Fault Attacks on Electronic Circuits

Jean-Luc DANGER, Sylvain GUILLEY

<jean-luc.danger@telecom-paristech.fr>

Institut TELECOM / TELECOM ParisTech

1. Introduction
   - Presentation Outline
   - Physical Faults
2. Fault Induction Attacks: FA and DFA on RSA & DES
   - The Differential Fault Attack
   - Faults Models and Tolerance
3. DFA on AES
   - Theoretical Fault Attacks
   - Practical Attacks
   - Fault Sensitivity Analysis (FSA)
4. Countermeasures
   - Generic

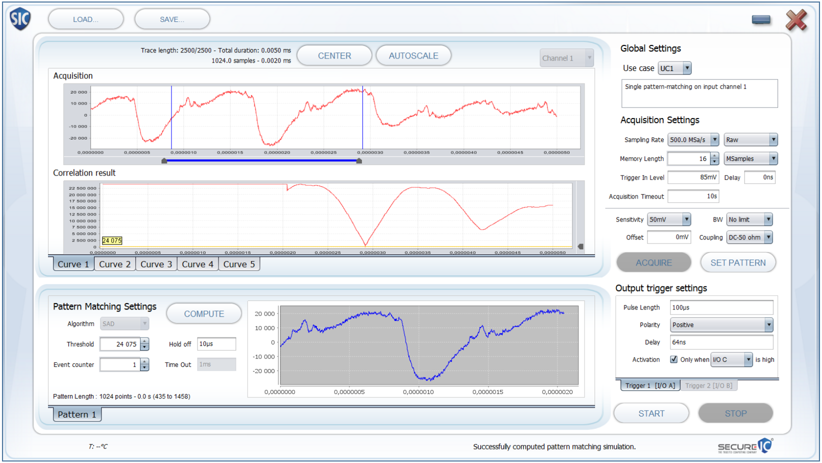
How Attackers Actually Inject Faults

- **Glitch** Attacks on the Power or the Clock (synchronous circuits)
- High Energy **Particles**. However, they can be replaced by:
- Focused **Laser** (spot Ø ~ 1 μm), front-side or back-side
- Using **bugged** HW/SW Components (Intel ® Pentium flawed floating point division, back to 1994)
- Eddy currents $\approx$ **EMI** (ElectroMagnetic Injection)
- etc.

See also: Fault Diagnosis and Tolerance in Cryptography (FDTC)

FDTC 2015
Fault Diagnosis and
Tolerance in Cryptography

Realignment



Trace length: 2500/2500 - Total duration: 0.0050 ms
1024.0 samples - 0.0020 ms

Pattern Matching Settings

Algorithm: SAD
Threshold: 24 075
Hold off: 10µs
Event counter: 1
Time Out: 1ms

Pattern Length : 1024 points - 0.0 s (435 to 1458)

Global Settings

Use case: UC1

Single pattern-matching on input channel 1

Acquisition Settings

Sampling Rate: 500.0 MSa/s — Raw
Memory Length: 16 — MSamples
Trigger In Level: 85mV — Delay: 0ns
Acquisition Timeout: 10s
Sensitivity: 50mV — BW: No limit
Offset: 0mV — Coupling: DC-50 ohm

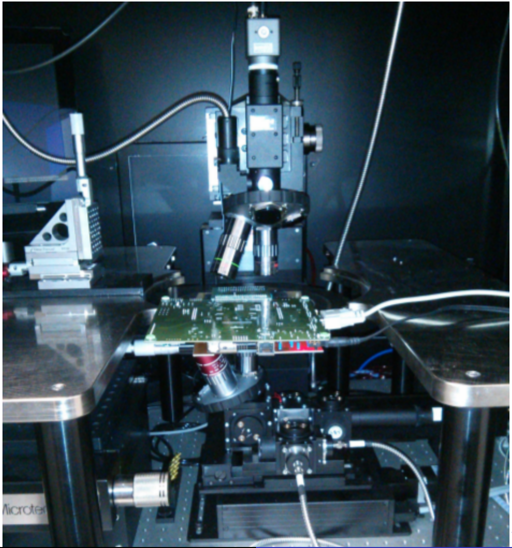
Output trigger settings

Pulse Length: 100µs
Polarity: Positive
Delay: 64ns
Activation: ☑ Only when I/O C is high

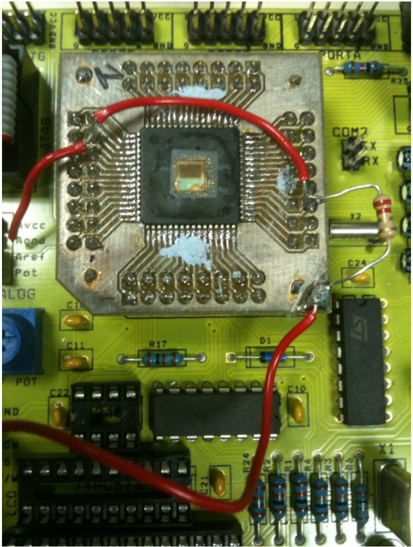
Successfully computed pattern matching simulation.

[WISTP ’11, Guilley et al.] [GKLD11]

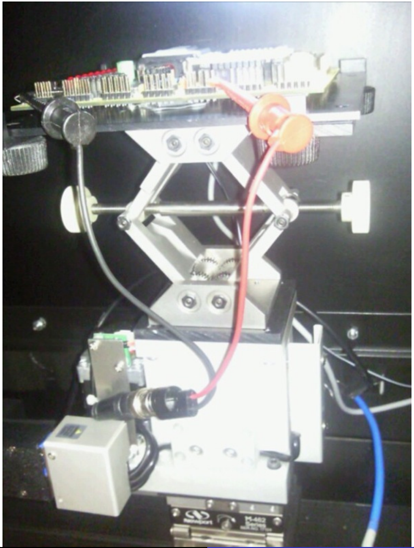
Laser station



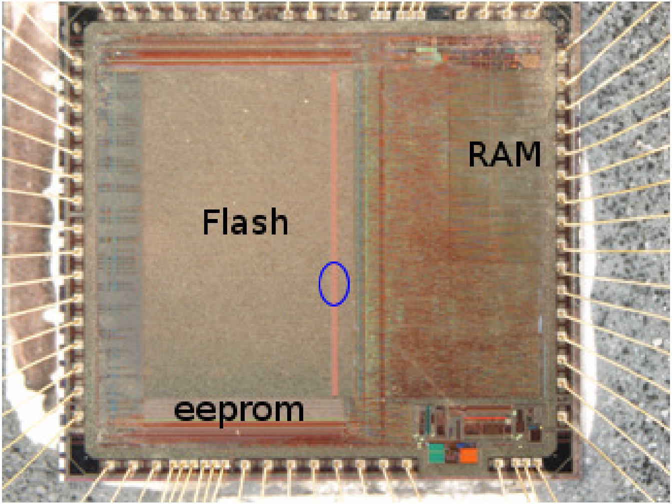
[1/3] Example @ TELECOM-ParisTech . . . . PCB



