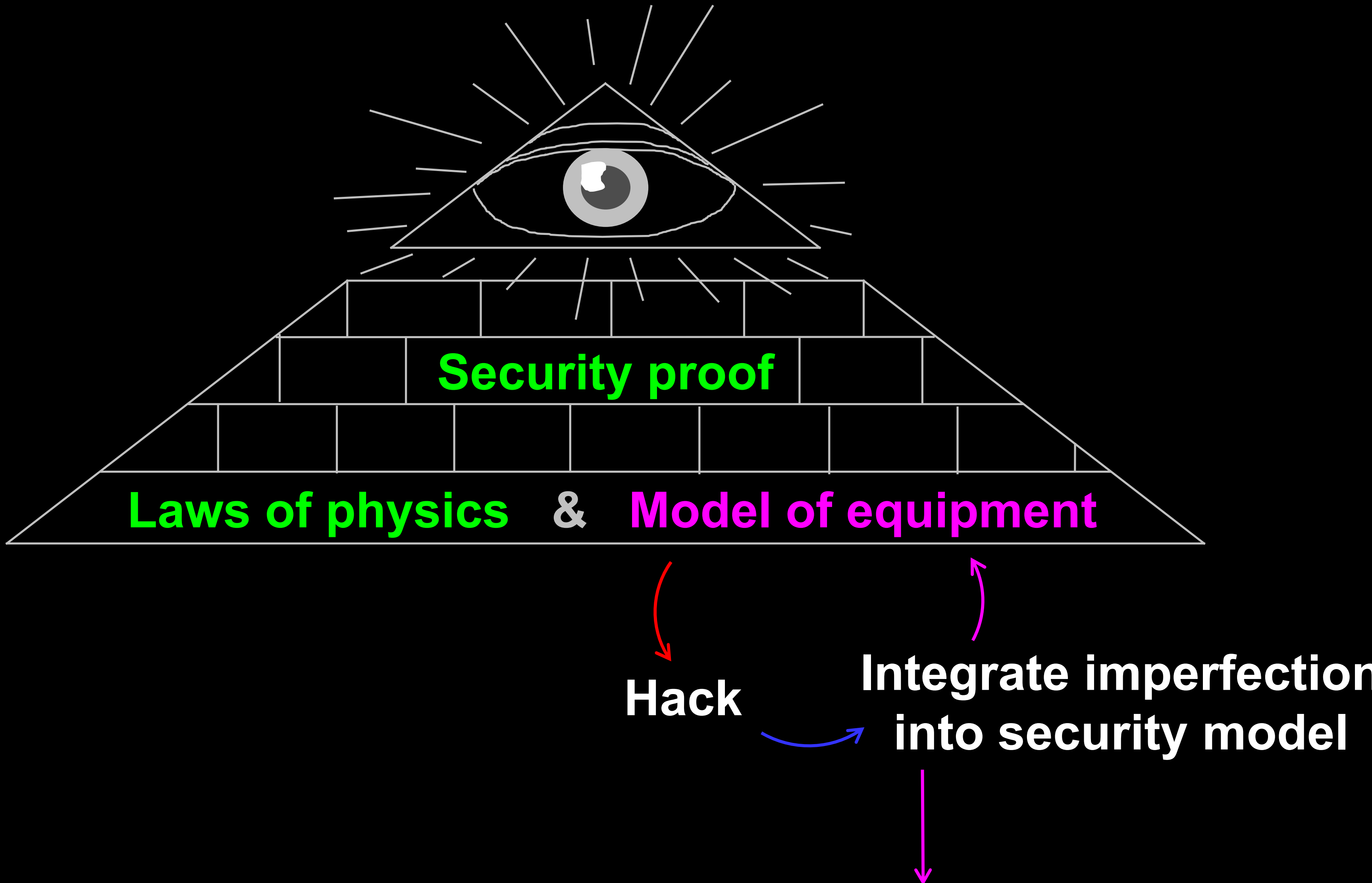
Image from cartoon “Dobrinya and the Dragon” (Melnitsa Animation Studio, 2006)

