QuIIN
Quantum Industrial Innovation

Quantum Cryptography

Dr. Alexandre Baron Tacla
alexandre.tacla@fieb.org.br

QuIIN – Quantum Industrial Innovation
EMBRAPII CIMATEC Competence Center in Quantum Technologies
SENAI - CIMATEC

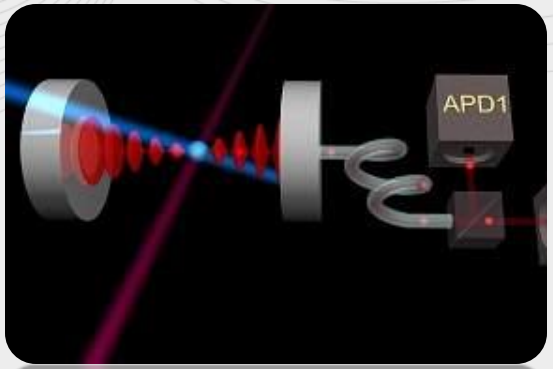
SENAI CIMATEC
EMBRAPII
Empresa Brasileira de Pesquisa e Inovação Industrial
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Financial resoures from the PPI IoT/Manufatura 4.0

Quantum Technologies

Quantum Computing

Quantum Communication & Cryptography



Quantum Sensors

Quantum Information Theory & Principles of Quantum Mechanics

Quantum Computing Dream or Nightmare?

Otimization

Logistics problems
Combinatorial optimization

Artificial Intelligence

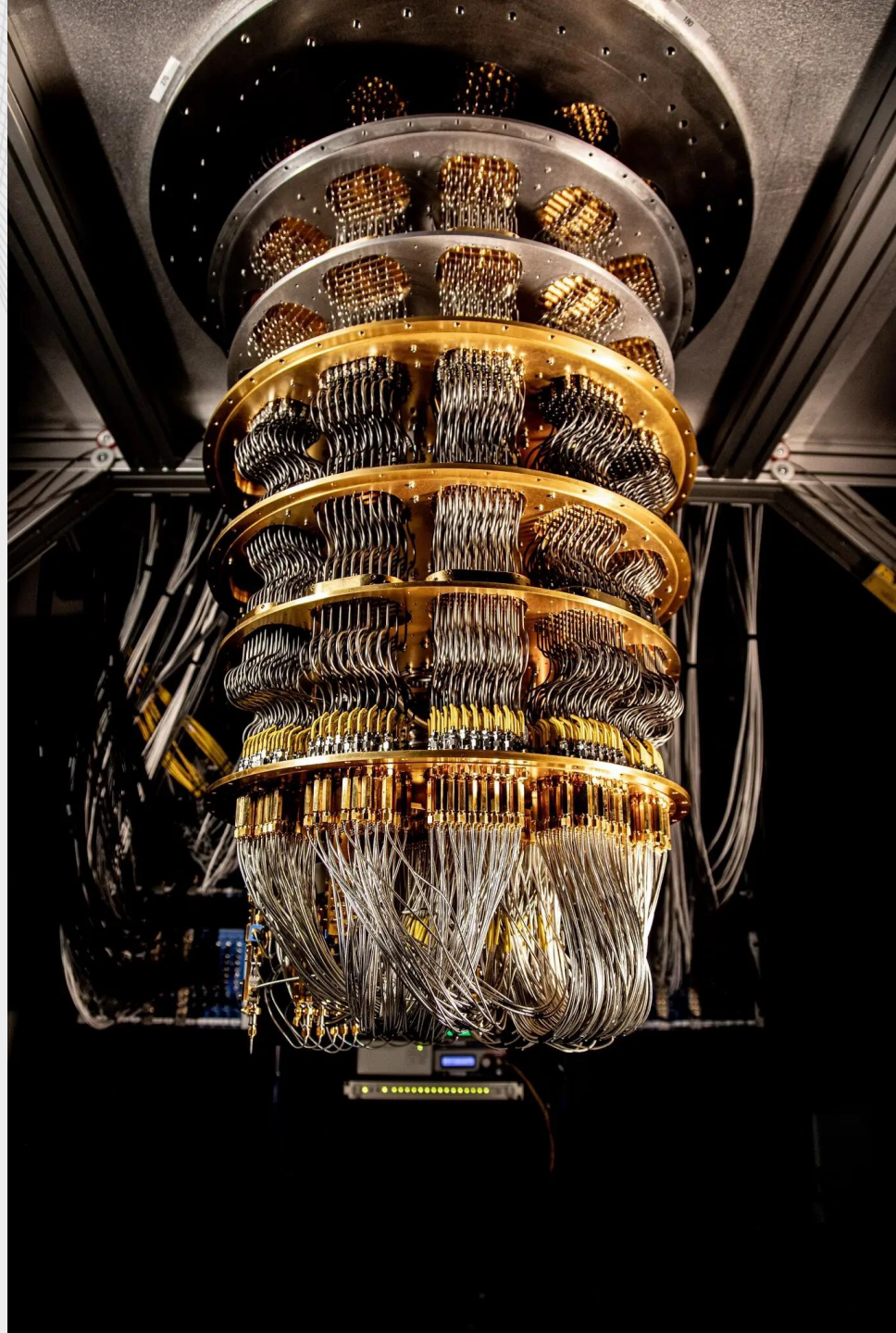
More compact models
Energy efficiency

Simulations

Precise molecular models
New materials

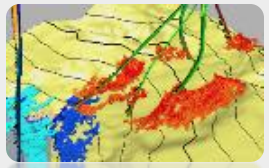
Criptanalysis

Breaking asymmetric cryptography protocols



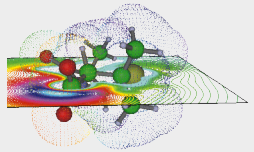
Quantum Computing
Potential Applications

Petroleum



- Geophysics and Seismic
- Inversion and Imaging
- Well Optimization
- Routing Problems

Chemistry



- Quantum Batteries
- Thermal Machines
- Molecules Simulation

Finance

- Portfolio optimization
- Credit Risk
- Credit Scoring
- Feature Selection

AI

- Quantum Classifiers
- Quantum Generative adversarial network (GANs)
- Variational Quantum Classifiers

