

Post-Quantum Diversity for DNSSEC: Routine Performance, Resilient Fallback

Taejoong (tijay) Chung¹ Joe Harvey² Burt Kaliski² Daniel McVicker²

Benno Overeinder³ Swapneel Sheth² Ondřej Surý⁴

¹Virginia Tech

²Verisign Labs

³NLnetLabs

⁴ISC

August 25, 2025

Abstract

We advocate for a post-quantum cryptography strategy for DNSSEC that includes two types of algorithms: a *conservatively designed algorithm* that is unlikely ever to need to be replaced, and a *low-impact drop-in algorithm* that is used the same way as a traditional signature algorithm. The conservatively designed algorithm would be used in a *mode of operation* that mitigates the operational impact of a large signature size. The combination provides both the *routine performance* of the low-impact algorithm and a *resilient fallback* to the conservatively designed choice. We detail our strategy for DNSSEC and outline next steps for testing it.

1 Introduction

The Domain Name System Security Extensions (DNSSEC)^{1,2,3} introduced in 2005, provide data origin authentication for DNS resource records. Like most other authentication applications, DNSSEC currently uses digital signature algorithms that are at risk of compromise by a cryptanalytically relevant quantum computer. Accordingly, DNSSEC deployments need to be migrated to post-quantum cryptography (PQC). However, the PQC signature algorithms that are currently standardized (e.g., ML-DSA in FIPS 204⁴ and SLH-DSA in FIPS 205⁵) have large signature sizes relative to the constraints of the DNS protocol. If used as

¹ Arends, R., Austein, R., Larson, M., et al. *Resource Records for the DNS Security Extensions*. IETF RFC 4034, Mar. 2005. <https://www.rfc-editor.org/info/rfc4034>

² Arends, R., Austein, R., Larson, M., et al. *Protocol Modifications for the DNS Security Extensions*. IETF RFC 4035, Mar. 2005. <https://www.rfc-editor.org/info/rfc4035>

³ Hoffman, P. *DNS Security Extensions (DNSSEC)*. IETF RFC 9364, Feb. 2023. <https://www.rfc-editor.org/info/rfc9364>

⁴ NIST. *FIPS 204: Module-Lattice-Based Digital Signature Standard*. Aug. 13, 2024. <https://doi.org/10.6028/NIST.FIPS.204>

⁵ NIST. *FIPS 205: Stateless Hash-Based Digital Signature Standard*. Aug. 13, 2024. <https://doi.org/10.6028/NIST.FIPS.205>

is, these algorithms will introduce operational risk to DNS. These factors have motivated research into PQC for DNSSEC.⁶

NIST's "onramp" call for additional PQC signature algorithms⁷ intends to standardize algorithms with smaller signature sizes. Such algorithms would be attractive for constrained use cases such as DNSSEC. However, some of the algorithms will likely be based on newer cryptographic assumptions. This introduces the long-term cryptographic risk, albeit with a low probability, that one of the new algorithms may eventually need to be replaced, or that its key and/or signature size may need to be increased, potentially reducing its operational benefit.

Given the importance of stability for a global, decentralized system such as DNSSEC, we advocate for an algorithm diversity strategy where there is a practical path to deploy *any* current or future standardized PQC signature algorithm in DNSSEC. Moreover, we recommend that when DNSSEC migrates to PQC, two diverse types of PQC signature algorithms be deployed at any point in time:

1. At least one *conservatively designed algorithm* integrated into DNSSEC using a "mode of operation" that ensures its operational impact is good enough for practical use; and
2. At least one *low-impact drop-in algorithm* integrated into DNSSEC as is.

The combination would provide DNSSEC with both *routine performance* — the resource efficiency of the low-impact algorithm — and a *resilient fallback* — the cryptographic confidence of the conservatively designed choice. As long as the security assumptions about the low-impact algorithm hold, DNSSEC enjoys the simplicity of a drop-in replacement. But if those assumptions ever become in question and a new low-impact algorithm needs to be rolled out, DNSSEC would already have a tested alternative in place to smooth the transition.

Our current recommendation for the conservatively designed algorithm is SLH-DSA in Merkle Tree Ladder (MTL) mode.^{8,9} NIST's "onramp" for additional PQC signature algorithms is in progress, and no algorithms with smaller signatures have been standardized yet. Therefore, we don't yet have a recommendation for the low-impact algorithm.

