DPA : Attaques et Contre-mesures

Shivam BHASIN, Taoufik CHOUTA, Guillaume DUC, Jean-Luc DANGER, Aziz EL AABID, Florent FLAMENT, Philippe HOOGVORST, Tarik GRABA, Sylvain GUILLEY, Houssem MAGHR’EBI, Olivier MEYNARD, Maxime NASSAR, Renaud PACALET, Laurent SAUVAGE, Nidhal SELMANE and Youssef SOUISSI.

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

GDR SoC-SiP
AMPHI SAPHIR, TELECOM ParisTech, PARIS.

S. Guilley, <sylvain.guilley@TELECOM-ParisTech.fr>
Presentation Outline

1. Context
2. Side-Channel Attacks
   - Side-Channels
   - Side-Channels Acquisitions
   - Attack Algorithms
3. Counter-Measures to SCAs
   - Protocol-Level
   - Register Transfer Level
   - Netlist Level
4. Attacks on Counter-Measures
   - Attack on Information Masking
   - Attack on Information Hiding
5. Conclusions and Perspectives
   - Conclusions
   - Perspectives
Presentation Outline

1. Context

2. Side-Channel Attacks
   - Side-Channels
   - Side-Channels Acquisitions
   - Attack Algorithms

3. Counter-Measures to SCAs
   - Protocol-Level
   - Register Transfer Level
   - Netlist Level

4. Attacks on Counter-Measures
   - Attack on Information Masking
   - Attack on Information Hiding

5. Conclusions and Perspectives
   - Conclusions
   - Perspectives
Adversary’s goal
- Secrets extraction.

Protection
- Conceal the secrets in a device (ASIC) ...
- ... or in the bitstream of an FPGA.

Representativity of the study
- Most problems come down to this...
- Example:
  - Fetching a data in an encrypted memory
  - ⇒ decrypt the memory,
  - ⇒ attack the CPU,
  - ⇒ use side-channel attacks = SCA (for instance).

S. Guilley, <sylvain.guilley@TELECOM-ParisTech.fr>
There are other applications of SCA

- SCARE: secret cryptography.
- Test (virtual oscilloscope).
- Subliminal channel for IPs watermarking.
Presentation Outline

1. Context
2. Side-Channel Attacks
   - Side-Channels
   - Side-Channels Acquisitions
   - Attack Algorithms
3. Counter-Measures to SCAs
   - Protocol-Level
   - Register Transfer Level
   - Netlist Level
4. Attacks on Counter-Measures
   - Attack on Information Masking
   - Attack on Information Hiding
5. Conclusions and Perspectives
   - Conclusions
   - Perspectives
Typical side-channels

- **Timing Attacks** [5].
- **Power Analysis Attacks** [6].
- **Electro-magnetic Attacks** [1].
Are SCAs intrusive?

**Side-Channel Attacks (SCA) versus Fault Injection Attacks (FIA)**

- SCA: passive
- FIA: active

**But what about the experimental setup?**

<table>
<thead>
<tr>
<th></th>
<th>Non-intrusive</th>
<th>Intrusive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deportable IC (smartcard)</td>
<td>Timing, power, EM</td>
<td>—</td>
</tr>
<tr>
<td>Soldered IC or BGA (FPGA)</td>
<td>Timing, EM</td>
<td>power</td>
</tr>
</tbody>
</table>

The know-how in measurements is capital.

→ The 3rd version (2010–2011) of the DPA contest ([http://www.dpacontest.org/](http://www.dpacontest.org/)) will have an acquisition competition, based on SASEBO GII.
ALTERA Excalibur evaluation board “customized for DPA”

Voltage regulator

Power pins of the FPGA unsoldered

Coaxial cable for the power acquisition

External 3.3V power supply

6.8 Ω resistor

Ground

External clock input

External 5.0 V power supply

External 1.8 V power supply

S. Guilley, < sylvain.guilley@TELECOM-ParisTech.fr >

OPA attacks & counter-measures
Parallax ALTERA Stratix board “customized for DPA” [3]
XCV800 home-made board suitable for global EMA

Antenna

Acquisition setup

Pictures are courtesy of ESAT, Katholieke Universiteit Leuven, Belgium, (Elke De Mulder [7]).
In-house ALTERA Stratix “as is” suitable for local EMA [9, 8]

S. Guilley, <sylvain.guilley@TELECOM-ParisTech.fr>
XILINX Virtex-5 evaluation board “customized for EMA”

XC5VLX50 evaluation board

FPGA chip

Metallic cover

FF324 (18^2 pins) socket
ALTERA Stratix with chemical preparation for EMA

S. Guilley, <sylvain.guilley@TELECOM-ParisTech.fr>
Modus operandi

Information known/unknown by the attacker

- Known: Observations $O$;
- Known: (usually) either the plaintext or the ciphertext.
- Unknown: the encryption key (case of symmetric encryption).

