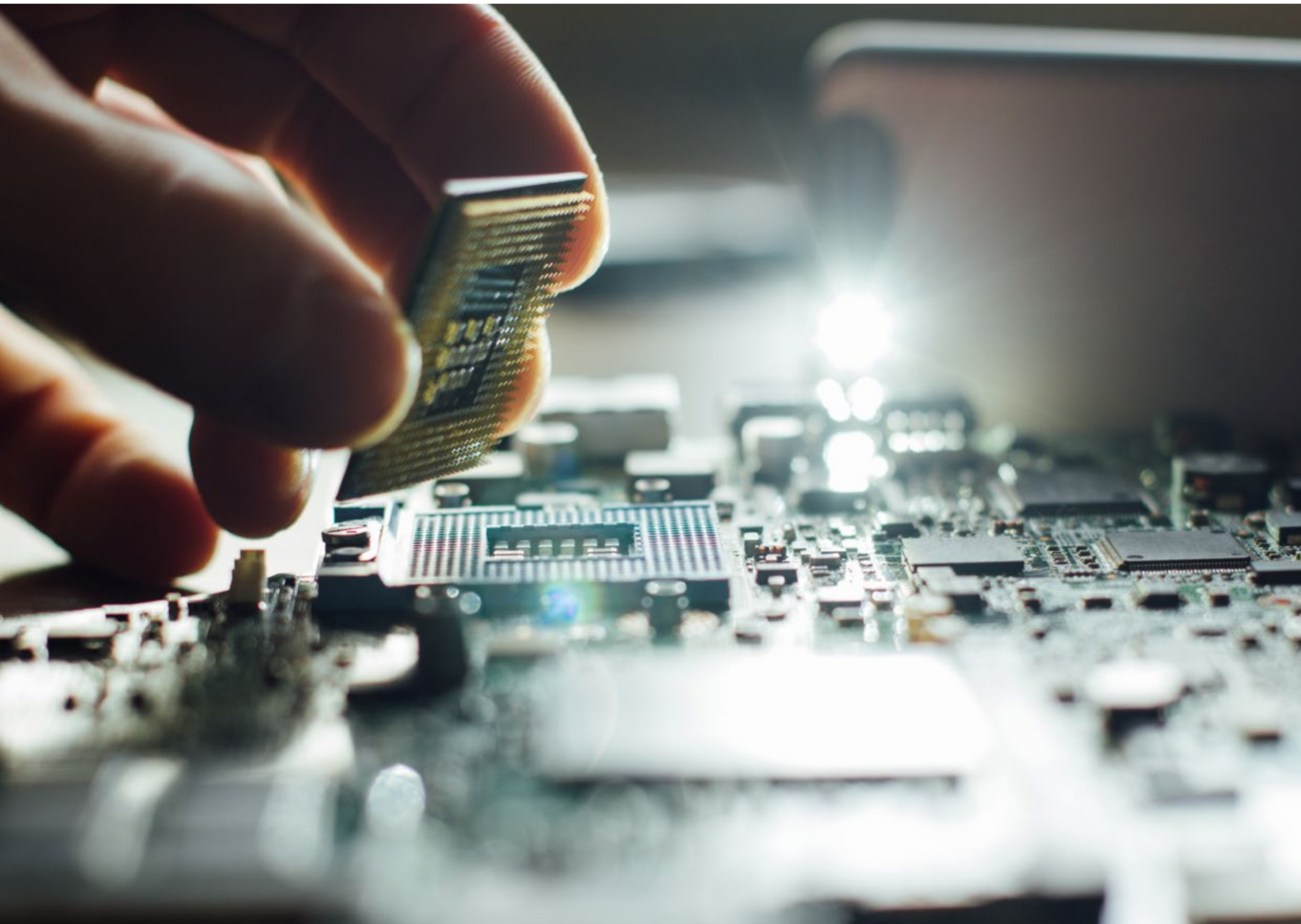
Australia's National Science Agency

The quantum threat to cybersecurity: Looking through the prism of post-quantum cryptography

New cryptography today for quantum-security tomorrow

2021



Citation

Galbraith S, Liu D, Nepal S, Ruj S, Pieprzyk J, Liu J, Steinfeld R, Sakzad A, Esgin M, Kuchta V, Susilo W, Plantard T & Dung D. 2021. The Quantum Threat to Cybersecurity: Looking Through the Prism of Post-Quantum Cryptography. CSIRO: Canberra, Australia.

Copyright

Important disclaimer

CSIRO advises that the information contained in this publication comprises general statements based on scientific research. The reader is advised and needs to be aware that such information may be incomplete or unable to be used in any specific situation. No reliance or actions must therefore be made on that information without seeking prior expert professional, scientific and technical advice. To the extent permitted by law, CSIRO (including its employees and consultants) excludes all liability to any person for any consequences, including but not limited to all losses, damages, costs, expenses and any other compensation, arising directly or indirectly from using this publication (in part or in whole) and any information or material contained in it.

