Security and Implementation Trade-offs in MPC-in-the-Head Post-Quantum Signatures

Stavros Kousidis

Master thesis · Published: 2026-10-15

Research question

Which construction and implementation choices most strongly influence the efficiency and security assumptions of selected MPC-in-the-Head post-quantum signature schemes?

Description

MPC-in-the-Head (MPCitH) signatures use simulated multiparty computation and proof techniques to construct digital signatures. They should not be confused with protocols in which several real participants jointly generate a signature. Candidates such as MQOM and SDitH are being studied in NIST's additional post-quantum digital signature process.

You will investigate the design and implementation of two appropriately selected signature candidates. The goal is to explain measurable trade-offs and relate them to concrete construction decisions and published security arguments, rather than merely rank benchmark numbers.

Scope and evaluation

Reproduce a well-defined subset of the candidates' public reference measurements using controlled compiler options, platforms and parameter sets. Examine signing and verification time, memory requirements, key and signature sizes, and relevant implementation properties. Select one construction-level or implementation-level question for deeper analysis, such as parameter sensitivity, representation choices or timing behavior.

Any analysis of side-channel behavior must identify the observable leakage model and distinguish preliminary measurements from evidence of exploitable leakage. Establish the feasibility and stability of the available implementations before fixing the comparison.

Licensing note: Before selecting reference implementations, record their licenses and third-party notices. Distinguish independent benchmark tooling from modifications to the reference code, and respect applicable reuse and redistribution conditions. Publish reproducibility scripts under an agreed license; do not assume all reference implementations share one license.

Expected outcome

A reproducible comparison, an explanation of observed trade-offs grounded in the candidate designs, and a critical discussion of security claims, measurement limits and remaining questions.

Starting points

- NIST: Additional Post-Quantum Digital Signature Schemes.
- NIST: Round 3 Additional Signatures, including MQOM and SDitH.
- Ishai et al., *Zero-Knowledge from Secure Multiparty Computation* (STOC 2007).

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