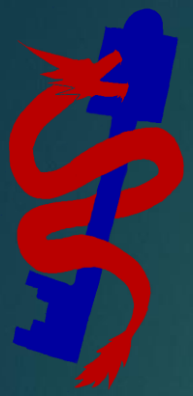


AsianHOST 2017

# DOST: Dynamically Obfuscated Wrapper for Split Test Against IC Piracy


**Xiaoxiao Wang, Yueyu Guo, Tauhid Ramhan, Dongrong Zhang, and Mark Tehranipoor**

**Beihang University**
**University of Florida**

# Motivation

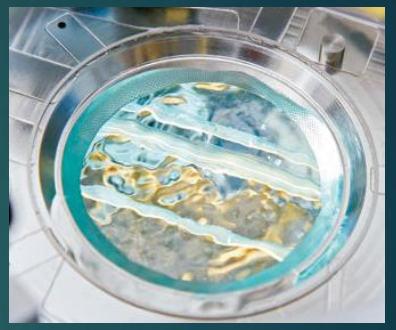


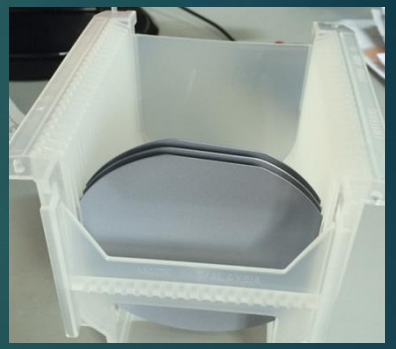
- Fabless Production Causes Trust Issues

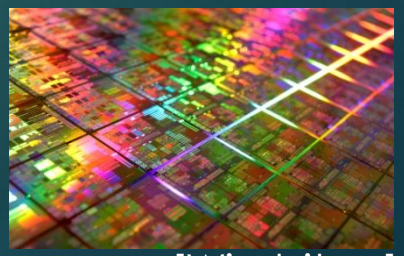
→ Our Objective

- Overproduction
  --Prevents illegal copies from being functional
- Releasing Defective/Out-of-spec IC
  --Prevents defective or out-of-spec devices from being activated
- Cloning
  --Prevents the design from being reverse engineered

[Intel]







[Wirebiters]

# Motivation



- Major Solutions to Deal with Fab Attacks
  - Split Manufacturing [10][11]
    --Cost is high; BEOL Can be fully or partly Recovered [12]
  - Metering/Locking [13,14]
    --IC needs to be unlocked before structural test
  - Secure Split Test (SST) [7,8]
    --IC needs to be unlocked before functional test
    --The structural response is uniquely encrypted

Address the Gap left for Defective /Out-of-spec ICs

# The Basic Concepts



- Reduce the data volume of secure structural test

→ Prevent **DEFECTIVE** IC from being activated

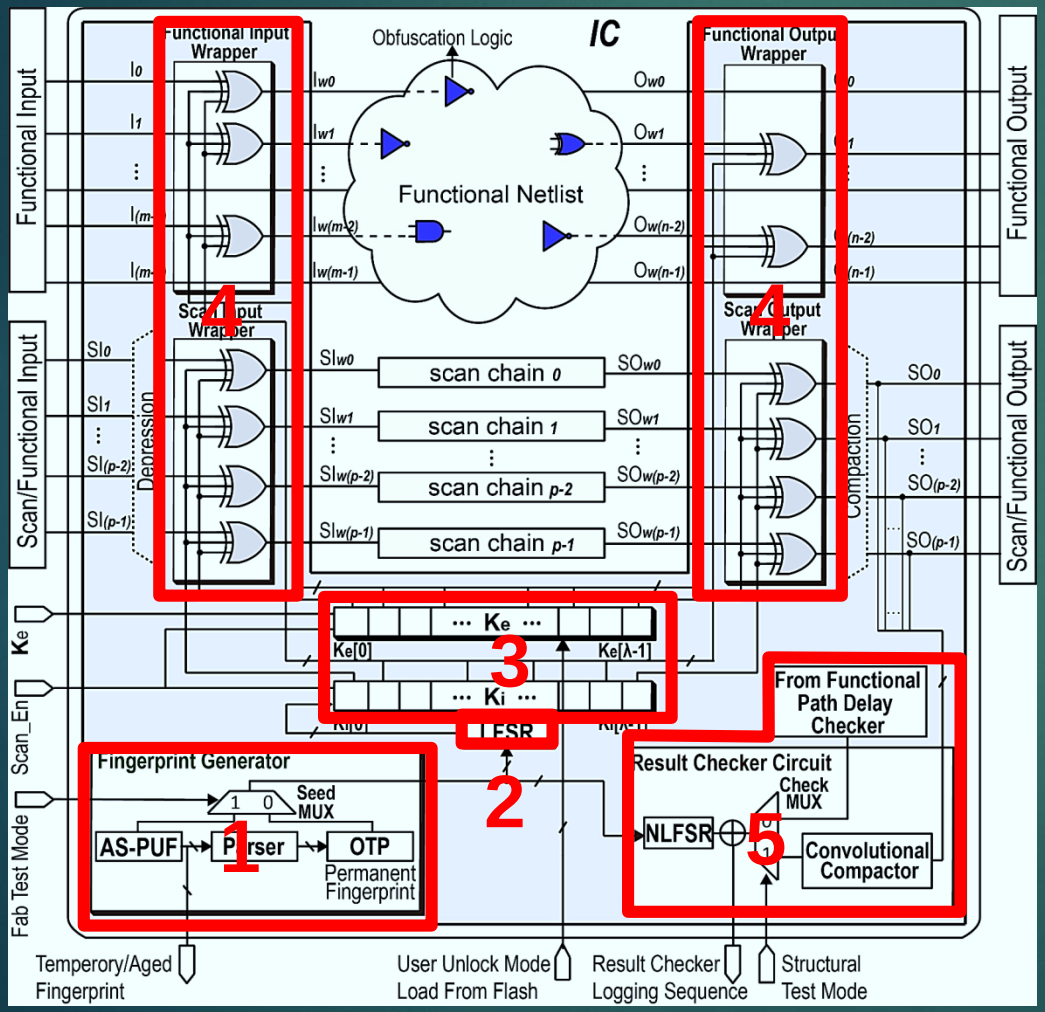
- Allow IP owner to perform final activation based on the functional test results

→ Prevent **OUT-OF-SPEC** IC from being activated

# Architecture



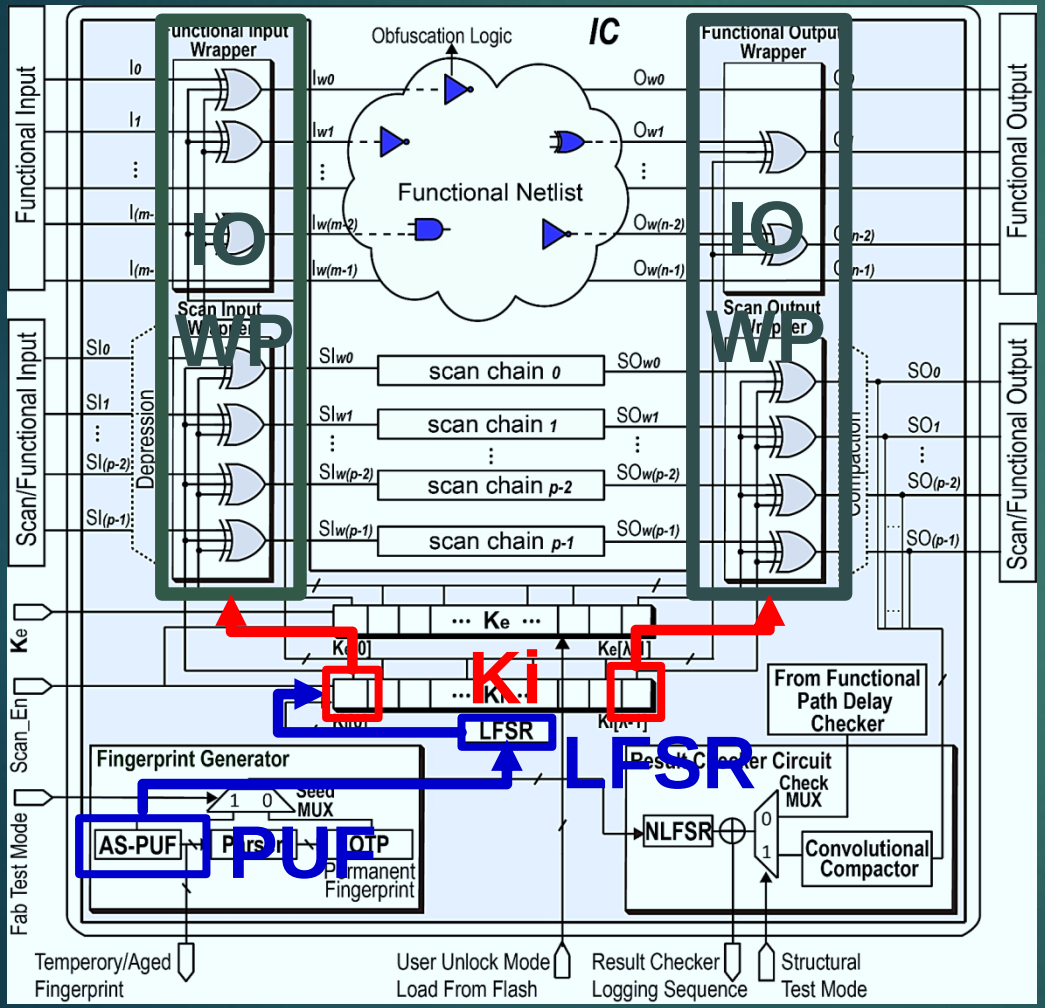
## Dynamically Obfuscated Wrapper for Split Test (DOST)




