# HOW CAN QUANTUM COMPUTERS AFFECT THE SECURITY OF DATA?

Moiz Saleem

## Introduction

Since the conception of the first modern computer system in 1937 (Mol, 2019), computer systems have advanced at an exponential rate, but the underlying principles behind their function have remained the same – until the conceptualisation of the first quantum computer. These systems use the quantum phenomena of superposition and entanglement to compute data using methods that differ from conventional computers (IBM, 2021), giving them unique properties that mean that quantum computers have the potential to provide us with limitless opportunities.

## Why is this an important topic?

The security of data is a concept critical for almost every aspect of society to function – banks, governments and whole industries operate off the principle that their data is kept secure using complex encryption methods and cryptography. However, due to the nature of quantum computers, they may have the ability to threaten the security of this data by having the potential to efficiently perform operations that would otherwise be impossible for conventional computers to complete in a practical amount of time – this has the capacity to threaten some of the principles that current cryptography methods operate using.

## Findings

A common encryption method used when communicating data is 2048-bit RSA encryption. It is an asymmetric encryption method, which means that it uses a public key to encrypt a message, and a secret private key to later decrypt the message so that it can be read again.

RSA encryption operates off the principle that it is a trapdoor function; it is relatively easy to compute the algorithm in one direction but to do it in reverse is almost impossible. This concept is used in creating the keys the algorithm uses. Computer systems are easily able to multiply two numbers, but it is much harder for the systems to reverse this process and factorise to get the original numbers back. As the numbers you multiply become even bigger, this process becomes even harder and it is considered practically impossible for a classical computer to factorise numbers that are longer than 2048 bits, which is what 2048-bit RSA encryption uses, therefore allowing for the secure transmission of data.

The principle that it is almost impossible to practically factorise a product of 2 large primes is what makes RSA encryption secure, but in 1994 Peter Shor, an MIT professor, proposed a quantum algorithm now named Shor's algorithm that could factorise any integer in a time and resource efficient manner that is impossible with conventional computers (IBM Quantum, n.d.). Shor's algorithm would then therefore be able to find the prime factors of the keys used in RSA encryption, which means that it would allow us to break RSA encryption. Shor's algorithm has a polynomial time complexity, while the problem on a conventional computer has an exponential time complexity, which means that a quantum computer with 4099 perfectly coherent qubits would be able to break RSA encryption in just 10 seconds, while it would take 300 trillion years for a conventional computer to complete the same task (Baumhof, 2019). Therefore, the currently secure RSA method would be under threat from a quantum system.

## Conclusions

While quantum computers do theoretically pose a threat to cryptography, currently there are no viable quantum systems that are advanced enough to do this, as there are still challenges with building useful quantum computers. However, with the rate of advancements being made outpacing even classical systems, there is a serious future potential threat to cryptography methods, and the danger that the encrypted data of today may be stockpiled in the hope of breaking the encryption in the future means that we could one day face disastrous implications.

## Bibliography

Baumhof, A., 2019. *Breaking RSA Encryption – an Update on the State-of-the-Art.* [Online] Available at: https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art/ [Accessed 23 August 2021].

IBM Quantum, n.d.. *Shor's algorithm.* [Online] Available at: https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm [Accessed 23 August 2021].

IBM, 2021. *What is quantum computing?.* [Online] Available at: https://www.ibm.com/quantum-computing/what-is-quantum-computing/ [Accessed 23 August 2021].

Mol, L. D., 2019. *Turing Machines.* [Online] Available at: https://plato.stanford.edu/entries/turing-machine/#Bib [Accessed 23 August 2021].