Path Swapping Method to Improve DPA resistance of Quasi Delay Insensitive Asynchronous circuits

Fraidy BOUESSE, Gilles SICARD, Marc RENAUDIN

TIMA Laboratory, Concurrent Integrated Systems Group
46, avenue Félix Viallet 38031 Grenoble, FRANCE
http://tima.imag.fr/cis
e-mail: fraidy.bouesse@imag.fr

October 2006

Ghislain Fraidy BOUESSE

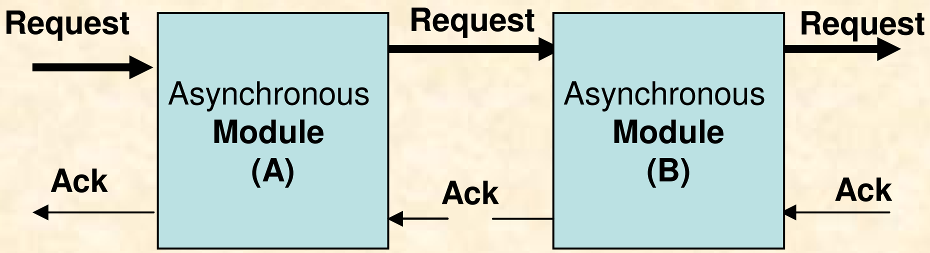
Path Swapping Method to Improve DPA resistance of Quasi Delay Insensitive Asynchronous circuits

Outline

- *QDI Asynchronous Circuits and Security*
  - » **QDI secure design style.**
  - » **Security characteristics.**
- *Path Swapping method*
  - » **Principle.**
    - - Definition.
    - - Swapping function
  - » **Formal approach.**
    - - Electrical model of QDI circuits
- *Case Study : DES crypto-processor*
  - » **Validations.**
    - - Electrical simulations
- *Conclusion and Prospects*

QDI Asynchronous Circuits and Security

No global clock, no global timing assumption
Sequencing is based on Handshaking



Ack=Acknowledgement

Handshake based communication between modules.
A module: any complexity.

