Institut
Mines-Télécom

Multi-Level Formal Analysis

A New Direction for Fault Injection Attack?

L. Sauvage, T. Graba, T. Porteboeuf

PROOFS – September 17, 2015

Presentation Outline

Introduction, Motivation

Multi-level Formal Verification by Example

Challenge Regarding EMI Modeling

Conclusion & Perspectives

Presentation Outline

Introduction, Motivation

Multi-level Formal Verification by Example

Challenge Regarding EMI Modeling

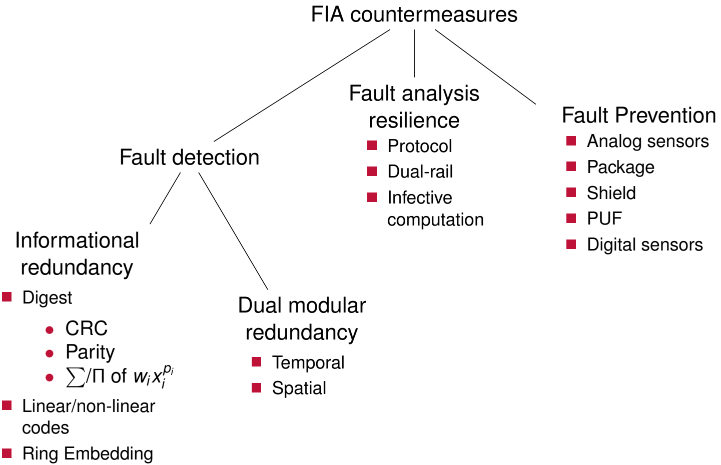
Conclusion & Perspectives

Simple & Differential Fault Analyses Are Powerful!

Number of faulted ciphertexts (C') to disclose the key

Algorithm	Key space	# C'	Fault model
RSA (CRT) [BDL97]	2^{1024}	1	Any @ S_p (or S_q)
RSA (L2R) [BDH+97]		3083	Bit error @ each S&M
DES [BS97, Riv09]	2^{56}	7	Bit error @ 12th round
		9	Byte error @ 12th round
AES [PQ03]	2^{256}	4	Byte error @ 8th round
ECDSA/P-192 [BBB+11]	2^{192}	36	Any in key d @ MULT

Protections Against FIA: a Classification



FIA countermeasures

Fault detection

Informational redundancy

- Digest
  - CRC
  - Parity
  - $\sum/\Pi$ of $w_i x_i^{p_i}$
- Linear/non-linear codes
- Ring Embedding

Dual modular redundancy

- Temporal
- Spatial

Fault analysis resilience

- Protocol
- Dual-rail
- Infective computation

Fault Prevention

- Analog sensors
- Package
- Shield
- PUF
- Digital sensors

Most countermeasures use fault detection with redundancy/check

A (Short) History of Shamir's Trick

$$S = \mathrm{CRT}(S_p, S_q) = S_q + q\Big(I_q\big(S_p - S_q\big) \bmod p\Big) \text{ with } \begin{cases} S_p = m^{d_p} & \bmod p, \\ S_q = m^{d_q} & \bmod q. \end{cases}$$

[Sha99]	Redundancy/check on S_p and S_q
[ABF$^+$02]	Redundancy/check on CRT
[YJ00]	Infective computation (no decisional test)
[YKM06]	Broken!
[KQ07]	2O-FIA attack and countermeasure
[DGRS09]	Broken! Counter-countermeasure
?	?

- Attacker underestimated: she can target operations, not only data.
- Highly time-consuming verification
  - All values (C_n^1, C_n^2, *etc.*)
  - All clock cycles
  - All order ?

