National Institute of Technology Rourkela

Departmental Seminar

Seminar Title	: Testing the Effect of Hardware Trojans: A Case Study
Speaker	: Shyamapada Mukherjee
Supervisor	: Sumanta Pyne , PIC, Seminar, CS Dept.
Venue	: New Conference Room (CS 323), CSE Dept.
Date and Time	: 09 Jan 2025 (17:30)
Abstract	: While outsourcing fabrication and integrating third party intellectual property has expedited IC development, it has also created substantial hardware attack surfaces, particularly Hardware Trojans (HTs). These harmful IC alterations, which are frequently hidden during design or production, present serious risks like data loss, illegal access, system malfunctions, and disastrous disruptions in vital industries like finance, health care, and defense. Due to their covert nature and dependence on uncommon circuit states, which are frequently outside the purview of conventional test sets, HT detection is difficult. Scalability, the lack of golden reference models in IP-based designs, and the adversary's capacity to target only subsets of ICs are the main drawbacks of the pre-silicon and post silicon verification techniques currently in use. Noise, ultra-small Trojan sensitivity, and variability in nanoscale processes impede advanced detection methods like side-channel analysis. This study investigates how a hardware Trojan affects a basic mathematical calculation running on a Basys3 FPGA board. When the Trojan is activated, the design which computes the square of a 4 bit binary number produces inaccurate results for particular inputs, highlighting the necessity of strong detection systems to guarantee IC security and dependability.