The state-of-the-art in Semiconductor Reverse Engineering at Chipworks

Randy Torrance
9th September 2009
Agenda

- About Us
- The What and Why of Reverse Engineering
- Product Teardowns
- System Analysis
- Process Analysis
- Circuit Analysis
- Putting it all together: A Case Study
Chipworks

Chipworks is a reverse engineering services company, based in Ottawa, Canada, with offices around the world providing semiconductor companies with:

- **Technical Intelligence** to engineers and business unit managers to give you a technical view of your competition.

- **Patent Intelligence** to IP groups and law firms providing technical intellectual property services to support licensing negotiations and patent portfolio development.
Reverse Engineering – What is it?

- In the semiconductor industry, reverse engineering (RE) can be:
  - Product Teardowns – what chips are used
  - System Analysis – how chips are used
  - Circuit Analysis – how chips work
  - Process Analysis – how chips are built, and what are they made of
Reverse Engineering - Is it legal?

Reverse Engineering is protected by the Semiconductor Chip Protection Act:

Title 17. Copy rights

Chapter 9. Protection of Semiconductor Chip Products

906. Limitations on exclusive rights; reverse engineering; first

(a) Notwithstanding the provisions of section 905, it is not an infringement of the exclusive rights of the owner of a mask for –

(1) A person to reproduce the mask work solely for the purpose of teaching, analyzing, or evaluating the concepts or techniques embodied in the mask work or the circuitry. Logic flow, or organization used in the mask work; or

(2) A person who performs the analysis or evaluation described in paragraph (1) to incorporate the results of such conduct in an original mask work which is made to be distributed.
Why Reverse Engineer?

**Patent Intelligence:**
- To determine if others are infringing your patents
- To find prior art to invalidate others’ patents

**Technical Intelligence:**
- To benchmark your designs versus your competitors
- To see new and innovative techniques
- To understand best practices

**Verification:**
- To understand how secure your own chips are
The Start to Reverse Engineering

Product Teardown – example: Apple’s iPhone
iPhone Product Teardown - iPod board

- **Wolfson WM8758BG audio codec** (fabbed by TI)
- **STMicroelectronics LIS302D 3-axis MEMS accelerometer**
- **Samsung 64-Gb dual-stack package, multi-level cell NAND Flash memory** (same as 8-GB iPod)
- **Apple (NXP) power manager**
- **Apple/Samsung application processor with ARM 1176 core + 1 Gb mobile DDR SDRAM memory, package-on-package configuration**
Types of System Analysis

- **Hardware analysis:**
  - Reverse-engineering at the physical circuit or board level
  - Functional analysis using test stimulus and monitoring outputs and internal signals

- **Software analysis:**
  - Software reverse engineering involves extraction and reconstruction of embedded code
  - Software functional analysis
System Analysis - Hardware Reverse Engineering

- **Teardown device**
  - Screwdrivers, etc
- **Identify components**
  - Datasheets, web, part number decoders
- **Remove components**
- **Delayer boards**
  - Delayering station
- **Trace connections**
  - ICWorks (our circuit analysis software)
- **Schematic capture**
  - ICWorks, Cadence

- **Hardware Reverse Engineering**
  - Screwdrivers, etc
  - Datasheets, web, part number decoders
  - Delayering station
  - ICWorks (our circuit analysis software)
  - ICWorks, Cadence
System Analysis - Hardware Functional Analysis

For example: Discover how a digital camera works in order to prove use of invention

Examine patent...

...disassemble camera to get a dismembered but functioning camera...
System Analysis - Hardware Functional Analysis

...connect probes between the interfaces and a logic analyzer...

...create testbench and test vectors, test, collect waveforms, study the timing...

...and document the evidence
System Analysis - Software Reverse Engineering

Binary

Disassemble code...

Extract code...

‘C-like’ Code

Decompile code...

