ISSN: 0974-5823 Vol. 6 No. 3 December, 2021

International Journal of Mechanical Engineering

Post Quantum Cryptography: A Literature Review

Shipra Srivastava
Research Scholar
Dr. K N Modi University, Newai
Rajasthan, INDIA
Shiprasrivastava2000@gmail.com

Dr. Anoop Tiwari
Professor, Department of C.S.E.
Dr. K N Modi University, Newai
Rajasthan, INDIA

Dr. Ramveer Singh
Professor, Departmet of I.T.
Greater Noida Institute of Technology
Greater Noida, U.P., INDIA

Abstract— The world is moving away from the classical computers whose basis is binary digits to a completely innovative way of computation whose working principle is based on qubits or quantum bits. As this quantum computer technology is in its early budding days which seem very promising as it can solve a complex problem using lesser processing time. Whereas, in a conventional computer it would take hours of processing time. An attack from a quantum computer to traditional cryptography will not be able to withstand the computational power. So, the researcher and scientists around the world are researching cryptography which is quantum secure, where the quantum computer fails to break such security. This paper discusses the algorithms that pose a threat to classical cryptography and a brief explanation about the current quantum secure algorithms that can handle the future world from the threats. This paper focuses on the devastating effects on Shor's and Grover's algorithm which lead to the further development of quantum secure Symmetric and Asymmetric algorithms.

Keywords— Quantum safe cryptography, quantum secure Symmetric Algorithm, quantum secure Symmetric Algorithm, quantum resistant AES, Lattice based encryption.

Introduction -This Cryptography is the technology that prevails in this era of computation to keep the information hidden from unapproved excess. The subject cryptography is a vast subject that is responsible for almost every aspect of a website to e-mail system to the electronic transaction to online shopping to online messaging implementing its protocols to keep the current architecture safe from any attempts of hacking and theft. This technology makes sure at the foremost to convert plaintext to encrypted text from the sender end and decrypted at the receiver end. It uses many protocols and techniques to encrypt and decrypt a plaintext. The algorithm which encrypts a plaintext is called 'cipher' and the output of the algorithm is called 'cipher-text' [2]. With an example of Bob and Alice, where Alice sends an important hidden message to Bob using an open unsecured channel where anyone can check the message. In this kind of situation, a secure way is to use encrypting the message. Using a hidden bit called 'key' which is shared by Alice to Bob. Alice transforms the plaintext message to ciphertext by using the key. Bob after receiving the message can transform the ciphertext using his key to plaintext [1] and their secret message remains hidden from other intruders in the channel.

In cryptography, its security is dependent on the key's secrecy which was played the most important role during World War II. The information sending over the unsecured channel was the only option back then, by using some mechanical devices to encrypt the messages. The messages and information that were transmitted were to determine the faith of World War II. One such machine that was used by German to encrypt messages was Enigma which was used to communicate by their military. The Germans considered Enigma as unbreakable, as the allied forces were working to decrypt the Enigma codes. In London, Bletchley Park a team of cryptanalysis headed by Alan Mathison Turing successfully decrypted the messages of Enigma which became the turning point of World War II.

The computer started coming into the picture and its working principle at mechanical levels is implicated by high and low voltage and at the software level, it is implicated by the binary method using 0's and 1's. These computers communicated between them, for secure communication, there are few techniques were set such as Rivest Shamir and Adleman (RSA) [4], Data Encryption Standard (DES) [5], and Advanced Encryption Standard (AES) [6], etc.

The greatest innovation of the 21st century in terms of computer is the prototype quantum computer which is very promising where quantum theories of physics are coupled with computer science [3].

As the theory of quantum mechanical computer was coined back in the 1980s [7] which theoretically looks very promising. According to the requirement, researchers started to coin algorithms that are quantum computer compatible. Such algorithms are Shor's and Grover that were developed and poses a threat to the entire cryptographic establishment that is in place.

Shor's Algorithm

Shor's Algorithm [10] which was formulated in the year 1994. This algorithm can break RSA public key system which makes many on the cryptographic systems that are implemented in the websites and communication system becomes vulnerable. Shor's efficient to solve integer factorization, it can break encryption by factoring large numbers. Suppose a plaintext is encrypted and it encrypted a number 'N'.