Certification of cryptographic tools




THEORY
EXPERIMENT
MStevens

Implementation security of quantum communications

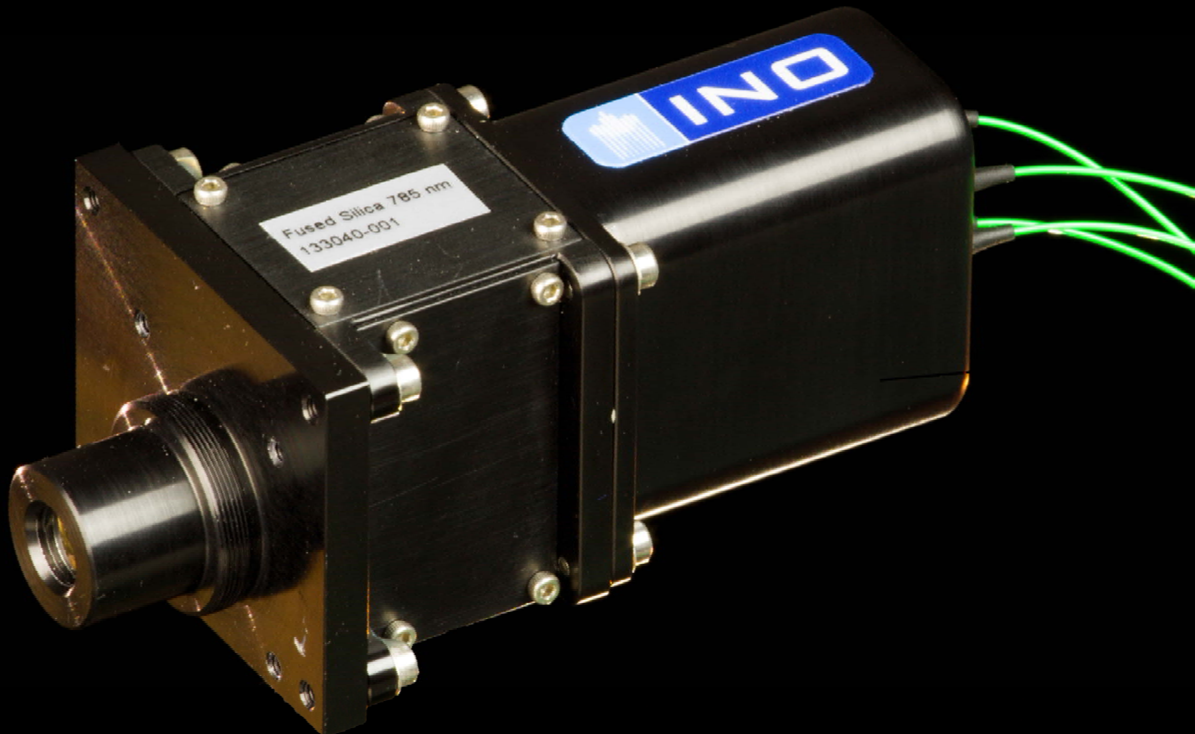


Formal certification: we need standards and labs ecosystem

Attack	Target component	Tested system
Distinguishability of decoy states A. Huang *et al.*, Phys. Rev. A **98**, 012330 (2018)	laser in Alice	3 research systems
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); A. Huang *et al.*, poster at QCrypt (2018)	any	5 commercial & 1 research systems
Spatial efficiency mismatch 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 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.*, Sci. Rep. **7**, 8403 (2017)	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 systems

