THIS WEEK IN QUANTUM SECURITY
September 6, 2026

By

Joel Van Dyk

Quantum Security Advisor and Strategist

This week brought developments across both sides of the quantum-security equation. IBM put its new 120-qubit Nighthawk r2 processor onto the IBM Quantum Platform with a substantial increase in circuit throughput; a new US bill aimed at strengthening American quantum competitiveness moved through congressional markup; QuFi launched a post-quantum verification layer designed to sit above existing digital-asset settlement networks; and hardware-security companies in Taiwan and Europe moved PQC further into chips, TPMs and embedded roots of trust.

The common thread is increasingly practical. A cryptographically relevant quantum computer has not arrived, and IBM's latest machine does not change that assessment. What is changing is the infrastructure around the problem. Quantum processors are getting faster, governments are organising industrial policy around quantum technology, and security vendors are trying to introduce post-quantum protection into systems that organisations cannot simply replace. The migration problem is becoming less abstract because the pieces required to carry it out are beginning to appear.

The Week's Key Developments

IBM increases quantum-computing throughput with Nighthawk r2

IBM announced Nighthawk r2 on 31 August and has already made the processor available through the payable part of the IBM Quantum Platform. The system has 120 programmable qubits, 218 couplers and 120 dedicated reset elements. IBM says it can execute more than 100,000 circuits per second, compared with roughly 4,000 circuits per second on its Heron systems, and has demonstrated accurate observable estimation on circuits containing more than 7,500 gates.

The important advance is not the qubit count. The Heron has more. The important part is the architectural change. The 1st part is reset. Nighthawk r2 uses independently controlled high-speed reset elements to return individual qubits to their ground state far more quickly between calculations. IBM says this reduces the idle time between circuit executions to as little as one microsecond and gives the processor up to 25 times the circuit throughput of Heron.

2nd connectivity. Heron uses IBM's heavy-hex topology. Nighthawk moves to a square lattice with four-degree connectivity. That means a qubit has more direct neighbours, so Qiskit has to insert fewer SWAP operations to implement algorithms requiring interactions between qubits that aren't adjacent. Every extra SWAP costs gates, and every gate adds error. So fewer routing gates can translate into deeper useful circuits.

3rd is throughput. With today's noisy quantum computers you typically don't execute a circuit once. You execute enormous numbers of circuits and shots, often with different parameters, error-mitigation settings,

randomized compilations, etc. Going from roughly 3,900 circuits/sec to over 100,000/sec changes how quickly those experiments can be completed.

Early advantage-candidate workloads have shown runtime reductions of up to ten times without a corresponding reduction in accuracy, according to IBM. Those are IBM's own performance measurements, so they should not be translated into claims about general-purpose quantum advantage or cryptographic capability. A 120-qubit processor executing circuits faster does not make RSA or elliptic-curve cryptography vulnerable. The more useful signal is engineering progress around the speed and repeatability of quantum workloads, alongside the error-correction capabilities enabled by mid-circuit reset and dynamic circuits.

For the quantum-security community, hardware progress like this is worth tracking without turning every processor announcement into a revised countdown clock. Migration timelines are already long enough to justify action. The relevant question is whether improvements in scale, quality and speed continue to arrive together over several generations rather than whether one system changes the cryptographic threat overnight. You won't see Crypto being broken overnight, but you will see what we've seen here: steady progress by the hardware vendors, of which IBM is one of the main, toward the goal of a cryptologically relevant computer. The debate over exactly when is almost irrelevant, although the predictions of most experts settle now around 2029/2030. The takeaway for most CyberSecurity departments is that preparation for the event should (have) start now, because it will come. The worst defense is to do nothing and hope nothing happens.

Read: IBM Quantum — Nighthawk r2.

QuFi proposes a post-quantum verification layer above existing blockchains

QuFi Network launched its QuFi Platform on 4 September, describing it as a post-quantum verification layer for digital assets and financial transactions that does not require the underlying settlement network to be replaced. Its architecture uses ML-DSA-65, SLH-DSA and ML-KEM-1024, with verification performed by a separate network before a transaction reaches the underlying settlement system.

The company has also built a proof of concept called uBTC on Bitcoin Testnet4. According to QuFi, minting, redemption and other actions are governed by hybrid ML-DSA and SLH-DSA verification challenges, while final redemption still settles as a standard Bitcoin transaction. QuFi has opened applications for independent verification nodes and says it plans integrations with EVM environments, Stellar, Solana and institutional infrastructure.

