Proc. of the Intl. Conf. on Advances In Information Processing And Communication Technology - IPCT 2014.
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-77

A chip ID generation circuit – latch based

Alexandra Stanciu [1] , Marius Tudorancea [2] , Florin Moldoveanu [1]

***Abstract*—In this paper, we introduce a chip ID generation circuit, which uses process variations, that appear during the physical execution of an FPGA. In [1] Gassend et al. introduced for the first time the ROs digital circuit with the aim of emphasizing the uncontrollable effect of silicon process variations at the delay of the digital component interconnection. After that, different constructions based on process variations start to appear. The digital circuit analyzed is a modification of the latch based circuit with the scope to minimizing the hardware resource usage and to fit an FPGA implementation. We also introduce a new statistic assessment method based on Kolmogorov-Smirnov test for the inter-distance and the intra-distance analysis. The chip ID generation circuit could produce FPGA secret keys that deal with the security issues such as: cloning, overproducing or stealing the implemented applications on FPGA.**

***Keywords*—process variation, latch, FPGA, chip ID**

I. Introduction

Uncontrollable effects of silicon process variations appear during the manufacturing process of an integrated circuit. These variations are translated into random variations of electrical parameters that will negatively affect the yield of integrated circuits. The manufacturers try to develop measures to reduce these undesirable process variations as much as possible. However it is impossible to completely eliminate the silicon process variations. As a consequence, attempts to harness security advantage for integrated circuits start to appear. One type of constructions that uses process variations with security purpose are delay-based silicon circuits. Those circuits measure random variations on the delay of a digital circuit. Also the more advanced digital storage elements which are based on the bistability principle such as: latch, flip-flop, could be used to emphasize the process variations – named memory based silicon circuits [2] .

In our paper we focus on a latch digital circuit implemented on FPGAs devices. A chip ID generation circuit based on latch generally contains two cross-coupled NOR or NAND gates. By asserting a reset signal, this latch becomes unstable and after a while it converges to a stable state depending on the process variations.

Su et al. used for the first time the latch as a chip ID generation circuit in [1] for an ASIC implementation. Each ID cell comprises a latch (comparator) composed of cross-coupled logic gates. Initially, both sides of the latch (Set and Reset) are pulled low. As reset is lowered, each latch evaluates to a state determined by the mismatch of the comparator [1]. In [3] a design and implementation of a true random generator is presented, which exploits the metastability of RS latch, for an FPGA device. In case of an RS latch, it is generally prohibited to activate both R and S inputs simultaneously; if it happens, an RS latch may become metastable and generate an indefinite output. The random number generator with an RS latch is presented in Fig.1 [3]. In [4] the author's introduced a novel structure with random latches for generating high-entropy responses using randomness. Responses are generated using the location information of the latches. The proposed method considers the three types of output patterns from the RS latches as ternary values (00/11/01). The proposed structure has new detection circuits located after the RS latches which distinguishes these three types. The detection circuit i outputs a 2-bit unique value Si[1 : 0] (=00/11/10) depending on the output of the RS latch i (0s/1s/random numbers). If the output stream of the RS latch i includes a transition from 0(1) to 1(0), the detection circuit i considers the RS latch i as a random latch, and from that point onwards continues outputting the 2-bit value '10' regardless of RS latch i's subsequent output stream. For experimental results they used FPGAs [4]. The latch based circuit is very similar to the butterfly circuit. Instead of cross-coupling two inverters or two latches, two NOR/NAND gates are cross-coupled.

The effectiveness of the chip ID generation circuit based on latch fundamentally depends on the symmetry of interconnects between the two NAND/NOR gates. In an FPGA implementation it is difficult to satisfy this requirement. In [3] and [4] the authors describe how they manually placed and routed the latch circuit on FPGA without mentioning if identical and symmetrical interconnections between gates have been achieved. The variation of the absolute length of interconnections that appear in an FPGA implementation is mentioned in [12] where the authors introduce a highly accurate programmable delay line (PDL) for the existing chip ID generation circuit. However, in this paper we modified the chip ID generation circuit based on latch. Using this modification the circuit could be implemented on FPGA devices

