International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 11, Issue 5, May 2022 **ISSN 2319 – 4847**

QUANTUM RESISTANT BLOCKCHAIN USING POST-QUANTUM CRYPTOGRAPHY

S.Brindha[1], T.P.Kamatchi[2], R.V.Harshal Ram[3], P.S.Goutham Balaji[4] and T.Karthikeyan[5]

S.Brindha, is with the Department of Computer Networking, PSG Polytechnic College, Tamil Nadu, India.

T.P.Kamatchi, is with the Department of Computer Networking, PSG Polytechnic College, Tamil Nadu, India.

R.V.Harshal Ram, is with the Department of Computer Networking, PSG Polytechnic College, Tamil Nadu, India.

P.S.Goutham Balaji, is with the Department of Computer Networking, PSG Polytechnic College, Tamil Nadu, India.

T.Karthikeyan, is with the Department of Computer Networking, PSG Polytechnic College, Tamil Nadu, India.

ABSTRACT

Considering significant progress as well as developments in the quantum computing field, modern cryptography algorithms and technologies like cryptocurrencies, NFT (non-fungible token) marketplaces, and other blockchain-based systems would be in jeopardy. If quantum computers keep evolving, they will eventually be able to break through the encryption of modern cryptography algorithms. Once encryption of these systems is compromised, they become unsafe and mutable. In this paper, we propose a blockchain system like bitcoin not vulnerable to a cryptanalytic attack by a quantum computer running Shor's or Grover's algorithm. This system is achieved by implementing post-quantum cryptography in the blockchain.

Keywords: Post-quantum cryptography, Blockchain, Quantum computing.

1. INTRODUCTION

The popular and frequently implemented modern cryptographic algorithms are not secure against a cryptanalytic attack by a strong quantum computer. These cryptographic algorithms are based on discrete logarithm problems and integer factorizations problems, which were first implemented since these cryptographic problems cannot be solved in polynomial time by classical computers. As of 1994, Shor's algorithm was invented by the American mathematician Peter Shor which made the security of asymmetric cryptographic algorithm somewhat questionable and in 1996 Lov Grover invented Grover's algorithm which sped up the process of decrypting symmetric ciphers. Within the next decade, the quantum computer will be able to break cryptographic algorithms implemented as of now, like RSA, ECC, Diffie-Hellman, AES, and SHA2 are not quantum-safe.

2. LITERATURE SURVEY:

Use the post-quantum cryptography to combat the threat of quantum computing, and to compare the security and performance of the finalist post-quantum cryptographic algorithms Dilithium, Falcon, and Rainbow. By studying the security in Universal Quantum, you can improve your security. Quantum Annealing and the Gate Model In order to conduct performance analyses, in terms of execution time, we compare the computational demands of the algorithms. as well as the expenses of communication and implementation when TLS (Transport Layer Security) and TCP/IP (Transmission Control Protocol/Internet Protocol) are combined (IP) [1].

Quantum computers use quantum mechanical processes to solve mathematical problems that are difficult or impossible for conventional computers have gotten a lot of attention in recent years. Many of the public-key cryptosystems which are popular can be broken easily by large-scale quantum computers are ever constructed. This would put the security and

integrity of digital communications on the Internet and elsewhere in jeopardy. The objective of post-quantum cryptography (also known as quantum-resistant cryptography) is to create algorithms that are safe against both quantum and classical computers while still being able to communicate with current protocols and networks [2]. The National Institute of Standards and Technology (NIST) provides its current understanding of quantum computing and post-quantum cryptography in this Internal Report.

In 2017, the NIST Post-Quantum Cryptography Standardization Process started with 69 candidate algorithms that passed the minimal acceptance criteria and submission procedures. Candidate algorithms were assessed based on their security, performance, and other qualities during the first round, which lasted until January 2019. NIST chose 26 algorithms to move on to the second round of testing. This paper details the second-round candidates' evaluation and selection process, which was based on public input and internal review [3]. The report covers the 26 second-round candidate algorithms and determines those that will advance to the competition's third round. Classic McEliece, CRYSTALS-KYBER, NTRU, and SABER are the third-round finalist public-key encryption and key-establishment algorithms. CRYSTALS-DILITHIUM, FALCON, and Rainbow are the third-round finalists for digital signatures.

