Power Analysis and Cryptosystem Security: Attacks and Countermeasures

Arnaud Tisserand
CNRS, IRISA laboratory, CAIRN research team

ECOFAC 2012
La Colle-sur-Loup, Alpes Maritimes, France
May 21th – 25th, 2012

Introduction: Security Aspects

- system security
- cryptology

- data
- networks
- operating systems
- programs
- devices

- cryptography
- cryptanalysis
- steganography

Introduction: Embedded Cryptosystems

Objectives:
- Confidentiality
- Integrity
- Authenticity
- Non-repudiation
- ...

Cryptographic primitives:
- Encryption
- Digital signature
- Hash function
- Random numbers generation
- ...

Hardware implementation issues:
- Performances: speed (delay, throughput, ...), low power/energy consumption, size and weight
- Security: protection against attacks
- Cost: device, design

Applications: smart cards, computers, Internet, telecommunications, set-top boxes, data storage, RFID tags, WSN, smart grids...
Introduction: Side Channel Attacks

**Attack**: attempt to find, without any knowledge about the secret:
- the message (or parts of the message)
- informations on the message
- the secret (or parts of the secret)

“Old style” side channel attacks:

Power Consumption: Basic Definitions

**Instantaneous power**:

\[ P(t) = i_{DD}(t) V_{DD} \]

**Energy** over some time interval \( T \):

\[ E = \int_0^T i_{DD}(t) V_{DD} \, dt \]

**Average power** over interval \( T \):

\[ P_{\text{avg}} = \frac{E}{T} = \frac{1}{T} \int_0^T i_{DD}(t) V_{DD} \, dt \]

Units:
- current A
- voltage V
- power W
- energy J or Wh

Power Consumption: Components

Power dissipation in CMOS circuits comes from 2 main components:

- **static** dissipation:
  - sub-threshold conduction through OFF transistors
  - leakage current through P-N junctions
  - tunneling current through gate oxide
  - ...

- **dynamic** dissipation:
  - charging and discharging of load capacitances (useful + parasitic)
  - short-circuit current

\[ P_{\text{total}} = P_{\text{static}} + P_{\text{dynamic}} \]

MOS Transistor: Logic Model

Simple logic behavior (≈ switch)
**MOS Transistors: Series and Parallel**

<table>
<thead>
<tr>
<th>Series</th>
<th>Parallel</th>
</tr>
</thead>
<tbody>
<tr>
<td>N Transistor: ON, P Transistor: OFF</td>
<td>N Transistor: OFF, P Transistor: ON</td>
</tr>
</tbody>
</table>

Series: both must be ON, Parallel: either can be ON

**MOS Transistor: Imperfect Switch**

<table>
<thead>
<tr>
<th>N Transistor</th>
<th>P Transistor</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRONG 0</td>
<td>DEGRADED 0</td>
</tr>
<tr>
<td>DEGRADED 1</td>
<td>STRONG 1</td>
</tr>
</tbody>
</table>

N transistor pull no higher than $V_{DD} - V_{T_N}$
P transistor pull no lower than $|V_{T_P}|$

**CMOS Logic**

CMOS = complementary MOS

N and P transistors are only used for passing strong signals

Techno.: $0.25 \mu m$, $V_{DD} = 2.5 V$, $W = 0.72 \mu m$, $L = 0.24 \mu m$, $V_{T_N} \approx 0.37 V$
Logic Gate: Inverter

The simplest gate: only 2 transistors (1 N and 1 P)

\[
\begin{array}{c|c|c}
A & Y \\
\hline
0 & 1 \\
1 & 0 \\
\end{array}
\]

All logic functions can be built using only NAND gates:

Logic Gate: NAND2 (2-input not–and)

\[
\begin{array}{c|c|c|c|c|c|c}
A & B & Y \\
\hline
0 & 0 & 1 \\
0 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 0 \\
\end{array}
\]

Short-Circuit Current in CMOS Gates

Occurs when both N and P transistors are ON while the input switches

Power reduction solution: use short transition (crisp edges)

The number of transistors in series is limited (3 to 5)
Charging and Discharging Load Capacitances

There are capacitances everywhere in the circuit: transistor gate, routing, parasitics...

