Prepare for the the next disrupting technology: quantum computing

Brian Andersen, HPE Country CTO Denmark

April 30, 2026

Hewlett Packard Enterprise

Solution: HPC/supercomputing, AI, data

Industry: Biotechnology

Country: Australia

OAK RIDGE National Laboratory

Quantum simulations break new ground in drug discovery

"It would've been technically impossible to simulate vast numbers of electrons because of the computational cost. Frontier and the EXESS algorithm let us model millions of electrons with quantum-level precision."

– **Giuseppe Barca**, Associate Professor, Faculty of Engineering and Information Technology, University of Melbourne, and Cofounder and Head of Research, QDX

Predicting molecular interactions with quantum accuracy was once out of reach, limiting how fast scientists could push boundaries in drug design and other fields. Now, researchers from QDX, the University of Melbourne, and the Australian National University are running simulations 1000x larger and faster than before, using supercomputing at Oak Ridge National Laboratory. Their Gordon Bell Prize–winning breakthrough enables scientists to model complex biosystems with unprecedented precision, accelerating drug discovery, enzyme-based sustainability solutions, and more.

Explore digital game changers

a50013238ENW

How can you, or can you get your arms around quantum?

University of Aarhus 1983
Computer Science and Physics

Deep understanding does not really matter!
Focus on using it?

Heisenberg and Schrödinger get pulled over for speeding

Quantum computing 101

Superpowers and Basic terms

Qubit

The basis of quantum computers, qubits take the values of 0 and 1 at the same time. A qubit can hold both bit states simultaneously but collapses to either 1 OR 0 when you measure it. Therefore, you can't watch a quantum computer at work.

Superposition

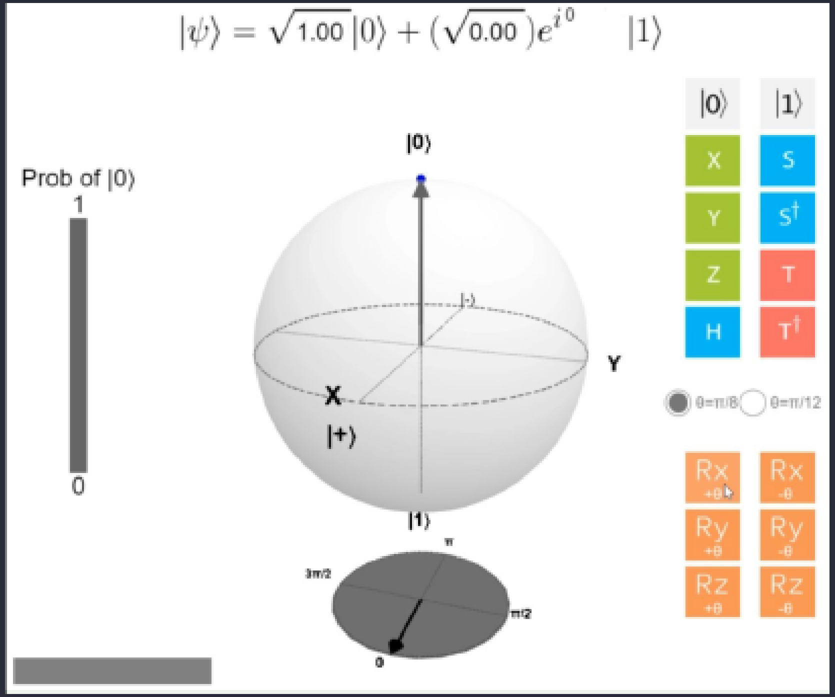
The ability for a qubit to simultaneously be in multiple states enables an infinite number of possibilities and access to tremendous potential.

Entanglement

The aspects of one qubit depend on aspects of another qubit, regardless of how far apart they are, or what lies between them.

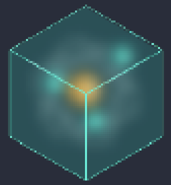
Interference

When a particle is in a superposition of multiple states, these states can interfere with each other.



Noise

Entangled qubits are linked with each other. This helps the qubits work together to search the Hilbert space for a solution. Noise in a system will break the link between qubits, making it difficult, slower or even impossible to get an answer.



Quantum advantage

Occurs when a quantum computer solves a problem you care about faster than a classical computer, for example in problems like drug discovery, new materials for electronic components, etc.

