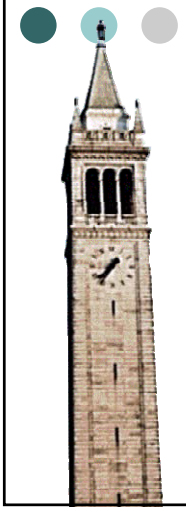


Fundamental Algorithms for System Modeling, Analysis, and Optimization

Edward A. Lee, Jaijeet Roychowdhury, Sanjit A. Seshia
UC Berkeley
EECS 144/244
Fall 2011

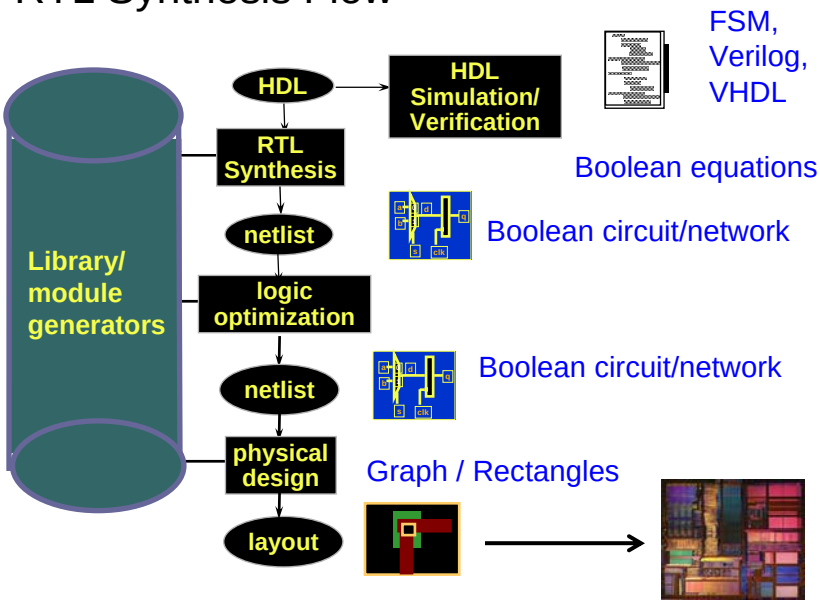
Lecture 2: RTL Design Flow

Register Transfer Level (RTL)

A level of abstraction for describing a digital circuit's behavior

Circuit's behavior described in terms of flow of signals between hardware "registers", and the logical operations performed on those signals.

RTL Synthesis Flow



Example: (Hardware) Electronic Voting Machine

C. Sturton, S. Jha, S. A. Seshia, D. Wagner,
On Voting Machine Design for Verification and Testability, ACM CCS 2009.

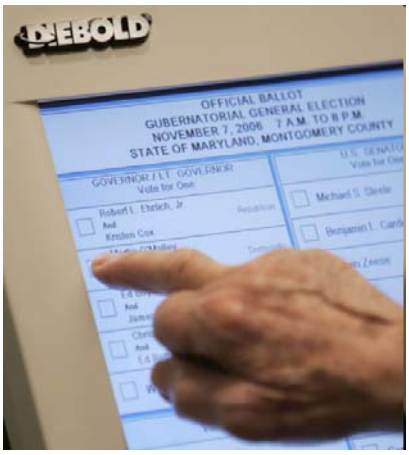
http://uclid.eecs.berkeley.edu/vvm/

Direct Recording Electronic Voting Machine

Contest: a particular race on the ballot
- E.g., Presidential
- *k* choices, pick *ℓ*

Voter session: a sequence of contests
- Navigate back and forth

Cast: commit all choices for all contests
- The last step of a voter session



uspolitics.about.com

Voting machines in the news

Can You Count on Voting Machines?
"Sliding finger bug on the Diebold AccuVote-TSX … machine would crash every few hundred ballots"
The New York Times Magazine. Jan 6, 2008.

Fairfax Judge Orders Logs of Voting Machines Inspected
"Voters complained that the machines were failing to register their votes for incumbent school board member"
Washington Post. Nov. 6, 2003.

Jefferson County Voters Continue To Raise Concerns About Voting Machines
"…voters complained that when they selected a particular candidate, another candidate's name would light up."
KDFM-TV Channel Six News. Oct. 28, 2006

Election officials would like to use electronic voting machines

- Configurable for different elections
- Provide usability features
  - Alternate input devices
  - Alternate languages
- No ambiguities in cast ballots

Using electronic voting machines introduces concerns about correctness

- Complex programs, hundreds of thousands of lines of code
- Buggy code can introduce errors
- Malicious code can allow attacks
- Incorrect code can lead to lost, mis-recorded, or altered votes

Our Paper

- We show that testing by humans plus formal verification can prove a voting machine will work correctly on election day
- We implement a simplified voting machine in *hardware* and prove its correctness
  - We implement a direct recording electronic voting machine (DRE) synthesized onto an FPGA --- *an example of the RTL design flow!*
  - Verification by *Model checking* and SMT solving
  - Polynomial number of tests
- See my CITRIS seminar talk for a gentle intro:
  http://www.youtube.com/watch?v=VUyfi6JJRgA

Remainder of RTL Flow lecture done on the whiteboard