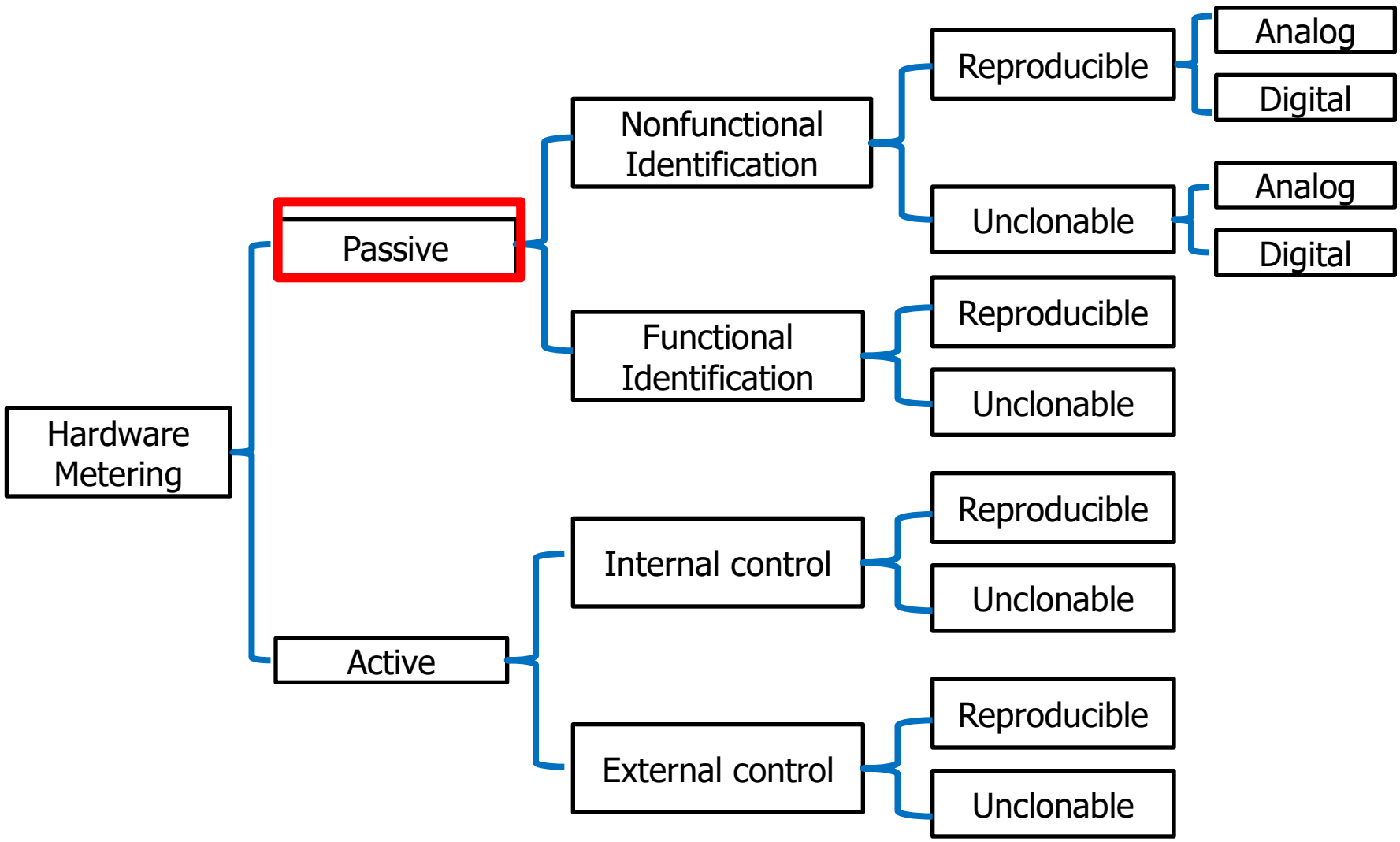
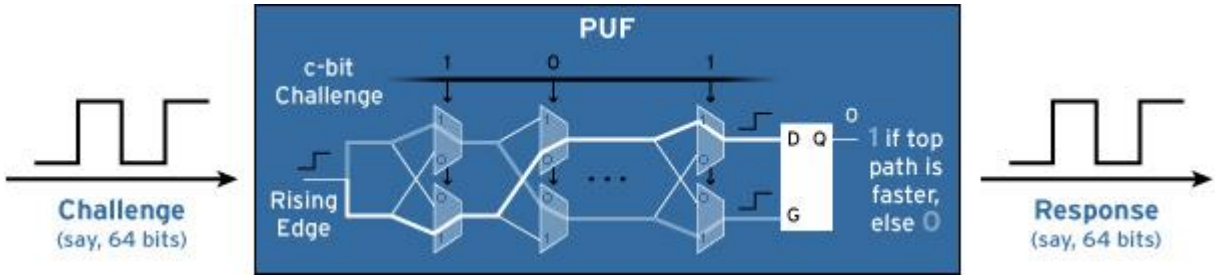
Hardware Metering

