SECURE-IC
THE SECURITY SCIENCE COMPANY

ADVANCED TRAININGS

EVALUATING SECURITY DURING IC DESIGN

Learn advanced analysis methods with Secure-IC experts, using Analyzr™, Virtualyzr™ and Catalyzr™ tools.

REGISTRATION

For further information and registration, please contact us at:

contact@secure-ic.com

or +33 2 99 12 18 78

Payment of registration fees is required to grant the participation

VENUE

AT SECURE-IC HQ:

15, Rue Claude Chappe
ZAC des Champs Blanc
35510 Cesson-Sévigné

PROGRAM

Day #1: Symmetric crypto analysis

- AES with protections in software and in hardware (theory)
- Known attacks: SPA, DPA, LRA, collision attacks, machine-learning, etc. (theory)
- Pre-silicon analysis (lab)
- Post-silicon analysis (lab)
- Analysis of design improvement (lab)

Day #2: Asymmetric crypto analysis

- RSA with protections, as a mixture of firmware + hardware arithmetic accelerator (theory)
- Known attacks: SPA (conditional tests, extra-reductions, etc.), DPA, machine-learning (clustering), etc. (theory)
- Pre-silicon analysis (lab)
- Post-silicon analysis (lab)
- Analysis of design improvement (lab)

Day #3: Microarchitectural attacks (cache timing, incl. Spectre, etc.)

- Post-quantum algorithm (theory)
- Known attacks: cache-timing attacks (theory)
- Static and dynamic analysis (lab)
- Analysis of design improvement (lab)
- Wrap-up: feedback about the program & the tools, the balancedness between theory/design/evaluation, suggestion of new topics

INFOS

- **It is preferred that attendees bring their own laptop for the lab.**
- **Coffee breaks & lunch are included**
- **Limited number of participants**

> For whom: designer of ASIC and FPGA solutions aiming at understanding security issues with respect to Software, Hardware and Mixed design.

> Some custom sessions to explain a breakthrough topic or created from Secure-IC off-the-shelf courses or.

> There are four regular sessions per year (April / June / September / November).

One day, security will be worth more than the devices