Taha Beyrouthy
Laurent Fesquet

Laboratoire TIMA
Groupe CIS
Grenoble

SÉCURITÉ DES FPGAS ASYNCHRONES

Journée Sécurité GDR SOC-SIP 2010

Taha.beyrouthy@imag.fr

Plan

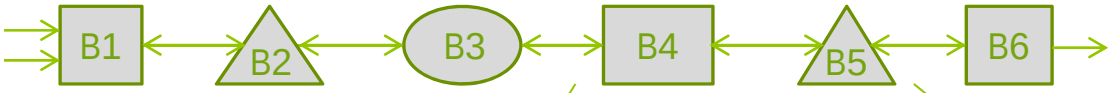
La logique asynchrone

1 - Principe de la logique asynchrone

2 - Logique asynchrone pour la sécurité

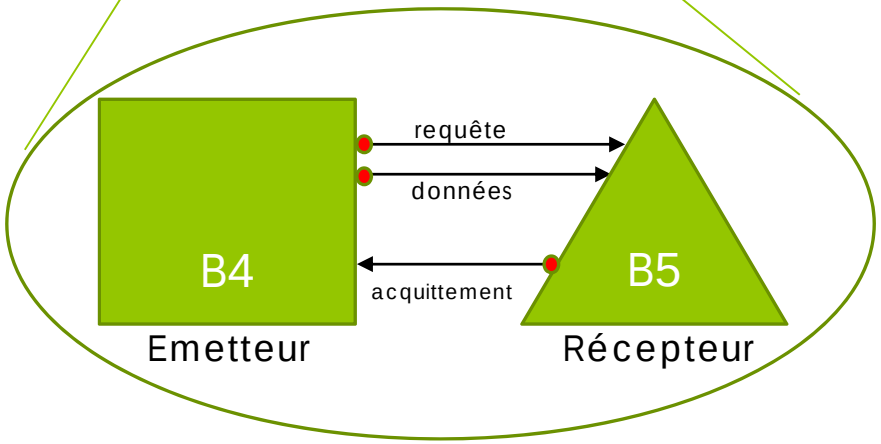
1 - Principe

Principe de synchronisation des circuits asynchrones.



Synchronisation entre les blocs d'un circuit asynchrone

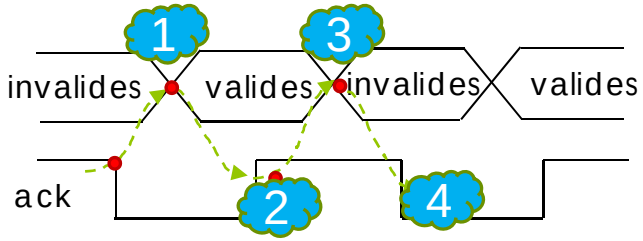
- Protocole de communication : *poignée de main*
- Pas de signal global de synchronisation (horloge)
- Une multitude de signaux locaux de synchronisation Ack/Req

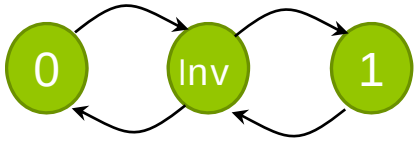


1 - Principe

Types de protocoles de communication :

Protocole 4-phase





Transitions des données sur 3-états

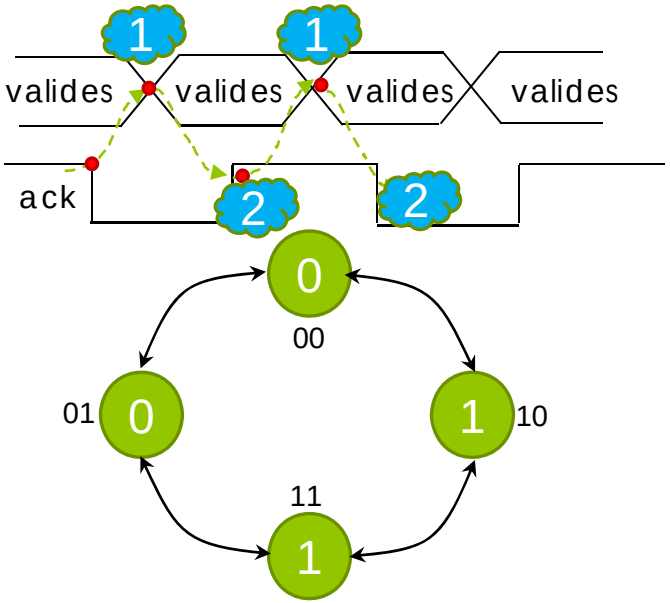
Codage 1-parmi-2		
	w1	w0
Invalide « E »	0	0
Valide « 0 »	0	1
Valide « 1 »	1	0
Non utilisée	1	1

Codage des données 1-parmi-N
Ici N = 2

1 - Principe

Types de protocoles de communication :

