Challenges of DNS in the Post-Quantum Era: Improving Security with Post-Quantum TLS

Abdullah Aydeger†, Sanzida Hoque†, and Engin Zeydan*

***Abstract*—The Domain Name System (DNS), an important component of the Internet infrastructure, is vulnerable to various attacks that can jeopardize the security and privacy of Internet communications. While DNS over TLS (DoT) is widely used to improve DNS security, the advent of quantum computing poses a significant threat to the underlying cryptographic algorithms used in TLS. In this paper, we propose a comprehensive framework for DNS over Post-Quantum TLS (DoPQT) to address this challenge. Our framework integrates post-quantum cryptographic algorithms into DoT, ensuring robust security against both classical and quantum attacks. We introduce a hybrid key exchange mechanism and post-quantum authentication procedures to protect the confidentiality, integrity, and authenticity of DNS traffic. DoPQT has the potential to offer comparable performance to existing solutions while demonstrating superior quantum resistance. This research contributes to the development of a secure and resilient DNS infrastructure in the post-quantum era. It has been observed that the handshake process is most affected by increased DNS queries and is the main source of the bottleneck. On the other hand, the percentage loss in throughput when using the PQC algorithm (i.e., ML-KEM) is about 33-40% for different DNS queries.**

***Index Terms*—DNS Security, TLS, PQC**

I. INTRODUCTION

The Domain Name System (DNS) is a fundamental component of the Internet. It enables the conversion of human-readable domain names into machine-readable IP addresses. This central function makes the DNS a prime target for various cyber threats, including cache poisoning, man-in-the-middle attacks, and DNS hijacking [1], [2]. Such attacks can have serious consequences, such as data exfiltration, unauthorized censorship, and redirection to malicious websites [3]. To mitigate these risks, DNS over TLS (DoT) was introduced, which encrypts DNS requests and responses to prevent eavesdropping and manipulation attempts [4]. However, the emergence of quantum computing poses a significant risk to the security of existing cryptographic protocols, including those used in TLS [5]. The extraordinary computational capabilities of quantum computers could potentially crack the public-key cryptographic algorithms that currently secure DoT, making DNS traffic vulnerable to sophisticated quantum-enabled attacks. This potential vulnerability underscores the urgent need to transition to Post Quantum Cryptography (PQC), which is designed to withstand the challenges posed by both classical and quantum computing [6].

† Dept. of Electrical Engineering and Computer Science, Florida Institute of Technology, Melbourne, FL, USA.

* Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), Barcelona, Spain.

(E-mail: aaydeger@fit.edu, shoque2023@my.fit.edu, engin.zeydan@cttc.cat)

DOI: 10.36244/ICJ.2025.3.2

Recent research has explored various post-quantum cryptographic schemes that could be integrated into DNS protocols to enhance security against quantum threats [7]. For instance, implementations of lattice-based cryptography and hash-based signatures have been suggested as viable options for securing DNS traffic in a post-quantum world [8]. Furthermore, the importance of transitioning DNS infrastructure to support quantum-resistant algorithms is gaining traction, with several proposals advocating for hybrid approaches that combine classical and post-quantum cryptographic techniques [9].

To address these concerns, we propose the integration of PQC into DoT, creating what we term DNS over Post-Quantum TLS (DoPQT). This approach is critical for ensuring the long-term security and resilience of DNS in the face of advancing quantum technologies. The main contributions of this paper are as follows:

- The paper introduces a novel integration of DNS with Post-Quantum TLS, aiming to protect DNS queries and responses against quantum computing attacks. This ensures that DNS communications remain secure in the post-quantum era.
- The paper provides a comprehensive performance evaluation of DNS over Post-Quantum TLS, demonstrating that the approach can be practically implemented with minimal impact on DNS query latency and overall system performance.
- A detailed security analysis is conducted, showing that the proposed method provides strong resistance to both classical and quantum attacks, highlighting the robustness of Post-Quantum TLS for DNS protection.
- By proposing this integration, the paper contributes to the future-proofing of DNS infrastructure against the growing threat of quantum computing, paving the way for broader adoption of post-quantum security measures in internet protocols.

The subsequent sections of the paper are structured in the following manner: Section II presents a concise overview of the existing literature on strategies for secure DNS solutions. Subsequently, the proposed approach is introduced in Section III. Section IV provides theoretical comparisons in terms of security and other metrics. Section V depicts the simulation setup and presents the findings of our evaluation. Section VI discusses the comparative analysis of PQC candidates and outlines future directions and efforts. Finally, Section VII concludes the paper via a thorough discussion and consideration of future research endeavors.

II. RELATED WORK

Research into quantum-resistant solutions for DNS security has gained momentum. Prior efforts on post-quantum secure DNS primarily center on securing DNSSEC, the application-layer authentication mechanism used for validating DNS records. In contrast, relatively fewer studies focus on the encryption and confidentiality of DNS traffic, which is the core problem addressed by DNS-over-TLS (DoT).

Research by Muller et al. (2020) investigated the potential of lattice-based cryptography, a promising area of PQC, in providing quantum-resistant signatures for DNSSEC [10]. Pan et al. [11] and Raavi et al. [12] enhance DNSSEC using hybrid signatures and fragmentation mitigation, respectively, but do not address transport-layer encryption. Similarly, Goertzen et al. [13], McGowan et al. [14], and Schutijser et al. [15] advance PQ DNSSEC reliability through fragmentation-aware mechanisms and testbeds, yet leave transport-layer encryption untouched. SL-DNSSEC and TurboDNS [16], [17] propose MAC- and KEM-based protocols to reduce resolution cost, diverging from traditional DNSSEC validation and lacking transport integration. These lightweight designs optimize DNSSEC but are not applicable to TLS-based secure DNS. Jafarli, Beernink, and Goertzen [18]–[20] offer implementation insights for DNSSEC using FN-DSA, ML-DSA, and XMSS. Their evaluations highlight signature size trade-offs, but none address encryption-layer issues or compatibility with DoT. TITAN-DNS over HTTPS (DoH), proposed by Ali and Chen [21], integrates trust mechanisms and FrodoKEM-based TLS handshakes to secure DoH. Their adaptive design combines Bayesian inference and verifiable delay functions to detect malicious queries. Their scope is limited to DoH and omits DoT and DNSSEC alignment. Additionally, recent efforts have focused on evaluating the feasibility of post-quantum cryptographic (PQC) algorithms across diverse platforms, particularly constrained environments. Kannwischer et al. [22] benchmarked NIST PQC candidates on the Arm Cortex-M4 using the pqm4 framework, highlighting performance bottlenecks due to large key sizes, dynamic memory usage, and unoptimized code. Fitzgibbon et al. [23] evaluated ML-KEM (aka Kyber), ML-DSA (aka CRYSTALS-Dilithium), and FN-DSA (aka Falcon) on Raspberry Pi 4 devices, identifying ML-KEM and ML-DSA as the most efficient in key encapsulation and signatures, with FN-DSA providing the smallest handshake size. Abbasi et al. [24] conducted extensive cross-platform benchmarks, showing that PQC adoption in high-performance systems incurs minimal overhead, while constrained devices can face up to 12× slowdown depending on algorithm choice. Lonc et al. [25] assessed PQC feasibility in V2X systems, while Kumar [26] surveyed global PQC efforts, emphasizing implementation challenges in real-world settings. Despite these valuable contributions, performance evaluations of PQC integration within DNS security protocols remain relatively limited. While prior studies have explored PQC in TLS and constrained devices more broadly, there is still a lack of detailed analysis targeting DNS-specific use cases, particularly DNS-over-TLS (DoT). Our work contributes to this emerging area by examining the practical implications of post-quantum transitions in DoT, considering protocol behavior, resource constraints, and algorithm suitability.

