# Experimental Assessment of FIRO- and GARO-based Noise Sources for Digital TRNG Designs on FPGAs

Martin Schramm*, Reiner Dojen* and Michael Heigl†
*Department of Electronic and Computer Engineering
University of Limerick, Ireland
Email: {martin.schramm, reiner.dojen}@ul.ie
†Deggendorf Institute of Technology, Deggendorf, Germany
Email: michael.heigl@th-deg.de

***Abstract*—The quality of TRNG designs mainly depends on the grade of the noise source from which the entropy will be harvested to extract randomness. Especially for purely digital noise sources suitable for FPGA implementations the use of Ring Oscillators is suggested in many scientific publications. Standard Ring Oscillator based noise sources however have earned some criticism regarding the amount of entropy generated. On this account different enhancements have been proposed, with Fibonacci Ring Oscillators (FIROs) and Galois Ring Oscillators (GAROs) being prominent examples, which under some circumstances are able to sustain a chaotic oscillation suitable for entropy extraction. This paper deals with the assessment of fully constrained FIRO and GARO noise source designs for a specific target FPGA. Due to the restrictive placement of ring elements the assessment yielded new criteria for choosing proper FIRO/GARO feedback configurations and an enhanced sampling method for entropy extraction has been derived.**

## I. Introduction

A broad range of cryptographic applications necessitate random numbers, e.g., for the determination of secret keys [1], the calculation of random prime numbers [2], secret parameters of key exchange schemes [3], challenges [4] and many more. Especially for FPGA designs purely digital true random number generators (TRNGs), which could be implemented by only utilizing internal logic gates are valuable. A physical TRNG design based on standard Ring Oscillators (ROs) has been proposed by B. Sunar, et al. in [5] which more implementation details given in [6]. The design has earned some criticism in [7] and some enhancements have been proposed in [8]. However such a design requires a huge amount of rings which potentially might interact and lower the available entropy.

To overcome the limitations of standard ring oscillator based TRNGs J. Golić in [9] has introduced a new method and technique for generating high-entropy binary numbers using logic gates only by replacing the classical ring oscillators by more complex asynchronous logic circuits with feedback, forming a generalisation of classical ring oscillator structures. One of these structures is named Fibonacci Ring Oscillator (FIRO) corresponding to the Fibonacci configuration of Linear Feedback Shift Registers (LFSRs) by simply using inverter gates instead of register elements.

A FIRO structure consists of a number of inverter elements $r$ connected in a cascade equally to standard ROs. The feedback XOR connections are specified by binary coefficients $f_i$ in which a connection to the XOR gate will be given if $f_i = 1$. The inverters and feedback coefficients are numbered from left to right. The feedback coefficients are represented by a binary polynomial $f(x) = \sum_{i=0}^{r} f_i \cdot x^i$ called feedback polynomial with $f_0 = f_r = 1$. As stated in [9] a FIRO does not exhibit a fixed point, a state in which the oscillation would stop, if and only if $f(x) = (1 + x) \cdot h(x)$ and $h(1) = 1$. The condition states that $f(x)$ is dividable by $(1 + x)$, therefore $f(1) = 0$, and that $h(x)$ is not dividable by $(1 + x)$. Furthermore it is stated that the degree of $f(x)$ can be odd or even. Recently in [10] M. Dichtl describes that Fibonacci Ring Oscillators possess a risk to oscillate periodically instead of chaotically. Experimental evidence is given for continuously running FIROs of length 16 and 32. However, no criteria for finding proper feedback polynomials for FIROs has been given. The second class of generalised ROs introduced by J. Golić is called Galois Ring Oscillator (GARO), also corresponding to the Galois configuration of a LFSR. A GARO structure consists of a number of inverter elements $r$ connected in a cascade. The input of an inverter gate may be given by XOR-ing the output of the preceding inverter with the output of the last inverter of the ring, representing the feedback line, depending on the specified feedback polynomial. The feedback XOR connections are specified by binary coefficients $f_i$ in which a XOR gate will be present if $f_i = 1$. The inverters and feedback coefficients of a GARO are numbered from right to left. The feedback coefficients are represented by a binary polynomial $f(x) = \sum_{i=0}^{r} f_i \cdot x^i$ called feedback polynomial with $f_0 = f_r = 1$. A GARO does not exhibit a fixed point in which the oscillation would stop, if and only if it is composed of an odd number of inverters and if $f(1) = 0$ meaning that $f(x) = (1 + x) \cdot h(x)$. In [10] it is assumed that GAROs could also possess a risk to show periodic instead of chaotic oscillations. However a broad statistical basis was missing so far.