Protocole 2-phase



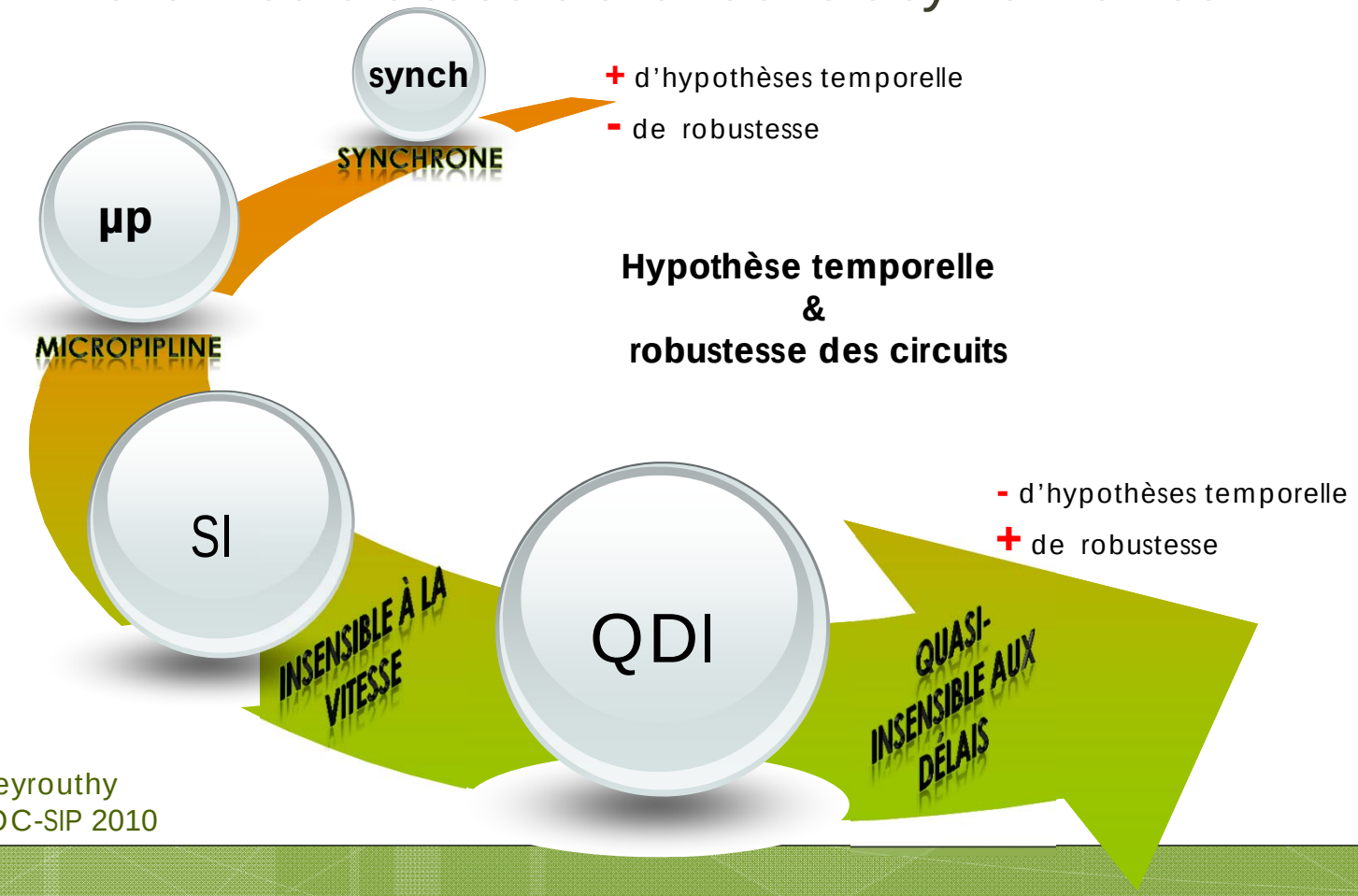
Transitions des données sur 4-états

Codage de Grey		
	w1	w0
Valide « 0 »	0	0
Valide« 1 »	0	1
Valide « 0 »	1	0
Valide« 1 »	1	1

Codage des données : Grey

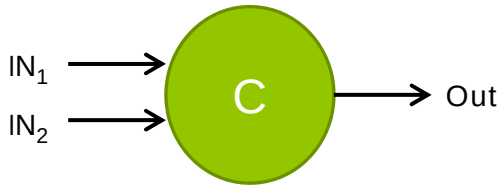
1 - Principe

Différentes classes de circuits asynchrones



1 - Principe

Porte élémentaire de Muller (C-Element)



Porte Muller ou C-Element

C-Element		
Out	IN_1	IN_2
0	0	0
Out^{-1}	0	1
Out^{-1}	1	0
1	1	1

Table de vérité de la porte Muller

2 - Asynchrone pour la sécurité

Avantage de la logique asynchrone vis-à-vis de la sécurité *[Bouesse 06], [Soares 08]* :

- Le codage des données de type 1-parmi-n
- Le protocole de communication
- Basse consommation distribuée
- Le contrôle local
- Difficile à synchroniser
- TA difficile à réaliser

