Noname manuscript No.
(will be inserted by the editor)

Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research

Ritik Bavdekar · Eashan Jayant Chopde ·
Ashutosh Bhatia · Sandeep Joshua Daniel · Atul ·
Kamlesh Tiwari

the date of receipt and acceptance should be inserted later

Abstract The development of large quantum computers will have dire consequences for cryptography. Most of the symmetric and asymmetric cryptographic algorithms are vulnerable to quantum algorithms. Grover's search algorithm gives a square root time boost for the searching of the key in symmetric schemes like AES and 3DES. The security of asymmetric algorithms like RSA, Diffie Hellman, and ECC is based on the mathematical hardness of prime factorization and discrete logarithm. The best classical algorithms available take exponential time. Shor's factoring algorithm can solve the problems in polynomial time. Major breakthroughs in quantum computing will render all the present-day widely used asymmetric cryptosystems insecure. This paper analyzes the vulnerability of the classical cryptosystems in the context of quantum computers, discusses various post-quantum cryptosystem families, discusses the status of the NIST post-quantum cryptography standardization process, and finally provides a couple of future research directions in this field. Post Quantum Cryptography, Quantum Computers, Shor's Algorithm, NIST Post Quantum Cryptography Standardization Process

1 Introduction

A new paradigm of computing is slowly emerging in form of quantum computers which is going to drastically change the capabilities of classical computers that we are using currently. Quantum computers will be able to perform certain compuations which are not possible by present day high performance multicore systems. The applications of quantum

Ritik Bavdekar, Ashutosh Bhatia, Kamlesh Tiwari, Sandeep Joshua Daniel, Atul
Dept. of Computer Science and Information Systems
Birla Insitute of Technology and Science Pilani, Pilani Campus
Jhunjhunu 333031, Rajasthan, INDIA
E-mail: {f20170349, ashutosh.bhatia, kamlesh.tiwari, h20200135, h20200138 }@pilani.bits-pilani.ac.in

Eashan Jayant Chopde
Department of Electrical and Electronics Engineering
Birla Insitute of Technology and Science Pilani, Pilani Campus
Jhunjhunu 333031, Rajasthan, INDIA
E-mail: f20171161@pilani.bits-pilani.ac.in

computers are countless including navigation systems, seismology, physics research, pharmaceuticals, etc. [1]. Quantum computers can be used to solve complex science problems which even present day supercomputers fail to solve. There are always two faces of a coin. On one hand, quantum computers provide us the hope to solve several problems across different verticals within a bounded time. On the other hand, their arrival may become a potential threat for us in certain scenarios. One such scenario is cryptanalysis. Cryptanalysis is the art of code-breaking. An unfortunate fact is that the hard problems of mathematics upon which our present day cryptographic algorithms are built will become solvable on quantum computers. This will make it easy to crack the cryptographic algorithms widely used in digital communication. The symmetric cryptographic algorithms that are widely used include Advanced Encryption Standard (AES) and 3DES (Data Encryption Statnadrd). Their bit security will be halved with the help of Grover's algorithm [2]. Asymmetric cryptosystems like RSA, Diffie Hellman and ECC are based on the classically hard problems of Prime Factorisation and Discrete Logarithm. Quantum computers can be used to solve these computationally secure problems in no time. This severely compromises the security of the asymmetric cryptosystems.

Post Quantum Cryptography is the study of new cryptosystems which cannot be cracked by both quantum and classical computers. The cryptosystems are divided into several families based on the underlying problem upon which the security is established. These underlying problems are believed to be unsolvable by both classical and quantum computers. The major families are lattice-based cryptography, isogeny-based cryptography, non-commutative cryptography, code-based cryptography, hash-based digital signatures, and multivariate cryptography [2]. The need for better cryptographic algorithms has led to various initiatives by the NIST to create Quantum Secure algorithms. In a drive to expedite current research into the creation of a standard, entries from all across the world were received and deliberated upon to create an appropriate standard for when the need arises. This paper discusses the implication of quantum computers on various cryptographic algorithms currently in use, by commenting on their security in the face of quantum adversaries. It also examines different widely researched algorithms (post-quantum cryptography) that would prove difficult to crack even by a quantum adversary. Finally, the survey culminates in an overview of the most viable candidates for the NIST standard and provides future research directions in the field of post-quantum cryptography.

