TECHNICAL REPORT – ENG1 (SEM2) [2023/2024]

A study on the potential transition from public key encryption to quantum safe encryption algorithms in organisations that support critical industry in order to prevent future cyber-attacks from quantum computers.

Matriculation number: s2483666

Executive summary

This report, commissioned by APPLE Inc., assess the potential transition from 2048-bit public key encryption to more advanced, quantum-safe algorithms.

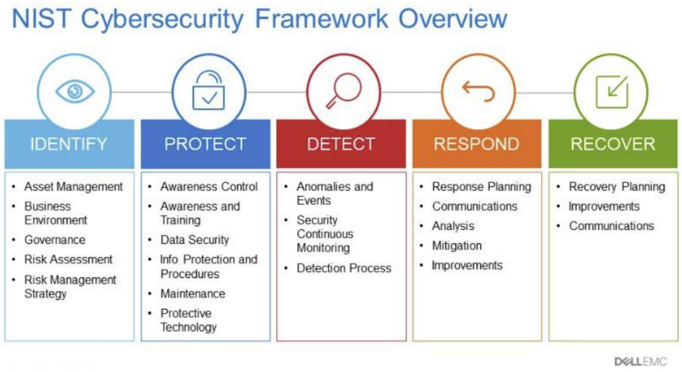

Fig 1.) Shows an overview of the NIST cybersecurity[5]

This transition aligns with a proposed quantum readiness roadmap by the US National Institute of Science and Technology(NIST)[4] aimed at preparing for the development of cryptanalytically relevant quantum computers (CRQC's).

This report found that currently only around 25% of companies are planning a transition to quantum-safe algorithms[23]. Reasons for this reluctance include an ignorance of the threat and concerns over the cost.

Despite the proposed benefits, barriers still apply to their implementation, so the following recommendations apply:

Summary recommendations

1. Governments should plan an international agreement on quantum safe algorithms to ensure compatibility between nations and ensuring a seamless quantum transition.
2. APPLE inc. should proactively create a quantum readiness road map[4]. This strategic planning aims to safeguard data with a long secrecy lifetime, as it may already be susceptible to "store now, decrypt later techniques"[13].
3. Manufacturers who design quantum-vulnerable technology should immediately begin to transition to producing technology which aligns with the new government legislation.
4. APPLE inc. should build an understanding of their dependencies on pre-quantum systems to ensure that future plans minimise as much quantum risk as possible.

1.0 Introduction

Today, Asymmetric key systems, like the Rivest-Shamir-Adleman cryptosystem (RSA) are key components of modern cryptography and used in conjunction with symmetric key systems in almost all modern encryption.

1.1 Asymmetric Key: how it works and its vulnerabilities

The premise of an asymmetric key algorithm is that it is computationally easy to compute in one direction, but near impossible in the other.

In the widely used RSA, the recipient and sender each have two prime numbers which they keep hidden(private keys). They then use Carmichael's totient function[5], a randomly chosen 'e' value and the modulus function to produce a larger public number (public key).

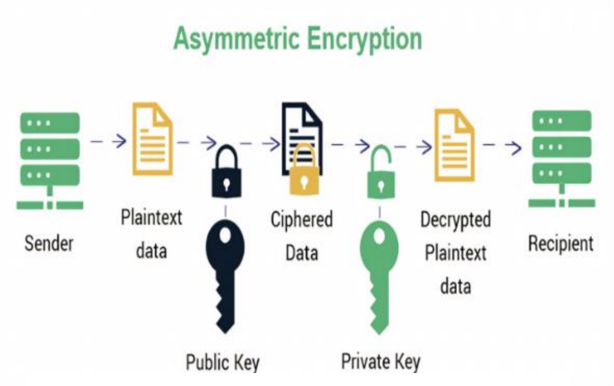

Fig 2.) Shows a simplified example of how an asymmetric system works with 2 keys, a public and private[7].

The sender encrypts their message in such a way that it is impossible to decrypt without knowing the two prime factors of the recipient's public key. It is easy for the recipient to decrypt with their private key but much harder for an outside observer as they have to perform a prime factorisation of the public key[6].

Today brute force attacks on RSA are near impossible. Modern cryptography uses primes that are 313 digits long (2048-bit encryption). It is estimated that a conventional computer would need 300 trillion years to perform a prime factorisation of 2048-bit encryption even using the best prime factorising algorithm known; the General Number Field Sieve[8] (GNFS).

Most other common vulnerabilities associated with this method can be mitigated using a number of techniques and proper standards and regulation[10].

But today quantum computers pose a threat to Asymmetric key algorithms by leveraging Shor's algorithm[11] to efficiently perform a prime factorisation of large numbers, undermining the security of widely used encryption methods like RSA which rely on the difficulty of large prime factorisation. It is widely predicted that within the next 15 years we will see quantum computers powerful enough to successfully run Shor's algorithm[11]. This could see the large integer factorisation problem completed within hours or minutes, rather than millions of years.

1.2 Quantum-safe : how it works and its benefits

Quantum safe algorithms are essentially problems that are deemed extremely difficult for both digital and quantum computers to solve, thereby rendering a brute force cyber-attack virtually impossible and ensuring absolute security for years to come.

Three of the four quantum safe algorithms chosen by the US National Institute of Standards and Technology (NIST)[4] use the mathematics of lattices. The main of these, being the CRYSTALS dilithium[1] approach, allows for varying levels of security to be chosen depending on the needs of the user and the anticipated capacities of the quantum computers they are being implemented against.

These lattice-based approaches are also very efficient and the three together provide flexibility for the level and efficiency of encryption required.

The last algorithm chosen is SPHINCS+[3] which is based on a different mathematical foundation called hash-functions. This algorithm is less efficient but is useful as a backup due to its basis on a different mathematical approach from the other three.

It is certain to say that the future of long-term cybersecurity lies with quantum-safe algorithms such as the ones mentioned above.

2.0 Review

2.1 Incentives to transition to Quantum-safe Economy

Evidently it is within organisations interests to make the switch, even if the timeline for quantum computers is exaggerated. Cybersecurity is hugely important. Many organisations such as the government hold information with a long secrecy lifetime and so long-term security is of the utmost importance.

Although a cryptanalytically relevant quantum computer(CAQC) is still some years away many experts believe that Harvest Now Decrypt Later(HNDL) techniques are currently being employed by rogue nation-states and cybercriminals[13]. These techniques make CAQC's an immediate threat and this has led the market for quantum cybersecurity to grow significantly[14].

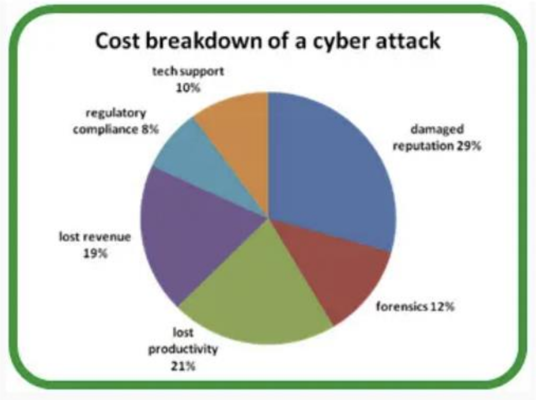

Fig 3.) Shows the cost breakdown of a cybersecurity attack[16].

Despite this, 53% of global respondents still reported not being "very concerned" about future quantum cyber-attacks[12]. This is down only slightly since the last census. Clearly there are factors holding organisations back from making the essential leap.

One of these factors is recognised to be ignorance. Some parties believe that quantum computers are much further off than anticipated and that the investment into security isn't worth it.

The reality is that a switch to quantum-safe cybersecurity is costly and many companies are wondering why they should invest this early. But although we don't know when a CAQC will be available, we do know that a new generation of cryptography is here, the adoption of which is already making its way into legislation[15]. It is difficult to predict the funds required for a complete transition but considering the average cost of a data breach these days is $4.35 million[16], then it is certainly within party's interests to prepare. Another huge financial incentive for a transition would come in the form of cryptocurrency. It is estimated that around 40 billion dollars or 25% of bitcoin assets are at risk if steps are not taken to secure them within the coming years[16]. Whatever some may believe, the threat should be considered too large to forgo.

Lastly a late quantum transition will put more legacy at need of an update. This will mean that organisations who have designated resources and invested time into planning an early transition will come off better in the long run.

2.2 Government Regulatory, Policy and Guidance Alignment

Governments worldwide have implemented numerous policies aimed at addressing cyber security concerns, with notable examples including the Budapest Convention in Europe, which has played a pivotal role in combating cybercrime through legal harmonization and international collaboration.

The United States was amongst the first to realise the potential issues when, in 2016 NIST put out a call for global cooperation in producing a set of quantum safe algorithms. This seen Cryptographers from all over the world submit different approaches to the problem which were then vetted and are currently in the process of being standardised.

The US National Security Agency (NSA) in conjunction with NIST and has recently announced the CNSA 2.0[18] to warn organisations of the timeline for quantum-resistant algorithms which will soon be required of US National Security System (NSS) owners[19].

Similarly, the United Kingdom unveiled a new 10-year vison plan by the Department of Science Technology and Innovation[20]. This plan sets specific goals, including ensuring that at least 75% of UK businesses have taken steps to implement quantum encryption algorithms.

To support the endeavour, UK government has promised £2.5 billion in quantum funding. They also intend to fund a further 1000 post-graduate quantum research positions to ensure the UK stays at the forefront of this new technology.

It is of worth to note that in 2022, record private investment in quantum technologies was achieved, totalling $2.35 billion[20]. This is a global phenomenon with the US investing $1.8billion, the EU set to invest $1.2 billion and China estimated to invest a whopping $15.2 billion in the coming years[20]. A new report by McKinsey[21] suggests this investment could be well placed as companies stand to gain $1.3 trillion by 2035[20].

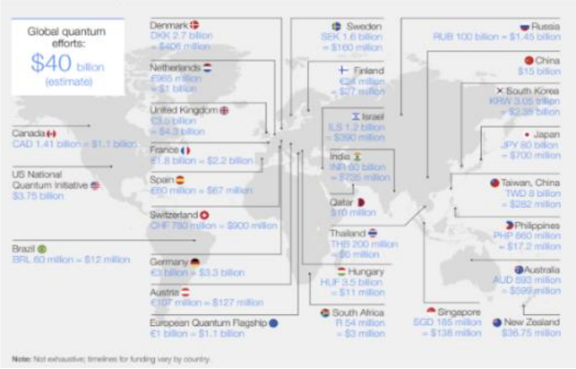
Global quantum efforts:
$40 billion (estimate)
Denmark DKK 2.7 billion ≈ $406 million
Netherlands €965 million ≈ $1 billion
United Kingdom £3.5 billion ≈ $4.3 billion
Canada CAD 1.41 billion ≈ $1.1 billion
France €1.8 billion ≈ $2.2 billion
US National Quantum Initiative $3.75 billion
Spain €60 million ≈ $67 million
Switzerland CHF 780 million ≈ $900 million
Brazil BRL 60 million ≈ $12 million
Germany €3 billion ≈ $3.3 billion
Austria €107 million ≈ $127 million
European Quantum Flagship €1 billion ≈ $1.1 billion
Sweden SEK 1.6 billion ≈ $160 million
Finland €24 million ≈ $27 million
Israel ILS 1.2 billion ≈ $390 million
India INR 60 billion ≈ $735 million
Qatar $10 million
Thailand THB 200 million ≈ $6 million
Hungary HUF 3.5 billion ≈ $11 million
South Africa R 54 million ≈ $3 million
Russia RUB 100 billion ≈ $1.45 billion
China $15 billion
South Korea KRW 3.05 trillion ≈ $2.38 billion
Japan JPY 80 billion ≈ $700 million
Taiwan, China TWD 8 billion ≈ $282 million
Philippines PHP 860 million ≈ $17.2 million
Australia AUD 593 million ≈ $399 million
Singapore SGD 185 million ≈ $138 million
New Zealand $36.75 million
Note: Not exhaustive; timelines for funding vary by country.

Fig 5.) Shows a breakdown of the world's total quantum investment to date[21].

Evidently, taking into account the above, quantum technology is well funded and there is huge global interest. If multiple parties' projections materialise then reliable quantum-resistant algorithms will soon be essential, aligning with the initiatives of at least 24 different countries[22].

3.0 SWOT Analysis

Concerning Quantum-safe over public-key encryption:

STRENGTHS • SECURITY AGAINST ATTACK – Safe from both digital and quantum computers. • COMPATIBILITY – Designed to be compatible with existing infrastructure. • INCREASED TRUST – Implementing demonstrates an organisations commitment to security, enhancing trust among stakeholders and customers.	**WEAKNESSES** • PERFORMANCE – Require more computational resources. • MATURITY AND STANDARDISATION – Not yet as standardised and tested as traditional algorithms. • TRANSITION ISSUES – Transitions can be costly and resource intensive
OPPORTUNITIES • MARKET DIFFERENTIATION – Early adopters can gain market differentiation through advanced security. • COLLABORATION AND PARTENRSHIPS – Collaboration efforts can accelerate knowledge exchange and foster innovation	**THREATS** • RELIANCE ON INSECURE SYSTEMS – Delayed adoption could leave organisations vulnerable to attack. • INTEROPERABILITY CHALLENGES – inconsistent adoption could hinder a seamless transition . • CYBERSECURITY RISKS – Still suffer from other cybersecurity risks such as social engineering.

4.0 Summary and recommendations

In short, the transition to quantum-safe algorithms is not without its barriers. Notably a lack awareness of the threat and the associated costs of a successful transition. Nevertheless proactive companies and governments are investing, recognising the importance and potential return . When assessing the potential returns, this report concludes that if APPLE inc. were to plan a transition now then the benefits - mainly increased security and shareholder trust - would greatly outweigh the negatives of a potentially crippling future cyber-Attack. This is especially crucial considering the vast amount of sensitive information in which people from all over the world entrust with the company. Furthermore this move would serve as a powerful message to other major companies, underlining the seriousness of the threat and would strengthen relationships with governments worldwide, signalling APPLE inc.'s commitment to the security of their citizens.

Summary recommendations

1. Governments should plan an international agreement on quantum safe algorithms to ensure compatibility between nations and ensuring a seamless quantum transition.
2. Apple should proactively create a quantum readiness road map[4]. This strategic planning aims to safeguard data with a long secrecy lifetime, as it may already be susceptible to store now, decrypt later techniques.
3. Manufacturers who design quantum-vulnerable technology should immediately begin to transition to producing technology which aligns with the new government legislation.
4. Apple should build an understanding of their dependencies on pre-quantum systems to ensure that future plans minimise as much quantum risk as possible.

