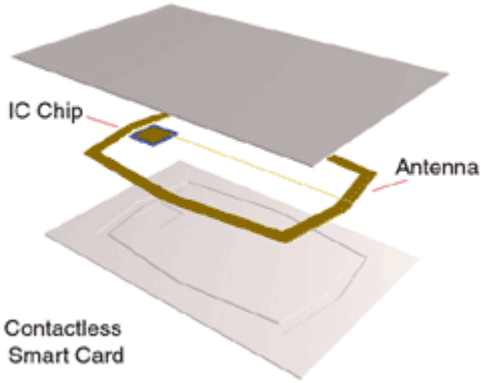
Smart Secure Devices
&
Embedded Operating Systems

Contact: pierre.dusart@unilim.fr

Team: XLIM/DMI/SSD

Limoges/FRANCE

Technology involved



iButton

USB token

Prices of these objects: less than 20 $

Applying Domains

- Telecom
- Banking industry
- Health
- Pay TV
- Access control

- Electronic services (signature, electoral vote)
- Identity Card / Biometric Passport

Various themes

- Improve the security of small devices
  - Attacks on smartcards
  - Hardware/software countermeasures
  - Audit or security evaluation methods
- Improve the global security
  - External or internal use of secure parts (TPM)
  - New cryptographic algorithms or secure implementation of approved ones

French Community (French Academic Teams)

- Modular Operating System
  INRIA team:
  Pops (Lille), new operating system for smart cards
  Sarde (Grenoble), dynamic reconfiguration capacity (Think kernel)
  ACES (Rennes) (ubiquitous computing OS)

- Security
  Everest (INRIA Sophia) security for dynamic upload of kernel components based on the Necula paradigm, (collaboration with Gemplus)
  Lande (IRISA Rennes) static analysis techniques for security properties (applied to Java Card application)
  LRI (Orsay) work on the security of pc based architecture and the relationship with TPM modules.

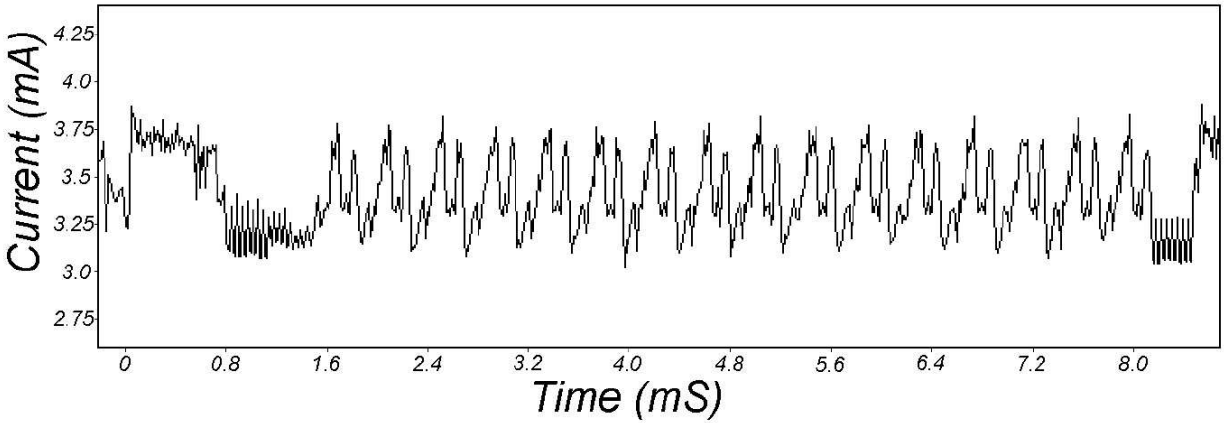
- Attacks
  Prism team Crypto (St Quentin) several thesis on fault attaks on crypto algorithms in collaboration with OCS and Gemalto
  EMSE-CEA (Ecole des Mines de St Etienne) fault attacks, post doc in collaboration with gemalto.
  Labri (O. Ly): Automata, Automatic Integration of Counter-Measures

Our specificity

- Security of operating systems (through a security module like smartcard, Trusted Platform Module)
- Tools for Evaluation and Audit of Virtual Machine
- Embedded cryptography
- Works with Physicians/Electronics engineers (SeFSI Project)
  - Hardware Design (Random Number Generator, Filtered LFSR)
  - Antenna Design (for EMA)

Attacks on SmartCards

- Power analysis: measurement of the consumption current to look into a cryptographic process
- You can recover implementation parts or cryptographic keys



