Reverse-Engineering of Hardware Circuits

Jean-Luc Danger, Sylvain Guilley

Institut Mines TELECOM / TELECOM-ParisTech

SR2I301

Presentation Outline

Presentation Outline

Definition of reverse-engineering

Definition

- When the algorithm to attack is unknown, the system is a “black-box”.
- This means that the only way to attack is to analyze the input/output relationships $\Rightarrow$ hard in general (but for cube attacks [DS09, DS10])
- Therefore, the first step is to recover the algorithm.

Hardware versus Software reverse-engineering

- **Software**: The compiled code can be read-out from memories, and disassembled. Typically A5/1, A5/2, Hitag2 and Keeloq have been retrieved like that.
- **Hardware**: The functionality is buried into an ASIC.

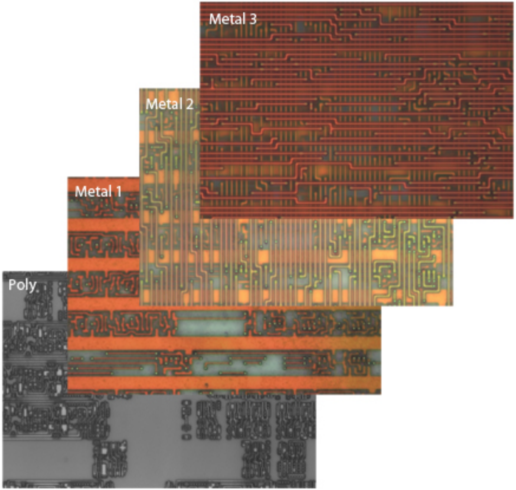
Goal of reverse-engineering

Goals

1. Retrieving an algorithm and then cryptanalyse it:
    - This was the case of CRYPTO1 (MyFare) or DSC (DECT).
    - Indeed, the confidential algorithm is most often weak.
2. Breaking a protection:
    - Understand how memories are encrypted by a secure microcontroller [Mah97].
    - Afterwards, all the code is exposed.
    - It thus becomes easy to identify bugs, that can be exploited at the software-level.
    - Thanks to buffer overflows, take the control of the application.
3. Intellectual property matters:
    - Accessing the design of a competitor, so as to steal it.
    - Checking that the competitor does not infringe my patents.

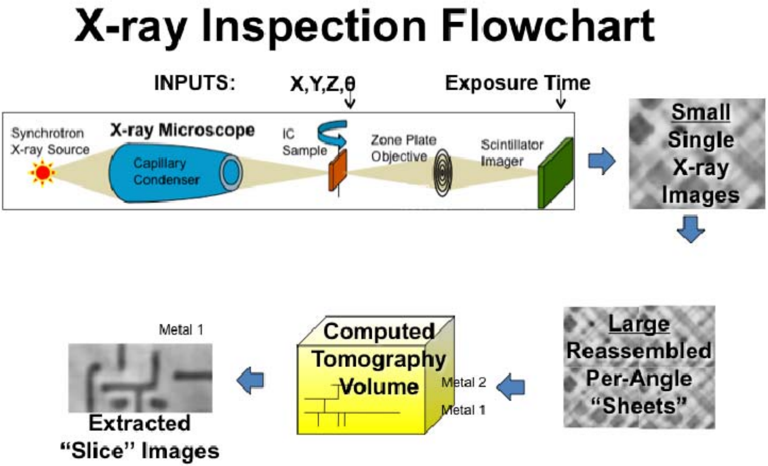
Presentation Outline

Principle of Circuit Reverse-Engineering: Delayering



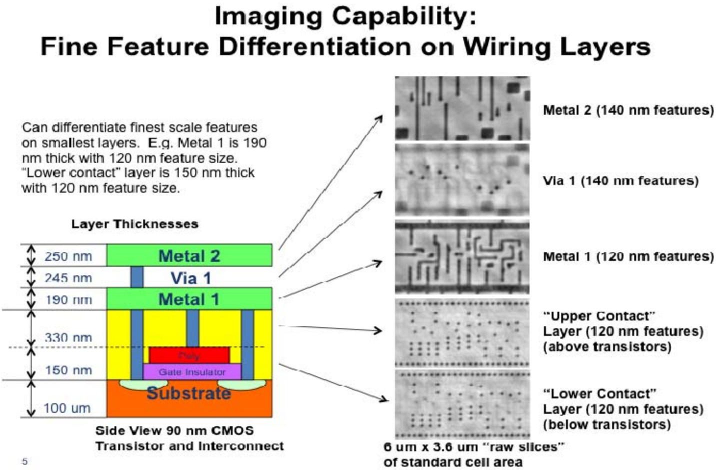
Principle of Circuit Reverse-Engineering:

Tomography [BBT+11] (see also [Zei13])