This is a company launch rather than an independently assessed security architecture, and the distinction between adding a quantum-resistant verification layer and making an underlying blockchain itself quantum-safe is important. Bitcoin's existing signature scheme does not become post-quantum simply because an external system has verified an instruction before settlement. The security model therefore depends on where authority ultimately sits and what an attacker could do at the settlement layer.

Even with that limitation, the architecture is interesting because it addresses a practical constraint that will affect many legacy systems: changing the cryptographic control layer without redesigning the entire infrastructure underneath it.

It also sits alongside the Tezos work announced earlier in the week, where contributors are preparing a fully post-quantum preview network. The two approaches attack the migration problem from opposite directions. Tezos is experimenting with changing the blockchain itself; QuFi is trying to introduce post-quantum verification above existing networks.

In contrast to both of these, Project Eleven is going to the core of the issue and building a ground up PQC KMS engine and infrastructure to aid in the migration as well as long term/future management of blockchains. (Disclosure: I consult at Project Eleven.)

Those experiments should produce useful evidence about which migration models can work for wallets, custodians and institutional digital-asset infrastructure.

US quantum policy moves toward industrial strategy

The American Quantum Competitiveness Act, H.R. 10163, was introduced on 27 August and went before a House Energy and Commerce subcommittee markup on 1 September. The legislation would direct the Commerce Secretary to promote trusted quantum supply chains and US commercial leadership in quantum technologies.

The legislation has attracted support from major technology companies including IBM, Microsoft and Google. Reporting around the bill has focused on its attempt to reduce fragmentation across government by giving the Commerce Department a stronger coordinating role around quantum technology, supply chains and commercialisation.

This is not primarily a post-quantum cryptography bill, and it should not be read as one. It is industrial policy. The useful quantum-security connection is supply-chain resilience and the growing assumption inside government that quantum computing, networking, sensing and quantum-safe cryptography are parts of a broader strategic technology ecosystem.

The distinction matters. Governments, just as FIs and other regulated entities, increasingly have two quantum problems to manage simultaneously: developing domestic quantum capability and protecting existing digital infrastructure against the consequences of future quantum capability.

The US already has separate post-quantum migration activity through NIST, federal identity work and the Treasury Quantum-Readiness Task Force. The Competitiveness Act adds an industrial and supply-chain layer to that picture rather than replacing those programmes. Treasury describes its own task force as a public-private effort to help the financial sector make an orderly and operationally resilient transition to quantum-safe technology.

The useful indicator now is not the number of quantum bills or task forces created. It is whether those programmes begin producing consistent procurement requirements, migration milestones and technical implementation guidance.

Post-quantum security moves further down into the hardware layer

Several developments this week point towards PQC becoming a hardware-security issue as much as a software issue.

Taiwanese startup Jmem Tek said its new security chip is approaching mass production after demonstrating its post-quantum and physical-unclonable-function technology at SEMICON Taiwan. The company is combining PQC acceleration with a hardware root of trust that uses manufacturing variations in individual chips to derive device identities and keys without storing those keys conventionally in memory. Jmem Tek says its Series A fundraising has reached $28 million and that it is working with foundry and semiconductor ecosystem partners internationally.

Separately, SEALSQ and wolfSSL announced support for ML-KEM and ML-DSA through the QVault TPM and wolfTPM interfaces. The companies describe QVault as being on track to become the first shipping TPM 2.0 device implementing the new post-quantum operations in the Trusted Computing Group's TPM specification.

Both announcements need qualification. Jmem Tek's manufacturing and customer claims come from the company, and SEALSQ's wording is explicitly forward-looking: "on track to be" is not the same as broad commercial deployment or independent certification.

The direction is nevertheless important.

PQC is moving into the components responsible for device identity, key generation, secure boot, authentication and protected storage. That is important for industrial equipment, IoT, automotive systems and other devices with long service lives because those systems cannot necessarily be replaced simply because their cryptography ages.

NIST's newly released IR 8615 reinforces the same broader point. Its secure-hardware recommendations call for cryptographic identities, provenance, attestation, supply-chain verification and continuous assurance across the semiconductor lifecycle. It also explicitly includes post-quantum computing among the emerging technologies that standards bodies need to accommodate.

For organisations planning PQC migration, hardware inventory will therefore become almost as important as cryptographic inventory.

Post-quantum standards work begins reaching candidate algorithms before final selection

A new IETF Internet-Draft published on 4 September defines COSE and JOSE representations for SQIsign, an isogeny-based signature algorithm currently being evaluated in NIST's additional post-quantum signature process.

