STSM Report – Hierarchical Secure DFT

REFERENCE: Short Term Scientific Mission, COST Action IC1204
Beneficiary: Mafalda Cortez, TU Delft, a.m.m.o.cortez@tudelft.nl
Host: Giorgio Di Natale, LIRMM, giorgio.dinatale@lirmm.fr
Period: from 1/09/14 to 15/12/14
Place: LIRMM, Montpellier, France
Reference code: C0ST-STSM-IC1204-20741

1. Purpose of the visit

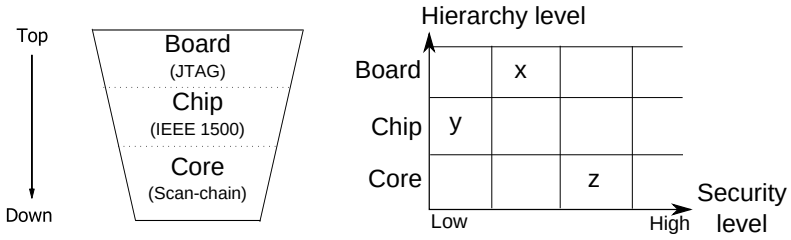
The Computer Engineering Lab, TU Delft, together with LIRMM, have initiated a collaboration more than one year ago. From this collaboration, a master student was graduated (master thesis entitled “Design for Testability for Secure ICs”), one paper was published at DATE’14 (Testing PUF-based Secure Key Storage Circuits) and a journal article at JETTA, volume 30, issue 5, 2014 (Testing Methods for PUF-Based Secure Key Storage Circuits). Common interests include hardware security and trust and design, test and reliability of secure devices.

The visit was part of the activities of WG1 (manufacturing test of secure devices). The topic we investigated was on the development of new secure DFT architectures. In more detail, we focused on methods to exponentially increase the attack time via authentication key introduced in the scan-chain, making the attack less attractive to the attacker. This visit resulted in two publications.

2. Description of the work carried out

Nowadays, most Integrated Circuits (ICs) integrate crypto cores to provide secure data storage and transfer. Testing ICs is essential to identify faulty devices. Design-for-Testability (DFT) structures are added to enhance testability; i.e., realize high fault coverage and respective diagnosis. The most used DFT structures are scan-chains, which allow shifting-in test vectors and shifting-out test responses to and from storage elements. These structures increase the observability and controllability of IC internal nodes, by enabling easy accessibility to internal states. Moreover, scan-chains facilitate the generation of test vectors. However, scan-chains open a back door that malicious users can exploit to gain access to sensitive information; these attacks are known as scan-based attacks [1–7]. Scan-based attacks typically aim at retrieving the secret encryption key of secure devices by using the scan-chains to shift out the information stored in the flip-flops (FF).

Several countermeasures against scan-based attacks have been proposed in literature [7–21]. These countermeasures can be divided into scan control methods [7–10], unauthorized scan-shift detection methods [7,9,11–16] and data confusion methods [17–21]. Scan control methods involve power-off or reset of scan FF when switching from mission to test mode; unauthorized scan-shift methods involve reset scan FF when an unauthorized shift is detected, and they include scan pattern watermarking [7,9,11–13], scan-enable tree monitoring [14] and spy FF [15–17]; while data confusion methods provide confusion on the stream shifted out of the scan-chain by shuffling the output according to a specific function. Although different solutions have been provided, industry is still very reluctant to deploying them as they believe that the provided level of security is not strong enough [22]; all these DFT solutions are based on the manipulation of scan-chains and therefore are obscure solutions [23]; note that the security countermeasures in [7–21] takes place at core level only. Moreover, the solutions do not provide enough flexibility to tune the level of security as different secure applications may need different level of security.



(a) Design/ DFT hierarchy (b) Hierarchical levels vs. Security levels

Fig. 1: Integrating security features at each DFT level

Fig. 1 (a) illustrates our view about a generic, hierarchical and flexible secure DFT for digital ICs. The solution should enable the integration of secure features within DFT infrastructure at each design level in a top-down design fashion including board level, (supported by JTAG), chip level (supported by IEEE 1500) and core level (supported by scan design). In addition, at each hierarchical level, different security features with different severity levels can be integrated; e.g., Fig. 1(b) shows that at each hierarchical level we can have different level of security ranging from low to high. This flexibility is important as it can allow for the combination of the appropriate security features and therefore the optimization of the secure DFT solutions depending on the targeted application. As Fig. 1 shows, a solution at scan chain level (e.g. z) can be combined with a solution at the chip level, with higher or lower security level (e.g. y), or even with another solution at board level (e.g., x), as that proposed in [24], in order to provide an optimal solution for the overall security level of the system.

In the rest of this work we focus only on the discussion of the solution at the core level; we introduce and design the solution, referred to as Multi-Level Secure Scan (MLSS) Test, that fits within the generic and hierarchical secure DFT approach shown in Fig. 1. MLSS test is flexible as it enables different levels of security, and it is not an obscure solution since it uses secret keys to be enable scan test rather than just manipulating the scan chains (as it is the case for prior work). These two properties make the solution fit within the visioned generic, hierarchical and flexible secure DFT for digital ICs. MLSS solution is secure against brute force attacks and has an inherent low area overhead and no impact on the circuit performance.

