'DPA contest' Mid-Term Report [6]

Sylvain GUILLEY, Laurent SAUVAGE, Florent FLAMENT,
Maxime NASSAR, Nidhal SELMANE, Jean-Luc DANGER,
Tarik GRABA, Yves MATHIEU & Renaud PACALET.

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

CryptArchi'09, June 24-27, 2009,
Prague, Czech Republic.

Presentation Outline

What is this http://www.DPAcontest.org/?

- It is a **key recover attack** contest
- **80k+ side-channel measurements** (*traces*) are freely available
- They have been measured **on a real circuit**, but are **ideal**:
  - Clock signal is **stable**.
  - Traces **synchronization** is perfect.
  - Power curves concern the DES crypto-processor **alone**.
  - Measurement bandwidth is **5 GHz**, and sampling rate is **20 Gsample/s**.
  - Horizontal resolution is **12.0 effective bits**.

Motivation + Ethics

Advantage

- Makes it possible for a laboratory **w/o measurement facilities** to experiment security evaluation algorithms.
- Allows a **fair comparison** of known attacks and tricks.
- **Stimulates the research** for better power attacks.

Ethics

- Such a contest on a **commercial** product would endanger all its users.
- Thus only a **public research group** can safely share measures from an **home-made academic circuit**.
- **Open source = danger**?
  No = possibility to improve on top of others' ideas!

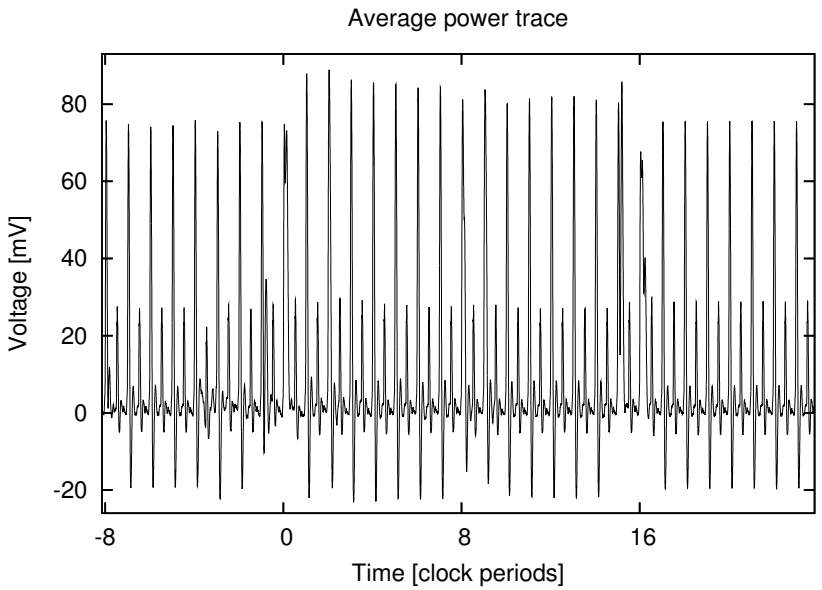
On-Line Example

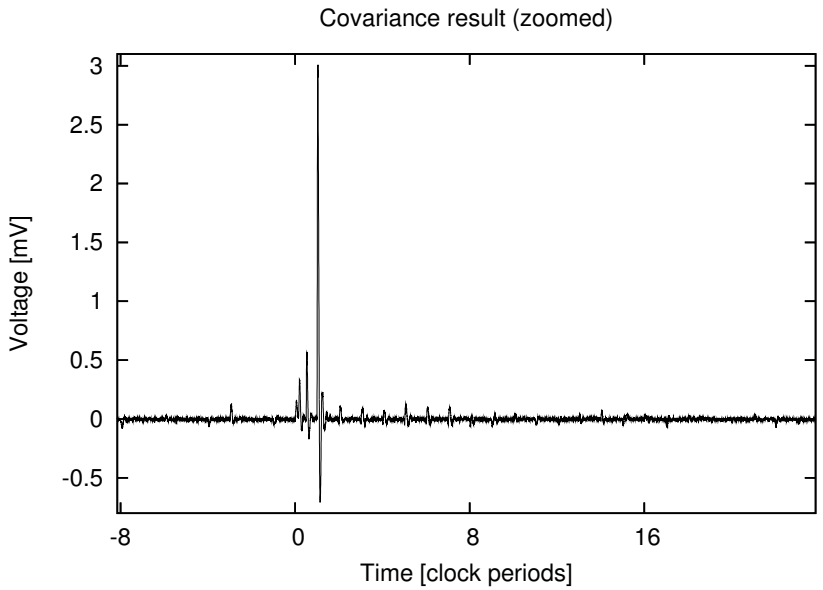
- Demonstration of the contest simplicity:

```
> svn co https://svn.comelec.enst.fr/dpacontest/
> cd code/reference/
> python main.py

# Table: secmatv1_2006_04_0809
# Stability threshold: 100
# Iteration threshold: 1800
#
# Columns: Iteration Stability Subkey0 ... Subkey7
   1
   2
   3
   ...
```

