FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Modulated CMOS Static Power is Data Dependent and Observable

Jan Bělohoubek

jan.belohoubek@fit.cvut.cz

Czech Technical University in Prague
Prague, Czech Republic

CryptArchi 2019, Prague – Průhonice, Czech republic

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

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Motivation – Novel Vulnerabilities Originating in the Modulated Static Power

We analyze the data dependency of the photocurrent induced by a laser beam in the illuminated CMOS device:

→ lasers are often used to induce faults into registers

→ we analyze static current of **combinational circuits** modulated by illumination (a laser beam)

\+ combinational logic provides **sufficient area** (to target laser beam) even in recent technology nodes

\+ stored **values remain unaltered**

  → error detection may not be raised

  → measurement time may be prolonged

– advisory values are *mixed together* → **the cocktail effect**

– possible **attack requirements are strong** – known layout, precise laser beam localization

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Experimental Setup

- We used TSMC 180nm technology node:
  - open standard cell library and SPICE models provided by Oklahoma State University (OSU)[1]
  - it does not represent the latest technology node, but it is still relevant for manufacturing devices like smart-cards or key-fobs
- The SPICE models of transistor under PLS: Sarafianos et al[2]
- Circuit layout:
  - for layout synthesis, the open *digital synthesis flow* – *Qflow* – was used (*Berkeley ABC*, *QRouter*, *GrayWolf* and *Magic*)
  - synthesized layouts were simulated in ngSPICE
- Models and experimental data are available on GitHub[3]

