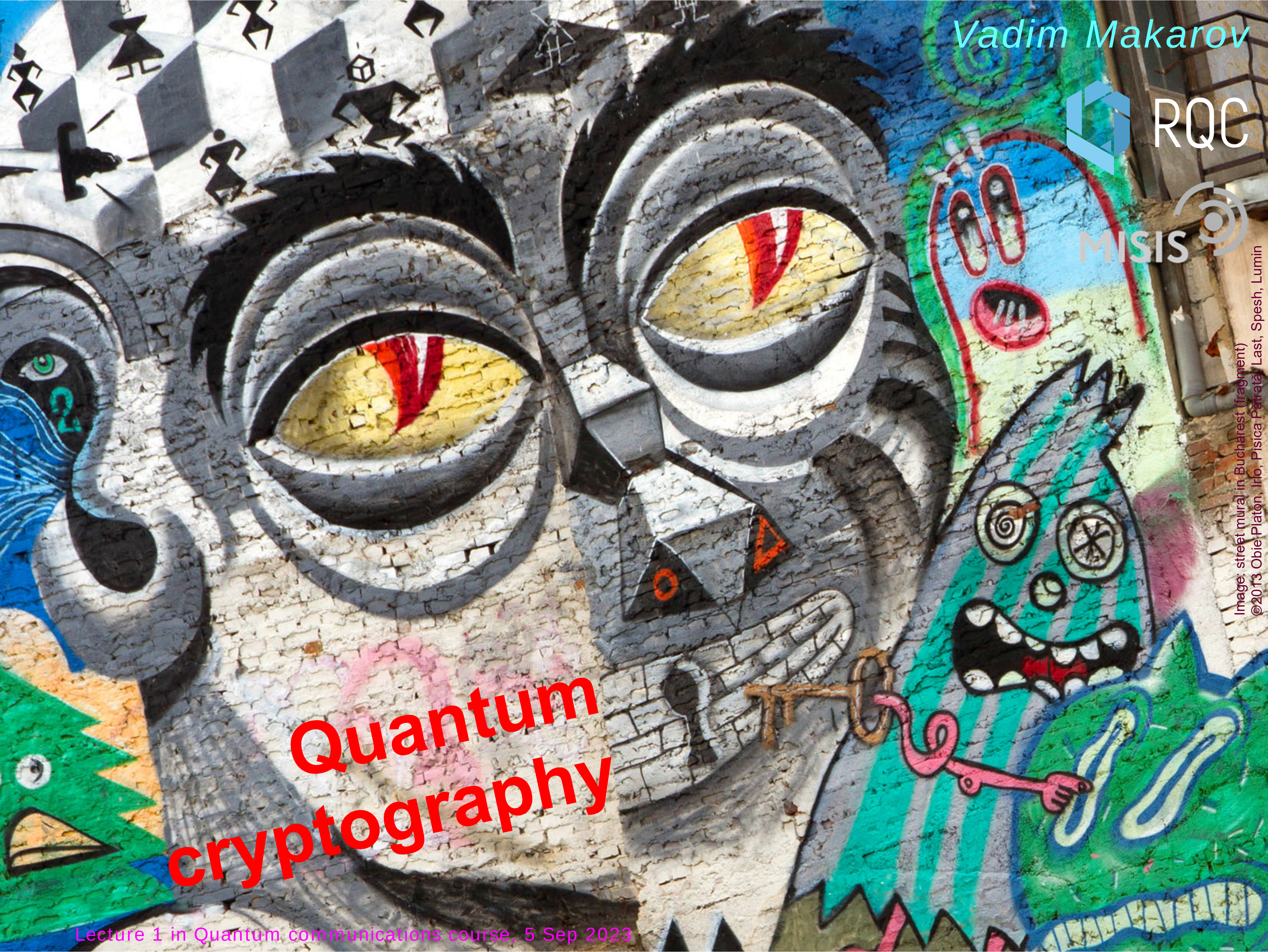


Image: street mural in Bucharest (fragment)
©2013 Obie Platon, Irlo, Pisica Pătrată, Last, Spesh, Lumin

Vadim Makarov

Quantum cryptography

Lecture 1 in Quantum communications course, 5 Sep 2023

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

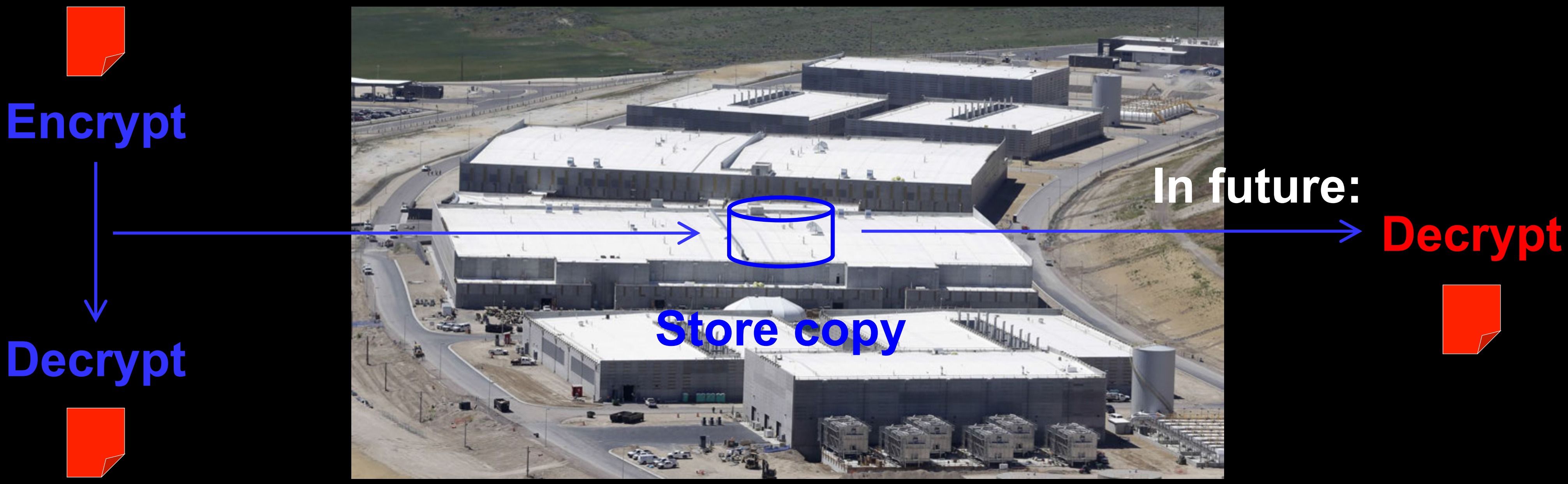
Bypassing government surveillance and censorship

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

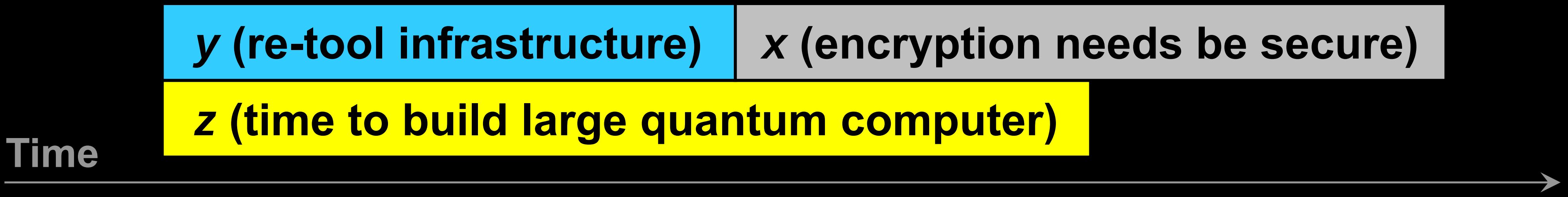
Store copy

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

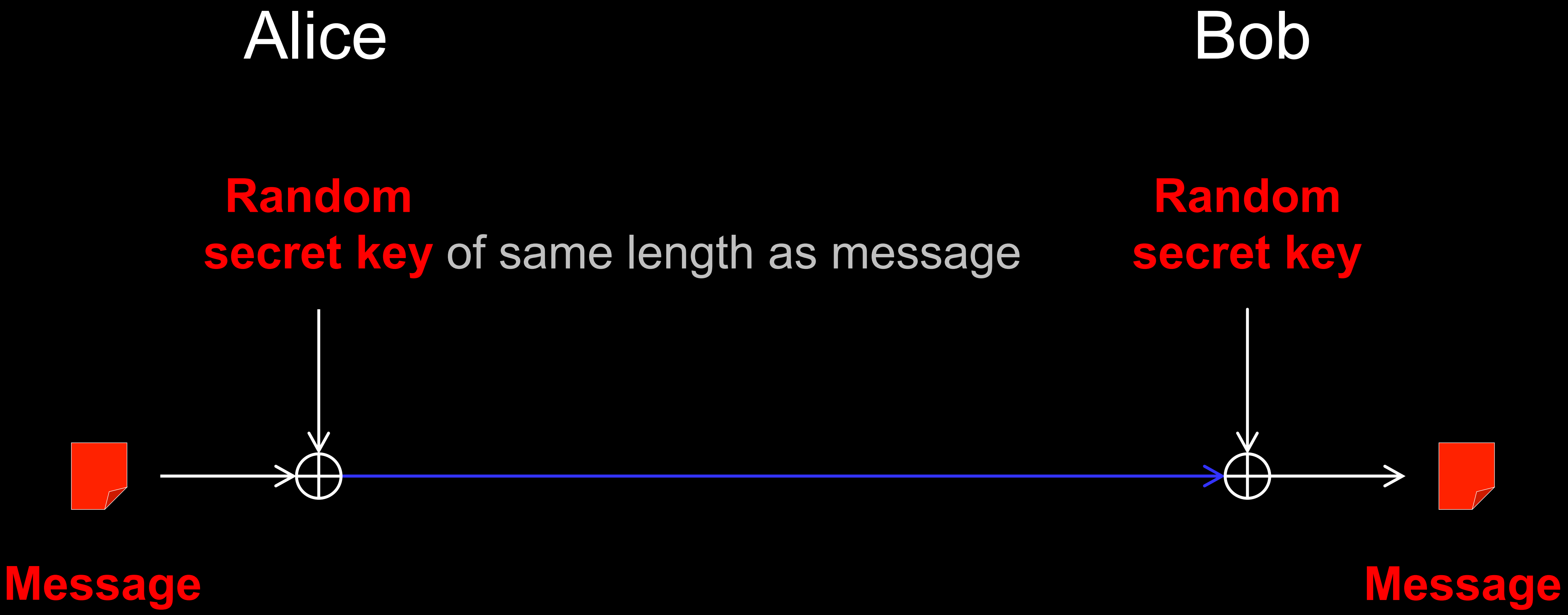
If $x + y > z$, then worry.

