Vadim Makarov

Quantum cryptography

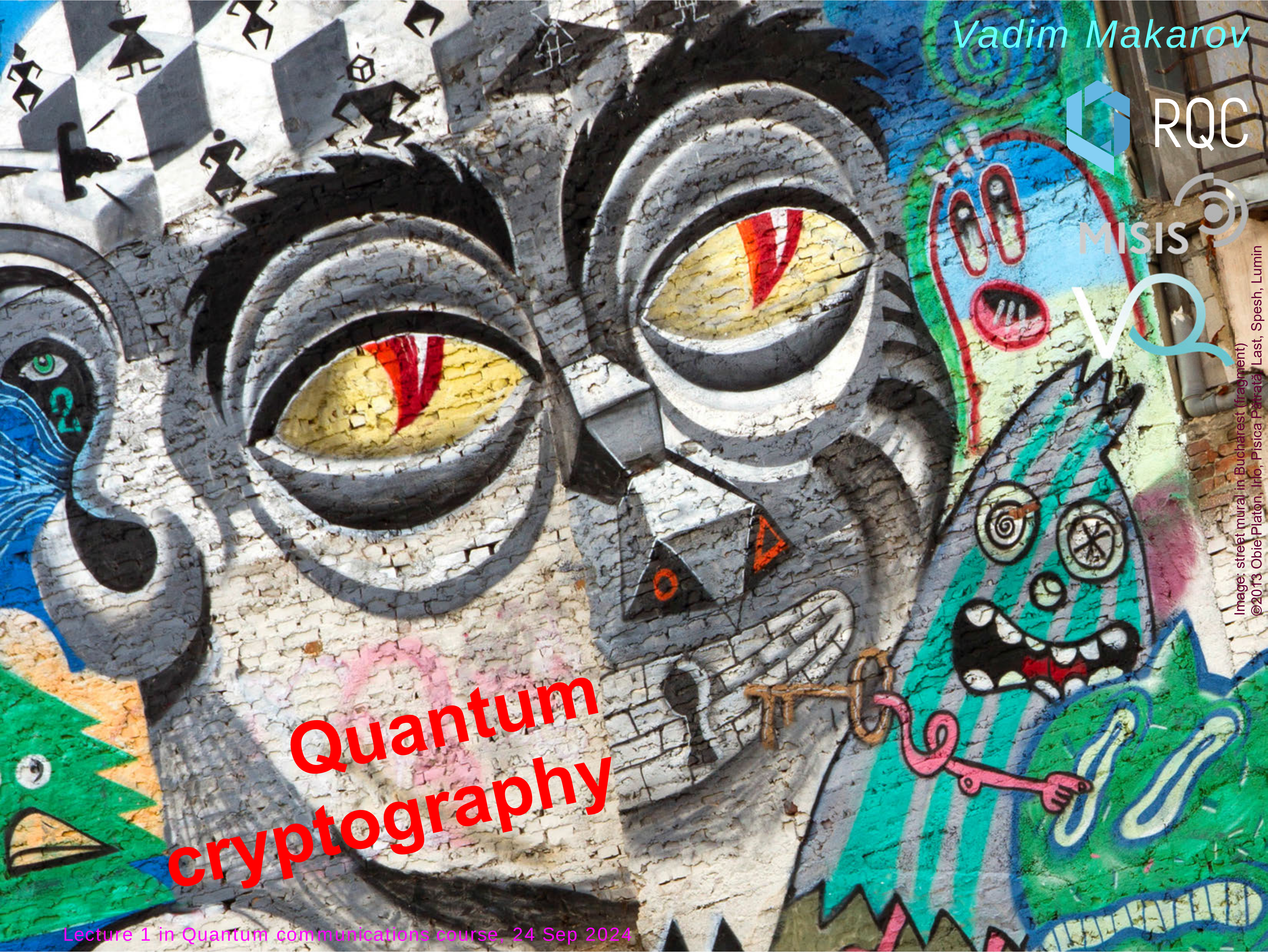


Image: street mural in Bucharest (fragment)

Lecture 1 in Quantum communications course, 24 Sep 2024

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

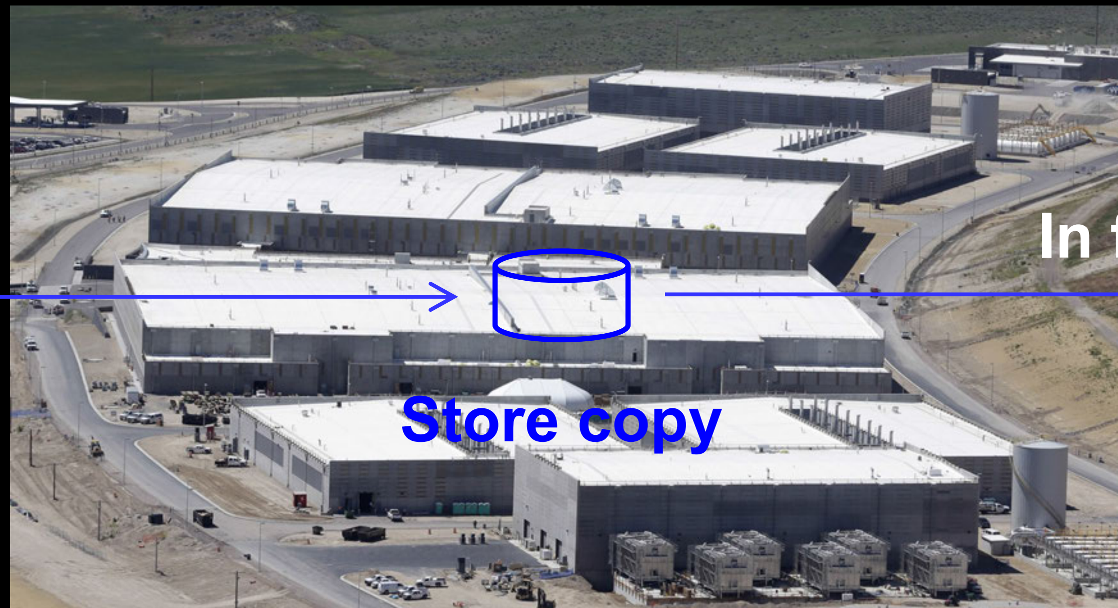


Photo ©2013 AP / Rick Bowmer

In future:

Decrypt

Mosca theorem

y (re-tool infrastructure) | *x* (encryption needs be secure)

z (time to build large quantum computer)

Time

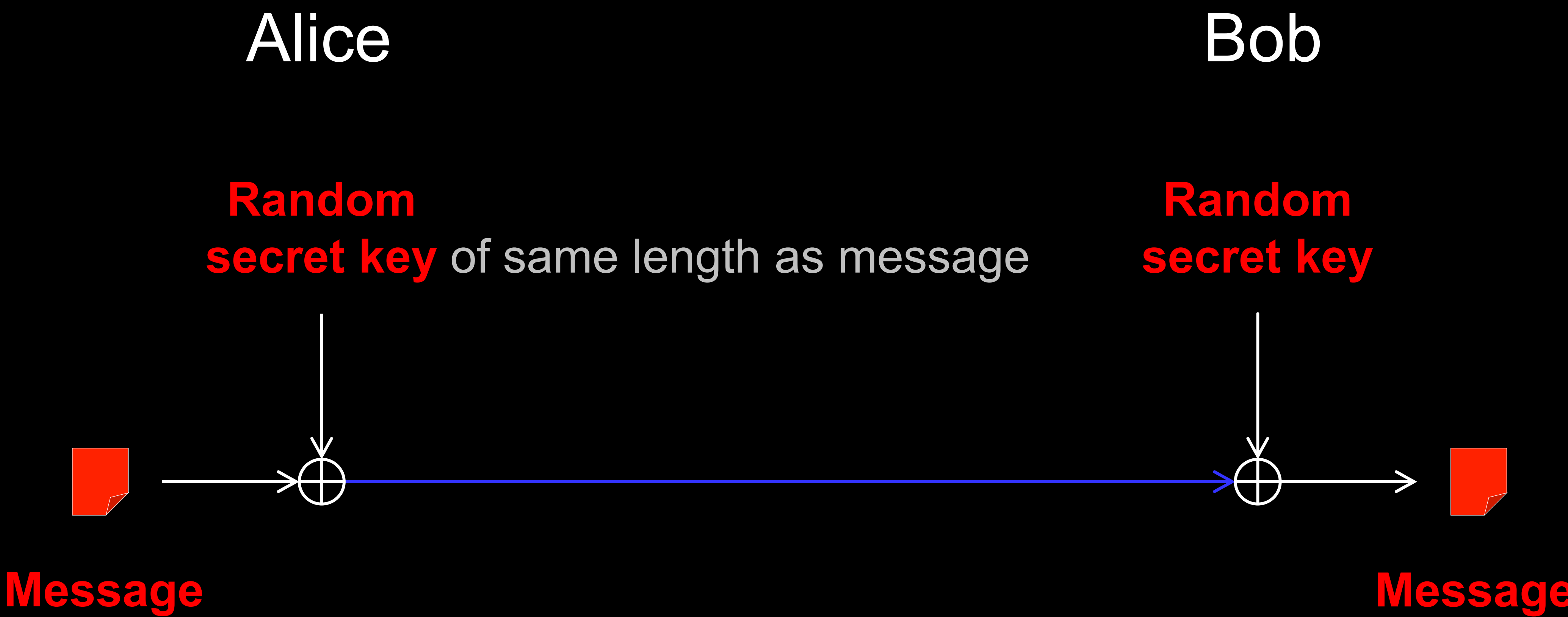
If $x + y > z$, then worry.

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



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)

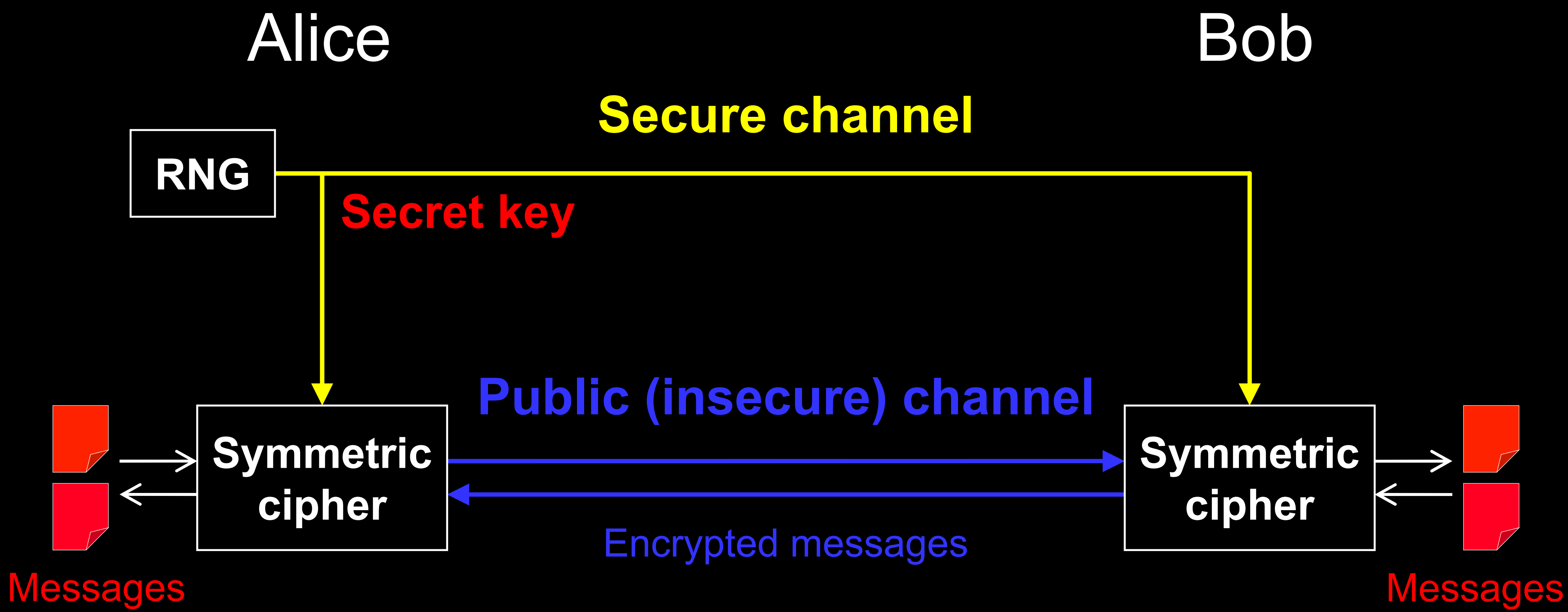
Quantum communication primitives

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, quside.com

Key distribution for encryption



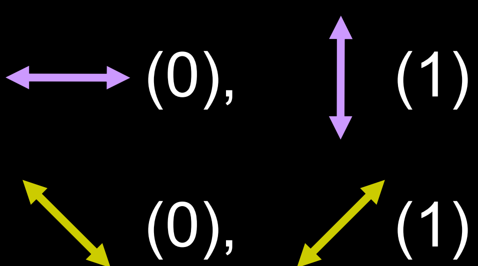
Quantum key distribution transmits secret key by sending quantum states over *open channel.*

Quantum key distribution (QKD)

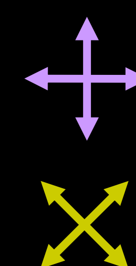
Alice

Bob

Prepares photons



Measures photons



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)

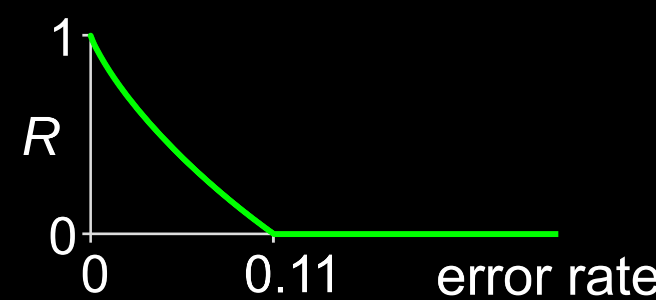
↓

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 → (back to Authentication)

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

Commercial QKD

Classical encryptors:

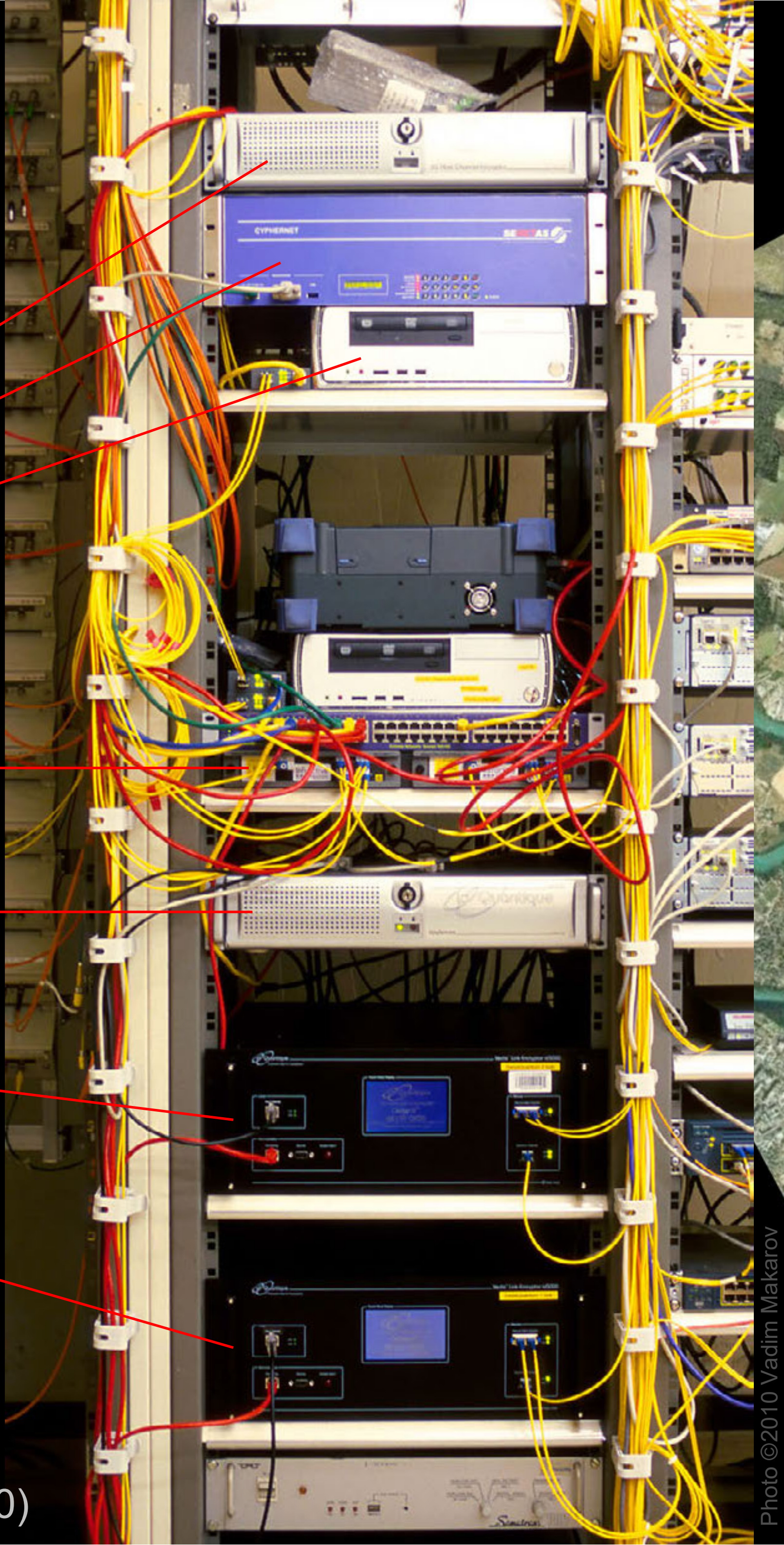
L2, 2 Gbit/s
L2, 10 Gbit/s
L3 VPN, 100 Mbit/s