- **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**

Taxonomy of Metering Methods

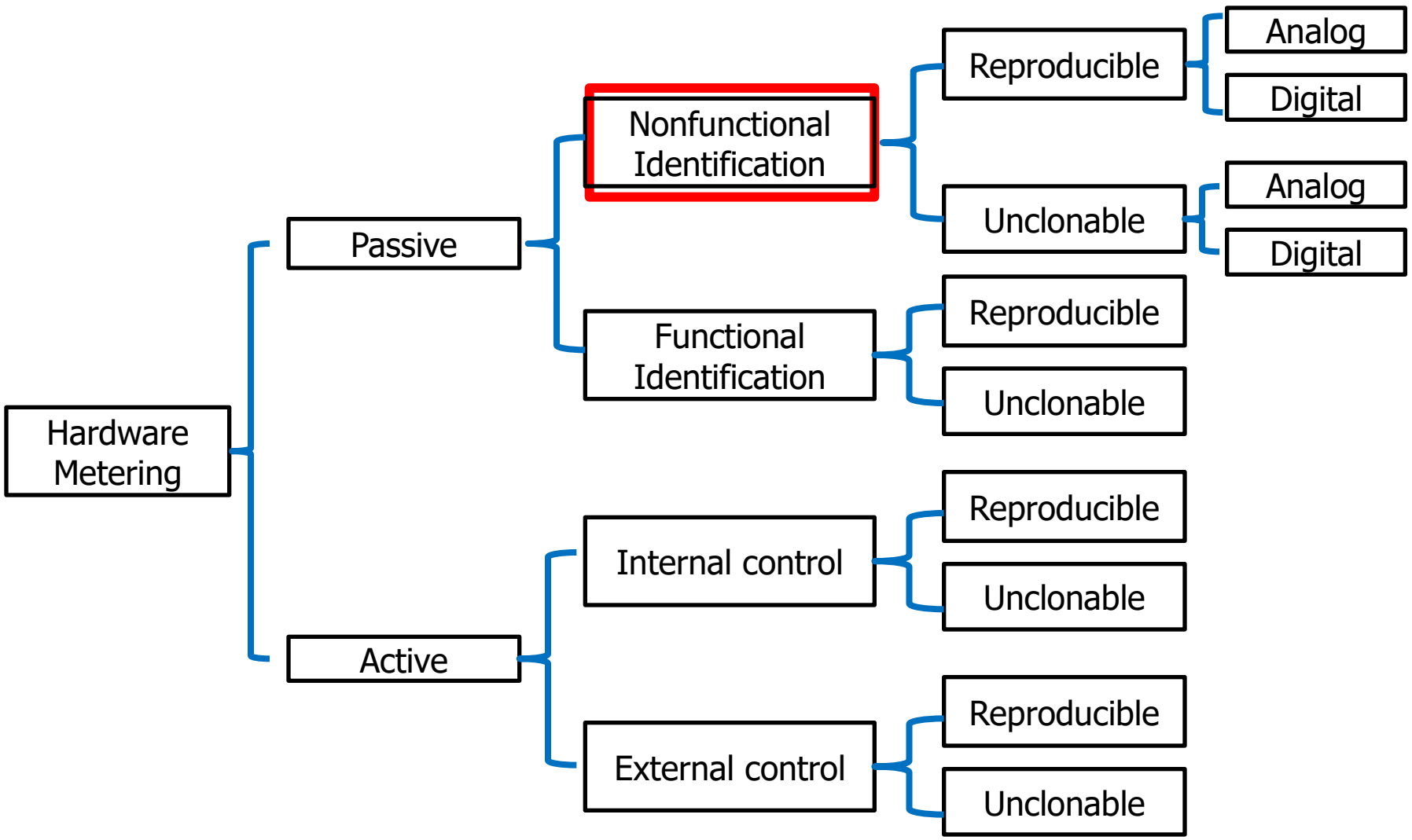


Passive Metering



- 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

Taxonomy of Metering Methods

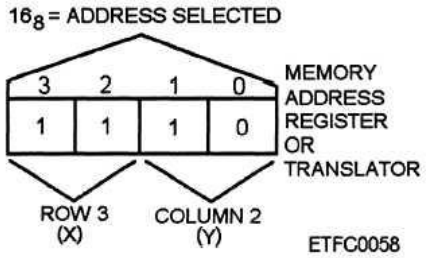


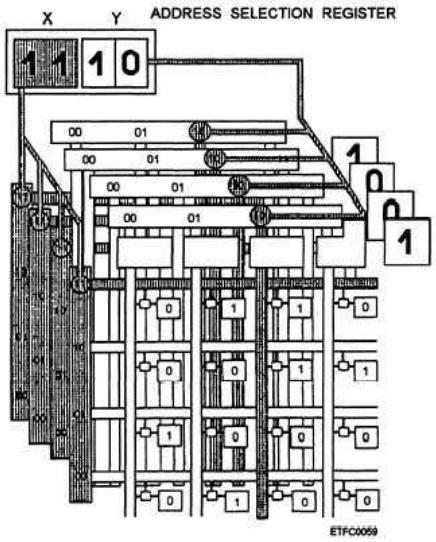
Nonfunctional Identification

- 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

Nonfunctional Identification: 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