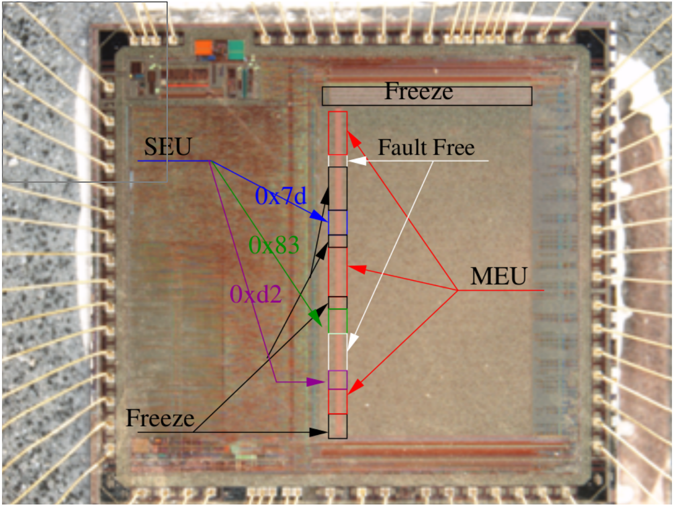
[2/3] Example @ TELECOM-ParisTech .... Setup



[3/3] Example @ TELECOM-ParisTech . . . . ASIC



[3/3] Example @ TELECOM-ParisTech . . . . ASIC

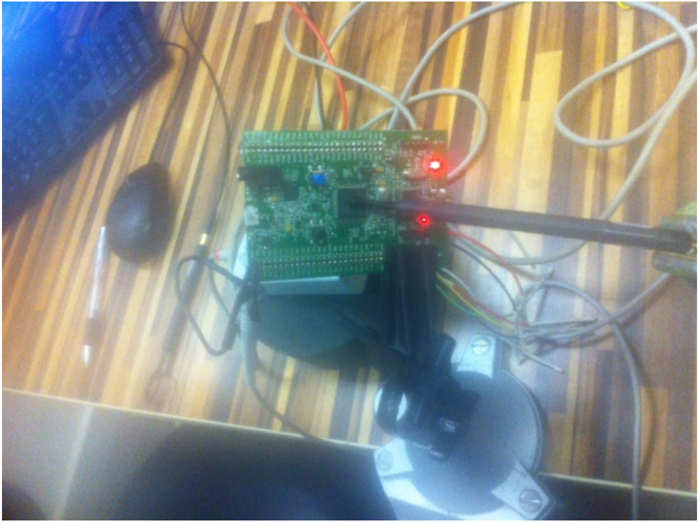


EMI disturbance system

Development System for Distubance Immunity E1
LANGER
EMV-Technik
SGZ 21
Search for fault locations with special field sources
Disturbance current injection
Location of points of fault inside the device

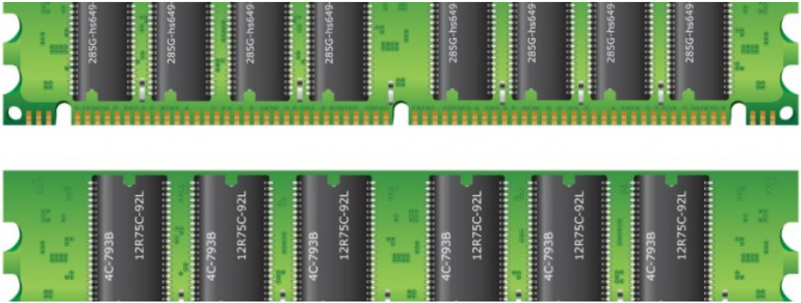
Example of setup for EMI

Example of setup for EMI

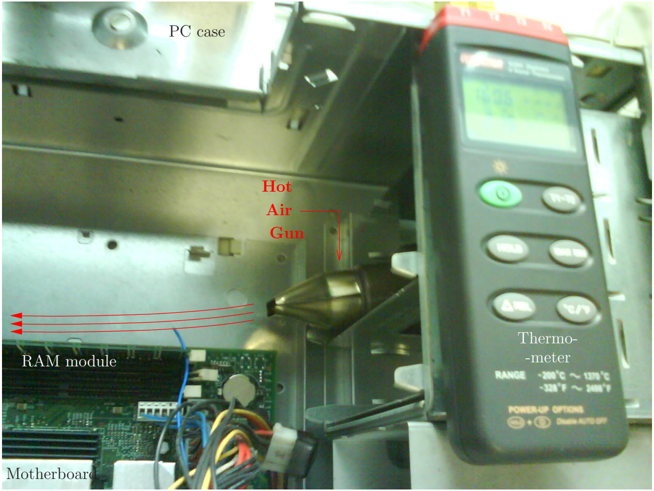


Flipping Bits in Memory Without Accessing Them

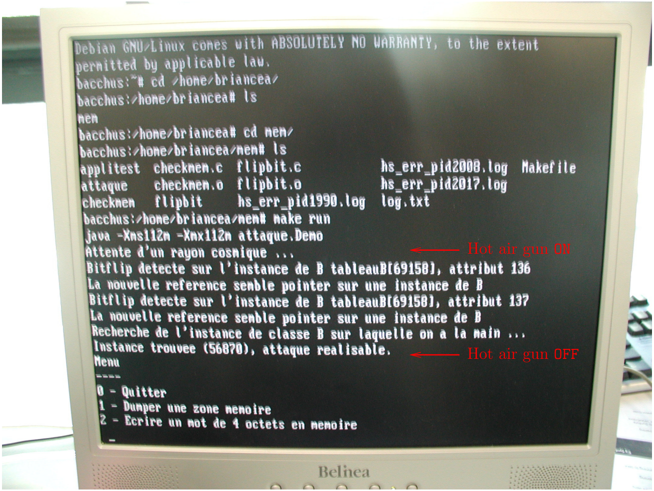
http://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf [KDK+14] — RowHammer.