Power reduction solutions:
- design small circuits (small transistor, short wires, technology shrinking)
- reduce the activity (algorithms, data coding, sleep mode)
- reduce $V_{DD}$ (without lowering speed)

Simple Power Consumption Model

Average dynamic power dissipation (no leakage, no short circuit):

$$P = \alpha \times C \times f \times V_{DD}^2$$

where
- $\alpha$ is the activity factor
- $C$ is the average switched capacitance (at each cycle)
- $f$ is the circuit frequency
- $V_{DD}$ is the supply voltage

Remark: the gate delay is

$$d = \gamma \times \frac{C \times V_{DD}}{(V_{DD} - V_T)^2} \approx \frac{1}{V_{DD}}$$

Cryptography: Basic Cyphering

Alice wants to secretly send a message to Bob in such a way Eve (eavesdropper/spy) should have no information
Symmetric / Private-Key Cryptography

- **A**: Alice, **B**: Bob
- **M**: plain text/message
- **E**: encryption/ciphering algorithm, **D**: decryption/deciphering algorithm
- **k**: secret key to be shared by A and B
- **E_k(M)**: encrypted text
- **D_k(E_k(M))**: decrypted text

**Analogy**

Asymmetric / Public-Key Cryptography

- **k**: B’s public key (known to everyone including E)
- **E_k(M)**: ciphered text
- **k’**: B’s private key (must be kept secret)
- **D_k’(E_k(M))**: deciphered text
Symmetric or Asymmetric Cryptography?

**Private-key or symmetric cryptography:**
- simple algorithms
  - fast computation
  - limited cost (silicon area, energy)
- requires a key exchange
- key distribution problem for \( n \) persons

**Public-key or asymmetric cryptography:**
- no key exchange
- only 2 keys per person (1 private, 1 public)
- allows digital signature
- more complex algorithms
  - slower computation
  - higher cost

RSA 768 Attack in December 2009

6 months on 80 parallel computers (\( \equiv 1500 \) years for a single computer!)

\[
\text{RSA-768} = \\
3347807169895689878604416984821269081770479498371376856891 \\
243138898288379878002287614711652531743087737814467999489 \\
\times \\
367460436667995904282446337962795263227915816434308764267 \\
60322831573966651127923337341743396810270092798736308917
\]

Source: article

**Factorization of a 768-bit RSA modulus.** Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thome, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann

---

**Theoretical Attacks**

\[ E \rightarrow k, M??? \]

\[ M \rightarrow A \quad E_k(M) \quad \rightarrow B \quad D_k(E_k(M)) = M \]

**Notations:**
- \( M \) plain text
- \( E \) encryption algorithm
- \( D \) decryption algorithm
- \( k \) secret key
- \( C = E_k(M) \) ciphered text
- \( \Box \) secured zone

**Various Types of Attacks**

- timing analysis
- power analysis
- EMR analysis
- observation
- attack
- perturbation
- fault injection
- theoretical
- invasive
- probing
- reverse engineering

**EMR = Electromagnetic radiation**
**Side Channel Analysis/Attacks (SCA)**

![Diagram of SCA](image)

**General principle:** measure external parameter(s) on running device in order to deduce internal informations

---

**What Should be Measured?**

**Answer:** *everything* that can “enter” and/or “get out” in/from the device

- power consumption
- electromagnetic radiation
- temperature
- sound
- computation time
- number of cache misses
- number and type of error messages
- ...

The measured parameters may provide informations on:

- **global** behavior (temperature, power, sound...)
- **local** behavior (EMR, # cache misses...)

---

**Power Consumption Analysis**

**General principle:**

1. measure the current $i(t)$ in the cryptosystem
2. use those measurements to “deduce” secret informations

---

**“Read” the Traces**

- algorithm $\implies$ decomposition into steps
- detect loops
  - constant time for the loop iterations
  - non-constant time for the loop iterations

Differences & External Signature

An algorithm has a current signature and a time signature:

\[ r = c_0 \]

for \( i \) from 1 to \( n \) do

if \( a_i = 0 \) then

\[ r = r + c_1 \]

else

\[ r = r \times c_2 \]

Source: [5]


Simple Power Analysis (SPA)

SPA in Practice

General principle:

Methods: interpretation of the differences in

- control signals
- computation time
- operand values
- ...


Limits of the SPA

Example of behavior difference: (activity into a register)

| \( t \) | \hline
| \( t + 1 \) |
| 0000000000000000 | 0000000000000000 |
| 1111111111111111 | 0000000000000001 |

Important: a small difference may be evaluated as noise during the measurement \( \Rightarrow \) traces cannot be distinguished

Question: what can be done when differences are too small?

