Hardware security is becoming increasingly important for many embedded systems applications and it is expected to increase in the upcoming decades as secure applications will keep growing. The vulnerability of electronic devices that implement cryptography functions has become the Achille’s heel in the last decade: fraudulent manipulations on the hardware implementing security algorithms can allow extracting confidential information, and new threats have menaced secure devices and the security of the manufacturing process. This training school aims at providing theoretical and practical lectures on topics related to hardware security.

Lectures
• Introduction to Hardware & Software security
• Manufacturing test of secure devices
• Trustworthy manufacturing of integrated circuits
• Fault attacks and countermeasures
• FPGA security
• Implementation attacks and countermeasures

Practical Sessions
• True Random Number Generators for Cryptography
• Differential Power Analysis for Beginners

IEEE sessions
• Computer Technology and Cryptography from the Ancient Past
• First Time on Interview: The Good, the Bad and the Ugly

PhD Session

Registration fee:

<table>
<thead>
<tr>
<th></th>
<th>Early: Until June 10</th>
<th>Late: From June 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Registration</td>
<td>€500</td>
<td>€600</td>
</tr>
<tr>
<td>Lectures+practical</td>
<td>€500</td>
<td>€600</td>
</tr>
<tr>
<td>sessions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lectures-Only</td>
<td>€400</td>
<td>€500</td>
</tr>
</tbody>
</table>

Available grants: Based on the availability of COST Action TRUDEVICE funding, students will be eligible for a grant to cover travel and accommodation.

In case of limited budget availability, the selection of beneficiaries will be based on the following criteria:
1) Young researchers (Master thesis / Ph.D. students)
2) First come first serve (date of registration)

Lecturers
• Lejla Batina, Radboud University Nijmegen
• Lilian Bossuet, University of Saint-Etienne
• Jiri Bucek, Czech Technical University in Prague
• Ricardo Chaves, University of Lisbon
• Amine Dehbaoui, SERMA Technologies
• Milos Drutarovsky, Technical University of Kosice
• Viktor Fischer, Jean Monnet University Saint-Etienne
• Julien Francq, AIRBUS Defense & Space
• Ilya Kizhvatov, RISCURE
• Patrick Haddad, STMicroelectronics and Jean Monnet University Saint-Etienne
• Vincent van der Leest, Intrinsic-ID
• Victor Lomné, Agence nationale de la sécurité des systèmes d’information (ANSSI)
• Nele Mentens, KU Leuven
• Giorgio Di Natale, LIRMM
• Martin Novotny, Czech Technical University in Prague
• Paul-Henri Pugliesi-Conti, NXP Semiconductors
• Francesco Regazzoni, AlAri Institute of University of Lugano
• Nicolas Sklavos, KNOSSOSNet Research Group, Technological Educational Institute of Western Greece

General Chair: Ricardo Chaves


Organizing Committee: Hector Pettenghi, Nuno Roma, Nuno Santos, Pedro Tomás

This training school is organized in the framework of the COST Action IC1204 - TRUDEVICE