Power Analysis and Cryptosystem Security: Attacks and Countermeasures

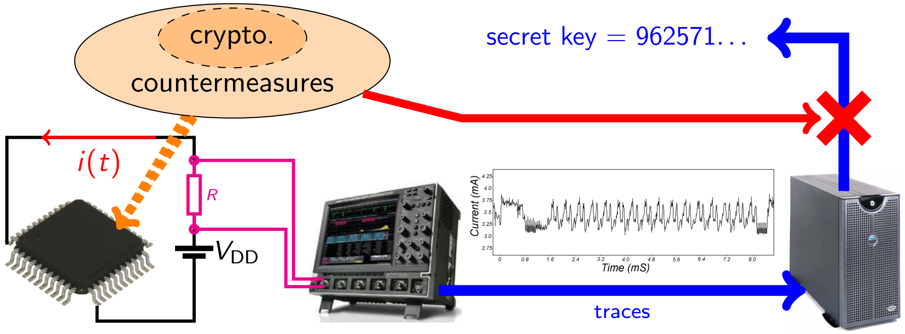
Arnaud Tisserand

CNRS, IRISA laboratory, CAIRN research team

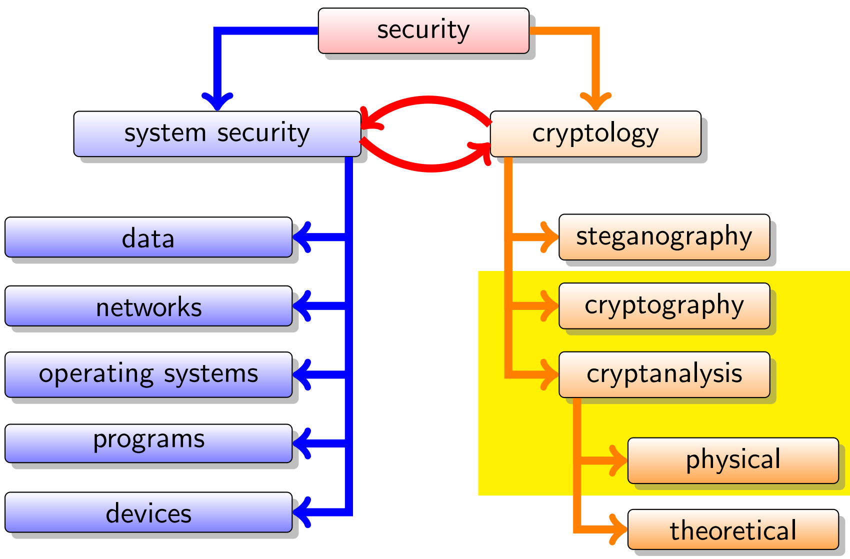
ECOFAC 2012
La Colle-sur-Loup, Alpes Maritimes, France
May 21th – 25th, 2012

Summary

- Introduction
- Power/energy consumption sources in integrated circuits
- Short introduction to embedded cryptosystems
- Side channel attacks based on power analysis
- Countermeasures
- Conclusion & References



Introduction: Security Aspects



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

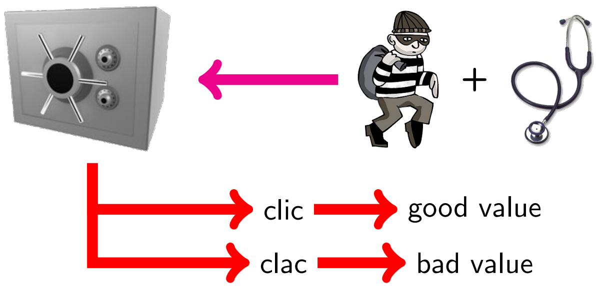
Applications: smart cards, computers, Internet, telecommunications, set-top boxes, data storage, RFID tags, WSN, smart grids...

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:

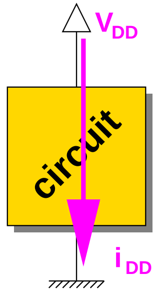
$$P(t) = i_{DD}(t)\, V_{\mathrm{DD}}$$

Energy over some time interval T:

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

Average power over interval T:

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



Units:

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

Power Consumption: Components

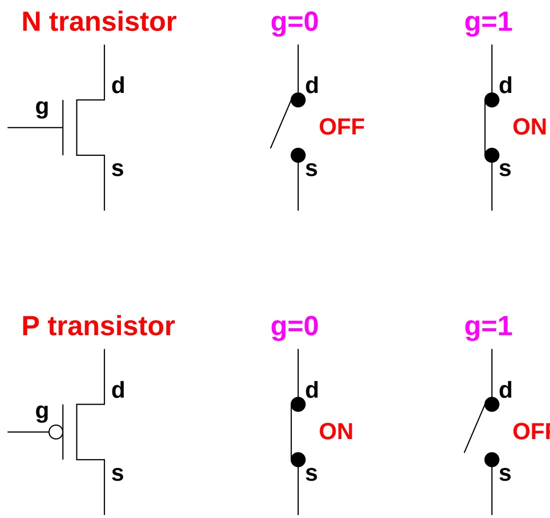
Power dissipation in CMOS circuits comes from 2 main components:

- 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

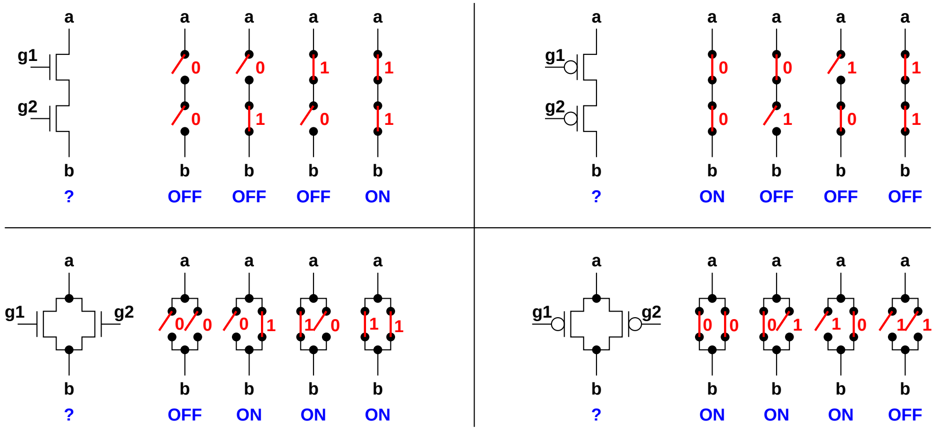
$$P_{\mathrm{total}} = P_{\mathrm{static}} + P_{\mathrm{dynamic}}$$

MOS Transistor: Logic Model

Simple logic behavior (≈ switch)



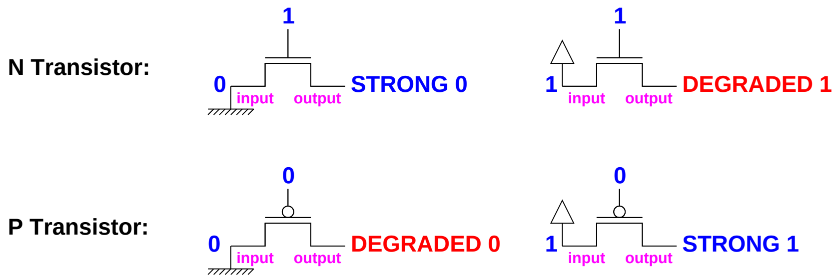
MOS Transistors: Series and Parallel



N: (1=ON, 0=OFF), P: (1=OFF, 0=ON)

