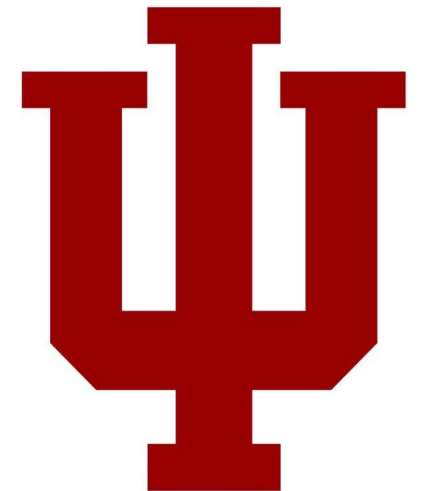


Work on project 4!

Exam Review

Engr 399/599: Hardware Security
Andrew Lukefahr
Indiana University



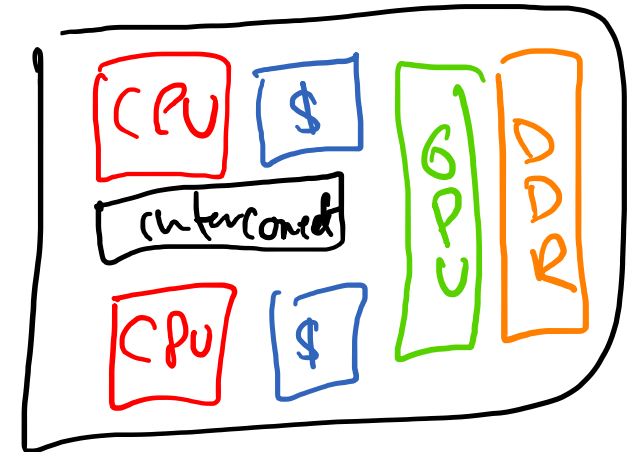
Adapted from: Mark Tehranipoor of University of Florida

Exam Style

→ short answer questions →
similar to review

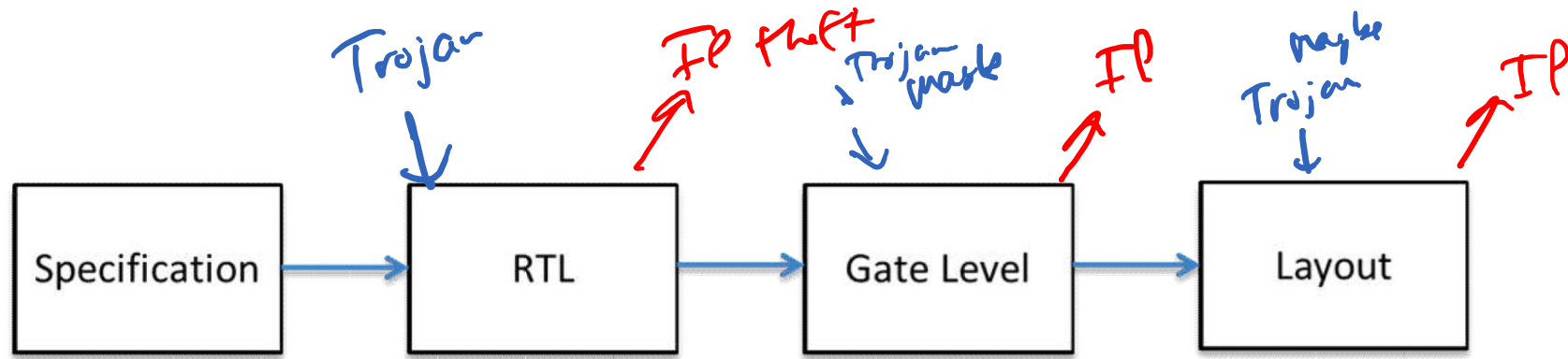
S-B questions

1 page "cheat sheet" → handwritten
front + back



Hardware Design

- What are the security vulnerabilities in each step of the design flow?