1. Fingerprint Generator
2. LFSR
3. Internal and External Key Registers
4. I/O Wrapper with the Obfuscation Logic
5. Result Checker Circuit

# Structural Test with DOST

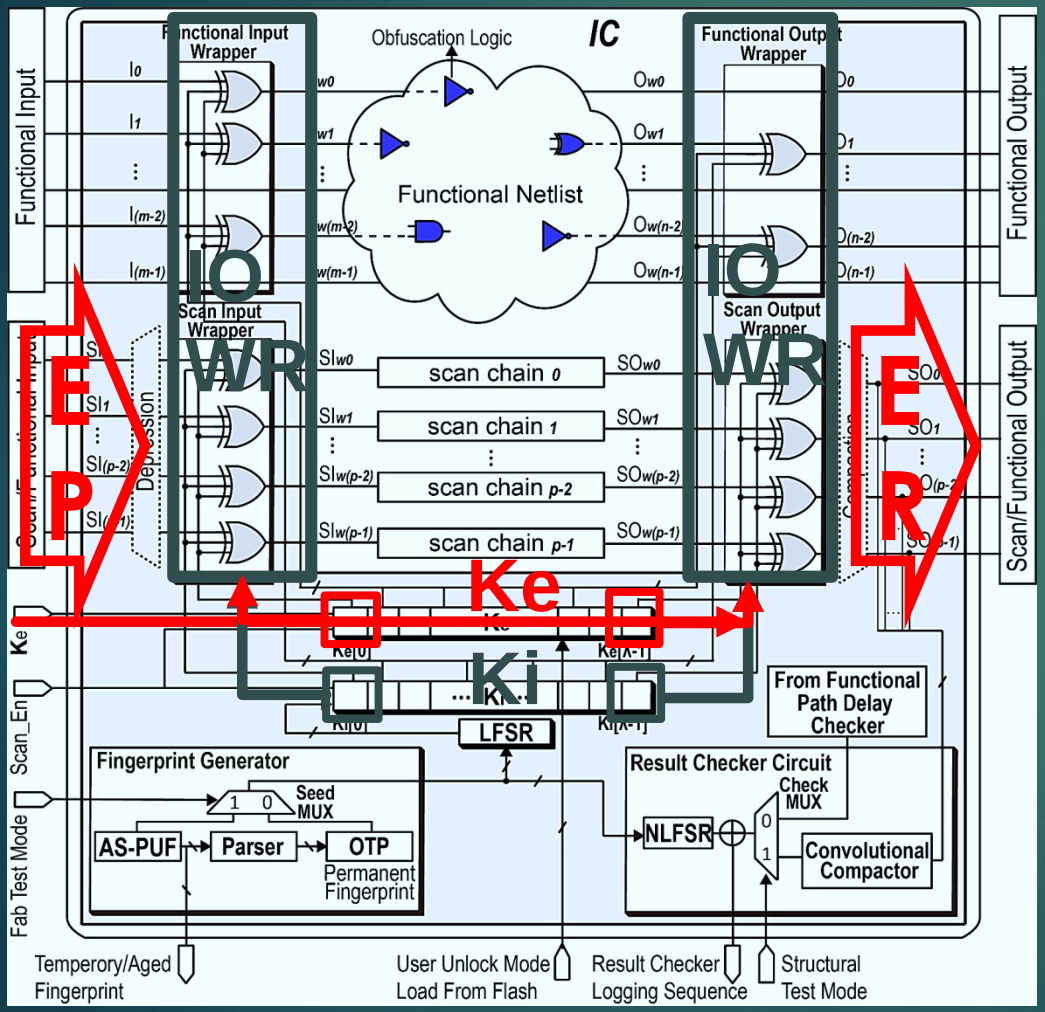





- The IO Wrapper is uniquely locked by $K_i$
- The value of $K_i$ is determined by the output of PUF and LFSR

# Structural Test with DOST

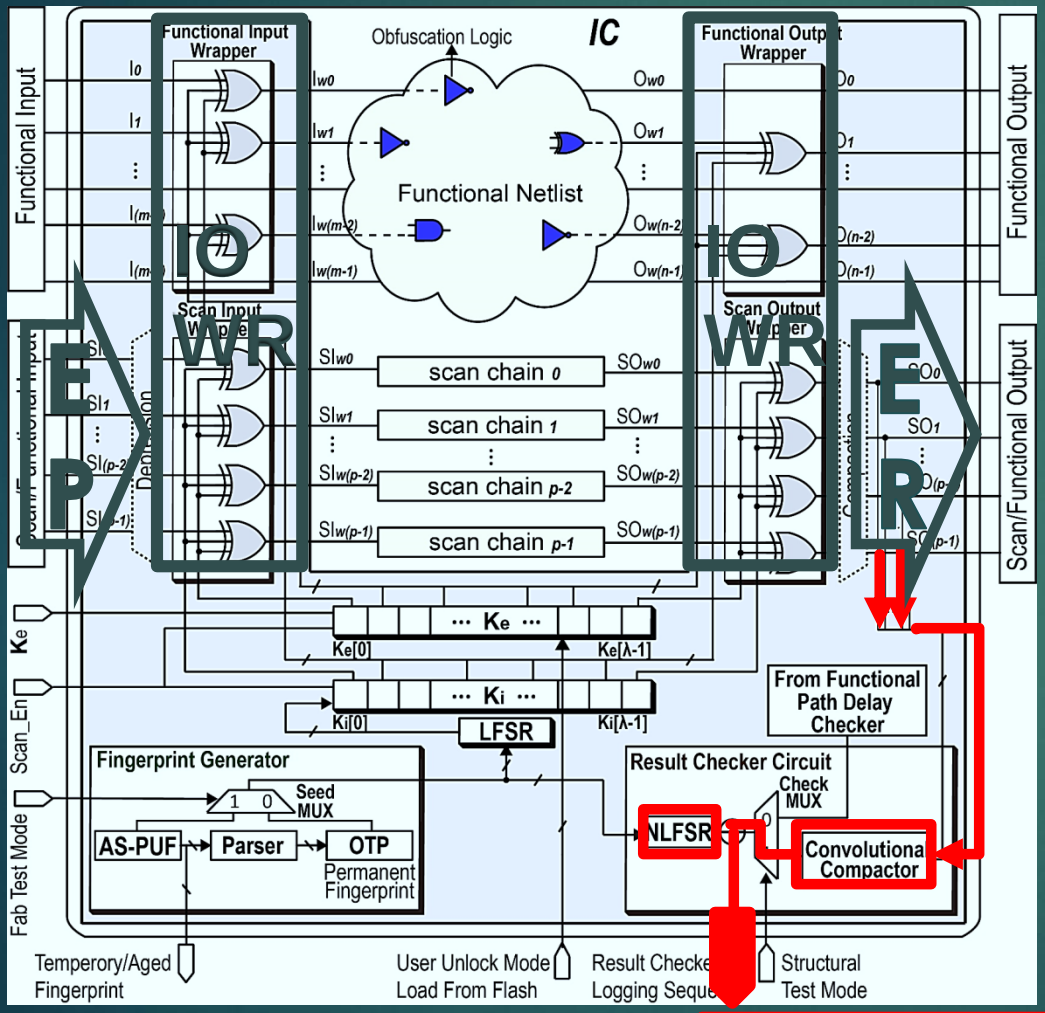





- The structural test pattern/responses set are universally encrypted for all DUTs.
- A unique $K_e$ is supplied externally to decrypt EP.

# Structural Test with DOST





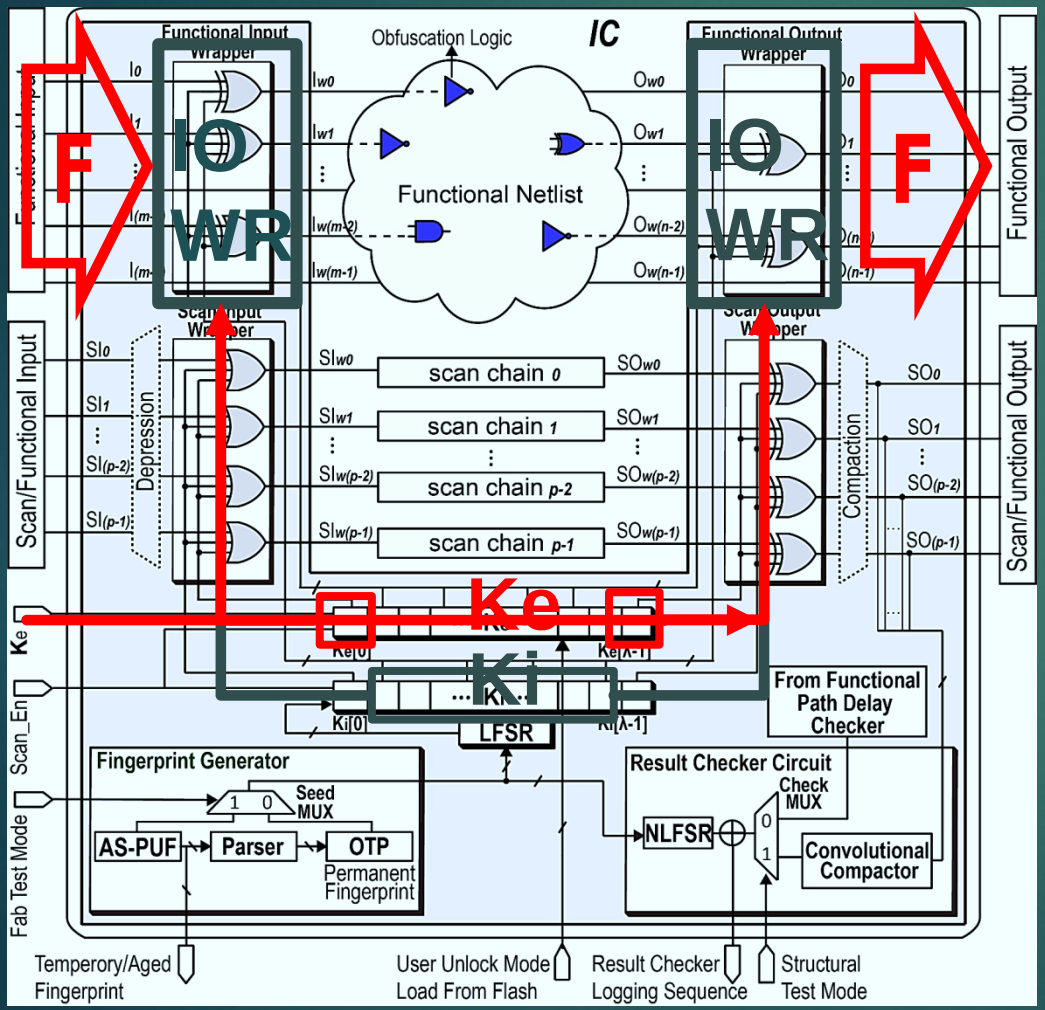

- The encrypted response is compacted into a <u>one-bit sequence</u>.
- The sequence is <u>uniquely encrypted</u> by NLFSR as structural test footprint.