This paper is organized as follows. Section 2 summarizes the challenges for the DNSSEC use case of post-quantum cryptography. Sections 3 and 4 detail our recommended PQC algorithm diversity strategy for DNSSEC and how we propose to achieve it. Section 5 outlines next steps for testing the strategy to see if it can deliver the routine performance and resilient fallback that PQC DNSSEC calls for.

⁶ Fregly, A.M., van Rijswijk-Deij, R., Müller, M., et al. *Research Agenda for a Post-Quantum DNSSEC*. Internet-Draft, Sept. 23, 2023 (latest revision Dec. 23, 2024). <https://datatracker.ietf.org/doc/draft-fregly-research-agenda-for-pqc-dnssec/>

⁷ NIST. *Post-Quantum Cryptography: Additional Digital Signature Schemes*. <https://csrc.nist.gov/projects/pqc-dig-sig>, accessed June 16, 2025

⁸ Fregly, A., Harvey, J., Kaliski, B. and Sheth, S. Merkle Tree Ladder Mode: Reducing the Size Impact of NIST PQC Signature Algorithms in Practice. In Rosulek, M., ed., *Topics in Cryptology – CT-RSA 2023*, pp. 415–441. Springer, 2023. https://link.springer.com/chapter/10.1007/978-3-031-30872-7_16. Extended version available at <https://eprint.iacr.org/2022/1730>

⁹ Fregly, A.M., Harvey, J., Kaliski, B., and Wessels, D. *Stateless Hash-Based Signatures in Merkle Tree Ladder Mode (SLH-DSA-MTL) for DNSSEC*. Internet-Draft, Dec. 19, 2023 (latest revision Apr. 2, 2025). <https://datatracker.ietf.org/doc/draft-fregly-dnsop-slh-dsa-mtl-dnssec/>

2 Post-Quantum DNSSEC Challenges

NIST identified several use cases for the use of PQC in its call for algorithms in 2016.¹⁰ Among them, DNSSEC faces two main challenges, both related to DNS's role as the global internet infrastructure protocol for name resolution.

The first challenge is *operational constraints*. The DNS protocol is run primarily over the User Datagram Protocol (UDP).¹¹ While UDP can support packets of up to 65,535 bytes in principle, a typical practical limit in DNS implementations is 1232 bytes. That limit, conveniently, is compatible with the signature sizes for traditional signature algorithms deployed in DNSSEC. In particular, the signature size for RSASHA256¹² is typically 128 to 256 bytes (1024 to 2048 bits); the signature size for ECDSA256SHA256¹³ is 64 bytes. In comparison, the signature sizes for the currently standardized PQC signature algorithms are 2420 to 4627 bytes for ML-DSA and 7856 to 49,856 bytes for SLH-DSA. (The signature size for Falcon, which NIST also intends to standardize, is 666 to 1280 bytes.¹⁴)

The comparison of packet size to signature size understates the challenge. In ordinary operations, a DNS response can in some cases include up to three signatures (an NSEC3 “non-existence” response¹⁵). During key rollovers, a DNS response may include signatures under both a previous and a new key — a consideration that can push beyond the UDP limit even with traditional signature algorithms, depending on what else is in the response. DNS implementations are designed to retry their requests over the Transmission Control Protocol (TCP)¹⁶ when the UDP limit is reached. But to manage the operational burden on the most critical exchanges within the DNS ecosystem, it is preferable to keep most of the traffic over UDP when possible.

A recent study showed that the DNS message size increase because of the larger signature size in the Falcon-512 case resulted in TCP protocol fallback, which negatively affected DNSSEC-validating DNS resolver performance. The DNS message size increase because of larger public keys produces minimal performance impact for algorithms in the study¹⁷ that included Falcon and several other proposed PQC signature algorithms (HAWK-256⁷, HAWK-512⁷, MAYO⁷, and ANTRAG-512¹⁸).

¹⁰ NIST. *Post-Quantum Cryptography Call for Proposals*. Jan. 3, 2017 (updated May 12, 2025).