Many encryption protocols in use today are vulnerable to quantum processing. It is predicted that a quantum computer capable of breaching the critical cryptography method RSA2048 would exist by 2035. For many of their fundamental sub-routines, blockchain technology rely on cryptographic protocols. Quantum attacks can be used against some, but not all, of these protocols. We look at the major blockchain-based cryptocurrencies in use today, such as Bitcoin, Ethereum, Litecoin, and ZCash, to see how vulnerable they are to quantum assaults [4]. We conclude with a comparison of the investigated cryptocurrencies and the blockchain technology that underpin them, as well as their respective levels of susceptibility to quantum assaults.

Encryption is required for the security of internet communications, automobiles, and medical implants. However, with the availability of large-scale quantum computers, many cryptosystems in use today will be destroyed. Post-quantum cryptography is encryption that is designed to be secure even if the attacker obtains a powerful quantum computer [5]. This relatively new field of research has found some success in discovering mathematical procedures for which quantum algorithms give minimal performance benefit, and then developing cryptography systems around those operations. The main problem of post-quantum cryptography is to satisfy needs for cryptographic usability and flexibility without losing security.

3. METHODS AGAINST STOPPING QUANTUM THREATS:

3.1. Quantum key distribution (QKD):

One way is to utilize the Quantum Key Distribution (QKD), which allows for Secure communication using Quantum Superposition and Quantum Entanglements. [6] Encoding data is done through quantum states and transmission of particles which are transmitted over QKD Physical Quantum. Generate and the QKD physical channel established is used to securely transmit keys. QKD is immune to cryptanalytic attack by a strong quantum computer using

This solution consumes many resources and the infrastructure required to establish a Physical Quantum channel is expensive.

3.2. Post quantum cryptography (PQC):

The other way is to deploy Post Quantum or quantum-resistant cryptography that runs on a classical computer. The mathematical hardness of these cryptographic algorithms makes them secure against quantum attacks by quantum computers running Grover’s and Shor’s algorithms, unlike public key cryptography. PQC does possess the disadvantages of QKD like high resource consumption and the requirement of expensive infrastructure.

Table 1 Cryptographic Schemes Against Quantum Threats

Type of Cryptography	**Vulnerability**
Asymmetric Cryptography	
RSA	Vulnerable to Shor's Algorithm
ECC	Vulnerable to Shor's Algorithm
Diffie-Hellman	Vulnerable to Shor's Algorithm
Symmetric Cryptography	
AES	Vulnerable to Grover's Algorithm

4. CRYPTOGRAPHIC SCHEME UTILIZED IN BLOCKCHAIN:

There are two areas where Cryptographic schemes are implemented in the blockchain. They are:

- ***ECDSA (Elliptical Curve Digital Signature Algorithm)*** is a Public Key Cryptography, used to sign the transaction between two nodes in a blockchain. ECDSA is Vulnerable to Quantum computers running Shor's Algorithm.

- ***Merkle-tree Hashing***is used to hash the public key and generate Blockchain Address. The haching message using Merkle-tree Hashing Algorithm is shown in fig 1. Having access to the Blockchain Address will not allow a quantum computer to 'undo' or decrypt the hash. Therefore, Merkle-tree Hashing is quantum-safe `and not vulnerable to quantum attacks.

  The Bitcoin protocol mainly uses SHA-256 for all hashing operations. ***SHA-256*** is used to verify a transaction in a blockchain via "Proof of Work" a consensus algorithm. SHA-256 is not vulnerable against Grover's Algorithm. Therefore, it is quantum safe.[7]

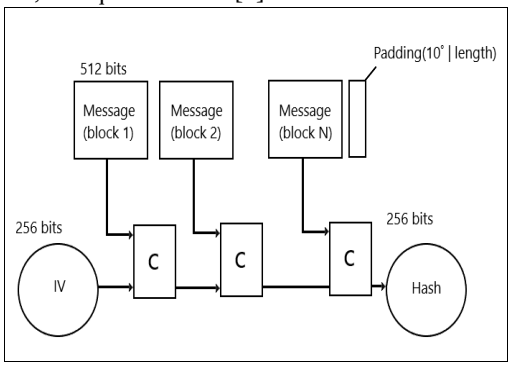

Figure 1 Merkle-tree Hashing Algorithm

5. TYPES OF POST QUANTUM CRYPTOGRAPHY

ECDSA is vulnerable to quantum attacks as stated above. Hence, it must be replaced by different cryptographic schemes which are quantum resilient. There are various types of PQC schemes that are safe against Shor's and Grover's algorithms. under some major categories PQC schemes. They include cryptographic schemes based on lattices, code Multivariate polynomial, hash, Super singular EC Isogeny,etc.