2 Quantum Computers and Algorithms

Quantum mechanics is characterized by its absurdity. This is due to the concepts like superposition, entanglement, and quantum uncertainty. Quantum superposition allows a particle to be at multiple places at the same time. Quantum entanglement describes correlations between particles that are not possible in the classical world. Quantum uncertainty states that if we observe one property of a particle some other property's information is lost [3]. The fundamental unit of information in classical computers is a bit [4]. This bit can take only two discrete values 0 and 1. In quantum information, the unit is a qubit [16]. This is a unit vector in a two-dimensional complex vector space. A qubit is represented using the ket notation. $<\psi>=\alpha|0>+\beta|1>$ is the notation for a qubit. Here $|0>$ and $|1>$ are basis vectors in the complex 2d space. α and β are complex numbers whose sum of squares adds up to 1.

A collection of quantum gates to form a circuit is called a quantum algorithm. Common quantum gates include Controlled NOT Gate, Hadamard gate, negation, and phase. There are a variety of different physical systems that can be used as quantum devices. These include superconduction qubits, photonic qubits (polarisation of light), and others. Photonic qubits are good for long-distance communication while supercomputing qubits are better for quantum interactions.

Shor designed two different quantum algorithms which can crack the two major hard problems on which the security of present-day cryptosystems is based: the Prime Factorisation Problem and the Discrete Logarithm Problem. Classical solutions to these problems have exponential solutions. With the help of period finding using Quantum Fourier Transformation Shor designed these probabilistic algorithms in polynomial time. Shor's algorithm can crack the factoring number problem in polynomial time while before this the best classical solution(General Number Field Sieve) takes exponential time [5]. Shor's algorithm is probabilistic. It doesn't always factor in the number in the first attempt. With the increase in the number of times, the algorithm is run the probability of getting a factor increases.

It's a quantum search algorithm that searches in an unsorted database in $O(n^{1/2})$ [2]. In classical computers, search over an unordered database is an O(n) problem. Grover's algorithm is also probabilistic and can be repeated several times to ensure the search is complete. To search a Grover iteration is performed. We can repeat iterations to increase the probability of finding the element in a database. Grover's algorithm can be used to find the mean and median of data, for finding the inverse value of a function, etc. These tools can be used by quantum cryptanalysts for cracking algorithms. It can also be used to search for keys in symmetric cryptosystems.

3 Security of Classical Cryptography

AES has proven to be one of the most robust cryptographic schemes currently in use, proving resilient to the level of exhaustive brute force attacks that are currently computationally viable. The recent advancements in the development of Quantum Computers have however led people to reopen the question of AES's security against Quantum Computer Brute Force Exhaustive Search attacks, Asymmetric Public-Key schemes such as RSA, ECC, etc have been known to be broken completely by Quantum Exhaustive Searches due to the immense parallel processing possible through superposition of qubits [6].

Grover's search algorithm reduces the exhaustive key search from $O(N)$ to $O((N/M)^{1/2})$ trials, where M can be reduced to 1 by choosing functions that give single solutions while implementing AES in a quantum circuit. A major drawback of Grover Search based cryptanalysis of symmetric cryptosystems is that the cryptosystems must be implemented as a quantum circuit. Many implementations of AES as a quantum circuit exist. The crack using Grover's search algorithm requires the AES algorithm to be on a quantum circuit. This limits the application of the crack only to quantum oracles. Furthermore, as mentioned above, current algorithms are only able to reduce the trials by $N^{1/2}$, where N is the length of the key. One can simply increase the key length to preserve security, for example, moving from AES-128 to AES-256 can still be considered unbreakable in the face of Brute Force Searches. Shor's factoring algorithm is a quantum circuit that can factorize big numbers in polynomial time [7]. This is a huge speedup compared to classical methods that are dependent on exponential solutions for the same. With the development of quantum computers, in the near future, the factorization problem will not be a hard problem to solve. This will make RSA cracking very easy. The first practical implementation of RSA for factorization big numbers required more than a billion qubits. This went down to 20 million qubits in late 2019 [8]. This implementation is capable of factoring 2048 RSA integers in less than 8 hours using 20 million noisy qubits. The most powerful present-day quantum computers have 50-100 qubits. In the next 25 years, the software improvements and hardware improvements will meet to make factoring prime numbers a reality. Shor's factoring algorithm taps at the root idea behind the RSA algorithm. A replacement for the same is required in the post-quantum world. NIST is looking for new post-quantum computer era encryption algorithms.

