A HIGH PERFORMANCE AND AREA EFFICIENT VLSI ARCHITECTURE FOR PRESENT LIGHT WEIGHT CIPHER

A Project report submitted in partial fulfilment of the requirements for the award of degree of

BACHELOR OF TECHNOLOGY
IN
ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted by

P. Ramya	**Regd.No.18815A0410**
R. Srilaxmi	**Regd.No.17811A0444**
P. Sravani	**Regd.No.17811A0438**
G. Gowri Rajayalakshmi	**Regd.No.17811A0419**

Under the guidance of

T. Pattalu Naidu M.Tech, (Ph. D)

ASSISTANT PROFESSOR

AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF

ELECTRONICS AND COMMUNICATION ENGINEERING

(NAAC Accredited, Accredited by NBA, Approved by A.I.C.T.E,

Permanently Affiliated to J.N.T.U. KAKINADA

TAMARAM (P.O), MAKAVARAPALEM (M.O), NARSIPATNAM (R.D)
VISAKHAPATNAM DISTRICT-531113

2017-2021

AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY

(NAAC Accredited, Accredited by NBA, Approved by A.I.C.T.E, Permanently Affiliated to J.N.T.U. KAKINADA)

TAMARAM (P.O), MAKAVARAPALEM (M.O), NARSIPATNAM (R.D)
VISAKHAPATNAM DISTRICT-531113

DEPARTMENT OF

ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that the project entitled "A HIGH PERFORMANCE AND AREA EFFICIENT VLSI ARCHITECTURE FOR PRESENT LIGHT WEIGHT CIPHER" in partial fulfilment for the of degree of Bachelor of Technology in ELECTRONICS AND COMMUNICATION ENGINEERING, at AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY, MAKAVARAPALEM, VISAKHAPATNAM is an bonafied work carried out by P. RAMYA (18815A0410), R. SRI LAXMI(17811A0444), P.SRAVANI (17811A0438),G.GOWRI RAJYALAKSHMI (17811A0419) under the guidance and supervision during 2017-2021.

T.P.Naidu
PROJECT GUIDE
T. PATTALU NAIDU M.Tech, (Ph.D.)
Assistant professor

HEAD OF THE DEPARTMENT
Mr. E.GOVINDA, M.Tech. (Ph.D.)
Associate Professor

HEAD OF THE DEPARTMENT
DEPARTMENT OF ECE
Avanthi Institute of Engg.&Tech.
Makavarapalem, Visakhapatnam Dist-531 113.

EXTERNAL EXAMINER

Abstract

Security and privacy are of prime concern in the emerging internet of things (IOT) and cyber-physical systems (CPS) based applications. Lightweight cryptography plays an essential role in securing the data in this emerging pervasive computing environments. In this paper, we propose a high performance and area-efficient VLSI architecture with 64-bit data path for the PRESENT block cipher. The proposed architecture performs an integrated encryption/decryption operation for both 80-bit and 128-bit key lengths. The architecture is synthesized for the Virtex-5 XC5VLX110T FPGA device, available on the Xilinx ML-505 platform. It has been observed that the proposed architecture utilizes 0.73% and 0.87% of FPGA slices for 80-bit and 128-bit key lengths, respectively. A throughput of 410 Mbps and power consumption is about 16 mw for both the key lengths.