The rest of the paper is structured as follows: Section II describes how the placement of the analysed

ISBN 978-80-261-0642-5, 

noise sources can be fully constrained for a chosen target FPGA device family, namely Altera Cyclone V devices. Section III gives some details about the assessment environment whereas section IV lists the main findings of the assessment and gives new criteria for choosing proper FIRO/GARO configurations and sampling methods. Section V finalizes the paper with a short conclusion and a glance at the future work of the ongoing research work.

## II. Constraining the Noise Sources

In order to be able to assess all possible combinations of feedback polynomials as well as different sampling methods, experimental architectures for both, fully constrained FIRO and GARO-based noise sources have been defined.

### A. Constrained FIRO

The experimental architecture of a FIRO based noise source is illustrated in figure 1. By the parameter FIRO_LENGTH, the length of the FIRO to be assessed can be adjusted. In order to guarantee the repeatability of the conducted experiments from identical starting conditions the outputs of all logic gates of the FIRO can be stabilised by replacing the first inverter of the FIRO by a NAND-gate.

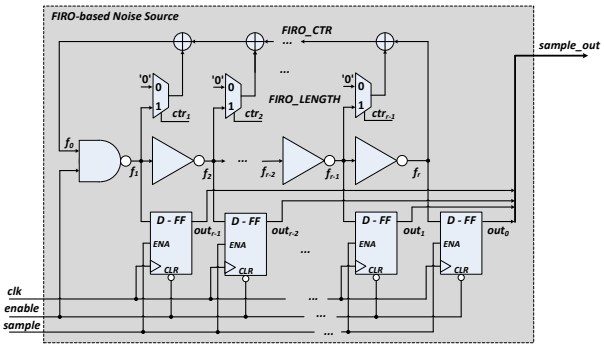


Fig. 1. Experimental Architecture of a FIRO-based Noise Source

To perform a systematic survey of all possible feedback configurations for a given FIRO length, a FIRO control vector (FIRO_CTR) has been introduced together with a multiplexer structure. If the specific bit of the feedback control vector is set, than the corresponding intermediate value of the FIRO will contribute to the feedback signal, otherwise the signal will not be altered. After an adjustable sampling time (T_SAMPLE) the internal state will be sampled by an array of D-type flip-flops. The total number of samples generated can be configured through the parameter N_SAMPLES.

In order to produce comparable results of different FIRO feedback polynomials special assignments have been set. In the design each XOR gate in the feedback line together with the corresponding multiplexer have been constrained to be implemented in a single Look-Up Table (LUT). The individual inverting elements of the ring have been constrained to be implemented in the Adaptive Logic Module (ALM) of a single Logic Array Block (LAB), the feedback chain has been constrained to be implemented in the ALMs of the LAB cell directly next to the inverter ring, ensuring a more stable routing delay. The description required usage of the *keep* attribute to prevent the optimisation engine from removing the combinatorial loop of inverters. The flip-flops used for sampling have been described using low-level primitives and constrained to be implemented in the appropriate ALM cell which also holds the preceding inverting element.

Figure 2 shows the Chip Planner View of a constrained exemplary FIRO. The LAB on the left-hand side accommodates the FIRO ring of inverters together with the sampling flip-flops, whereas the LAB on the right-hand side accommodates the individual XOR gates of the feedback line together with the multiplexer structure.

