# A Differentiated Approach for Post-Quantum DNSSEC

MARC ESPIE, EPITA, EPITA Research Lab (LRE), France
HUGO MAYER, EPITA, EPITA Research Lab (LRE), France
LUDOVIC PERRET, EPITA, EPITA Research Lab (LRE), France and Sorbonne Université, CNRS, LIP6, France

Post-quantum signature algorithms pose significant challenges for DNS Security Extensions (DNSSEC) migration: their larger keys and signatures exceed DNS over UDP transport limits, making TCP fallback unavoidable even for the most compact schemes. We propose a differentiated algorithm selection, assigning distinct signature algorithms to the Zone Signing Key (ZSK) and Key Signing Key (KSK) roles. This approach expands the space of deployable post-quantum configurations beyond what undifferentiated selection permits, enabling algorithms that would otherwise be impossible to deploy: UOV, with 128-byte signatures but 43 KB keys, produces DNSKEY responses exceeding the 64 KB DNS limit under undifferentiated constraints, yet becomes viable when paired with a compact-key KSK. We also evaluate hybrid PQ/T schemes through signature concatenation, combining classical P256 with post-quantum algorithms in a single RRSIG record to provide dual security during the transition period. Using a containerized testbed validated against AFNIC's .fr TLD structure (4.2 million domains), we systematically measure response sizes, resolution latency, TCP fallback rates, and signing performance across 18 configurations. Differentiated configurations achieve 1.28–1.52× latency overhead relative to classical ECDSA while enabling algorithms that undifferentiated constraints prohibit. Hybrid PQ/T concatenation introduces acceptable overhead (7–19%) for backward-compatible quantum resistance.

CCS Concepts: • **Security and privacy** → **Digital signatures**; *Key management*; *Security protocols*; • **Networks** → *Application layer protocols.*

Additional Key Words and Phrases: Post-Quantum Cryptography, DNSSEC, Multivariate Signatures Algorithm Differentiation, KSK/ZSK, Quantum Resistance, Network Security, UDP Constraints, TCP Fallback, Signature Size, NIST Standardization, Infrastructure Deployment, Performance Evaluation

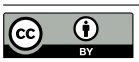
## 1 Introduction

The security of the global Domain Name System (DNS) depends on DNSSEC [1, 3, 2], which authenticates DNS responses through public-key signatures. Although most Internet protocols will integrate new post-quantum cryptography standards rather smoothly, DNSSEC stands apart. The larger public-key and signature sizes of post-quantum algorithms pose significant challenges to this latency-sensitive protocol, risking substantial performance degradation or even protocol failure.

Post-quantum DNSSEC migration faces a fundamental tension between cryptographic security and protocol constraints. The recommended UDP payload size of 1232 bytes [12] accommodates classical ECDSA signatures (64 bytes) with ample margin, but post-quantum signature schemes exceed this limit by an order of magnitude.

In 2024, NIST standardized three post-quantum signature algorithms: ML-DSA (FIPS 204), SLH-DSA (FIPS 205), and FN-DSA/Falcon (FIPS 206) [21, 22, 23]. ML-DSA signatures reach 2,420 bytes at security level 1, SLH-DSA ranges from 7,856 to 17,088 bytes depending on the variant, and FN-DSA, the most compact standardized option, produces signatures of 666 bytes. When keys and signatures

Authors' Contact Information: Marc Espie, EPITA, EPITA Research Lab (LRE), Le Kremlin-Bicêtre, France, marc.espie@epita.fr; Hugo Mayer, EPITA, EPITA Research Lab (LRE), Le Kremlin-Bicêtre, France, hugo.mayer@epita.fr; Ludovic Perret, EPITA, EPITA Research Lab (LRE), Le Kremlin-Bicêtre, France and Sorbonne Université, CNRS, LIP6, Paris, France, ludovic.perret@lip6.fr.



This work is licensed under a Creative Commons Attribution 4.0 International License.

must coexist in a single response, as in DNSKEY queries, the mismatch with UDP constraints becomes critical.

Aware that stringent size constraints require additional options, NIST launched a call for compact signature schemes in 2023 [20]. MAYO [7], achieving 186-byte signatures with 4.9 KB keys, has been identified as promising for DNSSEC. In this work, we show that UOV [8], producing the most compact post-quantum signatures (128 bytes) albeit with 43.5 KB keys, also becomes viable through differentiated algorithm selection—assigning distinct algorithms to Zone Signing Key (ZSK) and Key Signing Key (KSK) roles. This approach not only enables algorithms like UOV that undifferentiated deployment prohibits, but also rehabilitates schemes often dismissed as impractical, such as SLH-DSA (slow signing) or ML-DSA (large signatures), by confining their limitations to infrequent KSK operations.

### 1.1 State of the Art

This problem has motivated four main strategies for integrating post-quantum cryptography into DNSSEC: direct integration, optimization of the transport layer, modifications of the DNSSEC protocol, and encrypted DNS.

*Direct algorithm integration.* Can post-quantum algorithms replace classical ones without modifying the protocol? Müller et al.[19] systematically evaluated NIST candidates under DNSSEC size constraints. Among the candidates, only Falcon-512 (666-byte signatures, 897-byte keys) satisfies both signature and key constraints. Two multivariate schemes, Rainbow-Ia and GeMSS-128, offered compact signatures but required keys exceeding DNS transport capacity; both were subsequently eliminated from the NIST process[6].

Even Falcon-512 introduces deployment challenges. Müller et al. predicted significant increases in TCP fallback rates, motivating further investigation of post-quantum DNSSEC deployment. Beernink [5] validated these concerns using production traffic from the University of Twente resolver and proposed an out-of-band key exchange mechanism in Unbound[1], incurring approximately 30% latency overhead. More recently, SIDN Labs [28] evaluated MAYO-2 and Falcon-512 for TLD deployment using zone files from .nl, .se, and .nu ccTLDs. Their measurements show that MAYO-2 signing performance matches ECDSA-P256 on modern x86-64 CPUs with AVX2 support, while Falcon-512 performs comparably to RSA-1280. The tradeoff is MAYO-2's 4.9 KB public key, which generally requires TCP for distribution, and Falcon-512's larger signatures (666 bytes) that increase zone file sizes.

*Transport-layer optimization.* A second direction accepts that post-quantum signatures exceed UDP capacity and focuses on minimizing transmission overhead. Goertzen and Stebila [15] introduced ARRF (Application-layer Request-based Resource Record Fragmentation), splitting large records across multiple DNS exchanges. The first response returns a truncated fragment, and the resolver issues follow-up requests for remaining pieces. Their experiments with Falcon, ML-DSA, and SLH-DSA showed substantially lower resolution times than standard TCP fallback, although ARRF requires a non-standard pseudo-record (RRFRAG) and at least two round-trips. McGowan et al. [17] later analyzed ARRF's security, identifying vulnerabilities in fragment reassembly that must be addressed prior to deployment.

Rawat and Jhanwar [27] instead optimized TCP fallback itself. Their TurboDNS mechanism eliminates two round-trips from standard DNS-over-TCP by encapsulating handshake data and authenticating clients using cryptographic cookies. Their measurements show that TurboDNS achieves

[1]Unbound is a validating, recursive DNS resolver developed by NLnet Labs: https://nlnetlabs.nl/projects/unbound/

resolution times comparable to classical ECDSAP256SHA256 and RSASHA256 when used with Falcon-512 and ML-DSA-44.

*Architectural redesign.* Transport-layer optimizations reduce latency but do not address the underlying issue: post-quantum signatures consume bandwidth and increase amplification potential. More radical approaches aim to replace signatures entirely. Rawat and Jhanwar [26] proposed SL-DNSSEC (Signatureless DNSSEC), which replaces signatures with symmetric Message Authentication Codes. A post-quantum Key Encapsulation Mechanism (KEM) establishes a shared secret between resolver and nameserver, from which a MAC key is derived. The resulting tags reduce bandwidth by up to 95% relative to SLH-DSA and 58% relative to Falcon, achieving an amplification factor below unity. However, SL-DNSSEC requires resolvers to maintain per-nameserver state, departing from DNSSEC's stateless verification model.

Fregly et al. [14] proposed Merkle Tree Ladder (MTL) mode, which condenses signatures without protocol changes. Instead of transmitting full signatures, the signer provides a compact condensed signature (248–472 bytes) that includes an authentication path to evolving Merkle roots, while full reference signatures are distributed separately and reused. Analysis of .NZ traffic showed that reference values are often reused over ten times, and more than one hundred times at high-volume resolvers.

*Complementary work on encrypted DNS.* Parallel research addresses confidentiality through encrypted transport. Aydeger et al. [4] introduced DoPQT (DNS over Post-Quantum TLS), using ML-KEM for key exchange and FN-DSA for authentication. Their evaluation found a 33–40% throughput reduction relative to classical DoT, with the TLS handshake constituting the main bottleneck. DoPQT and post-quantum DNSSEC address orthogonal concerns, confidentiality and authenticity, and operators will likely deploy them together in a comprehensive post-quantum DNS architecture.

These research directions offer complementary strategies for post-quantum DNSSEC migration, yet none explores differentiated algorithm selection based on operational roles.

### 1.2 Organization of the Paper and Main Results

RFC 6781 [16] formalizes the operational distinction between ZSKs and KSKs, yet no prior work has explored whether different cryptographic algorithms might be suited to these distinct roles. This unexplored direction has significant implications for post-quantum DNSSEC: multivariate schemes such as UOV produce exceptionally compact signatures (128 bytes) but require large public keys (43 KB), making undifferentiated deployment infeasible because DNSKEY Resource Record Sets (RRsets) exceed DNS message size constraints (Section 2.2). Differentiated algorithm selection removes this barrier, transforming impossible deployments into viable configurations.

Existing approaches have not leveraged this asymmetry. Our work addresses this gap within the existing DNSSEC framework. Differentiated selection requires no protocol changes or resolver updates; hybrid PQ/T signatures use dedicated algorithm identifiers currently under IETF standardization, but this requirement applies to all hybrid schemes regardless of differentiation.

This paper makes two contributions. First, we demonstrate that differentiated ZSK/KSK algorithm selection expands the space of deployable post-quantum algorithms, enabling configurations such as Falcon-512/UOV-Ip-pkc that would be impossible under undifferentiated constraints. Second, we establish a reproducible containerized testbed validated against AFNIC's .fr TLD structure, supporting classical, post-quantum, hybrid PQ/T (P-256 concatenation), and differentiated setups, together with comprehensive performance measurements.

Our measurements demonstrate that differentiated configurations achieve latency overhead of ×1.28–1.52 relative to classical ECDSA. SLH-DSA-128f, dismissed for its 8-minute signing time under undifferentiated deployment, becomes practical as KSK with 60× speedup. UOV-Ip-pkc, impossible to deploy undifferentiated due to protocol limits, achieves the most compact post-quantum A record responses (327 B) as ZSK. Hybrid PQ/T concatenation adds 7–19% overhead for backward-compatible quantum resistance.

The paper proceeds as follows. Section 2 reviews DNSSEC fundamentals, DNS transport constraints, post-quantum signature algorithms, and hybrid PQ/T schemes. Section 3 analyzes existing approaches to overcome size constraints and presents our differentiated selection strategy. Section 4 describes our containerized testbed architecture. Section 5 presents experimental results across five dimensions: response sizes, TCP fallback rates, resolution latency, signing performance, and zone storage impact. Section 6 discusses deployment implications and limitations.

