Education and open benchmarking on side-channel analysis with the DPA contests

Jean-Luc Danger, Guillaume Duc, Sylvain Guilley and Laurent Sauvage
TELECOM-ParisTech, crypto lab, COMELEC dpt, 75.014 PARIS, FRANCE.
Email: contact@dpacontest.org

Abstract

The DPA contests represent an initiative towards enabling a fair confrontation of side-channel related techniques. The virtues of the contests are manifold: challenging leakage exploitation techniques, putting forward difficulties in side-channel analysis, stimulating the research for sound and practical attack and leakage metrics, *etc.* With time, the contest has moved from a competition to an open platform of knowledge sharing. The initial goal of "breaking as fast as possible" has shown its limits: many strategies can be thought of, and the comparison of attacks depends on the prior assumptions they make about the attacked implementation. Evaluation metrics have now been diversified, and also the side-channel acquisition stage has been taken into account. The past experience of the DPA contests has already taught a lot to the community. However, there still remains many open issues, that will be tackled with in the forthcoming editions. This article gives a quick overview of the DPA contests, and concludes on possible future directions. Of particular importance is the intention to help countermeasures designers in their work.

Keywords: Side-channel metrics, evaluation, comparison of methods, academic research.

Introduction

It is now well known that electronic systems implemented without protection are vulnerable to implementation-level attacks [7]. Notably, the side-channel attacks are of particular concern, as they can be done by adversaries with limited resources, without altering the system (especially when the side-channel is a radiated field [4]). From the embedded system developer's viewpoint, this means that solid countermeasures shall be designed since the system, once in the field, won't be able to adapt its defense as side-channel attacks can be conducted without leaving any evidence.

In this context, the goal of the DPA contests is to provide with an independent and up-to-date evaluation of the threats. Indeed, information about side-channel attacks is available from different communities:

- at the standardization-level (national certification bodies, CC [1], etc.),
- in the specialized industry laboratories,
- in the scientific community (at workshops such as CHES, CARDIS, HOST, COSADE, and many embedded security tracks in other conferences).

Nonetheless, the information shared by these communities can be slightly biased. Caricaturally, standardization organisms might demand too much security, whereas industrial labs might work towards the certification and not against real pirates, and the scientific community can go into sophisticated analysis without detailing practical aspects of attacks.

Thus, we advocate that the DPA contest is a forum that gives a rough idea of the skills of educated researchers. It represents the state-of-the-art of the attacks, thus providing a fair image of the know-how with current understanding of the attacks.

As a reminder, the DPA is an academic initiative to educate on side-channel analysis. It is interesting for people who wish to learn, as they are provided with traces, and can thus focus on the exploitation of the leakage, without have to bother with the boring aspects of identifying and capturing the side-channel. It is also of interest for the practitioners can easily estimate the average skills and the practicability of some attacks. Indeed, in security, not knowing the threat is the worst situation, because it is impossible to devise a countermeasure *in abstracto*.

In this article, we first intend to give a return of experiment based on the first two editions of the contest (2008–2009, in Sec. 1 and 2009–2010, in Sec. 2). We show that it has helped:

- standardize the way attacks are evaluated (efficiency, but also speed), and thus
- compare the efficiency of several distinguishers, preprocessing, attack methodology;
- see how attackers deal with real-world traces, especially weird leakage models and daily drifts in the measurements (2nd DPA contest).

A second part of the article, in Sec. 3, aims at presenting the contest that is currently ongoing, namely version 3 ("acquisition" contest, organized with the help of the Japanese AIST). It intends to improve the side-channel measures quality.

In a third part, namely in Sec. 4, we will present the roadmap of the DPA contests.

1 DPA Contest 1

The goal of the DPA contest version 1 is to make it possible for researchers to compare in an objective manner their different attack algorithms [5]. As this was impossible yesterday, because traces made by different laboratories are too different (acquisition platform sensitivity, cryptographic algorithm implementation, board's noise, ...), the `www.dpacontest.org` is an initiative towards an international benchmarking reference. Also, it is expected to stimulate significant advances or even breakthroughs by this peer-reviewed contest. It has been decided that the winning attack will be the one that uses in average the less number of traces to statistically retrieve all the key bits of a simple DES [8]. The motivation for this choice is to foster generic attacks, thus hopefully portable to other measurements, rather than *ad hoc* attacks, specific to the first DPA contest edition. The contest "hall of fame" is thus divided into four categories:

1. Representative order, meaning that the attack has been executed a large number of times and that score considered for the classification is the average number of traces for the key retrieval. The article "Improving the Rules of the DPA Contest" [10] gives some indications about the way to be rated under this category.
2. Chosen plaintext order, where the traces order is computed by an algorithm that is made explicit in the attack source code.
3. Fixed order, that models an attack at known albeit not chosen plaintext or ciphertext. The order is either that of the database without SQL `SORT BY` clause (preferred choice) or of the ZIP archive (secondary choice) or of the temporal acquisition (secondary choice).
4. Custom order, left at the discretion of the attacker (of course, an explanation of the sorting strategy is preferred).

