08 Hardware Metering

Engr 399/599: Hardware Security

Grant Skipper, PhD.

Indiana University

Adapted from: Mark Tehranipoor of University of Florida

Course Website

engr599.github.io

Write that down!

Agenda

Project 2 Assigned:
https://github.com/ENGR599/P2_Obfuscation/tree/2024_update

Due 3/10/24 - Same Groups!!

Review last class.

Vote on Midterms - before or after break?

Finish HW Metering, Begin Watermarking?

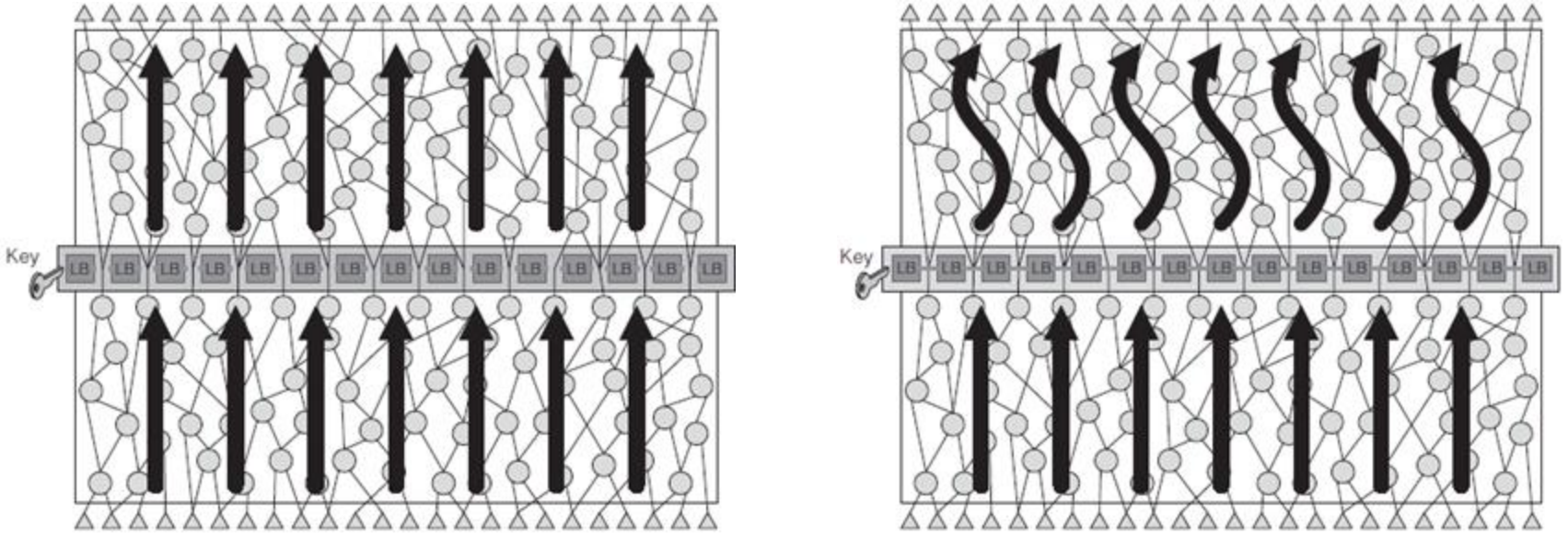
What is an eFPGA?

IP core integrated into an ASIC or SoC that offers the flexibility of programmable logic without the cost of FPGAs.

https://www.quicklogic.com/efpga-ip/

Reconfigurable Logic Barriers (LB)

- Separates inputs from outputs such that every path from input to output passes through a barrier.
- Logic barrier (LB) is a group of logic that allows correct path only if correct key is applied.



