THIS WEEK IN
QUANTUM SECURITY
August 28, 2026

By
Joel Van Dyk
Quantum Security Advisor and Strategist

The past two weeks have been unusually clarifying for quantum security.

The DCP (Dihedral Coset Problem) (see, for ex, https://www.linkedin.com/posts/woodwardalan_a-useful-reminder-about-judging-live-research-activity-7493324786232754176-JG0j/) alarm that dominated the start of August (e.g. https://www.linkedin.com/posts/woodwardalan_an-update-worth-sharing-on-the-quantum-vs-lattice-cryptography-activity-7494346779593785344-xVKO/) has now been formally refuted. Because the world's primary Post-Quantum Cryptography (PQC) standards (lattice-based encryption) rely on the mathematical hardness of problems closely tied to the DCP, if his algorithm had worked, it would have fundamentally broken the future of quantum-safe security.

At the same time, the first FIPS 140-3 Level 3 HSM supporting the full NIST post-quantum suite has reached validation, regulators are observing a cross-regional post-quantum digital-asset pilot, Pasqal has entered the public markets with fresh capital and a sovereign deployment strategy in the Middle East, and the academic community has gathered in Ottawa for QCrypt 2026 just days after the DCP question was closed.

In parallel, Japan has brought its first full-stack neutral-atom system online, Singapore is building a dedicated quantum-safe centre, Google Cloud has moved PQC further into enterprise key-management workflows, and the IETF community is now turning its attention to one of the harder parts of migration: post-quantum authentication.

The common thread is resolution followed by implementation. The mathematical alarm that briefly unsettled the lattice community did not hold, but the infrastructure work continued regardless. That is probably the most useful lesson of the fortnight. Organisations cannot wait for every research question to settle before they build procurement plans, migration programmes and cryptographic agility into the systems they already operate.

The Week’s Key Developments

The DCP claim is formally refuted, but the crypto-agility lesson remains

The most consequential research development arrived on 15 August, when Aparna Gupte, Seyoon Ragavan and Mark Zhandry published a formal no-go result showing that Daniel Simon’s proposed polynomial-time algorithm does not solve the Dihedral Coset Problem.

The distinction is important. The authors did not simply identify a mistake in Simon’s analysis. They showed that the algorithm itself discards too much information to recover the DCP secret with non-negligible probability. They also released a Lean-formalised version of the refutation, giving the result an unusually strong level of mechanical verification for a fast-moving cryptanalytic dispute.

The result is clear: the lattice assumptions underpinning ML-KEM and ML-DSA are not weakened by Simon's claim. The episode is closed.

What remains useful is the process itself. In less than two weeks, the community moved from a potentially serious claim to a formal, machine-checkable refutation. That is exactly how the research process should work.

For security teams, however, the operational lesson is independent of the final mathematical verdict. The organisations that spent those days asking what they would do if the claim held were effectively stress-testing their cryptographic agility. Teams with clear inventories, ownership models and replacement paths could answer that question quickly. Teams without them could not.

The threat turned out not to be real. The preparedness gap was.

Read: IACR ePrint 2026/1693 — The ePrint:2026/1591 Quantum Algorithm Does Not Solve DCP

Read: Postquantum.com — Simon DCP claim and refutation analysis

Read: Lean refutation on GitHub

The first FIPS 140-3 Level 3 HSM supporting the full NIST PQC suite reaches validation

Crypto4A announced on 20 August that its QASM cryptographic module had received FIPS 140-3 Level 3 validation through NIST's Cryptographic Module Validation Program.

That wording matters. Level 3 is not the highest FIPS 140-3 level, but it is a significant threshold because it includes strong physical tamper response, identity-based authentication and secure key-management requirements. Crypto4A's QASM supports ML-KEM, ML-DSA and SLH-DSA alongside classical cryptography, and the company positions the architecture as crypto-agile so that organisations can migrate without replacing the physical appliance.

For financial services, government and critical infrastructure, this is an important procurement milestone. One of the practical gaps in the PQC transition has been the distance between approved algorithms and independently validated hardware that can run them in environments where HSM certification is a requirement rather than a preference.

That gap has now narrowed materially.

The more important question for organisations planning HSM refreshes is whether full PQC support at the required validation level has moved from "nice to have" to an explicit procurement criterion. If the device being bought today is expected to remain in production for years, that question should already be part of the refresh cycle.

Read: NIST CMVP Certificate 5497 — Crypto4A QASM

Read: Crypto4A announcement via PR Newswire

Read: Quantum Computing Report — Crypto4A FIPS 140-3 Level 3 validation

Regulated digital-asset infrastructure enters a more serious post-quantum testing phase

The Responsible Fintech Institute and Safeheron have launched a cross-regional pilot to test post-quantum cryptography in digital-asset transaction infrastructure, with financial institutions participating and regulators from multiple jurisdictions observing.