## 2 Preliminaries

This section reviews DNSSEC fundamentals, transport constraints, post-quantum signature algorithms, and hybrid PQ/T schemes.

### 2.1 DNSSEC Trust Model

DNSSEC [1, 3, 2] authenticates DNS responses through a hierarchical chain of digital signatures rooted at a globally distributed trust anchor. Each signed zone contains two categories of cryptographic keys, formalized in RFC 6781 [16].

Zone Signing Keys (ZSKs) sign resource records within the zone. Every authoritative response for signed data includes an Resource Record Signature (RRSIG) record containing a ZSK signature. ZSKs are typically rotated frequently, on the order of weeks to months, to limit exposure from key compromise.

Key Signing Keys (KSKs) sign only the DNSKEY RRset. The KSK's hash, published as a DS record in the parent zone, anchors the zone to the trust hierarchy; the ZSK extends this trust to all other records. KSKs have longer validity periods, typically months to years, and their compromise has broader security implications because remediation requires coordination with the parent zone operator.

This separation, while not protocol-mandated, reflects operational reality: ZSK signatures appear in nearly every DNS response, whereas KSK signatures appear only when a resolver explicitly queries for DNSKEY records. RFC 6781[16] quantifies this asymmetry by noting that DNSKEY queries constitute a small fraction of total DNS traffic, typically triggered only during initial validation or key rollover events.

### 2.2 DNS Transport Constraints

DNS was designed for UDP transport with 512-byte messages [18]. EDNS(0) [11] allows clients to advertise larger buffer sizes, but IP fragmentation and middlebox filtering limit practical payloads to 1232 bytes [12].

Responses exceeding this threshold trigger TCP fallback: the server sets the truncated bit, prompting the client to retry over TCP. This adds latency from the TCP handshake, and overhead scales with message size a 60 KB response requires over forty TCP segments.

If the client cannot complete TCP fallback, or if intermediate devices block TCP port 53, resolution fails silently. This failure mode is particularly problematic because it provides no diagnostic information to the end user.

*The 64 KB hard limit.* RFC 1035 Section 4.2.2 specifies a 16-bit length field for TCP DNS messages, imposing an absolute ceiling of 65,535 bytes per message. Unlike zone transfers (AXFR), which can span multiple messages with one resource record per message, standard queries must return complete RRsets atomically. RFC 2181 [13] Section 5 mandates that a query for a specific label, class, and type must return all records in the associated RRset; partial responses are prohibited. If a DNSKEY RRset exceeds 64 KB, no standard mechanism exists to deliver it: the zone's trust chain becomes unverifiable, effectively breaking DNSSEC for that zone. While classical algorithms fit comfortably within this limit, post-quantum key sizes make it a practical concern.

### 2.3 Post-Quantum Signature Algorithms

Table 1 compares signature algorithms relevant to DNSSEC at NIST security levels 1–2. We include classical schemes for reference, the first generation of NIST-standardized post-quantum signatures, and candidates from the ongoing additional-signatures process. Timing data comes from the PQShield signatures zoo [25], measured on x86-64 with AVX2.

Table 1. Signature algorithm comparison at NIST security levels 1–2. Sizes in bytes; timings in thousands of CPU cycles (kcycles). The "combined" column represents the minimal DNSKEY response payload (two keys + one signature).

| **Algorithm** | **Family** | **Key** (bytes) | **Signature** (bytes) | **Combined** (bytes) | **Sign** (kcycles) | **Verify** (kcycles) | **Status** |
|---|---|---|---|---|---|---|---|
| *Classical (for reference)* | | | | | | | |
| RSASHA256 (2048-bit) | RSA | 256 | 256 | 768 | 27,000 | 45 | RFC 5702 |
| ECDSAP256SHA256 | ECDSA | 64 | 64 | 192 | 60 | 100 | RFC 6605 |
| Ed25519 | EdDSA | 32 | 64 | 128 | 42 | 130 | RFC 8080 |
| *NIST Standardized (2024–2025)* | | | | | | | |
| ML-DSA-44 | Lattice | 1,312 | 2,420 | 5,044 | 333 | 118 | FIPS 204 |
| SLH-DSA-128f | Hash | 32 | 17,088 | 17,152 | 239,794 | 12,910 | FIPS 205 |
| FN-DSA-512 (Falcon-512) | Lattice | 897 | 666 | 2,460 | 1,010 | 81 | FIPS 206 |
| *NIST Additional Signatures (Round 2)* | | | | | | | |
| MAYO-1 | Multivariate | 1,420 | 454 | 3,294 | 471 | 153 | Candidate |
| MAYO-2 | Multivariate | 4,912 | 186 | 10,010 | 286 | 56 | Candidate |
| UOV-Ip-pkc | Multivariate | 43,576 | 128 | 87,280 | 109 | 235 | Candidate |
| SQIsign-I[†] | Isogeny | 65 | 148 | 278 | 101,600 | 5,100 | Candidate |
| CROSS-R-SDP-1-small[‡] | Code | 77 | 12,434 | 12,511 | 4,048 | 2,725 | Candidate |

[†]SQIsign is included for comparison but not integrated into our testbed due to implementation complexity.
[‡]More optimized CROSS variants have been proposed; integration is left for future work.

We identify four observations from this comparison.

*No post-quantum algorithm matches classical compactness.* Even FN-DSA-512, the most compact standardized option, produces signatures ten times larger than ECDSA and keys fourteen times larger.

*Signature and key sizes exhibit an inverse relationship.* Lattice-based schemes balance key and signature sizes. Hash-based SLH-DSA achieves minimal keys (32 bytes) but produces signatures exceeding 17 KB. Multivariate schemes invert this tradeoff: UOV-Ip-pkc produces the smallest

signatures (128 bytes) but requires keys exceeding 43 KB. MAYO-2 occupies an intermediate position with 186-byte signatures and 4.9 KB keys.

*Signing and verification times vary by orders of magnitude.* Lattice schemes achieve sub-millisecond performance for both operations. Hash-based SLH-DSA-128f signs extremely slowly (239 million cycles), making it unsuitable for zones requiring frequent re-signing.

*Protocol limits exclude certain undifferentiated configurations.* The 64 KB DNS limit imposes a hard constraint on DNSKEY RRset size. Consider UOV-Ip-pkc with one ZSK, one KSK, and one RRSIG:

$$2 \times 43{,}576 + 128 = 87{,}280 \text{ bytes.}$$

This exceeds the 65,535-byte limit by 33%, making undifferentiated UOV-Ip-pkc deployment impossible. The trust chain becomes unverifiable.

### 2.4 Hybrid Signature Schemes

The transition to post-quantum cryptography introduces uncertainty: classical algorithms remain secure against current adversaries but are vulnerable to future quantum computers, while post-quantum algorithms resist quantum attacks but carry residual risk due to a shorter cryptanalytic record, particularly for side-channel attacks. Hybrid PQ/T [10]signature schemes resolve this tension by combining both, ensuring security as long as either component remains unbroken. We implement hybrids PQ/T through *parallel combiner*:

$$sig_{\text{hybrid}} = sig_{\text{P256}} \parallel sig_{\text{PQC}}, \qquad key_{\text{hybrid}} = key_{\text{P256}} \parallel key_{\text{PQC}}.$$

A single RRSIG carries the combined signature and a single DNSKEY carries both public keys, maintaining compatibility with RFC 4034 [3].

We select ECDSAP256SHA256 (P-256) following RFC 8624 [29] for universal resolver support and minimal overhead (64-byte signatures and keys). With MAYO-2 this yields 250-byte hybrid signatures and 4,976-byte hybrid keys. The classical overhead represents 7–19% depending on the post-quantum algorithm, acceptable for dual security guarantees.

Hybrid PQ/T schemes also provide operational flexibility: legacy resolvers validate only the P-256 prefix, treating the remainder as opaque data, while updated resolvers can verify the post-quantum component. Our testbed measures these verification paths independently (Section 4).

## 3 Differentiated Algorithm Selection

Section 2.3 showed that undifferentiated UOV-Ip-pkc deployment exceeds the 64 KB DNS limit, making direct post-quantum deployment infeasible. Existing attempts to bypass this limitation face major deployment obstacles: key separation violates RRset atomicity as defined by RFC 2181 [13], while application-layer fragmentation [15] requires resolver modifications and introduces unresolved security concerns [17]. To overcome these constraints without altering the DNSSEC protocol or impacting resolver compatibility, we propose *differentiated algorithm selection*.

The principle is straightforward: instead of using the same algorithm for both the Zone Signing Key (ZSK) and the Key Signing Key (KSK), we assign distinct algorithms to each role. This approach leverages their fundamentally different operational profiles. For example, undifferentiated deployment of UOV-Ip-pkc produces a DNSKEY RRset of 87,280 bytes, far beyond the 64 KB DNS limit. With differentiated selection, UOV-Ip-pkc is used only for the ZSK, while a compact algorithm such as Falcon-512 is used for the KSK. The resulting DNSKEY RRset then fits within protocol limits:

$$43{,}576_{(\text{ZSK})} + 897_{(\text{KSK})} + 128_{(\text{RRSIG})} = 44{,}601 \text{ bytes,}$$

transforming an impossible configuration into a viable one.

The motivation for differentiated selection stems from the asymmetry between ZSK and KSK functions. UOV-Ip-pkc offers extremely compact 128-byte signatures, ideal for high-frequency ZSK signing of A/AAAA/MX records, but its 43 KB public keys make undifferentiated deployment infeasible. By contrast, KSK operations are infrequent and can tolerate a slightly larger signature algorithm. Pairing UOV-Ip-pkc (ZSK) with Falcon-512 (KSK) therefore preserves UDP compatibility for routine traffic while ensuring that DNSKEY data remains under the 64 KB ceiling.

A further observation is that TCP fallback becomes unavoidable for DNSKEY queries with any post-quantum algorithm: even Falcon-512 alone exceeds typical UDP limits for DNSKEY responses. The objective is therefore not to eliminate TCP fallback, but to *confine* it to rare DNSKEY queries (less than 1% of traffic). Once validation material is cached, routine A/AAAA/MX lookups proceed entirely over UDP, with only the 128-byte UOV signature added per response. This sharply contrasts with undifferentiated deployment, where oversized signatures force frequent TCP fallback.

Differentiated algorithm selection is fully compatible with existing DNSSEC standards. RFC 4035 [2] explicitly allows zones to publish multiple DNSKEY records with distinct algorithm identifiers, and resolvers already validate heterogeneous key sets. Zone operator simply generates two key pairs with different algorithms, signs the DNSKEY RRset with the KSK, and signs all other RRsets with the ZSK. No protocol extensions or resolver modifications are required.

The only practical requirement is signing software capable of applying different algorithms to different RRset categories, a functionality we added to the `ldns` library [24]. Section 5 evaluates this strategy experimentally across 18 configurations, demonstrating its effectiveness for post-quantum DNSSEC deployment.

## 4 Testbed Architecture

To evaluate differentiated ZSK/KSK configurations, we designed a containerized testbed reproducing the full DNS hierarchy. The infrastructure consists of three NSD authoritative servers and an Unbound resolver, each running in isolated Docker containers. Appendix A details the query/response flow during resolution.

