FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Testability and Physical Security: The Cell-Level Approach

Jan Bělohoubek

jan.belohoubek@fit.cvut.cz

Department of Digital Design
Faculty of Information technology
Czech Technical University in Prague

Supervisor: doc. Ing. Petr Fišer, Ph.D.
Advisor: doc. Ing. Jan Schmidt, Ph.D.

January 14 2022

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

Introduction and Motivation

- Testability, Reliability, and Security and their interplay are hot topics in today digital design
- The aim of the thesis is a study of circuit-level approaches reacting to reliability and security issues
- Low-level approaches may influence system properties a lot:
  - reliability conditioned by increased testability
  - security conditioned by current balancing
- Minor topic touched by the thesis targets also the increase in understanding of the reliability-security interplay:
  - how increased reliability may affect the circuit security

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Outline

1. Testability and Design for Test
   - Introduction and Motivation
   - Contributions
     - A Short-Duration Offline Test
     - Time-Extended Duplex
2. Circuit Physical Security
   - Introduction and Motivation
   - Contributions
     - Novel CMOS Design Threat
     - Novel Protected CMOS Cells
3. Publications of the Author
4. Reviewers' Comments

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Outline

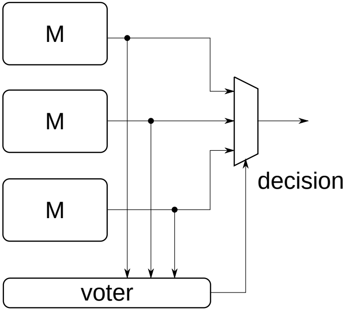
Introduction and Motivation
Testability and Design for Test

- Conventional circuit tests tend to be long and have limited fault coverage

→ controlability vs. observability

- A complete and really short test can reduce area and power of error-correcting scheme replacing TMR

Introduction and Motivation
Testability and Design for Test



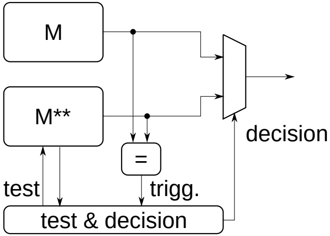
Conceptual scheme of an error-correcting Triple-Modular redundancy (TMR)

- traditional approach employs area redundancy to enable error masking

Introduction and Motivation
Testability and Design for Test

- an alternative approach employs a short-duration offline test to detect faulty part of the module and enable error masking
- 100% fault-coverage with an accurate fault model gives good evidence about the error-free module in the duplex error-correcting scheme

→ `M**` is fast offline-testable



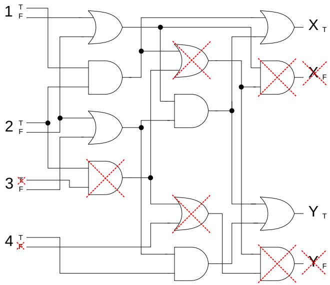
Conceptual scheme of proposed error-correcting Time-Extended Duplex (TED)

Contributions of the Thesis
Testability and Design for Test

- The Short-duration offline test[1]
→ may be incorporated into the normal computation flow[1]
→ *monotonicity* removes fault symptom masking → enabled by dynamic logic
→ *indication principle* holds if every gate output is connected to at least one AND and one OR gate → enabled by reconfigurable CMOS structures[2]
- A method for designing a system with increased reliability incorporating the proposed short-duration offline-test[2]
→ a Time-Extended Duplex (TED) system concept was described and evaluated in detail[2]

[1] DSD'15 [A.3], DSD'16 [A.4], MICPRO'17 [A.1]
[2] DSD'16 [A.4], MICPRO'17 [A.1]

Contributions of the Thesis (1)
Short-Duration Offline Test: Monotonicity



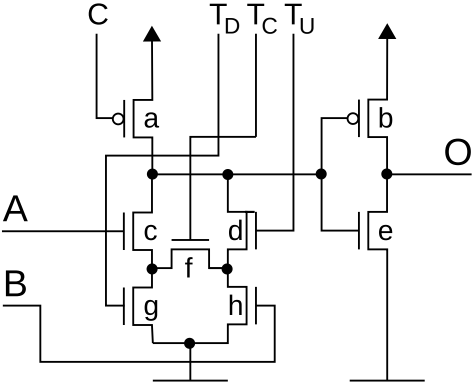
Dual-rail logic circuit derived from the sinle-rail one represents `M**`

Every `NAND` gate was replaced by an `AND` and `OR` gate pair[1].

