Research on post-quantum cryptography

Phonekeopaserth Soulivong

Abstract: This thesis investigates the practical implementation and security of post-quantum cryptography (PQC) in resource-constrained environments. As quantum computing advances threaten the security of classical public-key cryptosystems, the transition to quantum-resistant algorithms is imperative. This research focuses on the performance evaluation of selected PQC algorithms, including CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures, as standardized by NIST. Through comprehensive benchmarking on embedded devices and cloud servers, we analyze computational overhead, memory consumption, and communication bandwidth. The study further explores integration challenges within existing network protocols, specifically TLS 1.3, and proposes optimization strategies to mitigate latency and energy costs. Our findings reveal that while PQC algorithms impose a moderate performance penalty compared to classical counterparts, their feasibility is viable for most applications with careful parameter selection and hardware acceleration. This work contributes a practical framework for assessing PQC readiness and provides critical insights for system architects planning the migration to quantum-safe infrastructures.

Keywords: Post-quantum cryptography, lattice-based cryptography, code-based cryptography, multivariate cryptography