Overhead of Some Countermeasures

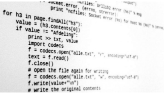
- Attacker overestimated: she can fault any bit (with SR $= 1$).
- Countermeasures designed to detect fault on 1+ bit
- All bits are considered, hence a high overhead

Reference	Algorithm	Countermeasure	Overhead	Non-detection
[BBK+03]	AES-128	Multiple parity bits	20 %	0.12
[KKT04]	AES-128	Partially robust code	80 %	2^{-32}
[AKS12]	ECC/P-192	Nonlinear robust code	114 %	2^{-128}

Actual Strategy

DFA

Secret extraction

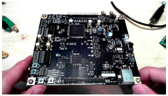


```
          socket.error, (errno, strerror):
               print "ncfiles: Socket error (%s) for host %s (%s)" % (errno,
for h3 in page.findAll("h3"):
    value = (h3.contents[0])
    if value != "Afdeling":
        print >> txt, value
        import codecs
        f = codecs.open("alle.txt", "r", encoding="utf-8")
        text = f.read()
        f.close()
        # open the file again for writing
        f = codecs.open("alle.txt", "w", encoding="utf-8")
        f.write(value+"\n")
        # write the original contents
```

Source (HDL/Soft) ← Countermeasure

01001101

Netlist/Inst. seq.



Platform (FPGA/SoC)

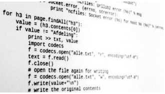
Disturbance

Proposal: Multi-Level Formal Analysis

DFA

Secret extraction

Faults properties



```
    socket.error, (errno, strerror):
        print "ncfiles: Socket error (%s) for host %s (%s)" % (errno,
for h3 in page.findAll("h3"):
    value = (h3.contents[0])
    if value != "Afdeling":
        print >> txt, value
        import codecs
        f = codecs.open("alle.txt", "r", encoding="utf-8")
        text = f.read()
        f.close()
        # open the file again for writing
        f = codecs.open("alle.txt", "w", encoding="utf-8")
        f.write(value+"\n")
        # write the original contents
```

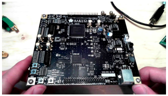
Source (HDL/Soft) ←

Countermeasure

01001101

Netlist/Inst. seq.

Delays/placement



Platform (FPGA/SoC)

Sensitivity

Disturbance

Accuracy

Principle: take into account characteristics of each level

Presentation Outline

Introduction, Motivation

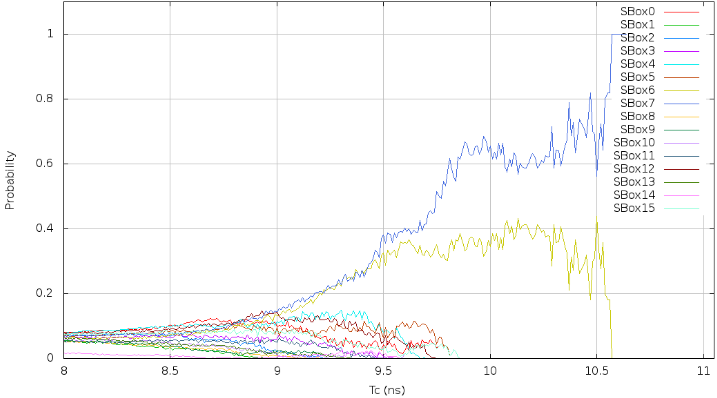
Multi-level Formal Verification by Example

Challenge Regarding EMI Modeling

Conclusion & Perspectives

Hardware Implementation of AES-128

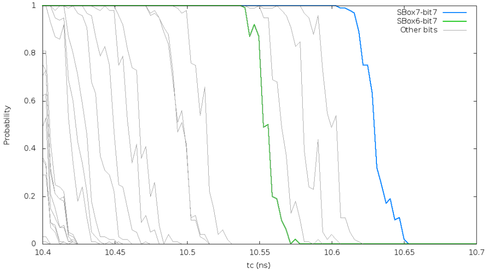
Probability to be faulted of each SBox



- $Tc = 10.64\,\text{ns}$: 1 bit of SBox7 is faulted
- $Tc = 10.56\,\text{ns}$: SBox6&7 are faulted

