Sécurité et intégrité dans un Contexte Embarqué

Sébastien Lapeyre, Nicolas Valette, Marc Merandat, Marie-Lise Flottes, Bruno Rouzeyre, Arnaud Virazel

Sécurité et intégrité dans un Contexte Embarqué

S. Lapeyre N. Valette M. Merandat
INVIA
Meyreuil, France
{firstname.lastname}@invia.fr

M.-L. Flottes B. Rouzeyre A. Virazel
LIRMM - Université de Montpellier / CNRS
Montpellier, France
{firstname.lastname}@lirmm.fr

***Abstract*—Lors du design d'un circuit intégré, il est nécessaire d'implémenter des fonctionnalités complémentaires de tests et sécuritaires pour assurer la qualité, la fiabilité et la sécurité. Nos travaux ont pour optique d'être implémentés dans des systèmes embarqués avec comme forte contrainte d'être le plus petit possible en termes de surface utilisée. Dans ce papier nous présentons une solution de test pour des capteurs analogiques à vocation sécuritaire, ainsi qu'une méthode d'authentification permettant de protéger l'accès à une infrastructure de test, le JTAG.**

***Keywords*—Sureté, Sécurité, Capteurs Analogues, tests, Autotests, JTAG, authentification défi-réponse, cryptographie légère**

I. INTRODUCTION

Les circuits intégrés sont devenus au fil des années des systèmes essentiels à notre société. Avec comme conséquence une attente de fiabilité, qualité et sécurité dont doit s'assurer le concepteur et fabricant du produit.

Les systèmes embarqués sont un parfait exemple de cette observation. Ils sont de nos jours utilisés dans de multiple domaines tels que l'automobile, la santé, la robotique, les technologie mobiles … En corrélation avec ce phénomène, leur complexité a augmenté avec des circuits comportant une logique de plus en plus complexe et des technologies de gravure de plus en plus fine. Pour assurer la qualité et la fiabilité de ces circuits, les protocoles de tests post-fabrication plus complets ont dû être développés et intégrés.

En parallèle, ces systèmes deviennent une cible privilégiée des attaquants. Avec un faible investissement, le nombre de victimes potentielles peut être très grand [1]. Il est de la responsabilité des concepteurs de proposer des solutions sécurisées.

Une part des circuits intégrés doit être conçus pour permettre la réalisation de tests de bas niveau et assurer la sécurité des données critiques. En considérant ces deux besoins, on s'aperçoit qu'ils ne peuvent être traités de manières dissociées. Il faut pouvoir tester la sécurité et sécuriser les solutions de test.

Dans le cas des systèmes embarqués, et particulièrement des objets connectés, s'ajoute à cette problématique des contraintes de coût de mise en œuvre de la sécurité et du test (surface, consommation, performances temporelles)

Nos travaux ont eu pour objectifs de :

- Proposer des solutions de tests d'un système embarqué à vocation sécuritaire ;
- Proposer une solution de contrôle d'accès sécurisé d'une infrastructure de test ;
- Présenter des solutions à faible coût pouvant être implémentés dans des circuits fortement contraints.

Dans les sections suivantes, nous présentons dans un premier temps une solution de test pour capteurs analogiques souvent présents dans les systèmes intégrés pour assurer la sécurité des données manipulées. Le cas d'étude présenté ici s'appuie sur un capteur de température typiquement embarqué dans des produits de type carte à puce. Ce capteur est chargé de monitorer les conditions environnementales d'utilisation du système afin de prévenir des attaques matérielles. Puis, nous décrirons notre solution d'authentification défi-réponse (challenge/response) avec un cœur cryptographique léger permettant le contrôle d'accès au JTAG [3] et ainsi prévenir l'utilisation frauduleuse des infrastructures intégrées de test.

II. TEST POUR LA SECURITE

A. Contexte

Les circuits intégrés sont la cible d'attaques physiques tel que les attaques par laser, par électromagnétisme, par augmentation de la température, etc. Pour détecter ces attaques, les circuits embarquent des IP analogiques en charge de lever une alarme lorsque les conditions environnementales dévient de l'attendu [4]. Dans le cas des attaques en température, un capteur vérifie que la température se situe dans une plage autorisée. Cette fonction sécuritaire doit être disponible tout au long du cycle de vie du produit. Des procédures de test externe et interne sont donc nécessaires pour vérifier le bon fonctionnement du capteur chaque fois que nécessaire.

