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 4: Reconfigurable devices for secure functions
WG Leaders: Viktor Fischer, Nele Mentens

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)
- Workshop CryptArchi 2013, June 23-26, 2014, Fréjus, France
- MC/WG meeting, December 12-13, 2014, Freiburg
- TRUDEVICE Workshop May 29-30, 2014, Paderborn, Germany
- Group meeting at the summer school in Sibenik, May 29 – June 1, 2014, Sibenik, Croatia
- TRUDEVICE TRAINING school, July 14-18, 2014, Lisbon, Portugal

Cooperation set-ups and execution:
Proposition of a common scientific project in the framework of the European call for projects Horizon 2020 (two partners of the COST Action are included: the Hubert Curien laboratory, France and the COSIC group of KU Leuven , Belgium).

2. Description and objectives of the Working Group

In our group, reconfiguration as a technique to make the overall system secure and trustworthy is investigated. Fault recovery and self-repairing procedures of secure devices are studied. The actions are divided into two areas:

1) Mitigation architectures on FPGAs to counteract fault attacks
Many techniques have recently been developed to protect critical systems on SRAM-based FPGAs against Single Event Upset. At the design level of the FPGA these techniques are classified as mitigation techniques, which prevent faults to affect the target design, and recovery techniques that repair erroneous bits of the FPGA configuration memory. These techniques together with the possibilities to detect dangerous events are investigated and re-adapted to cope with the issue of fault attacks.

2) Self-repairable architectures of secure devices

New characteristics of recent commercial FPGA devices allow the partial re-configuration of the circuit implemented in it. By exploiting this inherent property of FPGAs, new implementations of self-repairable cryptographic logic based on FPGA-implemented detection and recovery mechanisms will allow correcting errors provoked by fault attacks.

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.	□	☐	□	□	□
2) To provide solutions for required but conflicting relationships between Testability and Security	□	□	☐	□	□
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	☐	□	□	□	□
4) To define secure protocols to protect the access to necessary test infrastructures and to design secure access controllers	□	□	☐	□	□
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	□	□	☐	□	□
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	□	☐	□	□	□
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	☐	□	□	□	□
12) To explore formal verification methods to establish the robustness of a secure device against fault attacks	☐	□	□	□	□
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:	Viktor Fischer
	Nele Mentens
Members:	
1	Lejla Batina
2	Nele Mentens
3	Viktor Fischer
4	Róbert Lórencz
5	Nicolas Sklavos
6	Francesco Leporati
7	Lilian Bossuet
8	Julien Francq
9	Guy Gogniat
10	Carles Ferrer
11	Milos Drutarovsky
12	Francesco Regazzoni
13	Paolo Maistrii
14	Tim Güneysu
15	Apostolos Fournaris
16	Jo Vliegen
17	Selcuk Baktir
18	Konstantinos Markantonakis
19	Stjepan Picek
20	Patrick Haddak
21	Richard Newell
22	Ioannis Voyiatzis
23	Artemios G. Voyiatzis
24	Ricardo Chaves
25	Regis Leveugle
26	Nathalie Bochard
27	Paris Kitsos

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)
27	14	2	0	12	24/3

4. Activities and Results

Activities

Three Short-Term Scientific Missions took place within the scope of WG4. The results of the missions and other activities are summarized in the 'Results' section.

- Mission 1:
  - Host Institution: Michael Hübner, Tim Güneysu, Christof Paar, RUB, Bochum, (DE)
  - Visitor: Nele Mentens, KU Leuven, campus Diepenbeek, (BE)
  - Period: The visiting period was from September 30, 2013 to January 3, 2014
- Mission 2:
  - Host Institution: Tim Güneysu, Christof Paar, RUB, Bochum, (DE)
  - Visiting Researcher: Lejla Batina, Radboud University, Nijmegen, (NL)
  - Visiting Period: The visiting period was from October 1 to November 15, 2013
- Mission 3:
  - Host Institution: Nele Mentens, KU Leuven, (BE)
  - Visitor: Martin Petrvalsky, Slovakia, (SK)
  - Period: The visiting period was from February 24 to May 28, 2014
- Mission 4 (accepted):
  - Host Institution: Milos Drutarovsky, Technical University of Kosice, (SK)
  - Visitor: Tania Richmond, Hubert Curien Laboratory, (FR)
  - Period: The proposed visiting period is from September 15 to December 19, 2014

