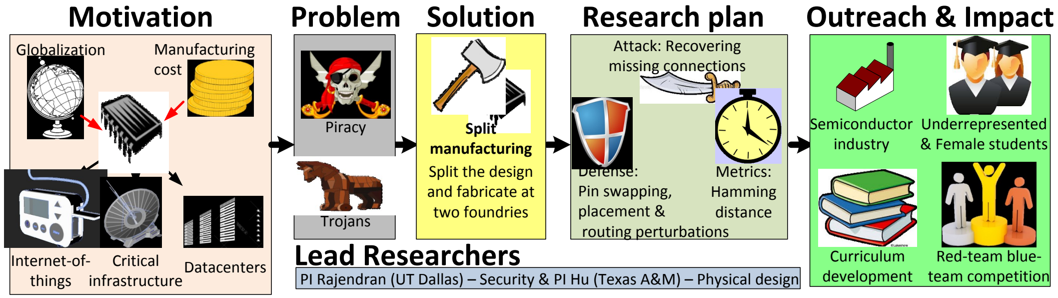
Physical Design for Secure Split Manufacturing of ICs

Challenge:

- Naïve split manufacturing alone does not ensure security
- Security enhancement entails significant timing, power and area overhead to chip products

Scientific Impact:

- Split manufacturing with greatly enhanced security
- Split manufacturing that is practical and compatible with existing design flow



Motivation

Globalization

Manufacturing cost

Internet-of-things

Critical infrastructure

Datacenters

Problem

Piracy

Trojans

Solution

Split manufacturing

Split the design and fabricate at two foundries

Research plan

Attack: Recovering missing connections

Defense:
Pin swapping, placement & routing perturbations

Metrics:
Hamming distance

Outreach & Impact

Semiconductor industry

Underrepresented & Female students

Curriculum development

Red-team blue-team competition

Lead Researchers

PI Rajendran (UT Dallas) – Security & PI Hu (Texas A&M) – Physical design

Solution:

- New techniques for modeling attacks
- Developing scientific security metrics
- Systematic physical design optimization with concurrent security enhancement and overhead control

Broader Impact:

- Collaboration with industry
- New curriculum development
- Security competition
- Participation of underrepresented students

NSF CCF-1618824, SRC 2016-TS-2688/2689, PI: JV Rajendran, UT Dallas, Co-PI: J Hu, TAMU