Shor's algorithm has the advantage of factoring large numbers quickly. Let try to guess a number and let it be 'g', just by guessing 'g' it won't take us to the number 'N'. More accurate guess would be $ggPP/2 \pm 1$ if we can find 'P'. It is possible to find 'P' immediately from g→P from quantum computation. The algorithm will take a random guess 'M' and it will check the random guessed number 'M' shares the factors with 'N', which will lead to the answer once $MMPP/2 \pm 1$ is calculated. At this part we are left with 'P' where quantum computation will play an important role such that $|xx\rangle$
$= MMxx \rightarrow |xx, MMxx\rangle$ it is superposition of all and calculating it the quantum computer will
calculate 'P'. After computing all superposition at the end one equation will be left such that $|xx\rangle + |xx + PP\rangle + |xx + 2PP\rangle + |xx + 3PP\rangle$

This equation will be used to determine the frequency using Quantum Fourier Transformation which will give a resultant of another superposition of $|1/PP\rangle + |2/PP\rangle +$
$|3/PP\rangle$ Computing this
superposition equation we will get the common factor 1 such that $ggPP/2 + 1$ will give
PP
a common factor 'a' and $ggPP/2 - 1$ will give a common factor 'b' such that a.b = N. This is how Shor's algorithm calculates 'N' by factorization, once 'a' and 'b' is calculated and encryption is compromised.

Grover's Algorithm

Grover's Algorithm was introduced in 1996 in Bell's laboratory. This algorithm was specifically meant for quantum computing. Grover's [9] algorithm was developed for searching in an unordered database of N size and searching with database quantum queries.
The Grover's algorithm can be explain as a searching algorithm that searches for a root of a function 'f', where it tries to find a solution of 'a' to the function f(a)=0. The algorithm can search the root just by $\sqrt{NN}$ quantum times [8]. So, implementing it on a quantum computer will require less time compared to conventional computers.
To avoid such cryptographic catastrophe in future the researchers and scientists have started to work on quantum-safe or quantum secure algorithms.

2. QUANTUM RESISTANT SYMMETRIC ALGORITHM

Symmetric algorithms are those algorithms that use a single key to encrypt the plaintext to a cipher-text and decrypt a cipher-text to plaintext with provable security [11].

I. QUANTUM SECURE SYMMETRIC ENCRYPTION SYSTEM

Advanced Encryption System (AES) is such symmetric algorithm which uses a single key and is very frequently implemented an algorithm which gives a solution that fulfils all the requirement for a longer- time security in everyday changing security threats. While using AES 126 bits key length might be fatal in terms of quantum attacks. But using AES - 256 with 14 rounds will be quantum secure as it was claimed by John Gregory [13] in their research paper. He also assumed how cryptographic researchers should keep in mind while searching about cipher such as

a + b < = c

where 'a' is the number of years a cipher will remain secure and 'y' is the time that will require to deploy a new cipher and 'c' is the time required to innovate new cipher which we thought interesting to highlight it in this paper.

Rashmi R. Rachh [12] proposed in their research paper an AES based key scheduler algorithm which is modified in such a way that it arrives at the last round of keys quickly as the technique is called look-ahead technique. In this paper, the authors have mentioned that the algorithm is efficient in decrypting cipher-text in a less time complexity which in turn makes this algorithm a feasible way to incorporate with key search engines and routers. The look-ahead technique can be implemented with 192 bits key as well as for 256 bit key [12] which makes it quantum attack resistant. While Ralf Laue in the research paper [14] has claimed to develop a cryptographic system which covers all the necessary aspects, AES based encryption and decryption, hash function and Cryptographically Secure Random Number Generation (CSRNG) can be implemented on 128, 192 and 256 bits of key length which will be a far more secure option as this club together three aspects where the classical cryptography becomes vulnerable. It started with encryption and decryption, which encrypt the plaintext to a random number generated using Reseed.

The key scheduler is constructed in such a way that supports a length of 256 bit key of maximum size. So, that the shift register can handle different key sizes, the researchers have bypassed the XOR and the rotating operation of the word. For rotating operation, it requires a RAM of dual port in the key scheduler for the substitutionof byte.