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	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

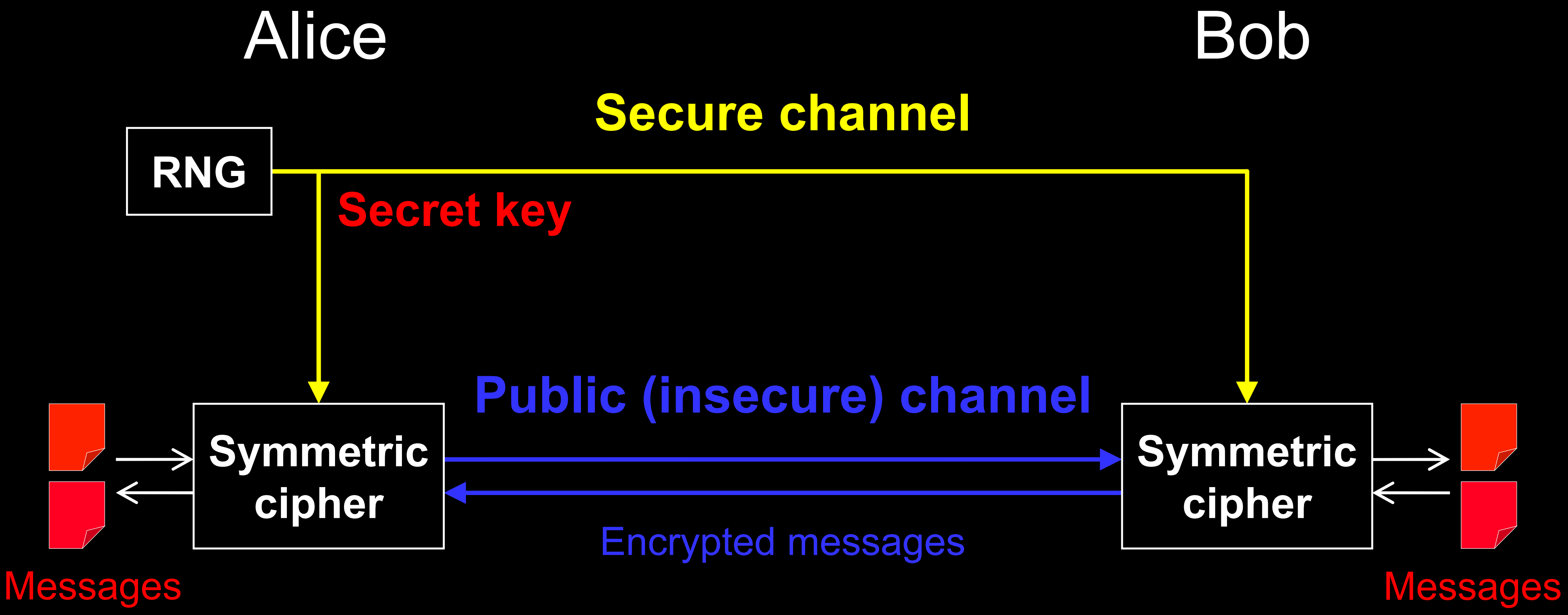
		Broken?
Monoalphabetic cipher	invented ~50 BC (J. Caesar)	~850 (Al-Kindi)
Nomenclators (code books)	~1400 – ~1800	✓
Polyalphabetic (Vigenère)	1553 – ~1900	1863 (F. W. Kasiski)
…		
One-time pad	invented 1918 (G. Vernam)	**impossible** (C. Shannon 1949)
Polyalphabetic electromechanical (Enigma, Purple,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

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.*

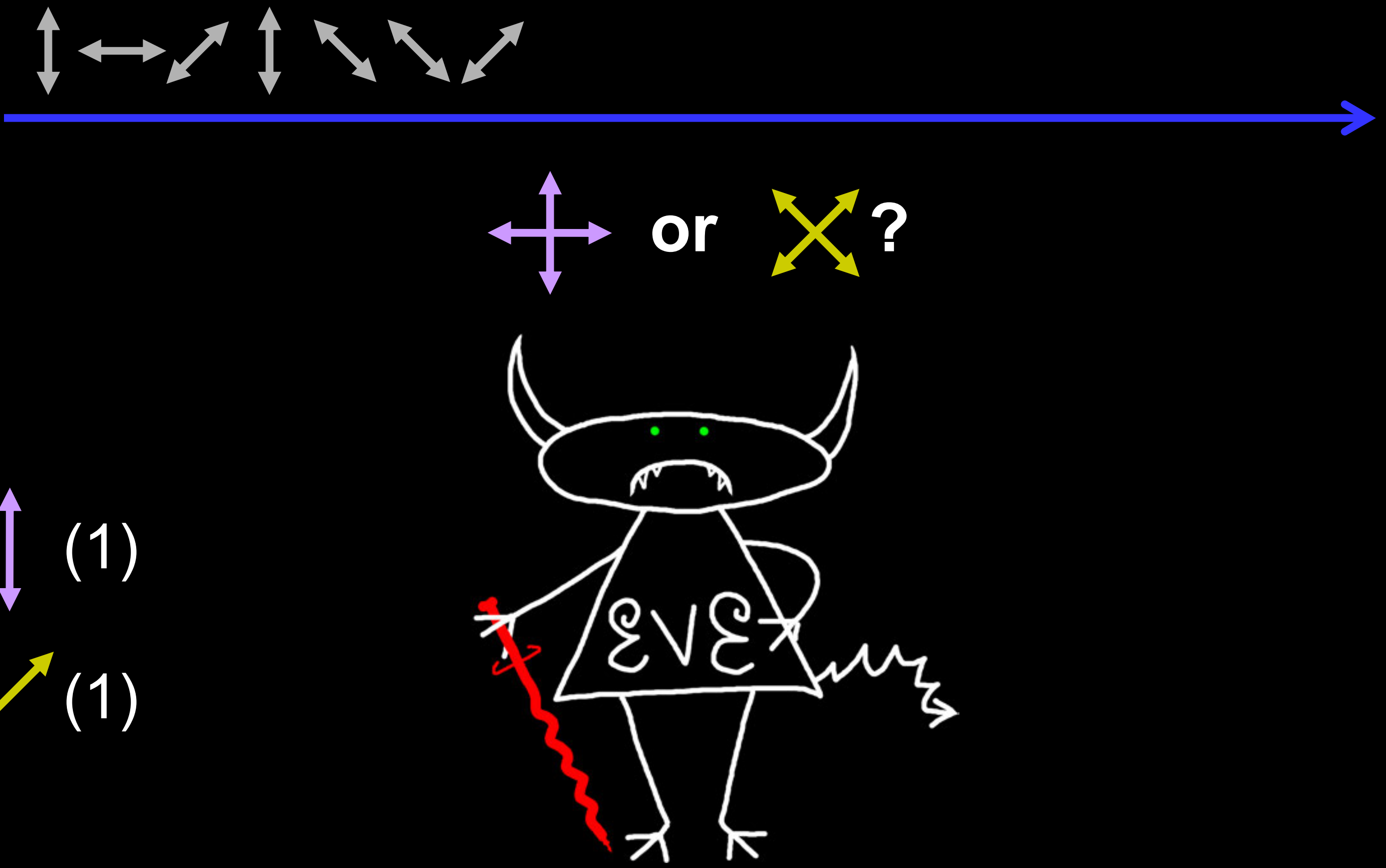
Quantum key distribution (QKD)

Alice

Prepares photons

↔ (0), ↕ (1)

↘ (0), ↗ (1)



Eavesdropping introduces errors

Bob

Measures photons

✛

✕

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)

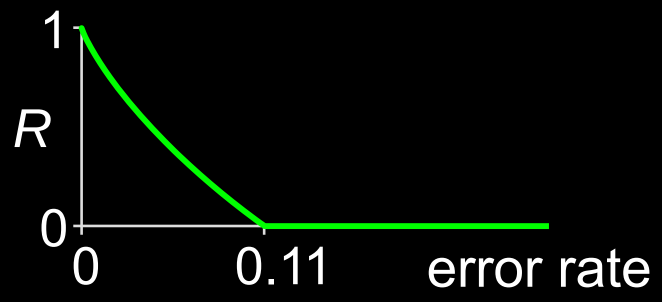
↓

Error correction

↓ error rate

Secret key rate estimation

↓ *R*



Privacy amplification (compress key using a hash function)

↓

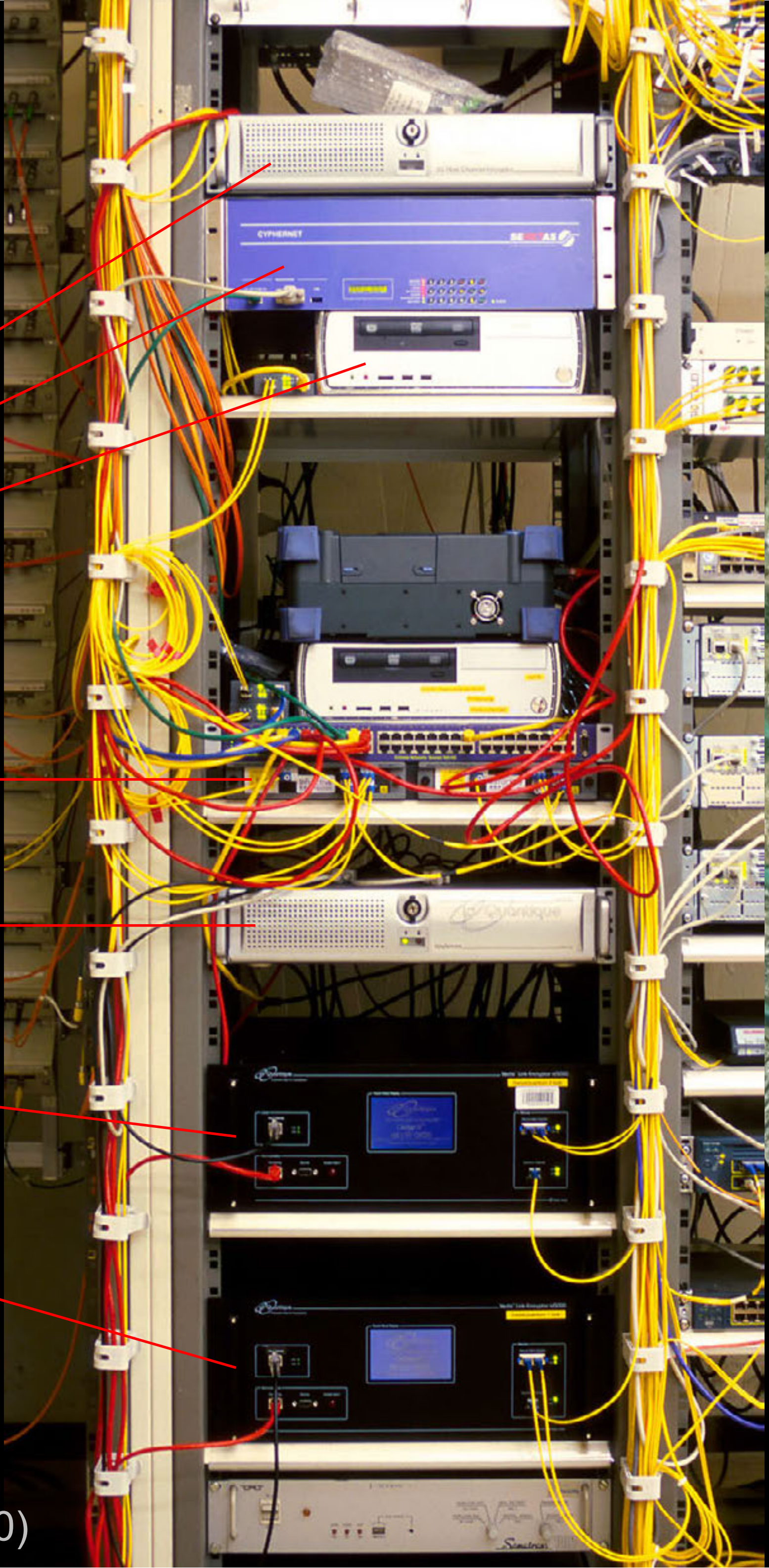
Authentication Alice–Bob ← 1st time: initial short key, or public-key infrastructure

