# Hardware & Embedded Security

## Part 2

Academic Year: 2024-2025

Prof Daniele Rossi


Via G. Caruso 16, room B-1-03


daniele.rossi1@unipi.it


050 221 7611

1

# Detection of Counterfeit ICs

Lecture 3 - DR



2

# Brief Outline

- Counterfeit detection
  - Basics on Hardware metering
  - Path delay fingerprinting for recycled IC detection
  - On-chip Ring Oscillators based sensor for recycled IC detection



3. • Limitation of standard electric tests: they require time (not scalable), sophisticated equipment
• Researchers produced a few alternatives. Hardware metering is one. Characterize a chip to provide unique fingerprints.

# Hardware Metering for Counterfeit Detection

- Is a set of security protocols that enable the design house to achieve post-fabrication control over their ICs
- Provides a way to **uniquely fingerprint** or tag each chip and/or each chip's functionality
- It is possible to distinguish between the different chips manufactured by the same mask
- First introduced in 2005 To uniquely tag each ICs functionality
- Example: **On-chip Aging Sensor**, **Physically Unclonable Functions (PUFs)**
- Similarly, to test for recycled IC detection, **on-chip sensors** can be adopted → this allows designer to increase accuracy and reduce test costs compared to standard rest procedures



4 Some techniques make use of on chip sensors that can help to detect counterfeit (recycled) components.

① First advantage of this approach

# Path Delay Analysis (I)

- **Path delay fingerprinting** can be adopted to screen recycled ICs **without** adding **extra hardware** in the design: since these recycled ICs have been used in the field, the **performance** of such ICs must have been **degraded** due to the impact of aging.
- Due to **process variation**, the delay distribution of the paths lies within the **specified range**, and the fingerprint of the new ICs can be generated during manufacturing test and stored in a secured database.
- Due to negative/positive bias temperature instability (NBTI/PBTI) and hot carrier injection (HCI), the path delays in recycled ICs will become larger

  → larger path delays indicate a higher probability of being an IC used for a long period of time in the field.



5

② Idea is using delay to identify counterfeit/recycled components. Delay can be effective, aging can affect propagation delay. But because of process variation, that's one thing that affects the delay of a chip too.

△

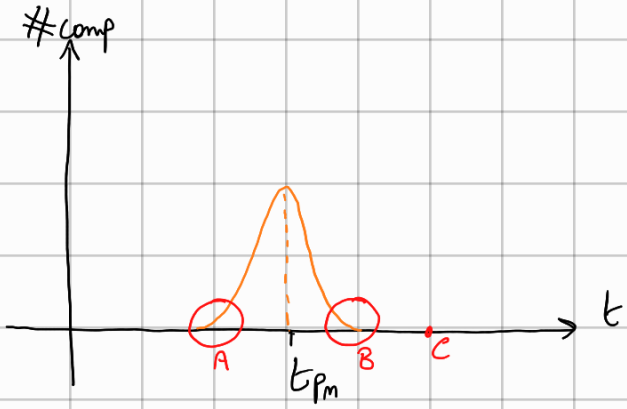
# Path Delay Analysis (II)

- In path delay fingerprinting approach, statistical data analysis is used to classify recycled (aging causes the delay variation) and new ICs (process variation causes the delay variation).
- Since the path delay information is measured during the manufacturing test process, no extra hardware circuitry is required for this technique.
- Note that no change is required in current well-established design and test flows.



6

Δ

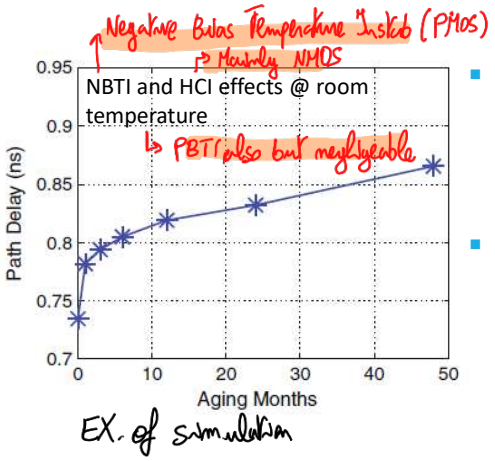



Time of prop. delay of the nominal chip

Problem: components falling in areas A, B are still new components. And if a component falls in B, you cannot properly tell if it is an aged lucky component, or a new unlucky one.
Of course if a $t_p$ falls completely outside of the distribution, we're sure it is a counterfeit.
So, what we could do is: select a bunch of fresh components, try to find an average of their behaviour and find a proper threshold for comparison.

- This is doable, but requires availability of golden models (components that are good). [SECOND DRAWBACK] [FIRST IS PROCESS VARIATION]

# Examples of Impact of Aging on Path Delays

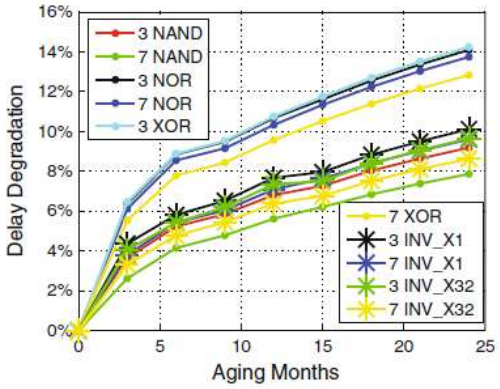



- Delay degradation of a randomly selected path of ISCAS'89 benchmark circuit s38417 when the circuit was driven with a **random workload** (random functional patterns are applied to the primary input).
- The degradation of the path used for 1 year is around 10% while if the circuit is used for 4 years, the degradation is about 17 %, indicating that most aging occurred at the early usage phase of the circuit.



7

# Examples of Impact of Aging on Different Gates

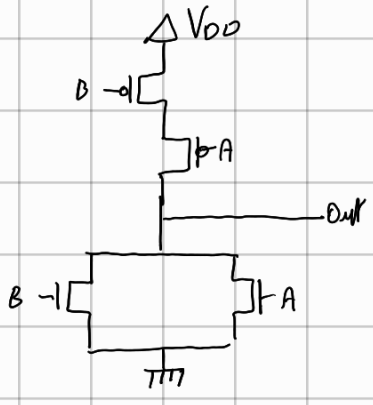



- Delay degradation of different chains, consisting of INVX1, INVX32, NAND, NOR, and XOR gates, after 2 years of aging.
- Different chains age at slightly different rates, which depends on the structure of the gates:
  - The XOR gate chain has the highest aging rate which will help to select the paths for fingerprinting.

