COSADE '2017

TELECOM ParisTech

WELCOME TO

Organisation

- http://cosade.org
- WIFI access:
  - Indications in the goodies bag
- Proceedings : USB key
  - At the top of the pen in the goodies bag
- Coffee an lunch
  - Go downstairs in room « E200 » to the left of the main entrance

Participants

- 82 people:
  - 66 registered + 16 sponsors/invited
- 15 countries:
  - Europe, middle east

    France, Germany, Belgium, Netherlands, UK, Poland, Austria, Israël, Switzerland,
  - America

    USA, Canada
  - Asia

    Japan, South Korea, China, Singapore

Social event

- Dinner and Cruise in a "Bateau Mouche"
- 2 metro tickets in the badge holder
- Indications in the goodies bag
- How many vegetarian meals ?

IMPORTANT :
19:45 at last at the departure platform

Pier number 5 at “Port de la Conférence”.

Boat: “Le Zouave”.

TELECOM ParisTech

Thanks the sponsors

SECURE-IC
THE SECURITY SCIENCE COMPANY

riscure
Challenge your security

ALPhA NOV
Optics & Lasers Technology Center

NewAE
Technology

INVIA
Secure Semiconductor IP

You are invited to visit their exhibition Booth during the breaks

Program Day 1

Thursday April 13

Conference at Télécom ParisTech

08:00	***Registration Opens***
08:45 09:00	***Welcome, Opening Remarks***
09:00 - 10:30	***Session 1: Side-Channel Attacks and Technological Effects*** ***Session chair: Naofumi Homma***
09:00	Does Coupling Affect the Security of Masked Implementations? Thomas De Cnudde, Begül Bilgin, Benedikt Gierlichs, Ventzi Nikov, Svetla Nikova and Vincent Rijmen.
09:30	Scaling Trends for Dual-Rail Logic Styles against Side-Channel Attacks: a Case-Study Kashif Nawaz, Dina Kamel, Francois-Xavier Standaert and Denis Flandre.
10:00	Dissecting Leakage Resilient PRFs with Multivariate Localized EM Attacks - A Practical Security Evaluation on FPGA Florian Unterstein, Johann Heyszl, Fabrizio De Santis and Robert Specht.
10:30 11:00	***Coffee break***
11:00 - 12:00	***Invited Talk I*** ***Session chair: François-Xavier Standaert***
	Overview of fault based cryptanalysis on block ciphers Victor Lomné
12:00 14:00	***Lunch break***
14:00 - 15:30	***Session 2: Side-Channel Countermeasures*** ***Session chair: Jens-Peter Kaps***
14:00	Toward More Efficient Tamper-Resistant AES Hardware Architecture Based on Threshold Implementation Rei Ueno, Naofumi Homma and Takafumi Aoki
14:30	Enhanced Elliptic Curve Scalar Multiplication Against Side Channel and Safe Error Jeremy Dubeuf, David Hely and Vincent Beroulle
15:00	Yet Another Way Toward Power-Equalized Design in FPGAs Maik Ender, Alexander Wild and Amir Moradi
15:30 16:00	***Coffee break***
16:00 - 17:00	***Session 3: Algorithmtic Aspects in Side-Channel Attacks*** ***Session chair: Benoît Feix***
16:00	On the Construction of Side-Channel Attack Resilient S-boxes Liran Lerman, Nikita Veshchikov, Stjepan Picek and Olivier Markowitch
16:30	Efficient Conversion Method from Arithmetic to Boolean Masking in Constrained Devices Yoo Seung Won and Dong-Guk Han
19:00 - 23:00	***Social Event (see instructions here)***