Hardware Implementation of AES-128

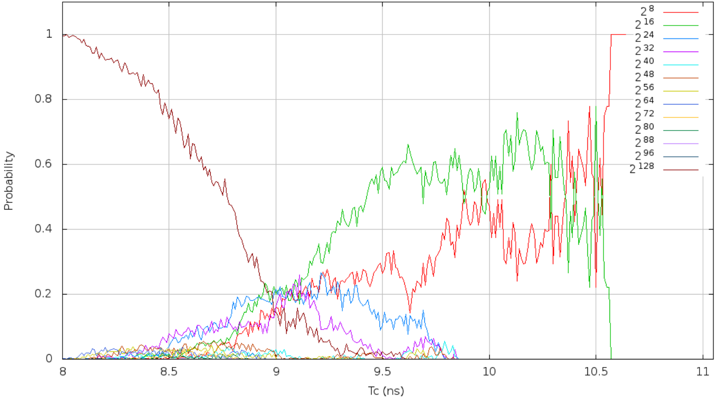
Probability to be faulted of slowest bits of SBox7 and SBox6



- Bit *b* faulted if it has to be updated and $t_b < Tc$
- Model complexity for verification: $16 \times 2^{2\times 8} \times 128$ only
- Countermeasure design: SBox6-bit7 faulted highly implies SBox6-bit7 is also faulted.
- Possibility to use this information?

Hardware Implementation of AES-128

Probability of key space.



Sufficient to protect only some SBoxes (instead of 16)?

Presentation Outline

Introduction, Motivation

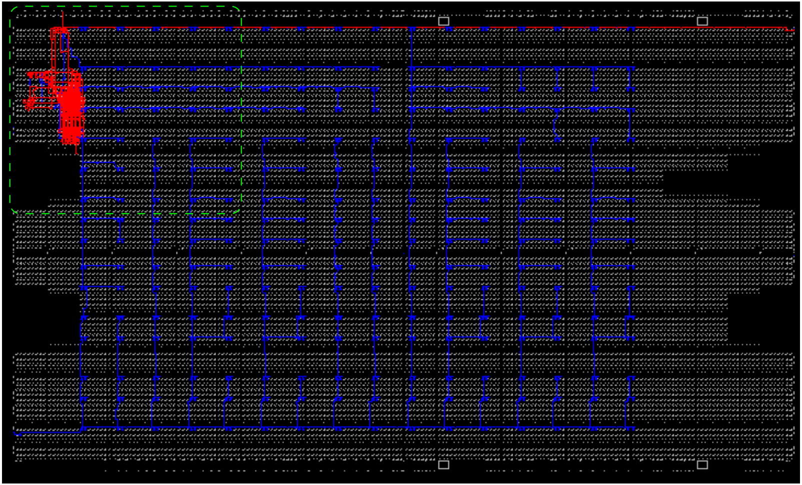
Multi-level Formal Verification by Example

Challenge Regarding EMI Modeling

Conclusion & Perspectives

Characterization of EMI Impact

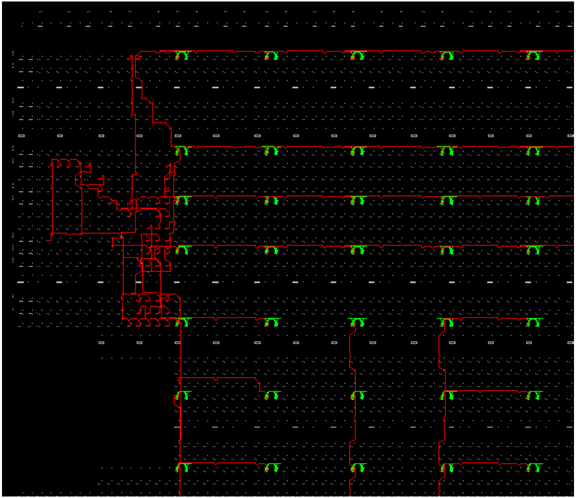
SASEBO-W/Spartan-6



16x16 array of sensors (*blue*) plus control block (*red*)