5.1 Lattice-based cryptography:

Cryptographic schemes are based on learning with errors (LWE). Lattice problems screens rely on the hardness of the computational lattice problems.[8] The newly introduced cryptographic scheme learning with errors ring (LWE) additional structures allows for a much smaller key size. Learning with errors, ring learning with errors (ring-LWE), the ring learning with errors key exchange and therefore the ring learning with errors signature, the earlier NTRU or GGH encryption methods, and thus the newer NTRU signature and BLISS signatures are also examples of this methodology. Several of these systems, such as NTRU encryption, have been investigated for several years without a viable attack being discovered. Others, such as the ring-LWE algorithms, provide demonstrations that their security is limited to the worst-case scenario.

5.2. Code-base cryptography:

This cryptographic scheme is space dawn the public key encryption that uses hey error-correcting codes to hey make it nonsensical or unusable during transmission on an unreliable channel. This allows for the prevention of unauthorized users from getting access to sensitive data.[9] Achieved through the addition of errors to the transmitted data to protect it from an eavesdropper. This comprises error-correcting cryptographic systems including the McEliece and Niederreiter encryption algorithms, as well as the associated Courtois, Finiasz, and Sendrier Signature technique. The original McEliece signature, which used random Goppa codes, has weathered the test of time. Many variations of the McEliece method, however, are unsafe, since they attempt to inject more structure into the code used to minimize the size of the keys. The McEliecepublic-key encryption scheme has been endorsed by the European Commission's Post Quantum Cryptography Study Group as a possibility for long-term security against quantum computer assaults.

5.3. Multivariate polynomial cryptography:

This cryptographic came is based on the hardness of solving systems of multivariate polynomials over finite fields.[10] The hardness of the systems lies in the size of the finite field variables and the degree of the system. Multivariate encryption schemes have historically been more successful as an approach to signatures. This includes cryptography techniques based on the difficulty of solving systems of multivariate equations, such as the Rainbow (Unbalanced Oil and Vinegar) scheme. Attempts to develop safe multivariate equation encryption techniques have always been unsuccessful. Multivariate signature systems like Rainbow, on the other hand, might serve as the foundation for a quantum-safe digital signature. The Rainbow Signature Scheme is protected by a patent.

5.4. Hash-based cryptography:

Hash-based signatures are based on digital signatures are constructed using hash functions. Cryptographic systems like Lamport signatures and the Merkle signature scheme, as well as the newer XMSS and SPHINCS schemes, fall within this category.[11] Ralph Merkle pioneered hash-based digital signatures in the late 1970s, and they've been researched as a fascinating alternative to number-theoretic digital signatures like RSA and DSA ever since. Their main disadvantage is that each hash-based public key has a limit on how many signatures may be signed with the associated set of private keys. This fact stifled interest in these signatures until it was reignited by demand for encryption that might withstand attacks by quantum computers.

5.5. Super singular Elliptic-Curve Isogeny:

Using difficulty in finding isogenies between super singular elliptic curves. They have a similar structure to classical Diffie-Hellman and ECDH approaches. To produce a Diffie-Hellman substitute with forwarding secrecy, this cryptographic system uses the features of super singular elliptic curves and super singular isogeny graphs.[12] This

cryptographic system employs the well-studied mathematics of super singular elliptic curves to construct a Diffie–Hellman-like key exchange that may be used as a simple quantum computing resistant alternative for the widely used Diffie–Hellman and elliptic curve Diffie–Hellman key exchange techniques. Because it functions similarly to existing Diffie–Hellman implementations, it provides forward secrecy, which is vital both for preventing government mass monitoring and for protecting long-term keys against failures.

