Aug 13, 2026 – Aug 14 · Daily Brief

HAWK signature scheme withdraws from the NIST third-round additional signature process

39 items · 11 sources | PDF | This issue's roundup is free

CONTENTS

Items	39
Sources	11
Reading time	~41 min read

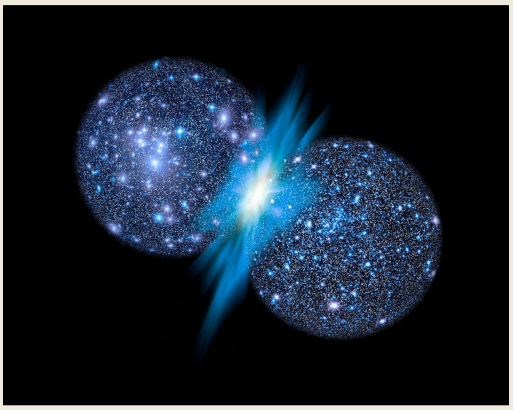
CURRENTSOTA

Physical qubits	1,180
2Q fidelity	99.99%
Logical qubits	96 LQ

Quantum hardware SOTA table →

01 Other

Three Things Today



1 **HAWK Signature Scheme Withdrawn** The lattice-based signature scheme HAWK has been withdrawn from the NIST third-round additional signature process due to an improved key-recovery attack (led by Anthropic's Claude Mythos Preview). Public disclosure was completed within approximately 17 hours [39] — the attack does not affect the finalized standards ML-KEM and ML-DSA, but it highlights the practical necessity of cryptographic agility in post-quantum migration planning.

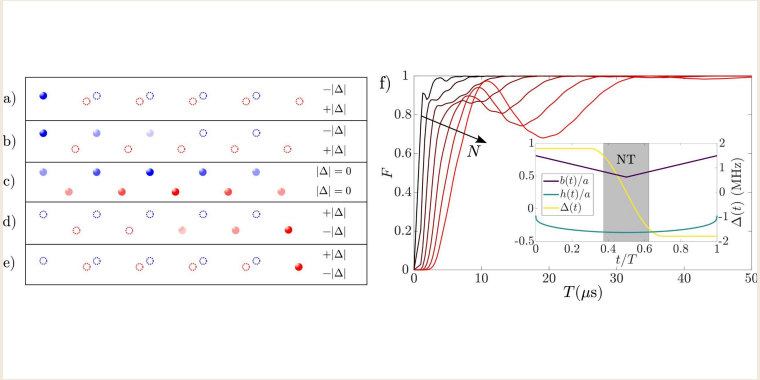
2 **New York State $60M RFP** New York State has launched a competitive solicitation to establish up to 4 regional quantum technology commercialization hubs, funded through the FY2027 budget [14] — direct state-level fiscal investment into quantum commercialization infrastructure.

3 **Xanadu × University of Alberta** Collaboration to develop quantum algorithms for photodynamic cancer drug discovery, focused on oncology and pharmaceutical design [11] — an algorithm R&D partnership bringing photonic quantum computing into drug discovery.

---

02 Hardware

Hardware Frontier



Superconducting

— Brazilian physicists have developed a continuous-variable universal computing building block based on superconducting

devices, with results published on August 13, 2026 [16]. Technical implication: demonstrates a universal computing primitive for continuous-variable encoding on a superconducting platform, complementing the mainstream discrete-variable superconducting qubit route. Landscape impact: if fidelity and scalability are validated, this could open a new paradigm for superconducting quantum computing, though error correction and multi-qubit integration are still needed before practical use.

