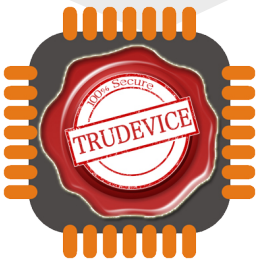

COST
EUROPEAN COOPERATION
IN SCIENCE AND TECHNOLOGY

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 2: Trustworthy manufacturing of secure devices
WG Leaders: Lilian Bossuet, Paris Kitsos

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, 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) PUFs for precise identification of secure devices
Physically Unclonable Functions (PUFs) are hardware components with the properties of inherent uniqueness, unclonability and tamper evidence which enable a number of interesting applications. A physical token embedding a PUF can use the PUF's responses as a unique identifier. Since the response behavior is in practice physically unclonable, even for the manufacturer of the tokens, they are effectively unforgeable. This makes PUFs a very useful tool for precise identification of secure devices, for creating custom and powerful authentication mechanisms, and for anti-counterfeiting technologies. This activity of the COST Action focus on the study and the implementation costs of the wide variety of known PUFs, and possibly to invent new architectures.

2) Hardware Trojan detection
In order to reduce manufacturing costs, the fabrication of integrated circuits is nowadays migrating offshore, making circuits vulnerable to security compromise, functional changes, information leaks or even catastrophic system failures under specific conditions. The threat brought by Hardware Trojans, which was under-estimated for long time, begins to materialize. On the other hand, Hardware Trojans can

even be an effective vehicle for destabilization of states (for terrorist or criminal organizations) and businesses (by mafias or fraudulent competitors). For this reason, Hardware Trojan detection mechanisms are becoming more important in ensuring a trustworthy hardware environment.

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) 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

List of members and involved people (you can find the updated list on the shared google document)

Chairs	Lilian Bossuet Paris Kitsos
Members	Nicolas Sklavos Artemios Voyiatzis Lejla Batina Julien Francq Nele Mentens David Hély Bruno Rouzeyre Pedro Peris-Lopez Philippe Loubet Moundi Milos Drutarovsky Marie-Lise Flottes Francesco Regazzoni Franck Courbon Konstantinos Markantonakis Róbert Lórencz

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

Total number of members	Number from Inclusiveness Countries	From Industry	From international cooperation institutions	Number of ESRs	Gender balance (men/ women)
17	9	3	0	10	14/3

4. Activities and Results

PUFs design, improvement, modeling and application

Two new PUF architectures were proposed by the University of Saint-Etienne (France), the first in collaboration with Telecom ParisTech (France) is a delay-based PUF call loop PUF or L-PUF [1, 2]. As the arbiter PUF, the loop PUF is based on *N* identical delay chains. The delay chains are connected serially and do not require routing constraints, except a mere copy/paste of each delay chain. When closed by an inverter, this structure forms a loop which oscillates, as a single ring oscillator. This PUF was used as a secure key generator in a secure boot by Airbus Group (France). This last work has proven that this kind of PUF is very lightweight, provides enough security for secure boot applications and can be corrected with very low-cost error-correcting codes [3].

The second is the TERO-PUF (Transient Effect Ring Oscillator) [4, 5]. By using the average number of oscillations as entropy extractor, the proposed TERO-PUF is not sensitive to the locking phenomenon. This phenomenon challenges the use of ring oscillators in both PUF and TRNG. As a consequence, TERO-PUF is a new candidate for FPGA dedicated PUF. Compared with other state-of-the-art PUFs, the proposed TERO-PUF is very attractive thanks to its low intra-device variation and large response. This PUF was used in a the case of access control in constrained environments [6].

Based on the same TERO cell, a common work between the Technical University of Kosice (Slovakia) and the University of Saint-Etienne (France) investigated a possibility to integrate TRNG and PUF capability into one building block. It proposed to use TERO loop and demonstrated its capability to generate TRNG as well as PUF functionality. The design was tested in Microsemi FPGA and results were presented in [7].

Other dual structure proving PUF and TRNG services both was proposed by Intrinsic-ID (The Netherlands). In this work, they have focused on identifying and evaluating SRAM in commercial off-the-shelf microcontrollers as an entropy source for PRNG seeding. They have measured and evaluated the SRAM start-up patterns of two popular types of microcontrollers, a STMicroelectronics STM32F100R8 and a Microchip PIC16F1825. They also developed an efficient software-only architecture for secure PRNG seeding [8].

