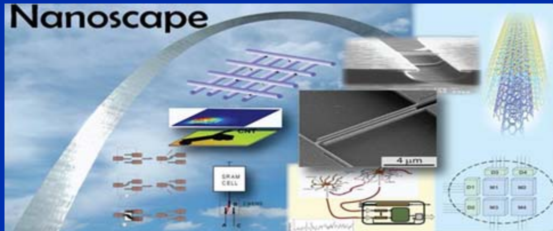
ScanPUF: Robust Ultralow-Overhead PUF using Scan Chain

Yu Zheng, Aswin Krishna, & Swarup Bhunia

Department of Electrical Engineering and Computer Science
Case Western Reserve University, Cleveland, OH, USA
Email: yu.zheng3@case.edu

CASE WESTERN RESERVE
UNIVERSITY
CASE SCHOOL OF ENGINEERING

ASP-DAC 2013



Outline

- Introduction
  - Fundamental of Physically Unclonable Function (PUF)
  - Existing PUFs
- Methodology of ScanPUF
  - Hardware architecture
  - Signature generation procedure
  - Design details
- Simulation and emulation results
  - Uniqueness and robustness
  - Aging effect
  - FPGA validation
- Discussion && Conclusion

The Fundamental of Physically Unclonable Function (PUF)

- Why PUF?
  - – The storage of digital key in non-volatile memory is vulnerable to invasive attacks.
  - – Highly tampering-resistance environment is expensive.
- What is PUF?
  - – Basically, a challenge-response protocol that exploits the inherent random variations in a manufacturing process to generate unique signatures.
- The advantages of PUF
  - – Random and vast challenge-response pairs.
  - – Only available when the chip is running.
  - – Cost is lower than key storage of tampering-resistance.

Existing PUFs

- Dedicated circuit structure
  - Ring-oscillator PUF (RO-PUF)
  - Arbiter PUF
  - Butterfly PUF
  - PE-PUF

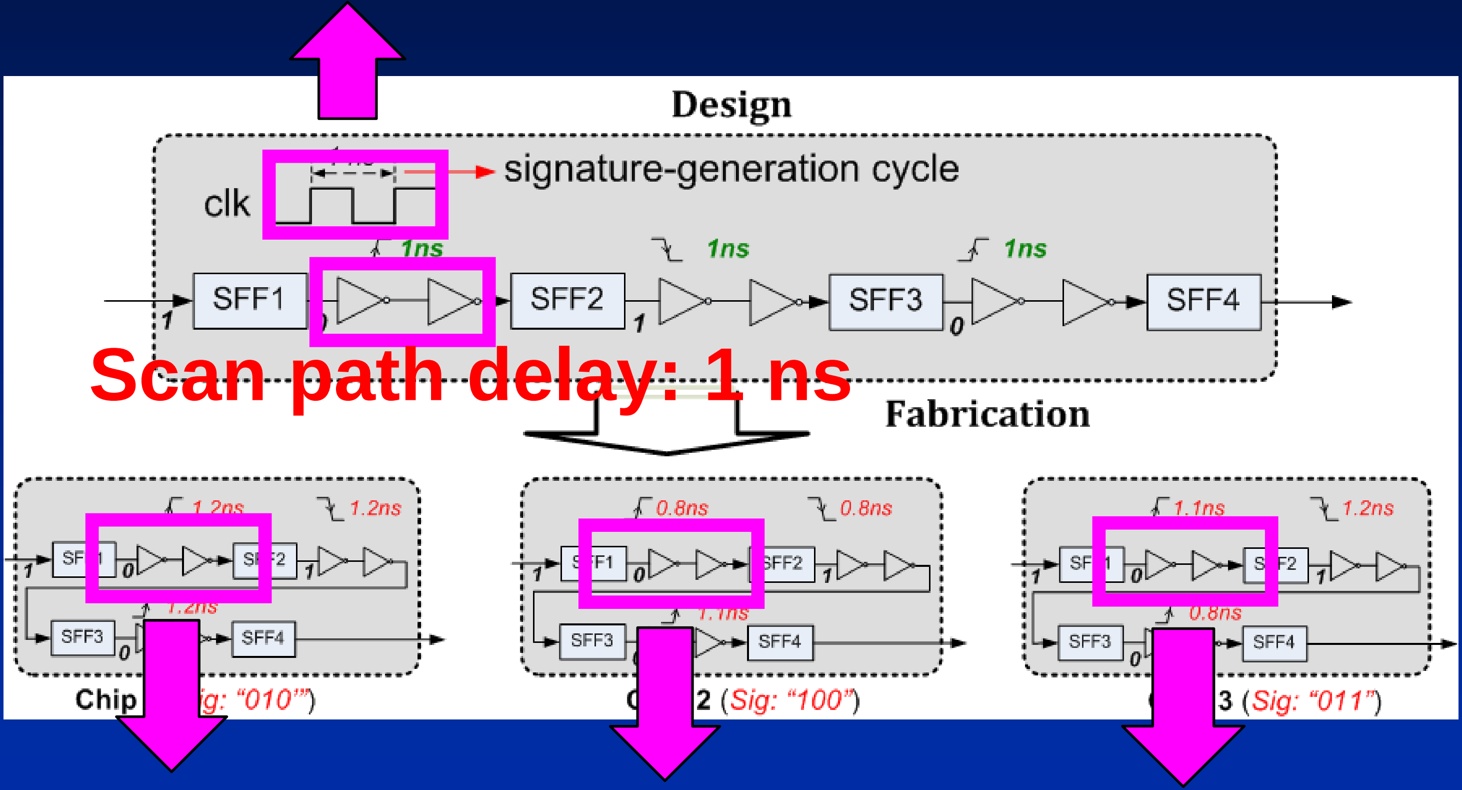
Non-negligible area overhead.

- Utilization the on-chip structure
  - SRAM PUF
  - MECCA
  - Intrinsic PUF

Limited challenge-response pairs or established on special structure.

