ATRIA INSTITUTE OF TECHNOLOGY

ASKB Campus, 1st Main Rd, AGS Colony, Anandnagar, Bengaluru,Karnataka 560024.

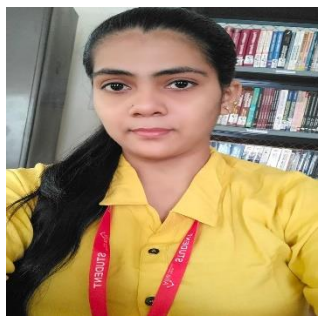
Department of Electronics & Communication Engineering

Title: Hardware Implementation of Present Cipher in FPGA

Mr. Akshay O
1AT19EC003
9844872508
akshayomanakuttan25@gmail.com

Mr. Arman Ali
1AT19EC010
9546188111
khanarmaan2510@gmail.com

Mr. Asutosh Jujare
1AT19EC034
8951961995
asutoshjujare18@gmail.com

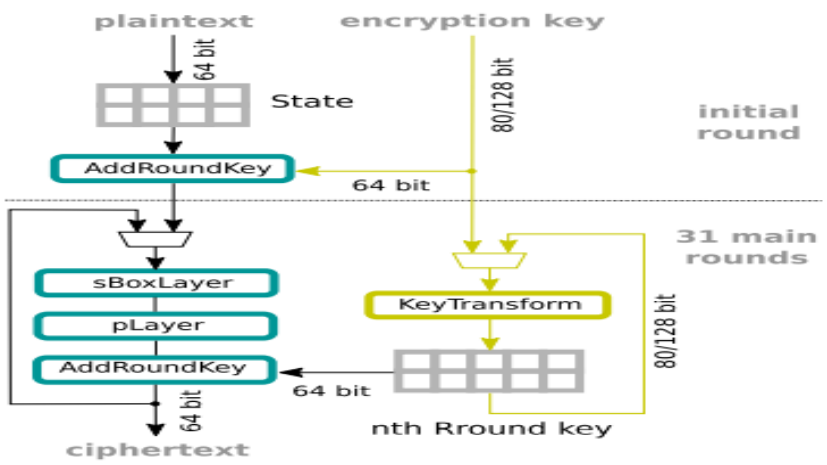


Miss. Jyoti Kumari
1AT19EC075
9262773580
jyotiatria2019@gmail.com

Project Guide:
Dr. Shipra Upadhyay
Associate Professor, Dept. of E&CE
Atria IT, Bengaluru

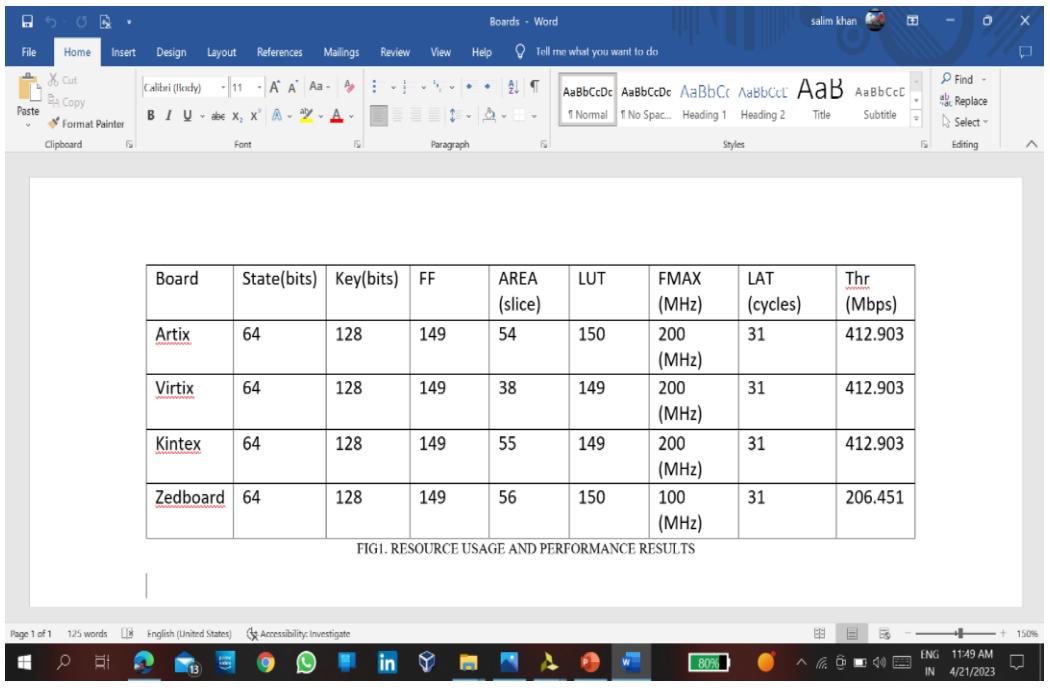
ABSTRACT: Our project is the, "Hardware Implementation of Present Cipher in FPGA for security Application" Literature survey of present Cipher based algorithm will be done and new designs will be implemented. A lightweight cipher intended for constrained applications. Several hardware implementations of PRESENT have been reported since its creation. In recent years, the study of lightweight symmetric ciphers has gained interest due to the increasing demand for security services in constrained computing environments, such as in the Internet of Things. However, when there are several algorithms to choose from and different implementation criteria and conditions, it becomes hard to select the most adequate security primitive for a specific application. This paper discusses the hardware implementations of PRESENT, a standardized lightweight cipher called to overcome part of the security issues in extremely constrained environments. The most representative realizations of this cipher are reviewed and two novel designs are presented. Using the same implementation conditions, the two new proposals and three state-of-the-art designs are evaluated and compared, using area, performance, energy, and efficiency as metrics. From this wide experimental evaluation, to the best of our knowledge, new records are obtained in terms of implementation size and energy consumption. In particular, our designs result to be adequate in regards to energy-per-bit and throughput-per-slice. It is mainly used digital signal processing for mostly security purposes.

METHODOLOGY & BLOCK DIGRAM:



FLOW CHART:

RESULT AND DISCUSSION: (With Images/Graphs)



Board	State(bits)	Key(bits)	FF	AREA (slice)	LUT	FMAX (MHz)	LAT (cycles)	Thr (Mbps)
Artix	64	128	149	54	150	200 (MHz)	31	412.903
Virtix	64	128	149	38	149	200 (MHz)	31	412.903
Kintex	64	128	149	55	149	200 (MHz)	31	412.903
Zedboard	64	128	149	56	150	100 (MHz)	31	206.451

FIG1. RESOURCE USAGE AND PERFORMANCE RESULTS

CONCLUSION & FUTURE SCOPE:

This paper presented a comparison of hardware architectures for the PRESENT cipher. Two alternatives have been studied to generate the round keys required by the algorithm. A 16-bit datapath architecture with 128-bit key schedule was presented and can be compared directly to relevant works in the literature. A 128-bit datapath architecture with 80-bit key schedule was developed for applications where an area/security trade-off can be established.