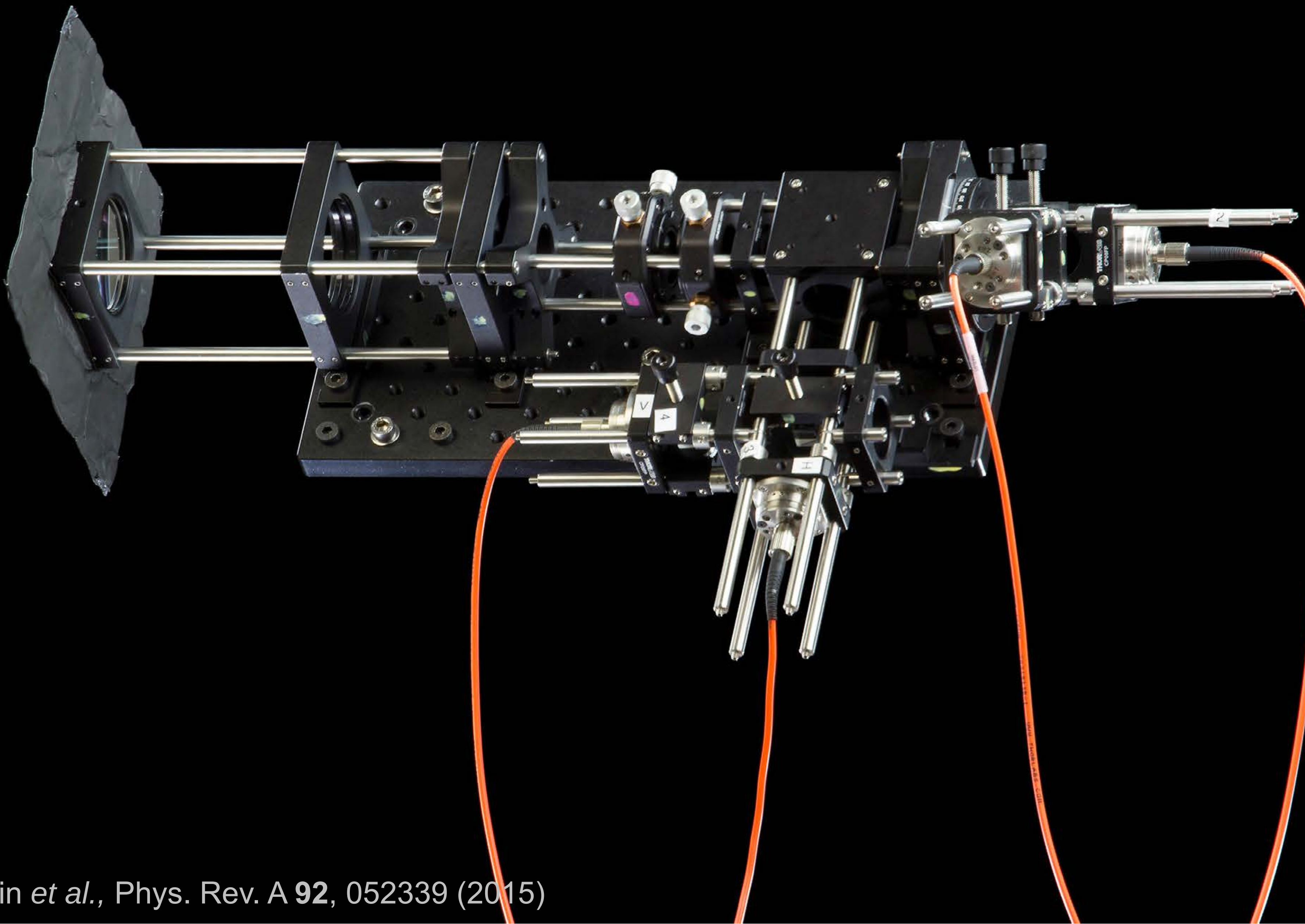

Anqi Huang tests countermeasure in Clavis2

Polarization receiver for satellite



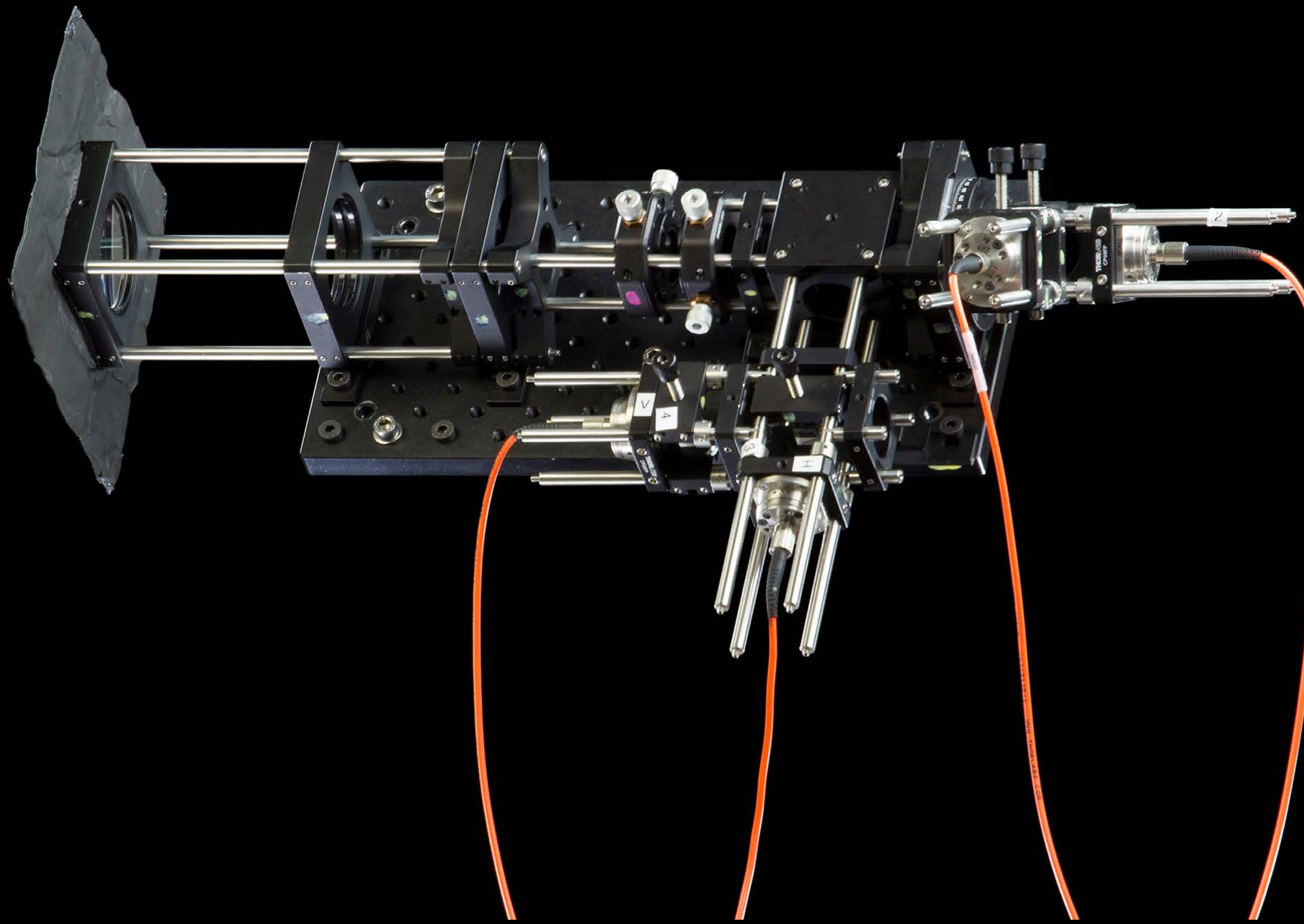
C. J. Pugh *et al.,* Quantum Sci. Technol. **2**, 024009 (2017)