### 4.1 Containerized Hierarchical Setup

The hierarchy follows the standard delegation chain root → .uov → example.uov, with each level implemented by a dedicated NSD instance (Figure 1). The root zone is signed with its own ZSK/KSK pair and delegates the TLD via DS records. The TLD publishes its DNSKEY sets and manages delegations to child domains. The leaf server provides a complete operational zone, allowing measurement of response sizes and TCP fallback rates. Unbound is configured with strict DNSSEC validation and no caching, ensuring independent resolution measurements.

### 4.2 Zone Signing Infrastructure

We extended the ldns library to support several post-quantum algorithms (Falcon, ML-DSA, MAYO, UOV) using liboqs and algorithm-specific libraries. The testbed also implements hybrid PQ/T keys and signatures by concatenating a classical P-256 component with a post-quantum component in DNSKEY and RRSIG records, using dedicated algorithm identifiers. A modified Unbound resolver parses and verifies these hybrid PQ/T structures.

Critically, the system supports independent configuration of ZSK and KSK algorithms at each hierarchy level. This enables evaluation of combinations infeasible under undifferentiated algorithm policies; for example, a Falcon-512 KSK combined with a UOV-Ip-pkc ZSK produces a DNSKEY

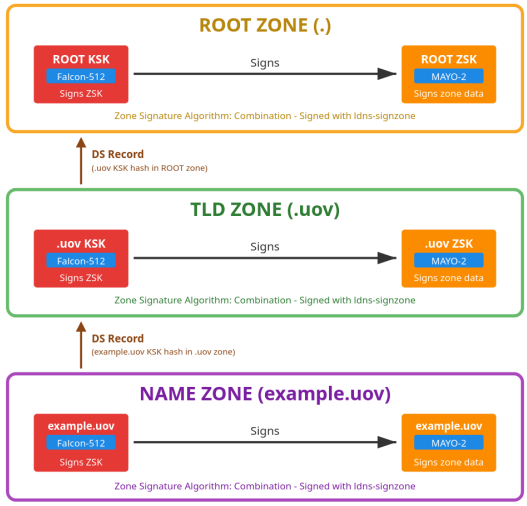



Fig. 1. Differentiated algorithm selection across the DNS hierarchy. Each zone uses Falcon-512 for the KSK and MAYO-2 for the ZSK. DS records in parent zones anchor child KSKs to the trust chain. Zone signing uses our extended `ldns-signzone` supporting per-role algorithm assignment.

RRset that remains within protocol limits, whereas a undifferentiated UOV deployment would exceed the maximum DNSKEY response size.

### 4.3 Large-Scale Zone Dataset

To evaluate post-quantum DNSSEC at production scale, we generated a synthetic TLD zone modeled after AFNIC's `.fr` structure (4.36M domains), reproducing the distribution of delegations and DS records observed in the real TLD. This full-scale zone serves for storage impact evaluation (Section 5.6). For signing, verification, and latency benchmarks, we extract 1,000-domain subsets from this zone to obtain statistically robust results within practical time constraints.

## 5 Experimental Results

This section evaluates post-quantum DNSSEC configurations across five dimensions: response sizes (Section 5.2), TCP fallback rates (Section 5.3), resolution latency (Section 5.4), signing performance (Section 5.5), and zone storage (Section 5.6). The experimental scope encompasses 18 configurations: 3 classical algorithms, 6 undifferentiated post-quantum deployments, 3 hybrid PQ/T schemes, and 6 differentiated KSK/ZSK combinations.

### 5.1 Experimental Configuration

The testbed isolates cryptographic and network performance from confounding factors. The Unbound resolver operates with caching disabled (cache-min-ttl, cache-max-ttl, msg-cache-size, rrset-cache-size set to zero) and single-threaded mode for deterministic measurements. Optimizations (prefetch, qname-minimisation, aggressive-nsec) are disabled to reflect worst-case validation overhead. Message buffers of 256 KB and socket buffers of 8 MB accommodate large post-quantum responses.

Each NSD instance runs in single-server mode (minimal-responses: yes), omitting optional additional records to isolate cryptographic overhead. Signed zones are pre-generated, ensuring consistent cryptographic material across test runs.

Network latency is simulated via `tc/netem` with 20 ms ± 5 ms per hop. Packet capture uses `tcpdump` with nanosecond-precision timestamps. All latency measurements report the mean of 100 independent resolutions with standard deviation and coefficient of variation. Signing benchmarks execute against a 1,000-domain dataset.

### 5.2 Response Size Analysis

Figure 2 presents DNS response sizes for DNSKEY and A record queries at the example.uov domain level across 18 configurations. We focus on this level because it represents the leaf of the delegation chain where operators have full control over algorithm selection. The root and TLD levels, operated by registries, will likely adopt conservative standardized algorithms during the transition period.

We measure DNSKEY and A record responses because they represent the two extremes of the key/signature tradeoff. DNSKEY responses contain both public keys plus one signature, revealing the impact of key sizes. A record responses contain minimal DNS payload plus one signature, isolating signature overhead. Together, these measurements characterize how each algorithm affects the infrequent key-distribution queries versus the routine record lookups that dominate operational traffic. Table 2 summarizes measurements with overhead factors relative to ECDSAP256SHA256.

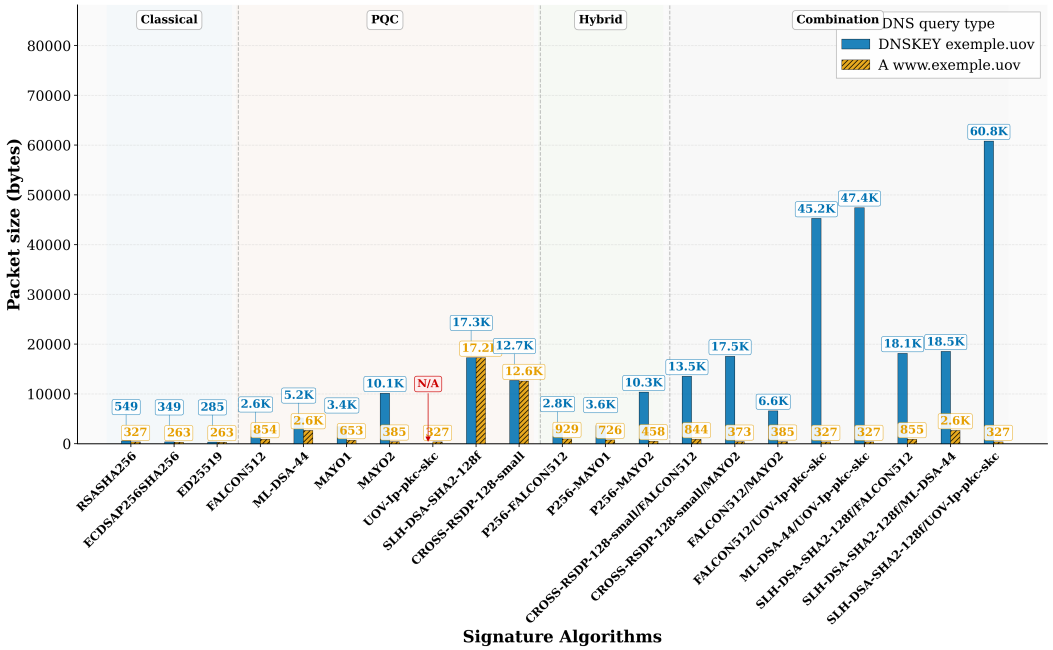



Fig. 2. DNS response sizes for DNSKEY and A record queries across algorithm families. N/A indicates DNSKEY retrieval failure for undifferentiated UOV-Ip-pkc (87 KB response exceeds 64 KB DNS limit).

Classical algorithms produce responses well within UDP constraints. ED25519 generates the most compact DNSKEY responses at 285 bytes, followed by ECDSAP256SHA256 at 349 bytes and RSASHA256 at 549 bytes. For A records, ED25519 and ECDSA produce identical 263-byte

responses, while RSA reaches 327 bytes. These values establish the baseline against which post-quantum configurations must be evaluated.

Post-quantum algorithms exhibit the fundamental tradeoff between key size and signature size inherent to each cryptographic family. MAYO-2 exemplifies the compact-signature approach: A record responses reach only 385 bytes (×1.46 overhead), but DNSKEY responses grow to 10,127 bytes as both 4.9 KB keys must be transmitted. MAYO-1 presents a different balance with smaller keys (1.4 KB) but larger signatures (454 bytes), yielding 653-byte A records and 3,411-byte DNSKEY responses. UOV-Ip-pkc pushes compact signatures to the extreme: its 128-byte signatures produce 327-byte A records matching RSA, but its 43.5 KB keys yield an 87 KB DNSKEY response exceeding the 64 KB DNS limit, making undifferentiated deployment impossible.

Falcon-512 and ML-DSA-44 balance key and signature sizes, producing moderate overhead for both query types. Falcon-512 achieves 2,632-byte DNSKEY and 853-byte A records, while ML-DSA-44 reaches 5,161 bytes and 2,645 bytes respectively. ML-DSA's 2.4 KB signatures generate A records exceeding the 1232-byte UDP threshold, triggering TCP fallback for routine queries. SLH-DSA-SHA2-128f represents the extreme of compact keys (32 bytes) offset by massive signatures (17 KB), making every query require TCP transmission. CROSS-R-SDP-1-small exhibits similar behavior: despite compact keys (77 bytes), its 12,434-byte signatures produce 12,579-byte A records, triggering TCP fallback for every query like SLH-DSA-128f

Table 2. DNS response sizes across algorithm configurations. Overhead computed relative to ECDSAP256SHA256 (349 bytes for DNSKEY, 263 bytes for A records). Differentiated configurations use notation KSK/ZSK.

| **Configuration** | **DNSKEY** | **DNSKEY** | **A record** | **A** |
|---|---|---|---|---|
| ED25519 | 285 B | ×0.82 | 263 B | ×1.00 |
| ECDSAP256SHA256 | 349 B | ×1.00 | 263 B | ×1.00 |
| RSASHA256 | 549 B | ×1.57 | 327 B | ×1.24 |
| Falcon-512 | 2,630 B | ×7.54 | 856 B | ×3.26 |
| MAYO-1 | 3,411 B | ×9.77 | 653 B | ×2.48 |
| ML-DSA-44 | 5,161 B | ×14.79 | 2,645 B | ×10.06 |
| MAYO-2 | 10,127 B | ×29.02 | 385 B | ×1.46 |
| CROSS-R-SDP-1-small | 12,703 B | ×36.40 | 12,579 B | ×47.83 |
| SLH-DSA-SHA2-128f | 17,269 B | ×49.48 | 17,247 B | ×65.58 |
| UOV-Ip-pkc | N/A | N/A | 327 B | ×1.24 |
| P256+Falcon-512 | 2,835 B | ×8.12 | 924 B | ×3.51 |
| P256+MAYO-1 | 3,614 B | ×10.36 | 726 B | ×2.76 |
| P256+MAYO-2 | 10,330 B | ×29.60 | 458 B | ×1.74 |
| Falcon-512/MAYO-2 | 6,583 B | ×18.86 | 385 B | ×1.46 |
| Falcon-512/UOV-Ip-pkc | 45,247 B | ×129.65 | 327 B | ×1.24 |
| ML-DSA-44/UOV-Ip-pkc | 47,425 B | ×135.89 | 327 B | ×1.24 |
| SLH-DSA-128f/Falcon-512 | 18,134 B | ×51.96 | 854 B | ×3.25 |
| SLH-DSA-128f/ML-DSA-44 | 18,549 B | ×53.15 | 2,645 B | ×10.06 |
| SLH-DSA-128f/UOV-Ip-pkc | 60,813 B | ×174.25 | 327 B | ×1.24 |
| CROSS/Falcon-512 | 13,523 B | ×38.75 | 843 B | ×3.21 |
| CROSS/MAYO-2 | 17,538 B | ×50.25 | 373 B | ×1.42 |

Hybrid PQ/T schemes concatenate classical and post-quantum signatures, increasing response sizes. P256+Falcon-512 produces 2,835-byte DNSKEY and 924-byte A records, representing 7.7% overhead

compared to pure Falcon-512. Notably, P256+MAYO-1 achieves 726-byte A records, smaller than pure Falcon-512's 856 bytes, demonstrating that a hybrid PQ/T with compact PQC signatures can outperform a pure PQC algorithm with larger signatures.

