Security in the Age of Nanocomputing

Matthew Tan Creti

Hacking Devices

The ESA estimates its total worldwide losses due to piracy at $3 billion annually [2]

One million unlocked iPhones could cost Apple $300 to $400 million in future revenue and profit [1]

Side Channel Attacks

- Classical cryptography considers abstract computational adversaries, modeled as Turing machines
- Physical cryptography takes into account specific implementations
- Information that an adversary can use to crack a device include:
  - Power consumption
  - Electromagnetic radiation
  - Computation timing
- Chips can also be attacked by purposely injecting faults

Trends of Nanocomputing

- Nanotechnology is enabling ubiquitous embedded devices (e.g. media players, mobile ad-hoc networking, RFID, smart cards, sensor networks)
- “With this ‘embedded systems everywhere’ paradigm comes an ‘embedded security everywhere’ question” [3]

Security of Scan Test Enabled Chips

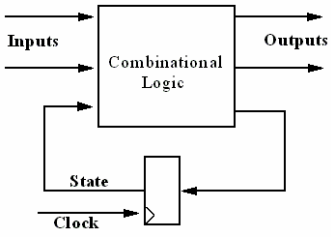
Jeremy Lee, Mohammad Tehranipoor, Chintan Patel, Jim Plusquellic. "**Securing Designs against Scan-Based Side-Channel Attacks**," IEEE Transactions on Dependable and Secure Computing, October 2007.

Levels of Hackers

1. *Beginners* are just getting started or hack out of curiosity. They rarely put in great effort unless they have access to step by step information. A simple encoding scheme may be enough to deter them.
2. *Independent* class know where to find what they need and are willing to put time, effort, and money into their endeavor. This class should not be underestimated, strong encryption algorithms should be used.
3. *Business* class are trying to get a step ahead of their competition. If the cost outweigh the gains they may give up. Short of that, protecting IP from the business hacker is very difficult.
4. Government class is nearly impossible to protect against due to almost unlimited resources.

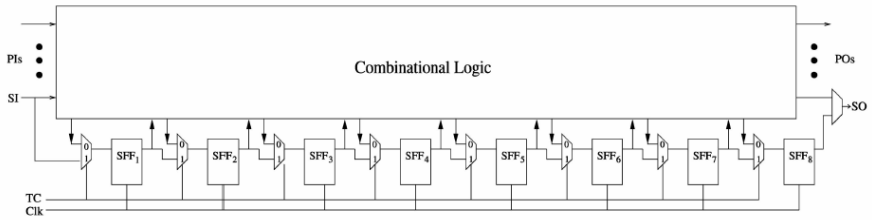
Scan Testing and Nanotech Trends

- Scan testing is the standard method for testing chips because it has high fault coverage and low overhead
- As chip densities continue to increase tests that are reliable and fast will become even more important



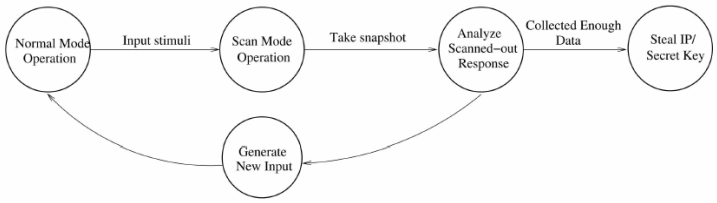
Tests for high fault coverage of unmodified sequential logic can be difficult to generate and slow to execute.

Scan Test



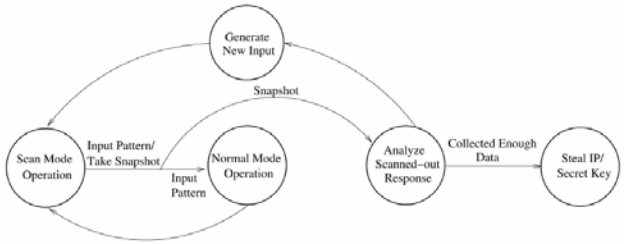
- The flip-flops of a regular sequential logic circuit are replaced with scan flip-flops that form a *scan chain*
- *Test Control* (TC) selects between test and functional mode using two-to-one multiplexers
- A new test pattern is shifted into the flip-flops though the *Scan In* (SI) pin with the results of the previous pattern is read on the *Scan Out* (SO) pin
- It is low overhead because the only extra pin added to primary I/O it TC

