




COST

**European Cooperation in Science
and Technology**

**Introduction to the
COST Framework Programme**



Added value and impact of participating in a COST Action

Milena Djukanovic, PhD

ICT COST Actions IC1204, IC1306, IC1403 – finished

CA COST Actions CA16222, CA16116



Action description – IC1204

Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE)



- Hardware security - increasingly important for many embedded systems applications.
- Its relevance is expected to increase.
- The vulnerability of hardware devices that implement cryptography functions has become the Achilles heel in the last decade.
- Therefore, the industry is recognizing the significance of hardware security.
- This COST action aims at creating a European network of competence and experts on all aspects of hardware security.

Action presentation –

Trustworthy Manufacturing and Utilization of Secure Devices

Participations

Country	Date	Status
▶ Austria	09/09/2013	Confirmed
▶ Belgium	21/09/2012	Confirmed
▶ Croatia	15/07/2013	Confirmed
▶ Czech Republic	06/12/2012	Confirmed
▶ Denmark	19/09/2014	Confirmed
▶ Estonia	24/09/2013	Confirmed
▶ Finland	10/09/2012	Confirmed
▶ France	25/07/2012	Confirmed
▶ FYR Macedonia	25/10/2012	Confirmed
▶ Germany	05/07/2012	Confirmed
▶ Greece	29/08/2012	Confirmed
▶ Ireland	11/09/2014	Confirmed
▶ Israel	15/10/2012	Confirmed
▶ Italy	28/11/2012	Confirmed
▶ Montenegro	04/06/2015	Confirmed
▶ Netherlands	27/06/2012	Confirmed
▶ Norway	20/12/2012	Confirmed
▶ Portugal	26/09/2012	Confirmed
▶ Slovakia	02/09/2012	Confirmed
▶ Slovenia	08/11/2012	Confirmed
▶ Spain	22/10/2012	Confirmed
▶ Sweden	20/09/2012	Confirmed
▶ Switzerland	16/07/2012	Confirmed
▶ Turkey	08/05/2013	Confirmed
▶ United Kingdom	13/06/2012	Confirmed
Total: 25		

ICT COST Action IC1204

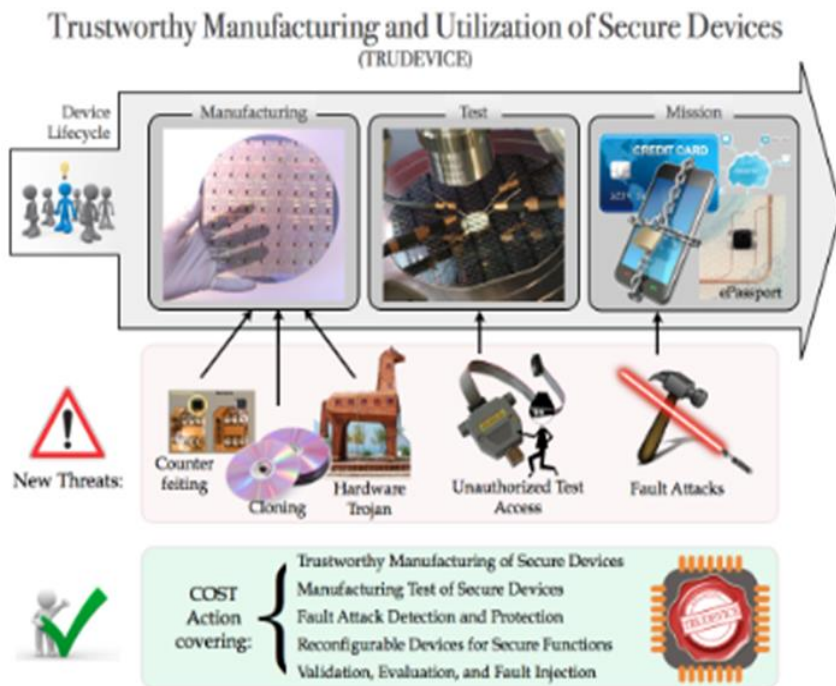
Management Committee

MC Chair	▶ Dr Giorgio DI NATALE (FR)
MC Vice Chair	▶ Prof Ilia POLIAN (DE)

Important names in the area of
Hardware Security:

Prof. Stefan Mangard,
Prof. Ingrid Verbauwhede
Dr Nele Mentens
Prof. Marin Golub
Dr Lejla Batina
Prof. Nicolas Sclavos

Action presentation – Trustworthy Manufacturing and Utilization of Secure Devices



- In the time of applying - Montenegro was a Non-COST country, so the procedure took around 6 months for UoM to be accepted in this action.