CSIRO is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document please contact csiro.au/contact.

Acknowledgments

This whitepaper has been prepared by a Trans-Tasman cybersecurity research project on “Post-Quantum Cryptographic Schemes” funded by MBIE (NZ), and CSIRO (Australia). We would also like to acknowledge the contributions made by researchers from the following institutions: University of Auckland, CSIRO’s Data61, Monash University, University of Queensland, and University of Wollongong.

Contents

Executive summary

Cryptography has become a foundational tool in providing security to Internet-based digital systems. It has enabled many modern digital services in cyberspace that we take for granted. Many of these digital systems rely on public-key cryptosystems, which are based on hard computational problems in mathematics. Advances in quantum computing present potentially efficient solutions to these hard problems. Hence, current public-key cryptosystems relying on the hardness of such mathematical problems are not quantum-safe.

There is now an urgent need to develop cryptosystems that can both run on current computing devices and be incorporated into existing internet protocols, while at the same time withstand an attacker with a quantum computer. Post-quantum cryptography (PQC) offers the potential to develop such systems. However, current post-quantum systems are not simple “drop-in” replacements for existing “pre-quantum” algorithms. This makes it difficult to migrate to post-quantum cryptography, and transform our digital systems to quantum-safe.

This report presents challenges that quantum computing poses to public-key cryptography, Internet protocols that use such cryptographic primitives, and in turn to the Internet-enabled digital systems and services. We showcase recent efforts by Australia/NZ researchers and practitioners in PQC. We also explore opportunities for Australia and New Zealand to develop domestic quantum-safe cyber security technology and success stories, perform assessment of the strengths and challenges of the two nations in PQC, and provide recommendations to achieve excellence in this area. As Australia and New Zealand focus on building capability in quantum technology, post-quantum cryptography capability should be developed simultaneously.

Cryptography

Cryptography is the technique of converting plain-texts into random-looking strings that are only readable to the intended recipients or that provide authentication of senders and integrity of messages.

There are two main forms of cryptography.

- Symmetric Key Systems: In these systems, both sender and receiver are required to hold the same secret key.
- Asymmetric or Public-Key Systems: A user here is allowed to make an encryption key public while keeping their decryption key secret. Public key systems also enable digital signatures.

Each type of cryptography has its strengths and weaknesses, and so large-scale systems usually use a combination of both approaches. In particular, symmetric key crypto is usually used to encrypt (and ensure integrity) of large volumes of data, while public-key cryptography is used for key management and authentication (digital signatures).

Almost all public key cryptosystems currently being used (such as RSA and ECC) rely on the difficulty of two mathematical problems: integer factoring, and elliptic curve discrete logarithms. These systems have been studied intensively for at least the last 30 years and have held up well in the face of sustained public scrutiny and mathematical analysis.

Secure internet-enabled digital systems

The field of cryptography is central to information security. It provides the main security building blocks of privacy and authentication/access control. Major examples of systems enabled by cryptography include TLS, secure email (i.e. S/MIME), private messaging (such as Signal and WhatsApp), e-commerce, cloud storage and computing, VPN, automatic software updates, e-voting, Internet of Things (IoT), blockchain, digital currencies, smart contracts, and many more.

Particularly, TLS (Transport Layer Security) enables HTTPS, the secure Internet protocol supported by most websites in our society, such as https://www.australia.gov.au/ and https://www.govt.nz/. Whenever a user accesses such websites supporting HTTPS, the web browser of the user (i.e., the client) and the website server execute the Transport Layer Security (TLS) protocol. In a nutshell, TLS has two main phases: (i) a handshake protocol and (ii) a record protocol. In the initial handshake protocol, the client and the server establish the "ground rules" for the communication and a secret key to be used to encrypt transmitted messages. For this key agreement, the protocol relies on asymmetric cryptography as the two parties do not have a shared secret at that point. Once the key agreement has been performed and a shared secret key is established between the two parties, the communication can now be secured using symmetric-key cryptography, which is more efficient than asymmetric cryptography. The record protocol is the phase where the client and the server exchange encrypted messages as needed.

More generally, a hybrid system is always employed for information security purposes. That is, the communicating parties first use more costly asymmetric cryptographic techniques to establish a shared symmetric key, which is then used to secure the communication using symmetric cryptographic techniques such as the well-known AES algorithm. When the asymmetric cryptographic techniques are not quantum-safe, leading to broken shared symmetric keys, the symmetric cryptography in hybrid systems can no longer be secure, either.

