INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student	:	Syam Sankar
Roll Number	:	216101010
Programme of Study	:	Ph.D.

Thesis Title:
Enhancing Security Features of Network-on-Chip Using Lightweight Cryptosystem, Trust-Aware Routing, and Anonymous Communication

Name of Thesis Supervisor(s)	:	Dr. John Jose
Thesis Submitted to the Department/ Center	:	Computer Science and Engineering
Date of completion of Thesis Viva-Voce Exam	:	28. 01. 2025
Key words for description of Thesis Work	:	NoC Security, Hardware Trojans

SHORT ABSTRACT

Multi-Processor Systems-on-Chips (MPSoCs) combine multiple hardware Intellectual Property (IP) components on a single chip. Modern SoC vendors use 3rd-party IPs to develop in-house chips in order to reduce design costs and compete with time-to-market constraints. With the rising popularity of fabless manufacturing and agile development, the use of third-party IP for design is becoming more accepted. However, such practices can sometimes significantly compromise the security and reliability of SoC computing systems. Modern MPSoCs, or Tiled Chip Multi-Processors (TCMPs), employ multi-hop packet-based Network-on-Chip (NoC) as their communication backbone due to their low-latency, high-bandwidth, and scalable topology. Adversaries use NoC IP as a major platform to launch security attacks and degrade SoC performance due to its close proximity and location criticality with respect to inter-core communication. Malicious circuits, such as Hardware Trojans (HT), use NoC as a carrier to float attacks such as eavesdropping, application profiling, packet modification, Denial-of-Service (DoS), and so on. Since on-chip communication plays a critical role in determining the SoC's performance, any HT attacks targeting this communication may impact the smooth running of applications on the processor cores or may even leak sensitive SoC data to external adversaries. The thesis details three countermeasures to enhance the security features of on-chip communication using lightweight cryptosystem (Sec-NoC), trust-aware routing (TROP), and anonymous communication (SARON) against HT attacks. These three measures defend packet leakage, DoS due to packet alteration, and application profiling, respectively.