Qubit Types – Enterprise, AI & Deployment Perspective

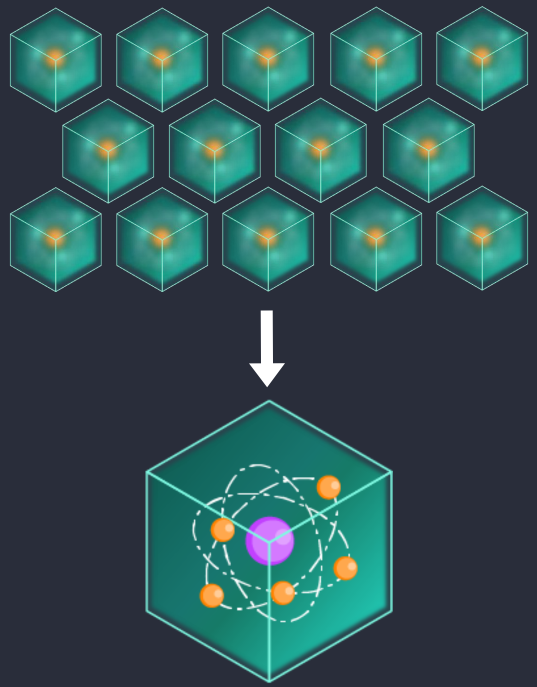
Qubit Type	Cooling Requirements	Maturity	Cloud vs On-Prem Feasibility	Enterprise / AI Relevance
Superconducting qubits	Extreme cryogenics (≈ 10–20 mK, dilution refrigerator)	High	Cloud-only (today)	Best suited for early hybrid AI + quantum experiments and optimization workloads
Trapped-ion qubits	Laser cooling near absolute zero (no dilution fridge)	Medium–High	Cloud-only (today)	High-precision workloads: chemistry, materials science, finance
Photonic qubits	Mostly room temperature (detectors may need cooling)	Medium	Cloud first → possible future on-prem	Quantum networking, secure AI pipelines, distributed quantum
Spin / quantum-dot qubits	Cryogenic (< 1 K)	Medium	Future on-prem potential	Long-term path toward quantum accelerators alongside CPUs/GPUs
Topological qubits	Cryogenic, but fewer error-correction overheads (in theory)	Low (emerging)	Strategic future on-prem candidate	Fault-tolerant systems suitable for mission-critical enterprise use
NV-center (diamond) qubits	Room temperature to modest cooling	Low–Medium	Specialized on-prem	Sensing, security, niche AI use cases
NMR qubits	Room temperature	Low	Not relevant	Research/education only

The challenges of building a useful quantum computer

Noise

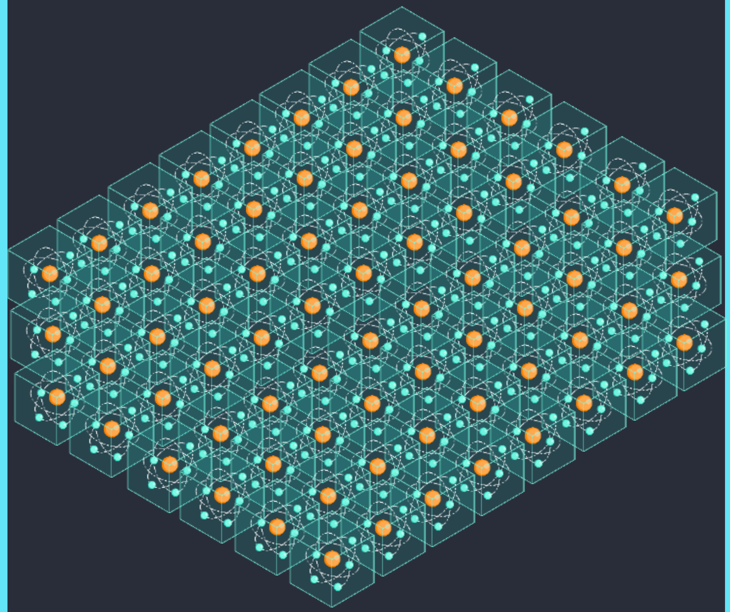
Physical qubit

Error correction



Logical qubit

Scaling



Utility-scale quantum computer

Criteria for a good candidate for quantum utility

1. Small amount of data in
2. Quantum algorithm that can evolve unsupervised with exponential speedup
3. Small amount of data out

