Introduction to Hardware Security and Trust

Ramesh Karri (rkarri@nyu.edu)
Professor of Electrical and Computer Engineering
IEEE Computer Society Distinguished visitor (Hardware Security)
http://engineering.nyu.edu/people/ramesh-karri

CYBER SECURITY

NYU School of Engineering

Fall 2014

A Reputation in Cyber Security

- One of the earliest to offer degrees
- Triple distinction
  - NSA Center of Excellence in Information Assurance Education
  - NSA Center of Excellence in Information Assurance Research
  - NSA Center of Excellence in Cyber Operations
- Over $25 million in funding for research and education over last10 years
- Strong research and training partnership with federal agencies
- Signature programs and partnerships

- Center for Research in Information Systems and Security (CRISSP)
  - Cutting-edge research collaboration of five NYU schools to integrate technology with policy, law, human psychology and business
  - NSF funding for 24 interdisciplinary PhD students and team of 20 researchers

NYU POLYTECHNIC SCHOOL OF ENGINEERING
NYU LAW
NYU ROBERT F. WAGNER GRADUATE SCHOOL OF PUBLIC SERVICE
NYU STEINHARDT
NYU STERN

CRISSP-Research Labs

Information Systems & Internet Security Lab

- AppSec
- Forensics
- Virtual Lab VITAL connects university partners in NYC

Information Forensics & Security Lab

- Media Forensics
- Network Forensics
- Data Recovery
- Incident Response
- Authentication

Secure Systems Lab

- Virtualization
- Cloud Computing
- Mobile Security

Secure & Reliable Hardware Lab

- Reliable & Trustworthy Hardware Design & Testing
- Encrypted computing

Privacy, Security & Networking Lab

- Internet Privacy
- P2P Security
- Internet Piracy

CRISSP-Cyber Security Programs

Founded on engineering principles and reinforced with lab experience.

8 faculty serving123 MS students and 20 PhD students with 17 classes

MS in Cyber Security
with Management Track
available online

NSA Certificates

Certificate in Security

Graduate & Undergraduate Courses

Application Security
Biometrics
Computer Security
Digital Forensics
Information Security Management
Modern Cryptography
Network Security and Management
Pen Testing and Vulnerability Analysis
Hardware Security

Special Topics:

Advanced Network Security
Psychology and Security
Wireless Security

CRISSP-Signature Programs and Offerings

- Cyber Security Awareness Week (CSAW)
  - Celebrating its 11th year
  - Largest student cyber competition in US
  - Largest Capture the Flag
  - 13,000+ HS and college students
- Summer Cyber Boot-camp for High School STEM Educators
- Sloan Speaker Series
- Hackers in Residence from Industry
- Host to NSF/NSA CyberCorps Program – over 75 sent to government service

EL 9423: Introduction to Hardware Security and Trust
Syllabus
Class: Tuesday 10:00 AM-12:30 PM
Office hours: Monday 10:00AM-11:00 AM
Instructor: Prof. Ramesh Karri (rkarri@duke.poly.edu; phone: 718 260 3596: cell: 917 363 9703)
Pre-requisites: EL 5493/EL4313 and/or EL 5473/EL3913

Motivation: Globalization has led to outsourcing of design, fabrication, test and packaging of ICs. Rogue elements in any of these phases can alter the design and embed malicious circuits. These malicious circuits may be triggered some time in the future. Classical VLSI design and test methods are inadequate to detect these malicious circuits. Even if there are no malicious circuits in designs, side channels of an implementation can leak the secrets and intellectual property. Examples include power, timing, EM radiation and deliberately introduced faults. Finally, the testing infrastructure used to improve the quality of ICs can be used to leak secrets.
Objective: Students will be introduced to all aspects of a VLSI design. The students will be exposed to defenses that can detect and protect against the variety of discussed threats. Following is a tentative list of topics that will be covered in the course:

Topic	Weeks
Introduction; Homework 1 on example hardware attacks not covered in class	1
Ciphers: Historical; Block (AES/DES), stream, (Trivium) public key ciphers (RSA. ECC), hash functions (SHA-1); Homework on the various ciphers	2
	2
	2
	2
	1
	1
	2
	1
	1

ple projects
ult and test
tacks etc…
Information
n Hardware
rdware and
EE explore

n: 10%

- White hat hardware hacking =>security mindset
- Design for security
  - Logic design+security
  - offline test+security
  - online test+security
  - PUFS, RNGs, …
- Labs
- Summer school: 6 weeks in July; (hardware) cybersecurity

Introduction to Hardware Security and Trust

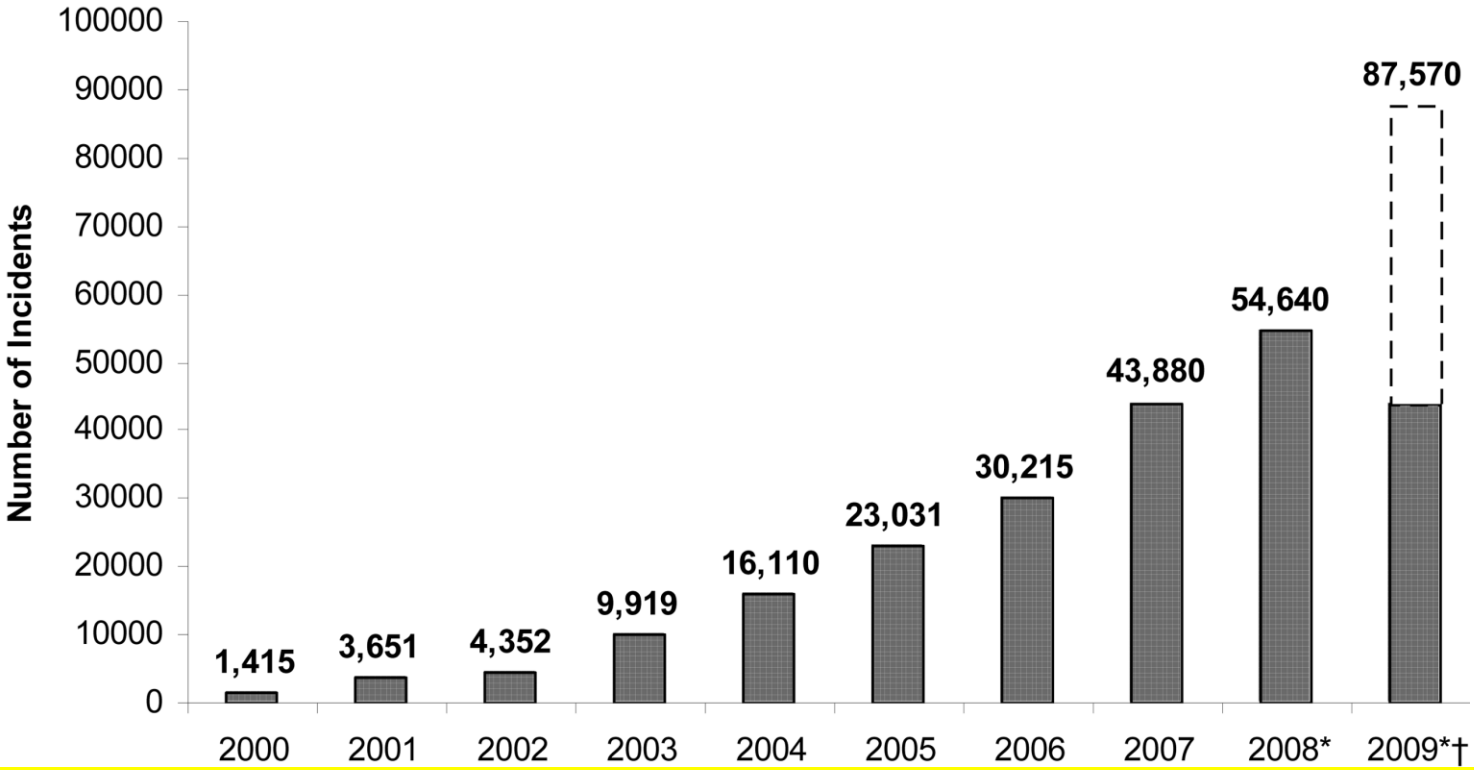
Ramesh Karri (rkarri@nyu.edu)
Professor of Electrical and Computer Engineering
IEEE Computer Society Distinguished visitor (Hardware Security)
http://engineering.nyu.edu/people/ramesh-karri
Cell: 917 3639703
Skype: karriramesh

How can a system be attacked?

- Application software
- Protocols
- Operating system software

Severity of incidents not considered

Is security worth my time?

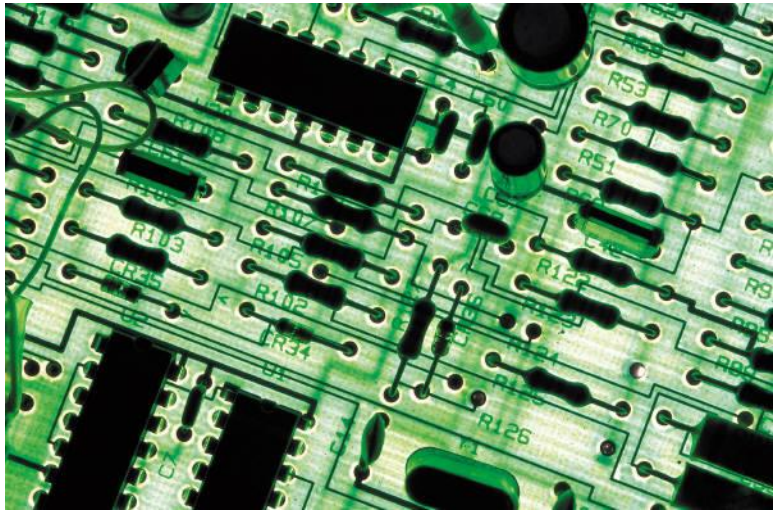


Source: http://www.uscc.gov/annual_report/2008/annual_report_full_09.pdf, page 168
US-China economic and security review commission hearing on China's proliferation practices and the development of its cyber and space warfare capabilities, testimony of Col. Gary McAlum.

How can a system be protected?

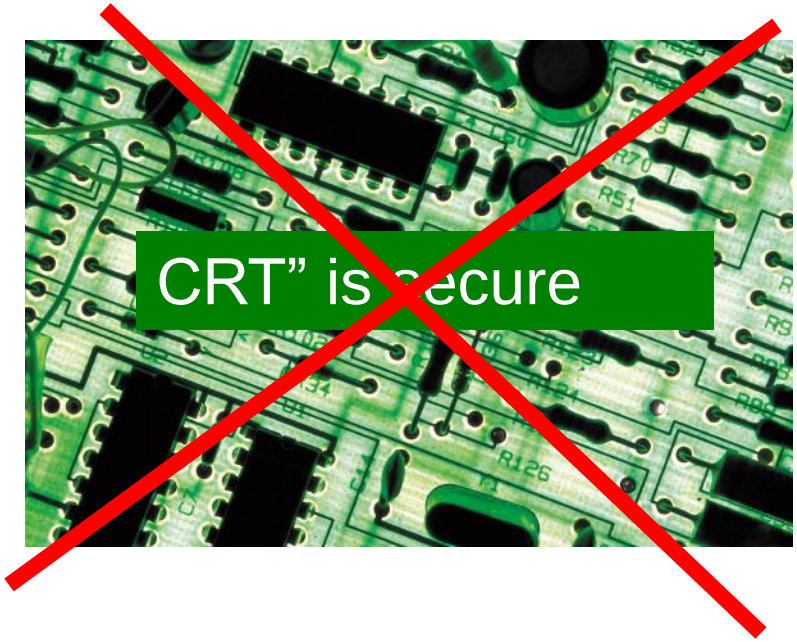
- Fix applications
- Fix protocols
- Fix operating systems

This assumes that…



“the core root of trust (CRT)” is secure

- But…



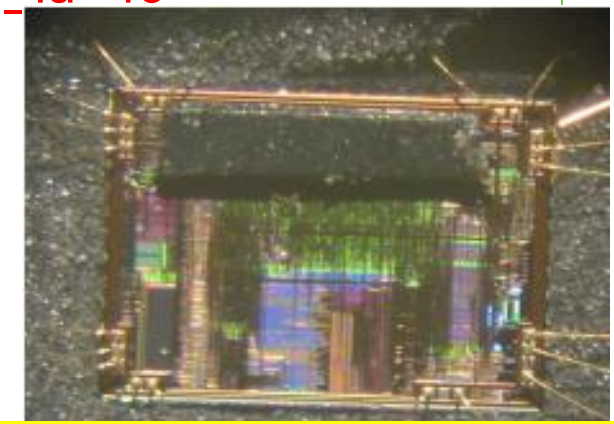
Example 1: Cap'n Crunch (1972)

- John Draper discovered he could make free, long distance phone calls using a whistle from Cap'n Crunch cereal box
  - whistle emitted a 2600 hertz tone
  - allowed user to route his call by emulating in band signaling
  - and make free calls
  - No longer works in western nations: digital+out of band signaling

Image Courtesy Wikipedia

Example 2

- Microchip PICs store “fuse” settings in Flash memory
  - code protection bits prevent mod. of select regions of mem.
  - code protection bits prevent read of select regions of mem.
  - PIC flash has transistor structure similar to UV-erasable EPROMs.
- ATTACK: access die and reset fuses with UV light
  - disable asserted code protection bits
  - read/modify stored program code
  - http://www.bunniestudios.com/blog/?page_id=40



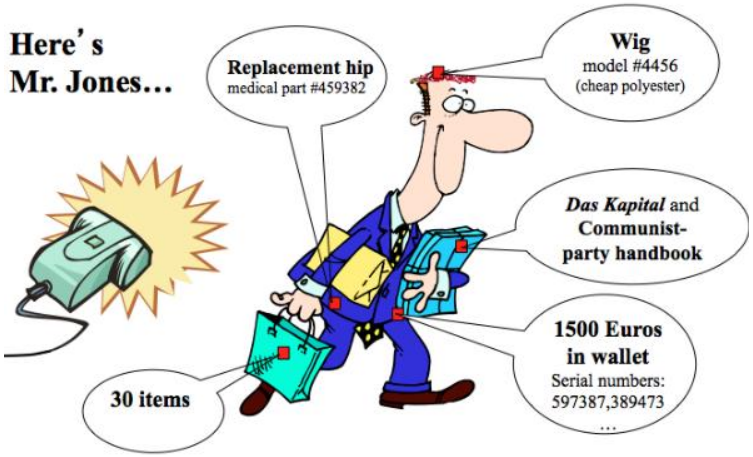
Exposed PIC18F1320: Electric tape covers flash mem; prevents erasure of firmware when UV light is shined onto config. fuses

