DPA contests

Guillaume Duc, Sylvain Guilley, Laurent Sauvage, Florent Flament, Maxime Nassar, Nidhal Selmane, Jean-Luc Danger, Tarik Graba, Yves Mathieu & Renaud Pacalet
< contact@DPAcontest.org >

Institut Télécom / Télécom ParisTech
CNRS – LTCI (UMR 5141)

CHES 2011, September 2011
Nara, Japan

The DPA contests

CHES'08
August 2008

CHES'09
August 2009

January 2010

COSADE'11
February 2011

DPA contest v1

Attack contest against ASIC implementation of DES

Organized by Télécom ParisTech
Current status: Finished

DPA contest v2

Attack contest against FPGA implementation of AES

Organized by Télécom ParisTech
Current status: Finished

DPA contest v3

Acquisition contest based on SASEBO GII board

Organized by AIST
Current status: Running

DPA contest v4

Attack contest against protected hw or sw AES implementation

Organized by Télécom ParisTech
Current status: Will open in 2011

The DPA contests

Aim

- Fair confrontation of side-channel related techniques (attacks, acquisition techniques, counter-measures)

Organizers

- Initiated by the VLSI research group of Télécom ParisTech (French research center and engineering school)
- Version 3 of the contest is jointly organized with the Japanese National Institute of Advanced Industrial Science and Technology (AIST)
- Inputs from all the cryptographic community about the rules of the contest

DPA contest v1

- Launched during CHES'08 (August 2008), results announced during CHES'09 (August 2009)
- Made it possible for researchers to compare in an objective manner their attack algorithms
- Targeted algorithm: DES implemented in an ASIC
- Participants were provided with a database of consumption traces
- Best attack submitted by Christophe Clavier, affiliated with UNILIM

DPA contest v2

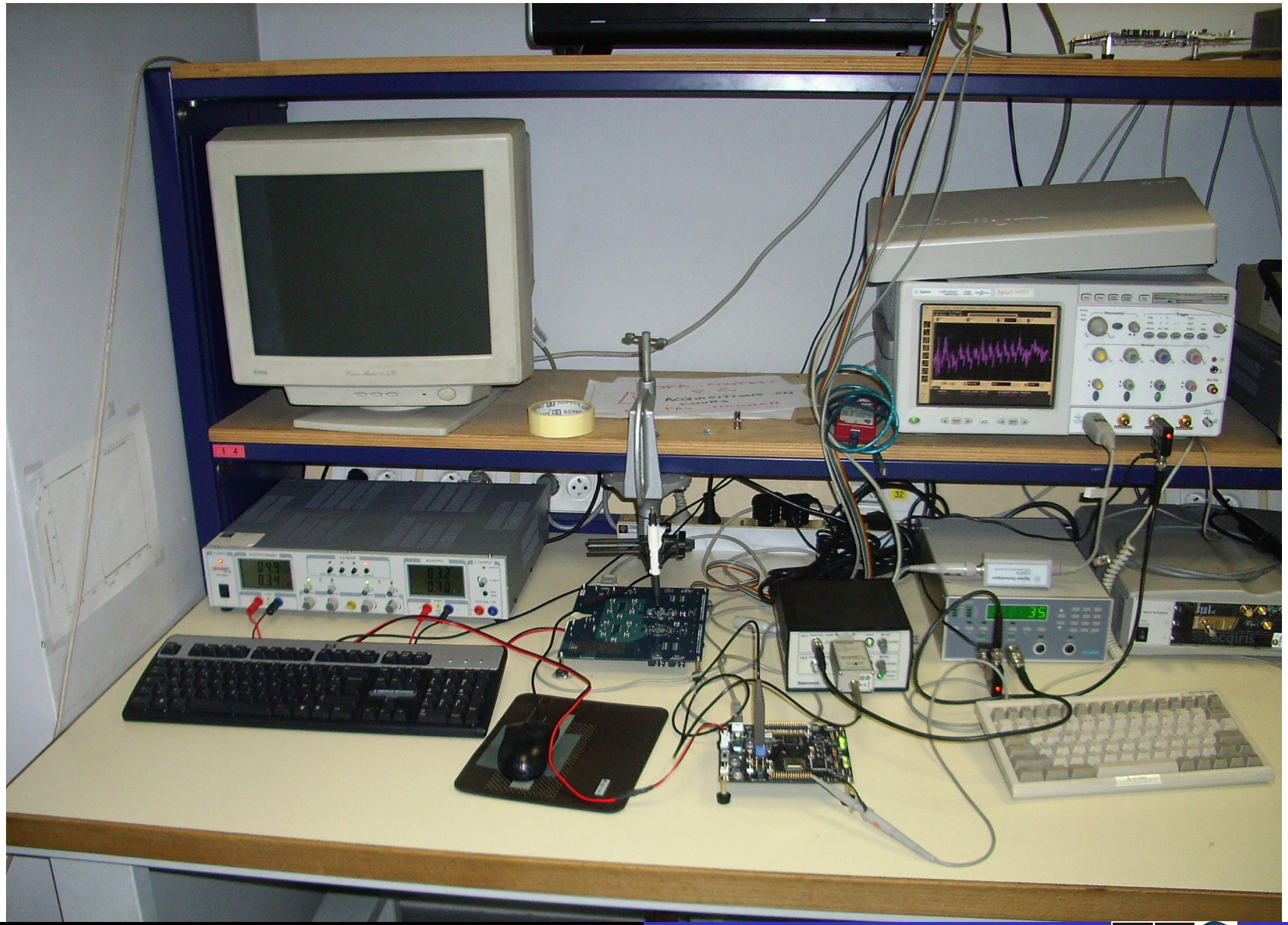
- Same objective as v1 (attack contest)
- Targeted algorithm: AES-128 implemented in a FPGA
- Acquisitions performed on a SASEBO GII board and the full design used for acquisition was provided
- Evaluation using several metrics (based on *A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks*, F.-X. Standaert and T. G. Malkin and M. Yung, Eurocrypt 2009, Lecture Notes in Computer Science, vol 5479, pp 443–461, Cologne, Germany, April 2009)
  - **Global Success Rate**
  - **Partial Success Rate**
  - **Partial Guessing Entropy**

