ELECTRICAL AND
COMPUTER ENGINEERING
SEMINAR

Fan Zhang

Zhejiang University

Persistent Fault Attacks in Practice

Friday, February 7th

ISEC 140
11:00am

Abstract:

Persistent fault analysis (PFA) was proposed at CHES 2018 as a novel fault analysis technique. It was shown to completely defeat standard redundancy based countermeasure against fault analysis. The original PFA was demonstrated with rowhammer-based fault injections. However whether such an analysis can be applied to traditional microcontrollers, together with its attack difficulty in practice, has not been investigated. In this talk, for the first time, a persistent fault attack is conducted on an unprotected AES algorithm implemented on ATmega163L microcontroller. Several critical challenges are coped with our new improvements. This talk will introduce the PFA at both theoretical and practical levels.

Bio:

Dr. Fan Zhang graduated from Department of Computer Science and Engineering, University of Connecticut, USA. He is currently an associate professor in College of Computer Science, Zhejiang University, China. He was a visiting scholar in National University of Singapore and currently he is a visiting professor in Singapore University of Technology and Design. His major research interest is the general cyber security which includes hardware security, system security, network security and more. His special expertise lies in the domain of side channel attacks (SCA) and countermeasures, fault attacks, cryptography, and computer architecture. He is the Program Chair of PROOFS, TPC member of DAC, AsiaCCS, AsianHOST, ASHES, COSADE, FDTC, Inscrypt, and the Associate Editor of IEEE Access, Cybersecurity. He has more than 60 publications in international conferences and journals such as CHES, DATE, COSADE, FDTC, TIFS, TPDS.