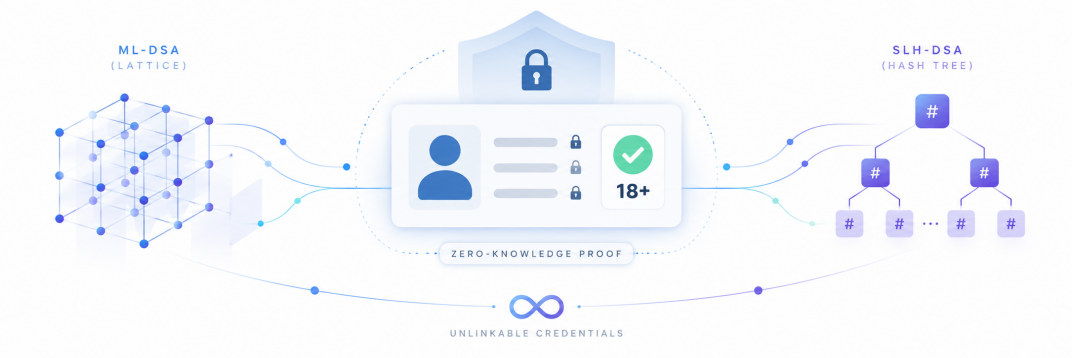
Anonymous Credentials from Post-Quantum Signatures



Anonymous Credentials (ACs) allow users to prove facts about themselves without revealing unnecessary personal information. Many efficient AC systems require credentials to be issued using special-purpose cryptographic signature schemes. This makes deployment difficult when credentials are already issued using conventional digital signatures.

Recent work, "Anonymous Credentials from ECDSA" (ePrint 2024/2010), takes a different approach. The issuer continues to use ordinary ECDSA signatures. Instead of changing the credential format, the holder uses zero-knowledge proofs to prove that they possess a valid ECDSA-signed credential and that selected statements about its contents are true. This makes it possible to add privacy to existing credential infrastructures without modifying the issuer.

Problem statement. With the transition to post-quantum (PQ) cryptography, signatures like ECDSA will be replaced by schemes such as NIST's ML-DSA (lattice-based) and SLH-DSA (hash-based). Can the same idea be applied to these new standardized signatures?

Can we efficiently prove in zero knowledge that we possess a valid, unmodified ML-DSA or SLH-DSA signature, and use this as the foundation for PQ anonymous credentials?

The challenge is performance. ML-DSA and SLH-DSA contain operations that can be expensive inside zero-knowledge proofs, including polynomial arithmetic, SHAKE/Keccak computations and, for SLH-DSA, large numbers of hash computations. Existing PQ AC proposals often modify the underlying signature scheme to make proving easier. In this thesis, we instead investigate whether standardized signatures can remain unchanged, following the philosophy of Longfellow.

Thesis goal. The student will first study Longfellow and existing approaches to PQ anonymous credentials. The main focus will then be ML-DSA, with SLH-DSA as an optional or comparative direction. The student will implement or adapt a zero-knowledge proof for standard ML-DSA signature verification, identify the computational bottlenecks, and investigate techniques for improving its performance. The implementation will be benchmarked in terms of proving time, verification time, memory consumption and proof size.

Keywords: Post-quantum, Anonymous credentials, Zero-knowledge proofs

Practicalities

Promotor:	Bart Preneel		
Daily supervisor:	Emad Heydari Beni	emad.heydaribeni@esat.kuleuven.be	office B01.34
	Omid Mirzamohammadi	omid.mirzamohammadi@esat.kuleuven.be	office B01.18
Nature of the work:	50% literature, 50% software		
Number of students:	1		

 © 2026 – 2027 COSIC