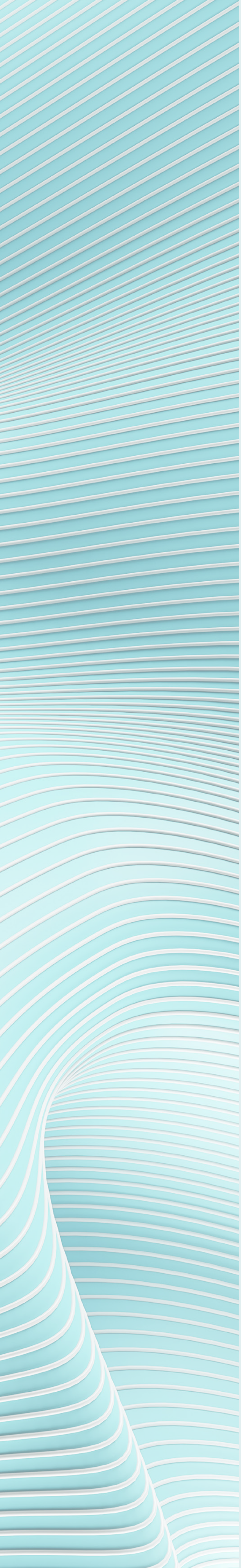
UNSW
Institute for
Cyber Security

Post-Quantum Cryptography



Preparing Australia for the Quantum threat

Quantum computing is poised to revolutionise science, medicine, and technology – but it also introduces new considerations for the digital systems we depend on daily. From online banking to government communications, the encryption that protects our data may eventually need to evolve to stay resilient.

While today's quantum machines aren't yet powerful enough to crack encryption, progress is accelerating. Experts suggest that within the next decade, quantum capabilities could begin to influence digital security. This makes it important for Australia to begin preparing now, to stay ahead of future developments.

Why Quantum changes everything

Modern encryption relies on mathematical problems that are practically impossible for traditional computers to solve. Quantum computers, however, operate differently which may allow them to solve these problems more efficiently. This means that some current encryption methods may eventually need to be replaced with alternatives that are secure against quantum techniques.

A powerful quantum computer could intercept secure communications, access financial transactions, decrypt classified government data and even forge digital signatures. One scenario being considered is ‘harvest now, decrypt later’ – where encrypted data is collected today with the hope that it could be decrypted in the future when quantum computers are more powerful. This highlights the importance of forward planning to ensure long-term data protection.

Understand the landscape

Some widely used encryption algorithms – mainly public key encryption technology - could be vulnerable to quantum attacks. These systems protect everything from credit card transactions to national security communications.

While quantum computers still need millions of qubits to break encryption, the pace of development is fast. In just two decades, we’ve gone from single-qubit experiments to machines with over 1,000 qubits. Because our digital systems are so interconnected, preparing early can help ensure continuity and resilience across sectors.

Post-Quantum cryptography: a path forward

Post-quantum cryptography (PQC) offers a solution. Unlike current systems based on factoring large numbers, PQC algorithms rely on mathematical problems that even quantum computers can’t solve efficiently.

The US National Institute of Standards and Technology (NIST) has already standardised several PQC algorithms, laying the groundwork for global adoption. Major tech companies are leading the way: Chrome now supports post-quantum Transport Layer Security (TLS), Apple has secured iMessages with quantum-resistant encryption, and Amazon offers post-quantum key management services.

During the transition, hybrid systems – combining classical and post-quantum algorithms – can help maintain compatibility while building quantum resilience.

Challenges to migration

Migrating to PQC isn't just a technical upgrade – it's a strategic shift. It requires funding, skilled personnel, and coordination with vendors. Many organisations still see quantum threats as a future issue, making it harder to justify immediate investment.

Post-quantum algorithms often demand more computational resources and larger key sizes. There's also a shortage of experts in this field, which can slow down implementation. And while guidelines exist, there are no binding regulations yet – leaving organisations uncertain about when and how to act.

Global momentum

Despite regulatory uncertainty, some sectors are moving quickly. The tech industry is already offering quantum-safe services, and telecommunications providers are actively migrating systems.

In the US, federal agencies have been directed to begin post-quantum transitions, though policy shifts have introduced some ambiguity. Europe has committed significant funding to quantum research and is embedding quantum resilience into cybersecurity regulations. Banks and financial institutions show mixed progress, with larger organisations generally more prepared than smaller ones.

