Report on cybersecurity risks and opportunities of quantum computing to industry in New Zealand and Australia
September, 2023

Executive summary

The purpose of this report is to provide government and industry with a better understanding of cybersecurity risks to various business sectors in Aotearoa New Zealand if large-scale quantum computers become available.

Cybersecurity risks to organisations include e-crime, attacks from nation states, and hacktivism. All organisations and all business sectors are vulnerable to cybersecurity risks. Defense against these risks involves a number of tools and technologies, one component of which is public key cryptography. Quantum computing is an entirely different paradigm of computing to traditional computing. Quantum computing allows to solve certain problems, including breaking public key cryptosystems, much more efficiently than a traditional (classical) computer can.

Post-quantum cryptography is based on mathematical problems that are believed to be intractable even for quantum computers. It allows the design of new cryptosystems that can still be run on existing (non-quantum) networks and computing hardware, but resist quantum computing attacks. But post-quantum cryptography can be less practical and efficient than current systems, and the process of migration to using new technology is slow, typically 5-10 years.

The main attack surface for quantum computing is the network protocols, operating systems, and cloud systems that are ubiquitous in modern IT. Most businesses and organisations in NZ use products and tools from trusted vendors, who can be expected to upgrade to use post-quantum cryptography when appropriate. Hence, the main sources of cyberattacks in practice will continue to be weak passwords, phishing, denial-of-service attacks, insider attacks, malware, ransomware, spyware, zero-day attacks, Java code injection, SQL injection, side channels, supply chain attacks, etc. Quantum computing has no impact on these sorts of attacks. Hence, the day-to-day cybersecurity challenges in a post-quantum world will be much the same as they are now.

Our main conclusion is that NZ business and industry does not have to be too concerned at the moment about the specific cybersecurity threat of quantum computing. Instead they can maintain their focus on the many and varied existing cybersecurity issues that they face daily. However, there are two caveats to this: (1) Organisations that collect and store data that needs to be confidential for very long timescales compared to average businesses may need to consider the risks of “harvest now and decrypt later” attacks. For example, personal health data should be considered carefully in this context. (2) Organisations should determine whether they have security-critical computer systems that are connected to networks and using cryptography, but that are hard to maintain/upgrade.

The above conclusion should not be interpreted as a validation of the current state of cybersecurity in NZ. Indeed, there are many very serious risks and challenges to cybersecurity at the moment, and greater awareness of cybersecurity in organisations and the wider public is necessary.

In summary, most NZ businesses and industries do not need to consider the threat of quantum computing. However, there are some sectors that do need to plan ahead for this, and they should begin risk assessments and planning now. These sectors are those that collect and store data that needs to be confidential for very long timescales (e.g., health data), and those who have a great complexity of computer systems and devices that are hard to maintain and upgrade.

Authorship and acknowledgements

This report is produced by a research project led by Professor Steven Galbraith at the University of Auckland and funded by the New Zealand Ministry of Business, Innovation and Employment (MBIE) under the project UOAX1933 Cyber Security Research Programme - Post-quantum cryptography. Assistance was given by Shalini Banerjee.

Methodology of the review and scope of the report

One objective of the MBIE funded research project was to understand the implications of quantum computing and post-quantum cryptography for current security tools and systems in the NZ/Australia context. To complete this objective we agreed to conduct a review of cybersecurity risks and opportunities associated with quantum computing and post-quantum cryptography within the NZ/Australia context, and to identify which industries and/or application areas are most vulnerable to attacks leveraging quantum computers. The purpose of the report is to provide a better understanding of risks to various business sectors in NZ and Australia if large-scale quantum computers become available.

A survey was conducted of selected companies and organisations in NZ. The goals of the survey included:

- To determine the level of awareness of the possible impacts of quantum computing on security.
- To identify which industries and/or application areas in NZ would be most vulnerable to attacks leveraging quantum computers.
- To determine how easy it would be to integrate post-quantum cryptography into existing systems, and to determine any consequences to usability.
- To investigate possible areas for future collaboration between university researchers and industry.

The data gathered in the survey provided insights for the preparation of this review document.

The full report is provided to NZ companies and government organisations, including those who completed the survey. A shorter summary report, which does not include names or details of the organisations surveyed, will be posted on the Internet.

Disclaimer

The authors, University of Auckland, and MBIE, are not responsible for the correctness and accuracy of this report. The authors and their organisations are not liable for any losses or damages from reliance on the information in this report.