Recent advancements have also seen the integration of hybrid cryptographic algorithms, which combine both classical and post-quantum techniques, to gradually transition DNSSEC to a quantum-resistant framework while maintaining compatibility with existing systems [19], [27], [28]. The integration of hybrid cryptography into DNSSEC can, therefore, be seen as a strategic approach to future-proofing DNS against the anticipated quantum threats [27]. The authors in [28] have shown how hybrid key exchange mechanisms can be integrated into TLS 1.3 and SSHv2 so that these protocols can use both classical and post-quantum keys simultaneously. Their work highlights the challenges of negotiating multiple algorithms and effectively combining keys without significantly compromising performance. In these hybrid approaches, conventional cryptographic algorithms (such as RSA or ECDSA) and post-quantum algorithms (such as lattice or hash-based signatures) are used simultaneously. This dual-use strategy ensures that even if one set of algorithms is compromised by quantum computing, the other provides another layer of security, maintaining the integrity of DNSSEC. Studies by Microsoft and others have demonstrated that hybrid TLS implementations, using algorithms like FrodoKEM and classical ECDH, can achieve this balance, making them a viable option for upgrading DNSSEC.

Intensive work has also been done on the development of quantum-resistant key exchange mechanisms specifically for the TLS handshake process [28], [29]. Paquin, Stebila, and Tamvada (2020) compared different cryptographic post-quantum primitives in the context of TLS and highlighted the trade-offs associated with their implementation, especially in environments with high packet loss rates [28]. In addition, significant progress has been made in the development of quantum-resistant key exchange mechanisms for the TLS handshake process, together with industry partners. Microsoft's collaboration with the Open Quantum Safe project [30] has led to the development of a PQC fork of OpenSSL that integrates quantum-resistant key exchange and signature algorithms such as FrodoKEM and qTESLA. These efforts are critical to protecting TLS from potential quantum attacks while enabling hybrid modes of operation that provide security against both current and future threats. Similarly, Meta has addressed the challenges of using post-quantum key exchange mechanisms in large environments, addressing issues such as the larger key sizes that complicate TLS session resumption [31]. Despite these advances, seamlessly integrating PQC into the DoT framework while maintaining backward compatibility and minimizing performance degradation remains a major challenge. The complexity of integrating PQC into existing protocols without significant performance degradation, as highlighted in the Microsoft and Meta studies, underscores the need for further research to optimize these algorithms for practical use in DNS and other Internet security protocols.

Overall, a systematic and deployable integration of PQC into DoT, which secures DNS queries in transit is missing. While prior work makes significant progress in DNSSEC and DoH contexts, a unified and post-quantum-resilient design for

DNS-over-TLS remains underexplored. Our proposed framework, DoPQT, fills this gap by conceptually integrating post-quantum key exchange (ML-KEM) and authentication (FN-DSA) into DoT, along with a simulation-based performance analysis to assess real-world feasibility.

III. PROPOSED FRAMEWORK

We propose a comprehensive framework for DNS over Post-Quantum TLS (DoPQT) that addresses the multiple challenges associated with securing DNS in a post-quantum world. Fig. 1 shows a post-quantum secured DNS system. Our framework is designed to strike a balance between improved security, performance efficiency, and compatibility with existing DNS infrastructure. The key components of our proposed framework include:

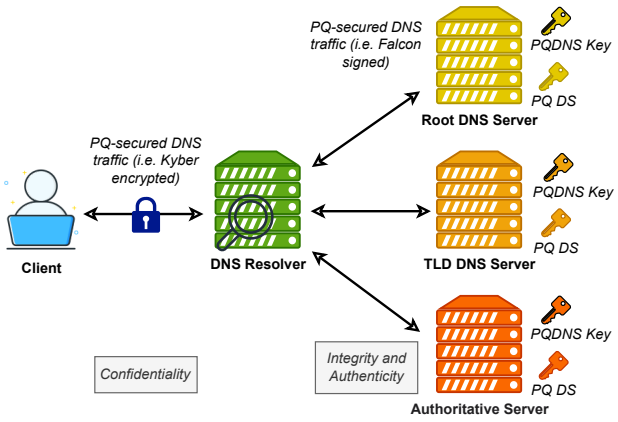

Fig. 1. PQ secured DNS system

- *Hybrid Key Exchange Mechanism:* Our framework uses a hybrid approach to key exchange that combines traditional cryptographic algorithms with post-quantum algorithms. This ensures that communication with both legacy systems and quantum-resistant clients remains secure and provides a smooth transition path when PQC technologies are introduced.
- *Post-Quantum Authentication:* To strengthen the authentication and integrity of DNS responses, we integrate post-quantum digital signature methods. These techniques provide robust protection against spoofing and data tampering and address vulnerabilities that could be exploited by attackers with quantum capabilities.
- *Lightweight Post-Quantum Cipher Suites:* Considering the potential computational overhead associated with PQC, our framework emphasizes the use of lightweight cipher suites. These suites are carefully selected to strike a balance between high security and acceptable performance and to minimize the impact on DNS query and response times.
- *Backward Compatibility:* A key aspect of our framework is its ability to integrate seamlessly with existing DoT implementations. This backward compatibility ensures that the transition to DoPQT can be gradual, allowing current systems to remain operational while adopting quantum-resistant features as they become available.

A. Steps for DoPQT

The packet exchange with DNS via Post-Quantum TLS (DoPQT), depicted in Fig. 2, proceeds as follows. Note that these steps are conceptually similar to DoT, but have been extended by the integration of post-quantum cryptographic algorithms:

Step 1: Client-Server Handshake (TLS 1.3) *(i) ClientHello:* The client initiates the connection by sending a ClientHello message containing: a. Supported TLS versions (likely TLS 1.3 for efficiency), b. Supported cipher suites (including post-quantum key encapsulation mechanisms (KEMs) and digital signature algorithms), c. Client random nonce, supported extensions (e.g., Server Name Indication (SNI) to specify the desired domain). *(ii) ServerHello:* The server responds with a ServerHello message: a. Selected TLS version, b. Selected cipher suite (including the chosen post-quantum KEM and signature algorithm), c. Server random nonce, d. Server's certificate (signed with a traditional or post-quantum digital signature). *(iii) EncryptedExtensions: (Optional)* The server may send additional extensions if needed. *(iv) CertificateRequest: (Optional)* If client authentication is required, the server requests the client's certificate. *(v) Certificate: (Optional)* The client sends its certificate if requested. *(vi) CertificateVerify: (Optional)* The client provides a digital signature to prove ownership of its certificate. *(vii) Finished:* Both client and server send Finished messages, verifying the handshake and establishing encrypted communication using the shared secret derived from the post-quantum KEM.