Reference attack





Rules

A valid attack shall:

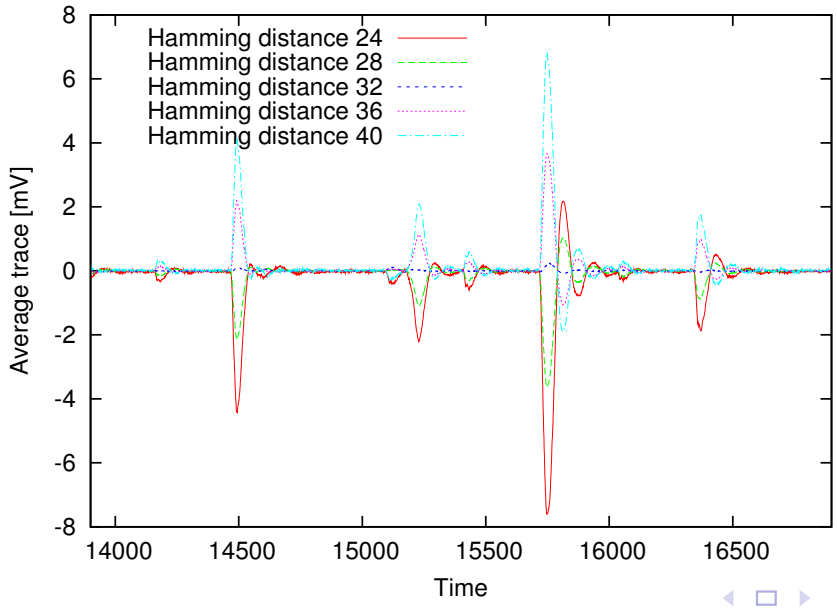
- **recover the correct key** with **a stability of additional 100 traces** usage.
- consist in **source code**, committed into an SVN repository.

The hall of fame is based on:

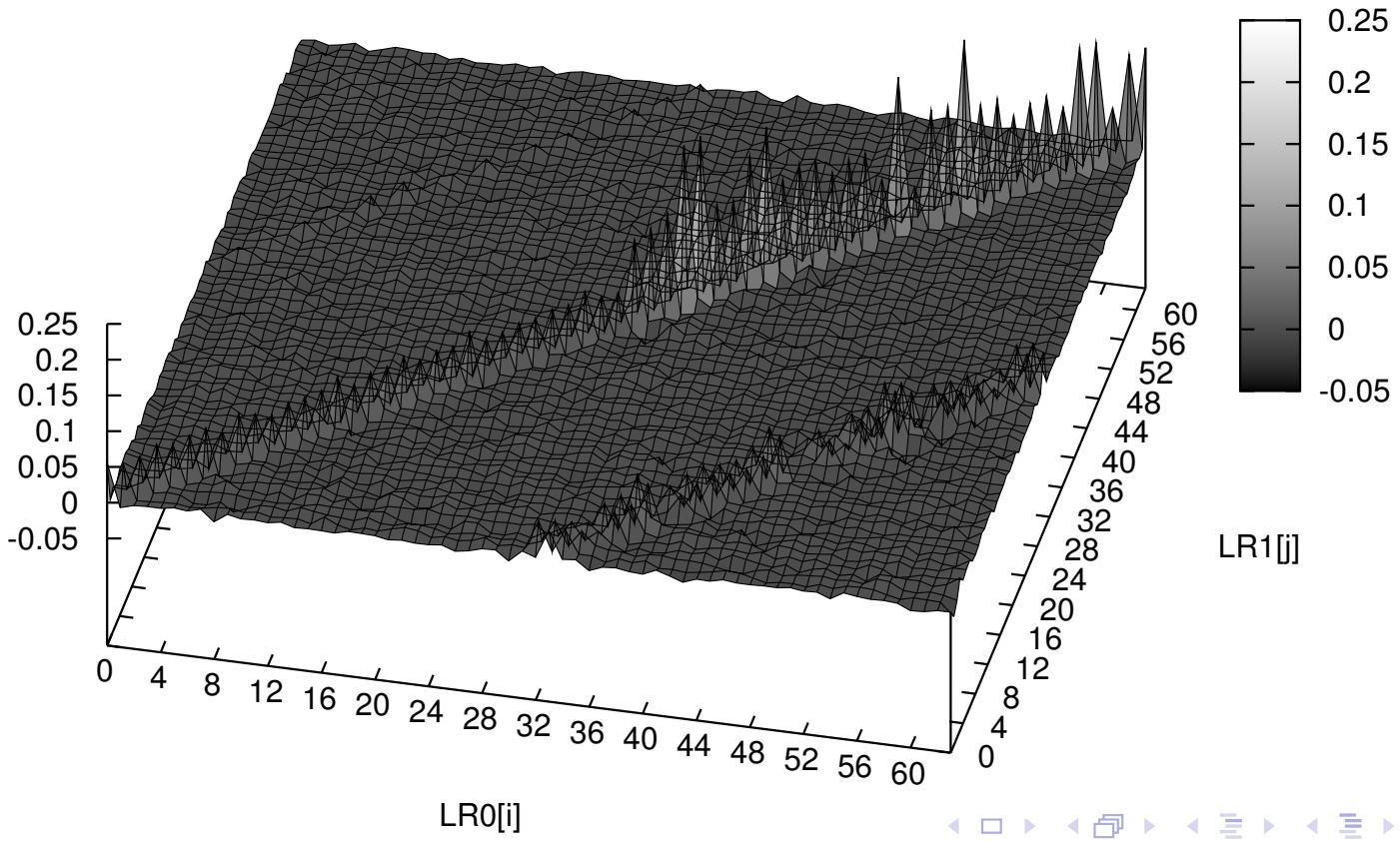
- An **eligibility** that is verifiable on a **peer-review** basis.
- The date of the **commit**, which must belong to: [Aug 12th 2008, Sep 6th 2009].

Presentation Outline

- Excellent **linear** and **temporally localized** leakage. Hence:
  - HO-DPA not suitable (need multiple sources of leakage).
  - Generalized CPA [1] or MIA [2] (with practical aspects detailed in [4]) are more appropriate for noisy signals.
  - **Boolean equations solving** (*cf.* work of Cédric Tavernier and Thomas Roche) is another credible option:
    stddev $\approx 3 \times \Delta$(avg).
  - Classical correlation power analysis (CPA) is preferred.

