Sep 10, 2026 – Sep 11 • Daily Brief

Quantum encryption chips found to be secretly emitting light, potentially leaking secrets

50 items • 8 sources | PDF | This issue's roundup is free

CONTENTS

Items	50
Sources	8
Reading time	~66 min read

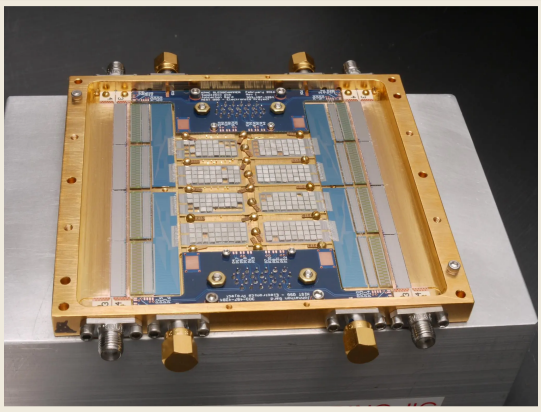
CURRENTSOTA

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

Quantum hardware SOTA table →

01 Other

Today's Three Key Developments



1 **Quantinuum pushes error correction from storing to computing** The Helix architecture demonstrated logical storage, Clifford computation, and inter-code interfaces simultaneously on the Helios machine, with no post-selection anywhere in the process [2] — error correction submits a full-match scorecard this time, though non-Clifford gates remain missing.

1 **SEALSQ revenue grows 131% in the first half** The company released its H1 2026

results, reporting 131% year-over-year revenue growth and issuing full-year 2026 guidance [35] — but the release does not break out how much of that came from post-quantum chips.

1 **F1 racing plugs a quantum solver into full-vehicle simulation** The BWT Alpine team expanded its partnership with SEALSQ, bringing in ColibriTD's quantum solver to handle multiphysics equations in race-car development while using post-quantum technology to protect design data [11] — high-budget engineering simulation becomes a new entry point for hybrid quantum computing; deal value and whether it is a paid engagement were not disclosed.

---

02 Hardware

Hardware Frontier

npj | quantum information — Article

Published in partnership with The University of New South Wales

Article in Press — https://doi.org/10.1038/s41534-026-01365-1

Security risks of VOA-induced luminescence in chip-based quantum key distribution

Check for updates

Zijian Li[1], Chenyu Xu[1], Xin Hua[2,3], Yongqiang Du[1], Xin Liu[1], Tao Lin[1], Xi Xiao[2,3] & Kejin Wei[1]

Integrated photonics is widely regarded as a key enabler for scalable quantum key distribution (QKD), offering compactness, stability, and compatibility with semiconductor fabrication. Despite rapid advances in chip-based QKD, the implementation security of integrated photonic components remains insufficiently understood. Here we present the first systematic study of an implementation-level security vulnerability associated with p–n junction–based variable optical attenuators (VOAs), a ubiquitous component in integrated QKD transmitters. We theoretically and experimentally demonstrate that electrically biased p–n junction VOAs emit spontaneous luminescence. Using a single-photon–sensitive spectral measurement technique, we identify the emission wavelength to be centered around 1107 nm, well separated from the C-band quantum signals. This spectral separation gives rise to a previously unrecognized wavelength-resolved side channel, enabling potential wavelength-splitting attacks without directly disturbing the encoded quantum states. By incorporating the measured luminescence into a quantitative security analysis, we show that even extremely weak emission can lead to non-negligible information leakage. Our findings reveal a fundamental and previously overlooked security risk in photonic integrated QKD systems and highlight the necessity of security-aware device design for future integrated quantum communication technologies.

Quantum key distribution (QKD) exploits fundamental principles of quantum mechanics to enable information-theoretically secure key exchange between remote parties. Over the past decades, remarkable progress has been achieved, including long-distance fiber transmission exceeding 1000 km, gigahertz-scale clock rates, and the deployment of metropolitan-scale quantum networks. These advances demonstrate the growing technological maturity of QKD and its potential for real-world deployment. However, large-scale adoption remains constrained by practical considerations such as system stability, footprint, and cost.