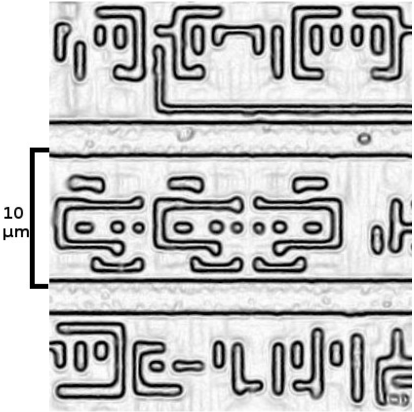


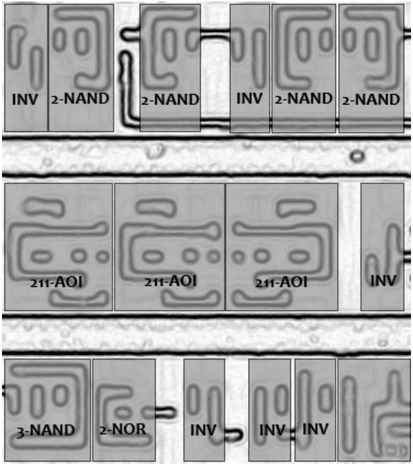
Principle of Circuit Reverse-Engineering:

Tomography [BBT+11] (see also [Zei13])

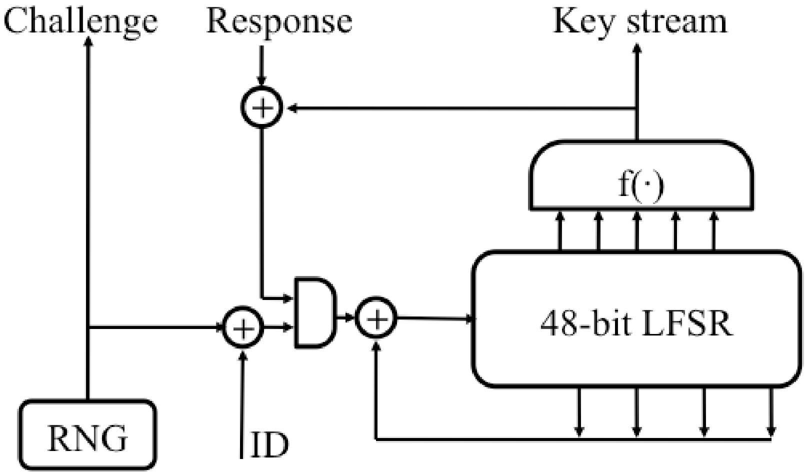


Example of MyFare (NXP) [NSP08]

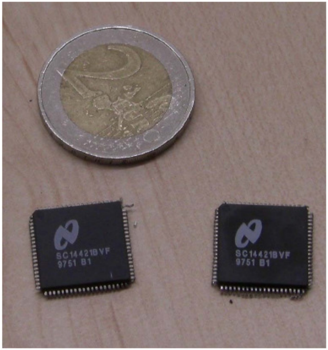


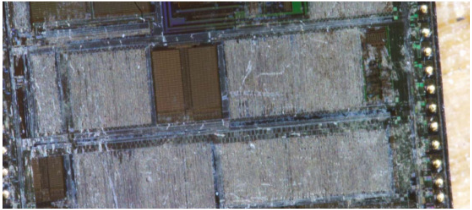


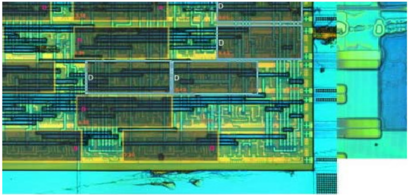
Example of MyFare (NXP) – CRYPTO1 exposed [NSP08]



Example of DECT (Alcatel) [NTW10]

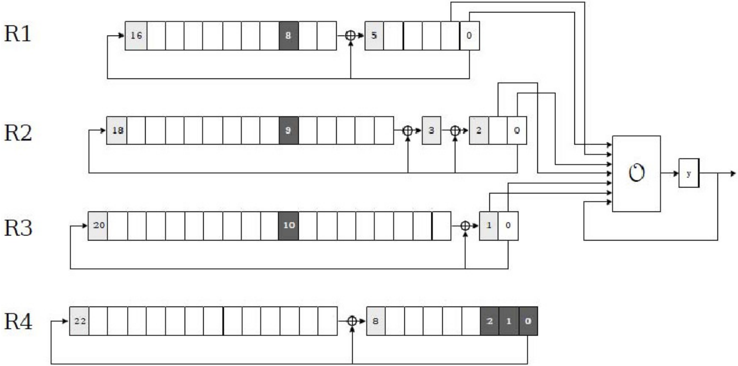






See also: https://deDECTed.org/.