Four-phase handshake protocol

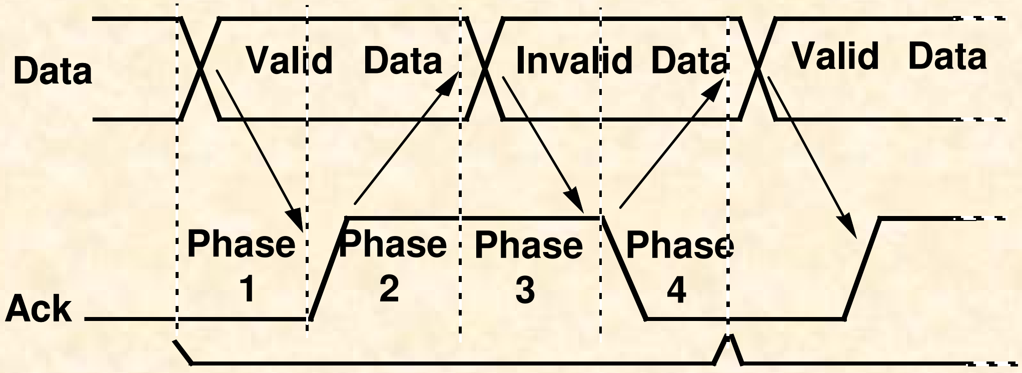
Phase1: Data detection

Phase2: Ack is set to one

Phase3: Data are re-initialized

Phase4: Ack is reset

Hazard free logic is required



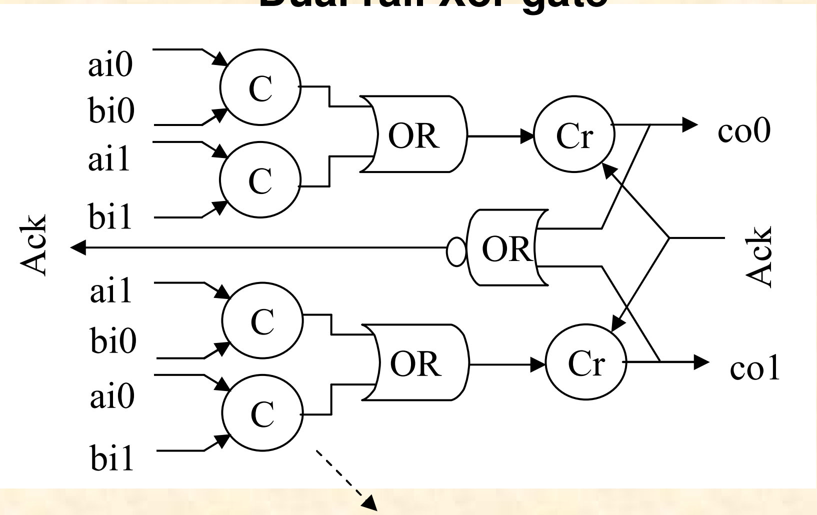
QDI Asynchronous Circuits and Security

- **Signalling**

1 bit Channel : Data encoding

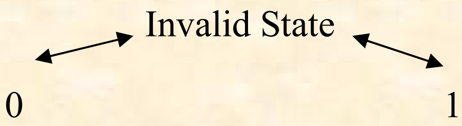
Channel data	A0	A1
0	1	0
1	0	1
Invalid	0	0
Unused	1	1

Dual rail Xor gate



Muller gate (C-element)

Types of transitions



Truth table

$Z = XY + Z(X+Y)$

X	Y	Z
0	0	0
0	1	Z^{-1}
1	0	Z^{-1}
1	1	1

- **Dual-rail encoding can be extended to N rails.**

QDI Asynchronous Circuits and Security

* Properties :

- **Hazard free:** All current variations caused by glitches are eliminated.
- **1-of-N encoded:** Balanced logical structure**.**
- **Four-phase handshake protocol:** re-initialization phase.

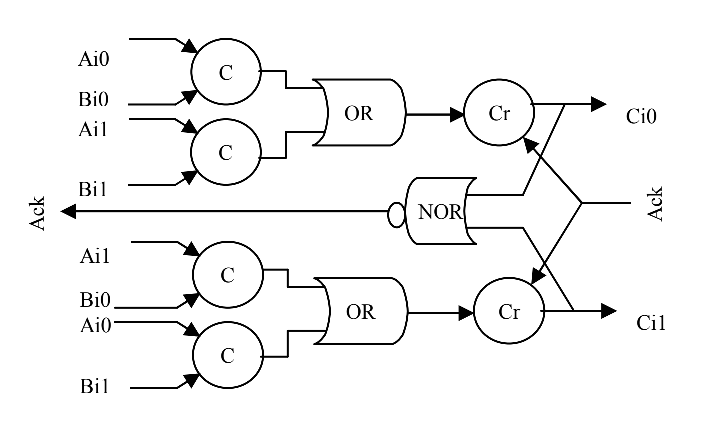
* Advantages :

- **Control the current :** all spurious transitions are removed.
- **Control the type of all transitions.**
- **Same number of transitions:** constant hamming weight**.**
- **Reduce the dependence between data and power consumption:**
  - symmetrical structures of data and control paths

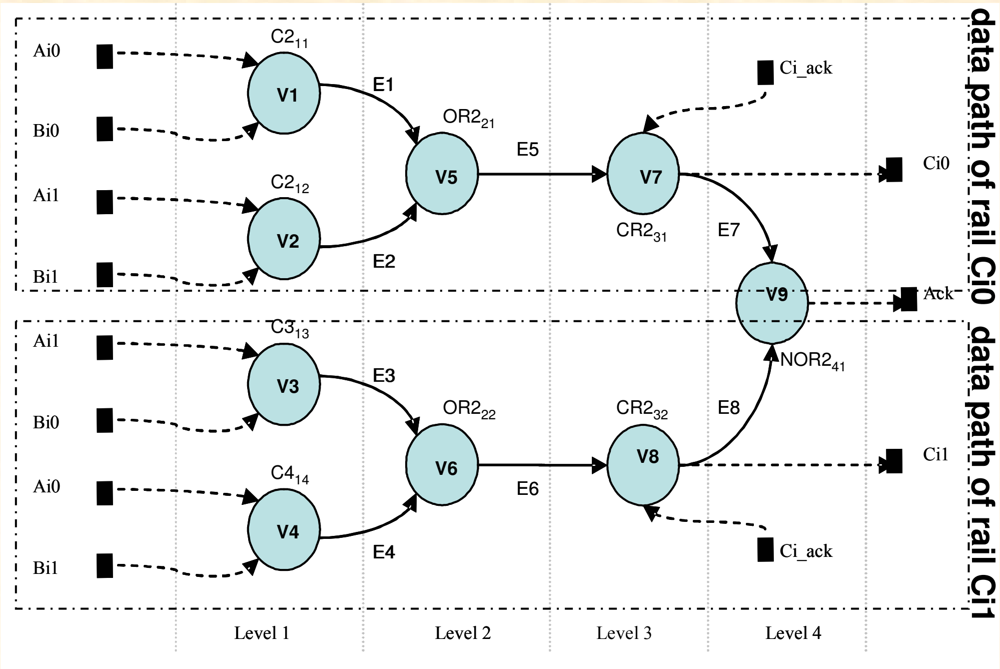
Path Swapping method

Eliminate the electrical effects which enable to succeed the DPA attack on QDI circuits.

