International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 10 (2015) pp. 26941-26950

http://www.ripublication.com

Delay Line Characterization and Generation of PVT (Process, Voltage, Temperature) Invariant Delay Line

N. Santhosh Priya[1]
[1]*M. Tech, VLSI Design, School of Computing,*
SASTRA University, India.
Email: santhoshpriz@gmail.com
Jayanta Biswas[2]
[2]*Assitant Professor, School of Computing,*
SASTRA University, India.
Email: jayantabiswas@ict.sastra.edu

Abstract

An integrated digital design of delay line is proposed in this paper. Applications of delay lines are found in realizing delay-line-ADC, self-clocking circuits and physical unclonable function (PUF). This proposal involves characterization of delay line behavior for its requirement in realization of PUFs. In this proposal, delay line behavior is characterized and a PVT (Process, Voltage, Temperature) invariant delay line topology.The target is to design a precision wide range delay chain whose delay is independent of PVT. Multiple taps are taken from the delay chain such that the intended delay of the corresponding multiple delay taps vary linearly. Modules are tested with multiple FPGA boards to find the unique signature requirement for PUF implementation. All the corner cases are tested to make sure that the proposed topology is PVT independent. Modules are also tested on multiple discrete delay line chips and a unique digital signature is found for each of them. The proposal is demonstrated with Altera FPGA and delay line fabricated with discrete chips. A PVT invariant general delay line topology and delay line characterization report is documented.

Keywords: PUF, PVT invariant delay line, discrete chips

Introduction

Delay line topology finds applications in ADC, Self Clocking Circuits, Instant Voltage change detection and Physical Unclonable Functional (PUF) circuits. The delay lines used for the first three applications are independent of process and temperature. The propagation delay of the delay line varies linearly based on supply voltage.

Physical Unclonable Function can be considered as a physical entity that gives a way for identification and authentication of Integrated Circuit (IC) designs.PUF is embedded into structures and thus works as a secret key for authentication of the device.They are easy to evaluate but hard to predict. The implementation of PUF is such that it is immune to the numerous ways of tampering the IC in order to obtain the secret key.PUFs are affected by variations due to temperature and supply voltage thatmaydegrade their performance.

A PUF can be viewed as a function that maps challenges to responses. A PUF is synonymous to a tag with a hardware secret key which is generated based on the physical parameters of the device. A software verifies that the secret key entered is valid and only then provides access to the device. PUFs are assumed to be tamper evident, i.e., the PUF is destroyed when an enemy tries to retrieve detailed information about its structure. Moreover, the secret key cannot be uncovered easily as the secret key space will be huge.

The uniqueness of a PUF embedded in an IC is derived from the fact that physical properties of an IC are unique to that particular IC. The manufacturing of an IC involves many factors that are random and uncontrollable by the manufacturer. These factors, mostly silicon wafer variations, give rise to unique physical properties embedded in an IC. The fact that wafer variations occur amongst all ICs even when the ICs are manufactured are from the same manufacturer, is exploited for the realization of a unique PUF for each and every IC.Inherent delay variations are found in ICs from the same lot or wafer. These may be due to mask variations or due to pressure and temperature variations in the different manufacturing steps. These variations are found to be inversely proportional to the device size.

In this proposal, characterization of PVT independent delay line is carried out. The ideal case would be when the digital signature depends only upon silicon wafer variations and is completely independent of PVT variations. Thus supply voltage, temperature and other variations due to process is avoided so that the PUF’s performance is not affected.The idea is to make the uniqueness PUF only based silicon wafer variations to increase its reliability. Thus, only the silicon wafer variations are captured which is desirable.

The requirement of implementing PUF is to capture the change in wafer variation with respect to delay with a unique digital signature. The digital signatures can be used as secret keys for security protocols in public-key and private-key cryptography. Hence it is essential that thedelay lines used for PUF applications must be PVT independent and the delay should vary linearly with the length of the delay chain.

