20th IMEKO TC4 International Symposium and
18th International Workshop on ADC Modelling and Testing
Research on Electric and Electronic Measurement for the Economic Upturn
Benevento, Italy, September 15-17, 2014

Simulation, Measurement and Test Environment for Pseudo Random Number Generator Circuits

Galia Marinova[1], Zdravka Tchobanova[2]

[1,2]*Technical University-Sofia, Telecommunications faculty, Sofia-1612, 8, boul."Kliment Ohridski", Bulgaria, gim@tu-sofia.bg, zchobanova@gmail.com*

***Abstract* – The paper presents an environment and methodology for analysis of Pseudo random bit sequence generator (PRBSG) and Pseudo random number generator (PRNG) circuits through simulation and measurement. Circuits' projects are described in VHDL and then simulated on FPGA devices. The programmed FPGAs are stimulated by vector signal generator and then measured with a logic analyzer. The bit sequences generated by the PRBSG circuits are tested for randomness with tests from the NIST test suit. The random numbers generated by the PRNG circuits are tested through histograms and chi-square tests for uniform distribution.**

I. INTRODUCTION

Pseudo random bit sequence generators (PRBSG) and pseudo random number generators (PRNG) are of great interest in communications. They have important applications in cryptography, adaptive filter coefficients calculation in equalizers, noise generation in measurement instruments and recently in analog to information converters. An implementation for emulating real traffic data transmission, using DPSK modulation format with two levels of phase, is presented in [1]. PRBSG and PRNG performance tests are defined in NIST(National Institute of Standardization and Technology) test suit [2,3] and later reviewed in [4]. In [5] an ASIC design hardware solution for PRNGs is proposed. In [6] PRNGs are studied through MATLAB simulations. The paper is focused on hardware implementation of PRBSG and PRNG circuits and their performance estimation. An environment for analysis of PRBSG and PRNG circuits through simulation and measurement is proposed. First circuits' projects are described in VHDL and then simulated on FPGA devices. The programmed FPGAs are stimulated by vector signal generator and then measured with a logic analyzer. The bit sequences generated by the PRBSG circuits are tested for randomness with tests from the NIST test suit. The random numbers generated by the PRNG circuits are tested through histograms and chi-square tests for uniform distribution. Four circuits with applications for PRBSG and 5 applications for PRNG are tested – 8-bit Galois LFSR and 9-bit Fibonacci LFSR, used for 8 bits and 9 bits numbers generation, 16 bits and 21 bits Fibonacci LFSR used for 8 bits generation. The Fibonacci LFSR circuits correspond to the PRNG circuits in the signal vector generator SMIQ 03B ROHDE&SCHWARZ [7]. In Section II are described the environment and 4 PRBSG circuits. In Section III are presented the simulations and tests of the PRBSG/PRNGs and in Section IV – the measurement results. Some conclusions are formulated for the performances of the circuits.

II. ENVIRONMENT AND PRBSG/PRNG CIRCUITS

A. Environment for PRBSG/PRNG

The environment for simulation, measurement and test of PRBSG/PRNG circuits integrates:

- FPGA VIRTEX 2 and development board DS-KITV2LC1000, Platform cable USB XILINX, 5V 2A power supply**;**
- ISE simulator;
- Portable LOGIC ANALYZER MAX – 8100;
- VECTOR SIGNAL GENERATOR SMIQ 03B ROHDE&SCHWARZ from 300 kHz to 3.3 GHz;
- NIST test suit and appropriate MATLAB programs, implementing the NIST tests;
- PRNG chi-squaretest for uniform distribution and appropriate MATLAB program implementing it;
- Histogram builder in MS-EXCEL, for the pseudo random numbers generated.

B. PRBSG/PRNG circuits

Four basic PRBSG/PRNG circuits are considered:

- PRBSG circuit realized as 8-bit Galois LFSR is shown on Fig.1. The Galois circuit has 3 internal XORs.