Step 2: DNS Query and Response (over Encrypted TLS Channel) *(i) DNS Query:* The client sends a DNS query message (e.g., an A or AAAA query to resolve a domain name to an IP address) over the encrypted TLS channel. *(ii) DNS Response:* The server processes the query and sends back a DNS response message containing the requested information (e.g., the IP address associated with the domain name).

Note that the post-quantum Key Encapsulation Mechanism (KEM) and digital signature algorithms used may depend on the chosen cipher suite and implementation. The exact format of the DNS query and response messages must comply with the standard DNS protocol specifications. Finally, the TLS handshake ensures the confidentiality, integrity, and authenticity of DNS traffic, protecting it from eavesdropping and tampering. The use of PQC provides an additional layer of security against possible quantum attacks in the future.

B. Example: Hybrid Key Exchange

In a hybrid key exchange scenario, the ClientHello could contain both traditional (e.g., X25519) and post-quantum (e.g., ML-KEM) KEMs. The server would then select one and include the corresponding public key in its ServerHello. The

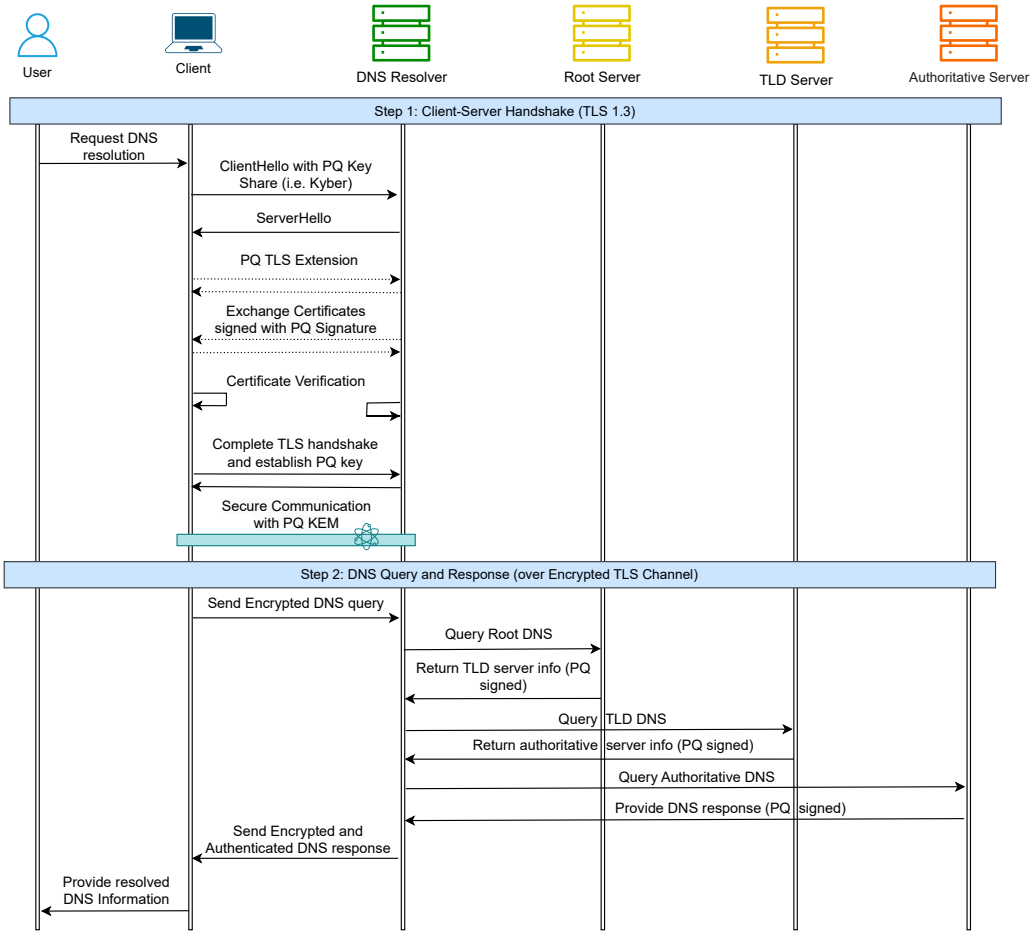

Fig. 2. Packet Exchange of DoPQT

client and server would then use their chosen KEMs to derive a shared secret for encryption.

IV. DoPQT: Theoretical and Quantifiable Comparisons

In the context of DoPQT, performance metrics are critical for assessing whether the integration of post-quantum cryptographic algorithms maintains, improves or reduces the efficiency and practicality of DNS over TLS (DoT). Key performance metrics for DoPQT compared to DoT with potential impacts include:

- *Latency:* The time it takes to complete a DNS query and response cycle. Post-quantum algorithms usually require more computing resources, which can increase latency. This can result in slightly slower DNS query resolution times compared to DoT. However, if optimized post-quantum algorithms are used, the increase in latency can be minimized, although DoPQT may still have a higher latency than conventional DoT due to the added complexity of quantum-resistant cryptography.
- *Computational Overhead:* The amount of computing power required to perform cryptographic operations during the TLS handshake. PQC typically involves higher computational overhead because it requires more complex mathematical operations, larger key sizes, and more intensive signature verification processes. This increased overhead could lead to slower performance during the initial handshake phase, resulting in higher CPU utilization and potentially longer connection setup times compared to DoT.
- *Bandwidth Consumption:* The amount of data transmitted during the cryptographic handshake and subsequent DNS query and response exchanges. Post-quantum algorithms often use larger key sizes and signatures, which can increase the overall bandwidth required during the handshake phase. This might lead to slightly higher data transfer requirements compared to DoT, particularly during the initial connection setup.
- *Memory Usage:* The amount of memory required to store cryptographic keys, certificates, and other relevant data structures. The larger key sizes and signatures associated with PQC may demand more memory resources. This increase in memory usage could affect systems with limited resources, making DoPQT more resource-intensive than DoT.
- *Security Strength:* The resilience of the cryptographic protocol against attacks, especially those that could be launched

by quantum computers. While DoPQT might introduce performance trade-offs in terms of latency, computational overhead, and bandwidth, it significantly enhances security. The use of post-quantum cryptographic algorithms provides robust protection against quantum computing threats, making DoPQT far more secure in the long term compared to DoT.

- *Scalability:* The ability of the protocol to handle a large number of concurrent DNS queries and responses. The increased computational and memory requirements of DoPQT may affect its scalability, especially in high-traffic environments. Systems may require optimization or more powerful hardware to maintain the same level of scalability as DoT.

A. DoPQT vs. DoT

Table I provides comparisons of DNS, DoT, and DoPQT in terms of various features. DoPQT will have a slightly higher latency and a slightly higher computational overhead due to the higher complexity of post-quantum operations. DoPQT may require more bandwidth and memory due to larger key sizes and cryptographic data, especially during the TLS handshake. DoPQT offers significantly more security compared to DoT, especially when it comes to defending against potential attacks on quantum computers, which outweigh the performance losses. The scalability of DoPQT could pose a problem due to the additional computing and resource requirements, but this can be mitigated by optimized algorithms and a more powerful infrastructure.

