CASSIDIAN
CYBERSECURITY

Construction d'un banc d'expérimentation pour les Hardware Trojans - GdR SoC-SiP

Julien FRANCQ, Florian FRICK

27/11/2012

Introduction aux Hardware Trojans et à HOMERE

Construction d'un banc d'expérimentations
- Nos objectifs
- Utilisation de SASEBO
- Comment déclencher un HT ?
- Analyse par canaux auxiliaires
- Scenarii de tests

Présentation d'un cas d'étude : contrôle d'accès
- Présentation
- Injecter/tester un HT combinatoire
- Autres Hardware Trojans

Conclusion et perspectives

Introduction aux Hardware Trojans et à HOMERE

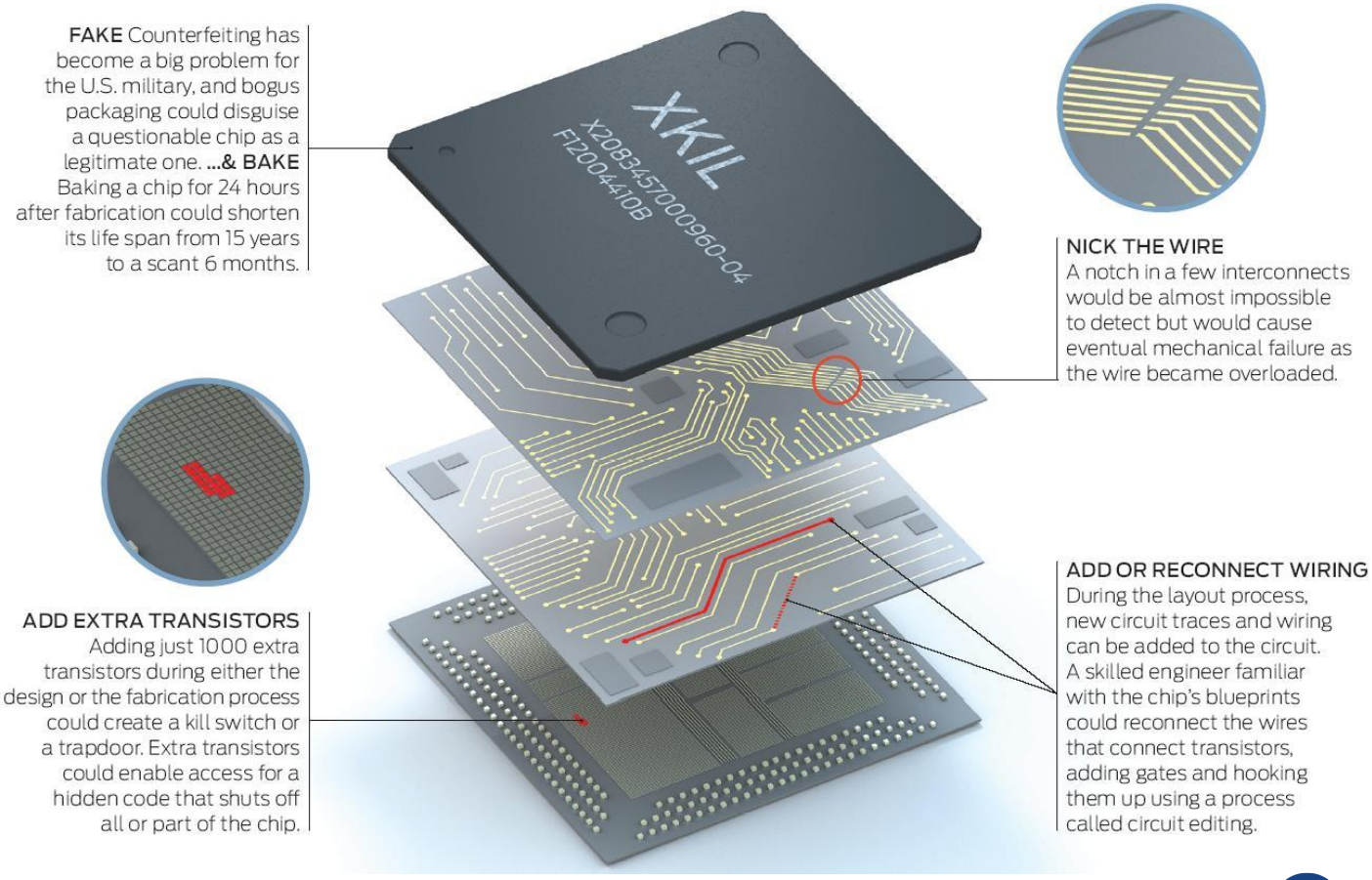
Construction d'un banc d'expérimentations
- Nos objectifs
- Utilisation de SASEBO
- Comment déclencher un HT ?
- Analyse par canaux auxiliaires
- Scenarii de tests

Présentation d'un cas d'étude : contrôle d'accès
- Présentation
- Injecter/tester un HT combinatoire
- Autres Hardware Trojans

Conclusion et perspectives

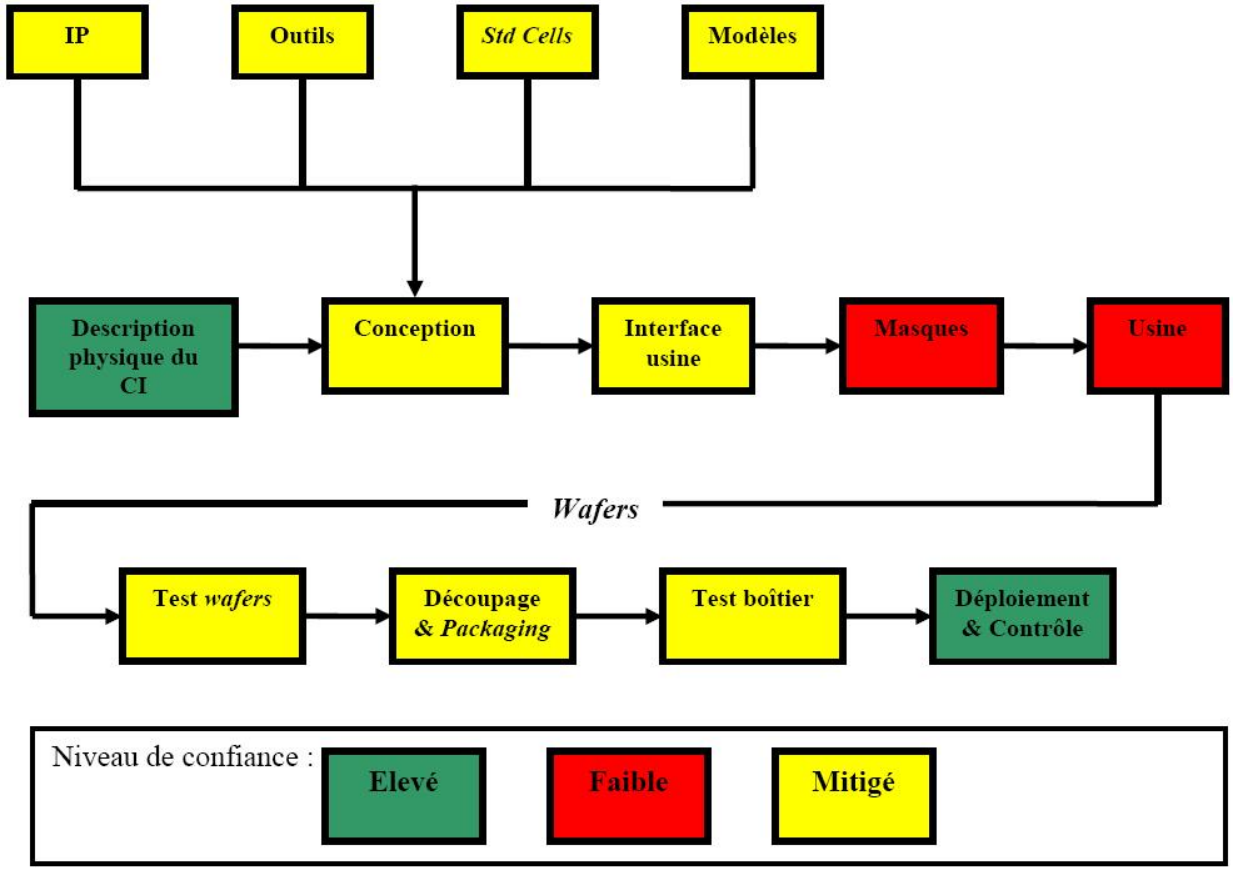
Hardware Trojan (HT)

- Modification frauduleuse d'un circuit intégré à n'importe quelle étape de sa fabrication