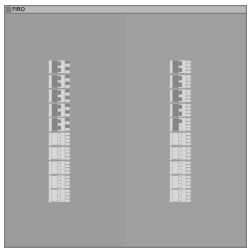

Fig. 2. Exemplary Chip Planner View of a Constrained FIRO

As a further requirement the ring of inverters together with the sampling flip-flops, as well as the feedback line together with the multiplexer structure should both fit in one single LAB, respectively, for the results to be comparable. Therefore FIRO lengths with up to 20 inverting elements have been assessed. For FIROs of even length $r_{even}$ the number of fixed point free feedback configurations is given by $2^{r_{even}-3}$, for FIROs of odd length $r_{odd}$ the number of fixed point free feedback configurations is given by $2^{r_{odd}-3}-1$.

### B. Constrained GARO

The experimental architecture of a GARO based noise source is illustrated in figure 3. The length of the GARO can be adjusted by the parameter GARO_LENGTH. For ensuring identical starting conditions the last inverter in the chain has been replaced by a NAND-gate.

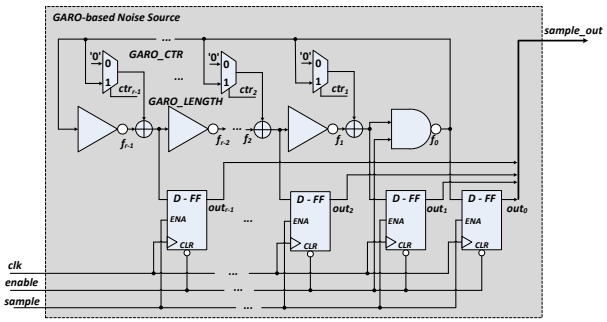


Fig. 3. Experimental Architecture of a GARO-based Noise Source

A control vector (GARO_CTR) together with a multiplexer structure has been introduced to be able to evaluate all possible feedback configurations. If the specific bit of the feedback control vector is set, than the feedback signal will be XOR-ed with the corresponding intermediate value of the inverter chain, otherwise the intermediate value will not be influenced. The internal state can be sampled after an adjustable time (T_SAMPLE). Again the total number of samples generated can be configured through the parameter N_SAMPLES.

The special assignments for constrained GAROs include fitting one inverter gate together with the multiplexer controlling the feedback and the XOR gate into one LUT. Therefore one ALM can comprise two stages of the ring together with the corresponding sample flip-flops, which again have been described by using low-level primitives. Also the *keep* attribute must be used to prevent the optimisation of the combinatorial loop described. Figure 4 shows the Chip Planner View of a constrained exemplary GARO.

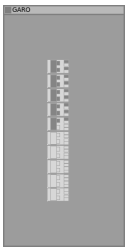


Fig. 4. Exemplary Chip Planner View of a Constrained GARO

As further requirement the whole described GARO should fit into one single LAB, therefore GARO lengths up to 19 inverting elements have been assessed. For GAROs of length $r$ the number of fixed point free feedback configurations is given by $2^{r-2}-1$.

## III. Noise Source Assessment Environment

The experimental environment for the assessment (given in figure 5) has been set up on DE1-SoC Development Kits, which are equipped with an Altera Cyclone V System On Chip FPGA with integrated ARM-based Hard Processor System (HPS) (5CSEMA5F31C6N) fabricated in $28nm$ technology featured with enhanced 8-input ALMs with four registers each.

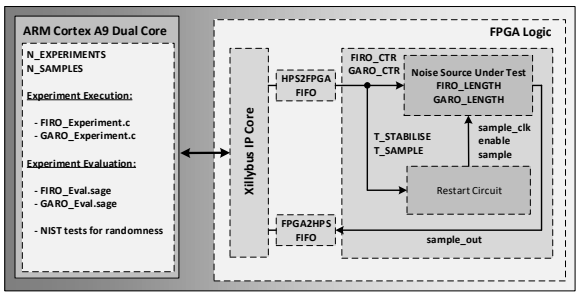


Fig. 5. FIRO/GARO Noise Source Assessment Environment

Therefore the configuration and evaluation of the experiments has directly be performed on the HPS side. The Xillybus IP Core has been utilized for the interconnection of the FPGA logic comprising the Noise Source Under Test as well as the Restart Circuit, with the HPS system. The Restart Circuit basically consists of a counter which can be parametrised by means of T_STABILISE and T_SAMPLE, which furthermore ensures that the Noise Source Under Test will stabilise between two consecutive samplings. This should guarantee that the individual samplings are independent from each other. During the execution phase, for a given length of the FIRO/GARO to assess, a total number of N_EXPERIMENTS for specified feedback polynomials, given by control vectors, will be conducted each gathering N_SAMPLES. During evaluation phase, for a specific experiment, information about all samples, different samples occurred, amount of different samples occurred, probability of sample occurrence and information about the last same sample state will be produced. With this information, for a specific FPGA fabrication technology, guidelines for choosing appropriate parameters can be established. Furthermore different sampling methods can be evaluated.

