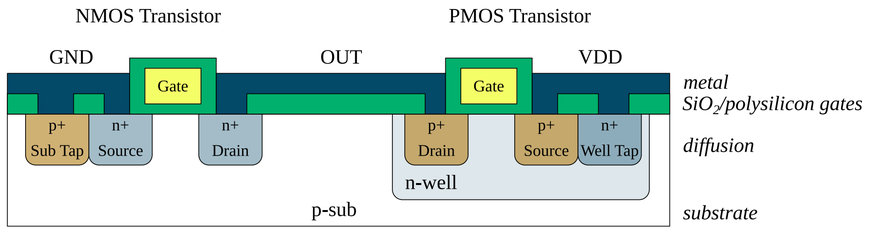
CMOS Illumination Enables Observation of Processed Data in Power Traces

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



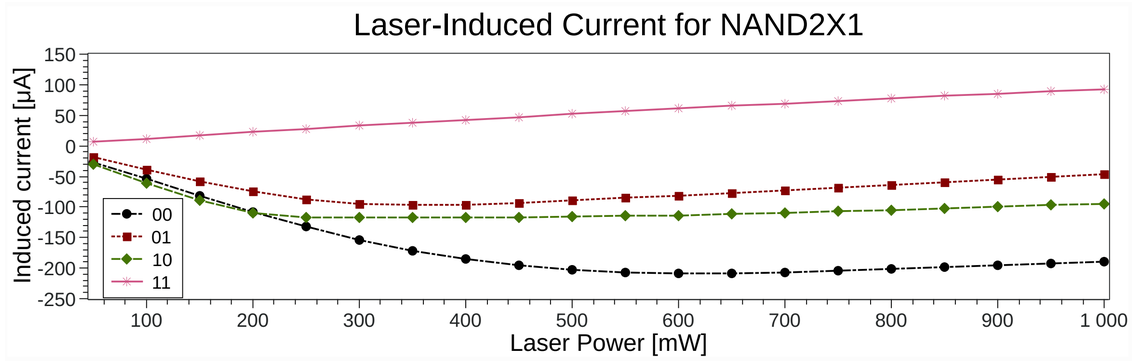
CMOS cross-section – the PN junctions

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

Contribution

- *Bělohoubek, J.; Fišer, P.; Schmidt, J.: CMOS Illumination Discloses Processed Data. In: Proceedings of the 22nd Euromicro Conference on Digital Systems Design. Los Alamitos, CA: IEEE Computer Soc., 2019. p. 381-388. ISBN 978-1-7281-2862-7.*
  - → Laser illumination of CMOS logic leads to data-dependent power trace imprint
- *Bělohoubek, J.; Fišer, P.; Schmidt, J.: "Using Voters May Lead to Secret Leakage". In: 22nd International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS 2019). Cluj-Napoca, Romania, April 24-26, 2019.*
  - → Laser illumination of CMOS conventional majority voter – in connection with SPA – allows to read logic values at the voter inputs – "Majority Voter as the Amplifier"

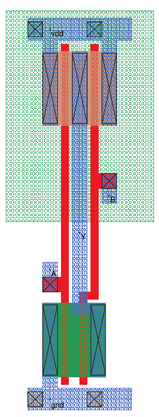
Data-Dependent Power Trace Imprint



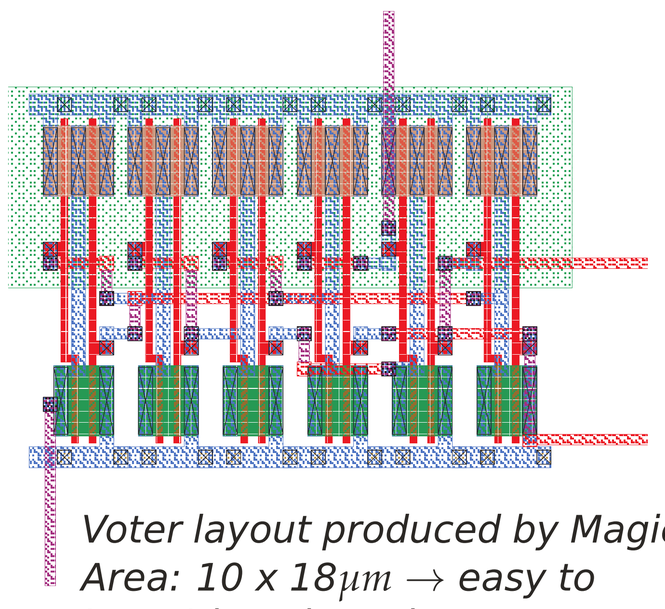
Laser Power and Input Data Dependency:

- all input values can be distinguished clearly (in the power trace) for the two-input NAND gate
- data-dependent part of the induced photocurrent depends on laser power

Experiment Setup and Replicability



NAND2X1 gate layout produced by Magic; Area: 10 x 3μm in TSMC 180nm technology



Voter layout produced by Magic Area: 10 x 18μm → easy to target by a laser beam

- SPICE models for *pulsed photoelectric laser stimulation* (PLS) of NMOS/PMOS based on work of Sarafianos et al.
  - → Available at the DDD Research Group website and on GitHub

    https://ddd.fit.cvut.cz/prj/CMOS-PLS/

    https://github.com/DDD-FIT-CTU/CMOS-PLS/
- The open tools: *digital synthesis flow* – Qflow, Magic, ngSPICE
- TSMC 180nm open standard cell library provided by Oklahoma State University

Proposed Attacks

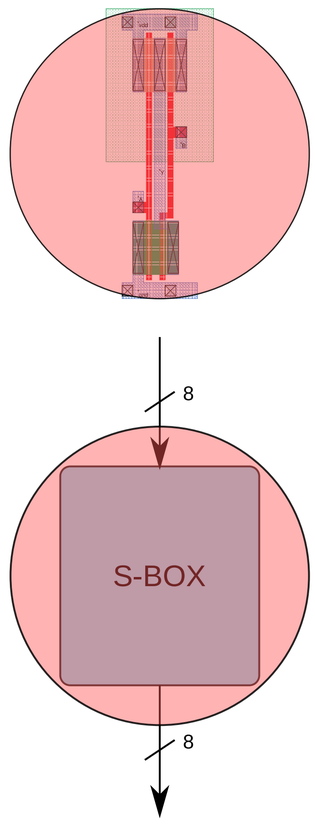
Proposed attacks are based on static power measurement:

- Static power is modulated by laser beam
- Simple Power Analysis (SPA) is employed

Template attacks are feasible:

- Monte Carlo SPICE simulations have shown, that the inter-die differences in laser-induced photocurrent are not significant
  - → Reading individual bits by the **single gate illumination** should be possible when gate sizes are reasonable with respect to the laser beam spot size
  - → For bigger circuits (e.g. AES S-BOX), a **circuit power model under illumination** may be composed (by measurements) and measured data from the device-under-attack may be correlated with the power model

Attack scenarios feasibility must be confirmed by measurement!



Future Work

- Measurements on real devices
- Comparison of the proposed Attack with State-of-the-art attacks (DPA)
- Influence of the logic surrounding the illuminated logic should be investigated
- Cocktail Effect Research – decreasing the entropy of processed data by the modulated static power analysis (for bigger circuits)

Conclusions

- The static power of CMOS logic under PLS is correlated with processed data
  - → **we identified the potential threat endangering the security of CMOS circuits in general and majority voters in particular**
- Our work is completely replicable: open tools were used, developed models and related resources were released under BSD-like license

If a CMOS circuit is illuminated (by a laser beam), while the activity of the circuit is suppressed (stable clock and inputs), the **laser-modulated static power** of the *circuit under attack* **is strongly influenced by logic values** at the circuit inputs.

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 the CTU grant SGS17/213/OHK3/3T/18.

Jan Bělohoubek, Vojtěch Miškovský, Petr Fišer, Jan Schmidt

{jan.belohoubek, vojtech.miskovsky, petr.fiser, jan.schmidt}@fit.cvut.cz

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research, Development and Education

MINISTRY OF EDUCATION, YOUTH AND SPORTS

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

RESEARCH CENTER FOR INFORMATICS
rci.cvut.cz