Date: 12th August 2024

Time: 12 noon

Venue: KD102 (CSE building)

Title: Hardware IP Security

Abstract:

Logic locking is a technique designed to protect digital circuits from counterfeiting, piracy, and malicious modifications by concealing their functionality with a secret key bit-string. While initially effective, traditional logic locking has been compromised by sophisticated attacks, especially SAT-based methods that exploit vulnerabilities to recover the key and reveal the hidden functionality. We propose two defenses to thwart state-of-the-art attacks. First, we propose a functional synthesis-based logic locking approach called Structurally Robust Stripped Functionality Logic Locking (SR-SFLL). SR-SFLL addresses the vulnerabilities found in the SFLL technique, which, despite being robust against SAT attacks, remains susceptible to structural attacks. SR-SFLL is designed to withstand both SAT and structural attacks, offering enhanced security. Second, we introduce Higher Order Logic Locking (HOLL), which advances traditional logic locking methods by concealing the circuit functionality using a higher-order relation (using functional synthesis) instead of a simple key bit-string. This approach makes it more challenging for attackers to decipher the complex key relation, thereby reducing the effectiveness of existing attacks.

Speaker Bio:

Gourav Takhar is a PhD student at CSE, IIT Kanpur with a focus on synthesis for security and bug finding. He has published research on security in esteemed conferences such as TACAS, CAV, ASE, HOST, and ICCAD. He also got best paper award in ICCAD for his work in validating hyper-properties for system-on-chip designs. More recently, he is working on program verification, specifically in incorrectness logic. Additionally, Gourav has developed tools for learning program verification and testing.