Masked Dual-Rail Pre-Charge Logic

DPA-Resistance without Routing Constraints

Thomas Popp, Stefan Mangard

Side-Channel Analysis Lab

VLSI

Presentation Outline

- Introduction
- Problems of Current DPA-Resistant Logic Styles
- MDPL Cells and Circuits
- Experimental Results
- Conclusions and Future Work

Introduction

- Differential Power Analysis (DPA)
  - Implementation attack, side-channel attack
  - Used side channel: power consumption
  - Exploits data-dependency of a device’s power consumption to get the secret key

Introduction

- DPA countermeasures overview
  - Protocol level
    - e.g. ephemeral keys
  - Algorithmic level
    - e.g. masked algorithms
  - Architectural level
    - e.g. noise engines, random delay cycles
  - Gate level
    - Dual-rail pre-charge (DRP) logic styles
    - Masking logic styles

Introduction

- DPA-resistant logic styles overview
  - Advantages
    - Hardware/software designers almost completely freed from considering DPA
    - “push-button” solution (semi-custom design)
  - Examples:
    - DRP: SABL, WDDL (C. Tiri et al.)
    - Masking: RSL (D. Suzuki et al.)

Masking CMOS Logic

Standard CMOS Logic

d_{t-1}	d_t	Energy	Probability
0	0	E_{00}	p_{00}
0	1	E_{01}	p_{01}
1	0	E_{10}	p_{10}
1	1	E_{11}	p_{11}

Transitions of the value *d* of a node

Masked CMOS Logic

Line no.	d_{t-1}	m_{t-1}	$d_{m_{t-1}}$	d_t	m_t	d_{m_t}	Energy	Probability
1	0	0	0	0	0	0	E_{00}	$\frac{1}{4}p_{00}$
2	0	0	0	1	1	0	E_{00}	$\frac{1}{4}p_{01}$
3	1	1	0	0	0	0	E_{00}	$\frac{1}{4}p_{10}$
4	1	1	0	1	1	0	E_{00}	$\frac{1}{4}p_{11}$
5	0	0	0	0	1	1	E_{01}	$\frac{1}{4}p_{00}$
6	0	0	0	1	0	1	E_{01}	$\frac{1}{4}p_{01}$
7	1	1	0	0	1	1	E_{01}	$\frac{1}{4}p_{10}$
8	1	1	0	1	0	1	E_{01}	$\frac{1}{4}p_{11}$
9	0	1	1	0	0	0	E_{10}	$\frac{1}{4}p_{00}$
10	0	1	1	1	1	0	E_{10}	$\frac{1}{4}p_{01}$
11	1	0	1	0	0	0	E_{10}	$\frac{1}{4}p_{10}$
12	1	0	1	1	1	0	E_{10}	$\frac{1}{4}p_{11}$
13	0	1	1	0	1	1	E_{11}	$\frac{1}{4}p_{00}$
14	0	1	1	1	0	1	E_{11}	$\frac{1}{4}p_{01}$
15	1	0	1	0	1	1	E_{11}	$\frac{1}{4}p_{10}$
16	1	0	1	1	0	1	E_{11}	$\frac{1}{4}p_{11}$

DPA attack

$$\mathcal{E}(DM_{d_t}) = \mathcal{E}(M_{d_t=1}) - \mathcal{E}(M_{d_t=0})$$

$$= \frac{p_{11}E_{11} + p_{01}E_{01}}{p_{11} + p_{01}} - \frac{p_{00}E_{00} + p_{10}E_{10}}{p_{00} + p_{10}}$$

$$\neq 0$$

$$\mathcal{E}(M_{d_t=0}) = \mathcal{E}(M_{d_t=1}) = \frac{1}{4}(E_{00} + E_{01} + E_{10} + E_{11})$$

$$\mathcal{E}(DM_{d_t}) = 0$$

CMOS Logic:

$$E_{00} \approx E_{11} \ll E_{10} \neq E_{01}$$

Problems of Current DPA-Resistant Logic Styles

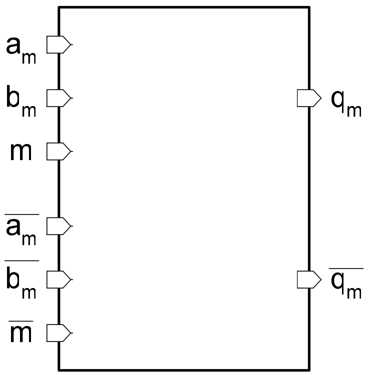
- Usability in semi-custom design flows
  - Design and characterization of new standard cells required
  - Tough constraints, e.g.
    - balancing of complementary wires (DRP)
    - careful timing of enable signal chains (RSL)
- Masking: glitches in masked CMOS circuits reduce its DPA resistance
  - RSA 2005: Mangard, Popp, Gammel

Masked Dual-Rail Pre-Charge Logic

- MDPL
  - Masked: for DPA resistance
    - one mask m for all signals: $d = d_m \oplus m$
  - Dual-rail pre-charged: to avoid glitches
  - Based on common standard cells
  - No tough constraints
    - no balanced wiring required
  - Suitable for semi-custom design

MDPL Combinational Cells

- MDPL AND



$$q_m = ((a_m \oplus m) \wedge (b_m \oplus m)) \oplus m$$

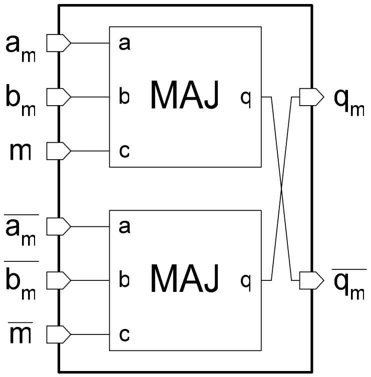
$$\overline{q_m} = ((\overline{a_m} \oplus \overline{m}) \wedge (\overline{b_m} \oplus \overline{m})) \oplus \overline{m}$$

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

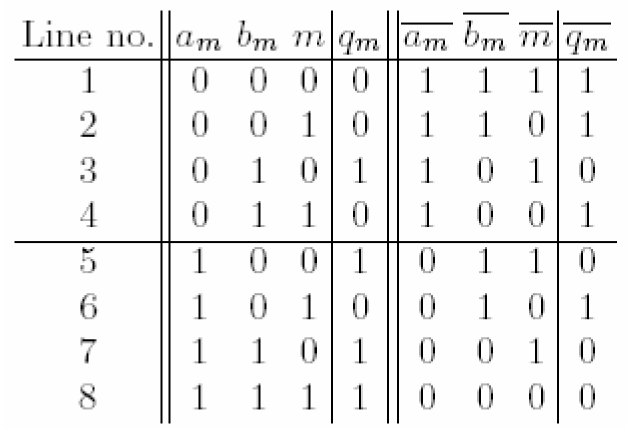
  - pre-charge wave propagates correctly
  - no glitches: monotonic transitions, MAJ is a monotonic increasing (positive) function

MDPL Combinational Cells

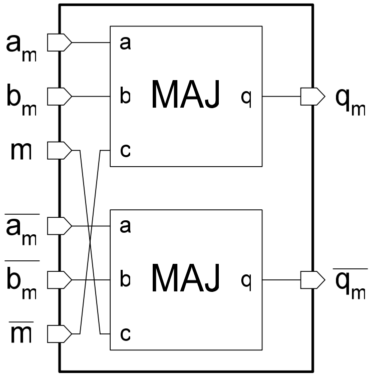
- MDPL NAND



- MDPL OR (MDPL NOR)