Example of DECT (Alcatel) – DSC exposed [NTW10]

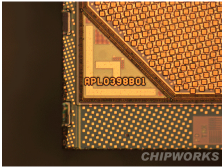


DSC = DECT Standard Cipher.

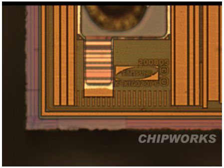
Professional techniques

Example of http://www.chipworks.com/ [TJ09] iPAD tear-down (see also http://www.ltecusa.com/ and many others).

Apple / Microprocessor (with DRAM)

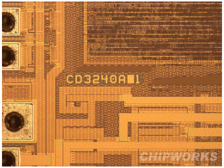


Samsung / 1 Gb mobile DDR SDRAM (x2)

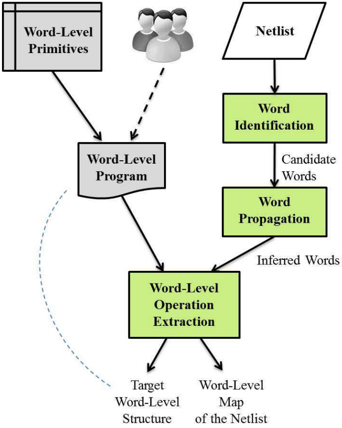


Broadcom / Microcontroller with NVM (used for touch-screen)

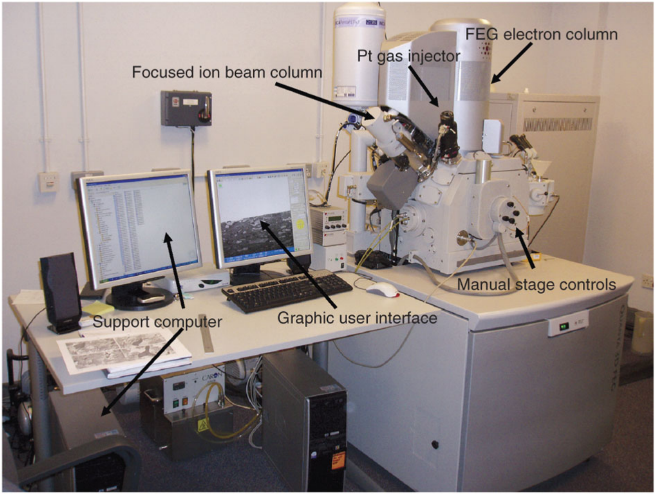
TI / Touchscreen line driver



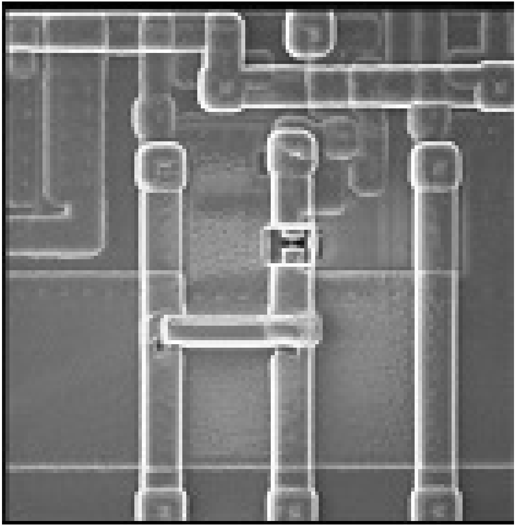
WordRev: Finding word-level structures in a sea of bit-level gates [LGS+13]



Focused Ion Beam (FIB)

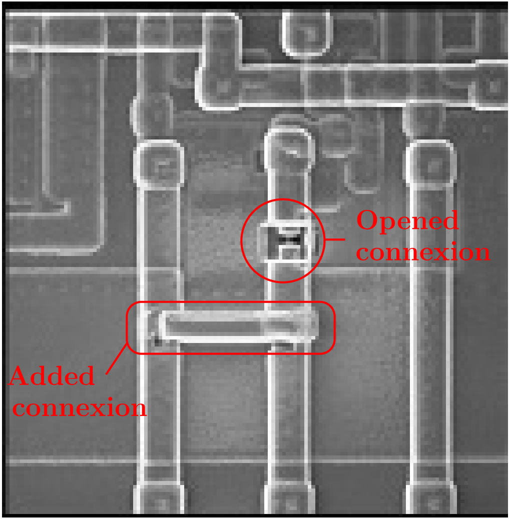


Edition of a circuit thanks to a FIB (Focused Ion Beam)



Can be used for instance to unlock memories [Gir07].