Differentiated configurations exploit the KSK/ZSK role distinction to optimize A record sizes while accepting larger DNSKEY responses. This approach transforms failed or impractical deployments into viable configurations. Undifferentiated UOV-Ip-pkc fails entirely—the 87 KB DNSKEY response exceeds the 64 KB DNS limit, breaking the trust chain (N/A in Table 2). Undifferentiated SLH-DSA-128f is impractical due to its 8-minute signing time and 17 KB signatures triggering TCP for every query. Similarly, undifferentiated CROSS triggers TCP fallback for every A record query due to its 12.4 KB signatures—even larger than ML-DSA-44's 2.4 KB signatures. Yet under differentiated selection, SLH-DSA-128f as KSK contributes only one signature, while UOV-Ip-pkc as ZSK provides the most compact A record responses.

Three configurations achieve the minimum post-quantum A record size of 327 bytes: Falcon-512/UOV-Ip-pkc, ML-DSA-44/UOV-Ip-pkc, and SLH-DSA-128f/UOV-Ip-pkc. Their DNSKEY responses vary based on KSK algorithm (45.2–60.8 KB) but remain below the 64 KB DNS ceiling. The SLH-DSA-128f/UOV-Ip-pkc configuration is particularly notable: it combines two algorithms that undifferentiated constraints would each prohibit, yet differentiation makes their pairing optimal for response compactness.

Falcon-512/MAYO-2 achieves 385-byte A records with a more moderate 6.6 KB DNSKEY response. This configuration pairs a NIST-standardized algorithm (FN-DSA-512, FIPS 206) for the trust-critical KSK role with MAYO-2's efficient signatures for routine traffic.

The response size analysis establishes a hierarchy for routine A record traffic: UOV-Ip-pkc as ZSK achieves minimum overhead (×1.24), followed by MAYO-2 (×1.46), MAYO-1 (×2.48), and Falcon-512 (×3.24). ML-DSA-44, CROSS, and SLH-DSA-128f as ZSK produce responses exceeding the UDP threshold, triggering TCP fallback for every query. However, response size alone does not determine operational performance; the critical factor is whether responses exceed the 1232-byte threshold.

### 5.3 TCP Fallback Analysis

Figure 3 and Table 3 present packet distribution for a complete resolution of `www.example.uov`, the same query used in Section 5.2. Classical algorithms complete resolution entirely over UDP. ECDSA, ED25519, and RSA each require 36 packets with zero truncations, establishing the baseline.Post-quantum algorithms divide into two categories. The first category (Falcon-512, MAYO-1/2, hybrids PQ/T, and differentiated configurations with compact-signature ZSKs) experiences truncation only for DNSKEY queries—exactly 3 events corresponding to each hierarchy level. TCP packet counts range from 19 to 52 (28–59% of traffic), but crucially, routine A record queries complete over UDP. TCP overhead is confined to initial trust chain establishment.The second category (ML-DSA-44, CROSS, and SLH-DSA-128f as ZSK) triggers truncation for all query types: 22–36 events affecting NS, DS, A, and DNSKEY queries. TCP packet counts reach 94 for ML-DSA-44 (68.1%) and 212 for SLH-DSA-128f (82.8%), transforming every DNS exchange into a TCP transaction. CROSS exhibits similar behavior to SLH-DSA-128f with 36 truncation events and 320 TCP packets (81.6%).Undifferentiated UOV-Ip-pkc (0% TCP, 8 packets) reflects resolution failure—the DNSKEY response exceeds protocol limit, not transport efficiency.

Signature size determines UDP packet counts through glue record eviction. NS responses typically include A records for nameservers in the Additional section. When signatures consume substantial response space, servers omit these glue records, forcing additional lookups. Configurations with the smallest signatures (UOV-Ip-pkc at 128 bytes, MAYO-2 at 186 bytes) preserve glue records,

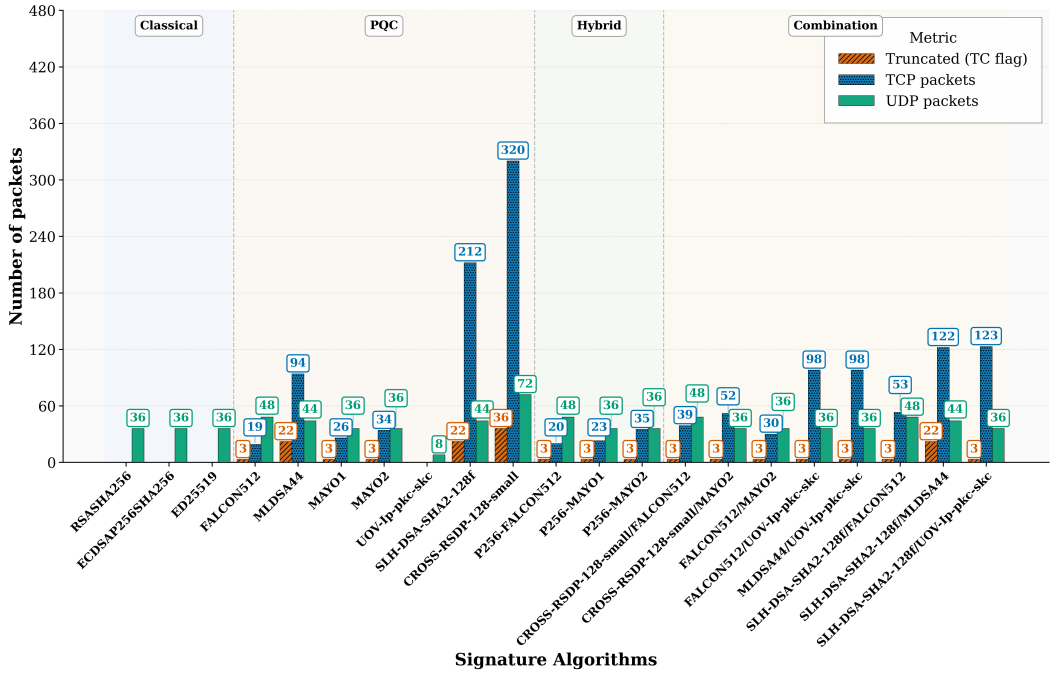



Fig. 3. Packet distribution for resolving `www.example.uov` across algorithm configurations. Classical algorithms complete entirely over UDP (36 packets). Post-quantum configurations exhibit two patterns: DNSKEY-only truncation (3 events, 19–52 TCP packets) versus generalized truncation (22–36 events, 94–320 TCP packets).

yielding 36 UDP packets identical to classical algorithms. Falcon-512's 666-byte signatures trigger eviction, adding 12 UDP packets for nameserver resolution.The critical metric is truncation count, not TCP percentage. Configurations with 3 truncations confine TCP to DNSKEY queries, which represent less than 1% of production traffic. Configurations with 22–36 truncations impose TCP on every query. Like SLH-DSA-128f, differentiated CROSS configurations reduce truncations to 3, confining TCP overhead to the KSK role.

### 5.4 Resolution Latency

We measure end-to-end resolution latency for `www.example.uov`, repeated 100 times with cold-start conditions: caching disabled and connection state reset between each measurement. Network latency is simulated via `tc/netem` (20 ms ± 5 ms per hop). Table 4 and Figure 4 report mean, standard deviation, and coefficient of variation.

Classical algorithms establish the baseline at 389–392 ms with CV (coefficient of variation) around 5–6%. The similarity across algorithms confirms that network round-trips dominate latency when responses fit within UDP limits.

Post-quantum latency correlates with truncation count. Algorithms with DNSKEY-only truncation (3 events) achieve 491–620 ms with CV below 5%: MAYO-2 leads at 491 ms (×1.26), followed by MAYO-1 at 494 ms and Falcon-512 at 620 ms. Algorithms with generalized truncation (22–36 events) exhibit higher latency and variance: ML-DSA-44 averages 995 ms (CV 13.3%), SLH-DSA-128f reaches

Table 3. TCP fallback analysis for resolving `www.example.uov`. Truncation count indicates TC-flagged responses; 3 truncations affect only DNSKEY queries, while 22–36 truncations indicate generalized fallback.

| Configuration | Trunc. | TCP | UDP | %TCP |
|---|---|---|---|---|
| ECDSAP256SHA256 | 0 | 0 | 36 | 0% |
| ED25519 | 0 | 0 | 36 | 0% |
| RSASHA256 | 0 | 0 | 36 | 0% |
| Falcon-512 | 3 | 19 | 48 | 28.4% |
| MAYO-1 | 3 | 26 | 36 | 41.9% |
| MAYO-2 | 3 | 34 | 36 | 48.6% |
| ML-DSA-44 | 22 | 94 | 44 | 68.1% |
| CROSS-R-SDP-1-small | 36 | 320 | 72 | 81.6% |
| SLH-DSA-SHA2-128f | 22 | 212 | 44 | 82.8% |
| UOV-Ip-pkc (uniform) | 0 | 0 | 8 | 0% |
| P256+Falcon-512 | 3 | 20 | 48 | 29.4% |
| P256+MAYO-1 | 3 | 23 | 36 | 39.0% |
| P256+MAYO-2 | 3 | 35 | 36 | 49.3% |
| Falcon-512/MAYO-2 | 3 | 30 | 36 | 45.5% |
| Falcon-512/UOV-Ip-pkc | 3 | 98 | 36 | 73.1% |
| ML-DSA-44/UOV-Ip-pkc | 3 | 98 | 36 | 73.1% |
| SLH-DSA-128f/Falcon-512 | 3 | 53 | 48 | 52.5% |
| SLH-DSA-128f/ML-DSA-44 | 22 | 122 | 44 | 73.5% |
| SLH-DSA-128f/UOV-Ip-pkc | 3 | 123 | 36 | 77.4% |
| CROSS/Falcon-512 | 3 | 39 | 48 | 44.8% |
| CROSS/MAYO-2 | 3 | 52 | 36 | 59.1% |

1,241 ms (CV 22.8%). CROSS exhibits similar behavior to SLH-DSA-128f with 1,095 ms mean latency and 21.4% CV. Undifferentiated UOV-Ip-pkc at 99 ms reflects resolution failure.