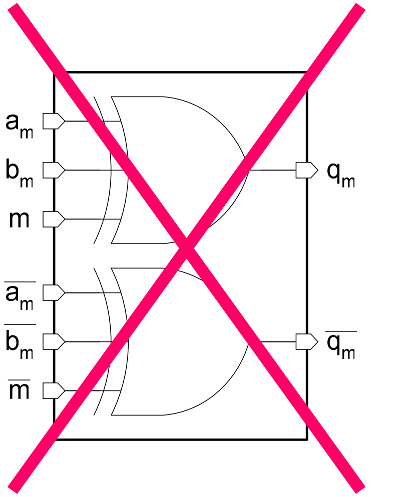


Line no.	a_m	b_m	m	q_m	$\overline{a_m}$	$\overline{b_m}$	$\overline{m}$	$\overline{q_m}$
1	0	0	0	0	1	1	1	1
2	0	0	1	0	1	1	0	1
3	0	1	0	1	1	0	1	0
4	0	1	1	0	1	0	0	1
5	1	0	0	1	0	1	1	0
6	1	0	1	0	0	1	0	1
7	1	1	0	1	0	0	1	0
8	1	1	1	1	0	0	0	0

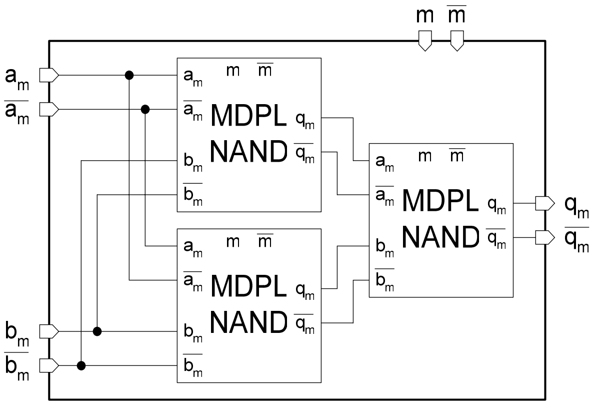


MDPL Combinational Cells

- MDPL XOR (MDPL XNOR)

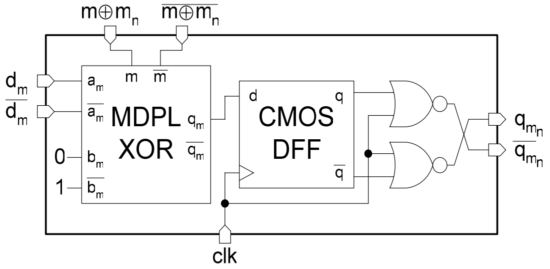


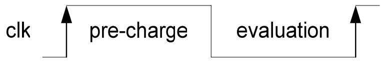
GLITCHES !!!



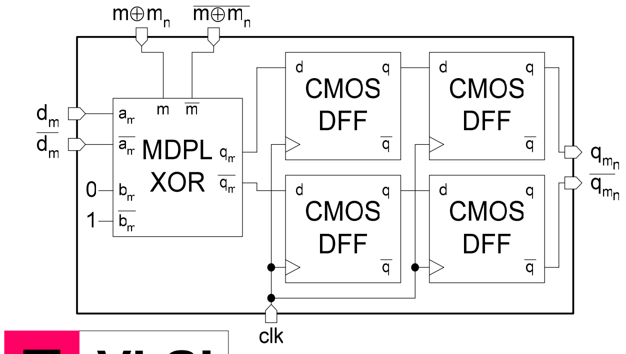
MDPL Sequential Cells

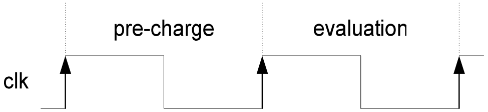
- MDPL DFF
  - performs mask switching (m, m_n)
  - starts pre-charge wave



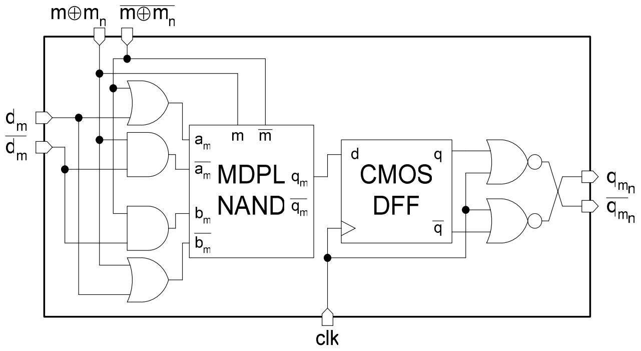


MDPL DFF that stores the pre-charge wave:





MDPL DFF with optimized MDPL XOR:

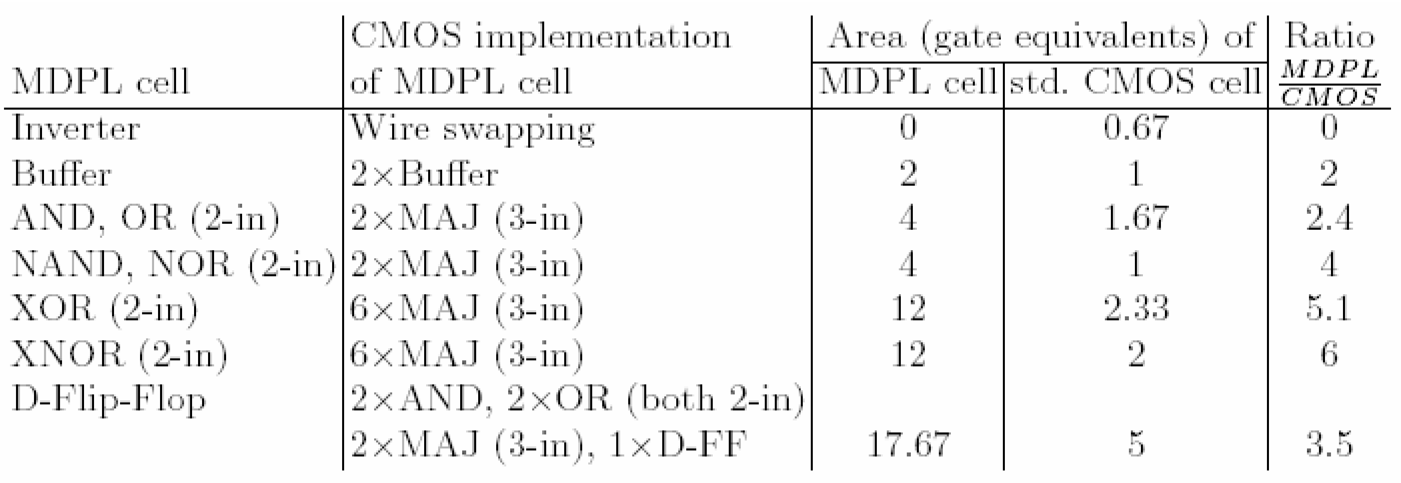


MDPL Cells Implementations

- Possibilities
  - **Out of common standard cells**
    - **cheap**
    - but not optimal:
      - time-of-evaluation of MAJ gate
      - not all internal nodes of the MAJ gate are pre-charged
  - New “CMOS” standard cells
  - New “DRP” standard cells
    - mask considered in differential pull-down network

MDPL Cells Summary

- MDPL cells and their CMOS implementations (austriamicrosystems C35B3 standard cell library)

