Storozhko A.
Kibitkin S.
Vilkhivska O.
Pecherytsia D.
Andriushchenko T.

Enhancing LoRa Encryption with Post-Quantum Algorithms for IoT Security

Storozhko A. Enhancing LoRa Encryption with Post-Quantum Algorithms for IoT Security / A. Storozhko, S. Kibitkin, O. Vilkhivska et al. // 2025 IEEE 6th KhPI Week on Advanced Technology (KhPIWeek), 06-10 October 2025. – Kharkiv, Ukraine, 2025.

Abstract. The growing demand for secure, long-range wireless communication in the Internet of Things (IoT) has led to widespread adoption of LoRa technology. However, traditional LoRa implementations remain vulnerable to quantum computing attacks. This paper proposes the integration of post-quantum cryptographic algorithms, specifically Niederreiter encryption and LDPC codes, into LoRa systems to enhance their resilience. We explore the theoretical foundation of these algorithms, practical implementation strategies, and their impact on system performance. Experimental results and security analyses validate the feasibility of this approach, establishing a pathway for future-proof secure communication in LoRa-based IoT networks.

Keywords: LoRa, post-quantum cryptography, IoT security, LDPC, Niederreiter, ESP32, UTM mapping, wireless encryption.