Links between successful SPA, DPA and DEMA on DES and the crypto-processor architecture
— Presentation at Crypto’Puces 2007 —

Sylvain GUILLEY, <sylvain.guilley@enst.fr>

Renaud PACALET, Philippe HOOGVORST, Jean-Luc DANGER, Sumanta CHAUDHURI & Florent FLAMENT

GET / Télécom Paris
CNRS – LTCI (UMR 5141)

Tuesday April 17th 2007.
Porquerolles.
1 Academic platform for embedded systems security evaluation
   - The platform
   - The SecMat DPA-Proof Cryptographic ASIC
   - The acquisitions

2 Attacks on unprotected DES implementation
   - SPA: Simple Power Analysis
   - Circuits reverse-engineering
   - Power model calibration
   - Information extraction
   - Decide: vectorial Boolean functions theory

3 Perspectives
   - Lessons learnt from power analyses and attacks
   - Future targets
   - Acknowledgements
Presentation Outline

1. Academic platform for embedded systems security evaluation
   - The platform
   - The SecMat DPA-Proof Cryptographic ASIC
   - The acquisitions

2. Attacks on unprotected DES implementation
   - SPA: Simple Power Analysis
   - Circuits reverse-engineering
   - Power model calibration
   - Information extraction
   - Decide: vectorial Boolean functions theory

3. Perspectives
   - Lessons learnt from power analyses and attacks
   - Future targets
   - Acknowledgements
Why academic platforms for security evaluation?

**Purpose**
- **Scientific** study of attacks on known implementations
- **Independent** evaluations

**Position in the security landscape**
- Not in conflict with CESTIs, because we cannot certificate products
- Not in conflict with industrials, because the studied counter-measures are more fundamental than pre-competitive
Why academic platforms for security evaluation?

Purpose

- **Scientific** study of attacks on known implementations
- **Independent** evaluations

Position in the security landscape

- Not in conflict with CESTIs, because we cannot *certificate* products
- Not in conflict with industrials, because the studied counter-measures are more *fundamental* than *pre-competitive*
Why academic platforms for security evaluation?

**Purpose**
- **Scientific** study of attacks on known implementations
- **Independent** evaluations

**Position in the security landscape**
- Not in conflict with CESTIs, because we cannot **certificate** products
- Not in conflict with industrials, because the studied counter-measures are more **fundamental** than **pre-competitive**
Why academic platforms for security evaluation?

Purpose
- **Scientific** study of attacks on known implementations
- **Independent** evaluations

Position in the security landscape
- Not in conflict with CESTIs, because we cannot **certificate** products
- Not in conflict with industrials, because the studied counter-measures are more **fundamental** than pre-competitive
Academic platform for embedded systems security evaluation

Attacks on unprotected DES implementation

Perspectives

The platform
The SecMat DPA-Proof Cryptographic ASIC
The acquisitions

Acquisition apparatus

Monitoring PC

Power supplies

Targeted ASIC

Sylvain GUILLEY
Successful SPA, DPA and DEMA on DES — 8
Traces Acquisition Setup – even from the internet

ASIC (SecMatV1) | PC (dpa_campaign.xpp) | Oscilloscope (Agilent 54855A)

- USB
- RS232
- GPIB
- Parallel Output (trigger $f$)

Monitor
Inhibit watchdog

PC:
- parse_command_line()
- initialize()
- $n++$
- set $n = 0$
- set_key()
- set_msg()
- trig_scope()
- start()
- acquire_data()
- stop()
- transfer_to_HDD()

- if $n = n_{max}$

Oscilloscope:
- Idle
- Load the setup (channels, calibers, etc.)
- Prepare for the acquisition task
- Sample the power; average if requested
- Save a new trace

Sylvain GUILLEY
Successful SPA, DPA and DEMA on DES — 9
Traces Acquisition Setup – *extensible SW design*

- **cmdline**
  - `+attackeeName: string`
  - `+attackerName: string`
  - `+// etc. Refer to the class itself`
  - `-parseMain(size_t, char* const*): void`

- **cmdline_singleton**
  - `-new_singleton(size_t, char* const*): void`
  - `-delete_singleton(): void`
  - `+get_cmdline(): cmdline const&`

- **attackee**
  - `+trace_filename(): string`
  - `+log(): string`
  - `+check_assertion(): void`
  - `+start(): void`
  - `+stop(): void`
  - `+update_params(): void`

- **acquisition**
  - `+launch(): void`

  - **the_attack**

- **attacker**
  - `+trig_scope(): void`
  - `+acquire_data(): void`
  - `+save_data(string): void`

Concrete implementations are based upon:
- `attackee_crypto`
- `attackee_rta`
- etc.