WDMs

Key manager

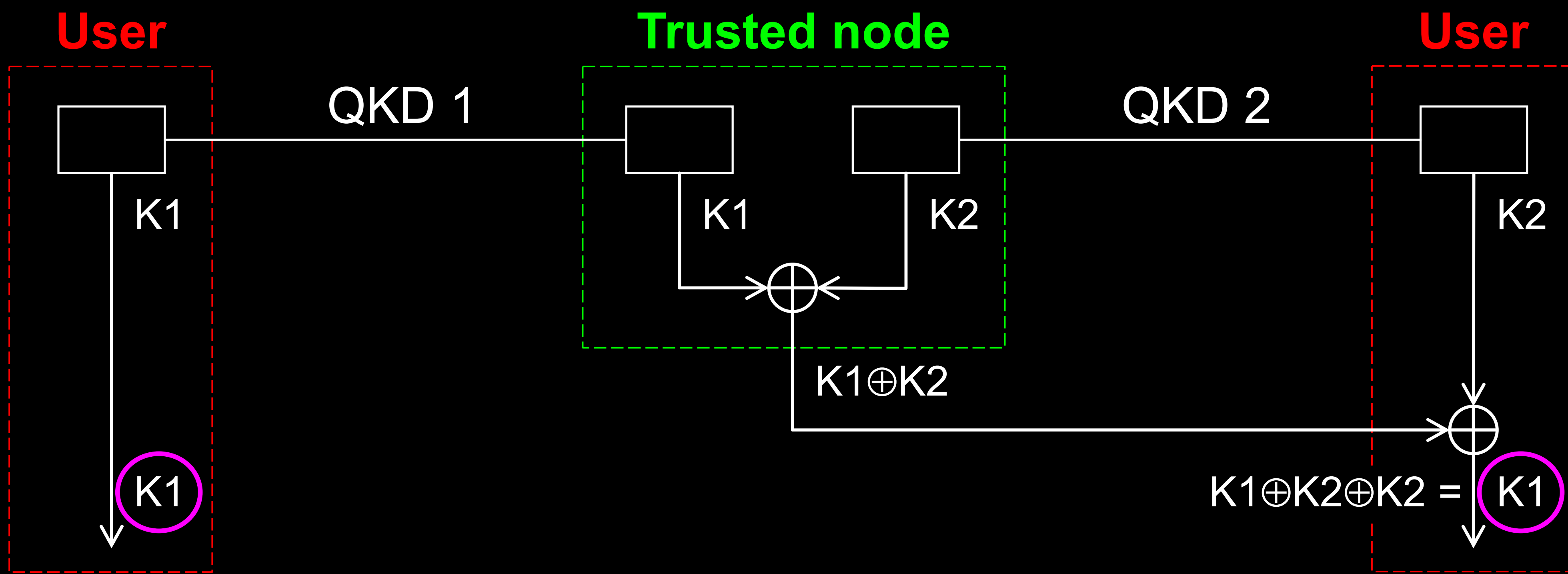
QKD to another node (4 km)

QKD to another node (14 km)

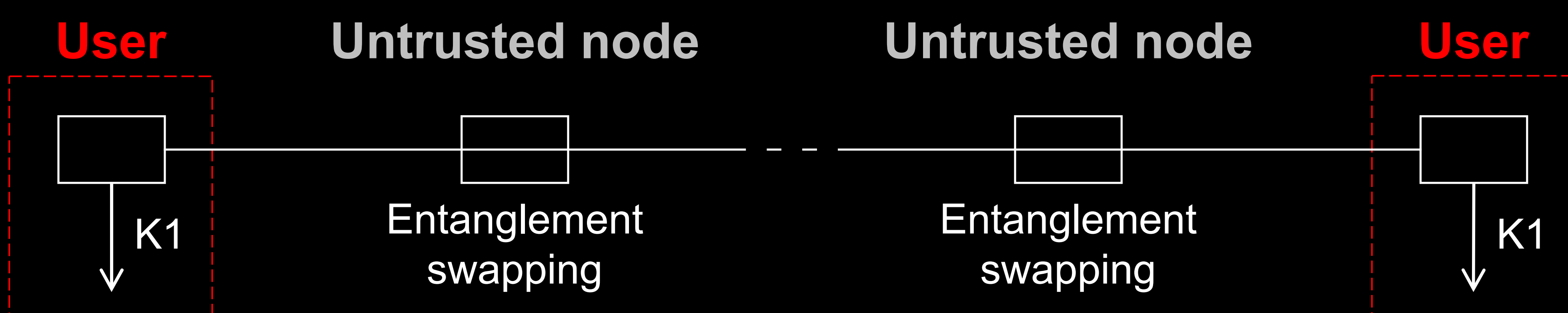


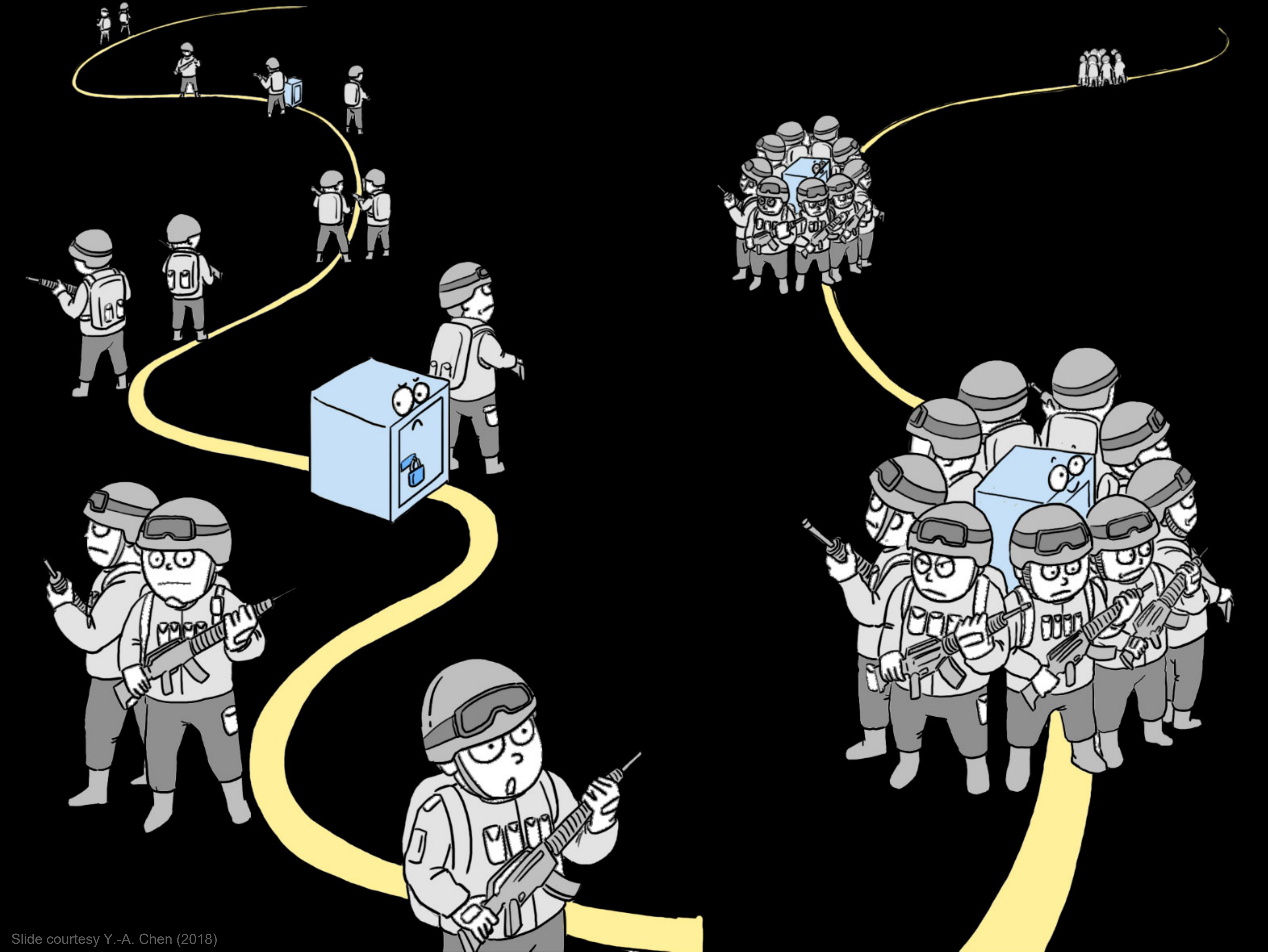
www.swissquantum.com
ID Quantique *Cerberis* system (2010)

Today: trusted-node repeater



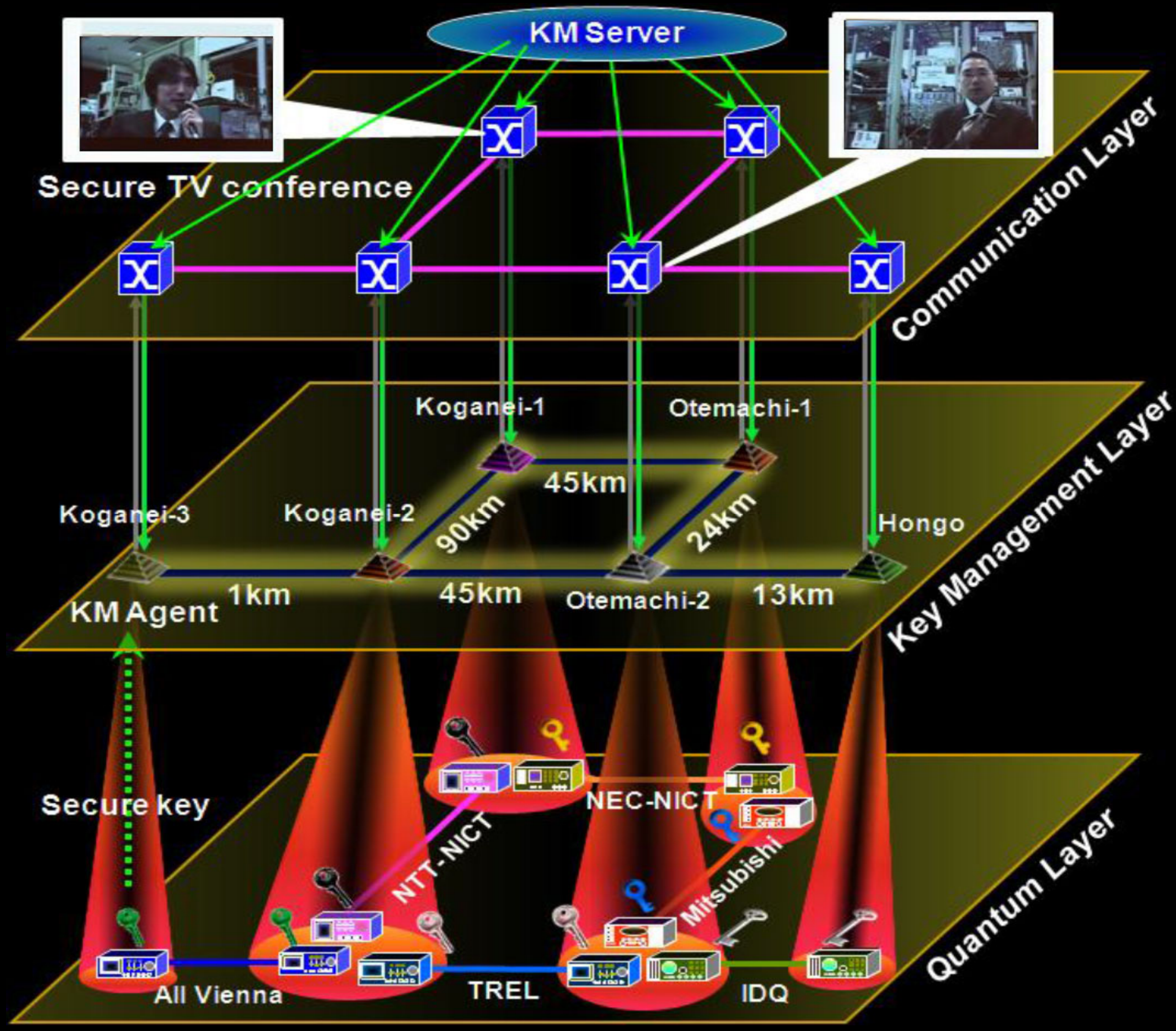
Future: quantum repeater





Slide courtesy Y.-A. Chen (2018)

Trusted-node network



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

China's QKD backbone network (as of July 2023)

North-south backbone	Length (km)
Beijing–Shanghai (completed in 2017)	2032
Beijing–Wuhan	1723
Wuhan–Guangzhou	1400
Hangzhou–Xiamen	1400
Yue–Gang–Ao	375
Beijing–Haerbin	1520
East-west backbone	
Wuhan–Hefei	592
Shanghai–Hangzhou–Hefei	830
Wuhan–Chongqing–Chengdu	1635
Jinan–Qingdao	533
Haikou–Wenchang	110
Total	**12150**