Strategy: divide-and-conquer

- **Partition** observations according to a **sensitive** variable $S$:
  - depends on the secret $K$,
  - not too many bits of $K$, since attack = exhaustive search,
  - is computable from the plaintext / ciphertext.

Therefore:

- attacks target the first or the last round (in general),
- MixColumns in AES hard to invert ⇒ attack the last round.
Use the traces $O$ to distinguishing between the **correct** partitioning from **wrong** ones

**Distinguishers use a model**

- $M(S)$ is the **physical syndrome** related to the **manipulation** of the secret $S$. It is called the **leakage model**.

**Examples of distinguishers**

- $|\mathbb{E}(O|M(S) = 0) - \mathbb{E}(O|M(S) = 1)|$: ................. DoM
- $\mathbb{E}_s ((O|M(S) - \mathbb{E}O|M(S))(M(S) - \mathbb{E}M(S)))$: ... Covariance
- $\rho_s (O|S = s; M(s))$: .............................................. CPA
- $\mathbb{E}_s H(O|M(S) = M(s))$ or $I(O; M(S))$: .................. MIA
Models $M(S)$

(classification by [10])

Partition-based:

- If unprotected:
  - $M(s) = |s|$; Hamming weight; Bus cleared in SW
  - $M(s) = |s \oplus R|$; Hamming weight; Bus precharged in SW
  - $M(s) = |s \oplus s_{−1}|$; Hamming distance; typical of HW
  - $M(s) = |\overline{s} \cdot s_{−1}| + (1 - \delta)|s \cdot \overline{s_{−1}}|$; Idem, but in near-field EMA

- If protected:
  - $M(s) = s$. **Warning**: $2^n$ values!
  - Difficult to be more inventive if the countermeasure is sound...
  - but we’ll see 😊

Comparison-based: (profiled attacks)

- $M(S) = \mathbb{E}(O|S)$; templates
Various leakage models for DES (iterative architecture)

Caption: black = known values; red = unknown sensitive values
Finding the best leakage models is not obvious

Success rate for model A.

Success rate for model B.

Success rate for model C.

Success rate for model D.
So, shall we conclude the Hamming distance (HD) — model D — is the ultimate model for HW?

SecMat v1[ASIC]:
- Typical trace: 92 mV
- Typical DPA: 3.0 mV
- Side-channel leakage: 3.3 %
- See [4]
Combined attacks!

1. Various distinguishers for a same partitioning;
2. One distinguisher can be evaluated on various partitionings;
3. The diversity can also come from the multiplicity of timing samples usually garnered during an acquisition campaign;
4. It can also arise from multi-modal acquisitions;
5. There can be situations where the most suitable partitioning can evolve from sample to sample in a side-channel capture.

S. Guilley, <sylvain.guilley@TELECOM-ParisTech.fr>
Presentation Outline

1. Context
2. Side-Channel Attacks
   - Side-Channels
   - Side-Channels Acquisitions
   - Attack Algorithms
3. Counter-Measures to SCAs
   - Protocol-Level
   - Register Transfer Level
   - Netlist Level
4. Attacks on Counter-Measures
   - Attack on Information Masking
   - Attack on Information Hiding
5. Conclusions and Perspectives
   - Conclusions
   - Perspectives

S. Guilley, <sylvain.guilley@TELECOM-ParisTech.fr>
Targeted strategies

- Protocol-level:
  - Most wanted since provable
- Register-Transfer Level:
  - Masking. Easiest to implement; Boolean or algorithmic.
  - Encrypted leakage
  - Glitch-full circuits
- Netlist or implementation level:
  - Hiding (= DPL, Dual-rail with Precharge Logic)

Degenerated counter-measures / “Make difficult” strategies

- DPL w/o precharge
- Noise generator, Dummy instructions, Varying clock, etc.

⇒ And as for attacks, countermeasures can be combined.
Protocol level: if $\approx 1$ bit is leaked per 100 encryptions...

Alice:

1. $AES_{k_0}$
2. hash
3. $k_1$
4. $AES_{k_1}$
5. hash
6. $k_2$

Bob:

1. $AES_{k_0}^{-1}$
2. hash
3. $k_0$
4. $AES_{k_1}^{-1}$
5. hash
6. $k_2$
Masking

**Principle**

- Every variable $s$, potentially sensible, is represented as a share \( \{s_0, s_1, \ldots, s_{n-1}\} \)
- To reconstruct $s$, all the $s_i$ are required.
- Example: $n = 2$, $s = s_0 \oplus s_1$.