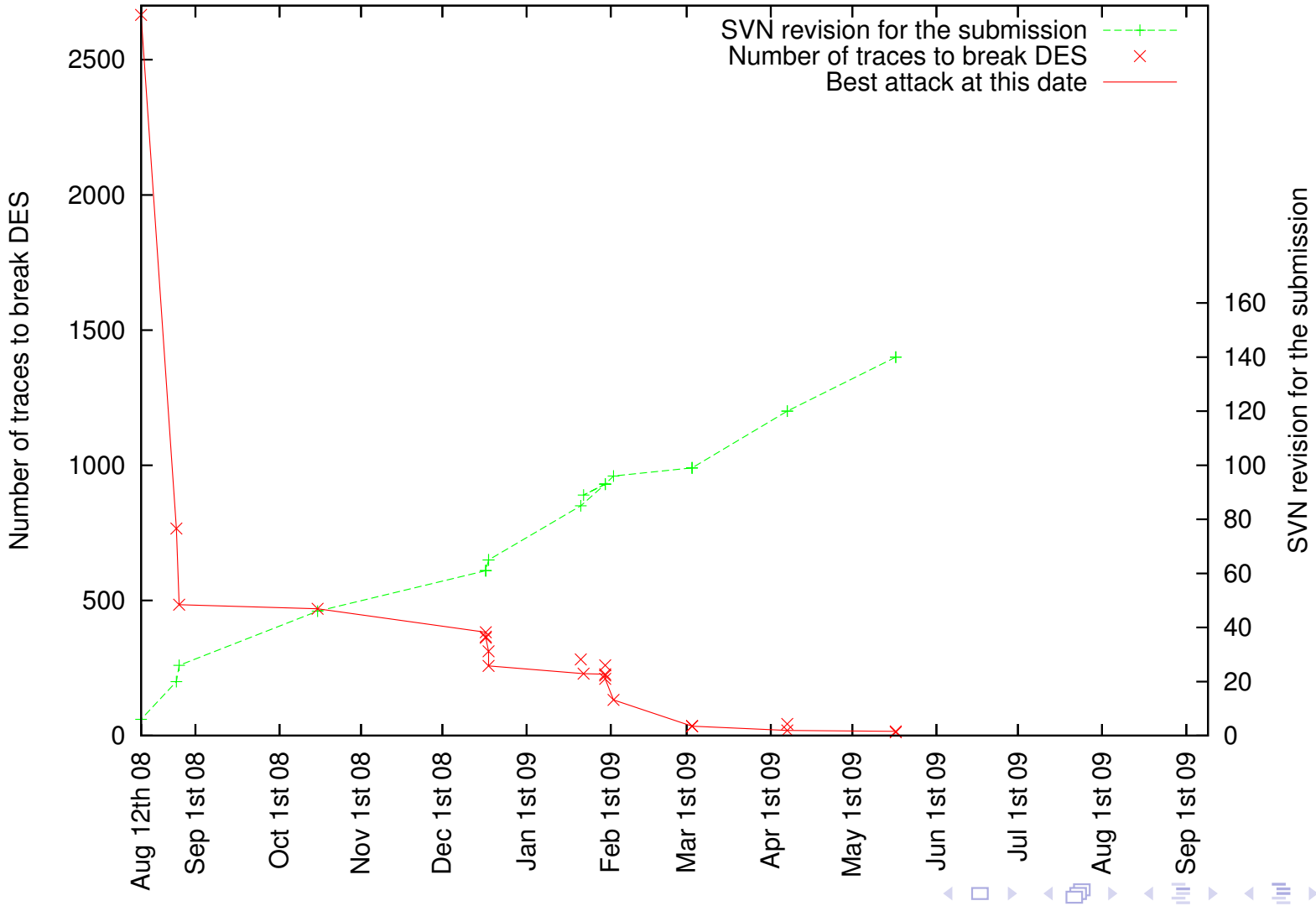


$\hat{\rho}(LR0[i], LR1[j])$ Estimation over the 80k Traces



Presentation Outline

Best Attacks



Hall of Fame Split in Four Categories

1. **Representative order**: the attacks have been carried out on various significative sets of traces.
2. **Chosen plaintext order**: where the traces order is computed by an algorithm that is explicited in the attack source code.
3. **Fixed order**: that models an attack at known albeit not chosen plaintext or ciphertext. The order is either
   - that of the database without the `SORT BY` clause, or
   - that of the ZIP archive.
4. **Custom order**: left at the discretion of the attacker . . . of course, an explanation of the sorting strategy is preferred.

Records, per Category

1. **Representative order**: . . . . . none so far
2. **Chosen plaintext order**: . . . . . none so far
3. **Fixed order**:
   - Best attack in **43** traces for a "Built-in determined Sub-key Correlation Power Analysis" (*a.k.a.* BS-CPA) using Pearson's correlation, described in [3] deposited by Yuichi KOMANO, Hideo SHIMIZU and Shinichi KAWAMURA (Toshiba Corporation, 2009 April 7th).
   - Worst attack in **2,666** traces for the "reference" implementation coded by Florent FLAMENT (TELECOM ParisTech, 2008 August 11th).

Records, per Category

1. **Representative order**: . . . . . none so far
2. **Chosen plaintext order**: . . . . . none so far
3. **Custom order**:
   - Best attack in **12** traces for a "DPA DoM 4bits on the 16th round of the DES selecting the good temporal window", deposited by Victor LOMNE (LIRMM, 2009 April 7th).
   - Worst attack in **312** traces for an attack that "exploits the $HW(L15 \oplus L16)$ (*last round*) CPA selection function", implemented by Victor LOMNE, (LIRMM, 2009 May 17th).

Outcome

Publications:

- Improving the rules of the DPA contest: [5].
- Attack of the harder sbox first: [3].