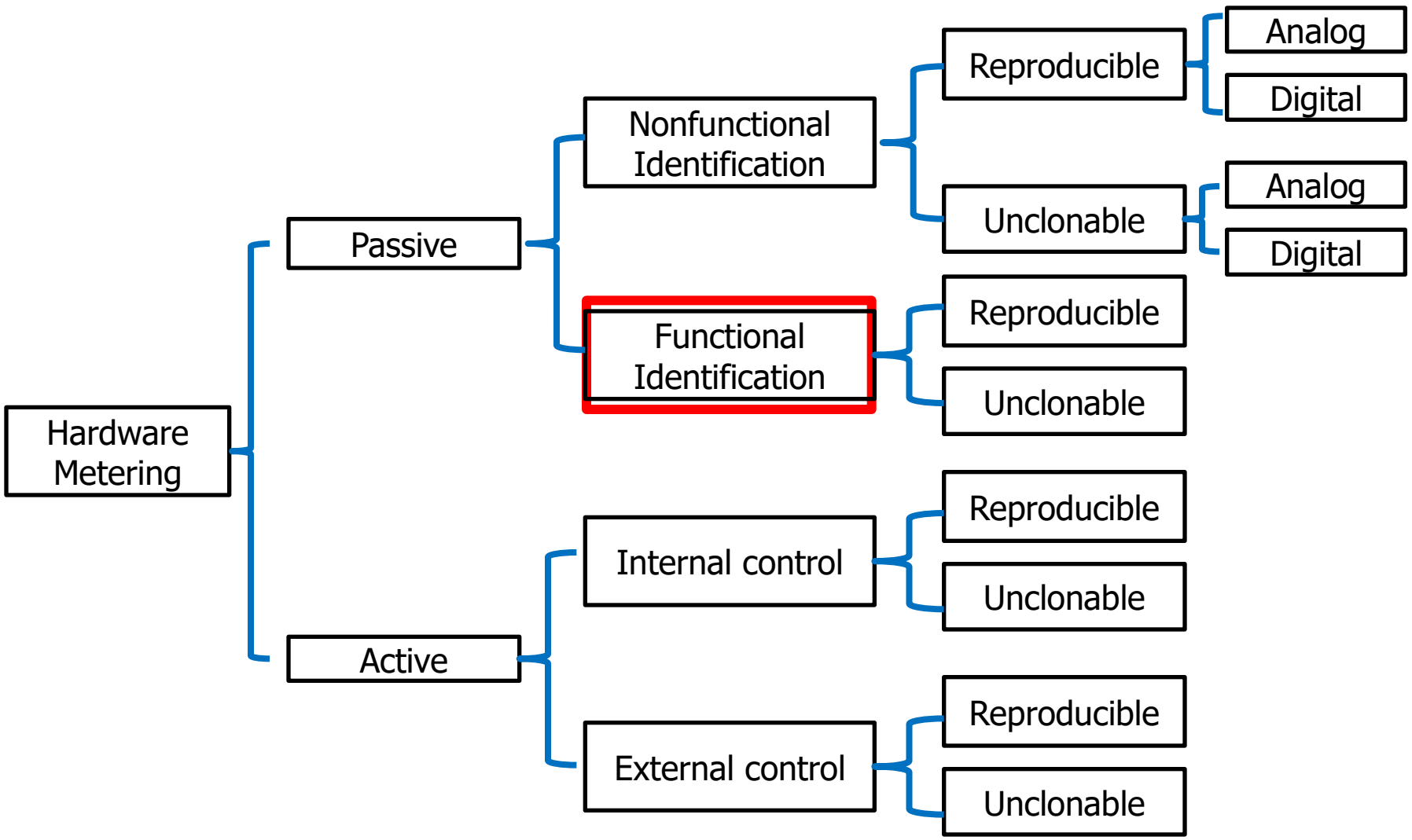
Nonfunctional Identification: Unclonable Identifiers

- 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: IC identification
    - 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

Taxonomy of Metering Methods



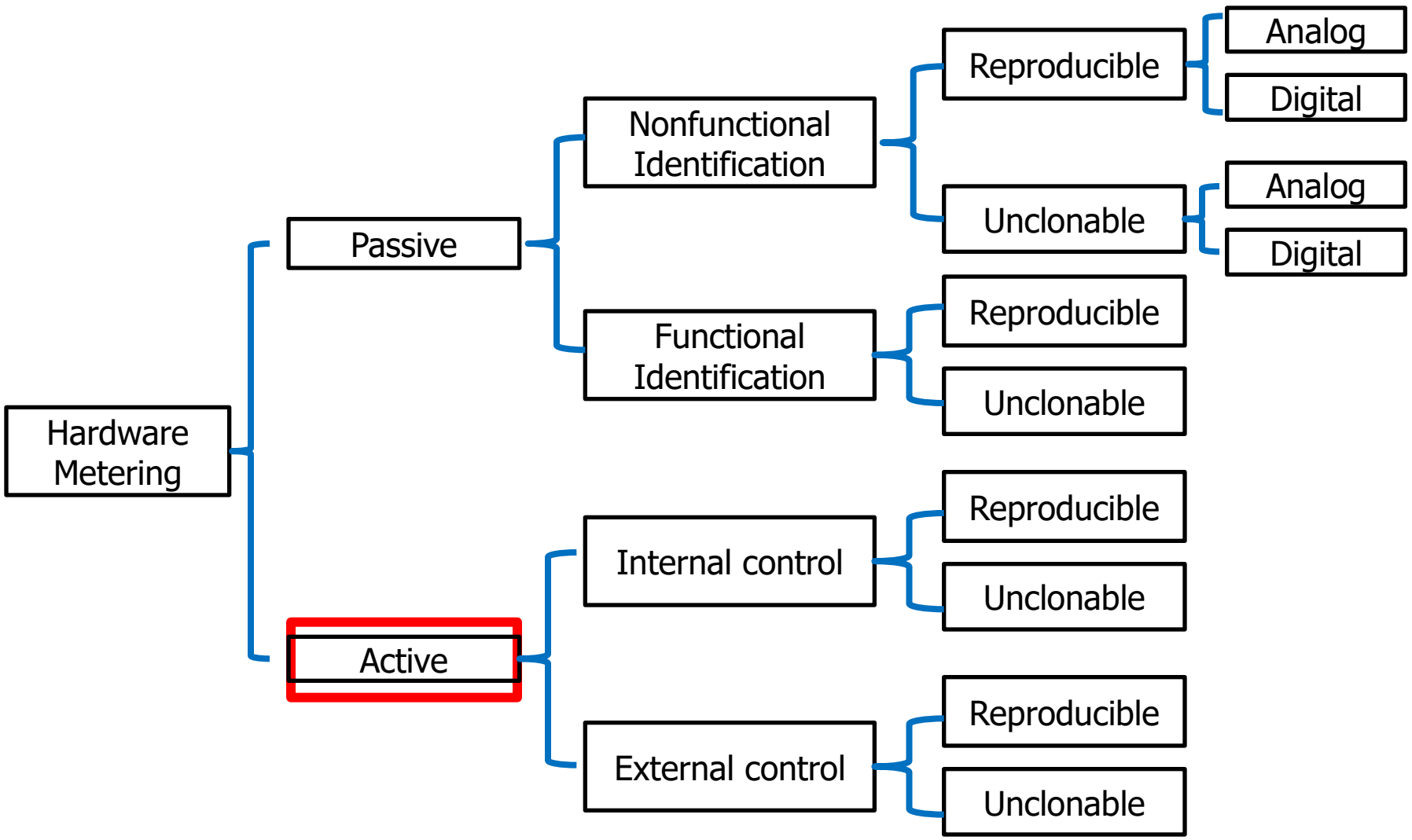
Functional Metering

- 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.

