IJISCS (International Journal of Information System and Computer Science)

Full Paper
eISSN 2598-246X
pISSN 2598-0793

DATA LOSS PREVENTION USING POST QUANTUM CRYPTOGRAPHY: OVERVIEW OF ROUND-3 ALGORITHMS

Augustine Chidiebere Onuora[1], ***Prince Ana***[2], ***Anthony O. Otiko***[3] ***Chibuike Ezeocha Madubuike***[4]
[1, 4] Department of Computer Science, Akanu Ibiam Federal Polytechnic Unwana. Ebonyi State, Nigeria.
[2,3]Department of Computer Science, Cross River State University of Technology, Cross-River State, Nigeria.

*Corresponding author
holyaustin@yahoo.com
aconuora@akanuibiampoly.edu.ng

Article history:
Received July 13, 2021
Revised October 25, 2021
Accepted November 1, 2021

Keywords:
KEM;
PKE;
Post quantum Cryptography;
Digital Signature;
Quantum Security;
Cryptosystem.

Abstract
The current hype of quantum computing has necessitated the need for computer security stakeholders to call for the design of security algorithms that will be quantum efficient when quantum computers finally grace our computing sphere. Recent advancements in quantum computing have made cryptographic schemes more vulnerable to quantum attacks like Shor's algorithm and Grove's algorithm. Therefore NIST call for a new set of algorithms known as Post-Quantum cryptography that would be quantum proof is imminent. Many Post quantum algorithms have been designed and tested. But only few of them made it to the round 3 (the final round). This paper reviewed these post quantum candidates. Literatures highlighting their scheme, properties, implementation and areas of security coverage was reviewed. Recommendations on future research areas in this field was itemized for this novel security paradigm as we await the final standardization of this cryptosystems.

1.0. INTRODUCTION

Cryptography can be referred to as the science of information hiding. When information is on transit from point A to Point B, it can be intercepted but when intercepted, the intruder is unable to understand the information. The intended recipient is the only one that can decipher the message using a key [1]. Post Quantum cryptography is the application of existing cryptographic algorithms or the design of new algorithms that are quantum proof [2]. The marriage of quantum theory in physics with computer science is known as quantum computing. Instead of bits, quantum computers use qubits. Unlike traditional computers, they do not use the two-state position of 0s and 1s. Quantum computers encode data using a four-state superimposition. On data processing devices, the four states of quantum computer qubits are represented as ions, atoms, photons, or electrons. Because of its ability to represent data in multiple states, a quantum computer will presumably be more powerful than even the most powerful supercomputer [3].

For some times now, quantum computers – machines that use quantum mechanical concepts to solve mathematical problems that are complicated or impossible for normal computers – have gotten a lot of press. If quantum computers are ever mass produced, many of the current public-key cryptosystems will be broken [4]. The security and privacy of electronic communications on the Internet and elsewhere will be compromised as a result. This will not be funny when it eventually happens. To this effect, The objective of post-quantum cryptography is to build cryptographic systems that can interact with present protocols and networks while safeguarding the computing realm against assaults from both quantum and conventional computers [5, 6]. Various attempts using classical cryptography to help protect data, didn't work out well. The MD5 hash function, which is used to encrypt passwords, has flaws in the context of Collision Attack, which causes thesame hashing to appear on two seperate input values, jeopardizing the data's protection and confidentiality [7]. [8] investigations led to the safeguard in the privacy of SNS consumer data using advanced cryptographic techniques. It also provides empirical data security data for SNS users by homomorphic encryption techniques but still will be ineffective for quantum computers.

A new scheme to improve data protection was introduced by [9]. This was done by combining encryption and steganography. This approach lack implementation on variety of devices. Consumers' Personally Identifiable Information (PII) is being exposed at an unprecedented pace, placing almost 300 million individuals at risk of identity theft and fraud. Cybercriminals are now concentrating their efforts on more profitable cyber-attacks like ransomware, password stuffing, malware, and VPN exploitation. One of the current data breach happened to Sina Weibo which is an alternative replacement of twitter in China. Over 500,000 user's data were compromised. In 2021 alone, sites like Facebook, Instagram, LinkedIn, Ubiquiti Inc, Experian, Reverb and many more have had data breaches [10]. This is the reason NIST highlighted the goal of post-quantum cryptographic system as building an enhanced or new cryptographic system that will secure both classical and quantum computers. They will seamlessly integrate with already existing network and communication protocols as well as been quantum proof [6].