↓

Secret key — small fraction

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

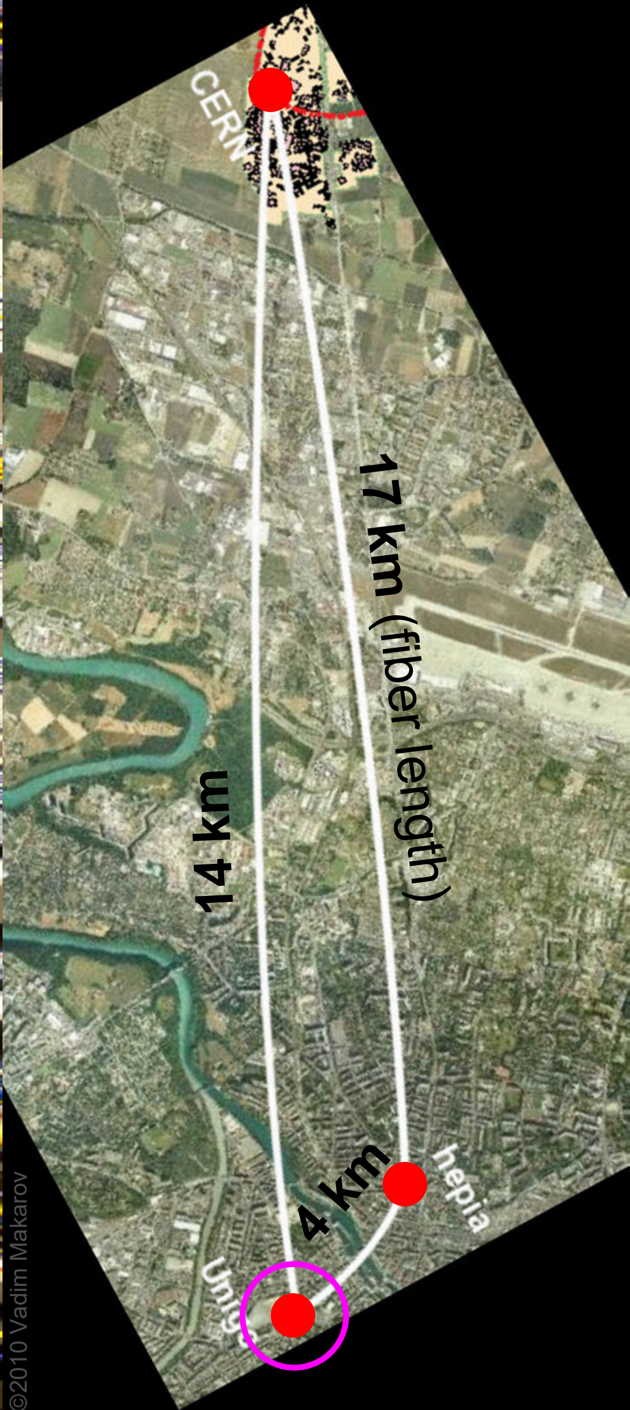
WDMs

Key manager

QKD to another node
(4 km)

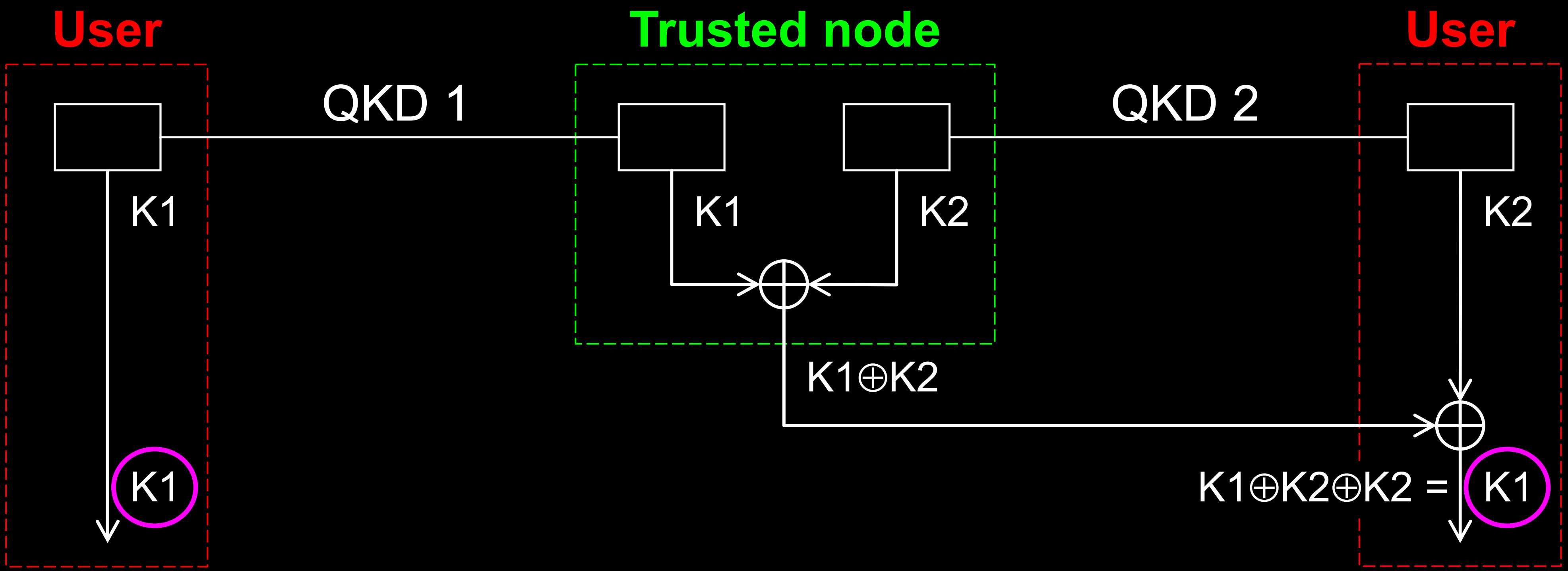
QKD to another node
(14 km)

Photo ©2010 Vadim Makarov

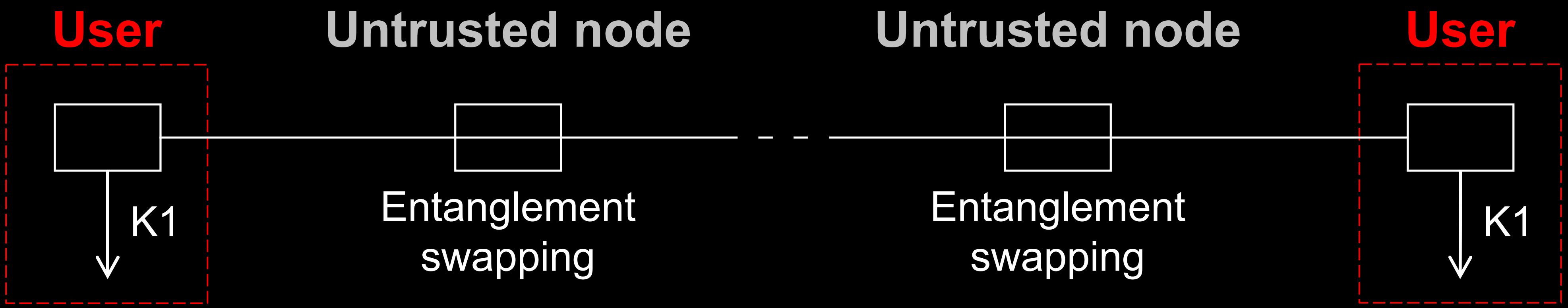


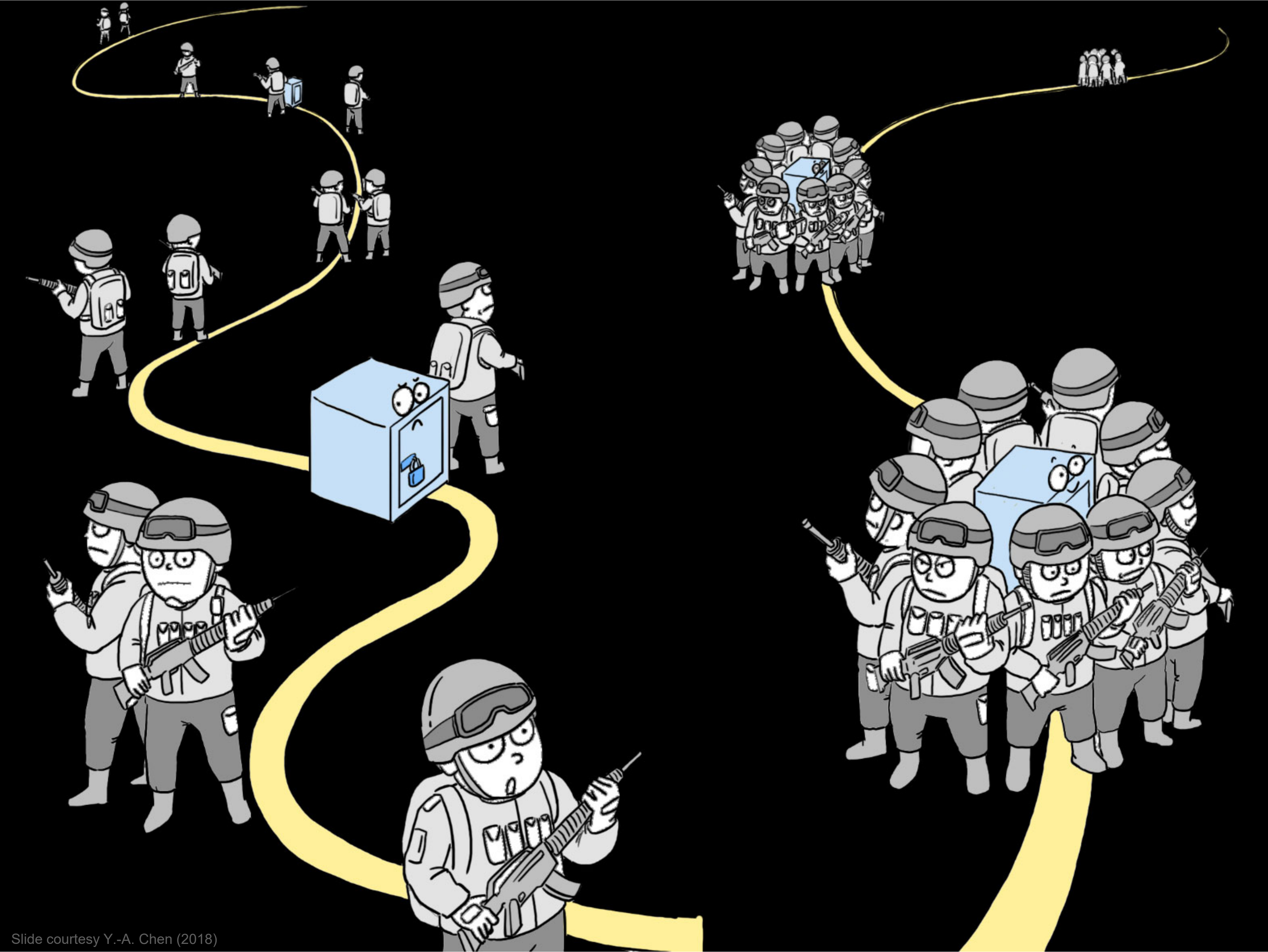
www.swissquantum.com
ID Quantique *Cerberis* system (2010)