Hybrid PQ/T configurations achieve latencies statistically indistinguishable from pure post-quantum counterparts. The additional 64-byte P256 signature has negligible impact as response sizes remain within the same TCP segment boundaries.

Differentiated configurations with UOV-Ip-pkc ZSK achieve 580–593 ms despite TCP percentages exceeding 73%. Once DNSKEY completes via TCP, A record queries benefit from UOV's 128-byte signatures without fallback. SLH-DSA-128f/UOV-Ip-pkc at 593 ms achieves 2.1× speedup compared to undifferentiated SLH-DSA-128f. Similarly, CROSS/MAYO-2 at 547 ms achieves 2.0× speedup compared to undifferentiated CROSS. However, SLH-DSA-128f/ML-DSA-44 at 1,184 ms remains the worst differentiated configuration—its 22 truncations negate the benefits of role separation.

Latency also includes verification time at the resolver, though this contribution remains marginal compared to network round-trips. The next section examines authoritative-side costs: zone signing time and verification performance.

### 5.5 Zone Signing and Verification Performance

Zone signing constrains update frequency for authoritative servers, while verification speed directly impacts resolver throughput—a critical metric for DNS where resolvers validate signatures on every authenticated response. We evaluate both on a 1,000-domain zone (100 iterations, CPU pinned at 3.6 GHz, zone files in tmpfs). All configurations achieved CV below 2%.

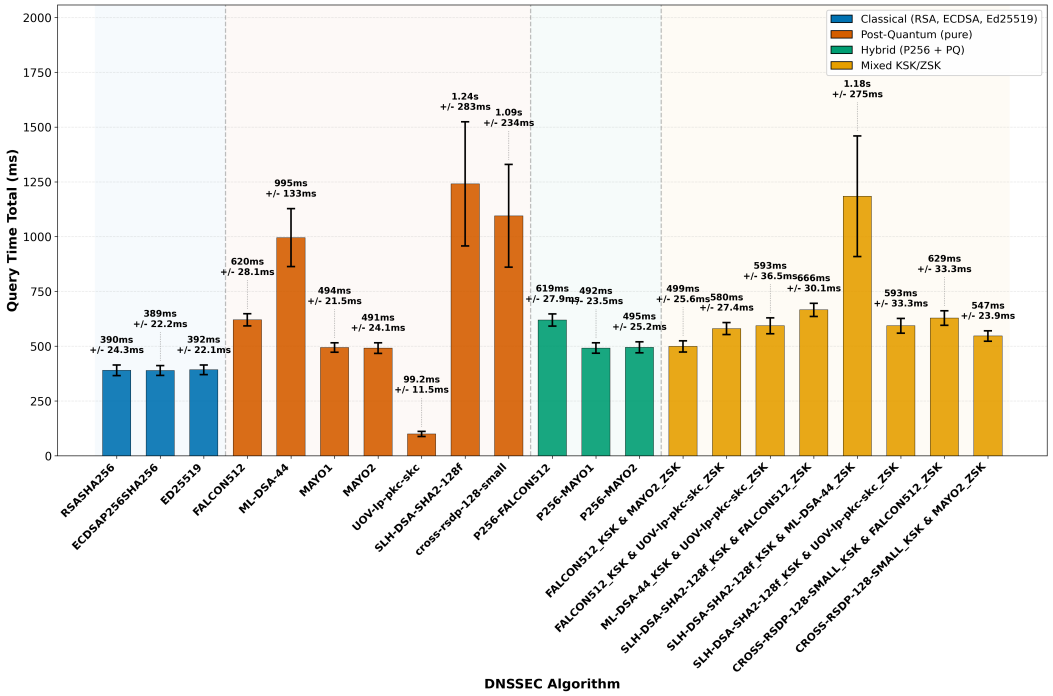



Fig. 4. Resolution latency comparison across algorithm categories ($n = 100$, error bars show ±1 standard deviation). Classical algorithms cluster around 390 ms; first-tier PQC achieves 491–620 ms with stable variance; second-tier PQC exhibits both higher latency and higher variance. Differentiated configurations with UOV-Ip-pkc ZSK achieve latencies below undifferentiated Falcon-512 despite high TCP percentages.

Classical algorithms establish the baseline. ECDSA achieves the fastest signing at 0.78 s with verification at 1.86 s. RSA exhibits an inverse profile: slow signing (9.22 s) due to modular exponentiation, but fast verification (1.14 s, 0.61× ECDSA) using the small public exponent—a tradeoff historically favoring resolver performance.

Post-quantum algorithms show diverse profiles. For signing, MAYO-2 (2.02 s, 2.6×) and ML-DSA-44 (2.33 s, 3.0×) remain competitive with classical algorithms, enabling frequent zone updates. Falcon-512 signs in 4.23 s (5.4×), acceptable for most deployments. UOV-Ip-pkc at 7.91 s (10.1×) is comparable to RSA despite its 43.5 KB keys. CROSS at 38.30 s (49.1×) and SLH-DSA-128f at 478.7 s (8 minutes) makes undifferentiated deployment impractical for zones requiring regular updates.

For verification—the critical path for resolver throughput—MAYO-2 leads at 1.07 s (0.58× ECDSA, 42% faster), making it attractive for high-volume resolvers. Falcon-512 verifies in 1.78 s (0.96×), comparable to ECDSA. ML-DSA-44 at 3.20 s (×1.7) penalizes resolver performance. CROSS at 35.53 s (×19.1) exhibits similar behavior to SLH-DSA-128f at 45.1 s, excluding both from production resolver deployments.

Differentiated configurations confirm that ZSK algorithm determines performance. The KSK signs only the DNSKEY RRset (one signature), while the ZSK signs thousands of RRsets. Configurations sharing the same ZSK exhibit equivalent signing and verification times regardless of KSK: all three UOV-Ip-pkc ZSK configurations sign in 7.90–7.94 s independent of whether paired with Falcon-512, ML-DSA-44, or SLH-DSA-128f.

Table 4. Resolution latency across algorithm configurations ($n = 100$). Overhead computed relative to ECDSAP256SHA256. High CV values (>10%) indicate unstable performance.

| Configuration | Mean (ms) | ± Std | CV | Overhead |
|---|---|---|---|---|
| ECDSAP256SHA256 | 389 | 22 | 5.7% | ×1.00 |
| RSASHA256 | 390 | 24 | 6.2% | ×1.00 |
| ED25519 | 392 | 22 | 5.6% | ×1.01 |
| MAYO-2 | 491 | 24 | 4.9% | ×1.26 |
| MAYO-1 | 494 | 22 | 4.4% | ×1.27 |
| Falcon-512 | 620 | 28 | 4.5% | ×1.59 |
| ML-DSA-44 | 995 | 133 | 13.3% | ×2.56 |
| CROSS-R-SDP-1-small | 1,095 | 234 | 21.4% | ×2.82 |
| SLH-DSA-SHA2-128f | 1,241 | 283 | 22.8% | ×3.19 |
| UOV-Ip-pkc (uniform) | 99 | 12 | 11.6% | — |
| P256+MAYO-1 | 492 | 23 | 4.8% | ×1.26 |
| P256+MAYO-2 | 495 | 25 | 5.1% | ×1.27 |
| P256+Falcon-512 | 619 | 28 | 4.5% | ×1.59 |
| Falcon-512/MAYO-2 | 499 | 26 | 5.1% | ×1.28 |
| Falcon-512/UOV-Ip-pkc | 580 | 27 | 4.7% | ×1.49 |
| ML-DSA-44/UOV-Ip-pkc | 593 | 37 | 6.2% | ×1.52 |
| SLH-DSA-128f/Falcon-512 | 666 | 30 | 4.5% | ×1.71 |
| SLH-DSA-128f/UOV-Ip-pkc | 593 | 33 | 5.6% | ×1.52 |
| SLH-DSA-128f/ML-DSA-44 | 1,184 | 275 | 23.2% | ×3.04 |
| CROSS/Falcon-512 | 629 | 33 | 5.3% | ×1.62 |
| CROSS/MAYO-2 | 547 | 24 | 4.4% | ×1.41 |

This independence rehabilitates SLH-DSA-128f and CROSS. As KSK, they contribute only one signature; SLH-DSA-128f/Falcon-512 signs in 4.26 s and verifies in 1.77 s, matching undifferentiated Falcon-512 while preserving hash-based security for the trust anchor. SLH-DSA-128f/UOV-Ip-pkc achieves 60× signing speedup versus undifferentiated SLH-DSA-128f. Similarly, CROSS/MAYO-2 achieves 19× signing speedup versus undifferentiated CROSS. For resolver-facing deployments, CROSS/MAYO-2 achieves the best verification at 0.99 s (0.53× ECDSA), slightly outperforming Falcon-512/MAYO-2 at 1.03 s (0.55× ECDSA).

Hybrid PQ/T schemes incur signing overhead from dual signature generation: P256+MAYO-2 signs in 2.61 s (29% over pure MAYO-2), P256+Falcon-512 in 4.74 s. For verification, these schemes offer flexibility. Classical verification at 1.89 s (P256+MAYO-2) matches ECDSA baseline, ensuring backward compatibility. Quantum verification at 1.15 s is 38% faster—upgraded resolvers benefit from MAYO-2's efficiency. P256+Falcon-512 shows quantum verification (1.85 s) outperforming classical (2.18 s) by 15%.

The next section projects these results to TLD-scale zones, examining storage overhead.

### 5.6 Zone Storage Impact

We generated a synthetic .fr zone using AFNIC structural statistics (4.36M domains) to evaluate storage impact. The unsigned zone occupies 0.51 GB; signed zone size scales with signature size multiplied by the number of RRsets.