Potential applications of quantum computing

Quantum data

Simulating quantum systems

Quantum chemistry

Machine learning on quantum data

Materials design

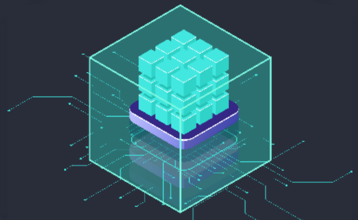
Drug discovery

Fundamental physics

Classical data

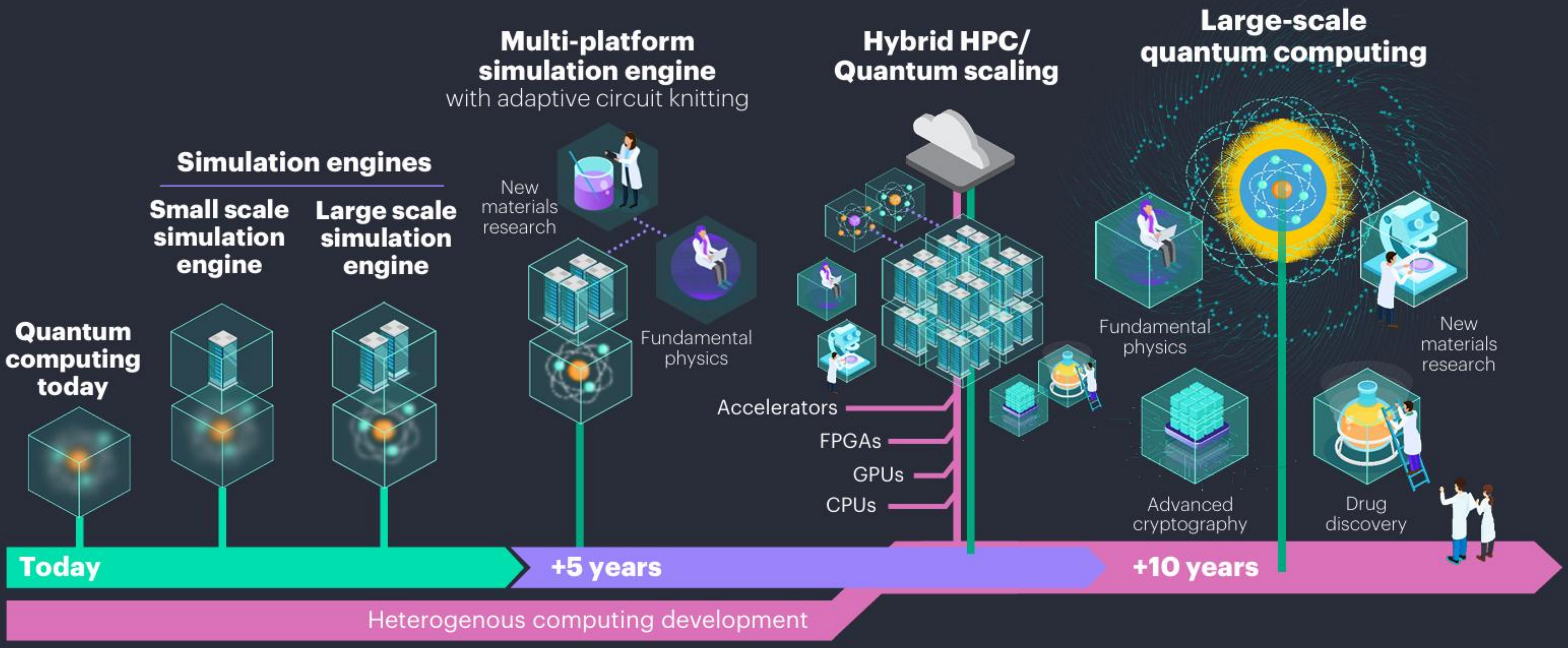
Breaking encryption

RSA encryption relies on the difficulty of factorizing large integers.



Shor's algorithm can factor integers in polynomial time on a quantum computer.

