Infineon

CHES 2006 - Yokohama

Three-Phase Dual-Rail Pre-Charge Logic

M. Bucci, L. Giancane, R. Luzzi, A. Trifiletti
{marco.bucci, raimondo.luzzi}@infineon.com
{giancane, trifiletti}@die.mail.uniroma1.it

Infineon technologies

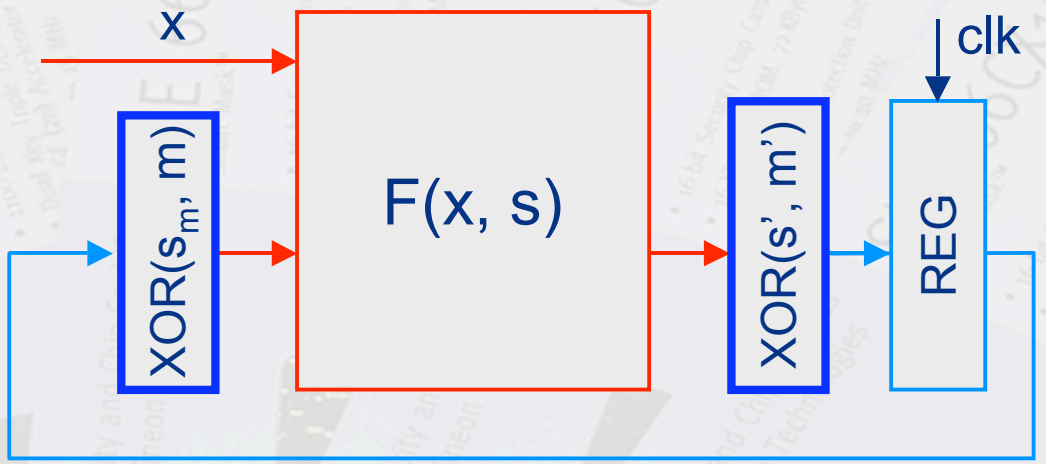
Never stop thinking.

Summary

- Advantages of pre-charged dual-rail logics
- Some implementation issues
- Impact of unbalanced loads and circuit asymmetries on the actual robustness against DPA
- The proposed logic style (TDPL) vs a reference dual-rail logic style (SABL)
- Simulation testbench and results on basic gates
- Case study: FULLADDER

Application scenario: masking a state machine

Busses and registers can be “easily” XOR-masked.
Unfortunately, this does not hold for combinatorial functions that, in general, are not linear with the XOR operator.

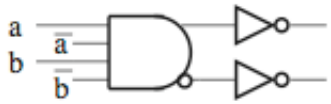


Dual-Rail pre-charged logic is a countermeasure suitable to be “transparently” applied to combinatorial functions.

It has also the advantage to be “glitch-free”.

Just two gates are needed for the implementation of a complete dual-rail family

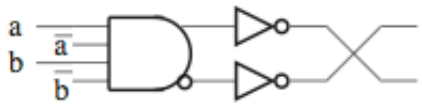
Basic gates



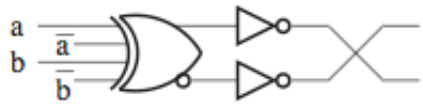
AND

XOR

NOT

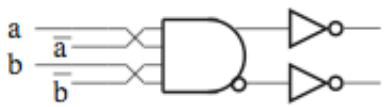


NAND



XNOR

OR



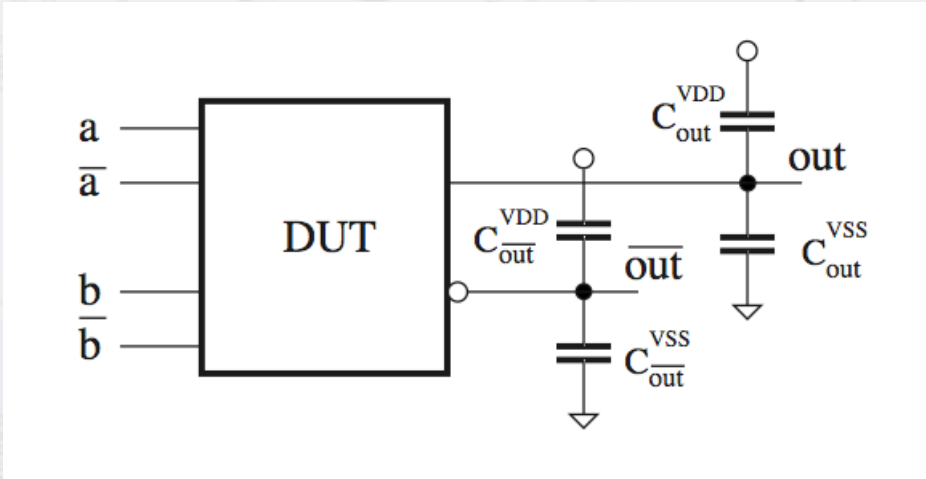
NOR

Using a dynamic logic, gates are cascoded in Domino style.