Embedded Cryptography

- Some attacks are specific:
  - Best theoric attack on D.E.S Cryptographic algorithm: 2^43 ciphertexts needed
  - Deep Crack: recover a DES-key in less than 1 day
  - Concrete attack on hardware device: less than 3 hours (by DFA or DPA)
- Depend on hardware, implementation,…

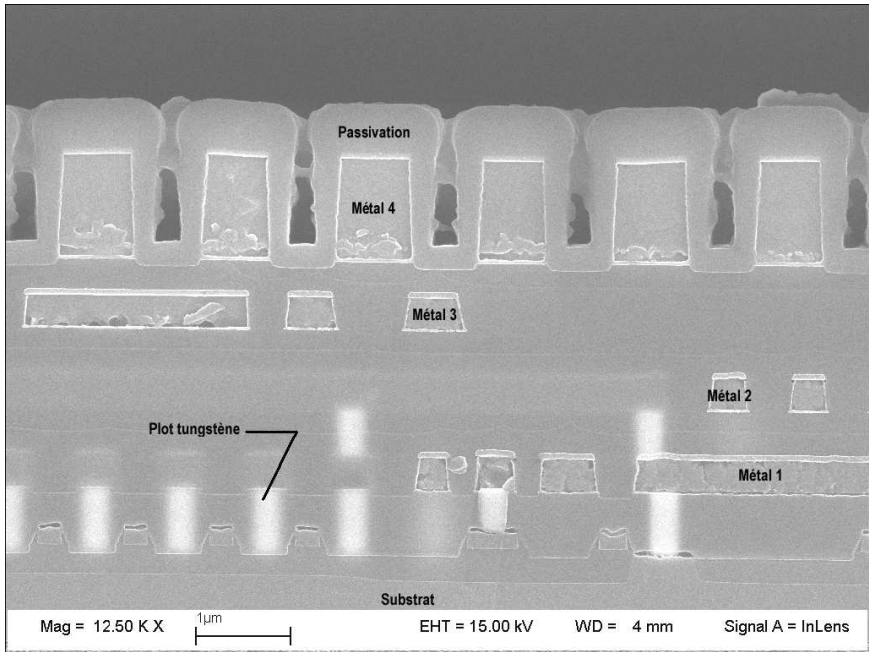
External attacks: Fault Injection on Hardware Device

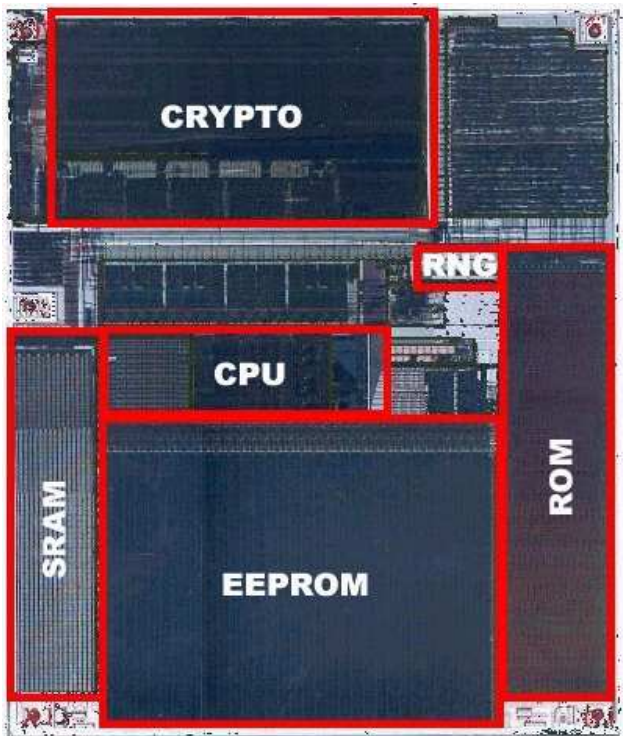
- Glitches on power supply
- Frequency Change
- Radiations (Laser, X-Ray, Flash)
- Circuit cutting, probing