3. Description of the main results obtained

To evaluate the effectiveness of our method we implement the system depicted in Fig. 2.

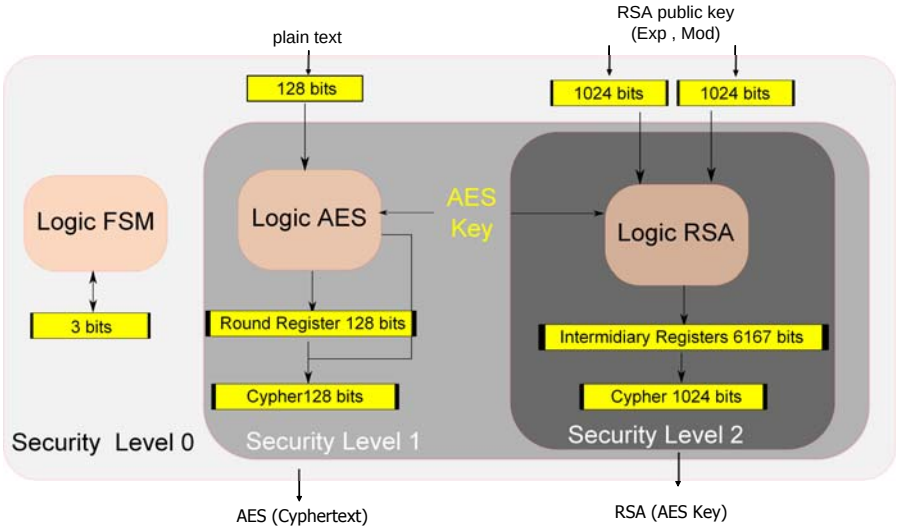


Fig. 2: Case study

The system comprises an AES crypto core, a RSA crypto core and a FSM. Consider the following scenario where a server and a client want to securely exchange data. The server generates a RSA key (i.e., a public and a private key), handing the public key to the client. The client encrypts (a) the data with its own AES key and (b) the used AES key with the public RSA key received by the server. The client sends to server the AES encrypted data and the RSA encrypted AES key. The server decrypts client data by decrypting the clients AES key using its RSA private key. The sensitive information in our circuit, i.e., the data we want to protect, is the AES key and the RSA private key. We divide our system into three hierarchical levels with three levels of security. As the leakage of RSA private key would also compromise the AES key, we define the access to RSA as the top level (most secure). Middle level grants access to AES. Finally, at down level (with no secure FFs) is the FSM, which any user can access. We synthesize the client circuitry in VHDL in 0.35µm technology node from AMS with Synopsys Design Compiler. From the netlist of the circuit we determine the logic output cones of each FF. This information allows identifying FFs that might not be suitable to integrate the Scan-Chain Secure Segment (SCSS). Furthermore, we develop a tool that given a netlist and a technology node library outputs a new netlist including the following five additions. (1) Two new ports to enable classic scan test (scan enable and scan-in). (2) Either a new MUX (scan MUX) or two new MUXes (scan MUX and secure MUX) prior to each unsecured or secured FF, respectively. (3) Connect the FFs in a scan-chain. (4) Insert Alternative Source (AS) and connect them to each SMUX input. (5) Insert LOCK (finite state machine, or FSM, which enables the security) per SCSS.

We implement the circuitry in Fig. 2 with the following parameters.

- Key length to unlock AES secure segment: 128 bits (taken from registers with security level 0, i.e, FSM, AES plain text and RSA public key).
- Key length to unlock RSA secure segment: 128 bits (taken from registers with security level 0 and 1, i.e, in addition to the registers listed before, round and cypher register from AES).
- 10 ASs of 16 bits each (5 ASs connected to AES segment and 5 ASs connected to RSA segment).

We extract the area overhead of our solution. Note that we do not perform fault simulation as the results would be equivalent to that of a classic scan-chain. As mentioned before, the combinational logic of the LOCK FSM can be easily tested functionally by inserting the correct key into the SCSS.

Results

Table 1: Area results

	#FF	#Combinational	# additional gates
FSM	3	24	75
AES	387	143	364
RSA	9239	2078	63

Our case study has no logic dependency issues. Table I shows the number of FFs and combinational logic elements each segment comprises and the number of gates added by implementing our method; e.g., FSM comprises 3 FFs, 24 logic gates and an additional 75 gates. The last row indicates the additional cost of implementing our solution. Our solution has an area overhead of 502 gates, i.e., 4% when compared against the area overhead of the original circuit. Analyzing the relative impact, our method increases significantly the area overhead of the FSM, as the FSM as a inherent low area overhead. This area corresponds to the AS. The relative impact on the AES area overhead is significant. This is mainly due to the

FSM counter to flush the entire scan chain. The larger the scan chain, the larger the counter. Finally, RSA has low area overhead as it comprises mainly a small FSM (not that the LOCK FSM is smaller than the LOCK FSM for the AES, as no flushing is required).