The technical work is centred on integrating ML-DSA-65 into a multi-party computation signing architecture and testing transaction flows on a quantum-resistant NEAR testnet. Regulators including MAS, HKMA and MFSA are participating in an observer role in the first phase, with a governance workstream expected later.

This is more structured than the usual vendor proof of concept, but the limits are worth keeping clear. The participating institutions have not all been named publicly, the regulators are observing rather than certifying, and a testnet is not the same thing as a production custodial environment.

Even so, the signal is important. Regulators are no longer discussing digital-asset quantum readiness only in policy documents. They are watching actual implementation work.

For financial institutions, this matters because the migration problem in digital assets is more complicated than replacing a certificate authority or updating TLS. Custody, Key Management Systems (see ProjectEleven.com), signing architecture, MPC, blockchain compatibility and governance all have to change without breaking transaction integrity.

That makes the pilot useful as a template even before it produces final results.

It also reinforces a point we have made repeatedly in this briefing: crypto-agility has to exist across the whole stack. That means alternative KEMs, alternative signature schemes, replaceable trust anchors and test environments where those swaps can actually be exercised rather than merely documented.

Read: RFI / Safeheron pilot announcement

Read: Quantum Computing Report — RFI / Safeheron pilot

Read: Fintech.Global — Banks move to secure digital assets against future quantum threats

Pasqal lists on Nasdaq and pushes a sovereign deployment strategy in the Middle East

French neutral-atom quantum company Pasqal completed its business combination with Bleichroeder Acquisition Corp. II and began trading on Nasdaq as PSQL, with approximately $360 million in cash available to support system deployment, commercial expansion and further development.

The stock-market reaction generated plenty of attention, but I think the more strategically interesting announcement came alongside it.

Pasqal has also formed Pasqal Arabia with Eleven Ventures to deploy neutral-atom quantum systems commercially across Saudi Arabia and the broader MENA region. The commitment includes on-premises systems and local talent development rather than simply access to a Western cloud service.

That distinction matters.

Sovereign quantum capability is becoming a category of its own. Governments increasingly want access to hardware, skills and infrastructure that sit within their own jurisdiction rather than depending entirely on remote systems operated elsewhere.

We have seen variations of that logic in Australia, Japan, Thailand and now Saudi Arabia. The same question will eventually apply to quantum security: does local hardware investment come with local PQC migration capability, standards expertise and cyber-readiness planning, or do those two tracks develop separately?

The ITU Global Quantum Drill in Dubai next month should provide one useful indication of how seriously the regional security side is developing alongside the hardware investment.

Read: Pasqal / Bleichroeder business combination announcement

Read: Pasqal Arabia announcement

Post-quantum authentication is emerging as the next migration bottleneck

The Internet Architecture Board is convening a workshop in Prague on 11–12 October focused specifically on post-quantum authentication, with position papers due on 4 September.

This is worth watching because the industry has made considerably more progress on post-quantum key exchange than on authentication.

Hybrid key exchange is already appearing in browsers, cloud platforms and network infrastructure. Certificates, signatures, PKI dependencies and trust chains are moving more slowly because changing authentication can have a much wider operational impact.

The workshop is therefore aimed at exactly the part of the migration that is beginning to matter most.

For enterprise teams, this is another reminder that a migration plan built only around ML-KEM is incomplete. Key establishment is one layer. Identity, code signing, device authentication, certificate issuance and long-lived trust anchors are separate migration problems with their own dependencies and timelines.

Read: IETF / IAB workshop announcement — Post-Quantum Authentication

Google Cloud moves PQC into key-management and sovereignty workflows

Google Cloud has announced a preview of quantum-safe key import in Cloud KMS.

This may sound like a relatively narrow product feature, but it is operationally important because customer-controlled key material sits at the intersection of cloud security, sovereignty and cryptographic lifecycle management.

As organisations begin to migrate keys into post-quantum-safe formats, they need a way to move that material into managed cloud environments without undermining the very controls they are trying to strengthen.

This is another example of PQC moving into the enterprise plumbing rather than remaining a standards conversation.

The practical migration question for cloud customers is now becoming less about whether their provider supports PQC and more about which parts of their own key lifecycle, HSM strategy, certificate architecture and application stack still depend on quantum-vulnerable cryptography.

The next step is to be able to generate PQC keys and store them natively. For that, take a look at ProjectEleven.com (full disclosure, I advise them).

Read: Google Cloud — Announcing quantum-safe key import in Cloud KMS

Singapore expands the enterprise quantum-safe ecosystem

Singapore Institute of Technology and IBM plan to establish a dedicated Quantum-Safe Centre by the end of 2026.

