Overview of the 2008-2009 'DPA contest'

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)

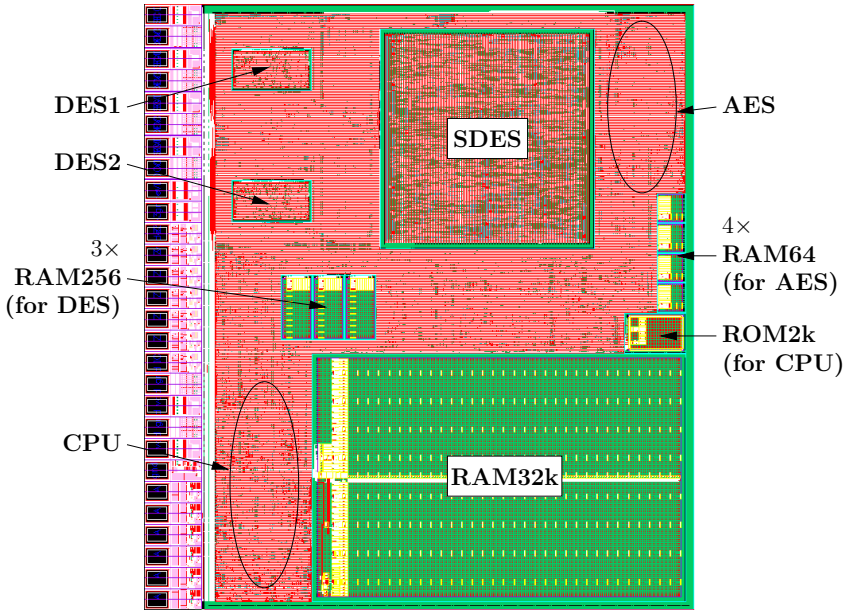
CHES'09, September 7th, 2009,
Lausanne, Switzerland.

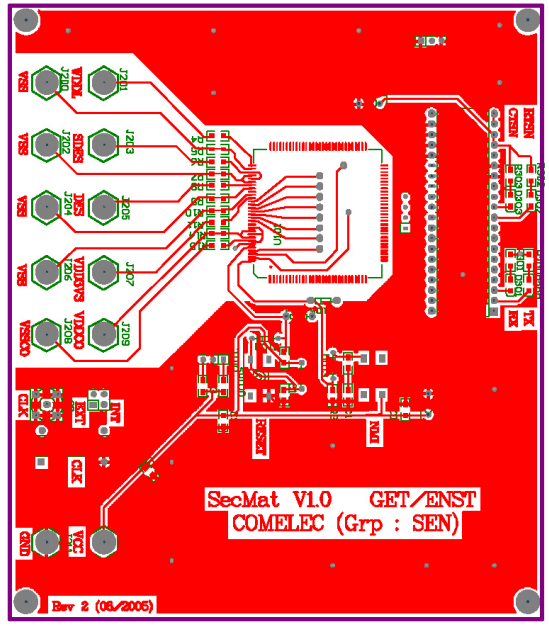
Presentation Outline

Presentation Outline

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

- It is a **key recover attack** contest
- **80k+ side-channel measurements** (*traces*) are freely available worldwide from a PostGreSQL database.
- They have been measured **on a real circuit**, but are somehow **ideal**, hence suitable for academic studies:
  - 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**.
  - Vertical resolution is **12.0 effective bits**.





Purpose	Characterization and attack on the symmetric encryption algorithms DES (`fips46-3`) and AES (`fips197`)
Programmation	C language, configuration via an RS232 or a USB port
Chip's size	4.0 mm^2, 2.0 million transistors
Power domains	5: pads (3.3 V), core + DES1 + DES2 + SDES (1.2 V)
Technology	STMicroelectronics 130 nanometer low-leakage (high Vt) with 6 layers of metal process, founded at Crolles, FRANCE
Fabrication	CMP run **S12C5_1** (13/01/2005) with the help of ST/AST

More information online: http://cmp.imag.fr/aboutus/gallery/details.php?id_circ=63&y=2005.

Motivation + Ethics

Advantages

- 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!