Example 3: apple laptop batteries

- Smart battery chips have a micro-controller
  - Help OS monitor/control battery/charger.
- Each battery has a unique password (not strong)
  - Loophole identified by Miller, Accuvant Lab
  - Once deciphered, a hacker could control smart battery.
  - Could permanently damage battery; Could infect computer w/ malware
  - may cause battery to overheat, catch fire or explode
    - but sensors can detect overheating

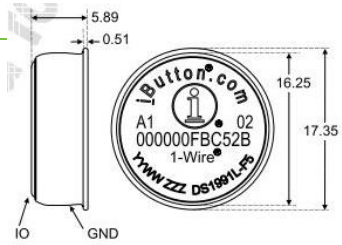
Example 4: RFIDs

- Credit Cards, Transit Cards, Passports, …
- RFID tags can be "skimmed" and cloned
  - Cost of hardware, software ~ US$100
  - No need for physical contact
  - Example RDIF theft: http://www.youtu



- Cover RFID tags with protective mesh: US 15 $

Example 5: authentication tokens



- Dallas semi iButton (DS 1991)
  - cashless transactions; copyright protection
  - user authentication; access control
- ibutton stores 1152 bits in non-volatile memory
  - in three pieces; each piece protected by 8-byte password
- Claim: correct password => ibutton returns the correct 48-byte piece
- Claim: incorrect password => ibutton returns “random” 48-byte piece
- REALITY: incorrect password => 48-byte piece NOT random
  - “Random” output = function (password, constant stored in ibutton)
  - all ibuttons have the same constant
  - function can be obtained from the weblink.
- Dictionary attack
  1. Guess password; pre-compute 48-byte “random” piece
  2. if ibutton output ≠ pre-computed output, 48-byte piece recovered
  3. if ibutton output = pre-computed output, then go to 1

http://grandideastudio.com/wp-content/uploads/ds1991_sect

Example 6: Hotel keycards

- Cody Brocious discovered vulnerabilities in Onity room locks
  - gain instant access to hotel rooms
  - http://daeken.com/blackhat-paper
- Attack: Dump memory of reader; 32-bit key of proprietary crypto
  - Get master key for all rooms
  - Cost of attack: $50

Source: http://cdn.pearltrees.com/s/preview/index?urlId=35156327

Example 7: Smart meters

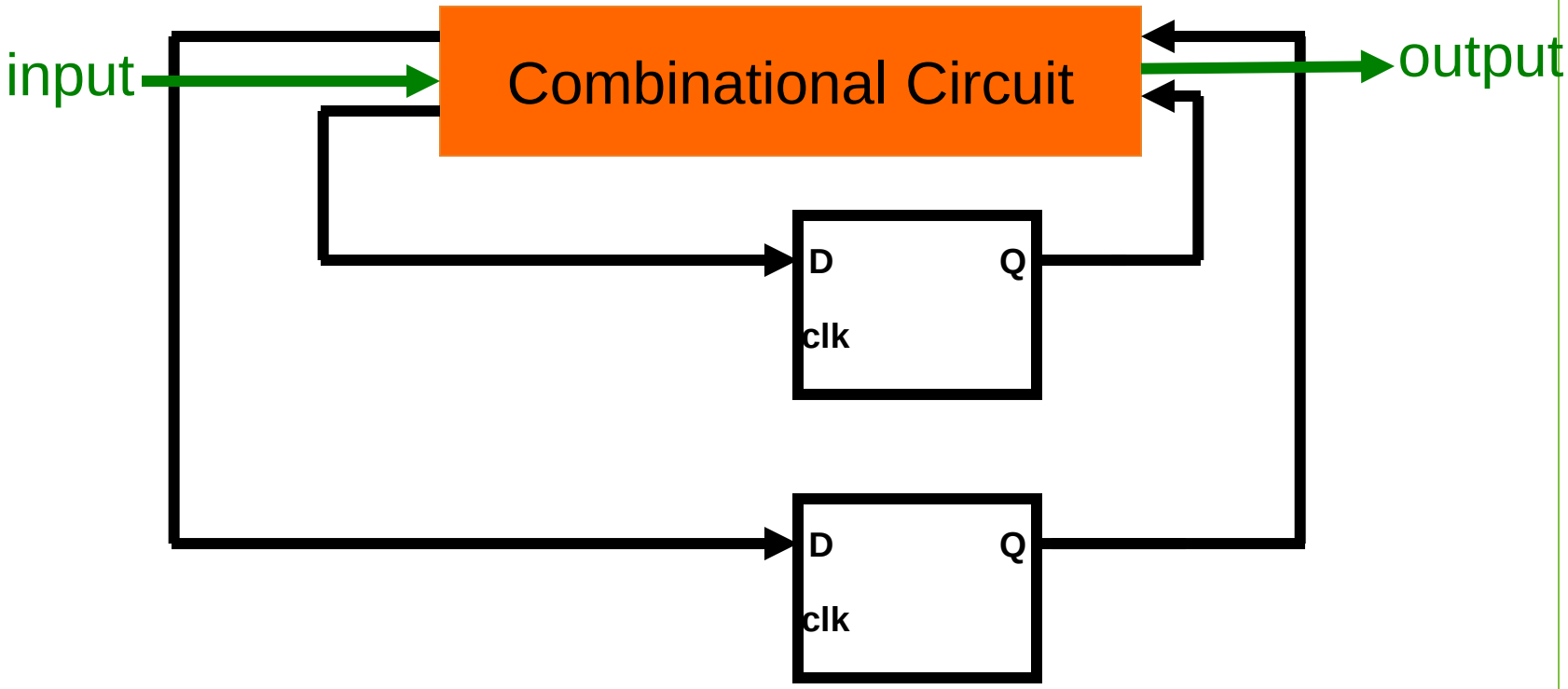
- Utilities are rolling out smart (electronic) meters
  - remote reading, activation, deactivation
  - tamper?
- Hacking a smart electric meter
  - CC2420 modules used for Zigbee comm. with AES-128.
  - Used two syringes to intercept Keys on SPI bus between the ROM and the zigbee module

http://www.forbes.com/2009/04/29/smart-grid-legislation-technology-security-smart-grid.html
http://travisgoodspeed.blogspot.com/2009/03/breaking-802154-aes128-by-syringe.html
http://www.blackhat.com/presentations/bh-usa-09/GOODSPEED/BHUSA09-Goodspeed-ZigbeeChips-PAPER.pd
http://www.ioactive.com/news-events/DavisSmartGridBlackHatPR.php

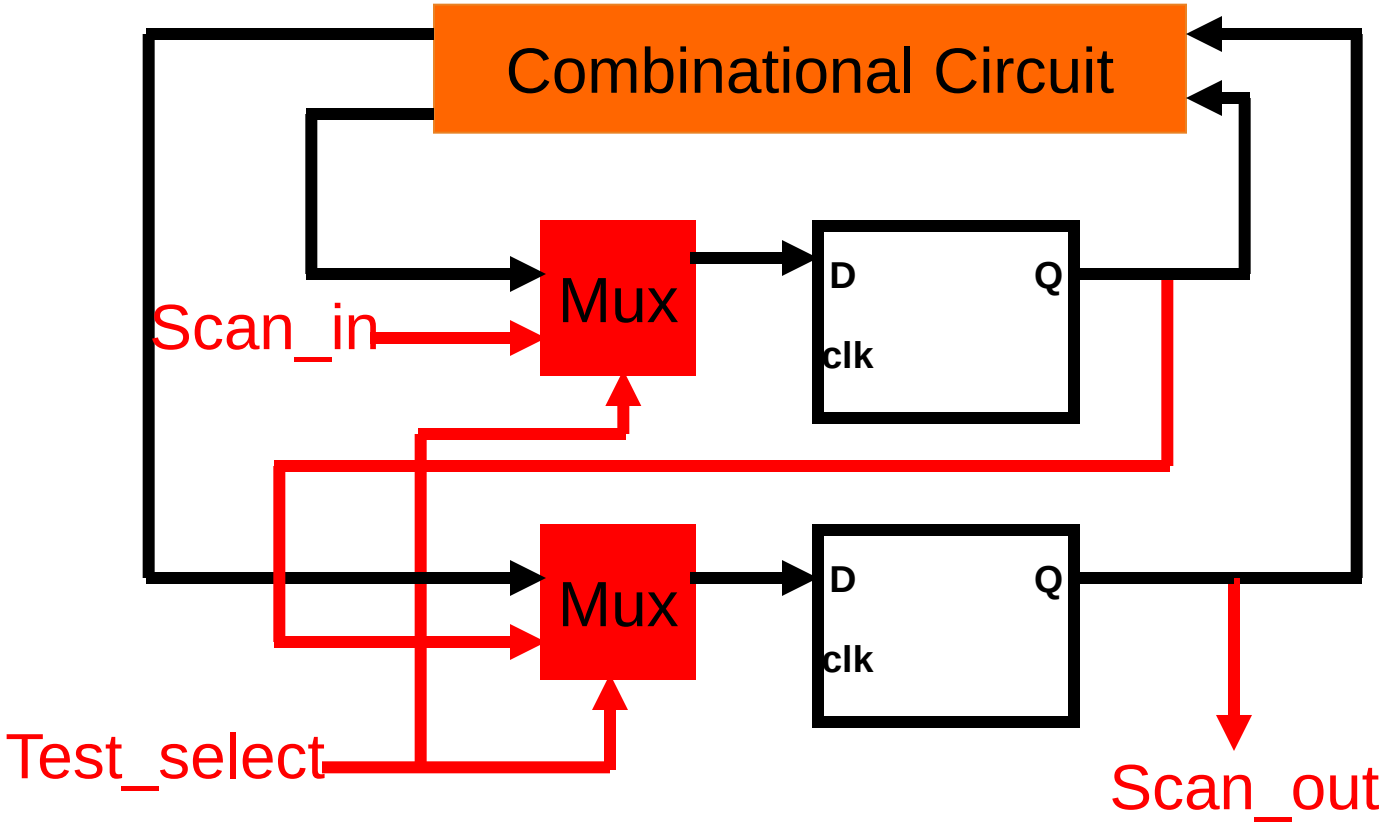
Hardware vulnerabilities

- Side channels
  - Power dissipation
  - Timing variation
  - Faults
  - Test infrastructure (scan, JTAG, P1500, online…)
  - interactions between side channels
- Cloning and overbuilding
- Reverse engineering
- Malicious logic (a.k.a. hardware Trojans)