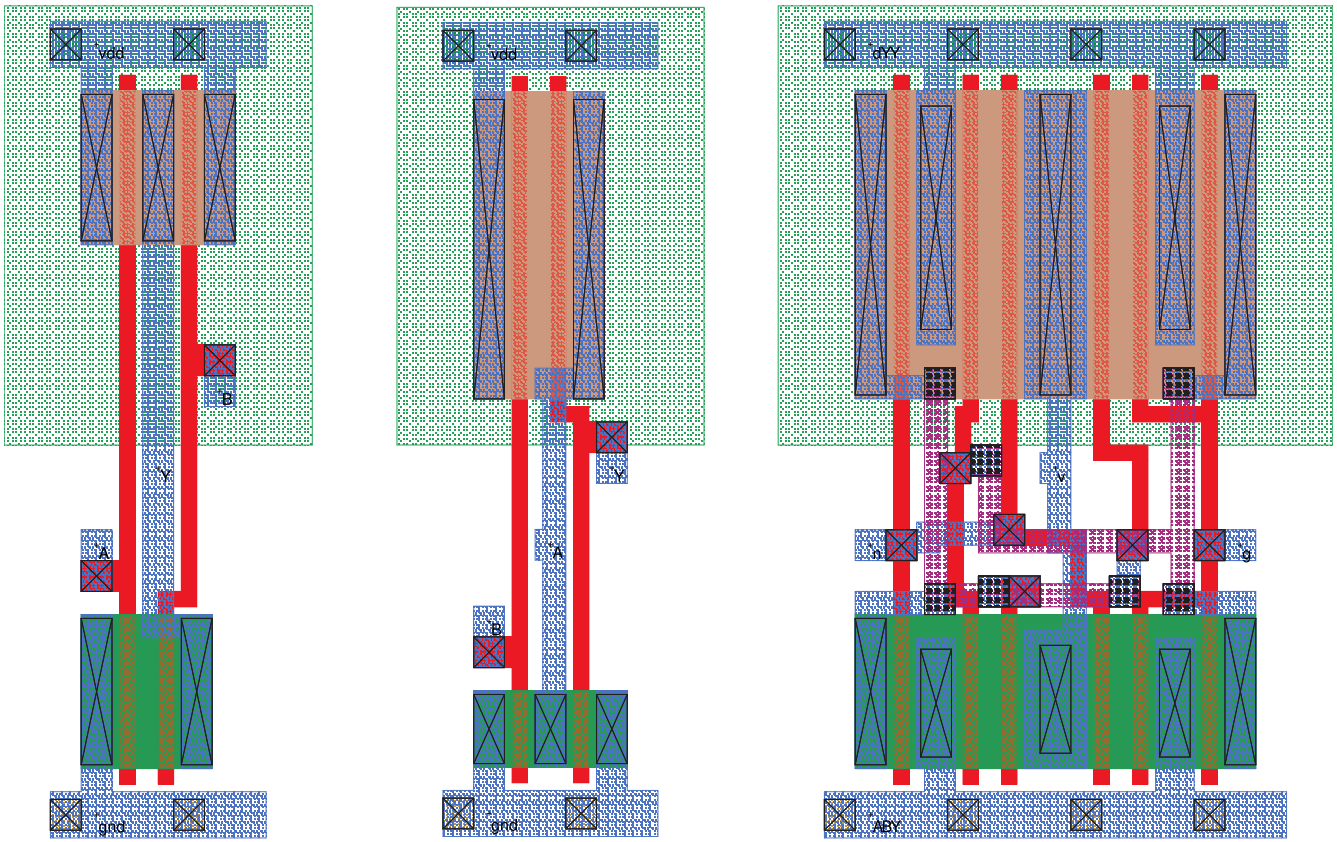
---

[1] https://vlsiarch.ecen.okstate.edu/flows/MOSIS_SCMOS

[2] Sarafianos et al, "Building the electrical model of the pulsed photoelectric laser stimulation of a PMOS transistor in 90nm technology,"; ...

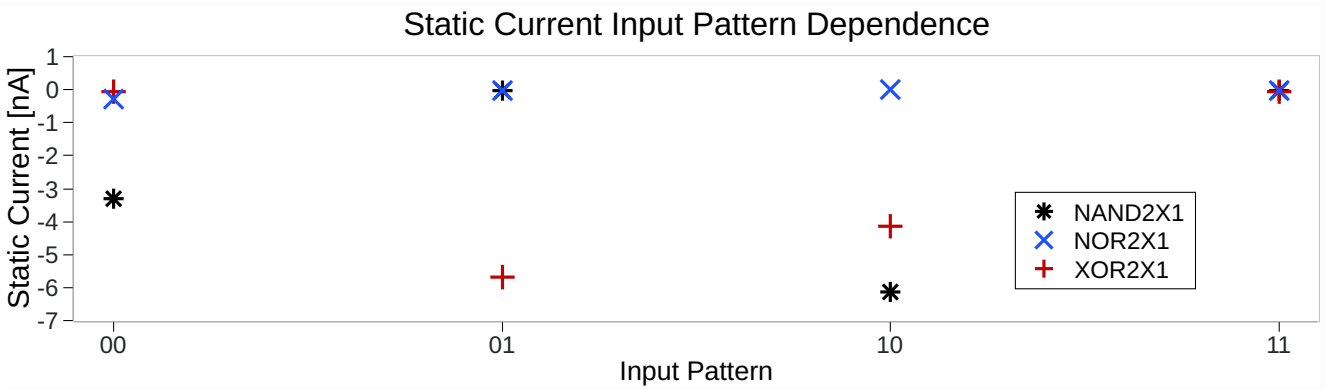
[3] https://github.com/DDD-FIT-CTU/CMOS-PLS

