FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

# Standard Cell Tuning Enables Data-Independent Static Power Consumption

Jan Bělohoubek, Petr Fišer, Jan Schmidt

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

Czech Technical University in Prague
Prague, Czech Republic

DDECS 2020

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

# Motivation
## Circuit Security

Research of physical circuit security:

- Physical attacks represent a great challenge for today's digital design
- Data dependency in CMOS static power and light-modulated static power – *Optical Beam Induced Current* (OBIC) – may be exploited
- Existing attack countermeasures widely adopted by industry are ineffective or inefficient
  - Dual-Rail encoding-based methods were introduced (into security area) to balance the **dynamic power**, not static power!
  - SecLib represents considerable area/delay overhead

# Motivation
## Data Dependency in CMOS

- Leakage is data dependent:
  - Alioto et al.; Giorgetti et al.; Moos et al. $\Longrightarrow$ **DPA is possible**
  - leakage data-dependency is harder to catch (compared to dynamic power) – it is normally deeply hidden in the *cocktail* of thousands of gates composing the digital circuit
  - gate leakage currents is in order of (tens of) **nanoamps**

- Photocurrent is data dependent:
  - we have shown, that the **static power data dependency** of the CMOS subcircuit may be **manifested by** using a (focused) **laser beam**
  - gate photocurrent is in order of (even hundreds of) **microamps**
  - increasing the order of the static current of the specific part of the circuit by the factor 4–5

# Motivation
## Eliminate the Dynamic Power Countermeasures

- Leakage attack:
  1. (optional) control the circuit clock (stop the clock to enlarge the measurement window)
  2. acquire a number of the circuit static power traces
  3. perform DPA as for dynamic power attack → get the secret
- Photocurrent attack:
  1. decapsulate the circuit
  2. (optional) control the circuit clock (stop the clock to enlarge the measurement window)
  3. illuminate the circuit/part of the circuit & acquire a number of the circuit static power traces
  4. perform DPA as for dynamic power attack → get the secret

FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

# Motivation
## Exploiting Static Power is Possible

⚠ Using Leakage

- + no circuit preparation is required
- + simple measurement setup (LNA must be employed)
- ± clock manipulation may help
- – measured leakage power is a cocktail of the whole circuit
- – leakages are low → **large power trace set** is required

⚠ Using Photocurrent

- – circuit must be decapsulated, the laser is used to initiate photocurrent in combinational logic
- + even simpler measurement setup (LNA may not be required)
- ± clock manipulation may help
- + measured current is the cocktail of the illuminated subcircuit
- + photocurrents are significant → **compact power trace set**
  - the required dataset size is comparable to dynamic power DPA (proven by simulation)

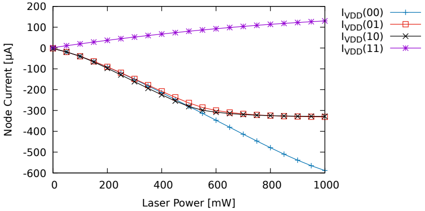
# Experimental Setup

- The TSMC180nm technology node is used
  - open standard cell library and SPICE models are provided by the Oklahoma State University (OSU)[1]
  - TSMC180nm does not represent the latest technology node, but it is still relevant for manufacturing devices like smart-cards or key-fobs
- SPICE models of CMOS under PLS by Sarafianos et al. were adopted
- Manufacturable circuit layout netlist is simulated
  - for layout synthesis, we use the open *digital synthesis flow* – *Qflow* (*Berkeley ABC*, *QRouter*, *GrayWolf* and *Magic*)
  - synthesized layouts were simulated in ngSPICE
- Models and experimental data are available on GitHub[2]

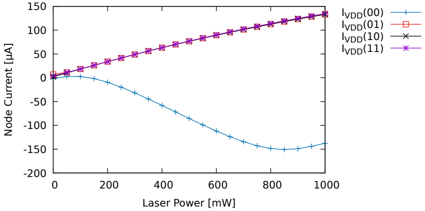
[1] https://vlsiarch.ecen.okstate.edu/flows/MOSIS_SCMOS

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

# Motivation
## Simulated Photocurrent for Bulk CMOS Gates

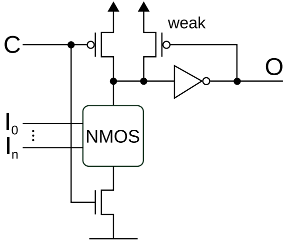


Photocurrent for `NAND2X1` for different input patters

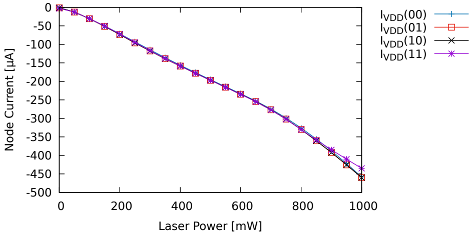


Photocurrent for `NOR2X1` for different input patters

# Existing Countermeasures
## Dynamic Domino Logic



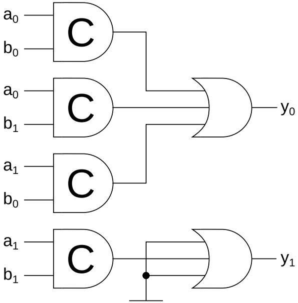
Footed domino logic gate employing standard *weak keeper*