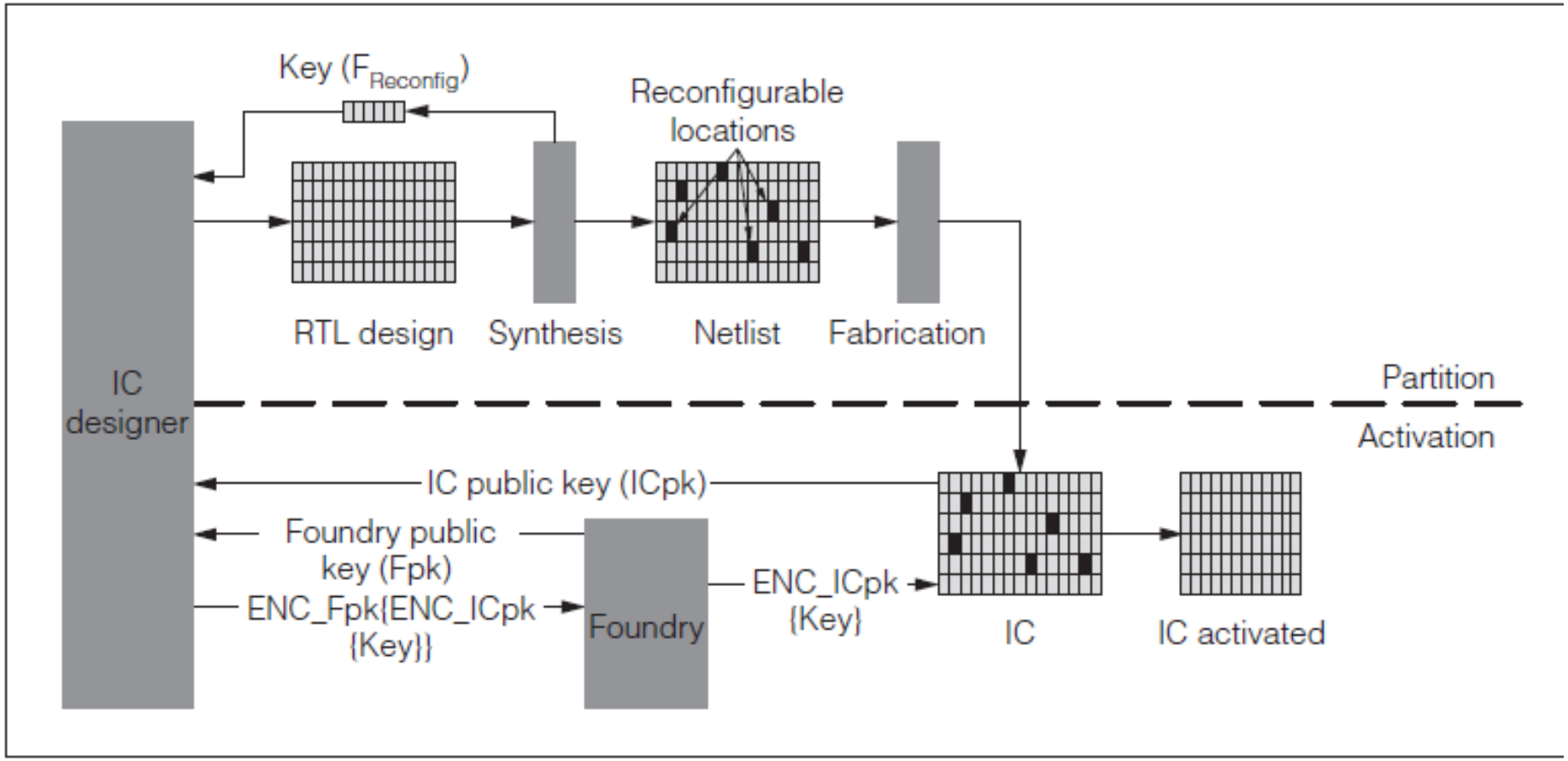
Reconfigurable Logic Barriers

- IP owner decomposes IC functionality into F_{fixed} and $F_{reconfig}$.
- F_{fixed} is given to foundry to fabricate.
- $F_{reconfig}$ is location of reconfigurable logic in combination with key needed to configure them correctly
- $F_{reconfig}$ can be programmed into reconfigurable locations using a secure key.