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

MOS Transistor: Imperfect Switch

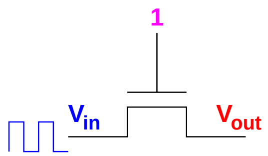


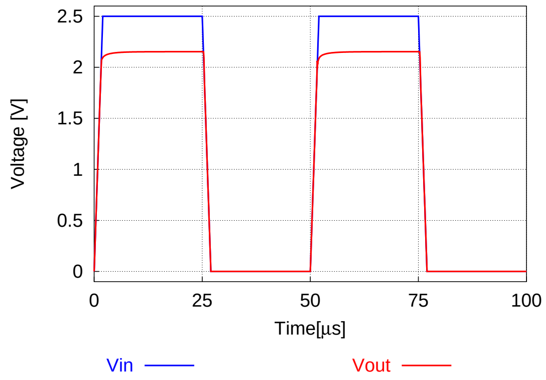
	0	1
STRONG	V_{SS}	V_{DD}
DEGRADED	greater than V_{SS}	less than V_{DD}

N transistor pull no higher than $V_{DD} - V_{T_N}$

P transistor pull no lower than $|V_{T_P}|$

MOS Transistor: Imperfect Switch Simulation



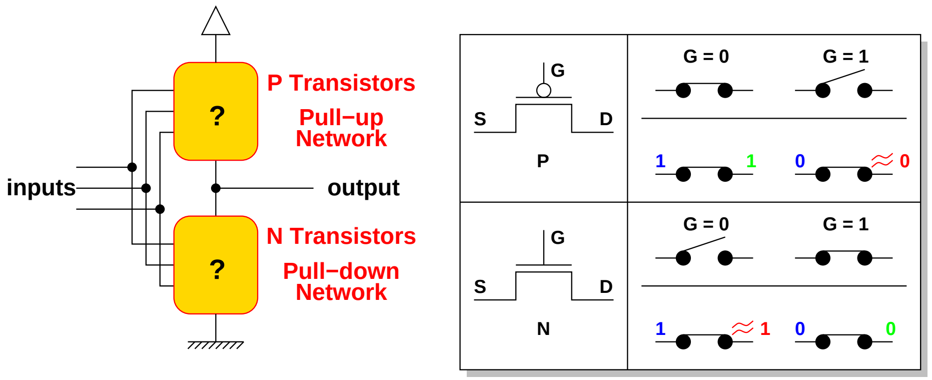


Techno.: $0.25\,\mu\text{m}$, $V_{DD} = 2.5\,V$, $W = 0.72\,\mu\text{m}$, $L = 0.24\,\mu\text{m}$, $V_{T_N} \approx 0.37\,V$

CMOS Logic

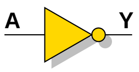
CMOS = *complementary MOS*

N and P transistors are only used for passing strong signals



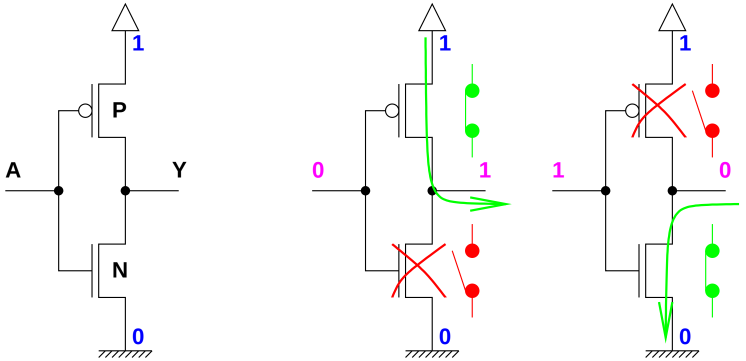
Logic Gate: Inverter

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

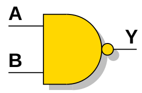


A	Y
0	1
1	0

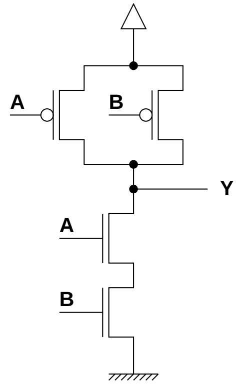
circuit: behavior:



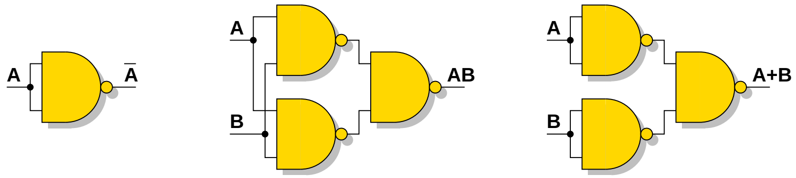
Logic Gate: NAND2 (2-input not–and)



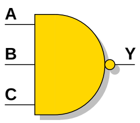
A	B	Y
0	0	1
0	1	1
1	0	1
1	1	0



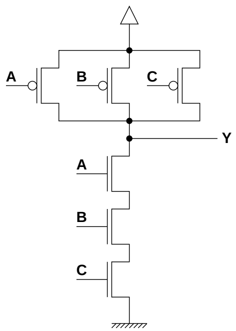
All logic functions can be built using only NAND gates:



Logic Gate: NAND3 (3-input NAND)



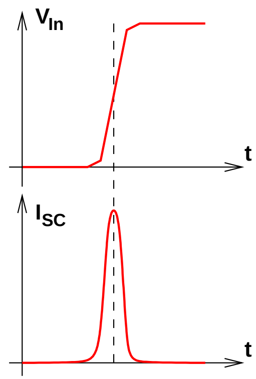
A	B	C	Y
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

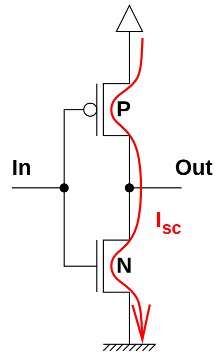


The number of transistors in series is limited (3 to 5)

Short-Circuit Current in CMOS Gates

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

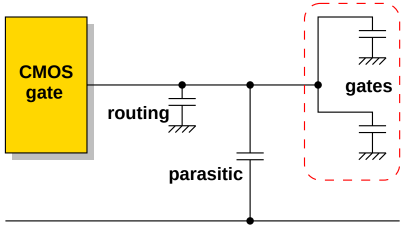




Power reduction solution: use short transition (crisp edges)

Charging and Discharging Load Capacitances

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



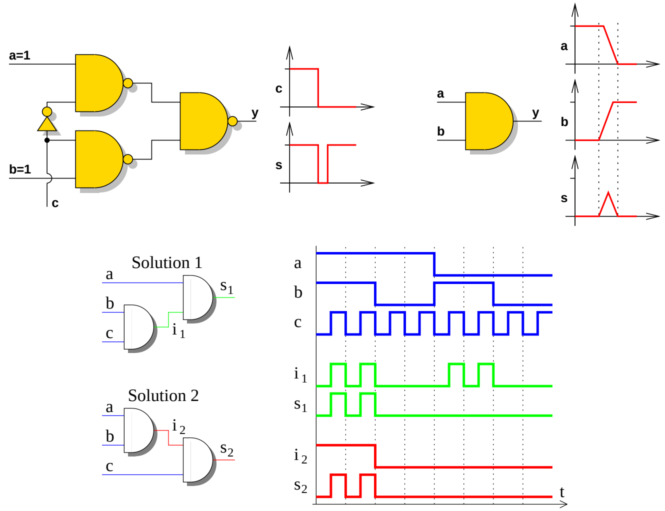
Power reduction solutions:

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

Transitions

There are 2 kinds of transitions:

- useful transitions (data switching)
- redundant or parasitic transitions (imperfections)



