Scan Chain Encryption

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

Scan Chain Encryption

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

***Abstract*—Crypto-processors are the target of attacks. For instance, an attacker may exploit facilities offered by scan chains to retrieve embedded secret data closely related to the key. However, scan design is the most popular and efficient method to test circuit. The goal of the technique proposed here is to preserve test efficiency, diagnostic and debug while counteracting security threats. This solution relies on using the secret key already stored in the circuit under test in order to encrypt test patterns by adding extra blocks ciphers. Both control and observed test data are thus unusable without the knowledge of the key.**

Keywords—Test and Security; Scan Attacks Countermeasure; Light Encryption

Manufacturing test is the process to sort fault-free from faulty circuits. It guarantees a high level of quality and reliability of integrated circuits (IC). A design approach called Design-for-Testability (DfT) aims to improve circuit testability. The most popular DfT method relies on scan design, which consists in replacing original FFs by so-called "scan FFs" organized in shift-registers during the test phase. Serial input/output provide a mechanism for controlling and observing internal states at test time. However, an attacker can use observability and controllability offered by scan registers to leak secret on the circuit, typically by observing intermediate states. Especially, crypto-processors are targets of scan attacks [1][2]. The attacks relies on the capability of shifting out scan chain's content while registers state are correlated with the secret key. The attacker is thus able to identify the key.

Several countermeasures have been proposed in the literature [3][4][5][6][7][8] to counteract scan attack. Each countermeasure has an impact on testability: test time, fault coverage and the facilities to diagnosis and debug. Applying those securing techniques has also a cost in terms of area and power consumption and can impact the DfT flow. A tradeoff between these aspects has to be chosen for the designer of secure circuits.

We propose here a new countermeasure [8] that consists in encrypting scan chain content of circuits embedding at least one crypto-core. Assuming a key management policy for the embedded crypto-processor, the secret key for scan chain encryption is stored in the same tamper-resistant memory with the management policy already implemented. Light block ciphers are added in input scan chain and output scan chain (Fig. 1). The procedure consists in encrypting test patterns off-chip, and then scanned them in the circuit to be decrypted by implemented block cipher. The next step is collecting test responses. Before test responses are shifted out, these ones are encrypted by another on-chip block cipher. Eventually, encrypted test responses are decrypted off-chip to be compared with expected ones.

Without the knowledge of the key, an attacker can not perform scan attacks. Decryption in input scan chain prevents control-based scan attacks; encryption in output scan chain prevents observation-based scan attacks. This solution keeps test, diagnosis and debug facilities. A developer wishing to debug an application can thus read and write on the registers of the processor. Nevertheless, this protection has a cost in term of area and test time. Applying the solution on a pipelined AES core, the area overhead related to the proposed secure scan infrastructure is of 2.92%. The test time is increased by 0.8% in relation to original test time. This experimental results showed a marginal impact on both area and test time.

REFERENCES

[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]

FIGURE

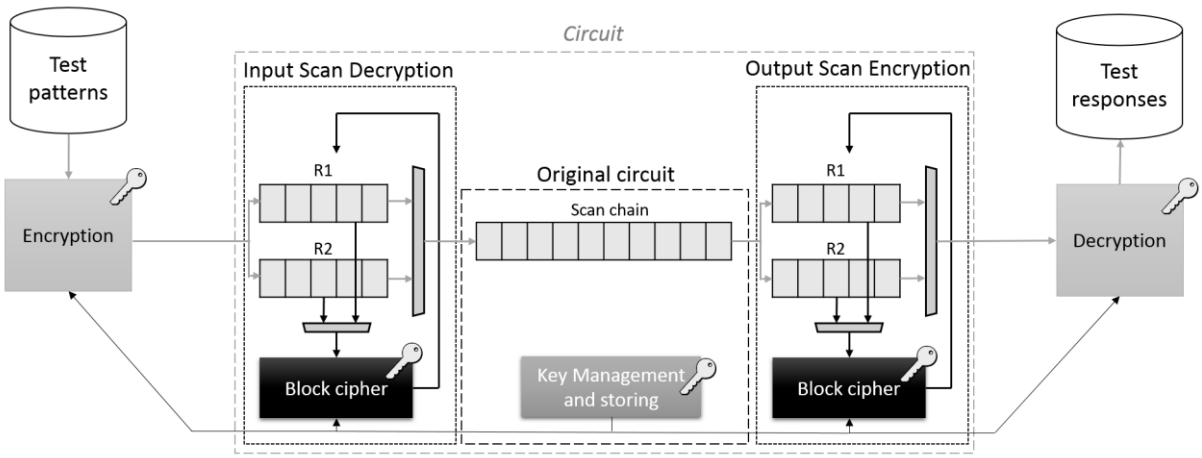

Fig. 1. Scan chain encryption implementation