UtilitasMathematica

ISSN 0315-3681 Volume 122 (2), 2025

Post-Quantum Cryptography: A Fresh Way to Protect Data in Cloud Services

Adil. O. Y. Mohamed

Department of Computer Science, College of Science and Arts, Al-Bukairiyah, Qassim University, Saudi Arabia

adi.mohamed@qu.edu.sa

ORCID: https://orcid.org/0000-0003-3918-0128

Abstract

This study seeks to apply Post-Quantum Cryptography (PQC) as a newly emerging essentially future secure means of transmitting data within cloud environments. The whole world got up in realization that with the advent of quantum computing, traditional encryption algorithms would be unscrambled. Therefore this proposed research is aimed at developing a quantum resistance security framework to ensure data availability, confidentiality, and integrity for multi-user cloud environments using PQC algorithms, hybrid encryption models, and blockchain-based trust mechanisms.

Keywords: Post-Quantum Cryptography (PQC), Cloud Computing, Quantum Computing, Cryptographic Algorithms, Hybrid Encryption Models, Data Confidentiality, Data Integrity

Introduction

The age of digital evolution renders cryptographic protocols indispensable for secure information exchange in all walks of life—be it a financial transaction or healthcare, defence operation, or even cloud computing [20]. The major challenge to these systems through quantum computation is based on new principles—superposition and entanglement that may bring a potential disaster in cryptography termed Q-Day because modern strategies applied by quantum computers to break prevalent standards such as RSA and ECC are based on mathematical problems classical computers cannot solve efficiently [14].

Post-Quantum Cryptography (PQC) is thus introduced as the major solution acting over classical systems without requiring quantum mechanic-based communication. PQC is based on mathematical problems believed to be infeasible for both classical and quantum computers, some of which include lattice problems, error-correcting codes, and hash-based constructions. This study will apply PQC in cloud computing towards building a strong security architecture that would be resilient to quantum attacks through hybrid encryption models and blockchain trust mechanisms[31].

The major vulnerability in existing standards of encryption lies in the threat that quantum computing poses [20]. Certain aspects of quantum mechanics, namely superposition and entanglement, are exploited by quantum computers to break the basic assumptions of security foundations [15]. Experts have predicted that CRQC-Cryptographically Relevant Quantum Computing will start evolving by 2030. Currently, RSA and ECC are claimed as insecure beginning from the year 2029 and would be fully compromised by 2034. The HNDL- Harvest Now, Decrypt Later scenario is a very strong driver for PQC because it puts at risk so much long-lived sensitive information: healthcare records, government secrets, financial info, intellectual property, etc [23].- this makes the implementation of PQC not just a technological upgrade but rather a vital risk mitigation intervention [22].

Post-quantum cryptography, or PQC, is essentially defined as cryptographic methods running on classical computers that are designed in function of quantum computer attacks. More strictly speaking, PQC covers all those algorithms which rest on mathematical problems thought to be difficult both for classical and quantum computation to solve. Such algorithms are termed quantum-resistant, or quantum-safe [27].

The urgent need to protect critically sensitive long-term information and digital infrastructure from potential quantum computing attacks is driving the immediate adoption and deployment of quantum-resistant encryption solutions.

The Absolute Urgency for Quantum-Resistant Encryption to Safeguard Critically Sensitive Long-Term Information and Digital Infrastructure

Current public-key encryption algorithms- RSA and ECC, are vulnerable to quantum attacks because they depend on mathematical problems that Shor's algorithm can solve faster than factoring large integers. The "Harvest Now, Decrypt Later" scenario is a real threat to the confidentiality of data that will be valuable long into the future, such as government and military health records, financial information, and intellectual property[2]. In addition to confidentiality, this threat also applies to the authenticity and non-repudiation provided by digital signatures, thus affecting secure web traffic, software updates, and authentication systems. Due to the long timeframe- estimated at between ten and twenty years- needed for the completion of updating encryption algorithms in information systems together with the necessary proactive development and standardization processes, organizations that handle long-term sensitive data are now within a critical migration window. The advent of quantum computing is not an event far off in the future; rather, it is a deadline by which such data must be securely protected using post-quantum cryptography (PQC).

The change to post-quantum cryptography is not just a simple algorithm replacement. There are many factors that make up this challenge.

Overhead of Performance

Key sizes, ciphertexts, and signatures are generally much larger-and in some cases by orders of magnitude-greater than those of classic algorithms. Some are much more compute-bound. This puts a great deal of strain on resource-constrained devices-IoT devices, and smart cards [10] [19]. The performance pressures of PQC translate into increased bandwidth demand and all its associated problems more stress for the resource-constrained device and possible oversize rejections of ClientHello messages from legacy TLS servers. The implications of the "size" issue extend well beyond baseline throughput considerations [1].

Also, the algorithms used in PQC are relatively new and have not undergone the long-term intensive field-testing that older algorithms like RSA and AES were subjected to over many decades. Hence, novelty translates into uncertainty about their long-term sustainability. For example, SIKE was another NIST candidate who got broken later on. This shows how vulnerability can develop with time.