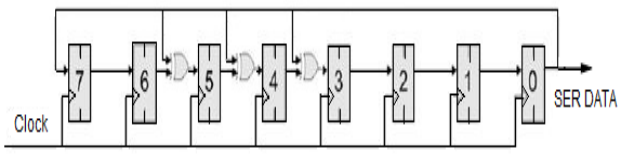

Fig. 1. PRBSG as 8-bit Galois LFSR

ISBN-14: 978-92-990073-2-7

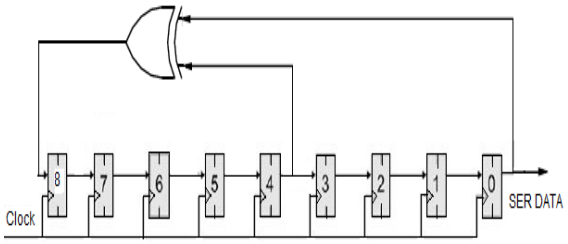

Fig. 2. PRBSG as 9-bit Fibonacci LFSR used in SMIQ03B signal vector generator

The PRBSG circuit realized as 9-bit Fibonacci LFSR is presented on Fig 2. This circuit is implemented in the SMIQ03B signal vector generator [7], so it's named SMIQ9bits circuit in the paper.

The circuit has feedback at registers 4 and 0. In SMIQ03B signal vector generator this circuit is used for the QPSK modulation. The other PRBS generators in SMIQ03B from [7] are presented in Table 1, where generated sequences lengths and feedback tap positions are indicated.

Table 1. PRBS Generators in SMIQ03B ROHDE&SCHWARZ

PRBS Generator	Length in bit	Feedback to
9 bits*	2^9-1=511	Register 4,0
15 bits	2^{15}-1=32767	Register 1,0
16 bits*	2^{16}-1=65535	Register 5,3,2,0
20 bits	2^{20}-1=1048575	Register 3,0
21 bits*	2^{21}-1=2097151	Register 2,0
23 bits	2^{23}-1=8388607	Register 5,0

* - these circuits are studied in the paper.

The study which follows can be applied for each one of the circuits in Table 1.

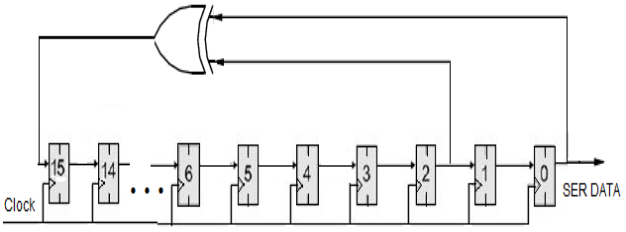

Fig. 3. PRBSG as 16-bit Fibonacci LFSR used in SMIQ03B signal vector generator

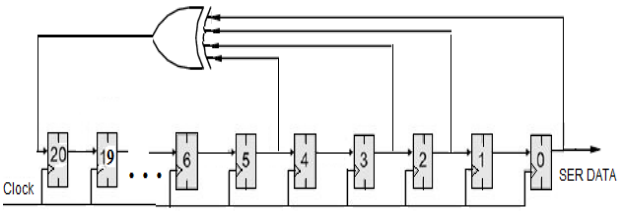

Fig. 4. PRBSG as 21-bit Fibonacci LFSR used in SMIQ03B signal vector generator

The PRBSGs realized as 16 bits and 21 bits Fibonacci LFSRs, from Table 1 are presented on Fig.3 and Fig. 4.

III. PRBSG/PRNG CIRCUITS SIMULATION AND TESTS

A. Simulation of PRBSG/PRNG Circuits

The Galois and the 3 SMIQ circuits are described in VHDL code with D flip-flops and then simulated in ISE on VIRTEX 2 FPGA. PRBSG versions of Galois and SMIQ9bits circuits are stimulated with 1 MHz clock stimulus and the output bit is simulated and presented on the waveforms on Figs.5a,5b. The bit sequences generated are stored and tested for randomness.