Domino logic two-input AND gate power imprint

⚠ Dual-Rail ready, small area and data-independent response, but different design style

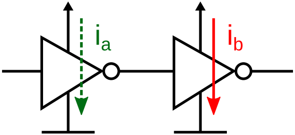
# Existing Countermeasures
## SecLib



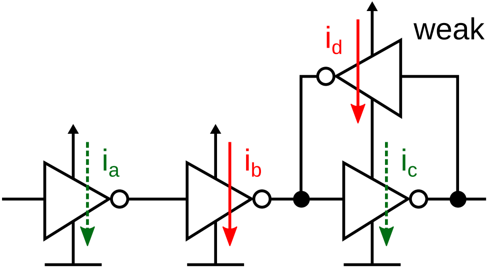
Secured 2-input NAND gate schematic: all input combinations at C-element inputs are represented; one C-element output is always equal to 1 and three remaining C-element outputs are always equal to 0

⚠ Dual-Rail ready, high symmetry and standard cell-based, but the significant area, delay, and power overhead

# Proposed Countermeasures
## Complementary Value Balancing



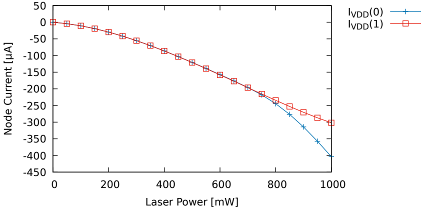
Two-inverter chain uses complementary power consumption to obtain a constant power imprint: $i_a + i_b = const$.



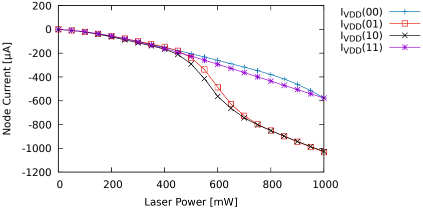
Three-inverter chain with feedback weak inverter uses the identical principle

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

# Proposed Countermeasures
## Complementary Value Balancing

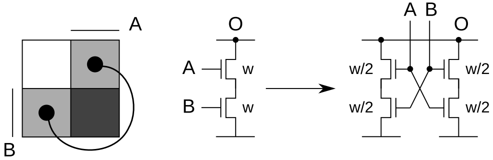


The power imprint of two-inverter chain: unmodified inverters from the TSMC180nm cell library were used



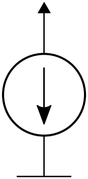
Two-input AND gate balanced by output inverter – 2x unmodified TSMC180nm inverters in parallel

# Adopted Countermeasure
## Increasing Transistor-Level Symmetry



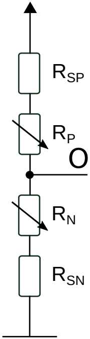
Removing asymmetries in CMOS to suppress the data dependence in leakage and OBIC induced by the *stack effect* asymmetric behavior. As the modified structure is functionally equivalent, the transistor sizes can be scaled down (if possible) without affecting the cell performance.

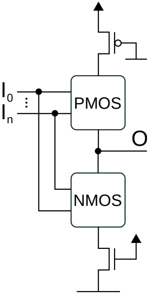
# Proposed Countermeasures
## Constant Current Source Approximation

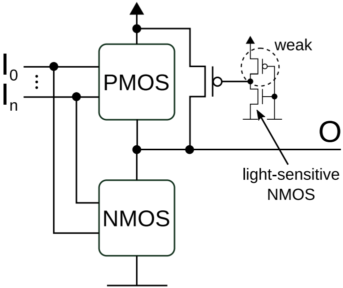


$R_{SP} > R_P$

$R_{SN} > R_N$

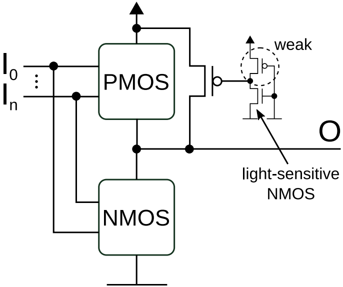






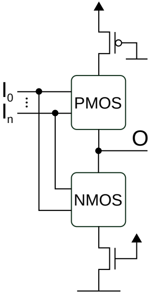
# Proposed Countermeasures
## Paralel Transistor Arrangement

- If permanently open, it has almost no influence during normal operation
- The parallel PMOS is closed by a light-sensitive inverter only in case of light-attack
- The parallel transistor decreases the significance of the data-dependent resistivity of the PMOS block

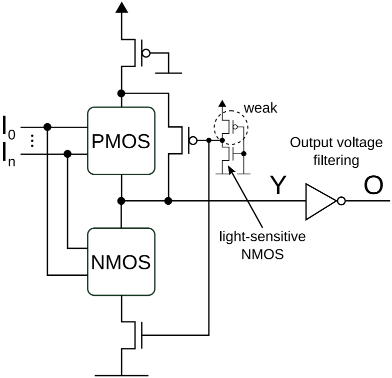


# Proposed Countermeasures
## Serial Transistor Arrangement

- If permanently closed, it has almost no influence during normal operation
- Effectively reduces the OBIC in case of illumination attack
- Disconnecting one of the rails is possible by using additional control → further decreasing the data dependency