2.0. REVIEW OF RELATED LITERATURE

Firstly, [11] stated that Quantum computers will render unsafe the present public-key systems as Peter Shor demonstrated. They summarized the various public-key schemes that are capable of withstanding quantum computer attacks. [12] presented the hardware application of super-singular-isogeny Diffie-Hellman (SIDH) public-key exchange, which features quantum-resistance. Implementation details showed that on reconfigurable hardware, the isogeny-based algorithm can be implemented with excellent efficiency [13]. According to [14], Hash-based schemes with hash functions were the focus. In terms of security with hash function properties, his work relied on Preimage and collision resistance. Hash-based signatures that were previously stateless were improved and made stateful. While [15] posited that multivariate scheme's algorithm is based on the Multivariate Quadratic polynomial (MQ) problem.

[16] studied a variety of post-quantum cryptographic algorithms He began by looking at the history of hash-based digital signature systems, including the SPHINCS+, XMSS and SPHINCS schemes. The researcher then went on to describe the scheme's concept and illustrate numerous implementations, notably on embedded systems, before concluding the study. To create signature schemes, he took a non-standard method based on the MQ problem, and the MQDSS and SOFIA schemes were introduced. Lattice-based Key-encapsulation techniques based on NTRU, was improved and implemented in this work.

[17] proved that cryptography algorithms based on lattices can be implemented in software, hardware, or both software and hardware. Schemes for public key encryption (PKE), digital signature, and key exchange are available in lattice-based cryptography. He emphasized the NTRU or LWE scheme for public key encryption (various variants exist such as RLWE, MLWE, ILWE, and MPLWE). He looked at how this post-quantum cryptography (Lattice-based) algorithm was implemented on various computing platforms. [18] proposed a quantum hybrid cryptographic scheme as a way of mitigating quantum threats and attacks. He proposed four different options of combining both classical algorithm and quantum algorithms. They are Classical/Quantum-Safe Hybrids, Quantum-Safe/Quantum-Safe Hybrids, Classical/Quantum Key Distribution (QKD) Hybrids and Classical Asymmetric/Symmetric Hybrids.

[19, 2] highlighted the various candidates that scaled the round one into round two. The qualified 17 algorithms for Key encapsulation mechanism are CRYSTALS-KYBER, NTRU Prime, SIKE, FrodoKEM, LAC, BIKE, LEDAcrypt, NTRU Prime, NewHope, NTRU, NTS-KEM, ROLLO, NTRU Prime, RQC, Round5 and SABER. In the cadre of digital signatures, there are nine qualifications namely qTESLA, CRYSTALS-DILITHIUM, FALCON, GeMSS, Rainbow, MQDSS, SPHINCS+, Picnic, LUOV. [20] conducted a performance of the algorithms described in this paper and compared them. For this, a 2.50GHz Intel i7-6500U quad-core, 16GB RAM, and Ubuntu 20.04 64-bit

operating system were used, with all protocols written in SAGE language. Code from Feo was used because the command Elliptic Curve Isogeny is inefficient.

Comparism of primitive algorithms to other post-quantum algorithms were made, the results show that super singular isogeny (SSI) uses small key sizes. The Right learning with error (RLWE) comes first, followed by the code-based algorithm. The results also showed that, when compared to Integer Factorization Problem (IFP), the code-based algorithm performs worse at first for security levels, but improves after a certain level of security. When it comes to protocol performance, the RLWE-based algorithm has the best performance amongst other post-quantum algorithms, followed by SSI and lastly, code-based algorithms.

For key size, SSI-based cryptosystem performed better than both the RLWE and code-based algorithms, while the RLWE protocol outperforms both the SSI-based and code-based algorithms in terms of performance. During protocol handshake, performance is assessed when post-quantum key exchange and authentication are added into TLS and SSH [21]. Their experiments, which utilized actual network conditions, found that the added handshake delay ranged from 1-300 percent for TLS and 0.5-50 percent for SSH, depending on the post-quantum algorithms used. A modest increase in TCP window size can reduce post-quantum TLS and SSH delay by 50%. [22] also proposed KEMTLS, a server authentication protocol built upon key-encapsulation mechanisms (KEMs). IND-CCS-Secure KEM was used for server authentication and that benefitted the cryptosystem in many areas. The bandwidth required by a size-optimized post-quantum instantiation of KEMTLS is not up to half of what is required by a size-optimized post-quantum instantiation of TLS 1.3. When compared to TLS 1.3, KEMTLS saves nearly 90% of server CPU cycles while reducing communication size.

