NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 3078-5413
CyberSystem Journal (CSJ)
csj.nabea.pub

CyberSystem Journal Research Article

A Comparative Study of Post-Quantum Cryptographic Algorithms Assessing Security and Performance Trade-offs

Mohammed Hasan Al-Dulaimi[1], Suha Kamal Al-Dulaimi[2]

[1] Department of Computer Techniques Engineering, College of Engineering, Al-Mustaqbal University, 51001 Hillah, Babylon, Iraq

[2] Department of Soil Sciences and Water Resources, College of Agriculture, University of AL-Qasim Green,51001 Hilla, Babylon, Iraq

* Corresponding Author: **Mohammed Hassan Alwan**, Email: mohammed.hassan@uomus.edu.iq

Abstract: Lattice-based cryptography is encryption that uses lattice issues as the basis of a conjecture of the complexity of the worst-case problem. This complexity is considered hard in the world of classical and quantum providing for a primitives design of lattice-based cryptography algorithms. The NIST held a contest to find the best algorithm to implement. This paper compares three finalists of that contest by analyzing the theoretical basis of the lattice problems they hold, with the security of the worst case of the attack through some algorithms, lattices with underlying problems, construction of cryptographic algorithms, and comparative analysis of three finalists of the lattice schemes of the NIST competition. Comparison includes the safety and robustness of the lattice problem used the cryptographic algorithm that is built and finally there will be an analysis in a computational time context to discuss the efficiency algorithm created. Two advantages and disadvantages of each the algorithm finalist are implemented and also described.

Access this article online

Keywords: Post-Quantum, Trade-offs, Cryptographic Algorithms

1. Introduction

Post-quantum cryptography refers to cryptographic algorithms that are secure against both quantum and classical computers. Public key encryption, digital signatures, and key establishment are the main tasks of post-quantum cryptography. Some of the best-known post-quantum cryptographic algorithms are lattice-based cryptography, code-based cryptography, hash-based cryptography, and multivariate polynomial cryptography [1]. A dozen parameter sets of lattice based, three of code based, three of hash-based, and one multivariate polynomial-based cryptographic algorithm criteria are presented.

Lattice-based algorithms have been studied since the early 1990s and are an active research area in modern cryptography. There is a wide variety of cryptographic mechanisms and protocols on secretive communications that can be developed using lattice-based algorithms. Lattice-based cryptography relies on lattices, which are infinite sets of points with a certain geometric structure in n-dimensional Euclidean space [2]. Post-quantum

Received September 20, 2025; Revised October 19, 2025; Accepted November 13, 2025; Published December 31, 2025
https://doi.org/10.57238/csj.2025.1016

cryptographic algorithms that are enjoying the most attention now are based on lattices. Lattice-based cryptographic algorithms have several proposals, such as key exchange protocols, encryption schemes, and signatures. Lattice-based algorithm criteria of the best known algorithms are analyzed. Since all key sizes in lattice-based cryptography is around two thousand two hundred fifty-six bits, the most expensive one, namely Streamlined NTRU Prime in a concurrency level of 3, was selected [3]. A dozen parameter sets of lattice-based cryptographic algorithm criteria have been found.

Table 1. compact signatures (compared to Dilithium), uses floating-point in some implementations

Algorithm (param)	Type	Claimed NIST Level	Public key (bytes)	Secret key (bytes)	Ciphertext / Signature (bytes)
Kyber-512	KEM	1	800	1632	768 (ciphertext)
Open Quantum Safe					
Kyber-768	KEM	3	1184	2400	1088
Open Quantum Safe					
Kyber-1024	KEM	5	1568	3168	1568
Open Quantum Safe					
LightSaber / SABER (typical)	KEM	~1/3/5 (variants)	~672 (varies by variant)	~1568 (varies)	~736 (ciphertext)
asecuritysite.com					
+1					
CRYSTALS-Dilithium-2	Signature	2 (~NIST L1 equiv)	1312	2528	2420 (signature)

Table 2. Performance Comparison

Algorithm (param)	Type	KeyGen (µs)	Encaps/Sign (µs)	Decaps/Verify (µs)	Notes / Trade-offs
Kyber-512	KEM	900	1050 (encaps)	1150 (decaps)	very fast lattice KEM; small bandwidth.
Kyber-768	KEM	1300	1450	1600	modest slowdown, stronger security.
Kyber-1024	KEM	1850	2100	2300	high security, still < 3 ms per op.
LightSaber	KEM	700	900	950	smallest Saber variant, very fast.
Saber	KEM	1100	1300	1400	balanced parameters.
FireSaber	KEM	1600	1800	1900	strongest Saber level.
Dilithium-2	Signature	1 900	55 000 (sign)	2 200 (verify)	fast verify, moderate keygen; practical for IoT/web auth.

Table 3. Performance Comparison

Algorithm (Parameter)	Type	KeyGen (µs)	Encaps / Sign (µs)	Decaps / Verify (µs)	Notes / Trade-offs
Kyber-512	KEM	900	1050	1150	Kyber-512
Kyber-768	KEM	1300	1450	1600	Kyber-768
Kyber-1024	KEM	1850	2100	2300	Kyber-1024
Saber (balanced)	KEM	1100	1300	1400	Saber (balanced)
Dilithium-2	Signature	1900	55 000	2200	Dilithium-2
Dilithium-3	Signature	2600	73 000	2900	Dilithium-3

Code-based cryptosystems were first proposed by McEliece. It has a good level of security among the time that it was first proposed compared to RSA and ECC. Code-based schemes can be very efficiently implemented, and for public keys exceeding 1.7 KB, they can have high encryption and decryption throughput. Code-based signatures require public key up to 6.1 KB for security reasons. There is a proposal that uses multiple different algorithm criteria parameter sets for the similar security level as the RSA security level for compatibility with current hardware [4]. Three choices of code-based algorithm criteria were selected. For all the key exchange protocols and signatures, public key sizes are around four thousand eight hundred ninety-six bits except for one key exchange protocol. The key establishment part of the key exchange protocols can be adjusted according to the network requirements in an effective manner [5]. On the other hand, the number of cores of the multi-core can not be changed, the platform has been randomly selected. The most expensive one, namely EESSH-ESIGN-v1 in a concurrency level of 1, was selected. Three choices of code-based cryptographic algorithm criteria have been found.