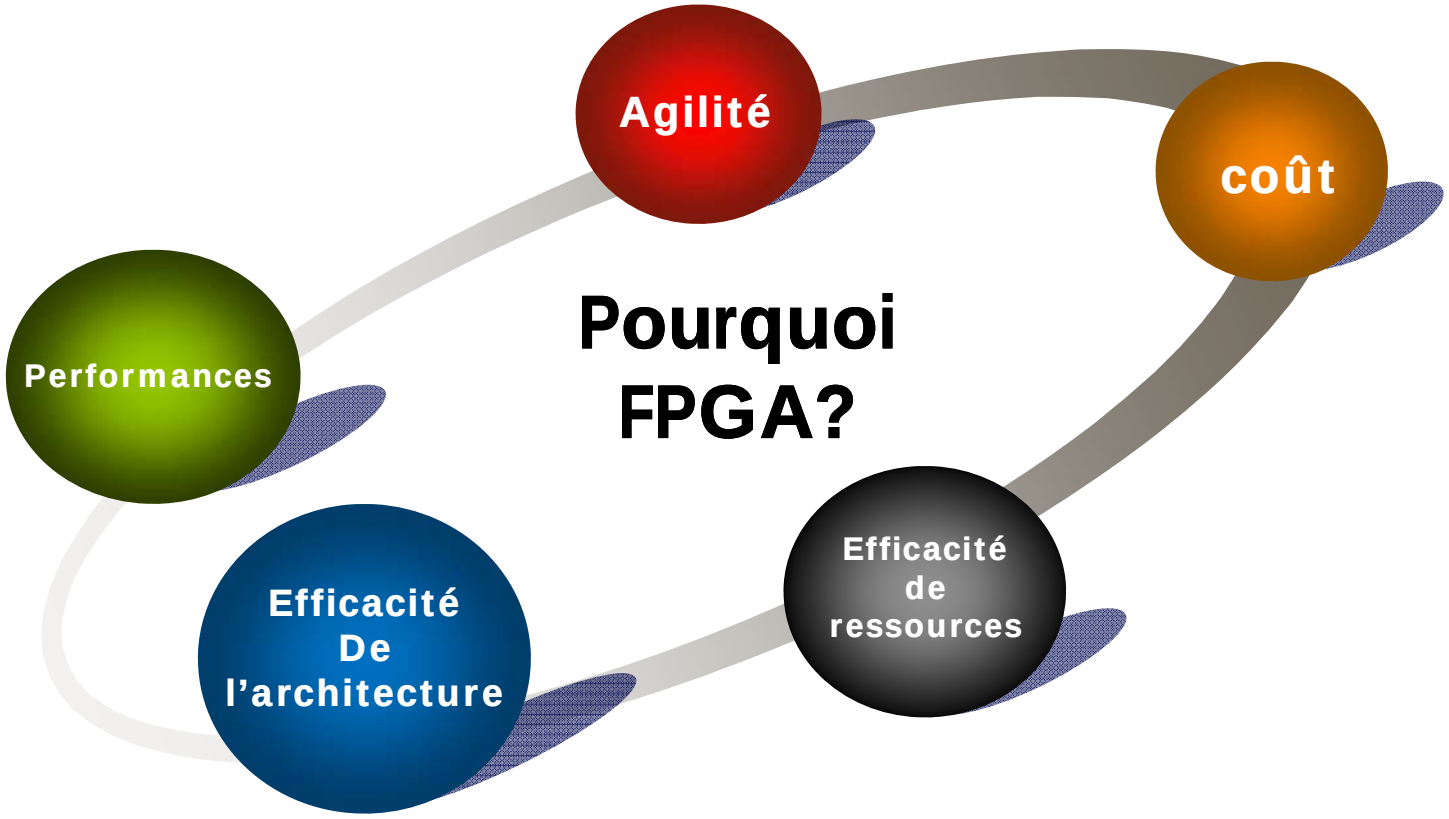
Les circuits programmables

1 - Avantages vis-à-vis de la cryptographie

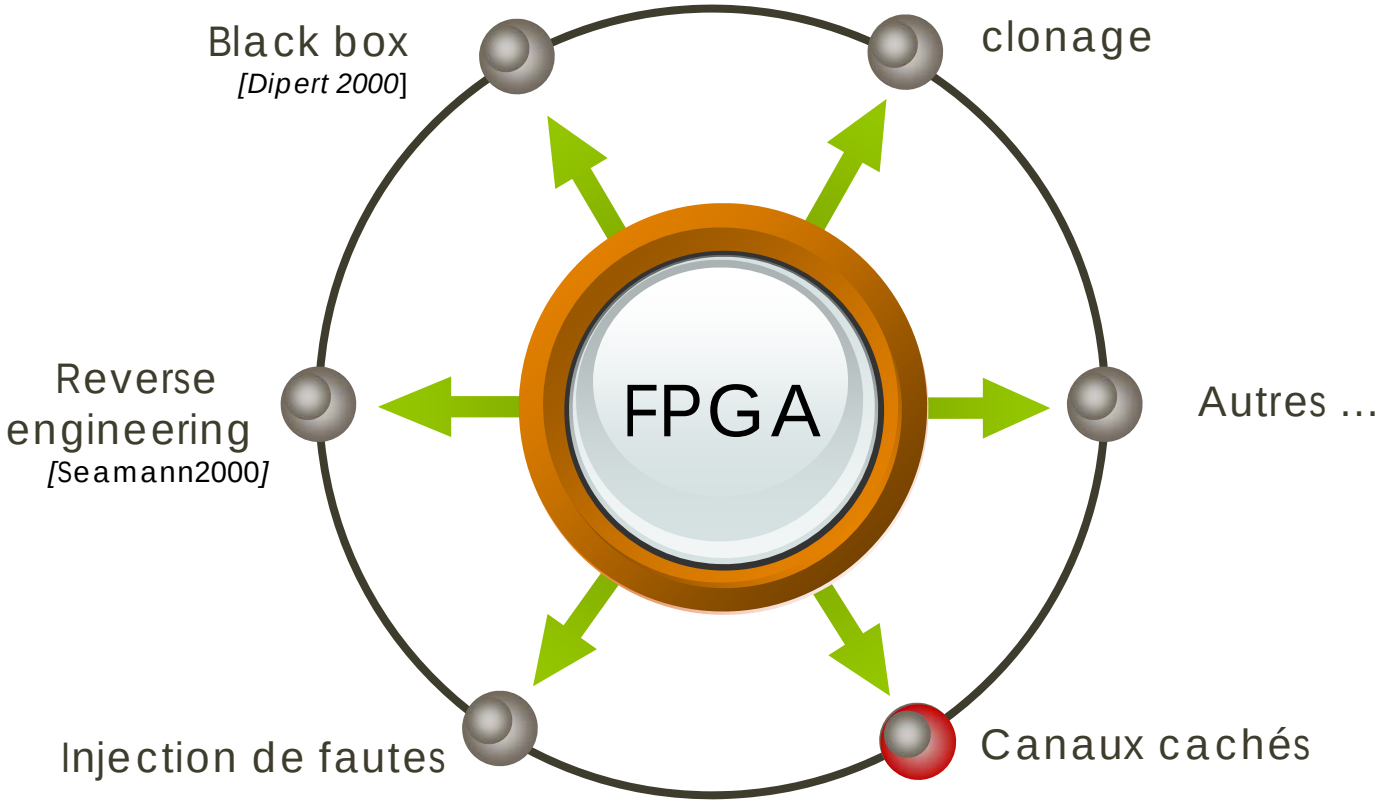
2 - Défauts vis-à-vis de la sécurité

3 - Contremesures existantes

1- Avantages vis-à-vis de la cryptographie



2 - Défauts vis-à-vis de la sécurité



2 - Défauts vis-à-vis de la sécurité

Les attaques par canaux cachés

Canaux cachés		Attaques
Le courant	→	DPA, SPA ..
L'émission électro-magnétique	→	EMA
Le temps	→	TA
Température, etc..	→	...

