Institut
Mines-Télécom

DPA contest status

CHES

September 2015

Saint-Malo, France

Nicolas BRUNEAU, Jean-Luc DANGER, Éloi DE CHERISEY, Guillaume DUC, Sylvain GUILLEY, Annelie HEUSER, Zakaria NAJM, Pablo RAUZY, Olivier RIOUL, Laurent SAUVAGE

September 2015

DPA contests

- Organized by Télécom ParisTech
- History
  - *V1* : attack contest, hardware implementation of DES on an ASIC
  - *V2* : attack contest, hardware implementation of AES on a FPGA
  - *V3* : acquisition contest, hardware implementation of AES on a FPGA (organized by *AIST*, Japan)

  - *V4* : attack contests, protected implementation of AES :
    - V4.1 protected SW AES implementation
    - V4.2 better protected SW AES implementation
  - Under study : *V5* (do not hesitate to contact us if you have ideas)

DPA contest purpose

- Benchmarking
- Education
- Publications
  - JCEN article with the V2 results (DOI : 10.1007/s13389-014-0075-9)
  - *Article about the submissions to v4.1 is being prepared (the participants will be contacted during September 2015)*
  - Thank you to cite the dpacontest website `http://www.dpacontest.org`

You are invited to use the DPA contest traces !

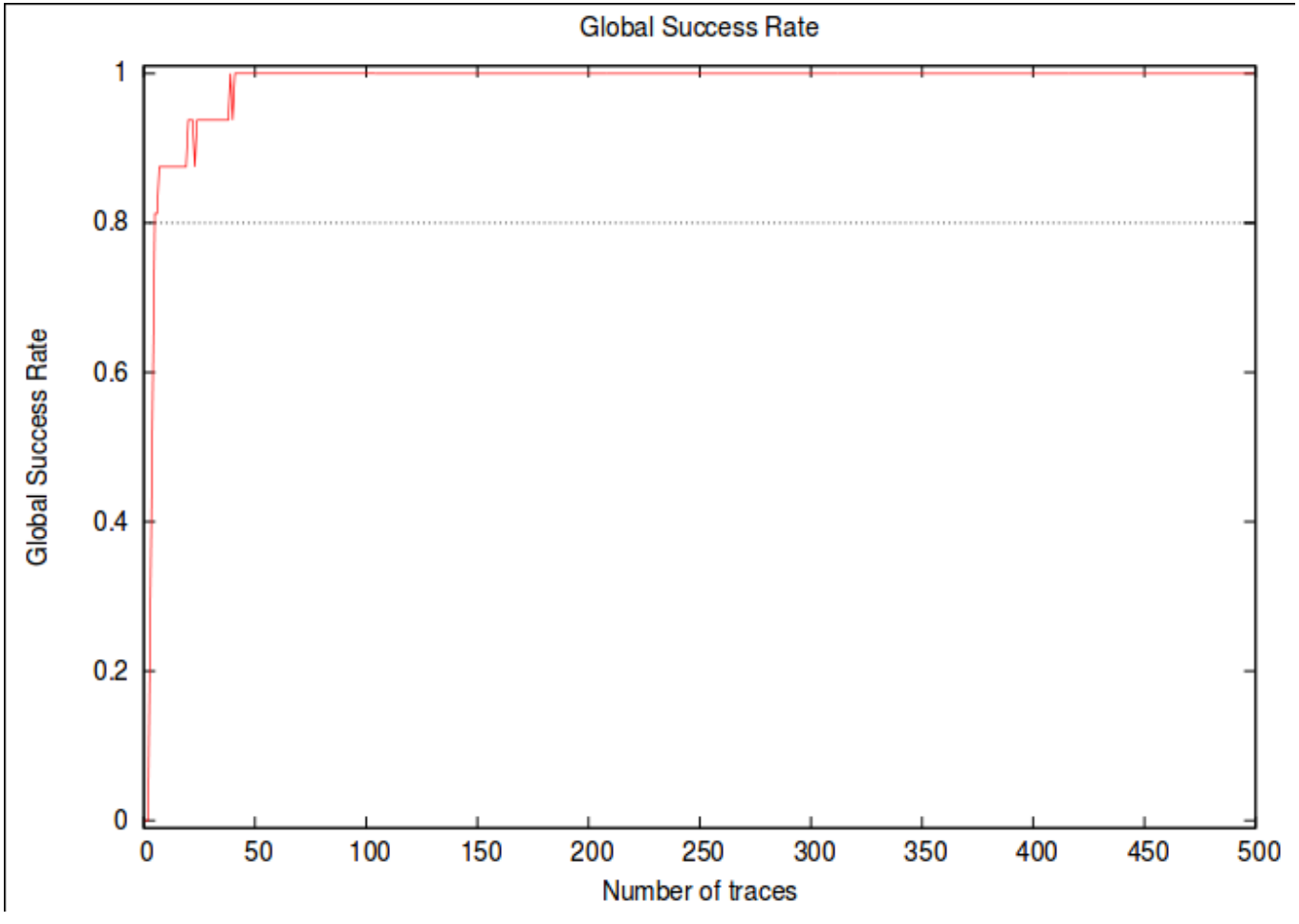
News

- July 2015 : new reference acquisitions for v4.2 to correct the bug discovered in October 2014
- July 2015 : new version of the tools (version 2.2) that provides more precise samples to the attack (use gain and offset information of each trace)
- August 2015 : creation of an announcement mailing list
- August 2015 : a new bug was discovered in v4.2 by Zdeněk Martinásek et Liran Lerman...

v4.2 participants

- Two different anonymous participants
- Liu Junrong, Guo Zheng, Zhang Chi, Xu Sen, Wang Weijia, Bao Sigang (SJTU-SHHIC Co-Lab of Data Security and Protection, Shanghai Jiao Tong University), China
- Tsunato Nakai, Daiki Tsutsumi, Mitsuru Shiozaki, Takaya Kubota, Takeshi Fujino (Ritsumeikan University), Japan
- **Li Yang, Wang Weiqi, Zhang Chi (Shanghai Fudan Microelectronics Group Company Limited), China**
- Zdeněk Martinásek (Faculty of Electrical Engineering and Communication, Brno University of Technology), Czech Republic
- Hideo Shimizu (Toshiba Corporation Corporate Research & Development Center), Japan

Example of extra-fast attack !



Stay tuned !

- Website (`http://www.dpacontest.org`)
- Twitter account : DPAContest
- New announcement mailing list (see the website for subscription)

The team ... has turned out pirate !

The team ... has turned out pirate !