Specificity of this second edition

- Three sets of traces
  - **Training** database: 1,000,000 traces (random keys and plaintexts)
  - **Public** database: 32 $\times$ 20,000 traces (32 random keys and for each key, 20,000 random plaintexts)
  - **Private** database: 32 $\times$ 20,000 traces
- All the traces were acquired under the same conditions

Signal / Noise ratio: ≈ 0.0078 $\Rightarrow$ $\sigma^2 \approx 11.3$.

Acquisition setup



Participants

Author	Affiliation	Attacks #
Thanh-Ha LE	MORPHO, France	2 attacks
Maël BERTHIER	MORPHO, France	1 attack
Alexis BONNECAZE	IML, ERISCS, France	6 attacks
Jeremy ABIHSSIRA & Céline THUILLET	EADS Defence & Security, France	1 attack
Daisuke NAKATSU	University of Electro-Communications, Japan	1 attack
Antoine WURCKER	UNILIM, Faculté des Sciences et Techniques de Limoges, France	2 attacks
Edgar MATEOS	University of Waterloo, Canada	1 attack
Matthieu WALLE	Thales Communications, France	4 attacks
Aziz M. ELAABID	University Paris 8 and Télécom ParisTech	1 attack
Reference attack	Télécom ParisTech, France	1 attack
Olivier MEYNARD	Télécom ParisTech, France	5 attacks
Shiqian WANG	MORPHO, France	1 attack
Maël BERTHIER & Yves BOCKTAELS	MORPHO, France	4 attacks
Victor LOMNÉ	ANSSI, France	1 attack
Aziz EL AABID	Télécom ParisTech, France	1 attack
Annelie HEUSER & Michael KASPER & Werner SCHINDLER & Marc STÖTTINGER	CASED (research group CASCADE), TU Darmstadt, Fraunhofer SIT, Bundesamt für Sicherheit in der Informationstechnik (BSI))	1 attack