Simple Power Consumption Model

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

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

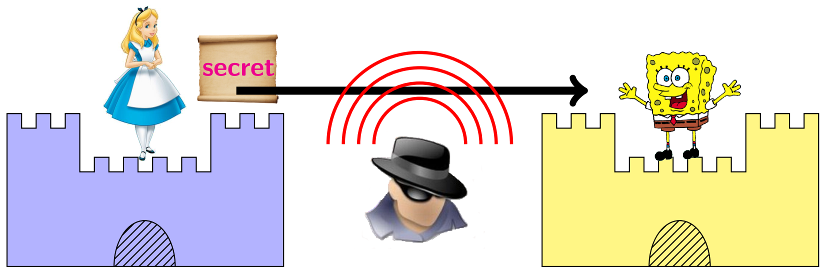
where

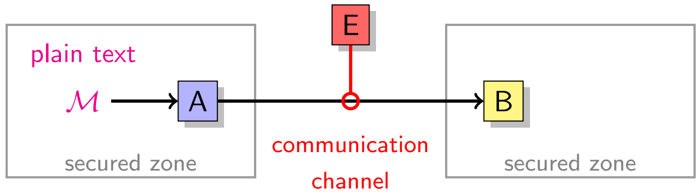
- α is the activity factor
- C is the average switched capacitance (at each cycle)
- f is the circuit frequency
- V_{DD} is the supply voltage

Remark: the gate delay is $d = \gamma \times \frac{C \times V_{\mathrm{DD}}}{(V_{\mathrm{DD}} - V_T)^2} \approx \frac{1}{V_{\mathrm{DD}}}$

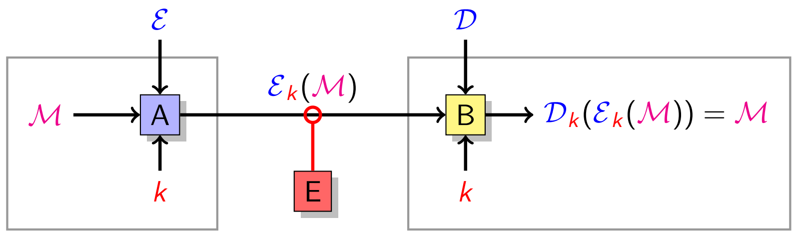
Cryptography: Basic Cyphering

Alice wants to secretly send a message to Bob in such a way Eve (eavesdropper/spy) should have **no** information



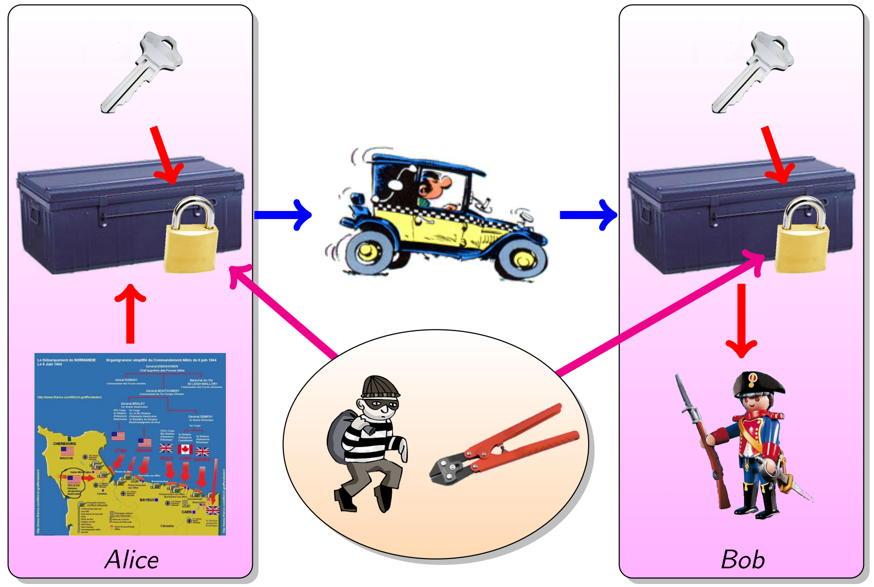


Symmetric / Private-Key Cryptography

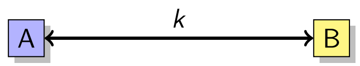
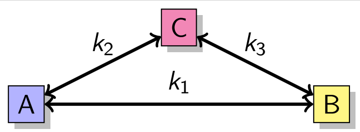
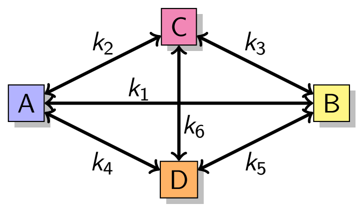


- A: Alice, B: Bob
- $\mathcal{M}$: plain text/message
- $\mathcal{E}$: encryption/ciphering algorithm, $\mathcal{D}$: decryption/deciphering algorithm
- k: secret key to be shared by A and B
- $\mathcal{E}_k(\mathcal{M})$: encrypted text
- $\mathcal{D}_k(\mathcal{E}_k(\mathcal{M}))$: decrypted text
- E: eavesdropper/spy

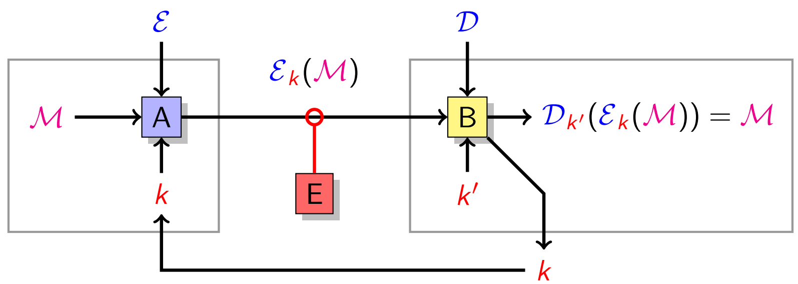
Analogy



Symmetric Cryptography Limitation

people		required keys	
n	list	list	number
2	A, B		1
3	A, B, C		3
4	A, B, C, D		6
n	A, . . .		$\frac{n\times(n-1)}{2}$

Asymmetric / Public-Key Cryptography



- k: B's public key (known to everyone including E)
- $\mathcal{E}_k(\mathcal{M})$: ciphered text
- k': B's private key (must be kept secret)
- $\mathcal{D}_{k'}(\mathcal{E}_k(\mathcal{M}))$: deciphered text

Symmetric or Asymmetric Cryptography?

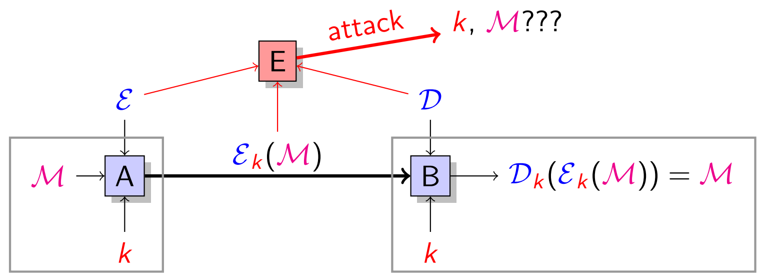
Private-key or symmetric cryptography:

- ☺ 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

Theoretical Attacks



Notations:

- $\mathcal{M}$ plain text
- $\mathcal{E}$ encryption algorithm
- $\mathcal{D}$ decryption algorithm
- k secret key
- $\mathcal{C} = \mathcal{E}_k(\mathcal{M})$ ciphered text
- ▭ secured zone

