Institut
Mines-Télécom

DPA contest v4

COSADE
March 7–8, 2013
Paris, France

Guillaume Duc
March 7–8, 2013

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)
  - v4...

DPA contests

- Purpose
  - In addition to the “contest”, DPA contests are often used as a benchmarking tool and for educational purpose
  - If you use the DPA contests traces/results/..., we would be pleased to know
- To improved scientific return on investment, a collaborative article on attack submitted to the v2 has been submitted to JCEN at beginning of 2013

DPA contest v4

Introduction

- Attack contest (like v1 and v2)
- Targets software implementation of AES
- Different implementations :
  - One not protected (some say that software implementations are easy to attack so it will be an opportunity to verify this assumption)
  - Several implementations with counter-measures (more challenging)
  - Submission of new counter-measures will be possible

DPA contest v4

Introduction

- Traces from a reference acquisition campaign will be published on our website for each implementation (like in v1 and v2)
- Measurements will be performed using the SASEBO-W board
- All details of the implementations will be given to allow participants to perform their own acquisitions (like in v3)
- Same evaluation protocol and metrics as in v2

DPA contest v4

When ?

- Now...

DPA contest v4

When ?

- Now...
- ... Sorry not yet but soon

DPA contest v4

When ?

- Launch date was postponed several times, mainly due to lack of manpower (problem solved now)
- Will do our best to launch a first iteration (with the not protected implementation and one implementation with counter-measure) before summer
- So stay tuned !
  - Website (`http://www.dpacontest.org`)
  - Twitter account : DPAContest