DPA contests

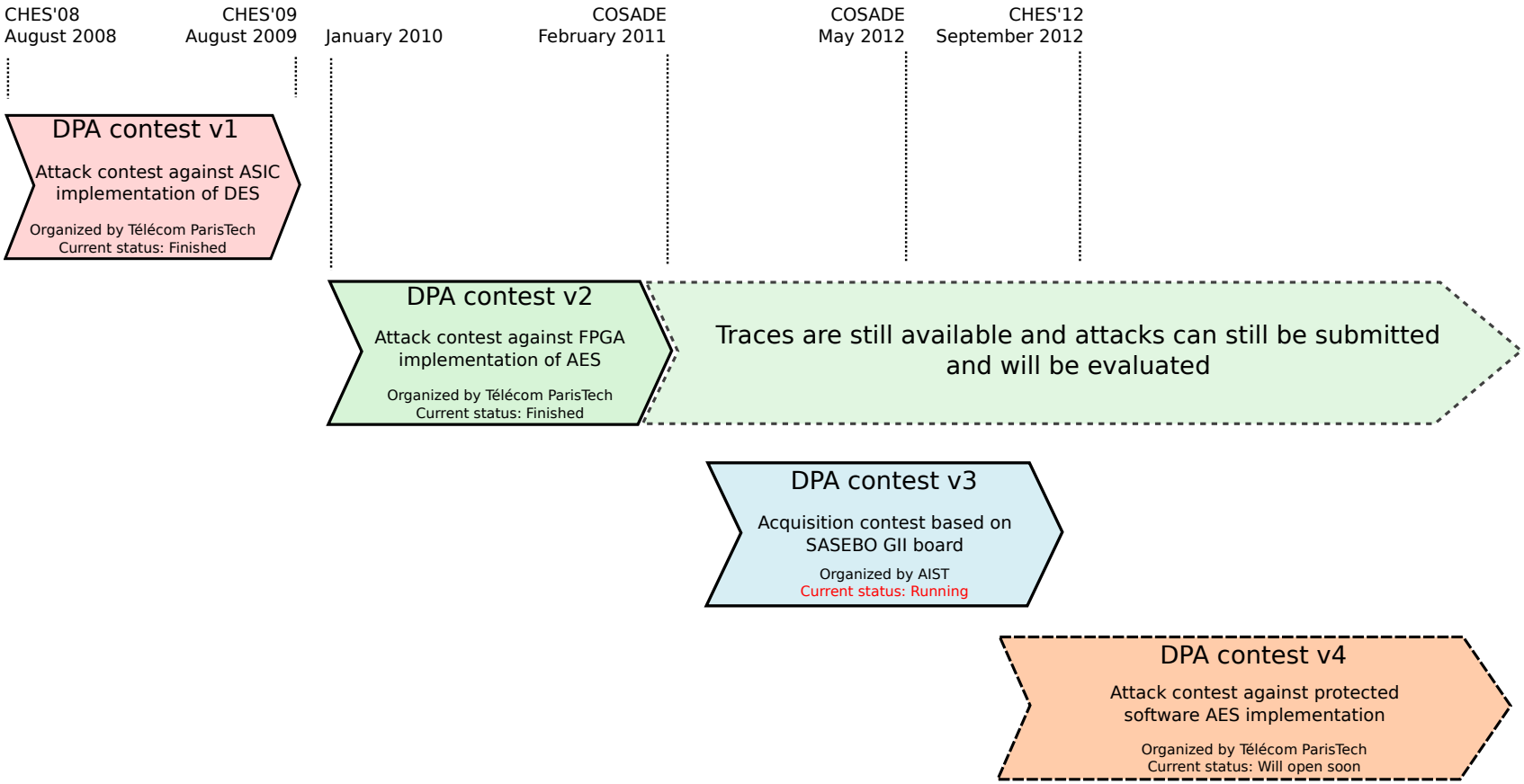
Guillaume Duc, Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, Tarik Graba, Yves Mathieu, Renaud Pacalet < contact@DPAcontest.org >

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

COSADE, May 3rd, 2012
Darmstadt, Germany

Presentation Outline

The DPA contest(s)



The ideas behind the DPA contests

- Promote the research on all aspects of Side-Channel Analysis
  - Development of new attacks
  - Improvement of acquisition techniques
  - Development of counter-measures
- To be used as a benchmark tool

Presentation Outline

What is this DPA contest v2?