- Exploitation of the circuit structure which exhibits a lot of symmetries



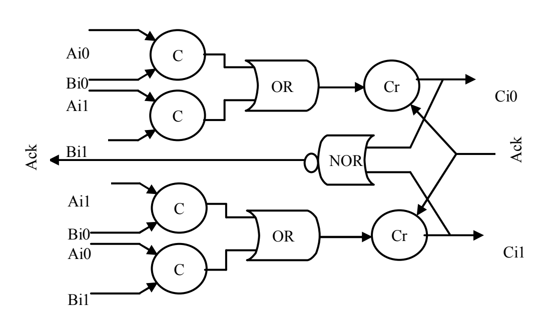
Dual rail Xor gate



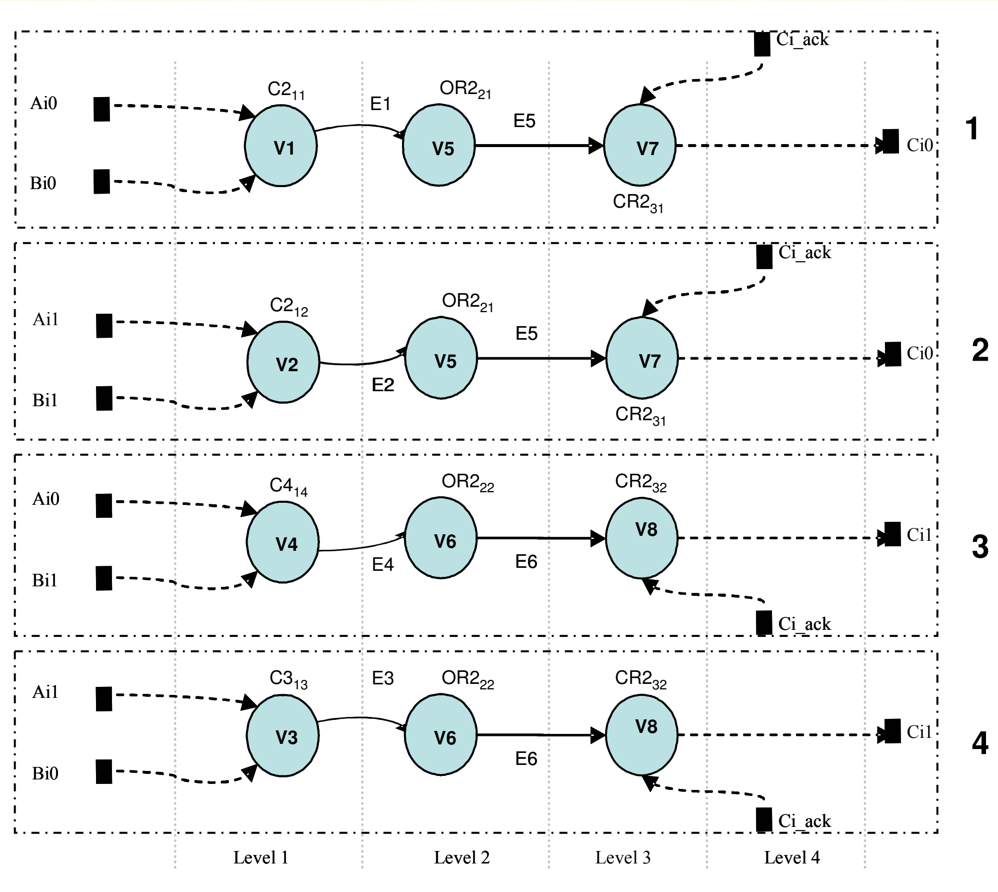
Digraph of Dual rail Xor gate

Path Swapping method

Dual rail Xor gate



