The “backend duplication” method

- A Leakage-Proof Place-and-Route Strategy for Secured ASICs -

CHES Workshop

August 30th – September 1st 2005

Edinburgh, Scotland, UK.

Sylvain GUILLEY (*),
Philippe HOOGVORST (*),
Yves MATHIEU (*) and
Renaud PACALET (**).

(*) GET/ENST, 46 rue Barrault
F-75634 Paris Cedex 13.
(**) GET/ENST, Institut Eurecom BP 193, 2229 route des Crêtes
F-06904 Sophia-Antipolis Cedex.

Outline

- Introduction
- Backend
- Standard *versus* Secured Logic Cells
- Secured Place-and-Route (P&R)
- Implementation
- Cross-coupling
- Security Evaluation
- Example of a Secured DES (SDES) design, embedded into the SECMAT ASIC
- Perspectives
- Acknowledgements

Introduction

- « Backend duplication » : a method at the backend level to secure the design of ASICs against Side-Channel Attacks (SCAs).

- Why ASICs?

  - Alternatives are SW, FPGAs and any mixture
  - ASICs always provide the best performance:
    - Implementation size,
    - Power consumption,
    - Computation speed.

    - And it is far more difficult to realize a SCA on an ASIC than on a µP.

Context

- SCAs are a serious threat
  - We consider power attacks in this talk
- Counter-measures are typically of two types: logical or physical
  - We consider physical counter-measures
- Leaked information is made unexploitable (e.g. randomization)
  - We consider constant syndrom
- Design style: full-custom versus standard cells based
  - We consider the use of « not so standard » gates
- We address the question of assembling the gates in a secured way

Frontend *versus* Backend

Hardware design divides into steps:

- **« frontend » = logical aspects**
  - **Specification**
  - **Definition of the architecture**
  - **Coding using a parallel language (VHDL, Verilog, SystemC)**
  - **Validation, by simulation or formal proof**
  - **⇒ logical synthesis, to obtain a netlist of cells**

- **« backend » = physical aspects**
  - **a) Floorplan**
  - **b) Placement**
  - **c) Routing**
  - **⇒ final circuit layout, ready to be sent to the silicon factory**

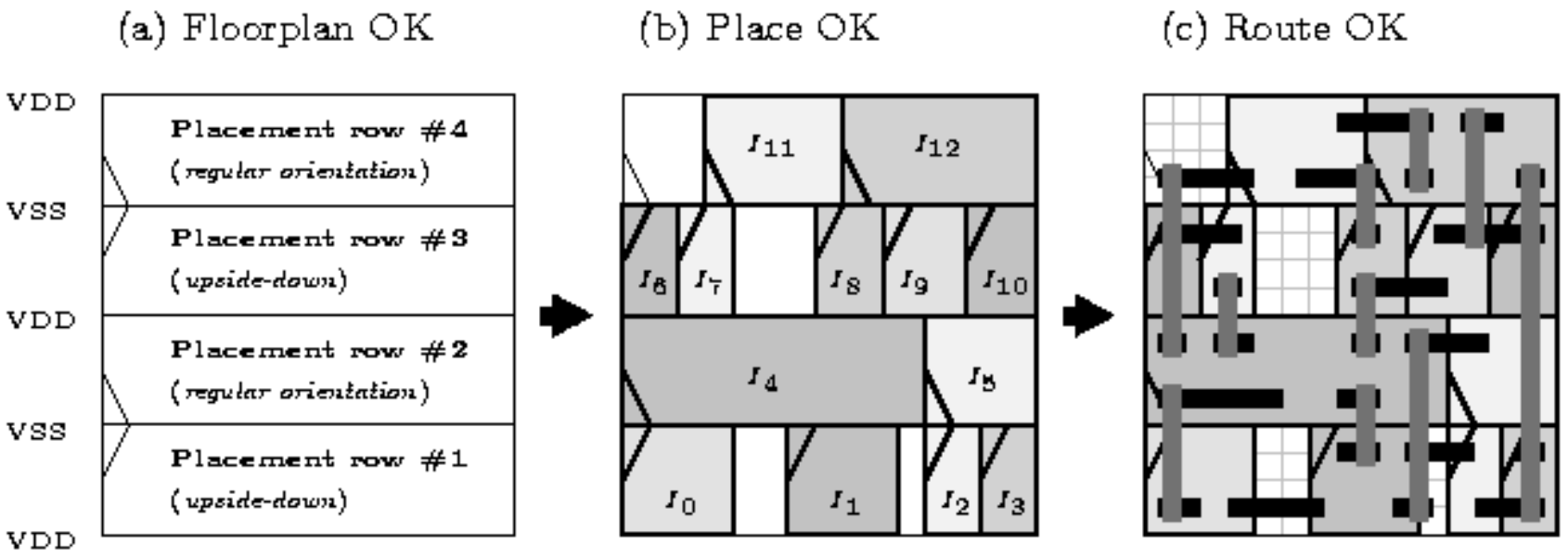
+ pads
+ **power management**
+ scan chain reordering
+ clock tree generation
+ **signal integrity**
+ « dummies » insertion
+ *etc*.

Regular Backend Flow in ASIC Design

a) **Floorplan split into rows**

b) **Instances I_x of the netlist are dispatched into the placement rows**
The cells share the supply (power or VDD / ground or VSS) lines

c) **Routes are created over the cells**
E.g. in HCMOS9GP, cell pins are in M1, thus M2 – M6 is devoted to interconnection
(M1 can be used to route side-by-side cells.)



Secured Logic Gates

- **Many secured cells type exist:**
  - **WDDL** **[Kris Tiri *et al.*]**
  - **SABL** **[Kris Tiri *et al.*]**
  - **QDI primitives** **[Marc Renaudin *et al.*]**
  - **DI primitives** **[Ross Anderson *et al.*]**

Built upon standard cells ←

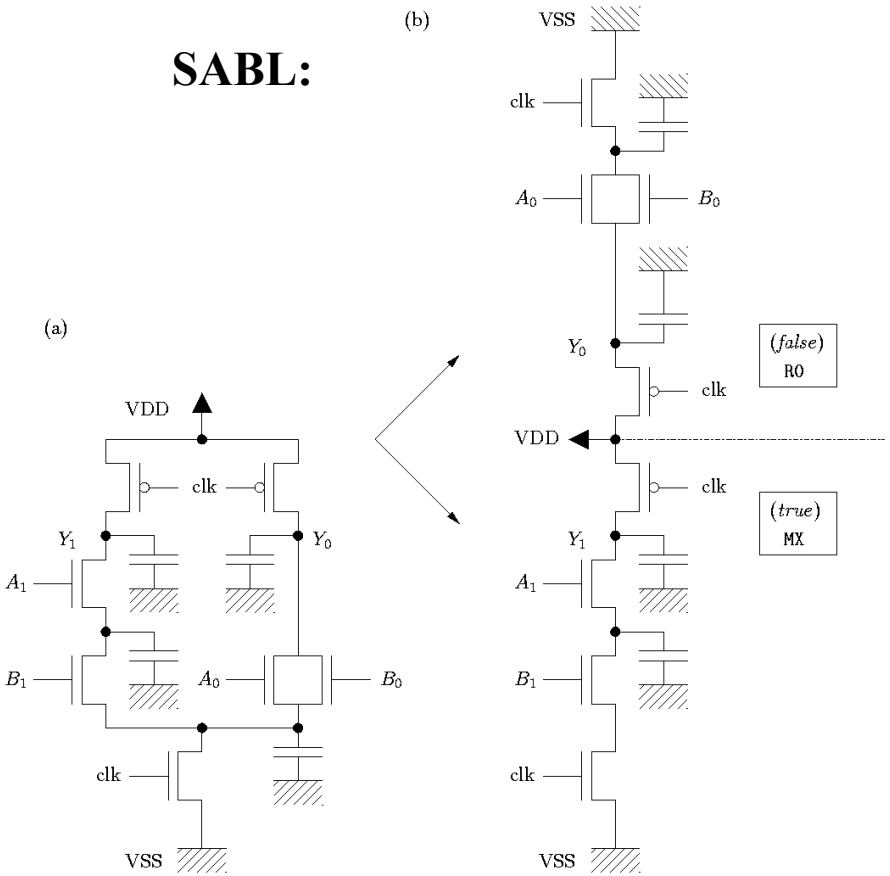
- **But how to use them in a secured Place-and-Route flow?**
  - **Differential routing with…**
  - **… balanced parasitic capacitances.**
  - **Nodes shielded against cross-talk.**

Secured Cells Come in Pairs: WDDL

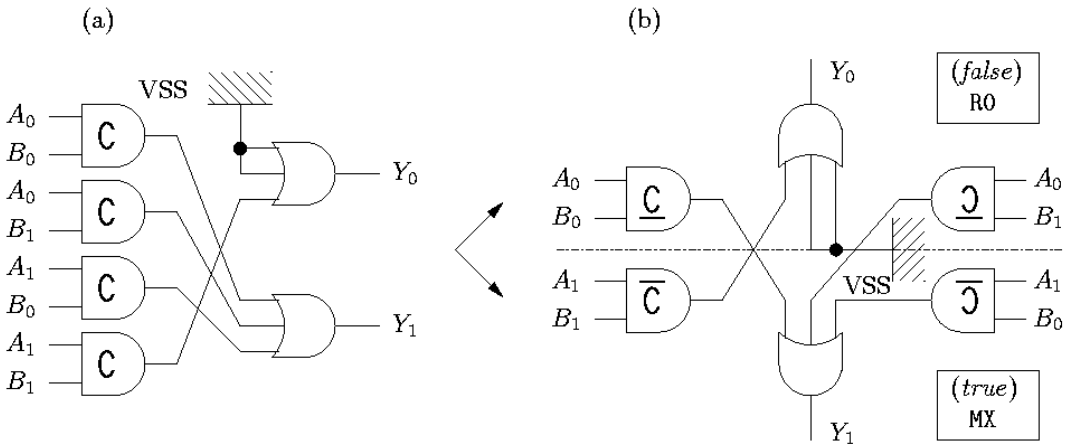
	Regular	Dual
Definition	$f(e_i)$, e_i being inputs	$\overline{f(\overline{e_i})}$
Examples	**NAND**	**NOR**
	XOR	**XNOR**
	INV, XOR3, MAJ	**INV, XOR3, MAJ**
	ΣΠ	ΠΣ