New attacks are based on one or more of the following techniques:

- pre-filtering the traces (window filters, or cropping),
- choice of the round to attack,
- number of key bits attacked simultaneously,
- number of unknown bits making up the selection function,
- statistical test to distinguish the correct guess from erroneous ones,
- taking advantage of the knowledge of the already broken sboxes to improve the correlation of hard to break sboxes.

Possible improvements:

- Attacking **all the sixteen** rounds
- Why is $\hat{\rho}(R0[i] \oplus R1[i])$ **much greater** for $i \in \{4, 5, 9, 17, 21\}$?

Presentation Outline

DPA Contest Popularity Indicators

Tableau de bord

12 août 2008 - 1 juin 2009

Fréquentation du site

2 604 Visites

8 672 Pages vues

3,33 Pages par visite

35,22 % Taux de rebond

00:04:12 Temps moyen passé sur le site

30,49 % Nouvelles visites (en %)

Vue d'ensemble des visiteurs

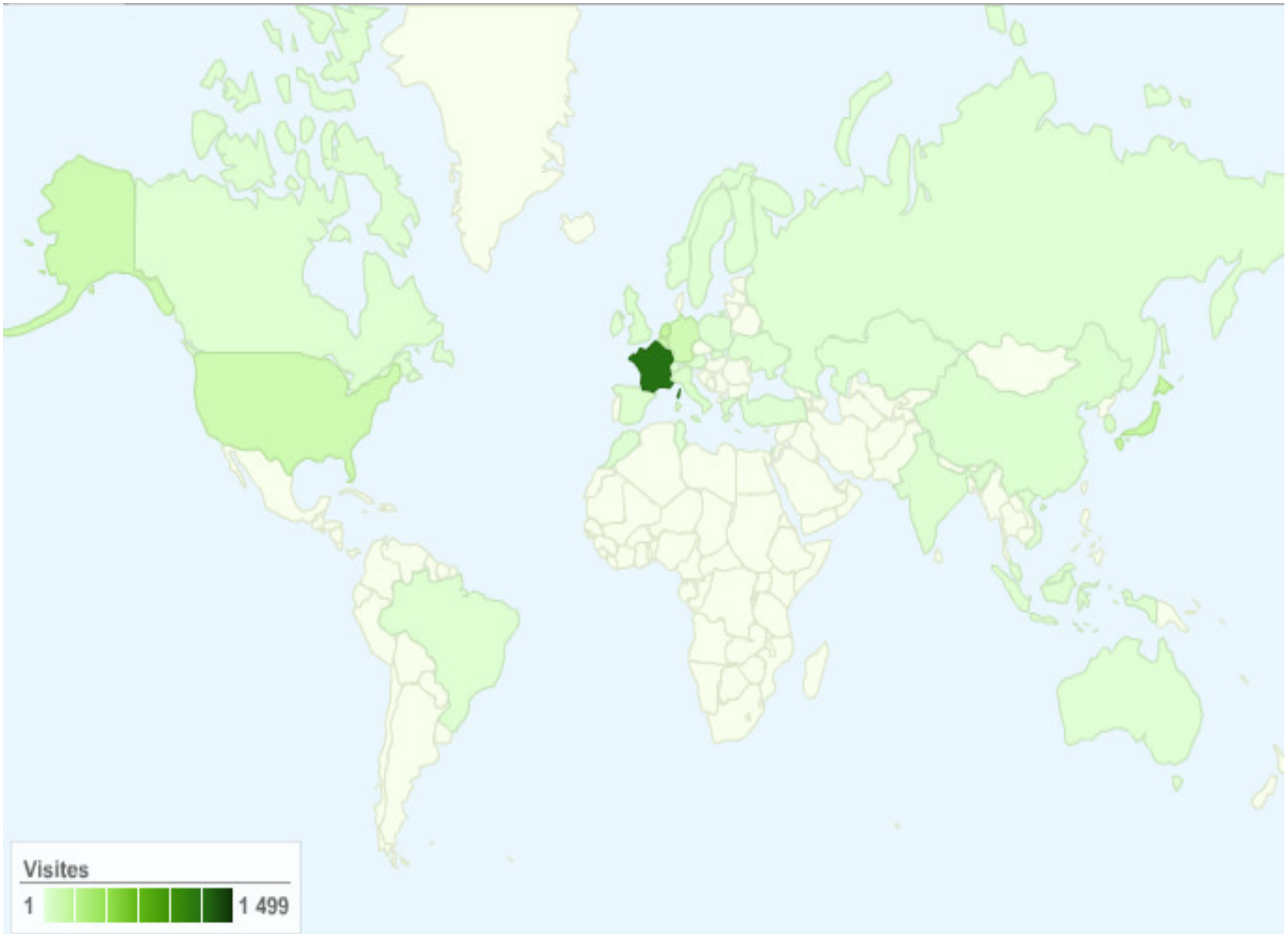
796 Visiteurs

Afficher le rapport

Synthèse géographique

Afficher le rapport

DPA Contest Map



DPA Contest Statistics

Visites	Pages par visite	Temps moyen passé sur le site	Nouvelles visites (en %)	Taux de rebond
2 604 Total du site (en %) : **100,00 %**	**3,33** Moyenne du site : **3,33 (0,00 %)**	**00:04:12** Moyenne du site : **00:04:12 (0,00 %)**	**30,57 %** Moyenne du site : **30,49 % (0,25 %)**	**35,22 %** Moyenne du site : **35,22 % (0,00 %)**

	Niveau de détail : Pays/Territoire	Visites ↓	Pages par visite	Temps moyen passé sur le site	Nouvelles visites (en %)	Taux de rebond
1.	France	**1 499**	3,33	00:03:43	29,22 %	35,89 %
2.	Netherlands	**225**	2,77	00:04:40	9,78 %	34,67 %
3.	Japan	**210**	3,29	00:04:11	20,00 %	24,29 %
4.	Belgium	**167**	3,34	00:03:56	34,73 %	32,34 %
5.	United States	**150**	3,57	00:06:25	42,67 %	37,33 %
6.	Germany	**135**	3,96	00:05:35	30,37 %	36,30 %
7.	South Korea	**43**	4,53	00:08:19	62,79 %	20,93 %
8.	Italy	**32**	2,06	00:02:05	34,38 %	71,88 %
9.	United Kingdom	**26**	2,92	00:02:22	34,62 %	42,31 %
10.	China	**18**	4,33	00:06:16	66,67 %	22,22 %

Presentation Outline

Conclusions