Digraph of the execution-path

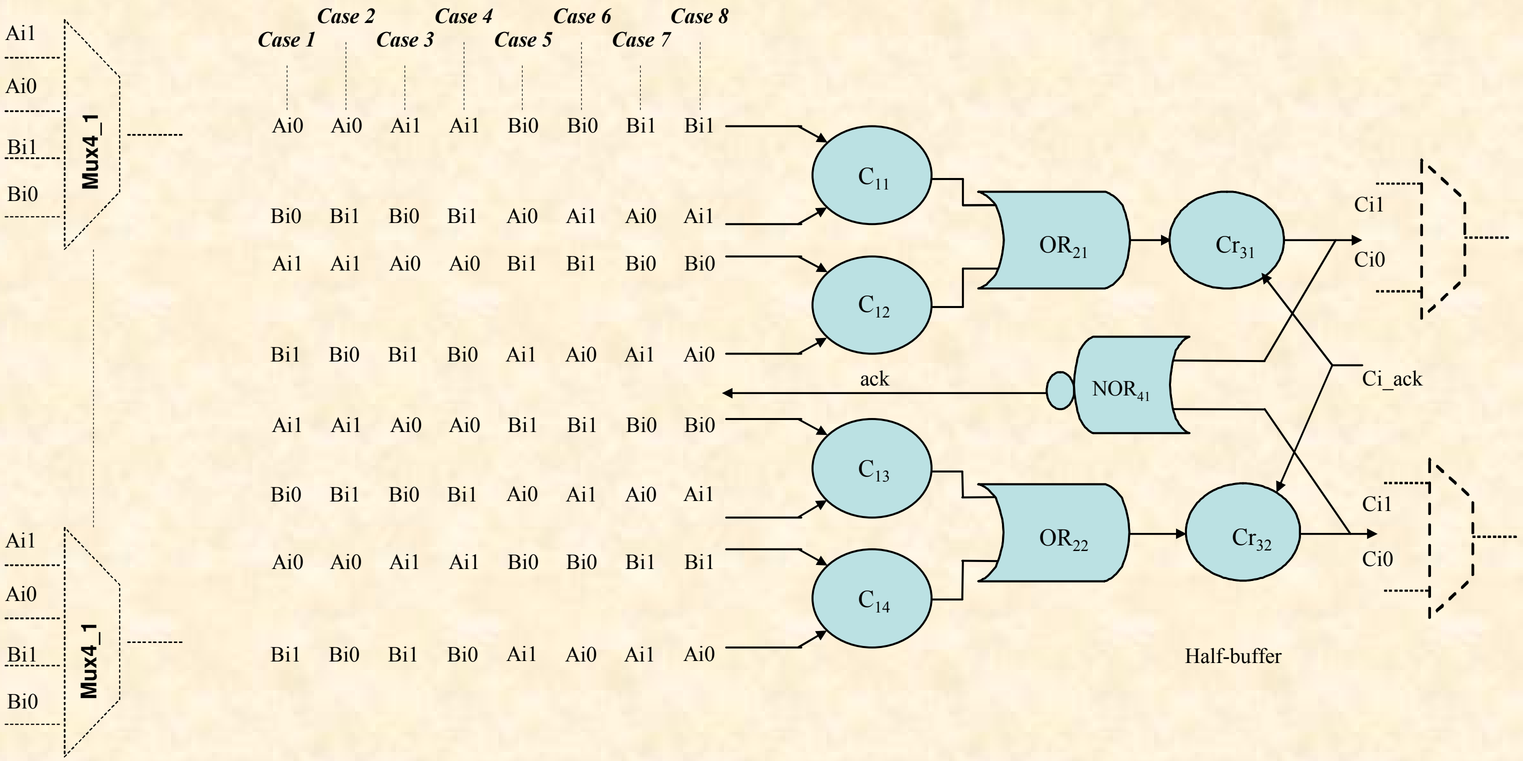


** The idea of the approach is to randomly choose one of the possible paths to compute the function.*

•The execution-path is defined as any exclusive path that can be used to process one output rail.

