International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 4, July-Aug-2020, ISSN (Online): 2395-566X

RO-PUF Delay Path Sensor

PG Students T. Usha, Dr.V.J. Arulkarthick
JCT College of Engineering and Technology
Coimbatore, Tamil Nadu,
Usharamya.ece@gmail.com, arulkarthick.vj@jct.ac.in

***Abstract*-There are different factors that one would like to optimize when designing a VLSI circuit. Often they cannot be optimized simultaneously, only improve one factor at the expense of one or more others. The design of an efficient integrated circuit in terms of Power, Area and Speed has become a very challenging problem. To quickly perform measurements and evaluate the test results Automatic test equipment or automated test equipment (ATE) is used to performs test on a device, device (DUT), equipment under test (EUT) or unit under test (UUT).Though it was efficient in calculating characteristic of internal circuit, but the cost in computing the calculation an timing efficiency is very high. To address these issues, delay sensors are more and more frequently implemented on hardware and embedded into the System-Under-Test (SUT).It decreases the cost of testing and implementation. The Existing technique can be used for delay estimation, delay characterization and on-demand, real-time, estimation of the delay of cell-based array logic units such as multipliers. In chip manufacturing technology, reduction in chip size possesses great concern for power dissipation. Low power testing has become an important issue as power dissipation during testing mode is very high as compare to normal mode. PUF is used in testing of ASIC chips by generating pseudo random patterns. Instead of RO in existing method has been replaced by PUF circuit.**

***Key words*-Physically Unclonable Function, observation point, control point, Ring Oscillator, carry save adder.**

I.INTRODUCTION

A new method to measure, characterizes, and estimate near-on-the-fly delay is introduced. Path analysis is the analysis of signal transition propagation, from an input to an output, along a path, activated given an input test vector. We propose a methodology for path analysis in circuits that comprise an array of cells, along with the test vector definition. Furthermore, architecture is introduced offering re configurability, the ability to measure the delay between any pair of input-output ports, provided that there exists a path that connects them, which can be sensitized given a test vector, and a near-on-the-fly mode of operation. Given the increasing circuit density and variability because of the shrinking technology, critical paths may change. The proposed technique offers the ability to further investigate such cases.

There are three fundamental types of on-chip delay sensors. The first one is based on custom cells and an Analog-to Digital Converter (ADC) measuring voltage drop or voltage difference.The second one is based on the Vernier Delay Line (VDL) and the third type, which is adopted in this paper, is based on a Ring Oscillator (RO). An analysis of the path formation in RO circuits, focusing on reconvergent fanouts. Proposed a novel RO test architecture which uses the formulated the problem of path finding using a graph in which each node is a wrapper cell used a calibration unit to form a Path-RO by modifying an existing path instead of employing an additional RO, reported an RO combined with adder units to measure and characterize delay variation.

II. OBJECTIVE

The method of analyzing signals propagation delay in certain digital circuits and a delay sensing architecture. Based on controllability probabilities, we present a graph model useful for path delay analysis, derivation of test vectors that sensitize paths of interest, and re-convergent path detection. A delay-sensing architecture is illustrated that offers different accuracy levels and provides a near-on-the-fly measurement of the delay. The synergy of the introduced model with the introduced architecture is demonstrated by means of an example. The proposed technique can be used for delay estimation, delay characterization and on-demand, real-time, near-on-the-fly estimation of the delay of cell-based array logic units such as multipliers. FPGA measurements show that a better estimation of the delay is possible, compared to simulations, and an increase by 30% of operating frequency is feasible in certain cases, compared to simulation-based frequency estimation.

III. CONTROL AND OBSERVATION POINTS

Test point insertion involves adding control and observation points to the circuit-under-test in a way that the system function remains the same, but the testability is improved. An observation point (OP) is an additional

primary output that is inserted in the circuit to increase the observability of faults in the circuit. A control point (CP) is inserted in the circuit such that when it is activated, it fixes the logic value of a particular node to increase the controllability of some faults in the circuit. A control point can also affect the observability of some faults in the circuit because it can change the propagation paths in the circuit.

IV. EXISTING METHOD

Critical-path analysis is a powerful technique for identifying the key bottlenecks in a complex system with multiple concurrent operations. It can also provide other useful metrics such as slack (the amount of additional time an operation could take without impacting the system) and speedup potential (the difference between the critical path and the next-most-critical path).

