Sécurité des Circuits FPGAs en arbre

Projet ANR ARFU7 « SeFPGA »

LIP6: E. Amouri, Z. Marrakchi, H. Mrabet et H. Mehrez

TELECOM ParisTech: J-L Danger, T. Graba,Y. Mathieu, S. Guilley, S. Somsavaddy, F. Flament, S. Bhasin et N. Selmane

PLAN

- Contexte
- Etat de l'art
- Architecture arborescente Multi niveaux MFPGA
- Partitionnement et placement contraints
- Routage balance-timing-driven

Contexte

- **Cryptographie:** l'art de chiffrer des messages pour les rendre incompréhensibles par des personnes n'ayant pas la clé de chiffrement

- Applications cryptographiques: carte bancaire, carte de santé, carte de transport, carte de télévision à péage, carte téléphonique prépayé…

- Algorithmes cryptographiques sont sécurisés au niveau mathématiques (DES, AES …)

- **Mais:** leur implémentation physique dévoile des informations reliées à la clé secrète

Contexte

- Attaques par canaux cachés (temps d'exécution, consommation de courant, radiation électromagnétique)

- **DPA** (Differential Power Analysis): proposée par Paul Kocher, 1999

Contexte

- Attaques par canaux cachés (temps d'exécution, consommation de courant, radiation électromagnétique)

- **DPA** (Differential Power Analysis): proposée par Paul Kocher, 1999

  - Basée sur une analyse statistique des profils en consommation de courant du circuit intégré
  - Exploite la corrélation entre la puissance consommée et l'activité du circuit
  - Transitions $0 \rightarrow 1$ et $1 \rightarrow 0$ consomment différemment

Contexte

- Attaques par canaux cachés (temps d'exécution, consommation de courant, radiation électromagnétique)

- **DPA** (Differential Power Analysis): proposée par Paul Kocher, 1999

  - Basée sur une analyse statistique des profils en consommation de courant du circuit intégré
  - Exploite la corrélation entre la puissance consommée et l'activité du circuit
  - Transitions $0 \rightarrow 1$ et $1 \rightarrow 0$ consomment différemment

➡ **Contres mesures:** chercher à rendre la consommation de courant indépendante des données

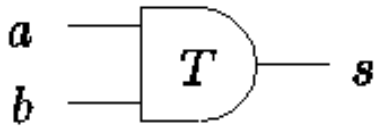
PLAN

- Contexte
- **Etat de l'art**
- Architecture arborescente Multi niveaux MFPGA
- Partitionnement et placement contraints
- Routage balance-timing-driven

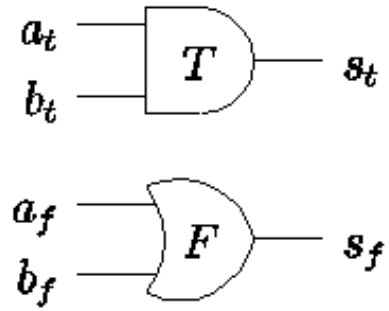
WDDL
(Wave Dynamic Differential Logic)

- Technique **WDDL**: proposée par Kris Tiri (2004)
- **Principe**: *rendre la consommation de courant constante (indépendante des données)*
- Duplication de la netlist en deux parties « True » et « False »

Porte ET

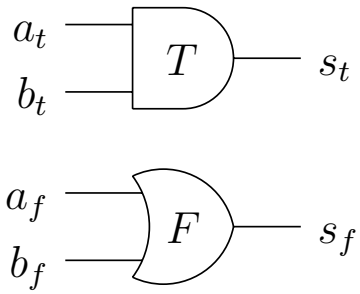


Porte ET WDDL



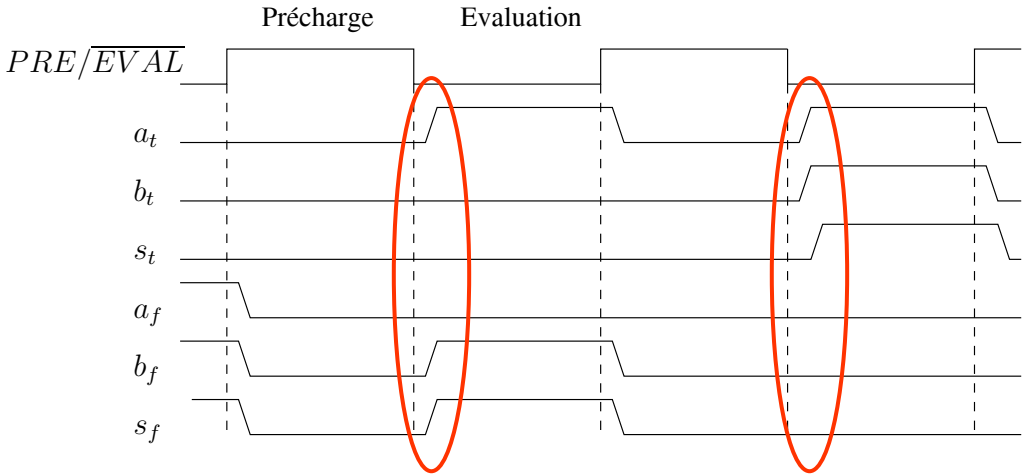
WDDL
(Wave Dynamic Differential Logic)

Porte ET WDDL



$$T(a_T, b_T) = \overline{F}(a_F, b_F)$$

- Activité constante du circuit



Nombre de Commutations = 3 = constante

WDDL
(Wave Dynamic Differential Logic)

- ***Problématique:*** Les ***signaux duaux*** doivent être ***équilibrés*** en termes de temps de propagation et de consommation de courant

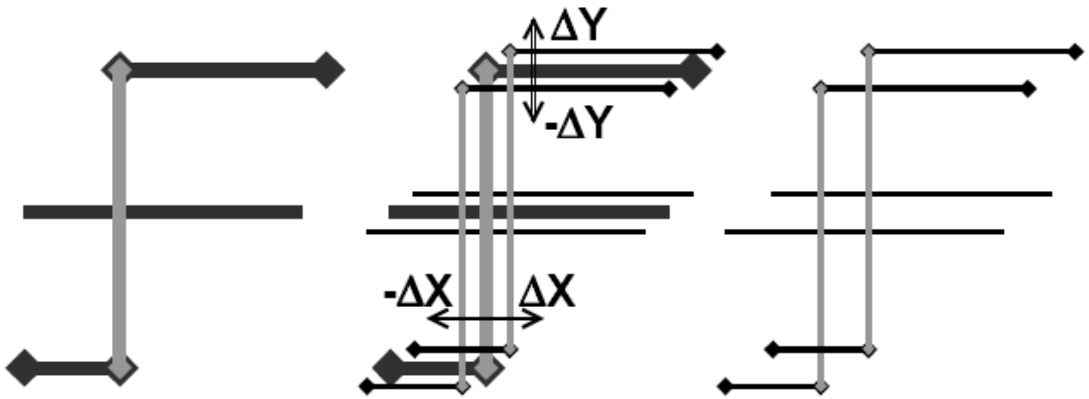
- DES WDDL a été attaqué avec succès par Laurent Sauvage et al. (2009) par attaque EMA (ElectroMagnetic Analysis)

⇒ Nécessité de placement et de routage équilibré

WDDL
(Placement et routage équilibrés)
(Travaux précédents)

ASICs

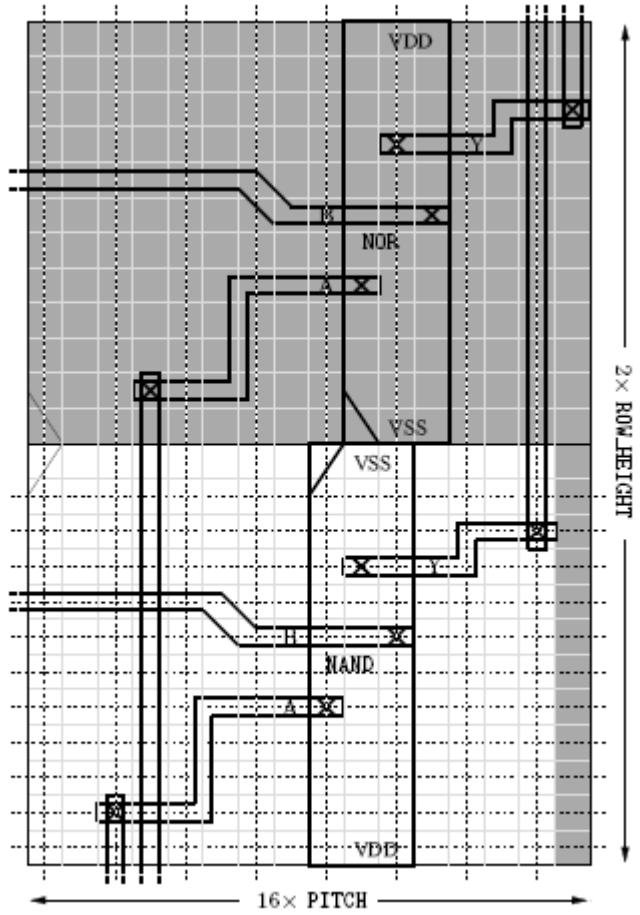
- ***Fat Wire :*** Kris Tiri (CHES, 2005)
  - Fat Wire = ensemble des deux signaux duaux
  - Transformation de deux signaux duaux en un seul signal
  - routage du circuit avec le Fat Wire
  - Décomposition du signal Fat Wire après le routage