Contexte

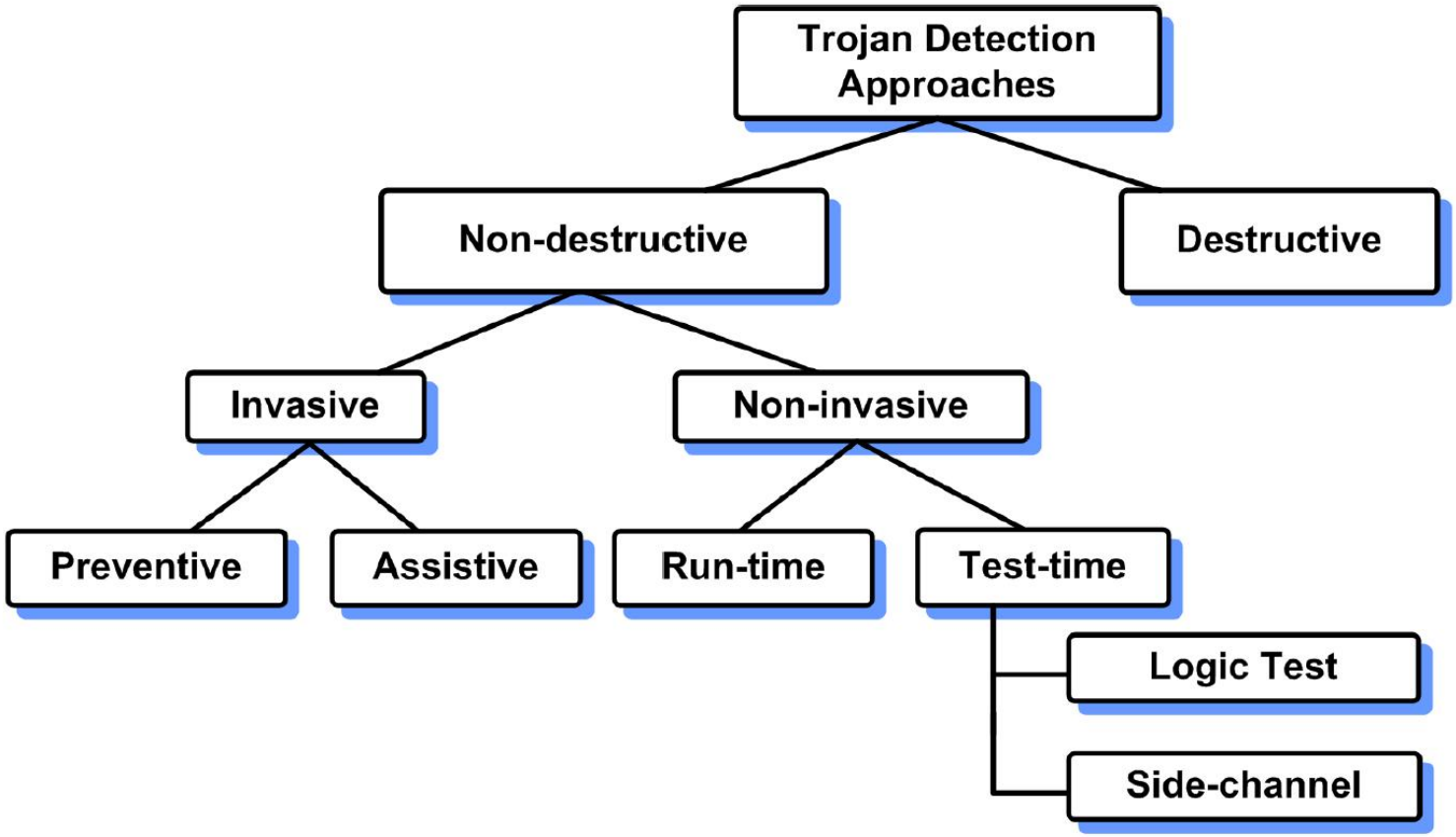
- Délocalisation de la fabrication des circuits intégrés
- Difficile d'assurer la confiance



Les partenaires du projet HOMERE

- FUI14 (2012-2015) : projet HOMERE (Hardware trOjans : Menaces et robustEsse des ciRcuits intEgrés)
- Grands groupes
  - Cassidian CyberSecurity, Gemalto
- PME
  - Secure-IC
- Académiques
  - ARMINES, CEA-LETI, LIRMM, Télécom ParisTech
- Gouvernemental
  - ANSSI, (DGA)

Méthodes de détection dans HOMERE



- Aucune méthode n'est pleinement satisfaisante aujourd'hui

Introduction aux Hardware Trojans et à HOMERE

Construction d'un banc d'expérimentations
- Nos objectifs
- Utilisation de SASEBO
- Comment déclencher un HT ?
- Analyse par canaux auxiliaires
- Scenarii de tests

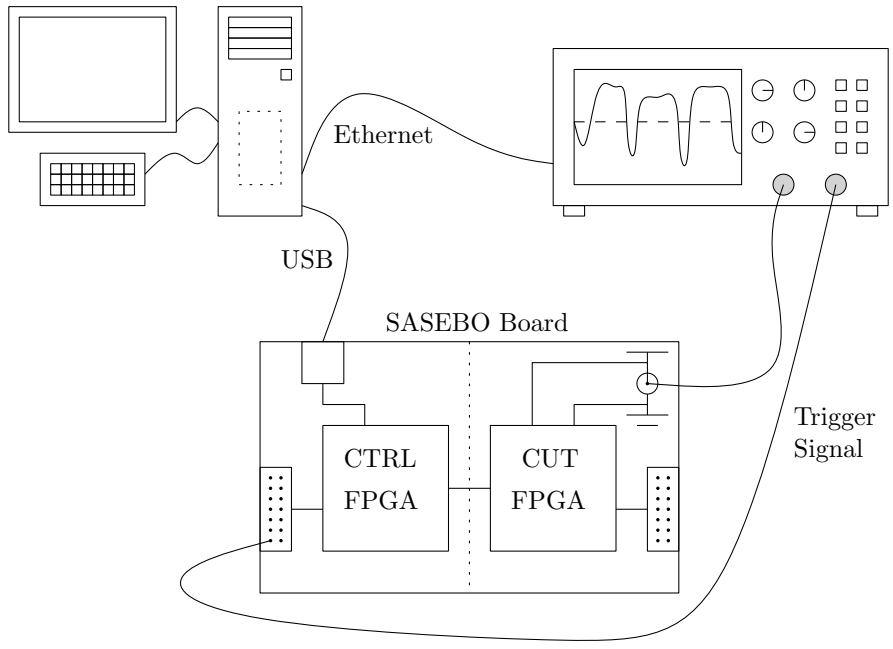
Présentation d'un cas d'étude : contrôle d'accès
- Présentation
- Injecter/tester un HT combinatoire
- Autres Hardware Trojans

Conclusion et perspectives

Nos objectifs

- On veut pouvoir :
  - Comprendre le processus de développement d'un HT,
  - Liste de HTs candidats,
  - Implanter ces HTs,
  - Vérifier que les HTs insérés peuvent être déclenchés.
- On veut un banc d'analyse par canaux auxiliaires :
  - le plus générique possible,
  - permettant de tester différents circuits...
  - ...infectés par différents HTs,
  - utiliser différentes méthodes statistiques.
- Side-chAnnel Standard Evaluation BOard (SASEBO)

Vue d'ensemble de SASEBO



- 2 FPGAs :
  - 1 pour le circuit testé (*Circuit Under Test*, CUT),
  - 1 pour le contrôle (utilisable pour différents CUTs).
- Connection USB entre le PC et SASEBO

Méthodes de déclenchement d'un HT

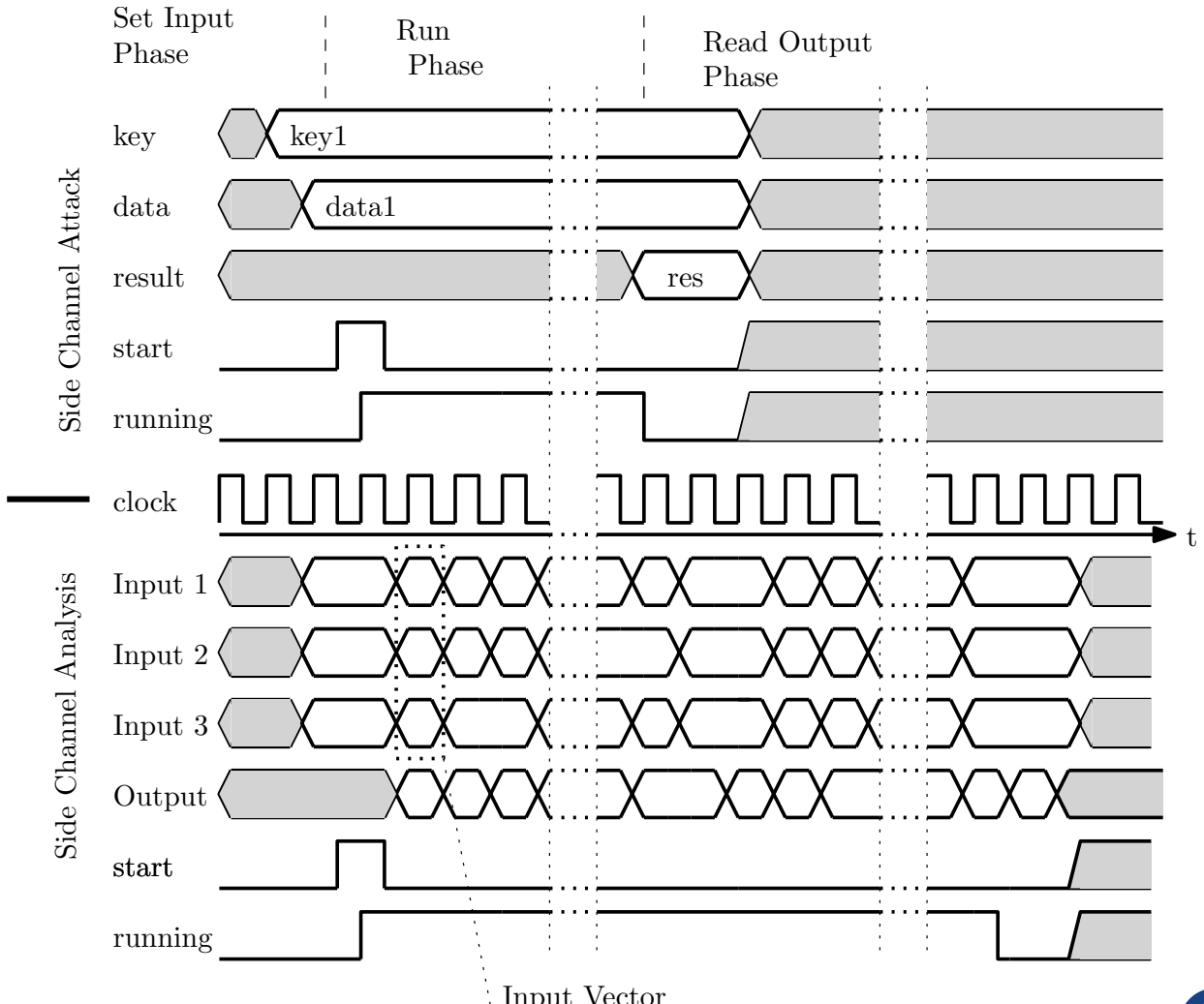
- Actif tout le temps
- Condition combinatoire
- Condition séquentielle
- *Time-bomb*
- Conditions physiques
- Conditions internes/externes