Answer: use statistics over several traces

Internal State of a Cryptosystem

\[ \mathcal{E}_k(\mathcal{M}) \]

**Notations:**
- \( t \) specific moment during the execution \( (t \in \{1, \ldots, T\}) \)
- \( S = \mathcal{E}_k(M, k, t) \) internal state of the cryptosystem
- **IMPORTANT:** \( S \) is hidden (secured zone)

**Objective:** try to discover \( b \) one element of \( S \) (e.g. one bit)

**Differential Power Analysis (DPA) (1/2)**

**General principle:**
1. run the cryptosystem \( N \) times
   - \( \triangleright \) save all plain text messages \( M_i \) \((i \in \{1, \ldots, N\})\)
   - \( \triangleright \) measure all traces \( P_{ij} \) \((j \in \{1, \ldots, T\})\)
2. compute the average trace \( \overline{P}_j = \frac{1}{N} \sum_{i=1}^{N} P_{ij} \)
3. select one bit \( b \) to attack (i.e. find internal \( b \))
4. split the traces \( P_{ij} \) into 2 sets:
   - \( S_0 \) the set where \( b = 0 \) (all \( i \) that lead to \( b = 0 \))
   - \( S_1 \) the set where \( b = 1 \) (all \( i \) that lead to \( b = 1 \))
5. select a test hypothesis \( b \):
   - \( H = H_{b=0} \) or \( H_{b=1} \)
6. perform the statistical comparison of the average trace \( \overline{P}_j \) with the average trace of \( S_0 \) or \( S_1 \) (the one that corresponds to \( H \))

**DPA Example**

Assume \( H = H_{b=0} \), compare \( \overline{P}_j \) and the average trace for \( S_0 \)

Possible comparison results:
- there is no significant difference \( \implies \) \( H \) was **incorrect** (i.e. \( b \neq 0 \))
- there is a significant difference at time \( t \) \( \implies \) \( H \) was **correct** (i.e. \( b = 0 \))

**Remark:** same thing with the other hypothesis

Assume \( H = H_{b=1} \), compare \( \overline{P}_j \) and the average trace for \( S_1 \)

Possible comparison results:
- there is no significant difference \( \implies \) \( H \) was **incorrect** (i.e. \( b \neq 1 \))
- there is a significant difference at time \( t \) \( \implies \) \( H \) was **correct** (i.e. \( b = 1 \))
**Why does it work?**

**Answer:** thanks to the partitioning $S_0 / S_1$ w.r.t. $H$

- if hypothesis $H$ is incorrect
  - $\Rightarrow$ the $N$ runs/traces correspond to a bad value of $b$
  - $\Rightarrow$ partitioning $S_0 / S_1$ is random
  - $\Rightarrow$ if $N$ is large, the global average trace and the partition average trace are close at time $j = t$

- if hypothesis $H$ is correct:
  - $\Rightarrow$ the $N$ runs/traces correspond to a good value of $b$
  - $\Rightarrow$ partitioning $S_0 / S_1$ is significant
  - $\Rightarrow$ if $N$ is large, the global average trace and the partition average trace are different at time $j = t$ because there is a behavior difference between $b = 0$ and $b = 1$

**Remarks on the DPA**

- partitioning requires the theoretical value of $b$ for each message $M_i$
- $N$ must be large enough in order to:
  - amplify the difference when $H$ is correct
  - leads to a random difference when $H$ is incorrect
- knowing $t$ is not necessary to attack, but it helps to reduce the size of the traces (then the cost)
- the difficult point is to determine which $b$ to attack!
  - $b$ should lead to a measurable difference in the behavior
  - $b$ should have a simple relation with the secret
  - $b$ may a single bit or a group of bits
- use advanced and higher order statistical tests
- this attack is very efficient in practice

**Electromagnetic Radiation Analysis (1/2)**

**General principle:** use a probe to measure the EMR

**EMR measurement:**
- global EMR with a large probe
- local EMR with a microprobe

**Electromagnetic Radiation Analysis (2/2)**

**EMR analysis methods:**
- simple electromagnetic analysis: SEMA
- differential electromagnetic analysis: DEMA

**Local EMR analysis may be used to determine internal architecture details, and then select weak parts of the circuit for the attack**

$\Rightarrow$ X-Y table
Subthreshold Current in CMOS Gates

TABLE I
LEAKAGE CURRENT (IN NANOAMPERES) IN VARIOUS CMOS LOGIC GATES (90-nm TECHNOLOGY)

