HARDWARE SECURITY

PROF. DEBDEEP MUKHOPADHYAY
Department of Computer Science and Engineering
IIT Kharagpur

TYPE OF COURSE : Rerun | Elective | PG
COURSE DURATION : 12 Weeks (24 Jan' 22 - 15 Apr' 22)
EXAM DATE : 24 Apr 2022

PRE-REQUISITES : Cryptography

INTENDED AUDIENCE : Post-graduate students, and final year undergraduate students

INDUSTRIES APPLICABLE TO : TexasInstruments/BOSCH/DRDO/HAL/Wipro/CDAC/ISRO/Rambus/Intel/Qualcomm/Synopsys/IBM/Microsoft/Cadence/SecureIC/Riscure/Mentor Graphics/Xilinx/Nvidia

COURSE OUTLINE :

This course will focus on the importance of addressing different security threats on modern hardware design, manufacturing, installation, and operating practices. In particular, the threats would be shown to be relevant at scales ranging from a single user to an entire nation's public infrastructure. Through theoretical analyses and relevant practical world case studies, the threats would be demonstrated, and then state-of-the-art defense techniques would be described. The course would borrow concepts from diverse fields of study such as cryptography, hardware design, circuit testing, algorithms, and machine learning.

ABOUT INSTRUCTOR :

Prof. Debdeep Mukhopadhyay is currently a full Professor at the Department of Computer Science and Engineering, IIT-Kharagpur, India.At IIT Kharagpur he initiated the Secured Embedded Architecture Laboratory (SEAL), with a focus on Embedded Security and Side Channel Attacks([http://cse.iitkgp.ac.in/resgrp/seal/ | http://cse.iitkgp.ac.in/resgrp/seal/]) . Prior to this he worked asAssociate Professor at IIT Kharagpur, visiting scientist at NTU Singapore, a visiting Associate Professor of NYU-Shanghai, Assistant Professor atIIT-Madras, and as Visiting Researcher at NYU Tandon-School-of-Engineering, USA. He holds a PhD, an MS, and a B. Tech from IIT Kharagpur, India.

COURSE PLAN :

Week 1**:** Introduction, Finite Fields, AES Hardware, S-Box

Week 2**:** Algorithm to Hardware, Case Study on ECC, Intro to ECC

Week 3**:** Implementation of ECC, Hardware Design of ECC

Week 4**:** Introduction to Side Channel Analysis

Week 5**:** Advanced SCA, Introduction to Fault Attacks

Week 6**:** Advanced Fault Attacks, Algebraic Fault Analysis

Week 7**:** Countermeasures-I

Week 8**:** Countermeasures-II

Week 9**:** Introduction to PUFs, Designs on FPGAs, Machine Learning of PUFs

Week 10: Design-for-Testability for Cryptographic Designs

Week 11: Protocols, Challenges, Introduction to Micro-architectural attacks

Week 12: Advanced Micro-architectural attacks, Hardware monitoring for malwares using Hardware Performance Counters