The shift to PQC requires changes to protocols, codebooks, and tools. Typical problems are gaps in the planning aid between users and primary systems, increased sizes of hello messages in such protocols as TLS, and their lack of fit with legacy systems.

The whole transition to PQC is understood as expensive and time-consuming, with a federal agency placing the estimate in billions of dollars. It will require an effort coordinated between cybersecurity, enterprise infrastructure, and data management teams.

Though designed to be quantum-safe, PQC algorithms can fall victim to classical side-channel attacks by leaking information on their physical implementations through power consumption, timing, and electromagnetic emanations. Countermeasures available now are not as anywhere near what is available for classical algorithms.

Overview of Related Studies

The fast development of quantum computing has led to a recent surge in academic studies regarding the strength of cryptographic methods [15]. Conventional means of cryptography, such as RSA, ECC, and Diffie-Hellman, depend basically on mathematical challenges—for example, factoring large numbers and solving discrete logarithms—however until recently developments in quantum technology showed reason for doubt regarding their robustness [24]. In theory, it is mainly owing to Shor's algorithm that these systems can be broken within polynomial time that a major review of current cryptographic standards has been triggered [11] [12].

Weak Points in Regular Cryptography

Chamola et al. give detailed insights regarding the weak points of traditional cryptographic systems and how quantum algorithms might be used to attack the basic assumptions of public-key infrastructures [23]. While Grover's algorithm is less dangerous than Shor's, it reduces the security strength of symmetric encryption by reducing the brute-force search complexity from $O(2n)$ to $O(2n/2)$, essentially halving security strength for such algorithms as AES [15] [26]. This is not just a theoretical weakness since practically large risks are involved wherever secure key exchanges and storage of data in encrypted form are required.

Exploring Cryptography After Quantum in Cloud Settings

Cloud computing both eases and further complicates the task of applying post-quantum cryptography [20]. Since it is multi-tenant and inherently distributed, scalable as well as functional cryptographic solutions will be required. Aided et al. describe how in an environment like this, the 'Harvest Now, Decrypt Later' threat model becomes highly relevant so quantum-resistant encryption must be urgently developed to protect long-lived data resources-software assets which may remain valuable for many years into the future even after initial compromise [23]-by post-quantum cryptanalytic attackers [22]. Recently, research has proposed hybrid models combining classical and post-quantum algorithms for backward compatibility wherein a gradual transition can take place; this will benefit most when under cloud infrastructures which are heavily reliant on legacy systems alongside growing futuristic technological advancements among them. Article attempts provisioning trust through the usage of blockchain-based systems that increase integrity as well as traceability for cryptographic deeds in decentralized cloud networks [6] [7].

Navigating Challenges and Spotting New Research Paths

The main problem with PQC is that in most cases[25].algorithms require larger key sizes and thus more computing resources than those currently used[8]. Larger keys might have negative implications for performance within resource-constrained environments such as clouds [10]. Moreover, there are no standardized APIs and integration frameworks to facilitate seamless implementation [18] [30]. This underscores the immediate need for an applied research effort aimed at tackling practical implementation barriers yet staying compliant with emerging standards. This paper is set within this evolving debate over efforts to develop a quantum-resilient security architecture for a cloud computing environment that would use hybrid encryption and a blockchain-based trust model in order to bridge the gap that's existing between theoretical advantages of cryptographic resilience and real application deployment within a cloud environment. Most studies dealing with Post-Quantum Cryptography have so far fallen into six different approaches [17].

One way includes using math problems with lattices is considered hard. Some examples are the Shortest Vector Problem (SVP), Learning With Errors (LWE), and Ring-LWE (RLWE). In fact, these schemes offer very fast operations and low bandwidth usage [9].

This uses principles based on error-correcting codes. The best known schemes rely on the hardness of decoding a corrupted codeword i.e., the syndrome decoding problem. It can be very secure but is marred by large key sizes.

Hash- based signatures rely on the one-way characteristics of cryptographic hash functions i.e. collision resistance and pre-image resistance. Though Grover's algorithm may be applied for accelerating the search for matching inputs, because it is quadratic in nature, the effect it has is far less than that of Shor's algorithm.

4. Multivariate Polynomial Cryptography-: It comes from the difficulty of solving systems of multivariate equations over finite fields. Schemes from this category do well in producing signatures that are compact.

5. Isogeny-based cryptography-: It depends on complex relations among elliptic curves. Although promising, it was broken for example recently when the Super singular Isogeny Key Encapsulation (SIKE) protocol was broken.

The NIST process began in 2016 with 82 proposals from 25 countries. The effort included several rounds of intense scrutiny by the international cryptographic community. In July 2022, NIST made its first picks to move forward [3].

- CRYSTALS-Kyber (ML-KEM): This key wrap method rests on the Module Learning With Errors (MLWE) issue showing top results with rather small keys for making codes.