2 - Défauts vis-à-vis de la sécurité

Les attaques par canaux cachés

1

Faible coût de réalisation

2

Facilité de mise en œuvre

3

Performants et efficaces

- **Consommation :**
  12x > ASIC
  [Gracia 2000]

- **Surface :**
  35x > ASIC
  [Kuon 2006]

3 - Certaines contremesures

Plusieurs contremesures ont été proposés :

- DPA/EMA
  - Consommation aléatoire : *Masking*
  - Consommation indépendante des données : WDDL, WDDL+, STTL , BCDL, etc…
- FA
  - Redondance
  - Détection de faute

Conclusion

Les FPGAs synchrones actuels:

- Pas protégés contre les attaques par canaux cachés : DPA , EMA …
- Placement et routage pas toujours maîtrisable
- La chaine de programmation n'est pas bien protégée
- Non prévus pour supporter des styles de circuits logiques alternatifs tels que les circuits asynchrones.

Conclusion

Les FPGAs asynchrones actuels:

- Les FPGAs asynchrones connus:
  - GALSA, PAPA, PGA-STC, PAP, MONTAGE,
  - STACC , Speedster …
- Problèmes:
  - Dédiés à un seul style de logique asynchrone.
  - Non protégés contre les attaques pas canaux cachés.

FPGA asynchrone sécurisé

1 – Critères de sécurité d'un FPGA asynchrone

2 - Architecture du FPGA asynchrone : S.A.F.E.

3 - Synthèse des circuits sur S.A.F.E.

4 - Test et validation

1 – Critères de sécurité d'un FPGA asynchrone

La sécurisation du FPGA contre les attaques par canaux cachés (notamment: DPA, SPA, EMA, TA) se fait aux niveaux :

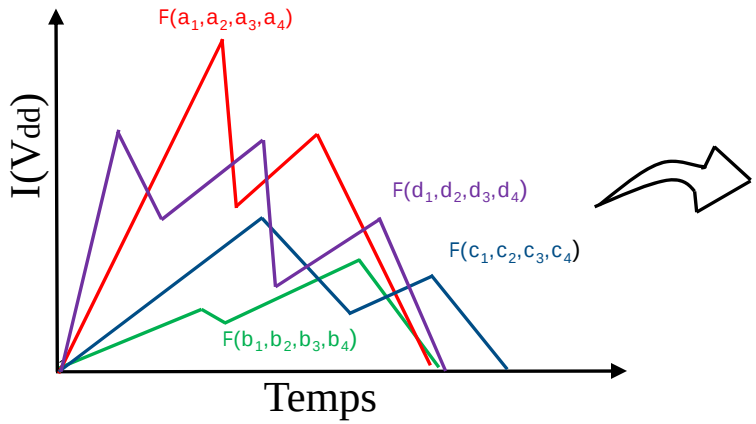
- Intrinsèque : architecture
  - Bloc programmable
  - Réseau d'interconnexion
  - Mémoire de programmation
- Extrinsèque : programmation
  - Synthèse
  - P/R

1 – Spécifications du FPGA asynchrone sécurisé : S.A.F.E.

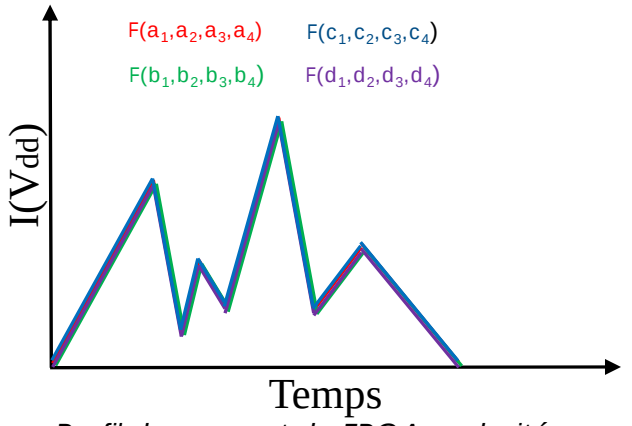
Objectif pour la sécurité :

Contre une attaque par analyse de courant:

- Consommation indépendante des données
- Temps de calcul indépendant des données



Profil du courant du FPGA non sécurisé



Profil du courant du FPGA souhaité

1 – Spécifications du FPGA asynchrone sécurisé : S.A.F.E.

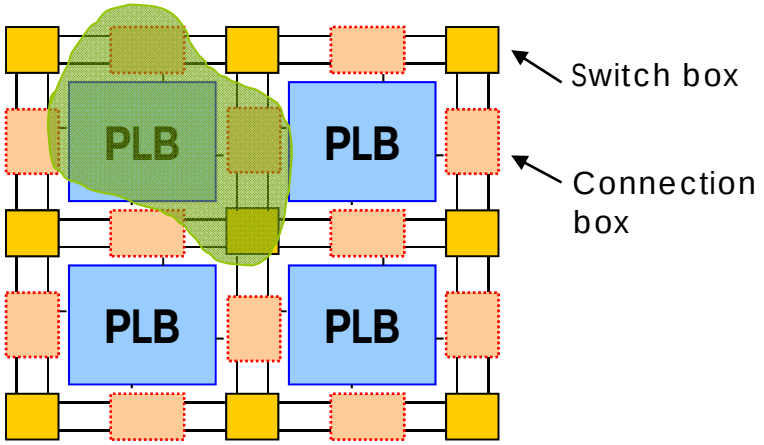
Objectif de programmabilité:

- Supporter plusieurs styles de logiques asynchrones
  - 4-phases
  - 2-phases
- Supporter plusieurs types de codage de données
  - 1-parmi-n : dual-rail, triple-rail, etc. → poids de Hamming constant.
  - Codage de Grey

2 – Architecture du FPGA asynchrone sécurisé : S.A.F.E.