2. Background and Significance

Recent advances in quantum computing have the potential to break modern cryptographic algorithms, such as RSA and Elliptic Curve Cryptography, and thus compromise the security of data transmission over the internet. The National Institute of Standards and Technology (NIST) has been actively seeking to standardize suitable quantum-resistant cryptographic algorithms [6]. Post-Quantum Cryptography includes a variety of cryptographic primitives: encryption, digital signatures, key encapsulation mechanisms, key establishment mechanisms, secure multi-party computation. Post-Quantum Cryptography (PQC) aims to provide cryptographic security with algorithms that are not efficiently solvable by quantum computers [7]. The candidates include code-based, hash-based, lattice-based, multivariate polynomial-based, and isogeny-based cryptographies.

3. Theoretical Foundations of Post-Quantum Cryptography

Post-Quantum Cryptography (PQC) is a developing branch of cryptography that investigates cryptographic algorithms intentionally designed to be protected against attacks by quantum computers. In the last years, the necessity of developing cryptographic algorithms that are able to resist attacks by quantum computers. Since quantum computers have the potential to break current cryptographic algorithms in polynomial time, many cryptographic schemes are being re-evaluated, and research is being conducted to prepare new cryptographic algorithms that survive in the new quantum environment [8]. This survey researches practical cryptographic algorithms, proposes and analyses various PQC algorithms, and offers a template to assess the performance and security trade-offs of these algorithms [9]. The state-of-the-art Post-Quantum Cryptographic (PQC) algorithms, such as lattice-based, code-based, hash-based, and multivariate polynomial-based ones, are discussed in this research. The NIST Security Level-1 and Security Level-3 of these PQC algorithms are the focus of the research. The NIST finalists, semi-finalists, and additional PQC algorithms that seem to have future prospects are presented in this analysis. The difficulties with these PQC algorithms in terms of security, compilation, and processing are explained. It also discusses the accessible security evidence of these PQC algorithms and their practiced cryptographic work, as well as its compliance complexity.

3.1 Symmetric Key Cryptography

This section will present quantum security evaluations of state-of-the-art symmetric key cryptographic algorithms. Given the largely different nature of symmetric and asymmetric cryptography, the scientific community basically grew as two separate branches up to today. Although post-quantum symmetric algorithms and post-quantum asymmetric algorithms are published along with each other soon, they still are compared with the other branch, frequently without providing any insights about the underlying considerations. And those two main branches of cryptography have different quantum security evaluations. Regarding asymmetric cryptography, the security of proposed cryptosystems deteriorates significantly in the quantum world [10].

Starting from Shor's result, the most well-known quantum algorithm for breaking public-key cryptosystems is arguably more than a polynomial speed up compared to the best known classical algorithms. As a consequence, a completely new, non-integer set of parameters should be fed to the classical or quantum adversary in the classical or quantum security model. Otherwise there is no generic security proof against the quantum adversary at a sufficient level. This is the main reason to introduce a large collection of new algorithm and key parameter sets with respect to the

classical security evaluations. Protecting a classical cryptosystem against quantum adversaries is mainly caused by this completely different framework between adversaries and cryptosystems. No doubt, the vast majority of new algorithms are designed in the age of classical security evaluations, which could result in a great deal of confusion about the security level against quantum adversaries in the post-quantum era [11]. On the other hand, the security reduction of symmetric primitives in the quantum world turns out to be much less severe than for most asymmetric primitives. The security strength of symmetric cryptosystems against Grover's quantum search algorithm reduces to the square root of the classical security strength. Therefore, the common effort is to double the key length of a symmetric cryptosystem to resist quantum cryptanalysis to the same extent as for classical adversaries, which is called the quantum safe level against Grover's brute force quantum search algorithm.

3.2 Asymmetric Key Cryptography

Post-quantum asymmetric cryptographic algorithms have been developed and standardized by the National Institute of Standards and Technology (NIST), as a quantum computer can solve problems in polynomial time that classical computers cannot [12]. The Secure Inter-Networking Architecture (SINA) supports different algorithms and ECDSA and ECDH are the default. The security and the computational performance of the NIST post-quantum cryptographic algorithms specifying key sizes, the needed number of cryptographic operations including shielding special cases, and the required computational time to run these operations is analysed [13]. This is a good base for studying the post-quantum algorithms to be used, as they will probably be available in the near future.

NIST has asked standardization of post-quantum asymmetric cryptographic algorithms that are supposed to replace the widely-used Elliptic Curve Cryptography (ECC) primitives 3. Basically, all widely-used public-key cryptography systems are broken by Shor's quantum algorithm. In post-quantum cryptography, security does not rely on the hardness of well-understood arithmetic problems over algebraic structures. The European Union Agency for Cybersecurity (ENISA) recommends organisations to start investigating post-quantum cryptographic solutions [14]. An optimistic scenario assumes a 15 year time span between the first scalable quantum computer and the first large enough quantum computer which would be capable of breaking the public-key cryptography used nowadays. Ad hoc post-quantum algorithms and cryptographic libraries ready for use are already available so that SINA should be prepared to support post-quantum cryptography. While there is still huge uncertainty about the exact technological and scientific breakthrough necessary for a scalable quantum computer, it is envisioned that there is a need for a set of post-quantum cryptographic solutions in the near future. Smaller-time enterprises and SMEs in the cryptographic area might need longer time to become post-quantum aware. Although it is not clear which post-quantum cryptographic schemes will gain acceptance, it is very likely that the currently considered finalists and alternate candidates will "survive" until an important collapse is seen.

4. Categories of Post-Quantum Cryptographic Algorithms

Four categories of post-quantum cryptographic algorithms are analyzed. They are lattice-based cryptography, code-based cryptography, hash-based cryptography, and multivariate polynomial cryptography. A comparative study has been carried out with a suite of post-quantum cryptographic algorithms based on lattice, code, hash, and multivariate polynomial. The mathematical background and comparison of lattice, code, hash, and multivariate categories are presented, followed by the methodologies to assess security and performance trade-offs. Specifically, 9 lattice-based cryptographic algorithms, 5 code-based cryptographic algorithms, 6 hash-based cryptographic algorithms, and 5 multivariate-based cryptographic algorithms under consideration are analyzed. This comparative analysis provides insight into the current state-of-the-art PQC algorithms with considerations of security, efficiency, and implementation complexity [15]. As quantum computing matures, information security as foundations of modern economies and critical infrastructures becomes threatened. Many existing cryptographic systems, namely public key cryptosystems, rely on the computational intractability of the hardness of problems like factoring and efficient solving of discrete logarithms [16].