Assembler

chipworks.com
Process Analysis

- Look at the structure of a chip
- Identify the chemical make-up of the structure
- Estimate the process sequence
The “Rules” of Process RE

- We see what we see!
- We can’t see everything we want to see
- Sometimes we don’t know what we see!
- Sample preparation isn’t perfect – it can create confusing artifacts
- What we see doesn’t always agree with corporate marketing hype
- SEM/TEM calibrations are NIST/NPL traceable and +/- 5% accurate
Process Analysis – Sony’s Clearvid IMX013 4-Mpixel CMOS Image Sensor

Extracted from Sony DCR-DVD505 Handycam
Process Analysis – IMX013 Pixel Array – Plan View

SEM images of organic & nitride lenses
Process Analysis – IMX013 Pixel Array – Plan View

Metal 3

Metal 1

Metal 2

Transistors

Substrate Doping (SCM)
Process Analysis – Cross-Section of Pixel Array

Nitride lens

SEM

SCM X-section

M1

Transistor TEM
Circuit RE Flow

- Die
- Layers
- Annotate
- Schematic
- Netlist
- Analysis, Verification
- Reports + ICWorks
- Simulate

**NetlistSimulate**

- Die Annotate Schematic
Circuit Analysis – Package Removal

- Remove plastic packaging by placing sample in acid bath
- A variety of acids and temperatures are used depending on package type
Circuit Analysis – Delayering

- Take cross-section SEM photo to identify layers

- Recent challenges:
  - 45nm
  - Low-K dielectrics
  - High-K gates
  - Metal gates
  - Copper
  - Gold
  - Mixed metals
  - MEMs
  - Stacked die

Samsung 8-Gb NAND Flash Memory
Delaying

An example:

- Metals: Al, Cu, TiN, TaN
- Metal thickness: 0.15um to 1.4um
- Dielectrics: silicon nitride, oxynitride, oxide, SiOC, SiONC, and PSG
- Dielectric thicknesses: 47nm to 2.6µm

SEM cross-section of 65-nm TI baseband chip for Nokia
Circuit Analysis – Delayering

- Chose a technique and recipe, or develop a new one
- Remove layers one by one, typically via:
  - Reactive Ion Etching (RIE)
  - Inductively Coupled Plasma (ICP)
  - Micro-polishing
Delayering

- A sample is prepared for each metal interconnect layer, polysilicon layer and substrate diffusions.
  - e.g. for 6 metal layer device, need to prepare 8 samples
Delaying

Atheros AR5110 - Metal 5

Atheros AR5110 - Metal 4
Delayering

Atheros AR5110 - Metal 3

Atheros AR5110 - Metal 2
Delayering

Atheros AR5110 - Metal 1

Atheros AR5110 - Poly
Image Capture

- Capture high magnification images using microscope (SEM and optical), automated stage and digital camera
- Use software to stitch all the images together, and for inter-layer registration
Image Capture

Optical vs. SEM – e.g TI OMAP1310, 0.13µm process, transistor layer
- 450nm optical light just doesn’t cut it anymore
Circuit RE Flow

- Depot
- Delayering
- Imaging
- Stitching, Aligning
- **Annotation**
- Extraction, Analysis
- Schematic Entry
- Netlist
- Simulation
- Verification
- Reports
Annotation

The old days...
• Wires are traced on the layer where they appear
• Layers are all aligned and any can be visible
• All layers can be shown at side
**Annotation**

Annotations on each image layer → Correct interlayer registration → Fast, accurate circuit extraction
 Annotation – Polygon Feature Extraction

Raw M4 layer image
Annotation – Polygon Feature Extraction

Edge Detection
Annotation – Polygon Feature Extraction

Fill in polygons based on heuristics (size, brightness, color, etc.)
Circuit Analysis – Polygon Feature Extraction

- Rule-based DRCs can improve accuracy
  - E.g. small breaks in wires, floating or missing contacts

- Can move to centerline wires and point contacts

- Feature extraction challenges:
  - Visibility of other layers
  - Brightness variability
  - Sample prep artifacts
Further automation is possible after the feature recognition:

- After wires are annotated vias can often be placed automatically.
- Once a device is defined, identical instances of this device can be searched for and found using pattern matching image recognition.
- This is especially useful for digital logic.

