Quantum computing and quantum security

Junyu Liu 2024 @ Quantum Greater PGH

Worldline of Junyu Liu

1995
Born

2012-2016
USTC
Bachelor of Science

2016-2021
Caltech
Ph.D in Physics

2021-2024
UChicago-IBM
Postdoc Scholar

2024
University of Pittsburgh
Assistant Professor of CS

Research Interest:

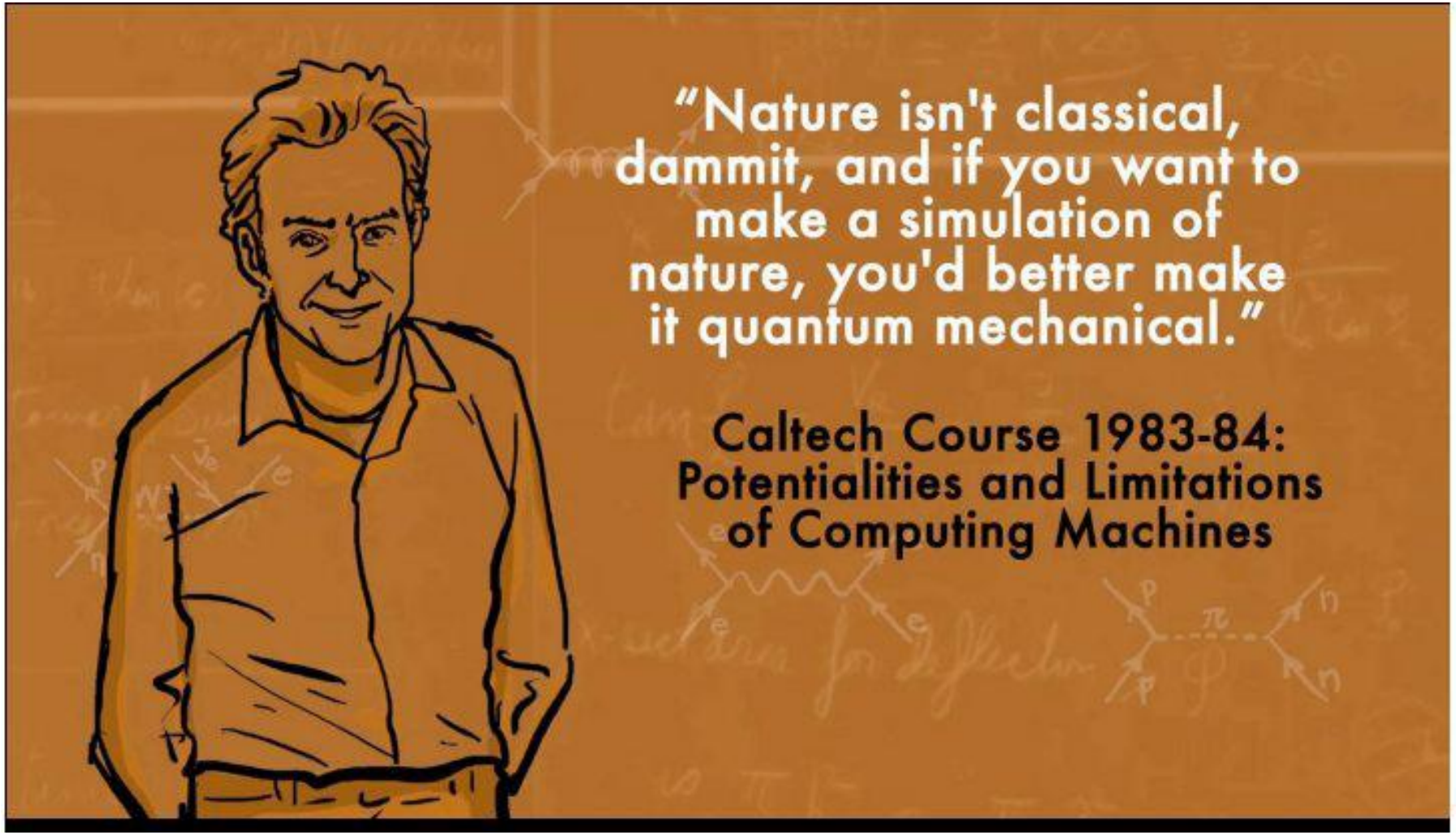
Quantum algorithms + Quantum networks

a. Near-term Quantum Algorithms: Fundamental principles of quantum machine learning algorithms that can run on currently available noisy machines, hardware experiments, and various possible applications (such as in natural sciences, biomedicine, financial technology, and supply chain optimization). Quantum computer systems and architectures.