ASICs

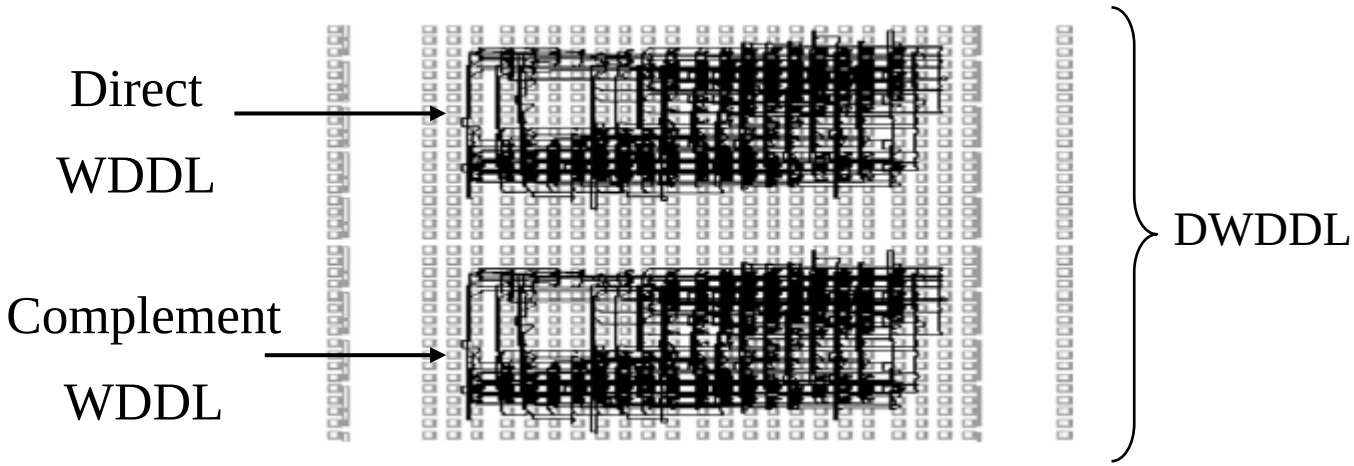
❖ ***Backend Duplication :*** Sylvain Guilley et al. (CHES, 2005)

- Placement et routage d'une sous-netlist (True ou False)
- Translation des cellules et des fils de routage



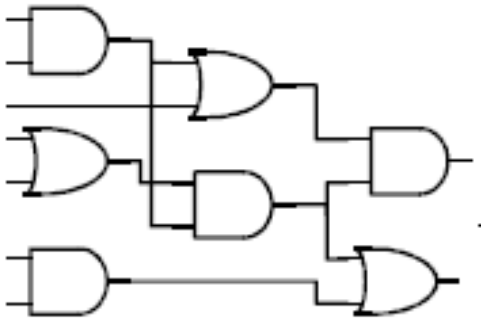
FPGAs

- ***Double WDDL (DWDDL) :*** Patrick Schaumont
  - Duplication du circuit WDDL
  - Les réseaux « True » et « False » sont inversés entre les deux circuits WDDL
  - Copie du placement et routage du circuit WDDL direct
  - ***Inconvénient:*** doubler la surface du circuit WDDL

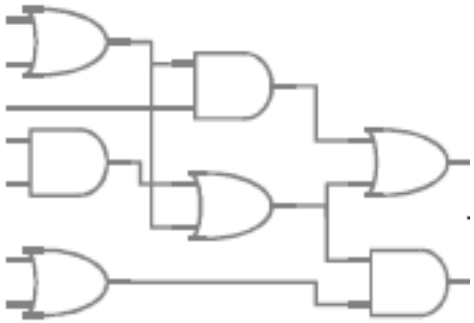


Double WDDL (DWDDL)

Patrick Schaumont



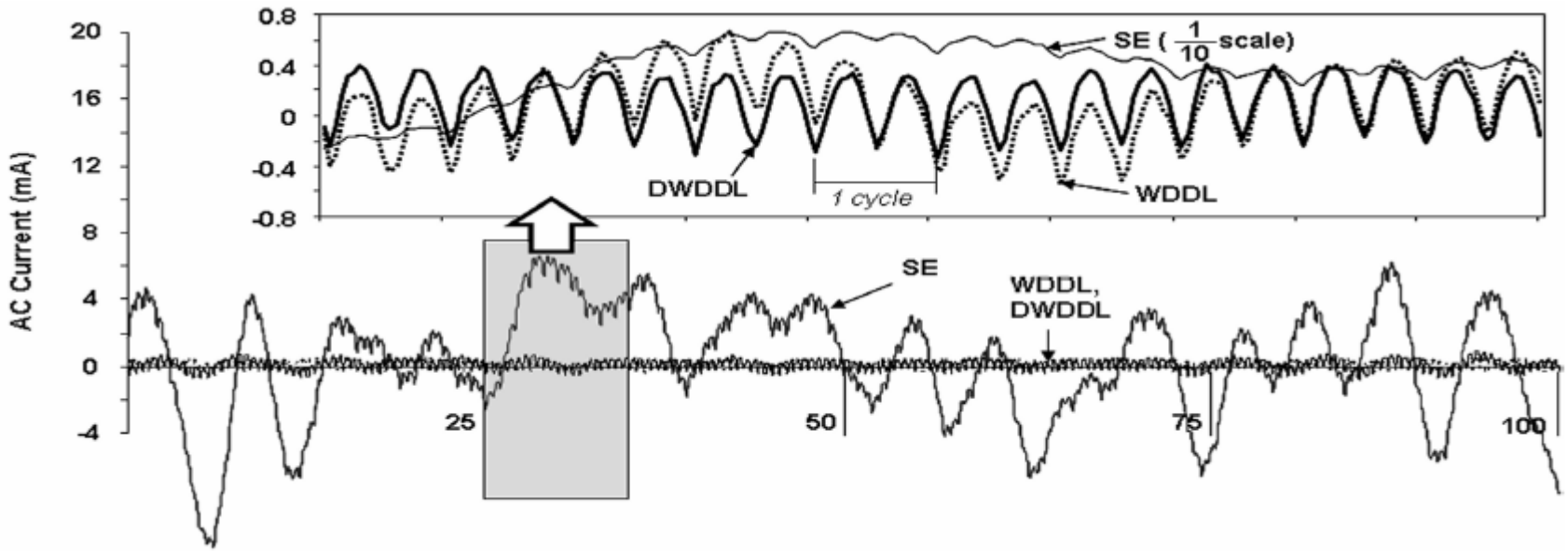
Placer & router le circuit WDDL original



1. Copier le placement et le routage du circuit WDDL original
2. Inter-changer les portes ET et les portes OU

Double WDDL (DWDDL)