Data Dependency in CMOS
Conductivity is Influenced by Geometry



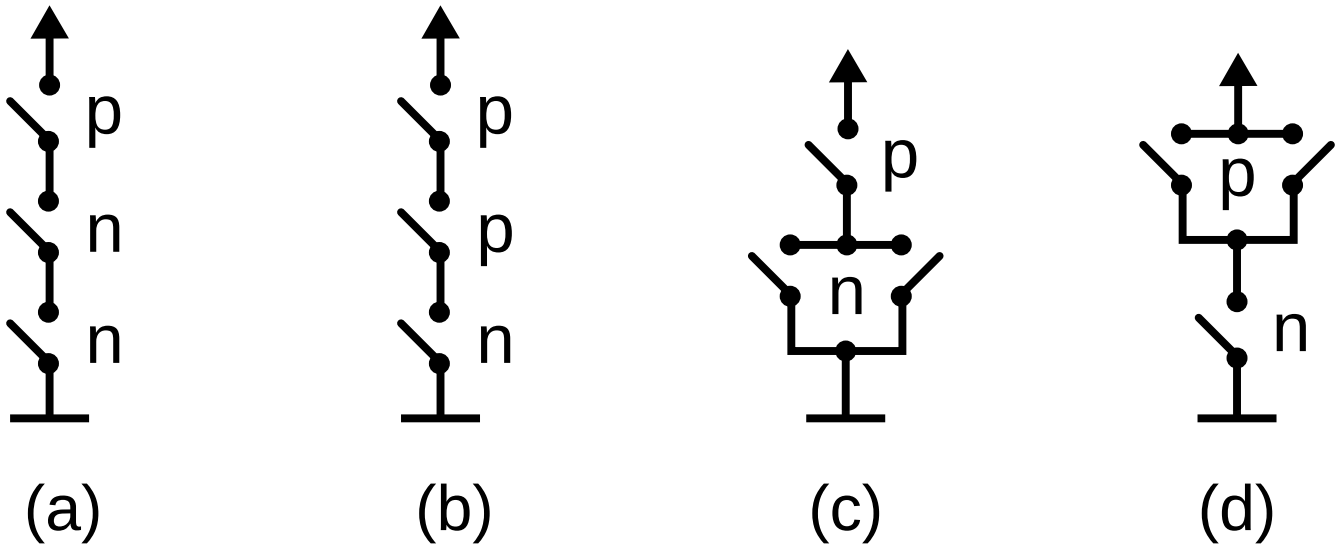
Layout of `NAND2X1` (4 x 10.8 μm), `NOR2X1` (4 x 10.8 μm) and `XOR2X1` (7.2 x 10.8 μm) cells in 180nm TSMC technology

Data Dependency in CMOS



The data dependency of the static current on the input pattern for three standard cell SPICE models – namely `NAND2X1`, `NOR2X1`, and `XOR2X1` – in 180nm TSMC technology

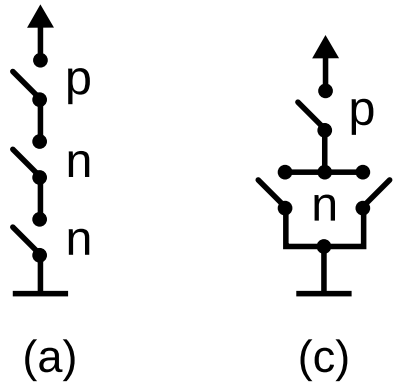
Data Dependency in CMOS
Serial/Parallel Transistor Structures



(a) (b) (c) (d)

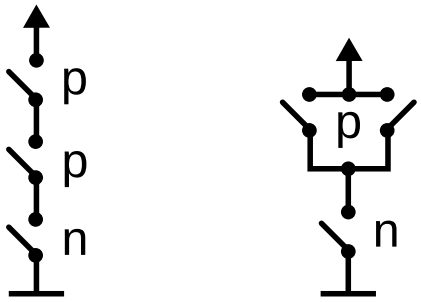
Simulated transistor structures displayed as serial/parallel switches. Note, that these structures are not included in the standard cell library: SPICE models were derived from standard cells with equal geometry of NMOS/PMOS parts

Data Dependency in CMOS
Serial/Parallel Transistor Structures



- in structures (a) and (c), the static current is influenced (mainly) by the state of the PMOS transistor – the dependency on any combination of NMOSes is distinctly less significant;
- for NMOSes, it holds, that the serial structure (a) introduces a stronger data dependency than the parallel structure (c). Naturally, there is a difference in the static current when opening (only) the *top* or (only) the *bottom* transistor because of induced drain/source voltage differences;

Data Dependency in CMOS
Serial/Parallel Transistor Structures



(b) (d)