Path Swapping method

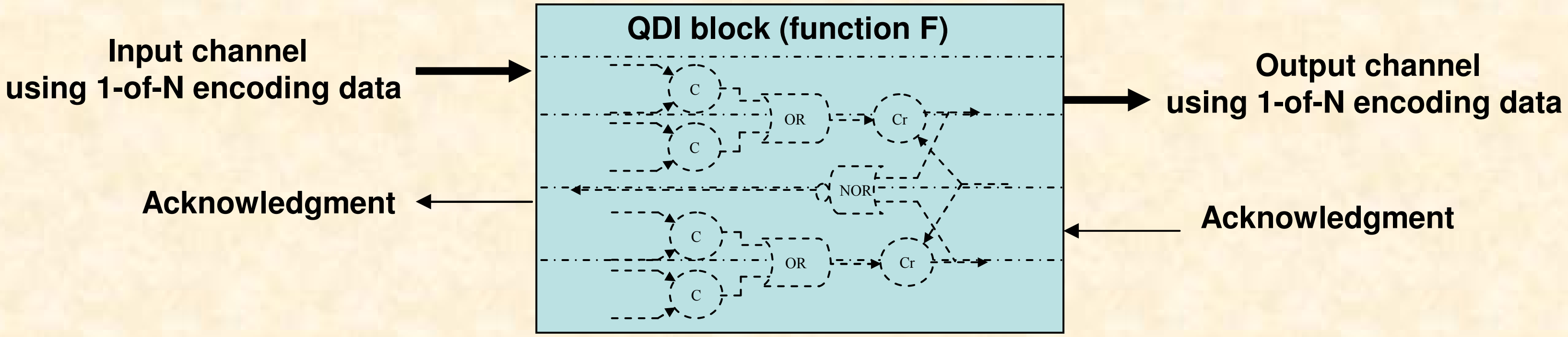
Path Swapping method applied to the Dual-rail Xor gate



Case 1	*Case 2*	*Case 3*	*Case 4*	*Case 5*	*Case 6*	*Case 7*	*Case 8*
Ai0	Ai0	Ai1	Ai1	Bi0	Bi0	Bi1	Bi1
Bi0	Bi1	Bi0	Bi1	Ai0	Ai1	Ai0	Ai1
Ai1	Ai1	Ai0	Ai0	Bi1	Bi1	Bi0	Bi0
Bi1	Bi0	Bi1	Bi0	Ai1	Ai0	Ai1	Ai0
Ai1	Ai1	Ai0	Ai0	Bi1	Bi1	Bi0	Bi0
Bi0	Bi1	Bi0	Bi1	Ai0	Ai1	Ai0	Ai1
Ai0	Ai0	Ai1	Ai1	Bi0	Bi0	Bi1	Bi1
Bi1	Bi0	Bi1	Bi0	Ai1	Ai0	Ai1	Ai0

Path Swapping method

Principle



Input channel
using 1-of-N encoding data

QDI block (function F)

Output channel
using 1-of-N encoding data

Acknowledgment

Acknowledgment

If all data-paths are logically symmetric, it means that:

$$\forall \ A_x \in E_i \quad \Rightarrow \quad f_{i1}(A_x) = \ldots = f_{iN}(A_x)$$

$$and \quad P_{i1}(t / A_x) \neq \ldots \neq P_{iN} \ (t / A_x)$$

Each output channel *i* has *N* rails.
fij(Ax) represents the logical equation of each rail *i* and *Pij(t/Ax)* its dynamic current profile.
The value *Ax* is one element of *Ei*, the set of all possible input values which activate the channel *i.*
The indexes *i* and *j* identify the channel number and the rail number respectively.
For each rail there is a data-path from the primary output rail considered to the primary inputs (*N* data-paths).

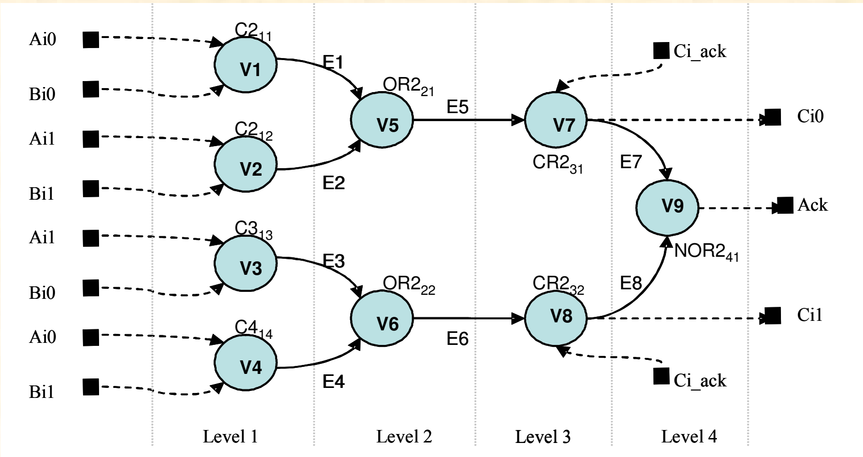
Path Swapping method: formalization

Electrical Model of QDI Circuits: Definition

Dynamic current profile

$$P_{dc}(t) = \sum_{i=1}^{Nc} \left[\sum_{j=1}^{N_{ij}} I_{ij}(t_i) \right] + P_{dn}(t)$$