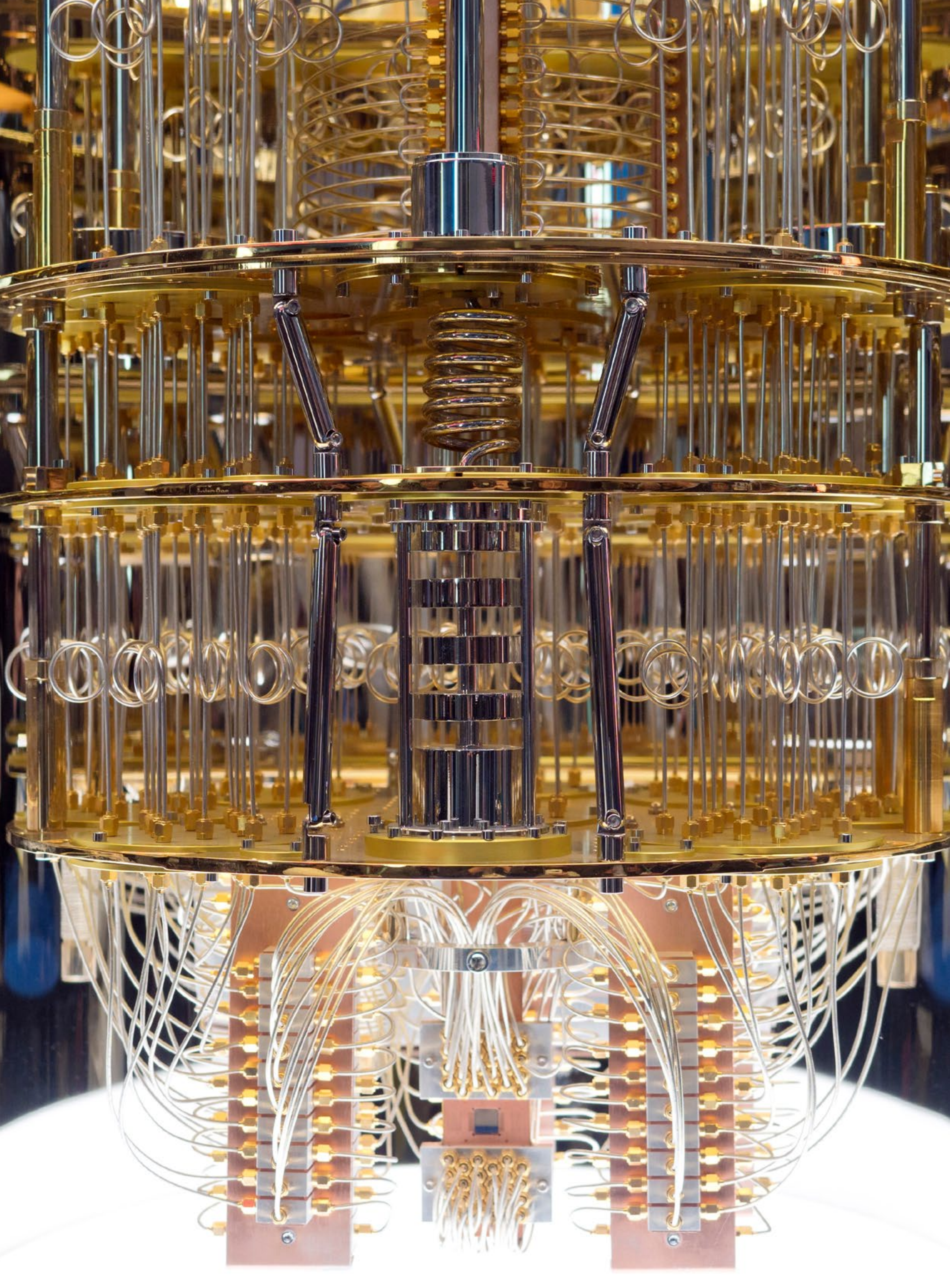
Quantum computing

Quantum computing is a new model of computing that replaces a binary state (which can be either zero or one) with a “qubit”, which is a superposition of both bits zero and one. Qubits exhibit unusual properties that make them attractive for both communication and computing. They cannot be copied (according to the no-cloning theorem) and any measurement converts them into classical bits. These characteristics have been used by Bennett and Brassard to design their famous quantum key distribution (QKD) protocol. It enables two communicating parties to establish a common and secret cryptographic key. The secrecy of the key is perfect (i.e. to get a key, an adversary has no better chance than by guessing it).

On the other hand, a word of n-qubits represents an exponential number (i.e. 2^n) of possible binary strings. This means that, in principle, a quantum computer may offer exponential speedup. Unfortunately, there are many hurdles. The fundamental one is the extraction of a requested outcome from a quantum output (that after any measurement becomes classical). A fast evolving theory of quantum algorithms addresses this problem. A typical approach relies on designing an algorithm that produces a quantum output with a biased probability distribution so after a few measurements, it is possible to obtain the requested outcome.