The centre is intended to help organisations assess post-quantum risk, plan migration and build the skills needed to operate quantum-safe environments. That is significant because it moves beyond general awareness and into capability development for enterprises and the workforce.

Singapore has consistently taken a practical approach to quantum readiness, particularly across financial services and critical infrastructure. The new centre fits that pattern.

For security teams, one of the largest constraints over the next few years may not be algorithm availability at all. It may be the number of people who understand cryptographic inventories, PKI, application dependencies, HSMs, protocol migration and the operational consequences of changing them.

Centres like this are therefore as relevant to readiness as the algorithms themselves.

Read: Singapore Institute of Technology — SIT and IBM aim to establish Quantum-Safe Centre

Global Signals

North America

North America produced the most important research resolution of the fortnight with the formal DCP refutation, while the US market continued to move deeper into procurement and commercialisation.

New York State has launched a $60 million RFP for up to four Regional Quantum Technology Commercialization Hubs, with applications due 14 October. Each hub can receive up to $15 million, building on the state's existing quantum investment around SUNY Stony Brook.

At the federal level, the June executive orders on post-quantum migration continue to drive the compliance timetable. NIST has until 19 December to revise the Cryptographic Module Validation Program, and federal procurement teams should be watching how those changes affect module validation, FIPS requirements and vendor timelines.

QCrypt 2026 also ran in Ottawa this week, bringing the global quantum-cryptography research community together only days after the DCP episode was formally resolved.

Read: Governor Hochul — Regional Quantum Technology Commercialization Hub RFP

Read: QCrypt 2026

United Kingdom and Europe

In Europe, Pasqal's Nasdaq listing and planned Euronext path reinforce a broader pattern of European quantum companies seeking access to US capital while retaining a European market anchor.

France's 2027 certification requirement for quantum-safe security products remains the most immediate compliance deadline in the region and continues to influence product roadmaps for vendors serving financial services, government and critical infrastructure.

Israel also launched a domestic post-quantum communications consortium chaired by Allot, bringing together industry and academia to evaluate quantum-safe technologies across optical, mobile, satellite and data-centre communications.

Read: The Quantum Insider — Israel launches post-quantum communications consortium

Asia

Japan brought its first operational full-stack neutral-atom quantum computer, Shunkai, online on 24 August.

The system was developed through the National Institutes of Natural Sciences with Hitachi providing software and Infleqtion supplying the quantum processing unit. It begins with around 50 qubits, with a roadmap towards 500 qubits in the nearer term and 10,000 physical qubits by 2031.

The current qubit count is not the part I would focus on. The more useful signal is Japan's continuing move towards domestically operated quantum infrastructure with external research access and a stated commercialisation path.

South Korea also continues to expand its post-quantum ecosystem. BTQ Technologies has signed an MOU with ITCEN PNS to support quantum-safe deployment across financial, public-sector and enterprise infrastructure.

Singapore's new Quantum-Safe Centre adds another practical readiness layer in the region, while AQIS 2026 brought together the Asian quantum-information community this week.

Read: Infleqtion — Shunkai neutral-atom quantum computer now operational

Read: AQIS 2026

Australia

Australia's existing policy position remains one of the clearest internationally.

The ASD's 2030 deadline for moving away from quantum-vulnerable cryptography continues to give Australian financial institutions and critical-infrastructure operators a concrete migration horizon.

The practical implication is that research conferences, cloud-provider roadmaps and HSM validation milestones are not abstract developments for Australian organisations. They are inputs into a timetable that already exists.

Africa

No major commercial quantum-security announcements from Africa during the week.

The more important near-term event remains the ITU-T Study Group 17 Regional Group for Africa meeting in Dubai on 16 September, immediately before the Global Quantum Drill.

That gives African national CERTs and cybersecurity organisations a direct route into international quantum-readiness exercises and standards coordination.

The absence of large commercial announcements should not be mistaken for irrelevance. The long-term issue for African economies will be whether standards, workforce capability and migration expertise develop early enough to avoid creating a second-order dependency on technology decisions made elsewhere.

Middle East

Saudi Arabia produced the most significant regional commercial signal through the Pasqal Arabia joint venture.

The planned deployment of on-premises neutral-atom systems makes this a sovereign-hardware strategy rather than a cloud-access agreement and gives the region another route into domestic quantum capability.

The ITU Global Quantum Drill in Dubai on 17–18 September remains the most operationally important near-term security event, followed by the Quantum Innovation Summit in Dubai from 28–30 September.

For the region, the question is increasingly whether quantum-computing investment and quantum-security preparation are being developed as one programme or as two separate policy tracks.

Latin America

No major commercial or regulatory quantum-security announcement emerged from Latin America in the past week.

Brazil remains the centre of gravity for academic quantum activity in the region, with university and ICTP-SAIFR programmes continuing to build capability across quantum computing, error correction and cryptography.