V. INTRODUCED ARCHITECTURES

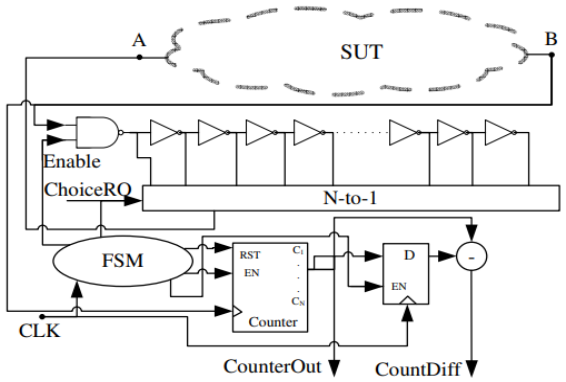

Fig no 1 RO Path Architecture

The proposed architecture is called Reconfigurable RO-Path (RRO-Path). Point A is connected to the output of the inverter chain following the N-to-1 multiplexer. Point B is connected to the input of the inverter and specifically to one input of a NAND gate. The "Enable" signal from the Finite State Machine (FSM) enables the RO for L clock periods.

The FSM also controls the counter and register "D". The RO output is used as a clock to the counter. The particular setup ensures that each rising edge of the RO is counted, provided that the generated frequency of the RO is less than the maximum operating frequency of the counter and the pulse width is larger than the inertial delay of the first gate in the path.

This can be guaranteed by controlling the RRO-Path length since the proposed architecture allows on-the-fly adjustments of the number of involved inverters. Count Diff can be used as an indication of the variance of the measured delay while Counter Out indicates the measured delay.

VI. PATH ANALYSIS MODEL

Here Full Adder which is the basic building block of CSA (Carry Save Adder) has been employed here. First the CPs is calculated moving from inputs to outputs and then the OPs, moving from outputs to inputs. Each of the primary inputs is annotated with a probability of assuming a 0 or a 1 value.

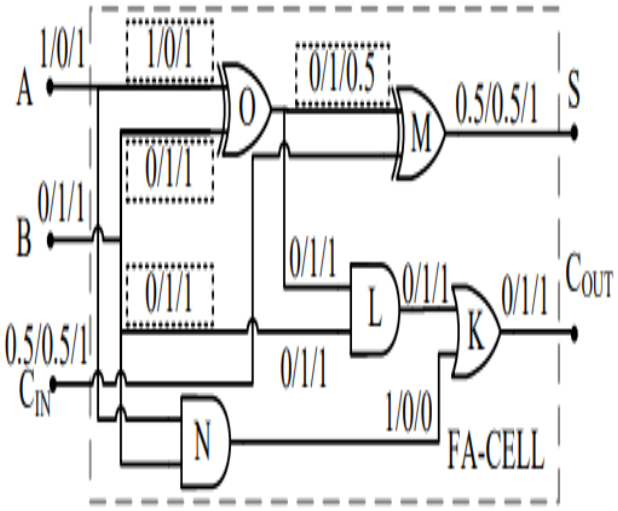

Fig no 2 Full Adder circuit with a sample of proposed controllability and observability probabilities

When an input remains constant at a value of zero during measurement, it is assigned with a Controllability Probability-zero (CP-0), CP-0=1 and CP1=0. Similarly, when an input is at constant one, it holds that CP-1=1 and CP-0=0. If an input alternates during the measurement, then the CP equals to the probability of the particular input value change.

The vector v1/v2/v3 annotating a signal line in the circuit, comprises the CP-0 of having value 0 (v1), the CP-1 of having value 1 (v2) and the Observability Probability (OP) (v3). For example, if CP-1A = 1, CP-1B = 1, CP-1C = 0.5, and the OP of all primary outputs is 1 (OPS = 1, OPCOUT = 1), then the remainder of the OPs and CPs in the circuit under test can be calculated.

A RO Path can be formed by connecting the output of a chain of N inverters to an input of a circuit, called Point of-Insertion (PI). Forming such oscillating path is equivalent to setting the corresponding input CP to 0.5. An output of the SUT, called Point-of-Observation (PO) can be selected to be connected to the RO chain. The values of CPs and OPs of signal lines between nodes can indicate whether there might be an oscillation along a path that connects the selected (PI, PO) pair for a given input vector.

