Title: Securing Semiconductor IP Cores for DSP and multimedia applications

Speaker: Dr. Mahendra Rathore, postdoc candidate in the Department of Computer Science and Engineering and broadly interested in Hardware Security

Date and Time: 22nd March 2022 (Tuesday), 3:30 PM

Venue: Online

Abstract:

The security of semiconductor intellectual property (IP) cores can be challenged by a potential adversary in untrustworthy design houses and foundry (chip fabrication unit). An adversary in an untrustworthy system-on-chip (SoC) design house or foundry may steal the IP of genuine vendor and sell into the market claiming the IP as his/her own. This kind of threat is referred to as 'false claim of IP ownership' which may lead to huge revenue loss to the true IP vendor. Moreover, an adversary in the SoC design house may instantiate/clone the vendor's IP in his/her systems more number of times than specified in the licensing agreements. This results into IP cloning threat which may also lead to substantial revenue loss to the true IP vendor. Additionally, the design chain is also vulnerable to the threat of IP counterfeiting in which an IP broker can sell the fake or poor quality IPs to the SoC integrator under the brand name of any authentic IP vendor. This may inadvertently lead to the integration of fake components (pretending to be genuine) into the systems and hence not only ruins the authentic vendor's reputation but also impacts adversely the system functionality, performance and end users. The aforementioned hardware security threats can be handled using vendor's secret mark such as watermark that can be implanted into the IP cores during their design process. Furthermore, the hardware designs are also susceptible to the potential hardware Trojan insertion in untrustworthy houses. Structural obfuscation is a potential security mechanism to thwart the insertion of hardware Trojan. Our research work targeted the security of IP cores against the hardware threats of IP piracy, counterfeiting and hardware Trojan insertion. We mainly targeted the security of the IP cores used for executing DSP and multimedia applications. In our research works, novel methodologies of securing IP cores during the high level synthesis (HLS) phase of VLSI design process have been developed. The proposed techniques offer robust security at negligible design overhead, which highlights the practical consideration of our work.