The crossed-out gates, and IOs were choosen not to be used by the reduction heuristic

[1] DSD'15 [A.3], DSD'16 [A.4], MICPRO'17 [A.1]

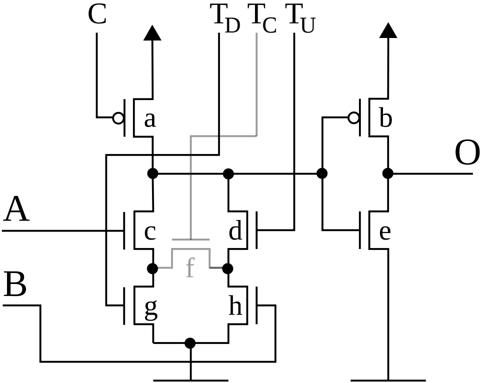
Contributions of the Thesis (1)
Short-Duration Offline Test: Indication



- Domino-logic AND/OR gate with increased controlability[1]

[1] DSD'16 [A.4], MICPRO'17 [A.1]

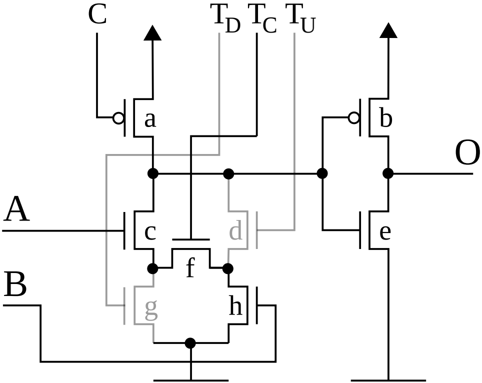
Contributions of the Thesis (1)
Short-Duration Offline Test: Indication



- Domino-logic OR gate $T_D = 1,\ T_C = 0,\ T_U = 1$

[1] DSD'16 [A.4], MICPRO'17 [A.1]

Contributions of the Thesis (1)
Short-Duration Offline Test: Indication



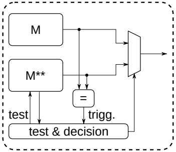
- Domino-logic AND gate $T_D = 0,\ T_C = 1,\ T_U = 0$

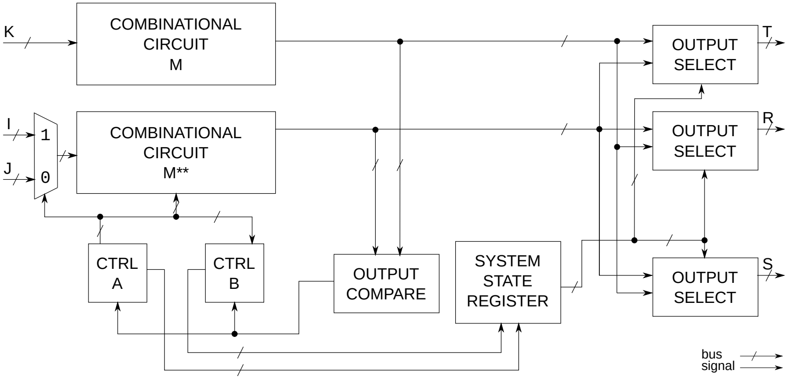
[1] DSD'16 [A.4], MICPRO'17 [A.1]

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Contributions of the Thesis (2)

Time-Extended Duplex





A high-level scheme of the Time-Extended Duplex[1]

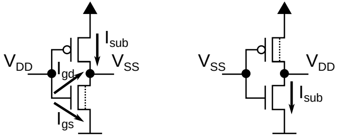
[1] DSD'16 [A.4], MICPRO'17 [A.1]

