Journal of Technological Information, Management & Engineering Sciences (2023),4(1), 40-52

Evaluating the performance of the post-quantum cryptographic algorithms in the modern network protocols: latency, throughput and security trade-offs

[1] Dr. Hamza Rahman
[2] Ayesha Khan

How to cite this article:

Rahman, H., & Khan, A. (2023). Evaluating the Performance of the Post-Quantum Cryptographic Algorithms in the Modern Network Protocols: Latency, *Throughput and Security Trade-offs. Journal of Technological Information, Management & Engineering Sciences, 4(1), 1–12.*

Received	Accepted	Published
15 February 2023	20 April 2023	15 June 2023

Abstract

Public-key cryptosystems are used in widely adopted protocols for networks, including Transport Layer Security (TLS) and QUIC, and their security is now threatened by the prospect of large-scale quantum computers. In response, the National Institute of Standards and Technology (NIST) has published several standardized post-quantum cryptographic (PQC) algorithms, such as Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM, formerly CRYSTALS-Kyber) and Module-Lattice-Based Digital Signature Algorithm (ML-DSA, formerly CRYSTALS-Dilithium). This paper brings together recent empirical investigations of these algorithms applied to modern network protocols, highlighting their latency, throughput and security trade-offs. The analysis is based on controlled lab studies and heterogeneous platform benchmarks conducted since 2023 up to 2026, illustrating that lattice-based schemes, especially ML-KEM and ML-DSA, add a small amount of computational cost on server-class machines and hybrid schemes (classical–post-quantum) also help reduce the transition risks. However, size of the key and the signature do have a significant impact on handshake latency in the presence of high round-trip-time network conditions, lossy networks, or bandwidth-constrained networks since they lead to higher numbers of packets and increased interaction with congestion-control mechanisms. The overhead for PQC is absorbed well by QUIC, as compared with TLS over TCP. They show that most Internet-scale applications can be deployed without significant performance overheads, and that careful algorithm selection, hybrid modes, and protocol-level optimizations can allow for such applications to be quantum-resistant. Security levels and practical considerations for the multi-year migration period are discussed and recommendations are given to practitioners on balancing security levels against operational considerations.

Keywords: *post-quantum cryptography, TLS 1.3, QUIC, ML-KEM, ML-DSA, hybrid cryptography, handshake latency, throughput, NIST standardization, security trade-offs*

1. Introduction

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.

Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

Confidentiality, integrity, and authentication are the basis for virtually all modern network protocols: public-key cryptography. To date, algorithms such as integer factorization and discrete log algorithms, including RSA and elliptic-curve cryptography (ECC), have been used to deliver adequate security for decades. Shor has, however, devised an algorithm for a quantum computer that can solve these basic hard problems in polynomial time, making classical public-key schemes vulnerable (Shor, 1997). While cryptographically significant quantum computing hardware has not yet materialized on a large scale, the "harvest-now, decrypt-later" threat model and long lifetimes of many existing deployed systems and stored data warrant the need to urgently transition to quantum-resistant cryptography.

In 2016, NIST started a multi-year standardization effort that led to the release of three new Federal Information Processing Standards (FIPS) in 2024: FIPS 203, 204 and 205. The standards include ML-KEM for key encapsulation, ML-DSA for digital signatures and SLH-DSA (based on SPHINCS+) as an alternative to digital signatures based on hashing. Authorized candidates like Falcon (FN-DSA) are also being considered for the standardization process, with HQC being selected as an additional candidate for further standardization to diversify the portfolio of key establishment candidates (National Institute of Standards and Technology [NIST], 2024a, 2024b, 2024c, 2025). Especially as these algorithms are deployed within high-volume protocols like TLS 1.3 (which protects most Web traffic) and QUIC (which supports HTTP/3), the practical deployment of these algorithms brings up important questions regarding performance. The use of larger public keys, ciphertexts, and signatures consume more bandwidth and can interact negatively with TCP congestion windows, packet-loss recovery, middlebox behavior, and initial congestion-window limits.