Field Programmable Gate Array (FPGA) is an integrated circuit which consists of a set of interconnected blocks which can be reconfigured multiple times. Flexibility, lower time-to-market and easy availability are the properties that give an edge to FPGAs over ASICs. These properties make FPGA a more suitable platform for PUFs than ASICs. In this proposal, delay line characterization is also implemented for delay lines fabricated on discrete chips. These discrete chips consist of a chain of nor gates that form the delay line. Thus the idea of PVT independent PUFs has also been extended to ASIC platforms.

The target is to design a high precision delay chain whose delay is independent of PVT and the same property should also hold for the wide range of supply voltages. Delay line provides a unique digital signature (with multiple delay taps) by capturing the minute wafer length variations. Each delay line is optimized locally with assignment of separate assignment groups.Fine tuning is done in order to cancel out delay skews. Delay line is tuned such that the propagation delay varies linearly based on the supply voltage.Delay increases linearly with the length of the delay line.

Background

Earlier works have been done on implementing real-time arbiter-based PUF on FPGA using programmable delay lines [1]. Two identical delay paths are constructed such that they differ only due to manufacturing imperfections. Both the paths are fed with step inputs and the difference in the delay at the last edge of the paths is taken as the response. Robustness responses have been evaluated to reduce the temperature dependency. It is evident that the larger the delay differences caused by challenges, the lesser the responses get affected by temperature and voltage variations. Robustness has been exploited with respect to temperature variations, however the proposal lacks complete isolation between temperature and wafer variations.

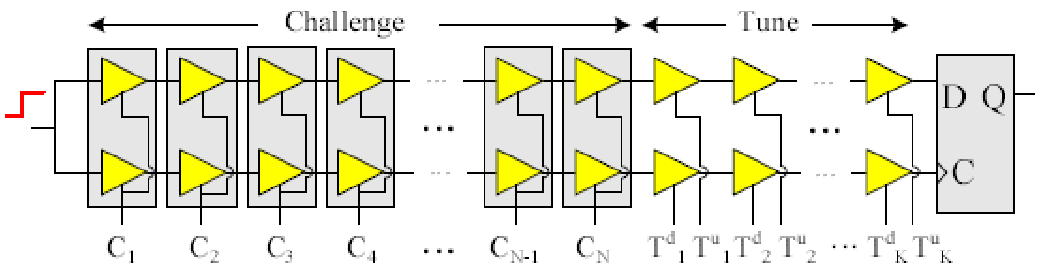

Figure 1.1: Existing arbiter PUF structure

Figure 1.1 shows the existing arbiter PUF structure where it lacks complete isolation between wafer and temperature variation. They have added an extra delay line inorder to get the wafer variation. But they failed to the temperature variation for the extra added delay line.

The delay Vs supply voltage characteristics constitute a non-linear relationship. The hitches that come across due to this non-linear behavior and the need to overcome it concerning an ADC (Analog to Digital Converter) has been addressed in [2]. A delay-line ADC with several bands has been composed and delay variation is uniform with respect to supply voltages. Hence such a model has been devised by altering these parameters. We make use of the same parameters and target it for FPGAs. An uneven distribution of taps is devised that it gives rise to a linear relationship between supply voltage and delay.

Experimental Setup

FPGA Boards

The proposed effective design of delay line PUF is implemented in Altera DE I education boards that consist of Cyclone II family of FPGAs. The design has two delay chains. One chain is signal chain and one chain is clock chain. Each delay cell consists of one D flip-flop, appended with three nor delay cells each. Starting from the output side of the signal chain and working inwards,32 output taps are taken. These taps are then sampled by feeding them to sampling D flip-flops. The output of the second chain or the clock chain, i.e., clkout is fed as the clock input to the sampling flip-flops. The sig to sigout delay and clk to clkout delay vary linearly with increase in length of the delay chain.

