

Quantum cryptography

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



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.

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	?

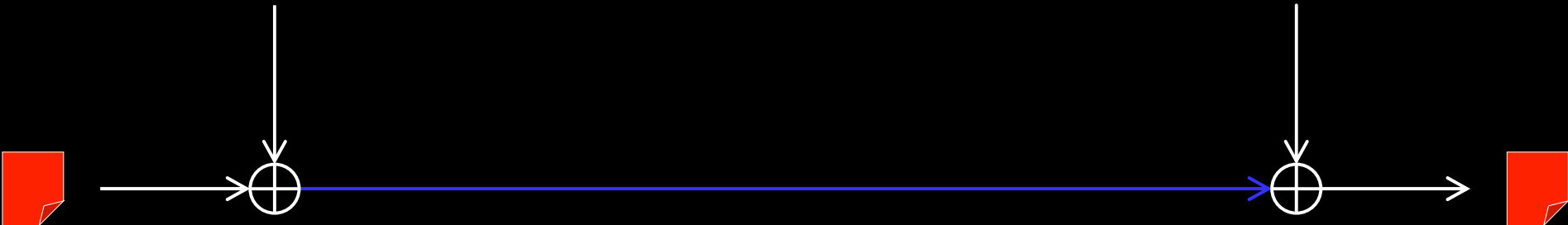
One-time pad

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

Teleportation

Entanglement swapping

Interaction-free measurement



(no classical equivalent)

Random number generators



Quantum communication primitives

Money

Key distribution

Secret sharing

Digital signatures

Superdense coding

Fingerprinting

Oblivious transfer

Bit commitment

Coin-tossing

Cloud computing

Software leasing

Bitcoin

Bell inequality testing

Teleportation

Entanglement swapping

Interaction-free measurement

Random number generators

S. Wiesner, unpublished circa 1970, *Sigact News* **15**, 78 (1983);
S. Aaronson, P. Christiano, *Proc. STOC'12*, 41 (2012)
idquantique.com, quantum-info.com, qasky.com, goqrates.com

W. P. Grice *et al.*, *Opt. Express* **23**, 7300 (2015).

R. Collins *et al.*, *Phys. Rev. Lett.* **113**, 040502 (2014)

C. H. Bennett, S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992)

J.-Y. Guan *et al.*, *Phys. Rev. Lett.* **116**, 240502 (2016)

C. Erven *et al.*, *Nat. Commun.* **5**, 3418 (2014)

T. Lunghi *et al.*, *Phys. Rev. Lett.* **111**, 180504 (2013)

A. Pappa *et al.*, *Nat. Commun.* **5**, 3717 (2014)

S. Barz *et al.*, *Science* **335**, 303 (2012)

A. Broadbent *et al.*, *Lect. Notes Comp. Sci.* **13042**, 90 (2021)

J. Jogenfors, *Proc. IEEE ICBC 2019*, 245 (2019)

B. Hensen *et al.*, *Nature* **526**, 682 (2015)

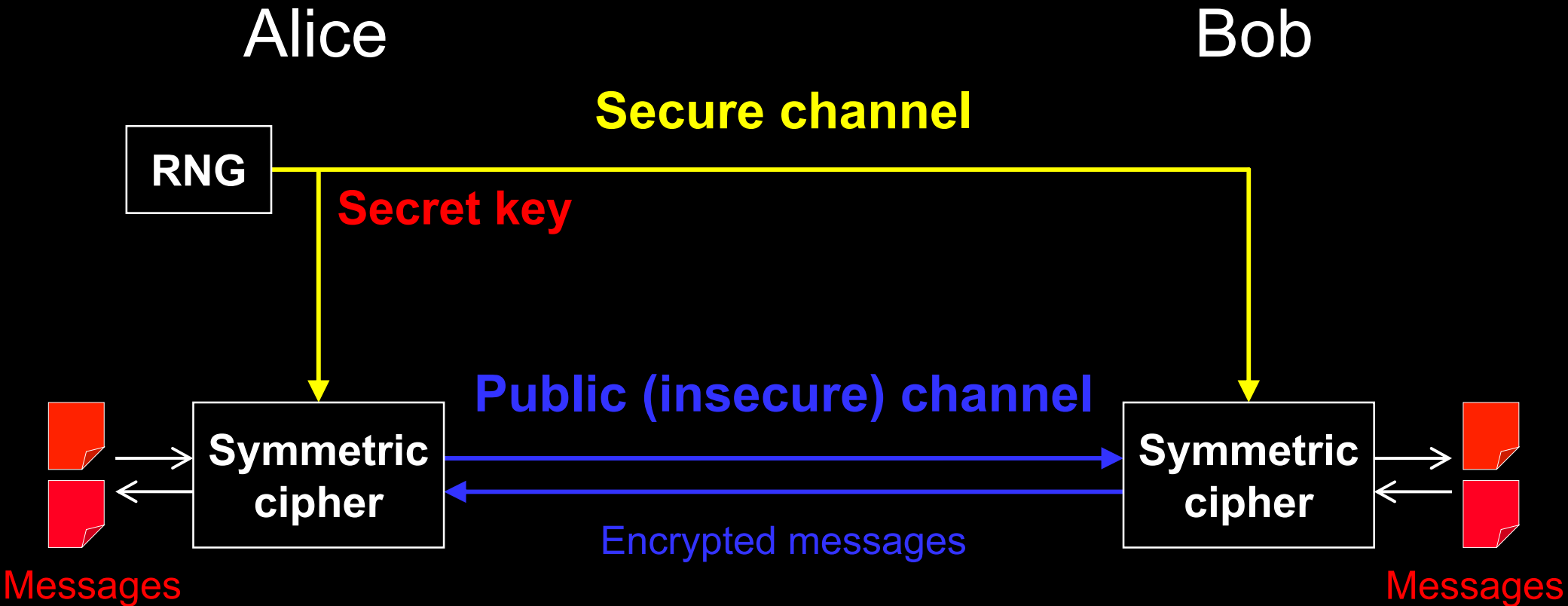
X.-S. Ma *et al.*, *Nature* **489**, 269 (2012)