Today: trusted-node repeater



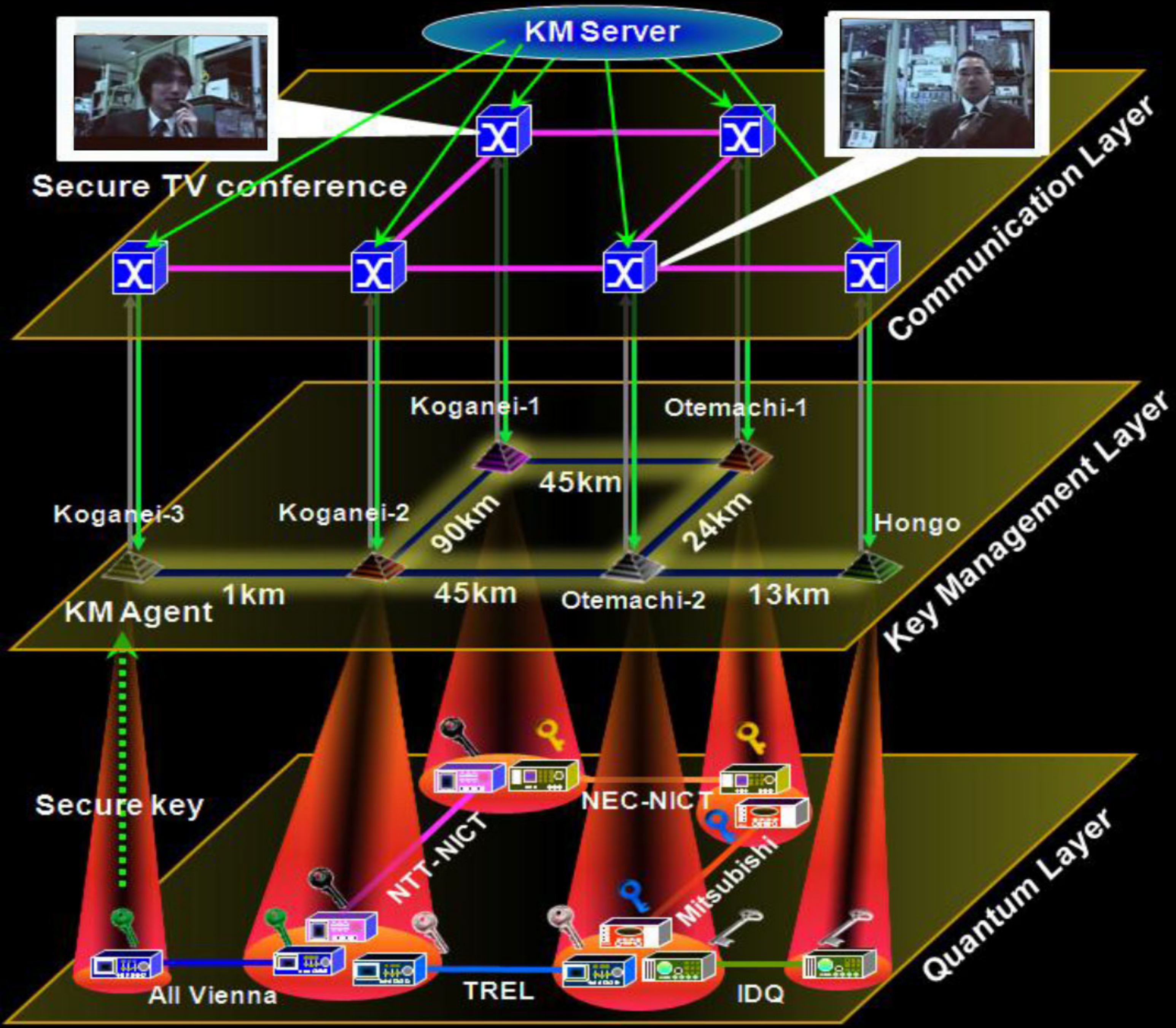
Future: quantum repeater





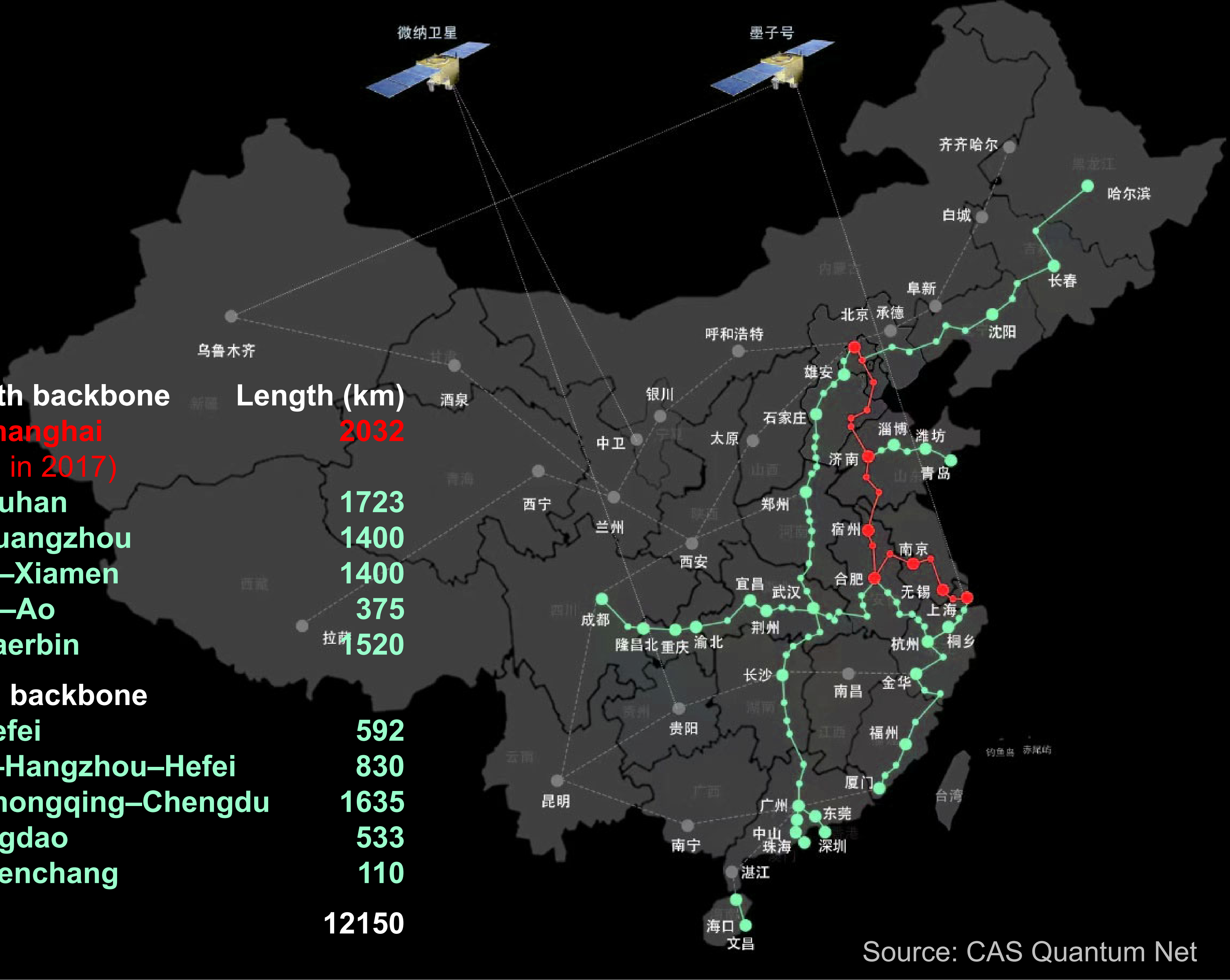
Slide courtesy Y.-A. Chen (2018)

Trusted-node network



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

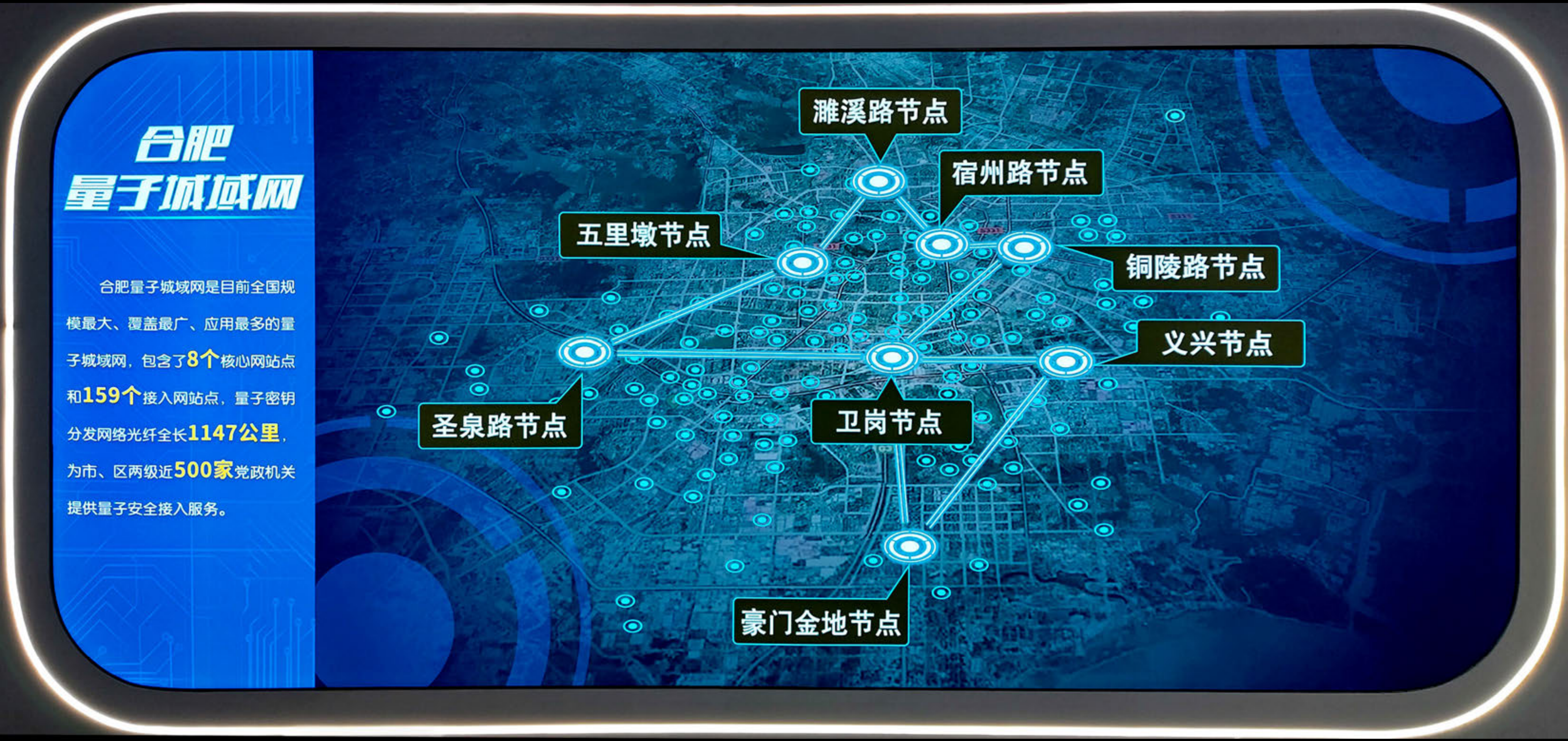
China’s QKD backbone network (as of July 2023)



