Chapter 10
Post-quantum Cryptography

Linus Gasser

10.1 Introduction

The chapter about Post-quantum Cryptography discusses the need for a new generation of cryptography to protect against future quantum computers. These computers will likely reverse many of the one-way functions used in current asymmetric encryption methods, making encrypted data vulnerable. The US government advocates vigorously to implement post-quantum algorithms by 2035, as an enemy could decrypt encrypted data or messages copied today. Symmetric encryption is not significantly faster for quantum computers to break, but asymmetric encryption, which relies on one-way functions, is vulnerable. NIST started a Post-Quantum Cryptography (PQC) challenge in 2016, with four algorithms selected as safe against quantum computers in 2022. The first implementations have started to appear, combining PQC with classical algorithms for added security. The research will continue to find faster and more secure algorithms, but no known cryptographic algorithm is *provably* secure against quantum computers and allows homomorphic encryption. Hybrid encryption is becoming more common, but protocols without a fallback must be considered carefully, as some quantum-safe algorithms may be attackable.

L. Gasser (✉)
EPFL, Lausanne, Switzerland
e-mail: linus.gasser@epfl.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_10

10.2 Analysis

Cryptography is widely used to encrypt (hide) and sign (prove the source) electronic documents and internet traffic. The underlying mathematical concept is a one-way function [1] that makes it easy to encrypt but challenging to decrypt without a secret. However, future quantum computers will likely be able to reverse many of these one-way functions that are widely used and allow the calculation of the secret needed to decrypt the data.

The US government urges its services to implement post-quantum algorithms by 2035 [2]. The urgency comes from the fact that even if quantum computers are expected to be available after that date, an enemy who copied encrypted data or encrypted messages might decrypt them at this point. For data with a long secrecy requirement, it is thus crucial to start using quantum-safe encryption well before such quantum computers exist.

10.2.1 Definition

Current encryption algorithms can be separated into two groups: symmetric encryption (see Chap. 2) and asymmetric encryption (see Chap. 3).

As of 2022, quantum computers are not significantly faster at breaking symmetric cryptography [3]. However, asymmetric encryption is based on one-way functions which can take a random, secret key and create a corresponding public key. The inverse function, taking a public key, and finding the secret key, is supposed to be hard for the two most commonly used algorithms, namely RSA and Elliptic Curves.

Future quantum computers should be able to speed up this reversing operation and make it possible to use a public key to find the corresponding private key within minutes instead of eons. They will use the Shor algorithm to break the one-way functions of RSA and Elliptic Curves. However, as seen in [4], there are still exponential advancements in terms of the number of qubits and their quality (error rate) required until quantum computers are powerful enough to run the Shor algorithm for today's asymmetric encryption algorithms.

Various propositions exist for one-way functions where quantum computers do not have an advantage. There are a couple of challenges: similar to one-way functions in widespread use today, these new ones need to be secure against any type of attack. It is not because nobody found an attack that would break an algorithm that the algorithm is secure as it often takes years to find such attacks, as seen in the example of two entries in the NIST post-quantum standardization effort [5]. Another problem is the encryption's speed, the keys' size, and the corresponding messages.

10.2.2 Trends

NIST started a Post-Quantum Cryptography (PQC) challenge in 2016, intending to find suitable algorithms for Public-key Encryption and Key-establishment as well as Digital Signature Algorithms. All cryptographers can participate in both proposing new algorithms, as well as in attacking existing algorithms. In July 2022, NIST published four algorithms that it believes to be safe against quantum computers [6].

Now that the winners of the NIST PQC challenge are known, the first implementations have started to appear. Because these algorithms are still very new, most implementations combine a PQC algorithm with a classical one. This is done so that even if one of the two turns out to be broken, the security of the other algorithm remains. One downside of the NIST PQC winners is that there is only one encryption algorithm but three signature algorithms. This means that if the encryption algorithm is broken, no alternative exists.

Google already tested quantum-safe encryption [7], and the SSH application, used to connect a user to a remote computer securely, proposes a hybrid encryption scheme as of April '22 [8].

Of course, research will continue with the goal of finding faster, more compact, and more versatile algorithms than the ones being submitted to NIST. Nevertheless, most importantly, there is currently no known cryptographic algorithm that is provably secure against attacks from quantum computers that allows homomorphic encryption.

More and more protocols will propose hybrid encryption, like SSH in [8], and later quantum-safe protocols only. However, the protocols that do not offer a fallback will have to be taken into account carefully, as there is a high probability that some of the currently proposed quantum-safe algorithms will turn out to be attackable either by quantum computers or even by classical computers.

10.3 Consequences for Switzerland

To understand why it is important to speed up the development and usage of quantum-safe algorithms, one has to look at Fig. 10.1:

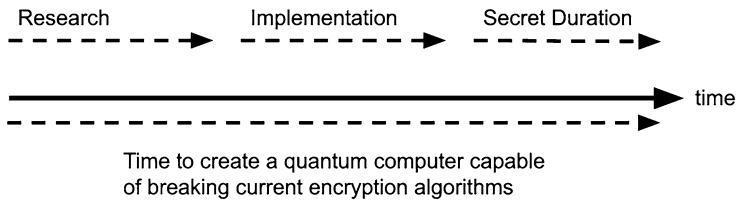

Fig. 10.1 Timelines of development of new algorithms and development of quantum computers

Even if we do not know whether or when a quantum computer capable of breaking today's encryption algorithms will be available, this does not mean we should wait until we know to switch to quantum-safe algorithms. This is because we need to add the time for research on quantum-safe algorithms, transitioning to them (updating old software and replacing non-upgradable legacy systems), and most importantly, the duration for which something encrypted today needs to stay secret. If an adversary stores encrypted messages in the hope of being able to decrypt them later using a quantum computer, the usefulness of these secrets must have expired by the time a quantum computer gets available.