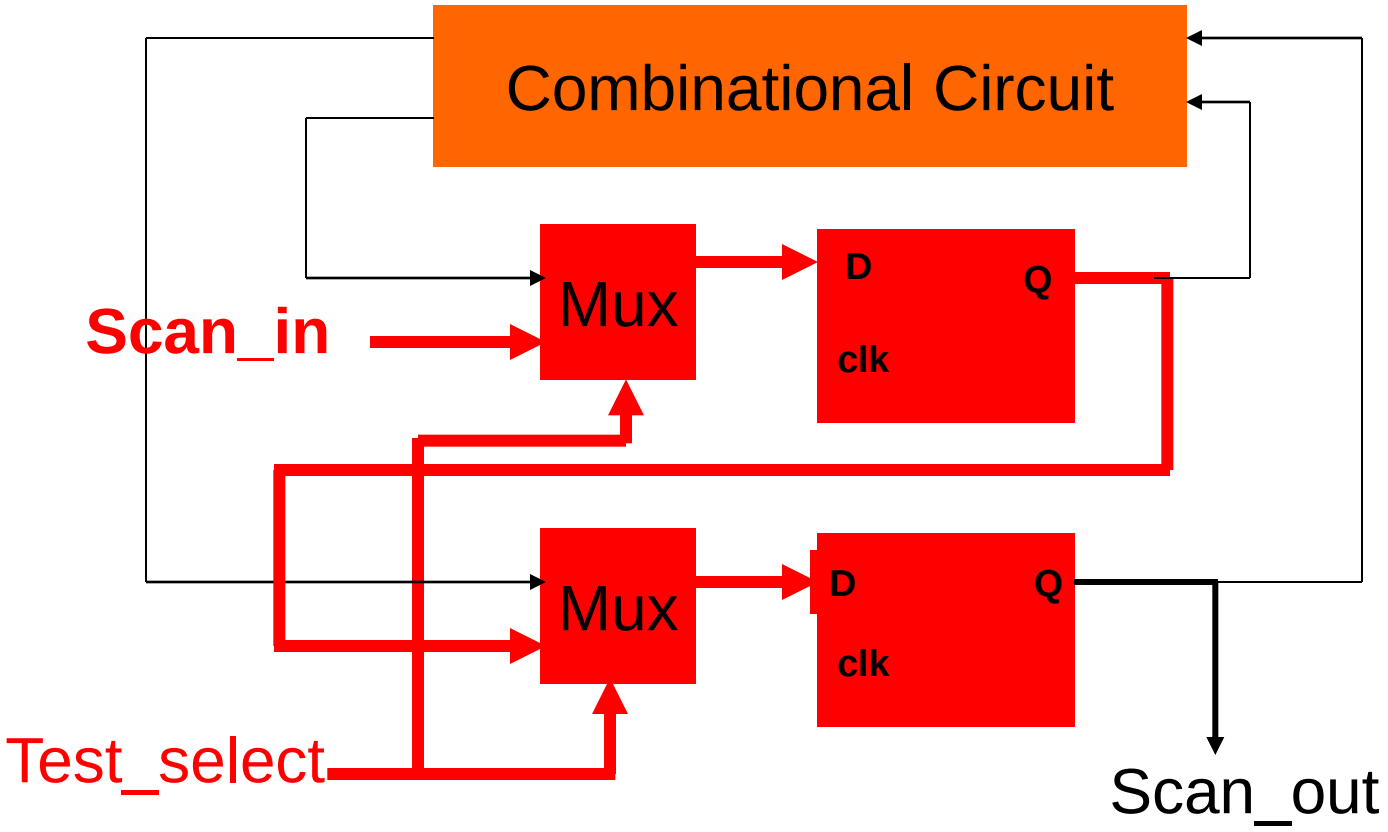
Combinational logic+ state elements



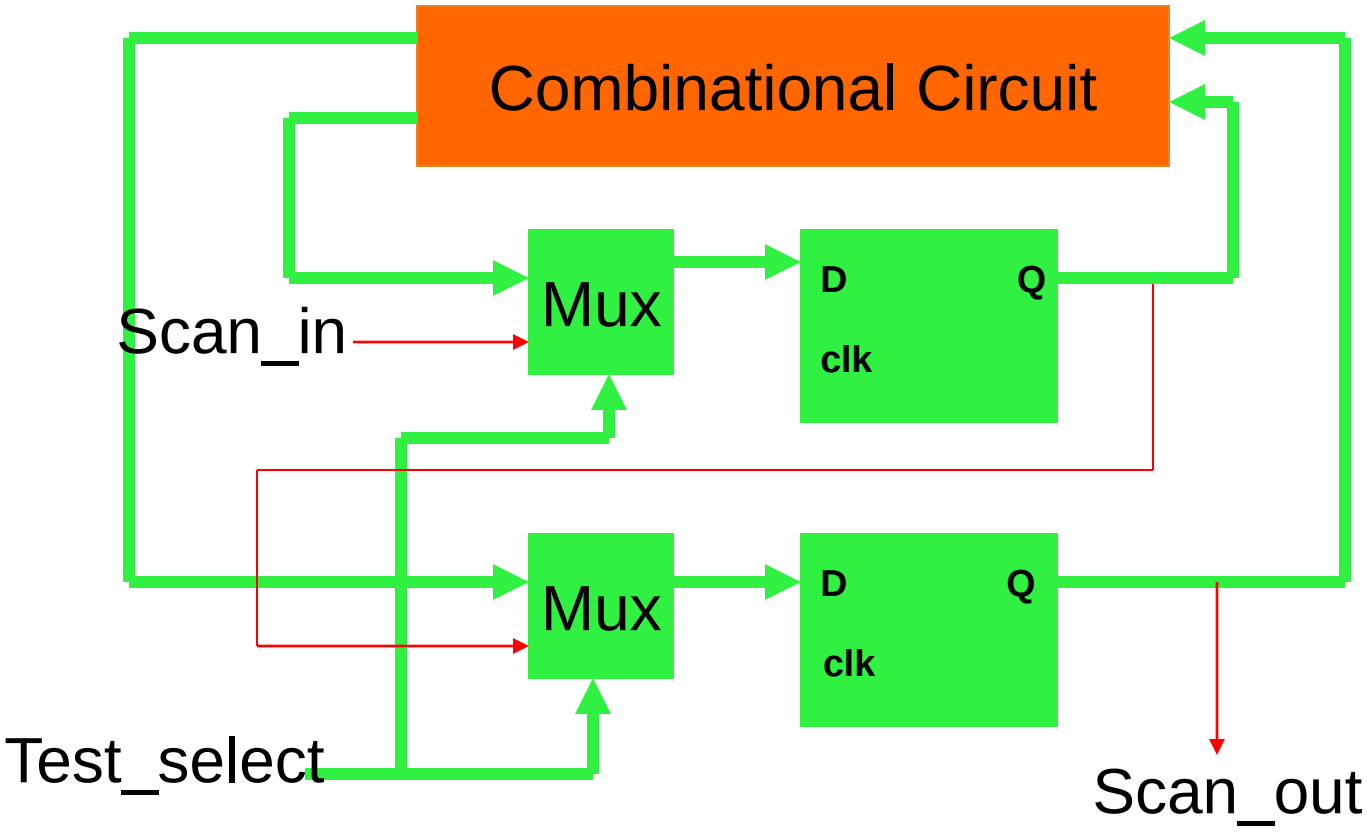
Scan chain: chain all FFs



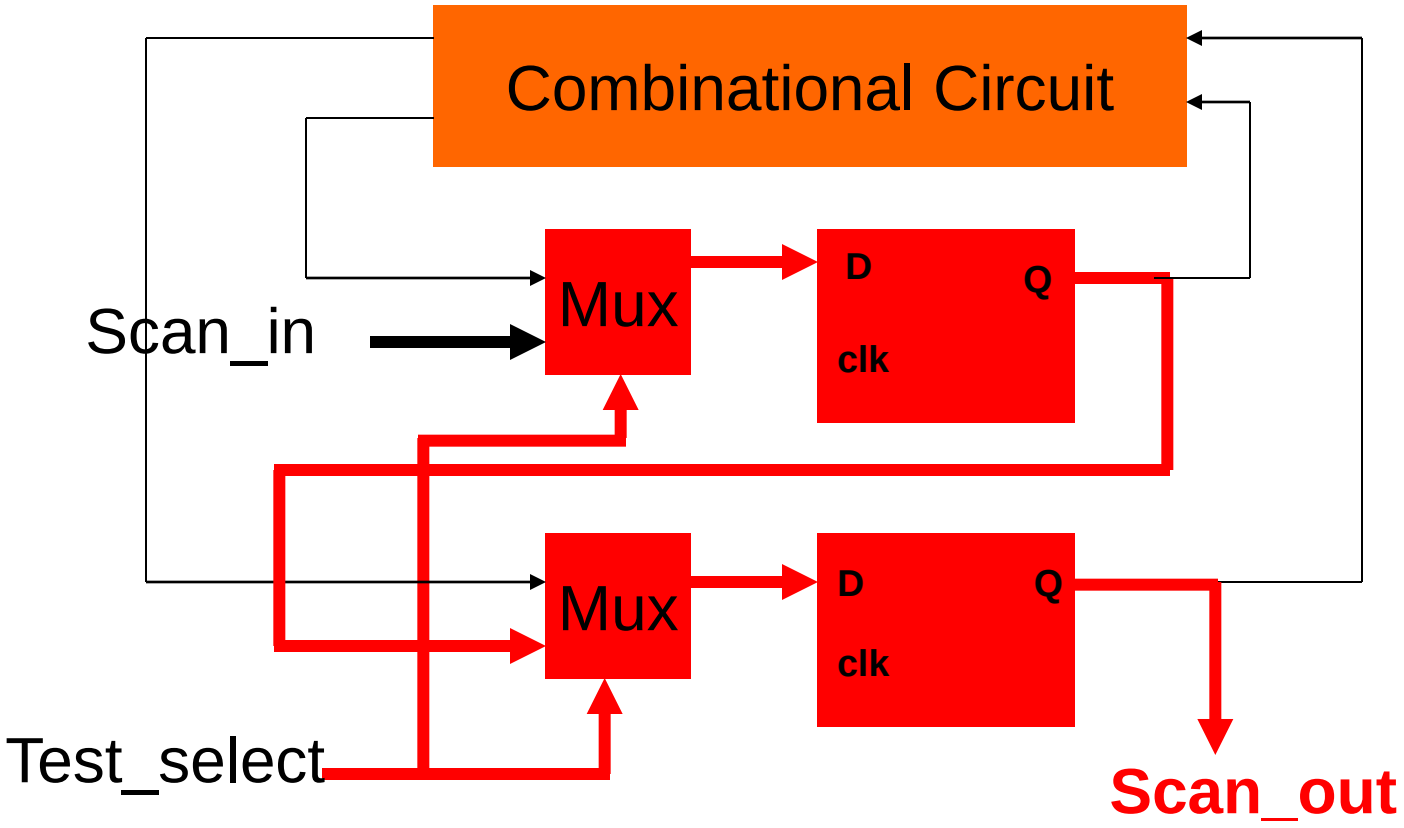
Scan chain: scan in data



Scan chain: normal mode



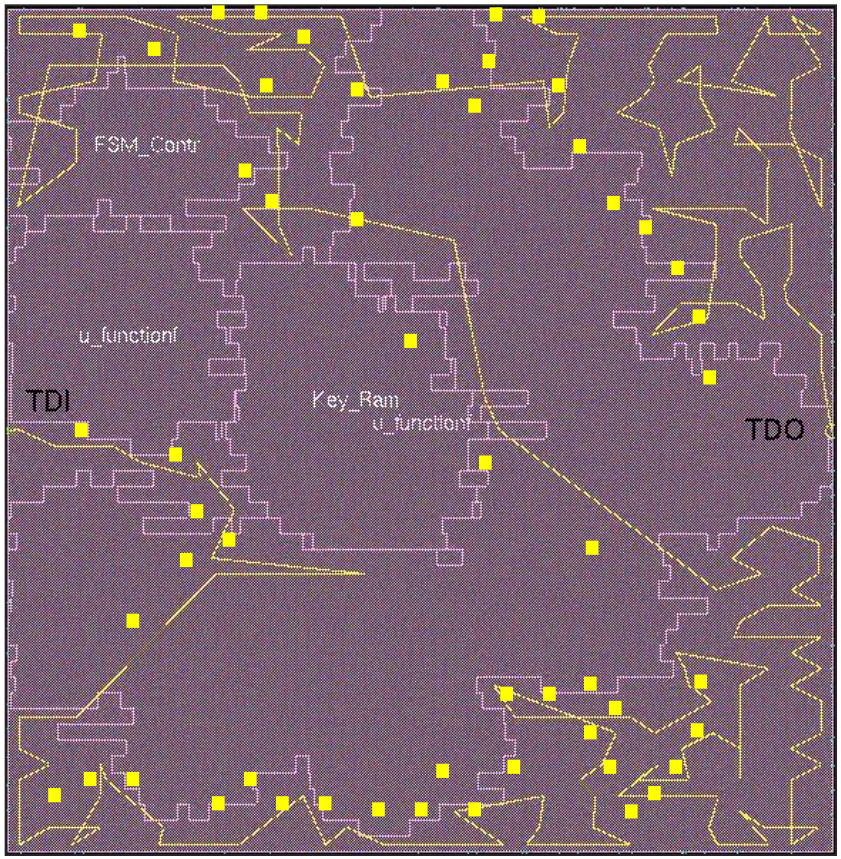
Scan chain: scan out data



Scan chains are extremely popular…

- >80 % of ICs use scan chains for test/debug/validation
- Scan DFT is widely supported
  - Fast Scan/TestKompress: Mentor Graphics
  - DFT compiler/TetraMAX ATPG: Synopsys
- Readback and test infrastructure in FPGAs
  - Load configuration bitstream from external PROM
  - Readout bitstream for debug

Scan chains are a portal for hackers



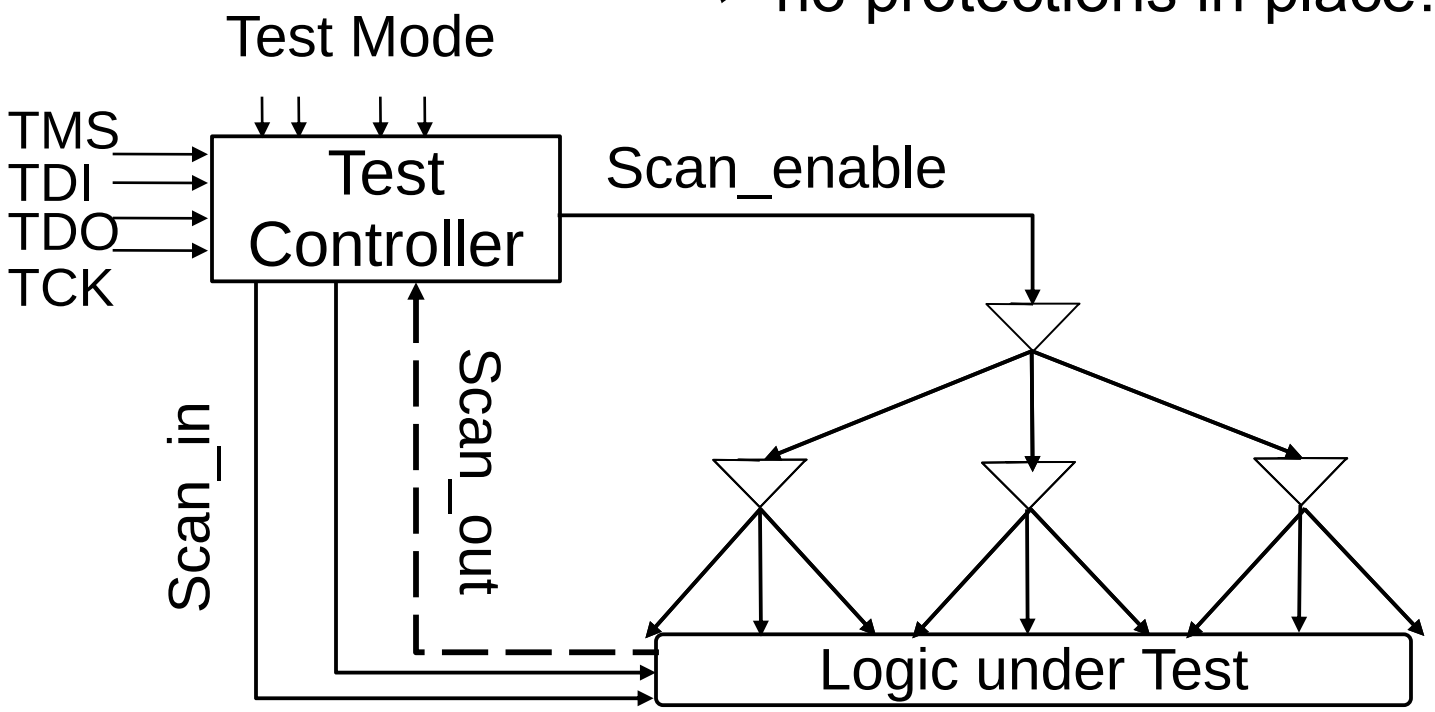
[1]http://www.eedesign.com/story/showArticle.jhtml?articleID=51200154

Scan attack outline

- Step 1: access scan chains
  - Approach L: Get lucky (don't do anything)
  - Approach A: bypass test authentication steps
  - Approach B: activate scan chain using physical attacks
- Step 2: use scan chains to leak secrets
  - Approach A: observe (normal➔scan out)
  - Approach B: control+observe (scan in ➔normal➔ scan ou

