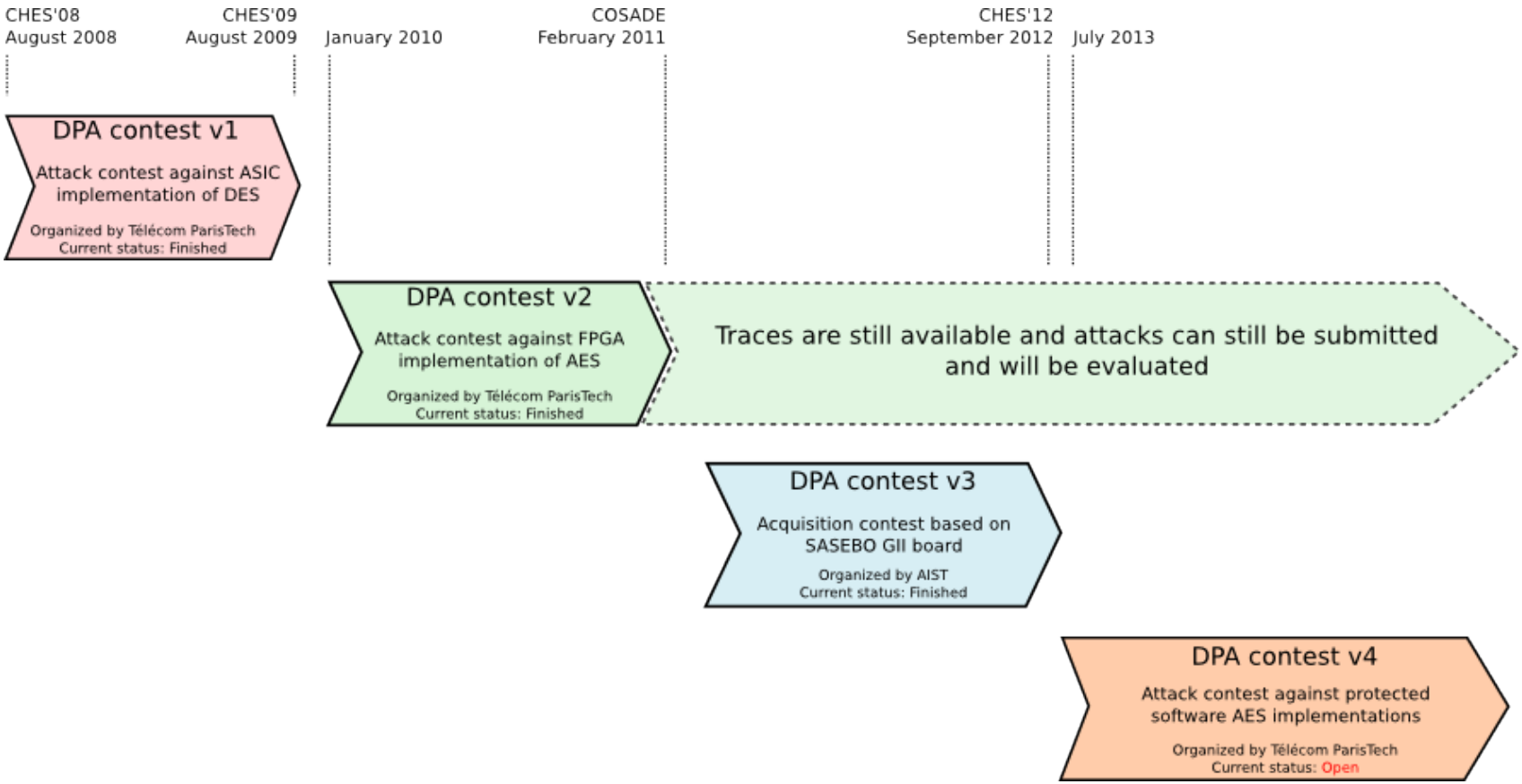