TABLE I
COMPARISON OF DNS, DOT, AND DOPQT

Feature	DNS	DoT	DoPQT
Encryption	No	Yes	Yes
Authentication	No	Yes	Yes
Integrity	No	Yes	Yes
Confidentiality	No	Yes	Yes
Quantum Resistance	No	No	Yes
Performance	Fastest	Slower than DNS	Slower than DoT
Deployment	Widely deployed	Increasing adoption	Future deployment
Complexity	Low	Moderate	High

B. Security Comparisons

The conventional DNS protocol works without encryption and is therefore vulnerable to eavesdropping and manipulation. DoTprovides confidentiality, integrity, and authentication by encrypting DNS traffic with TLS. However, it is vulnerable to attacks from quantum computers. DoPQT offers the same security benefits as DoT, but with the added benefit of being resistant to quantum attacks. This is achieved by incorporating post-quantum cryptographic algorithms. The disadvantage is increased complexity and potentially lower performance compared to DoT. On the other hand, while DoPQT is the most secure option, its widespread adoption will depend on the development and standardization of PQC. The choice between DNS, DoT, and DoPQT depends on specific security requirements and available resources. Organizations should consider transitioning to DoT as an interim solution while preparing for the later adoption of DoPQT.

C. Discussion on security performance trade-offs

1) Security: DoPQT can effectively prevent passive eavesdropping on DNS traffic due to the strong encryption provided by the post-quantum TLS channel. The use of post-quantum authentication mechanisms prevents an attacker from impersonating the DNS server or client, thwarting man-in-the-middle attacks. DoPQT's integrity protection ensures that DNS responses cannot be tampered with, preventing cache poisoning attacks.

2) Key performance metrics: The computational overhead and latency caused by the post-quantum cryptographic algorithms in DoPQT can be higher. The handshake time is the time required to establish a secure TLS connection. DoPQT may have a slightly longer handshake time compared to DoT due to the additional computations involved in hybrid key exchange and post-quantum authentication. Query/Response Latency is the time it takes for a DNS query to be sent, processed, and answered. DoPQT can have a slightly higher latency compared to DoT, which is primarily due to the encryption and decryption of messages using post-quantum cipher suites.

3) Comparison with Existing Solutions: The performance of DoPQT with traditional DoT and other relevant solutions, such as DNS over HTTPS (DoH) are compared in Table I. DoPQT offers comparable performance to DoH, while providing superior quantum resistance. While DoT remains the fastest option, its lack of quantum resistance makes it a less desirable choice for long-term security.

Overall, DoPQT can provide a viable solution for securing DNS in the post-quantum era. While there is a performance trade-off compared to traditional DoT, the improved security and resistance to quantum attacks outweigh the slight increase in latency. It is expected that further optimizations and advancements of PQC will reduce the performance overhead in the future, making DoPQT an even more attractive solution for securing the DNS infrastructure.

V. SIMULATION RESULTS

A. Simulation Parameters, Setup and Metrics

We used a discrete-event simulator in Python for event-driven updates to model the DNS resolution workflow, including cryptographic operations, network latency, and system load. The simulation parameters were calibrated using realistic latency distributions and published cryptographic benchmarks. While direct network and system measurements were outside the scope of this study, the log-normal distribution for network latency was chosen to reflect skewed delay distributions seen in Internet measurements. The log-normal distribution is often used to model network latencies because it naturally deals

with the skewness observed in real latency data, where most latencies are small but there are occasionally higher values [32], [33]. The gamma distribution is often used to model the times required for operations or processes that are additive in nature, such as the time required for multiple steps in the TLS handshake or PQC operations. For instance, the authors in [34] discuss how end-to-end delay distribution (which is additive), when individual router delays are assumed to be exponential, leads to a gamma distribution. The exponential distribution is useful for modeling the time between events, e.g., the response time of a server, where the likelihood of longer times decreases exponentially. Table II contains the assumed parameters for the DNS query scenario for the above distributions. For ML-KEM-512, we use the key generation of 19.8 microseconds, 22.4 microseconds for key encapsulation, and 14.8 microseconds for key decapsulation[1]. Server load is modeled using a simple, linear model that assumes processing time increases gradually as more queries are handled, reflecting a straightforward degradation in performance due to resource contention. Although simplified, this approach captures the essential trend of load-dependent processing delays observed in large-scale systems [35]. DNS resolution processes are simulated by breaking down the total latency into several components:

- *Network Latency:* Time taken for a DNS query to reach the root server. It is modelled with a log-normal distribution. This choice is selected based on empirical findings from latency measurements in wide area networks, where latency distributions are known to be positively skewed and have been successfully modelled with lognormal distributions in the past [32], [33].
- *TLS Handshake Latency:* Time required to establish a secure connection using TLS. This includes cryptographic operations such as key exchange. When PQC is enabled, this includes post-quantum primitives like ML-KEM-512. TLS handshake latency without PQC is modeled using a Gamma distribution to reflect multi-step operations in classical TLS. Parameters were selected to approximate handshake latencies observed in production TLS deployments. The Gamma distribution was chosen due to its suitability for modeling the total duration of sequential, variable-length processes, which aligns with the structure of TLS handshakes [34]. TLS handshake latency with PQC is the same distribution family (Gamma), but with a larger scale to account for the added cost of post-quantum cryptographic primitives.
- *PQC Operations Latency:* Additional time introduced by PQC operations (key generation, encapsulation, decapsulation). This is a sub-component of the handshake when PQC is used.
- *Response Latency:* Time taken for the DNS server to process the query and send a response. This is modeled as exponential, representing time to process and generate a DNS response on the server side. This reflects the memoryless nature of lightweight tasks like DNS query parsing and cache lookups.

[1]Online: https://medium.com/asecuritysite-when-bob-met-alice/bursting-the-myth-on-post-quantum-cryptography-pqc-being-slow-8d98d30b9a69, Available: September 2024.

- *Overall DNS Query Latency:* The sum of all above components (network + handshake [+ PQC] + response) for a complete resolution round.

Throughout the paper, we refer to individual latency components using the terms above and reserve overall latency to mean the total DNS resolution time observed by the client.

TABLE II
ASSUMED PARAMETERS FOR DNS QUERY SCENARIO

Component	Distribution	Parameters
Network Latency	Log-Normal	Mean: 3, Sigma: 0.5
TLS Handshake Without PQC	Gamma	Shape: 2, Scale: 5
TLS Handshake With PQC	Gamma	Shape: 3, Scale: 20

The simulation was performed with multiple DNS queries and the average latencies for each of these components were calculated, both with and without PQC. We simulated DNS queries for different batch sizes (50 to 1000 queries) and ran each simulation 100 times to obtain average values. DNS resolution for a given number of queries with and without using PQC uses a priority queue (*heapq*) to manage events, ensuring they are processed in the correct order based on the event time. It involves the following steps: (i) DNS Query that simulates the network latency. (ii) TLS Handshake that simulates the time required to establish a secure connection. (iii) DNS Response that simulates the time taken by the server to process and respond to the query. Additionally, with PQC, we have (iv) PQC Operations that simulate ML-KEM-512 key generation, encapsulation, and decapsulation.