Other faults on the RAM [Ver06]



Other faults on the RAM [Ver06]



```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
bacchus:~# cd /home/briancea/
bacchus:/home/briancea# ls
mem
bacchus:/home/briancea# cd mem/
bacchus:/home/briancea/mem# ls
applitest  checkmem.c  flipbit.c              hs_err_pid2008.log  Makefile
attaque    checkmem.o  flipbit.o              hs_err_pid2017.log
checkmem   flipbit     hs_err_pid1990.log     log.txt
bacchus:/home/briancea/mem# make run
java -Xms112m -Xmx112m attaque.Demo
Attente d'un rayon cosmique ...
Bitflip detecte sur l'instance de B tableauB[69158], attribut 136
La nouvelle reference semble pointer sur une instance de B
Bitflip detecte sur l'instance de B tableauB[69158], attribut 137
La nouvelle reference semble pointer sur une instance de B
Recherche de l'instance de classe B sur laquelle on a la main ...
Instance trouvee (56870), attaque realisable.
Menu
----
0 - Quitter
1 - Dumper une zone memoire
2 - Ecrire un mot de 4 octets en memoire
_
```

← Hot air gun ON

← Hot air gun OFF

The So-Called "Bellcore" Attack

Bellcore = Bell Communications Research

- Three employees of Bellcore (and Pr. @ Stanford) find an attack that breaks RSA by injecting a single fault.
- Reference: "*On the importance of checking cryptographic protocols for faults*". by D. Boneh, R. DeMillo, and R. Lipton. Journal of Cryptology, Springer-Verlag, Vol. 14, No. 2, pp. 101–119, 2001. Extended abstract in Proceedings of Eurocrypt'97, Lecture Notes in Computer Science, Vol. 1233, Springer-Verlag, pp. 37–51, 1997.
- http://crypto.stanford.edu/~dabo/papers/faults.ps.gz

Bellcore attack against RSA signatures with CRT

- Signature S of message x: $S \doteq x^d \mod N$, with $N = p \cdot q$.
- Using Chinese Remainder Theorem (CRT), the signature can be simplified as:
  - $S_1 = x^{d \mod (p-1)} \mod p$ and
  - $S_2 = x^{d \mod (q-1)} \mod q$, both operations working on half bitwidth.
- The signature is obtained back using the two constants:

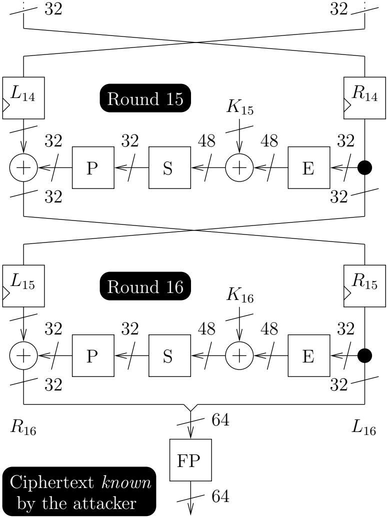
$$\left\{\begin{array}{lcll} a & = & 0 & \mod q \\ a & = & 1 & \mod p \end{array}\right. \quad \text{and} \quad \left\{\begin{array}{lcll} b & = & 1 & \mod q \\ b & = & 0 & \mod p \end{array}\right.$$

- $S = a \cdot S_1 + b \cdot S_2 \mod N$.
- Now, if S_1 happens to be faulty: $S_1 \rightarrow \widehat{S_1}$ for whatever reason,
- $\gcd(S - \widehat{S}, N) = \gcd(a \cdot (S_1 - \widehat{S_1}), N) = q$.

The *Almost Universal* Differential Fault Attack

- Bellcore attack targets public key cryptosystems
  - It needs algebraic properties to work
- DFA targets *almost whatever* algorithm (*known* or even *unknown*)
  - It works on complex bit operations, such as the ones involved in secret key cryptography
  - It is demonstrated on DES
- Reference: “Differential Fault Analysis of Secret Key Cryptosystems”, by Eli Biham, Adi Shamir, CRYPTO 1997, LNCS 1294, pp. 513–525.

DFA Attack Setting



Ciphertext *known* by the attacker

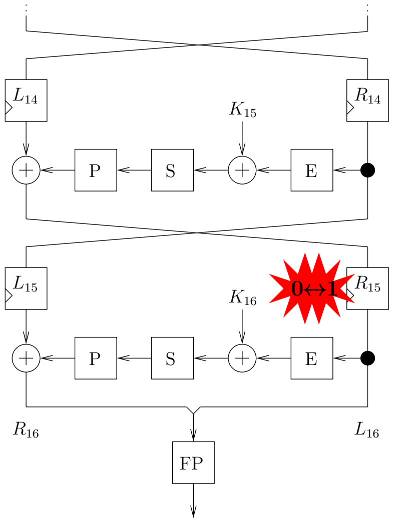
DFA Assumptions

- Unrolled implementation.
- Single bit-flips on any right register R_i, for $i \in [1, 16]$.
- Ciphertext-*only* attack.

DES Properties

- All the DES constitutive boxes, but the S, are linear: $f(x \oplus a) = f(x) \oplus f(a)$, for $f \in \{\mathrm{Id}, \mathrm{P}, \mathrm{E}, \mathrm{FP}\}$.
- $L_{16} = R_{15}$.

One Fault Occurs in R_{15}



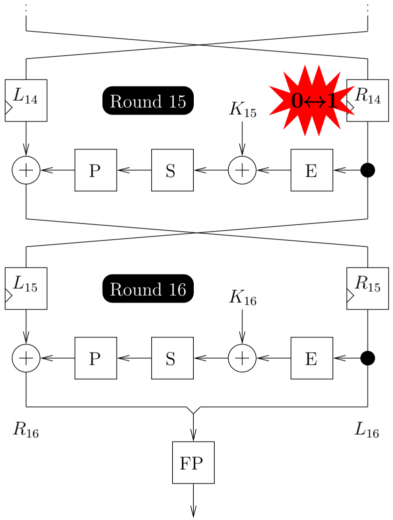
What Has Happened?

Bit $b \in [1, 32]$ of R_{15} is flipped.

Attack Scenario

- Find b by looking in L_{16}.
- Deduce which S_i, $i \in [1, 8]$, (there can be two of them) has output a wrong value.
- Solve the equation couple:
$$\begin{cases} R_{16} = L_{15} \oplus \mathsf{S}_i(K_{16} \oplus R_{15}), \\ \tilde{R}_{16} = L_{15} \oplus \mathsf{S}_i(K_{16} \oplus \tilde{R}_{15}). \end{cases}$$
- It has ≈ four 6-bit solutions.

One Fault Occurs in R_{14}



What Has Happened?

Bit $b \in [1, 32]$ of R_{14} is flipped.

Attack Scenario

- Previous attack on R_{15} allowed a straightforward subkey K_{16} retrieval at the input of $(b-1)/8^{\text{th}}$ S-box.
- Current attack requires a differential analysis of the last two rounds of DES.
- Details to come. . .

