Motivation

- Security of many digital devices strongly depends on a secret value stored in them
- New attacks are invented continuously
  → it is important to analyze even potential threats to mitigate device vulnerability during its lifetime
  → yet unexplored properties of CMOS may lead to security threats

Photoelectric Laser Stimulation

The laser beam passing through silicon creates, as a result of energy absorption, electron-hole pairs along its path, generating the Optical Beam Induced Current (OBIC) along PN junctions.

Conventional Majority Voter

Security-reliability interplay research:
- is circuit security influenced by voter – yet unknown threats?
- is voter side-channel emission influenced by input data?

Contribution: Majority Voter as the Amplifier

It is possible to deduce voter’s input value by combining circuit illumination (by a laser) and side channel emission measurement:
- The voter size for conventional technologies, e.g. for 180nm (and also for sub-100nm processes), is large enough for precise laser-beam targeting into the voter area only
- The voter depends on a single logic value represented by multiple bits (at all its inputs): the voter may be understood as the physical amplifier of the (side channel) emissions related to the single logic value
- The majority voter is designed to mask errors → if the voter is affected by fault injection, the voter’s output tends to remain stable → fault injection side-effects tend to be localized to the voter area only

Experiment Setup and Replicability

- SPICE models for pulsed photoelectric laser stimulation (PLS) of NMOS/P MOS based on work of Sarafianos et al.
  → Available at the DDD Research Group website
  (http://ddd.fit.cvut.cz/prj/MajVoterPLS)
- The open tools: digital synthesis flow – Qflow, Magic, ngSPICE
- TSMC180 nm open standard cell provided by Oklahoma State University

Results

The current peaks induced by a PLS in a voter circuit depending on the laser beam position: average for voter all-1 and all-0 inputs is shown

The difference in current peaks induced by PLS targeting the voter with all-1 and all-0 inputs depending on the laser beam position

Future Work

- Measurements on real devices should be performed to confirm the severity of the reported threat
- The influence of voter architectures should be studied
- Data dependence of CMOS under PLS should be studied in general (Work-in-Progress)

Conclusions

- The power trace imprint of the conventional voter under PLS is correlated with processed data
  → we identified the potential threat endangering the security of CMOS circuits employing voters
- Our work is completely replicable: open tools were used, developed models and related resources were released under BSD-like license

The authors acknowledge the support of the OPVVV 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.

Jan Bělohoubek, Petr Fišer, Jan Schmidt
{jan.belohoubek, petr.fiser, jan.schmidt}@fit.cvut.cz