This paper offers a systematic review of the recent empirical performance assessments. It discusses computational latency of standalone primitives, end-to-end handshake latency and throughput for TLS and QUIC on various network scenarios, and the security–performance trade-off of pure post-quantum constructions versus hybrid ones. The objective is to raise awareness of those

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.

Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

implementing the protocol, designing the protocol, and running the system about the real-world expenses of migration and when the expenses become a factor. The work brings together results of controlled experiments, from heterogeneous hardware benchmarks and from real-network measurements published up to 2026 to provide a coherent picture of the state of PQC readiness for network protocols.

2. Literature Review

2.1 NIST Post-Quantum Standardization and Algorithm Families 2.1 NIST Post-Quantum Standardization and Algorithm Families

Candidates from three general categories – lattice-based, code-based, multivariate, and hash-based – were evaluated by the NIST process. Two types of lattice schemes, derived from two problems called the Module Learning With Errors (MLWE) and Module Short Integer Solution (MSIS), proved to be the most balanced with respect to security confidence, performance and maturity of implementation. There are three sets of parameters for ML-KEM that support NIST levels 1, 3, and 5, with public-key sizes of about 800 to 1568 bytes and ciphertext sizes of 768 to 1568 bytes. The size of the signature produced by ML-DSA is approximately 2420–4595 bytes at different security level. At the expense of more complex floating-point arithmetic and extra side-channel considerations, Falcon produces more compact signatures (around 666-1280 bytes). While the security assumptions made by SPHINCS+ are conservative, based on the hash functions, its signatures are significantly larger, from several kilobytes to tens of kilobytes depending on the parameter set selected for size and speed optimization (NIST, 2024a, 2024b, 2024c).

Later rounds were used to keep or further develop code-based alternatives like BIKE, HQC, to ensure cryptographic diversity. These schemes tend to have greater public keys or ciphertext sizes than a structured lattice and thus higher bandwidth costs, but have different performance characteristics in lossy or bandwidth constrained environments (NIST, 2025). Given that there are several standardized and near-standardized options, the protocol designer can choose the algorithms based on the target environment.

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.
Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

2.2 Standalone Primitive Performance

Optimized implementations of ML-KEM perform key generation, encapsulation, and decapsulation in well under 1 millisecond for today's x86-64 processors, typically faster than RSA-2048 and comparable to ECDH on NIST P-256 curves with AVX2 instructions (Demir et al., 2025). The total cycle time of Kyber-512 (ML-KEM Level 1) is reported to be 0.02 to 0.13 ms with vectorized code, and even for the highest security parameter set is below 0.3 ms in the reference implementations. Signing is a relatively time-consuming process (a few hundred microseconds to low milliseconds) but is still faster than Dilithium than verification. The key generation and signing operations of Falcon show the most variation and sensitivity to the floating-point implementation details, with its verification being one of the fastest signature schemes that have been studied.

When compared to high-end servers a factor of 5-12× more data is required to be executed on resource-constrained platforms including ARM Cortex-A series processors or microcontroller-class devices typical of Internet-of-Things (IoT) and edge deployments. However, the relative efficiency of the lattice-based schemes is mostly maintained; that is, MDPI Cryptography 2025 and constrained-device studies 2024, ML-KEM and Dilithium are the most efficient of the NIST-selected schemes. Memory footprints, too, vary: Lattice schemes typically need a small working memory, while some code-based and hash-based schemes have to reserve more memory for buffers, which may be limiting on devices with only a few hundred kilobytes of RAM.

2.3 Integration into TLS 1.3 and QUIC

There are a number of empirical studies that have measured the computational complexity of pure ML-KEM handshakes, comparing against X25519 in the same pure environments (Henrich et al., 2025; layered TLS analyses, 2026; Elsevier Computer Networks, 2026), and they have consistently reported the few milliseconds of additional computational overhead in production-grade libraries (OpenSSL, BoringSSL, and QUIC stacks like lsquic and quiche). The hybrid constructions that use a classical ECDH share and an ML-KEM share have marginal extra costs (typically a few hundred microseconds) and remain secure against

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.

Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

classical and quantum attackers during the transition period. This blended approach has been generally recommended as a viable migration strategy.

The size of the signature has more impact on the number of handshake bytes than the size of the key-encapsulation. This is because a naive substitution of ECDSA certificates with ML-DSA certificates will increase the size of the ServerHello–Certificate–CertificateVerify flight by 10–18 KB, which could exceed the initial congestion window for many TCP stacks, and thus cause additional round trips (Kampanakis & Weibel, 2025). The effects of the larger messages are more noticeable under realistic network conditions such as higher latency (50-150ms RTT), packet loss rates of 1-3%, or bandwidth constraints. Studies that mimic or measure along intercontinental routes demonstrate the highest degradation for algorithms using most massive objects (some of the HQC and BIKE parameter sets, SPHINCS+); other algorithms, such as ML-KEM with Falcon or appropriately sized Dilithium, are still competitive (Henrich et al., 2025, Springer ISC proceedings).

QUIC's design features, such as stream multiplexing, independent packet-number spaces, and increased loss-recovery aggressiveness, can often lead to lower relative penalties for PQC than TLS-over-TCP. Based on comparative evaluation, QUIC handles the extra cryptographic data with greater grace particularly on lossy paths (ScienceDirect 2026). This means that the journey towards HTTP/3 will be less painful for environments already on the path of moving to the new protocol, as opposed to those still on the traditional TLS/TCPs.

2.4 Prior Benchmarking Frameworks and Real-World Observations:

Initial experimental evidence for the potential of post-quantum key exchange at Internet scale with small latency impact, under typical network conditions, has been obtained by early large-scale experiments by Google and Cloudflare. These findings have been refined by subsequent laboratory frameworks that systematically change latency, loss rate and bandwidth, allowing to differentiate between the contribution of the cryptographic object size and pure computation (Paquin-style emulation frameworks; Sosnowski et al., 2023). The overwhelming majority of PQC handshake costs are in the ClientHello construction, and not in

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.
Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

the TLS server-side cryptographic operations, and more recent multi-layer analyses decompose TLS handshakes into four phases: TCP handshake, TLS context initialization, cryptographic exchange, and application response (layered analyses, 2026). These methodological advances allow better precision in the attribution of performance costs and in designing optimization strategies.

3. Research Gap

While there are many studies measuring the performance of individual algorithm implementations or single-protocol handshakes, comprehensive side-by-side performance comparisons that take into account latency, throughput, hybrid versus pure modes, and the effect of PQC object sizes and congestion control on both TLS and QUIC under controlled but realistic network conditions are relatively few. In addition, much existing research has been done in lab or data center settings; far fewer measurements include the impact of certificate chains, middlebox interference, and heterogeneous client devices on end user metrics like time-to-first-byte or full page-load time. Production hybrid data is just starting to come out on the long haul. This paper aims to fill the void by consolidating the latest multi-layer and multi-protocol measurements into a unified latency–throughput–security design space to illustrate advances made and remaining uncertainties to be pursued via future empirical study.

4. Objectives

The main aims of this synthesis are fourfold:

2. To measure the computational and bandwidth costs of NIST standardised and 4th round PQC algorithms as compared to classical algorithms within TLS 1.3 and QUIC.

2. To determine the operational conditions (latency, loss, bandwidth) of a network where PQC latency has an impact on the typical Internet applications.

3. To perform a comparison across diverse hardware architectures between pure quantum, hybrid and classical configurations in terms of security and measurable performance.

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.

Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

4. To come up with working suggestions for algorithm selection, certificate-chain management, and protocol tuning to minimize performance–security trade-offs during the migration period.

5. Methodology

It is a structured literature synthesis and secondary analysis of peer-reviewed empirical work and high-quality technical reports published between 2023 and the early part of 2026, with a particular focus on the most recent literature. We decided to include algorithms if they were measured in one of the at least one NIST-selected or the fourth round of PQC algorithms, implemented in TLS 1.3 or a QUIC implementation, and reported latency, throughput, handshake-size, or similar metrics under documented hardware and network conditions. IEEE, ACM, Springer, MDPI Cryptography, Elsevier Computer Networks, NIST publications, and arXiv preprints that later were published in refereed journals or in major industry workshops were sources used to find primary sources.

