Network Working Group
Internet-Draft
Intended status: Informational
Expires: 19 October 2026

S. Sheth
Verisign Labs
T. Chung
Virginia Tech
B. Overeinder
NLnet Labs
17 April 2026

Post-Quantum Cryptography Strategy for DNSSEC
draft-sheth-pqc-dnssec-strategy-01

Abstract

This document proposes a post-quantum cryptography (PQC) strategy for Domain Name System Security (DNSSEC) that includes two types of algorithms: one or more conservatively designed algorithms that are unlikely ever to need to be replaced, and one or more low-impact drop-in algorithms that are used the same way as a traditional signature algorithm. The conservatively designed algorithms can 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. The draft outlines the strategy, provides recommendations for future testing and deployment, and highlights operational considerations in adopting PQC for DNSSEC.

Status of This Memo

Copyright Notice

Table of Contents

1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Introduction

DNSSEC [RFC4034][RFC4035][RFC9364] provides data origin authentication for DNS resource records. Current algorithms, such as RSASHA256 (8) and ECDSA (13), are vulnerable to cryptanalytically capable quantum computers. While "harvest now/decrypt later" is not a concern for DNSSEC, as it is for some other protocols such as TLS, "trust now/forge later" is a concern for DNSSEC. Ensuring that signatures are valid and secure from inception until expiration is critical. This combined with the fact that standards bodies like the

National Institute of Standards and Technology (NIST) are deprecating support for classical algorithms ensures that migration to post-quantum cryptography (PQC) is necessary. Large system operators are also publishing statements[Google-PQC][Cloudflare-PQC] encouraging full migration to PQC in the next four years. Unfortunately, migration with the large signature sizes introduce operational risks.

This draft proposes a strategy deploying:

* One or more conservatively designed PQC algorithm in a mode mitigating large signature sizes.
* One or more low-impact drop-in PQC algorithm analogous to traditional DNSSEC signatures.

This dual-algorithm approach ensures routine performance and resilient fallback during PQC transition.

This draft is intended as a contribution to ongoing algorithm updates and the algorithm lifecycle per drafts [I-D.ietf-dnsop-rfc8624-bis] and[I-D.crocker-dnsop-dnssec-algorithm-lifecycle]

3. Post-Quantum DNSSEC Challenges

3.1. Operational Constraints

DNS primarily runs over UDP, with packet sizes limited to a maximum of ~1232 bytes. Traditional signatures (e.g., RSASHA256, ECDSA) fit within this limit. PQC signatures (ML-DSA: 2420-4627 bytes, SLH-DSA: 7856-49856 bytes) exceed it, risking excessive TCP fallback, latency, and resolver performance degradation [Sury2025].

3.2. Deployment Cycles

DNSSEC upgrades occur over years. Novel PQC algorithms may face uncertain adoption timelines, requiring fallback mechanisms. Some algorithms (e.g., SQIsign) impose verification overhead, slowing response times [Sury2025].

4. Proposed PQC Algorithm Diversity Strategy

DNSSEC should deploy two types of PQC signature algorithms:

Currently standardized post-quantum secure algorithms that provide cryptographic confidence and resilient fallback. Examples: SLH-DSA in Merkle Tree Ladder (MTL) mode [I-D.harvey-cfrg-mtl-mode], Falcon[FALCON], XMSS[RFC8391], LMS[RFC8554].

New algorithms such as the ones that remain under NIST onramp evaluation or under consideration by other standards bodies. These provide routine performance with minimal operational impact. They may leverage newer but less well-established mathematical concepts. Examples: MAYO[MAYO], SNOVA[SNOVA].

4.1. Mode of Operation

MTL mode signs a Merkle tree ladder rather than individual DNS responses, amortizing signature size across multiple responses [Fregly2023]. In DNSSEC, this reduces operational impact while maintaining security[I-D.fregly-dnsop-slh-dsa-mtl-dnssec].