Polarization analyzer



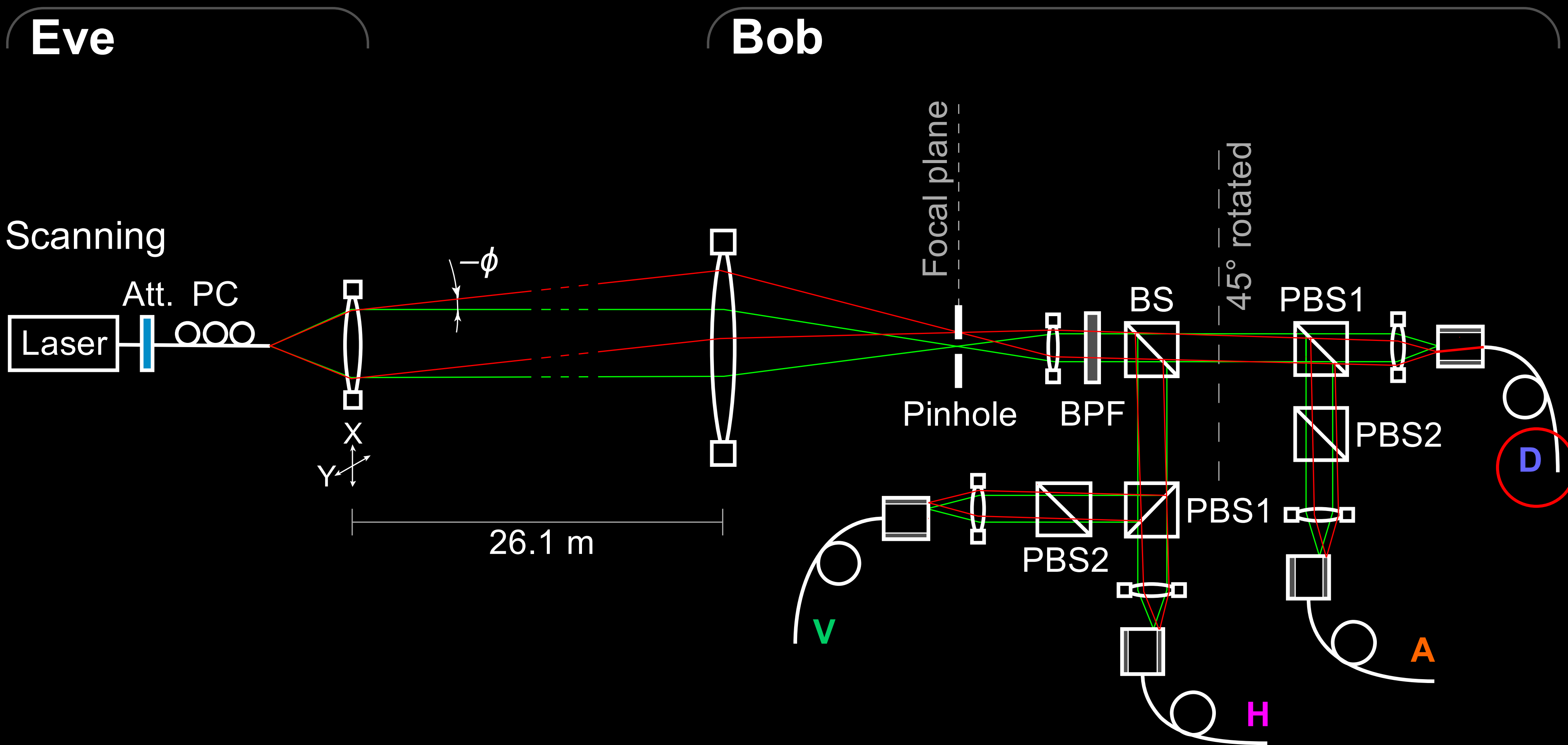
J.-P. Bourgoin *et al.,* Phys. Rev. A **92**, 052339 (2015)

Polarization analyzer



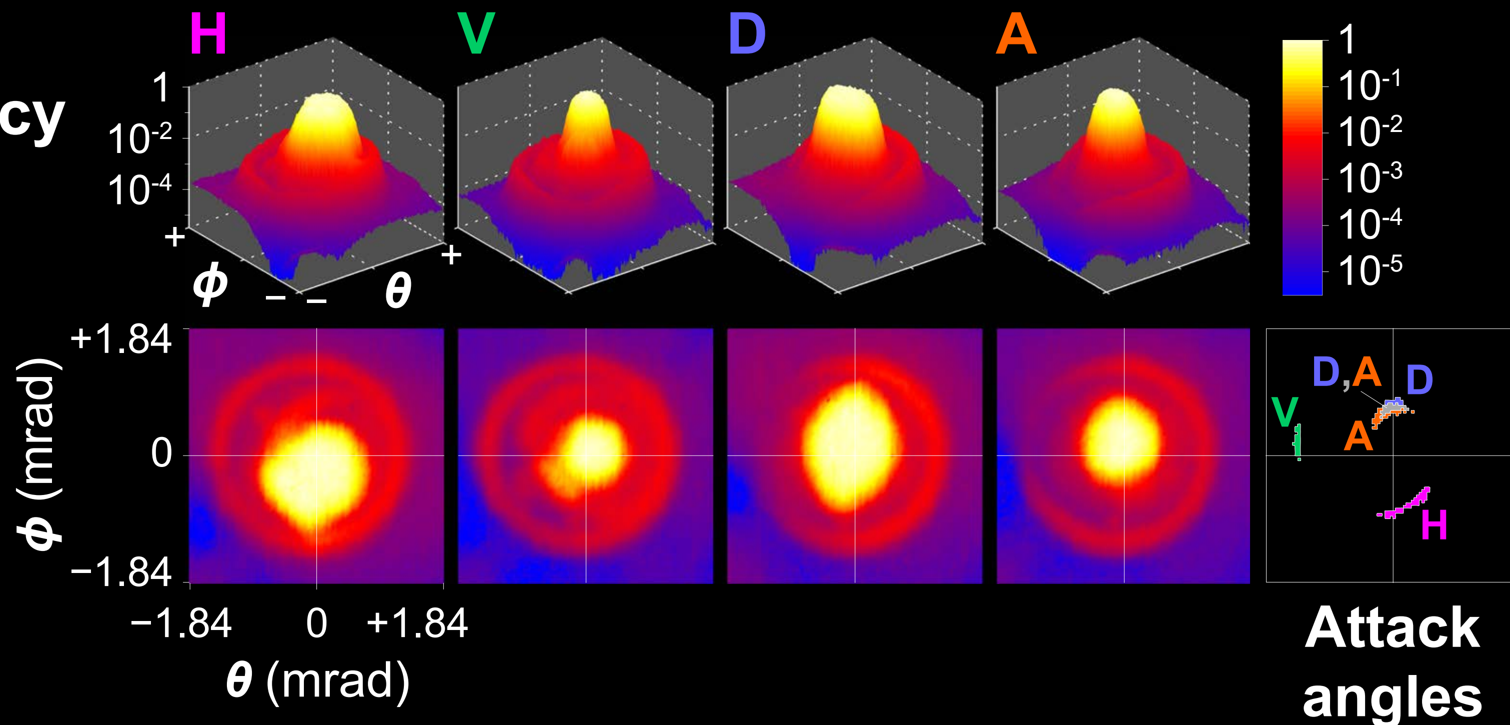
J.-P. Bourgoin *et al.*, Phys. Rev. A **92**, 052339 (2015)