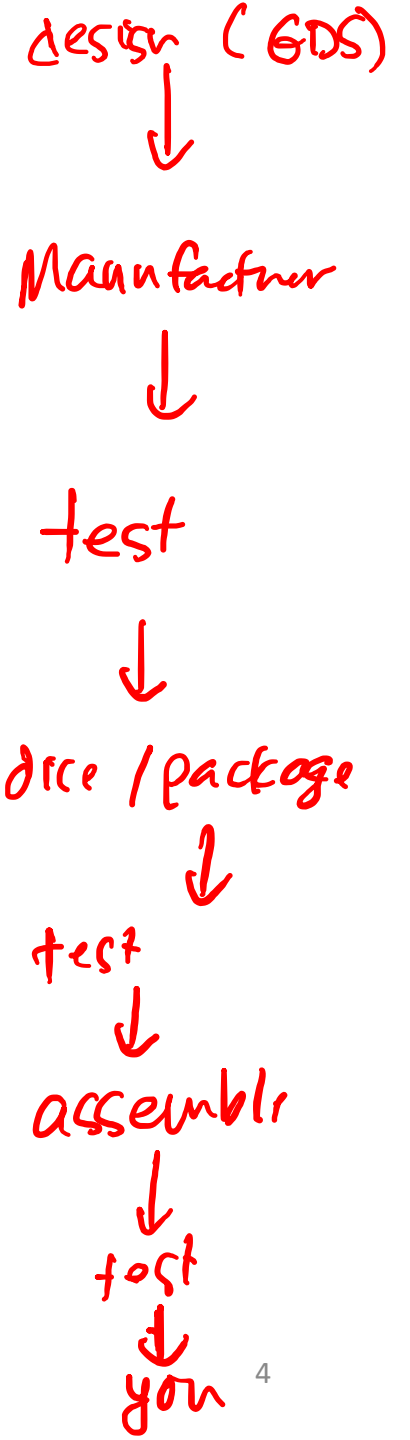


- Where are individual companies involved in the design flow?



Hardware Manufacturing

- Describe a typical hardware manufacturing / testing flow.
- What is Yield?



Cryptography

- What is the difference between symmetric and asymmetric cryptographic ciphers?
- How is a Caesar cipher vulnerable?

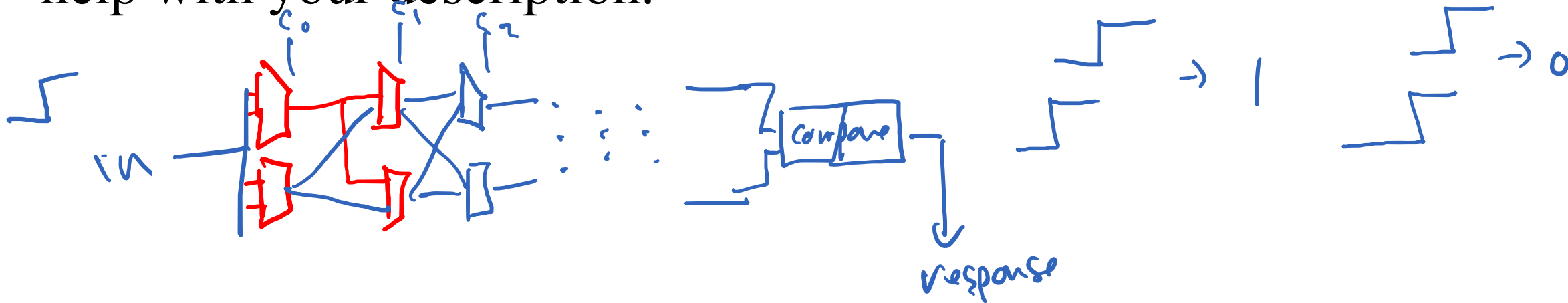
PUFs

- What is a PUF? What does it do?

chip specific
↓
unique output for each input

physical HW-based one-way function

- How does an arbiter PUF work? You can include a diagram to help with your description.



Hardware Metering — prevent over-manufacturing

- Give a method of passive metering?

Serial #, unique chip ID

- Give a method of active metering?

logic locking

Watermarking

- What is Watermarking?

secret identifier in your design

- Name and explain a digital IP watermarking technique?

- Apple ROM

- Out-of-spec inputs → predictable outputs

- Scan-chain values

Physical Attacks

- Name the 3 different Physical attack classes.

Non-invasive

don't tear apart
still works

- Give examples of each

temp - variation

side-channel

clock faults

Semi-invasive

some tear,
still works

etch + pictures

etch + laser fault

etch + probe

Invasive



tear apart
Not works after

delayering

Fault Injection

- How does a fault injection attack work?

- What are some of the ways to inject faults into a circuit?

clock 
temp
voltage 
laser - non-invasive
or
semi-invasive






Side-Channel Analysis

- What is the difference between Simple Power Analysis and Differential Power Analysis?

SPPA: measuring power differences between 2 inputs
→ control dependence / differences
→ if/else dependence

DPA: measuring power differences between 2 inputs
→ data dependent
→ computational dependent
→ model "referenced"

+1 
t2 



Hardware Trojans

- What is a hardware Trojan?

malicious modification to prevent normal functionality

- Why are they difficult to using test patterns that are used to detect faults.

designed to be difficult to "activate"