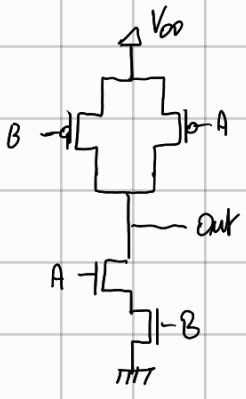


8

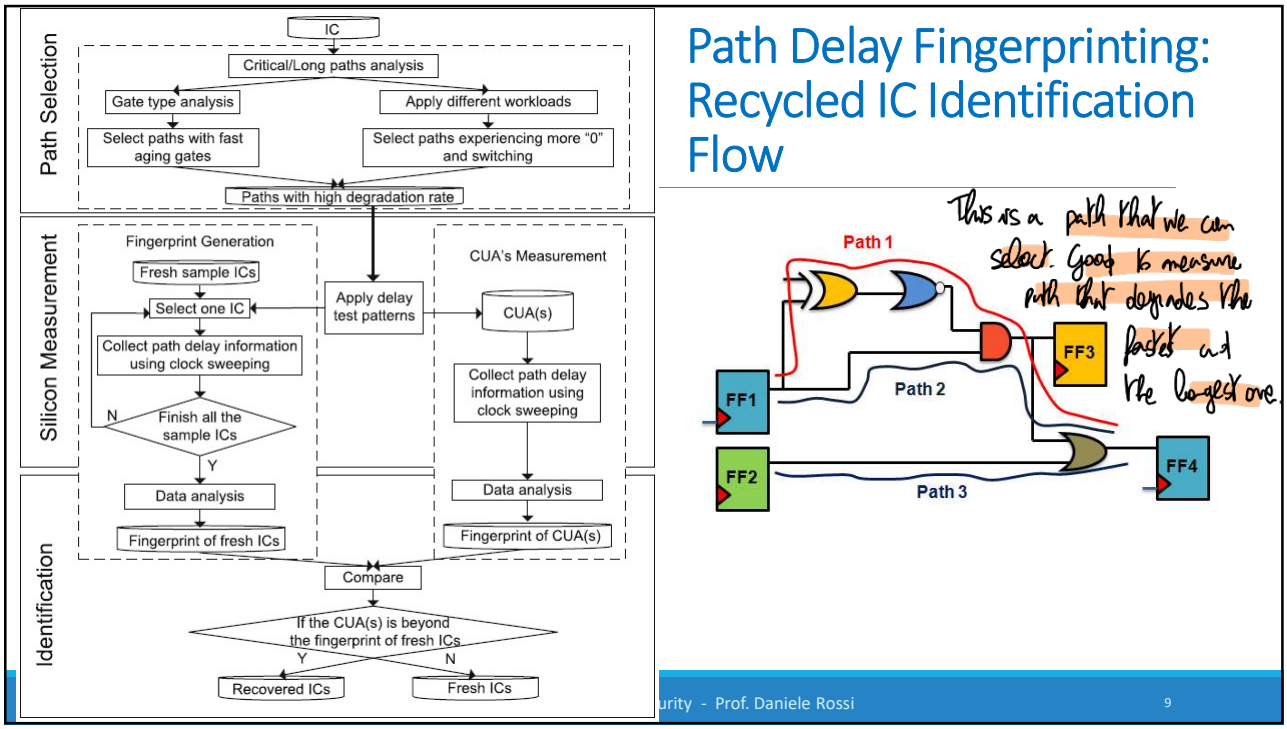
The XOR has the highest degradation, much more than the NAND! Even NOR is good. It is good to select paths we expect to degradate more.




If we want to propagate a 1, current has to flow to the senses of PMOS. So we can expect a faster degradation in a NAND.



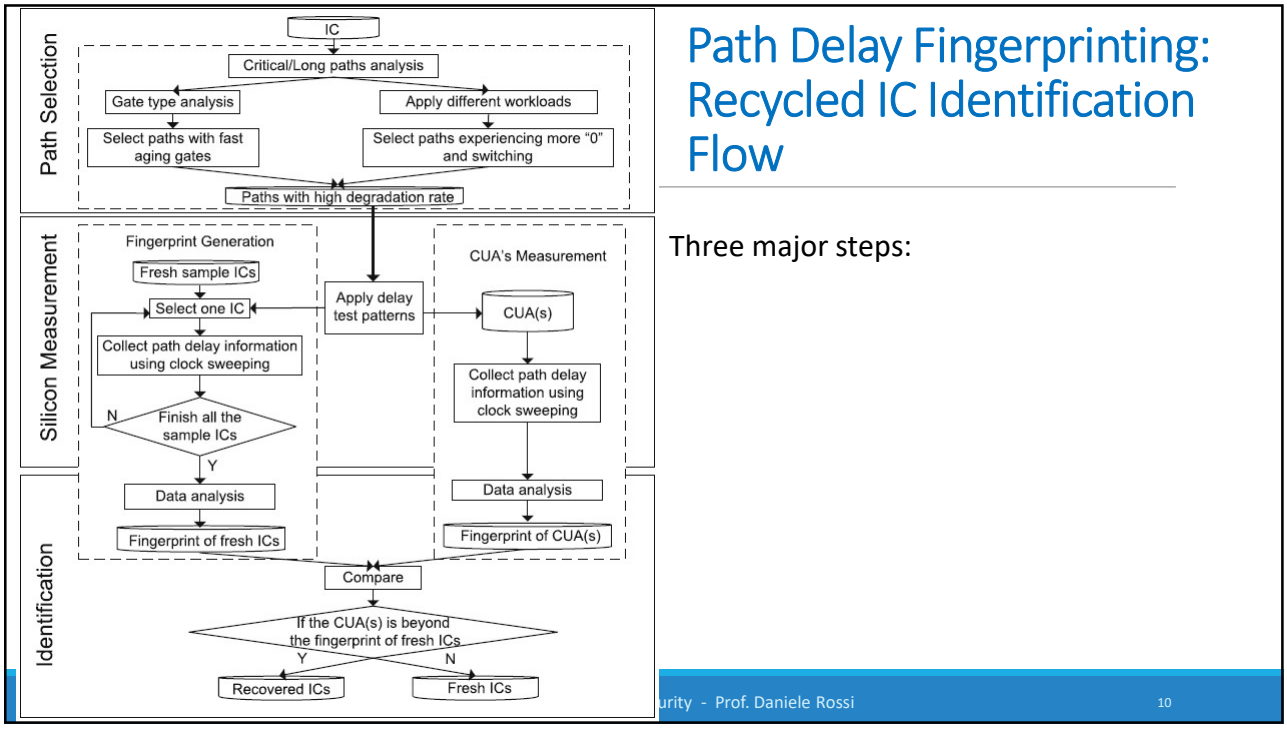

Here current has to flow through a senses of NMOS, that degrade less than PMOS.




# Path Delay Fingerprinting: Recycled IC Identification Flow



9 Idea: take the clock frequency until you see the path fail (so if a path is fastest or degrading and is the longest, you will sooner find that).

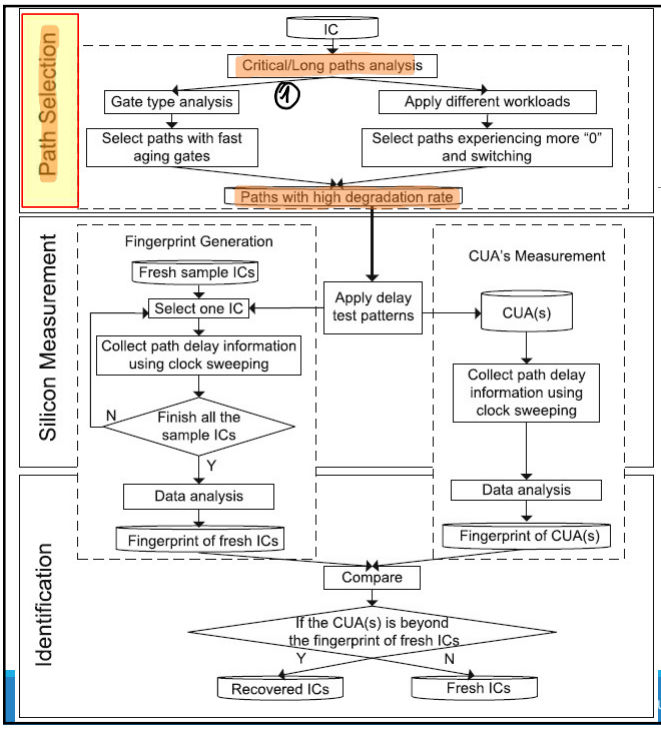



# Path Delay Fingerprinting: Recycled IC Identification Flow

Three major steps:



10




# Path Delay Fingerprinting: Recycled IC Identification Flow

Three major steps:

1. **Path Selection**: paths are selected for generating the fingerprints → the **paths with higher degradation rate** are selected. We select paths based on two criteria:

(i) those paths having **large number of XOR** gates

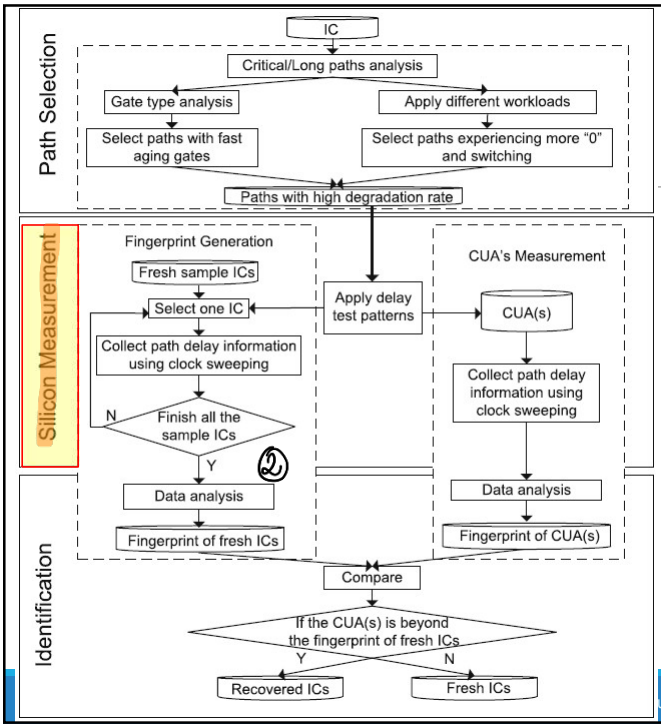
(ii) those with **more number of gates having "0"** at their inputs during a random workload (transistors degrades when they are ON, and pMOS transistors degrade faster than nMOS).

△

• Long paths ko! ①



11




# Path Delay Fingerprinting: Recycled IC Identification Flow

Three major steps:

① 2. **Silicon Measurement**: Using **clock sweeping** technique, the delay information of these paths are measured either during **manufacturing tests** or during **authentication** on a large sample of new ICs:

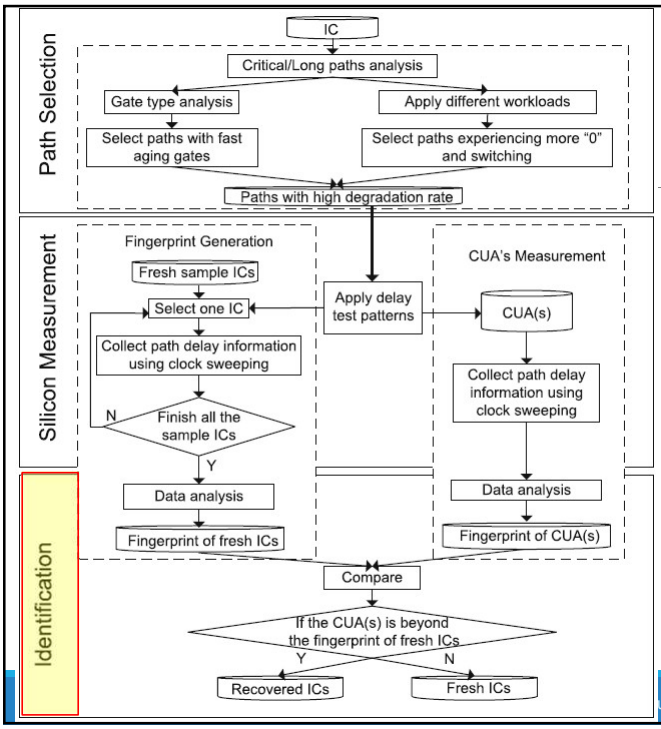
- We measure the delays for the **same paths** registered during manufacturing tests of ***circuits under authentication*** **(CUAs)**.
- The **measurement environment** should be controlled properly to keep the **temperature stable** as it may also impact the delay.



12

△ To switch a PMOS on, you need a 0 value. Otherwise for NMOS a 1.
If you have a majority of 0s, PMOSes are mostly on and one going to age more.

① Clock sweeping is used generally for those kind of measurement.
② Determination of fingerprints: we build golden model from chips we know are good. And we do the same for the CUA (circuit under auth.) and apply the same data analyses.




# Path Delay Fingerprinting: Recycled IC Identification Flow

Three major steps:

3. **Identification**: Once the path delays in all the new ICs are measured, **statistical data analysis** will be used to generate the **fingerprint**.

Two statistical data analysis methods can be used:

- simple outlier analysis (SOA), or
- principal component analysis (PCA).

If the CUA is outside of the set created by the new ICs, there is a high probability that the CUA is recycled.



13 ① We have fingerprints of fresh IC and CUAs. Fingerprint can be average of prop. delay. And when we compare. If comparison is not succesfull, recovered. If we were only considering propag. delay, we would also need safeguards against process variation.

# Clock Sweeping

- Clock sweeping technique proposed for identifying recycled ICs [r1] [but not only. Also to characterize prop. D. of components]
- This technique uses path delay information to create unique binary identifiers, and **does not require any area overhead** as it utilizes the common design or test processes:
  - This technique can be **applied to ICs already in the supply chain**
  - **No additional hardware** is necessary—there is no area, power, or timing overhead to the technique (of course you need to consider the time to run the technique)
- Clock sweeping is the process of **applying patterns to a path multiple times** with **different frequencies** to find a **frequency at which the path cannot propagate its signal**
- By observing the frequencies at which the path can and cannot propagate its signal, we can measure the **delay of the path**

[r1] N. Tuzzio, K. Xiao, X. Zhang, M. Tehranipoor, A zero-overhead ic identification technique using clock sweeping and path delay analysis, in *Proceedings of the Great Lakes Symposium on VLSI, ser. GLSVLSI '12* (ACM, New York, 2012), pp. 95–98. [Online], Available: http://doi.acm.org/10.1145/2206781.2206806

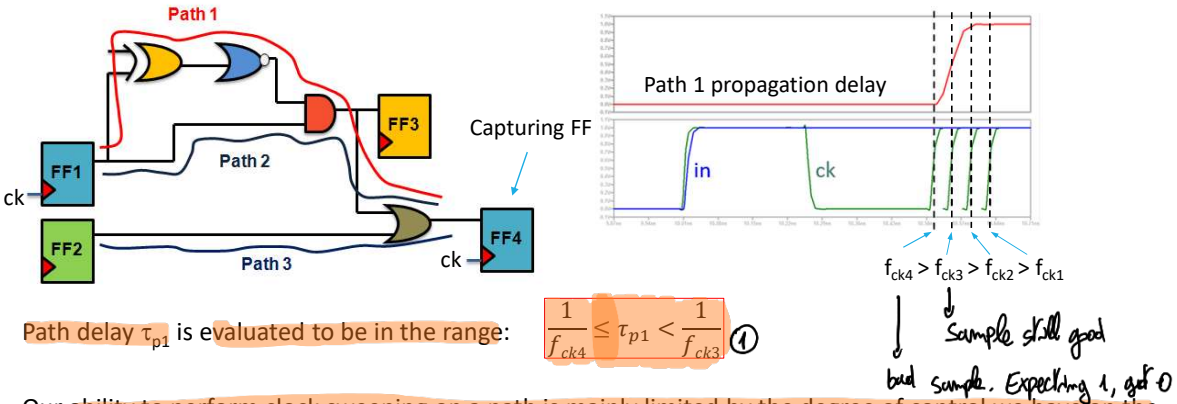


14

Clock sweeping is also done for speed binning.

Assume you have access to clock of your system and to registers as input and output of port. We can apply inputs to registers, trigger clock, see signal propagate and then trigger output clock. We know expected outputs. We apply inputs that activate longest paths. We can verify wether expected output = actual output. We can only say that prop. delay is shorter than clock period. Then we can reduce it and move to higher frequencies.