MoU	4135/12
C SO Approval date	07/06/2012
Start of Action	12/12/2012
End of Action	11/12/2016
End of prolongation	—

Networking activities – Personal highlight experiences

- STSM – Short Term Scientific Mission
 - Especially useful for Early-Stage collaboration, to learn a new way of using instruments and/or methods at a new institution/laboratory.
- MC Meetings and Workshops:
- Training School - Portugal





COST Cryptanalysis of Ubiquitous C
March 14-15, 2017, Sutomore, Montenegro
<https://www.cryptacus.eu/>

BOOKLE OF ABS

TABLE OF CONTENTS

1. Davide Bellizia, Milena Djukanovic, Giuseppe Scotti, and Alessandro Trifiletti
„Template Attacks Exploiting Static Power And Application To CMOS Lightweight Crypto-Hardware“
2. Cesar Pereida Garcia and Billy Bob Brumley
„A Tale of Cache-Timing Attacks in OpenSSL: Constant-Time Callees with Variable-Time Callers“
3. Ziya Alper Genc, Suleyman Kardas, Mehmet Sabir Kiraz
„Enhancing the Honeywords System: Mitigating Active Adversaries and Increasing Typo-safety of Honeywords“
4. David G rault
„Security Evaluation of Symmetric Key Primitives using CP“
5. Thomas Gougeon, Morgan Barbier, Patrick Lacharme, Gildas Avoine, and Christophe Rosenberger
„Memory carving in ubiquitous devices“
6. Eleni Isa, Nicolas Sklavos
„On the Hardware Trojans and Confidentiality“
7. Orhun Kara and Muhammed F. Esgin
„Analysis of Keystream Generators With KUF“
8. Miodrag J. Mihaljević, Siniša Tomović and Milica Knežević
„An Improved Man-in-the-Middle Attack Against HB# Authentication Protocols“
9. D. Bellizia, S. Bongiovanni, P. Monsurr , G. Scotti, A. Trifiletti
„Univariate Power Analysis Attacks Exploiting Static Dissipation of Nanometer CMOS VLSI Circuits for Cryptographic Applications“
10. Constantinos Patsakis, Efthimios Alepis
„UI deception at its finest: The Android case“
11. Darren Hurley-Smith and Julio Hernandez-Castro
„Certifying the Uncertifiable: A Critique of Common Criteria EAL4+ using the DESFire EV1 TRNG“
12. Darren Hurley-Smith and Julio Hernandez-Castro
„Measuring the Distance: Reverse Engineering the DESFire EV2 Distance Bounding Protocol“
13. Siniša Tomović, Milica Knežević and Miodrag J. Mihaljević
„The Success Rate Reconsideration of the MIM Attack Against HB# Authentication Protocols“
14. Nicola Taveri, Billy Bob Brumley, and Patrick Longa
„Pushing elliptic curve speed limits in OpenSSL“

successful first Cryptacus' event in Montenegro. Cryptacus has funded the event in Montenegro, Italy, Luxembourg,

if Abstracts useful and

Gildas Avoine
Julio Hernandez-Castro
Milena Djukanovic



EUROPEAN COOPERATION IN SCIENCE AND TECHNOLOGY



COST is supported by the
EU Framework Programme
Horizon 2020

Action description – IC1403

Cryptanalysis of ubiquitous computing systems (CRYPTACUS)

- STSM – Short Term Scientific Missions
 - Especially useful for Early-Stage Researchers to foster collaboration, to learn a new technique or to take measurements using instruments and/or methods not available in their own institution/laboratory.
- Milena Djukanovic, from University of Montenegro, visiting Università degli Studi di Roma (Italie) during 27 days to work on "Research in the area of Hardware Security and Side-Channel Attacks"