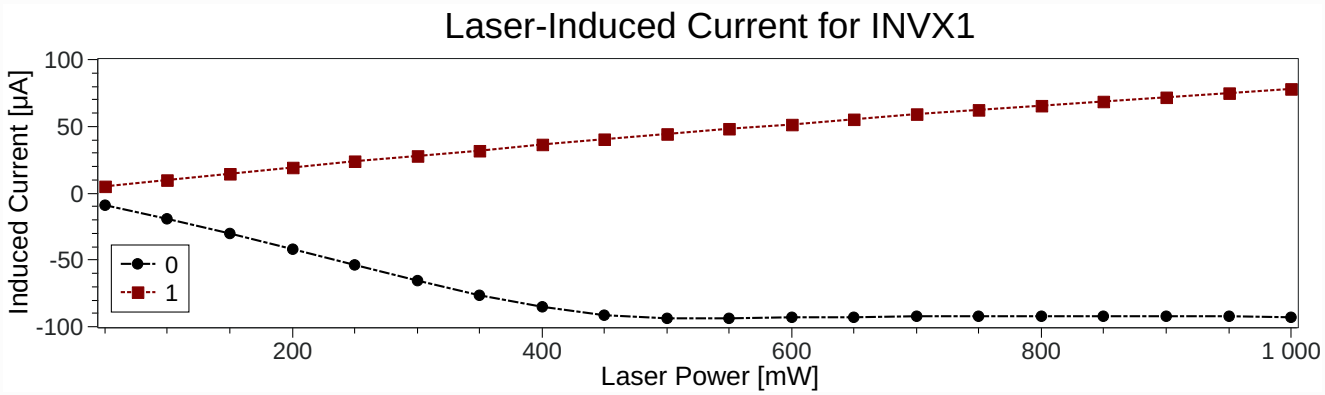
- for structures (b) and (d), we observed very little (almost none) data dependency on the (single) NMOS transistor state;
- for PMOSes, in contrast to NMOSes, the parallel structure (d) introduces (a bit) stronger data dependency than the serial structure (b). This is apparently caused by lower hole mobility in PMOSes.

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Data Dependency in CMOS
Influence on Standard Cells

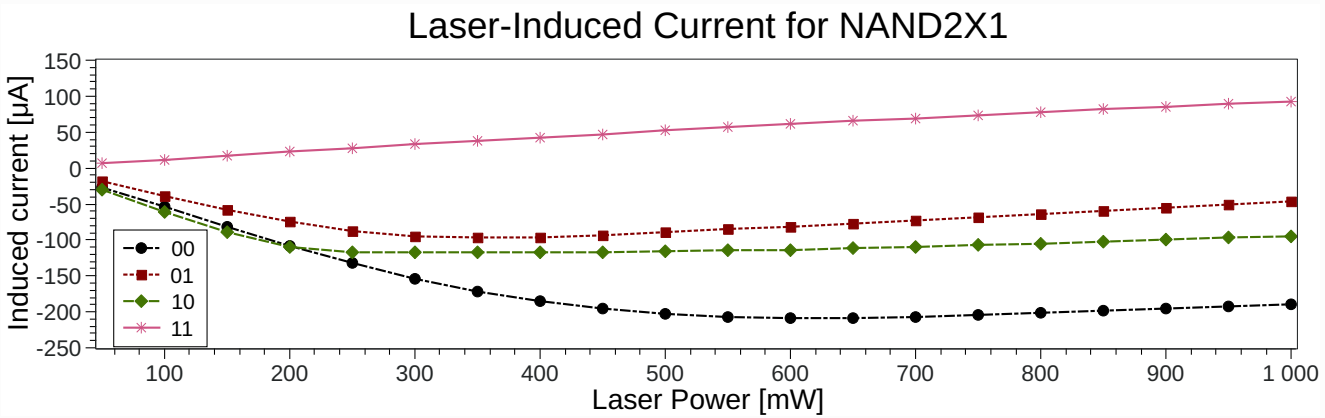
- the `NAND2X1` cell is the most asymmetric one, which is caused by the NMOS serial arrangement;
- the `XOR2X1` cell power imprint allows a clear distinction of the XOR output state, which demonstrates the symmetry of the XOR gate;
- the `NOR2X1` power imprint is very narrow compared to the other two gates, which is apparently caused by the serial arrangement of PMOSes (introducing low conductivity when one of them is closed).

