White-paper: Australian Banking Websites Are Not Ready for Post Quantum Cryptography

Andrew E Scott

andrew@farphase.com

March 2025

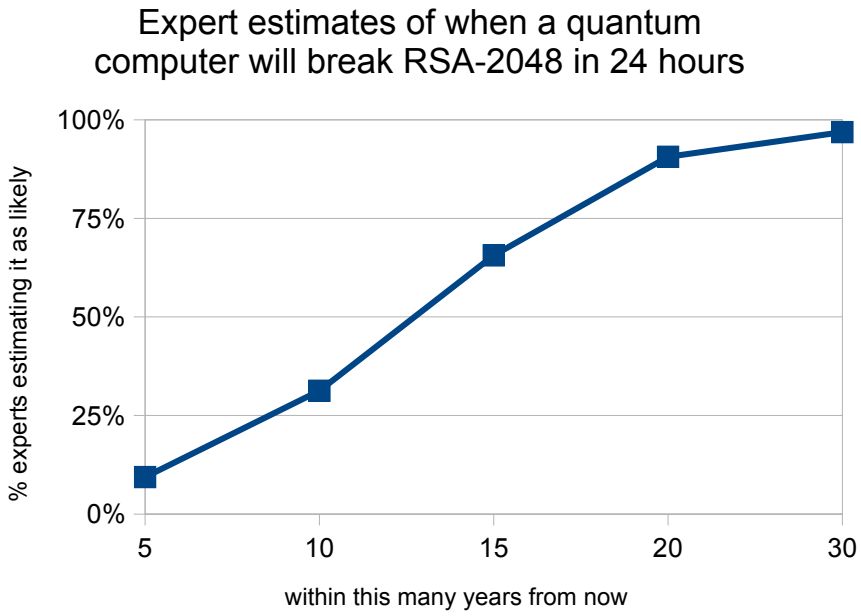
FAR PHASE

Introduction

Ever since 1994, when Peter Shor developed a way to use quantum computers to efficiently solve the mathematical problem of factorisation,[1] it has been clear that **future quantum computers present a risk to current security**. The security of the Internet has relied on the difficulty of certain mathematical problems to ensure that encrypted information stays private, and that it is sent by the equipment that it claims to come from. However, quantum computers that break today's Internet security are soon to appear.

The Canada-based Global Risk Institute regularly gathers a global panel of quantum technology experts to inform their Quantum Threat Timeline reports. These reports estimate the likelihood of quantum computers appearing which threaten today's Internet security, represented by breaking the RSA-2048 standard within a day. The most recent report[2] indicates **that around a third of experts saw such quantum computers as likely within 10 years of 2024** (see Diagram 1).

Diagram 1: Expert opinions of when a quantum computer is likely to appear that can break today's Internet security.



Source: Global Risk Institute, 2024 Quantum Threat Timeline Report, December 2024.

Anticipating this, the United States National Institute of Standards and Technology (NIST) has been working since 2017 to develop new security algorithms that should continue to offer protection, even in a post-quantum world. These **Post Quantum Cryptography (PQC) standards were published in August 2024**, and included two standards that protect authenticity and a standard that protects privacy.[3] This latter PQC standard is called ML-KEM.

1 https://en.wikipedia.org/wiki/Shor%27s_algorithm
2 https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/
3 https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

In December 2024, the Australian Government updated the Information Security Manual (ISM) to include guidelines that any new IT systems have ML-KEM support by 2030, and that the cryptography standards that it replaces would not be acceptable beyond that point.[4] The ISM is widely used by government and large organisations to define their cybersecurity risk approach, so is highly influential. **ISM gives such organisations and their suppliers up to five years to fully transition to ML-KEM**.

Many leaders in the IT supplier ecosystem have already moved to ML-KEM, or have been vocal on the need for organisations to begin work on this PQC migration. For example,

- Apple upgraded iMessage to protect users with ML-KEM since February 2024.[5]
- Google has stated "it's crucial for organizations to initiate the transition immediately."[6]
- Microsoft has said "the time to start planning is now".[7]
- Gartner has stated "Quantum computing will render traditional cryptography unsafe by 2029. It's worth starting the post-quantum cryptography transition now."[8]
- IBM has written "The time to prepare is now. Data not secured today is already lost."[9]

IBM was referring to the Store Now Decrypt Later threat (also known as Harvest Now Decrypt Later), where **otherwise-secure information sent over the internet might be captured today by a malicious party, and then when a suitable quantum computer emerges, that information is stripped of its security**. It is believed that nation states and other well-resourced cybercriminals are engaged in storing such data, and it is just a matter of time before this data is used for targeted leaks and ransoms.[10] Once an organisation fully migrates to ML-KEM, it prevents such attacks.

The Australian banking sector

Australian banks are technologically advanced, leading to a high adoption of digital banking in this market. The ABA has reported that in 2024, **99.1% of consumer banking interactions were made via online banking and apps**.[11] This highlights the importance of ensuring that these interactions are kept secure.

The data that is most critical to protect from a Store Now Decrypt Later attack is: (i) sent over the Internet, (ii) highly sensitive/valuable if it leaks, and (iii) remains relevant for another 10 years or more. In the context of an Australian finance system, there are many examples of such data. In addition, there are instances of long-lived equipment that are deployed into the

4 https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cryptography
5 https://security.apple.com/blog/imessage-pq3/
6 https://cloud.google.com/blog/products/identity-security/cloud-ciso-perspectives-why-we-need-to-get-ready-for-pqc
7 https://quantum.microsoft.com/en-us/vision/quantum-cryptography-overview
8 https://www.gartner.com/en/articles/post-quantum-cryptography
9 https://www.ibm.com/quantum/assets/quantum-safe/IBM_Quantum-Safe-Technology-Brochure.pdf
10 https://therecord.media/us-leaders-prep-for-quantum-cryptography-concerns
11 https://www.ausbanking.org.au/report/bank-on-it-customer-trends-2024/

field for 10 years or more, and could be difficult to upgrade cost-effectively (for example, without having a technician visit them). New instances of such equipment should implement ML-KEM immediately to avoid future expensive upgrades. Examples of relevant data and equipment are listed in Table 1.

Table 1: Examples of data and equipment that should be prioritised in an ML-KEM implementation.

Type of item	Examples
Customer data	Loan applications and contracts
	KYC records (passports, drivers licenses)
	High-value customer transactions
Employee data	Salary/tax records
	Medical certificates
Supplier data	Joint-Venture agreements
Operational data	Company strategies
	Board papers
Long-lived equipment	ATMs
	EFTPOS devices

Source: Far Phase, 2025

Some of the customer data listed in Table 1 is shared over the Internet via banking websites and apps. However, **despite the strong advice offered by IT industry leaders and the Australian Government to begin migrating to ML-KEM and other PQC approaches, there has been little outward sign of progress from the banking sector.**

Given that Google has even implemented ML-KEM to protect their search engine pages and free email service, it is clear that it is quite possible to provide an online service that protects against future quantum computers. However, **a review by Far Phase has found that none of the popular Australian banking websites protect people from quantum threats**. (See the appendix for the methodology and full results of this review.) It is not clear how the sector will have migrated to ML-KEM by 2030, and for now it fails to protect customers from the Store Now Decrypt Later threats.

Of the 18 Australian banking websites examined, two banks provide ML-KEM based protection to their main webpage (Bendigo Bank and Beyond Bank). However this protection is enabled through their use of Cloudflare which applies to largely static pages that do not contain customer data. It does not extend to their Internet banking login pages, for example.

Further, two Australian bank websites (Commonwealth Bank and BOQ) were found to still be using an older version (v1.2) of the TLS security protocol that cannot support ML-KEM without being upgraded. This could further slow their migration to the new standard.

In general, **Australians would not expect that a search engine offers better post-quantum protection for their sensitive data than Australia's biggest banks**.

Technology enablers and blockers

Despite the poor state of Australian banking website protection today, **there are some shifts in the technology ecosystem that will allow Australian banks to progress more rapidly now to implementing ML-KEM**. Also, there are some blockers that prevent ubiquitous access to PQC in the near-term, although these should not be used as an excuse to avoid protecting anyone.

Key technology enablers include:

- OpenSSL, the most widely-used encryption library, will support ML-KEM in its v3.5 release, due around April 2025. [12]The alpha version of this library is already available.
- Standardisation by IETF of the use of ML-KEM in TLS is underway.[13] This standard reflects the way it is already in use in many production environments, but some IT suppliers have flagged that IETF standardisation will be the trigger for ML-KEM deployment across their offerings, e.g. AWS cloud endpoints[14] and Java software.[15]
- Akamai, used by many of the bank websites, has flagged PQC support from early 2025.[16]

Technology blockers include:

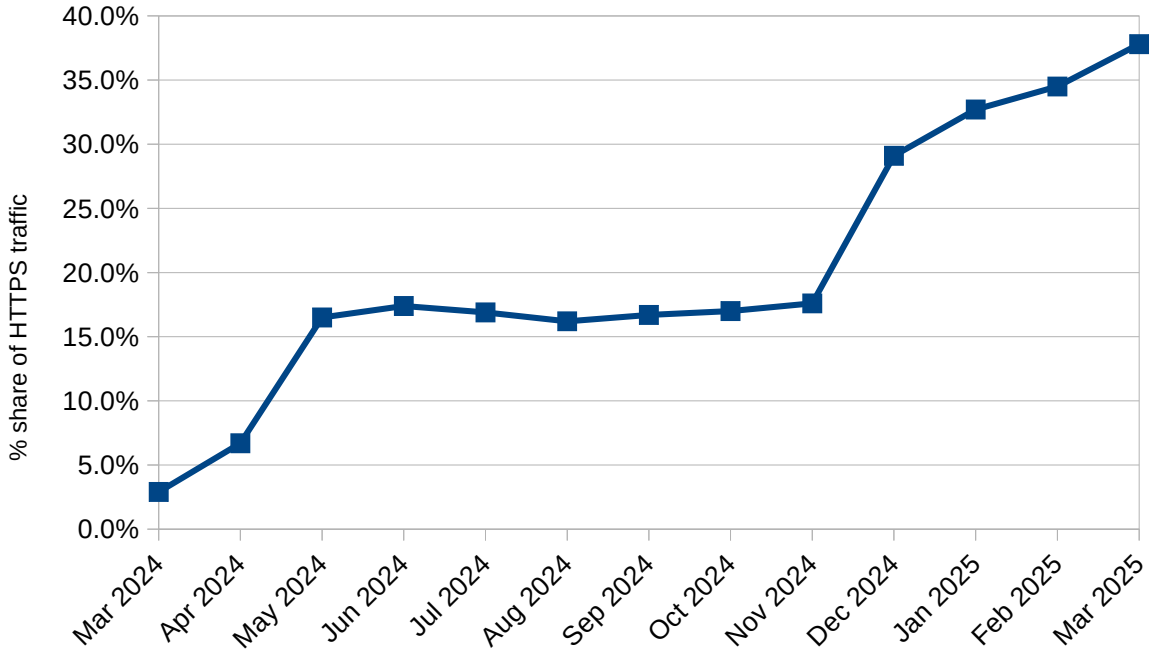
- Apple Safari is the only major web browser that does not support ML-KEM. Outside of the EU, this is the only browser engine allowed on iPhone devices, and so also prevents other iPhone web browsers from providing ML-KEM support.
- Mobile device operating systems such as iOS and Android do not currently provide native support for PQC. Mobile apps that wish to use ML-KEM today need to integrate a third-party cryptography library such as BouncyCastle or (soon) OpenSSL.
- Windows 10 supports only the older version of TLS (v1.2),[17] so Windows users will likely need to upgrade to Windows 11, perhaps involving new hardware, in order to make use of ML-KEM natively. Alternatively they will need to use applications that integrate a third-party cryptography library, such as web browsers.

Despite the current state of technology, according to Cloudflare, PQC-based protection of websites has been growing rapidly over the past year. The Cloudflare Radar shows that about 97% of web traffic is secured by HTTPS (Hypertext Transfer Protocol Secure), and the proportion of that traffic that is protected using PQC has grown from 2.9% to 37.8% since

12 https://openssl-library.org/post/2025-02-04-release-announcement-3.5/
13 https://datatracker.ietf.org/doc/draft-kwiatkowski-tls-ecdhe-mlkem/
14 https://aws.amazon.com/blogs/security/aws-post-quantum-cryptography-migration-plan/
15 https://bugs.openjdk.org/browse/JDK-8339009
16 https://www.akamai.com/blog/security/taking-steps-to-prepare-for-quantum-advantage
17 https://learn.microsoft.com/en-us/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp-

March 2024 (see Diagram 2). This illustrates that **banks who migrate to ML-KEM today will give protection to a significant fraction of their customers**.

Diagram 2: Share of secure web traffic seen by Cloudflare that is also protected by PQC.



Source: Cloudflare Radar, Far Phase, March 2025

Conclusion

Since 1994, it has been clear that future quantum computers will pose a threat to current security, and since 2017, NIST has been working on PQC standards to offer protection in a post-quantum world. With NIST's standardisation of ML-KEM last year and the update of the Australian ISM to require new IT systems migrate to ML-KEM by 2030, there is a clear direction for how Australian organisations should protect users of their websites and apps.

Additionally, the Store Now Decrypt Later threat means that every day that migration to ML-KEM is delayed is another day for data to be captured by malicious actors for later decryption by a suitable quantum computer. Long-lived, sensitive data sent over the Internet and captured in this way is a ticking time-bomb, as it could be later leaked or result in a ransom demand.

Today, none of the popular Australian banking websites protect people from this quantum threat. Despite nearly 40% of global secure web traffic being protected with PQC, Australian banks are far behind.

Australian banks should urgently update their websites to protect their users from Store Now Decrypt Later threats. Over 99% of customer interactions with banks are via apps and websites, and banks are recipients of the type of long-lived, sensitive data that is particularly affected by Store Now Decrypt Later.

Terminology

For convenience, a number of the terms or acronyms used in this white-paper are defined below.

Term	Definition/explanation
ABA	Australian Banking Association
Android	Google's operating system used on mobile devices
APRA	Australian Prudential Regulation Authority
ATM	Automated Teller Machine
AWS	Amazon Web Services
CDN	Content Delivery Network
EFTPOS	Electronic Funds Transfer at Point of Sale
HTTPS	Hypertext Transfer Protocol Secure is used to securely connect with websites
IETF	Internet Engineering Task Force
iOS	Apple's operating system used on mobile devices
ISM	Information Security Manual
KYC	Know Your Customer
ML-KEM	Module-Lattice-based Key Encapsulation Mechanism, a standardised PQC algorithm
NIST	National Institute of Standards and Technology
OpenSSL	A widely-used cryptography library
PQC	Post Quantum Cryptography
RSA-2048	A 617-digit long number (represented by 2,048 bits in binary) that poses a very difficult mathematical problem to factorise
TLS	Transport Layer Security

Appendix: Methodology and Results

On 18 March 2025, a set of websites was tested based on two sources:

1. The list of "Most Visited Banking Websites in Australia – February 2025" from Semrush (https://www.semrush.com/website/top/australia/banking/), indicated by a number in the table below.
2. The top 15 banks by total residents deposits from "APRA Monthly authorised deposit-taking institution statistics January 2025 (https://www.apra.gov.au/monthly-authorised-deposit-taking-institution-statistics), where additional bank websites from this list are indicated by a letter in the table below.