<table>
<thead>
<tr>
<th>In</th>
<th>T=0°C</th>
<th>T=25°C</th>
<th>T=50°C</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1.36</td>
<td>3.19</td>
<td>6.52</td>
</tr>
<tr>
<td>1</td>
<td>0.24</td>
<td>0.73</td>
<td>1.90</td>
</tr>
</tbody>
</table>

NAND gate

<table>
<thead>
<tr>
<th>InA</th>
<th>InB</th>
<th>T=0°C</th>
<th>T=25°C</th>
<th>T=50°C</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0.17</td>
<td>0.47</td>
<td>1.1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1.36</td>
<td>3.19</td>
<td>6.52</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1.02</td>
<td>2.44</td>
<td>5.09</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0.48</td>
<td>1.42</td>
<td>3.79</td>
</tr>
</tbody>
</table>

TABLE II
LEAKAGE CURRENT (IN NANOAMPERES) IN VARIOUS CMOS LOGIC GATES (65-nm TECHNOLOGY)

<table>
<thead>
<tr>
<th>InA</th>
<th>InB</th>
<th>T=0°C</th>
<th>T=25°C</th>
<th>T=50°C</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0.27</td>
<td>3.78</td>
<td>5.86</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0.13</td>
<td>0.47</td>
<td>1.40</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0.25</td>
<td>0.98</td>
<td>3.66</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0.30</td>
<td>0.94</td>
<td>2.71</td>
</tr>
</tbody>
</table>

NAND gate

TABLE V
S-BOX TRUTH LEAKAGE CURRENT (65-nm TECHNOLOGY, \(T = 25°C\) AND \(100°C\))

<table>
<thead>
<tr>
<th>IN</th>
<th>OUT</th>
<th>(I_{lep}(\mu A)) @T=25°C</th>
<th>(I_{lep}(\mu A)) @T=100°C</th>
</tr>
</thead>
<tbody>
<tr>
<td>0100</td>
<td>1111</td>
<td>121.6</td>
<td>130.1</td>
</tr>
<tr>
<td>0101</td>
<td>1100</td>
<td>121.6</td>
<td>130.1</td>
</tr>
<tr>
<td>0110</td>
<td>1010</td>
<td>121.6</td>
<td>130.1</td>
</tr>
<tr>
<td>0111</td>
<td>0110</td>
<td>121.6</td>
<td>130.1</td>
</tr>
</tbody>
</table>

Leakage-Based Differential Power Analysis

Summary of Leakage Power Attacks

Source: [1]
Source: [7]
Countermeasures

**Principles for preventing attacks:**
- embed additional protection blocks
- modify the original circuit into a secured version
- application levels: circuit, architecture, algorithm, protocol...

**Countermeasures:**
- electrical shielding
- use uniform computation durations
- use uniform power consumption
- use detection/correction codes (for fault injection attacks)
- provide a random behavior (algorithms, representation, operations...)
- add noise (e.g. useless instructions/computations)
- circuit reconfiguration (algorithms, block location, representation of values...)

---

Low-Level Coding and Circuit Activity

**Assumptions:**
- \( b \) is a bit (i.e. \( b \in \{0,1\} \), logical or mathematical value)
- electrical states for a wire \(-\): \( V_{DD} \) (logical 1) or GND (logical 0)

**Low-level codings of a bit:**

<table>
<thead>
<tr>
<th></th>
<th>( b = 0 )</th>
<th>( b = 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>standard</td>
<td>GND</td>
<td>( V_{DD} )</td>
</tr>
<tr>
<td>dual rail</td>
<td>( r_0 = V_{DD} )</td>
<td>( r_0 = \text{GND} )</td>
</tr>
<tr>
<td></td>
<td>( r_1 = \text{GND} )</td>
<td>( r_1 = V_{DD} )</td>
</tr>
</tbody>
</table>

---

Countermeasure: Architecture

**Increase internal parallelism:**
- replace one fast but big operator
- by several instances of a small but slow one

---

Important overhead: silicon area and local storage (registers)

---

Other current works: use reconfigurable architectures
GF(2^m) Multipliers with Reduced Activity Variations (1/3)
Collaboration with Danuta Pamula, protection schemes for GF(2^{233}).