According to the research of [23], their work targeted post quantum cryptographic implementation in lightweight, embedded, and mobile systems. An energy demand study was performed on a Cortex M4-based reference platform based on comprehensive measurements of PQC candidate algorithms, a lot of energy and bandwidth is required to run PQC algorithms, which has an influence on battery life, the user experience, and protocol architecture. For IoT and mobile systems, they developed measurements metrics and guidelines based on their findings. They found that fast structured-lattice PQC schemes are the preferable choice for cloud-connected mobile devices in most situations, even when per-bit data transmission energy costs are high.

[24] provided a research on the importance of isogenic cryptographic algorithms in mobile applications. Studies were conducted on the implementation of cryptography based on isogenies of elliptic curves on mobile devices, comparing post-quantum algorithms in terms of cryptographic stability and speed. To safeguard sensitive data in mobile devices and apps, they investigated the cryptosystems based on the isogeny of elliptic curves and result proved that the sensitive data were secured.

Furthermore [25] Researchers have suggested using joint QKD and post-quantum cryptosystems in QKD protocols in order to increase the transmission distance and/or secret-key rate of the protocol. QKD is used for raw-key transmission, while a PQC subsystem is used to transmit parity bits for information reconciliation. There is an implementation of a McEliece cryptosystem on an FPGA that complies with ETSI [26]. Quantum security was provided by the proposed implementation, which uses a public key of 2,097,152 bytes. According to the proposal, the system uses an ARM Cortex-A53 core linked to a coprocessor through the AX14-lite interface. The complete system is based on a Xilinx Zynq UltraScale+ processor that can decode texts up to 8192 bits in 47.39 milliseconds.

In the review of [27], they evaluated the present state of post-quantum cryptosystems and how they may be used in blockchain and distributed ledger technology. Likewise, thorough comparisons of the features and performance of the most promising post-quantum public-key encryption and digital signature methods for blockchain were provided. Additionally, realistic suggestions for implementing post-quantum blockchain security were presented.

[28] suggested a novel hybrid universal network-coding cryptosystem to achieve safe post-quantum cryptography at high transmission speeds (HUNCC). There's no doubt that public key cryptography and information-theoretic security go hand-in-hand. As a result of its universality, the method may be utilized with any communication network or public-key cryptosystem based on the information-theoretic idea of individual secrecy, their hybrid method makes the assumption that an eavesdropper can only view a fraction of the communication channels between trustworthy parties-an assumption that can be hard to

enforce. They above literatures have given us an insight to the degree of various researches currently been conducted on this novel emerging technology called post quantum cryptography. From the foregoing, many researchers have conducted implementations from cloud security, lightweight implementations like IOT, embedded systems and mobile devices. Network implementations are not left out equally. Implementation in of these cryptosystems on TLS and SSH. Hardware benchmarking and software benchmarking also implemented on Cortex M4 platforms and more.

3.0. POST-QUANTUM CRYPTOGRAPHY

For the Post-Quantum Cryptography Standardization Process (PQC), researchers submitted 69 algorithms to the National Institute of Standards and Technology (NIST) in 2017. For the competition's second round, NIST selected 26 of these algorithms and examined them [2]. As part of NIST's post-quantum cryptography program, the third round of semi-finalists has been selected. There were four cryptosystems that made it into the Public Key Encryption (PKE) and Key Establishment Management (KEM). They are;

- Classic McEliece
- SABER
- CRYSTALS-KYBER
- NTRU

For digital signatures category, three finalist made it. They are

- CRYSTALS-DILITHIUM
- FALCON
- Rainbow

A total of 8 algorithms were selected as alternate algorithms (PKE/KEM and DSA) that will be watched closely and still has the potential of been among those to be selected for standardization. There were five alternates for public key encryption and key establishment management (PKE/KEM). They are:

- BIKE
- FrodoKEM
- HQC
- NTRU Prime
- SIKE

Three candidate algorithms made it for digital signature algorithm (DSA). They are:

- GeMSS
- Picnic
- SPHINCS+

[10] reviewed the NIST final candidates. In this work, the review was based on a brief history, features, security level and list of authors/researchers involved in the development of the algorithm.