Integrated photonics has emerged as a leading platform to address these challenges by enabling compact, stable, and scalable QKD implementations compatible with mature semiconductor fabrication technologies. A wide range of QKD protocols have now been successfully realized on photonic chips, including decoy-state BB84, continuous-variable QKD, and measurement-device-independent QKD. These demonstrations establish integrated photonics as a promising route toward scalable quantum communication infrastructures.

Despite this rapid progress, the security of chip-based QKD systems is still predominantly assessed at the protocol level, often assuming idealized device behavior. In practice, integrated photonic platforms combine quantum and classical functionalities within tightly confined structures, where non-ideal physical processes may give rise to unintended information leakage. Recent studies have revealed several implementation-level vulnerabilities in integrated QKD systems, including state-preparation loss, optical back-reflections, light-injection-induced effects in modulators, side channels associated with electronic power consumption, and carrier-induced fluctuations in integrated phase modulators. These findings indicate that device-level physical mechanisms, if overlooked, can fundamentally undermine the security assumptions of QKD protocols.

Here, we identify and investigate a previously unreported implementation security vulnerability associated with p–n junction-based variable optical attenuators (VOAs), which are widely used for intensity control in integrated QKD transmitters. We theoretically predict and

[1]Guangxi Key Laboratory for Relativistic Astrophysics, School of Physical Science and Technology, Guangxi University, Nanning, China. [2]National Information Optoelectronics Innovation Center (NOEIC), Wuhan, China. [3]State Key Laboratory of Optical Communication Technologies and Networks, Wuhan, China. e-mail: kjwei@gxu.edu.cn

npj Quantum Information — Article in Press

Trapped Ions

Quantinuum fills in the compute piece of error correction

Quantinuum released measured results for the Helix architecture on Helios: logical storage, Clifford computation (a class of basic gate sets that can be efficiently simulated classically), and inter-code interfaces all realized on the same compact error-correcting code, with no reliance on post-selection at any point[2].

Technical significance: post-selection means discarding failed runs after the fact and tallying only the successful data, and it has long been the most-questioned methodological issue in logical-qubit demonstrations; remove that step, and the reported logical error rate becomes a full-match score rather than a highlight reel. Against current baselines, the report states only that this is a compact error-correcting code; Helios's qubit count, two-qubit gate fidelity, and physical-to-logical encoding ratio are not disclosed within it (the relevant figures mostly appear in the company's own announcements and await independent verification) — this is not a new fidelity record but the filling-in of one more capability dimension on the same hardware. What's still missing: non-Clifford gates (the magic-state-injection class, which determines

whether universal computation is possible) and sustained long-duration operation; the report frames that gap as the next step.

Competitive impact: the trapped-ion camp continues to counter the neutral-atom route's scale advantage in qubit count with logical-qubit quality; for buyers, whether post-selection was used is becoming a mandatory field on the due-diligence sheet, on a timescale of quarters.

Clarendon Laboratory proposes a scheme for 200,000 atom-atom entangled pairs per second

A temporal- and wavelength-multiplexed protocol based on cavity-assisted photon scattering predicts generation of 2×10^5 atom-atom Bell pairs (the most basic two-body entangled state) per second, with a predicted heralded fidelity of 0.999 and no need for intracavity qubit reset[22].

Technical significance: this is a proposal with numerical predictions, not yet validated on hardware; the source also gives no comparable baseline rate from existing experiments, so whether it pans out awaits an experimental group picking it up. Competitive impact: remote entanglement rate is the hard bottleneck in stitching many small machines into one large one, and also the rate-limiting

link in quantum network repeaters; if an experimental group takes up and reproduces this protocol, the modular-architecture route would be affected fastest, on a timescale of years.