Outline

Introduction and Motivation
Circuit Physical Security

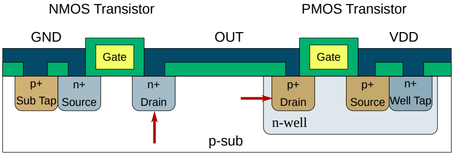
- Physical attacks represent a great challenge for today's digital design
- Data dependency in CMOS static power and light-modulated static power – *Optical Beam Induced Current* (OBIC) – may be exploited
- Existing hiding attack countermeasures adopted by industry or proposed by academia are ineffective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

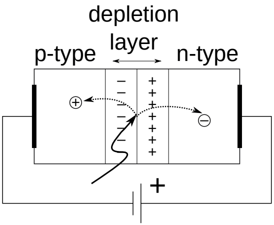
Introduction and Motivation
Circuit Physical Security



a) b)

a) The closed NMOS transistor experiences a gate leakage and open PMOS experiences subthreshold leakage current;
b) the open NMOS transistor experiences subthreshold leakage current





OBIC is induced in the illuminated reverse-biased PN junction

Contributions of the Thesis
Circuit Physical Security

- A novel CMOS design threat[2]

→ the proposed attack combines combinational logic illumination and static power measurement – proved by simulation[3]

→ arises especially in redundant structures like voters[4]

→ endangers also dynamic power countermeasures based on balancing[3]

[2] DSD'19 [A.5], DDECS'19 [A.6], MicRel'21 [A.2]
[3] DSD'19 [A.5], MicRel'21 [A.2]
[4] DDECS'19 [A.6]

Contributions of the Thesis
Circuit Physical Security

- Circuit-level (standard-cell level) attack countermeasures – novel CMOS cells[5]

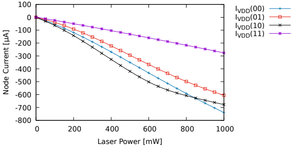
→ may replace conventional CMOS cells in the common design process

→ cell properties were confirmed by simulation

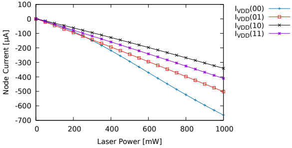
→ a case study on the AES SBOX design was provided[6]

[5] DDECS'20 [A.7], CZ 308895 B6, 2021 [A.12], MicRel'21 [A.2]
[6] MicRel'21 [A.2]

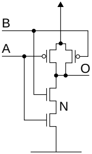
Contributions of the Thesis (3)
Novel CMOS Design Threat Identified



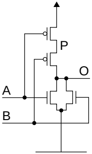
(a) NAND2X1



(b) NOR2X1



(c) NAND2

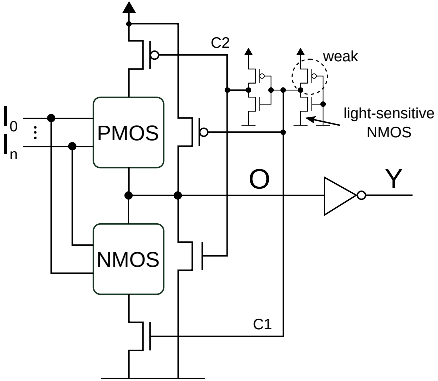


(d) NOR2

Simulated power imprints for standard cells in TSMC180nm library – the area is uniformly illuminated[2]

[2] DSD'19 [A.5], DDECS'19 [A.6], MicRel'21 [A.2]

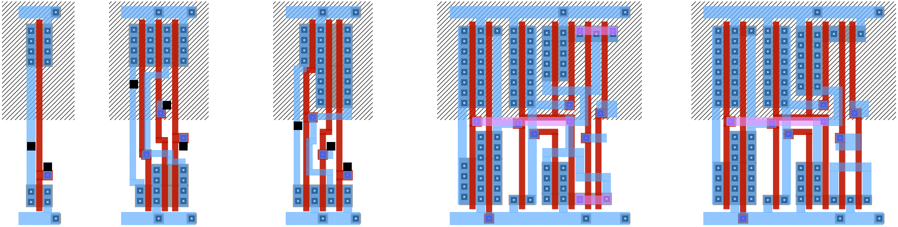
Contributions of the Thesis (4)
Novel Protected CMOS Cells



Completely balanced positive gate[5]