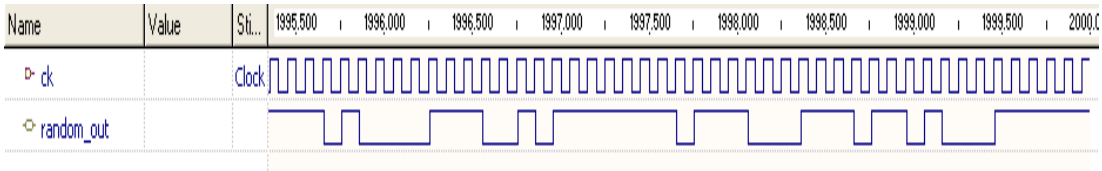

Fig. 5a. Simulation of bit sequence generated by PRBSG Galois

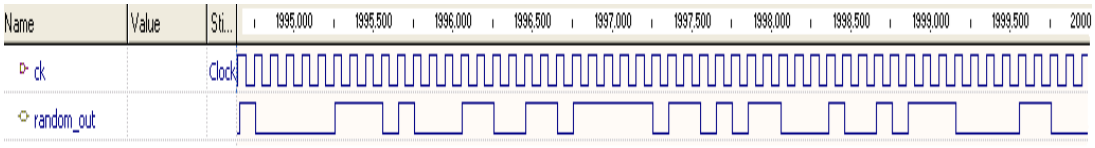

Fig. 5b. Simulation of bit sequence generated by PRBSG SMIQ9bits

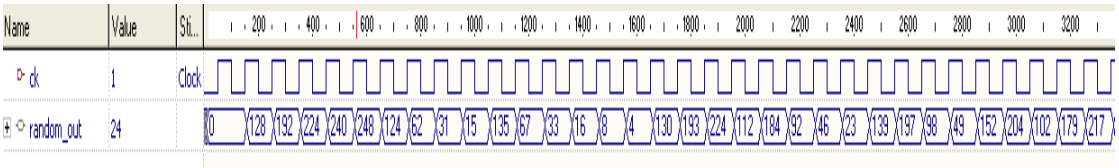

Fig. 6a. Simulation of random 8-bit sequence generated by PRNG Galois

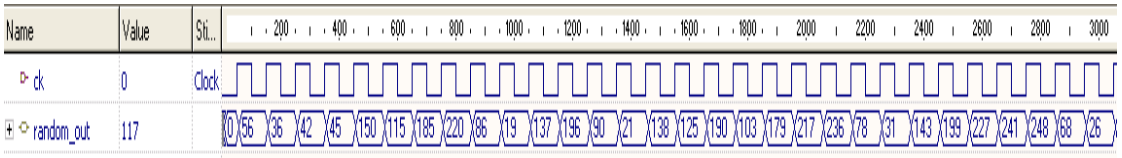

Fig. 6b. Simulation of random 8-bit sequence generated by PRNG SMIQ9bits

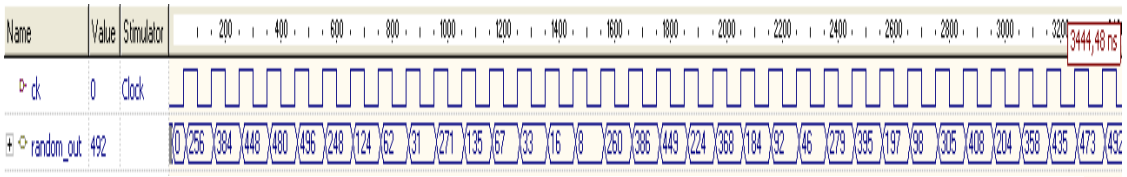

Fig. 6c. Simulation of random 9-bit sequence generated by PRNG SMIQ9bits

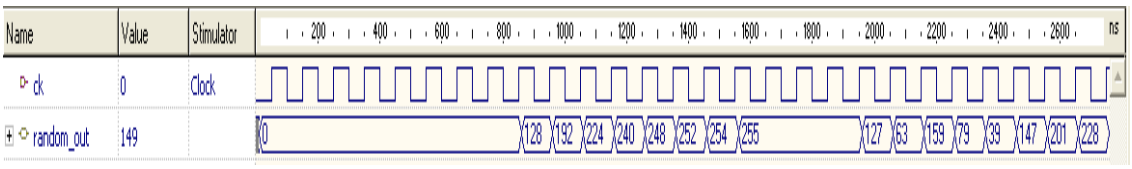

Fig. 6d. Simulation of random 8-bit sequence generated by PRNG SMIQ16bits

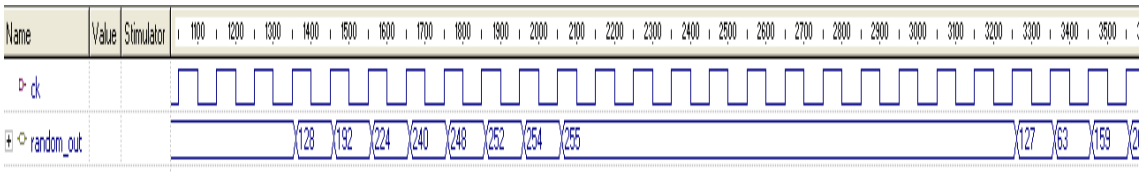

Fig. 6e. Simulation of random 8-bit sequence generated by PRNG SMIQ21bits

All four circuits are simulated and the output is taken as 8-bit randm numbers generated. The circuit SMIQ9bits has also a version with 9-bit numbers generated. The generated sequences of pseudo-random numbers obtained through simulation are presented on Figs.6a,6b,6c,6d,6e. The beginning of the sequence for each SMIQ PRBSG is given in [7] and sequences obtained through simulation coincide fully with them.

C.Tests of the generated pseudo random bit sequences

Three tests from NIST test suit[2] are applied to four circuits from Figs.1,2,3,4 – the Frequency (Monobit) test, the Runs test and the Spectral test.