Analyse par canaux auxiliaires

- Littérature pas assez précise
- On ne sait pas où chercher
  - Durée de la mesure ?
  - Résolution ?
- $\Rightarrow$ Approche adaptative
- Vecteurs d'entrées à envoyer potentiellement à chaque cycle
  - Synchronisation

Analyse par canaux auxiliaires

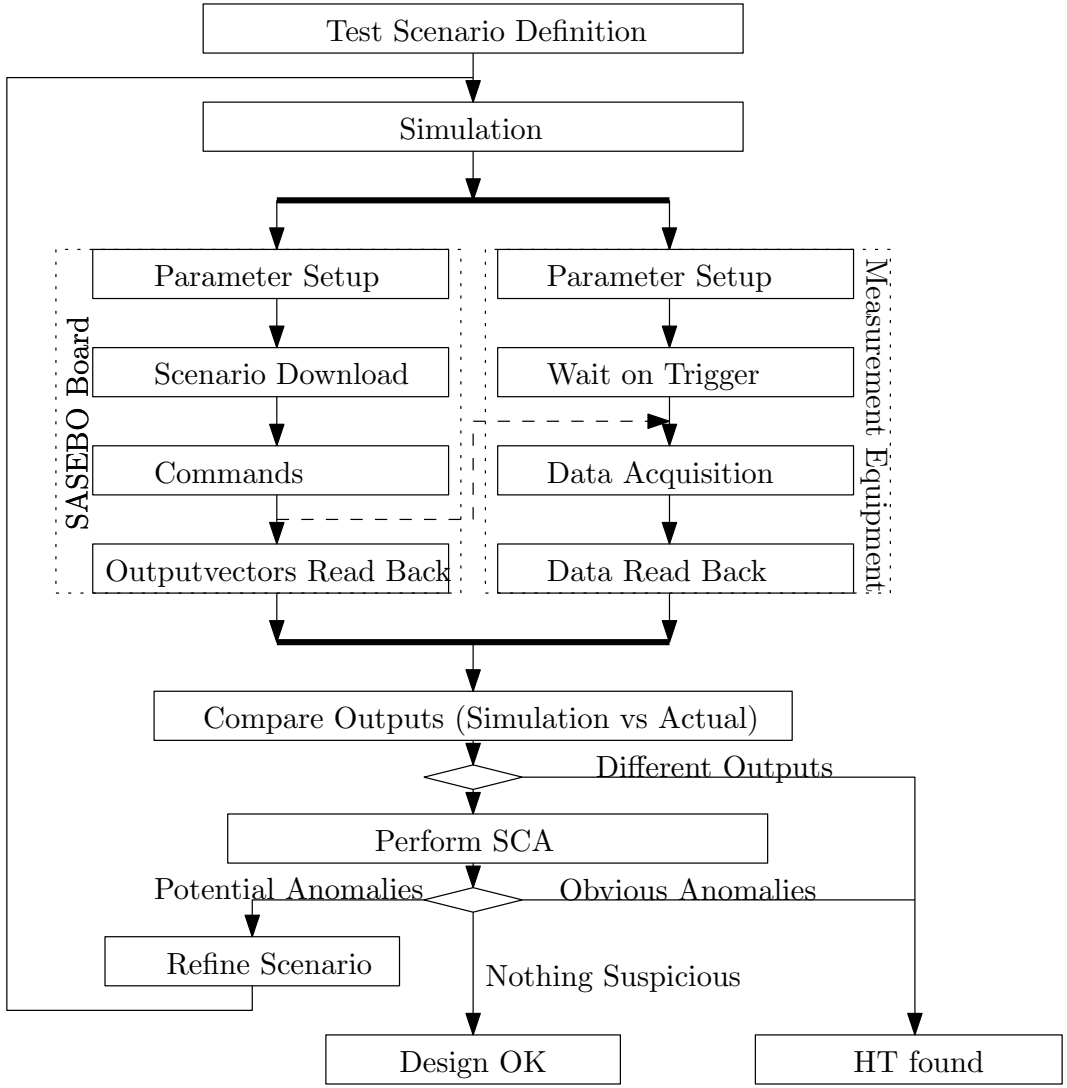
- Attaque (pour trouver des clés) $\neq$ Analyse (pour trouver des HTs)



Leçons à tirer pour notre banc

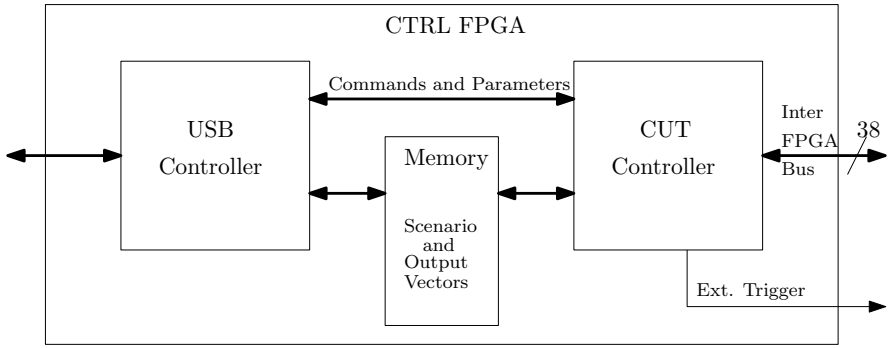
- En général :
  - il faut générer des séquences de vecteurs complexes,
  - on doit pouvoir acquérir des sorties intermédiaires,
  - données (I/O) manipulables en temps réel.
- Pour déclencher un HT, et donc pour le détecter, on a donc besoin
  - d'attendre longtemps,
  - de réagir suivant l'état du circuit testé.
- Pour les canaux auxiliaires :
  - Déclenchement dynamique des mesures

Déroulement des opérations



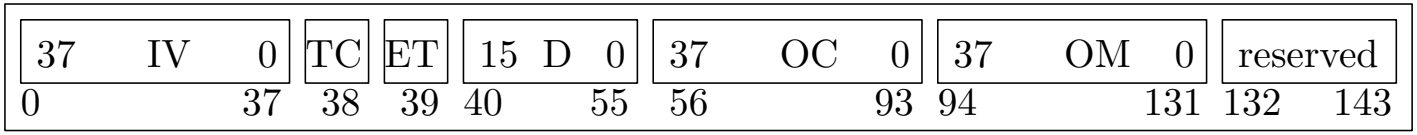
Description d'un scénario de test

- Communication via USB du fichier du scénario de test
- Il sera stocké dans la mémoire (BRAM) du FPGA de contrôle



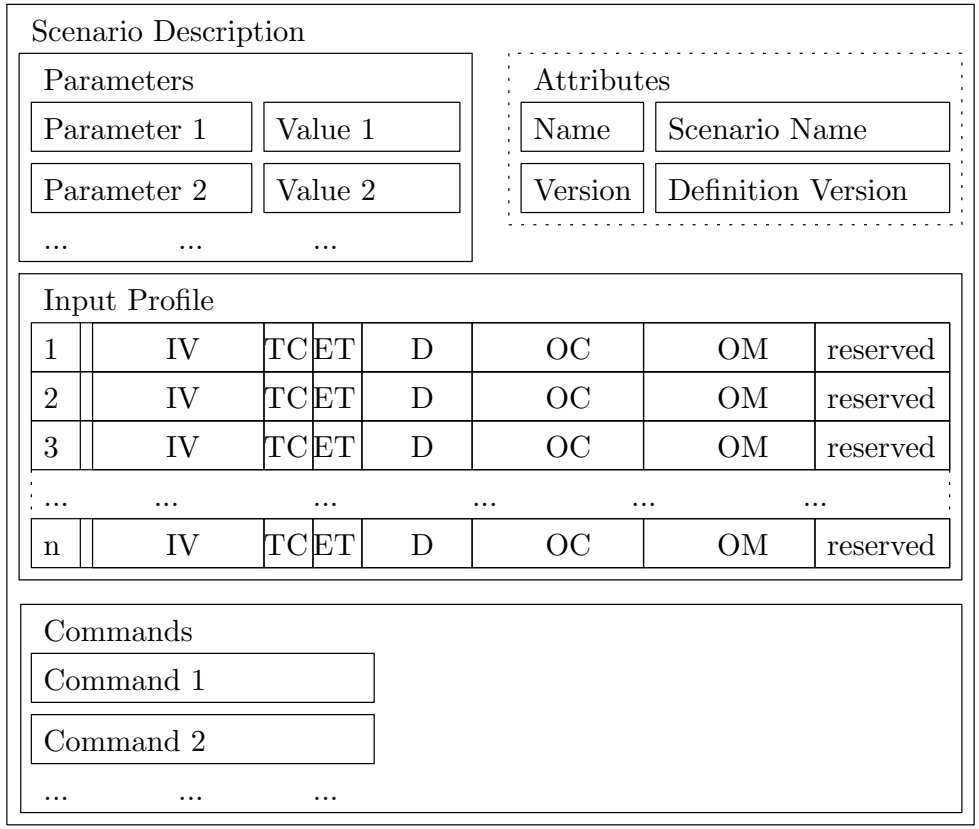
- 3 options pour l'envoi du prochain vecteur d'entrée
  - Immédiat
  - Condition sur le temps
  - Condition sur les sorties
- Indicateur de déclenchement externe
- Quel format de données adopter ?