Classic McEliece: falls under the category of Key encapsulation mechanism (KEM). Robert McEliece launched this cryptosystem in 1978, and it hasn't changed much since then. The only difference from the original McEliece is a quick "upgrading" of the security parameters to keep up with faster processing speeds and possible quantum attacks. Classic McEliece has parameter sets that correspond to all five NIST security tiers, and it is by far the most thoroughly studied nominee in this NIST phase, resulting in the highest degree of assurance. Other code-based cryptosystems as well as Classic McEliece has fast computational time but they have large public key sizes, which range from 250KB for NIST security level 1 to 1.3MB for NIST security level 5. These are the researchers who worked on this project: Martin R. Albrecht, Daniel J. Bernstein Tung Chou Carlos Cid Jan Gilcher Tanja Lange Varun Maram, Ingo von Maurich Rafael Misoczki Ruben Niederhagen Kenneth G. Paterson, Edoardo Persichetti, Christiane Peters Nicholas Sendrier Jakub Szefer Cen Jung Tjhai Martin Tomlinson Wen Wang.

CRYSTALS-KYBER: Based on the difficulty of solving the learning with mistakes problem across modules, this public-key cryptosystem uses lattices (M-LWE). The three parameter sets in CRYSTALS-KYBER correspond to NIST security levels 1, 3, and 5. It also complies with IND-CCA2 standards. Algorithms that use lattices have a small public key and a low computation time, which makes them attractive. When it comes to balancing this trade-off, CRYSTALS-KYBER excels, with a range of public key sizes ranging from 800 bytes to 1.5KB. They include Peter

Schwabe, Roberto Avanzi Joppe Bos, Leo Ducas, Eike Kiltz and Tancrede Lepoint as well as John M. Schanck and Gregor Seiler as well as Damien Stehle who worked on the project.

NTRU: Is another another structured lattice-based public-key cryptosystem that complies with IND-CCA2. For NTRU to be secure, it has to be difficult to solve the Ring Learning with Error Problem, which has existed since the 1990s in various forms. Before the commencement of Round 2, many cryptosystems were examined, including NTRUEncrypt and NTRU-HRSS-KEM. Cong Chen, Oussama Danba, Jeffrey Hoffstein, Andreas Hulsing, Joost Rijneveld, John M. Schanck, Peter Schwabe, William Whyte, Zhenfei Zhang, Tsunekazu Saito, Takashi Yamakawa, and Keita Xagawa are the developers of this cryptosystem.

SABER: SABER is based on a variant of the LWE issue called the Module-Learning-With-Rounding Problem (M-LWR). SABER is a KEM with a lattice-based organization. It is offered in three different models: LightSABER, SABER (NIST security level 3), and FireSABER (NIST security level 5) Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, Frederik Vercauteren, Jose Maria Bermudo Mera, Michiel Van Beirendonck, and Andrea Basso are among the developers.

CRYSTALS-DILITHIUM: This is referred to a highly secure digital signature method (DSA) based on the difficulty of lattice issues over module lattices. This cryptosystem was created by Vadim Lyubashevsky, Leo Ducas, Eike Kiltz and Tancrede Lepoint with assistance from Peter Schwabe and Damien Stehle.

FALCON: short integer solutions (SIS) are the subject of an NTRU lattice digital signature method. The effect of this is that Falcon has concise signatures and quick implementations. NIST levels 1, 3, and 5 are met by Falcon. Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang are some of the programmers involved in this project.

Rainbow: multivariate digital signature technique based on unbalanced oil-vinegar signature scheme that employs stacked unbalanced oil-vinegar (UOV) structures.It has been around since 2005, Rainbow was just given few minor tweaks. It features small signatures and a fast signing/verification procedure, but its public and private keys are enormous. Development is being carried out by Albrecht Petzoldt, Jintai Xiao, and Ming-Shing Chen. The authors are Dieter Schmidt, Bo-Yin Yang, Matthias Kannwischer, and Jacques Patarin.

Alternate Cryptosystems

BIKE: is a robust KEM that is compliant with both the IND and the CCA, based on quasi-cyclic moderate density parity-check codes (QC-MDPC) BIKE's specs are aimed for NIST security levels 1 and 3. Among the people who worked on this project were Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Shay Guieron, Tim Guneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti and Nicolas Sendrier, Jean-Pierre Tillich and Gilles Zemor as well as Valentin Vasseur and Santosh Ghosh.