M. Żukowski *et al.*, *Phys. Rev. Lett.* **71**, 4287 (1993)

A. C. Elitzur, L. Vaidman, *Found. Phys.* **23**, 987 (1993)

idquantique.com, picoquant.com

Key distribution for encryption



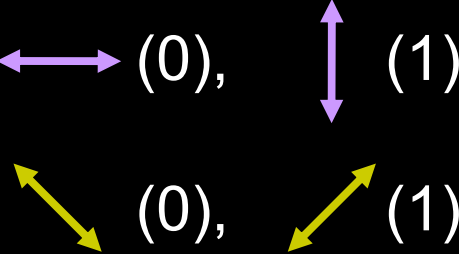
Quantum key distribution transmits secret key by sending quantum states over *open channel*.

Quantum key distribution (QKD)

Alice



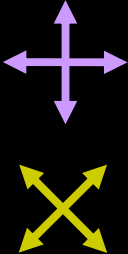
Prepares photons



Bob



Measures photons

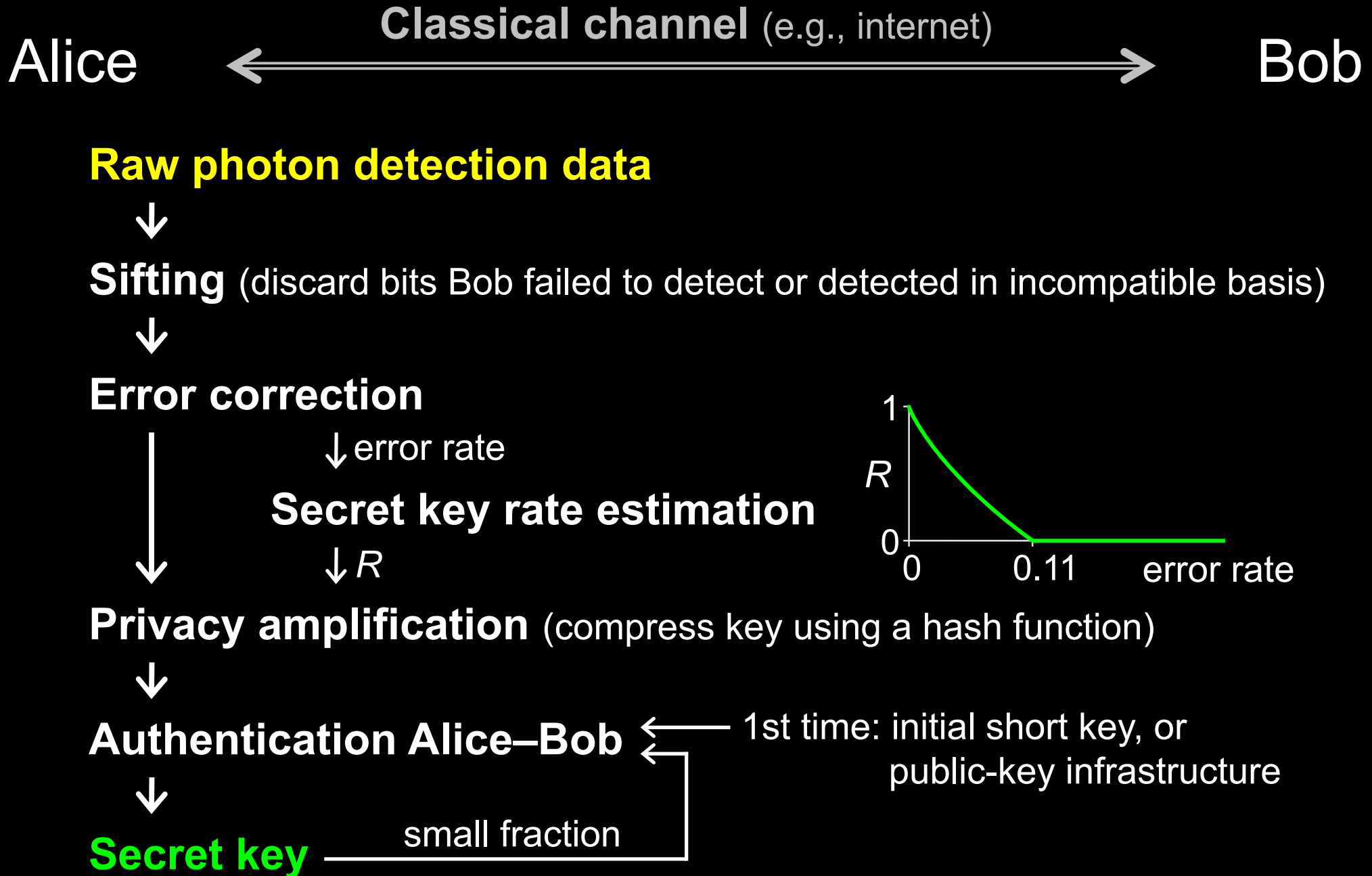


or ?