Classic unprotected multiplier:

![Graph showing number of transitions over cycles for classic unprotected multiplier]

Classic protected multiplier:

![Graph showing number of transitions over cycles for classic protected multiplier]

GF(2^m) Multipliers with Reduced Activity Variations (2/3)
Mastrovito unprotected multiplier:

![Graph showing number of transitions over cycles for Mastrovito unprotected multiplier]

Mastrovito protected multiplier:

![Graph showing number of transitions over cycles for Mastrovito protected multiplier]

GF(2^m) Multipliers with Reduced Activity Variations (3/3)
FFT and spectral flatness measure (SFM) analysis:

![Graph showing power (log scale) over normalized frequency for different multipliers]

Typical ECC Computations

- $E : y^2 = x^3 + 4x + 20$ over GF(1009)
- Points on $E$: $P, Q = (x,y)$ or $(x,y,z)$ coordinates: $x,y,z \in GF(\cdot)$
- $GF(p), GF(2^m), t : 160–600$ bits
- $k = (k_1, k_2, ... k_t) z \in \mathbb{N}$

Scalar multiplication operation:

$$k \cdot P = k_1P + k_2P + ... + k_tP$$

![Diagram showing typical ECC computations]

Double-Base Number System

Standard radix-2 representation:

\[ k = \sum_{i=0}^{t-1} k_i 2^i \]

where \( k_i \in \{0,1\} \), typical size: \( t \in \{160, \ldots, 600\} \)

Digits: \( k_i \in \{0,1\} \)

DBNS is a very redundant and sparse representation:

\[ DBNS \text{ of } 1701 = \{k_{n-1}, k_{n-2}, \ldots, k_1, k_0\} \]

where \( n (2,3) \)-terms and \( k_i \in \{1\} \) or \( k_j \in \{-1,1\} \)

DBNS is redundant \( \Rightarrow \) security

DBNS is sparse \( \Rightarrow \) 20–30% speed

Randomized DBNS Recoding of the Scalar \( k \)

Possible rules:

\[ R_1(k) \rightarrow R_2(k) \rightarrow \cdots \cdot \]


Proposed solution: use random redundant representations of \( k \)
Conclusion

- Side channel attacks are serious threats
- Attacks are more and more efficient (many variants)
- Security analysis is mandatory at all levels (specification, algorithm, operation, implementation)
- Security = trade-off between performances, robustness and cost
- Security = \text{func}(\text{secret value, attacker capabilities})
- security = computer science + microelectronics + mathematics

Current works examples:

- Methods/tools for automating security analysis
- Circuit reconfiguration (representations, algorithms)
- Circuits with reduced activity variations
- Representation of numbers with error detection/correction codes
- Design space exploration
- CAD tools with security improvement capabilities

References I

- M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti.
  Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits.

  The sorcerer's apprentice guide to fault attacks.

  Hardware implementation of DBNS recoding for ECC processor.

- P. C. Kocher.
  Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems.

  Differential power analysis.

References II

- F. Koeune and F.-X. Standaert.
  A tutorial on physical security and side-channel attacks.

- L. Lin and W. Burleson.
  Leakage-based differential power analysis (LDPA) on sub-90nm CMOS cryptosystems.

- D. Pamula and A. Tisserand.
  \text{GF}(2^m) finite-field multipliers with reduced activity variations.
  In 4th International Workshop on the Arithmetic of Finite Fields, pages 1–16, Bochum, Germany, July 2012.

Good Books (in French)

- \textit{Histoire des codes secrets}
  Simon Singh
  1999
  Livre de poche

- \textit{Mathématiques, espionnage et piratage informatique}
  Joan Gomez
  2010
  Le monde est mathématique, RBA
Cryptographie appliquée
Bruce Schneier
1997, 2ème édition
Wiley

Courbes elliptiques
Philippe Guillot
2010
Hermes

Cours de cryptographie
Gilles Zémor
2000
Cassini

Micro et nano-électronique
Bases, Composants, Circuits
Hervé Fanet
2006
Dunod

CMOS VLSI Design
A Circuits and Systems Perspective
Neil Weste and David Harris
3rd edition, 2004
Addison Wesley

Power Analysis and Cryptosystem Security: Attacks and Countermeasures

Handbook of Applied Cryptography
Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone
2001
CRC Press
ISBN:0-8493-8523-7
Web: http://cacr.uwaterloo.ca/hac/
The end, some questions?

Contact:

- mailto:arnaud.tisserand@irisa.fr
- http://people.irisa.fr/Arnaud.Tisserand/
- CAIRN Group http://www.irisa.fr/cairn/
- IRISA Laboratory, CNRS–INRIA–Univ. Rennes 1
  6 rue Kérampont, BP 80518, F-22305 Lannion cedex, France

Thank you