The journey to Quantum Computing



Holistic co-design from the tops down

Applications

Hybrid quantum/classical compilers, distributed workload hypervisor, adaptive circuit knitting

Exascale Infrastructure: GPU, CPU, Fabric

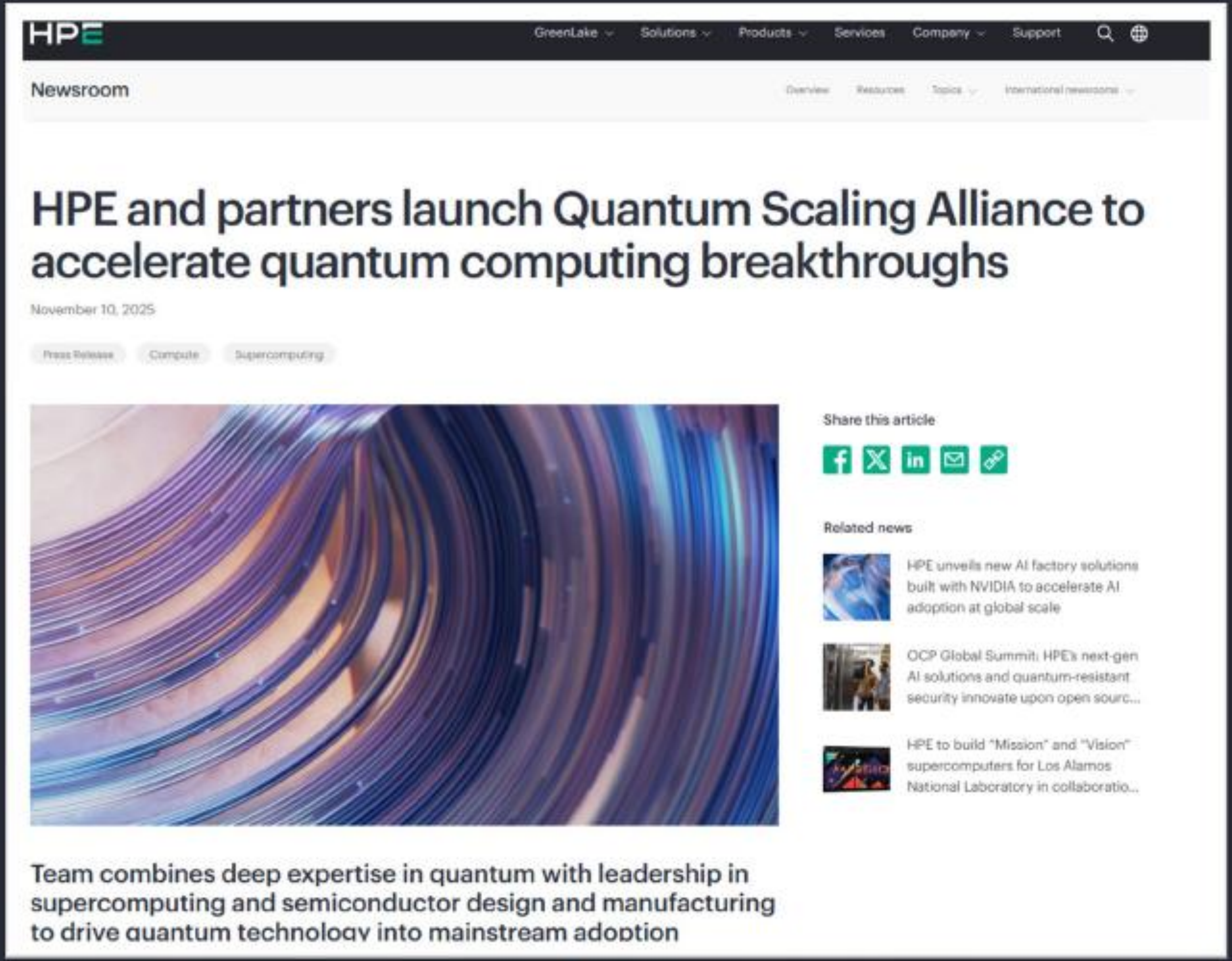
FTQC compilers, distributed error correction, high-performance control and calibration