b. Fault-Tolerant Quantum Algorithms: Fundamental principles of quantum machine learning algorithms that can run on large future devices capable of quantum error correction, software simulation, and their various possible applications, quantum error correction algorithms, and hardware for early fault-tolerant quantum computers.

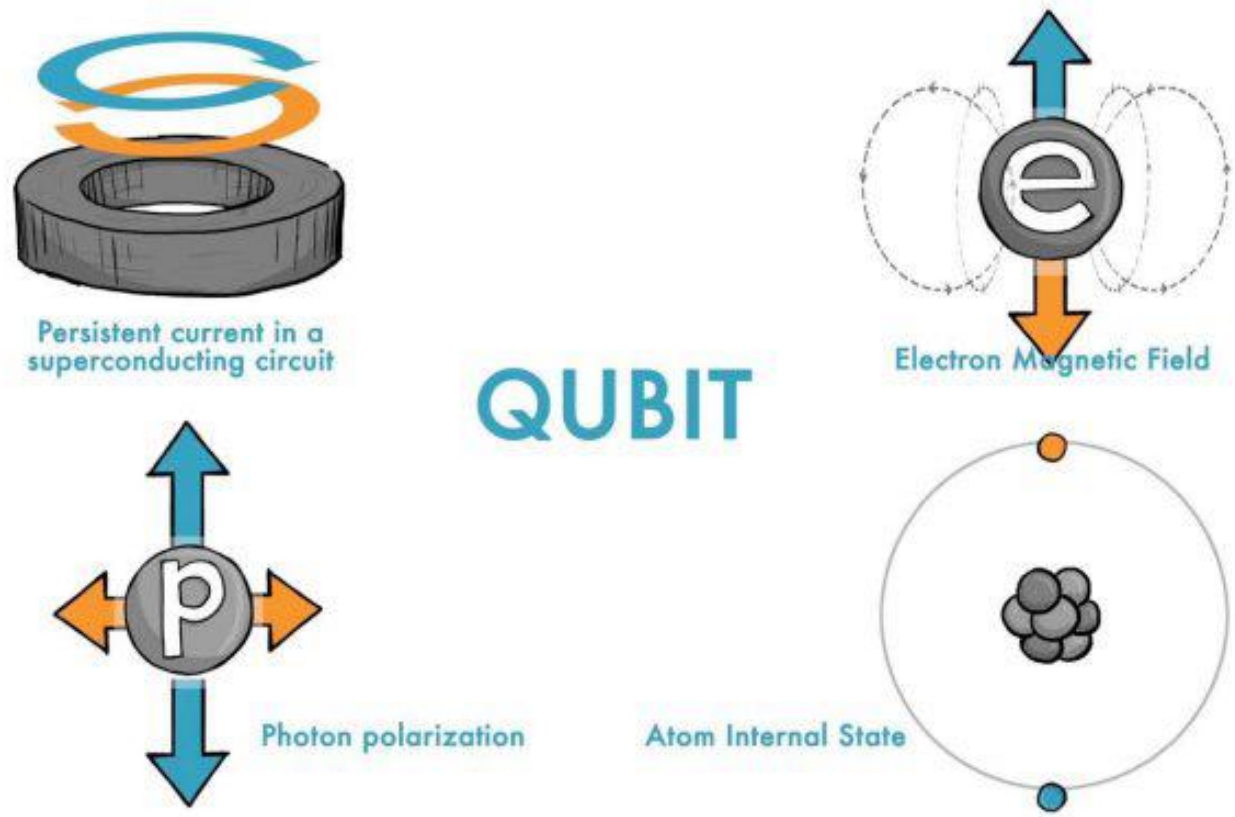
c. Quantum Networks and Quantum Data Centers: Quantum security, quantum cryptography and **post-quantum cryptography**, **quantum network** theory, quantum sensing, and their applications.