B. Solution de test

Dans un premier temps, nous avons augmenté l'observabilité et la contrôlabilité de la structure du capteur de température étudié. Multiplexeur, transistor de bypass et commandes digitales (*pmos_en*, *tog_en* et *mux_en*) permettent de contrôler sa configuration et d'observer les signaux produits (Figure 1). Les résultats des tests sont observés sur un bus digital *res*. Les temps d'observation des réponses de test sont dépendants du type de capteur sous test.

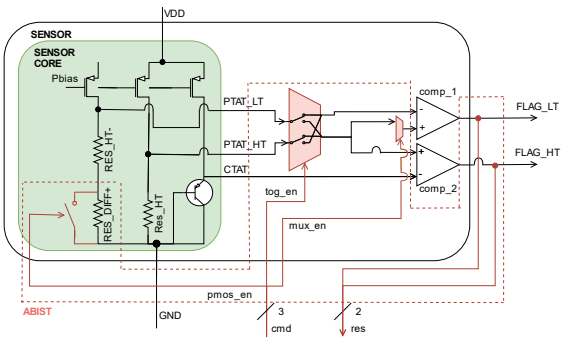

Figure 1: Insertion de test dans un capteur de température

Grâce à l'ajout de ces fonctionnalités de test, il est possible de vérifier que les tensions de référence sont correctement polarisées, que les comparateurs ne sont pas collés à 1 ou 0 et que le réseau de résistance a été correctement implanté.

Un contrôleur digital permet de réaliser des tests tout au long du cycle de vie, notamment un test externe à l'aide du

standard IEEE 1149 et des autotests internes par CPU. Son architecture générique permet une modularité importante dans son implémentation. Selon les besoins de test, le nombre de bits de commandes/résultats peut être adapté. La surface du contrôleur digital ainsi que les temps d'exécution de test externe (post-fabrication) et interne (sur le terrain) sont indiqués dans le Tableau 1.

		Pour 1 capteur température*
Surface	665+55*(len(cmd))+27*len(res) GE	866 GE
Temps test externe	$T_{tck} \times (len(TDI) + 2 \times len(TDR)) + \max(t_d; 2 \times T_{tck})$	3,1 µs
Temps test interne	$42 \times T_{sck} + t_d$	2,42 µs

* : T_{tck}= 10MHz (période horloge externe) ; T_{sck} = 100MHz ; t_d = 2µs ;
len(TDR) = 3 (longueur Test Data Register) ; len(TDI) = 5 (longueur Test Data Input)
TDI et TDR sont des outils proposés par le standard JTAG

Tableau 1: Résultat de surface et de temps d'exécution

III. SECURISATION DU TEST

Le standard JTAG est une infrastructure de test largement répandue qui est également utilisée pour reprogrammer des puces. Ces deux fonctions peuvent être la cible d'attaquant ayant comme objectif d'observer ou de contrôler des systèmes à des fins malicieuses. Pour cela l'attaquant utilise les canaux séries du JTAG pour récupérer des informations sensibles ou introduire des données erronées. Pour se prémunir de ce type d'attaque, nous avons concentré nos travaux sur le contrôle d'accès à ces canaux séries à l'aide d'un protocole d'authentification.

A. Protocole d'authentification

Nous avons choisi d'utiliser un protocole d'authentification symétrique permettant de s'assurer que le testeur connait la clé secrète partagée en amont. Ce protocole est basé sur la méthode défi-réponse. Cette méthode permet d'éviter le rejoue de l'authentification dans le cas où un attaquant a été en mesure d'enregistrer une authentification correcte (attaque man-in-the-middle). Un hash cryptographique permet de ne pas échanger la clé en clair.