Photonic

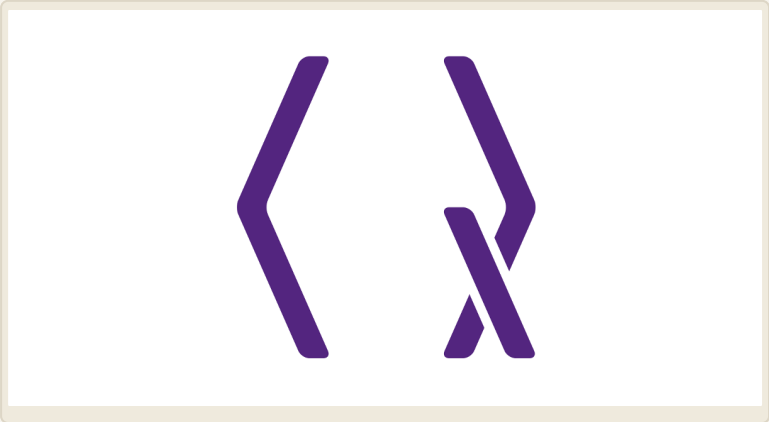
- Queen Mary University of London has developed Clavina, a modular photonic quantum computing architecture that designs quantum modules like computer components [26]. Technical implication: building photonic quantum computing systems in a modular fashion could improve system flexibility and maintainability. Landscape impact: the photonic route has long been constrained by loss and connection success rates; modular design, if paired with high-fidelity interconnects, could accelerate the deployment of medium-scale photonic processors.
- A quantum chip isolator has achieved 30 dB back-reflection suppression, demonstrating a magnet-free, broadband traveling-wave isolator for photonic integrated circuits [23]. Technical implication: achieves approximately 30 dB peak

isolation on a photonic integrated circuit without requiring magnetic materials. Landscape impact: provides a critical component for signal integrity in photonic quantum chips, reducing noise sources and advancing toward practical photonic quantum computing.

Neutral Atoms

— A theoretical framework enables robust topological quantum state transfer under long-range interactions in Rydberg arrays [29]. Technical implication: proposes a theoretical framework for fast, high-fidelity topological state transfer in one-dimensional long-range coupled systems, optimized for Rydberg atom dipole–dipole interactions. Landscape impact: the neutral-atom route gains new tools for quantum state transport and logical operations, but no experimental verification yet; timeline estimated at 2–3 years.

Algorithms & Software



— Catalytic z-rotations achieve constant T-depth: research shows that using specific catalytic states, the T-depth of arbitrary single-qubit z-rotations can be reduced to 3, with catalytic state size growing logarithmically polynomially in precision [28]. Technical implication: compresses the T-depth of single-qubit z-rotations to a constant of 3 when catalytic states are available; T gates are among the most expensive operations in fault-tolerant computation. Landscape impact: this result can significantly reduce gate overhead in fault-tolerant quantum circuits, with direct implications for quantum compiler and error-correction architecture design.

— Efficient graph-state generation in linear optics: proposes a method for efficiently generating graph states in photonic systems; graph states are a core resource for quantum computation, communication, and error correction [30]. Technical implication: bypasses traditional probabilistic fusion gates, directly generating

caterpillar graph states (CGS) using only single-photon sources, linear optics, and heralded measurements, reducing overhead from photon number and success probability. Landscape impact: one of the key bottlenecks in photonic quantum computing is large-scale entangled-state preparation; if experimentally validated, this scheme could advance the photonic route toward practicality.

— Measurement incompatibility in Bayesian multiparameter quantum estimation: systematically expounds the theory of multiparameter quantum estimation in the Bayesian framework and quantifies the impact of measurement incompatibility on achievable precision [27]. Technical implication: provides quantitative bounds on the impact of measurement incompatibility on multiparameter estimation precision; the authors describe it as a comprehensive and pedagogical treatment, drawing analogies to the multi-copy case in local estimation theory. Landscape impact: provides theoretical guidance for quantum metrology and sensing design, influencing the optimization of quantum-enhanced measurement schemes.

Industry & Ecosystem

Funding & Policy

— New York Governor Kathy Hochul announced the launch of a competitive RFP to establish up to 4 regional quantum technology commercialization hubs, with total funding of $60 million, administered by Empire State Development's NYSTAR division [14]. Business implication: direct state-level government investment into quantum commercialization infrastructure, attracting companies and forming regional clusters. Landscape impact: New York State intends to become a core hub of the U.S. quantum industry; other states may follow suit, with a 1–2 year timeline.