Development of quantum computing



Using quantum mechanics itself to do computing!

Development of quantum computing



If the world is a game simulation, then quantum computer is a cheater.

Development of quantum computing

Using quantum mechanics itself to do computing!

1981: Richard Feynman talks about concepts of quantum computers to simulate the quantum world.

1994: Peter Shor discovers so-called Shor's algorithm that could crack RSA and ECC within polynomial time with quantum computers.

1995: Shor discovers so-called Shor's code, showing quantum error correction is possible.

2018: National quantum strategy of US is initiated.

2019: Google announces they achieved quantum supremacy (quantum advantage): solving a specific task beyond the capability of all existing classical computers, although it is not convincing for everyone especially people from IBM.

Development of quantum computing

What a quantum computer **can** do at least:

1. Shor's algorithm cracking most asymmetric cryptographic systems like RSA, ECC (affecting bank accounts, cryptocurrency, ID card numbers, VPN services, website certifications……). It is runnable in a large-scale, fault-tolerant quantum computer which does not exist at this moment based on public information.

2. Performs searching (Grover's algorithm), and sparse, low-conditioned matrix inversion (HHL algorithm) faster than all known classical algorithms, assuming that we have a good enough quantum memory and good enough quantum downloader (tomography) methods for a large-scale, fault-tolerant quantum computer.

3. Simulating quantum chemistry, quantum phenomena in materials/drug and biology, and learning from quantum experiments faster than all known classical methods.

Development of quantum computing

What a quantum computer **might** be able to do (under research):

1. Large-scale machine learning applications (quantum machine learning).

2. Seemingly already observed applications in quantum optimization better than known classical algorithms polynomially with experimental demonstration (Harvard and Quera 2022, Science)

3. Other applications: solving some non-linear ODEs faster than known classical methods.

Development of quantum computing

Where are we now? Maybe around the end of so-called NISQ era.