Photonics and Quantum Communication

The attenuator inside a QKD chip is emitting light on its own

A peer-reviewed study found that the variable optical attenuator in integrated QKD (quantum key distribution, an encryption method that distributes keys using photons) chips emits unintended light near 1107 nanometers, and that this light forms a wavelength-distinguishable side channel that standard BB84 security analysis does not account for[3].

Technical significance: QKD's selling point is that security is guaranteed by the laws of physics, but that guarantee covers only the degrees of freedom written into the security proof; the attenuator's emission is unintended device-level radiation, an item the proof simply does not contain — a textbook implementation loophole rather than a protocol loophole. This is not a theoretical derivation but an emission spectrum measured on an actual chip.

Competitive impact: every QKD vendor pursuing on-chip integration, plus telecom and government customers currently running QKD procurement certification, is directly affected — security proofs need supplementary device modeling, and certification processes need a wavelength-scan item added; for deployed systems this is a patch cycle rather than a teardown, on a timescale of months.

Superconducting

A quantum memory scheme stores signals for 620 microseconds

Researchers used a new quantum memory technique to improve the coherence performance of superconducting qubits, storing signals for up to 620 microseconds[24].

Against baselines: the source gives only the single figure of 620 microseconds, with no coherence-time comparison for equivalent superconducting devices; moreover, a memory device's retention duration and a qubit's own T1 (energy relaxation time, how fast a qubit forgets its own state) are not the same metric and cannot be placed side by side as a record. What's still missing: superconducting's perennial problem is defect-induced timing drift, and beyond a single best value one must look at the long-term stability distribution.

Competitive impact: synchronization and buffering capability determine the efficiency of multi-qubit scheduling, and the major superconducting players' compiler layers can absorb components like this directly — an incremental improvement, not a change of route.

Neutral Atoms

Controlling where atoms are lost improves logical error rates 5.3× under realistic conditions

A new optimization method folds atom loss (an error mode specific to neutral-atom arrays: atoms escaping from the optical tweezers) into the design variables of the error-correcting code, improving logical error rates in up to 73% of tested scenarios, with a 5.3× gain under realistic conditions[23].

Technical significance: previously this route mainly cared about how many atoms were lost; this work turns where in the code they are lost into an actively manageable quantity. Against baselines: neutral atoms' strength has always been array scale, with weaknesses in cycle repetition rate (typically 1–10 Hz) and mid-circuit measurement; atom loss is a derivative problem of the latter, and what improves here is the error-correction-layer strategy, leaving

the hard constraint on repetition rate untouched.

Competitive impact: the error-correction stacks at QuEra, Pasqal, and Atom Computing can absorb compile-time optimizations like this without changing hardware, with effects on a timescale of quarters.

Materials and Devices

University of Vienna etches atomic-scale holes in white graphene

A team led by Jani Kotakoski used electron irradiation combined with oxygen to precisely shape atomic-scale holes in hexagonal boron nitride (the two-dimensional insulating material commonly known as white graphene) [19]. Technical significance: controllable hole position and size is a prerequisite for turning single-photon emitters into reproducible devices; previously such defects were largely generated by chance. Competitive impact: affects the materials supply side for single-photon sources and quantum sensing, still years away from a device product.

The hydrogen defects dragging down diamond sensors are fully traced

DEER spectroscopy revealed an X ensemble defect whose vacancy and interstitial

components disappear before 650°C, while vacancy clusters persist up to 1000°C[13]. Technical significance: assessing irradiation's effect on diamond quantum sensing has previously required analyzing the processing stage and the growth stage separately; this work connects the defect's evolution from creation through annealing into a single complete picture. Competitive impact: diamond quantum sensor manufacturers now have an evidence-based temperature boundary for their annealing process window — a process-parameter-level improvement.

03 Algorithms

Algorithms and Software

BB84 proven to reach the highest security level of unclonable encryption

Earlier unclonable encryption schemes achieved only search security, meaning an attacker has difficulty finding the correct key;

the new result raises this to unclonable indistinguishability, guaranteeing that an attacker cannot tell two encrypted messages apart, and completes the implementation using the well-established BB84 protocol[12].