Diffie Hellman key exchange protocol and ECC are based on the discrete logarithm problem.Shor published two algorithms in his famous paper. One of them was for factoring big numbers and the other was a solution to the discrete logarithm problem in any group. The idea behind Shor's algorithm can be used to give an exponential speedup to solve the discrete logarithm problem. Both the security protocols are easy to crack in the post-quantum era.

4 Post Quantum Cryptography

Post Quantum cryptography is the field of cryptography where encryption algorithms are developed which are secure from an adversary with quantum computers. Mathematicians and cryptographers are finding new number theory problems to base the security of the asymmetric algorithms. Now they have to search for new mathematical problems which can't be solved by quantum computers easily. Symmetric Algorithms and hash functions are comparatively secure in a post-quantum world. Grover's Algorithm can speed up the attacks by square root complexity [9]. However, most of the algorithms can be made secure again by doubling the key size.

Presently most of the post-quantum algorithms are part of 6 different families. All of them are a different family of mathematical problems which are difficult to solve even for quantum computers. These mathematical problems will form the base for the next generation of asymmetric algorithms. NIST started the Post Quantum Cryptography standardization process in 2016. It is searching for new digital signature schemes and Public Key Encryption schemes.

4.1 Lattice-based Cryptography

Lattice-based cryptography algorithms are based on hard mathematics lattice problems. The family of lattice problems is used in this type of cryptography. A key feature of lattice-based cryptography is that it involves security based on the worst case problems. Most of the other cryptosystems have security based on the average case [10]. Ajtai-Dwork [10]came up with a cryptosystem using the Shortest Vector Problem in 1997. It was cracked in 1998 by Nguyen and Ster [11]. Goldreich-Goldwasser-Halevi algorithm [12]as published based on the Closest Vector Problem. This was cracked by Nguyen in 1999 [13]. NTRU [14]was published in 1996. Over the years it has been modified and improved and the NTRU encryption system is a final candidate for the NIST Standardization process. The present NTRU is a merger of two different second-round NTRU candidates.

4.2 Hash-based Digital Signatures

Hash-based digital signature schemes are an alternative to present day digital signature schemes which use asymmetric algorithms like RSA. They depend on 2 properties of the hash function's collision resistance and preimage resistance. Finding collisions and preimages is a difficult problem if the underlying hash function is good. Finding quantum algorithms to perform these tasks will be hard if not impossible. Hence these hash-based digital signature schemes can be used for authentication in the post-quantum world. However, they suffer from a serious disadvantage that each digital signature can be used only once.

2 of the 69 schemes in the NIST competition are hash-based cryptosystems. Lamport introduced the hash digital signature scheme in 1979 [15] . Witernitz described a One Time Signature scheme which was significantly more efficient than Lamport's scheme. It has the smaller key size and signature size. Merkle introduced a new scheme that combined the Witernitz approach with binary trees and called it Merkle Signature Scheme. SPHINCS+ an alternative candidate for digital signatures uses a combination of the Witernitz One-Time Signature Plus Scheme and Merkle hash trees in the Forest of Random Subsets signature scheme.

4.3 Code-based Cryptography

Code-based cryptography is based on error-correcting codes [3]. Computer scientists have been working on these for over 40 years. Error correction codes are codes used widely in communications to correct transmission errors. To send a message the text is sent into an error correction code. Then to the output, a few errors are randomly introduced and sent. An example of a well-known code-based cryptosystem is the McEliece algorithm [16]. It takes the help of linear error correction codes(matrix multiplication). The receiver has a good error correction code as the private key. This is multiplied by 2 blinding matrices to produce a bad error correction code, the public key. The public key is shared with everyone. A sender sends the plaintext through the bad error correction code. Then according to the overhead, the sender adds errors. This is the final ciphertext that is transmitted. The receiver uses her good error correction code to decrypt the ciphertext.

McEliece algorithm was introduced in 1978 [17] and nobody has found a weakness in it till now. The major reason why it is not practically implemented is the size of the public key. It is much larger than its asymmetric counterparts like RSA. In the NIST competition, 21 of the 69 algorithms are code-based cryptosystems.

4.4 Multivariate Cryptography

Multivariate cryptography is based on the hard mathematics problem of solving a system of multivariate polynomials. Multivariate cryptosystems are all based on the multivariate quadratic map [18]. The quadratic map takes a sequence $x = (x_1, ..., x_n) \in F_q^n$ and returns an output $y = (p_1(x), ..., p_m(x)) \in F_q^m$ where $p_i(x)$ are multivariate quadratic polynomials for $i = 1, .., m$ and the coefficients of the polynomials are in F_q . The map is called a multivariate quadratic map P with m components and n variables.