The draft is unusually explicit about its status: SQIsign has not been selected as a NIST standard, and the underlying primitive may change during evaluation. The work is therefore not a recommendation for production deployment.

It is still useful as a standards signal.

One reason SQIsign continues to attract interest is its relatively compact signatures and public keys compared with some other post-quantum schemes. That can matter for constrained devices, authentication protocols and environments where message size is operationally important. The IETF work is essentially examining what interoperability would look like if the algorithm ultimately progresses.

This is also where the migration problem becomes more complicated. NIST already has standardised ML-DSA and SLH-DSA, but the additional signature process continues because different applications have different constraints.

Crypto-agility therefore cannot mean "replace RSA with one permanent PQC algorithm." It has to include the ability to support multiple algorithms and change between them as standards, cryptanalysis and operational requirements evolve.

Global Signals

North America

Summarizing what we talked about above, IBM's Nighthawk r2 was the most substantial North American hardware announcement this week. The processor's higher throughput is technically meaningful, but it does not represent a cryptographic break or a change in the immediate PQC threat model. IBM will hold a technical webinar on the system on 10 September, which should provide more detail on its real-world performance characteristics.

US policy is also becoming more explicitly commercial through the American Quantum Competitiveness Act, while Treasury's financial-sector readiness work and NIST's migration programme continue in parallel. The GSA Post-Quantum Cryptography Summit on 16 September should provide a useful test of how much of the federal effort has moved from policy into procurement and implementation.

United Kingdom and Europe

No major new UK government PQC policy was announced in the immediate window, so the NCSC's existing phased migration guidance remains the principal domestic planning framework.

Across Europe, the more useful development continues to be implementation in embedded and identity infrastructure rather than another high-level strategy document. The SEALSQ/wolfSSL work is particularly relevant for Europe's industrial and connected-device ecosystem because it puts standardised PQC operations behind established TPM interfaces.

The emerging question for European organisations is increasingly interoperability: how NIST algorithms, national assurance regimes, European identity systems and hardware trust infrastructure will operate together during a migration that may last most of the next decade.

Asia

As we saw above, Taiwan produced one of the more concrete regional signals this week through Jmem Tek's hardware-security work. A post-quantum accelerator tied to a device-level root of trust is a different proposition from adding a PQC library to enterprise software, particularly for AI hardware, defence systems and connected devices expected to remain in use for long periods.

Malaysia also continues to move toward practical enterprise readiness through the Pos Digicert and Quantum Secure Encryption partnership announced earlier in the week, combining existing PKI and digital identity with cryptographic risk assessment and quantum-readiness services.

The broader Asian signal is that PQC is increasingly being attached to existing trust infrastructure rather than treated as a stand-alone quantum-security product.

Australia

Australia remains one of the clearer policy environments because organisations already have a 2030 target for moving away from vulnerable public-key cryptography.

The Diraq/Equinix announcement from earlier this week also gives Australia an interesting parallel track: quantum computing infrastructure is moving into a conventional commercial data centre at the same time that the country is planning the retirement of vulnerable cryptography.

Those are different timelines, and the small Diraq system presents no cryptographic threat. What matters is that quantum computing and quantum-security migration are increasingly becoming ordinary parts of infrastructure planning rather than isolated research programmes.

Africa

I did not identify a significant new commercial or regulatory PQC announcement from Africa in the additional weekend research.

The most relevant near-term development remains the ITU-T Study Group 17 Regional Group for Africa meeting in Dubai on 16 September, followed immediately by the Global Quantum Drill.

For African governments and national cybersecurity teams, participation in standards, exercises and migration planning may currently be a more useful readiness indicator than domestic quantum-computing investment.

Middle East

The region remains unusually active following the recent Pasqal Arabia announcement, Quantinuum's Aramco memorandum and the Qatar satellite-security demonstration.

The next meaningful checkpoint is the ITU Global Quantum Drill in Dubai on 17–18 September. The useful output will not be another declaration that quantum security matters, but whether participants publish operational scenarios, readiness criteria or reusable migration exercises that organisations can apply to their own infrastructure.

The Quantum Innovation Summit later in September will provide another opportunity to see whether sovereign quantum-computing investment and PQC preparedness are beginning to converge into the same regional technology strategy.

Latin America

Brazil produced some of the most practically relevant PQC research in the previous few days through SBSeg 2026, including work on post-quantum PKI, crypto-agile Ethereum transactions, UAV communications and incremental migration of legacy signature systems.

That matters because it focuses on the transition layer rather than simply evaluating algorithms in isolation.