FrodoKEM: Is an unstructured lattice IND-CCA compliant KEM with a bigger public key but less parameter restrictions. In terms of NIST security standards, FrodoKEM strives for levels 1, 3 and 5. Michael Naehrig, Erdem Alkim, Joppe Bos, Leo Ducas, Karen Easterbrook, Brian LaMacchia, Patrick Longa, Ilya Mironov, Valeria Nikolaenko, Christopher Peikert, Ananth Raghunathan, and Douglas Stebila are working on this cryptosystem.

HQC: This code-based KEM targets NIST levels 1, 3, and 5 and is based on IND-CPA (indistinguishability against preferred plaintext attack). Even if the public key and ciphertexts are slightly larger than that of BIKE, there are certain efficiencies. Carlos Aguilar Melchor, Nicolas Aragon, Slim &Bettaieb, Loc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, and Jurjen Bos are among the developers of the cryptosystem.

NTRU Prime: uses rings without the structural constraints of the original NTRU suggested in the 1990s. NTRU Prime is also compliant with IND-CCA2. Daniel J. Bernstein, Billy Bob Brumley, Ming-Shing Chen, Chitchanok Chuengsatiansup, Tanja Lange, Adrian Marotzke, Bo-Yuan Peng, Nicola Tuveri, Christine van Vredendaal, and Bo-Yin Yang are among the developers.

SIKE: is the only KEM based on isogeny. isogenies are elliptic curve maps, and share several operations with elliptic curve cryptography. However, SIKE has the slowest public key of all post quantum cryptosystem. Those that worked on this research include David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Amir Jalali, Brian Koziel, Brian LaMacchia and Patrick Longa, Michael Naehrig and Joost Renes.

GeMSS: uses slightly larger public keys, but it's a multivariate digital signature method that produces small signatures and quick verification. GeMSS is based on the hidden Field equation cryptosystem and employs minus and vinegar modifiers (HFEv-). In addition to Casanova and Faugere, Macario-Rat and Patarin also contributed to the development of GeMSS.

Picnic: uses the notion of zero-knowledge proofs and does not rely on number theoretic or formal hardness assumptions to generate digital signatures. A number of programmers contributed to the project, including Greg Zaverucha and Melissa Chase; Steven Goldfeder; Claudio Orlandi; Sebastian Ramacher; David Derler; Jonathan Katz; Xiao Wang; Vladmir Kolesnikov; and Daniel Kales.

SPHINCS+: improved on SPHINCS' initial hash-based digital signature algorithm while retaining the same public key size. This work was developed by Andreas Hulsing, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kolbl, Tanja Lange, Martin M Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Jean-Philippe Aumasson, Bas Westerbaan and Ward Beullens.

Table1: Complete list of PQC Round -3 algorithms (Selected finalist)

S/No	PQC Algorithm	Type	Mechanism
1	Classic McEliece	Code-Based	PKE / KEM
2	CRYSTALS-KYBER	Lattice-Based	PKE / KEM
3	NTRU	Lattice-Based	PKE / KEM
4	SABER	Lattice-Based	PKE / KEM
5	CRYSTALS-DILITHIUM	Lattice-based signature	Digital Signature
6	FALCON	lattice-based signature	Digital Signature
7	Rainbow	Multivariate-based	Digital Signature

Table2: Complete list of PQC Round -3 algorithms (Alternative Candidates)

S/No	PQC Algorithm	Type	Mechanism
1	BIKE	Code-Based	PKE / KEM
2	FrodoKEM	Lattice-Based	PKE / KEM
3	HQC (Hamming Quasi-Cyclic)	Code-Based	PKE / KEM
4	NTRU Prime	Lattice-Based	PKE / KEM
5	SIKE	Isogeny-Based	PKE / KEM
6	GeMSS	Multivariate-Based	Digital Signature
7	Picnic	Hash-based	Digital Signature
8	SPHINCS+	Hash-based	Digital Signature