Source: CAS Quantum Net

Metropolitan QKD network in Hefei

Source: QuantumCTek

Metropolitan QKD network in Hefei

Source: QuantumCTek

Photo ©2023 Vadim Makarov

Printed circuit board assembly lines

Assembling quantum computers

Photo ©2023 Vadim Makarov

Production ward

Photo ©2023 Vadim Makarov

QKD testing stations

Environmental testing chambers

QKD burn-in racks and units ready for shipment

QKD packaging line

QKD repair-and-service ward

QKD repair-and-service ward

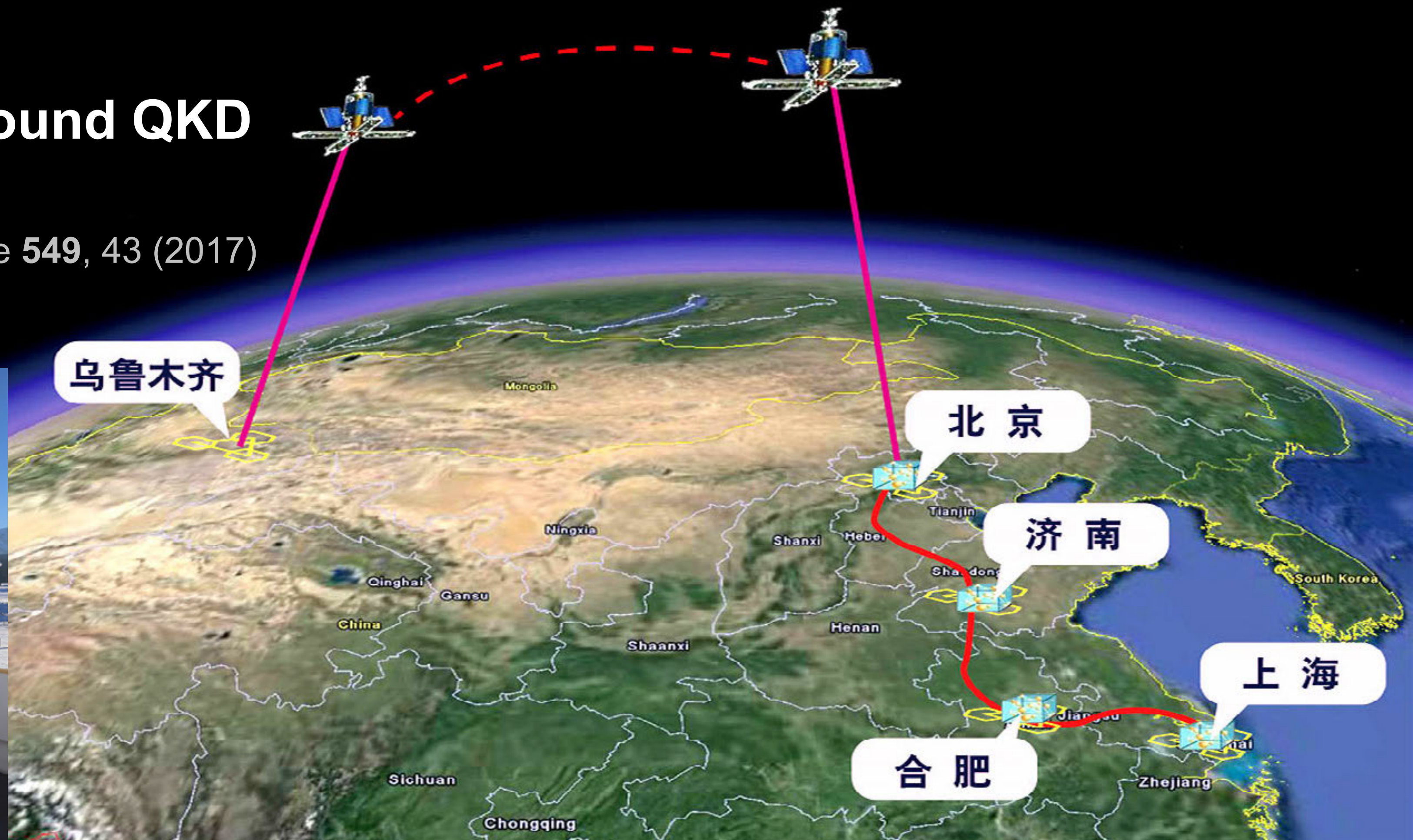
Global quantum key distribution

Video ©2012 IQC / group of T. Jennewein

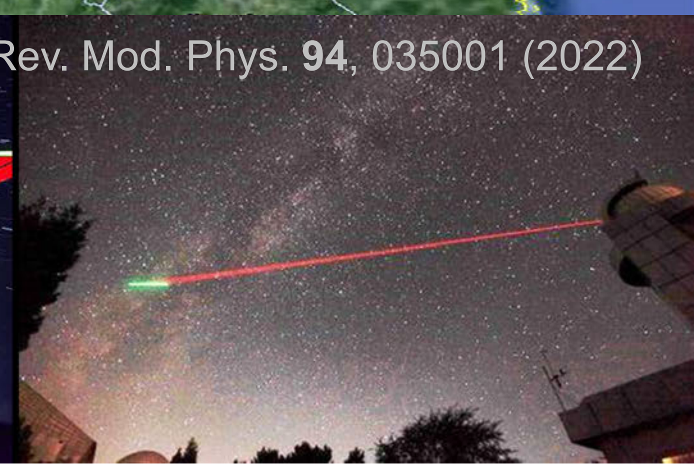
Hybrid QKD network

Satellite-to-ground QKD at 1 kbit/s

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

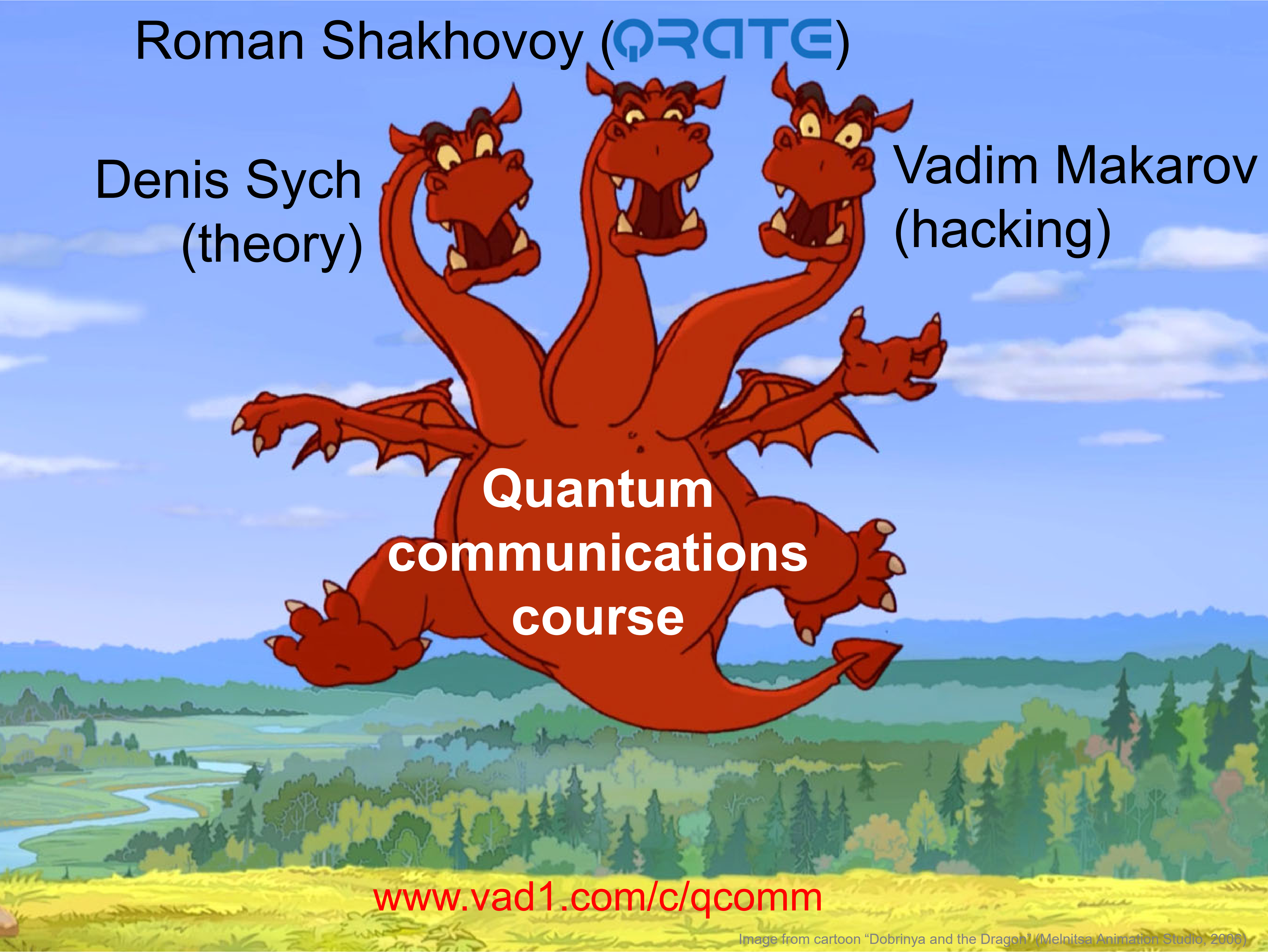


Review: C.-W. Lu, Y. Cao, C.-Z. Peng, J.-W. Pan, Rev. Mod. Phys. **94**, 035001 (2022)



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

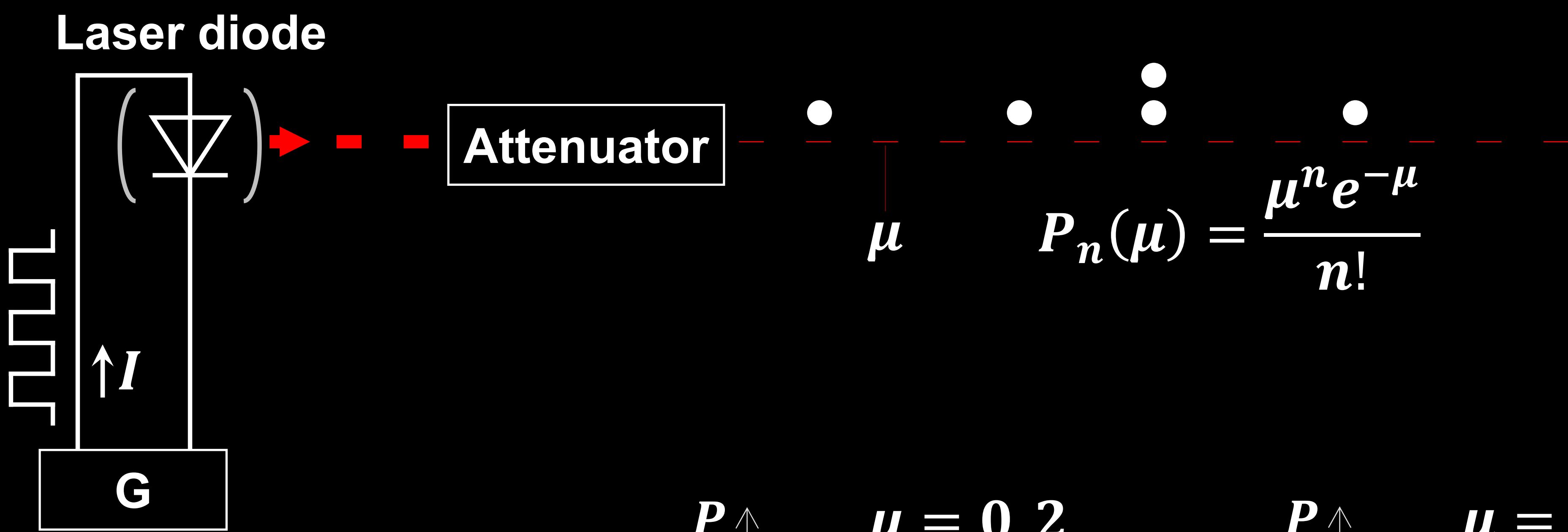
Ground station in Zvenigorod communicates with Micius satellite (18 Jan 2021)


Roman Shakhovoy (QRATE)
Denis Sych
(theory)
Vadim Makarov
(hacking)
Quantum
communications
course
www.vad1.com/c/qcomm
Image from cartoon “Dobrinya and the Dragon” (Melnitsa Animation Studio, 2006)

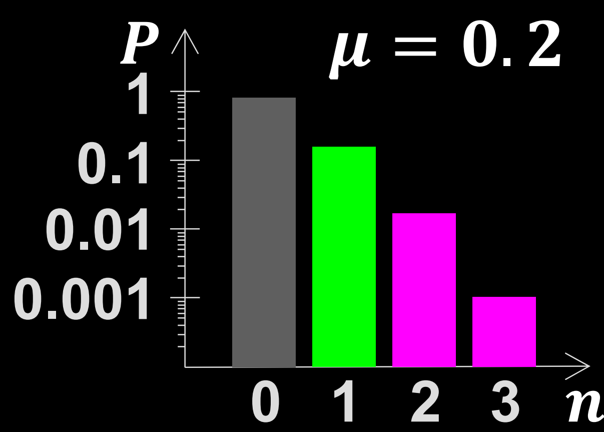
Components of quantum-optical systems

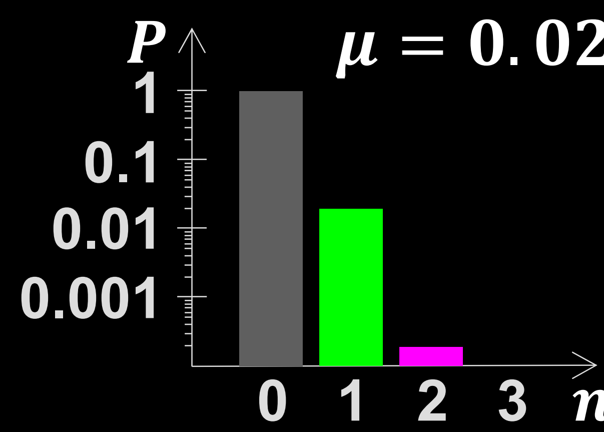
Photon sources ____ **Transmission channels** ____ **“Processing” elements** ____ **Photon detectors**

Attenuated laser source



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





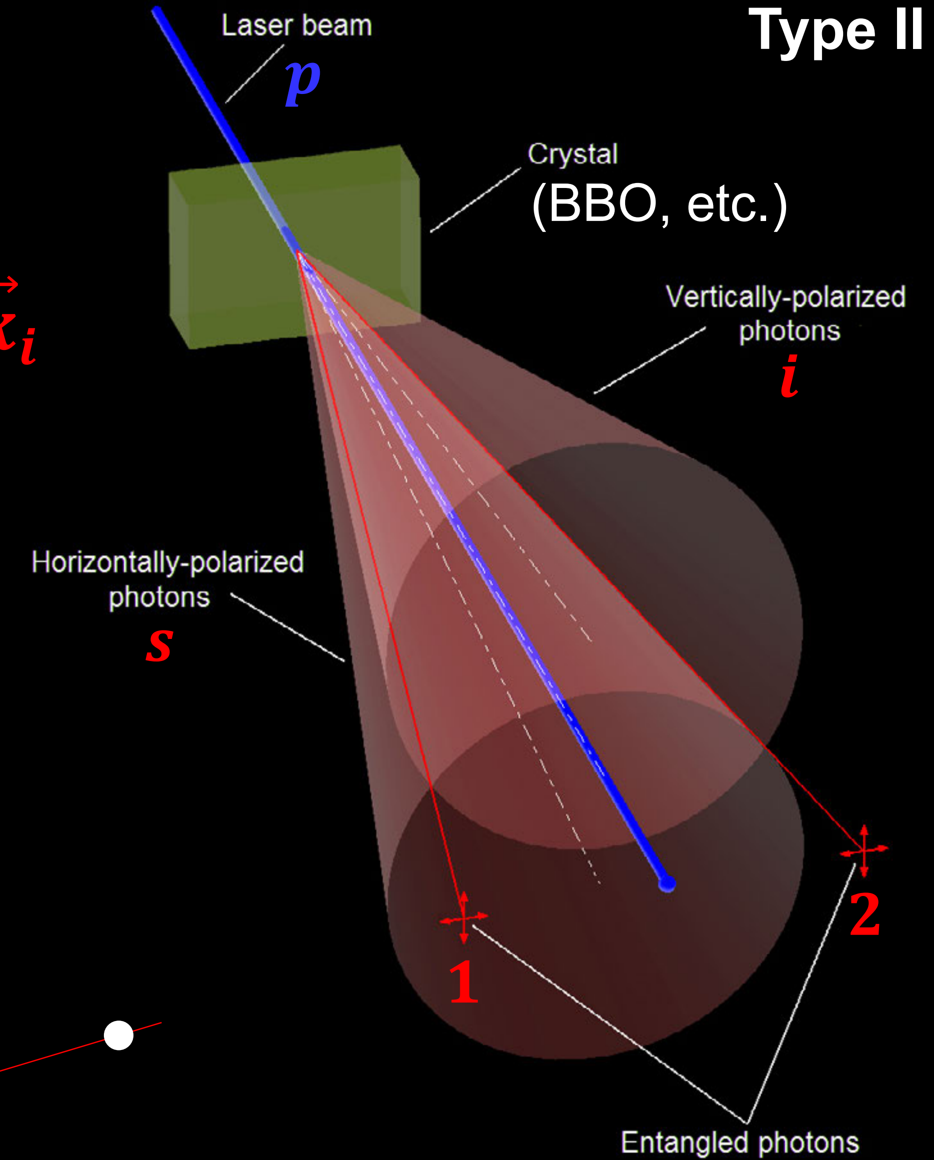
S. J. van Enk, C. A. Fuchs, arXiv:quant-ph/0111157

Spontaneous parametric down-conversion

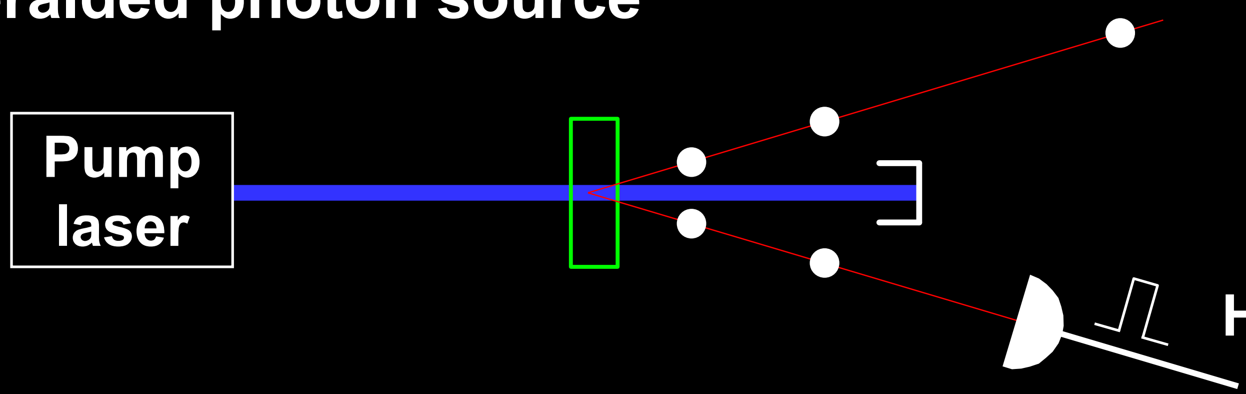
Energy conservation: $\omega_p = \omega_s + \omega_i$