<https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals>, accessed June 16, 2025

¹¹ Postel, J. *User Datagram Protocol*. IETF RFC 768, Aug. 1980. <https://www.rfc-editor.org/info/rfc768>

¹² Jansen, J. *Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC*. IETF RFC 5702, Oct. 2009. <https://www.rfc-editor.org/info/rfc5702>

¹³ Hoffman, P. and Wijngaards, W.C.A. *Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC*. IETF RFC 6605, April 2012. <https://www.rfc-editor.org/info/rfc6605>

¹⁴ Alagic, G., Apon, D., Cooper, D., et al. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST IR 8413-upd1, July 2022 (updated Sept. 26, 2022). <https://doi.org/10.6028/NIST.IR.8413-upd1>

¹⁵ Laurie, B., Sisson, G., Arends, R., and Blacka, D. *DNS Security (DNSSEC) Hashed Authenticated Denial of Existence*. IETF RFC 5155, March 2008. <https://www.rfc-editor.org/info/rfc5155>

¹⁶ Eddy, W., ed. *Transmission Control Protocol (TCP)*. IETF RFC 9293, Aug. 2022. <https://www.rfc-editor.org/info/rfc9293>

¹⁷ Surý, O. *Feasibility of the new Post Quantum Cryptography for DNSSEC*. Master's Thesis, University of Ostrava, June 2025. <https://portal.osu.cz/wps/portal/dipl?urlid=prohlizeni-prace-detail&praceldno=64457>

¹⁸ Espitau, T., Nguyen, T., Sun, C., Tibouchi, M., Wallet, A. *Antrag: Annular NTRU Trapdoor Generation*. *Cryptology ePrint Archive*, Paper 2023/1335. <https://eprint.iacr.org/2023/1335>

Another consideration is computational cost. As internet applications rely on the proper function of the DNS protocol, any slowdown in DNS resolution caused by the cryptographic algorithm used in DNSSEC can add delays to protocols using domain names. Particularly, in the case of SQIsign¹⁹, one of the submissions in the call for additional PQC signature algorithms, both the public key and signature sizes may be favorable for DNSSEC, but in one study¹⁷, the cost of signature verification reduced the number of DNS queries that could be resolved in under 1 millisecond by 5% delaying the function of the DNS system when a test version of the DNS root zone was signed with SQIsign.

The second challenge is *deployment cycles*. While the DNS protocol is standardized, DNS implementations are highly decentralized. DNS protocol upgrades and DNSSEC algorithm changes can take years to reach broad deployment.

Authentication use cases like DNSSEC have been positioned as a lower priority for PQC migration use cases than confidentiality use cases, which are subject to “harvest now / decrypt later” attacks. Both challenges counter that prioritization. DNSSEC may require more time than other use cases both for determining how to apply PQC signature algorithms effectively given the operational constraints and to deploy a solution.

3 Our Proposed PQC Algorithm Diversity Strategy

One approach for addressing the operational constraints is to wait until NIST’s onramp effort concludes, anticipating the availability of one or more additional signature algorithms more suitable for DNSSEC in terms of signature size.

That approach may work, but it also brings several risks.

First, the effort might not produce any DNSSEC-suitable algorithms at all. NIST’s PQC project had 20 signature algorithm submissions; only three made it into standards (one still being prepared). A size constraint could narrow the success probability even further.

Second, the effort might produce only one DNSSEC-suitable algorithm, leaving no immediate backup if the cryptographic confidence in the algorithm were later to come into question — a possibility given the novelty of the algorithms involved.

Third, the effort might produce two or more DNSSEC-suitable algorithms — a “best case” scenario — but the market for hardware and software implementations of these algorithms might be limited compared to conservatively designed signature algorithms. If vendor support for the algorithms is limited, maintaining operational readiness for DNSSEC key-signing ceremonies may be difficult.

Because of these risks, we advocate for an approach where while waiting for a low-impact algorithm, the DNS community *finds a way to deploy the currently standardized PQC algorithms* while mitigating their operational impact.

Our rationale is straightforward: the more standardized algorithms that can potentially be deployed with DNSSEC, the more flexibility the DNS community will have for managing DNSSEC in the long term.

