PQ-SHIELD
Sept 2026

Quantum Risk on Critical National Infrastructure (CNI): Why We Must Act Now

WHY MIGRATION, GOVERNANCE AND CRYPTOGRAPHIC INNOVATION MUST MOVE NOW

Professor Ali Safaa Sadiq

Director, Cyber Technology Innovations (CTI)
De Montfort University

Mini Symposium 2026 | 8 September 2026 | Obuda University

DE MONTFORT UNIVERSITY LEICESTER
Gold Award
in association with National Cyber Security Centre
Department for Science, Innovation & Technology
Academic Centre of Excellence in Cyber Security Education
ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

THE DECISION CLOCK

The deadline is not Q-day. It is the point at which migration can no longer finish safely.

2028
Discovery + initial plan

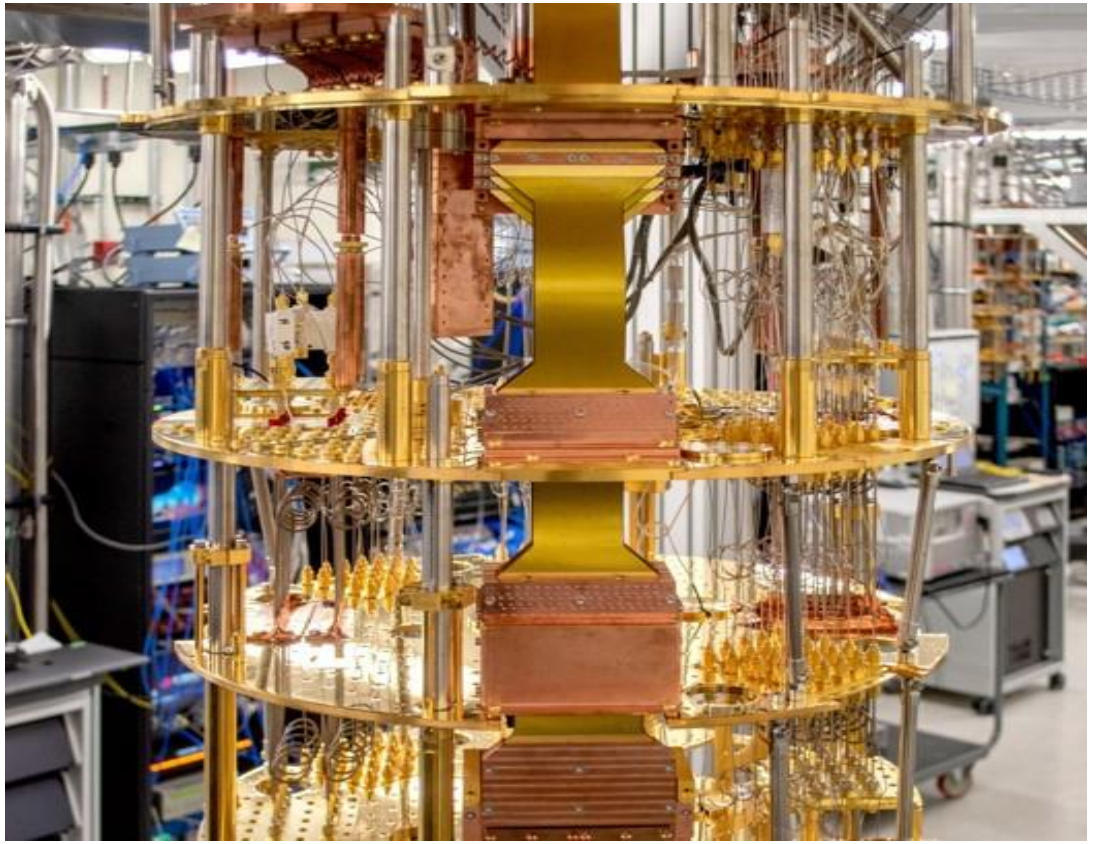
→

2035
Complete estate migration

The NCSC roadmap is a planning window, not a prediction of when a cryptographically relevant quantum computer will arrive.

