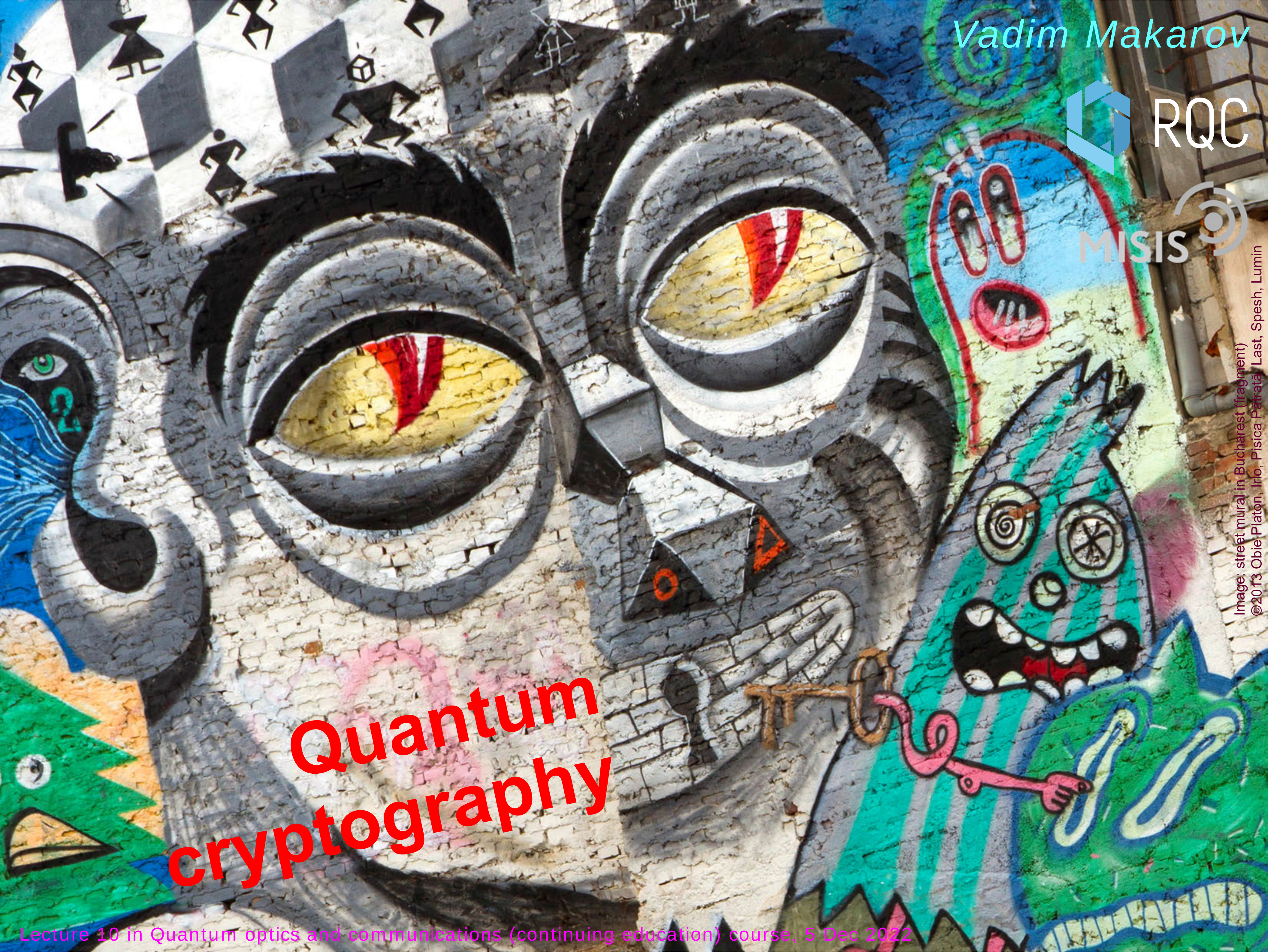


Vadim Makarov

Quantum cryptography

Image: street mural in Bucharest (fragment)
©2013 Obie Platon, Irlo, Pisica Pătrată, Last, Spesh, Lumin

Lecture 10 in Quantum optics and communications (continuing education) course, 5 Dec 2022

Communication security you enjoy daily

Paying by credit card in a supermarket

Cell phone conversations, SMS

Email, chat, online calls

Secure browsing, shopping online, content delivery

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

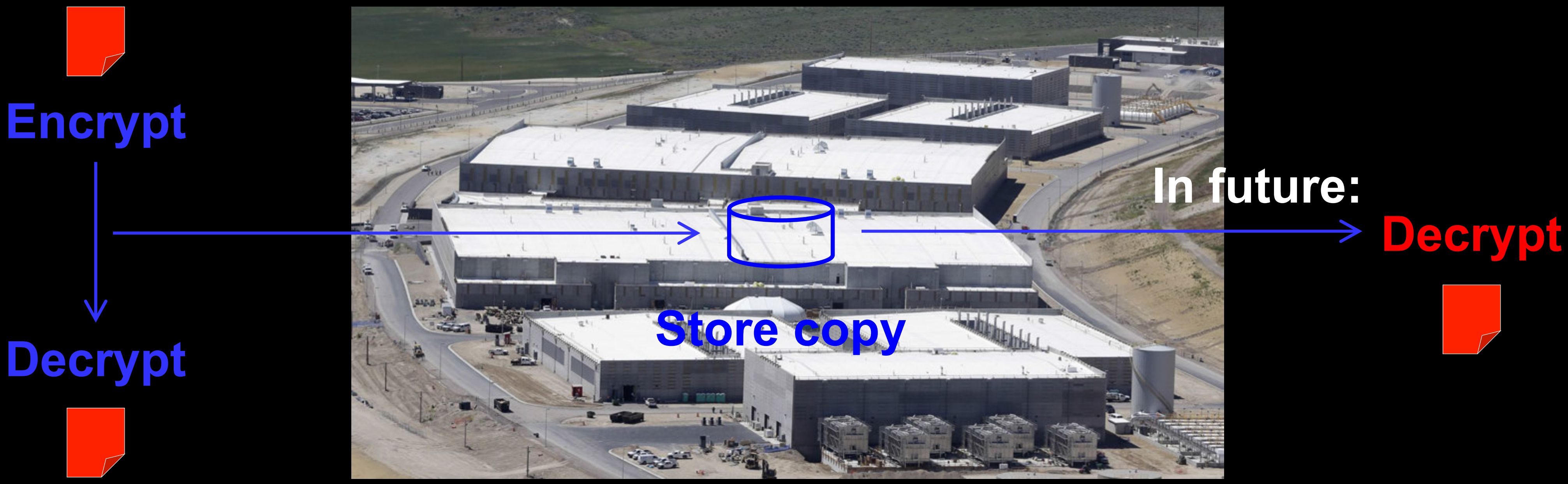
Bypassing government surveillance and censorship

CCTV, industrial automation, military, spies...

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



Encrypt

Decrypt

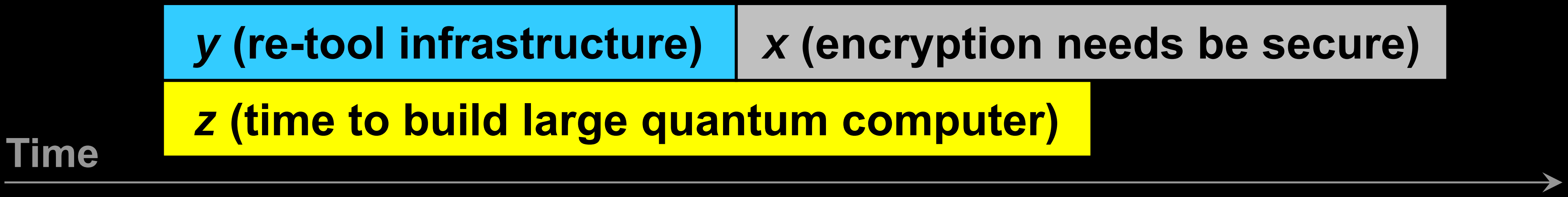
Store copy

In future:

Decrypt

Photo ©2013 AP / Rick Bowmer

Mosca theorem



y (re-tool infrastructure)

x (encryption needs be secure)

z (time to build large quantum computer)

Time

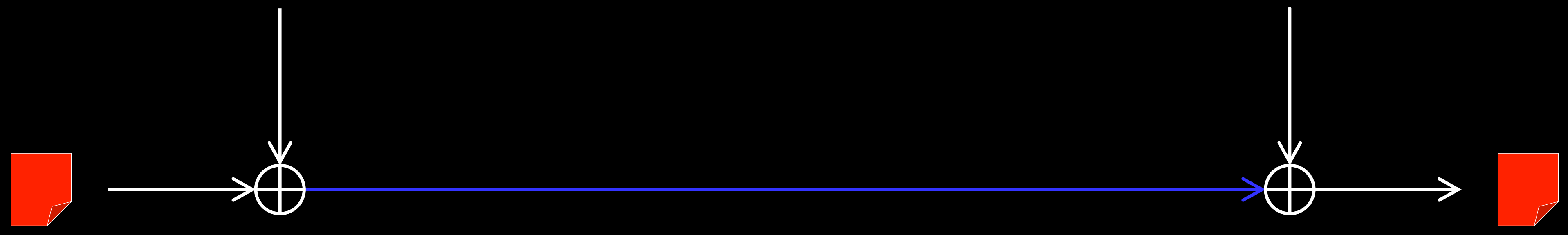
If $x + y > z$, then worry.

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	$\alpha \oplus \beta$
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

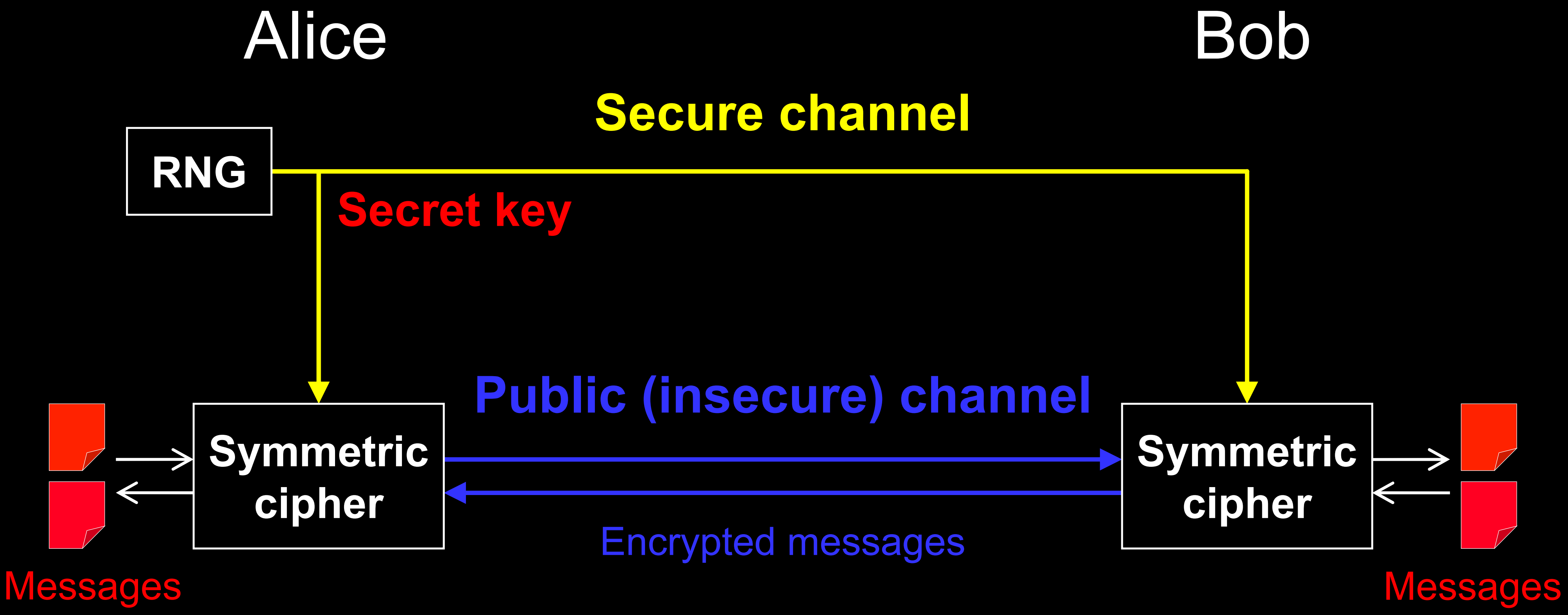
		Broken?
Monoalphabetic cipher	invented ~50 BC (J. Caesar)	~850 (Al-Kindi)
Nomenclators (code books)	~1400 – ~1800	✓
Polyalphabetic (Vigenère)	1553 – ~1900	1863 (F. W. Kasiski)
…		
One-time pad	invented 1918 (G. Vernam)	**impossible** (C. Shannon 1949)
Polyalphabetic electromechanical (Enigma, Purple, 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	**?**

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

Quantum communication primitives

Money	S. Wiesner, unpublished circa 1970, Sigact News **15**, 78 (1983); S. Aaronson, P. Christiano, Proc. STOC'12, 41 (2012)
Key distribution	idquantique.com, quantum-info.com, qasky.com, goqrate.com
Secret sharing	W. P. Grice *et al.*, Opt. Express **23**, 7300 (2015).
Digital signatures	R. Collins *et al.*, Phys. Rev. Lett. **113**, 040502 (2014)
Superdense coding	C. H. Bennett, S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992)
Fingerprinting	J.-Y. Guan *et al.*, Phys. Rev. Lett. **116**, 240502 (2016)
Oblivious transfer	C. Erven *et al.*, Nat. Commun. **5**, 3418 (2014)
Bit commitment	T. Lunghi *et al.*, Phys. Rev. Lett. **111**, 180504 (2013)
Coin-tossing	A. Pappa *et al.*, Nat. Commun. **5**, 3717 (2014)
Cloud computing	S. Barz *et al.*, Science **335**, 303 (2012)
Software leasing	A. Broadbent *et al.*, Lect. Notes Comp. Sci. **13042**, 90 (2021)
Bitcoin	J. Jogenfors, Proc. IEEE ICBC 2019, 245 (2019)
Bell inequality testing	B. Hensen *et al.*, Nature **526**, 682 (2015)
Teleportation	X.-S. Ma *et al.*, Nature **489**, 269 (2012)
Entanglement swapping	M. Żukowski *et al.*, Phys. Rev. Lett. **71**, 4287 (1993)
Interaction-free measurement	A. C. Elitzur, L. Vaidman, Found. Phys. **23**, 987 (1993)
Random number generators	idquantique.com, picoquant.com

Key distribution for encryption

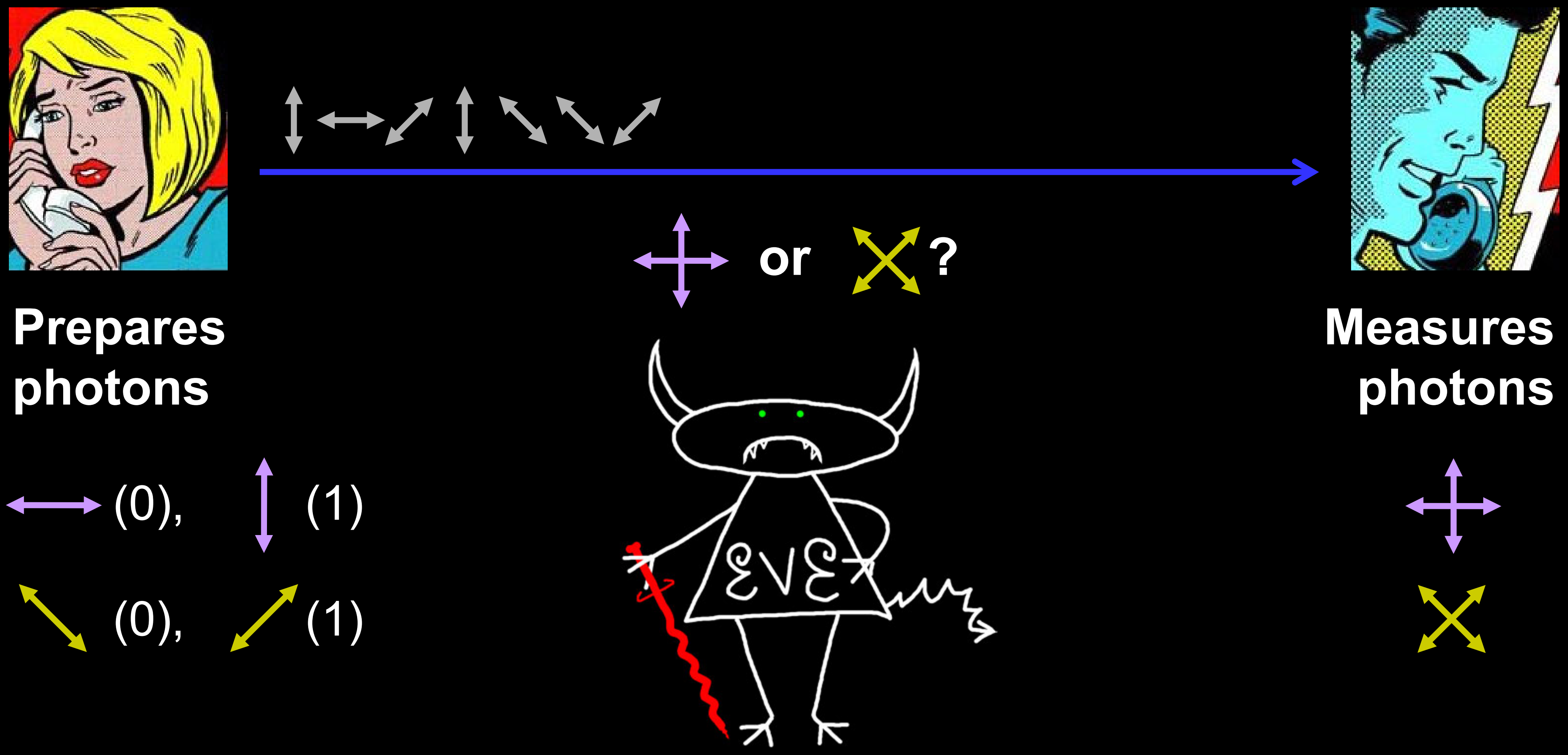


Quantum key distribution transmits secret key by sending quantum states over *open channel.*

Quantum key distribution (QKD)

Alice

Bob



Prepares photons

Measures photons

↔ (0), ↕ (1)

↘ (0), ↗ (1)

✛ or ✕ ?

Eavesdropping introduces errors

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

Post-processing in QKD

Classical channel (e.g., internet)

Alice ⟷ Bob

Raw photon detection data

↓

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

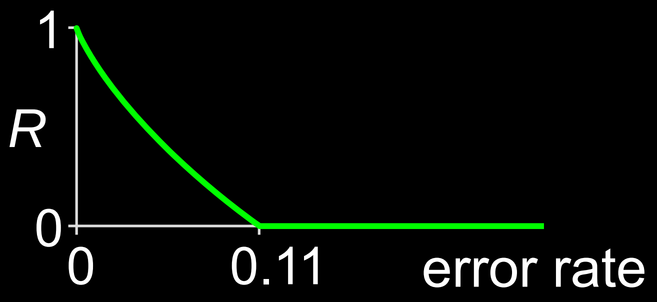
↓

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)

Dealing with errors

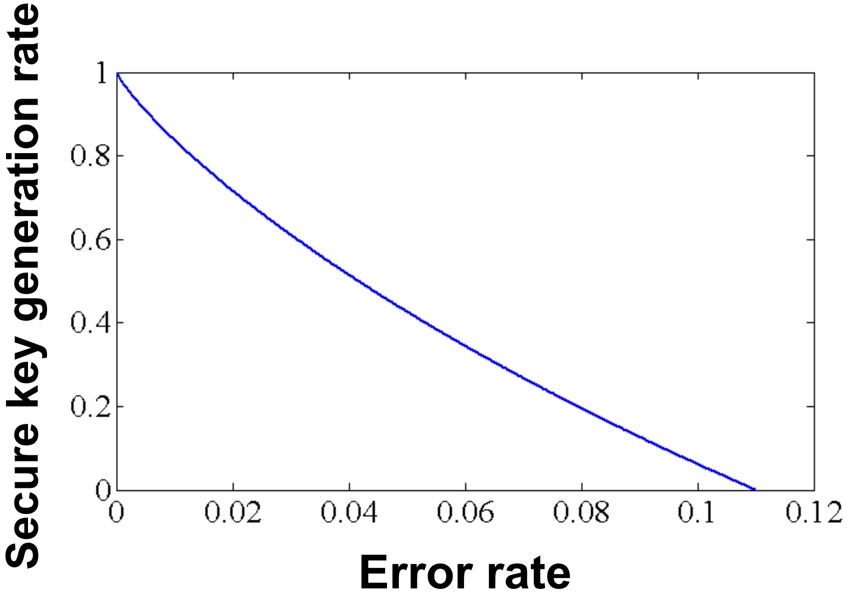
Errors due to imperfections and Eve.
Must assume that all errors are due to Eve!

- **Error correction: standard classical protocols**
- **Privacy amplification:**

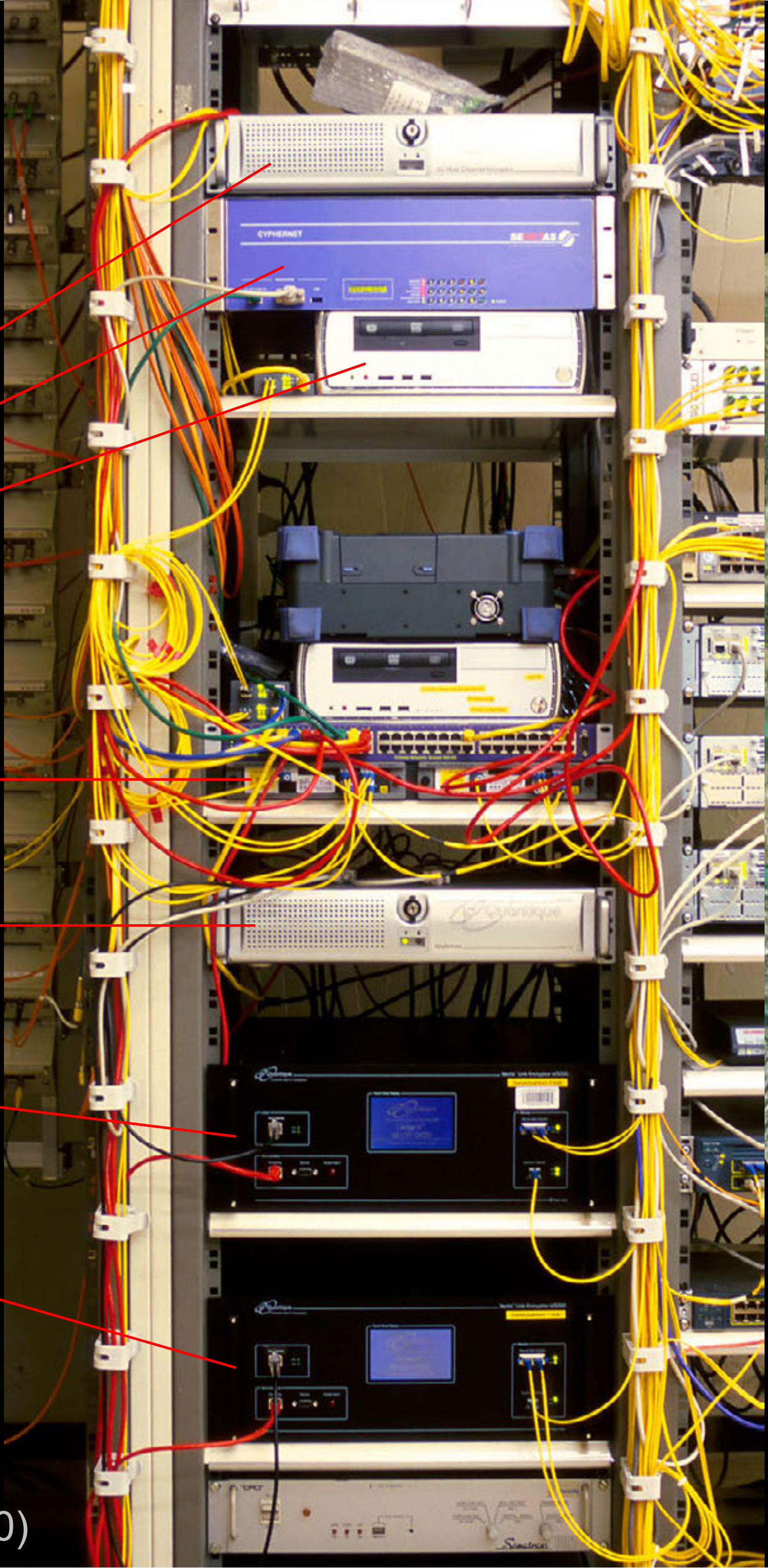
secure key **random matrix** **raw key**

$$\begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Security proof:



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)