Solving the "R_{14} bit flip" plot (1/2)

Notations

- Tilded symbols, *e.g.* $\tilde{L_{16}}$, denote faulted quantities.
- $R_{14} \oplus \tilde{R_{14}} = 00 \cdots 010 \cdots 00 \doteq \mathbb{1}_b$, the "1" lying at position b.

Which bit b was flipped?

- Notice that $\Delta \doteq L_{16} \oplus \tilde{L_{16}}$ is also the difference at the output of S, at round 15.
- For each S-box i, $S_i(x) \oplus S_i(x \oplus \mathbb{1}_b) = \Delta$, x being the unknown value $(R_{14} \oplus K_{15})\,[8{\cdot}i, 8{\cdot}(i+1)[$, has few solutions b.
- Validate potential b by verifying that Δ passed through S, at round 16, can generate the difference $R_{16} \oplus \left(\tilde{R_{16}} \oplus \mathbb{1}_b\right)$.

Solving the "R_{14} bit flip" plot (2/2)

Retrieving Information on K_{16} subkey

- Now that flipped bit b in R_{14} is known, the differences *before* and *after* S-boxes in round 16 are known.
- This property allows to eliminate many subkeys K_{16} 6-bit parts at the input of activated S-boxes (6 out of 8.)

Attack Extension

- Basically the same differential attack can be used if the error occurs in round 14 (*but not higher. . .*).
- Not surprisingly, Eli Biham and Adi Shamir, inceptors of the DFA, are also the fathers of the *differential cryptanalysis*.
  - ↦ *"Differential Cryptanalysis of the Full 16-Round DES", CS 708, December 1991, Proceedings of Crypto'92, LNCS 740.*

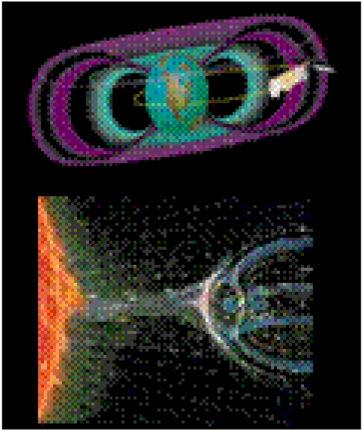
The DFA Efficiency

A Powerful Attack!

- According to authors, between 50 and 200 faults on whatever round are required to fully expose the last round subkey.
- Once K_{16} is known, the key K can be retrieved by an exhaustive search attacks on the $56 - 48 = 8$ remaining bits.

Generalization

- If K_{16} is known, the DFA can be applied to the 15-round DES variant. . .
- The rounds are peeled off (and detected faults corrected).
- Thus, Triple-DES and DES with independent subkeys (768 bit) can be attacked.



Data courtesy of the MARS project.

↦ http://www.comelec.enst.fr/recherche/mars/

Single Event Effects (SEE)

SET: Single Event Transient Fault.

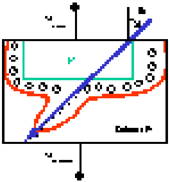
SEU: Single Event Upsets. Transient Fault. Memory point inversion by current peak (soft error) It was the fault model of the DFA.

SEL: Single Event Latchups. Short-circuit between `Vss` and `Vdd`, causing a permanent fault (hard error)

SEUs Can Be Modeled at Various Levels

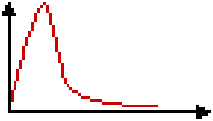
Physical

Creation of e^-/h^+ pairs.



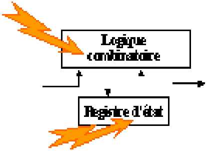
Electrical

Current or voltage pulse.



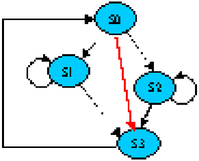
Logical

Bit flips, signal inversion.

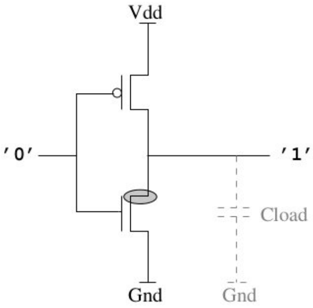


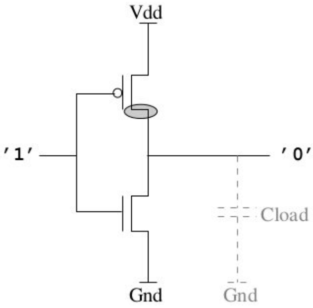
Behavioral

Erroneous transitions.

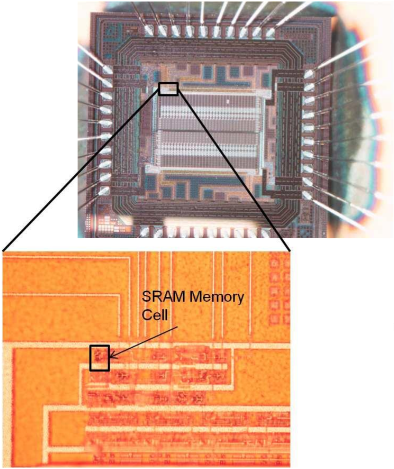


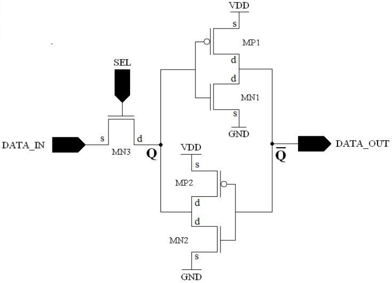
Observable impacts on an inverter



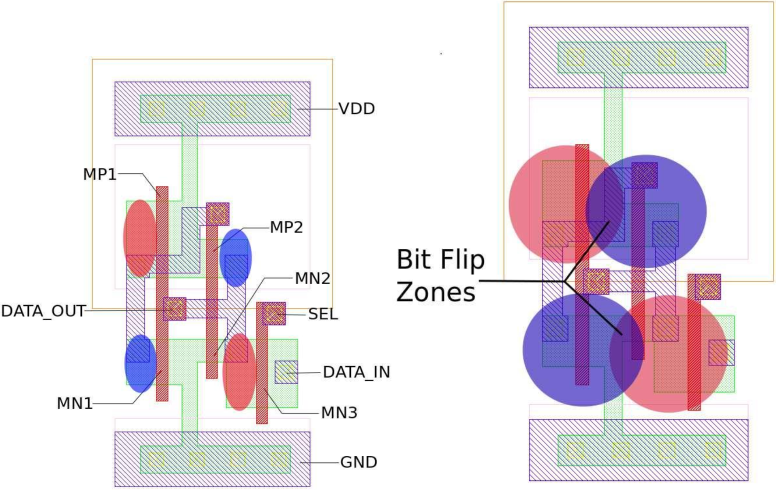


SRAM cell (two inverters)