B. Numerical Results

1) Latency: Fig. 3 shows a detailed breakdown of how different latency components contribute to the total time required to respond to DNS queries, both with and without the use of PQC (ML-KEM-512). The impact of PQC operations on DNS resolution performance is visualized by running the simulation for different query counts and averaging the results. As the number of DNS queries increases, handshake latency becomes the dominant component, far exceeding network, PQC and response latency. The handshake latency increases by approximately 250% for 400 queries and by 500% for 800 queries. This indicates that the process of establishing secure connections significantly impacts performance under high load. On the other hand, both network and PQC latencies remain relatively stable under varying workloads, which means that they are not significantly affected by the number of DNS queries. The network latency is generally stable due to the constant transmission overhead, while the PQC latency is low and efficient in this context. The response latency increases steadily and is about 71.4% to 114.3% at 400 and 800 queries, respectively. This indicates that the server's ability to process and respond to requests decreases with the load, although not as much as with the handshake process.

2) Throughput: Throughput as the number of DNS requests processed per second. This can be done by measuring the

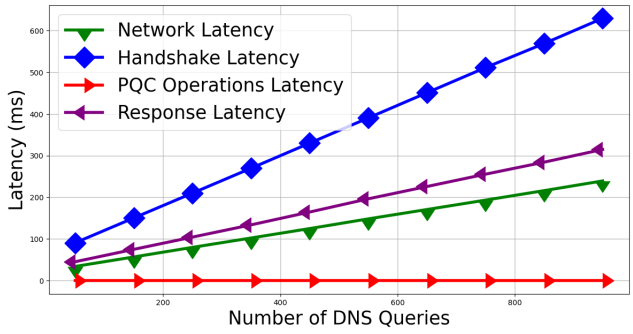

Fig. 3. Latency breakdown compared to the number of DNS queries (averaged over 100 runs) with PQC.

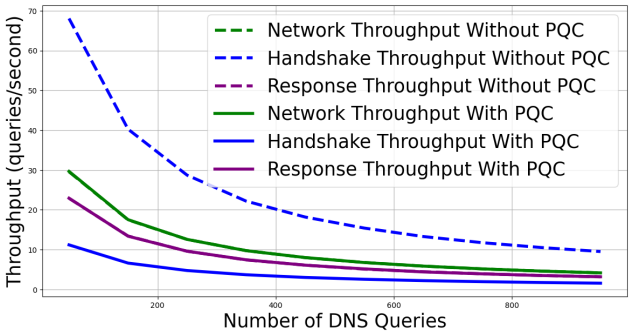

Fig. 5. Throughput vs. number of DNS queries for each phase of the workflow (averaged over 100 runs) with and without PQC.

total time taken to process a batch of DNS requests and then dividing the number of requests by this total time. In simulations, throughput is calculated for each stage by dividing the number of DNS queries by the total time spent in that stage (converted from milliseconds to seconds). Total throughput is the total throughput taking into account the entire DNS resolution process. Network throughput is the throughput considering only the network latency. Handshake throughput is the throughput taking into account the TLS handshake latency. PQC throughput is the throughput taking into account the PQC operations (ML-KEM-512). Response throughput is the throughput taking into account the response time of the server.

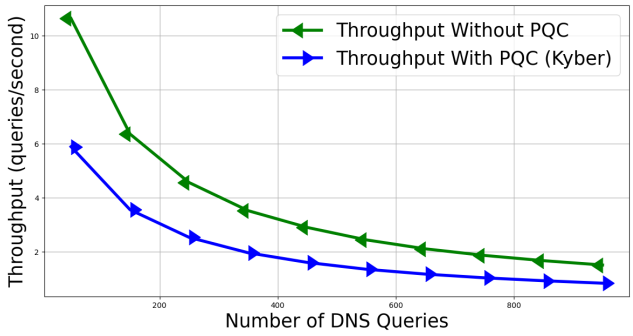

Fig. 4. Throughput vs. number of DNS queries (average over 100 runs) with and without PQC

Fig. 4 shows the impact of PQC on the throughput of DNS query processing. The overall throughput decreases significantly when PQC is enabled, especially at higher load (i.e. with a large number of DNS queries). It stabilizes around 1.5-2 queries/second for higher query counts with PQC. There is performance cost of PQC. As the number of DNS queries increases, the computational load of PQC becomes more significant, resulting in lower throughput compared to the scenario without PQC. Throughput decreases by about 40% and 33% when PQC is used for 100 and 800 DNS queries respectively. The results in Fig. 4 also show that while PQC (especially ML-KEM, also known as Kyber) ensures post-quantum security, it incurs additional overhead that can affect the server's ability to process DNS queries efficiently, especially when the load increases.

Fig. 5 shows all throughput (queries per second) across different stages of DNS resolution (network, handshake, and response) both with and without PQC. The most important effect of PQC is the handshake throughput. The handshake process is much slower with PQC, with a decrease of 80-82% due to the computational overhead introduced by PQC. This is due to the additional cryptographic operations (e.g., ML-KEM-512 operations such as key generation, encapsulation, and decapsulation). The decrease in throughput with increasing number of queries is more pronounced in the handshake phase, especially when PQC is enabled. It decreases by 80-82% due to the computational overhead caused by PQC. The network throughput is largely unaffected by PQC, as PQC mainly influences the cryptographic processes and not the network transmission itself. With PQC, the throughput only decreases by 28.6-33.3% as the number of queries increases. Response throughput is affected to some extent, but remains stable as the server processes an increasing number of queries. It decreases by 25-33.3%, which shows that PQC moderately affects the server's ability to respond to DNS queries.

VI. Discussion

A. Comparative View of PQC Candidates

While our performance evaluation focused on ML-KEM (KEM) due to the strong NIST standing and compatibility with TLS handshake constraints [24], other PQC candidates offer different trade-offs. Table III [36]–[38] compares major classes of PQC primitives, emphasizing their relevance to DNS security protocols, particularly DNS-over-TLS (DoT). Among the NIST-standardized algorithms, lattice-based schemes (ML-KEM for KEM and ML-DSA/FN-DSA for DS) are best suited for DNS environments due to their balance of small key/signature sizes, high performance, and stateless operation. Notably, FN-DSA offers the smallest signature sizes (e.g., 666 bytes for FN-DSA-512), but its sensitivity to side-channel attacks and reliance on constant-time floating-point arithmetic complicate secure deployment. SPHINCS+, a hash-based and conservative digital signature algorithm, provides strong security guarantees without relying on algebraic structures, but its large signatures [23] (8–17KB) and statefulness introduce challenges in bandwidth-limited or high-throughput DNS scenarios. Classic McEliece remains the only code-based KEM accepted in NIST's standardization process. It is known for its mature security foundations and fast encryption/decryption.