Status

- Launched in January 2010
- Results announced during COSADE 2011 (February 2011)
- **But you can still participate!** (new submissions are evaluated on best-effort basis, results are published on the website and announced during COSADE conferences)

Aim

- As the DPA contest v1, it is a **key recover attack** contest
  - Participants submit programs that must find the key using consumption traces
- **More than 1,000,000 side-channel measurements** (*traces*) are freely available from the website
  - Can be used in scientific publications as a benchmark tool even if you do not participate

What is this DPA contest v2?

Specificity of this second edition

- Target: Hardware AES block cipher algorithm implementation on FPGA
- Acquisition platform: SASEBO-GII board
- 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**

What is this DPA contest v2?

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
- Each attack is evaluated against the 20.000 traces of each 32 keys of the private database (640.000 traces)

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
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), Germany**	2 attacks
Yang LI & Daisuke NAKATSU & Kazuo SAKIYAMA	**University of Electro-Communications, Japan**	1 attack

Results — GSR stable $> 80\,\%$

Results announced at COSADE 2011

1. Matthieu WALLE (Thales Communications), attack 7T: **7,061** (+ his 3 other attacks)

Updated results (April 2012)

1. Yang LI & Daisuke NAKATSU & Kazuo SAKIYAMA (University of Electro-Communications): **2,256**
2. Annelie HEUSER & Michael KASPER & Werner SCHINDLER & Marc STÖTTINGER (CASED / TU Darmstadt / Fraunhofer SIT / BSI): **3,589** (+ 1 other attack)
3. Matthieu WALLE (Thales Communications), attack 7T: **7,061** (+ his 3 other attacks)

Results — Min PSR stable $> 80\,\%$

Results announced at COSADE 2011

1. Matthieu WALLE (Thales Communications), attack 9T: **5,890** (+ his 3 other attacks)

Updated results

1. Yang LI & Daisuke NAKATSU & Kazuo SAKIYAMA (University of Electro-Communications): **2,155**
2. Annelie HEUSER & Michael KASPER & Werner SCHINDLER & Marc STÖTTINGER (CASED / TU Darmstadt / Fraunhofer SIT / BSI): **2,748** (+ 1 other attack)
3. Matthieu WALLE (Thales Communications), attack 9T: **5,890** (+ his 3 other attacks)

Results — Max PGE stable < 10

Results announced at COSADE 2011

1. Maël BERTHIER & Yves BOCKTAELS (MORPHO), attack CPA AP SBOX: **2,767** (+ 1 of their other attacks)

Updated results

1. Annelie HEUSER & Michael KASPER & Werner SCHINDLER & Marc STÖTTINGER (CASED / TU Darmstadt / Fraunhofer SIT / BSI): **1,356** (+ 1 other attack)
2. Maël BERTHIER & Yves BOCKTAELS (MORPHO), attack CPA AP SBOX: **2,767** (+ 1 of their other attacks)
3. Yang LI & Daisuke NAKATSU & Kazuo SAKIYAMA (University of Electro-Communications): **3,181**

Other news

Scientific contribution

- Collaborative journal paper about the results of the DPA contest v2 is being written
  - If you submit an attack to the DPA contest v2 and if you have not answered yet, your contribution is welcome

The contest is still open!

- Do not hesitate to use traces we provide in your publications, teaching activities, etc.
- Do not hesitate to submit new attacks for evaluation

Presentation Outline

What is this DPA contest v3?

Status

- Launched in February 2011 during COSADE
- First deadline February 29th 2012
- Organized by National Institute of Advanced Industrial Science and Technology (AIST)

Aim

- In practice, the acquisition phase is an important part of the success of a SCA
- Contrary to DPA contests v1 and v2, it is an **acquisition** contest
  - Participants perform their own acquisition and trace processing and submit the "best" traces

What is this DPA contest v3?

Rules

- The acquisitions shall be performed on a SASEBO-GII board using the AES design provided by the AIST
- 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 is this DPA contest v3?