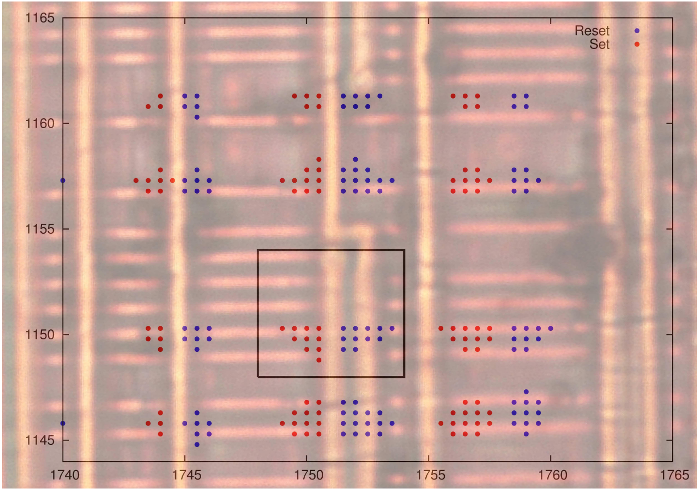




Laser beam impact (if '1', → 0 / if '0', → 1)



Laser cartography



State-of-the-Art of Fault Attacks against AES

- Giraud in 2003: (50 faults) [Gir04]
- Dusart, Letourneux & Vivolo in 2002: (5×4 faults) [DLV03]
- Piret & Quisquater in 2004: 2 faults [PQ03]
- Tunstall, Mukhopadhyay & Ali: 1 fault [TMA11]

Ch. Giraud in 2003

Bit-fault e_j attack on the last round

Regular encryption (C):

- $C_{\texttt{ShiftRow}(i)} = \texttt{SubBytes}(M_i^9) \oplus K^{10}_{\texttt{ShiftRow}(i)}$ for $i \in [1, 16]$

Faulted encryption (D):

- $D_{\texttt{ShiftRow}(i)} = \texttt{SubBytes}(M_i^9) \oplus K^{10}_{\texttt{ShiftRow}(i)}$ for $i \in [1, 16] \backslash \{j\}$ and
- $C_{\texttt{ShiftRow}(j)} = \texttt{SubBytes}(M_j^9 \oplus e_j) \oplus K^{10}_{\texttt{ShiftRow}(j)}$.

Attack:

- $C_{\texttt{ShiftRow}(j)} \oplus D_{\texttt{ShiftRow}(j)} = \texttt{SubBytes}(M_j^9) \oplus \texttt{SubBytes}(M_j^9 \oplus e_j)$.

Detail of Ch. Giraud's attack

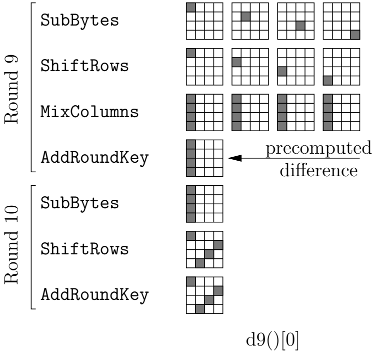
Goal: finding the value of M_j^9.

- $C_{\texttt{ShiftRows}(j)} \oplus D_{\texttt{ShiftRows}(j)} = \Delta = SubBytes(M_j^9) \oplus SubBytes(M_j^9 \oplus e_j)$ has between 2 and 14 solutions in (e_j, M_j^9) (set of 8×2^8 unknown), and 8 in average.
- However, the exact value of e_j is of no importance.

Attack Strength

- Thus, with 2 faults, there is 50 % chance to get one M_j^9.
- With 3 faults, there is 97 % chance to get one M_j^9.
- Once M_j^9 is known, we have $K_j^{10} = C_j \oplus SubBytes(M_j^9)$.

G. Piret & J.-J. Quisquater in 2003



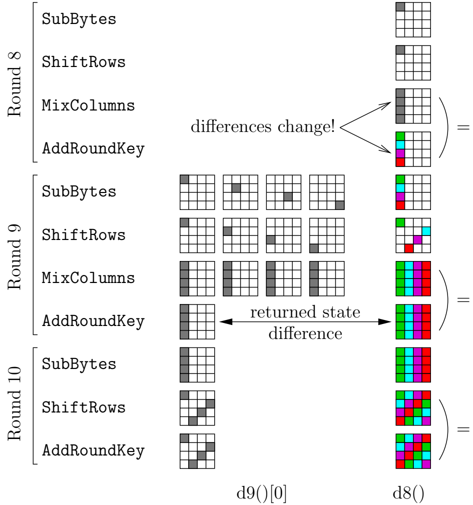
One faulty Byte at round 9 generates 4 faulty Bytes at the output

255x4 candidates for K_{10}

2 faults ⇒ 98%

8 faults ⇒ 100%

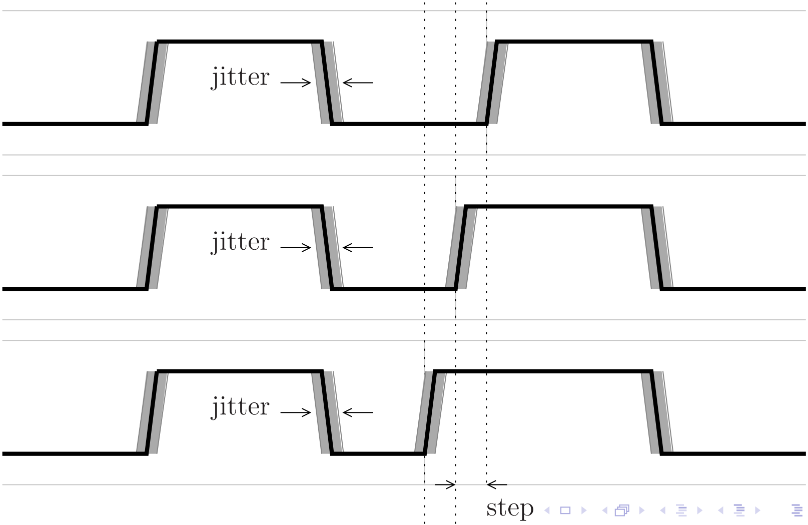
G. Piret & J.-J. Quisquater in 2003



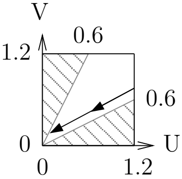
Kill 4 birds with one stone

A fault at round 8 yields 4 faults at round 9! This is optimal. . .