Template attacks exploiting static power and application to CMOS lightweight crypto-hardware

9 2017

D Bellizia, M Djukanovic, G Scotti, A Trifiletti

International Journal of Circuit Theory and Applications 45 (2), 229-241

Multivariate analysis exploiting static power on nanoscale CMOS circuits for cryptographic applications

6 2017

M Djukanovic, D Bellizia, G Scotti, A Trifiletti

International Conference on Cryptology in Africa, 79-94

Action description – IC1403 Cryptanalysis of ubiquitous computing systems (CRYPTACUS)

- INCLUSIVENESS TARGET COUNTRIES (ITC) CONFERENCE GRANTS

22. doi:10.1007/978-3-030-02577-9_34	Title	Programming of the Robotic Arm/Plotter System
	Authors	Milena Djukanovic; Rade Grujicic; Luka Radunovic; Vuk Boskovic
	DOI	doi:10.1007/978-3-030-02577-9_34
	Type	Chapter
	Published in	Advanced Technologies, Systems, and Applications III
	Published by	Springer International Publishing
	ISSNs	2367-3370 ; 2367-3389
	Link	http://link.springer.com/content/pdf/10.1007/978-3-030-02577-9_34

Action description – IC1403 Cryptanalysis of ubiquitous computing systems (CRYPTACUS)

- INCLUSIVENESS TARGET COUNTRIES (ITC) CONFERENCE GRANTS

ETS 2018

23rd IEEE European Test Symposium | May 28 - June 01, 2018 | Bremen, Germany



PROGRAM

Thursday, May 31st, 2018

16:30-16:40 Opening

16:40-17:40 Invited speaker 1

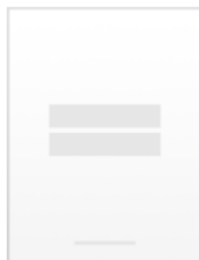
- **Functional Safety and Security: the Challenges in Developing IP for These Markets**
Pete Harrod, ARM

17:40-19:00 Regular session 1

- **Comparison of American and European Approaches in RNG online and offline testing**
Viktor Fischer
- **Security of the robotic ARM/PLOTTER**
Milena Djukanovic, Luka Radunovic
- **Detection and Defense against Covert Channel Cyber-attack over video stream payload**
Ofar Hadar, Raz Birman, Yoram Segal and Eldad Hadas
- **Model-Driven Analysis of Security, Reliability, Test, Privacy, Safety and Trust of IoE Services**
Eugenio Villar

Action description – IC1403

- Sa
- Sp
- Ed



© 2021

Open Access

Sec
CoI

Editors:

Ubiquitous computing
security
Result of the successful
Cryptacus
Contributions from to
cryptography
Open Access

About this book

The chapters in this open access objective of which was to improve ubiquitous computing framework. models, cryptanalysis of building assessment of real-world systems

The authors are top-class researchers and practitioners in

It started with templates: The future of profiling in Side-channel Analysis

Lejla Batina¹, Milena Djukanovic², Annelie Heuser³, and Stjepan Picek⁴

¹ Radboud University Nijmegen, The Netherlands

² Faculty of Electrical Engineering, University of Montenegro, Montenegro

³ CNRS/IRISA, Rennes, France

⁴ Cyber Security Research Group, Delft University of Technology, Mekelweg 2, Delft, The Netherlands

Abstract. Side-channel attacks (SCAs) are powerful attacks against cryptographic devices where the most potent ones are profiling attacks. In this case, the attacker has access to a specific device and is consequently able to find the “fingerprints” of all the keys through profiling. Afterwards, he can use that knowledge to extract a secret from another similar device. Profiling side-channel attacks have received a lot of attention in the last years due to the fact that this type of attacks defines the worst case security assumptions. It all started with template attack (TA) [1], a technique that is still the best (optimal) from an informa-

Action description –



New COST actions – New possibilities

- “Hoping to have a Training school or Workshop organized in Montenegro!”
- Hoping to have more COST Actions with Action Chair from Montenegro, as a leading country!!!