Therefore, different fanouts can be simply obtained by using a suitable pair of static inverters

Load capacitances in a dual-rail gate

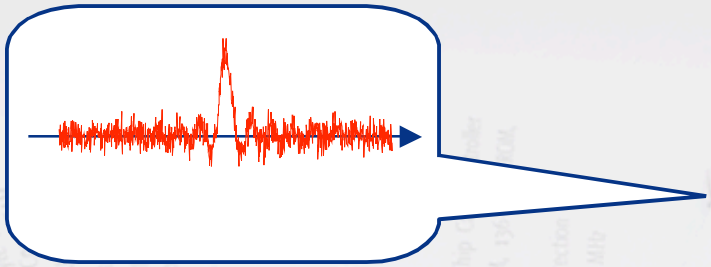
The actual robustness of a dual-rail device depends on the actual balancing of its implementation.



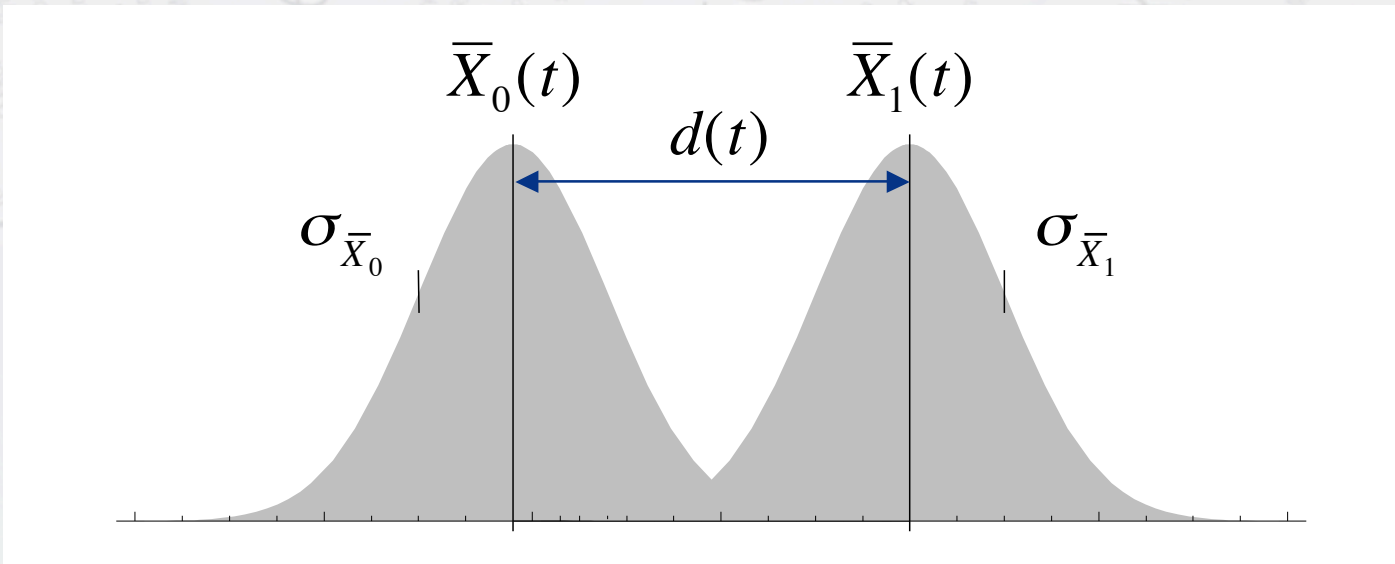
Load capacitance are the main issue, but also internal nodes are relevant.

In facts, an accurate load balancing requires a full custom design flow (i.e. manual or semi-manual routing and a large amount of post-layout simulations).

Effect of unbalancing of complementary wires



$$d(t) = \overline{X}_1(t) - \overline{X}_0(t)$$



A DPA peak appears when a set ***X*** of traces is partitioned on two sets $\boldsymbol{X_0}$ and $\boldsymbol{X_1}$ in such a way their averages can be “distinguished”.

Effect of unbalancing of complementary wires (cont.)

$\frac{d}{\sigma_d}$ is, in facts, the "signal/noise" ratio of a DPA peak

where $\sigma_d^2 = \sigma_{\bar{X}_0}^2 + \sigma_{\bar{X}_1}^2$ and $\sigma_{\bar{X}_i} = \frac{\sigma_{X_i}}{\sqrt{N_i}}$

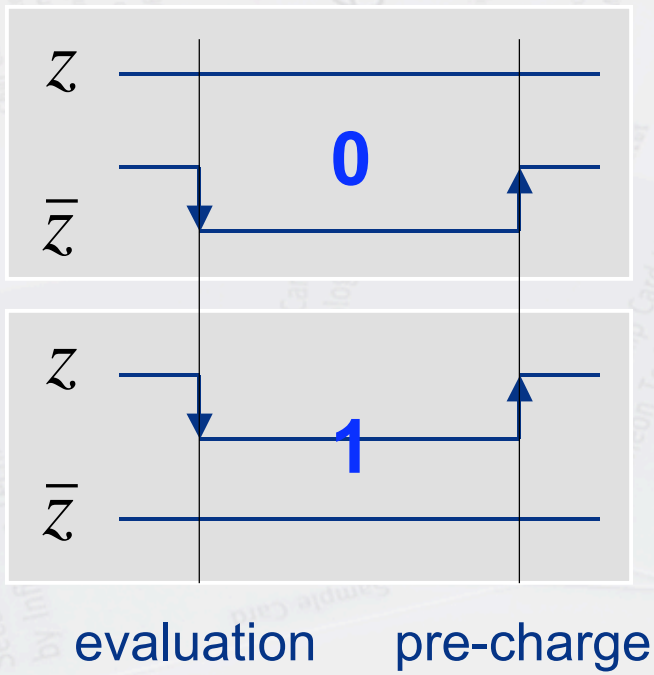
What does it mean?