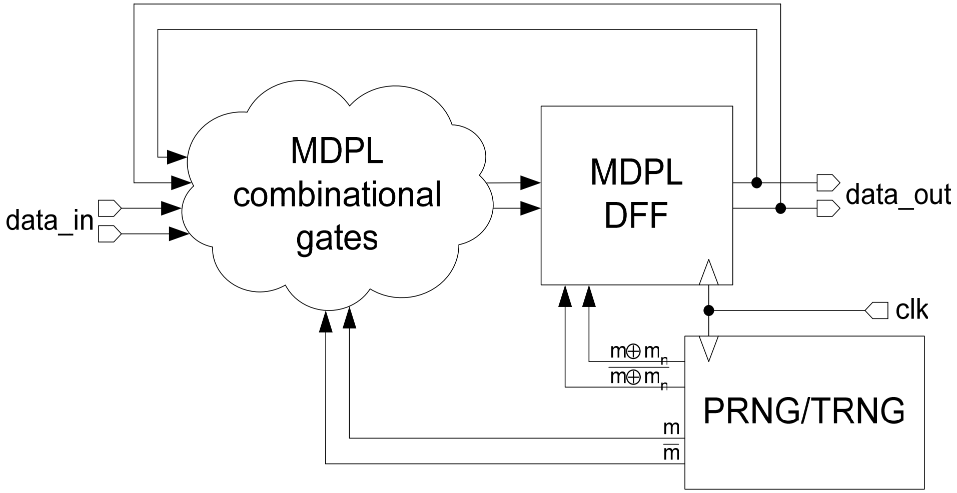


MDPL cell	CMOS implementation of MDPL cell	Area (gate equivalents) of		Ratio
		MDPL cell	std. CMOS cell	$\frac{MDPL}{CMOS}$
Inverter	Wire swapping	0	0.67	0
Buffer	2×Buffer	2	1	2
AND, OR (2-in)	2×MAJ (3-in)	4	1.67	2.4
NAND, NOR (2-in)	2×MAJ (3-in)	4	1	4
XOR (2-in)	6×MAJ (3-in)	12	2.33	5.1
XNOR (2-in)	6×MAJ (3-in)	12	2	6
D-Flip-Flop	2×AND, 2×OR (both 2-in) 2×MAJ (3-in), 1×D-FF	17.67	5	3.5

- Indicates 4 to 5 times area increase

MDPL Circuits

- General architecture
  - 1 mask for the whole circuit, changed every clock cycle
  - SPA on mask nets not possible

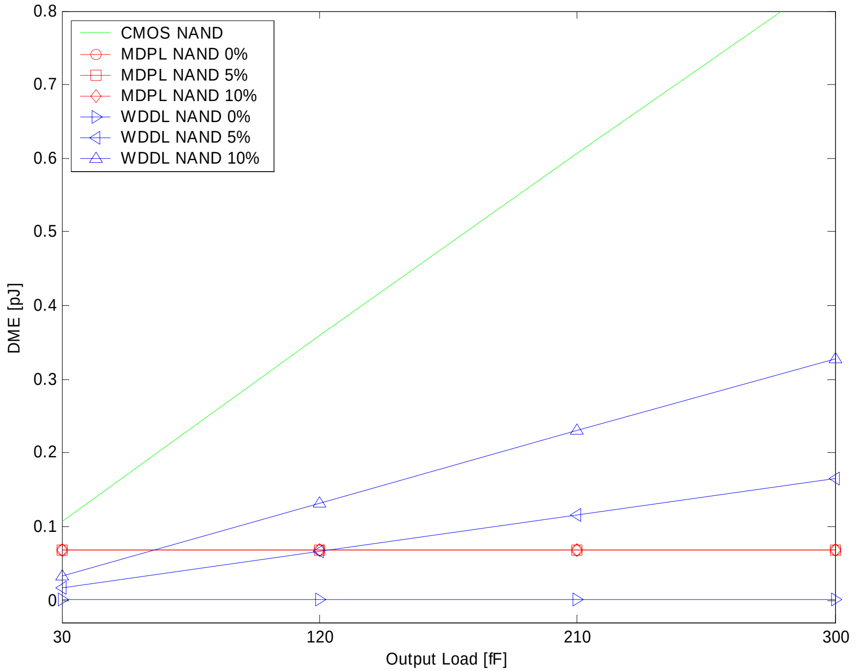


MDPL Circuits

- MDPL semi-custom design
  - HDL high-level design
  - Synthesis
    - restrict available standard cells
  - Logic style conversion
    - cell output load OK?
      - replace CMOS cells by corresponding MDPL cells
      - removal of inverters
    - insertion of CMOS <-> MDPL interface circuitry
  - CTG
    - set clock-tree leaf pins within MDPL DFFs
  - Place
  - Route

Experimental Results

- Comparison of DPA-resistance of CMOS, WDDL and MDPL NAND gates concerning unbalanced complementary wires



