« Safe (hardware) design methodologies against fault attacks »

Bruno ROBISSON
Assia TRIA
SESAM Laboratory (joint R&D team CEA-LETI/EMSE),
Centre Microélectronique de Provence
Avenue des Anémones, 13541 Gardanne, France
Introduction

Securing today’s devices

Securing tomorrow’s devices
Integrated Circuit « Classical » Design Flow

Specifications:
- Fonctionnality
- Power,
- Speed,
- Price

Technology:
- CMOS
- SOI
- Molecular
- ...

Simulation → Synthesis → Fabrication → Characterization

Virtual

Modeling

Real
Securing today’s devices

How to secure devices to known attacks?

Specifications:
X - resistance

Technology

DFA and DPA test benches

Syndroms

Simulation

Characterization

Fabrication

Synthesis
Example: Securing AES against DFA

Specifications:
- DFA-resistant
- DPA-resistant

Technology:
- CMOS

Commercial logic simulators
ad hoc and commercial power estimation tools

Error detection via spatial duplication
+ Error spreading
+ Balancing

C Implementation of CPA/DPA
Matlab Implementation of main DFA

Counter-measures validated
Detecting sensitivity to round reduction attacks
Securing today’s devices: the challenges

- Specifications
  - Securing today’s devices: the challenges
  - Specifications
  - Xs - Resistance

- Fabrication
  - Fabrication
  - Synthesis

- Simulation
  - Simulation
  - Fabrication

- Characterization
  - Characterization
  - Few available

- CAD to be adapted
  - CAD to be adapted
  - Constant

- Enhance
  - Enhance
  - Incomplete understanding

- Virtual
  - Virtual
  - Modeling

- Real
  - Real
  - Modeling

- NO realistic specifications
  - NO realistic specifications
  - Securing today’s devices: the challenges
Securing today’s chip: Addressing the challenges

- **Characterization**
  - Sharing equipments
  - Publications should describe experimental protocols and equipments
  - Towards an *a minima* standardization of security measurements (devoted to R&D’s activities)

- **Physics of attacks**
  - Modeling physical phenomena which make attacks possible (faults, EM)
  - Dedicated test IC

- **CAD tools to be adapted (simulation and synthesis)**
  - Simulators should support models dedicated to security
  - Development of *ad hoc* verification tools (based on formal methods)
  - Formalization of security constraints
  - Towards automatic synthesis of circuits verifying such constraints
Securing today’s chip: Adressing the challenges

Data retrieval
- Data base of physical signals (power and EM waveforms, faulty executions traces)
- Challenges from this data base to improve data retrieval algorithms
- Open library of optimized cryptographic primitives (DPA, DFA and cryptanalysis)

Specifications
- Take care of « naive » counter-measures
- Take into account all the known attacks
- Always test counter-measures on real devices
Securing tomorrow’s devices

Given an advanced technology:
- Will it resist to existing attacks?
- Will it lead to new attacks?

Specifications → Technology

Simulation → Synthesis → Fabrication → Characterization
Example: QDI asynchronous circuit

Permanent « stuck-at zero » on a wire of a dual rail may induce deadlock

Deadlock instants depend on the data values

Deadlock instants may be easily detected by monitoring the power consumption
DBA principles

| Safe-error | Key bits leak only through the information whether the device has a normal **behavior** or not in presence of fault |
| + | **DPA** |
| **Differential Behavioral Analysis** | **Correlating** a power model parameterized by the value of a small number of bits of the key (the partial key) to power measurements |
| | **Correlating** a functional model parameterized by the value of a partial key to **behaviors** of the device in presence of faults |
DBA hypothesis

- DPA hypothesis
  - Known cryptographic algorithms,
  - Known plain texts (or cipher texts)
  - There must exist intermediate variables that can be expressed as functions depending on the plain texts and on only a small number of key bits

- Fault injection
  - Type: Stuck-at zero (or one)
  - Location: On one bit in the set of the attack bits defined in DPA
  - Duration: Permanent (or transient)
  - Repetitiveness: Same fault, at same time, on same bit

- Detecting behavior between faults which create an error during round one or during another round

![Graph showing deadlock during round 1 ≠ deadlock during round 2](image)
DBA on a QDI asynchronous DES

QDI asynchronous DES
DPA counter-measures (logical balancing)
Standard cells
0.13 μm STMicroelectronics
180 ns for DES encryption
0.94mm² with interfaces

Faults injected on a bit at the output of the Sboxes
15 faulty executions with random values but known plain texts

Simulation

Value of the partial key (6 bit long)
Location of the faulty bit
Value of the faulty bit
Repetition of the fault injection
Securing tomorrow’s chip

- Evaluate advanced architectures
  - Asynchronous circuits, GALS
  - Reconfigurable devices
  - SOC, NOC
  - …

- Evaluate advanced technologies
  - SOI
  - Memories MRAM
  - Technology shrinking
  - Nano-technologies
  - Above-IC power sources
  - Smart packaging
  - …

- Anticipate attacker’s means
  - Equipments
  - Towards hybrid attacks
Conclusion

- A lot of work…
- Towards a more collaborative approach
  - Sharing some competences and equipments
  - Objective comparison of counter-measures

- But with incorporate industrial constraints
  - Fears and secrets around cryptographic developments
  - Time and cost constraints

CIMPACA/ Micro-Packs
- Gemalto, STMicroelectronics, Atmel, CEA
- LIRMM, ENST, ENSMSE,…