COST Office
Avenue Louise 149
1050 Brussels, Belgium
t: +32 (0)2 533 3800
f: +32 (0)2 533 3890
office@cost.eu

www.cost.eu

Subject | Working Group Report of the COST Action IC1204 "Trustworthy Manufacturing and Utilization of Secure Devices"

Working Group 1: Manufacturing test of secure devices
WG Leaders: Marie-lise Flottes (LIRMM), Said Hamdioui (Delft U. of Technology)

1. Executive summary

Participation in the organization of the following events:
- First Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (May 30th-31st, 2013, Avignon, France)
- MC/WG meeting (Dec.12-13, 2014, Freiburg, Germany)
- TRUDEVICE workshop on Test and Fault Tolerance for Secure Devices, Joint Working Group Meeting WG1-WG3 (May 29-30, 2014, Paderborn, Germany)
- TRUDEVICE TRAINING school (July 14-18, 2014, Lisbon, Portugal)

Collaboration set-ups

2. Description and objectives of the Working Group

1. Tools and methodologies to improve test production coverage for secure functions

Classical techniques for digital circuit testing cannot be easily used for testing of secure devices. They are based on Design-for-testability techniques that add hardware components to the circuit, aiming to provide full controllability and observability of the internal states. Because crypto-processors and other cores in a secure system must pass through high-quality test procedures to ensure that data are correctly processed, testing of crypto chips faces a dilemma. Design-for-testability schemes require high controllability and observability of the device while security necessitates minimal controllability and observability in order to better hide the secret information. Developing innovative design-for-testability techniques and test methods becomes therefore a fundamental task for manufacturing high quality secure devices.

2. Secure protocols and controllers to protect the access to necessary test infrastructures

Typical test access points are inputs and outputs of scan chains, JTAG (Joint Test Action Group) port and other mechanisms. Reinforcing the protection based on the differentiation of the test mode from the user mode is the proposed approach in the academic world. Its integration in real secure devices is still an

issue. Therefore, new secure test protocols based on the use of enhanced test controllers must be investigated. Moreover, access strategies might change during the lifetime of the device and this must be taken into account.

3. Extending security for IEEE system-level test standards

Test standards like IEEE 1149 and IEEE 1500 do not explicitly take into account security issues. One important aspect of this Action is the opportunity of joining the knowledge of academic and industrial researchers to integrate security in current standards.

In addition to these test-related WG1activities, test basics (testability analysis, Design-For-Testability, test application procedures, fault simulation, fault diagnosis...) are at the heart of other activities in other Working Groups WGx (attacks/countermeasures/tools/trojan-injection/trojan-detection) because test infrastructure or test-related activities/knowledge are used for the implementation/validation of these activities.

Please also fill the following table (only lines concerning your WG) :

Objective as described in MoU	Current Level of Achievement in % [1]				
	0	25	50	75	100
1) T*o identify new design and manufacturing flows for the production of secure integrated circuits by creating a strong network between several centers of expertise on hardware security at European level.*	□	X	□	□	□
2) *To provide solutions for required but conflicting relationships between Testability and Security*	□	□	X	□	□
3) To develop innovative design-for-testability Computer-Aided Design (CAD) tools for supporting security issues and with a specific attention to compliance with existing commercial tools	X	□	□	□	□
4) To define secure protocols to protect the access to necessary test infrastructures and to design secure access controllers	□	□	X	□	□
5) To contribute in the definition of new test standards that intrinsically include security issues	X	□	□	□	□
6) To study new mechanisms for devices identification and authentication based on the usage of Physically Unclonable Functions (PUFs) and True Random Number Generators (TRNGs)	□	X	□	□	□
7) To address issues related to counterfeiting and Hardware Trojan insertion and to propose new methods and algorithms for their identification	□	X	□	□	□
8) To define new architectures able to detect faults and to resist to fault attacks	□	□	X	□	□
9) To establish a design and synthesis flow, which will transform a given circuit into a secure design incorporating counter-measures against fault attacks	□	X	□	□	□
10) To explore implementation and security issues of cryptographic logic based on Field-Programmable Gate Array (FPGA)	□	X	□	□	□
11) To collect statistically significant data related to fault injection campaigns	X	□	□	□	□
12) To explore formal verification methods to establish the robustness of a secure device against fault attacks	X	□	□	□	□
13) To aid towards the development of early-stage faculty researchers into	□	X	□	□	□