Each block of the delay line is designed using Verilog HDL (Hardware Description Language). The design is synthesized using Altera Quartus II 12.1. Time Quest Timing Analyzer is used for Static Timing Analysis and QSIM is used for functional and timing simulation of the design. The effective design of delay line PUF is implemented in FPGA with a 200 KHz clock. A clock divider is used to divide the inbuilt 50 MHz clock into a 200 KHz (5 us) clock. The design is dumped on eleven DE I boards out of which we are able to isolate five boards and signature for each boards are obtained. The design is also tested for the case where a 50 MHz clock input is used.In this case, multiple edges are observed for all the eleven boards, thus isolating all the eleven boards.

Static timing analysis is done to verify that the modules meet the timing requirements when different constraints are specified. Altera Time Quest Timing Analyzer is used for this purpose. An SDC (Synopsys Design Constraint) file is written into the project. The SDC file is used to specify the timing constraints for the design. Various clock frequencies and input and output delays of the various paths are specified in the SDC file. The project is compiled again and Time Quest Timing Analyzer is used to verify if the setup and hold requirements of the design are met. This is implied by positive values for setup and hold slacks. The maximum frequency requirement is verified by the FMAX Summary. It is also checked that all paths present in the design are constrained. Timing simulation is carried out using Quartus Simulator to verify whether the design behaves in expected manner.

Thus functional simulation, static timing analysis and timing simulation for all modules are completed, followed by pin assignments. Pin assignments are done in such a way that the output taps are assigned to LEDs present and the clock and reset signal are assigned to the switches in the Altera DE I board. The same procedure is followed for all the boards.

The basic diagram of the design is given below.

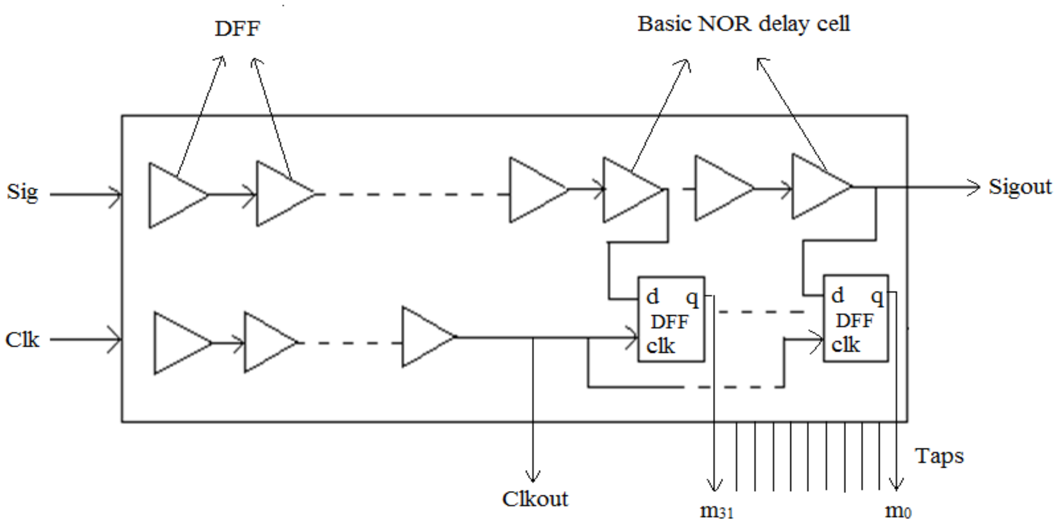

Figure 1: Block diagram

The below fig. shows the D Flip Flop with reset signal. The input is given as signal and output as q. This block is used in the place of series of DFF in the main block.

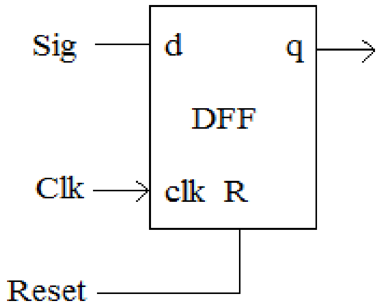

Figure 2: D Flip Flop

The below fig. shows the basic NOR delay cell unit. It has a series of three NOR delay cell. This is placed in between each DFF at the output side.

