Post-Quantum Cryptography, A Window Into The Future

Author: Jean-Michel Batista

Supervisor: Dr Derrick Newton

Introduction

Cryptosystems are a vital aspect for achieving secure communications in today's modern world. The vast majority of technological devices that surround our society such as cell phones, cars, and computers make use of cryptography in order to maintain confidentiality between two or more communicating parties. However, cutting-edge advances in technology have allowed for the continuous development of quantum computers, creating a race-against-time problem that surrounds the question of not if, but when quantum computers will make the most commonly used cryptosystems obsolete. Consequently, the demand for cryptosystems to remain secure and flexible in the event an attacker has a powerful quantum computer is leading the research area and development of post-quantum cryptosystems. This report will aim to extend your knowledge and understanding in this subject by carrying out a comprehensible literature-based research.

Main

A common attribute that is given to current and future quantum computers is the processing speed at which they are able to perform mathematical operations to solve extremely difficult problems, a speed our current normal computers would never achieve. Post-quantum cryptography is a hypothetical area of cryptography that assumes a potential attacker has the resources and ability to use a powerful quantum computer to break commonly used cryptosystems, it thus strives in identifying mathematical operations where quantum computers would not have an advantage in terms of speed in order to build post-quantum cryptosystems (Bernstein et al., 2017).

Quantum supremacy

The race for quantum supremacy is a relatively recent topic, but one that should not be ignored. Private companies such as Google and entire countries such as China are continuously working to stay competitive in the quantum computing race. In 2019, the company Google had claimed to achieve a quantum leap in computer science and claimed quantum supremacy; with their newly developed quantum computer called Sycamore, Google claimed to perform complex calculations 1.5 trillion times faster than the world's most powerful known supercomputers (Childers, 2019). Nonetheless, Google's reign on quantum supremacy only lasted a year before China reported their quantum computer called Juizhang being 10 billion times faster than

Google's Sycamore (Letzter, 2020), showing us the monstrous speed at which quantum computers are currently evolving. The phenomenon we are living now with quantum computers is objectively a race for power and not only does it affect science, it also affects everything surrounding it as there are shaking socio-political and economical consequences that come with it, it is arguably the space race or the nuclear arms race of our modern day and age. The quantum computing market is projected to reach $64.98 billion by 2030 compared to $507.1 million in 2019 and it will only keep growing as it has the potential to become a multi-purpose standard in the future for never seen before sophisticated advances in research as well as technological attacks and defenses (Robison, 2021).

Power^{qubits}

Intuitively, quantum computers can achieve an exponential growth in computing power the more qubits they have at their disposal. Unlike bits used in normal computers, qubit values can be both 0 and 1 at the same time, a phenomenon known as quantum superposition and a fundamental principle of quantum mechanics (Dirac, 1930). The superposition of qubits is managed by quantum algorithms, which will in turn make transformations of the probabilities characterized by the state of superposition of the qubits and create quantum states, or, in simpler terms, complex numbers that can't be achieved outside the quantum spectrum (Weinberg, 2002). However, it is estimated that a quantum computer would require thousands if not millions of qubits in order to make cryptosystems used in today's world entirely obsolete (Aumasson, 2017), creating a problem of not if but when will quantum computers be capable of such achievement.

Public-Key Cryptosystems

The era of large-scale quantum computers is expected to be the end of all widely used public key cryptosystems currently in use, these include ECC, RSA and Diffie-Hellman as they make use of the integer factorization and discrete logarithm problems (Paar & Pelzl, 2010) that would take very long for a normal computer to solve, but fast for a quantum computer to solve. The proof of concept to break public-key cryptosystems exists as Shor's algorithm, a polynomial-time quantum computer algorithm which can efficiently solve integer-factorization problems public-key cryptosystems are based on (Shor, 1994). In terms of reliability, Shor's algorithm falls in the bounded-error quantum polynomial-time complexity class due to an error probability of ⅓ for all instances (Nielsen & Chuang, 2000) which remains a very reliable margin. If a security system had a chance to be exploited every ⅔

time it would not be secure at all as the confidentiality and integrity of the system would be non-existent.