Quantum computing changes which problems are practical

- Qubits use superposition and interference to process selected computations differently from classical machines.
- The security concern is specific, the mathematics behind RSA, Diffie-Hellman and elliptic-curve cryptography.
- A cryptographically relevant quantum computer would undermine today's asymmetric trust mechanisms.



THE CRYPTOGRAPHIC BREAK

A capable quantum computer changes the mathematics behind today's public-key trust.

RSA/ECC → **AT RISK**

Encryption + digital signatures

Under Shor's algorithm

Impact: key exchange, certificates, digital signatures and firmware-signing chains need quantum-resistant alternatives.

THE FALL OF RSA

We’re not trying to break RSA faster. We’re estimating when it could be broken and moving to quantum-safe cryptography in time.

300T
Years (Classical Computer)

→

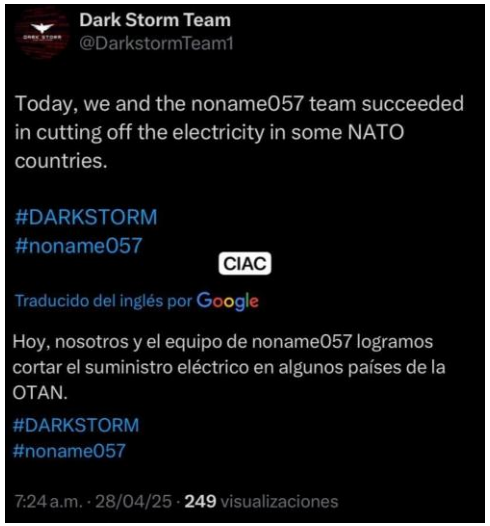
8
Hours (Quantum Computer)

Shor’s Theorem (1994): Provably demonstrates that a sufficiently large quantum computer can factor integers in polynomial time, breaking RSA and ECC fundamentally.

The 2025 Continental Crisis

A cyber attack on April 28, 2025, devastated the power grids of Spain, Portugal, and parts of France.

- Coordinated strike on high-voltage grid control systems.
- Millions without power; critical hospital and transport systems disrupted.
- Demonstrates the immediate threat to cyber-physical systems (CNI).



Reported Caracas Blackout During U.S. Operation - Why It Matters (3rd Jan 2026)

During the U.S. raid that captured Nicolás Maduro,
large areas of Caracas went dark.

- Why is this relevant? A cyber-enabled blackout, whether via grid control systems, telecoms, or supporting IT, shows that targeted cyber actions can create real-world power disruption during a kinetic event. That's directly in the threat model for UK critical infrastructure.
- Red flags:
  Unencrypted/weakly protected protocols on legacy links (e.g., IEC-104 without TLS).
  Remote-access exposures (vendor tunnels, weak MFA, shared accounts).

THE RISK IS ALREADY PRESENT

Harvest now, decrypt later

Long-lived secrets are exposed before Q-day.

Adversaries do not need a quantum computer today. They can retain encrypted traffic, backups or archives until future decryption becomes feasible.

Prioritise data and systems whose required secrecy life extends beyond the migration window - especially identity, operational, health, defence and research data.

CNI exposure is systemic - not confined to the data centre

Operational technology

Long asset lives, constrained devices and safety rules make upgrades slow.

Digital trust

Certificates, remote access, code signing and device identity rely on public-key cryptography.

Supply chain

Operators inherit cryptographic choices and timelines from suppliers.

The UK roadmap sets three delivery milestones

2028

Discover and plan

Define goals, complete discovery and build the first migration plan.

2031

Migrate priorities

Upgrade highest-priority services and refine the route to completion.

2035

Complete migration

Move all systems, services and products to post-quantum cryptography.