One of crucial technical obstacles in making quantum computing a reality is stability of qubits. This leads us to the problem of implementation of logical qubits (that are stable and control potential errors) from physical qubits (that are error-prone). In general, to construct a logical qubit, it is necessary to use a collection of physical qubits together with an appropriate error correcting infrastructure. How to design such an infrastructure is an active area of research. IBM plans to develop the 127-qubit IBM Quantum Eagle in 2021 which “will allow us to implement the heavy-hexagonal error-correcting code that our team debuted last year, so as we scale up the number of physical qubits, we will also be able to explore how they’ll work together as error-corrected logical qubits – every processor we design has fault tolerance considerations taken into account.” The plan for 2022 includes a 433-qubit IBM Quantum Osprey system and for 2023, the 1,121-qubit IBM Quantum Condor processor. Their announcement says “We think of Condor as an inflection point, a milestone that marks our ability to implement error correction and scale up our devices.”

The current main progress in quantum computing is being led by tech giants such as Google, IBM, Microsoft, DWave and others. It is also safe to assume that governments of major nations are also developing quantum computers. This does not mean that the risk to business may be low, as the business model followed by Google, IBM and others is to offer quantum computing as a software service. There is substantial research in quantum computing in Australia, such as the ARC Centre of Excellence for Quantum Computation and Communication Technology (CQC2T). For a full survey of strengths and opportunities of quantum computing in Australia and New Zealand see these surveys [3, 4].



Quantum threat to cybersecurity

The security threat from quantum computers is triggered by the invention of Shor's algorithm, which requires an appropriately general-purpose quantum computer, and efficiently solves the two problems underlying almost all currently used public-key cryptosystems, namely integer factoring, and elliptic curve discrete logarithms (ECDLP). The first implementation of Shor's algorithm (which produced the factorisation 15 = 3 * 5) took place in 2001. In 2020, after almost 20 years of progress, IBM produced a 65 (physical) qubit machine.

Hence, if large-scale general quantum computers can be built then we immediately lose all security for the current public-key cryptosystems that are widely used to secure a wide range of systems. With quantum computing as a software service offered by tech giants, any entity will be able to employ these services to break any public-key cryptosystem of interest. On the other hand, the impact of quantum computers on symmetric cryptography is less extreme, but still potentially requires some adjustments to their use (mainly, increasing key sizes), due to Grover's quantum search algorithm which can perform a brute-force search over all 2^n possible n-bit keys in just $2^{n/2}$ amount of time.

Researchers have been estimating the number of logical qubits needed to solve instances of the ECDLP using Shor's algorithm on a fault-tolerant quantum computer as well. Some notable papers on this topic include:

- Roetteler, at al. [13] considered quantum circuits for elliptic curve exponentiation as required to run Shor's algorithm. Their analysis for elliptic curves over prime fields of size around 256-bits are that the implementation would require 2,338 qubits, $1.26 * 10^{11}$ Toffoli gates and $1.16 * 10^{11}$ Toffoli depth. (The Toffoli gate is also known as the controlled NOT gate, and is a fairly simple universal reversible logic gate which is commonly used by theoretical researchers to estimate the cost of a quantum computation). These figures are reproduced in Table 9.2 of the extensive report [2] by the German Federal Office for Information Security (BSI).
- In a very recent work [8], Haner et al. have revisited these calculations. As well as giving some improvements to the circuits, they consider different trade-offs that are appropriate for different measures of cost. For elliptic curves over 256-bit prime fields, they can reduce the number of qubits from 2,338 to 2,124. Alternatively, they can reduce the number of Toffoli gates to $1.08 * 2^{31} \approx 2.3 * 10^9$ gates and the Toffoli depth to $1.12 * 2^{24} \approx 1.9 * 10^7$ (but this now needs 2,871 qubits).

A survey and report has been conducted by Mosca and Piani for the Global Risk Institute [9]. In particular, they have surveyed a wide range of experts to determine estimates for when quantum computers will be a "significant threat" to public-key cryptography. The majority of experts believe the risk is low (less than 5 percent) for the next 5-10 years, though this still does not exclude the possibility of a breakthrough. Looking ahead 15 years, about half the responders consider the risk to be at least 50 percent. By this measure, a reasonable recommendation would be to migrate to post-quantum cryptography within the next 10 years. Given the standardisation and development cycle for security products, it means we need to be acting with urgency now.