International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 4, July-Aug-2020, ISSN (Online): 2395-566X

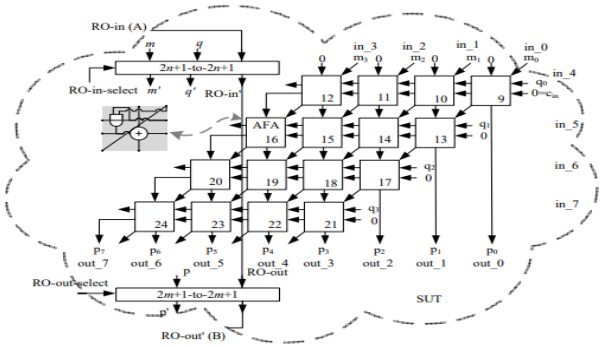

Fig no 3 A 4-bit CSA Multiplier with addition circuits.

An n-bit multiplier is constructed using n 2 AND-Full Adder(s) (AFAs). An AFA is a cell composed of an AND gate and a FA cell. To reduce processing time and storage requirements, only the CPs are calculated and stored in an n×n table. To also keep the information about the inputs/outputs, the table is increased by 2 · n (for the inputs) +2 · n (for the outputs) words, thus becoming of size n 2 + 4n words in total. If a CP of an input of a cell has a value different than 0 or 1, then this cell may contribute to the signal propagation of the forming oscillating path.

VII. RE CONVERGENT PATHS

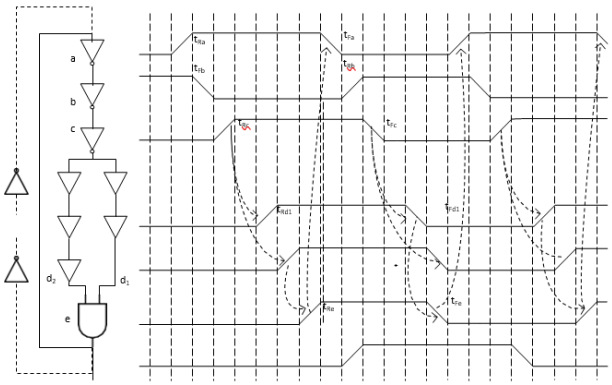

Fig no 4 Oscillation formed by reconvergent paths

In presence of reconvergent paths, it is possible that a path capable of oscillation cannot be formed. In order to determine whether a path can oscillate in presence of reconvergent paths, accurate timing information should be added to the introduced model provide timing-related constraints that need to be satisfied in order to have oscillation paths in multiple reconvergent fanouts. Illustrates such a case. If there is a gate and its inputs depend on the same PI, then the two corresponding driving signals may have different arrival times or even different pulse duration due to variability or different path length along which they propagate before they reach this gate. At the output of the AND gate, a pulse of period T1 is observed provided that there is a loop in the circuit and there is an inversion within the introduced loop.

Ring Oscillator

A "ring oscillator" (RO) comprises an odd number of NOT gates in a ring, whose output oscillates between two voltage levels, representing true and false. The NOT gates, or inverters, are attached in a chain and the output of the last inverter is fed back into the first.

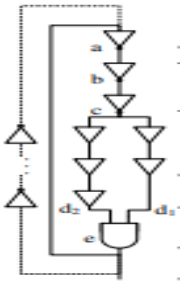

Fig no 5 Ring oscillator with configurable length

The oscillation frequency changes based on the input provided to the MUX, since a different number of gates is used to form the ring. The enable signal controls the operation of the RO: when the signal equals to "1", the circuit oscillates; when it equals to "0", the feedback path is broken and there is no oscillation. This design decision provides the capability to dynamically switch the RO length at the runtime. This is useful when testing a circuit so as to adjust the RO and achieve maximum sensitivity without restarting the testing procedure.

A single inverter computes the logical NOT of its input, it can be shown that the last output of a chain of an odd number of inverters is the logical NOT of the first input. The final output is asserted a finite amount of time after the first input is asserted and the feedback of the last output to the input causes oscillation. A circular chain composed of an even number of inverters cannot be used as a ring oscillator. The last output in this case is the same as the input. However, this configuration of inverter feedback can be used as a storage element and it is the basic building block of static random access memory or SRAM. The stages of the ring oscillator are often differential stages that are more immune to external disturbances. This renders available also non-inverting stages. A ring oscillator can be made with a mix of inverting and non-inverting stages, provided the total number of inverting stages is odd.