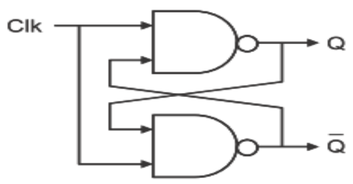

Fig. 1

Alexandra Stanciu, Florin Moldoveanu
"Transilvania" University of Brasov
Romania

Marius Tudorancea
Siemens SRL
Romania

By instantiating multiple chip ID generation circuits we created an identification sequence or a secret key for each FPGA device. The identification sequence could be used in a secure authentication technique to prevent FPGAs or IP cores cloning, overproducing FPGAs or IP cores and stealing the implemented application (bitstream) from an FPGA. In order to validate a secret key based on the intrinsic properties of an FPGA device, there are two mandatory metrics that a chip ID generation circuit must complete: reliability and uniqueness. Maes and Verbauwhede described two metrics that can be used to characterize these identification sequences. They introduced inter-distance as the Hamming distance between the identification sequences of two different chips that quantifies the uniqueness property. They also define intra-distance as the Hamming distance between two identification sequences generated on the same FPGA and under the same conditions that quantifies the reliability property. In this paper, we introduce a new statistic assessment technique based on Kolmogorov-Smirnov test to analyze the differences between FPGAs, differences generated by the process variations.

II. Latch based chip ID generation circuit

A. *Bistable latch circuit*

The latch is a circuit that has two stable states and can be used to store information. An example of an RS latch is presented in Fig. 2a. The circuit can be made to change state by signals applied to one or more control inputs and will have one or two outputs. The NAND gates could be replaced by NOR gates. In order to turn the latch into a chip ID generation circuit the two inputs R and S are connected to each other as shown in Fig. 2b. If a pulse is applied at the connected inputs, the RS latch becomes metastable and generates an indefinite output. The metastability appears only if the interconnects between gates are identical and symmetrical, that means: AB=A'B'and XY=XY'. Otherwise one of the outputs will be first set in 1, depending on the shortest length of the interconnections. To serve our purpose it is mandatory to have identical and symmetrical interconnects.

B. *FPGA Architecture and Resources*

Xilinx FPGA devices contain configurable logic components called "logic blocks" and reconfigurable interconnections. Every configurable logic block (CLB) contains a number of slices (usually 2 or 4). Every slice contains logic-function generator (look-up table or LUTs) and storage elements. Each CLB is surrounded by reconfigurable interconnections. Therefore, more CLB cells could be interconnected to perform complex digital circuits. The CLBs are fixed and the reconfigurable interconnects could be programmed in a limited number of possibilities. For example, there are over 100 arcs going into and coming out of each CLB.

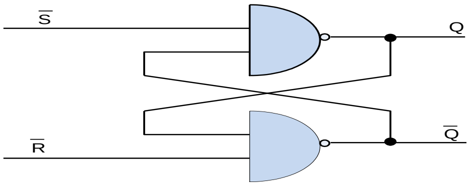

Fig. 2a

The majority of arcs are unidirectional, meaning they can only propagate a signal one way [5]. Even if the FPGA is a matrix of identical CLBs and a switch of programmable interconnections, surrounded by IO cells as shown in Fig 4, it is very difficult to obtain symmetrical interconnections. All the internal connections are made of metal segments linked to the connection points of the programmable switch. Each switch of programmable connections contains pass transistors used to connect the CLBs. At first glance the examination of the interconnections between CLBs appears promising: there exist direct routes to all adjacent CLBs in most of the FPGA. It also means that the potential for the required symmetry exists: a signal from CLB X1Y1 can be routed to CLB X2Y1, while a signal from CLB X2Y1 can be routed to CLB X1Y1 [5]. However, many practical attempts have led to the conclusion that it is almost impossible to have identical and symmetrical interconnections between CLBs. Moreover we rely only on estimates offered by Xilinx synthesis tools. Even if the interconnections appear to be symmetric in the FPGA design tool, we can draw no conclusion as to the delay of the route. Even near identical looking routes between slice A and slice B created by the routing software may differ in their estimated delay [5].

