Cryptographic Engineering Research Group Presents

ECE DEPARTMENTAL SEMINAR

Towards Automatic Application and Verification of Countermeasures Against Physical Attacks

Monday, May 11th, 2015
3:00 pm — 4:00 pm
Engineering Building, Room 3507

Speaker: Francesco Regazzoni
Postdoctoral Researcher,
ALaRI Institute of University of Lugano, Switzerland

Abstract:

Physical attacks exploit the physical weaknesses of cryptographic devices to reveal the secret information stored on them. Countermeasures against these attacks are often considered only in the later stages of the full design flow, and applied manually by designers with strong security expertise. This approach, however, negatively affects the robustness, the cost, and the production time of secure devices. In view of this increasingly relevant problem, it is crucial to address the design challenges associated with the proliferation of physical attacks, developing a methodology to automate the design and the verification of secure embedded systems. This talk focuses on one type of physical attacks, the differential power analysis (DPA), and presents the design and the implementation of the infrastructure needed to enable the automatic application and verification of DPA countermeasures.

Biography:

Dr. Francesco Regazzoni is a postdoctoral researcher at the Advanced Learning and Research Institute (ALaRI) of University of Lugano (Lugano, Switzerland). He received his Master of Science degree from Politecnico di Milano and his PhD degree at the ALaRI Institute of University of Lugano. He has been an assistant researcher at Université Catholique de Louvain and at Technical University of Delft, and visiting researcher at several institutions, including NEC Labs America, Ruhr University of Bochum, EPFL, and NTU. His research interests are mainly focused on embedded systems security, covering in particular side channel attacks, cryptographic hardware, and electronic design automation for security.