**Structural Test Footprint**

101100011100001100001010011000 1…

# Functional Test with DOST

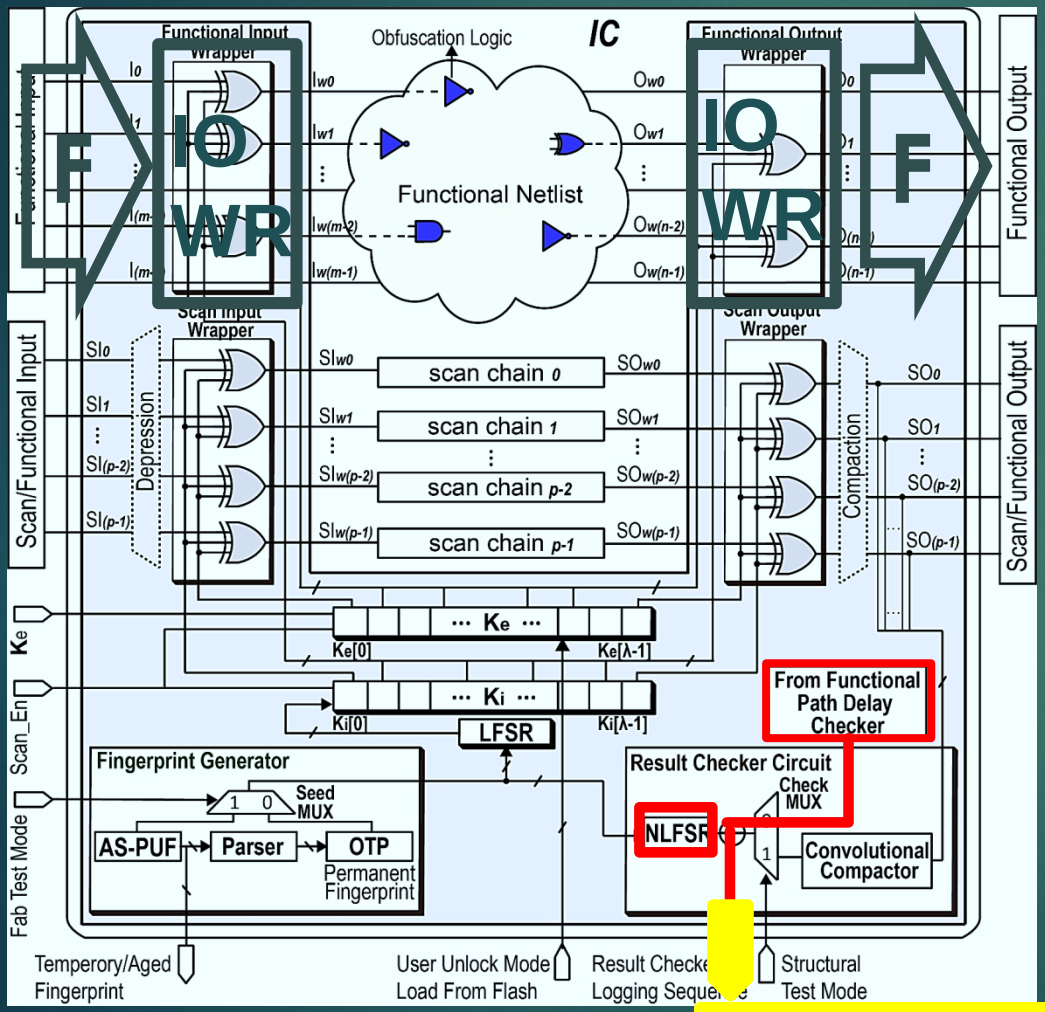





- Another unique $K_e$ for functional test is applied to unlock the functional IO.
- All functional tests can be applied.

# Functional Test with DOST






- Functional sensors' signatures can be scanned, uniquely encrypted by NLFSR as functional test footprint.

**Functional Test Footprint**

101100101110001110000110000110001…

# Data Logging File



| $ECID_1$ | $ECID_2$ | ... | $ECID_n$ |
|---|---|---|---|
| AS-PUF Value: 101101.. | AS-PUF Value: 101011.. | | AS-PUF Value: 101001.. |
| $K_{es}$: 1001010... | $K_{es}$: 1011010... | | $K_{es}$: 1001010... |
| $K_{ef}$: 0101110... | $K_{ef}$: 0111010... | | $K_{ef}$: |
| $FK_e$: 1101110... | $FK_e$: 0101110... | | F |
| Result Checker Logging for Functional Test: 101010... | Result Checker Logging for Functional Test: | | Res gging for Functional Test: 010010 |
| Result Checker Logging for Structural Test: 101001... | Result Checker Logging for Structural Test: | | Result Checker Logging for Structural Test: 101101... |

