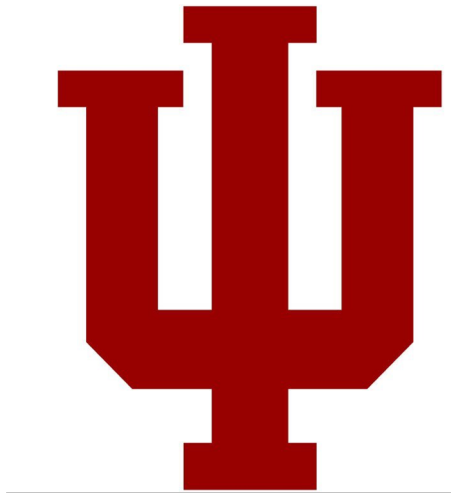
# Hardware Security Papers

Engr 399/599: Hardware Security

Andrew Lukefahr
*Indiana University*



Adapted from: Mark Tehranipoor of University of Florida

# Course Website

## engr599.github.io

- Write that down!

# Exam

- 83% Average (Pre-curve)
- Curve
  - +10% for Undergraduate
  - +5% for Graduate

# The difference between asymmetric and symmetric crypto?

# What is a cryto processor and why do we rely on them?

# What is a Physical Unclonable Functions (PUF)? Describe two issues associated with PUFs

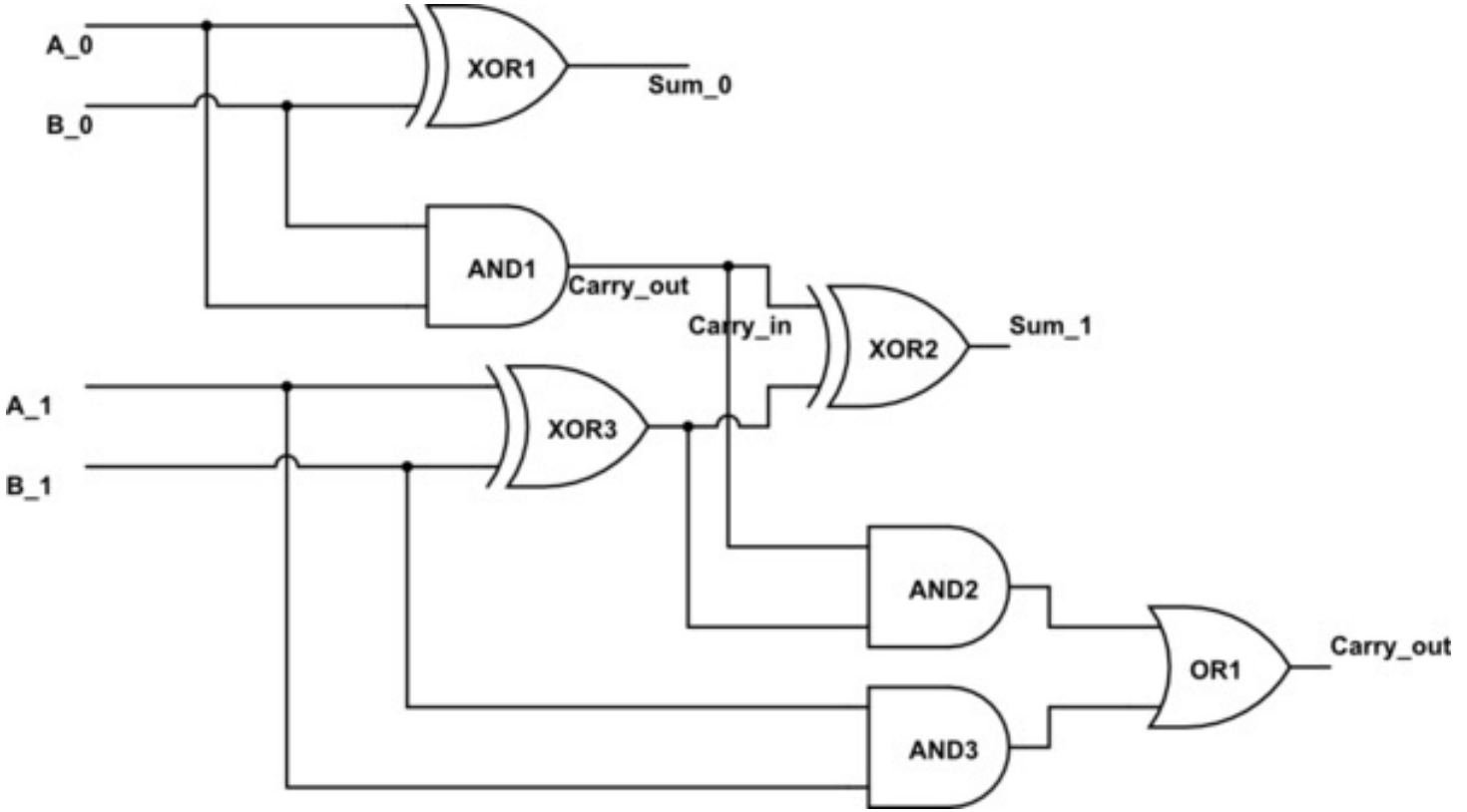
# Describe a method for calculating a true random number?

