

Overview of the 2009-2010 'DPA contest v2'

Guillaume DUC, Sylvain GUILLEY, Laurent SAUVAGE,
Florent FLAMENT, Maxime NASSAR, Nidhal SELMANE,
Jean-Luc DANGER, Tarik GRABA, Yves MATHIEU & Renaud
PACALET. < contact@DPAcontest.org >

Institut TELECOM / TELECOM-ParisTech
CNRS – LTCI (UMR 5141)



CHES'10, August 19th, 2010,
Santa Barbara, CA, USA.

- As the **v1**, it is a **key recover attack** contest
- **More than 1,000,000 side-channel measurements** (*traces*) are freely available worldwide from a PostgreSQL database.
- NIST AES 128-bit parallel block cipher encryption,
- **SASEBO-GII** board,
- Clock signal is **stable**: traces **synchronization** is perfect,
- Measurement bandwidth is **5 GHz**, and sampling rate is **5 Gsample/s**. The oscilloscope is configured to average the traces 128 times. The FPGA runs at 24 MHz and there are 3253 samples per trace. Thus, we have:
 - 208.333 samples per clock, and
 - 15.6 clocks per trace (*i.e.* more than the 10 rounds).
- Vertical resolution is **8.0 effective bits** (no averaging).

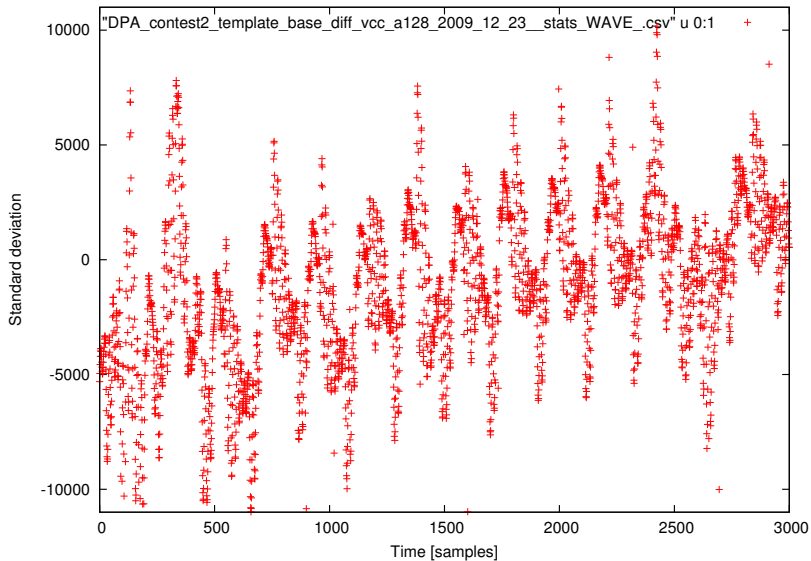
Specificity of this second edition

- Profiling is permitted.
- Evaluation using built-in success rate and guessing entropy metrics.

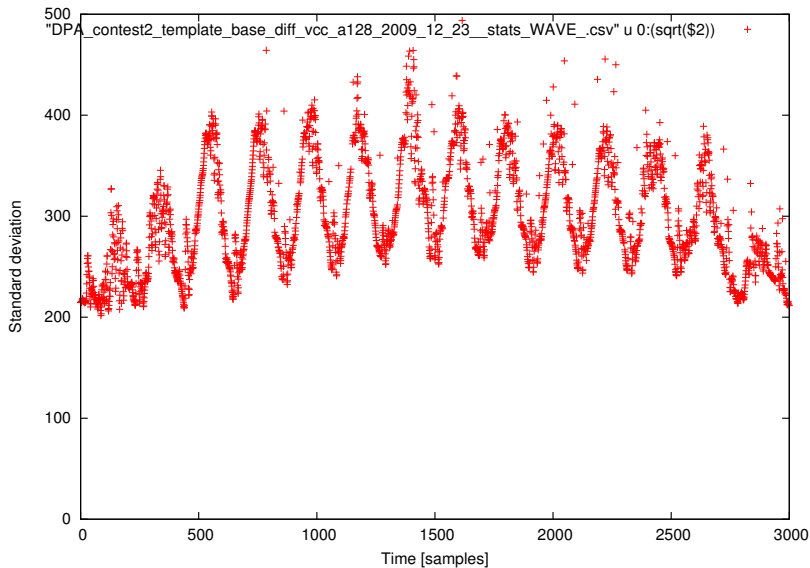
| Training | Matching (public) | Matching (private) |
|------------------|--------------------------|---------------------------|
| 1,000,000 traces | — | — |
| — | 32 × 20,000 traces | — |
| — | — | 32 × 20,000 traces |

Signal / Noise ratio: ≈ 0.0078 .