Illustration of ScanPUF Realization

Signature generation cycle: 1 ns



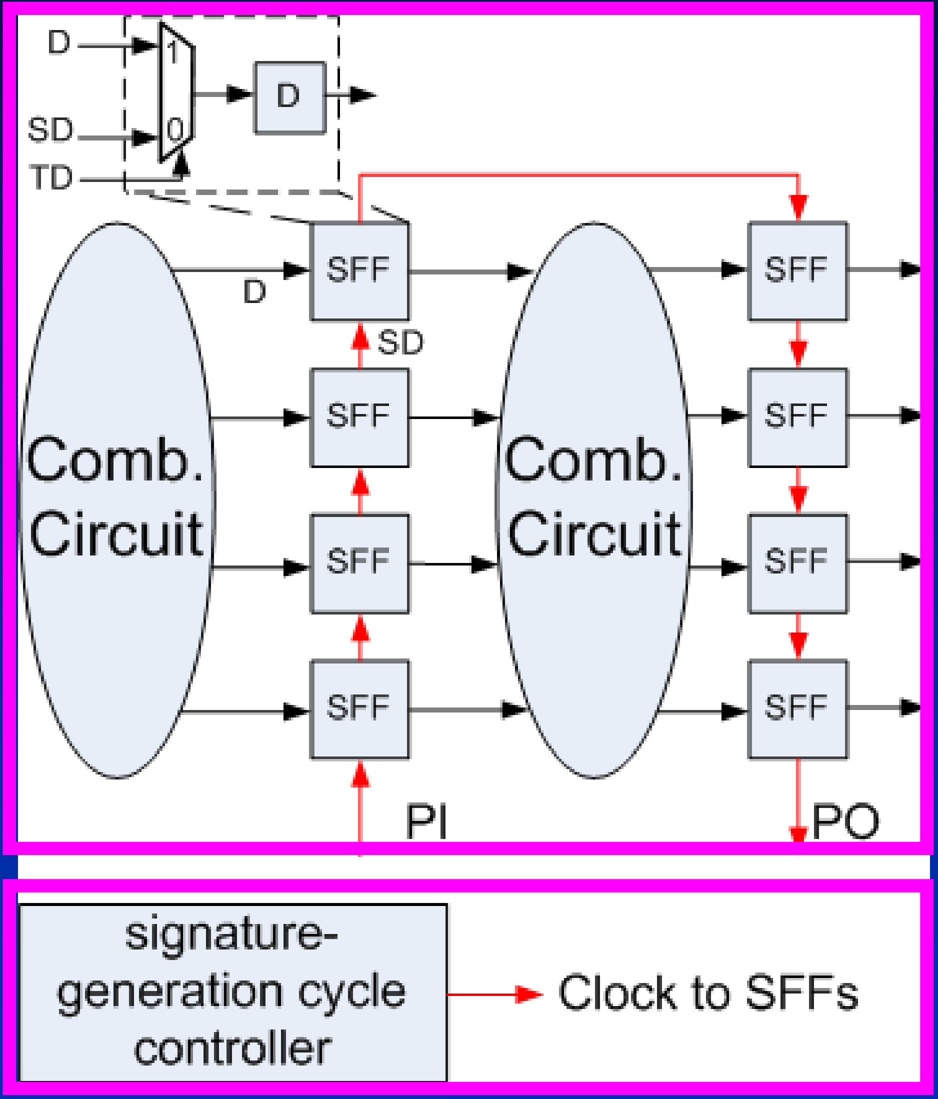
Scan path delay: 1 ns

1.2 ns → 0

0.8 ns → 1

1.1 ns → 0

The Architecture of ScanPUF



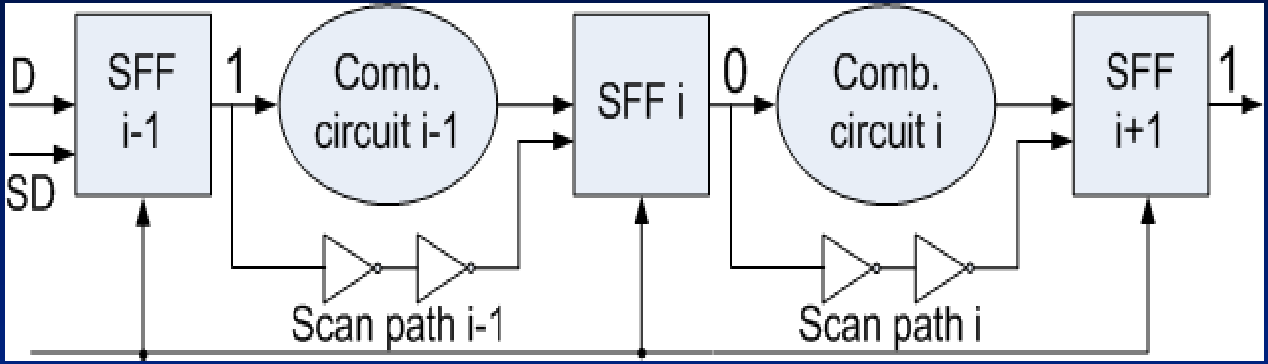
The structure of Scan Flip-flop (SFF) && scan chain