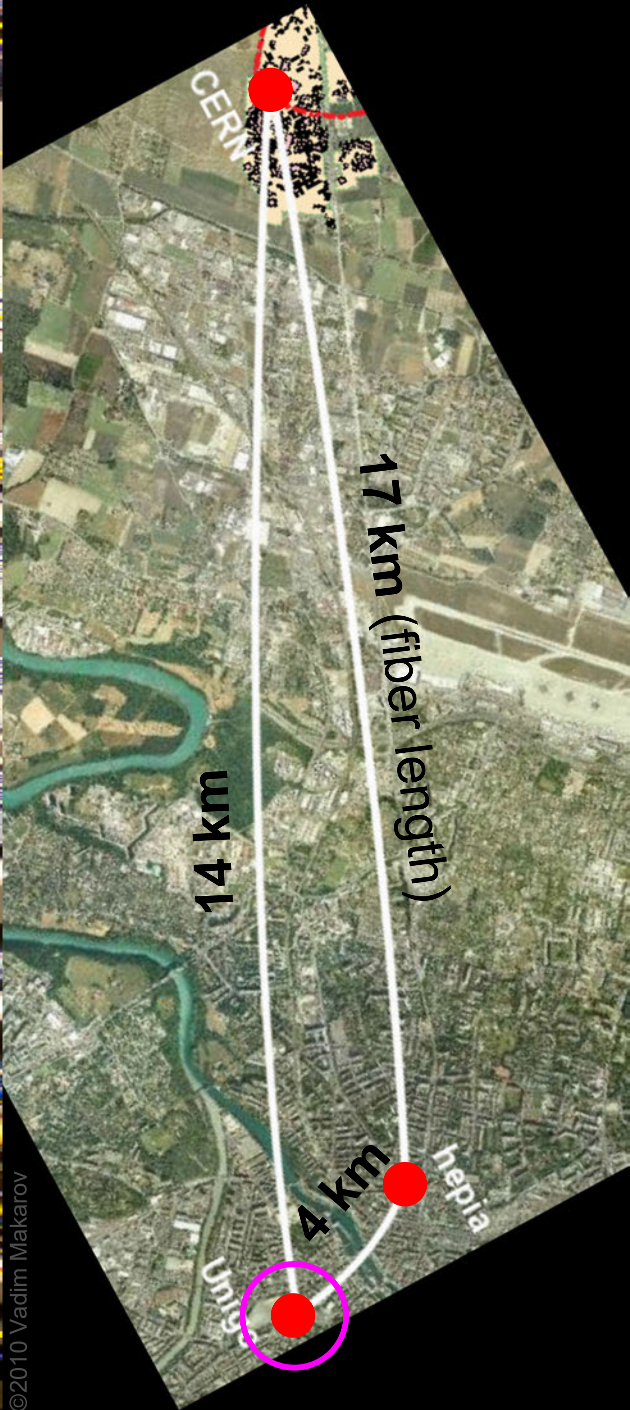
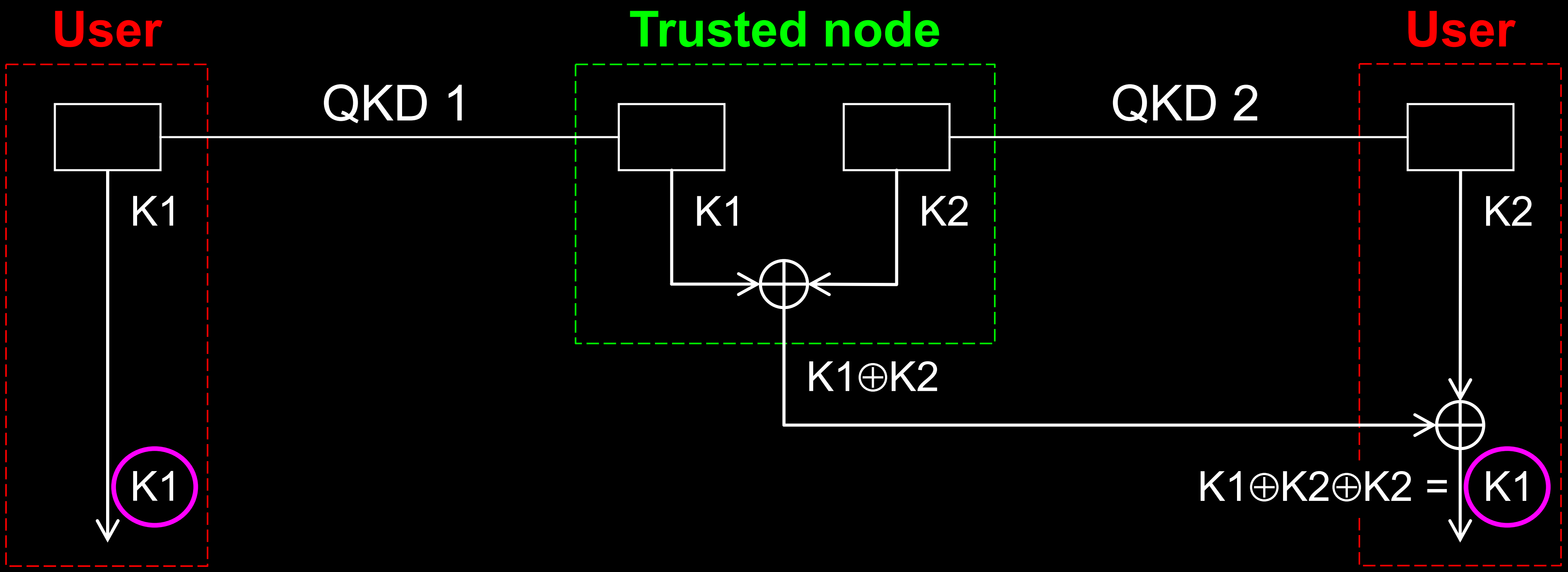


Photo ©2010 Vadim Makarov

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

Today: trusted-node repeater



User

Trusted node

User

QKD 1

QKD 2

K1

K1

K2

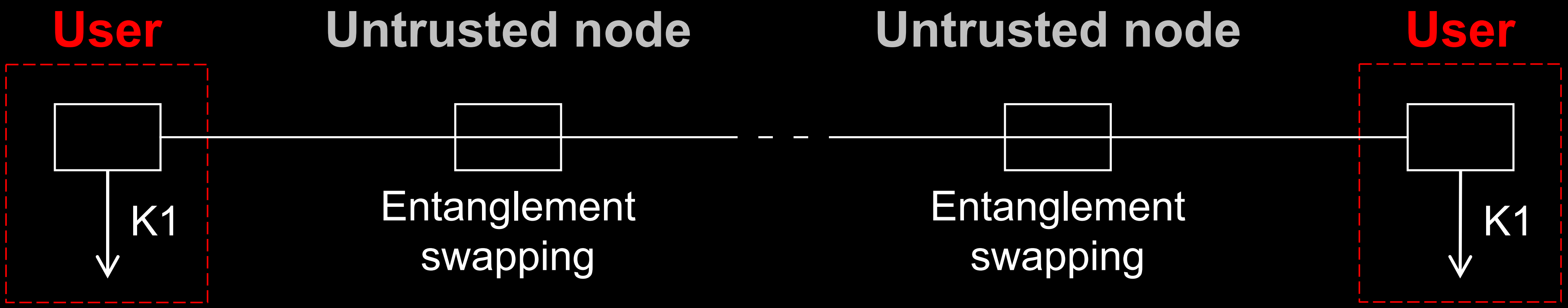
K2

K1⊕K2

K1

K1⊕K2⊕K2 = K1

Future: quantum repeater



User

Untrusted node

Untrusted node

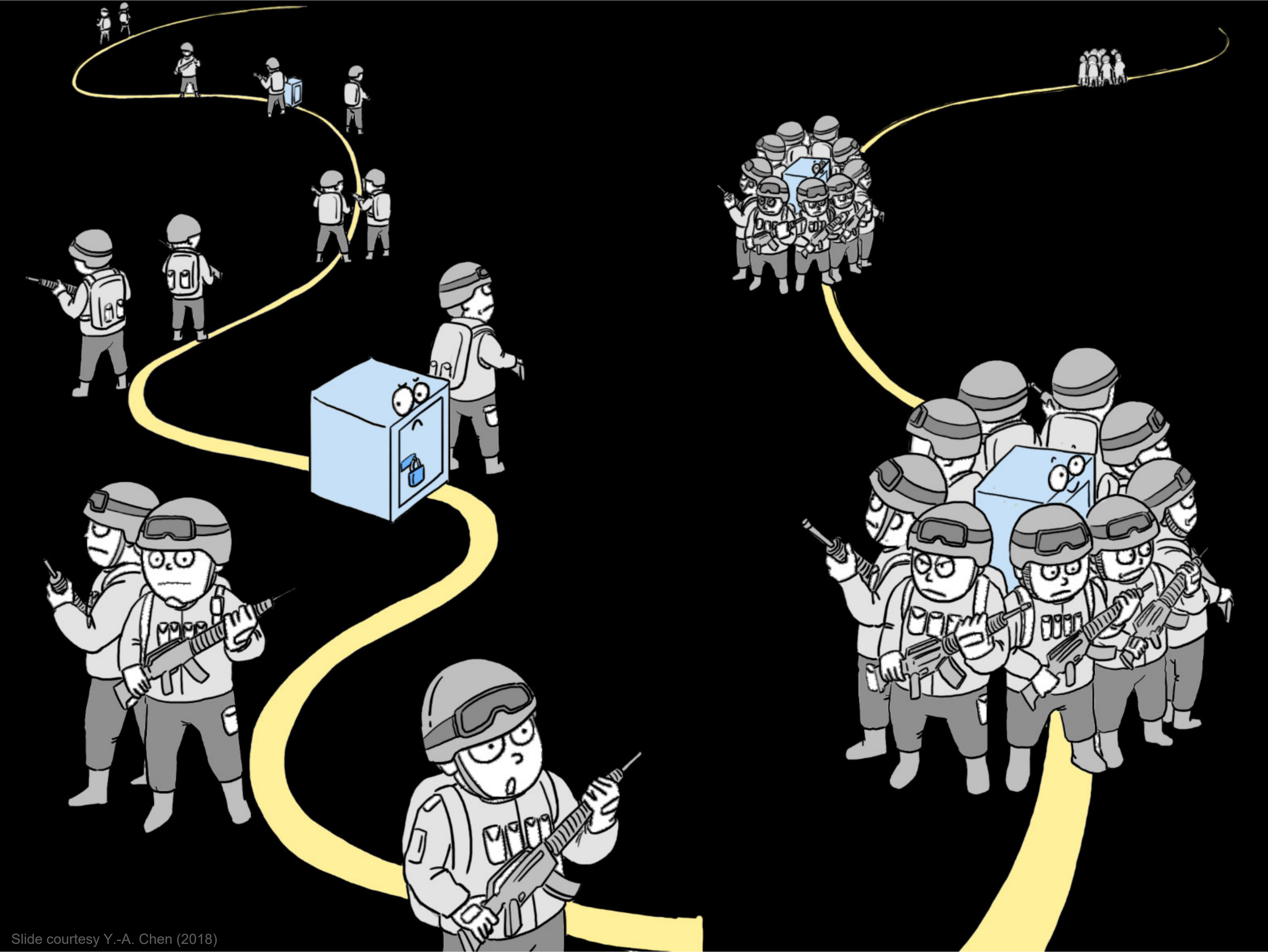
User

K1

Entanglement swapping

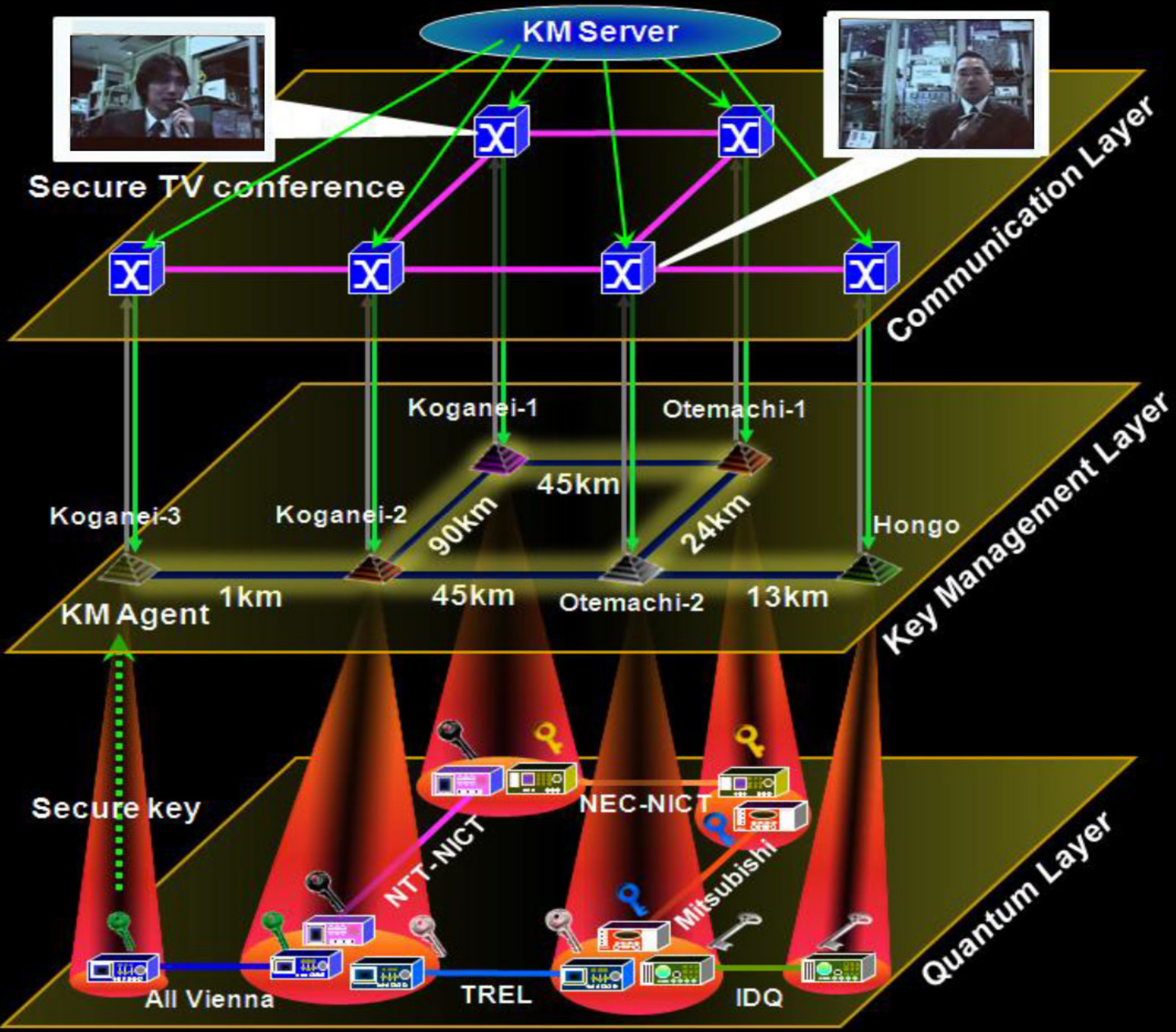
Entanglement swapping

K1



Slide courtesy Y.-A. Chen (2018)

Trusted-node network



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

Photo ©2016 Vadim Makarov

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

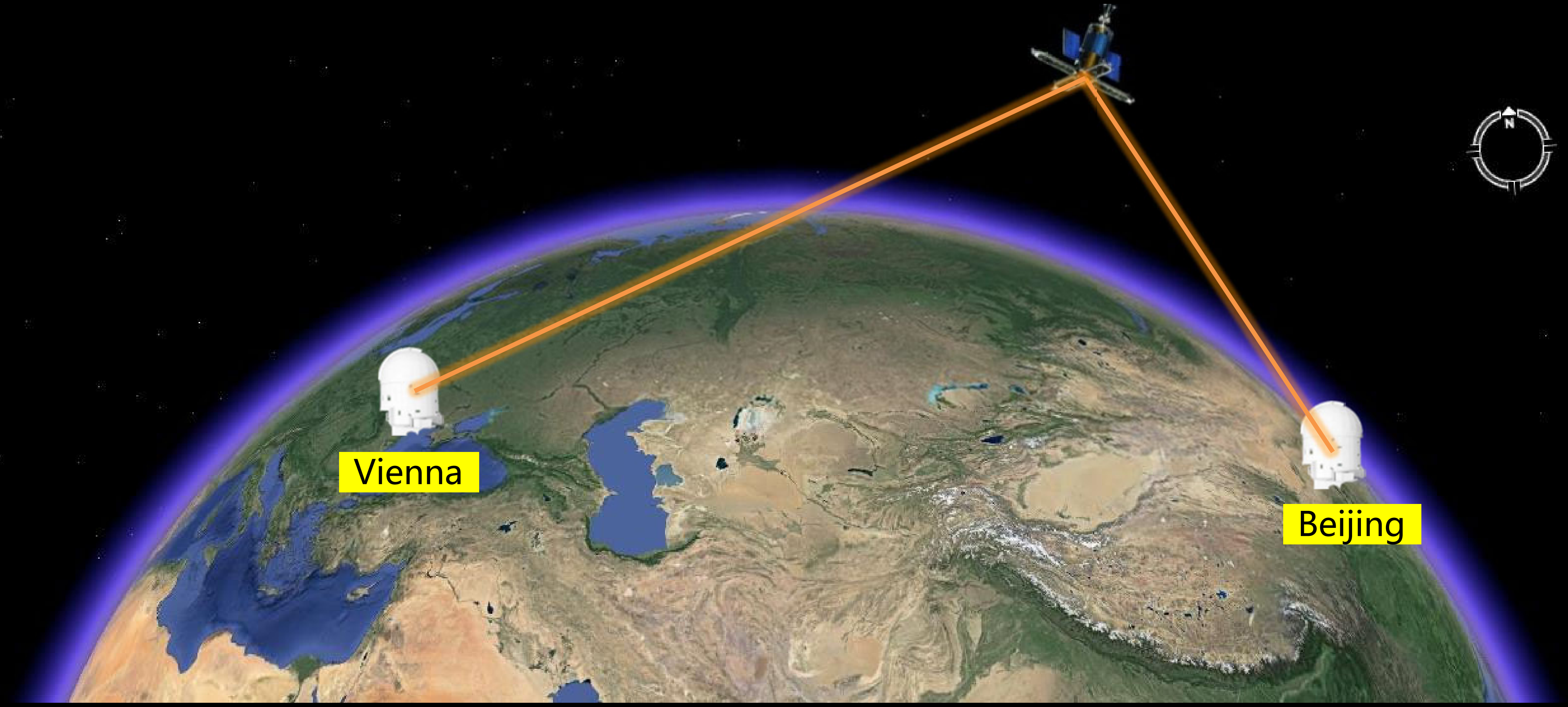
Global quantum key distribution

Video ©2012 IQC / group of T. Jennewein

Video ©2012 IQC / group of T. Jennewein

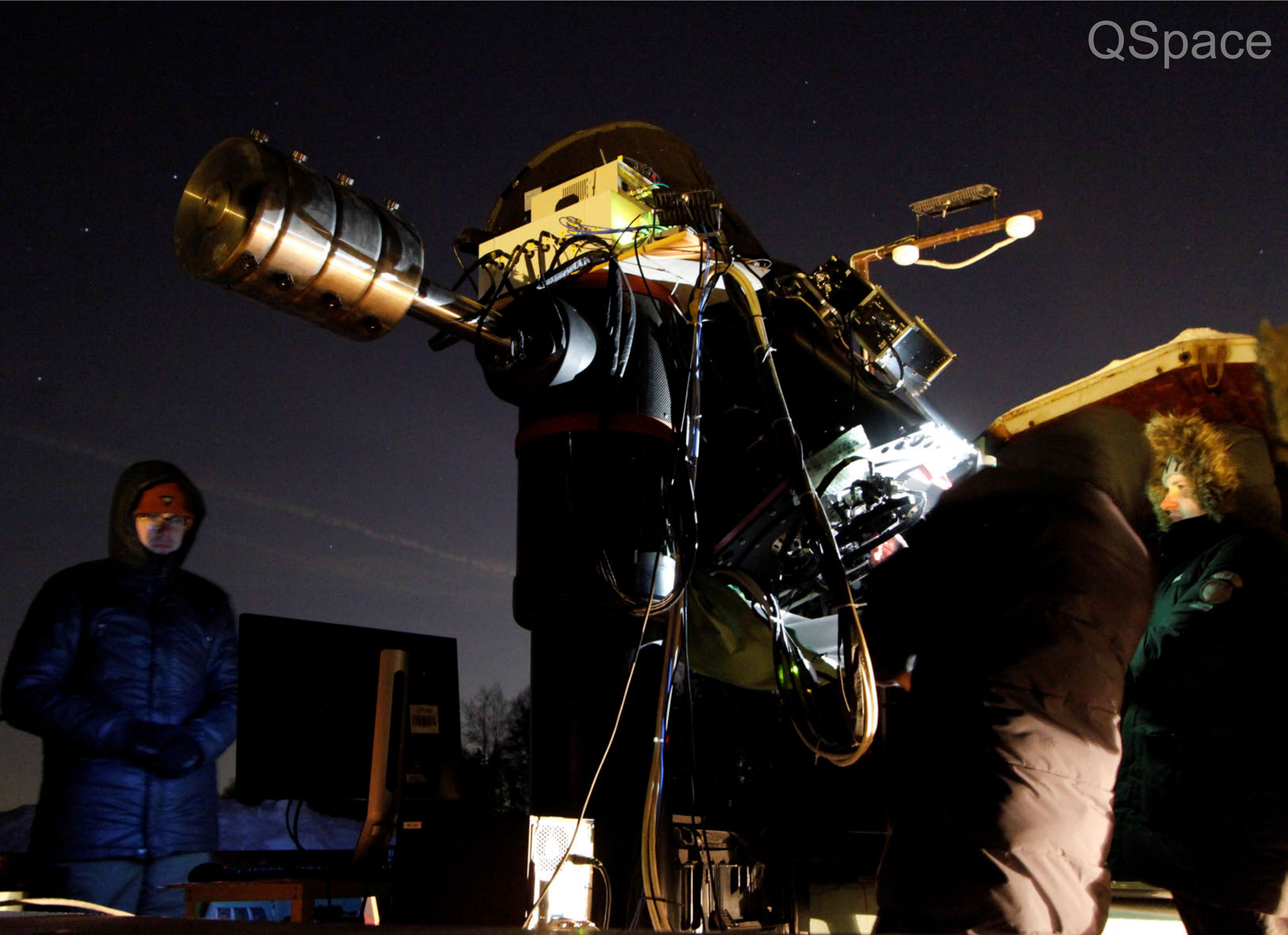
CAS Strategic Priority Research Program: Quantum Satellite

- Intercontinental quantum key distribution



Slide presented by Jian-Wei Pan at TyQI conference, Shanghai, June 27–30, 2016

Review of results: C.-W. Lu, Y. Cao, C.-Z. Peng, J.-W. Pan, Rev. Mod. Phys. **94**, 035001 (2022)



Ground station in Zvenigorod communicates with Micius satellite (18 Jan 2021)

Photo ©2021 Vadim Makarov / RQC

QSpace

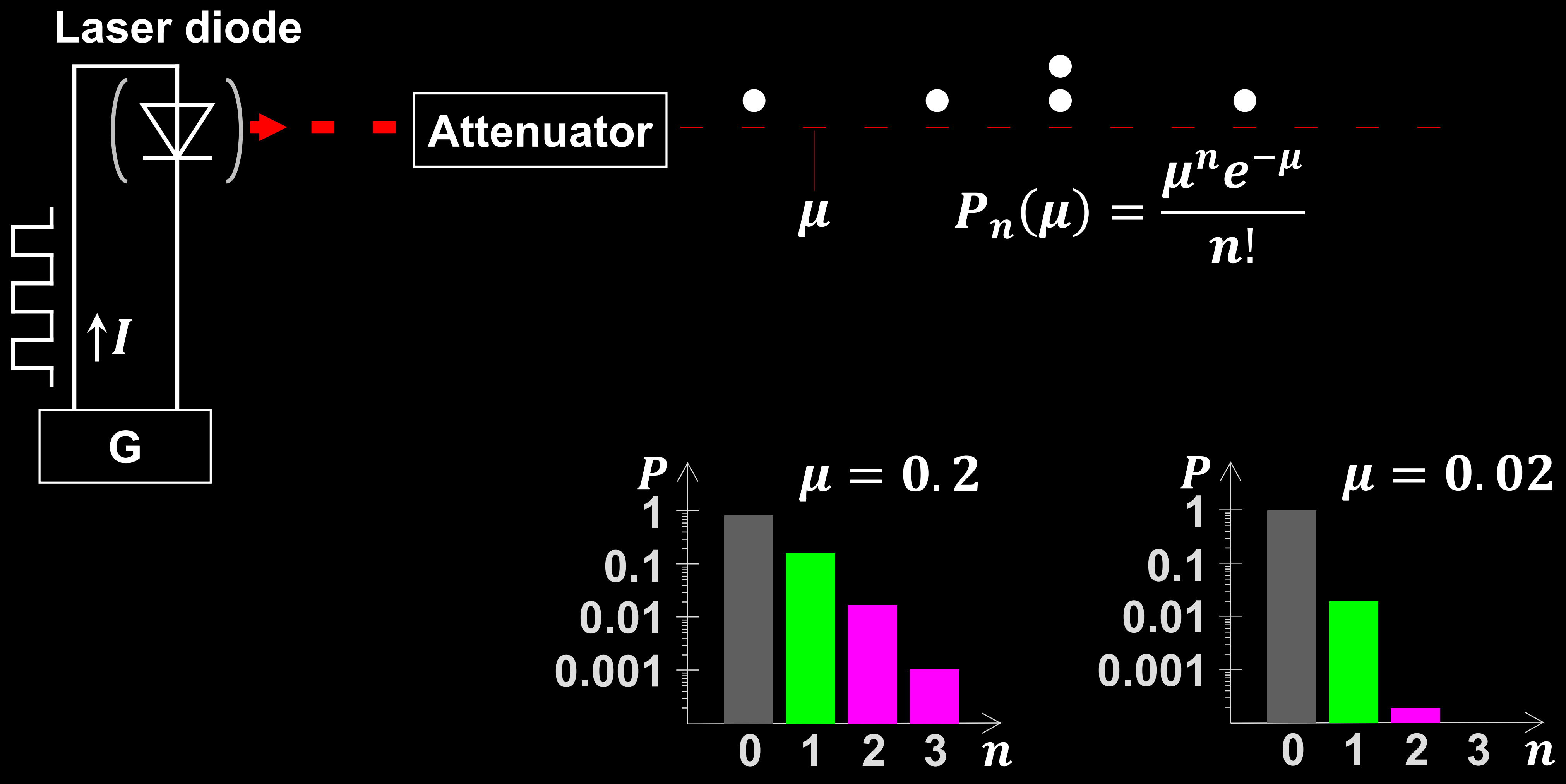
Ground station in Zvenigorod communicates with Micius satellite (18 Jan 2021)

Photo ©2021 Vadim Makarov / RQC

Components of quantum-optical systems

Photon sources ____ **Transmission channels** ____ **“Processing” elements** ____ **Photon detectors**

