
Institut
Mines-Télécom

# DPA contest v4

**COSADE**
**April 14–15, 2014**
**Paris, France**

Guillaume DUC, Sylvain GUILLEY, Laurent SAUVAGE, Jean-Luc DANGER, Tarik GRABA, Yves MATHIEU and Renaud PACALET

April 14–15, 2014

# DPA contests

- Organized by Télécom ParisTech
- History
  - v1 : attack contest, hardware implementation of DES on an ASIC
  - v2 : attack contest, hardware implementation of AES on a FPGA
  - v3 : acquisition contest, hardware implementation of AES on a FPGA (organized by AIST)
  - v4 : attack contest, protected implementation of AES (hardware and/or software)

# DPA contests

- Purpose
  - In addition to the “contest”, DPA contests are often used as a benchmarking tool and for educational purpose
  - If you use the DPA contests traces/results/..., we would be pleased to know
- To improved scientific return on investment, a collaborative article on attack submitted to the v2 has been published in JCEN (DOI : 10.1007/s13389-014-0075-9)

# DPA contest v4

## Introduction

- Attack contest (like v1 and v2)
- Several different protected implementations of AES
- Traces from a reference acquisition campaign are published on our website for each implementation (like in v1 and v2)
- Measurements performed using the SASEBO-W board
- All details of the implementations are given to allow participants to perform their own acquisitions (like in v3)
- ... (hopefully) reactive support to questions !

# DPA contest v4

## First implementation (4.1)

- Published in July 2013
- AES-256 RSM software implementation on ATmega163 smartcard
- 30 attacks submitted from 10 countries
- Several profiled attacks manage to extract the key within (in average) one trace !

# DPA contest v4

## Participants (4.1) — 1/2

- Liran Lerman (Université Libre de Bruxelles), Belgium
- Benoît Gérard (DGA), France
- Amir Moradi (RUB), Germany
- Zheng Kanghong (DSO National Laboratories) & Sebastian Kutzner (Nanyang Technological University), Singapore
- Tang Ming, Qiu Zhenlong, Peng Hongbo, Wang Xin, Li Yanbin, Xiang Xiao, Chen Xiaobing, Chen Zhenling (School of Computer, Wuhan University), China
- Heorhi Liasneuski, Stanislau Piatrusha (Belarusian State University), Belarus
- Liu Junrong, Guo Zheng, Sui Yijie, Shen Xiangxiang, Wang Weijia, Xu Sen, Bao Sigang (Shanghai Jiao Tong University), China
- Yongbin Zhou, Lin Meng, Hailong Zhang, Yingxian Zheng, Mingliang Feng, Guangjun Fan (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences), China

# DPA contest v4

## Participants (4.1) — 2/2

- Ofir Weisse, Yossi Oren, Avishai Wool (Cryptography and Network Security Lab, Tel-Aviv University), Israel
- Anonymous (K)
- Frank Schuhmacher (Segrids), Germany
- Hideo Shimizu (Toshiba Corporation Corporate Research & Development Center), Japan
- Xavier Bodart, Liran Lerman (Université Libre de Bruxelles), Belgium
- Alexander DeTrano, Xiaofei Guo, Naghmeh Karimi (NYU Polytechnic School of Engineering), United States of America
- Tsunato Nakai, Daiki Tsutsumi, Takaya Kubota, Mitsuru Shiozaki, Takeshi Fujino (Ritsumeikan University), Japan
- D-G Han, Y-R Lee, B-Y Sim, H-Y Kim, H-J Ahn, Y-S Won, S-J Lee (SICADA (SIde Channel Analysis Design Academy), Kookmin University), South Korea
- Zdenek Martinasek, Ondrej Zapletal (Faculty of Electrical Engineering and Communication, Brno University of Technology), Czech Republic

# DPA contest v4

## Results (4.1)

### Non profiling

- **Alexander DeTrano, Xiaofei Guo, Naghmeh Karimi** (NYU Polytechnic School of Engineering, United States of America) : **19 traces**
- **Tsunato Nakai, Daiki Tsutsumi, Takaya Kubota, Mitsuru Shiozaki, Takeshi Fujino** (Ritsumeikan University, Japan) : **43 traces**
- **Zheng Kanghong** (DSO National Laboratories, Singapore), **Sebastian Kutzner** (Physical Analysis and Cryptographic Engineering (PACE), Temasek Laboratories, Nanyang Technological University, Singapore) : **78 traces**

# DPA contest v4

## Results (4.1)

### Profiling

- **Frank Schuhmacher** (Segrids, Germany) : **1 trace**
- **Hideo Shimizu** (Toshiba Corporation Corporate Research & Development Center, Japan) : **1 trace**
- **Yongbin Zhou, Lin Meng, Hailong Zhang, Yingxian Zheng** (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China) : **2 traces**

