FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Standard Cell Design For Data-Independent Static Power Under Illumination

Jan Bělohoubek, Petr Fišer, Jan Schmidt

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

Czech Technical University in Prague
Prague, Czech Republic

PESW 2021

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 CPA or 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 CPA as for dynamic power attack → get the secret

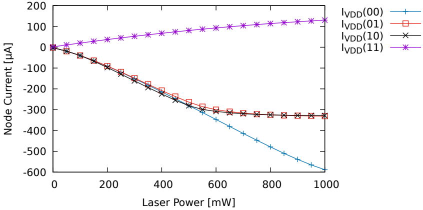
Experimental Setup

- 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]

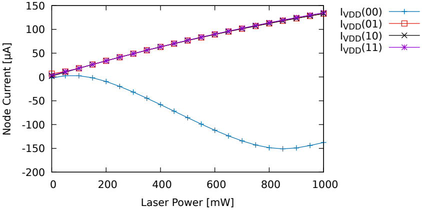
[1] https://vlsiarch.ecen.okstate.edu/flows/MOSIS_SCMOS

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

Motivation
Simulated Photocurrent for Bulk CMOS Gates

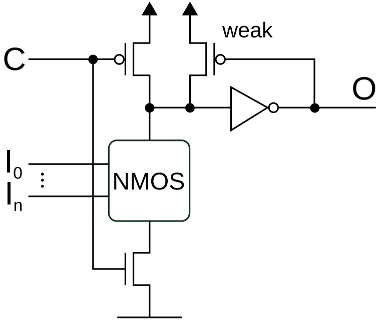


Photocurrent for NAND2X1 for different input patters

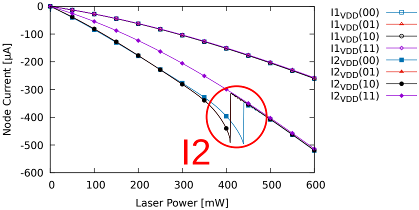


Photocurrent for NOR2X1 for different input patters

Existing Countermeasures (An Example)
Dynamic Domino Logic

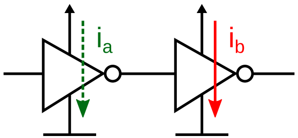


Footed domino logic gate employing standard *weak keeper*

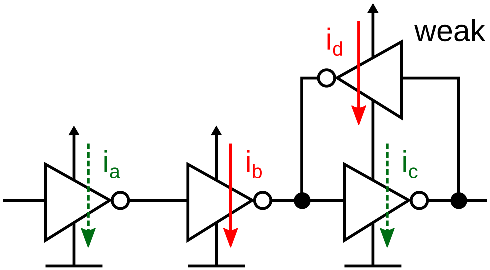


Domino logic two-input AND gate without keeper (I1) and with the standard weak-keeper (I2) power imprints

Proposed Countermeasures
Complementary Value Balancing

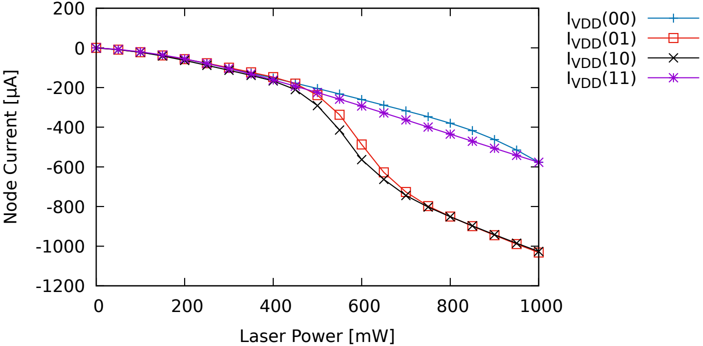


Two-inverter chain uses complementary power consumption to obtain a constant power imprint: $i_a + i_b = const.$



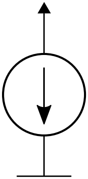
Three-inverter chain with feedback weak inverter uses the identical principle