The oscillator period is in all cases equal to twice the sum of the individual delays of all stages. A real ring oscillator only requires power to operate. Above a certain threshold voltage, oscillations begin spontaneously. To increase the frequency of oscillation, two methods are commonly used. Firstly, making the ring from a smaller number of inverters results in a higher frequency of oscillation, with about the same power consumption. Secondly, the applied

voltage may be increased. In circuits where this method can be applied, it reduces the propagation delay through the chain of stages, increasing both the frequency of the oscillation and the current consumed. The maximum permissible voltage applied to the circuits limits the speed of a given oscillator.

VIII. PROPOSE METHOD

A Physically Unclonable Function (PUF) is a hardware security fundamental that translates an input challenge into an output response through a physical system in a manner that is specific to the exact hardware instance (unique) and cannot be replicated (unclonable).

This allows the system, and by extension any object or device it is attached to or embedded within, to be uniquely authenticated. At the point of manufacture, the system is subjected to one or more challenges, and the response to these challenges is taken and recorded. From then on, it is known that if a challenge is repeated at any point and its expected response is verified, the device must be the same as the one characterized previously. The characteristics of a PUF are to be robust (stable over time), unique (so no two PUFs are the same), easy to evaluate (to be feasibly implemented), difficult to replicate (so the PUF cannot be copied), and very difficult or impossible to predict (so the responses cannot be guessed). Many concepts have been put forward as candidates for PUFs.

Some, such as the Arbiter PUF, have become very well established with a large number of variations (such as the basic Arbiter PUF,1 N-XOR Arbiter PUF,2 Double Arbiter PUF,3 and so forth). Others, such as the MEMS PUF4 or BoardPUF5 do not appear to have significant current industry focus. While papers exist that provide information and organization to a selection of proposed PUFs, no paper sets out to provide a full review and organization scheme for all suggested PUFs at the concept level and above. This review will attempt to exhaustively catalogue all the different concepts that have been suggested as ways to implement PUFs and to create a coherent taxonomic system to organize them.

IX. PHASE CALIBRATED RING OSCILLATOR PUF DESIGN

Figure shows the traditional design of a ROPUF, which contains an array of ring oscillators (RO), two multiplexers (MUXes), two counters, and a comparator. Because of manufacturing variations, the wire delay and inverter delays in each RO is not controllable, which leads to different frequencies of the RO output. By selecting two ROs according to the PUF input, we can measure the pulses in a defined unit time with the counters. For example, if the first counter holds the larger value than the second one, the PUF output is '1'. Otherwise the PUF output is '0'. Ideally, the ROPUF output keeps the same bit value giving a certain input, but in reality bit errors and bias are involved in the output. Though the systematic or correlated process variation and the environmental noise caused by the voltage and temperature variations degrade the output stability, the bit errors of FPGA-based PUFs are directly generated by a selected pair of ROs with close frequencies, which lead to the unstable measurement in the counters and the flipped output in the comparator.

In, RO PUFs are characterized over 125FPGAs. To improve the quality of ROs, the surrounding logic effect on the oscillator frequencies was studied and a strategy was proposed by placing and comparing ROs in a chain-like structure. A reliability-improvement technique was used in pre-quantization phase of RO PUFs to reduce the noise in PUF responses. More optimized approaches were mentioned by introducing configurable ROs. They also suggested comparing adjacent RO pairs by controlling RO placement, but the FPGA implementations were not clear. A group-based RO PUF was introduced in, which described a new framework to filter the systematic variation and improve the hardware efficiency. However, it still required ECC for the PUF responses.

Authentication is an essential cryptographic primitive that confirms the identity of parties during communications. For security, it is important that these identities are complex, in order to make them difficult to clone or guess. In recent years, physically unclonable functions (PUFs) have emerged, in which identities are embodied in structures, rather than stored in memory elements. PUFs provide "digital fingerprints," where information is usually read from the static entropy of a system, rather than having an identity artificially programmed in, preventing a malicious party from making a copy for nefarious use later on. Many concepts for the physical source of the uniqueness of these PUFs have been developed for multiple different applications. While certain types of PUF have received a great deal of attention, other promising suggestions may be overlooked. To remedy this, we present a review that seeks to exhaustively catalogue and provide a complete organizational scheme towards the suggested concepts for PUFs.