- **Frequency (Monobit) Test**

This is the first test from the NIST suit and it determines whether the number of 0's and 1's in the sequence generated, is close to this in a truly random sequence, where the numbers of 0's and 1's should be nearly equal. The parameters in this test are:

ε – bit sequence generated by the circuit;

$\varepsilon = \varepsilon_1, \varepsilon_2, ..., \varepsilon_n$, n – number of bits in the sequence under test; X_i – Elements with values ± 1, where $X_i = 2\varepsilon_i - 1$

S_{obs} – absolute value of the sum of X_i, divided by the square root of n. S_n – sum of the values X_i. erfc - Complementary Error Function. The reference distribution is half normal. The test steps are:

Step 1. X_i are calculated: 0's and 1's in the sequence (ε) are transformed in -1 and +1, and summed:

$$S_n = X_1 + X_2 + ... + X_n, \text{ where } X_i = 2\varepsilon_i - 1. \quad (1)$$

Step 2. S_{obs} is calculated:

$$S_{obs} = \frac{|S_n|}{\sqrt{n}} \qquad (2)$$

Step 3. The P-value is calculated

$$\text{P-value} = \text{erfc}\left(\frac{S_{obs}}{\sqrt{2}}\right) = \frac{2}{\sqrt{\pi}} \int_z^{\infty} e^{-u^2} du. \qquad (3)$$

If P-value<0,01, the sequence is not random, else if P-value>0,01, the sequence is random.

P-value<0.01 when values of S_n or S_{obs} are big. When S_n is a big positive value, the sequence has too many 1's, when S_n is a big negative value, 0's are too many.