# Clock Sweeping: Explicative Example




- Path delay $\tau_{p1}$ is evaluated to be in the range: $\frac{1}{f_{ck4}} \leq \tau_{p1} < \frac{1}{f_{ck3}}$ ①
- Our ability to perform clock sweeping on a path is mainly limited by the degree of control we have on the **clock that controls the capturing memory elements** (i.e., the flip-flops).

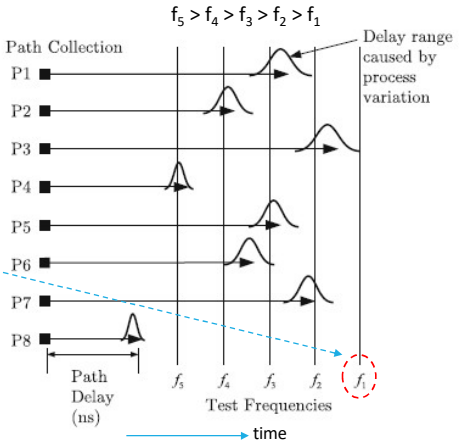


15

① In first order approx. neglect setup time.
→ But doesn't require additional hw and equipment you already have for standard tests.

# Clock Sweeping: Example (I)

- Example**: paths P1 through P8** are paths in the circuit which end with a capturing flip-flop
- Each of the eight paths can be swept (tested) at the frequencies f1 through f5
- All paths are able to propagate their signal at **f1**, as this is the rated frequency of the IC design
- However, at **f2**, the path **P3 will usually fail** to propagate its signal, whereas at frequency **f3**, it will **always fail** to propagate its signal.




[r1] N. Tuzzio, K. Xiao, X. Zhang, M. Tehranipoor, A zero-overhead ic identification technique using clock sweeping and path delay analysis, in *Proceedings of the Great Lakes Symposium on VLSI, ser. GLSVLSI '12* (ACM, New York, 2012), pp. 95–98. [Online], Available: http://doi.acm.org/10.1145/2206781.2206806

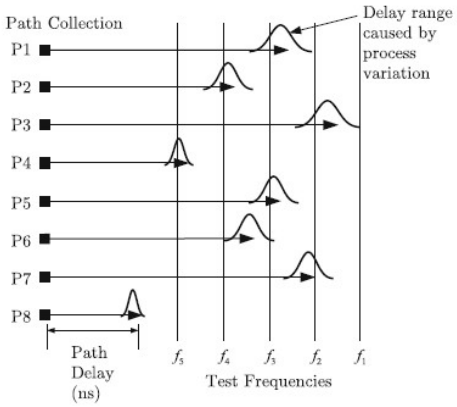


16

8 different paths with their prop. delay considering process variation.

# Clock Sweeping: Example (II)

- Path **P8** will succeed in propagating its signal at all five clock frequencies in this example, because it is **too short to test with clock sweeping**
- All of the paths have some number of frequencies they will pass at, some they may fail at, and some they are guaranteed to fail at
- Process variations change which frequency each path will fail at between different Ics.




[r1] N. Tuzzio, K. Xiao, X. Zhang, M. Tehranipoor, A zero-overhead ic identification technique using clock sweeping and path delay analysis, in *Proceedings of the Great Lakes Symposium on VLSI, ser. GLSVLSI '12* (ACM, New York, 2012), pp. 95–98. [Online], Available: http://doi.acm.org/10.1145/2206781.2206806



17

# Comments on & Limitations of Clock Sweeping

↑ if you have a large number of components and paths to measure ①

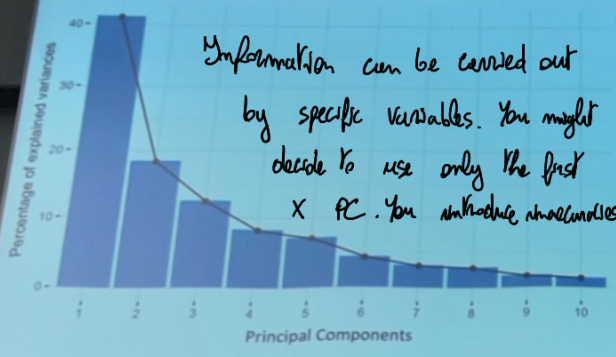
- The dimension of the collected data can be large (several hundreds), even if we collect a small percent of long, or critical paths → it is necessary to reduce the dimensions to create the fingerprint → for example, **Principle Component Analysis** (PCA) [r2], one of the popular multivariate analysis methods, can be used to reduce this large data dimensions
- The detection rate of recycled ICs can be very high (**> 99%**) if they have aged long enough (e.g., 6 months or longer)
- The detection rate reduces significantly when the ICs used shorter period of time. For example, the rate can reduce down to **~ 70%** when the ICs are used only for **1 month**
- The test can be **time consuming** (need to identify long/critical paths and to post-process the collected data) and requires specialised test equipment to apply test patterns and collect the results at **multiple clock frequencies**. Availability of multiple clock frequencies can be a limitation.

[r2] S. Wold, K. Esbensen, P. Geladi, Principal component analysis. Chemom. Intell. Lab. Syst. 2(1), 37–52 (1987)



18 ① Because you don't know how IC has been used. You might want to measure a lot of different paths.

# Notes on PCA




Information can be carried out by specific variables. You might decide to use only the first X PC. You will reduce dimensionality.

- Principal components (PCs) are new variables that are constructed as linear combinations or mixtures of the initial variables.
- These combinations are done in such a way that the new variables (i.e., PCs) are uncorrelated and most of the information within the initial variables is squeezed or compressed into the first components.
- PCs will allow you to reduce dimensionality without losing much information → discarding the components with low information and considering the remaining components as your new variables.

- *An important thing to realize here is that the principal components are less interpretable and don't have any real meaning since they are constructed as linear combinations of the initial variables.*

# Any questions so far?

Note: When we run those kinds of tests we need to make sure that environment conditions are the same (ex. temperature)



19

Motivation to change approach to determine recycled: idea is integration of a kind of aging/performance sensor on a chip.

# Design for Anti-Counterfeit

- The detection of counterfeit ICs poses a significant challenge to the global electronic component supply chain due to the lack of efficient, robust, and low-cost detection and avoidance technologies
- Standard electrical and physical test defined to identify counterfeit ICs are usually characterized by excessive test time, high cost, and low confidence

  → there is a clear need for the development of alternative approaches that can be integrated into new components at very low costs and can enable fast detection of recycled ICs: **Design for Anti-Counterfeit (DFAC)**
- One of the **main shortcomings** of standard, available test procedures for recycled IC detection (like path delay fingerprinting) is that **they require data from** (large set of) **genuine ICs** and cannot be easily applied to analog/RF/mixed-signal devices

  → practical DFAC structures must enable easy counterfeit detection without the need for existing expensive test methods and/or genuine ICs.

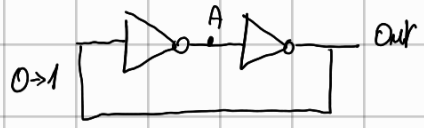


20

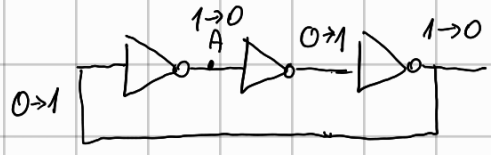
The base blocks we can use to determine counterparts are RING OSCILLATORS.

UP:

Let's start with 2 inverters:




Let's assume that at a given point, input switches from 0 to 1.
After some time, node A will switch from 1→0, and Out will switch from 0 to 1.
So after a while circuit moves to a new stable state, 1 in, 1 out.
This does not oscillate. If you have an odd # of inverters:




So, the output switching from 1→0 brings input back to 0 and starts with oscillation.

