Date: 3rd June, 2024 (Monday)

Time: 4 pm to 5 pm

Venue: KD101, Department of CSE

Speaker: Rahul Chaurasia

Title: Designing secure and low-cost Hardware IPs for computationally intensive application frameworks

Abstract:

In large computing devices or systems, performing data intensive and computationally intensive tasks requires significant energy, resources, time and space. This is because, several applications require to perform computationally intensive tasks related to image, audio and video processing. For example, the convolution layer in CNNs and the JPEG codec in image processing are some of the frameworks that are computationally intensive. To speed up processing in such scenarios, hardware intellectual property (IP) is used. A hardware IP represents the unique set of instructions, architectures, and functionalities that define hardware behaviour, helping to achieve higher performance and efficiency by accelerating the underlying processes. Hardware IPs are also crucial in biomedical fields, robotics, IoT-based systems, autonomous vehicles, and various consumer electronics (CE) devices. This wide applicability creates a high demand for hardware IPs in the semiconductor industry, necessitating the development of such IPs. However, in today's rapidly evolving technological landscape, designing hardware IPs from scratch is not economically viable due to time to market pressure. Consequently, IPs are often imported from third-party design vendors, which may be untrustworthy. This involvement of third-party IP vendor/untrustworthy broker in the integrated circuit (IC) supply chain, makes them susceptible to various hardware threats. Therefore, it becomes crucial to not only having low-cost IP designs but also ensuring their robust and reliable hardware security measures. This is essential to safeguard not only the end consumer but also the authentic IP vendor and the system on chip (SoC) integrator against security threats such as reverse engineering, malicious backdoor Trojan insertion, IP piracy, and IP ownership abuse. Additionally, designing the hardware IPs from low level of abstraction is more complex than designing them at a higher level of abstraction. High level synthesis (HLS) provides an alternative to design hardware IPs, enabling the integration of modules for architectural optimization and robust security against hardware threats at low cost. We then show the design methodology for generating low-cost and secure hardware IPs for various domains such as digital signal processing (DSP), multimedia, healthcare, and machine learning (ML) etc.

Bio:

Rahul Chaurasia, received the Ph.D. degree in CSE from Indian Institute of Technology Indore, India, in August 2023. Currently, he is a post-doc in the Department of CSE at IIT Indore. His areas of research include hardware security, high-level synthesis, architectural optimization hardware acceleration and IP protection. For his contributions to the field, he received 'Young Scientist Award' by M.P. Council of Science and Technology (MPCST) in 38th M.P. Young Scientist Congress. He also received 'First Prize-Best Paper Award' in 2022 IEEE International Symposium on Smart Electronic Systems (IEEE – iSES), held at NIT Warangal, India.