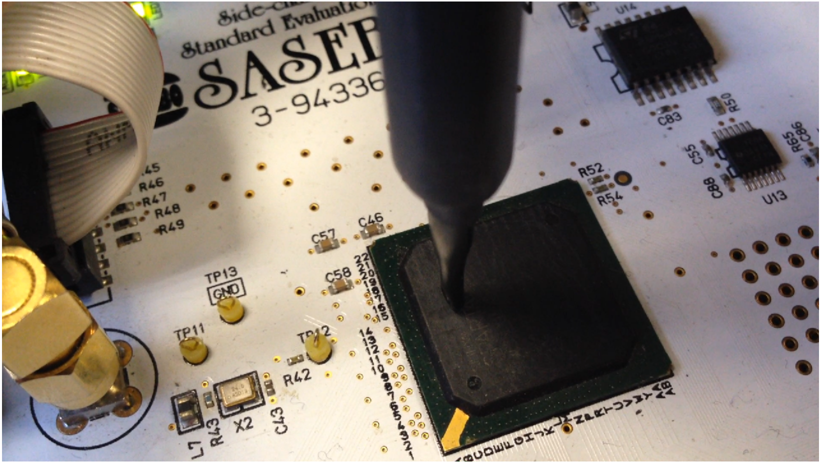
Characterization of EMI Impact

SASEBO-W/Spartan-6 (zoom)

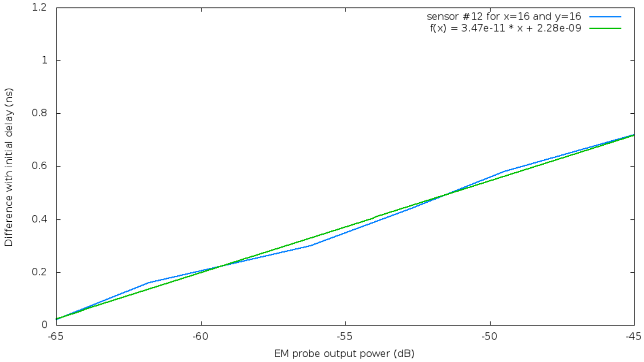


Each sensor is placed into a single configurable logic block (CLB).

Scan over Spartan-6 with 1 mm EM probe

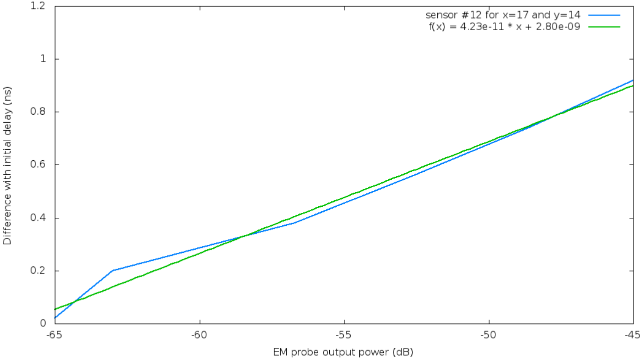


Impact on sensor #12 @ (x=16,y=16)



- $a_{12}^{(16,16)} = 1.74\,\text{ps}/\text{dB}$
- Asymptotic standard error with linearity: 3.782 %

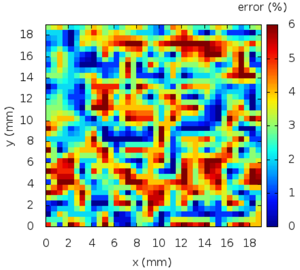
Impact on sensor #12 @ (x=17,y=14)

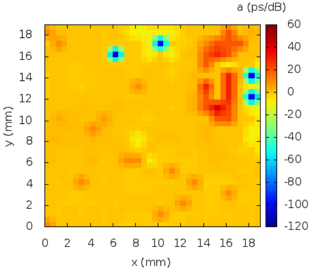


- $a_{12}^{(17,14)} = 2.11\,\text{ps}/\text{dB} > a_{12}^{(16,16)}$: greater impact
- Asymptotic standard error with linearity: 5.324 %