Given $P : F_q^n \mapsto F_q^m$ a multivariate quadratic map and a target $t \in F_q^m$ find a value s such that $P(s) = t$. Here s is not unique as map P is not an injective map. This problem is considered a hard problem even for quantum computers. There are methods like the Grobner basis that help solve the problem. Recently many Grobner basis-like algorithms such as F4/F5 and XL [19] are used for solving the MQ Problem. Mainly digital signature schemes are designed on top of the MQ problem. The most widely known digital signature algorithm in multivariate cryptography is the Oil and Vinegar Scheme. Rainbow is a digital signature scheme based on the Unbalanced Oil and Vinegar scheme and a finalist in the NIST competition.

5 NIST Post Quantum Cryptography Standardization Process

The latest advancements in Quantum Computing have led to the construction of a 53-qubit Quantum Computer by Google, although this is nowhere near powerful enough to expose public-key cryptography, it has changed the question of 'if' they can be broken to 'when they can be broken. Google and IBM are in a race to build noise-robust high qubits quantum computers. As a result, many algorithms are being developed that move away from the prime factorization problem, or problems vulnerable to parallel computing. These algorithms are mainly based on Lattices and Error-Correcting Codes. Most algorithms are tending towards using hard-to-solve lattice problems due to their security in both worst-case as well as average case scenarios. In light of the growing need for Post-Quantum Security, NIST gave out a worldwide call for submissions of problems that could be used to substitute current Public Key Encryption Schemes and Digital Signature Schemes.

69 algorithms were submitted for the NIST- Post-Quantum cryptography competition. The best ones will be selected by 2023. These algorithms will be standardized and will be used for many years to come. This 69 consists of 20 digital signature schemes and 49 public-key encryption schemes. 26 algorithms were selected after round 1. The algorithms in NIST round 1 were evaluated on 3 major aspects: security, cost and performance, and algorithm and implementation characteristics [20]. Security was the most important aspect. The algorithms were encouraged to be semantically secure against adaptive chosen-ciphertext attacks. NIST also considered algorithms which are semantically secure against chosen-plaintext attack. Also, digital signature schemes were required to generate unforgeable signatures concerning adaptive chosen message attack. NIST defined 5 separate security categories and included a list of other desirable security properties like side-channel resistance and resistance to multi-key attack, etc.

Cost and performance was the second most important aspect. This cost includes computational efficiency(speed of algorithm) and memory requirements(code size and RAM requirements). Algorithm and implementation characteristics include features like simple and elegant designs, flexibility (runs on different platforms and parallelism). After round 2 NIST has selected 15 algorithms. These algorithms can be listed out based on the type of Hard Problem used to ensure the security of such algorithms.

5.1 Lattice Based Cryptography Candidates

5.1.1 CRYSTALS-KYBER (Finalist)

CRYSTALS-KYBER is a finalist in the NIST PQC standardization process. It belongs to a family of primitives from the Cryptographic Suite for Algebraic Lattices (CRYSTAL). The same suite has been used for generating the DILITHIUM Digital Signature Algorithm. Kyber is a key encapsulation mechanism (KEM) that conforms to IND-CCA2-security. This algorithm relies on the hardness of solving the module learning-with-errors (MLWE) problem [21].KYBER has been proposed as a public key algorithm that provides levels of security comparable to AES schemes. NIST uses AES-128,192,256 as standards for the security of level 1,3,5 respectively. Kyber flavors such as kyber-512,768,1024 can provide mildly comparable levels of security (approx. within 230 of AES-256). It is one of the most competitive proposals in place due to its performance in comparison with other proposed cryptographic schemes. The change in levels of security can be implemented by simply changing the order of the block matrices used in the algorithm.

CRYSTALS-KYBER along with other post-quantum algorithms have been implemented by CloudFare in its Reusable Cryptographic Library. Amazon has introduced a hybrid KYBER mode for its AWS Key Management Service. Also, IBM has used the KRYSTAL Suite, KYBER and DILITHIUM in what it claims to be the world's first quantum computing safe tape drive.