Technical significance: going from cannot find the answer to cannot see the difference is a level jump in cryptographic security definitions, and the latter is the standard bar for modern encryption schemes. Competitive impact: the theoretical foundation of unclonable encryption is now firmer, but deployment remains limited by the practical channels for photon distribution; the beneficiaries are the academic and standardization circles that have long worked on quantum cryptographic proofs, with productization on a timescale of years.

Gate count for 200-qubit state preparation compressed from forty thousand to fifty-five hundred

A complex probability-distribution preparation task that previously required more than forty thousand quantum operations now needs only about 5500 CNOT gates using an optimized tensor-network method; the source gives a target-state metric of 7.44×10^{-9} (the original wording is fidelity; the exact definition needs checking against the paper)[14].

Technical significance: state preparation is the first step in nearly every practical quantum algorithm and also the most frequently overlooked hidden overhead; cutting gate count to roughly one-seventh demotes this upfront cost from a primary burden on the algorithm to a secondary item. Competitive impact: the resource-estimation baselines for financial derivatives pricing and Monte Carlo–class quantum algorithms need recomputing, directly affecting every team that publishes a quantum advantage timeline.

Quantum state tomography overhead drops from exponential to linear

By representing the density matrix as a contracted block tensor train, the memory and compute time needed to characterize a quantum system scales linearly rather than exponentially with qubit count[15].

Technical significance: the exponential overhead of quantum state tomography (fully measuring and reconstructing a quantum state) has long capped verifiable system size at a dozen-odd qubits; linear scaling means verification tools can finally keep pace with hardware qubit-count growth. Competitive impact: hardware vendors' acceptance-testing and verification steps benefit first — without scalable tomography, logical-qubit quality

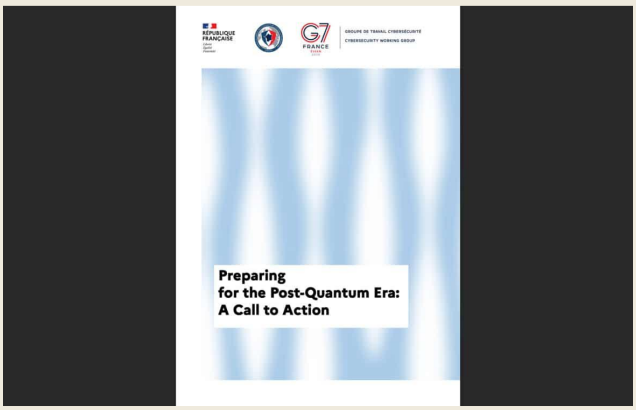
claims can only rest on sampled comparisons; toolchain deployment on a timescale of quarters.

Jolt zero-knowledge virtual machine switches to lattice cryptography

The open-source zkVM project Jolt released a LatticeJolt version that replaces elliptic curves with lattice cryptography, gaining speed and quantum resistance at the same time[21].

Technical significance: this is a rare positive case in post-quantum migration — switching to quantum-resistant primitives buys performance rather than costing it; in most migration scenarios lattice cryptography means larger keys and signatures. Competitive impact: the motivation for post-quantum migration in blockchain and zero-knowledge-proof infrastructure shifts from compliance to performance, and migration will move noticeably faster than in traditional IT, on a timescale of quarters.

Industry and Ecosystem



G7 urges all institutions to begin post-quantum migration; the real teeth are in procurement clauses

The G7 Cyber Expert Group issued a call to action in September 2026 urging all organizations to begin PQC (post-quantum cryptography, encryption algorithms resistant to being broken by quantum computers) migration [1]. The document is guidance rather than regulation, but its language on procurement and supply chains carries substantive force for enterprises and their suppliers [1].

Business significance: how hard regulation bites depends not on whether the document itself carries penalties but on whether it gets written into tender documents; once procurement language lands, small and mid-sized suppliers' migration windows are set by

their customers' contract cycles rather than their own technical roadmaps.