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

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



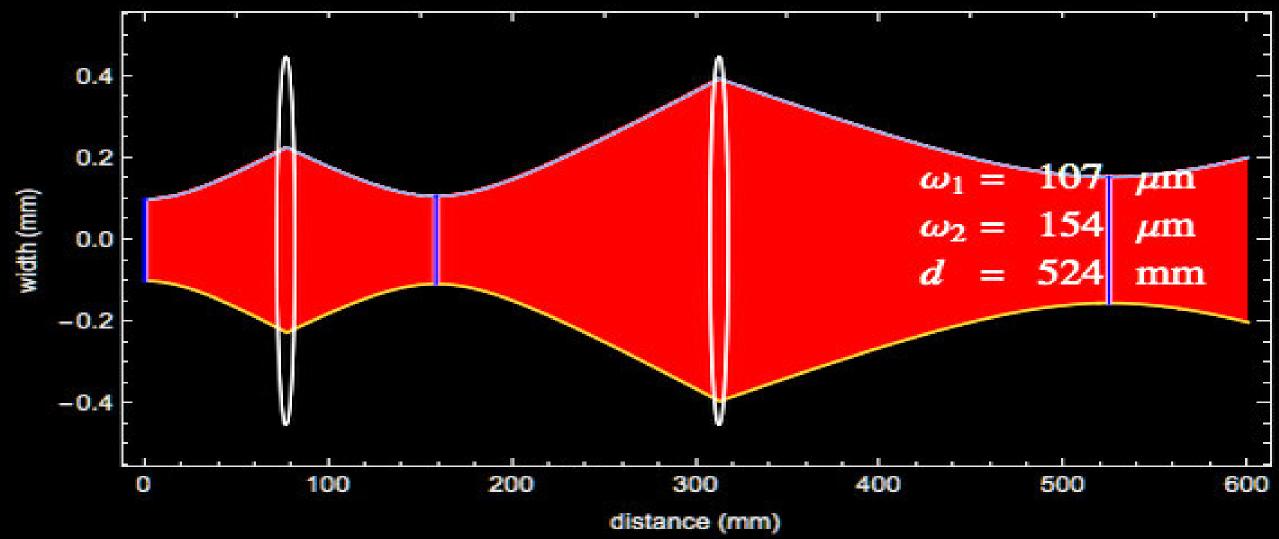
Heralded photon source

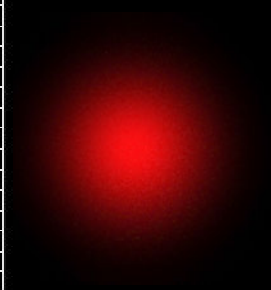


P. G. Kwiat *et al.*, Phys. Rev. Lett. **75**, 4337 (1995)

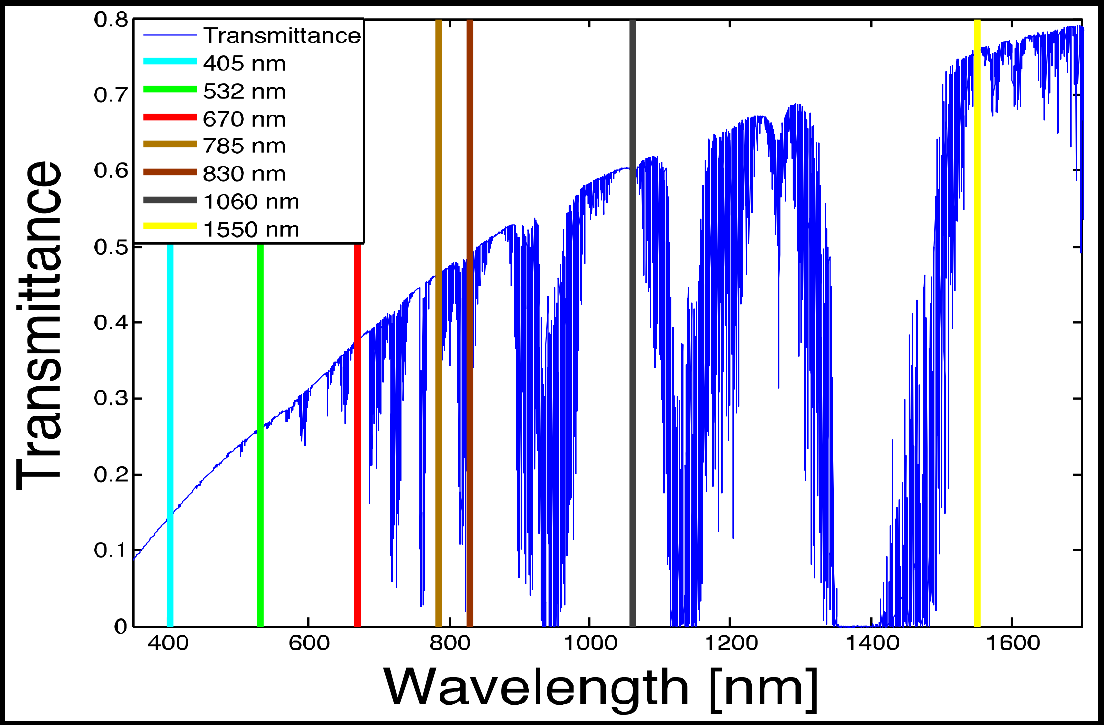
Transmission in free space

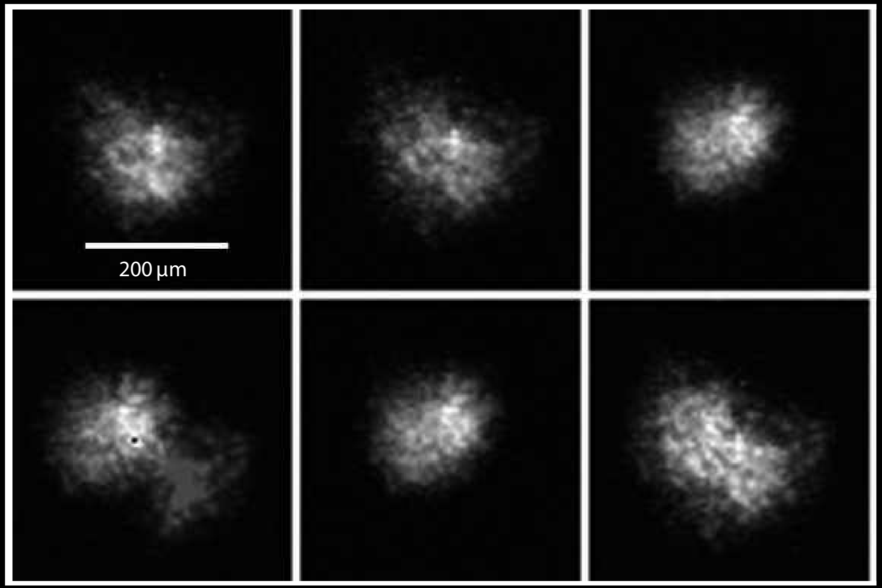
Vacuum:
Gaussian optics





Atmosphere: loss, turbulence





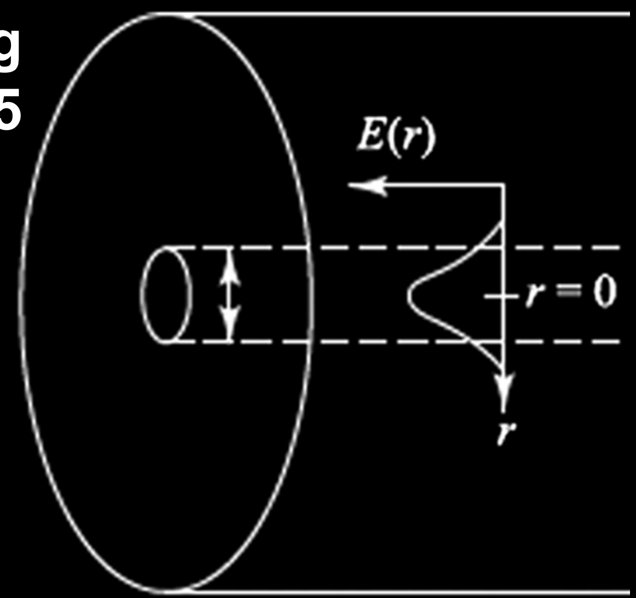
Images reprinted from: https://demonstrations.wolfram.com/GaussianBeamPropagationThroughTwoLenses/; Wikipedia; J.-P. Bourgoin *et al.*, New J. Phys. **15**, 023006 (2013); R. Ursin *et al.*, Nat. Phys. **3**, 481 (2007)

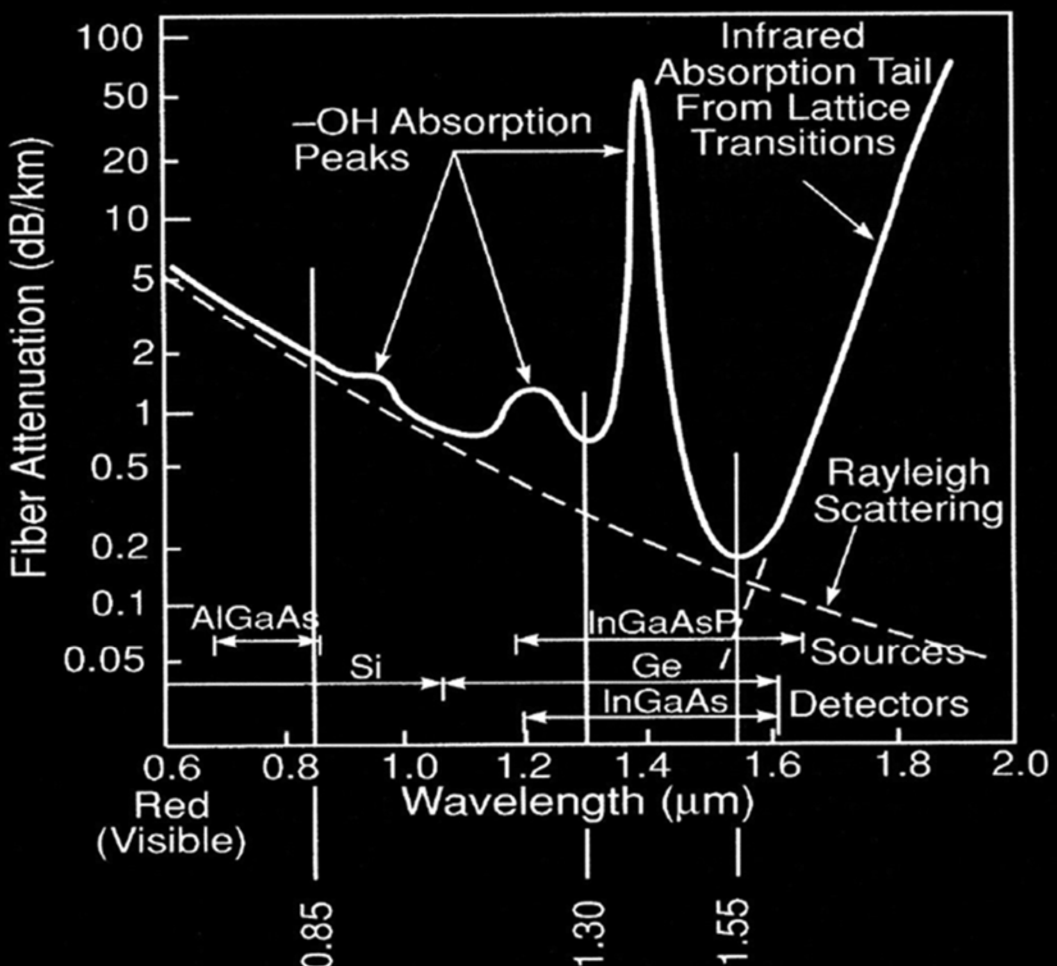
Transmission in optical fiber

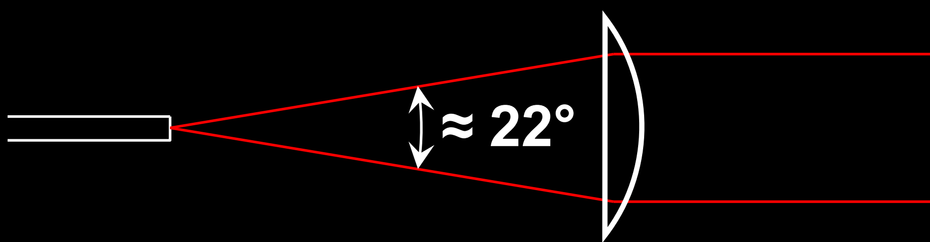
Single-mode fiber

125 μm diameter cladding
fused quartz, n_1 = 1.45

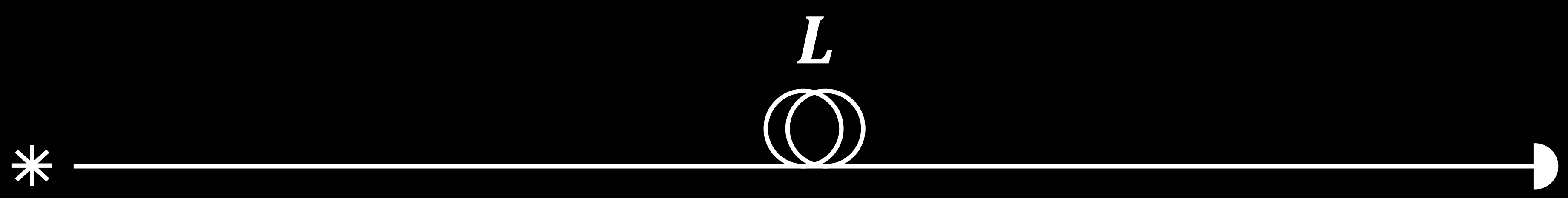
8 μm diameter core
$n_2 > n_1$





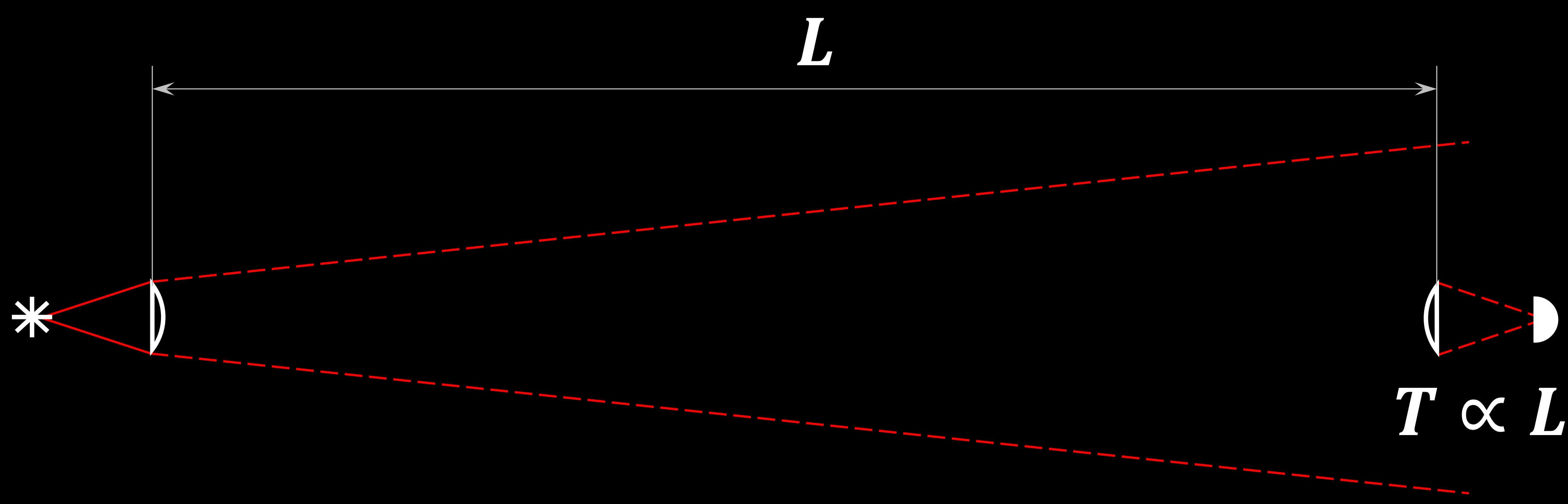


Fiber vs. beam in vacuum: loss scaling



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

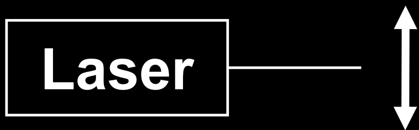
Exponential



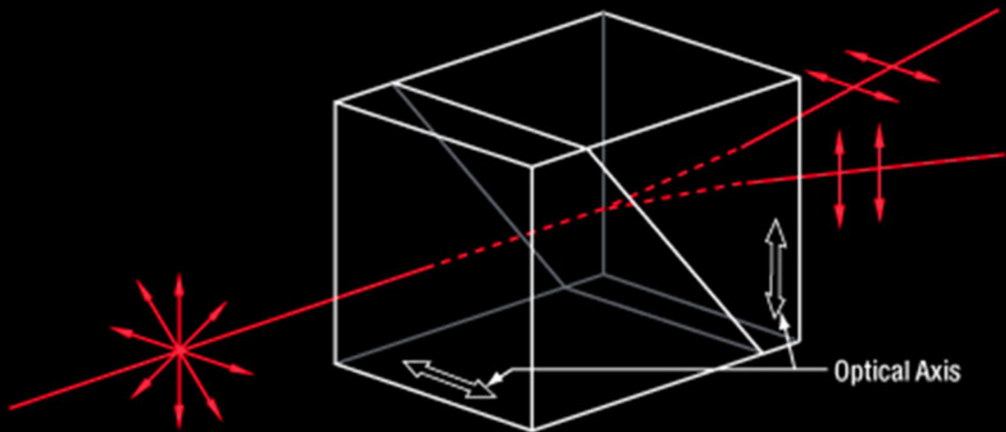
$T \propto L^{-2}$

Polynomial

Polarizers

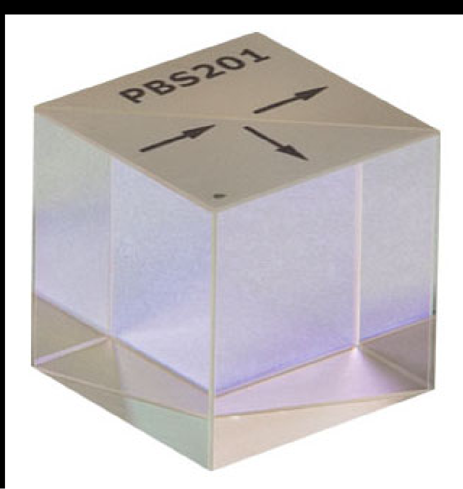


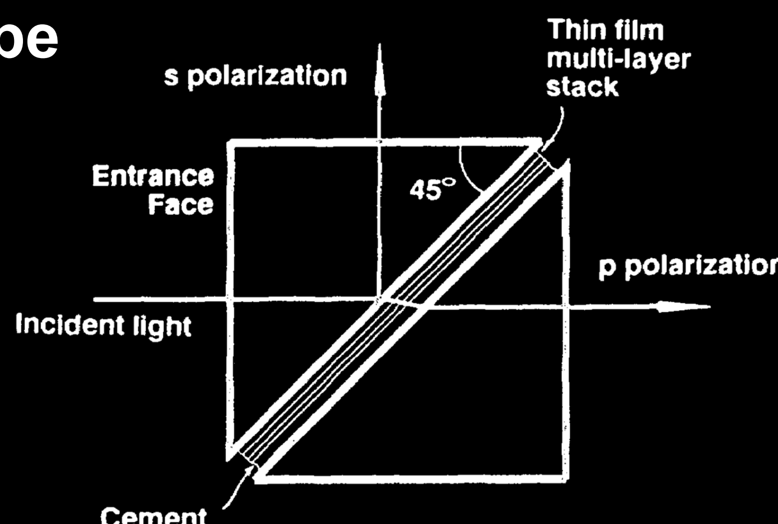
Birefringent polarizing beamsplitter



Wollaston prism

Polarizing beamsplitter cube



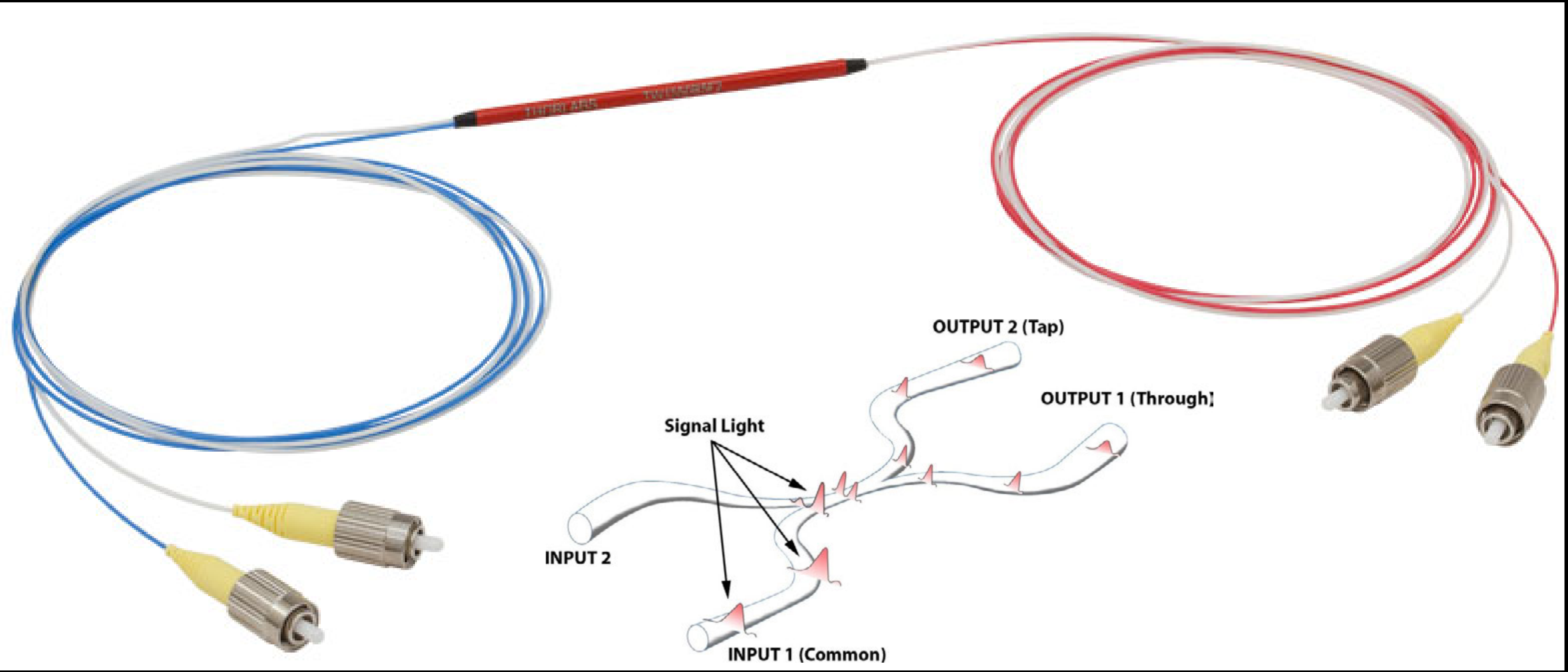


Images reprinted from: Thorlabs; J. L. Pezzaniti, R. A. Chipman, Appl. Opt. **33**, 1916 (1994)

