International Journal of Advanced Trends in Computer Applications
www.ijatca.com

The Fate of Cryptography in a Post-Quantum World

[1]Udugahapattuwa D.M.R, [2]Amarathunga A.A.S.R, [3]M.A.D.S.R.Perera
Faculty of Computing – Cyber Security Department,
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka
[1]manula.udugahapattuwa@my.sliit.lk, [2]sandun.amarathunga@my.sliit.lk, [3]roshli.perera@my.sliit.lk

Abstract: *When the rate of technological advancement is considered, it is clear that a Post-Quantum World is inevitable. Trying to prevent or delay the advancement of Quantum Technology is not the answer as it could be the silver lining to today's science fictional ideology such as achieving speed of light, time traveling and also the next level of machine learning. But it will be the demise of all cryptosystems available today. The only solution available is to evolve, adopt and adapt to Post-Quantum Cryptosystems. The intention of this paper is to provide an insight on the probable scenarios that may occur in a Post-Quantum world, the solutions for arising issues and to provide our own input in how to manage such technology with the main focus on cryptography.*

Keywords: Cryptography; Post-Quantum Cryptosystems; Quantum Technology; Evolution of Cryptography; One Time Signature.

I. INTRODUCTION

Cryptography is made of two Greek words Keyptos and Graphos which implies Secret Writing. In other words Cryptography is the exploration of Secret Writing. Main focus point of the cryptography is to shield information from unapproved parties. [1] A Cryptosystem has two operations. They are Encryption and Decryption. Cryptanalysis is the investigation of breaking down approaches to crack cryptography. Current computers utilize bits to store information as binary 1 and 0. Quantum computers utilize Quantum bits (Qubits) which can store more data than bits because of the fact that Qubits have a physical phenomenon called superposition and entangled states. Using Quantum computers we can easily solve mathematical problems. As an example we can find large prime numbers, which plays a major role in cryptography. As a result of that quantum computers leads to crack existing public key cryptosystems. That makes a huge demand for new cryptography methods which are resistant to quantum computing. Only then we can ensure the data security over the internet in the future.[3]

II. LITERATURE REVIEW

A. Basic Evolution of Cryptography

There are three significant periods of cryptography:

Period	*Duration*
Ancient Period	until 1918
Technical Period	1919-1975
Paradoxical Period	From 1976

Table 1: Periods of cryptography

a. Ancient Period

Cryptography can trace back to 3500 B.C. where Egyptians developed hieroglyphic writing. They developed it not to hide but tell stories. Hebrew scholars were noted to have Atbash cipher in 600B.C. It is a simple mono-alphabetic substitution cipher. This is done by reversing the alphabet. 1st military cryptographic device was scytal. It was used by spartan in 500B.C. to implement transportation cipher. Mono-alphabetic substitution cipher is a method which has one to one or one to many relationships between plain text and the cipher text. Having one to many relationships makes the scheme more attack resistant. Frequency analysis is then introduced in 9th century by Abu Yusuf Ya'qub al-Kindi. It had the ability to break mono-alphabetic substitution. This way of encryption concerns about the statistical distribution of letters in cipher text and average distribution of letters in a language. Polyalphabetic substitution cipher is a way which uses more than one alphabet and switching

between them. Vigenere cipher is a popular polyalphabetic substitution cipher invented in 16th century and unbreakable for almost 300 years.[2] Then Friedrich Wilhelm Kasiski cracked Vigenere cipher. Kasiski's method is a strong cryptanalysis way against Vigenere cipher.[1]

b. Technical Period

During World War I, mechanical machines were used to do the encryption. Encrypted messages were all over the air using radio transmission. Germans' Enigma was the most famous cryptographic device in this period. This had 10,000,000,000,000,000 number of different states. Finally Poland mathematician Rejewski cracked this device. In 1975 Data Encryption Standard (DES) was introduced by IBM. Initially it had a 128-bit key size and then NSA reduced it to 56-bits. DES is proven to be strong standard for 20 years. In 1998 DES was cracked. Triple-DES introduced. Then Rijndael designed Advanced Encryption Standard (AES) in 2001. [1]

c. Paradoxical Period

Public key cryptography was introduced. It is also known as asymmetric cryptography. It uses two keys. They are public key and private key. Public key mainly use to encrypt a message and public key uses to decrypt a message. RSA (Rivest–Shamir–Adleman) is a popular asymmetric algorithm. RSA key size is between 1024bits – 4096bits. 768-bit key has been broken using today's computer power. Latest cryptographic topic is Quantum Cryptography.

