The Design-Time Side-Channel Information Leakage Estimation

Jan Bělohoubek

jan.belohoubek@fit.cvut.cz

Faculty of Information Technology
Czech Technical University in Prague

Abstract

The design of today's circuits is an iterative process, where every iteration could influence the information leakage into the side channel. During the design time, bugfixes must be incorporated, and sometimes even architectural changes are performed.

The principles of a new analytical simulation-based method allowing an efficient side-channel information leakage evaluation in various steps of the digital design flow will be presented. If applied, the method allows to decide, if a certain design decision has a positive or negative influence on the side-channel information leakage independently of any current or future attack schemes.

The experiments with the benchmark circuits and no manufacturing variations showed interresting facts: the N-Modular-Redundancy offers no additional information leakage compared to the single module and the unbalanced dual-rail implementation offers additional information compared to the single-rail implementation.

Acknowledgement

This research has been partially supported by the grant GA16-05179S of the Czech Grant Agency and by CTU grant SGS17/213/OHK3/3T/18.

Computational resources were provided by the CESNET LM2015042 and the CERIT Scientific Cloud LM2015085, provided under the programme "Projects of Large Research, Development, and Innovations Infrastructures".

Reference

[1] C. Y. Chu, *Improved Models for Switch Level Simulation.* Stanford University, 1988.

[2] J. Schmidt and P. Fišer, "A prudent approach to benchmark collection," *in Proc. of 12th Int. Workshop on Boolean Problems (IWSBP), Freiberg (Germany)*, 2016.

[3] D. Karaklajić, J.-M. Schmidt, and I. Verbauwhede, "Hardware designer's guide to fault attacks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 12, pp. 2295–2306, 2013.