The inserted structure: Sig

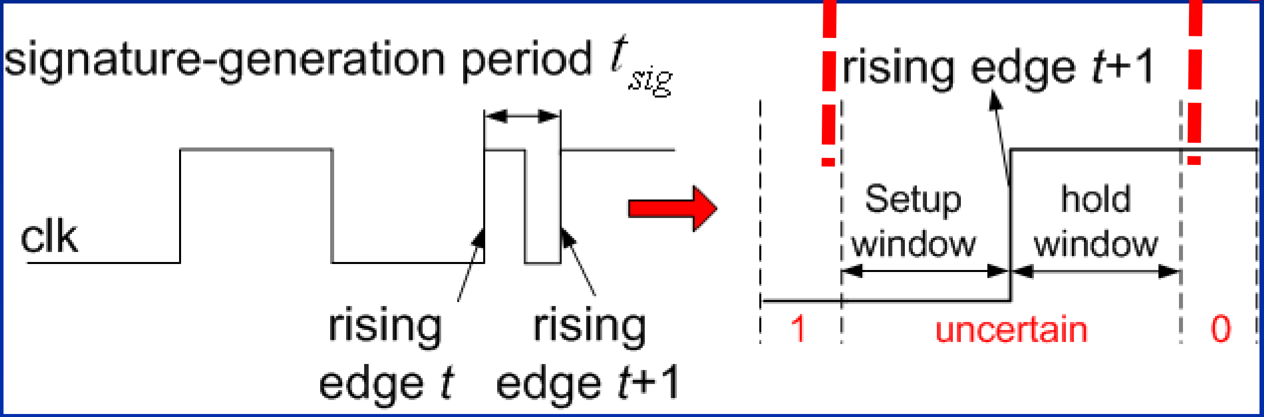
generation cycle controller

Signature Generation Illustration

Rising edge *t* +1: **1** **0** $0 \rightarrow 1$ **1**



1 uncertain 0



$$O_{i+1} = \begin{cases} 1 & if \quad t_{sig} > t_{clk2q,i} + t_{com,i} + t_{setup,i+1}, \; i = 0,1... \\ 0 & \qquad\qquad otherwise \end{cases}$$

Signature Generation Procedure

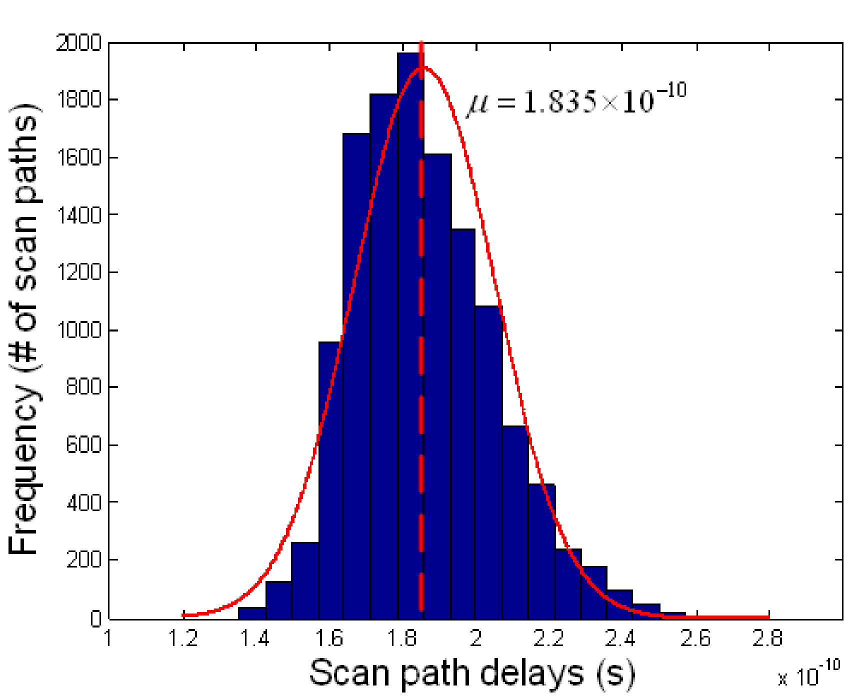
- Select the SFFs in a design to generate the signature.
- In the test mode, scan sequence of alternating ‘0’ and ‘1’ from primary inputs (PIs) into SFFs.
- Produce the signature-generation cycle.
- Shift out the response bits (signature) stored in the SFFs through primary outputs (POs).

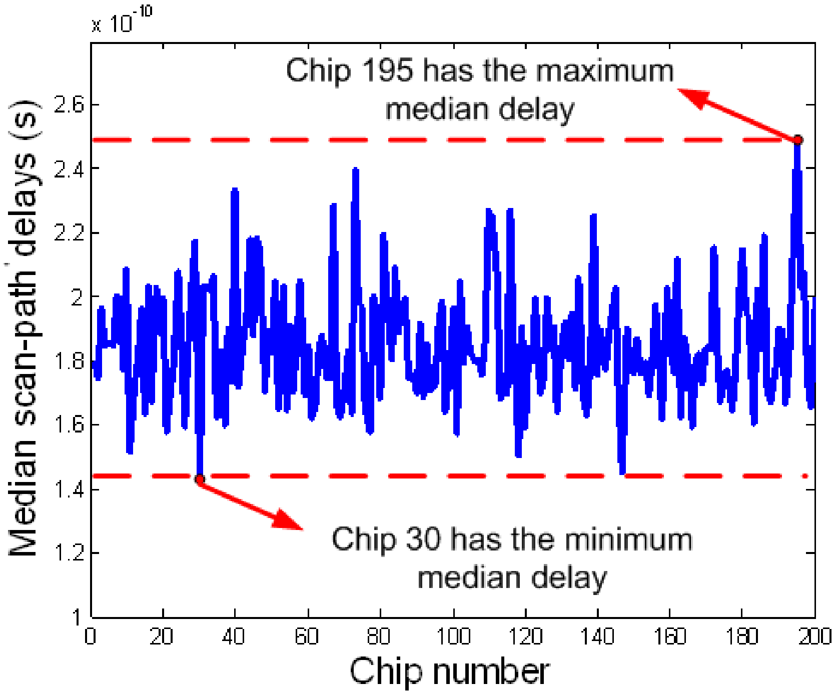
Hspice Simulation Setup

- 128-bit signature is evaluated in Hspice simulation under 45 nm PTM CMOS process.
- Process variation of V_{th}: $\sigma_{th,inter} = 15\%$ and $\sigma_{th0,intra} = 10\%$.
- Four inverters on each clock delay line of SGCC.
- Four inverters on each scan path.
- Eight clock delay lines are employed in the SGCC and each one produces an 16-bit signature.
- 1000 chips are simulated and 0 -> 1 is generated on the scan path.

Scan Path Distribution

Scan path follows the Gaussian distribution.