Symmetric Cryptosystems

Other known symmetric-key cryptosystems such as AES, Salsa and SHA will also be affected by quantum computers, but not on the same scale of Shor's algorithm and public-key cryptosystems. The proof of concept that most symmetric-key cryptosystems will have the effectiveness of their security level halved exists as Grover's algorithm, a quantum algorithm that makes use of function inverting mathematical properties to find out the root of a function (Grover, 1996). Taking the advanced encryption standard (AES) as an example, a secret 128-bit AES key $\boldsymbol{k}$ has a security level of 2^{128}, meaning that it would take 2^{128} steps to crack or billions of years for today's available computers (Daemen & Rijmen, 2002). The quadratic speed-up that can be achieved through Grover's algorithm allows the algorithm to find the root of a secret 128-bit AES key function using approximately 2^{64} quantum evaluations of the function, effectively halving the amount of time needed to crack the cryptographic key (Bernstein & Lange, 2017). However, Grover's algorithm does not impact all symmetric cryptosystems and symmetric ciphers such as AES-256 have been categorized as quantum resistant because of the unfathomable computational power and time that would be required to crack a 256 bit key, so doubling the key size can effectively block quantum computing attacks (Bernstein. (2010).

Quantum resistant cryptosystems

Because there is a real-time demand to understand the long term impact of quantum computers on cryptography there is also a demand to develop and standardize post-quantum cryptosystems that can withstand their integrity assuming they are attacked by a quantum computer. Post-quantum cryptosystems are designed with the assumption an attacker has unlimited computing power, which has led to different approaches that could be implemented into existing systems in the future. These approaches include lattice-based cryptography, multivariate cryptography and hash-based cryptography among others (Bernstein, 2019). Below we will review two examples.

Lattice-Based Cryptography: NTRU Encryption

Novel quantum resistant approaches such as NTRU encryption include lattice-based cryptographic constructions that make use of the shortest vector problem, which requires to approximate the minimal Euclidean length of a non-zero lattice vector (Miklós, 1996). According to Berstein (2017), given a lattice **L** in 2p-dimensional space containing a point close to (0,c), namely (d, c - e) where **d** and **e** are two secret polynomials, an attacker's problem would be to find the hidden secrets **d** and **e** within a point of a high-dimensional lattice. This method of encryption has achieved quantum resistance by using a public key represented as a degree 613 polynomial with coefficients mod(2^{10}), resulting in a 6130 bits public key and a 6743 bits private key (Hirschborrn et al., 2014) to achieve 128 bits of security. Despite the relatively young development of the NTRU cryptosystem it has found implementations in the financial services industry as a standard due to its speed and low memory usage (Robinson, 2011) so it might not be long before this method of encryption extends to other industries.

Multivariate Cryptography: Rainbow Signature

The Rainbow Signature is one out of four multivariate cryptography signature schemes that has made its way past the first round of NIST's post-quantum cryptography competition (Moody, 2019). These schemes are based on multivariate polynomials over a finite field, multivariate polynomial equations have been proven to be NP-complete (Garey, 1979) and they have been categorized as excellent solutions for quantum secure digital signatures (Ding & Schmidt, 2005). When compared to lattice-based cryptography, Rainbow's signature will achieve the same amount of bits of security with smaller keys, meaning that it has the potential for easier implementations as a cryptosystem.

Results: Pre-quantum vs Post-quantum Public key cryptography

$b=2^b$ steps to break

Name	Function	Pre-quantum security level b	Post-quantum security level b
DH-3072	**Key exchange**	**128b**	**Broken (Shor)**
DSA-3072	**Signature**	**128b**	**Broken (Shor)**
256-BIT ECDH	**Key exchange**	**128b**	**Broken (Shor)**

256-BIT ECDSA	**Signature**	**128b**	**Broken (Shor)**
RSA-3072	**Encryption**	**128b**	**Broken (Shor)**
RSA-3072	**Signature**	**128b**	**Broken (Shor)**
NTRU	**Encryption**	**128b**	**128b (No impact)**
Rainbow	**Signature**	**128b**	**128b (No impact)**

Results: Pre-quantum vs Post-quantum symmetric key cryptography

---

$b=2^b$ steps to break

Name	Function	Pre-quantum security level b	Post-quantum security level b
SHA-256	**Hash function**	**256b**	**128b (Grover)**
SHA3-256	**Hash function**	**256b**	**128b (Grover)**
Salsa20	**Symmetric encryption**	**256b**	**128b (Grover)**
AES-128	**Symmetric encryption**	**128b**	**62b (Grover)**
AES-256	**Symmetric encryption**	**256b**	**128b (Grover)**
GMAC	**MAC**	**128b**	**128b (No impact)**
Poly1305	**MAC**	**128b**	**128b (No impact)**
Merkle Trees	**Hash Function**	**128b**	**128b (No impact)**