The structural issue remains the absence of clear national migration timelines comparable to those now visible in North America, Europe, Australia and parts of Asia.

As global interoperability requirements begin to harden, that policy gap will become more important.

Research Worth Reading

“The ePrint:2026/1591 Quantum Algorithm Does Not Solve DCP” — Gupte, Ragavan and Zhandry. This is the essential paper of the fortnight. The authors formally show that Simon’s algorithm cannot recover the DCP secret because the relevant processing step discards too much information. The result closes the immediate lattice alarm.

Read IACR ePrint 2026/1693

“Module Learning With Errors and Structured Extrapolated Dihedral Cosets” — Weiqiang Wen and Jinwei Zheng. This CRYPTO 2026 paper proves a polynomial-time relationship between Module-LWE and a structured EDCP variant. It does not present an attack on ML-KEM, but it is an important contribution to the continuing research programme around lattice assumptions and dihedral problems.

Read IACR ePrint 2026/155

“quantum-safe: Bridging the Post-Quantum Production Gap with a Hybrid-by-Default Python Cryptography Library” — Animesh Shaw. The most useful part of this paper is not the library ranking but the gaps it identifies: weak hybrid-KEM support, limited migration tooling and poor protocol integration. Those are exactly the kinds of implementation problems enterprise teams are now running into.

Read arXiv 2605.17061

“Post-Quantum Cryptography Network Instrument: Measuring PQC Adoption Rates and Identifying Migration Pathways” — Sowa et al. This remains one of the more useful attempts to measure real network deployment rather than survey intention. The study finds only limited production adoption and provides a useful counterweight to enterprise surveys reporting high levels of “implementation.”

Read arXiv 2408.00054

“Post-Quantum Cryptography and Quantum-Safe Security: A Comprehensive Survey” — Chhetri et al. A broad reference covering algorithms, side-channel risk, TLS, DNSSEC, PKI, implementation and deployment. Useful for teams building migration programmes that need one map of the overall stack.

Read arXiv 2510.10436

Meetings and Events to Watch

31 August–4 September — TQC 2026, Sherbrooke, Canada. The Theory of Quantum Computation, Communication and Cryptography conference is directly relevant after the DCP episode and the CRYPTO 2026 Module-LWE/EDCP paper. I will be watching for further work on lattice hardness and quantum algorithms.

31 August–2 September — Silicon Quantum Electronics Workshop, Incheon, South Korea. Hardware focused, but worth following given South Korea's broader quantum investment programme and recent post-quantum commercial partnerships.

4 September — IAB Post-Quantum Authentication Workshop paper deadline. This is one of the most important immediate dates for the migration community because authentication is becoming the next major PQC deployment bottleneck.

Read the IAB workshop announcement

16–18 September — ITU Regional Meetings and Global Quantum Drill, Dubai. The Africa and Arab regional SG17 groups meet on 16 September, followed by the Global Quantum Drill on 17–18 September. This remains the most operationally significant international quantum-security exercise on the calendar.

ITU Global Quantum Drill

22–24 September — Quantum World Congress, College Park, Maryland. Worth watching for federal, defence and enterprise migration discussions following the US executive orders and NIST implementation work.

28–30 September — Quantum Innovation Summit, Dubai. Likely to surface further regional announcements following the Pasqal Arabia deal and the ITU Drill.

What I'm Watching Next

The DCP issue is now closed, but I am interested in how the community talks about the episode after the fact. The technical result matters, but so does the way research claims are communicated before review. The speed of the refutation was encouraging, but organisations still had to decide how seriously to treat the original claim while the mathematics was unsettled.

I will also be watching the post-quantum authentication discussion closely. Hybrid key exchange is moving faster than certificates, signatures and trust chains, and that imbalance will increasingly become the practical bottleneck for enterprise migration.

The Crypto4A validation is another one to follow. A certified HSM supporting the full NIST PQC suite gives procurement teams something concrete to evaluate, and I expect competing vendors to accelerate their own validation timelines.

The RFI and Safeheron pilot should also become more informative if regulators move from observer status into the governance phase. The publication of a technical whitepaper or open-source implementation would make the work considerably more useful to other financial institutions trying to understand what ML-DSA looks like inside real custody and signing architectures.

Finally, Pasqal's public listing will generate plenty of market noise. The more useful questions remain the same ones we have been asking across the sector: named customers, deployments, bookings, remaining performance obligations and whether the technology is being purchased again after the first experiment.

The interesting thing about this fortnight is that the infrastructure side of quantum security continued to advance while the research community was debating the foundations underneath it.

That is exactly why crypto-agility matters.

The mathematics will keep moving. The hardware will keep moving. The standards will keep moving.

The organisations that do well will be the ones that can move with them.

— Joel Van Dyk