Some experts [16], recommend having a sufficiently long period between the point in time when the cryptosystem ceases to be used and the point in time when the cryptosystem becomes susceptible to practical quantum attacks. This is because the encrypted information may be recorded and archived for decryption in the future. Therefore, if information we need to protect is to remain encrypted for 15 years, then we must stop using asymmetric schemes at least 15 years before quantum computers will become available to the adversaries.

Not all experts think the risk is immediate. For example, the BSI commissioned a report in 2018 on the current state of quantum computers. The report concluded "At this point in time, quantum processors that have been realised are far from those needed to attack cryptography". The report was updated in 2020, but the conclusions remain the same. In a lecture at the PQCrypto conference in late 2020, Frank Wilhelm-Mauch (one of the authors of the report) speculated that quantum computers will stay at the 50-100 qubit range for the near future, while researchers focus on controlling the errors. On the other side, in 2020, IBM announced a roadmap for scaling quantum technology with the main target to achieve a 1,000-plus qubit device by the end of 2023. Even though a 1,000-qubit quantum computer would be a significant milestone in the development of quantum computers, it would still be 1,000 times too small to fulfil a full-fledged quantum computer, IBM researchers say. Nevertheless, the BSI are actively working on post-quantum cryptography and are promoting the adoption of post-quantum systems for high-security applications.

Post-quantum cryptography

The defining feature of post-quantum public-key cryptography, compared to the older pre-quantum generation of quantum-insecure public-key cryptography, is that the former uses for its security different intractable mathematical problems that are believed to stay intractable even for quantum computers. This allows the design of new cryptosystems that can still be run on existing (non-quantum) computing hardware, but resist quantum computing attacks.

There are two general approaches to design of post-quantum cryptosystems. The first approach looks at mathematical objects with less algebraic structure than those used in pre-quantum generations of public-key cryptography; examples include multivariate polynomial systems, hash trees, non-abelian groups, and isogenies. The second approach makes use of "noise" to disrupt exact algebraic equations- examples include lattices and codes. These systems are being actively studied by the academic community, and results are shared at international research conferences in cryptography such as the annual conference PQCrypto on Post-Quantum Cryptography, as well as the annual CRYPTO, EUROCRYPT and ASIACRYPT conferences organised by the International Association for Cryptologic Research (IACR).

There are pockets of excellence in post-quantum public-key cryptography in Australia and New Zealand, in particular at Monash University, University of Wollongong, CSIRO's Data61 and University of Auckland. These groups have developed novel cryptographic protocols and primitives which include post-quantum public-key encryption algorithms, post-quantum signature schemes, lattice-based privacy-preserving authentication and 'zero-knowledge' proof protocols, among others. These groups have also made contributions to understanding and quantifying the security foundations of the intractable problems underlying post-quantum cryptosystems, such as the hardness of problems on structured lattices and on isogenies.

Worldwide, post-quantum cryptographic systems are being standardized. Current standardisation initiatives include the following:

- The US National Institute of Standards and Technology (NIST). The NIST Post-Quantum Cryptography Standardization process [11]. This was launched in 2016 with an open call for algorithms to be submitted and reviewed in a public competitive process. The initial round attracted 69 submissions. The goal is to standardize one or more public-key encryption and key-establishment algorithms, and one or more digital signature algorithms.
- Among the original submissions were several involving authors in Australia, including: DRS (a lattice based signature proposed by Thomas Plantard and Willy Susilo at Wollongong, and their co-authors), Odd Manhattan (a lattice based key encapsulation mechanism by Thomas Plantard at Wollongong), Titanium (a lattice based Public-key Encryption and KEM by Ron Steinfeld, Amin Sakzad and Raymond K. Zhao at Monash), and Compact-LWE (by the CSIRO's Data61 team, extended to Compact-LWE-MQ^H recently).
- Currently the NIST project is in the third round, comprising 7 finalists and 8 alternate candidates. The final standard is expected to be produced in 2022 or 2023.
- European Telecommunications Standards Institute (ETSI) Quantum-Safe Cryptography (QSC) working group. This group aims to assess and make recommendations for quantum-safe cryptographic primitives protocols and implementation considerations, such as the paper [6]. It is not developing new algorithms.
- The International Organization for Standardization (ISO). This body is currently engaged in preparing for the standardisation of Quantum-Resistant Cryptography in ISO/IEC JTC1 SC27. It is not developing new algorithms.
- The German Federal Office for Information Security (BSI). This agency is developing recommendations for German government and industry for migration to post-quantum cryptography. It is not developing new algorithms.

Currently there is no single post-quantum system that has the same performance across all measures (key size, message size, speed) as the state of the art for pre-quantum systems. Hence the development and refinement of post-quantum cryptography is an active international research effort. We discuss some of the challenges to adopting PQC in the next section.