Table 5. Zone signing and verification time for 1,000 domains (mean ± std, $n = 100$ except SLH-DSA undifferentiated with $n = 10$). Overhead relative to ECDSAP256SHA256.

| **Algorithm** | **Sign (s)** | **Verify (s)** | **Sign** | **Verify** |
|---|---|---|---|---|
| ECDSAP256SHA256 | 0.78 ± 0.01 | 1.86 ± 0.01 | ×1.0 | ×1.0 |
| ED25519 | 1.04 ± 0.01 | 2.39 ± 0.01 | ×1.3 | ×1.3 |
| RSASHA256 | 9.22 ± 0.02 | 1.14 ± 0.01 | ×11.8 | ×0.61 |
| MAYO-2 | 2.02 ± 0.01 | 1.07 ± 0.01 | ×2.6 | ×**0.58** |
| MAYO-1 | 3.41 ± 0.05 | 2.08 ± 0.01 | ×4.4 | ×1.1 |
| Falcon-512 | 4.23 ± 0.02 | 1.78 ± 0.01 | ×5.4 | ×0.96 |
| ML-DSA-44 | 2.33 ± 0.02 | 3.20 ± 0.01 | ×3.0 | ×1.7 |
| UOV-Ip-pkc | 7.91 ± 0.04 | 2.60 ± 0.02 | ×10.1 | ×1.4 |
| CROSS-R-SDP-1-small | 38.30 ± 0.20 | 35.53 ± 0.11 | ×49.1 | ×19.1 |
| SLH-DSA-SHA2-128f | 478.7 ± 28.3 | 45.1 ± 3.3 | ×612 | ×24.3 |
| Falcon-512/MAYO-2 | 2.00 ± 0.01 | 1.03 ± 0.01 | ×2.6 | ×0.55 |
| Falcon-512/UOV-Ip-pkc | 7.90 ± 0.09 | 2.15 ± 0.02 | ×10.1 | ×1.2 |
| ML-DSA-44/UOV-Ip-pkc | 7.90 ± 0.04 | 2.17 ± 0.02 | ×10.1 | ×1.2 |
| SLH-DSA-128f/Falcon-512 | 4.26 ± 0.02 | 1.77 ± 0.01 | ×5.5 | ×0.95 |
| SLH-DSA-128f/ML-DSA-44 | 2.35 ± 0.01 | 3.19 ± 0.01 | ×3.0 | ×1.7 |
| SLH-DSA-128f/UOV-Ip-pkc | 7.94 ± 0.04 | 2.16 ± 0.02 | ×10.2 | ×1.2 |
| CROSS/Falcon-512 | 4.22 ± 0.01 | 1.73 ± 0.00 | ×5.4 | ×0.93 |
| CROSS/MAYO-2 | 2.01 ± 0.01 | 0.99 ± 0.01 | ×2.6 | ×**0.53** |

Table 6. Hybrid PQ/T performance. Classical verification uses only P256; quantum verification uses only the PQC component.

| **Configuration** | **Sign (s)** | **Classical (s)** | **Quantum (s)** | **Sign ×** |
|---|---|---|---|---|
| P256+Falcon-512 | 4.74 ± 0.02 | 2.18 ± 0.01 | 1.85 ± 0.01 | 6.1 |
| P256+MAYO-1 | 3.88 ± 0.02 | 2.02 ± 0.01 | 2.15 ± 0.04 | 5.0 |
| P256+MAYO-2 | 2.61 ± 0.01 | 1.89 ± 0.01 | 1.15 ± 0.01 | 3.3 |
| *Reference* | | | | |
| ECDSAP256SHA256 | 0.78 ± 0.01 | 1.86 ± 0.01 | — | 1.0 |
| MAYO-2 | 2.02 ± 0.01 | — | 1.07 ± 0.01 | 2.6 |

Classical algorithms establish moderate overhead: ECDSA and ED25519 at 1.69 GB (×3.3), RSA at 2.09 GB (×4.1).Post-quantum algorithms span two orders of magnitude. UOV-Ip-pkc achieves 2.10 GB (×4.1), equivalent to RSA despite quantum resistance. MAYO-2 follows at 2.47 GB (×4.8). Falcon-512 reaches 5.52 GB (10.8×), manageable with current infrastructure. ML-DSA-44 at 16.98 GB (33.2×), CROSS at 88.66 GB (173.5×), and SLH-DSA-128f at 112.48 GB (220×) require storage infrastructure upgrades for TLD-scale deployment. Beyond storage, large-signature algorithms also increase memory requirements during signing. SLH-DSA-128f additionally requires multithreaded signing to complete within practical time constraints—our single-threaded measurements (478.7 s for 1,000 domains) would extrapolate to over 24 days for a 4.36M-domain zone.

Differentiated configurations confirm that storage depends exclusively on ZSK signature size. Falcon-512/MAYO-2 matches undifferentiated MAYO-2 at 2.47 GB; all UOV-Ip-pkc ZSK configurations yield 2.10 GB regardless of KSK algorithm. Similarly, CROSS/MAYO-2 achieves the same 2.47 GB as

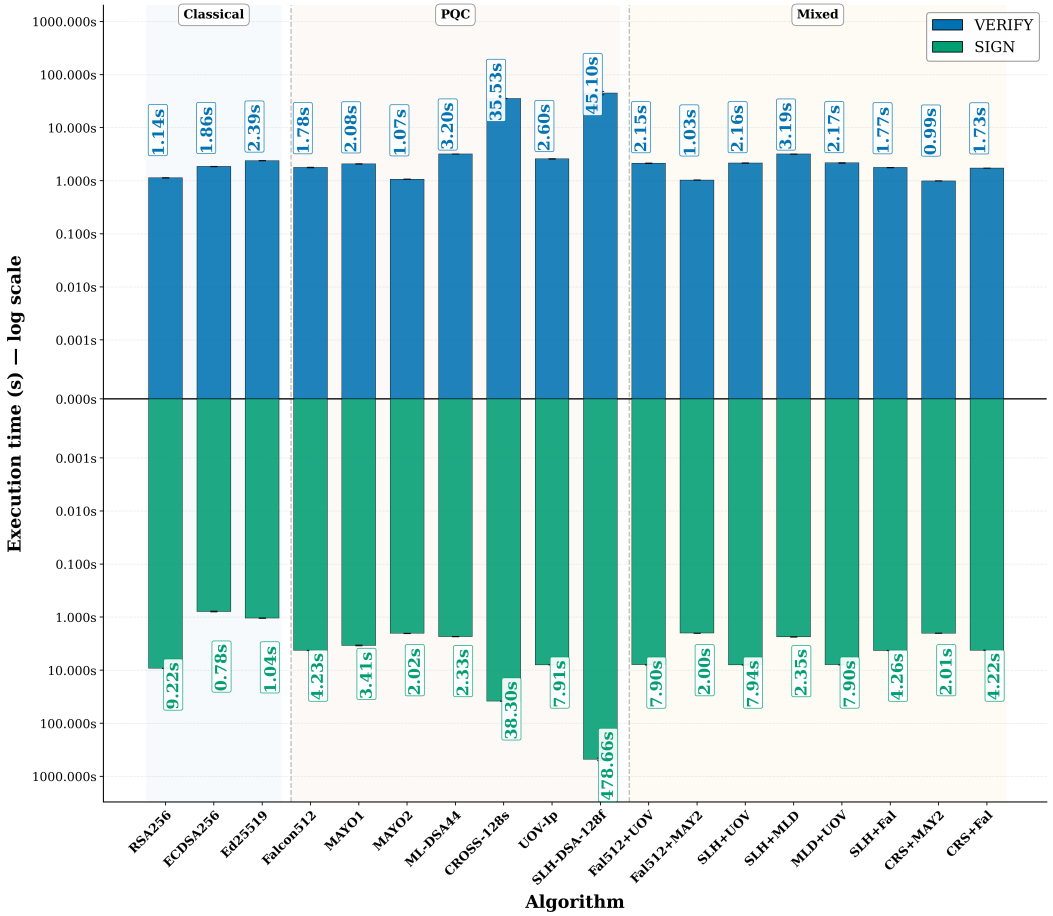



Fig. 5. Zone signing and verification performance (1,000 domains, $n = 100$). Logarithmic scale reveals the two-order-of-magnitude gap between SLH-DSA-128f undifferentiated and all other configurations.

undifferentiated MAYO-2, representing a 36× reduction compared to undifferentiated CROSS.Hybrid PQ/T schemes add 64 bytes per signature. P256+MAYO-2 produces 2.95 GB (19% over pure MAYO-2); P256+Falcon-512 reaches 6.00 GB (8.7% over pure Falcon-512)—acceptable overhead for dual security.The following section synthesizes these five evaluation dimensions to identify optimal deployment strategies.

### 5.7 Summary

Table 8 synthesizes experimental results across the five evaluation dimensions, revealing how differentiated algorithm selection and hybrid PQ/T schemes expand viable deployment options. Four findings emerge from our measurements:

**ZSK determines performance.** Signing time, verification speed, response size, and storage depend entirely on ZSK choice; KSK contributes negligibly (Section 5.5). Operators can select conservative KSK algorithms without performance penalty.

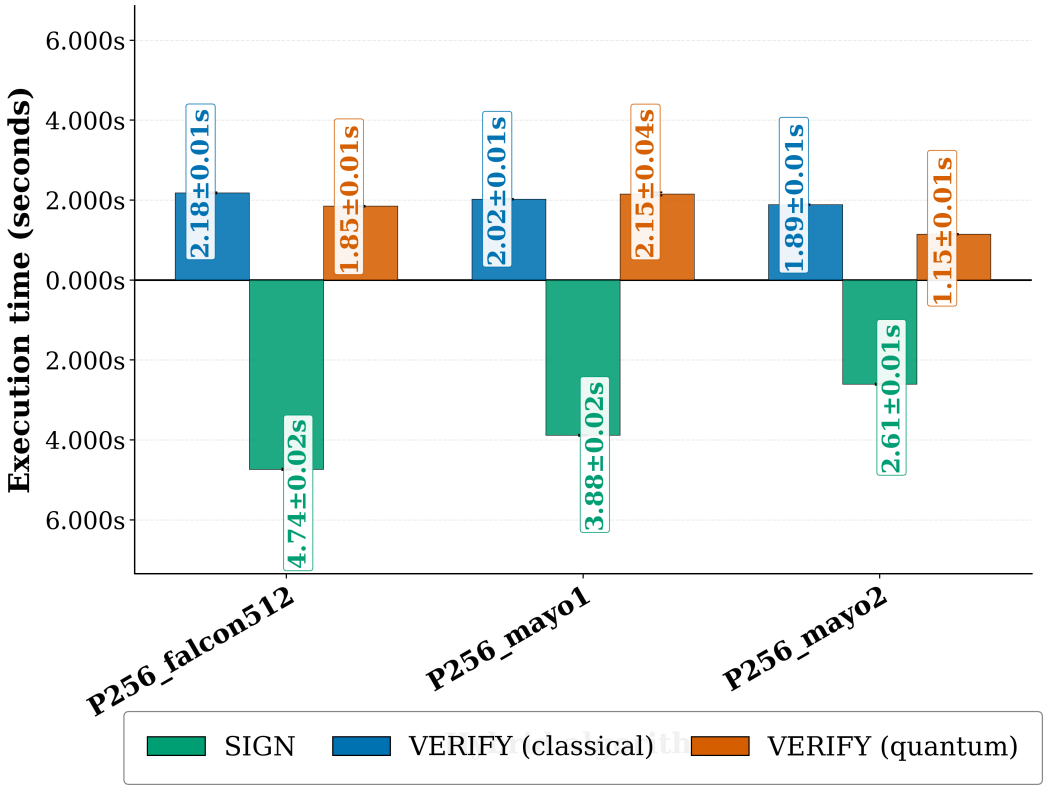



Fig. 6. Hybrid PQ/T dual verification paths. Classical verification (blue) enables backward compatibility; quantum verification (red) provides post-quantum security. P256+MAYO-2 quantum path achieves 38% faster verification than pure ECDSA.

**Differentiation rehabilitates impractical algorithms.** Algorithms dismissed under undifferentiated constraints become viable components. UOV-Ip-pkc, which fails undifferentiated deployment due to protocol limits (Section 5.2), achieves minimum A record overhead as ZSK. SLH-DSA-128f, impractical due to 8-minute signing (Section 5.5), becomes viable as KSK with ×60 speedup while preserving hash-based security. ML-DSA-44, penalized by 23 truncations and high latency variance as ZSK (Section 5.3), could serve as KSK where its fast signing (2.33 s) benefits zones with frequent key rollovers.