Eavesdropping introduces errors

Post-processing in QKD



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)

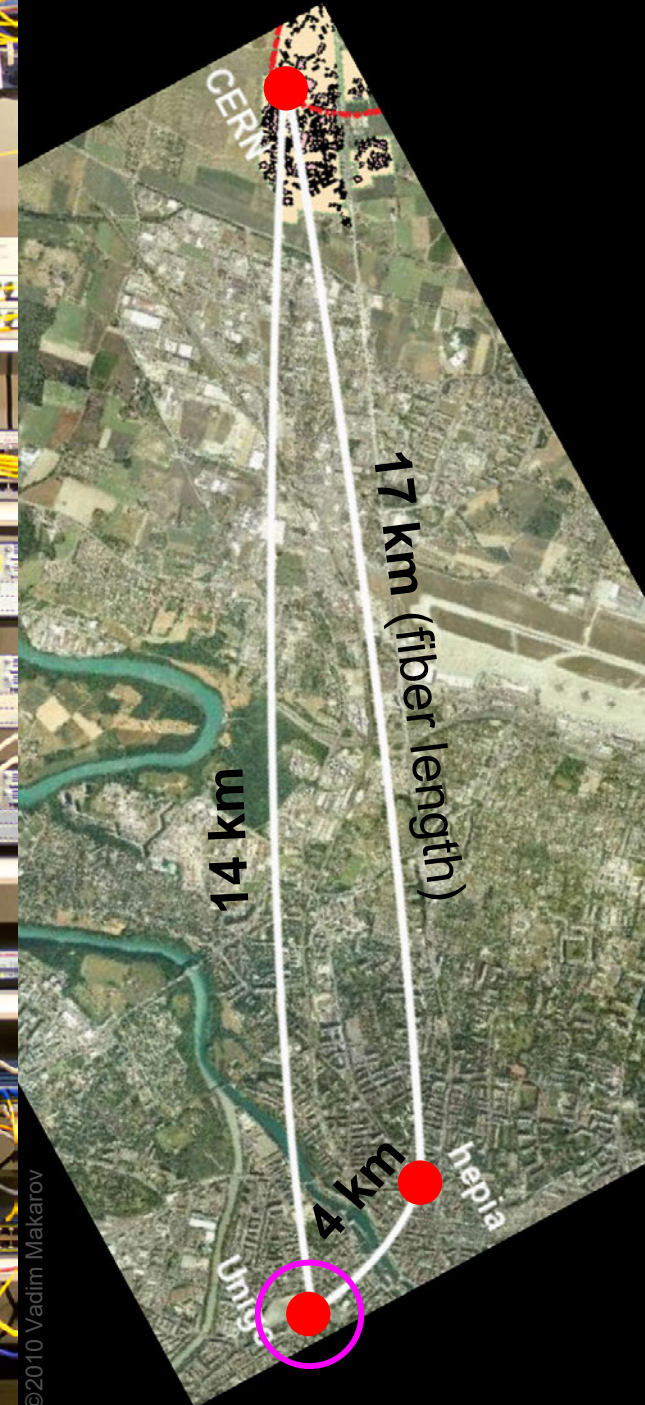