Challenges of migration to post-quantum cryptography

The PQC schemes under standardisation provide the same interfaces for cryptographic operations as the current public-key schemes. However, this does not mean that the deployment of new PQC schemes can be a simple replacement of the existing ones. For the migration, there are multiple challenges, either administrative or technical.

Legacy Issues. Public-key cryptography has been widely deployed in various systems for authentication, key management, access control, identity management, data integrity protection, etc. Given the large number of computing devices and the complexity of devices, it is hard to know exactly where public-key cryptography has been deployed. For devices that have been operating for a long period of time, the manufacturers of the devices might no longer exist and there might be no source code for such devices.

Interoperability. Cryptographic protocols implement secure communication among two or more computing devices. To enable the correct communication, the public-key cryptography underlying such protocols must be the same or compatible. Otherwise, the messages encrypted or signed by one device cannot be accepted by other devices. The devices might belong to different parties and they must coordinate and ensure all their devices are upgraded with compatible PQC schemes to benefit from security of PQC schemes. This is why international standards are necessary. There may need to be a transition stage where systems have to be able to operate with pre-quantum and post-quantum cryptosystems depending on the abilities of their communication partner.

Performance versus Security. PQC schemes and current public-key schemes have very different performance characteristics in terms of ciphertext/signature size, key size, processing time, and memory usage. As an example, the key and signature of CRYSTALS-Dilithium in NIST Round 3 can be more than one or two thousand bytes, compared with tens of bytes of the current ECDSA scheme. The performance change of cryptographic operation will affect the performance of whole systems; particularly for real-time systems like remote medical systems. The effect of this performance change needs case by case analysis. Further, it is not clear whether the big keys and ciphertexts of the new PQC schemes can even fit into packet formats of current communication systems without major re-design.

Diversity of PQC Schemes. Multiple PQC schemes of the same kind (encryption or signature) could be standardized by NIST. The requirement of multiple PQC schemes is partially due to the quite different performance characteristics and security consideration of different schemes. They have big keys with short ciphertexts/signatures, or short keys with big ciphertexts/signatures. They can find their suitability in different application scenarios. Thus, users need to analyze their particular requirements to determine which PQC schemes should be adopted. Moreover, a computing device might run applications with heterogeneous requirements, and then it is harder to make a selection of PQC schemes.

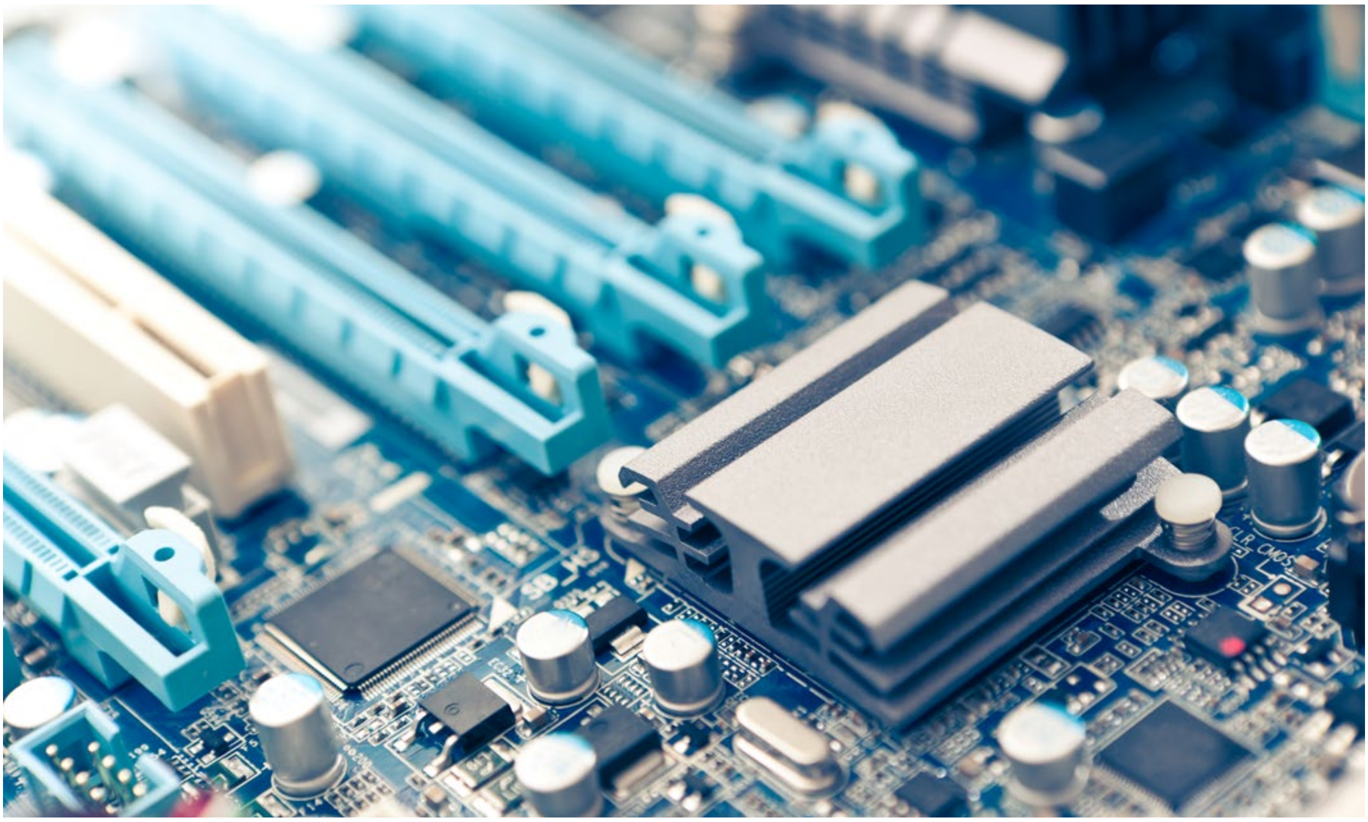
Limited Implementations. PQC schemes are relatively new and there are few implementations available for different platforms or languages. A developer might not have suitable PQC software libraries for the programming languages being used for software development. It is challenging to securely implement PQC schemes even for cryptographic experts. There is also a shortage of knowledge about how to use hardware to accelerate PQC schemes.