Secured Cells Come in Pairs: SABL & DI gates

SABL:



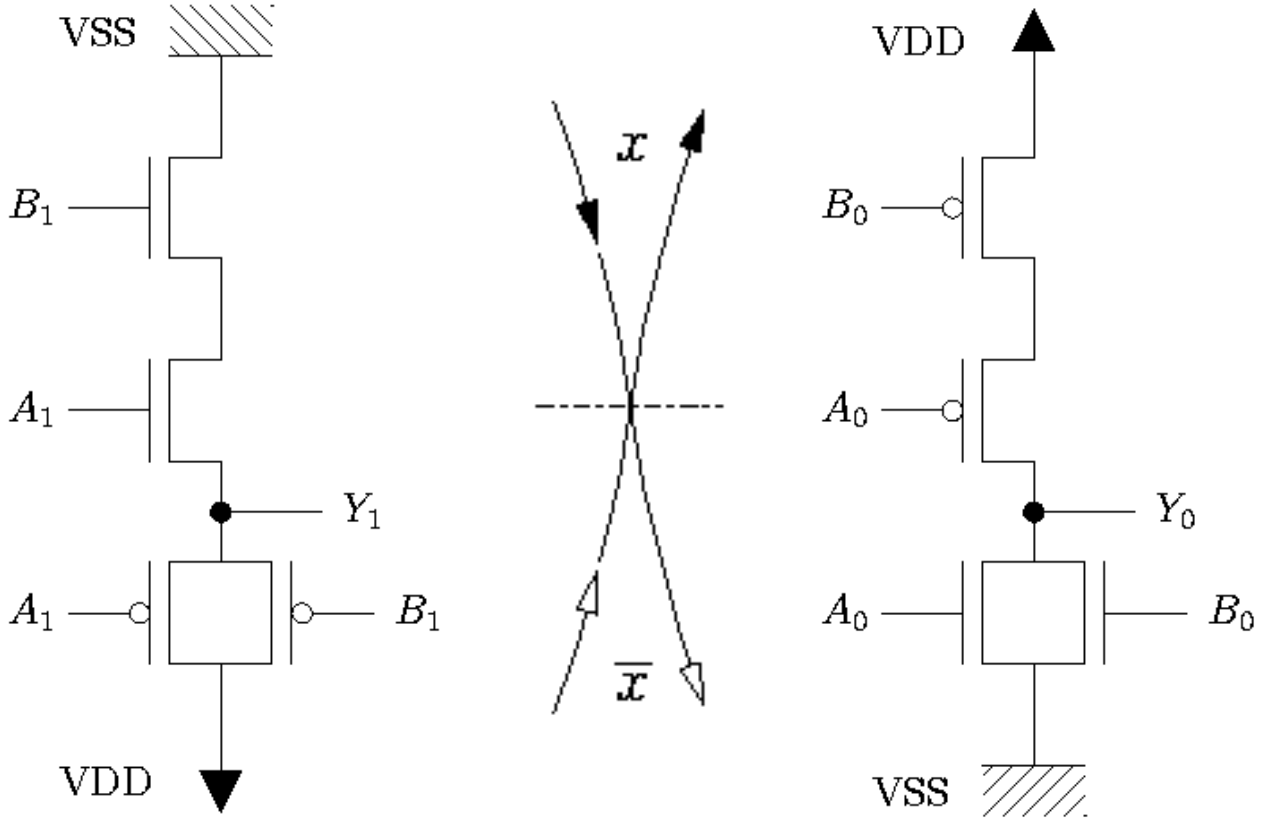
DI:



WDDL example: placement strategy

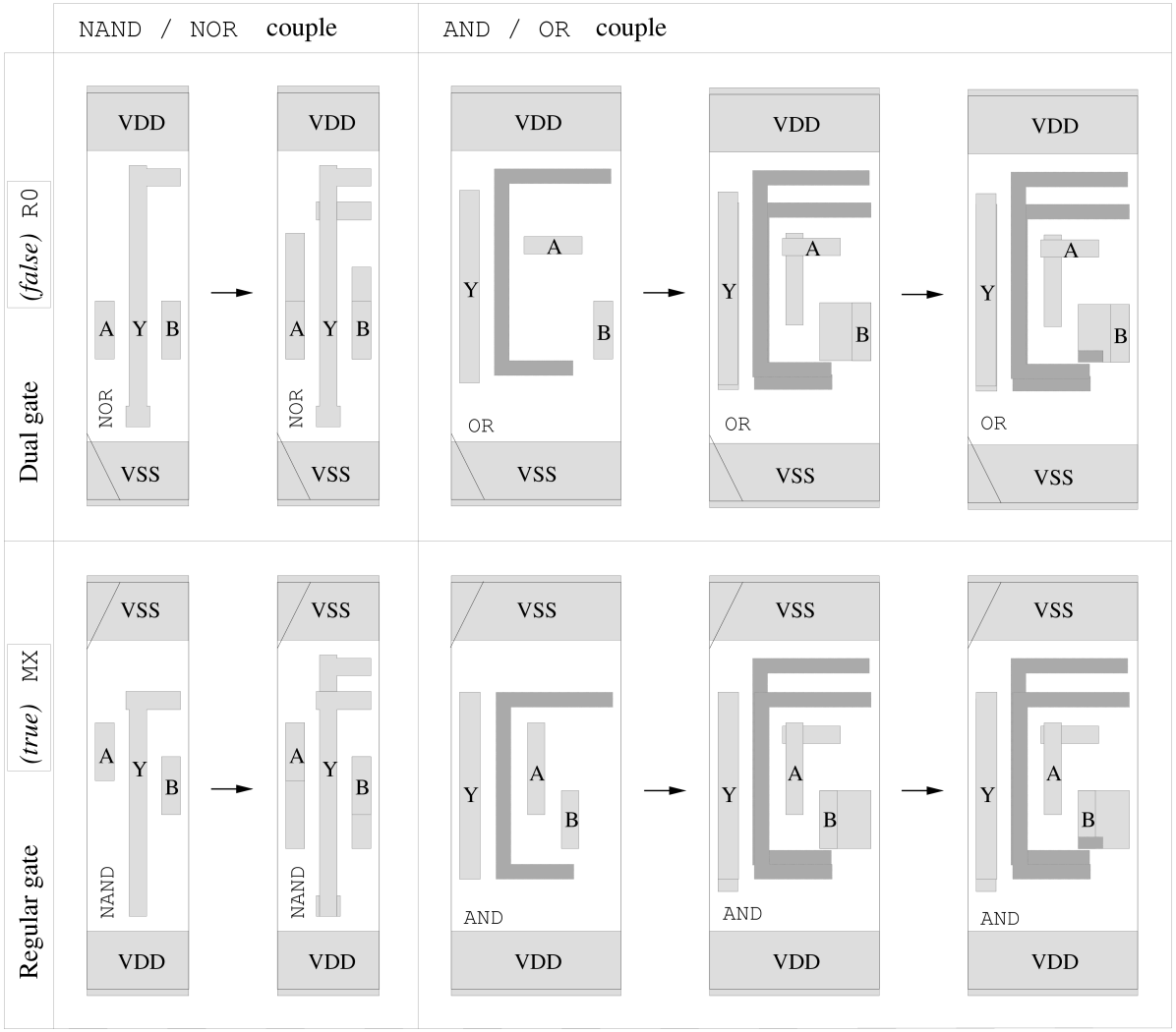
NAND (R0)
placed into row *i*

NOR (MX)
Placed into row *i+1*



After they are flipped R0 and MX, dual gates are much alike!

Making Standard Cells Compliant with WDDL



Each dual pair must have a compatible interface.

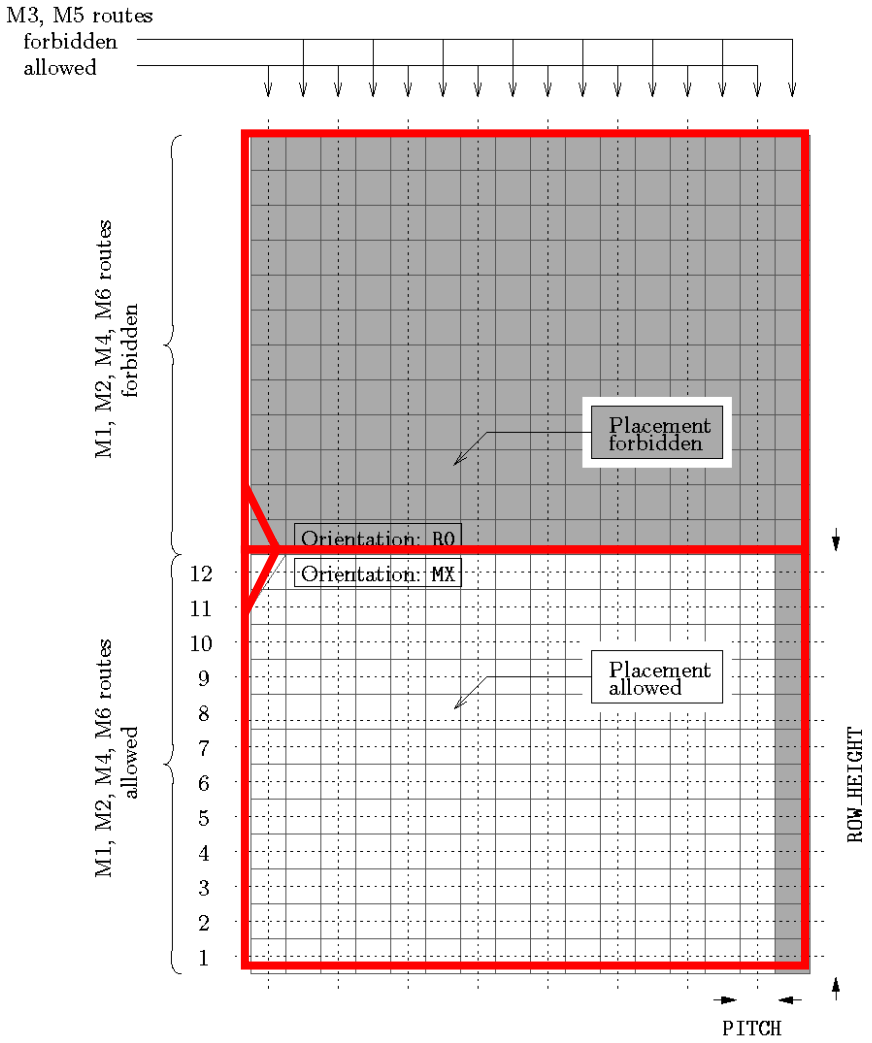
The transformation done on the abstracts (LEF description) + pins metal consists in:

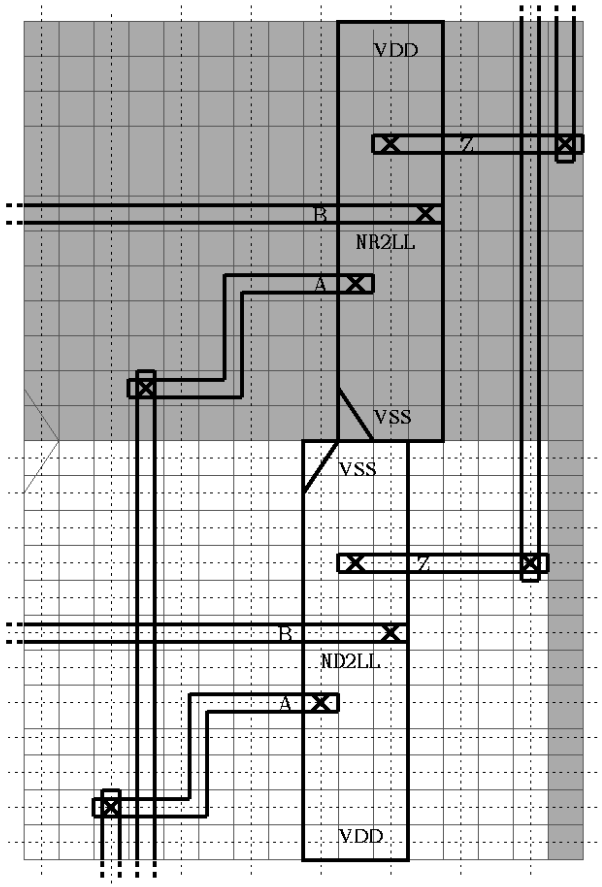
1. **Reorder pins**
2. **Enlarge pins for overlap**
3. **Keep pins intersection**

At that point:

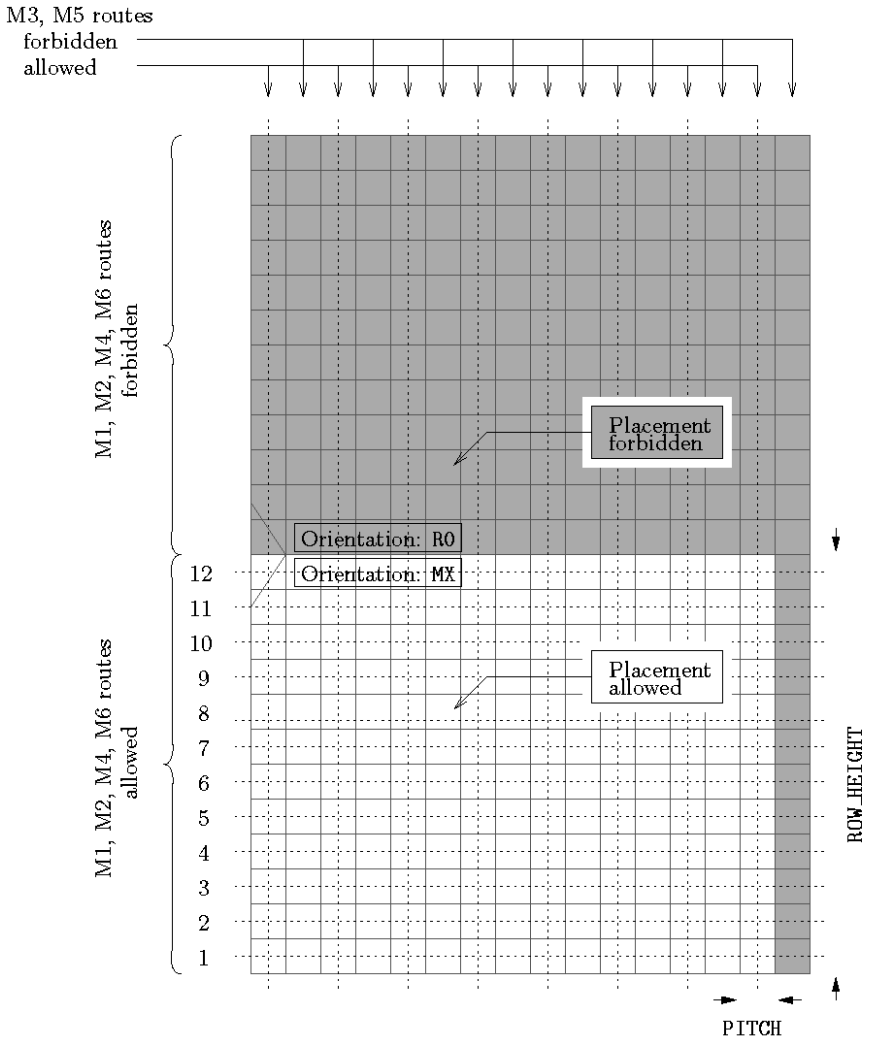
- **dual cells have similar layout in transistor**
- **the port position allow for a differential routing**