Architecture du FPGA de type « Island », conçue pour être :

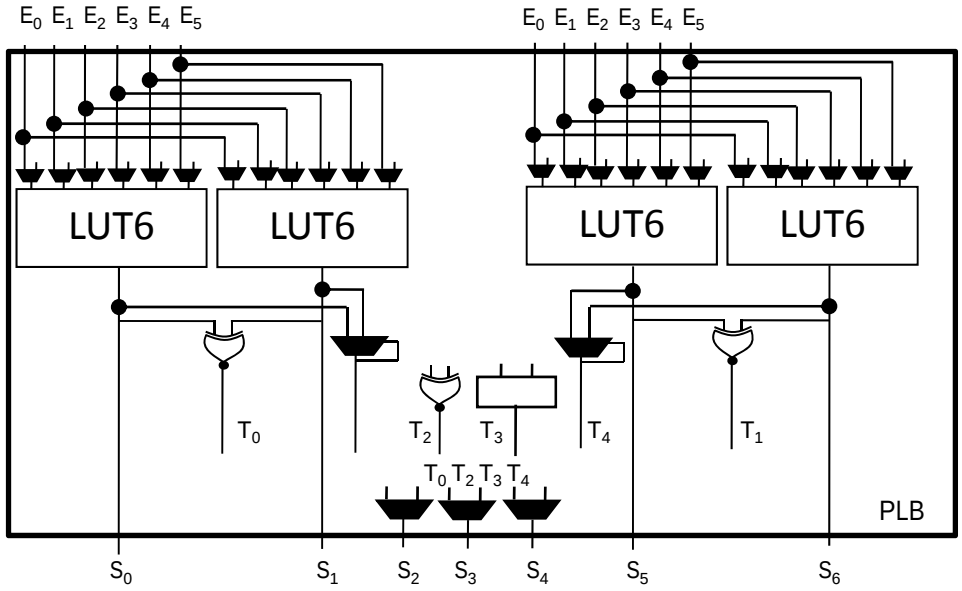
- Equilibrée au niveau électrique (capacité d'entrée)
- Equilibrée au niveau logique (profondeur logique)



Architecture globale du FPGA Asynchrone

2 – Architecture du FPGA asynchrone sécurisé : S.A.F.E.

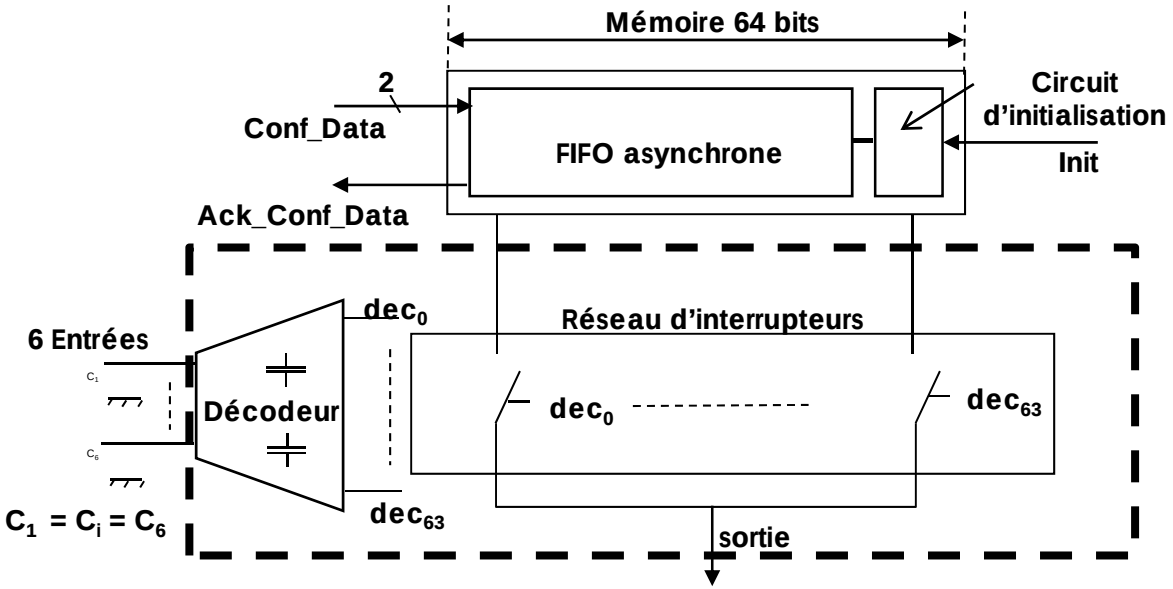
Programmable Logic Bloc (PLB)



Architecture du PLB

2 – Architecture du FPGA asynchrone sécurisé : S.A.F.E.