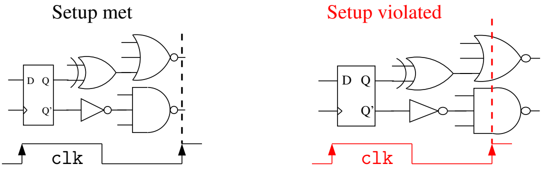
Faults injection: Local Over-Clocking



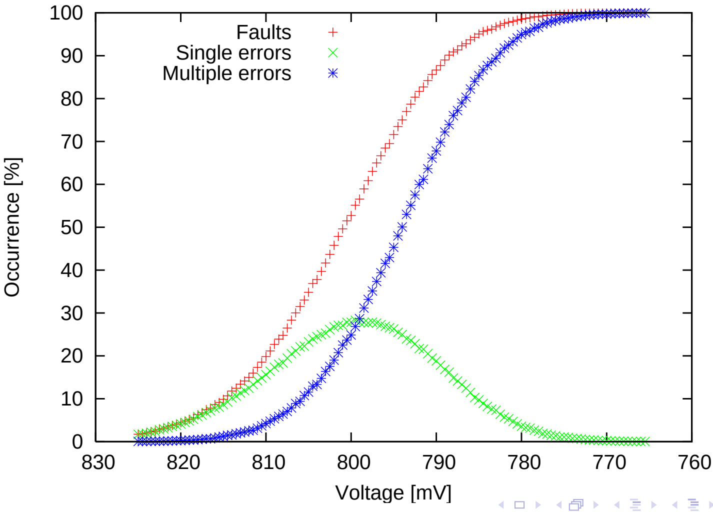
Faults injection: Setup-Time Violation Attack Sketch



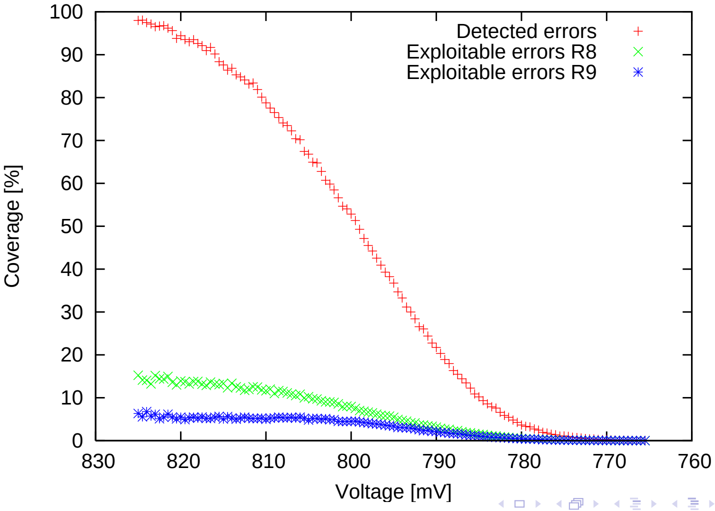
$$\boxed{V \downarrow \;\Rightarrow\; T_{\text{propagation}} \uparrow}$$



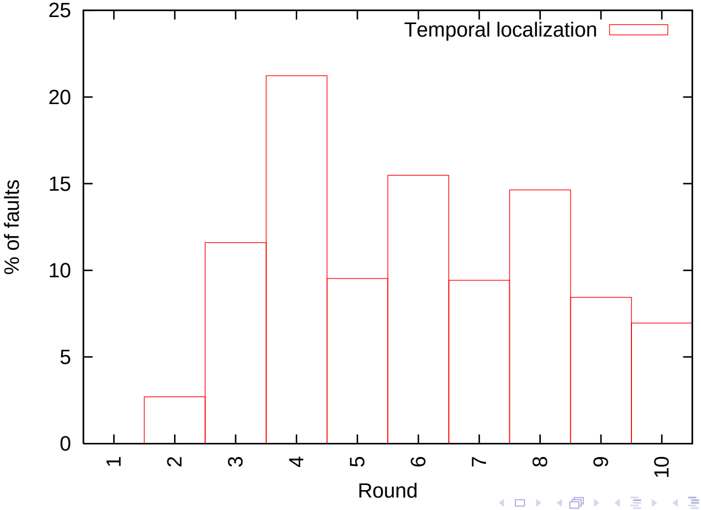
Occurrence (*nominal voltage is 3.3 V*)



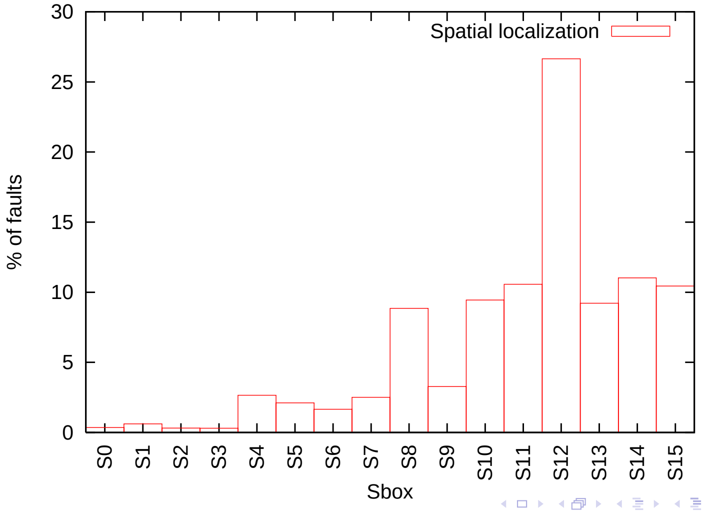
Coverage


Detected errors +
Exploitable errors R8 ×
Exploitable errors R9 ✳
Coverage [%]
100
90
80
70
60
50
40
30
20
10
0
830
820
810
800
790
780
770
760
Voltage [mV]

Round statistics



Sbox statistics



FSA: Principle [LSG+10]

- The stress level at which a fault occurs...
- ... might be related to the computed value.

- Ex: any combinational circuit
- Ex: DPL circuit with early evaluation (e.g. WDDL)
- Ex: Key-dependent clock-wise collisions [NLS+12]

Redundance

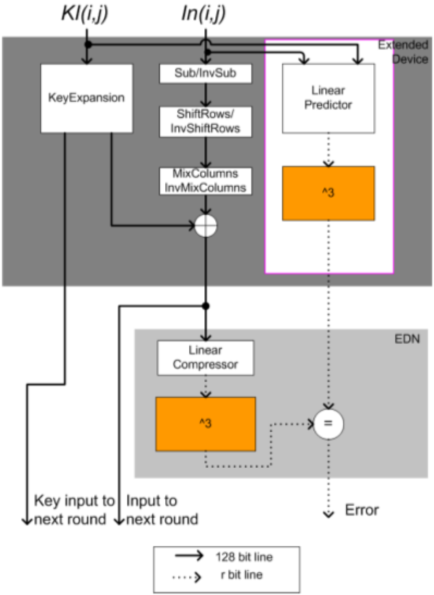
- Time
- Space
- Information

Authenticated encryption is one protocol-level solution (see CAESAR competition).

