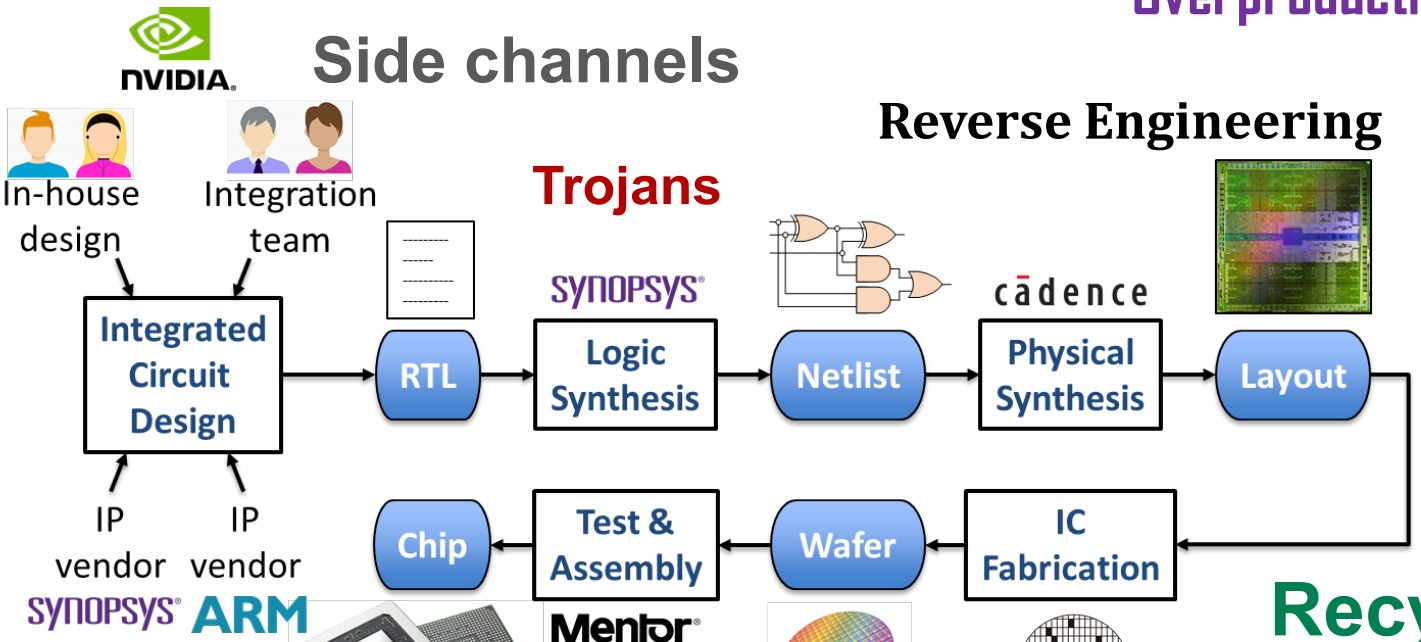
Carnegie Mellon University

Characterizing Hardware Security

Shawn Blanton

Trustee Professor in Electrical and Computer Engineering

Integrated Circuit Design Flow



Carnegie Mellon University

Security Desires for Hardware

Obstruction: Do not use my circuit.

Confidentiality: My circuit function is unknown.

Corruptibility: My circuit operates incorrectly when use is unauthorized.

Integrity: Do not alter my circuit.

Existence: There is no circuit.

Goal: Metrics for comparison of security-enhancing techniques.

Carnegie Mellon University

Security Metric Challenges

Why is it challenging to develop security metrics for hardware?

- Defining security is challenging because attack vectors are ever changing.
- Conventional hardware metrics (volume, area, power, performance, etc.) are static.
- Security metrics are not static: new attack can instantly change security from high to low.

CMU Hardware Security Metrics

Two examples of metrics under development:

Confidentiality: My circuit function is unknown.

Corruptibility: My circuit operates incorrectly when use is unauthorized.