C. *Our proposed chip ID generation circuit*

Our proposed circuit is composed of the latch shown in Fig. 2b and a capture signal. The capture signal could be the terminal counter signal generated by a counter when it over- or underflows. Starting from the premise that interconnections between gates are identical and symmetrical and applying a high active signal on the circuit's input, the two outputs of the NAND gates will oscillate as shown in Fig. 3a. In reality, even with the NAND gates and the interconnections between them manually placed and routed, there will be differences between the interconnections, and the two outputs of the NAND gates will oscillates as shown in Fig. 3b or in Fig. 3c. On account of FPGA routing complexity and limitations, the delay differences between the interconnections start to appear. The output of the latch circuit is biased because of this inconvenient.

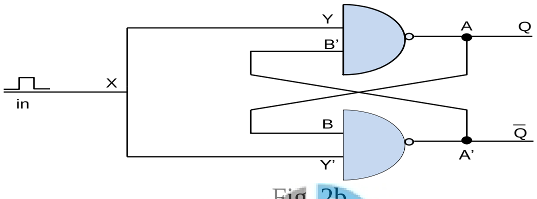

Fig. 2b

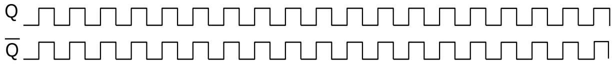

Fig. 3a

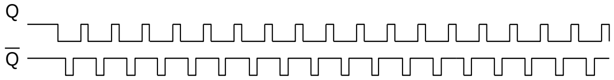

Fig. 3b

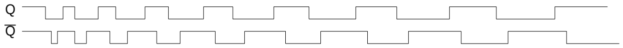

Fig. 3c

For the existing chip ID generation circuits based on silicon process variations the differences between interconnects are required to be exclusively dependent on the uncontrollable effect of the silicon process variations, so the output will be unpredictable. In order to obtain an unpredictable response from the latch, despite the delay differences, we oscillate the two NAND outputs for a period of time and capture their values in a moment specified by a capture signal. The oscillating period depends on how long the applied input is active high. Why does the output response depend on the process variations? Firstly, the signal's oscillating period T depends on the propagation time of the NAND gates t_{NAND}, on the propagation time of the interconnect routes $t_{\text{interconnects}}$ and on the process variations Δp_1. Secondly, the propagation time of the interconnect between the circuit that generates the oscillating signal and the NAND gates is also influenced by the process variations Δp_2. Thirdly, the propagation time of the interconnect between the circuit that generates the capture signal and the outputs of the NAND gates is also determined by the process variations Δp_3. The process variations from three distinct places $\Delta p_1, \Delta p_2, \Delta p_3$ determine the unpredictable response. The location information of the latches determines the differences between latch responses from the same FPGA or from different FPGAs. For this type of chip ID generation circuits the requirement for identical and symmetrical interconnections is not necessary. However, for better results, the difference between interconnects Δx must be infinitesimal, $\Delta x \to 0$. In order to claim that the proposed circuit is a chip ID generation circuit there are two mandatory constraints: 1) the response of the circuit instantiated on the same CLB to be unpredictable for different FPGA devices 2) the response of the circuit instantiated on the same CLB to be stable for a given FPGA device.