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

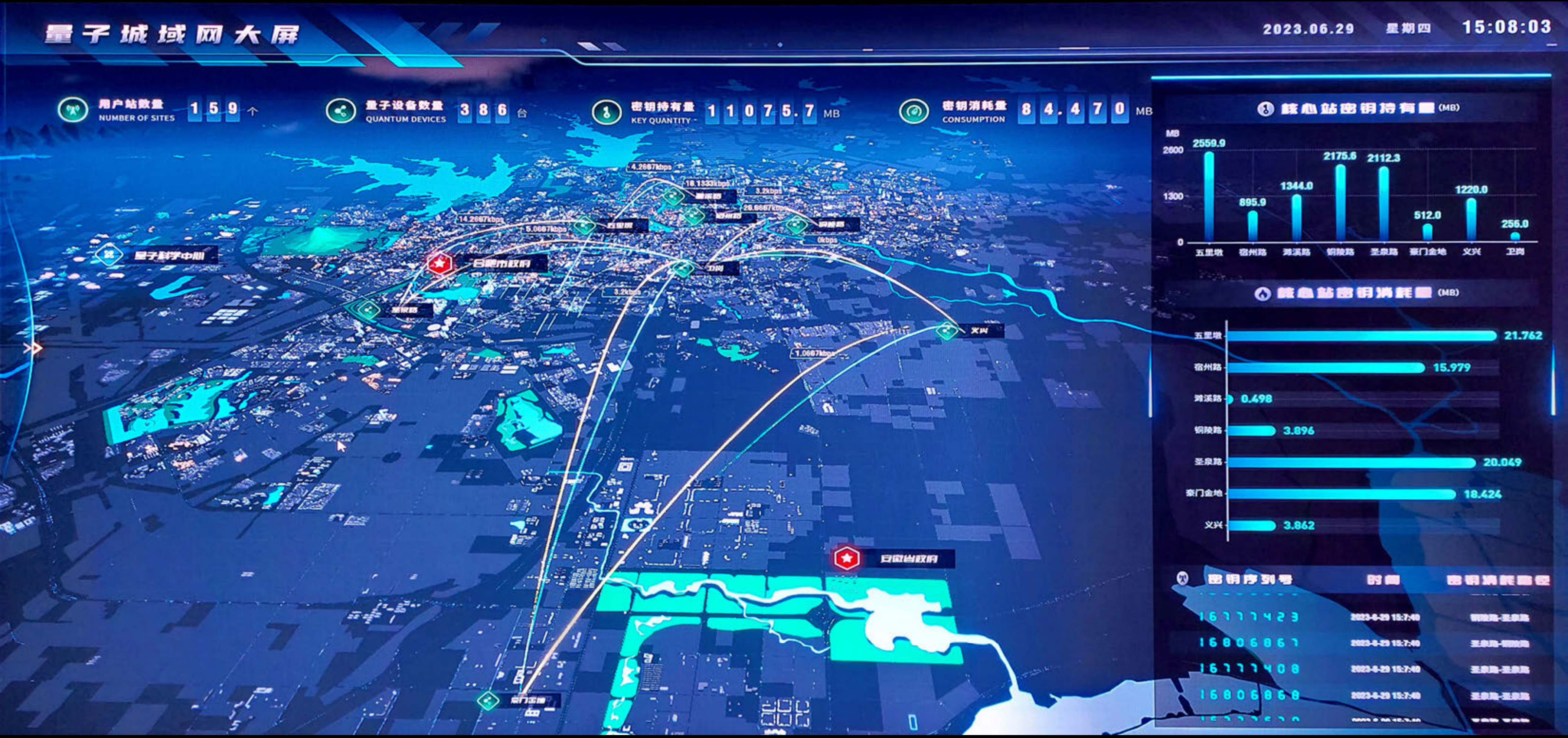


合肥
量子城域网

合肥量子城域网是目前全国规模最大、覆盖最广、应用最多的量子城域网，包含了**8个**核心网站点和**159个**接入网站点，量子密钥分发网络光纤全长**1147公里**，为市、区两级近**500家**党政机关提供量子安全接入服务。

Source: QuantumCTek

Metropolitan QKD network in Hefei



量子城域网大屏

2023.06.29 星期四 15:08:03

用户站数量 NUMBER OF SITES 159 个

量子设备数量 QUANTUM DEVICES 386 台

密钥持有量 KEY QUANTITY 11075.7 MB

密钥消耗量 CONSUMPTION 84.470 MB

密钥序列号	时间	密钥消耗路径
16777423	2023-6-29 15:7:40	铜陵路-圣泉路
16806867	2023-6-29 15:7:40	圣泉路-[illegible]
16777408	2023-6-29 15:7:40	圣泉路-圣泉路
16806868	2023-6-29 15:7:40	圣泉路-圣泉路

Source: QuantumCTek

Photo ©2023 Vadim Makarov

Superconducting quantum computer (~60 qubit)

