ECE 4301 Final Project Abstract

This project explores the benchmarking of lightweight cryptographic algorithms, focusing on Ascon, TinyJAMBU, and Xoodyak, on a MicroBlaze softcore processor programmed on a Nexys Artix7-100T FPGA board. Lightweight cryptography is increasingly vital for IoT and embedded systems due to their constraints on resources and power consumption. The study evaluates the algorithms' performance using key metrics such as encryption and decryption time, throughput, and estimated power consumption, with optimization and without (-os). Each lightweight cryptographic algorithm was tested with five cases: edge test, functional, performance 1KB, 1MB. Results highlight Ascon’s efficiency for larger inputs, TinyJAMBU’s advantages for constrained environments, and Xoodyak’s balanced performance across scenarios. Challenges faced, including hardware implementation errors and suboptimal algorithm behaviors, are discussed, along with recommendations for further testing and optimizations to enhance the reliability of lightweight cryptographic systems in embedded environments.