Development of quantum computing

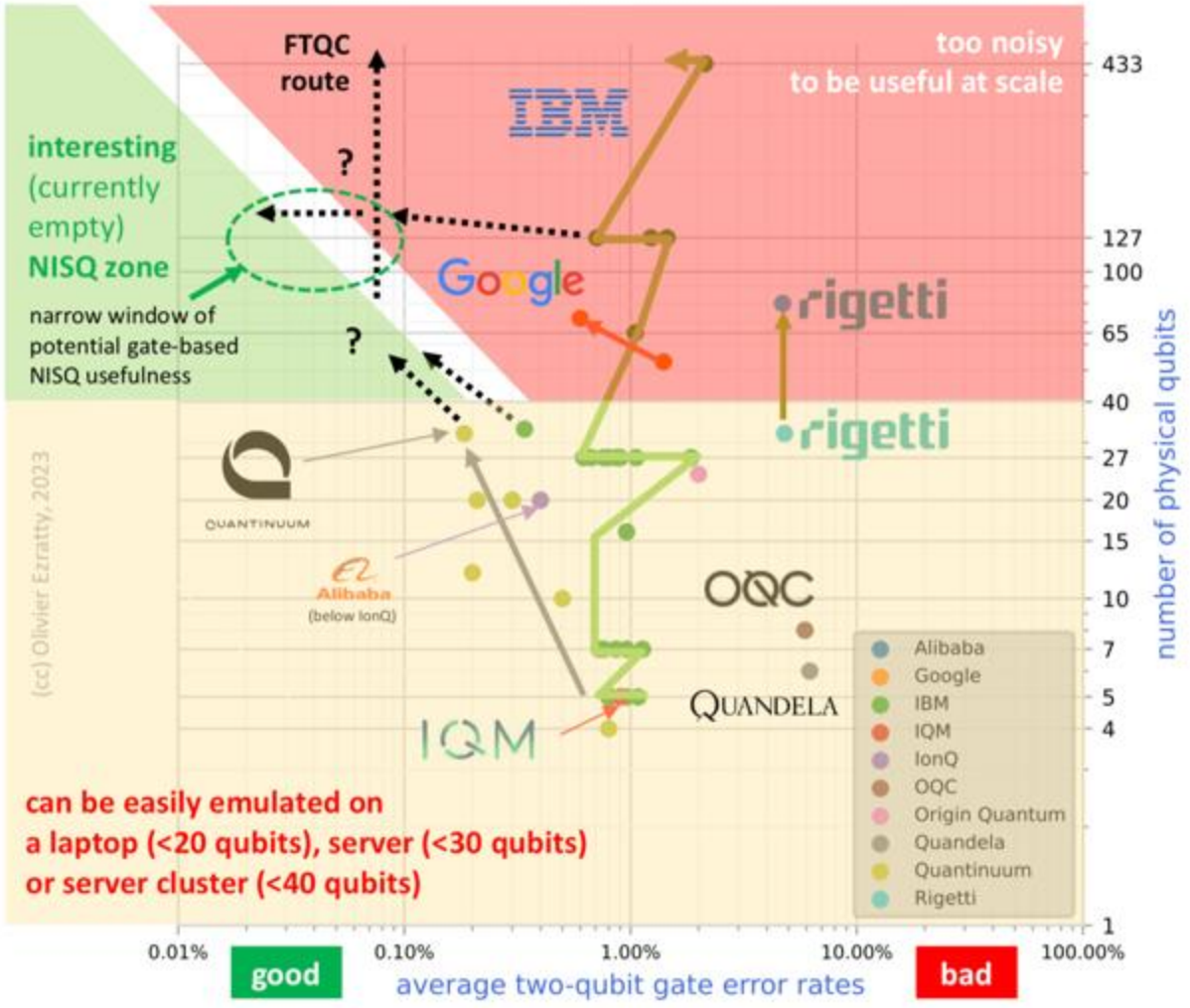


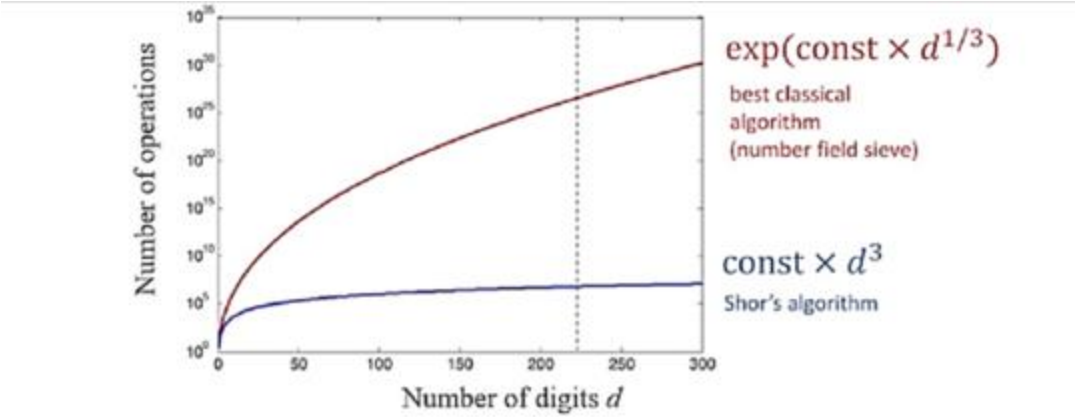
Figure from Olivier Ezratty, 2023

Currently we are around the so-called NISQ (noisy intermediate-scale quantum) era, where we are able to control 100-1000 qubits, But there are significant limitations from quantum noises.