with $$I(t) = C\frac{dV}{dt}$$



I

$\boldsymbol{I_{ij}}$: dynamic current of *jth* gate of level *I*

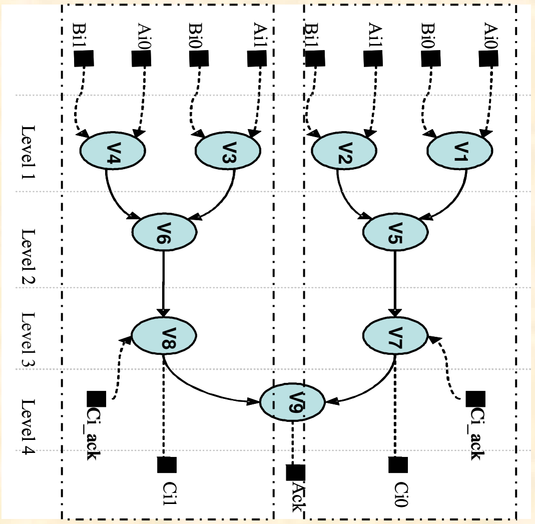
$\boldsymbol{N_c}$ *: number of gates in critical path*

$\boldsymbol{N_{ij}}$ *: number of gates switching at each logical level*

$\boldsymbol{P_{dn}}$*: noise function*

Path Swapping method: formalization

DPA on Dual rail Xor gate



* Average current signal of both sets :

$$A_{xor0}[t] = \frac{1}{2}\left(I_{11}(t_1) + I_{12}(t_1) + I_{21}(t_2) + I_{31}(t_3) + I_{41}(t_4) + I_n(t)\right)$$

$$A_{xor1}[t] = \frac{1}{2}\left(I_{13}(t_1) + I_{14}(t_1) + I_{22}(t_2) + I_{32}(t_3) + I_{41}(t_4) + I_n(t)\right)$$

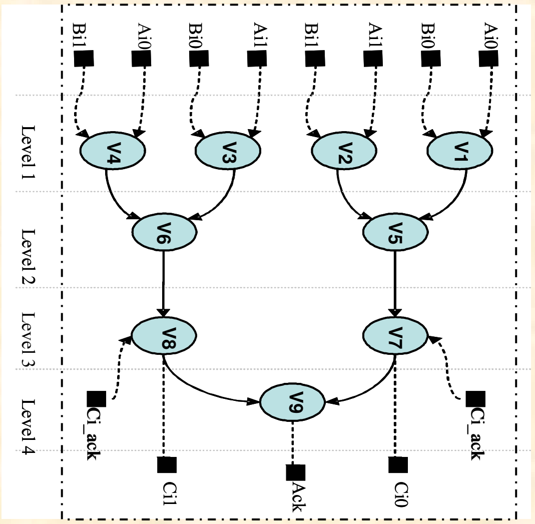
* Expression of a DPA bias signal is given by :

$$S[t] = \Delta V.\left(\frac{C_{11}}{\Delta t_{11}} + \frac{C_{12}}{\Delta t_{12}} - \frac{C_{13}}{\Delta t_{13}} - \frac{C_{14}}{\Delta t_{14}}\right) + \Delta V.\left(\frac{C_{21}}{\Delta t_{21}} - \frac{C_{22}}{\Delta t_{22}}\right) + \Delta V.\left(\frac{C_{31}}{\Delta t_{31}} - \frac{C_{32}}{\Delta t_{32}}\right)$$

DPA on 2 symmetric data-paths reveals the effects of each gate’s charge capacitance

Path Swapping method: formalization

DPA on Dual rail Xor gate with Path Swapping



All data-paths are used to compute outputs, the average current signal of each set contains all gates' current of the structure.

* Average current signal of both sets :

$$A_{xor0}[t]=A_{xor1}[t]=\frac{1}{4}(I_{11}(t_1)+I_{12}(t_1)+I_{21}(t_2)+I_{31}(t_3)+I_{13}(t_1)+I_{14}(t_1)+I_{22}(t_2)+I_{32}(t_3)+I_{41}(t_4)+I_n(t))$$