As an example: a 5% unbalanced dual-rail will feature only a 1/20 attenuation and could be attacked, using 400*N traces, the same as a single rail using N traces.

...and 5% is a quite optimistic unbalancing estimation.

How can we make the energy consumption of the circuit “balanced”?

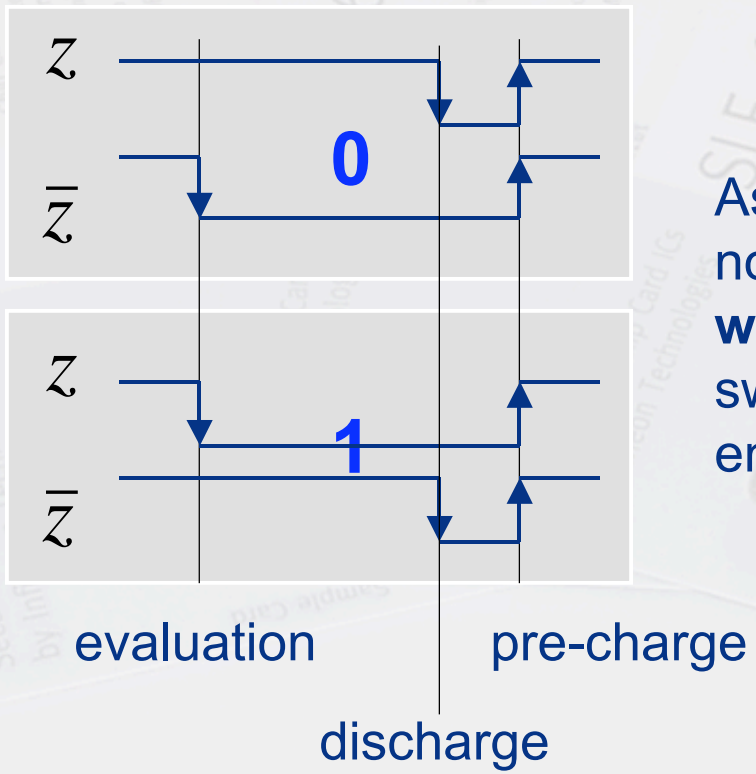
Normally, both rails are pre-charged, but only one is discharged during the evaluation phase.



The problem comes from the fact that the energy consumption depends on **which** wire (or internal node) switches.

