National Institute of Technology Rourkela

Departmental Seminar

Seminar Title	: A Security Framework for RISC-V SoC using Hardware Software Co-Design.
Speaker	: Bharat Patidar
Supervisor	: Prof A K Swain
Venue	: VLSI Lab - (EC-121)
Date and Time	: 01 Sep 2025 (11.30AM)
Abstract	: The open source nature of the RISC-V architecture has led to its rapid adoption across various computing domains, from embedded IoT devices to high-performance computing. However, this openness also introduces unique security chal lenges. The background study done in the paper highlights the ongoing works in the field of RISC-V vulnerabilities and counter measures, suggests the need for a security framework addressing key vulnerabilities. We identify cache-based side-channel attacks as a significant concern in current RISC-V implementations. A short description of ongoing research work and experimental setup of RISC-V is presented. We used FPGA ARTY A7-100 and CDAC RISC-V IP AT1051 for the SoC. The resource utilization was 76% of the total LUTs and 57% of BRAM. The SoC is hold violation free, where WHS is 0.013 ns. A security core AES IP was developed and tested. To enhance the security, the integration of the IP is planned as a future scope.