5. Alternatives and Considerations

* Conservative candidates: SLH-DSA, ML-DSA (possibly combined with traditional algorithms), Falcon, XMSS, LMS.
* Low-impact candidates: New algorithms such as the ones that remain under NIST onramp evaluation or under consideration by other standards bodies.
* Use of modes of operation (like MTL mode) to mitigate large signature sizes.

6. Recommended Next Steps

* Evaluate the impact of increased truncated responses and traffic over TCP on DNS recursive resolvers and authorities at all scales.
* Conduct hackathons testing multiple algorithms in BIND, NSD, and CoreDNS (see current progress in Section 7).
* Measure latency, fallback rates, and resilience under adversarial conditions, including KeyTrap-style attacks [HeBrig2024].
* Research countermeasures against denial-of-service risks for MTL mode.

7. Current Community Efforts

Several efforts are underway to implement, test, and discuss PQC algorithms in DNSSEC.

* IETF PQC DNSSEC Side Meeting - https://wiki.ietf.org/en/group/pq-dnssec
* IETF 123 Hackathon - PQC DNSSEC Implementation [HACAKTHON-123]
* IETF 122 Hackathon - PQC for DNSSEC - New Kids on the Block [HACAKTHON-122-NEW]
* IETF 122 Hackathon - PQC DNSSEC Metrics with MTL Mode [HACAKTHON-122-MTL]

8. IANA Considerations

This document makes no requests of IANA. Future work may include registration of new DNSSEC algorithm codes for PQC algorithms.

9. Security Considerations

The deployment of PQC algorithms strengthens DNSSEC against quantum attacks but introduces operational risks. Proper testing, fallback mechanisms, and mode-of-operation considerations are essential to avoid new vulnerabilities.

Continued community participation in PQC DNSSEC research, in particular around low-impact drop-in algorithms, is essential to standarizing secure PQC DNSSEC solutions. Additional considerations will be described based on continued analysis and feedback.

10. References

10.1. Normative References

[I-D.crocker-dnsop-dnssec-algorithm-lifecycle]
Crocker, S., Housley, R., and W. Hardaker, "Documenting and Managing DNSSEC Algorithm Lifecycles", Work in Progress, Internet-Draft, draft-crocker-dnsop-dnssec-algorithm-lifecycle-02, 2 November 2025, <https://datatracker.ietf.org/doc/html/draft-crocker-dnsop-dnssec-algorithm-lifecycle-02>.

[I-D.ietf-dnsop-rfc8624-bis]
Hardaker, W. and W. Kumari, "DNSSEC Cryptographic Algorithm Recommendation Update Process", Work in Progress, Internet-Draft, draft-ietf-dnsop-rfc8624-bis-13, 4 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-rfc8624-bis-13>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/info/rfc9364>.

10.2. Informative References

[Cloudflare-PQC] Westerbaan, B., "Cloudflare targets 2029 for full post-quantum security", 7 April 2026, <https://blog.cloudflare.com/post-quantum-roadmap/>.

[FALCON] Fouque, P., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., and Z. Zhang, "Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU", 10 January 2020, <https://falcon-sign.info/falcon.pdf>.

[Fregly2023] Fregly, A., Harvey, J., Kaliski, B., and S. Sheth, "Merkle Tree Ladder Mode: Reducing the Size Impact of NIST PQC Signature Algorithms in Practice", 2022, <https://eprint.iacr.org/2022/1730>.

[Google-PQC] Adkins, H. and S. Schmeig, "Quantum frontiers may be closer than they appear", 25 March 2026, <https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/>.

[HACAKTHON-122-MTL] Harvey, J. and S. Sheth, "IETF 122 - PQC DNSSEC Metrics with MTL Mode", 16 March 2025, <https://datatracker.ietf.org/meeting/122/materials/slides-122-hackathon-sessd-pqc-dnssec-metrics-with-mtl-mode-00>.

