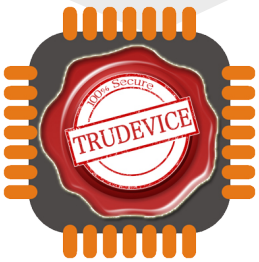

EUROPEAN COOPERATION
IN SCIENCE AND TECHNOLOGY

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 3: Fault attack detection and protection
WG Leaders: Bernd Becker, Bruno Rouzeyre

1. Executive summary

Participation in the organisation of the following events :
- First Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (May 30th-31st, 2013, Avignon (France)
- MC/WG meeting, December 12-13, 2014, Freiburg
- TRUDEVICE Workshop 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) Using redundancy to detect fault attacks
Redundancy methods have been proposed to detect errors in data processed by a device embedding secret information. Error detection exploits different forms of redundancy, namely temporal (i.e., calculating twice the same function and comparing the two results), hardware (where two devices are instanced for the same function) and information redundancies (that consists in checking for possible mismatches between a code predicted for an output from the current input, and the code of the actual output of the process). The action investigates design methods and synthesis flow to transform an unprotected circuit into a robust design protected by such techniques.
2) Cross-level optimizations on residual weak spots in the circuit
This activity provides methodologies for designing cost-efficient robust circuits that have limited energy budget and constraints on area overhead at the same time. The robustness is achieved by an efficient cross-level combination of redundancy techniques. Parts of the circuit will be protected by low-level hardening techniques such as transistor upsizing or gate duplication (hardware redundancy), while the residual circuitry is protected by advanced error-detecting codes (information redundancy). Related

selective hardening strategies have been applied in the past to protect circuits against random errors at low cost. Their application to security threats and the combination with information redundancy is a novel approach.

Objective as described in MoU	Current Level of Achievement in %[1]				
	0	25	50	75	100
1) To *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 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	□	□	X	□	□
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	□	□

[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

3. Participants

Chairs:	Bernd Becker
	Bruno Rouzeyre
Members:	
1	Nicolas Sklavos
2	Lilian Bossuet
3	Zebo Peng
4	Osnat Keren
5	Lejla Batina
6	Julien Francq
7	Assia Tria
8	Ilia Polian
9	Nele Mentens
10	David Hély
11	Said HAMDIOUI
12	Carles Ferrer
13	Philippe Loubet Moundi
14	Viktor FISCHER
15	Marie-Lise FLOTTES
16	Francesco Regazzoni
17	Paolo Maistri
18	Tim Güneysu
19	Franck Courbon
20	Róbert Lórencz
21	Viacheslav Izosimov
22	Urban Ingelsson
23	Jean-Max Dutertre
24	Linus Feiten
25	Ricardo Chaves
26	Noemie Boher
27	Apostolos Fournaris
28	Suleyman.Tosun
29	Giorgio Di Natale
30	Feng Lu

Statistics (number of people, ratio young/senior, gender balance, ratio academics/industrials)

Total number of members[2]	Number from Inclusiveness Countries	From Industry	From international cooperation institutions	Number of ESRs	Gender balance (men/ women)
32	12	5	0	5	26/6

[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.

4. Activities and Results

Faut injection in secure devices :
LIRMM and ENSMSE have experienced laser attacks against secure circuits in different technologies (from 130nm downto 28nm) in order to assess the actual efficiency of such attacks and to derive electrical and behavioral models of such laser effects on silicon. According to these models LIRMM has developed a laser fault simulator geared toward designers for testing countermeasures prior to actual IC fabrication. LIRMM has also developed specific countermeasures against laser attacks [1-11]. ENSMSE, LIRMM and TIMA have deeply improved tat ability of current sensors for detecting laser attacks.

TIMA designed countermeasure against [Electromagnetic] side channel analysis for the Advanced Encryption Standard [26-27]. In relation with LIRMM, ENSMSE and LCIS, TIMA defined a design methodology for early evaluation of laser [21, 25, 32] and pulsed EM [22-24, 29, 31] fault injections. TIMA also designed cryptographic accelerator for scalar multiplication in elliptic curves protected against simple and differential side channel analysis [26, 30]. Besides RT level laser attack evaluation, LCIS also developed methodologies to analyze analog circuit sensitivity to fault attacks [37-39] and their effects on the whole circuit for mixed-signal ones.

Code based fault detection :
Prof Kerens team together with Prof Polian's research team have developed, implementd and tested a new family of security oriented codes was developed, implemented and tested [14,20] as countermeasures against fault injection attacks. The major degradation in the efficiency of robust codes observed when the codes were not uniformly distributed was studied[6]. Encoding techniques that strengthen the codes against such scenarios were introduced [13,18].