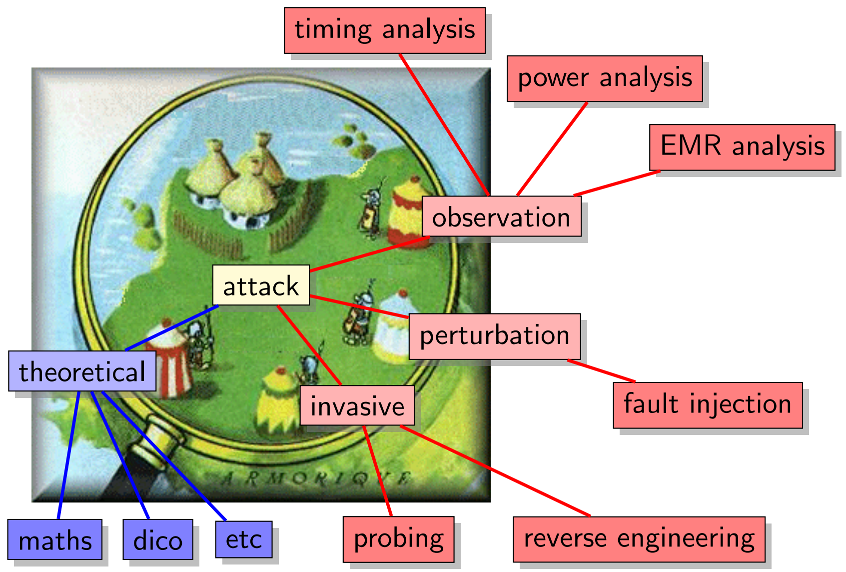
RSA 768 Attack in December 2009

6 months on 80 parallel computers (≡ 1 500 years for a single computer!)

RSA-768 =
3347807169895689878604416984821269081770479498371376856891
2431388982883793878002287614711652531743087737814467999489
×
3674604366679959042824463379962795263227915816434308764267
6032283815739666511279233373417143396810270092798736308917

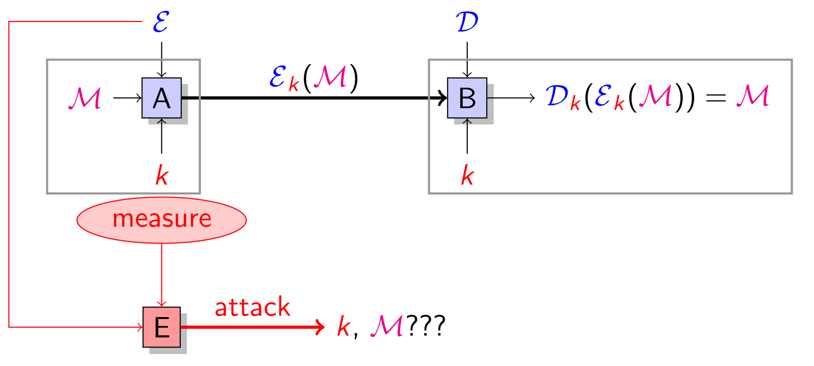
Source: article
`http://eprint.iacr.org/2010/006.pdf`
Factorization of a 768-bit RSA modulus. Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thome, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann

Various Types of Attacks



EMR = Electromagnetic radiation

Side Channel Analysis/Attacks (SCA)



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
- ...

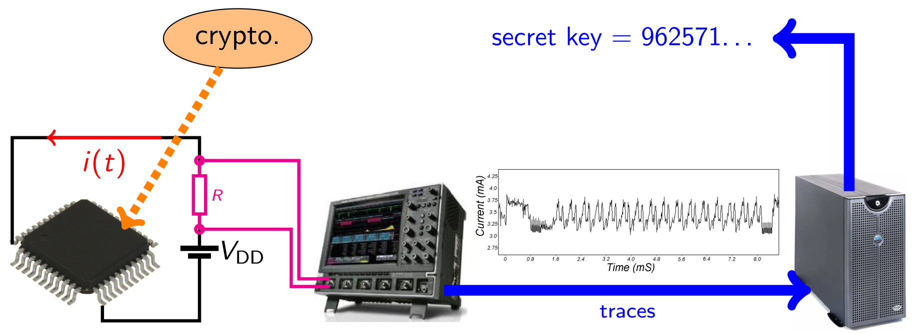
The measured parameters may provide informations on:

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

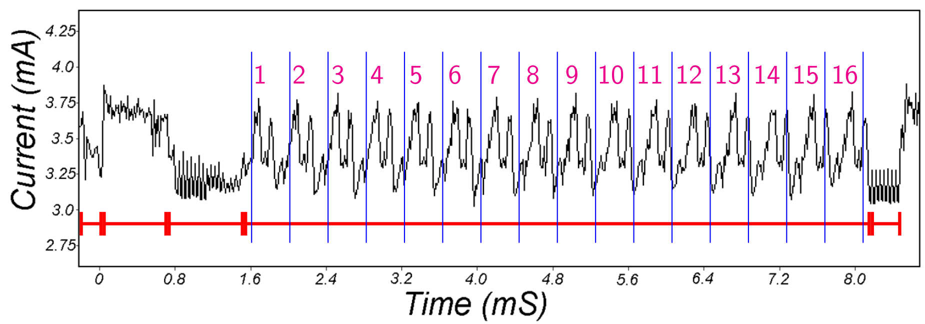
Power Consumption Analysis

General principle:

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



"Read" the Traces



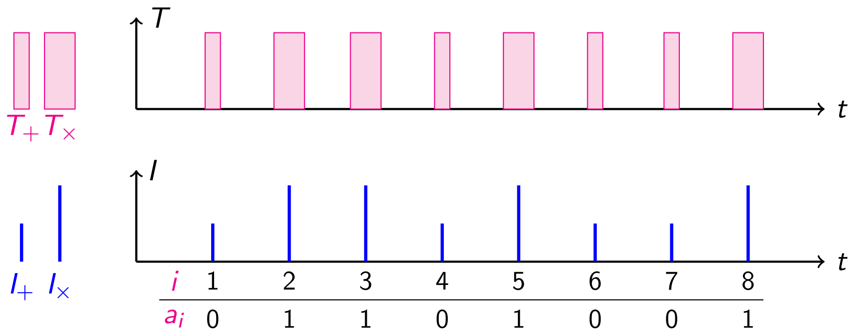
- algorithm $\Longrightarrow$ decomposition into steps
- detect loops
  - constant time for the loop iterations
  - non-constant time for the loop iterations

Source: [5] Kocher, Jaffe and Jun. **Differential Power Analysis**, Crypto99

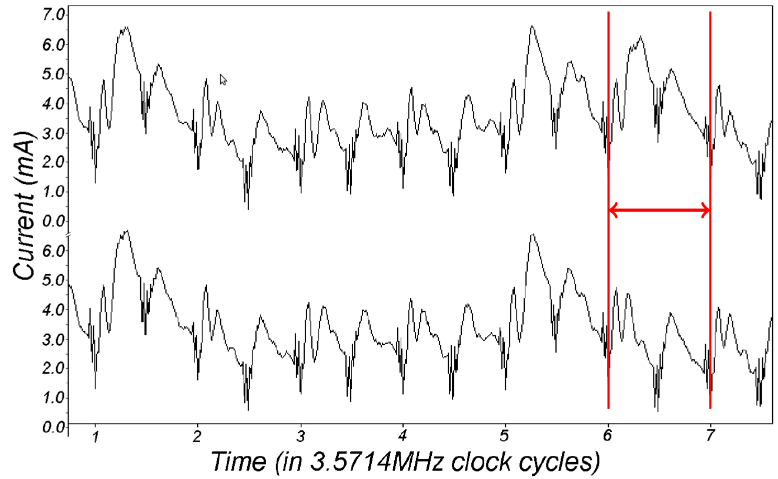
Differences & External Signature

An algorithm has a current signature and a time signature:

```
r = c0
for i from 1 to n do
   if a_i = 0 then
      r = r+c1
   else
      r = r×c2
```