Standard cell recognition
Circuit RE Flow

Depot

Delaying

Imaging

Stitching, Aligning

Annotation

Extraction, Analysis

Schematic Entry

Verification

Netlist

Simulation

Reports
Auto-extracted devices placed on schematic in same relative positions as the layout

However, this arrangement of transistors or gates does not convey a great deal of information, so...
The analysis phase:

- arranging the transistors and gates
- organizing a readable, hierarchical schematic set
- understanding the function and reason behind the design
Analysis

- **Tools**
  - Schematic organization can be done using the usual design schematic editors (e.g. Cadence Composer)
  - However, these tools tend to be optimized for forward design rather than reverse engineering
  - ICWorks Arranger is optimized for schematic organization from layout
    - Simple structures such as diff pairs and current mirrors can be found automatically
    - Subcircuits are easily grouped, created, and linked hierarchically
    - Subcircuit input devices can all be gathered with one keystroke
    - Identical subcircuits can be located and organized automatically
Analysis

- One instance defined manually, others matched and organized automatically

Example sub-circuit search and organization
Analysis

- Other inputs
  - Public information and datasheets can help with schematic organization
  - Technical papers and patents hold interesting clues
  - Floorplan and layout information can be very valuable
    - For analog circuits the layout often follows a logical progression
    - For digital... not so much
  - An experienced RE analyst is invaluable
Circuit RE Flow

[Diagram showing steps: Depot, Delayering, Imaging, Stitching, Aligning, Annotation, Extraction, Analysis, Schematic Entry, Verification, Netlist, Simulation, Reports]
Verification

- As with forward design, the first pass schematic is not always 100% correct
- However, in contrast to forward design, 100% correct is often not essential:
  - Clients are usually most interested in circuit structure
  - Device sizes only need to be approximate
  - Even if simulation is desired, we rarely have process models for competitive chips, and hence accurate device sizes are not critical
- Of course, device sizes can only be as accurate as measured from actual devices:
  - As measured on silicon, not mask sizes or layout database sizes
  - The process on any particular device could be anywhere between best and worst case
Verification

- Multiple techniques are available:
  - Redundant annotation
  - DRCs: floating wires and contacts, floating gates, shorted outputs...
  - Greater use of automated extraction tools
  - Our schematic editor flags errors whenever the connectivity is broken (connectivity derived from annotated images)
  - Simulation (either digital or analog)
  - Microprobing
  - And, of course, experienced analysts who can quickly see when a circuit makes sense, and when it doesn’t

![Diagram of Schematic Editor and Spice workflow](image-url)
Circuit RE Flow

- Depot
- Delayering
- Imaging
- Stitching, Aligning
- Annotation
- Extraction, Analysis
- Schematic Entry
- Verification
- Netlist
- Simulation
- Reports
Circuit Analysis - Deliverable

- Organized, readable, hierarchical schematics

- Optional Outputs: Netlists, simulated waveforms, micro-probed waveforms, block diagrams, timing diagrams, circuit equations
Chipworks ICWorks Browser

Interactive software application to view both schematics and images, and to pan, zoom, trace and bi-directionally cross-probe between the two.
Chipworks ICWorks Browser

Highlight and easily trace one or more circuit paths throughout the device’s layers (example shown – power routing)
Powerful Export Capability

Schematic Editors (EDIF200)

Netlist

ICWorks Browser

Simulate
Mixed Functional/Physical Chip Analysis

- Combine functional testing, physical extraction, and simulation to understand chip

- Result is not schematics, but specific understanding of a chip, such as a portion of a datasheet or functional specification

- Powerful method of understanding complex chips and SOCs using many RE techniques together to complement each other

- Can be useful for chips with hardware security and encryption also
Mixed Functional/Physical Chip Analysis