Energy

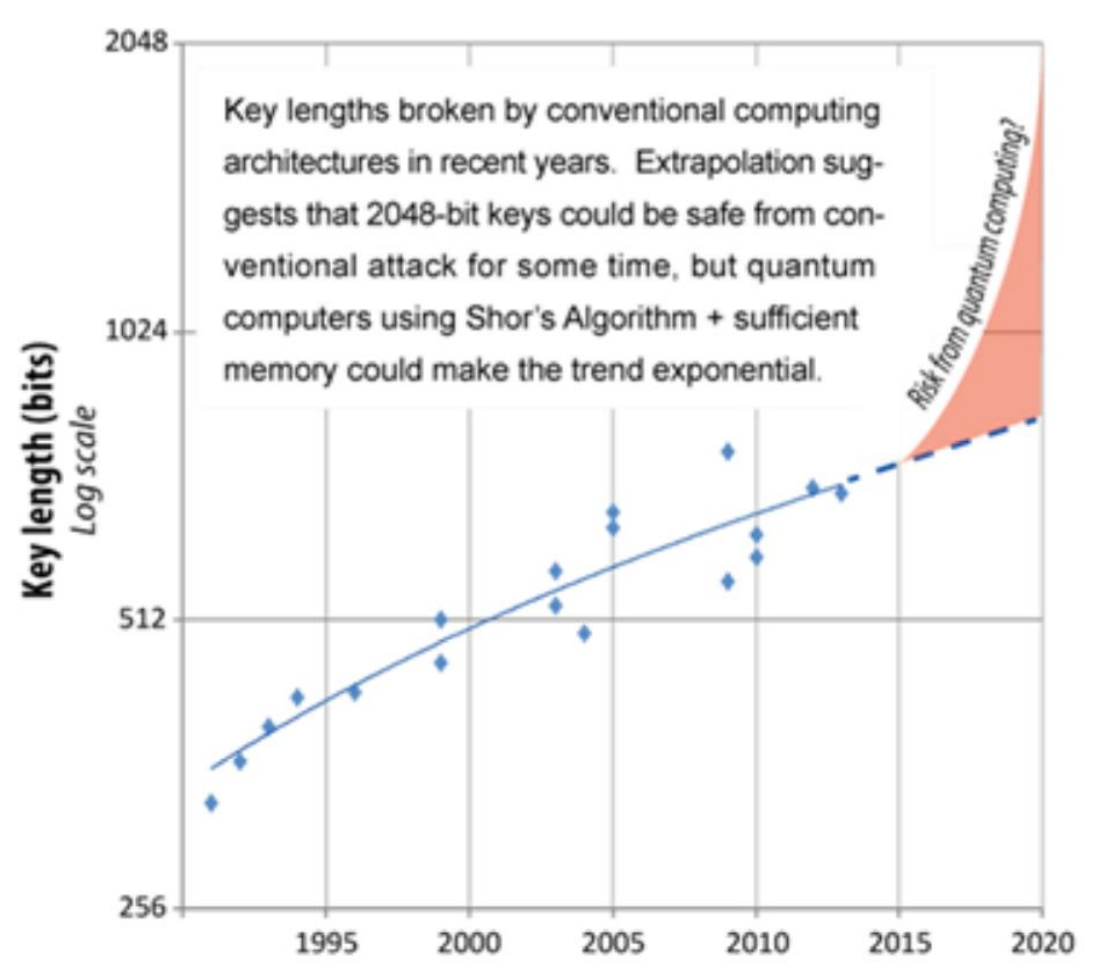
- Unit Commitment Problem
- Multisource simulations

Quantum Computing
Quantum Threat

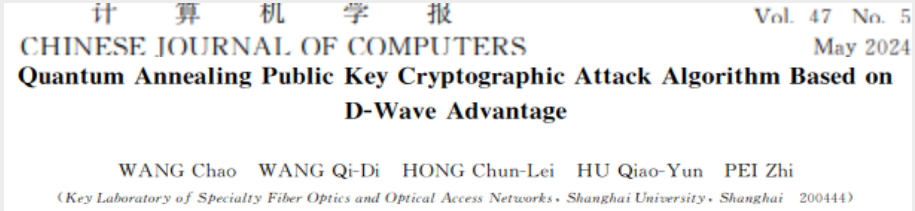
- Quantum algorithms have the potential to break current classical cryptography
- **Grover's Algorithm** (https://arxiv.org/pdf/quant-ph/9605043)
  - Faster search algorithm for unsorted data

- **Shor's Algorithm** (https://arxiv.org/abs/quant-ph/9508027)
  - Can break asymmetric algorithms (RSA, DH, ECC)
  - Solves the underlying hard-problems – factoring large integer numbers, discrete logarithm – exponentially faster than best known classic algorithm