One of the goals of quantum computing community at the moment is to improve the precision by reducing the error and implementing quantum error correction codes.

Error correction could suppress the error exponentially, with only polynomially more overheads. Eventually, we could arrive at the FTQC (fault-tolerant quantum computing) era

Post-quantum cryptography: its coming!



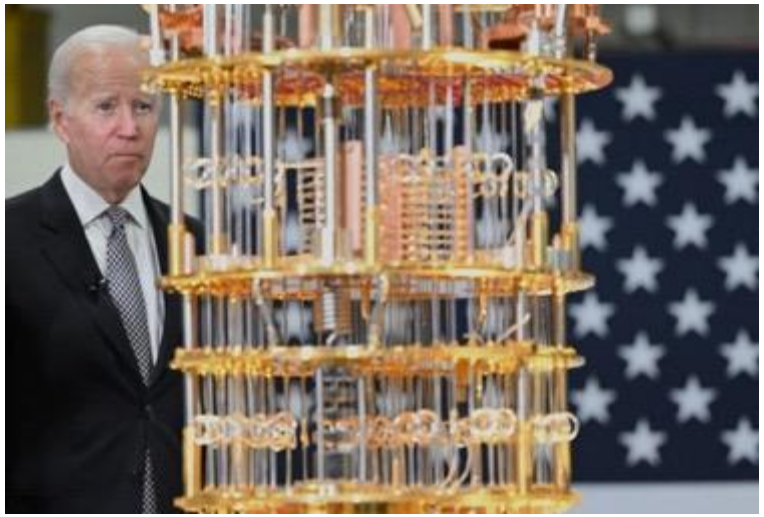
In 1994, Peter Shor (now MIT) invented an algorithm that could factor large numbers in polynomial time, challenging the foundation of RSA asymmetric key distribution and digital signatures. (ECC as well)

Post-quantum cryptography: its coming!

1. Post-quantum cryptography: classical algorithms that are different from RSA and ECC, which should be hard even for quantum computers.

2. Quantum cryptography: algorithms like quantum key distribution and quantum digital signature that are secured by laws of quantum mechanism instead of complexity theory (unconditionally secure).

Post-quantum cryptography: its coming!



National Regulations:

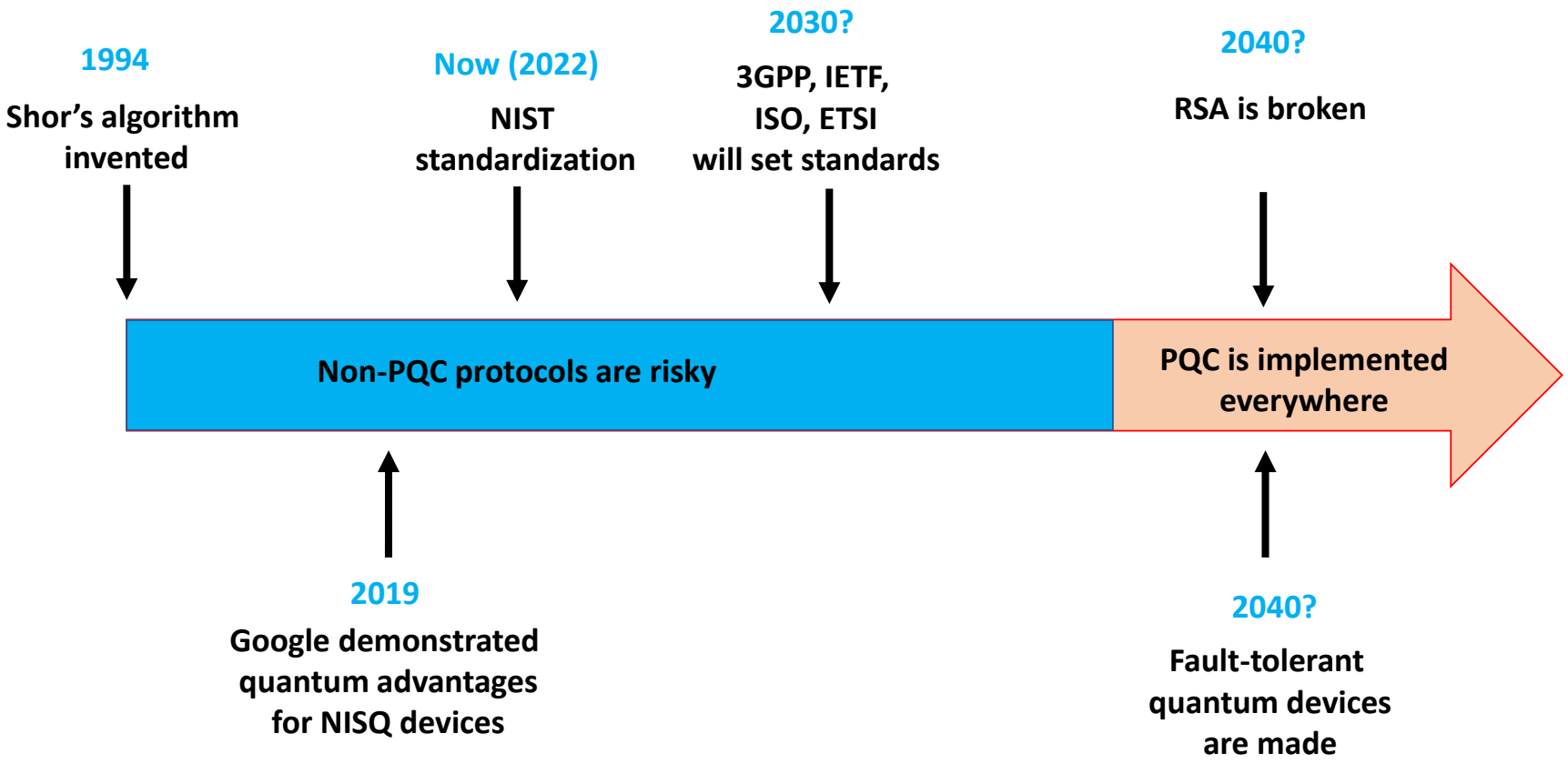
Quantum Computing Cybersecurity Preparedness Act (2022)

NSM-10 (2022)

M-23-02 (2022)

NIST FIPS 203, 204, 205 (2024)!

Post-quantum cryptography: its coming!



Post-quantum cryptography: its coming!