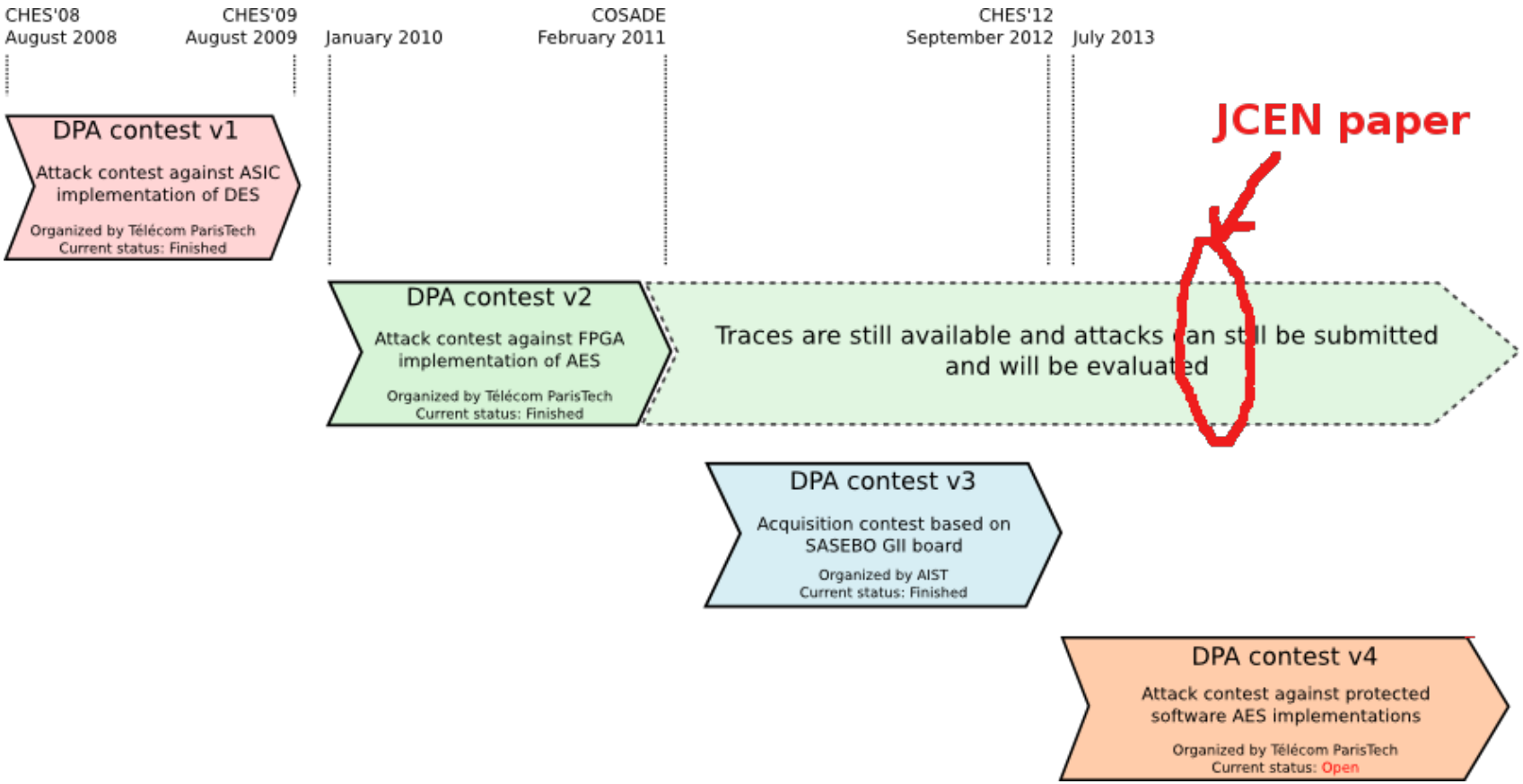
DPA contests: from V4 to V4.x !!!

