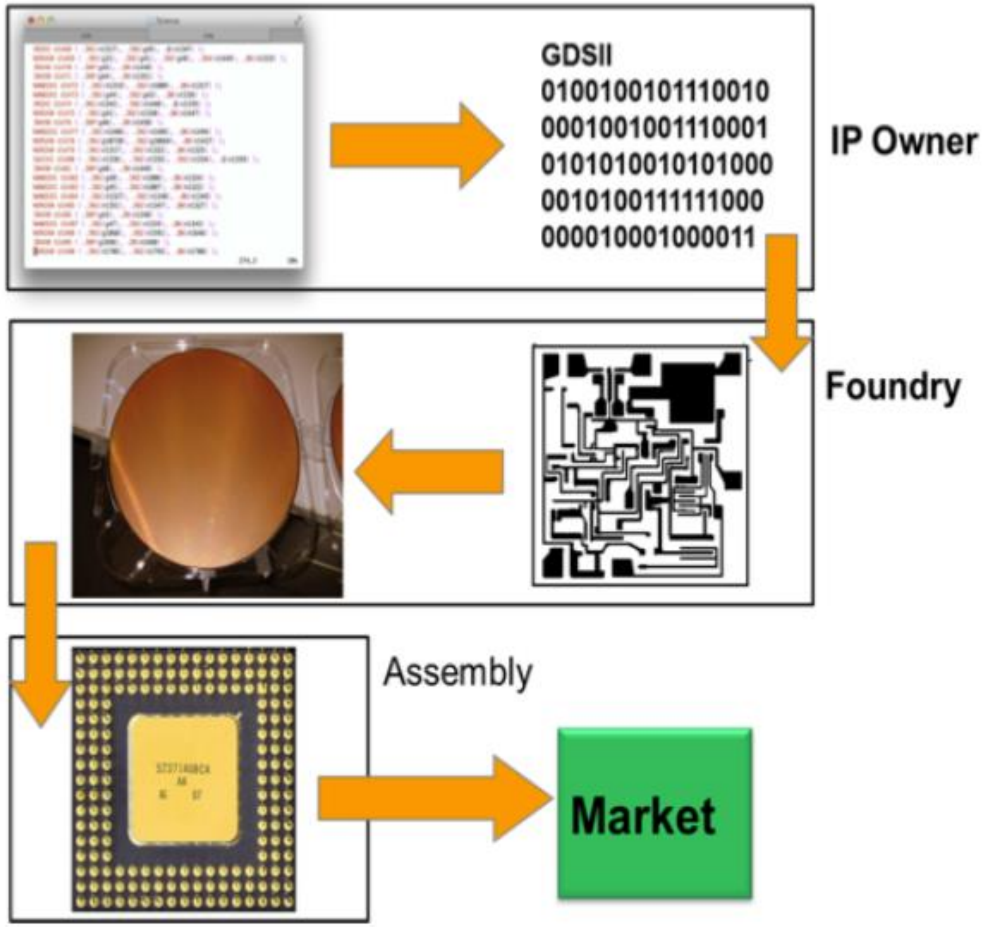
Hardware Metering

Yu Bi

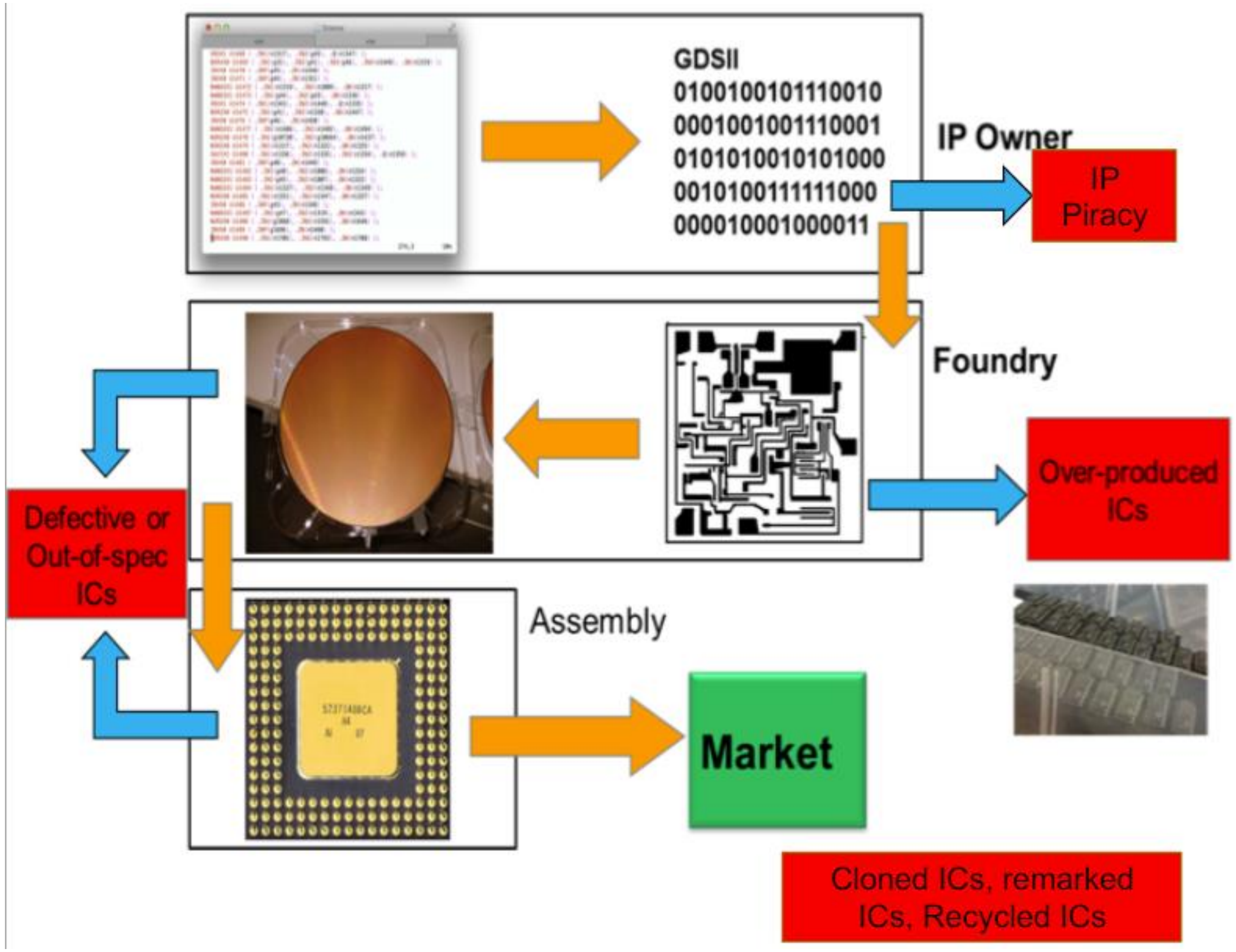
ELE594 – Special Topic on Hardware Security & Trust
University of Rhode Island

Chip Production Flow



- Little communication between IP Owner and Foundry.
- Foundry is trusted with full design.
- Responsible for production of requested amount of chips.
- IP holder provides foundry/assembly with all **test patterns** and **responses**.

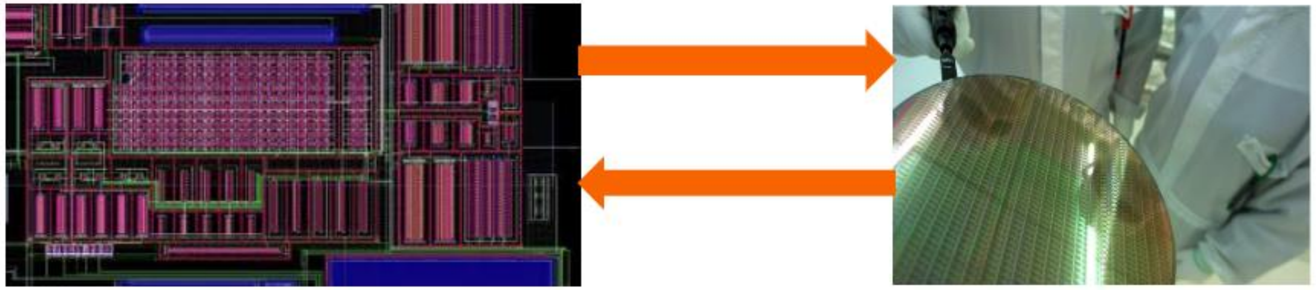
Chip Production Flow



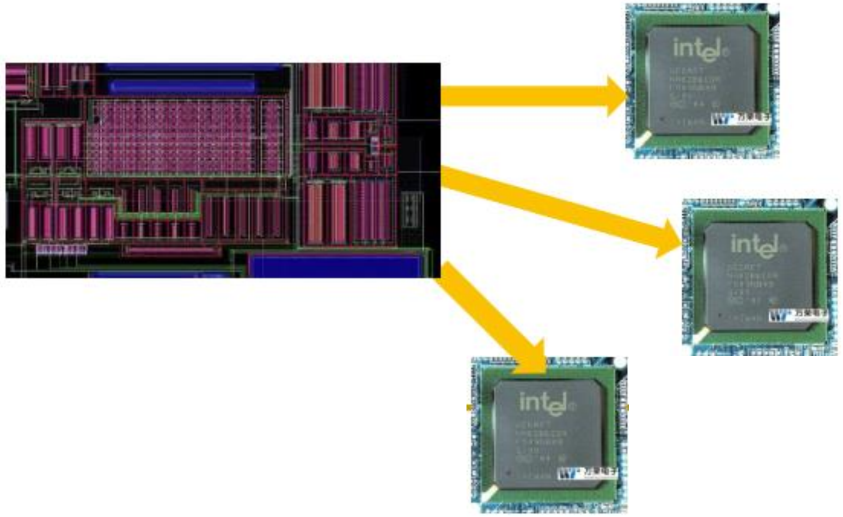
- Foundry looks for its own profit.
- Once mask is produced, producing IC's is simple and cheap.
- Lack of communication makes it difficult for owner to track produced chips.

Need for Hardware Metering

- Need for better communication between IP Owner and foundry/assembly.