Results

Mitigation architectures on FPGAs to counteract fault attacks

A new approach has been designed and experimented at TIMA Grenoble, France, in order to quickly react against attacks leading to modify the configuration of SRAM-based FPGAs [1]. The approach takes advantage of unused resources to implement error detection at no cost at the system level [2,3] and has been applied to several SRAM-based FPGA families. This type of protection is well-suited for medium security, since trade-offs are made between costs and the achieved detection rate.

The research team from the Hubert Curient laboratory, Saint-Etienne, France is oriented in secure implementation of Physical Unclonable Functions (PUFs) and True Random Number Generators (TRNGs) in reconfigurable devices (FPGAs). Results of the team concerning PUFs are reported in the report of WG 2. The main objective in securing TRNGs implemented in FPGAs was to propose stochastic models of generators (serving for entropy estimation) and, based on these models, to propose fast and efficient embedded test that will be capable to react immediately on natural or forced variations of generator's environment (such as temperature, power voltage, EMI, etc.).

Before starting to work on dedicated statistical tests that can be embedded in FPGAs, the research team from the Hubert Curient laboratory developed hardware and software support aimed at implementation of gerators and embedded tests – Evariste II [12]. The system was for the first time presented during the first workgroup meeting during the CryptArchi 2013 workshop at Fréjus, France [13] and at the FPL conference in 2013 [15]. Since this first presentation the same system as acquired by another member of the COST Action – the team from the Czech Technical University, in order to reinforce cooperation, share achievements and compare obtained results.

The next step in securing TRNGs was to propose new principles that are robust to manipulations and fault injection [6], [8], to propose stochastic models for these generators [10], and last, but not least, to prose fast and efficient dedicated statistical test [11]. The final step consists in attacking the proposed generators and verifying efficiency of proposed generators [9].

Thanks to cooperation between the team of the Hubert Curien laboratory and the group COSIC from KU Leuven that started in the frame of the COST Action, the two teams prepared a common scientific project oriented in secure PUF and TRNG design (HECTOR – Hardware Hardware Enabled Crypto and Randomness) that was accepted for funding in the frame of the European call for projects – Horizon 2020.

The Evariste II system mentioned above is now used by the Czech team for achieving basic understanding of the fault-tolerant and attack-resistant system design. Their results in this field were presented and discussed on various occasions (PESW 2014, Cryptarchi 2014, TRUDEVICE 2014) with emphasizing the possible leakage of the information through side channel.

The STSM of Tania Richmond (Hubert Curien Laboratory) to TUKE will focus on (1) fault injection attacks on cryptographic protocols based on error-correcting codes and (2) the modification of existing algorithms in order to make them more resistant to selected attacks.

Self-repairable architectures of secure devices

Prof. C. Ferrer's team at the Universitat Autònoma de Barcelona (UAB) has been working on the implementation of critical systems in SRAM-based FPGAs [14]. Specifically they have implemented key management schemes and symmetric cryptographic algorithms in Spartan-6. They have focused on partial reconfiguration as a mechanism to dynamically modify the hardware and also for correction purposes. Once a fault has been detected on a module implemented in the dynamic reconfigurable part of the device, it can be partially reconfigured to correct the anomaly without affecting the remaining part of the device. A controller engine, to efficiently manage the special internal reconfiguration port (ICAP) has been designed. This component, combined with fault detection mechanisms, can improve the robustness of the system.