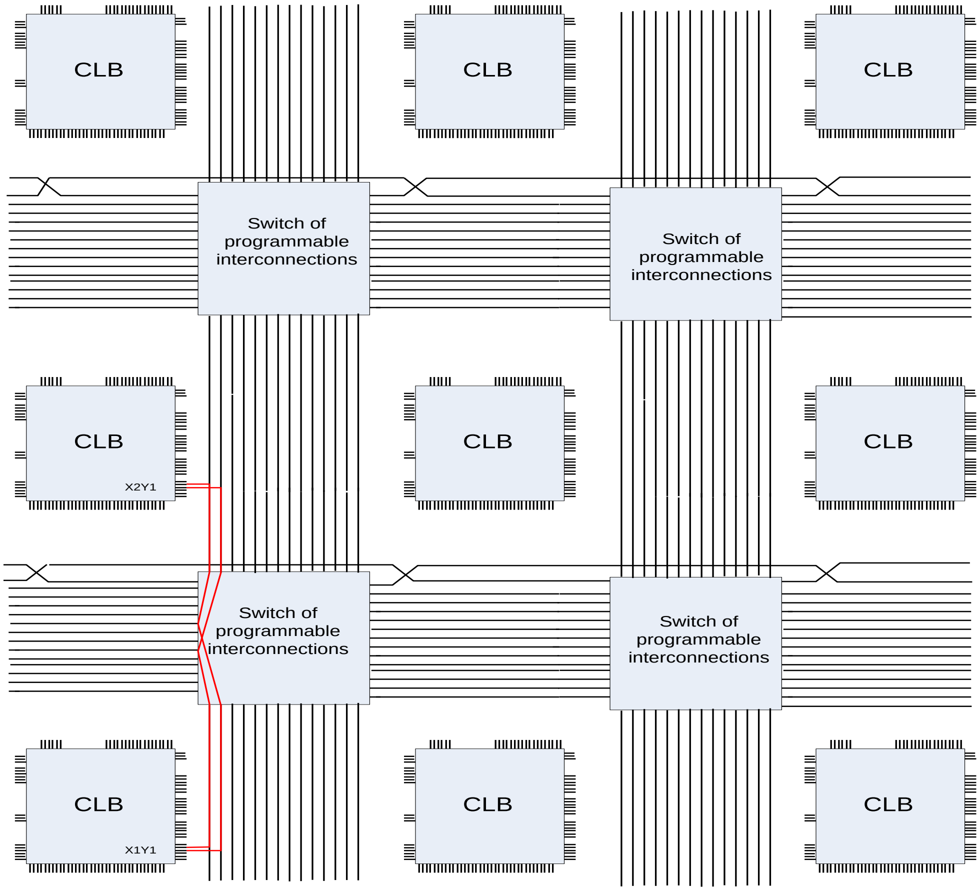
CLB
CLB
CLB
Switch of programmable interconnections
Switch of programmable interconnections
CLB
X2Y1
CLB
CLB
Switch of programmable interconnections
Switch of programmable interconnections
CLB
X1Y1
CLB
CLB

Fig. 4

Proc. of the Intl. Conf. on Advances In Information Processing And Communication Technology - IPCT 2014.
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-77

III. Generating a unique identifier for FPGA

In order to generate a unique identifier for FPGA devices, multiple circuits as we proposed in section II must be instantiated. How many circuits? It depends on how long the unique identifier should be. The chip ID generation circuit proposed in section II outputs one bit as a response. Fig. 5a shows an example of how multiple hard macros could be instantiated on FPGAs using the available hardware resources. Some timing and placing constraints must be considered in order to generate a unique identifier. Ideally the oscillating and capturing signals arrive at the same time to all the flip-flops. In practice this is impossible to achieve. In order to minimize the magnitude of the time difference between two events that would ideally occur simultaneously a signal distribution network must be implemented. The differences between the arrival times of oscillating signals result in differences between the beginnings of the periods of latch output oscillations, as shown in Fig. 5b. The capture signal jitter is generated by the differences between the arrival times. These are systematic variations and they also influence the responses of the chip ID generation circuits. In the absence of the process variations the latch output could be a stable response (0 or 1) or a random response owed to the metastability generated by the capture signal jitter. In case of a stable response, the result will be identical for a latch instance placed in a fixed location, on different FPGAs. In case of an unstable response, the result will be random on the same FPGA device or on different FPGA devices. Neither case is useful to generate a unique identifier. Also on the same FPGA the latch responses will differ from location to location because of the signal skew, signal jitter or asynchronous signals fan-out. But from FPGA to FPGA these responses will be identical in the absence of the process variations. Process variations is the naturally occurring variation in the attributes of transistors (length, widths, oxide thickness) when integrated circuits are fabricated [6].

