Evaluation of the Masked Logic Style MDPL on a Prototype Chip

Thomas Popp, Mario Kirschbaum, Thomas Zefferer

Graz University of Technology
Institute for Applied Information Processing and Communications (IAIK)
Side-Channel Analysis Lab

Stefan Mangard

Infineon Technologies AG Munich
Security Innovation

Presentation Outline

Introduction

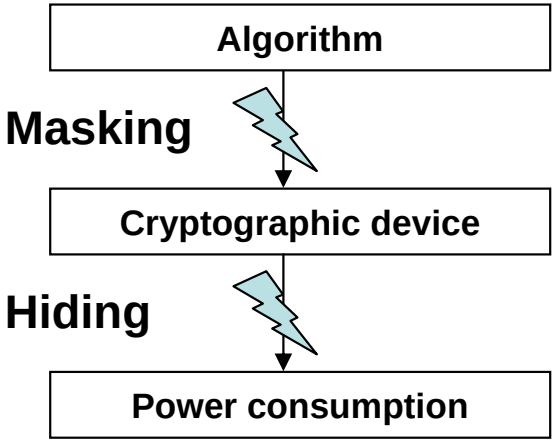
SCARD Chip Analysis

MDPL Problem Analysis

Improvements of MDPL: iMDPL

Conclusions

Introduction (1/3)



DPA Countermeasures

- Hiding, Masking ($v_m = v * m$)
- Levels: Protocol, Architecture, Cell

Cell-level countermeasures

- Typically a significant increase in area and power consumption
- Cells from scratch/based on common standard cells
- Suitability for semi-custom design? (constraints)
- Various limiting factors, e.g.:
  - Timing constraints - enable signals
  - Balancing of complementary wires
  - Glitches
  - Early propagation

Introduction (2/3)

The early propagation effect (EPE)

- Generating the output “as soon as possible” and not until all input signals are “valid”
  - E.g.: OR gate with one input = 1
- Moment of switching (power consumption) becomes data-dependent
- Affects both hiding and masked logic styles
  - Cells based on common standard cells

Suzuki and Saeki analyzed the EPE for MDPL

- Practical verification on FPGA

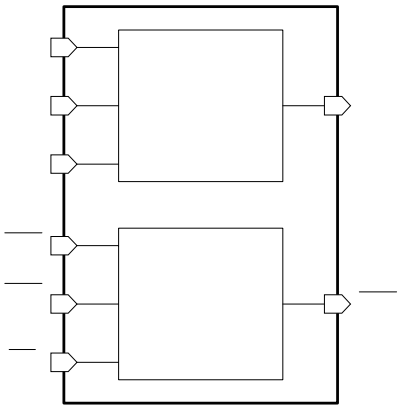
We confirmed the findings for an MDPL-ASIC

Introduction (3/3)

MDPL

- Masked: for DPA resistance
  - one mask m for all signals: $d = d_m \oplus m$
- Dual-rail pre-charged: to avoid glitches
- Mask switches encoding on complementary wires
  - No need for perfect balancing

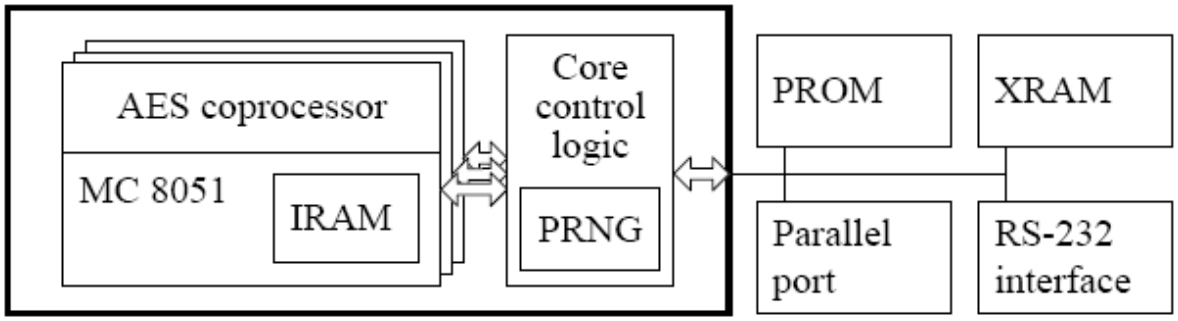
Line no.	a_m	b_m	m	q_m	$\overline{a_m}$	$\overline{b_m}$	$\overline{m}$	$\overline{q_m}$
1	0	0	0	0	1	1	1	1
2	0	0	1	0	1	1	0	1
3	0	1	0	0	1	0	1	1
4	0	1	1	1	1	0	0	0
5	1	0	0	0	0	1	1	1
6	1	0	1	1	0	1	0	0
7	1	1	0	1	0	0	1	0
8	1	1	1	1	0	0	0	0