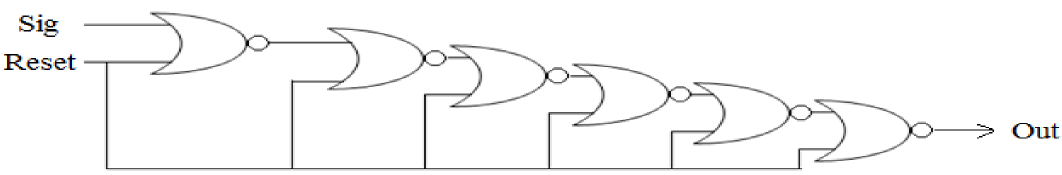

Figure 3: Basic NOR delay unit

External Delay Boards:
The setup for finding digital signatures for external delay boards consists of two delay chains, consisting of three delay boards each. Each delay board consists of a series of nor gates embedded in them along with input pins for clock and power supply and output pins for delay chain output and several taps. Each of the delay boards are connected to a regulated power supply. Several taps are taken from the sig chain and given as inputs to one Altera DE II board through the GPIO ports present on the DE II board.

The delay chain output from the clk chain is also fed as an input to the DE II board. The tap inputs from the sig chain are sampled using D flip-flops designed in the DE II board using Altera Quartus II 12.1 software. The clk chain output is fed as the clock input to these sampling D flip-flops. The taps are sampled with respect to the clk out edge. The taps that are obtained after sampling are taken as outputs to the GPIO ports. These taps that are obtained after sampling are observed on an oscilloscope. This model is tested for several such set of external delay boards and the digital signatures for each of these models is obtained and recorded.

Experimental Results and Discussion:
The design is tested in 11 DE I boards of cyclone II family, from that 5 boards are isolated. The unique signature for 5 boards are given in the table below.

Table 1: CLK 5us signature output

	BOARD 1	BOARD 2	BOARD 3	BOARD 4	BOARD 5
DFF NOR3 (5us)	00000111111 1111111	000011111 111111111	0111111111 11111111	001111111 111111111	000111111 111111111
Signatures	0000	0001	1111	0111	0011