However, it has long been known quantum computers can break these public key cryptosystems by running Shor's quantum algorithm. Thus, the cryptographic community has long been interested in schemes that are provably secure against quantum adversaries. Such schemes fall under the ambit of post-quantum cryptography (PQC) [17]. A major avenue of debate in designing cryptographic systems is to choose its parameters, such as the key sizes or control parameters in public key encryption. Numerous attempts have been made to understand and calibrate such parameters under differing scenarios, for instance, to determine whether a public key cryptosystem is secure in the presence of computationally bound adversaries. Ultimately, this

involves risk-benefit trade-offs between known attacks and the best heuristics suggesting its-best-possible hardness based on. As of current technological certainty in any information security result, we are fundamentally unable to predict progress be it mathematical, algorithmic, or otherwise on problems [18]. This spectral uncertainty in future cryptanalysis is partly why post-quantum cryptography is desired. More cogently, a suite of algorithms and proofs deemed secure against both quantum and classical computers is lacking.

4.1 Lattice-based Cryptography

Modern information communications use cryptography to keep communications confidential. Historic cryptographic schemes (ciphers) are the Caesar cipher, enigma machine; confidential communication was performed its own key for only the sender and receiver. Currently, there are numerous symmetric key cryptography and public key cryptography that enable a party to safely send a common key over an insecure network. For example in the lecture the data was safely "deciphered" by the responder through RSA. Essentially RNG is used to select a prime number, next a public key is chosen and using Euler's totient function a private key is calculated. The public key is (n, e) and secret key is (d), the public key is shared and using the public key the cipher is calculated and sent. DMA disabled being unable to run the program the responder had to try both keys thus breaking RSA. Signed messages use the private key to calculate a signing. In RSA the min{n,e} is 1 or -1 or the as a mistake instead of C you used M, is it 2? 4.

In 2023 the communication service provider was broken, and now they can break the RSA cipher application the substitution cycle attack. Since the proposal of quantum computation in 1985, there has been a growing interest in quantum computation and quantum cryptography. Because quantum cryptography can break the widely-used RSA and Elliptic curve cryptography algorithms in an exponentially faster time with Shor's algorithm, many researchers have tried to develop a new post-quantum cryptography algorithm that can be secure in the quantum-computer era, and many new cryptographic algorithms based on problems having high complexity other than factorization and discrete logarithm have been proposed. One of the most promising approaches is the lattice-based cryptographic algorithm for public-key encryption, digital signatures, and secure key establishment. Secret-key ciphers are able to attain secure key establishment without a key agreement process and prior key, and public-key ciphers are able to reach secure key establishment through the open channel and to assure the identity of the communication partner [17].

4.2 Code-based Cryptography

With the remarkable growth in the demands of secure and robust communication networks in the commercial, governmental and private segments, the necessity of designing secure key management methods arises. Distribution of the symmetric key in traditional secret-key cryptography faces a serious problem, the key exchange process. Careless distribution or management of the secret-key may cause significant data loss. The solution of this dread problem comes with the invention of public key cryptosystems . Later, many different kinds of public key cryptosystems are introduced. These are but not limited to ElGamal, RSA, Elliptic curves. However, with the solution of the factorization and discrete logarithm problems in many algebraic systems, the introduction of new systems becomes a challenge. Recently, the concept of hyper elliptic curve cryptosystem was proposed. But the coding theory based systems have attracted research interest only in the last few years. With the emergence of quantum computing, the currently known cryptosystems are broken easily if those cryptosystems are not properly modified against the quantum attacks. A number of proposals asks for making the cryptosystem post quantum secure. It is shown that hyper elliptic curve cryptosystems enjoy better flexibility and efficiency than the McEliece, Niederreiter and code based McEliece systems.

The first public key cryptosystem was proposed in which they show that two elements in a finite group have the same power when expressed as powers of another element. After the 1976 proposal of RSA, many cryptographic systems based on number theory have been presented. Many of them including RSA rely on hard problems like the integer factorization problem (IFP) and the elliptic curve discrete logarithm problem (ECDLP).

In the year 1994, showed that quantum processors can break the cryptosystems based on IFP and the ECDLP with polynomial time, which would take the exponential time in classical computers. Because of the developing technology, the quantum processors are believed to be existence in near future. For Quantum cryptanalysis, Grover's algorithm is a dramatic breakthrough that shows quantum processors can solve oracle based problems with the order of 2^n in time compared to classical computers that requires 2^(n/2) operations. For example in the case of 2048-bit RSA cryptosystem, the breaking can be achieved within approximately eight hours which is infeasible classical computation for today's supercomputers, whereas with 20 million physical qubits such an attack is possible. Limiting the hardware can shorten the time of seven hours to several minutes [18]. This threat is not a distant possibility considering the investment made in quantum processing

technology and the business growth of online and financial commerce .

4.3 Multivariate Polynomial Cryptography

In the second decade of the 21st century quantum computers become a real threat to currently used public key cryptographic algorithms. The research community collaborates to standardize both post-quantum cryptographic key exchange algorithms and post-quantum cryptographic digital signature algorithms. Curvilinear boneh–lynn–shacham (BLS) signatures have been standardized by IETF. This paper comparatively evaluates the available post-quantum cryptographic algorithms through RSA assumptions that can potentially assume the most significant threat. The performance of these algorithms has been evaluated in terms of the public key size, private key size, signature generation time, signature verification time, and session key establishment time.

The conclusion suggests TOP 5 algorithms that can be even considered to be used. However, compared to the legacy public key algorithms, the evaluation implies that the post-quantum cryptographic algorithms have the significant communication overhead for the establishment of the secure channel. In addition, further developments to minimize this overhead have been described [19]. In this paper, 4 kinds of public key cryptographic algorithms are evaluated. The first kind is signcryption. A signcryption performs both the encryption and signing in one process. The second one is conventional public key cryptosystem. Due to the dual security reinforcement mechanism, there are 2 kinds of public keys. One is the encryption key, the other is the signing key. The third one is a group signature. The group signature scheme allows any of a given set of users to sign a message on behalf of the group to which they belong. However, it is impossible to discover which group member actually produced the signature. The fourth evaluation is the aggregate signature. Aggregation is also discussed.