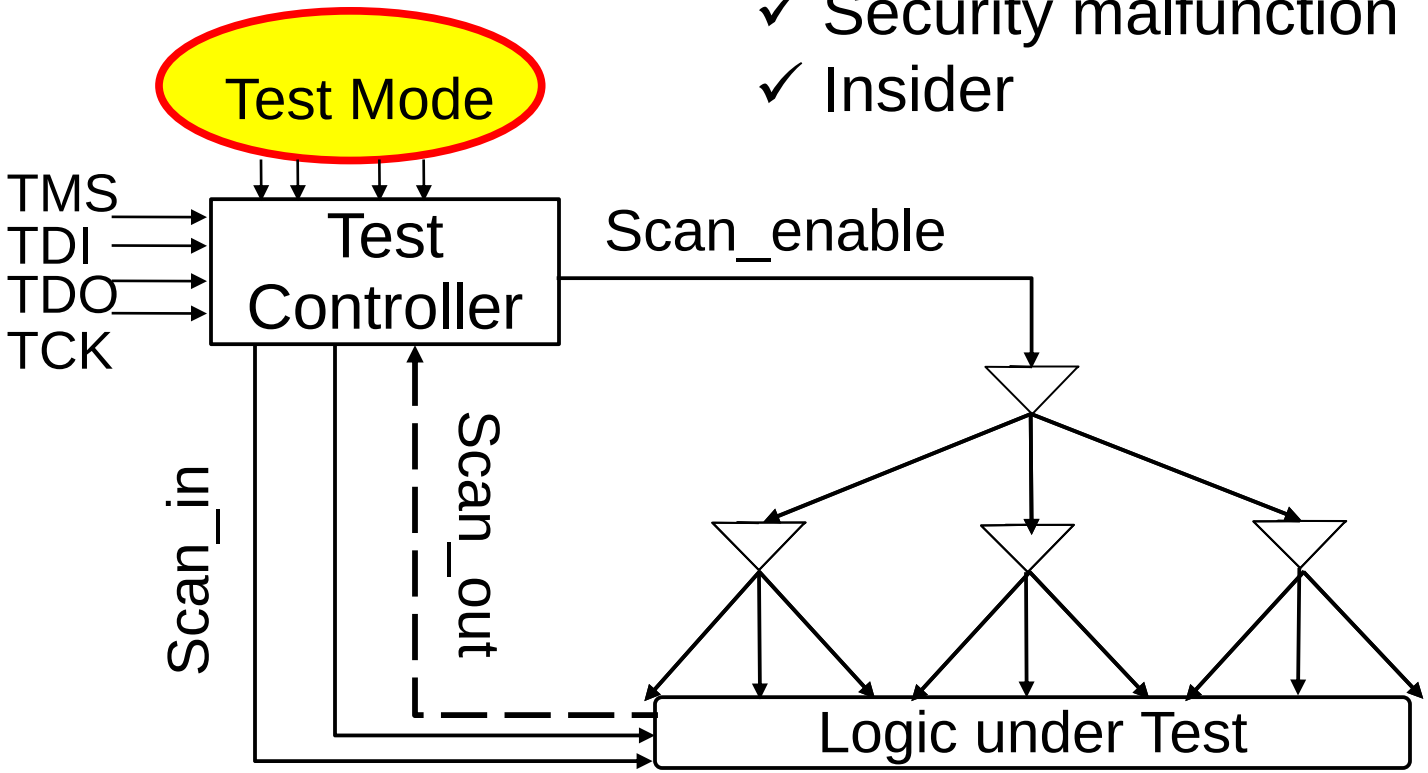
Access scan chains: get lucky !!!

✓ no protections in place…



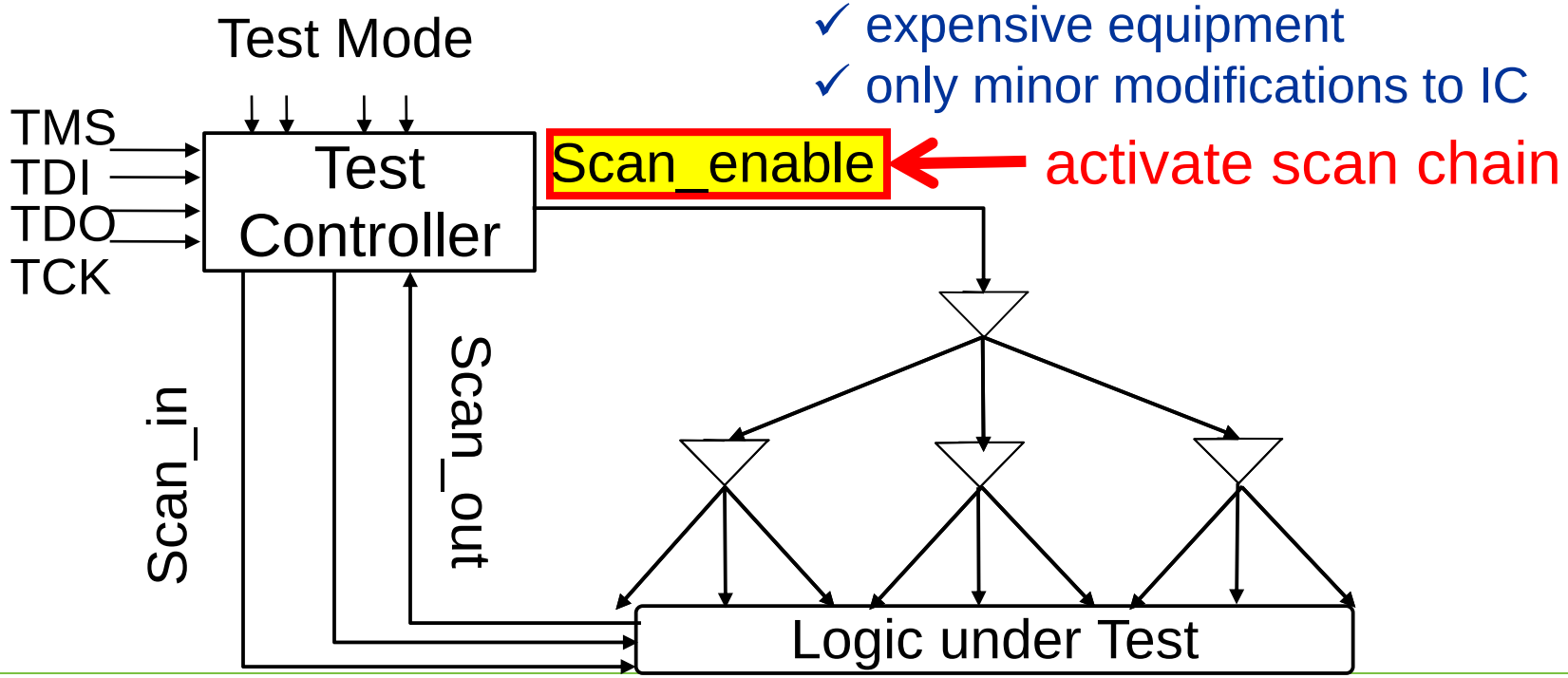
Access scan chains: malicious use of test features

- ✓ Corrupt authentication
- ✓ Security malfunction
- ✓ Insider

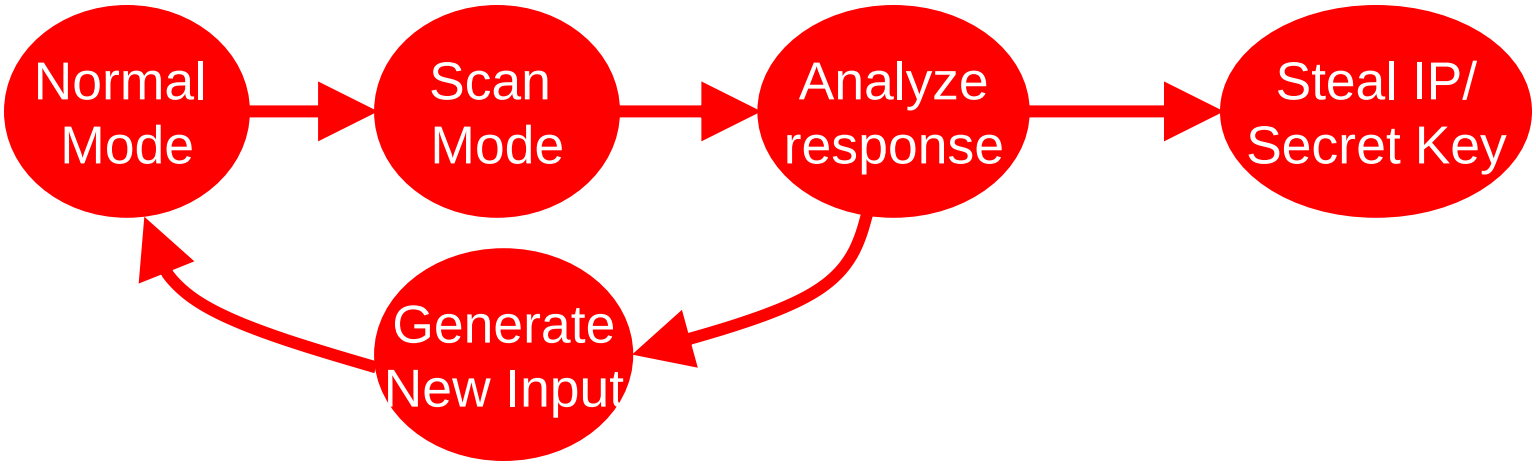


Access scan chains: physical attack

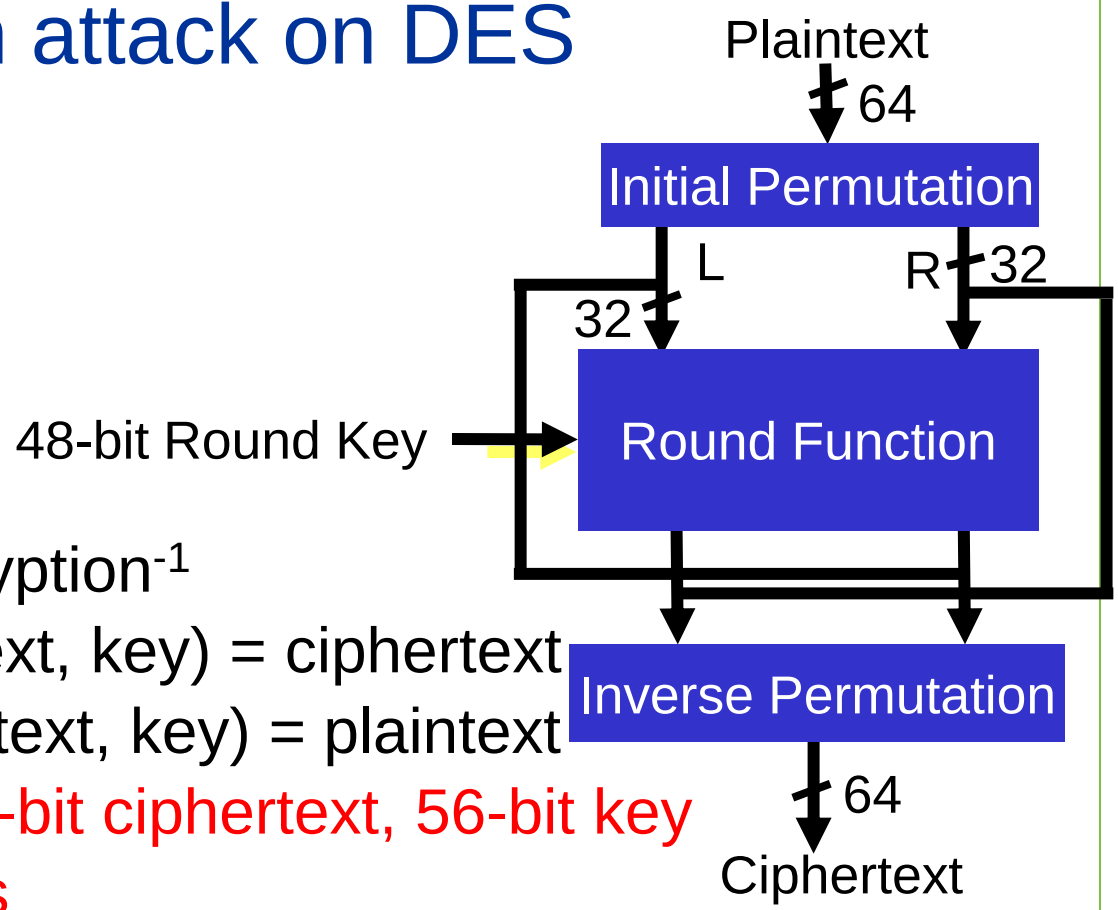
- FIB/probing requires
  - ✓ Expertise in semi. tech.
  - ✓ Detailed knowledge of IC
  - ✓ expensive equipment
  - ✓ only minor modifications to IC