[5] DDECS'20 [A.7], CZ 308895 B6, 2021 [A.12], MicRel'21 [A.2]

Contributions of the Thesis (4)
Novel Protected CMOS Cells



Standard cells in TSMC180nm: (a) `INVX1`, (b) `AND2X1` and (c) `OR2X1` from the TSMC180nm library provided by Oklahoma State University (OSU); and proposed [A.2, A.7]: (d) `PAND2X1` and (e) `POR2X1`

Summary

1. A short-duration offline test
   - → tens of clock cycles
   - → special domino-like CMOS cell required
2. Time-Extended Duplex
   - → overcomes TMR for bigger circuits (area and power)
3. A novel CMOS design threat
   - → balancing protection schemes are ineffective (including WDDL or SecLib)
   - → subcircuits may amplify the leakage (voters)
4. Circuit-level attack countermeasures – novel CMOS cells
   - → compact footprint; no process tunning required

Outline

Publications of the Author

- Reviewed relevant publications
  - 2 journal articles: A.1 (2 cit.), A.2 (1 cit.)
  - 5 international conference papers: A.3 (1 cit.), A.4, A.5, A.6, A.7 (1 cit.)
  - 4 other reviewed papers: A.8 – A.11
- Relevant patents
  - 1 national patent: A.12
  - 1 running international patent (EPO) submission: A.12
- Other relevant publications: A.13 – A.20

- Other reviewed publications
  - 1 international conference paper A.21 (2 cit.)
- Other publications: A.22 – A.24

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Publications of the Author
Reviewed Relevant Publications

A.1 J. Bělohoubek, P. Fišer and J. Schmidt Error Masking Method Based On The Short-Duration Offline Test. Microprocessors and Microsystems (MICPRO), Elsevier, vol. 52, pp. 236-250, ISSN: 0141-9331, July 2017.

> R. Panek, J. Lojda, J. Podivinsky, and Z. Kotasek Partial Dynamic Reconfiguration in an FPGA-based Fault-Tolerant System: Simulation-based Evaluation, IEEE East-West Design & Test Symposium (EWDTS) 2018, Kazan, Russian Federation, 2018.

> Arista Networks Inc. Logic Buffer for Hitless Single Event Upset Handling. Inventors: D. A. Cananzi, E. B. Van Hartingsveldt, M. Romain. U.S. Patent No 10,997,011 B2, 2021.

A.2 J. Bělohoubek, P. Fišer and J. Schmidt Optically Induced Static Power in Combinational Logic: Vulnerabilities and Countermeasures. Microelectronics Reliability, Elsevier, vol. 124, ISSN: 0026-2714, September 2021.

> A. Kumar, S. L. Tripathi, and U. Subramaniam: Variability Analysis of SBOX With CMOS 45 nm Technology, Wireless Personal Communications, 2021, 1-12.

A.3 J. Bělohoubek, P. Fišer and J. Schmidt Novel C-Element Based Error Detection and Correction Method Combining Time and Area Redundancy. Euromicro Conference on Digital System Design (DSD), 2015, Funchal, Madeira – Portugal, 2015.

> J.-P. Anderson Duplicate with Choose: Using Statistics for Fault Mitigation Dissertation, Brigham Young University, BYU Scholars Archive, 2016.

Publications of the Author
Reviewed Relevant Publications

A.4 J. Bělohoubek, P. Fišer and J. Schmidt Error Correction Method Based On The Short-Duration Offline Test. 2016 Euromicro Conference on Digital System Design (DSD), Limassol, Cyprus, 2016.

A.5 J. Bělohoubek, P. Fišer and J. Schmidt CMOS Illumination Discloses Processed Data. 22nd Euromicro Conference on Digital Systems Design (DSD), Kallithea - Chalkidiki , Greece, 2019.

A.6 J. Bělohoubek, P. Fišer and J. Schmidt Using Voters May Lead to Secret Leakage. 2019 22nd IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS), Cluj-Napoca, Romania, 2019.

A.7 J. Bělohoubek, P. Fišer and J. Schmidt Standard Cell Tuning Enables Data-Independent Static Power Consumption. 23rd IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS), Novi Sad, Serbia, 2020.