— SEALSQ and Quobly have reached a $5 million commercial agreement to integrate post-quantum security technology into Quobly's silicon-based quantum computing platform [18]. Business implication: quantum computing hardware vendors are beginning to embed post-quantum security modules, providing

security assurance for future quantum-classical hybrid systems. Landscape impact: the silicon-based quantum computing route gains security-layer support, advancing the commercial deployment process.

Partnerships & Deployment

- Xanadu and the University of Alberta are collaborating to develop quantum algorithms for photodynamic cancer drug discovery, led by Xanadu's algorithms team and Professor Alex Brown, Chair of the Department of Chemistry at the University of Alberta [11]. Business implication: a photonic quantum computing company is entering the drug discovery vertical, validating algorithmic advantages on real chemistry problems. Landscape impact: if the project produces viable algorithms, it will attract pharmaceutical industry investment, with a 2–3 year timeline.
- BTQ Technologies and ITCENGLOBAL subsidiary ITCEN PNS have signed an MOU to deploy post-quantum security solutions in South Korea, including PQC, quantum-safe authentication, and hardware root of trust [12]. Business implication: demand for post-quantum security is growing in the South Korean market, and BTQ is entering through a local partner. Landscape impact: post-quantum security deployment in Asia is accelerating,

with South Korean financial and government institutions likely to be early adopters.

— Canadian non-profit Open Quantum Design has reached a manufacturing partnership with South Korea's SDT, which will translate open-source hardware blueprints into physical ion-trap quantum processing units [13]. Business implication: open-source quantum hardware design gains a major commercial manufacturing partner, lowering the barrier to entry for ion-trap quantum computers. Landscape impact: if the open-source model succeeds, it will spawn more small and medium-sized quantum hardware vendors, with a 2–4 year timeline.

— Qunnect has received a DARPA contract to advance real-time polarization compensation technology for quantum networks, under the QuANET program and SBIR initiative [8]. Business implication: a quantum network hardware startup receives defense funding to validate the stability of entanglement distribution over telecom fiber. Landscape impact: quantum network infrastructure is moving toward practicality, with defense applications likely to deploy first.

— T-SQUARED has begun construction of a quantum innovation center for Infleqtion at Oxford Science Park; the facility will triple Infleqtion's UK operational capacity [9].

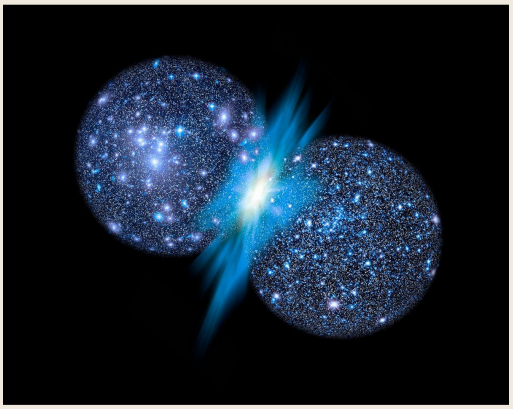
Business implication: a neutral-atom quantum technology company is expanding R&D and manufacturing scale in preparation for commercial production. Landscape impact: the UK quantum supply chain gains manufacturing capacity, intensifying competition in the neutral-atom route.

— The University of Guelph and Xanadu have signed an MOU to collaborate on quantum computing education and talent development, with the partnership running through 2028 [10]. Business implication: a photonic quantum computing company is investing in the education ecosystem, cultivating potential customers and talent. Landscape impact: the quantum talent pipeline is extending from research into industry, a long-term positive for the sector.

— CO.LAB Q is offering a 12-month commercialization studio to help quantum startups scale in Chattanooga, now open for applications [21]. Business implication: the accelerator model is entering the quantum space, providing entrepreneurial mentorship and resource connections. Landscape impact: the quantum startup ecosystem is further enriched, potentially spawning a new batch of application-oriented companies.

05 Other

Academic Frontier



— Coherent quantum light from single-impurity bound excitons: npj Quantum Information published research demonstrating the generation of coherent quantum light from single-impurity bound excitons [3]. Technical implication: demonstrates a coherent light source based on single-impurity bound excitons (source provides only paper title and DOI, no abstract available), offering a new pathway for solid-state quantum optics. Landscape impact: if integrable on-chip, this will advance on-chip quantum light sources, impacting quantum communication and computing.