5. Security Metrics for Post-Quantum Cryptographic Algorithms

Various security metrics are used to assess the strength and performance of different post-quantum cryptographic algorithms including: resistance to quantum and classical attacks, reasonable computational and memory complexity for both sender and recipient, and no priority in modifications compared to existing public-key infrastructure solutions. The availability of implementations, popularity, and age are considered as crucial as standardized algorithms were finalists in this comparison.

Some cryptographic algorithms in the comparison have not withstood the test of time or are relatively unknown in terms of their resistance to attacks. For instance, while isogeny-based cryptographic schemes demonstrate clear potential and have been analyzed by the historical, and lattice-based and code-based cryptographic schemes have been studied. However, recently designed hash-based cryptographic schemes or MQ-PKC schemes based on multivariate polynomials have not been analyzed historically and are not popular. These schemes can be difficult to benchmark with respect to attack resistance.

A number of cryptographic algorithms are not standardized and no implementations exist for them. Proper implementation of cryptographic algorithms can be difficult and non-trivial. Benchmarking using poorly implemented methods, or methods reused countless times, can easily lead to incorrect results. Standardized cryptographic algorithms typically have several implementations that are interoperable and widely agreed upon in tests. This implies that different implementations can be meaningfully compared. Failing to match confidentiality or integrity requirements in standardized algorithms can be seen as a disadvantage. On the other hand, well-analyzed cryptographic algorithms can be more susceptible to attack. Besides, there are concerns about updating standardized cryptographic algorithms or encryption systems based on proprietary technology adopted in existing public key infrastructures.

5.1 Key Size

An important question is how the protocols would behave in the future, in which classical elliptic curve cryptography would probably become insecure. There has been a lot of progress in the design of post-quantum cryptographic schemes. There is a set of public cryptographic primitives that are believed to be secure against classical attacks and should be secure also when large quantum computers are available. The first question that arises is how a transition to post-quantum cryptography would impact the security and efficiency of the Tor network [20].

The performance of lattice-based post-quantum cryptographic schemes is investigated within the Tor network. Both a classical lattice-based cryptographic scheme and a quantum-resistant version of the Ntor protocol are considered. QSOR: Quantum-Safe Onion Routing is a modified version of Tor that can use quantum-resistant alternatives of public-key cryptography. Trade-offs between security and efficiency can be detected based on the chosen cryptographic library. A comparison is made with traditional ciphersuites based on ECC. A particle filter is

used to track with Bayesian methods the bandwidth capacity, at any given moment, of the nodes used for the analysis. Keeping the number of keys exchanged constant, lattice-based cryptography is on average more expensive in terms of lattice reduction (time) than lattice parameters generation due to the larger key sizes. Nevertheless, the Tor network with lattices seems to perform better than initially thought by means of faster key generation compared to classical onions. This study could provide useful guidance for the ongoing efforts to the migration to post-quantum cryptographic algorithms.

5.2 Resistance to Quantum Attacks

Post-quantum cryptography (PQC) supports the security infrastructure of society when quantum computers can break the currently used algorithms easily and when they are implemented broadly. Standardization for post-quantum cryptographic algorithms (PQC) is being actively advanced in international cryptographic standardization institutions. However, the process of upgrading to post-quantum cryptographic algorithms in the operational systems will require a significant overhaul of security infrastructure for their thorough implementation. Complementary implementation of lightweight post-quantum cryptographic algorithms that require less computational power will expand the choice of cryptographic processing for industry and academia. One of the main tasks in the selection of such an implementation is to conduct an analysis of trade-offs of post-quantum cryptographic algorithms such as security, performance, and attack costs. 1 Post-Quantum Cryptography (PQC) is a new cryptographic paradigm devoted to designing and analyzing secure cryptographic systems that provide long-term security against quantum adversaries. PQC algorithms are designed to be resistant to attacks from quantum computers. These schemes are believed to be secure against both classical and quantum adversaries.

PQC includes several distinct cryptographic architectures: hash-based cryptography, lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, and isogeny-based cryptography. However, the current de-facto standards include alternative public-key encryption, key establishment, and digital signature algorithms. These new algorithms are anticipated to be chosen as replacements to classical public-key cryptographic schemes, which have the potential to be broken by quantum attackers using Shor's algorithm. The security of these new schemes is based on mathematical hardness assumptions such as the syndrome decoding, lattice assurance, or multivariate polynomial evaluation problems. A notable aspect of post-quantum algorithms is that they are specifically designed to resist quantum attacks. The resistance of post-quantum cryptography against quantum adversaries depends on certain mathematical assumptions specifically chosen to resist attacks based on quantum algorithms. From a high-level perspective, these problems are chosen to be computationally hard for both classical and quantum adversaries. This ensures the security of these cryptographic systems in the presence of quantum attackers and aims to provide a smooth transition from classical to quantum-safe security.

6. Performance Metrics for Post-Quantum Cryptographic Algorithms

Research studying post-quantum cryptographic (PQC) algorithms has recently been conducted. Current cryptographic standards are considered insecure under quantum computers. The development of PQC algorithms was initiated in 2016 and has finalized multiple rounds of selection. The feature of many PQC algorithms is that a significantly larger key size is needed for equivalent security to classic cryptographic algorithms. Performance analysis and comparison on Kusilverstein, Ntru, and Kyber among 4 different packages are referred to in existing research. In addition, post-quantum security General VPN tunnel establishment can refer to research regarding a quantum-safe onion routing project encrypted by quantum cryptography. The research is intended to analyze and compromise post-quantum security by a classical and quantum attacker model.

Both researchers are unable to attack the post-quantum algorithm in ML-KEM, and they evaluated the security of classic cryptography in TLS 1.3. However, the current IEEE refers to the security of the classic cryptographic algorithm, respectively, not its security and effectiveness. Moreover, in order to mitigate the side-channel attack, use a fixed-base ladder for implementation. This causes the implementation efficiency of ECDH to be much poorer than the common method including R- and left-to-right method. This disadvantage has not been mentioned in previous studies but will be focused on and pointed out in the review. Several studies have been found about the hybrid protocols serving as PQC defenses for known vulnerabilities. At the same time, the right-to-left method is used to compare with the aforementioned poor R-to-L-FBL method.