¹⁹ <https://sqisign.org>

Anticipating the availability of a broader range of PQC signature algorithms, we envision a post-quantum diversity strategy for DNSSEC that involves at least one algorithm from two sets with complementary properties:

- at least one *conservatively designed algorithm* whose security is based on a long-established cryptographic assumption, but whose signature size may be relatively long; and
- at least one *low-impact drop-in algorithm* whose security may be based on a novel cryptographic assumption, but whose signature size is relatively short.

The low-impact algorithm would be used as is. The conservatively designed algorithm, on the other hand, would be used in a mode of operation that reduces its operational impact (see Section 4 below).

The advantage of the conservatively designed algorithm is that it is unlikely ever to need to be replaced, providing a *resilient fallback* in case the security of the other algorithm is in question.

The advantage of the low-impact drop-in algorithm is that it is used the same way as a traditional signature algorithm, delivering *routine performance*.

As is the case for DNSSEC today, though implementations would support multiple signature algorithms, DNS operators could choose which supported algorithm to use to sign a particular zone.²⁰ Different algorithms may be appropriate for the root zone, a top-level domain (TLD) zone, and other zones.

The combination of both types of algorithms brings a further advantage. With the conservatively designed algorithm in place, the low-impact algorithm doesn't need as much cryptographic confidence as if its backup were another low-impact algorithm that is also based on a novel cryptographic assumption. Indeed, the presence of a resilient fallback based on a long-established cryptographic assumption makes it reasonable to entertain low-impact algorithms that are based on even more novel assumptions — but also deliver even better routine performance.

4 Finding a Way – Alternatives and Considerations

We have selected SLH-DSA for the conservatively designed algorithm in our prototypes because its security is based on hash function security in various forms, which has a long history. However, we are open to considering ML-DSA (perhaps in a composite mode with a traditional algorithm as contemplated by the IETF LAMPS working group²¹) as well as Falcon. We are also open to HSS-LMS and XMSS[^]MT, recommended in NIST SP 800-208,²² but appreciate that state management introduces an operational risk that may be too much for some implementations. As stated earlier, we do not yet have a recommendation for the low-impact algorithm.

²⁰ Wouters, P., and Sury, O. *Algorithm Implementation Requirements and Usage Guidance for DNSSEC*. IETF RFC 8624, June 2019. <https://www.rfc-editor.org/info/rfc8624>

²¹ Ounsworth, M., Gray, J., Pala, M., et al. *Composite ML-DSA for use in X.509 Public Key Infrastructure*. Internet-Draft, Mar. 18, 2019 (latest revision June 16, 2025). <https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/>

²² NIST SP 800-208: *Recommendation for Stateful Hash-Based Signature Schemes*. Oct. 2020. <https://doi.org/10.6028/NIST.SP.800-208>

Given our selection of SLH-DSA as the conservatively designed algorithm, our strategy is critically dependent on the goal stated above: finding a way to deploy currently standardized PQC algorithms — the ones with long signature sizes — within the operational constraints of the DNS protocol.

There have been some efforts to relax the constraints. For instance, encrypted DNS (e.g., DNS-over-HTTPS²³) has become the norm for communications between DNS clients and resolvers. Such transports can readily accommodate long DNSSEC signatures. A move to new transports for the most critical part of DNS — communications between resolvers and root / top-level domain servers — is less certain, however, due to the importance of uninterrupted global availability for these exchanges.²⁴

Moreover, even if DNS deployments could accommodate a 10 to 100-fold increase in signature sizes compared to traditional signature algorithms, the overhead would be well out of proportion to the small size of the DNS resource records being protected.

An alternative to relaxing the constraints is to change how signature algorithms are deployed. This difference in perspective was the motivation for Verisign’s research into Merkle Tree Ladder (MTL) mode, which provides a way to deploy signature algorithms with long signature sizes while largely operating within DNSSEC’s operational constraints. (Verisign announced²⁵ a public, royalty-free license to Merkle Tree Ladder mode in 2023.)

In MTL mode, rather than signing each message individually, an evolving Merkle tree forest is formed from a series of messages being authenticated. Selected nodes of the forest — called a “ladder” in MTL mode terminology — are signed with the underlying PQC signature algorithm. The MTL mode “signature” on the message is the Merkle tree inclusion proof for the message, which can be relatively short. The inclusion proof is verified in conjunction with the ladder and its underlying PQC signature, which is distributed separately.

