Results 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 >

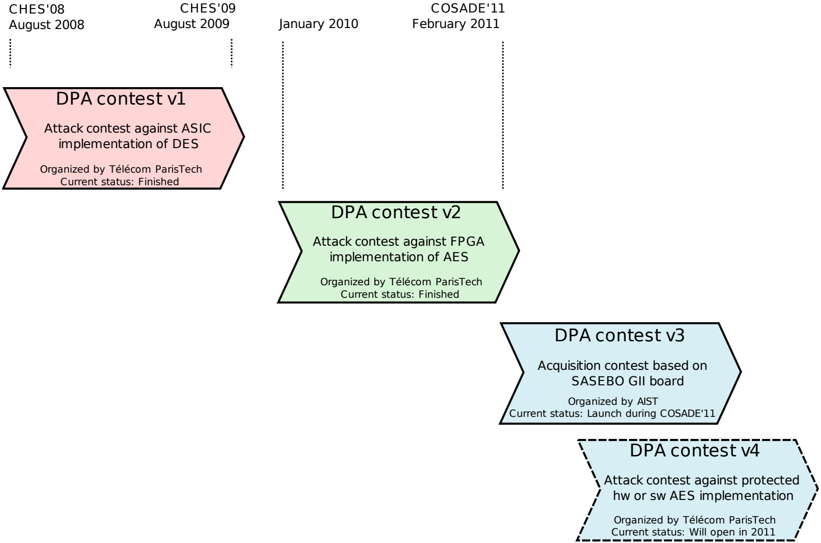
Institut Télécom / Télécom ParisTech
CNRS – LTCI (UMR 5141)

COSADE'11, February 24th, 2011
Darmstadt, Germany

Presentation Outline

1. Introduction
2. Results
3. Overview of the attacks
4. Conclusion

The DPA contest(s)



CHES'08
August 2008

CHES'09
August 2009

January 2010

COSADE'11
February 2011

DPA contest v1

Attack contest against ASIC implementation of DES

Organized by Télécom ParisTech
Current status: Finished

DPA contest v2

Attack contest against FPGA implementation of AES

Organized by Télécom ParisTech
Current status: Finished

DPA contest v3

Acquisition contest based on SASEBO GII board

Organized by AIST
Current status: Launch during COSADE'11

DPA contest v4

Attack contest against protected hw or sw AES implementation

Organized by Télécom ParisTech
Current status: Will open in 2011

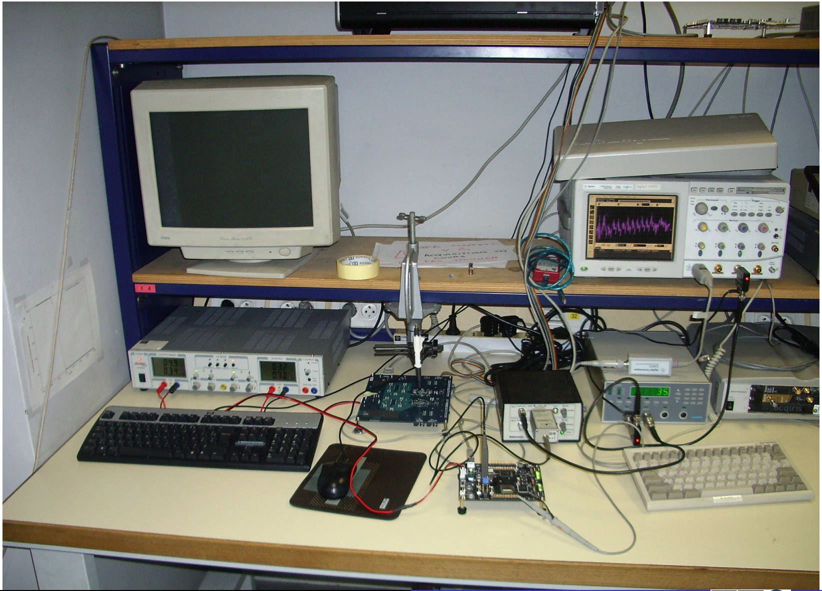
What is this DPA contest v2?

- As the v1, it is a **key recover attack** contest
- **More than 1,000,000 side-channel measurements** (*traces*) are freely available worldwide
- 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).