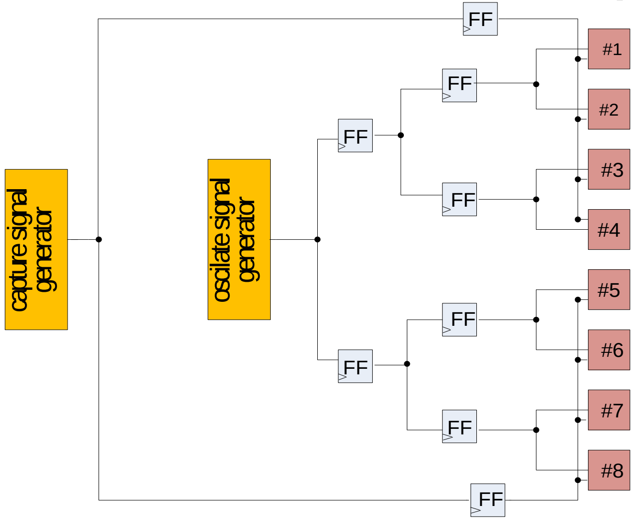

Fig. 5a

Minimizing the deterministic differences caused by signal skew or jitter and emphasizing the process variations, leads to the latch's responses being unpredictable, almost stable from a latch instance on the same FPGA, and different for distinct FPGA devices. The latch response depends on the local process variations that appear on interconnections between gates and on the global process variations that appear on interconnections between oscillate/capture circuits and latch.

IV. A Test Statistic for measuring FPGAs inter-distance

We need to specify statistical hypotheses which are statements about theoretical models or about probability or sampling distributions. One hypothesis of interest in our study is whether chips are different from each other [9]. Kim et al. motivated in [9] the need for a new test statistic for verifying the hypothesis, H0: the distribution of any two chips is the same vs Ha: the distribution of some two chips is different. They used two statistical methods: bootstrap - based confidence interval and Kolmogorov - Smirnov test. In our paper we developed a test statistic for computing the distribution of an FPGA and then used the Kolmogorov – Smirnov test to compare distributions from different FPGAs.

We consider the chip ID generation circuit instantiated everywhere on FPGA and collect their responses from entire FPGA surface. We finally obtain a binary matrix for each FPGA. We compute the statistical mean on this binary matrix and compare the statistical means of different distributions in order to test if the FPGAs are different. We did this for 3 FPGA devices and obtained the next values for the statistical mean: FPGA1:0.350847, FPGA2:0.391525, FPGA3:0.398305. As you can see, the three averages are close in values. In case of a large number of FPGAs, it is hard to tell whether they are different from each other only by statistical mean. Two FPGAs could have the same values of one but their distribution to be distinct, and in this case the two FPGAs are not identical. In order to obtain the distribution of an FPGA we consider an NxN window. We place the NxN window on each location of the binary matrix and with the values comprised in this window we compute the statistical average. We also applied other statistical tests on the values within NxN window such as: frequency test, cumulative sums or other NIST tests. The NIST tests involve determining whether or not a specific sequence of zeroes and ones is random. With the value from the statistical test applied on the NxN window we obtain a new RxC matrix, which we call the Q distribution of an FPGA device.

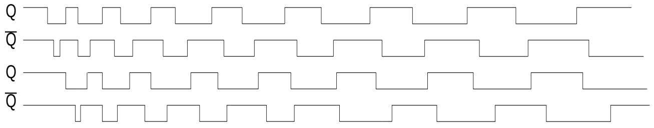

Fig. 5b

ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-77

Firstly we applied the Kolmogorov – Smirnov test to verify if this distribution is a normal distribution. In case of a negative response we use Kolmogorov – Smirnov method to compare the two distributions. In case of a positive response we can choose a parametric test to verify if two FPGAs have identical distributions.

Kolmogorov – Smirnov test can be applied on FPGAs statistical distributions in order to verify if two distributions differ. It is a nonparametric test which means that it has the advantage of making no assumption about the distribution of data. The Kolmogorov – Smirnov statistic quantifies the distance between two distributions of Q values obtained from two chips. If the distance is larger than a critical value of the Kolmogorov distribution, we take the decision to reject H0 which means that there is statistical evidence that the two chips are different [9].

V. Experimental results

A. *FPGA implementation for chip ID generation circuit*

The circuit shown in Fig. 6 was implemented on a Spartan 6 XC6SLX45 FPGA. The NAND gates and interconnections between them were manually placed and routed. The chip ID generation circuit was constructed as a hard macro. The wire interconnections between the circuits that generate the oscillator signal and capture signal were routed using the Xilinx tool chain. In order to minimize the oscillator signal skew and capture signal skew we synchronize these signals with flip flops. We counted on the fact that the Xilinx Place and Route (PAR) tool exploits the rich interconnect array to deliver optimal system performance.[7] The interconnections between synchronization flip flops and latch were also manually routed. The propagation delays on interconnections depicted in Fig. 5 are estimated by the Xilinx FPGA Editor tool. Based on this estimation, after many attempts we succeeded to have identical propagation delays on AB and A'B' interconnections. We also obtained a minimum difference between XY and XY' interconnections. We tried to unsuccessfully route identical XY and XY' interconnection. However on a real hardware FPGA we could not be certain of the fact that these interconnections have the propagation delay provided by the Xilinx FPGA Editor tool.