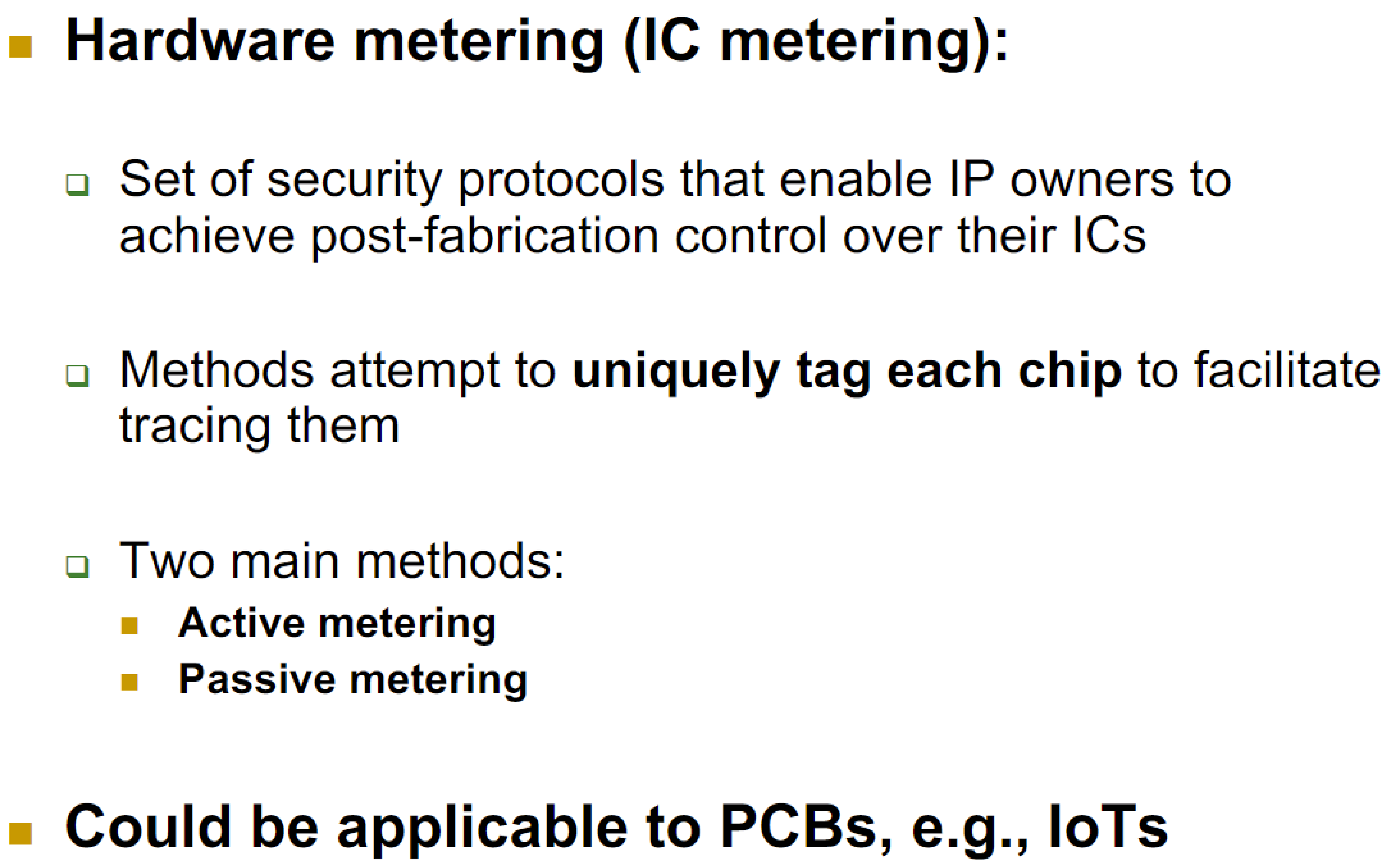


- Need for IP Owner to be able to track produced chips.



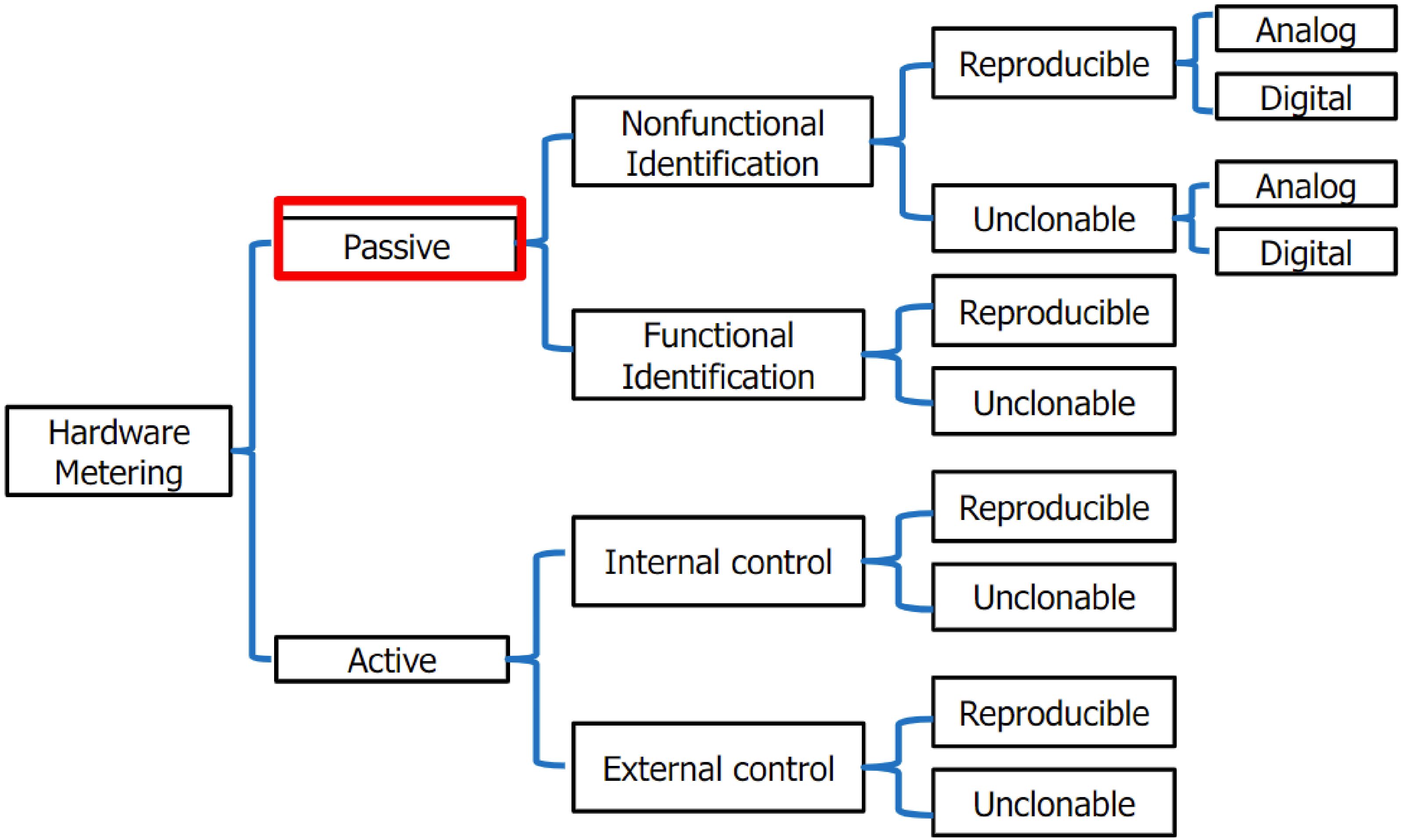
Electronic Chip ID (ECID)

Hardware Metering

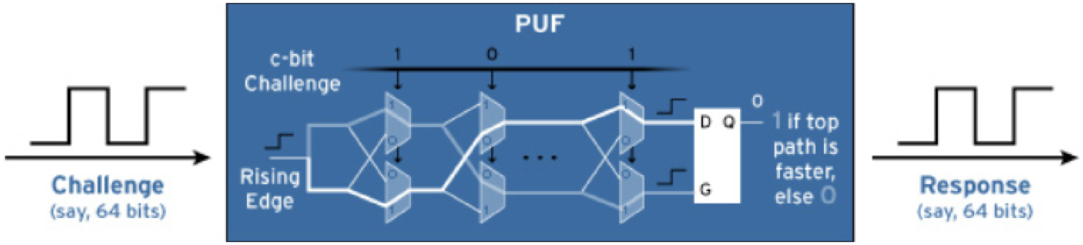


- **Hardware metering (IC metering):**
  - Set of security protocols that enable IP owners to achieve post-fabrication control over their ICs
  - Methods attempt to **uniquely tag each chip** to facilitate tracing them
  - Two main methods:
    - **Active metering**
    - **Passive metering**
- **Could be applicable to PCBs, e.g., IoTs**