Evaluation

- Traces submitted by participants are compared using one or several attacks (at least a CPA provided by the AIST)

Participants (March 2012)

Author	**Affiliation**
Shaohua TANG, Weijian LI, Houwen ZOU, Yaolei LV, Bin LI, Kai SUN	School of Computer Science and Engineering, South China University of Technology, China
Colin O'FLYNN	Dalhousie University, Canada
Stephane Fernandes MEDEIROS, Liran LERMAN, Nikita VESHCHIKOV	Université Libre de Bruxelles, Belgium
Kaoru OKAMOTO	Department of Communication Network Engineering, Faculty of Engineering, Okayama University, Japan

Status / Extension

Issue with submissions

- Several of the received contributions on the official deadline (February 29th 2012) were not following the rules (either they do not respect the format of the traces or do not use the correct design)
- These participants are being contacted by the AIST to correct their submission
- So, the contest is open again until July 31st 2012 and results will be announced during CHES 2012

Special offer (sponsored by CRI)

CRI will provide a free SASEBO-W board to academic participants to the DPA contest v3

Presentation Outline

What is this DPA contest v4?

Motivations

- Stay a benchmarking tool
- Introduce new target (v1: DES on ASIC, v2/3: AES on FPGA)
- Introduce counter-measures

What is this DPA contest v4?

Summary

- Organized by Télécom ParisTech (such as v1 and v2)
- As the DPA contests v1 and v2, it is a **key recover attack** contest with possibility for participants to perform their own acquisitions (as DPA contest v3)
- Target: Several software implementation of AES on ATMega smart-card
  - One not protected implementation (provided by AIST)
  - One implementation with simple masking countermeasure (provided by Télécom ParisTech)
  - Several other implementations with countermeasures will be provided during the life of the contest
- Participants will be provided with the details of the implementation of the counter-measures

What is this DPA contest v4?

Summary

- Standardized evaluation platform: SASEBO-W
- Reference acquisition traces for all implementations will be published on the website
  - To allow researchers without acquisition lab to participate and to provide "benchmarks" for papers
- Participants can perform their own acquisitions
  - To encourage the development of new acquisition techniques that may be specific to a counter-measure
- Same evaluation process as the DPA contest v2 (evaluation on private traces, same evaluation metrics)

Launch

Launch

- The contest with the two first implementations will be launched during summer 2012
- A first submission deadline will be set around March 2013 to allow the presentation of the first results at COSADE 2013
- New implementations with counter-measures will be published later

Presentation Outline

Acknowledgments

- Philippe Bulens [2]
- Jean-Luc Danger [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] Institut Mines-Télécom / Télécom ParisTech
[2] Université catholique de Louvain
[3] Tohoku University
[4] DGA-MI (formerly CELAR)
[5] National Institute of Advanced Industrial Science and Technology