Intrinsic-ID's researchers proposed a new model for binary-output PUFs such as SRAM, DFF, Latch and Buskeeper PUFs, and a method to accurately estimate their entropy [9]. They determined an upper bound on the 'extractable entropy', i.e. the number of key bits that can be robustly extracted, by calculating the mutual information between the bias measurements done at enrollment and reconstruction. The proposed new approach has the advantage that it simultaneously captures both of properties that are vital for key storage: uniqueness and robustness. Therefore it will be possible to fairly compare performance of PUF implementations using the proposed new method. They also introduced a new PUF reliability model taking this observed heterogeneous nature of PUF cells into account [10]. A substantial experimental validation demonstrates that the new predicted distributions describe the empirically observed data statistics almost perfectly, even considering sensitivity to operational temperature. This allows to study PUF failure behavior in full detail, including the average and the *worst case* probabilities. This is an invaluable tool for the future design of more efficient and better adapted PUFs and PUF-based systems.

In order to improve SRAM based PUF, Intrinsic-ID team investigated the effects of data-dependent silicon aging on SRAM PUF reliability under a number of realistic scenarios [11]. In an accelerated aging experiment on a 65nm CMOS SRAM PUF implementation it is observed that many scenarios cause a smaller reliability reduction than natural aging. Some scenarios even show anti-aging effects, i.e. they cause the SRAM PUF to grow more reliable over time. This is a significant improvement when using an SRAM PUF. Even more so because data-dependent (anti-)aging has a particularly low overhead, requiring neither any changes to the PUF circuit nor any pre-deployment effort.

Finally, Intrinsic-ID work presented a lightweight anti-counterfeiting solution using intrinsic Physically Unclonable Functions (PUFs), which are already embedded in most commodity hardware platforms [12]. The presented solution is particularly suitable for low-end computing devices without on-board security features. The proposed anti-counterfeiting approach was based on extracting a unique fingerprint for individual devices exploiting inherent PUF characteristics from the on-chip static random-access memory (SRAM), which in turn allows to bind software to a particular hardware platform. The proposed solution does not require additional hardware, making it flexible as well as cost efficient. SRAM PUF was also used to key generation and chip identification (Atmel ATmega Microcontrollers) by people from the Czech technical University in Prague (Czech Republica) [13].

Hardware Trojan

Work in collaboration between ALaRI - University of Lugano (Switzerland), Ruhr University of Bochum (Germany) and University of Massachusetts (Amherst, USA) have explored the possibility to implement Trojans by changing the dopant polarity of existing transistors and we evaluate their impact on security. The work appeared in references [14, 15].

Industrial Systems Institute in Patras (Greece) has established the research project “ISRTDI” that is financially supported by GSRT Action “KRIPIS”. The major focus is to set up efficient methods for pre-silicon and/or post silicon Trojan detection methods. Initially they analyze the capabilities and limitations of the existing methods, in order to frame a testing strategy for uncovering efficiently hardware Trojan horses [16]. Then a technique based on Ring Oscillator for FPGA was proposed [17].

In Grenoble Institute of Technology (Valence, France), the team from LCIS has proposed hardware Trojan detection techniques based on EM measurement [18]. In this institute, a work has been carried out in order to study the hardware Trojan threat in RFID system [19], as a result an emulation platform is available for a red team blue team approach. Finally collaboration is ongoing with New-York University (USA) in order to propose some methods for the runtime detection of Hardware Trojan [20] and [21]. The main purpose is to add within a SoC extra hardware resilient to malicious modification and providing a monitoring function in order to detect any abnormal activities due to hardware Trojan or software attack. People from Airbus Group were also active on this field [22, 23].

Protection of the designer intellectual properties

This field is not in the original topics of the WG2, nevertheless during the workshops, it was important to add it to the WG2 topics list. A project from University of Saint-Etienne (France) describes all the hardware parts use to protect intellectual properties of the fabless designs and the IP designers as salutary hardware (salware). The new term salware is the opposite of the widely used term *malware* (malicious hardware such as hardware trojans), but uses the same techniques, strategies and means [24]. For example, IP watermarking, as developed by the University of Saint-Etienne and the Southern Polytechnic State University [25], is a type of salware.

5. List of publications related to the Working Group

[1] Z. Cherif, J.L. Danger, F. Lozac’H, Y. Mathieu, L. Bossuet. “Evaluation of delay PUFs on CMOS 65nm technology: ASIC vs FPGA”. International Workshop on Hardware and Architectural Support for Security and Privacy, HASP 2013, Tel-Aviv, Israel, June 2013.

[2] Z. Cherif, J.L. Danger, L. Bossuet. “Evaluation of Delays PUFs on CMOS 65 nm Technology: ASIC vs FPGA”. In Workshop on Trustworthy Manufacturing and Utilization of Secure Devices, TRUDEVICE 2013, Avignon, France, 30-31 Mai 2013.

[3] J. Francq and G. Parlier: “Implementing a PUFKY using a LPUF”, TOISE Book chapter, Springer 2014 (to appear).

[4] L. Bossuet, X. T. Ngo, Z. Cherif, V. Fischer. “A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon”. IEEE Transactions on Emerging Topics in Computing, Vol. 2, Issue 1, pp. 30-36, 2014.