LB: Public Key Cryptography

- ICs use PUFs or TRNGs to generate a private and public random keys.
  - Public key from chip is sent to IP Owner
- IP Owner uses public key and its own private key to encrypt unlocking key.
  - Encrypted key is decrypted on chip using IP Owner's public key and chip's private key.

LB: Partitioning of Design



Logic Barriers Analysis

- **Effective against cloned ICs.**
  - Chips are only functional if correct key is entered which only IP Owner can provide
- **Ineffective against over-produced, defective, and out-of-spec ICs**
  - Foundry can lower yield in order to receive additional keys to activate functionality.
  - Key generated by chip does not have information about its functionality. Once key is applied, chip is functional.
- **Disadvantages:**
  - Look up tables require significant area overhead – 5X more than using XOR gates, and timing overhead.

Test Seems to be a Challenge!

Designer

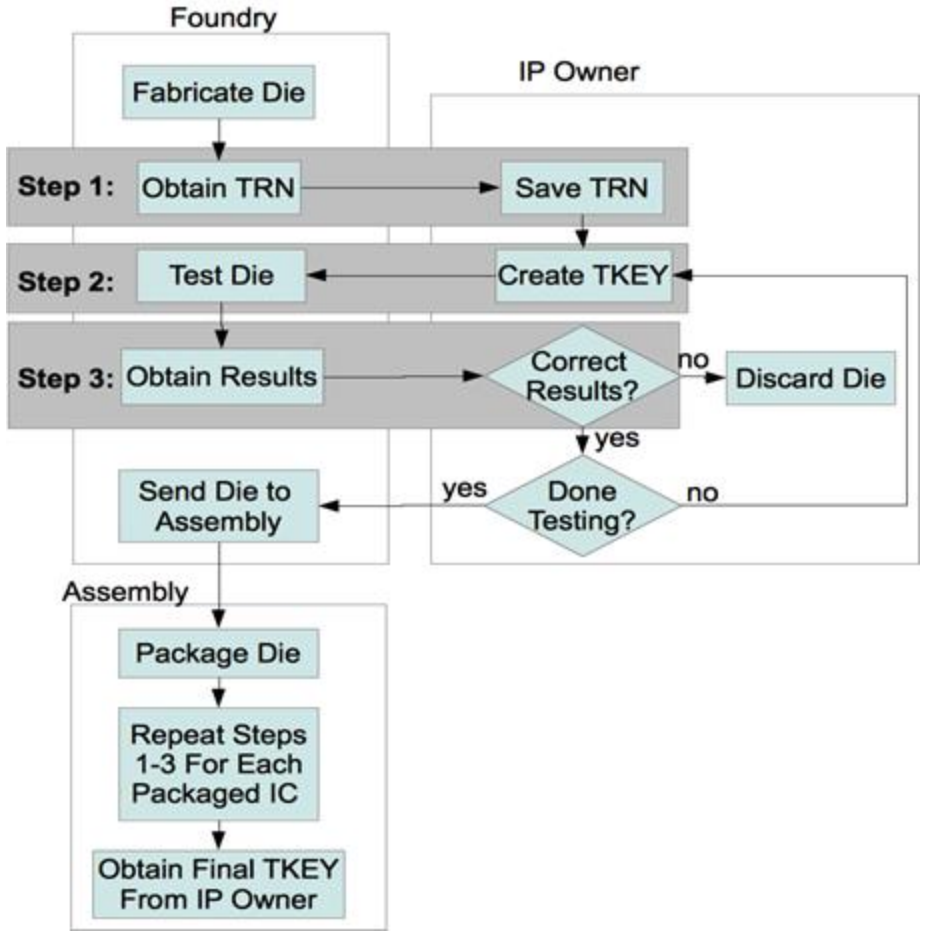
Test Patterns
Test Responses

Most techniques do not take into account the role “test” plays in the decision making process

Foundry & Assembly

Secure Split-Test (SST)

- Adds multiple layers of communication between IP owner, foundry, and assembly
- Ensures that IP owner will know exactly how many chips pass the test and how many have failed.
- Only chips that IP Owner has deemed functional will be given a functional key.



