Institut
Mines-Télécom

DPA contest status

COSADE
April 13–14, 2015
Paris, France

Jean-Luc DANGER, Guillaume DUC, Sylvain GUILLEY, Zakaria NAJM, Laurent SAUVAGE
April 13–14, 2015

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, Japan)
  - V4 : attack contests, protected implementation of AES :
    - V4.1 protected SW AES implementation
    - V4.2 better protected SW AES implementation
    - to be soon launched : V4.3 : protected HW AES implementation
  - under study : V5

DPA contest Purpose

- Benchmarking
- Education
- Publications
  - JCEN article with the V2 results (DOI : 10.1007/s13389-014-0075-9)
  - thank you to cite the dpacontest website http ://www.dpacontest.org

You are invited to use the DPA contest traces !

DPA contest V4

Introduction

- Attack contest
- Several different protected implementations of AES
- Traces from a reference acquisition campaign are published on the website for each implementation
- Measurements performed using the SASEBO-W board
- Description of the implementations (code for SW)
- (hopefully) Reactive support to questions !

DPA contest V4.1

- 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 V4.1 participants 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 V4.1 participants 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
- Li Yang, Wang Weiqi, Zhang Chi (Shanghai Fudan Microeletronics Group Company Limited), China

DPA contest V4.1 Results 1/2

Non profiling

- Anonymous : **15 traces**
- **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**

DPA contest V4.1 Results 2/2

Profiling

- **Frank Schuhmacher** (Segrids, Germany) : **1 trace**
- **Hideo Shimizu** (Toshiba Corporation Corporate Research & Development Center, Japan) : **1 trace**
- **Yongbin Zhou, Yingxian Zheng, Hailong Zhang, Guangjun Fan, Lin Meng** (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China) : **1 trace**
- **Li Yang, Wang Weiqi, Zhang Chi** (Shanghai Fudan Microeletronics Group Company Limited, China) : **1 trace**

DPA contest V4.2

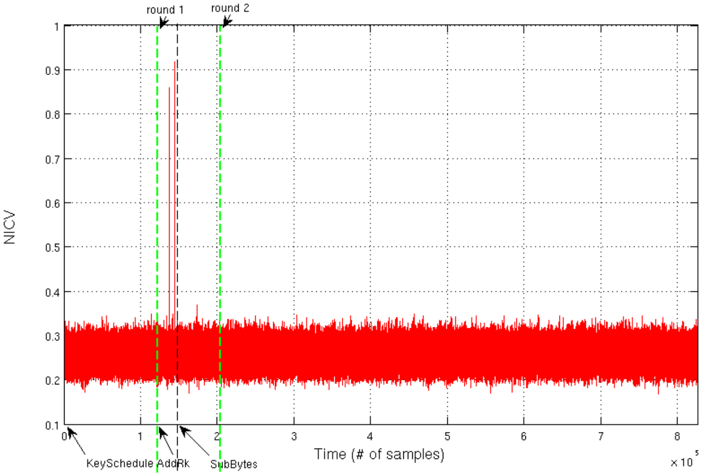
Functional changes

- 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 mask shuffling between rounds.

DPA contest V4.2 1st order leakage points



NICV (Normalized Inter-Class Variance)

DPA contest V4.2 new traces

- Acquisitions (32 keys with 1,000 traces for each key) has been published in September 2014
- However, a bug has been discovered : the Shuffle10 used in the last round is not properly applied (Shuffle0 is applied instead)
- New acquisitions have been performed (with 5,000 traces for each key) and will be published soon (they are currently being processed for publication)

DPA contest V4.2 participants

- Anonymous (2 attacks)
- Liu Junrong, Guo Zheng, Zhang Chi, Xu Sen, Wang Weijia, Bao Sigang (SJTU-SHHIC Co-Lab of Data Security and Protection, Shanghai Jiao Tong University), China
- Tsunato Nakai, Daiki Tsutsumi, Mitsuru Shiozaki, Takaya Kubota, Takeshi Fujino (Ritsumeikan University), Japan
- Yang, Wang Weiqi, Zhang Chi (Shanghai Fudan Microeletronics Group Company Limited), China

NEW : DPA contest V4.3

- FPGA-based implementation of 1st-order Boolean masking
- In cooperation with Ruhr-Universität Bochum, Germany
  - The scrambled-BRAM design of the COSADE'15 talk "Side-Channel Protection by Randomizing Look-Up Tables on Reconfigurable Hardware" : Sasdrich et al.
  - AES-128
  - Round-bases architecture (all 16 Sboxes in parallel)
  - 256 clock cycles for the mask update
  - 20 clock cycles for the masked encryption
  - SPARTAN-6 FPGA (SAKURA-G)
  - Power measurements, 20 million traces
  - 1st-order resistance examined by non-specific *t*-test
  - 2nd-order vulnerability is expected
- Will be available June-July 2015

Stay tuned !

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