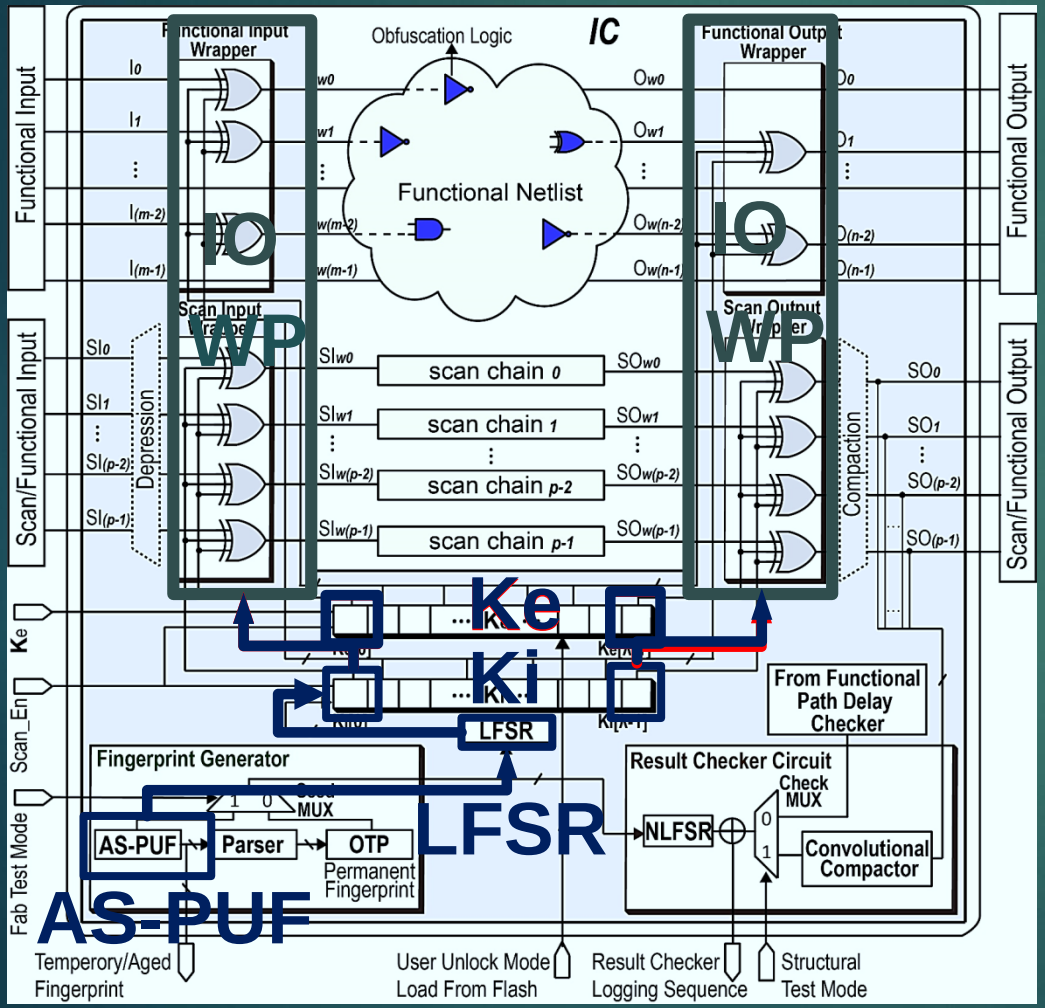
Functional Foot Prints

Structural Foot Prints

**Data Volume increase = 1~2 Scan IO**

# Inactivation Decision

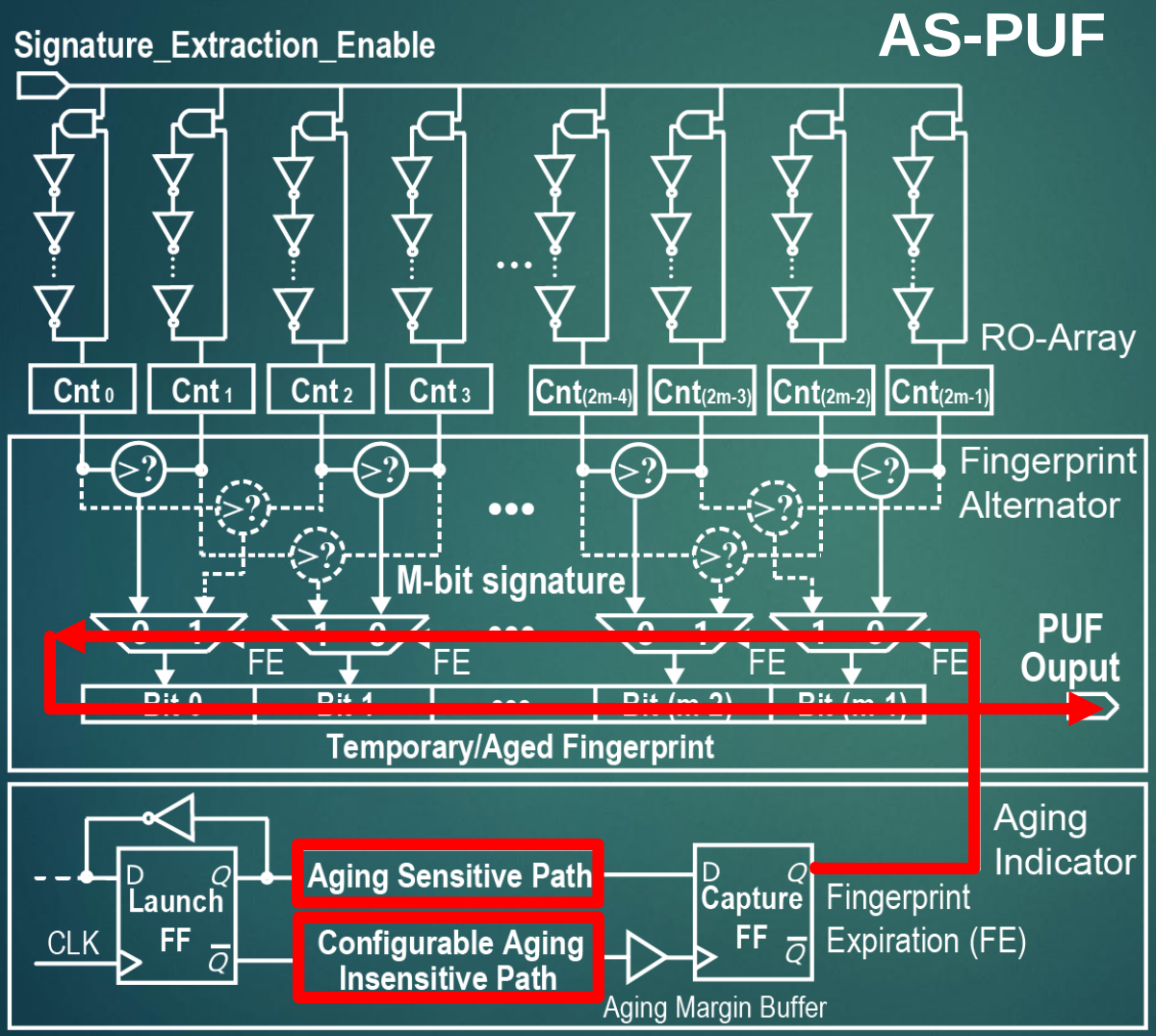





- Aging sensitive PUF's signature expires after test time window.
- $K_i$ expires.
- The current $K_e$ cannot unlock the IO Wrapper any more.
- The chip is locked again.

# Aging Sensitive PUF Design

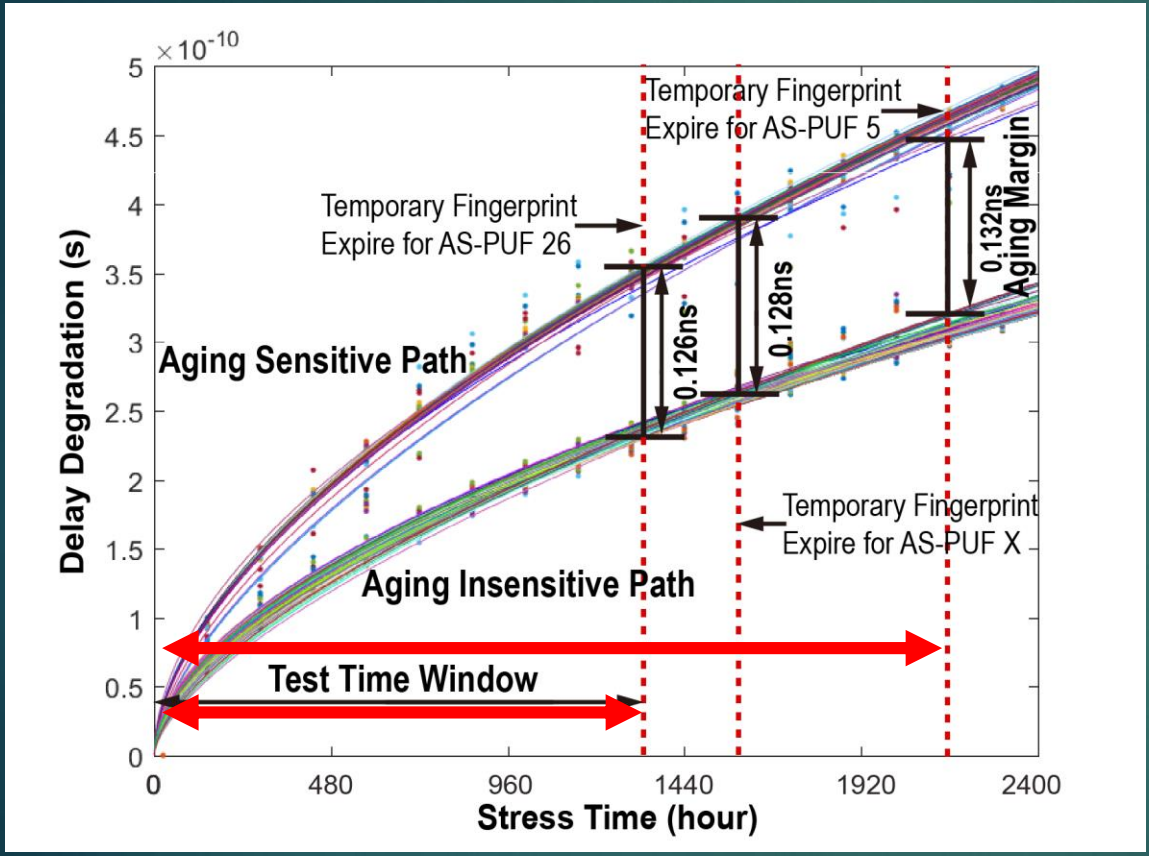





- The degradation gap between the aging sensitive and insensitive paths increases with aging.
- Flips the PUF signature after IP owner's test time window.

# AS-PUF Results

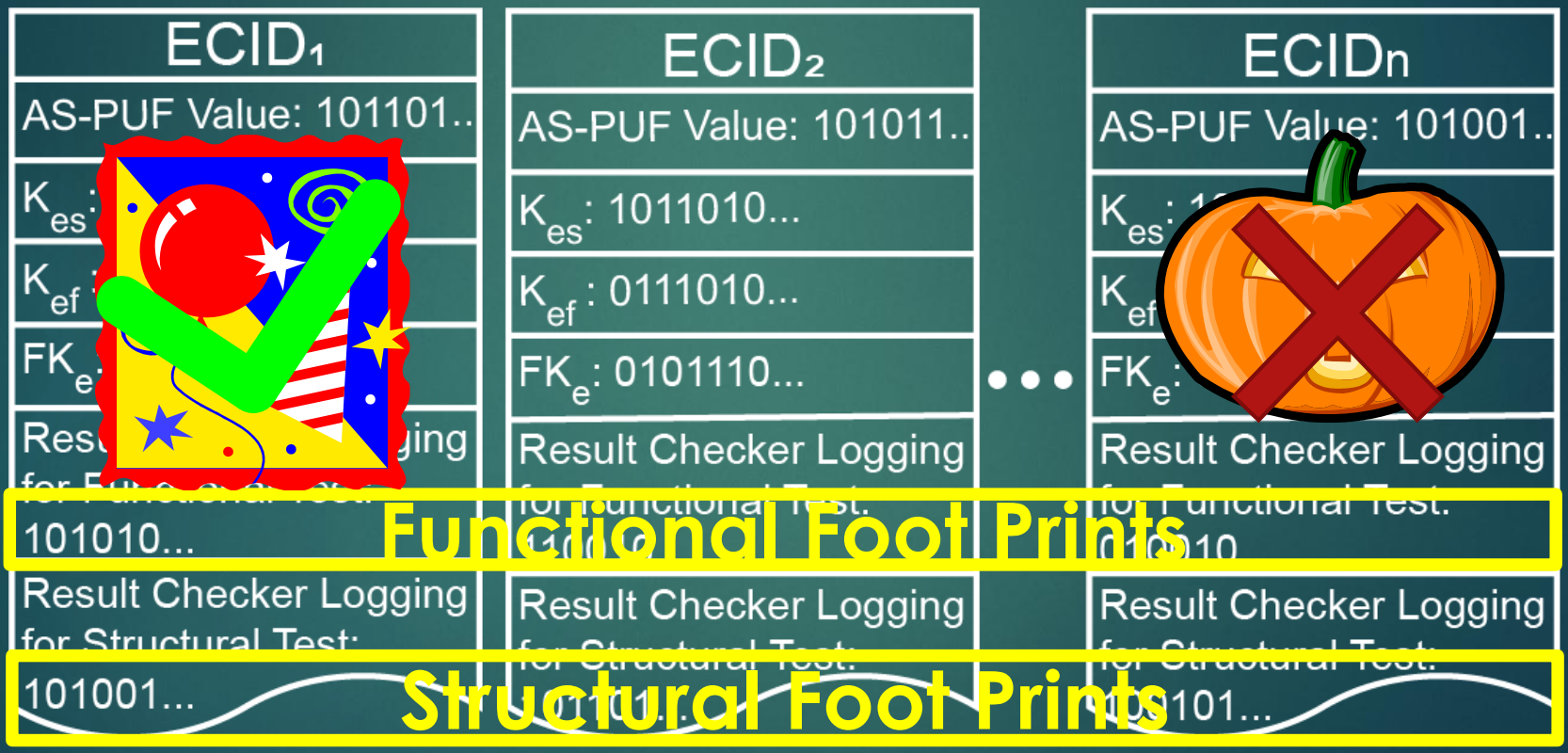





- Delay degradations of 100 samples, with 30% Vth,10% L, 10% W, and 20% tox variations, at 25°C, 32nm without acceleration.
- The test time window distributes in the range between 1329.3 to 2156.2 hours.