Program Day 2

Friday April 14

Conference at Télécom ParisTech

09:00 - 10:30	***Session 4: Side-Channel Attacks*** ***Session chair: Benoît Gérard***
09:00	**Side-Channel Analysis of Keymill** Christoph Dobraunig, Maria Eichlseder, Thomas Korak and Florian Mendel
09:30	**On the Easiness of Turning Higher-Order Leakages into First-Order** Thorben Moos and Amir Moradi
10:00	**Side-Channel Attacks Against the Human Brain: the PIN Code Case Study** Joseph Lange, Clément Massart, André Mouraux and Francois-Xavier Standaert
10:30 11:00	***Coffee break***
11:00 - 12:00	***Invited Talk II*** ***Session chair: Yannick Téglia***
	Securing SoCs in advanced technologies Philippe Maurine
12:00 14:00	***Lunch break***
14:00 - 15:00	***Session 5: Fault Attacks*** ***Session chair: Pierre-Yvan Liardet***
14:00	**Low-cost Setup for Localized Semi-invasive Optical Fault Injection Attacks - How Low Can We Go?** Oscar Guillen, Michael Gruber and Fabrizio De Santis
14:30	**DFA on LS-Designs with a Practical Implementation on SCREAM** Benjamin Lac, Anne Canteaut, Jacques Fournier and Renaud Sirdey
15:00 - 15:30	***Session 6: Embedded Security*** ***Session chair: Jean-Luc Danger***
15:00	**Multiple-Valued Debiasing for Physically Unclonable Functions and Its Application to Fuzzy Extractors** Manami Suzuki, Rei Ueno, Naofumi Homma and Takafumi Aoki
15:30 16:00	***Coffee break***
16:00 - 17:00	***Session 7: Side-Channel Tools*** ***Session chair: Guillaume Barbu***
16:00	**Getting the Most Out of Leakage Detection - Statistical tools and measurement setups hand in hand** Santos Merino Del Pozo and Francois-Xavier Standaert
16:30	**Mind the Gap: Towards Secure 1st-order Masking in Software** Kostas Papagiannopoulos and Nikita Veshchikov
17:00 17:05	***Closing Remarks and Farewell***

Statistics

General Statistics

Submissions	30
Accepted	16
Acceptance rate	0.53
Reviews	90
External reviewers	39
External reviews	42

Reviewing

reviews for a paper	number of papers
3	30

Statistics by Country

country	authors	submitted	accepted	acceptance rate	PC members
Austria	4	1.00	1.00	1.00	1
Belgium	17	5.25	5.25	1.00	1
China	8	2.00	0.00	0.00	-
France	12	4.00	2.00	0.50	8
Germany	24	8.00	4.00	0.50	6
India	-	-	-	-	1
Italy	-	-	-	-	1
Japan	8	3.00	2.00	0.67	2
Korea	3	2.00	1.00	0.50	-
Luxembourg	-	-	-	-	1
Netherlands	1	0.50	0.50	1.00	-
Singapore	-	-	-	-	1
Switzerland	1	0.25	0.25	1.00	1
USA	11	4.00	0.00	0.00	2
United Kingdom	-	-	-	-	1

COSADE '2017

TELECOM ParisTech

Program Committee (26)

- Shivam Bhasin
- Christophe Clavier
- Hermann Drexler
- Cécile Dumas
- Thomas Eisenbarth
- Wieland Fischer
- Christophe Giraud
- Johann Groszschaedl
- Sylvain Guilley
- Benoît Gérard
- Tim Güneysu
- Johann Heyszl
- Naofumi Homma
- Michael Hutter
- Thanh Ha Le
- Kerstin Lemke-Rust
- Houssem Maghrebi
- Marcel Medwed
- Amir Moradi
- Debdeep Mukhopadhyay
- Stjepan Picek
- Francesco Regazzoni
- Matthieu Rivain
- Kazuo Sakiyama
- Ruggero Susella
- Carolyn Whitnall

External Reviewers (25)

- Yves Bocktaels
- Jakub Breier
- Samuel Burri
- Eleonora Cagli
- Anupam Chattopadhyay
- Guillaume Dabosville
- Alessio Davide
- Elke De Mulder
- Soumyajit Dey
- Daniel Dinu
- Vincent Grosso
- Bernhard Jungk
- Yann Le Corre
- Sikhar Patranabis
- Christian Pilato
- Emmanuel Prouff
- Bastian Richter
- Sayandeep Saha
- Tobias Schneider
- Marc Stöttinger
- Robert Szerwinski
- Michael Tunstall
- Praveen Kumar
- Vadnala
- Felipe Valencia
- Dai Yamamoto

Thank you for your hard work !

Proceedings

Revised papers to appear in :

- Springer Verlag, Lectures Notes in Computer Science