6. NIST POST-QUANTUM SIGNATURE ALGORITHMS:

6.1 Crystals-Dilithium:

Dilithium is a lattice-based signature method that was submitted to NIST's request for post-quantum cryptographic standards as part of the CRYSTALS (Cryptographic Suite for Algebraic Lattices) suite.[13] The approach is designed to eliminate the usage of discrete Gaussian sampling and is simple to implement in constant time. Our system has a public key that is 2.5X smaller than the previously most efficient lattice-based schemes that did not employ Gaussians for the same security levels, while maintaining practically the same signature size. In addition to the novel design, we have greatly improved the running time of the number theoretic transform, which is a key component of many lattice-based structures. Our AVX2-based approach achieves a speedup of around a factor of two over the old method.

6.2 Falcon:

On November 30th, 2017, Falcon, a cryptographic signature technique, was submitted to the NIST Post-Quantum Cryptography Project. Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang were responsible for its design.[14]
The goal of a post-quantum cryptography method is to maintain its security properties even in the presence of quantum computers. According to our present knowledge of the rules of physics, quantum computers are believed viable, but certain substantial technological challenges must be resolved before a fully functional device can be built. The typical asymmetric encryption and digital signature schemes based on number theory would be extremely effectively broken by such a quantum computer (RSA, DSA, Diffie-Hellman, ElGamal, and their elliptic curve variants).

6.3 Rainbow

Rainbow, an efficient asymmetric multivariate signature technique devised by J. Ding and D. Schmidt. This study proposes a Rainbow cryptanalysis that allows an attacker who has access to the public key to recover an equivalent representation of the secret key, allowing her to easily forge any message signature.[15] The complexity of our attack is less than 271 operations for the set of parameter values specified by the designers of Rainbow in order to obtain a security level strictly greater than 280. This is 240 times less difficult than the authors' most well-known assault, which they used to size their system.

6.4. Proposed System:

The proposed blockchain system is modeled after bitcoin’s blockchain but this proposed system enables quantum secure blockchain transactions between peers and quantum secure consensus mechanism, unlike bitcoin. This is made possible by implementing Post Quantum or quantum-resistant cryptography. The cost and time-effective method to counter these quantum threats is to implement Post Quantum or quantum-resistant cryptography which runs on a classical computer.
The mathematical hardness of these cryptographic algorithms makes them secure against quantum attacks by quantum computers running Grover’s and Shor’s algorithms, unlike public key cryptography. Cryptographic algorithms like RSA, ECDSA, Diffie-Hellman, AES, and SHA2 are vulnerable to quantum attacks as stated above. Hence, they must be replaced by different cryptographic schemes which are quantum resilient. The post quantum cryptography signature scheme known as Falcon is best suited to replace ECDSA is this blockchain system. The fig 3 shows the Falcon signature scheme working.

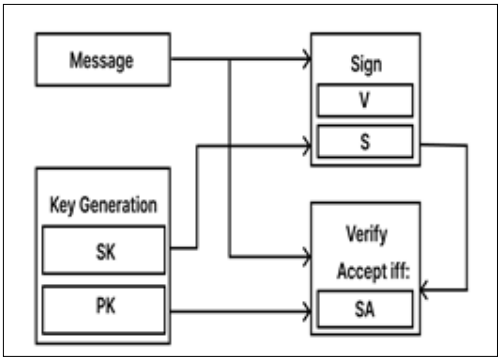

Figure 2 Falcon Signature Scheme Flow Diagram

6.4.1 Key Pair Generation

Keygen is the main algorithm in the process. At begin, the polynomials f and g are generated at random. A couple situations above f and g are put to the test to determine if they are suitable. It is worth noting that:

1. First, the polynomials f, g are generated randomly. It particular:
   a) The public key h can be calculated using f and g. This is true if and only if f mod q is invertible, which is true if and only if NTT(f) has no coefficient set to 0.
   b) The polynomials f, g, F, G must allow short signatures to be generated. If this is the case,

$$\gamma = max\left\{ ||(g, -f), \left|\left| \frac{qf*}{ff*+gg*}, \frac{qg*}{ff*+gg*} \right|\right| \right\} \leq 1.17\sqrt{q}$$

2. Second, short polynomials F, G are computed such that f, g, F, G verify (3.15). This is done by the procedure NTRUSolve [14].