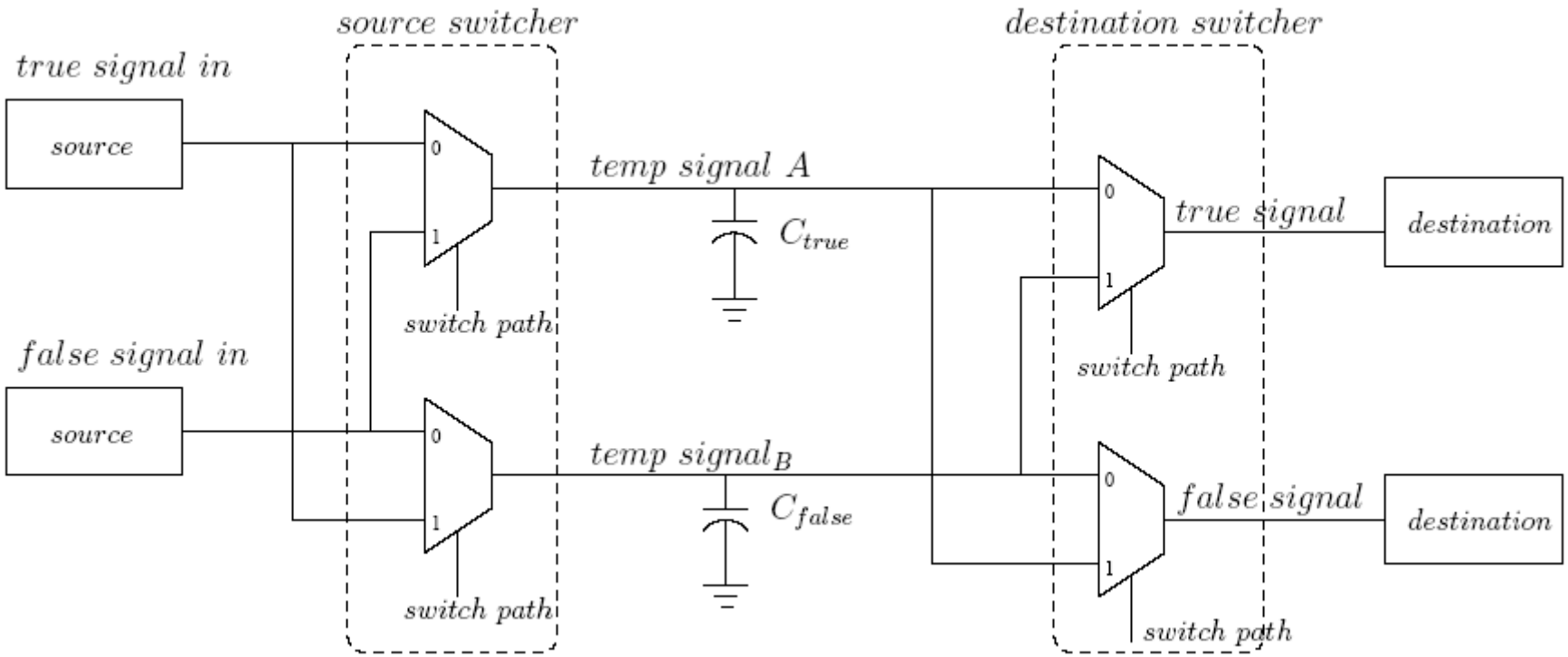
Patrick Schaumont

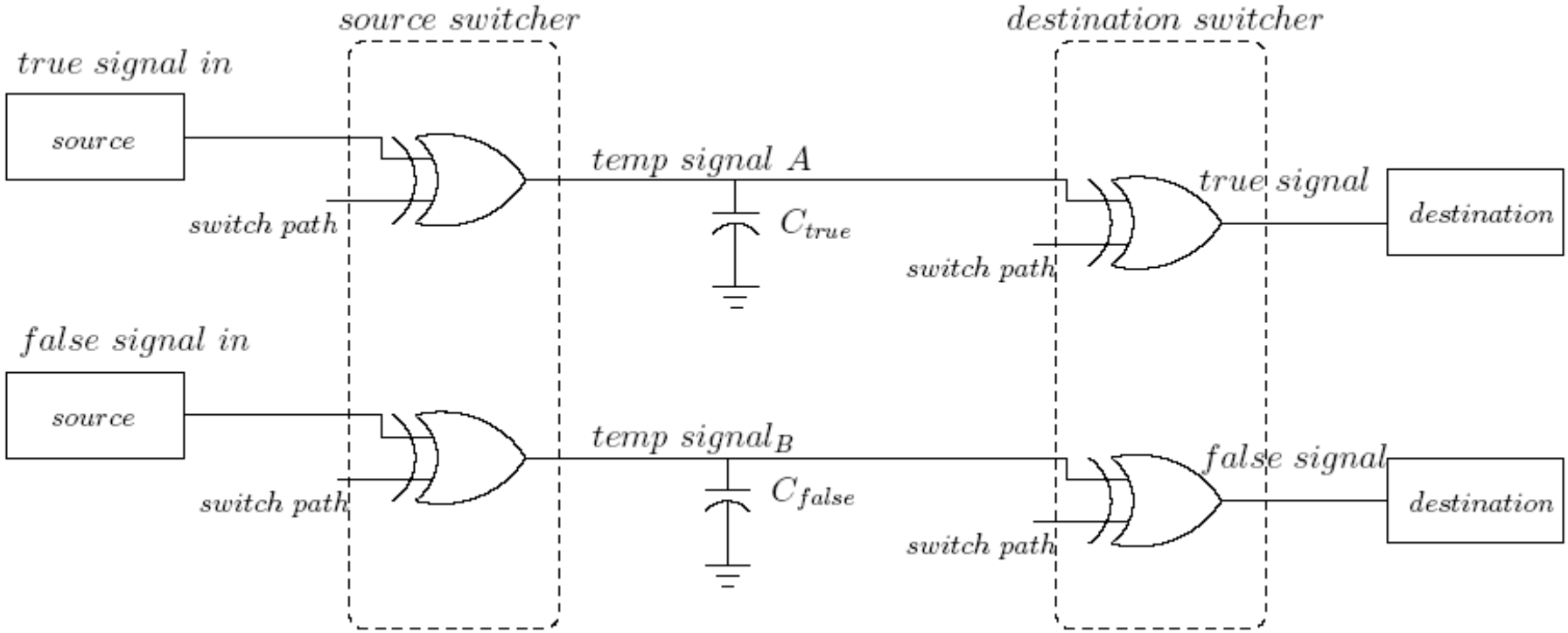


Consommation de courant pour les circuits SE (Single Ended), WDDL et DWDDL

FPGAs

- ***Path Switching Dual Rail:*** Baddam et Zwolinski



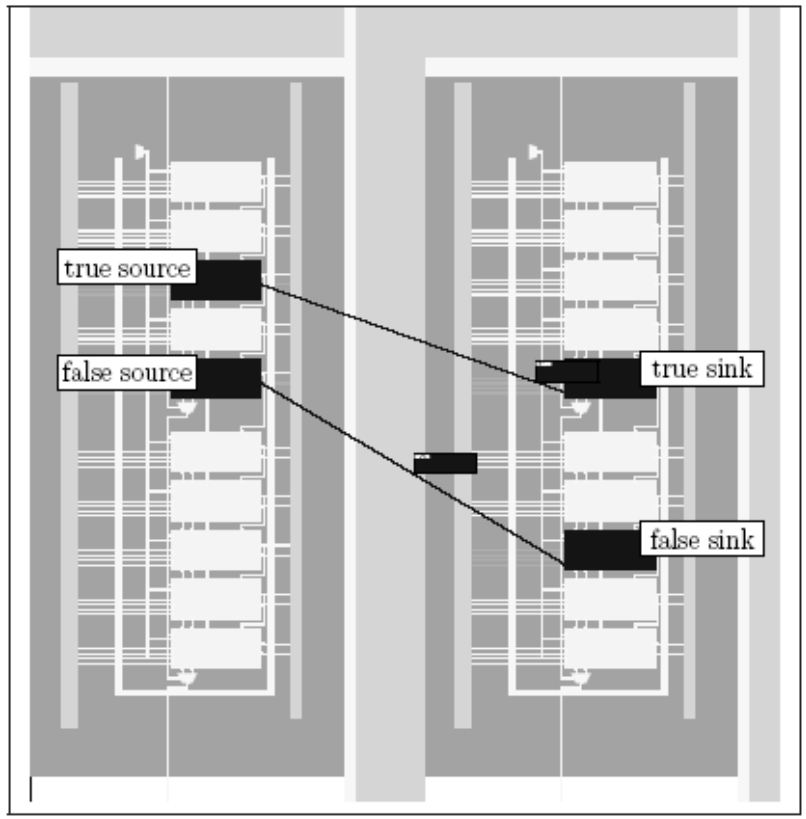


- Utilisation des XOR: surface réduite et moins de connexion
- le signal switch path est aléatoire
- But: rendre la consommation aléatoire
- lorsque le signal switch path change d'état, les chemins True et False sont inversés, mais la fonctionnalité ne change pas grâce à une inversion à la fin des chemins (juste avant la destination)

FPGAs

❖ ***Dual Placement:*** Sylvain GUILLEY

- Mettre les cellules duales dans un même LAB (ALtera) et dans un même Slice (Xilinx)
- Résultat: améliorer l'équilibre entre les signaux duaux en termes de temps de propagation.