5.1.2 SABER (Finalist)

SABER is another lattice-based KEM algorithm which is a finalist in the NIST PQC Standardization process. It has 3 flavors namely, LightSABER, SABER, and FireSABER, offering level 1,3,5 security by the NIST requirements. The security of LightSABER, SABER, and FireSABER are equivalent to AES 128, AES 192, and AES 256 respectively. It is dependent upon the Module Learning with Rounding problem(MLWR) which differs from the MLWE problem in a sense where the errors are introduced by rounding off the values. Like CRYSTALS-KYBER, the implementation of different flavors simply requires a change in the dimensions of the block matrices used in the algorithm. Unlike KYBER, SABER uses a non-NTT method of multiplication, which is unique to this algorithm out of all the NIST Round 3 submissions.

SABER uses learning with rounding which does not require sampling from an error distribution. This decreases the pseudo-randomness of the algorithm and makes the implementation easier. Also, its security rests on only one core element. This makes it easy to implement it with applications with different. At the end of Round 3 of NIST Standardization, SABER is proposed to be improved by studying side-channel attack resistance and misuse resistance. It is one of the most promising candidates for standardization.

5.1.3 NTRU (Finalist)

NTRU is a lattice-based finalist cryptosystem that does not derive its security from the hardness of the Ring Learning With Error(RLWE) problem or the Module Learning with Error problem. This makes it different from the other lattice-based cryptosystems. Along with Classic McEliece it is one of the oldest cryptosystems of all the submissions. Due to its age, there is extensive research and literature on attacks and problem difficulty, giving us better confidence in the algorithm. The current Round 3 submission of NTRU is a merger of Round 2 submissions NTRUEncrypt and NTRU HRSS-KEM [21].

It is faster and more compact than widely used RSA. There also exist certain redundancies in the algorithm which may be removed at the cost of perfect correctness. Research into proper parameterization of NTRU has been going on since the 1990s, therefore being one of the better documented and trusted cryptosystems in Round 3. It has the advantage of not being subject to intellectual property claims, as all or most patents regarding the structures used in the cryptosystem have expired.

5.1.4 CRYSTALS-DILITHIUM(Finalist)

CRYSTALS-DILITHIUM is a digital signature algorithm that belongs to the Cryptographic Suite for Algebraic Lattices [21]. The difficulty of this algorithm relies on the Short Integer Solutions Problem and the MLWE problem. DILITHIUM has the smallest combination of public key and signature size compared to any lattice-based signature scheme that only uses uniform sampling [22]. DILITHIUM has the lowest core-SVP performance of all the Round

3 lattice-based cryptosystems and does not qualify for NIST Level 5 security as of now. However, DILITHIUM performs well in real-world experiments and is available for use with different parameter sets.

5.1.5 FALCON (Finalist)

Fast-Fourier Lattice-based Compact Signature over NTRU is a lattice-based cryptosystem. Its security is based on the hardness of the Shortest Integer Solution problem over NTRU lattices. The framework is based on NTRU lattices, with a trapdoor sampler "Fast Fourier sampling". It is a combination of NTRU lattices, Fast Fourier Sampling and the GPV framework (hash and sign lattice-based signature schemes). NIST selected FALCON as a finalist for the digital signature schemes [21]. It plans to standardize either FALCON or DILITHIUM. More analysis on floating-point operations causing errors and side-channel attacks have to be done. Also, more study on its sampler has to be done. FALCON's key generation algorithm uses less than 30KB of RAM [23].

5.2 Code-Based Cryptography Candidates

5.2.1 Classic McEliece

Classic McEliece is the oldest cryptosystem present in the Round 3 of submission for the NIST PQC standard [21]. It is based on the 1979 McEliece cryptosystem which used hidden Goppa Codes. The original cryptosystem was not based on the necessity for conforming to public use computation restrictions and was able to offer one-way chosen-plaintext attack security meaning that an attacker cannot efficiently find the message from a ciphertext and public key when the message is chosen randomly [24]. The current submission modifies the original cryptosystem to provide efficient implementation and CCA security which has somewhat compromised the OW-CPA security. The current system is a merger of the NTS-KEM and Classic McEliece submissions of Round 1.

Classic McEliece is remarkable in the sense that there has been 0% improvement in the attacks on the cryptosystem with the increase in computational resources. It utilizes the tight conversion methods of PKE to IND-CCA2 secure KEM to provide security against ROM, and on proper parameterization, QROM attacks. To protect against attacks on hashing functions, well-studied, highly unstructured hashing functions are used. Classic McEliece produces remarkably small ciphertexts, of around 256 bytes, enabling ease of integration into network packets for transmission of data. However one of the biggest drawbacks of this cryptosystem is the large size of the public key of around 1.5 MB.

