INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student	:	Bhoopal Rao Gangadari
Roll Number	:	11610227
Programme of Study	:	Ph.D.

Thesis Title: Low Power VLSI Architectures for Cryptographic Algorithms.

Name of Thesis Supervisor(s)	:	Prof. Shaik Rafi Ahamed
Thesis Submitted to the Department/ Center	:	EEE
Date of completion of Thesis Viva-Voce Exam	:	30-07-2018
Key words for description of Thesis Work	:	Wireless Body Area Network (WBAN), Advanced Encryption Standard (AES), Very Large Scale Integration (VLSI).

SHORT ABSTRACT

With the advent of technology and portable devices for communications, cryptography algorithms are widely used in the modern days. Cryptographic algorithms have diverse applications to protect data from unauthorized attacks. This thesis proposes novel approaches for low power Very Large Scale Integrated Circuits (VLSI) architectures for Wireless Body Area Network (WBAN) cryptographic applications so as to improve the performance in terms of area utilization and energy consumption. Motivated by the fact that the present cryptographic algorithms consume high power and energy, there is need to develop low power architectures. Cryptography algorithms like Advanced Encryption Standard (AES), Camellia are widely used in RFID, secure communications, WBAN applications. The block cipher cryptographic algorithms like AES, Camellia are adopted in the latest WBAN standard IEEE 802.15.6 for cryptographic applications. The Substitution Box (S-Box) of these algorithms play a vital role in cryptography. The S-Box is realized using a standard polynomial equation and design is achieved using memory cells. These Look-Up-Table (LUT) based S-Boxes eventually occupy more area and hence consume high power, delay and energy. To overcome the limitation involved in the implementation of classical S-Box, in this thesis, we have proposed several efficient VLSI architectures for S-Box. This thesis investigates on the construction of S-Box using different irreducible polynomial equation. The S-Box can also be realized using Composite Field Arithmetic (CFA) which reduces hardware consumption and low power dissipation. This thesis then characterizes a special class of Cellular Automata (CA) based architectures for hardware implementation of S-Box. The special class of CA based S-Box for AES and Camellia algorithms are realized and implemented using CMOS technology libraries. In addition, we have also proposed hybrid linear cellular automata and hybrid second order reversible cellular automata based low energy/ power architecture for encryption algorithms. The last part of this thesis deals with the security analysis of the proposed architectures against cyber-attacks. We have carried out the security analysis on the proposed encryption algorithms using cryptographic properties such as Non Linearity, Strict Avalanche Criteria, Correlation Immunity Bias and entropy. Results show that the proposed architectures are efficient in terms of low power dissipation, low energy consumption and secure against any cryptographic attacks.