In order to evaluate the chip ID generation circuit we measured the Hamming intra- and inter-distance.

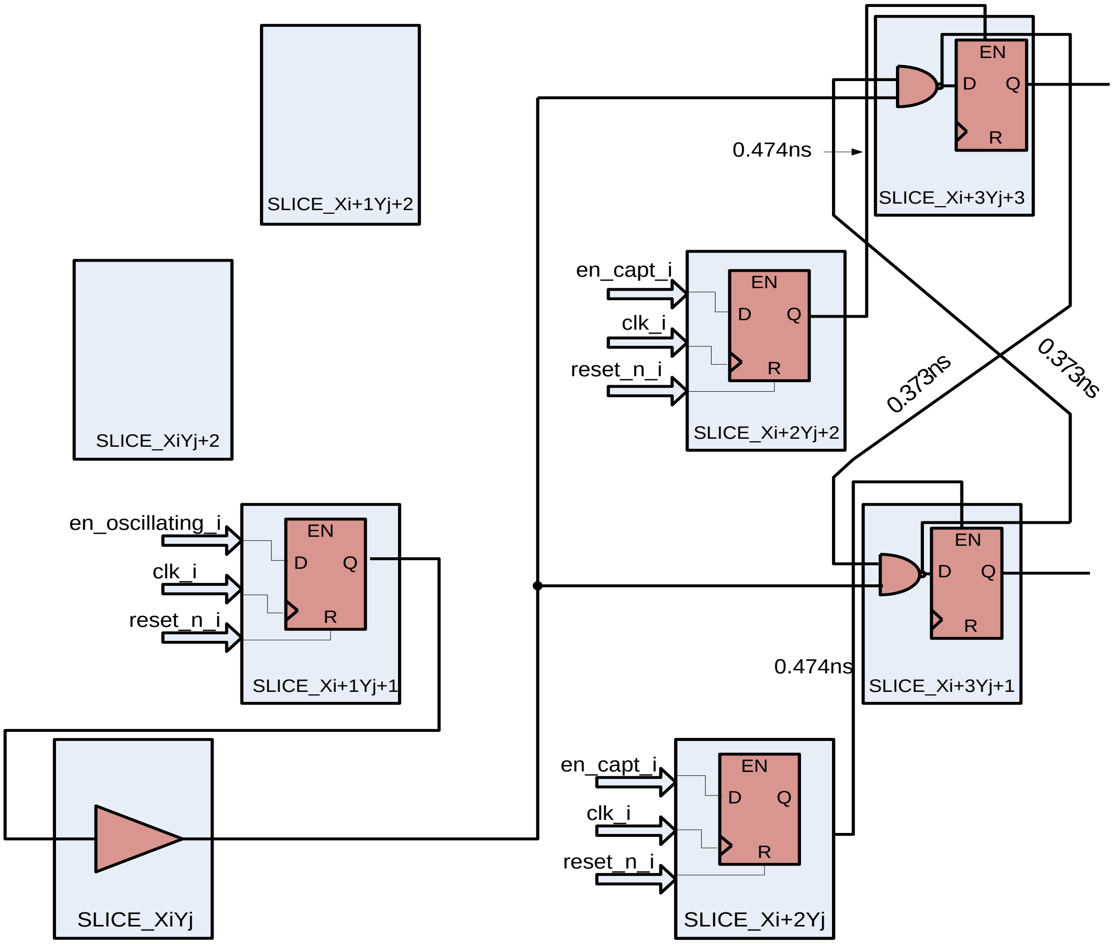

Fig. 6

Considering that the FPGA is a CLB matrix, chip ID generation circuits were instantiated on each row. The number of circuits on each row is presented in Fig. 7. At a certain time, circuits were instantiated only on a row together with the generator circuits for capturing and oscillating signal, as shown in Fig. 5a. The circuit results were captured with a logic analyzer. We used three identical FPGA devices XC6SLX45.