The results from the Frequency (Monobit) test for the sequences of 1000 bits generated by the circuits from Figs.1,2, 3,4 are presented in Table 2.

Table 2. Results from the Frequency test

Test parameter	Galois circuit	SMIQ 9bits circuit	SMIQ 16bits circuit	SMIQ 21bits circuit
n	1000	1000	1000	1000
Nbr of 1's	521	496	490	692
Nbr of 0's	479	504	510	308
Sn	42	-8	-20	384
Sobs	1.3281	0.2530	0.6325	12.1431
P-value	0.1841	0.8003	0.5271	6.24e-34

For the circuits Galois, SMIQ 9 bits, and SMIQ16 bits from Figs.1,2,3 :

Nbr 1-s ≈ Nbr 0-s and P-value>0.01.

These PRBSG circuits pass the Frequency (Monobit) test. For the SMIQ21bits circuit P-value<0.01 and this circuit fails the test.

- **Runs Test**

This test focuses on the number of runs which represent uninterrupted sequences of identical bits in the sequence generated. K is the length of the runs. The goal is to determine the number of runs of 0's and 1's corresponding to a random sequence. This test shows how fast or slow are the oscillations between 0's and 1's.

The main parameter in this test is:

$V_n(obs)$: - Total number of runs in the sequence.

The referent distribution is chi-square χ^2.

The test steps are:

Step 1. A pre-request for performing Runs test is that the sequence have passed the Frequency test.

The pre-test proportion π of ones in the sequence is calculated as:

$$\pi = \frac{\sum_j \varepsilon_j}{n}. \qquad (4)$$

Verification is done whether the Frequency test is satisfied: If it can be proved that $|\pi - ½| \geq \tau$, then the Runs test is not performed. In this case the P-value is tuned to 0.0000. For this test, $\tau = \frac{2}{\sqrt{n}}$ is predefined in the test code.

Step 2. Then $V_n(obs)$ is calculated:

$$V_n(obs) = \sum_{k=1}^{n-1} r(k) + 1 \qquad (5)$$

where r(k)=0, if $\varepsilon_k = \varepsilon_{k+1}$, else r(k)=1.

Step 3. *P-value* is calculated:

$$P\text{-}value = erfc\left(\frac{|V_n(obs) - 2n\pi(1-\pi)|}{2\sqrt{2n\pi(1-\pi)}}\right) \qquad (6)$$

Table 3. Results from the Runs test

Test parameter	Galois circuit	SMIQ9bits circuit
N	256	256
Nbr of 1-s	127	129
Nbr of 0-s	129	127
$\tau = \frac{2}{\sqrt{n}}$	0.125	0.125
$\pi = \frac{\sum_j \varepsilon_j}{n}$	0.49609375	0.50390625
$\lvert\pi - ½\rvert$	0.00390625	0.00390625
$V_n(obs) = \sum_{k=1}^{n-1} r(k) + 1$	129	127
$\frac{\lvert V_n(obs) - 2n\pi(1-\pi)\rvert}{2\sqrt{2n\pi(1-\pi)}}$	0,089084319	0,087703167
P-value	0.9	0.901

A big value for V_n(obs) means too fast oscillations in the sequence, a small value for V_n(obs) means too slow oscillations in the sequence. The sequence to be tested should have at least 100 bits ($n \geq 100$).

If P-value>0.01, the sequence is random.

The results from the Runs test on the sequences of 256 bits generated by the circuits from Fig.1 and Fig.2 are presented in Table 2.

The PRBSG circuits from Fig.4 is not studied with runs test because it doesn't meet the Frequency test which is a precondition. The circuits from Figs.1,2,3 generate random sequences, since P-value>0.01 for all.

- **Spectral test**

The test verifies the peak heights in the DFT of the sequence, through counting the number of peaks above the 95% threshold. If this number is not above 5% then the sequence is considered random. The test is described in [2]. A MATLAB program is developed to verify this test. A P_{value} for each sequence is calculated through ***ercf*** function. If P_{value}>0.01 then the sequence is considered random.