Quantum Modality Independent Control Processor ASIC

Semiconductor process, fabrication, and tools

Multi-physics design and simulation: Wafer scale, DC to RF

Quantum Scaling Alliance



- **1QBit**: Fault-tolerant quantum error correction design and simulation, algorithm compilation, and automated resource estimations
- **Applied Materials, Inc.**: Materials engineering and semiconductor fabrication
- **HPE**: Full-stack quantum-HPC integration and software developments
- **Qolab**: Qubit and circuit design
- **Quantum Machines**: Hybrid quantum-classical control for scalable quantum computing
- **Riverlane**: Quantum error correction
- **Synopsys**: Simulation and analysis technology, EDA tools, and semiconductor IP
- **University of Wisconsin**: Algorithms, benchmarks

Unlocking Quantum Computing at scale

NETWORKING

+

HPC

+

QUANTUM DEV ENVIRONMENT

HPE Labs

Learn More

Quantum Scaling Alliance

How to Build a Quantum Supercomputer

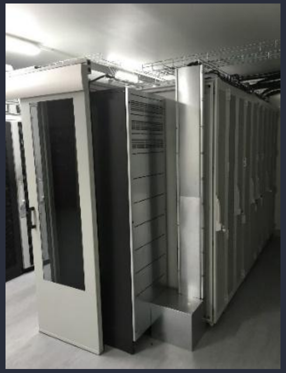
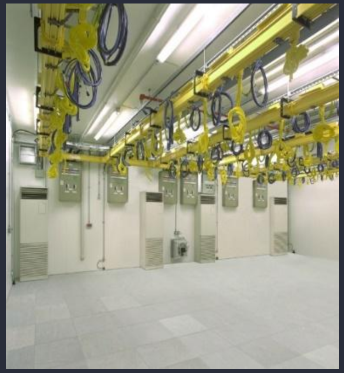
HPE modular data center product family

Secure edge, room (indoor), or site (outdoor)

Secure edge

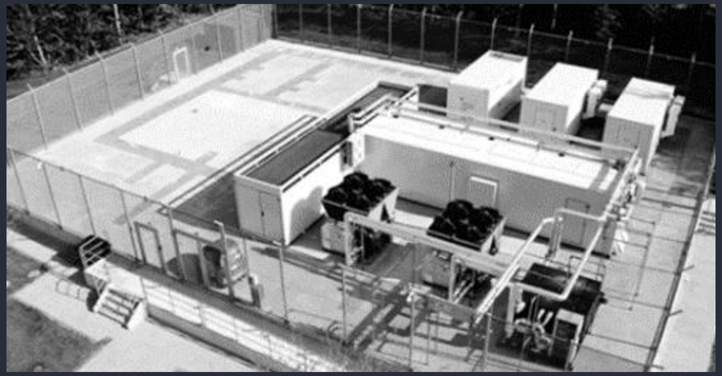

- Capacity of 5 or 10 kW (redundant or not)
- Facilities/IT-integrated, single- or dual-rack solution
- Indoor installation IP 55

Room (indoor)

- Indoor room-in-room IT integrated multi-rack solution, expandable in multiples of 4 racks,
  for example
- Full DC solution (including power distribution, switchgear, fire extinguishing system, etc.)
- Optional: generator (and transformer)

Site (outdoor)



- Outdoor, IT-integrated multi-rack solution expandable in multiples of 4, 5, 8, 10, 21 or 44 racks (standardized catalog configuration)
- Pre-engineered and swiftly deployed
- Including facilities: power modules (UPS, batteries, gears, generators, transformers), Cooling modules (chillers, pumpskids, dry/hybrid coolers, etc.)

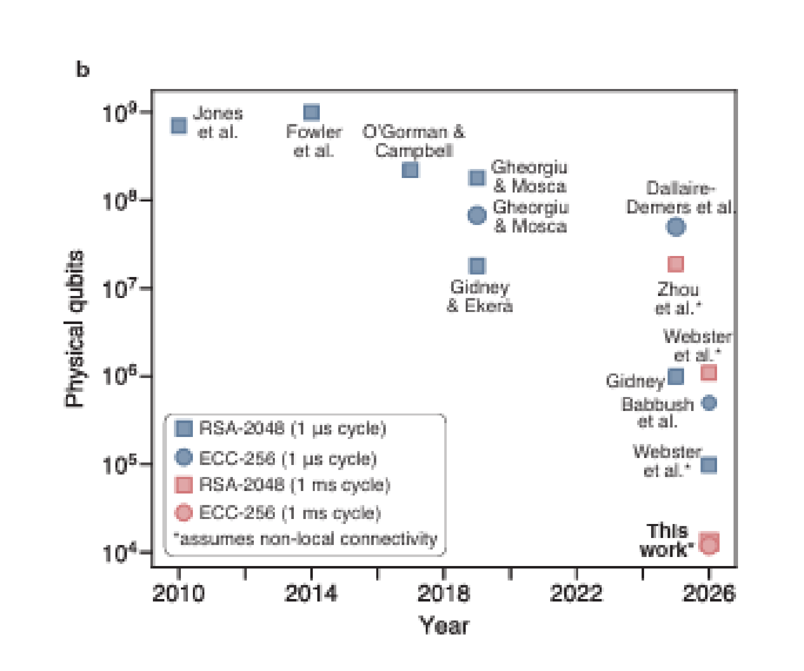
Quantum algorithms exist which break the cryptographic algorithms on which we depend