B. Quantum Computing

The idea of quantum computing was came through by an American theoretical physicist Richard Feynman in 1982. It's an idea where a computer uses the effects of quantum mechanics to its advantage. In quantum mechanics it works with the mathematical description of interaction of sub atomic particles, assimilating the concepts of quantization of energy. In day-to-day computers each and every process works in bits which is represented using ones and zeros but in quantum computers instead of bits it uses quantum bits which are also referred as qubits. The difference between bits and qubits is, a qubit is a two-state quantum mechanical system which is known as superposition. In quantum computers they take the advantage of this to solve complex problems. The physical phenomenon of quantum entanglement is used in quantum computers which provide true parallel processing power. The combination of superposition and quantum entanglement can process exponential increase in one single operation. Which means n-qubit quantum computers can process two operations inparallel.

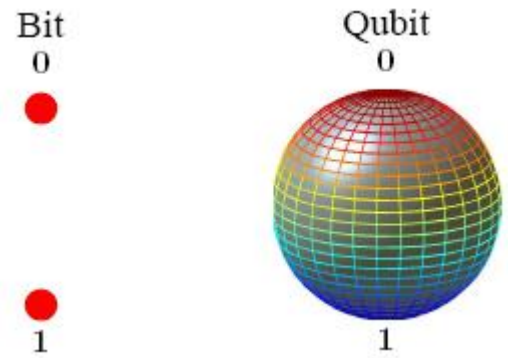


Figure 1: Bit vs Qubit

Quantum computers fall under two categories known as Universal and Non-Universal. The difference in between these two types is that Universal Quantum computers are built to do any task while Non-Universal Quantum computers built to perform a specific task.

In accordance to Bone and Castro Quantum computer is a completely different in design than a regular computer which is made up of transistors and diodes. Many researchers were done based on quantum dots and computing liquids. But according to researchers multiplication on quantum computers will not be faster than a regular computer instead it will be very similar to a regular computer.

When universal and non-universal quantum computers are available and able to perform in maximum capacity the prevailing cryptosystems will be broken in matter of hours or even minutes. There will be no security or authenticity in any data flow that takes place in a network. This will be the main issue that has the most negative impact when it comes to Quantum Computing.

C. Solutions for the Problem

Post quantum cryptography is also known as Quantum resistant cryptography. The proposition is to flourish a cryptographic system which is resistant against quantum computers but still compatible with all breathe communication protocols and networks. At the moment both NIST is taking several steps to come up with some standards for the implementation of post quantum cryptographic systems [4]. NSA already announced plans to mitigate their cryptographic standards to post-quantum cryptography [5].

In this section some main algorithms which for post quantum cryptography is been explained.

i. Lattice-Based Cryptography

Asymmetric cryptography is already a part of the cryptographic systems prevailing in the current days.

Lattice-Based cryptography is the use of mathematical calculations built upon lattices with the concepts of asymmetric cryptography. As the context of the paper has already highlighted, advancement of quantum technology will be the demise of all current cryptographic systems. The solution or the ideology to protect the world against the god like abilities of quantum computing is to find an extremely complex calculation that will take a considerable amount of time for a quantum computer to break or solve[7].