Impact on sensor #12

Susceptibility maps: what happens outside the FPGA

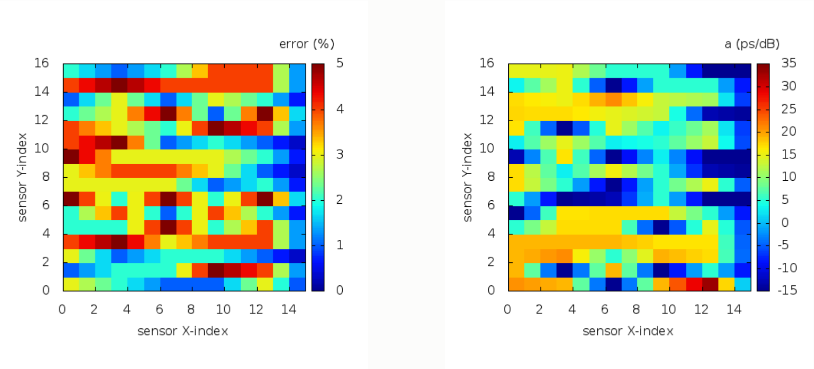




- According to the EMI probe position, the delay is increased or decreased.
- The spatial distribution is not trivial (*e.g.*, Gaussian).
- Model complexity: multiplied by the number of spatial points.

Impact on all sensors @ (*x*=16, *y*=16)

Functionnal maps: what happens inside the FPGA



- All delays are impacted

Presentation Outline

Introduction, Motivation

Multi-level Formal Verification by Example

Challenge Regarding EMI Modeling

Conclusion & Perspectives

Conclusion & Perspectives

- FIA countermeasure verification is highly time-consuming.
- FIA countermeasure overhead is high.
- Proposal take into account characteristics of each level.
- Does it help reduce verification time/overhead?

Thanks for your attention.
Any question?

References

[ABF$^+$02] Christian Aumüller, Peter Bier, Wieland Fischer, Peter Hofreiter, and Jean-Pierre Seifert, *Fault attacks on RSA with CRT: concrete results and practical countermeasures*, Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers (Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, eds.), Lecture Notes in Computer Science, vol. 2523, Springer, 2002, pp. 260–275.

[AKS12] Kahraman D. Akdemir, Deniz Karakoyunlu, and Berk Sunar, *Non-linear error detection for elliptic curve cryptosystems*, IET Information Security **6** (2012), no. 1, 28–40.

[BBB$^+$11] Alessandro Barenghi, Guido Marco Bertoni, Luca Breveglieri, Gerardo Pelosi, and Andrea Palomba, *Fault attack to the elliptic curve digital signature algorithm wit multiple bit faults*, Proceedings of the 4th International Conference on Security of Informatio and Networks, SIN 2011, Sydney, NSW, Australia, November 14-19, 2011 (Mehmet A. Orgun an Atilla Elçi an Oleg B. Makarevich an Sorin A. Huss an Josef Pieprzyk an Lyudmila K. Babenko an Alexander G. Chefranov an Rajan Shankaran, ed.), ACM, 2011, pp. 63–72.

[BBK$^+$03] Guido Bertoni, Luca Breveglieri, Israel Koren, Paolo Maistri, and Vincenzo Piuri, *Error analysis and detection procedures for a hardware implementation of the advanced encryption standard*, IEEE Trans. Computers **52** (2003), no. 4, 492–505.

[BDH$^+$97] Feng Bao, Robert H. Deng, Yongfei Han, Albert B. Jeng, A. Desai Narasimhalu, and Teow-Hin Ngair, *Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults*, Security Protocols, 5th International Workshop, Paris, France, April 7-9, 1997, Proceedings (Bruce Christianson, Bruno Crispo, T. Mark A. Lomas, and Michael Roe, eds.), Lecture Notes in Computer Science, vol. 1361, Springer, 1997, pp. 115–124.