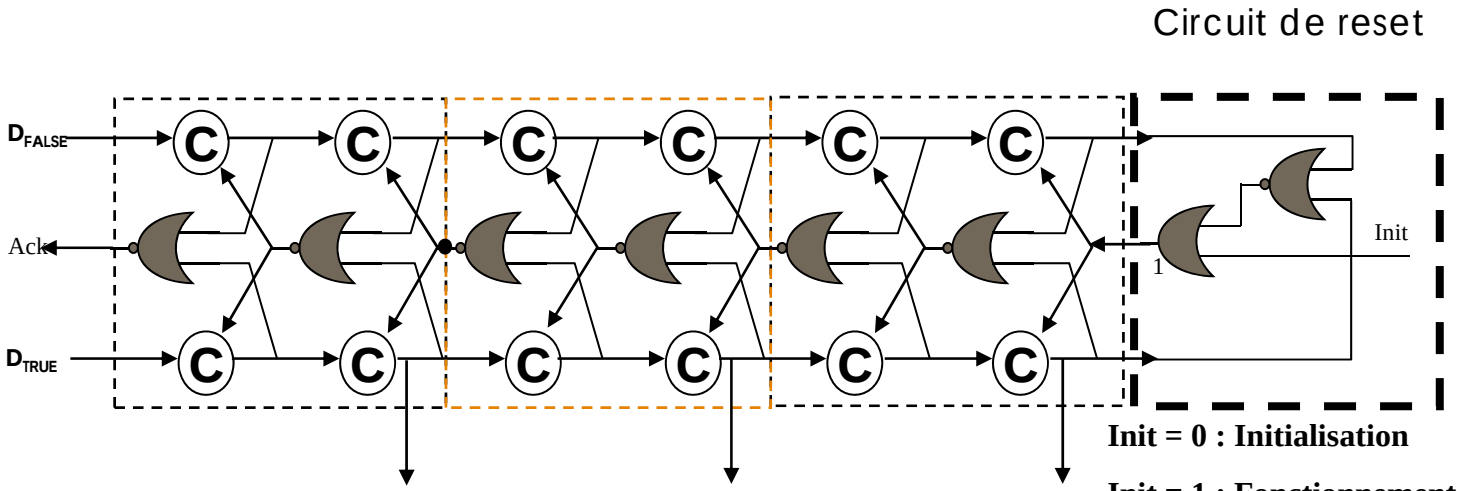
Look Up Table (LUT6)



Architecture de la LUT6

2 – Architecture du FPGA asynchrone sécurisé : S.A.F.E.

Look Up Table (LUT6) – Fifo asynchrone



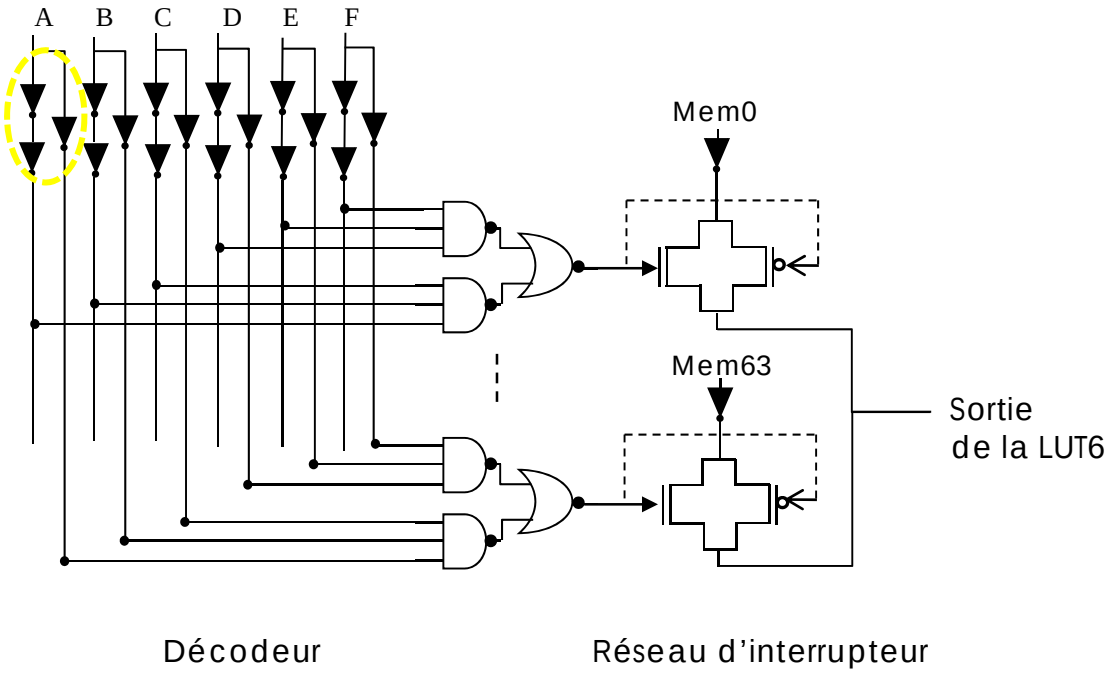
Architecture de la FIFO

Init = 0 : Initialisation

Init = 1 : Fonctionnement normal

2 – Architecture du FPGA asynchrone sécurisé : S.A.F.E.

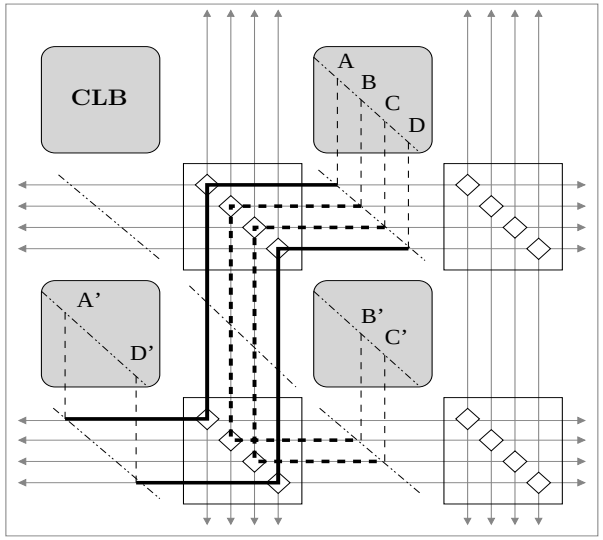
Look Up Table (LUT6) - Décodeur



2 – Architecture du FPGA asynchrone sécurisé : S.A.F.E.

