COST

European Cooperation in Science and Technology

Introduction to the

COST Framework Programme

COST is supported
by the EU Framework Programme

Added value and impact of participating in a COST Action

Milena Djukanovic, PhD
ICT COST Action IC1204,
Trustworthy Manufacturing and Utilization of Secure Devices,
University of Montenegro

Outline

1. Action presentation

- Objectives (description, goals)
- Foreseen scientific, technological, and/or socio-economic impacts
- Management structure (MC, WGs, STSM, Training school etc.)

2. Networking activities

- Added value of networking
- Good practice examples
- Personal experience as participant and MC member in the Action

Action description –

Trustworthy Manufacturing and Utilization of Secure Devices

- 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 objectives –

Trustworthy Manufacturing and Utilization of Secure Devices

- **Main objective :**
  - 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.

- **Secondary objectives:**
  - To explore implementation and security issues of cryptographic logic based on Field-Programmable Gate Array (FPGA),
  - To collect statistically significant data related to fault injection campaigns
  - To define new architectures able to detect faults and to resist to fault attacks
  - To explore formal verification methods to establish the robustness of a secure device against fault attacks etc.

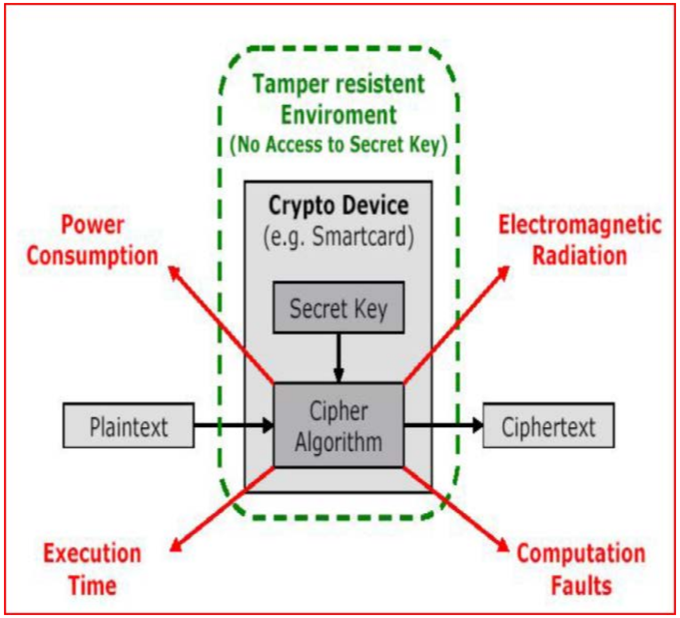
COST is supported by the
EU Framework Programme
Horizon 2020

Action objectives –

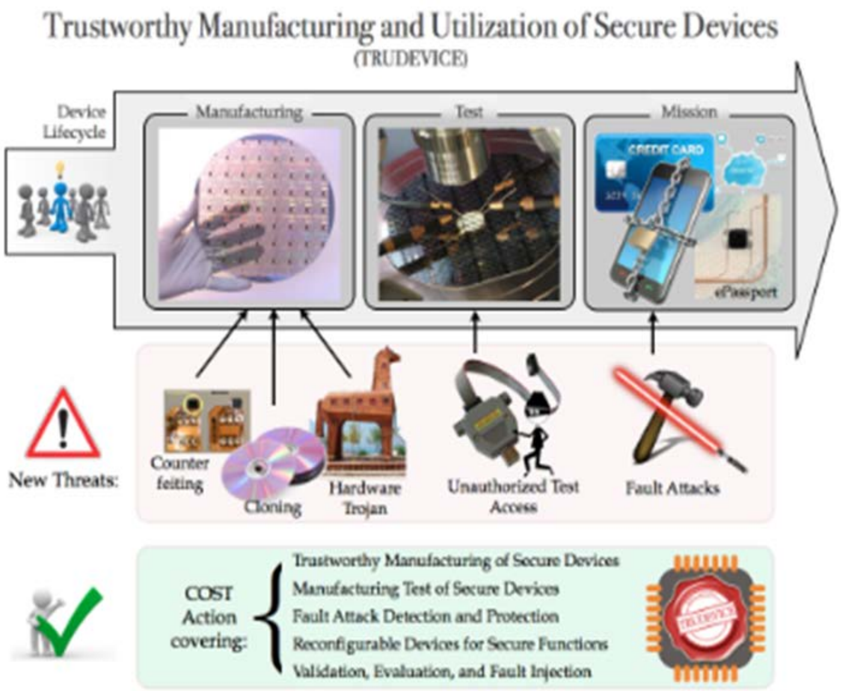
Trustworthy Manufacturing and Utilization of Secure Devices