- Leakage resistant since variables are never used plain;
- Attractive but works only fine for registers.
- Efforts done to protect also the combinational logic.
Encrypted Leakage

\[ y = \text{DES}(x, k_c) \]

Side-channel: EMA, power

FPGA

Encrypted bitstream

Masked DES

Masked DFF

\[ k_i \]

\[ k_c \]

\[ k_b \]

\[ x \]

\[ y = \text{DES}(x, k_c) \]

ASIC (tamper-proof)

Trusted Platform Module

Masked DES

Masked DFF

\[ k_i \]

\[ k_c \]

\[ x \]

\[ y = \text{DES}(x, k_c) \]

personalization

NVM
Glitch-full circuits

(a) IP

(b) FP

Parity bits

IF → 1 MUX

LR → 1 MUX

CD

Round 1: Round logic

Round 2: Round logic

Round 15: Round logic

Round 16: Round logic

“Normal” representation

purely combinatorial logic

S. Guilley, < sylvain.guilley@TELECOM-ParisTech.fr >
Glitch-full circuits
(a) Sequential iterative DES encryption signature, with the average variation margin, for statistics collected on 10k measurements.

(b) Average combinatorial DES encryption signature, with the average variation margin, for statistics collected on 100k measurements.
Hiding: Placement and Routing of Xilinx WDDL+ Netlists.

- P&R tools “naturally” separate true and false paths
- Example with AES substitution box SUBBYTES with and without placement constraints (2 × 2 LuT4 per slice)

Unconstrained placement | Constrained placement
Presentation Outline

1. Context
2. Side-Channel Attacks
   - Side-Channels
   - Side-Channels Acquisitions
   - Attack Algorithms
3. Counter-Measures to SCAs
   - Protocol-Level
   - Register Transfer Level
   - Netlist Level
4. Attacks on Counter-Measures
   - Attack on Information Masking
   - Attack on Information Hiding
5. Conclusions and Perspectives
   - Conclusions
   - Perspectives

S. Guilley, <sylvain.guilley@TELECOM-ParisTech.fr>
Side-Channel Attacks
Counter-Measures to SCAs
Attacks on Counter-Measures
Conclusions and Perspectives

Context

Attack on Information Masking
Attack on Information Hiding

S. Guilley, < sylvain.guilley@TELECOM-ParisTech.fr >
Context
Side-Channel Attacks
Counter-Measures to SCAs
Attacks on Counter-Measures
Conclusions and Perspectives

Attack on Information Masking
Attack on Information Hiding

S. Guilley, <sylvain.guilley@TELECOM-ParisTech.fr>

\[
\text{Message} \quad k_i
\]

\[
\text{IP} \quad \text{IP}
\]

\[
\text{Left masked data (L}_i\text{)} \quad \text{Left mask (ML}_i\text{)}
\]

\[
\text{Right mask (MR}_i\text{)} \quad \text{Right masked data (R}_i\text{)}
\]

Feistel function \( f \)

\[
S(x \oplus k_c)
\]

\[
m' \quad m
\]

\[
x_m
\]

\[
k_c
\]

\[
\text{FP}
\]

\[
\text{Ciphertext}
\]
Attacks on masking

<table>
<thead>
<tr>
<th>Correct key (i.e. physical $L$)</th>
<th>$p(L=0)=1/16$</th>
<th>$p(L=1)=4/16$</th>
<th>$p(L=2)=6/16$</th>
<th>$p(L=3)=4/16$</th>
<th>$p(L=4)=1/16$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H(O</td>
<td>L=0) = 0$</td>
<td>$H(O</td>
<td>L=1) = 0$</td>
<td>$H(O</td>
<td>L=2) = 0$</td>
</tr>
</tbody>
</table>

| Incorrect key (i.e. random $L$) | $H(O|L=0) = 2.03$ | $H(O|L=1) = 2.03$ | $H(O|L=2) = 2.03$ | $H(O|L=3) = 2.03$ | $H(O|L=4) = 2.03$ |
|---------------------------------|--------------------|--------------------|--------------------|--------------------|--------------------|
| $H(O|L) = 2.03$ bit             | $H(O|L) = 2.03$ bit | $H(O|L) = 2.03$ bit | $H(O|L) = 2.03$ bit | $H(O|L) = 2.03$ bit | $H(O|L) = 2.03$ bit |

Incorrect key (i.e. random $L$)

Correct key (i.e. physical $L$)

