From an overview of hardware reverse engineering techniques to the practical evaluation of partial reverse engineering on 45-90nm targets.

Franck Courbon
Leverhulme Trust Early Career Fellow
Department of Computer Science and Technology
Security Group
Interest: Hardware Security

- 2.5 years at the department of Computer Science and Technology within the Security Group
- ‘Extending and characterising the capability of hardware based data-extraction techniques’ Principal Investigator
- Research and Teaching activities
A vertical point of view

- Very very low level security investigations (technologies)
  - Chemistry, materials science

- Very low level security (transistor based)
  - Physics, side channel leakage

- Low level security (root of trust, firmware)
  - Computer architecture, software reverse engineering

- Attack development and product application
Outline

- Integrated circuits structure
- Hardware reverse engineering techniques
- Partial reverse engineering application
A large range of Integrated Circuits

- Various targets, black box approach
  - Critical social, societal, financial impact
  - Design is confidential
  - Connected devices

- Targets have different features:
  - Types
  - Packages
  - Design
  - Technology nodes
  - Security design approaches taken
Integrated Circuits

- **Topview:** 3 main areas: analog part, core/synthesized logic (a sea of standard cells are combined together) and memories (arrays of 0's and 1's)

- **Sideview:** substrate, doped area (transistors active region), polysilicon (transistors gate), Al/Cu layers (metal layers), dielectric, vias, passivation
Integrated Circuits (a banking card example)

- Current smart cards have 65nm technology node process (2006)
- Surface: ~6*8mm
- Two main area: Synthesized logic (inc. core) and memories
  - Synthesized logic: ~200k standard cells: a cell has 2 to ~26 transistors
  - About 600 cells are different (drive, inputs, functions)
  - They are based on ~15 base functions OR-AND-NOT-FLIP-FLOP…
Memory element

- From FF to off site memory
- Memories are regular structures organized in rows and columns
- Presence of a certain material
- Presence of a certain charge
- Presence of a certain polarization
- Various failure analysis techniques exist
Integrated Circuits (a SoC example)

- Different package
- Different thickness
  - Silicon substrate (650-850μm)
  - Doped areas (transistors’ drain and source)
- Different techno.
  - Poly-Silicon (transistors’ gate)
  - Stack of 7+ Metal layers and dielectrics (ascending about 0.2 to 0.9μm)
  - Passivation: Si3N4 /SiO2 /Si3N4 (0.6/0.1/0.6μm)
  - Polyimide (5μm)
- Different blocks
  - Die bumps
  - PCB substrate
  - Copper balls
- Different area size
Security characterization covers several types of attacks; products are tested by certified laboratories.

- Include logical, fault, side-channel and invasive attacks.
- Basically ranked in terms of sample accessibility, attack time, attack platform cost and required skills.
- If scores too low for instance, the product does not meet security requirements: increase time to market, loss of market shares…

- Designers, founders, integrators, state agencies, certification authority, certified laboratories, academics…

- Various type of attacks for various type of attackers.
Physical attacks may not be assessed

Various applications

More complex

But attacks tools evolve too

Lower cost

Multi area perturbation

Higher power
Hardware reverse engineering

- Xray
- Laser
- FIB/SEM reverse engineering
- Delayering/Imaging/Proprietary software solution

Criteria: Cost/Surface covered/Process dependability

Schellenberg et al.
Backside approach

- Back to the initial drawing

- Removing substrate?
Mechanical lapping and polishing

- ‘Easy’ packages
- 5000£ mechanical polishing machine to remove Si
Hardware reverse engineering application

- In-house application
- Combined attack/information extraction
- Integrity verification / IP infringement
Sample preparation is needed

- Information of interest are ‘hidden’ in the component, frontside/backside imaging don’t give enough information

- For precise laser fault injection

- For malicious hardware modification detection
Our approach

- Frontside partial reverse engineering on CHIP A
- Backside precise laser fault attack on CHIP B
We remind that we only recover the transistor’s active region, we don’t know the function of each gate.

Flip flops may have the largest number of transistors, this is the main assumption taken.
Manufacturing flow add-on

- Methodology

  S1. Chip Preparation

  S2. Image Acquisition & Registration

  S3. Hardware Trojan Detection

  - D1. Detection by correlation with a golden circuit
  - D2. Detection by correlation with GDSII file
  - D3. Detection by correlation with a text CAD file

- Only picking up non functional circuits from the wafer
Access to 2 circuits from ETH Zurich, a genuine and a second one with a HT.

A denial of service is triggered once a specific value is present in a 32 bits counter.
Another view of the different layers
After a frontside preparation developed

- Another view of the different layers

- No direct information on standard cell; poly (T-gates) and Metal1 are removed!
Frontside sample preparation full process

- At polyimide layer

- At active area
Automatic acquisition and registration

- SEM acquisition routine and offline image registration based on phase transform algorithm

Area of interest definition and scan recipe

Acq. 1 + Acq. 2 = Acq. 1&2
Automatic acquisition and registration

- Alignment artefacts with SEM software

Proc. 1: Proprietary

Proc. 2: Offline
Partial reverse engineering for Hardware Security

- Ultra cheap, low cost and efficient sample preparation
- For attack positioning or malicious circuit modification detection
Hardware AES example – Differential Fault Attack

Pattern recognition of flip flop gates and fault sensitivity map

Is a single shot enough? Is it precise enough?
Forcing bits by laser spot location

Blue: ‘0’ to ‘1’ sensitive position, bit-set
Orange: ‘1’ to ‘0’ sensitive position, bit-reset, gray: no effect

One shot over one position forces a bit to one distinct value

Init at “0000 0000”
Init at “1111 1111”
Both mapping
Forcing bits by laser energy level

Blue: ‘0’ to ‘1’ sensitive position
Orange: ‘1’ to ‘0’ sensitive position, gray: no effect
Register initialized at ‘00001111’

Targeting the zone with this energy leads to clear the register
Low-cost, fast, efficient and industry compliant
Applied with success over different circuits
Characteristics of SEM make them a tool of choice (low rent cost, accessibility, large area compliant, automating)
Destructive but manufacturing yield not impacted
Require a reference (but can be a design file)
SEM for laser fault attack conclusion

SEM image of a full synthesized logic can be used as reference

Correspondence between the SEM information and the functional chip is made by an infrared camera

Laser sensitive area matches with underlying hardware presence

A single bit set or bit reset can be obtained in a 90nm register depending on the beam energy or the beam location

- ‘1 to 0’ transitions are present over NMOS transistors
- ‘0 to 1’ transitions are present over PMOS transistors
Image processing need

Chemistry robust

Comply with computer design principles

The goal being not to have false positive
Statistical analysis

Area, size, dependancies, number of occurences

=> hypothesis on functions

Correlation with available information (datasheet, certification, side-channel, chip version)
As an example of application

What are the changes?

Automatic approach
Difficulties/Countermeasures?

Time to image on standard SEM, manual only contrast/brightness modification.

Metal layer programmable device
Conclusion
SEM for hardware security conclusion

- Fast, low-cost, reliable, efficient, automatic, in-house
- Memory content extraction is also key
- On-going analysis (processing tool, open analysis)
Thank you for your attention

@FranckCourbon