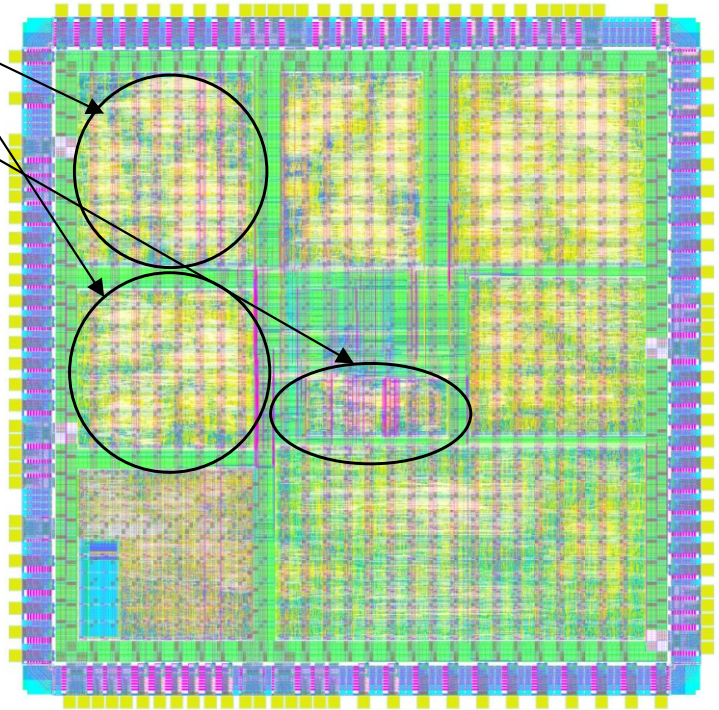


SCARD Chip Analysis (1/3)

The SCARD chip

- 8051-compatible MC with AES-128 coprocessor
- Implemented in CMOS, MDPL, DRP-variant (custom cells, parallel routing, no EPE)
- PRNG provides mask bit
- Used clock: 3.686 MHz





SCARD Chip Analysis (2/3)

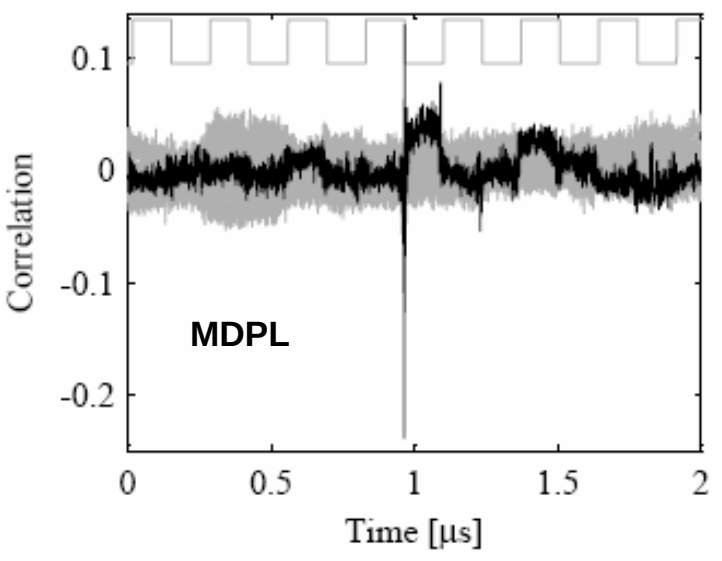
MDPL 8051-microcontroller shows significant DPA weaknesses

- suffers from EPE
- MDPL AES coprocessor still not broken
  - Up to 3 million measurements
  - Needs further investigations

