Security and Performance Evaluation of Post-Quantum Signatures for DNSSEC

Stavros Kousidis

Master thesis · Published: 2026-10-15

Research question

How do selected post-quantum signature schemes and Merkle Tree Ladder constructions affect the security assumptions and operational performance of DNSSEC?

Description

Migrating DNSSEC to post-quantum cryptography requires more than replacing one signature algorithm. Signature and public-key sizes, zone-signing workloads, network response behavior, resolver compatibility and key management all influence feasibility. Proposed Merkle Tree Ladder (MTL) constructions introduce different authentication structures and assumptions that must be considered separately from the underlying signature algorithms.

You will investigate a small selection of candidate approaches against an established DNSSEC baseline. Relevant work includes IETF proposals for SLH-DSA-MTL and ML-DSA-MTL; compact signatures such as FN-DSA may provide another comparison point. Draft protocol formats must not be presented as deployed standards.

Scope and evaluation

Establish a reproducible zone-signing and verification test environment or, where an interoperable implementation is unavailable, a clearly delimited prototype or measurement model. Compare selected configurations in terms of signature and key size, zone storage, signing and verification costs, and DNS transport implications. State explicitly which security properties are inherited from the underlying signature scheme and which depend on the MTL construction or protocol integration.

Do not attempt to implement every candidate or claim production interoperability from prototype measurements. Choose the algorithms and tooling after a brief feasibility study.

Expected outcome

A comparative experimental study, an analysis of security and compatibility assumptions, and deployment recommendations qualified by the maturity of the evaluated mechanisms.

Starting points

- IETF: SLH-DSA-MTL for DNSSEC (work in progress).
- IETF: ML-DSA-MTL for DNSSEC (work in progress).
- DNSSEC protocol overview, RFC 4033.
- NIST FIPS 205, *Stateless Hash-Based Digital Signature Standard.*

Contact: stavros.kousidis@th-koeln.de
Code publication: open source by default; exceptions require prior agreement (policy).