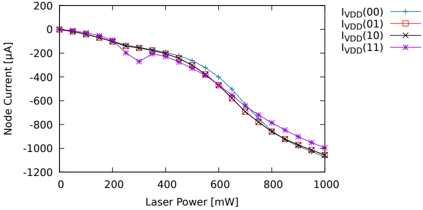


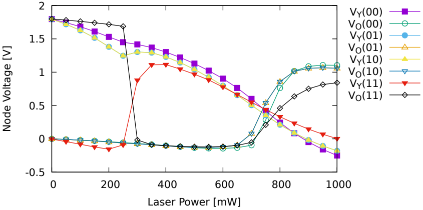
# Experimental Evaluation
## Completely Balanced Positive Gate



Completely balanced positive gate: the VSS rail is disconnected during the light attack and the output inverter serves for power balancing and as the output voltage filter at the same time

# Experimental Evaluation
# Completely Balanced AND Gate





Two-input AND gate completely balanced

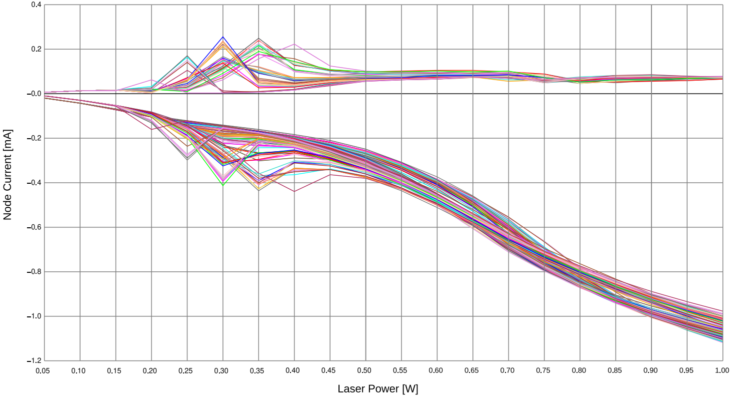
Two-input AND gate completely balanced is operational below ≈ 200mW

# Experimental Evaluation
## Proposed Approach Overhead Comparison

| Standard Cell Gate Description | Proposed Area | Proposed Delay | SecLib (dual-rail) Area | SecLib (dual-rail) Delay |
|---|---|---|---|---|
| Two-INV chain (buffer) | ≈200% | <200% | – | – |
| Three-INV chain with feedback | ≈400% | <300% | – | – |
| Custom protected AND2 | ≈200% | ≈110% | – | – |
| AND2 composed of std. cells only | >300% | <110% | ≈600% | ≈200% |
| Custom protected OR2 | ≈200% | ≈200% | – | – |
| OR2 composed of std. cells only | ≈160% | <120% | ≈600% | ≈200% |

Area/Delay overhead comparison of balanced gates with their std. equivalents and with SecLib in TSMC180nm

# Experimental Evaluation
## Robustness – Process Variations

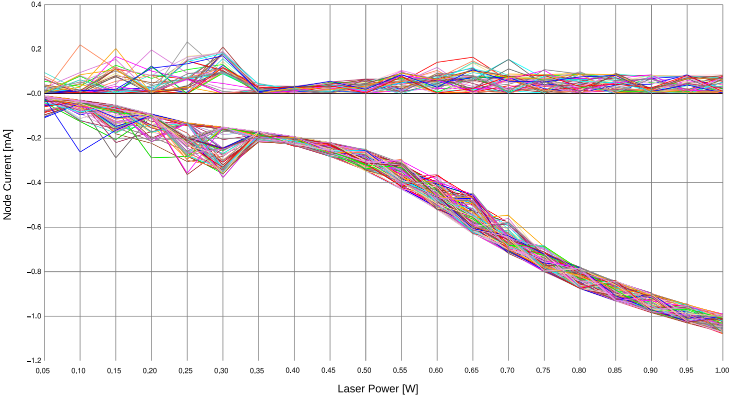


MonteCarlo simulation with different CMOS models[3] corresponding to 35 different MPW runs

[3] https://github.com/DDD-FIT-CTU/CMOS-SPICE-Model-Collections

FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

# Experimental Evaluation
## Robustness – Voltage Drops



MonteCarlo simulation with gate input voltage variances from [(0 - 0.3) V, (VDD + 0.3) V] corresponding to possible laser-induced voltage drops

# Highlights

- Principle of attacks on static power and OBIC are presented
- Overview of approaches usable for leakage and OBIC balancing is provided
- Novel flexible balancing structures surpassing the static bulk CMOS state-of-the-art approaches in area, delay and power are proposed
- The proposed structures may be combined with existing attack countermeasures to increase both static and dynamic power attack resistance

*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".*

*The novel structures presented in this paper are subject of the patent application.*