4.0 DISCUSSION

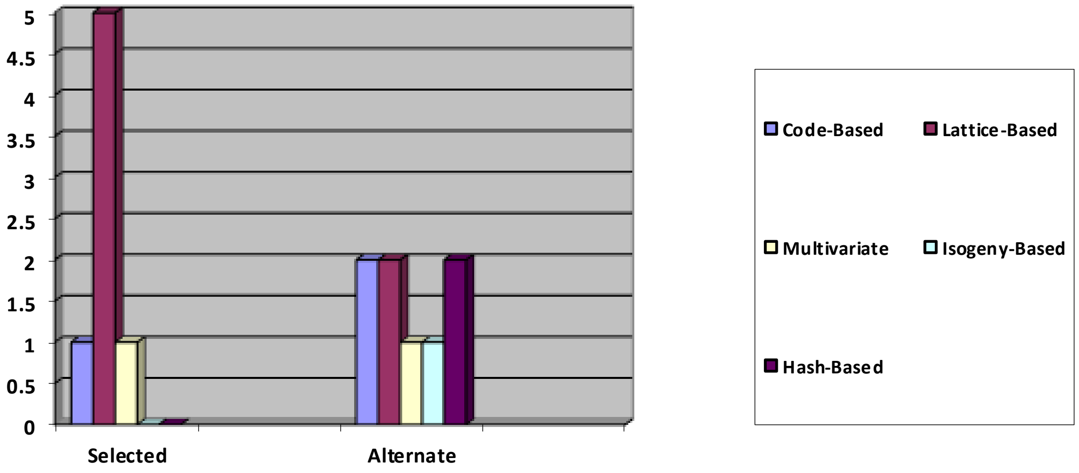

Figure 1. Chart showing types of post quantum algorithm.

The above chart clearly shows the pictorial representation of table 1 and 2. From the group of selected algorithms, lattice-based algorithm have five candidates. Code-based algorithm has one and multivariate-based has one also. This clearly shows that lattice-based algorithm has better chance of been selected and standardized due to the fact that it has more survivors than any other type. From the little review of various algorithm, lattice-based algorithms has better implementation models, small keys and fast computational time.

The alternate algorithms has a total of eight candidates. Code-based algorithms has two candidates, lattice based has two candidates, hash-based algorithm has two, multivariate and isogeny based algorithm has one candidates. As the cyber space continues to be vulnerable to attacks from cyber criminals and hackers, Online and cloud service providers need to start working on models for migrating into the PQC enable servers. This will not only yield a high return on investment but would also make users who store that data up there in the cloud to have confidence that their data is in safe hands.

As data breaches increases and data privacy violated, online vendors and service providers should start a road map to mitigate compromise of data and loss of data. Companies need to plan for the future, the future is here. These cryptosystems that have made it this far have some potentials for post quantum security. They should test and start implementing the one that suits their need.

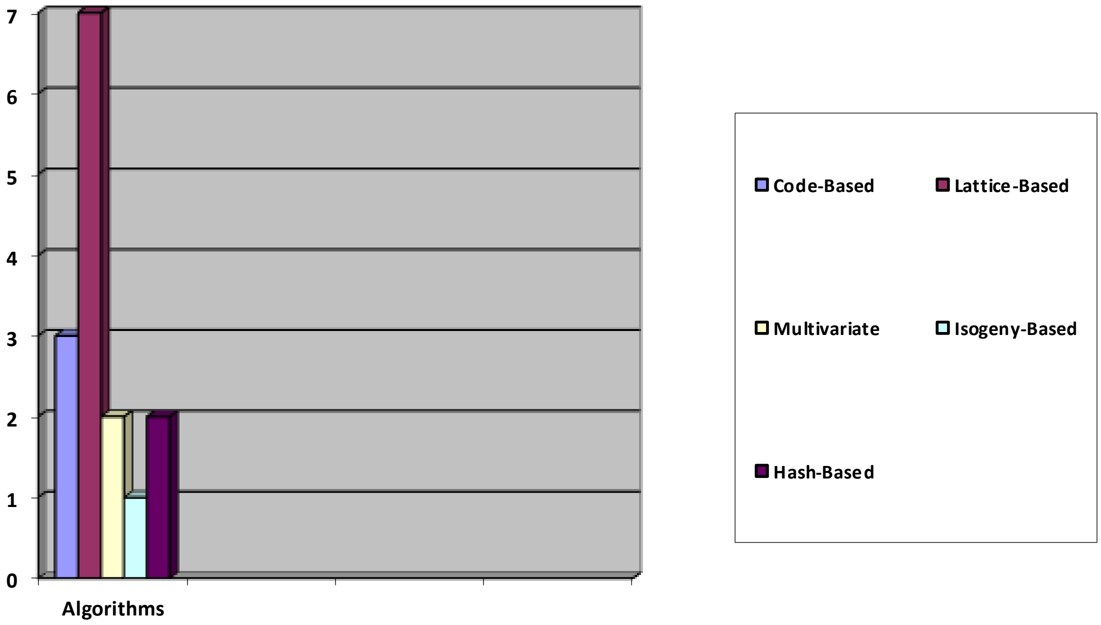

Figure 2. Chart showing cumulative of all types of post quantum cryptographic algorithm.

