CSCI 4974 / 6974
Hardware Reverse Engineering

Lecture 1: Course Introduction

Today

- Course overview
- Motivation
- Legal / ethical issues
- Introduction to switch model of CMOS logic

Course info

- Website: http://security.cs.rpi.edu/courses/hwre-spring2014/
- TA: Andrew Zonenberg <azonenberg@drawersteak.com>
- Classes: Tues/Fri 2:00 - 3:50
- Lectures in Low 3130
- Lab locations vary depending on work to be performed

Prerequisites

- Basic understanding of Boolean algebra and logic gates
- Lack of EE background is OK, our analysis is qualitative only
- Class is self-contained, we will introduce background material

Web resources

- http://www.siliconpr0n.org/wiki/
  Online encyclopedia of hardware RE
- http://www.siliconpr0n.org/archive/
  Database of die images, RE reports, etc
- Run by John McMaster '10
- Disclaimer: RPI is not affiliated with either site, however I personally contribute material to both frequently and use their content in my lecture notes

Software

- Schematic capture for drawing circuits
  - KiCAD is my tool of choice
- Image editors
  - Inkscape is good for netlist/cell tracing
  - GIMP is good for editing etc

Grading

- Four equally weighted parts
  - Quizzes
  - Labs
  - Homework
  - Project

Quizzes

- 15 minutes, roughly once a week at the start of class
- Covers most recent material
- Work individually
- Computers OK, but no network access allowed
- 1-2 questions, focus is on at-a-glance basic concepts

Labs

- About once a month
- Demo of sample prep, data capture, etc
- May include hands-on component
- Write 1-2 page report after each lab

Homework

- Simple analysis projects
- Given part of a real-world system, tell me what you can about it
- Collaboration with classmates OK, but submit separate answers
- Outside resources OK (cite!), but no help from non-students

Project

- Teams (size TBD)
- Larger-scale analysis of portions of a commercial IC
- Create gate-level schematic
- Figure out what it actually does
- Write a report on your findings

Other notes

- .doc, .ppt, and friends are evil
- Send me PDF for documents etc
- Inkscape SVG preferable for tracings (embed images!)

Topics: chip level RE

- Photos to vectorized layout
- Layout to transistor-level schematic
- Transistors to gates
- Figuring out what groups of gates do
- Floorplan analysis, vendor ID, misc.

Topics: board-level RE

- Component identification (including unmarked/rebranded)
- Bus identification
- Firmware dumps
- Ties into chip-level stuff for defeating anti-RE

Legal issues

- Semiconductor designs are protected by copyright
- Mask copyright only lasts 10 years
- Cloning chips is not allowed but analysis is explicitly OK
- United States Code, title 17, section 906:
  “it is not an infringement ... for a person to reproduce the mask work solely for the purpose of teaching, analyzing, or evaluating the concepts or techniques ... or the circuitry, logic flow, or organization of components used in the mask work

Legal issues

- Firmware has same copyright protection as any other software
- Patents have no effect on reverse engineering, but may keep you from being able to use what you find
- If in doubt, talk to company legal counsel etc

Ethical issues

- Consider impact of releasing sensitive data
- Class discussion

Motivation

- Why are we even doing this again?

Supply chain verification

- You've just bought 10,000 of some part from a sketchy vendor.
- Are they actually what they say they are?
- Cannot detect “new is really used” or speed grade mis-marking
- But can easily ID entirely wrong components

Component ID for PCB RE

- You're reversing a PCB and find an epoxy glob-top
- Or maybe the part number was just sanded off
- Hard to do much until you know what the part is

Litigation

- Competitor Inc. sells a product that seems identical to yours.
- You suspect they copied your firmware, patented algorithm, etc.
- Can you prove it to a judge?