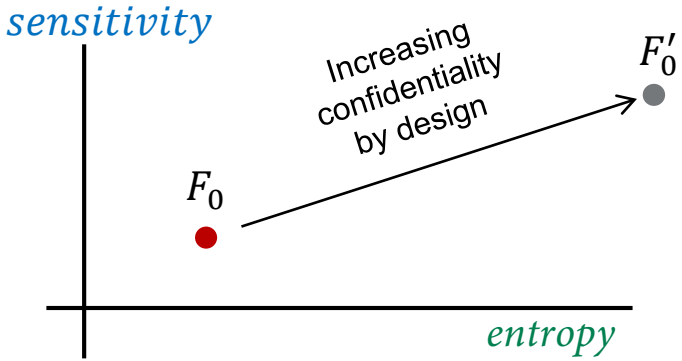
***Important*: Metric values can change over time.**

Confidentiality ≡ circuit function is unknown!

Metric requirements:

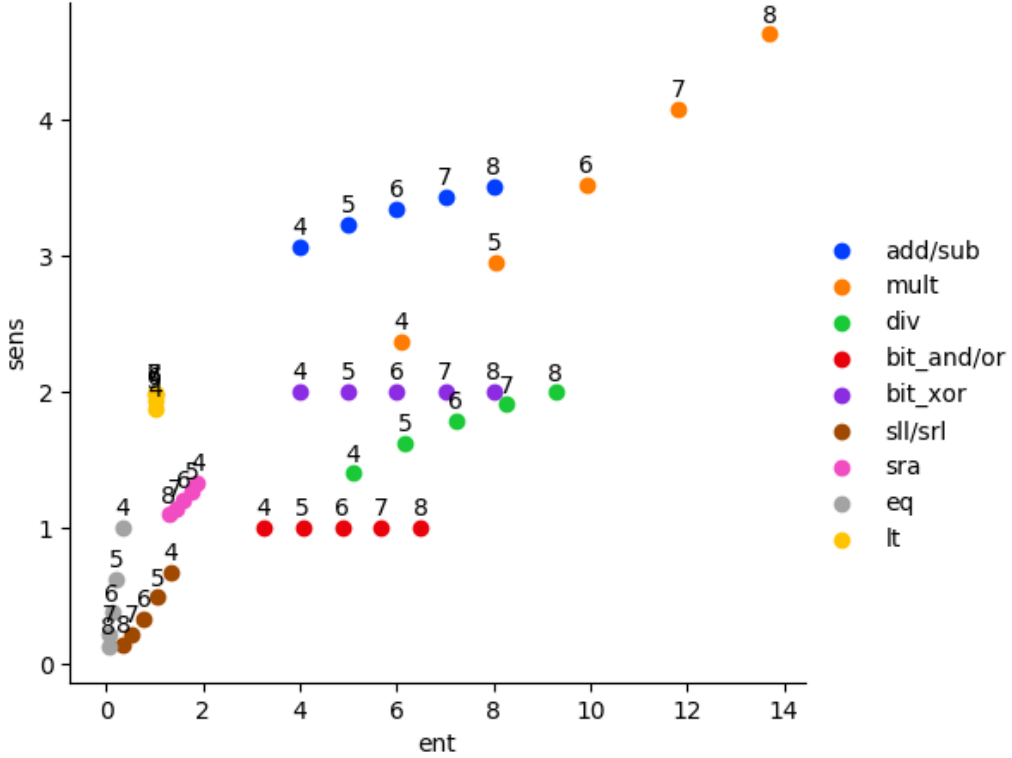
- Should be independent of physical implementation.
- Functions of different “sizes” (e.g., 8-bit adder, 16-bit adder, etc.) should have similar metric values.
- Ideally, should be easily altered through design to increase confidentially.

- Sensitivity = likelihood that an input controls a given output
- Influence = average sensitivity
- Entropy = distribution of output values



Carnegie Mellon University

Sensitivity and Entropy, are they sufficient?



Carnegie Mellon University

On-Going Work

- Measuring sensitivity, entropy, etc. for large circuits is not trivial.
- Extending the CMU metrics to sequential circuits.
- Design approaches for trading off the security with conventional PaP.
- Understanding impact on global supply chain.