TABLE III
COMPARISON OF POST-QUANTUM CRYPTOGRAPHIC PRIMITIVES FOR DNS SUITABILITY

Parameter	**Isogeny-based** (SIKE, SQISign)	**Lattice-based** (ML-KEM, ML-DSA)	**Code-based** (McEliece)	**Multivariate-based** (Rainbow)	**Hash-based** (SPHINCS)
Platform Suitability	IoT-friendly (but slow)	Suitable for general and embedded platforms	Not ideal for constrained devices	Not practical	Good for high-assurance systems
Computational Efficiency	Slow	Fast	Moderate	Fast	Fast
Hardware Acceleration	Limited availability	Strong (widely implemented)	Moderate	Limited	Moderate
Public Key Size	Small (around hundreds of bytes)	Moderate (a few KB)	Large (tens to hundreds of KB)	Large (tens to hundreds of KB)	Small (a few bytes to KB)
Private Key Size	Small	Moderate	Large	Large	Small
Signature Size	Small (around hundreds of bytes)	Moderate to large (KB)	Large	Moderate to large (KB)	Large (tens to hundreds of KB)
NIST Status	SIKE: Rejected (Broken), others: experimental	Standardized (ML-KEM, ML-DSA)	Alternate finalist	Rainbow: Rejected (Broken)	Standardized (SPHINCS+)
Side-Channel Resistance	Poor (needs careful masking)	Moderate to good (with constant-time impl.)	Good (structure-dependent)	Weak	Good
Stateful / Stateless	Stateless	Stateless	Stateless	Stateless	Stateful
DNS Suitability	Low	High	Low	Low	Medium

However, its massive public key sizes (over 1MB) make it entirely unsuitable for DNS or TLS scenarios, especially those relying on UDP transmission. Due to this key size constraint [23], McEliece is rarely considered in PQC DNS discussions and is not a viable candidate for DNS-over-TLS deployments. Isogeny-based schemes such as SIKE previously attracted attention due to their remarkably small key sizes, which seemed ideal for constrained protocols like DNS, especially in IoT environment [39]. However, SIKE was broken in 2022 by Castryck and Decru [40], removing it from NIST consideration. SQISign [41], a newer isogeny-based signature scheme, remains a research candidate but is not yet mature enough for deployment. While isogeny cryptography holds theoretical appeal for bandwidth-constrained environments, no current scheme from this class is suitable or secure enough for PQC DNS integration. Multivariate schemes like Rainbow have been cryptanalytically broken and excluded from NIST's standardization.

Among all classes, lattice-based cryptography, specifically ML-KEM for key encapsulation and ML-DSA or FN-DSA for digital signatures, offers the best balance of security, performance, and compatibility for post-quantum DNS security, especially DNS-over-TLS. Our work reflects this by choosing ML-KEM for integration and evaluation within the DoPQT framework, supported by simulation-based measurements and compatibility analysis.

B. Future Directions and Efforts

The need to transition to PQC to secure the Internet infrastructure goes beyond DoT and also includes other important DNS protocols. DoH and DNS over QUIC (DoQ), both of which are growing in popularity due to their enhanced privacy and performance benefits, must also be adapted to withstand potential quantum attacks. We provide the implementation strategies for the DoPQT in Table IV.

- *Post-Quantum DoH (DoH-PQC):* The integration of PQC in DoH is crucial for the protection of DNS requests transmitted over HTTPS. This requires careful selection of post-quantum algorithms for the TLS layers, striking a balance between security, performance, and backward compatibility. Research efforts must focus on optimizing the implementation to minimize the latency and computational overhead incurred by PQC within DoH. The project also aims to investigate how PQC can further improve privacy protection in DoH to ensure that quantum attackers cannot compromise user data. Finally, prototyping and testing under real-world conditions are necessary to evaluate the feasibility and performance of DoH PQC under different network conditions.
- *Post-Quantum DoQ (DoQ-PQC):* The development of a quantum-resistant DoQ requires the identification and implementation of post-quantum key exchange mechanisms that are tuned to the fast handshake process of QUIC. The challenge is to preserve the low-latency advantages of DoQ even when integrating PQC. In addition, since QUIC supports multiplexed connections, efficient integration of PQC into this model is critical to avoid performance bottlenecks. Researchers must ensure that DoQ-PQC remains interoperable with existing QUIC implementations and is resistant to both quantum and conventional network attacks.
- *Unified Framework for PQC in DNS Protocols:* A standardized framework for the seamless integration of PQC across different DNS transport protocols (DoT, DoH, DoQ) is an important long-term goal. This includes standardizing PQC implementations and ensuring a consistent transition to post-quantum security across DNS-over-encryption protocols. Collaboration with standardization bodies such as the IETF will be critical to promote broad adoption and interoperability. The framework should also consider phased transition strategies that take into account the evolving net-

TABLE IV
IMPLEMENTATION STAGES FOR DOPQT

Stage	Objective	Key Activities	Expected Outcome	Reference Performance Metric [42]
Research & Development	Identify PQC algorithms suitable for DoPQT	Evaluate NIST PQC finalists (e.g., ML-KEM, FN-DSA); prototype DoPQT resolver	Ranked list by key metrics; Identified PQC candidates	*Latency* $\leq$ 36 ms median (Baseline: Google DoT)
Pilot Testing	Test DoPQT in controlled environments	Deploy in test networks, evaluate DoPQT performance	Performance data, feedback	*Query success rate* $\geq$ 99% within 150 ms (Baseline: Cloudflare DoT)
Optimization	Enhance efficiency and compatibility with existing DNS infrastructure	Algorithm tuning, hardware acceleration strategies	Optimized DoPQT implementation	*Throughput* $\geq$ 500 queries/sec (Baseline: DoT throughput trends)
Deployment	Roll out DoPQT in production networks	Phased deployment, monitoring	Secure DNS with minimal disruption	*Failure rate* $\leq$ 0.1% (Baseline: DoT failure rates)

work infrastructure and ensure uninterrupted DNS services during the transition.

- *Prototype Validation with OQS and OpenSSL:* While our evaluation provides insight into the performance implications of post-quantum cryptography in DNS resolution workflows, we acknowledge that our current evaluation is limited to simulation-based analysis. Although the parameters were chosen based on realistic distributions and empirical cryptographic benchmarks, actual deployment in live networks may introduce additional overheads or optimizations not captured here. To further strengthen the credibility and practical relevance of our work, we plan to implement the DoPQT framework using DoPQT framework using DNS server software such as BIND, Unbound, or Knot DNS, built with libraries such as Open Quantum Safe (OQS) and patched versions of OpenSSL PQC support or alternative TLS libraries such as BoringSSL and wolfSSL [43]. This will allow us to assess real-world performance, interoperability with existing TLS implementations, and protocol behavior in dynamic network environments. Prototype-based testing will also provide insights into handshake latency, cryptographic overhead, and compatibility across different resolver configurations. Validating our findings on an experimental testbed with real DNS server implementations and hybrid TLS configurations will be an important direction for future work, and we plan to explore this as PQC support matures in production systems.
- *Real-World Integration Challenges:* While the proposed DoPQT framework has been evaluated in a simulated environment, its integration into real-world DNS infrastructure introduces additional challenges. The hierarchical structure of DNS, including recursive resolvers, forwarders, and caching mechanisms, can impact performance, especially when incorporating post-quantum TLS handshakes with larger key exchanges and signature payloads. Moreover, CDN infrastructures often optimize DNS queries using proprietary techniques. This ensures that the privacy, efficiency, and reliability that users expect from a modern Internet infrastructure are maintained even in the face of threats from quantum computing. Cross-layer optimizations across these layers are essential for practical deployment and will be explored in future work.