« Backend-duplication » overview

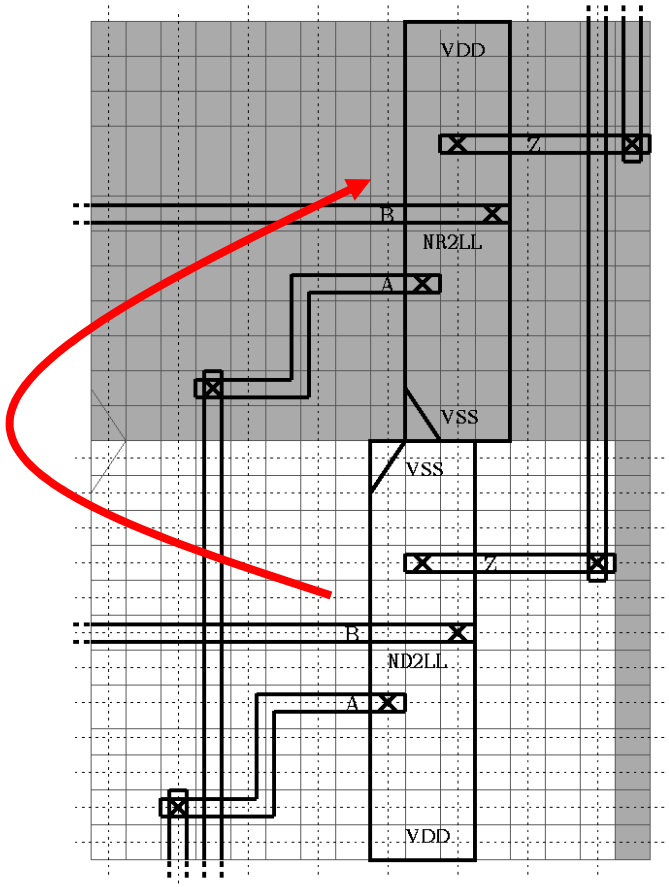




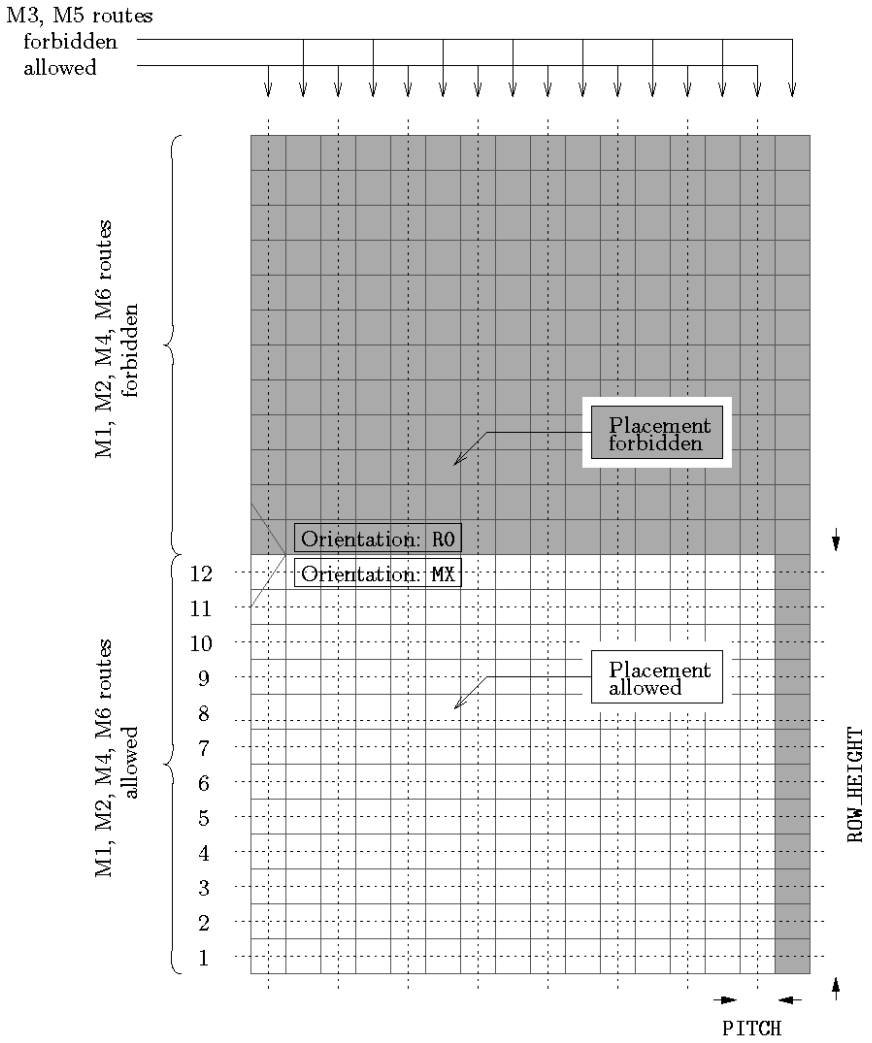
« Backend-duplication »: placement



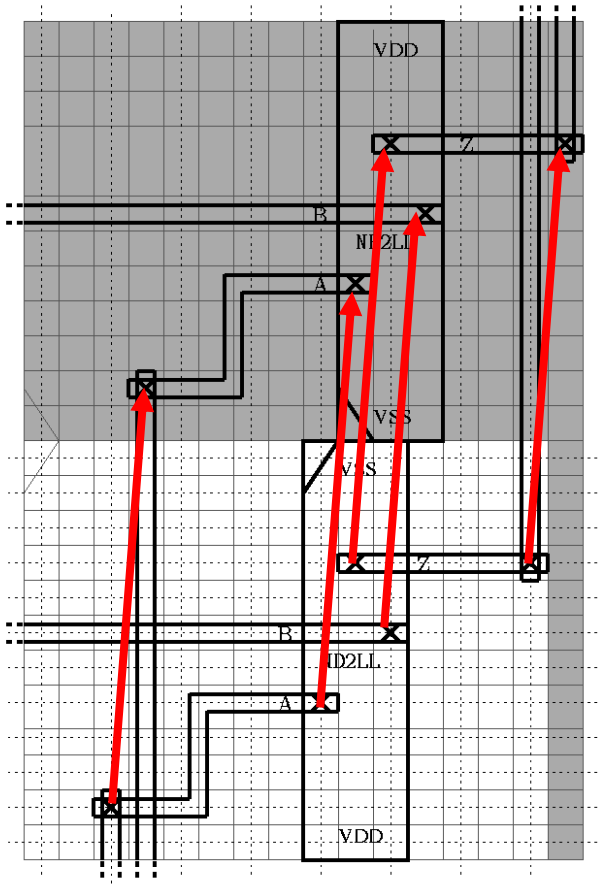
Flip Placement



« Backend-duplication »: routing

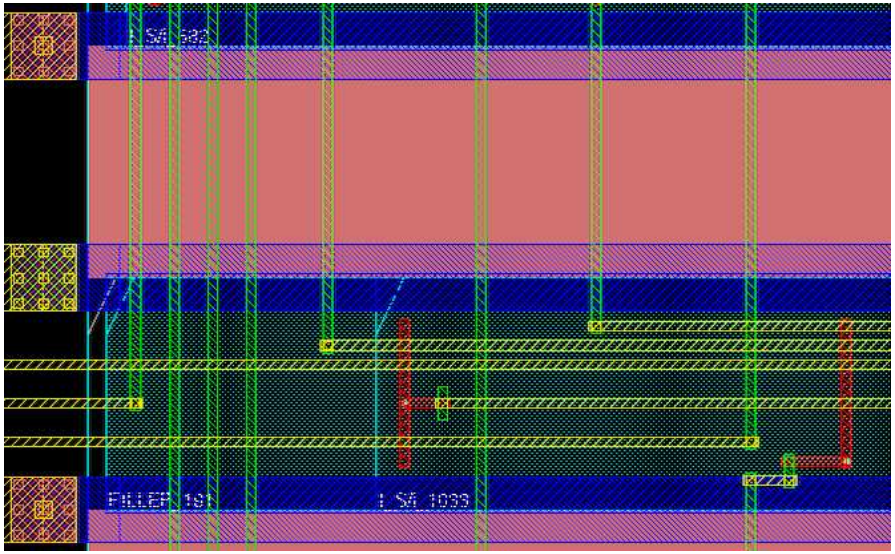


Translate routing



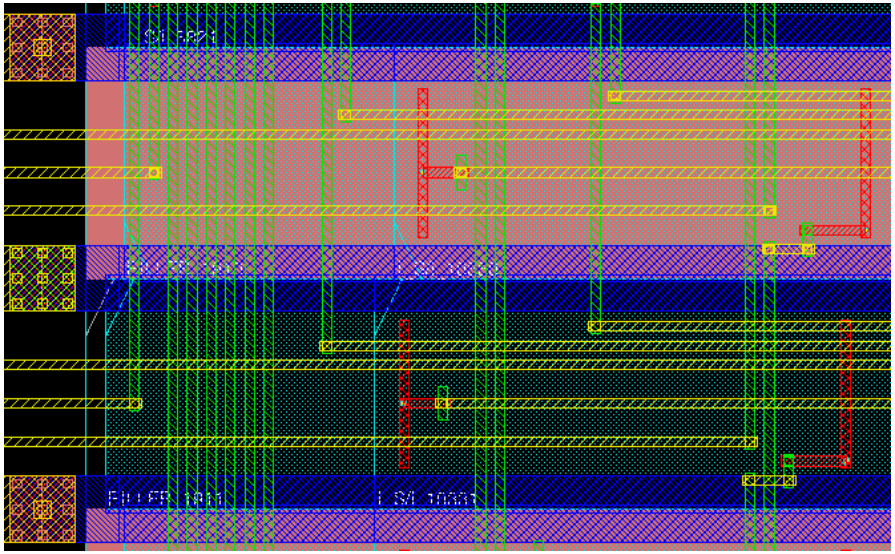
« Backend-duplication » Realization

Before duplication



- Half of the placement rows are obstructed
- Half of the routing channel are obstructed

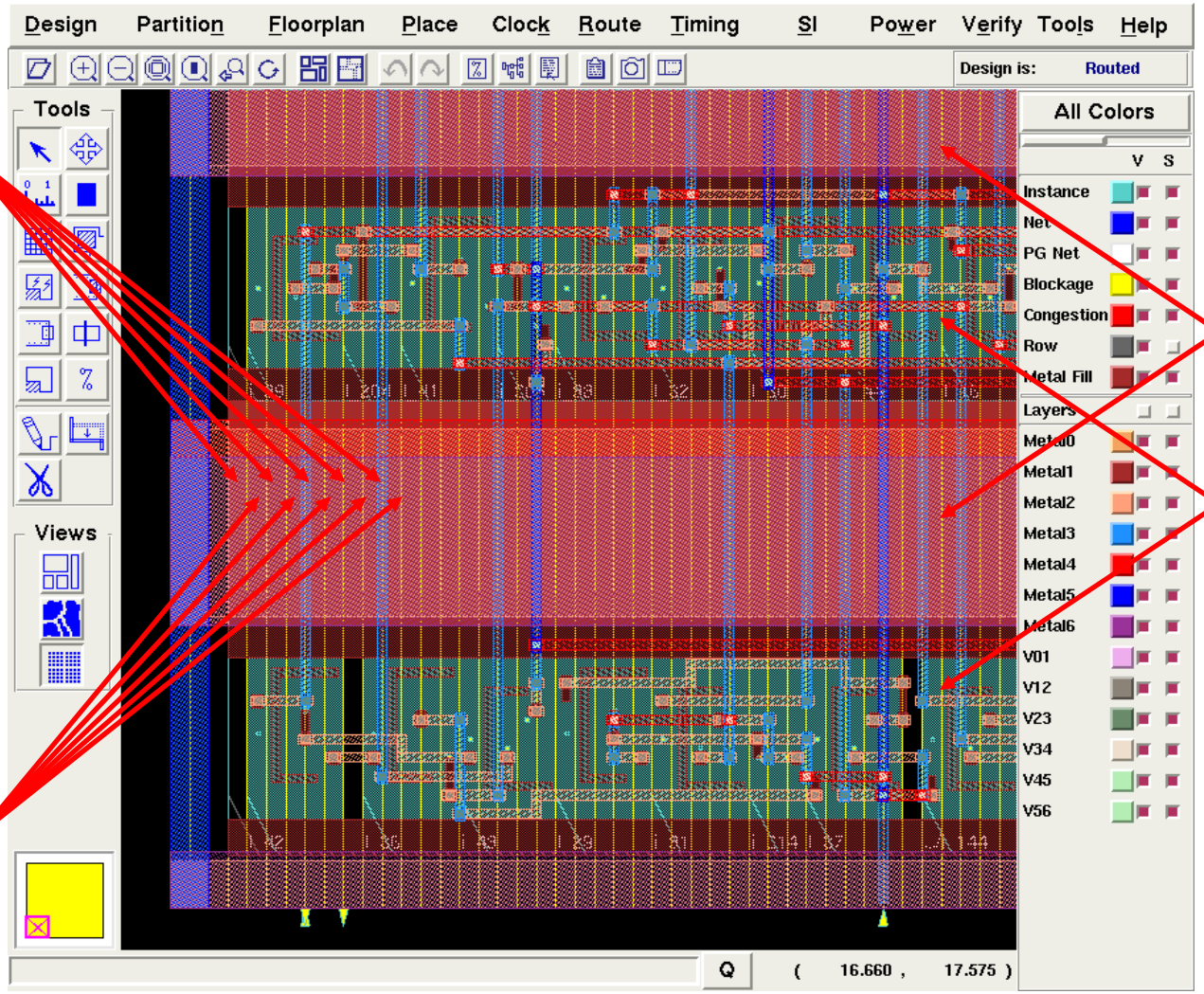
After duplication



- Cells are duplicated by vertical flip (`R0`→ `MX`)
- Routing is translated by: (`PITCH`, `ROW_HEIGHT`)