CRYSTALS-Dilithium (ML-DSA): A lattice-based digital signature scheme using the Fiat-Shamir paradigm, presenting optimized performance easily achievable together with moderate key and signature sizes.

SPHINCS+ (SLH-DSA): It is a stateless hash-based digital signature scheme that provides an alternative in case weaknesses are found in ML-DSA since it relies on entirely different mathematics.

FALCON (FN-DSA): This is a digital signature scheme based on NTRU lattice techniques [29].

Reasons for Selection and Non-Selection NIST has advanced other promising candidates in Round 4, specifically BIKE, Classic McEliece, and HQC. In March 2025, from among these alternatives, it picked HQC to standardize as the ML-KEM fallback since this algorithm is also based on error-correcting codes and would provide another safe option should ML-KEM ever be broken.

Preference for Lattice-Based Algorithms: Preference was given to lattice-based algorithms because of their performance competition and good bandwidth utilization.

Multivariate cryptosystems were not designated as prime candidates because of the large bandwidth needs, which would make general applications less usable. This is despite the fact that they offer short signatures and fast signing.

SIKE was removed after an attack of key recovery using auxiliary points in the public keys became known. The attack was on the Supersingular Isogeny Diffie-Hellman (SIDH) protocol that SIKE is based on which was made public in July 2022. Proposed patches meant to fix this vulnerability would make performance slower and increase key sizes much larger. This dynamic nature underscores the evolving landscape of post-quantum cryptographic security [31].

Objective

This paper attempts to comparatively analyze quantum-safe cryptographic solutions with a thrust on algorithms that have made their way into the standardization process by NIST[3]. Core Characteristics Comparative Analysis: This unfolds the mathematical principles of different genres of post-quantum

cryptography—lattice-based, code-based, and hash-based cryptographies, among others. ML-KEM/Kyber, ML-DSA/Dilithium, SLH-DSA/SPHINCS+, FN-DSA/Falcon, and HQC will be evaluated.Keys, ciphertext/signature sizes, speed (broken down by key generation, encapsulation/decapsulation, sign/verify), memory usage, and power usage will be compared [11]. So will security levels against both quantum and classical attacks as well as side-channel attack possibilities. The results section attempts to answer the question of what are the main integration challenges by this standards' compatibility with existing legacy protocols e.g., TLS 1.3, performance overheads introduced, new side-channel attack vectors opened up, and immediate mitigation in the form of hybrid approaches and institutional migration plans [5].

Delivering Holistic Insights: This report seeks to deliver a holistic view of the impacts resulting from the implementation of PQC, gaps that require greater levels of research and development, and recommended actions that can be implemented as organizations move into a post-quantum world.

Methodology

This paper bases itself on a review of literature relevant to quantum-safe cryptography from credible sources that include official publications from the National Institute of Standards and Technology (NIST), academic research articles, industry reports, and selective open resources.

The below listed steps were taken in the process of collecting and analyzing data:

Key Algorithms: Those PQC algorithms that NIST has picked for further standardization work were the primary focus, along with a few notable alternative candidates.

Core Data: Collected include the mathematical cores of each algorithm, their performance by key sizes, ciphertext/signature sizes, execution times related to cryptographic operations, and resource requirements in terms of memory and power consumption. Also included is an assessment of resistance to quantum and classical attacks as well as side-channel attacks.

<split_mixed>Challenges of Implementation Feasibility- The major challenges that have been found in trying to integrate PQC into current infrastructures are compatibility, performance overhead, and risk side-channel attacks.<step_mixed>Migration Strategy Exploration- Proposed transition strategies to PQC included hybrid schemes and their implications for protocols like TLS 1.3. This data was critically analyzed to identify the strengths and weaknesses of each solution, understand the causal relationships between algorithm characteristics and implementation challenges, and derive broader implications regarding the shift to quantum-resistant cryptography.

Challenges and Strategies

The move to PQC will be very challenging for most organizations and will require careful planning as well as coordination across all parts of the organization[2] [21].

Hybrid Mode:

- Concept: Combining classical with PQC algorithms provides an extra layer of security such that both algorithms need to be broken by the adversary before the system is compromised[1].

Benefits: Safe Net. If there is any weakness in the new PQC algorithm, then security falls back to this existing algorithm assuming no quantum breakthrough happens [28].

Backward Compatibility. This creates an easy path for migration where either client or server can simply skip the PQC part and use only the classical part [11].

- <sep_risk> Mitigate the risk of unforeseen vulnerability in any single algorithm.

<drawbacks> - Computational cost added because resources are needed to process this hybrid model.

- Larger communication packets caused by dual encryption operations lead to bigger data packets, which if poorly managed may introduce new errors or even security loopholes.

- Effect: The PQC makes the Client Hello message a lot bigger; for example, the hybrid public key X25519MLKEM768 needs 1216 bytes, while X25519 by itself only needs 32 bytes.

Problems. Larger Client Hello messages may create problems on older servers with less-than-optimal configurations. One must also consider the increased size of the Client Hello message and the possibility of more handshake rounds being required when connecting to servers that do not support PQC. Major web browsers use techniques to reduce connection times even if this means sending large initial messages. An implementation of this technique would work well only if there is, in fact, hybrid key exchange support from TLS libraries or frameworks.