A MATLAB program is developed to verify this test. The bit sequences generated from the 4 PRBS generators are estimated by the Spectral test. On Figs.7a,7b,7c,7d are presented the spectrums of the bit sequences and the 95% threshold for each one.

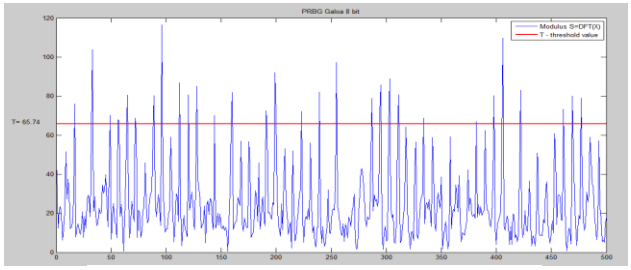

Fig. 7a. Spectrum of the Galois PRBSG

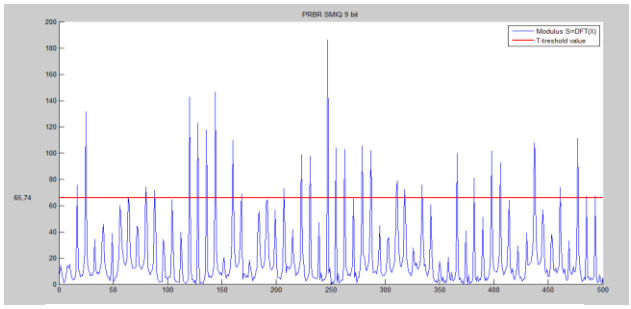

Fig. 7b. Spectrum of the SMIQ9bits PRBSG

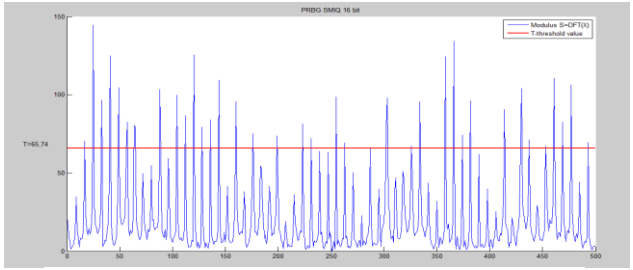

Fig. 7c. Spectrum of the SMIQ16 bits PRBSG

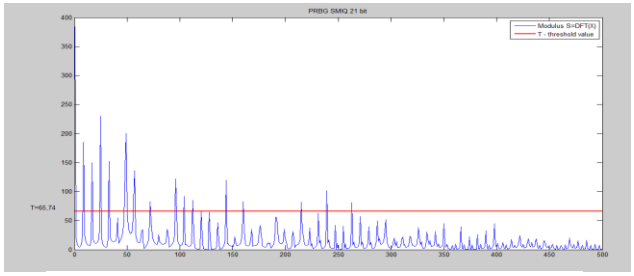

Fig. 7d. Spectrum of the SMOQ21bits PRBSG

In Table 4 n is the number of bits in the sequence, T is the 95% threshold of the height of a peak, N_o is the expected theoretical number of peaks above the threshold, N_1 is the observed number of peaks above the threshold, d is the normalized difference between the observed and the expected number of frequency components that are beyond the 95% threshold.