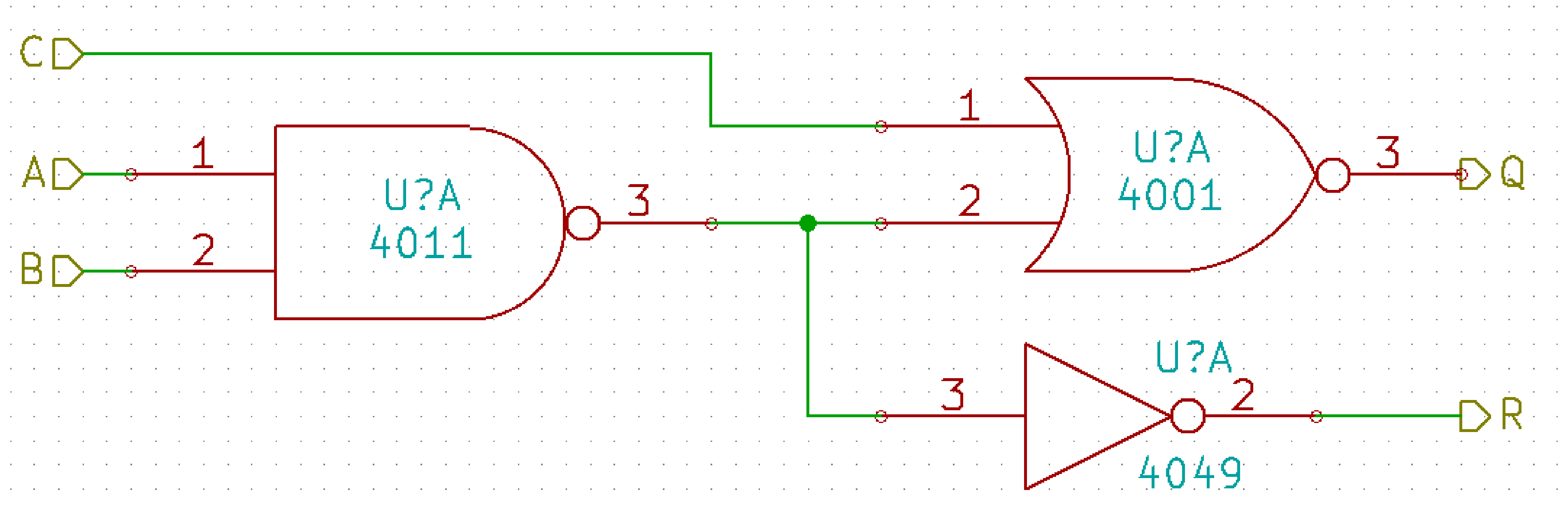
Competition

- Competitor Inc. came out with a better widget.
- What makes it harder/better/faster/stronger?
- Can you study their design to make yours better (without actually copying it exactly)?

Idealized circuit model

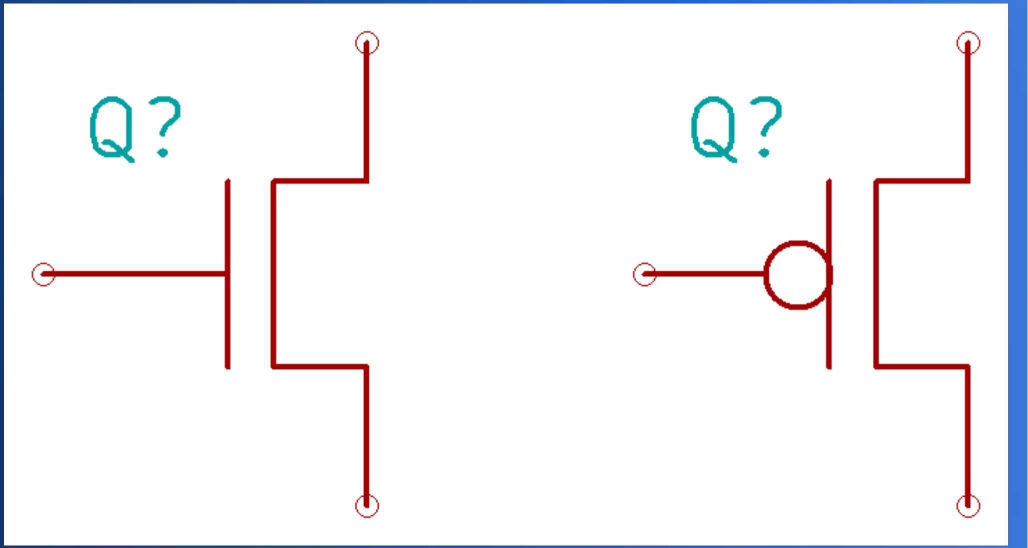
- Real wires are full of nasty RLC parasitics.
- Real transistors take time to switch and have Rds(on).
- Lots of other subtleties involved in designing ICs
- But we know the chip works, so we can forget about all that ;)
- Except in rare exceptions (DRAM, old-school dynamic logic) we can just do RTL modeling