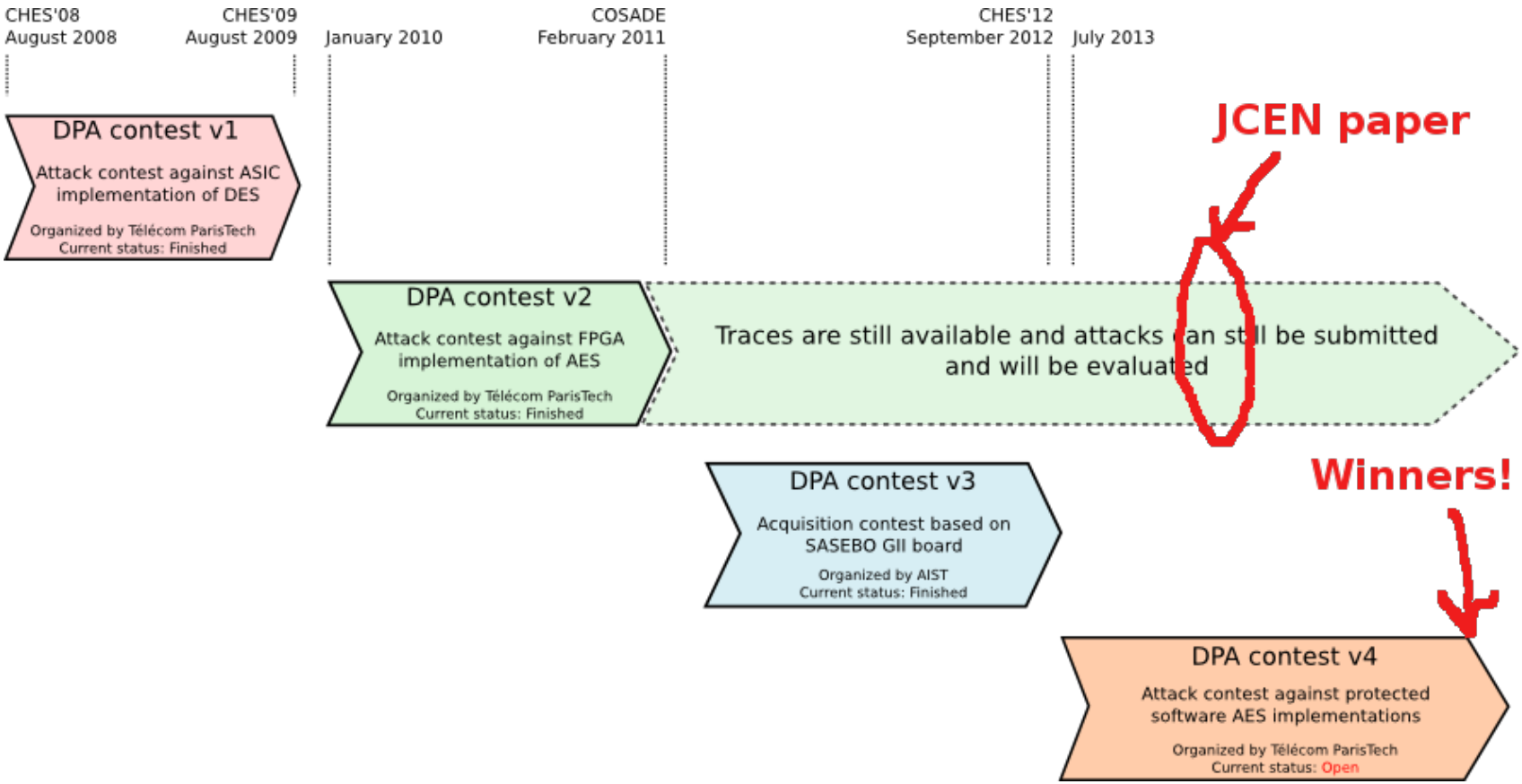
Nicolas Bruneau, Jean-Luc Danger, Guillaume Duc, Sylvain Guilley, Annelie Heuser, Zakaria Najm, Laurent Sauvage.
< contact@DPAcontest.org >