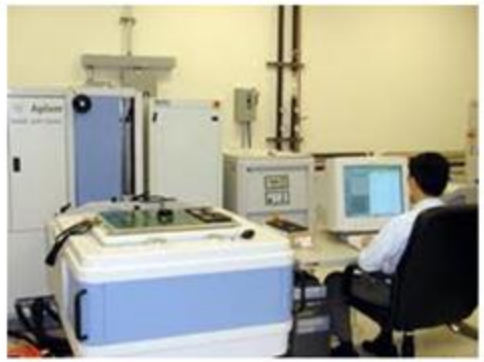
Secure Split-Test

Designer

1. Designer has already put in hooks in the design that can ensure non-functional operation if the correct key is not included in the chip
2. Detecting a non-functional chip is significantly easier than using PUF and dealing with process variations

Secure Spilt Test

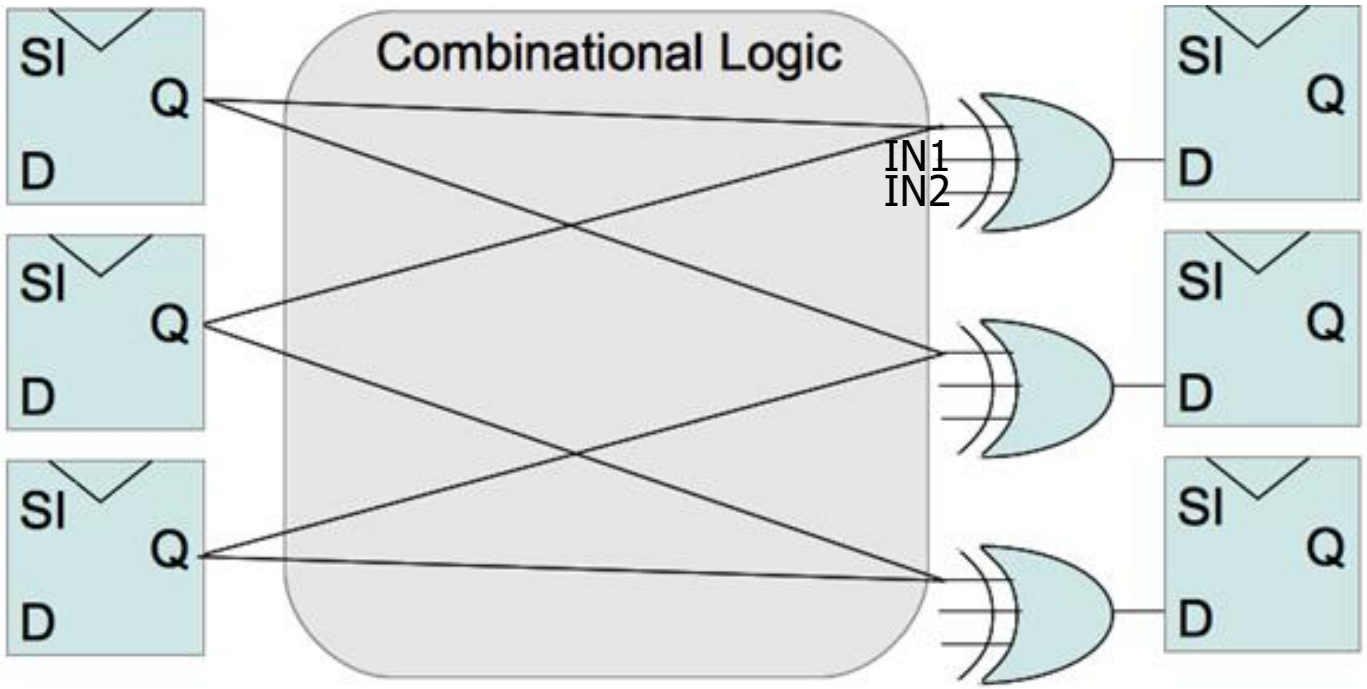
1. Foundry will not be able to ship any functional chips to the market
2. Same for defective chips and out-of-spec chips; the chips are simply non-functional.