Keygen(ϕ, q)
Require: A monic polynomial $\phi \in \mathbb{Z}[x]$, a modulus q
Ensure: A secret key sk, a public key pk
$f, g, F, G \leftarrow$ NTRUGen(ϕ, q) ▷ Solving the NTRU equation
$\mathbf{B} \leftarrow \left[\begin{array}{c|c} g & -f \\ \hline G & -F \end{array}\right]$
$\hat{\mathbf{B}} \leftarrow$ FFT$(\mathbf{B})$ ▷ Compute the FFT for each of the 4 components $\{g, -f, G, -F\}$
$\mathbf{G} \leftarrow \hat{\mathbf{B}} \times \hat{\mathbf{B}}^*$
$\mathbf{T} \leftarrow$ ffLDL*$(\mathbf{G})$ ▷ Computing the LDL* tree
for each leaf leaf of T do ▷ Normalization step
  leaf.value $\leftarrow \sigma/\sqrt{\text{leaf.value}}$
sk $\leftarrow (\hat{\mathbf{B}}, \mathbf{T})$
$h \leftarrow gf^{-1} \bmod q$
pk $\leftarrow h$
return sk, pk

6.4.2 Signature Generation

Because it uses the Falcon tree and discrete Gaussians across Z, the fast Fourier sampling described in sampling is the most sensitive aspect of our signature technique. The rest of the technique, including signature compression, is rather simple to construct.

Given a private key sk and a message m, the signer can use sk to sign m in the following way:

1. A evenly produced random saltris in the range of 0 to $\{0, 1\}^{320}$. HashToPoint [14] specifies that the concatenated string (r‖m) be hashed to a point c ∈ $\mathbf{Z}_q$ [x] /(ϕ).
2. A (not necessarily brief) preimage t of c is calculated and sent into the fast Fourier transform.

3. sampling algorithm, which outputs two short polynomials s1,s2∈**Z** [x] /(ϕ) (in FFT representation) such that s1 + s2h = c mod q, as specified by ffSampling [14].
4. s2 is encoded (compressed) to a bitstring s as specified in Compress [14].
5. The signature consists of the pair (r,s).

Sign (m, sk, $\lfloor\beta^2\rfloor$)
Require: A message m, a secret key sk, a bound $\lfloor\beta^2\rfloor$
Ensure: A signature sig of m
1: $r \leftarrow \{0,1\}^{320}$ uniformly
2: $c \leftarrow \mathsf{HashToPoint}(r\|m, q, n)$
3: $t \leftarrow \left(-\frac{1}{q}\mathsf{FFT}(c) \odot \mathsf{FFT}(F), \frac{1}{q}\mathsf{FFT}(c) \odot \mathsf{FFT}(f)\right)$ ▷ $t = (\mathsf{FFT}(c), \mathsf{FFT}(0)) \cdot \hat{B}^{-1}$
4: do
5: do
6: $z \leftarrow \mathsf{ffSampling}_n(t, T)$
7: $s = (t - z)\hat{B}$ ▷ At this point, s follows a Gaussian distribution: $s \sim D_{(c,0)+\Lambda(B),\sigma,0}$
8: while $\|s\|^2 > \lfloor\beta^2\rfloor$ ▷ Since s is in FFT representation, one may use (3.8) to compute $\|s\|^2$
9: $(s_1, s_2) \leftarrow \mathsf{invFFT}(s)$ ▷ $s_1 + s_2 h = c \bmod (\phi, q)$
10: $s \leftarrow \mathsf{Compress}(s_2, 8 \cdot \mathsf{sbytelen} - 328)$ ▷ Remove 1 byte for the header, and 40 bytes for r
11: while $(s = \perp)$
12: return sig $= (r, s)$

6.4.3 Signature Verification

The signature verification technique is far less complicated than the key pair and signature creation procedures. The verifier uses pk to verify that sig is a valid signature for the message m as described herein: Given a public key pk = h, a message m, a signature sig = (r,s), and an acceptance bound ⌊β2⌋, the verifier uses pk to check that sig is a valid signature for the message m as defined herein:

1. The value r (called "the salt") and the message m are concatenated to a string (r‖m) which is hashed to a polynomial [x] c ∈ $\mathbf{Z}_q$ [x] / (ϕ) as specified by HashToPoint[14] .
2. s is decoded (decompressed) to a polynomial, see s_2 ∈ **Z** [x] /(ϕ) Decompress[14].
3. The value $s_1 = c - s_2 h \bmod q$ is compu1ted.
4. If $\|(s_1, s_2)\|^2 \leq \lfloor\beta^2\rfloor$, then the signature is accepted as valid. Otherwise, it is rejected.