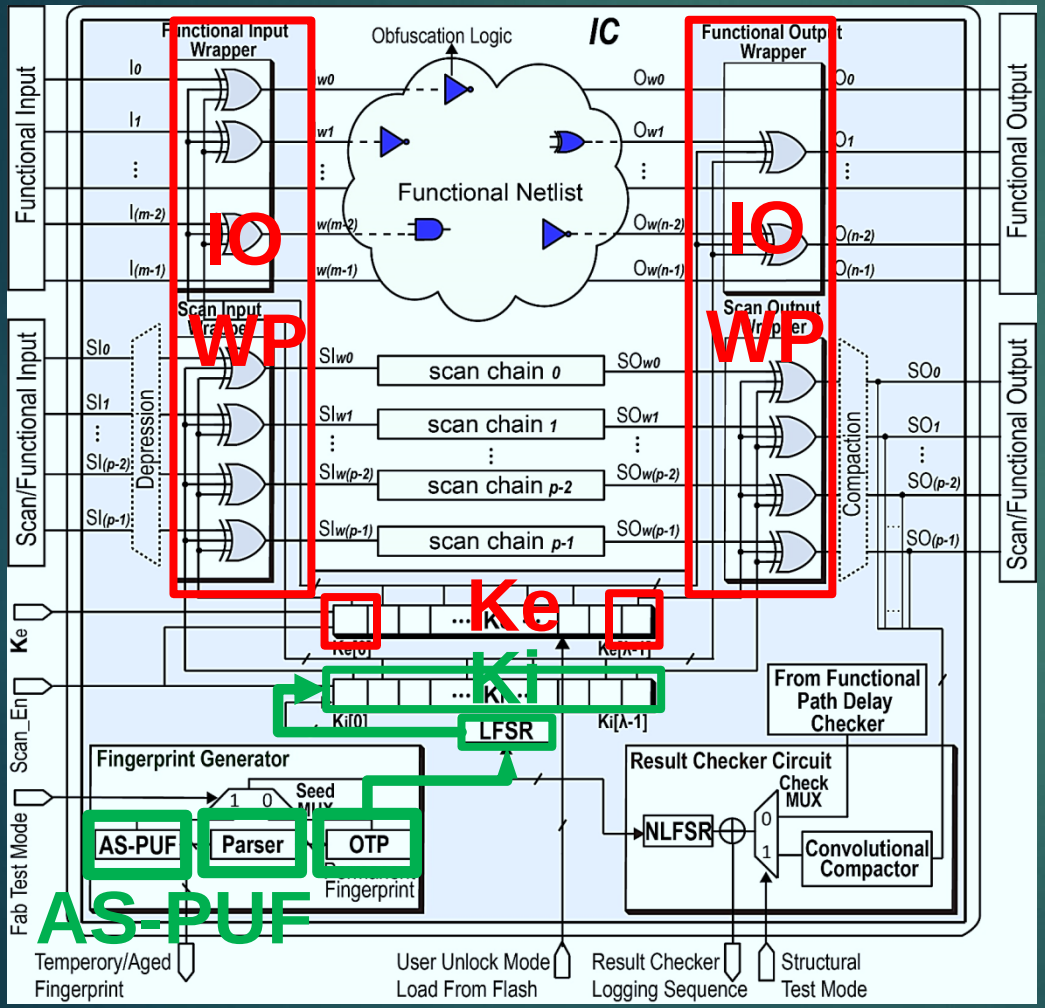
# Data Logging File





# IP Owner Activation

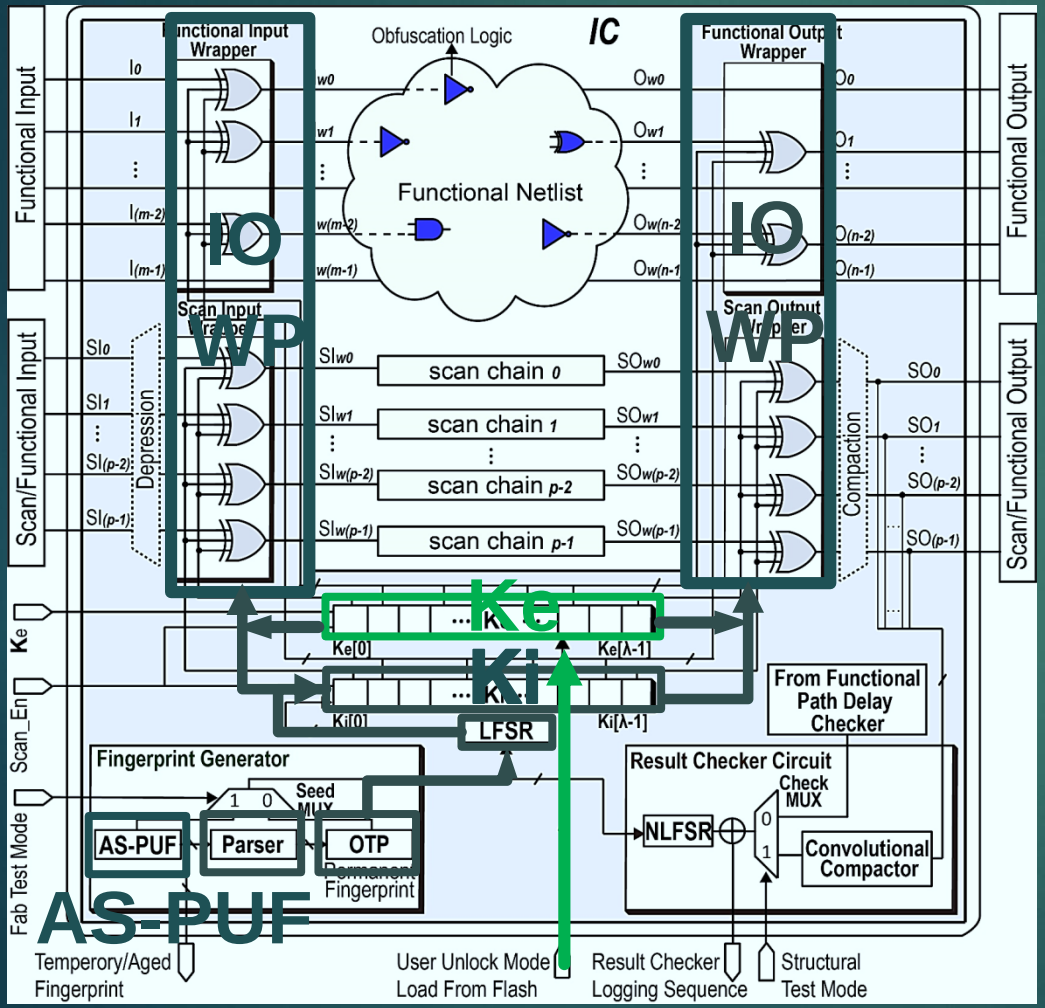





- Another permanent PUF signature is used to generate $K_i$.
- This permanent signature is obtained at fresh time by varying the PUF signature and storing it into OTP.