Quantum Threat to Cryptographic Systems



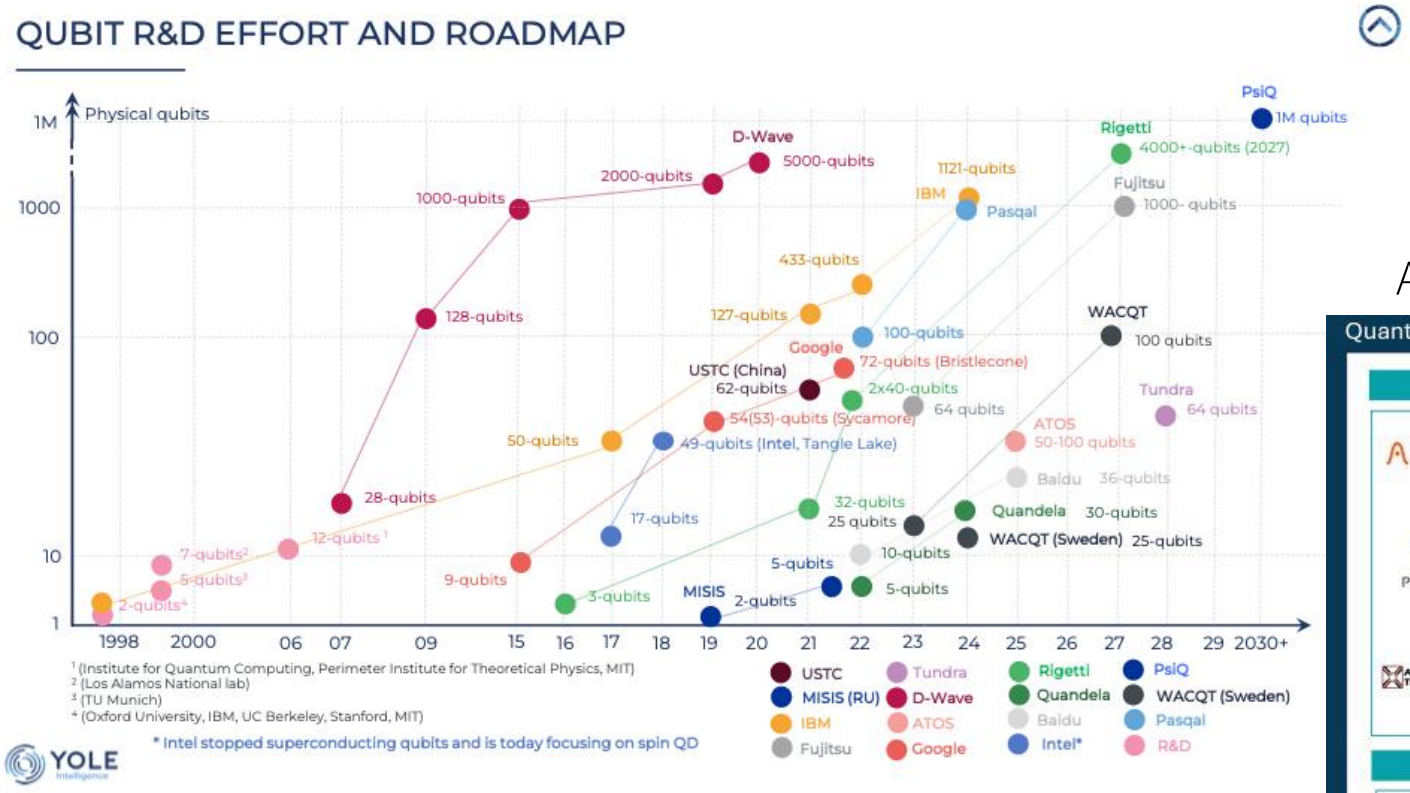
- RSA Encryption based on key size: Current RSA keys are 2048 bits.
- In May 2024, Shanghai University researchers factored a 50-bit integer using D-Wave's Advantage quantum computer.


计 算 机 学 报 Vol. 47 No. 5
CHINESE JOURNAL OF COMPUTERS May 2024
Quantum Annealing Public Key Cryptographic Attack Algorithm Based on D-Wave Advantage
WANG Chao WANG Qi-Di HONG Chun-Lei HU Qiao-Yun PEI Zhi
(Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai 200444)

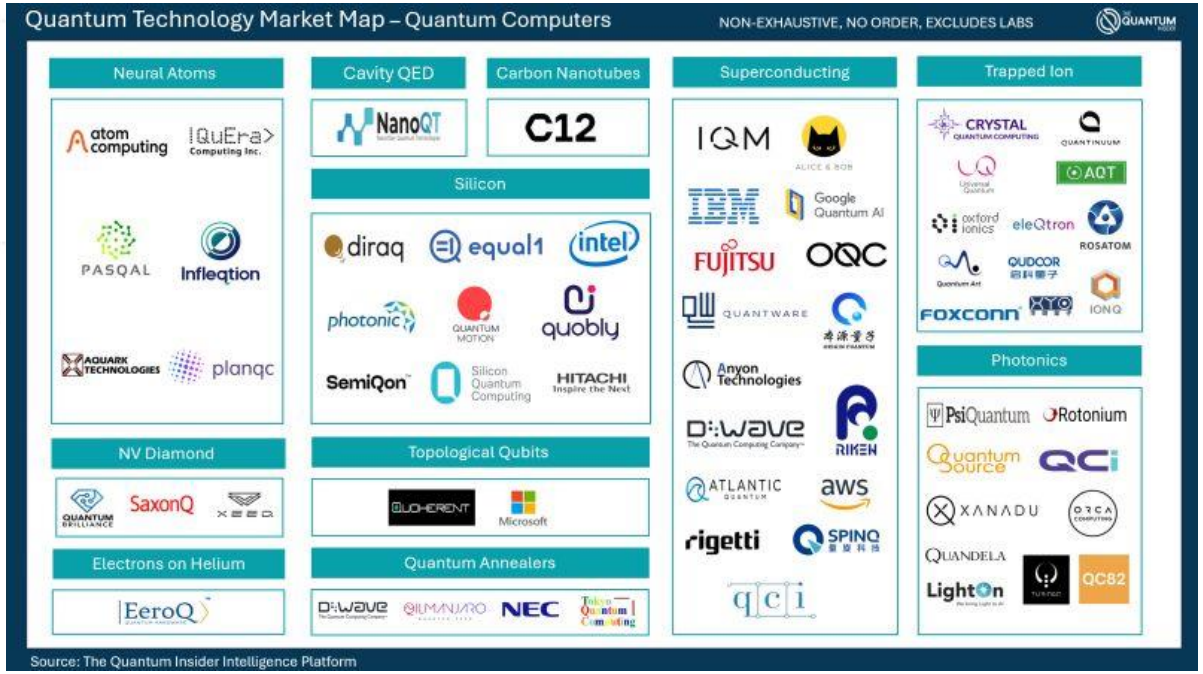
- Currently, 3072 bits are considered safe for RSA
- BUT until when?

"*Quantum Safe Cryptography and Security*", ETSI.