Countermeasures against fault/delay injection attacks on GALS: The performance of conventional unordered codes for asynchronous communication channels under delay injection attacks was evaluated [12]. A code that can correct any maliciously distorted data with zero error was developed.

Countermeasures against DPA attacks: Two new technologies of logic gates that flatten the power profile (and hence are immune to DPA attacks) was introduced [16,17].

Impact of fault attack countermeasures :
Prof Z. Peng's team have been working on design and optimization techniques of embedded systems for security-critical applications. In particular they address the problems related to real-time constraints and secure communications, such as AES encryption on messages. Since AES is known to be vulnerable to differential power analysis (DPA) attacks, they have recently developed a scheduling-based countermeasure to find the most robust solution against DPA attacks while satisfying real-time constraints. They have cooperated with Radboud University Nijmegen (Prof. Lejla Batina) on this research issue. ref 33-35

IC sensitivity to fault attacks :
We investigated the possibility of predicting, at design time which parts of the chip are more likely to be sensitive to faults compliant with the fault models required to perform attacks against the AES cipher. Result of this work are reported in [24] and [36]

With respect to hardware security and fault attacks, the group of Bernd Becker (in cooperation with Ilia Polian's group) has been working on the formal analysis of circuits' vulnerabilities to malicious fault attacks [42,43,44]. The second area of activity consists of practical experiments examining the capabilities of Altera FPGAs to realise Ring-Oscillator Physically Unclonable Functions [40,41].

5. List of publications related to the Working Group

1. "FPGA Emulation of Laser Attacks Against Secure DeepSubmicronIntegrated Circuits" A. Papadimitriou , D. Hély, V. Beroulle, P. Maistri, R. Leveugle, LCIS and TIMA, Colloque GDR SOC-SIP 10-12 june 2013
2. "Multi-Level Laser-Induced Fault Simulation" Feng Lu, Colloque GDR SOC-SIP 10-12 june 2013
3. " tLIFTING: an Open-Source Multi-Level Fault Simulator for Ionizing Effects" Feng Lu, Giorgio Di Natale, Marie-Lise Flottes and Bruno Rouzeyre. Conférence PRIME 2013, 9th Conference on Ph. D. Research in Microelectronics and Electronics, Villach, Austria, June 24th-27th, 2013
4. "Laser-Induced Fault Simulation" Feng Lu, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre, conference DSD 2013, Santander, Spain, Sept. 4-6, 2013
5. "A New Recovery Scheme Against Short-to-Long Duration Transient Faults in Combinational Logic" Possamai Bastos R., Di Natale G., Flottes M.-L., Lu F., Rouzeyre B. Journal of Electronic Testing: Theory and Application (2013) 001-010
6. "Customized Cell Detector for Laser-Induced-Fault Detection", Feng LU (LIRMM - France), Giorgio DI NATALE (LIRMM - France), Marie-Lise FLOTTES (LIRMM - France), Bruno ROUZEYRE (LIRMM - France) IOLTS 2014
7. "A Multiple Fault Injection Methodology based on Cone Partitioning towards RTL Modeling of Laser Attacks", A. Papadimitriou, D. Hély, V. Beroulle, P. Maistri, R. Leveugle, Design, Automation and Test in Europe Conference (DATE), 2014
8. "On error models for RTL security evaluations", P. Vanhauwaert, P. Maistri, R. Leveugle, A. Papadimitriou, D. Hély, V. Beroulle, 9th International Conference on Design & Technology of Integrated Systems in Nanoscale Era" (DTIS), 2014
9. "Layout-Aware Laser Fault Injection Simulation and Modeling: from physical level to gate level", L. Feng, M.L. Flottes, B. Rouzeyre, G. Hubert, 9th International Conference on Design & Technology of Integrated Systems in Nanoscale Era" (DTIS), 2014
10. "Laser attacks on integrated circuits: from CMOS to FDSOI"J.-M. Dutertre, S. De Castro, A. Sarafianos, N. Boher, Ph. Candelier, J. Damiens, M.-L. Flottes, M. Lisart, G. Di Natale, B. Rouzeyre, 9th International Conference on Design & Technology of Integrated Systems in Nanoscale Era" (DTIS), 2014
11. FPGA Emulation of Laser Attacks Against Secure Deep Submicron Integrated Circuits A. Papadimitriou , D. Hély, V. Beroulle, P. Maistri, R. Leveugle, LCIS and TIMA, Colloque GDR SOC-SIP 10-12 juin 2013
12. A. Burg and O. Keren, "On the Efficiency of Berger Codes against Error Injection Attacks on Parallel Asynchronous Communication Channels", Information Security Journal: A Global Perspective. Special issue on Trustworthy Manufacturing and Utilization, Vol. 22, No. 5-6, pp. 208-215, 2013. Published on-line 2014.
13. I. Sumsky and O. Keren, " Enhancement of Hardware Security by Hamming Ball Based State Assignment", Information Security Journal: A Global Perspective. Special issue on Trustworthy Manufacturing and Utilization, Vol. 22, No. 5-6, pp. 208-215, 2013. Published on-line 2014.
14. Y. Neumeier, O. Keren, "Robust Generalized Punctured Cubic Codes", IEEE Trans. on Information theory, Vol. 60, No. 5, pp. 1-10, May 2014.