The simulation-based evaluation provided indicative trends to understand the impact of PQC on DNS resolution performance. Future work will also include measurements from a deployed PQC-enabled DNS prototype to validate and refine these results.

VII. CONCLUSION

The impending threat of quantum computing necessitates immediate action to fortify DNS security through post-quantum cryptographic solutions. Our proposed DNS over Post-Quantum TLS (DoPQT) framework represents a proactive and comprehensive approach to addressing these emerging challenges. By combining traditional and post-quantum cryptographic algorithms, we offer a robust defense against both classical and quantum-enabled attacks, ensuring the continued integrity and security of DNS. While DoPQT introduces some performance trade-offs, particularly in terms of latency, computational overhead, bandwidth, and memory usage, these are balanced by the substantial increase in security against quantum threats. Optimizations and future advancements in PQC are expected to reduce these impacts, potentially bringing DoPQT performance closer to that of traditional DoT over time. The hybrid key exchange mechanism, emphasis on lightweight cipher suites, and focus on backward compatibility further enhance the practicality and effectiveness of our solution. As PQC continues to evolve, ongoing research and development will be essential to optimizing performance, identifying and mitigating vulnerabilities, and promoting widespread adoption. The successful implementation of DoPQT will play a pivotal role in securing the DNS infrastructure and safeguarding the future of internet communications in a post-quantum world.

REFERENCES

[1] M. Taleby Ahvanooey, W. Mazurczyk, J. Zhao, *et al.*, "Future of cyberspace: A critical review of standard security protocols in the post-quantum era," *Computer Science Review*, vol. 57, p. 100 738, 2025. DOI: 10.1016/j.cosrev.2025.100738.

[2] A. Aydeger, P. Zhou, S. Hoque, M. Carvalho, and E. Zeydan, "Mtdns: Moving target defense for resilient dns infrastructure," in *2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC)*, IEEE, 2025, pp. 1–6. DOI: 10.1109/CCNC54725.2025.10975971.

[3] M. M. Nesary and A. Aydeger, "Vdns: Securing dns from amplification attacks," in *2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, IEEE, 2022, pp. 102–106. DOI: 10.1109/BlackSeaCom54372.2022.9858278.

[4] C. Deccio and J. Davis, "Dns privacy in practice and preparation," in *Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies*, 2019, pp. 138–143. DOI: 10.1145/3359989.3365435.

[5] N. Alnahawi, J. Müller, J. Oupickỳ, and A. Wiesmaier, "A comprehensive survey on post-quantum tls," *IACR Communications in Cryptology*, 2024. DOI: 10.62056/ahee0iuc.

[6] D. Joseph, R. Misoczki, M. Manzano, *et al.*, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, 2022. DOI: 10.1038/s41586-022-04623-2.

[7] Y. Hanna, D. Pineda, K. Akkaya, A. Aydeger, R. Harrilal-Parchment, and H. Albalawi, "Performance evaluation of secure and privacy-preserving dns at the 5g edge," in *2023 IEEE 20th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, IEEE, 2023, pp. 89–97. DOI: 10.1109/MASS58611.2023.00019.

[8] L. Malina, P. Dobias, J. Hajny, and K.-K. R. Choo, "On deploying quantum-resistant cybersecurity in intelligent infrastructures," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023, pp. 1–10. DOI: 10.1145/3600160.3605038.

[9] A. Aydeger, E. Zeydan, A. K. Yadav, K. T. Hemachandra, and M. Liyanage, "Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography," in *2024 15th International Conference on Network of the Future (NoF)*, IEEE, 2024, pp. 195–203. https://doi.org/10.1109/NoF62948.2024.10741441.

[10] M. Müller, J. de Jong, M. van Heesch, B. Overeinder, and R. van Rijswijk-Deij, "Retrofitting post-quantum cryptography in internet protocols: A case study of dnssec," *ACM SIGCOMM Computer Communication Review*, vol. 50, no. 4, pp. 49–57, 2020. DOI: 10.1145/3431832.3431838.

[11] S. W. S. Pan, D. D. N. Nguyen, R. Doss, W. Armstrong, P. Gauravaram, *et al.*, "Double-signed fragmented dnssec for countering quantum threat," *arXiv preprint arXiv:2411.07535*, 2024. DOI: 10.48550/arXiv.2411.07535.

[12] M. Raavi, S. Wuthier, and S.-.-Y. Chang, "Securing post-quantum dnssec against fragmentation misassociation threat," in *ICC 2024-IEEE International Conference on Communications*, IEEE, 2024, pp. 97–102. DOI: 10.1109/icc51166.2024.10622607.

[13] J. Goertzen and D. Stebila, "Post-quantum signatures in dnssec via request-based fragmentation," in *International Conference on Post-Quantum Cryptography*, Springer, 2023, pp. 535–564. DOI: 10.1007/978-3-031-40003-2_20.

[14] C. McGowan, J. Liu, and S. Ruj, "Security considerations for post-quantum signatures in dnssec via request-based fragmentation," in *Companion Proceedings of the ACM on Web Conference 2025*, 2025, pp. 1189–1193. DOI: 10.1145/3701716.3715585.

[15] C. Schutijser, E. E. Lastdrager, R. Koning, and C. E. Hesselman, "A testbed to evaluate quantum-safe cryptography in dnssec," in *DNS and Internet Naming Research Directions, DINR 2024*, 2024.

[16] A. S. Rawat and M. P. Jhanwar, "Quantum-safe signatureless dnssec," *Cryptology ePrint Archive*, 2024. DOI: 10.1145/3708821.3710837.

[17] A. S. Rawat and M. P. Jhanwar, "Post-quantum dnssec with faster tcp fallbacks," in *International Conference on Cryptology in India*, Springer, 2024, pp. 212–236. DOI: 10.1007/978-3-031-80311-6_11.

[18] S. Jafarli, "Providing dns security in post-quantum era with hash-based signatures," M.S. thesis, University of Twente, 2022.

[19] G. Beernink, "Taking the quantum leap: Preparing dnssec for post quantum cryptography," M.S. thesis, University of Twente, 2022.

[20] J. Goertzen, "Enabling post-quantum signatures in dnssec: One arrf at a time," M.S. thesis, University of Waterloo, 2022.

[21] B. Ali and G. Chen, "Titan-doh: Trust-integrated threat adaptive network for post-quantum secure dns over https," *Available at SSRN 5230452*, DOI: 10.2139/ssrn.5230452.

[22] M. J. Kannwischer, M. Krausz, R. Petri, and S.-Y. Yang, *Pqm4: Benchmarking NIST additional post-quantum signature schemes on microcontrollers*, Cryptology ePrint Archive, Paper 2024/112, 2024.