Implement the acquisition loops, that confront the attackee with the attacker

Concrete implementations:
- `gpiB_device_54850_3`
- `gpiB_device_54850_3_4`
- etc.
More to be said about “faults” in Christophe Clavier’s next presentation!
Academic platform for embedded systems security evaluation
Attacks on unprotected DES implementation
Perspectives

The platform
The SecMat DPA-Proof Cryptographic ASIC
The acquisitions

**Modules Architecture**

Every module communicates via a shared local RAM.

**SecMat ASIC Architecture**

Modules are connected to a bus, and are able to send interrupts to the CPU.

---

Sylvain GUILLEY

Successful SPA, DPA and DEMA on DES — 12
The platform
The SecMat DPA-Proof Cryptographic ASIC.
Perspectives
The acquisitions

SecMat V1 Layout

Characteristics
- **Process:** STMicroelectronics HCMOS9GP 130 nm technology.
- **Area:** 4 mm\(^2\) for about 2 million transistors.
- **Power domains:** 1 @ 3.3 V (pads), 4 @ 1.2 V (core.)
- **Standard cells:** CORE9GPLL 4.1 “Low Leakage” library.
- **Pads:** IOLIB\_65\_M6\_LL and IOLIB\_65\_3V3\_M6\_LL\_65A 6.0.
- **Memories:** ugnLib RAM/ROM UniCAD generator.
- **Development methodology:** SystemC and VHDL co-design for some blocks.
- **Validation strategy:** Simulation of the entire SoC in a mixed RTL/Netlist description, using ModelSim controlled externally via a FLI.

Sylvain GUILLEY
Successful SPA, DPA and DEMA on DES — 13
Academic platform for embedded systems security evaluation
Attacks on unprotected DES implementation
Perspectives

The platform
The SecMat DPA-Proof Cryptographic ASIC
The acquisitions

Power supplies
Control via USB

Attacked ASIC

66 MHz clock
DPA probe
Academic platform for embedded systems security evaluation
Attacks on unprotected DES implementation
Perspectives

The platform
The SecMat DPA-Proof Cryptographic ASIC
The acquisitions

Sylvain GUILLEY
Successful SPA, DPA and DEMA on DES — 15
Power trace of a smartcard (ATMEL ATMega)
Power trace of a 6502 (8-bit CISC) microcontroller
Academic platform for embedded systems security evaluation
Attacks on unprotected DES implementation
Perspectives

The platform
The SecMat DPA-Proof Cryptographic ASIC
The acquisitions

Sylvain GUILLEY
Successful SPA, DPA and DEMA on DES — 18
Tampering with the power supplies of SecMat

\[ R = 0 \ \Omega, \ V \text{ varies}, \ U = 1.2 \ \text{V}. \]

\[ R \text{ varies}, \ V = 1.2 \ \text{V}, \ U = 1.2 \ \text{V}. \]

Percentage of correct encryptions

Sylvain GUILLEY
Successful SPA, DPA and DEMA on DES — 18
Presentation Outline

1. Academic platform for embedded systems security evaluation
   - The platform
   - The SecMat DPA-Proof Cryptographic ASIC
   - The acquisitions

2. Attacks on unprotected DES implementation
   - SPA: Simple Power Analysis
   - Circuits reverse-engineering
   - Power model calibration
   - Information extraction
   - Decide: vectorial Boolean functions theory

3. Perspectives
   - Lessons learnt from power analyses and attacks
   - Future targets
   - Acknowledgements
Attack steps:

1. Localize in time the cryptographic operation (SPA)
2. Reverse-engineer the architecture (ad hoc CPA)
3. Calibrate the correlations (information extraction)
4. Exhaustive attack (DPA in HW/HD, template)
5. Decide (Boolean functions)
Attack steps:

1. Localize in time the cryptographic operation (SPA)
2. Reverse-engineer the architecture (ad hoc CPA)
3. Calibrate the correlations (information extraction)
4. Exhaustive attack (DPA in HW/HD, template)
5. Decide (Boolean functions)
Attack steps:

1. Localize in time the cryptographic operation (SPA)
2. Reverse-engineer the architecture (ad hoc CPA)
3. Calibrate the correlations (information extraction)
4. Exhaustive attack (DPA in HW/HD, template)
5. Decide (Boolean functions)
Attack steps:

1. Localize in time the cryptographic operation (SPA)
2. Reverse-engineer the architecture (ad hoc CPA)
3. Calibrate the correlations (information extraction)
4. Exhaustive attack (DPA in HW/HD, template)
5. Decide (Boolean functions)
Attack steps:

1. Localize in time the cryptographic operation (SPA)
2. Reverse-engineer the architecture (ad hoc CPA)
3. Calibrate the correlations (information extraction)
4. Exhaustive attack (DPA in HW/HD, template)
5. Decide (Boolean functions)
Power trace of DES @ 66 MHz (k=0000^4, m=00^8)
Power trace of DES @ 66 MHz (k=00ff^4, m=00^8)
Difference of the two previous power traces of DES
CMOS circuits dissipation model

\[
\text{Power} = \sum_{i \in \text{nets}} \xi_i \bar{i}(t - 1) \cdot i(t) + \xi_i i(t - 1) \cdot \bar{i}(t)
\]

Model (in)validity?

- No static power leakage
  - term \(\propto i(t)\).
- No correlation over more than two clock periods
  - term \(\propto i(t - 2) \cdot i(t)\).
- No correlation between nets
  - term \(\propto i(t) \cdot j(t)\), with \(i \neq j\).
Extraction of the Activity of a Single Net

Sane hypotheses

- **Liveness:**
  \[ \mathbb{E}\{i(t)\} = \frac{1}{2}, \]

- **Fast decorrelation (permutation):**
  \[ \mathbb{E}\{i(t) \cdot j(t)\} = \mathbb{E}\{i(t)\} \cdot \mathbb{E}\{j(t)\}, \]

- **Fast decorrelation (substitution):**
  \[ \mathbb{E}\{i(t-1) \cdot i(t)\} = \mathbb{E}\{i(t-1)\} \cdot \mathbb{E}\{i(t)\}. \]

Information Extraction for Target Net \( j \)

\[
\mathbb{E}\left\{ \sum_{i \in \text{nets}} \xi_i^\uparrow i(t-1) \cdot i(t) + \xi_i^\downarrow i(t-1) \cdot \bar{i}(t) \right\} \\
\times \left\{ -4 \times \bar{j}(t-1) \cdot (-1)^{j(t)} \right\} \\
= \xi_j^\uparrow.
\]

But how to choose \( j \)?
Academic platform for embedded systems security evaluation
Attacks on unprotected DES implementation
Perspectives

SPA: Simple Power Analysis
Circuits reverse-engineering
Power model calibration
Information extraction
Decide: vectorial Boolean functions theory

DES Architecture under Attack (Integration’07)

Domains:
- 8 bit
- 48 bit
- 2 x 28 bit
- 2 x 32 bit
- 8 x 8 bit

Sylvain GUILLEY
Successful SPA, DPA and DEMA on DES — 31
DES Architecture under Attack (Integration’07)

Selection

Domains:
- 8 bit
- 48 bit
- 2 x 28 bit
- 2 x 32 bit
- 8 x 8 bit

Sylvain GUILLEY

Successful SPA, DPA and DEMA on DES — 32
Datapath of DES involved in the DPA of the 1\textsuperscript{st} round

\begin{figure}
\centering
\includegraphics[width=\textwidth]{datapath_des.png}
\end{figure}

\begin{table}
\centering
\begin{tabular}{|c|c|c|c|c|}
\hline
Sbox & R\textsubscript{0} & E & S & P \\
\hline
\#1 & \{32, 1, 2, 3, 4, 5\} & \{1, 2, 3, 4, 5, 6\} & \{1, 2, 3, 4\} & \{9, 17, 23, 31\} \\
\#2 & \{4, 5, 6, 7, 8, 9\} & \{7, 8, 10, 11, 12, 13\} & \{5, 6, 7, 8\} & \{13, 28, 2, 18\} \\
\#3 & \{8, 9, 10, 11, 12, 13\} & \{13, 14, 15, 16, 17, 18\} & \{9, 10, 11, 12\} & \{24, 16, 30, 6\} \\
\#4 & \{12, 13, 14, 15, 16, 17\} & \{19, 20, 21, 22, 23, 24\} & \{13, 14, 15, 16\} & \{26, 20, 10, 1\} \\
\#5 & \{16, 17, 18, 19, 20, 21\} & \{25, 26, 27, 28, 29, 30\} & \{17, 18, 19, 20\} & \{8, 14, 25, 3\} \\
\#6 & \{20, 21, 22, 23, 24, 25\} & \{31, 32, 33, 34, 35, 36\} & \{21, 22, 23, 24\} & \{4, 29, 11, 19\} \\
\#7 & \{24, 25, 26, 27, 28, 29\} & \{37, 38, 39, 40, 41, 42\} & \{25, 26, 27, 28\} & \{32, 12, 22, 7\} \\
\#8 & \{28, 29, 30, 31, 32, 1\} & \{43, 44, 45, 46, 47, 48\} & \{29, 30, 31, 32\} & \{5, 27, 15, 21\} \\
\hline
\end{tabular}
\end{table}
The layout of DES is far more messy than the algorithm...