Beamsplitters

50:50
10:90
1:99

Fiber-optic fused beamsplitter (or coupler)

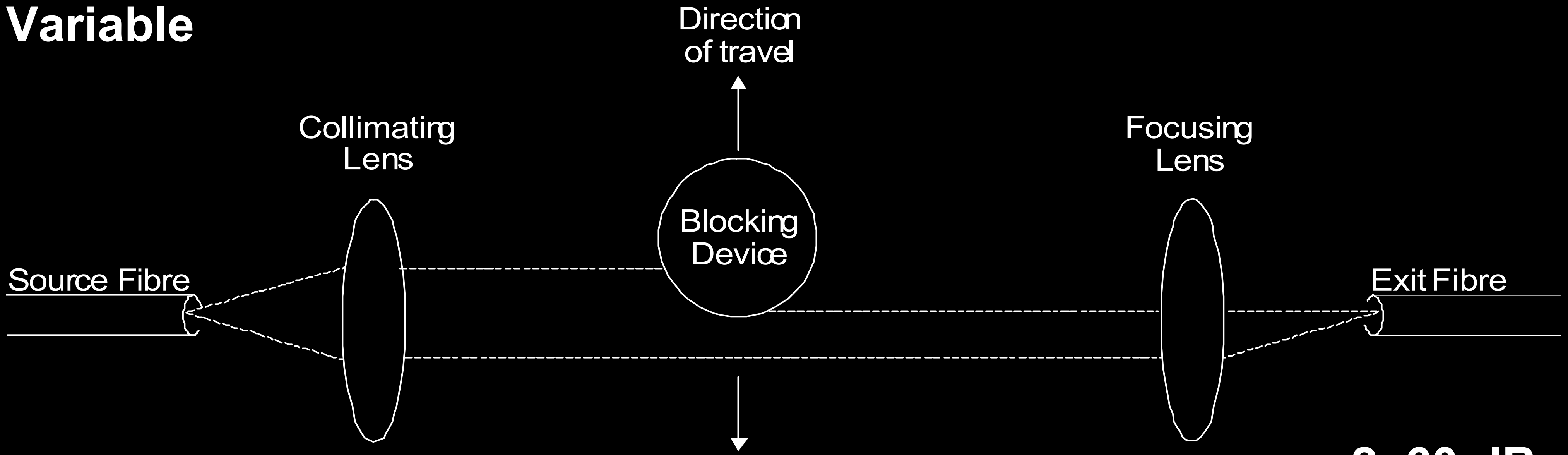


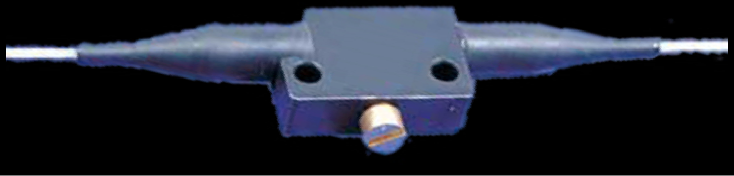
Images reprinted from: Thorlabs; Go!Foton

Attenuators

Absorbing or partially reflecting coated glass

Variable





2–60 dB

Wavelength filters

Colored glass

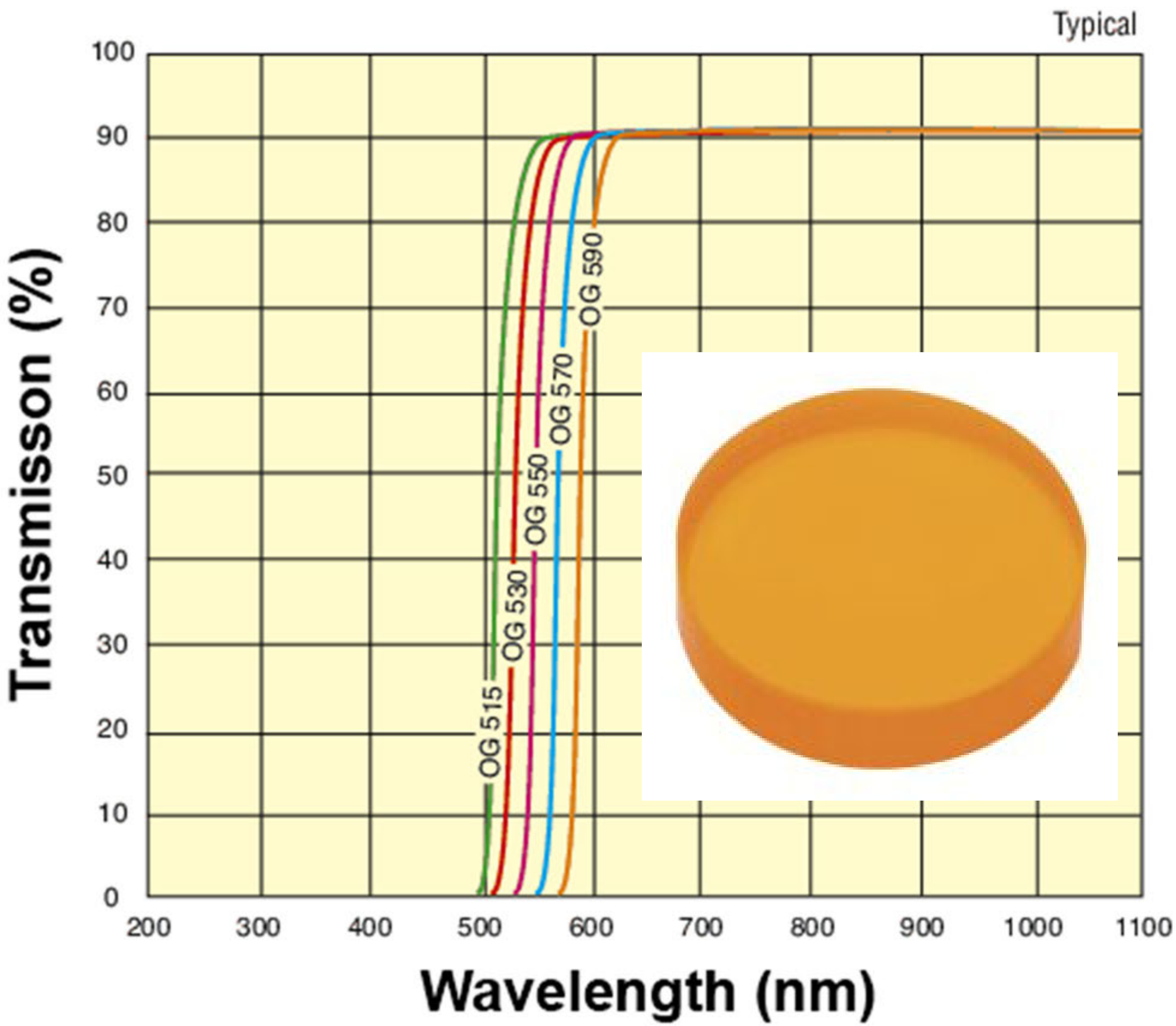
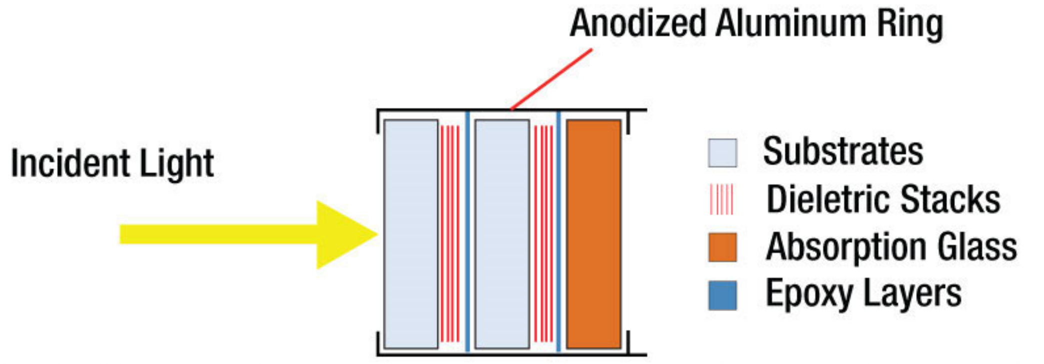
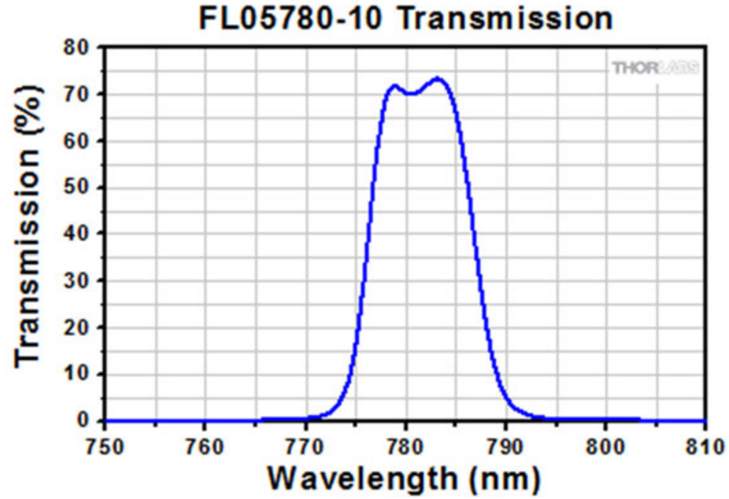