Proposed Countermeasures
Complementary Value Balancing

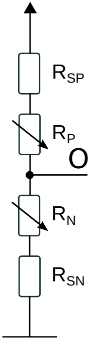


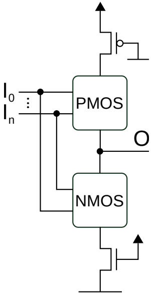
Two-input AND gate balanced by output inverter – 2x unmodified TSMC180nm inverters in parallel

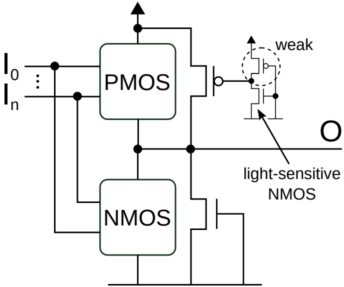
Proposed Countermeasures
Inspiration: Constant Current Source



$$R_{SP} > R_P$$
$$R_{SN} > R_N$$





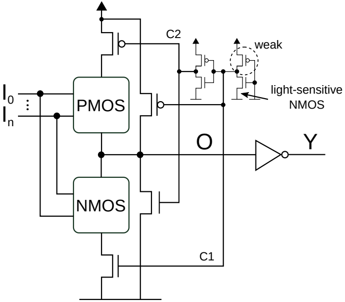


Proposed Countermeasures
Paralel Transistor Arrangement

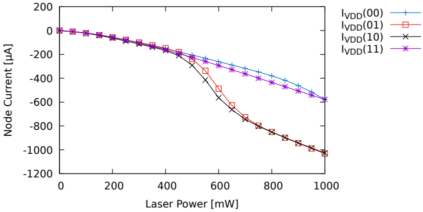
- Parallel structures (mostly) balance output inverter

- Serial structures size is minimized and can be disconnected to diminish data-dependency

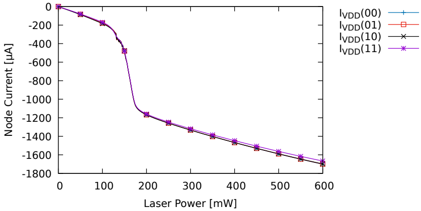
- Short-circuit in case of high illumination energy



Proposed Countermeasures
CMOS Cell Simulation

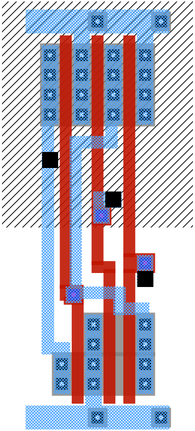


Two-input AND gate balanced by output inverter – 2x unmodified TSMC180nm inverters in parallel

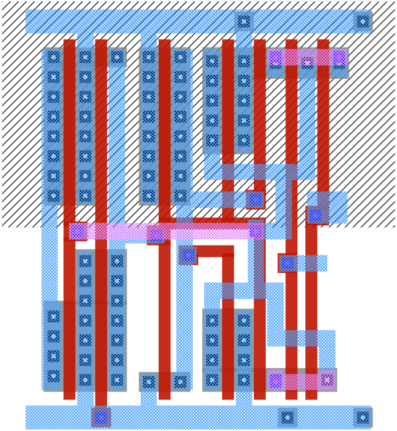


Proposed AND gate power imprint in TSMC180nm

Proposed Countermeasures
CMOS Cells



AND2X1

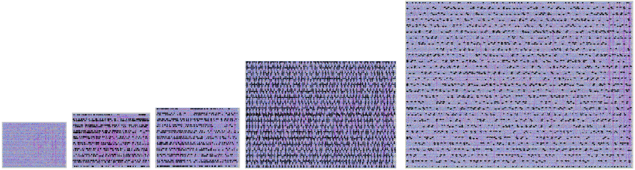


PAND2X1

Experimental Evaluation
AES SBOX Logic

- Core part of the SBOX cipher
- Larger combinational circuit – 866 NAND2 gates
- Variants under coparison:
  - *singleRail* employs only two-input NAND gates (`NAND2X1` and `INVX1`)
  - *dualRailAS* a non-conventional dual-rail implementation with alternating spacer
  - *dualRail* a conventional dual-rail implementation employing only two-input AND and OR gates (`AND2X1` and `OR2X1`)
  - *pDualRail* a conventional dual-rail implementation employing only proposed two-input AND and OR gates (`PAND2X1` and `POR2X1`)
  - *secLibDualRail* a protected implementation employing secLib gates based on six dynamic C-elements and library cells (`INVX1` and `OR3X1`)