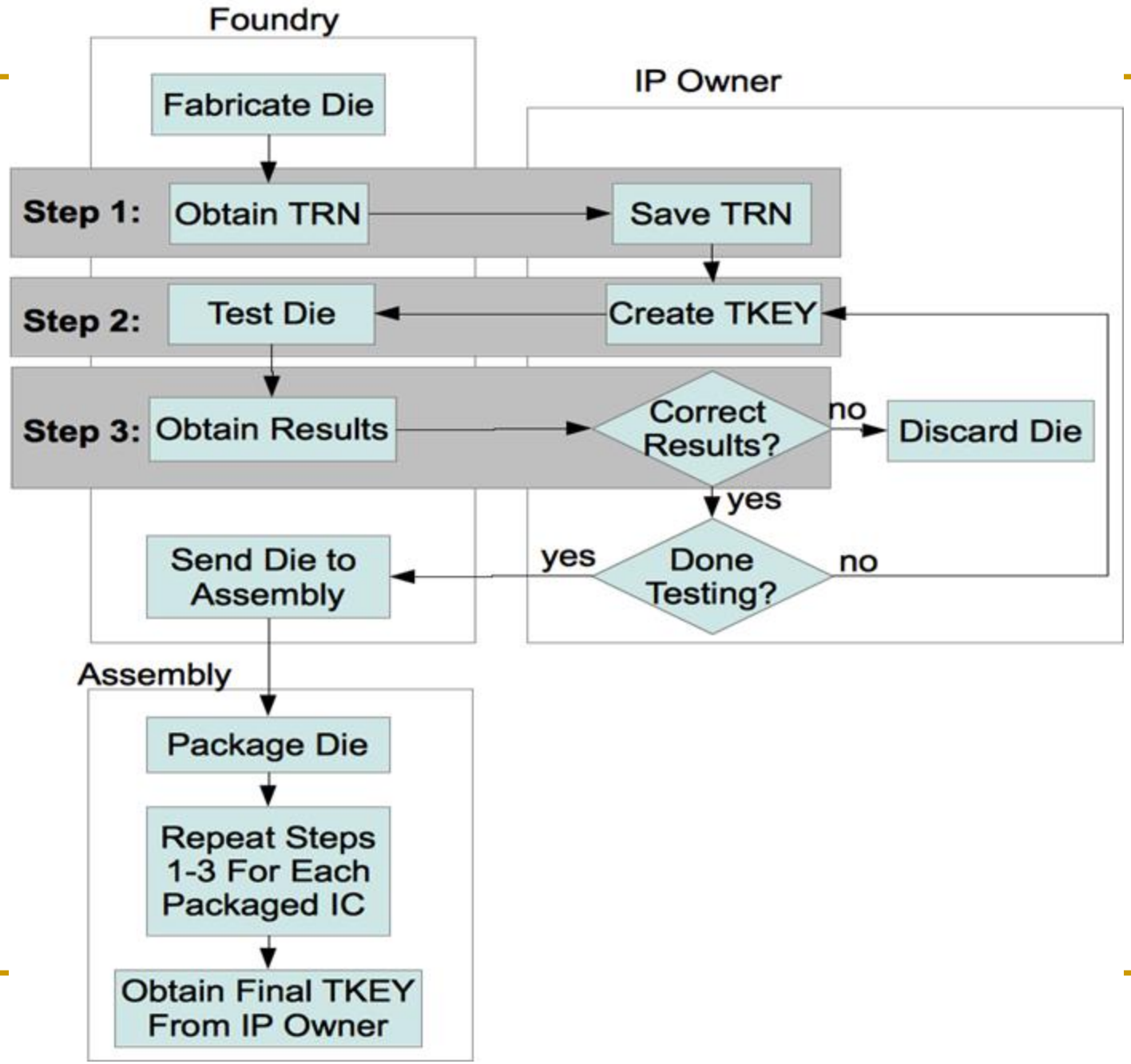
Foundry & Assembly

XOR Mask

- **Three-input XOR logic added to non-critical paths.**
- **XOR logic additional inputs are IN1 and IN2**