Although the underlying PQC signature may still be relatively long, because the same underlying signature can authenticate multiple messages, it only needs to be distributed and verified occasionally. The operational impact of the long signature size is therefore amortized across a potentially large message series — a good match to the DNSSEC use case, where a potentially large “zone” of DNSSEC resource record sets is protected with a given key.

5 Recommended Next Steps

Over the past several years, Verisign has been drawing attention to the DNSSEC use case for PQC at standards meetings and conferences. We have published an Internet-Draft⁹ on how to apply SLH-DSA-

²³ Hoffman, P. and McManus, M. *DNS Queries over HTTPS (DoH)*. IETF RFC 8484, Oct. 2018. <https://www.rfc-editor.org/info/rfc8484>

²⁴ Kaliski, B. *A Balanced DNS Information Protection Strategy: Minimize at Root and TLD, Encrypt When Needed Elsewhere*. Verisign blog, Dec. 7, 2020. <https://blog.verisign.com/security/a-balanced-dns-information-protection-strategy-minimize-at-root-and-tld-encrypt-when-needed-elsewhere/>

²⁵ Kaliski, B. *Next Steps in Preparing for Post-Quantum DNSSEC*. Verisign blog, July 20, 2023. <https://blog.verisign.com/security/post-quantum-dnssec-preparation/>

MTL mode to DNSSEC and an open-source implementation of the draft.^{26,27} We have also hosted several IETF hackathons to test performance and interoperability of the implementation.

Exploring how to integrate onramp candidates and other signature algorithms into DNSSEC is an active area of research.^{28,29,30,31,32, 33,34,35} The IETF has also established a mailing list, pq-dnssec@ietf.org,³⁶ for discussions of research in this area. Participants have gathered several times at IETF meetings to review their progress.

The PQC DNSSEC hackathon at IETF 123³⁷, in July 2025, brought together several open-source resolvers implementing conservative and low-impact PQC drop-in algorithms to facilitate further evaluation and measurement. The POC implementations in Bind, NSD³⁸, and Core-DNS³⁹ now support ML-DSA, FN-DSA, SLH-DSA, SLH-DSA with MTL mode, MAYO, SQIsign, Hawk, and SNOVA. Bind also supports ANTRAG-512. These implementations will be instrumental to further measurement studies and operational research including at the IETF-124 hackathon in November 2025.

The recent KeyTrap attack⁴⁰ on DNSSEC highlights the vulnerability of DNS resolvers to resource-exhausting interactions with malicious authoritative name servers. In the KeyTrap attack, a malicious

²⁶ verisign/MTL. <https://github.com/verisign/MTL>, accessed June 16, 2025

²⁷ verisign/mtl-mode-ldns. <https://github.com/verisign/mtl-mode-ldns>, accessed June 16, 2025

²⁸ Müller, M., de Jong, J., van Heesch, M., et al. *Retrofitting post-quantum cryptography in internet protocols: a case study of DNSSEC*. In *ACM SIGCOMM Computer Communication Review*, 50(4), pp. 49–57. ACM, 2022. <https://dl.acm.org/doi/abs/10.1145/3431832.3431838> 2020

²⁹ Beernink, G.J. *Taking the Quantum Leap: Preparing DNSSEC for Post Quantum Cryptography*. Thesis, University of Twente, 2022. <https://essay.utwente.nl/89509/>

³⁰ Goertzen, J. *Enabling Post-Quantum Signatures in DNSSEC: One ARRF at a time*. Thesis, University of Waterloo, 2022. <https://dspacemainprd01.lib.uwaterloo.ca/server/api/core/bitstreams/f1f2ae4d-358c-4257-b2fb-211f01011a8e/content>

³¹ Rawat, A.S. and Jhanwar, M.P. Post-quantum DNSSEC over UDP via QNAME-Based Fragmentation. In *Security, Privacy, and Applied Cryptography Engineering (SPACE 2023)*. Springer, 2023. https://link.springer.com/chapter/10.1007/978-3-031-51583-5_4

³² Raavi, M., Wuthier, S., and Chang, S.-Y. Securing Post-Quantum DNSSEC Against Fragmentation Mis-Association Threat. In *ICC 2024 - IEEE International Conference on Communications*. IEEE, June 2024. <https://ieeexplore.ieee.org/abstract/document/10622607>