Circuit schematic review



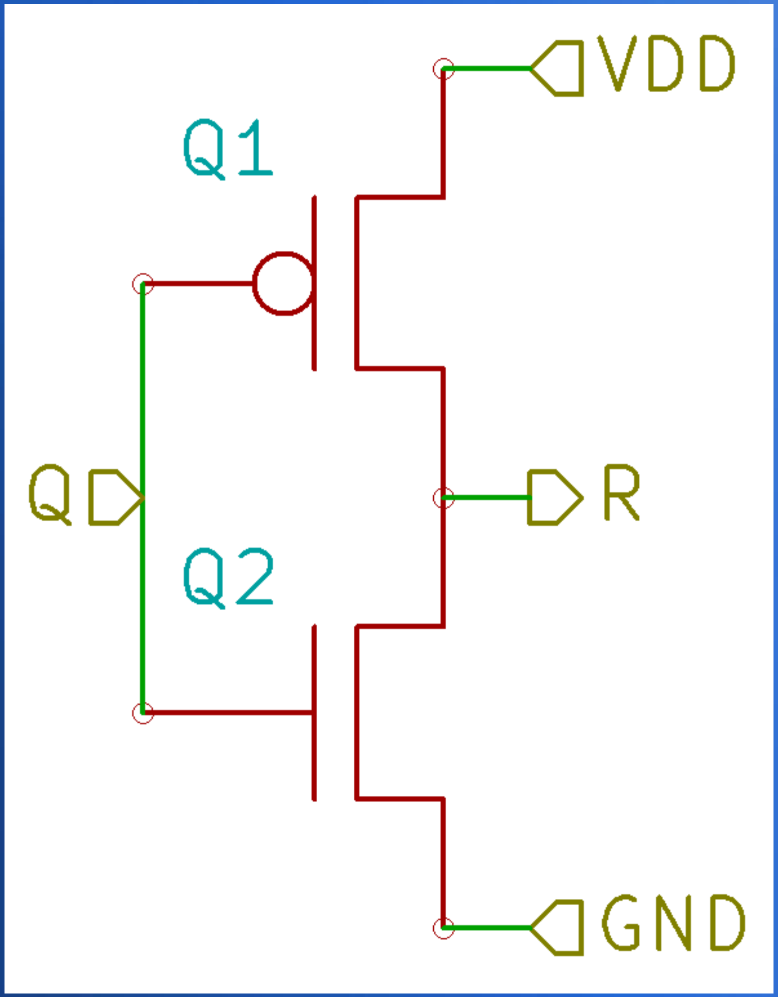
Switch model of transistors

- For the scope of this class, a transistor is a switch.
- Source/drain path switched on/off by gate
- Analog effects, body diode, etc irrelevant for digital CMOS RE
- NMOS (left): normally open
- PMOS (right): normally closed
- Several alternate symbols



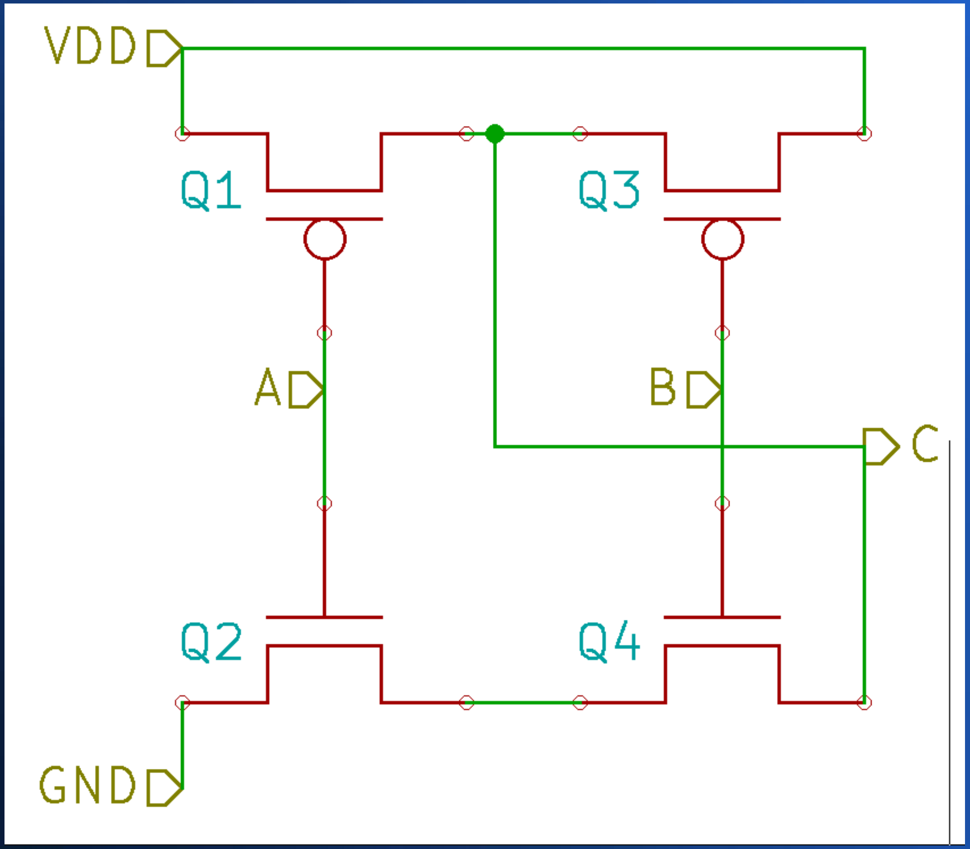
CMOS

- “Complementary” MOS
- Pair a NMOS and PMOS together
- PMOS pulls high, NMOS pulls low
- Only one is ever on at a time
- Vdd/Vss labeling



More CMOS gates

- What does this one do?



KiCAD

- Open source (GPLv2) electronics CAD tool
- http://www.kicad-pcb.org/
- We will be using it for drawing schematics
- Can be used for PCB layout, but we won't do that in this class
- You should all install it by next class
- Optional: Download my CMOS library (link to be posted)
- In-class demo

Questions?

- TA: Andrew Zonenberg <azonenberg@drawersteak.com>