SST


Foundry
Fabricate Die
IP Owner
Step 1:
Obtain TRN
Save TRN
Step 2:
Test Die
Create TKEY
Step 3:
Obtain Results
Correct Results?
no
Discard Die
yes
Send Die to Assembly
yes
Done Testing?
no
Assembly
Package Die
Repeat Steps 1-3 For Each Packaged IC
Obtain Final TKEY From IP Owner

SST Analysis

- Effective against overproduced ICs, cloned ICs, and defective ICs
  - **Overproduced**:
    - IP Owner has control over number of TRNs received and TKEY/FKEYS sent to foundry/assembly
  - **Cloned**:
    - Chips are not functional unless FKEY has been produced by IP Owner
  - **Defective ICs:**
    - Foundry sends test results to foundry who checks results and decides if chip has correct test responses (chip is not yet functional at this stage)

SST Analysis

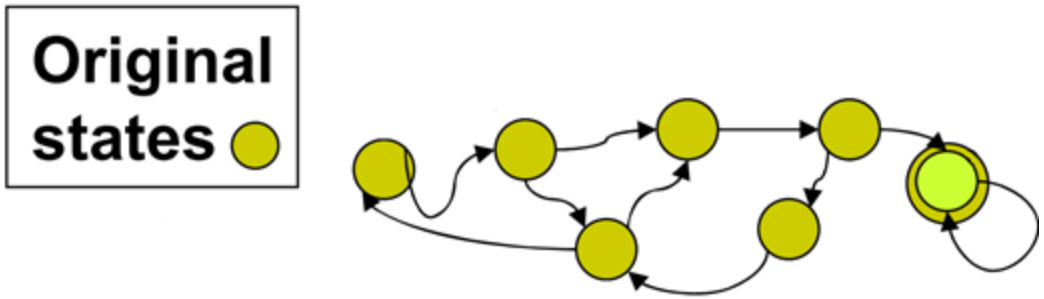
- **Prevents out-of-spec ICs**
  - Some specifications cannot be determined from patterns testing alone. If a chip does not meet these specifications, it could be considered as a passing chip.
  - With the addition of a few sensors on the chip, these specifications can be tested and checked by IP Owner during SST
  - The IP owner will then be able to decide whether or not a chip passes the desired specifications in order to prevent out-of-spec ICs from going into market.

Remote Activation of ICs Through FSM Modification

- FSM: Finite State Machine
- Sequence of inputs drive machine through different functional states
- Correct transitions give functional output