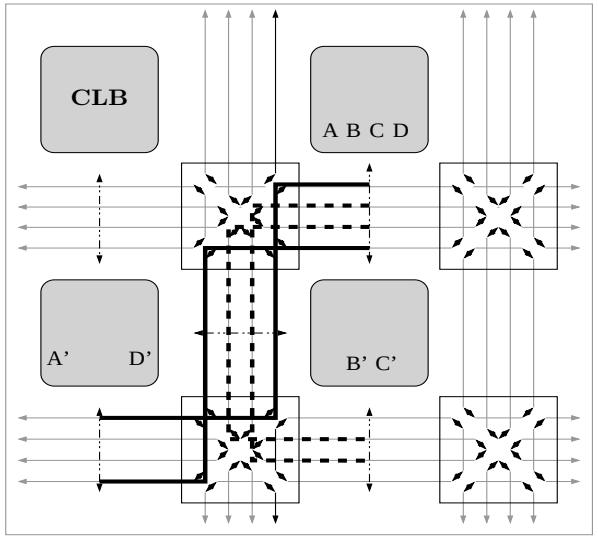
Interconnexion – Telecom Paristech

« Subset » switch Matrix



Elmore's model: identical shape and length

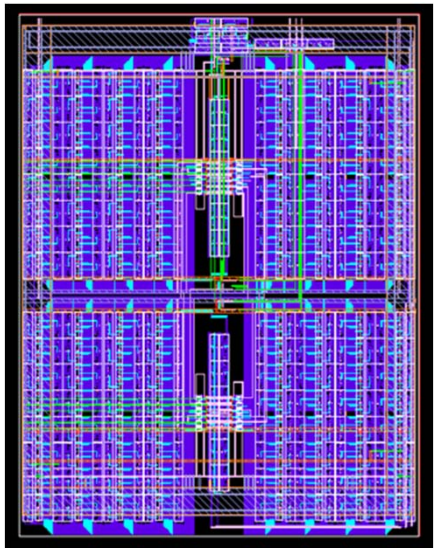
« Twisted pair » switch Matrix

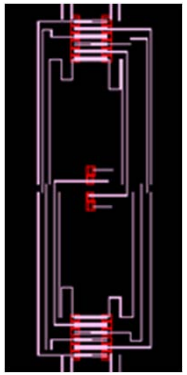


Crosstalk protection: twisted pairs

2 – Architecture du FPGA asynchrone sécurisé : S.A.F.E.

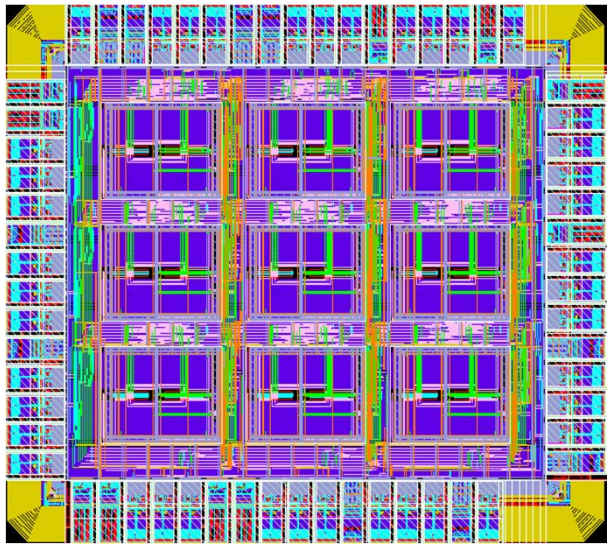
Layout du PLB équilibré - Full custom



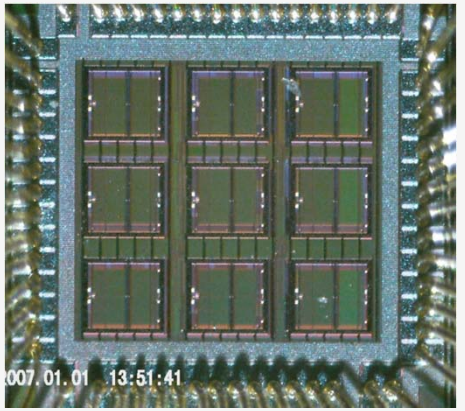


- Full custom layout
- Dimensionnement basé sur la méthode *'logical effort'* [Sutherland99]

Architecture du PLB : Niveaux de métaux équilibrés



Layout du FPGA asynchrone



Die-view du FPGA asynchrone

Caractéristiques:

- 9 PLBs.
- Technologie CMOS 65 nm de ST Microelectronics.
- 36 Entrées/Sorties
- Surface : 1111.6 x 947.6 µm² et contient environ 200,000 transistors.

3 – Synthèse des circuits sur le FPGA asynchrone : S.A.F.E.

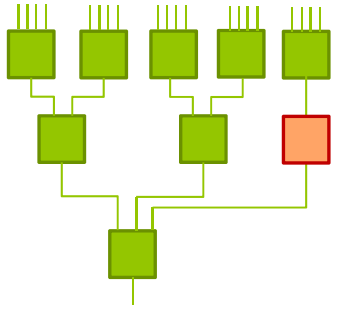
Un algorithme spécifique de synthèse à été développé pour :

- Générer une architecture symétrique et équilibré du circuit à implémenter
- Utiliser le minimum de ressources programmables du FPGA

3 – Synthèse des circuits sur le FPGA asynchrone : S.A.F.E.

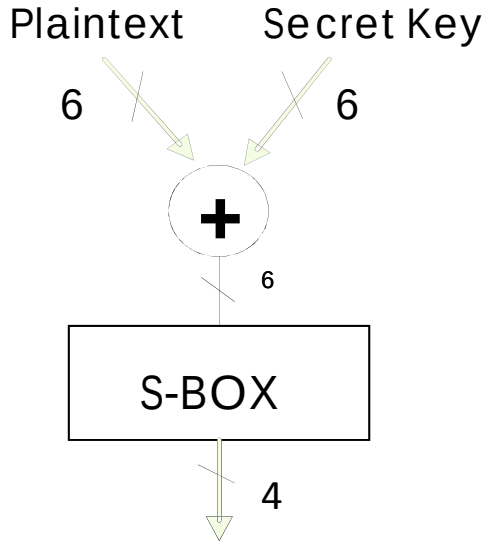
Un algorithme spécifique de synthèse à été développé pour :

