Research on hash-based quantum digital signature schemes

Khit Bounsaveng

Abstract: This thesis investigates the security and efficiency of hash-based quantum digital signature schemes, which are considered a leading candidate for post-quantum cryptography. As the advent of large-scale quantum computers threatens the security of classical public-key cryptosystems like RSA and ECDSA, hash-based signatures offer a robust alternative due to their reliance solely on the security of hash functions. The study provides a comprehensive analysis of foundational constructions, including the Lamport and Winternitz one-time signature schemes, and their extension to multi-signature frameworks via Merkle trees. We evaluate the trade-offs between signature size, key generation time, and computational overhead across different parameter sets. Furthermore, the thesis explores stateful versus stateless implementations and their practical implications for real-world deployment. Our findings demonstrate that while hash-based signatures provide strong security guarantees against quantum adversaries, their practical adoption requires careful optimization of key management and signature size. This research contributes to the ongoing standardization efforts by providing a detailed performance benchmark and security analysis for next-generation cryptographic infrastructures.

Keywords: quantum digital signatures, hash-based cryptography, post-quantum cryptography, quantum-resistant signatures