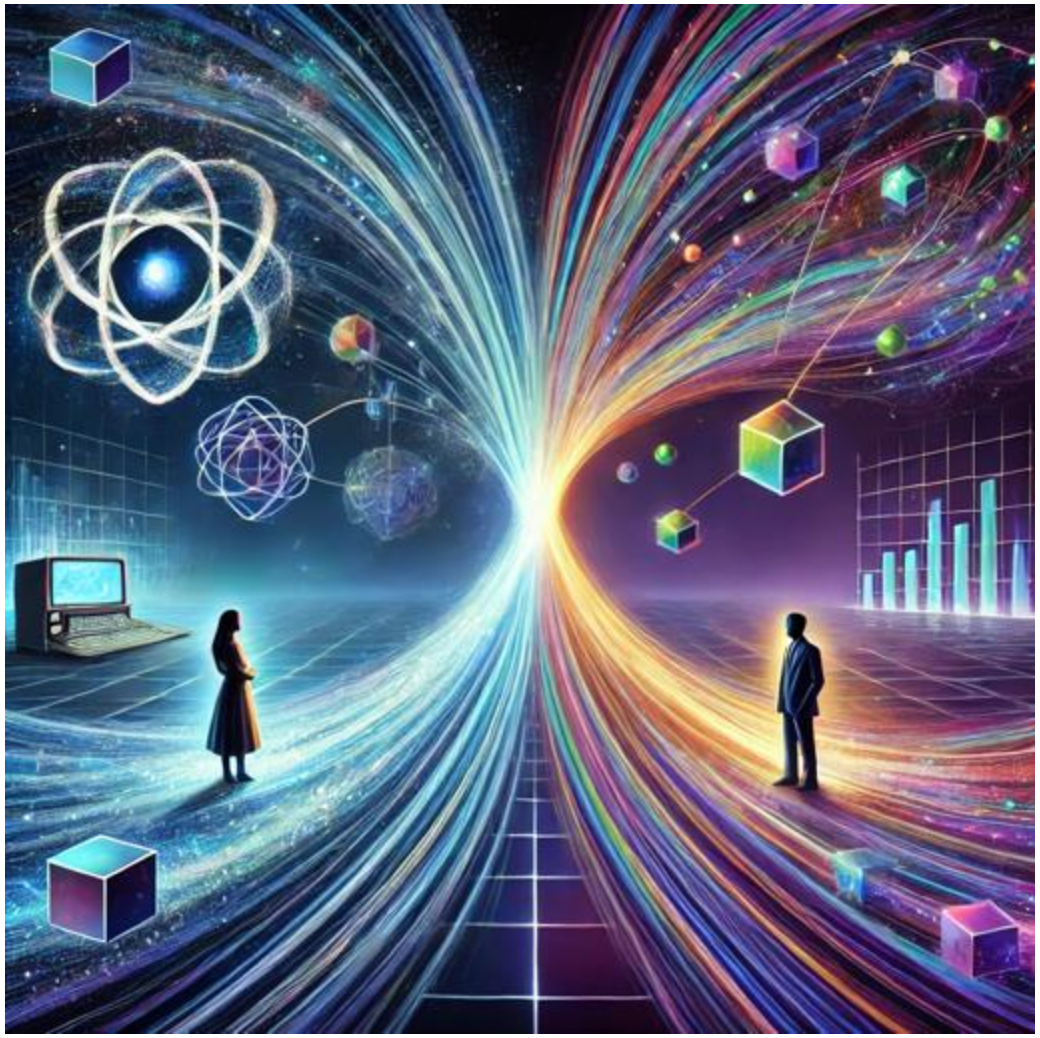
Feature	Lattice-Based	Code-Based	Multivariate	Hash-Based
Security	Strong resistance to quantum attacks, based on lattice problems	Strong resistance, based on code decoding problems	Moderate to strong, depending on scheme	Strong resistance, based on hash function properties
Efficiency	Generally efficient in key generation and signing (medium computational cost)	Efficient in encryption/decryption, slower in key generation	Fast for small field sizes, slow for verification	Efficient for short signatures; less efficient for large signatures
Maturity and Trust	High, well-studied and actively researched	High, very mature (e.g., McEliece since 1970s)	Moderate, less mature than others	High, very mature and well-understood
Key Size	Medium to Large (1 KB to 10 KB)	Very Large (tens to hundreds of KB)	Small to Medium (usually under 1 KB)	Small to Medium (varies, but generally small)

Post-quantum cryptography: its coming!

Post-quantum cryptography: its coming!

www.infrax.ltd
Delaware, 2022-now
Contact: junyuliucaltech@gmail.com

Quantum networks



BB84: quantum key distribution protocol (1984) by Charles H. Bennett and Gilles Brassard.

Unconditionally secure due to quantum mechanics!