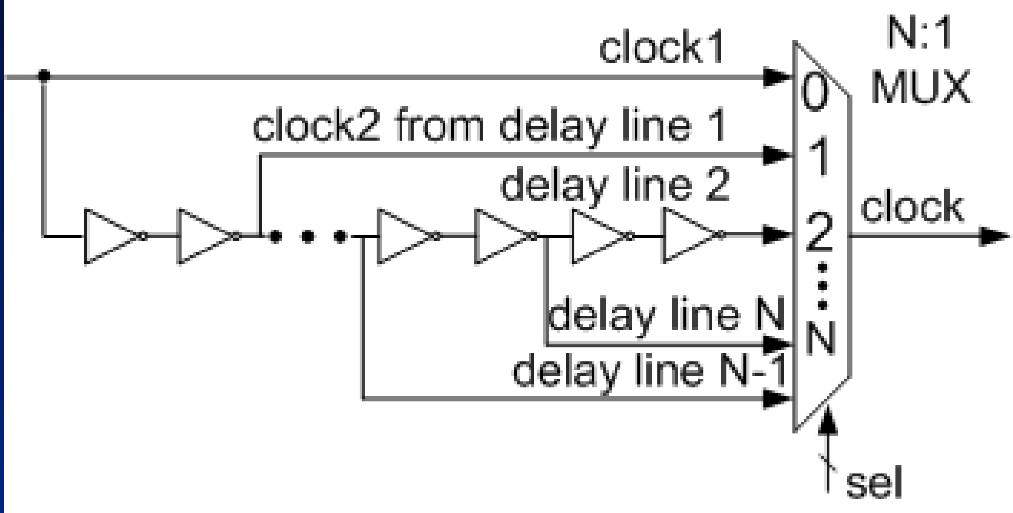




Median delay of each chip fluctuates largely due to the inter-die variation.

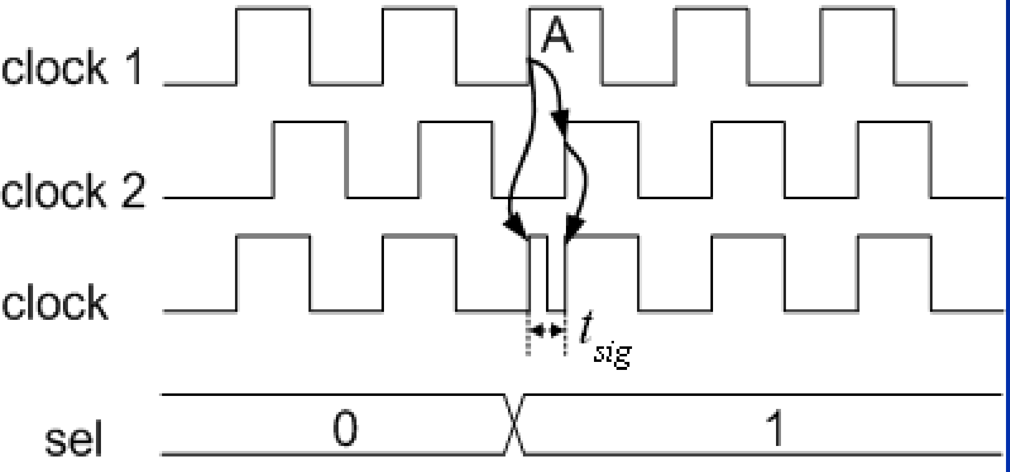
Signature Generation Cycle Controller (SGCC)

SGCC is comprised of N clock delay lines and a (N+1):1 multiplexor.



Architecture of SGCC

he switch between clock 1 and clock 2 generates a cycle of signature-generation period.

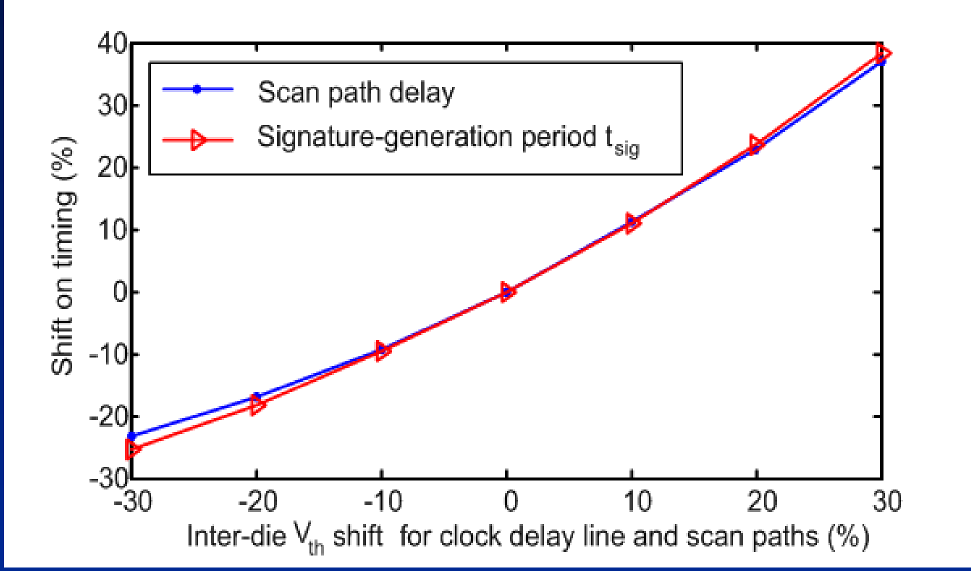


Timing of SGCC

Design keynote of SGCC for the signature of good uniqueness

Signature-generation cycle and scan path delay should have the approximate shift on the inter-die corner.

Approximate shift



Intra-die variation on SGCC

$$\sigma_{th,intra} = \boxed{\sigma_{th0,intra}} \cdot \sqrt{\frac{W_{min} L_{min}}{WL}}$$

The upsize of *W* and *L* drops the influence from the intra-die process variation.