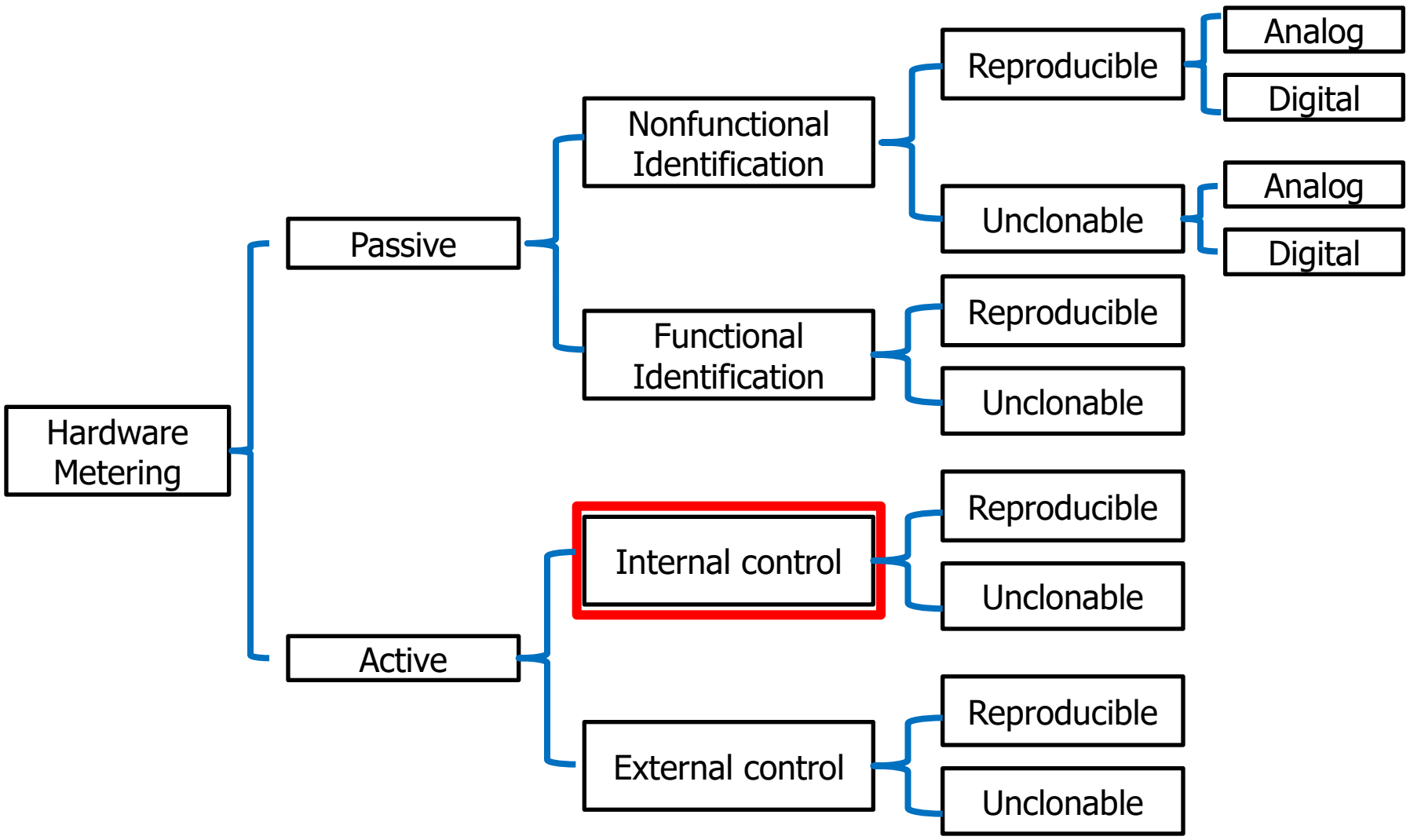
Taxonomy of Metering Methods



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***.
- In active metering, ICs are not fully functional after fabrication. A key or sequence of that only the IP owner can generate is needed to activate the ICs.
- Two types:
  - ❑ Internal active metering does not require external logic blocks. Internal metering methods usually use states within the system.
  - ❑ External active metering requires external logic such as cryptographic logic and PUFs.

Taxonomy of Metering Methods



Internal (Integrated) 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.