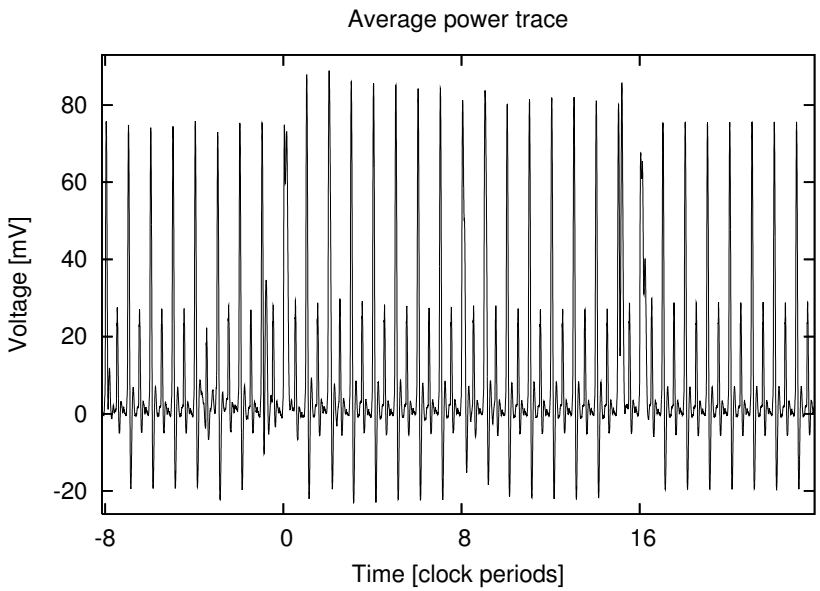
Example with the reference code

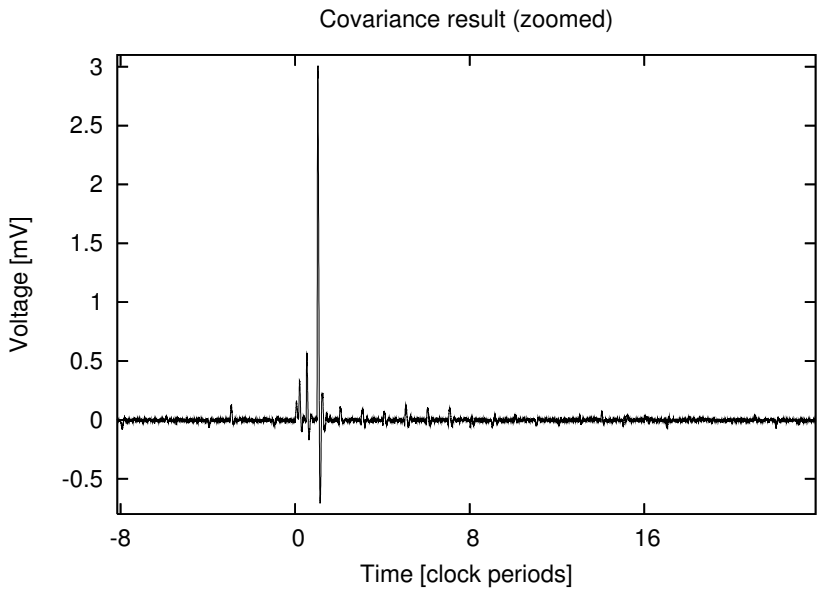
- **Demonstration of the contest simplicity:**

```
> 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: Difference-of-Means [P. Kocher, 1998]





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.

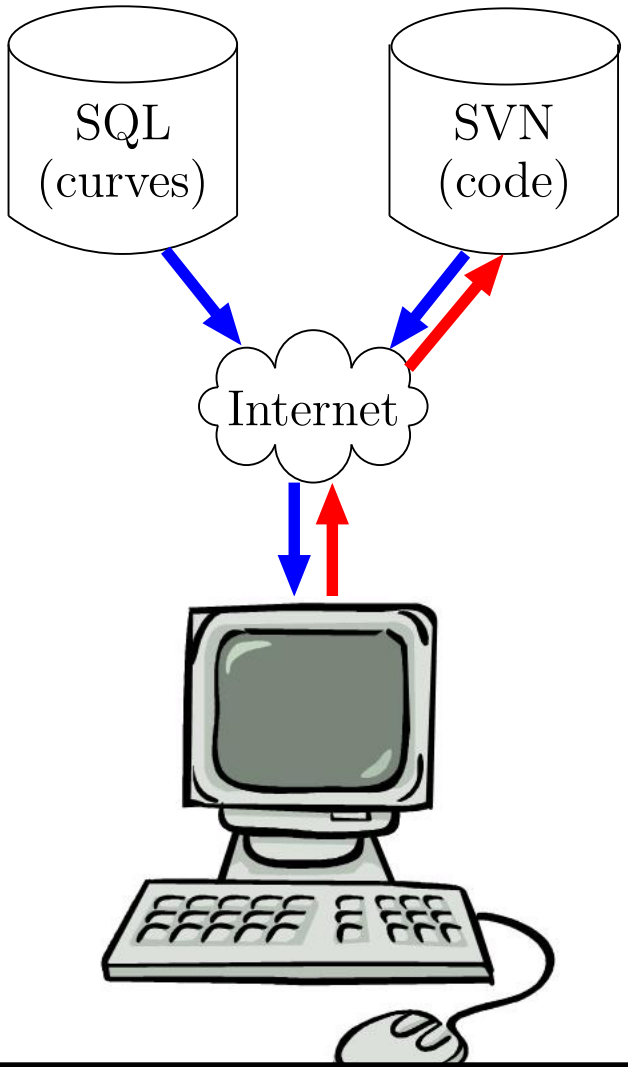
The hall of fame is based on:

- An **eligibility** that is verifiable on a **peer-review** basis.
- Objective: use **as few traces as possible**.
- The date of the **commit**, which must belong to: [Aug 12th 2008, Aug 30th 2009].

Presentation Outline

Two Kinds of Involvements

Download & **Contribute**



Observers: download the traces and/or the attack source code.

- Key figure: 4,355 visits.

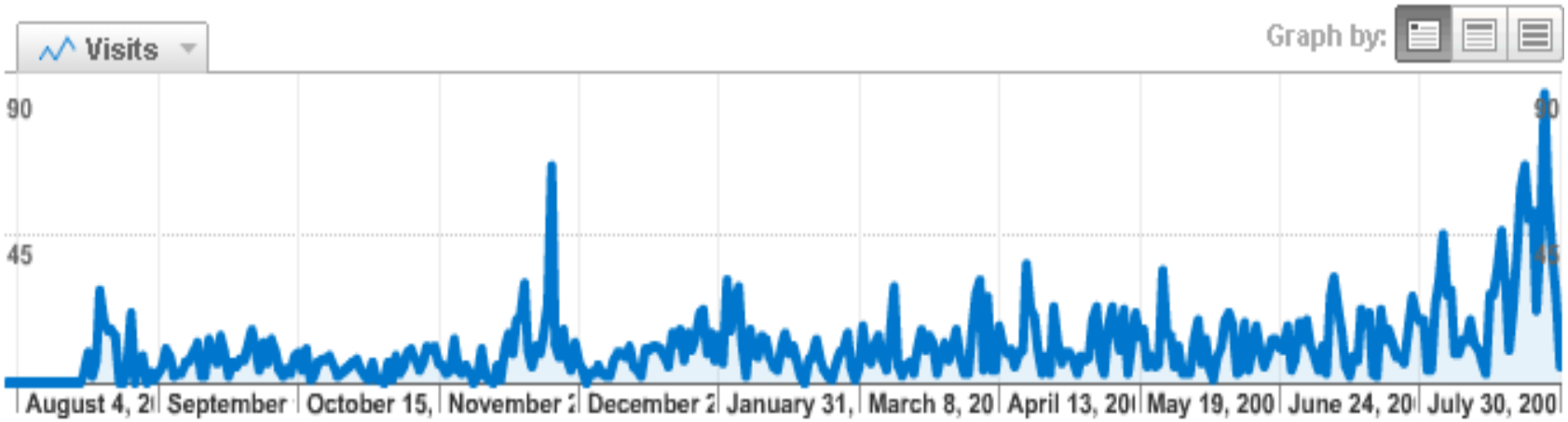
Players: upload attack source code.

- Key figure: 44 submissions.

DPA Contest Popularity Indicators

Dashboard

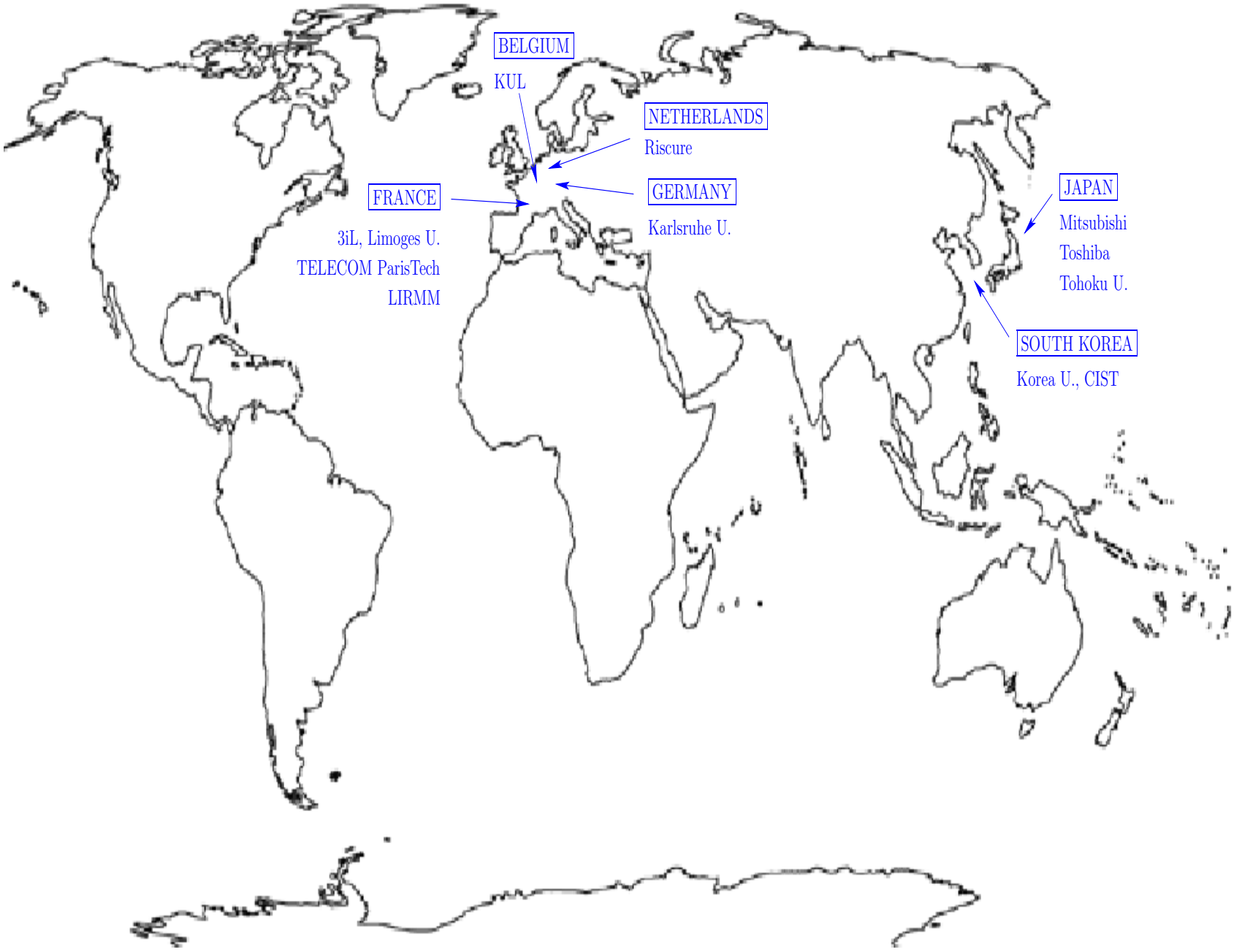
Aug 1, 2008 - Sep 4, 2009