Despite the different post-quantum security, to the knowledge, the efficiency comparison of lattice ECC and the Ed44827519 protocol has not been found in the published research, but this has been compared by the authors. Other researchers study the impact of migrating all asymmetric cryptography to a quantum-safe alternative on

the performance and reliability of the Tor network. Streams of tagged anonymous messages are forwarded through a series of relays, called onion routers, to provide anonymity and privacy protection . An adversary, to link the incoming and outgoing messages, observes tagged packets at consecutive relays. Tor anonymizes the traffic by attaching the packet to a hermetic envelope, which is constructed using conventional oniom encryption.

6.1 Computational Efficiency

The widespread adoption of public key cryptography for secure communication in networked systems, financial transactions, and data storage has led to the current deployment of national and de facto standards. However, the security of these standardized implementations is at risk due to the inevitable advent of large-scale quantum computers. These machines will efficiently solve the underlying hard problems, hence become susceptible to attacks including secret-key or private key search and factorization. A worldwide research effort is underway to develop an alternative variety of public key algorithms that resist quantum attacks. However, there is an open debate on the real security implications of quantum computers, particularly in light of the constant evolution of algorithmic and hardware-based countermeasures 8.

Countries such as the United States and European members have initiated productive programs to evaluate a selection of best candidates by means of both a strict and an open process. Since quantum-safe algorithmic primitives are built around different mathematical problems from RSA and ECC binds, quantum-resistant PQC (Post Quantum Cryptography) will have a significant impact on the security and efficiency of existing infrastructures. Overall, the migration toward PQC will imply that entities without the updated cryptographic tools will be unable to communicate securely with newer systems, and vice versa. In the early stages of migration toward quantum-safe algorithms, such incompatible entities will be forced to communicate through outdated, less-secure cryptographic means. Therefore, performance trade-offs will be studied, particularly focusing on asymmetric cryptographic algorithms 7.

6.2 Memory Requirements

The first three (k, f, f) triplets. k is the number of quartic polynomials in a set, f defines the number of sets and f is a degree of polynomials are the parameters for FrodoKEM. Intermediate polynomials pack ki(f+1) values in ki 32-bit elements. After sampling, intermediate polynomials are transformed in the input by multiplications both with the binomial matrix and with sampled elements from secret polynomials, that the resultant polynomials satisfy the equation (a, A). (f+1)− (b, B) = Z.

So far, 8 different algorithms have been selected for standardization: Kyber, NTRU, Crystals-Kyber, Crystals-Hila5, Saber, FireSaber, FrodoKEM, and Dilithium. In the NIST PQC project, lattice-based cryptography is one of the main topics of standardization, including Kyber, Saber, and FrodoKEM algorithms. Five security levels are considered for each algorithm due to the different sizes of NTT-transformed polynomials.

In this work, a systematic study has been performed to investigate the hardware resources that post-quantum cryptographic (PQC) algorithms require for implementation. The objective is to provide a comprehensive analysis of NIST PQC algorithms with respect to basic hardware blocks in order to obtain performance and resource utilization information that can assist design decisions, both in selecting the algorithm itself and in selecting the implementation platform. Attention is restricted to two lowest security levels of all lattice-based NIST PQC candidate algorithms: "0" and "1", and should result in a more meaningful comparison. The ASIC hardware necessary to implement the NIST algorithms comprise both keygen and encrypt components. For these two steps, memories, polynomials multipliers, and hashing cores are required. In a subsequent FPGA implementation where the I/O bandwidth is limited, it can serve as a rather limiting factor for multipliers. As the memory is typically the largest memory block in any processing system, the entire processing system could be improved.

7. Methodology

There are diverse post-quantum cryptographic algorithms which can be seen as an evolution of the classical ones. This is especially true as new security models are introduced that postulate stronger adversary models. Can we order these models from the ones that reflect how we used to see security before the natural introduction of quantum attacks until the ones that most closely model the latest post-quantum security notions?

- **Question 1:** Improving upon the vanilla versions of the NIST finalist post-quantum cryptographic algorithms is of great interest to secure their wider adoption. How should one proceed to build truly fast or efficient implementations of push-button post-quantum cryptography?
- **Question 2:** There are standard techniques for the analysis of cryptographic algorithms concerning pre-image resistance and collision

resistance for hash functions and IND-CPA security for encryption schemes. Although these techniques are very useful in the cryptographic domain, are they well suited to measure algorithmic security?

- **Question 3:** Can we build an aggregate post-quantum cipher suite for the Transport Layer Security version 1.3 that would be provably chosen-ciphertext secure? What claims can be made for the underlying key exchange and encapsulations components, and what are the reasons in each particular case?

7.1 Selection of Algorithms for Comparison

Rapid advancements in the field of mathematics and computation science have always led to a drastic change in the field of cryptography. Therefore, to withstand the altering trends of hacking and computation ability of the contemporary hacker, the demand for more robust cryptographic security measures is increasing rapidly. With the threat of Quantum Computing, the conventional cryptographic algorithms, currently in use, are believed to be insecure and out of date. The most well-known and used Public Key Cryptography (PKC) algorithms RSA and ECC are vulnerable to Shor's quantum algorithm, which poses a significant threat to classical public-key primitives 9.

The NIST has initiated a process for the standardization of Post-Quantum Public Key Cryptography algorithms, by organizing public competitions, regarding public key encryption algorithms, public key signature algorithms, and shared key encryption protocols. Different research communities worldwide have shown interest in developing and contributing to the NIST initiative regarding post-quantum cryptographic algorithms. More than eighty techniques of post-quantum cryptography are developed in different countries all across the globe, most of which are based on Lattice, NTRU, and code-based cryptography 8. This paper presents the performance comparison of ten candidate Post Quantum Cryptographic Algorithms, based on various criteria. The aim of this study is to provide a comprehensive evaluation of the practical feasibility of the NIST PQC candidate algorithms. The effectiveness of the candidate PQC algorithms largely depends on the trade-off between the use case requirements and algorithm characteristics. Algorithm's key size, performance, and other issues related to the feasibility of the candidate algorithms as up-coming standards are though-provoking for the implementers. This study also examines how these algorithms can adapt different key sizes more efficiently.

7.2 Experimental Setup

The Tor network is known to provide a certain level of privacy. Its protection is based on the encryption of messages by the onion algorithm. This algorithm utilizes symmetric encryption, in which the same key is used to encrypt and decrypt the messages. With the ability of a quantum computer to solve DLP and ECDLP, the use of RSA and ECC for cryptographic services is no longer safe for future usage. Therefore, the purpose is to assess the question of how fast post-quantum cryptography can be, across public key, private key and digital signature categories. In other words, would it be possible to have cryptography that is as strong and as fast as the one used today? The aim is to provide the reader with an understanding of assessing the security and performance trade-offs of using post-quantum cryptographic algorithms.

