Multi-Objective Optimised Synthesis to Improve Cybersecurity
MOOSIC

Appel : AAP générique

Année : 2018

Instrument : PRCE

Contact : roselyne.chotin@lip6.fr

COORDINATEUR : Roselyne CHOTIN, LIP6

PARTENAIRES :
CEA Tech, LIP6, LIRMM, Secure-IC

Résumé :
Le projet MOOSIC vise à intégrer la sécurité vis à vis d'entreprises tierces non dignes de confiance, dans le flot de conception des circuits intégrés lors de l'étape de synthèse. Des techniques de verrouillage logique qui garantissent les performances sont ainsi proposées, dans le but de garantir l'intégrité du circuit.

CONTEXTE ET OBJECTIFS

Afin de réduire les coûts de mise sur le marché, les entreprises de conception de circuits intégrés ont de plus en plus recours à des entreprises tierces. Ceci fait qu'elles perdent de plus en plus le contrôle de leur chaîne de fabrication (Fig.1) et sont sujettes à des menaces telles que la **surproduction** ou l'insertion de **chevaux de Troie matériels, composants malicieux** introduits à leurs dépends afin de compromettre le fonctionnement du circuit. Notre but est donc de proposer des méthodes **garantissant la sécurité et s'insérant dans le flot de conception** traditionnel. Nous proposons ainsi d'explorer des méthodes de verrouillage logique rendant un circuit impropre à l'usage tant qu'il n'est pas déverrouillé par son concepteur après fabrication. L'**insertion automatique** des mécanismes de verrouillages lors de la conception, l'**évaluation** de ces mécanismes tant en termes de protection de la conception qu'en termes de résistance aux attaques et d'**impact sur les performances** sont autant de points explorés dans le projet MOOSIC.

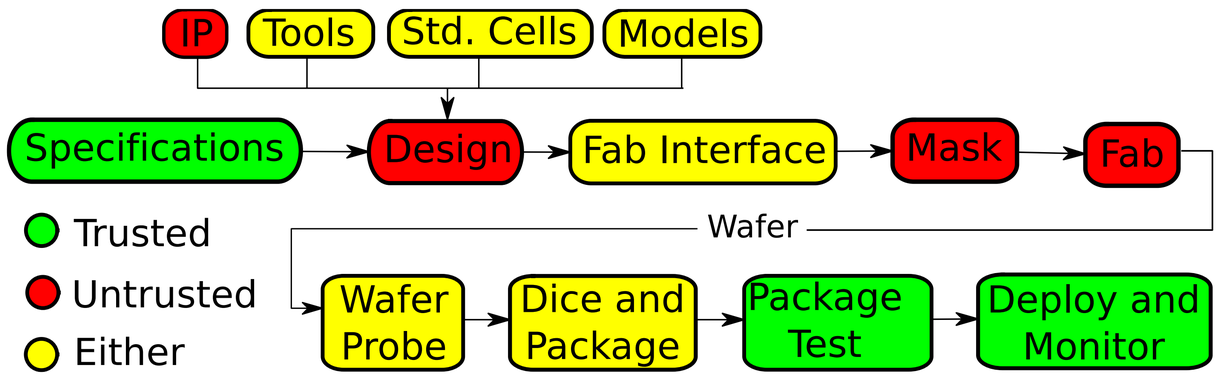

Fig.1 : Chaîne de production des circuits intégrés (Mentor)

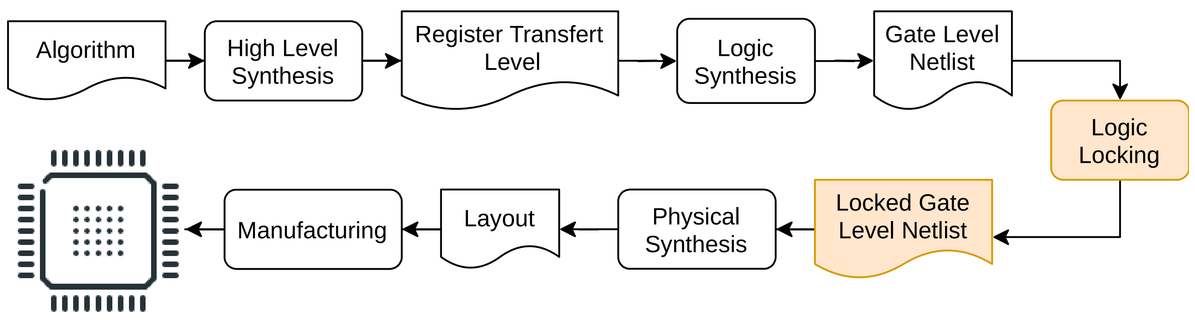

Fig.2 : Le verrouillage logique dans le llot de conception traditionnel

MÉTHODOLOGIE ET RÉSULTATS

Méthodologie :
Le verrouillage logique s'insère dans le flot de conception traditionnel au moment de l'étape de synthèse (Fig.2).Il consiste à verrouiller au moyen de portes clés qui seront activées au moyen d'une clé. Dans le cadre du projet MOOSIC, nous proposons :

1. Un modèle mathématique permettant de déterminer la meilleure localisation possible des portes clés,
2. Une approche heuristique permettant l'insertion de ces portes clés en un temps raisonnable,
3. Une évaluation de techniques de verrouillage vis-à-vis des attaques SAT,
4. Une méthode de protection du verrouillage logique contre les attaques SAT
5. Une évaluation des différentes techniques sur des circuits académiques et industriels

Résultats majeurs du projet :

1. Les résultats montrent une amélioration de la sécurité et une bonne résistance aux attaques SAT,
2. Les différentes techniques proposées ont été intégrées dans le flot de conception traditionnel, notamment au sein de la plateforme Coriolis développée au LIP6

Diffusion :

- Ces résultats ont été publiés dans des conférences internationales par les différents partenaires,
- Un article de revue a été soumis avec l'ensemble des partenaires,
- Au sein de la plateforme libre Coriolis du LIP6

Perspectives :
Les résultats seront valorisés au sein du CEA et de Secure-IC afin d'accroître leurs parts de marché, notamment l'intégration dans l'outil Virtualyzr de Secure-IC.
La diffusion sous forme de logiciel et matériel libre des résultats permettra d'accroître la visibilité et l'impact du projet dans la communauté des concepteurs de circuits.