Average curve

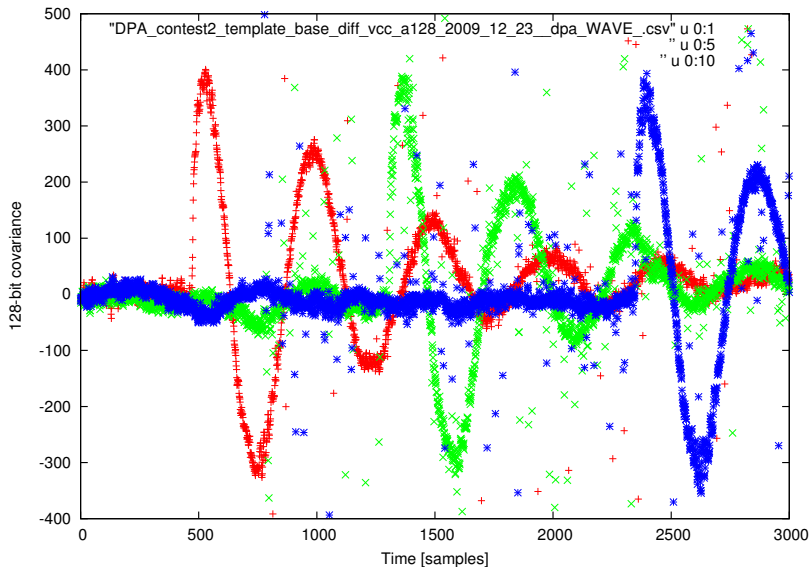


Standard Deviation curve



128-bit covariance curve

(Hamming distance model for rounds 1, 5 & 10)



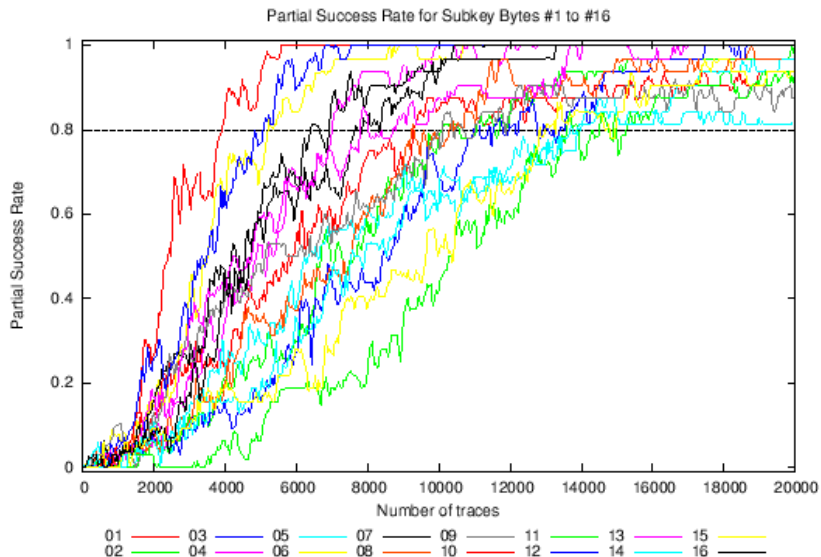
Participants

| 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 TELECOM-ParisTech | 1 attack |
| Reference attack | TELECOM-ParisTech | 1 attack |

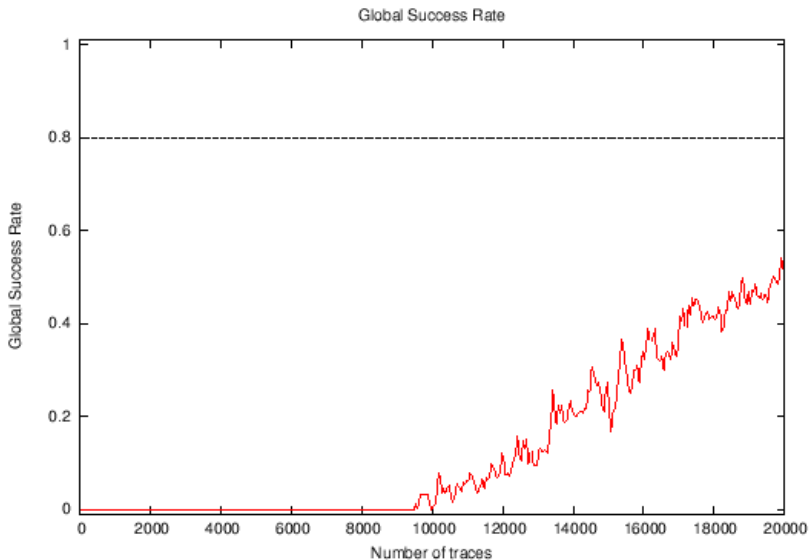
How your attack is processed?

