Australian Government

CTPCO
CRITICAL TECHNOLOGIES POLICY COORDINATION OFFICE

Post-Quantum cryptography

Mathematical techniques for ensuring that information stays private, or is authentic, that resist attacks by both quantum and non-quantum (i.e. classical) computers. The leading application for post-quantum cryptography is securing online communications against attacks using quantum computers.

Key Sectors

Influences all sectors of the economy, including:

- Government
- Agriculture
- Banking & Finance
- Communications
- Defence & Defence Industry
- Energy & Environment
- Health
- Transport & Logistics
- Education & Research
- Mining & Resources
- Manufacturing
- Space

Estimated impact on national interest	Low	Med	High
Economic Prosperity			X
National Security			X

Key Australian Government Actions

Initiatives

- Australian Cyber Security Centre (ACSC)
- The ARC Centre of Excellence for Quantum Computation and Communication Technology
- Next Generation Technologies Fund
- Silicon Quantum Computing
- Quantum Technology Roadmap
- Digital Economy and Technology Policy
- Australian Cyber Security Growth Network

Regulations

- Defence and Strategic Goods List 2021

Example Outcomes

- Sensitive information communicated before practical quantum computers become available are protected from future advancements in quantum computing
- E-commerce, internet banking, secure software distribution and other applications that depend on public-key cryptography and use post-quantum cryptography are not adversely affected by advancements in quantum computing

Underpinning Science

ANZ Standard Research Classification Category

- Applied Mathematics
- Mathematical Physics
- Numerical and Computational Mathematics
- Software Engineering
- Data Management and Data Science
- Theory of Computation
- Electronics, Sensors and Digital Hardware
- Mechanical Engineering
- Electrical Engineering
- Optical Physics
- Quantum Physics
- Electronics, Sensors and Digital Hardware

Example Applications

Readiness Level – Now

- Implementation of pre-standardised post-quantum cryptography for classified networks
- Cyber security companies providing pre-standardised post-quantum cryptography services
- Laboratory testing of hardware accelerators for pre-standardisation post-quantum cryptographic algorithms

Readiness Level – 2–5 years

- Early adopters in the commercial sector (e.g. financial institutions) may implement post-quantum cryptography for critical networks

Readiness Level - Beyond 5 years

- Post-quantum cryptographic algorithms are incorporated in all consumer, commercial and industrial devices and software that need to store, send or receive sensitive information
- Dedicated hardware for increasing the speed of post-quantum cryptography

Australia's place in the world

The United States leads public research in post-quantum cryptography, with the highest research impact and two of the top ten institutions. Seven of the top ten institutions are based in the European Union, with Netherlands alone holding three. Australia is ranked 19th for research impact. Given the sensitive nature of this technology much cutting-edge research is unlikely to be in the public domain, meaning this assessment may not be a true reflection of overall research capability. This assumption is also supported by the limited patent activity in this area, which is led by the United State, followed closely by China. Australia has no patents in this area. The United Kingdom has the highest amount of venture capital (VC) investment in this area, ahead of Canada and the United States.

Opportunities and Risks

Post-quantum cryptography provides assurance that advances in quantum computing will not adversely affect the confidentiality and authenticity of digital communications and information, which currently use methods that are theoretically vulnerable to attacks using practical quantum computing.

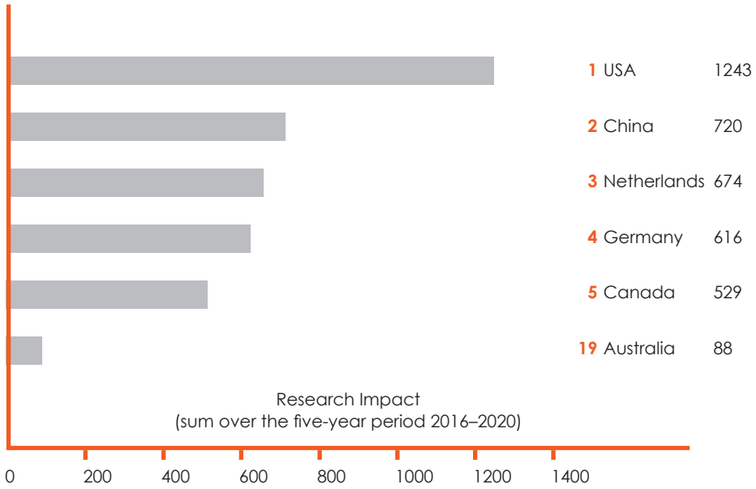
The opportunity offered by post-quantum cryptography is that Australians can continue to use their digital devices to communicate sensitive information with confidence that what is private today will stay private in the future. This applies to both government communications and communications between businesses and individuals. Subject to appropriate safeguards, Australia can also potentially export post-quantum cryptography hardware and software implementations.

Australia must have domestic expertise in PQC to ensure that we can usefully contribute to international efforts to develop suitable systems and to provide expertise in the deployment and testing of these technologies locally. Assuming that practical quantum computing is achievable, Australia faces risks to security until appropriately secure post-quantum cryptography is available to government, businesses and individuals. Because malicious actors can intercept and store encrypted communications today for decryption by a future practical quantum computer, the security risks increase the longer it takes to develop and deploy appropriately secure post-quantum cryptography. Australia also faces economic risks if our trading partners do not also have access to appropriately secure (and compatible) post-quantum cryptography, as that would limit the security of digital trade and ecommerce.