REFERENCES AND EXTERNAL WEB LINKS

1. Schwabe.P (2020) , “CRYSTALS, Cryptographic Suite for Algebraic Lattices” [online] Available at : CRYSTALS (pq-crystals.org) [Accessed: 08/03/2024]
2. “FALCON, Fast-Fourier Lattice-based Compact Signatures over NTRU” (2017) [online] Available at : Falcon (falcon-sign.info) [Accessed: 08/03/2024]
3. Schwabe.P(2023), “SPHINCS$^+$, Stateless Hash-based Signatures” [online] Available at SPHINCS+ [Accessed: 08/03/2024]
4. “QUANTUM READINESS, MIGRATION TO POST QUANTUM CRYPTOGRAPHY” (2023) [online] Available at : CSI-QUANTUM-READINESS.PDF (defense.gov) [Accessed: 05/03/2024]
5. Dulavitz.M (2019) “NIST cybersecurity framework” [online] available at: Strengthen Security of Your Data Center with the NIST Cybersecurity Framework | Dell USA [Accessed: 20/03/2024]
6. Lake.J (2024) “Exploring RSA encryption: a comprehensive guide to how it works” [online] Available at : What is RSA encryption and how does it work? (comparitech.com) [Accessed: 08/03/2024]
7. Mehta.M (2020) “What is Asymmetric encryption” [online] Available at: What Is Asymmetric Encryption & How Does It Work? - InfoSec Insights (sectigostore.com) [Accessed: 20/03/2024]
8. Shankland.S (2021) “Quantum computers could crack todays encrypted messages. That’s a problem” [online] Available at: Quantum computers could crack today's encrypted messages. That's a problem - CNET [Accessed: 08/03/2024]
9. Lake.J (2024) “What is a side channel attack and how do they work?” [online] Available at: What is a Side Channel Attack? (with Examples) (comparitech.com) [Accessed : 08/03/2024]
10. NIST (2024) “Cryptographic Standards and Guidelines” [online] Available at: Cryptographic Standards and Guidelines | CSRC (nist.gov) [Accessed: 08/03/2024]
11. Parker.E (2023) “When a Quantum Computer Is Able to Break Our Encryption, It Won’t Be a Secret” [online] Available at: When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret | RAND [Accessed: 11/03/2024]

12. Borgeaud.A (2023) “Global security concerns about quantum 2021, by region” [online] Available at: Quantum computing security concerns worldwide 2021 | Statista [Accessed: 11/03/2024]
13. Noone.G (2023) “Are harvest now, decrypt later cyberattacks actually happening?” [online] Available at: Are harvest now, decrypt later cyberattacks actually happening? (techmonitor.ai) [Accessed: 11/03/2024]
14. Alsop.T (2023) “Quantum Security market revenue worldwide 2021-2030” [online] Available at: Quantum security market size 2021-2030 | Statista [Accessed: 11/03/2024]
15. Department of Science, Technology and Innovation (2023) “National Quantum Strategy” [online] Available at: National quantum strategy - GOV.UK (www.gov.uk) [Accessed: 11/03/2024]
16. World Economic Forum (2022) “Transitioning to a Quantum Secure Economy” [online] Available at: WEF_Transitioning to_a_Quantum_Secure_Economy_2022.pdf (weforum.org) [Accessed: 11/03/2024]
17. Council of Cybercrime (2024) “The Budapest Convention (ETS NO. 185) and its Protocols” [online] Available at: Budapest Convention - Cybercrime (coe.int) [Accessed: 17/03/2024]
18. US National Security Agency (2022) “Announcing the Commercial National Security Algorithm Suite 2.0” [online] Available at: CSA_CNSA_2.0_ALGORITHMS_.PDF (defense.gov) [Accessed: 17/03/2024]
19. US National Security Agency (press release) (2022) “NSA Releases Future Quantum Resistant (QR) Algorithm Requirements For NSS” [online] Available at: NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems > National Security Agency/Central Security Service > Article [Accessed: 17/03/2024]
20. Morrison.R (2023) “Investment in Quantum technology hit a record 2.35 billion last year” [online] Available at: Quantum investment hit a record $2.35bn last year (techmonitor.ai) [Accessed: 17/03/2024]
21. McKinsey Digital (2023) “Quantum Technologies Sees Record Investment, Progress On Talent Gap” [online] Available at: Record investments in quantum technology | McKinsey [Accessed: 17/03/2024]
22. World Economic Forum (2023) “Can we build a safe and inclusive ‘quantum economy’?” [online] Available at: Can we build a 'quantum economy'? | World Economic Forum (weforum.org) [Accessed: 17/03/2024]