Standard deviation for the minimum gate in a process

Shannon Entropy Estimation

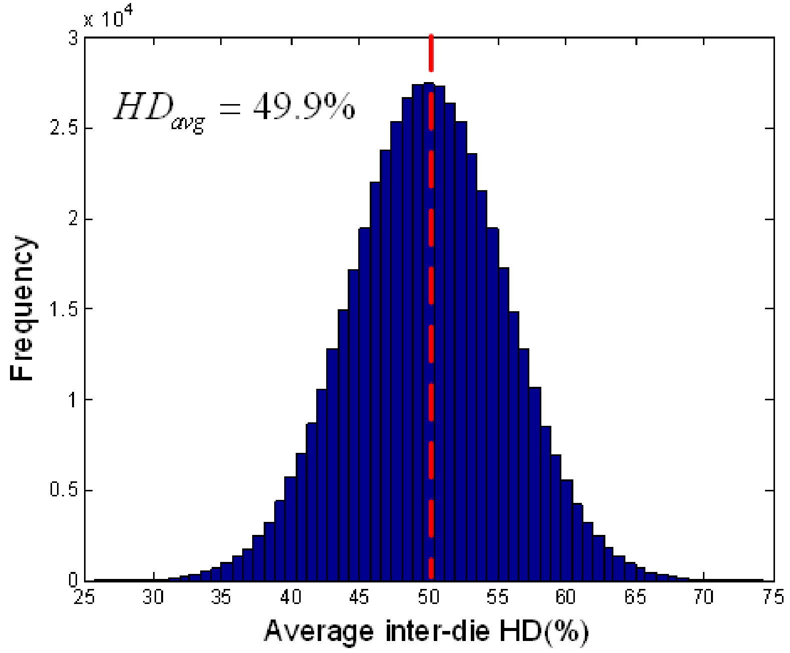
- The Shannon Entropy is related to: (1) selection of SFFs, (2) signature-generation cycles, (3) pre-stored value in SFF (0->1, 1->0 transition) .
- For only one signature-generation cycle, the maximum entropy for one SFF under (0->1 or 1->0 transition) is one bit.
- For m signature-generation cycles, the maximum entropy for an SFF under (0->1 or 1->0 transition) is larger than one bit, but less than m bits.

Uniqueness analysis

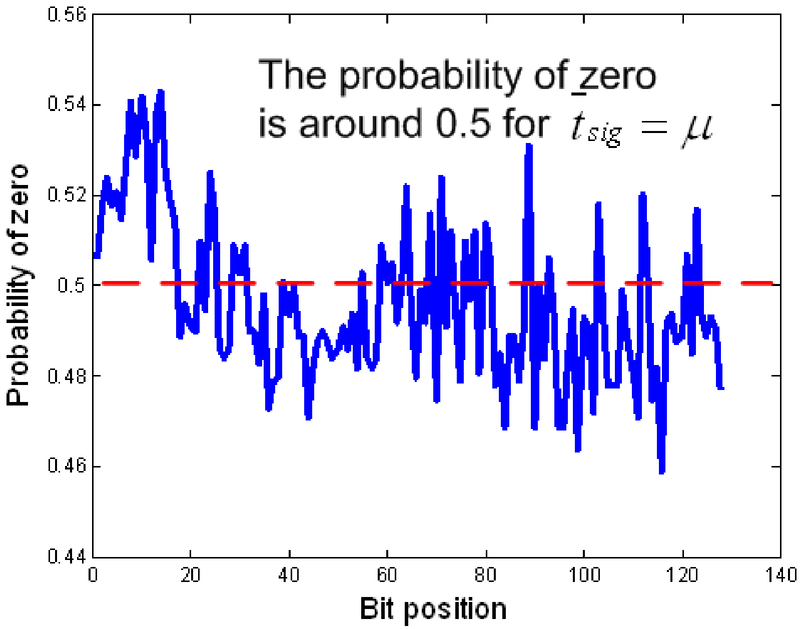
Signature-generation cycle (nominal)

↓ Equal

Scan path delay (nominal)



$HD_{avg} = 49.9\%$



The probability of zero is around 0.5 for $t_{sig} = \mu$

Average Inter-die Hamming Distance (HD)：49.9%

Probability of zero in the signature：0.5

Uniqueness analysis (cont'd)

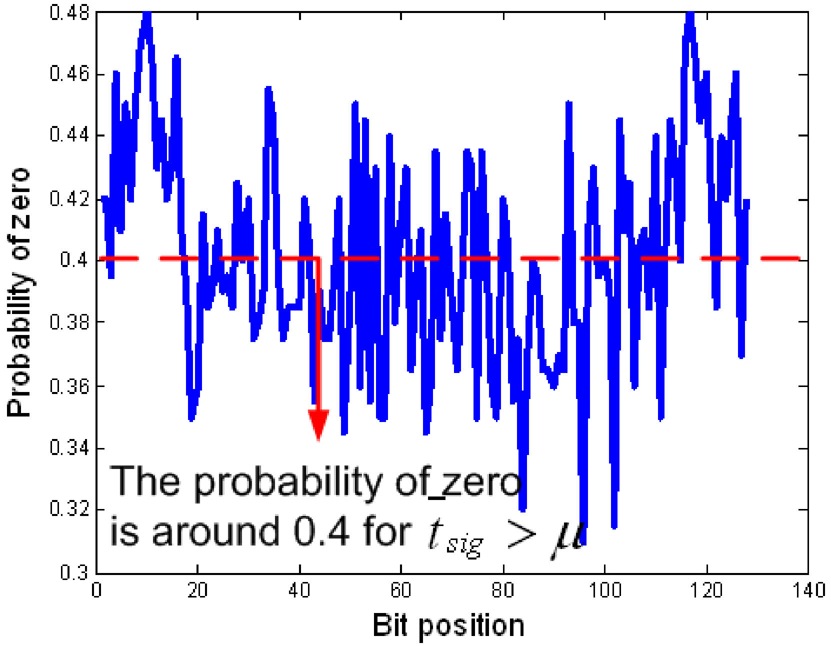
Signature-generation cycle (nominal)