[BDL97] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton, *On the importance of checking cryptographic protocols for faults (extended abstract)*, Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding (Walter Fumy, ed.), Lecture Notes in Computer Science, vol. 1233, Springer, 1997, pp. 37–51.

[BS97] Eli Biham and Adi Shamir, *Differential fault analysis of secret key cryptosystems*, Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings (Burton S. Kaliski Jr., ed.), Lecture Notes in Computer Science, vol. 1294, Springer, 1997, pp. 513–525.

[DGRS09] Emmanuelle Dottax, Christophe Giraud, Matthieu Rivain, and Yannick Sierra, *On second-order fault analysis resistance for CRT-RSA implementations*, Information Security Theory and Practice. Smart Devices, Pervasive Systems, and Ubiquitous Networks, Third IFIP WG 11.2 International Workshop, WISTP 2009, Brussels, Belgium, September 1-4, 2009, Proceedings (Olivier Markowitch, Angelos Bilas, Jaap-Henk Hoepman, Chris J. Mitchell, and Jean-Jacques Quisquater, eds.), Lecture Notes in Computer Science, vol. 5746, Springer, 2009, pp. 68–83.

[KKT04] Mark G. Karpovsky, Konrad J. Kulikowski, and Alexander Taubin, *Differential fault analysis attack resistant architectures for the advanced encryption standard*, Smart Card Research and Advanced Applications VI, IFIP 18th World Computer Congress, TC8/WG8.8 & TC11/WG11.2 Sixth International Conference on Smart Card Research and Advanced Applications (CARDIS), 22-27 August 2004, Toulouse, France (Jean-Jacques Quisquater, Pierre Paradinas, Yves Deswarte, and Anas Abou El Kalam, eds.), IFIP, vol. 153, Kluwer/Springer, 2004, pp. 177–192.

[KQ07] Chong Hee Kim and Jean-Jacques Quisquater, *Fault attacks for CRT based RSA: new attacks, new results, and new countermeasures*, Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing Systems, First IFIP TC6 / WG 8.8 / WG 11.2 International Workshop, WISTP 2007, Heraklion, Crete, Greece, May 9-11, 2007, Proceedings (Damien Sauveron, Constantinos Markantonakis, Angelos Bilas, and Jean-Jacques Quisquater, eds.), Lecture Notes in Computer Science, vol. 4462, Springer, 2007, pp. 215–228.

[PQ03] Gilles Piret and Jean-Jacques Quisquater, *A differential fault attack technique against SPN structures, with application to the AES and KHAZAD*, Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings (Colin D. Walter, Çetin Kaya Koç, and Christof Paar, eds.), Lecture Notes in Computer Science, vol. 2779, Springer, 2003, pp. 77–88.

[Riv09] Matthieu Rivain, *Differential fault analysis on DES middle rounds*, Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings (Christophe Clavier and Kris Gaj, eds.), Lecture Notes in Computer Science, vol. 5747, Springer, 2009, pp. 457–469.

[Sha99] A. Shamir, *Method and apparatus for protecting public key schemes from timing and fault attacks*, November 23 1999, US Patent 5,991,415.

[YJ00] Sung-Ming Yen and Marc Joye, *Checking before output may not be enough against fault-based cryptanalysis*, IEEE Trans. Computers **49** (2000), no. 9, 967–970.

[YKM06] Sung-Ming Yen, Dongryeol Kim, and Sang-Jae Moon, *Cryptanalysis of two protocols for RSA with CRT based on fault infection*, Fault Diagnosis and Tolerance in Cryptography, Third International Workshop, FDTC 2006, Yokohama, Japan, October 10, 2006, Proceedings (Luca Breveglieri, Israel Koren, David Naccache, and Jean-Pierre Seifert, eds.), Lecture Notes in Computer Science, vol. 4236, Springer, 2006, pp. 53–61.