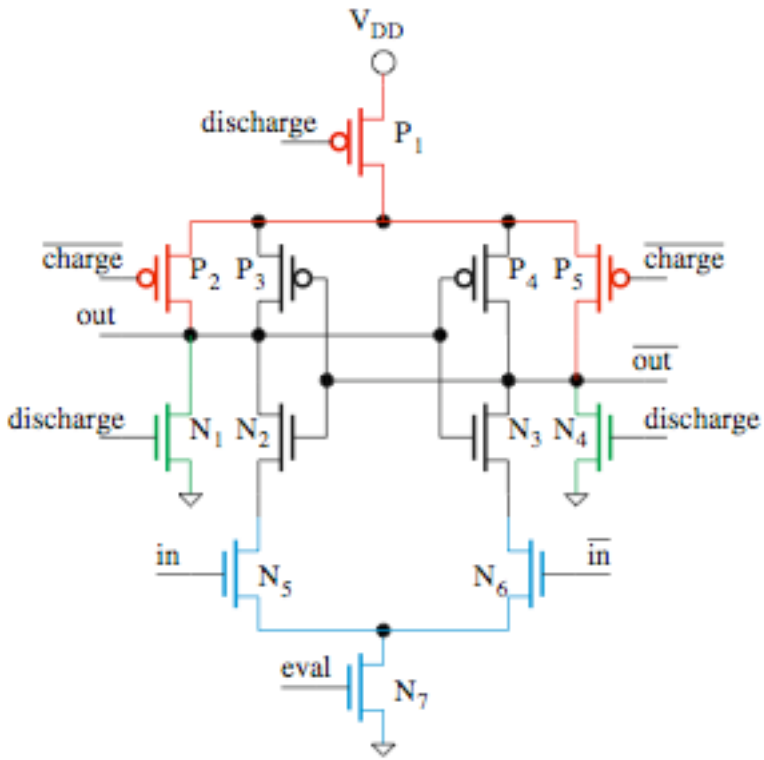
Three-phase dual-rail

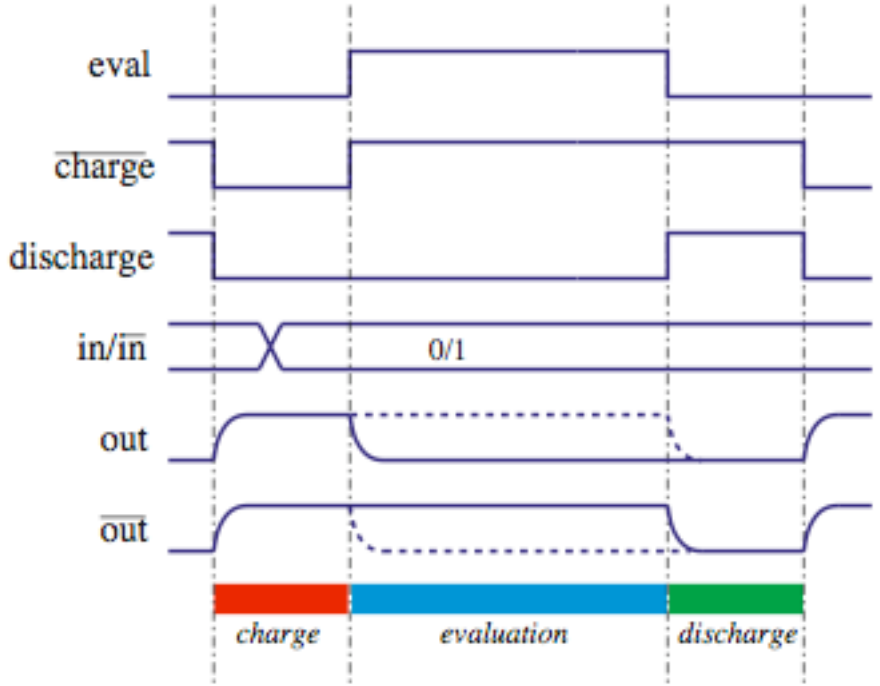
In order to balance energy consumption we can simply make both the wires switch by adding a discharge phase.



As a matter of fact, we can notice that now the information is not anymore on **which** wire switches, but on **when** wire switches (i.e. we use a sort of phase-encoding).

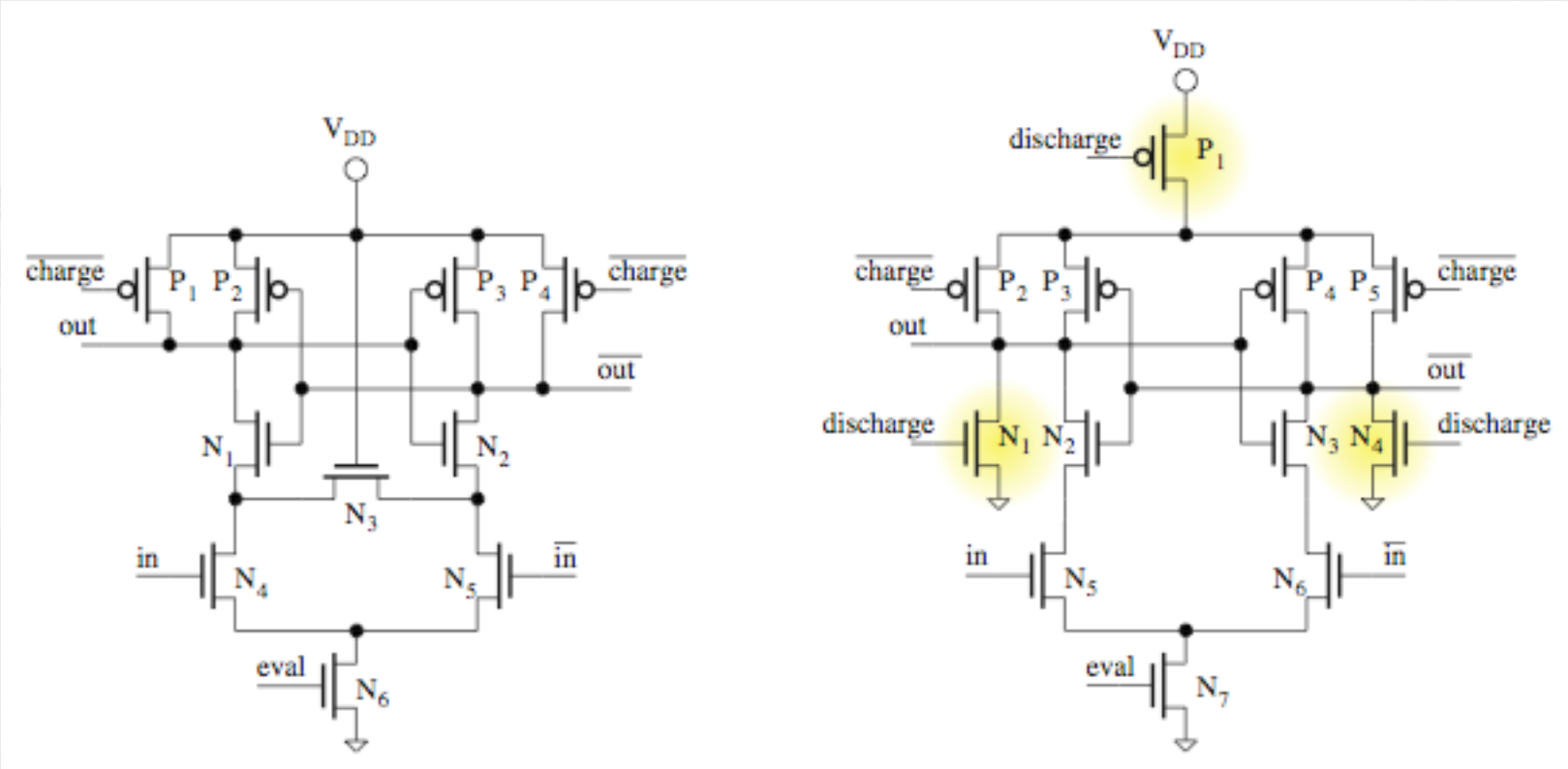
The proposed logic style (inverter)