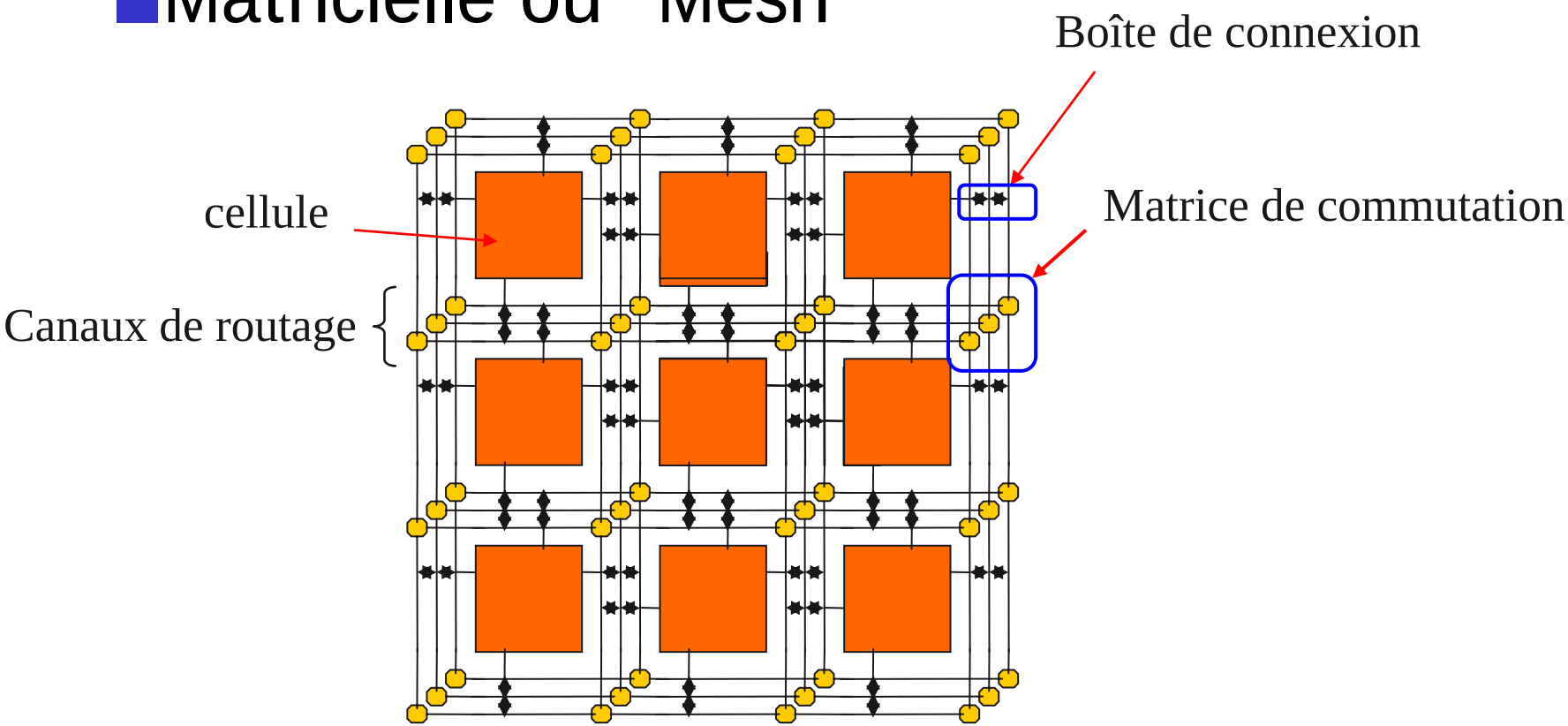


PLAN

- Contexte
- Technique de contre-mesure: WDDL
- **Architecture arborescente Multi niveaux MFPGA**
- Partitionnement et placement
- Routage balance-timing-driven

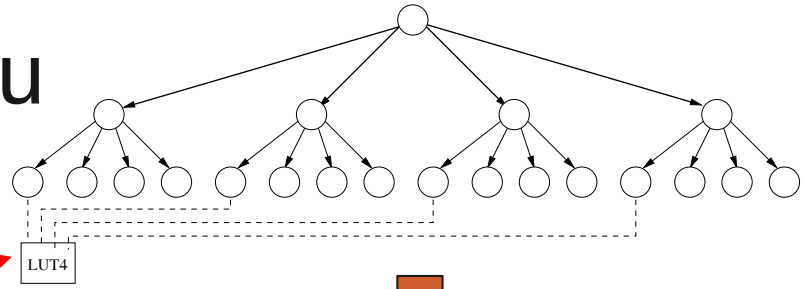
Topologie des FPGAs

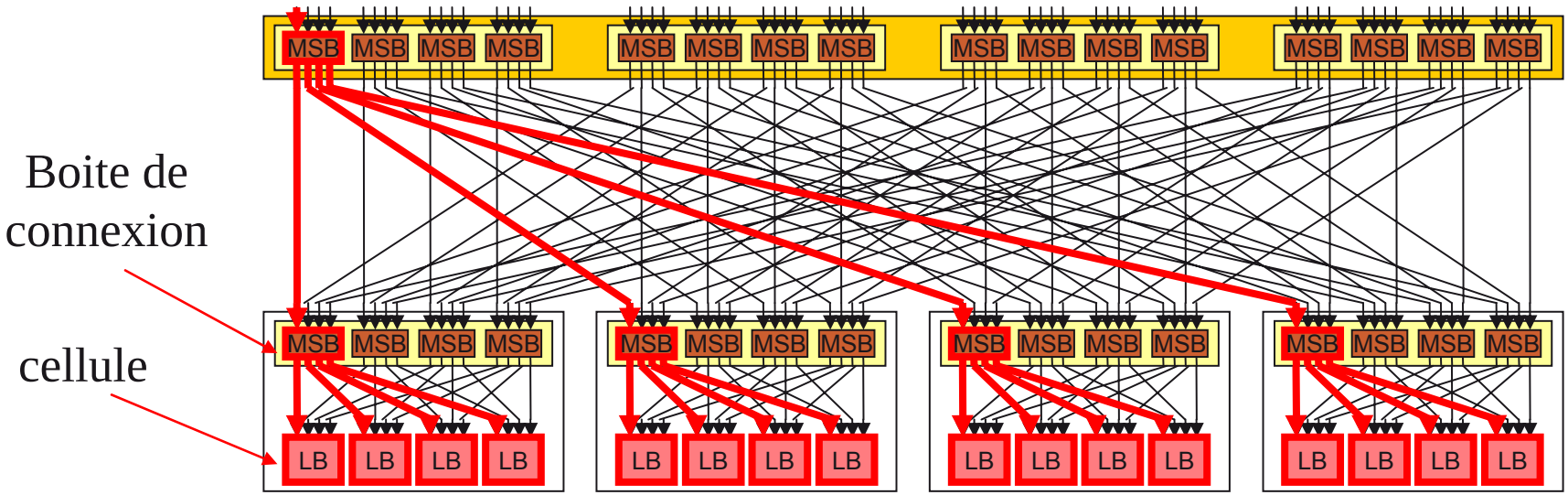
- Matricielle ou "Mesh"