- The contest is a success (more than 20 attacks posted so far);
- However, some subtleties about the contest rules still remain:
  - **the order** in which the traces are consumed,
  - the amount of **initial knowledge** about the circuit's characteristics and/or its traces (for instance the temporal localization of the encryption rounds),
  - more generally, the use of **undocumented constants** in the attack code,
  - the possibility of using **simultaneously the known plaintext and ciphertext couple**.

2009–2010 Contest Features

- **Protected** circuit (DPL? masking?)
- **SASEBO** as an acquisition board and **EveSoC** as the environment
- On-demand traces acquisition (to train?)
- **AES** instead of **DES**?
- **Any other suggestion?**

References

[1] Sébastien Aumônier.
Generalized Correlation Power Analysis.
In *ECRYPT Workshop "Tools for Cryptanalysis"*, 24-25 September 2007.
Krakow, Poland, PDF.

[2] Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel.
Mutual information analysis.
In *CHES*, volume 5154 of *Lecture Notes in Computer Science*, pages 426–442. Springer, August 10-13 2008.
CHES 2008, 10th International Workshop, Washington, D.C., USA.

[3] Yuichi Komano, Hideo Shimizu, and Shinichi Kawamura.
Build-in determined sub-key correlation power analysis.
Cryptology ePrint Archive, Report 2009/161, 2009.
http://eprint.iacr.org/2009/161.

[4] Emmanuel Prouff and Matthieu Rivain.
Theoretical and Practical Aspects of Mutual Information Based Side Channel Analysis.
In Springer, editor, *ACNS*, volume 5536 of *LNCS*, pages 499–518, June 2-5 2009.
Paris-Rocquencourt, France.

[5] François-Xavier Standaert, Philippe Bulens, Giacomo de Meulenaer, and Nicolas Veyrat-Charvillon.
Improving the Rules of the DPA Contest.
Cryptology ePrint Archive, Report 2008/517, 2008.
http://eprint.iacr.org/2008/517.

[6] Sylvain Guilley and Laurent Sauvage and Florent Flament and Maxime Nassar and Nidhal Selmane and Jean-Luc Danger and Tarik Graba and Yves Mathieu and Renaud Pacalet.
Mid-Term Report of the DPA Contest.
In *CryptArchi*, Prague, Czech Republic, June 24th–27th 2009.