...nonetheless, information can indeed be extracted surgically! (see next slides)
The layout of DES is far more messy than the algorithm... 

... nonetheless, information can indeed be extracted surgically! (see next slides)
Signature of message loading/unloading in IF
(reminder: IF is the InterFace register)

Hamming distance 1 for IF register loading/unloading the message

Differential wave [mV] vs. Time [clock cycles]
Signature of key loading / unloading in IF, plus the CD activity

Hamming distance 1 for IF register loading/unloading the key

Differential wave [mV]

Time [clock cycles]

Sylvain GUILLEY

Successful SPA, DPA and DEMA on DES — 37
Signature of distance-2 key loading/unloading in IF and of \(LS^2\) in CD

![Graph showing Hamming distance 2 for IF register loading/unloading the key with different trigger types: combinatorially-triggered, sequentially-triggered, and sel_not_shift, sel_one_not_two labels.](image)
Attacks on unprotected DES implementation

Perspectives

SPA: Simple Power Analysis
Circuits reverse-engineering
Power model calibration
Information extraction
Decide: vectorial Boolean functions theory

Voltage [mV] vs. Time [ns]


E

S

\[ \cdots 1 \ 2 \ 3 \ 4 \ \cdots \]

\[ \cdots \text{sbox \#1} \ \cdots \]

Sylvain GUILLEY

Successful SPA, CPA and DEMA on DES — 39
From Extraction to Hypotheses Testing

Which target net $j$?
- in the **first** round of cipher or
- in the **last** round,

... because the dependance in the key is limited to 6 or 8 bits!

Relevance of the attack
- if $j$ is tested, the correlation yields a **non-zero value**, say $\xi_j^\uparrow$,
- otherwise, the correlation is **null**, because the $j' \not\in$ nets.

... at least **in principle**.
Attacks on Crypto-processors Power Supply Signatures

Insulation by correlation of three rounds out of sixteen in the DES algorithm

Realization of the “Differential Power Analysis” (aka DPA) on the first round of DES

Sylvain GUILLEY
Hamming weight versus Hamming distance

- **Hamming weight**: selection irrespective of the initial state
- **Hamming distance**: selection matches the dissipation

It is easy to compute the average signal got by an attacker:

- **Hamming weight**: 
  \[ \mathbb{E} \left\{ \sum_{i \in \text{nets}} \xi_i^\uparrow i(t) \cdot i(t+1) + \xi_i^\downarrow i(t) \cdot \bar{i}(t+1) \right\} \times (-1)^{j(t+1)} \]
  \[= \frac{1}{2} \cdot (\xi_j^\uparrow - \xi_j^\downarrow) ,\]

- **Hamming distance**: 
  \[ \mathbb{E} \left\{ \sum_{i \in \text{nets}} \xi_i^\uparrow i(t) \cdot i(t+1) + \xi_i^\downarrow i(t) \cdot \bar{i}(t+1) \right\} \times (-1)^{j(t) \oplus j(t+1)} \]
  \[= \frac{1}{2} \cdot (\xi_j^\uparrow + \xi_j^\downarrow) .\]
Difference between $\xi_j^{\uparrow} - \xi_j^{\downarrow}$ and $\xi_j^{\uparrow} + \xi_j^{\downarrow}$

Voltage [mV] vs. Time [clock cycles] for transfers in the register R and L.

- 'Rising edge' selection function
- 'Falling edge' selection function

Maximum for R: 1.65 mV
Maximum for L: 1.39 mV
Hamming weight differential trace

1 correct guess (red) / 63 bad guesses (green)
Exploitation of XOR dissymmetry: a is Sbox output, b is L.