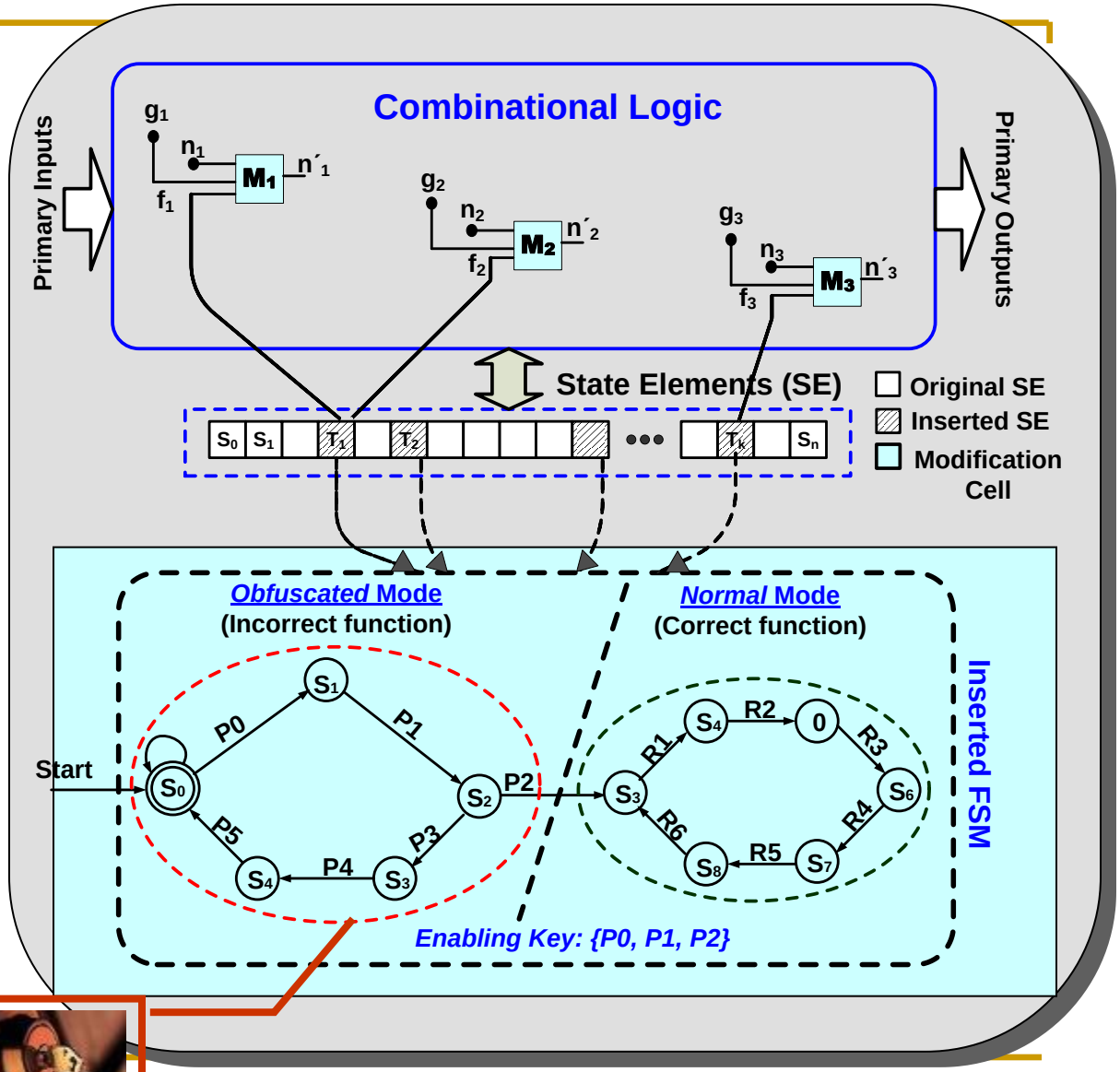
State Space Obfuscation

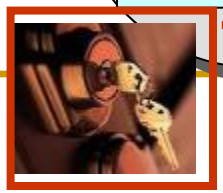
Basic Idea:

- 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





Protects against Piracy, RE & Tampering

The Flow

Input: Netlist **Const.** **Key**

Analyze input netlist to identify suitable nodes {S} for structural mod.

Design modification cells and insert them in {S}

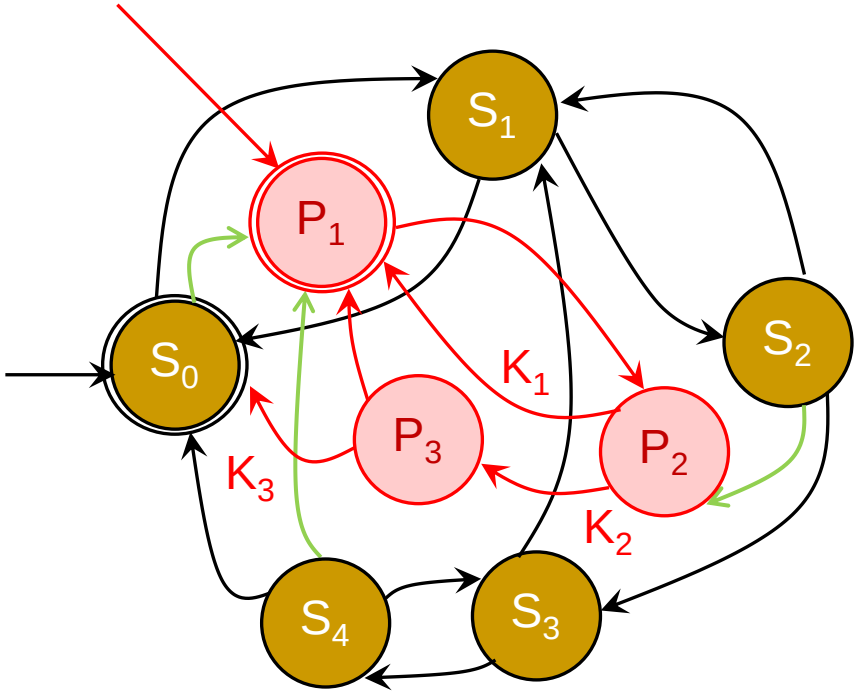
Create a separate FSM (O_{FSM}) using additional state elements (SEs)