— Missing eigenstates in the metric completion of the BBM Hamiltonian: analyzes the Bender–Brody–Müller Hamiltonian as a Hilbert–Pólya operator, showing that certain candidate eigenfunctions do not exist in the completion

space [20]. Technical implication: clarifies the mathematical structure of non-Hermitian Hamiltonians in quantum mechanics. Landscape impact: theoretical significance for foundations of quantum mechanics and quantum chaos research; no near-term industrial impact.

— Hamad Bin Khalifa University team sets quantum prediction limits: studies the constructive realization of self-referential prediction limits in quantum control, resource bounds, and Gödel security architectures [17]. Technical implication: constructively demonstrates limits of quantum prediction and Gödel security architectures. Landscape impact: provides boundary conditions for quantum machine learning and quantum control theory.

— Globular cluster streams in distant ultra-diffuse galaxies reveal new dark matter clues: Nature published research using stellar streams in distant ultra-diffuse galaxies to map dark matter distribution [25]. Technical implication: stellar streams discovered in distant ultra-diffuse galaxies provide a rare opportunity to map dark matter. Landscape impact: dark matter research gains a new probe, with potential crossover to quantum sensing technologies.

— Physicists determine baryon number, solving one of matter's greatest mysteries: research precisely determines the baryon number, potentially explaining the matter-antimatter asymmetry in the universe [31]. Technical implication: determines the elusive baryon number; the source does not disclose precision values, nor whether the result is experimental or theoretical. Landscape impact: a fundamental physics breakthrough may inspire new directions in quantum simulation.

— Neuroscientists underestimate brain cell computational power: new research shows each neuron can perform multiple computations simultaneously, thanks to hundreds of branches [33]. Technical implication: proposes a correction to neural computation models. Landscape impact: may influence neuromorphic computing and quantum-classical hybrid architecture design.

06 Impact

Today's Impact

1. **NIST post-quantum standardization process suffers a setback**: the HAWK withdrawal shows that even schemes reaching the third round can harbor fatal vulnerabilities. The attack does not affect the finalized standards ML-KEM and ML-DSA, but enterprises and governments must incorporate cryptographic agility into post-quantum migration planning [39].

2. **New York State quantum commercialization accelerates**: the $60M RFP will attract quantum companies to New York, forming regional clusters; investors should watch winning bidders and related supply chain opportunities [14].

3. **South Korean post-quantum security market launches**: BTQ and ITCEN PNS have signed an MOU establishing a commercial framework (no deployment or delivery yet); South Korean financial and government institutions may be the first to procure post-quantum security

products, providing a template for other Asian countries [12].

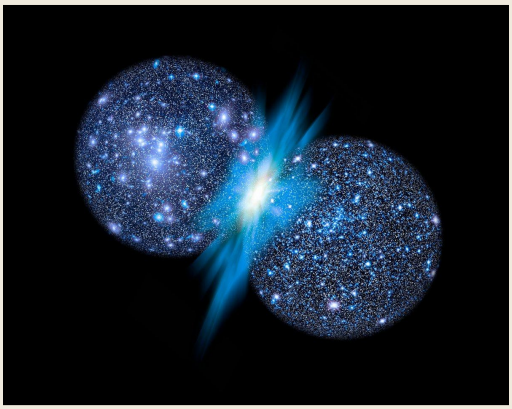
4 **Photonic quantum computing enters drug discovery**: if the Xanadu–University of Alberta collaboration produces effective algorithms, it will attract pharmaceutical industry investment and accelerate photonic quantum computing applications in vertical domains [11].

5 **Quantum network infrastructure receives defense funding**: Qunnect's DARPA contract, if the real-time polarization compensation technology succeeds, will advance quantum network deployment in defense communications and drive related hardware supply chains [8].