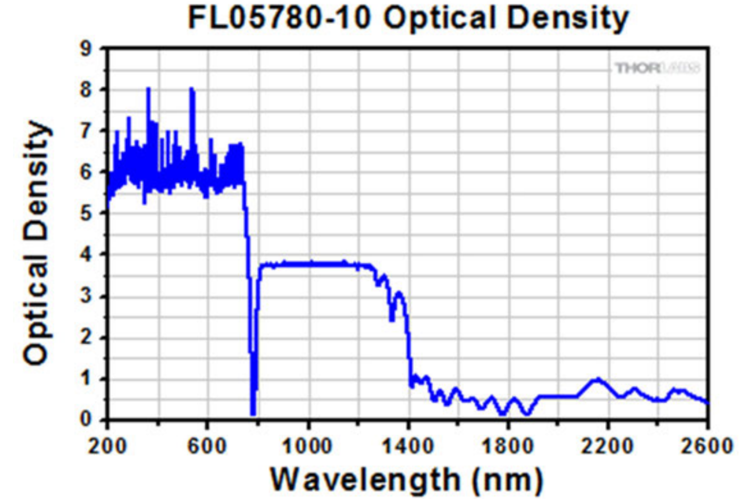
Image reprinted from: Newport

Wavelength filters

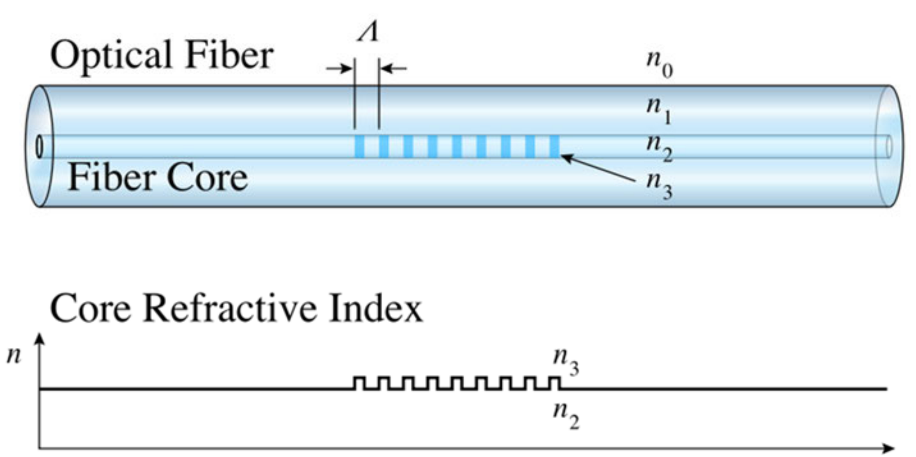
Interference filter

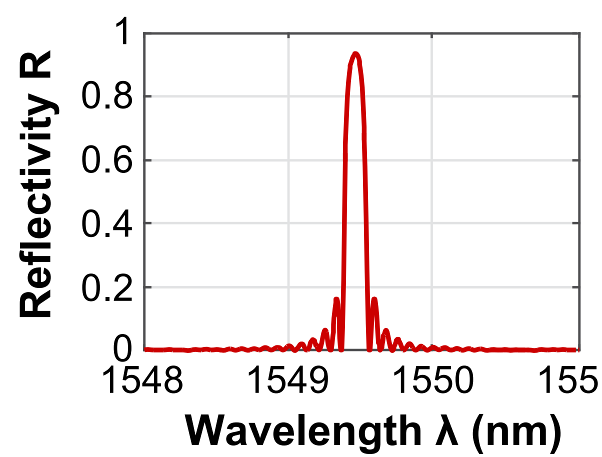






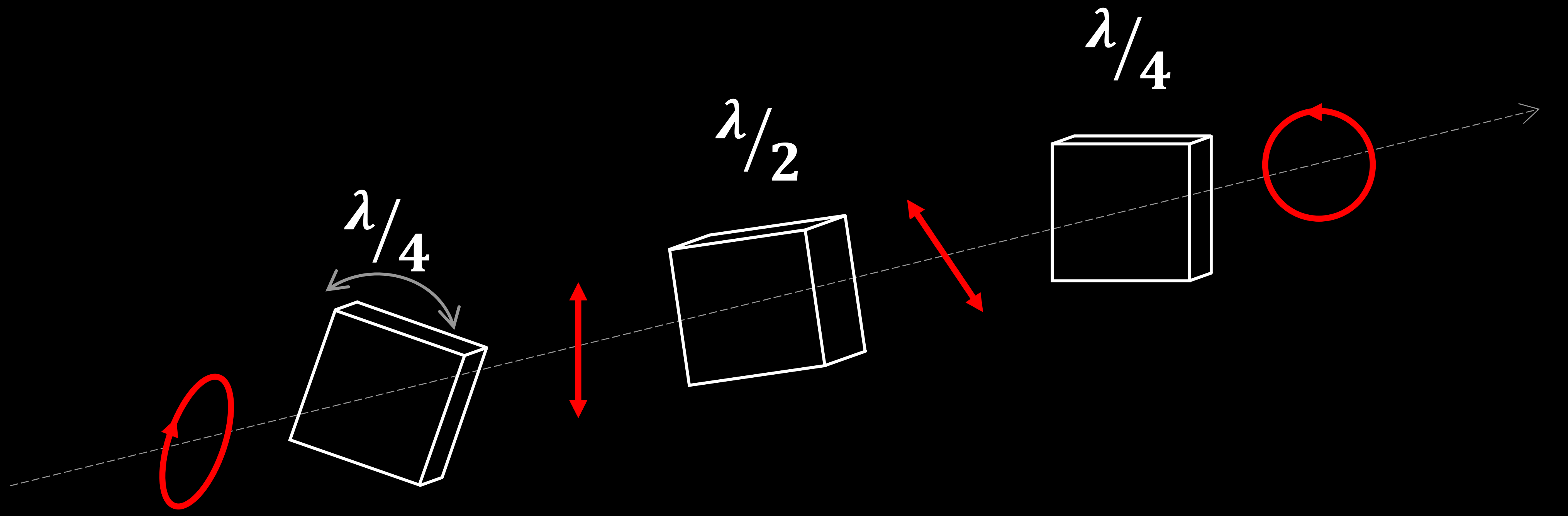
Fiber Bragg grating





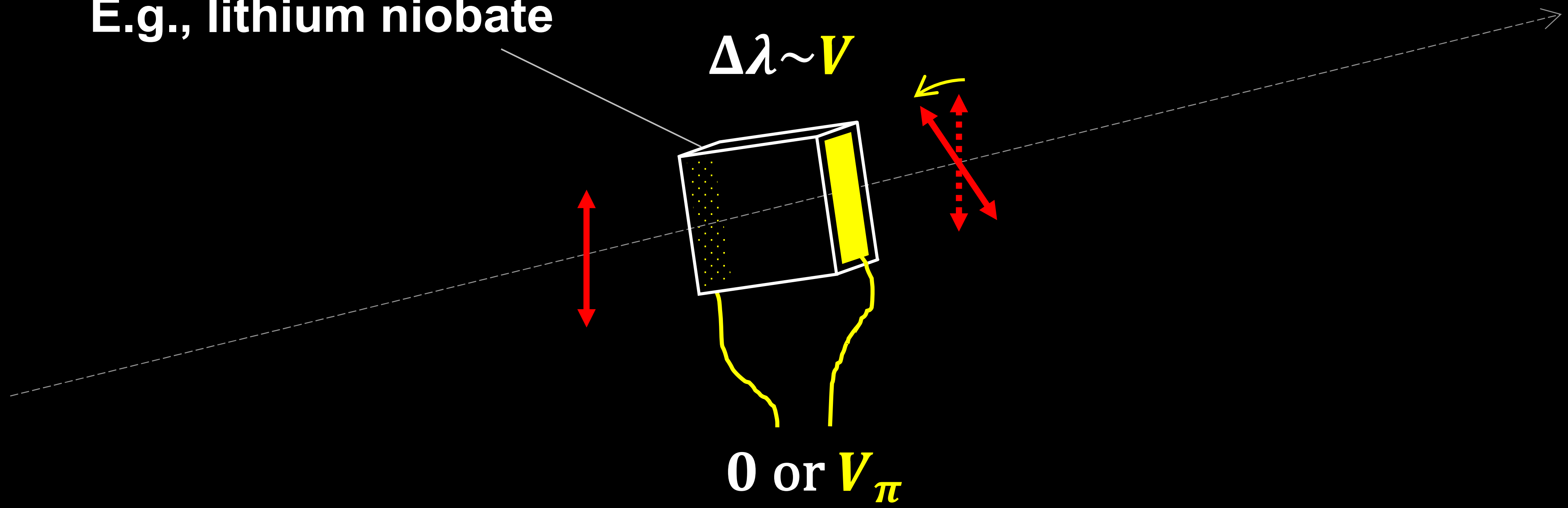
Images reprinted from: Thorlabs; Wikipedia; F. Seng *et al.*, Appl. Opt. **55**, 7179 (2016)

Polarization controller (slow)



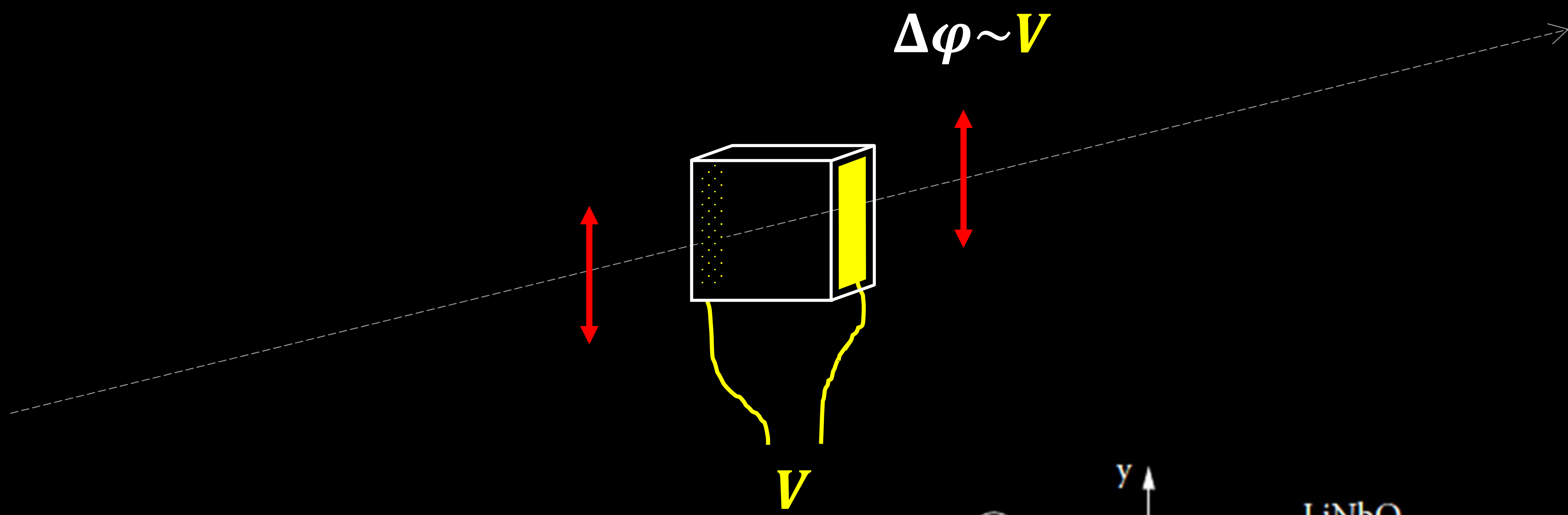
www.thorlabs.com/NewGroupPage9.cfm?ObjectGroup_ID=343

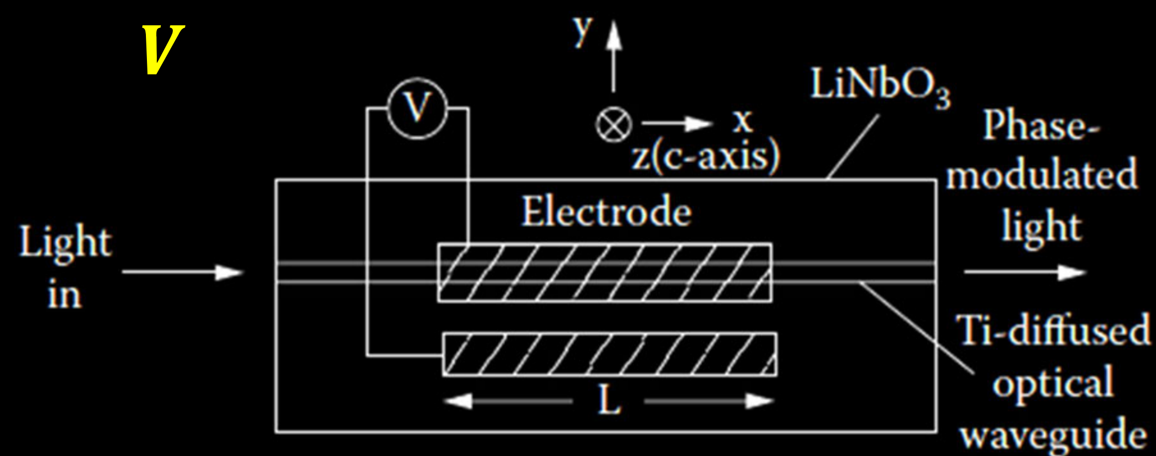
Polarization modulator (fast)

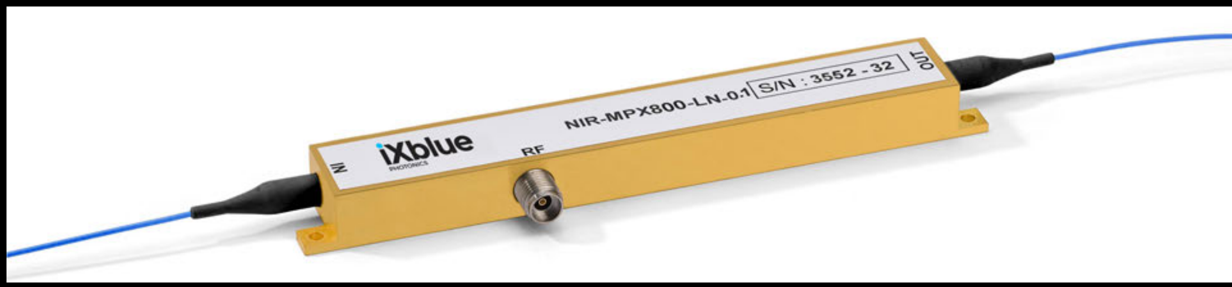


Pockels cell

Phase modulator

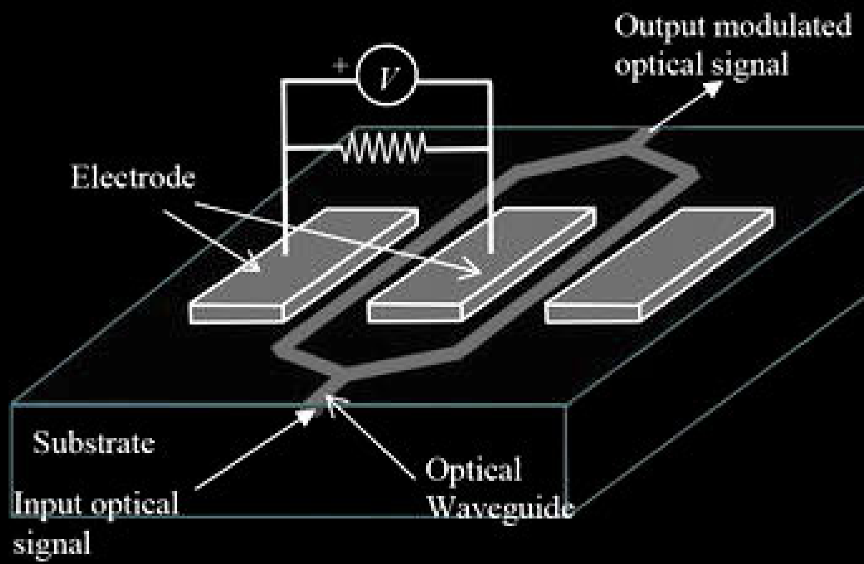


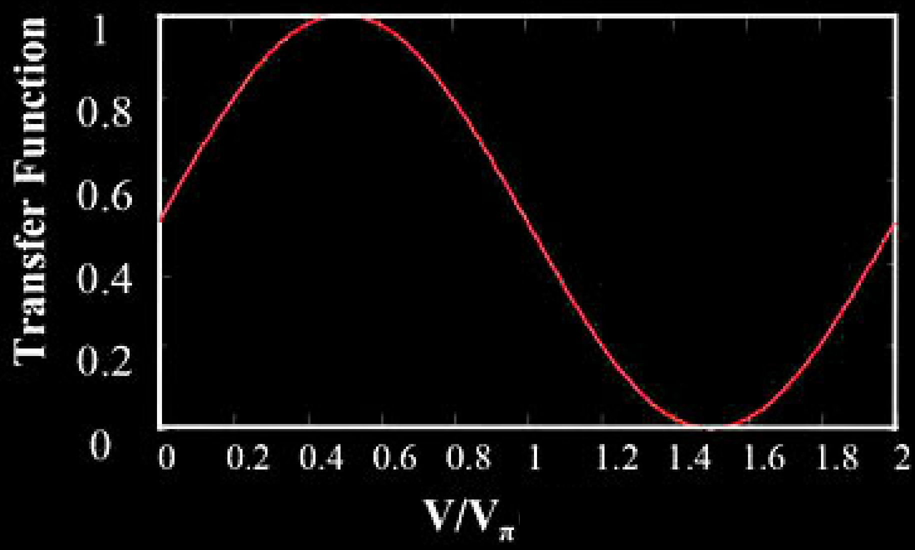




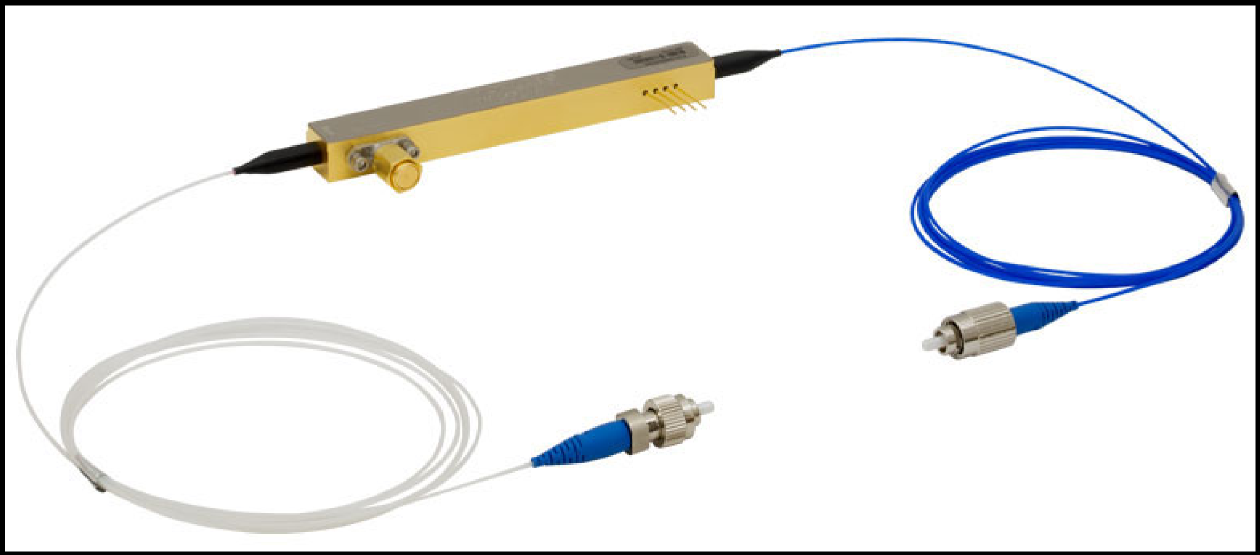
Images reprinted from: A. E.-N. A. Mohamed *et al.*, Int. J. Multidiscip. Sci. Eng. **2**, 13 (2011); iXblue Photonics

Intensity modulator





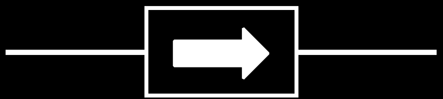
Mach-Zehnder interferometer

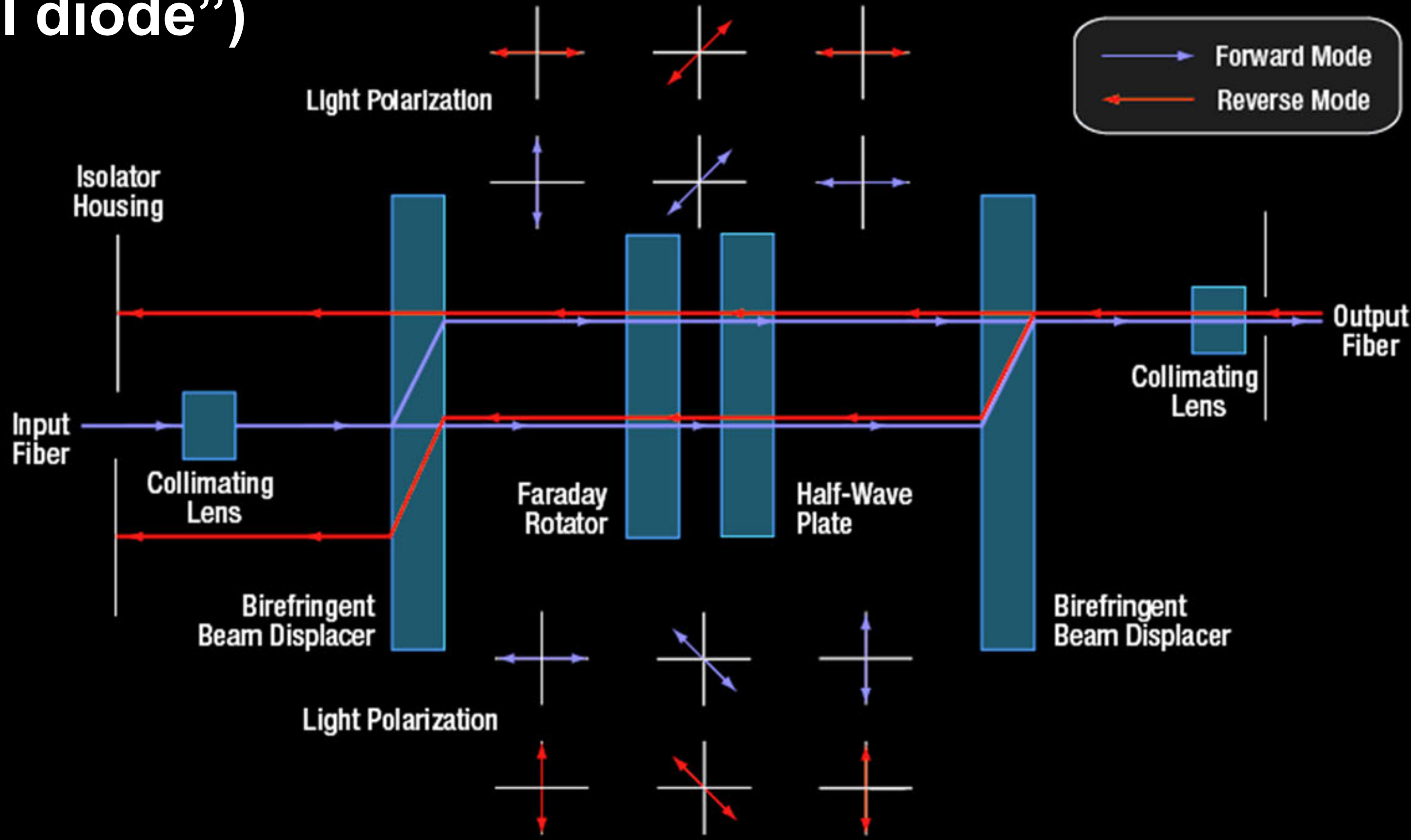


Images reprinted from: Optical Communication Technology, P. Pinho, ed., IntechOpen (2017); Thorlabs

