National Institute of Technology Rourkela

## Departmental Seminar

Seminar Title : Novel Hardware Architectures for PRESENT Block Cipher and its FPGA Realizations.

Speaker : Prof. Manish Okade

Supervisor : Prof M. Okade

Venue : EC-138

Date and Time : 15 Jan 2025 (05.30PM)

Abstract : The paper investigates novel hardware architectures for PRESENT Block Cipher with the motivation of its applicability to IoT applications. PRESENT has been chosen for two reasons: firstly, it belongs to the lightweight cipher category, and secondly, existing works haven’t fully focused their attention on power metric optimization of this cipher. The Substitution Permutation Network (SPN) module of PRESENT cipher is optimized by modifying its datapath and utilizing additional hardware units that significantly reduce power consumption and achieve high throughput. The novel aspect of the SPN module design is the input selection and feeding technique to the substitution and permutation layers via the hardware units comprising multiplexers. The optimized SPN module is then included in the overall encryption architecture of PRESENT for performance analysis. The proposed architectures have been evaluated on NEXYS4 DDR FPGA at an RFID operating frequency of 13.56 MHz, making them suitable for IoT applications. Additionally, the paper also throws light on how a designer can optimally harness the resources available in an FPGA architecture to achieve improvement in the performance of the cipher architecture. Comparative analysis with state-of-the-art shows dynamic power reduction by 28.57% and a reduction of 32.81% in the area for the proposed architectures. Besides, performance parameters like the throughput of the proposed design have been significantly improved while maintaining an optimized energy consumption when compared with state-of-the art architectures.