What Quantum Computing Means for the Future of Encryption

Alistair Horwood

June 16, 2021

What Quantum Computing Means for The Future of Encryption

Alistair Horwood
COMP1002 Foundations of Computational Intelligence
Flinders University, South Australia

horw0017@flinders.edu.au

Abstract

'Quantum Computing will end encryption as we know it is a very grabbing statement but is not the exact truth. This paper will research how quantum computing can break traditional public-key encryption and hence the future risks and social implications of the further evolution of this new generation of computing technology.

1 Introduction

Encryption methods help protect data in the digital world. This means that having your data in an encrypted state when it is being stored, sent and received is vital for the security of your personal information. As with any encryption method, raw data is hashed and turned into a seemingly random string of characters and sent somewhere. At the other end, this encrypted data needs to be put back into its unencrypted state to be read. With encryption methods such as RSA, the opposite mathematical operations used to encrypt are repeated. Because of how encryption works, it is always possible for someone to guess these operations and intercept the data. One method of doing this is to try every possible combination (also known as a brute force attack); this attack vector is time and resource-intensive on traditional computing architecture.

2 The RSA Encryption Method

Designed in 1977, the RSA (Rivest–Shamir–Adleman) algorithm is currently the most prevalent encryption algorithm used to create secure connections between web servers and their clients. The critical premise of encryption algorithms such as RSA is that they multiply two large prime numbers together; because of the laws of mathematics, it is straightforward for a computer to multiply these numbers together but is very hard for traditional computers to work backwards from the previously multiplied number back to the two prime numbers. Because of the premise of RSA, trying to brute force (guess) these two prime numbers are a challenge, and there is no way that the encrypted data can be broken into without first cracking the prime numbers.

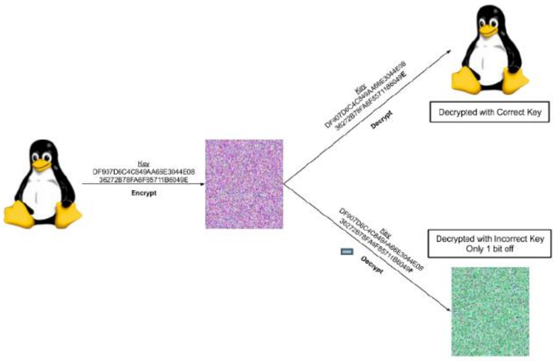
Key
DF907D6C4C849AA66E3044E08
36272B78FA6F85711B6049E
Encrypt
Key
DF907D6C4C849AA66E3044E08
36272B78FA6F85711B6049E
Decrypt
Decrypted with Correct Key
Key
DF907D6C4C849AA66E3044E08
36272B78FA6F85711B6049F
Decrypt
Decrypted with Incorrect Key
Only 1 bit off

Figure 1: Example of RSA encryption *(Source: J. Tibbetts, Quantum Computing and Cryptography: Analysis, Risks and Recommendations for Decisionmakers)*

As shown in *Figure 1*, the image on the left is encrypted with a private key and becomes a seemingly random image. One of the computers with the correct copy of the private key can decrypt the image and gain access to the original data. The other device uses the same encryption key, except it is incorrect by a single character; because of the algorithm used, this ruins the entire decrypting process, and hence the data is safe.

The general formula to encrypt data in the RSA format is the following:

$$\text{Key} = (m^e)^b (mod n)$$

With m, e, b and n being randomly assigned values and this equation evaluating to the public or private key. Even with e and n known, it is not easy to find the n value. (Sharma, Choudhary et al. 2020)

3 Quantum Computing

Quantum computers are fundamentally different from how a 'normal' computer works and operates. They can do this by instead not working with zeros and ones (bits and bytes) but qubits. This entirely different set of rules of how the central processing works allows them to be up to 8 orders of magnitude compared to their binary computer counterparts. (Arslan, Ulker et al.) This immediately puts the entire RSA and many other encryption methods at risk.

4 Brute forcing Algorithms & the Use of Quantum Computers

As discussed previously, brute-forcing the solution to data protected by RSA takes a while; this is because a computer needs to try every single number and depending on how large, it could take many centuries to complete. This is because every single calculation is completed separately using bits. In quantum computing, qubits can take on a superposition (not just a zero or 1), this allows a problem to be inputted, broken up into more minor problems, and then all of them run simultaneously and only produce a single value. Parallelism is based on the fact that all the guesses will interfere and cancel out, leaving behind a single possible solution.

5 Conclusion

Whilst quantum computers are not at a stage where they can use Shor’s algorithm to break standard RSA encryption in a short amount of time; it does not mean that everything is safe. Many attacks on personal data, including man-in-the-middle attacks, allow someone’s data to be downloaded; whilst this data is encrypted, nothing stops an attacker from downloading this data today and simply breaking it later when quantum computing has progressed to the stage you can rent server time. This means that how encryption is used and implemented on most of the internet needs to be rethought; previously created encryption algorithms that favour speed rather than security (such as RSA) need to be moved away to create cryptographically sound encryption; how powerful new computing architecture gets. (Tibbets 2019)

References

Arslan, B., et al. A study on the use of quantum computers, risk assessment and security problems, IEEE.

Bhatia, V. and K. R. Ramkumar An Efficient Quantum Computing technique for cracking RSA using Shor’s Algorithm, IEEE.

Fedorov, A. K., et al. (2018). "Quantum computers put blockchain security at risk." Nature 563(7732): 465-467.

Lanzagorta, M. and J. Uhlmann (2008). "Is quantum parallelism real?" Proc SPIE 6976.

Majot, A. and R. Yampolskiy (2015). "Global catastrophic risk and security implications of quantum computers." Futures 72: 17-26.

Mavroeidis, V., et al. (2018). "The Impact of Quantum Computing on Present Cryptography." International Journal of Advanced Computer Science and Applications 9(3).

Sharma, M., et al. (2020). "Leveraging the power of quantum computing for breaking RSA encryption." Cyber-Physical Systems: 1-20.

Tibbets, J. (2019). "Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decision-makers." Centre for Global Security Research.