1. Depot, Delayer, Image
2. Annotation
3. DRC, Netlist
4. Partial Schematic Org
5. Run System, Collect Test cases
6. Build Test Bench
7. Simulate
8. Monitor key blocks
9. Analyze Results
10. Collect Functional and Datasheet Information
Case Study

- Goal: to understand a mixed analog digital ASIC with embedded SRAM, ROM and EEPROM, and a hardware encryption algorithm running on-chip.
- Interface to chip was an unknown encrypted protocol.
- Many techniques need to be utilized.
- Step one: Depot, delayer, image, stitch, and align.
Case Study

- Annotate, Design rule checks
Case Study

- Export to flat un-organized schematic and netlist
Case Study

- Do limited schematic organization, often to find specific functions
  - In this case we found a 56-bit register, very interesting...
- Usually the analog logic is more fully organized than digital
Case Study

- From the functioning system with the chip, collect waveforms and hence test case vectors
- Inputs to chip form test vectors, outputs can be used to check accuracy of netlist
Case Study

- Run top level test cases captured from system to verify and debug the netlist
- In this case we found the netlist simulated fine, and the outputs of the netlist simulation matched the actual chip outputs up to a point
- At that point nothing matched, likely the chip started encrypting its responses
- The matching outputs up to that point indicated that our netlist was at least fairly accurate
Case Study

- We assumed encryption keys were stored on the chip in the EEPROM, and with these we thought we may be able to get vectors to match... but how to get the keys
- SRAMs can be modeled, or netlisted directly
  - They hold no non-volatile data
- Most ROMs can be read directly via physical RE methods (e.g. the M1 programmed ROM below), then modeled in the netlist
There are many possible methods for reading on-chip EEPROMs
- Sometimes test modes can be discovered to read these
- Other times microprobing can help
- Chip microsurgery using focused ion beam (FIB) is also possible
**Case Study**

- **Step 1: what modes exist:**
  - In this case our circuit analysis revealed 3 modes on this chip: normal, scan, and built in self test (BIST)
Case Study

- We considered using a test mode to read the EEPROM, however
  - BIST only returned a PASS or FAIL, no data
  - Scan did not run through the EEPROM data, but did allow access to most registers
- Another option: load data and control using scan, then switch to normal mode to read memory, then switch back to scan to read out memory
  - However, the only way to switch modes was to power down, erasing the state just set
- Solution: FIB microsurgery to enable switching modes while powered
Case Study

- We then took a few chips and:
  - Jet-etched the package off, leaving the chip operational
  - Removed the top layer of glass
  - Cut some on-chip wires, and added others
- Through analysis of the extracted schematics of the EEPROM access circuits and digital logic, determine the state required to read the EEPROM
- Using our altered chips, load in this state through the scan path, switch to normal mode to read EEPROM, and switch back to scan to read it out.
- Success: the EEPROM was read
- Next this memory data is added to our model of the chip
Case Study

- Now we could run top level test cases captured from system using our extracted keys: success, the outputs of simulation matched the captured system data
- Now we can also create new test cases if desired
- The full netlist means that all nodes in the chip are observable!

```verilog
// File        : Dig_Top_TB.v
// Generated   : Tue Jan 20 11:39:10 2009
// From        :
c:\Dig_Top\TestBench\Dig_Top_TB_settings.txt
// By          : tb_verilog.pl ver. ver 1.2s
//
```

```verilog
module Dig_Top_tb;
//Internal signals declarations:
wire X24_Z;
wire X37_Z;
wire X100_Z;
```
Case Study

- Results of sims can be used to understand functions
- And datasheet type information can be collected
Summary

- I have reviewed the reverse engineering of electronic systems, circuits, and component structures.
- RE of semiconductors requires state-of-the-art, leading-edge equipment.
- There are many different techniques used to understand chips.
- It is possible to extract operational and manufacturing information as well as system, circuit, and process.
- Chipworks uses all these methods to gain an understanding of how chips work.
I would like to thank Chipworks’ laboratory staff and analysts, who actually do all the hard work of analyzing these complex devices. They do a great job!