Quantum Computing
Rapid Advancements

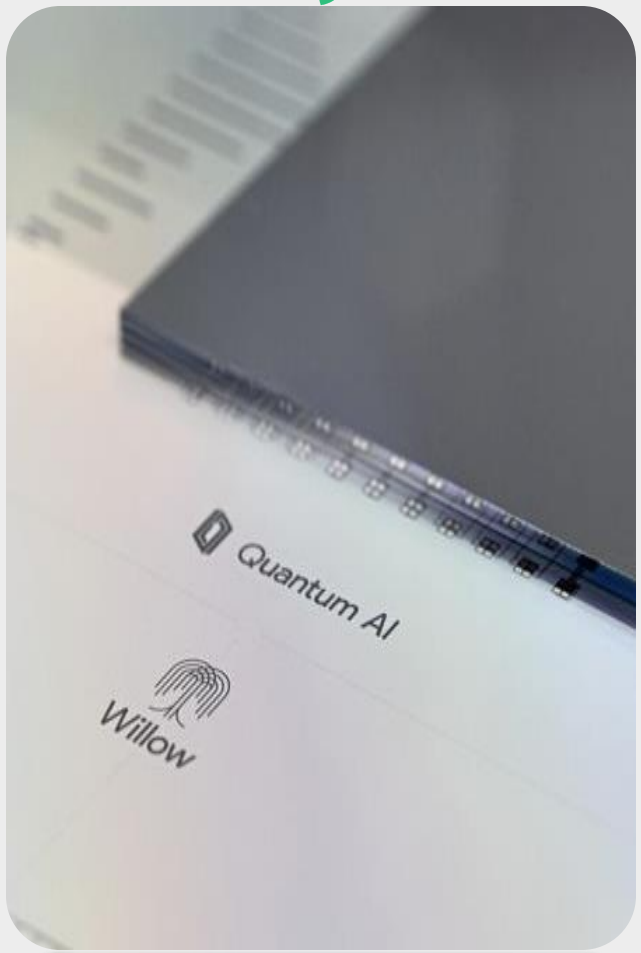


A variety of architectures/hardwares is available



- QPUs with hundreds/thousands of qubits is a reality
- Suppressing errors due to noise/imperfections is a challenge

Quantum Computing Today



Technology

Google breakthrough paves way for large-scale quantum computers

Google has built a quantum computer that makes fewer errors as it is scaled up, and this may pave the way for machines that could solve useful real-world problems for the first time

By Matthew Sparkes

5 September 2024

Quantum Computing Is Developing Faster Than Expected — QuEra Survey

Quantum Computing Business, Research Matt Swayne • August 6, 2024

Microsoft-Led Team Achieves Record For Reliable Logical Qubits In Quantum Computing

Research Matt Swayne • September 10, 2024

FT Financial Times

Scientific breakthrough gives new hope to building quantum computers

One of the biggest remaining technical hurdles in the race to build practical quantum computers has been cleared, according to experts in...

09 December 2024

Possible solutions

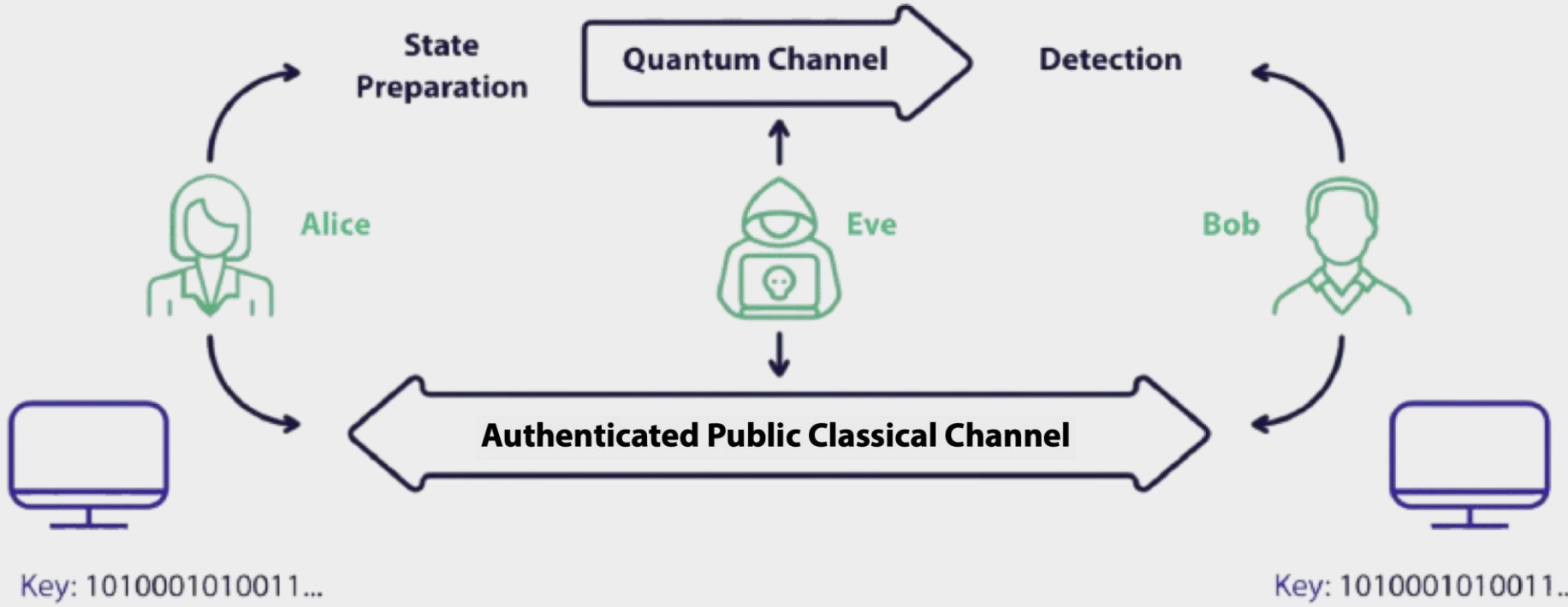
Post-quantum Cryptography

- Security based on the computational complexity of encryption algorithms
- May not be a long-term solution
  - More efficient key-cracking algorithms are coming
  - Evolution of computing power

Quantum Criptography

- Security based on the laws of physics
- Unconditional security
- Requires dedicated hardware
- Field tests around the world
- Commercial solutions
  - Easy integration with existing network infrastructure
  - Range of up to ~350 km demonstrated
  - Mbps (kbps) secret key rate for short (long) distances