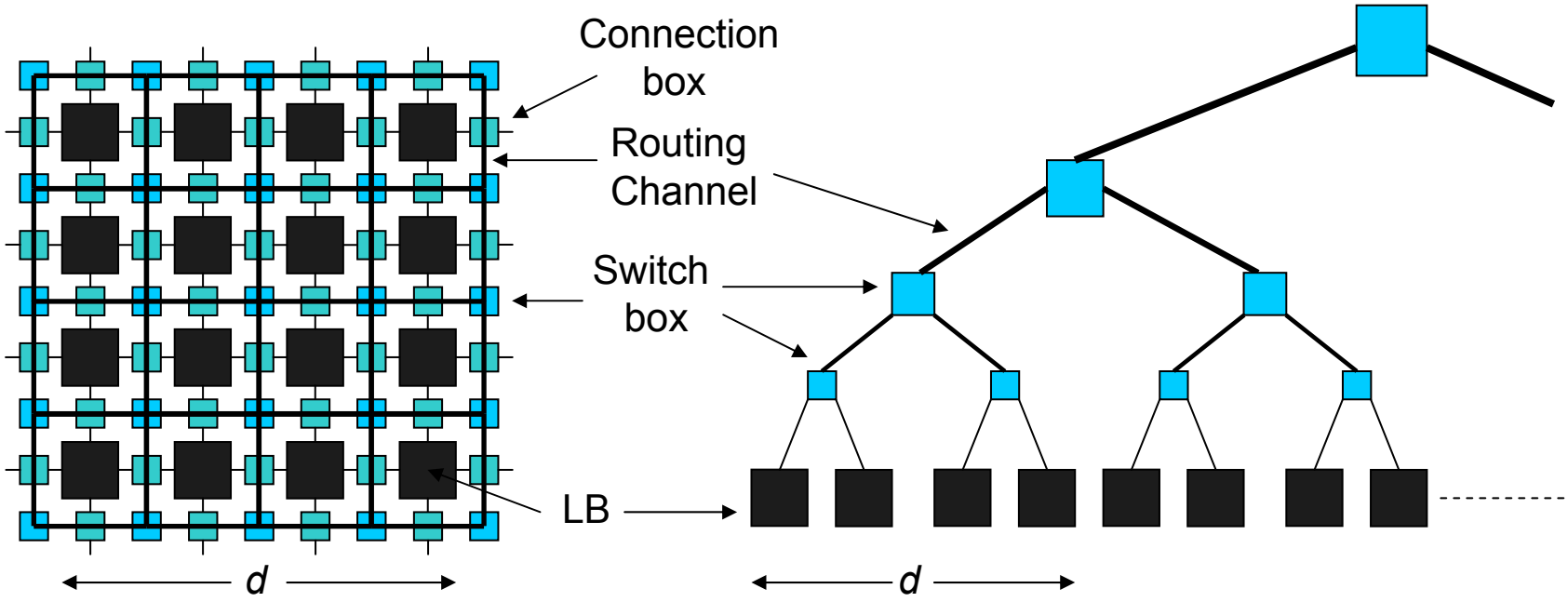
Topologie des FPGAs

- Hiérarchique ou Arborescente





Hierarchical Topology for FPGA

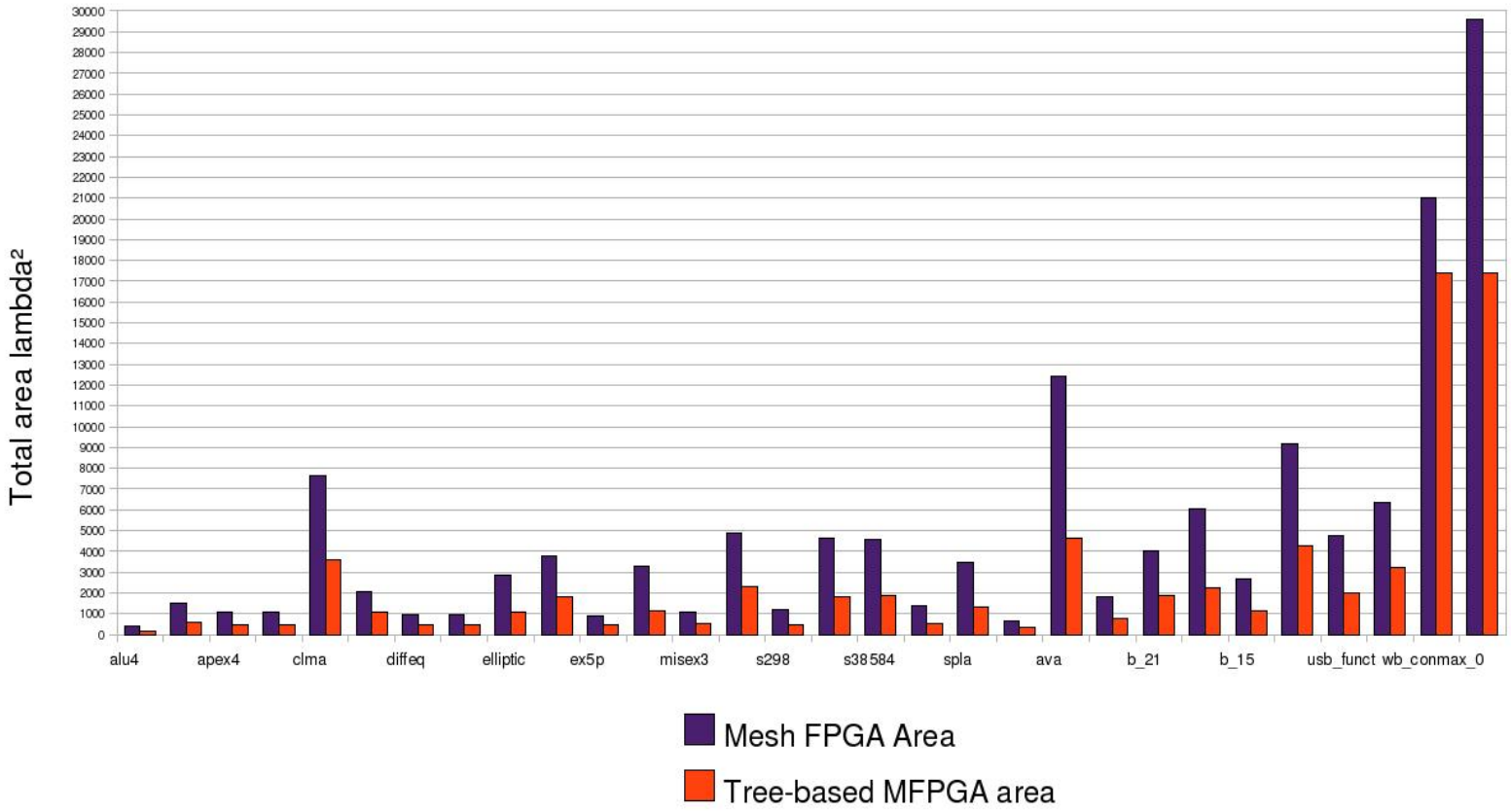


Mesh-based architecture
The number of segments in series has a linear growth with d

Tree-based architecture
The number of segments in series has a logarithmic growth with d

Experimental results

30 Benchmark circuits: MCNC, ITC, ISCAS, Opencores

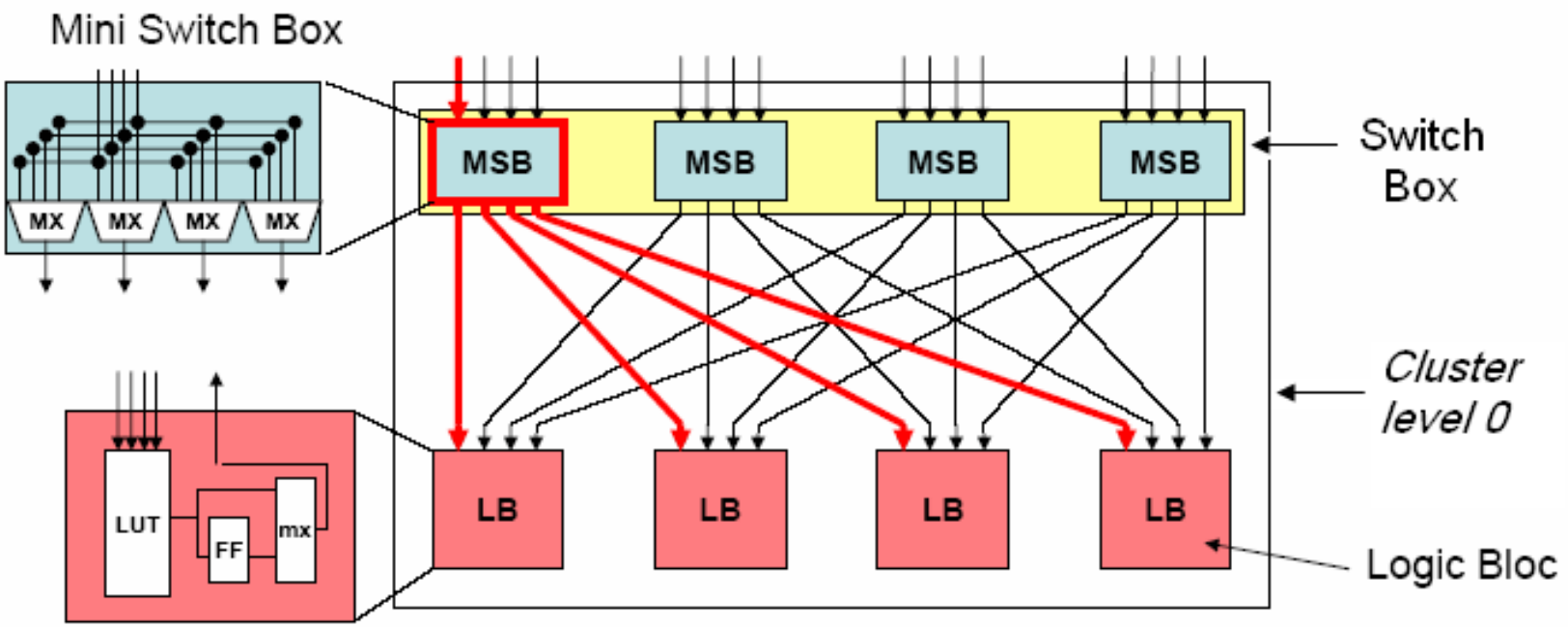


Area is reduced by 54% compared to Mesh-based architecture

Architecture arborescente Multi niveaux MFPGA

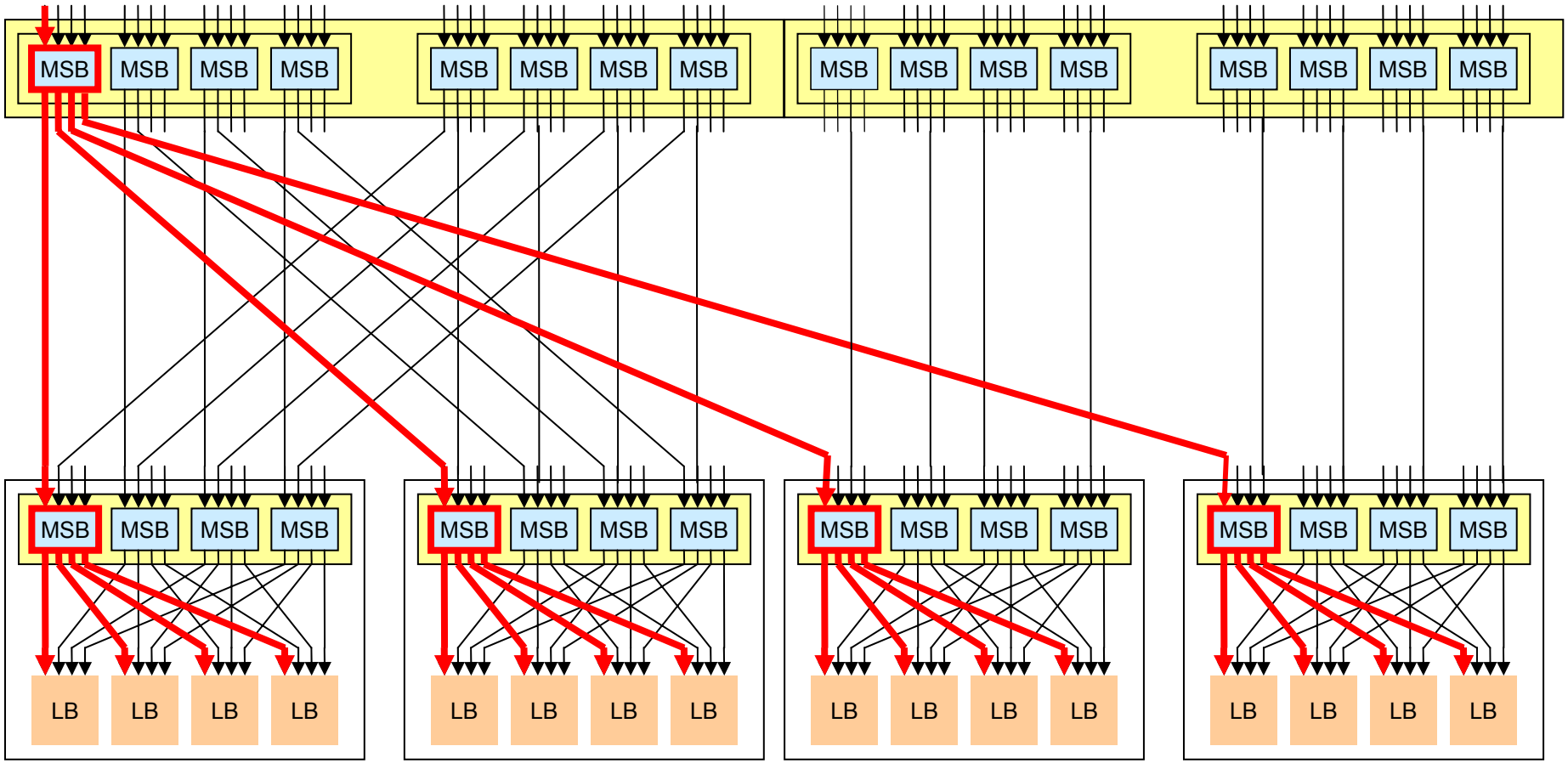
- Architecture hiérarchique multi niveaux
- Blocs logiques sont placés au niveau le plus bas de l'hiérarchie
- Fils et switches unidirectionnels
- Deux réseaux d'interconnexion:
  - Réseau d'interconnexion descendant
  - Réseau d'interconnexion montant

