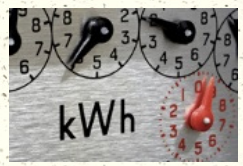
Intellectual Property Protection -- Hardware Metering

Cybersecurity Specialization
-- Hardware Security

Why Hardware Metering?

- Integrated circuit (IC) metering is a set of security protocols that enable the design house to achieve post-fabrication control over their ICs.
  Source: F. Koushanfar, "Hardware Metering: A Survey", 2012
- IC overbuilding and metering
  - Asymmetric relationship between design house and the foundry → overbuilding
  - Can we use digital watermarking?
  - Can we use digital fingerprinting?

How Metering Works?



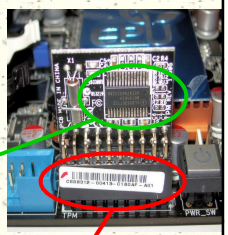
- Metering in utilities
  - Provider monitors users
- IC overbuilding
  - Foundry is the provider (of ICs)
  - Design house is the user (receiving ICs)
  - Reverse metering: user monitors provider!
- Idea of IC metering
  - Tag each copy of the IC
  - Control the tags

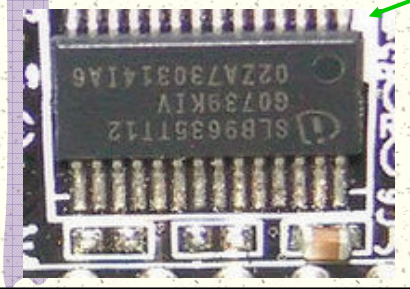
Taxonomy of Metering Methods

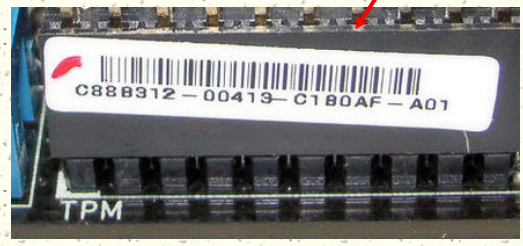
- Passive vs. active
  - Identification only or more involvements
- Internal control vs. external control
  - Whether the control is part of the design
- Intrinsic vs. extrinsic
  - Whether additional components are needed
- Non-functional vs. functional
  - whether the tag is related to functionality
- Reproducible vs. unclonable
  - Whether the tag can be reproduced

Serial Number and ICID

- Serial number (ID):
  - Physically indented on the device
  - Stored in memory
  - Passive, extrinsic, non-functional, reproducible





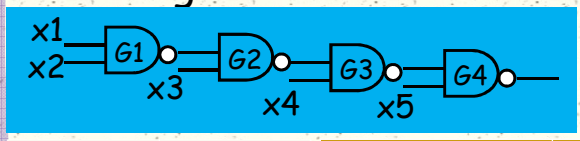


Serial Number and ICID

- Serial number (ID):
  - Physically indented on the device
  - Stored in memory
  - Passive, extrinsic, non-functional, reproducible
- ICID:
  - Based on silicon fabrication variation (e.g. SRAM PUF, timing, leakage)
  - Passive, intrinsic or extrinsic, non-functional, unclonable

An Intrinsic Unclonable ICID

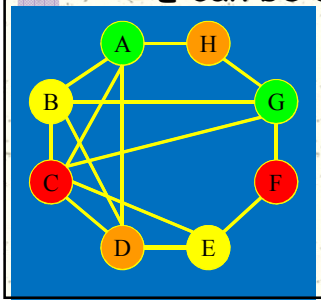
- Consider a subcircuit of 4 NAND2 gates
- Leakage of an ideal NAND2 gate
- Leakage on two identical ICs



Input	Leakage	Input Vector	IC1	IC2
00	37.84	00011	1391	2055
01	100.3	10101	2082	1063
10	95.7	01110	1243	2150
11	454.5	11001	1841	1905

A Functional Passive Tagging

- IP: solution to a GC problem.
- Find a high quality solution (optimal here)
  - H can be RED, or YELOW
  - F can be BROWN
  - E can be GREEN



- Functional tag:
  - 3x2x2=12 distinct coloring schemes (tags) by changing the colors of H, F, E.

Active IC Metering

- Design house modifies the functional description of the design (e.g. FSM)
- 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.

An External Active IC Metering

- Add control signals and logic (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.