Competitive impact: the most directly affected are hardware and software vendors supplying G7 governments and financial institutions, who will hit this threshold at their next contract renewal, on a timescale of years; cryptographic asset inventory and certificate management vendors are clear revenue-side beneficiaries.

Cloudflare's 1.1.1.1 begins validating post-quantum DNSSEC signatures

Cloudflare enabled ML-DSA-44 DNSSEC signature validation on its 1.1.1.1 public resolver; no other major public resolver has yet announced equivalent support[4].

Technical significance: DNSSEC (digitally signing domain resolution results to prevent tampering) signature sizes balloon under post-quantum algorithms, running straight into DNS message transport limits; this deployment moves transport, downgrade attacks, and trust-chain issues from paper to production, exposing post-quantum migration as systems engineering rather than swapping a crypto library.

Competitive impact: registrars, authoritative DNS providers, and recursive resolver operators are forced to follow with testing,

giving the post-quantum migration of internet infrastructure its first observable real-world sample, on a timescale of years.

SEALSQ revenue grows 131% in the first half

SEALSQ released its H1 2026 results, reporting 131% year-over-year revenue growth and issuing full-year 2026 guidance[35].

Business significance: post-quantum security has long been a strong-narrative, weak-revenue sector, and this is rare revenue-side evidence; however, the company does not break out post-quantum chips' revenue contribution, and the low growth base and product mix mean it is still some distance from validation at scale. Competitive impact: over the same period the company is also building a post-quantum chip security center in Seoul with the municipal government, embedding quantum-resistant keys directly into semiconductor chips[20], and has expanded its partnership with the BWT Alpine F1 team to protect race-car design assets with post-quantum technology[11] — three threads pointing to the same play: don't sell algorithms, sell chips with keys in them plus a compliance on-ramp.

Qubic lands a CAD 1.5 million government contract after a USD 3.5 million seed round

Qubic signed a CAD 1.5 million quantum cryogenic amplifier contract with the Canadian government, having just closed a USD 3.5 million seed round[16].

Business significance: cryogenic amplifiers are a required component in the readout chains for superconducting and spin qubits — a classic picks-and-shovels business, with higher revenue certainty than full-system makers. Competitive impact: government orders provide early hardware supply-chain companies with bridge revenue between seed and Series A, a model becoming standard practice across North America and Europe.

Qilimanjaro selected for phase one of the EuroHPC Quantum Grand Challenge

Spanish company Qilimanjaro was among the 13 European quantum companies selected from 27 eligible proposals — the only Spanish firm — and its EuroQ-Stack project also received the STEP Seal of Excellence[17].

Business significance: the STEP Seal is the EU's endorsement label for strategic technology projects, and this recognition designates EuroQ-Stack as a high-quality strategic technology project bearing on European technological sovereignty and competitiveness. Competitive impact: Europe's quantum funding allocation is shifting from

casting a wide net to filtering, and the 13-company shortlist essentially defines the short list of European domestic suppliers for the next several years.

Ecosystem Briefs

The Quantum Insider launched an analyst-verified quantum market dataset product[36] — data about the quantum industry itself is now being sold as a commodity. Qtonic Quantum published its Q4 2026 quantum cybersecurity report[40]. QClairvoyance and Samgnya signed a memorandum of understanding on quantum technology research[39]. Quip Network will launch its Quantum Echoes QFT series[41]. Bull was selected to build the modernization upgrade of Spain's national weather forecasting infrastructure[37], a quantum-adjacent high-performance computing order.

