PHISIC 2013

Workshop on Practical Hardware Innovations in Security Implementation and Characterization

13th and 14th of June 2013

Centre Microélectronique de Provence, Gardanne

www.phisic.emse.fr

Call For Short talk

Organizational Committee

Assia Tria
CEA-TECH
Gardanne, France
Email: assia.tria@emse.fr

Amine Dehbaoui
EMSE
Gardanne, France
Email: dehbaoui@emse.fr

Program Committee

Alain Merle
CEA-LETI, France
Assia Tria
CEA-TECH, France
Amine Dehbaoui
EMSE, France
Bruno Robisson
CEA-TECH, France
Philippe Maurine
LIRMM, France
Sylvain Guilley
ENST, France
Yannick Teglia
STMicroelectronics, France
Jean-Max Dutertre
EMSE, France

IMPORTANT DATES

Paper Submission	**May 1, 2013**
Authors Notification	**May 15, 2013**
Registration Deadline	**May 30, 2013**
Workshop Dates	**June 13-14, 2013**

The protection of information and communications infrastructures against unauthorized accesses threatening data integrity, confidentiality and availability is a buoyant field of research and commercial innovations which has grown and evolved significantly over the recent years because of the constant battle between those looking to improve security and those looking to circumvent it.

Among the security threats, integrated circuits' vulnerability to side channel analysis and fault attacks is one of the most important one since it is correlated to the ubiquitous use of cryptography by those circuits in a whole plethora of applications managing users' authentication, data confidentiality and privacy. Indeed, these attacks are based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the cryptographic algorithms. Therefore, countermeasures to side channel analysis and fault attacks are a major stake in information security.

The main objective of the PHISIC workshop is to provide an environment for exchange among academic and industrial stakeholders of the embedded security arena, more precisely to:

- Share ideas and exchange on the latest trends in terms of academic research, collaborative funded (ANR, EU FP7, FUI…) projects and industrial challenges.
- Identify security trends for the next 5 years.
- Exchange on advanced practices in fault injection and side channel analysis.
- Define the future challenges in embedded security
- Initiate strong European cooperation

This workshop is supported by the "**Secured Communicating Solutions**" cluster and the French National Research Agency **ANR**. The attendees will be given an opportunity to visit the MicroPackS™ mutualised security platform (https: //ssl.arcsis.org/cimpaca.html). This platform hosts six laboratories equipped for state-of-the-art hardware security characterizations.

TOPICS

- Side channel attacks and countermeasures
- Cryptographic processors and co-processors
- Tools and Methodologies
- Security Applications
- Security Trends of Novel Technologies
- Hardware tamper resistance
- Fault attacks and countermeasures
- Hardware accelerators for security
- Software implementations

Short Presentation Abstract submission

Authors are invited to submit a short abstract of 1 page via the Abstract Submission System. The authors of the selected abstracts will be given the opportunity to present their work during the presentation session of PHISIC workshop. The presentations should be in English. They will be 15 minutes long. Observe that presenting does not prevent future or concurrent submission to any journal or conference with proceedings.