(IP Protection using Metering)

Metering

- Today's design houses can not afford the in-house chip fabrication cost and that they have to outsource this fabrication to foundries elsewhere.

- This gives the foundries access to the details of the chips and the possibility of overbuilding them without the authorization from the design house.

- IC metering or hardware metering, is an effective method to defend against this IP infringement.
- It is a set of tools, methodologies, and protocols that enable the design house to achieve post-fabrication control over their ICs.

- **Basic Idea of IC metering:**
  - The basic concept behind IC metering is to enable a unique tag to each copy of the IC and make sure that the tag is under the control of the design house, not the foundry.

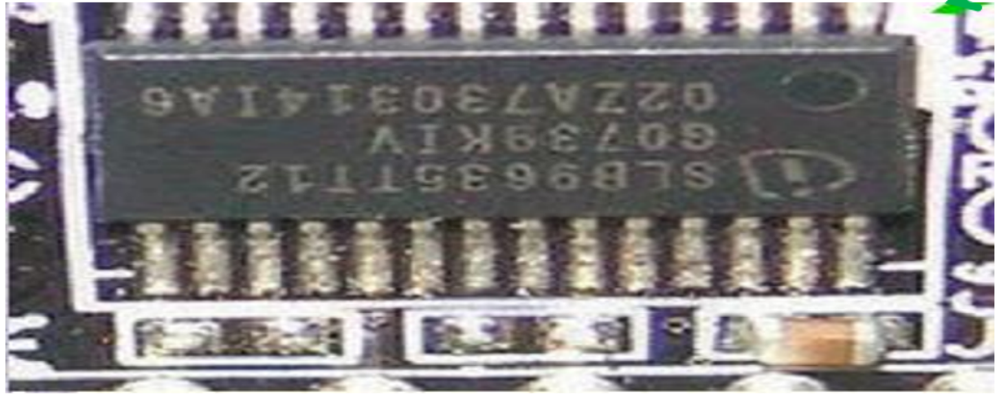
- ***The difference between metering and obfuscation is that while metering uses a unique unlock key per IC, obfuscation just locks the IC.***

Metering : Taxonomy

- Different types of tags have been proposed and used for hardware metering:
- **Passive vs. Active:**
  - when the tag can only be used for chip identification, it is called a passive metering.
  - The tag in active metering can also do a lot of other functionalities, such as enable the chip, disable the chip, or control the chip.
- **Internal control vs. external control**
  - Whether the control is part of the design
- **Intrinsic vs. Extrinsic**
  - Whether additional hardware components, or the modification of the design needed.
- **Non-functional vs. Functional**
  - Whether the tag is related to functionality
- **Reproducible vs. Unclonable**
  - Whether the tag can be reproduced

Metering : Tags Example

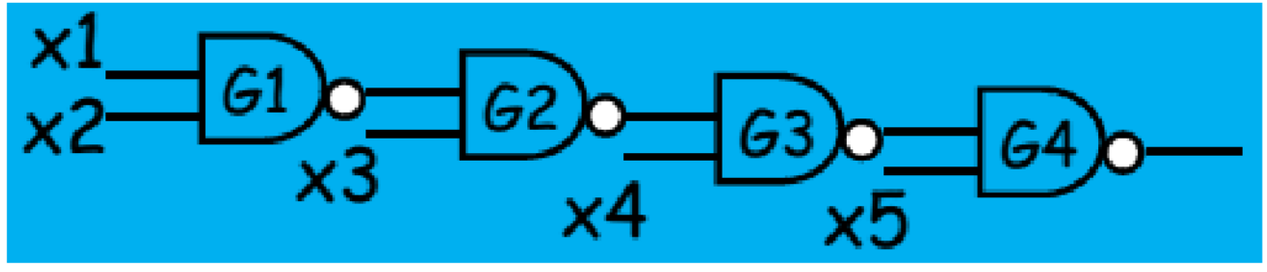
- **Serial Number (ID):**
  - Physically indented on the device
  - Stored in memory
  - Passive, extrinsic, non-functional,
  - Reproducible



- **ICID:**
  - Proposed in 2007 based on silicon fabrication variation (e.g. SRAM PUF, timing, leakage)
  - Passive, intrinsic or extrinsic, non-functional, unclonable.

Metering : ICID Example Based on Leakage Current

- **An Intrinsic Unclonable ICID:** Not Required Additional Hardware
  - Consider a subcircuit of 4 NAND2 gates



Leakage of an ideal NAND2 gate

Input	Leakage
00	37.84
01	100.3
10	95.7
11	454.5

Leakage on two identical ICs from different foundry

Input Vector	IC1	IC2
00011	1391	2055
10101	2082	1063
01110	1243	2150
11001	1841	1905

Metering : Example (Cont...)

- **Active IC Metering:**
  - Design house modifies the functional description of the design (e.g. FSM) to insert a lock.
  - Foundry fabricates the ICs
  - Each IC will have a unique and unclonable identifier due to the manufacture variation (e.g. PUF)
  - Design house utilizes the ID and the modification for active metering (e.g. enabling, disable, lock, unlock ICs)
- **An Internal Active IC Metering:**
  - **Metering scheme**
    - Add FF's to boost FSM
      - One extra FF doubles the number of states
    - Power up FSM determined by PUF
      - Good chance the power up state is not in the original FSM. But the IC has to start with a specific initial state to keep its functionality
    - Design house provides correct input sequence to reach the initial state
  - **Active, internal, extrinsic, functional, unclonable.**

Metering : Example (Cont...)

