Test Circuits Sécurisés 2

Bruno Rouzeyre, Marie-Lise Flottes

CONVENTION UM2-ST : 530S

RAPPORT D'AVANCEMENT DE DEUXIEME 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

Aux cours des douze derniers mois, les travaux de recherche ont porté principalement sur deux techniques de test: le « scan path » et le « LogicBIST ».

Concernant la technique du scan, la première année de thèse avait permis de définir les principales failles sécuritaires induites par une telle technique. L'étude approfondie de ces failles sécuritaires nous a permis d'imaginer des contre-mesures rendant la technique du scan appropriée aux circuits sécurisés. Ces contre-mesures peuvent être envisagées à différents niveaux du système de scan; soit en modifiant le protocole de test; soit en modifiant l'implémentation physique de la chaîne de scan.

Une première réflexion a donc été menée afin de modifier le protocole de test. Un protocole dit sécurisé a été défini, puis implémenté sur un prototype. Ce protocole consiste en une adaptation du protocole JTAG aux contraintes sécuritaires. Le prototype embarquant cette solution permet désormais de valider le système de test sécurisé embarqué suivant deux points de vue:

- le gain en testabilité
- la résistance sécuritaire du système de test.

Des manipulations sur testeurs sont en cours afin de valider le système de test mais aussi de stresser ce système afin de mettre en évidence sa robustesse contre les attaques définies dans la première partie de la thèse. Le système de test embarqué sur ce prototype a fait l'objet de deux demandes de brevet et une publication soumise à un symposium.

Dans le même temps la sécurisation de le chaîne de scan proprement dite a fait l'objet de divers travaux permettant l'élaboration d'une solution engendrant la modification de la conception scan traditionnelle de telle sorte que l'analyse des données contenues dans la chaine est difficilement réalisable par des fraudeurs. Cette solution, le « scrambling de chaîne de scan » a fait l'objet d'une publication [1] et d'une demande de brevet. La validation de cette solution est actuellement en cours, celle-ci est réalisée via simulation. Cette validation consiste à mesurer l'efficacité de la solution face à une attaque sur les chaînes de scan décrites dans [2]. De plus cette validation a pour but de mesurer l'impact de la solution sur la surface, la consommation, la complexité du design supplémentaire. et de définir un compromis entre tous ces paramètres et le niveau de sécurité atteint. Une publication sur ce thème [3] a été soumise à l'European Test Symposium 2005.

La technique du LogicBist est basée sur la technique du scan, la différence réside dans le fait que les vecteurs de test et la réponse du circuit sont traités en interne sur la puce. Une étude sécuritaire de cette technique a été menée, s'appuyant largement sur celle effectuée pour la technique du scan. En respectant les contraintes sécuritaires, les travaux sur cette technique ont pour but de définir et implémenter une architecture LogicBist s'adaptant aux mieux aux spécificités des circuits type carte à puce. Une caractéristique de ces circuits est leur très faible surface, ainsi l'architecture proposée doit être optimale afin de minimiser l'impact en surface. Une partie importante d'une structure Logic Bist concerne la génération des vecteurs de test, plusieurs solutions sont envisagées pour réaliser cette fonction en réutilisant des parties fonctionnelles du circuit qui serait reconfigurée en générateur de vecteur en mode de test. Notamment, une étude actuelle a pour but d'étudier l'efficacité des crypto-processeurs reconfigurés en générateur de vecteurs.

References

[1] D. Hély, M-L. Flottes, F. Bancel, B. Rouzeyre, M. Renovell, N. Bérard, “SCAN Design and Secure Chip” International On-Line Test Symposium (IOLTS), Funchal, July 12-14, 2004, pp 219-224.

[2] B. Yang, K. Wu, R. Karri, Polytechnic University, "Scan-based Side-Channel Attack on Dedicated Hardware Implementations od Data Encryption Standard", Proc. ITC 2004.

[3] David Hély, Marie-Lise Flottes, Frédéric Bancel, Bruno Rouzeyre, "Test Control for Secure Scan Designs", soumis à European Test Symposium 2005