  > F. Bijan, T. Moos and A. Moradi BSPL: Balanced Static Power Logic, IACR Cryptology ePrint Archive, 2020.

A.8 J. Bělohoubek Novel Error Detection and Correction Method Combining Time and Area Redundancy. Počítačové architektury a diagnostika 2015, Zlín, Czech Republic, 2015.

Publications of the Author
Reviewed Relevant Publications

A.9 J. Bělohoubek Využití rychlého offline testu v systému se schopností maskování jedné chyby. Počítačové architektury a diagnostika 2016, Kraví Hora - Bořetice, Czech Republic, 2016.

A.10 J. Bělohoubek Error Correction Method Based on the Efficient Offline Test. A Doctoral Study Report submitted to the Faculty of Information Technology, Prague, Czech Republic, 2016.

A.11 J. Bělohoubek Zvyšování spolehlivosti a bezpečnosti číslicových obvodů na úrovni mikroarchitektury. Počítačové architektury a diagnostika 2018, Churáňov, Czech Republic 2018.

Publications of the Author
Relevant patents

A.12 Czech Technical University in Prague Connection of a standard CMOS cell with reduced data dependence of static consumption. Inventors: J. Bělohoubek, P. Fišer and J. Schmidt. Czech Republic. Patent No CZ 308895 B6, 2021.

- European patent (EPO) submission is running

Publications of the Author
Other relevant publications

A.13 J. Bělohoubek and J. Schmidt Fully asynchronous QDI implementation of DES in FPGA. Cryptographic architectures embedded in reconfigurable devices (CryptArchi), Annency, France, 2014 (unpublished lecture).

A.14 J. Bělohoubek Novel gate design method for short-duration test. POSTER 2015, Prague, Czech Republic, 2015.

A.15 J. Bělohoubek The Design-Time Side-Channel Information Leakage Estimation. Cryptographic architectures embedded in reconfigurable devices (CryptArchi), Smolenice, Slovakia 2017 (unpublished lecture).

A.16 J. Bělohoubek, P. Fišer and J. Schmidt Effect of Power Trace Set Properties to Differential Power Analysis. TRUDEVICE 2018, Dresden, Germany, 2018.

A.17 J. Bělohoubek and R. Vik Low-Cost CMOS Power Consumption Data Dependency Demonstrator Concept. The 7th Prague Embedded Systems Workshop, Roztoky u Prahy, Czech Republic, 2019.

A.18 J. Bělohoubek and J. Schmidt CMOS Illumination Enables Observation of Processed Data in Power Traces. Workshop on Practical Hardware Innovations in Security Implementation and Characterization, Gardanne, France, 2019.

A.19 J. Bělohoubek Modulated CMOS Static Power is Data Dependent and Observable. Cryptographic architectures embedded in reconfigurable devices (CryptArchi), Pruhonice, Czech Republic 2019 (unpublished lecture).

A.20 J. Bělohoubek, P. Fišer and J. Schmidt Standard Cell Design For Data-Independent Static Power Under Illumination. The 9th Prague Embedded Systems Workshop, Roztoky u Prahy, Czech Republic, 2021.

Publications of the Author
Other publications

A.21 J. Bělohoubek, J. Čengery, J. Freisleben, P. Kašpar, A. Hamáček KETCube – the Universal Prototyping IoT Platform. 21st Euromicro Conference on Digital System Design (DSD), Prague, Czech Republic, 2018.

> Alsukayti, Ibrahim S. An Internet-of-Things Educational Platform, International Journal of Computer Science and Network Security (IJCSNS) 2019, Seoul, South Korea, 2019.
>
> S. Douglas, K. Gary and S. Sohoni Impact of a Virtualized IoT Environment on Online Students, IEEE Frontiers in Education Conference (FIE) 2020, Uppsala, Sweden, 2020.

A.22 J. Bělohoubek Smart re-use of hardware peripherals for better software UART. The 3rd Prague Embedded Systems Workshop, Roztoky u Prahy, Czech Republic, 2015.

A.23 J. Bělohoubek KETCube – the Prototyping and Educational Platform for IoT Nodes. The 6th Prague Embedded Systems Workshop, Roztoky u Prahy, Czech Republic, 2018.