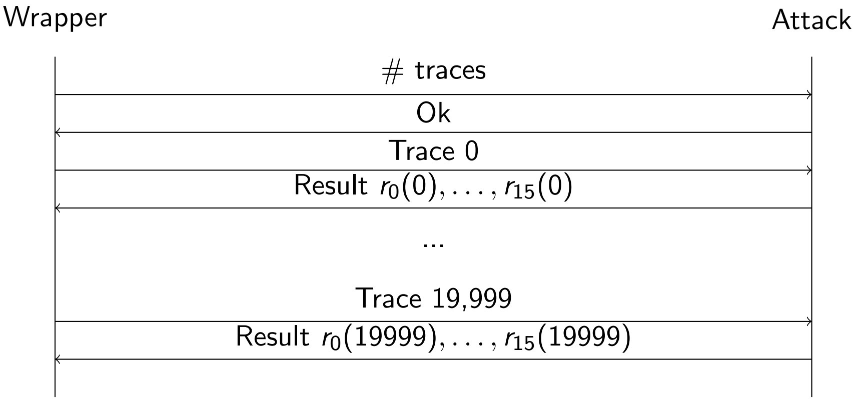
Specificity of this second edition

- Evaluation using several metrics (based on *A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks*, F.-X. Standaert and T. G. Malkin and M. Yung, Eurocrypt 2009, Lecture Notes in Computer Science, vol 5479, pp 443–461, Cologne, Germany, April 2009)
  - **Global Success Rate**
  - **Partial Success Rate**
  - **Partial Guessing Entropy**
- Three sets of traces
  - **Training** database: 1,000,000 traces (random keys and plaintexts)
  - **Public** database: 32 × 20,000 traces (32 random keys and for each key, 20,000 random plaintexts)
  - **Private** database: 32 × 20,000 traces
- All the traces were acquired under the same conditions

Acquisition setup



Evaluation protocol



Wrapper

Attack

# traces

Ok

Trace 0

Result $r_0(0), \ldots, r_{15}(0)$

...

Trace 19,999

Result $r_0(19999), \ldots, r_{15}(19999)$

Definition of attack metrics

- On iteration i, the attack receives the trace i and produces the result $r_0(i), \ldots, r_{15}(i)$ where $r_s(i)$ is a vector containing the 256 possible values of the byte s of the selected subkey rated according to their likelihood
- Results are averaged over the 32 campaigns (32 keys in the private database), but we will employ notations borrowed from the statistics
- If we denote by $r_s^c(t)$ the result $r_s(t)$ obtained for campaign $c \in [0, 32[$, then the notation $\mathrm{P}(r_s^c(t) = x^c)$ stands for the empirical estimation $\frac{1}{32}\sum_{c=0}^{31} \delta(r_s^c(t) = x^c)$
- We also note that the expectation $\mathrm{E}(X)$ of a random variable X is defined as: $\mathrm{E}(X) = \sum_x x \cdot \mathrm{P}(X = x)$
- In the sequel, we therefore forget the index of the campaign c and abridge the notation of $r_s^c(t)$ as $r_s(t)$, considered a random variable

Definition of attack metrics

GSR $> 80\%$	$\text{argmin}_t \, \text{P}(\forall s, r_s(t)[\dot{k}_s] = 0) > 0.80$
Min PSR $> 80\%$	$\text{argmin}_t \, \min_s \text{P}(r_s(t)[\dot{k}_s] = 0) > 0.80$
Max PGE < 10	$\text{argmin}_t \, \max_s \text{E}(r_s(t)[\dot{k}_s]) < 10$
GSR stable $> 80\%$	$\text{argmin}_t \, \forall t' \geq t, \text{P}(\forall s, r_s(t')[\dot{k}_s] = 0) > 0.80$
Min PSR stable $> 80\%$	$\text{argmin}_t \, \forall t' \geq t, \min_s \text{P}(r_s(t')[\dot{k}_s] = 0) > 0.80$
Max PGE stable < 10	$\text{argmin}_t \, \forall t' \geq t, \max_s \text{E}(r_s(t')[\dot{k}_s]) < 10$
GSR @20k	$\text{P}(\forall s, r_s(20\,000 - 1)[\dot{k}_s] = 0)$
Min PSR @20k	$\min_s \text{P}(r_s(20\,000 - 1)[\dot{k}_s] = 0)$
Max PSR @20k	$\max_s \text{P}(r_s(20\,000 - 1)[\dot{k}_s] = 0)$
Min PGE @20k	$\min_s \text{E}(r_s(20\,000 - 1)[\dot{k}_s])$
Max PGE @20k	$\max_s \text{E}(r_s(20\,000 - 1)[\dot{k}_s])$

How the attacks were evaluated?