Site Usage

4,355 Visits	**35.29%** Bounce Rate
14,050 Pageviews	**00:04:25** Avg. Time on Site
3.23 Pages/Visit	**25.81%** % New Visits

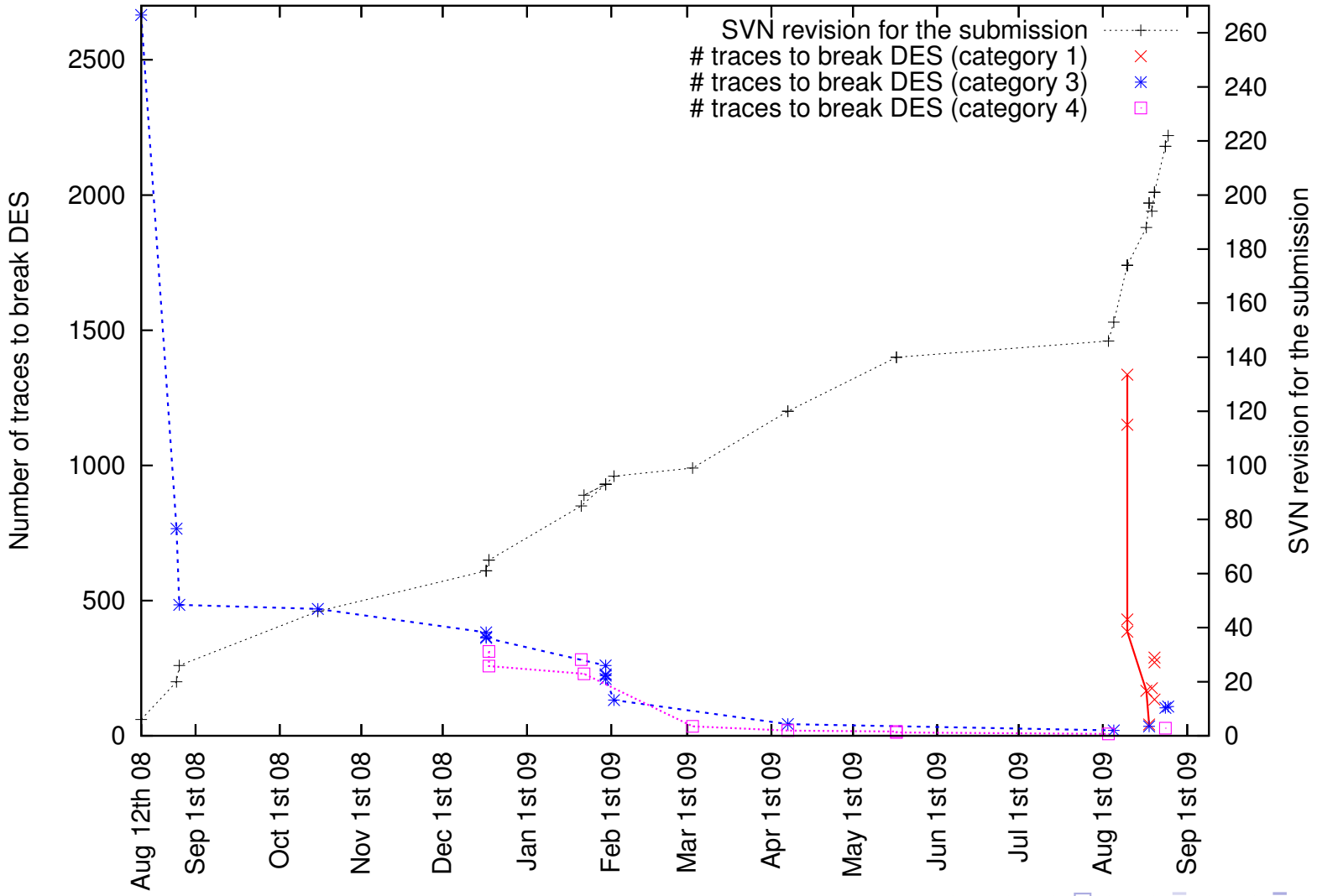
DPA Contest Map: 45 countries / territories



Hall of Fame Split in Four Categories

1. **Order-independent**: the attacks have been carried out on various significant sets of traces, ordered in a *random* way.
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, or
   - lexicographical (corresponding to acquisition order).
4. **Custom order**: left at the discretion of the attacker ... of course, an explanation of the sorting strategy is preferred.

Events for each category



Category	# Attacks	Best attack
#1	17	141.42 traces, by Christophe Clavier of 3iL & U. of Limoges, FRANCE.
#2	0	No submission ☹.
#3	17	120 traces, by Daisuke Suzuki & Minoru Saeki of Mitsubishi, JAPAN.
#4	10	107 traces, by Hideo Shimizu of Toshiba, JAPAN.
Total	44	$\longrightarrow$ *winner chosen as the best submission in category #1.*