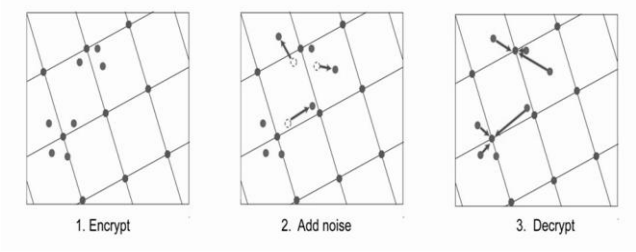


Figure 2: Points placed in identical sarroundings [2]

A lattice is a regular point arrangement which can be 1, 2 or 3 dimensionally placed in identical surroundings. The use of mathematical concepts behind the lattices fall into an area of mathematics named as the geometry of numbers. The possibility to use lattices to develop a cryptographic primitive was brought forward by Miklos Ajtai.[8] A workable primitive equation based on public key cryptosystem was then constructed by him and Cynthia Dwork. They combined several extremely hard problems such as the shortest vector problem and closest vector problem which can be found in lattice a lattice in R^n, to construct a one way function.[8] A one way function is a process which can convert a value to another easily but the resulting value cannot be reversed. A trap door is usually introduced into such functions which can be opened using a key and is the way to decode the cipher.

Example definition for a problem used in Lattice-based cryptosystems [7]: Shortest vector Problem: If given an arbitrary basis B of a lattice given as $\mathscr{L}$ find the shortest non zero lattice vector where $\mathscr{L} = \mathscr{L}(B)$.

A feature of a good cryptosystem is to have security proof as to how complex the underlying mathematical problem is. When it comes to Lattice based cryptographic protocols, there are two types. Practical proposals which are proved to be efficient and can be implemented in real life, lack true support for security proof. Even though the complexity is way beyond generally used problems such as discrete factorization and discrete logarithms [9], the complexity of these lattice based systems cannot be numerically measured simply due to the fact that there exist no quantum computer which can perform in full capacity, yet. The second type is the theoretical worst case lattice problems which guarantee security proof due to its extreme complexity. But the drawback is not being able to implement them in a practical scenario. Nonetheless Lattice-Based Cryptography is a potential solution to keep the field of cryptography intact in a post quantum world.

There are several cryptosystems already using lattice problems. Not all of them may be able to successfully build a barrier for quantum processors but the development and constant experimenting will polish them into good cryptographic algorithms to face the post quantum world. Some of such cryptosystems are:

a. Ajtai's and The Ajtai-Dwork cryptosystem

Technical Insight[7]: The public key of the Ajtai algorithm is a random instance $\{y_i\}$. The private key is its solution s derived from the hidden hyperplanes problem. When encrypting a single bit, it generates either a random point in $\mathbb{R}^n$ if it is a 0, or the sum of points from the subset $\{y_i\}$ if it is a 1. After encryption, the point resulting is either far or close to one of the hidden hyperplanes H_j. Using the secret key, the receiver can deduce between these two possibilities and thereby decrypt the cipher simply by computing whether <s,y> is close or far to an integer.

b. Goldreich-Goldwasser-Halevi cryptosystem

Technical Insight [7]: When encrypting with GGH, the sender takes the public key and uses it to choose a random point v in a lattice vector such that $v \varepsilon \mathscr{L}$. Then the sender sums the chosen point v with a small error e $\varepsilon\mathbb{R}^n$. Now the cipher text would be $c = v + e\ \varepsilon\mathbb{R}^n$. When decrypting, the use of bounded-distance decoding problem should be solved which is the point where a quantum processor may fail. For the function to work, the error introduced by the sender should still make the c value closer to v than to any other point in the lattice [7].

c. NTRU family of cryptosystems

Technical Insight: Uses a polynomial ring basis constructed using algebraically structured lattices. This was the first system to use such a base to build the cryptographic properties upon. The encryption is achieved using the public key h multiplied by a blinding factor (noise) (figure 1) [8] and adding a small error e to get the cipher $c = h \cdot r + e\ \varepsilon\mathbb{R}^n$. Decryption is done using the function $c \cdot s = 2g \cdot r + e \cdot s \varepsilon R_q$ where s is the secret key. NTRU is practical as well as efficient as it uses compact keys. But as discussed previously, with practicality, comes lack of concrete security [7].

ii. Multivariate Cryptography

Post quantum cryptography basically introduced to prepare for the quantum computer world. In other words, ubiquitous computing world. Multivariate cryptosystems has public keys which are a set of multivariate functions. This is based on 20th century mathematics (Algebraic Geometry - Theory of Polynomial Rings). When the system (P) is the public key, Q is the original system and the S and T from the secret key.