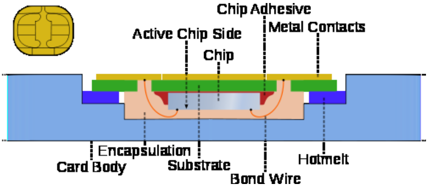
Edition of a circuit thanks to a FIB (Focused Ion Beam)

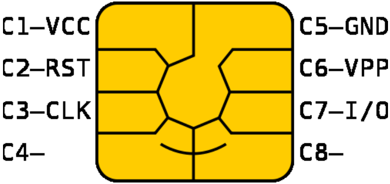


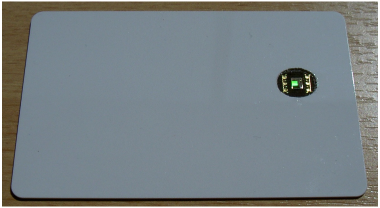
Can be used for instance to unlock memories [Gir07].

Presentation Outline

Preparation of a smartcard front- and rear-side



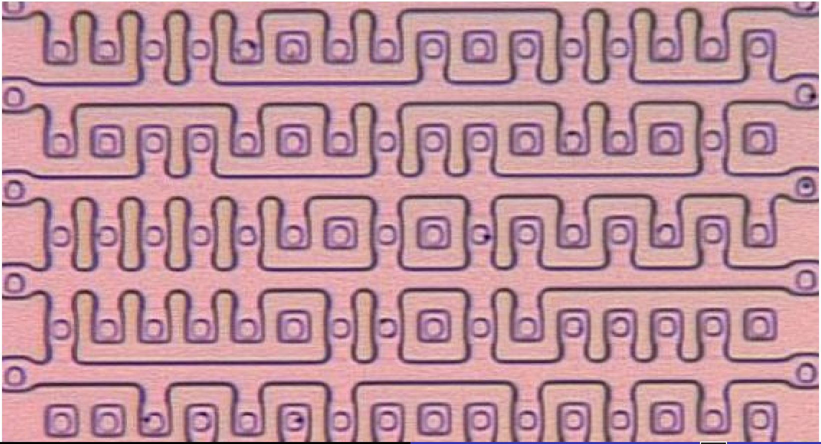




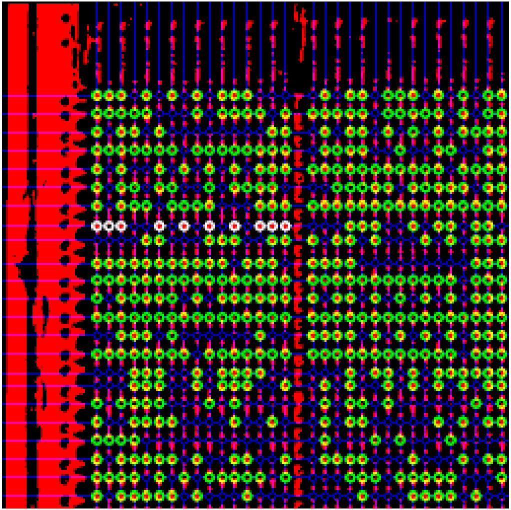
This chemical preparation enables probing and fault injection attacks.

Reading ROMs [KK99]

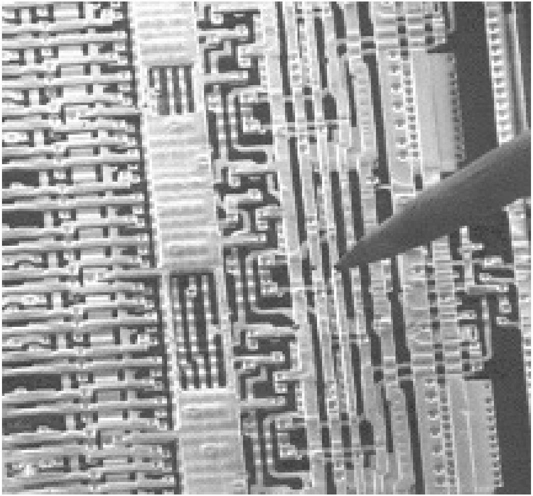
The image shows 16 × 10 bits in an ST16xyz. Every bit is represented by either a present or missing diffusion layer connection.



Semi-automatic extraction of ROM data (`rompar`)



Needles can be used to actively / passively probe signals



- Can be used for instance to read keys as they circulate into the circuit.
- This technique gives the attacker a considerable power.
- However, probing stations allow to simultaneously read only a couple of bits [HPS99]... and only those that are on top of the circuit.

Faults Injection Reverse-Engineering

FIRE on DES / AES

- Already illustrated by Biham & Shamir (reconstructing unknown ciphers [BS97]) on Feistel schemes.
- Works on DES, because the attacker sees *inputs and outputs* differentials (improvement in [LBGRT13]).
- With secret encodings, it still works on DES, because the sbox is non-injective [Cla07].
- FIRE on SPNs (such as AES) is an emerging topic [PMG11].