- Each attack is evaluated against the 20.000 traces of each 32 keys of the private database (640.000 traces)
- We only have Linux computers so we have converted the attacks if they were developed for Windows
  - C/C++: simple compilation from sources
  - C#: use of Mono (open source .NET implementation)
  - Matlab: compilation using `mcc` (also used to avoid license token problems)
- $\sim$ 2 years of CPU time
- Execution in parallel on up to 16 Linux computers

Presentation Outline

1. Introduction
2. Results
3. Overview of the attacks
4. Conclusion

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 Télécom ParisTech	1 attack
Reference attack	Télécom ParisTech, France	1 attack
Olivier MEYNARD	Télécom ParisTech, France	5 attacks
Shiqian WANG	MORPHO, France	1 attack
Maël BERTHIER & Yves BOCKTAELS	MORPHO, France	4 attacks
Victor LOMNÉ	ANSSI, France	1 attack
Aziz EL AABID	Télécom ParisTech, France	1 attack

Attacks statistics — First submission period

- 20 attacks submitted
  - 17 evaluated
  - 1 segmentation fault
  - 1 does not respect the protocol (and too difficult to adapt)
  - 1 takes too long time to evaluate
- Languages
  - 11 C or C++
  - 5 Matlab
  - 4 C#
- Execution time
  - Min: < 0.01 s/trace
  - Max: 8.77 s/trace
  - Mean: 1.38 s/trace

Attacks statistics — Second submission period

- 12 attacks submitted
    - 12 evaluated
- Languages
    - 7 C or C++
    - 5 Matlab
- Execution time
    - Min: < 0.01 s/trace
    - Max: 8.59 s/trace
    - Mean: 2.35 s/trace

Results — GSR stable > 80 %

First submission period

1. Matthieu WALLE (Thales Communications), attack 7T: **7.061** (+ his 3 other attacks)
2. Maël BERTHIER (MORPHO), attack CPA: **15.943**
3. Alexis BONNECAZE (IML, ERISCS), attack SPE: **18.458**

First & second submission period

1. Matthieu WALLE (Thales Communications), attack 7T: **7.061** (+ his 3 other attacks)
2. Victor LOMNÉ (ANSSI), attack Recursive CPA: **10.666**
3. Maël BERTHIER & Yves BOCKTAELS (MORPHO), attack CPA AP SBOX PRD2: **10.796**

Results — Min PSR stable > 80 %

First submission period

1. Matthieu WALLE (Thales Communications), attack 9T: **5.890** (+ his 3 other attacks)
2. Alexis BONNECAZE (IML, ERISCS), attack SPE: **12.318**
3. Antoine WURCKER (UNILIM), attack A: **12.631**

First & second submission period

1. Matthieu WALLE (Thales Communications), attack 9T: **5.890** (+ his 3 other attacks)
2. Maël BERTHIER & Yves BOCKTAELS (MORPHO), attack CPA AP SBOX PRD2: **7.510** (+ 1 of their other attacks)
3. Olivier MEYNARD (Télécom ParisTech), attack A5: **8.835**