---

07 Other

Editorial Commentary



The most striking item in this issue is not a technological breakthrough but HAWK's

withdrawal from the NIST third-round additional signature process. HAWK was not withdrawn because quantum computers became more powerful, but because classical attacks, aided by more thorough analytical methods (including Anthropic's Claude Mythos Preview), discovered vulnerabilities. This reminds the industry that post-quantum security cannot rely solely on standardization processes; it also requires continuous security auditing and rapid response mechanisms. For investors, the PQC sector presents both risks and opportunities — companies that can iterate quickly and validate security are more likely to earn trust.

At the same time, New York State's $60M RFP and the deployment of post-quantum security in the South Korean market indicate that quantum technology is moving from the laboratory into regional economic competition and geopolitical security dynamics. The injection of funds from state-level governments and defense agencies will accelerate quantum commercialization, but may also lead to market fragmentation. Over the next 12–18 months, watch which regions can build sustainable quantum industry ecosystems rather than relying solely on one-time appropriations.

References

[1] Industry Opportunities for Advancing Non-Military Drone Computing

[2] Three Regional Quantum Finance Strategies Differ

[3] Generation of coherent quantum light from a single impurity-bound exciton

[4] Google Cloud Put Dates on Its PQC Migration. Signatures Trail Confidentiality by a Year.

[5] I Set Five Tests for Silicon Spin in March. One of Them Was Too Weak.

[6] Six Teams Shipped the Same ZK Verifier Bug. Quantum Doesn't Get a Patch.

[7] Ph.D Positions in Post Quantum Cryptography, VIT vellore

[8] DARPA Awards Contract to Qunnect to Advance Real-Time Polarization Compensation for Quantum Networks

[9] T-SQUARED Begins Construction on Infleqtion's Quantum Innovation Centre in Oxford

[10] University of Guelph and Xanadu Sign MOU to Advance Quantum Education and Talent Development

[11] Xanadu and University of Alberta Partner to Accelerate Photodynamic Cancer Drug Discovery

[12] BTQ Technologies Signs MOU with ITCENGLOBAL Subsidiary ITCEN PNS to Deploy Post-Quantum Security in South Korea

[13] SDT Joins Canadian Non-Profit Open Quantum Design as Official Manufacturing Partner

[14] New York State Launches $60M RFP for Regional Quantum Technology Commercialization Hubs

[15] WarpSpeed Says its AI cuts quantum encryption cracking cost sharply

[16] Superconducting device develops continuous-variable quantum computing

[17] Hamad Bin Khalifa University team sets bounds on quantum prediction

[18] SEALSQ & Quobly Seal $5 Million Post-Quantum Security Deal

[19] Gemma models surpass 900 million downloads, Google says

[20] Hilbert–Pólya Finds Missing Eigenstates in BBM Hamiltonian's Metric Completion

[21] CO.LAB Q offers 12 months to build a quantum business in Chattanooga

[22] Kagome metal's quantum effects yield strong heat-to-power at zero field

[23] Quantum chip isolator cuts back-reflections by 30 decibels

[24] Neuromorphic Labs builds a 'trust layer' for business AI

[25] Globular cluster stream in distant galaxy offers new dark matter insights

[26] Queen Mary University of London builds quantum modules like computer components

[27] Measurement incompatibility in Bayesian multiparameter quantum estimation

[28] Catalytic z-rotations in constant T-depth

[29] Robust topological quantum state transfer with long-range interactions in Rydberg arrays

[30] Efficient Graph State Generation in Linear Optics

[31] Physicists find major clue to matter's biggest mystery

[32] Rare Tropical Storm Lala on course for Hawaii, with hurricane conditions possible

[33] Neuroscientists have vastly underestimated brain cells' computing power

[34] Popular drug metformin transforms your gut into a sugar sink

[35] Squishies are everywhere—but what are they made of?

[36] Guest Post: Why Quantum Readiness Is Becoming a Venture Capital Question

[37] Guest Post — Quantum Strategy Demands a New Operating Model: From Uncertainty to Readiness.

[38] Kartik Srinivasan Appointed Editor-in-Chief of Optica Quantum

[39] HAWK Lattice Signature Scheme Withdrawn from NIST Round 3 After AI-Assisted Key-Recovery Attack