Presentation Outline

Campaign Characteristics

- **Unprotected** and **little noisy** traces.
- Excellent **linear** and **temporally localized** leakage.

Hence:

- The dominant strategy has been **model-based** attacks:
  - Differential Power Analysis or
  - Correlation Power Analysis,

Overview of the State-of-the-Art Advance [1/4]

New attacks are based on one or more of these techniques:

- **Pre-filtering** the traces (window filters, or cropping):
  - Victor LOMNE from LIRMM was the first to attack the last round and to select a good temporal window
- Choice of which **round** to attack:
  - Daisuke SUZUKI from Mitsubishi dual round attack by BS-CPA
- **Number of key bits** attacked simultaneously:
  - Eloi SANFELIX from Riscure attacked two sboxes simultaneously

Overview of the State-of-the-Art Advance [2/4]

New attacks are based on one or more of these techniques:

- Number of unknown bits making up the **selection function**:
  - Most attacks were multi-bit, and Daisuke SUZUKI proposed an improved power model
  - Antonio SOBREIRA from Universität Karlsruhe performed a classical CPA considering the left side of the message register
- **Statistical test** to distinguish the correct guess from erroneous ones:
  - Benedikt GIERLICHS from KUL implemented a t-test;
  - Yongdae KIM from Tohoku University tested Pearson, Kendall and Spearman correlations

Overview of the State-of-the-Art Advance [3/4]

New attacks are based on one or more of these techniques:

- Taking advantage of the **knowledge of the already broken sboxes** to improve the correlation of hard to break sboxes:
  - Hideo SHIMIZU from Toshiba coined the Built-in determined Sub-key Correlation Power Analysis (BS-CPA), described in http://eprint.iacr.org/2009/161.
- **Cooperation** between hypotheses:
  - Renaud PACALET from TELECOM ParisTech finds the best key candidates by optimization algorithm based on the theory introduced by Xiaofei Huang

Overview of the State-of-the-Art Advance [4/4]

New attacks are based on one or more of these techniques:

- On-line **model estimation**:
  - Christophe CLAVIER estimated on-line a multi-variate linear model
- **Stochastic model** attack:
  - contributed by Yongdae KIM from Tohoku university
- **Multi-DPA**:
  - Jung HAE-IL from Korea University combined multi-bit DPA of Thomas MESSERGES and Régis BEVAN
- **Combined attacks**:
  - *e.g.* BS-CPA on 2-sboxes by Laurent SAUVAGE, from TELECOM ParisTech

Presentation Outline

2008–2009 Winner

Congratulations!

Winner identity

Name	Prof. Christophe CLAVIER
Affiliation #1	Institut d'Ingénierie Informatique de Limoges (3iL), 42 rue Sainte Anne, 87 000 Limoges.
Affiliation #2	Université de Limoges – Laboratoire XLIM, 83 rue d'Isle, 87 000 Limoges, FRANCE.

Winning attack

Attack algorithm	Maximum likelihood method with a bivariate *known* model
Number of traces	141.42 traces as an average success rate, estimated with 100 attacks
SVN tag	Revision 197, 2009 August 18th