Sécurisation des structures de test : étude comparative

Mathieu da Silva, Marie-Lise Flottes, Giorgio Di Natale, Bruno Rouzeyre

Sécurisation des structures de test : étude comparative

Mathieu Da Silva, Marie-Lise Flottes, Giorgio Di Natale, Bruno Rouzeyre
LIRMM (Université de Montpellier/CNRS)
161 rue Ada, Montpellier, France
{mathieu.da-silva,flottes,dinatale,rouzeyre}@lirmm.fr

Abstract

Les chaînes de scan rendent possible le test et le debug des circuits intégrés en offrant contrôlabilité et observabilité des états internes du circuit. Cependant, leur implantation ainsi que celles des mécanismes d'utilisation de ces structures peut compromettre la sécurité des données. Les attaques par chaîne de scan permettent notamment de voler des secrets liés à la clé secrète d'un crypto-processeur en observant les étapes intermédiaires d'encryption. Plusieurs contremesures existent pour protéger les circuits. Certaines d'entre elles consistent à utiliser un mécanisme de verrouillage avec protocole d'identification. D'autres limitent l'accès en contrôle et en observation au cours du test. Le but de ce papier est de comparer les différentes techniques au niveau de leurs coûts en surface, en temps de test, en consommation, et sur leur capacité de debug et de diagnostics.

Mots-clés *: Test et Sécurité ; Contremesure contre les attaques par chaîne de scan ; Méthode de test sécurisée*

1. Introduction

Le test est une étape importante dans la production des circuits intégrés (CIs). Il permet d'identifier les circuits exempts de défauts de fabrication et participe donc à la définition d'un haut niveau de qualité et de fiabilité.

Le meilleur moyen de tester les CIs est l'ajout de structures de test en phase de conception. Parmi les méthodes de conception en vue du test (Design-for-Test,ou DfT), la mise en œuvre de chaînes de scan reste le moyen le plus efficace. La méthode est parfaitement automatisable et apporte un moyen de contrôle et d'observation de tous les états du CIs à moindre coût. L'insertion de chaînes de scan permet de différencier deux modes de fonctionnement. En mode fonctionnel (mode originel), les bascules du circuit mémorisent les états successifs du CIs. En mode test, les bascules sont reliées les unes aux autres et forment un registre à décalage dont l'entrée et la sortie sont respectivement contrôlable et observable à partir des entrées/sorties du circuit. Il est alors possible de contrôler et d'observer chaque bascule par décalages successifs.

Un utilisateur mal intentionné peut utiliser ces mêmes mécanismes pour contrôler/observer les données manipulées par le dispositif. Dans le cas d'un crypto-processeur, il est possible d'observer le résultat d'encryption après une ronde et ainsi récupérer des informations sur la clé secrète [1] [2]. La procédure consiste à exécuter le circuit en mode fonctionnel jusqu'à mémorisation d'un état intermédiaire d'encryption, puis de déclencher le décalage série de la chaîne de scan pour observer cet état intermédiaire et en déduire la clé. La chaîne de scan permet aussi d'initier l'attaque en contrôlant les entrées du crypto-processeur à des valeurs connues.

D'autres attaques sont possibles en utilisant des méthodes de probing. Grâce à une sonde, l'attaquant est capable de décaler en série le contenu de registres ciblés. Elles sont cependant difficiles à mettre en œuvre, il est nécessaire d'identifier les signaux sur le circuit où l'on souhaite insérer une sonde. Ces attaques sont très coûteuses et ne seront pas considérées par la suite. Seules les contremesures contre les attaques par canaux cachés basés sur les chaînes de scan seront étudiées.

Ce papier présentera dans la section suivante une étude comparative de 6 contremesures vis-à-vis de leur coût en surface, en temps de test, en consommation et sur leur capacité de debug et diagnostic.