Verify (m, sig, pk, $\lfloor\beta^2\rfloor$)
Require: A message m, a signature sig $= (r, s)$, a public key pk $= h \in \mathbb{Z}_q[x]/(\phi)$, a bound $\lfloor\beta^2\rfloor$
Ensure: Accept or reject
1: $c \leftarrow \mathsf{HashToPoint}(r\|m, q, n)$
2: $s_2 \leftarrow \mathsf{Decompress}(s, 8 \cdot \mathsf{sbytelen} - 328)$
3: if $(s_2 = \perp)$ then
4: reject ▷ Reject invalid encodings
5: $s_1 \leftarrow c - s_2 h \bmod q$ ▷ s_1 should be normalized between $\lceil -\frac{q}{2} \rceil$ and $\lfloor \frac{q}{2} \rfloor$
6: if $\|(s_1, s_2)\|^2 \leq \lfloor\beta^2\rfloor$ then
7: accept
8: else
9: reject ▷ Reject signatures that are too long

7. EXPERIMENTAL ANALYSIS:

Table 2 contains NIST post quantum cryptography standardization round 3 finals and table 3 consists of CPU usage of PQC Algorithms.Falcon signature scheme was chosen because it's very time efficient and it has smaller key size when compared with other signature schemes at NIST PQC standardization as shown in table 4.

Table 2 NIST Post-Quantum Cryptography Standardization Round 3 Finalists

Type	**PKE/KEM**	**Signature**
Lattice[a]	CRYSTALS-Kyber NTRU SABER	CRYSTALS-Dilithium FALCON
Code-based	Classic McEliece	-
Multivariate	-	Rainbow

Table 3 CPU usage of Algorithms

Algorithm	**CPU ±CI**
Dilithium 2	23.90% ±2.25%
Dilithium 3	27.33% ±2.17%
Dilithium 4	31.29% ±0.51%
Falcon 512	29.84% ±0.47%
Falcon 1024	31.43% ±0.61%
Rainbow Ia Cyclic*	26.04% ±1.39%
Rainbow Ia Classic*	31.78% ±0.82%
Rainbow Vc Cyclic*	32.45% ±0.73%

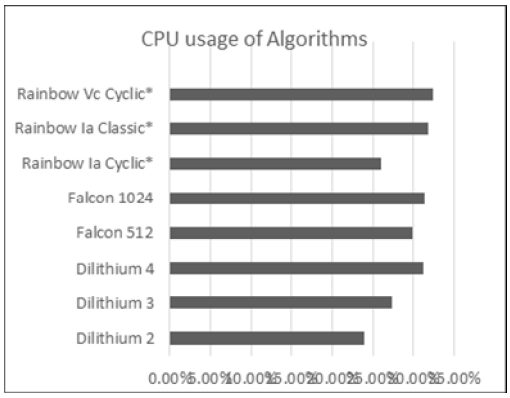

Figure 5 CPU usage of Algorithms

Table 4 Key and Signature size of PQC NIST Algorithms

Signature Scheme	Public Key Size (Bytes)	Private Key Size (Bytes)	Signature Size (Bytes)
Falcon	897	1281	690
Dilithium	1184	2800	2044
Rainbow	58144	92960	64

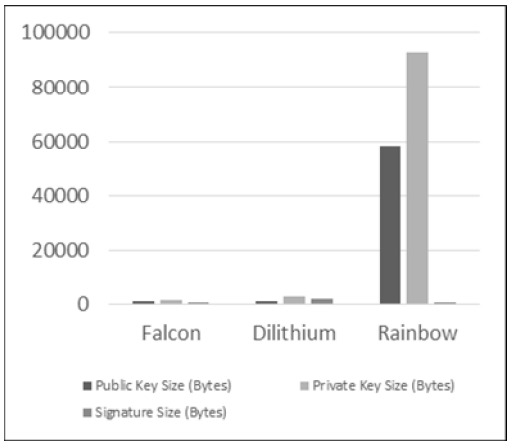

Figure 4 Key and Signature size of PQC NIST Algorithms

8. CONCLUSION:

Various types of Post-Quantum Cryptography schemes are safe against Shor's and Grover's algorithms. under some major categories Post-Quantum Cryptography schemes. They include cryptographic schemes based on lattices, code Multivariate polynomial, hash, Super singular EC Isogeny, etc.