Where possible, results were normalized to common NIST security levels (Levels 1, 3, and 5), and compared to classical baselines (X25519, ECDSA P-256, and RSA-2048/3072). Studies reported both median and tail latency (p95, p99) statistics and those that controlled or systematically varied network parameters (RTT, loss rate, bandwidth) were emphasized. For this paper no new experimental data was produced but instead all quantitative statements refer directly to the cited primary studies. The synthesis aims for internal consistency in methodology of measurement within the individual sources, but recognises that there are variations in hardware, software stack and experimental design between sources.

6. Results

Computational Latency of Cryptographic Primitives (6.1)

Using a state-of-the-art CPU supporting AVX2 or similar vectorization, the implementation of ML-KEM-512 takes about 0.02–0.13 ms for a single round of key-generation–encapsulation–decapsulation, faster than or competitive with the RSA-2048 standard and faster than X25519 (Demir et al., 2025). The higher the parameter sets, the more roughly linear the security level. Signing takes ~0.1-0.45 ms (0.1 ms or less with optimization) in reference implementations; verification is

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.
Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

much faster. Falcon verification is one of the fastest signature schemes studied, often times taking only a few tens of microseconds to perform on server-grade hardware. The absolute times increase for constrained devices, but the relative ranking of the lattice based schemes remains unchanged, thereby justifying them as primary candidates in most deployment scenarios (MDPI Cryptography, 2025).

6.2 Handshake Latency and Size in TLS 1.3.

In low latency lab settings, the extra computation time of ML-KEM is often < 1-3ms and often hidden in the network's RTT. Hybrid X25519+ML-KEM allows for only a few hundred microseconds overhead on top of a pure classical and pure ML-KEM handshake (layered TLS analyses, 2026). Multi-layer decompositions show that the most visible PQC impact tends to be in the construction of the ClientHello and TLS context initialization on the client side, not in the exchange of cryptographic operations itself. Under controlled load, median end-to-end handshake delays of 15-25 % have been reported when using hybrid and pure ML-KEM configurations compared to using pure X25519, although differences are still small (a few milliseconds) for short RTT.

In most realistic situations, the most important variable is the size of the message. It has been shown in studies that pure ML-DSA certificate chains are able to improve the amount of handshakes by about 5-7 times compared to classical ECDSA chains. If the resulting flight exceeds the initial congestion window, an additional round trip is added, increasing the median handshake latency by a few milliseconds to tens of milliseconds based on the path RTT (Kampanakis & Weibel, 2025). For latency critical applications, tail latencies (p95 and p99) are more susceptible to these size induced effects than the median value.

6.3 Adverse Network Conditions (ANC)

If there is a lot of packet loss (3–5 %), and if the bandwidth is reduced, it increases the loss of the schemes that are separated over many packets. The bigger the object size, the bigger the degradation: HQC and some sets of BIKE show the highest degradation, whereas ML-KEM combined with Falcon or properly-sized Dilithium chains are relatively resilient (Henrich et al., 2025). By evoking the initial congestion window or by using certificate compression, or by distributing

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.
Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

certificates using DNS, most performance is recovered. The absolute effect of this extra data, although more pronounced for high-RTT intercontinental paths, is still not substantial for typical web content after the handshake is over, and the relative portion of cryptography to the overall page-load time remains low.

Lastly, the results of comparing 6.4 QUIC with TLS.

Comparative evaluations show that QUIC consistently decreases the relative performance degradation of the post-quantum primitives relative to TLS over TCP, particularly on lossy paths. The benefit of this is the stream multiplexing, independent packet-number spaces, and recovery mechanisms of QUIC that are more aggressive (ScienceDirect Computer Networks, 2026). While both protocols have the highest overhead for Hybrid KEMs, the pure ML-KEM provides a good security–performance trade-off. The post-quantum transition, on the other hand, seems less disruptive than for pure TLS deployments, for environments already using or planning to use HTTP/3.