Scan-Based Observability Attack



- We assume a hacker knows chip timing from the datasheet
- This gives the hacker a good idea of what registers are being written to on a chip at any given time
- By feeding in well planed inputs and then and then taking snapshots of the chip at different times the hacker may be able to reverse engineer a chip or steal a vital key from a cryptochip
- This form of attack exploits the property that a scan test enabled chip should be easily observable

Scan-Based Controllability and Observability Attack

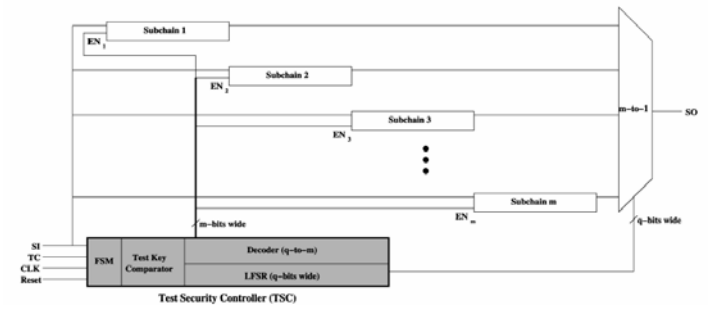


- Attack starts in scan mode
- By applying random patterns the hacker tries to expose random faults that bypass security
- By analyzing the output when faults are present or not present the hacker can deduce properties of the chip
- This form of attack exploits the property that a scan test enabled chip should be easily observable and controllable

Possible Solutions

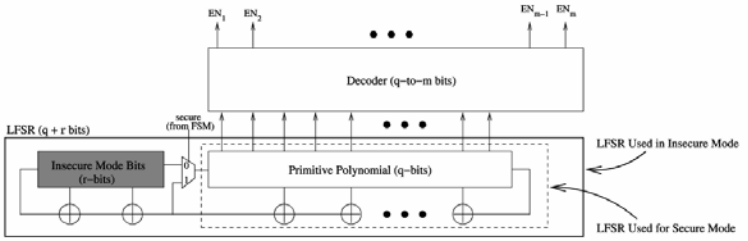
- Built-In Self Test (BIST) can perform on chip testing of the most sensitive parts of a chip while scan testing is applied to the rest. This compromise sacrifices some testability for security.
- Fuses have become popular in smart card security. However, it has been shown that fuses can be reconnected and fuses also eliminate the ability to perform in-field testing.

Lock and Key



- A *Test Security Controller* (TSC) makes the scan chain more difficult to access and manipulate in test mode
- The scan chain is split into m subchains
- A linear feedback shift register (LFSR) selects the order in which subchains are enabled
- When a user presents the correct key, the LFSR is seeded with a known value, otherwise the LFSR is seeded randomly when the chip starts up (is it easy to bias a random generator?)

LFSR Predictability



- In secure mode (i.e. the user provided the correct key) the LFSR is based on primitive polynomials
- Primitive polynomial ensures that every subchain is selected once and only once in a round
- To reduce predictability of the LFSR extra bits are added to make it non-primitive polynomial in insecure mode

Steps to Hack

1. Hackers must learn what security strategy is being used.
2. Then they must find the secret key to make operation of the chains predictable. There are 2^k possibilities where k in number of bit in key.
3. Then they must determine the pseudorandom order of the LFSR. There are 2^q possible orders in secure mode and 2^{q+r} in unsecure mode where q is the bit size of the LFSR in secure mode and r is the number of bits added in insecure mode.

Overhead

Number of Gates in TSC for 4-Bit, 8-Bit, and 12-Bit

Number of LFSR Bits (q)	Size of FSM	Size of Test Key Comparator	Size of LFSR ($q+r$)	Size of Decoder	Total Size of TSC	% Overhead s38417	% Overhead s38584
4-bit LFSR	113	54	48	25	327	**2.9**	**3.8**
8-bit LFSR	133	54	71	307	652	**5.7**	**7.5**
12-bit LFSR	153	54	91	5432	5817	50.8	66.8

References

1. Connie Guglielmo, “Apple Users Unlocked 1 Million IPhones, Analyst Says,” bloomberg.com, January 2008.
2. Eric Bangeman, “Console mod-chippers busted in nationwide raids,” arstechnica.com, August 2007.
3. Jean-Jacques Quisquater and François Xavier Standaert, “Physically Secure Cryptographic Computations: From Micro to Nano Electronic Devices,” Workshop on Dependable and Secure Nanocomputing 2007.
4. Jeremy Lee, Mohammad Tehranipoor, Chintan Patel, Jim Plusquellic. “Securing Designs against Scan-Based Side-Channel Attacks,” IEEE Transactions on Dependable and Secure Computing, October 2007.