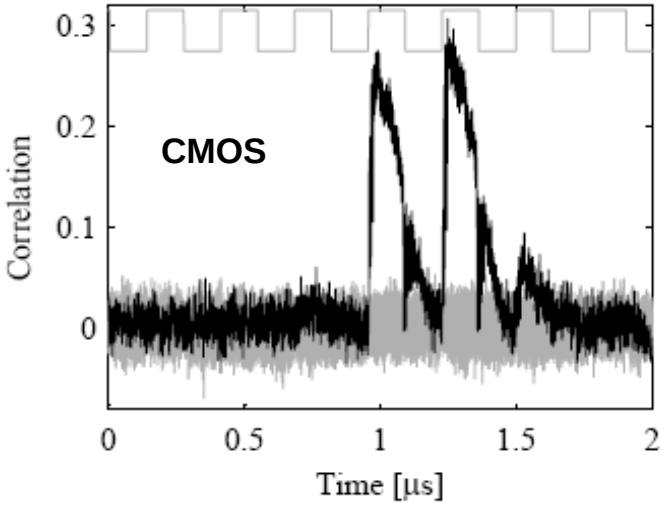
DPA Attack

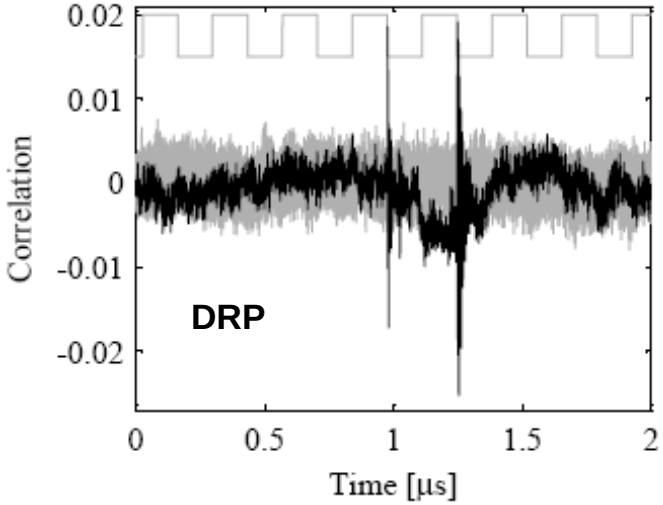
- MOV byte in registers (destination cleared beforehand)
- H = HW(moved_byte)
- Digital sampling oscilloscope
  - 1 GHz bandwidth, 4 GS sampling rate
  - Differential probe in V_{DD} line over 10 Ω resistor

SCARD Chip Analysis (3/3)



	Used power traces	Highest absolute correlation peak	Required power traces
CMOS	5000	0.3068	279
DRP	300000	0.0253	43201
MDPL	5000	0.2385	471





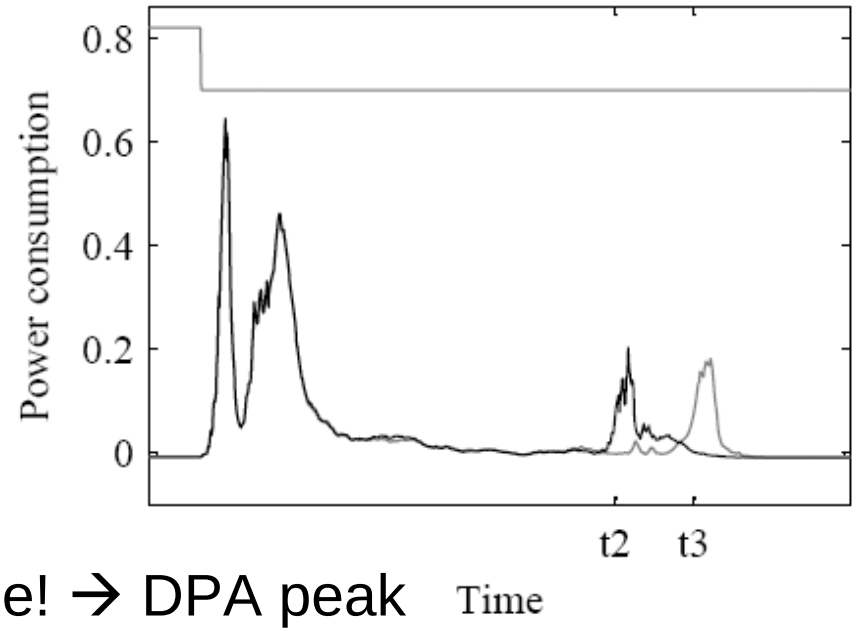
MDPL Problem Analysis (1/4)