The best attack in the first category is a "maximum likelihood method with a bivariate known model" by Christophe CLAVIER, who gave a talk during the plenary special session of CHES'2009 devoted to the DPA contest [2].

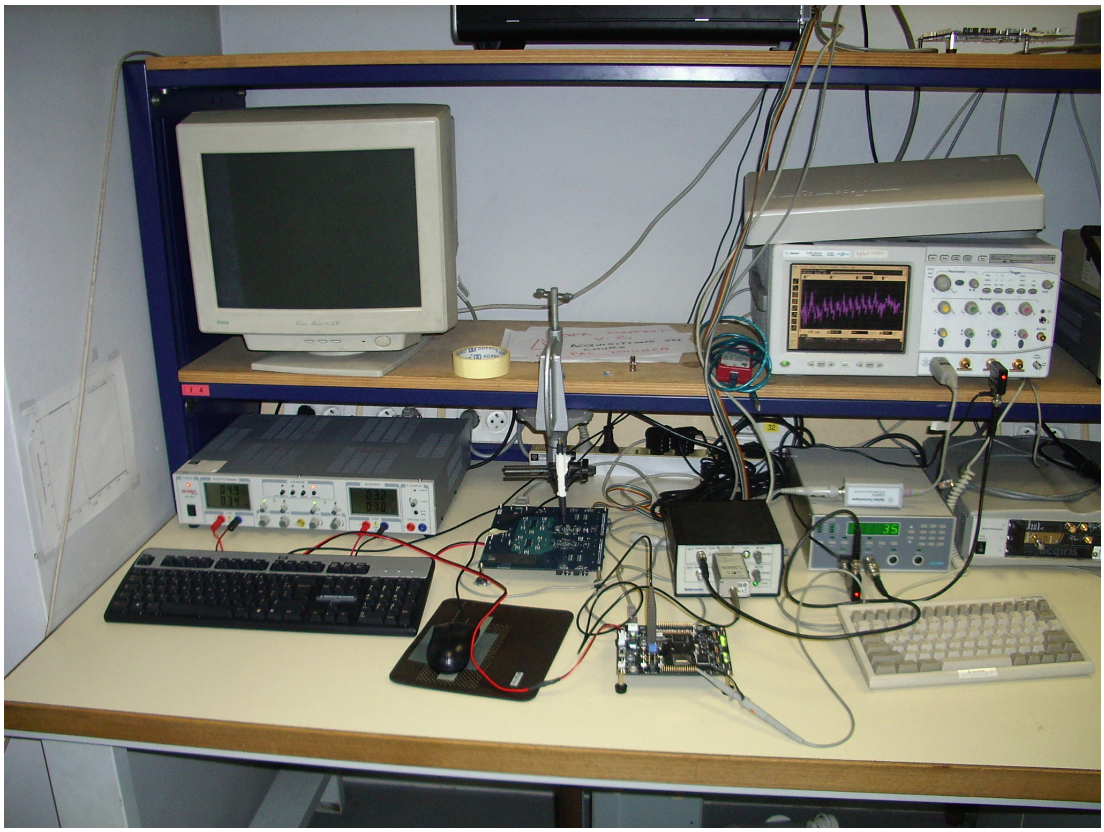

Figure 1: Acquisition setup for the second DPA contest.

2 DPA Contest 2

The key points of the second version of the DPA contest are summarized below.

- The class of attacks considered is Differential Power Analysis like attacks (SPA, DPA, CPA, MIA, and any variant).
- The analyzed algorithm is now AES-128 [9].
- Both known-message and profiled attacks are possible.
- Different metrics are introduced to evaluate the efficiency of the submitted attacks:
  - partial success rate (PSR),
  - partial guessing entropy (PGE),
  - global success rate (GSR),
  - execution time and
  - memory footprint.
- The acquisitions have been performed on a SASEBO GII [6] board (see Fig. 1) and the full design used for the acquisitions is provided.

The ranking is given in the three next subsections. The first submission period ended at COSADE 2011, where the results have been presented [3]. Then, the contests was left open for improvements.