Format des données



- IV: *Input Vector*,
- TC: *Transition Condition*, conditions sur le temps ou sur la sortie pour envoyer le prochain IV,
- ET: *External Trigger*, envoie l'ordre à l'oscilloscope de lancer la mesure,
- D: *Delay* : nombre de cycles d'horloge pour retarder le prochain IV,
- OM: *Output Mask* : quels bits regarde-t-on ?
- OC: *Output Condition* : valeurs de ces bits pour passer au prochain IV.

Format d'un scénario de test



- Paramètres : *tristate mask*
- Contrôleur supportant ce format implanté

Introduction aux Hardware Trojans et à HOMERE

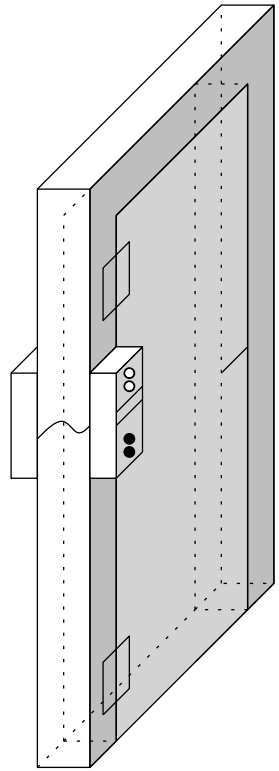
Construction d'un banc d'expérimentations
- Nos objectifs
- Utilisation de SASEBO
- Comment déclencher un HT ?
- Analyse par canaux auxiliaires
- Scenarii de tests

Présentation d'un cas d'étude : contrôle d'accès
- Présentation
- Injecter/tester un HT combinatoire
- Autres Hardware Trojans

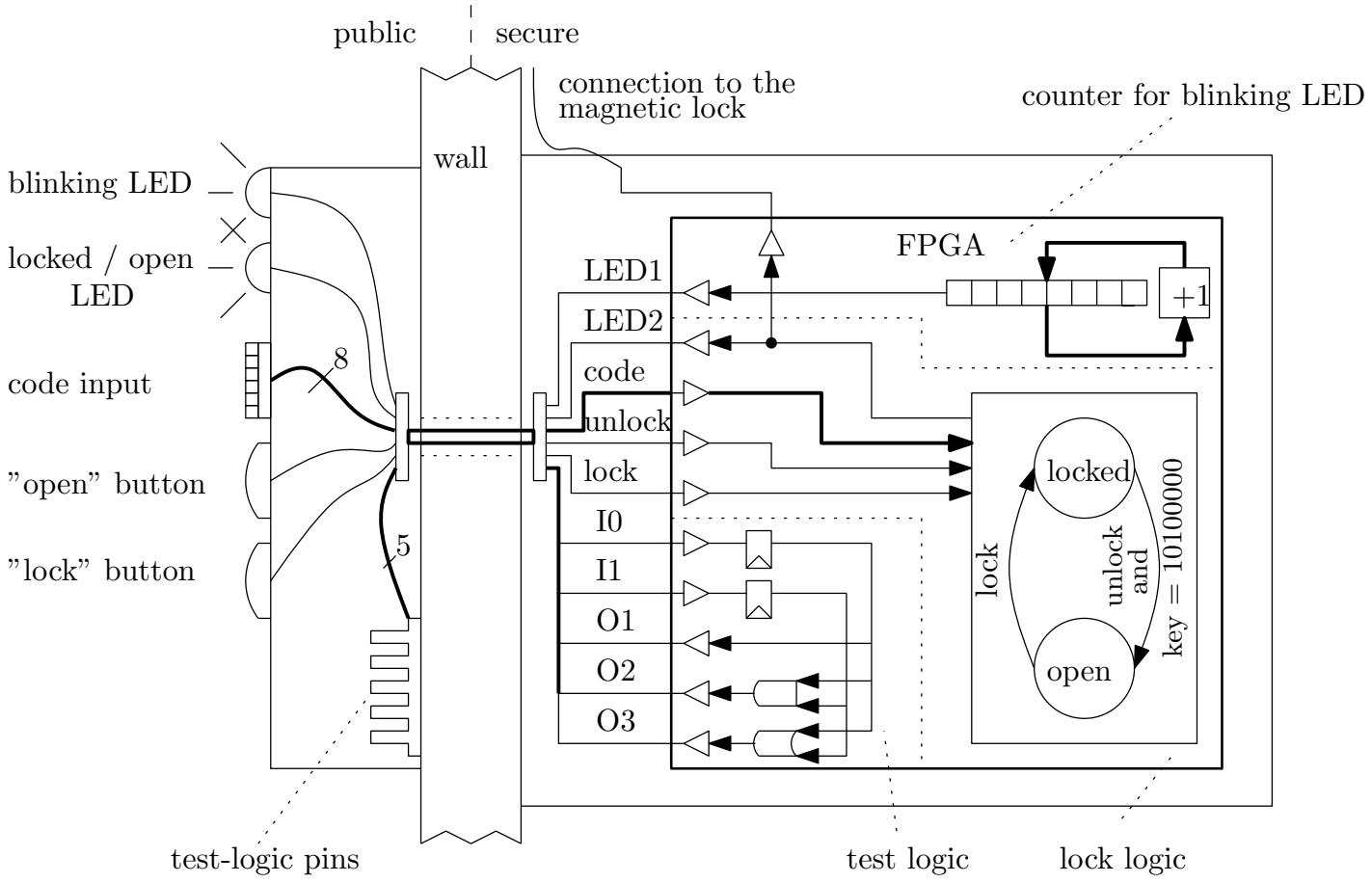
Conclusion et perspectives

Étude de cas : contrôle d'accès

- Buts de cette étude de cas :
  - Montrer la fonctionnalité de l'environnement de test
  - Montrer comment un circuit peut être infecté
  - Pris volontairement simple



Cas d'étude



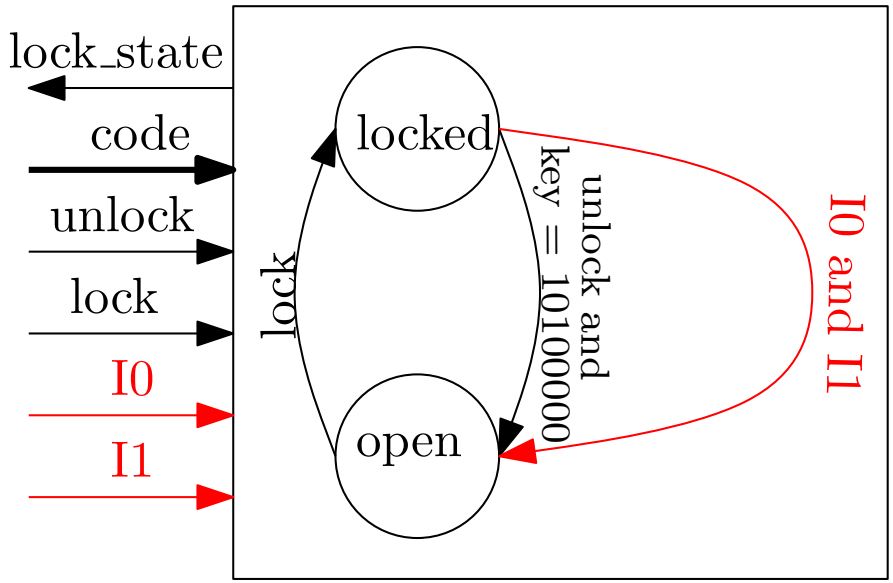
- Code d'accès 8 bits, 2 boutons de contrôle, LED clignotante (implanté avec un compteur 8 bits), 2 pins de test

Scénario d'attaque

- But de l'attaquant : ouvrir la porte sans la clé !
- Note : 8 bits insuffisants dans la réalité
  - "*Toy example*"
- Accès public à l'interface, aux boutons et aux LEDs
- On considère dans notre cas d'étude que les 2 pins de test sont accessibles
  - But initial : test fonctionnel

HT1 (combinatoire)

- Idée : ouvrir la porte en utilisant les pins de test
- Changer le circuit de telle sorte que si les deux signaux sont égaux à 1, la porte s'ouvre



- Très simple à concevoir et à activer mais facile à détecter pendant le test fonctionnel ou l'implantation du système

Implantation de HT1

- Peut être faite à un haut niveau (ex. : VHDL)
- Mais cela peut causer des changements majeurs dans le layout final
- Au niveau configuration du FPGA (via FPGA Editor)
  - Contenu des LUTs
  - Routage
  - Configurations (FFs or LATCH, IBUF delays in IOB, etc.)
- On travaille sur une information équivalente au bitstream
- Une telle attaque peut être effectuée si le système est livré en boîte noire