# Difference between non-invasive, semi-invasive, and invasive physical attacks.  Give an example of each

# Explain how one can detect a hardware Trojan using transient power analysis?

# Explain how Differential Power Analysis can be used to recover secret information?

# In the following design, insert a Trojan that is difficult to detect



# Paper Presentations

# Each Group gets to present 2 papers

- We'll pick them in a little while.
- From suggested list, exceptions possible

# Non-presenting individuals:

- Read 1 of the 2 papers before class
- Submit short write up to canvas
- Come to discuss

# Canvas Writeup (1 sentence/ question)

- What's the problem?
- Why is it important?
- What did this paper do about it?

# Presenting group

- ~~45~~ 20 minute presentation (!!!) +5 minutes for questions
- ~~Shared between the 3 of you~~ Not shared

# Suggested Presentation Slides

- Title – 1 slide
- Big Picture – 1 slide
- Overview – 1 slide
- Intro – [illegible] slides 3
- Overview – 1 slide
- Meat – [illegible] slides 10
- Overview – 1 slide
- Results/Graphs – [illegible] slides 3
- Overview – 1 slide
- Conclusions – [illegible] slides 2 slides

# Title – 1 slide

- Paper title
- Paper authors

- Presentation authors

# Big Picture – 1 slide

- What's the problem?
- Why does it matter?
- What are the author's going to do about it?

# Overview – 1 slide

- Introduction
- Meat
- Results
- Conclusions

# Introduction – 7 slides

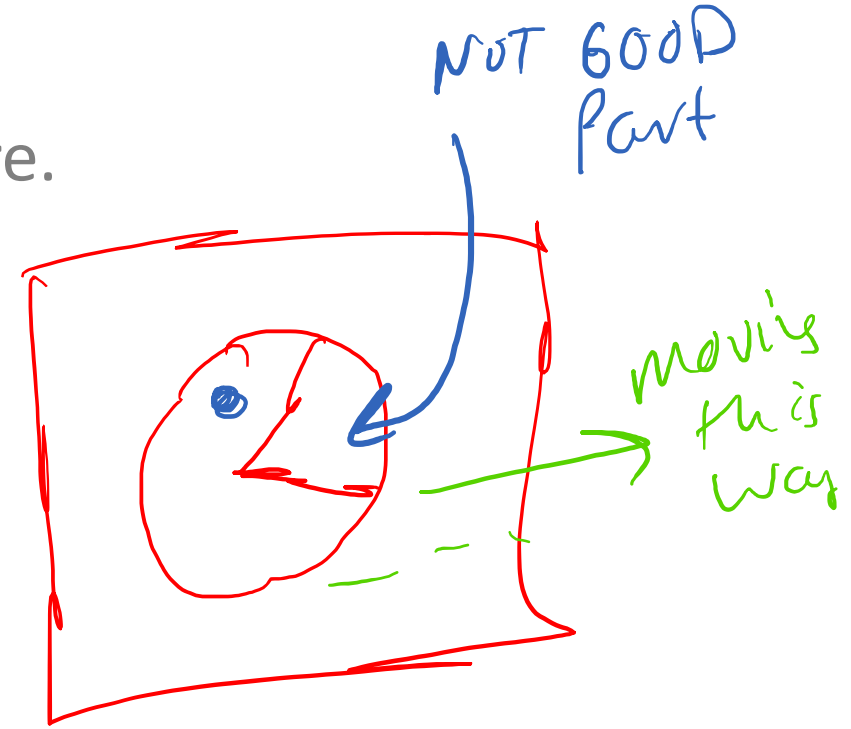
- How did we get here?
- Why is this problem important to solve?
- What background do I need to know?