Quantum Key Distribution (QKD)



$$\begin{array}{ll} & 0100101110110110 \text{ - Mensagem} \\ \oplus & 1101010110101011 \text{ - Chave} \\ \hline & 1001111000011101 \text{ - Cifra} \end{array}$$

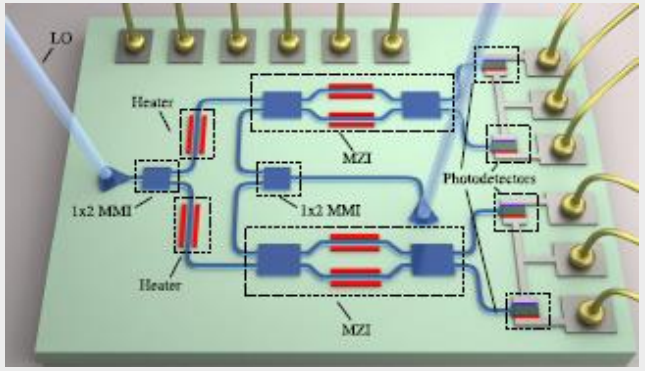
$$\begin{array}{ll} & 1001111000011101 \text{ - Cifra} \\ \oplus & 1101010110101011 \text{ - Chave} \\ \hline & 0100101110110110 \text{ - Mensagem} \end{array}$$

Quantum light: discrete or continuous

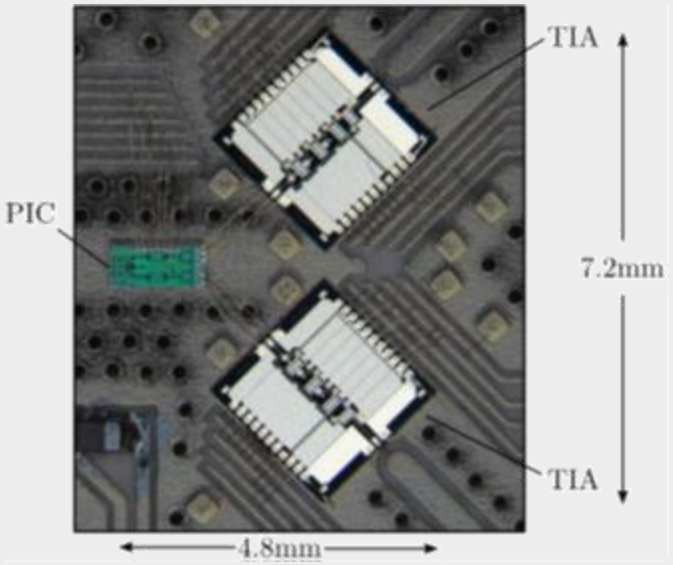
	Discrete variables	Continuous variables
Key coding	• Polarization of single photons • Weakened coherent pulses	Quadrature field modulation
Detection	Single photon	Coherent detection (homodyne/heterodyne)
Pre-processing	-	DSP routines (synchronization, equalization, etc.)
Error correction	Low computational complexity	High computational complexity
Throughput	• 6.5 b/s @ 405km • (b/pulse) @ 1002km (TF)	• 0.7 Gb/s @ 5km • 0.3 Gb/s @ 10km • 25.4 Kb/s @ 100km
Limitations	• Detector temperature • System speed • Sensitive to co-propagation with classic signs	• High computational load (pre/post) • Reach • Security analysis in development

Quantum cryptography
with continuous variables

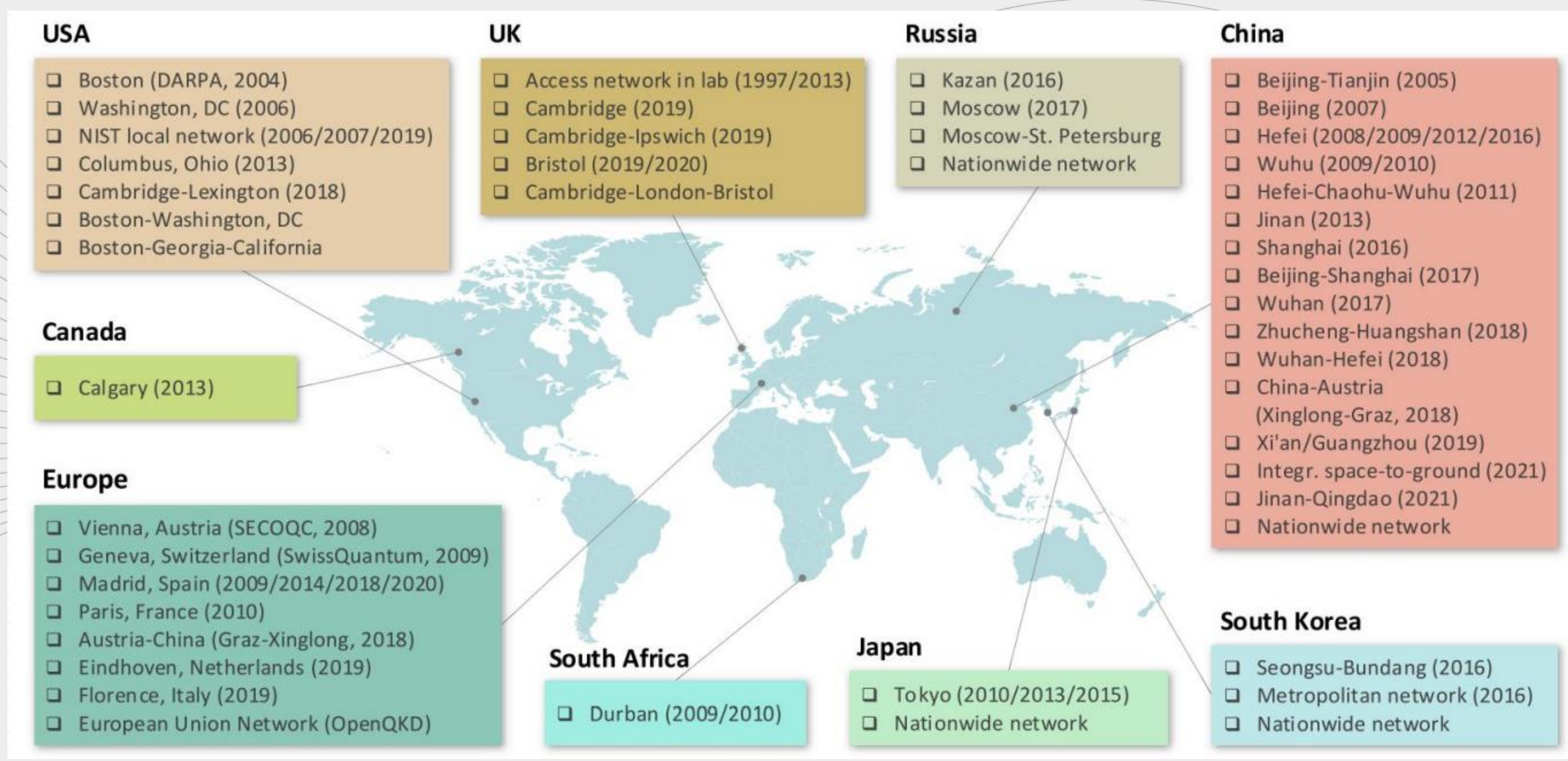
- **Integration with current telecom technologies**
  - **Miniaturization (photonic circuits)**
  - **Increased distance and key generation rate**
- **New, more secure protocols**
  - **Measurement Device Independent**
  - **Twin-field**
  - **Distribution of entanglement**
- **The road to quantum internet**
  - **Quantum Memories**
  - **Quantum Repeaters**