HT1 en RTL

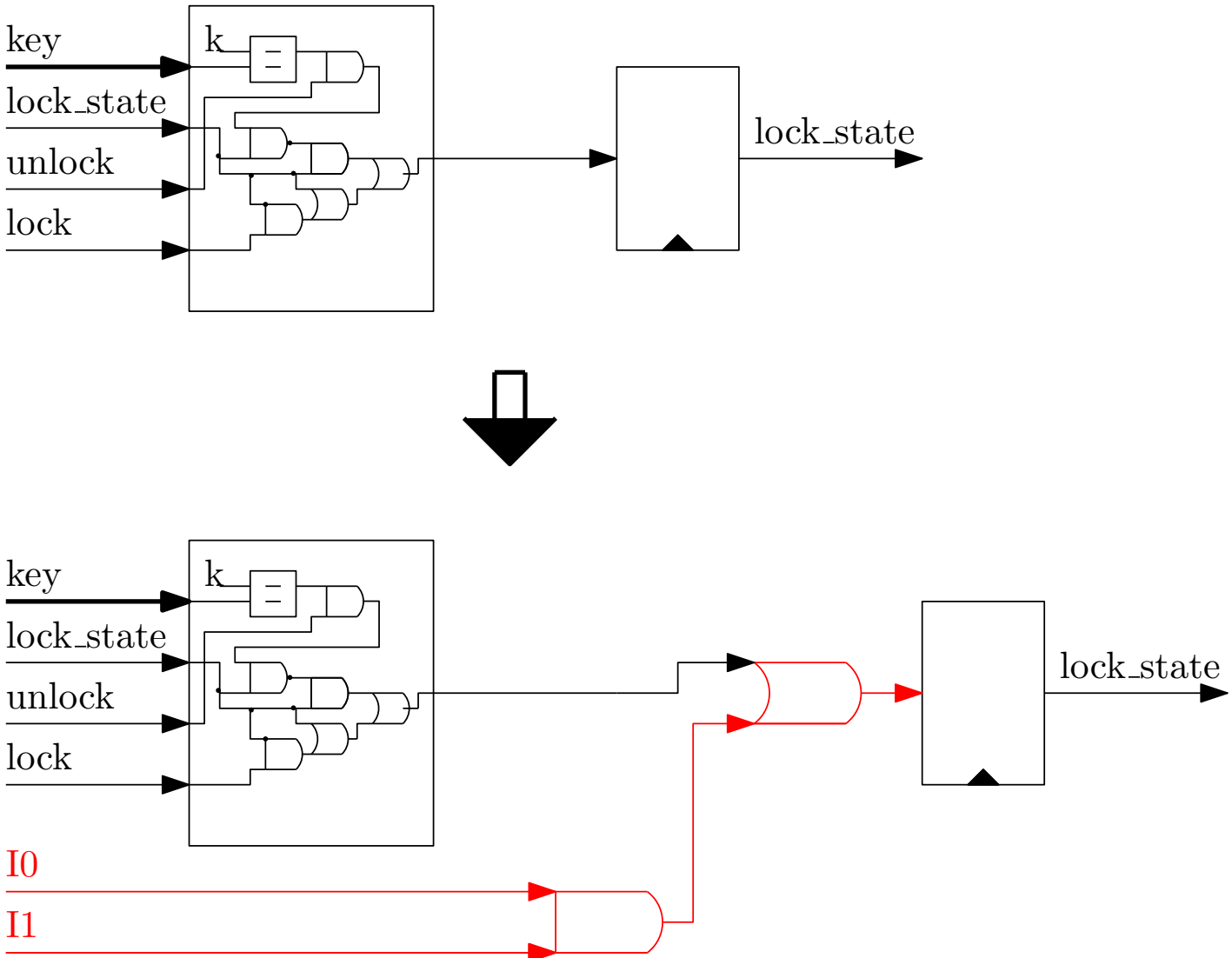
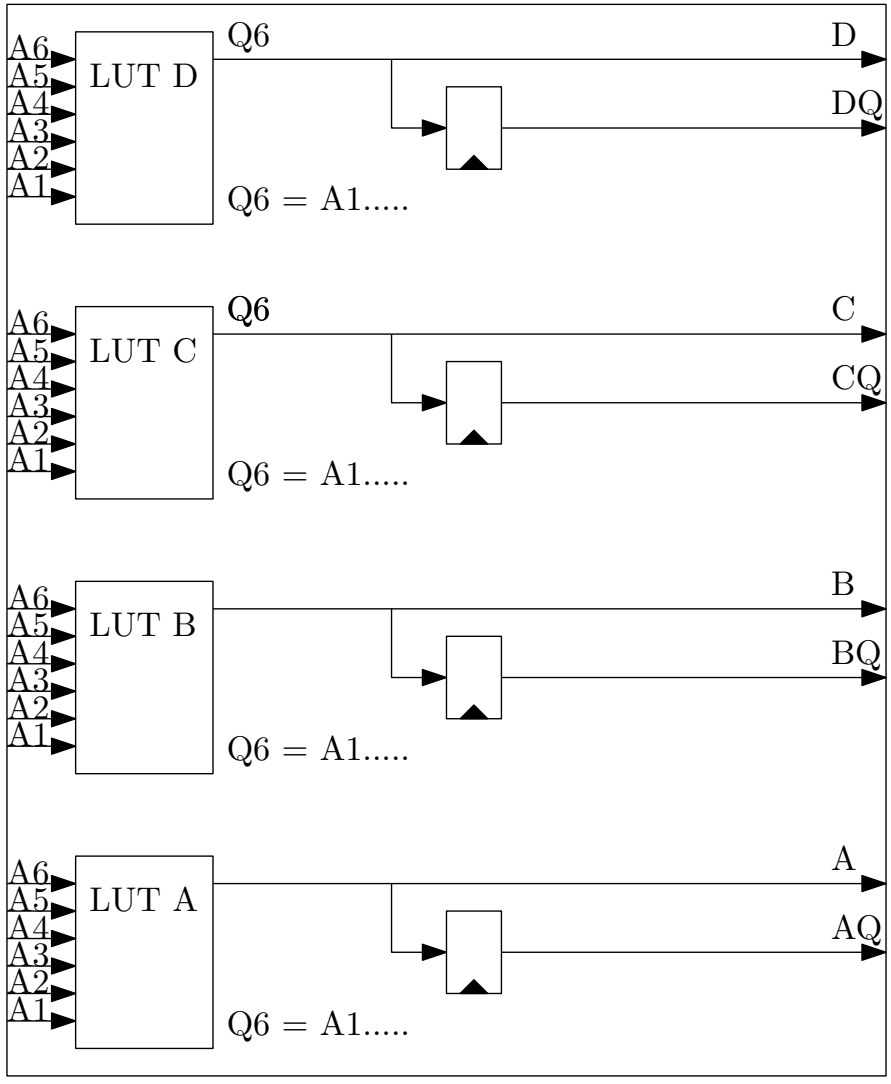
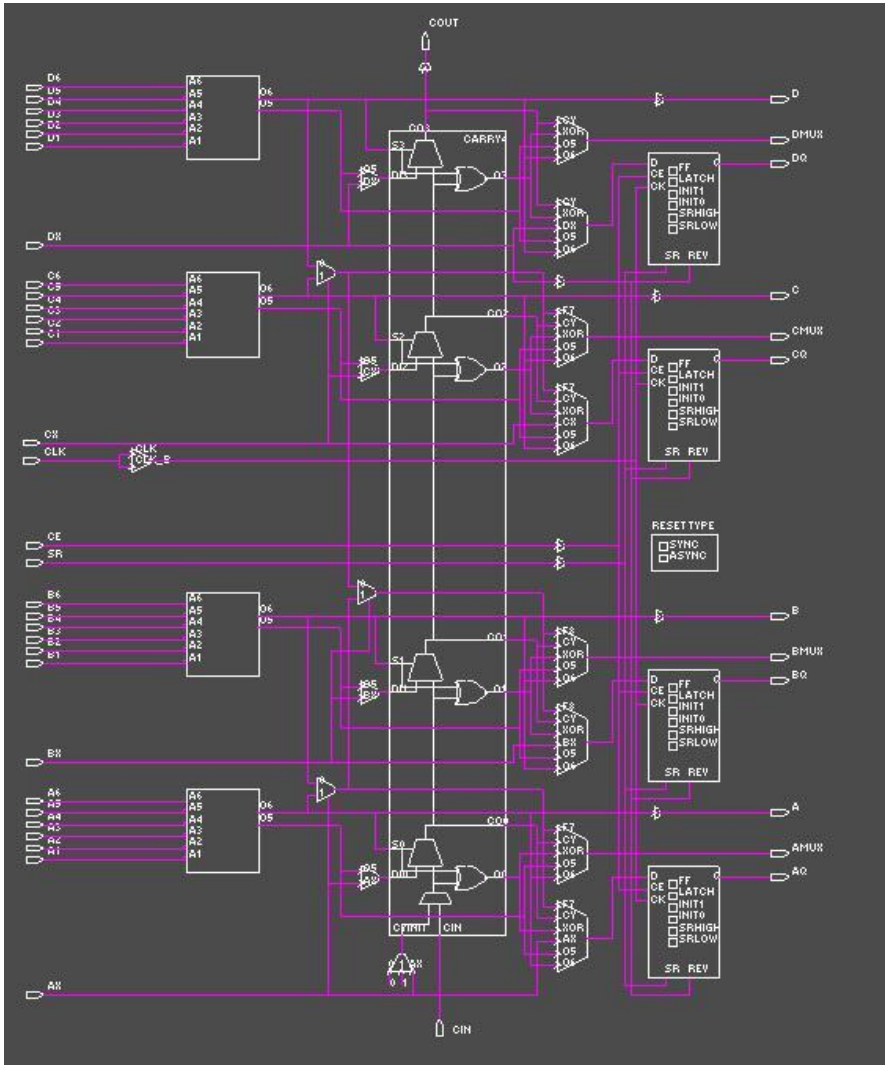


