Latice-based crypto and side-channel attacks: A Journey through IoT Paradigm

Dr. Soumya Banerjee
Senior Vice President Innovation, Trasna-Solutions Ltd. (Europe)
Senior industrial Research Fellow (University College Cork, Ireland
Senior Associated Researcher at Conservatoire National des Arts et Métiers (CNAM), Laboratoire CEDRIC and INRIA–EVA Paris, France

Abstract
Envisaging the boom of different IoT applications across the different cyber-physical systems, set the diversified objectives according to the use-cases. The different electronic devices in a standard cyber physical systems (CPS) including IoT, CPU & peripheral devices perform electromagnetic (EM) noise emission in CPS. It is worthy to mention that the associated instruction and machine cycle of specific CPU could demonstrate the behavior and pattern of software including of any malicious activity across the CPS. There are plenty of research investigations concerning the hardware-oriented encryption. Trusted platform module (TPM), secure booting could be few proposals on the same. Therefore, side channel attacks are critical with respect to the IoT systems. In ideal situation side channel attacks (SCA) broadly demonstrate the unwanted exposure of the critical information. Hence, those exposures can be subjected to different attacks categories like power attacks, EM attacks, timely attacks etc. This talk will explore the scope of Lattice based crypto to prevent those type of attack.

Short CV
Dr. Soumya (SM-IEEE) is Senior Vice President Innovation, Trasna-Solutions Ltd. (Europe) https://www.trasna.io/ and Senior industrial Research Fellow (University College Cork, Ireland, www.ucc.ie). He is also an adjunct invited Research professor and at present as Senior Associated Researcher at Conservatoire National des Arts et Métiers (CNAM), Laboratoire CEDRIC and INRIA–EVA Paris, France (https://aio.inria.fr/team/ (the French National Institute for computer science) Paris since November 2018. He was the Chief Technology Officer of MUST-B2B, Paris, where he is developing of Deep hybrid learning based recommendation and unsupervised machine learning for business Eco-system and communication systems. He is having several projects and product implementation on private Blockchain, e-SIM and smart manufacturing & logistics. Prior to that he was senior Associate Professor, Computer Sc.& Engg., Birla Institute of Technology Mesra, India, Vising research professor at CNRS–INSA de Lyon, Lyon, France (2016), Invited Research professor at TU-Ostrava, Cz Republic respectively (2015). He also spends several years with MSR Seattle, USA, in Cognizant Technology Solution, ICICI InfoTech both in India, south East Asia and Europe almost a decade. Dr. Banerjee completed his Bachelors in Engg. (At present VNIT Nagpur) in Computer Sc. (Hons.), did his masters from IISC Bangalore (MS- Research) and Ph.D in Computer Science and Engg. from Birla Institute of Technology, Mesra, India on Stigmergic optimization with Hybrid Intelligence in 2008-2009. He has more than 130 international journal publications including 34 book chapters and 55 International top level conference proceedings published from Elsevier Science, IEEE Transactions, ACM, Springer– Verlag Germany, CRC Press, and Idea Publication USA to his credit covering machine learning, security measures, prediction and data analytics, bio inspired intelligence, soft computing and optimization, hybrid intelligence, social networking applications and social media, Wiki analysis, machine learning with complex system and evolutionary computing. He also guided more than 10 Ph.D scholars in India and abroad. Dr. Banerjee had also developed a new artificial agent known as emotional ant colony for crowd modelling with European patent. Now he is having a patent with French govt. of business recommendation and ML. He is also an active project participant and consultant in IRIDIA (The National Lab of Computational Intelligence), Belgium, and Simula lab. Norway. He was leading a project as academic consultant with Yahoo Research Spain, and also envisaged new project on graph mining on FaceBook Friends analysis network from FaceBook UK and Luxemburg. He is involved also in several technical consultances at France with Netflix, Germany (University of Stutgart) and Ireland.