Hardware Security -- IP Protection

Cybersecurity Specialization

What Do We Expect to Learn?

- Design intellectual property (IP)
- Self-protection methods for design IPs
  - Watermarking, fingerprinting, metering, obfuscation
- Tradeoff assessment
  - Security, cost, performance
- Background:
  - Basic digital logic design
  - Graph coloring and graph partitioning

Intellectual Property

- Intellectual property is an original idea which can be used to earn money.

  The person or group who is recognized as having the idea can use the law to prevent other people from earning money by copying it.

  (from *Cambridge International Dictionary of English*)
- IP: product, technology, software, …
- Law protection: patent, copyright, trade secret, etc.

What Are VLSI Design IPs?

- IP is a design unit that can be reasonably viewed as a stand-alone sub-component of a complete SOC design.

  (from *Reuse Methodology Manual*)
- Design IP: any innovation and technology that makes design better.
  - Design algorithm, technique, methodology
  - Microprocessor, memory, Verilog chip description
- Virtual component, block, core, macro, …

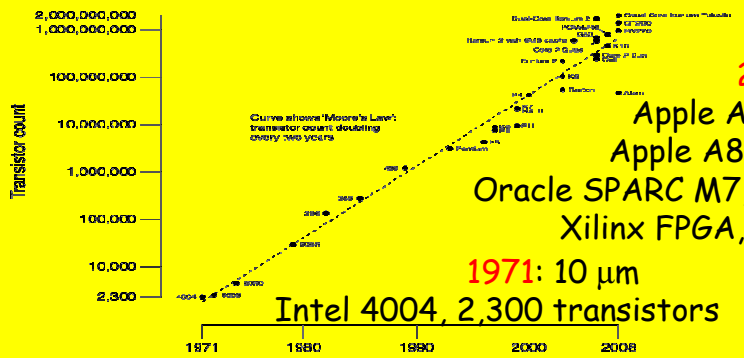
Soft, Firm, and Hard Design IPs

- Hard IP:
  - Examples: GDSII file with test lists and high level model, custom physical layout, fully placed and routed netlist for specific technology library
  - Predictable (optimized) performance, not flexible
- Soft IP:
  - Example: synthesizable HDL source code
  - Very flexible, unpredictable performance
- Firm IP:
  - Examples: placed RTL sub-blocks, fully placed netlist for a generic library.

Why IP and IP Protection?

- Design productivity gap: *what can be built and what can be designed.*

CPU Transistor Counts 1971-2008 & Moore's Law



2014: 20 nm
Apple A8, 2 billions
Apple A8X, 3 billions
Oracle SPARC M7, >10 billions
Xilinx FPGA, >20 billions

1971: 10 μm
Intel 4004, 2,300 transistors

Source: http://en.wikipedia.org/wiki/Transistor_count

Why IP and IP Protection?

- Design productivity gap: *what can be built and what can be designed.*
- (IP) Reuse-base design
  - VSIA, VCX
  - Design and Reuse
  - IP-Highway
- Hardware IP Piracy
  - Reverse engineering
  - Chip overbuilding
  - Counterfeiting

Goals of IP Protection

- Enable IP providers to protect their IPs against unauthorized use
- Protect all types of design data used to produce and deliver IPs
- Detect use of IPs
- Trace of IPs

Source: VSIA white paper on IPP

IP Protection: State-of-the-Art

- Deterrent: patent, contract, legal enforcement, partnership, …
- Protection: encryption, chemicals, obfuscation, dedicated hardware, …
- VSI tagging standards: Hard IP, soft IP

- Detection:
  - Digital watermarking
  - Digital fingerprinting
  - IC metering