

PHISIC 2015

Workshop on Practical Hardware Innovation in Security and Characterization

18th and 19th of May 2015

Centre Microélectronique de Provence

phisic2015.emse.fr

Call for Participation and talks

Committee

Philippe Maurine

philippe.maurine@cea.fr

Anne-Lise Ribotta

ribotta@emse.fr

Assia Tria

Assia.tria@cea.fr

Topics

Side Channel Attacks

Fault Attacks

SW and HW countermeasures

Counterfeiting and Hardware

Trojans

Cryptographic algorithms and
related implementations

New technologies for secure
devices, systems and cyber-
physical systems

Presentation or Poster Submission

Speakers 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 its work during the presentation or poster session of PHISIC. Presentations (25min) or posters should be in English.

Submission deadline

April 3th, 2015

Notification

April 17th, 2015

PHISIC 2015 (18th and 19th of May 2015)

Workshop on Practical Hardware Innovations in Security Implementation and Characterization

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, implementation's vulnerability (from devices to cyber-physical infrastructures) to Physical Attacks is one of the most important threatening a plethora of applications managing users' authentication, data confidentiality and privacy.

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

- Share ideas and exchange on the latest trends in terms of academic research, collaborative funded (H2020, FUI, ANR ...) projects and industrial challenges.
- Identify security trends for the next 5 years.
- Exchange on advanced practices in physical and cyber-physical security threats
- 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**.

Contact and questions: philippe.maurine@cea.fr ribotta@emse.fr