Security and Cryptography

Cybersecurity is a broad topic that covers a wide range of attacks by a wide range of attackers. It is common to categorise attacks into broad groupings such as the following (see CrowdStrike Global Threat Report[1]):

- ECrime - Financially motivated criminal activity, such as ransomware, scams and fraud.
- Targeted - State-sponsored activity that includes cyber espionage, strategic competition[2], and generating currency to support a regime.
- Hacktivist - Activity undertaken to gain visibility or publicity for a cause or ideology, or to damage an organisation that is seen to be in opposition to the cause or ideology.

Cybersecurity involves both technical and human issues. The CrowdStrike 2022 Global Threat Report writes that “62% of attacks comprise non-malware, hands-on-keyboard activity” and “The most common causes of cloud intrusions continue to be human errors such as omissions introduced during common administrative activities.”

New Zealand’s Security Threat Environment 2023 - An assessment by the New Zealand Security Intelligence Service notes that “Cyber-enabled espionage poses a significant threat to New Zealand’s national security and economic prosperity. Foreign states highly likely target New Zealand individuals, industry and government to gather information for their own economic, military or political advantage. The threat to critical national infrastructure is a particular area of concern. The impact of malicious cyber activity targeting NZ’s critical national infrastructure (such as electricity grids or telecommunication networks) would likely be significant.”

Cryptography is a set of tools to provide privacy and authentication. It underlies many secure systems, and aims to prevent attacks of the above types. For example, most connections to websites use HTTPS, which employs encryption for privacy (eg encrypting passwords and credit card numbers) and digital signatures for authenticating the domain. The TLS (Transport Layer Security) protocol enables HTTPS. Other widely-used and important protocols include SSH and IPSec. Services and applications enabled by public key cryptography and digital signatures include private messaging (such as Signal and WhatsApp), e-commerce, secure cloud storage and computing, VPN, automatic software updates, e-voting, Internet of Things (IoT), blockchain, digital currencies, smart contracts, and many more.

There are two types of encryption: Secret key encryption requires the sender and receiver to both have the same secret key. Key exchange protocols are a way for a sender and receiver to set up such a random secret key. Public key cryptosystems require the receiver to have a secret, but anyone with public information can encrypt a message.

Almost all key exchange, public key encryption, and digital signature algorithms currently being used fundamentally depend on just two computational problems: integer factoring, and elliptic curve discrete logarithms. These problems have been studied intensively for at least the last 30 years and have survived sustained public scrutiny and mathematical analysis. The integer factoring problem is the basis for RSA encryption and signatures. The elliptic curve discrete logarithm problem is the basis for ECDSA, ECDH, etc.

[1] https://www.crowdstrike.com/global-threat-report/

[2] The recent document “New Zealand’s Security Threat Environment 2023 - An assessment by the New Zealand Security Intelligence Service”, defines strategic competition as “states seeking to advance competing visions for regional and global orders”. https://www.nzsis.govt.nz/assets/NZSIS-Documents/New-Zealands-Security-Threat-Environment-2023.pdf

Quantum Computing

Quantum computing is a paradigm of computing that is completely different from the computers we are familiar with. Classical computers, such as laptops, mobile phones, and the chips in our cars and appliances, use bits (zero or one) represented in silicon (built from transistors and capacitors). Quantum computing employs quantum bits (qubits) instead of classical bits. A qubit can store a superposition of two states, which is substantially more powerful than storing just one of two values. For this, transistors no longer suffice. There are many proposals for how to represent qubits (e.g., using superconductors, trapped ions, photons, etc). In classical computing, different bits are independent of each other, but quantum computing generally requires qubits to be entangled. The notions of superposition and entanglement come from quantum mechanics.

Quantum computing is not more powerful than classical computing due to increased storage or faster processing. The key feature of quantum computing is that one can perform certain operations on qubits in a way that is different to what is possible using classical computers. This allows to solve certain problems much more efficiently using a quantum computer than a classical computer. For example, it is said that quantum computing has the potential to revolutionize areas such as drug discovery and logistics. Large tech firms such as google and IBM are developing quantum-computing-as-a-service, so it will not be necessary for individuals or organisations to build or own a quantum computer to make use of the benefits of the technology.