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

CHES 2014 rump session
September 25, 2014 — Busan, South Korea.


CHES'08
August 2008
CHES'09
August 2009
January 2010
COSADE
February 2011
CHES'12
September 2012
July 2013
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
Traces are still available and attacks can still be submitted and will be evaluated
DPA contest v3
Acquisition contest based on SASEBO GII board
Organized by AIST
Current status: Finished
DPA contest v4
Attack contest against protected software AES implementations
Organized by Télécom ParisTech
Current status: Open


CHES'08
August 2008
CHES'09
August 2009
January 2010
COSADE
February 2011
CHES'12
September 2012
July 2013
JCEN paper
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
Traces are still available and attacks can still be submitted and will be evaluated
DPA contest v3
Acquisition contest based on SASEBO GII board
Organized by AIST
Current status: Finished
DPA contest v4
Attack contest against protected software AES implementations
Organized by Télécom ParisTech
Current status: Open


CHES'08
August 2008
CHES'09
August 2009
January 2010
COSADE
February 2011
CHES'12
September 2012
July 2013
DPA contest v1
Attack contest against ASIC implementation of DES
Organized by Télécom ParisTech
Current status: Finished
JCEN paper
DPA contest v2
Attack contest against FPGA implementation of AES
Organized by Télécom ParisTech
Current status: Finished
Traces are still available and attacks can still be submitted and will be evaluated
DPA contest v3
Acquisition contest based on SASEBO GII board
Organized by AIST
Current status: Finished
Winners!
DPA contest v4
Attack contest against protected software AES implementations
Organized by Télécom ParisTech
Current status: Open

Thank you!

Thank you!

- Overall, **30 participations**!!!
- 73% from academia ; 17% from gvt agencies ; 10% from industry
- From 10 countries: CN, KR, CZ, JP, BE, GE, IL, FR, BY, SG

Thank you!

- Overall, **30 participations**!!!
- 73% from academia ; 17% from gvt agencies ; 10% from industry
- From 10 countries: CN, KR, CZ, JP, BE, GE, IL, FR, BY, SG

Participant	Submission date	Key found	Max PGE < 10	Key found (stable)	Max PGE stable < 10	Time/Trace (ms)	Attack type	Description
Liran Lerman Université Libre de Bruxelles, Belgium	19/09/2013	22	13	22	13	24 ms	Profiling	Description below
Amir Moradi RUB, Germany	02/10/2013	174	148	174	148	305 ms	Non Profiling	Description below
Tang Ming Wuhan University, China	03/11/2013	763	465	990	482	271 ms	Non Profiling	
Zheng Kanghong DSO National Laboratories, Singapore **Sebastian Kutzner** Physical Analysis and Cryptographic Engineering (PACE) Temasek Laboratories Nanyang Technological University, Singapore	07/11/2013	69	55	78	55	261 ms	Non Profiling	Description below
Tang Ming, Qiu Zhenlong, Peng Hongbo, Wang Xin, Li Yanbin, Xiang Xiao School of Computer, Wuhan University, China Attack v2	21/11/2013	140	56	297	115	8 ms		
Tang Ming, Qiu Zhenlong, Peng Hongbo, Wang Xin, Li Yanbin, Xiang Xiao School of Computer, Wuhan University, China Attack v3	21/11/2013	177	103	212	143	11 ms		
Heorhi Liasneuski Belarusian State University, Belarus	01/12/2013	38	15	38	23	5 ms	Profiling	Description below Source code

. . . . . .

Used techniques

- Neural networks, SVM
- Clustering, K-means
- F-test, Filtering
- ...

Used techniques

- Neural networks, SVM
- Clustering, K-means
- F-test, Filtering
- ...

Dissemination

- CARDIS
- **CHES** (thanks Ofir Weisse!)
- COSADE
- HASP
- SPACE
- WESS
- ...

Winners!

Winners!

Profiled

- **Frank Schuhmacher** ..... 1.0 trace!
- Template matrices for each sbox index, with pre-whitening and a projection to the first 10 principal components of the signal covariance matrix.
- Segrids, Germany

Winners!