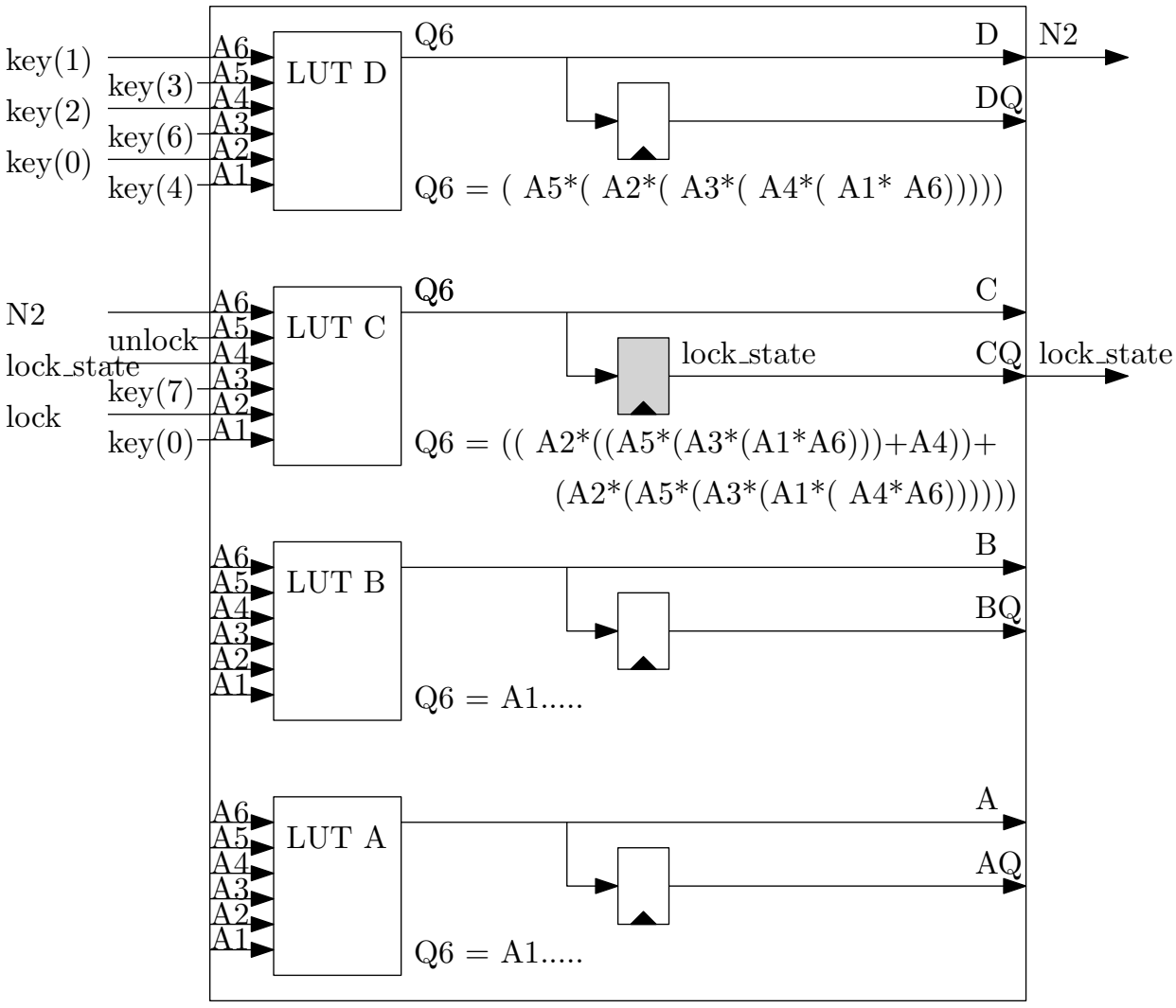
Schéma d'une slice d'un Virtex-5 50T



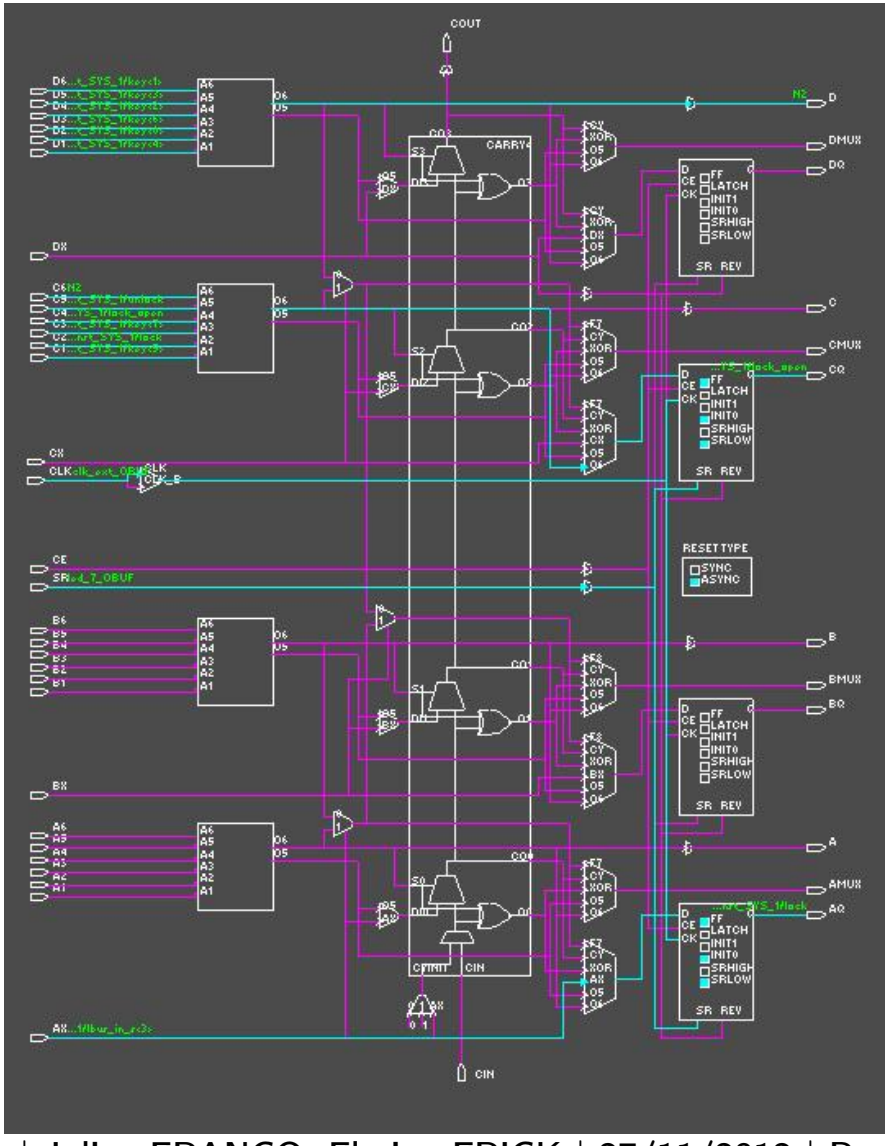
La même sur FPGA Editor



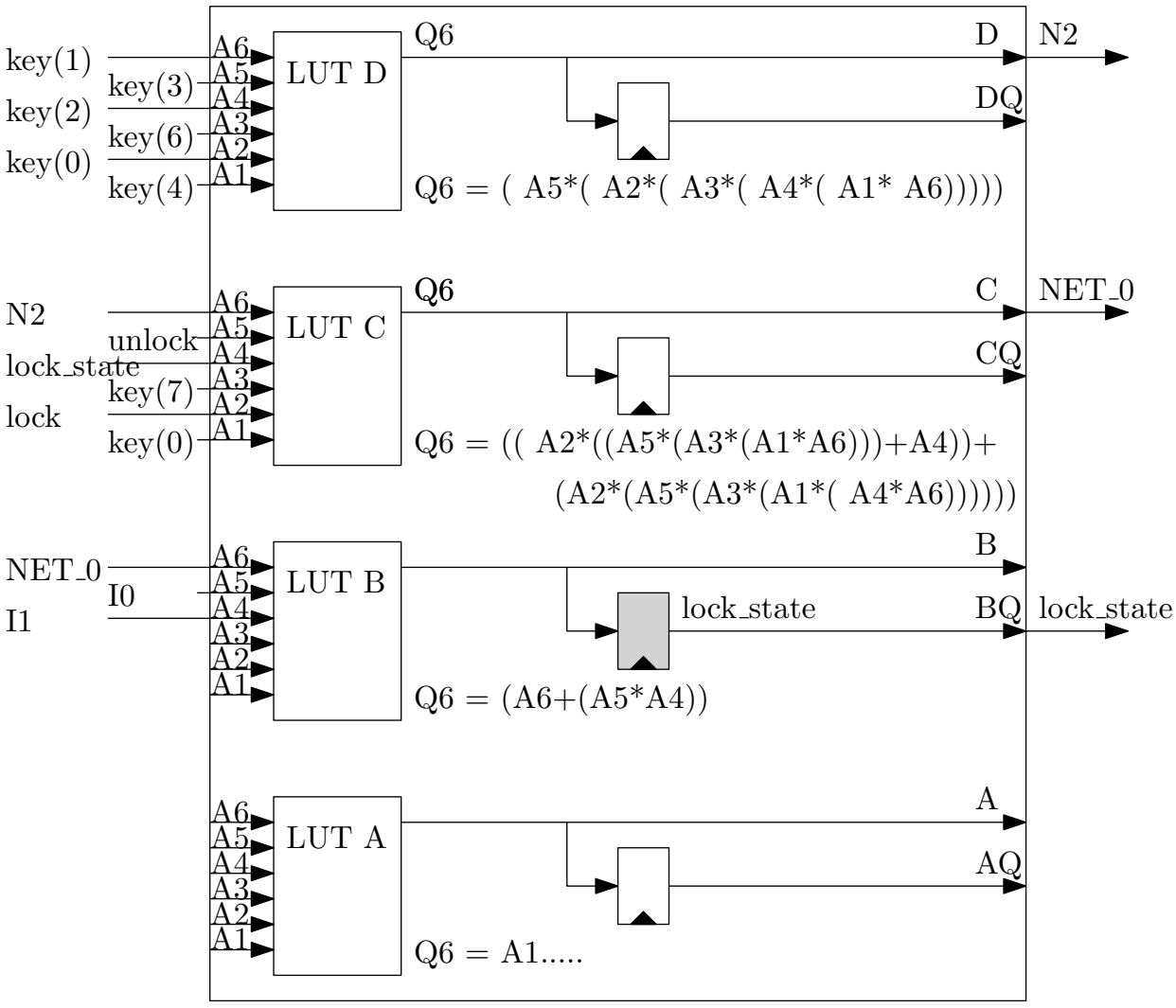
Circuit non-infecté



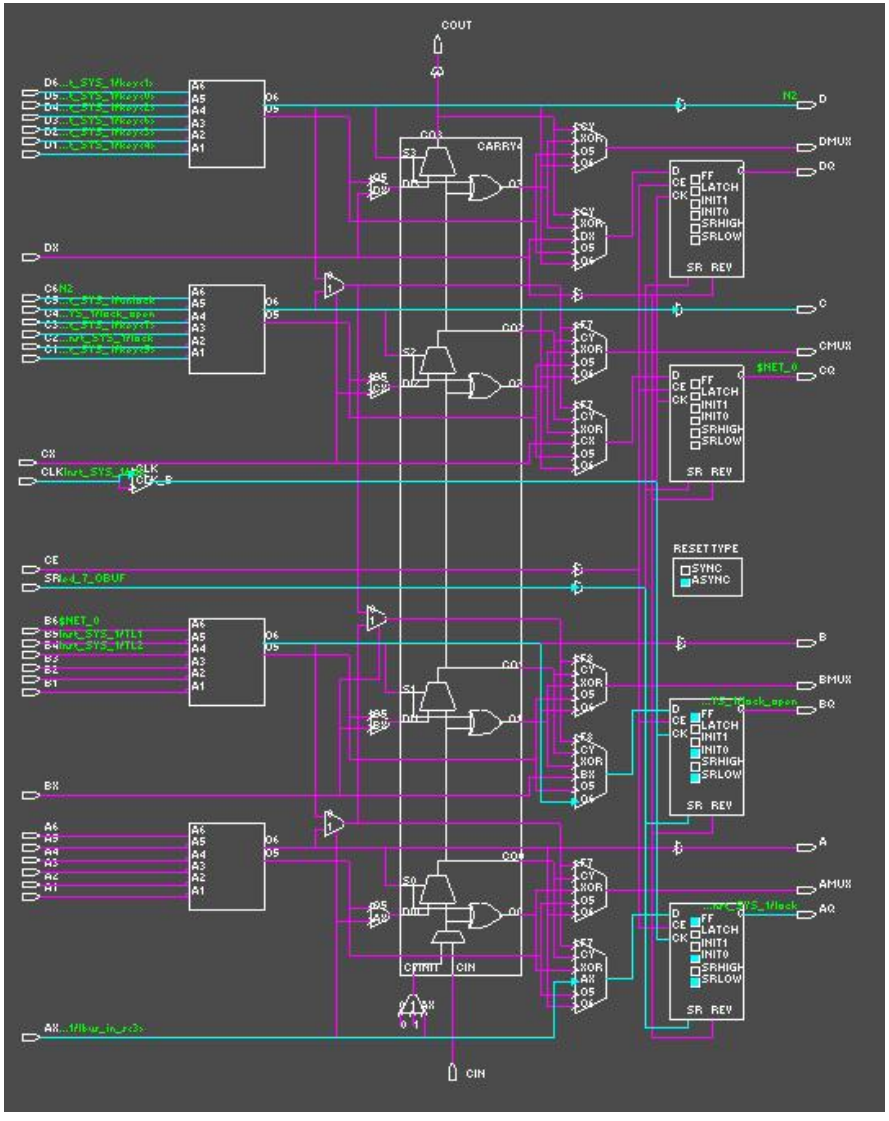
Circuit non-infecté



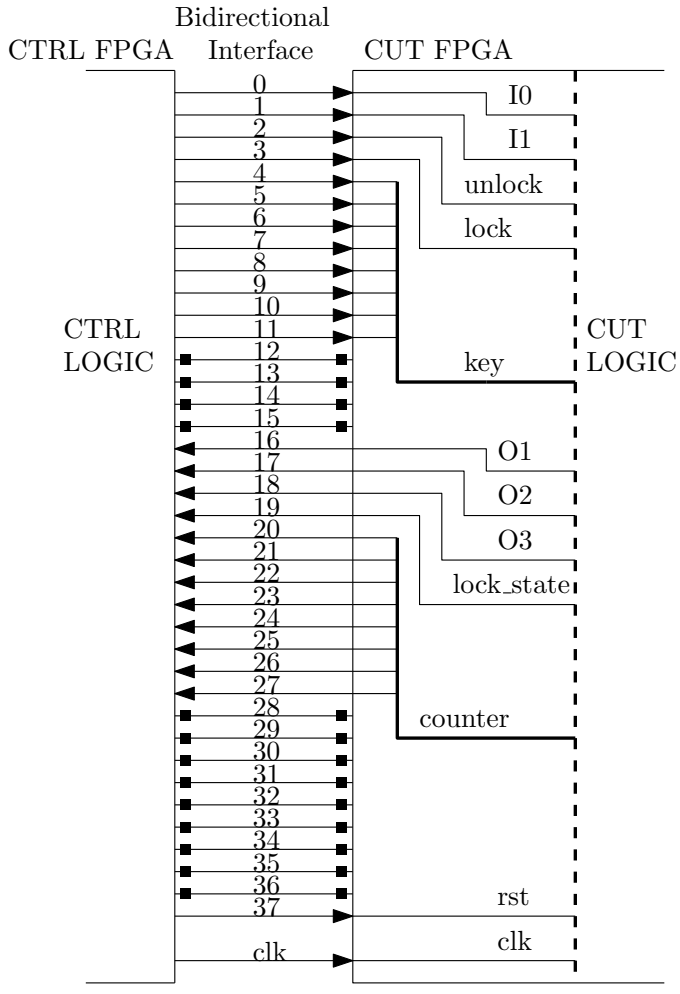
Circuit infecté par HT1



Circuit infecté par HT1



Port Map dans SASEBO



Validation du fonctionnement

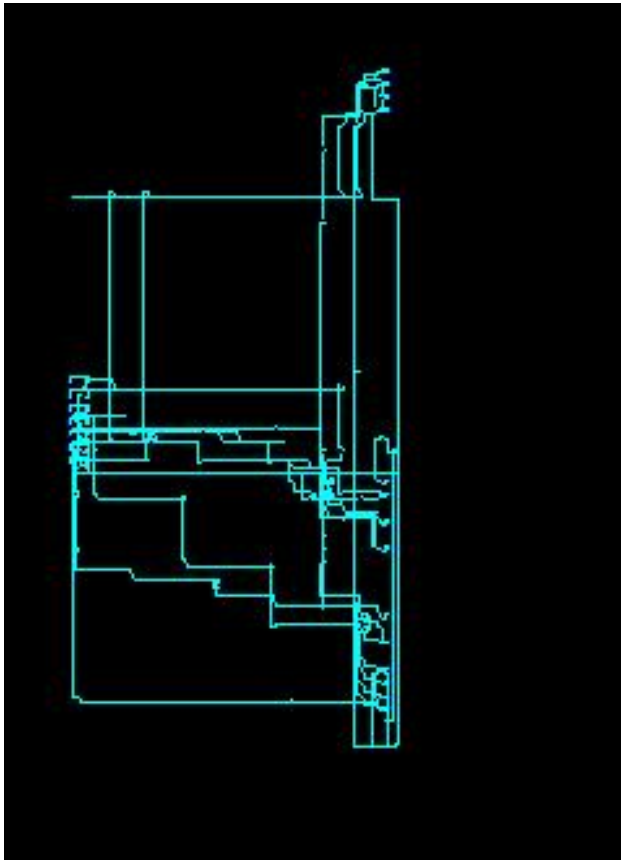
	Input					Output				
cycle	unlock	lock	key	TP1	TP2	state	TO1	TO2	TO3	counter
0	0	0	0	1	0	locked	0	0	0	0