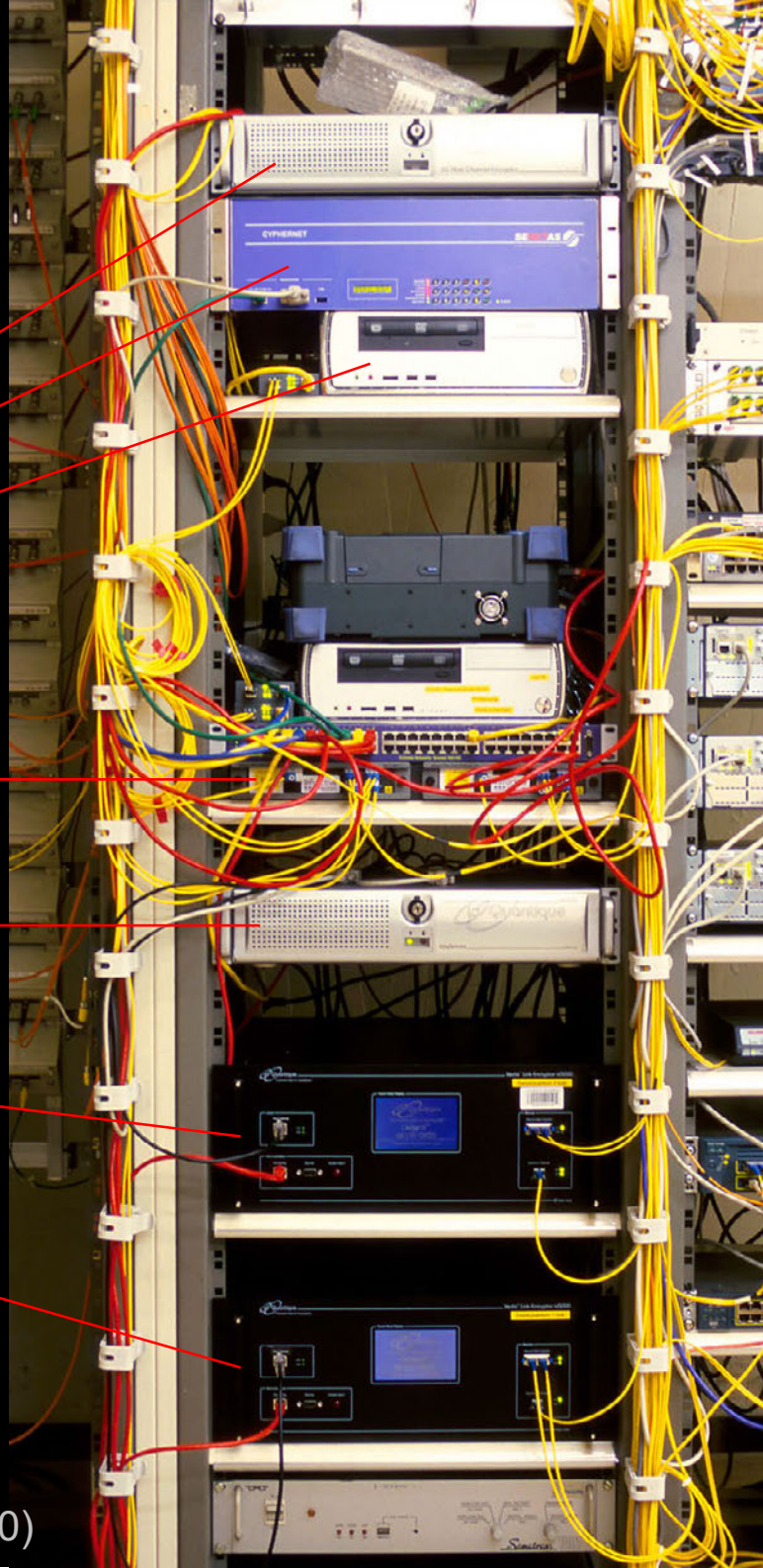
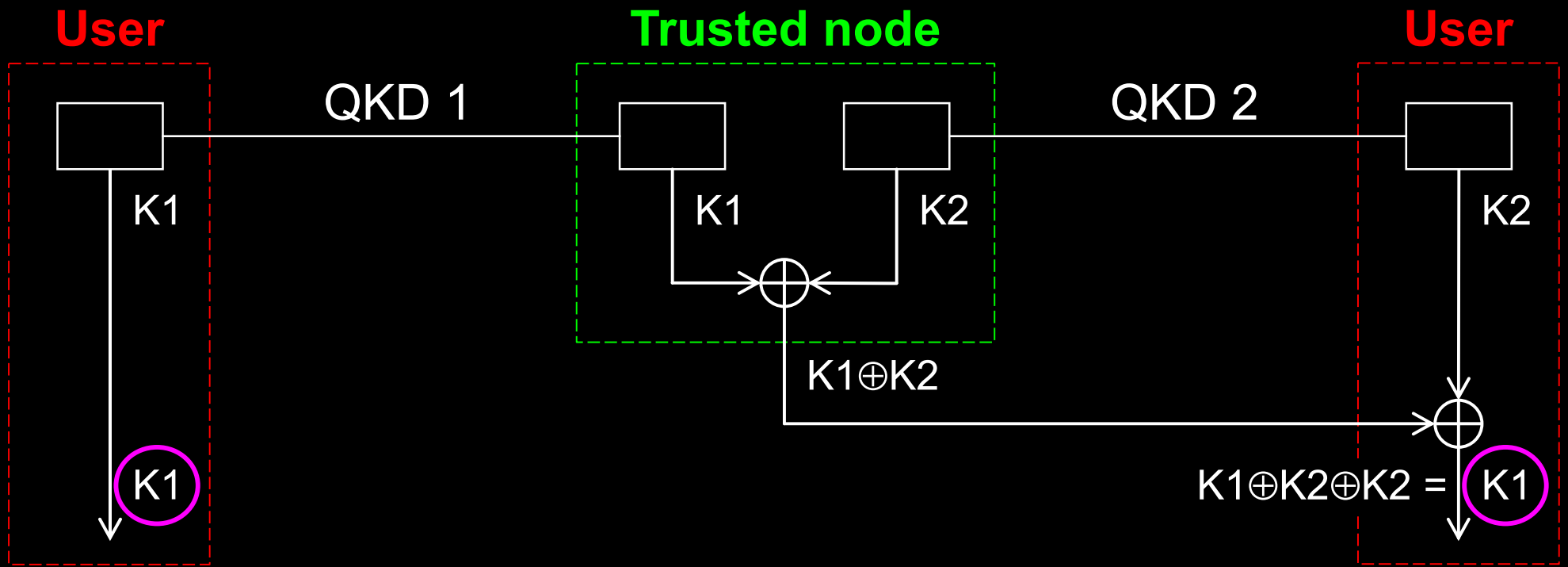
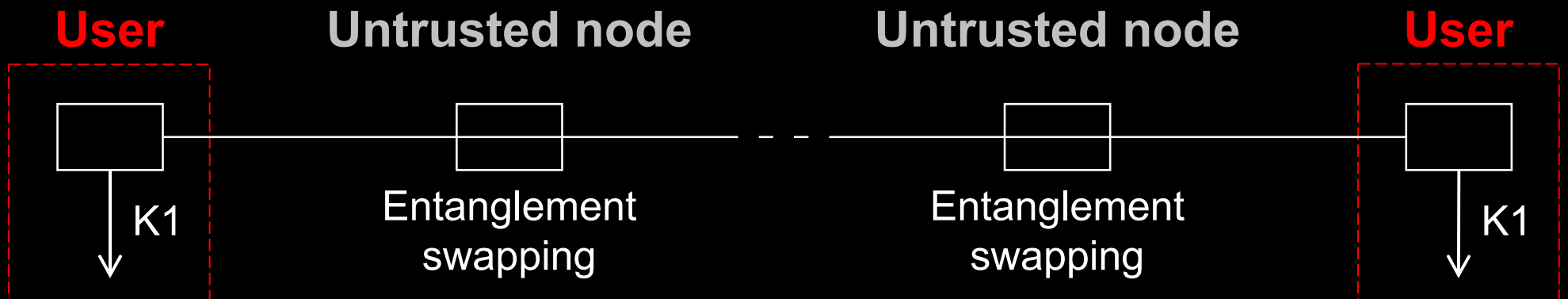