1. **charge**: outputs are pre-charged to VDD via P_1, P_2, P_5;
2. **evaluation**: N_7 is closed thus discharging one of the outputs via the pull down circuit (N_5, N_6) according on the input lines;
3. **discharge**: the additional pull down N_1, N_3, discharges the output line that was not discharged during the evaluation phase.

SABL vs TDPL



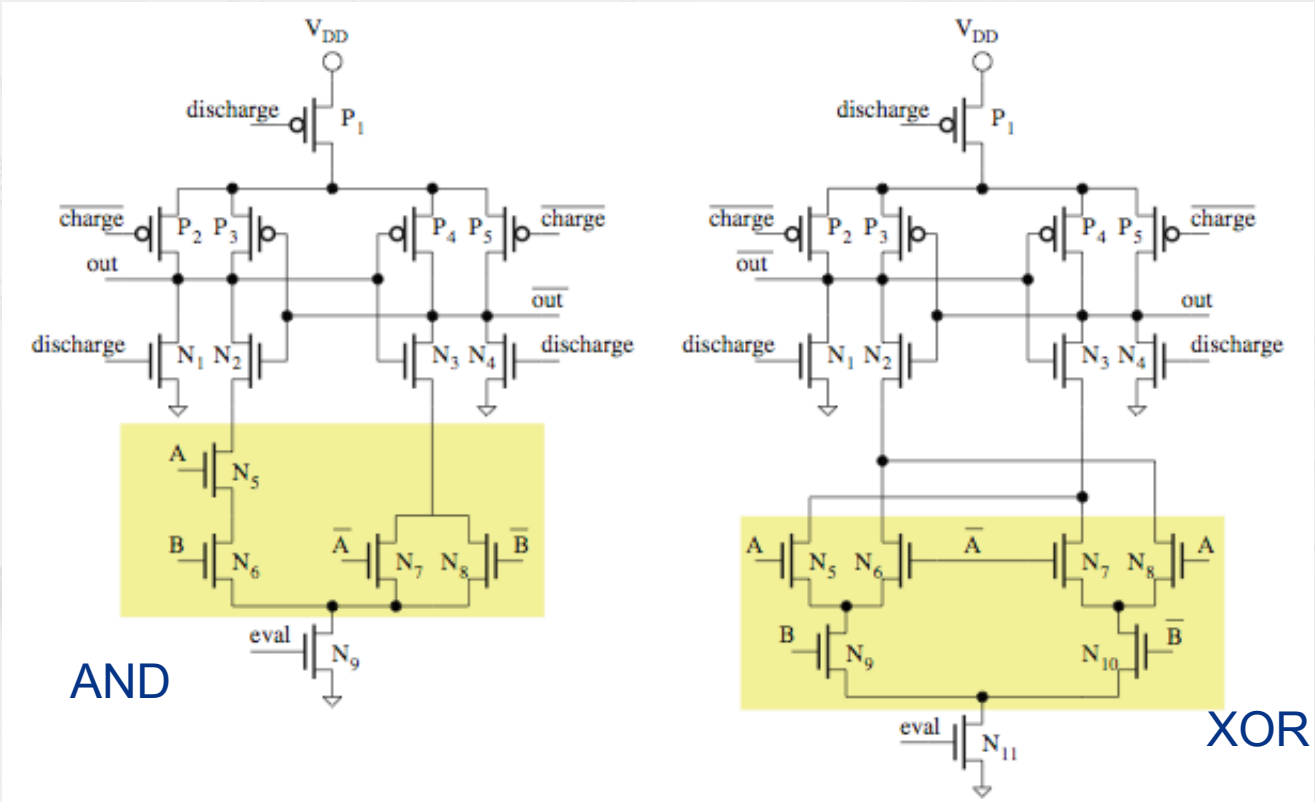
SABL inverter

TDPL inverter

In TDPL, two additional pull-downs NMOS (N_1, N_4) and a PMOS switch (P_1) are added in order to implement the discharge phase.