This is built from an easy to solve Q(x) = y, the central map. It is hidden by affine transformations S:wx and T:yz to get P by composing with Q.

When the public map P, or trapdoor one way function, is given as a set of m polynomial of a small degree d equations over n variables in a finite field F. The alternate name for this is "Multivariate Quadratic" (MQ) because usually d=2.

For a user to decrypt, authenticate or digitally sign For a given m-tuple where $z = (z_1,...,z_m)$ is respectively the hash of the message to be signed, the challenge and the cipher text have to find the solution for $w = (w_1,...,w_n)$ which is respectively the message signature, response and the plaintext. The system;

$$(\mathcal{P}) \begin{cases} p_1(w_1, \ldots, w_n) = z_1 \\ \cdots \\ p_m(w_1, \ldots, w_n) = z_m \end{cases}$$

When the secret key is unknown it should be impossible to get the plaintext from the cipher text (decrypt) forge the digital signature or authenticate. That's the basic definition of this cryptosystem.

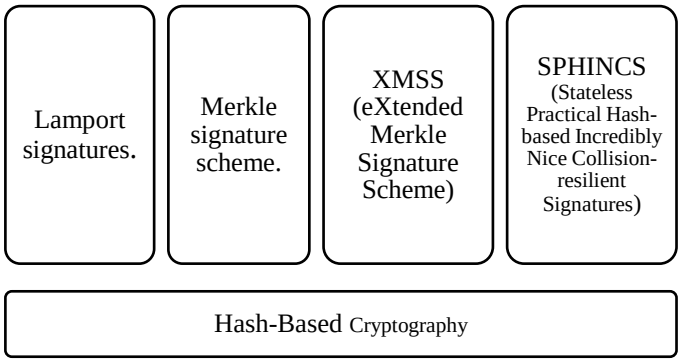
Applications: There are many applications of multivariate public key schemes such as C*, Hidden Field Equations (HFE), Unbalance Oil and Vinegar (UOV), Rainbow/TTS, Intermediate Field System (IFS), but unfortunately most of them have been broken.

Implementations: Multivariate cryptography is significantly fast in both public and private maps. As an example Rainbow/TTS are one of the fastest scheme for digital signatures which can be implemented cheaply on ASICs. Also this scheme has short signatures as in QUARTZ. It allows upto 100 bits. Multivariate scheme is a flexible in the design with ad-hoc properties.

Issues: Key size is large and it is uncertain about its security. When we say about the resistance it the implementation it relies on the results of all known attacks. It is difficult to manage large keys and continue optimize on current hardware. [6]

iii. Hash-Based Cryptography

Hash based cryptography includes several cryptographic systems;



Ralph Merkle invented hash based digital signatures during late 1970s thenceforward studies on hash based cryptographic systems were done and a replacement for number-theoretic digital signatures were emerged. But the limitation is on the number of signatures that can be signed using the corresponding set of private keys therefore the interest was less but the resistance to attack by quantum computers changed it.

In this section in detailed description on Lamport signature scheme is introduced and it's based on the research of [12]. Lamport signature scheme is invented in 1979 by Leslie Lamport. The desired security level of a system is described using a parameter b. Hash function takes an arbitrary length input and facilitate an output of 256 bits, to have a security level of 128-bits.
Private Key Generation: - using a RNG (Random Number Generator) 256-bit pairs of random numbers are generated. The generated total is 2256256=16 KB. Which means the private key consists of 8b2 bits.

Public Key Generation: Generated private keys are hashed and 512 different hashes are generated each of length 256-bits. The public key also consists of 8b2 bits.