**Hybrid PQ/T overhead is acceptable.** P256 concatenation adds 7–19% to response sizes (Section 5.2) and 29% to signing time (Section 5.5), providing backward-compatible quantum resistance during the transition period.

**The design space remains open.** The configurations tested here do not exhaust viable combinations. Differentiation enabes operators to match algorithm characteristics—compact signatures, fast verification, conservative security assumptions—to their specific operational requirements. Future work may explore additional pairings as new post-quantum candidates emerge from NIST standardization.

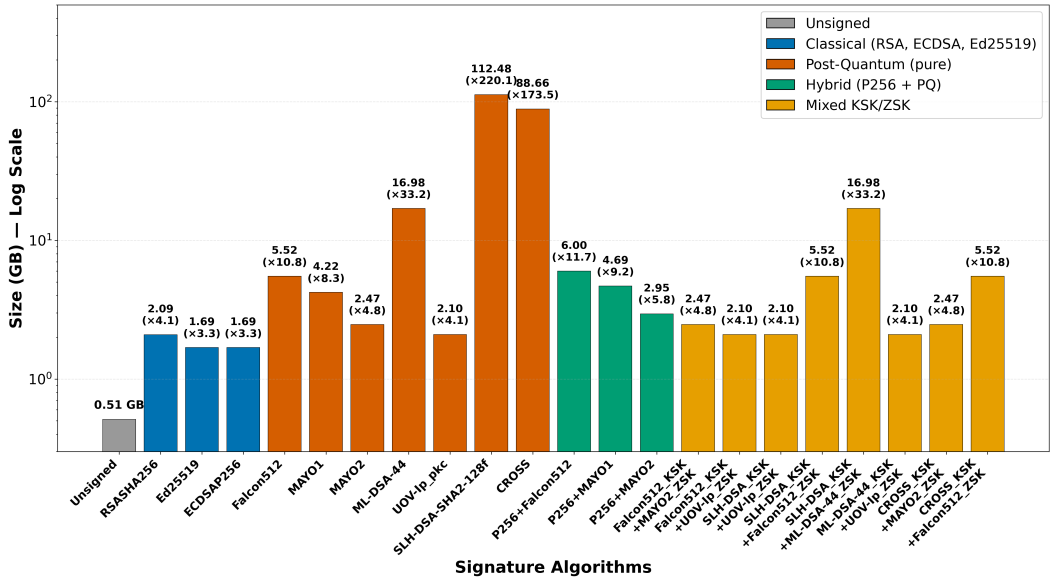



Fig. 7. Zone size for the synthetic .fr zone (4.36M domains). Classical algorithms increase storage 3–4×. Post-quantum algorithms range from 4× (UOV-Ip-pkc) to 220× (SLH-DSA-128f). Differentiated configurations match their ZSK algorithm's footprint.

## 6 Discussion and Conclusion

### 6.1 Implications for Deployment

The central finding of this work is that differentiation transforms the landscape of deployable algorithms. Under undifferentiated constraints, only Falcon-512 and MAYO variants achieve practical deployment profiles among post-quantum candidates. SLH-DSA-128f's 8-minute signing time eliminates it from consideration; UOV-Ip-pkc's 87 KB DNSKEY response violates protocol limits entirely. Differentiation removes these barriers by confining each algorithm's limitations to its designated role.

This expanded algorithm space has significant implications for the DNS root zone, where cryptographic conservatism is paramount. SLH-DSA's hash-based security relies solely on SHA-2 properties rather than the number-theoretic assumptions underlying lattice or multivariate schemes. A differentiated configuration placing SLH-DSA-128f as root KSK and Falcon-512 or MAYO-2 as root ZSK would combine conservative trust anchor security with acceptable operational performance. Similar reasoning applies throughout the DNS hierarchy: TLD operators could adopt SLH-DSA KSKs for defense-in-depth while deploying MAYO-2 ZSKs for resolver performance; domain operators could select UOV-Ip-pkc ZSKs for minimum response overhead.

Hybrid PQ/T schemes, evaluated alongside differentiated configurations, address cryptographic uncertainty during the transition period. Our measurements demonstrate acceptable overhead with P256+MAYO-2 achieves classical verification within 2% of pure ECDSA, while quantum verification runs 38% faster than the classical baseline. This suggests a migration path where legacy resolvers validate the P256 component transparently while upgraded resolvers benefit from post-quantum efficiency.

Table 7. Zone sizes for the synthetic .fr zone. Storage correlates directly with ZSK signature size; KSK contributes only one signature per zone.

| Configuration | Signature size | Zone size | Overhead |
|---|---|---|---|
| Unsigned | — | 0.51 GB | ×1.0 |
| ED25519 | 64 B | 1.69 GB | ×3.3 |
| ECDSAP256SHA256 | 64 B | 1.69 GB | ×3.3 |
| RSASHA256 | 256 B | 2.09 GB | ×4.1 |
| UOV-Ip-pkc | 128 B | 2.10 GB | ×4.1 |
| MAYO-2 | 186 B | 2.47 GB | ×4.8 |
| MAYO-1 | 454 B | 4.22 GB | ×8.3 |
| Falcon-512 | 666 B | 5.52 GB | ×10.8 |
| ML-DSA-44 | 2,420 B | 16.98 GB | ×33.2 |
| CROSS-R-SDP-1-small | 12,434 B | 88.66 GB | ×173.5 |
| SLH-DSA-SHA2-128f | 17,088 B | 112.48 GB | ×220.1 |
| P256+MAYO-2 | 250 B | 2.95 GB | ×5.8 |
| P256+Falcon-512 | 730 B | 6.00 GB | ×11.7 |
| Falcon-512/MAYO-2 | 186 B | 2.47 GB | ×4.8 |
| Falcon-512/UOV-Ip-pkc | 128 B | 2.10 GB | ×4.1 |
| SLH-DSA-128f/UOV-Ip-pkc | 128 B | 2.10 GB | ×4.1 |
| SLH-DSA-128f/Falcon-512 | 666 B | 5.52 GB | ×10.8 |
| SLH-DSA-128f/ML-DSA-44 | 2,420 B | 16.98 GB | ×33.2 |
| ML-DSA-44/UOV-Ip-pkc | 128 B | 2.10 GB | ×4.1 |
| CROSS/Falcon-512 | 666 B | 5.52 GB | ×10.8 |
| CROSS/MAYO-2 | 186 B | 2.47 GB | ×4.8 |

### 6.2 Security Considerations

Our approach relies on NIST-standardized algorithms (ML-DSA, SLH-DSA, FN-DSA) and Round 2 candidates (MAYO, UOV) that have undergone extensive cryptanalytic evaluation. We follow NIST, and international, recommendations for post-quantum transition, including the use of direct signature concatenation for hybrid PQ/T schemes. Should any candidate algorithm be broken before standardization, it would naturally be excluded from deployment.

The use of different signature algorithms at distinct hierarchy levels has already been used in prior work on hierarchical PKI [9]. The DNSSEC trust model requires that both KSK and ZSK signatures verify correctly; an attacker cannot force acceptance of a weaker algorithm without compromising the entire chain. Differentiation does not introduce new downgrade attack vectors: resolvers validate the complete chain regardless of which algorithms are used at each level.

Combining algorithms from different cryptographic families (such as, hash-based KSK with multivariate ZSK) provides defense-in-depth. A cryptanalytic breakthrough against one family would not compromise zones using differentiated configurations with algorithms from unaffected families. This diversity improves the resilience of the overall security posture.

### 6.3 Algorithm Rollover

RFC 6781 defines procedures for algorithm rollovers in DNSSEC, and our differentiated approach remains fully compatible with these established practices. Operators can rotate ZSK independently without modifying the KSK, and vice versa. This independence actually provides *more* flexibility

Table 8. Configuration summary across evaluation dimensions. Latency, verification, and storage relative to ECDSAP256SHA256 (×1.0). Values below 1.0 indicate faster verification. Undifferentiated UOV-Ip-pkc fails due to protocol limits (Section 5.2). †Classical verification path; quantum path achieves ×0.62 (P256+MAYO-2) and ×0.99 (P256+Falcon-512).

| **Configuration** | **A record size** (Section 5.2) | **Truncations** (Section 5.3) | **Latency** (Section 5.4) | **Verification** (Section 5.5) | **Storage** (Section 5.6) |
|---|---|---|---|---|---|
| *Classical (baseline)* | | | | | |
| ECDSAP256SHA256 | 263 B | 0 | ×1.00 | 1.00 | ×1.0 |
| *Undifferentiated post-quantum* | | | | | |
| MAYO-2 | 385 B | 3 | ×1.26 | **0.58** | ×1.5 |
| Falcon-512 | 856 B | 3 | ×1.59 | 0.96 | ×3.3 |
| ML-DSA-44 | 2,645 B | 22 | ×2.56 | 1.72 | ×10.0 |
| CROSS-R-SDP-1-small | 12,579 B | 36 | ×2.82 | 19.1 | ×52.5 |
| SLH-DSA-128f | 17,247 B | 22 | ×3.19 | 24.3 | ×66.5 |
| UOV-Ip-pkc | 327 B | — | — | 1.40 | ×1.2 |
| *Hybrid PQ/T* | | | | | |
| P256+MAYO-2 | 458 B | 3 | ×1.27 | 1.02† | ×1.7 |
| P256+Falcon-512 | 924 B | 3 | ×1.59 | 1.17† | ×3.6 |
| *Differentiated KSK/ZSK* | | | | | |
| Falcon-512/MAYO-2 | 385 B | 3 | ×1.28 | 0.55 | ×1.5 |
| Falcon-512/UOV-Ip-pkc | 327 B | 3 | ×1.49 | 1.16 | ×1.2 |
| ML-DSA-44/UOV-Ip-pkc | 327 B | 3 | ×1.52 | 1.16 | ×1.2 |
| SLH-DSA-128f/Falcon-512 | 854 B | 3 | ×1.71 | 0.95 | ×3.3 |
| SLH-DSA-128f/UOV-Ip-pkc | 327 B | 3 | ×1.52 | 1.16 | ×1.2 |
| CROSS/Falcon-512 | 843 B | 3 | ×1.62 | 0.93 | ×3.3 |
| CROSS/MAYO-2 | 373 B | 3 | ×1.41 | **0.53** | ×1.5 |

than undifferentiated deployment, where changing the algorithm requires rotating both keys simultaneously.

A potential concern is tight coupling between KSK and ZSK sizes: if a ZSK algorithm is broken, can operators rotate to a backup without exceeding protocol limits? Our analysis shows this remains feasible. For example, SLH-DSA-128f as KSK (7,856 B signature) combined with Falcon-512 as emergency backup ZSK (897 B key + 666 B signature) totals under 10 KB, well within the 64 KB limit. Even the largest practical KSK leaves ample room for alternative ZSK algorithms.

Emergency rotation scenarios benefit from differentiation: if UOV is compromised, operators rotate only the ZSK to Falcon-512 or MAYO-2 without touching the KSK trust anchor. This localized response minimizes coordination overhead with parent zone operators, who must update DS records only during KSK rollovers.

### 6.4 Orthogonality with Others Approaches

Differentiated algorithm selection addresses a distinct layer of the post-quantum DNSSEC challenge compared to transport-layer optimizations. TurboDNS [27] reduces TCP fallback latency via DNS-over-QUIC with 0-RTT; ARRF [15] fragments large records across multiple exchanges; MTL mode [14] condenses signatures using Merkle trees. These approaches optimize *how* post-quantum data is transmitted, whereas differentiation optimizes *which* algorithms are selected for each role.