Larger

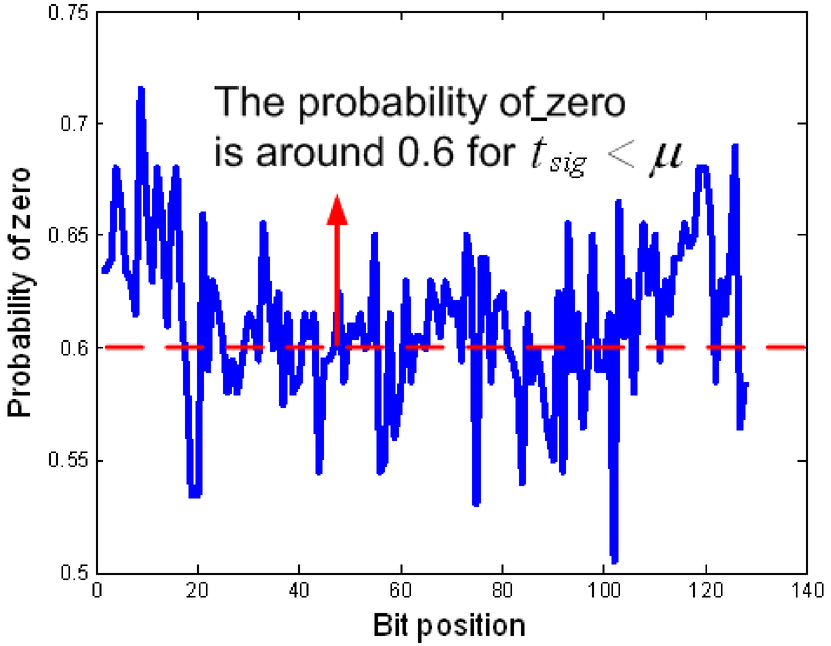
Smaller

Scan path delay (nominal)

Scan path delay (nominal)



The probability of_zero is around 0.4 for $t_{sig} > \mu$

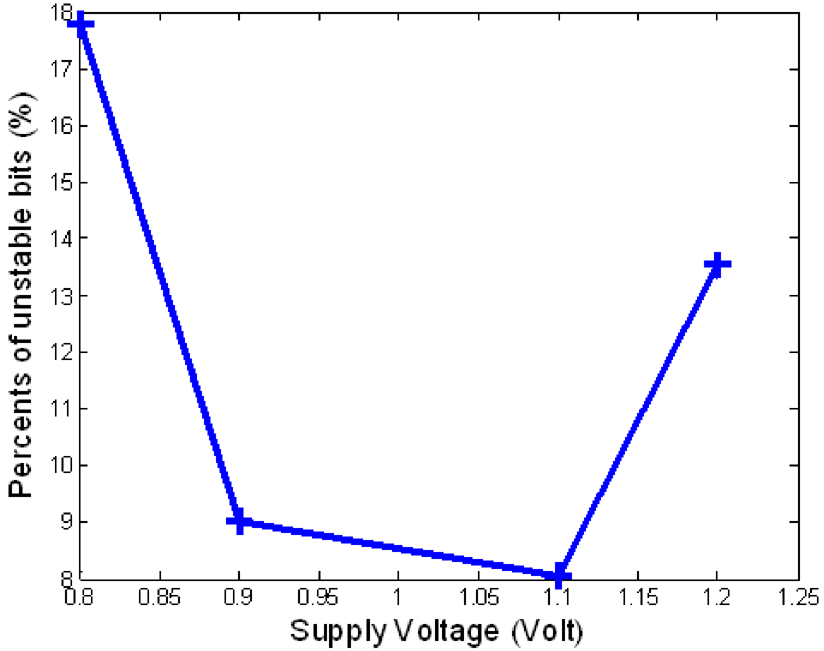


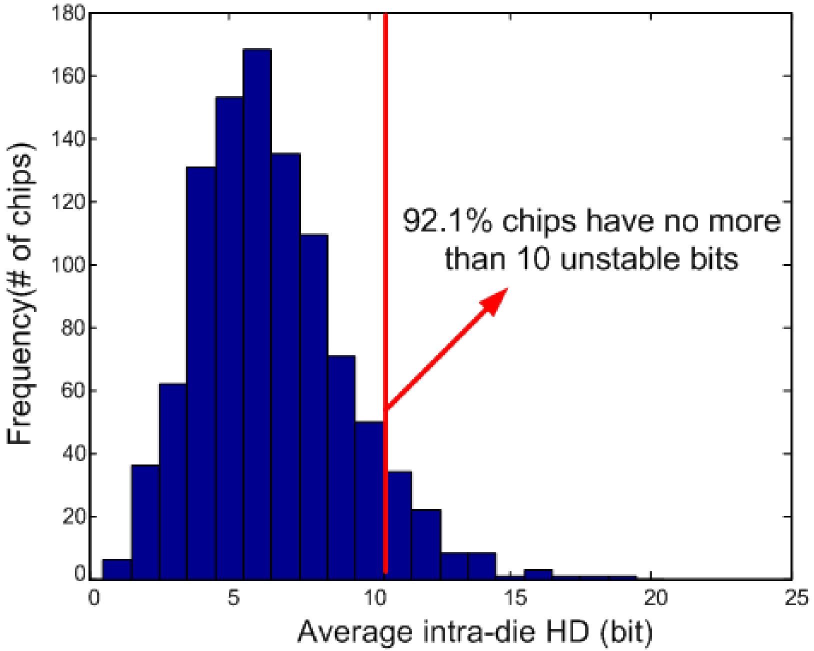
The probability of_zero is around 0.6 for $t_{sig} < \mu$