Other gates in TDPL

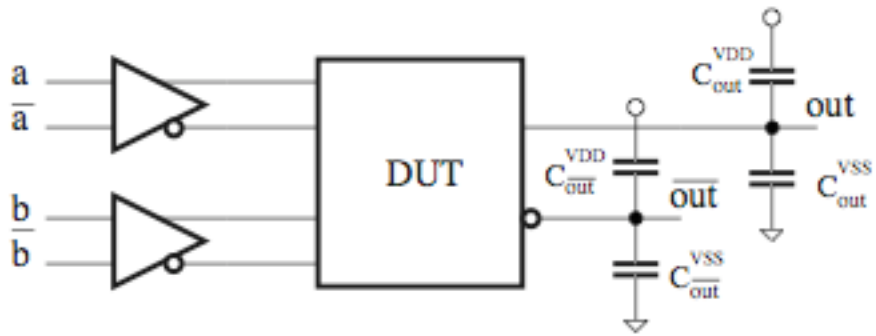
As in SABL, gates differ only in the pull-down circuit.



Notice that, being a dual-rail logic, the AND gate is actually a "universal gate" (AND, NAND, OR, NOR).

Simulation testbench (TDPL vs SABL)

- Process: Infineon 0.12µm, 1.5V supply voltage;
- Transistor sizes: W = 0.68µm; L = 0.12µm;
- Simulation: Spectre/BSIM3v3.

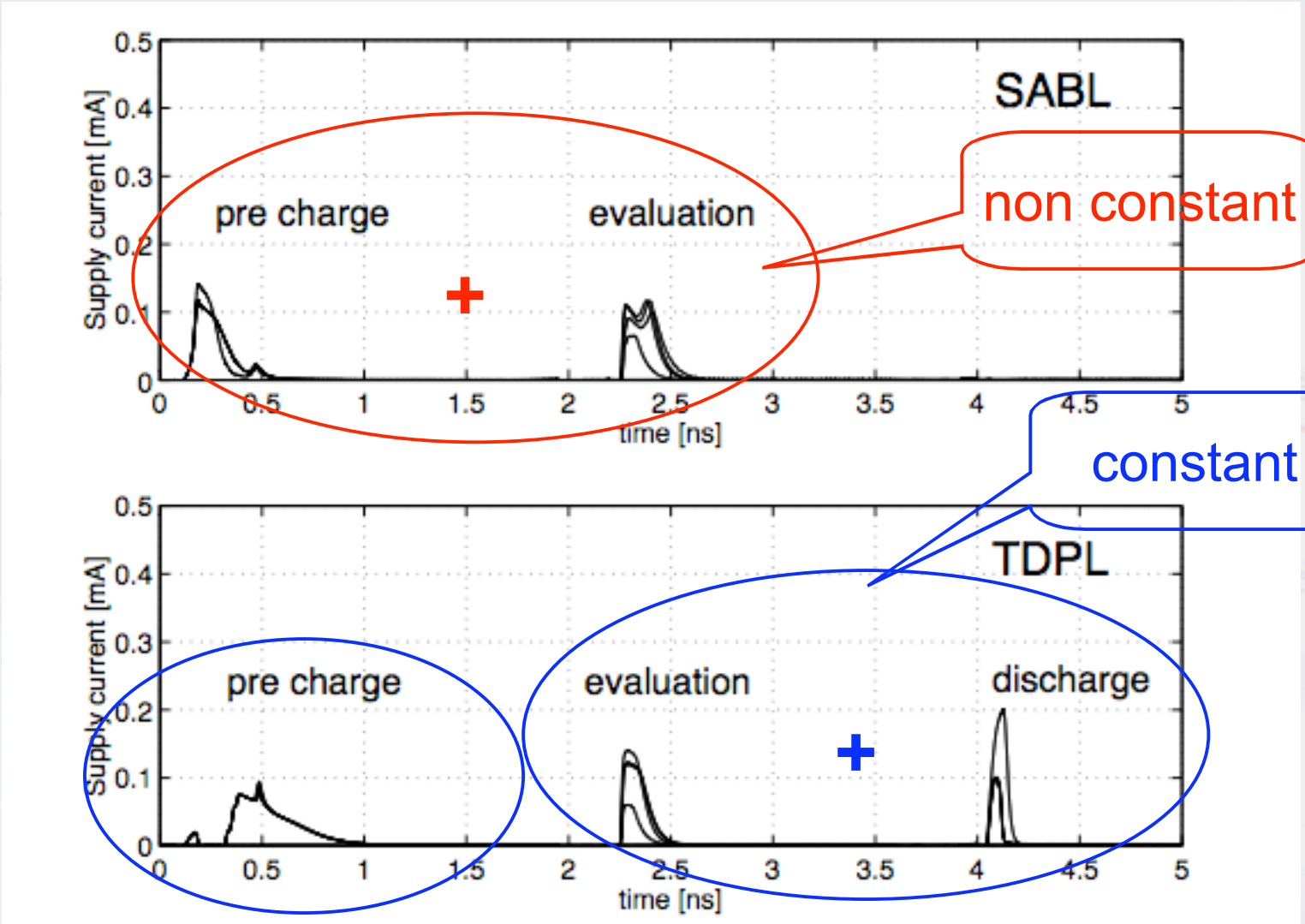


	to V_{DD}	to V_{SS}
from out	C_{out}^{VDD} = 8 fF	C_{out}^{VSS} = 4 fF
from $\overline{out}$	$C_{\overline{out}}^{VDD}$ = 1 fF	$C_{\overline{out}}^{VSS}$ = 3 fF

Capacitive Loads

Since power consumption mainly depends on transitions, all possible input transitions have been simulated.