Metering Methods

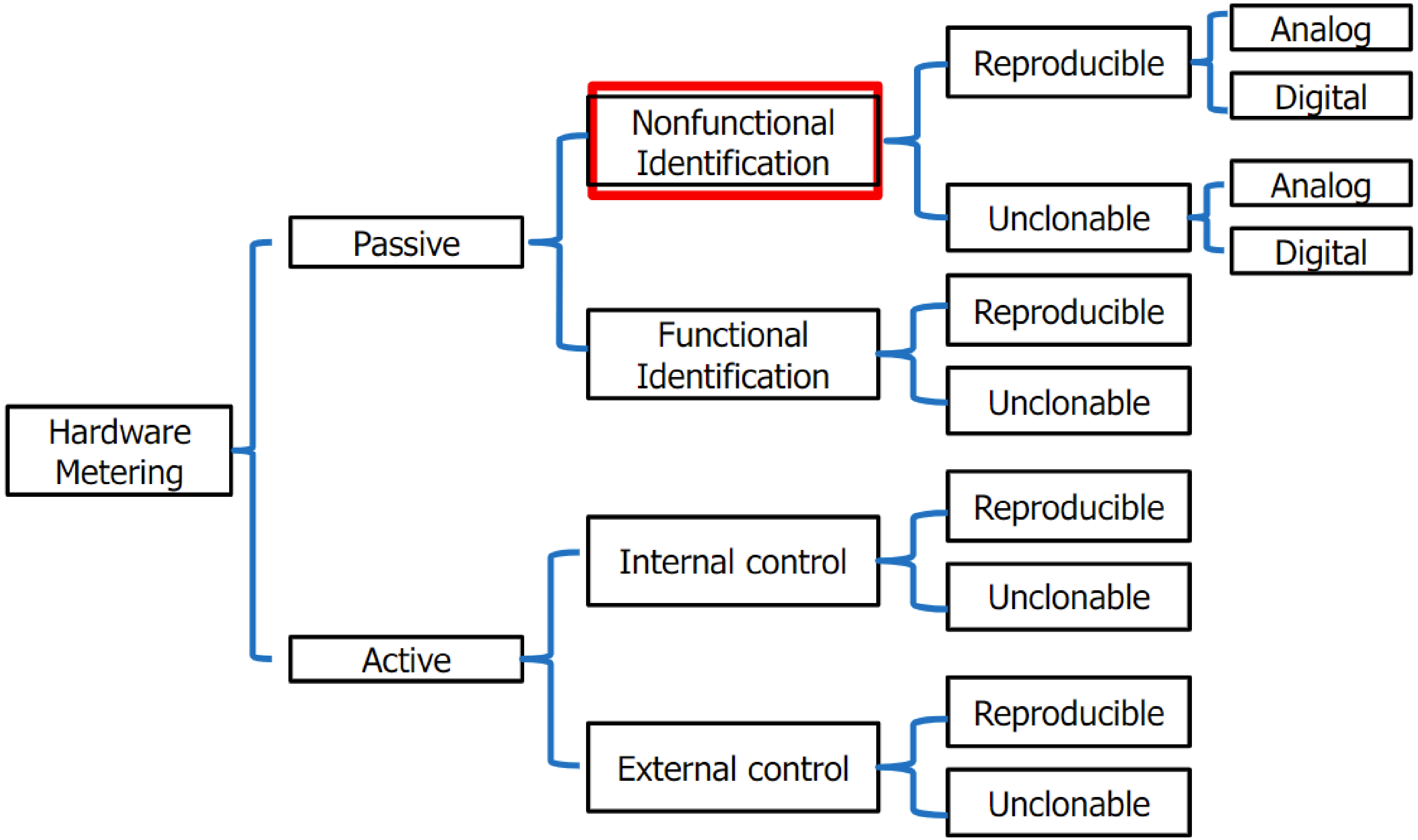


Passive Metering



- ICs can be **passively monitored**.
- Can be achieved by physically identifying:
  - Serial numbers on chips
  - Storing unique identifiers in memory. These are called Nonfunctional Identification
    - E.g., Electronic Chip ID (ECID)
- Tagging an IC’s functionality: Functional Identification

Metering Methods



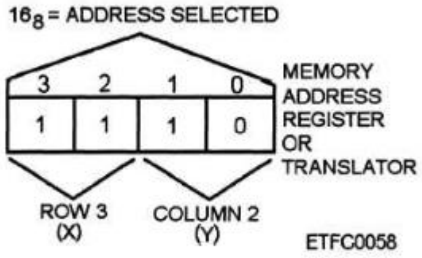
Nonfunctional Identification

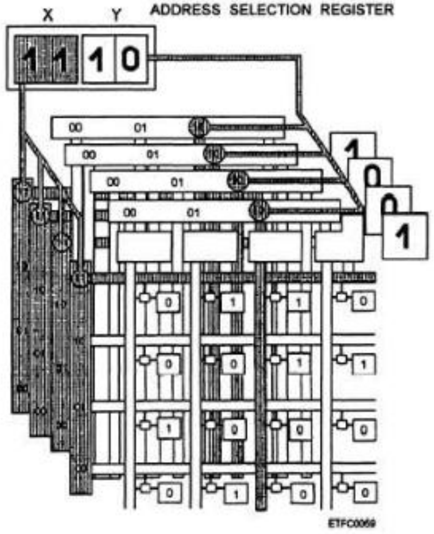
- Unique ID is separate from the chip’s functionality.

- Vulnerable to cloning and/or removal.
  - Once chip is tagged, foundry can copy same tag on other chips or simply remove tag so chip cannot be traced.
- Possible to overproduce.
  - Foundry can produce multiple chips with same tag.
  - Out of millions of chips, probability of finding two matching tags is small.
- Two main types:
  - Reproducible
  - Unclonable

Reproducible Identifiers

- Unique ID’s are stored on the chip package, on die, or in a memory on-chip.
- Examples:
  - Indented serial numbers
  - Digitally stored serial numbers
- Advantages:
  - Do not depend on randomness
  - Easy to track / identify.
- Disadvantages:
  - Easy to clone/modify
  - Easy to overproduce





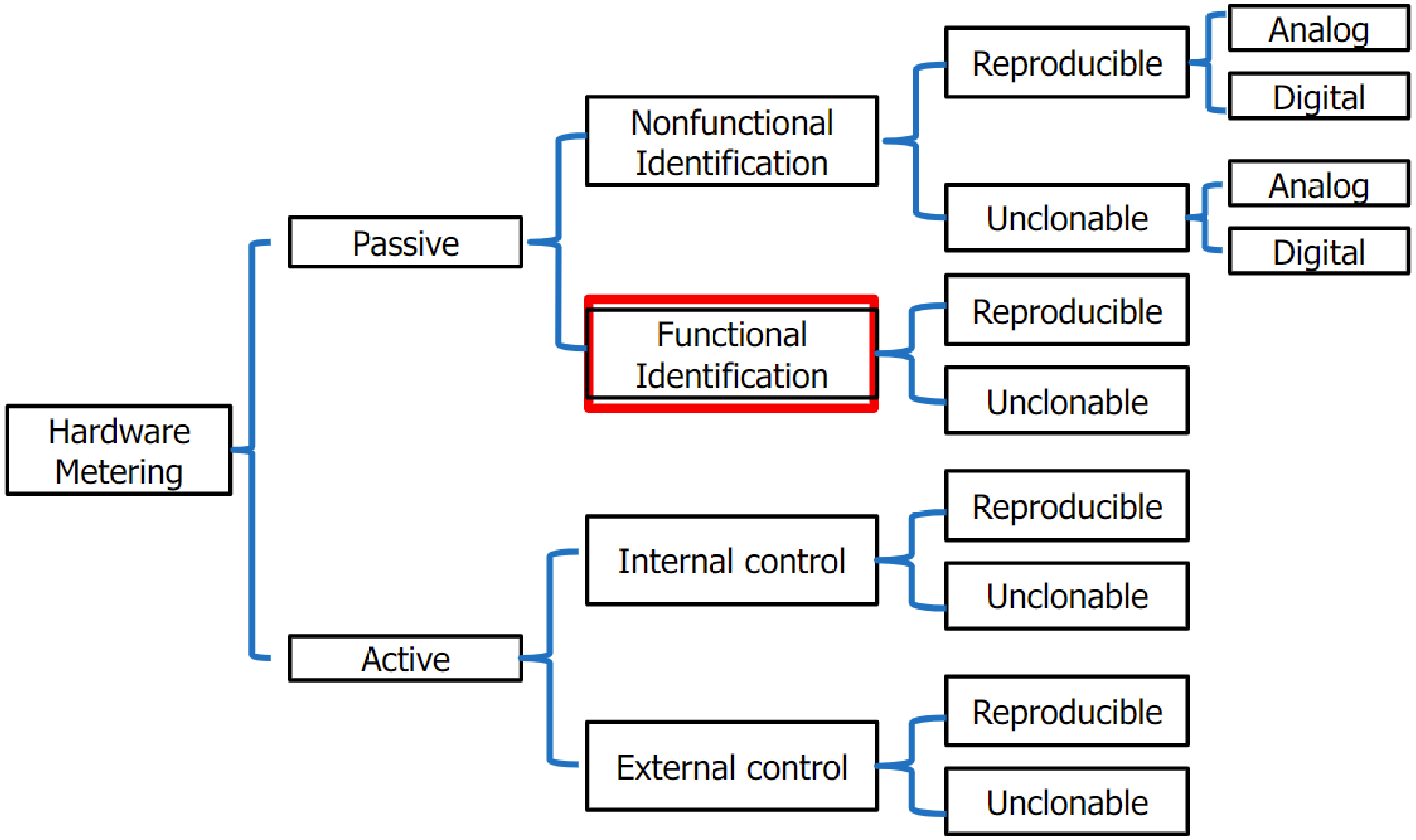
Unclonable Identifiers

- Uses random process variations in silicon to generate random unique numbers called fingerprints.
- If additional logic is needed to generate these value, the method is said to be extrinsic.
- If no additional logic is needed, the method is called intrinsic.
- Advantages:
  - Values cannot be reproduced due to randomness in process variations
- Disadvantages:
  - Foundry could overproduce ICs without knowledge of IP owner
    - i.e., these methods do not prevent counterfeiting. The over-produced chip can be detected if IP owner gets his/her hands on those chips by comparing the identifier on the chip with his/her database

Unclonable Identifiers

- **Extrinsic methods:**
  - Require additional logic such as PUF (Physical Unclonable Function) or ICID
  - ICID
    - Threshold mismatches in array of transistors incurred different currents and therefore unique random numbers.
  - PUFs
    - Series of ring oscillators (ROs) generate random value due to process variations.
- **Intrinsic methods:**
  - Unique identification if external test vectors can be applied.
  - Uses IC **leakage**, **power**, **timing**, and **path signatures** (unique due to process variations).
  - Does not need additional logic and can be readily used on existing designs