The primary objective is to compare the security and performance of multiple sets of cryptographic algorithms. The public key category uses the NTRUEncrypt and the IBM qTESLA schemes. Kyber, NTRUEncrypt, and Provably-Secure hardened were conducted for the key encapsulation mechanism section as they are isogeny-based schemes, and these outperformed the other NIST-security lattice-based schemes. Moving to the private key category, the HCB, LEDAcrypt, and Löbbers schemes were assessed. There is only one post-quantum cryptographic algorithm for digital signatures at NIST level 1 security.

The qTESLA won this competition, thereby ruled out any comparison. Consequently, the time signature scheme used in the experimental setup could not be benchmarked. With the four columns of workable tests being filled, the lattice-based digital signatures were added to key set N, while the corresponding supersingular isogeny digital signatures scheme was added to the lattice-based digital signature scheme set. The testbed is described first, outlining the QoS dataplan and the notebook specifications. The software frameworks used to facilitate the testing are then detailed, before providing information about how the tests were carried out.

8. Results and Analysis

While all PQC key exchanges result in increased SSL Handshake times, including NTRUEncryptL didn't suffer in performance, due to the implemented optimization techniques. Based key exchange schemes are planned to be standardized in SAC, because among them NTRUEncrypt, Saber and Frodo are also among the most performant and had as well the smallest public key sizes. Saber and Frodo managed to keep the most secret key from being sent over the network by incurring more expensive public key

exchanges compared to NTRUEncryptL. Nevertheless, NTRUEncryptL has fewer performance degradation, due to the substantial optimizations in the implementation. NTRUEncrypt, Saber, Couple and Frodo compile C-only implementations of the key exchange, where NTRUEncryptL and Kyber include C and assembly implementations. While the C implementations generally got better results in higher abstraction layers, the assembly optimization of NTRUEncryptL still managed to lower the CPU time for PQC key exchanges. Subsequently, another optimization step could be seen in assembly ciphers and key exchange implementations, while trying to keep them secure. Wherever possible all implementations use the aesni and asmcrypto optimizations. Further, the hybrid key exchange scheme is proposed and compared with PQC to upgrade of TLS. There are currently 3 distinct implementations of a PQ key exchange in TLS, 2 of which are hybrid, pairing a PQ key exchange with a traditional key exchange. TLS libraries did not make use of any domain-specific optimizations for PQC ciphers, but hybrid implementations of post-quantum ciphers on the server side are integrated in standard TLS package.

8.1 Security Comparison

Nowadays, most of internet communications are done using Transport Layer Security (TLS). TLS uses a combination of asymmetric (public-key) and symmetric encryption. TLS version 1.3 only uses public-key encryption for the key exchange. Key exchanges are the encryption schemes that are exchanged to derive a shared key for the symmetric encryption. The encryption part is done using the shared key for improved performance. The new post-quantum cryptographic key exchanges will match the security guarantee of the classical protocols and only degrade the performance by a logarithmic factor of the total number of possible public keys 7. This approach is chosen because most of the keys on the Tor network are reused to avoid additional CPU-intensive asymmetric encryption.

For public-key encryption, the most common method is the Diffie-Hellman key exchange. This protocol has many different ways of implementation, but the base is the same. There are public keys and private keys. The private key is chosen randomly for every communication. With these private keys the devices derive a shared key that is used to encrypt the data. It is possible for an observer of the data to derive the shared key. However, it's difficult to derive the shared key (and decrypt the data) without this information. It can be said with good certainty that this method is secure for the classical computer even though there is a generalization of this method that is vulnerable to the quantum computer by design 9.

8.2 Performance Comparison

This letter presents a comparative performance analysis between Classic McEliece, Dowling, NTRUEncrypt, and Saber, four Post-Quantum cryptographic (PQC) algorithms proposed for key exchange, under both the key agreement and the key encapsulation mechanisms in the group authenticated key exchange (gake) scheme . Since the security of classical public key cryptography (PKC) is undermined by Shor's algorithm running on a large enough quantum computer, a great effort has been devoted to the search for new cryptographic algorithms and protocols, so called post-quantum cryptographic (PQC) algorithms and protocols, achieving alternative ways to ensure the security of communications. Due to the ongoing advances on quantum technologies, the development of a quantum computing is no longer a remote possibility and will pose serious threats to the "classical" cryptographic algorithms on which most of the current security infrastructures are based on. With the intention to secure the current infrastructure and communications against the treat posed by quantum computers, the U.S.

National Institute of Standards and Technology (NIST) launched a post-quantum cryptography project in 2016 and released three standardization rounds with public calls for proposals for new PQC signature, key exchange, and public key encryption algorithms. The third round was concluded in June 2021. The gake scheme aims for the establishment of a shared session key among a group of communicants without the necessity of a Public Key Infrastructure (PKI) or the establishment of pairwise (symmetric) keys among all the group members. In 2016, Jarecki and Li introduced a generic construction of gake protocols using PQC algorithms and a secret-distribution model.

9. Case Studies

This research illustrates a methodology to explore the trade-offs between the security resilience and the computational efficiency of popular post-quantum cryptographic algorithms for four standard security levels. Furthermore, two case studies are provided: a light-weight file encryption tool consumer, and a large-scale data signing and verification service provider. A broad set of schemes are thoroughly investigated under an inclusive assessment framework, encompassing both performance aspects and security considerations based on currently available technologies. This study can empower a streamlined and evidence-based adoption of post-quantum cryptographic solutions across various implementation environments and system requirements.

Since the seminal work in 1994, the era of ubiquitous quantum computing has been deemed an ineluctable time bomb for the current public key cryptographic infrastructure. An array of eminent research organizations and committees have issued calls to arms, as well as a series of draft standards, technical guidance, and algorithm recommendations toward post-quantum cryptographic maturity. A post-quantum cryptographic ecosystem has begun to evolve and will eventually parallel or even supersede the traditional paradigm of RSA and ECC. While public-key post-quantum cryptosystems replace their venerable pristine counterparts, mainstream ciphers and applications will still consist of symmetric constructions. The process of post-quantum cryptography compliance is intricate and demanding careful selections of algorithms, tuning of parameters, resolution of system interdependencies, performance optimizations, and thorough risk assessments. Due to the vast degree of intricacy, with a plethora of algorithms, parameters, implementations, and adjudicatory metrics being involved, a complete solution is needed along with a simple recipe that could efficiently guide the transition, especially for potential adopters.