Quantum networks

China’s quantum satellite, 2016

Quantum networks

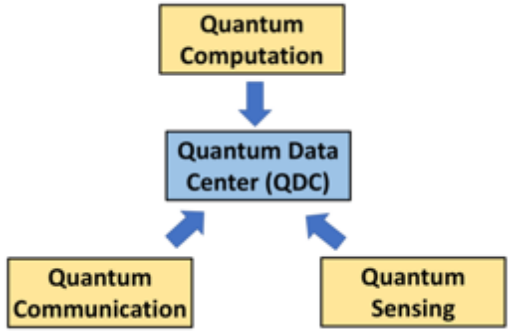
PHYSICAL REVIEW A

covering atomic, molecular, and optical physics and quantum science

Highlights Letters Recent Accepted Collections Authors Referees Search Press Abou

Data centers with quantum random access memory and quantum networks

Junyu Liu, Connor T. Hann, and Liang Jiang
Phys. Rev. A **108**, 032610 – Published 20 September 2023

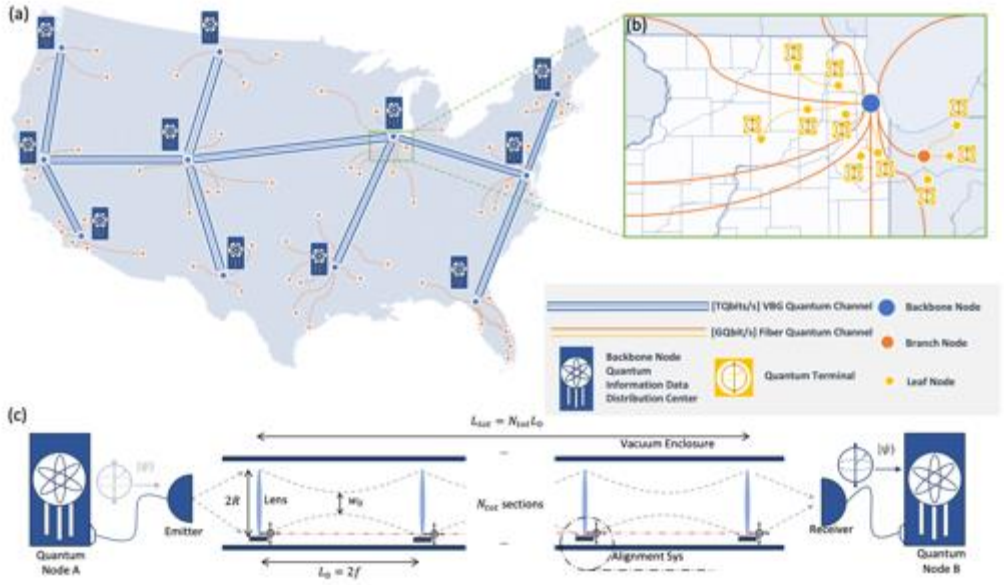


Journals & Magazines > IEEE Network > Volume: 38 Issue: 5

Quantum Data Center: Perspectives

Publisher: IEEE Cite This PDF

Junyu Liu ; Liang Jiang **All Authors**



PHYSICAL REVIEW LETTERS

Highlights Recent Accepted Collections Authors Referees Search Press About Editorial Team

Vacuum Beam Guide for Large Scale Quantum Networks

Yuexun Huang, Francisco Salces-Carcoba, Rana X. Adhikari, Amir H. Safavi-Naeini, and Liang Jiang
Phys. Rev. Lett. **133**, 020801 – Published 9 July 2024

Article References No Citing Articles Supplemental Material PDF HTML Export Citation

Here @ Pitt SCI

Xulong Tang
Computer Science
Quantum architectures
Quantum systems
Quantum computing

Youtao Zhang
Computer Science
Quantum architectures
Quantum systems
Quantum computing

Kaushik Seshadreesan
Information Science
Quantum networks
Quantum sensing
Quantum security

Junyu Liu
Computer Science
Quantum algorithms
Post-quantum crypto
Quantum systems

Other fantastic quantum scientists from:
Pitt Physics, ECE, MSEE, Statistics, Business, Chemistry, Medicine, Bioengineering……

<P|Q|I> PITTSBURGH QUANTUM INSTITUTE

Thanks for your attendance!