Table 4. Results from the Spectral test

PRBSG	Galois 8bits	SMIQ 9bits	SMIQ 16bits	SMIQ 21bits
n -Number of bits	1000	1000	1000	1000
$T = \sqrt{\left(\log \frac{1}{0,05}\right) n}$	65.74	65.74	65.74	65.74
$N_0 = 0.95n/2$	475	475	475	475
N_1- observed	467	467	461	480
$d = \frac{(N_1 - N_0)}{\sqrt{n.0,95.0,05/4}}$	-2.3215	-1.3215	-4.0627	1.4509
$P_{value}=erfc\left(\frac{\lvert d \rvert}{\sqrt{2}}\right)$	0.0203	0.1468	0.000048	0.1468
$P_{value}>0.01$	Yes	Yes	No	Yes

The results from the Spectral test show that the bit sequences generated by the PRBSG Galois8bits, SMIQ9bits and SMIQ21bits are random and the bit sequence of the PRBSG SMIQ16bits is not random. Repetitive patterns near each other might be available in this sequence.

- **Tests of the generated pseudo random numbers sequences**

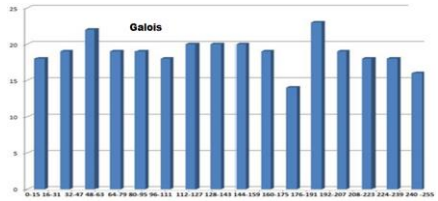

Fig. 8a. Histogram of the 8-bit random numbers generated by Galois circuit

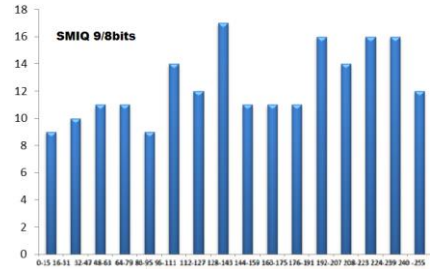

Fig. 8b. Histogram of the 8-bit random numbers generated by SMIQ9bits circuit

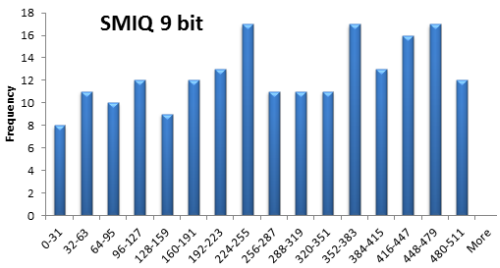

Fig. 8c. Histogram of the 9-bit random numbers generated by SMIQ9bits circuit

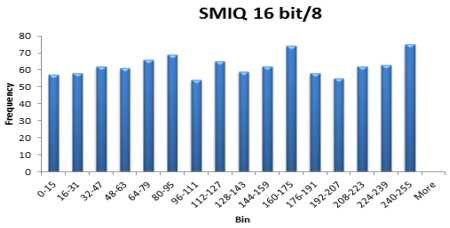

Fig. 8d. Histogram of the 8-bit random numbers generated by SMIQ16 bits circuit

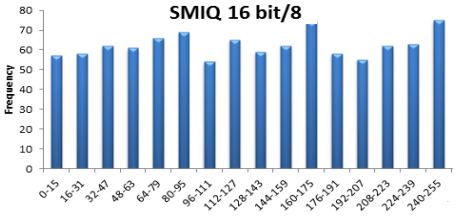

Fig. 8e. Histogram of the 8-bit random numbers generated by SMIQ21bits circuit

The 8-bit random numbers generated by the Galois and SMIQ circuits are retrieved from the simulations on Figs. 6a,6b,6c,6d,6e. Histograms are built with MS-EXCEL for 200 random numbers generated and they are shown on Figs. 8a,8b,8c,8d,8e. The 5 sequences are tested for uniformity through the chi square test $\chi^2_{16-1}(c,\infty) = 0{,}05$ with critical value c=25. The results for the chi-square test for uniformity are shown in Table 5. The circuit SMIQ21bits does nor pass the test for uniformity. All the other circuits generate uniformly distributed pseudo random numbers. The conclusion from the tests is that Galois and SMIQ9bits circuits pass all the tests for randomness and they generate uniformly distributed 8-bit/9-bit numbers. The SMIQ16bits circuit fails the Spectral test but still generates uniformly distributed 8-bit numbers. The SMIQ21bits circuit passes only the Spectral test and fails all the other tests. The 8-bit numbers it generates are not uniformly distributed.