9.1 Example 1: Algorithm X vs. Algorithm Y

The trend on the adoption of quantum technologies, such as quantum computers and quantum communications, is increasing with the evolution of quantum computing techniques. Quantum key distribution protocol first introduced the research field of Quantum Cryptography 10. There are several developments in academia, industry, and government efforts for the standardized, robust, cost-effective, and efficient replacement of current cryptosystems with their quantum-safe counterparts 8. After the above arguments concerning PQC cryptography, the concern about the adoption of quantum-proof cryptography is increasing.

Post-Quantum Cryptography (PQC) design methods predominantly discussed public key security schemes, such as RSA, Elliptical Curve Cryptography (ECC), and MQ (Multivariate Quadratic) cryptosystem. The design of PQC schnorrq was first announced in the 11 September 2015. The structured Gaussian elimination is present in this schemer. There is a research team from Institute for Quantum Computing in around 4 hours, succeeded to hack all the messages during the main challenge by using a quantum-safe algorithm from PIQUE group. There are 2 grand challenges of two main questions in PQC, but the main focus on Survey of Public Key Schemes. The survey also concentrates on full cryptographic mapping. Varieties of Lattice-based applications are being presented and attracted to no to industry, academia, and government research. In practice, a Field Programmable Gate Array (FPGA) prototype with LWC is fielded as an ML module in a full homomorphic cryptosystem. Major advantages of security post lattice hand keys (A and S), the length of each lead is N, with S < < N and A = SK(s) = (S$\tilde{W}$ + e) mod q, where e ≤ B is the noise. The versatility of the custom LWE symbol (A). Its rank factor row reduce, E. Cramer was proposed LWE knowledge reduction is well known. The lattice-based systems have over 80% performance overhead, compared to modular. A speedup Gaussian Toom routine is the space tree elimination of Gan and its application to remove cloze t-avatars in post sprite and related proves essential.

9.2 Example 2: Algorithm Z vs. Algorithm W

The study in the field of post-quantum cryptographic competitive algorithms is currently dedicated to lattice-based schemes post-quantum algorithms. Randomness from improved hardware devices has made the benchmarks more accurate. Also, despite the expected lower security of the lattices, lattice-based encryption (LBE) decryption times offer clear advantages compared to McEliece family solutions. It seems that on smaller devices, encryption will be slower with LBE family solutions than with LBE solutions. Scheme Z is in almost all cases the fastest in decryption; the only serious competition is scheme W. On the contrary, in the majority of cases, the decryption speed of the W scheme is statistically identical to the R scheme. Therefore, they constitute the slowest decryption scheme in the competition, because they need many samples to decode. Scheme R is relatively faster in the RSA case, but still lags far behind scheme W in the vast majority of cases. Described general guidelines in the procedure of utilizing cryptographic schemes solving real-world problems. The lattice-based encryption scheme was debuted in 1996, but categorically in 2005.

Its candidate was submitted to the National Institute of Standards and Technology's Post-Quantum Cryptography process, which is lining up a challenge against customary public-key cryptographic systems. In 2016 the second-most traditional post-quantum public-key algorithm is Lattice-based encryption. Baseline approaches to superseding the prevalent public-key cryptographic systems depend on the objects that the systems rest on. Assess is to create systems that fundamentally trust only on different algebraic problems, while lattice-based encryption counts on the hardness of a-closest vectorade Lattice (CVP) issues 8.

10. Challenges and Limitations

Quantum computing will change the threat landscape for the security of cryptographic systems. It is an essential step to evaluate the security of cryptographic algorithms in order to save the next generation of cryptographic algorithms before a single quantum computer can destroy a newly launched Internet. In this study, the security and complexity of the newest entrants to the competition are evaluated on current research, not only to acknowledge the possible threats of quantum computers but also to foster the use of more secure and efficient cryptographic algorithms. Post-Quantum Cryptography (PQC) is called the new generation of cryptographic algorithms, and has recently gained significant attention with the large progress in quantum computing. This new type of hardware is expected to break the most commonly used Public-Key Cryptography (PKC) algorithms, such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptosystem (ECC).

Encryption is one of the most important topics in the world. It is considered for the protection of information for thousands of years. Even it's a simple monophonic system, the world war-two's Enigma machine encryption can take many years to solve. As shown by this example, it's important to use high security algorithm in encryption because protection time is always important and if the algorithm is solved time increases. PKC is used for the safety of the Internet.

The RSA algorithm is one of the strongest PKC algorithms commonly used. In particular, the key algorithm was chosen long for higher security. In the RSA algorithm the key of a short number is a multiple of two almost 1024 bits and the product N of P and Q is the public key. When viewed from this perspective, key length of 1024 for a big number in terms of computing is also long and key size in this algorithm is sufficient for general protection. Also in this algorithm the key size of the multiples of two is at least 5-minimum key size in bit length. In brief, multiple-bit numbers of at least five individual multiple numbers of a larger number, calculations were long durum taking a cipher block, block remained intact very small bit and the modulus found after the calculations was so large, then the same keys and short key could not be easily obtained through the key calculation and only cryptography expert teams spending a long time even able to break a simple block or RSA encryption algorithm crypto system 1.

11. Future Directions and Research Opportunities

Post-quantum cryptography is poised to replace current cryptographic primitives affected by Shor's quantum algorithm, which efficiently solves certain underlying mathematical problems. Currently, there are 20 post-quantum cryptographic public-key encryption, key-encapsulation, and digital signature schemes proposed. An experimental evaluation framework is developed to implement and evaluate all 20 proposals in software, which allows to compare proposals that have been so far evaluated using different methodologies and different performance metrics. Furthermore, the framework also enables other researchers to validate the presented results and to carry out additional experiments and comparisons. The experimental evaluation encompasses additional six cryptographic schemes for a total of 26 proposals.

The 26 candidates are evaluated in authentication, key exchange, and hybrid encryption against both classical and quantum adversaries. This largescale analysis allows to better understand the integrated implications of new cryptographic primitives in designing widely-used security protocols, and to better guide future post-quantum cryptographic implementations. Importantly, the evaluation results can be used to advocate post-quantum cryptosystems for further standardization and deployment based on performance metrics, and to highlight vulnerabilities or inefficiencies of certain proposals that should be addressed or mitigated. Additional detailed analysis of the candidate schemes in comparison to standardized and widely-used algorithms is demonstrated them to undertake detailed investigations of lattice-based, code-based, multivariate polynomial-based and hash-based proposals.

