Hardware Metering

M. Tehranipoor

ECE5451: Hardware Security & Trust
University of Connecticut
ECE Department

Background: Test and Yield

- Errors in fabrication process cause defects on chip which causes chip to malfunction.
- Chips are tested in order to detect defects
- Failing chips are discarded
- Fraction (percentage) of remaining good chips is called the yield.

\[
\text{Yield} = \frac{\text{total chips} - \text{discarded chips}}{\text{total chips}}
\]

- Foundry decides/predicts yield

HW Threats

- IP Vendor
- System Integrator
- Manufacture

Any of these steps can be untrusted

IP Piracy
System Trust

Untrusted

IC Trust

Secure Manufacturing Test

Untrusted Foundry

IC Piracy (Counterfeiting)
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.

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.

Taxonomy of Metering Methods

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 and Passive

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

- Tagging an IC’s functionality: Functional Identification
**Taxonomy of Metering Methods**

<table>
<thead>
<tr>
<th>Passive</th>
<th>Functional Identification</th>
<th>Nonfunctional Identification</th>
<th>Internal control</th>
<th>External control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reproducible</td>
<td>Analog</td>
<td>Digital</td>
<td>Reproducible</td>
<td>Unclonable</td>
</tr>
</tbody>
</table>

**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. Ex. PSN
    - 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 their database.
**Functional Metering**

- Identifiers linked to chip’s internal functional details during synthesis.
- Each chip’s function gets a unique signature.
  - additional states added that 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.

One method is fabricating chips from same mask and maintaining one programmable path. 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 actually functionality of the chip is hidden during the test process by foundry and assembly
- It requires additional circuitry that is useless after testing.

---

**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 and 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.
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 $S_1$ states requires $K_1 = \log_2(S_1 + S)$ flip flops
- Few additional flip flops can exponentially increase the number of states.

---

Taxonomy of Metering Methods

- Passive
  - Non-functional Identification
  - Reproducible
  - Internal control
  - Reproducible
  - External control
  - Unclonable
- Functional Identification
  - Reproducible
  - Analog
  - Digital
- Hardware Metering
  - Reproducible
  - Unclonable
- Active
  - Reproducible
  - Unclonable

---

External 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.

---

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

EPIC High Level

**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, Out-of-Spec ICs and defective ICs.
  - Over-produced:
    - 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 IC.
  - Out-of-Spec:
    - 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.
Reconfigurable Logic Barriers (LB)

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

20 October 2014

Reconfigurable Logic Barriers

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

20 October 2014

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.

20 October 2014

LB: Unlocking Framework

- k- input lookup tables (LUTs) are used for logic barrier combinational locking.
  - LUTs preferred over XOR gates due to their exponential number of locking combinations.
  - k inputs, $2^k$ possible combinations
- Location of LUT based on observability and controllability.

20 October 2014

LB: Partitioning of Design

20 October 2014

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.
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.

Traditional Test

- Designer
- Foundry & Assembly

Secure Split-Test

- 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.
- Detecting a non-functional chip is significantly easier than using PUF and dealing with process variations.

XOR Mask

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

IN1: True Random Number Generator

- Input IN1 is connected to a TRNG.
- TRNG generates a random number TRN.
- Same TRN is needed at foundry and assembly.
- TRNG outputs are burnt into fuses so same TRN can be read.

IN2: RSA - Asymmetric Encryption

- Encryption mechanism that uses a set of private and public keys to perform reversible encryption.
**SST Communication Flow**

Foundry → Fabricate Die → Obtain TRN → Uses TRN to create TKEY → RSA Private Key → TKEY → RSA Public Key → IN2 → RSA → Discard Die

Assembly → Package Die → Obtain TRN → RSA Private Key → TKEY → RSA Public Key → IN2 → RSA → FKEY → Check Results → Yes → Fully Functional Chip

**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)

- 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.
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.

On startup: PUF generates random sequence as input to FSM.
- Due to large number of added states, high probability that starting state will be an added state.

Foundry communicates current state to IP Owner
- Owner knows FSM and can generate key (sequence) to reset FSM

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.
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