5.3 Multivariate Cryptography Candidates

5.3.1 Rainbow (Finalist)

Rainbow is a digital signature algorithm based on a variant of the Unbalanced Oil and Vinegar (UOV) multivariate scheme. The algorithm has barely been changed since its introduction in 2005. It is characterized by its use of small signatures and an extremely fast signing and verification process. Due to the layered UOV structure, it is naturally resistant to sidechain attacks, while offering security against traditional UOV attacks such as the

Kipnis-Shamir attack. However, the increase in the complexity of the structure has led to further exploitations. Since 2008 there have been no new attacks on this scheme, and it is sufficient to say even the current attacks can be protected against by choosing appropriate parameters.

Currently, Rainbow digital signature scheme is at par with NIST Level 1,3,5 and is considered to be NP-hard [21]. However, after the Round 3 submission 2 attacks have been proposed by Ward Buellens. The first reduces the security of the Rainbow 1,3,5 schemes by 7 bits, 4 bits, and 19 bits respectively, and is based on the original Kipnis-Shamir attack, this attack also exposes the UOV signature scheme. The second attack reduces the security of Rainbow 1,3,5 by 20 bits, 40 bits, and 55 bits respectively. In the light of such attacks, it is highly unlikely for NIST to consider current parameter models, and the developers must now work on establishing new parameters to maintain the level of security NIST requires. Rainbow DSA is also limited by its large public and private key sizes, reaching up to 1.8 MB.

6 Performance comparison of Post Quantum cryptosystems

Table 1 shows the level of security provided by post-quantum ciphers covered in the study. The performance of an algorithm is normally measured by the number of clock cycles it takes for completion and the amount of circuitry/area needed to implement it on a hardware platform. It also depends on the key length or any other similar metric used within the algorithm. For this purpose, many algorithms have different versions with different parameters which affect the performance.

Table 1: Family and Security Levels of PQC algorithms

Algorithm	**Algorithm Family**	**Security Level**
Classic McEliece	Code	5 [26]
Saber	Lattice	1, 3, 5 [26]
Crystals-Kyber	Lattice	1, 3, 5 [26]
NTRU-HRSS	Lattice	1 [26]
NTRU-HPS	Lattice	1,3,5 [25]
Crystals-Dilithium	Lattice	1, 2, 3 [26]
SIKE	Isogeny	1, 2, 3, 5 [25]
SPHINCS+	Hash	1, 3, 5 [26]

For example, kyber512, kyber768, and kyber1024 are essentially the same algorithm but they use a different key length and other metrics which affects the performance and the security of the cipher. To get a fair comparison of performance algorithms with the same security level must be compared.

In an analysis done by Kanad Basu et al. [26], the authors found that among algorithms using key encapsulation techniques, NTRU-HRSS has the highest latency (in clock cycles). Among level 1 signature algorithms, CRYSTALS -Dilithium has lowest latency. For decapsulation techniques, NTRU-HRSS (level 3) and Classic McWliece (level 5) have the higher latency while CRYSTALS-Dilithium has least latency as shown in Table 2. These values were taken from testing the algorithms on an FPGA (Virtex 7). From these results, we can

Table 2: Performance comparison of PQC algorithms on different platforms

Algorithm	Sec. Level	Encapsulation latency in clk cycles (FPGA) [26]	Decapsulation Latency in clk cycles (FPGA) [26]	Encapsulation latency in clk cycles (micro controller) [27]	Decapsulation latency in clk cycles(micro controller) [27]
3CRYSTALS Kyber	1	$5.6X10^4$	$5.3X10^4$	$8.0X10^6$	$2.0X10^6$
	3	-	-	$9.0X10^6$	$3.0X10^6$
	5	-	-	$1.1X10^6$	$5.0X10^6$
Crystals DILITHIUM	1	$6.0X10^5$	$5.3X10^3$	-	-
2NTRU-HPS	1	-	-	$9.0X10^6$	$1.5X10^6$
	3	-	-	$1.0X10^7$	$2.0X10^6$
NTRU-HRSS	1	$1.4X10^6$	$1,003,222$	$9.5X10^6$	$2.5X10^6$
2Saber	1	-	-	$8.0X10^6$	$2.5X1^06$
	3	$4.9X10^5$	$89,392$	$9.0X10^6$	$3.0X10^6$
Classic McEliece	5	$5.1X10^6$	146,126,996	-	-
SIKE	2	-	-	$> 3.3X10^{10}$	$> 3.3X10^{10}$
SPHINCS+	1	6.2×108	937,935	-	-

