Debayan Das received his PhD and MS in Electrical and Computer Engineering from Purdue University, USA, in 2021 and his Bachelor of Electronics and Telecommunication Engineering degree from Jadavpur University, India, in 2015.

He is an Assistant Professor with the Department of Electronic Systems Engineering (DESE) at the Indian Institute of Science (IISc), Bangalore. He has worked as a Security Researcher at Intel, USA, during 2021-22 and as a Research Scientist in the Intel Labs, USA, during 2022-23. Before his Ph.D., he worked as an Analog Design Engineer at a startup based in India. He has interned with the Security Research Lab, Intel Labs, USA, over the summers of 2018 and 2020. His research interests include mixed-signal IC design, biomedical circuits, and hardware security.

Dr. Das received the IEEE HOST Best Student Paper Award in 2017 and 2019, IEEE CICC Best Student Paper Award in 2021, the Third Best Poster Award in IEEE HOST 2018, and the 2nd Best Demo Award in HOST 2020. In 2019, one of his papers was recognized as a Top Pick in Hardware and Embedded Security. He was recognized as the winner (third place) of the ACM ICCAD 2020 Student Research Competition (SRC). During his Ph.D., he was awarded the ECE Fellowship during 2016–2018, the Bilsland Dissertation Fellowship in 2020–2021, the SSCS Pre-doctoral Achievement Award in 2021, and the Outstanding Graduate Student Research Award by the College of Engineering, Purdue University, in 2021 for his outstanding overall achievements. He has authored/co-authored more than 55 peer-reviewed conferences and journals, including 2 book chapters and 3 US patents. He has been a technical program committee (TPC) member and primary reviewer for multiple reputed journals and conferences, including TCAS-I, TVLSI, TCAD, Design & Test, TODAES, JETCAS, TBME, IEEE Access, IoTJ, DAC, GLSVLSI, IMS, VLSI Design.

EM/Power Side-Channel Analysis: Advanced ML attacks and Low-overhead Countermeasures

Debayan Das, Indian Institute of Science, Bangalore

Abstract: The huge gamut of today's internet-connected embedded devices has led to increasing concerns regarding the security and confidentiality of data. To address these requirements, most embedded devices employ cryptographic algorithms, which are computationally secure. Despite such mathematical guarantees, as these algorithms are implemented on a physical platform, they leak critical information in the form of power consumption, electromagnetic (EM) radiation, timing, cache hits and misses, and so on, leading to side-channel analysis (SCA) attacks. The complexity of breaking AES-256 is reduced from ~2^{256} to ~2^{13} when side channels are utilized. An attacker does not need to know specific implementation details of the cryptographic device to perform these attacks and extract keys. Going from AES128 to AES 256 only improves protection by 2x when side-channel attacks are employed, making physical side-channel attacks a significant threat.

Existing countermeasures (e.g. algorithmic, masking, power balancing, shielding) generally suffer from high overheads, sometimes performance degradations, and often are algorithm-specific. Generic low-overhead countermeasures require white-box modeling of the physical emissions and low-level countermeasures. Current statistical techniques for power and EM side-channel attacks during secure computation require multiple traces to be collected, and for low SNR, they require thousands of traces. Recent advances in Deep Learning power/EM Side-Channel Analysis (DL-SCA) allow an attack with a single or a few encryptions. Thus, DL-SCA increases the attack surface massively, as an attacker who has access to a device for minutes can now attack instead of hours of possession that were required with previous attacks like CPA. Recent work has shown how training on multiple devices can be used to generalize a DL-SCA machine learning (ML) model and can be used to carry out an attack on a new and similar device in very few encryptions. This puts a huge dent in the security of embedded devices.

In this tutorial, we will cover the following (a) Threats and impacts of physical side-channels (b) In-depth analysis of power side-channel and low-overhead generic power-side channel countermeasure using in-line current domain signature attenuation (c) White-box modeling of EM leakage from cryptographic ICs starting from Maxwell's equations and accelerating electrons and analysis of the impact of metal layers on EM information leakage (d) Generic low-overhead EM side-channel countermeasures (e) Intelligent EM sniffing using automated algorithmic automated detection of highest leakage-point (f) Machine-Leaning Side-channel attack and techniques for cross-device DL-SCA and (g) countermeasures for ML-SCA (h) pro-active power and EM SCA attack detection (i) a summary of open problems and future research directions for side-channel attacks and defenses.