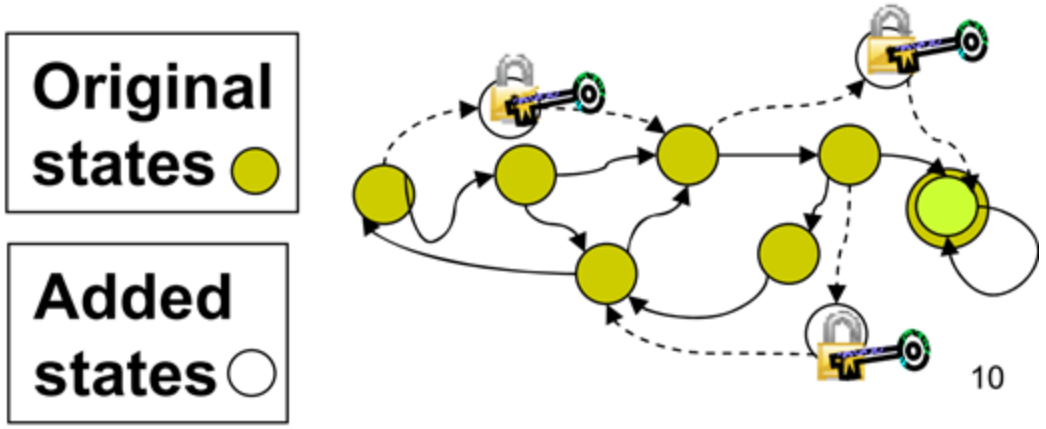
FSM

- Correct transitions give functional output



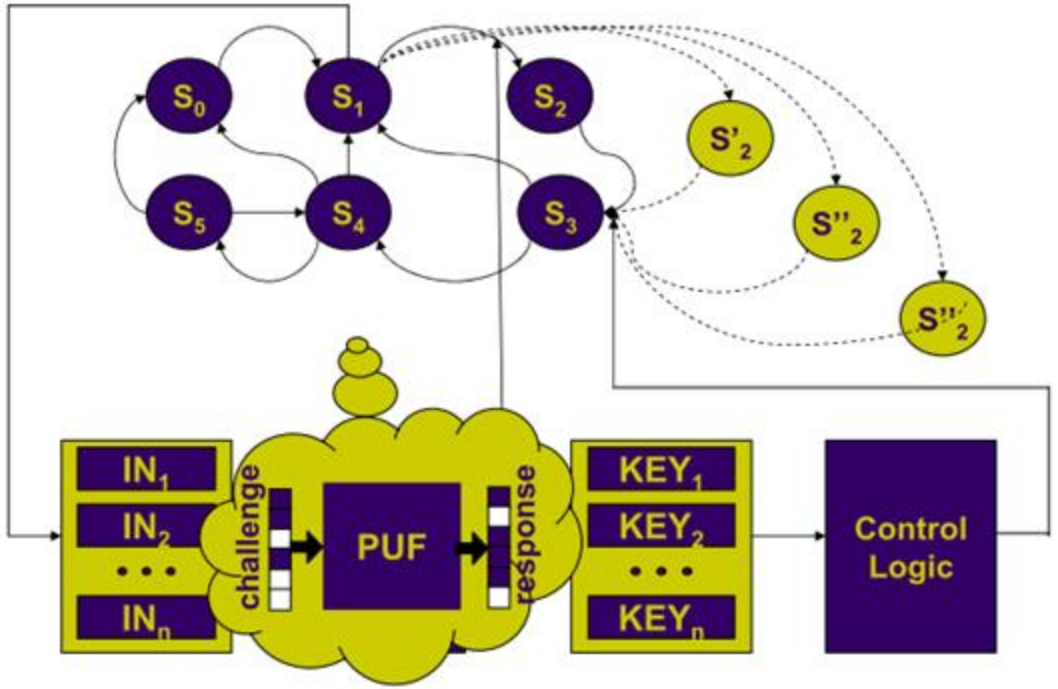
- Adding states to FSM gives IP owner controllability over sequence to reach functional states.

Boosted FSM (BFSM)



- On startup, inputs cause chip to go to one of added states
- IP Owner is only one with knowledge of FSM
- Only IP Owner knows right sequence (key) to bring FSM back to functional states.