The method fully relies on the setting of appropriate constraints

WDDL example: constraints



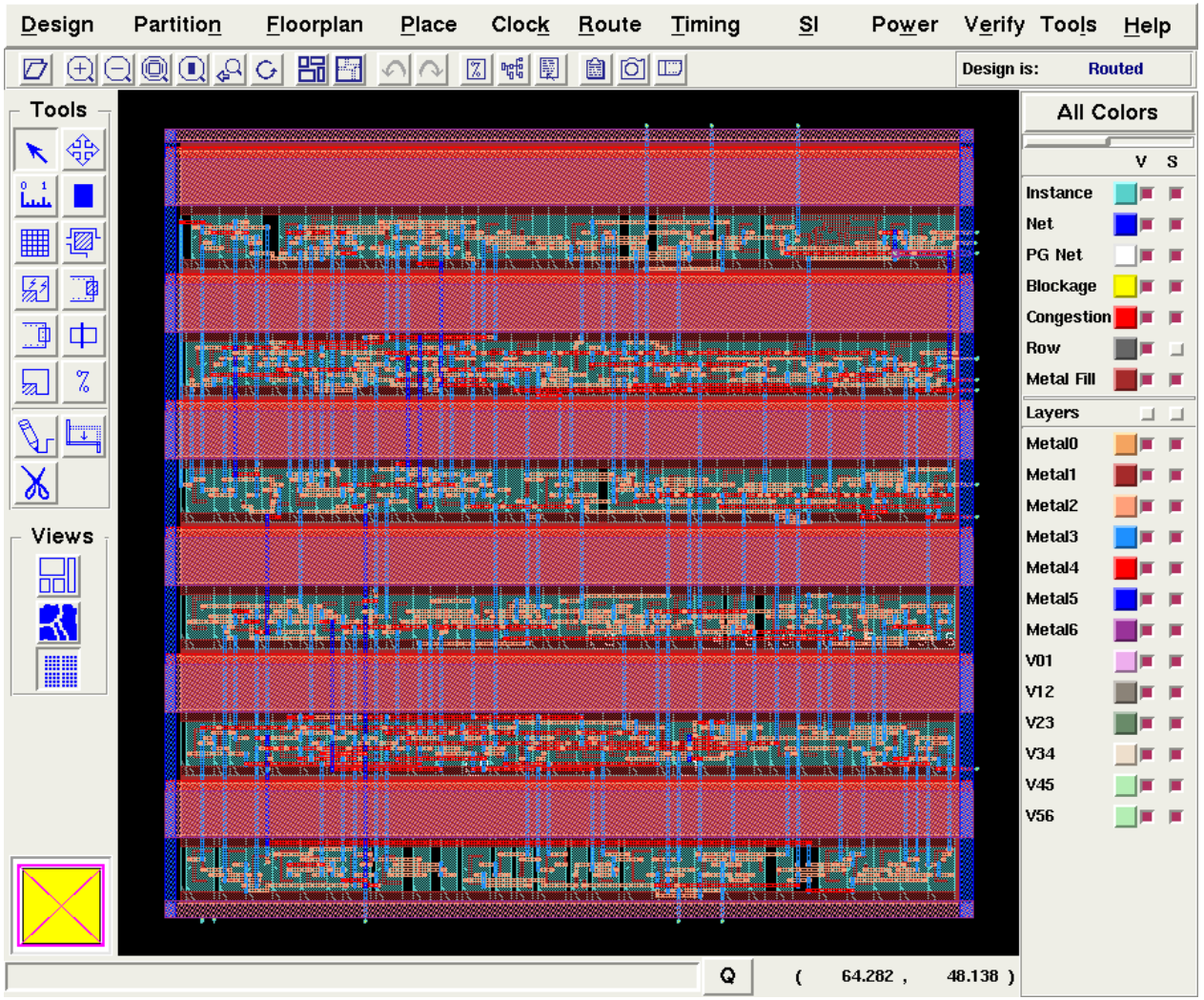
No vertical routing

Vertical routing OK

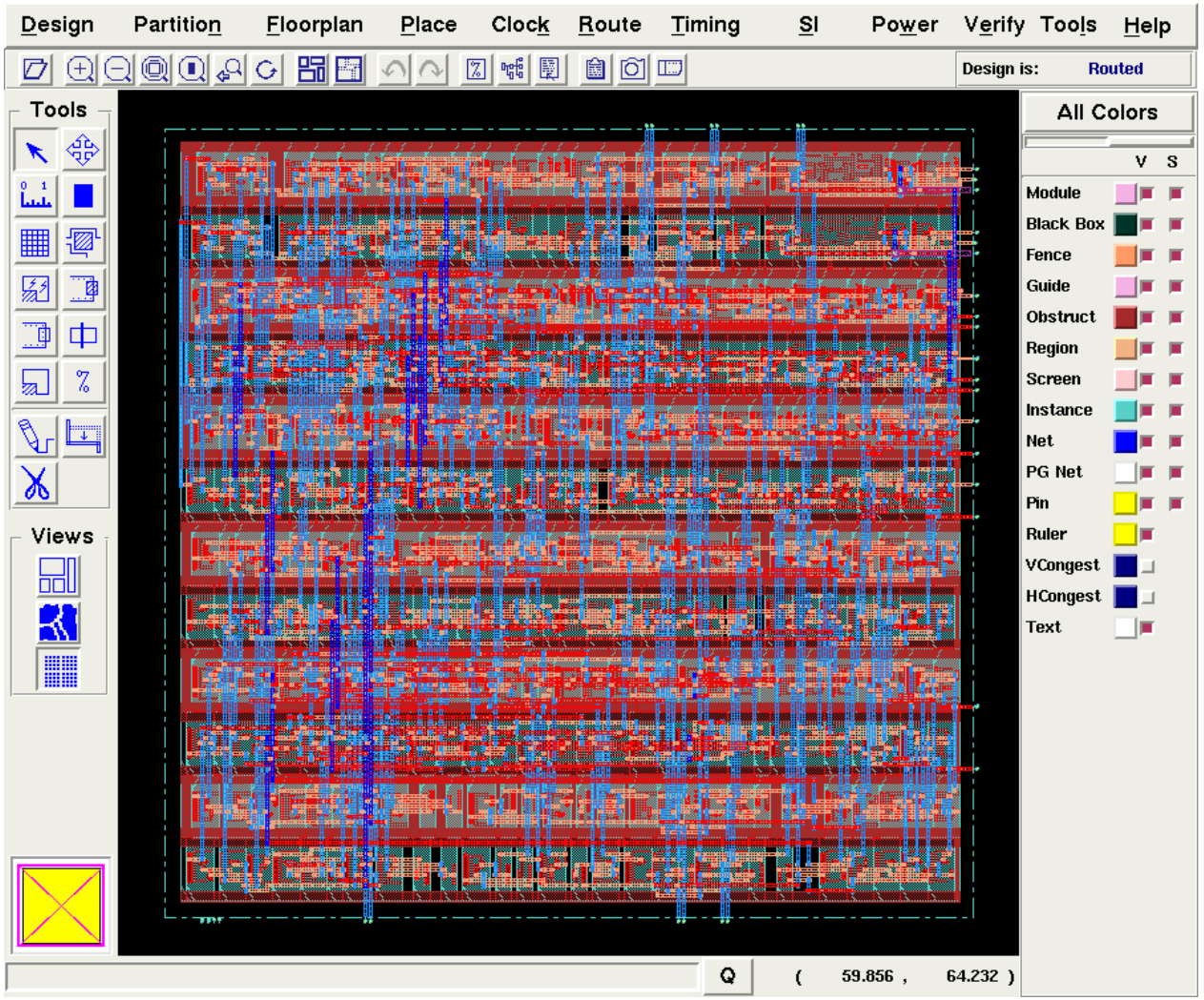
No placement
No routing

Placement OK
Horizontal routing OK

WDDL example: before duplication



WDDL example: after duplication

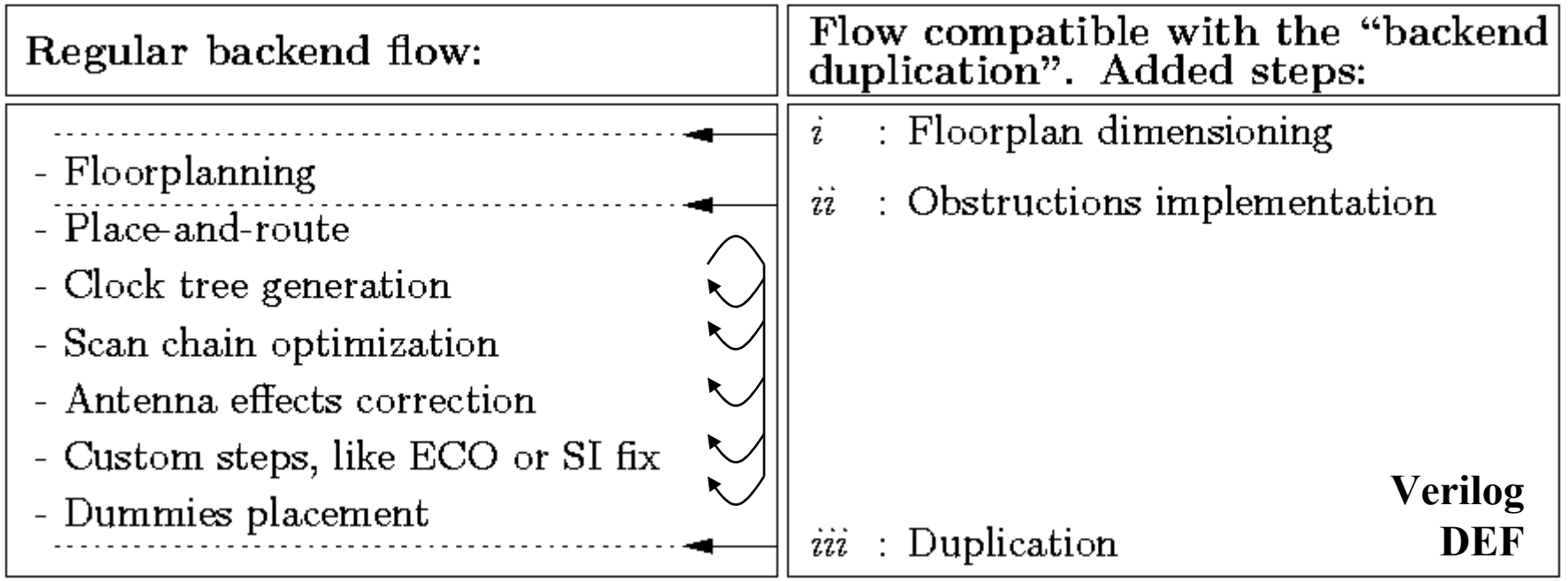


Note:

Results can be visualized in a backend tool without rewritting (*error-prone*) nor reloading (*not interactive*) design rules.