Goal: false computations, differential methods to recover key

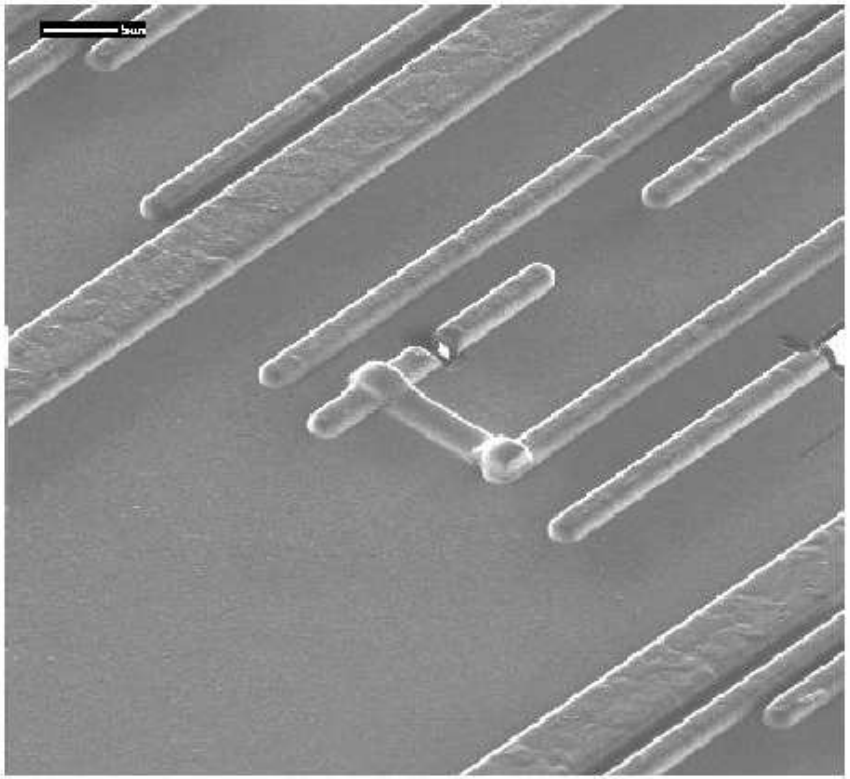
Hardware views of a SmartCard

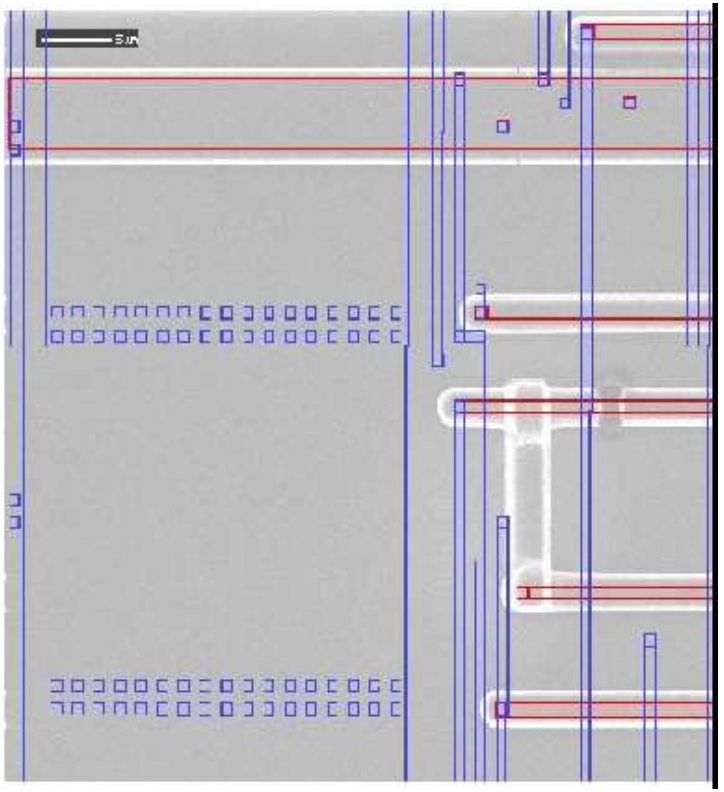
- Many parts and levels



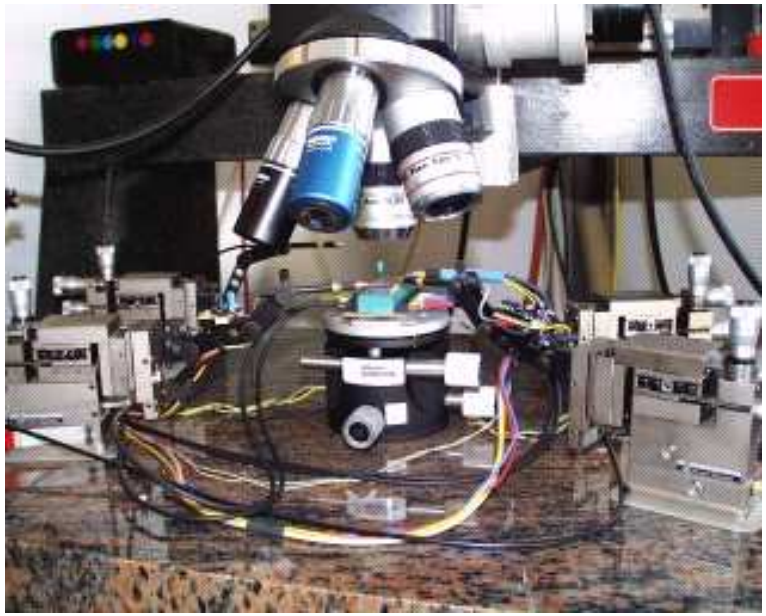


Acute Cutting with FIB





Probing and Antenna



Example: Fault on RSA-CRT

- We know the correct signature *s* of a message *m* computed by *RSA-CRT*. One fault is injected during the p-modular exponentiation. We obtain a erroneous signature *s'*.
- We have $s' = a\, s'_p + b\, s_q$
- Hence $s' = s \bmod q$ but $s' \neq s \bmod p$
- Now $gcd(s-s',n) = gcd(a(s_p - s'_p),n) = q$
- We find *q* then *p*, the two prime factors of n.

Inside Attacks

- Multi-applicative systems (Java Card)
- We can dynamically upload applications on modern hardware (with virtual machine)
- Corrupted Application tries to access to private elements like a virus and passes through the firewall

Our competences

- Secure the load process of new applications
- Complete control of Access Rights of applications
- Automatic tests and static analysis of system security to security level evaluation
- Study new problems with hot swapping/plugin devices like memory atomicity
- Tamperproof execution: ensure the complete execution of a program to be without faults on sensitive data.

Projects

- In progress
  - SARAH (Delay-Tolerant Distributed Services for Mobile Ad Hoc Networks)
    - funded by the french ANR (National Agency for the Research)
    - LaBRI, LITIS, VALORIA and XLIM
  - Mobile Java Card Grid
    - selected by gemalto in the SIMagine contest
    - LaBRI, Royal Holloway, University of London and XLIM
- Future/Pending
  - MECANOS (Methodology for the applications of the future secure object)
    - Trusted Labs, Trusted Logic, Gemalto, Oberthur Card Systems, Soliatis, IdConcept, Eurécom, XLIM

Main Academic Partnerships

- LaBRI, UMR Université Bordeaux 1/CNRS 5800

  one of the largest academic group of research in computer science in France.