## IV. Assessment Results

In this section the main findings in assessing FIRO and GARO based noise sources on a Altera Cyclone V FPGA are stated. For a better readability the outcome is reported by means of exemplary FIROs of length 16 and 10 as well as exemplary GAROs of length 15 and 11. All further investigated FIRO/GARO lengths produced the same results.

### A. FIRO Assessment

Analysing fully constrained FIROs shows that most of the possible feedback polynomials result in a high number of different samplings occurring. Figure 6 illustrates the sorted number of different samples for all fixed point free feedback polynomials of a FIRO of length 16.

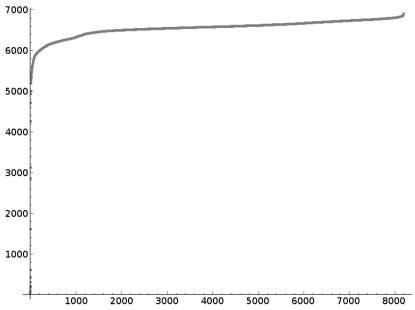


Fig. 6. Sorted number of different samples for 8192 feedback configurations of a FIRO of length 16

However, some feedback configurations result in a very low number of different samples, indicating a periodic behaviour, whereas feedback configurations resulting in an intermediate number of different samples indicate a trend to switch to periodic behaviour. By linking the amount of different occurring samples with the number of bits set in the feedback polynomial, a

relationship could be derived, as shown in (shortened) table I for a FIRO of length 10.

TABLE I
RELATIONSHIP OF NUMBER OF DIFFERENT SAMPLES WITH AMOUNT OF XOR TAPS (FIRO)

| FIRO_CTR $[x^1, x^2, \ldots, x^8, x^9]$ | # different samples | # taps |
|---|---|---|
| [0, 0, 0, 1, 0, 0, 1, 0, 0] | 13 | 2 |
| [1, 1, 0, 0, 0, 0, 0, 0, 0] | 112 | 2 |
| [1, 0, 0, 0, 0, 1, 0, 0, 0] | 162 | 2 |
| [1, 0, 0, 1, 0, 0, 0, 0, 0] | 177 | 2 |
| [0, 0, 0, 1, 0, 0, 0, 0, 1] | 193 | 2 |
| [0, 1, 0, 0, 0, 0, 0, 0, 1] | 288 | 2 |
| [0, 0, 0, 0, 0, 1, 0, 0, 1] | 396 | 2 |
| [1, 1, 0, 0, 0, 1, 0, 1, 0] | 409 | 4 |
| ... | ... | ... |
| [1, 1, 1, 0, 0, 1, 0, 1, 1] | 867 | 6 |
| [1, 1, 1, 0, 0, 1, 1, 1, 0] | 868 | 6 |
| [1, 1, 1, 0, 1, 1, 1, 1, 1] | 872 | 8 |
| [1, 1, 1, 1, 0, 1, 1, 0, 0] | 873 | 6 |
| [1, 1, 1, 1, 1, 1, 0, 0, 0] | 875 | 6 |
| [1, 1, 1, 1, 1, 1, 1, 0, 1] | 876 | 8 |