1	1	0	160	0	1	locked	1	0	1	1
2	0	1	0	0	0	locked	0	0	1	2
3	0	0	0	0	0	open	0	0	0	3
4	0	0	0	1	1	locked	0	0	0	4
5	0	0	0	0	0	locked	1	1	1	5
6	0	0	0	0	0	locked	0	0	0	6

Validation du fonctionnement

	Input					Output				
cycle	unlock	lock	key	TP1	TP2	state	TO1	TO2	TO3	counter
0	0	0	0	1	0	locked	0	0	0	0
1	1	0	160	0	1	locked	1	0	1	1
2	0	1	0	0	0	locked	0	0	1	2
3	0	0	0	0	0	open	0	0	0	3
4	0	0	0	1	1	locked	0	0	0	4
5	0	0	0	0	0	locked	1	1	1	5
6	0	0	0	0	0	open	0	0	0	6

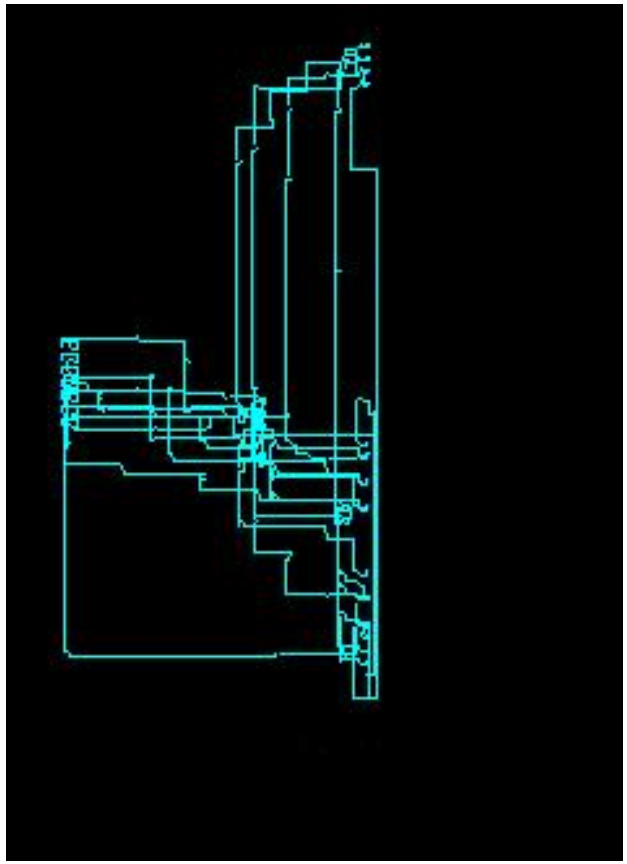
- Fonctionne en simulation et sur notre banc