Next the message is signed. For this process for each bit of a hashed message m, a number is chosen which encompasses the private key. In consequence there will be a sequence of 256 numbers. This number sequence will be the digital signature that will be published along with the plain text message. Then it'snot worth to use the private key again and the remaining 256 number pairs should be destroyed (Lamport one-time signature).

For the verification process the recipient calculates the hash of the message, for each bit of the hashed message corresponding hash from the public key is chosen. The recipient hashes each number of the sender's private key and it should be same as the same sequence of hashed value with the recipients chosen public key value. The security of the system be contingent on only if the private key is used once. It's almost impossible to forge a new valid signature because an adverse can only retrieve fifty percent of the private key.

Channing can be used to sign more than one message. A newly generated public is included in the signed message by the signer to verify the receiving next message.

With the combination of Witernitz's OTS (One Time Signature) and binary trees Markle introduced a new approach. The binary tree which consist of nodes and each node represents the hash value of the concatenation of the of the child nodes. The leaf nodes includes an OTS which is used for the signing process. The public key is the root node which is the first node in the hierarchy. That public key can verify the OTS in the leaf Nodes.

XMSS and SPHINCS are under evaluation for standardization. XMSS is a state-full signature scheme while SPHINCS is a stateless signature scheme.

III. METHODOLOGY

- ***Selecting a suitable research area***

We surfed through the internet and came across some research areas on cryptography. With the help of Wikipedia we acquired basic knowledge on these research areas to find out what will be the next big phenomena that will arise in the tech world based on cryptography. Post Quantum Cryptography was an interesting area we already had an idea about through the lectures. Thus we chose to work on what the fate of cryptography will be, in a Post-Quantum World.

- ***Information Gathering***

We came across some research papers based on the topic that we selected. We found some web sites and blogs which provide useful information on post quantum cryptography. After gathering that information we tried to link each data that we found and we created a simple map of the research area. Finally from the information we gathered and with the knowledge that we gained from course content we came up with this report.

IV. RESULTS AND DISCUSSION

The dawn of a post quantum world will not take long. According to studies and in depth calculations taking the rate of technological advancement into account, a functional quantum computer that will be able to function in its full capacity will be built by the year 2035 [7].

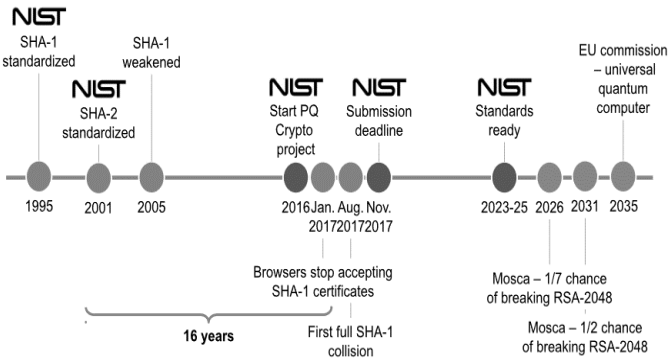


Figure 3: Cryptographic timeline by NIST

It is horrific to even imagine a scenario where the world reaches a time where quantum computing is a reality but cryptographic systems are not up to par. [10] None of the data passed through the internet will be safe from attackers. Interception will only take a matter of minutes or seconds. All the available classical encryption techniques will not be strong enough to fight a quantum processor. An example for a worst case scenario would be a successful hacking attempt to gain the private key of a Root Certificate Authority. [10] The human kind will have to give up technology given that the concept of IoT [11] is already in place which contains an uncountable number of vulnerabilities even in the smart refrigerators used in common households. The world will go back to analog unless a worthy cryptosystem to fight a quantum computer is developed.

With this mental image in mind, the professionals in the industry have taken steps to accompany different types of mathematical problems that may challenge a quantum processor. The effort is to build a primitive cryptologic function that can withstand enormous calculation power.