The above chart (table 1 and 2) shows that Lattice-based algorithm has the highest number of survivors which is seven. Code-based algorithm has three, Hash-based algorithm has two while isogeny and multivariate has one candidates each. As the cyber space continues to be vulnerable to attacks from cyber criminals and hackers, Online and cloud service providers need to start working on models for migrating into the PQC enable servers. This will not only yield a high return on investment but would also make users who store that data up there in the cloud to have confidence that their data is in safe hands.

Effort should be made to secure our data by quick adoption of this cryptosystem. Service providers should not wait until it is late to mitigate a post-quantum attack. Since this cryptosystem have the capacity of both running on our classical computers now and on quantum computers when they are fully available, Let the service providers leverage on the security measures for optimal security of our data. Hardware manufacturers and software developers should immediately adopt this cryptosystem.

4.0. CONCLUSION

NIST have taken the unusual step of dividing the remaining candidate algorithms into two groups, which they refer to as tracks, for this third round. The seven algorithms that appear to have the most promise are featured in the first track. They're mostly general-purpose algorithms that we believe could have a wide range of applications and will be ready to go after the third round. In the second track, there are eight alternate algorithms that either require more time to mature or are tailored to more specific applications. After the third round, the review process will continue, and some of the second-track candidates may eventually be included in the standard. Since all still participating candidates are essentially survivors of the initial group of applications from 2016, further consideration will be given to more recent ideas [6]. Technological giants and network administrators should begin implementing these algorithms into their systems to help avert data breaches and secure user data on their network now and whenever quantum computer takes over our computing space.

5.0. FUTURE RESEARCH AREAS

Post-Quantum Cryptography (PQC) has a lot of areas begging for research and according to [29], they include;

A. PQC migration: Research of potential algorithms in certain circumstances and how to migrate inside a cryptographic usage domain in a secure manner. Deploying this algorithm on several platforms like Web, Mobile IOT, VPN and Trusted computing architectures

B. Cryptographic agility: Our worldwide cryptographic infrastructure must be future-proofed in a flexible and robust manner. Implementation Agility, Compliance Agility, Security Strength Agility and other areas of research are required.

C. Other Areas like Policy making, Process and people. Areas of emerging trends like Blockchain PQC, Password authenticated Key Agreement (PAKE), Secure Multi Party Computation (MPC) and more.

REFERENCES

[1] Research Institute. 2021. A Guide to Post-Quantum Cryptography. https://medium.com/hackernoon/a-guide-to-post-quantum-cryptographyd785a70e-a04b.

[2] Onuora, A. C., Madubuike, C. E., Otiko, A. O. and Nworie, J. N. 2020. Post-Quantum Cryptographic Algorithm: A systematic review of round-2 candidates. Academia in Information Technology Profession AITP.

[3] Zentachain. 2021. Quantum Computers & Encryption. https://medium.com/@zentachain/ quantum-comp uters-encryption-b3d407da5099 (retrieved May 2, 2021).

[4] Horowitz, M. A., Aspuru-Gujzik,A., Awschalom, D. D. , B Blakley, B., Boneh, D., Coppersmith, S. N. and Vazirani, U. V. 2019. Quantum computing's implications for cryptography. In Quantum computing.

[5] Renty, D. 2021. Status of post-quantum cryptography. https://www.riskinsight-wavestone.com/en/ author/david-renty/ (retrieved May 2, 2021).

[6] Post-Quantum Cryptography. 2021. NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization. (Retrieved May 1, 2021).

[7] Sumagita, M., and Riadi, I. 2018. Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application. The International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7, no. 4.

[8] Kapis, K., and Mshangi, M. 2018. Privacy protection of Users' Data in Social Network Systems based on Homomorphic Cryptography Techniques. The International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7, no. 4.

[9] Dehkordi, M. H., Asgari, A. and Moradian, A. 2018. A New Scheme to Secure Communication and Data, based on the Integration of Cryptography and Steganography. The International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7, no. 2.

