

Post-quantum Cryptography for DNSSEC, a temporary view

Paul Hoffman

DNSOP Working Group interim meeting
October 2026

Many orthogonal considerations

- [draft-hoffman-pq-dnssec-considerations](#)
 - Standardization (NIST, non-NIST)
 - Speed of deployment
 - Size of records (keys, sigs, both)
 - CPU usage other than TCP (intensive signing, validating, both)
 - Changes needed to the DNS protocol (some algorithms require processing changes)
 - Likelihood of inclusion in HSMs (do they care about DNSSEC?)
 - Amount and assuredness of cryptanalysis (who to trust, after how long, ...)
- Opinions abound about the relative importance of each of these, and there may be other significant considerations

ML-DSA-44 (1)

- By far the most popular PQC signing algorithm for the web, secure email, and so on
 - Already widely deployed in these protocols
- Has an IANA number (18)
- Is already being deployed in some resolver, authoritative, and signing software

ML-DSA-44 (2)

- Standardization: NIST FIPS 204
- Speed of deployment: Doable
- Size of records: Sig=2420, Key=1312
- Other CPU usage: Moderately fast
- DNS protocol changes: No
- Inclusion in HSMs: Already there
- Assuredness: High due to intensive ongoing study

FN-DSA (1)

- Previously known as Falcon
- Has great interest in the DNSSEC community because the signatures do not cause TCP fallback
- Has interest in IoT world for similar reasons
- Originally required floating-point arithmetic for signing, but that has been changed to fixed-point (so it is now slower)
- NIST standardization process has been stalled, but was recently restarted
- Warnings about security of signing

FN-DSA (2)

- Standardization: Likely NIST FIPS 206 in the future (probably at least a year, maybe two)
- Speed of deployment: Doable if standardization happens quickly
- Size of records: Sig=666, Key=897
- Other CPU usage: Moderate
- DNS protocol changes: No
- Inclusion in HSMs: Maybe if it becomes important
- Assuredness: Medium high: some related protocols have weaknesses, signing can be tricky

SLH-DSA in MTL mode (1)

- MTL = Merkle Tree Ladder
- Based on Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), already standardized by NIST, plus a creative way to split the signatures into smaller pieces
- Many DNSSEC signatures would be small
- Signatures have two modes, condensed and full, so protocol changes are needed to get the full key without falling back to TCP
- Verisign has well-documented patents and licensing for the technology

SLH-DSA in MTL mode (2)

- Standardization: SLH-DSA is NIST FIPS 205
- Speed of deployment: Doable if DNS protocol changes can be standardized quickly
- Size of records: Sig=mixed, Key=mixed
- Other CPU usage: High
- DNS protocol changes: Yes
- Inclusion in HSMs: Maybe if it becomes important
- Assuredness: Incredibly high

Others (1)

- There are dozens of other signature algorithms being considered by NIST, China's Next-generation Commercial Cryptographic Algorithms Program (NGCC), and others
- Many of the proposals have very attractive properties for DNSSEC
- Many of the proposals have already been weakened by analysis