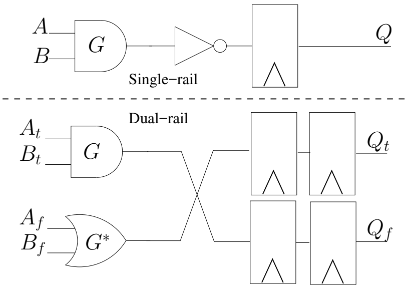
Resilience

- Let the system output erroneous errors, as long as they convey no information about the internal sensitive values [GSDS10]

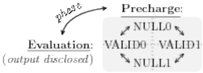
Redundance in information [KKT04]



DPL overview

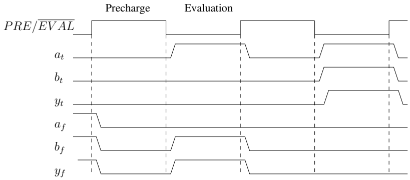


2 Networks: T and F


phase

Precharge:
NULL0
VALID0 VALID1
NULL1

Evaluation:
(output disclosed)

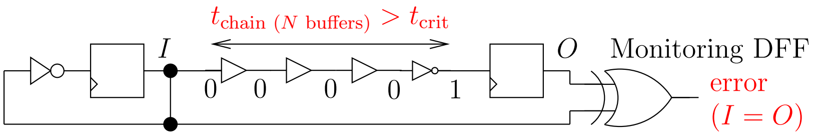


2 phases

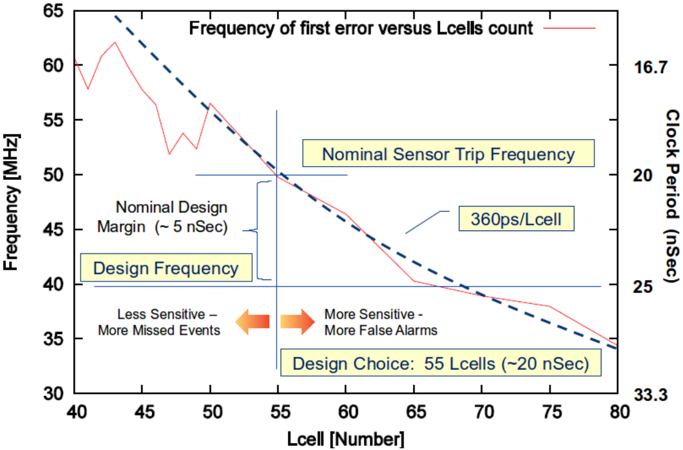
Digital Sensor

IET Inf. Secur., 2011, Vol. 5, Iss. 4, pp. 181–190
doi: 10.1049/iet-ifs.2010.0238

[SBGD11]

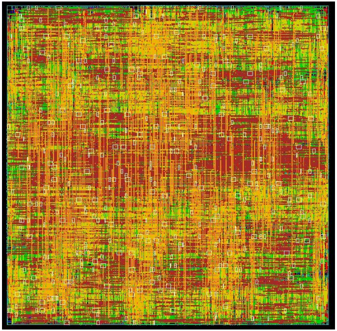


Design Example: Frequency Sensitivity



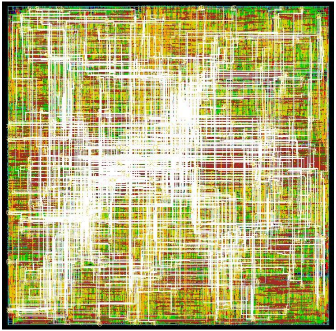
2. Main technical characteristics

- Digital, hence:
  - **Simple API**
  - **Stable**
  - **Small**
  - **Discreet, more difficult to recognize**



2. Main technical characteristics

- Digital, hence:
  - **Simple API**
  - **Stable**
  - **Small**
  - **Discreet, more difficult to recognize**
  - **Melted within the rest of the SoC, more difficult to by-pass**



A protection against instruction-skip attacks

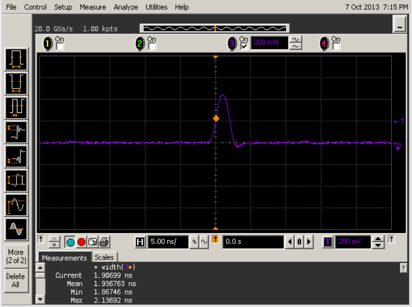
Instruction skip attacks and protection [HMER13, MHER14]

- One instruction can be skipped
- Replacement sequences for idempotent instructions:

Instruction	Description	Replacement
`mov r1,r8`	Copies `r8` into `r1`	`mov r1,r8` `mov r1,r8`
`ldr r1,[r8,r2]`	Loads the value at the address `r8+r2` into `r1`	`ldr r1,[r8,r2]` `ldr r1,[r8,r2]`
`str r3,[r2,#10]`	Stores `r3` at the address `r2+10`	`str r3,[r2,#10]` `str r3,[r2,#10]`
`add r3,r1,r2`	Puts `r1+r2` into `r3`	`add r3,r1,r2` `add r3,r1,r2`

Fault injection [RG14, Appendix 2.A]

- Pulse amplitude: . . . 0 – 500 mV.
- Pulse duration: . . . . 2 ns.
- Repeatability: . . . . 500 MHz.



```
+ width(3)
Current   1.90699 ns
   Mean   1.936763 ns
    Min   1.86746 ns
    Max   2.13692 ns
```

A protection against instruction-skip attacks

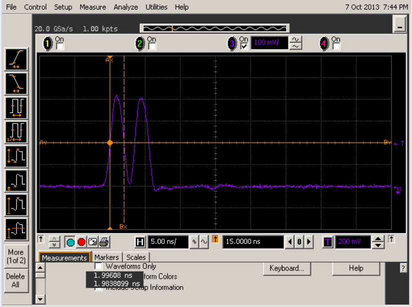
Instruction skip attacks and protection [HMER13, MHER14]

- One instruction can be skipped
- Replacement sequences for idempotent instructions:

Instruction	Description	Replacement
`mov r1,r8`	Copies `r8` into `r1`	`mov r1,r8` `mov r1,r8`
`ldr r1,[r8,r2]`	Loads the value at the address `r8+r2` into `r1`	`ldr r1,[r8,r2]` `ldr r1,[r8,r2]`
`str r3,[r2,#10]`	Stores `r3` at the address `r2+10`	`str r3,[r2,#10]` `str r3,[r2,#10]`
`add r3,r1,r2`	Puts `r1+r2` into `r3`	`add r3,r1,r2` `add r3,r1,r2`

Fault injection [RG14, Appendix 2.A]

- Pulse amplitude: . . . 0 – 500 mV.
- Pulse duration: . . . . 2 ns.
- Repeatability: . . . . 500 MHz.



