Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis

Parameter Optimitzation for On-Chip Voltage Sensor

In a Multi-tenant FPGA scenario multiple users have their own partial reconfigurable region on a single FPGA. Each of theses regions allows a single user to implement her/his design, without being able to directly interact with the design of another user on the same FPGA. So-called Time to Digital Converters (TDCs) can be used to perform remote side-channel attacks in such multi-tenant FPGAs, to extract secrets from other users.

The TDC is used as remote power measurement unit of the FPGA. The working principle is to use a long path in which timing violations are caused. Since the delay of transistors are proportional to the supply voltage, the amount of timing violations is a measure of the devices power consumption.

Different publications have already shown that cryptographic implementations [1, 2] and neural networks [3] can be attacked with such sensors.

In this work, design parameters of the TDC should be explored, in order to evaluate the influence on measurements of the on-device power consumption.

[1] F. Schellenberg, D. R. E. Gnad, A. Moradi, and M. B. Tahoori, “An inside job: Remote power analysis attacks on FPGAs,” in Design, Automation and Test in Europe Conference & Exhibition (DATE), 2018, pp. 1111–1116.

[2] O. Glamočanin, L. Coulon, F. Regazzoni, and M. Stojilović, “Are cloud fpgas really vulnerable to power analysis attacks?” in 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2020, pp. 1007–1010.

[3] V. Meyers, D. Gnad and M. Tahoori, "Reverse Engineering Neural Network Folding with Remote FPGA Power Analysis," 2022 IEEE 30th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), 2022, pp. 1-10, doi: 10.1109/FCCM53951.2022.9786107.

Prerequisites

VHDL/Verilog knowledge, Python skills

Contact

manuel.brosch@tum.de
matthias.probst@tum.de

Advisors

Manuel Brosch, Matthias Probst