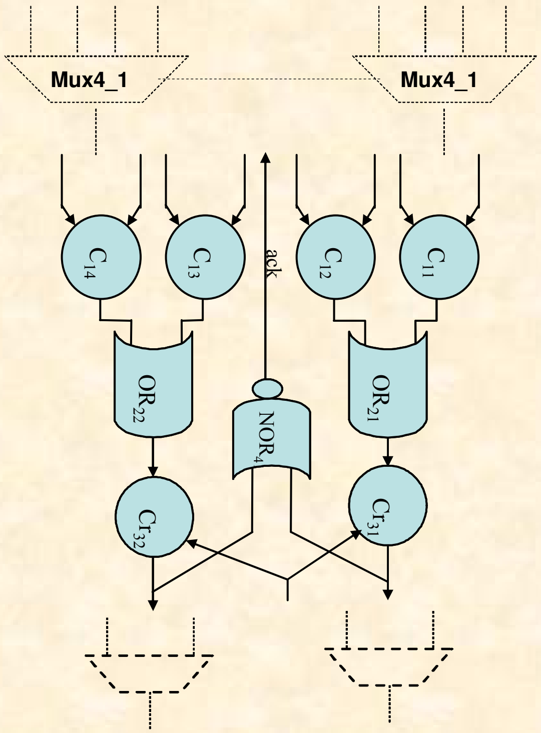
* Expression of a DPA bias signal is given by :

$$S[t] = \quad \approx \quad 0$$

Path Swapping method: Discussion

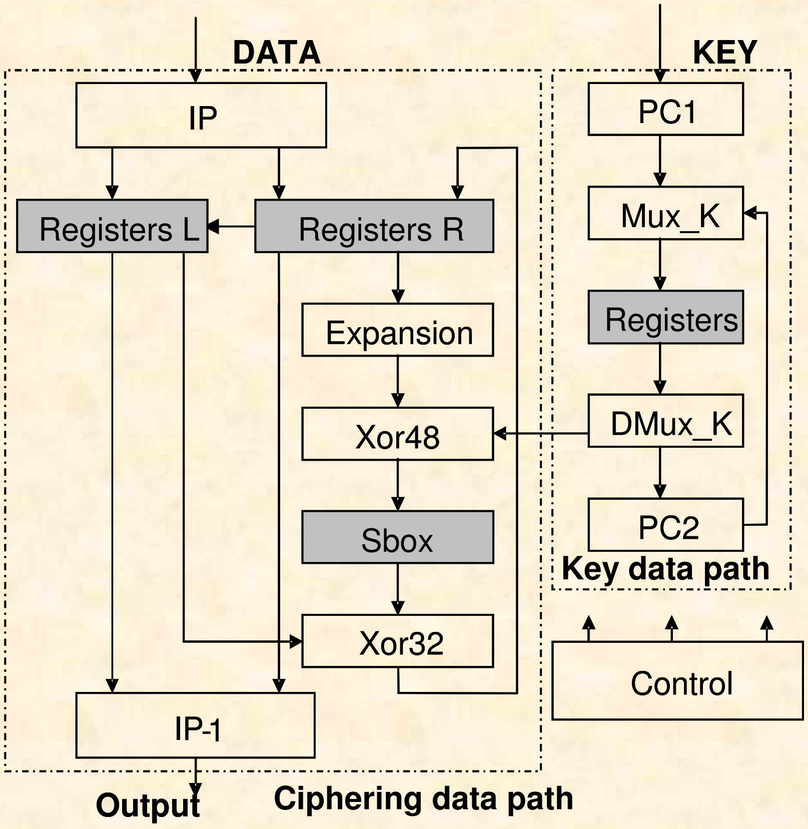
*** Randomizing the path swapping:**
The objective is to ensure unpredictable apportionment of path swapping inside a block.

*** Multiplexers/Demultiplexers Implementation:**
A particular care must be done when implementing these functions.



Case Study: DES Crypto-processor

DES architecture



A new ordering of the SBOX1

Output values	Input values				Sets
0	14/0	0/1	15/2	13/3	E0
15	5/0	1/1	8/2	0/3	
1	3/0	7/1	1/2	6/3	E1
14	0/0	4/1	2/2	11/3	
2	4/0	5/1	6/2	3/3	E2
13	2/0	6/1	4/2	15/3	
3	8/0	14/1	12/2	10/3	E3
12	11/0	10/1	9/2	1/3	
4	1/0	3/1	0/2	4/3	E4
11	6/0	11/1	7/2	9/3	
5	12/0	13/1	14/2	8/3	E5
10	9/0	8/1	13/2	12/3	
6	10/0	9/1	5/2	14/3	E6
9	13/0	12/1	13/2	12/3	
7	15/0	2/1	11/2	7/3	E7
8	7/0	15/1	3/2	2/3	