15. Moshe Avital, Hadar Dagan, Osnat Keren, and Alexander Fish, "Randomized Multi Topology Logic (RMTL) against Differential Power Analysis", IEEE TRANS. On Very Large Scale Integration (VLSI) Systems. (to appear 2014).
16. Hadar Dagan, Moshe Avital, Osnat Keren, and Alexander Fish, "DPA-Secured Quasi-Adiabatic Logic (SQAL) for Low-Power Passive RFID Tags", (submitted to TCAS-I , March 2014(
17. O. Keren and M. Karpovsky, "Relations between the Entropy of a Source and the Error Masking Probability for Security Oriented Codes", (submitted to IEEE trans. On Communications, April 2014)
18. I. Shumsky, O. Keren and M. Karpovsky, " Security-Oriented Encoding of Robust Codes for Non-Uniformly Distributed Words", (submitted to IEEE IT , July 2014)
19. Y. Neumeier, O. Keren, "A New Efficiency Criterion for Security Oriented Error Correcting Codes", *19th IEEE European Test Symposium,* Germany, May 2014.
20. Victor Tomashevich, Yaara Neumeier, Raghavan Kumar, Osnat Keren and Ilia Polian, "Protecting Cryptographic Hardware against Malicious Attacks by Nonlinear Robust Codes", *The IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT'14),* Amsterdam, 1-3 October 2014
21. Papadimitriou A., Hély D., Beroulle V., Maistri P., Leveugle R., A multiple fault injection methodology based on cone partitioning towards RTL modeling of laser attacks, Design, Automation and Test in Europe Conference (DATE), Dresden, Germany, 2014
22. Alberto D., Maistri P., Leveugle R., Electromagnetic attacks on embedded devices: a model of probe-circuit power coupling, 9th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS), Santorini, Greece, 2014
23. Alberto D., Maistri P., Leveugle R., Forecasting the effects of electromagnetic fault injections on embedded cryptosystems, Information Security Journal: A Global Perspective, , page: , 2014
24. Bhasin S., Maistri P., Regazzoni F., Malicious Wave: a Survey on Actively Tampering Using Electromagnetic Glitch, International Symposium on Electromagnetic Compatibility (EMC 2014), Raleigh Convention Center Raleigh, NC, USA, 2014
25. Vanhauwaert P., Maistri P., Leveugle R., Papadimitriou A., Hély D., Beroulle V., On error models for RTL security evaluations, 9th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS), Santorini, Greece, 2014
26. Pontié S., Maistri P., Randomized Windows for a Secure Crypto-Processor on Elliptic Curves, 25th IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP 2014), Zurich, Switzerland , 2014
27. Maistri P., Tiran S., Maurine P., Koren I., Leveugle R., An evaluation of an AES implementation protected against EM analysis, 23rd ACM international conference on Great lakes symposium on VLSI (GLSVLSI'13), Paris, France, 2013
28. Maistri P., Tiran S., Maurine P., Koren I., Leveugle R., Countermeasures against EM analysis for a secured FPGA-based AES implementation, International Conference on ReConFigurable Computing and FPGAs (ReConFig' 13), Cancun, Mexico, 2013
29. Alberto D., Maistri P., Leveugle R., Investigation of Electromagnetic Fault Injection Effects on Embedded Cryptosystems, First Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE'13), Avignon, France, 2013
30. Simon Pontié and Paolo Maistri. An Elliptic Curve Crypto-Processor Secured by Randomized Windows, DSD 2014, to appear.
31. Paolo Maistri, Regis Leveugle, Lilian Bossuet, Alain Aubert, Viktor Fischer, Bruno Robisson, Nicolas Moro, Philippe Maurine, Jean-Max Dutertre and Mathieu Lisart.