Attacks statistics — First submission period

- 20 attacks submitted
  - 17 evaluated
  - 1 segmentation fault
  - 1 does not respect the protocol (and too difficult to adapt)
  - 1 takes too long time to evaluate (quadratic in trace count)
- Languages
  - 11 C or C++
  - 5 Matlab
  - 4 C#
- Execution time
  - Min: < 0.01 s/trace
  - Max: 8.77 s/trace
  - Mean: 1.38 s/trace

Attacks statistics — Second submission period

- 12 attacks submitted
  - 12 evaluated
- Languages
  - 7 C or C++
  - 5 Matlab
- Execution time
  - Min: < 0.01 s/trace
  - Max: 8.59 s/trace
  - Mean: 2.35 s/trace

Results — GSR stable $> 80\,\%$

First submission period

1. Matthieu WALLE (Thales Communications), attack 7T: **7,061** (+ his 3 other attacks)
2. Maël BERTHIER (MORPHO), attack CPA: **15,943**
3. Alexis BONNECAZE (IML, ERISCS), attack SPE: **18,458**

All time

1. Annelie HEUSER & Michael KASPER & Werner SCHINDLER & Marc STÖTTINGER (CASED, TU Darmstadt, Fraunhofer SIT, BSI), Stochastic attack (stochastic approach): **6,729**
2. Matthieu WALLE (Thales Communications), attack 7T: **7,061** (+ his 3 other attacks)
3. Victor LOMNÉ (ANSSI), attack Recursive CPA: **10,666**

Participation per Affiliation

DPA contest v1

- **National agencies**: 0 %.
- **Industry**: 30 %, Mitsubishi, Riscure, Toshiba.
- **Academia**: 70 %, Karlsruhe U., Korea U. CIST, K.U. Leuven, LIRMM, TELECOM-ParisTech, Tohoku U., UNILIM.

DPA contest v2

- **National agencies**: 18 %, ANSSI, BSI.
- **Industry**: 27 %, EADS, Morpho, Thales.
- **Academia**: 55 %, Darmstadt U. IML ERISCS, TELECOM-ParisTech, UEC Japan, UNILIM, Waterloo U.

DPA contest v3

3rd edition

- New objective: Compare acquisition platforms and techniques
- Organized with AIST
- Launched in beginning 2011
- Results will be announced during COSADE 2012 and/or CHES 2012

Rules

- Participants are free to:
  - Modify the design of the control FPGA of the board (the Spartan 3)
  - Use any measurement technique (power, EM...)
  - Use any measurement equipment (EM probe, differential probe, oscilloscope, amplifier...)
  - Use any post-processing function (noise filtering, trace resynchronization...)
- Participant shall not:
  - Modify the AES circuit on the cryptographic FGPA of the board

Invasive methods

Pocket antenna

“Hello Kitty” microscope

Techniques borrowed from other scientific topics

Techniques borrowed from other scientific topics

What's next?

4th edition

- Attack contest
- Organized by Télécom ParisTech
- Still in maturation, Will be launched later in Q4 2011

Ideas?

Several choices are still discussed

- Counter-measure?, one idea:
  - A small number of counter-measures is proposed by a committee of experts
  - Reference traces for each counter-measures implementations are provided to participants
  - Bitstreams are also provided so participants can perform their own acquisition campaigns
- Targeted algorithm
  - Block cipher (AES)

Ideas?

Several choices are still discussed

- Implementation
  - Hardware
  - Software
    - Real processor/micro-controller
    - Smart-card
    - Soft core processor on a FPGA
- Acquisition type
  - Power consumption
  - EM

Longer term vision

Ideas

- Contests are never closed
  - Participants can submit attacks after the official deadline
  - Results will be published on the DPA contest website on a best effort basis
- Traces published (v1, v2 and v4) will stay available for download to allow people to use them to develop and test attacks without needing an acquisition platform
  - The traces provided by the DPA contest can be used (and are currently used) as a "standard" benchmark to evaluate the efficiency of attacks
- Focus on counter-measures in future editions