Attenuated laser source



$$P_n(\mu) = \frac{\mu^n e^{-\mu}}{n!}$$

S. J. van Enk, C. A. Fuchs, arXiv:quant-ph/0111157

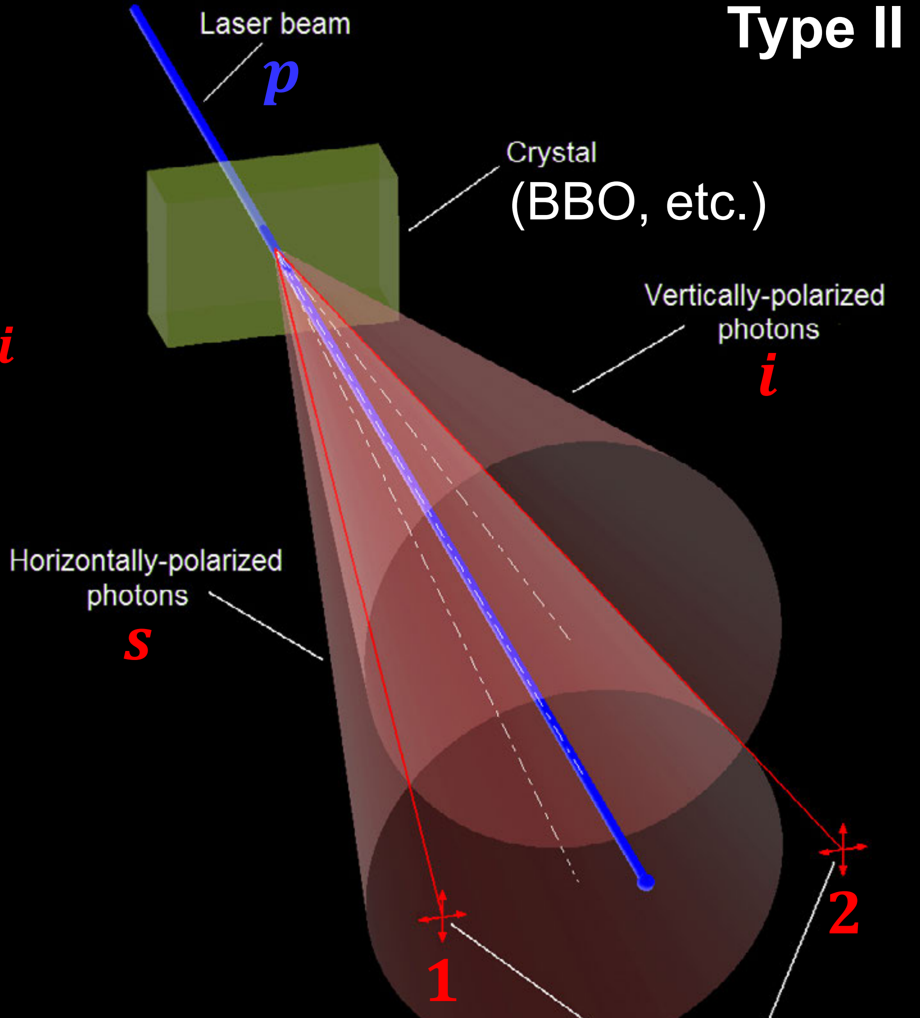
Spontaneous parametric down-conversion

Type II

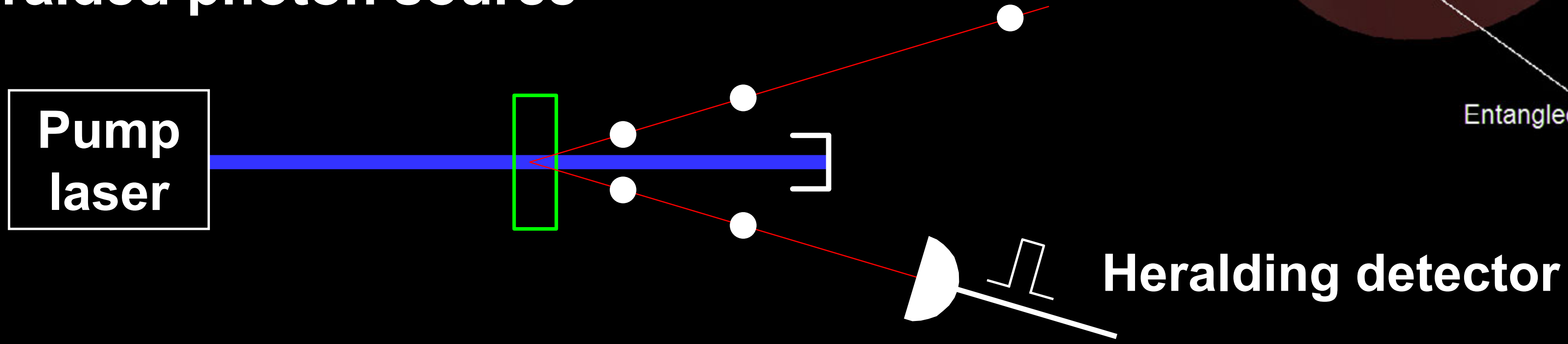
Energy conservation: $\omega_p = \omega_s + \omega_i$

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

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



Heralded photon source

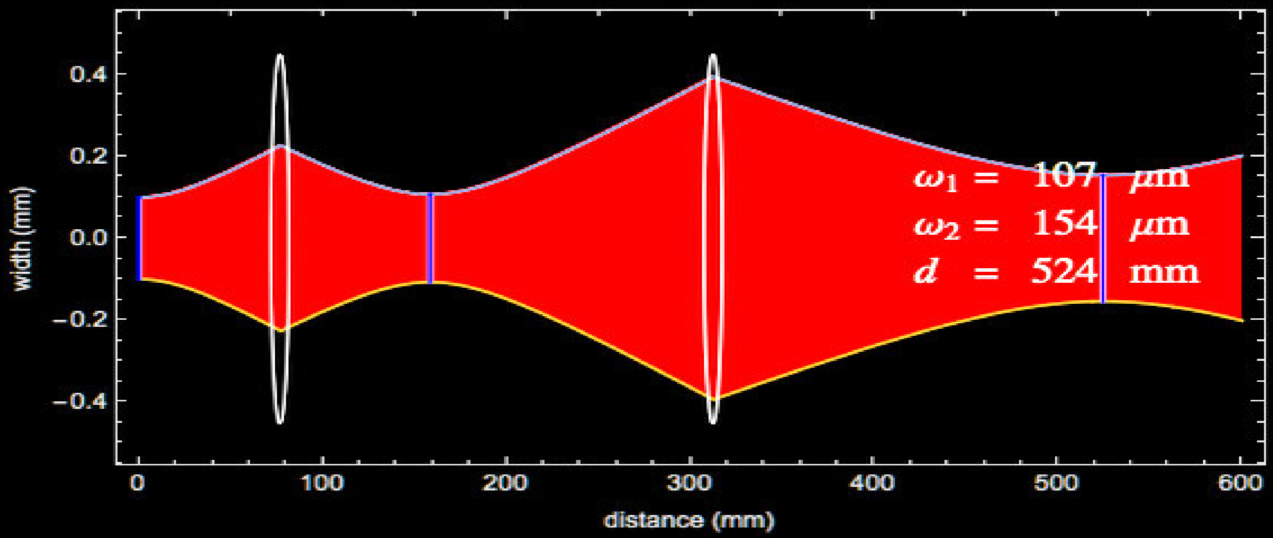


P. G. Kwiat *et al.*, Phys. Rev. Lett. **75**, 4337 (1995)

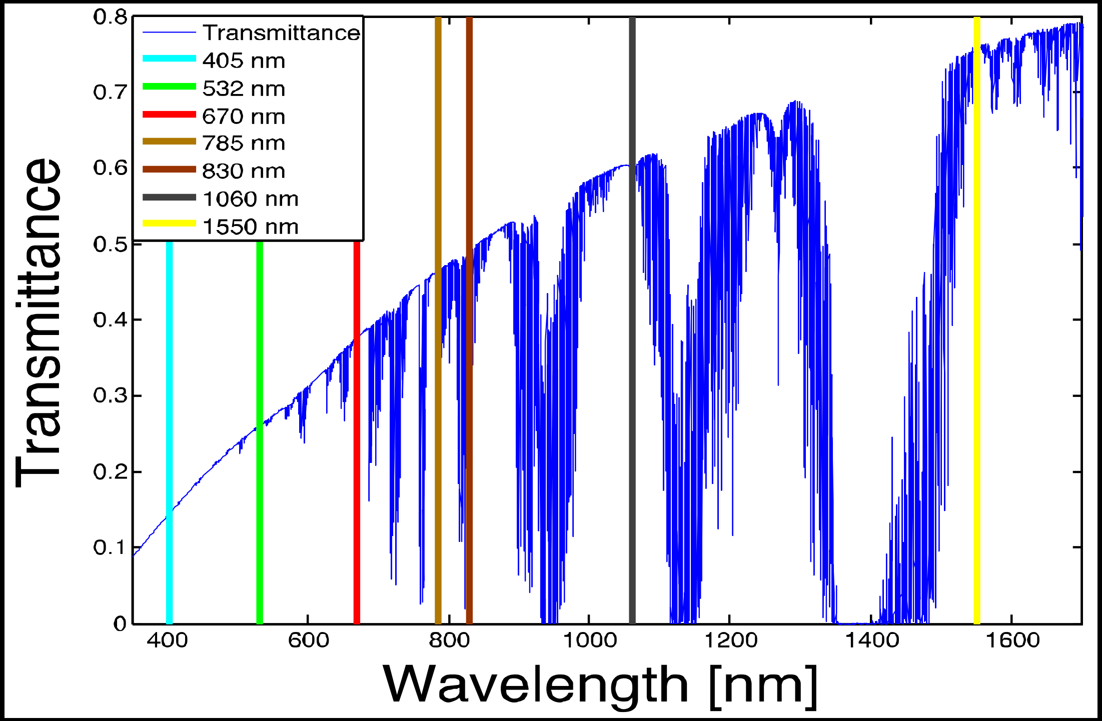
Image reprinted from: Wikipedia

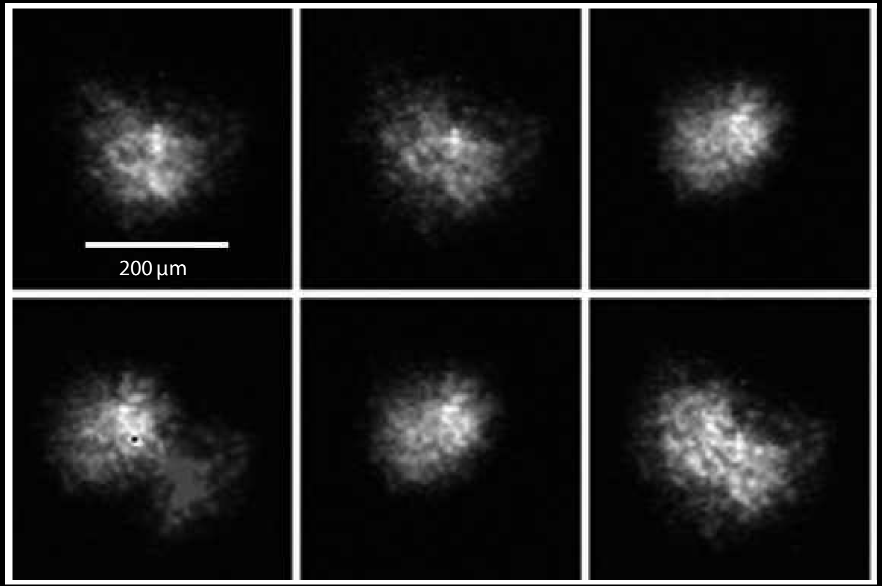
Transmission in free space

Vacuum:
Gaussian optics



Atmosphere: loss, turbulence





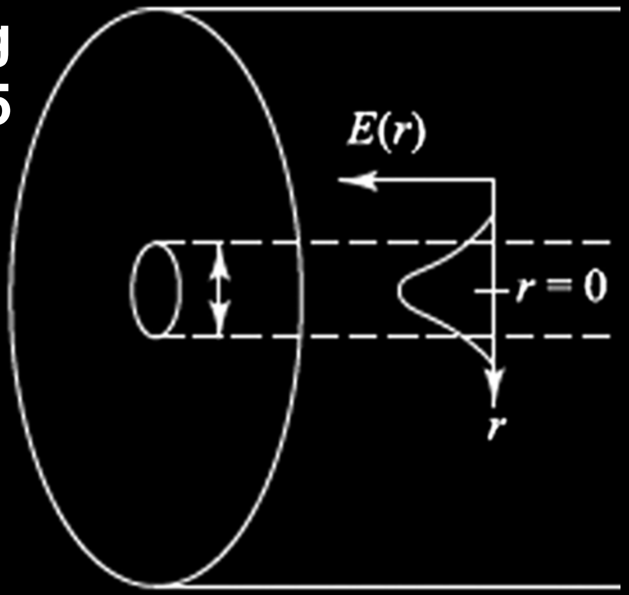
Images reprinted from: https://demonstrations.wolfram.com/GaussianBeamPropagationThroughTwoLenses/; Wikipedia;
J.-P. Bourgoin *et al.*, New J. Phys. **15**, 023006 (2013); R. Ursin *et al.*, Nat. Phys. **3**, 481 (2007)

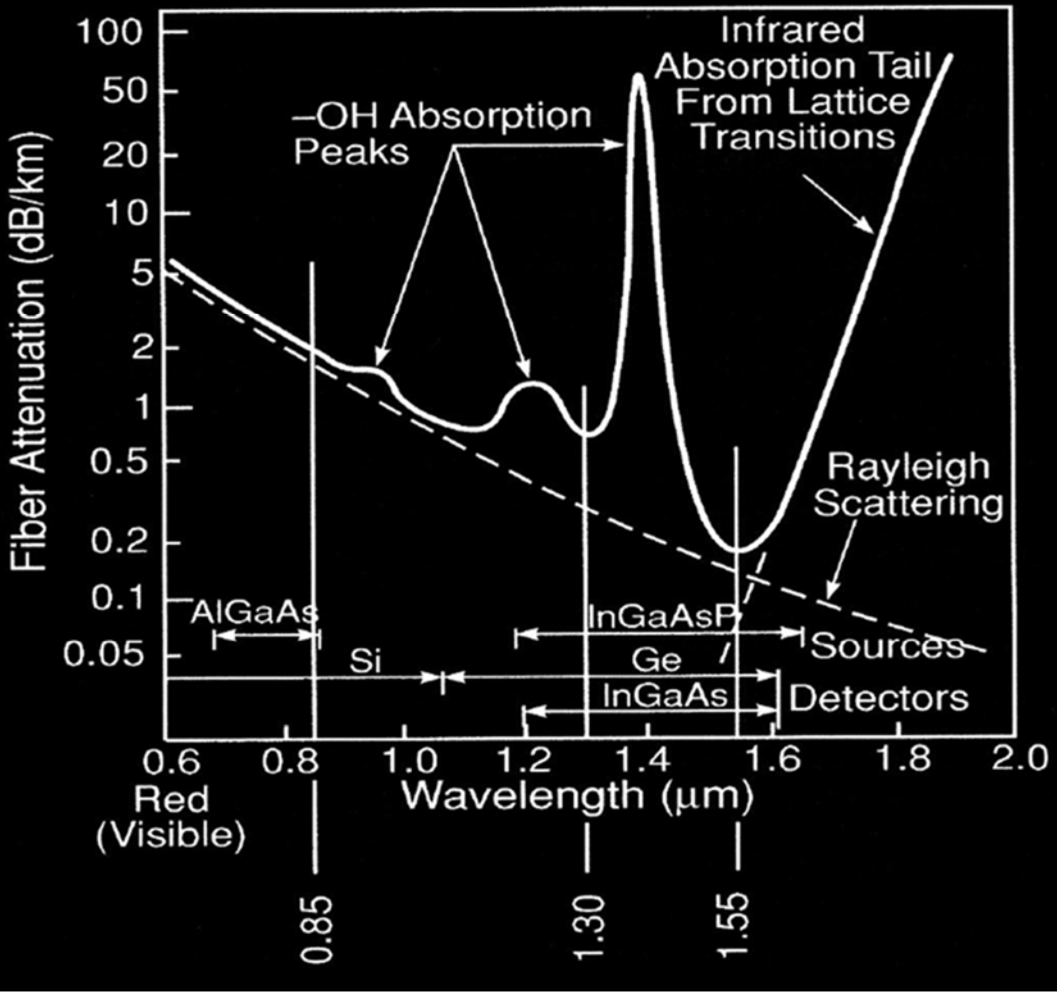
Transmission in optical fiber

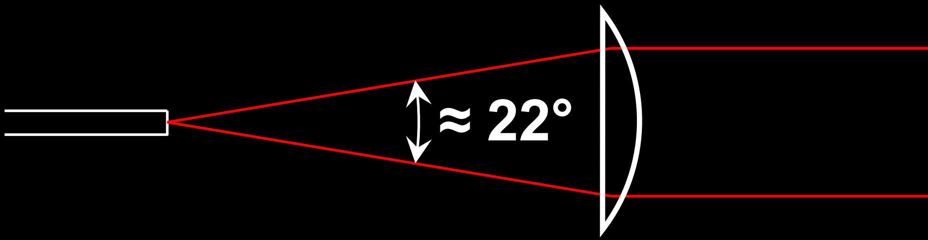
Single-mode fiber

125 µm diameter cladding
fused quartz, n_1 = 1.45

8 µm diameter core
$n_2 > n_1$

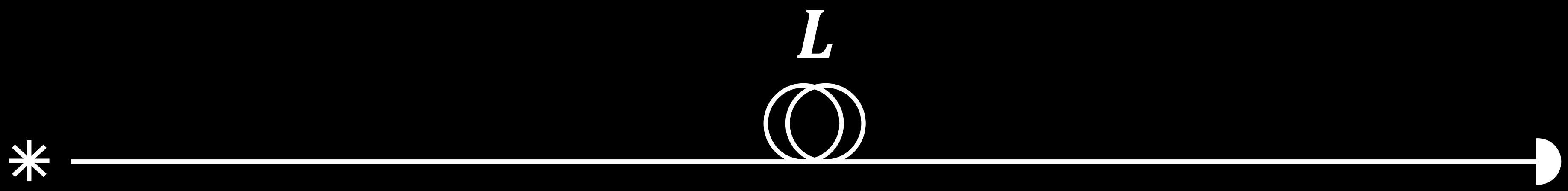






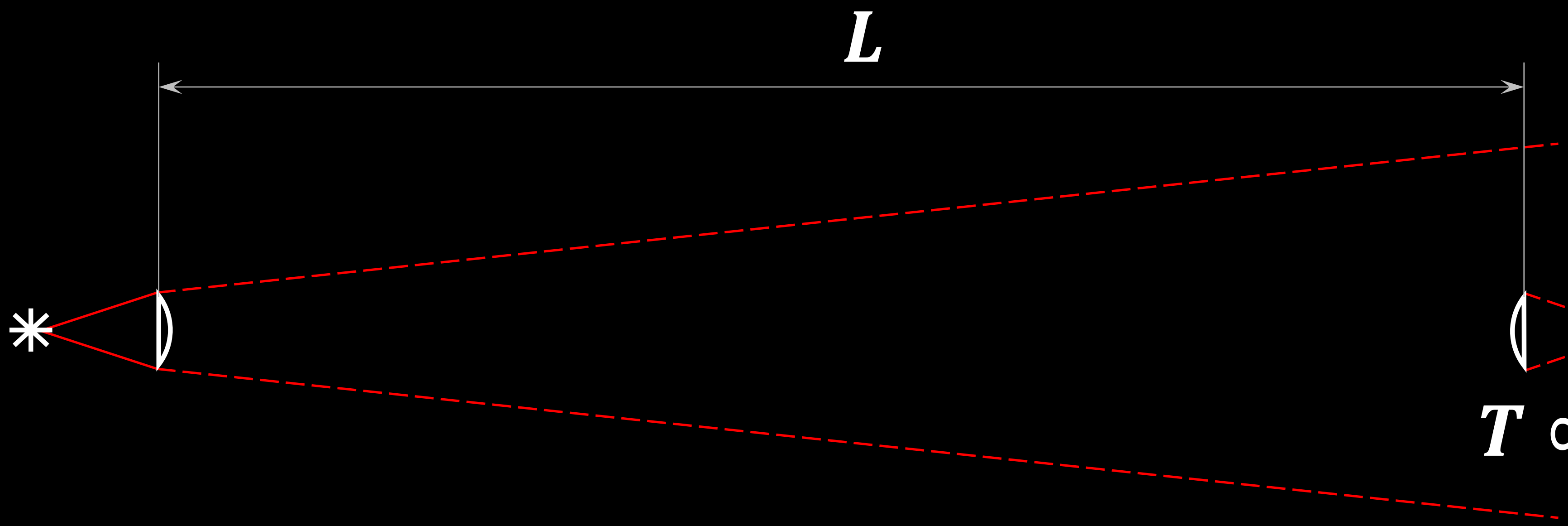
Images reprinted from: G. Keiser *et al.*, J. Biomed. Opt. **19**, 080902 (2014); ViaLite

Fiber vs. beam in vacuum: loss scaling



$T \propto e^{-\alpha L}$

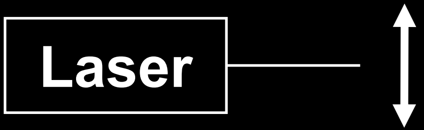
Exponential



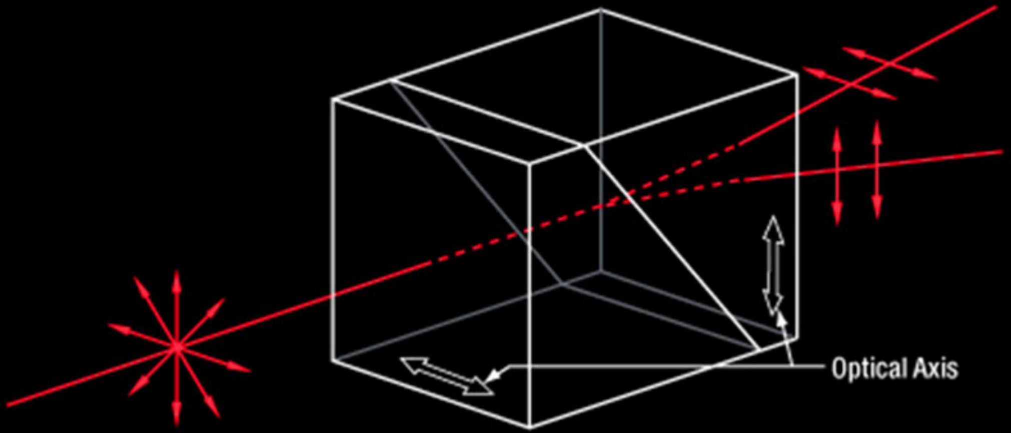
$T \propto L^{-2}$

Polynomial

Polarizers

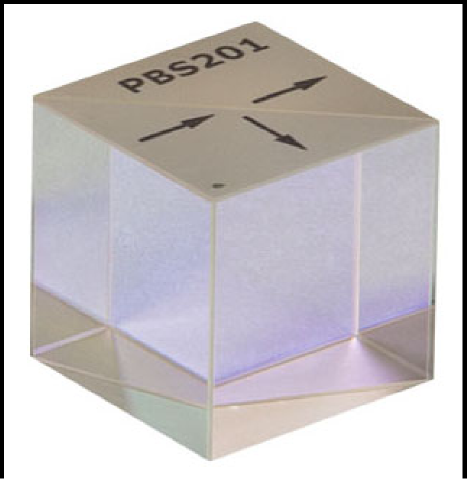


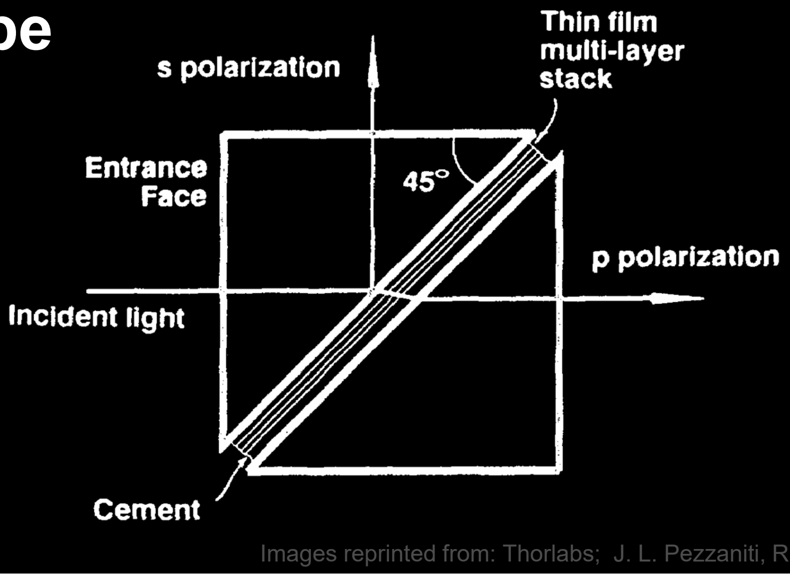
Birefringent polarizing beamsplitter



Wollaston prism

Polarizing beamsplitter cube



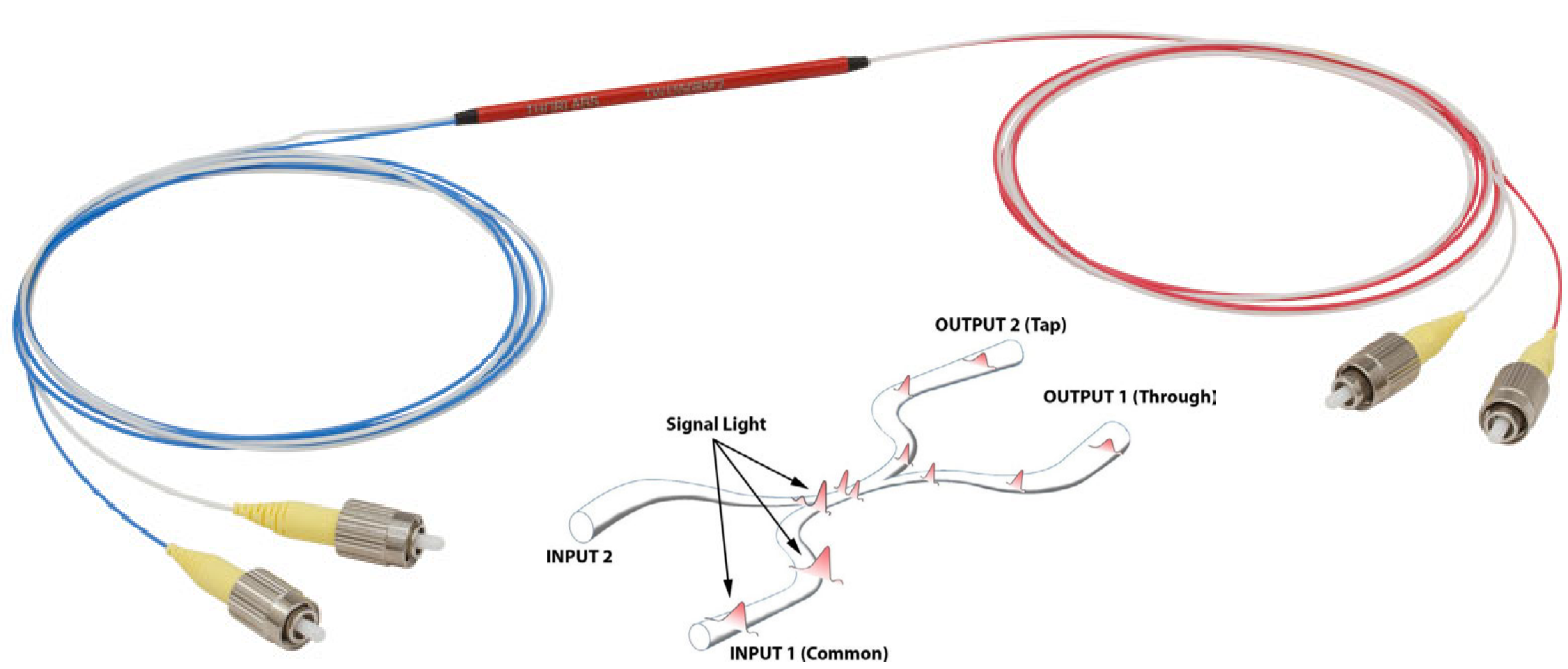


Images reprinted from: Thorlabs; J. L. Pezzaniti, R. A. Chipman, Appl. Opt. **33**, 1916 (1994)

