ARC 6 : Technologies de l'Information et de la Communication et Usages Informatiques Innovants

Technologies et composants avancés pour l'électronique, l'optique et les systèmes intégrés - Microélectronique

Système sécurisé d'activation à distance de circuits intégrés et de composants virtuels

- **Nécessité de pouvoir (dé)verrouiller les circuits à distance (protection),**
- **Utilisation de graphes pour représenter les designs,**
- **Sélection optimale des lieux d'insertion des portes logiques de verrouillage,**

POINTS CLES

Verrouillage à distance :
- **Léger**, pour ne pas engendrer un surcoût trop important,
- **Sûr**, pour ne pas pouvoir être contourné facilement,
- **Rapide** à insérer dans le design de départ,
- **Facile** à utiliser pour un client légitime.

PROBLEMATIQUE

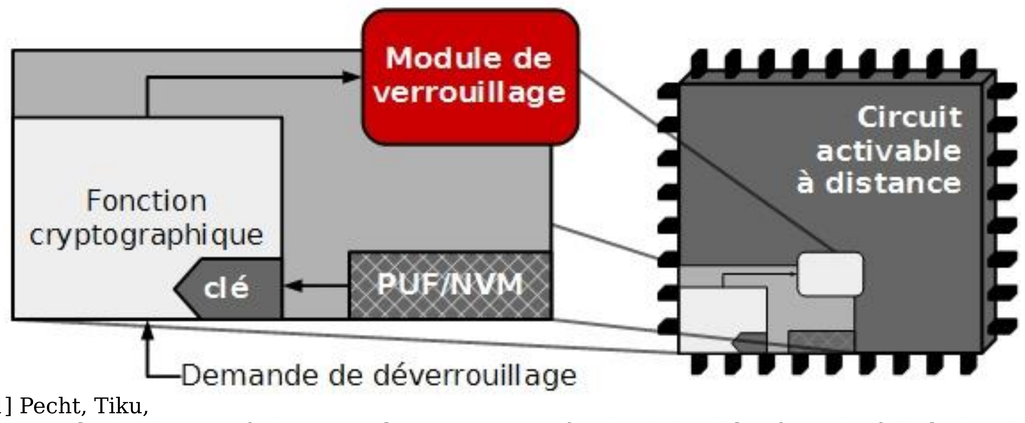
Fabrication des circuits intégrés délocalisée :
- séparation entre conception et fabrication,
- transfert **total** du design.

Problèmes : surproduction et contrefaçon.

Un article [1] de 2006 estimait à 100 milliards de dollars par an les pertes associées.

Solution proposée :
Le circuit doit être **activé** pour fonctionner.
Ainsi, les copies illégales sont inutiles.

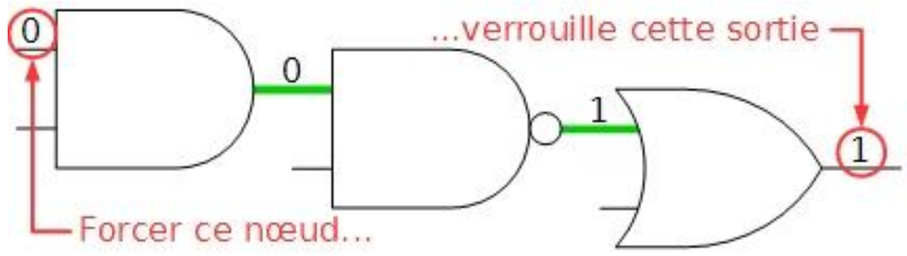
Caractéristiques :
- Sécurité : fonction cryptographique
- Unicité : identifiant unique par instance (PUF/NVM)
- Efficacité : module de verrouillage.



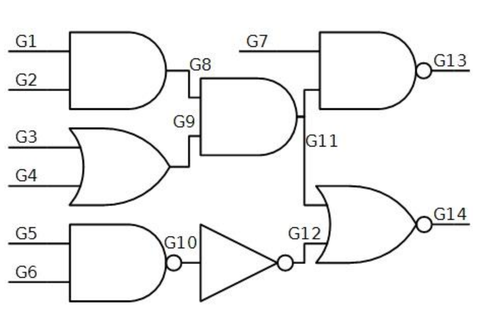
[1] Pecht, Tiku,
Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics
IEEE Spectrum, **2006**, *43*, 37-46

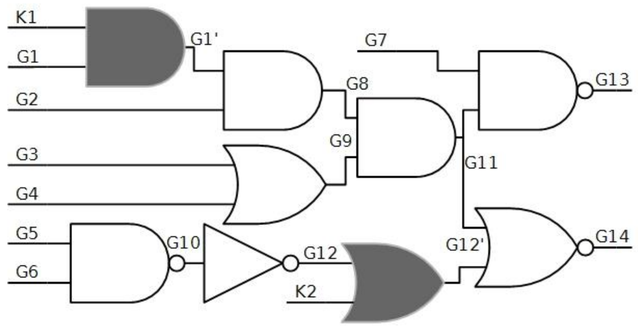
TRAVAUX ENGAGES / RESULTATS

Verrouillage fonctionnel :
Identifier les suites de portes logiques pouvant **verrouiller** une ou plusieurs sorties du circuit en propageant une valeur de verrouillage.



Méthode :
- Convertir la netlist en **graphe orienté**,
- Identifier les suites d'arcs et sommets intéressants, qui peuvent **propager une valeur de verrouillage**,
- Insérer une **porte de verrouillage** au début des suites Identifiées pour appliquer la valeur de verrouillage.
- Générer une netlist **verrouillable**.





Comparaison :

	État de l'art [2]	Méthode présentée
Surcoût en ressources logiques	+6%	+3%
Durée d'analyse d'une netlist type (3500 portes)	4h30min	0,87s
Choix des lieux d'insertion	Approximatif (simulation)	Optimal (analyse)

À faire :
- Protocole d'activation sécurisé,
- Implantation du système global et évaluation du coût,
- Évaluation de la sécurité du système.

[2] Rajendran, Zhang, Rose, Pino, Sinanoglu, Karri
Fault analysis-based logic encryption
IEEE Transactions on Computers, **2015**, *64*, 410-424

Publications associées :
- Conférence internationale ISVLSI, Juillet, Montpellier.
- Workshop Cryptarchi, Juin, Leuven, Belgique.

Brice Colombier, Lilian Bossuet
Laboratoire Hubert Curien, UMR CNRS 5516
Saint-Étienne
b.colombier@univ-st-etienne.fr

David Hély
LCIS – Grenoble Institute of Technology
Valence