It turned out, that maximising the number of contributing XOR taps can better propagate the inherent jitter leading to a higher collectable entropy. For FIROs of even length, $r_{even}$, the maximum number of XOR taps of FIRO_CTR is given by $r_{even} - 2$, and the number of fixed point free feedback configurations with maximum number of XOR taps is the highest even number less or equal to $r_{even}/2$. For FIROs of odd length, $r_{odd}$, the maximum number of XOR taps of FIRO_CTR is given by $r_{odd} - 3$ if $r_{odd} \equiv 3 \, mod \, 4$ and $r_{odd} - 1$ if $r_{odd} \equiv 1 \, mod \, 4$. When $r_{odd} \equiv 3 \, mod \, 4$ the number of possible fixed point free feedback configurations with maximum number of XOR taps is given by $(\lfloor r_{odd}/2 \rfloor)^2$. If $r_{odd} \equiv 1 \, mod \, 4$ there exists only one possible fixed point free feedback configuration with maximum number of XOR taps, therefore also feedback configurations with $r_{odd} - 3$ XOR taps have been considered. Here the number of possible fixed point free feedback configurations is given by $(\lfloor (r_{odd} - 2)/2 \rfloor)^2 + \lfloor (r_{odd} - 2)/2 \rfloor$.

TABLE II
OVERVIEW OF FIRO_LENGTH, NUMBER OF XOR TAPS AND QUANTITY OF FIRO_CTR VECTORS

| FIRO_LENGTH | # taps | Qty. of FIRO_CTR vectors |
|---|---|---|
| 4 | 2 | 2 |
| 5 | 2 / 4 | 2 / 1 |
| 6 | 4 | 2 |
| 7 | 4 | 9 |
| 8 | 6 | 4 |
| 9 | 6 / 8 | 12 / 1 |
| 10 | 8 | 4 |
| 11 | 8 | 25 |
| 12 | 10 | 6 |
| 13 | 10 / 12 | 30 / 1 |
| 14 | 12 | 6 |
| 15 | 12 | 49 |
| 16 | 14 | 8 |
| 17 | 14 / 16 | 56 / 1 |
| 18 | 16 | 8 |
| 19 | 16 | 81 |
| 20 | 18 | 10 |

In table II for all examined FIRO lengths, the number of XOR taps and the quantity of remaining fixed point free feedback polynomials are given. Figure 7 shows a semi-logarithm plot of the last same sampling for a FIRO of length 10 with feedback polynomial $x^{10} + x^9 + x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$. Note that this is not a mathematical function. In the figure a point at position $-2$ means that this specific sample has not been generated before. The rest of the points yield information about how many samples before a specific pattern has been sampled displayed as decimal logarithm value. The plot illustrates the sustained chaotic behaviour.

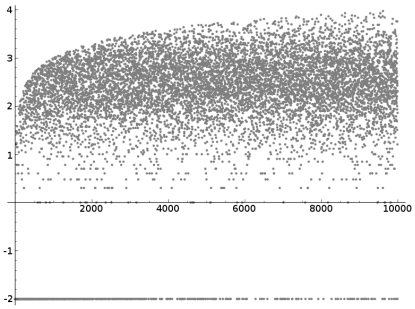


Fig. 7. Last same sampling plot for a FIRO of length 10 with feedback polynomial $x^{10} + x^9 + x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$

Furthermore different sampling methods have been evaluated. In [7] it has been stated that the output of a FIRO based noise source might be biased if a D-type flip-flop is used for sampling. In order to get a more balanced output a T-type flip-flop is proposed in [7] counting the $0 - 1$ transitions in the oscillating signal. However the conducted experiments show that this cannot be confirmed in general. A novel sampling method is proposed, termed *state sampling*, which utilizes the whole internal state of the FIRO at sampling time, by XOR-ing the sample bits. Table III gives a comparison of the Shannon Entropy for the three different sampling methods of a FIRO of length 10 and exemplary feedback polynomials.

TABLE III
SHANNON ENTROPY (SE) OF DIFFERENT SAMPLING METHODS (FIRO)

| FIRO_CTR $[x^1, x^2, \ldots, x^8, x^9]$ | SE D-FF sampling | SE T-FF sampling | SE State sampling |
|---|---|---|---|
| [0, 0, 0, 1, 0, 0, 1, 0, 0] | 0.92162 | 0.08605 | 0.94514 |
| [0, 1, 0, 0, 0, 0, 0, 0, 1] | 0.28084 | 0.79354 | 0.98295 |
| [1, 1, 1, 0, 1, 1, 1, 1, 1] | 0.99835 | 0.99937 | 0.99999 |
| [1, 1, 1, 1, 1, 1, 0, 0, 0] | 0.99939 | 0.99926 | 0.99979 |
| [1, 1, 1, 1, 1, 1, 1, 0, 1] | 0.99889 | 0.99969 | 0.99997 |