Find Reason for MDPL DPA-leakage

- Transistor-level simulations (Synopsys Nanosim)
  - No interconnect parasitics
- Parts of the 8051-MC that are involved in the MOV

MDPL core simulation

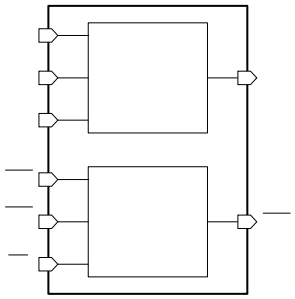
- Moving 0x00 (black) and 0xFF (gray) with mask=0
- Clock cycle in which the correlation peak occurred
- $t_3 - t_2 \approx 1$ ns
- Picture for random mask the same! → DPA peak

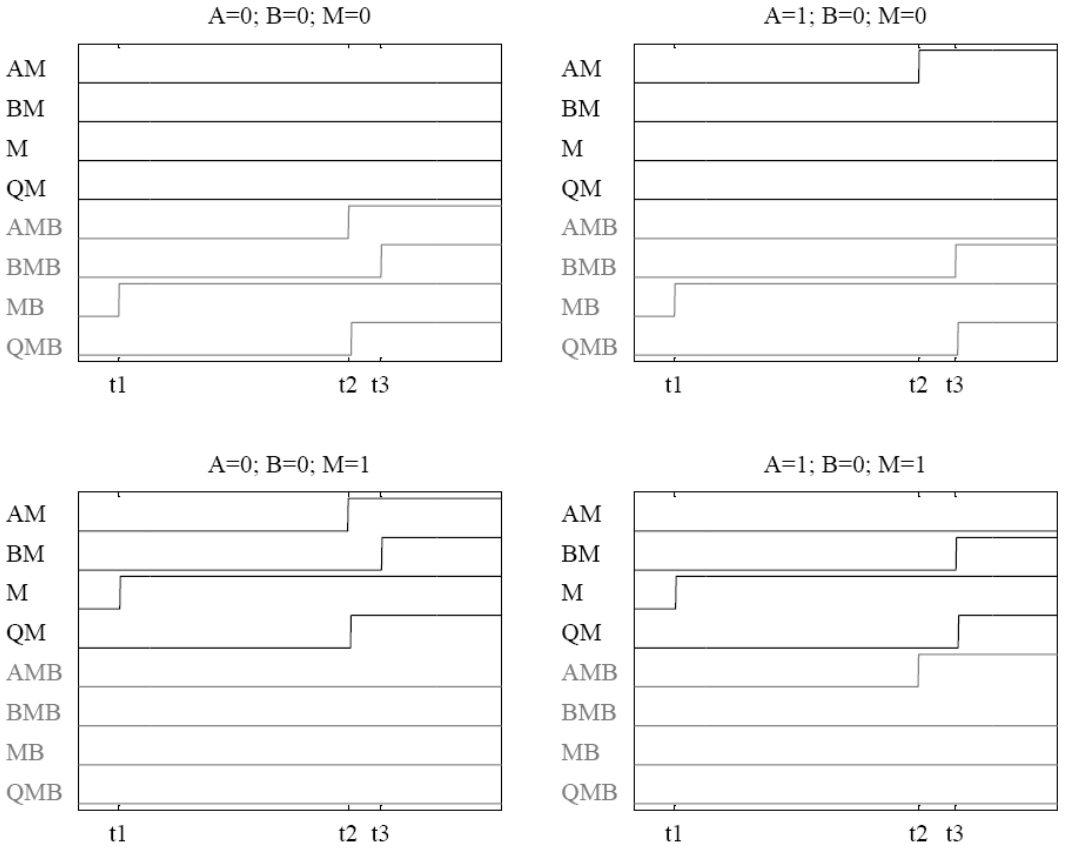


MDPL Problem Analysis (2/4)

What causes $t_3 - t_2 \approx 1$ ns?