Column number

Cx/Rx

Row number

SBOX1 : ≈ 30%.
Reg L and R : ≈ 45%
Reg K : ≈ 20%

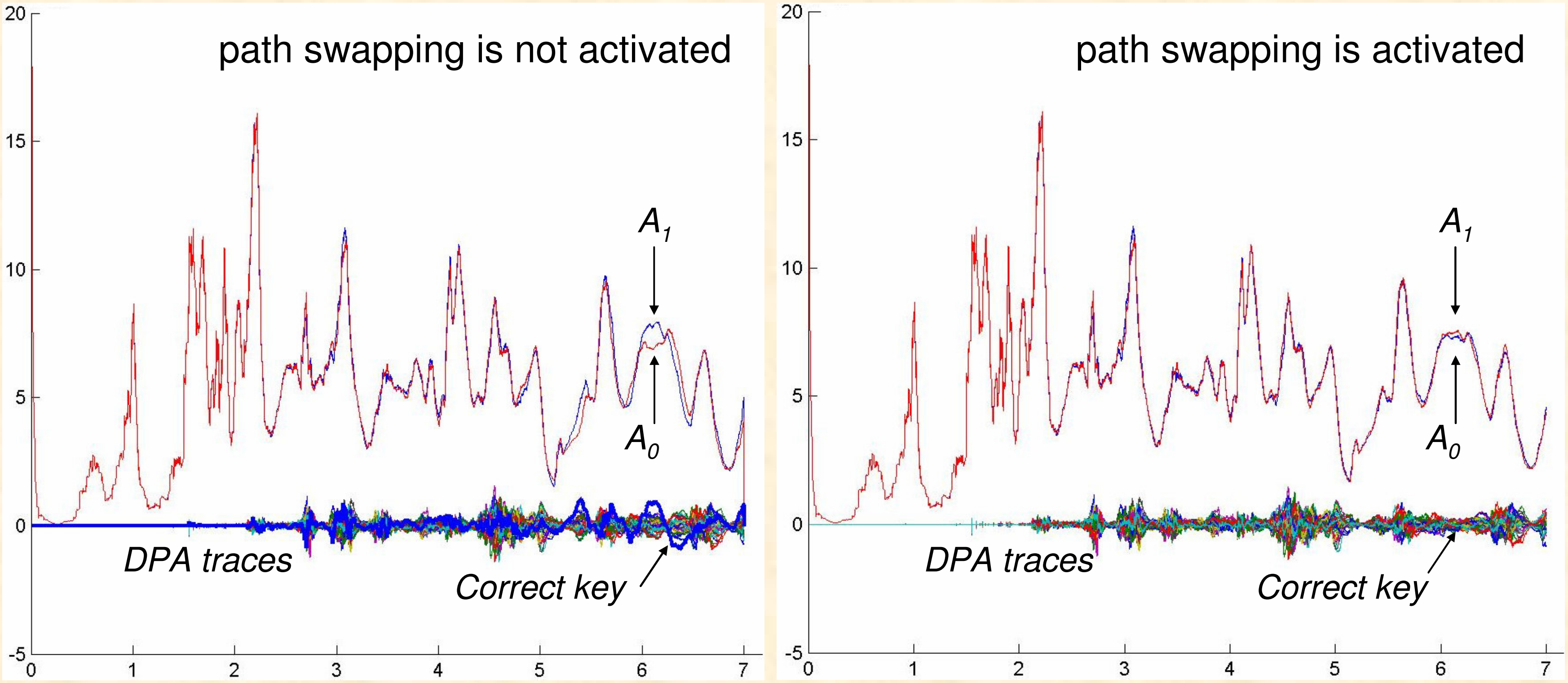
Case Study: DES Crypto-processor

- **Circuits' Characteristics**

Technology	CMOS 0,13 µm (HCMOS8) from STMicroelectronics 6-LM, Power Supply 1.2 V		
	Area / Gate counts	Current/power (Average)	Speed
Asynchronous DES	without PS ≈ 6,6 Kgates with PS ≈ 7,2 Kgates 10%	Current ≈ 0,6 mA Peak ≈ 0,9 mA Power ≈ 0,7 mW	1.2 µs

Case Study: DES Crypto-processor

Electrical Signature when performing DPA attack on bit 4 of the SBOX1



Loading charge difference of both rails of this bit is 32 femtoF.

Conclusion & Perspectives

- **This work demonstrates how the PS (Path Swapping) method can be used to enhance QDI asynchronous circuits' resistance against DPA attack.**

This design approach exploits all properties of QDI asynchronous logic which are suited to design secure chips, particularly the logical data-path symmetries

* Important issues

- **The evaluation on silicon …**
- **Extending the approach on asymmetric cryptography …**

Path Swapping Method to Improve DPA resistance of Quasi Delay Insensitive Asynchronous circuits

Thank you for your attention

Questions ?