Results — Max PGE stable < 10

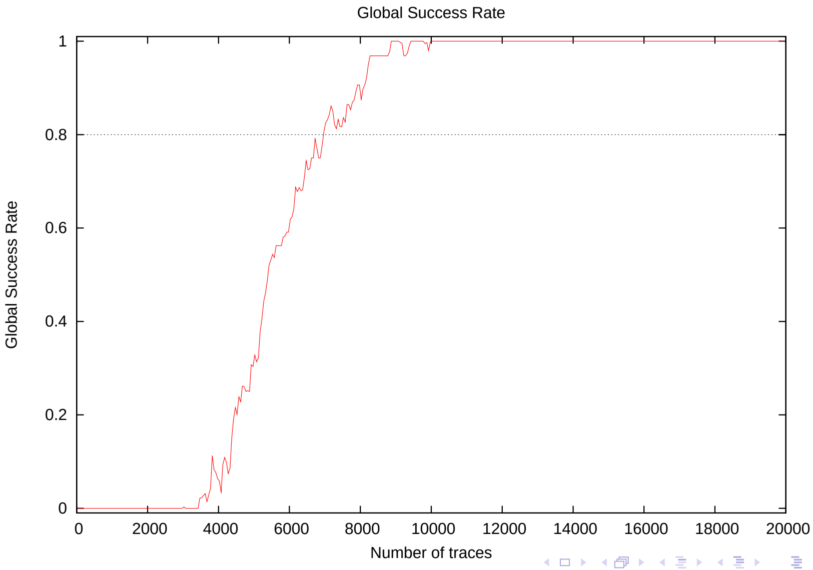
First submission period

1. Matthieu WALLE (Thales Communications), attack 7T: **3.388** (+ his 3 other attacks)
2. Antoine WURCKER (UNILIM), attack A: **4.192** (+ his other attack)
3. Maël BERTHIER (MORPHO), attack CPA: **4.706**

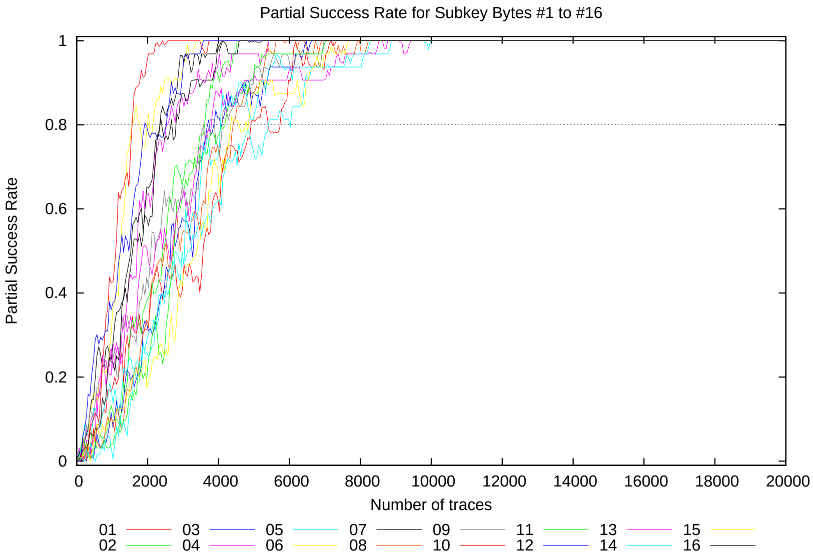
First & second submission period

1. Maël BERTHIER & Yves BOCKTAELS (MORPHO), attack CPA AP SBOX: **2.767** (+ 1 of their other attacks)
2. Matthieu WALLE (Thales Communications), attack 7T: **3.388** (+ his 3 other attacks)
3. Antoine WURCKER (UNILIM), attack A: **4.192** (+ his other attack)

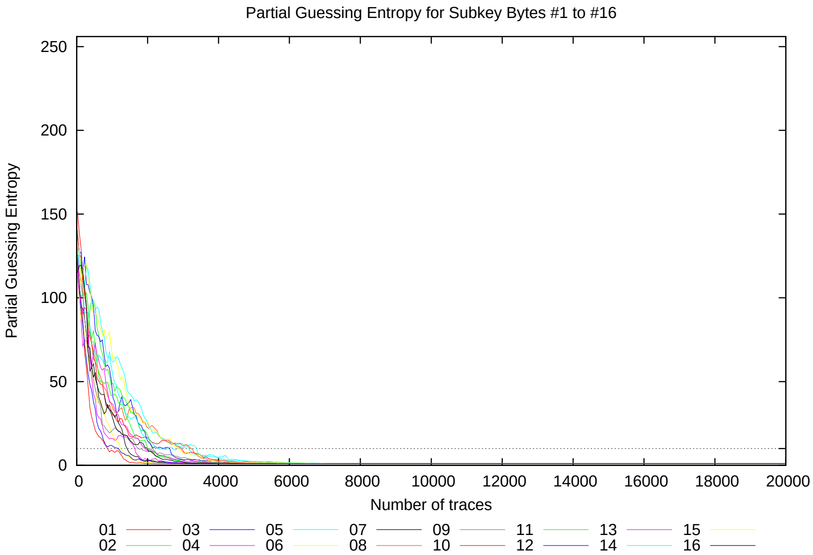
Walle (Thales) — Global success rate (attack 7T)



Walle (Thales) — Partial success rate (attack 7T)



Walle (Thales) — Partial guessing entropy (attack 7T)



Presentation Outline

1. Introduction
2. Results
3. Overview of the attacks
4. Conclusion

Overview of the attacks

- Descriptions of the attacks in this section were provided by the participants

Matthieu Walle (Thales)

