Research on lightweight block ciphers for wireless sensor networks

Au The Linh

Abstract: This thesis investigates lightweight block ciphers tailored for resource-constrained Wireless Sensor Networks (WSNs). Given the inherent limitations in energy, memory, and processing power of sensor nodes, traditional cryptographic algorithms are often impractical. This research systematically evaluates the performance and security of several prominent lightweight block ciphers, including PRESENT, SPECK, and SIMON, within a simulated WSN environment. The study focuses on key metrics such as energy consumption, memory footprint, encryption speed, and resilience against common cryptanalytic attacks. Through comparative analysis, the thesis identifies optimal cipher configurations that balance robust security with minimal resource overhead. Furthermore, it proposes a novel, optimized implementation of a selected cipher that reduces power consumption by up to 15% compared to standard implementations, without compromising security. The findings provide a practical framework for selecting and deploying efficient cryptographic solutions, thereby enhancing data confidentiality and integrity in WSN applications such as environmental monitoring and smart infrastructure.

Keywords: Lightweight block cipher, Wireless sensor networks, IoT security, Energy-efficient cryptography