INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student	:	THOCKCHOM BIRJIT SINGHA
Roll Number	:	166102102
Programme of Study	:	Ph.D.

Thesis Title: Design and analysis of countermeasures for securing IoT edge devices against power analysis attacks

Name of Thesis Supervisor(s)	:	Prof. Roy Paily Palathinkal & Prof. Shaik Rafi Ahamed
Thesis Submitted to the Department/ Center	:	EEE
Date of completion of Thesis Viva-Voce Exam	:	02/09/2024
Key words for description of Thesis Work	:	Hardware security, IoT edge devices, AES, Side-channel attacks

SHORT ABSTRACT

IoT edge devices are plagued by power analysis attacks despite the usage of Advanced Encryption Standard (AES) as a part of securing information exchange. However, owing to the resource constraint environment offered by the IoT environment, an AES design consuming low resources with an embedded countermeasure providing high security ensuring minimal area and power overheads, is the need of the hour. This thesis presents four cumulative approaches in designing a countermeasure for AES to thwart the attacks. The first step is the wise choice of Masoleh S-box against other available S-boxes, providing minimal switching and enhanced nonlinearity. The second stride is by designing a novel Cipher Feed Back-64 mode inspired by the standard modes of AES operation. The third scheme is by splitting the SubBytes round operation into multiple clocks to reduce side-channel leakage. Finally, a novel expansion-compression Random Number Generator (RNG) assisted with buffer-based delay element is proposed to corrupt the meaningful samples of AES, acquired by the attacker. Analysis of hardware security metrics, like Measurements To Disclose (MTD), Signal-to-Noise Ratio (SNR), Mutual Information (MI) and Test Vector Leakage Assessment (TVLA) render this proposed four-dimensional approach to be highly resilient against the attacks, with minimal area and power overheads. The testing of the designs is performed for Application Specific Integrated Circuit (ASIC) using Synopsys and Cadence tools with UMC 65 nm technology node, and on Field Programmable Gate Array (FPGA) using Side-channel Attack Standard Evaluation BOard (SASEBO). Upon amalgamation of all the four works into one, the results showed negative area and power overheads of -2.91% and -5.61 %, respectively, when referenced with an AES design with LUT-based S-box, apart from being resilient to CPA attack with 1 million plaintexts. A compromise in throughput is incurred owing to the usage of excessive clocks, however satisfying the moderate-speed IoT applications.