³³ Goertzen, J., Melchor, C.A., Huque, S., et al. *Field Experiments on Post-Quantum DNSSEC*. Presented at RWC 2025, March 2025. <https://pub.sandboxaq.com/publications/field-experiments-on-post-quantum-dnssec>, accessed June 16, 2025

³⁴ Schutijser, C., Koning, R., Lastdrager, E. and Hesselman, C. Evaluating Post-Quantum Cryptography in DNSSEC Signing for Top-Level Domain Operators. In *2025 IEEE/IFIP Network Traffic Measurement and Analysis Conference (TMA 2025)*. Preprint available at <https://www.sidnlabs.nl/downloads/1dhFbUOVFLvHC0Zsf9C1p/e1228adb6943353d052b59294456df77/tma2025-pqc.pdf>, accessed June 16, 2025

³⁵ Surý, O. *Feasibility of the new Post Quantum Cryptography for DNSSEC*. Thesis, University of Ostrava, 2025. Preprint available at <https://typst.app/project/rJ0w6uUpoHWo6Pjd1fbUx6>, accessed June 16, 2025

³⁶ PQ DNSSEC Research. Wiki page, pq-dnssec@ietf.org mailing list. <https://wiki.ietf.org/en/group/pq-dnssec>, accessed June 16, 2025

³⁷ <https://wiki.ietf.org/en/meeting/123/hackathon#pqc-dnssec-algorithms-and-non-existence-responses>

³⁸ <https://github.com/NLnetLabs/nsd/pull/397> with signing via LDNS <https://github.com/verisign/mtl-mode-ldns>

³⁹ https://github.com/fjblanco/mtl_coredns_plugin

⁴⁰ Heftrig, E., Schulmann, H., Vogel, N. and Waidner, M. The Harder You Try, The Harder You Fail: The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC. In Kirda, E., and Lie, D., eds., *CCS '24: Proceedings of*

server responds to a DNS resolver’s query with a large number of DNSSEC signatures, each of which appears to have been signed by one of a large number of similarly identified public keys. Given such a large set of signatures and keys, an unaware resolver would try every combination looking for a valid signature — a quadratic amplification of response size into compute cost. An adversary can trigger the attack simply by asking the resolver to query the malicious server.

One of the authors previously observed that MTL mode is potentially subject to a related resource-exhaustion attack.⁴¹ In this attack, the malicious name server responds to a DNS resolver’s query for a DNSSEC record with a MTL mode inclusion proof that references a new Merkle tree ladder. Because the ladder is new, the resolver would then query for the associated signed ladder — contradicting the design goal that the ladders and their long underlying PQC signatures are only distributed and verified occasionally.

Analyzing such attacks and assessing potential countermeasures will be a focus of upcoming research, just as is already being done for KeyTrap.⁴² In particular, we expect that these attack considerations will play an important role in establishing best practices for DNS operators who sign DNS records using a conservatively designed algorithm in MTL mode.

Given a better understanding of the operational impact of a broad range of PQC signature algorithms on DNSSEC, including attacks and countermeasures, the DNS community can then proceed to selecting specific algorithms for future use.

6 Conclusion

The applications of digital signatures that need to be migrated to PQC algorithms — NIST’s original call for proposals listed “TLS, SSH, IKE, IPsec, and DNSSEC” as examples, and there are many others — present diverse environments for integrating PQC signature algorithms. For some, any standardized PQC signature algorithm can in principle be used as a drop-in replacement. For others, it may only be practical to use a low-impact algorithm, e.g., only an algorithm with a small signature size.

DNSSEC falls between the two extremes because signatures are applied to a *series* of messages, making it possible to amortize the operational impact of a long signature. As a result, it’s reasonable to aim for a goal where any standardized PQC signature algorithm can be integrated into DNSSEC in principle, perhaps combined with a mode of operation that mitigates its operational impact. The flexibility provided by a range of algorithms leads to our diversity strategy: PQC DNSSEC should support a conservatively designed algorithm and a low-impact drop-in algorithm.

