Modulated CMOS Static Power is Data Dependendent and Observable

Jan Bělohoubek

jan.belohoubek@fit.cvut.cz

Faculty of Information Technology
Czech Technical University in Prague

Abstract

As digital devices penetrate into many areas important for the present society, it is important to analyze even potential threats to mitigate device vulnerability during the lifetime of a digital device.

Skorobogatov has shown, that it is possible to obtain data stored in a register by using the invasive methods [1] (the chip decapsulation and the laser beam). The disadvantage is, that the probing method is strongly limited by the transistor size and it is not applicable to recent technologies.

To overcome the size limitation, we analyzed the data dependency of the static power of CMOS combinational logic. We found that the static power (of a relative large combinational logic) modulated by the laser beam may decrease the entropy of the processed data. This is achieved by correlating the measured current consumption (induced by a laser beam) with the power model reflecting the data dependency of the laser-induced current.

Moreover, the results have shown, that in certain cases, it is possible to obtain the processed data directly. When targeting sufficiently large combinational logic with the special structure, namely majority voter, the processed bit leaks [2].

Acknowledgement

The authors acknowledge the support of the OP VVV MEYS funded project CZ.02.1.01/0.0/0.0/16_019/0000765 "Research Center for Informatics" and grants GA16-05179S of the Czech Grant Agency and the CTU grant SGS17/213/OHK3/3T/18.

Reference

[1] S. Skorobogatov, "Optically enhanced position-locked power analysis," in *Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2006, pp. 61–75.

[2] J. Belohoubek, P. Fiser, and J. Schmidt, "Using Voters May Lead to Secret Leakage," in *22nd International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS 2019)*, Apr 2019.