Efficiency mismatch in polarization analyzer

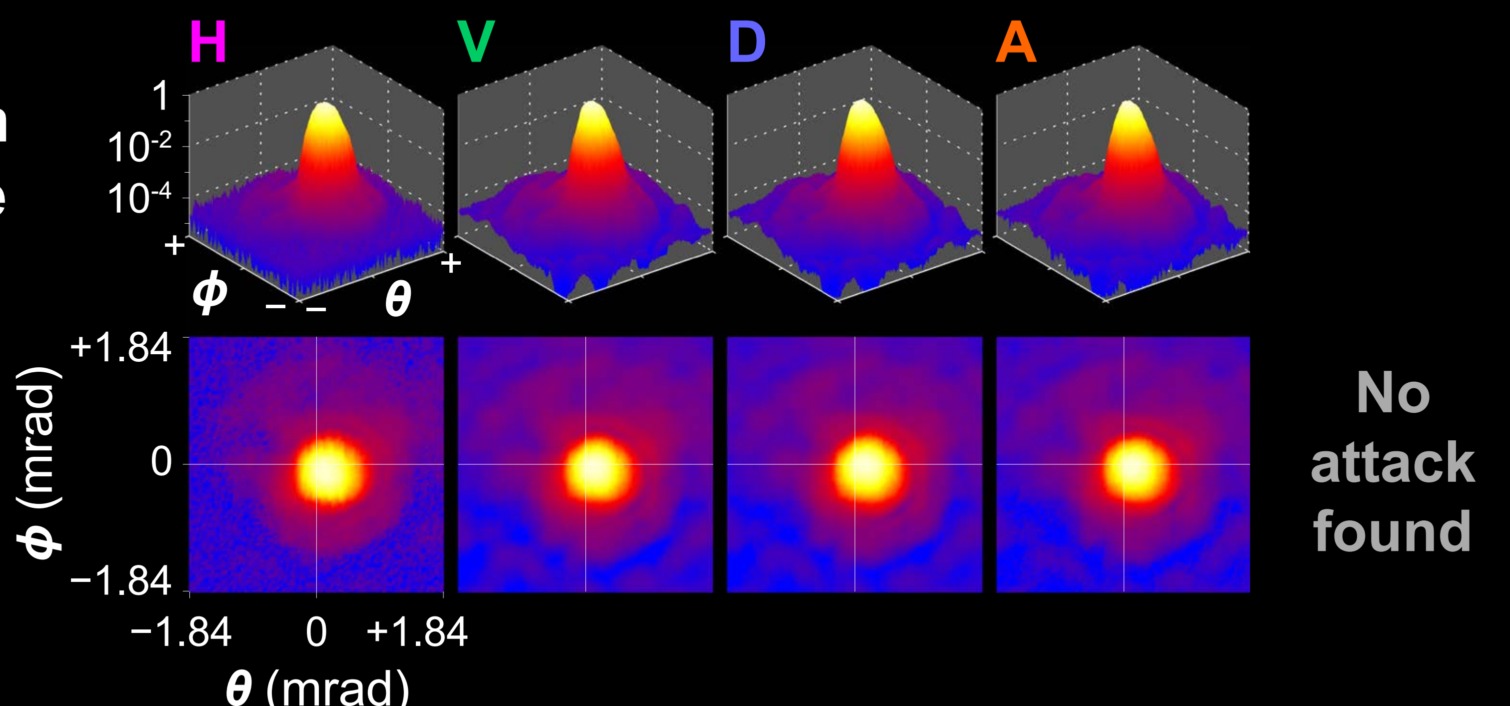


S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015)