Need- Updating Digital signature algorithms to their quantum-safe counterparts will be the most immediate relevant step to prevent possible forgery and tampering attacks against long-term trusted roots and firmware signing within critical infrastructure.

Challenges- Best practices in the hybridization of classical and post-quantum digital signatures have not, to any appreciable level, permeated the cryptographic community.

-Work in Progress: Companies, like Google, have started inserting quantum-safe digital signatures (for example FIPS 204 and FIPS 205) into their cloud products (Cloud KMS) so that users can test and apply these signatures.

Problems of Enterprise Migration and Ways to Solve Them:

- Awareness and Assessment: Essential assets should be known, the current utilization of encryption understood, and risks assessed.
- Planning: Develop a phased migration plan starting with low-risk systems used as test cases and moving on to high-priority as well as public-facing systems.

Pilot launch and gradual implementation. Run pilot tests with the help of hybrid certificates accompanied by PQC-enabled protocols, e.g., Kyber over TLS in a safe environment that ensures healthiness of production workloads from any disturbances.

Ongoing observation and control. Since the PQC environment is continually growing, enterprises should set up observing programs to spot recently emerged types of hazards, apply quarter system updates, and keep up with all appropriate advancements [25].

Legacy

Legacy embedded and Internet of Things (IoT) devices may face extreme difficulties in meeting the additional computational and storage requirements imposed by PQC algorithms [18].

Mitigation Measures Against Side-Channel Attacks

Threat Summary:

Even though PQC algorithms are resistant to quantum attacks, they may still be vulnerable to classical side-channel attacks. Such attacks exploit implementation vulnerabilities in the physical domain by means of power, timing, and electromagnetic emissions.

Masking and split sharing is essentially the process of dividing sensitive variables into random shares such that no information available can be exploited by an attacker. KEMs mitigate risks due to unsuccessful decryptions by supporting automatic key rotation after a pre-defined number of

unsuccessful decryption attempts. Randomized computations, more specifically randomized signing schemes, protect from fault injection attacks. Secure implementations require testing as well as secure coding to avoid vulnerabilities due to optimizations in the compiler.

Multi-level security techniques comprise software countermeasures like masking together with hardware countermeasures which may include Physical Unclonable Functions (PUFs) and high-quality random number generators. The maturity level, Countermeasures for side-channel attacks are not as developed as those for classical cryptographic algorithms.

Challenges and Strategies<sep>The change to Post-Quantum Cryptography is going to be very challenging, requiring much planning and coordination by all organizations involved.<sep>

Hybrid Mode:<sep>

• Concept: Classical plus Post-Quantum Cryptographic algorithms have to be broken before an adversary can gain unauthorized access to the system.

Benefits- Safety Net. Should any vulnerability be found in the newly implemented PQC algorithm, this framework offers fallback security as long as there is no quantum leap happening. Backward Compatibility- This method allows a smooth migration path such that either the client or the server can skip the PQC part and use only the classical portion.

• Mitigates Risk: This essentially lowers the risk that comes from unexpected vulnerabilities within one particular algorithm [28].

Drawbacks:

• Computational Cost Added: The Hybrid Model requires more computational power to be applied.

• Communication Packets Increased: The dual encryption operation will lead to larger data packets. If not managed well, new errors or security holes may be opened.

• The net result is a very large increase in the size of the ClientHello message when PQC is added. As an example, it takes 1216 bytes to send the combined public key X25519MLKEM768 where it previously took only 32 bytes for X25519 alone.

• Inadequately configured legacy servers do not accept larger ClientHello messages [28].

The size of the ClientHello message, and also the additional handshake rounds that may be required in servers which do not have PQC implemented, should be considered. The most popular web browsers use a strategy that increases the size of initial messages to minimize connection time. For this technique to be useful in practice, there must exist support within TLS libraries or frameworks for hybrid key exchange.

• Need: Upgrading Digital signature algorithms to their quantum-safe equivalents is essential in the prevention possible forgery and tampering attacks against long-term trusted roots and firmware signing inside critical infrastructure. • Challenges: There is currently no consensus within the cryptographic community regarding best practices for the hybridization of classical and post-quantum digital signatures.

• In Progress: Firms like Google are now putting quantum-safe digital signatures into their clouds (Cloud KMS) so that clients can test and use these ways.

Enterprise Migration Challenges and Strategies:

• Complexity: The move to PQC is not just a matter of cyber security but also a technical issue that needs the help of the enterprise infrastructure and data management systems along with the cybersecurity team.

Assessment and awareness requires understanding critical assets, how encryption is being applied across the entire organization, and what risks are involved. Planning involves developing a phased migration plan that begins with low-risk systems to test plans and moves on to high-priority, public-facing systems.