Standard Cell Illumination
INVX1



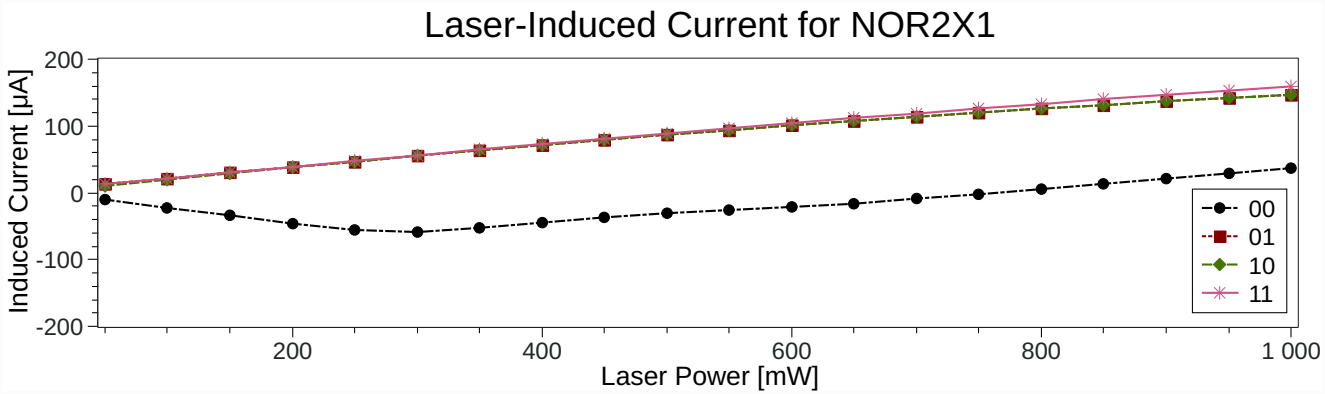
The photocurrent for `INVX1` for different input patters and increasing laser power. The 0 and 1 input patterns are easy to distinguish

Standard Cell Illumination
NAND2X1



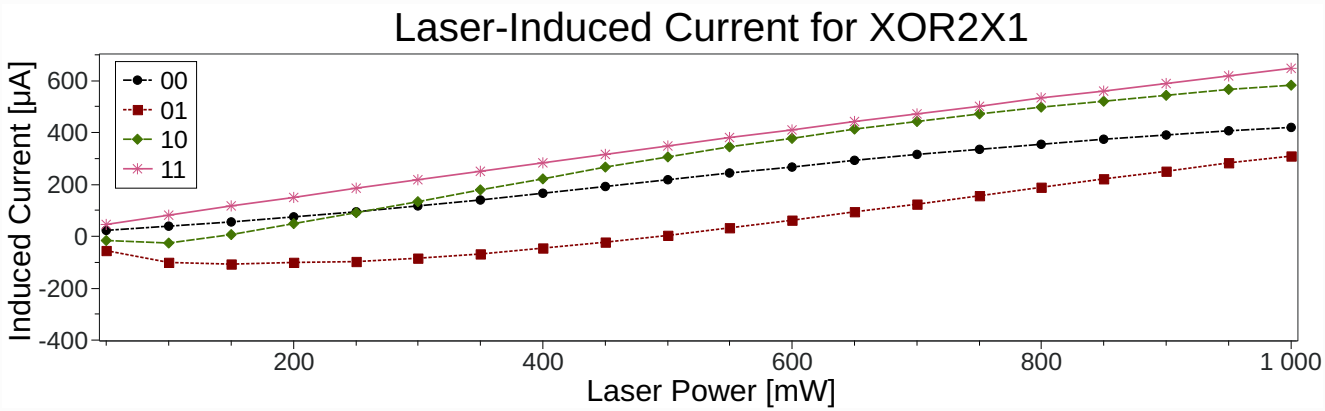
The photocurrent for `NAND2X1` for different input patters and increasing laser power. The 00 and 11 input patterns are easy to distinguish; patterns 01 and 10 cause similar currents, although the 20μA difference (for 100mW and above) is still distinguishable