Probability of zero： 0.4

Probability of zero： 0.6

Robustness Analysis



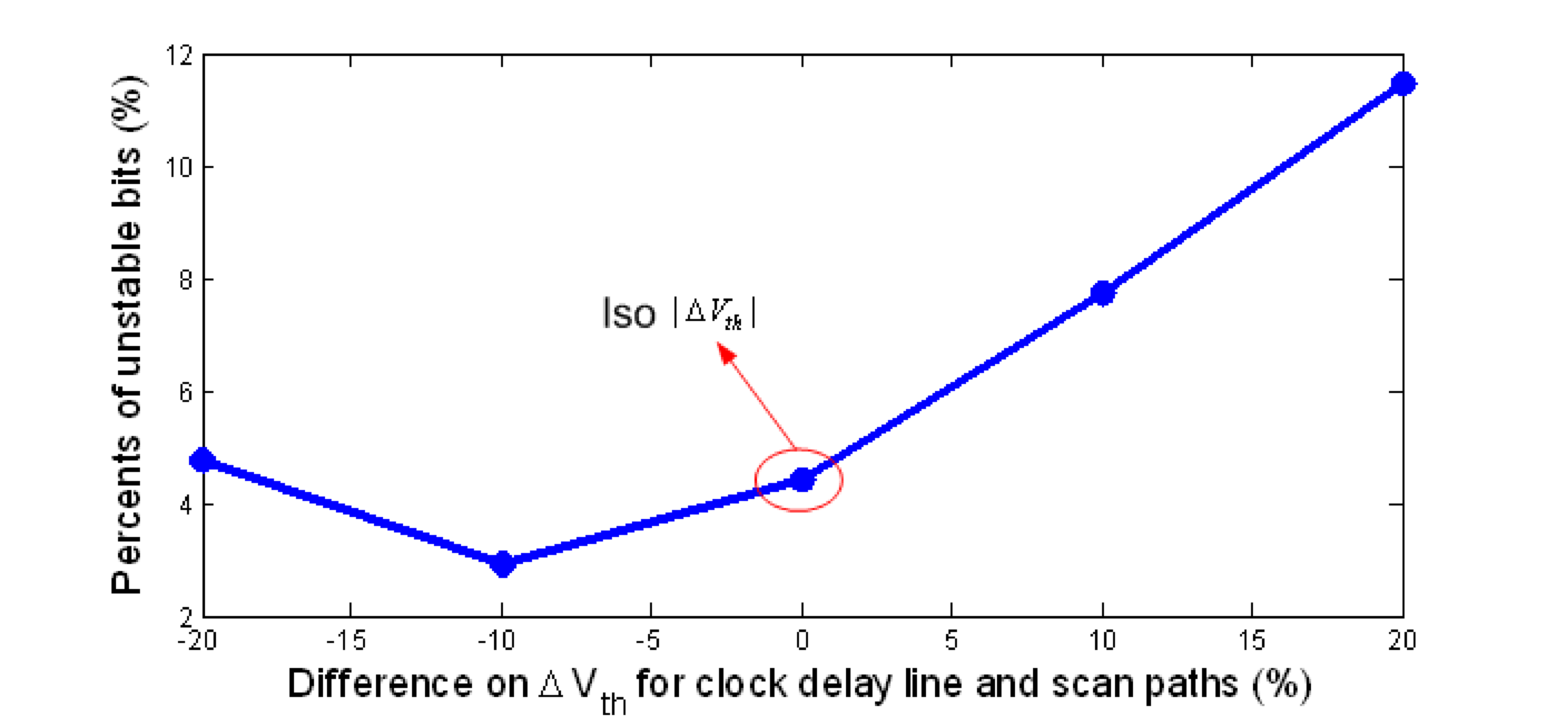


18% bits flip when the supply voltage is reduced to 0.8 Volt from 1 Volt.

92.1% chips has no more than 10 unstable bits within 85 degree Celsius.

Aging Effect Analysis

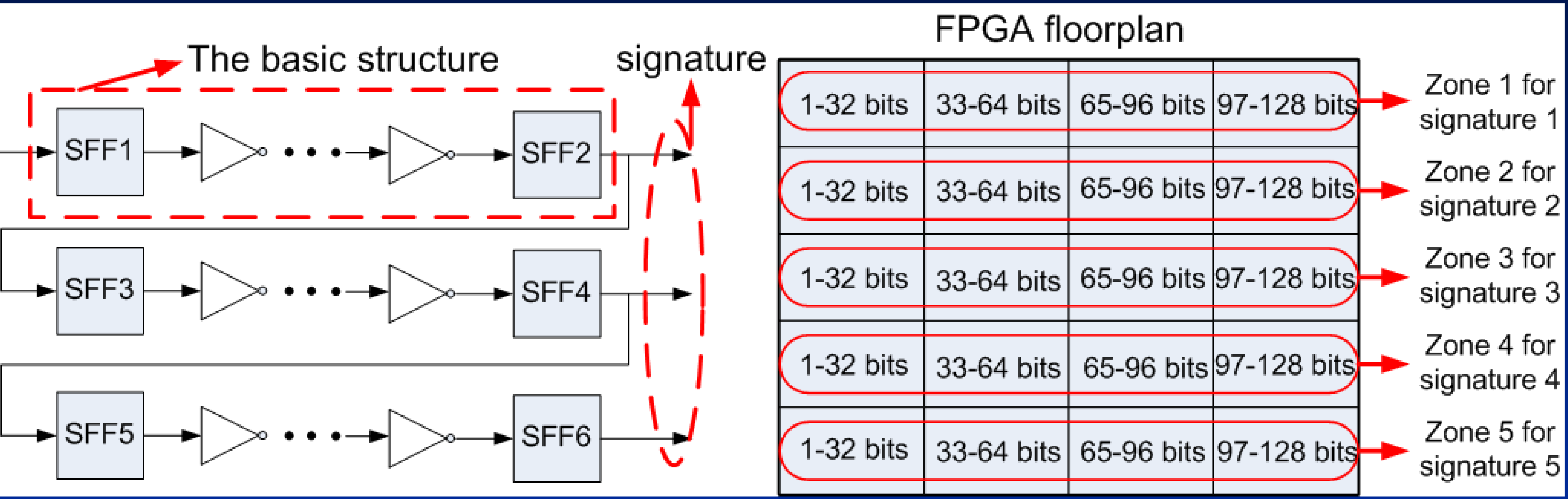
Unstable-bit percentage under non-identical NBTI on clock delay line and scan paths.