- **An External Active IC Metering :**
  - Add control signals and logical unit (e.g. via XOR) to non-critical parts of the design
  - Each fabricated IC will be locked unless all control signals have correct values
  - Design house provides an external key to unlock each IC based on an asymmetric cryptographic primitives (e.g. PKI)
  - Active, external, extrinsic, functional, unclonable.

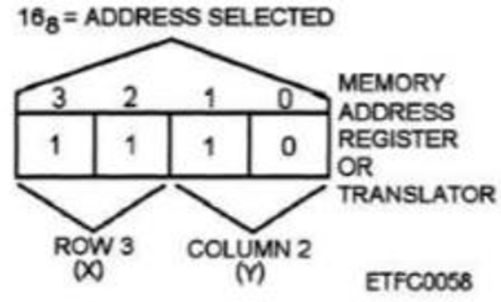
- **Note:** The difference between metering and obfuscation is that while metering uses a unique unlock key per IC, obfuscation just locks the IC.

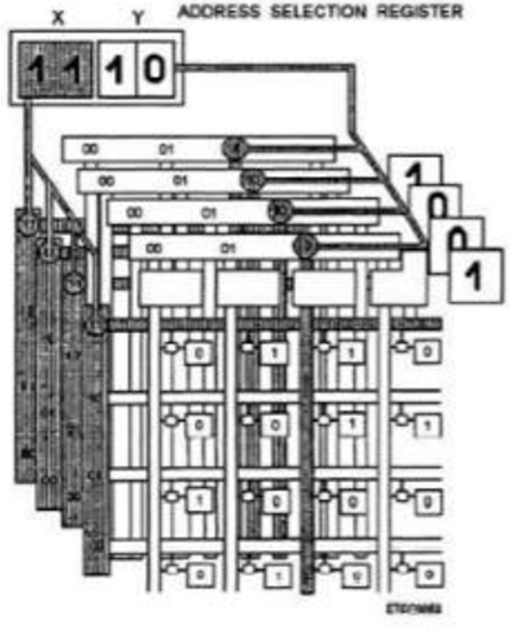
Metering : Non-functional Identification

- 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 tagso 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: R**eproducible and Unclonable**

Metering : Reproducible Identifiers

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





Metering : 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.

Metering : 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 : Functional Metering

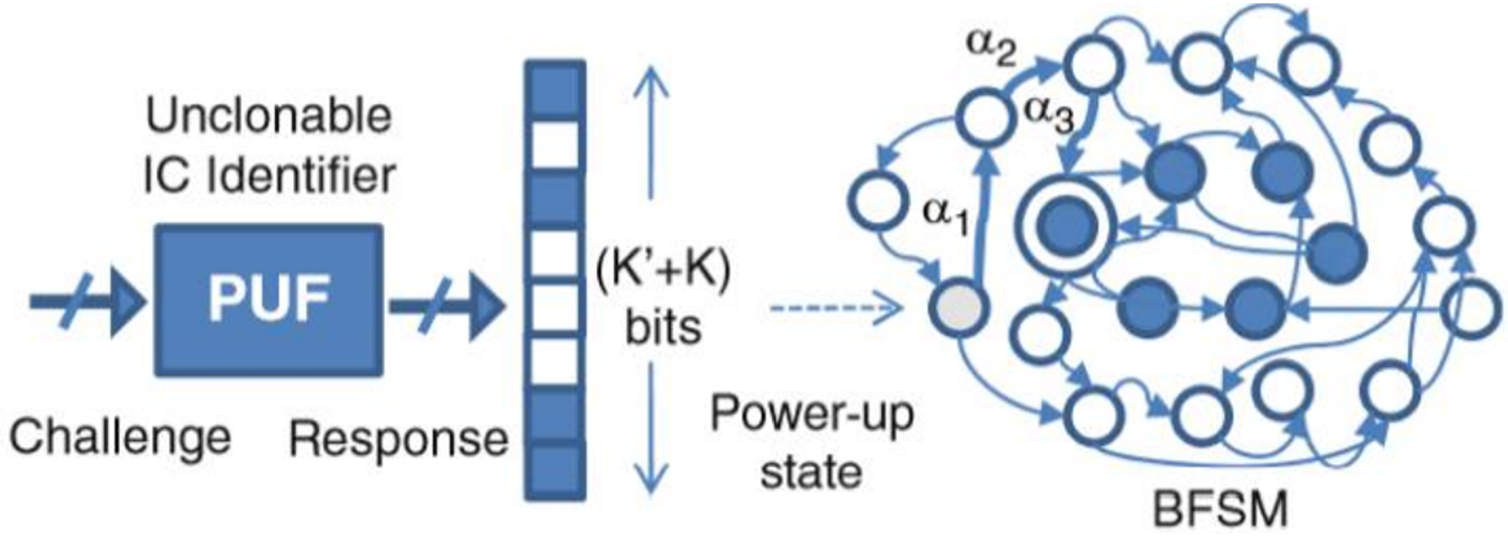
- Identifiers linked to chips internal functional details during synthesis.
- Each chip’s function gets a unique signature, E.g., additional states added to generate same output.
- Function unchanged from input to output.
- Internal transactions unique to each chip.
- Challenge in fabricating ICs with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

Metering : 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:** 1. Internal and 2. External.
- 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.

Metering : 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.

Metering : External Active Metering

- **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.