Beamsplitters

50:50
10:90
1:99

Fiber-optic fused beamsplitter (or coupler)

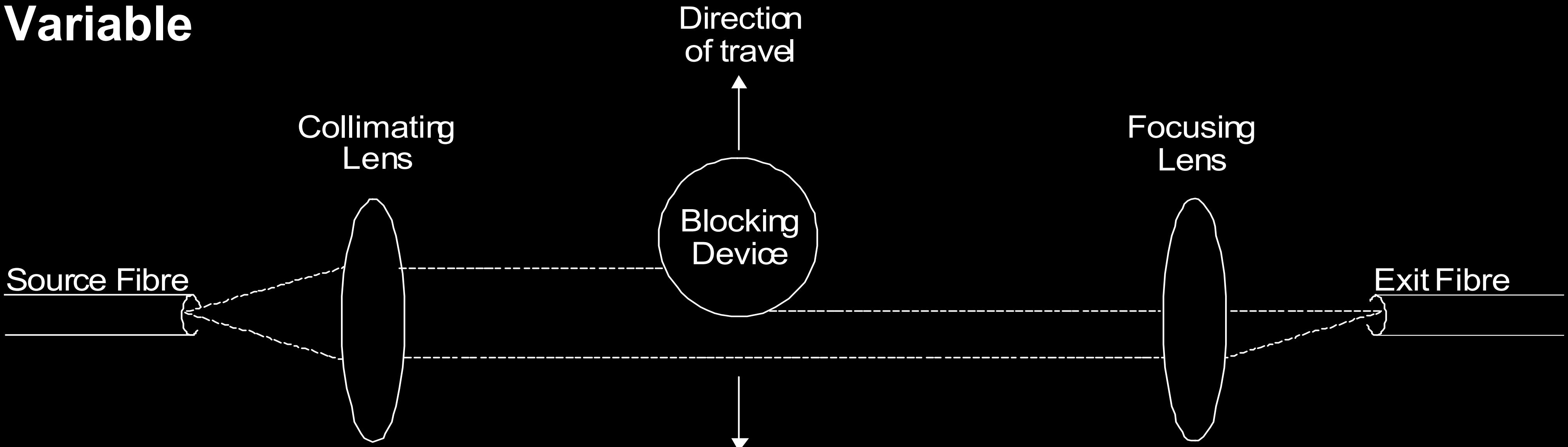


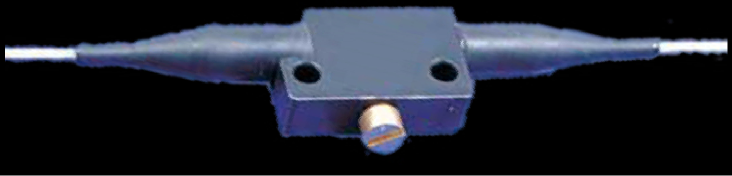
Images reprinted from: Thorlabs; Go!Foton

Attenuators

Absorbing or partially reflecting coated glass

Variable





2–60 dB

Images reprinted from: Thorlabs; OZ Optics

Wavelength filters

Colored glass

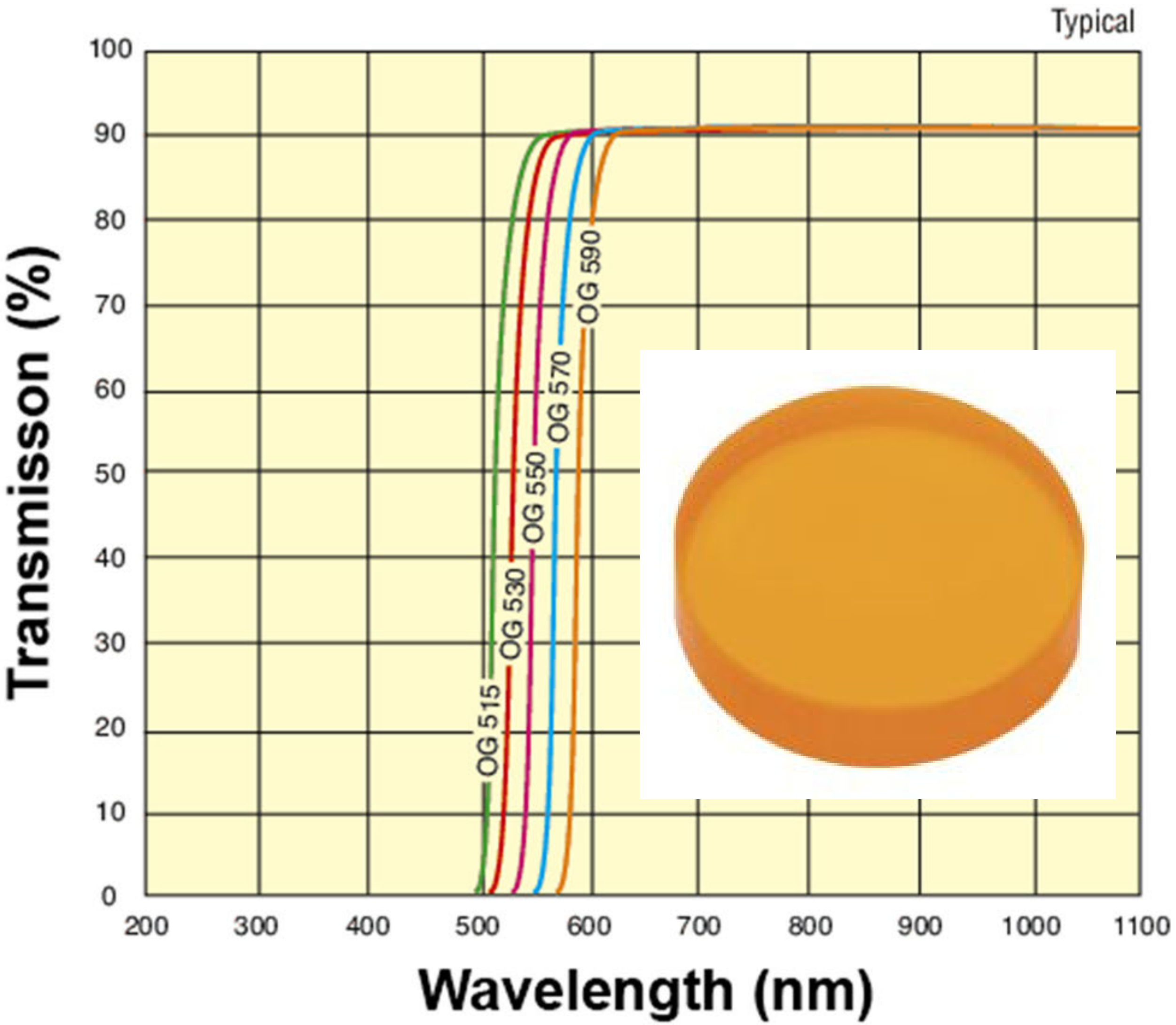
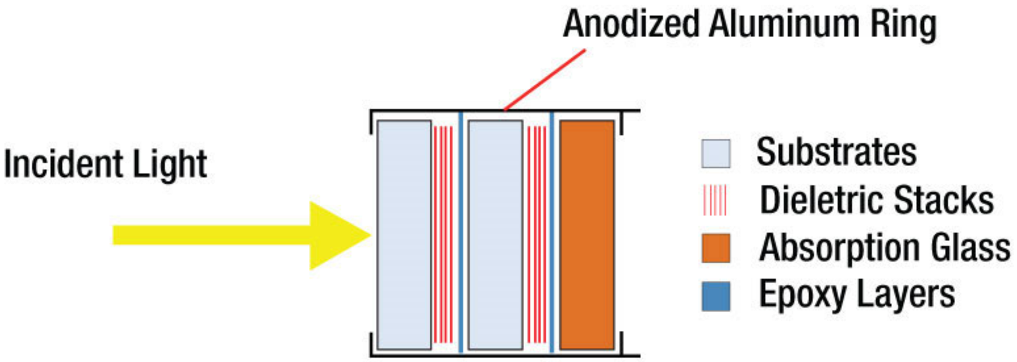
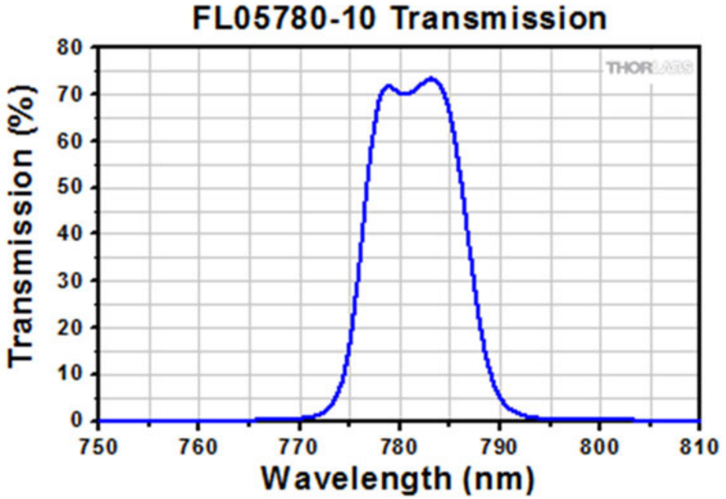


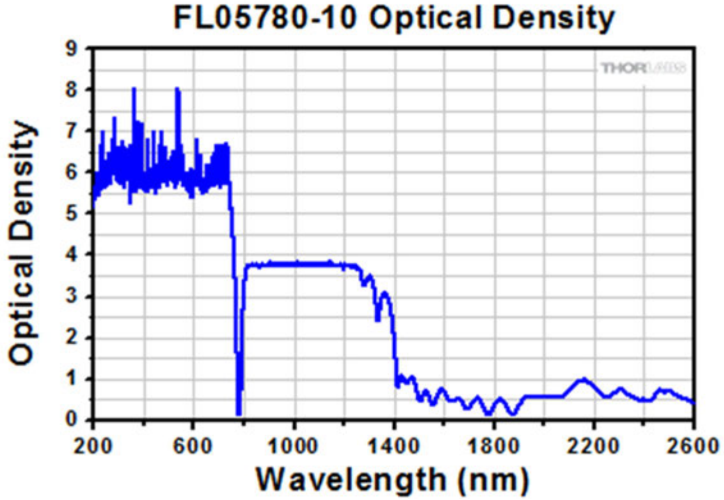
Image reprinted from: Newport

Wavelength filters

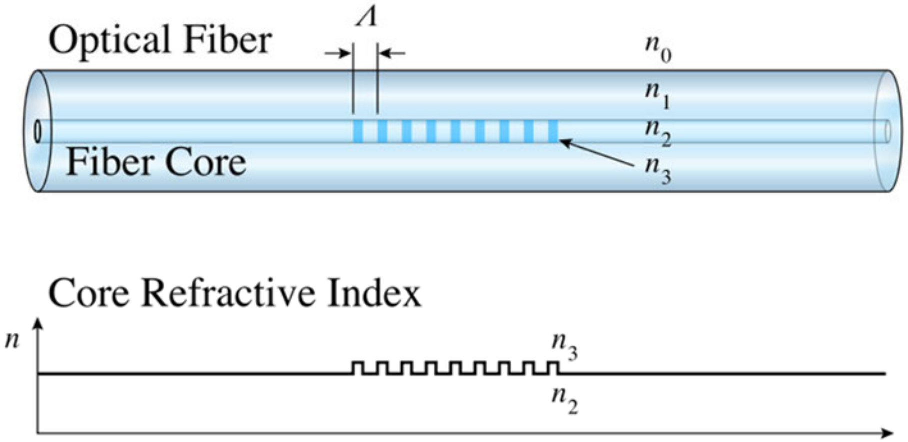
Interference filter

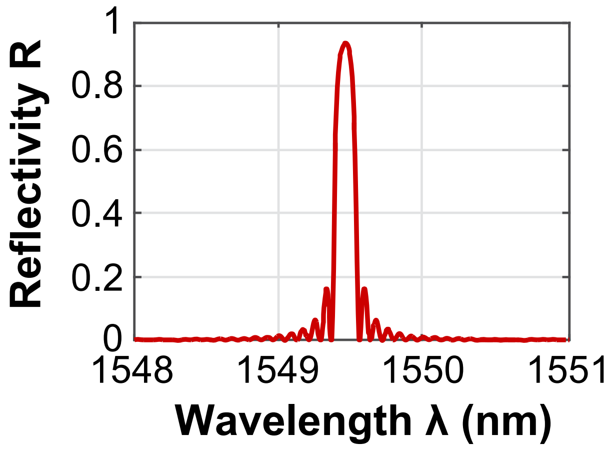






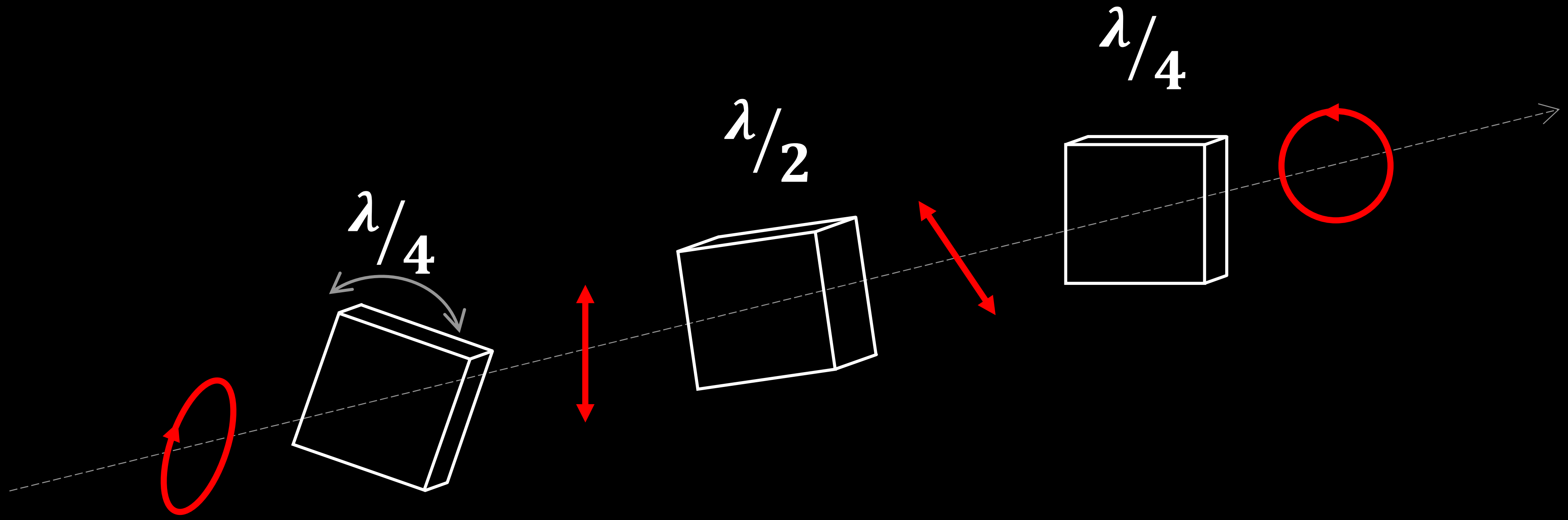
Fiber Bragg grating

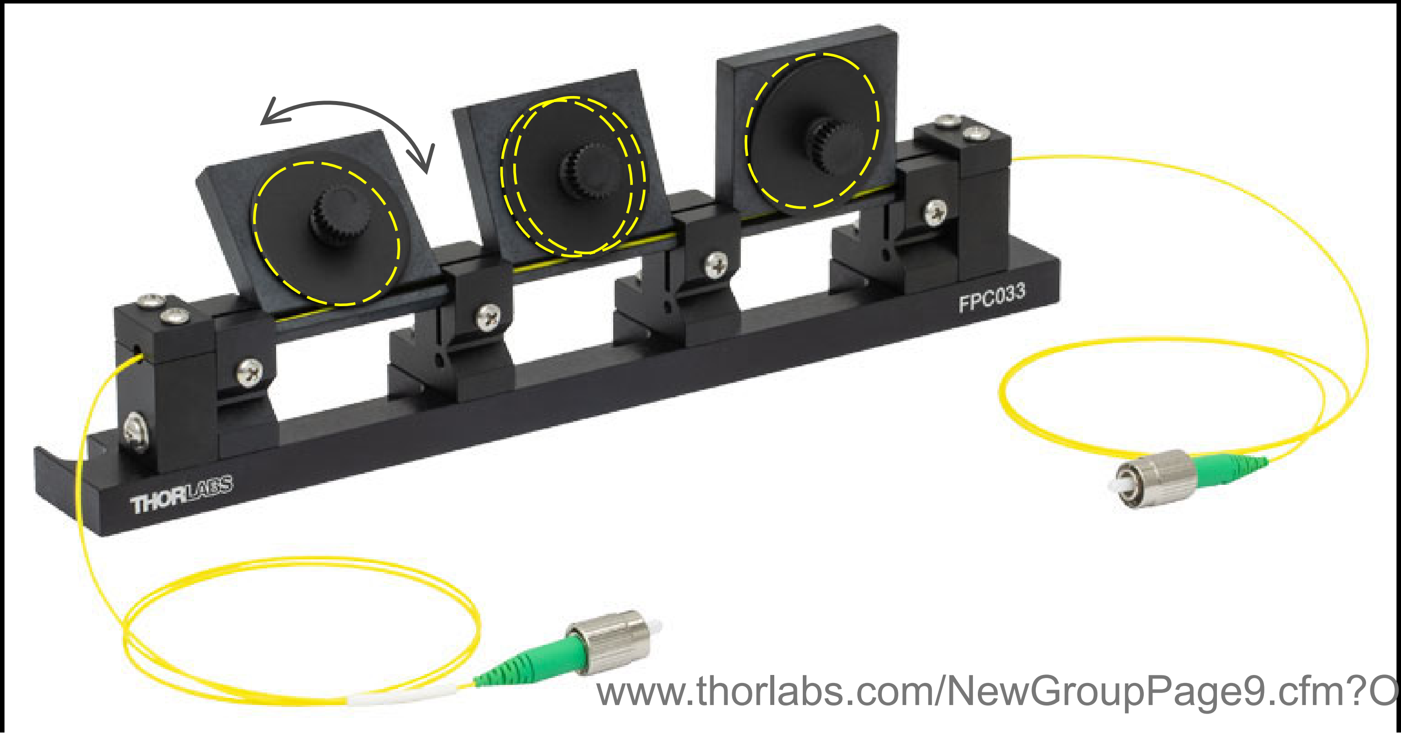




Images reprinted from: Thorlabs; Wikipedia; F. Seng *et al.*, Appl. Opt. **55**, 7179 (2016)

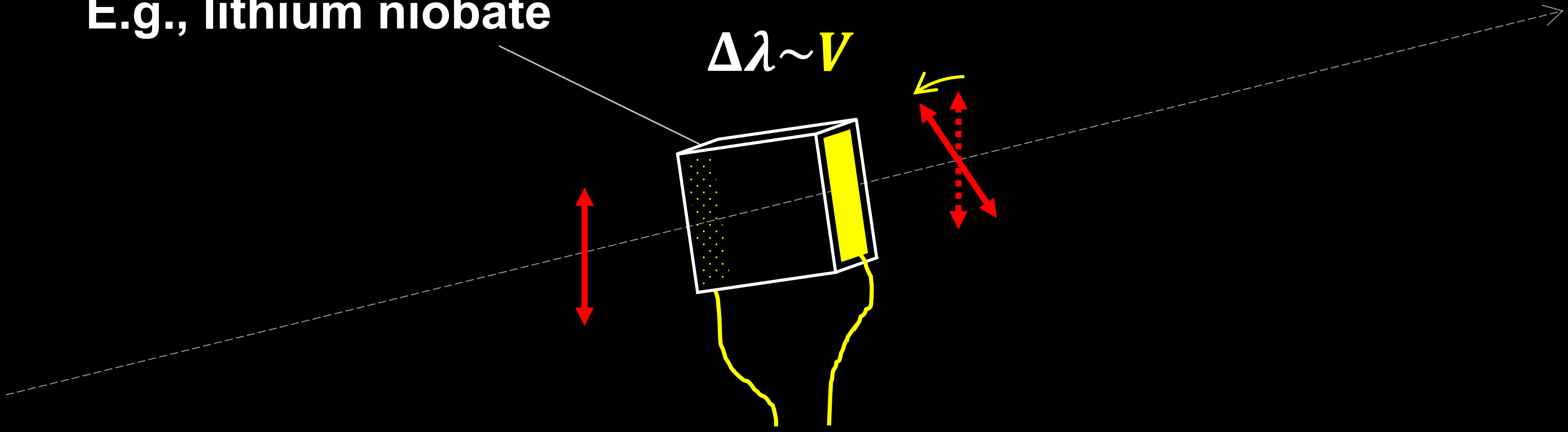
Polarization controller (slow)





www.thorlabs.com/NewGroupPage9.cfm?ObjectGroup_ID=343

Polarization modulator (fast)