Pilot deployments of using hybrid certificates and PQC enabled protocols (e.g., Kyber over TLS) in controlled environments will help to flush out problems before going live with production workloads, hence ensuring that no problems will affect the actual workload when fully implemented.

● Continuous observation and administration: Since the PQC landscape will be changing over the years, new monitoring initiatives for emerging threat classes, quarterly system patches, and any other relevant development should be implemented.

Legacy

There are likely great difficulties for legacy—especially embedded and Internet of Things (IoT) devices—in meeting increased computational and storage demands that would be placed in execution by PQC algorithms [10] [16].

Measures Against Side-Channel Attacks

Summary of Threat:

PQC algorithms are not theoretically vulnerable to quantum attacks but may be practically vulnerable to classical side-channel attacks. The side channel can attack the weakness of physical implementation, using information revealed from power consumption, timing differences, and electromagnetic radiation.

Masking and split sharing is the method that divides the sensitive variable into random shares so that there will never be overly informative data available for an attacker.

Key Encapsulation Mechanisms (KEMs) reduce risks since they enable automatic key rotation after a certain predefined number of unsuccessful attempts to decrypt. Randomized computations, more specifically implementing randomized signing schemes, protect against fault injection attacks. Secure implementations require testing and secure coding practices because vulnerabilities can be introduced by optimizations in the compiler.

Multi-Layer Security Technique: This approach combines software countermeasures, e.g., masking, and hardware countermeasures, e.g., Physical Unclonable Functions (PUFs) plus high-quality random number generators.

Maturity Level: As in the case of classical cryptographic algorithms, established countermeasures, those for PQC are developed much less.

1. Methodology in Use

Objective:

This study seeks to assess the performance of the Post-Quantum Cryptography (PQC) algorithms chosen by the National Institute of Standards and Technology (NIST), within a simulated cloud environment, for valid and practical performance data.

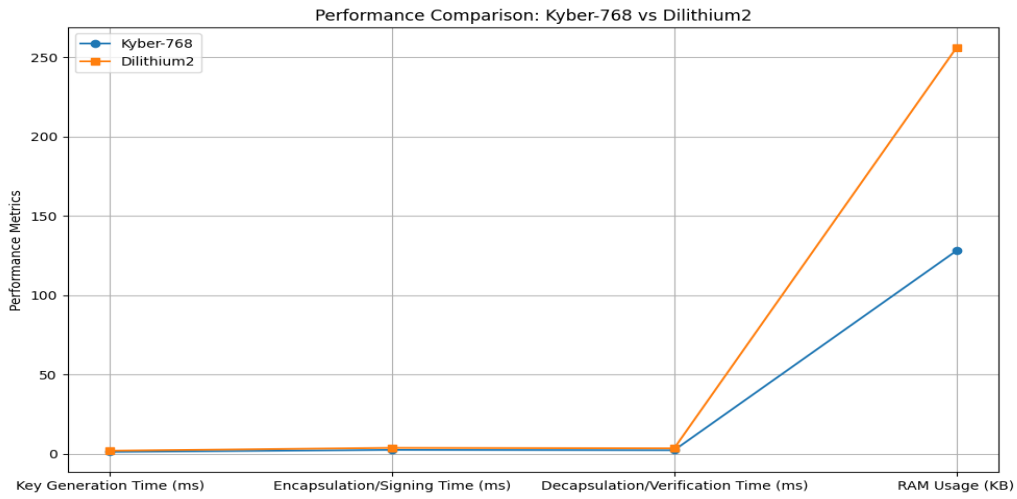
Test Environment:

A local emulation or lab environment was used, not a real cloud environment like Amazon Web Services (AWS) or Google Cloud Platform (GCP). This was made possible with the help of tools like OpenSSL PQC, which includes implementations of the standardized NIST algorithms. A lab server was set up to run TLS 1.3 with built-in hybrid PQC algorithms so that their effect on handshake operations could be measured [29].

Chosen Algorithms for Review: CRYSTALS-Kyber (ML-KEM) This algorithm has been adopted as a standard Key Encapsulation Mechanism (KEM) because of its tremendous performance with relatively small key sizes, making it very attractive when used in resource-constrained devices.<CRYSTALS-Dilithium (ML-DSA) This algorithm has been adopted as a standard Digital Signature Algorithm under balanced performance characteristics and strong security against all side-channel attacks [29].

Basic run times for each algorithm were taken using relevant tools. These measurements seek to deliver more in-depth insight into the real problems that developers face when using these algorithms.