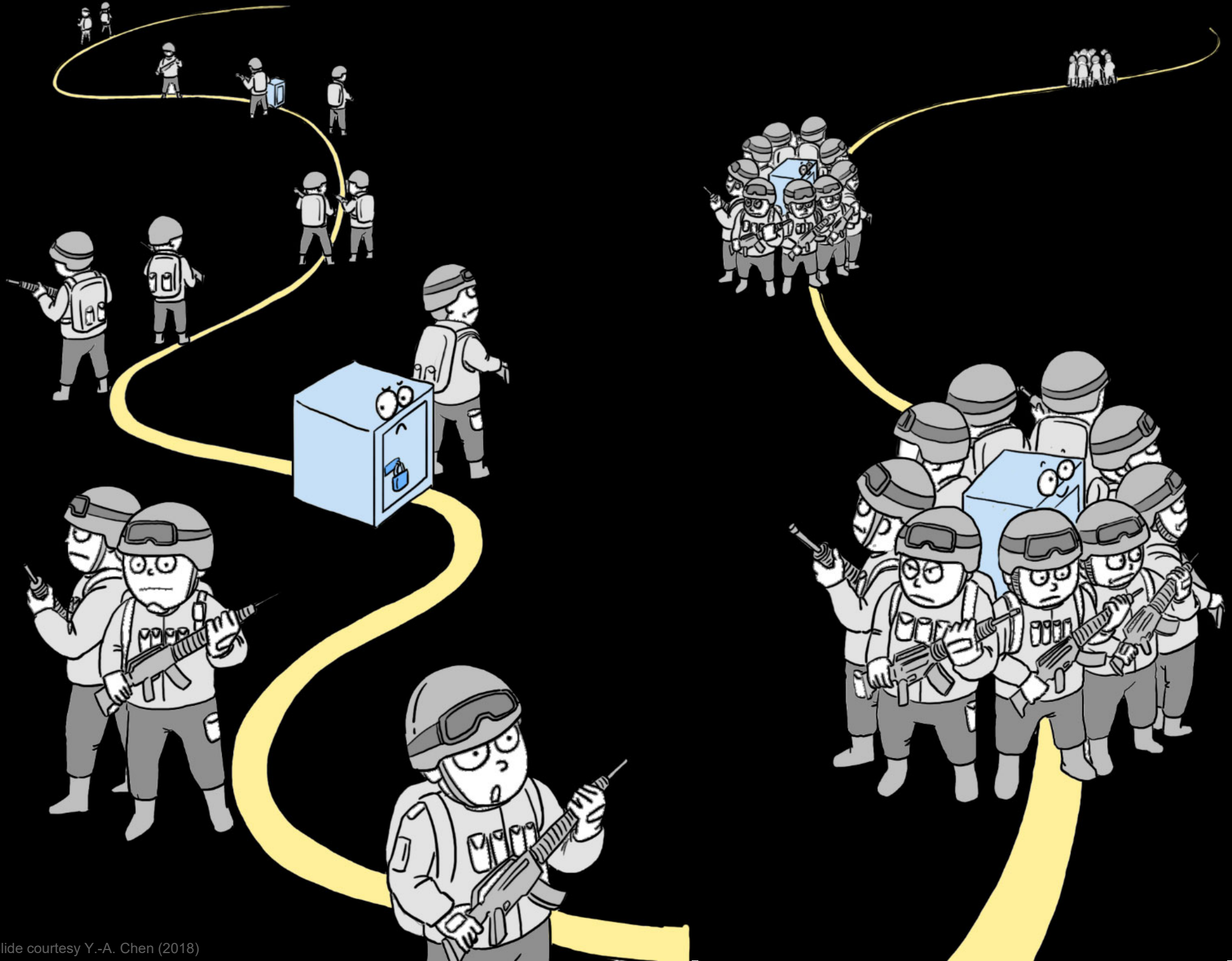
Photo ©2010 Vadim Makarov

Today: trusted-node repeater

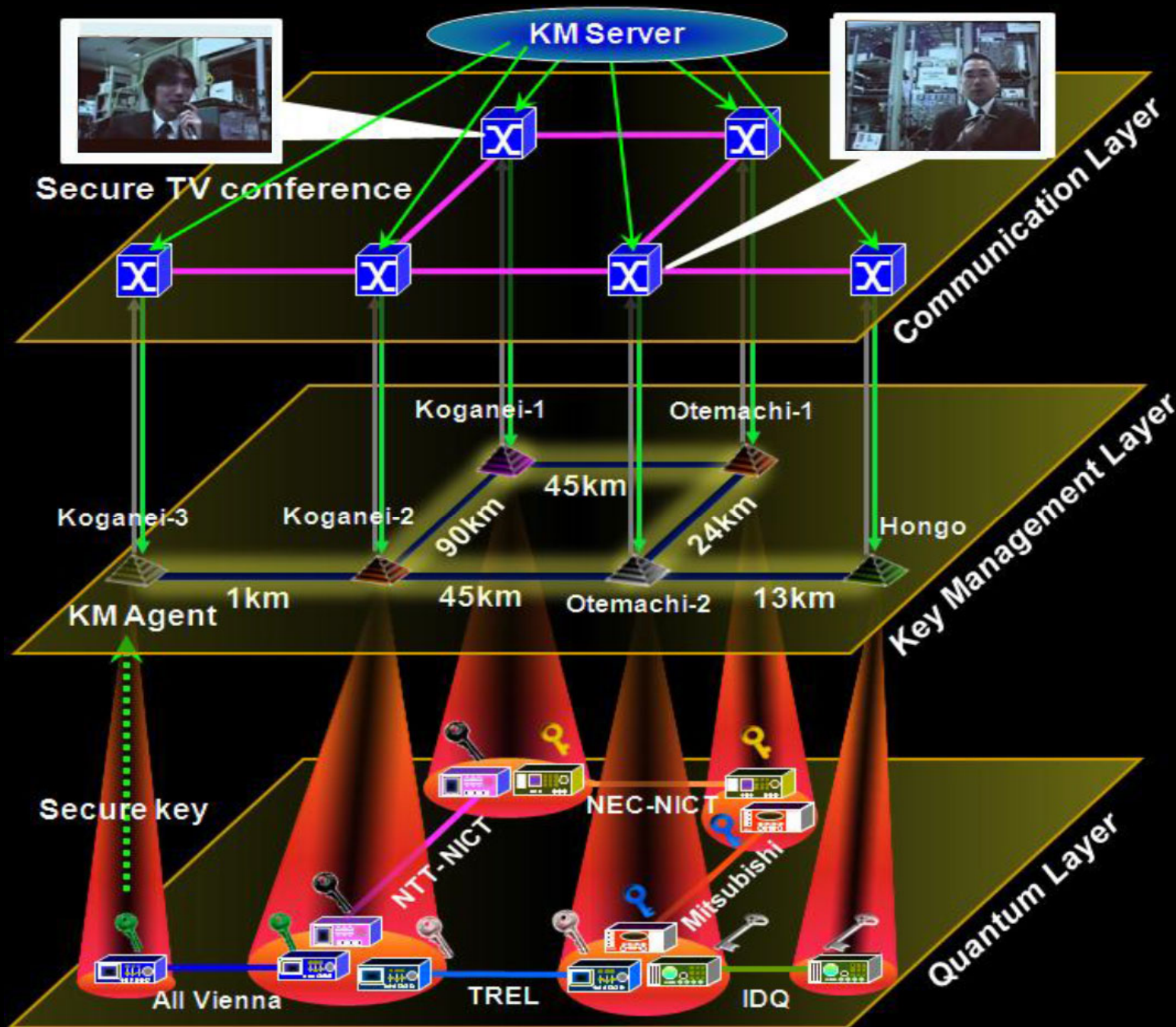


Future: quantum repeater





Trusted-node network





量子保密通信京沪干线



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