At INESC-ID/IST, Technical University of Lisbon, a technique has been developed for performing secure partial dynamic reconfiguration with unsecured external memory [15]. The proposed solution uses high performance encryption engines to change the encryption key of the remotely received bitstream by a randomly generated key, unique to each configuration, when storing the bitstream in the external unsecured memory. An additional CBC-MAC authentication mechanism is also considered that combined with the frame-wise error detection mechanism of the configuration port, allows for an improved countermeasure against replay attacks and wrongful bitstream usage.

The STSMs of Lejla Batina (Radboud University Nijmegen) and Nele Mentens (KU Leuven) to Tim Güneysu (Ruhr University Bochum) resulted in a joint research topic on dynamic reconfiguration of FPGA LUTs. The block cipher PRESENT was used as an example case. PRESENT was recently included in the new international standard for lightweight cryptographic methods by ISO/IEC. Xilinx FPGAs were used, which made it possible to use LUTs that are configurable at run-time through a shift register (SRL) that is addressable from within the FPGA logic. The architecture also contains a True Random Number Generator (TRNG) of which the output is used to choose between different configurations. The architecture allows to dynamically change the position of pipelining registers, which makes it more difficult to perform fault attacks and side-channel attacks.

Another cooperation of Radboud University Nijmegen and KU Leuven resulted in a paper that was accepted at Indocrypt 2014 [16]. In this work, the challenge of keeping area under control while optimizing throughput was tackled. The work was based on the AES substitution box (S-box). Relying on composite field arithmetic for reducing the area implementation of the AES S-box is a commonplace in literature. However, maximizing the circuit throughput via pipelining, i.e. selecting the right positions for inserting Flip-Flops (FF), is not a trivial task given the complexity of the circuit. On the other hand, Genetic Algorithms (GA) are generally used for addressing large search problems. A methodology was developed for finding the optimal position of pipelining registers in the composite field S-box in order to optimize the throughput. In a later stage, the different pipelining options can be used to dynamically change the position of the pipelining registers in order to increase the resistance against fault attacks and side-channel attacks.

The STSM of Martin Petrvalsky (Tuke) to KU Leuven focused on attacking the hardware implementation of a promising scheme called inner product masking, which can defend an implementation against DPA attacks. We used the Altera Cyclone III DISIPA FPGA board as a hardware platform. At KU Leuven, a software implementation for the 8-bit Atmel AVR ATMega128 in assembly language was already realized. This STSM focused on following a similar strategy in hardware.

Other publications of Ruhr University Bochum that are related to FPGA security are published in [17,18,19,20,21]. Researchers of the KNOSSOSnet research group also published their work on S-box optimization [22].

5. List of publications related to the Working Group

[1] M. Ben Jrad, R. Leveugle, "Evaluating a low cost robustness improvement in SRAM-based FPGAs", 18th IEEE International On-Line Testing symposium, Chania, Crete, Greece, July 8-10, 2013, pp. 173-174.

[2] R. Leveugle, M. Ben Jrad, "On improving at no cost the quality of products built with SRAM-based FPGAs", 5th Asia Symposium on Quality Electronic Design (ASQED 2013), Penang, Malaysia, August 26-28, 2013, pp. 295-301.

[3] M. Ben Jrad, R. Leveugle, "Automated design flow for no-cost configuration error detection in SRAM-based FPGAs", International Conference on ReConFigurable Computing and FPGAs (ReConFig' 13), Cancun, Mexico, December 9-11, 2013.

[4] F. Stepanek, M. Novotny, “Comparison of various approaches in Fault-Tolerant and Attack-Resistant system design”, Proceedings of the 2nd Prague Embedded Systems Workshop, 2014.

[5] V. Fischer, F. Bernard, and P. Haddad. *An Open-source Multi-FPGA Modular System for Fair Benchmarking of True Random Number Generators.* Accepted for publication in Proceedings of Field Programmable Logic and Applications - FPLA 2013, Porto, Portugal, September 2013.