Conclusion

There is no date for when to expect the availability of a powerful enough quantum computer that will break our widely implemented cryptosystems, the one thing that remains true is that it will happen. Multiple other public-key cryptosystems such as NTRU and Rainbow's signature are being developed with the goal of being implemented on a world-wide scale. Doubling the size of symmetric-key cryptosystems has been recommended to be efficient against quantum computing attacks based on Grover's algorithm, however, other symmetric-key cryptosystem solutions that are naturally quantum resistant such as GMAC, Poly1305 and Merkle Trees might be a better option in the long term. The race to develop stronger quantum computers goes hand in hand with the race to develop quantum resistant cryptosystems, we can't know for sure how things will turn out as we are limited to technological advances both in computing and cryptography, but at least we have an idea of what to expect, a window into future.

References

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194. doi:10.1038/nature23461

Childers, T. (2019). Google's Quantum Computer Just Aced an 'Impossible' Test. Retrieved 19 April 2021, from https://www.livescience.com/google-hits-quantum-supremacy.html

Letzter, R. (2020). China claims the fastest quantum computer in the world. Retrieved 19 April 2021, from https://www.livescience.com/china-quantum-supremacy.html#:~:text=That%20suggests%20the%20quantum%20computer,milestone%20on%20the%20way%20there.

Robison, K. (2021). Here's how quantum computing could transform the future. Retrieved 19 April 2021, from https://www.businessinsider.com/quantum-computing-investing-computers-enterprise-2021-3?r=US&IR=T#:~:text=Big%20companies%20are%20investing%20in%20quantum%20tech&text=reverse%20climate%20change.-,The%20quantum%20computing%20market%20is%20projected%20to%20reach%20%2464.98%20billion,just%20%24507.1%20million%20in%202019.

Dirac (1947). *The Principles of Quantum Mechanics*(2nd ed.). Clarendon Press. p. 12.

Weinberg, S. (2002), *The Quantum Theory of Fields*, I,Cambridge University Press, ISBN 978-0-521-55001-7

Aumasson, J.-P. (2017). The impact of quantum computing on cryptography. Computer Fraud & Security, 2017(6), 8-11. doi:https://doi.org/10.1016/S1361-3723(17)30051-9

Paar, Christof; Pelzl, Jan; Preneel, Bart (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer. ISBN 978-3-642-04100-6.

Shor, P.W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring". *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press: 124–134. doi:10.1109/sfcs.1994.365700. ISBN 0818665807.

Nielsen, M. and Chuang, I. (2000). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press. ISBN 0-521-63503-9.

Grover, L. K. (1996) A fast quantum mechanical algorithm for database search. In *Proc. 28th Ann. ACM Symp. on Theory of* Computing (ed. Miller, G. L.) 212–219 (ACM, 1996)

Bernstein. D. J. Bernstein. (2010). "Grover vs. McEliece"(PDF).

Daniel J. Bernstein (2009). "Introduction to post-quantum cryptography" (PDF). *Post-Quantum Cryptography*.

Hirschborrn, P; Hoffstein; Howgrave-Graham; Whyte. (2013). "Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches" (PDF). NTRU. Archived from the original (PDF) on 30 January 2013.

Miklós, Ajtai. (1996). "Generating Hard Instances of Lattice Problems". *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. pp. 99–108. CiteSeerX 10.1.1.40.2489. doi:10.1145/237814.237838. ISBN 978-0-89791-785-8. S2CID 6864824.

Moody, D. (2019). "The 2nd Round of the NIST PQC Standardization Process". NIST.

Ding, J. Schmidt, D. (2005). "Rainbow, a New Multivariable Polynomial Signature Scheme". In Ioannidis, John (ed.). *Third International Conference, ACNS 2005, New York, NY, USA, June 7–10, 2005. Proceedings*. Lecture Notes in Computer Science. 3531. pp. 64–175. doi:10.1007/11496137_12.ISBN 978-3-540-26223-7.