For the identical shift on V_{th} , nearly 4% bits flip.

FPGA Validation

Structure of scan chain mapping into FPGA



FPGA floorplan

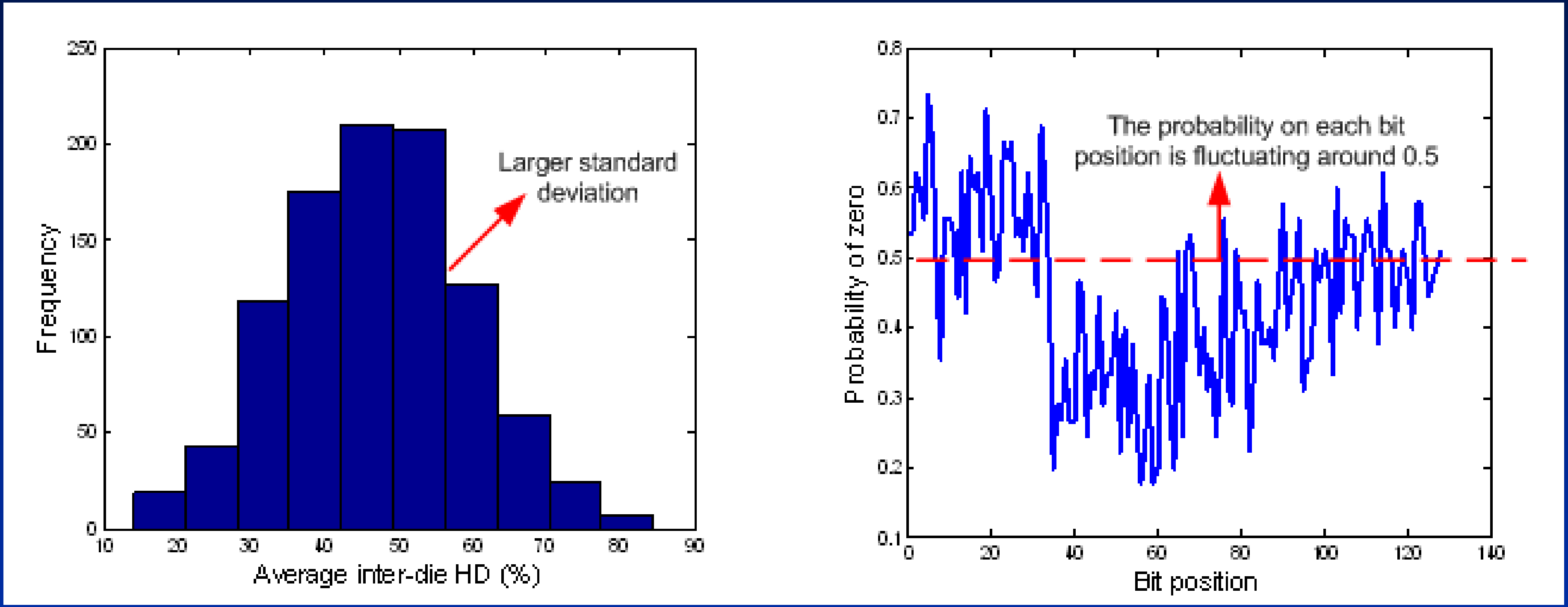
1-32 bits	33-64 bits	65-96 bits	97-128 bits	Zone 1 for signature 1
1-32 bits	33-64 bits	65-96 bits	97-128 bits	Zone 2 for signature 2
1-32 bits	33-64 bits	65-96 bits	97-128 bits	Zone 3 for signature 3
1-32 bits	33-64 bits	65-96 bits	97-128 bits	Zone 4 for signature 4
1-32 bits	33-64 bits	65-96 bits	97-128 bits	Zone 5 for signature 5

Each basic structure is mapped into a LE for one-bit signature with the delay as 5.42 ± 0.02 ns.

Totally, five 128-bit signatures are arranged on a FPGA from the top to bottom.

FPGA Validation (cont’d)

Result:



arge standard deviation of inter-die HD is due to the uncontrollability of intra-die V_{th} process variation on clock delay line because of the uniform structure of LE.

Discussion

- Because of the unbalanced wire lengths, fanout loads and residual clock skewing, the nominal delays of different scan paths may be far ways from identity in real IC design.
- We can obtain the signature by two steps:
  - Put scan paths with near-identical nominal delays into a set.
  - Each set has a clock delay line to trigger its own signature bits and aggregate them from different sets as the signature.

Area Overhead

- We make the comparison on the area of 128-bit ScanPUF and RO-PUF.
- For the ScanPUF, 8 clock delay lines (four inverters each) are included in the signature-generation controller.
- For the RO-PUF, if all ordering of ROs are possible, it requires 35 2:1 MUXs, two 32-bit counters and one 32-bit comparators.

	RO-PUF	ScanPUF	
		w/ INVs	w/o INVs
Area(um^2)	2721.40	303.96	62.04

Without INVs on scan path

Only take up to 62.04/2721.4=2.3%

Influence on Power

- Some inverters may be inserted into scan path that impacts the power of circuit in the function mode and test mode.
- For the function mode, power-gating can prevent the signal propagation on scan path and therefore incur no extra power overhead.
- For the test mode, when four inverters are on the scan path, the test power grows by 9.65% in Hspice.
- Since 78% test power is consumed by the combinational logic, taking 64-bit Alpha processor with 2408 SFFs for example, the overall power is increased by 0.11%.

Conclusion

- We have presented a novel PUF (ScanPUF) established on the scan chain, a prevalent on-chip structure.
- Since the on-chip structure is exploited, we show that the area overhead and design effort are reduced significantly.
- The extensive circuit-level Hspice simulation and FPGA validation show excellent signature uniqueness and robustness under temperature and supply voltage fluctuation and aging effect.
- It can provide a large number of challenge-response pairs.

Thank You

Questions ??