Shor's algorithm is based on some of the special features that are only possible with a quantum computer, such as entanglement and the Quantum Fourier Transform. Shor's algorithm breaks certain public key cryptosystems that are currently in widespread use. In particular, Shor’s algorithm efficiently solves the integer factoring and elliptic curve discrete logarithm problems. As we have already mentioned, these problems underpin the RSA and elliptic curve cryptosystems that are used in TLS, SSH, IPSec, and many more security protocols and systems. Therefore Shor's algorithm breaks all these algorithms, and with them all the public-key cryptography mechanisms deployed on the Internet.

Quantum Risk

For a number of technical reasons, current quantum computers are not powerful enough to break the security systems being used today. In short, they cannot process enough data (i.e., they do not have enough qubits to store large enough numbers) and they cannot yet accurately perform the operations required (due to issues of decoherence that need to be solved using error-correction). The challenge for quantum computing, at least in the context of breaking cryptography, is to construct a large-scale and error-tolerant quantum computer on which Shor’s algorithm can be performed to break the public keys currently in use on the internet. Some researchers claim that such a computer may be available in as little as 5-10 years, but others are more cautious in their predictions of the development of quantum computing.

If a large-scale quantum computer becomes available in 10 or 20 or 30 years, what will an attacker be able to do? They will be able to read messages sent using secure end-to-end encrypted messaging systems like Signal. They will be able to spoof webpages and hence steal user data without resorting to phishing. They will be able to bypass the security checks on software updates, and hence install malware on systems without having to trick users into clicking a link.

Most critically for some government agencies and institutions, an attacker with a large-scale and error-tolerant quantum computer will be able to decrypt private communications from decades in the past. Suppose an attacker today (or already in the past) intercepts files from your organisation that are encrypted using public key cryptography, or with secret keys from an RSA or elliptic curve key exchange protocol. Are there consequences if those files are decrypted in 10 or 20 or 30 years time?

As already mentioned, it will not be necessary for the attackers to build or buy their own quantum computer, since the computing resource will be available as quantum-computing-as-a-service. However, it is known that the large nation states are all investing heavily in quantum computing.

Post-Quantum Security

Since large-scale and error-tolerant quantum computers would seriously compromise the confidentiality and integrity of digital communications on the internet and elsewhere, it is necessary to consider alternatives to the current systems. It has been recognised for the last 5-10 years that there is an urgent need to develop cryptosystems that can be used today on current computing devices and be incorporated into existing internet protocols, while at the same time withstand an attacker in the future with a quantum computer. The field of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can operate with existing computing devices, communications protocols and networks. Using post-quantum cryptography, we can use today's computers to protect our information against a quantum attacker in the future.

The US National Institute of Standards and Technology (NIST) is currently standardizing post-quantum cryptosystems that will be recommended for future use[3]. Similar standardization processes are being conducted by other standards bodies internationally. The timeline for large-scale quantum computers could be anywhere from 5 to 50 years, but many government and industry groups are preparing for the post-quantum future and will begin using the new protocols as soon as the final NIST standards are written. Indeed, starting from August 2023 the chrome browser supports the X25519Kyber768 hybrid post quantum key exchange for TLS[4].

It is worth noting that post-quantum cryptosystems are typically less efficient than current systems, either in terms of bandwidth/storage or in terms of execution time/computing power required, or both. Hence the migration to post-quantum cryptography may cause some inconvenience to some businesses and users.

Post-quantum cryptography will gradually be implemented and supported in a wide range of products and systems. As an example of how this will work in practice, let us recall the TLS handshake process used in secure internet protocols. During a TLS handshake, the client and server exchange messages that, among other things, list the cipher suites each of them supports. If both systems have been upgraded to support post-quantum cryptosystems, then the session will be secure against a quantum attacker. But if one system is poorly maintained or is not powerful enough to support the new protocols, then the handshake will default to use weaker legacy systems. This opens the door to TLS downgrade attacks. As always, a system is only as secure as its weakest component.

Results of our Survey

We conducted a survey in mid-2023 of selected companies and organisations in NZ to determine the awareness and scale of cybersecurity risks from quantum computing. The survey was emailed to certain mailing lists of NZ cybersecurity practitioners in industry (mainly CISOs etc). The

[3] https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[4] https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html

completion rate was low (just 5 responses). The results of the survey were augmented with interviews and discussions with attendees at the 2023 NZ ICS/OT Cybersummit, some of whom were from Australia, and with some other NZ-based cybersecurity practitioners known to the authors. Overall, the survey gathered input from a variety of sectors, including energy, transport, IT and manufacturing.