[1] Give an approximate estimation in percentage on the current level of achievement of each of the Action Objectives by clicking on the empty boxes. Update at the beginning of each Work & Budget Plan negotiation

experts in their respective fields, and improve the knowledge and skills of Ph. D. students and post-doctoral fellows, which will enable them to perform high-quality research					
14) To support mobility between participating research centers, both of senior researchers to foster exchange of ideas through short term visits, and of junior researchers/PhD students to enable the exchange of technical knowledge through longer term visits	□	X	□	□	□
15) To promote dissemination activities by joint papers in international journals and conference proceedings, and through the organization of special sessions at international conferences.	□	X	□	□	□

3. Participants

List of members and involved people

Members:	Marie-Lise FLOTTES (Chair)
	Said HAMDIOUI (Chair)
	Nicolas Sklavos
	Lejla Batina
	Nele Mentens
	David Hély
	Bruno Rouzeyre
	Francesco Regazzoni
	Viacheslav Izosimov
	Urban Ingelsson
	Salvador Manich
	Giorgio Di Natale
	Paul Henri Pugliesi Conti
	Ilia Polian
	Ingrid Verbauwhede
	David Hernandez
Others:	*(Involved in other WG but interested by activities in WG1)*
	Lilian Bossuet
	Bernd Becker
	Paris Kitsos
	Osnat Keren
	Julien Francq
	Assia Tria
	Guy Gogniat
	Carles Ferrer
	Pedro Peris-Lopez
	Philippe Loubet Moundi
	Geert-Jan Schrijen
	Vincent van der Leest
	Milos Drutarovsky

	Viktor FISCHER
	Tim Güneysu
	Franck Courbon
	Róbert Lórencz

Statistics: (Members)

Total number of members[2]	Number from Inclusiveness Countries	From Industry	From international cooperation institutions	Number of ESRs	Gender balance (men/ women)
16	16	4	0	5	12/4

4. Activities and Results

Delft Uni. Of Technology (NL) and LIRMM (Fr) developed two secure build-in-self-test methods for Physical Unclonable Function (PUF) based systems. The methods target high stuck-at-fault (SAF) coverage by performing scan-chain free functional testing, to prevent scan-chain abuse for attacks. The first test method reuses existing blocks of the PUF based system to generate the test vectors and to compress the test result (pass/fail) to minimize the area overhead. The second test method tests all block simultaneously with dedicated random test pattern generators for both test and compression to minimize the test time.
The methods are integrated in PUF based system design and simulated; the results show that for the first test method, a SAF fault coverage of 95% can be realized with no more than 47.1k clock cycles at the cost of a negligible area overhead of only 2.2%; while for the second test method a SAF fault coverage of 95% can be realized with 3.5k clock cycles at the cost of 18.6% area overhead [1-3].

Univ. Politècnica di Catalonya (SP) and Technische Universität München (GE) worked on test infrastructures (scan designs). Up to now no security is embedded in the standard and therefore several ad-hoc solutions are used which present more or less limitations. In [4] and [5] a technique is invented that protect the internal state of the chip from being fully revealed while the scan-path is shifted out.

Univ. Politècnica di Catalonya and Technische Universität München also worked on reverse engineering techniques are the most powerful techniques that allow the tampering of chips. Inside this group, the probe attacks can effectively extract data traveling inside busses. A minimal intrusive probe is placed in contact with a specific line of the chip and the traffic is investigated. Also, these probes can be used to modify the state of certain control lines. The probe attacks is an expensive but every effective means for counteracting many scan protections which only rely on few signals. In [6] a detector that reacts when a physical contact is realized in a given line is presented.