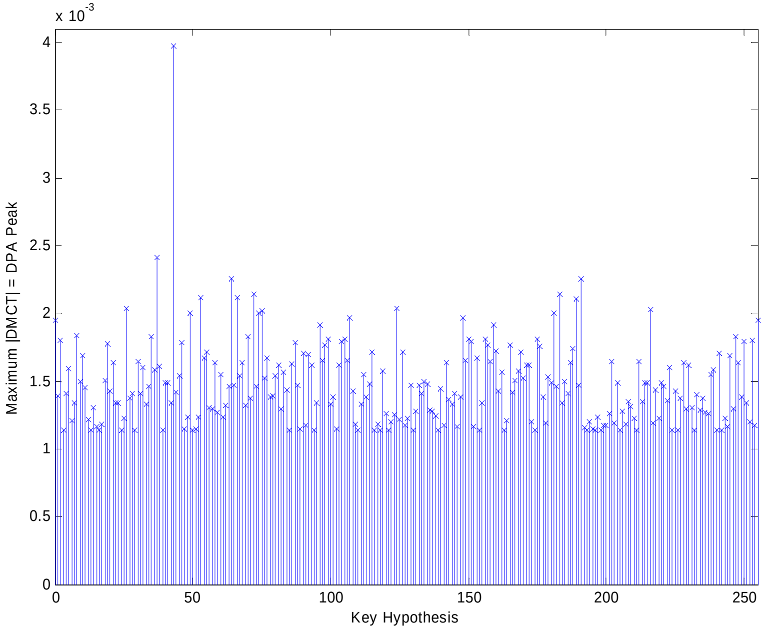
Experimental Results

- Comparison of an AES module implemented in CMOS and in MDPL
  - Area
    - 4.54x higher for MDPL
  - Speed
    - 0.58x of CMOS
  - Power
    - 4x – 6x higher for MDPL

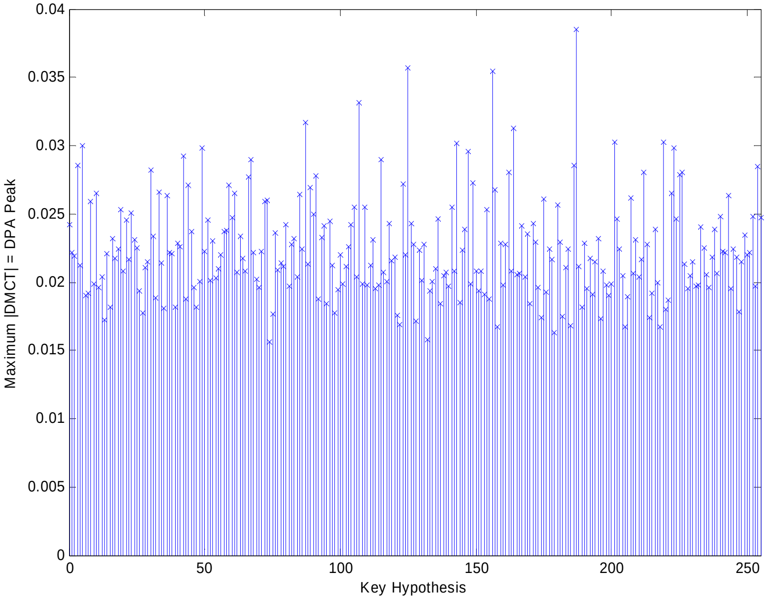
Experimental Results

- DPA-resistance (simulated power traces)
  - output of first SubBytes operation was targeted
  - 256 encryptions

AES implemented in CMOS:



AES implemented in MDPL:



Conclusions and Future Work

- MDPL is suitable for semi-custom design
  - Only commonly available standard cells are necessary
  - No balancing wires constraint – is usually the biggest problem of many DPA-resistant logic styles
- Experimental results are OK
  - Practical results expected from SCARD project
    - http://www.scard-project.org
- Trade-off is in increased area and power and reduced speed

The Team

IAIK

Graz University of Technology

The Side-Channel Analysis Lab

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