This is true for both stored secrets and secret communications. As has been shown by the Snowden revelations, the NSA (and probably other secret services as well) is storing encrypted secrets and communications in the hope of being able to decrypt them at a later time [9]. For Switzerland, this means that it is of utmost importance for the banking and the military sector to drive the move to quantum-safe encryption. Otherwise, copies of the current safe data will be decrypted by third parties once quantum computers that can do so should become available. Stories about a quantum computer breaking a well-known algorithm like RAS-2048 will continue to emerge. But, they still do not achieve a scientific consensus [10].

For governments, one consequence is that future e-voting systems (see Chap. 23) need to be evaluated regarding their quantum-safe operations. If, for example, all encrypted votes are publicly available for verification, a future quantum computer might breach voting secrecy. On the other hand, businesses will mostly want to follow regulations and ensure that they implement the necessary and available technology. Otherwise, they might be penalized because they needed to implement better practices.

10.3.1 Implementation Possibilities: Make or Buy

Make: developing custom cryptographic algorithms is strongly discouraged since they are likely to be insecure. Custom implementations of existing algorithms (e.g., NIST candidates) might be considered, but usage (and review/analysis) of existing and well-tested implementations should be preferred.

Buy: use an existing library—NIST candidates are supposed to be patent-free, and most are available as Open Source implementations (Table 10.1).

10.3.2 Variations and Recommendation

There are different options for quantum-safe implementations. The first one would be to implement the probable best algorithm available. The second would be a hybrid combination of classical and quantum-safe algorithms to get the most secure option. Moreover, to wait until a consensus emerges on the best algorithm existing (Table 10.2).

Table 10.1 Implementation possibilities for different sectors

	Make		Buy	
	Pros	Cons	Pros	Cons
Military	Augment legacy systems, protection against backdoors	Potential error in implementation adding attack surface will leak	Access to peer-reviewed library	Might contain accidental or purposeful backdoors
Civil Society	None	None	Use library compatible with other services	None
Economy	Sell hardened library	Liability in case the library has an error	Faster development of quantum-secure products	Less advantage over competition

Table 10.2 Variation and recommendation for different sectors

	Military		Civil Society		Economy	
	Pros	Cons	Pros	Cons	Pros	Cons
Wait	No expense	Secrets will leak	Most easy solution	No e-voting	No cost	Liability issues
Hybrid	Maximum protection	Only feasible for the most sensitive data	More security	Only feasible for very few use-cases	Security and PR	Cost and need to follow development
Quantume-safe	Easier than hybrid	Might be broken	None	Hassle because it will need to change	None	Need to be updated

10.4 Conclusion

For the time being, symmetric encryption is secure and a quantum computer will not be able to create a significant speedup over classical computers for decrypting messages. However, the estimations of if and when a quantum computer capable of breaking RSA and Elliptic Curves will become available differ significantly between experts. As Fig. 10.1 indicates, not switching to quantum-safe algorithms would mean that long-term secrets might get compromised. For this reason, switching to quantum-safe algorithms is critical for data that must remain secret for years (e.g., military secrets or e-voting data). For all other data, it is crucial to ensure that systems are at least crypto-agile (migration path exists) or already come with support for hybrid algorithms, primarily when they are widely used like SSH [8].

While a complete migration to quantum-safe algorithms will only happen after 2035 [11], the start for tests and migrating critical systems should start much earlier. For example, the military should start testing systems now and move systems requiring long-term security to quantum-safe algorithms well before 2035. The economy, more specifically banks, should start with testing at the latest in 2025 and also consider having done most of the adaption by 2035.

References

1. Erica Klarreich. Researchers Identify 'Master Problem' Underlying All Cryptography. https://www.quantamagazine.org/researchers-identify-master-problem-underlying-all-cryptography-20220406/, April 2022. Quanta Magazine.
2. National security memorandum on promoting united states leadership in quantum computing while mitigating risks to vulnerable cryptographic systems.
3. Quantum computing: Progress and prospects (2019) - chapter:4 quantum computing's implications for cryptography. https://nap.nationalacademies.org/read/25196/chapter/6#98, January 2019. Washington, DC: The National Academies Press.
4. Samuel Jaques. Landscape of Quantum Computing in 2021. https://sam-jaques.appspot.com/quantum_landscape, May 2021.
5. Post-quantum encryption algorithms under rigorous scrutiny: expect more hacks.
6. Post-quantum cryptography pqc - selected algorithms 2022. https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022, July 2022. NIST.
7. TLS Post-Quantum Experiment. https://blog.cloudflare.com/the-tls-post-quantum-experiment/, October 2019. The Cloudflare Blog.
8. Openssh 9.0 release. https://www.openssh.com/txt/release-9.0, August 2022.
9. Leaked nsa doc says it can collect and keep your encrypted data as long as it takes to crack it.
10. admin. Researchers' Quantum Threat Debunked, RSA Safe for Now. https://thenetworkcompany.net/researchers-quantum-threat-debunked-rsa-safe-for-now/, January 2023.
11. National Security Agency. Announcing the Commercial National Security Algorithm Suite 2.0, 2022.