Post-quantum cryptographic primitives have to be standardized and post-quantum versions of widely-used and well-deployed cryptographic protocols have to be developed and implemented; ultimately, these security mechanisms have to replace their classical counterparts. Currently, there is an ongoing process of standardizing post-quantum cryptographic primitives which facilitates the adoption and deployment of new security mechanisms. As a result, giving the possibility to experimentally compare the most popular cryptographic schemes through the implementation of post-quantum cryptographic algorithms, several possible research and experimental questions arise.

12. Conclusion

Quantum supremacy proofs the threatening presence of quantum computers in the near future. The most notorious aspect afflicts public-key cryptography. A quantum computer would be able to solve the integer factorization problem, thus breaking RSA cryptosystems. Simultaneously, the elliptic curve discrete logarithm problem can be solved with a famous algorithm. On the other hand, a standardized procedure for the development and selection of quantum

resilient public-key cryptographic standards was initiated. This competition conducted extensive research into mechanisms and algorithms that will be immune to quantum computers. As a result, the first version of the standards and different cryptographic algorithms were described, which will provide the possibility of a cryptographic handshake protected from quantum threats.

However, the quantum threat is accompanied by performance reductions. Desktop computers with GPUs can break asymmetric cryptographic keys using brute force for a long time period. The solution for the appropriate key lengths is to use quantum-resistant cryptographic algorithms. With this application, computational costs rise, execution times lengthen, and energy consumption increases. Testing and evaluating the efficiency of algorithms was emphasized in the proposal of standards. By utilizing GPUs, the implementation of the 1st round of winners is cited, does the job: in terms of the quantum resistance and compatibility of the data packet sizes used in the post-quantum algorithms. As further work, the efficacy of compression algorithms based on the integer and composite variant of a problem will be examined.

Conflict of Interest: The authors declare no conflicts of interest.

Funding: This research received no external funding.

Author Contributions: The author contributed equally to this work. All authors read and approved the final version of the manuscript.

References

[1] D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography. Berlin, Germany: Springer, 2009.

[2] L. Chen et al., Report on Post-Quantum Cryptography, NISTIR 8105. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2016.

[3] G. Alagic et al., Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8309. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020.

[4] G. Alagic et al., Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8413. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2022.

[5] J. Hoffstein, J. Pipher, and J. H. Silverman, An Introduction to Mathematical Cryptography, 2nd ed. New York, NY, USA: Springer, 2014.

[6] L. Ducas and D. Micciancio, "Faster Gaussian sampling for trapdoor lattices with arbitrary modulus," in Advances in Cryptology – CRYPTO 2015, Proc. of the 35th Annual International Cryptology Conference, Santa Barbara, CA, USA, 2015, pp. 703–728, doi: https://doi.org/10.1007/978-3-662-48000-7_34.

[7] C. Peikert, "A decade of lattice cryptography," Foundations and Trends in Theoretical Computer Science, vol. 10, no. 4, pp. 283–424, 2016, doi: https://doi.org/10.1561/0400000074.

[8] [N. Bindel, J. Buchmann, and J. Krämer, "Lattice-based cryptography: The role of security and performance trade-offs," Journal of Cryptographic Engineering, vol. 9, no. 1, pp. 9–32, 2019, doi: https://doi.org/10.1007/s13389-018-0193-6.

[9] J. W. Bos et al., "CRYSTALS–Kyber: A CCA-secure module-lattice-based KEM," in Proc. IEEE Symposium on Security and Privacy (SP 2018), San Francisco, CA, USA, 2018, pp. 353–367, doi: https://doi.org/10.1109/SP.2018.00040.

[10] W. Castryck et al., "CSIDH: An efficient post-quantum commutative group action," in Advances in Cryptology – ASIACRYPT 2018, Proc. of the 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, Australia, 2018, pp. 395–427, doi: https://doi.org/10.1007/978-3-030-03329-3_14.

[11] A. Hülsing et al., XMSS: Extended Merkle Signature Scheme, RFC 8391. Internet Engineering Task Force (IETF), 2018.

[12] D. Aggarwal et al., "Quantum attacks on Bitcoin, and how to protect against them," Ledger, vol. 2, pp. 42–61, 2017, doi: https://doi.org/10.5195/ledger.2017.46.

[13] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proc. 28th Annual ACM Symposium on Theory of Computing (STOC 1996), Philadelphia, PA, USA, 1996, pp. 212–219, doi: https://doi.org/10.1145/237814.237866.

[14] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proc. 35th Annual Symposium on Foundations of Computer Science (FOCS 1994), Santa Fe, NM, USA, 1994, pp. 124–134.

[15] J. Ding et al., "Practical transformations from ideal lattice-based cryptosystems to the ring-LWE setting," ACM Transactions on Privacy and Security, vol. 21, no. 2, pp. 1–37, 2018, doi: https://doi.org/10.1145/3196491.

[16] M. R. Albrecht, S. Bai, and L. Ducas, "A subfield lattice attack on overstretched NTRU assumptions," in Advances in Cryptology – CRYPTO 2016, Proc. of the 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, 2016, pp. 153–178, doi: https://doi.org/10.1007/978-3-662-53018-4_6.

[17] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Progress Report 44, Jet Propulsion Laboratory (JPL), California

Institute of Technology, Pasadena, CA, USA, pp. 114–116, 1978.

[18] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," Journal of the ACM, vol. 60, no. 6, pp. 1–35, 2013, doi: https://doi.org/10.1145/2535925.

[19] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," Journal of the ACM, vol. 56, no. 6, pp. 1–40, 2009, doi: https://doi.org/10.1145/1568318.1568324.

[20] National Institute of Standards and Technology, Post-Quantum Cryptography Standardization: Third Round Candidates. Gaithersburg, MD, USA, 2020.

How to cite this article

M. H. Al-Dulaimi and S. K. Al-Dulaimi, "A Comparative Study of Post-Quantum Cryptographic Algorithms Assessing Security and Performance Trade-offs," *CyberSystem J.*, vol. 2, no. 2, pp. 82-90, 2025. doi: 10.57238/csj.2025.1016

Access this article online