Integrate O_{FSM} with original FSM

Perform constrained logic synthesis; Add active monitors in obf. space

Output: Obfuscated Netlist

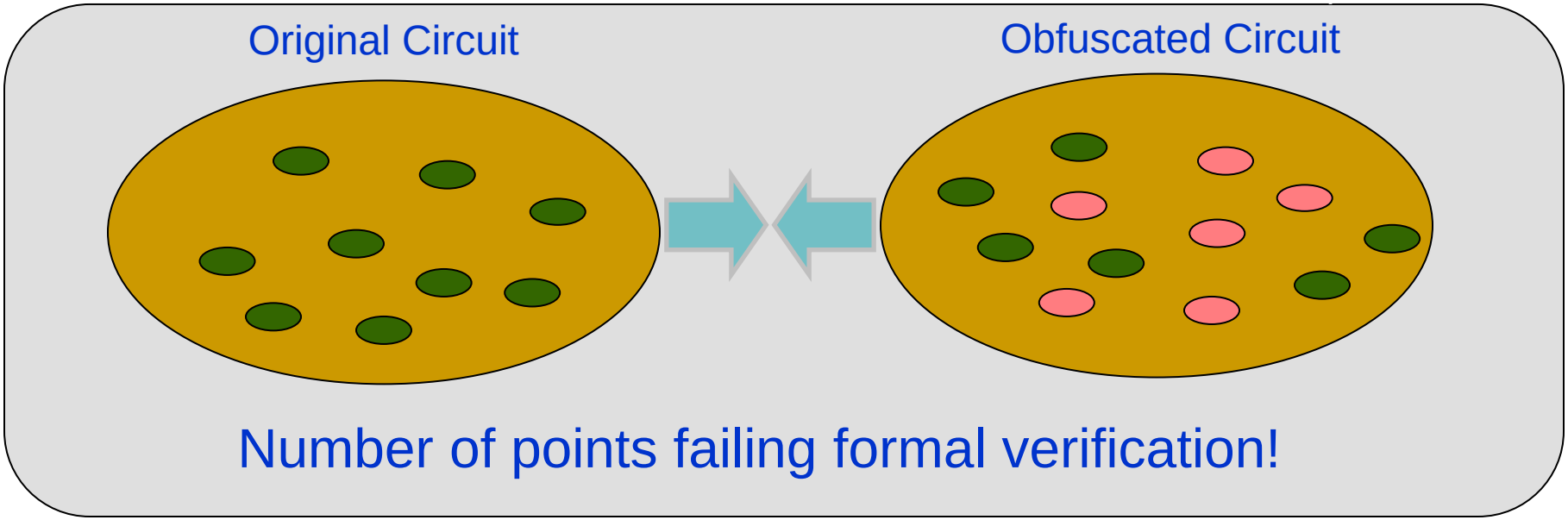
- Transforms underlying state machine



- Affects the dynamic behavior of the machine

Challenges

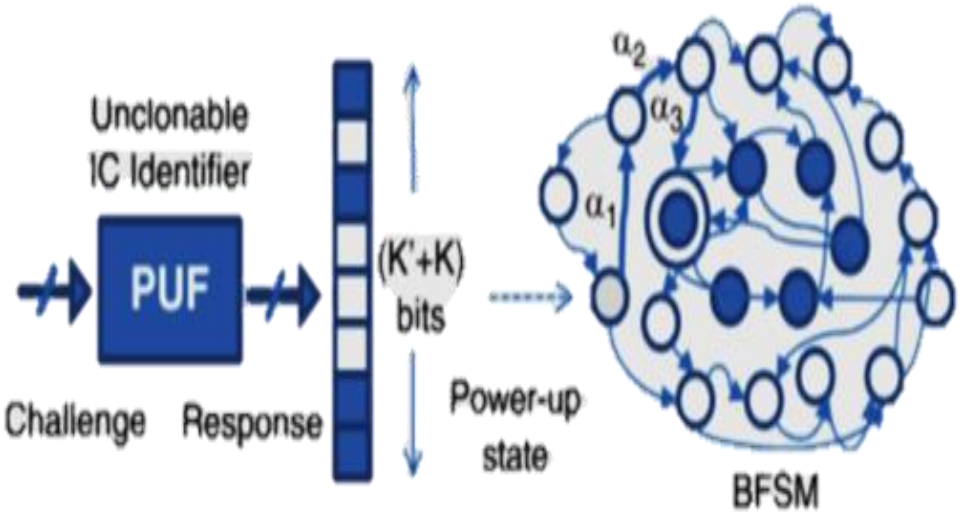
1. How to measure level of obfuscation?
2. How to measure the corresponding security benefit?



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

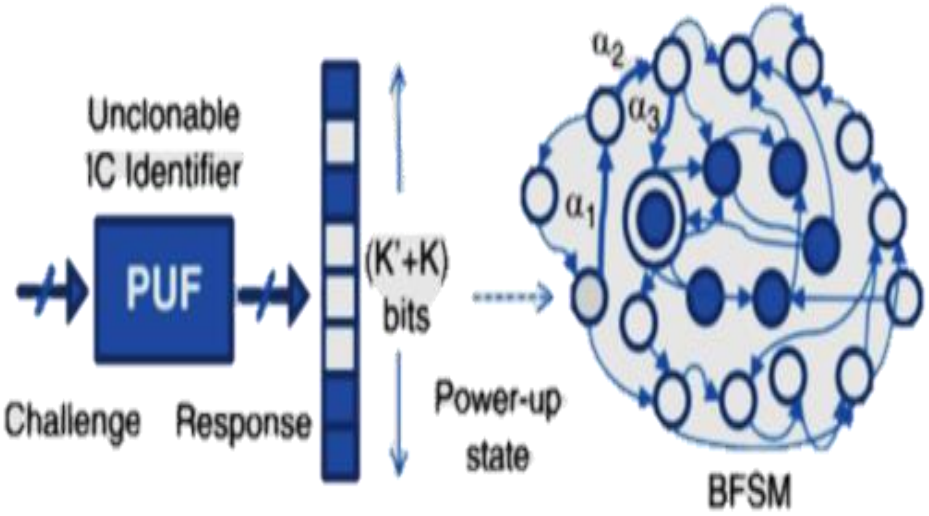
Internal (Integrated) Active Metering

- States and transitions for controlling chips are integrated within functional specifications
- K = $\log_2(S)$ flip flops needed to implement S states
- Adding S1 states requires K1=log(S1+S) flip flops
- Few additional flip flops can exponentially increase the number of states.