- Use scan chain: to observe internal state

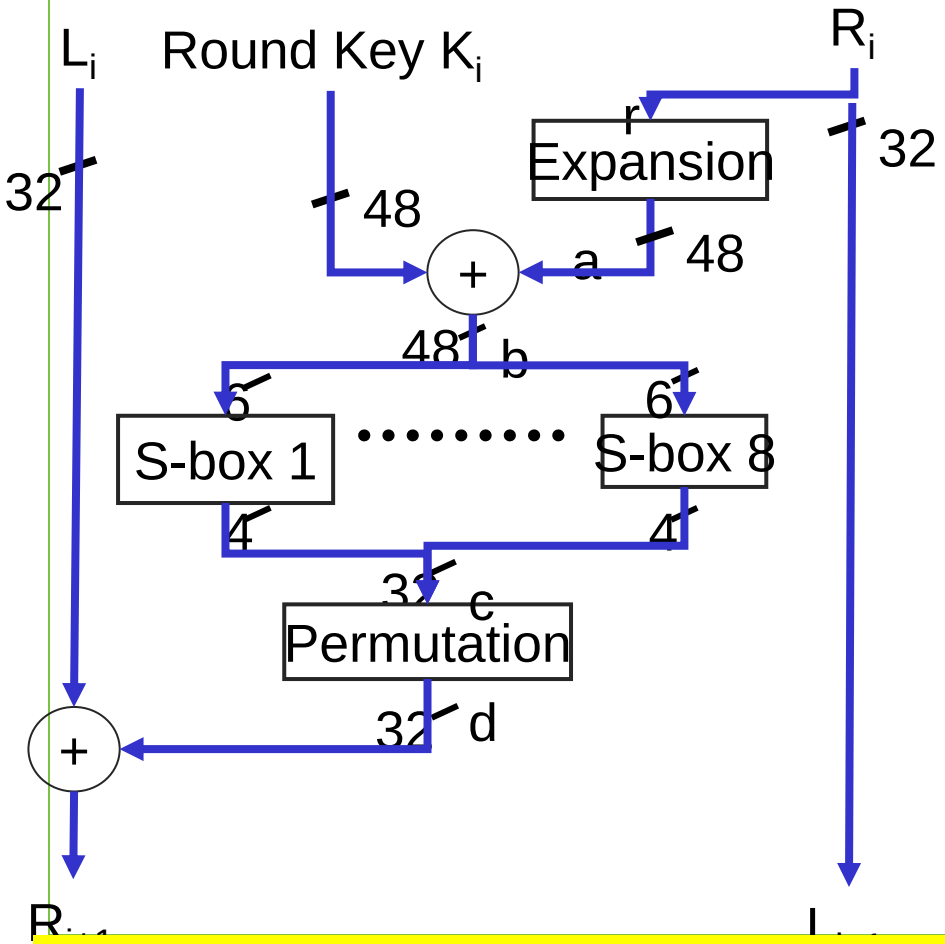


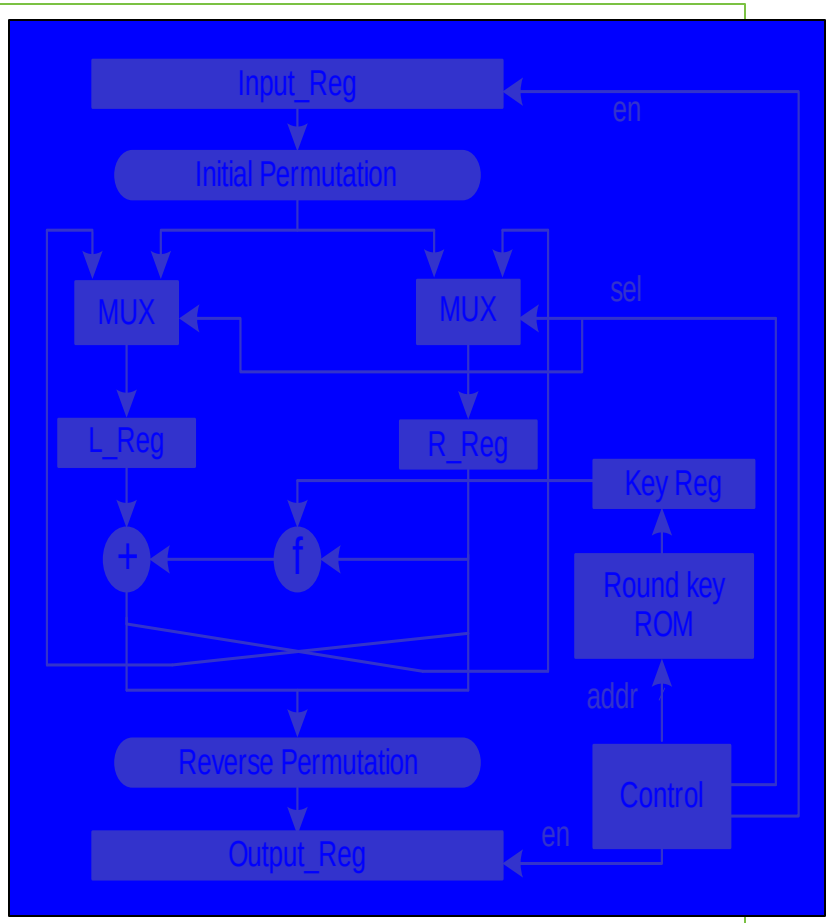
Practical scan attack on DES



- Decryption = Encryption^{-1}
- ENCRYPT (plaintext, key) = ciphertext
- DECRYPT (ciphertext, key) = plaintext
- 64-bit plaintext, 64-bit ciphertext, 56-bit key
- 16 identical rounds
- 56-bit secret $\Rightarrow$16x 48-bit round keys

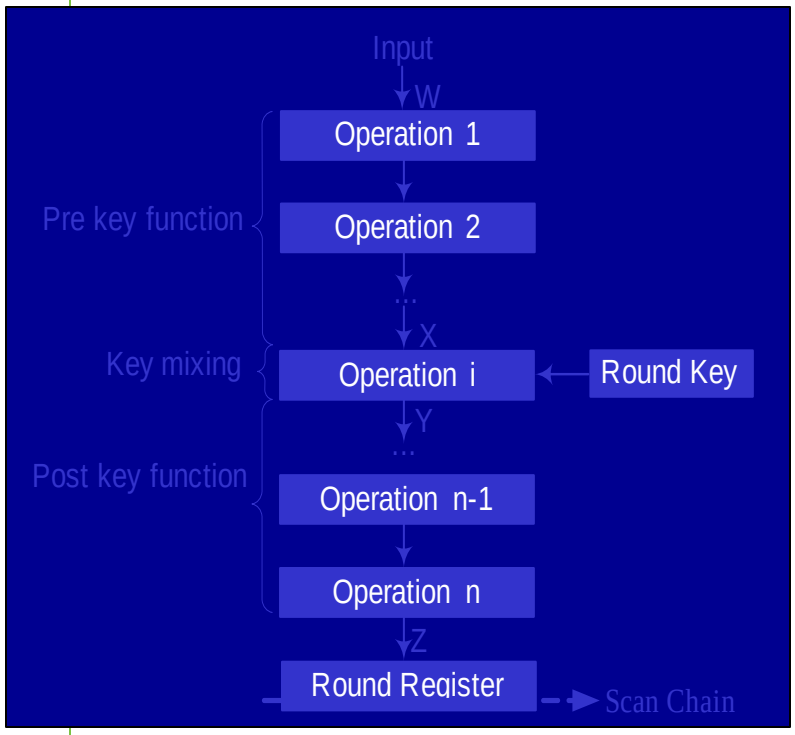
DES architecture



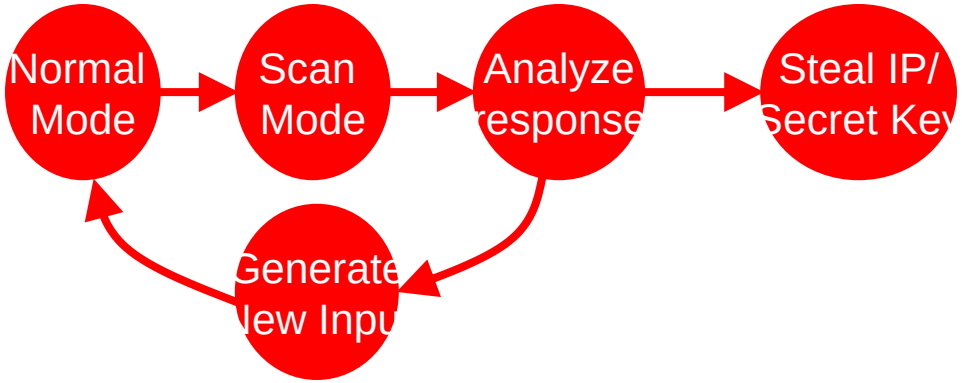


- Cipher Block Chaining mode ⇒ Iterative architecture
- Input, L, R, Output Regs (64+32+32+64= 192 FFs)

DES scan-based attack

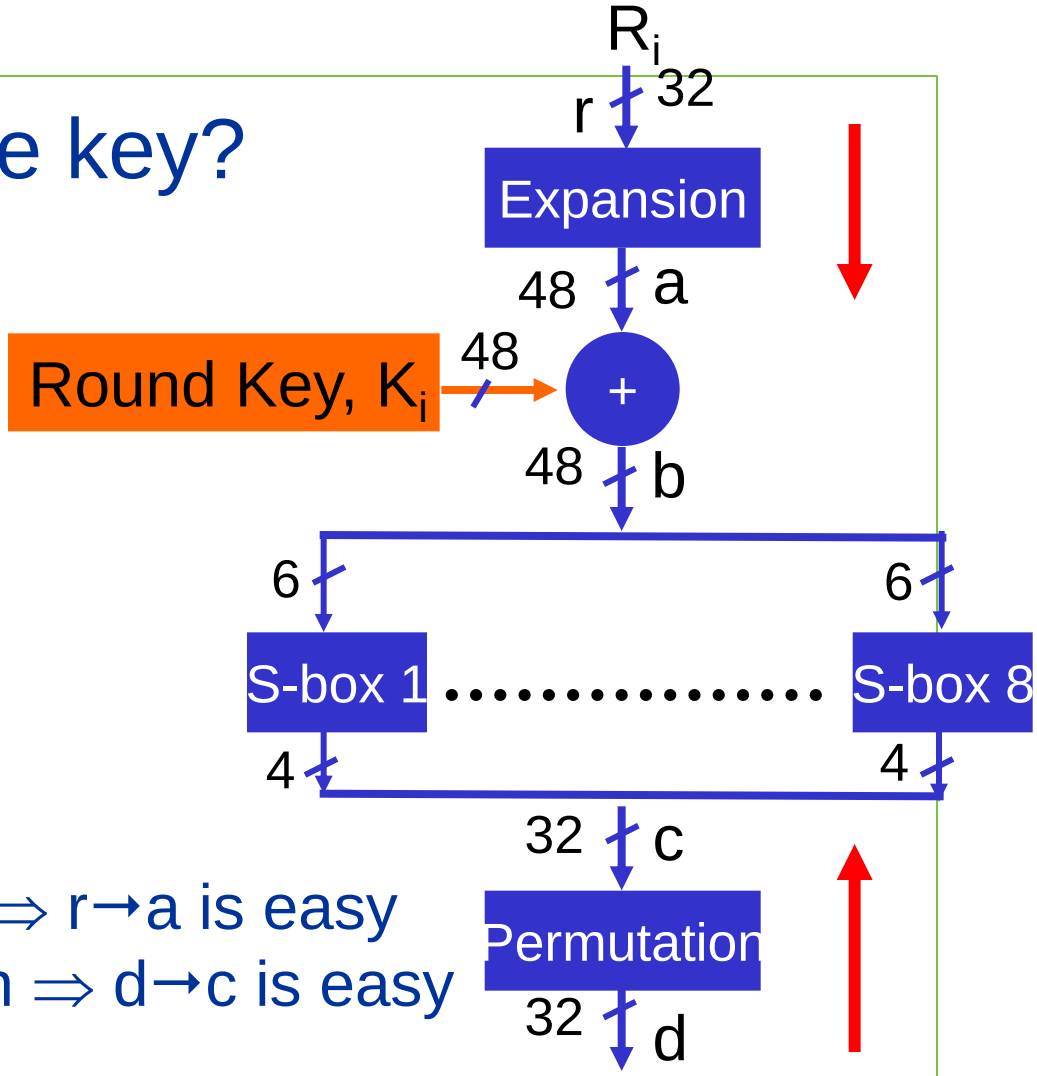


- round key reg not in scan chain
- Calculate X from W
- Scan out Z
- Calculate Y from Z
- Solve key xor



B. Yang, K. Wu, R. Karri, *"Scan Chain Based Side Channel Attack on dedicated hardware implementations of Data Encryption Standard"*, ITC Oct 2004

- How can we get the key?



- Round Key K_i = a xor b
- Expansion is a bijection ⇒ r→a is easy
- Permutation is a bijection ⇒ d→c is easy

B. Yang, K. Wu, R. Karri, *"Scan Chain Based Side Channel Attack on dedicated hardware implementations of Data Encryption Standard"*, ITC Oct 2004

Scan DFT: takeaways

✓Designed to access the internal system state !

✗ Can be used to access proprietary info in the system !!

Countermeasure 1

- Leave scan chains unbound [Kömm99]
  - compromises maintenance and in-field debug

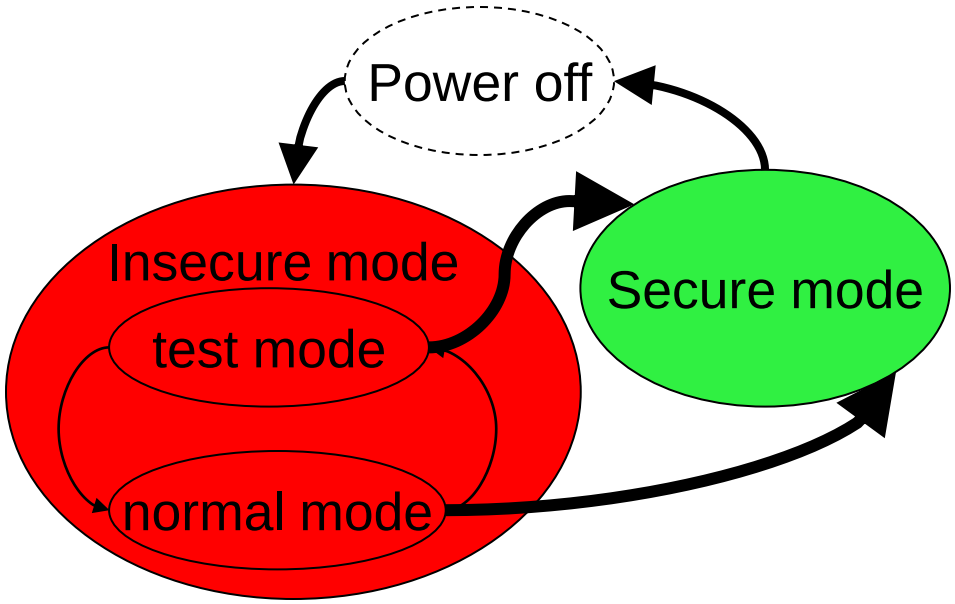
O. Kömmerling, M. G. Kuhn, Design Principles for Tamper-Resistant Smartcard Processors, USENIX Workshop on Smartcard Technology, pp.9-20, May, 1999.

Countermeasure 2: secure scan

- information obtained from scan chains should not be useful in retrieving the secret key
- Two copies of key
  - Secret key: use in normal mode (secure memory)
  - Mirror Key: use for testing (mirror key register)
- Two modes of operation: insecure and secure
  - Secure/Normal: use secret key; disable test/debug
  - Insecure/Test: use MK (isolate secret); enable test/debug

B. Yang, K. Wu and R. Karri "Secure scan: a design-for-test architecture for crypto chips," IEEE/ACM Symposium on Design Automation Conference, 2004
B. Yang, K. Wu and R. Karri "Secure scan: a design-for-test architecture for crypto chips," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 2006, **25**(10): 2287-2293.