These three different sampling methods have been evaluated for all supported FIRO lengths with suitable feedback polynomials defined prior. The statistical tests on randomness have been carried out by using the NIST RNG test suite with the recommended parameter settings given in [11]. The conducted experiments demonstrated that solely the proposed state sampling

method generates random output bits which pass all the statistical tests. As a further outcome for the target FPGA a minimal FIRO length of 8 is necessary to produce random numbers with good statistical properties.

### B. GARO Assessment

Figure 8 shows the sorted number of different samples among 10000 for the 8192 feedback polynomials for an exemplary fully-constrained GARO consisting of 15 inverting elements.

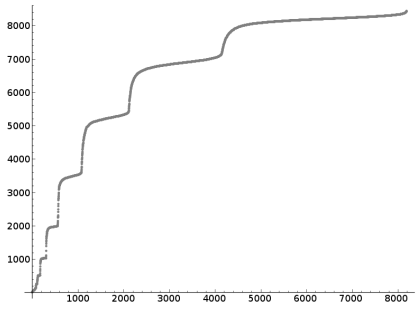


Fig. 8. Sorted number of different samples for 8191 feedback configurations of a GARO of length 15

In comparison examining the sorted number of different samples occurring from the same GARO configuration without any constraints yielded results given in figure 9, clarifying the need for proper design placement.

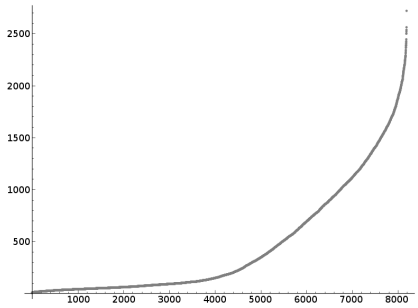


Fig. 9. Sorted number of different samples for an unconstrained GARO of length 15

The stair like structure of constrained designs results due to the placement constraints on the target FPGA since the first inverter together with the first multiplexer and XOR gate will be synthesised in one single LUT. If the following feedback taps will not be set, the feedback signal cannot contribute to the chain of inverting elements (see figure 10) which will lead to fixed voltage levels in the chain until the first XOR gate which will be fed with the feedback signal.

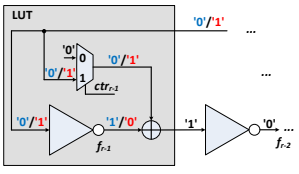


Fig. 10. Impact of setting the msb of a GARO feedback polynomial

As a first criteria the experiments showed that it is necessary for the most significant bit (msb) of a GARO control vector to be zero. Excluding the msb of the feedback polynomial leads to a result comparable to the one of assessed FIROs, illustrated in figure 11 for a GARO of length 15.

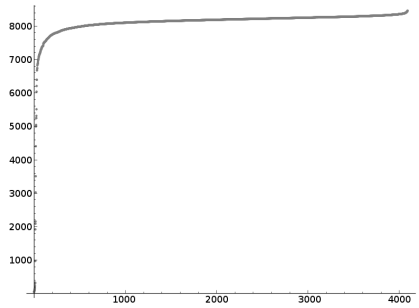


Fig. 11. Sorted number of different samples for 4096 feedback configurations without $x^{14}$ being set of a GARO of length 15

Again, most of the feedback polynomials yield a high number of different samples, but some lead to periodic oscillation or partly chaotic oscillation becoming periodic. The same relationship (number of feedback taps to number of different samples occurring) could be derived, as show in (shortened) table IV for a GARO of length 11.