Latin America still lacks the coordinated migration timelines visible in parts of Europe, North America and Australia, but the Brazilian research community is increasingly working on the implementation problems that those timelines will eventually create.

Research Worth Reading

“Open EM Side-Channel Dataset for ML-KEM Implementations.” This new IACR work provides electromagnetic traces captured during ML-KEM decapsulation, creating a reproducible dataset for researchers working on implementation leakage and countermeasures. Its significance is practical rather than mathematical: it does not weaken ML-KEM itself, but it provides another reminder that a secure algorithm can still be implemented insecurely.

“Cryptocurrencies in the Quantum Age: Migration Paths to PQC.” This recent arXiv paper examines the exposure and migration options of Bitcoin, Ethereum and Solana. Its useful contribution is separating different threat and migration models rather than treating all blockchains as equally vulnerable. It is a review of migration options, not evidence that any of these networks are currently cryptographically compromised.

NIST IR 8615 — “Workshop Report on Rolling Next-Generation Secure Hardware into Standards.” This is not exclusively a PQC report, but its focus on continuous assurance, cryptographic identity, attestation, provenance and lifecycle security is directly relevant as PQC moves into HSMs, TPMs and semiconductor hardware.

IETF — “COSE and JOSE Registrations for SQIsign.” The new draft, already mentioned, is worth reading precisely because SQIsign is still being evaluated rather than standardised. It provides a useful view of how protocol designers prepare for interoperability while the underlying cryptographic selection process is still moving.

Meetings and Events to Watch

8 September — IonQ Investor Day, webcast. IonQ is expected to discuss its broader strategy following acquisitions including SkyWater. The useful indicators will be hardware milestones, manufacturing integration, customer commitments, capital requirements and revenue rather than short-term movement in the stock.

10 September — IBM Nighthawk r2 technical webinar, online. IBM will provide more detail on its latest processor and performance. The useful question is whether the throughput improvements translate consistently across useful workloads rather than just headline circuits-per-second measurements.

13–18 September — IEEE Quantum Week, Toronto, Canada. One of the year's major multidisciplinary quantum engineering meetings, covering hardware, software, networking and applications.

16 September — GSA Post-Quantum Cryptography Summit, Washington, DC and online. Federal identity, procurement, crypto-agility and migration implementation are expected to feature prominently. This should provide a clearer indication of how US federal policy will reach actual acquisition programmes.

17–18 September — ITU Global Quantum Drill, Dubai, UAE. The practical value will be in the exercise outputs: what organisations were asked to test, what evidence was produced and whether the resulting scenarios can be reused by national CERTs and critical-infrastructure operators.

22–24 September — Quantum World Congress, College Park, Maryland.

28–30 September — Quantum Innovation Summit, Dubai, UAE.

What to Watch Next Week

IonQ will probably attract the most investor attention next week. The useful questions are not whether quantum-company valuations move after Investor Day but whether the company can show that its acquisitions materially improve manufacturing, hardware delivery and access to paying customers.

IBM is worth watching for a different reason. Nighthawk r2 demonstrates a substantial improvement in throughput without a dramatic increase in qubit count. If that pattern continues, performance measures beyond raw qubit numbers will become increasingly important when assessing quantum-computing progress.

On the security side, the QuFi and Tezos experiments are worth following together. They represent different responses to the same digital-asset migration problem: change the underlying network or add a post-quantum control layer around infrastructure that already exists. The useful evidence will come from transaction overhead, wallet and custody compatibility, key-management requirements and how much trust remains in the legacy settlement layer.

The hardware-security developments deserve similar scrutiny. Saying that a chip or TPM "supports PQC" is only the beginning. Certification, side-channel resistance, update mechanisms, interoperability and deployment at scale will matter much more to enterprise buyers.

Taken together, this week looks less like a sudden acceleration toward a cryptographically relevant quantum computer and more like the gradual construction of everything organisations will need before one arrives.

That is probably the more important development.

— Joel Van Dyk

Source Links

1. IBM Quantum — Nighthawk r2

2. QuFi post-quantum verification platform coverage

3. H.R. 10163 — American Quantum Competitiveness Act

4. House markup including H.R. 10163

5. Treasury Quantum-Readiness Task Force
6. Jmem Tek PQC hardware-security development
7. SEALSQ and wolfTPM PQC integration
8. NIST IR 8615 secure-hardware report
9. IETF SQIsign COSE/JOSE Internet-Draft
10. NIST Post-Quantum Cryptography project
11. NIST PQC publications and crypto-agility guidance