Profiled

- **Frank Schuhmacher** ..... 1.0 trace!
- Template matrices for each sbox index, with pre-whitening and a projection to the first 10 principal components of the signal covariance matrix.
- Segrids, Germany

Non-profiled

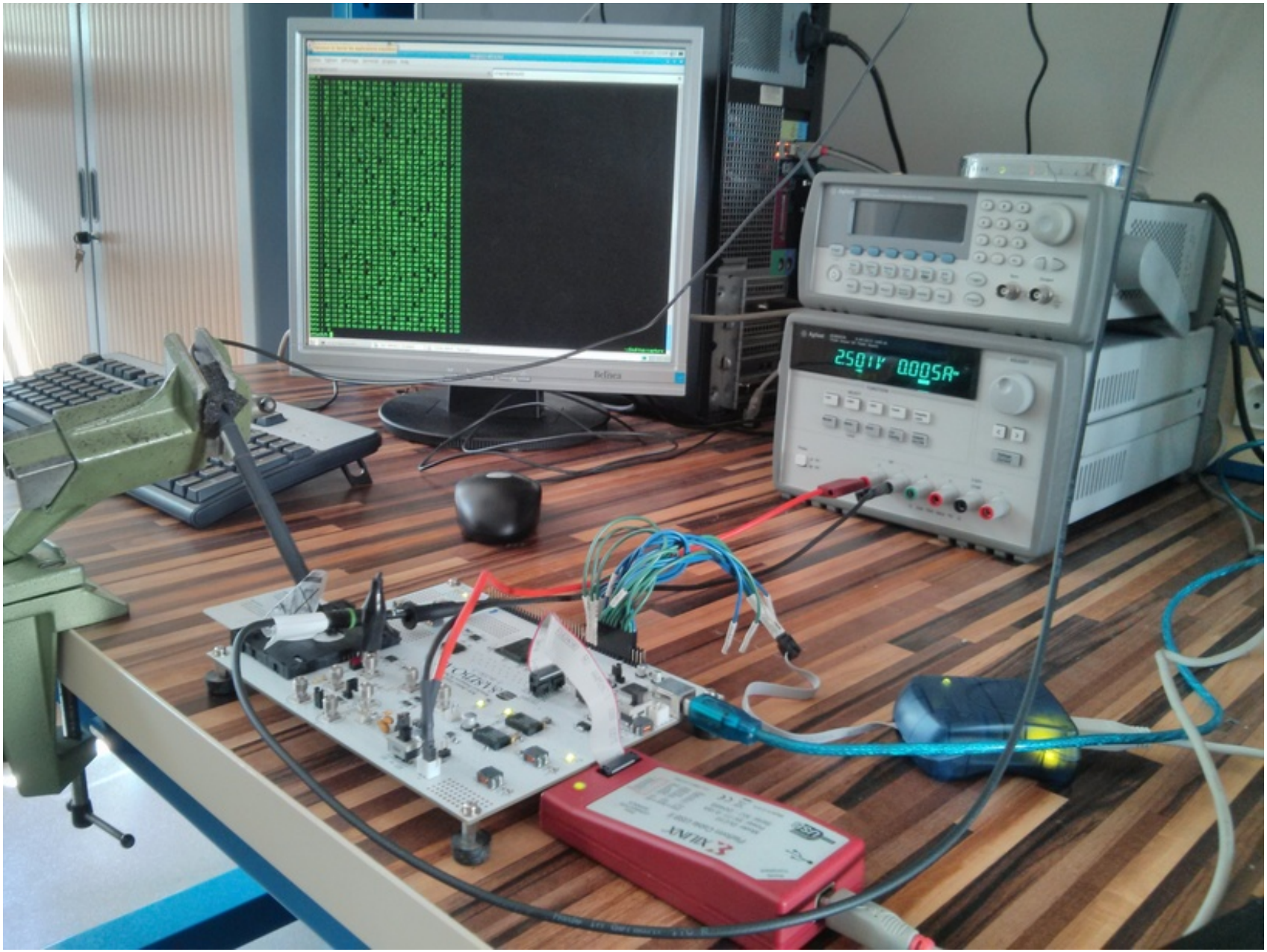
- **Yongbin Zhou, Lin Meng, Hailong Zhang, Yingxian Zheng, Mingliang Feng** ..... 12.0 trace!
- State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China
- 1st order CPA attack II