Input $a = '0'$ is steady

$$a = '0' \quad \text{or} \quad b \quad \text{or} \quad z$$

<table>
<thead>
<tr>
<th>Input $b$ has a ↑ edge at $t = 0$</th>
<th>Input $b$ has a ↓ edge at $t = 0$</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total energy: 7.72 pJ</strong></td>
<td><strong>Total energy: 11.21 pJ</strong></td>
</tr>
</tbody>
</table>

---

Sylvain GUILLEY

Successful SPA, DPA and DEMA on DES — 45
Hamming distance differential trace

1 correct guess (red) / 63 bad guesses (green)
For $i \in [1, 14]$,

\[
\begin{align*}
LR_{i-1} \oplus LR_i &= (L_{i-1} \oplus L_i) \parallel (R_{i-1} \oplus R_i) \\
LR_i \oplus LR_{i+1} &= (R_{i-1} \oplus R_i) \parallel (L_{i+1} \oplus L_{i+2}) \quad // \text{See the note} \\
LR_{i+1} \oplus LR_{i+2} &= (L_{i+1} \oplus L_{i+2}) \parallel (R_{i+1} \oplus R_{i+2}).
\end{align*}
\]

Note: The left half of $LR_i \oplus LR_{i+1}$ is equal to $R_{i-1} \oplus R_i$ because $L_i = R_{i-1}$ and $L_{i+1} = R_i$. Identically, the right half of $LR_i \oplus LR_{i+1}$ is equal to $L_{i+1} \oplus L_{i+2}$ because $R_i = L_{i+1}$ and $R_{i+1} = L_{i+2}$.
DPA signal amplitude and ghost peaks for some Sboxes

Academic platform for embedded systems security evaluation
Attacks on unprotected DES implementation
Perspectives

SPA: Simple Power Analysis
Circuits reverse-engineering
Power model calibration
Information extraction
Decode: vectorial Boolean functions theory

Sylvain GUILLEY
Successful SPA, DPA and DEMA on DES — 48
Model Description

CARDIS’04 Model: *ideal* and *scalar* dissipation

- **ideal**: one event always consumes the same amount of energy, irrespectively of the environmental conditions.
- **scalar**: the phenomenon is not represented as a waveform, but rather as an amplitude.

The model shows that:

- The DPA success does not depend on the key
- The correlation is not perfect: wrong guesses do match!
- The SNR of the attack depends only on the Sbox’s properties
- The attack is all the better as the Sbox is strong against known cryptanalyses
Model Description

CARDIS’04 Model: *ideal* and *scalar* dissipation

- **ideal**: one event always consumes the same amount of energy, irrespectively of the environmental conditions.

- **scalar**: the phenomenon is not represented as a waveform, but rather as an amplitude.

The model shows that:

- The DPA success does not depend on the key
- The correlation is not perfect: wrong guesses do match!
- The SNR of the attack depends only on the Sbox’s properties
- The attack is all the better as the Sbox is strong against known cryptanalyses
Model Description

CARDIS’04 Model: *ideal* and *scalar* dissipation

- **ideal**: one event always consumes the same amount of energy, irrespectively of the environmental conditions.
- **scalar**: the phenomenon is not represented as a waveform, but rather as an amplitude.

The model shows that:

- The DPA success does not depend on the key
- The correlation is not perfect: wrong guesses do match!
- The SNR of the attack depends only on the Sbox’s properties
- The attack is all the better as the Sbox is strong against known cryptanalyses
CARDIS’04 Model: *ideal* and *scalar* dissipation

- **ideal**: one event always consumes the same amount of energy, irrespectively of the environmental conditions.
- **scalar**: the phenomenon is not represented as a waveform, but rather as an amplitude.

The model shows that:

- The DPA success does not depend on the key
- The correlation is not perfect: wrong guesses do match!
- The SNR of the attack depends only on the Sbox’s properties
- The attack is all the better as the Sbox is strong against known cryptanalyses
Model Description

CARDIS’04 Model: *ideal* and *scalar* dissipation

- **ideal**: one event always consumes the same amount of energy, irrespectively of the environmental conditions.
- **scalar**: the phenomenon is not represented as a waveform, but rather as an amplitude.