A through B is the design assumption that is verified when testing.A through B is the design assumption that is tested.

After the handshake is complete, bulk data transfer throughput is mostly determined by the symmetric authenticated encryption with associated data (AEAD) cipher used, which is usually AES-GCM or ChaCha20-Poly1305, and the choice of asymmetric algorithm has little effect. The biggest performance difference for PQC seems to be in the rate of connection establishment and short lived latency of sessions, not sustained throughput. For the metrics of the web pages loading, it is observed that the load time of the web pages is degraded by just 1–2 % even if the handshake latency increases by several percent under realistic 4G and simulated network conditions (Kampanakis & Weibel, 2025). This is because handshake time is a small portion of the time required for a moderate **size page to load.**

6.6 Platform Heterogeneity

Modern desktop- and server-class hardware can accommodate PQC overhead without significant impact (typically <5 % extra latency). In contrast, the relative cost for edge and IoT devices can be orders of magnitude greater, with the

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.
Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

computational needs varying by an order of magnitude between different algorithms at the same security levels (MDPI Cryptography, 2025). The choice of algorithm for these platforms will therefore have to be based on the smallest miminimum set of parameters and the fastest verification schemes. Hybrid modes continue to be appealing on devices with limited resources where it may not be possible to replace all the cryptographic components at the same time, or where there is fallback or gradual transition.

7. Discussion

The overall evidence shows that computational expense for NIST primary algorithms is not a major barrier to use on server and desktop platforms. Optimised implementations of ML-KEM and ML-DSA run in time that is deemed satisfactory, and in many cases this is hidden by the latency of the network. The more significant trade-off is bandwidth vs. latency when there are sub-optimal network scenarios. Larger cryptographic objects interact with these protocols in such a way that can result in additional round trips and inflated tail latencies from TCP congestion control, initial window sizes and packet-loss recovery. These effects can be significantly reduced using protocol-level mitigations such as certificate compression, higher initial congestion windows, DNS-based certificate distribution and careful chain construction.

Hybrid modes offer a promising middle ground: they will be secure assuming a lattice-based assumption is invalidated, and they will be a relatively small overhead if it is. Pure post-quantum deployments with ML-KEM and ML-DSA or Falcon are already viable for long-lived or high-security scenarios, with optimised certificates chains. In resource-constrained environments, there is a greater trade-off. If the absolute (amount of time) increase in latency is important on such old hardware as IoT, then the smallest parameter sets and the most quickly verifiable schemes will be preferred. Thus, protocol designers need to demonstrate algorithm agility and to enable clients and servers to agree on the best possible mixture of algorithms for the observed path characteristics and device capabilities. Security is always at the forefront. Currently, the family of lattice-based schemes has the best performance/cryptanalytical confidence of the standardised ones. In

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.
Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

cases where the size of the signature is acceptable and there is no need to rely on lattices for the keys, hash-based signatures like SPHINCS+ provide a conservative solution. It is important to monitor cryptanalytic progress, side-channel resistance and implementation quality throughout the migration process, which will typically span several years. Multiple standardized algorithms will further facilitate a defense in depth strategy where various algorithms can be used for various scenarios and/or can be cycled as threat surfaces change.

Operational tooling, certificate lifecycle management and monitoring of handshake failure rates are key areas of focus today, from a systems perspective, as part of the transition. Initial production hybrid implementations have shown this to be possible, but the implementation of pure post-quantum operation at Internet scale will require ongoing improvements in the cryptographic implementations, as well as in the protocol and infrastructure stack.

8. Conclusion

Many Internet applications will be able to use post-quantum cryptographic algorithms standardized by NIST with an acceptable performance penalty. The best latency/throughput/security tradeoff known today is provided by ML-KEM and lattice-based signatures. Hybrid constructions are also effective in minimizing migration risk with minimal extra cost and are advocated as a transitional measure. The major remaining issues are congestion control under poor network conditions with larger cryptographic objects and the increased per-device price of the type of devices involved. Almost all penalties observed can be reduced by protocol optimizations including certificate compression, larger initial windows, DNS-based certificate delivery, and algorithm agility.