- **Matthieu WALLE (Thales, France)**
- Min trace GSR $>$ 80 %: 6,704 (stable: 7,061)
- Min trace Min PSR $>$ 80 %: 5,408 (stable: 6,028)
- Min trace Max PGE $<$ 10: 3,388 (stable: 3,388)
- GSR at trace 20000: 1.00
- PSR at trace 20000: 1.00
- PGE at trace 20000: 1.00
- 0.03 s/trace
- Written in C/C++

Matthieu Walle (Thales)

- Last round / Known ciphertext
- Distinguisher : Correlation coefficient estimation
- Observation Preprocessing
  - Normalization and empirical treatments
  - Integral of the signal of the interesting time span (when the device is leaking information about the sensitive variable)
- Leakage model : Switching distance updated on the fly
  - Up to 8 sub-key bytes injected in the model
  - The traces are re-used for each update

Fast Correlation in the Frequency Domain

- **Edgar MATEOS (University of Waterloo, Canada)**
- Min trace GSR $> 80\,\%$: F
- Min trace Min PSR $> 80\,\%$: F
- Min trace Max PGE < 10: 5,994
- GSR at trace 20,000: 0.59
- PSR at trace 20,000: Min $= 0.78$, Max $= 1$
- PGE at trace 20,000: Min $= 1$, Max $= 3.41$
- Extremely fast (< 0.01 s/trace)
- Written in Matlab (so yes, attacks can be fast even if written in Matlab)

Fast Correlation in the Frequency Domain

- Designed to return faster results than correlation analysis in the time domain
- Immune to small misalignments or delays
- Requires less traces than the time domain analysis
- Exploits the fact that few frequencies are more likely to leak computing information
- Uses the Pearson correlation to measure the relationship between the hypothetical power consumption from the algorithm attacked in a given point and the spectral magnitude of the signals acquired
- Uses the FFT to speed up the attack because
  - FFT requires $N \log_2(N)$ operations when N is a power of 2
  - FFT transformation is symmetrical (it's possible to analyze only one-half of the frequencies returned by the algorithm)
- Results obtained over different platforms show that analyzing a reduced range of frequencies usually is enough to recover the cryptographic keys

Recursive CPA

- **Victor LOMNÉ (ANSSI, France)**
- Min trace GSR $> 80\,\%$: 10,666 (stable: 10,666)
- Min trace Min PSR $> 80\,\%$: 9,492 (stable: 9,492)
- Min trace Max PGE < 10: 4,840 (stable: 6,053)
- GSR at trace 20,000: 0.97
- PSR at trace 20,000: Min $= 0.97$, Max $= 1.00$
- PGE at trace 20,000: Min $= 1.00$, Max $= 1.09$
- 0.13 s/trace
- Written in C/C++

Recursive CPA — Principles

- Mix between the BS-CPA (Build-in Determined Sub-key Correlation Power Analysis), and a brute-force attack on the best candidates of several sub-keys
- Tries to exploit the parallelism of hardware implementations of block ciphers, and to improve the classical *divide-and-conquer* strategy used in the classical DPA algorithm
- Parameters
  - a stability threshold for the BS-CPA part (1000)
  - a number of sub-key indexes to test and the number of best candidates to test, for the brute-force part, here: 3 sub-key indexes to test, and for each one test the 16 best candidates (trade-off between the number of keys tested and the computational time).

Recursive CPA — Main iteration I

- Each sub-key is attacked independently using a classical CPA attack on the last round of the AES (Hamming Distance between one byte of ciphertext and the corresponding byte of the state at the begining of the last round)
- For each sub-key, its stability is incremented if the candidate guessed with $(i-1)$ traces is the same than the one guessed with i traces, else, its stability is reset at 0
- For the 3 sub-key indexes the harder to attack (those having the smallest stability), one tests for each one the 16 best candidates (according to the current correlation value computed in the CPA for each candidate). That means that one computes, from the round key hypothesis, the corresponding master key, and tests it with a couple of plaintext/ciphertext. If the master key is the correct one, the attack succeeds

Recursive CPA — Main iteration II

- For a sub-key, if its stability is equal to 1000, then this sub-key is considered as cracked. Then one starts again the CPA attack for the other sub-keys, using the traces already used, but taking into account in the computation of the correlation also the value of the sub-key which is considered as cracked. Thus one increases the partial correlation between the attacked sensible value and the leakage