Hajomer et al, Optica 11, 1197-1204 (2024)

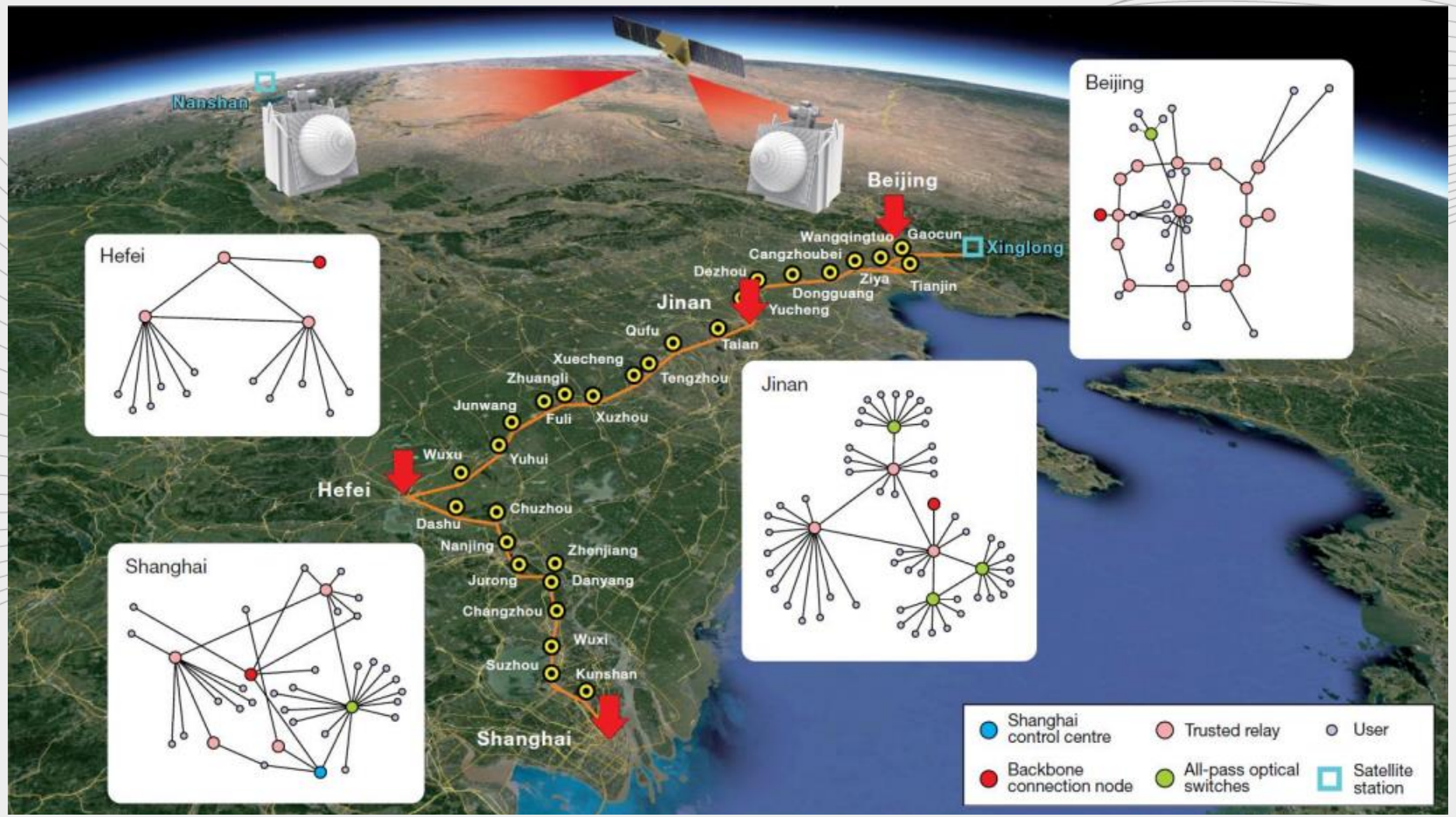


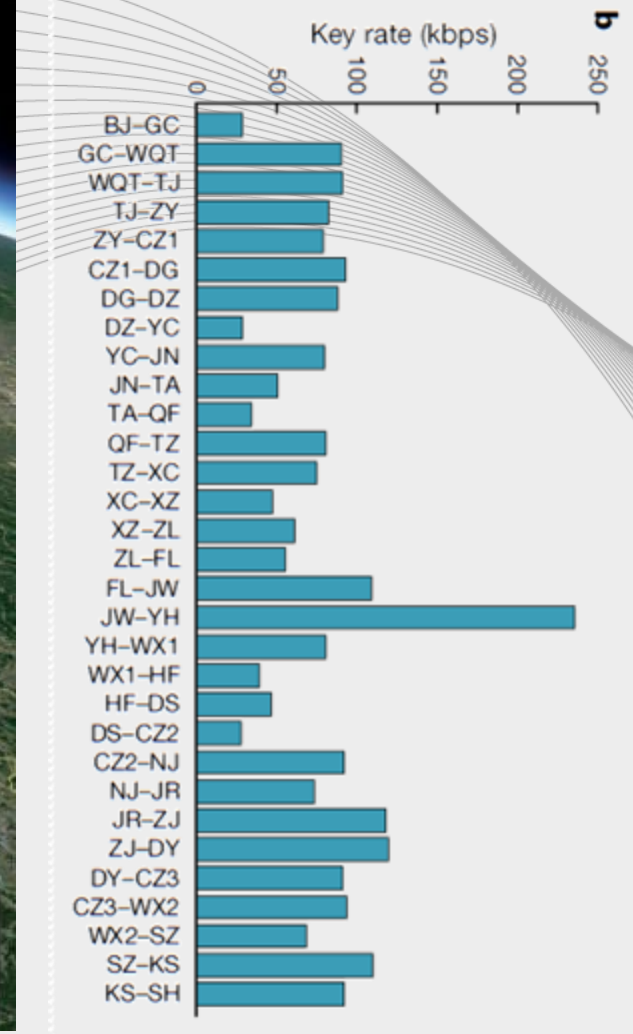
Quantum Networks Worldwide



IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 839-894 (2022)

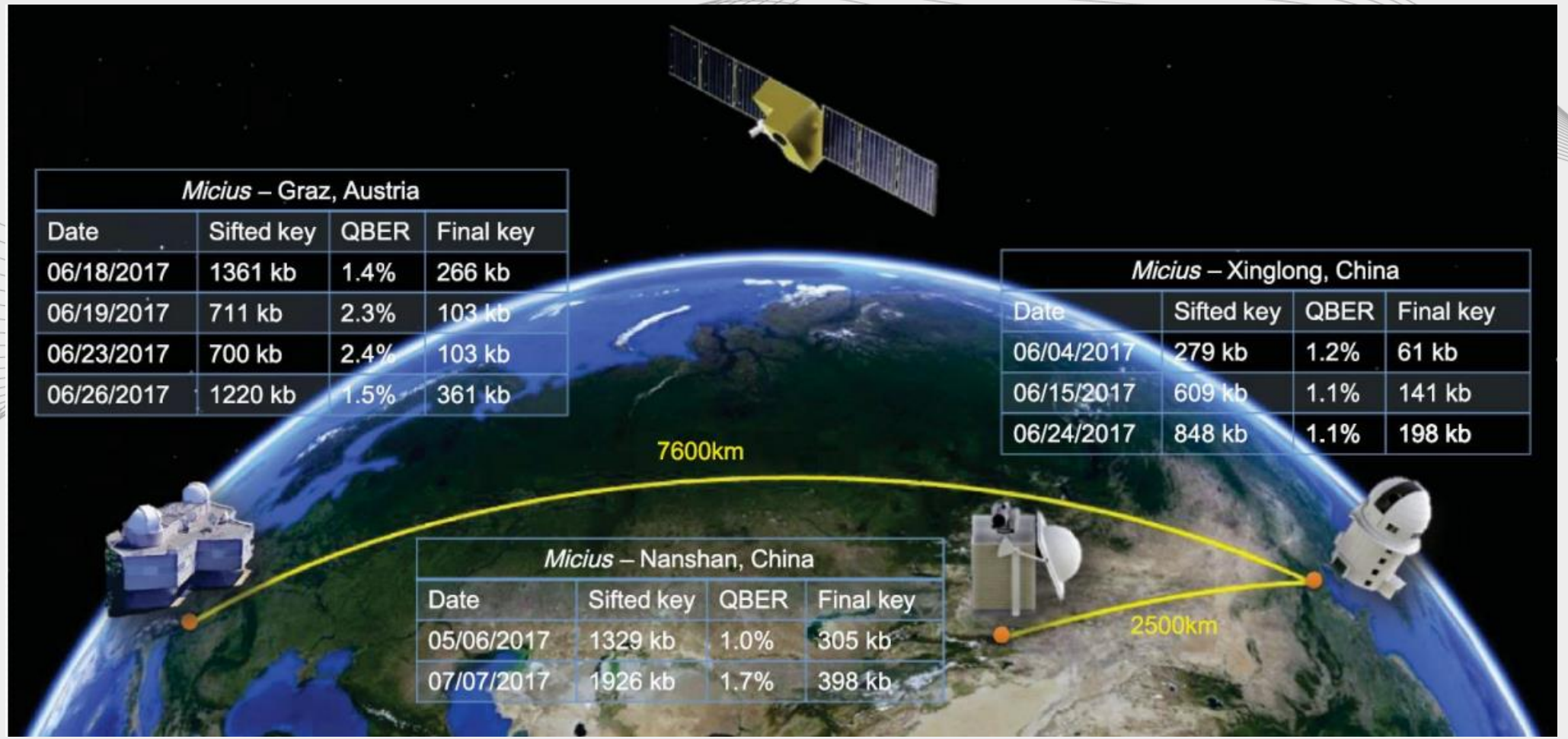
China Quantum Network – Beijing-Shangai





Chen et al., Nature 589, 214 (2021)