Furthermore, by carefully considering the physical mechanisms underpinning the operation of different PUFs, we are able to form relationships between PUF technologies that previously had not been linked and look toward novel forms of PUF using physical principles that have yet to be exploited. While PUFs have been primarily targeted towards ASIC designs, in this paper, we explore their potential on FPGAs. According to our test on the Kintex-7 FPGA, the frequency of a 5-stage inverter chain RO is approximately 475MHz when the system clock is 200 MHz In the crossing timing domain between the ROs

and PUF control logic circuit, a high RO frequency adds to the instability of measurements. As with all oscillators, the rate of oscillation is determined by the length of a delay implemented in a loop. Thus, to reduce the frequency, more inverters can be added in the ROs, but it requires more hardware resources. We provide an improved RO design that takes advantage of the lookup tables (LUTs) of the configurable logic blocks (CLBs) and the general purpose interconnect in the FPGA. The first part consists of a 4-LUT delay and a 1-LUT inverter. The reset signal is used to control the enable timing of all LUTs. In the second part, a single inverter in the loop implements a high gain inverting amplifier. The output frequency is divided by 2in order to eliminate output glitches. This design only needs six LUTs and a D-type flip-flop (FD).

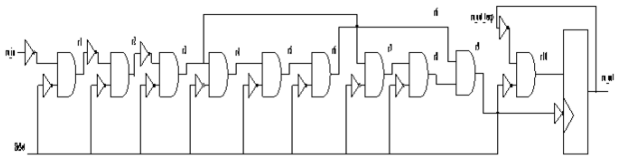

Fig no 6 An improved RO design for an FPGA

In order to generate variable length responses, we choose a design as shown in Figure. Once a challenge is received, it is stored in a shift register. We select the first 7 bits from the register as the input of the upper decoder and MUX in order to select an RO from the array. Likewise, another RO is selected using the next 7 bits from the challenge shift register. If the addresses are the same, the second 7-bit address is added by1 to avoid selecting the same RO for comparison. Next, we shift the challenge register to select a new RO pair. The shift pattern can be complex for security consideration. To make it easy to understand, we shift one bit to the left each time.

X. PUF APPLICATIONS

While the most common use of physically unclonable functions is for authentication, many additional applications exist. Fundamentally, the weak PUF can be described as a mechanism to generate on manufacture and store a single (or small number of) cryptographic keys. This key can then be compared to an external database for identification or authentication as previously discussed, or used as part of other protocols such as secure communication or memory encryption. As with the previously described authentication protocols, the number of keys stored is small, so an attacker could have access to the PUF in such a way as to determine those keys, making the system then unsecure. This would be the same as an attacker discovering the password or key for the communication or encryption in a more conventional system. The strong PUF can also be used for the same applications and can be considered as a mechanism for generating a large number of keys upon manufacture to be thereafter stored. Like in the strong PUF authentication protocol this means that the keys can be used redundantly, enhancing security. This would operate like a one-time-pad in conventional cryptography, where each authentication exchange, secure communication message, or bit of encrypted data can utilize a different key and the compromise of a single key would not necessarily impact the whole system. Additionally, should the key be chosen randomly from the large possible set, access to the PUF must occur at the same time as the authentication, communication, or decryption, as determining which key is necessary to record and replay would not be possible ahead of time in addition to these applications, protocols have been devised that specifically allow for bit commitment, oblivious transfer, and secure key exchanges.

Certain PUF designs can also involve enclosing the PUF evaluation and/or other critical components within the source of entropy itself, in a system commonly known as an enclosure PUF. These can be electronically evaluated, for instance, in the case of the coating PUF, or non-electronically evaluated such as a version of an optically evaluating nanoparticle distribution PUF. The value of this system is tamper evidence, where an attempt to physically accessory probe inside the PUF would rearrange the source of entropy and change the readout of the PUF when it is next evaluated. This can be valuable to prevent side channel attacks on the PUF's own electronics, or to even void memory or nullify other circuits should the enclosure be breached.