1.99608 ns
1.9838099 ns

A protection against instruction-skip attacks

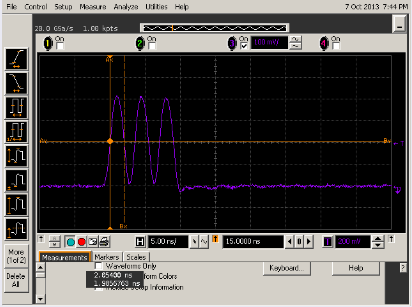
Instruction skip attacks and protection [HMER13, MHER14]

- One instruction can be skipped
- Replacement sequences for idempotent instructions:

Instruction	Description	Replacement
`mov r1,r8`	Copies `r8` into `r1`	`mov r1,r8` `mov r1,r8`
`ldr r1,[r8,r2]`	Loads the value at the address `r8+r2` into `r1`	`ldr r1,[r8,r2]` `ldr r1,[r8,r2]`
`str r3,[r2,#10]`	Stores `r3` at the address `r2+10`	`str r3,[r2,#10]` `str r3,[r2,#10]`
`add r3,r1,r2`	Puts `r1+r2` into `r3`	`add r3,r1,r2` `add r3,r1,r2`

Fault injection [RG14, Appendix 2.A]

- Pulse amplitude: . . . 0 – 500 mV.
- Pulse duration: . . . . 2 ns.
- Repeatability: . . . . 500 MHz.



```
2.05400 ns
1.9856763 ns
```

EM pulses should not be too long!

References on Fault Attacks I

[DLV03] Pierre Dusart, Gilles Letourneux, and Olivier Vivolo.
Differential Fault Analysis on A.E.S.
In Jianying Zhou, Moti Yung, and Yongfei Han, editors, *ACNS*, volume 2846 of *LNCS*, pages 293–306. Springer, 2003.

[Gir04] Christophe Giraud.
DFA on AES.
In Hans Dobbertin, Vincent Rijmen, and Aleksandra Sowa, editors, *AES Conference*, volume 3373 of *Lecture Notes in Computer Science*, pages 27–41. Springer, 2004.

[GSDS10] Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, and Nidhal Selmane.
Fault Injection Resilience.
In *FDTC*, pages 51–65. IEEE Computer Society, August 21 2010. Santa Barbara, CA, USA. DOI: 10.1109/FDTC.2010.15; Complete version: `http://hal.archives-ouvertes.fr/hal-00482194/en/`.

References on Fault Attacks II

[HMER13] Karine Heydemann, Nicolas Moro, Emmanuelle Encrenaz, and Bruno Robisson.
Formal Verification of a Software Countermeasure Against Instruction Skip Attacks.
Cryptology ePrint Archive, Report 2013/679, 2013.
http://eprint.iacr.org/2013/679.

[KDK$^+$14] Yoongu Kim, Ross Daly, Jeremie Kim, Chris Fallin, Ji-Hye Lee, Donghyuk Lee, Chris Wilkerson, Konrad Lai, and Onur Mutlu.
Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors.
In *ACM/IEEE 41st International Symposium on Computer Architecture, ISCA 2014, Minneapolis, MN, USA, June 14-18, 2014*, pages 361–372. IEEE Computer Society, 2014.

[KKT04] Mark G. Karpovsky, Konrad J. Kulikowski, and Alexander Taubin.
Robust Protection against Fault Injection Attacks on Smart Cards Implementing the Advanced Encryption Standard.
In *DSN*, pages 93–101. IEEE Computer Society, June 28 – July 01 2004. Florence, Italy.

References on Fault Attacks III

[LSG+10] Yang Li, Kazuo Sakiyama, Shigeto Gomisawa, Toshinori Fukunaga, Junko Takahashi, and Kazuo Ohta.
Fault Sensitivity Analysis.
In *CHES*, volume 6225 of *Lecture Notes in Computer Science*, pages 320–334. Springer, August 17-20 2010.
Santa Barbara, CA, USA.

[MHER14] Nicolas Moro, Karine Heydemann, Emmanuelle Encrenaz, and Bruno Robisson.
Formal verification of a software countermeasure against instruction skip attacks.
J. Cryptographic Engineering, 4(3):145–156, 2014.

[NLS+12] Toshiki Nakasone, Yang Li, Yu Sasaki, Mitsugu Iwamoto, Kazuo Ohta, and Kazuo Sakiyama.
Key-Dependent Weakness of AES-Based Ciphers under Clockwise Collision Distinguisher.
In Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon, editors, *ICISC*, volume 7839 of *Lecture Notes in Computer Science*, pages 395–409. Springer, 2012.

References on Fault Attacks IV

[PQ03] Gilles Piret and Jean-Jacques Quisquater.
A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD.
In *CHES*, volume 2779 of *LNCS*, pages 77–88. Springer, September 2003. Cologne, Germany.

[RG14] Pablo Rauzy and Sylvain Guilley.
Formal Analysis of CRT-RSA Vigilant's Countermeasure Against the BellCoRe Attack.
In *3rd ACM SIGPLAN Program Protection and Reverse Engineering Workshop (PPREW 2014)*, January 25 2014.
San Diego, CA, USA. ISBN: 978-1-4503-2649-0.

[SBGD11] Nidhal Selmane, Shivam Bhasin, Sylvain Guilley, and Jean-Luc Danger.
Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks.
IET Information Security, 5(4):181–190, December 2011.
DOI: 10.1049/iet-ifs.2010.0238.

References on Fault Attacks V

[TMA11] Michael Tunstall, Debdeep Mukhopadhyay, and Subidh Ali.
Differential Fault Analysis of the Advanced Encryption Standard Using a Single Fault.
In Claudio Agostino Ardagna and Jianying Zhou, editors, *WISTP*, volume 6633 of *Lecture Notes in Computer Science*, pages 224–233. Springer, 2011.

[Ver06] Olli Vertanen.
Java Type Confusion and Fault Attacks.
In *FTDC*, volume 4236 of *LNCS*, pages 237–251. Springer, 2006.
DOI: 10.1007/11889700, ISSN 0302-9743 (Print) 1611-3349 (Online), ISBN 978-3-540-46250-7.