- We found many MDPL-AND cells with the following settings in the clock cycle of interest
  - M: arrives at t_1
  - A: depends on moved byte, arrives at t_2
  - B: constant 0, arrives at t_3 (longer path)
- Mask changes only the Majority cell that switches





MDPL Problem Analysis (3/4)

Suzuki and Saeki showed the occurrence of leakage for a more general case

- Input B can also be variable

Many MDPL cells behave in the same way

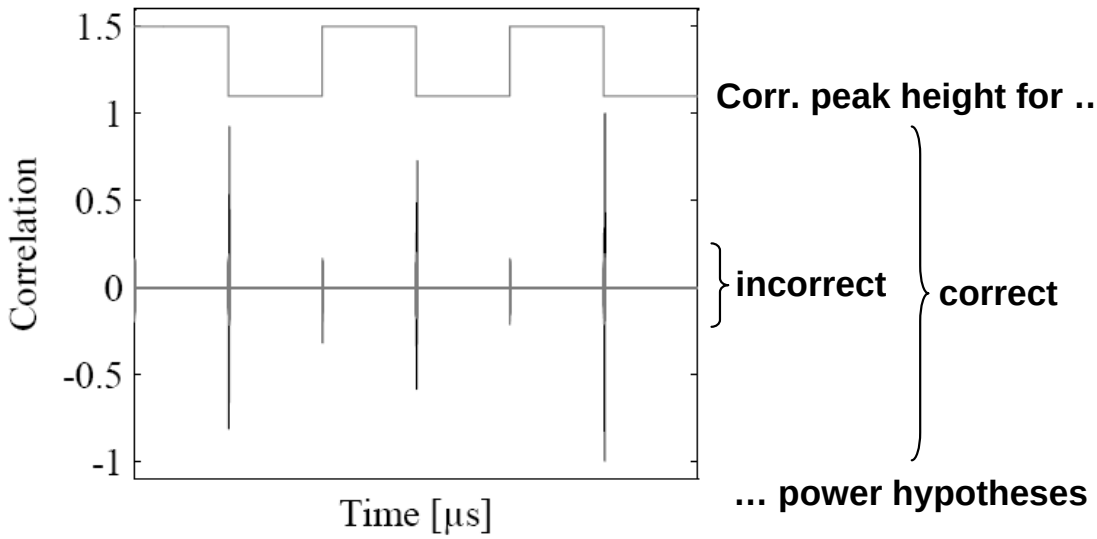
- Other 7 bits
- Other MDPL-AND cells in a similar setting
- Other MDPL cells are fed with the data-dependently delayed signals

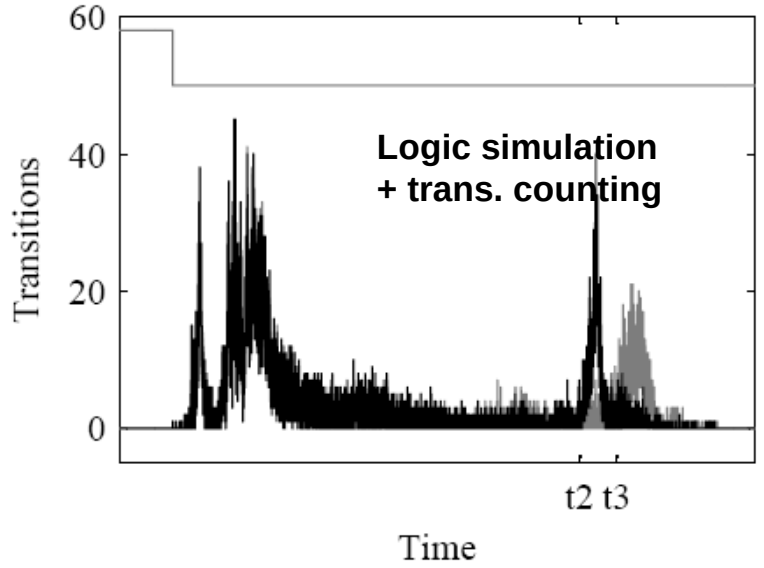
- ➔ Hundreds of MDPL cells behave in a data-dependent manner