Photo ©2016 Vadim Makarov

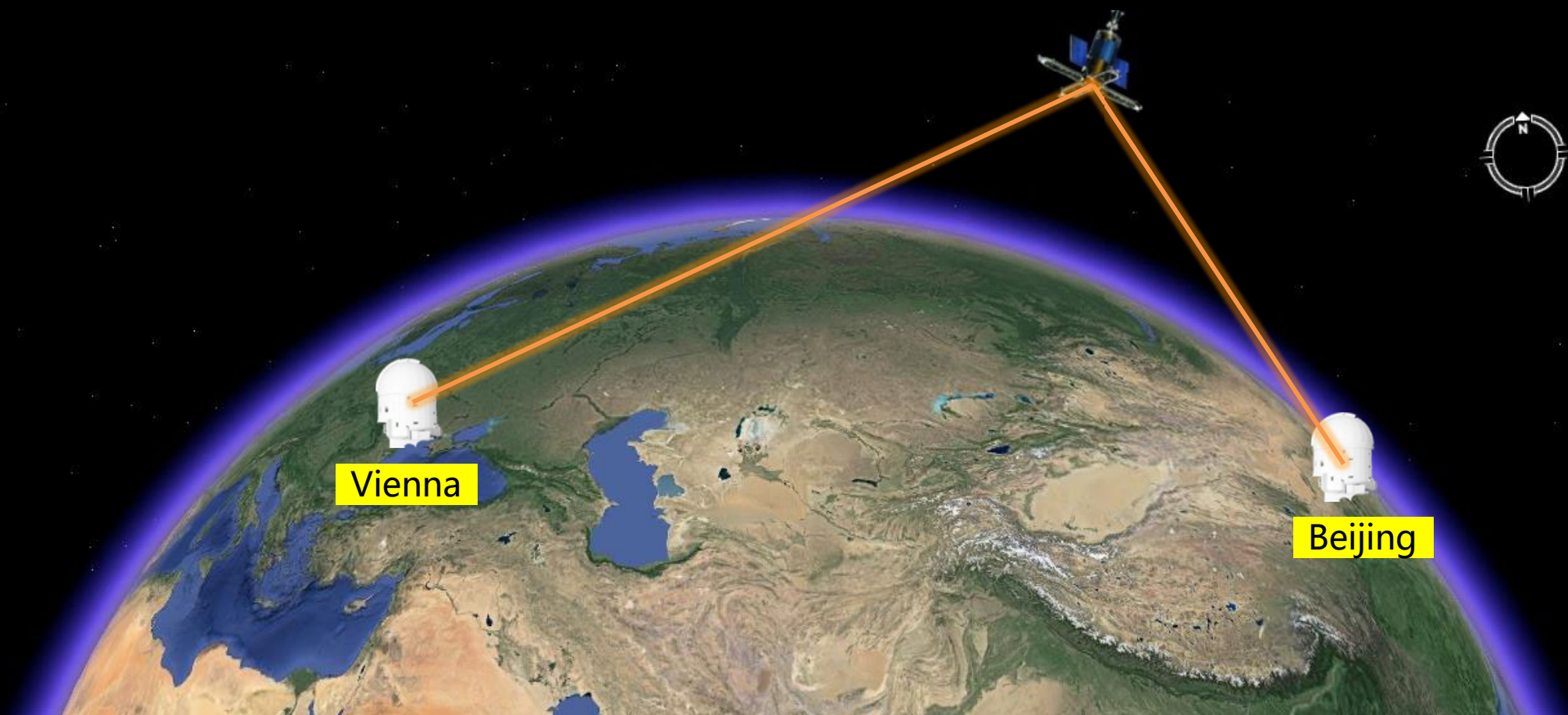


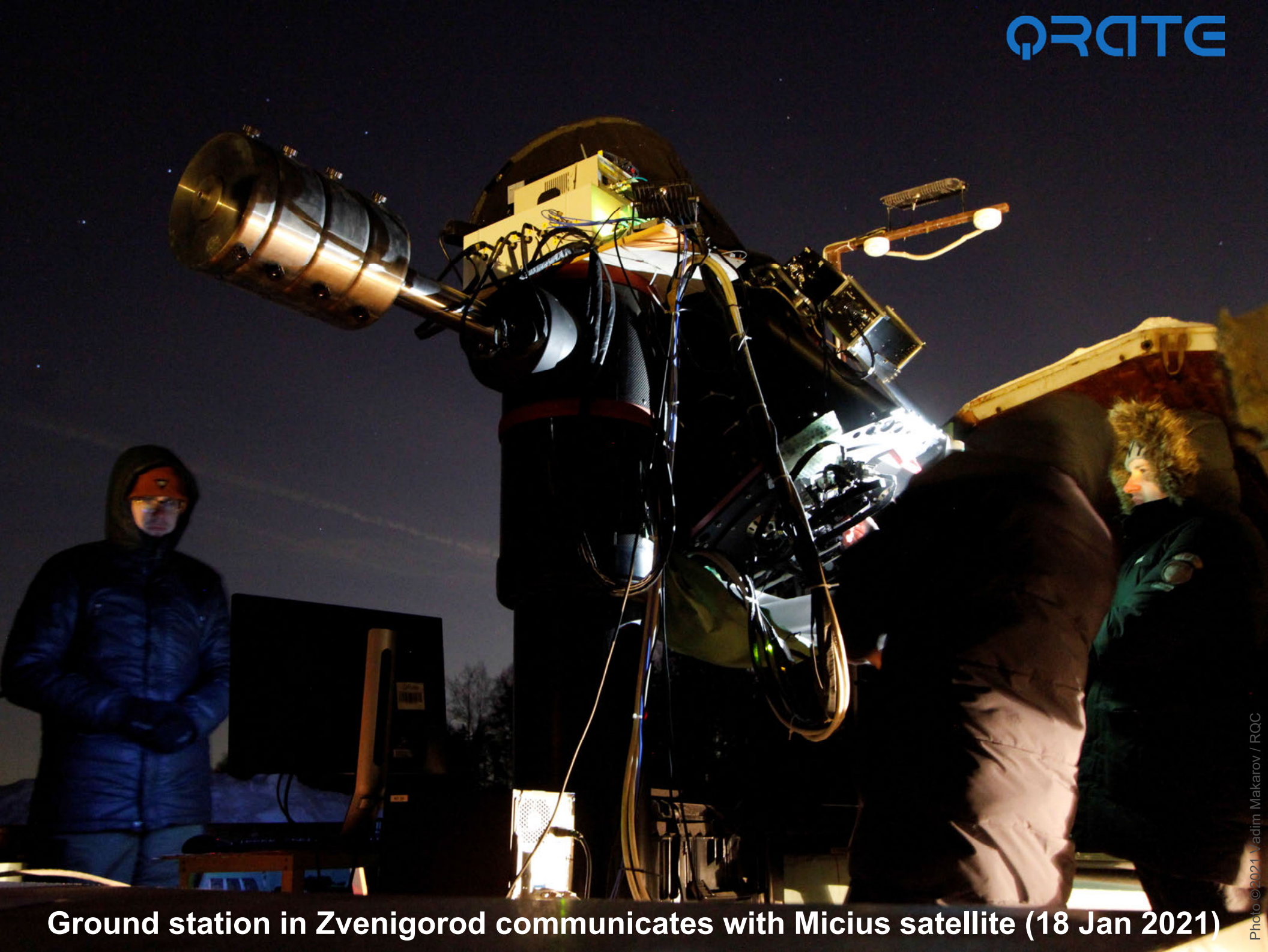
Global quantum key distribution



CAS Strategic Priority Research Program: Quantum Satellite