conclude that when the base algorithms are used without any modifications, CRYSTALS-Dilithium is a good candidate for IoT for both encapsulation and decapsulation. However for decapsulation, the only practical options are level 1 algorithms for servers since all the level 5 algorithms tested do not have low latency. As IoT implementations would be more often hardware implementations testing on an FPGA serves, as a good benchmark on how the algorithm would perform on an IoT device. The techniques like loop unrolling and loop pipelining can reduce the overall latency. Brian Hession et al. [27] used the tended eXternal Benchmarking eXtension (XXBX) to test the performance of the PQC algorithms on a 32-bit ARM microcontroller (EK-TM4C123GXL). The algorithms were benchmarked according to the RAM, ROM, speed/latency (clock cycles) and Energy used.

In terms of RAM usage NTRU is by far the most expensive with the least usage being done by Kyber (in all 3 security levels). In terms of ROM usage, NTRU is still the most expensive, however the next most expensive algorithm is Saber, though it uses only half the ROM space then the NTRU. When it comes to speed (clock cycles) SIKE is the slowest by a large margin, A single encapsulation takes seven minutes. Kyber, Saber and NTRU are reasonably close with higher security levels taking slightly longer time as shown in Table 2. The same pattern seen in the time consumed is present in the energy consumed. This is simply because the longer the algorithm runs the more time power is required hence the more power is consumed.

7 Future Prospects and Challenges

The NIST PQC process will have its next meeting in June 2021. We will hear new comments on all the finalists and alternatives. Post Quantum Cryptography is a new research topic that will be ubiquitous in the coming years. There are 6 major families upon which cryptosystems are being built. All of them have their advantages and disadvantages in terms of bit security, size and memory overhead and computational requirements Researchers can find new mathematical problems which are hard for quantum computers and base new cryptosystems on them. They can search for new problems which require small overheads and less computational requirements.

The researchers are working hard on the NIST cryptosystem proposals. They have been cryptanalyzing the algorithms for a long time. They are searching for implementation issues, mathematical attacks, side-channel attacks , etc. This is a major research topic and cryptanalyzing the security of the finalists and alternatives will help improve the security of the algorithms and prevent standardization of algorithms that may not be secure. The present algorithms can also be optimized by implementing new hardware and software designs. This could help decrease the time and space overhead of the algorithms. The researchers can work on techniques to decrease the computation requirements by building specialized hardware or by improving the software. They can also decrease the memory overhead.

Researchers can work on lightweight post-quantum cryptography. The increase in IoT devices have made lightweight cryptography a requirement. IoT devices communicate with each other using encrypted data as some of the data may be private(business secrets) . Lightweight post-quantum cryptography is also an important field in which research has to be done. We would require algorithms that are quantum-safe and require little overhead. Number theoretic and algorithmic research is another field where researchers can work on the post-quantum hard problems. They can work on new mathematical techniques to crack the hard problems upon which the security of the post-quantum cryptosystems is based. There is a lot of research being done on the Multivariate Quadratic map problem and the lattice based hard problems. Researchers are coming up with new solutions and techniques to solve the hard problems.

Quantum cryptanalysis and developing new quantum algorithms is another research area that is very little explored. Shor presented two quantum algorithms that cracked the security of the present-day asymmetric algorithms. The Post Quantum Cryptography algorithms may also have different quantum algorithms which could compromise their security. Hence more research has to be done in the field.

8 Conclusion

Quantum algorithms exist for cracking all the major public key cryptosystems. It is only a matter of time before they are broken completely. Researchers have come up with new hard problems which can be used to create new cryptosystems.Symmetric key cryptosystems will remain secure by doubling the key size. NIST has called papers for the 3rd NIST PQC Standardization Conference which will be held in June 2021. NIST plans to discuss various aspects of the algorithms and to obtain valuable feedback for informing decisions on standardization.

