HSM backed post-quantum safe Hash-based Signature Service

Student

Florian Müller

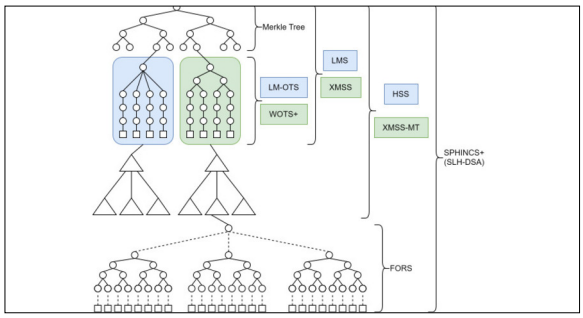
Introduction: The rapid advancement of quantum computing technology poses a significant threat to current cryptographic standards, as quantum algorithms have the potential to compromise widely used security protocols. To address this approaching challenge, the National Institute of Standards and Technology (NIST) has recommended and standardised several hash-based digital signature schemes, including the stateful Leighton-Micali Signature (LMS) and eXtended Merkle Signature Scheme (XMSS), as well as the stateless SPHINCS+ (SLH-DSA) scheme. These schemes offer promising solutions for achieving postquantum security across various applications since their only security assumption is based on the security of the underlying hash function.

This thesis provides a comprehensive exploration of hash-based digital signatures as viable post-quantum security mechanisms. The theoretical component addresses the fundamental concepts, and explains the progression from simple hash functions to fully developed digital signature schemes. This analysis covers the underlying principles and constructs that enable hash functions to ensure data integrity and authenticity in a quantum-resistant manner.

The practical contribution of this work involves the design and implementation of a cutting-edge hash-based signature service. This service leverages Hardware Security Modules (HSMs) for robust and secure management of private keys and execution of signature operations. The system is developed using C and Rust, chosen for its security features, performance and energy efficiency, and employs grpc to facilitate efficient and secure communication between components. The architecture effectively addresses the complexities associated with state management in stateful schemes like LMS and XMSS, ensuring scalability, efficiency, and enhanced security.

This study contributes to the field of post-quantum cryptography by providing both a detailed theoretical framework and a practical, implementable solution for quantum-safe digital signatures. The findings and developments presented herein advance the preparedness of cryptographic systems for a future dominated by quantum computing, ensuring continued data security and trust in digital communications.

Overview with the hash-based signatures schemes and their components
Own presentment



Advisor
Prof. René Pawlitzek

Subject Area
Computer Science