This modal lattice-based cryptography has been chosen to be implemented in the blockchain system because it's most effective against the quantum attack, performs well when implemented in decentralized networks like blockchain, and its security properties are based on worst-case assumptions. These are the key points that make lattice-based cryptography a suitable candidate for this modal. Therefore, replaces the ECDSA (Elliptical Curve Digital Signature Algorithm) with a suitable lattice-based algorithm.

REFERENCES:

[1] Raavi, Manohar, Simeon Wuthier, Pranav Chandramouli, Yaroslav Balytskyi, Xiaobo Zhou, and Sang-Yoon Chang. "Security comparisons and performance analyses of post-quantum signature algorithms." In International Conference on Applied Cryptography and Network Security, pp. 424-447. Springer, Cham, 2021.

[2] Chen, Lily, Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. Report on post-quantum cryptography. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2016.

[3] Alagic, Gorjan, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu et al. "Status report on the second round of the NIST post-quantum cryptography standardization process." US Department of Commerce, NIST (2020).

[4] Kearney, Joseph J., and Carlos A. Perez-Delgado. "Vulnerability of blockchain technologies to quantum attacks." Array 10 (2021): 100065.
[5] Bernstein, Daniel J., and Tanja Lange. "Post-quantum cryptography." Nature 549, no. 7671 (2017): 188-194.
[6] Scarani, Valerio, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. "The security of practical quantum key distribution." Reviews of modern physics 81, no. 3 (2009): 1301.
[7] Bamakan, Seyed Mojtaba Hosseini, Amirhossein Motavali, and Alireza Babaei Bondarti. "A survey of blockchain consensus algorithms performance evaluation criteria." Expert Systems with Applications 154 (2020): 113385.
[8] Peikert, Chris. "Lattice cryptography for the internet." In International workshop on post-quantum cryptography, pp. 197-219. Springer, Cham, 2014.
[9] Ding, Jintai; Schmidt (7 June 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. Vol. 3531. pp. 64–175. doi:10.1007/11496137_12. ISBN 978-3-540-26223-7.
[10] Ding, Jintai, and Dieter Schmidt. "Rainbow, a new multivariable polynomial signature scheme." In International conference on applied cryptography and network security, pp. 164-175. Springer, Berlin, Heidelberg, 2005.
[11] Sobti, Rajeev, and Ganesan Geetha. "Cryptographic hash functions: a review." International Journal of Computer Science Issues (IJCSI) 9, no. 2 (2012): 461.
[12] De Feo, Luca, David Jao, and Jérôme Plût. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies." Journal of Mathematical Cryptology 8, no. 3 (2014): 209-247.
[13] Ducas, Léo, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "Crystals-dilithium: A lattice-based digital signature scheme." IACR Transactions on Cryptographic Hardware and Embedded Systems (2018): 238-268.
[14] Fouque, Pierre-Alain, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. "Falcon: Fast-Fourier lattice-based compact signatures over NTRU." Submission to the NIST's post-quantum cryptography standardization process 36, no. 5 (2018).
[15] Billet, Olivier, and Henri Gilbert. "Cryptanalysis of rainbow." In International Conference on Security and Cryptography for Networks, pp. 336-347. Springer, Berlin, Heidelberg, 2006.

AUTHOR

S Brindha received the M.S and PHD. She currently is working as the head of computer networking department at PSG polytechnic college. Her are area of specialization is Network Maintenance & Troubleshooting, Biometric Security, Linux Administration, Electrical Sciences, Network Security.

T P Kamatchi received the M. E. degree She currently is working as the lecture in computer networking department at PSG polytechnic college. Her are area of specialization is Computer hardware and networks, Linux Administration, Router Administration.

R V Harshal Ram received the SSLC in 2019. He currently is a student of computer networking department at PSG polytechnic college. His area of specialization web development and android app development.

P S Goutham Balaji received the SSLC in 2019. He currently is a student of computer networking department at PSG polytechnic college. His area of specialization web development and android app development.

T Karthikeyan received the SSLC in 2019. He currently is a student of computer networking department at PSG polytechnic college. His area of specialization web development and Linux penetration testing.