ElectroMagnetic Analysis and Fault Injection onto Secure Circuits, VLSI-SoC 2014, to appear.
32. R. Leveugle, P. Maistri, P. Vanhauwaert, F. Lu, G. Di Natale, M.-L. Flottes, B. Rouzeyre, A. Papadimitriou, D. Hély, V. Beroulle, G. Hubert, S. De Castro, J.-M. Dutertre, A. Sarafianos, N. Boher, M. Lisart, J. Damiens, P. Candelier, C. Tavernier. Laser-induced Fault Effects in Security-dedicated Circuits, VLSI-SoC 2014, to appear.
33. "Energy-Aware Design of Secure Multi-Mode Real-Time Embedded Systems with FPGA Co-Processors," by Ke Jiang, Adrian Lifa, Petru Eles, Zebo Peng, and Wei Jiang, Proceedings of 21st International Conference on Real-Time Networks and Systems (RTNS2013), Sophia Antipolis, France, October 16-18, 2013.
34. "Robustness Analysis of Real-Time Scheduling Against Differential Power Analysis Attacks", by Ke Jiang, Lejla Batina, Petru Eles, and Zebo Peng, Proceedings of IEEE Computer Society Annual Symposium on VLSI, Tampa, Florida, USA, July 9-11, 2014.
35. "Energy Aware Real-Time Scheduling Policy with Guaranteed Security Protection," by Wei Jiang, Ke Jiang, Xia Zhang, and Yue Ma, Proceedings of 19th Asia and South Pacific Design Automation Conference (ASPDAC2014), SunTec, Singapore, January 20-23, 2014.
36. Alessandro Barenghi, Cédric Hocquet, David Bol, Francois-Xavier Standaert, Francesco Regazzoni, and Israel Koren, "A Combined Design-Time/Test-Time Study of the Vulnerability of Sub-Threshold Devices to Low Voltage Fault Attacks", in IEEE Transactions on Emerging Topics in Computing.
37. "Increasing the security level of analog IPs by using a dedicated vulnerability analysis methodology", N. Boher, D. Hély, V. Beroulle, J. Damiens, P. Candelier, 14th International Symposium on Quality Electronic Design (ISQED), 2013 (ISQED 2013), pp 531-537, March 2013
38. "Evaluating and Enhancing the Security of Analog and Mixed IPs in Complex System On Chip", N. Beringuier Boher, D. Hely, V. Beroulle, K. Gomina, J. Damiens, P. Candelier, TRUDEVICE 2013, Avignon May 31st 2013
39. "Voltage Glitch attacks on Mixed-Signal Systems" Noemie Beringuier-Boher, Kamil Gomina, David Hely, Vincent Beroulle, Jean-Baptiste Rigaud, Assia Tria, Joel Damiens, Philippe Gendrier and Philippe Candelier in 7th Euromicro Conference on Digital Systems Design (DSD14) Verona, Italy, in August 27-29, 2014.
40. Feiten, Spilla, Sauer, Schubert, and Becker, 2014. Implementation and Analysis of Ring Oscillator PUFs on 60 nm Altera Cyclone FPGAs. In Information Security Journal: A Global Perspective, Volume: 22, Number: 5-6, pages: 265 – 273
41. Feiten, Spilla, Sauer, Schubert, and Becker, 2013. Analysis of Ring Oscillator PUFs on 60nm FPGAs. In Online-Proceedings of the 1st TRUDEVICE-Workshop, Avignon.
42. Feiten, Sauer, Schubert, Czutro, Böhl, Polian, and Becker, 2012. #SAT-Based Vulnerability Analysis of Security Components - A Case Study. In Proceedings of IEEE Int'l Symp. on Defect and Fault Tolerance, Austin.
43. Feiten, Sauer, Schubert, Czutro, Tomashevich, Böhl, Polian, and Becker, 2013. #SAT for Vulnerability Analysis of Security Components. In informal Proceedings of IEEE European Test Symp., Avignon.
44. Sauer, Burchard, Schubert, Polian, Becker, 2013. Waveform-Guided Fault Injection by Clock Manipulation, In Online-Proceedings of the 1st TRUDEVICE-Workshop, Avignon.
45. J.M. Dutertre, R. Possamai Bastos, O. Potin, M.L. Flottes, B. Rouzeyre, G. Di Natale, A. Sarafianos, "Improving the ability of Bulk Built-In Current Sensors to detect SEEs by using triple-well CMOS". In Press Microelectronic Reliability