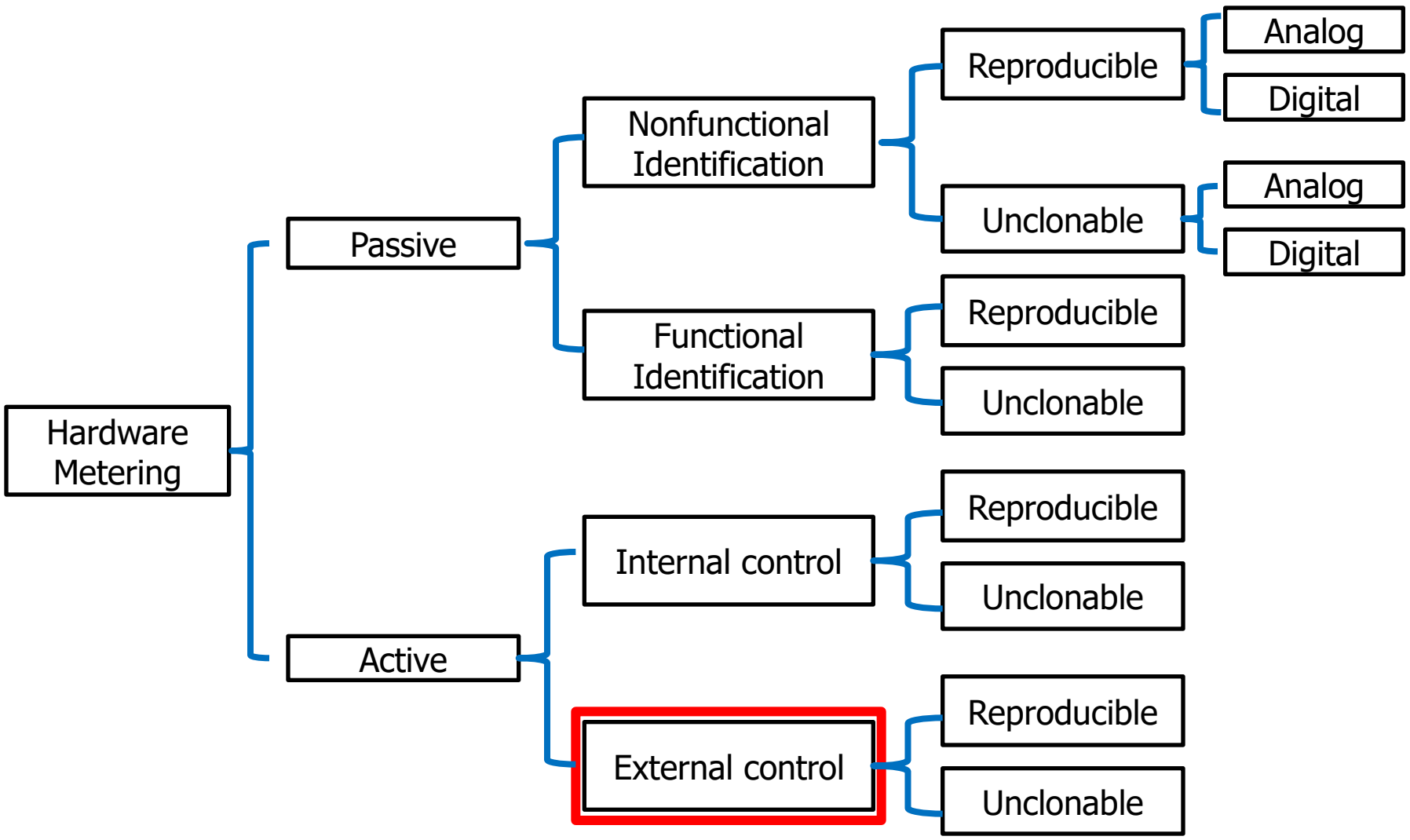


Internal (Integrated) Active Metering

- PUF generates random values, it sends device to random FSM state.
- Only IP owner with knowledge of FSM can find correct sequence to set FSM to reset state.
- Storing a sequence on chip requires additional logic such as clocks and memory and also requires chip to wait until entire sequence has been shifted in.



Taxonomy of Metering Methods

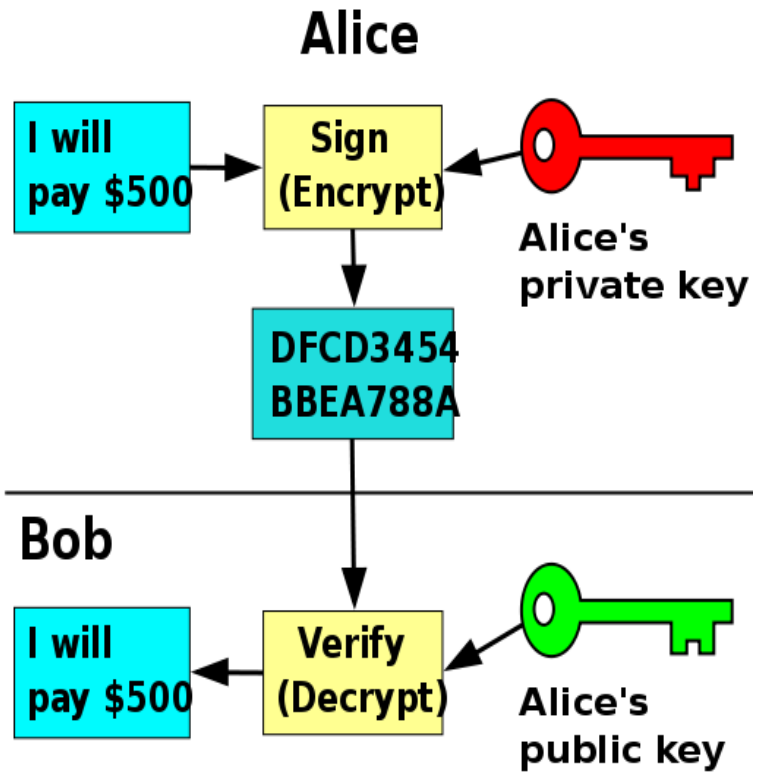


External Active Metering

- 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.
- these blocks usually include random number generators such as PUFs or TRNGs (True random number generators), and cryptographic logic.