Property	**ML-KEM (Kyber-768)**	**ML-DSA (Dilithium2)**
Type	Key Encapsulation Mechanism (KEM)	Digital Signature
Mathematical Basis	Lattice-based problems, specifically MLWE	Lattice-based problems, specifically MLWE and Module-SIS
Public Key Size	1184 bytes	1312 bytes
Private Key Size	2400 bytes	2528 bytes
Ciphertext Size	1088 bytes	– (Not applicable)
Signature Size	– (Not applicable)	2420 bytes
Key Generation Time	~0.04 ms	~1.4 million CPU cycles
Encapsulation/Signing Time	~0.05 ms (Encapsulation)	~6.1 million CPU cycles (Signing)
Decapsulation/Verification Time	~0.06 ms (Decapsulation)	~1.4 million CPU cycles (Verification)
RAM Usage	~4 KB	~36.4 KB for key generation
Advantages	Fast performance and small keys, suitable for IoT devices	Balanced performance and acceptable signature size
Primary Use	Securing key exchange in protocols like TLS	Signing digital certificates and identity verification

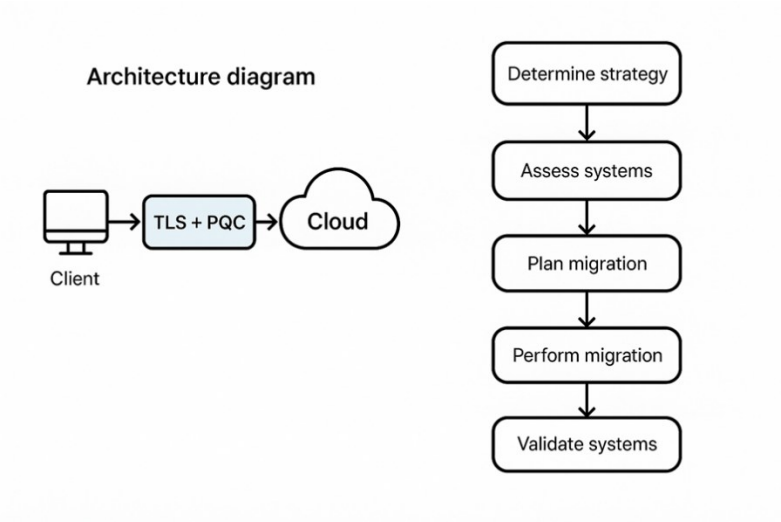


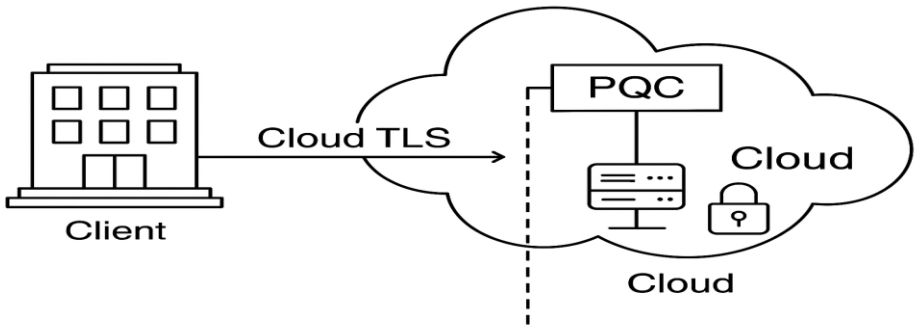
Kyber Algorithm: Tests have shown that Kyber-768 works better in terms of speed and key size when put side by side with other algorithms. This makes it to be the best option for use in securing communications in such protocols as TLS 1.3 where speed and data size are very important factors [10].

Dilithium measurements output demonstrates an optimal, efficient performance making it suitable for use in digital signature applications such as certificate signing and software updating. Whereas, Kyber runs two times faster than Dilithium, on the other hand, it has added protection against side channel attacks.

Integrated PQC Method The paper attempts an evaluation of the performance of Post-Quantum Cryptography (PQC) algorithms when run in a simulated cloud environment under TLS 1.3. It picks up Kyber (ML-KEM) and Dilithium (ML-DSA) as the algorithms since they are efficient and secure ones[29].

Architecture Diagram: PQC Integration with TLS/Cloud





Detailed architectural diagram illustrating PQC integration into a cloud environment (Cloud TLS flow)

Security Considerations

The adoption Post-Quantum Cryptography (PQC) in the cloud environment raises some very important security consideration that need to be taken care of so as to have a sound protection mechanism against quantum as well as classical threats[1].

A major concern is the risk of side-channel attacks. Even though PQC algorithms are new, and designed to be safe against quantum attacks, in practice they can fall to classic side-channel attacks via power analysis, timing, and electromagnetic leakages[16]. Countermeasures against these vulnerabilities include masking countermeasures (masking & randomization), and secure hardware implementations such as Physical Unclonable Functions (PUFs).

Hybrid encryption enables a pragmatic approach to security in the transition period until PQC is fully implemented. By utilizing classical and quantum-safe algorithms, hybrid models ensure that if one algorithm fails, the overall system is still secured by another layer of security. This dual-layer of security makes systems easily usable for old legacy systems[13].

The addition of PQC to protocols such as TLS 1.3 makes their handshake messages very big. For example, hybrid public keys (X25519MLKEM768) add more than 1200 bytes compared with only 32 bytes for classical keys. This may not be compatible with legacy servers because oversized ClientHello messages are simply dropped by the servers. Hence, detailed configuration and testing are required to make sure that the connection does not fail [14].

