Test Circuits Sécurisés 1

Bruno Rouzeyre, Marie-Lise Flottes

CONVENTION UM2-ST : 530S

RAPPORT D'AVANCEMENT DE PREMIERE ANNEE

Références

CONVENTION CIFRE N° 550/2002

Travaux effectués par David Hély

Sujet de recherche : Mise place de techniques de « Design For Test » et d'une stratégie spécifiques aux circuits sécurisés que sont les circuits pour « cartes à puces ».

Laboratoire

LIRMM
161, Rue Ada
34392 Montpellier Cedex

Entreprise

STMicroelectronics
ZI Rousset
13106 Rousset

Correspondant :

Frédéric BANCEL

La convention a débuté le 1er Janvier 2003, elle implique la division smartcard de STMicroélectronics et le LIRMM. Les travaux sont réalisés au sein des locaux de STMicroelectronics sur le site de Rousset (Bouches du Rhône).

L'objectif général de cette thèse consiste à définir des notions de testabilité ainsi qu'une stratégie de test prenant en compte la spécificité des circuits sécurisés.
Les règles de testabilité utilisées dans les circuits intégrés, qui ne sont pas destinés à des applications nécessitant un degré de sécurité important vis à vis des fraudeurs, sont souvent incompatibles avec les exigences sécuritaires. Dans ce contexte le but fixé lors de la première année de thèse était :

- inventorier les principales solutions de test,
- inventorier les problèmes à résoudre,
- proposition de solutions.
-

Concernant l'inventaire des principales solutions de test, il a été fait suivant plusieurs axes :

- solutions destinées aux blocs constitués de portes logiques (de type scan et logic BIST).
- solutions destinées aux blocs mémoires
- solutions systèmes, appropriées aux circuits complets (intégrant une partie logiques, des mémoires et des blocs analogiques).

Parallèlement à cette étude une analyse de vulnérabilité de ces solutions fut menée. Il s'agissait de définir les « faiblesses » de ces solutions déjà existantes vis à vis de la sécurité.
Ces analyses sont réalisées suivant un schéma et des règles publiées dans [1]. Dans notre cas il a été ainsi possible de quantifier le degré de résistance de certaines des techniques de test ou certaines des règles de conception pour la testabilité vis à vis d'attaques susceptibles d'être utilisées pour tenter une fraude sur un circuit sécurisé.

A la fin de cette étape nous avons obtenu une vision globale des « défauts » des principaux concepts d'amélioration de la testabilité en regard de la sécurité.

L'étape suivante a été menée en s'appuyant sur les constatations obtenues dans l'étape précédente. Elle a consisté à inventorier les problèmes à résoudre en analysant en détail le contenu des circuits ST et les mécanismes sécuritaires, déjà implémentés, qui seraient affectés par l'introduction de méthode de conception pour le test.
L'étude s'est concentrée durant cette première année sur la partie logique.

Notre stratégie, dans la recherche de solutions, s'est orientée vers une adaptation aux circuits sécurisés, de solutions de test déjà existantes. Nous avons opté pour une utilisation d'un large éventail de techniques déjà éprouvées plutôt que de travailler à la définition d'un concept prenant en compte des règles d'amélioration de la testabilité novatrice, et qui soient intrinsèquement adaptées à la sécurité.
Le travail a porté sur la technique du scan, qui dans son utilisation classique permet d'améliorer considérablement la testabilité mais qui aussi réduit de façon notable la sécurité.
Nous avons définit des règles visant à combler le déficit sécuritaire sans toutefois altérer sa valeur ajoutée au niveau de la testabilité.

Cet ensemble de règles permet d'atteindre un niveau de résistance élevée aux attaques suivant la méthode citée ci-dessus.

Ces travaux ont fait l'objet d'une proposition d'article dans une conférence internationale.

Les résultats ont aussi été implantés dans un prototype afin d'être évalués sur le silicium. Dans cette phase d'implantation, David Hély a participé au travail de conception par l'application des résultats théoriques obtenus et leur adaptation aux contraintes d'architecture de design et de flot de conception.

Le retour de la fabrication de ces prototypes est planifié pour le mois de mai.

La collaboration entre STMicroelectronics et le LIRMM s'est traduite par de fréquentes réunions de travail. Elle a permis de définir les meilleures stratégies de conception pour améliorer la testabilité à adapter aux circuits ST, ainsi qu'à définir les améliorations sur le plan sécuritaire.

Au cours de la deuxième année, le travail de recherche consistera à définir des règles de sécurité pour d'autres techniques adaptées à la structure des circuits STM.

[1] "Application of Attack Potential to Smartcards". document confidentiel