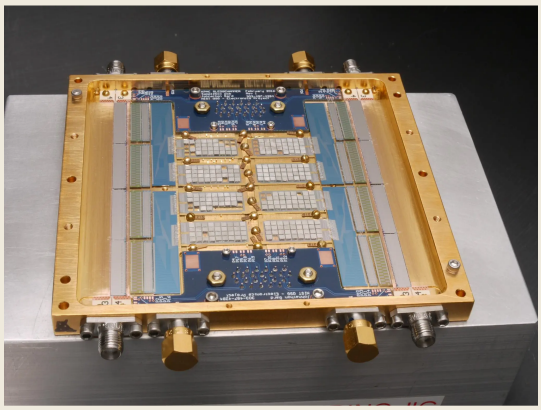
A practitioner-facing analysis has begun systematically mapping the patent eligibility of four core classes of quantum algorithms under US law[10] — the intellectual property boundaries of quantum software have no settled case law to this day, making it the least-priced risk item in valuation models.

On the talent side, Stockholm University concurrently posted three trapped-ion positions, targeting open quantum system

simulation, two-dimensional Rydberg ion simulation, and collective quantum phenomena in trapped ions respectively[7] [8] [9]; the University of Bologna opened PhD places in the mathematical physics of classical and quantum complex systems[6].

05 Other

Academic Frontier



A new measurement scheme approaches the ultimate precision bound in quantum sensing

Using a physical measurement scheme with boson-ancilla modes, multiparameter estimation precision is pushed close to the Holevo–Nagaoka bound (the theoretical upper limit on quantum measurement precision)[18].

Technical significance: this bound has largely been regarded as a mathematical existence result, lacking a corresponding scheme that

could be built in a laboratory; landing it on a concrete physical apparatus amounts to drawing a measurable ceiling for sensing precision. Competitive impact: performance claims in quantum sensing now have a common yardstick, and the comparison metrics used by magnetometer, atomic clock, and gravimeter makers will be progressively standardized, on a timescale of years.

Time itself may carry a minimum uncertainty

A result derived from unconventional quantum theory indicates that time itself may have a fundamental uncertainty, setting an ultimate upper limit on the measurement precision of any clock; the effect falls far below current detection capability but may point to hidden connections among quantum mechanics, gravity, and spacetime[25].

Technical significance: this is a falsifiable proposition at the theoretical level, not an engineering specification; its value lies in converting a metaphysical question into a long-term target for the atomic-clock precision race. Competitive impact: no near-term industry impact, but it gives the precision goals of next-generation optical clocks a physical motivation rather than purely engineering momentum.

Google's many-worlds claim: the argument is serious, the experiment is the wrong hook

Commentators note that Google attached a serious argument about the interpretation of quantum mechanics to a benchmark test whose results every standard interpretation predicts equally well, and whose headline data has never been directly verified; ten months later the same lab retained the interference portion[5].

Technical significance: distinguishing between interpretations of quantum mechanics requires experiments that can tell them apart, and the benchmark Google hung its case on is precisely one that cannot — every standard interpretation predicts the same result; this mismatch between the validity of an argument and the design of an experiment is a recurring structural problem in quantum computing publicity. Competitive impact: what's affected is the whole industry's credibility account; for investors, the practical test is to ask whether this experiment could falsify the opposite conclusion, rather than how striking the conclusion sounds.

06 Impact

Today's Impact

1 **QKD vendors pursuing on-chip integration need to rerun their security assessments.** The attenuator's unintended emission near 1107 nanometers constitutes a side channel that standard BB84 analysis does not cover[3], meaning security proofs need a device-radiation model added and certification processes need a wavelength-scan item. Worth watching next: whether any vendor publishes a device-level shielding solution, and whether standards bodies write spectral testing into QKD certification specifications.

1 **The due-diligence checklist for evaluating logical qubits has changed.** Helix's demonstration on Helios used no post-selection at any point[2], elevating whether post-selection was used from a paper footnote to the primary methodological question; from now on, whenever any vendor reports a logical error rate, the first

question should be whether data was discarded. Worth watching next: when non-Clifford gates and magic state injection appear on the same hardware — that is the tipping point for universal logical computation.