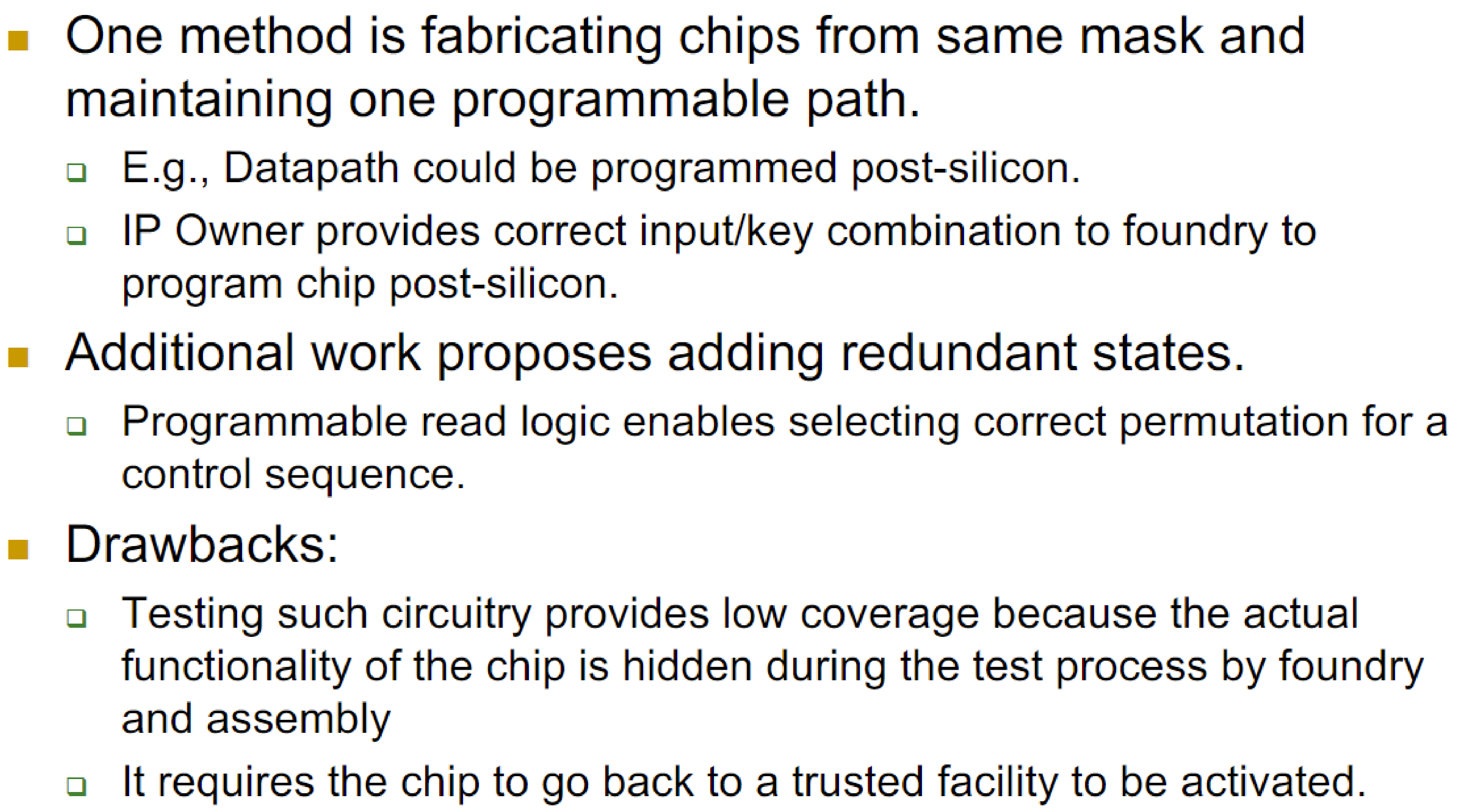
Metering Methods



Functional Metering

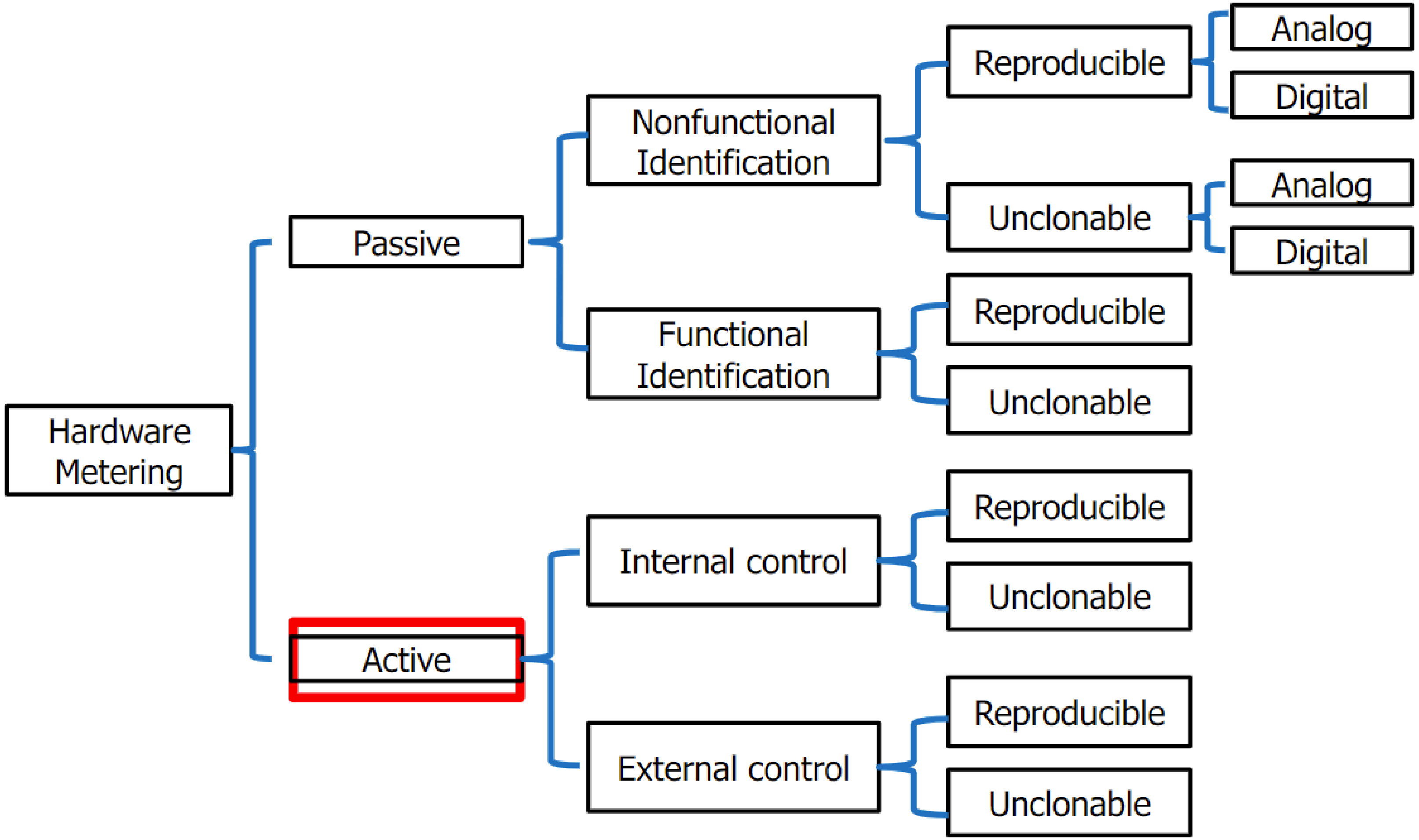
- Identifiers linked to chip’s internal functional details during synthesis.
- Each chip’s function gets a unique signature.
  - E.g., additional states added to generate same output
- Function unchanged from input to output
- Internal transactions unique to each chip
- Challenge in fabricating ICs with different paths from same mask.

Functional Metering



- One method is fabricating chips from same mask and maintaining one programmable path.
  - E.g., Datapath could be programmed post-silicon.
  - IP Owner provides correct input/key combination to foundry to program chip post-silicon.
- Additional work proposes adding redundant states.
  - Programmable read logic enables selecting correct permutation for a control sequence.
- Drawbacks:
  - Testing such circuitry provides low coverage because the actual functionality of the chip is hidden during the test process by foundry and assembly
  - It requires the chip to go back to a trusted facility to be activated.