A.24 L. Menšík, R. Vik, S. Pretl, J. Bělohoubek, T. Syrový, L. Syrová, L. Kubáč, L. Menšík Možnosti uplatnění internetu věcí (IoT) v precizním zemědělství v ČR. Úroda 12/2019, pp. 341-350., ISSN: 0139-6013, 2019.

Highlights

- A short-duration offline test
- Time-Extended Duplex was proposed and evaluated
- A novel CMOS design threat
- Circuit-level attack countermeasures – novel CMOS cells

The author acknowledges the support of GA16-05179S of the Czech Grant Agency, CTU grants SGS14/105/OHK3/1T/18, SGS15/119/OHK3/1T/18, SGS16/121/OHK3/1T/18, SGS17/213/OHK3/3T/18, and the OP VVV MEYS funded project CZ.02.1.01/0.0/0.0/16_019/0000765.

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Outline

Common Remark

- Thesis are not completely self-containing
  - missing a complete overview of fault models
  - chapter 3
  - authors' publications were often referenced

→ this is mostly true, as I was concerned about covering topics and state-of-the-art closely related to contributions of the thesis, thus some of the side branches potentially enriching the context were omitted

Comments A I
prof. Michel Renovell

- Testing terminology used in Chapter 2 – all terms are not common

→ consistency reasons lead to term-mixing from both areas (one term was selected or common term was used) – e.g. *symptom*, *cocktail*

Comments A II
prof. Michel Renovell

- Area-increase estimation of the configurable gate

→ we drew no layout, but we did a rough logical-effort-based model of proposed gates used for quantitative comparison, which was published in DSD 2016 [A.4] and MICPRO [A.1]

gate	input capac-itance	output cur-rent	precharge delay	internal delay	area
NAND_{static}	4.5	1	-	-	9
inverter_{static}	3.5	1	-	-	3.5
AND_{domino}	1.0	0.4	5.0	6.0	6.0
OR_{domino}	1.0	0.4	5.0	4.0	6.0
$\text{AND}_{proposed}$	1.0	0.4	5.0	6.0	8.0
$\text{OR}_{proposed}$	1.0	0.4	5.0	4.0	8.0

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Comments A III
prof. Michel Renovell

- TMR-TED comparison with domino logic only

→ we employed domino-only comparison, as it is fair

→ inter-paradigm comparison discriminates one or another side and would be biassed – the comparison would finaly collapse to *domino vs. anything*, e.g. *domino vs. static*

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Comments B I
prof. Milos Krstic

- Silicon verification of proposed attack and countermeasures

→ silicon verification is a pending work-in-progress

→ we initiated the communication with group of Jean-Max Dutertre from EMSE, Centre Microélectronique de Provence, but the collaboration unfortunately stalled

→ any collaboration opportunity is welcome

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Comments B II
prof. Milos Krstic

- Comment the benefits of the short-duration test compared to the state of the art approaches (e.g. scan-based)

→ the short-duration test control is more complex, but the test generation/compaction logic is simpler; the advantage would be the area, but main pros are in the time-domain, or lower test-time overheating, and lower power (test length)

- How to detect transient faults near the clock edge?

→ the output voters are triplicated

Comments B III
prof. Milos Krstic

- How to handle metastability?

→ could not be completely avoided, but the duplex comparator should signalize the problem and in such a case recomputation will be probably initiated, and the output voters are triplicated

- Comparison to partial duplication approaches

→ we did a brief review and we discussed the comparison to the Modified Duplex Scheme employing parity bit co-generation, but comparison to the TMR was selected from didactic reasons

Comments B IV
prof. Milos Krstic

- Overhead of the AES block needs some explanation (Table 5.2)

→ the countermeasure is (mostly) *paid by area*, not by time or dynamic power

From left to the right: singleRail, dualRailAS, dualRail, pDualRail (proposed), secLibDualRail (optimized)

Comments B V
prof. Milos Krstic

- Technology scaling and variants like FDSOI or FinFET

→ technology scaling will increase the number of irradiated cells but subcircuit targeting is still possible