- PASSIVE ATTACKS ARE ALSO CALLED SIDE-CHANNEL ATTACKS AS THEY BENEFIT FROM SIDE-CHANNEL INFORMATION, WHICH IS COLLECTED BY MEASURING SOME PHYSICAL DATA.

- For instance, by correlating the power consumed and the data manipulated by the device, it is possible to discover the secret encryption key.



Action presentation – Trustworthy Manufacturing and Utilization of Secure Devices



Trustworthy Manufacturing and Utilization of Secure Devices
(TRUDEVICE)

Device Lifecycle

Manufacturing

Test

Mission

CREDIT CARD

ePassport

New Threats:

Counter feiting

Cloning

Hardware Trojan

Unauthorized Test Access

Fault Attacks

COST Action covering:

Trustworthy Manufacturing of Secure Devices

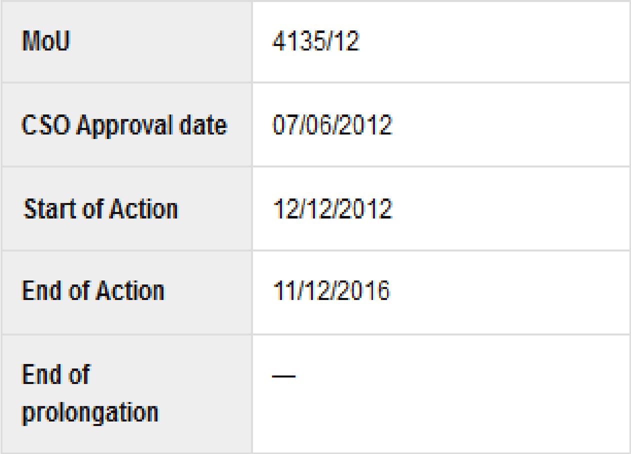
Manufacturing Test of Secure Devices

Fault Attack Detection and Protection

Reconfigurable Devices for Secure Functions

Validation, Evaluation, and Fault Injection

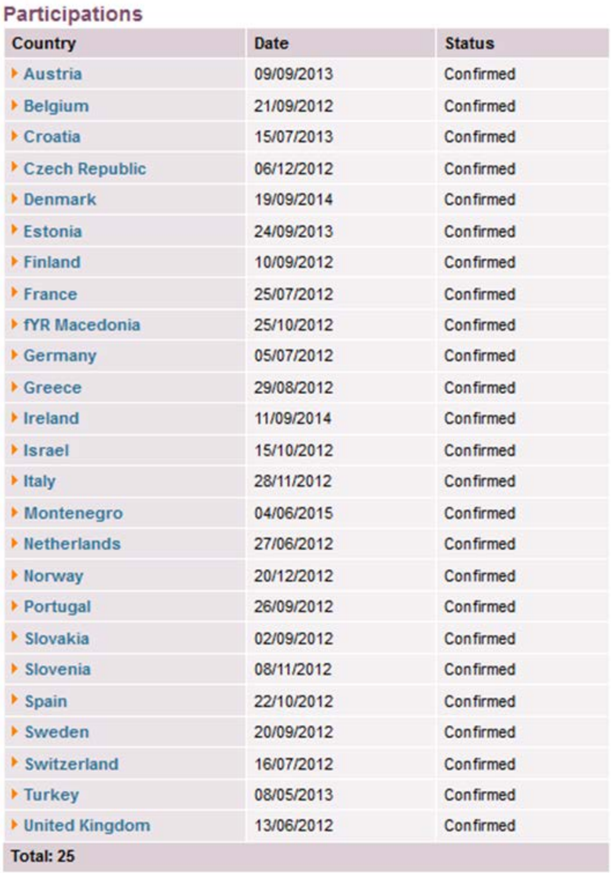
- In the time of applying - Montenegro was a Non-COST country, so the procedure took around 6 months for UoM to be accepted in this action.