Detector efficiency without pinhole

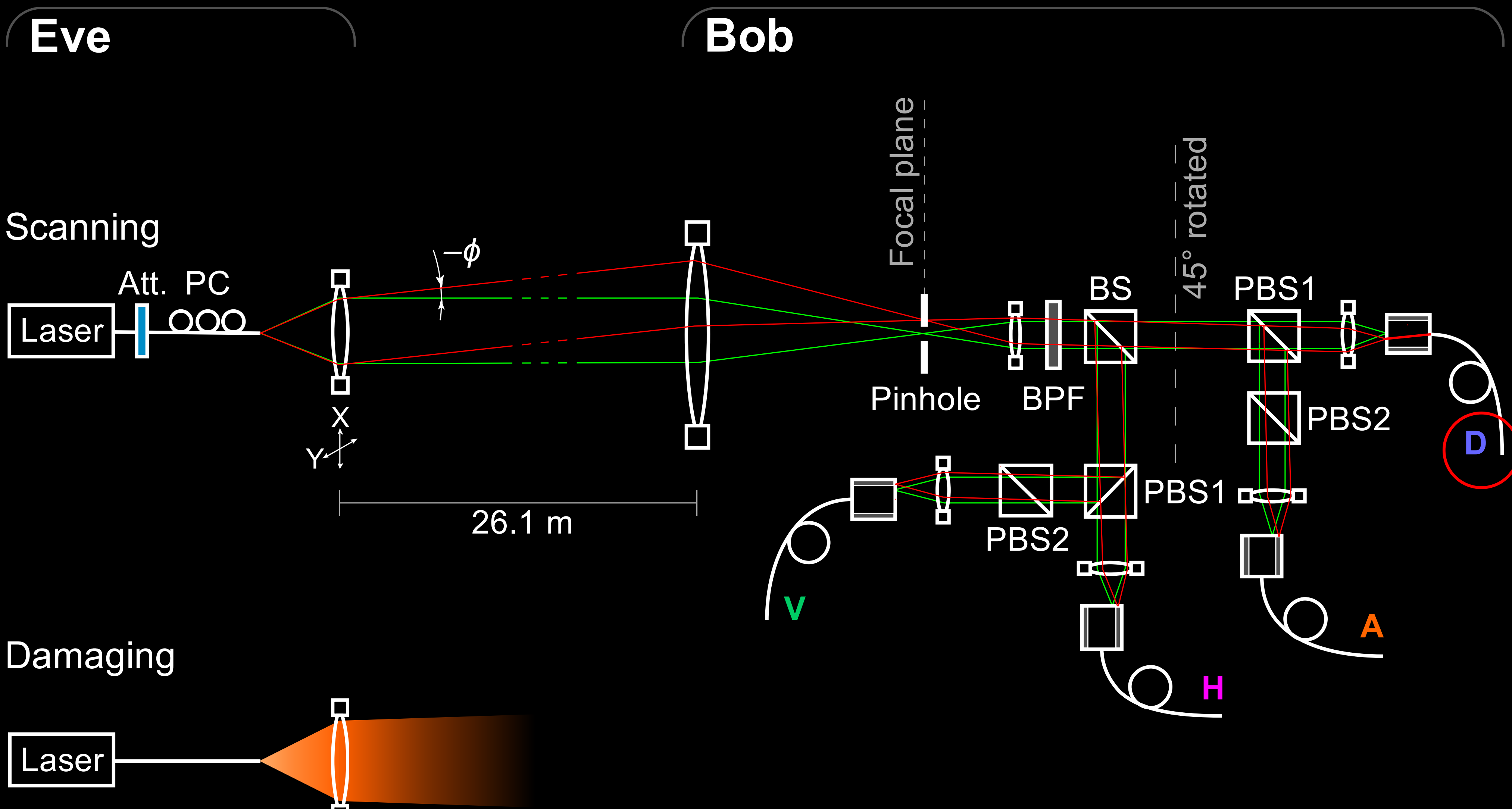


...and with 25 µm diameter pinhole