→ denser structures and/or metalization is generally a great issue and de-facto an intrinsic countermeasure

→ FDSOI could have a significant advantage for the attacker, as the data-unrelated and structure-dependent source of the parasitic photocurrent is removed compared to BULK CMOS – substrate-well PN junction

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Comments C I
prof. Amir Moradi

- 3.3.3 gives a misleading impression to the reader that the method can remove half of the logic, but later it is explained that the reduction is lower in practice

→ 50% gate reduction is hard to achieve in practice, but possible in a special case – the best case was announced

- Routing complexity of additional control signals in domino logic

→ detailed description of the problem was avoided due to the fact that this problem is addressed in domino logic itself even it is more complex here, as there are more control signals

Comments C II
prof. Amir Moradi

- Why was domino logic chosen?

→ domino logic allows to implement more complex structures with lover area (and delay) overhead than common static CMOS and lead to simpler CMOS structures (inside of the cell is simpler to test)

→ the original short-duartion offline test proposed in [A.3] employed dynamic but not domino logic: it employes C-element-like datapaths, it employs preset and evaluation phases, and it requires less control signals which are not timing/routing critical, but it offers 100% fault-coverage with respect to stuck-at fault model only

Comments C III
prof. Amir Moradi

- → the usability of the static CMOS will probably lead to significantly increased area overhead, and the short-duration offline test in static CMOS is still an open question
- → exotic approaches may offer a testability bonus (in a constrained area)

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Comments C IV
prof. Amir Moradi

- DPA/CPA basics description is informal as like as the proposed attack

→ there are deficiences in the formal description

- Hiding approaches are preferred even they do not sound compared to masking

→ I completely agree that the fact is mostly ignored in the introduction. Masking was only briefly noticed, as the primary aim of the thesis is related to hiding. Theoretical security of hiding is generally low, but it offers straight and low-overhead solutions especially for constrained devices.

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Comments C V
prof. Amir Moradi

- Figures 4.4 and 4.5 are misleading

→ VDD – VSS NMOS connection is the testcircuit, not a real CMOS gate. Figures are for illustration only and they do not represent real connection in ASIC, but they represent a possible state of transistors – in context of a real CMOS gate, VDD actually means *voltage close to VDD*

- Experiments are hard to replicate – a lot of noise

→ we discussed this in the community and the conclusion was that it is feasible even challenging. Problem is that we currently miss experimental results and experience with experiment setup

Comments C VI
prof. Amir Moradi

- Targeting single cell in recent technology is NOT possible

→ this is true and I completely agree. It is feasible in the technology used for evaluation (TSMC180nm + OSU libs). Older technologies are still sound in specific applications. Targeting subcircuits would be possible also in recent technology – we presented the vulnerability originally on the voter circuit

- Attacks presented in 4.4.2 and 4.4.3 are highly ad-hoc

→ the intuitive approach was proposed for ideal-case-attack only. CPA algorithm was proposed as an established way to exploit OBIC

Comments C VII
prof. Amir Moradi

- Footed domino logic is not clearly described

→ footed domino logic is a standard even an exotic approach – the reference is there

- All results are based on simulations only

→ This is a pending future work

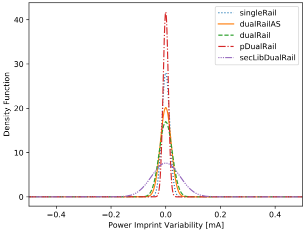
FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Comments C VIII
prof. Amir Moradi

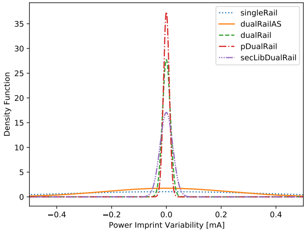
- New techniques are not compared to static/dynamic power attacks

→ comparison was briefly mentioned in the discussion and the AES case study, but the emphasis was on the – subthreshold leakage balancing is increased and parasitic capacitances are smaller. In terms of hiding, the proposed countermeasures have a positive impact n both static and dynamic power balancing

Comments C IX
prof. Amir Moradi



(e) Static Power



(f) Dynamic power

Selected density functions (PDF) for power imprints of all implementations - a narrower curve means a better protection.