MFPGA: Réseau d'interconnexion descendant



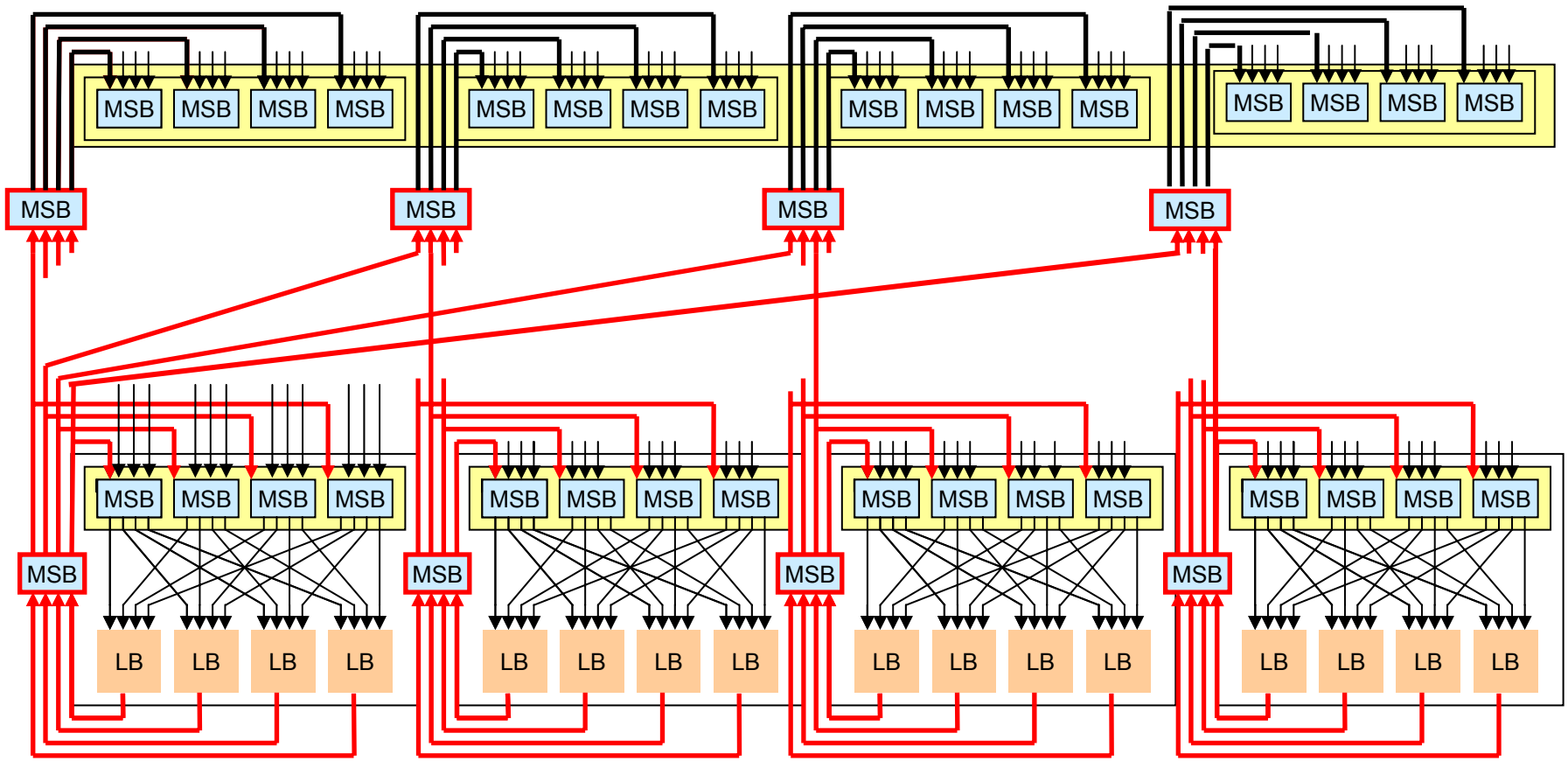
Réseau d'interconnexion descendant au niveau 0

MFPGA: Réseau d'interconnexion descendant



Réseau d'interconnexion descendant au niveau 1

MFPGA: Réseau d'interconnexion montant

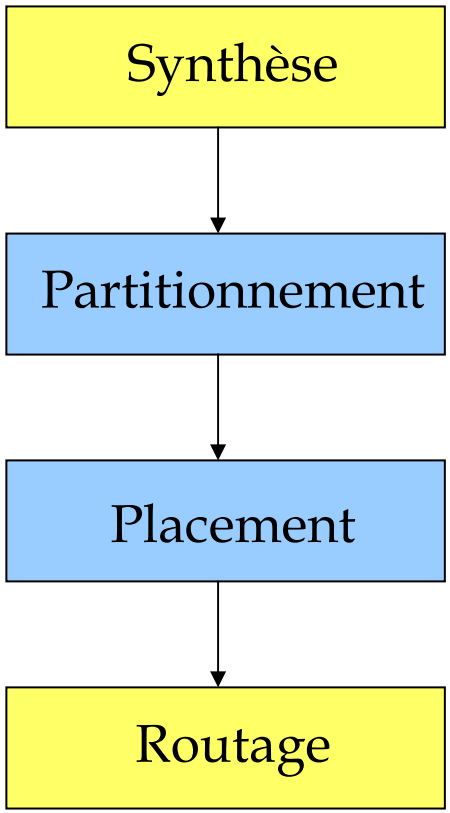


Réseaux d'interconnexion descendant et montant

PLAN

- Contexte
- Technique de contre-mesure: WDDL
- Architecture arborescente Multi niveaux MFPGA
- **Partitionnement et placement**
- Routage balance-timing-driven

Partitionnement et placement contraints



Flot de conception

- **Partitionnement:**
  - décomposer une netlist de blocs logiques en clusters de taille égale
  - objectif: minimiser les communications externes entre les clusters
  - basé sur l'approche « top down » récursive
- **Placement:** choisir des endroits spécifiques sur le FPGA pour les blocs logiques

Métrique d'évaluation de l'équilibre du circuit WDDL

- Evaluation de l'équilibre des signaux duaux :
  - calculer pour chaque deux connexions duales:

$$\Delta delay = \left| delay(true) - delay(\ false) \right|$$

  - ***delay*** : délai de l'interconnexion
    - modèle Elmore
    - technologie 130 nm

Modèle du délai

- Modèle Elmore

- Les résistances et les capacités des fils sont proportionnels à leurs longueurs

- La longueur du fil dépend de son niveau dans l'architecture, de sa direction (montant ou descendant), sa source, sa destination et de l'arité de l'architecture

- Le routeur construit l'arbre de routage et calcule les longueurs de tous les fils

- Après le routage d'un net, le routeur crée un arbre RC associé, et calcule le temps de propagation entre la source et chaque destination