[6] A. Cherkaoui, V. Fischer, L. Fesquet, and A. Aubert. *A Very High Speed True Random Number Generator with Entropy Assessment.* Cryptographic Hardware and Embedded Systems – CHES 2013, LNCS 8086, pp. 179-196, Santa Barbara, USA, August 2013.

[7] P. Bayon, L. Bossuet, A. Aubert, V. Fischer. *EM radiation analysis on true random number generators: Frequency and localization retrieval method.* In Proceedings of the IEEE Asia-Pacific International Symposium and Exhibition on Electromagnetic Compatibility, APEMC 2013, Melbourne, Australia, May 2013.

[8] A. Cherkaoui, V. Fischer, A. Aubert, and L. Fesquet. *A Self-timed Ring Based True Random NumberGenerator.* In Proceedings of the 19th IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC 2013), pp. 99 – 106, Santa Monica, USA, May 2013.

[9] P. Bayon, L. Bossuet, A. Aubert, V. Fischer. *Electromagnetic Analysis on Ring Oscillator-Based True Random Number Generators.* In Proceedings of the IEEE International Symposium on Circuits and Systems, ISCAS 2013, pp. 1954 – 1957, Beijing, China, May 2013.

[10] P. Haddad, F. Bernard, V. Fischer, and Y. Teglia, On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models, DATE 2014, Dresden, Germany, March 2014.

[11] V. Fischer and D. Lubicz, Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG, CHES 2014, Busan, Corea, September 2014.

[12] Evariste II – A Modular Hardware System for Development and Evaluation of Cryptographic Functions and Random Number Generators, On-line, Available at: http://labh-curien.univ-st-etienne.fr/wiki-evariste-ii/index.php/Main_Page.

[13] V. Fischer, Evariste II – Modular hardware system for fair TRNG benchmarking, Workshop CrypArchi 2013, Fréjus, France, 2013.

[14] L.A. Cardona, B. Lorente, S. de La Fe Siverio, S. Villar, C.Ferrer. Secure Key Management in Low Power Wireless Sensor Meshed Networks, 47th IEEE International Carnahan Conference on Security Technology (ICCST 2013), 2013.

[15] H. J. Kashyap and R. Chaves. Secure partial dynamic reconfiguration with unsecured external memory, In International Conference on Field Programmable Logic and Applications (FPL), Munich, Germany, September 2014.

[16] L. Batina, D. Jakobovic, N. Mentens, S. Picek, A. de la Piedra, and D. Sisejkovic. S-box pipelining using genetic algorithms for high-throughput AES implementations: How fast can we go?, accepted at Indocrypt 2014.

[17] Pascal Sasdrich, Tim Güneysu: Efficient Elliptic-Curve Cryptography Using Curve25519 on Reconfigurable Devices. ARC 2014: 25-36

[18] Thomas Pöppelmann, Léo Ducas, Tim Güneysu: Enhanced Lattice-Based Signatures on Reconfigurable Hardware. CHES 2014: 353-370

[19] Ingo von Maurich, Tim Güneysu: Lightweight code-based cryptography: QC-MDPC McEliece encryption on reconfigurable devices. DATE 2014: 1-6

[20] Stefan Heyse, Tim Güneysu: Code-based cryptography on reconfigurable hardware: tweaking Niederreiter encryption for performance. J. Cryptographic Engineering 3(1): 29-43 (2013)

[21] Thomas Pöppelmann, Tim Güneysu: Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable Hardware. Selected Areas in Cryptography 2013: 68-85

[21] Thomas Pöppelmann, Tim Güneysu: Area optimization of lightweight lattice-based encryption on reconfigurable hardware. ISCAS 2014: 2796-2799

[22] A. Bikos, N. Sklavos, A. Fournaris, On the Optimization of S-Box Functionality in 4G LTE Security Ciphers, joint MEDIAN-TRUDEVICE Workshop, co-located with International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT□14), Amsterdam, The Netherlands, 2-3 October 2014.