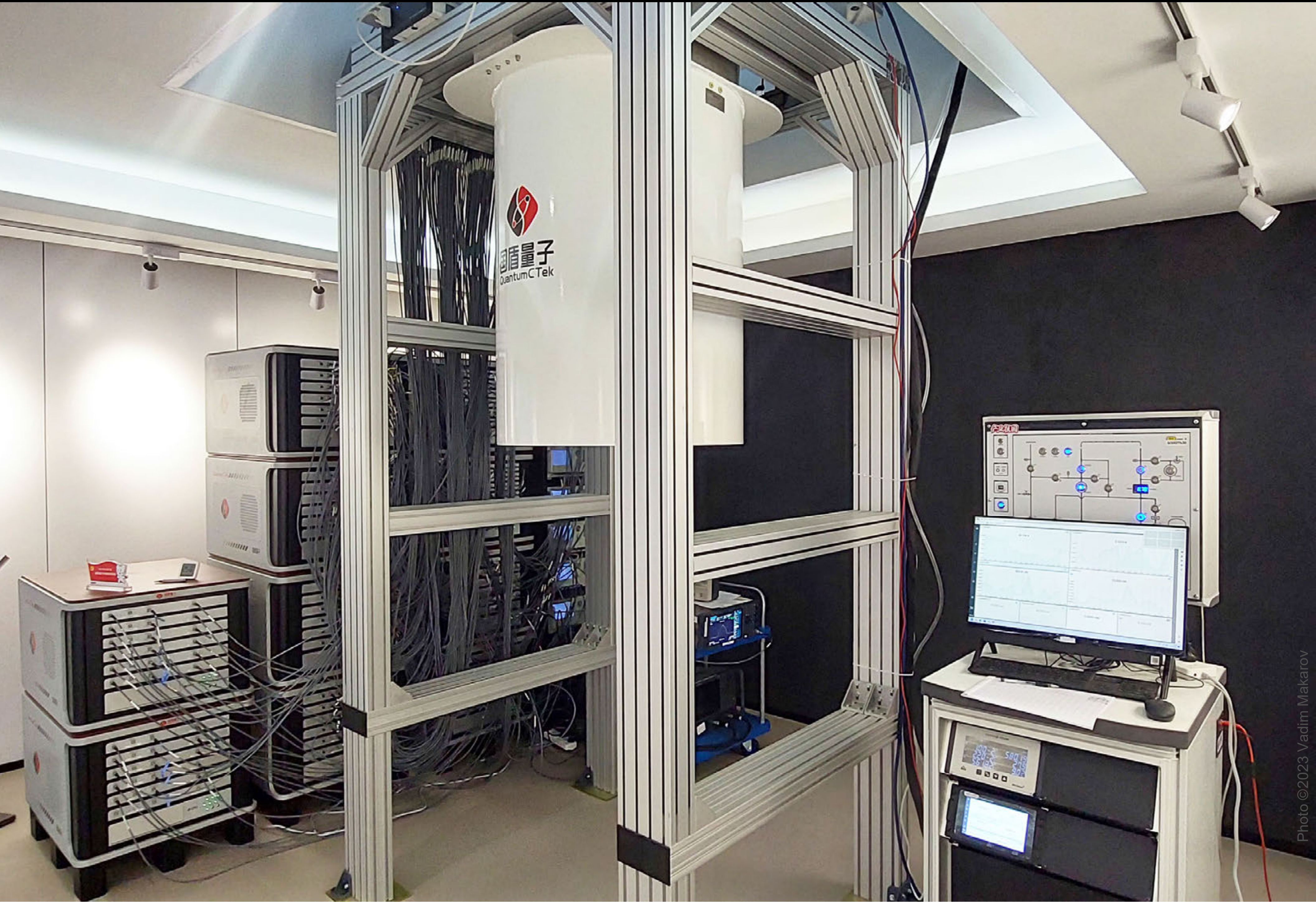


Photo ©2023 Vadim Makarov

Printed circuit board assembly lines

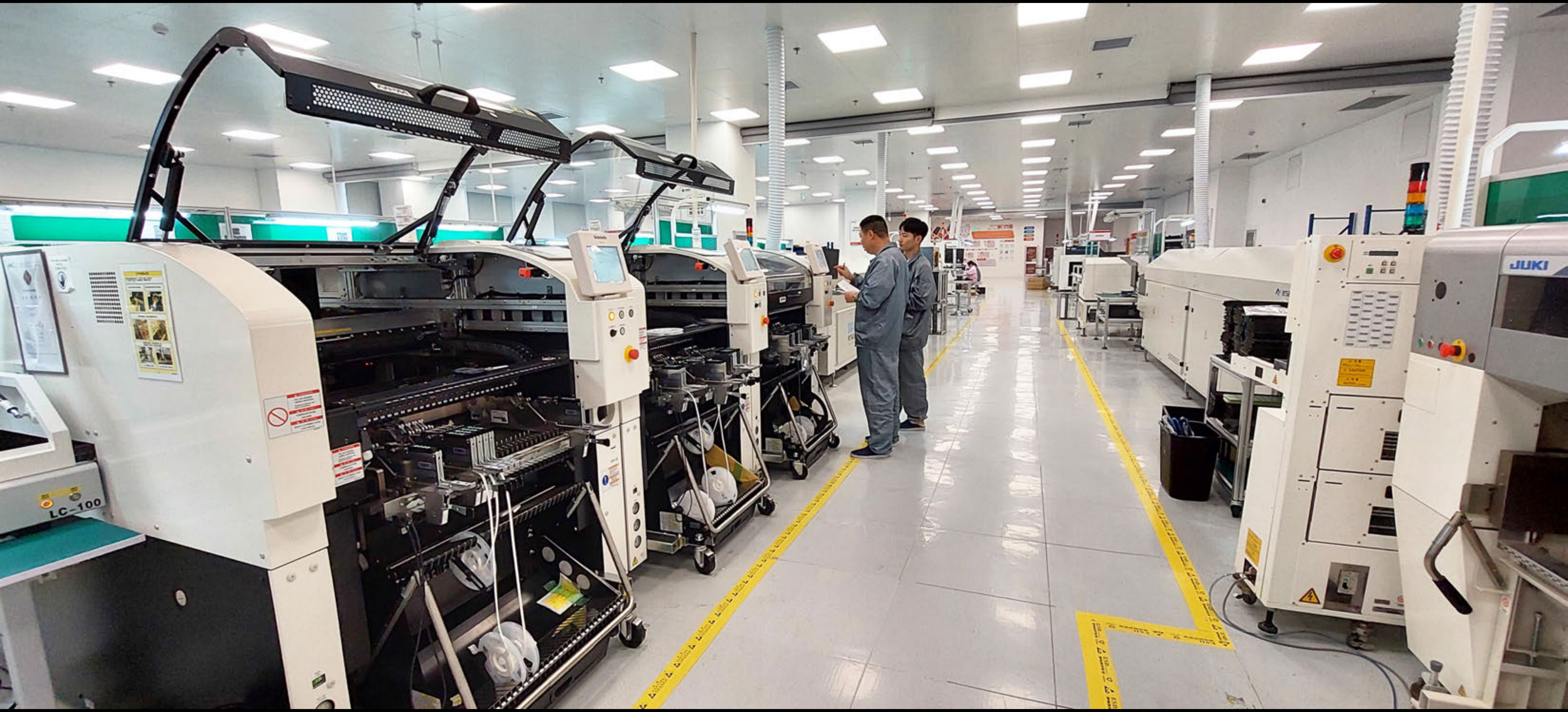


Photo ©2023 Vadim Makarov

Assembling quantum computers

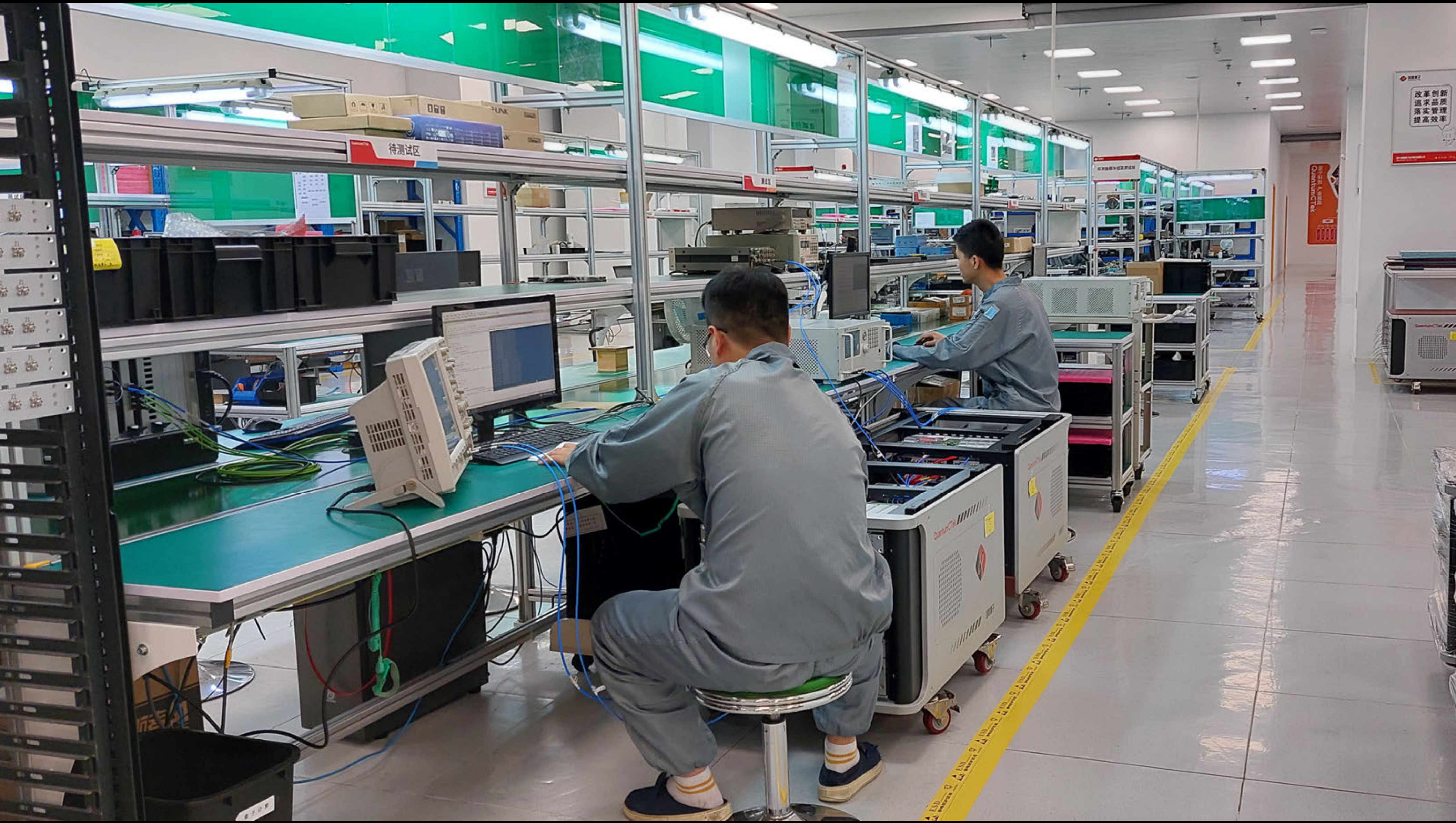


Photo ©2023 Vadim Makarov

Production ward

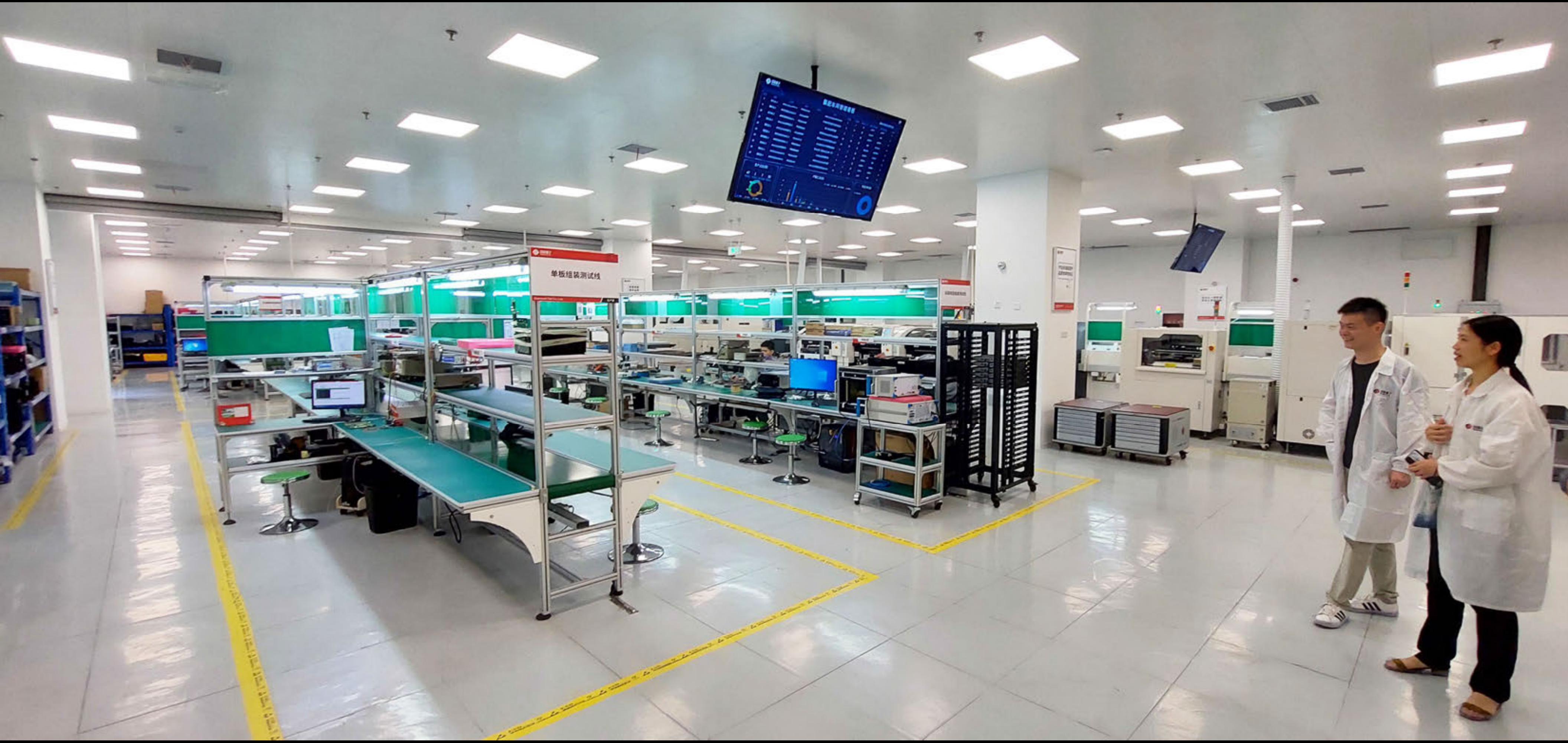


Photo ©2023 Vadim Makarov

QKD testing stations

Photo ©2023 Vadim Makarov