What was clear from the survey is that cybersecurity is a major challenge in all sectors, and that many organisations have experienced a cyber attack. Organisations tend to use a mixture of outsourced/cloud-based solutions and internally managed networks and systems. There is a good awareness in large organisations about cryptography standards and the risks of quantum computing.

What was also clear from the survey is that the main risks of cyber attack to NZ businesses and organisations are not due to the types of cryptography being used. We discuss this further below.

Findings for Business and Industry, especially in NZ and Australia

All industries and businesses use IT and computing. Every business has a digital footprint. All industries and businesses have security concerns. These concerns may be due to the storage and handling of sensitive data about customers, due to the risk of ransomware attacks, due to concerns about security of electronic payments, or due to many other possible threats. Industries such as healthcare and finance are particularly susceptible as they handle sensitive personal data that customers expect to remain private for their whole lifetimes, and so these areas are popular targets for ransomware or identity theft. Reputational risk is a serious matter for many businesses, since customers will go elsewhere if they do not trust the organisation. For this reason, many small businesses do not survive a major cyberattack. Hence, every business in NZ and Australia is exposed to cybersecurity risks.

Most businesses rely to a greater or lesser extent on third parties to assist with their security. For example, cloud-based tools and services allow an organisation to outsource much of the management of security to the provider of the service. Nevertheless, all such solutions typically take place over TLS connections and use authentication methods such as passwords and two- or three-factor authentication. In short, they rely on cryptography, and so are susceptible to breakthroughs in quantum computing. Hence it is important for businesses to work with trusted vendors who are keeping up-to-date with developments in cybersecurity and who will migrate to post-quantum cryptography at a suitable time.

Having established there is no organisation that is immune to the risks associated with quantum computing and cybersecurity, the relevant question for the purposes of this report is: What do industries and businesses need to do themselves to prepare for future risks from quantum computing?

To answer this question it is worth to recall the main sources of cyberattacks in the real world. These include weak passwords, phishing, denial-of-service attacks, insider attacks, malware, ransomware, spyware, zero-day attacks, Java code injection, SQL injection, side channels, supply chain attacks etc. A common feature of such attacks is that, generally, they are not prevented by cryptography. Indeed, attackers have been forced to exploit these types of attack precisely because of the need to bypass the cryptography.

For example, consider an attacker trying to gain access to a system that is protected by a high quality access control, VPN, and end-to-end encryption. Rather than trying to directly break TLS connections, perhaps using a quantum computer or other very powerful computing, attackers find it much more practical to guess common weak passwords, or to find a user with some other online account that has been compromised and to hope that user is using the same password for both systems. If these approaches don't work, an attacker can try a phishing attack or some other social engineering. In fact, this is cryptography working: The use of strong cryptography and other technical tools means that attackers need to find other ways to achieve their goals.

Since we are mentioning passwords, it is worth noting that, while in theory quantum computing may provide attackers with a small improvement for offline password guessing or other brute-force attacks, this doesn't seem to be the case. This question has been analysed by researchers[5].

The focus in this report is on attacks using quantum computing. So for convenience we divide the problem into two main areas of concern:

Area 1. Cybersecurity issues in products and/or services that are provided by vendors or service providers.
Area 2. Cybersecurity issues that are primarily the responsibility of businesses and organisations to manage themselves.

Examples of area 1 products and services include operating systems (Windows, iOS, Linux, Android, etc), networks (telecoms, internet service providers), cloud storage and backups (google, amazon), cloud-based services (payroll, HR, accounting, databases, payments, authentication and access control systems, etc). Typically, the providers and vendors are large organisations that maintain skilled teams of engineers. These organisations keep abreast of developments in security (including post-quantum security) and are expected to ensure their products and services maintain the highest standards. From the point of view of an individual business who uses such services, it suffices to work with trusted vendors and to ensure that systems and software are kept up-to-date on the client side.

Examples of area 2 issues include training and managing staff (e.g., onboarding and offboarding), providing access to systems for staff and contractors, monitoring networks and devices, checking logs, etc. In principle, an organisation could run a network or system based on their own home-made protocols and code, or using custom-built devices. But we are not aware of any such home-made security systems in NZ industry.

