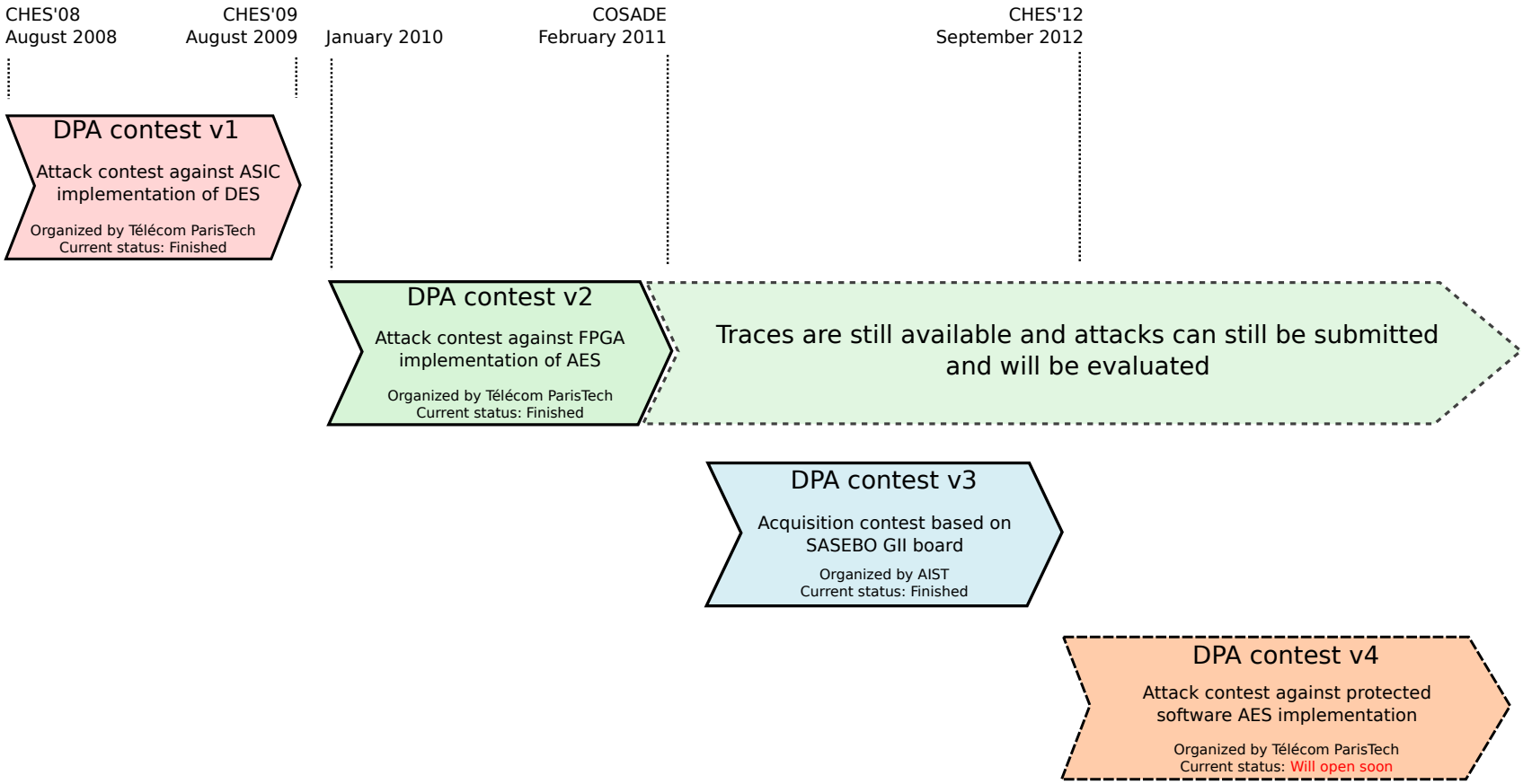
DPA contests

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)

CHES, 2012
Leuven, Belgium

The DPA contest(s)



http://www.DPAcontest.org/

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

Participants (v2)