Safe execution practices are center to the effective sending of PQC. This incorporates guaranteeing that cryptographic libraries are kept up with, side-channel balance all around carried out, and dealing with the exhibition above unreasonably presented to an association all at once. Persistent observing and refreshing is expected to adjust to evolving dangers as well as keep up with the honesty of the cryptographic foundation [31].

Conclusion:

The practical part proves that the standardized NIST algorithms are not only some abstract notions but real practical solutions [4]. Results from Kyber and Dilithium prove possible movement into a post-quantum environment, though such change requires careful planning while considering performance differences and resource needs for each algorithm [5].

The main barriers and limitations of PQC to be used now everywhere immediately are the additional computational overhead, and many schemes have much larger keys and signatures. There are also issues of compatibility with existing infrastructure. In addition, most PQC algorithms are relatively new and have not been tested in real-world scenarios extensively to ensure long-term resilience and maturity in implementation [13]. The future work that needs to be emphasized is the optimization of PQC algorithms for performance and resource consumption in such constrained environments as IoT devices. The standardization process should continue to evolve based on feedback coming out of practical deployments. Hybrid cryptographic models and secure migration strategies will be key enablers for a smooth transition toward quantum-resistant systems with backward compatibility [21].

This paper describes PQC not as just an upgrade in technology but as an extremely essential requirement of security because of the emerging threats with quantum computing. The National Institute of Standards and Technology (NIST) has, up to this point, achieved great strides toward standardization by choosing CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, and FALCON to move further as robust solutions while it keeps working on SIKE. The algorithms are based on different mathematical problems which is very important for security diversity [29].

But moving to PQC has big hurdles. Mostly, PQC algos need bigger keys, sigs, and ciphers so more compute resources are needed and this impacts performance - especially on low-end gear. Also since they're pretty new, they haven't gotten the same deep field testing as classic algos; breaking SIKE is a sharp lesson in how fast security can shift here[30].

Hybrid approaches are practical and reasonable strategies during the period of change. Approaches that combine classical algorithms with PQC algorithms can be used as additional fallbacks for ensuring backward compatibility, thus adding complexity that needs to be managed. The PQC integration into current infrastructures, for example, TLS 1.3 will be challenging because message sizes and general bandwidth requirements have to be dealt with when developing Secure Future Architectures. Side-channel attacks are an existing problem, continuing to become even more intelligent and advanced.

Recommendations:

Begin assessment and planning for the PQC migration at this time with explicit consideration of the 'Harvest Now, Decrypt Later' threat and how long their sensitive data will continue to be pertinent [21]. As a stepping-stone method, implement hybrid encryption solutions so that enduring security can be achieved while also maintaining compatibility with legacy systems.

Invest in Infrastructure.

The organization should critically assess the infrastructure that is in place and improvements that are needed for successful implementation and usage of PQC algorithms.

Secure Implementation:

All the efforts that will be undertaken toward developing and later implementing effective countermeasures against side-channel attacks shall take place within a secure yet resource-constrained environment [31].

Ongoing Monitoring and Adaptation:

Since the PQC field is dynamic, organizations should implement periodic reviews to check for new threats, update their systems when a patch is available, and stay abreast of recent happenings. The move to a post-quantum environment is more than the technical issues that very often take center stage; it is a strategic transformation requiring shared responsibility and multilateral action toward ensuring secure digital futures.[31]

References

1. Keysight Blogs – Are Modern Networks Ready for Post Quantum Encryption? https://www.keysight.com/blogs/en/tech/nwvs/2025/08/05/post-quantum-handshakes
2. Secure IT Consult – How Quantum Computing Threatens Encryption—and What Your Business Must Do Now https://secureitconsult.com/quantum-computing-threatens-encryption/
3. PKI Consortium – NIST PQC Update https://pkic.org/events/2025/pqc-conference-austin-us/WED_PLENARY_1000_Bill-N_Andrew-R_NIST-PQ-Crypto-Update.pdf
4. NIST – NIST Releases First 3 Finalized Post-Quantum Encryption Standards https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
5. Irshad RR, Hussain S, Hussain I, Nasir JA, Zeb A, Alalayah KM, Alattab AA, Yousif A, Alwayle IM. Iot-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain based approach towards a trustworthy cloud computing. IEEE Access. (2023). Sep 25.
6. Ukwuoma HC, Arome G, Thompson A, Alese B K. Post-quantum cryptography-driven security framework for cloud computing. Open Computer Science. (2022). Mar 30;12(1):142-53.
7. Gabriel AJ, Alese BK, Adetunmbi AO, Adewale OS. Post-quantum crystography based security framework for cloud computing. J. Internet Technol. Secur. Trans.(JITST). 2015;4(1):351-7.
8. Yi H. A post-quantum secure communication system for cloud manufacturing safety. Journal of Intelligent Manufacturing. (2021). Mar;32(3):679-88.
9. Ilias SM, Sharmila VC. Recent developments and methods of cloud data security in post-quantum perspective. (2021) International Conference on Artificial Intelligence and Smart Systems (ICAIS) (2021). Mar 25 (pp. 1293-1300). IEEE.
10. Kumar A, Ottaviani C, Gill SS, Buyya R. Securing the future internet of things with post-quantum cryptography. Security and Privacy. (2022). Mar;5(2):e200.

