Pinpointing the leakage of dual-rail logics in FPGAs

Philippe NGUYEN and Hassan TRIQUI
Secure-IC S.A.S.

Abstract

Dual-Rail with Precharge Logics (DPL) make up a class of side-channel countermeasures attempting to minimize the leakage via the power consumption and the electromagnetic fields emanations.

These countermeasures have been implemented with success in ASIC circuits.

Starting from the first portable DPL countermeasure, called WDDL, a bunch of refinements such as MDPL, DRSL, divided backend duplication, STTL, iMDPL, SecLib, BCDL, have been devised.

They cover most of the known sources of remaining biases, such as the true/false networks unbalance or the early propagation effect.

However, when implemented in FPGAs, those logics always prove to be attackable fairly easily: many research papers report that the security gain of an unprotected reference is significantly lower for designs in FPGAs than in ASICs.

In this talk, we introduce a practice-oriented robustness evaluation based on the theoretical framework presented by F.-X. Standaert et al. at EUROCRYPT 2009.

The computation of mutual information based on a bitwise partitioning allows to quantify the amount of bits leaked by each resources of the circuit during each step of operations.

We exemplify this leakage analysis tool on an AES accelerator, implemented in WDDL and BCDL logics, in a Stratix FPGA.

In this case study, the methodology successfully identifies the most vulnerable bits.

This knowledge allows the designer to check the post place-and-route netlists (.vo), constraints (.rcf) and characterization (.sdo) files to diagnose the origin of the problem.

Specifically, we illustrate how a retiming optimization of Quartus introduces a major vulnerability.
Finally, we conclude all the same that FPGAs can be suitable, if used in a sensible manner, to prototype quickly countermeasures principles, when they are coupled to an efficient leakage investigation tool.