Name: Edward Gray
Student Number: UP939720

What is Shor's algorithm?

In 1994 a scientist called Peter Shor created Shor's algorithm which is designed for use in a quantum computer and facilitates extremely efficient integer factorization as well as the solving of Discrete Logarithm problems. (Mavroeidis, Vishi, D. & Jøsang, 2018, p. 8) Using Shor's algorithm on a quantum computer is polynomial, whereas a factoring algorithm on a normal computer is exponential. (Hayward, 2008, p. 13). The normal computer's algorithm grows in complexity exponentially with larger numbers, meaning that factoring the large numbers used in asymmetric encryption algorithms is impractical, even in a best case scenario. Shor's algorithm on the other hand is much better at factoring large prime numbers because it does not experience such a tremendous increase in complexity. (Mavroeidis, Vishi, D. & Jøsang, 2018, p. 3).

What is Grover's algorithm?

In 1996 a scientist called Lov Grover created Grover's algorithm that is designed for use in a quantum computer to search an unsorted database on size N. When a normal computer searches a database of size N, it must make N/2 searches to find a specific entry. When Grover's algorithm is used in a quantum computer on the same database, it is capable of finding a specific entry in N operations. This is a considerable increase in speed and can be used against symmetric key encryption to find the correct key in fewer cycles. (Mavroeidis, Vishi, D. & Jøsang, 2018, p. 3).

How will the security of asymmetric algorithms be affected?

There have been numerous papers published that discuss how badly asymmetric algorithms will be compromised following the creation of a general purpose quantum computer. [examples here] The ability to use Shor's algorithm means that most widespread asymmetric algorithms such as RSA will be compromised.(Mavroeidis, Vishi, D. & Jøsang, 2018, p. 2). Not all Asymmetric algorithms are affected however, there are 2 asymmetric algorithms that could be suitable replacements. Bernstein & Lange, 2017, p. 190-191). These alternative algorithms use mathematical problems that are not susceptible to any quantum algorithms for them although they each have their drawbacks making it a common topic of debate.

The first type is Lattice based cryptography. The security of lattice encryption schemes can differ considerably depending on the implementation and as a result of this early versions of the system where the victims of attacks that could compromise the algorithm if a key size of insufficient length was used. The resulting versions of the algorithm suffered from large key sizes although the keys are still relatively short and efficient to compute. (Bernstein & Lange, 2017, p. 4). There is one implementation of lattice encryption called NTRU that appears to be a viable choice for replacing RSA as a quantum-safe asymmetric algorithm. NTRU has other advantages, aside from being Quantum-Safe and efficient - It's also highly parallelizable making it a good replacement for RSA. (Chen et al., 2016, p. 8-9).

The second type is Code Based cryptography. Error correcting codes are algorithms used in server RAM where data integrity is crucial and allows for the recovery of data that has been corrupted. This can be used to conceal messages by applying errors to them. (Chen et al., 2016, p. 9).The algorithm works as such. The client has a message that they encode and then add noise to it, or partially corrupt it in a way that allows the recipient's algorithm to decode it. The host has an Error Correction Algorithm that can correct certain errors. The client knows what errors can be corrected by the host. When the client wishes to send a message to the host, the client will encode their message into a bit

stream and apply a specific amount of noise to the bit stream. When sent to the host, it is impossible to decode this message without the host's error correcting algorithm. (Bernstein & Lange, 2017, p. 3). This has a similar effect to XOR in theory because it combines a binary message with a specific amount of noise that only the host's algorithm can reverse. The oldest most popular implementation of this method is called McEliece after the creator Robert McEliece. The primary advantage of this algorithm was quick execution, although this was counteracted by a relatively large key size. (Chen et al., 2016, p. 9). There are multiple cryptographic implementations of this protocol that try to introduce a more rigid structure to shorten the key length. Whilst this had some effect, it introduced flaws into the algorithms. The original McEliece algorithm was created in 1978 and has been tested for flaws extensively since it's creation with none being found as of 2020. (Bernstein & Lange, 2017, p. 3).

How will the security of symmetric algorithms be affected?

Symmetric algorithms do not use complex mathematical problems as the basis of their security - they instead use the same key for encryption and decryption. This means that to decrypt the message without the key you must keep generating and trying keys until you eventually find the right key. Grover's algorithm can be used to search for the key in fewer tries, although this does not entirely compromise the security of the asymmetric algorithm. (Bernstein & Lange, 2017, p. 2). Multiple papers have discussed this and the consensus is that Grover's algorithm has approximately the same effect as halving the key size would have on an algorithm. If we wish to keep symmetric algorithms safe in the post-quantum age, we would simply need to double the key size used in an algorithm to keep it safe. (Bernstein, 2010, p. 1).

Bibliography:

Bernstein, D., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 189-192. doi: 10.1038/nature23461

Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography (pp. 2-7).

Mavroeidis, V., Vishi, K., D., M., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. International Journal Of Advanced Computer Science And Applications, 9(3), 1-6. doi: 10.14569/ijacsa.2018.090354

Hayward, M. (2008). Quantum computing and shor's algorithm. Sydney: Macquarie University Mathematics Department, 13-14.

Bernstein, D. J. (2010, May). Grover vs. mceliece. In International Workshop on Post-Quantum Cryptography (pp. 73-80). Springer, Berlin, Heidelberg.