Towards the Automatic Application of Countermeasures Against Physical Attacks

Francesco Regazzoni

Abstract

Physical attacks exploit the physical weaknesses of cryptographic devices to reveal the secret information stored on them and pose a major security threat for embedded systems. 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 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 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 of DPA countermeasures at hardware and software level.

Dr. Francesco Regazzoni is a postdoctoral researcher at ALaRI Institute of University of Lugano (Lugano, Switzerland). He received his Master of Science degree from Politecnico di Milano (Italy) and his PhD degree from University of Lugano (Switzerland). He has been assistant researcher at the Crypto Group of the Université Catholique de Louvain (Louvain-la-Neuve, Belgium) and has been visiting researcher at several institutions, including NEC Labs America (Princeton, NJ, USA), Ruhr University of Bochum

(Bochum, Germany), and EPFL (Lausanne, Switzerland). His research interests are mainly focused on embedded systems security, covering in particular side channel attacks, cryptographic hardware, and electronic design automation for security.