Abstract:

Today we manage and store very important and sensitive information in electronic computers i.e. IC chips. Cryptography is one of the powerful tools to protect such sensitive information in a cyber (software) domain. However, the cryptographic processing is anyway finally done in IC hardware. Malicious attackers exploit or break physical weakness of the IC hardware implementations. In this presentation, some existing threats to actual secure hardware electronic devices will be introduced with some countermeasures that we (IC designers) can do against these threats.

Speaker:

NORIYUKI MIURA received the Ph.D. degree in electrical engineering from Keio University, Yokohama, Japan in 2007. During his Ph.D. study and postdoc research activity under Prof. Tadahiro Kuroda’s guidance, he worked for developing inductive-coupling wireless interconnect technology for 3D IC integration. He is currently an assistant professor at Kobe University working on hardware security, smart sensor, and 3D heterogeneous integration. Dr. Miura has published more than 50 international conference papers including 16 ISSCC papers, and was selected as one of the top ISSCC paper contributors from 2004 to 2013. He is currently serving for Symposium on VLSI Circuits, A-SSCC, ASP-DAC, and VLSI-DAT TPC.