4. Projected publications/articles resulting or to result from the STSM

- Towards a Generic and Hierarchical Secure DFT for Digital ICs – submitted to European Test Symposium 2015 (ETS'15)
- Generic and Hierarchical Secure DFT for Digital ICs - Extension of the ETS'15 work to be submitted as a journal (on going work)

5. References

[1] S. Hamdioui *et al.* , "Hacking and protecting IC hardware", *DATE*, pp.1-7,2014
[2] Y. Liu, K. Wu, and R. Karri, "Scan-based Attacks on Linear Feedback Shift Register Based Stream Ciphers", *ACM Trans. on Design Automation of Electronic Systems (TODAES)*, vol. 16, no. 2, Mar 2011.
[3] R. Nara *et al.* , "Scan-Based Side-Channel Attack against RSA Cryptosystems Using Scan Signatures", *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E93-A, no.12, pp. 2481-2489, 2010.
[4] R. Nara *et al.* , "Scan-based Attack Against Elliptic Curve Cryptosystems", *ASP-DAC*, pp. 407 - 412, 2010.
[5] J. Darolt *et al.* , "Are advanced DfT structures sufficient for preventing scan-attacks?", *VLSI Test Symposium*, pp. 246 - 251, 2012.
[6] B. Yang, K. Wu, and R. Karri, "Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard",
International Test Conference, pp. 339 - 344, 2004.
[7] B. Yang, K. Wu, and R. Karri, "Secure Scan: A Design-for-Test Architecture for Crypto Chips", *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, vol.25, no. 10, pp. 2287 - 2293, 2006.
[8] A. Das and ¨Unal Kocabas¸ and Ahmad-Reza Sadeghi and Ingrid Verbauwhede, "PUF-based Secure Test Wrapper Design for Cryptographic SoC Testing", Design, Automation and Test in Europe, 2012
[9] D. Hely, F. Bancel, M.-L. Flottes, B. Rouzeyre, "Securing Scan Control in Crypto Chips", *JETTA*, 23, 5, pp. 457-464, 2007
[10] J. Darolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "Thwarting Scan-based Attacks on Secure-ICs with on-chip comparison", *IEEE Trans. on VLSI Systems*, 2013
[11] D. Hely et al., "Scan Pattern Watermarking, *LATW*, 2006
[12] J. Lee, M. Tebranipoor, and J. Plusquellic, "A low-cost solution for protecting IPs against scan-based side-channel attacks", *Proc. VTS*, pp.93-99, 2006.
[13] S. Paul, R.S. Chakraborty, S. Bhunia, "VIm-Scan: A Low Overhead Scan Design Approach for Protection of Secret Key in Scan-Based Secure Chips", *Proc. VTS*, pp.455-460, 2007.
[14] D. Hely, F. Bancel, M.-L. Flottes, B. Rouzeyre, "Test Control for Secure Scan Designs", *Proc. ETS*, pp. 190-195, 2005.
[15] D. Hely, "Testability of Secure ICs", *PhD report University of Montpellier 2*, 2005
[16] D. Hely, F. Bancel, M.-L. Flottes and B. Rouzeyre, "A secure Scan Design Methodology", Design, Automation and Test in Europe, 2006.
[17] G. Sengar, D. Mukhopadhyay, and D.R. Chowdhury, "Secured Flipped Scan-Chain Model for Crypto-Architecture", *IEEE Trans. on CAD*, vol. 26, no.11, pp.2080-2084, Nov. 2007.
[18] D. Mukhopadhyay *et al.* "CryptoScan: A Secured Scan Chain Architecture", *Proc. 14th ATS*, pp. 348-353, 2005.
[19] D. Hely *et al.* ,"Scan design and secure chip [secure IC testing]", *Proc. IOLTS*, pp. 219-224, 2004.
[20] J. Lee, M. Tehranipoor, C. Patel, and J. Plusquellic, "Securing Designs against Scan-Based Side-Channel Attacks", *IEEE Trans. on Dependable and Secure Computing*, vol.4, no.4, pp.325-336, 2007.
[21] J. Lee, M. Tehranipoor, C. Patel and J. Plusquellic, "Securing Scan Design Using Lock and Key Technique", *IEEE Int. Symp. on Defect*
and Fault Tolerance in VLSI System, 2005
[22] M. Cortez *et al.* , "Testing Methods for PUF-Based Secure Key Storage Circuits", *JETTA*, vol. 30, no. 5, 2014
[23] J.J. Stapleton, "Security without Obscurity: A Guide to Confidentiality, Authentication, and Integrity", *Auerbach Publications*, 2014
[24] A. Zygmontowicz, J. Dworak, A. Crouch, and J. Potter, "Making it harder to unlock an LSIB: Honeytraps and misdirection in a P1687
network", *DATE*, pp.1 - 6, 2014
[25] J. Darolt, G Di Natale, M.-L. Flottes and B. Rouzeyre, "New security threats against chips containing scan chain structure", *IEEE Int. Symp. on Hardware-Oriented Security and Trust*, 2012
[26] Application of Attack Potential to Smart-Card, Common Criteria, "www.commoncriteriaportal.org"