The oscillation frequency depends on the propagation delay of the inverters.
RET

# Aging Effects Analysis for Recycled IC Detection

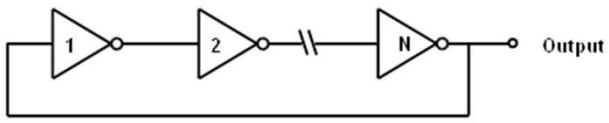
- Since recycled ICs have been impacted by these aging effects when used in the field, the circuit parameters of recycled ICs would be different from those of new ICs
- If a **fast-aging sensor** was embedded into the circuit to help detect its usage, then recycled ICs could be identified → → **Ring Oscillators (ROs)** are good candidate DFAC circuit → **RO-based on-chip sensor** to detect recycle ICs
- According to the results shown in previous slides, **INVX1 with HVT** will be used to create the ring oscillators used to detect recycled ICs.



21

YR is about a cascading chain of inverters feedback. CALL UP

# RO Structure




- A ring oscillator RO has an **odd number** (**N**) of inverting stages connected in series with the output fed back to the input
  - The RO and related circuits are **fundamental building** blocks used as clock oscillators in computers and frequency generator phase locked loops in wireless communications
- An RO is also a fundamental circuit for **evaluating the intrinsic speed** of a CMOS logic process
- The frequency of oscillation is inversely proportional to the number of stages and the propagation delay times:

$$f_{osc} = \frac{1}{N\,(\tau_{LH} + \tau_{HL})} = \frac{1}{2N\tau_p}, \qquad \tau_p = \frac{\tau_{LH} + \tau_{HL}}{2}$$

ASSUMPTION: $\tau_p$ is same for all inverters



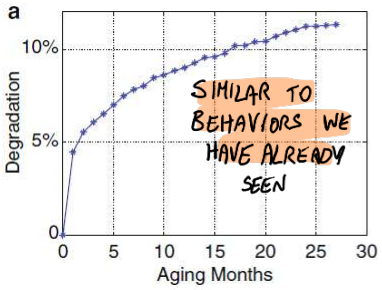
22

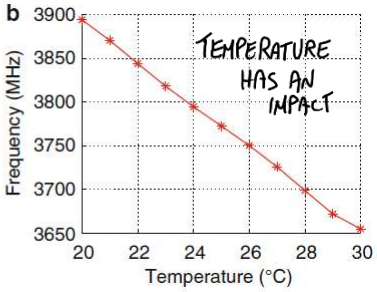
Time it takes for signal to propagate (frequency, so 2 switches)

- Minimum N is 3.
- This is a kind of performance sensor / aging sensor. If aging increases, propagation delay increases and oscillation freq. decreases.


# RO Oscillation Freq Variation with Aging

- Freq degradation of a 5-stage RO with HVT inverters after 27 months of aging



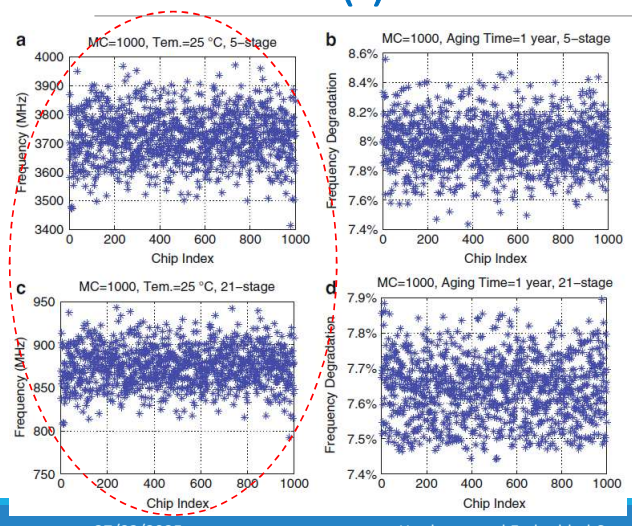

- **Fig. b**: the frequency of the 5-stage RO will decrease as the temperature increases, and frequency variation could be very large
- Note that increasing temperature can also increase circuit degradation

- **Fig. a**: The freq of the RO in a recycled IC will be lower than that in a new IC
- If there were no environmental or process variations, recycled ICs could be easily identified by measuring the frequency of the RO embedded in the circuit



23

# RO Oscillation Freq Variation with Process Variation (I)



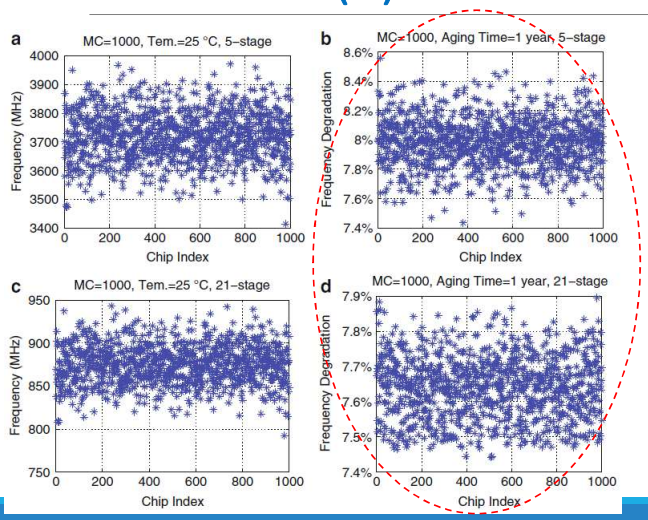

- Plots showing results from **Monte Carlo** simulation with 1000 circuit instances and including **10% variation** of process parameters (tox, L, Vth)
- RO's frequency can vary as much as **20%** under process variations ①

You can simulate impact of process variation through the use of monte carlo simulations. You have several parameters over which you define parameters distributions ($T_{ox}$, L, $V_{TH}$...) and pick values in the distribution and simulate.



24 ① How can we differentiate impact of process variation for delay?

# RO Oscillation Freq Variation with Process Variation (II)




- Plots showing results from Monte Carlo simulation with 1000 circuit instances and including 10% variation of process parameters (tox, L, Vth)
- RO's frequency can vary as much as 20% under process variations.
- In addition, **process variations impact the aging rate of the RO**:
  - The frequency degradation of the 1000 chips varies around 8% for 1 year of aging
  - This frequency shift caused by the aging effects in recycled ICs can help separate them from those caused by process variations in new ICs



25

# Properties of an On-chip Aging Sensor (ideally)

- The main objectives in designing an aging sensor to detect recycled ICs are:
  - the **sensor must age at a very high rate** to help detect ICs used for a short period of time, Very accurate
  - the sensor must experience **no aging during manufacturing testing**,
  - the impact of **process variations and temperature** on the RO-based sensor must be **minimal**, (we can ignore impact of temperature because it will be negligeable)
  - the sensor must be resilient to attacks, and finally,
  - the measurement process must be done using **low-cost equipment**, and be **very fast and easy**



26

# Properties of an On-chip RO-based Aging Sensor (II)

- Aging effects can slow down the frequencies of ROs embedded into the ICs
- With an embedded RO, these recycled ICs can be identified based on their frequency, which will be lower than that of a new IC
- It does not require any memory element to store the usage time since it is hidden in the degraded RO frequency because of aging

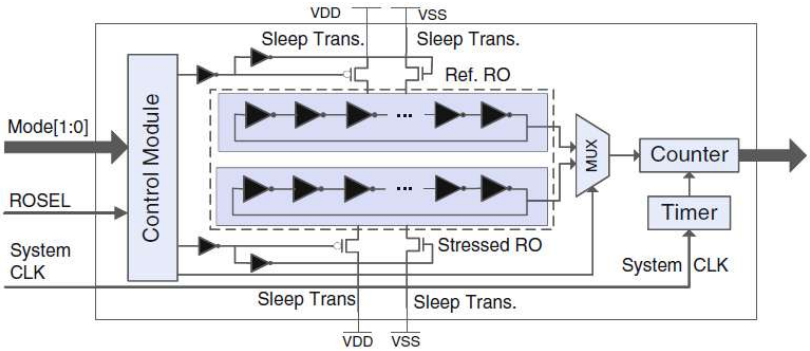


27

SOLUTION PROPOSED

# On-chip RO-based Aging Sensor (I)

Combating Die and IC Recycling (CDIR) Sensor [r3]




[r3]: X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ICS using fingerprints from a light-weight on-chip sensor," in Proc. IEEE Design Autom. Conf., Jun. 2012, pp. 703–708

- RO-based sensor is based on the aging differences between 2 ROs to record the usage time of ICs.
- It does not require any memory element to store the usage time since it is hidden in the degraded RO frequency because of aging: "**self-referencing**" concept

→ Results from the 2 embedded ROs are compared to detect prior IC usage



28

2 main components are 2 ring oscillators.