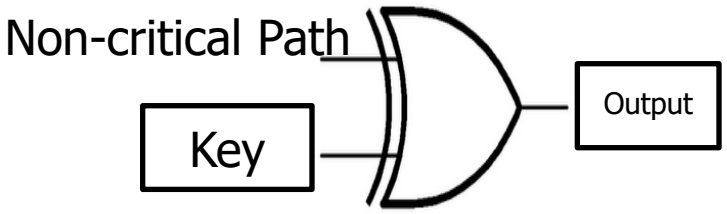
Background: Public Key Cryptography

- Uses two large prime numbers
  p and q to generate co-prime n=pq
- Private (d) and public (e) keys based on n, p, and q are calculated
  - (e,n) are shared, message is encrypted using (d,n)
  - Decryption can be done using (e,n)
- Security relies on magnitude of prime numbers p and q



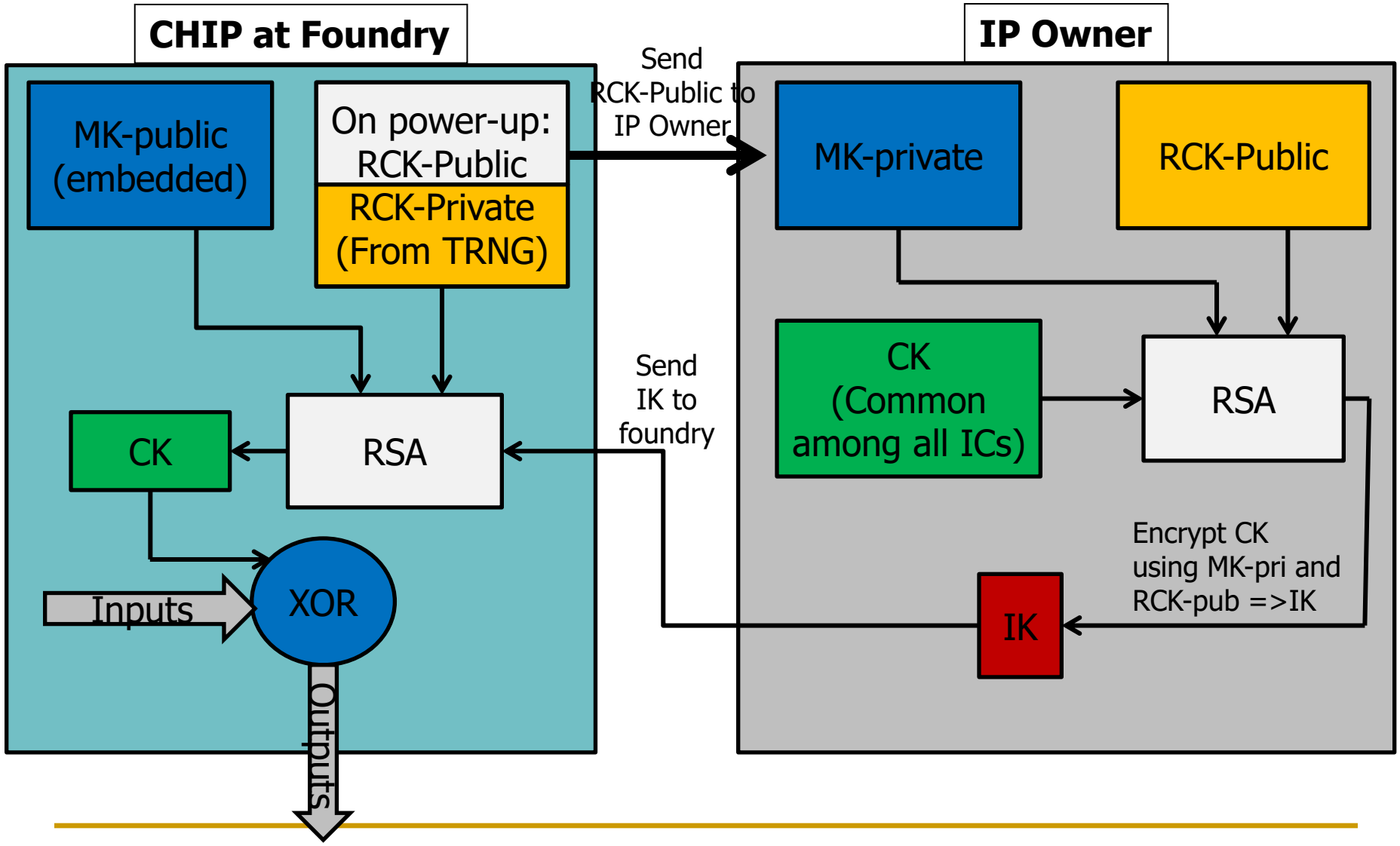
EPIC: Ending Piracy of Integrated Circuits

- 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
  - The correct key is encrypted by IP owner and can only be decrypted by the RSA built into the chip.

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

- A common key (CK) is needed to active the chips. This is the key that connects to the XOR gates and is the same key for all ICs, hence the Common Key.
- In the design stage, the IP owner generates a Master Public Key (MK-public) and a Master Private Key (MK-private). The public key is embedded into the chip so that it is always there and does not have to be transmitted to the chip.
- The chip is also designed with a true random number generator(TRNG) in order to obtain a key unique to each IC.
- In the fabrication stage, once the chip is ready to be tested, the chip's built-in (TRNG) generates a public and private Random Chip Key pair (RCK-public, RCK-private). RCK-public is sent to the IP owner while RCK-private is kept on the chip.

EPIC

- The IP owner uses MK-private and RCK-public to encrypt CK (which only the IP owner knows). These two layers of encryption add some security to the process. The encrypted common key is IK. IK will be different for each chip since it is encrypted using different keys.
- IK is sent to the chip at the foundry, and is an input to the RSA decryption logic. The built-in RSA uses the RCK-private and MK-public to decrypt IK and obtain CK. CK should be invisible to the foundry and only visible to the inputs of the XOR gates.
- If IK is correct, the XOR gates will allow the correct functionality of the circuit.

Analysis of 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.