

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)



NIAT 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

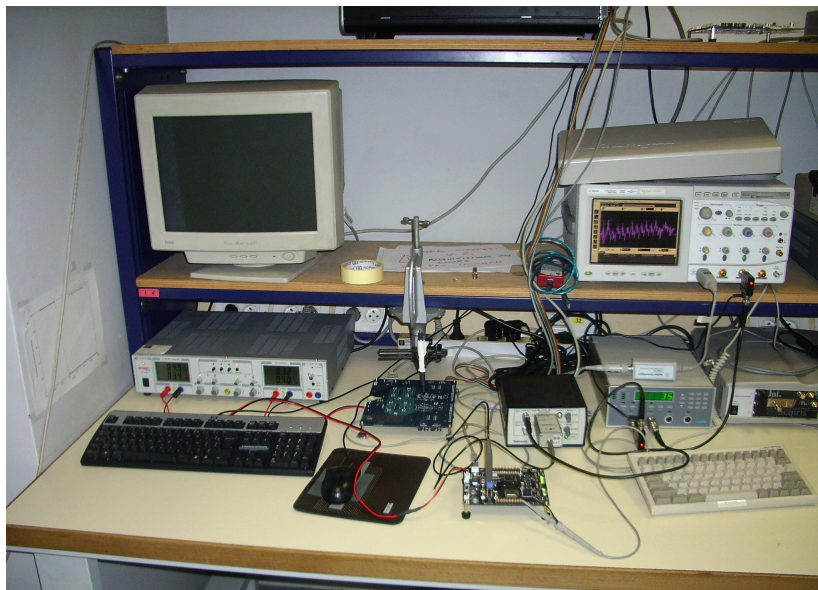
- Same objective as v1 (attack contest)
- Targeted algorithm: AES-128 implemented in a FPGA
- Acquisitions performed on a SASEBO GII board and the full design used for acquisition was provided
- Evaluation using several metrics (based on *A Unified Framework for the Analysis of Side-Channel Key Recovery 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 $\Rightarrow \sigma^2 \approx 11.3$.

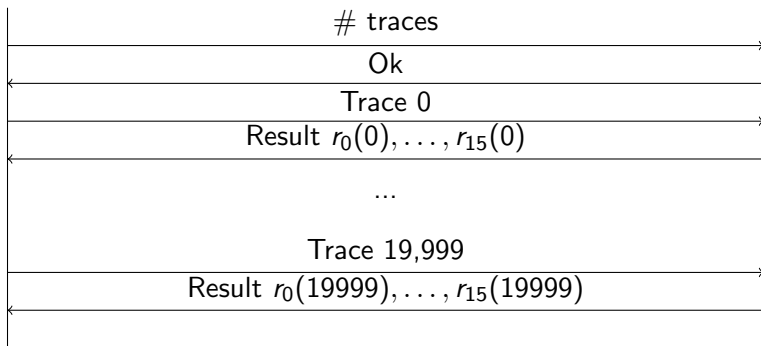
Acquisition setup



Evaluation protocol

Wrapper

Attack



Definition of attack metrics

- On iteration t , the attack receives the trace t and produces the result $r_0(t), \dots, r_{15}(t)$ where $r_s(t)$ is a vector containing the 256 possible values of the byte s of the selected subkey rated according to their likelihood
- Results are averaged over the 32 campaigns (32 keys in the private database), but we will employ notations borrowed from the statistics
- If we denote by $r_s^c(t)$ the result $r_s(t)$ obtained for campaign $c \in [0, 32[$, then the notation $P(r_s^c(t) = x^c)$ stands for the empirical estimation $\frac{1}{32} \sum_{c=0}^{31} \delta(r_s^c(t) = x^c)$
- We also note that the expectation $E(X)$ of a random variable X is defined as: $E(X) = \sum_x x \cdot P(X = x)$
- In the sequel, we therefore forget the index of the campaign c and abridge the notation of $r_s^c(t)$ as $r_s(t)$, considered a random variable

