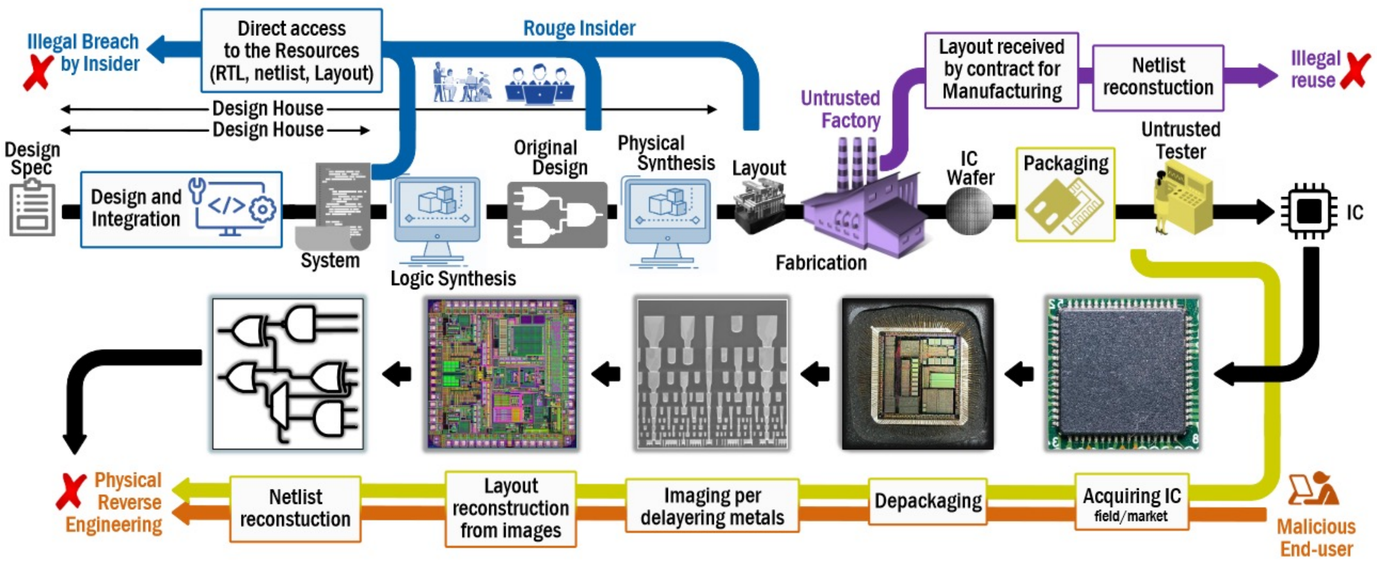
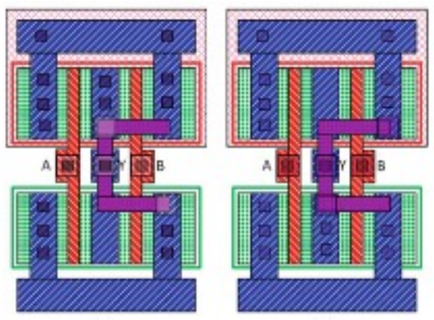
Méthodes de Logic Locking résistantes aux attaques par canaux auxiliaires

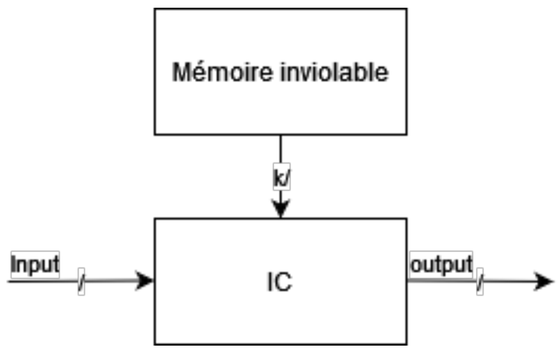
Nassim Riadi, Marie-Lise Flottes, Florent Bruguier, Sophie Dupuis, Pascal Benoit
LIRMM, Université de Montpellier, CNRS, Montpellier, France
<prénom>.<nom>@lirmm.fr

MOTIVATIONS

- Globalisation de l'industrie microélectronique.
- Vol de la propriété intellectuelle.
- Contrefaçon.
- Surproduction ou manipulation frauduleuse de la part d'une fonderie non digne de confiance.
- Développement de solution souveraines pour la protection de la propriété intellectuelle.