10 measurements were done for each row in order to compute the intra-distance. For each FPGA, the collected responses obtained at the first running formed the identification sequence. The means of distinct bits between the identifier and the values form other 9 measurements were calculated for each row. As shown in Table 1, there are on average 4.5 undetermined bits from a total of 51 bits. It is a satisfactory situation, considering that the undetermined bits could be corrected with an error detection and correction algorithm.

In order to evaluate if the FPGAs have different distributions obtained with the circuits proposed by us, we applied the Kolmogorov – Smirnov test, which was described in Section IV. The Monobit Frequency test was used to compute the FPGA distribution. The purpose of this test is to determine whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence [11]. We considered NxN window with different sizes: N=5, N=7 and N=9. As shown in Table 2 the results are satisfactory - the distribution of some two chips is different. The FPGA distributions are different when the Kolmogorov-Smirnov statistic $D_{n,n'}$ meet the condition: $D_{n,n'} > c(\alpha)\sqrt{\frac{n+n'}{nn}}$, where n and n' represents the size of the compared distribution and $c(\alpha)$ is given for each critical value α in scientific tables.

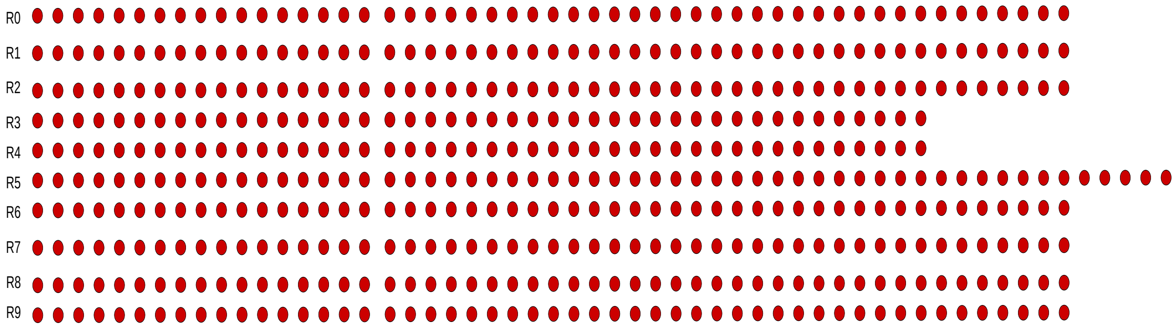

Fig. 7. The number of chip ID generation circuits on each row: R0-51, R1-51, R2-51, R3-44, R4-44, R5-56, R6-51, R7-51, R8-51, R9-51, R10-51

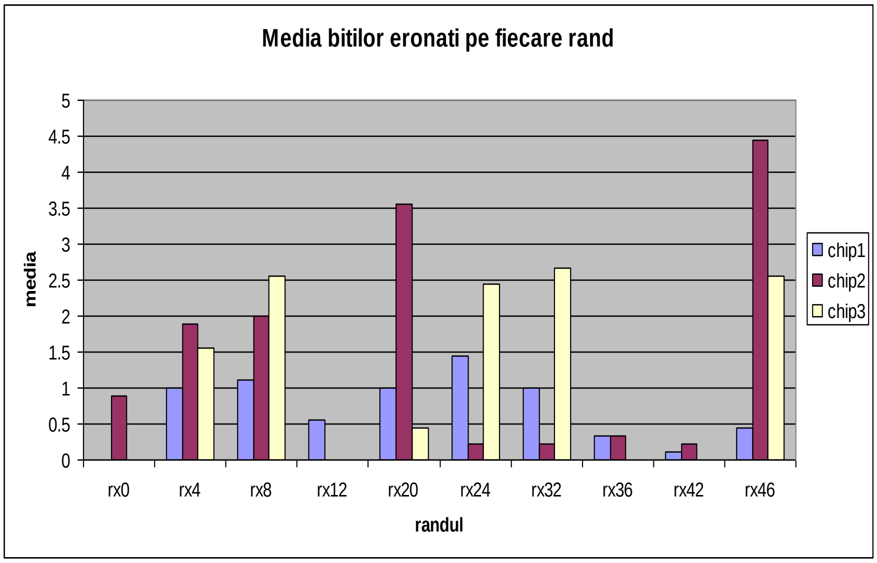

Table 1

Chip #	Chip #	$D_{n,n'}$	α	$c(\alpha)$	$c(\alpha)\sqrt{\frac{n+n'}{n*n'}}$	Different chips?
1	2	0,179012346	0.001	1.95	0.00007	Yes
	3	0,262345679				Yes
2	3	0,089506173				Yes