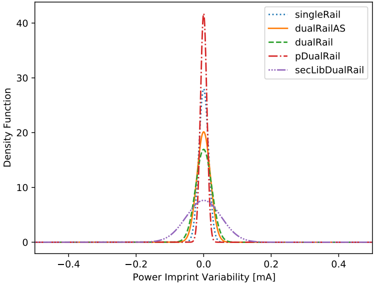
Experimental Evaluation
Proposed Approach Overhead Comparison



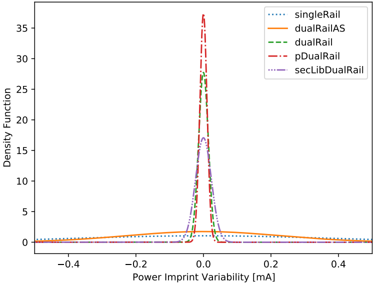
Size comparison of different SBOX implementations. From left to the right: singleRail, dualRailAS, dualRail, pDualRail (proposed), secLibDualRail

SBOX implementation	Area [mm^2]	Delay [ns]
singleRail	0.038 (100%)	≈ 9 (100%)
dualRailAS	0.057 ≈150%	≈ 11 (≈120%)
dualRail	0.066 (≈170%)	≈ 11 (≈120%)
pDualRail	0.158 – 0.196 (≈400% – 530%)	≈ 12 (≈130%)
secLibDualRail	0.294 – 0.431 (≈780% – 1150%)	≈ 15 (≈ 160%)

Experimental Evaluation
Probability Density Functions – Conventional



Subthreshold Leakage



Dynamic Power

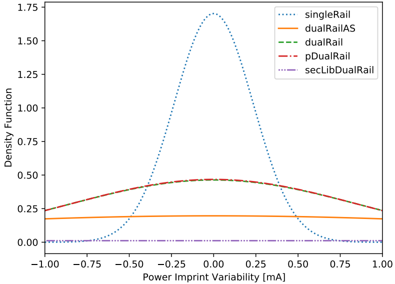
⚠ Smaller data-dependent parts in the protected implementation

→ smaller parasitics

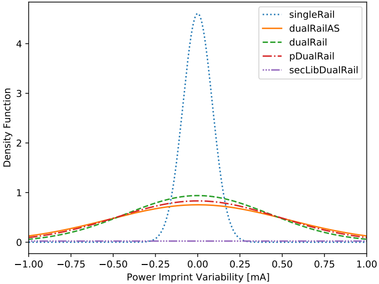
→ lower leakage

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Experimental Evaluation
Probability Density Functions – PLS



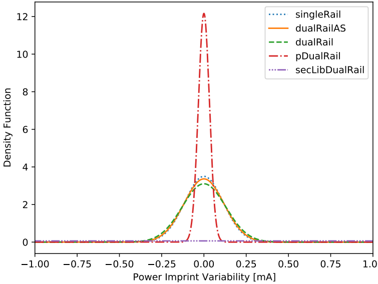
300 mW



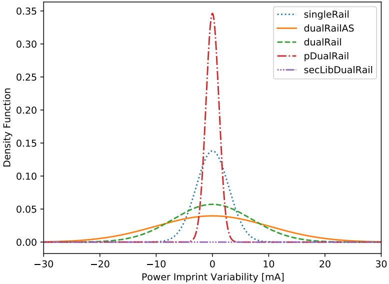
150 mW

⚠ Smaller might be better (the sensitive area)

Experimental Evaluation
Probability Density Functions – PLS



50 mW



600 mW

⚠ Protected implementation wins in the low-energy and in the hard-to-survive regions

Highlights

- Protected CMOS cells proposed and evaluated at the cell- and circuit-level
- Cell Design Rules were Proposed
- SecLib vulnerability was described – *omitted in this talk*
- Positive Impact to both static and dynamic power vulnerability

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.