1. **The cost accounting for post-quantum migration is being rewritten from both ends.** At one end, the G7 transmits migration pressure to supply chains through procurement clauses[1]; at the other, Cloudflare's actual deployment on 1.1.1.1 exposes systemic difficulties in transport, downgrade, and trust chains[4]. For enterprise security leads, the real bulk of the migration budget is not swapping crypto libraries but auditing the protocols that larger signatures will burst. Worth watching next: whether a second major public resolver follows with post-quantum DNSSEC validation.

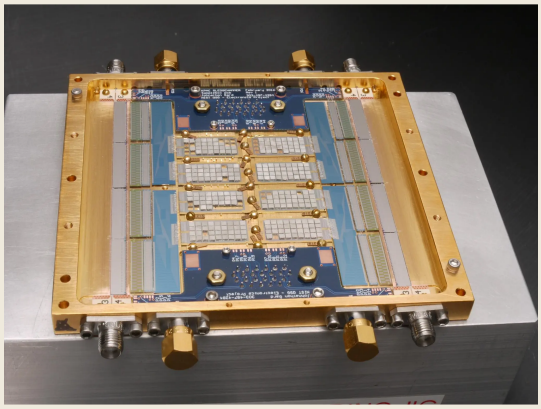
1. **Resource-estimation baselines for quantum software are being revised downward across the board.** Gate count for 200-qubit state preparation fell from over forty thousand to about 5500[14], and tomography overhead dropped from exponential to linear scaling[15] — both act on the front-end and verification stages of algorithms. Any team that ran a quantum

advantage timeline calculation in the past year needs to recompute its denominator. Worth watching next: whether these two methods can run on real hardware rather than remaining simulation benchmarks.

1 **Revenue-side evidence is starting to appear in post-quantum security.** SEALSQ's first-half revenue grew 131%[35], with a chip security center landed in Seoul over the same period[20] and an expanded partnership in F1 race-car development protecting design data with post-quantum technology[11] — the sell-chips-not-algorithms path is starting to show returns on the books. Worth watching next: whether the full-year guidance is met, and how much of the growth genuinely comes from post-quantum migration rather than the traditional security chip business.

07 Other

Editor's Take



The most noteworthy thing about these two days is not which number set another record, but that several methodological standards are tightening at once. Error-correction demonstrations are starting to stress no post-selection, measurement precision is starting to benchmark against theoretical limits, quantum state verification tools can finally keep up with qubit-count growth, and even interpretational claims are being publicly interrogated on whether the experimental design can support the conclusion. These all point to the same thing: this industry is shifting from competing on whose numbers are bigger to competing on whose numbers hold up under questioning. For people doing due diligence, this is good news — comparability is improving; for people valuing companies off single best-case figures, this is bad news — claims like best pair, post-selected results, and conditional fidelity will be discounted ever more sharply.

Another thread is on the security side. Quantum-resistant encryption has long been treated as a future problem, and over these two days it became a present problem from three directions at once: procurement clauses make it a contractual obligation, infrastructure deployment exposes systemic friction, and unintended emission inside integrated devices reminds people that security guaranteed by

the laws of physics covers only the degrees of freedom written into the proof — the parts left out will leak all the same. Worth noting is that the pace of all three is not determined by technology — the rhythm of cryptographic migration is set by contract cycles, certification processes, and supply-chain replacement cycles, typically on a timescale of years. The real risk is not what year a quantum computer gets built, but that the organizational cost of migration keeps being underestimated while the window is narrowed notch by notch by procurement clauses.