Presentation Outline

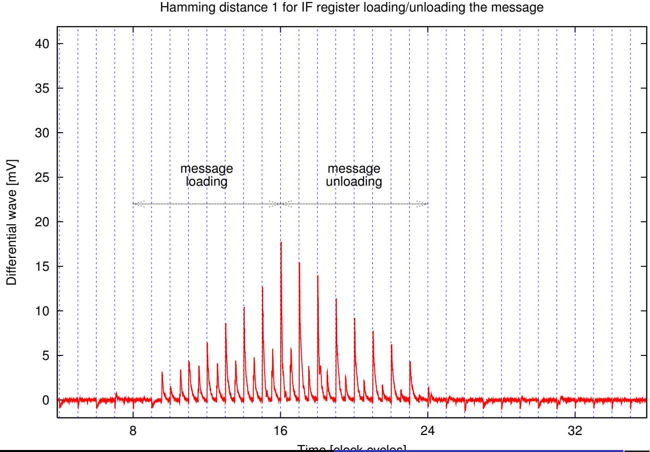
Principle of temporal localization

Use **specific inputs** and **monitor the differences** via one side-channel. For instance, imagine that the key is known.

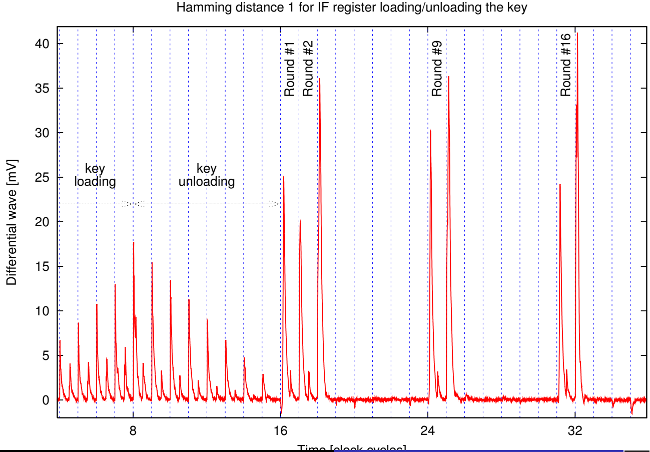
In the next three slides, we suggest to locate:

1. the plaintext loading,
2. the key loading,
3. the key schedule (diversification of the root key for each round).

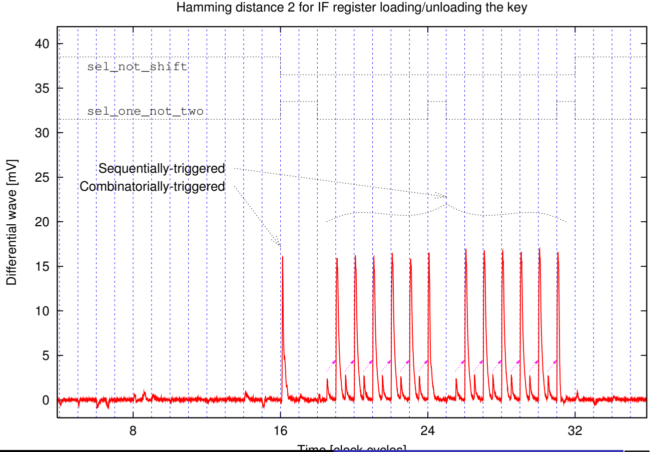
Signature of message loading / unloading in IF (**Reminder**: IF is the InterFace register)



Signature of key loading / unloading in IF, plus the CD activity

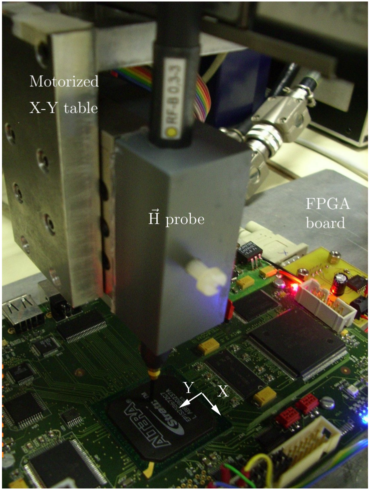


Signature of distance-2 key loading / unloading in IF and of LS^2 in CD



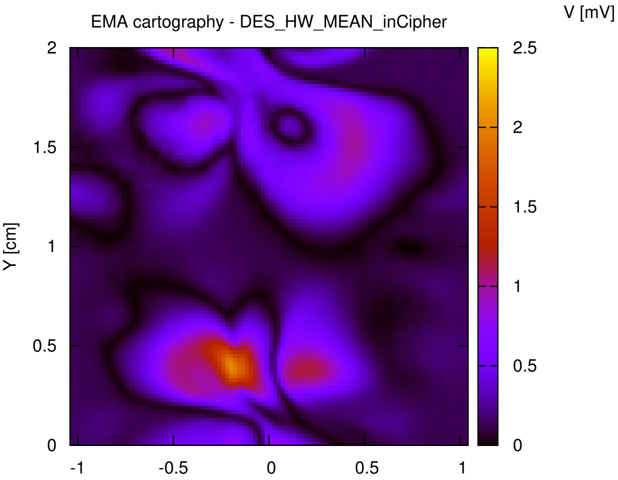
Principle of spacial localization

Using an (X, Y) cartography tool



- Extension: (X, Y, Z, θ) table.
- Helps identify zones that leak a lot; they do not necessarily correspond to the location of the modules! *Id est* they can maybe guide an attack by EMI but not by laser.

