COVENANT AEGIS REVIEW OF ADVANCED COMPUTING VOL. 4 · NO. 1 · 2026 · PP. 3–24

Quantum Computing: From NISQ Devices Toward Fault-Tolerant Advantage

M. Lindqvist[1], P. Vasquez[2], H. Said[1], A. Kowalski[3]

[1]*Covenant Aegis Technology Division, Quantum Information Laboratory*

[2]*Department of Physics, Partner Research Network*

[3]*Center for Quantum Algorithms and Error Correction*

Received 9 Jan 2026 · Revised 28 Feb 2026 · Accepted 4 Mar 2026 · REVIEW ARTICLE · DOI 10.48-CA/advcomp.2026.0401 ·
Corresponding author: m.lindqvist@covenantaegis.com

ABSTRACT

Background. Quantum computing exploits superposition and entanglement to perform certain computations infeasible for classical machines, but device noise currently limits practical value. **Objective.** To review the field's trajectory from provable-speedup algorithms through noisy intermediate-scale quantum (NISQ) devices to fault tolerance, and to assess realistic applications and cryptographic implications. **Methods.** Narrative review of foundational algorithms, advantage demonstrations, error-correction theory and resource estimates. **Results.** A 2019 superconducting processor performed a sampling task in ~200 s argued to require millennia classically; error-correction experiments now show logical error decreasing with code distance; yet cryptographically relevant factoring is estimated to need on the order of 10^6–10^7 physical qubits. **Conclusion.** Broadly useful, general quantum advantage hinges on fault-tolerant logical qubits; the credible path is error correction, honest benchmarking and application discovery, not hype.

Keywords: quantum computing; NISQ; quantum advantage; error correction; Shor's algorithm; fault tolerance; post-quantum

1. Introduction

Since Feynman's proposal to simulate physics with quantum systems, quantum computing has promised speedups for specific problems. Shor's factoring and Grover's search algorithms established provable advantages [1,2], but realising them requires controlling fragile quantum states at scale—the central experimental challenge [3].

2. Foundational Algorithms

Shor's algorithm factors integers and computes discrete logarithms in polynomial time, threatening widely used public-key cryptography [1]. Grover's algorithm provides a quadratic speedup for unstructured search [2]. Quantum simulation of many-body systems—chemistry and materials—remains among the most physically motivated applications,

where even modest fault-tolerant machines could outperform classical methods [4].

Table 1. Representative quantum algorithms and asymptotic advantage.

Algorithm	Problem	Speedup
Shor [1]	Factoring / dlog	Exponential
Grover [2]	Unstructured search	Quadratic
HHL	Linear systems	Exp. (conditioned)
Quantum simulation [4]	Many-body physics	Exponential

3. The NISQ Era and Quantum Advantage

Preskill coined "NISQ" for present-day processors of tens to hundreds of noisy qubits without error correction [3]. In 2019 a superconducting processor performed random-circuit sampling argued to be intractable classically, a landmark advantage demonstration on a contrived benchmark [5]; photonic boson-sampling reported analogous claims [6]. These results are scientifically important but do not yet solve useful problems, and classical algorithms have repeatedly narrowed claimed gaps (Figure 1).

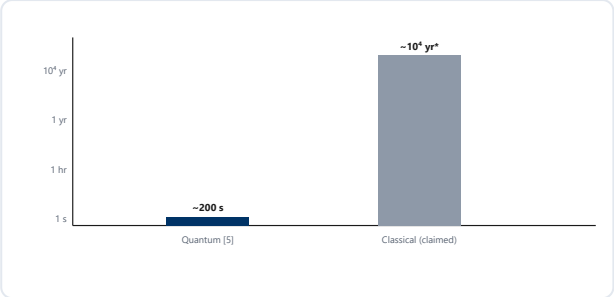


Figure 1. Reported 2019 random-circuit-sampling runtime: ~200 s on the quantum processor versus the originally claimed classical estimate [5]. *The classical estimate was later contested and reduced by improved algorithms—illustrating that advantage claims are moving targets. Log scale, schematic.