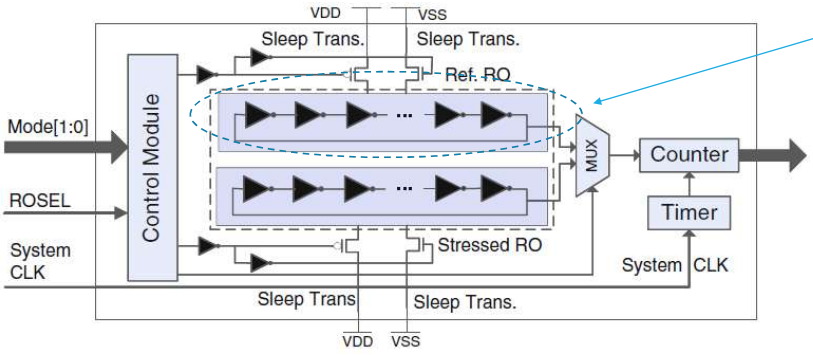
- This component is "self referencing": we don't need a golden model.

Let us try to define why this works:

* Remember: circuits in the same area show pretty much same process variation.
  - ↳ We have a Reference and Stress RO. That's why we have self-referencing. Reference is embedded within the sensor.
  - ↳ We design cards to have 1 of them continuously stressed, the other not, so when comparing degradation, we compare their frequencies to assess difference. Since ROs are very close to each other, they undergo same kind of process variations; this applies also to temperature. We can expect temperature in that area to be the same. Temperature and process variation impacts them in the same way.

# On-chip RO-based Aging Sensor (II)

Combating Die and IC Recycling (CDIR) Sensor




- The first RO is called the reference RO and is designed to age at a slow rate.

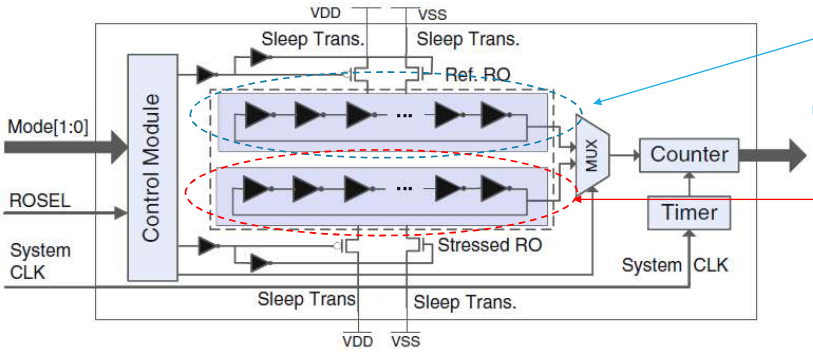
Ideally not age at all



29

# On-chip RO-based Aging Sensor (II)

Combating Die and IC Recycling (CDIR) Sensor



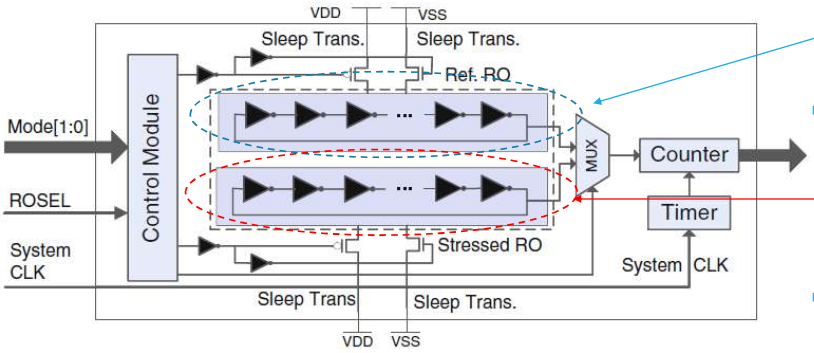

- The first RO is called the reference RO and is designed to age at a slow rate.
- The second RO (identical to the first) is referred to as the **stressed RO**, and it is designed to age at a much faster rate than the reference RO

any time in which circuit operates normally.



30

# On-chip RO-based Aging Sensor (II)



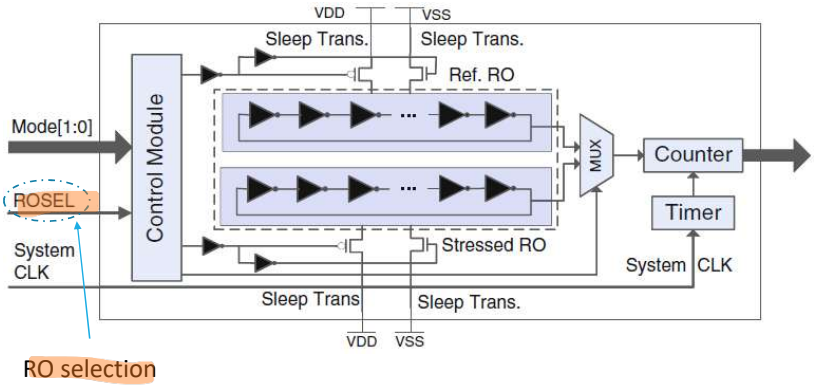

- The first RO is called the reference RO and is designed to age at a slow rate.
- The second RO (identical to the first) is referred to as the stressed RO, and it is designed to age at a much faster rate than the reference RO
- The use of **2 ROs** allows us to separate the aging effects from process/environmental variations

- Number of inverter stage depends on the max freq of the counter (e.g., count fmax = 1 GHz → 21 stages in 90nm tech) ex.



31

# On-chip RO-based Aging Sensor (III)

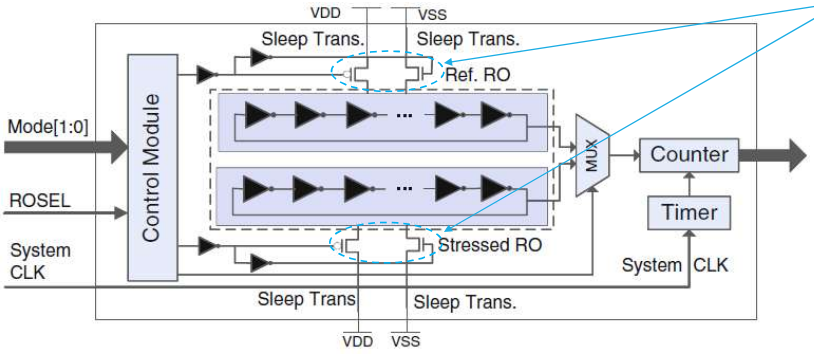



- The **counter** measures the cycle count of the two ROs during a pre-specified time period, which is controlled by the **timer**.
- **System clock** is used in the timer to minimize the measurement period variations due to circuit aging
- The **MUX** selects which RO is going to be measured, and is controlled by the ROSEL signal



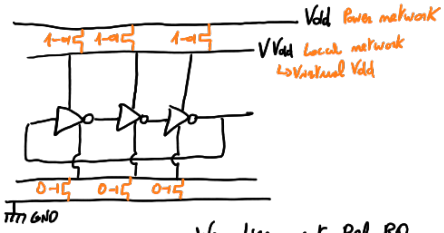
32 Counter will count number of rising or falling edges in a specific time interval. This # depends on frequency of oscillation. Timer enables and disables clk during measurement.