Metering Methods



Hardware Metering

Passive

Nonfunctional Identification

Reproducible

Analog

Digital

Unclonable

Analog

Digital

Functional Identification

Reproducible

Unclonable

Active

Internal control

Reproducible

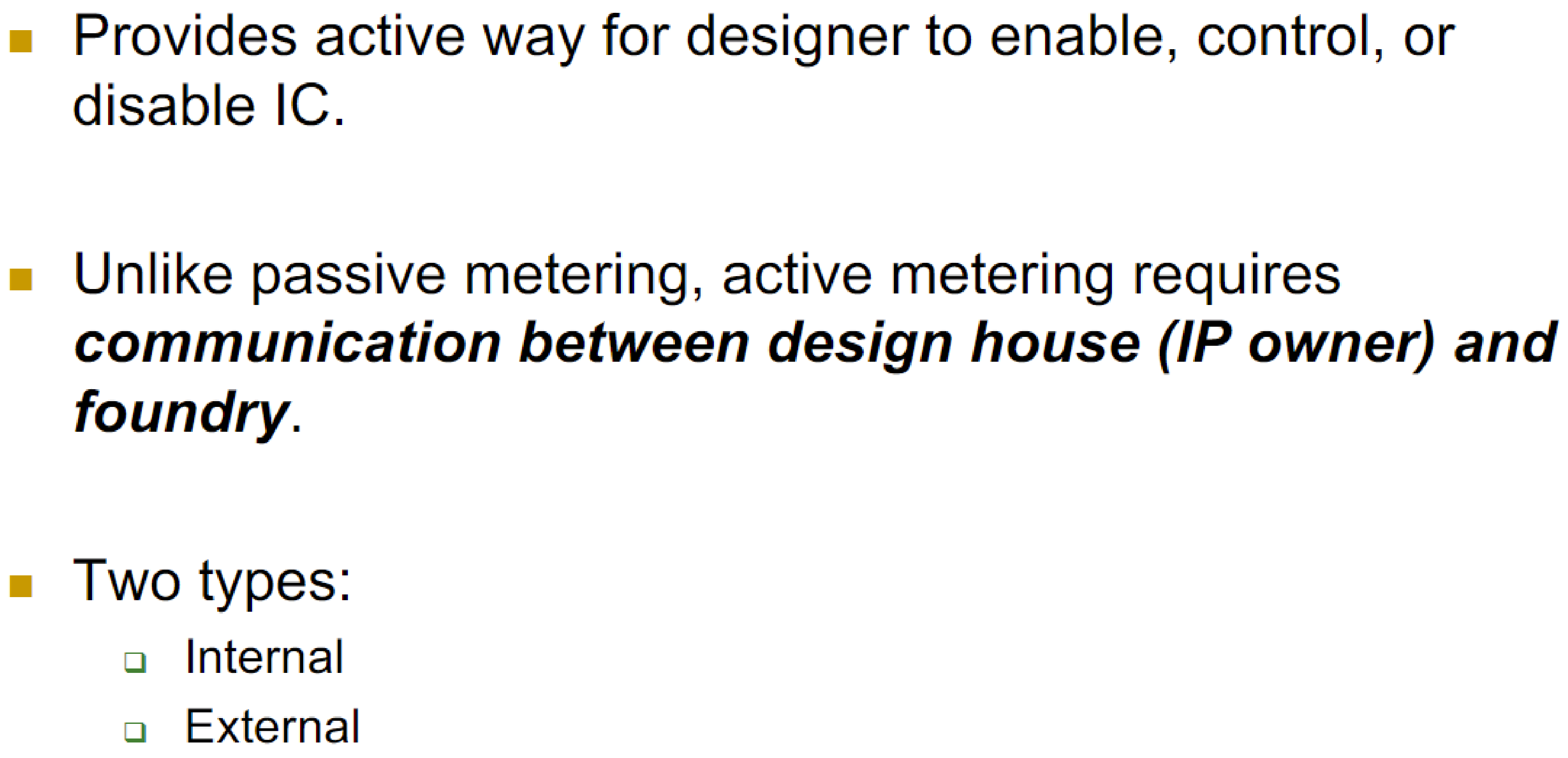
Unclonable

External control

Reproducible

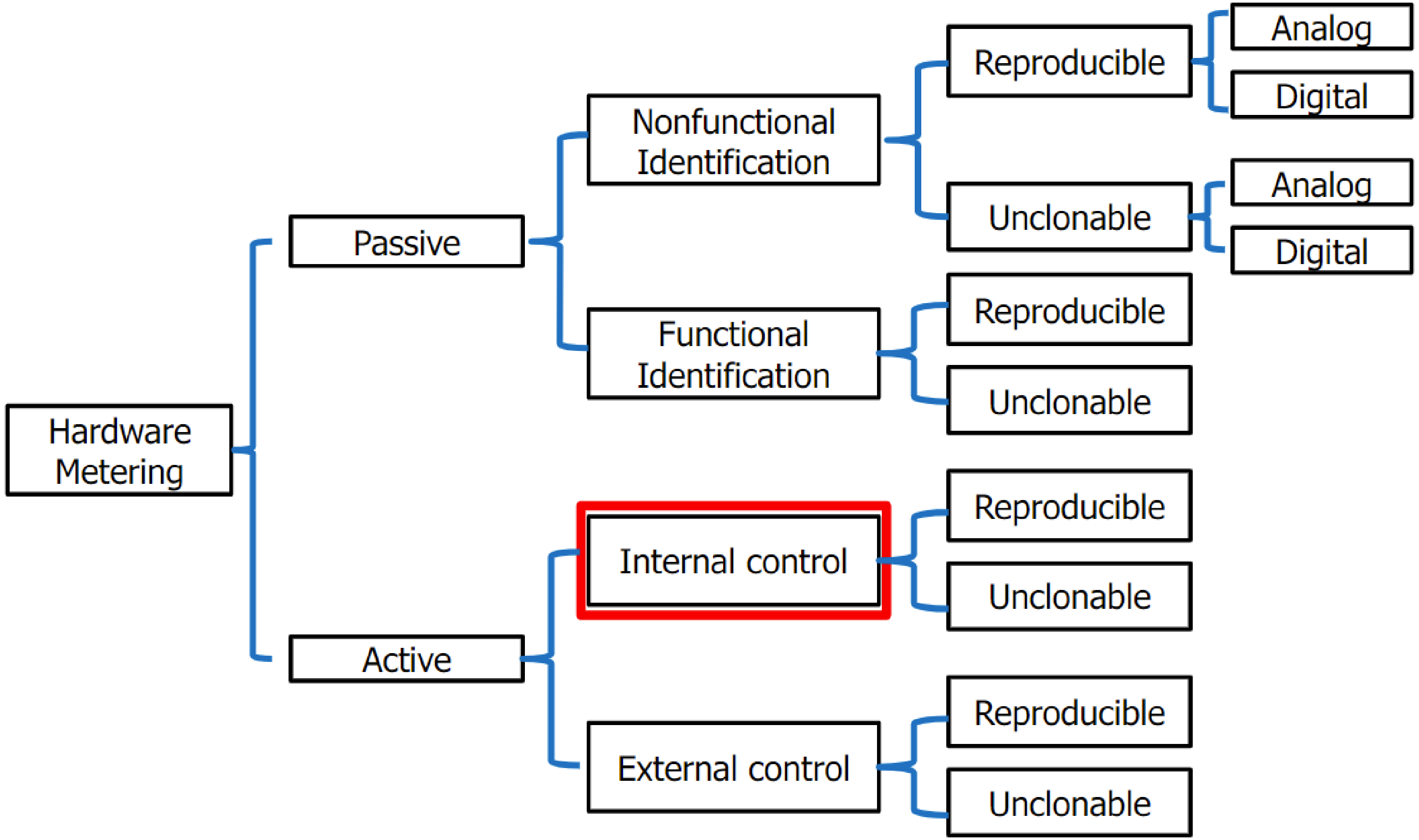
Unclonable

Active Metering

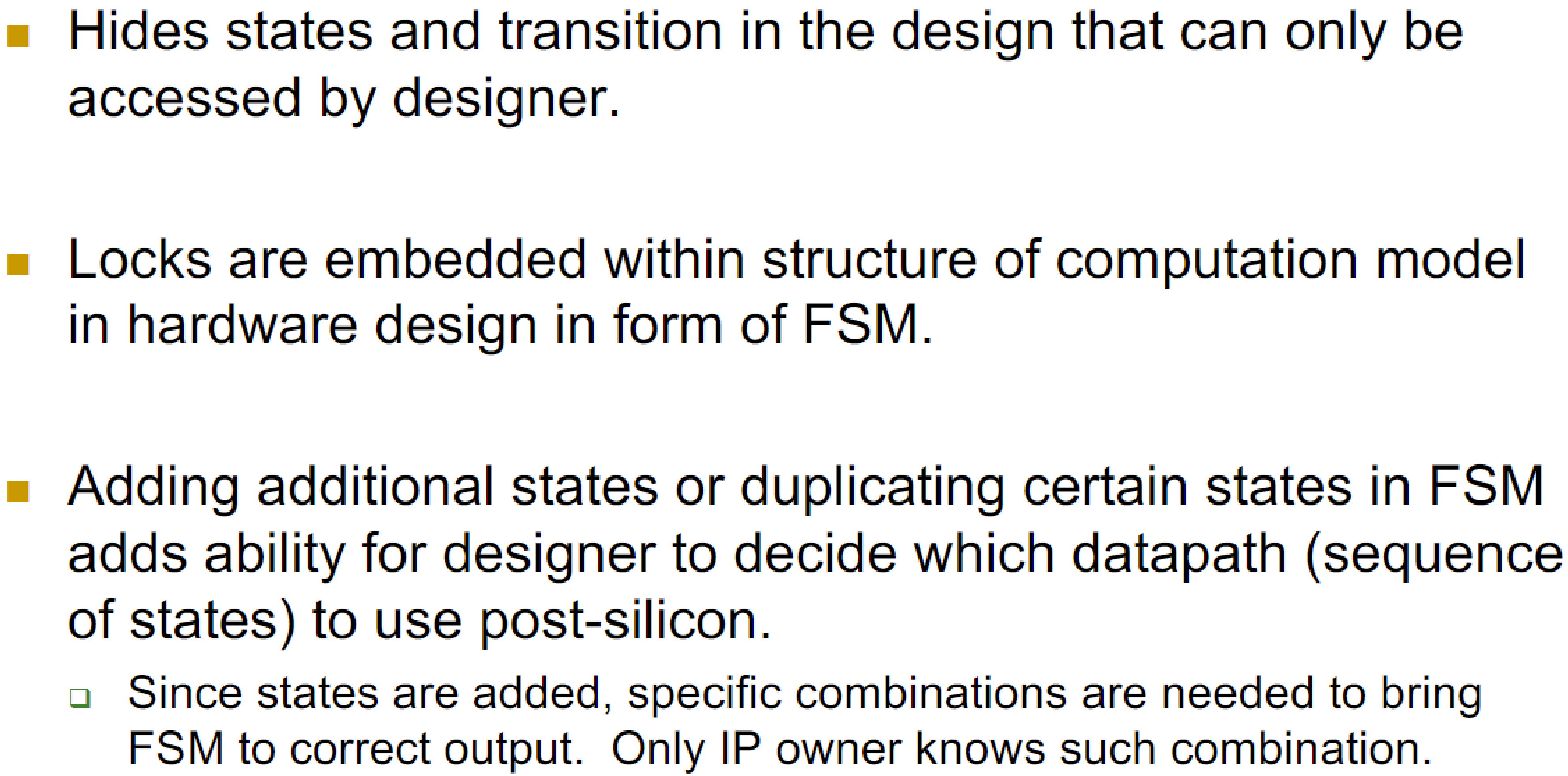


- Provides active way for designer to enable, control, or disable IC.
- Unlike passive metering, active metering requires ***communication between design house (IP owner) and foundry***.
- Two types:
  - ❑ Internal
  - ❑ External

Metering Methods



Internal Active Metering



- Hides states and transition in the design that can only be accessed by designer.
- Locks are embedded within structure of computation model in hardware design in form of FSM.
- Adding additional states or duplicating certain states in FSM adds ability for designer to decide which datapath (sequence of states) to use post-silicon.
  - Since states are added, specific combinations are needed to bring FSM to correct output. Only IP owner knows such combination.

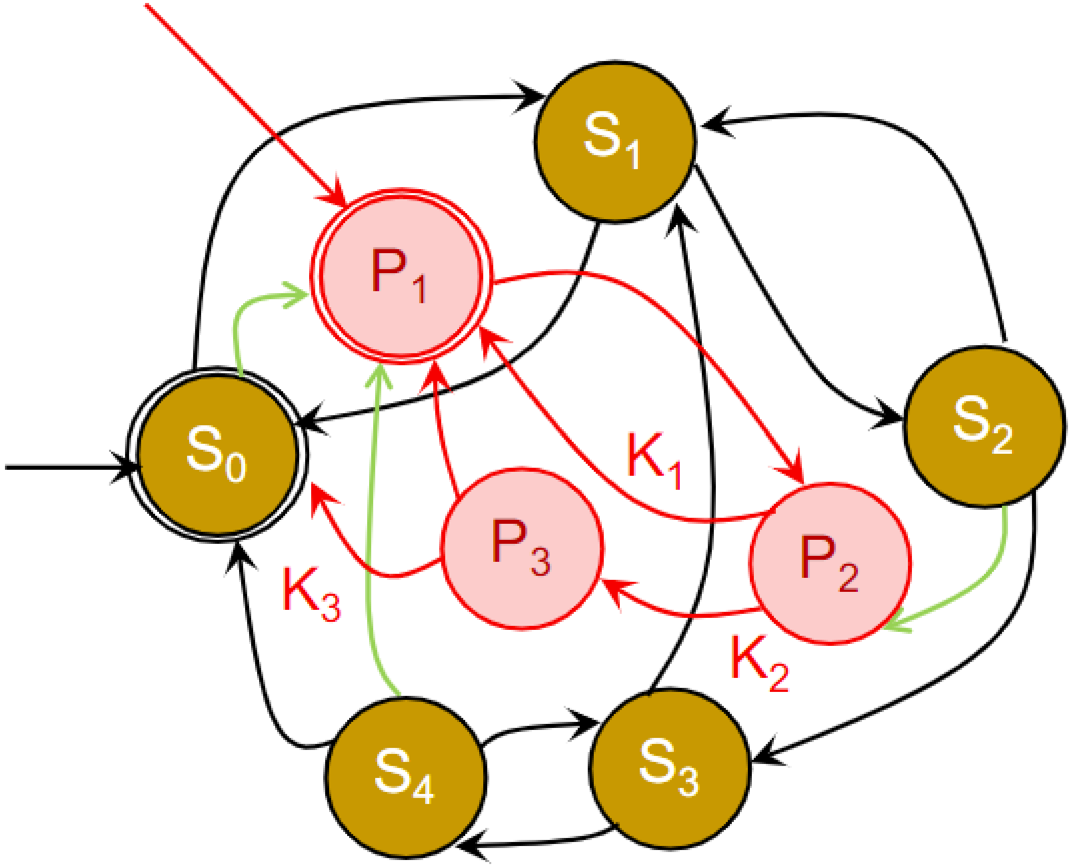
Internal Active Metering

Basic Idea:

- A locking approach where normal behavior is *enabled* only upon appn. of a key
- Provable robustness

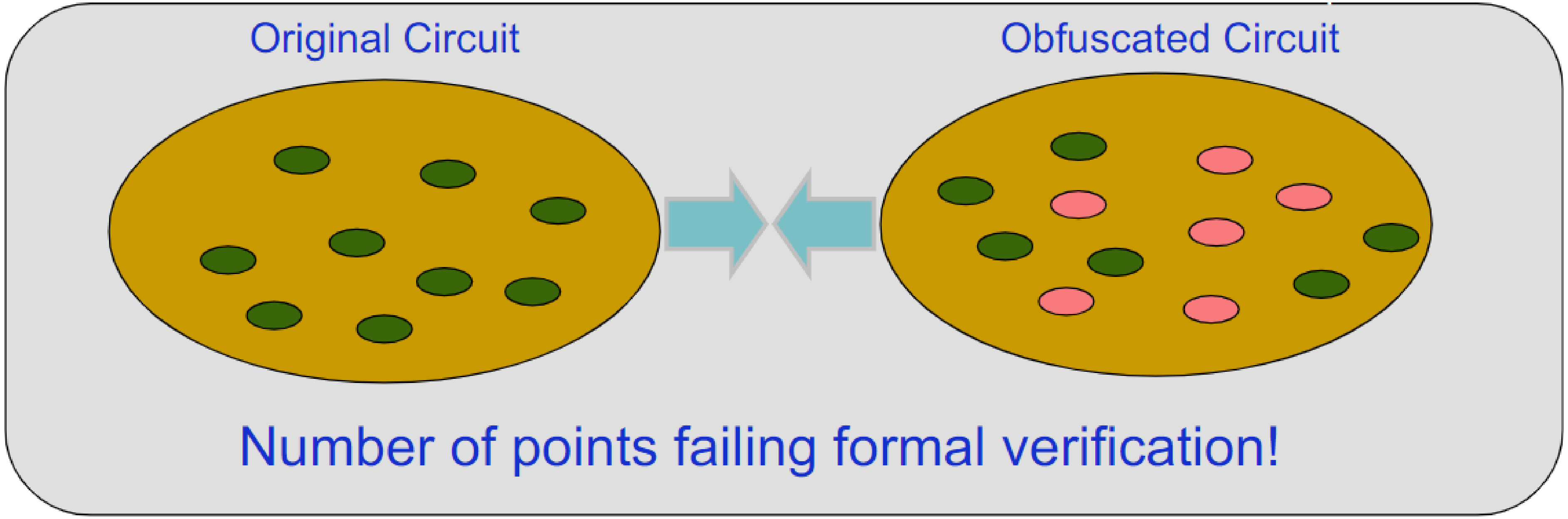
Key Innovations:

- It obfuscates the state space AND the comb. logic
- Uses rich theory of automata to transform the state space & associated logic



Challenges

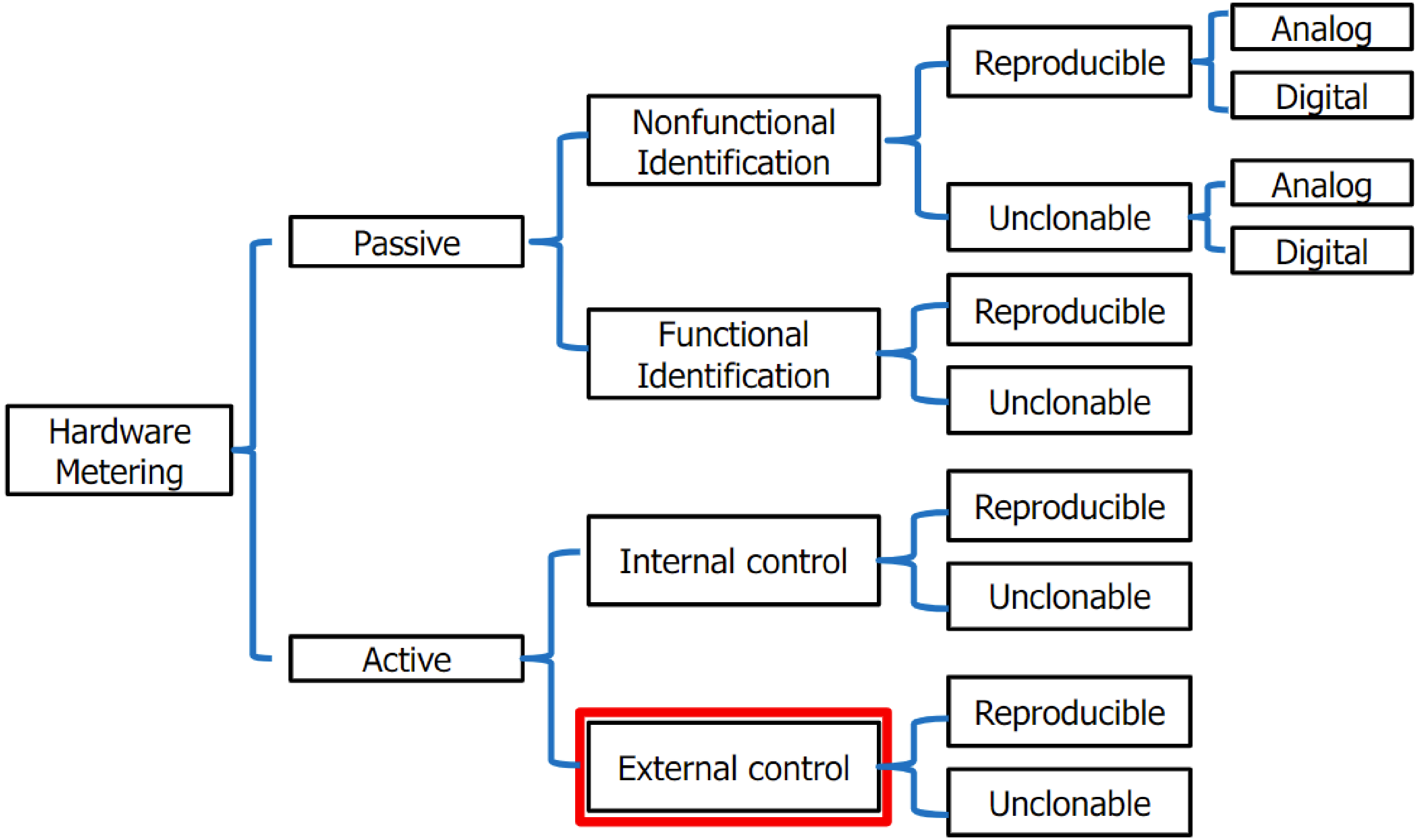
1. How to measure level of obfuscation?
2. How to measure the corresponding security benefit?



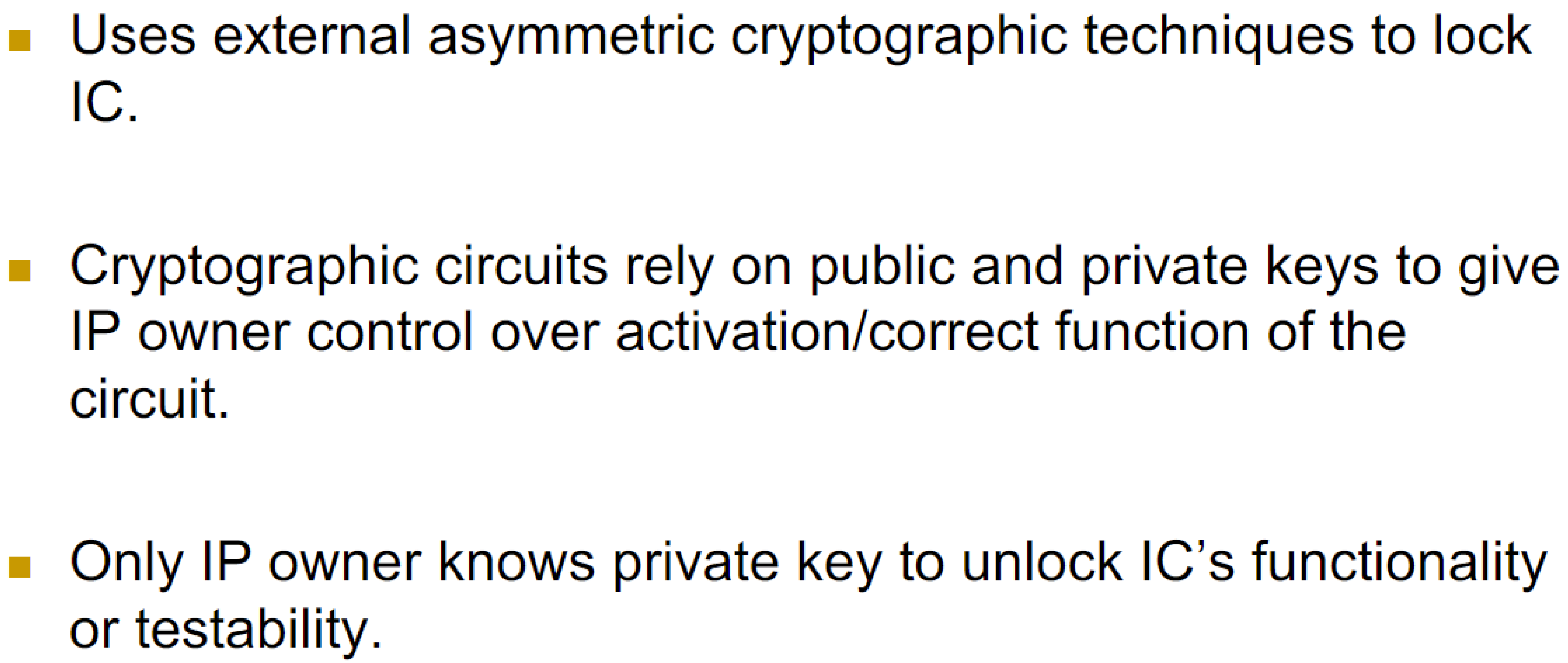
Number of points failing formal verification!