Industry and application areas vulnerable to quantum attacks

Attacks leveraging quantum computing poses a threat to any industry or application area that has digitalized their businesses and services. In Australia and New Zealand, the following industry and application areas are more vulnerable to quantum attacks, since they involve major cyberspace activities in the countries.

- Banking and finance industry underlies normal daily operations of corporate businesses, individual life, and the whole society. Financial transactions, such as money transfers between banks and their customers over Internet, must be securely protected. They are protected currently with traditional public-key cryptographic schemes and protocols, which are vulnerable to quantum attacks.
- Critical infrastructure, such as power grid systems, are important for national security. An established critical infrastructure usually has a long life span. Public-key cryptographic schemes were deployed to protect the infrastructure long ago when the infrastructure was constructed. These will be vulnerable to newly crafted attack methods, including attacks with quantum computers.
- Mining, manufacturing, oil and natural gas in the Industry 4.0 relies on networked operational technology (OT) to monitor and control physical devices like mining robots and processes in factories. Attacks to such networked devices and processes can be fatal. Traditional public-key encryption enabling secure remote operations of devices is an attractive target to attack with quantum computers.
- Governments are providing more and more digital services to citizens over Internet, with secure connection provided in TLS over traditional key exchange mechanisms and public-key cryptographic schemes. Moreover, if a global incident like a pandemic shuts down cities and offices, their staff may need to work remotely via secure connections built with Virtual Private Network (VPN) technology. All such connections secure for current classic computers will be vulnerable to quantum attacks.

In addition to the above mentioned application areas, other areas like defense industry, retail industry, and small-medium enterprises in supply chain are also vulnerable to quantum attacks, because they generate sensitive information or they are not well equipped in terms of technology and funding to defend against quantum attacks.



Future perspectives

As already mentioned, if one has a system that requires data to remain private for a long time then one should consider urgently migrating to post-quantum encryption schemes. This is because the development time to bring new tools to market is long. As an intermediate step one might also consider "hybrid" schemes, which combine both pre-quantum and post-quantum cryptography.

The situation with authentication systems is a little different. For many (but not all) applications of digital signatures it is acceptable to continue using elliptic curve public key signatures until such time as there is a realistic threat that the ECDLP can be solved using a quantum computer.

Nevertheless, government and commercial organisations should be thinking about their security needs and risk management, and planning for when they may need to move to post-quantum cryptograhy. Organisations need to invest in reviewing their systems. As stated in [1] it is "difficult to determine where and with what priority post-quantum algorithms will need to replace the current public-key systems. Tools are urgently needed to facilitate the discovery of where and how public-key cryptography is being used in existing technology infrastructures".

There is currently a strong trans-Tasman project working on post-quantum cryptography, that includes researchers from CSIRO's Data61, Monash University, University of Wollongong, University of Auckland, University of Canterbury, University of Queensland, and others. The project will examine a broad range of urgent issues surrounding the impact of quantum computers in practice, and the development of post-quantum cryptosystems. It will determine the implications of quantum computing and post-quantum cryptography for current security tools and systems, particularly in the New Zealand and Australia context. It will investigate the security and efficiency of post-quantum cryptosystems, and contribute critical new knowledge to the field of post-quantum cryptography.