2.1 GSR stable above 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
- First & second submission period:
  1. Matthieu WALLE (Thales Communications), attack 7T: 7,061 (+ his 3 other attacks)
  2. Victor LOMNÉ (ANSSI), attack Recursive CPA: 10,666
  3. Maël BERTHIER & Yves BOCKTAELS (MORPHO), attack CPA AP SBOX PRD2: 10,796
- All time (including after the end of the contest):
  1. Annelie Heuser, Michael Kasper, Werner Schindler, Marc Stöttinger (CASED (research group CASCADE); TU Darmstadt, Fraunhofer SIT, Bundesamt für Sicherheit in der Informationstechnik (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

2.2 Min PSR stable above 80%

- First submission period:
  1. Matthieu WALLE (Thales Communications), attack 9T: 5,890 (+ his 3 other attacks)
  2. Alexis BONNECAZE (IML, ERISCS), attack SPE: 12,318
  3. Antoine WURCKER (UNILIM), attack A: 12,631
- First & second submission period:
  1. Matthieu WALLE (Thales Communications), attack 9T: 5,890 (+ his 3 other attacks)
  2. Maël BERTHIER & Yves BOCKTAELS (MORPHO), attack CPA AP SBOX PRD2: 7,510 (+ 1 of their other attacks)
  3. Olivier MEYNARD (Télécom ParisTech), attack A5: 8,835
- All time (including after the end of the contest):
  1. Annelie Heuser, Michael Kasper, Werner Schindler, Marc Stöttinger (CASED (research group CASCADE); TU Darmstadt, Fraunhofer SIT, Bundesamt für Sicherheit in der Informationstechnik (BSI)), Stochastic attack (stochastic approach): 4,358
  2. Matthieu WALLE (Thales Communications), attack 9T: 5,890 (+ his 3 other attacks)
  3. Maël BERTHIER & Yves BOCKTAELS (MORPHO), attack CPA AP SBOX PRD2: 7,510 (+ 1 of their other attacks)

2.3 Max PGE stable below 10

- First submission period:
  1. Matthieu WALLE (Thales Communications), attack 7T: 3,388 (+ his 3 other attacks)
  2. Antoine WURCKER (UNILIM), attack A: 4,192 (+ his other attack)
  3. Maël BERTHIER (MORPHO), attack CPA: 4,706
- First & second submission period:
  1. Maël BERTHIER & Yves BOCKTAELS (MORPHO), attack CPA AP SBOX: 2,767 (+ 1 of their other attacks)
  2. Matthieu WALLE (Thales Communications), attack 7T: 3,388 (+ his 3 other attacks)
  3. Antoine WURCKER (UNILIM), attack A: 4,192 (+ his other attack)
- All time (including after the end of the contest):
  1. Annelie Heuser, Michael Kasper, Werner Schindler, Marc Stöttinger (CASED (research group CASCADE); TU Darmstadt, Fraunhofer SIT, Bundesamt für Sicherheit in der Informationstechnik (BSI)), Stochastic attack (stochastic approach): 1,894
  2. Maël BERTHIER & Yves BOCKTAELS (MORPHO), attack CPA AP SBOX: 2,767 (+ 1 of their other attacks)
  3. Matthieu WALLE (Thales Communications), attack 7T: 3,388 (+ his 3 other attacks)

3 DPA Contest 3

The DPA Contest v3 is organized jointly by the National Institute of Advanced Industrial Science and Technology (AIST) and the VLSI research group from TELECOM-ParisTech french University.

The two first editions of the contest were attack contests (the first against DES and the second against AES), i.e. participants were asked to develop their own attacks that used traces acquired by the organizers to find the key.

However, for Side Channel Analysis, the organizers on this website and will be evaluated against several attacks using different metrics.

The acquisitions shall be performed on a SASEBO-GII board using the AES design provided by the AIST (which can be downloaded from the Tools page) on the cryptographic FPGA (the Virtex 5).

