MARS Project (ACI SI 2004)

Robust hardware for dependable systems – Matériel robuste pour systèmes sûrs –

Régis Leveugle, Abdelaziz Ammari, Vincent Maingot, Michele Portolan
TIMA - 46, av. Félix Viallet - 38031 Grenoble Cedex

Sylvain Guilley, Guillaume Leconte, Philippe Hoogvorst, Yves Mathieu, Renaud Pacalet
ENST/CNRS LTCI - 46, rue Barrault - 75013 Paris

MARS Motivations

Security is getting omnipresent in smart devices

Hardware accelerators are absolutely necessary to speed up the computations and to save the batteries

« Security hardware » is vulnerable to attacks targeting its implementation:
- Passive attacks, exploiting side-channel information leakage
- Active attacks, disturbing the system to gain information

MARS Goals

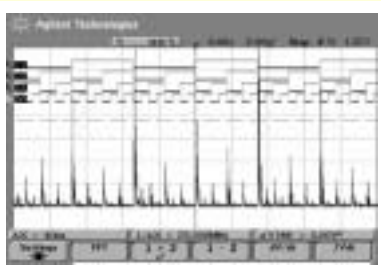
1. Provide dual countermeasures against both passive and active attacks:
   - Most counter-measures against side-channel attacks can be thwarted by an appropriate fault attack
   - Most counter-measures against active attacks increase information leakage

2. Define a multi-level hardening strategy:
   - Systems are complex
   - Every level of abstraction is a possible hook for an attack
   - Security level is equal to that of its weakest link

Side-Channel Attacks (SCAs)

- Side-channels can be:
  - Execution duration, if computations are optimized
  - Power consumption, allowing Simple and Differential Power Analysis (SPA & DPA)
  - Electro-magnetic radiations (*see below*)
    Side-channel can be the overall B field (loop), or the E field at a given frequency (*ad hoc* antenna)
- Acquisition strategy:
  - Fast oscilloscope (20 GSa/s, 6 GHz BW, 8 bit)
  - Differential probes
- Signal processing:
  - Filter-out de-correlated frequencies
  - Averaging to increase SNR

(S)EMA with a coil



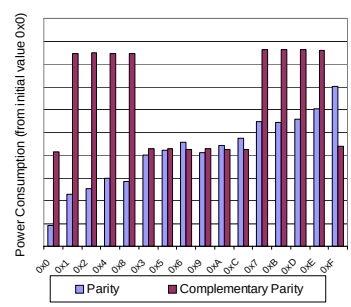
Fault Attacks (FAs)

- Power of fault induction:
  - RSA with CRT broken with two faults
  - DFA breaks all the cryptosystems with as few as 100 faults
- Non-invasive attacks or probing attacks
- Selection of efficient countermeasures against FA:
  - Evaluation of robustness vs. fault attacks: links with VENUS
  - Impact on side-channel characteristics (*see below*)

Example of two codes with similar error detection capabilities

Correlation between Hamming weight and power consumption:

Parity	0.9766
Comp. Parity	0.0558



Towards an ASIC robust against SCAs and FAs

Generic Security Methods and Tools

- DPA-Proof library in 130 nm process
- Balanced Place-and-Route Strategy
- Fault detection mechanisms
- Early dependability analysis tools

Prototype dedicated circuits

Dependable IPs

- Symmetrical Cryptography: DES
  - Hardened against SCA (ASIC demonstrator under test)
  - Also in WDDL and SI-WDDL logic
  - With multiple modes of operation and 3DES
- AES hardened against FA
- Asymmetrical Cryptography: RSA
  - Pipelined architectures
  - Adapted to multiple modulus size
  - Optional CRT
  - Embedded « proof by 2^m-1 »
- Processors: 8051 & 32-bit SPARC v8 LEON

Specially crafted Primitives (Symmetrical C-Element) → Robust Gate (DPA-Proof NAND) → Robust Algorithm (DES) → ASIC layout