When it comes to practicality [7] as mentioned before, the currently available post quantum cryptosystems have a trade-off. With practicality the lack of security proof arises. When the security proof is concrete, the practical nature diminishes. But the bright side is that 17 years prior to the 1st predicted full scale Quantum computer (2035), the scientists are already in route to perfecting post quantum cryptosystems. Hopefully there will be a practical and efficient encryption method that has concrete security proof before the dawn of a Post-Quantum World.

V. CONCLUSION

When going through all the mentioned points, predictions and facts, it conveys and highlights the idea that the quantum technology is inevitable. It will be foolish to give up or prevent quantum advancement as even if it may cripple the prevailing cryptosystem, such computational power maybe the key to a new phase of human kind. It might be the single ingredient required to achieve speed of light, time travel [9], advanced artificial intelligence and many other ideologies that fall under science fiction in this 21st century. Thus the one and only solution to stay strong in a post quantum world is to come up with a post quantum cryptographic system.

The vision or the suggestion that can be introduced via this paper is that, it would be time saving, more efficient and secure if the new ideologies such as lattice problems are used along with the classical or prevailing cryptosystems. This can be called a hybrid cryptosystem where pre-quantum and post-quantum algorithms work together, entwined with the different technologies specific to each. Even though the classical systems are no match for the quantum processors, the ideas behind them such as key exchanging, authentication mechanisms and signing can still be used rather than introducing alien mechanisms. The advantage of using prevailing mechanisms is that the vulnerabilities are known. A zero day vulnerability arising in an already used mechanism is rare. To conclude, the authenticity of the data transferred through internet, is based on how well the private key of the Root Certificate Authorities (CA) are secured. Thus, to protect the future in a Post-Quantum World, the very first and obvious initiative required is to find the cryptosystem with maximum concrete security proof and apply it to Root CA private keys. In preliminary stages of a post quantum world, we suggest that the governments register the quantum computers in use within the country and create policies and do audit trail check regularly. It will require a new set of rules for quantum computer based attacks and disruptions along with brand new policies on proper use of this technology.

Acknowledgment

This work was supported by the Cyber Security lecturer panel at Sri Lanka Institute of Information Technology, Sri Lanka. Special overlook and cryptography knowledge was induced to us by Mr.KavingaYapaAbeywardena.

References

[1] Waqiyuddin, M. (2007). Evolution of Cryptography.
[2] Staff, S. (2018). Cryptography. [online] Cs.wellesley.edu. Available at: http://cs.wellesley.edu/~cs110/reading/cryptography.html [Accessed 11 Oct. 2018].
[3] Zhou, T., Shen, J., Li, X., Wang, C. and Shen, J. (2018). Quantum Cryptography for the Future Internet and the Security Analysis. Security and Communication Networks, 2018, pp.1-7.
[4] D. Moody, "The ship has sailed: The nist post quantum crypto competition."
[Online]. Available: https: //csrc.nist.gov/CSRC/media//Projects/Post-Quan.
[5] N. KOBLITZ AND A. MENEZES, "A RIDDLE WRAPPED IN AN ENIGMA," IEEE SECURITY PRIVACY, VOL. 14, NO. 6, PP. 34–42, NOV 2016
[6] Goubin, L., Patarin, J. and Yang, B. (n.d.). Multivariate Cryptography.
[7] Chris Peikert, "A Decade of Lattice Cryptography",University of Michigan, pp. 8-72, February 17, 2016.
[8] M. Ajtai., "Generating hard instances of lattice problems. Quaderni di Matematica", 13:1–32
[9] Daniel M. Greenberger, Karl Svozil "Quantum Theory Looks at Time Travel", pp 8-12, June 21, 2005.
[10] Bennett, C., Brassard, G., Ekert, A.: Quantum cryptography. Scientific American 267, 50–57 (1992)
[11] Seiki Akama, "Elements of Quantum Computing", ISBN 978-3-319-08283-7, 6:101-104, 2015
[12] Mavroeidis, V., Vishi, K., D., M. and Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. International Journal of Advanced Computer Science and Applications, 9(3).