October 13, 2017 at 2:00 PM in ENGR 1101

Securing Physically Unclonable Functions

Sandip Kundu
Department of Electrical & Computer Engineering
University of Massachusetts Amherst

Abstract

Proliferation of mobile computing hardware and emergence of Internet-of-Things have created a need for low-cost solutions for cryptographic functions such as authentication, encryption and digital signatures. Current best practices involve storing a secret key in a nonvolatile memory or battery backed SRAM which are vulnerable to invasive attacks. Physically Unclonable Functions (PUF) have been touted as an alternative for authentication and low-cost key generation. Due to the nature of applications, a PUF may operate in an untrusted environment where an adversary has the capability to eavesdrop on communications or even have physical possession of the PUF with the ability to apply any input and observe outputs. Securing PUF in this environment is challenging. While the actual threat model varies from application to application, there are some common security challenges for a PUF. In this talk, we will describe two such challenges: (i) ensuring uniqueness (ii) and thwarting modeling attacks. We will then present novel solutions to address those problems. Finally, we will conclude this talk with some open challenges.

Bio

Sandip Kundu is a Professor at the University of Massachusetts at Amherst. Currently, he is serving at the National Science Foundation as a Program Director of the division of Computer Network Systems, within the directorate of Computer and Information Science and Engineering. He obtained his PhD in 1988 and then spent 17 years in industry before joining academia. First he joined the IBM Research Division as a Research Staff Member and then Intel Corporation as a Principal Engineer. He has published well-over 200 research papers in VLSI design and test, holds several key patents including ultra-drowsy sleep mode in processors, and has given more than a dozen tutorials at various conferences. He is a Fellow of the IEEE, Fellow of the Japan Society for Promotion of Science (JSPS), Senior International Scientist of the Chinese Academy of Sciences and was a Distinguished Visitor of the IEEE Computer Society. He is currently an Associate Editor of the IEEE Transactions on Dependable and Secure Computing. Previously, he has served as an Associate Editor of the IEEE Transactions on Computers, IEEE

Transactions on VLSI Systems and ACM Transactions on Design Automation of Electronic Systems. He has been Technical Program Chair/General Chair of multiple conferences including ICCD, ATS, ISVLSI, DFTS and VLSI Design Conference.