Table 5. Results from the chi-square test for uniformity

PRNG	T	T<25?
Galois 8bits	2.40	Yes
SMIQ 9bits/8bits	8.32	Yes
SMIQ 9bits	9.76	Yes
SMIQ 16bits	9.02	Yes
SMIQ 21bits	347.62	No

IV. PRBSG/PRNG CIRCUITS MEASUREMENT IN THE ENVIRONMENT

Finally the PRBSG circuits are programmed on VIRTEX 2 FPGA. They are stimulated by 1MHz clock signal from the signal vector generator and generated sequences are measured on the logic analyzer as shown on Figs.9a,b. Sequences generated from each one of the PRNGs are stored on the logic analyzer and it's verified that they coincide the simulated sequences from Figs.6a,6b,6c,6d,6e for each circuit.

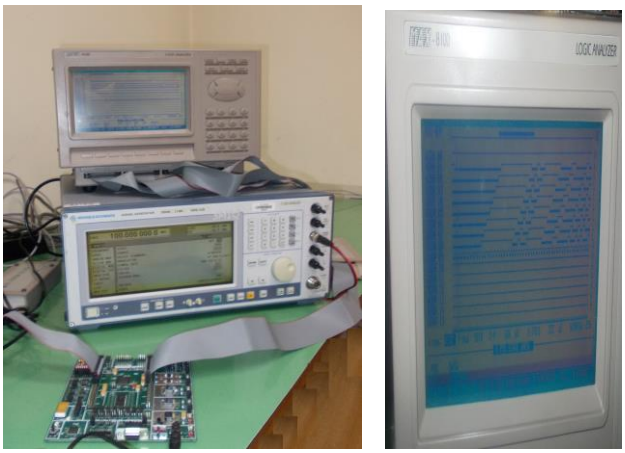

Fig 9a. Measurement of the PRBSG SMIQ circuit programmed on FPGA. Fig.9b. Measured 8 bits pseudo random numbers generated by PRBSG SMIQ16 bits

V. CONCLUSION

The environment proposed in the paper permits the simulation, measurement and test of different kinds of PRBSG/PRNG circuits through a methodology for their performance estimation in order to select the most suitable circuit for a concrete hardware application, especially in communications.

REFERENCES

[1] H. Badaoui et al., "PRBS Analysis for the Modeling of Optical DPSK Transmission Systems", Int. J. of C.Sc&C., Vol.1, No2, July-Dec.2010, pp.369-372

[2] A. Rukhin et al., Revised: April2010 L.E. Bassham III, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", NIST Special Publication 800-22 revision 1a Natl. Inst. Stand. Technol. Spec. Publ. 800-22rev1a, (April 2010)

[3] U. Maurer, "A Universal Statistical Test for Random bit Generators", J. of Cryptology, vol.5, no.2, 1992, pp.89-105

[4] J.K.M. Sadique Uz Zaman, R. Ghosh, "Review on fifteen Statistical Tests proposed by NIST", *IJTPC, Vol. 1, November 2012.*, www.IJTPC.org, pp.18-31

[5] E. Laskin, S.P. Voinigescu, "A 60mW per Lane, 4x23-Gb/S, 27-1 PRBS Generators", IEEE J. of solid-state circuits, Vol.41, No1, Oct. 2006, pp.2198-2208

[6] A. Čitavičius, A. Jonavičius, "Analysis of Unpredictable Cryptographic Pseudo-random Number Generator based on Non-linear Dynamic Chaotic System", ISSN 1392-1215, Electronics and electrical engineering, 2009, №7(95), pp.25-28

[7] Vector Signal Generator SMIQ03B, Operating manual, Vol.1 and 2, Rohde&Schwarz, Germany