These recommendations will need to be refined as implementations progress, as more data becomes available from the real world and as other algorithms become standardized. Organisation should start planning and testing hybrid deployments in early 2022, first in some high value or long-lived systems, and keeping an eye on performance metrics and the changing cryptanalytic landscape. By carefully choosing algorithms and paying attention to the protocols at the quantum level, the shift to network security with quantum-resistant protocols can be made

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.

Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

without compromising the responsiveness and scalability required by the modern Internet service.

References

Demir, E. D., et al. (2025). Evaluating and implementing post-quantum cryptography algorithms in the industry. Cryptography.

Henrich, J., et al. (2025). There is a lot of data and added complexity: What impact does PQC have on my TLS connection? In ISC 2025 – The 28th International Conference on Information Security, 2025. 107–128). Springer. https://doi.org/10.1007/978-3-032-08124-7_6

Kampanakis, P., & Weibel, A. (2025). (Yet another) study of the impact of MLWE in selected TLS use-cases. Transcribed from a presentation made at the NIST Sixth PQC Standardization Conference.

National Institute of Standards and Technology (NIST). (2024a). Key-encapsulation mechanism standard (FIPS 203) based on module-lattice. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203

The National Institute of Standards and Technology. (2024b). Digital signature standard (FIPS 204) based on modules lattice. The U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.204

The National Institute of Standards and Technology. (2024c). State-less hash-based digital signature standard (FIPS 205). U.S. Department of Commerce. 205. https://doi.org/10.6028/NIST.FIPS.205

National Institute of Standards and Technology. (2025). Status report on the fourth round of the NIST post-quantum cryptography standardization process (NIST IR 8545). https://doi.org/10.6028/NIST.IR.8545

Rios, R., & Montenegro, J. A. (2026). Multi-layer Bottleneck Analysis of Post-quantum Cryptography. International Journal of Information Security, 25, Article 89. https://doi.org/10.1007/s10207-026-01242-0

Shor, P. W. (1997). Prime factorization algorithms and discrete logarithm algorithms in polynomial time on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.

Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.

Sosnowski, M., et al. (2023). The performance for TLS 1.3 post-quantum. In coNEXT '23 Companion, the 19th International Conference on Emerging Networking EXperiments and Technologies. 19–27). ACM. https://doi.org/10.1145/3624354.3630585

Various authors. (2024). Constrained device performance benchmarking with the implementation of post-quantum cryptography. Cryptography, 8(2), Article 21. https://doi.org/10.3390/cryptography8020021

Various authors. (2025a). A useful practical performance test of post-quantum cryptography on heterogeneous computing. Cryptography, 9(2), Article 32. https://doi.org/10.3390/cryptography9020032

Various authors. (2025b). Further analysis of the performance of new TLS 1.3 cryptographic standards in post-quantum key exchange. Cryptography, 9(4), Article 73. https://doi.org/10.3390/cryptography9040073

Various authors. (2025c). Evaluation of QUIC protocol in a comprehensive way using post-quantum cryptography. The IEEE Conference on Communications and Network Security (CNS) 2025 will be held in Paris, France. https://doi.org/10.1109/CNS66487.2025.11195046

Various authors. (2025d). Security and performance analyses of post-quantum digital signature algorithms and their TLS and PKI integrations. Cryptography, 9(2), Article 38. https://doi.org/10.3390/cryptography9020038

Various authors. (2026a). Performance of post-quantum handshake between QUIC and TLS. Computer Networks, 275, Article 111957. https://doi.org/10.1016/j.comnet.2025.111957

Various authors. (2026b). Supporting layered TLS 1.3 handshake analysis: Classical, hybrid and pure post-quantum key exchange. arXiv preprint. https://arxiv.org/html/2603.11006

[1] Department of Computer Science, Islamia College Peshawar, Pakistan.
[2] Department of Computer Science, Islamia College Peshawar, Pakistan.

Copyright (c) 2023 Author(s)
This work is licensed under a Creative Commons Attribution 4.0 International License.