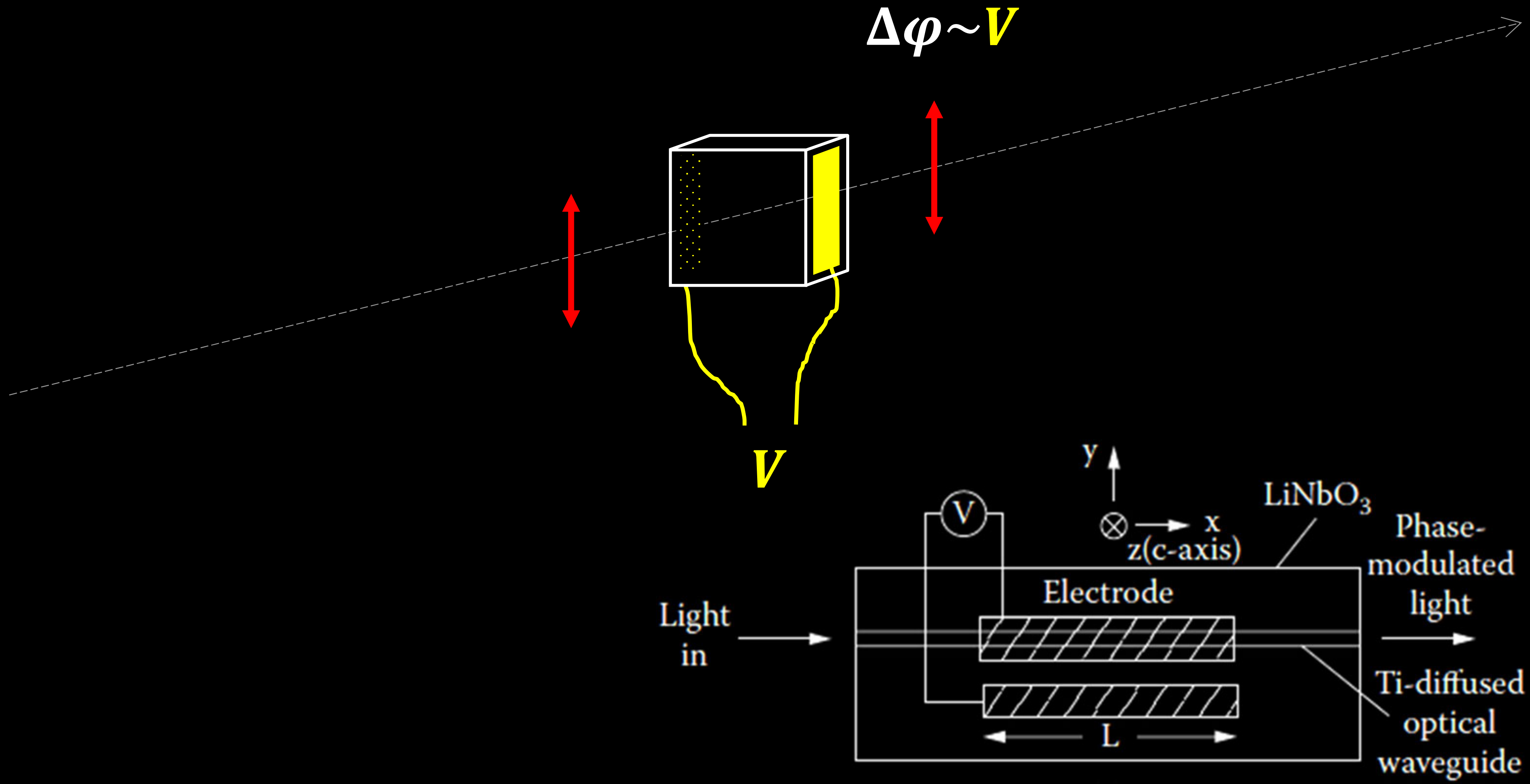
E.g., lithium niobate

$\Delta\lambda \sim V$

0 or V_{π}

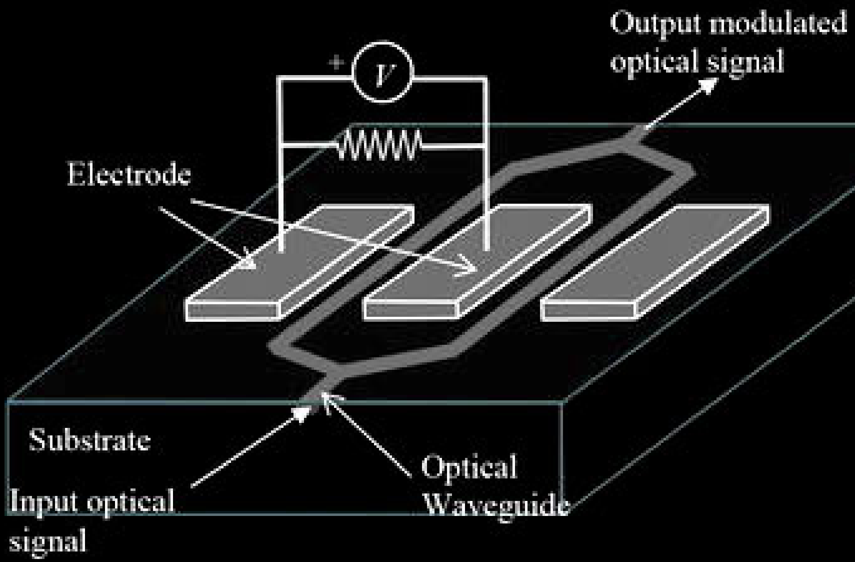
Pockels cell

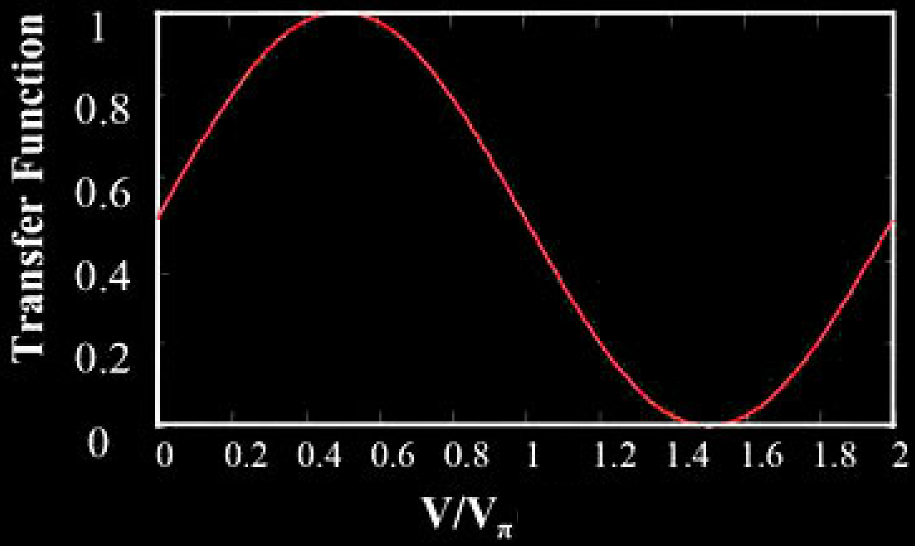
Phase modulator



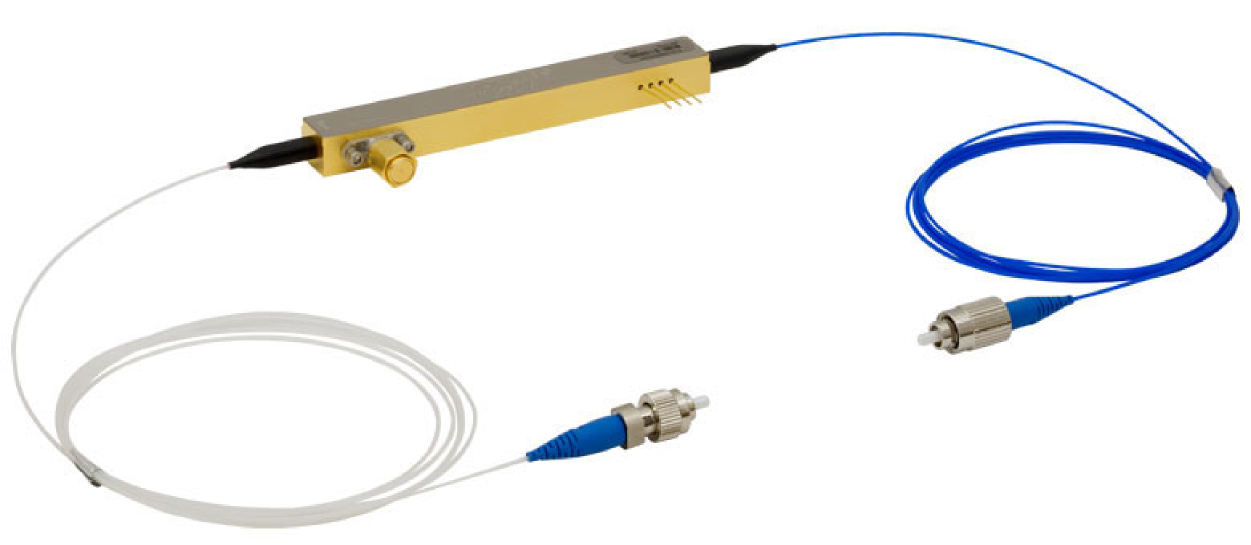
Images reprinted from: A. E.-N. A. Mohamed *et al.*, Int. J. Multidiscip. Sci. Eng. **2**, 13 (2011); iXblue Photonics

Intensity modulator





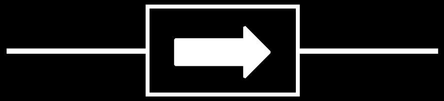
Mach-Zehnder interferometer

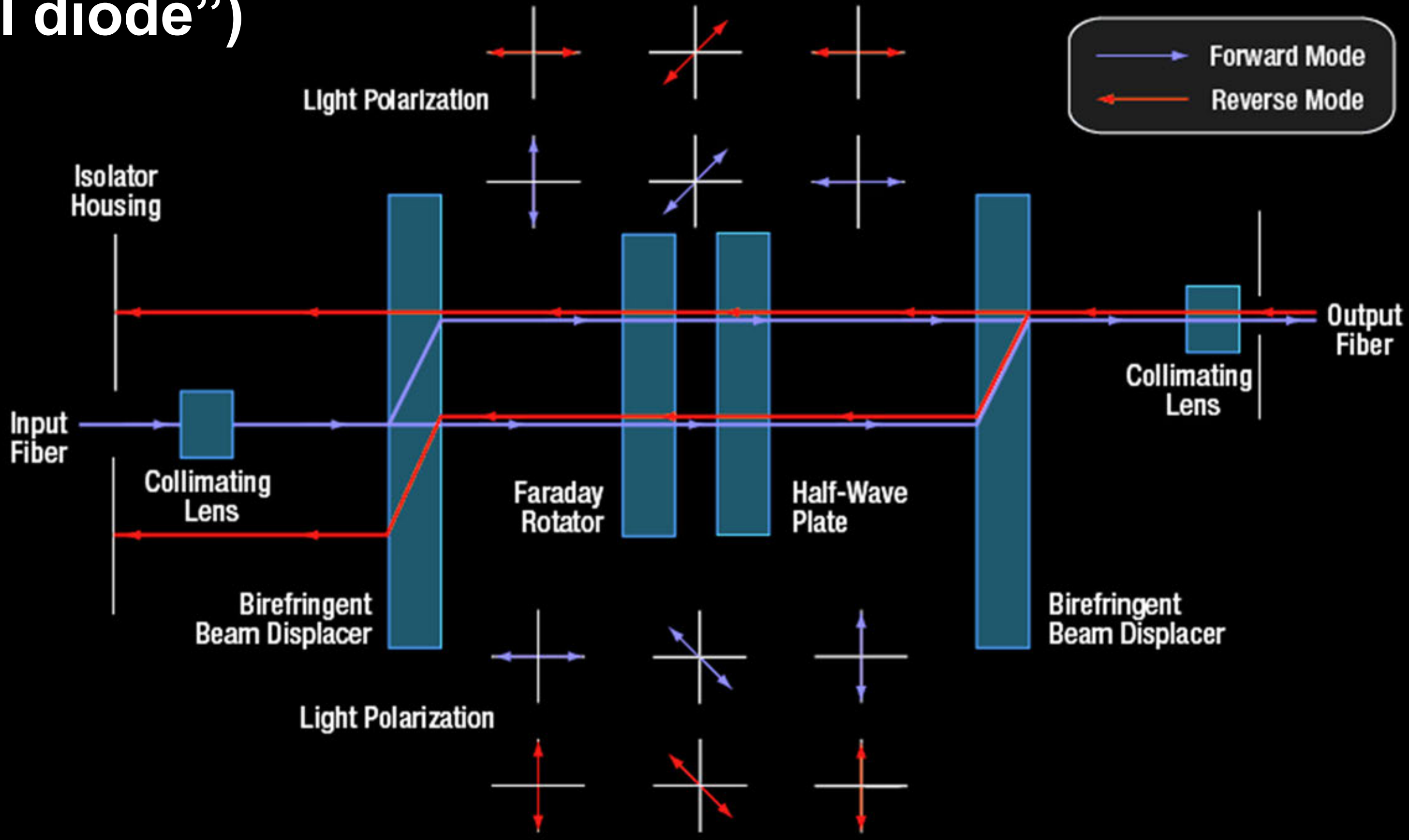


Images reprinted from: Optical Communication Technology, P. Pinho, ed., IntechOpen (2017); Thorlabs

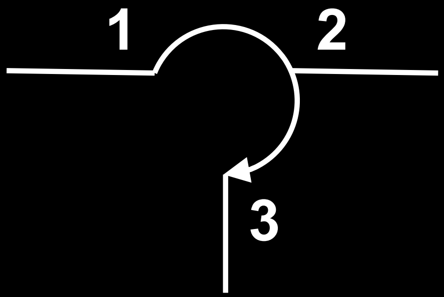
Directional elements

Isolator (an “optical diode”)



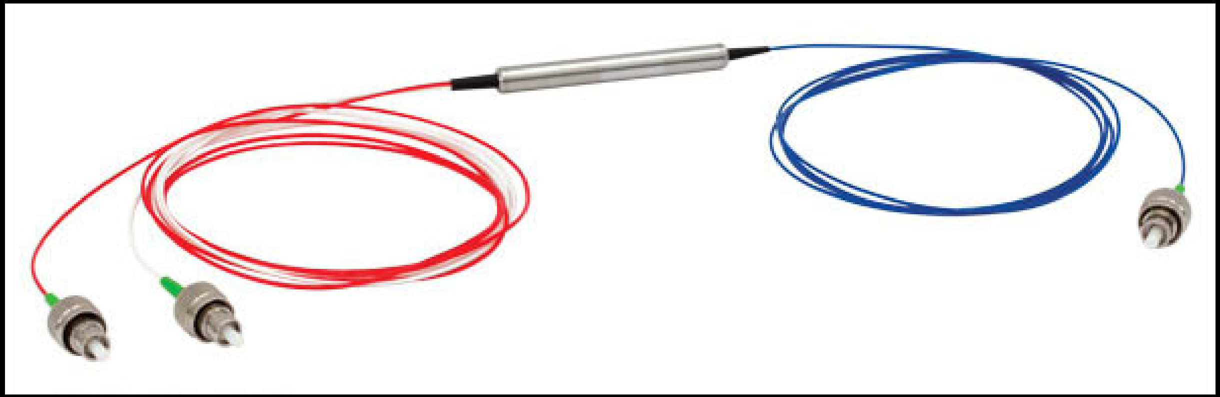


Circulator



1 → 2

2 → 3

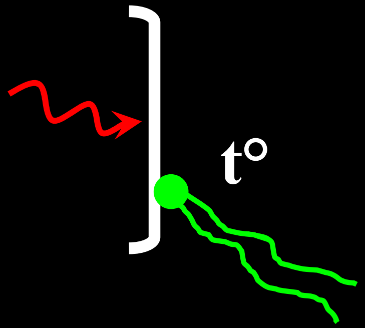


Images reprinted from: Thorlabs

Optical power meters

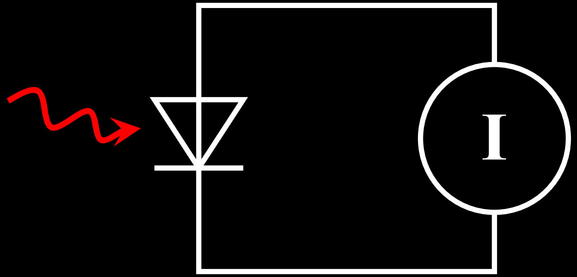
Thermal

> 10 µW



Photodiode

> 0.1 nW



Single-photon detectors

Photon energy

$$E = \frac{hc}{\lambda} = \frac{19.9 \times 10^{-26}}{1.55 \times 10^{-6}} = 1.28 \times 10^{-19}\ \mathrm{J}$$

⬇

Need a gain mechanism

Photomultiplier tube

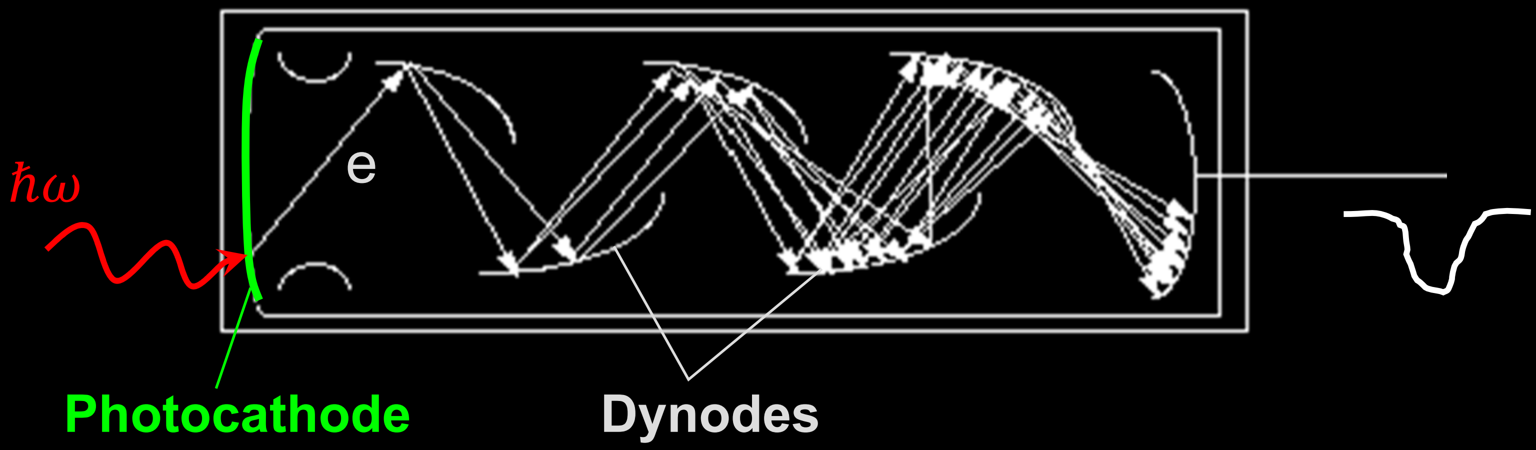
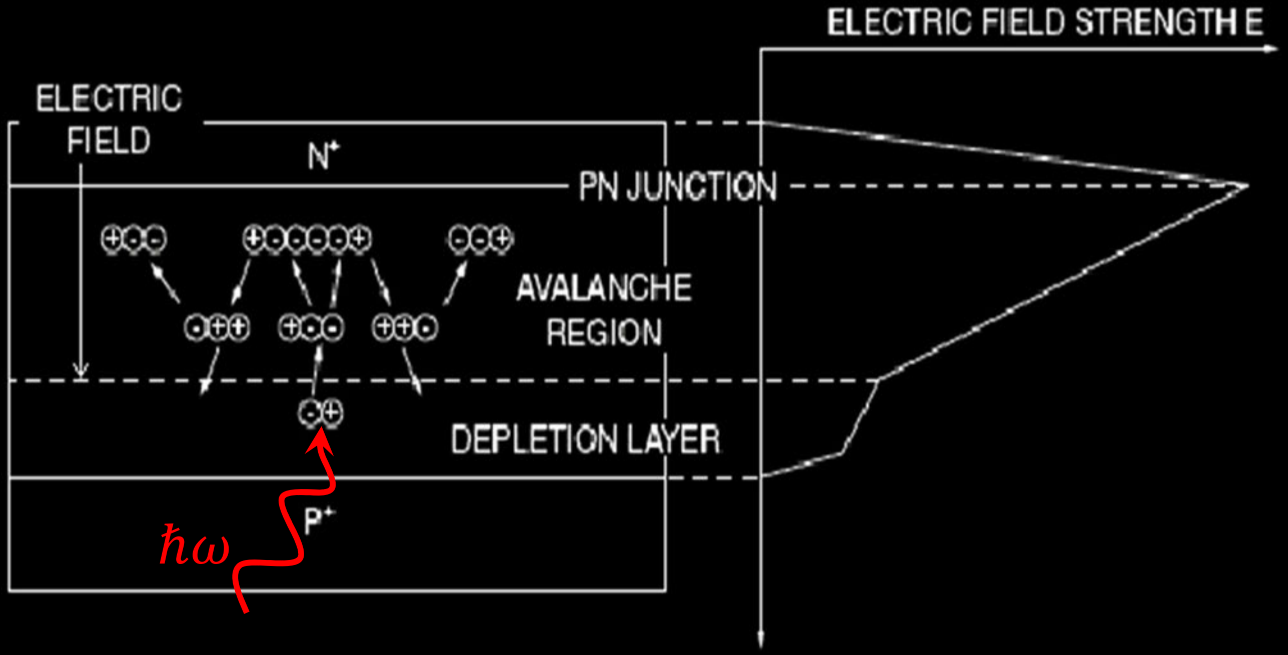
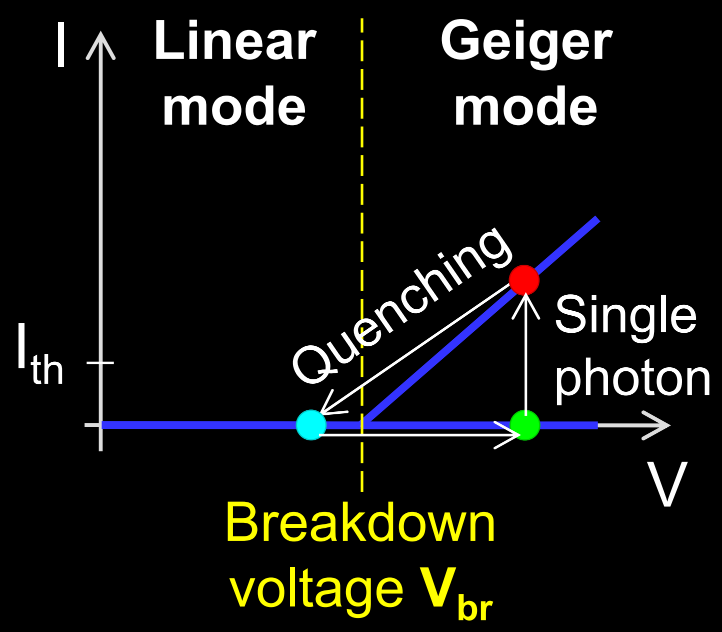
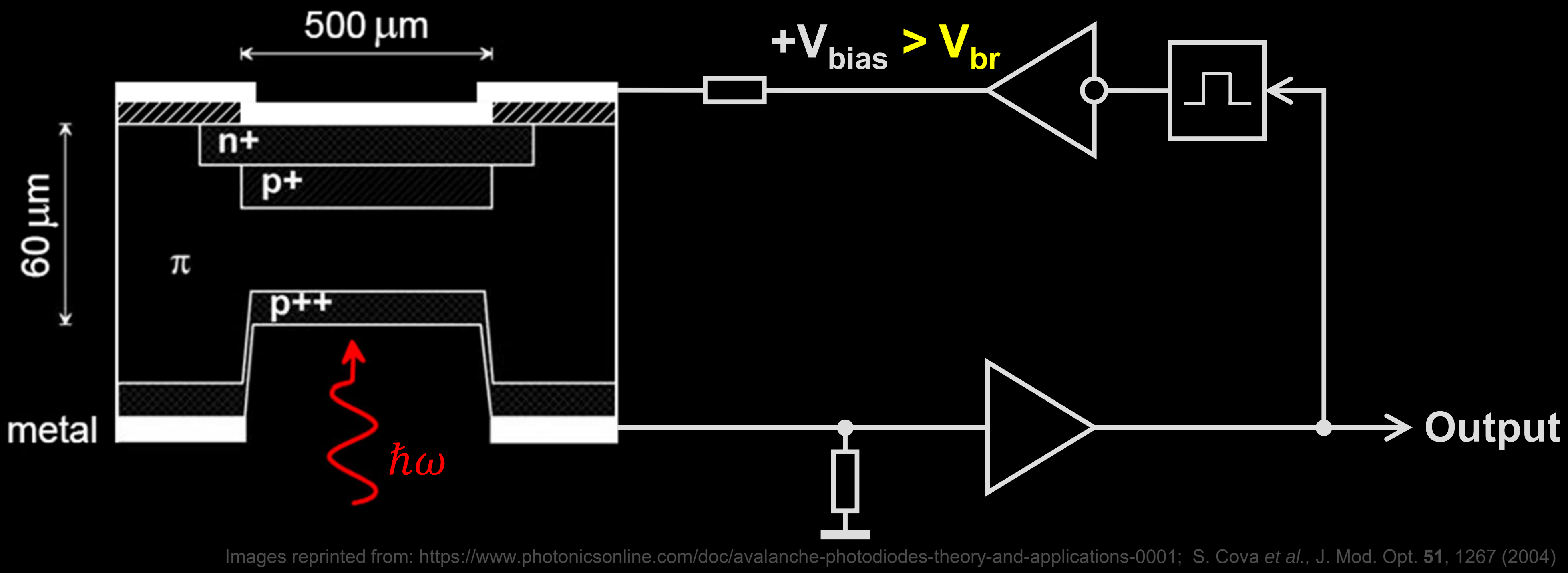


Image reprinted from: http://www.frankswebspace.org.uk/ScienceAndMaths/physics/physicsGCE/D1-5.htm

Single-photon avalanche photodiode



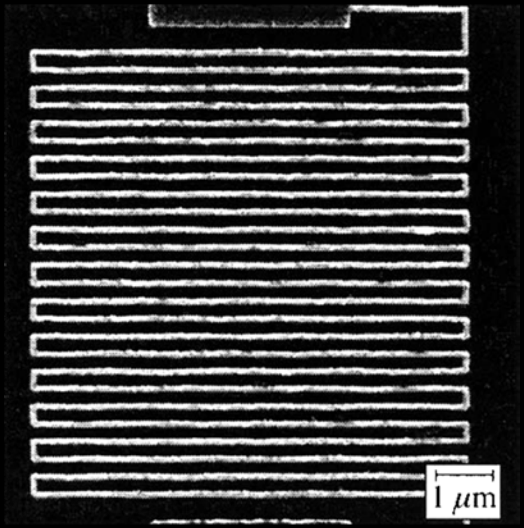


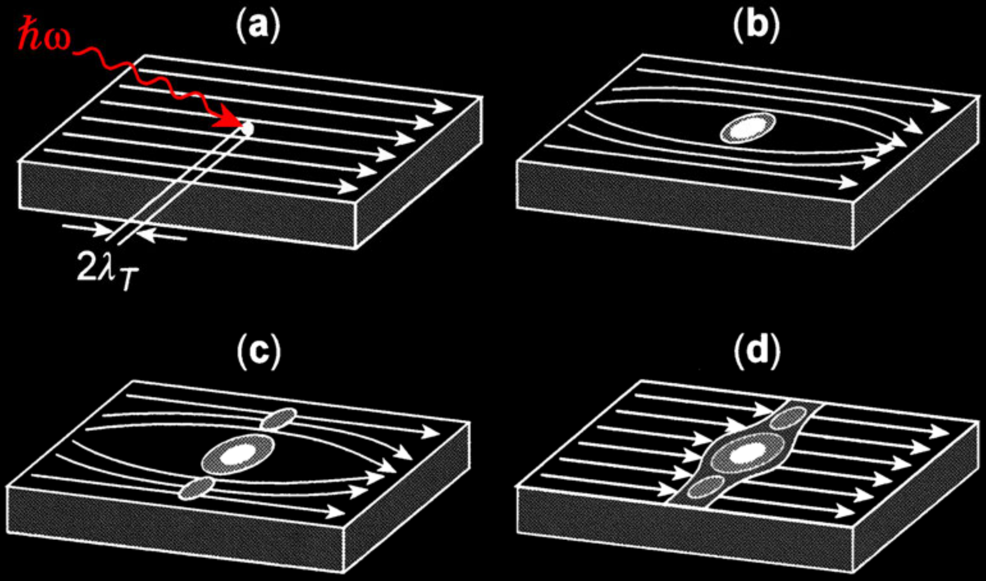


Images reprinted from: https://www.photonicsonline.com/doc/avalanche-photodiodes-theory-and-applications-0001; S. Cova *et al.*, J. Mod. Opt. **51**, 1267 (2004)

Superconducting single-photon detectors

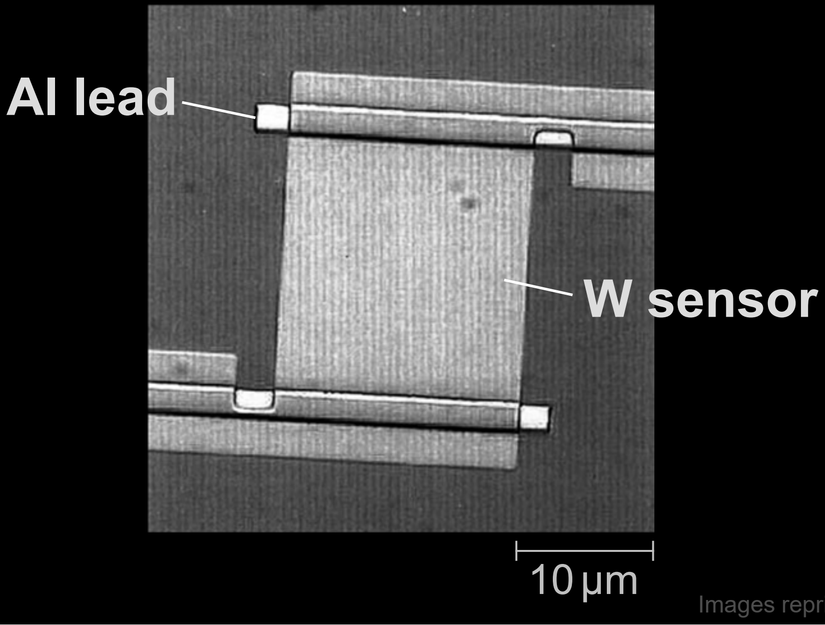
Superconducting nanowire

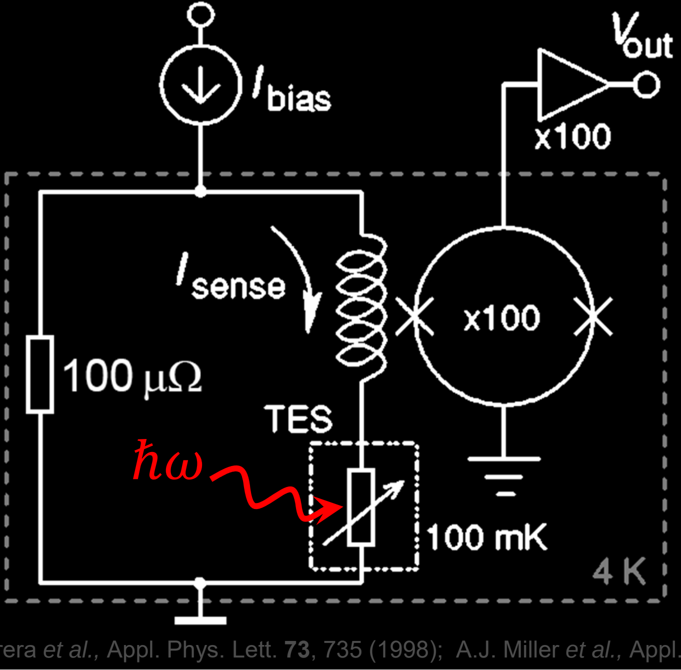




Images reprinted from: R. Sobolewski *et al.*, IEEE Trans. Appl. Supercond. **13**, 1151 (2003)