4. Error Correction and Fault Tolerance

Physical qubits decohere; useful computation requires encoding logical qubits across many physical ones using quantum error-correcting codes such as the surface code, with the threshold theorem guaranteeing arbitrarily long computation below a hardware error rate [7,8]. Recent experiments showed that increasing code distance can reduce logical error rates—an essential milestone [9]. Resource estimates indicate cryptographically relevant factoring will require millions of physical qubits, underscoring the distance still to travel [10] (Table 2).

Table 2. Indicative scale gap between today and fault-tolerant cryptanalysis [9,10].

Milestone	Physical qubits (order)
Advantage demo (2019)	~50–70
Early logical qubits	~10^2–10^3
RSA-2048 factoring	~10^6–10^7

5. Implications and Realistic Applications

Near-term value is most credible in quantum simulation and algorithmic research, while broad commercial advantage awaits fault tolerance. The cryptographic threat from future error-corrected machines has already prompted standardisation of post-quantum cryptography, motivating migration well before large quantum computers exist [11].

6. The Covenant Aegis Program

Our quantum effort is hardware-agnostic and application-led: benchmarking devices on honest metrics, developing error-mitigation and, prospectively, error-correction techniques, and identifying problems—chemistry, optimisation and simulation—where quantum methods may eventually complement classical high-performance computing. We treat extravagant near-term claims with scientific caution.

7. Discussion and Limitations

Benchmark contrivance, the volatility of classical-simulation baselines, and the enormous overhead of error correction temper optimism. Useful fault-tolerant computation likely remains years away; interim value must be demonstrated, not assumed.

8. Conclusion

Quantum computing has moved from theory to demonstrable advantage on artificial tasks, but practically useful, general advantage depends on fault-tolerant logical qubits. The serious path forward is error correction, honest benchmarking and application discovery.

References

1. Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J Comput*. 1997;26(5):1484–1509.
2. Grover LK. A fast quantum mechanical algorithm for database search. *STOC*. 1996:212–219.
3. Preskill J. Quantum computing in the NISQ era and beyond. *Quantum*. 2018;2:79.
4. Cao Y, et al. Quantum chemistry in the age of quantum computing. *Chem Rev*. 2019;119(19):10856–10915.
5. Arute F, et al. Quantum supremacy using a programmable superconducting processor. *Nature*. 2019;574:505–510.
6. Zhong HS, et al. Quantum computational advantage using photons. *Science*. 2020;370(6523):1460–1463.
7. Fowler AG, Mariantoni M, Martinis JM, Cleland AN. Surface codes: towards practical large-scale quantum computation. *Phys Rev A*. 2012;86:032324.
8. Shor PW. Fault-tolerant quantum computation. *FOCS*. 1996:56–65.
9. Google Quantum AI. Suppressing quantum errors by scaling a surface code logical qubit. *Nature*. 2023;614:676–681.
10. Gidney C, Ekerå M. How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*. 2021;5:433.
11. National Institute of Standards and Technology. Post-Quantum Cryptography Standardization (FIPS 203/204/205). 2024.

9. Physical Qubit Modalities

Several hardware platforms compete to realise qubits, each with distinct coherence, gate-speed and connectivity trade-offs. Superconducting circuits offer fast gates and mature fabrication; trapped ions offer long coherence and high-fidelity all-to-all connectivity at slower speeds; neutral atoms enable large reconfigurable arrays;

and photonic and spin qubits pursue other niches [A1]. No platform yet dominates on all axes, and the field's progress is measured less by raw qubit count than by gate fidelity and coherence.

Table A1. Qubit modalities and representative characteristics [A1].

Modality	Strength	Challenge
Superconducting	Fast gates	Coherence, cryogenics
Trapped ion	Fidelity, connectivity	Gate speed, scaling
Neutral atom	Large arrays	Gate fidelity
Photonic	Room temp, networking	Deterministic gates

10. Quantum Error Correction in Depth

Error correction encodes a logical qubit across many physical qubits so that errors can be detected and corrected faster than they accumulate. The surface code is the leading near-term candidate due to its high threshold and planar connectivity [A2]. The threshold theorem guarantees that, below a hardware error rate, logical error can be suppressed exponentially in code distance [A3]. A 2023 experiment demonstrated that a larger-distance surface code achieved lower logical error than a smaller one—crossing a qualitative milestone toward scalable fault tolerance [A4]. Figure A1 shows the schematic suppression of logical error with code distance below threshold.