A. Wrucker — Attack A

- **Antoine Wrucker (Université de Limoges, France)**
- Min trace GSR $> 80\,\%$: 13,474 (stable: 19,858)
- Min trace Min PSR $> 80\,\%$: 11,501 (stable: 12,631)
- Min trace Max PGE < 10: 4,179 (stable: 4,192)
- GSR at trace 20,000: 0.81
- PSR at trace 20,000: Min $= 0.88$, Max $= 1.00$
- PGE at trace 20,000: Min $= 1.00$, Max $= 1.16$
- 0.25 s/trace
- Written in C/C++

A. Wrucker — Attack B

- **Antoine Wrucker (Université de Limoges, France)**
- Min trace GSR $> 80\,\%$: F
- Min trace Min PSR $> 80\,\%$: 11,525 (stable: 12,866)
- Min trace Max PGE < 10: 4,179 (stable: 4,192)
- GSR at trace 20,000: 0.69
- PSR at trace 20,000: Min $= 0.88$, Max $= 1.00$
- PGE at trace 20,000: Min $= 1.00$, Max $= 1.16$
- 0.25 s/trace
- Written in C/C++

A. Wrucker — Attack A

- Classical correlation power analysis at round 10
- Improved the signal to noise ratio between the relevant correlation peak and its challenging ones
  - Limit the search for the correlation peak to a small portion of the signal which includes the last round
  - Filter the correlation curve by means of mobile average before capturing the maximum height
- Includes a particular treatment for byte number 13 of K10
  - In an early caracterisation phase of the leakage produced by this AES, we noticed that some particular bit curiously behaves quite differently than other ones
  - Indeed bit number 141 of the end of the ninth round happens to be fairly correlated to power consumptions
  - We chose to take advantage of this observation and recovered the value of byte 13 of K10 as the one showing the best correlation between this bit and the power curves

A. Wrucker — Attack B

- Another particular behaviour of bit 14 also occurs at the begining of the AES
  - Denoting m_{14}, c_{14} and k_{14} bits 14 of the plaintext, the ciphertext and the key respectively, we observed that power curves are strongly correlated with $m_{14} - c_{14}$ when $k_{14} = 0$, and with $-(m_{14} + c_{14})$ when $k_{14} = 1$
- Attack B just differs from attack A by taking advantage of that opportunity to identify bit 14 of K
- Should a solution for K10 issued by attack A be not consistent with the recovered value of k_{14}, it is considered incorrect and is slightly modified to conform to that key bit.

Presentation Outline

1 Introduction

2 Results

3 Overview of the attacks

4 Conclusion

Opinion poll

- Opened in May 2010
- Lots of useless answers (automatic spam and SQL injection attempts)
- 11 real answers
- Operating system
    - Linux: 5
    - Windows: 5
    - Mac OS X: 1
- Programming Language
    - C/C++: 7
    - Matlab: 3
    - Ruby: 1
- Good point
    - Interest of the contest

Opinion poll

- Topics that can be improved
  - Easiness of participation
  - Quality of the evaluation report
- Free comments
  - Metrics used to evaluate attacks is a subject of discussion
  - Website could be improved
  - The storage and distribution of traces (lots of small text files distributed in a large archive) could be improved (*and they will be improved in v4!*)
  - Need to clarify the links between the organizer (Télécom ParisTech) and commercial companies (SecureIC)

Acknowledgments

- Philippe Bulens [2]
- Jean-Luc Danger [1]
- Aziz Elaabid [1]
- Florent Flament [1]
- Sylvain Guilley [1]
- Naofumi Homma [1,3]
- Philippe Hoogvorst [1]
- Olivier Meynard [1,4]
- Frédéric Pauget (and all the IT staff) [1]
- Akashi Satoh [5]
- Laurent Sauvage [1]
- François-Xavier Standaert [2]
- Nicolas Veyrat-Charvillon [2]

[1] Télécom ParisTech
[2] Université catholique de Louvain
[3] Tohoku University
[4] DGA-MI (formerly CELAR)
[5] National Institute of Advanced Industrial Science and Technology

What's next?

3rd edition

- Acquisition contest
- Organized with AIST
- Launched today!

4th edition

- Attack contest
- Organized by Télécom ParisTech
- Attack against protected hardware or software implementation of AES
- Will be launched later in 2011 (Q3 or 4)

Thank you!

- Thank you for your attention
- Questions?