These strategies are orthogonal, still complementary. Operators could deploy TurboDNS for transport optimization while using differentiated PQC selection for cryptographic flexibility. The combination would yield both reduced fallback latency (from TurboDNS) and minimized response sizes (from differentiation). Similarly, MTL mode could compress signatures generated by differentiated configurations.

A key distinction is deployment complexity. Transport-layer approaches require changes at both authoritative servers and resolvers: TurboDNS requires QUIC support, ARRF requires RRFRAG parsing, and SL-DNSSEC requires per-nameserver state. Differentiation requires signing only software changes on the authoritative side, while remaining fully transparent to existing resolvers. This asymmetry favors differentiation for initial deployment, with transport optimizations added incrementally as resolver support matures.

### 6.5 Reproducibility

To facilitate reproducibility and further research, we release the complete experimental infrastructure as open source. The main experimental framework, including the containerized testbed configuration, is available at: **https://gitlab.lre.epita.fr/hugomayer57/project_dnssec_pqc** In addition, we provide a modified version of the `ldns` library [24], supporting post-quantum and hybrid PQ/T signatures. This implementation is available in our fork, specifically in the `optimizations-pqc` branch: **https://gitlab.lre.epita.fr/hugomayer57/ldns/-/tree/optimizations-pqc?ref_type=heads**

### 6.6 Future Works

Our experimental methodology relies on a containerized testbed simulating DNS hierarchy rather than measurements on production infrastructure. While this approach ensures reproducibility and isolates cryptographic performance from confounding factors, it does not capture all operational realities. Production DNS deployments involve caching at multiple levels, anycast routing, varying client populations, and heterogeneous network conditions. The 20 ms ± 5 ms latency profile reflects typical broadband connectivity but may not represent mobile networks, satellite links, or enterprise environments with different characteristics.

The zone signing benchmarks use a 1,000-domain dataset extrapolated from AFNIC statistics. Although this dataset reflects realistic record type distributions, TLD-scale zones with millions of domains may exhibit different performance profiles due to memory pressure, disk I/O patterns, and parallelization opportunities not captured in our single-threaded measurements.

Our hybrid PQ/T implementation concatenates signatures within a single RRSIG record, maintaining compatibility with existing resolvers that ignore unknown trailing data. This approach differs from proposals requiring separate RRSIG records per algorithm, which would necessitate resolver modifications. The tradeoffs between these approaches, backward compatibility versus explicit dual validation, merit further investigation as the ecosystem matures.

### 6.7 Concluding Remarks

Post-quantum DNSSEC migration presents challenges distinct from other protocol transitions. The size constraints imposed by UDP transport and the 64 KB DNS message limit create hard boundaries that implementation optimization cannot overcome. Our work demonstrates that these limits need not dictate undifferentiated algorithm choice across all cryptographic roles.

Differentiated KSK/ZSK selection, grounded in the operational asymmetry that RFC 6781 documents but prior work has not exploited, expands the viable algorithm space. By decoupling key roles, differentiation enables algorithms that undifferentiated constraints prohibit: UOV-Ip-pkc becomes

deployable as ZSK despite its 43 KB keys, SLH-DSA-128f becomes practical as KSK despite its 8-minute signing time. The SLH-DSA-128f/UOV-Ip-pkc configuration exemplifies this approach, combining two otherwise excluded algorithms to achieve both hash-based trust anchor security and minimum response overhead.

## Acknowledgments

The authors thank David Bessara for providing access to his hardware, which enabled signing performance evaluation on large-scale zones. The authors also thank the reviewers of AsiaCCS for their valuable comments and suggestions, which helped improve the first version of this paper.

## A Testbed Network Architecture

Figure 8 details the query/response flow during DNS resolution in our testbed environment.

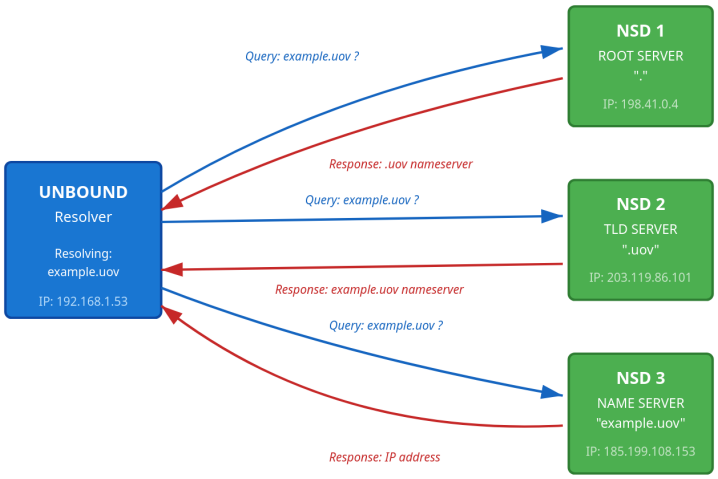



Fig. 8. Testbed network architecture. The Unbound resolver queries three NSD authoritative servers following the standard delegation chain: root (.), TLD (.uov), and leaf domain (example.uov). Each exchange is captured via `tcpdump` for packet and latency analysis.

## References

[1] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. 2005. DNS security introduction and requirements. RFC 4033. (Mar. 2005). doi:10.17487/RFC4033.

[2] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. 2005. Protocol modifications for the DNS security extensions. RFC 4035. (Mar. 2005). doi:10.17487/RFC4035.

[3] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. 2005. Resource records for the DNS security extensions. RFC 4034. (Mar. 2005). doi:10.17487/RFC4034.

[4] Abdullah Aydeger, Nicholas Saputro, and Kemal Akkaya. 2025. DoPQT: DNS over post-quantum TLS. *Infocommunications Journal*, 17, 3, 2–10. doi:10.36244/ICJ.2025.3.2.

[5] Gijs Jan Beernink. 2022. *Taking the Quantum Leap: Preparing DNSSEC for Post Quantum Cryptography*. Master's thesis. University of Twente. https://essay.utwente.nl/89509/.

[6] Ward Beullens. 2022. Breaking Rainbow takes a weekend on a laptop. Presented at CRYPTO 2022. (2022). arXiv: 2206.02879.

[7] Ward Beullens, Fabio Campos, Sofía Celi, Basil Hess, and Matthias J. Kannwischer. 2024. MAYO: practical post-quantum signatures from oil-and-vinegar maps. NIST Additional Digital Signatures Round 2 Submission. (2024). https://pqmayo.org/.

[8] Ward Beullens, Andreas Hülsing, Tanja Lange, and Lorenz Panny. 2024. UOV: unbalanced oil and vinegar digital signature scheme. NIST Additional Digital Signatures Round 2 Submission. (2024).

[9] Nina Bindel, Udyani Herath, Matthew McKague, and Douglas Stebila. 2017. Transitioning to a quantum-resistant public key infrastructure. In *Post-Quantum Cryptography (PQCrypto)*. doi:10.1007/978-3-319-59879-6_22.

[10] Flo D, Michael P, and Britta Hale. 2025. Terminology for Post-Quantum Traditional Hybrid Schemes. RFC 9794. (June 2025). doi:10.17487/RFC9794.

[11] J. Damas, M. Graff, and P. Vixie. 2013. Extension mechanisms for DNS (EDNS(0)). RFC 6891. (Apr. 2013). doi:10.17487/RFC6891.

[12] DNS Flag Day. 2020. DNS flag day 2020: TCP and EDNS buffer size. Accessed: 2024-12-01. (2020). https://dnsflagday.net/2020/.

[13] R. Elz and R. Bush. 1997. Clarifications to the DNS specification. RFC 2181. (July 1997). doi:10.17487/RFC2181.

[14] Andrew Fregly, Joseph Harvey, Burt Kaliski, and Swapneel Sheth. 2022. Merkle tree ladder mode: reducing the size impact of NIST post-quantum signature algorithms in practice. Cryptology ePrint Archive, Paper 2022/1730. (2022). https://eprint.iacr.org/2022/1730.

[15] Jason Goertzen and Douglas Stebila. 2022. Post-quantum signatures in DNSSEC via request-based fragmentation. (2022). https://arxiv.org/abs/2211.14196 arXiv: 2211.14196.

[16] O. Kolkman, W. Mekking, and R. Gieben. 2012. DNSSEC operational practices, version 2. RFC 6781. (Dec. 2012). doi:10.17487/RFC6781.

[17] Nathan McGowan and Douglas Stebila. 2025. Security analysis of ARRF for post-quantum DNSSEC. In *Proceedings of the 2025 ACM Asia Conference on Computer and Communications Security (ASIA CCS)*. doi:10.1145/3701716.3715585.

[18] P. Mockapetris. 1987. Domain names - implementation and specification. RFC 1035. (Nov. 1987). doi:10.17487/RFC1035.

[19] Moritz Müller, Jins de Jong, Maran van Heesch, Benno Overeinder, and Roland van Rijswijk-Deij. 2020. Retrofitting post-quantum cryptography in internet protocols: a case study of DNSSEC. In *ACM SIGCOMM Computer Communication Review* number 4. Vol. 50, 49–57. doi:10.1145/3431832.3431838.

[20] National Institute of Standards and Technology. 2023. Call for additional digital signature schemes for the post-quantum cryptography standardization process. Accessed: 2024-12-01. (2023). https://csrc.nist.gov/projects/pqc-dig-sig.

[21] National Institute of Standards and Technology. 2024. FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA). Federal Information Processing Standards Publication. NIST, (Aug. 2024). doi:10.6028/NIST.FIPS.204.

[22] National Institute of Standards and Technology. 2024. FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA). Federal Information Processing Standards Publication. NIST, (Aug. 2024). doi:10.6028/NIST.FIPS.205.

[23] National Institute of Standards and Technology. 2024. FIPS 206: FFT (Fast-Fourier Transform) over NTRU-Lattice-Based Digital Signature Standard (FN-DSA). Federal Information Processing Standards Publication. Draft. NIST, (Nov. 2024).

[24] NLnet Labs. 2024. ldns: DNS programming library. (2024). https://nlnetlabs.nl/projects/ldns/about/.

[25] PQShield. 2024. Post-quantum signatures zoo. (2024). https://pqshield.github.io/nist-sigs-zoo/.

[26] Aditya Rawat and Mahabir Prasad Jhanwar. 2024. SL-DNSSEC: signatureless DNSSEC using post-quantum key encapsulation. Cryptology ePrint Archive, Paper 2024/1319. (2024). https://eprint.iacr.org/2024/1319.

[27] Aditya Rawat and Mahabir Prasad Jhanwar. 2024. TurboDNS: post-quantum DNSSEC with faster TCP fallbacks. In *Progress in Cryptology – INDOCRYPT 2024*, 212–236. doi:10.1007/978-3-031-80311-6_11.

[28] SIDN Labs. 2025. Post-quantum DNSSEC: algorithm evaluation for TLD deployment. Technical Report. (2025).

[29] P. Wouters and O. Sury. 2019. Algorithm implementation requirements and usage guidance for DNSSEC. RFC 8624. (June 2019). doi:10.17487/RFC8624.