[10] Swinhoe, D. 2021. The 15 Biggest Data Breaches of the 21st Century. CSO Online. Last modified January 8, 2021. https://www.csoonline.com/ article/2130877/the-biggest-data-breaches-of-the-21st-century.html

[11] Buchmann, J. A., Butin, D., Göpfert, F. and Petzoldt, A. 2016. Post-quantum cryptography: State of the art. The New Codebreakers, 88-108. doi:10.1007/978-3-662-49301-4_6.

[12] Koziel, B., Azarderakhsh, R., Mozaffari Kermani M., and Jao, D. 2017. Post-quantum cryptography on FPGA based on Isogenies on elliptic curves." IEEE Transactions on Circuits and Systems I: Regular Papers 64, no. 1, 86-99. doi:10.1109/tcsi.2016.2611561.

[13] Costello, C. 2017. An introduction to supersingular isogeny-based cryptography.

[14] Endignoux, G. 2017. Design and implementation of a post-quantum hash-based cryptographic signature scheme (Unpublished master's thesis)." Ecole Polytechnique of Palaiseau.

[15] Yang, B. 2021. Multivariate Quadratic Public-Key Cryptography In the NIST Competition. https://www.maths.ox.ac.uk/system/files/attachments/MQ%20Public-Key%20Crypto %20 in%20the%20NIST%20competition.pdf (retrieved May 5, 2021).

[16] Rijneveld, J. 2016. Practical Post-Quantum Cryptography - Joost Rijneveld. Joost Rijneveld, joostrijneveld.nl/thesis/.

[17] Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I and Cammarota, R. 2019. Post-Quantum Lattice-Based Cryptography Implementations. ACM Computing Surveys 51, 1-41.

[18] Faux, R. 2019. Mitigating the Quantum Threat with Hybrid Cryptography." Cloud Security Alliance. https://cloudsecurityalliance.org

[19] Alagic, G., J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, Y. Liu, C. Miller, et al. 2019. Status report on the first round of the NIST post-quantum cryptography standardization process. NISTIR 8240. doi:10.6028/nist.ir.8240.

[20] Borges, F., Reis, P. R. and Pereira, D. 2020. A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography. IEEE. doi:10.1109/ access.2020.3013250.

[21] Sikeridis, D., Kampanakis, P. and Devetsikiotis, M. 2020. Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH. Proceedings of the 16th International Conference on emerging Networking Experiments and Technologies. doi:10.1145/3386367.3431305.

[22] Schwabe, P., Stebila, D. and Wiggers, T. 2020. Post-Quantum TLS Without Handshake Signatures. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. doi:10.1145/3372297.3423350.

[23] Saarinen, M. 2020. Mobile Energy Requirements of the Upcoming NIST Post-Quantum Cryptography Standards. 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud). doi:10.1109/mobilecloud48802.2020.00012.

[24] Bobrysheva, J., and Zapechnikov, S. 2020. The Relevance of Using Post-quantum Cryptography on the Isogenies of Elliptic Curves for Mobile Application Protection. Advanced Technologies in Robotics and Intelligent Systems, 99-103. doi:10.1007/978-3-030-33491-8_11.

[25] Djordjevic, I. B. 2020. Joint QKD-Post-Quantum Cryptosystems. IEEE Access 8, 154708-154712. doi:10.1109/access.2020.3018909.

[26] López-García, M., and Cantó-Navarro, E. 2020. Hardware-Software Implementation of a McEliece Cryptosystem for Post-quantum Cryptography. Advances in Intelligent Systems and Computing, 814-825. doi: 10.1007/978-3-030-39442-4_60.

[27] Fernandez-Carames, T. M., and Fraga-Lamas, P. 2020. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access 8, 21091-21116. doi:10.1109/access.2020. 2968985.

[28] Cohen, A., D'Oliveira, R. G., Salamatian, S. and Medard, M. 2021. Network Coding-Based Post-Quantum Cryptography. IEEE Journal on Selected Areas in Information Theory 2, no. 1, 49-64 (2021). doi:10.1109/jsait.2021.3054598.

[29] Ott, D. and Peikert, C. 2021. Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility. "https://cra.org/ccc/wp-conntent/uploads/sites/2/ 2018/11/CCC-Identifying-Research-Challenges-in-PQC-Workshop-Report.pdf (retrieved May 5, 2021).