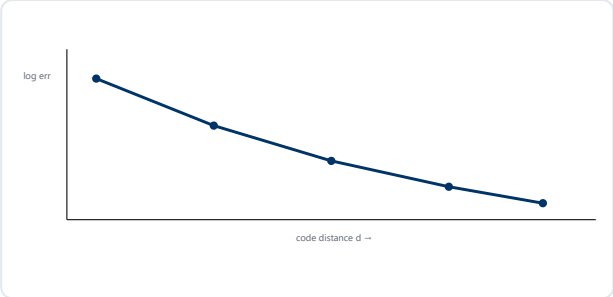


Figure A1. Schematic exponential suppression of logical error rate with increasing code distance below the fault-tolerance threshold [A2–A4]. Conceptual (log vertical axis).

11. Algorithms and Realistic Applications

Beyond Shor and Grover, the most physically grounded applications are quantum simulation of chemistry and materials, where representing entangled states is natural [A5]. Variational and hybrid quantum-classical algorithms are explored for NISQ devices but lack proven advantage and face barren-plateau optimisation issues. Claims of near-term advantage in optimisation and machine learning remain contested and frequently overturned by improved classical methods, reinforcing the need for honest benchmarking.

12. Resource Estimation for Cryptanalysis

Detailed resource estimates indicate that factoring RSA-2048 with Shor's algorithm would require on the order of millions of physical qubits and many hours of run time under realistic error rates [A6]. This enormous overhead—driven almost entirely by error-correction costs—explains why cryptographically relevant quantum computing remains distant even as small

advantage demonstrations exist, and why post-quantum migration is nonetheless urgent due to harvest-now-decrypt-later.

13. Benchmarking and Honest Metrics

Comparing devices requires metrics beyond qubit count: gate and measurement fidelity, coherence time, connectivity, and holistic measures such as quantum volume and application-level benchmarks [A7]. Because advantage claims depend on the best available classical baseline—which improves over time—benchmarks must be reported transparently and revisited as classical simulation advances.

14. Cryptographic Implications and Migration

The prospect of future Shor-capable machines has driven standardisation of post-quantum cryptography; organisations are advised to inventory cryptography and migrate long-lived secrets now [A8]. Quantum key distribution offers an alternative physical-layer approach for specific links but does not replace the broad need for post-quantum public-key algorithms.

15. Future Directions

Priorities are higher-fidelity qubits, demonstrated logical-qubit scaling, error-corrected algorithmic primitives, and identification of problems with credible, classically hard advantage. Useful, general fault-tolerant computation likely remains years away; interim value must be demonstrated rather than assumed.

Extended References

12. Bruzewicz CD, Chiaverini J, McConnell R, Sage JM. Trapped-ion quantum computing: progress and challenges. *Appl Phys Rev*. 2019;6:021314.
13. Fowler AG, et al. Surface codes: towards practical large-scale quantum computation. *Phys Rev A*. 2012;86:032324.
14. Aharonov D, Ben-Or M. Fault-tolerant quantum computation with constant error. *STOC*. 1997:176–188.
15. Google Quantum AI. Suppressing quantum errors by scaling a surface code logical qubit. *Nature*. 2023;614:676–681.
16. McArdle S, et al. Quantum computational chemistry. *Rev Mod Phys*. 2020;92:015003.
17. Gidney C, Ekerå M. How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*. 2021;5:433.
18. Cross AW, et al. Validating quantum computers using randomized model circuits (quantum volume). *Phys Rev A*. 2019;100:032328.
19. NIST. Post-Quantum Cryptography Standardization (FIPS 203/204/205). 2024.

Author contributions: ML and AK wrote the algorithmic and error-correction sections; PV and HS reviewed applications; all authors revised. **Funding:** Covenant Aegis Technology Division. **Competing interests:** Authors are affiliated with Covenant Aegis.

© 2026 Covenant Aegis Technology Division. This review synthesises publicly available peer-reviewed literature; figures are illustrative. For professional and educational use.