A hash function takes input 'n' of any length for output of T(n) of a particular fixed length. The hash function must comply with some properties which make such that to find two inputs 'n' and 'ń' when ń ≠ n and T(ń) = T(n) [16]. The Hash function is based on AES, it uses the methodology of Davies – Meyer [15] it gives a hash output of 256 bit length. The hash function string is substituted into 'x' numbers such that n1, n2, n3, , nn each of 256 bit of length and't' value is calculated such that

T = IV= 2256-1 and Ti = Eni(Ti-1) ⊕ Ti-1 0 < i

≤ x and H = Hx+1 = EHx⟨$HHxx$⟩⊕ Hx Ea(f) implicates encryption of 'f' block with 'f' key. VI is the vector initialization in the memory to the initial value 2256 -1.

CSRNG produced string bit should satisfy two properties, the output is random

i.e. it shouldn't match with the actual random string. And lastly, the output should also be unpredictable. Employing all of these techniques of CSRNG and comparing it with other such models it requires 33.5% fewer resources.

The conclusion is that qubit of quantum computers are small but fast enough, implementing Grover's algorithm on it will make many cryptographic systems vulnerable for those whose security is aimed for 128 bit AES keys. It is recommended to implement 256 bit AES [8], that will protect the cryptographic system against any possible quantum computer attacks without drastic modification.

II. QUANTUM SAFE SYMMETRIC DIGITAL SIGNATURE

A digital signature is an important part of a cryptographic system that makes communication secure in an insecure channel. This system verifies the authenticity and integrity of any electronic document much like a handwritten signature.

The digital signature mechanism uses a secret signing key generally using a hash function. In the case of the symmetric digital signature, it uses only one key to encrypt and decrypt data.

While in the quantum secure signature there are multiple protocols such as zero- knowledge (ZK) [17]. ZKBoo is an extension ZK and ZKBoo is modified to ZKB++ with and an additional feature of NIZK proof which is half of the size of ZKBoo proof. Implementing ZKB++ [19] the authors have proposed two signature mechanisms for post-quantum Fish and Picnic schemes. While using ZKB++ it reduces the signature size and these signature schemes are quantum secure. And ZKB++ with NIZKPoK [19] gives a shorter signature when compared with one which is currently working. Using zero-knowledge proof [20] is used to generate small size proof such as a logarithm ring signature is implemented.

A signature can also be constructed using symmetric – key primitives such as block-cipher and hash function. In this paper [21], authors have proposed two post- quantum signature i.e. Fish and Bagol, generated a new design for secure signature

i.e. EUFCMA scheme. Post-quantum signature cannot rely on traditional technologies such as AES or SHA-3 [22], which can be replaced by LowMC [23] but there are drawbacks such as the signature size where it resultant signature are quite large. For Fish it 61124 bytes and in the post-quantum setting, it increases to 178860 bytes in 128 bits. Using Random Oracle mode (ROM), as it gives additional security, many post-quantum models were implemented, such a model is EPID signature, i.e. Enhanced Privacy ID [24] which any member of a group can sign a message to authenticate and the benefit of this method is that group manager can revisit and cancel any signature when the member is compound.

Quantum security can be given to computers using the classical systems also which remains secure such that, the classical signatures. While it is visible that Lamport one- time signature [25] and signature such as Merkle – tree [26], are quantum secure schemes using two keys, i.e. both public key and symmetric key. The encryption is done using Chameleon hash function, it a provenresistance to collision [27].

3. Quantum resistant Asymmetric Cryptography

Asymmetric cryptography is different from symmetric cryptography as asymmetric cryptography uses a pair of keys, a public key, and a private key but in symmetric cryptography, it uses a single key. Asymmetric cryptography is considered more secure as it uses a public key to encrypt a message and after delivery of the message, the recipient has to decrypt using the private key which is also called the secret – key. And asymmetric cryptography is also called a public – key cryptography.