Post-quantum cryptography is a new and emerging field and presents Australia and New Zealand with significant opportunities. Our team of experts will position Australia and New Zealand as leaders in the field, by developing a critical knowledge-base within New Zealand and Australia, and by training the next generation of experts in this field. Finally, the foundational research and new intellectual property in cryptography created via this project will have the potential for future commercialisation.

Further reading

For readers who wish to get a deeper understanding of the challenges and opportunities of post-quantum cryptography, we strongly recommend these other whitepapers and documents.

- NIST whitepaper "Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms" [1].
- ETSI whitepaper "Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges" [6].
- US National Academies of Sciences, Engineering, and Medicine, "New Cryptography Must Be Developed and Deployed Now, Even Though A Quantum Computer That Could Compromise Today's Cryptography Is Likely At Least A Decade Away" [10].
- Thales, "Cryptography for a Post-Quantum Era" [14].
- Ericsson report "What Next in the World of Post-Quantum Cryptography?" [5].
- Research and Markets Revenue Assessment 2020 "Quantum Supremacy - Progress and Controversy in the Past Year and Likely Timetable" [12].
- Computing Community Consortium, "Identifying Research Challenges in Post-Quantum Cryptography Migration and Cryptographic Agility" [15].
- PQShield, "Understanding the Quantum Threat, Post-Quantum Cryptography and the Upcoming NIST Standards" [17].
- Cloud Security Alliance, "Confidence in Post Quantum Algorithms" [18].
- ENISA, "Post-Quantum Cryptography: Current state and quantum mitigation" [19].

References

1. William Barker, William Polk and Murugiah Souppaya (2020) Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms. https://csrc.nist.gov/publications/detail/white-paper/2020/05/26/getting-ready-for-post-quantum-cryptography/draft

2. Federal Office for Information Security, Bonn, Germany (2020) Status of quantum computer development, Version 1.2.

3. Wayne Crump (2019) Quantum Computing. Office of the Prime Minister's Chief Science Advisor, Kaitohutohu Matanga Putaiao Matua ki te Pirimia, New Zealand.

4. CSIRO Futures (2020) Growing Australia's Quantum Technology Industry. CSIRO, Australia.

5. Ericsson (2020) What next in the world of post-quantum cryptography? https://www.ericsson.com/en/blog/2020/3/post-quantum-cryptography-symmetric-asymmetric-algorithms

6. ETSI White Paper No. 8 (2015) Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges. http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

7. IBM (2020) IBM roadmap to quantum computing. https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/

8. Thomas H¨aner, Samuel Jaques, Michael Naehrig, Martin Roetteler and Mathias Soeken (2020) Improved Quantum Circuits for Elliptic Curve Discrete Logarithms. PQCrypto 2020.

9. Michele Mosca and Marco Piani (2019) Quantum Threat Timeline. Global Risk Institute, https://globalriskinstitute.org/publications/quantum-threat-timeline/

10. US National Academies of Sciences, Engineering, and Medicine (2018) New Cryptography Must Be Developed and Deployed Now, Even Though A Quantum Computer That Could Compromise Today's Cryptography Is Likely At Least A Decade Away.

11. NIST (2021) Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography

12. Research and Markets (2020) Post-Quantum Cryptography (PQC) Revenue Assessment 2020: Quantum Supremacy - Progress and Controversy in the Past Year and Likely Timetable.

13. Martin Roetteler, Michael Naehrig, Krysta M. Svore and Kristin E. Lauter (2017) Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms. ASIACRYPT 2017.

14. Thales (2018) Cryptography for a post-quantum era.

15. Computing Community Consortium (2018) Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility. https://cra.org/ccc/wp-content/uploads/sites/2/2018/11/CCC-Identifying-Research-Challenges-in-PQC-Workshop-Report.pdf

16. Craig Gidney, Martin Ekera (2019) How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. https://arxiv.org/pdf/1905.09749.pdf

17. PQShield White Paper Series (2021) Understanding the quantum threat, post-quantum cryptography and the upcoming NIST standards. https://pqshield.com/quantum-threat/

18. Cloud Security Alliance (2021) Confidence in Post Quantum Algorithms. https://cloudsecurityalliance.org/artifacts/confidence-in-post-quantum-algorithms/

19. ENISA (2021) Post-Quantum Cryptography: Current state and quantum mitigation. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

As Australia's national science agency and innovation catalyst, CSIRO is solving the greatest challenges through innovative science and technology.

CSIRO. Unlocking a better future for everyone.

Contact us
1300 363 400
csiro.au/contact
csiro.au

For further information
Dr Surya Nepal
Senior Principal Research Scientist
Surya.Nepal@data61.csiro.au
www.data61.csiro.au

B&M | 21-00107