# On-chip RO-based Aging Sensor (IV)




- Sleep transistors are used to connect/disconnect the ROs to the power supply in the RO-based sensor;

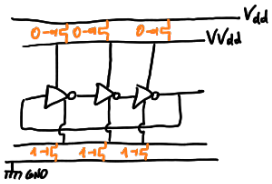
Similar to power gating idea.



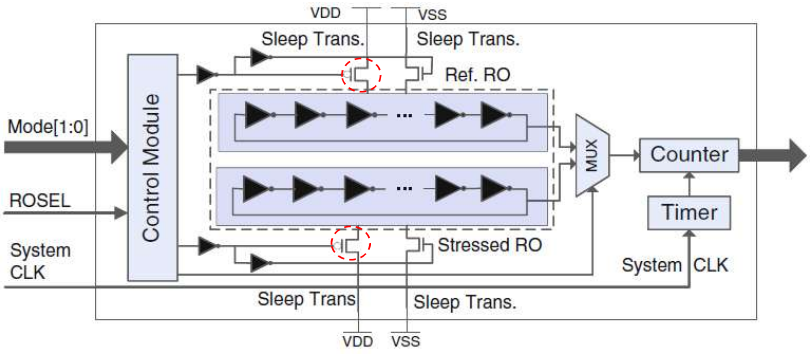

We disconnect Ref. RO.



33 While for the stressed RO we do the opposite:




# On-chip RO-based Aging Sensor (IV)

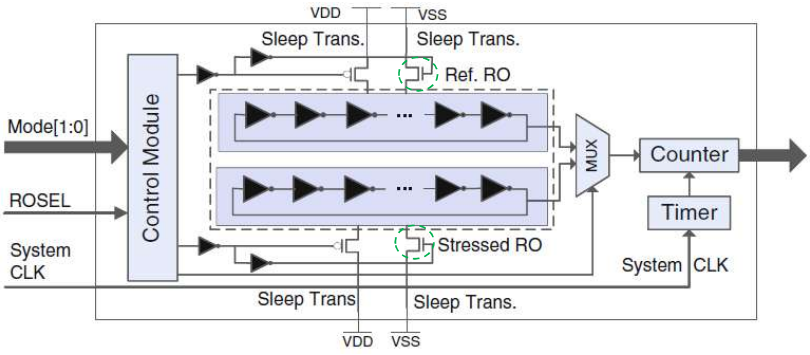



- Sleep transistors are used to connect/disconnect the ROs to the power supply in the RO-based sensor;
- PMOS sleep transistors control the connection between VDD and the inverters



34

# On-chip RO-based Aging Sensor (IV)

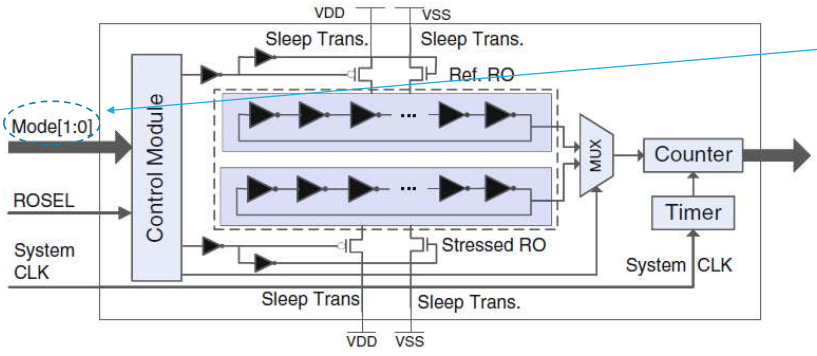



- Sleep transistors are used to connect/disconnect the ROs to the power supply in the RO-based sensor;
  - PMOS sleep transistors control the connection between VDD and the inverters
  - NMOS sleep transistors control the connection between VSS and the inverters.



35

# On-chip RO-based Aging Sensor (V)



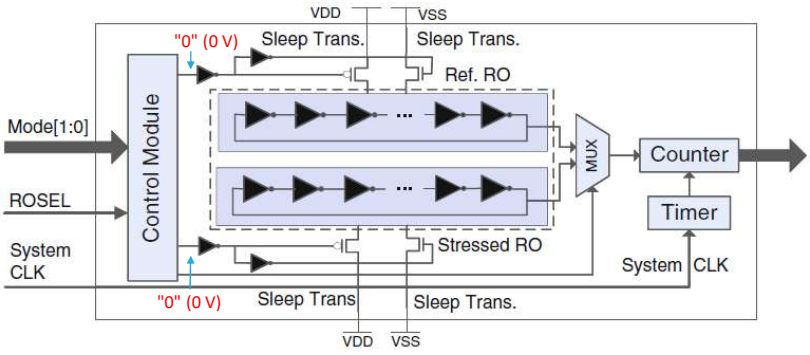

- Three modes of operation controlled by *Mode* signal



36

# On-chip RO-based Aging Sensor (V)

(VSS: groud, 0 V)




- Three modes of operation controlled by *Mode* signal

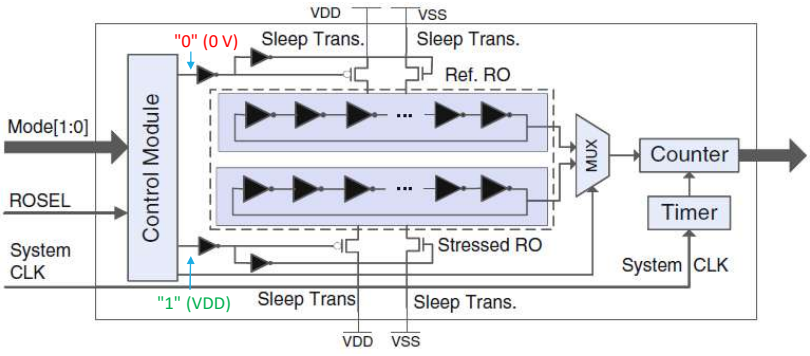
1. When the IC is in **manufacturing test mode**, both the Reference RO and Stressed RO will be disconnected from the power supply and experience no aging (sleep transistors are OFF).

This mode only lasts a short time, depending on the IC test procedures.



37

# On-chip RO-based Aging Sensor (VI)



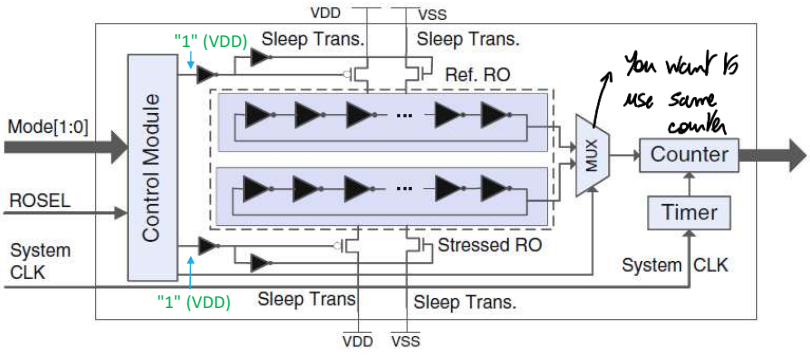

2 . When the IC is in normal **functional mode**, the Ref RO will be disconnected from VDD and VSS, but the Stressed RO will be connected to power supply and will age

→ the frequency of the Stressed RO will drop while the Reference RO will not change very much.