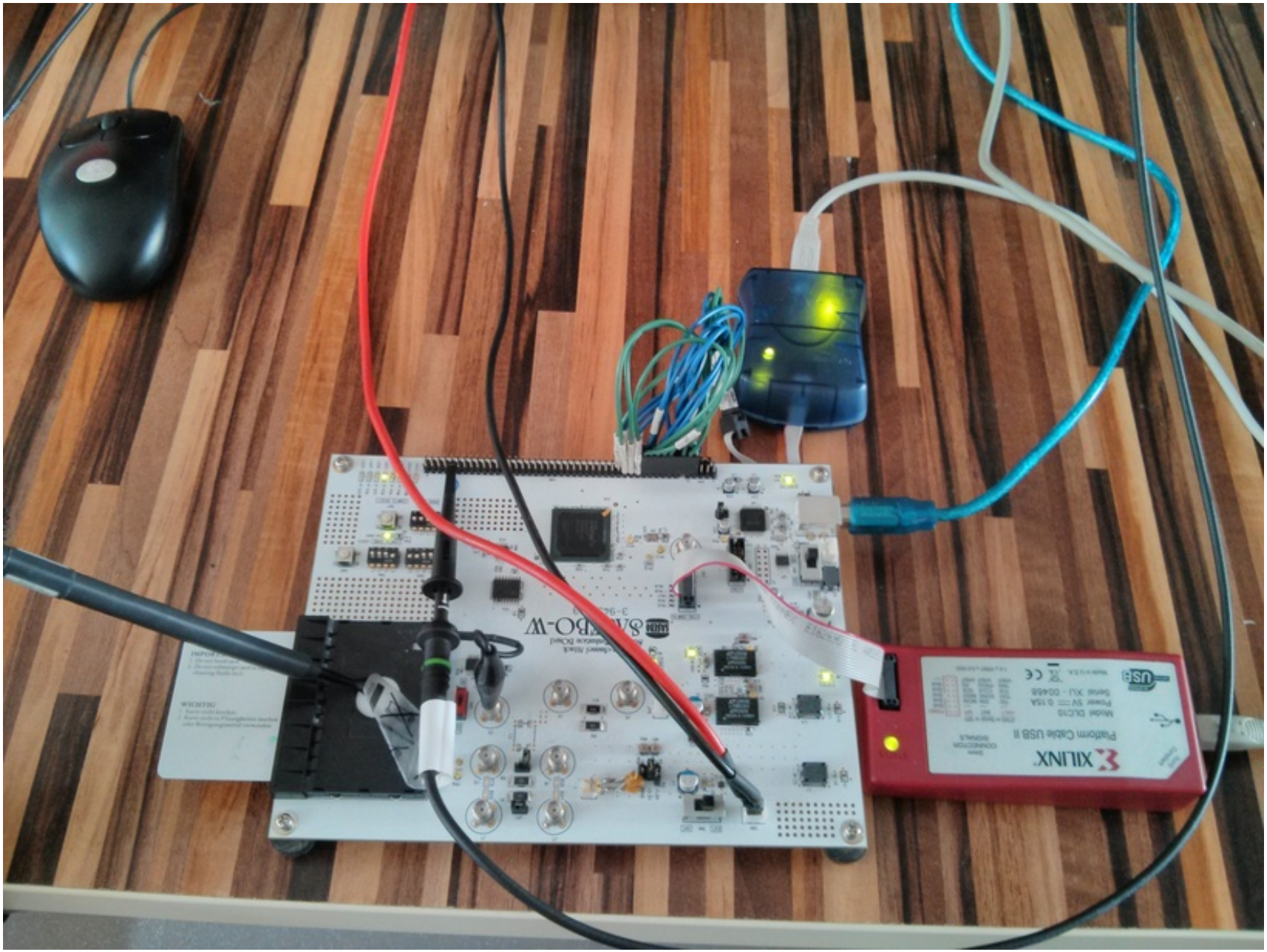
What is next?

DPA contest v4.2

- Atmel ATMega-163 smart card
- Each state byte has its own mask (4 bit entropy)
- Shuffling
- Fully written in ASM
- Register transfers checked carefully

$\Longrightarrow$ http://www.dpacontest.org/v4/42_doc.php




XILINX
Platform Cable USB II
USB

What is next?

DPA contest v4.3

- Tim Güneysu and Amir Moradi
- Generic Side-Channel Countermeasures for Reconfigurable Devices
- CHES 2011