Cartography results



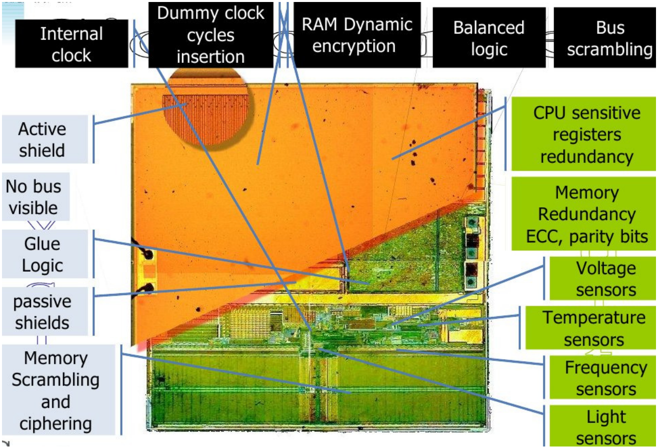
Presentation Outline

Example of the white-box cryptography

White-box cryptography [BCD09, CFD+10]

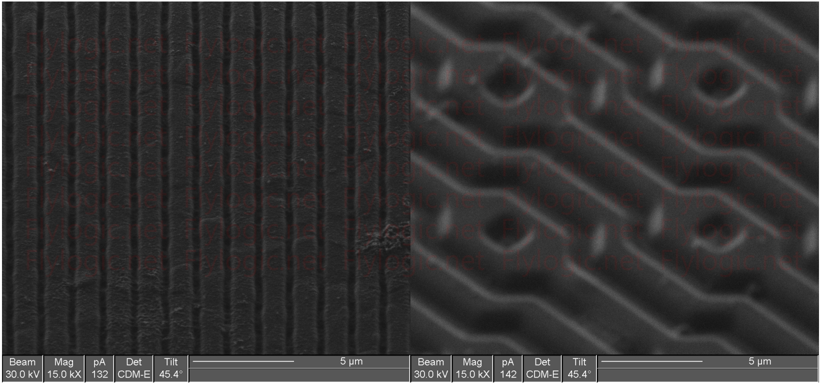
- **Principle**: provide everything (*i.e.* the compiled or the source code of the software) of an algorithm embedding a secret key.
- **Goal**: deny to the attacker the power of retrieving the couple (algorithm + key).

A summary of the countermeasures embedded in a smartcard

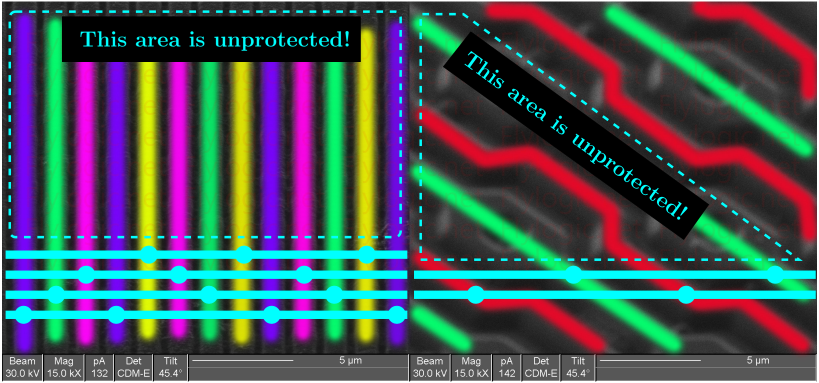


Courtesy of Assia Tria, CEA/LETI.

