Towards Automatic Application Of Power Analysis Countermeasures

Lecturer: Francesco Regazzoni, Ph.D.
Place: T9:349 NB CTU in Prague
Time: Wednesday, November 30th 2011, 6-8 pm

Abstract:

Security is a fundamental feature for nowadays embedded systems; however, due to the advent of side channel attacks, satisfaction of this need is a challenging task. These new, cheaper and faster attacks derive the secret key from the information leaked while data is being processed. In particular, power analysis attacks are very dangerous since they do not require a deep knowledge of the target device to be effective.

In view of this increasingly relevant problem, this talk proposes a methodology to automate the design of systems characterized by robustness with respect to attacks based on power-related side effects as well as by low-energy consumption and high performances. More in details, the presented work proposes an infrastructure for bringing the security to the forefront of design variables by associating it with a clear quantitative metric, and shows how such infrastructure can be realized using standard tools. The talk will conclude proposing examples which illustrate the tradeoff between the security achieved and the cost of several points of the design space.

About the lecturer:

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 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.