$H(O|L)=0$ bit

$H(O|L)=2.03$ bit

S. Guilley, <sylvain.guillely@TELECOM-ParisTech.fr>
Attacks on masking

\[ p(L=0) = \frac{1}{16} \quad p(L=1) = \frac{4}{16} \quad p(L=2) = \frac{6}{16} \quad p(L=3) = \frac{4}{16} \quad p(L=4) = \frac{1}{16} \]

Correct key (i.e. physical \( L \))

- \( O|L=0 \)
- \( O|L=1 \)
- \( O|L=2 \)
- \( O|L=3 \)
- \( O|L=4 \)

\[ H(O|L=0) = 2.03 \quad H(O|L=1) = 1.81 \quad H(O|L=3) = 1.5 \quad H(O|L=3) = 1 \quad \Rightarrow H(O|L) = 1.39 \text{ bit} \]

Incorrect key (i.e. random \( L \))

- \( O|L=0 \)
- \( O|L=1 \)
- \( O|L=2 \)
- \( O|L=3 \)
- \( O|L=4 \)

\[ H(O|L=0) = 2.54 \quad H(O|L=1) = 2.54 \quad H(O|L=2) = 2.54 \quad H(O|L=3) = 2.54 \quad \Rightarrow H(O|L) = 2.54 \text{ bit} \]

S. Guilley, sylvain.guilley@TELECOM-ParisTech.fr
Models $M(S)$ (classification by [10])

Partition-based:

- If unprotected:
  - $M(s) = \left| s \right|$; Hamming weight; Bus cleared in SW
  - $M(s) = \left| s \oplus R \right|$; Hamming weight; Bus precharged in SW
  - $M(s) = \left| s \oplus s_{-1} \right|$; Hamming distance; typical of HW
  - $M(s) = \sum_i \bar{s} \cdot s_{-1} + (1 - \delta)s \cdot \bar{s}_{-1}$; Idem, but in near-field EMA

- If protected:
  - $M(s) = s$. WARNING: $2^n$ values!
  - Difficult to be more inventive if the countermeasure is sound...
  - $M(S) = S_1 + S_2$ ; Zero-offset
  - $M(S) = (S_1, S_2)$ ; Multi-variate MIA (MMIA [2])

Comparison-based: (profiled attacks)

- $M(S) = \mathbb{E} \left( O \mid S \right)$; templates
Attacks on DPL

- AES–WDDL–no–EE
- AES–WDDL–EE

Mutual Information vs. Samples

Sensitive vs. Not Sensitive

Evaluation Rounds
Precharge Rounds

S. Guilley, < sylvain.guilley@TELECOM-ParisTech.fr >

OPA attacks & counter-measures
Presentation Outline

1. Context
2. Side-Channel Attacks
   - Side-Channels
   - Side-Channels Acquisitions
   - Attack Algorithms
3. Counter-Measures to SCAs
   - Protocol-Level
   - Register Transfer Level
   - Netlist Level
4. Attacks on Counter-Measures
   - Attack on Information Masking
   - Attack on Information Hiding
5. Conclusions and Perspectives
   - Conclusions
   - Perspectives

- Attacks metric
- Leakage metric
Counter-Measures are still *ad hoc*

1. Multiplicative masking of AES (M.-L. Akkar and Ch. Giraud, CHES 2001)

2. Provable secure S-Box implementation based on FFT (E. Prouff et al, CHES 2006)
   - Bias of the mask attack (S. Coron, CHES 2008)

3. MDPL (Th. Popp and S. Mangard, CHES 2005)
   - Folding attack (P. Schaumont and K. Tiri, CHES 2007),
     Subset attack (E. de Mulder et al, WIFS 2009)

4. DRSL (Z. Chen and Y. Zhou, CHES 2006)
   - Glitch on precharge (M. Nassar, DATE 2009)
Call for Further Researches

Need for formal proofs of security

- Can be at protocol level (*work in progress*).
- Could also be at implementation level (*new research area*).

Devise countermeasures globally ...

... taking into account all possible weaknesses:

- Observation.
- Perturbation.
- Manipulation.


Electromagnetic Analysis Attack on an FPGA Implementation of an Elliptic Curve Cryptosystem.
Belgrade, Serbia & Montenegro.

[8] Laurent Sauvage, Sylvain Guilley, Jean-Luc Danger, Yves Mathieu, and Maxime Nassar.
Successful Attack on an FPGA-based Automatically Placed and Routed WDDL+ Crypto Processor.
In *DATE, track A4 (Secure embedded implementations)*, April 20–24 2009.
Nice, France. Electronic version: http://hal.archives-ouvertes.fr/hal-00325417/en/.

[9] Laurent Sauvage, Sylvain Guilley, and Yves Mathieu.
Full text in http://hal.archives-ouvertes.fr/hal-00319164/en/.

Seoul, Korea.

A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks.
Cologne, Germany.