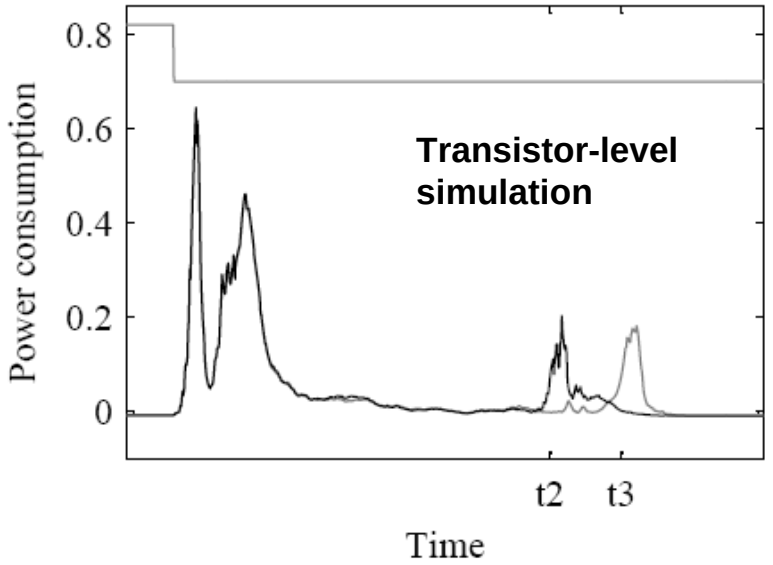
MDPL Problem Analysis (4/4)

DPA on simulated power traces

- Use logic simulation + transition counting
  - Significant speed-up
  - Verify MDPL improvements





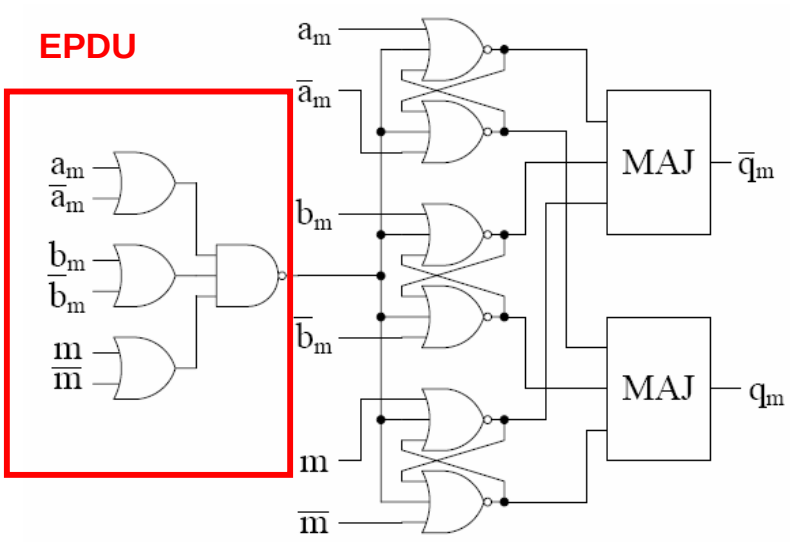


Improvements of MDPL: iMDPL (1/3)

Avoid early propagation

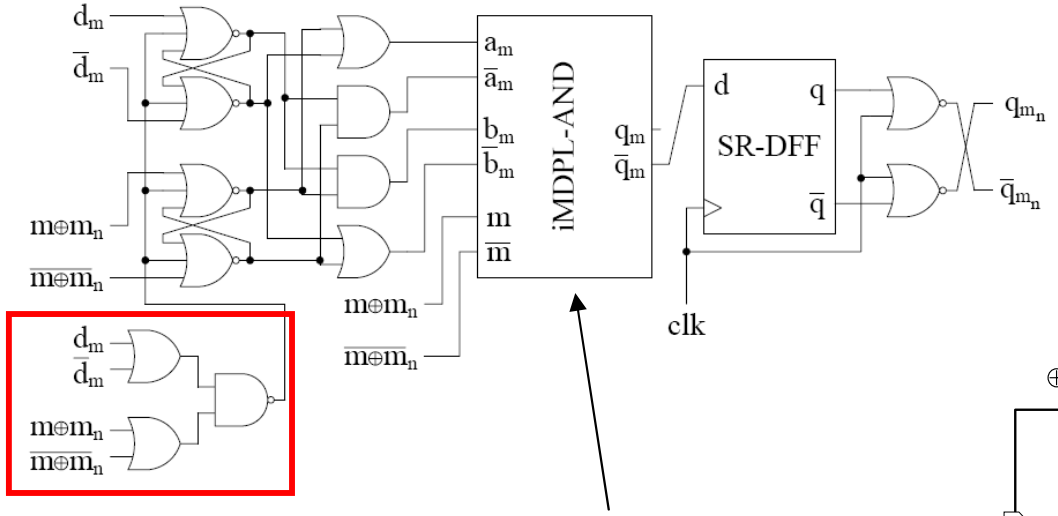
- In the precharge and the evaluation phase
- DRSL presented by Chen and Zhou avoids early propagation only in the evaluation phase
- Use SR-latches to stop signals until all have arrived in a differential manner
- Cells of an iMDPL-AND must be connected in a balanced way
  - Only internally

iMDPL-AND:



Improvements of MDPL: iMDPL (2/3)

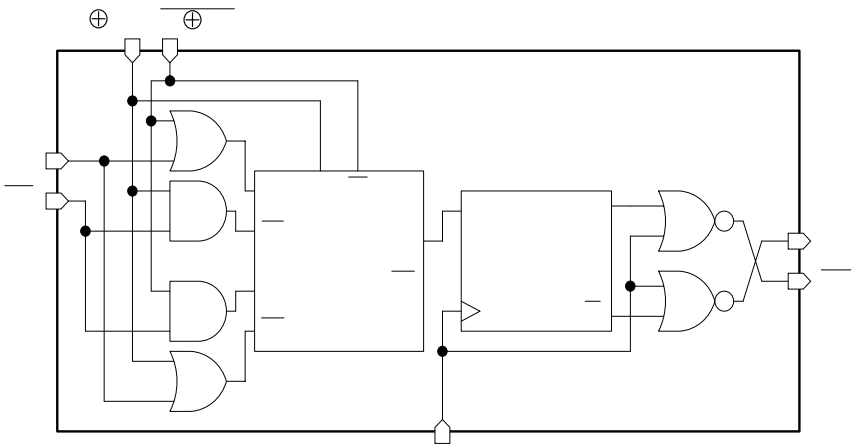
iMDPL-DFF:



EPDU

iMDPL-AND used as an iMDPL-NAND

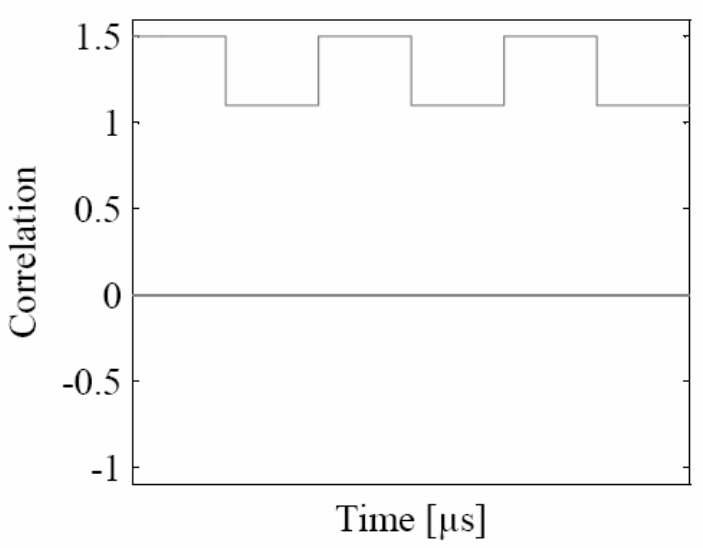
Original MDPL-AND cell:



Improvements of MDPL: iMDPL (3/3)

DPA on simulated power traces

- iMDPL netlist
- MOV instruction
- Logic simulation + transition counting
- Ideal flat line



iMDPL circuit properties

- Area: ~ 3x MDPL (~15x CMOS)
- Speed: ~1/3x MDPL (~1/6x CMOS)
- Power: ~1.5x MDPL (~ 5x – 10x CMOS)

Conclusion and Future Work

Early propagation is another severe problem for DPA-resistant logic styles

MDPL suffers from early propagation

- Verified for ASIC
- But problem seems not to occur always (see AES coprocessor)

iMDPL

- Huge
  - Use it only for critical parts (e.g. non-linear function like S-boxes) that cannot be protected by architectural masking
- Still built from common CMOS standard cells

IAIK

Graz University of Technology

The Side-Channel Analysis Lab

http://www.iaik.tugraz.at/research/sca-lab

Side-Channel Analysis Lab