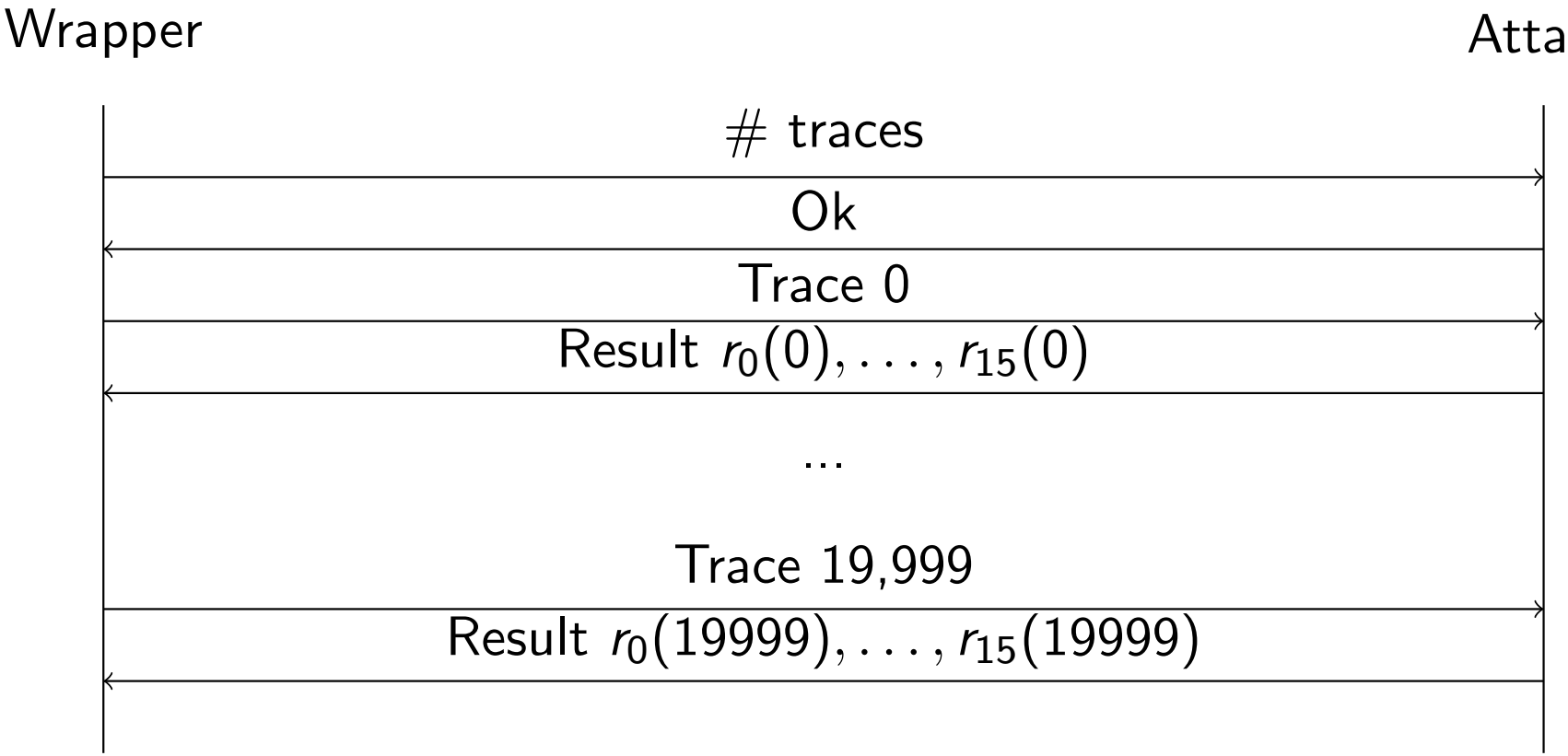
Thank you!

- Thank you for your attention
- Questions?

DPA contest v2

- Evaluation and metrics

Evaluation protocol



Definition of attack metrics

- On iteration i, the attack receives the trace i and produces the result $r_0(i), \ldots, r_{15}(i)$ where $r_s(i)$ 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 $\mathrm{P}(r_s^c(t) = x^c)$ 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 $\mathrm{E}(X)$ of a random variable X is defined as: $\mathrm{E}(X) = \sum_x x \cdot \mathrm{P}(X = x)$
- 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 $> 80\%$	$\text{argmin}_t \, \text{P}(\forall s, r_s(t)[\dot{k}_s] = 0) > 0.80$
Min PSR $> 80\%$	$\text{argmin}_t \, \min_s \text{P}(r_s(t)[\dot{k}_s] = 0) > 0.80$
Max PGE < 10	$\text{argmin}_t \, \max_s \text{E}(r_s(t)[\dot{k}_s]) < 10$
GSR stable $> 80\%$	$\text{argmin}_t \, \forall t' \geq t, \text{P}(\forall s, r_s(t')[\dot{k}_s] = 0) > 0.80$
Min PSR stable $> 80\%$	$\text{argmin}_t \, \forall t' \geq t, \min_s \text{P}(r_s(t')[\dot{k}_s] = 0) > 0.80$
Max PGE stable < 10	$\text{argmin}_t \, \forall t' \geq t, \max_s \text{E}(r_s(t')[\dot{k}_s]) < 10$
GSR @20k	$\text{P}(\forall s, r_s(20\,000 - 1)[\dot{k}_s] = 0)$
Min PSR @20k	$\min_s \text{P}(r_s(20\,000 - 1)[\dot{k}_s] = 0)$
Max PSR @20k	$\max_s \text{P}(r_s(20\,000 - 1)[\dot{k}_s] = 0)$
Min PGE @20k	$\min_s \text{E}(r_s(20\,000 - 1)[\dot{k}_s])$
Max PGE @20k	$\max_s \text{E}(r_s(20\,000 - 1)[\dot{k}_s])$

DPA contest v2

- Statistics

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
- 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