Facteurs du déséquilibre dans l'architecture MFPGA

- Différence entre les longueurs des fils d'un même niveau

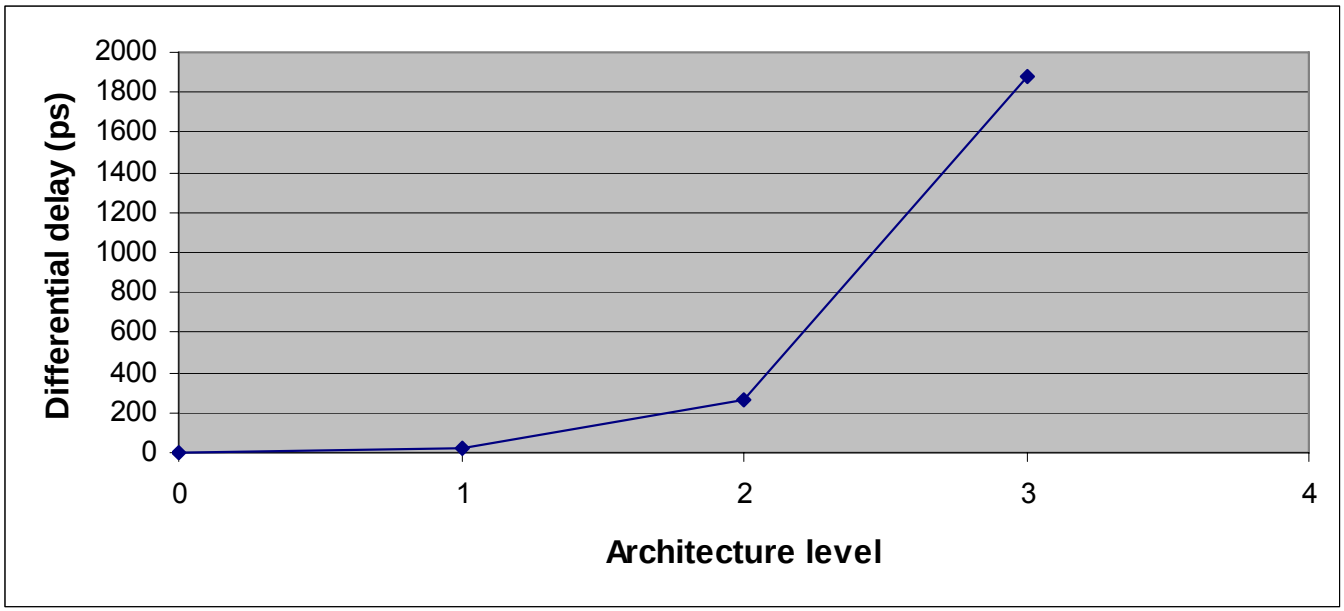


Fig.1: Différence de délais entre les feedbacks de longueur maximale et minimale en fonction du niveau de l'architecture

Facteurs du déséquilibre dans l'architecture MFPGA

- Différence du nombre de niveaux (nombre de switches) utilisés pour le routage des signaux duaux

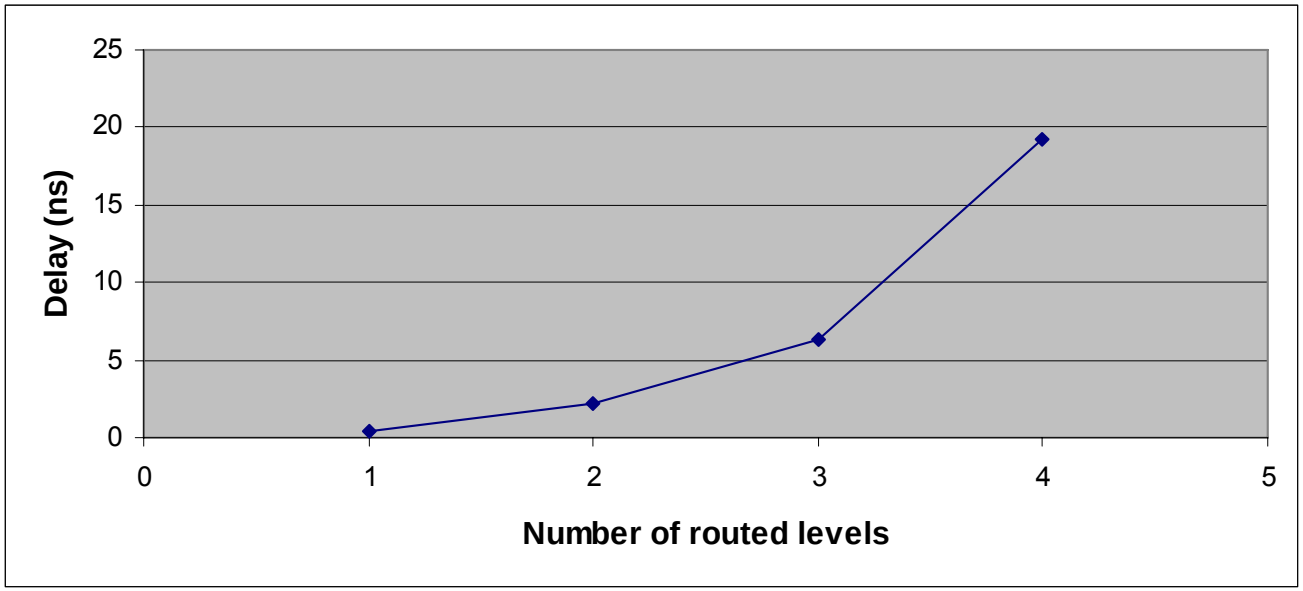
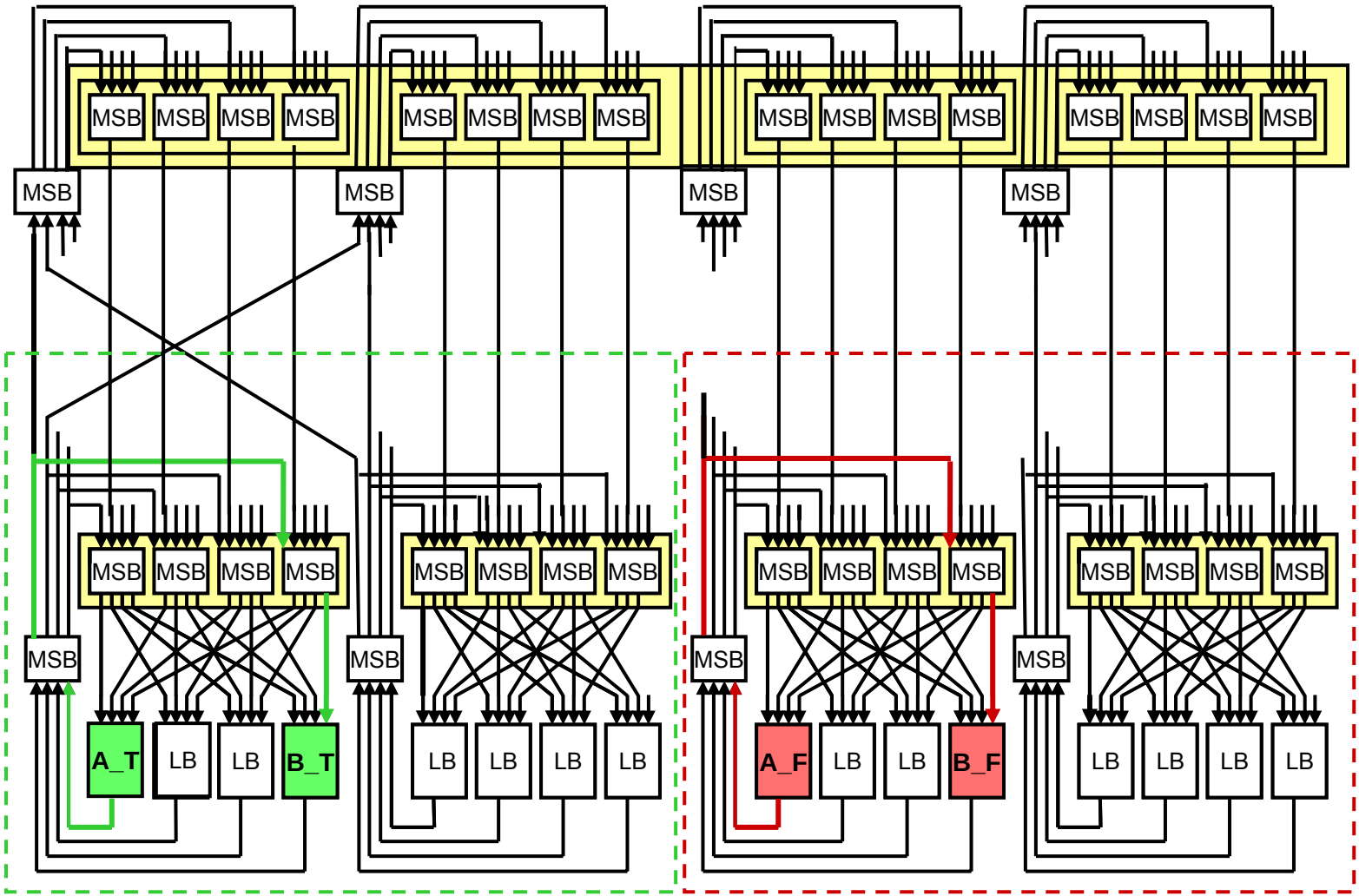


Fig. 2: Délai moyen d'un net en fonction du nombre de niveaux (nombre de switches) utilisés pour le routage

Placement Symétrique



Placement Symétrique

Résultats du placement ($\Delta delay$) (en ps) de DES- WDDL

(a) Placement sans Contraintes

Des S-Box	Max	Mean	Std Dev
# 1	8345	1595	1772
# 2	8428	1594	1873
# 3	8273	1439	1843
# 4	8147	1706	1973
# 5	8851	1584	1830
# 6	7456	1747	1571
# 7	8838	1669	1887
# 8	7321	2071	1879
Des S-Boxes	**8851**	**1671**	**1890**
DES WDDL	**9357**	**1711**	**1874**