Shor’s Algorithm

- Shor's algorithm is a **quantum algorithm** developed by Peter Shor in 1994 that factors large integers exponentially faster than the best-known classical algorithms. By utilizing quantum superposition and the Quantum Fourier Transform (QFT) to find the period of a function, it can break widely used RSA public-key cryptography.
- To factor a large n-bit integer using Shor's algorithm, approximately 2n to 4n logical qubits are required, though error correction brings the total physical qubit count to thousands or millions. Recent studies suggest optimized approaches may require around 10,000 to 350,000 physical qubits to break cryptographically relevant RSA-2048 keys.
- Key Takeaways
  — Small Integers (e.g., 15): Can be factored with 7 or fewer qubits (demonstrated in 2001).
  — Cryptographical Relevance (e.g., RSA-2048): While early estimates were in the millions, improved algorithms and error correction suggest 10,000 to 14,000 physical qubits could work, though standard consensus for robust factoring is higher.
  — Logical vs. Physical Qubits: The algorithm needs roughly 2n high-quality logical qubits, but because of noise, each logical qubit requires hundreds or thousands of physical qubits for error correction.

Steps of the Algorithm:

1. **Select a random integer a:** Pick $a < N$.
2. **Compute GCD:** Find $GCD(a, N)$. If it is not 1, the factor is found.
3. **Period Finding (Quantum Part):** Use a quantum computer to find the period r of the function $f(x) = a^x \pmod N$.
4. **Compute Factors:** If r is even and $a^{r/2} \not\equiv -1 \pmod N$, calculate the factors using $GCD(a^{r/2} \pm 1, N)$. Classiq Technologies +4



Government security agencies are publishing timelines

Date	Requirement
1 January 2027	All new acquisitions to be CNSA 2.0 compliant
31 December 2030	All equipment and services that cannot support CNSA 2.0 to be phased out, unless exception granted
31 December 2031	All equipment and services to be using CNSA 2.0, unless exception granted
1 January 2035	All equipment and services to be using CNSA 2.0 exclusively

https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3020175/president-biden-signs-memo-to-combat-quantum-computing-threat/
https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF
https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography

HPE ProLiant Compute Gen12 is designed to meet the evolving security needs of our customers, aligning with the CNSA 2.0 timelines.

By incorporating state-of-the-art cryptographic solutions, HPE ensures that your customers' critical data remains secure in a post-quantum world.

- Firmware flash updates leverage quantum-resistant signing algorithms. Firmware flash updates for ProLiant Compute Gen12 iLO7 will be signed and authenticated using a CNSA 2.0 approved algorithm, preventing malicious entities with quantum computers from creating indistinguishable malicious firmware. Additionally, iLO7 can authenticate other firmware updates signed with quantum-resistant algorithms, enhancing future security.
- Silicon root of trust is enhanced with quantum-resistant algorithms. HPE ProLiant Compute Gen12 systems feature an enhanced silicon root of trust using quantum-resistant algorithms. During power-up, the iLO7 firmware is authenticated with these algorithms, preventing attackers with quantum computers and physical access from replacing the authentic firmware with malicious versions.
- Industry leaders as part of the ecosystem. Industry leaders like Thales and DigiCert highlight the importance of future-proofing crypto strategies in the post-quantum age. Their alignment with HPE's vision underscores the importance of proactive measures to ensure data security.

Thank you

Brian.Andersen@hpe.com