Definition of attack metrics

GSR > 80%	$\operatorname{argmin}_t P(\forall s, r_s(t)[\dot{k}_s] = 0) > 0.80$
Min PSR > 80%	$\operatorname{argmin}_t \min_s P(r_s(t)[\dot{k}_s] = 0) > 0.80$
Max PGE < 10	$\operatorname{argmin}_t \max_s E(r_s(t)[\dot{k}_s]) < 10$
GSR stable > 80%	$\operatorname{argmin}_t \forall t' \geq t, P(\forall s, r_s(t')[\dot{k}_s] = 0) > 0.80$
Min PSR stable > 80%	$\operatorname{argmin}_t \forall t' \geq t, \min_s P(r_s(t')[\dot{k}_s] = 0) > 0.80$
Max PGE stable < 10	$\operatorname{argmin}_t \forall t' \geq t, \max_s E(r_s(t')[\dot{k}_s]) < 10$
GSR @20k	$P(\forall s, r_s(20\,000 - 1)[\dot{k}_s] = 0)$
Min PSR @20k	$\min_s P(r_s(20\,000 - 1)[\dot{k}_s] = 0)$
Max PSR @20k	$\max_s P(r_s(20\,000 - 1)[\dot{k}_s] = 0)$
Min PGE @20k	$\min_s E(r_s(20\,000 - 1)[\dot{k}_s])$
Max PGE @20k	$\max_s E(r_s(20\,000 - 1)[\dot{k}_s])$

How the attacks were evaluated?

- Each attack is evaluated against the 20.000 traces of each 32 keys of the private database (640.000 traces)
- We only have Linux computers so we have converted the attacks if they were developed for Windows
 - C/C++: simple compilation from sources
 - C#: use of Mono (open source .NET implementation)
 - Matlab: compilation using `mcc` (also used to avoid license token problems)
- ~ 2 years of CPU time
- Execution in parallel on up to 16 Linux computers

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

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)
 - Stream cipher
 - Asymmetric algorithm
 - Hash algorithm

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 Bulens²
- Jean-Luc Danger¹
- Guillaume Duc¹
- Aziz Elaabid¹
- Florent Flament¹
- Sylvain Guilley¹
- Naofumi Homma^{1,3}
- Philippe Hoogvorst¹
- Olivier Meynard^{1,4}
- Frédéric Pauget (and all the IT staff)¹
- Akashi Satoh⁵
- Laurent Sauvage¹
- François-Xavier Standaert²
- Nicolas Veyrat-Charvillon²

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



Jean-Luc Danger, Guillaume Duc and Sylvain Guilley

Thank you!

- Thank you for your attention
- An extended discussion follows with a panel of experts

Round Table

Panelists

- Certification bodies:
 - NIST: **Randall J. Easter**
 - ANSSI: **Victor Lomné**
 - AIST: **Akashi Satoh**
- Industry:
 - Oberthur Technologies: **Emmanuel Prouff**
- Academia:
 - K.U. Leuven: **Benedikt Gierlichs**

Questions to the panel and the audience

Not included in the version of the slides presented at NIAT'2011

- The DPA contest: threat of opportunity for the security business?
- Evolution towards a "countermeasures contest": what are the challenges?
- How to bridge the gap between practical and theoretical security analyses?
- Institutionalization of the DPA contest – means to maximize its impact.
- Technical aspects: is diversification interesting? (symmetric vs asymmetric algorithms, HMACs, fault attacks)

Opinion Poll

Opinion poll about the fourth edition of the DPA contest

As the administrator and the support of the DPA, we would like to ask you some questions, you can answer in your opinion about it using this poll. If you have any remarks that do not fit the poll, feel free to send us a mail using the address admin@dpacontest.org

What type of programming algorithm should we target?

- Basic algorithm (e.g. BFS)
- Classic algorithm (e.g. Dijkstra)
- Advanced algorithm (e.g. RMQ, LCA, etc.)
- MLCC algorithm (e.g. RMQ, LCA, etc.)
- No opinion

What kind of problem should we target?

- Hardcore (DPOC)
- Hardcore (DPOC)
- Challenge on a real programming contest
- Challenge on a real contest
- Challenge on a real contest on DPOC
- No opinion

Should we target an algorithm problem against DPA?

- Yes
- No
- No opinion

What type of capabilities should we use?

- Power consumption
- RM
- No opinion

Can you make any ideas, comments, suggestions, remarks about the contest edition of

Name (optional)

Email (optional)

- 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!