Graduate School of Science and Technology Master's Thesis Abstract

Laboratory name (Supervisor)	Cyber Resilience (Youki Kadobayashi (Professor))		
Student ID	2311406	Submission date	2025 / 1 / 20
Name	BORHAN ROWNAK		
Thesis title	Optimizing CRYSTALS-Dilithium: Enhancing Speed and Security for IoT in the Quantum Age		

Abstract

Quantum computing is on the verge of becoming a practical reality, offering unprecedented computational capabilities that could revolutionize various industries. However, this progress also poses a serious threat to the security of current cryptographic systems. To counter this risk, significant efforts have been made to develop quantum-resistant cryptographic standards. Among these, the National Institute of Standards and Technology (NIST) has recognized CRYSTALS-Dilithium, a lattice-based digital signature algorithm, as a leading candidate after an extensive standardization process. While notable strides have been made in enhancing computational efficiency, especially in polynomial multiplication, there has been comparatively little focus on optimizing the hashing process and addressing security issues within CRYSTALS-Dilithium's digital signature framework. This study proposes an innovative solution by replacing the SHAKE function in CRYSTALS-Dilithium with a hybrid approach combining IOSHA and AES, specifically designed for Internet of Things (IoT) applications. Leveraging dynamic parameters and a pseudorandom number-based IOSHA, this approach substantially enhances computational speed on ARM Cortex-M7 processors while offering improved security over SHAKE-256. The integration not only accelerates processing but also strengthens defenses while maintaining MLWE, MSIS, and SelfTargetMSIS, all without requiring any hardware upgrades.