[5] L. Bossuet, X.T. Ngo, Z. Cherif, V. Fischer. “Practical Study of A Physical Unclonalbe Function Based on Transient Effect Ring Oscillators”. In Workshop on Trustworthy Manufacturing and Utilization of Secure Devices, TRUDEVICE 2013, Avignon, France, 30-31 Mai 2013.

[6] A. Cherkaoui, L. Bossuet, L Seitz, G. Selander and R. Borgaonkar. “New Paradigms for Access Control in Constrained Environments”. In Proceedings of the IEEE International Symposium on Reconfigurable Communication-centric Systems-on-Chip, ReCoSoC 2014, Montpellier, France, Mai 2014.

[7] Varchola, M. ; Drutarovsky, M. ; Fischer, V., “New universal element with integrated PUF and TRNG capability”, International Conference on Reconfigurable Computing and FPGAs (ReConFig), 2013
PP. 1 – 6.

[8] A. van Herrewege, V. van der Leest, A. Schaller, S. Katzenbeisser, I. Verbauwhede. “Secure PRNG seeding on commercial off-the-shelf microcontrollers”. TrustED 2013, workshop at CCS 2013: 55-64.

[9] R. van den Berg, B. Skoric, V. van der Leest. “Bias-based modeling and entropy analysis of PUFs”. TrustED 2013, workshop at CCS 2013: 13-20.

[10] R. Maes. “An Accurate Probabilistic Reliability Model for Silicon PUFs”. In Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2013, 2013.

[11] R. Maes, V. van der Leest. “Countering the effects of silicon aging on SRAM PUFs”. HOST 2014: 148-153.

[12] A. Schaller, T. Arul, V. van der Leest, S. Katzenbeisser. “Lightweight Anti-counterfeiting Solution for Low-End Commodity Hardware Using Inherent PUFs”. TRUST 2014: 83-100.

[13] Platonov, M. - Hlaváč, J. - Lórencz, R. “Using Power-up SRAM State of Atmel ATmega1284P Microcontrollers as Physical Unclonable Function for Key Generation and Chip Identification”. Information Security Journal: A Global Perspective, Taylor & Francis, May 15, 2014.

[14] G. Becker, F. Regazzoni, C. Paar, and W. Burleson, “Stealthy Dopant-Level Hardware Trojans: Extended Version”, in Journal of Cryptographic Engineering. April 2014

[15] G. Becker, F. Regazzoni, C. Paar, and W. Burleson, ”Stealthy Dopant-Level Hardware Trojans”, in Proceedings of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2013), Santa Barbara, California, USA, 18-22 August 2013.

[16] P. Kitsos and A. G. V., “Towards a Hardware Trojan Detection Methodology”, 2nd EUROMICRO/IEEE Workshop on Embedded and Cyber-Physical Systems (ECYPS 2014), Budva, Montenegro, 15-19, June 2014.

[17] P. Kitsos and A. G. Voyiatzis, “FPGA Trojan Detection Using Length-optimized Ring Oscillators”, 17th Euromicro Conference on Digital Systems (DSD'14), Verona, Italy, 27-29 August, 2014.

[18] D. Hély, J. Martin, G. Triana, S. Piroux Mounier, E. Rivière, T. Sahuc, J. Savonet, L. Soundararadjou, “ Experiences in Side Channel and Testing based Hardware Trojans Detection” , Proceedings of 31th IEEE VLSI Test Symposium, May 2013

[19] E. Hidalgo, O. Abdelmalek, D. Hély, V. Beroulle, “Triggering Hardware Trojans in EPC C1G2 RFID Tags” Workshop on Trustworthy Manufacturing and Utilization of Secure Devices, TRUDEVICE 2013, Avignon May 31st 2013.

[20] J. Dubeuf, D. Hély, R. Karri, “RunTime Dection of Hardware Trojans : The Processor Protection Unit”, Proceedings of 18th IEEE European Test Symposium, May 2013

[21] J. Backer, D. Hély, R. Karri, “Reusing The Design for Test Infrastructure For Online Security Monitoring of Systems-on-Chip” to appear in Defect and Fault Tolerance Sympoisum 2014

[22] Julien Francq: “Hardware Trojans: A Threat for CyberSecurity”. PERSYVAL-Lab Summer School on Cyber-Physical Systems, July 2013.

[23] Julien Francq: “Hardware Trojans: A French Initiative and First Results”. International Workshop on Practical Hardware Innovations in Security Implementation and Characterisation – PHISIC, July 2013.

[24] L. Bossuet, D. Hely. “SALWARE: Salutary Hardware to Design Trusted IC”. In Workshop on Trustworthy Manufacturing and Utilization of Secure Devices, TRUDEVICE 2013, Avignon, France, 30-31 Mai 2013.

[25] C. Marchand, L. Bossuet, E. Jung. “IP Watermark Verification Based on Power Consumption Analysis”. In International CryptArchi Workshop 2014, Annecy, France, 30 June – 02 Jully, 2014.