# IP Owner Activation

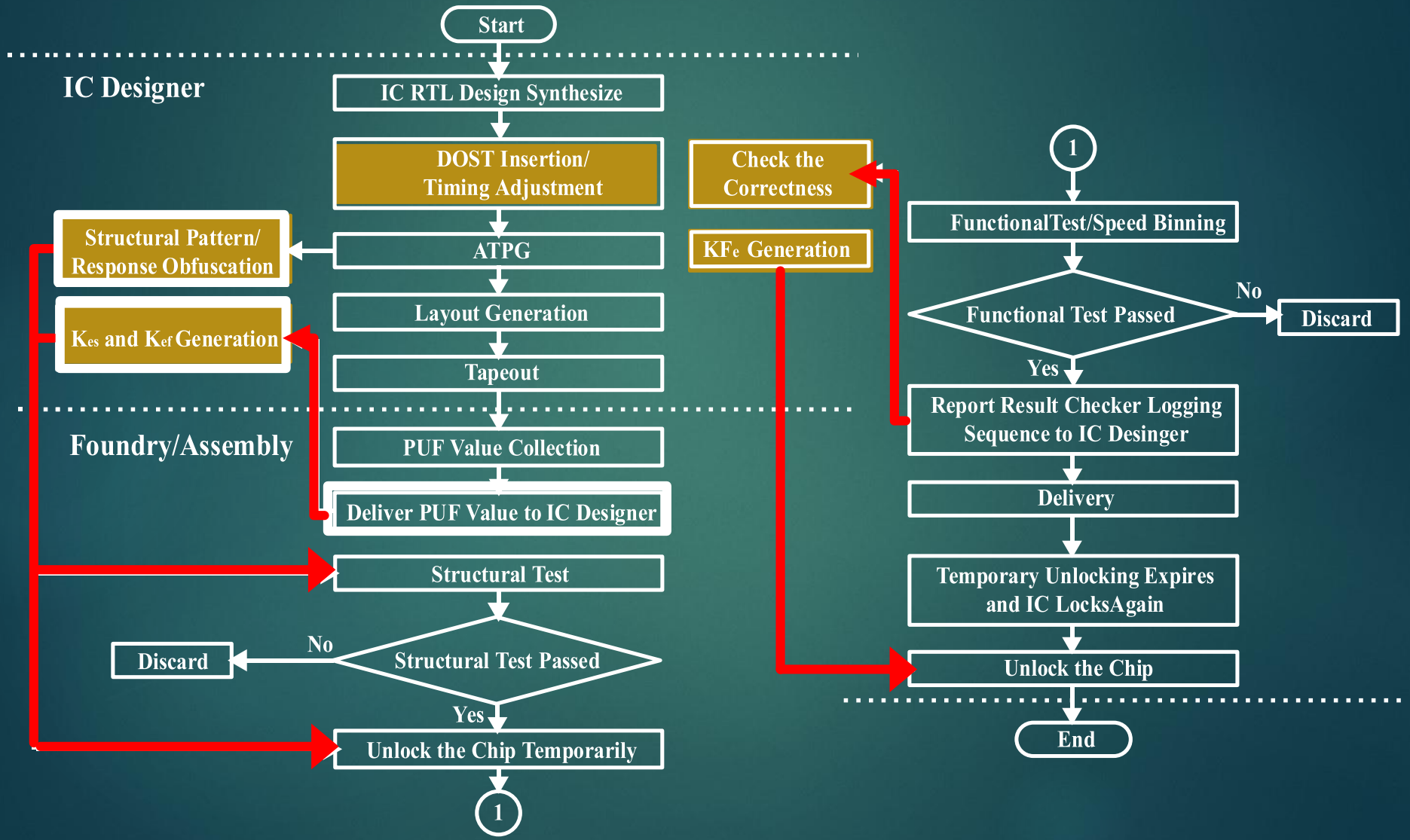





- The new $K_i$ is known by the IP Owner.
- IP owner assigns an activation $K_e$ for final activation.

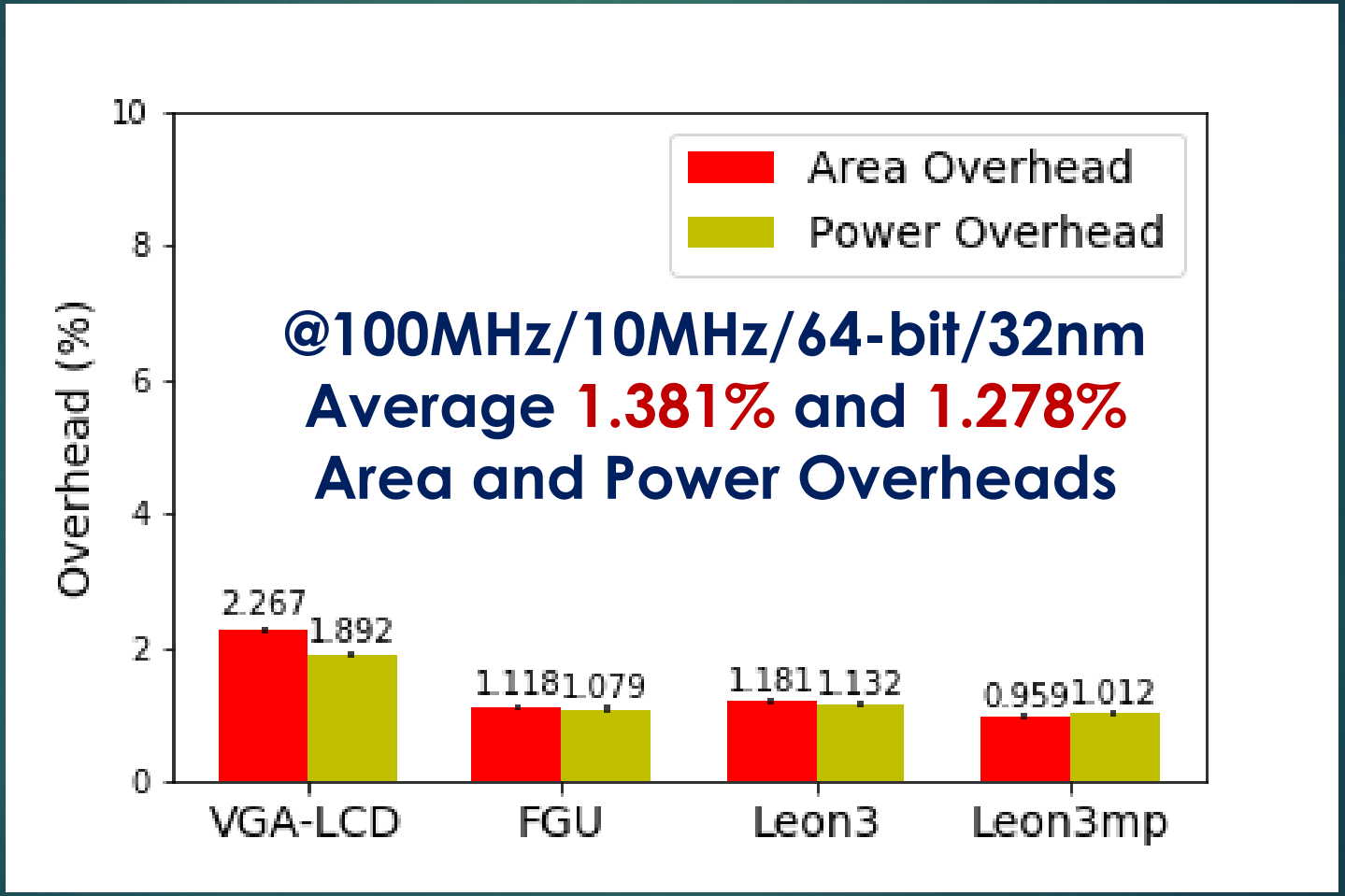
# DOST Flow




Start
IC Designer
IC RTL Design Synthesize
DOST Insertion/ Timing Adjustment
Structural Pattern/ Response Obfuscation
ATPG
Kes and Kef Generation
Layout Generation
Tapeout
Foundry/Assembly
PUF Value Collection
Deliver PUF Value to IC Designer
Structural Test
Discard
No
Structural Test Passed
Yes
Unlock the Chip Temporarily
1
Check the Correctness
KFe Generation
1
FunctionalTest/Speed Binning
Functional Test Passed
No
Discard
Yes
Report Result Checker Logging Sequence to IC Desinger
Delivery
Temporary Unlocking Expires and IC LocksAgain
Unlock the Chip
End