Implementation

+3 lines added in the Makefile:

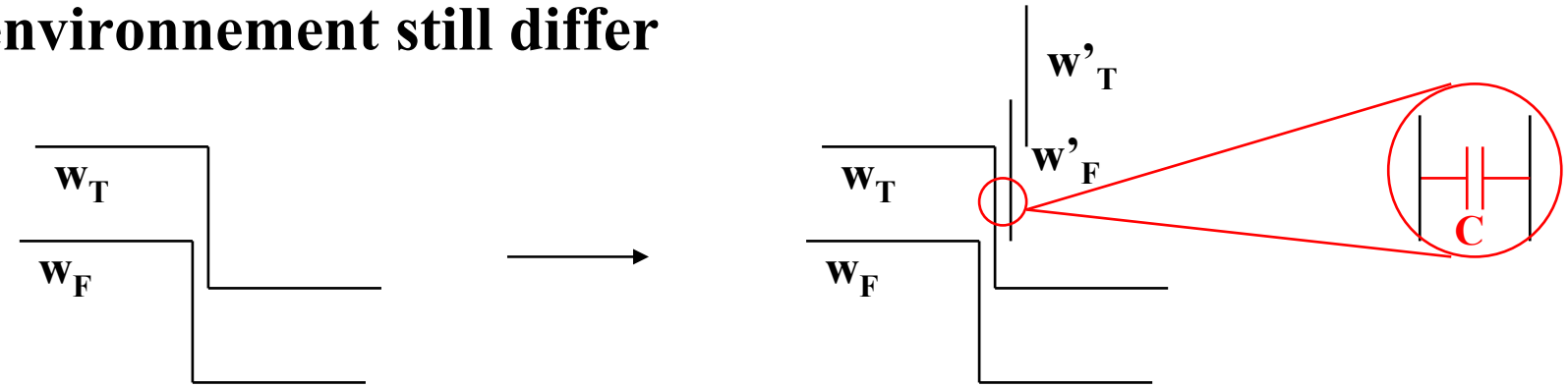


Execution time in the example of DES:

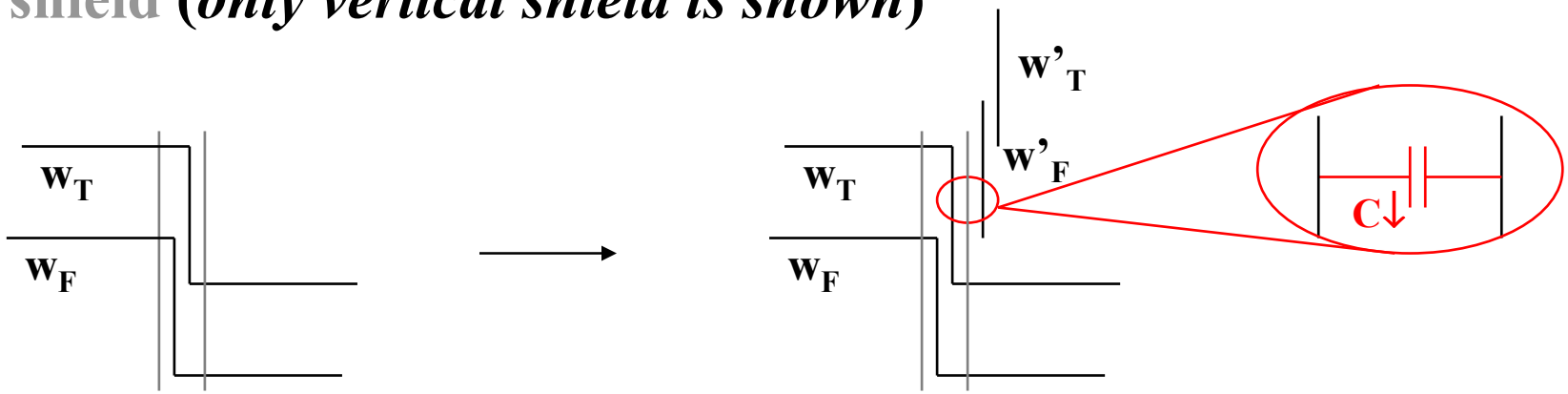
	Regular	Backend-duplicated
Place	1.9 s	6.2 s
Route	39.0 s	80.0 s
Duplication	-	77.5 s

Cross-coupling

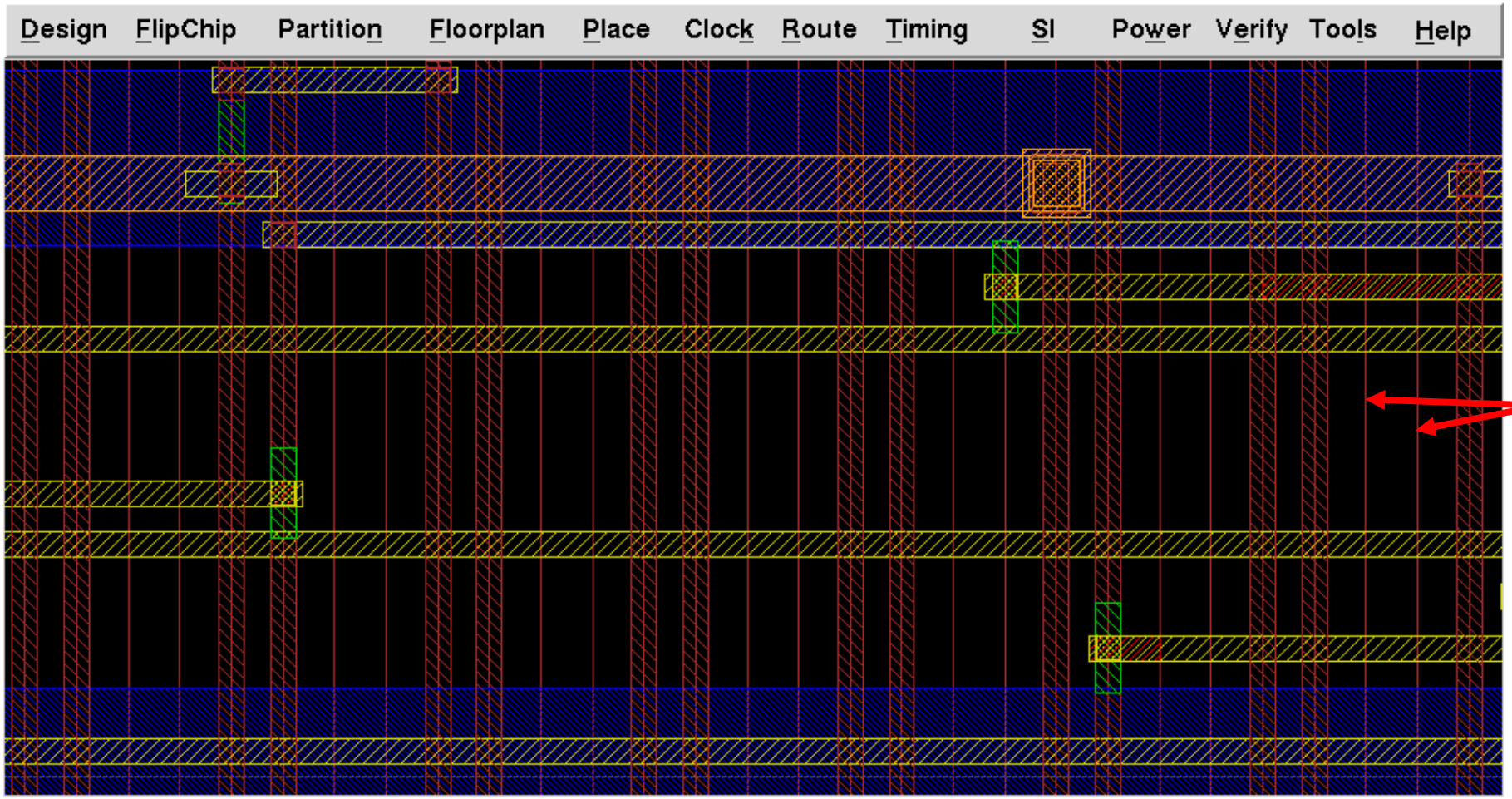
- The method achieves the same routing length and shape
- But the environnement still differ