FPGA Board Results

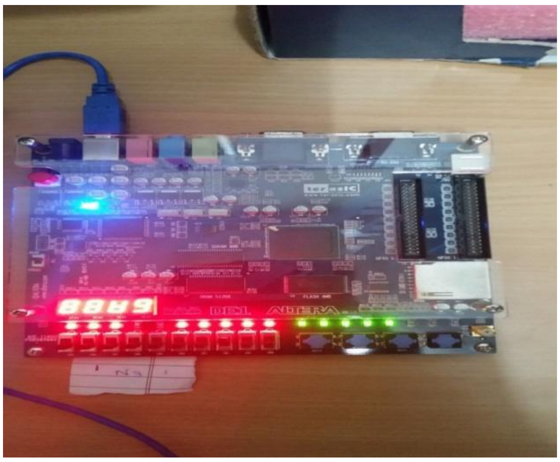

Figure 4: Altera DE I FPGA Board 1

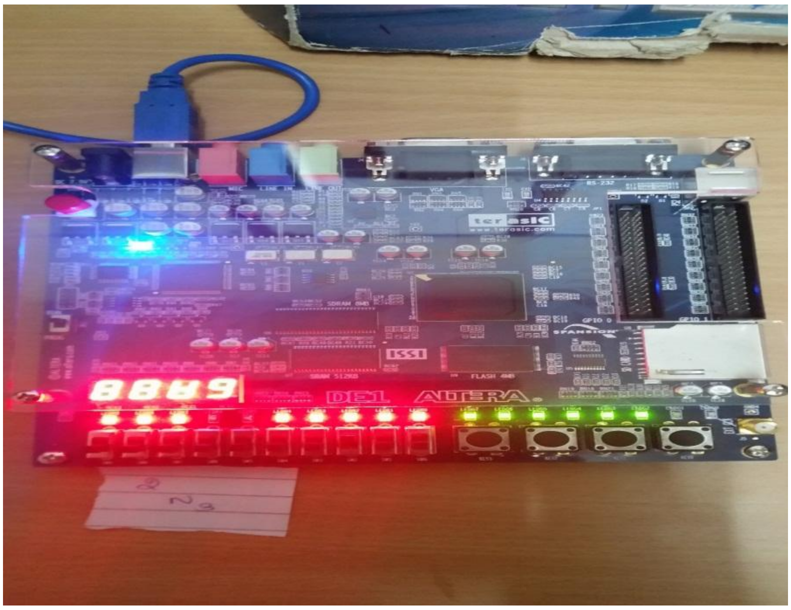

Figure 5: Altera DE I FPGA Board 2

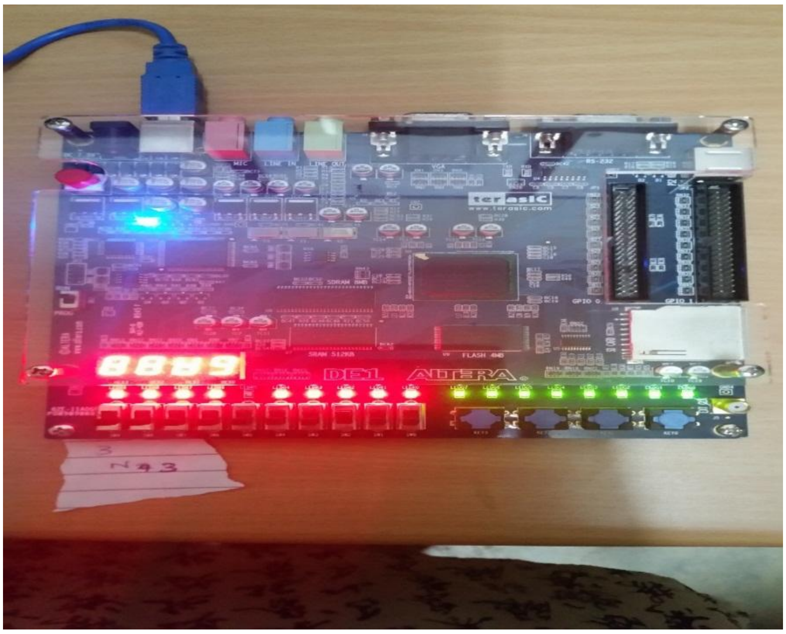

Figure 6: Altera DE I FPGA Board 3

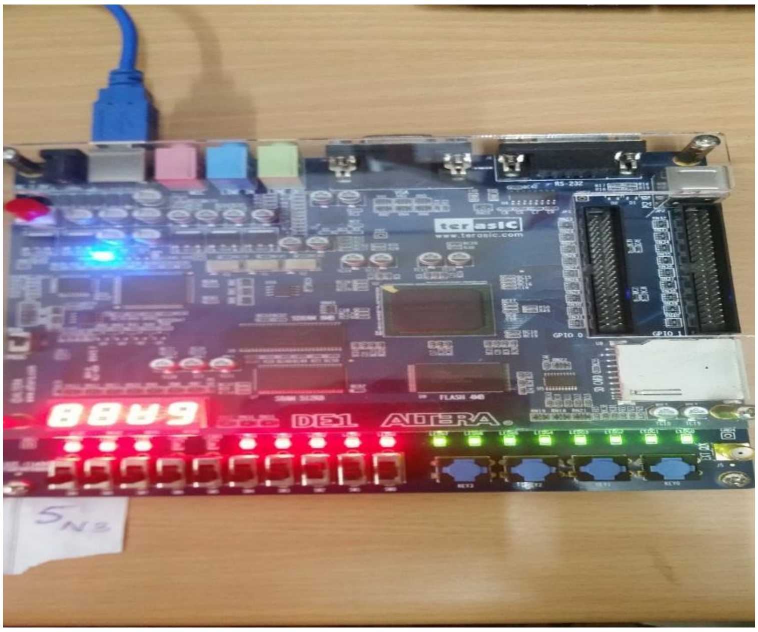

Figure 7: Altera DE I FPGA Board 4

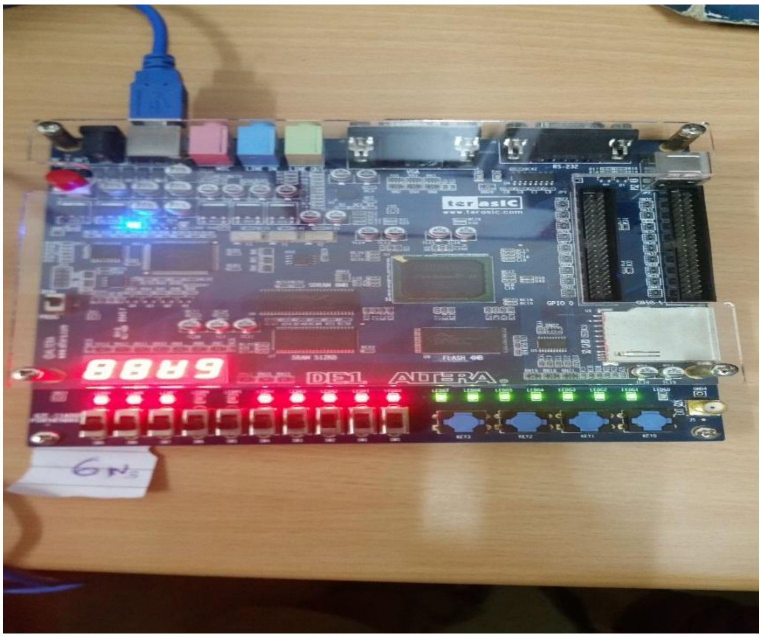

Figure 8: Altera DE I FPGA Board 5

The above figures shows the experimental results of delay line design which is implemented for PUF circuits in Altera DE I FPGA Boards. These are the wafer variation which we got in the 5 isolated Altera DE I FPGA boards. Here the feasibility for the wafer variation is shown and the results are given. So we can able to achieve this wafer variation as many as number of Altera DE I FPGA boards.

External Delay Board Results

The figure 5.3 shows the result of external delay board where the edge is caught between 1st and 2nd tap and also at 4th and 5th taps. This is the edge difference which is achieved so that we got the wafer variation in multiple set of external delay boards.