- Information Security Group of the Royal Holloway, University of London

  one of the largest academic security groups in the world. It brings together in a single institution expertise in education, research and practice in the field of information security.

- TEI of Athens

  Existing student exchanges, licensing of our Master and research collaboration (PhD co-supervisions, papers co-authoring, etc.)

Main Industrial Partnerships

- Gemalto
  - a world leader in digital security
    - hey range from the development of software applications through the design and production of secure personal devices such as smart cards, SIMs, e-passports and tokens to the deployment of managed services for our customers.
    - More than one billion people worldwide use our products and services for telecommunications, financial services, e-Government, identity management, multimedia content, digital rights management, IT security, mass transit and many other applications.
- Trusted Labs & Trusted Logic
  - Security of embedded systems (identification, banking and mobile telephony), Common Criteria, Evaluation of embedded systems
- Thales Security
  - In security markets, Thales leverages advanced technologies and risk management methodologies very similar to those required on defence programmes.
  - The company integrates security solutions for critical applications and supplies a range of security products, including cryptographic devices and payment terminals.

Involvement in events

- Past events
  - Organization of WISTP'2007 (Heraklion, Greece)
    - IFIP, IEEE, ACM
    - CrispTelecom, Eurosmart, GlobalPlatform, Nokia, Vodafone
    - 70 attendees
    - 68 submissions and 21 acceptances
  - PC of SECRYPT2007, IAS2007, ...
- Future events
  - Organization of WISTP'2008 (13-16 May 2008, Sevilla, Spain)
  - PC of Cardis 2008 (September 2008, London, UK)

Our inquiries / expectations

- More relationships between universities and/or collegues
- Students exchanges
- Security feeling: are the security objectives the same than in France?