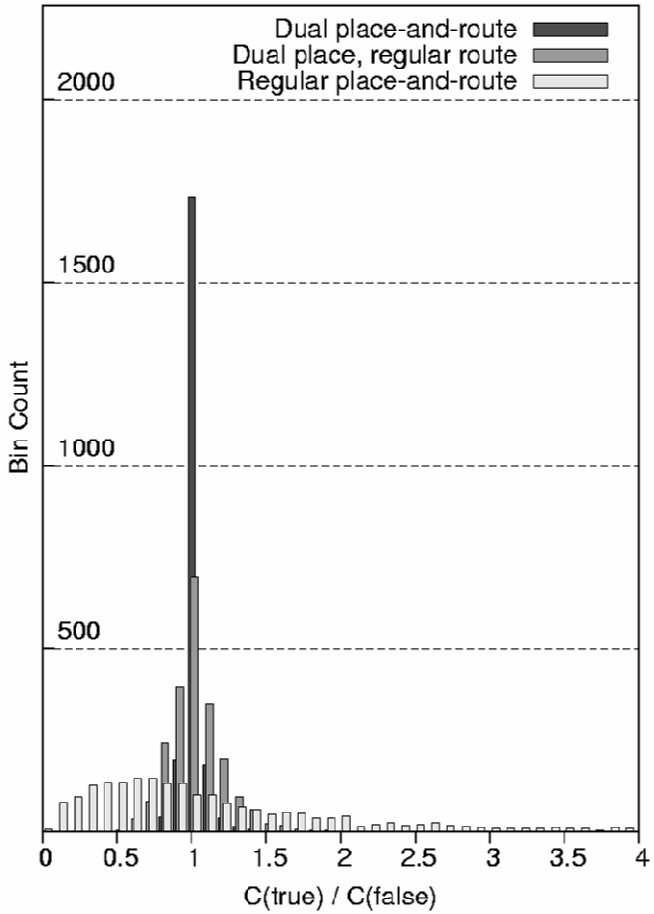
- Solution: shield (*only vertical shield is shown*)

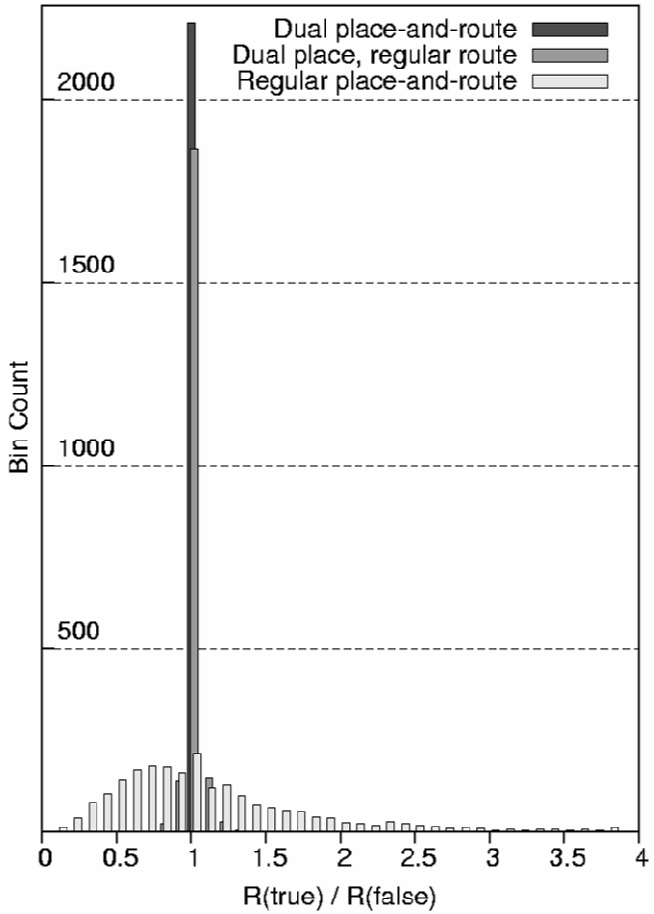


Reducing the cross-coupling: routing constraints



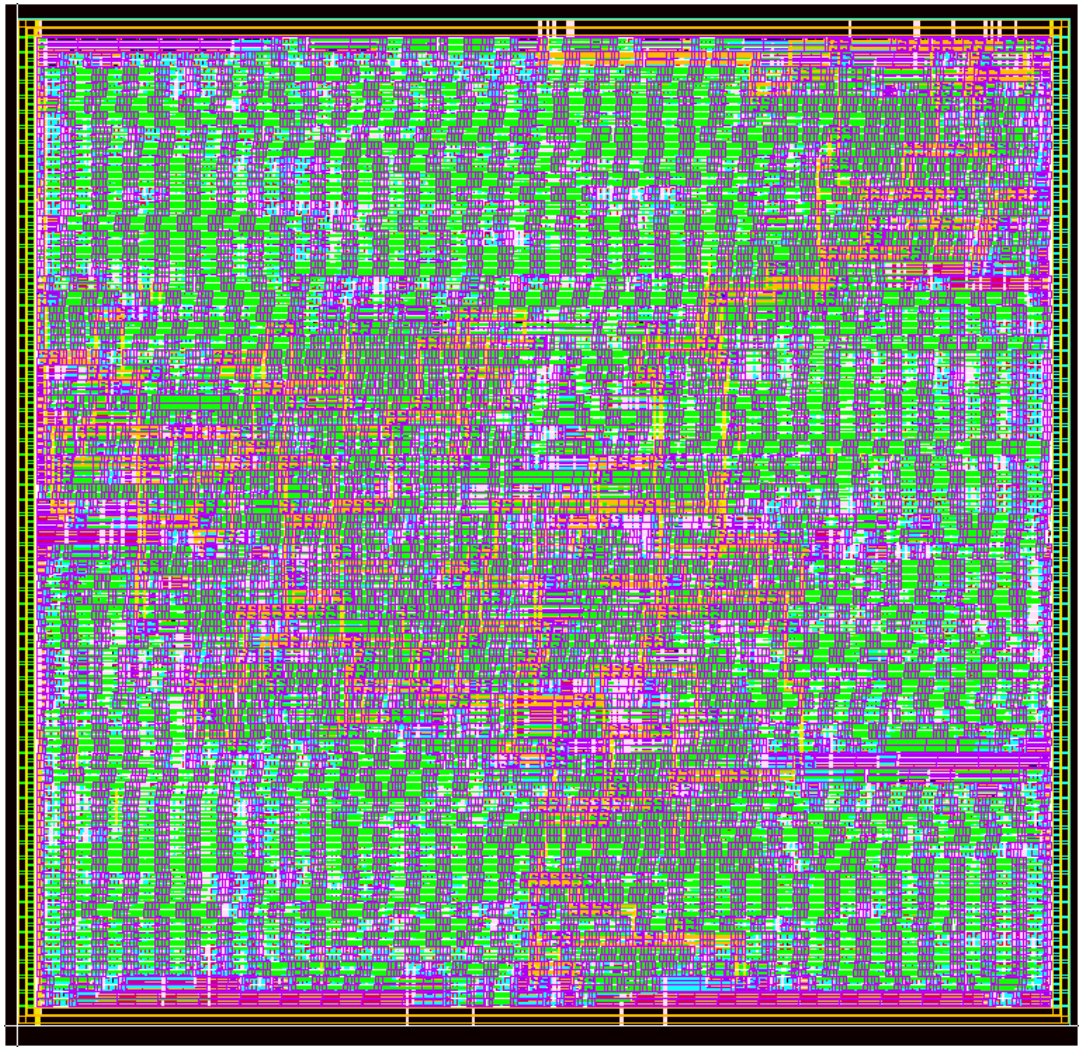
« Backend Duplication » Efficiency Assessment





Secure DES (SDES) after P&R

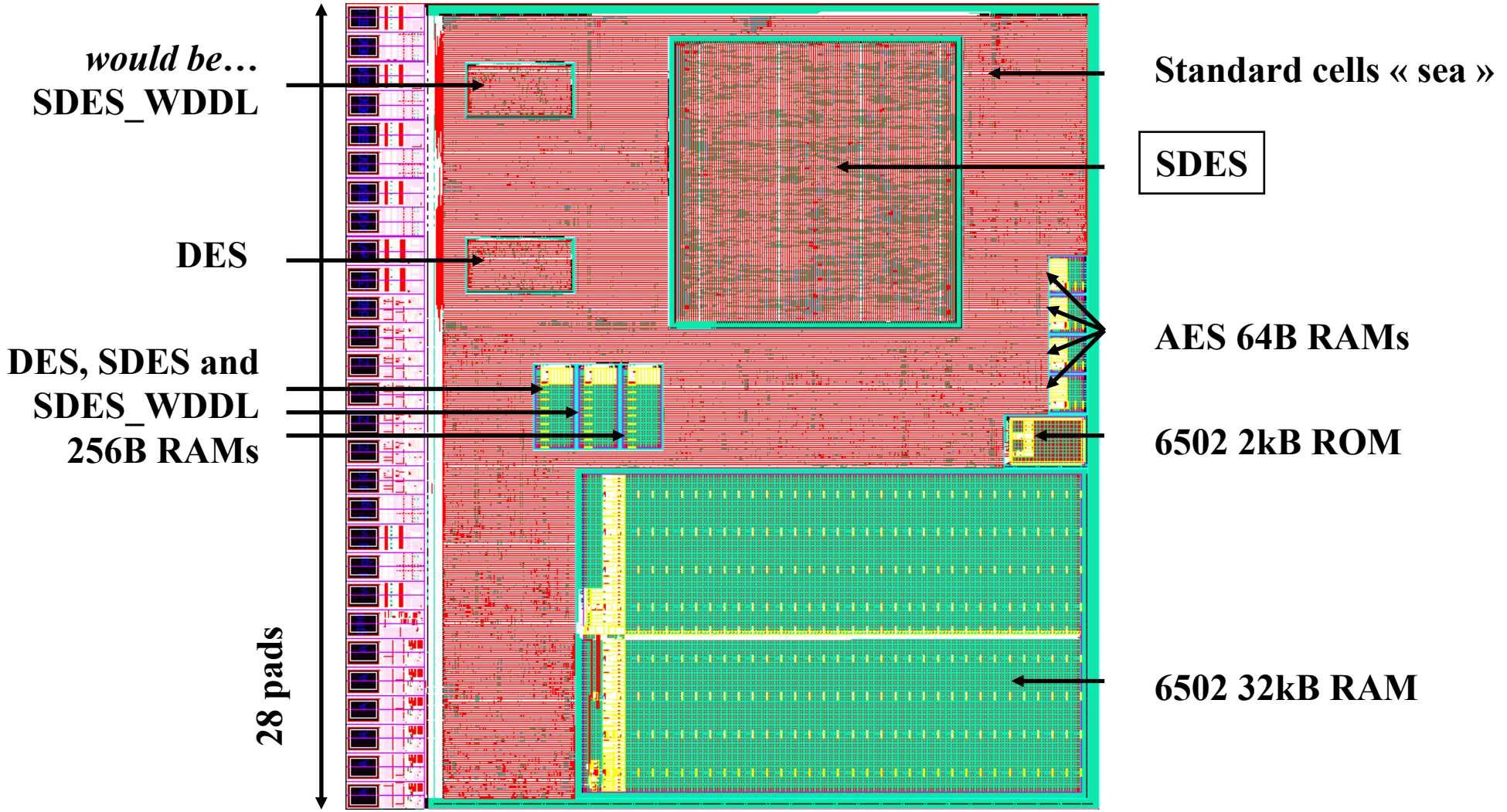
This P&R has been done with **SecLib** auto-dual cell pairs. The dual abstracts superimpose.