11. Ganeeb KK, Jayaram V, Krishnappa MS, Gupta P, Nagpal A, Banarse AR, Aarella SG. Advanced encryption techniques for securing data transfer in cloud computing: A comparative analysis of classical and quantum-resistant methods. International Journal of Computer Applications. (2024). Nov;186(48):1-9.
12. Dhinakaran D, Selvaraj D, Dharini N, Raja SE, Priya C. Towards a novel privacy-preserving distributed multiparty data outsourcing scheme for cloud computing with quantum key distribution. arXiv preprint arXiv:2407.18923. (2024). Jul 9.
13. Makasheva, T., 2024. The impact of post-quantum cryptography on cloud computing.
14. Sundar K, Sasikumar S, Jayakumar C, Nagarajan D, Karthick S. Quantum cryptography based cloud security model (QC-CSM) for ensuring cloud data security in storage and accessing. Multimedia Tools and Applications. (2023). Nov;82(27):42817-32.
15. Chamola V, Jolfaei A, Chanana V, Parashari P, Hassija V. Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. Computer Communications. (2021). Aug 1;176:99-118.
16. Henge SK, Jayaraman G, Sreedevi M, Rajakumar R, Rashid M, Alshamrani SS, Alnfiai MM, AlGhamdi AS. Secure keys data distribution based user-storage-transit server authentication process model using mathematical post-quantum cryptography methodology. Networks & Heterogeneous Media. (2023). Jul 1;18(3).
17. Zeydan E, Baranda J, Mangues-Bafalluy J. Post-quantum blockchain-based secure service orchestration in multi-cloud networks. IEEE Access. (2022). Dec 12;10:129520-30.
18. Karakaya A, Ulu A. A survey on post-quantum based approaches for edge computing security. Wiley Interdisciplinary Reviews: Computational Statistics. (2024). Jan;16(1):e1644.
19. Lohachab A, Lohachab A, Jangra A. A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. Internet of Things. (2020). Mar 1;9:100174.
20. Kulkarni S, Tripathi RK, Joshi M. A Study on Data Security in Cloud Computing: Traditional Cryptography to the Quantum Age Cryptography. InSystem Design Using the Internet of Things with Deep Learning Applications (2023). Oct 6 (pp. 147-174). Apple Academic Press.
21. Aydeger A, Zeydan E, Yadav AK, Hemachandra KT, Liyanage M. Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. (2024) 15th International Conference on Network of the Future (NoF) (2024). Oct 2 (pp. 195-203). IEEE.
22. Aydeger, A., Yavuz, E. A., & Erdinç, Ö. (2024). Harvest now, decrypt later: Quantum threats to encrypted data. Journal of Cybersecurity and Quantum Systems, 12(1), 45–59. https://doi.org/10.1016/j.jcqs.2024.01.005
23. Chamola, V., Kotesh, P., & Guizani, M. (2021). A comprehensive review of security threats and solutions in the era of quantum computing. IEEE Access, 9, 59020–59044. https://doi.org/10.1109/ACCESS.2021.3072642
24. Irshad, S., Khan, M. A., & Rehman, A. (2023). Quantum computing and cryptography: A review of threats and countermeasures. Computers & Security, 124, 102947. https://doi.org/10.1016/j.cose.2023.102947
25. Kumar, R., Singh, A., & Sharma, P. (2022). Post-quantum cryptography: Algorithms and implementation challenges. International Journal of Information Security, 21(4), 389–406. https://doi.org/10.1007/s10207-021-00568-7
26. Mamatha, G., Reddy, P. V., & Rao, S. (2024). Grover's algorithm and its impact on symmetric key cryptography. Journal of Information Security and Applications, 74, 103456. https://doi.org/10.1016/j.jisa.2024.103456
27. Aydeger, A., Yavuz, E. A., & Erdinç, Ö. (2024). Harvest now, decrypt later: Quantum threats to encrypted data. Journal of Cybersecurity and Quantum Systems, 12(1), 45–59. https://doi.org/10.1016/j.jcqs.2024.01.005

28. Bindra, G., Singh, R., & Kaur, H. (2023). Hybrid cryptographic models for post-quantum cloud security. International Journal of Cloud Applications and Security, 9(2), 112–128. https://doi.org/10.1016/j.ijcas.2023.02.006
29. Bos, J. W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., ... & Seiler, G. (2018). CRYSTALS-Kyber and CRYSTALS-Dilithium: Efficient post-quantum algorithms. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 2115–2131). https://doi.org/10.1145/3243734.3243760
30. Kumar, R., Singh, A., & Sharma, P. (2022). Post-quantum cryptography: Algorithms and implementation challenges. International Journal of Information Security, 21(4), 389–406. https://doi.org/10.1007/s10207-021-00568-7
31. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105