Active shield 1/2

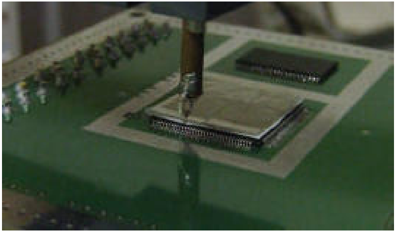


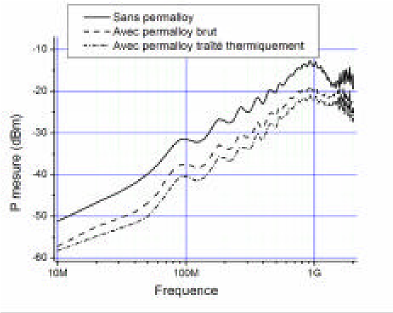
Active shield 2/2



Radiation suppression with a ferromagnetic film

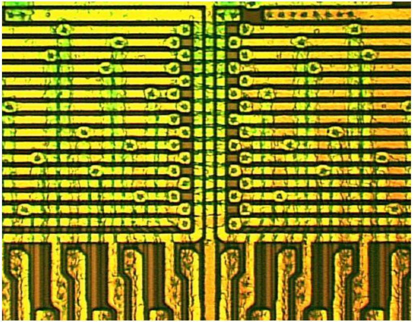
Ferromagnetic material $Ni_{80}Fe_{20}$, *aka* Permalloy.
Experiment with a layer of 20 μm depth [BBD+07].





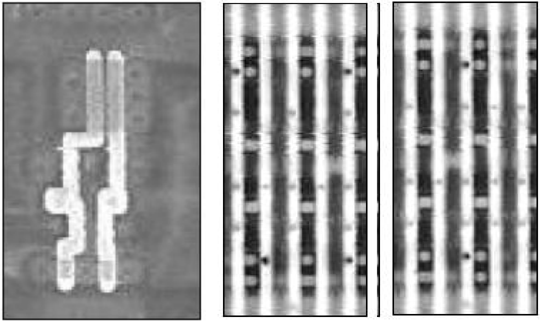
Bus scrambling

- Scrambling can be static or dynamic.
- Static scrambling can also be a feature
  - The mixing comes from a problem of routability of the data/address bus to the memory.
  - Possible because permutations affect equally the `write` and `read` operations.



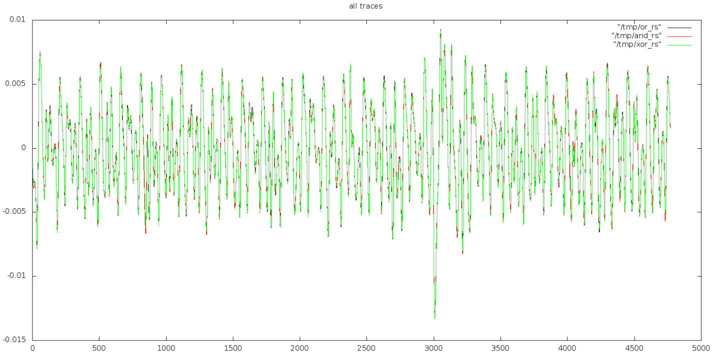
Beware of attacks [FLM10] on scrambled EEPROMs!

Hardware Camo



Hardware-level camouflage of gates. Left: an unprotected gate, whose function is easy to identify. Center, right: *almost* indistinguishable AND/OR camouflaged gates. *[courtesy of SMI / SypherMedia Library]*

Software Camo ARM7 Native Machine Code



Traces of the electromagnetic leakage of the AND, XOR and OR

[BBD+07] L. Bouhouch, A. Boyer, S. Ben Dhia, É. Sicard, and M. Fadel.
Amélioration des performances CEM d'un microcontrôleur à l'aide d'un film ferromagnétique.
In *TELECOM 2007, 5th JFMMA*, March 2007.
Fes, Morocco. (Online PDF).

[BBT+11] M. Bajura, G. Boverman, J. Tan, G. Wagenbreth, C. M. Rogers, M. Feser, J. Rudati, A. Tkachuk, S. Aylward, and P. Reynolds.
Imaging Integrated Circuits with X-ray Microscopy.
In *Proceedings of the 36th GOMACTech Conference*, March 2011.
Orlando, FL, USA.
`http://www-ssrl.slac.stanford.edu/research/highlights_archive/circuitintegrity.pdf`.

[BCD09] Julien Bringer, Hervé Chabanne, and Jean-Luc Danger.
Protecting the NOEKEON Cipher against SCARE Attacks in FPGAs by Using Dynamic Implementations.
In *ReConFig*, pages 183–188. IEEE Computer Society, December 9–11 2009.
Cancún, Quintana Roo, México. DOI: 10.1109/ReConFig.2009.19,
`http://eprint.iacr.org/2009/239.pdf`.

[BS97] Eli Biham and Adi Shamir.
Differential Fault Analysis of Secret Key Cryptosystems.
In *CRYPTO*, volume 1294 of *LNCS*, pages 513–525. Springer, August 1997.
Santa Barbara, California, USA. DOI: 10.1007/BFb0052259.

[CFD+10] Zouha Cherif, Florent Flament, Jean-Luc Danger, Shivam Bhasin, Sylvain Guilley, and Hervé Chabanne.
Evaluation of White-Box and Grey-Box Noekeon Implementations in FPGA.
In Viktor K. Prasanna, Jürgen Becker, and René Cumplido, editors, *ReConFig*, pages 310–315. IEEE Computer Society, 2010.