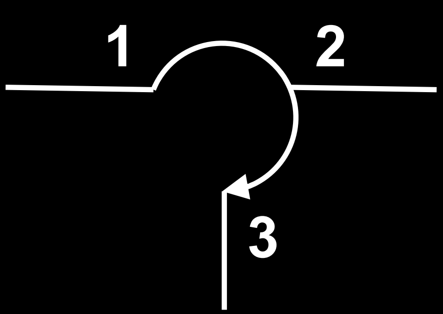
Directional elements

Isolator (an "optical diode")



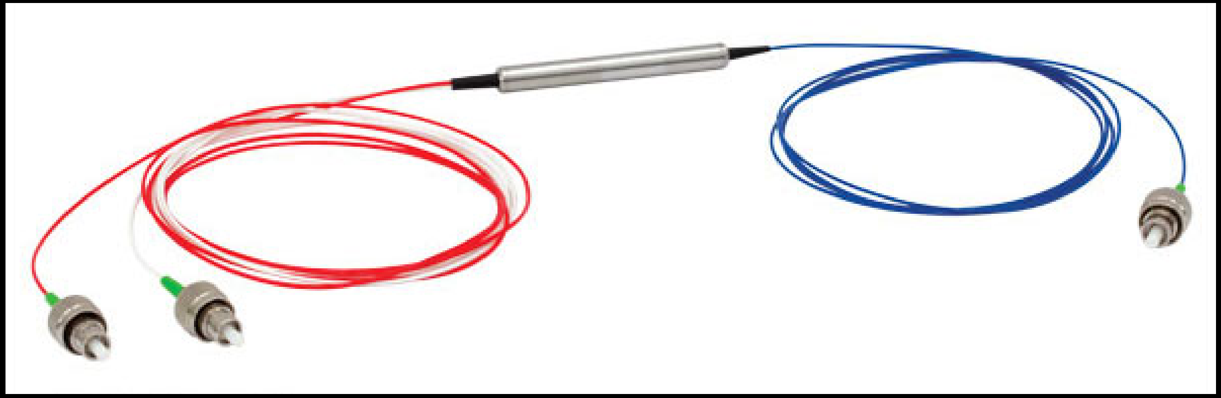


Circulator



1 → 2

2 → 3

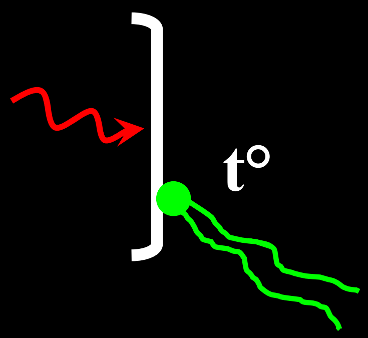


Images reprinted from: Thorlabs

Optical power meters

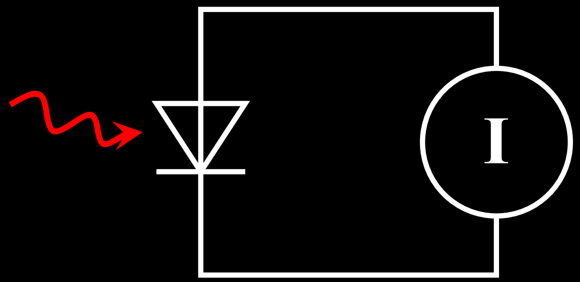
Thermal

> 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

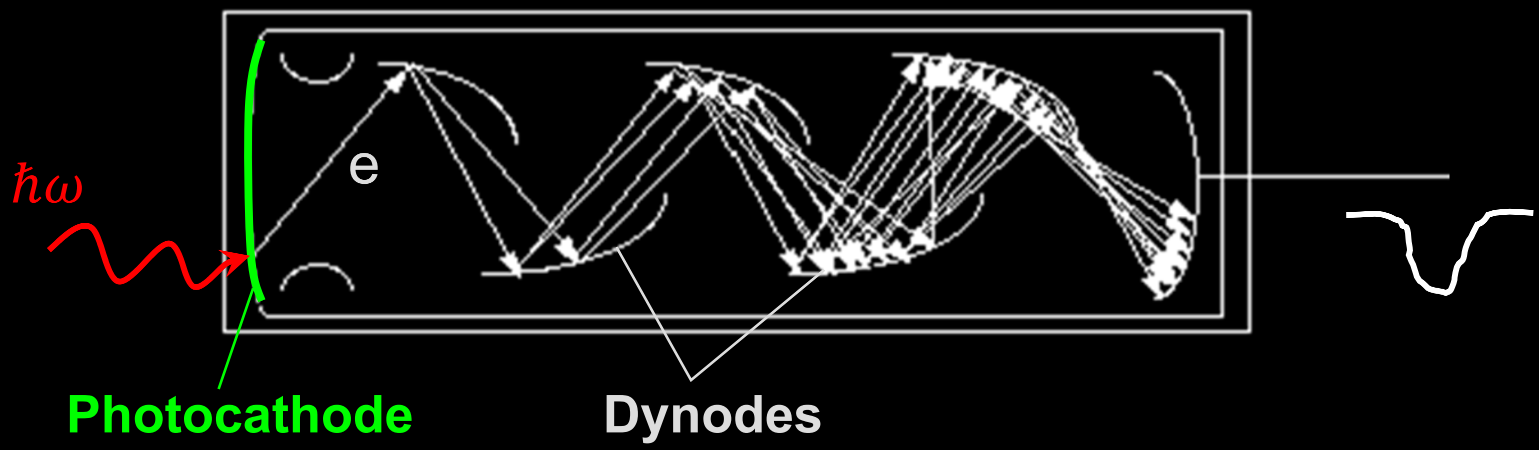
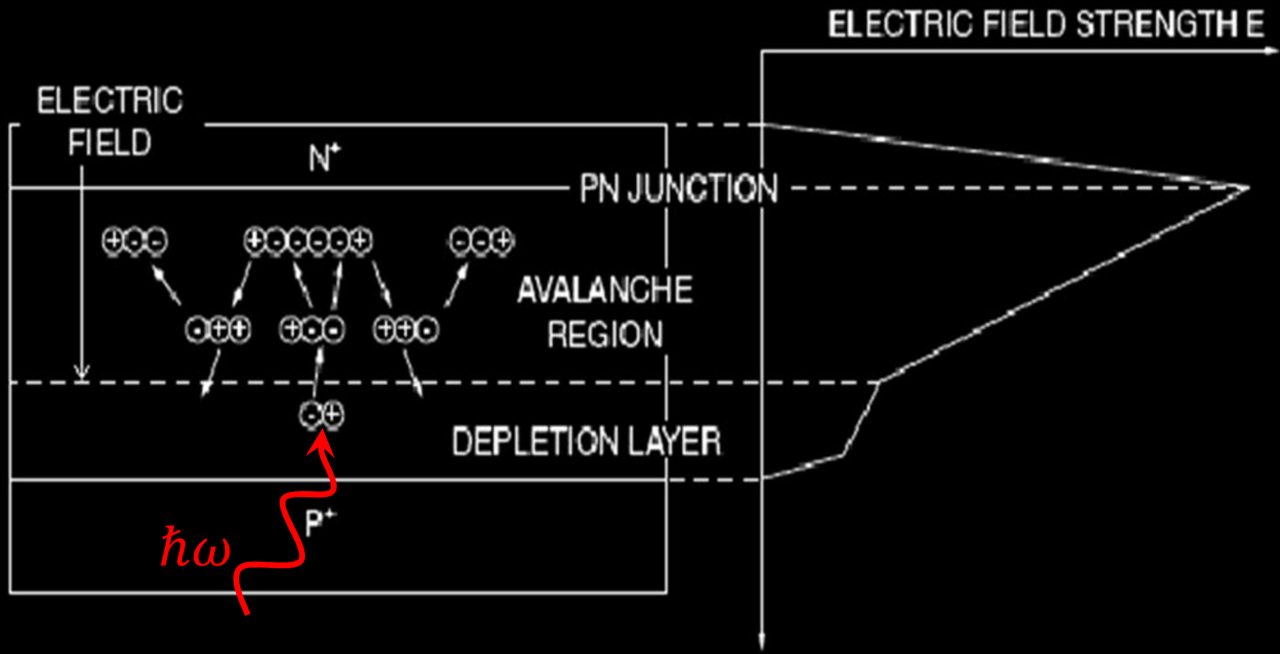
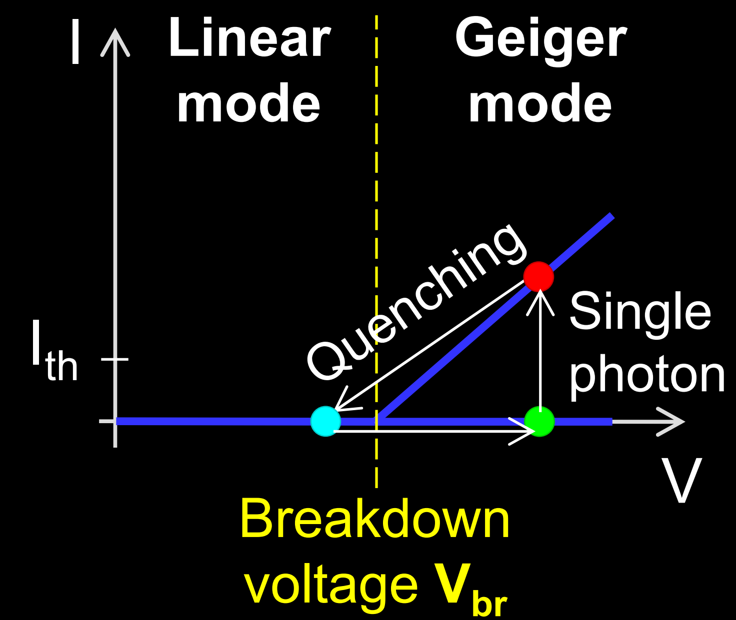
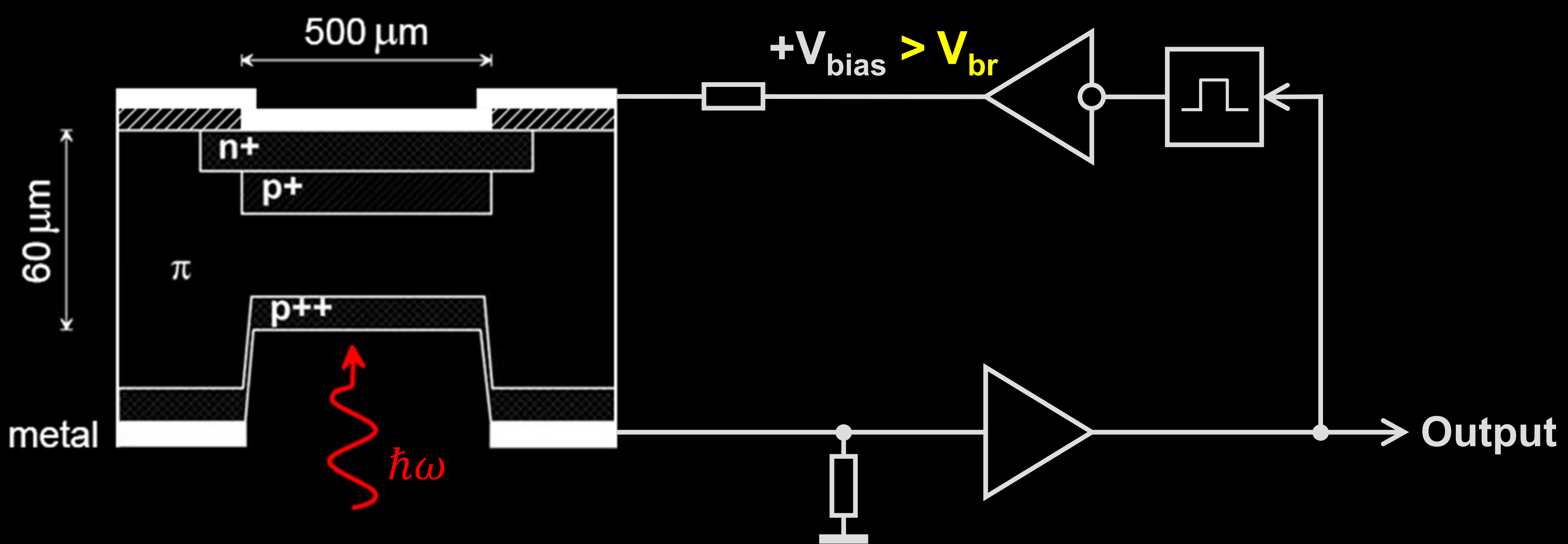


Image reprinted from: http://www.frankswebspace.org.uk/ScienceAndMaths/physics/physicsGCE/D1-5.htm

Single-photon avalanche photodiode



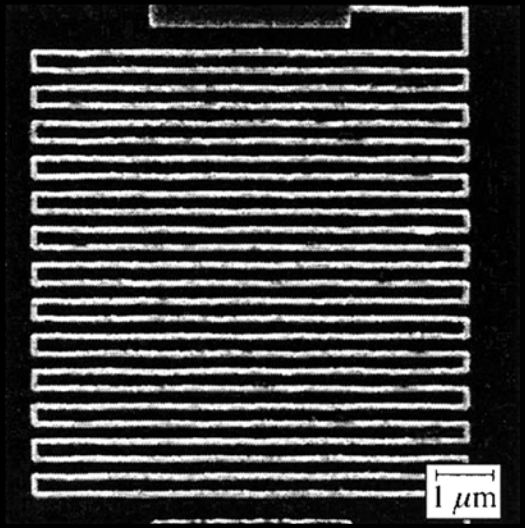


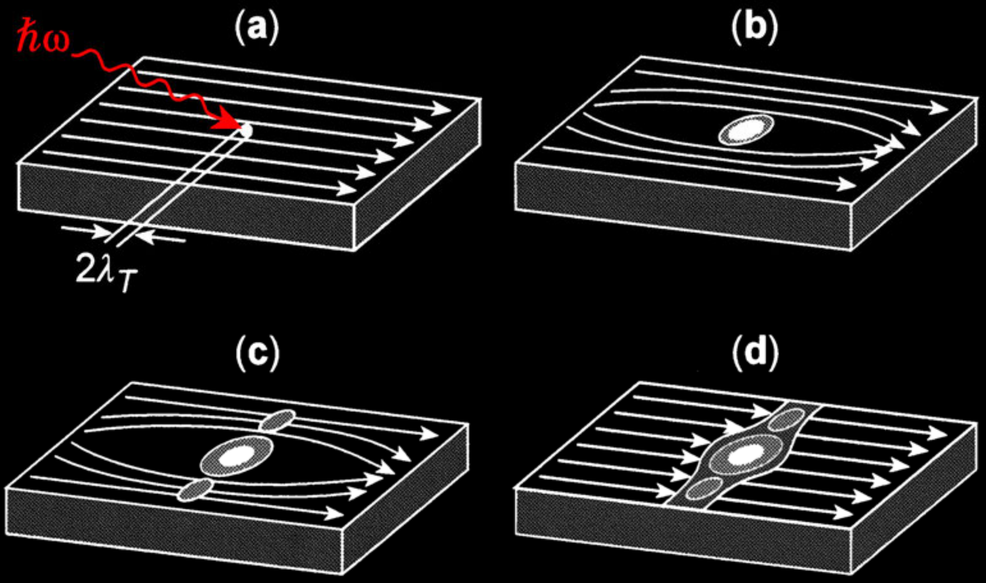


Images reprinted from: https://www.photonicsonline.com/doc/avalanche-photodiodes-theory-and-applications-0001; S. Cova *et al.*, J. Mod. Opt. **51**, 1267 (2004)

Superconducting single-photon detectors

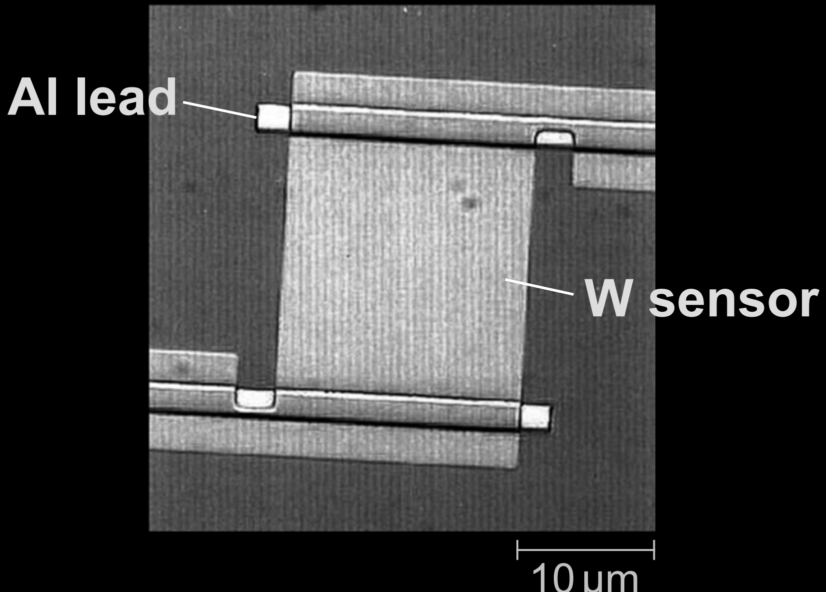
Superconducting nanowire

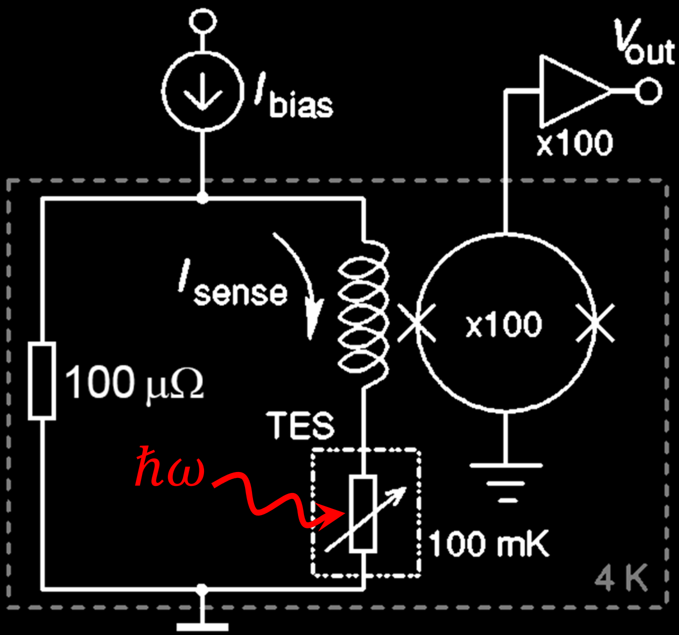




Images reprinted from: R. Sobolewski *et al.*, IEEE Trans. Appl. Supercond. **13**, 1151 (2003)