Environmental testing chambers

Photo ©2023 Vadim Makarov

QKD burn-in racks and units ready for shipment

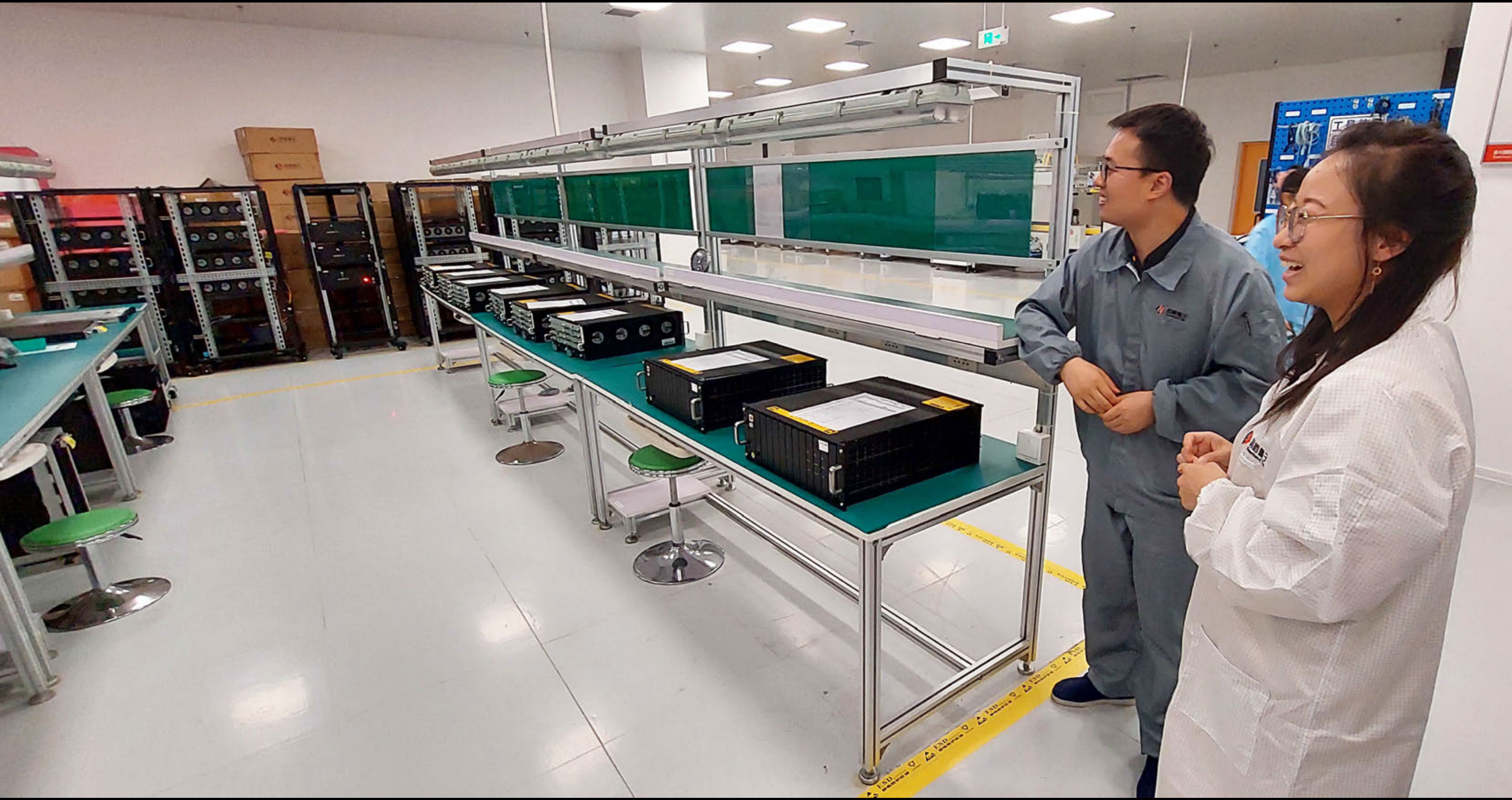


Photo ©2023 Vadim Makarov

QKD packaging line

Photo ©2023 Vadim Makarov

QKD repair-and-service ward

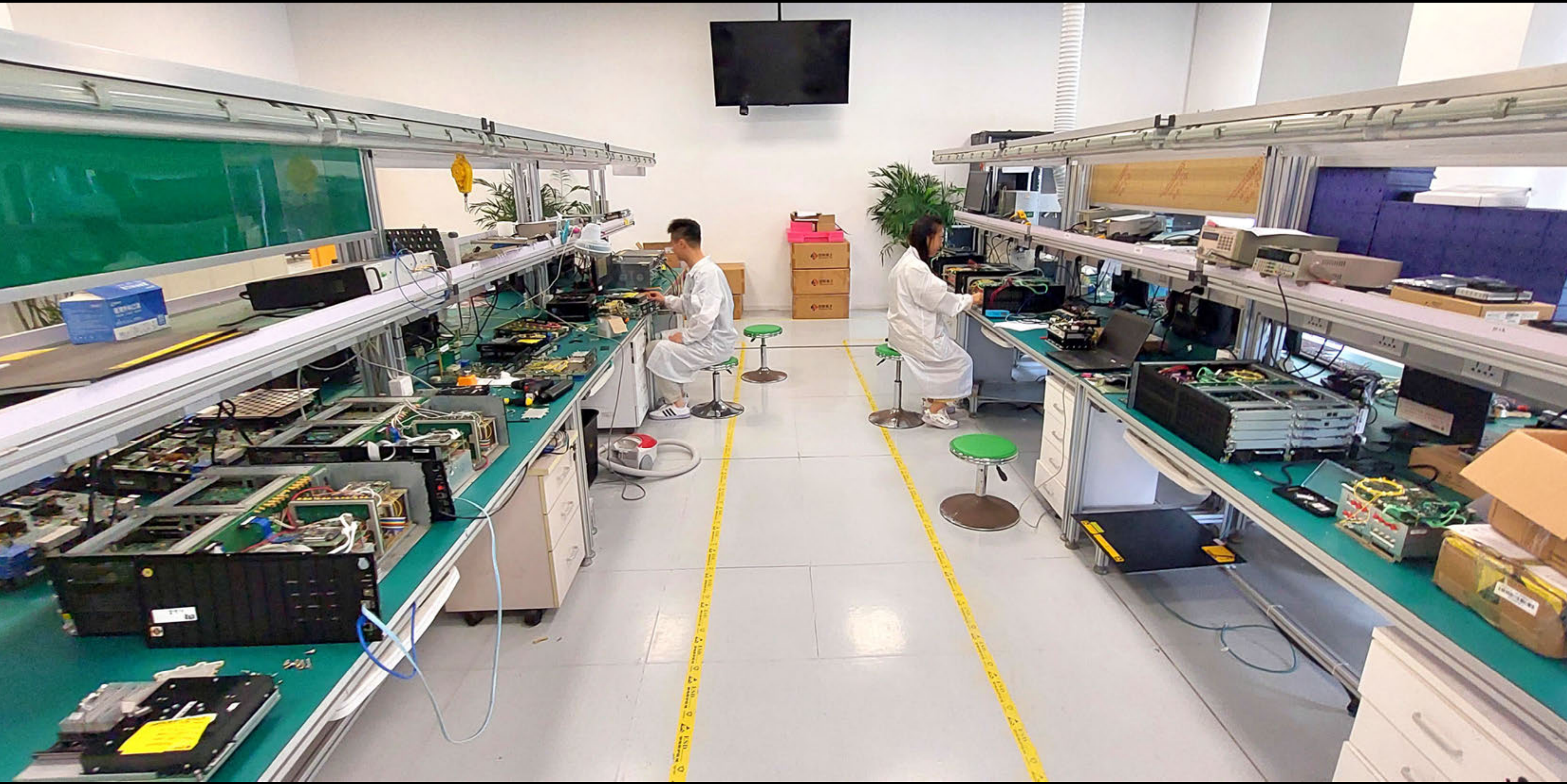


Photo ©2023 Vadim Makarov

QKD repair-and-service ward

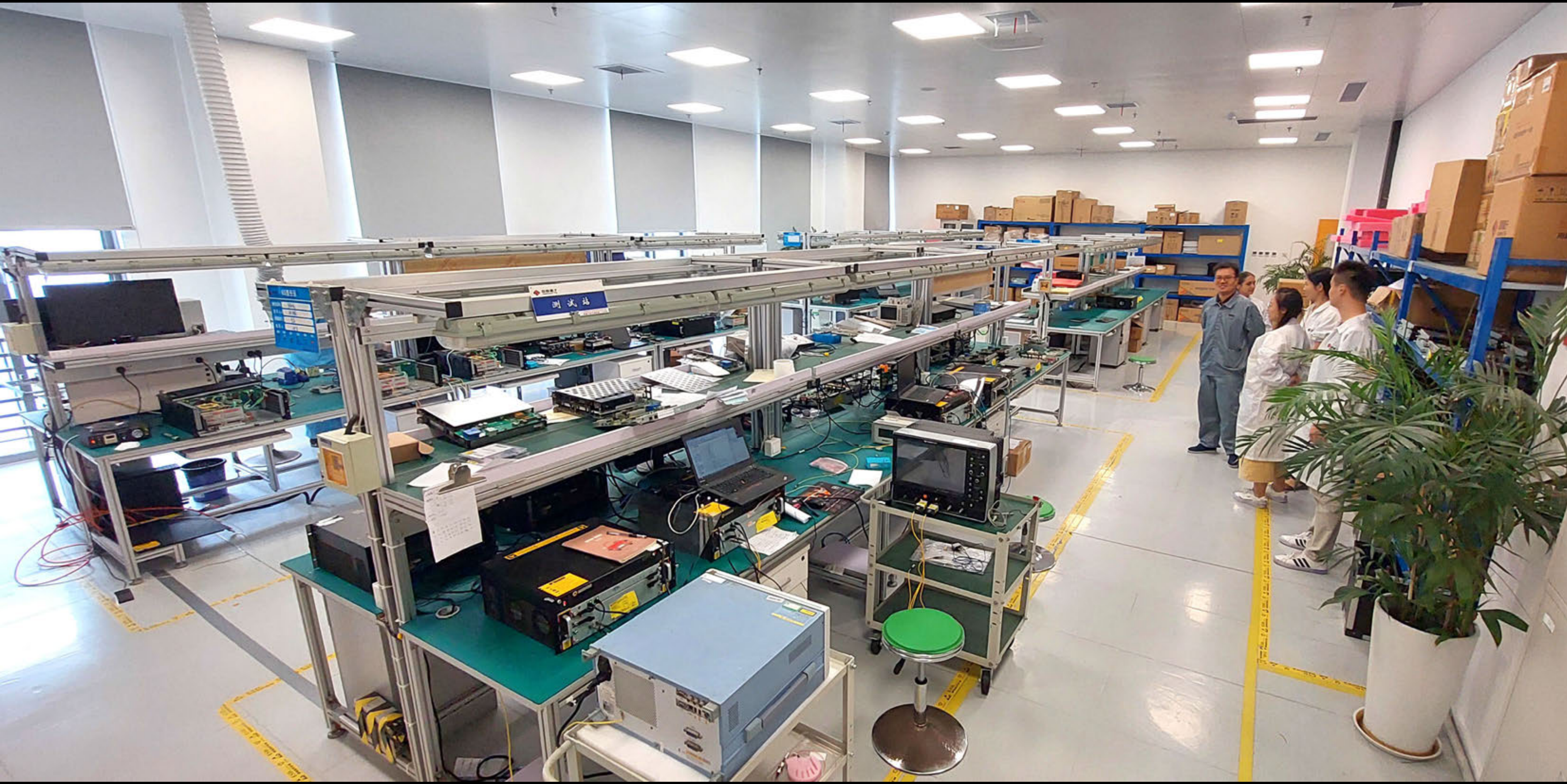
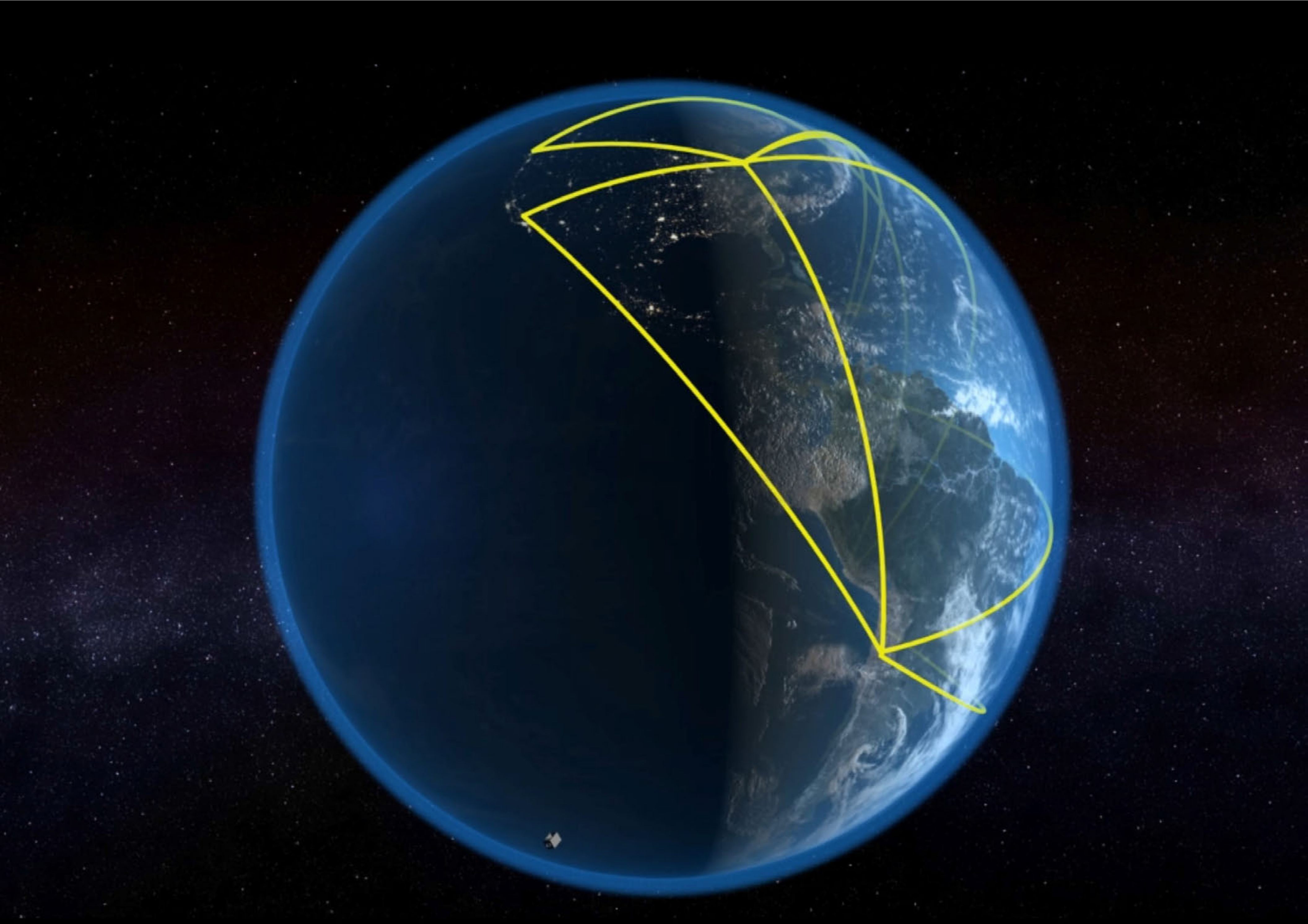