- Intercontinental quantum key distribution





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

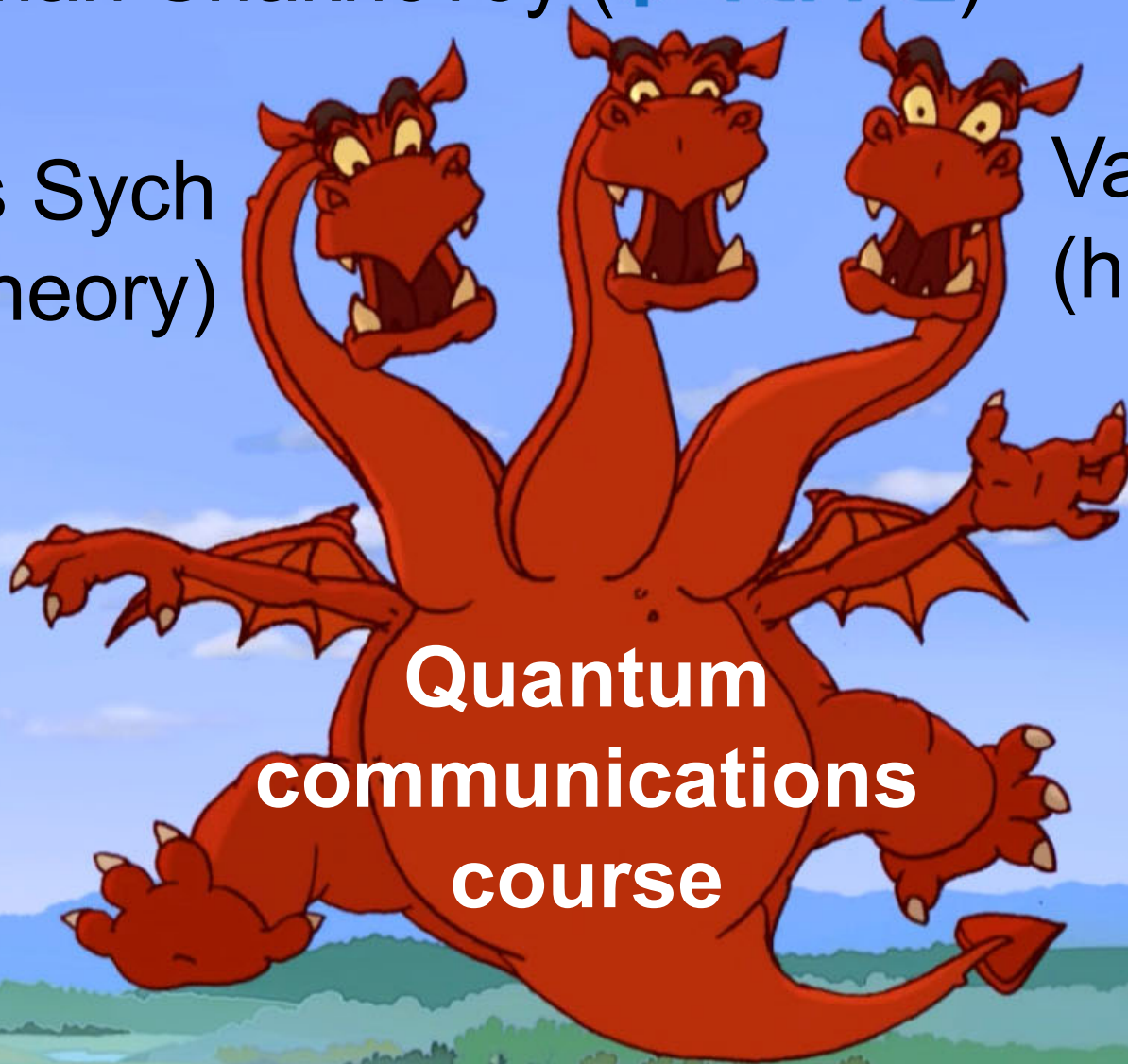


Ground station in Zvenigorod communicates with Micius satellite (18 Jan 2021)

Roman Shakhovoy (QRATE)

Denis Sych
(theory)

Vadim Makarov
(hacking)



**Quantum
communications
course**

www.vad1.com/c/qcomm



Photo ©2020 Vadim Makarov

Labs in quantum photonics and cryptography

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

Manual