Circuit original



Circuit infecté “manuellement”

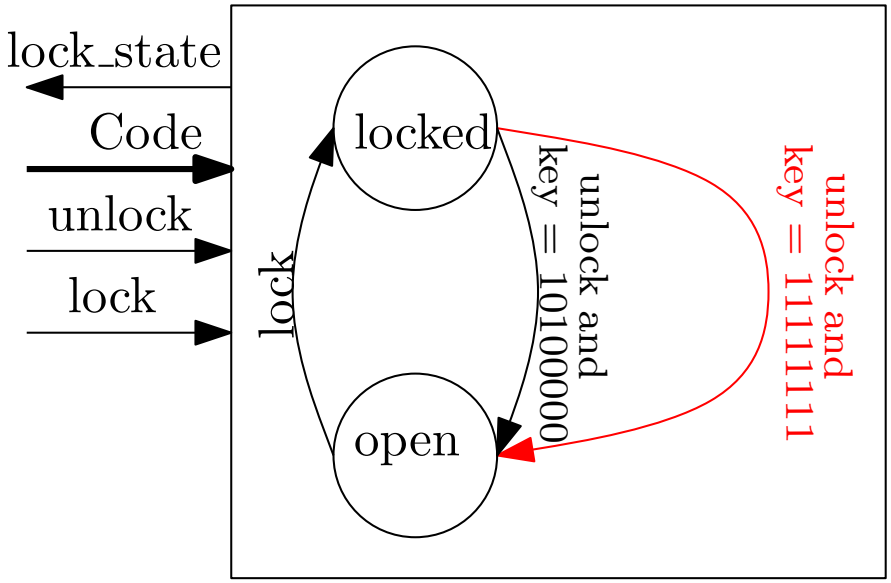
Circuit infecté en VHDL



- if ((unlock = 1) and (key = 10100000)) or ((TL1 = 1) and (TL2 = 1)) then lock open <= 1; end if;

HT2 (combinatoire)

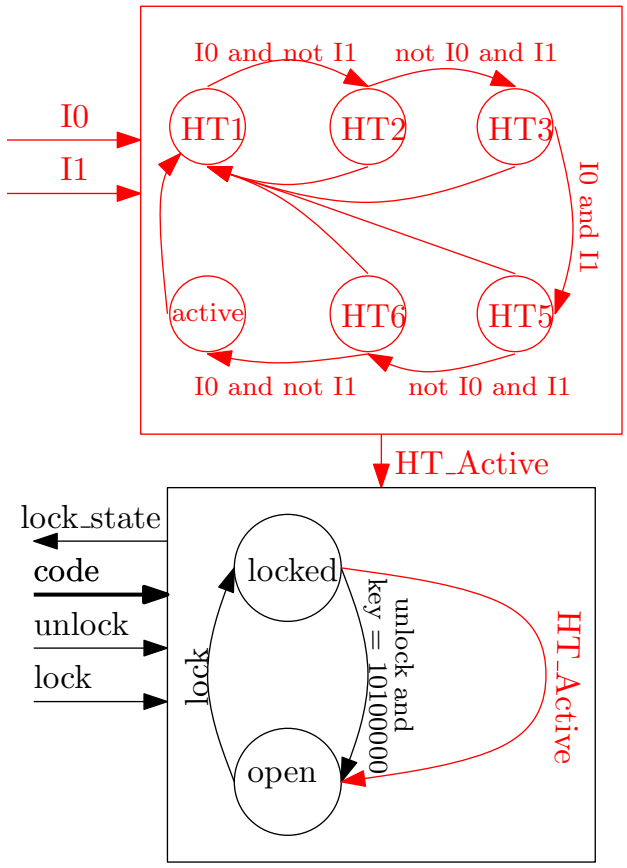
- Ajouter une clé maître qui marchera tout le temps



- Dans le cas d'un code 8 bits, facile à détecter lors du test fonctionnel
  - "Toy example"

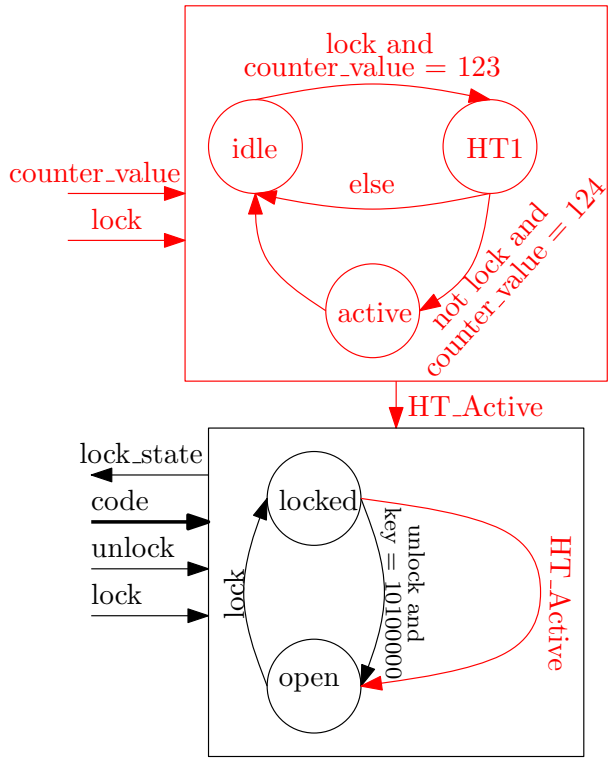
HT3 (séquentiel)

- Utiliser les pins de test (ou peut-être le bouton de fermeture de la porte) pour contrôler une petite machine à états finis
- Si une certaine combinaison est entrée, cela ouvre la porte



HT4

- Réutiliser le compteur de la LED
- Récupérer son état en observant le signal de la LED
- Le coupler avec une condition séquentielle simple



Introduction aux Hardware Trojans et à HOMERE

Construction d'un banc d'expérimentations
- Nos objectifs
- Utilisation de SASEBO
- Comment déclencher un HT ?
- Analyse par canaux auxiliaires
- Scenarii de tests

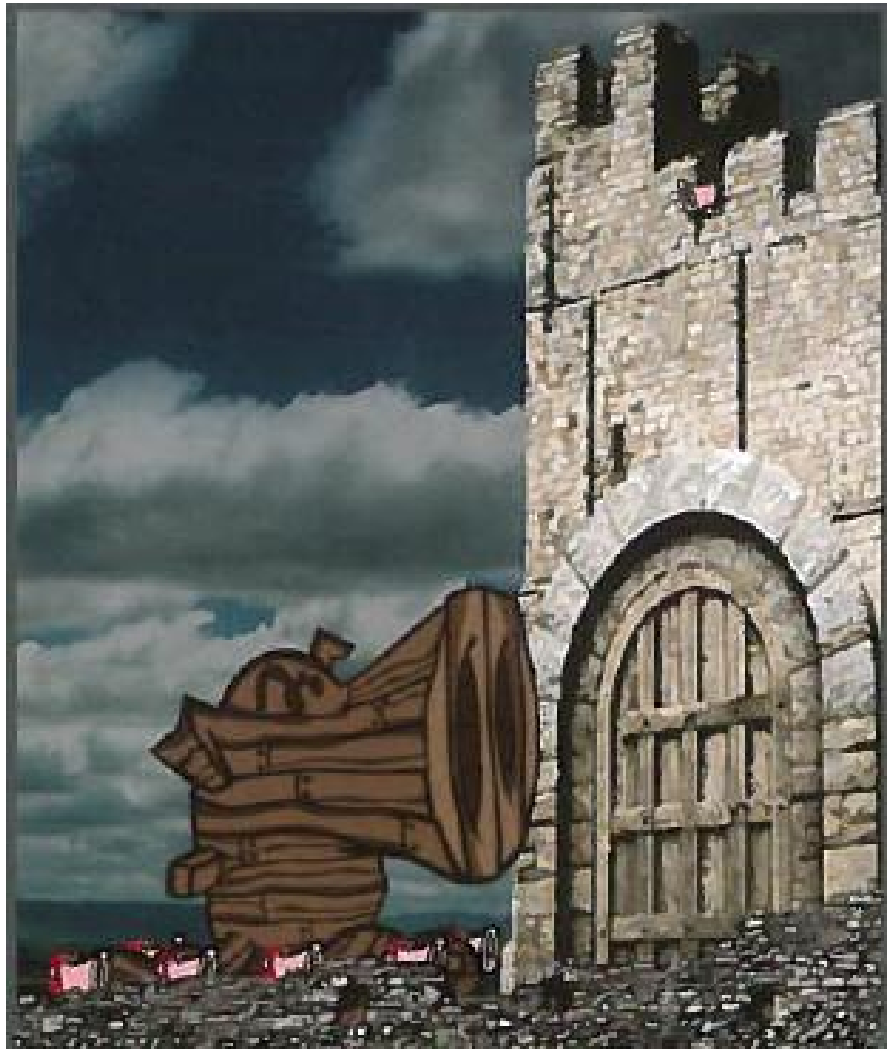
Présentation d'un cas d'étude : contrôle d'accès
- Présentation
- Injecter/tester un HT combinatoire
- Autres Hardware Trojans

Conclusion et perspectives

Conclusion

- Preuve de concept de notre banc fonctionne avec un cas d'étude simple
- Architecture flexible
- L'infection d'un circuit par des HTs par la manipulation de la configuration d'un FPGA est possible...
- ...et modifications limitées (proche de la réalité)
- *Side-Channel Analysis* $\neq$ *Side-Channel Attack*
- Plusieurs trojans trouvés sur un cas simple...
- Approche sur SASEBO transposable aux ASICs
- Commandes pour l'oscilloscope
- Approche adaptative ?

Je vous remercie de votre attention. Avez-vous des questions ?



Credits: Snort