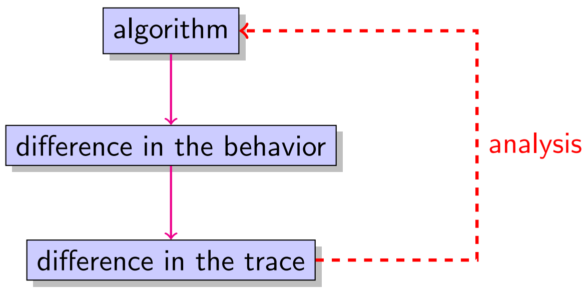
Simple Power Analysis (SPA)



Source: [5]

SPA in Practice

General principle:

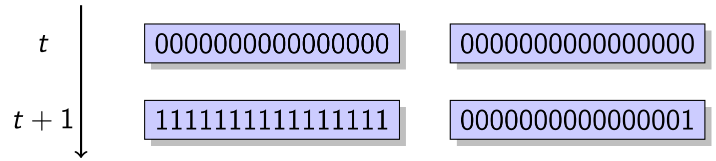


Methods: interpretation of the differences in

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

Limits of the SPA

Example of behavior difference: (activity into a register)

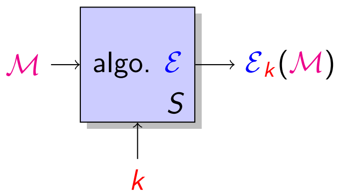


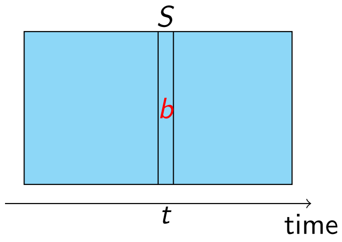
Important: a small difference may be evaluated has a noise during the measurement $\Longrightarrow$ traces cannot be distinguished

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

Answer: use statistics over several traces

Internal State of a Cryptosystem





Notations:

- t specific moment during the execution ($t \in \{1, ..., T\}$)
- $S = F_{\mathcal{E}}(\mathcal{M}, k, t)$ 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
   - save all plain text messages $\mathcal{M}_i$ ($i \in \{1, ..., N\}$)
   - measure all traces P_{ij} ($j \in \{1, ..., T\}$)
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)

Differential Power Analysis (DPA) (2/2)

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

Possible comparison results:

- there is no significant difference $\Longrightarrow$ H was incorrect (i.e. $b \neq 0$)
- there is a significant difference at time t $\Longrightarrow$ H was correct (i.e. $b = 0$)

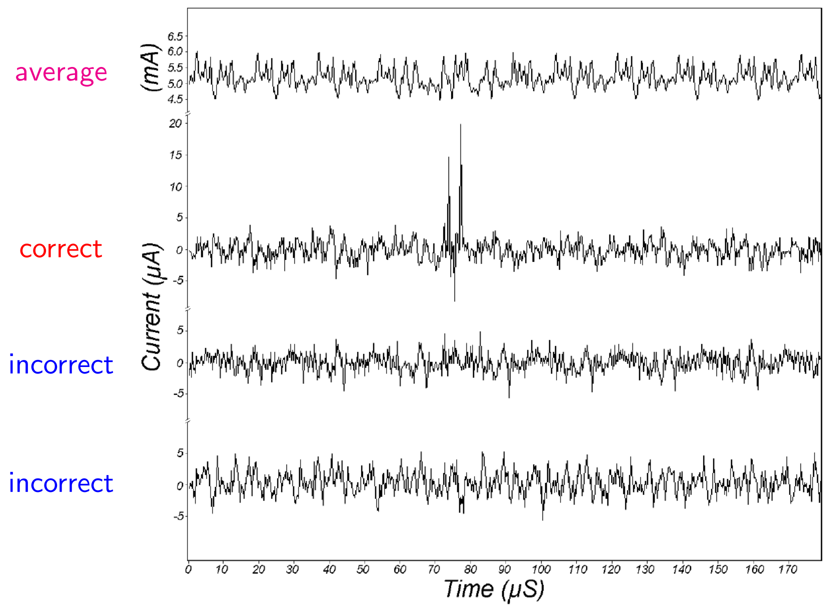
Remark: same thing with the other hypothesis

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

Possible comparison results:

- there is no significant difference $\Longrightarrow$ H was incorrect (i.e. $b \neq 1$)
- there is a significant difference at time t $\Longrightarrow$ H was correct (i.e. $b = 1$)

DPA Example



Why does it work?

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

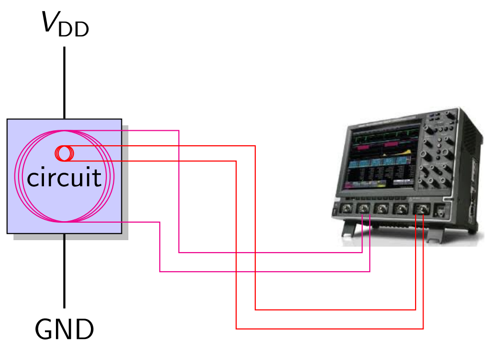
- if hypothesis H is incorrect
  - $\Longrightarrow$ the N runs/traces correspond to a bad value of b
  - $\Longrightarrow$ partitioning S_0 / S_1 is random
  - $\Longrightarrow$ if N is large, the global average trace and the partition average trace are close at time $j = t$
- if hypothesis H is correct:
  - $\Longrightarrow$ the N runs/traces correspond to a good value of b
  - $\Longrightarrow$ partitioning S_0 / S_1 is significant
  - $\Longrightarrow$ 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 $\mathcal{M}_i$
- 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

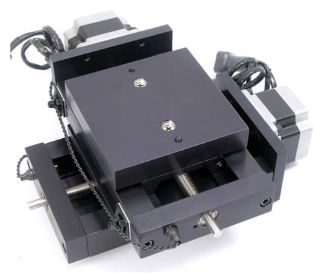
Electromagnetic Radiation Analysis (2/2)

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

$\Longrightarrow$ X-Y table



Subthreshold Current in CMOS Gates

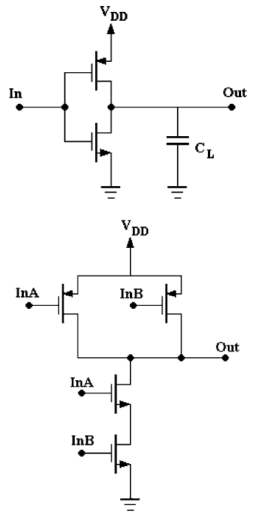


TABLE I
LEAKAGE CURRENT (IN NANOAMPERES) IN VARIOUS CMOS LOGIC GATES (90-nm TECHNOLOGY)

Inverter gate				
In		*T*=0 °C	*T*=25 °C	*T*=50 °C
0		1.36	3.19	6.52
1		0.24	0.73	1.90
NAND2 gate				
InA	*InB*	*T*=0 °C	*T*=25 °C	*T*=50 °C
0	0	0.17	0.47	1.1
0	1	1.36	3.19	6.52
1	0	1.02	2.44	5.09
1	1	0.48	1.47	3.79

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

Inverter gate				
InA		*T*=0 °C	*T*=25 °C	*T*=50 °C
0		2.67	2.98	3.66
1		0.13	0.47	1.40
NAND2 gate				
InA	*InB*	*T*=0 °C	*T*=25 °C	*T*=50 °C
0	0	2.37	2.45	2.59
0	1	2.65	2.98	3.66
1	0	2.52	2.77	3.29
1	1	0.26	0.94	2.81

Source: [1]