Intercontinental link – Austria-China

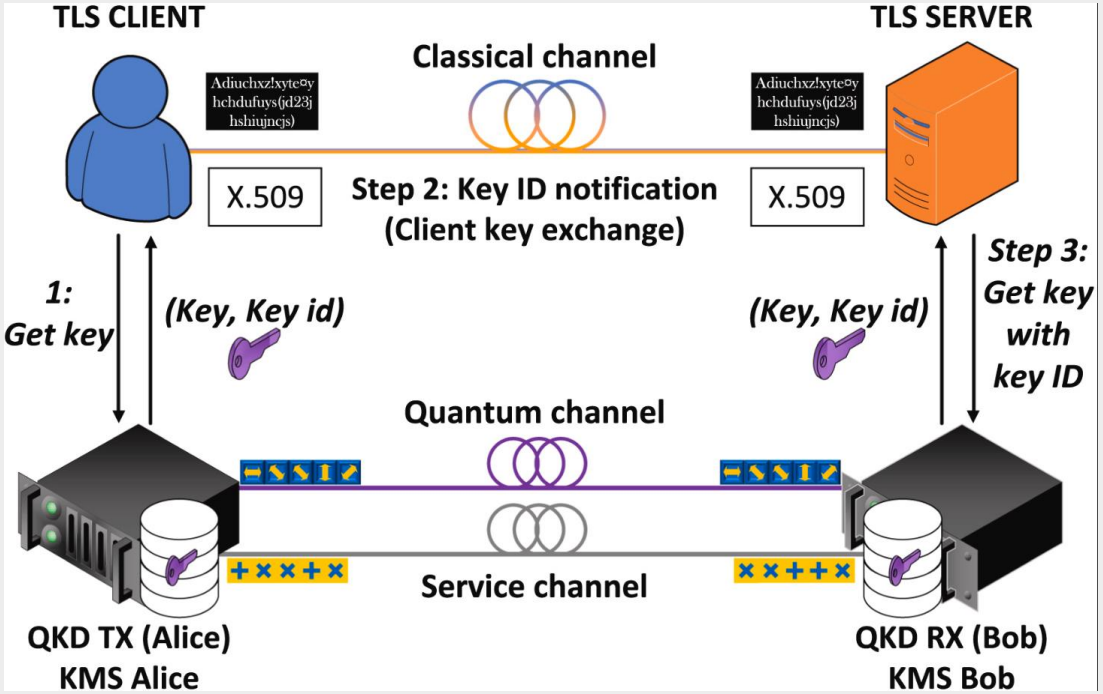


Liao et al., PRL 120(3): 030501 (2018)

QKD Applications

- **Unconditional security of sensitive and confidential information**
- **Integrity of critical infrastructure and sensitive data**

Garcia et. al (2024) https://doi.org/10.1016/j.comcom.2023.11.010



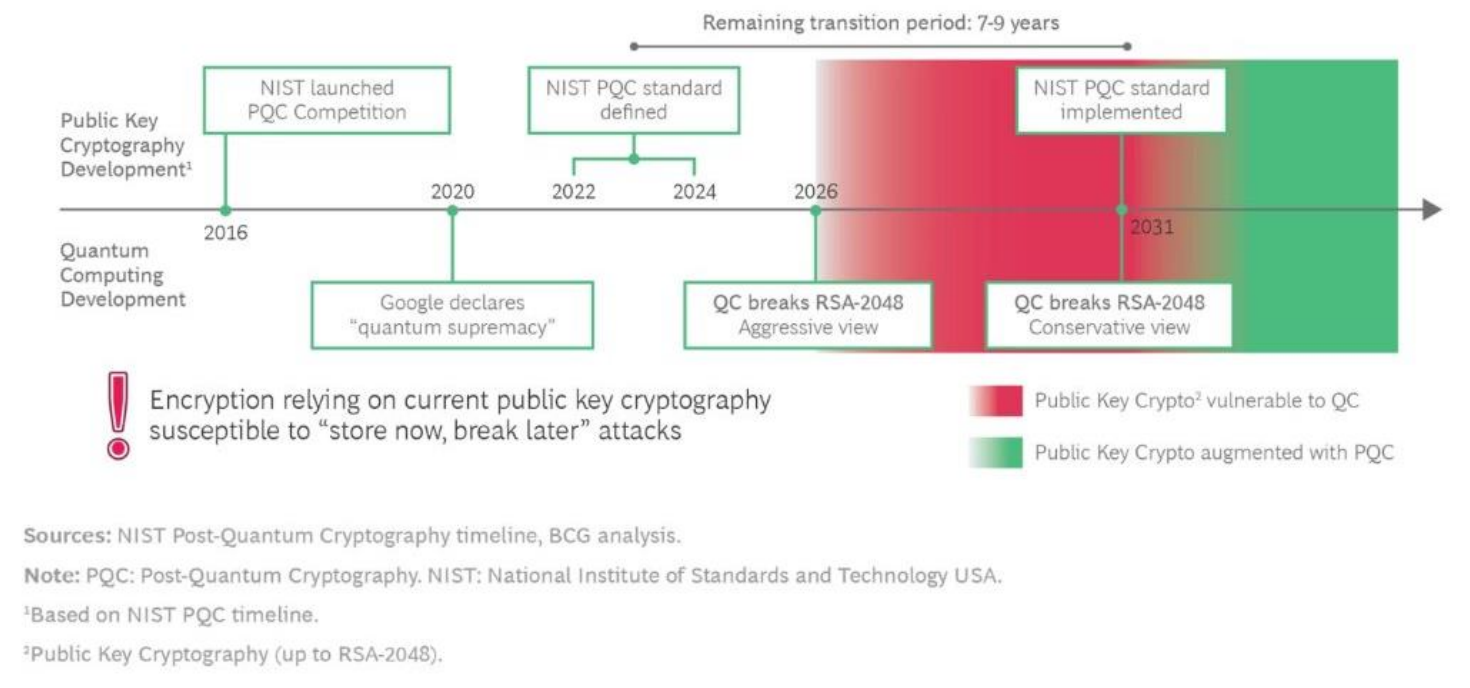
Examples:

- **TLS (transport layer security) - client-server protocol for internet**
- **Communication between remote datacenters**
- **Protecting cloud services**

Quantum Cryptography
When to invest?

y = Tempo de migração	x = Prazo de segurança para a informação
z = Tempo para ameaça quântica	

x + y > z ⇒ problem!!!



M. Mosca (2013), "Setting the Scene for the ETSI Quantum-safe Cryptography Workshop", https://docbox.etsi.org/Workshop/2013/201309_CRYPTO/e-proceedings_Crypto_2013.pdf