Secure Scan



⇒test mode: erase data from normal mode

reset chip⇒verify reset ⇒enter test mode

⇒normal mode: erase scanned-in data from registers

reset chip ⇒verify reset⇒ enter system mode

Security-aware SoC test access

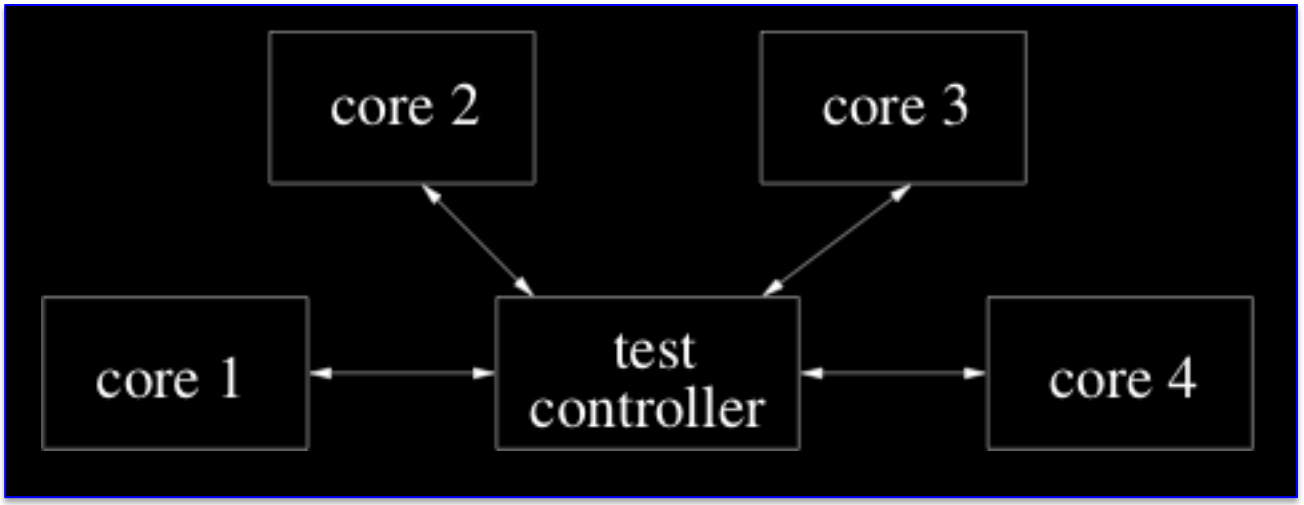
✗ Shared test wiring
✗ Untrusted third-party SoC cores

Security-aware SoC test access

- Can SoC tester safely exchange sensitive data with cores on a shared test bus?
- SoC integrator trusts CAD tools, fabrication, packaging
- SoC integrator does not trust except third-party cores

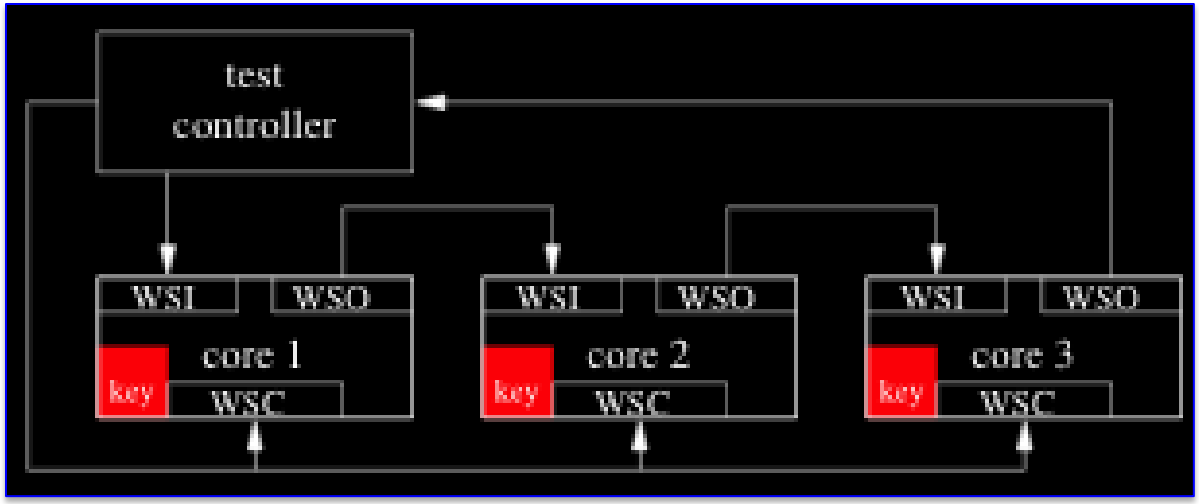
K. Rosenfeld, R. Karri, Security-aware SOC test access mechanisms. IEEE VLSI Test Symposium 2011: 100-10

Approach 1: star topology



- Protects test data secrecy
- Boosts test bandwidth
- High die area cost due to wiring complexity

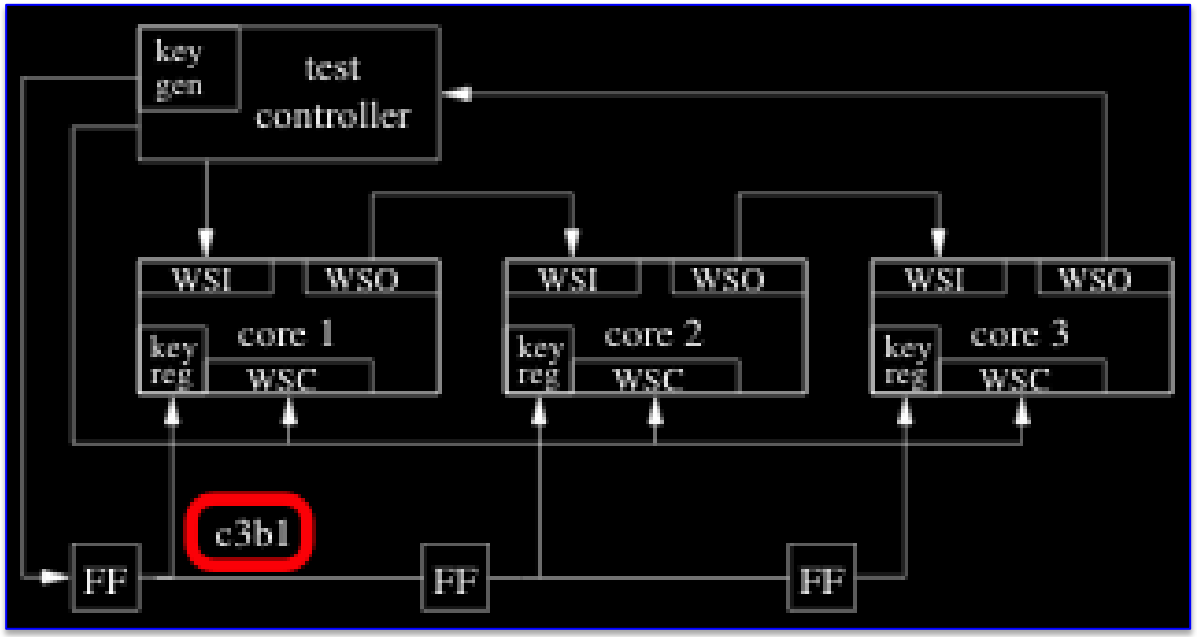
Approach 2: fixed keys



Shared wiring with pre-shared keys embedded in design

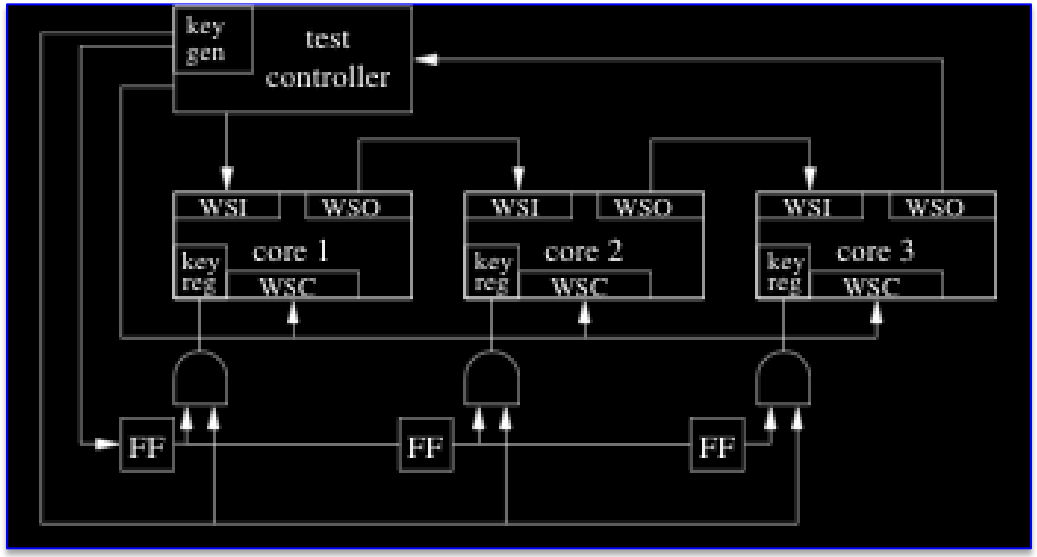
- No need for key setup at test time
- Requires secrecy of design (netlist, mask, etc.)
- Key management logistics difficult with multiple users

Approach 3: shift key in



- Idea: Distribute keys to each core using a shift register.
- Problem: Core 1 sees key bits for core 3 as it is shifted.

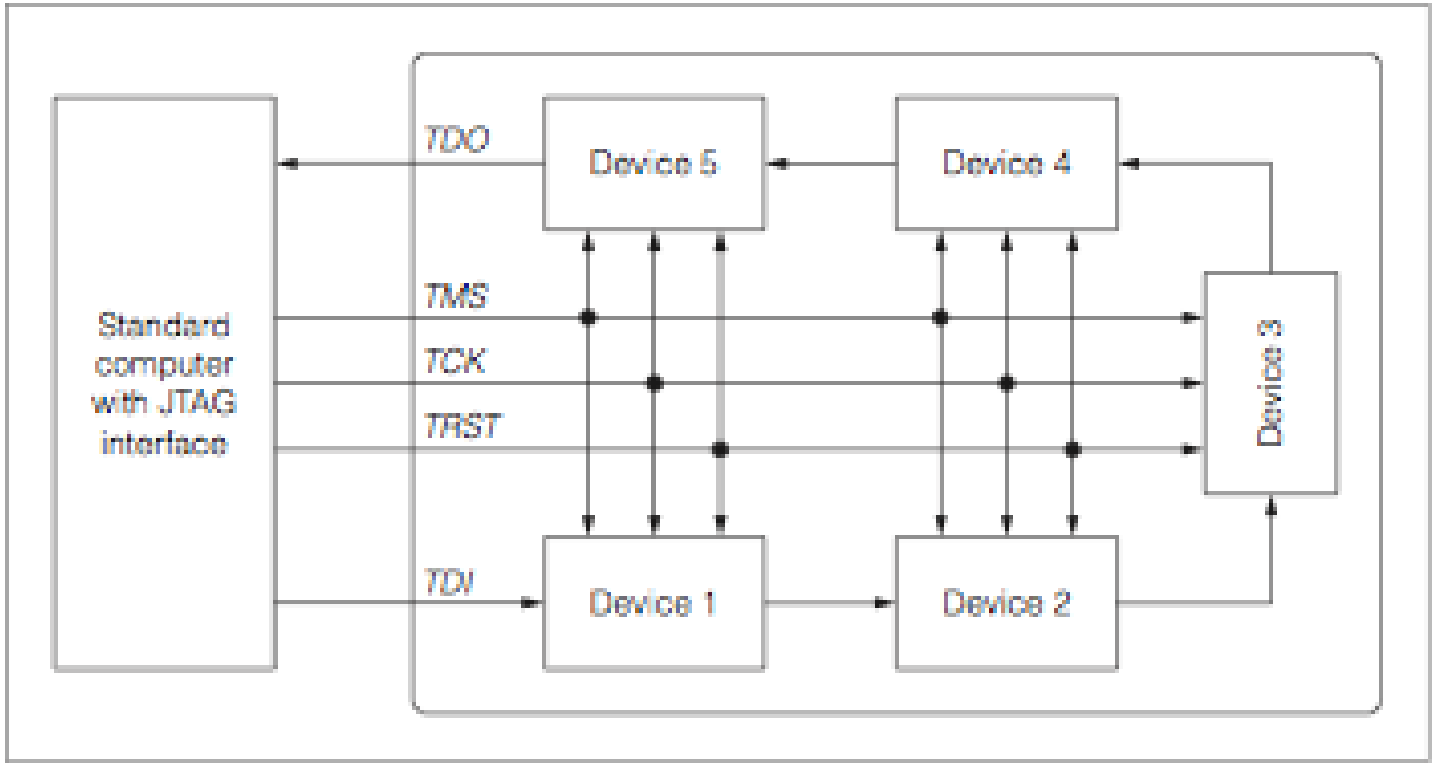
Approach 4: inhibit and shift-in



Key setup

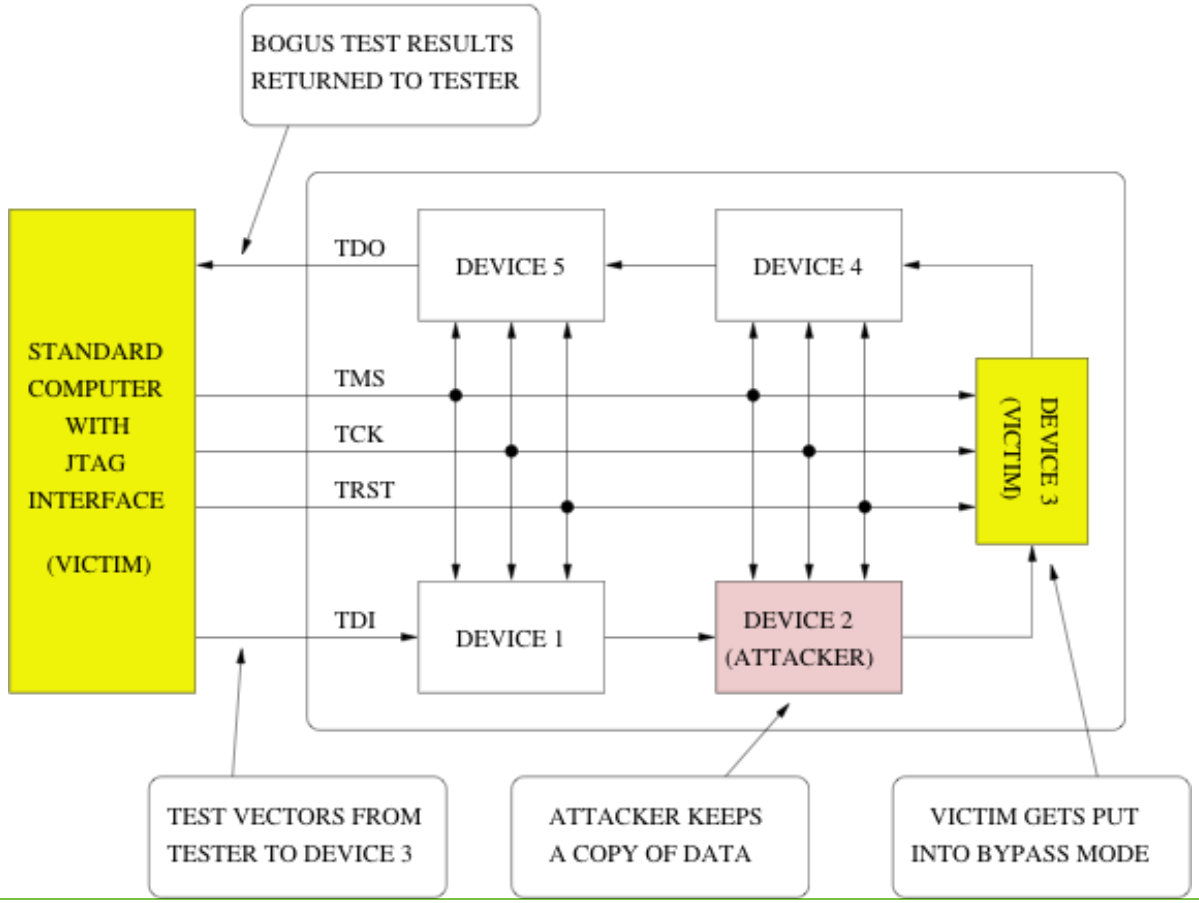
- Assert output inhibit on the trusted scan chain
- Shift key into the trusted scan chain
- De-assert output inhibit on the trusted scan chain
- Latch bit from trustworthy scan chain into shift reg. in core