- Synthèse de la fonction
- Équilibrer la profondeur logique



4 – Test et Validation

Implémentation d'une S-BOX + XOR, en 2-phase et 4-phase



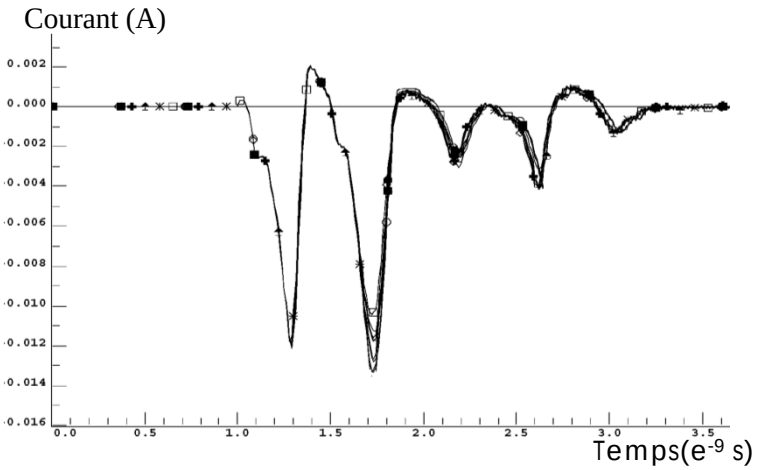
Module du DES sensible aux SCAs

	implémentation 2-phase	Implémentation 4-phase
Nb of LUT6 SBOX + XOR	31	31
Nb of LUT6s pour équilibrer	8	8

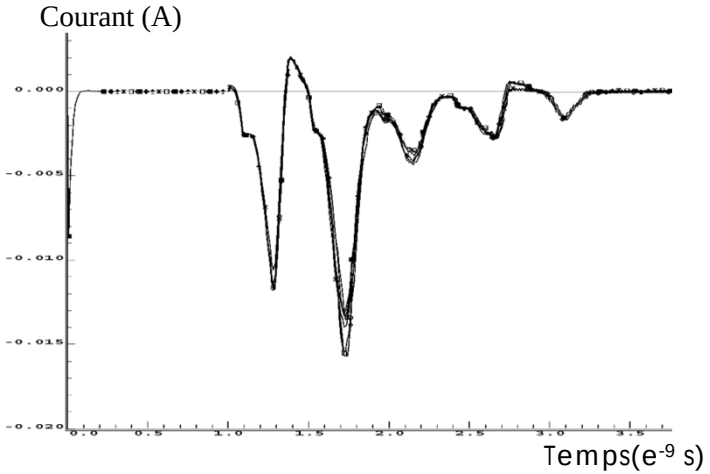
4 – Test et Validation

Simulation du circuit post-Layout

- Consommation indépendante des données



Profil de courant du bloc en ***4 phases*** *– double rails*

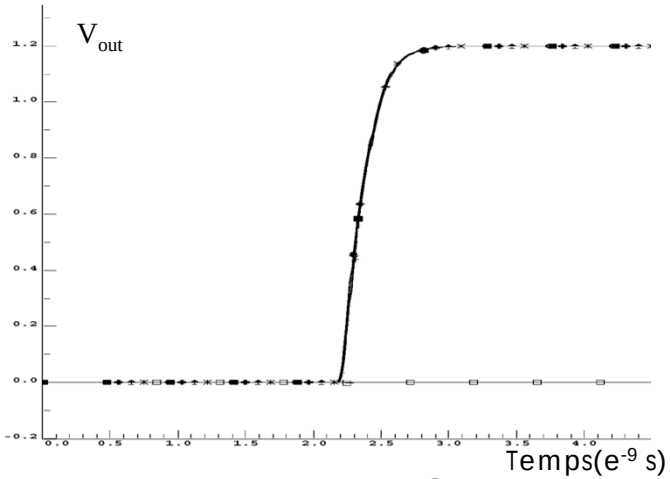


Profil de courant du bloc en ***2 phases*** *– double rails*

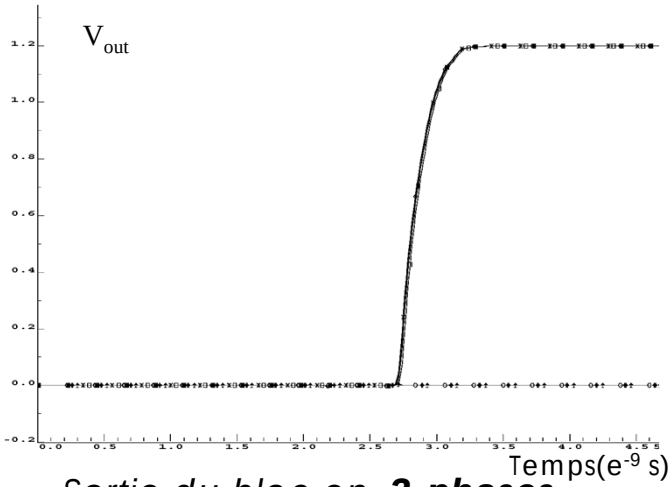
4 – Test et Validation

Simulation du circuit post-Layout

- Temps de calcul et de propagation indépendants des données



*Sortie du bloc en **4-phases** double rails*



*Sortie du bloc en **2-phases** double rails*

Conclusion et Perspectives

1 - Conclusion

2 - Perspectives

1 – Conclusion

- La Logique asynchrone est très bien adaptés pour des applications de sécurité
  - Contre-mesures logiques
  - Contre-mesures électriques
  - Contre-mesures contre les FA
- L'implémentation de la logique asynchrone sur des FPGAs synchrones est toujours possible mais …
  - Bibliothèques de cellules spécifiques
  - Non adapté pour la sécurité
- Les FPGAs asynchrones actuels sont dédiés pour un style de logique spécifique et ne sont pas protégés contres les SCAs.

1 – Conclusion

- La sécurisation des FPGAs asynchrones nécessite plusieurs niveaux de protection:
  - Protection intrinsèque
  - Protection extrinsèque

- Finalement :
  - Les contre-mesures contre les SCAs sont implémentables dans des FPGAS sécurisés