Security and Migration Challenges of Post-Quantum Software Signing with Sigstore

Stavros Kousidis

Master thesis · Published: 2026-10-15

Research question

How can Sigstore's software-signing and verification infrastructure migrate to post-quantum mechanisms while preserving defined authenticity and verification guarantees during a transitional period?

Description

Sigstore's identity-based signing architecture combines multiple cryptographic roles: artifact signatures, certificate authorities, transparency logs, timestamps and distribution of verification trust roots. These components need not migrate simultaneously. A valid signature on an artifact is not sufficient if a verifier cannot establish an acceptable chain of trust or interpret its verification evidence.

In October 2026, the Sigstore project published a post-quantum migration direction. This thesis investigates one clearly defined transition scenario, treating announced plans as plans rather than deployed security guarantees.

Scope and evaluation

Select a small set of classical and post-quantum algorithm combinations, for example a classical signing mechanism and a candidate based on ML-DSA or SLH-DSA. Model the trust boundaries and compare verifier acceptance decisions when certificates, log evidence or trusted roots use different algorithm generations. Implement a limited verification prototype or test harness using locally generated artifacts and synthetic trust configurations.

Measure signature sizes, verification costs and compatibility where implementations permit. Investigate downgrade or migration-failure conditions under an explicit attacker model. Do not attempt a full replacement of Sigstore's public infrastructure.

Expected outcome

A documented threat and migration model, reproducible acceptance and rejection tests, and an analysis of which security properties survive a staged post-quantum transition.

Starting points

- Sigstore, *Post-Quantum Cryptography for Sigstore* (October 2026).
- Sigstore: Client architecture and verification.
- NIST FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA).
- The Update Framework specification.

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