

Sécurisation des circuits intégrés contre le piratage

Projet SESI proposé par Alan DIAZ RIZO

Maître de Conférences

Sorbonne Université, Laboratoire LIP6, équipe CIAN

alan-rodrigo.diaz-rizo@lip6.fr

2024-2025

1 Contexte

Pour développer et fabriquer un circuit intégré (CI) ou « puce électronique », la plupart des entreprises font appel à des concepteurs tiers de blocs IP, à des intégrateurs de systèmes sur puce (SoC), à des fonderies délocalisées, ainsi qu'à d'autres services sous-traités. Cette situation, combinée à la capacité de rétro-ingénierie des puces permettant d'en extraire la conception du CI, introduit plusieurs vulnérabilités en matière de sécurité, comme l'illustre la figure. 1. Un attaquant peut (i) voler la conception d'un CI (clonage), (ii) copier des parties et les réutiliser, ou (iii) produire des contrefaçons (surproduction et utilisation non autorisée). De plus, il/elle peut (iv) falsifier les résultats des tests pour conserver des puces fonctionnelles et les revendre (remarquage). En fin de vie du CI, (v) il est également possible de recycler des puces anciennes et de les revendre comme neuves (recyclage non autorisé). En outre, un attaquant peut également effectuer des modifications malveillantes dans la conception, c'est-à-dire insérer des chevaux de Troie matériels (*Hardware Trojans* HT), afin de perturber les performances, de créer des canaux cachés pour exfiltrer des données sensibles, ou de provoquer une attaque par déni de service. Le piratage des CI et l'insertion de HT constituent des préoccupations majeures pour l'industrie des semi-conducteurs et pour la société dans son ensemble.

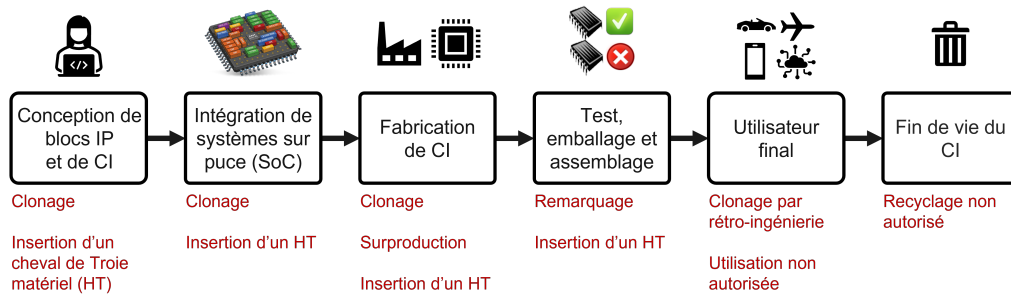


FIGURE 1 – Menaces pesant sur la sécurité de la chaîne d'approvisionnement des Circuits Intégrés.

Pour prévenir le piratage des CI, le verrouillage est la solution la plus efficace [1]. Le verrouillage, effectué par le concepteur légitime de l'IP, du CI ou du SoC, intègre dans la conception d'origine un circuit, appelé mécanisme de verrouillage, contrôlé par une clé, qui est généralement une chaîne binaire. Pour la clé correcte, le mécanisme de verrouillage est transparent et la fonctionnalité du CI attendue est établie, tandis que pour une clé incorrecte, la fonctionnalité du CI est corrompue. Le mécanisme de verrouillage est mêlé à la conception d'origine et la clé n'est jamais partagée avec des parties non fiables.

La Fig. 2 montre un exemple de verrouillage pour un circuit numérique, également appelé verrouillage logique (*logic locking*). La sortie Y du circuit verrouillé (*locked circuit*) est corrompue par l'insertion de portes-clés (XOR, XNOR), illustrées avec un cadenas rouge. La sortie Y n'est corrigée que si les bits de clé (k_1, k_2) sont (0,1), toute autre entrée de clé ne corrige pas la sortie Y , de sorte que le circuit est dit verrouillé.

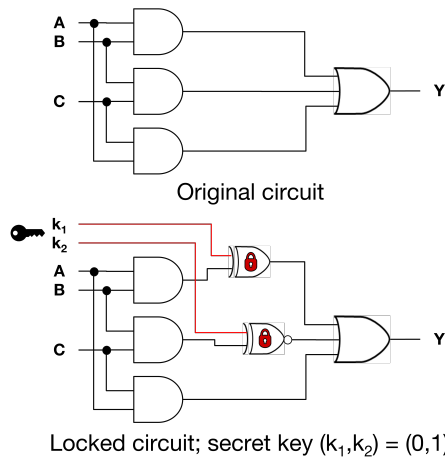


FIGURE 2 – Exemple de verrouillage logique (*logic locking*).

2 Objectif

L'objectif du projet est de sécuriser un CI en utilisant une technique de verrouillage pour le protéger contre le piratage.

3 Description du projet

Le CI à verrouiller est un modem WiFi implémenté en VHDL pour la radio logicielle (Software Defined Radio) bladeRF[2]. Les tâches à réaliser sont :

- Étudier le modem WiFi.
- Identifier le(s) bloc(s) IP à verrouiller.
- Implémenter une technique de verrouillage.
- Démontrer l'efficacité du verrouillage.

3.1 Connaissances Requises

- Intérêt pour le traitement du signal, la sécurité du matériel et l'implémentation matérielle (VHDL).

3.2 Outils Utilisés

- Software : Intel Quartus Prime.
- Hardware : Software Defined Radio bladeRF.

3.3 Nombre d'étudiants

- 2 étudiantes / étudiants.

3.4 Démonstration

Le modem Wi-Fi peut être configuré comme un point d'accès mobile permettant aux dispositifs mobiles de se connecter au modem. Il est donc possible de faire une démonstration de l'efficacité du verrouillage à l'aide de smartphones.

Références

- [1] A. Chakraborty, N. G. Jayasankaran, Y. Liu, J. Rajendran, O. Sinanoglu, A. Srivastava, Y. Xie, M. Yasin, and M. Zuzak, "Keynote : A disquisition on logic locking," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 10, pp. 1952–1972, 2019.
- [2] Nuand, "Open-source ieee 802.11 compatible software defined radio vhdl modem (bladerf-wiphy)," <https://github.com/Nuand/bladeRF-wiphy/>, online.