Attack Simulation: Serpent 4 × 4 S-Box Transform

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

IN	*OUT*	$I_{leak,i}$ (nA) @*T*=25 °C	$I_{leak,i}$ (nA) @*T*=100 °C
0100	1111	114.6	941.6
1001	1101	115.0	950.0
0000	0011	117.1	950.2
0001	1110	117.9	959.7
1000	1000	118.8	964.0
0011	0111	121.9	999.8
1100	0001	122.9	1007.8
0010	1010	123.4	1016.2
1011	0000	124.0	1024.0
1010	0110	124.8	1026.3
1111	1100	125.4	1031.6
0101	0100	127.1	1031.9
1101	0010	128.2	1032.7
0110	0101	129.6	1051.9
1110	1011	130.7	1052.8
0111	1001	131.6	1071.7

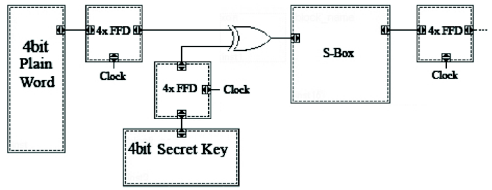
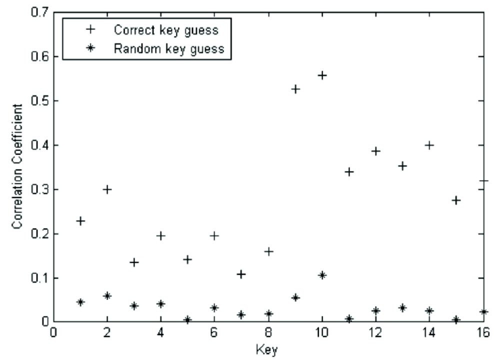


Fig. 6. Crypto core based on Serpent S-Box.



Leakage-Based Differential Power Analysis

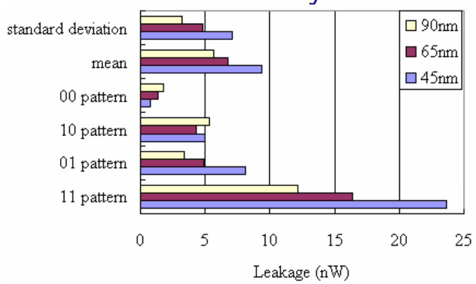


Figure 2. Leakage dependence on input patterns of NAND gate in Sub-90nm standard CMOS.

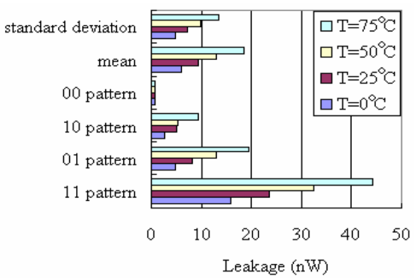
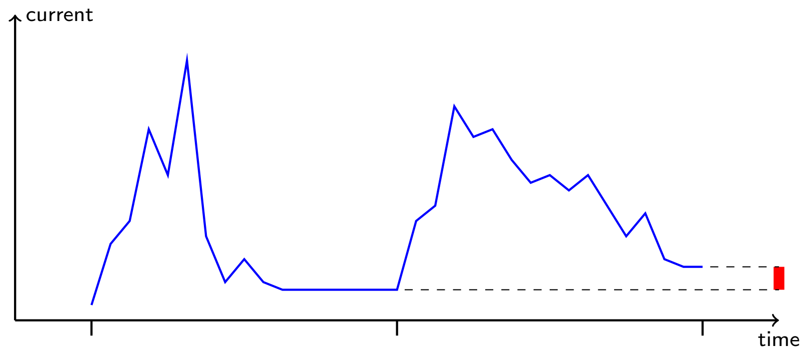


Figure 3. Leakage dependence on input patterns with temperature variations

Source: [7]

Summary of Leakage Power Attacks



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...)

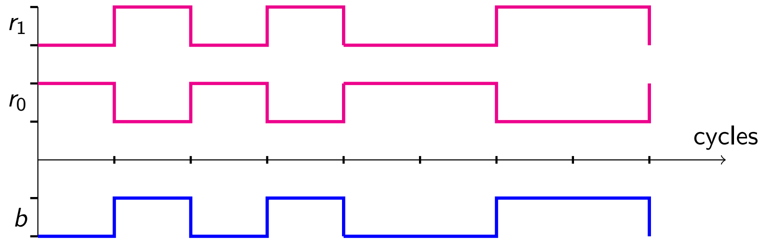
Low-Level Coding and Circuit Activity

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:

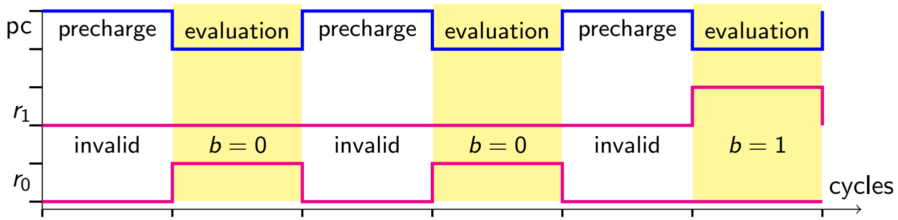
	$b=0$	$b=1$
standard	GND	V_{DD}
dual rail	$r_0 = V_{DD}$, $r_1 = GND$ $(1,0)_{DR}$	$r_0 = GND$, $r_1 = V_{DD}$ $(0,1)_{DR}$



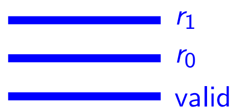
Circuit Logic Styles for Power Uniformization

Countermeasure principle: uniformize circuit activity

Solution based on precharge logic and dual-rail coding:



Solution based on validity line and dual-rail coding:

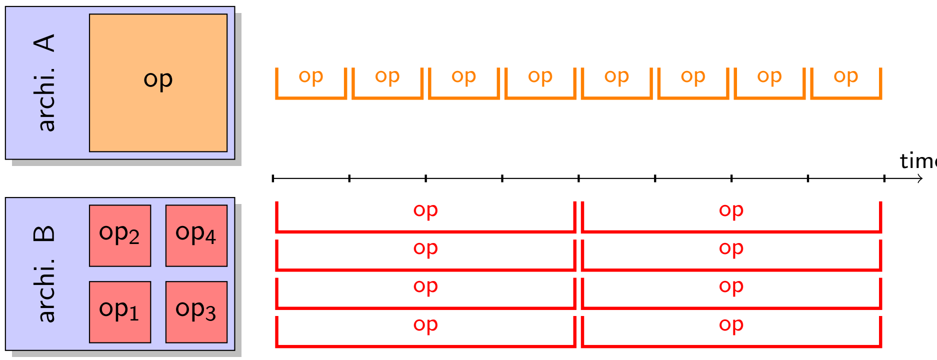


Important overhead: silicon area and local storage (registers)

Countermeasure: Architecture

Increase internal parallelism:

- replace one fast but big operator
- by several instances of a small but slow one

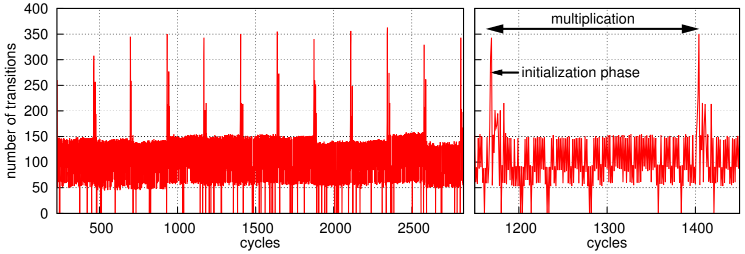


Other current works: use reconfigurable architectures

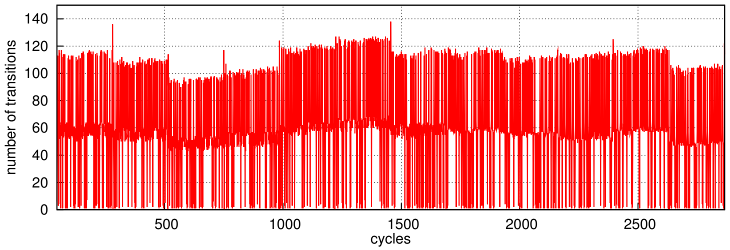
$\mathrm{GF}(2^m)$ Multipliers with Reduced Activity Variations (1/3)

Collaboration with Danuta Pamula, protection schemes for $\mathrm{GF}(2^{233})$.