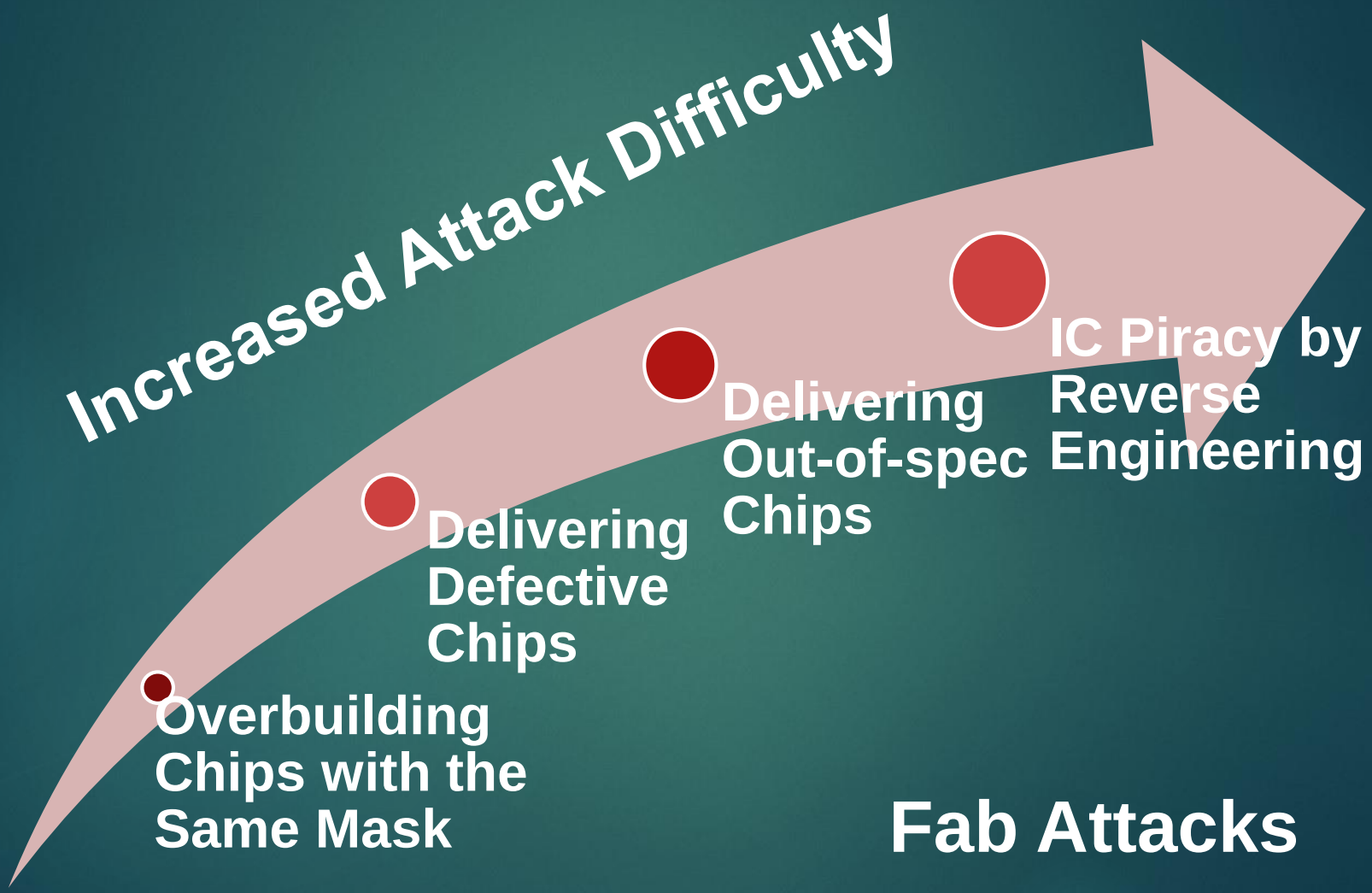
# Area and Power Overheads





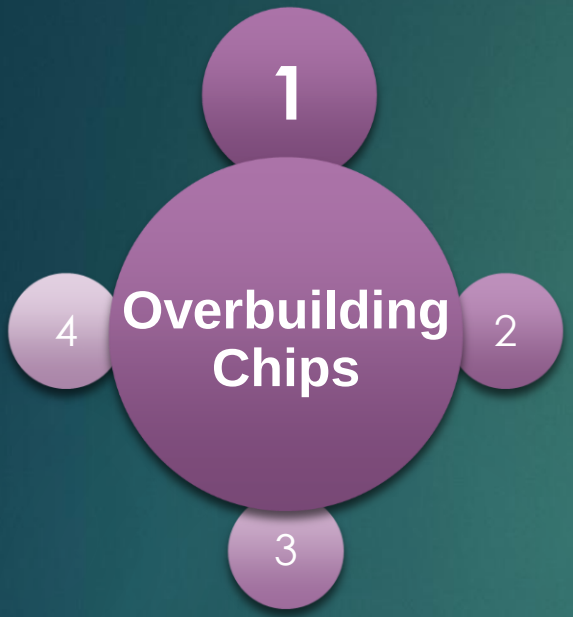
# Security Analy. @ Fab Attacks





# Security Analy. @ Fab Attacks





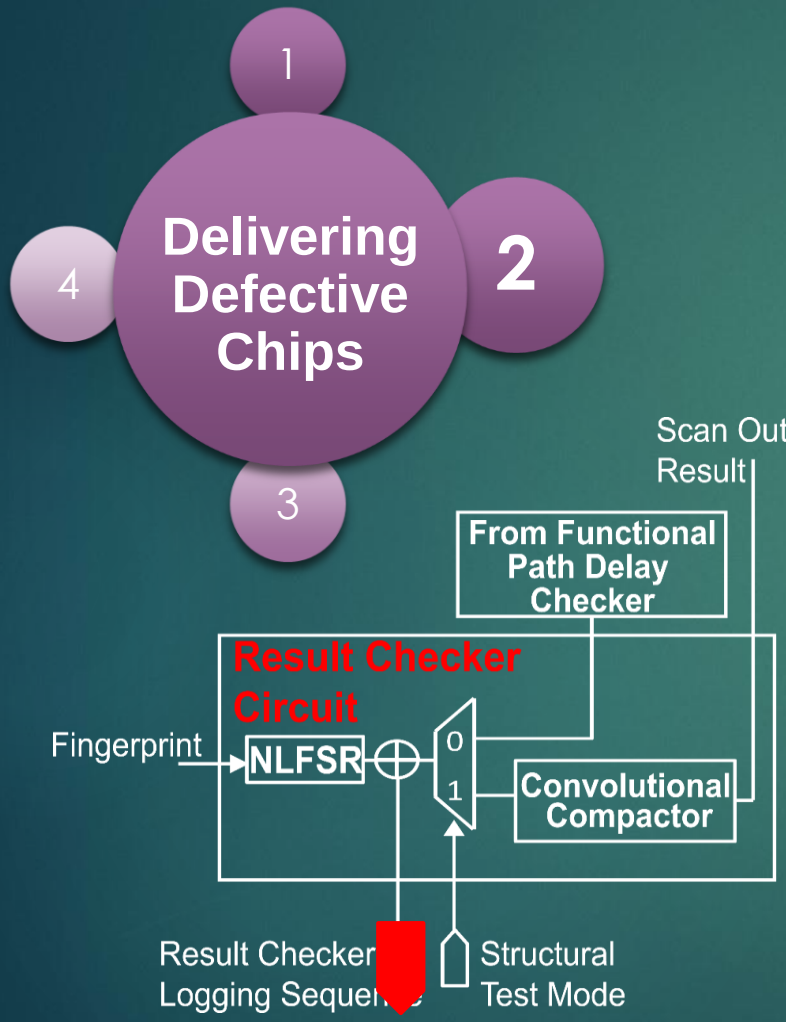

**Fab reuses the mask to overbuild**

**Only contracted number of *FKe* are given**

**Overbuilding is prevented**

# Security Analy. @ Fab Attacks






**Foundry may deliver defective chips as fault-free ones**

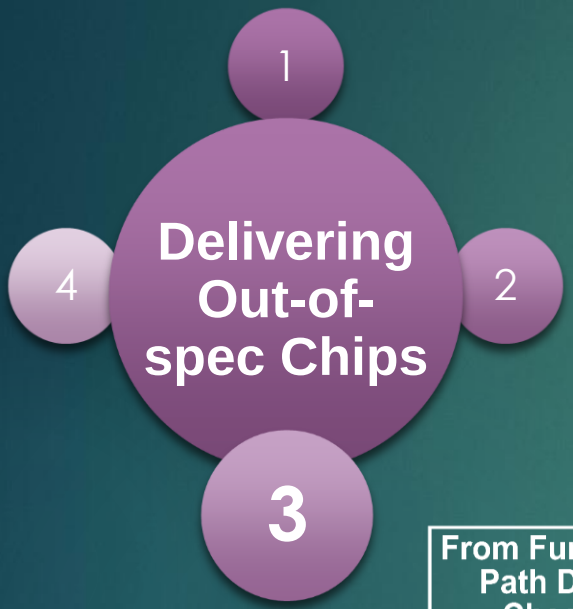
**A unique and encrypted structural test logging sequence is included in the report data base**

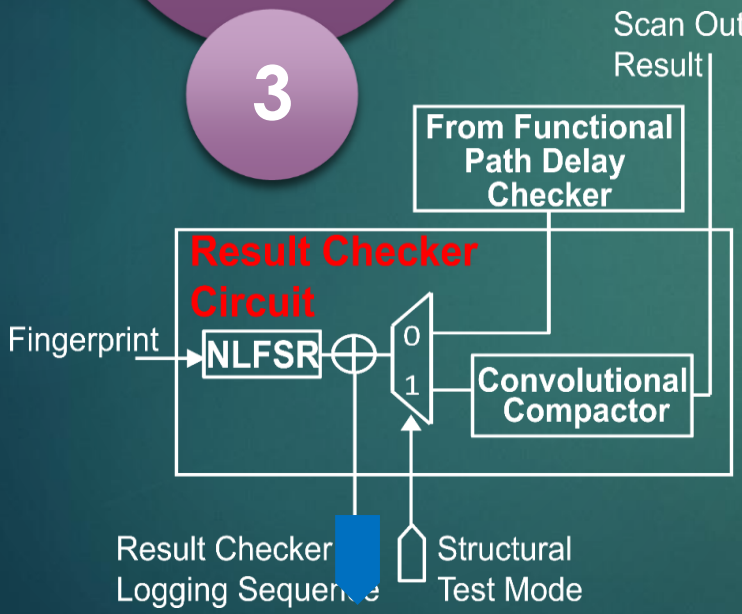
***Activated* when defect free**

**10110001110000110000101001100001…**

# Security Analy. @ Fab Attacks






**Out-of-spec devices can be labeled as in-spec ones**

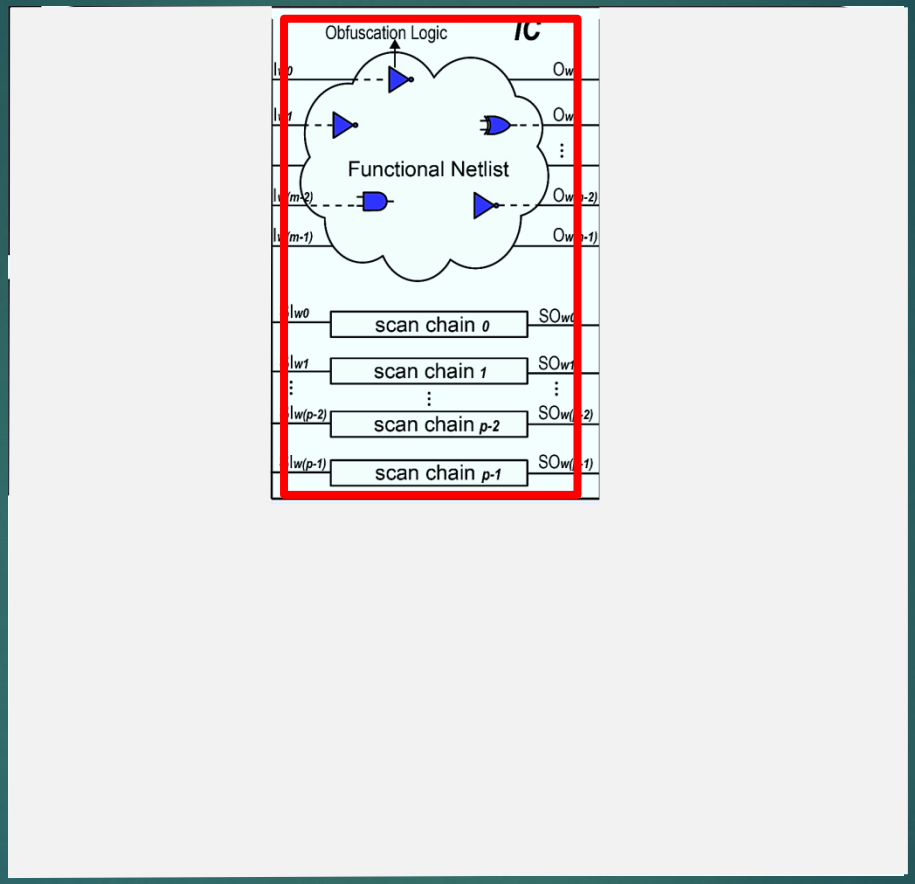
**IP owner can verify the uniquely encrypted functional data logging sequence in the data base**