- You get a 25-page PDF with an exhaustive security evaluation
 - comes with the figures and \LaTeX source code:
 - \Rightarrow directly reusable for publications.
- Partial/global success rate
- Partial guessing entropy

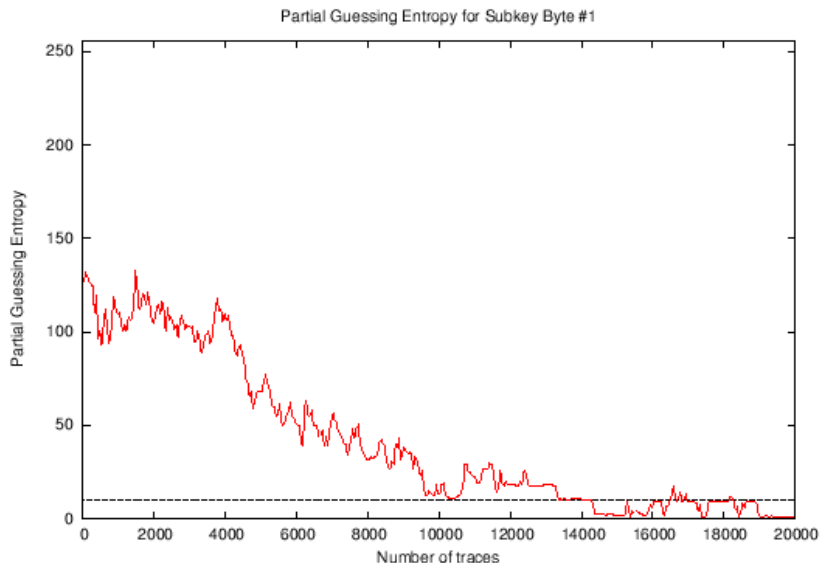
Partial success rate



Global success rate



Partial guessing entropy



Some Results

| Attack | GSR >80% | Min PSR >80% | Max PGE <10 | GSR stable >80% | Min PSR stable >80% | ... |
|-------------------------------|-------------|-----------------|----------------|--------------------|------------------------|-----|
| Reference | F | 13,876 | F | F | 15,316 | ... |
| Template | F | F | F | F | F | ... |
| A. Bonnecaze, IML ERISCS DPA | F | F | 9561 | F | F | ... |
| A. Bonnecaze, IML ERISCS SPE | 17 340 | 11 818 | 5908 | 18 458 | 12 318 | ... |
| A. Bonnecaze, IML ERISCS VAR | F | F | 18 938 | F | F | ... |
| A. Bonnecaze, IML ERISCS VDPA | F | F | 15 191 | F | F | ... |
| A. Bonnecaze, IML ERISCS CVM | F | F | 15 516 | F | F | ... |
| A. Wurcker, UNILIM A | 13 474 | 11 501 | 4 179 | 19 858 | 12 631 | ... |
| A. Wurcker, UNILIM B | F | 11 525 | 4 179 | F | 12 866 | ... |

| ... | Max PGE stable < 10 | GSR 20k | Min PSR 20k | Max PSR 20k | Min PGE @20 k | Max PGE 20k | Time per Trace |
|-----|------------------------|------------|----------------|----------------|------------------|----------------|-------------------|
| ... | F | 0.53 | 0.81 | 1.00 | 1.00 | 40.25 | 1.10 s |
| ... | F | 0.19 | 0.35 | 1.00 | 1.00 | 37.84 | 0.05 s |
| ... | 9629 | 0.41 | 0.75 | 1 | 1 | 1.72 | 0.00 s |
| ... | 6262 | 0.88 | 0.94 | 1 | 1 | 1.06 | 0.83 s |
| ... | 19631 | 0.53 | 0.69 | 1 | 1 | 9.16 | 0.00 s |
| ... | 17646 | 0.25 | 0.53 | 1 | 1 | 5.22 | 0.00 s |
| ... | 17526 | 0.44 | 0.69 | 1 | 1 | 6.56 | 0.31 s |
| ... | 4192 | 0.81 | 0.88 | 1 | 1 | 1.16 | 0.25 s |
| ... | 4192 | 0.69 | 0.88 | 1 | 1 | 1.16 | 0.25 s |

F = Fails.

If we let part:

- *Automatic spam* and
- *human SQL injection* attempts,

there are those real issues left:

- Attacks' language standardization not completed:
(C++, C#, matlab);
- Industrial worried about submitting code;
- Access to the database uneasy.

- Final debriefing at **COSADE**'2011, in January/February at Darmstadt.
- Remember that participants to the DPA contest 2nd edition are eligible for a free SASEBO GII board.
- 3rd edition:
 - Acquisition contest in parallel to the attack contest
 - Protected implementation
 - Opinion pool for the type of countermeasure