Improvement in *Trojan coverage* (w.r.t. defense against Trojan attacks)!

Metering Methods



External Active Metering



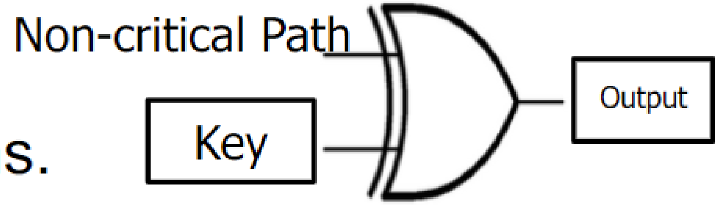
- Uses external asymmetric cryptographic techniques to lock IC.
- Cryptographic circuits rely on public and private keys to give IP owner control over activation/correct function of the circuit.
- Only IP owner knows private key to unlock IC’s functionality or testability.

EPIC: Ending Piracy of Integrated Circuits

- This technique tries to allow IP Owner to have control over number of chips activated.

- Uses public-key encryption to lock correct functionality of chip.

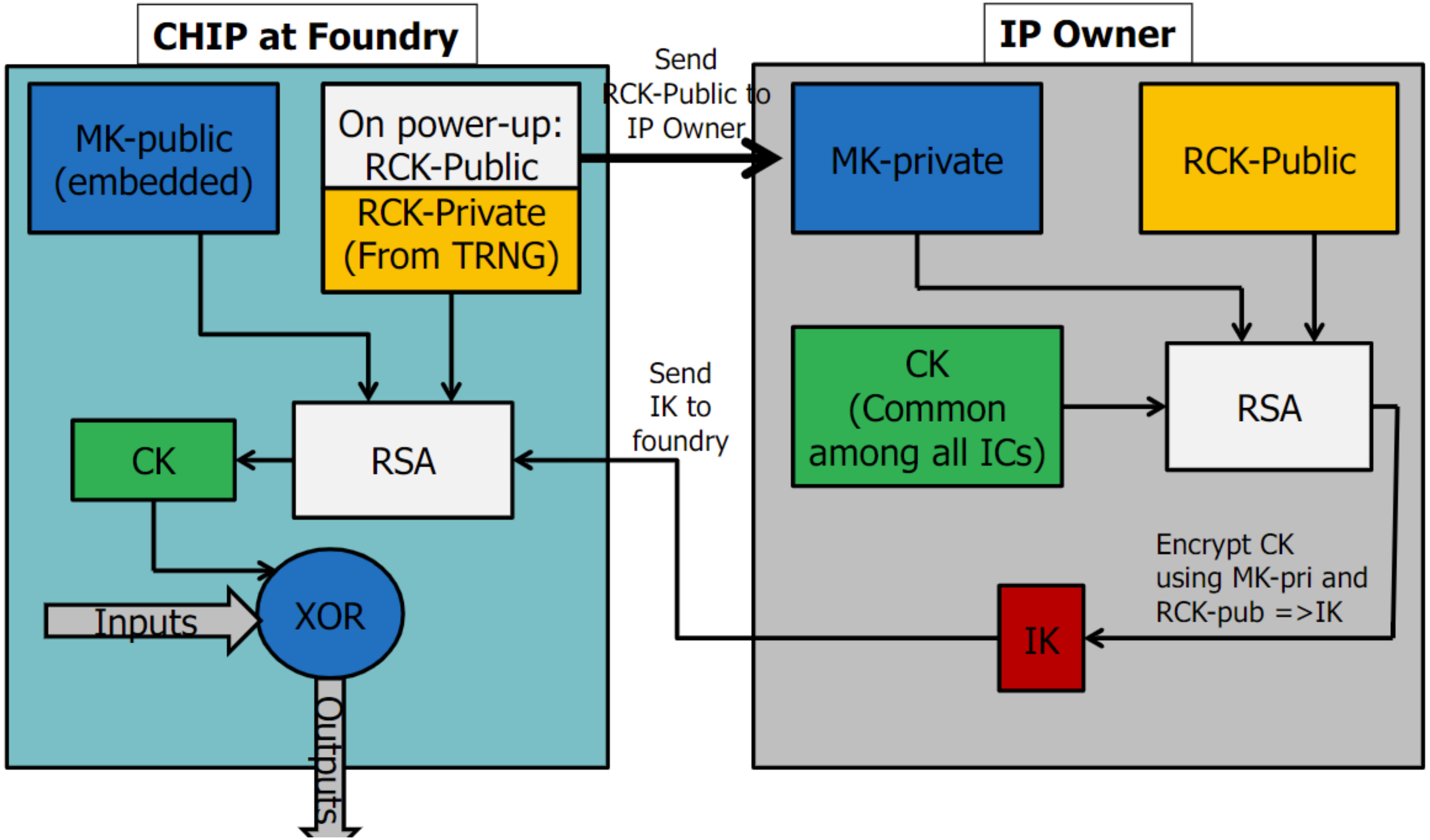
- At the gate level, XOR gates are placed on selected non-critical paths.



- Requires that every chip be activated with an external key
  - ❑ Only IP owner can generate key

Roy et al., DATE 2008

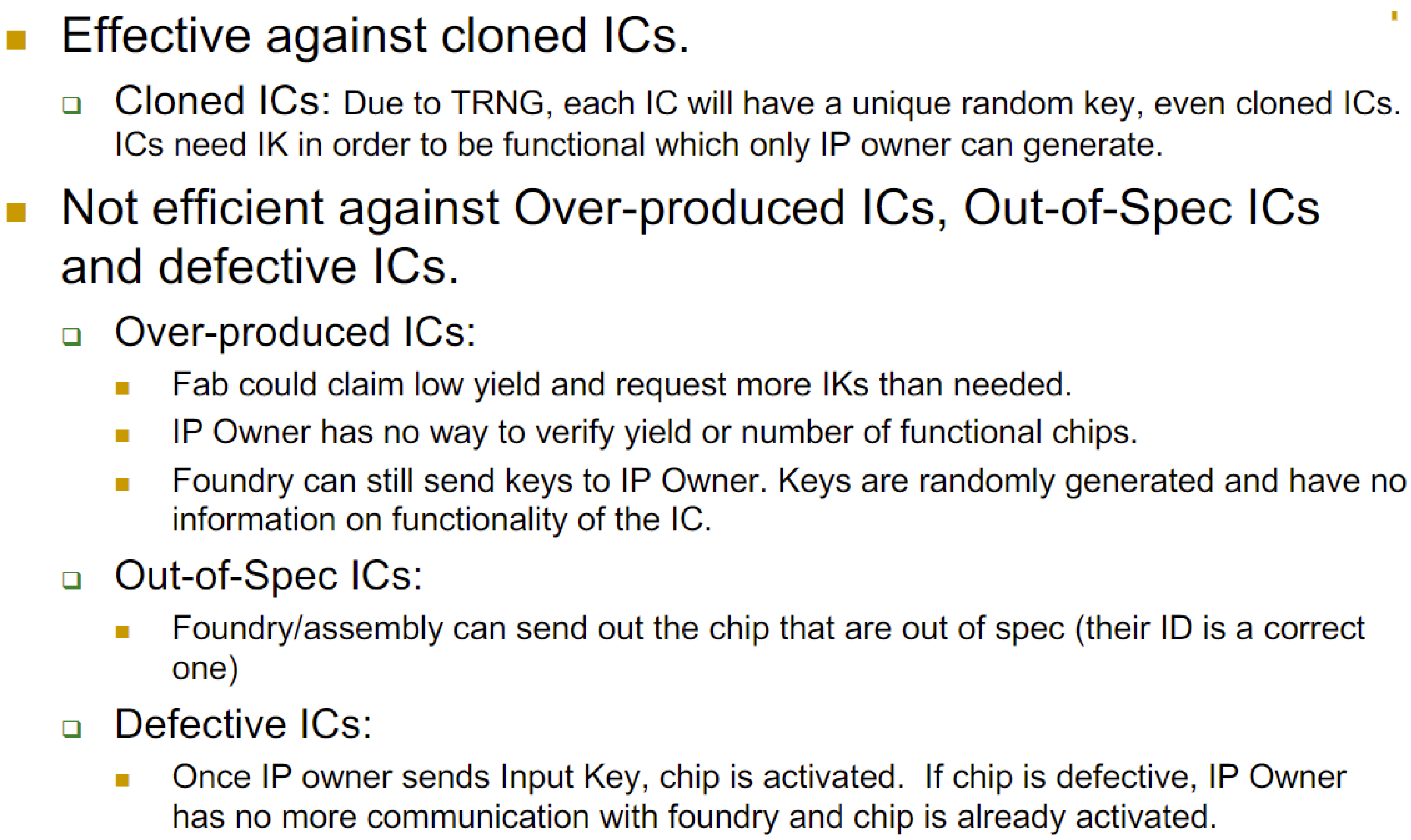
EPIC High Level



EPIC

- Embedded in RTL is public Master Key (MK-Pub)
- XOR gates are controlled by Common Key. Correct Common Key unlocks circuit's correct functionality.
  - k-XOR gates need a common key of length k
- TRNG (True Random Number Generator) used to generate Random Chip Keys (RCK) on start up.
  - Upon power-up each chip generates a pair of private and public RCKs (RCK-private, RCK-public) which are **burned into programmable fuses.**
- Fab sends RCK-public to IP owner.