2. Analyse comparative

Plusieurs contremesures ont été proposées pour limiter le contrôle et l'observation offerts par la chaîne de scan [3][4][5][6][7][8]. Cette liste n'est pas exhaustive mais représente différentes catégories de contremesure.

Une technique [3] consiste à modifier dynamiquement l'ordre de propagation série des bascules dans la chaîne de scan lorsque le circuit est en mode fonctionnel. Le déclenchement d'un décalage série dans ce mode ne permet donc pas d'analyser l'état mémorisé puisque l'ordre des bits observé est aléatoire. En mode test, le circuit attaqué est supposé utiliser une autre clef d'encryption. Tout attaque en mode test ne pourra donc révéler que la clé de test. Cette contremesure qui n'impacte pas les activités de tests, n'empêche ni diagnostic ni debug. Elle engendre néanmoins un coût en surface additionnel de 156% par rapport au contrôleur de test sans sécurité. La méthode demande l'ajout d'un générateur de nombre aléatoire ainsi que l'ajout de multiplexeurs devant les bascules. Durant le mode fonctionnel, les multiplexeurs commutent à chaque modification de l'ordre des bascules entrainant une consommation supplémentaire de 7% dans le cas de 6

segments sur une longueur totale de chaîne de scan de 198 bascules.

La solution proposée en [4] consiste à intégrer un comparateur chargé de comparer in-situ les réponses de test obtenues avec celles attendues. Seul le résultat de la comparaison finale est observable, rendant les activés de diagnostic et de debug plus difficile à réaliser. Cette contremesure appliquée à un circuit avec 32 chaînes de scan de 10 000 bascules représente un coût supplémentaire de 32 bascules, 98 portes, 64 buffers et un compteur 14-bits. Le temps de test n'est pas impacté puisque les réponses attendues sont comparées au moment où la réponse est reçue par le comparateur. Il est cependant nécessaire de tester le comparateur lui-même par une séquence particulière appliquée directement à ces entrées primaires. Ce test est réalisé en 60 006 coûts d'horloge sur des longueurs de chaîne de scan de 10 000 bascules.

Concernant les tests de type Built-In Self-Test (BIST) [5], alternative au test externe par chaîne de scan, suppriment totalement les accès en contrôle et en observation au cours du test. Seul le déclenchement de la procédure et la signature finale, OK/KO, sont accessibles à l'utilisateur. Cette approche peut toutefois impacter la qualité du test (compromis temps de test/taux de couverture) et rend le diagnostic impossible. Tout déclenchement intempestif d'un décalage série de la chaîne de scan en mode fonctionnel ne permettra pas d'observer les réponses du circuit puisqu'aucun mécanisme ne permet de les propager jusqu'à une sortie observable. Implanté sur un AES, le coût en surface est de 3.31% comparé à l'AES original.

L'approche proposée en [6] consiste en la mise en œuvre d'un mécanisme de verrouillage avec protocole d'identification. Elle vise à sécuriser les moyens d'accès aux chaînes de scan de cœurs au sein de systèmes sur puce. Elle protège donc de l'utilisation frauduleuse des modes test ou de debug en les restreignant aux seuls utilisateurs autorisés. Une fois l'utilisateur authentifié, celui-ci a accès à toutes les fonctionnalités de debug et de diagnostic. Cette méthode nécessite toutefois une gestion des clés d'accès. L'utilisation de cette solution sur un crypto-processeur AES implique un coût en surface de 5.2%. Le temps de test est impacté seulement au début de la procédure de test. Il faut 256 coups d'horloge pour authentifier l'utilisateur.