Photo ©2023 Vadim Makarov

Global quantum key distribution

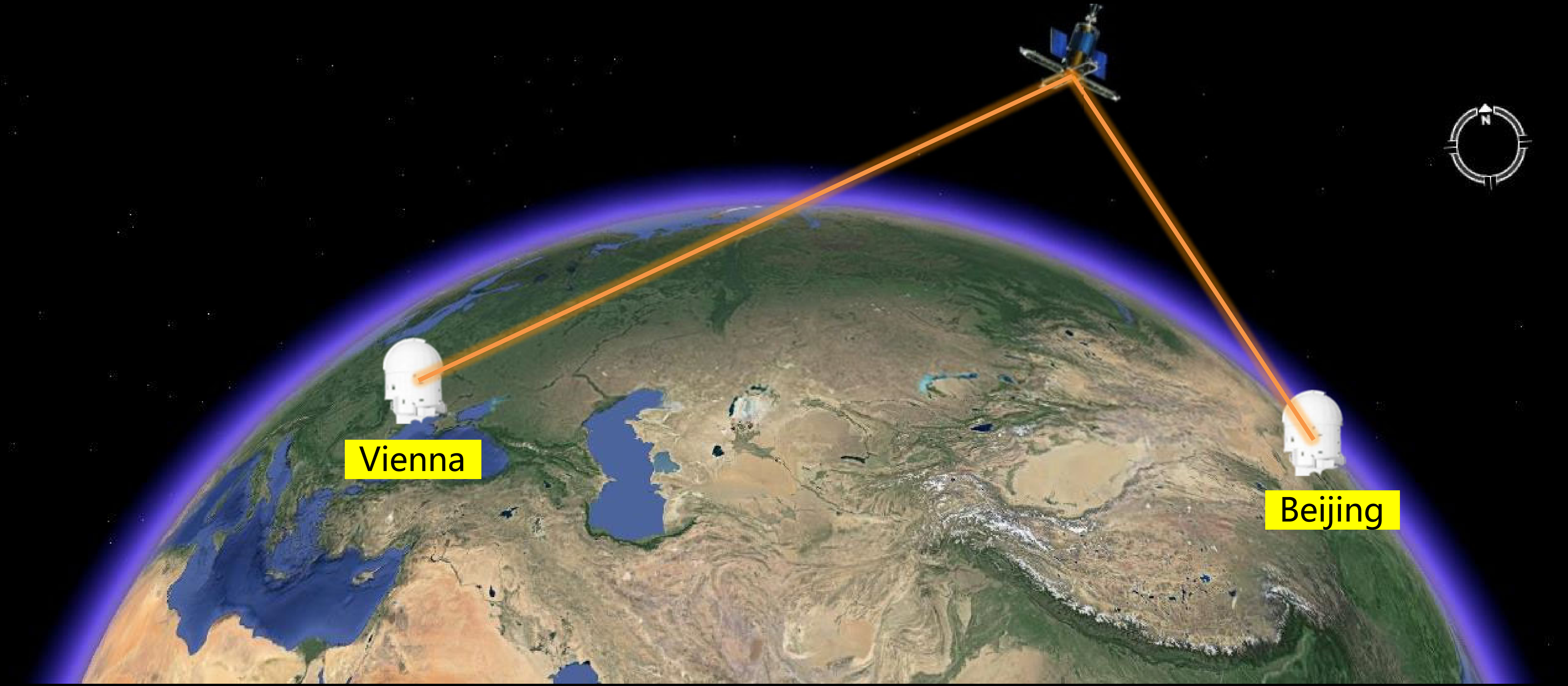
Video ©2012 IQC / group of T. Jennewein



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

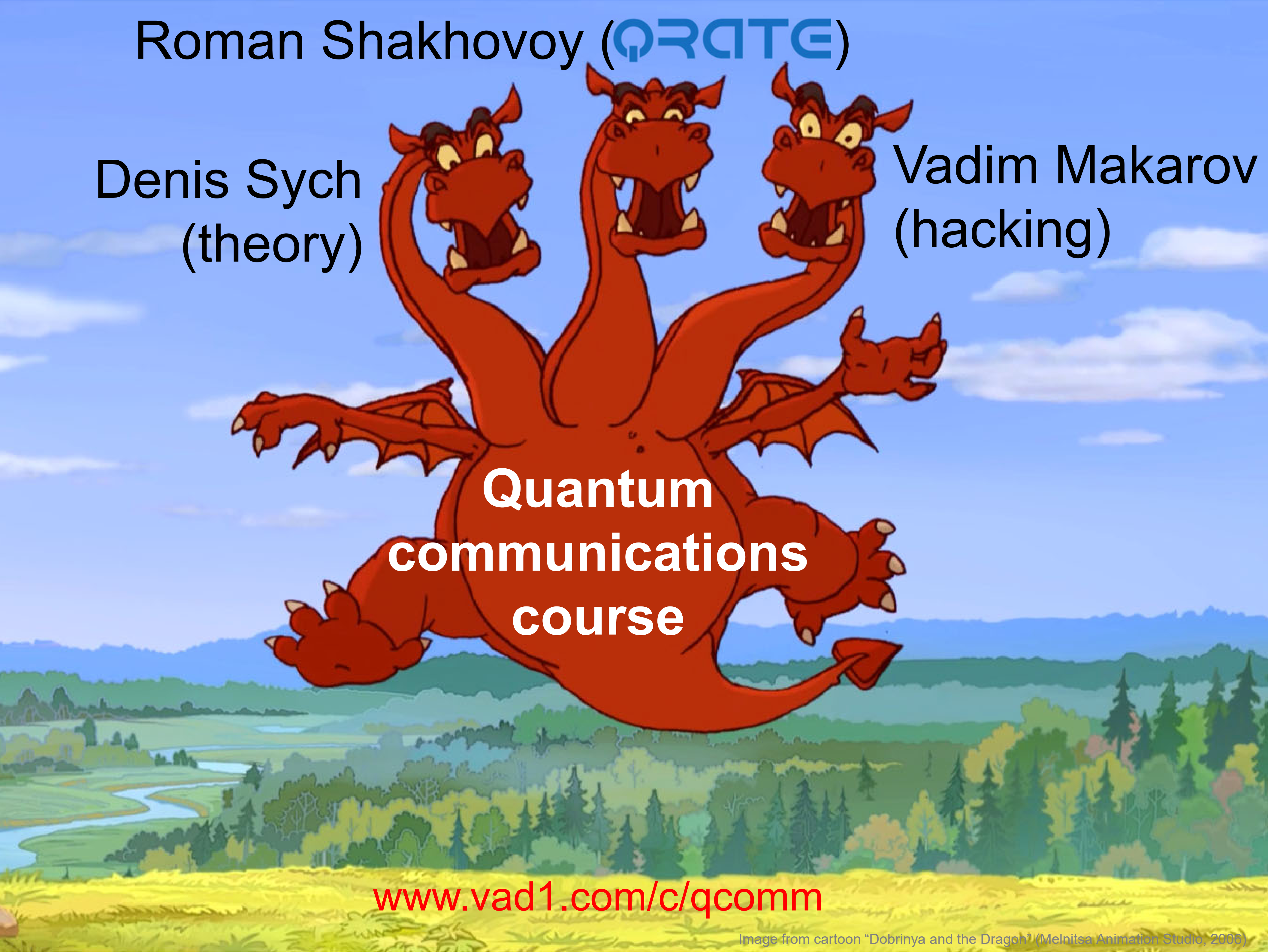
Review of results: C.-W. Lu, Y. Cao, C.-Z. Peng, J.-W. Pan, Rev. Mod. Phys. **94**, 035001 (2022)

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

Photo ©2021 Vadim Makarov / RQC

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

Photo ©2021 Vadim Makarov / RQC



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)