The model shows that:

- The DPA success does not depend on the key
- The correlation is not perfect: wrong guesses do match!
- The SNR of the attack depends only on the Sbox’s properties
- The attack is all the better as the Sbox is strong against known cryptanalyses
Model Description

CARDIS’04 Model: *ideal* and *scalar* dissipation

- **ideal**: one event always consumes the same amount of energy, irrespectively of the environmental conditions.
- **scalar**: the phenomenon is not represented as a waveform, but rather as an amplitude.

The model shows that:

- The DPA success does not depend on the key
- The correlation is not perfect: wrong guesses do match!
- The SNR of the attack depends only on the Sbox’s properties
- The attack is all the better as the Sbox is strong against known cryptanalyses
Two bounds between *physical* and *logical* distinguishers:

\[
\text{SNR}(\text{DPA})(F) \geq \frac{2^{3p-2}}{q \Lambda_S^2} = O\left(\frac{1}{\Lambda_S^2}\right),
\]

\[
\text{SNR}(\text{DPA})(F) \geq \frac{2^p}{\Delta_S} = O\left(\frac{1}{\Delta_S}\right).
\]

**Figure 1:** Simplified DES cipher flow showing a single S-Box out of eight.

**Figure 2:** Schematic DPA setup on an SPN structure.
Validation of the Model: the SNR of the DPA depends neither on the attacked board nor on the acquisition conditions.

![Graph showing DPA on DES Sbox #1 (attack of the first round)](graph.png)

- Setup 1 / Correct key
- Setup 2 / \([V=U]\) Correct key
- Setup 2 / \([V=U/2]\) Correct key

Theoretical SNR (Asymptotic value)
Using all the energy, even that from ghost peaks

\[
\varepsilon = 0x00 \quad 0x01 \quad 0x02 \quad 0x03
\]

The attack will be all the more easy as the following metric is high:

\[
\min_{\varepsilon \neq 0} \sum_e \left( \text{tr} \sum_{b, b'} (-1)^{f_b \circ \tau_e} \cdot \left( (-1)^{f_{b'} \circ \tau_e} - (-1)^{f_{b'}} \right) \right)^2 . \quad (3)
\]

Demo presented on May 2nd at BFCA’07 (Paris)
Presentation Outline

1. Academic platform for embedded systems security evaluation
   - The platform
   - The SecMat DPA-Proof Cryptographic ASIC
   - The acquisitions

2. Attacks on unprotected DES implementation
   - SPA: Simple Power Analysis
   - Circuits reverse-engineering
   - Power model calibration
   - Information extraction
   - Decide: vectorial Boolean functions theory

3. Perspectives
   - Lessons learnt from power analyses and attacks
   - Future targets
   - Acknowledgements
Lessons learnt from power analyses and attacks

- Hamming weight model can work, because of glitches and dissymmetry of gates:
  - Remove glitches!
  - Balance the gates inputs too!
- Logical correlations might appear out of the blue:
  - Secure all the data- and key-path!
  - Use a static simulator to determine the percolation of information.
- Correlations over two clock cycles exist:
  - Remove all compromizing Z state!
- Cross-talk manifests:
  - Shield the routing!
- Attacks on averaged traces are practical:
  - A sound solution must be deterministic!
Home-made smart-card running customized SOSSE

- Trigger
- External power supply
- EEPROM
- Target CPU (ATMega)
- Test LEDs
- Smartcard contacts
- JTAG flash programmation
- Debug serial port
- Differential probe for voltage acquisition

Sylvain GUILLEY
Successful SPA, CPA and DEMA on DES — 60
SecMat prototype ASICs genealogy ...
Acknowledgements

- SEN  ... http://www.comelec.enst.fr/recherche/sen/
- LabSoC           http://labsoc.comelec.enst.fr/
- STM AST/SmartCard          http://www.st.com/
- CMP  ......................... http://cmp.imag.fr/
On-going works

- Template attacks ............................ Moulay EL AABID
- Secured FPGA CAD ............................ Ziming ZOU
- Asynchronous FPGA ......................... Sumantà CHAUDHURI
- Acquisition methodology .................... Laurent SAUVAGE
- Attacks ........................................ Ying ZHUANG
- DFA on AES ................................. Nidhal SELMANE
- Characterization of CPUs .................... Zhiguo SONG

GET / ENST has open positions!

- Permanent position
  http://www.get-telecom.fr/p_fr_recrut_offres_01ENST_881.html
- PhD, Post’docs, CDDs
  http://www.iacr.org/jobs/