38

# On-chip RO-based Aging Sensor (VII)



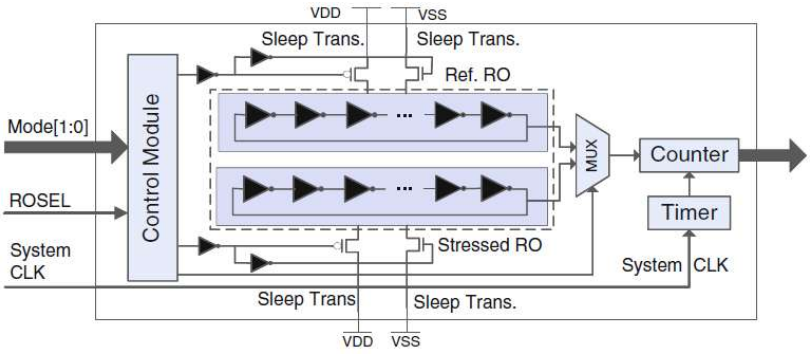

3 . When the IC is in **authentication mode** (i.e., when an IC is taken from the market, and its authenticity is to be verified), both the Reference RO and Stressed RO will be gated on by connecting to the power supply.

The timer and counter will be enabled to measure ROs' cycle count and the ROSEL signal will select which RO to measure.



39 You store the counted values you measured to check.

# On-chip RO-based Aging Sensor




**Exercise**: Design the additional logic networks to:

- Enable the Timer and the Counter during Authentication only
- Reset the Counter and the Timer after the each of the two freq measurement operations
- Make any assumptions you deem necessary



40 Is this robust enough against attacks? How can you tamper it? You could use memory to store values, but memory can be tampered with. Also, you would not be safe against temperature variations. Plus, overhead of this is absolutely negligible.

# On-chip RO-based Aging Sensor: Recap (I)

- The three modes of operation ensure that
  - (i) the frequency difference between the Reference RO and Stressed RO will be larger over time since the Reference RO cannot be gated on alone, and
  - (ii) it is extremely difficult for adversaries to force the RO-based sensor to operate in authentication mode when it is supposed to be in its normal functional mode, which would eliminate the aging difference.

    → The only method to do that would be to modify the original RO-based sensor module, which is impossible during a simple recycling process



41

# On-chip RO-based Aging Sensor: Recap (II)

- The **inverters** of the Reference RO and the Stressed RO are placed **next to each other physically**, designed as a single small module → the process and environmental variations between them should be very small
- In a new IC, the frequency difference between the Reference RO and the Stressed RO would be within a certain small range
- In a recycled IC, the Stressed RO will have suffered aging from its own oscillation, since the chip has been working in normal functional mode for a long time



42

# On-chip RO-based Aging Sensor: Recap (III)

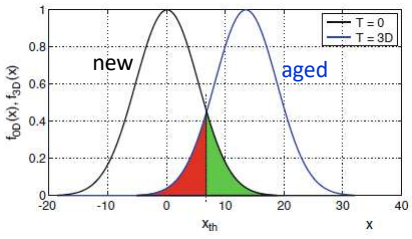
- The **Reference RO** will not have experienced as much aging since it was **gated off** → the **frequency difference** between the Reference RO and the Stressed RO will grow **larger** as the chip operates longer
- If the frequency difference is outside of the new ICs' frequency difference range considering process variations, it can be concluded with high confidence that the CUT was recycled from used boards
- The area overhead of the RO-based sensor is negligible when compared to the millions of gates in modern ICs. Power consumption is also limited to that consumed by the Stressed RO in the RO-based sensor





# Misprediction Rate

- Misprediction rate: recycled ICs identified as new ($\Delta_1$), and new ICs identified as recycled ($\Delta_2$)




Two distribution functions of the new and aged ICs having 21-stage ROs (aged for 3 days with process variation).
x-axis represents the frequency differences between the two ROs ($f_{diff}$)

$f_{0D}(x)$: distribution function of oscillation freq difference for new IC

$f_{3D}(x)$: distribution function of oscillation freq difference for aged (recycled) IC

- The overlap area represents the misprediction rate for identifying new or recycled ICs
- The decision threshold should be the point $x_{th}$ where both distributions intersect each other

$$\Delta_1 = \int_{-\infty}^{x_{th}} f_{nD}(x)dx \qquad \Delta_2 = \int_{x_{th}}^{\infty} f_{0D}(x)dx$$

**Misprediction rate = $\Delta_1 + \Delta_2$**

$f_{0D}$ and $f_{nD}$ corresponds to the distribution of frequency differences for new ICs and ICs with n days of aging, respectively

# Attack Analysis (I)

- Counterfeiters are continuously improving their techniques through experience → it is of the utmost importance to analyze all of the possible attacks on these RO-based CIDRs
- **Removal/Tampering attacks**: It is fairly impossible for the counterfeiter to replace the stressed RO with a new one or to tamper with the stressed/reference RO in order to match their frequency.
  - If we assume that a removal or tampering attack is possible, then the counterfeiter must remove the old package and then again repackage and remark it according to its original specifications: removal and then repackaging may not be cost effective to the counterfeiters → it is unlikely to be used in practice



45

# Attack Analysis (II)

- Age Reference RO: counterfeiter may try to **intentionally age the Reference RO** to mask the difference between the ROs → counterfeiter might attempt to force the RO-CDIR to work in authentication mode for a period of time under accelerated stress conditions (e.g., burn-in)
- With the accelerated aging at the same time, the frequency difference between the Stressed RO and the Reference RO would shrink since both of them could asymptotically approach maximum degradation
- Burn-in is a very expensive process and the counterfeiter must have an expensive setup for that
- The primary incentive for counterfeiting is **cheap recycling**, not adding extra cost to the components → there might not be any motivation left for the counterfeiters when they are forced to add burn-in to their recycling process → this attack might not be feasible as there is **no cost incentive.**



46

# Additional References and Readings


- SAE, Counterfeit electronic parts; avoidance, detection, mitigation, and disposition, 2019. https://www.sae.org/standards/content/as5553c/
- IDEA, Acceptability of electronic components distributed in the open market. http://www.idofea.org/products/118-idea-std-1010b
- CTI, Certification for coutnerfeit components avoidance program, September 2011
- U. Guin, D. DiMase, M. Tehranipoor, Counterfeit integrated circuits: detection, avoidance, and the challenges ahead. J. Electron. Test. 30(1), 9–23 (2014)
- U. Guin, K. Huang, D. DiMase, J. Carulli, M. Tehranipoor, Y. Makris, Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain. Proceedings of the IEEE, 102(8), 1207–1228 (2014)
- U. Guin, D. Di Mase, M. Tehranipoor, A comprehensive framework for counterfeit defect coverage analysis and detection assessment. J. Electron. Test. 30(1), 25–40 (2014)
- U. Guin, M. Tehranipoor, On selection of counterfeit IC detection methods, in IEEE North Atlantic Test Workshop (NATW), May 2013
- U. Guin,M. Tehranipoor, D. DiMase, M. Megrdichian, Counterfeit IC detection and challenges ahead, in ACM/SIGDA E-NEWSLETTER, vol. 43(3), March 2013
- X. Zhang, K. Xiao, M. Tehranipoor, Path-delay fingerprinting for identification of recovered ics, in Proceedings International Symposium on Fault and Defect Tolerance in VLSI Systems, October 2012
- K. Huang, J. Carulli, Y. Makris, Parametric counterfeit IC detection via Support Vector Machines, in Proceedings International Symposium on Fault and Defect Tolerance in VLSI Systems, 2012, pp. 7–12




47

# Thank you!

# Any questions?



48