PART II: DELIVERY

A GOVERNED PROGRAMME ACROSS CRYPTOGRAPHY, OT/IT AND SUPPLIERS

Start with visibility, prioritisation and evidence

Discover

Map algorithms, keys, certificates, protocols, data lifetimes and hardware roots of trust.

Prioritise

Rank assets by consequence, secrecy life, migration difficulty and supplier dependency.

Pilot

Test standards-aligned PQC for performance, safety, interoperability and rollback.

CNI DELIVERY PRIORITIES

- ✓ Build a cryptographic inventory across OT, IT, cloud and vendor-managed services.
- ✓ Prioritise long-lived data, code and firmware signing, remote access and device identities.
- ✓ Align change windows with safety assurance, asset refresh and outage planning.
- ✓ Ask every critical supplier for its PQC roadmap, supported standards and upgrade path.
- ✓ Establish cryptographic agility so algorithms can change without redesigning the system.
- ✓ Govern evidence, exceptions, residual risk and accountable ownership.

THRESHOLD TRUST

RESULTANT-BASED RESEARCH FOR DISTRIBUTED, VERIFIABLE TRUST

Two schemes expand verifiable threshold secret sharing

Numerical shares

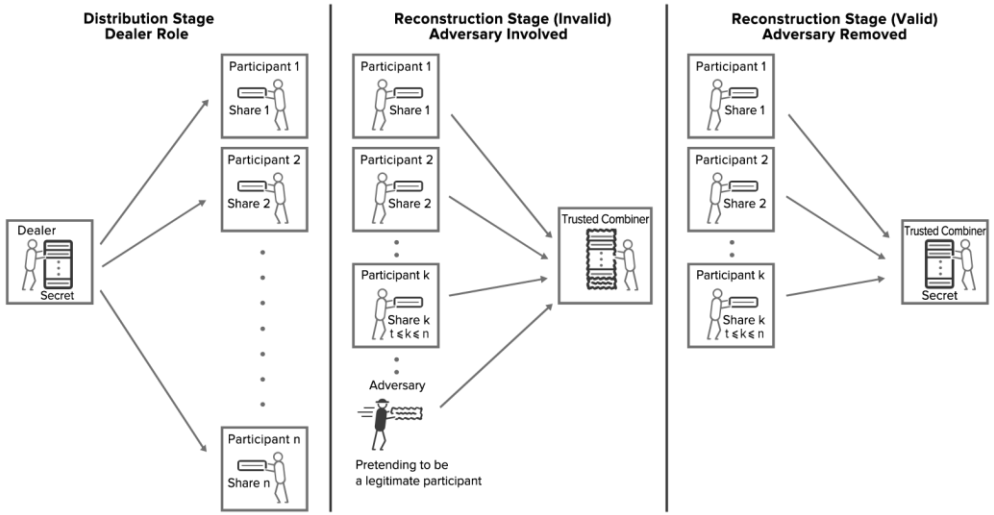
Efficient shares derived from evaluations of bivariate-polynomial resultants.