Acknowledgments

- Philippe Bulens [2]
- Jean-Luc Danger [1]
- Guillaume Duc [1]
- Aziz Elaabid [1]
- Florent Flament [1]
- Sylvain Guilley [1]
- Naofumi Homma [1,3]
- Philippe Hoogvorst [1]
- Olivier Meynard [1,4]
- Frédéric Pauget (and all the IT staff) [1]
- Akashi Satoh [5]
- Laurent Sauvage [1]
- François-Xavier Standaert [2]
- Nicolas Veyrat-Charvillon [2]

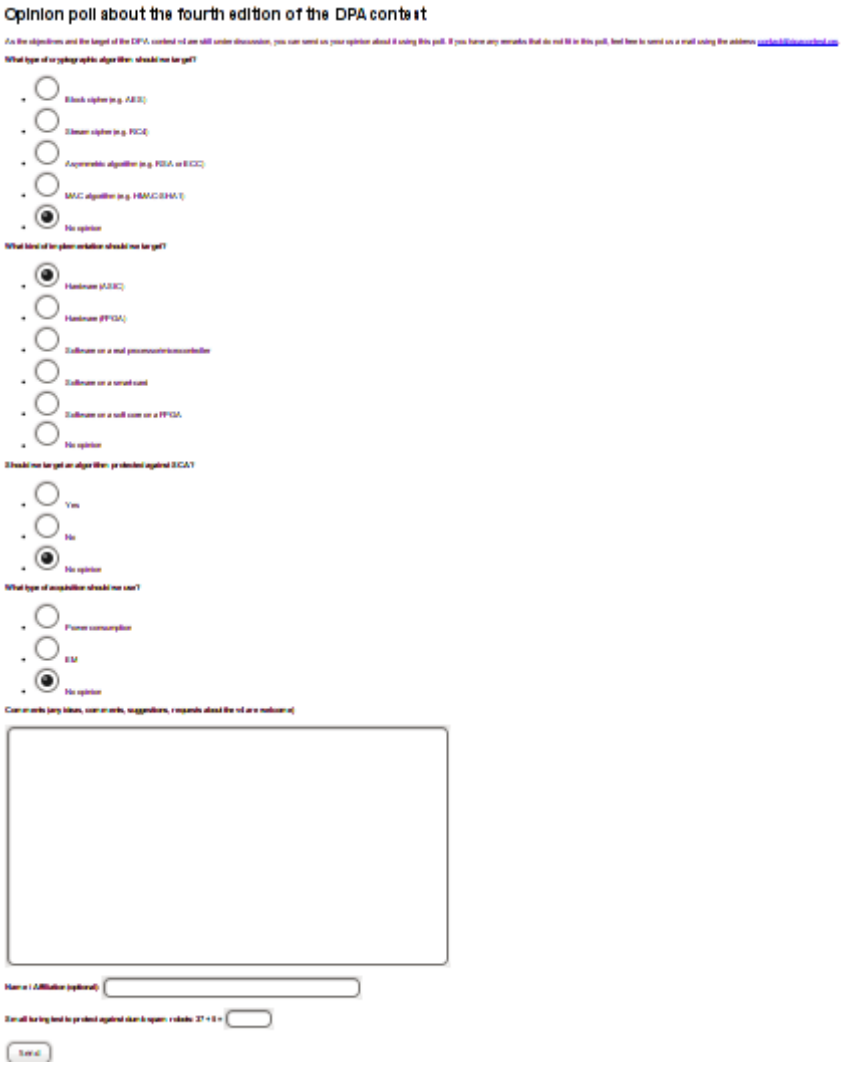
[1] Télécom ParisTech
[2] Université catholique de Louvain
[3] Tohoku University
[4] DGA-MI (formerly CELAR)
[5] National Institute of Advanced Industrial Science and Technology

The DPA contest team

Thank you!

- Thank you for your attention
- Participants to the "DPA contest" V2: we are preparing a common publication. Please stay tuned!

Opinion Poll


Opinion poll about the fourth edition of the DPA contest

- At: http://www.dpacontest.org/v4/
- And more precisely at http://www.dpacontest.org/v4/poll4.php
- Please, take 5 minutes to answer it
- Your feedback is precious for us!