[Cla07] Christophe Clavier.
Secret External Encodings Do Not Prevent Transient Fault Analysis.
In *CHES*, volume 4727 of *Lecture Notes in Computer Science*, pages 181–194. Springer, 2007.
Vienna, Austria.

[DS09] Itai Dinur and Adi Shamir.
Side Channel Cube Attacks on Block Ciphers.
Cryptology ePrint Archive, Report 2009/127, March 2009.
http://eprint.iacr.org/2009/127/.

[DS10] Itai Dinur and Adi Shamir.
Generic Analysis of Small Cryptographic Leaks.
In *FDTC*, pages 39–48. IEEE Computer Society, August 21 2010.
Santa Barbara, CA, USA. DOI: 10.1109/FDTC.2010.11.

[FLM10] Jacques J. A. Fournier and Philippe Loubet-Moundi.
Memory Address Scrambling Revealed Using Fault Attacks.
In *FDTC*, pages 30–36. IEEE Computer Society, August 21 2010.
Santa Barbara, CA, USA. DOI: 10.1109/FDTC.2010.13.

[Gir07] Christophe Giraud.
Attaques de cryptosystèmes embarqués et contre-mesures associées.
PhD thesis, Université de Versailles Saint-Quentin-en-Yvelines, 26 octobre 2007.
http://www.prism.uvsq.fr/fileadmin/CRYPTO/TheseCG-new.pdf.

[GMN+13] Sylvain Guilley, Damien Marion, Zakaria Najm, Youssef Souissi, and Antoine Wurcker.
Software Camouflage.
In *FPS*, volume 8352 of *LNCS*. Springer, October, 21–22 2013.
La Rochelle, France.

[HPS99] Helena Handschuh, Pascal Paillier, and Jacques Stern.
Probing Attacks on Tamper-Resistant Devices.
In *CHES*, volume 1717 of *LNCS*, pages 303–315. Springer, August 12-13 1999.
Worcester, MA, USA.

[KK99] Oliver Kömmerling and Markus G. Kuhn.
Design Principles for Tamper-Resistant Smartcard Processors.
In *WOST '99 (USENIX Workshop on Smartcard Technology)*, pages 9–20, Berkeley, CA, USA, May 10-11 1999. USENIX Association.
Chicago, Illinois, USA (On-line paper). ISBN: 1-880446-34-0.

[LBGRT13] Hélène Le Bouder, Sylvain Guilley, Bruno Robisson, and Assia Tria.
Fault Injection to Reverse Engineer DES-like Cryptosystems.
In *FPS*, volume 8352 of *LNCS*. Springer, October, 21–22 2013.
La Rochelle, France.

[LGS+13] Wenchao Li, Adria Gascón, Pramod Subramanyan, Wei Yang Tan, Ashish Tiwari, Sharad Malik, Natarajan Shankar, and Sanjit A. Seshia.
WordRev: Finding word-level structures in a sea of bit-level gates.
In *HOST*, pages 67–74. IEEE, 2013.

[Mah97] David Paul Maher.
Fault Induction Attacks, Tamper Resistance, and Hostile Reverse Engineering in Perspective.
In *Financial Cryptography*, volume 1318 of *Lecture Notes in Computer Science*, pages 109–122. Springer, February 24-28 1997.

[NSP08] Karsten Nohl, David Evans Starbug, and Henryk Plötz.
Reverse-Engineering a Cryptographic RFID Tag.
In *USENIX Security Symposium*, pages 185–193, July 31 2008.
San Jose, CA, USA (Online HTML).

[NTW10] Karsten Nohl, Erik Tews, and Ralf-Philipp Weinmann.
Cryptanalysis of the DECT Standard Cipher.
In *FSE*, volume 6147 of *Lecture Notes in Computer Science*, pages 1–18. Springer, February 7-10 2010.
Seoul, South Korea.

[PMG11] Manuel San Pedro, Soos Mate, and Sylvain Guilley.
FIRE: Fault Injection for Reverse Engineering.
In LNCS, editor, *WISTP: Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing*, volume 6633 of *LNCS*, pages 280–293. Springer, June 1-3 2011.
Heraklion, Greece. DOI: 10.1007/978-3-642-21040-2_20.

[TJ09] Randy Torrance and Dick James.
The State-of-the-Art in IC Reverse Engineering.
In *CHES*, volume 5747 of *LNCS*, pages 363–381. Springer, September 6-9 2009.
Lausanne, Switzerland.

[Zei13] Carl Zeiss.
Package Optimization and Failure Analysis with 3D X-ray Microscopy, November 2013.
https://zeiss-microscopy.uberflip.com/i/547299-package-optimization-and-failure-analysis-with-3d-x-ray-microscopy.