

SECURE-IC

One-day tutorial with hands-on labs

Singapore - 25th April 2018

Evaluating SECURITY DURING IC-design: use-cases

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

150 EUR / 230 SGD

Venue

SECURE-IC premises in Singapore:

#05-04, 1, Fusionopolis Way
138632, Singapore

Program

- ISO/IEC 17825 test methodology
- Vulnerabilities of hardware and software AES implementation:
 - Correlation power analysis
 - Linear regression analysis
 - Collision attacks
 - Lab: analysis of an AES White Box Cryptography (WBC) implementation
- Vulnerabilities of a software RSA implementation:
 - Advanced post-processing for Timing/Horizontal analysis
 - Vertical analysis
 - Lab: using machine learning techniques to extract a secret exponent
- Vulnerabilities of Classical and Post-quantum Cryptography Implementation:
 - Cache timing analysis
 - Static analysis of source code
 - Dynamic analysis of source code
 - Lab: patch vulnerability and re-check

Secure-IC proposes MORE TUTORIALS on www.secure-ic.com

PRACTICAL INFOS

- For the lab sessions, it is preferred that participants bring their own laptop
- Coffee breaks & lunch are included
- Limited number of participants

An event collocated with:

9th International Workshop on Constructive Side-Channel Analysis and Secure Design

COSADE 2018

Singapore

23th - 24th April 2018



www.cosade.org/sq2018