Table 2 FPGA Distributions computed with 5x5 Window and n=n$'$ = 324

VI. Conclusion

In this paper we introduced a chip ID generation circuit based on the digital latch, which constitute a physical circuit feature that can be embedded in an FPGA structure. For a given model, identical ICs have small unpredictable differences due to random variations in the manufacturing process. Emphasizing the process variations we could create identification sequences with the purpose of uniquely identifying an FPGA for detection of counterfeit products, protection against software piracy, and protection of FPGA design Intellectual Property (IP). According to the experimental results we succeeded to validate the use of the chip ID generation circuit to generate a unique identifier for FPGA chips, in normal conditions. As future work we also intend to analyze the effects of other factors that may influence integrated circuits identifier(ageing, voltage and temperature fluctuations).

Acknowledgment

This paper is supported by the Sectoral Operational Programme Human Resources Development (SOP HRD), ID137070 financed from the European Social Fund and by the Romanian Government.

References

[1] Y. Su, J. Holleman, B. Ottis, "A 1.6pJ 96% Stable Chip-ID Generating Circuit using Process Variations,". In IEEE Interanational Solid-State Circuits Conference – ISSCC 2007

[2] R. Maes, "Physically Unclonable Functions: Constructions, Properties and Applications," Phd Thesis, Katholieke Universiteit Leuven – Faculty of Engineering, Belgia, 2012

[3] H. Hata, S. Ichikawa, "FPGA Implementation of metastability-based true random number generator", IEICE Trans. 95-D(2), 426-436(2012)

[4] D. Yamamoto et al. "Variety enhancement of PUF responses using the locations of random outputting RS latches"

[5] S. Morozov, A. Maiti, P. Schaumont, ''A Comparative Analysis of Delay Based PUF Implementation on FPGA", Virginia Polytechnic Insitute and State University

[6] Wikipedia, Process Variations

[7] Xilinx Support Documentation

[8] R. Maes, I. Verbauwhede, "Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions", book chapter in "Towards Hardware-Intrinsic Security"

[9] I. Kim et al, "From Statistics to Circuits: Foundations for Future Physical Unclonable Functions", book chapter in "Towards Hardware-Intrinsic Security"

[10] A. Sadeghi and D. Naccache, "Towards Hardware-Intrinsic Security," Springer, 2010

[11] A. Rukhin et al. , "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", NIST Special Publications, April 2010

[12] M. Majzoobi, F. Koushanfar, and S. Devadas, "FPGA PUF using programmable delay lines," in IEEE Workshop on Infotmation Forensics and Security(WIFS), 2010

About Author (s):

Alexandra Stanciu is a first year doctoral student active in the System Engineering research field at the "Transilvania" University of Brasov, Romania. The working title of her thesis is "Security in digital electronic systems". Her research is focused on trusted systems on chip with untrusted IP cores. She holds a diploma in Computers and a master degree in Electronics and Communications Integrated Systems both from the "Transilvania" University of Brasov. She is also with Siemens Corporate Technology as a scholar since 2010.

Marius Tudorancea has received Bachelor and Master of Science degrees in Electronics and Computers Science, respectively, Electronic Design Automation from Transilvania University in 2001 and 2002. He joined Siemens in 2004 after he gained experience in ASIC and FPGA development. Currently, he is part of "Electronics Technology Field" within Siemens Corporate Technology.

Florin Moldoveanu received the B. Sc., and Ph. D. degrees in electrical engineering from Transilvania University of Brasov, Romania, in 1975 and 1998, respectively. He is currently Professor as part of the Department of Automation and Information Technology, Faculty of Electrical Engineering and Computer Science, Transilvania University of Brasov. His main research interests focus on digital circuits, discret event systems, sliding mode control, digital image processing