9 References

[1] T. S. Humble, “Consumer Applications of Quantum Computing: A Promising Approach for Secure Computation, Trusted Data Storage, and Efficient Applications,” IEEE Consumer Electronics Magazine, 2018.
[2] D. J. Bernstein, “Introduction to Post-Quantum Cryptography,” Springer, p. pp. 1–14, 2009.
[3] M. Gilles, 2019. [Online]. Available: https://www.techn ologyreview.
com/2019/01/29/66141/what-is-quantum-computing/.

[4] V. Feldman, “Basics of Quantum Mechanics,” 2003. [Online]. Available: https://ocw.mit.edu/courses/ mathematics/ 18-435j-quantum-computation-fall-2003/lecture-notes/qc_lec02.pdf.
[5] P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” SIAM Journal on Computing, p. 1484–509, 1997.
[6] X. e. a. Bogomolec, “Towards Post-Quantum Secure Symmetric Cryptography: A Mathematical Perspective,” IACR Cryptol. ePrint Arch. 2019 (2019).
[7] D. J. B. a. N. H. a. P. L. a. L. Valenta, “Post Quantum RSA,” in Post-Quantum Cryptography, Springer, 2017.
[8] C. a. M. E. Gidney, “How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits,” ArXiv:1905.09749 [Quant-Ph], 2019.
[9] M. K. a. G. L. a. A. L. a. M. Naya-Plasencia, Breaking Symmetric Cryptosystems using Quantum Period Finding, arXiv, 2016.
[10] D. C. Ajtai M, “A public-key cryptosystem with worstcase/average-case equivalence,” in twenty-ninth annual ACM Symposium on Theory of Computing (STOC ’97), New York, 1997.
[11] P. N. a. J. Stern, “Cryptanalysis of the Ajtai-Dwork Cryptosystem,” Springer.
[12] S. G. a. S. H. O. Goldreich, “Public-Key Cryptosystems from Lattice Reduction Problems,” in Advances in Cryptology -CRYPTO ’97, 17th Annual International Cryptology Conference, Santa Barbara, 1997.
[13] P. Nguyen, “Cryptanalysis of the Goldreich-Goldw asser- Halevi Cryptosystem,” Advances in Cryptology - CRYPTO, pp. 288-304, 1999.
[14] J. P. a. J. H. S. J. Hoffstein, “NTRU: A ring-based public key cryptosystem,” in International Algorithmic Number Theory Symposium, 1998.
[15] L. Lamport, “Constructing digital signatures from a one-way function,” Palo Alto: Technical Report CSL-98 SRI International, vol. 238, 1979.
[16] S. N. Biswas B., “McEliece Cryptosystem Implementation: Theory and Practice,” in PQCrypto, 2008.
[17] R. McEliece, “A public-key cryptosystem based on algebraic coding theory,” DSN Prog. Rep., Jet Prop. Lab, pp. 114-116, 1978.
[18] Y. B. Ding J., “Multivariate Public Key Cryptography,” in Post-Quantum Cryptography, Berlin, Springer, 2009, pp. 193-241.
[19] A. K. J. P. a. A. S. Nicolas Courtois, “Efficient algorithms for solving overdefined systems of multivariate polynomial equations,” in EUROCRYPT 2000, 2000.
[20] L. e. a. Chen, “Report on Post-Quantum Cryptography,” NIST Internal or Interagency Report (NISTIR) 8105, National Institute of Standards and Technology, 2016.
[21] G. J. A.-S. D. A. D. C. Q. D. J. K. e. a. Alagic, “Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process,” NIST Internal or Interagency Report (NISTIR) 8309, 2020.
[22] P. Schwabe, “Crystals Dilithium,” [Online]. Available: https://pq-crystals.org/dilithium/index.shtml.
[24] “Classic McEliece: Introduction,” December 2020. [Online]. Available: https://classic.mceliece.org/.
[25] F. F. M. A. K. M. ,. T. N. a. K. G. Viet Ba Dang, Implementation and Benchmarking of Round 2 Candidates in the NIST Post-Quantum Cryptography Standardization Process Using Hardware and Software/Hardware Co-design Approaches, Cryptology ePrint Archive, Report 2020/795, 2020.
[26] D. S. M. N. a. R. K. Kanad Basu, NIST Post-Quantum Cryptography- A Hardware Evaluation Study, Cryptology ePrint Archive, Report 2019/047, 2019.
[27] B. a. J.-P. K. Hession, “Feasibility and Performance of PQC Algorithms on Microcontrollers,” in Second PQC Standardization Conference, NIST.