# Overview – 1 slide

- Introduction
- Meat
- Results
- Conclusions

# Meat – 20 slides

- What does the system work?
- Figures / Diagrams are helpful here.
- Sub-sections are also useful.



# Overview – 1 slide

- Introduction
- Meat
- Results
- Conclusions

# Results / Graphs - 5 slides

- Does it work?

# Overview – 1 slide

- Introduction
- Meat
- Results
- Conclusions

# Conclusion – 1 slide

- What did I learn?
- What do you (presenter) think of paper?
- What do you (presenter) think we should do next?

- Starbleed (2019) - https://www.usenix.org/conference/usenixsecurity20/presentation/ender
- MORPHEUS (2019) - https://web.eecs.umich.edu/~barisk/public/morpheus.pdf
- Side-Channel Analysis of the Xilinx Zynq UltraScale+ Encryption Engine (2021) - https://pdfs.semanticscholar.org/100d/983ed1192e1274dd71558eef30b352fa0dc5.pdf
- Insights into the Mind of a Trojan Designer (2019) - https://arxiv.org/pdf/1910.01517.pdf
- FLATS: Filling Logic and Testing Spatially for FPGA Authentication and Tamper Detection (2019) - https://ieeexplore.ieee.org/abstract/document/8741025

VoltPillager: Hardware-based fault injection attacks against Intel SGX Enclaves using the SVID voltage scaling interface (2021) - https://www.usenix.org/conference/usenixsecurity21/presentation/chen-zitai

Self-Encrypting Deception: Weaknesses in the Encryption of Solid State Drives (2019) - https://ieeexplore.ieee.org/abstract/document/8835339

Golden Gates: A New Hybrid Approach for Rapid Hardware Trojan Detection using Testing and Imaging (2019) - https://ieeexplore.ieee.org/document/8741031

Toward a Hardware Man-in-the-Middle Attack on PCIe Bus for Smart Data Replay (2020) - https://ieeexplore.ieee.org/document/8875023

On the Usability of Authenticity Checks for Hardware Security Tokens (2021) - https://www.usenix.org/conference/usenixsecurity21/presentation/pfeffer

A2: Analog Malicious Hardware (2016) - https://web.eecs.umich.edu/~taustin/papers/OAKLAND16-a2attack.pdf

Spectre Attacks: Exploiting Speculative Execution - https://ieeexplore.ieee.org/document/8835233

| | | |
|---|---|---|
| 11/08 | Monday | Today |
| 11/10 | Wednesday | No class Will ① |
| 11/15 | Monday | Chris ⑥ Trey ⑧ |
| 11/17 | Wednesday | |
| 11/22 | Monday | NO CLASS |
| 11/24 | Wednesday | NO CLASS |
| 11/29 | Monday | Jack ② Yifan ⑦ |
| 12/01 | Wednesday | Max ③ Michael ⑤ |
| 12/06 | Monday | Austin ④ Clare ⑨ |

SSD's

No Class

- Clare:  A2
- Trey: Side Channel
- Yifan:  Trojan Designer
- Chris:  Spectre
- Michael:  Morphius
- Austin:  FLATS
- Max: VoltPillager
- Jack: Starbleed