La contremesure décrite dans [7] prévient le contrôle frauduleux de l'infrastructure JTAG par un chiffrement par flux des données de test. Trois niveaux de sécurité sont proposés assurant l'authenticité du circuit, la confidentialité des données transmises et l'intégrité de celles-ci. Pour initialiser la communication sécurisée entre le testeur et le circuit, l'utilisateur envoie un challenge au circuit dont sa réponse sera utilisée comme clé de chiffrement. Toutes les données de test envoyées et reçues par le testeur seront par la suite encryptées avec le secret partagé. En plus de l'encryption, une fonction de hachage est implantée permettant de vérifier que les données n'ont pas été altérées par un device dans la chaîne JTAG. Cette solution entraîne un coût en surface de 9% par rapport à un circuit utilisant 10 000 slices d'un FPGA Xilinx Spartan 3. La contremesure implique un coût en temps de test initial de 2464 cycles d'horloge correspondant à la phase d'initialisation de l'encryption. Chaque vecteur de test entraîne en plus un coût en temps additionnel pour la génération du Message Authentication Code (MAC).

Une nouvelle proposition de contremesure [8] consiste à encrypter par blocs toute donnée de contrôle ou d'observation d'une chaîne de scan. Pour encrypter le canal de test, deux étages de chiffrements par bloc sont insérés respectivement en entrée et en sortie de la chaîne de scan. Les patterns générés pour tester le circuit original sont dans un premier temps encryptés puis stockés dans le testeur. Lorsqu'ils sont appliqués en entrée de la chaîne de scan, ils sont alors décryptés in-situ avant d'être appliqués au circuit original. De même chaque réponse à un vecteur de test est d'abord encryptée avant d'être délivrée en sortie de chaîne de scan pour comparaison. Cette contremesure conserve les capacités de debug et de diagnostic. Pour un crypto-processeur AES 128 bits pipeline, la solution entraîne un coût en surface de 3.26%. Le temps de test est quant à lui impacté de 0.8% par rapport au temps de test du circuit original.

3. Conclusion

Les attaques par chaîne de scan permettent de voler les secrets d'un circuit. Plusieurs contremesures ont été présentées, chacune présentant un compromis entre différents coûts : surface, temps de test, consommation, capacité de diagnostic et de debug.

Références

[1] Bo Yang, Kaijie Wu, and Ramesh Karri. Scan Based Side Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard. In ITC, pp 339-344. IEEE, 2004.

[2] Jean DaRolt, Giorgio Di Natale, Marie-Lise Flottes, and Bruno Rouzeyre. Scan Attacks and Countermeasures in Presence of Scan Response Compactors. In European Test Symposium, pp 19-24. IEEE Computer Society, 2011.

[3] D. Hely, M.-L. Flottes, F. Bancel, B. Rouzeyere, N. Bernard, Scan design and secure chip. In Proc. IEEE Int. On-Line Test. Symp., pp. 219-224, 2004.

[4] Da Rolt J.; Di Natale G.; Flottes M.-L.; Rouzeyre B. Thwarting Scan-Based Attacks on Secure-ICs With On-Chip Comparison. In Proc. IEEE Trans. on Very Large Scale Integration (VLSI) System, no. 22 pp. 947-951, 2013.

[5] M. Doulcier, M.-L. Flottes, B. Rouzeyre. AES-based BIST: Self-test, Test Pattern Generation and Signature Analysis. In 4th IEEE International Symposium on Electronic Design, Test & Applications, Hong-Kong, IEEE, pp.314-321, 2008

[6] Chiu G.-M.; Li J.; C.-M. A Secure Test Wrapper Design Against Internal and Boundary Scan Attacks for Embedded Cores, IEEE Trans. on Very Large Scale Integration (VLSI) System, vol 20, issue 1, p 126-134, 2010

[7] Kurt Rosenfeld, Ramesh Karri, "Attacks and Defenses for JTAG", IEEE Design & Test of Computers, vol.27, no. 1, pp. 36-47, January/February 2010, doi:10.1109/MDT.2010.9

[8] Mathieu Da Silva, Marie-Lise Flottes, Giorgio Di Natale, Bruno Rouzeyre, Marco Restifo, Paolo Prinetto. Scan Chain Encryption for the Test, Diagnosis and Debug of Secure Circuits. 22nd IEEE European Test Symposium (ETS'17) [accepted for publication]