Camoufaging.

Logic Locking.

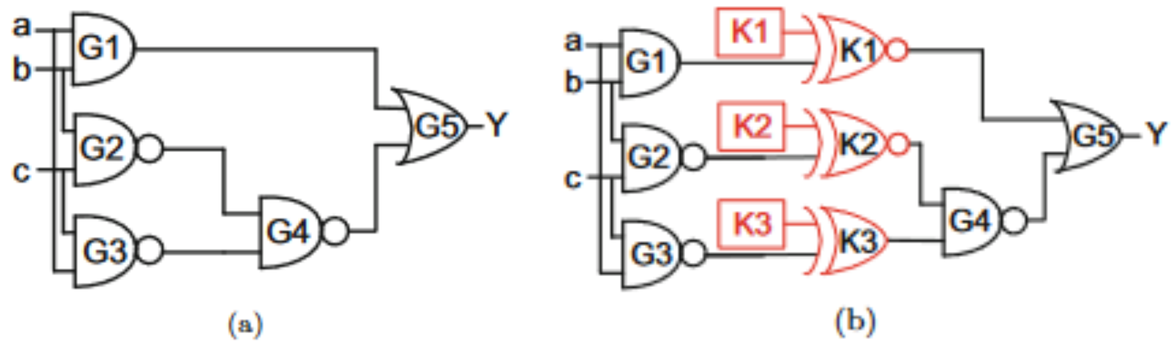
SOLUTIONS

Les solutions proposées dans la littérature contre ces risques sont regroupés sous le nom de DFTr (Design Fort Trust), e.g:

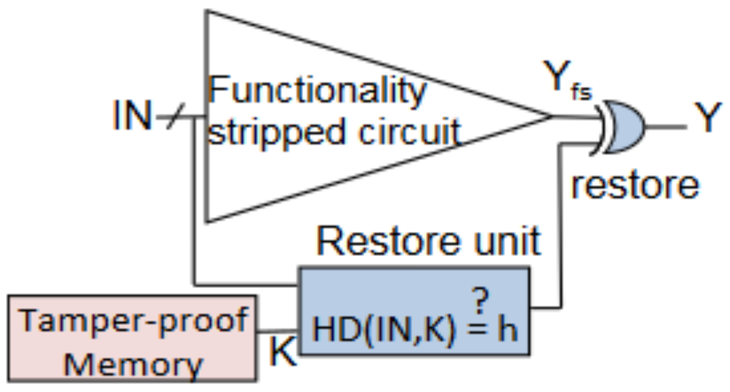
- Camouflaging.
- Logic Locking.

SOLUTION EXPLOREE : LOGIC LOCKING

Le ***Logic Locking*** consiste à verrouiller un circuit à l'aide d'une clé secrète connue du seul concepteur. Le comportement du circuit n'est conforme au cahier des charges que lorsqu'il est programmé avec la clé secrète après fabrication par ce dernier.



Principe du Logic Locking.



SFLL (Stripped Funcitonnality Logic Locking).

ATTAQUES SUR LE LOGIC LOCKING

En 2015 une attaque basée sur la satisfiabilité booléenne (SAT attack) a réussi à casser tous les schémas pré-existants.

Les nouvelles approches résistent à la SAT Attack (e.g. SFLL) mais présentent des faiblesses vis-à-vis d'attaques de plus en plus puissantes et ciblées.

TRAVAUX EN COURS

Dans le cadre du projet **PEPR ARSENE**, cette thèse a pour but l'évaluation de la robustesse des schémas actuels de Logic Locking face aux attaques par analyse de consommation (DPA, CPA).

PERSPECTIVES

- Attaques de nouveaux schémas par analyse de consommation.
- Etudes de nouvelles méthodes de protection d'IP (eFPGA, TLL).

Références:

[1] H. M. Kamali, K. Z. Azar, F. Farahmandi, et M. Tehranipoor, « Advances in Logic Locking: Past, Present, and Prospects ».

[2] M. Yasin, J. Rajendran, et O. Sinanoglu, Trustworthy Hardware Design: Combinational Logic Locking Techniques.

[3] J. A. Roy, F. Koushanfar and I. L. Markov, "EPIC: Ending Piracy of Integrated Circuits".

Plus d'infos > www.lirmm.fr