III. Quantum Resistant Asymmetric Encryption System

Lattice Based Encryption is an asymmetric algorithm [28]

[29] which is a very well protected encryption mechanism against quantum computer attacks. As in asymmetric algorithm lattice based also have two keys which is based on NTRUencryption [30] the public key is the polynomial coefficient P = P0 + P1 x +…..+ Ph-1xh-1, where every co-efficient is a set of {0, 1, ….., j-1}. As the calculation of a public key can be usually h = 743 and j = 2043 = 211. The resultant public key has 743x11=8173 bits. Here a cipher-text is considered as a polynomial ‘d’. The sender will have two keys

i.e. secret ‘e, f’ such that (-1, 0, 1) co-efficient and calculate d=((Pe + f) mod xh -1) mod j. Where mode ‘mod xh-1’ implies that ‘xh’ is changed to 1 and ‘xh+1’ is changed with ‘x’ and goes on…

R = (v, w) of co-efficient polynomial such that 0= ((Pw- v) mod xh-1) mod j. Here ‘R’ is a lattice in 2-dimentional space a point (0, d), such that (e d –f).The issue will be will the hacker or attacker is to find secret ‘e, f’ given public key ‘p’ and ‘h’ as key. NTRU is based on the hardness of short lattice vector computing making it quantum computer resistant scheme [31] [33] and its extended version of it is NTRUReEncrypt

[32] which is a proxy re-encryption scheme based on NTRU.

Goldreick, Goldwasser, and Halevi (GGH) encryption scheme [34] have proposed a trapdoor one-directional function where there are computational complexities of lattice reduction problem, where it hard to find the closet lattice vector at a given point (CVL). Where it acquires a public key and a signature [35] [36]. The key is generated based on a good basis ‘S’ and the ‘S’ is transformed to a bad basis ‘P’ using unimodular transformation. Here the bad basis ‘P’ is the public key and a good basis ‘S’ is the private key. For the encryption, the algorithm takes any arbitrary vector ‘V’ using the public key ‘P’ and the plaintext is converted to a vector ‘R’. The cipher-text vector is created as C = V+. While the decryption process to a plain text such that R= C-V [37]. But the issue with GGH scheme is the length of the public key which is very large, to reduce the length there are schemes like low- density lattice code scheme [38] [39] and [40].

To create a digital signature in the Lattice based domain there are schemes such as Ring LWE signature [41], GGH signature [34] as well as NTRUsign [42] Schemes which are based on the same schemes that are explained above in details. There are hash functions based on Lattices such as SWIFFT [35] and Lattice based Hash Function (LAHF).

IV. CONCLUSION

As the concept of a mechanical quantum computer was proposed theoretically in the ’80s and the mid-’90s two algorithms were coined which showed devastating effectsof its calculation capacity that cripple the cryptographic world with Shor’s and Grover’s algorithms. After such algorithms were introduced the researchers tried to make the existing cryptographic models quantum resistant. The classical RSA, DES, and AES failed to protect but the modification of AES 128 bit to AES 256 bit which becomes quantum resistant. After that, the researches moved along the asymmetric algorithm that leads to the development of Lattice-based systems. This paper explains in detail the devastating impact of Shor’s and Grover and explains how it works. This paper also focuses on the quantum-safe symmetric algorithm such as 256 bit in details and it tries to differentiate quantum symmetric algorithms from asymmetric algorithms which have led to a detailed review of latticed based algorithms. This paper can help upcoming researchers to understand the differences and perform better in their respective research fields.

REFERENCES

[1] Lo, H.K., Curty, M. and Tamaki, K.: Secure quantum key distribution. Nature Photon- ics, 8(8), pp.595-604 (2014)

[2] Bruss, D., Erdélyi, G., Meyer, T., Riege, T. and Rothe, J.: Quantum cryptography: A sur- vey. ACM Computing Surveys (CSUR), 39(2), pp.6-es (2007)

[3] Ying, M.: Quantum computation, quantum theory and AI. Artificial Intelligence, 174(2), pp.162-176 (2010)

[4] Barrett, P.: Implementing the Rivest Shamir and Adleman public key encryption algo- rithm on a standard digital signal processor. In Conference on the Theory and Application of Cryptographic Techniques, Springer, Berlin, Heidelberg, pp. 311-323 (1986)

[5] Davis, R.: The data encryption standard in perspective. IEEE Communications Society Magazine, 16(6), pp.5-9 (1978)

[6] Heron, S.: 2009. Advanced encryption standard (AES). Network Security Volume, Issue 12, ISSN 1353- 4858, pp.8-12 (2009)

[7] Benioff, P.: The computer as a physical system: A microscopic quantum mechanical Ham- iltonian model of