Transition-edge sensor



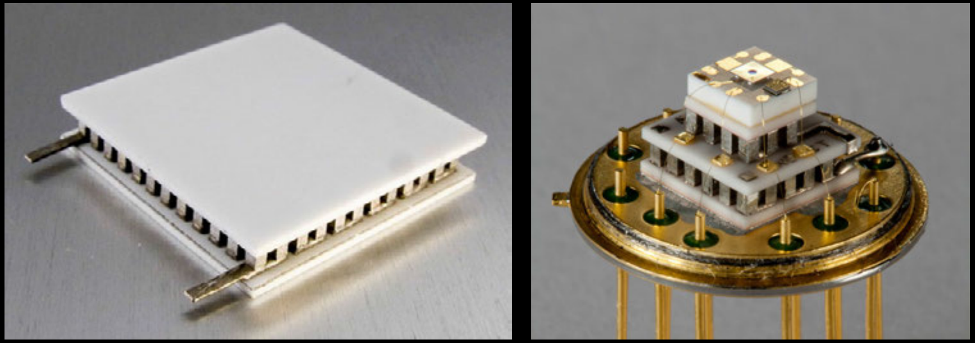


Images reprinted from: B. Cabrera *et al.*, Appl. Phys. Lett. **73**, 735 (1998); A.J. Miller *et al.*, Appl. Phys. Lett. **83**, 791 (2003)

Cooling requirements

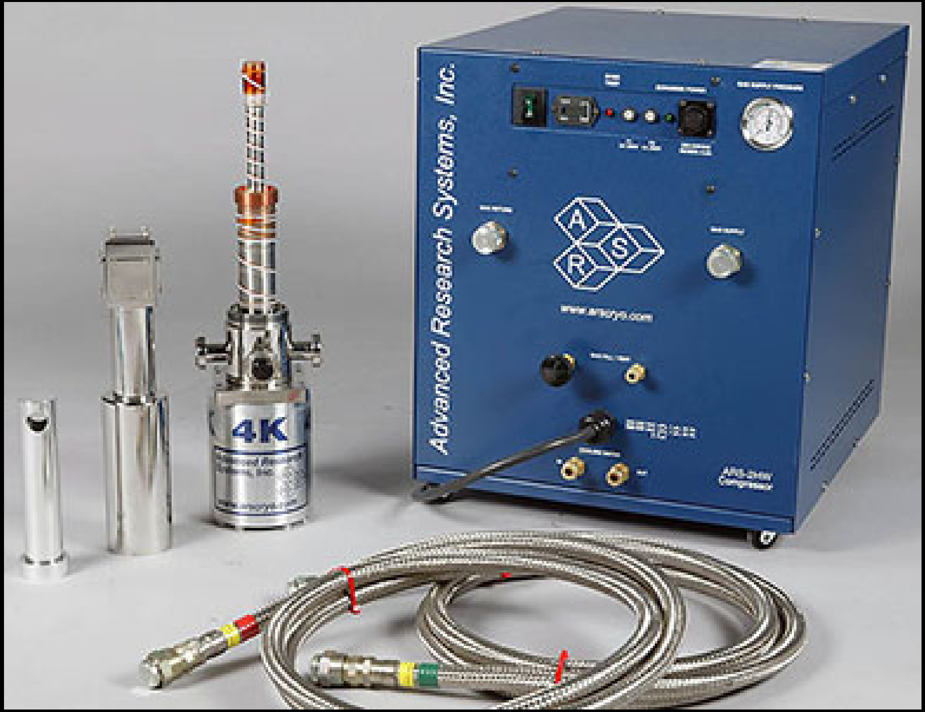
Photomultiplier: room temperature

Avalanche photodiode: −50 °C



Thermoelectric cooling

Superconducting nanowire: 4 K

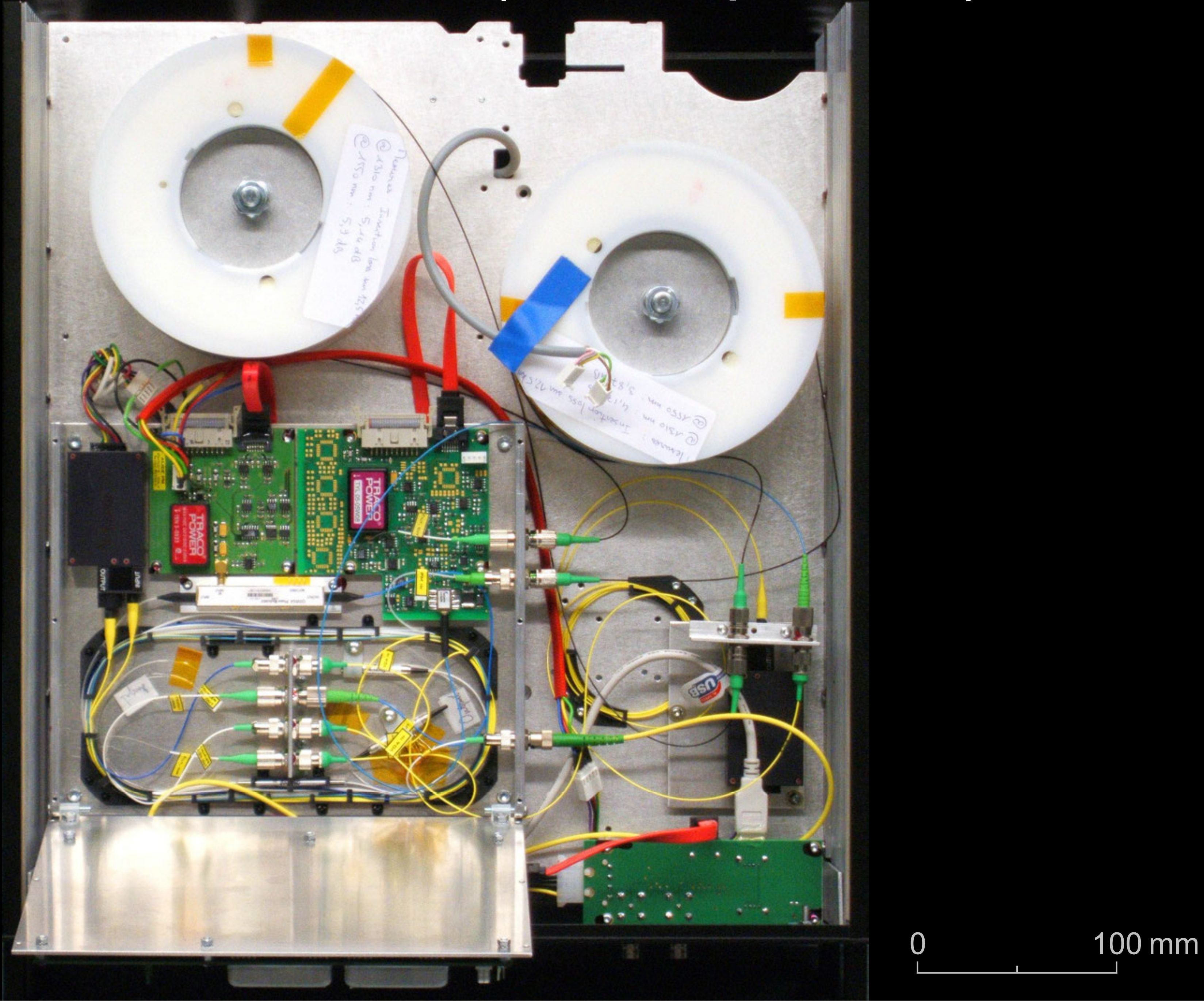


Transition-edge sensor: 100 mK

Images reprinted from: Kryotherm; S. Sauge *et al.*, Opt. Express **19**, 23590 (2011); Advanced Research Systems; University of Cape Town

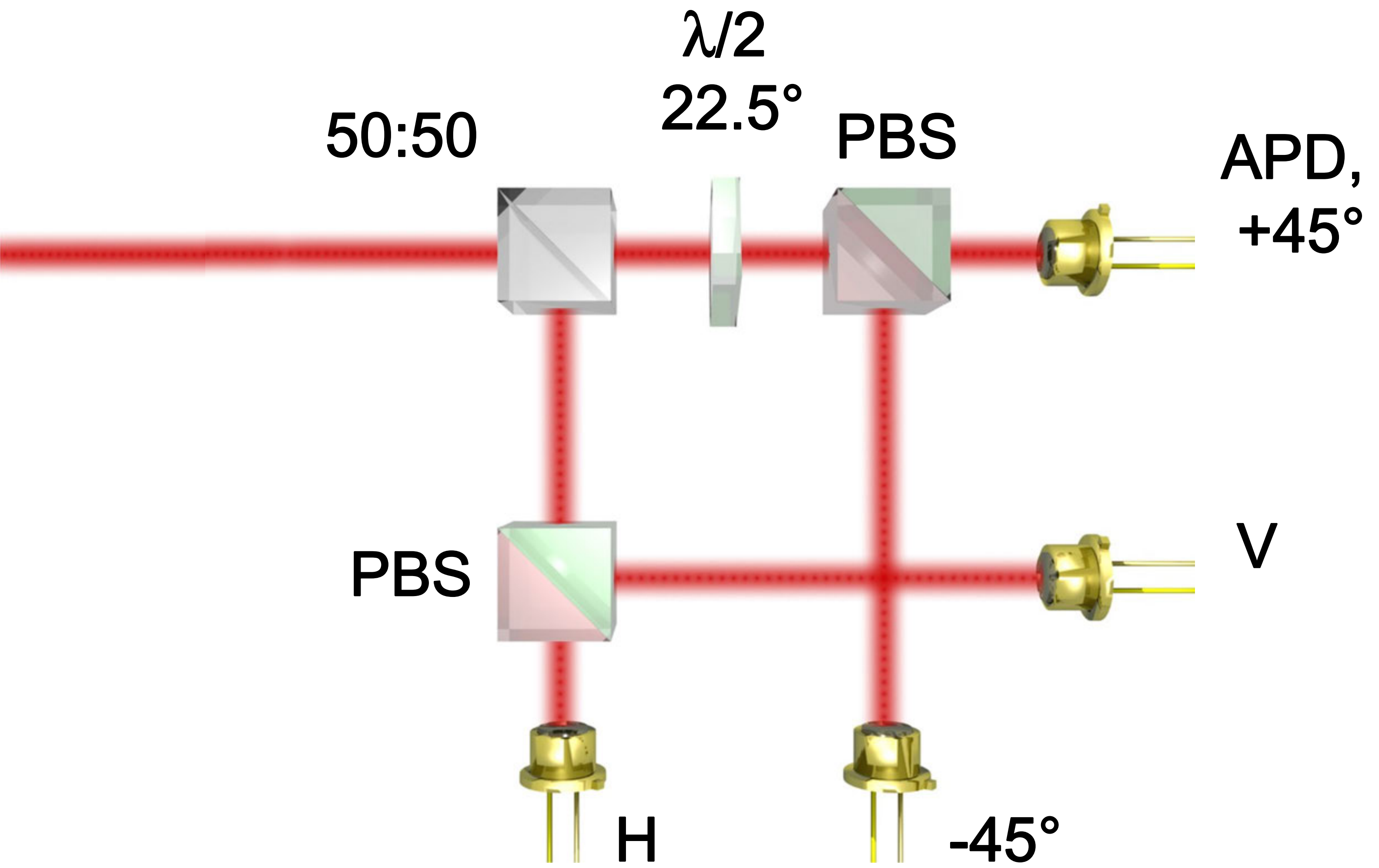
Assembled fiber optics

Quantum key distribution unit Alice (ID Quantique Clavis2)



Assembled free-space optics

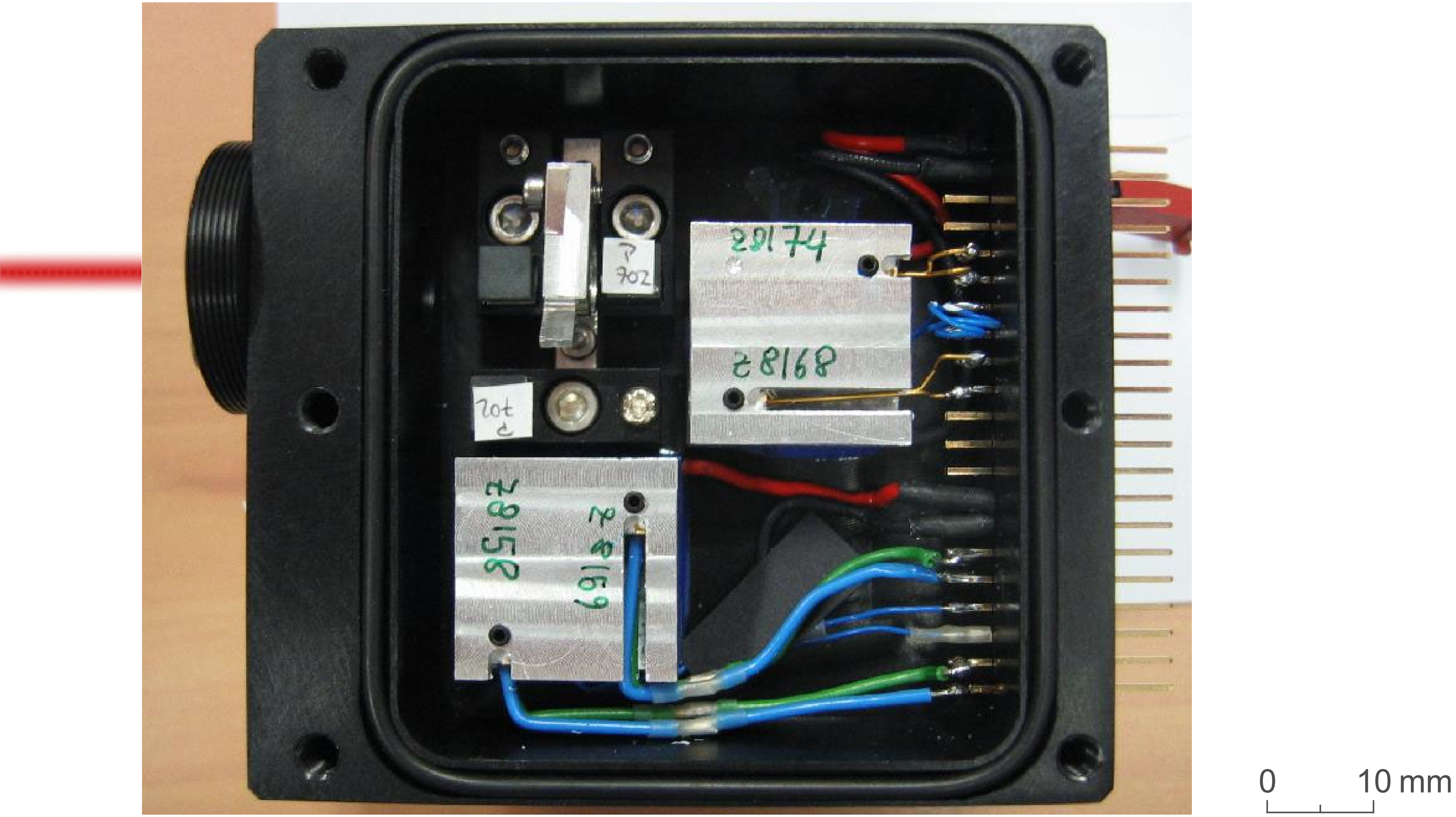
Bob’s polarization analyzer with single-photon detectors



J. G. Rarity, P. C. M. Owens, P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994)

Assembled free-space optics

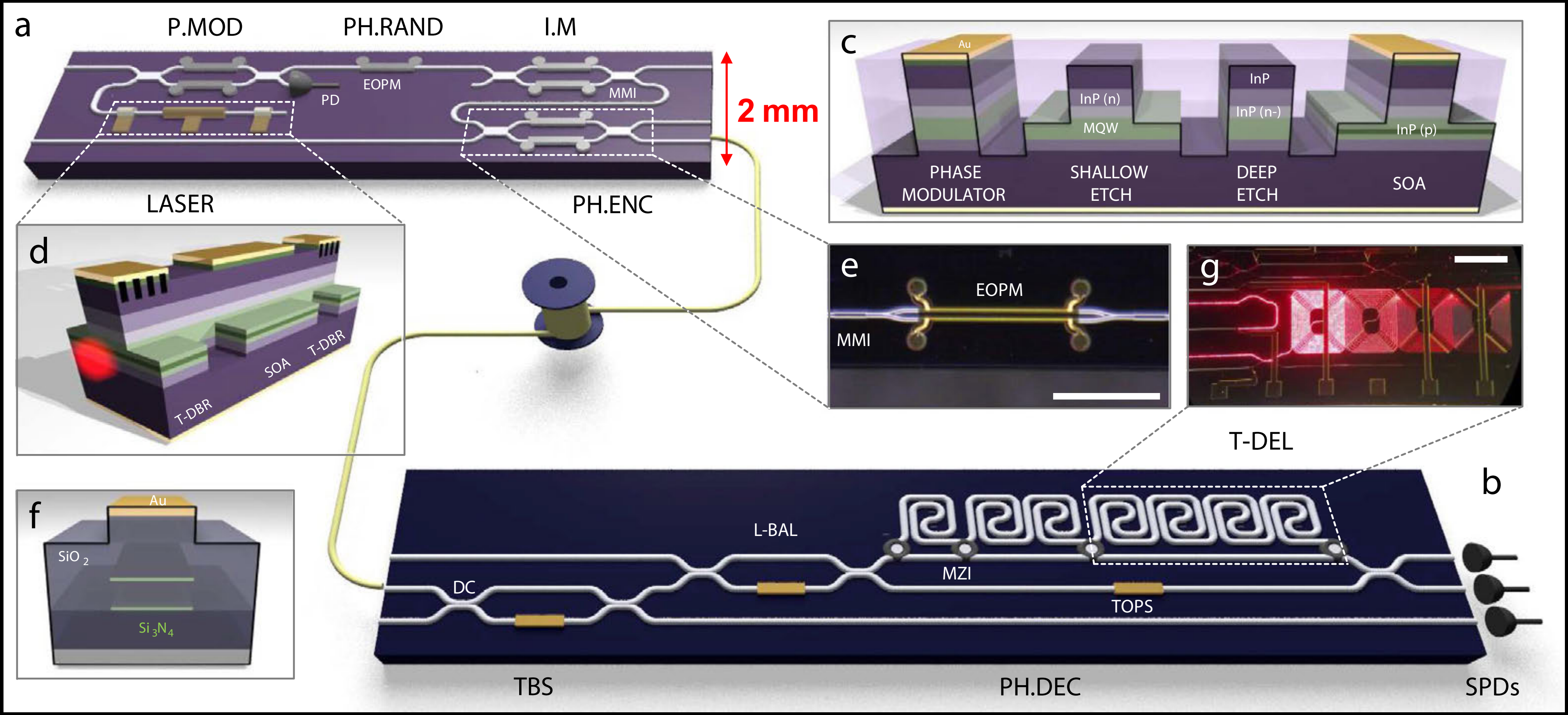
Bob’s polarization analyzer with single-photon detectors



J. G. Rarity, P. C. M. Owens, P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994)

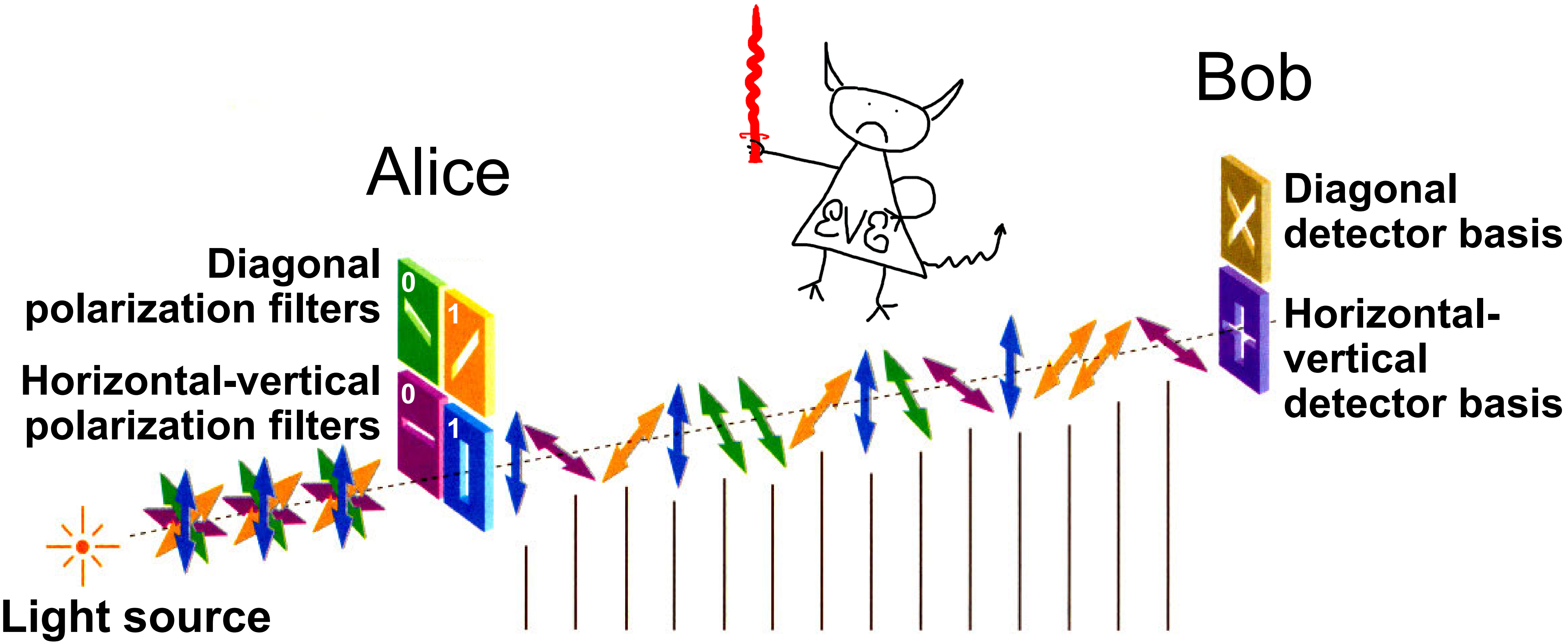
Emerging: integrated optics

Quantum key distribution system



P. Sibson *et al.*, Nat. Commun. **8**, 13984 (2017)
A. W. Elshaari *et al.*, Nat. Photonics **14**, 285 (2020)

Bennett-Brassard 1984 (BB84) QKD protocol



Alice

Bob

Diagonal polarization filters

Horizontal-vertical polarization filters

Diagonal detector basis

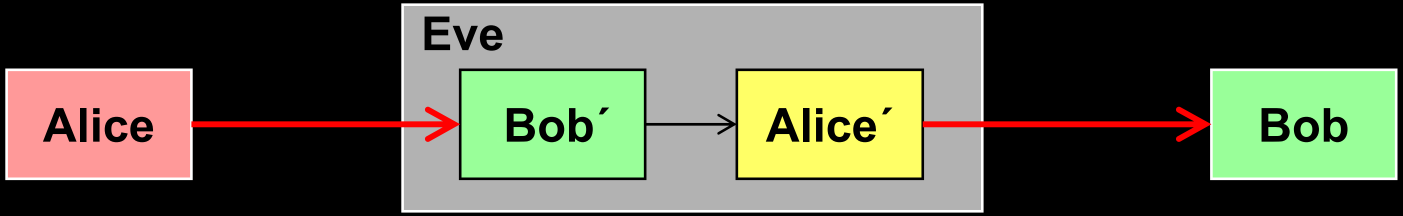
Horizontal-vertical detector basis

Light source

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



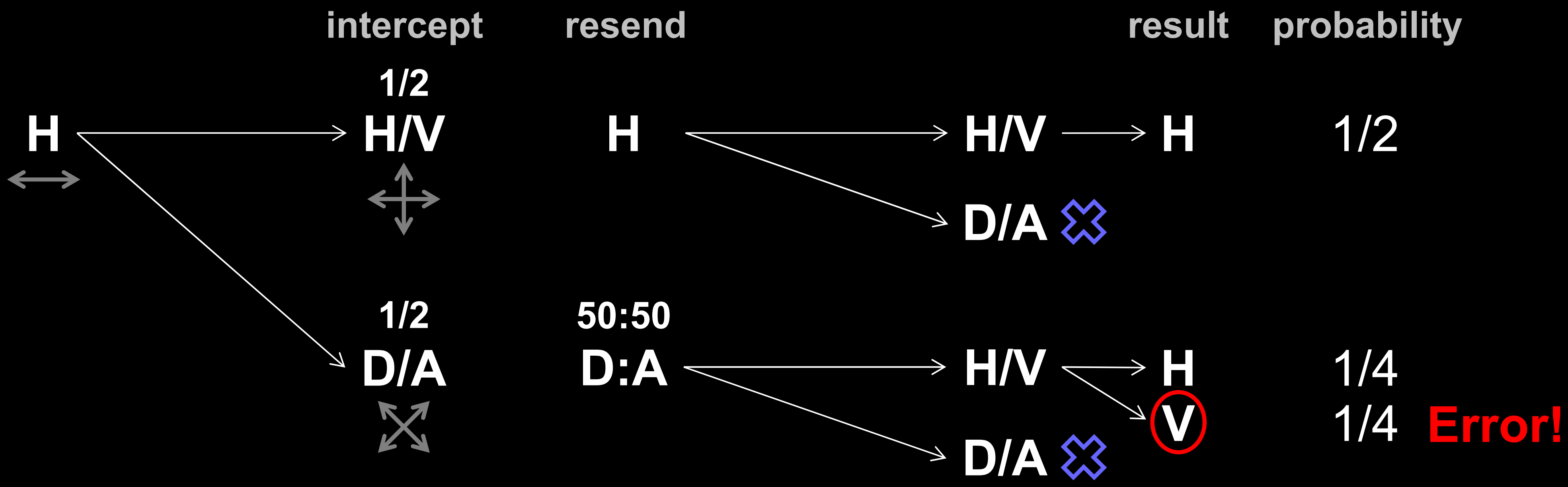
Eve

Alice

Bob´

Alice´

Bob



intercept resend result probability

1/2

H H/V H H/V H 1/2

D/A

1/2 50:50

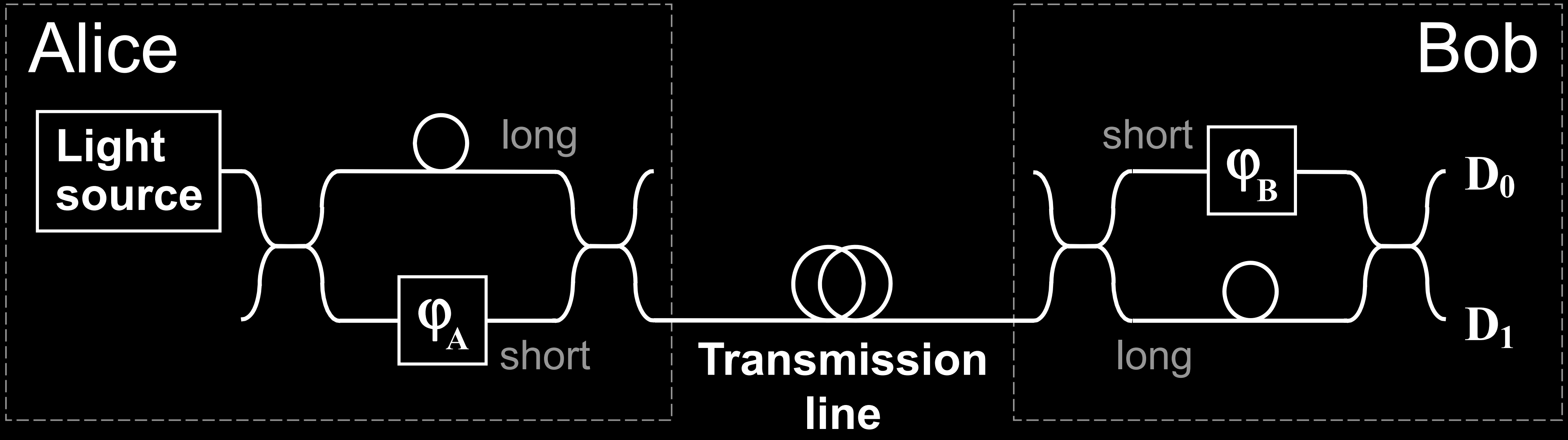
D/A D:A H/V H 1/4

V 1/4 Error!