# DPA contest v4

## New implementation (4.2)

### Functional changes

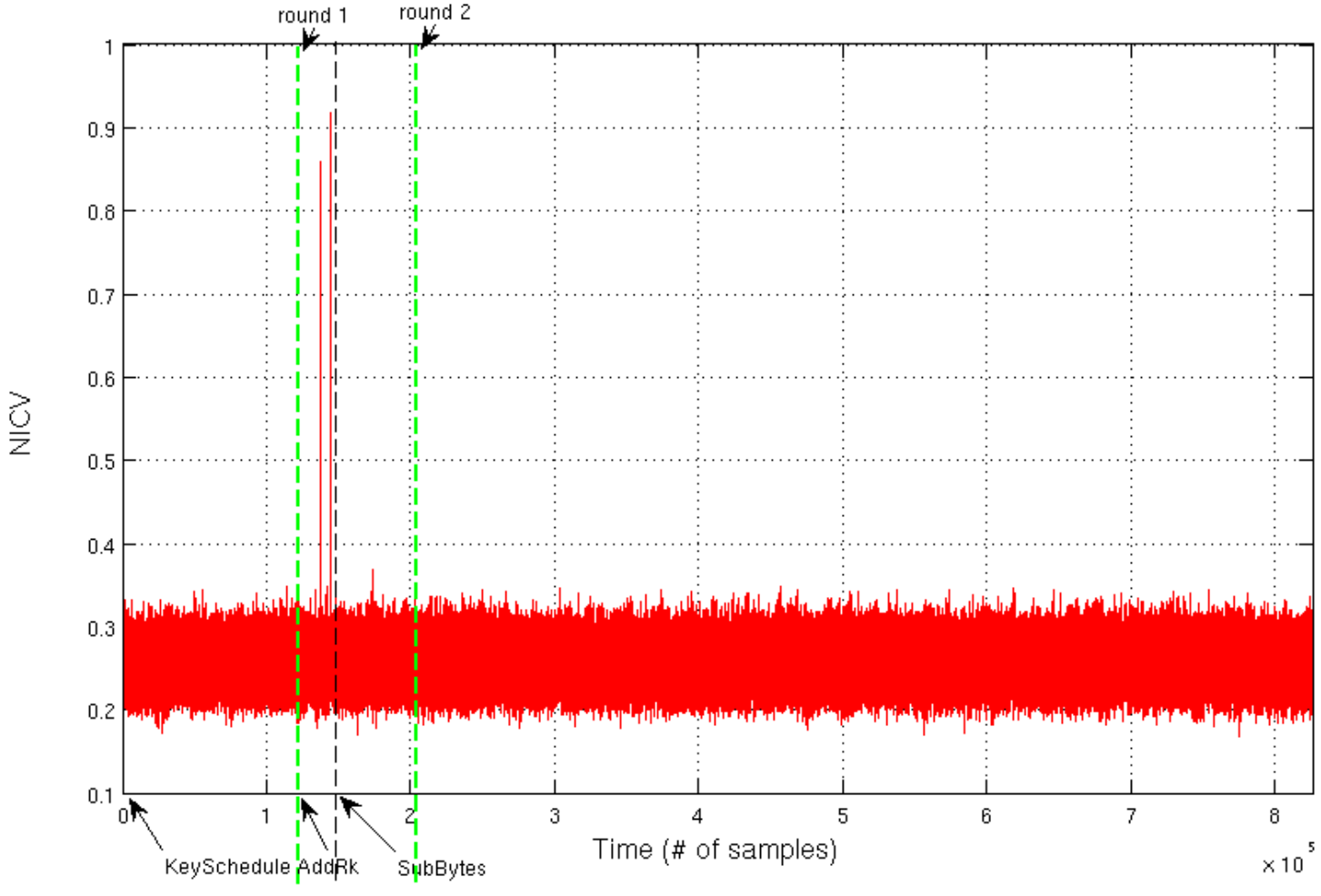
- AES-128, easier to attack (one round key yields the master key)
- Optimized in speed (ASM, inspired from RijndaelFurious) : the whole AES in each trace

### Security changes

- Still RSM (16 values for the per-byte mask), i.e., a LEMS.
- But with one mask per sbox (to thwart collision attacks),
- and a shuffling (to thwart 2O-CPA based on recombinaison).

# DPA contest v4

## New implementation (4.2)




NICV (Normalized Inter-Class Variance)

# DPA contest v4

## New implementation (4.2)

- Acquisitions (32 keys with 1,000 traces for each key) have been completed last week
- Will be available on the website at the end of April / beginning of May

# DPA contest v4

## New implementation (4.3)

- “Unbreakable” implementation in FPGA proposed by Amir Moradi (Ruhr-Universität Bochum)
  - AES-128
  - SPARTAN-6 FPGA (SAKURA-G)
  - Round-bases architecture (all 16 Sboxes in parallel)
  - Boolean masking
  - BRAM scrambling (Generic Side-Channel Countermeasures for Reconfigurable Devices. CHES 2011)
  - Power measurements, 1GS/s, 20 million traces
- Will be available latter this year

# Stay tuned !

- Website (`http://www.dpacontest.org`)
- Twitter account : DPAContest