Two extra activities from the same groups in order to counteract non-intrusive (cold boot) and intrusive (backside polishing and imaging) attacks: Cold boot attacks have been demonstrated in the literature as a mean to remove information from memory in either PCs or mobile phones. The principle uses the retention memory effect that makes data not to disappear completely after a power shut-down, at least for a certain amount of time. This effect can be even enhanced if the memory is cooled down. Critical memories like cache, where no latency is accepted, do not accept encryption methods being applied as a means for protecting data. However, stream cyphers based on the scrambling concept can be used since

[2] Estimated number (update at the beginning of each Work & Budget Plan negotiation); those that are a member of more than one WG must be counted in each WG.

their latency is minimal. In [7] this technique is presented that also decreases the power consumption if compared to classical scrambling techniques.
In literature it has been shown that chips can be polished from the backside to a certain degree where FIB edition can open direct access to transistors. Also in this situation, infrared emission coming from transistors in saturation allows to do map imaging and to detect certain areas of interests. Despite so far no attacks have demonstrated in practice this possibility, it has been clearly pointed out. In [8] the design principle of a detector has been presented that generates an alarm when material from the backside of the chip is removed.

ENSMSE (Fr), TIMA (Fr) and LIRMM (Fr), studied concurrent error detection and recovering mechanisms based on BBICS (Built-In Bulk Induced Current Sensors). Bulk Built-In Current Sensors (BBICSs) are able to detect anomalous transient currents induced in the bulk of integrated circuits when hit by ionizing particles. Original strategies to design BBICSs with different constraints have been explored (optimal transient-fault detection sensitivity, low area and power overheads). Proposed approaches allow increasing the detection sensitivity (asymmetry in the flipping ability of the sensor's latch, delay tuning of the bulk access transistors). Several versions have been designed and implemented on silicon [9-11].

LIRMM (Fr) and K.U. Leuven (B) worked on scan attacks with the demonstration of new and generic attacks based on the information leaked from the test infrastructure (Scan designs). Resistant hardware implementations of private and public key cryptography were proposed in order to prevent scan-based attacks on crypto-cores. A secure implementation of the test standard JTAG 1149 has been developed based on the Schnoor protocol [12-19].

5. List of publications related to the Working Group

1. A.M.M.O. Cortez, G. Roelofs, S. Hamdioui, G. Di Natale, Testing Methods for PUF-Based Secure Key Storage Circuits (to appear: October 2014), Journal of Electronic Testing: Theory and Applications (JETTA) [Journal Paper]
2. A.M.M.O. Cortez, G. Roelofs, S. Hamdioui, G. Di Natale, Secure Test Method for Fuzzy Extractor (to appear: September 2014), Joint MEDIAN–TRUDEVICE Open Forum, 30 September 2014, Amsterdam, The Netherlands [Conference Paper]
3. A.M.M.O. Cortez, G. Roelofs, S. Hamdioui, G. Di Natale, Testing PUF-based Secure Key Storage Circuits (March 2014), Design, Automation & Test in Europe (DATE 2014), 24-28 March 2014, Dresden, Germany [Conference Paper]
4. S.Manich, Markus S.Wamser, Oscar M. Guillen, G. Sigl, "Differential Scan-Path: A Novel Solution for Secure Design for Testability", Trudevice workshop, May 2013
5. S. Manich, Markus S. Wamser, Oscar M. Guillen, G. Sigl, "Differential Scan Path: A Novel Solution for Secure Design for Testability", International Test Conference, September 2013
6. M. Weiner, S. Manich, G. Sigl, "A Low Area Probing Detector for Security ICs", Trudevice, May 2014
7. M. Neagu, L. Miclea, S. Manich, "Interleaved Scrambling Technique: A Novel Low-Power Security Layer for Cache Memories", European Test Symposium, May 2014
8. S. Manich, S. Arumi, R. Rodriguez, G. Sigl, J. Mujal, "Backside Polishing Detector", Trudevice 2013, December 2013
9. R. Possamai Bastos, G. Di Natale, M. Flottes, F. Lu, B. Rouzeyre, "A New Recovery Scheme against Short-to-Long Duration Transient Faults in Combinational Logic", Journal of Electronic Testing (JETTA), Springer, June 2013, Volume 29, Issue 3, pp 331-340, DOI: 10.1007/s10836-013-5359-y.
10. J.M. Dutertre, R. Possamai Bastos, O. Potin, M.L. Flottes, B. Rouzeyre, G. Di Natale "Sensitivity tuning of a bulk built-in current sensor for optimal transient-fault detection", Microelectronics Reliability, Volume 53, Issues 9–11, September–November 2013, Pages 1320-1324
11. Rodrigo Possamai Bastos, Frank Sill Torres*, Jean-Max Dutertre, Marie-Lise Flottes, Giorgio Di Natale, Bruno Rouzeyre, "A Bulk Built-in Sensor for Detection of Fault Attacks", IEEE