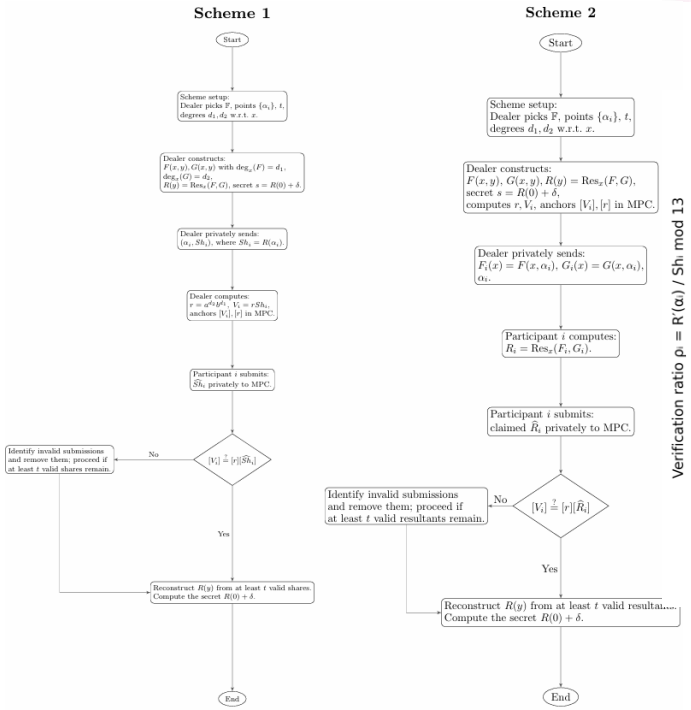
Symbolic shares

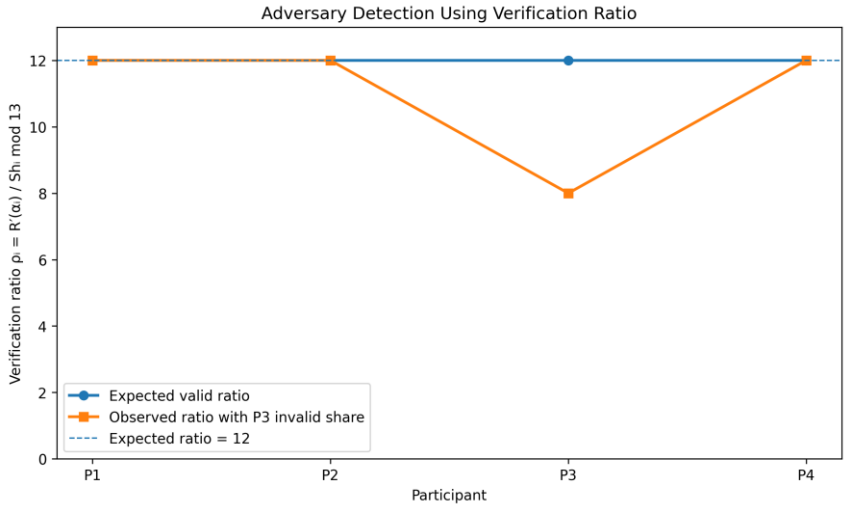
Polynomial shares offer enhanced security and post-quantum potential.

Proven verification

Formal proofs establish correctness, adversary detection and dealer construction.







Adversary detection in Scheme 1 using the verification ratio ρi = R′(αi)/Shi.

Threshold trust reduces dependence on any single key holder

Distribute

Split a secret across n participants; any t valid shares can reconstruct it.

Verify

Detect malicious or inconsistent contributions during recovery.

Deploy carefully

Promising for key custody, but deployment needs benchmarking, integration and standards alignment.

ECOSYSTEM READINESS

Readiness is a supply-chain property

CNI operators cannot migrate alone. Vendors determine protocol support, firmware availability, certificate formats and hardware refresh options.

- ✓ Make PQC requirements visible in procurement.
- ✓ Synchronise roadmaps with critical suppliers.

Capacity must scale early

- Discovery, architecture, testing and assurance require uncommon cryptographic, OT and programme skills.

Starting early spreads cost and complexity - and reduces the risk of a compressed transition.

Board ownership matters

Make quantum readiness executable

- Name a senior sponsor and accountable risk owner.
- Fund discovery, pilots and supplier engagement before 2028.
- Track coverage, priority migrations, exceptions and residual risk.

Resilience is designed before Q-day

- **Risk now: Long-lived encrypted data may already be collectible through HNDL.**
- **Deadline: Finish discovery and an initial migration plan by 2028.**
- **Delivery: Build crypto-agility across OT/IT, procurement and suppliers.**
- **Innovation: Threshold schemes can complement PQC by distributing trust and detecting adversarial shares.**
- **The Innovation:** Moving to **Symbolic Key Exchange** offers a mathematically resilient path.

DISCUSSION

A question to take away

ARE YOU READY FOR POST QUANTUM FUTURE SECURITY?

Thank You