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
Benoît GÉRARD & Nicolas VEYRAT-CHARVILLON	**Université Catholique de Louvain (UCL), Belgium**	3 attacks

New exciting results (v2)

GSR stable $> 80\,\%$

- End 2010 (official deadline): **7,061** (Matthieu WALLE, Thales)
- 07/2011: **6,729** (Annelie HEUSER *et al.*, CASED)
- 09/2011: **3,589** (Annelie HEUSER *et al.*, CASED)
- 01/2012: **2,256** (Yang LI *et al.*, UEC)
- 08/2012: **439** (Benoît GÉRARD *et al.*, UCL)

New exciting results (v2)

GSR stable $> 80\,\%$

- End 2010 (official deadline): **7,061** (Matthieu WALLE, Thales)
- 07/2011: **6,729** (Annelie HEUSER *et al.*, CASED)
- 09/2011: **3,589** (Annelie HEUSER *et al.*, CASED)
- 01/2012: **2,256** (Yang LI *et al.*, UEC)
- 08/2012: **439** (Benoît GÉRARD *et al.*, UCL)
- **Who's next?**

Other news (v2)

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

What is this DPA contest v3?

Status

- Launched in February 2011 during COSADE
- Deadline: End of July 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" set of traces

Participants (v3)

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
Ming TANG, Zhenlong QIU, Pingpan CHENG, Li ZHAO	Computer School of Wuhan University, China
Kim YONGDAE	The Attached Institute of ETRI (Electronics and Telecommunications Research Institute), Korea
Daisuke FUJIMOTO	Kobe University, Japan
Emiri KAMAGATA	Keirex Technology Inc., Japan
Yuu TSUCHIYA, Takeshi KISHIKAWA, Shohei SAITO, Tsuyoshi TOYAMA, Akihiko SASAKI, Tsutomu MATSUMOTO	Yokohama National University, Japan

Participants have received a SASEBO-W board from AIST, offered by CRI.

Results (v3)

With a CPA attack

Results (v3)

With a CPA attack

- The winners are Yuu TSUCHIYA, Takeshi KISHIKAWA, Shohei SAITO, Tsuyoshi TOYAMA, Akihiko SASAKI and Tsutomu MATSUMOTO
  (Yokohama National University, Japan)

Results (v3)

With a CPA attack

- The winners are Yuu TSUCHIYA, Takeshi KISHIKAWA, Shohei SAITO, Tsuyoshi TOYAMA, Akihiko SASAKI and Tsutomu MATSUMOTO
  (Yokohama National University, Japan)
- Only requires **800 traces** to find the correct key (and this key remains stable during the processing of the next 100 traces)

Results (v3)

With a CPA attack

- The winners are Yuu TSUCHIYA, Takeshi KISHIKAWA, Shohei SAITO, Tsuyoshi TOYAMA, Akihiko SASAKI and Tsutomu MATSUMOTO
  (Yokohama National University, Japan)
- Only requires **800 traces** to find the correct key (and this key remains stable during the processing of the next 100 traces)
- No trace post-processing, only acquisition tricks (reduction of the voltage of the two FPGA, ferrite core on the USB cable, analog low-pass filter, power amplifier)

Results (v3)

With a CPA attack

- The winners are Yuu TSUCHIYA, Takeshi KISHIKAWA, Shohei SAITO, Tsuyoshi TOYAMA, Akihiko SASAKI and Tsutomu MATSUMOTO
  (Yokohama National University, Japan)
- Only requires **800 traces** to find the correct key (and this key remains stable during the processing of the next 100 traces)
- No trace post-processing, only acquisition tricks (reduction of the voltage of the two FPGA, ferrite core on the USB cable, analog low-pass filter, power amplifier)
- All results and descriptions of the acquisition platforms are available on the website

DPA contest v4?

Motivations

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

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 unprotected implementation
  - 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

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 (v4)

Launch

- The contest with the two first implementations will be launched before the end of 2012
- New implementations with counter-measures will be published later

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