TRUDEVICE 2014
14-18 July, 2014, Lisbon Portugal
Training School on Trustworthy Manufacturing and Utilization of Secure Devices
### Program Schedule

<table>
<thead>
<tr>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00 - 09:30 Registration</td>
<td>Security Evaluation Techniques</td>
<td>Manufacturing test of secure devices</td>
<td>IEEE Session B</td>
<td>Introduction PhD Session</td>
</tr>
<tr>
<td>09:30 - 10:00</td>
<td>Introduction Session</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00 - 10:30 Opening Session</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:30 - 11:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00 - 11:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:30 - 12:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00 - 12:30</td>
<td>Lunch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:30 - 13:00</td>
<td>Lunch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:00 - 13:30</td>
<td>Lunch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:30 - 14:00</td>
<td>Fault attacks and countermeasures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:00 - 14:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:30 - 15:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:00 - 15:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:30 - 16:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:00 - 16:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:30 - 17:00</td>
<td>Social Event Walk around Lisbon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17:00 - 17:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17:30 - 18:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18:00 - 18:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18:30 - 19:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19:00 - 19:30</td>
<td>DPA Session</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19:30 - 20:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Technical content

• Lectures
  – 5 main topics:
    • Fault attacks and countermeasures
    • Security Evaluation Techniques
    • Trustworthy manufacturing of integrated circuit
    • Manufacturing test of secure devices
    • FPGA security
    • DPA Session (theoretical background for the DPA practical session)

• Practical sessions
  • Differential Power Analysis for beginners
  • True Random Number Generation for Cryptography

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

• The practical session will take place at the north tower
  – At the Computer Engineering Labs
    • Inside the building follow the signs for directions

  – Participants will be divided into two groups
    • Group 1:
      – Thursday: Differential Power Analysis for beginners
      – Friday: True Random Number Generation for Cryptography
    • Group 2:
      – Thursday: True Random Number Generation for Cryptography
      – Friday: Differential Power Analysis for beginners
Practical sessions

• Practical sessions competition:
  – The groups with the best performance
    • Better TRNG
    • Discover more key bits
    • Take less time to do it
  – Will be awarded with 3 smartfusion, 2 development kits and 3 books
  – Participants cannot:
    • Disconnect the other teams’ computer
    • Bribe the jury
    • Cause physical injuries to the other participants
Poster session

- **Friday Morning**
  - PhD Session Introduction
  - Poster session
    - *present your ongoing work*
      - Using a A1 poster
    - The best presentations will be invited to participate on a book to be published by Springer (under negotiation)
      - *Selection will be made by the TRUDEVICE 2014 Program Committee*
    - Posters can be printed locally
      - *Speak with me for this*
Participation Certificate

- All participants will receive a certification of participation

For a certificate of attendance with a description of the courses taken, for credits at your University, please send us an email.
Coffee breaks

- **Monday:**
  - 9:45 – 10:10
  - 15:30 – 16:00
- **Tuesday:**
  - 10:00 – 10:30
  - 16:00 – 16:30
- **Wednesday:**
  - 10:00 – 10:30
- **Friday:**
  - 10:30 – 11:00

Ginjinha (sour cherry licor)

Pasteis de Belém (egg tart pastry)
Lunches

• Held on the ground floor
  – At the opposite side of the building

• Meal
  – Soup
  – Main dish
    • At least one meat and one fish dish
      » Vegetarian for those who requested it
  – Drink:
    • Water, beer, or juice
  – Desert
  – Coffee
    • Use the colored ticket for the corresponding day
Social Events

• Monday
  – Walkabout Lisbon downtown *(16:30 for the bus)*
    – About 2:30 hours; Use comfortable shoes
  – Dinner
    • “Cervejaria Trindade” [www.cervejariatrindade.pt](http://www.cervejariatrindade.pt/)
      – *Beer house* where we’ll have a nice traditional stake

• Wednesday
  – Site seeing tour *(14:00 for the bus)*
    – Sintra, Cabo da Roca, Cascais, Belém
  – Dinner
      – Wine cellar of Mr. Machado where we’ll have the traditional codfish
    • With Fado singing
Social Events

Monday:

- Trip start at the TRUDEVICE 2014 venue (at 16:30 for the bus)
  - http://goo.gl/3dtuDf
- the bus will take us to “Praça do Comércio” where the walkabout starts
  - http://goo.gl/eGdTaj
- the walkabout will end at “Rua Nova da Trindade”, very near “Bairro Alto” famous for the night life,
- where will have dinner at “Cervejaria Trindade”
  - http://goo.gl/maps/BA6Pv
- there is a bus taking us back to TRUDEVICE venue at 23:00 from “Largo Trindade Coelho”
  - http://goo.gl/9Fwrel
Social Events

Wednesday:

- Trip **start** at the TRUDEVICE 2014 venue (at **14:00** for the bus)
  - [http://goo.gl/3dtuDf](http://goo.gl/3dtuDf)
    - Sintra, Cabo da Roca, Cascais, Belém

- from Belém will go towards “Bairro Alto” to the restaurant
  - [http://goo.gl/LpVds9](http://goo.gl/LpVds9)

- where we’ll have dinner at “Adega do Machado”
  - [http://goo.gl/maps/LJ3j1](http://goo.gl/maps/LJ3j1)

- there is a **bus** taking us **back to TRUDEVICE venue at 23:00** from “Largo Trindade Coelho”
  - **Same location as Monday**

[http://goo.gl/maps/dpiIT](http://goo.gl/maps/dpiIT)
Social Events

Returning from “Bairro Alto” by yourselves 😊

- Take the subway station at Baixa / Chiado
  - blue line

- Change at Marquês do Pombal
  - yellow line

- Exit at Saldanha towards the university/hotel
  » http://goo.gl/3dtuDf
Special Thanks

- To the local committee
- The organizing and program committee
- The lectures
- The students who helped glue everything
- TRUDEVICE COST action and Giorgio Di Natale
- The sponsors
There is a Contact.txt file in the USB pen with a small contact list:

- Taxi
- Restaurants
- Mine

**VERY IMPORTANT:**

- sign the presence list every day *specially those with a grant*
  - at the TRUDEVICE reception desk
Portuguese words

- Thank you
- Hello
- Beer
- I want more
- Have fun
- Obrigado
- Olá
- Cerveja
- Quero mais
- Divirtam-se