Standard Cell Illumination
NOR2X1



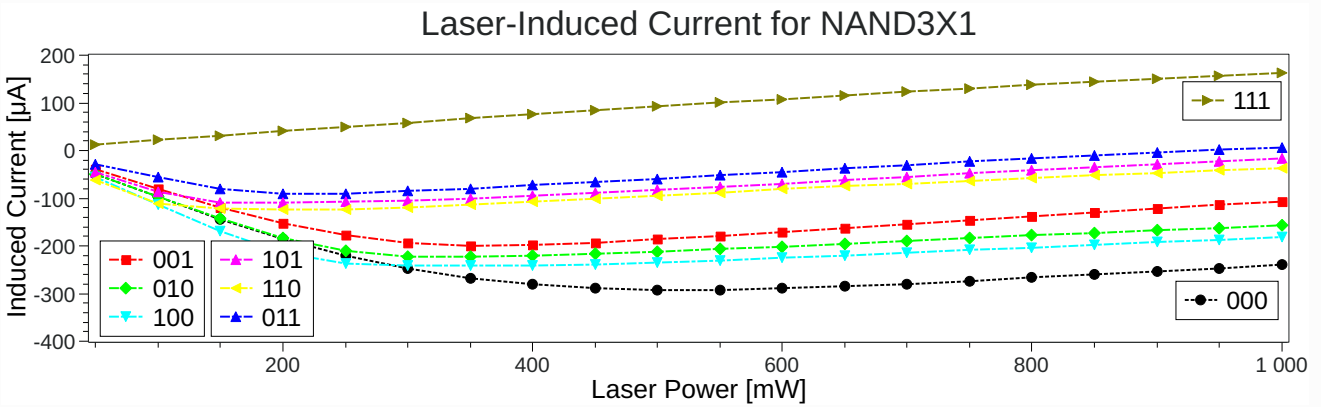
The photocurrent for `NOR2X1` for different input patters and increasing laser power. The (00) and (11, 01, 10) input pattern subsets are easy to distinguish

Standard Cell Illumination
XOR2X1



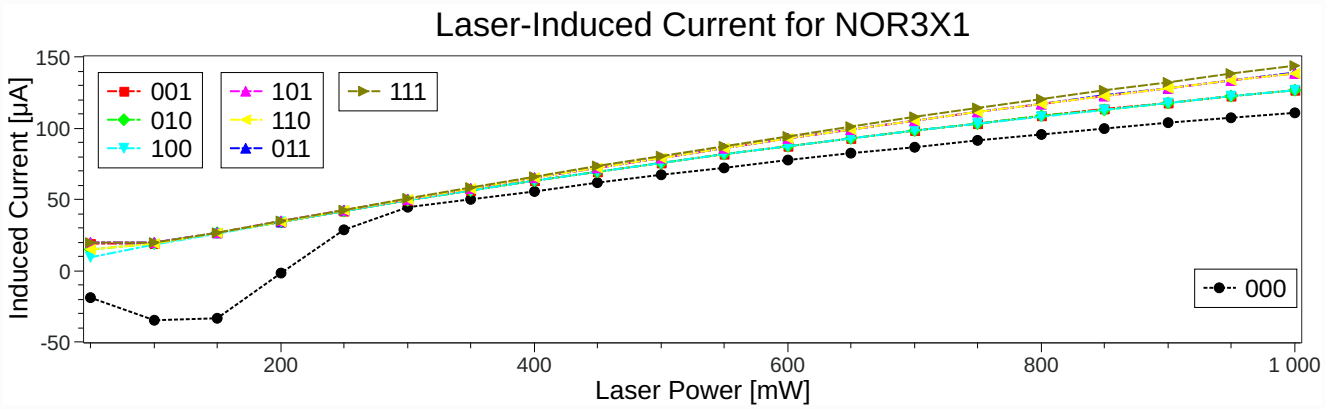
The photocurrent for `XOR2X1` for different input patters and increasing laser power. The 00 and 11, 01 and 10 input patterns can be distinguished