D/A

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



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

π or $3\pi/2$: 1

Detection basis:

$\varphi_B =$ 0 : X

$\pi/2$: Z

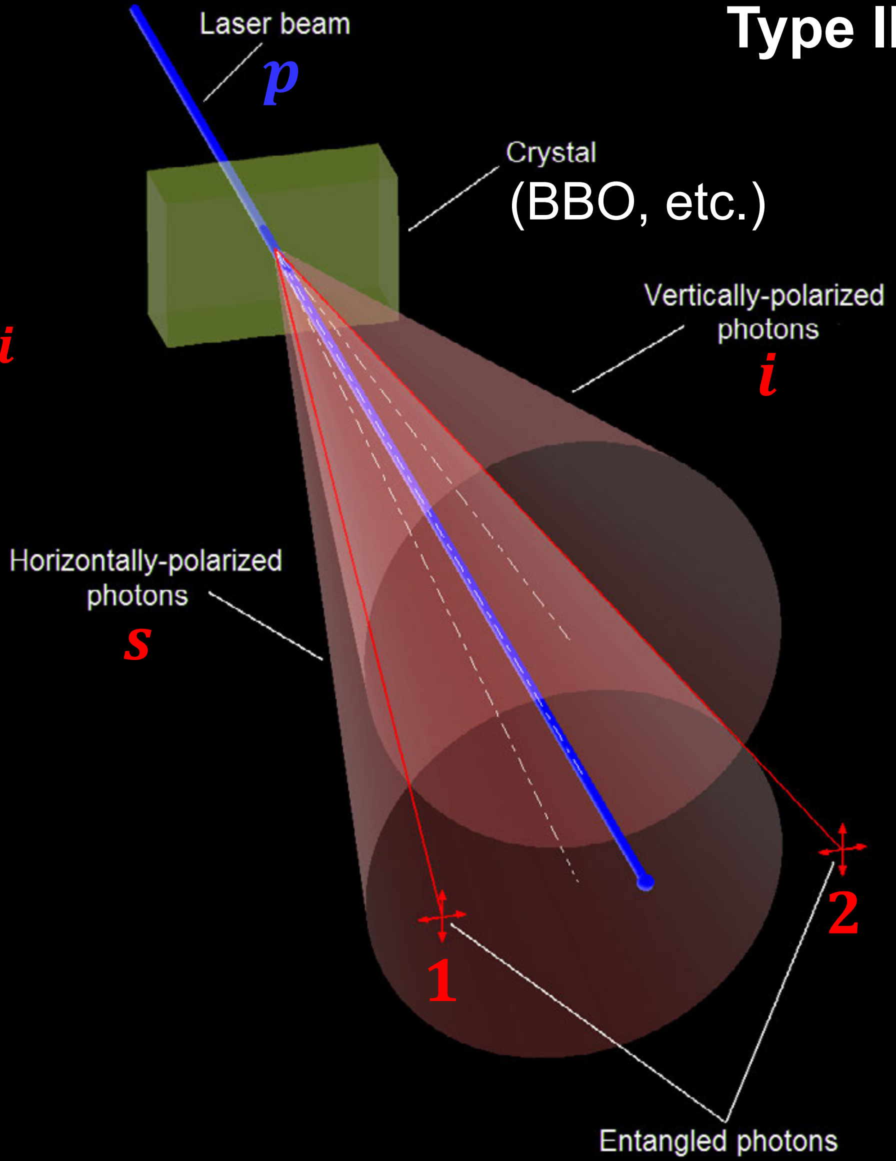
Spontaneous parametric down-conversion

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

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

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

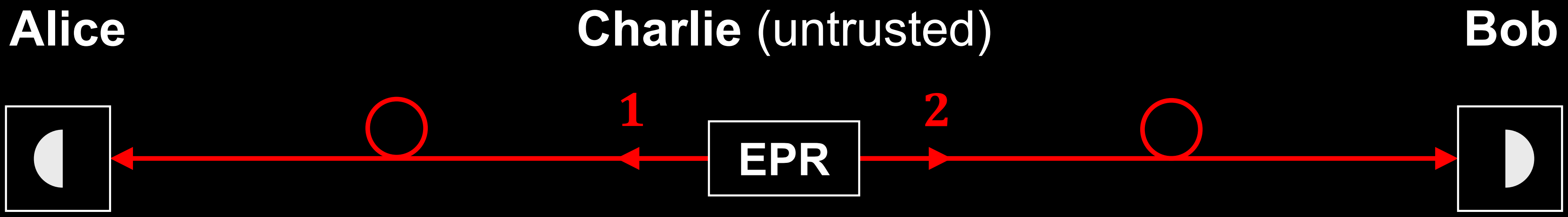
Type II



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

Image reprinted from: Wikipedia

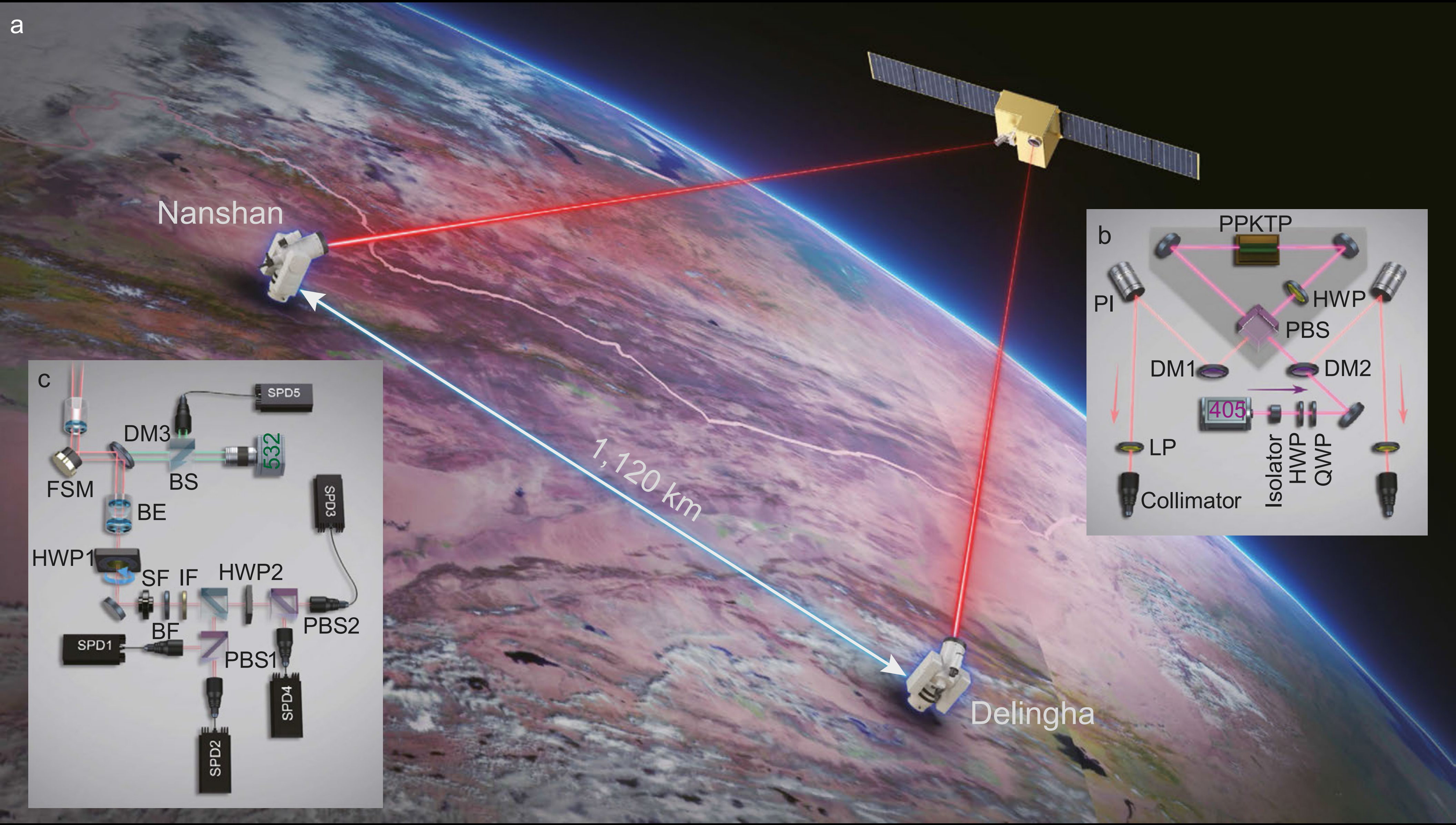
Entangled-pair QKD



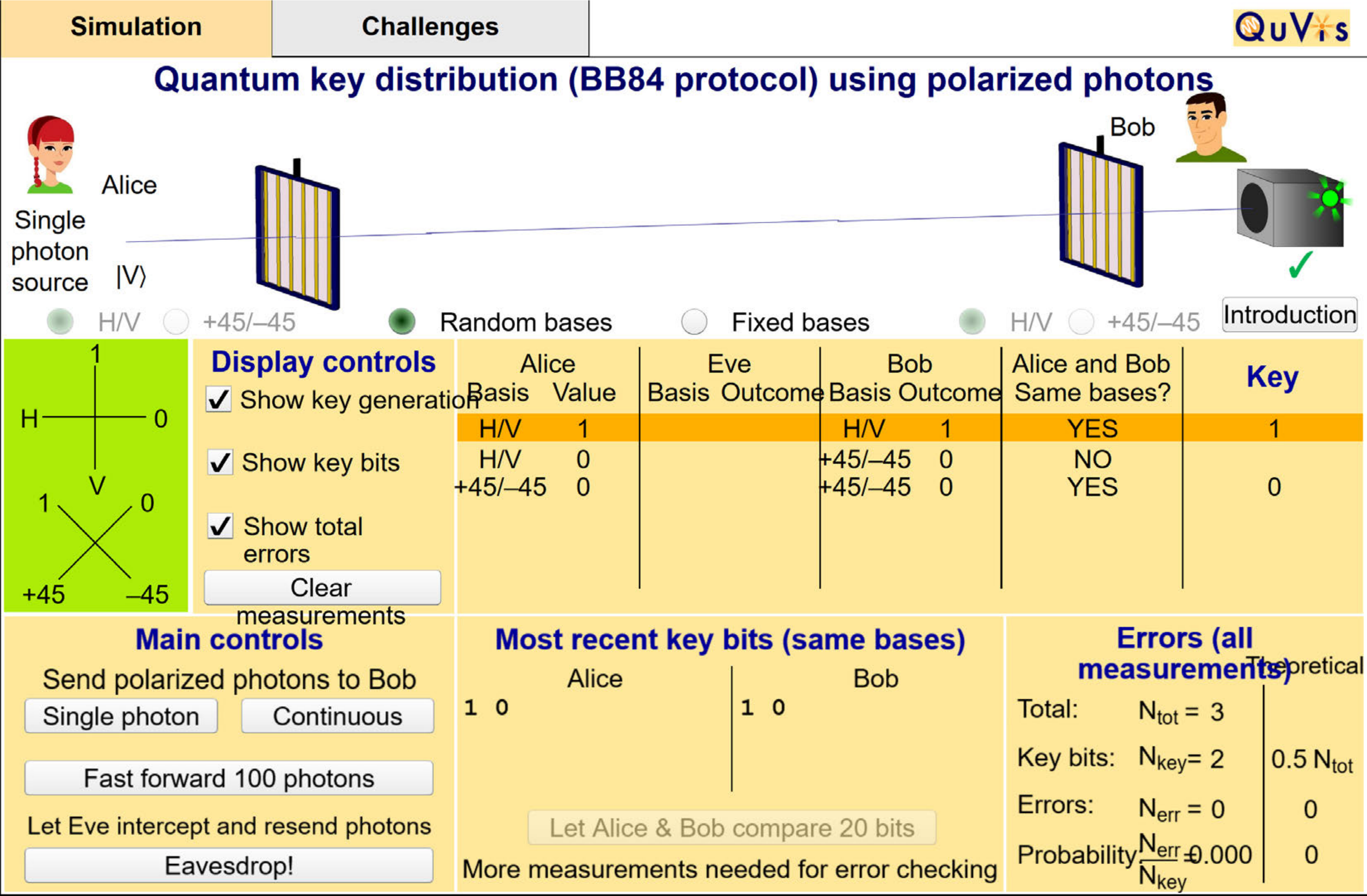
$$|\psi\rangle = (|H_1, V_2\rangle + |V_1, H_2\rangle)/\sqrt{2}$$
$$= (|D_1, A_2\rangle + |A_1, D_2\rangle)/\sqrt{2}$$

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)



Quantum key distribution (BB84 protocol) using polarized photons

● H/V ○ +45/–45 ● Random bases ○ Fixed bases ● H/V ○ +45/–45

Display controls

☑ Show key generation

☑ Show key bits

☑ Show total errors

Alice Basis	Alice Value	Eve Basis	Eve Outcome	Bob Basis	Bob Outcome	Alice and Bob Same bases?	Key
H/V	1			H/V	1	YES	1
H/V	0			+45/–45	0	NO	
+45/–45	0			+45/–45	0	YES	0

Main controls

Send polarized photons to Bob

Let Eve intercept and resend photons

Most recent key bits (same bases)

Alice	Bob
1 0	1 0

More measurements needed for error checking

Errors (all measurements)

		Theoretical
Total:	$N_{tot} = 3$	
Key bits:	$N_{key} = 2$	$0.5\ N_{tot}$
Errors:	$N_{err} = 0$	0
Probability	$\frac{N_{err}}{N_{key}} = 0.000$	0