NAND current traces for all input transitions: SABL vs TDPL



Simulation results for the three basic gates

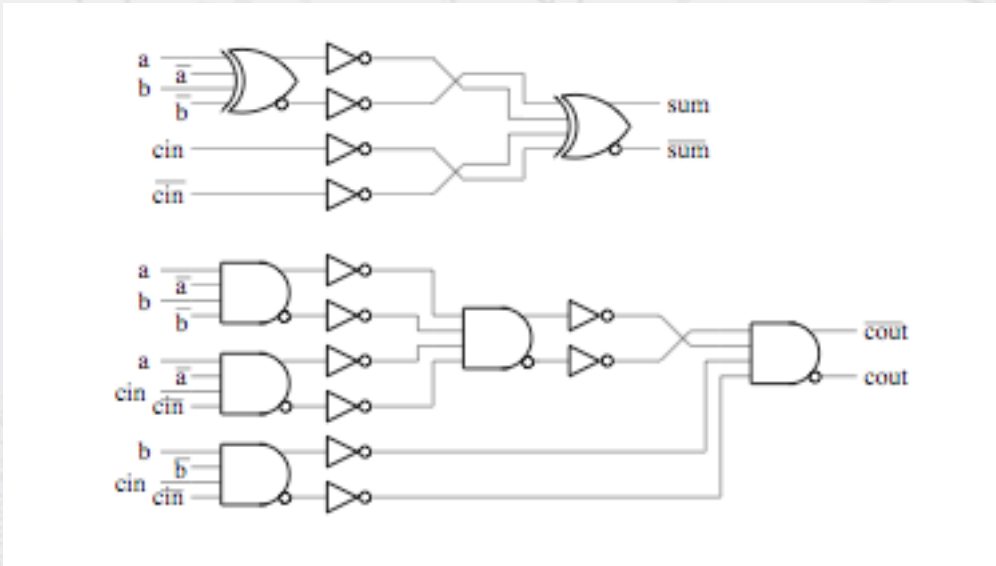
	INV		NAND/AND		XOR/NXOR	
	SABL	This work	SABL	This work	SABL	This work
max (E)	52.3	65.6	56.3	68.3	58.4	69.5
min (E)	31.1	65.3	35.2	66.4	39.4	68.0
NED	40.4%	0.4%	37.5%	2.7%	32.6%	2.1%
$\overline{E}$	41.7	65.5	50.5	67.3	48.9	68.7
σ_E	10.9	0.1	8.0	0.6	8.5	0.4
NSD	26.1%	0.2%	15.9%	0.9%	17.4%	0.6%