XI. RESULT ANALYSIS

The ring oscillator Delay path analysis of 4-bit CSA Multiplier with addition circuits output is simulated using Xilinx software. Consequently, based on the architecture of the CSA multiplier, it is possible to estimate the average delay of the cells through the product-calculation path by dividing the measured delay with the number of the involved cells. Following the path in 3–16–19–22–23–out 5 it is possible to measure its delay. This path includes a carry-calculation path a horizontal path between AFA cells of from node 22 to 23. In this method using Xilinx 14.2 to programme the RO, D-latch, subrector, Counter, and 4 bit CSA simulated and identified the delay path. In the exiting method area and speed of the circuit is large and cost also large. In the proposed method to overcome the existing system disadvantages.

XII. CONCLUSION AND FUTURE SCOPE

A methodology of path analysis based on controllability and observability probabilities is presented. These probabilities are used to investigate RO paths and acquire the input test vectors in order to sensitize paths of interest such as critical path(s). An innovative RRO-Path architecture is presented, providing a reconfigurable

number of active inverters in the RO. The total power of delay estimation is 0.144(W). The introduced model, which can be further expanded and combined with the proposed RRO-Path architecture, can be used for delay analysis, delay characterization and near-on the-fly measurement of the delay. The ability of updating the model with measured results can increase the accuracy and the characterization ability of the delay estimation. The Existing technique can be used for delay estimation, delay characterization and on-demand, real-time, estimation of the delay of cell-based array logic units such as multipliers. The proposed method phase calibrated ring oscillator PUF design. In the crossing timing domain between the ROs and PUF control logic circuit, a high RO frequency adds to the instability of measurements. As with all oscillators, the rate of oscillation is determined by the length of a delay implemented in a loop. Thus, to reduce the frequency, more inverters can be added in the ROs, but it requires more hardware resources. The total power of delay estimation is 0.014(W).

REFERENCES

[1] C. L. Lee (2008) -,"Path-RO: A novel on-chip critical path delay measurement under process variations," in Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design, Piscataway, NJ, USA.

[2] 2. C. Wu, C. L. Lee, M. S. Wu, J. E. Chen, and M. S. Abadir (Feb 2000) -"Oscillation ring delay test for high performance microprocessors," Journal of Electronic Testing, W.

[3] E. J. Jang, A. Gattiker, S. Nassif, and J. Abraham(May 2011) - "Efficient and product-representative timing model validation," in IEEE 29th VLSI Test Symposium.

[4] G. Sai, B. Halak, and M. Zwolinski (2017) "Multi-path ageing sensor for cost-efficient delay fault prediction," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. PP, no. 99, pp. 1–1.

[5] K. S.-M. Li, , C. Su, and J. E. Chen. (2005) - "Oscillation ring based interconnect test scheme for SOC," in Proceedings of the 2005 Asia and South Pacific Design Automation Conference. New York, NY, USA: ACM.

[6] L.-T. Wang, Y.-W. Chang, and K.-T. T. Cheng (Mar. 2009) - Electronic Design Automation: Synthesis, Verification, and Test. Morgan Kaufmann,

[7] M. Vesterbacka - (Nov 2009) -"A novel architecture for on-chip path delay measurement," in International Test Conference.

[8] N. U. Andersson and M. Vesterbacka (Oct 2014) - "A vernier time-to-digital converter with delay latch chain architecture," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 61, no. 10, pp. 773–777.

[9] N. Drego, A. Chandrakasan, and D. Boning (Mar. 2010) - "All-digital circuits for measurement of spatial variation in digital circuits," IEEE Journal of Solid-State Circuits.

[10] P. Sakellariou and V. Paliouras (2000)- "Low-power delay sensors on FPGAs," in Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation, 2013, vol. 7606, pp. 194–204.

[11] R. Datta, A. Sebastine, A. Raghunathan, and J. A. Abraham (2004)-"On-chip delay measurement for silicon debug," in Proceedings of the 14th ACM Great Lakes Symposium on VLSI. New York, NY, USA: ACM.

[12] S. Ghosh, S. Bhunia, A. Raychowdhury, and K. Roy(Dec 2006) -"A novel delay fault testing methodology using low-overhead built-in delay sensor," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,

[13] X. Wang, M. Tehranipoor, S. George, D. Tran, and L. Winemberg (Aug.2017) -"Design and analysis of a delay sensor applicable to process/ environmental variations and aging measurements," IEEE Transactions on Very Large Scale Integration (VLSI) Systems.

[14] Y. Kim and C. Yoo (JUNE-2014) - "A 100-kS/s 8.3-ENOB 1.7- µW time-domain analog-to-digital converter," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 61, no. 6, pp. 408–412.