Standard Cell Illumination
NAND3X1



The photocurrent for `NAND3X1` for different input patterns and increasing laser power. The four sets of input patterns are easy to distinguish: these sets of input patterns distinguished by the Hamming Weight (HW): 000 with HW(0); 001, 010 and 100 with HW(1); 011, 101 and 110 with HW(2) and 111 with HW(3)

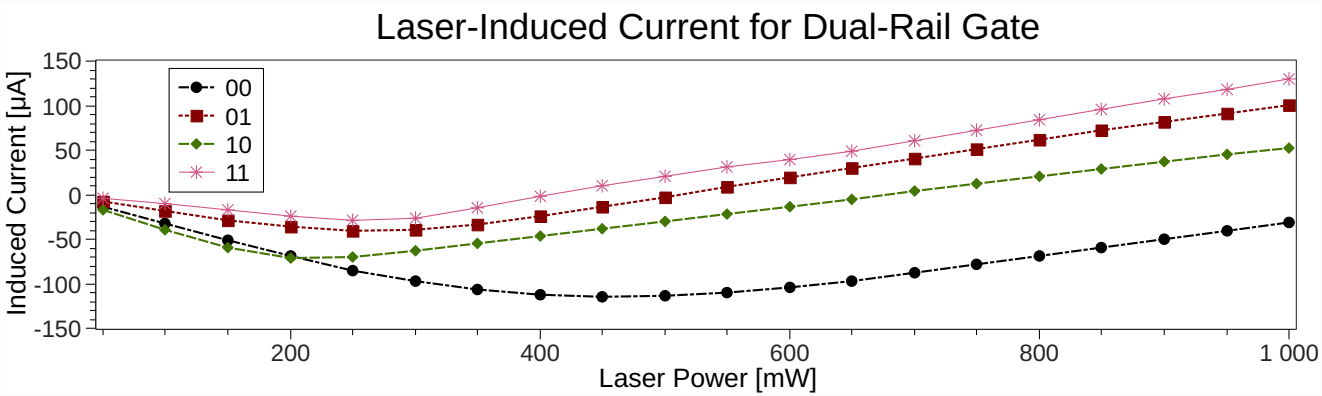
Standard Cell Illumination
NOR3X1



The photocurrent for `NOR3X1` for different input patterns and increasing laser power. It is simple to distinguish the 000 input pattern. Additionally, it is possible to distinguish 4 sets of input patterns: these sets of input patterns distinguished by Hamming Weight (HW): 000 with HW(0); 001, 010 and 100 with HW(1); 011, 101 and 110 with HW(2) and 111 with HW(3)

Dual-Rail is Not Safe

- dual-rail encoding-based methods were introduced (into security area) to balance the **dynamic power**
- our method exploits the differences in the geometry and the data dependency of the (modulated) **static power**



The photocurrent for the conventional WDDL `NAND` gate composed of `NAND2X1` and `NOR2X1` gates for different input patterns and increasing laser power. The 00 input pattern (logical inputs) is easy to distinguish; other patterns (11, 01 and 10) are also distinguishable

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Cocktail Effect Work-In-Progress

- the "cocktail effect" is the situation, when the (modulated) static currents of many gates are mixed together
- the in depth research of the "cocktail effect" influence is currently work-in-progress
- we have already shown, that there are special cases, where "cocktail effect" has, in fact, positive influence from the attacker's perspective – voters may behave as amplifiers[4]
- in many cases, the "cocktail effect" allows to decrease entropy of processed data

[4] 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). April 24-26, 2019.

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Highlights

- static power of a selected CMOS sub-circuit can be modulated by a laser beam (the sub-circuit area is "selected")

→ visibility of the processed data in the device's power trace

- laser beam may be used to obtain potentially sensitive data processed by a combinational sub-circuit targeted by the laser beam
- the method has strong requirements
- approaches based on dual-rail logic cannot be used to fight against the potential attacks based on the presented method

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Thank You!
Work-In-Progress and Future Work

- research of the "cocktail effect" influence
- modulated static current variability modeling and simulation
- measurements using devices manufactured by using corresponding (in the field) technologies
- attack scenario formulation and validation

The author acknowledges 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.