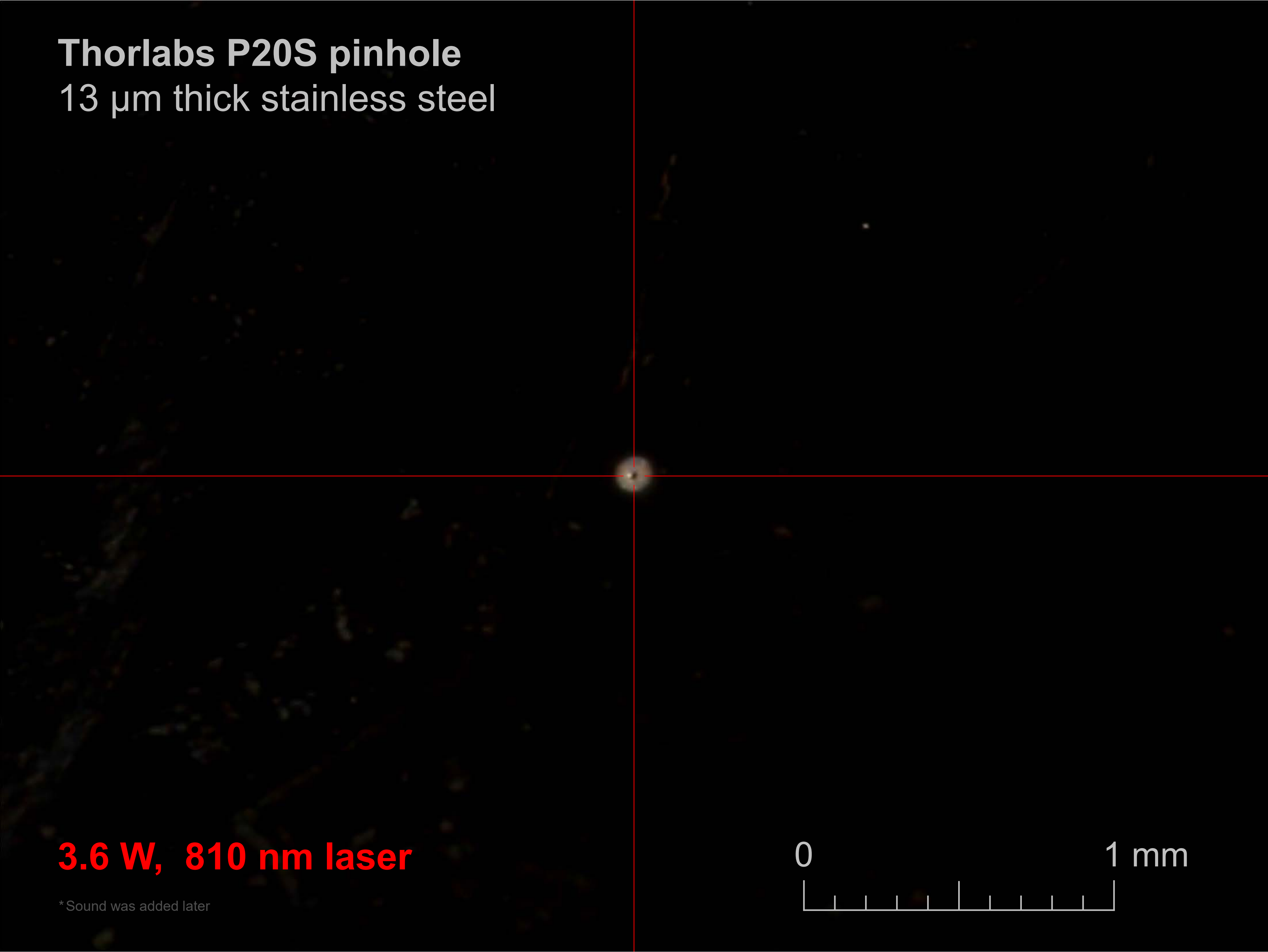


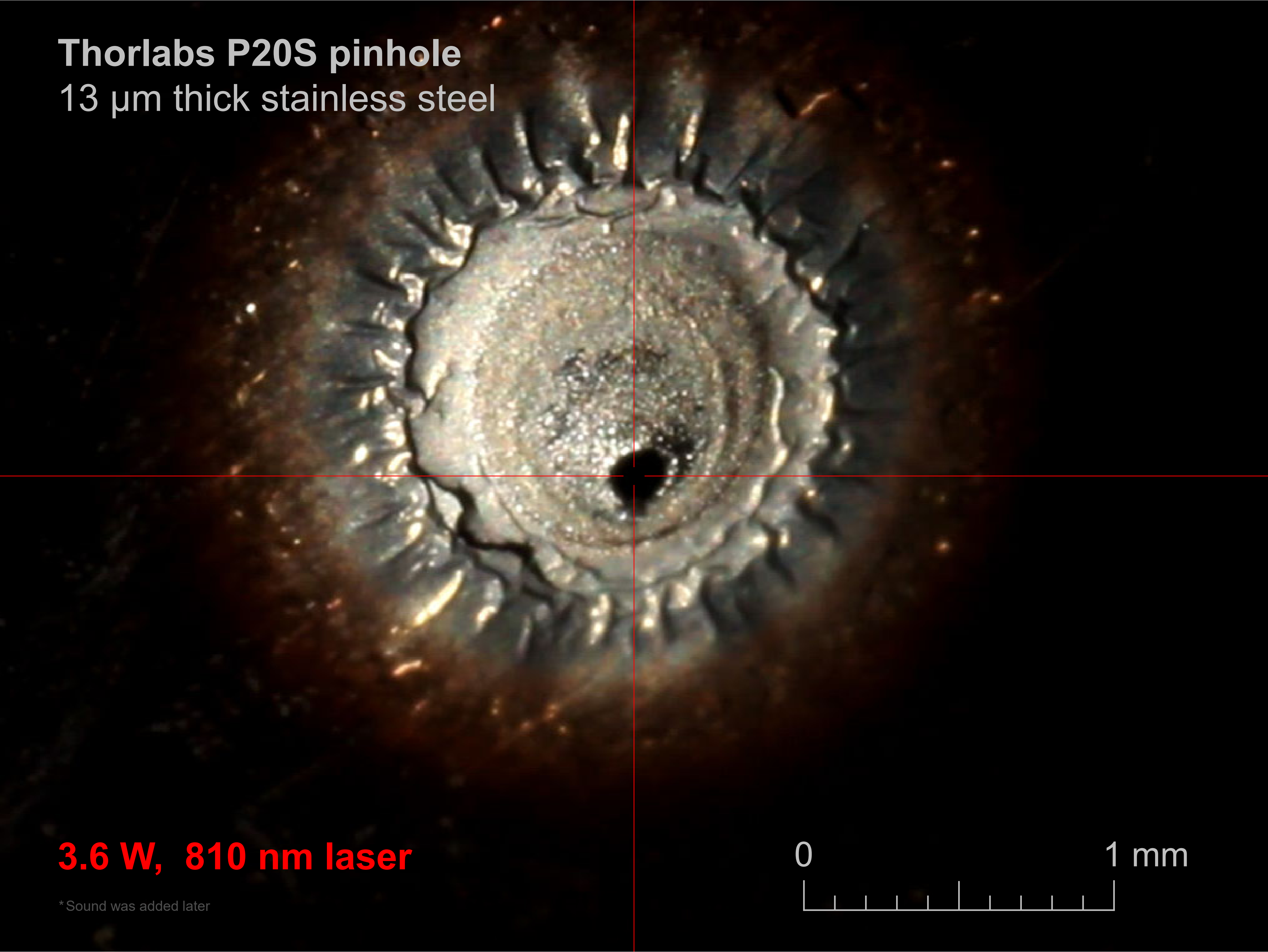
S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015)