EPIC



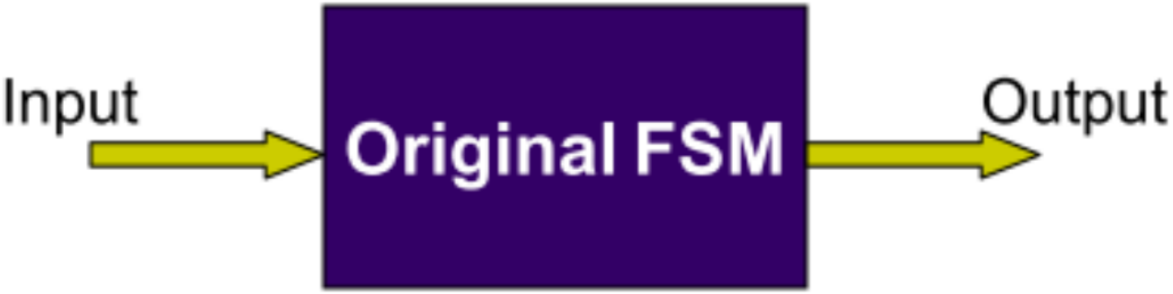
- Effective against cloned ICs.
  - ❑ Cloned ICs: Due to TRNG, each IC will have a unique random key, even cloned ICs. ICs need IK in order to be functional which only IP owner can generate.
- Not efficient against Over-produced ICs, Out-of-Spec ICs and defective ICs.
  - ❑ Over-produced ICs:
    - Fab could claim low yield and request more IKs than needed.
    - IP Owner has no way to verify yield or number of functional chips.
    - Foundry can still send keys to IP Owner. Keys are randomly generated and have no information on functionality of the IC.
  - ❑ Out-of-Spec ICs:
    - Foundry/assembly can send out the chip that are out of spec (their ID is a correct one)
  - ❑ Defective ICs:
    - Once IP owner sends Input Key, chip is activated. If chip is defective, IP Owner has no more communication with foundry and chip is already activated.

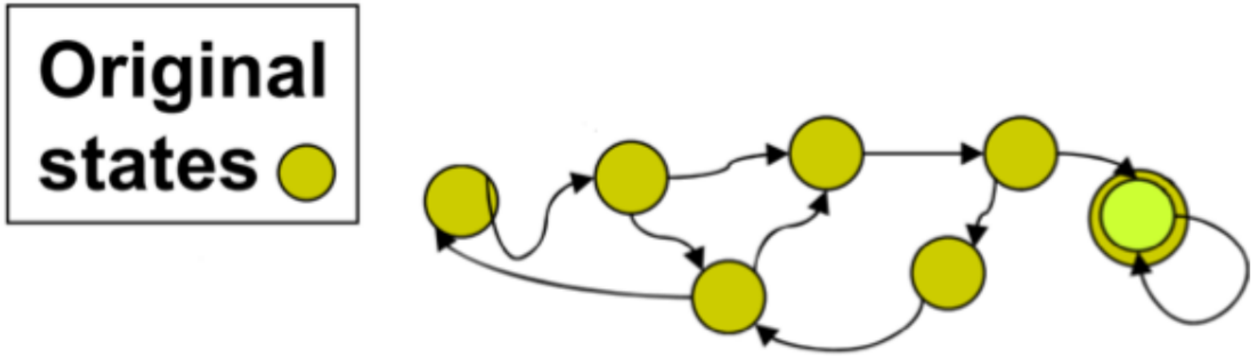
Activation of ICs Through FSM Modification

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

Input
Original FSM
Output

FSM

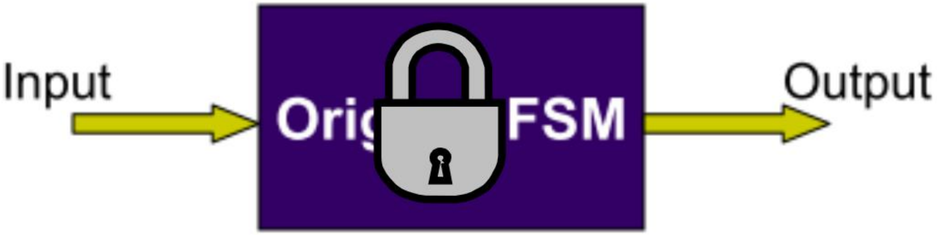


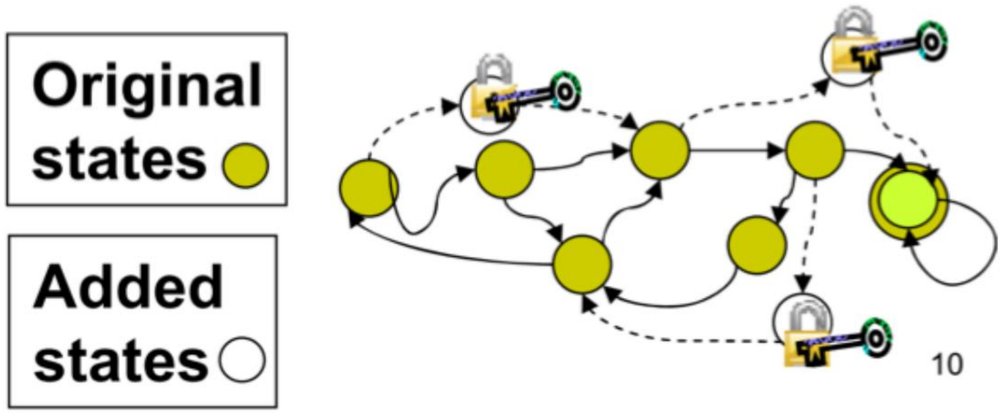


- Correct transitions give functional output

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

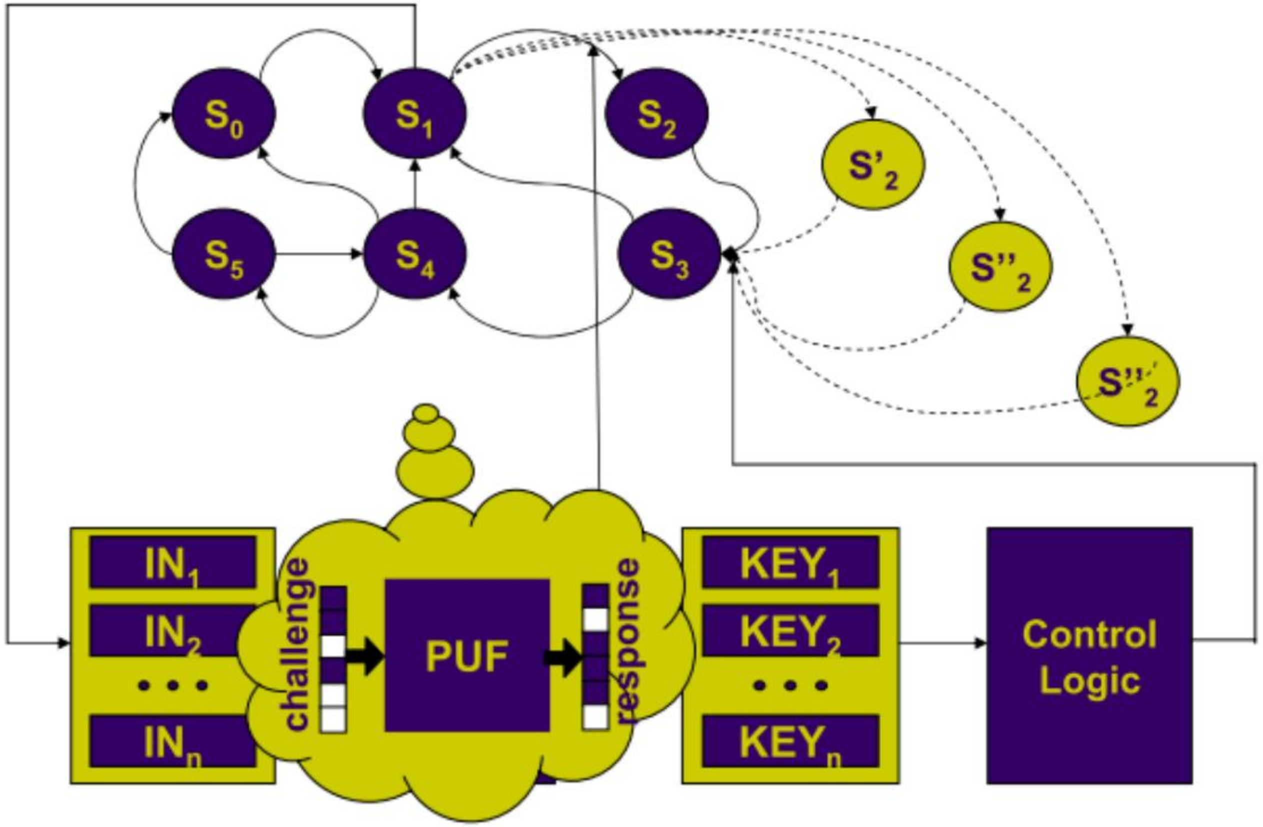
Boosted FSM





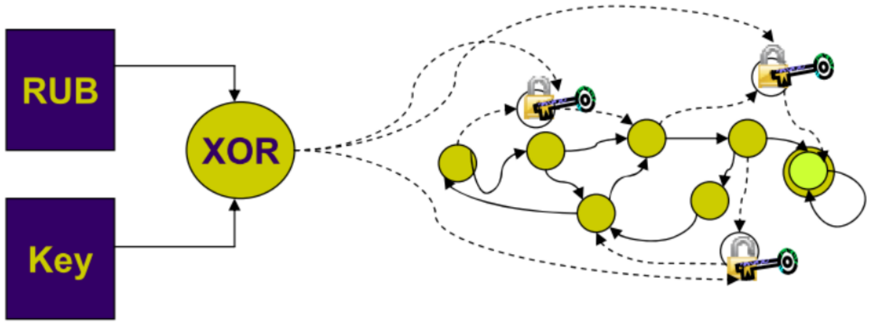
- On startup, inputs cause chip to go to one of added states
- IP Owner is only one with knowledge of FSM
- Only IP Owner knows right sequence (key) to bring FSM back to functional states.

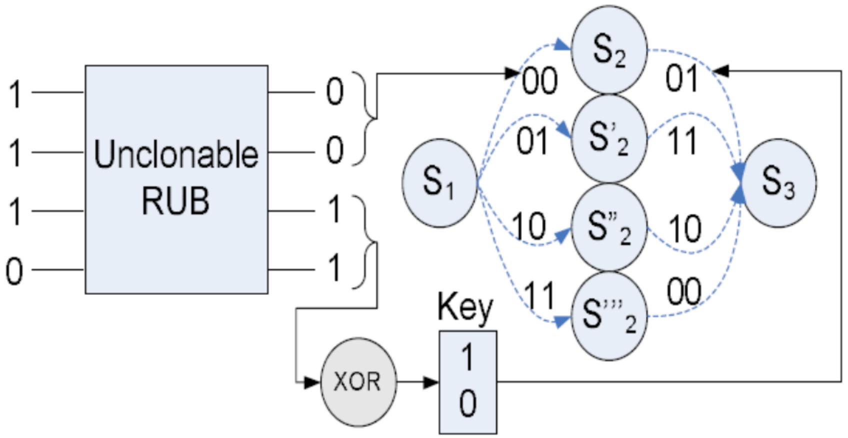
Activation of ICs



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

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

- 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.