$$NED = \frac{\max(E) - \min(E)}{\max(E)}$$

$$NSD = \frac{\sigma_E}{\overline{E}}$$

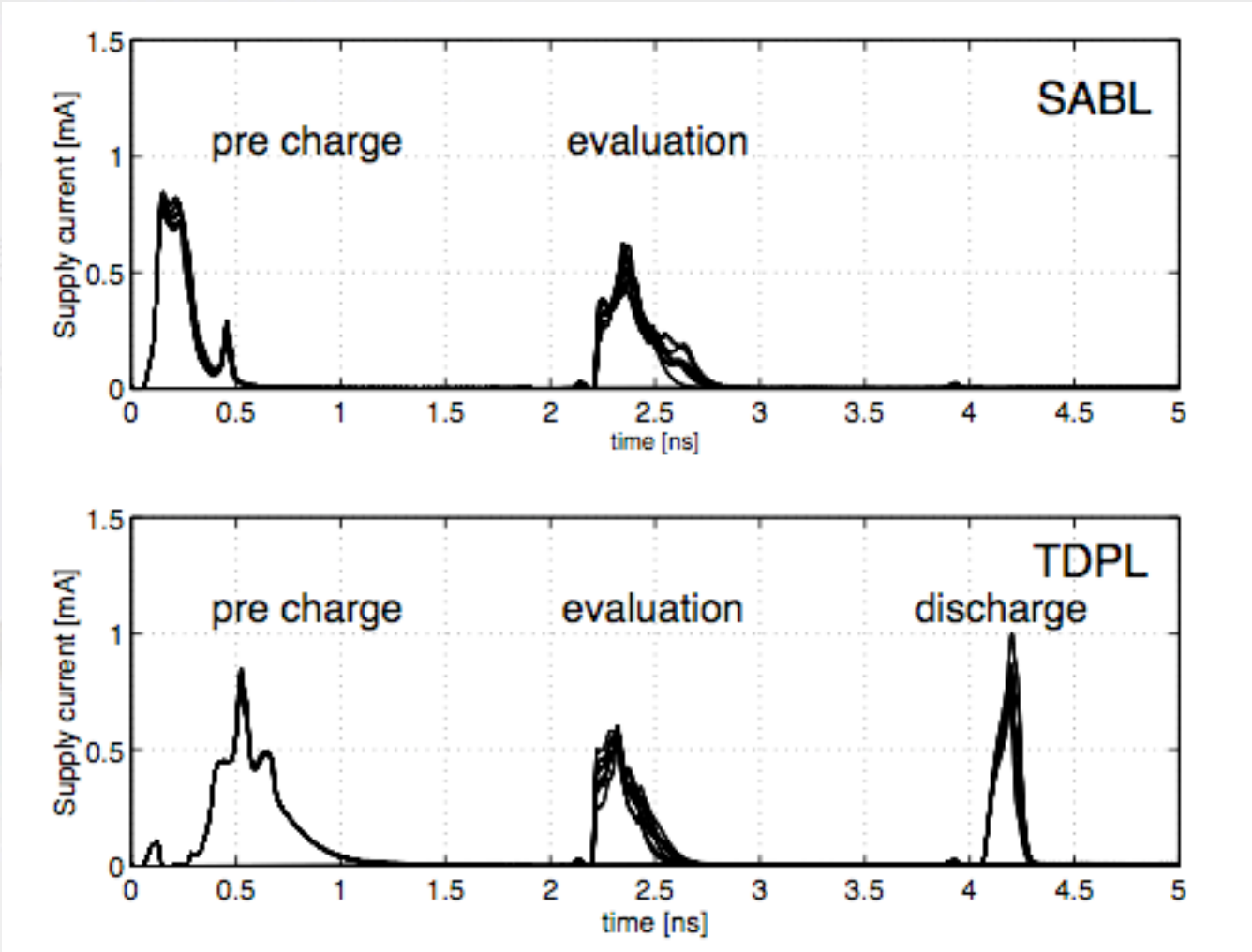
Case study: TDPL vs SABL Full Adder

Dual-rail FULLADDER based on XOR and NAND gates cascaded using a Domino logic (static inverters).



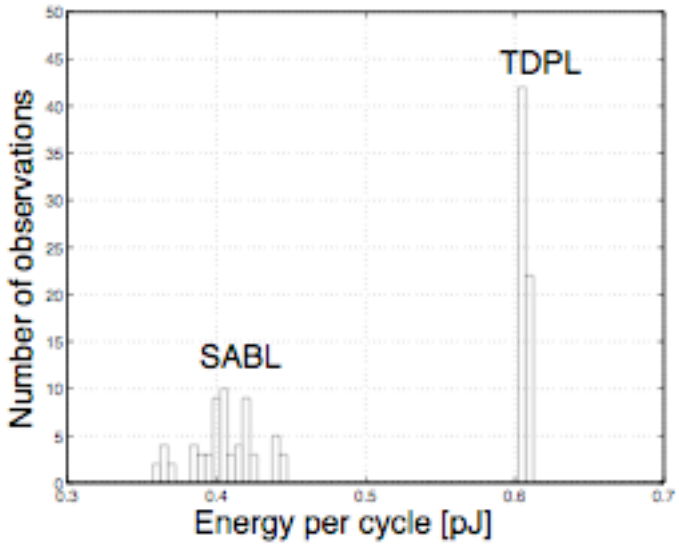
Notice that, in TDPL, static inverters do not cause unbalanced energy consumption since, as the connection wires, each inverter switches the same number of times.

FULLADDER current traces: SABL vs TDPL



Simulation results for the FULLADDER

- (8x8) traces related to all possible input transitions
- each gate is unbalanced as shown in the previous testbench



	FULLADDER	
	SABL	This work
max(E) [pJ]	447.0	609.6
min(E) [pJ]	360.1	604.1
NED	19.4%	0.9%
$\overline{E}$ [pJ]	405.6	606.8
σ_E [pJ]	22.1	1.3
NSD	5.4%	0.2%

- NSD improvement over 25 times
- power consumption increasing about 50%

Balanced vs unbalanced TDPL

Balanced and unbalanced TDPL behave almost the same: **i.e. the goal to avoid full-custom layout seems to be achieved!**

C BALANCED [pQ]	C UNBALANCED 10% [pQ]
0,1761	0,1836
0,1761	0,1836
0,1764	0,1839
0,1764	0,1839
0,1761	0,1836
0,1761	0,1836
0,1764	0,1839
0,1764	0,1839
0,1764	0,1839
0,1764	0,1839
0,1761	0,1836
0,1761	0,1836
0,1764	0,1839
0,1764	0,1839
0,1761	0,1836
0,1761	0,1836

	C BALANCED	C UNBALANCED 10%
MAX	0,1764	0,1839
MIN	0,1761	0,1836
AED	0,0003	0,0003
NED	**0,002**	**0,002**
SD	**0,000**	**0,000**
NSD	**0,001**	**0,001**

The residual leakage seems to depend on second order effects such as:
- parasitics which depend on the state of adiacent nodes;
- power transfer through inputs;
- ...

Conclusions

- DPA-resistant dual-rail logic family suitable for a semi-custom design flow
- almost constant energy consumption even in presence of heavily asymmetric interconnections and pull-downs:
  - about 25 times more balanced than SABL in case of a FULLADDER;
  - in facts, the same robustness as a full-custom dual-rail logic
- power consumption and area penalties smaller than MDPL

Questions?