Nous nous sommes concentrés sur des solutions de hash cryptographique légères tout en considérant le niveau de sécurité. Ces solutions légères reçoivent un intérêt grandissant récent, dû au marché des objets connectés, avec des processus de standardisation en cours. A notre connaissance, aucun processus d'authentification pour le JTAG n'utilise ces outils cryptographiques. Leur utilisation nous permet de réduire significativement les coûts de mise en œuvre.

B. IP d'authentification JTAG

L'architecture de notre système d'authentification est présentée en Figure 3.

La génération d'un nombre aléatoire et d'une clé nécessaire au défi-réponse (nonce-data) sont externe à l'IP d'authentification, qui est chargée de :

- Réaliser la communication aux travers du JTAG (à l'aide du TAP et du TDR) ;
- Réaliser le calcul de la réponse attendue au défi (grâce au CRYPTO_WRAPPER) ;
- D'attester que l'authentification s'est correctement déroulée (avec le signal auth_ok)

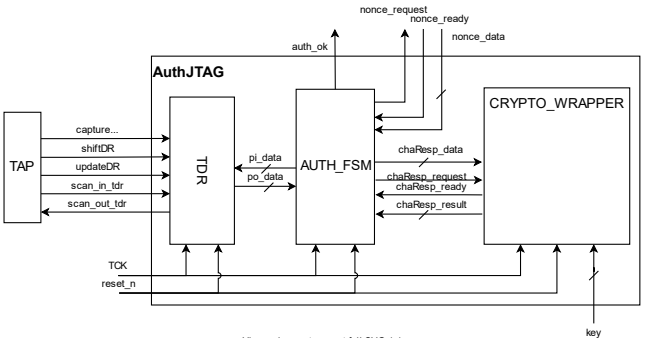

Figure 2: Architecture IP authentification

C. Résultats

Plusieurs solutions de hash ont été explorées. Le Tableau 2 présente les résultats obtenus à partir de deux solutions de hash légères, SPONGENT [5] et ASCON [6] et du hash standardisé SHA3 [7] aujourd'hui largement utilisé dans l'industrie. La solution ASCON montre de bons résultats en termes de sécurité avec une complexité pour les attaques de pré(seconde)-image et de collisions de 128 et un bon compromis surface/temps d'exécution.

Hash	Propriétés de sécurité		Porte (CMOS 55nm)	Temps d'exécution
	Collision	*Pré & Seconde image*		
Spongent 256/256/128	128	128	8005	353 cycle
SHA3 256/512/1088	128	256	27109	28 cycle
ASCON 256/256/64	128	128	8543	63 cycle

Tableau 2: Résultat d'implémentation

IV. CONCLUSION

Il est essentiel de s'assurer du bon fonctionnement de l'ensemble d'un système intégré après fabrication et durant son cycle de vie, particulièrement lorsqu'il doit assurer en plus de sa fonction, la sécurité numérique des données manipulées. Dans cette étude, nous avons traité le cas particulier du test d'éléments critiques intégrés pour prévenir des attaques matérielles (capteur analogique). Nous avons aussi présenté une infrastructure de test permettant de sécuriser son utilisation, la rendant ainsi uniquement disponible aux utilisateurs légaux. L'ensemble des solutions proposées est compatible avec le standard IEEE 1149.1.

REFERENCES

[1] Antonakakis, Manos, et al. "Understanding the mirai botnet." *26th {USENIX} security symposium ({USENIX} Security 17)*. 2017

[2] S. Lapeyre, N Valette, M. Merandat, M-L. Flottes, B. Rouzeyre, A. Virazel, "A Plug and Play Digital ABIST Controller for Analog Sensors in Secure Devices", Manuscript submited for validation.

[3] "IEEE Standard 1149.1: Standard Test Access Port and Boundary Scan", 1990

[4] NIST 2001. FIPS 140-2, "Security Requirements for Cryptographic Modules", Washington, US Government Printing OfficeQsd.

[5] Bogdanov, Andrey, et al. "SPONGENT: A lightweight hash function." International workshop on cryptographic hardware and embedded systems. Springer, Berlin, Heidelberg, 2011.

[6] Dobraunig, Christoph, et al. "Ascon v1. 2. Submission to NIST, 2019."

[7] Dworkin, Morris J. "SHA-3 standard: Permutation-based hash and extendable-output functions." (2015)