Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Quantum technology primer: Computing

For cyber security leaders

Content complexity
MODERATE

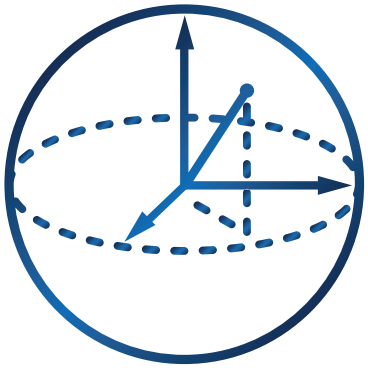
cyber.gov.au

Quantum computing seeks to leverage quantum mechanics to accelerate specific and complex computing tasks. Quantum computers are more efficient with certain computations than classical computers, making them a powerful complement to high-performance computing.

Despite these advancements, classical computers are still essential for everyday tasks. Quantum computers will depend on them for functions like controlling operations and reading results. This means quantum computers won't fully replace classical computers.

A sufficiently powerful quantum computer could break classical asymmetric encryption methods by performing calculations that are currently too complex for classical computers. Such capable systems are known as cryptographically relevant quantum computers (CRQC).

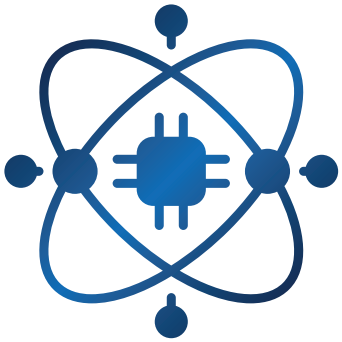
This guidance is part of a series of quantum technology primers. To learn more, refer to cyber.gov.au/quantum



About quantum computing

While a classical computer uses bits (0s and 1s) to process data, a quantum computer uses special qubits (quantum bits). Qubits allow quantum computers to perform certain tasks much faster than classical computers. Quantum computers can also do complex calculations that would otherwise be infeasible.

For example, imagine looking for a specific name in a long list. A classical computer checks each name one by one. A quantum computer could use superposition to explore many possibilities at the same time, making the search faster and more efficient.



The impact on cyber security

Quantum computing has the potential to disrupt some current cryptography. As CRQCs emerge, organisations will need to rely on quantum-resistant cryptography, known as post-quantum cryptography (PQC).

It is crucial that organisations understand the risks and challenges quantum computing poses, and plan for a future secured by PQC to maintain the security of systems and data. Rapid advancements in quantum computing are narrowing the window to prepare, making early action crucial to avoid future vulnerabilities.

Cyber security risks

Quantum computing introduces a range of cyber security considerations for network owners. While a CRQC does not yet exist, following proactive cyber security best practices is more secure than relying on reactive measures. This is especially critical as data encrypted today using classical methods may be vulnerable to 'harvest now, decrypt later' (HNDL) attacks.

The following are some potential risks organisations should factor into their cyber security plans and posture.

Cryptographic vulnerability resulting from cryptographically relevant quantum computers

CRQCs represent a future generation of quantum computers, capable of solving specific and complex problems that are infeasible for classical computers. They may need many millions of physical qubits to remain connected and perform useful calculations while generating almost no noise.

The presence of a CRQC will threaten the security of systems that rely on classical asymmetric cryptographic algorithms. This poses a major risk to encrypted data, secure communications and digital signatures.

To mitigate these risks, organisations should start transitioning to quantum-resistant algorithms by planning for PQC. Early action not only strengthens resilience but also aligns with cyber security best practice, helping protect systems and assets from the potential impact of a CRQC before it emerges. For more information, search 'planning for PQC' on cyber.gov.au

'Harvest now, decrypt later' attacks

HNDL is an attack method where malicious actors collect encrypted data even if they cannot decrypt it yet. They store this data to decrypt it in the future using technologies that will be more powerful, such as a CRQC.

HNDL attacks are of particular concern for current encrypted data that is highly sensitive or classified. Organisations should assume that any encrypted data compromised today could become readable in the future. This highlights the need for organisations to plan for their PQC transition early.

Supply chain risks

While most quantum technologies currently rely on classical components, their unique application of quantum phenomena can introduce new vulnerabilities. Quantum technologies may depend on specialised materials or vendors. The associated hardware and firmware could be prone to tampering, counterfeit parts or malicious implants.

Organisations should consider measures such as hardware provenance, digital attestation and secure boot mechanisms for supply chain integrity. It is important to assess vendors for secure development practices and require transparency across the supply chain.

Cloud application programming interface vulnerabilities

Vendors may offer quantum-computing services through hosted cloud platforms. This allows remote access to quantum processors through an application programming interface. These access points can introduce vectors for exploitation, resulting in unauthorised access or use, manipulation of quantum jobs, or denial-of-service attacks.

Both vendors and their customers should consider implementing strong authentication and access controls, rate-limiting, and continuous monitoring for abnormal activity. These measures reflect a shared responsibility model, requiring both parties to manage their respective roles actively to ensure secure and trustworthy use of cloud services.

Lack of expertise and resources

Organisations may struggle to find, train and retain staff with sufficient expertise in quantum computing and PQC. A gap in skills can lead to delays in PQC transition, misconfigurations, and implementation errors.

Organisations should consider investing in targeted training and certification programs. Complement these efforts by forming cross-disciplinary teams that combine expertise in cryptography, quantum technologies, software development, engineering, and network architecture.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre