

Title: How Merkle Trees Can Help Address Post-Quantum DNSSEC and Other Challenges

Presenters: Joe Harvey, Andrew Kaizer, Burt Kaliski, and Swapneel Sheth, Verisign

Since 2005^{1,2,3}, the global DNS has been secured by digital signatures under a global root cryptographic trust anchor. These digital signatures, secured primarily by algorithms 8 (RSA/SHA-256⁴), 13 (ECDSA Curve P-256 with SHA-256⁵), and 15 (Ed25519⁶), have provided DNS resource record authentication with small signature sizes. These algorithms have also provided cryptographic diversity to ensure that operators can use what works best for their operations and have alternatives should any vulnerabilities be discovered.

Concerns about quantum computers and the power of Shor's algorithm make it necessary to migrate DNSSEC to new post-quantum cryptography (PQC). The algorithms that are currently standardized by NIST (ML-DSA in FIPS 204⁷ and SLH-DSA in FIPS 205⁸) have significant impacts on size and/or speed compared to the legacy algorithms. While the algorithms in NIST's additional PQC signature onramp⁹ are intended to improve the operational tradeoffs and may provide good alternatives in the future, many are based on newer cryptographic assumptions and would benefit from having resilient fallback¹⁰ (example: ML-DSA or SLH-DSA).

The FIPS 204 algorithm, ML-DSA-44, is a very popular NIST standard PQC algorithm. While the signing and verification performance of the algorithm are somewhat like the current classical algorithms, the algorithm is impactful regarding key and signature sizes. In testing environments¹¹, the signature sizes increase the signed zone by 11 times over algorithm 13 (ECDSAP256SHA256) (see Figure 1). This means that responses to queries will be much larger and that zone synchronization, such as zone transfer operations, will consume significantly more resources. Resolvers will need a lot more memory to load zones and high-performance caches will no longer fit in currently allocated memory. Caching resolvers will need to either allocate more resources for cache or will need to store significantly fewer records, which increases the response latency and increases the volume of queries issued by a recursive resolver.

¹ <https://datatracker.ietf.org/doc/rfc4033/>

² <https://datatracker.ietf.org/doc/rfc4034/>

³ <https://datatracker.ietf.org/doc/rfc4035/>

⁴ <https://www.rfc-editor.org/info/rfc5702/>

⁵ <https://datatracker.ietf.org/doc/rfc6605/>

⁶ <https://datatracker.ietf.org/doc/rfc8080/>

⁷ <https://csrc.nist.gov/pubs/fips/204/final>

⁸ <https://csrc.nist.gov/pubs/fips/205/final>

⁹ <https://csrc.nist.gov/projects/pqc-dig-sig>

¹⁰ <https://datatracker.ietf.org/doc/draft-sheth-pqc-dnssec-strategy/>

¹¹ <https://datatracker.ietf.org/doc/slides-126-hackathon-sessd-pqc-dnssec-mtl-benefits/>

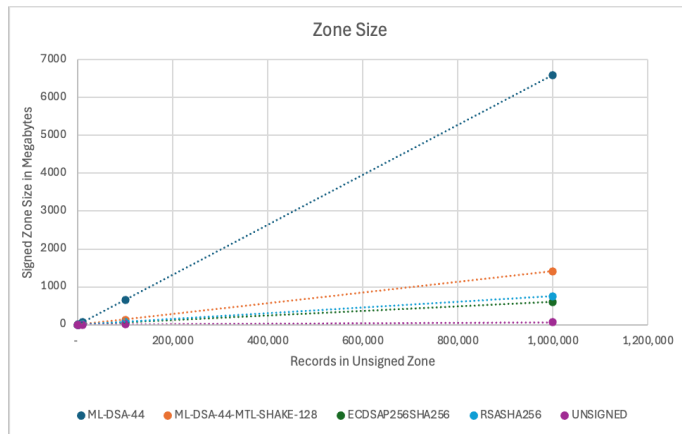


Figure 1 - DNS zone size by signing algorithm (from [11])

NIST's hash-based algorithm SLH-DSA (FIPS-205) has even larger signatures than ML-DSA and takes longer to perform cryptographic operations¹² — potentially orders of magnitude more.

As in other data authentication applications, Merkle Tree-based techniques can be used to amortize the size and performance impact of digital signature operations across large numbers of data elements. Testing of one such technique, Merkle Tree Ladder

(MTL)^{13,14}, has shown an orders-of-magnitude reduction in DNS zone size compared with ML-DSA signatures, compared to the conventional approach of one signature per DNS resource record set (RRset) (see Figure 1). The reason is that in MTL, the post-quantum signature algorithm is applied only to the root or to designated nodes of a Merkle tree; the signature on an individual RRset is a hash-based inclusion proof from the RRset to the root/designated nodes.

With the PQC transition timeframes that have been published, the internet community needs ways to use already standardized PQC signature algorithms. Merkle Tree-based techniques can help ensure the resilient and stable operations that the global DNS provides today as well as the ongoing operational effectiveness and security of other applications such as PKIs with Certificate Transparency¹⁵. By signing data structures representing multiple elements rather than signing each element individually, Merkle Tree-based techniques also represent a *new paradigm* for Internet authentication. Accordingly, the internet community also needs *architectural* guidance on how to design and deploy this paradigm as it moves ahead with post-quantum authentication including environmental impacts of internet applications and systems as discussed in RFC9547¹⁶.

¹² <https://pqshield.github.io/nist-sigs-zoo/>

¹³ <https://datatracker.ietf.org/doc/draft-kaizer-dnsop-ml-dsa-mtl-dnssec/02/>

¹⁴ <https://datatracker.ietf.org/doc/draft-hdong-dnsop-ml-dsa-mtl-dnssec-sigtag-ext/>

¹⁵ <https://datatracker.ietf.org/group/plants/about/>

¹⁶ <https://www.rfc-editor.org/info/rfc9547/>