International Symposium on Hardware-Oriented Security and Trust (HOST'13), pp 51-54, ISBN: 978-1-4799-0559-1, DOI: 10.1109/HST.2013.6581565.

12. Jean Da Rolt, Amitabh Das, Santosh Ghosh, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rozeyre, Ingrid Verbauwhede "Scan attacks on side-channel and fault attack resistant public-key implementations", Journal Of Cryptographic Engineering (JCEN), Nov. 2012, Vol.2, Issue 4, pp 207-219, DOI: 10.1007/s13389-012-0045-z.
13. Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre "A Novel Differential Scan Attack on Advanced DFT Structures", ACM Transactions on Design Automation of Electronic Systems Volume 18 Issue 4, October 2013, Article No. 58, DOI: 10.1145/2505014.
14. Jean Da Rolt, Amitabh Das, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre, Ingrid Verbauwhede, "Test versus Security: Past and Present", Manuscript Type: SI:Emerging Nanoscale Architectures for Hardware Security, Trust, and Reliability, IEEE Transactions on Emerging Topics in Computing, March 2014 (vol. 2 no. 1), DOI 10.1109/TETC.2014.2304492
15. J. Da Rolt, G. Di Natale, M.-L. Flottes, B. Rouzeyre, "A Smart Test Controller for Scan Chains in Secure Circuits", IEEE International On-Line Testing Symposium 2013 (IOLTS,13), 8-10 July 2013, pp 228-229.
16. Jean Da Rolt, Amitabh Das, Giorgio Di Natale, Marie-Lise Flottes and Bruno Rouzeyre, Ingrid Verbauwhede, "A New Scan Attack on RSA in Presence of Industrial Countermeasures", Third International Workshop on Constructive Side-Channel Analysis and Secure Design, publication: Lecture Notes in Computer Science, Volume 7275, pp 89-104, 2012.
17. Jean Da Rolt, Amitabh Das, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre and Ingrid Verbauwhede, "A New Scan Attack on Elliptic Curve Cryptosystems in presence of Industrial Design for Testability Structures", IEEE International Symposium On Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT'12), 3-5 octobre 2012, USA, pp 43-48, DOI : 10.1109/DFT.2012.6378197.
18. Jean Da Rolt, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre, "On-Chip Test Comparison for Protecting Confidential Data in Secure ICs", IEEE European Test Symposium (ETS'12), 28 mai – 1er juin 2012, France, Interactive Presentation, DOI : 10.1109/ETS.2012.6233039.
19. A. Das, J. Da Rolt, S. Ghosh, S. Seys, S. Dupuis, G. Di Natale, M-L. Flottes, B. Rouzeyre, and I. Verbauwhede, "Secure JTAG Implementation using Schnorr Protocol", Journal of Electronic Testing: Theory & Applications (JETTA), Springer Science and Business Media New York 2013, Inc., vol. 29, no. 2, pp. 193-209, 2013, DOI: 10.1007/s10836-013-5369-9.