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	System	Report	Tests
IDQ		2016	–2018 interrupted
国盾量子 QuantumCTek		2016, 2018–19	ongoing
ITMO UNIVERSITY (ООО Квантовые коммуникации)	Subcarrier scheme	2018	ongoing
QRATE	New 312.5 MHz system	(2020)	ongoing

S. Sajeed *et al.*, arXiv:1909.07898

Certification standards are being drafted since 2019 in

ETSI Industry standards group in QKD

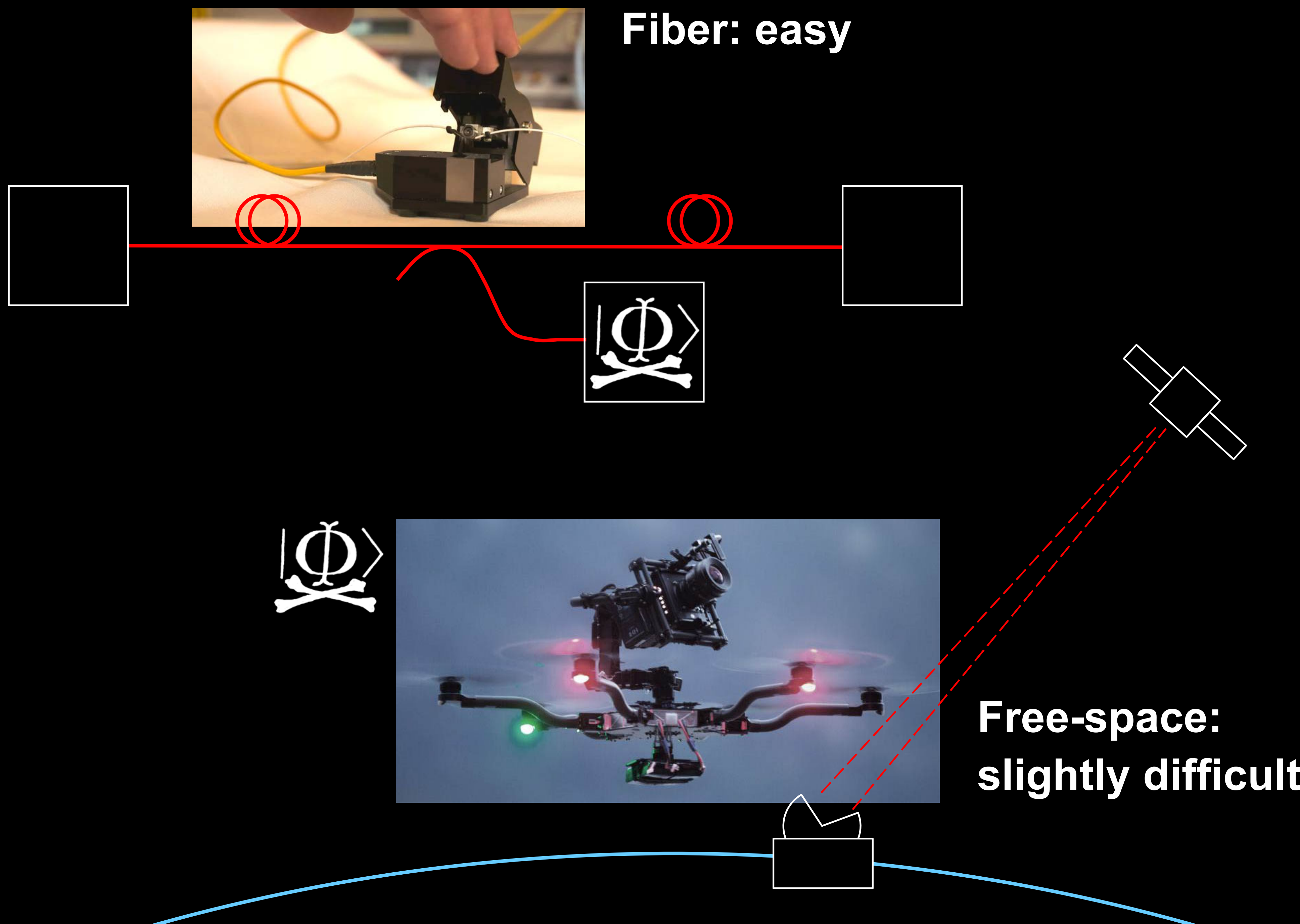
ISO

Example of initial analysis report

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

Attacks require realtime physical access to channel



RQC MISIS Quantum hacking lab vad1.com/lab