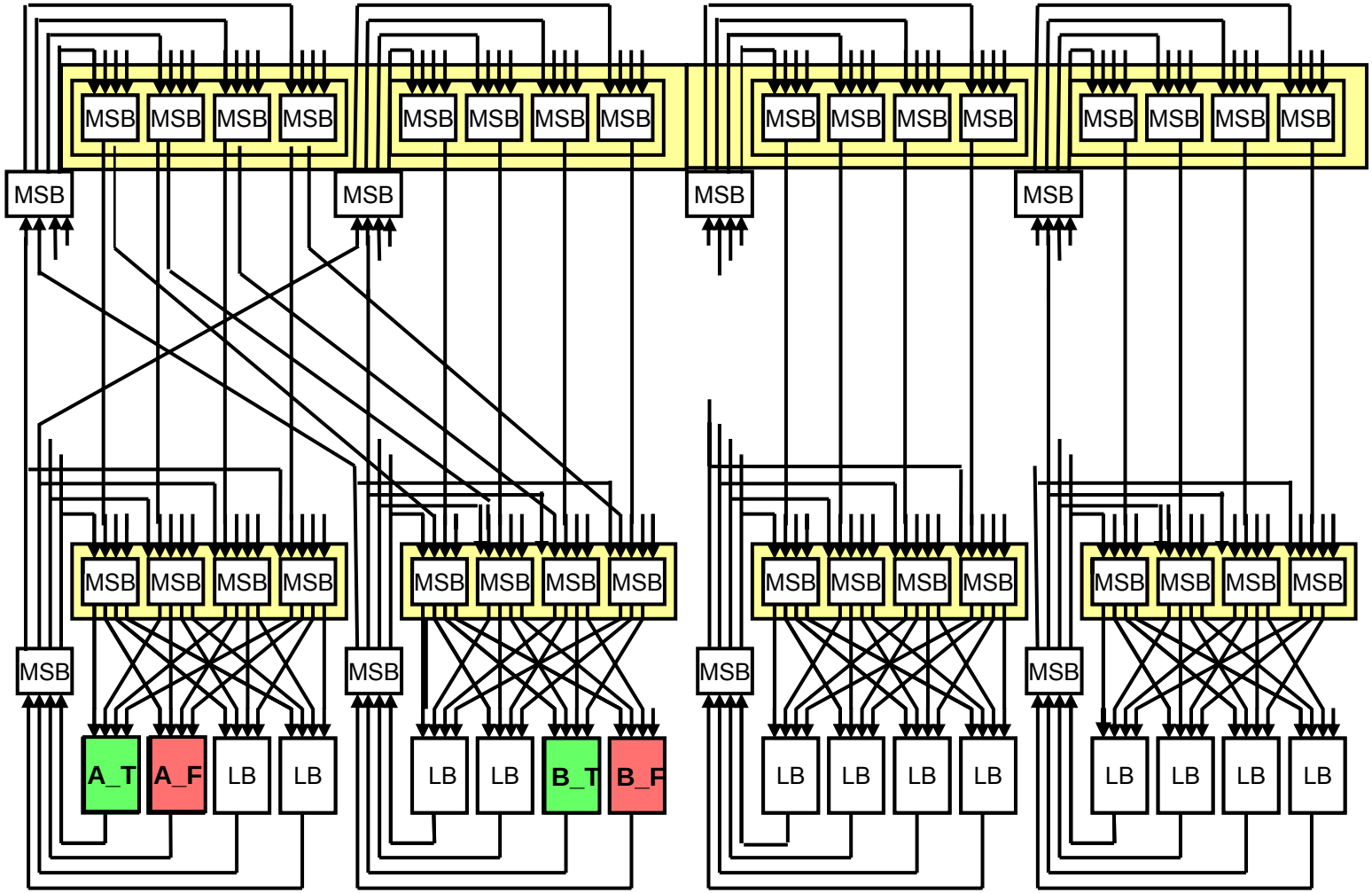
(b) Placement Symétrique

Des S-Box	Max	Mean	Std Dev
# 1	4832	1160	915
# 2	3040	890	742
# 3	3671	1172	1051
# 4	6854	1178	859
# 5	6421	1025	1021
# 6	3470	915	772
# 7	5994	888	887
# 8	4923	1209	1072
Des S-Boxes	**6854**	**1054**	**941**
DES WDDL	**8039**	**1133**	**987**

Gain :

- Délai moyen du DES WDDL réduit de 33 %
- Nombre de connexions déséquilibrés en termes de nombre de switches réduit de 1948 à 210

Placement Adjacent



Placement Adjacent

Résultats du placement ($\Delta delay$) (en ps) de DES- WDDL

(a) Placement sans Contraintes

Des S-Box	Max	Mean	Std Dev
# 1	8345	1595	1772
# 2	8428	1594	1873
# 3	8273	1439	1843
# 4	8147	1706	1973
# 5	8851	1584	1830
# 6	7456	1747	1571
# 7	8838	1669	1887
# 8	7321	2071	1879
Des S-Boxes	**8851**	**1671**	**1890**
WDDL design	**9357**	**1711**	**1874**

(b) Placement Adjacent

Des S-Box	Max	Mean	Std Dev
# 1	4017	626	772
# 2	3951	449	598
# 3	5205	607	776
# 4	3440	417	480
# 5	4777	480	532
# 6	3027	532	514
# 7	3893	591	632
# 8	3530	435	469
Des S-Boxes	**5205**	**517**	**620**
WDDL design	**7137**	**479**	**587**

Gain :

- Délai moyen du DES WDDL réduit de 72 %
- Nombre de connexions déséquilibrés en termes de nombre de switches réduit de 1948 à 146

PLAN

- Contexte
- Technique de contre-mesure: WDDL
- Architecture arborescente Multi niveaux MFPGA
- Partitionnement et placement contraints
- **Routage balance-timing-driven**

Routage timing-balance-driven

- Routage ***Pathfinder***
  - ***Objectif :*** router les signaux avec le chemin le plus court (le minimum de ressources de routage)
  - ***Principe :***
    - Algorithme itératif
    - Fonction de coût = coût de congestion de la ressource

- Routage ***timing_balance-driven***

Routage timing-balance-driven

- Routage ***Pathfinder***
  - ***Objectif :*** router les signaux avec le chemin le plus court (le minimum de ressources de routage)
  - ***Principe :***
    - Algorithme itératif
    - Fonction de coût = coût de congestion de la ressource

- Routage ***timing_balance-driven***
  - ***Objectif*** **:** router les signaux en équilibrant les temps de propagation de deux signaux duaux

Routage timing-balance-driven

- Routage ***timing_balance-driven***
  - ***Principe :***
    - Basé sur l'algorithme itératif Pathfinder
    - Nouvelle *fonction de coût* tient en compte de :
      - la *congestion* des ressources
      - la *différence de délai* entre les connexions duales
      - la *différence en nombre de switches* entre les connexions duales
    - Donner la priorité aux connexions les plus critiques (***Δdelay*** important)

Routage timing-balance-driven

Résultats du routage (en ps) de DES- WDDL avec placement adjacent

(a) Routage Pathfinder

	Max	Mean	Std Dev
Des S-Boxes	**5205**	**517**	**620**
DES WDDL	**7137**	**479**	**587**

(b) Routage timing-balance-driven

	Max	Mean	Std Dev
Des S-Boxes	1505	193	226
DES WDDL	**1505**	**160**	184

Gain :

- 64 % de délai moyen du DES WDDL (vs. placement adjacent et routage Pahfinder)
- 90 % de délai moyen du DES WDDL (vs. Placement sans contraintes et routage Pathfinder)
- Nombre de connexions déséquilibrés en termes de nombre de switches réduit à 2

Conclusion & Perspectives

- Placement adjacent
- Routage timing-balance-driven

→ ***Gain (DES WDDL) :***

- $\Delta delay$ moyen réduit de 90 % (1711 ps à 160 ps)
- Nb. de connexions déséquilibrés en termes de nombre de switches réduit de 1947 à 2

Conclusion & Perspectives

- Placement adjacent
- Routage timing-balance-driven

→ ***Gain (DES WDDL) :***

- $\Delta delay$ moyen réduit de 90 % (1711 ps à 160 ps)
- Nb. de connexions déséquilibrés en termes de nombre de switches réduit de 1947 à 2

- Perspectives :
  - Améliorer les outils de placement et de routage
  - Equilibrer la consommation de courant entre les signaux duaux
  - Appliquer les méthodes proposées sur un circuit réel (en cours de conception)

Merci pour votre attention

Communauté et Conférences

- *Equipe Française*: SEN de ENST
- *Equipes Internationales*: Jonathan Rose (Université de Toronto), Kris Tiri (Intel, Oregon), Patrick Schaumont (Virginia Tech), EmSec (Ingrid Verbauwhede, UCLA)

Communauté et Conférences

- *Equipe Française*: SEN de ENST
- *Equipes Internationales*: Jonathan Rose (Université de Toronto), Kris Tiri (Intel, Oregon), Patrick Schaumont (Virginia Tech), EmSec (Ingrid Verbauwhede, UCLA)

- Conférences :
  - ReConFig (International Conference on Reconfigurable Computing and FPGAs)
  - FPT (International Conference on Field-Programmable Technology)
  - ICECS (IEEE International Conference on Electronic Circuits and Systems)
  - ICM (International Conference on Microelectronics)
  - HOST (IEEE International Workshop on Hardware-Oriented Security and Trust)
  - CHES (Workshop on Cryptographic Hardware and Embedded Systems)