***FK*$_e$ will not be released to out-of-spec devices**

1011000111000011000010100110001…

# Security Analy. @ Fab Rev. Engr

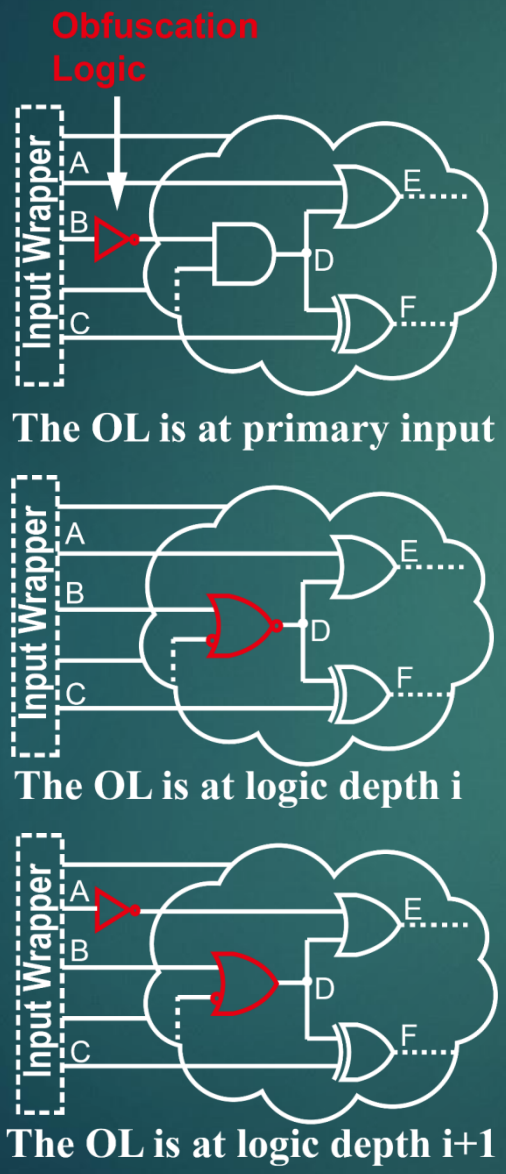





**Untrusted foundry can bypass DOST and extract the netlist in center**

# Security Analy. @ Fab Rev. Engr






**Untrusted foundry can bypass DOST and extract the netlist in center**

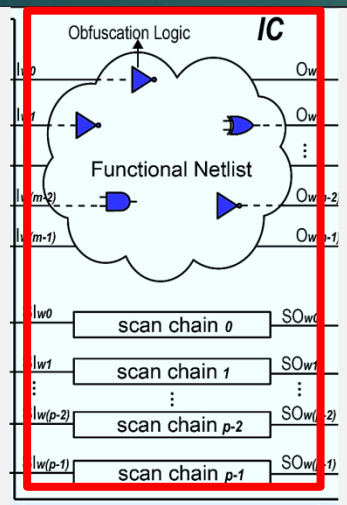
**As the IO Wrapper is configurable by the keys, we randomly invert the original netlist's IOs**

**Move the obfuscation inverters into larger logic depth**

**And even generating camouflaging inverters at other inputs and outputs**

# Security Analy. @ Fab Rev. Engr






**Even DOST is removed, Obfuscation Logic still exists**

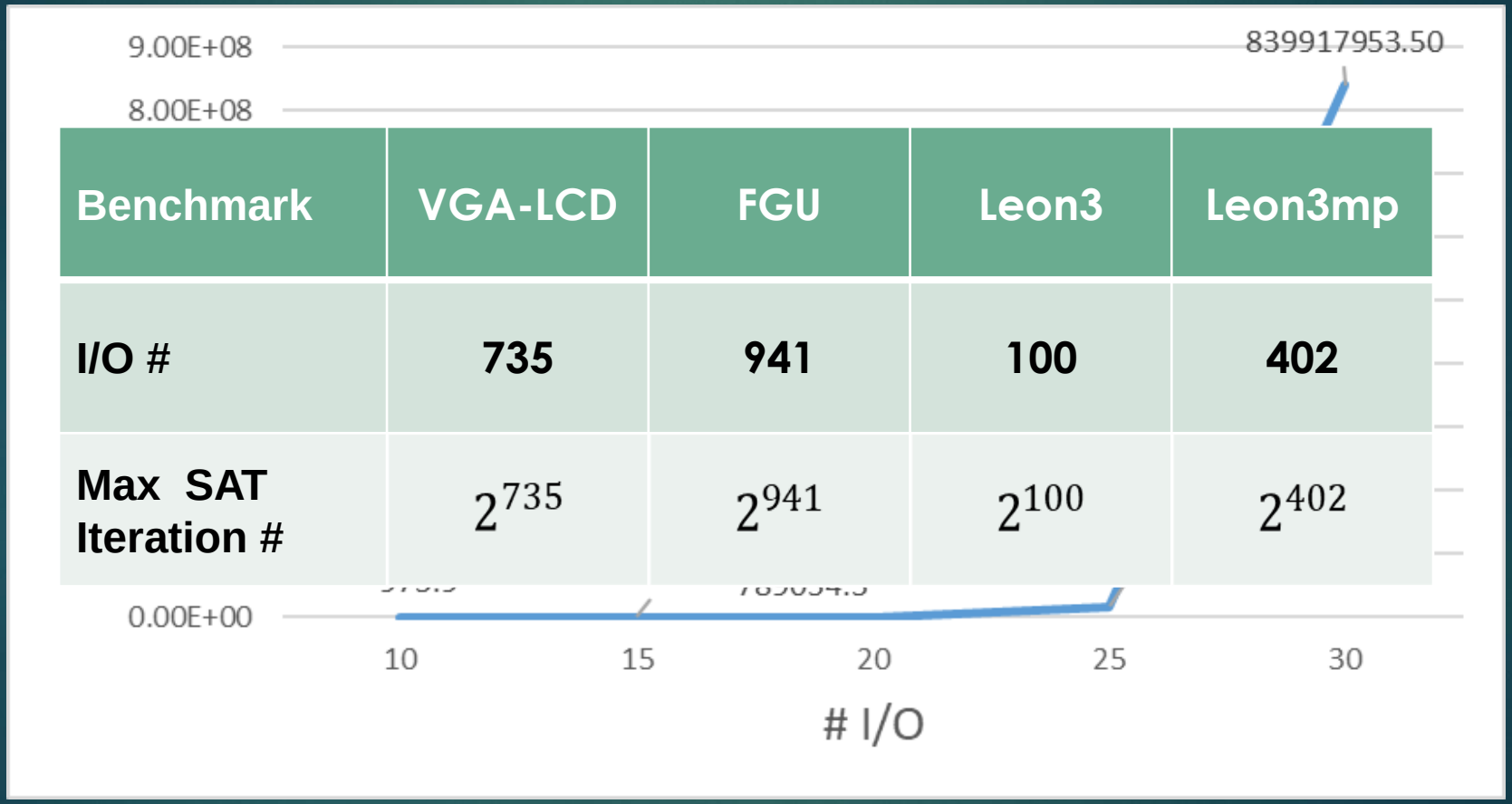
**The brute force attack probability is $1/2^{mn}$**

# Security Analy. @ Fab Rev. Engr



- SAT Analysis Difficulty for Obfuscation Identification

| Benchmark | VGA-LCD | FGU | Leon3 | Leon3mp |
|---|---|---|---|---|
| I/O # | 735 | 941 | 100 | 402 |
| Max SAT Iteration # | $2^{735}$ | $2^{941}$ | $2^{100}$ | $2^{402}$ |




The average iteration count by randomly selecting keys

# Conclusion



## Comparing with Existing Secure Scan Solutions

| Metrics | DOST | CSST [7][8] | Hardware Metering [4] | Logic Barrier [17] |
|---|---|---|---|---|
| Area Overhead | Extra RO-based PUF, | Extra RSA module | tra FSM logic and PUF (low-medium) | Extra reconfigurable-logic barriers for IOs, lookup table, and PUF (high) |
| Security during Production Tests | takes places after all tests | | ither structural or functi-l tests is conducted with tection. A Large volume f authentication takes place before all tests. | Neither structural or functi-onal tests is conducted with protection. A Large volume of authentication takes place before all tests. |
| Overproduced IC Deactivation | Yes | | No. Foundry can roduce ICs by claiming wer (than the original) yield. | No. Foundry can overproduce ICs by claiming lower (than the original) yield. |
| Defective IC Deactivation | Yes | | No | No |
| Out-of-spec (speed) IC Deactivation | Yes | No Speed binning takes | No | No |
| Extra Work Load for DFT Engineers | pattern/response generation | response generation for | —- | —- |
| Data Exchange Volume between IC Designer and Test Facilities | 3 Kes, result checker logging sequence. | All test responses, test and activation keys for each IC. | —- | —- |

**Both structural and functional tests are conducted with protection with extra data volume equals to 1 to 2 scan IOs.**

**Data security against flushing, resetting and FSR hash function attacks.**

# Thank You!