For websites, they were manually classified into one of four types: (i) bank, (ii) money transfer service ("transfer"), (iii) payment card or service ("payment"), or (iv) informational website ("info"). Only those classified as type bank were tested for Post Quantum Cryptography (PQC) support.

This resulted in 18 individual bank websites, noting that one is listed twice (anz.com / anz.com.au) in the table below due to how it appears on the Semrush list.

All websites had their CDN (Content Delivery Network) identified through use of the CDN Finder tool by CDN Planet (https://www.cdnplanet.com/tools/cdnfinder/), focussing on the CDN most applicable to the online banking function, e.g. ignoring website analytics tools. If no CDN was identified, a dash was used in the table below.

Each bank website was visited with two web browsers:

1. Firefox Browser 136.0.1 using the Quantum Safety add-on v0.3 (https://addons.mozilla.org/en-US/firefox/addon/quantum-safety/)
2. Google Chrome 134.0.6998.89 using the Developer Tools feature, looking at the Privacy & security tab.

In every case, both web browsers consistently reported the level of support for PQC. The TLS version information was obtained solely from the Google Chrome browser Developer Tools feature. Note that TLS v1.3 is required to provide PQC.

The main page of the bank website was visited, and if PQC was supported (currently, the X25519-MLKEM768 hybrid algorithm), it received a tick for "Main page PQC". Then the login page for the Internet banking service was accessed, and if that page showed support for PQC, it received a tick for "Login form PQC".

Table 2: Post Quantum Cryptography support by the most popular Australian banks.

	Bank	Website	Type	CDN	Main page PQC?	Login form PQC?	TLS
1	Commonwealth Bank	commbank.com.au	bank	Akamai	×	×	1.2
2	Westpac	westpac.com.au	bank	Amazon	×	×	1.3
3	NAB	nab.com.au	bank	Akamai	×	×	1.3
4	ANZ	anz.com	bank	Imperva	×	×	1.3
5	ANZ	anz.com.au	bank	Imperva	×	×	1.3
6	CBA	commsec.com.au	bank	Akamai	×	×	1.3
7	St.George Bank	stgeorge.com.au	bank	Amazon	×	×	1.3
8	Wise	wise.com	transfer	Cloudflare			
9	American Express	americanexpress.com	payment	Akamai			
10	ING	ing.com.au	bank	-	×	×	1.3
11	Xe	xe.com	transfer	Amazon			
12	Bendigo Bank	bendigobank.com.au	bank	Cloudflare	✓	×	1.3
13	Suncorp Bank	suncorpbank.com.au	bank	Fastly	×	×	1.3
14	Bankwest	bankwest.com.au	bank	Fastly	×	×	1.3
15	Moneysmart	moneysmart.gov.au	info	Cloudflare			
16	BOQ	boq.com.au	bank	Akamai	×	×	1.2
17	BPOINT	bpoint.com.au	payment	-			
18	ubank	ubank.com.au	bank	Akamai	×	×	1.3
19	Remitly	remitly.com	transfer	Amazon			
20	Beyond Bank	beyondbank.com.au	bank	Cloudflare	✓	×	1.3
A	Macquarie Bank	macquarie.com.au	bank	Akamai	×	×	1.3
B	HSBC Bank	hsbc.com.au	bank	Amazon	×	×	1.3
C	BNP Paribas	cib.bnpparibas	bank	Akamai	×	×	1.3
D	Heritage Bank	heritage.com.au	bank	-	×	×	1.3
E	Citibank	citibank.com.au	bank	Akamai	×	×	1.3

Source: Far Phase, March 2025