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

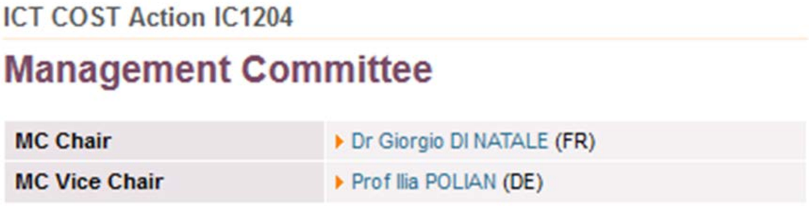
Action presentation –

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:

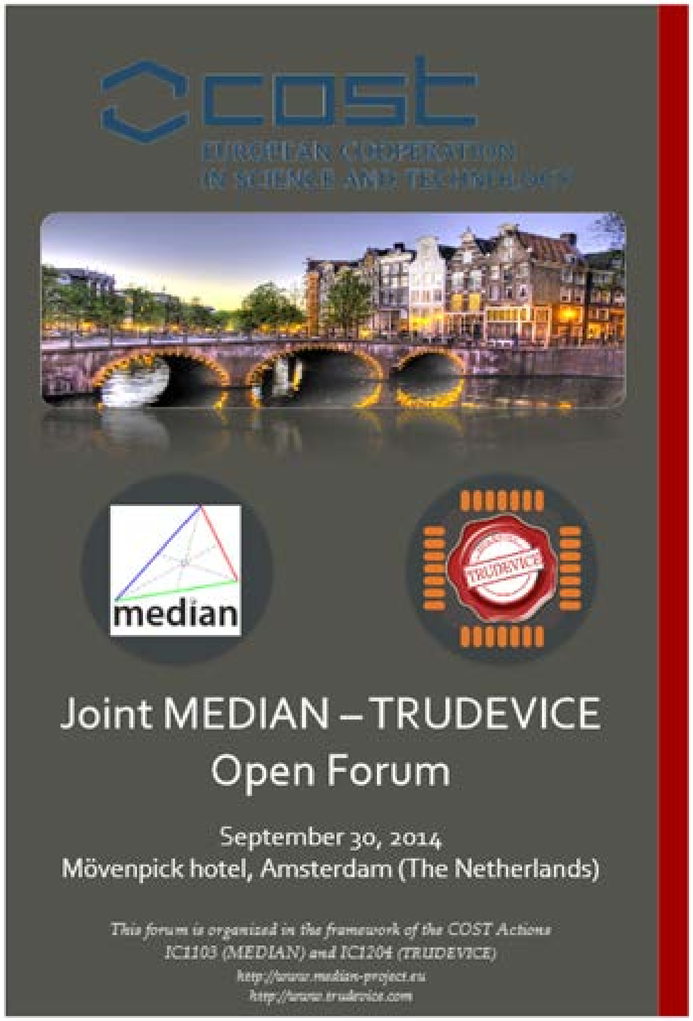
Prof. Stefan Mangard,
Prof. Ingrid Verbauwhede
Dr Nele Mentens
Prof. Marin Golub
Dr Lejla Batina
Prof. Nicolas Sclavos

Fila A

Networking activities – Personal highlight

- STSM – Short Term Scientific Missior
  - Especially useful for Early-Sta collaboration, to learn a new te using instruments and/or meth institution/laboratory.

- MC Meetings and Workshops:



EUROPEAN COOPERATION IN SCIENCE AND TECHNOLOGY

median
TRUDEVICE

Joint MEDIAN – TRUDEVICE Open Forum

September 30, 2014
Mövenpick hotel, Amsterdam (The Netherlands)

This forum is organized in the framework of the COST Actions IC1103 (MEDIAN) and IC1204 (TRUDEVICE)
http://www.median-project.eu
http://www.trudevice.com

New COST actions – New possibilities

- Hoping to have a Training school or Workshop organised in Montenegro!