The transition to post-quantum cryptography will also require significant updates to current cryptography, which will take significant time and money, and require hardware as well as software updates. This transition could give rise to additional risks and it is foreseeable that many existing and legacy systems may never be updated and remain vulnerable until they are retired.

Research Impact (RI)

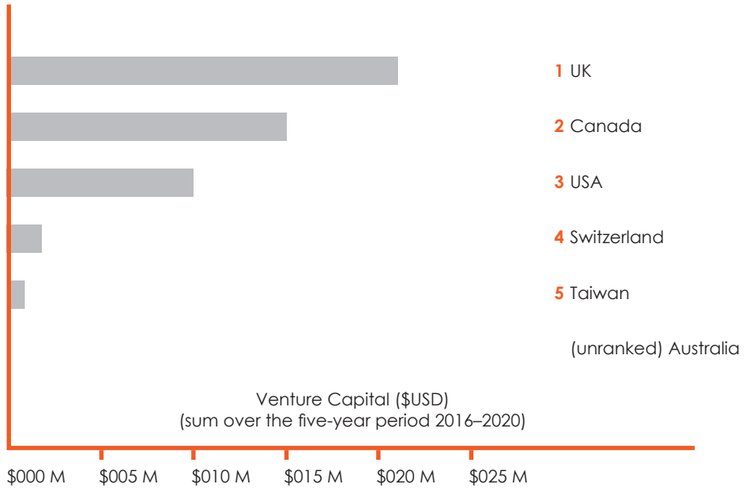
The United States has the highest research impact, with Australia ranked 19th. Total volume of published research has increased at around 33% p.a. over the 5 year period 2016–2020, with 31% of research involving international collaboration.



The research impact provides an indication of the productivity of a country or institution. Here, productivity was assumed to be represented by the volume of publications (i.e. scholarly output) as an indicator of the resources & facilities, and the level of interest in the publications as an indicator of quality

VC Investment

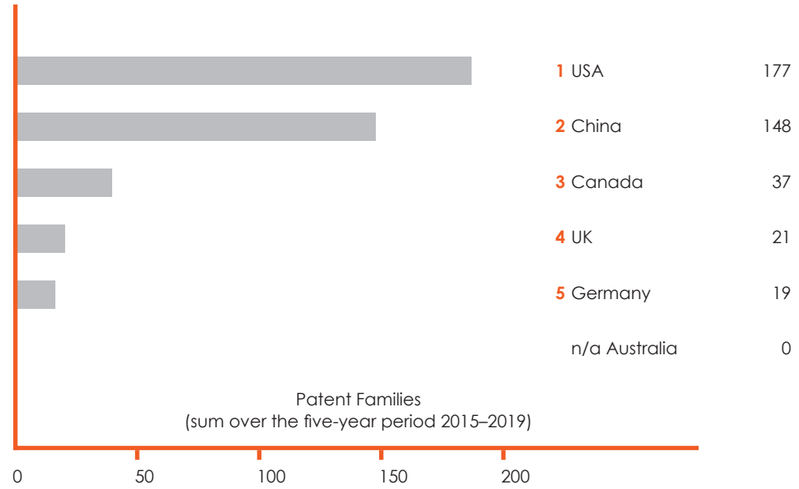
The United Kingdom has the highest venture capital (VC) investment in post quantum cryptography, ahead of Canada and the United States. Australia is unranked for VC investment in this area. Globally VC investment into post-quantum cryptography has increased by around 37% over the past 5 years.



Data from Crunchbase. The Crunchbase database provides a partial view of the global VC landscape. However the quantity, quality and richness of the data are considered to be statistically significant, and indicative of global trends.

Patents – International

Most patents for this technology were filed by applicants or inventors in the United States, slightly more than Chinese applicants or inventors. Overall patent applications have been increasing at 40% annually since 2015. There have been no patent filings originating from Australia for this technology.



Research Institutions – International

The European Union has 7 of the top 10 international institutions for research impact, with Netherlands alone holding 3. The United States has 2 institutions.

Rank	Top International Institution	Research Impact
1	Radboud University Nijmegen | Netherlands	382
2	University of Waterloo | Canada	327
3	Eindhoven University of Technology | Netherlands	259
4	Microsoft USA | United States	257
5	Centrum voor Wiskunde en Informatica | Netherlands	253
6	Florida Atlantic University | United States	198
7	French National Centre for Scientific Research (CNRS) | France	195
8	Institut national de recherche en informatique et en automatique | France	165
9	Ruhr University Bochum | Germany	155
10	Technische Universität Darmstadt | Germany	151

Research Institutions – Australia

Australia has limited research capability in this area, based on the research impact derived from publically available information. Monash University has the highest research impact, but there are no institutes in the top 50. Only 8 Australian institutes had publically available information to calculate research impact.

Rank	Top Australian Institution	Research Impact
1	Monash University	44
2	University of Wollongong	20
3	University of Adelaide	15
4	CSIRO	8
5	Queensland University of Technology	6
6	Swinburne University of Technology	2
7	University of Technology Sydney	2
8	University of New South Wales	1

Patents – Australia

There are no patents filed in Australia by Australian applicants identified for this technology.