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

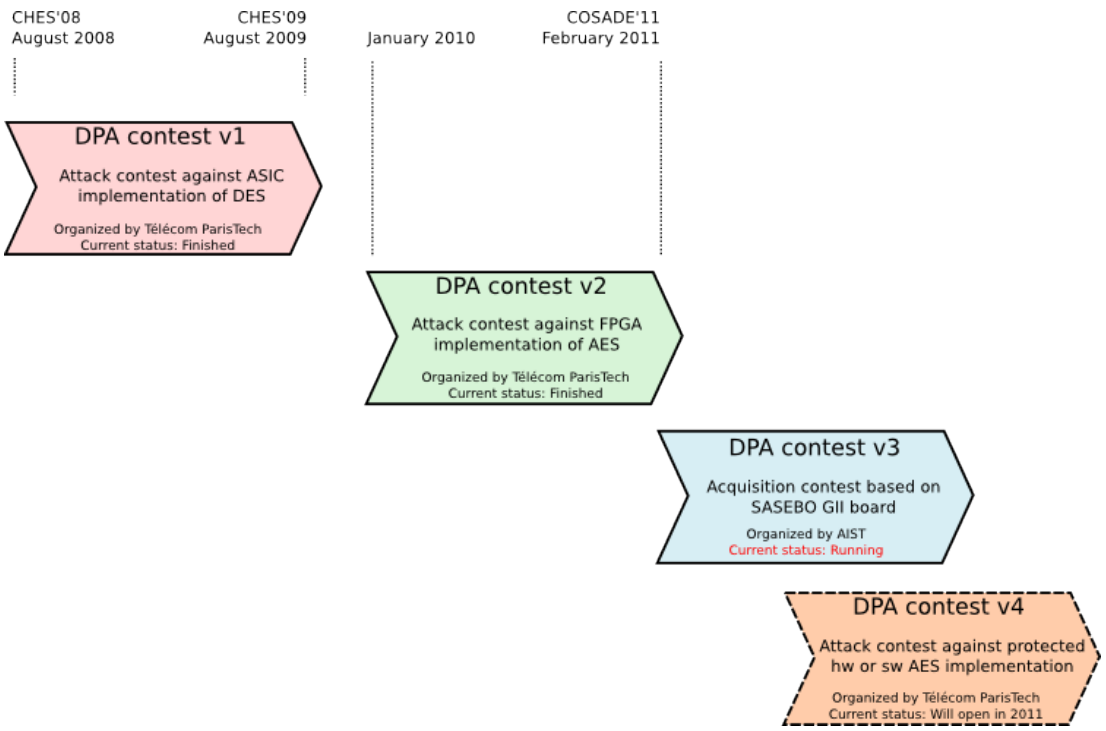

Figure 2: DPA contests roadmap.

4 DPA Contest 4

This version of the DPA contest is still in maturation, as shown in the DPA contests roadmap of Fig. 2. Examples of research directions are:

- compare various countermeasures, in a view to make more clear which one is more relevant than another in which context,
- test attacks that involve very long captures, and thus require a large computing power or special heuristics ("software attack" contest),
- examine asymmetric cryptography (that are *almost always* vulnerable to timing attacks and/or SPA),
- benchmark fault injection attacks,
- organize an "open physical attack contest" (where the attacker can intervene anywhere from the acquisition to the exploitation).

This paper is accompanied by a talk and a round table at the Non-Invasive Attack Testing (NIAT) workshop. The NIAT workshop attendance will be asked about future directions for the DPA contest versions 4+, in a view to keep the DPA contest as useful as possible. Also, a survey will be distributed to gather opinions.

References

[1] Common Criteria (*aka* CC) for Information Technology Security Evaluation (ISO/IEC 15408).
Website: `http://www.commoncriteriaportal.org/`.

[2] Christophe Clavier. DPA Contest 2008–2009, Less than 50 traces allow to recover the key, September 6-9 2009. CHES Special Session 1: DPA Contest. Lausanne, Switzerland, (slides).

[3] Guillaume Duc, Sylvain Guilley, Laurent Sauvage, Florent Flament, Maxime Nassar, Nidhal Selmane, Jean-Luc Danger, Tarik Graba, Yves Mathieu, and Renaud Pacalet. FPGA Implementations of the AES Masked Against Power Analysis Attacks. In *COSADE*, pages 56–66, February 2011. Darmstadt, Germany. (slides).

[4] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis: Concrete Results. In *CHES*, volume 2162 of *LNCS*, pages 251–261. Springer, May 14-16 2001. Paris, France.

[5] Sylvain Guilley, Laurent Sauvage, Florent Flament, Maxime Nassar, Nidhal Selmane, Jean-Luc Danger, Tarik Graba, Yves Mathiew, and Renaud Pacalet. Overview of the 2008-2009 'DPA contest', September 6-9 2009. CHES Special Session 1: DPA Contest. Lausanne, Switzerland, (slides).

[6] Japanese RCIS-AIST, SASEBO development board:
`http://www.rcis.aist.go.jp/special/SASEBO/index-en.html`.

[7] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In *Proceedings of CRYPTO'99*, volume 1666 of *LNCS*, pages 388–397. Springer-Verlag, 1999.

[8] NIST/ITL/CSD. Data Encryption Standard. FIPS PUB 46-3, Oct 1999.
`http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`.

[9] NIST/ITL/CSD. Advanced Encryption Standard (AES). FIPS PUB 197, Nov 2001. `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`.

[10] François-Xavier Standaert, Philippe Bulens, Giacomo de Meulenaer, and Nicolas Veyrat-Charvillon. Improving the Rules of the DPA Contest. Cryptology ePrint Archive, Report 2008/517, December 8 2008. `http://eprint.iacr.org/2008/517`.