JTAG

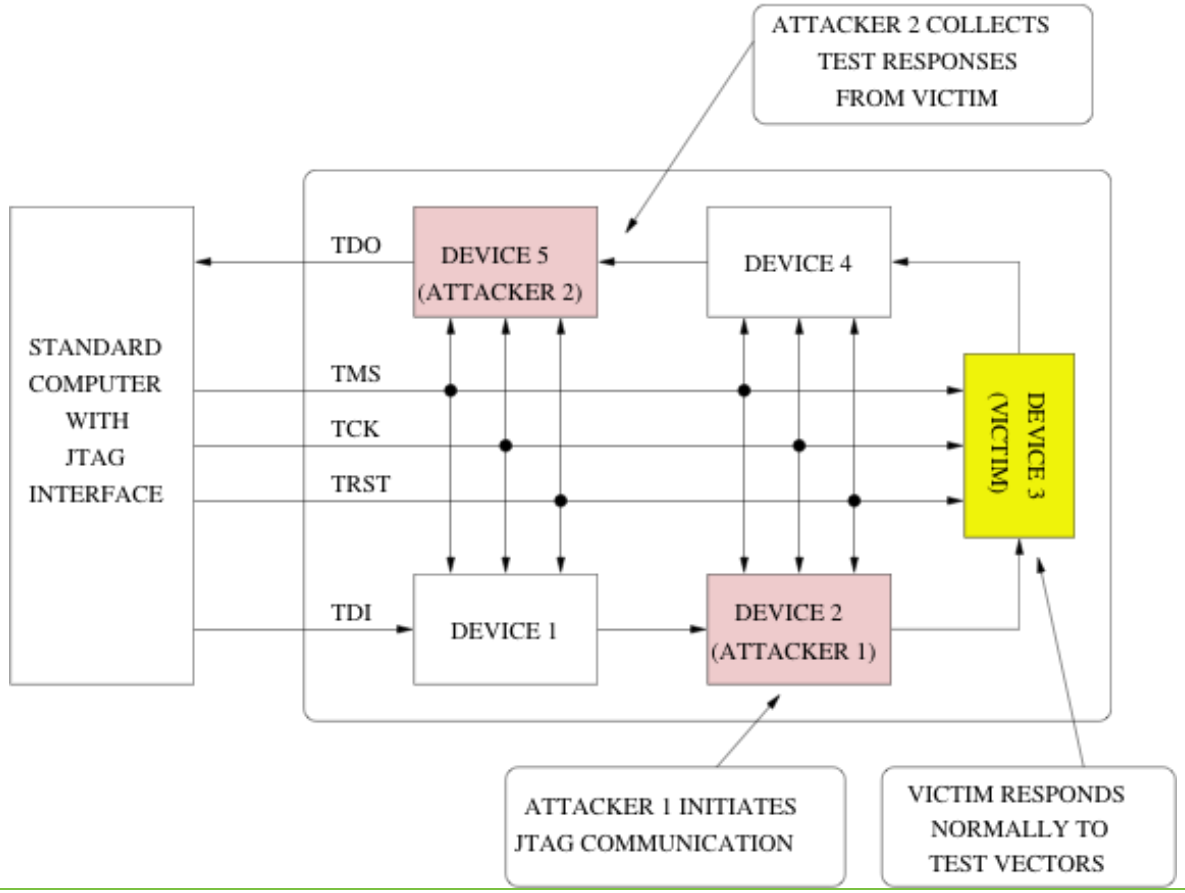


K. Rosenfeld and R. Karri, “Attacks and Defenses for JTAG”, IEEE Design & Test of Comp., pp. 36-47, 2010

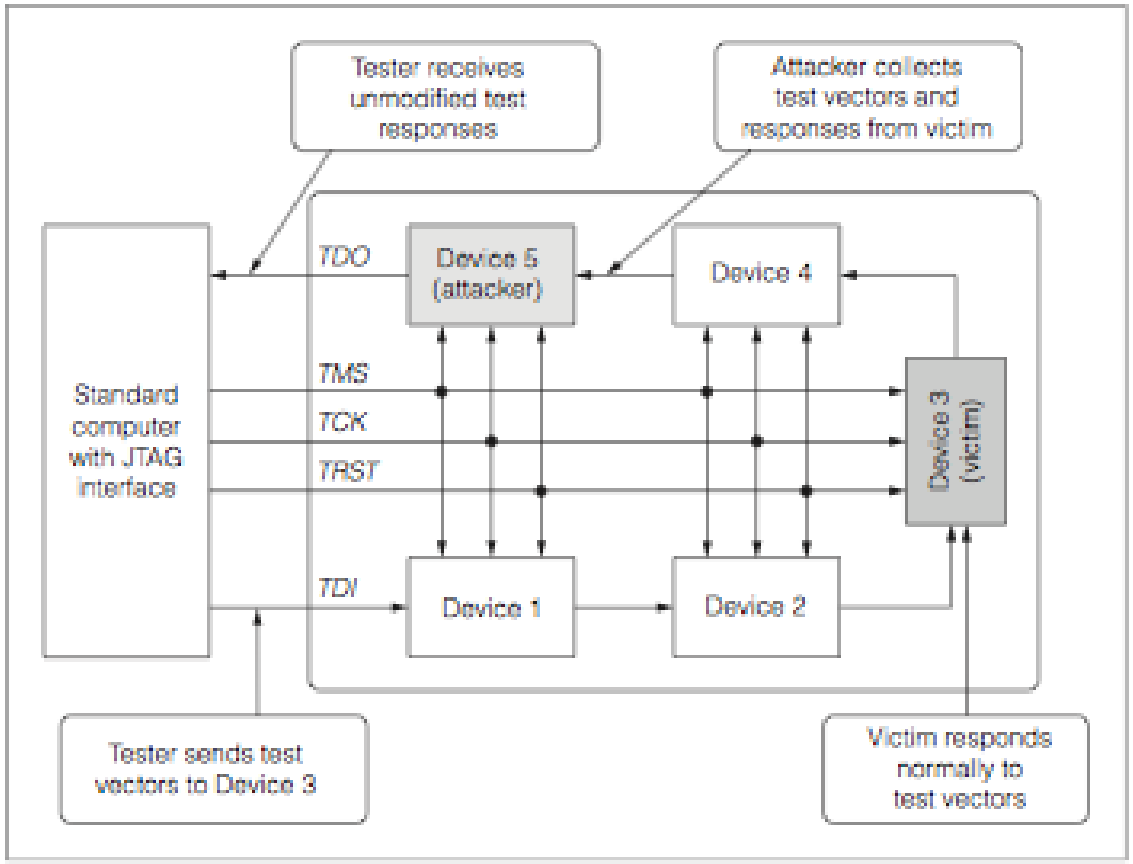
JTAG attack 1: tester gets false responses



JTAG attack 2: attacker reads secrets



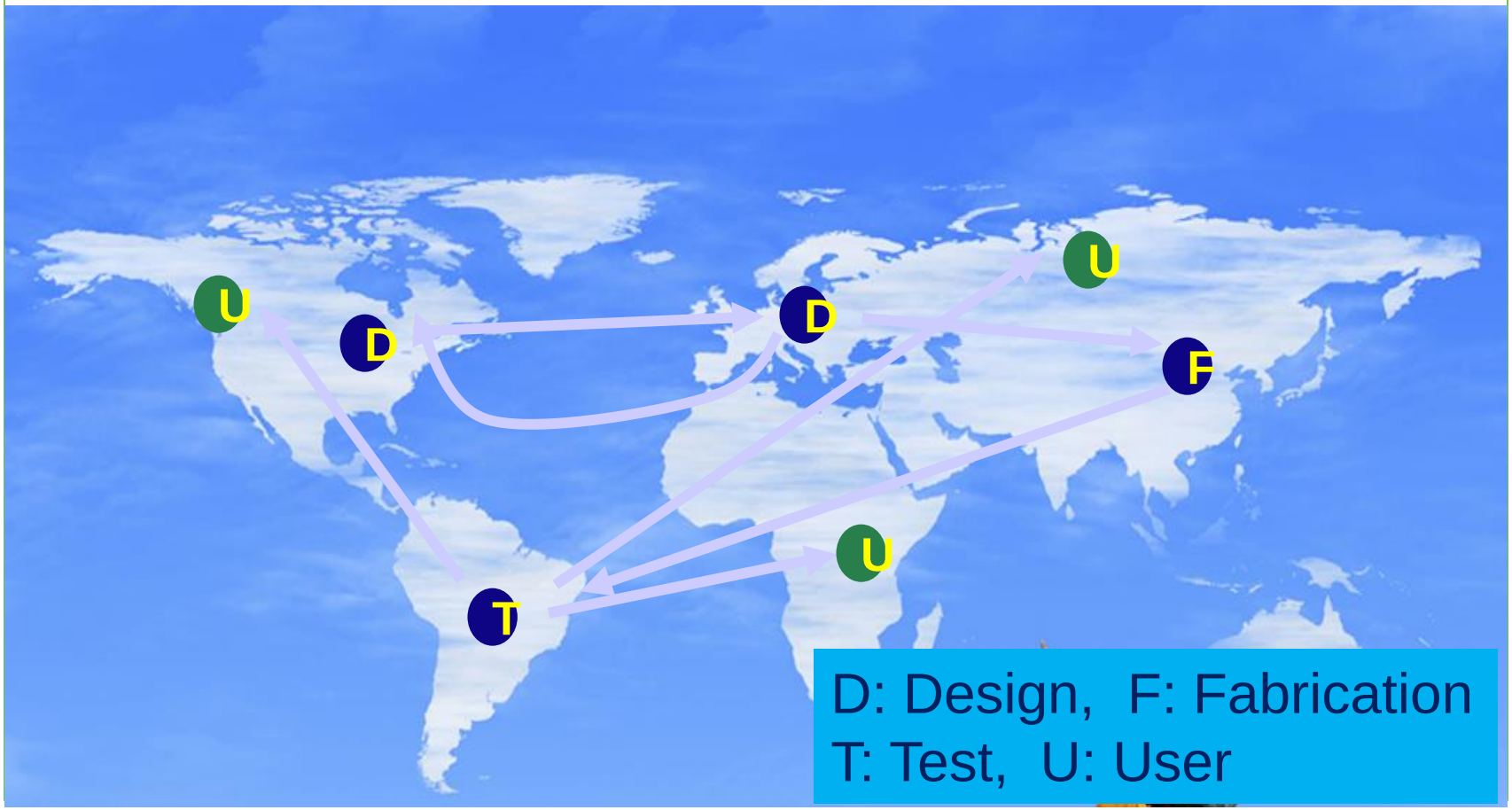
JTAG attack 3: collects test vectors



JTAG Security: defenses

Level	Authenticity	Secrecy	Integrity
0	No	No	No
1	Yes	No	No
2	Yes	Yes	No
3	Yes	Yes	Yes

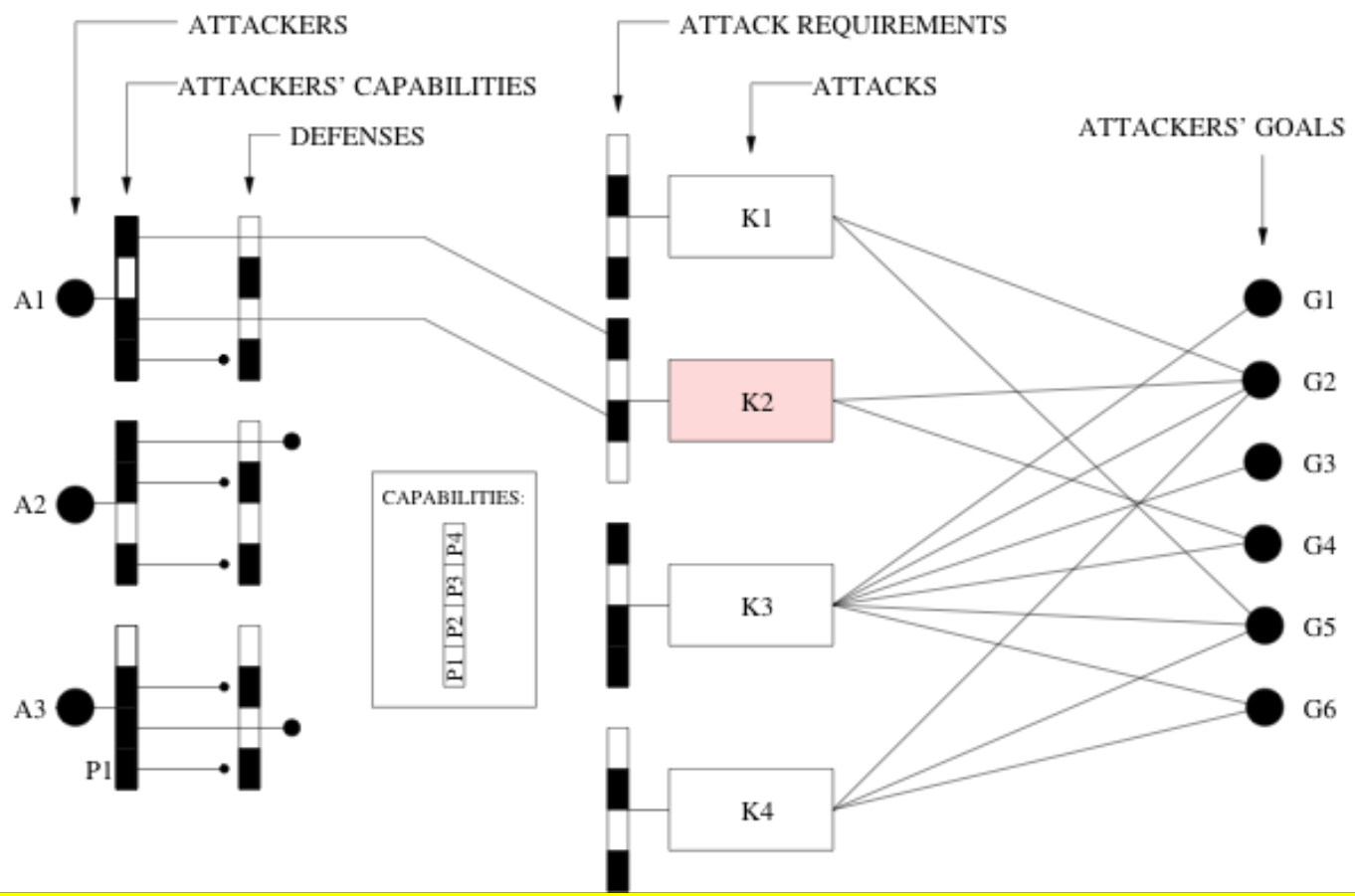
Globalized IC design flow



Hardware vulnerabilities

- Side channels
  - Power dissipation
  - Timing variation
  - Faults
  - Test infrastructure (scan, JTAG, P1500, online…)
  - interactions between side channels
- Cloning and overbuilding
- Reverse engineering
- Malicious logic (a.k.a. hardware Trojans)