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

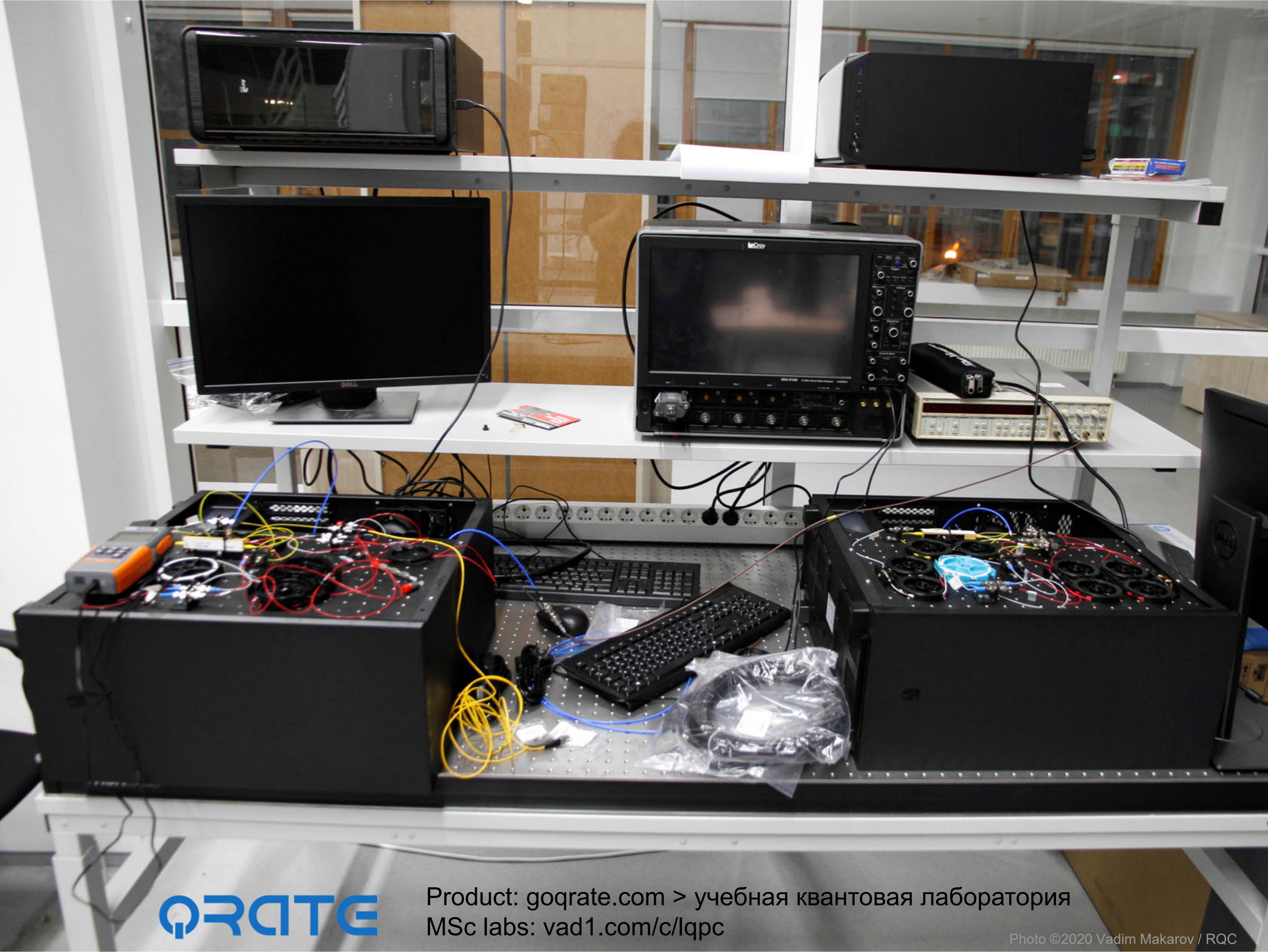
THORLABS

Discovery

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

Manual

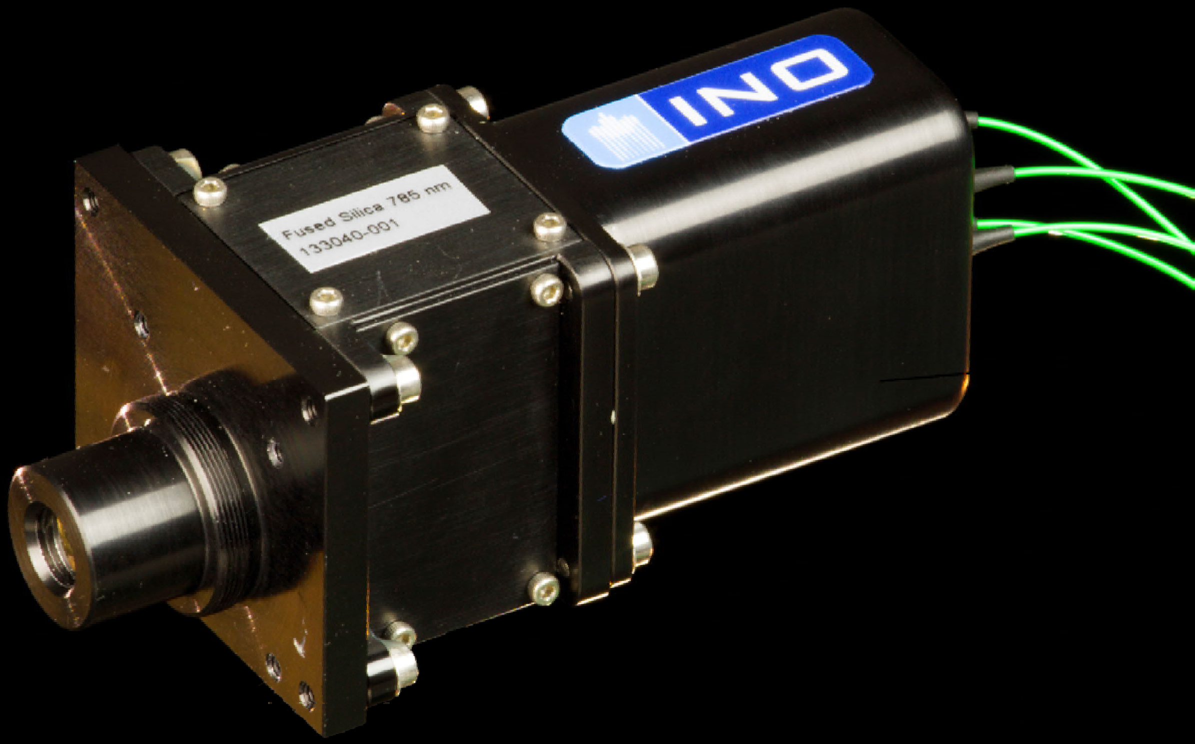
Photo ©2020 Vadim Makarov / RQC



Product: goqrate.com > учебная квантовая лаборатория
MSc labs: vad1.com/c/lqpc

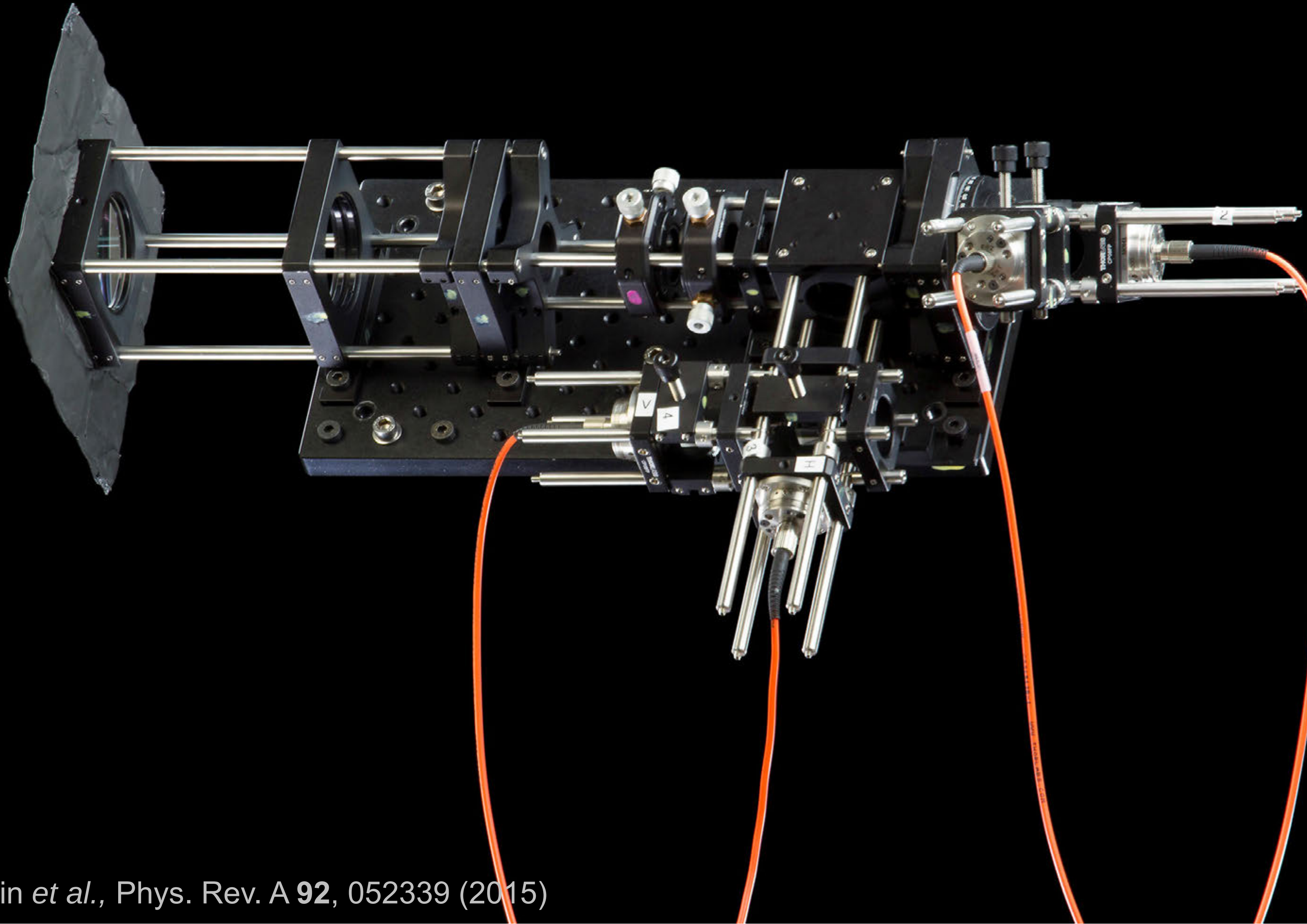
Photo ©2020 Vadim Makarov / RQC

Polarization receiver for satellite



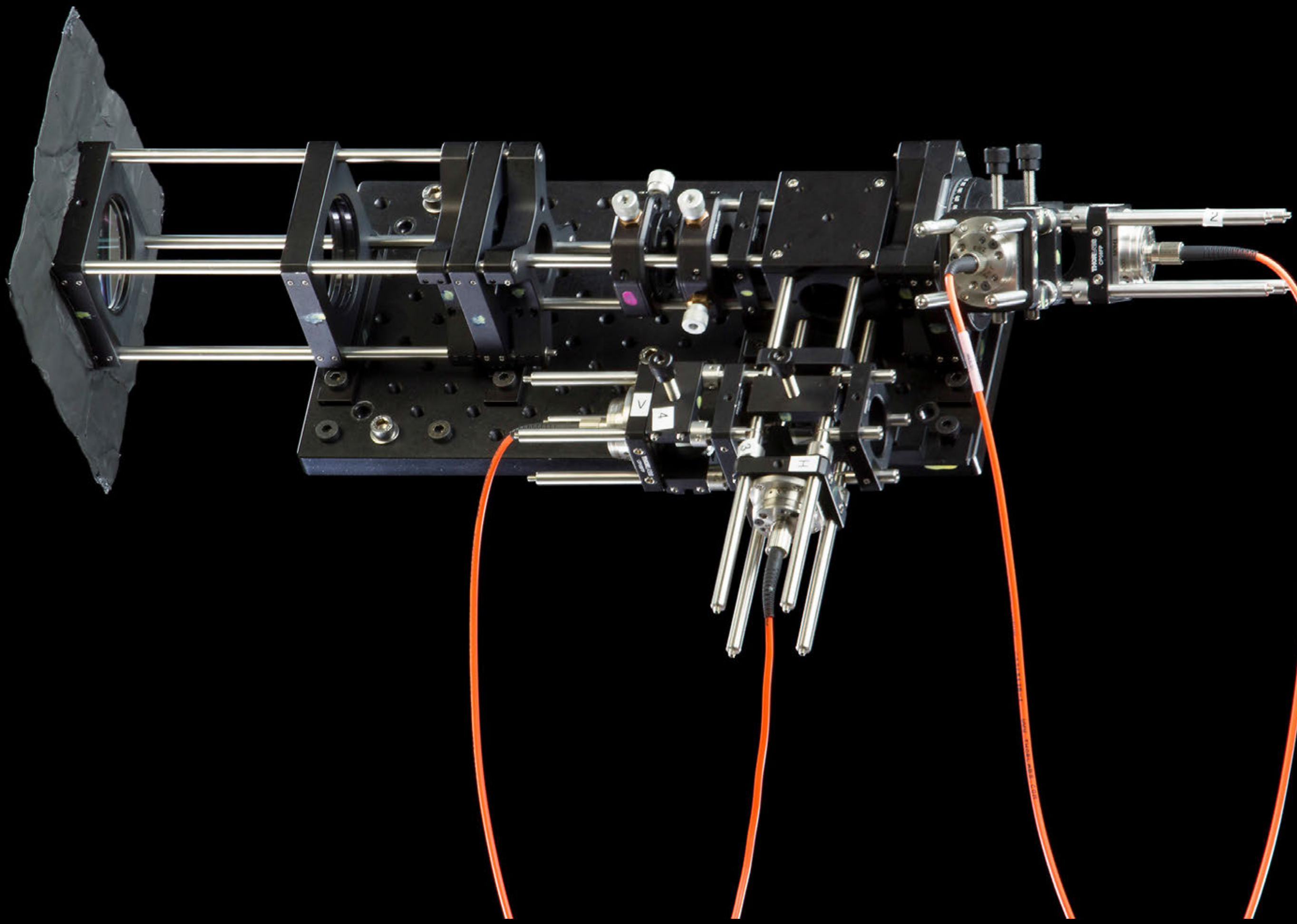
C. J. Pugh *et al.,* Quantum Sci. Technol. **2**, 024009 (2017)

Polarization analyzer



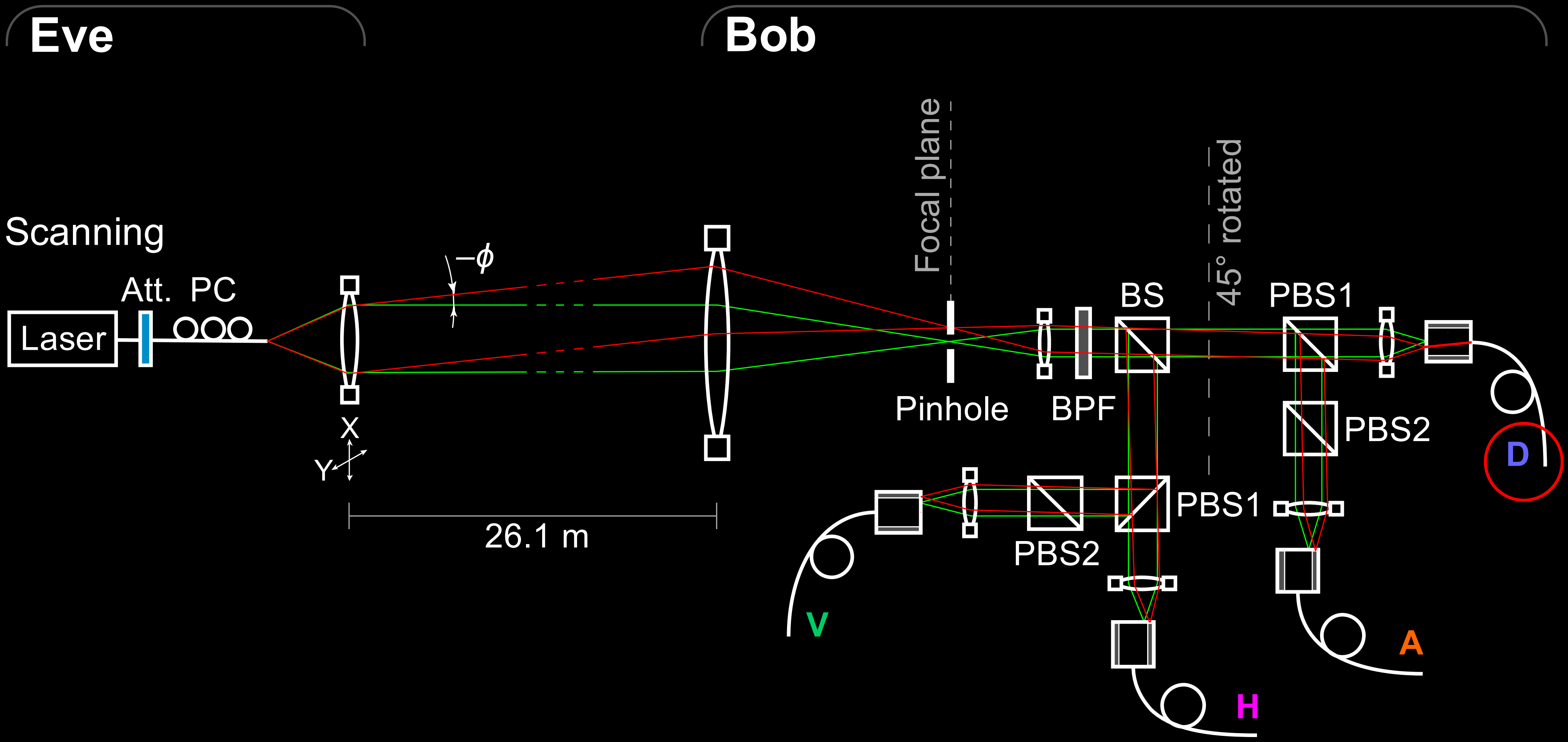
J.-P. Bourgoin *et al.,* Phys. Rev. A **92**, 052339 (2015)

Polarization analyzer



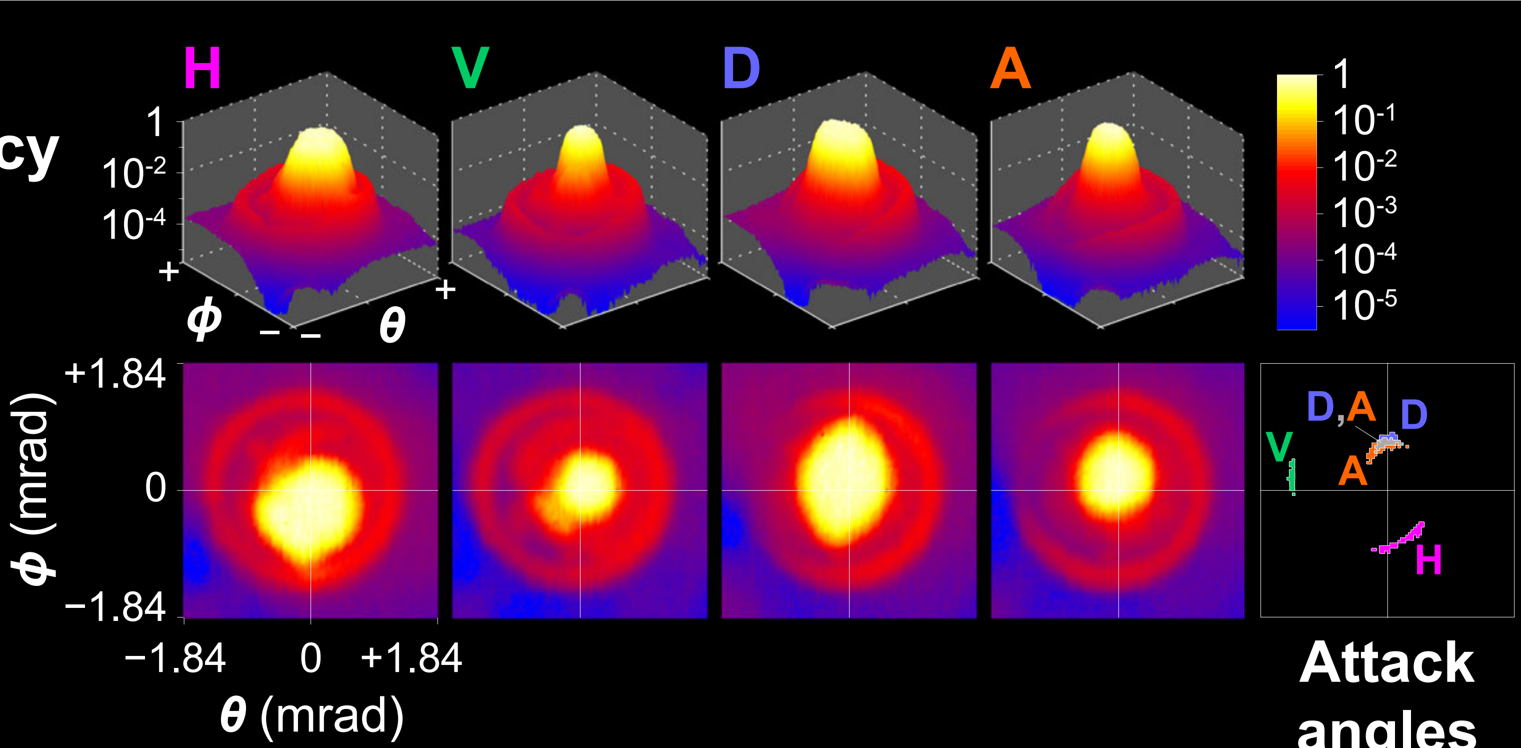
J.-P. Bourgoin *et al.,* Phys. Rev. A **92**, 052339 (2015)

Efficiency mismatch in polarization analyzer



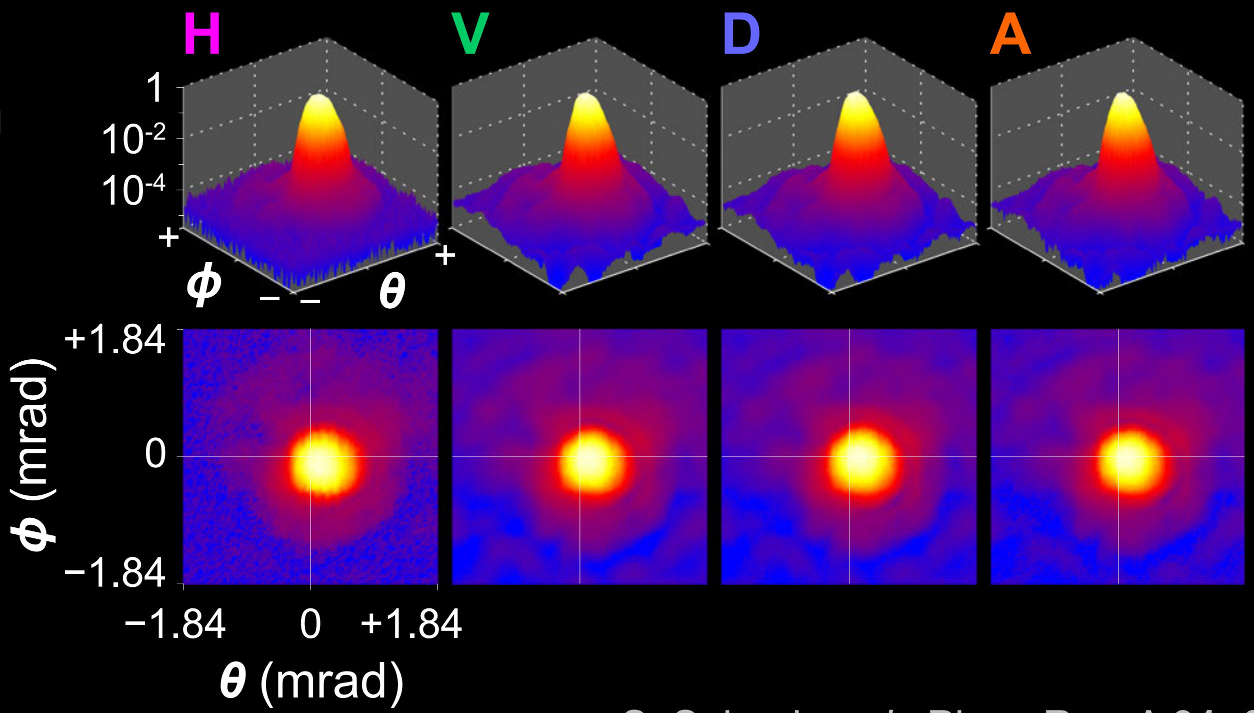
S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015)

Detector efficiency without pinhole



Attack angles

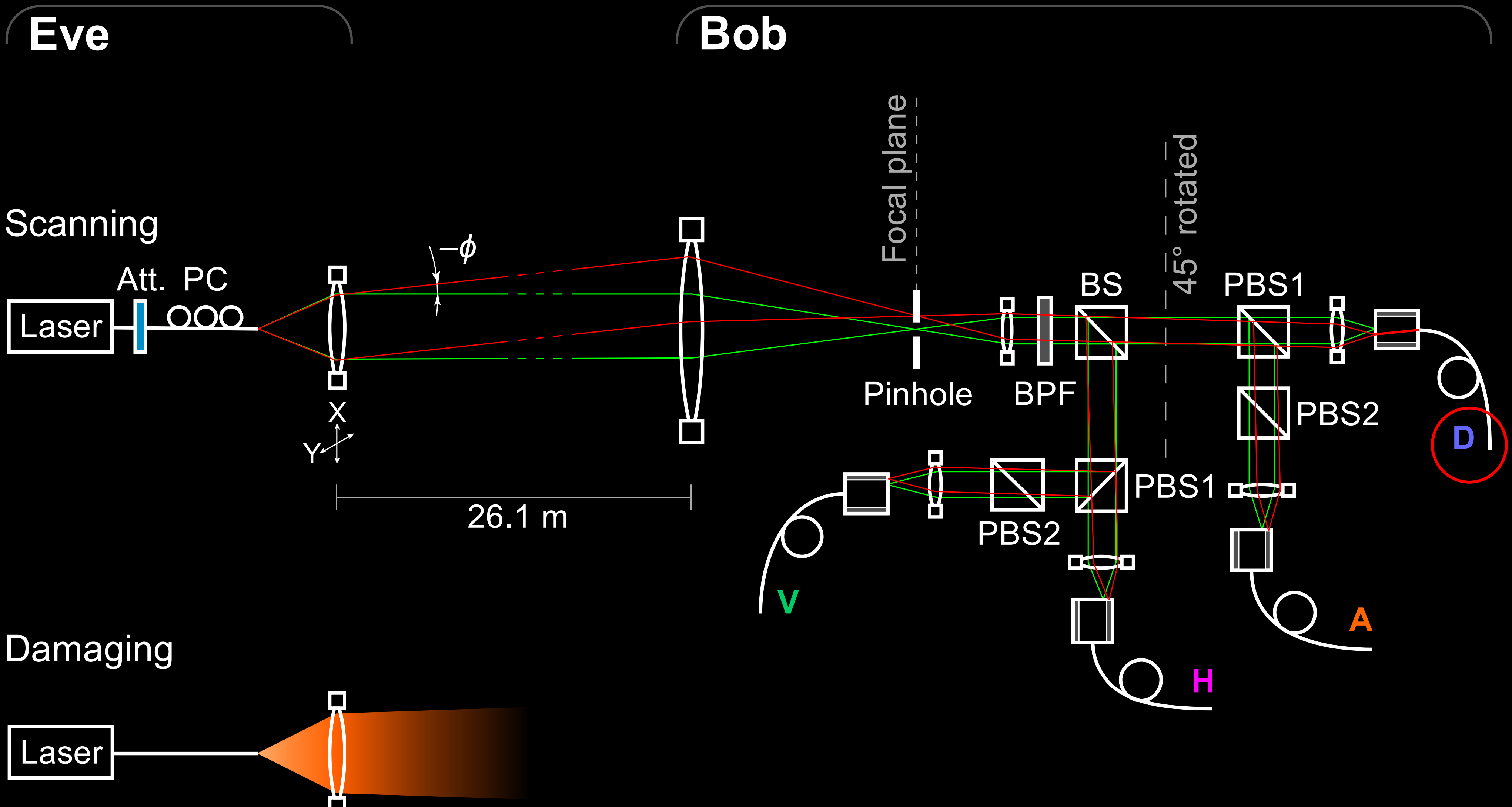
...and with 25 µm diameter pinhole



No attack found

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

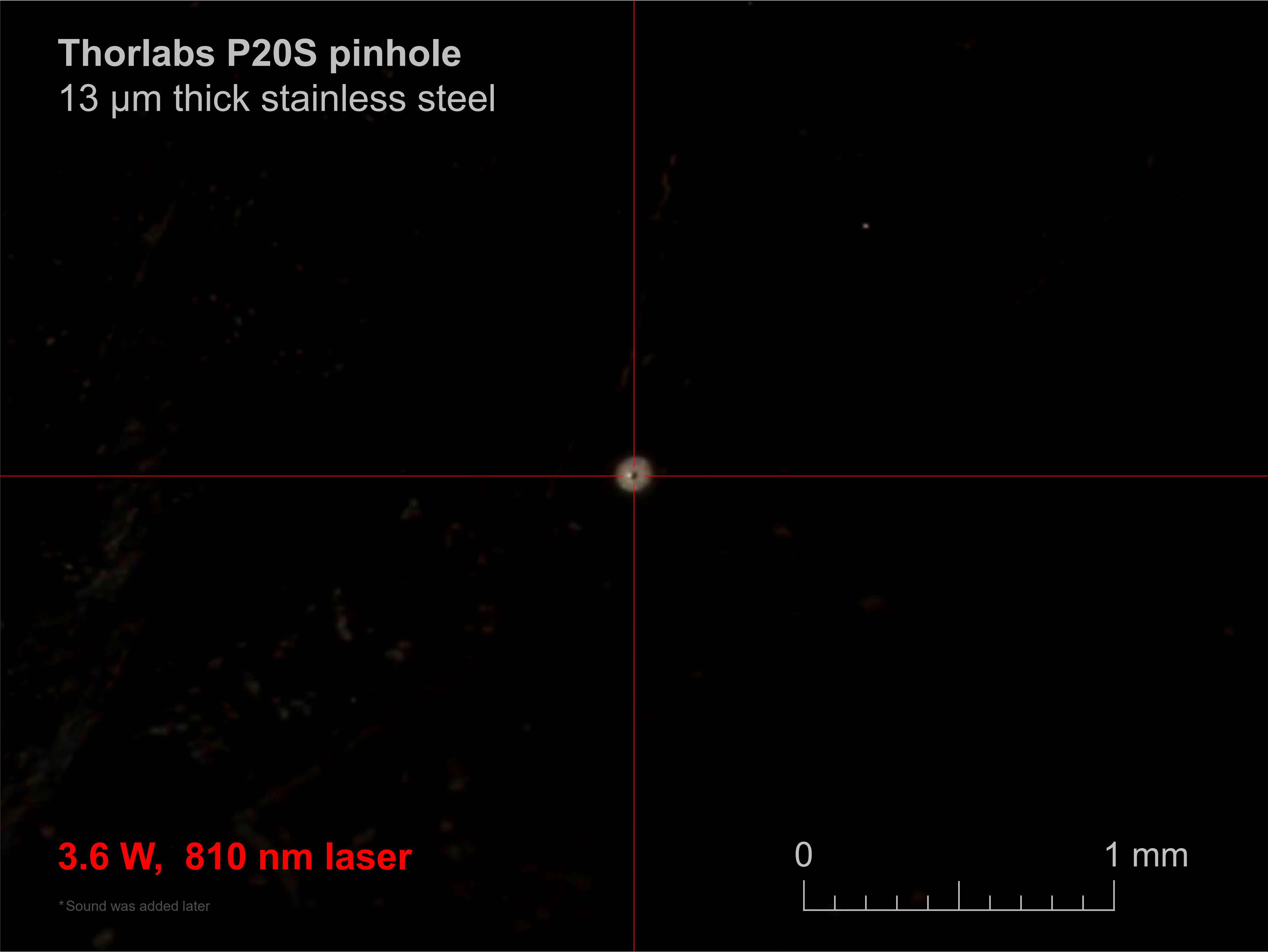
Counter-attack



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

Thorlabs P20S pinhole

13 µm thick stainless steel

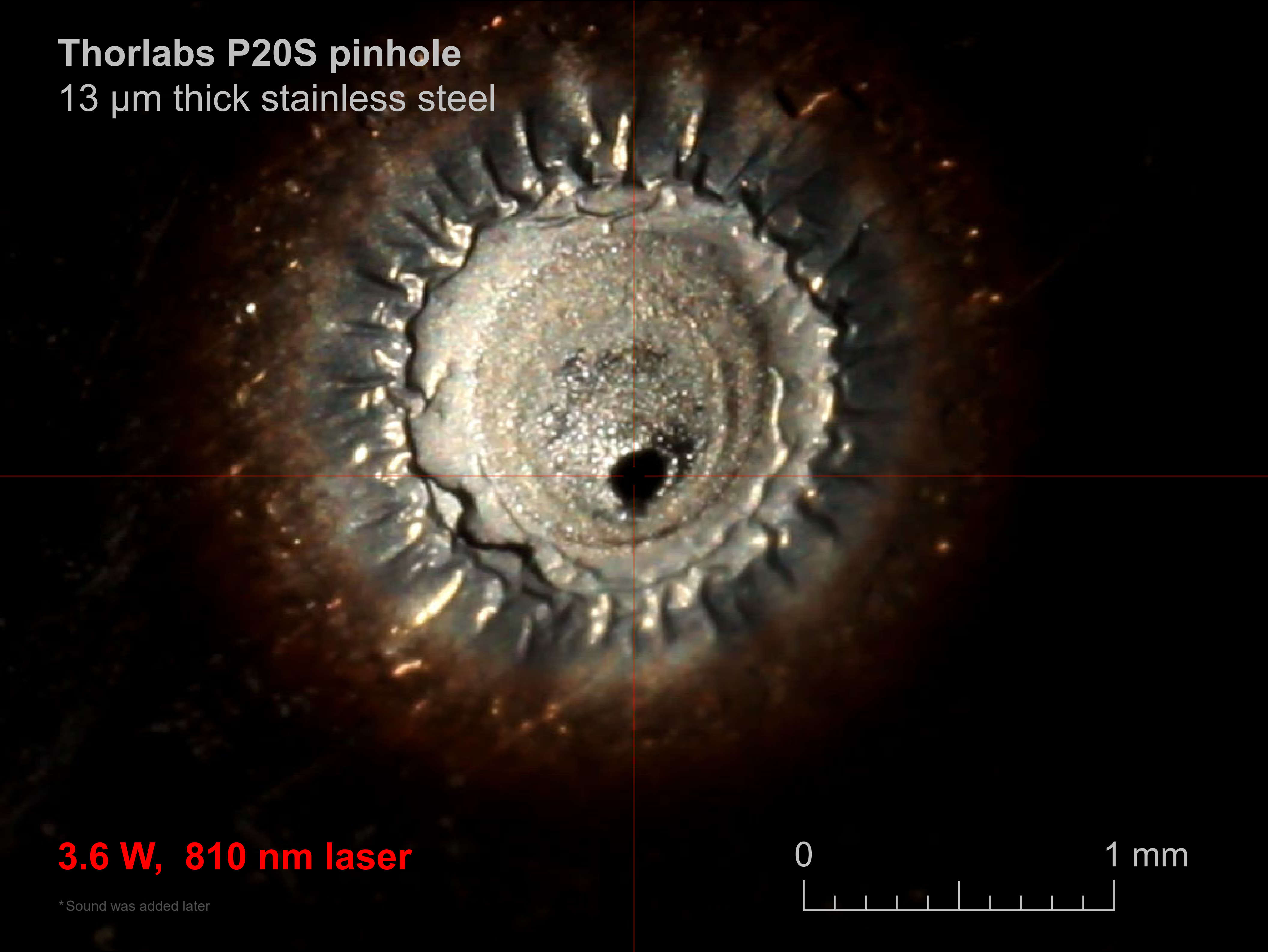


3.6 W, 810 nm laser

*Sound was added later

Thorlabs P20S pinhole

13 µm thick stainless steel



3.6 W, 810 nm laser

*Sound was added later