Our main finding is that, at least in New Zealand, industries and businesses are not generally implementing or maintaining their own public key cryptography to provide security for their operations. Sensibly, if using any cryptography at all, they are relying on trusted international vendors. What this means is that there is relatively little attack surface in Area 2 for attacks specifically relying on quantum computing.

Instead, the main attack surface for quantum computing is the network protocols, operating systems, and cloud systems that are ubiquitous in modern IT. The good news, from the point of view of small or medium businesses, is that these services are generally provided by large organisations that employ cryptography experts and can be expected to upgrade to use post-quantum cryptography when appropriate. As always, outsourcing security to trusted vendors and suppliers is a good way for most businesses to manage their cybersecurity concerns.

One important question is how easy it will be to upgrade and integrate post-quantum cryptography into existing systems, and whether there will be any consequences to usability. As explained, the migration should be seamless via software updates. However it is expected that post-quantum

[5] Markus Dürmuth, Maximilian Golla, Philipp Markert, Alexander May, and Lars Schlieper, Towards Quantum Large-Scale Password Guessing on Real-World Distributions, https://eprint.iacr.org/2021/1299

cryptography will have slightly worse performance than current systems, and so there may be some impact on real-time systems. As far as we can tell from our survey, there is no public key cryptography being used in industrial control systems (ICS) or operational technology (OT) in New Zealand, so there is nothing to upgrade. Hence there will be no impact on usability or security for these systems.

Our conclusion is that NZ business and industry does not have to be too concerned about the specific cybersecurity threat of quantum computing. In most instances, the migration to post-quantum cryptography will be seamless and invisible. Instead they can maintain their focus on the many and varied existing cybersecurity issues that are part of their day-to-day concern. However, there are two caveats to this:

- Organisations that collect and store data that needs to be confidential for very long timescales compared to average businesses may need to consider the risks of "harvest now and decrypt later" attacks. For example, personal health data should be considered carefully in this context.
- Organisations should consider carefully whether they have computer systems that are connected to networks but hard to maintain/upgrade. An example of this would be devices that are part of industrial plant equipment or embedded in physical infrastructure. If it is not possible to upgrade software and hardware in such systems to support post-quantum cryptography (e.g., for TLS connections), then the entire networks and systems in the organisation might have to still support weak legacy components. Such a state of affairs could open the door to downgrade attacks, as were mentioned earlier in this report.

Organisations are advised to consider such issues in their ongoing cybersecurity risk evaluation process.

Timeline for Change

The question of when a large-scale and error-tolerant quantum computer will be built is very hard to answer. It is clear that significant progress has been made in quantum computing for applications in science and medicine. But it is less clear if there has been any progress on breaking cryptosystems. Nevertheless, some experts predict that within the next 10 to 20 years sufficiently large quantum computers will be built that break essentially all public key schemes currently in use.

We must pay attention to the long timeline needed to migrate to new technologies: first the cryptosystems and protocols need to be standardized, then the major software developers need to ensure that their products support the new protcocols, then organisations need to upgrade their systems (eg installing software upgrades to all components of a system, or possibly even having to upgrade hardware). Therefore, regardless of whether we can estimate the exact time of the arrival of code-breaking quantum computing, we need to allow plenty of time to prepare our systems to be able to resist quantum computing.

Consequences for Business and Industry, especially in NZ and Australia

On the basis of our survey and review of the NZ cybersecurity landscape, we have not identified any issues that are specific to our region. NZ organisations, systems, and infrastructure are not more or less advanced than other nations. The risk of quantum computing to NZ businesses and industries is much the same as everywhere else. No industry or sector in NZ is particularly more vulnerable than any other. What this means is that the solutions are the same, which are broadly to work with trusted products from respected vendors and to keep systems updated.

For these same reasons, we have not identified any particular opportunity for innovation or collaboration to advance quantum-secure systems in NZ. The opportunities for collaboration between industry and academia in cybersecurity in NZ are limited, as most organisations use security products and services from major vendors based in the US or other large nations.

The question of integrating post-quantum cryptography into current systems is part of a wider question about integrating cryptography and other best-practice technologies into current systems. Our finding that NZ business and industry does not have to be too concerned about the specific cybersecurity threat of quantum computing should not be construed as a validation of the current state of cybersecurity in NZ. Indeed, the lack of exposure to quantum risk is precisely because most systems are fairly primitive and not using advanced cryptographic tools at all. There are many risks and challenges, and greater awareness of cybersecurity in organisations and the wider public is necessary.