Classic unprotected multiplier:

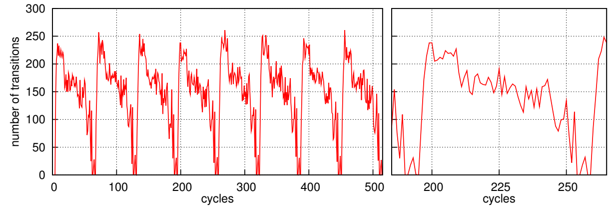


Classic protected multiplier:

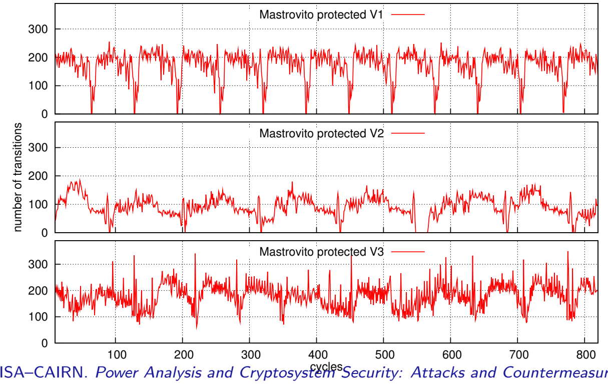


$\mathrm{GF}(2^m)$ Multipliers with Reduced Activity Variations (2/3)

Mastrovito unprotected multiplier:

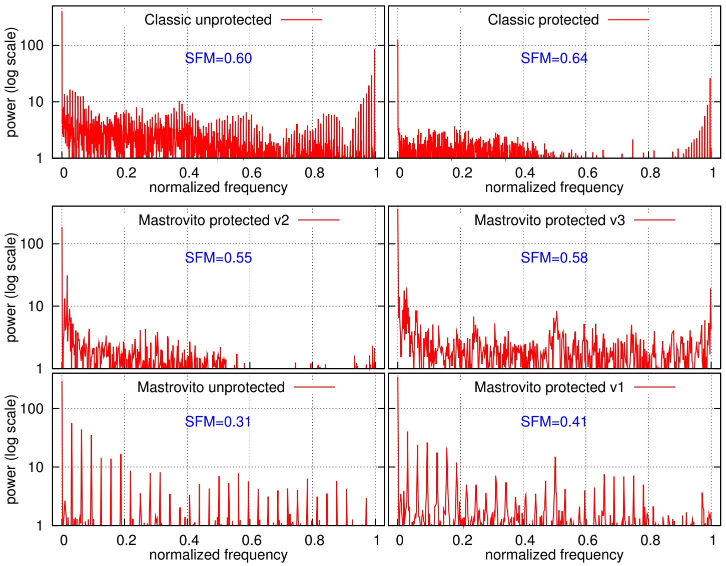


Mastrovito protected multiplier:



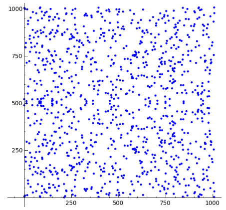
$\mathrm{GF}(2^m)$ Multipliers with Reduced Activity Variations (3/3)

FFT and spectral flatness measure (SFM) analysis:



Reference: [8] D. Pamula & A. Tisserand. WAIFI 2012.

Typical ECC Computations



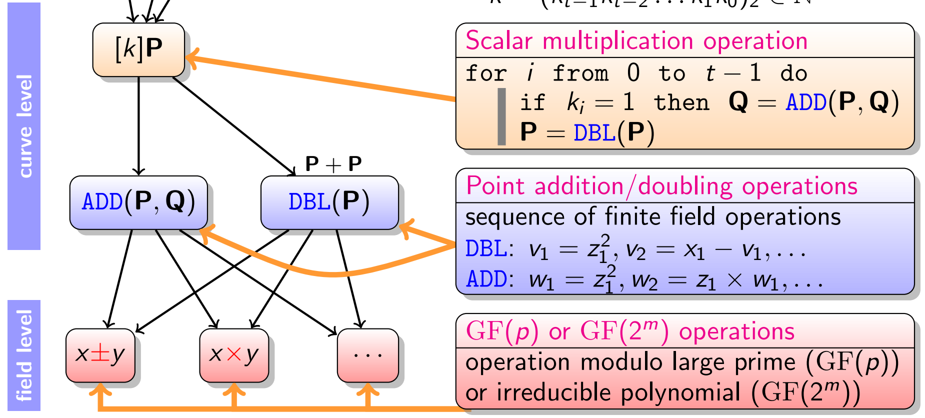
$E : y^2 = x^3 + 4x + 20$ over $\mathrm{GF}(1009)$

points on E: $\mathbf{P}$, $\mathbf{Q}$= (x, y) or (x, y, z)

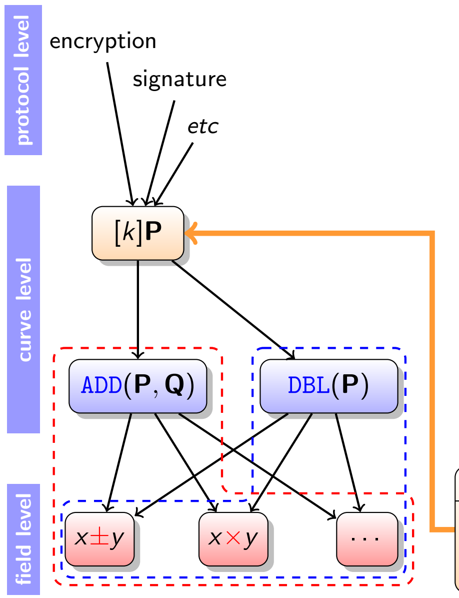
coordinates: $x, y, z \in \mathrm{GF}(\cdot)$

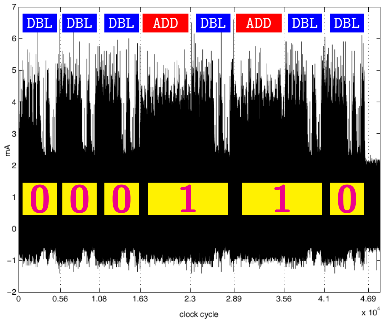
$\mathrm{GF}(p)$, $\mathrm{GF}(2^m)$, t : 160–600 bits

$k = (k_{t-1}k_{t-2} \dots k_1k_0)_2 \in \mathbb{N}$



Basic Power Analysis Attack on ECC

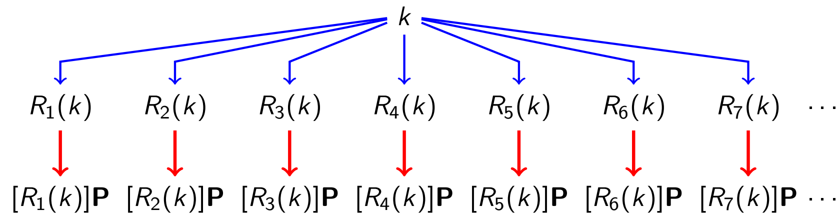




Arithmetic Level Countermeasures

Redundant number system =

- a way to improve the performance of some operations
- a way to represent a value with different representations