[HACAKTHON-122-NEW]
Sury, O., "PQC for DNSSEC - New Kids on the Block", 16 March 2025, <https://datatracker.ietf.org/meeting/122/materials/slides-122-hackathon-sessd-pqc4dnssec-00>.

[HACAKTHON-123]
Jimenez-Berenguel, A., Harvey, J., Blanco-Romero, J., Sheth, S., Sury, O., and W. Toorop, "IETF 123 - PQC DNSSEC Implementation", July 2025, <https://datatracker.ietf.org/meeting/123/materials/slides-123-hackathon-sessd-ietf-123-pqc-dnssec-implementation-00>.

[HeBrig2024]
Heftrig, E., Schulmann, H., Vogel, N., and M. Waidner, "The Harder You Try, The Harder You Fail: The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC", 2024, <https://arxiv.org/abs/2406.03133>.

[I-D.fregly-dnsop-slh-dsa-mtl-dnssec]
Fregly, A., Harvey, J., Kaliski, B., and D. Wessels, "Stateless Hash-Based Signatures in Merkle Tree Ladder Mode (SLH-DSA-MTL) for DNSSEC", Work in Progress, Internet-Draft, draft-fregly-dnsop-slh-dsa-mtl-dnssec-06, 30 March 2026, <https://datatracker.ietf.org/doc/html/draft-fregly-dnsop-slh-dsa-mtl-dnssec-06>.

[I-D.harvey-cfrg-mtl-mode]
Harvey, J., Kaliski, B., Fregly, A., Sheth, S., and D. McVicker, "Merkle Tree Ladder (MTL) Mode Signatures", Work in Progress, Internet-Draft, draft-harvey-cfrg-mtl-mode-09, 24 March 2026, <https://datatracker.ietf.org/doc/html/draft-harvey-cfrg-mtl-mode-09>.

[MAYO] Beullens, W., Campos, F., Celi, S., Hess, B., and M. Kannwischer, "MAYO", 5 February 2025, <https://pqmayo.org/assets/specs/mayo-round2.pdf>.

[RFC8391] Huelsing, A., Butin, D., Gazdag, S., Rijneveld, J., and A. Mohaisen, "XMSS: eXtended Merkle Signature Scheme", RFC 8391, DOI 10.17487/RFC8391, May 2018, <https://www.rfc-editor.org/info/rfc8391>.

[RFC8554] McGrew, D., Curcio, M., and S. Fluhrer, "Leighton-Micali Hash-Based Signatures", RFC 8554, DOI 10.17487/RFC8554, April 2019, <https://www.rfc-editor.org/info/rfc8554>.

[SNOVA] Wang, L., Chou, C., Ding, J., Kuan, Y., Leegwater, J., Li, M., Tseng, B., Tseng, P., and C. Wang, "SNOVA Proposal for NISTPQC: Additional Digital Signature Schemes", 25 January 2025, <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/snova-spec-round2-web.pdf>.

[Sury2025] Sury, O., "Feasibility of the new Post Quantum Cryptography for DNSSEC", 2025, <https://typst.app/project/rJ0w6uUpoHWo6Pjd1fbUx6>.

Acknowledgements

Thanks to Andrew Fregly for early contributions in promoting PQ DNSSEC and uniting the research community around a post-quantum research agenda.

Change Log

00: Initial draft of the document.

01: Update intro and next steps based on latest publications.

Authors' Addresses

Swapneel Sheth
Verisign Labs
12061 Bluemont Way
Reston, VA 20190
United States of America
Email: ssheth@verisign.com
URI: https://www.verisignlabs.com/

Taejoong Chung
Virginia Tech
220 Gilbert Street, RM 4303
Blacksburg, VA 24060
United States of America
Email: tijay@vt.edu
URI: https://www.vt.edu/

Benno Overeinder
NLnet Labs
Science Park 400
1098 XH Amsterdam
Netherlands

Email: benno@nlnetlabs.nl
URI: https://nlnetlabs.nl