Australia's position

The Australian Signals Directorate (ASD) recommends migrating to PQC by 2030–2035, but these are guidelines, not mandates. To meet these guidelines, a clear strategy at a federal level is needed.

Telecommunications providers are developing quantum-safe strategies, and the Reserve Bank of Australia is actively engaging with the PQC community. However, Australia still relies heavily on international standards and expertise, which increases costs and supply chain risks.

A practical strategy for implementation

Phase 1: assessment and planning (2026)

Start by auditing existing cryptographic systems – this will involve building an inventory of crytographic assets. Identify the risks associated with these assets, and engage vendors about their quantum roadmaps to develop migration timelines and budgets. Training key staff is essential - to understand the basics of quantum computing and the risks it poses to encryption. This will help organisations make informed decisions and align their strategies with emerging standards.

Phase 2: pilot implementation (2026–2027)

Deploy PQC in non-critical environments to test performance and compatibility. Use pilot results to refine migration procedures and establish hybrid systems. These pilots are an opportunity to evaluate performance, compatibility, and integration challenges.

Phase 3: full migration (2027–2030)

Systematically replace vulnerable systems, maintain compatibility during the transition, and verify security through independent assessments. Document lessons learned to guide future updates.

Recommendations

For government:

Introduce binding regulations with clear deadlines, invest in domestic R&D, support smaller organisations, and lead by example through early adoption.

For organisations:

Start planning now. Discuss at board level and educate C-suite executive staff members - migration could take years but it can be done in small, bite-size steps. Prioritise critical systems and build strong vendor relationships.

For industry:

Collaborate through standards bodies, develop sector-specific guidance, invest in workforce development, and support smaller players with shared resources.

Conclusion

- The quantum threat is real and approaching fast. But Australia isn't defenceless. Post-quantum cryptography offers proven protection, and early adopters are already implementing these solutions.
- Success depends on proactive planning and coordinated action. By preparing early, Australia can ensure its digital infrastructure remains secure and resilient.
- UNSW researchers Sushmita Ruj, Kayleen Manwaring, Ron van der Meyden and Marc de Leeuw have been actively working on this problem.
- UNSW's Institute for Cyber Security (IFCyber) can provide vendor-neutral guidance and support to organisations navigating this critical transition. Our experts can help Australian businesses and government agencies build quantum-resilient security frameworks tailored to their specific needs.
- Australia has the chance to lead in quantum-resilient cyber security. By working together across government, industry, and academia, we can build the secure digital infrastructure needed for the quantum age.

Further Reading

ASD guidelines for cryptography:
Australian government recommendations for post-quantum migration planning
https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cybersecurity-guidelines/guidelines-for-cryptography

Planning for post-quantum cryptography:
Australian resources for business and government
https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography

NIST Post-Quantum Cryptography standards:
Official US documentation of standardised algorithms and implementation guidance
https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

NIST Internal Report:
Transition to Post-Quantum Cryptography standards
nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

Post-Quantum Cryptography Migration:
Advanced technical and legal perspectives
https://github.com/sush-ruj/PQC-Migration/blob/main/PQC-Migration.pdf

UNSW Researchers

Sushmita Ruj: Associate Professor Sushmita Ruj is the UNSW Faculty of Engineering Lead for the Institute for Cyber Security at UNSW. Her primary research interests include applied cryptography, post-quantum cryptography, cyber security, blockchains and data privacy.

Kayleen Manwaring: Kayleen Manwaring is Associate Professor in the School of Private and Commercial Law at the UNSW Faculty of Law & Justice. Her research concentrates on the intersection of sociotechnical change and private and commercial law, with a particular focus on challenges arising out of cyber-physical technologies.

Ron van der Meyden: Ron van der Meyden is a professor at the UNSW School of Computer Science and Engineering. His research interests include computer security, logic in computer science, blockchain and smart contract. He leads the UNSW Interest Group in Blockchain, Smart Contracts and Cryptocurrency.

Marc de Leeuw: Marc de Leeuw is an Associate Professor at the UNSW Faculty of Law & Justice working at the edges of law, on domains that, due to radical technological change or ruptures in our ethical imagination, require legal consideration in a philosophical register.

Further enquiries

UNSW Institute for Cyber Security (IFCYBER)

✉ ifcyber@unsw.edu.au

🖥 ifcyber.unsw.edu.au

SCIENTIA
CORDE MANU ET MENTE
UNSW

CRICOS 00098G | 4891711