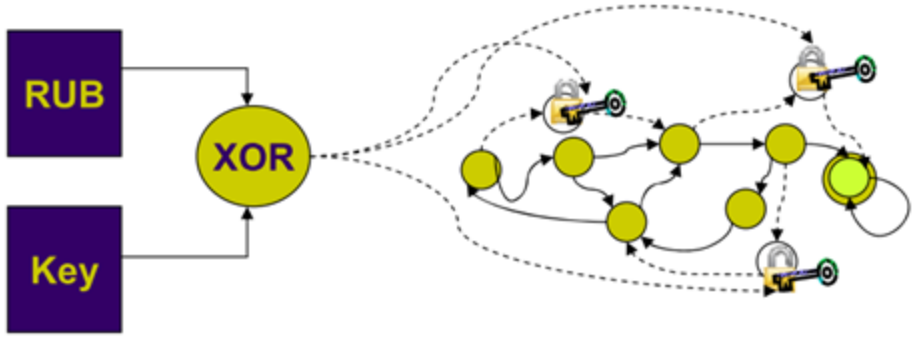
Remote Activation of ICs



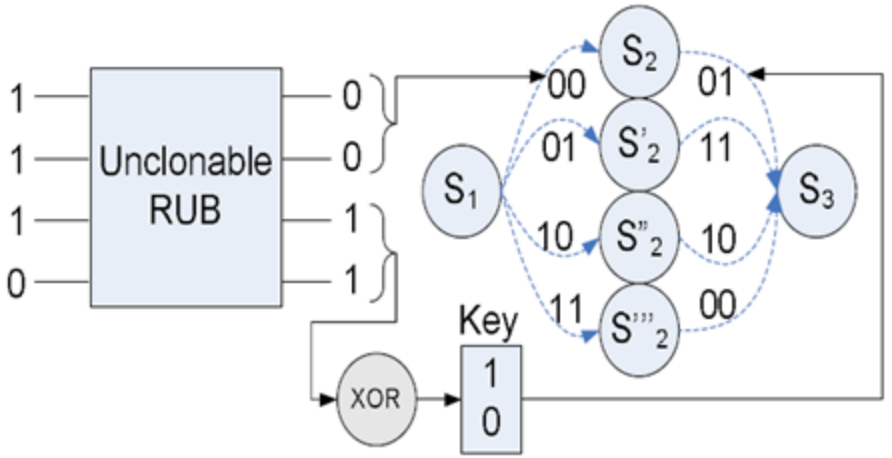
- Redundant states are added.
- Far less states needed than BFSM
- PUF response will send FSM to one of redundant states.

- **Challenge**: PUF is yet to be reliable.

Remote Activation of ICs



- RUB: Random Unique Block
- RUB must be stable – not change over time



- PUF (RUB) response is sent to IP Owner to generate key
- Key is then used to send FSM to correct state.

Analysis of Boosted FSM and Remote Activation

- BFSM requires many additional FSM states.
- Remote activation only uses a few redundant states.
- Both use PUF which is affected by age, temperature, noise, etc.
- Both effective against cloned ICs but not effective against defective, over-produced, or out-of-spec ICs.

References

- F. Koushanfar and G Qu. Hardware Metering. In DAC 2001, 2001
- Y. Alkabani and F. Koushanfar. Active Hardware Metering for Intellectual Property Protection and Security. In USENIX Security, 2007
- F. Koushanfar, G. Qu, and M. Potkonjak. Intellectual Property Metering. In IH, pp.81-95, 2001.
- J.A. Roy, F. Koushanfar, and I.L. Markov. EPIC: Ending Piracy of Integrated Circuits. In EDAA, 2008.
- A. Boumgarten, A. Tyagi, and J. Zambreno. Preventing IC Piracy Using Reconfigurable Logic Barriers. In IEEE Design and Test of Computers, 2010
- M. Tehranipoor and C. Wang. Introduction to Hardware Security. Springer, pp. 103-120, 2012
- Y. Alkabani, F. Koushanfar, M Potkonjak. Remote Activation of ICs for Piracy Prevention and Digital Rights Management. In IEEE, 2007
- M. Tehranipoor. VLSI Design Verification and Testing: Test Economics. http://www.engr.uconn.edu/~tehrani/teaching/test/03_Test%20Economics%20and%20Product%20Quality.pdf
- R.L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communication of the ACM, 1978.
- G. Contreras, T. Rahman, and M. Tehranipoor, ” Secure Split-Test for Preventing IC Piracy by Untrusted Foundry and Assembly," Int. Symposium on Defect and Fault Tolerance in VLSI Systems (DFT), 2013.
- T. Rahman, D. Forte, Q. Shi, G. Contreras, and M. Tehranipoor, "CSST: Preventing Distribution of Unlicensed and Rejected ICs by Untrusted Foundry and Assembly,” IEEE Int. Symposium on Defect and Fault Tolerance Symposium (DFTS), Oct. 2014.