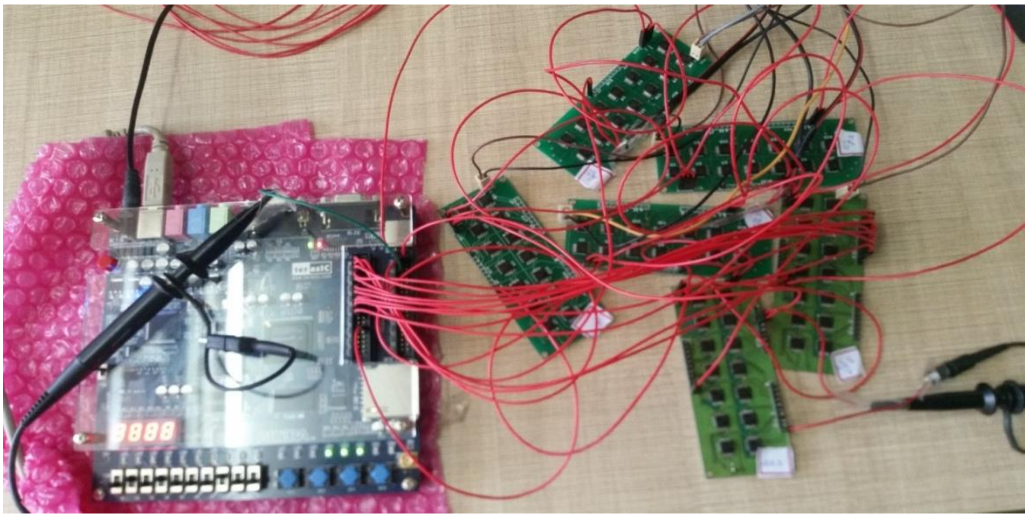

Figure 9: External delay board with discrete chips

Conclusion

This design offers an optimized delay line implementation that meets the PUF application requirement and provides a linear delay variation with respect to wide range of supply voltage and also for the variation in temperature. In this work an optimized delay line PUF design has been proposed for the PUF circuits. Digital signatures are taken from the corner of the delay line. The proposed PUF can work at 200 KHz clock frequency with maximum number of hardware and the complete design can be fully synthesized with HDL tools. This paper achieves a minute wafer variation in Altera DE I board which is a main requirement of PUF circuits. And also wafer variation is achieved in external delay boards for a change in supply voltage of 2.1V to 3.3 V. The results illustrates the linear response in the delay curve which is distributed in the normal distribution curve. The experimental evaluation shows the delay line is wafer dependent even when the temperature variations is from 100ºC to 300ºC.

References

[1] MehrdadMajzoobi, FarinazKoushnafar, SrinivasDevadas -2010-"FPGA PUF using Programmable Delay Lines" –Electrical and Computer Engineering Departments, Rice University, WIFS 2010, December 12-15 2010, Seattle, WA, USA.

[2] MuktiBarai, Member, IEEE, SabyasachiSengupta, and Jayanta Biswas 2010,"Digital Controller for DVS-Enabled DC-DC Converter, IEEE Transactions on Power Electronics, vol 25, no 3,March 2010.
[3] PreethiVarma, R.A.Mishra,2011-"Temperature Dependence of propagation delay characteristics in LECTOR based CMOS circuits", Special issue of international journal of computer application(0975-8887), on electronics information and communication engineering- ICEICE No,6 Dec 2011.
[4] Gyudong Kim, Min-Kyu Kim, Byoung-Soo Chang, and Wonchan Kim – 1996,"Low-Voltage, Low-Power CMOS Delay Element, IEEE journal of solid state circuits,Vol 31,No 7, july 1996.
[5] J.Guajardo, S.Kumar,G,Schrijen, and P.Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in CHES, 2007, pp. 63-80.
[6] S.Kumar, J.Guajardo, R.Maes, G.-J, Schrijen, and P.Tuyls, "the butterfly PUF protecting IP on every FPGA," in HOST, 2008, pp 67-70.
[7] G.Suh and S. Devadas, "Physical UnclonableFuntions for device authentication and secret key generation," in DAC, 2007, pp, 9-14.
[8] M.Barai, S.SenGupta, and J.Biswas,"Dual mode multiple band digital controller for high frequency DC-DC converter," IEEE Tans, Power Electronics, vol. 24, no. 3, pp. 752-766, Mar.2009.
[9] M.Majzoobi, A.Elnably, and F.Koushanfar, "FPGA time-bounded unclonable authentication," in IH, 2010.
[10] U.Ruhmair, "SIMPL, system: on a public key variant of physical unclonable function," Cryptology ePrint Archive, 2009.
[11] N.Beckmann and M.Potkonjak, "Hardware-based public key cryptography with public physically unclonable functions," in IH,2009, pp.206-220.
[12] T.D.Burd and R.W..Brodersen, "Design issues for dynamic voltage scaling," in Proc. IEEE Int.Symp.Low power Electron. Des, pp 9-14.2010.