References

[1] G7 Tells Every Organization to Start PQC Migration – But the Procurement Signal Matters More Than the Headline

[2] Quantinuum's Helix Demonstrates How a Compact Error-Correcting Code Can Compute

[3] Chip-Based QKD Has a Glow Problem: VOA Luminescence Creates a Side Channel That Standard Security Analyses Miss

[4] Cloudflare's 1.1.1.1 Now Validates Post-Quantum DNSSEC Signatures – And Shows Why PQC Migration Is a Systems Problem

[5] Google's Multiverse Claim Was a Serious Argument Attached to the Wrong Experiment

[6] PhD fellowship in Mathematics @University of Bologna on Mathematical physics of classical and quantum complex systems

[7] PhD position in open quantum system simulations with trapped ions at Stockholm University

[8] PhD position in 2D quantum simulations with trapped Rydberg ions at Stockholm University

[9] Postdoc position in investigation of collective quantum phenomena with trapped ions at Stockholm University

[10] Patenting Quantum Computing Innovations: Lessons from Four Core Quantum Algorithms – Part 1

[11] LUMI AI Factory Selects IQM's Halocene Roadmap for Europe's First Superconducting Logical Qubit System

[12] Infleqtion and Cisco Partner to Advance Distributed Neutral-Atom Quantum Networking Architectures

[13] Altera and Riverlane Partner on QEC Interfaces for Agilex FPGAs Following Post-Quantum Security Rollout

[14] Chalmers Researchers Accelerate Bosonic Quantum Operations by 1,000x Using Quantum Lattice Gates

[15] BWT Alpine Formula One Team and SEALSQ Expand Quantum Partnership into Multiphysics Simulation

[16] Researchers Prove BB84 Encryption Achieves Top Security Level

[17] Researchers Map Hydrogen Defects Limiting Diamond Qubit Coherence

[18] NIST quantum sensors help verify nuclear safeguards internationally

[19] Researchers Achieve 7.44e-9 Fidelity for 200-Qubit States

[20] Xanadu and AMD speed up quantum computing with Backline link

[21] Researchers Cut Complexity of Quantum State Estimation

[22] $1.5M contract follows $3.5M seed for Qubic's quantum hardware

[23] Spanish Firm Qilimanjaro Joins EuroHPC Quantum Push

[24] A new measurement scheme nears the ultimate precision for quantum sensing

[25] Vienna team sculpts quantum atomic-scale pores in 'white graphene'

[26] Seoul and SEALSQ build center for post-quantum chip security

[27] Jolt zkVM switches to lattices for faster, post-quantum proofs

[28] Clarendon Laboratory boosts atom-atom entanglement with cavity design

[29] Researchers Cut Quantum Error Rates with Optimised Atom Loss

[30] Researchers synchronize qubits using a new quantum memory trick

[31] Physicists just found a tiny glitch in time itself

[32] AI researcher Jacob Coxon quit, fearing extinction. Security

experts see a familiar fight

[33] Unique, mathematical 60-sided "Go First Dice" go on display

[34] The Atlantic hurricane season just quietly broke a new weather record

[35] Giant armored crustaceans survive thanks to a gene stolen from bacteria

[36] 'Odd couple' black holes can find each other in space

[37] Why the Swift telescope was so special

[38] Are AI chatbots making us less human?

[39] 25 years after 9/11, survivors are still getting sick—here are the numbers

[40] 9/11 in Berkeley

[41] SEALSQ Reports 131% Revenue Growth in H1 2026

[42] Stevens Researchers Take Step Toward More Precise, Practical Quantum Technologies

[43] The Quantum Insider Launches Datasets, Analyst-Verified Quantum Market Information

[44] Bull Selected to Modernize Spain's National Weather Forecasting Infrastructure

[45] Quantum Cybersecurity Explained: Preparing for Quantum Computing

[46] Qubic Secures $1.5 Million Canadian Government Contract for Cryogenic Amplifiers

[47] BWT Alpine and SEALSQ Explore Quantum-Classical Simulation for Formula One

[48] QClairvoyance and Samgnya Sign MoU on Quantum Technology Research

[49] Qtonic Quantum Publishes Q4 2026 Quantum Cybersecurity Report

[50] Quip Network to Launch Quantum Echoes QFT Collection

Quantum Brief

All issues · Weekly analysis · Daily brief → qbitbrief.com

FOR RESEARCH REFERENCE ONLY

Images are sourced from the cited papers and press releases; if any citation is improper, please contact the editorial team for removal.