We recognize that testing this strategy might show that the operational impact of a long signature size can’t be mitigated effectively. Indeed, even within the DNSSEC use case, there are situations where the overhead of the long signature size would remain problematic, including signatures on DNSKEY records

the 2024 on ACM SIGSAC Conference on Computer and Communications Security, pp. 497–510. ACM, Dec. 9, 2024. <https://dl.acm.org/doi/abs/10.1145/3658644.3670389>

⁴¹ Sury, O. Re: *Stateless Hash-Based Signatures in Merkle Tree Ladder Mode (SLH-DSA-MTL) for DNSSEC*. dnsop@ietf.org mailing list, July 17, 2024.

<https://mailarchive.ietf.org/arch/msg/dnsop/RwZaviMFpJec4OSV4xZV852YCQY/>

⁴² Heftrig, E., Schulmann, H., Vogel, N. and Waidner, M. Protocol Fixes for KeyTrap Vulnerabilities. In *ANRW '24: Proceedings of the 2024 Applied Networking Research Workshop*, pp. 74–80. ACM, July 20, 2024. <https://dl.acm.org/doi/abs/10.1145/3673422.3674902>

(because there's only one DNSKEY record set at a given time to amortize the overhead across for a zone; only nine at a time if we take the ceremonial pre-signing of multiple key sets into account⁴³), and signatures on “dynamic” records computed in response to a DNS query. But for the thousands of regular signed DNS records in the root zone, and the millions of in a typical TLD zone, impact reduction may well be possible, thus motivating our research.

In 2023, ICANN requested comments on a draft study on future DNSSEC root zone algorithm rollovers.⁴⁴ As Verisign pointed out in its comments,⁴⁵ PQC migration would become an important consideration in the future timeline for DNSSEC algorithm rollovers (internal footnotes omitted):

- *Draft recommendation 26 proposes a timeline for the algorithm rollover “following the second KSK rollover, in approximately five years”— or around 2028–2029. Meanwhile, the timeline for the US government’s migration to post-quantum algorithms includes dates as early as 2035. Accordingly, with root zone KSK rollovers planned at five-year intervals, the second root zone algorithm rollover in the mid-2030s may well involve the incorporation of post-quantum cryptography. That timeline means that while post-quantum DNSSEC is still long-term for deployment, it should be medium-term for standardization and thus short-term — now — for research and development.*

The timelines proposed in the draft NIST IR 8547⁴⁶ directly impact DNSSEC: 2048-bit RSASHA256 would be deprecated after 2030 and disallowed after 2035; ECDSA256SHA256 would be disallowed after 2035. Research, prototyping, and standardization of PQC DNSSEC over the next several years — with deployment to follow in the next decade — are therefore essential to the routine and resilient cryptographic future of this critical internet technology.

7 Acknowledgements

The authors would like to thank Andrew Fregly^{6,8,9} for his early contributions in promoting PQ DNSSEC and bringing the community together around the PQ DNSSEC research agenda⁶.

⁴³ RZ KSK PMA. *DNSSEC Practice Statement for the Root Zone KSK Operator*. 8th edition, Apr. 14, 2025.

<https://www.iana.org/dnssec/procedures/ksk-operator/ksk-dps-20250414.html>

⁴⁴ ICANN. *Draft Report of the Root Zone DNSSEC Algorithm Rollover Study*. Oct. 19, 2023.

<https://www.icann.org/en/public-comment/proceeding/draft-report-of-the-root-zone-dnssec-algorithm-rollover-study-19-10-2023>

⁴⁵ Kaliski, B. and Wessels, D. *Comments on ICANN’s Draft Report of the Root Zone DNSSEC Algorithm Rollover Study*.

Verisign, Dec. 4, 2023. <https://www.icann.org/en/public-comment/proceeding/draft-report-of-the-root-zone-dnssec-algorithm-rollover-study-19-10-2023/submissions/verisign-inc-04-12-2023>

⁴⁶ Moody, D., Perlner, R., Regenscheid, A., et al. *Transition to Post-Quantum Cryptography Standards*. NIST IR 8457 ipd, Nov. 2024. <https://doi.org/10.6028/NIST.IR.8547.ipd>

⁴⁶ Peters, J. *Impact of Merkle Tree Ladder (MTL) Mode Signatures on DNSSEC*. Jul. 6, 2025.

https://www.nlnetlabs.nl/downloads/publications/Jannik-Peters_rp2_mtl-mode-signatures-dnssec_2025-07-06.pdf