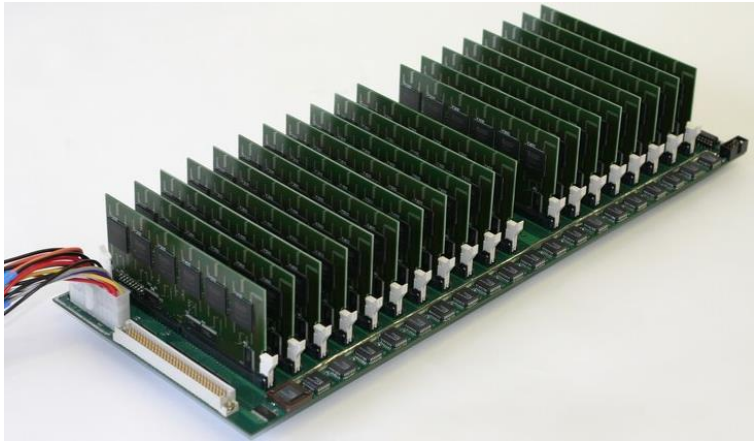
Takeaway: security- the big picture

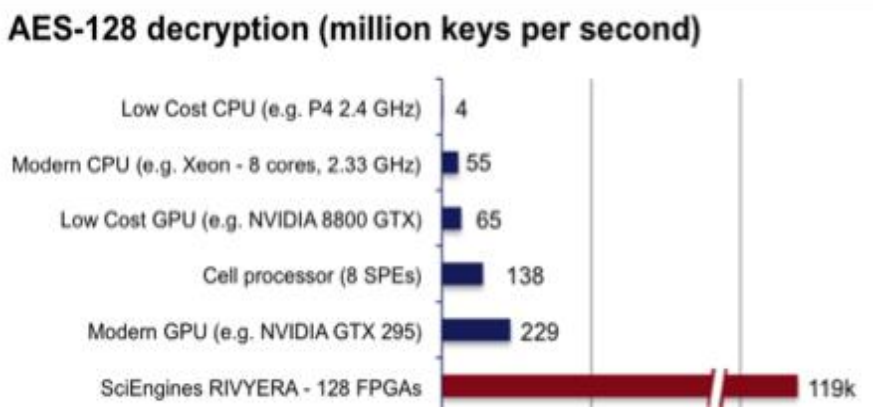


K. Rosenfeld and R. Karri, "Attacks and Defenses for JTAG", IEEE Design & Test of Comp., pp. 36-47, 2010

Takeaway: Moore' law and hacking

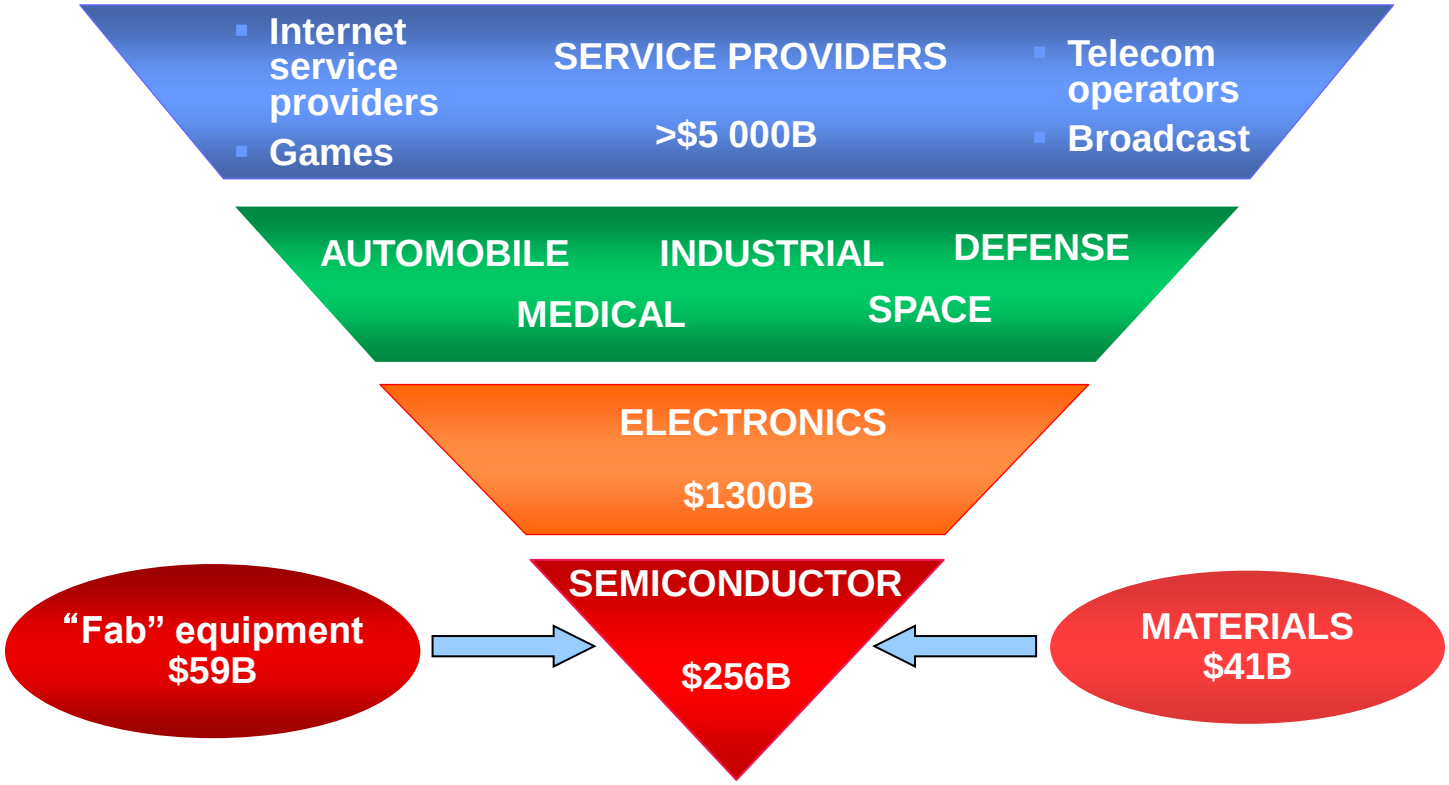
- 1970: DES was designed to withstand 30 years of cryptanalysis
- 1998: Deep Crack (custom hardware; $250,000; recover key in ~56 hrs)
- 2006: COPACOBANA (FPGAs; $10,000 recover key in ~6.4 days on avg)





http://www.sciengines.com/solutions/crypto.html

Takeaway: securing CRT is worth my time!



WSC presentation by Dr. Frank Huang, May 2008

Takeaway: Inculcate the security mindset

EL 9423: Introduction to Hardware Security and Trust
Syllabus
Class: Tuesday 10:00 AM-12:30 PM
Office hours: Monday 10:00AM-11:00 AM
Instructor: Prof. Ramesh Karri (rkarri@duke.poly.edu; phone: 718 260 3596: cell: 917 363 9703)
Pre-requisites: EL 5493/EL4313 and/or EL 5473/EL3913

Motivation: Globalization has led to outsourcing of design, fabrication, test and packaging of ICs. Rogue elements in any of these phases can alter the design and embed malicious circuits. These malicious circuits may be triggered some time in the future. Classical VLSI design and test methods are inadequate to detect these malicious circuits. Even if there are no malicious circuits in designs, side channels of an implementation can leak the secrets and intellectual property. Examples include power, timing, EM radiation and deliberately introduced faults. Finally, the testing infrastructure used to improve the quality of ICs can be used to leak secrets.
Objective: Students will be introduced to all aspects of a VLSI design. The students will be exposed to defenses that can detect and protect against the variety of discussed threats. Following is a tentative list of topics that will be covered in the course:

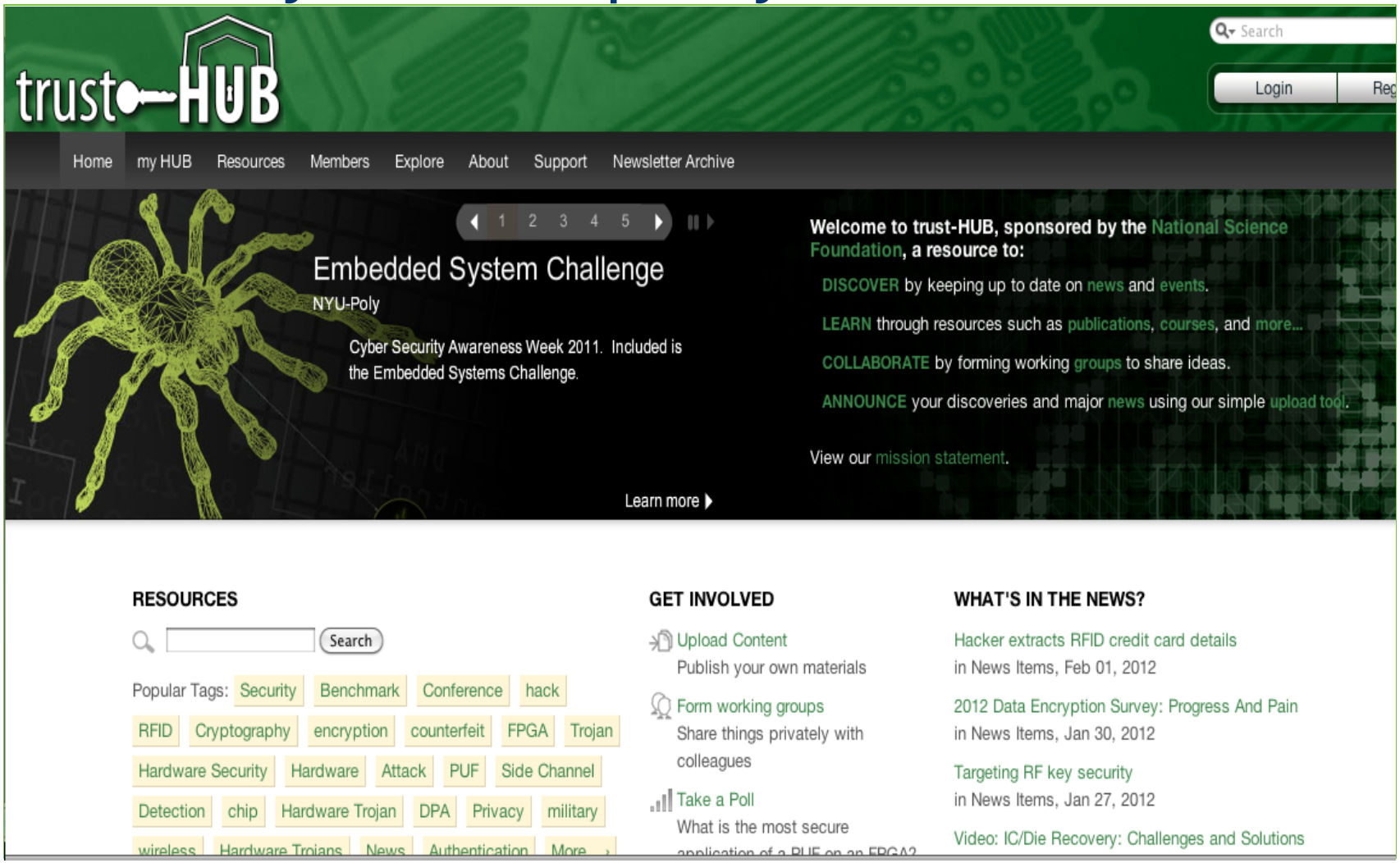
Topic	Weeks
Introduction; Homework 1 on example hardware attacks not covered in class	1
Ciphers: Historical; Block (AES/DES), stream, (Trivium) public key ciphers (RSA. ECC), hash functions (SHA-1); Homework on the various ciphers	2
	2
	2
	2
	1
	1
	2
	1
	1

ple projects
ult and test
tacks etc…
Information
n Hardware
rdware and
EE explore

n: 10%

- White hat hardware hacking =>security mindset
- Design for security
  - Logic design+security
  - offline test+security
  - online test+security
  - PUFS, RNGs, …
- Labs
- Summer school: 6 weeks in July; (hardware) cybersecurity

Takeaway: Build capacity



Conclusions

- Critical infrastructures are unprotected (power grid, water, finance, etc) $\Rightarrow$ risks are real
- Do not wait for a disaster due to IC (in)security to initiate research and development
- Industry is losing US $1-10 billion per year because of counterfeit electronics (probably more world wide)
- Enhance competitiveness in microelectronics
  - Supply chain and design environments are untrusted
  - cannot secure software, systems and networks unless we secure the core root of trust

- Questions?

  rkarri@nyu.edu,