[23] G. Fitzgibbon and C. Ottaviani, "Constrained device performance benchmarking with the implementation of post-quantum cryptography," *Cryptography*, vol. 8, no. 2, p. 21, 2024. DOI: 10.3390/cryptography8020021.

[24] M. Abbasi, F. Cardoso, P. Váz, J. Silva, and P. Martins, "A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments," *Cryptography*, vol. 9, no. 2, p. 32, 2025. DOI: 10.3390/cryptography9020032.

[25] B. Lonc, A. Aubry, H. Bakhti, M. Christofi, and H. A. Mehrez, "Feasibility and benchmarking of post-quantum cryptography in the cooperative its ecosystem," in *2023 IEEE Vehicular Networking Conference (VNC)*, IEEE, 2023, pp. 215–222. DOI: 10.1109/vnc57357.2023.10136335.

[26] M. Kumar, "Post-quantum cryptography algorithm's standardization and performance analysis," *Array*, vol. 15, p. 100 242, 2022. DOI: 10.1016/j.array.2022.100242.

[27] A. A. Giron, J. P. A. do Nascimento, R. Custódio, L. P. Perin, and V. Mateu, "Post-quantum hybrid kemtls performance in simulated and real network environments," in *International Conference on Cryptology and Information Security in Latin America*, Springer, 2023, pp. 293–312. DOI: 10.1007/978-3-031-44469-2_15.

[28] C. Paquin, D. Stebila, and G. Tamvada, "Benchmarking post-quantum cryptography in tls," in *Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020*, Paris, France, April 15–17, 2020, Proceedings 11, Springer, 2020, pp. 72–91. DOI: 10.1007/978-3-030-44223-1_5.

[29] P. Schwabe, D. Stebila, and T. Wiggers, "Post-quantum tls without handshake signatures," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 1461–1480. DOI: 10.1145/3372297.3423350.

[30] D. Stebila and M. Mosca, "Post-quantum key exchange for the internet and the open quantum safe project," in *International Conference on Selected Areas in Cryptography*, Springer, 2016, pp. 14–37. DOI: 10.1007/978-3-319-69453-5_2.

[31] Meta Engineering, *Post-Quantum Readiness: TLS PQR at Meta*, [Online]. Available: https://engineering.fb.com/2024/05/22/security/post-quantum-readiness-tls-pqr-meta/, Accessed: August 2024, 2024.

[32] A. B. Downey, "Lognormal and pareto distributions in the internet," *Computer Communications*, vol. 28, no. 7, pp. 790–801, 2005. DOI: 10.1016/j.comcom.2004.11.001.

[33] D. Mödinger, J.-H. Lorenz, R. W. van der Heijden, and F. J. Hauck, "Unobtrusive monitoring: Statistical dissemination latency estimation in bitcoin's peer-to-peer network," *Plos one*, vol. 15, no. 12, e0243475, 2020. DOI: 10.1371/journal.pone.0243475.

[34] R. Wallace, X. G. Andrade, P. Kayser, *et al.*, "Models of network delay," in *International Workshop on Statistical Modelling*, Springer, 2024, pp. 231–238. DOI: 10.1007/978-3-031-65723-8_36.

[35] R. Jain, *The art of computer systems performance analysis*. john wiley & sons, 1990.

[36] M. Raavi, S. Wuthier, P. Chandramouli, Y. Balytskyi, X. Zhou, and S.-Y. Chang, "Security comparisons and performance analyses of post-quantum signature algorithms," in *International Conference on Applied Cryptography and Network Security*, Springer, 2021, pp. 424–447. DOI: 10.1007/978-3-030-78375-4_17.

[37] J. Henrich, A. Heinemann, A. Wiesmaier, and N. Schmitt, "Performance impact of pqc kems on tls 1.3 under varying network characteristics," in *International Conference on Information Security*, Springer, 2023, pp. 267–287. DOI: 10.1007/978-3-031-49187-0_14.

[38] S. Hoque, A. Aydeger, and E. Zeydan, "Exploring post quantum cryptography with quantum key distribution for sustainable mobile network architecture design," in *Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems*, 2024, pp. 9–16. DOI: 10.1145/3659997.3660033.

[39] A. Aydeger, S. Hoque, E. Zeydan, and K. Dev, "Analysis of robust and secure dns protocols for iot devices," *arXiv preprint arXiv:2502.09726*, 2025. DOI: 10.48550/arXiv.2502.09726.

[40] W. Castryck and T. Decru, "An efficient key recovery attack on sidh," in *Annual international conference on the theory and applications of cryptographic techniques*, Springer, 2023, pp. 423–447. DOI: 10.1007/978-3-031-30589-4_15.

[41] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski, "Sqisign: Compact post-quantum signatures from quaternions and isogenies," in *International conference on the theory and application of cryptology and information security*, Springer, 2020, pp. 64–93. DOI: 10.1007/978-3-030-64837-4_3.

[42] A. Hounsel, K. Borgolte, P. Schmitt, J. Holland, and N. Feamster, "Comparing the effects of dns, dot, and doh on web performance," in *Proceedings of The Web Conference 2020*, 2020, pp. 562–572. DOI: 10.1145/3366423.3380139.

[43] S. Hoque, A. Aydeger, and E. Zeydan, "Post-quantum secure ue-to-ue communications," in *2024 15th International Conference on Network of the Future (NoF)*, IEEE, 2024, pp. 28–30. DOI: 10.1109/nof62948.2024.10741456.

Abdullah Aydeger is currently an assistant professor at the Electrical Engineering and Computer Science Department at Florida Institute of Technology. Prior to joining Florida Tech in August 2022, he was an assistant professor at the School of Computing at Southern Illinois University, Carbondale, since 2020. Dr. Aydeger obtained a Ph.D. Degree in Electrical and Computer Engineering from Florida International University in 2020. His research interests are network security, network virtualization, and post-quantum cryptography.

Sanzida Hoque is a Ph.D. student in Computer Science at the Florida Institute of Technology, currently working as a Graduate Assistant. She completed her MS in Computer Science from the University of Missouri-St. Louis in August 2023 and her B.Sc. in Computer Science and Engineering from the Military Institute of Science and Technology (MIST) in March 2019. She worked as a Graduate Research Assistant from the Fall of 2021 to the Summer of 2023. Her research interests span various areas, including Network Systems, Post-Quantum Cryptography, DNS Security, Next-Generation Internet, Wireless Networks, Mobile/Edge Computing, IoT, SDN, and related fields. Website: sites.google.com/view/sanzidahoque

Engin Zeydan received his Ph.D. degree in February 2011 from the Department of Electrical and Computer Engineering at Stevens Institute of Technology, Hoboken, NJ, USA. He is currently a Senior Researcher at Services as Networks (SaS) Research Unit in CTTC, Barcelona, Spain and Project Coordinator of the Horizon Europe Unity6G European Project (January 2025-present). He was the Project Coordinator of the European H2020 MonB5G Project [2021-2023]. His research interests are in the areas of telecommunications, data engineering and network security.