Transition-edge sensor



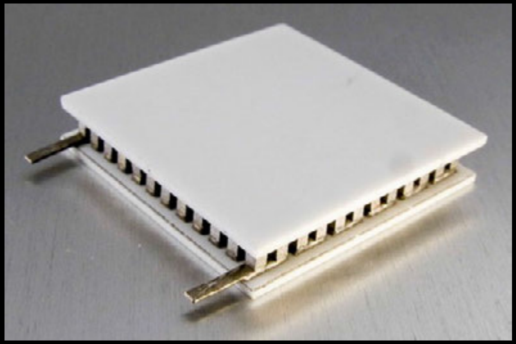


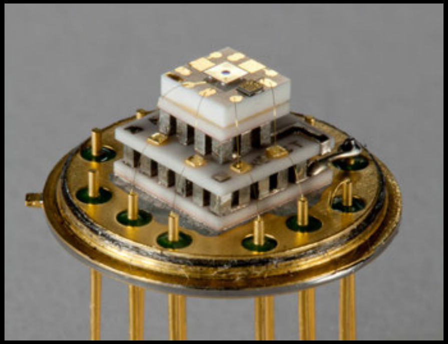
Images reprinted from: B. Cabrera *et al.*, Appl. Phys. Lett. **73**, 735 (1998); A.J. Miller *et al.*, Appl. Phys. Lett. **83**, 791 (2003)

Cooling requirements

Photomultiplier: room temperature

Avalanche photodiode: −50 °C





Thermoelectric cooling

0 5 mm

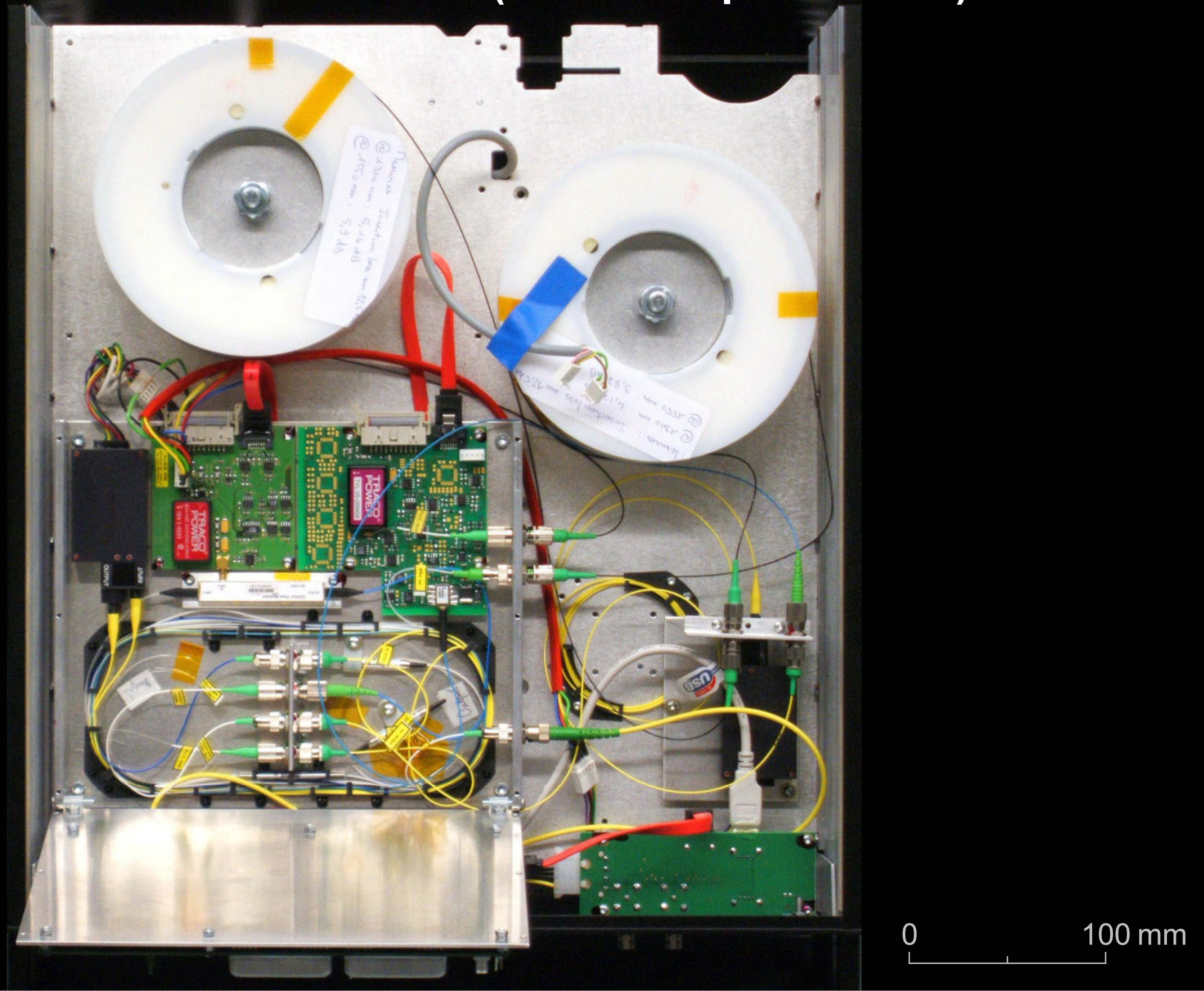
Superconducting nanowire: 4 K

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

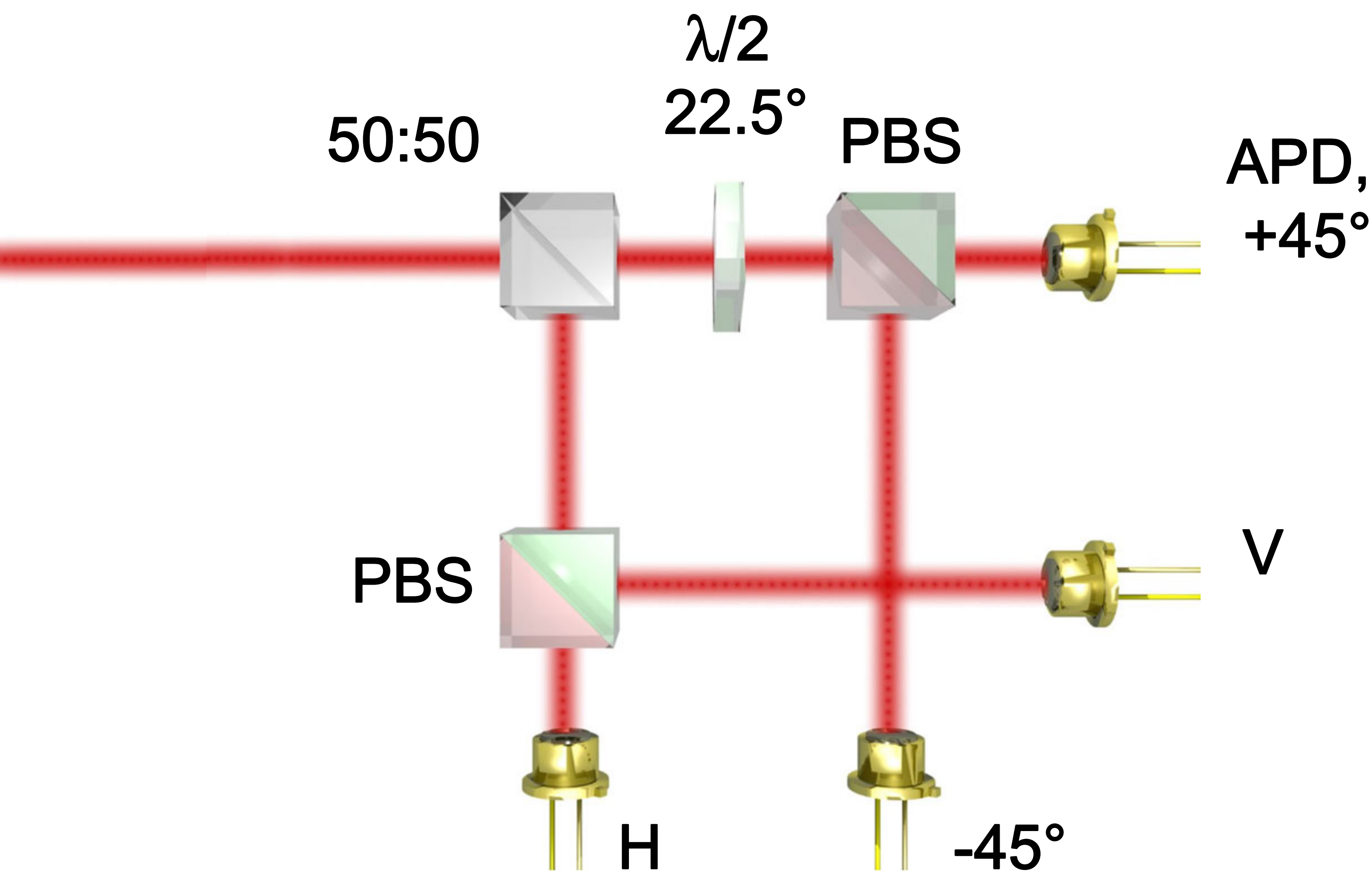
Assembled fiber optics

Quantum key distribution unit Alice (ID Quantique Clavis2)



Assembled free-space optics

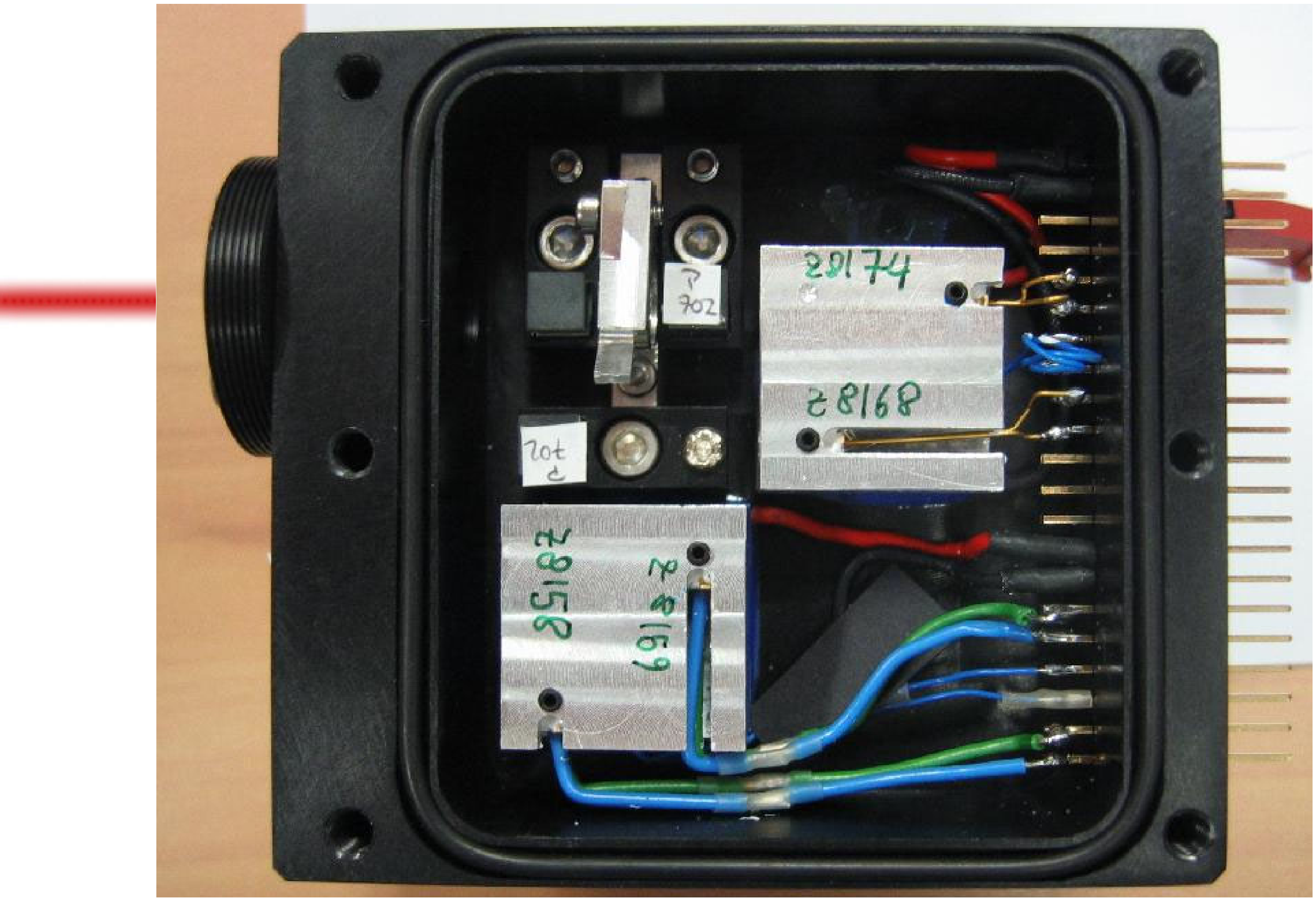
Bob's polarization analyzer with single-photon detectors



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

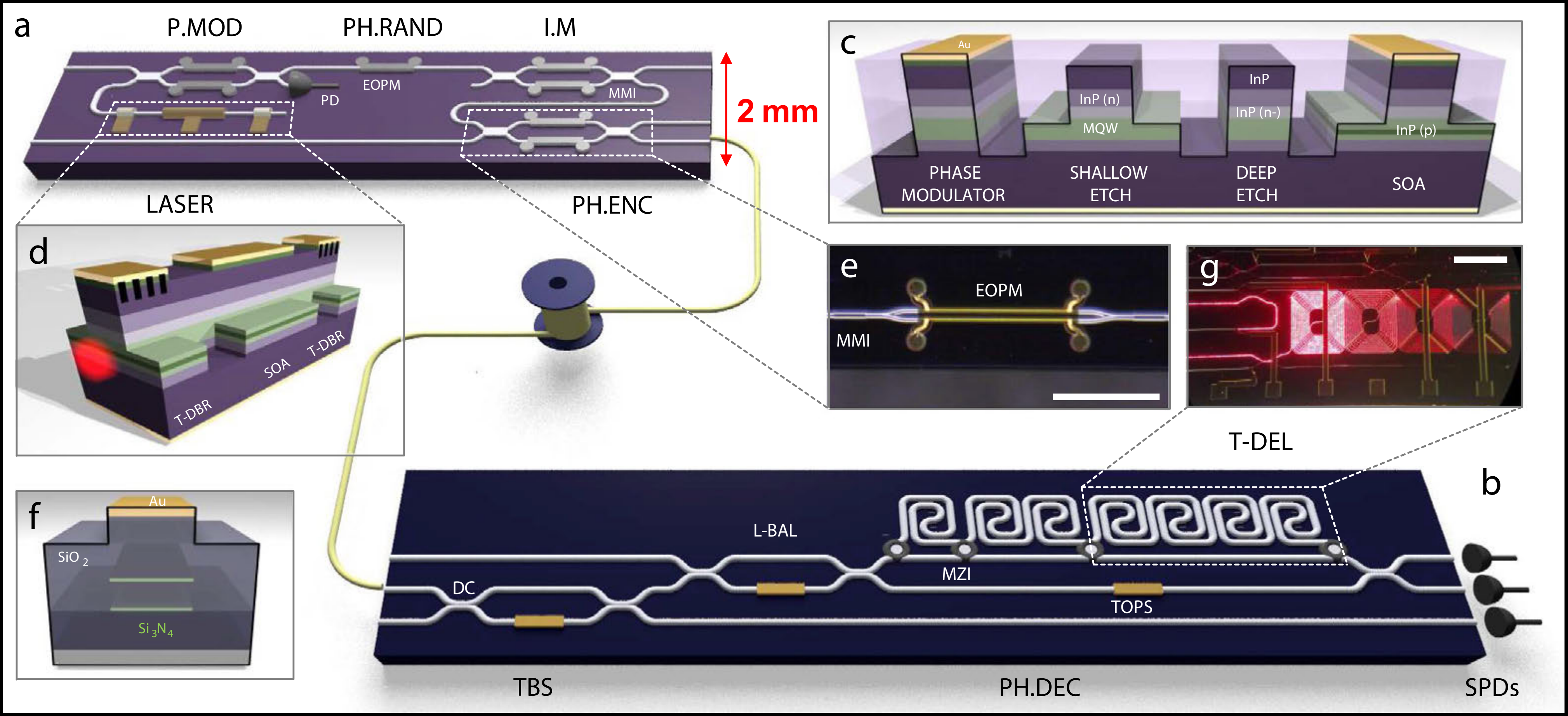


0 10 mm

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)