Important property: $\forall i \quad [R_i(k)]\mathbf{P} = [k]\mathbf{P}$

Proposed solution: use random redundant representations of k

Double-Base Number System

Standard radix-2 representation:

$$k = \sum_{i=0}^{t-1} k_i 2^i = \boxed{k_{t-1} \,|\, k_{t-2} \,|\, \cdots \,|\, k_2 \,|\, k_1 \,|\, k_0}$$

2^{t-1}	2^{t-2}	$\cdots$	2^2	2^1	2^0	implicit weights
k_{t-1}	k_{t-2}	$\cdots$	k_2	k_1	k_0	t explicit digits

Digits: $k_i \in \{0, 1\}$, typical size: $t \in \{160, \ldots, 600\}$

Double-Base Number System (DBNS):

$$k = \sum_{j=0}^{n-1} k_j 2^{a_j} 3^{b_j} =$$

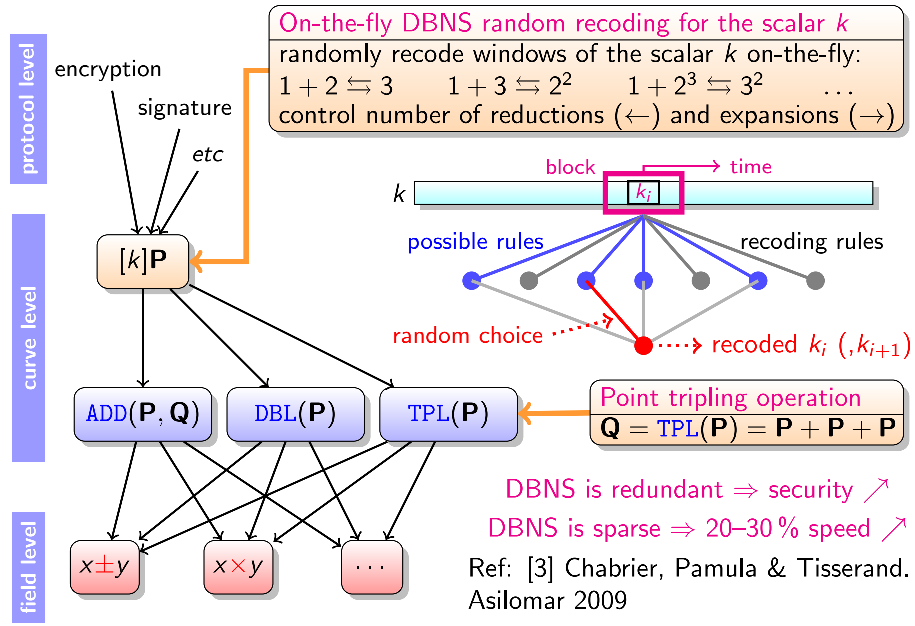
k_{n-1}	$\cdots$	k_1	k_0	n (2, 3)−terms
a_{n-1}	$\cdots$	a_1	a_0	explicit "digits"
b_{n-1}	$\cdots$	b_1	b_0	explicit ranks

$a_j, b_j \in \mathbb{N}$, $k_j \in \{1\}$ or $k_j \in \{-1, 1\}$, size $n \approx \log t$

DBNS is a very redundant and sparse representation: $1701 = (11010100101)_2$

$$\begin{aligned} 1701 &= 243 + 1458 &= 2^0 3^5 + 2^1 3^6 &= (1, 0, 5), (1, 1, 6) \\ &= 1728 - 27 &= 2^6 3^3 - 2^0 3^3 &= (1, 6, 3), (-1, 0, 3) \\ &= 729 + 972 &= 2^0 3^6 + 2^2 3^5 &= (1, 0, 6), (1, 2, 5) \\ &\ldots \end{aligned}$$

Randomized DBNS Recoding of the Scalar k



DBNS is redundant ⇒ security ↗

DBNS is sparse ⇒ 20–30 % speed ↗

Ref: [3] Chabrier, Pamula & Tisserand. Asilomar 2009

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 = *func*(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.
IEEE Transactions on Circuits and Systems I, 57(2):355–367, February 2010.

H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan.
The sorcerer's apprentice guide to fault attacks.
Proceedings of the IEEE, 94(2):370–382, February 2006.

T. Chabrier, D. Pamula, and A. Tisserand.
Hardware implementation of DBNS recoding for ECC processor.
In *Proc. 44rd Asilomar Conference on Signals, Systems and Computers*, pages 1129–1133, Pacific Grove, California, U.S.A., November 2010. IEEE.

P. C. Kocher.
Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems.
In *Proc. Advances in Cryptology (CRYPTO)*, volume 1109 of *LNCS*, pages 104–113. Springer, August 1996.

P. C. Kocher, J. Jaffe, and B. Jun.
Differential power analysis.
In *Proc. Advances in Cryptology (CRYPTO)*, volume 1666 of *LNCS*, pages 388–397. Springer, August 1999.

References II

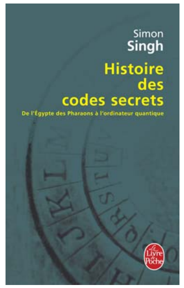
F. Koeune and F.-X. Standaert.
A tutorial on physical security and side-channel attacks.
In *5th International School on Foundations of Security Analysis and Design (FOSAD)*, volume 3655 of *LNCS*, pages 78–108. Springer-Verlag, 2005.

L. Lin and W. Burleson.
Leakage-based differential power analysis (LDPA) on sub-90nm CMOS cryptosystems.
In *Proc. IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 252–255, Seattle, WA, USA, May 2008.

D. Pamula and A. Tisserand.
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)

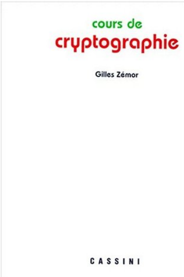
Histoire des codes secrets
Simon Singh
1999
Livre de poche



Mathématiques, espionnage et piratage informatique
Joan Gomez
2010
Le monde est mathématique, RBA

Good Books (in French)

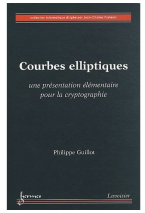
Cryptographie appliquée
Bruce Schneier
1997, 2ème édition
Wiley
ISBN: 2–84180–036–9



Cours de cryptographie
Gilles Zémor
2000
Cassini
ISBN: 2–84225–020–6

Good Books (in French)

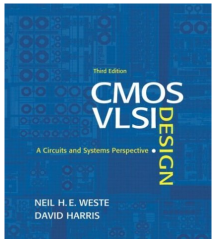
Courbes elliptiques
Philippe Guillot
2010
Hermes
ISBN: 978-2-7462-2392-9

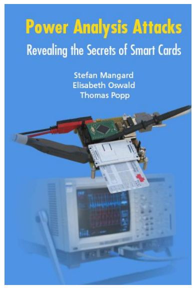


Micro et nano-électronique
Bases, Composants, Circuits
Hervé Fanet
2006
Dunod
ISBN: 2–10–049141–5

Good Books (in English)

CMOS VLSI Design
A Circuits and Systems Perspective
Neil Weste and David Harris
3rd edition, 2004
Addison Wesley
ISBN: 0–321–14901–7

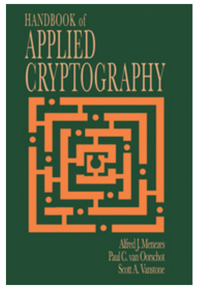




Power Analysis Attacks
Revealing the Secrets of Smart Cards
Stefan Mangard, Elisabeth Oswald and Thomas Popp
2007
Springer
ISBN:978-0-387-30857-9

Good Books (in English)

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