Floorplan duplication visual « effect »: the rows go by pairs.

The duplication flow is independent of the CAD tools used.

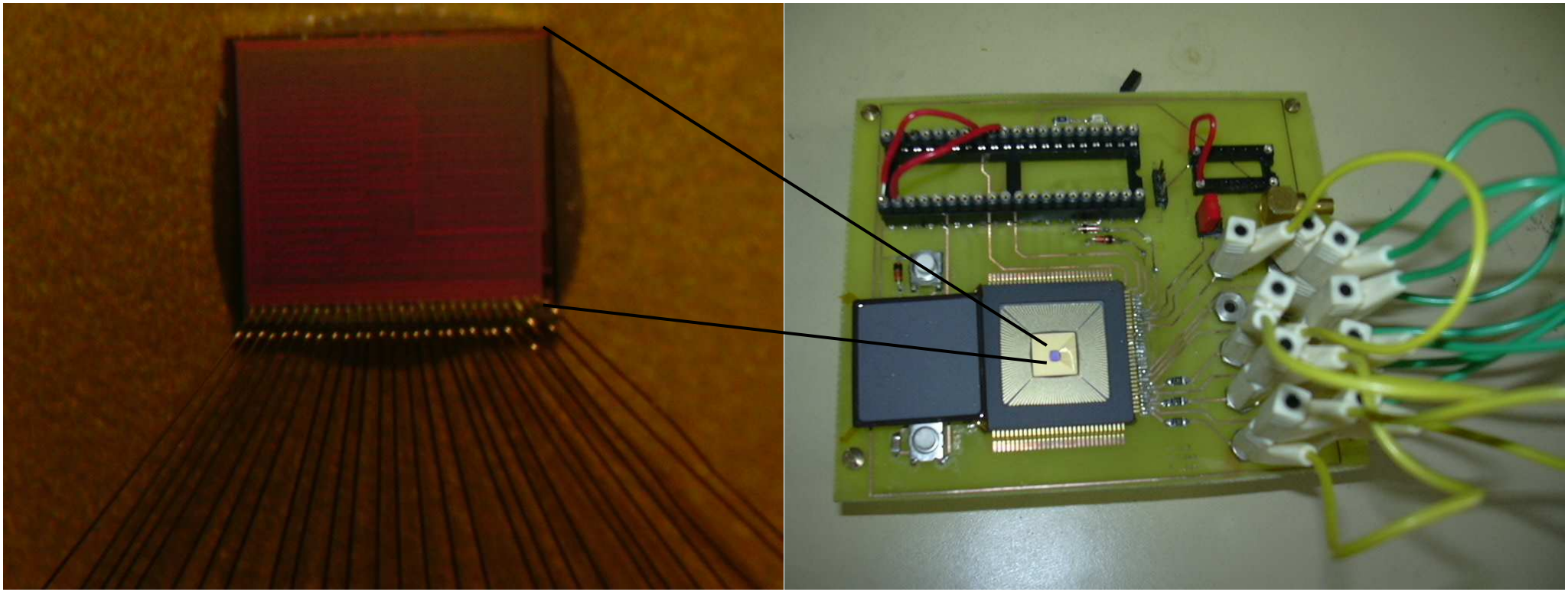
SECMAT chip under Cadence



SECMAT Pictures

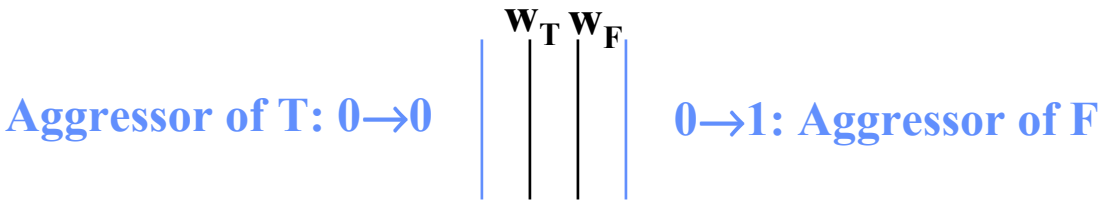
The silicon die

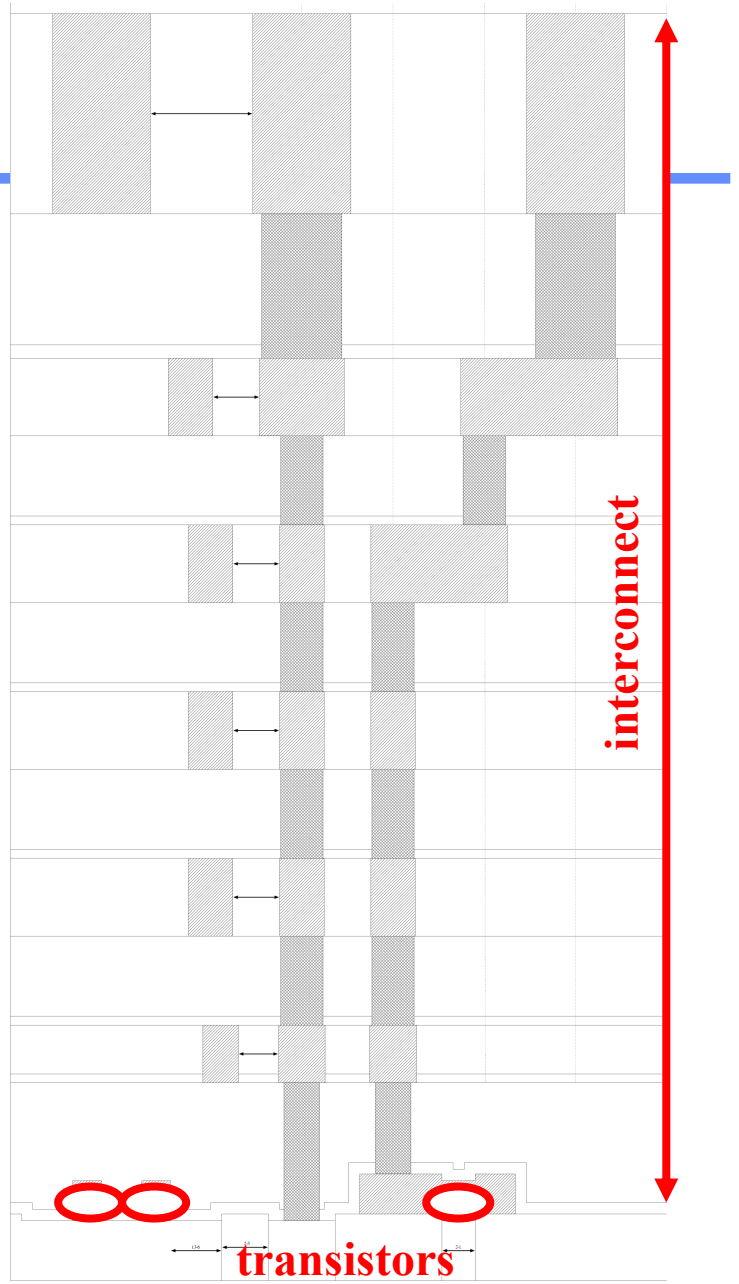
The test motherboard



Secured P&R: Perspectives

- In deep submicron technologies, the interconnect accounts for a large amount of the power dissipation
- Twisted pairs routing to thwart EMA?
- Efficiently using cross-talk strategies to decrease the dissymmetry of signal pairs
- Study dynamic dissymmetries occurring because of cross-talk
  - Spice simulations are the last resort?





Acknowledgements

- This work has been partially funded by:
  - the “conseil régional Provence Alpes Côte d'Azur” and
  - the French Research Ministry, through ACI SI MARS: http://www.comelec.enst.fr/recherche/mars/

- The authors are also grateful to the AST division of STMicroelectronics (Rousset, France), for help in the design and the fabrication of the secured DES ASIC prototype.

Any question?

- Comments / feedback welcomed:
  < sylvain.guilley@enst.fr >