TABLE IV
RELATIONSHIP OF NUMBER OF DIFFERENT SAMPLES WITH AMOUNT OF XOR TAPS (GARO)

| GARO_CTR $[x^1, x^2, \ldots, x^9, x^{10}]$ | # different samples | # taps |
|---|---|---|
| [0, 0, 1, 0, 0, 1, 0, 0, 0, 0] | 5 | 2 |
| [1, 0, 0, 0, 0, 0, 1, 0, 0, 0] | 6 | 2 |
| [1, 0, 1, 0, 0, 0, 0, 1, 1, 0] | 17 | 4 |
| [1, 1, 0, 0, 0, 1, 0, 0, 1, 0] | 23 | 4 |
| [1, 1, 0, 0, 1, 1, 0, 0, 0, 0] | 34 | 4 |
| [1, 1, 0, 1, 1, 1, 0, 1, 0, 0] | 43 | 6 |
| [1, 0, 0, 0, 0, 0, 0, 0, 1, 0] | 50 | 2 |
| [0, 0, 1, 1, 1, 1, 1, 1, 0, 0] | 142 | 6 |
| ... | ... | ... |
| [0, 1, 1, 1, 1, 1, 1, 1, 1, 0] | 1954 | 8 |
| [0, 1, 1, 1, 0, 1, 1, 1, 0, 0] | 1955 | 6 |
| [0, 1, 0, 1, 1, 1, 1, 0, 1, 0] | 1955 | 6 |
| [0, 1, 1, 0, 1, 1, 0, 1, 1, 0] | 1955 | 6 |
| [0, 1, 1, 1, 1, 0, 0, 1, 1, 0] | 1958 | 6 |
| [0, 1, 1, 1, 0, 1, 0, 1, 1, 0] | 1962 | 6 |
| [0, 1, 1, 0, 1, 1, 1, 0, 1, 0] | 1964 | 6 |
| [0, 1, 1, 0, 1, 1, 1, 1, 0, 0] | 1971 | 6 |
| [0, 1, 1, 1, 1, 0, 1, 0, 1, 0] | 1981 | 6 |
| [0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0] | 1985 | 6 |

For GAROs of length $r$, the maximum number of XOR taps of GARO_CTR is given by $r - 3$, and the number of possible fixed point free feedback configurations with maximum number of XOR taps is given by $r - 2$. In table V for all examined GARO lengths, the maximum number of taps set in the feedback polynomial and the quantity of remaining fixed point free configurations is given. Compared to FIRO based noise sources with increasing length of the GARO there is a constant increase of suitable feedback polynomials to choose from.

TABLE V
OVERVIEW OF GARO_LENGTH, NUMBER OF XOR TAPS AND QUANTITY OF GARO_CTR VECTORS

| GARO_LENGTH | # taps | Qty. of GARO_CTR vectors |
|---|---|---|
| 5 | 2 | 3 |
| 7 | 4 | 5 |
| 9 | 6 | 7 |
| 11 | 8 | 9 |
| 13 | 10 | 11 |
| 15 | 12 | 13 |
| 17 | 14 | 15 |
| 19 | 16 | 17 |

Figure 12 illustrates the frequency distribution of 10000 samples for a GARO of length 11 with feedback polynomial $x^{11}+x^9+x^6+x^5+x^4+x^3+x^2+1$. In total 1985 out of 2048 possible 11-bit samples, exhibiting a smooth frequency distribution, occurred.

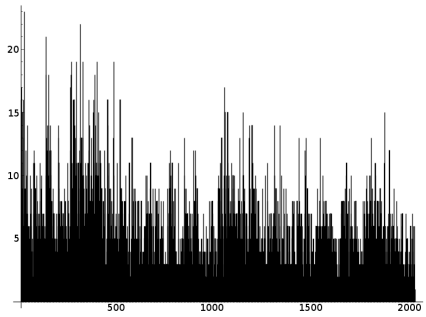


Fig. 12. Frequency distribution of 10000 samples for a GARO of length 11 and $x^{11}+x^9+x^6+x^5+x^4+x^3+x^2+1$ as feedback polynomial

Since the output of a GARO based noise source might be biased D-type flip-flop sampling, T-type flip-flop sampling and the proposed *state sampling* methods have been compared. Table VI lists the Shannon Entropy for the three different sampling methods of a GARO of length 11 and exemplary feedback polynomials. Again, it cannot be confirmed that the T-type flip-flop sampling performs better than the D-type flip-flop sampling, but the proposed state sampling indeed leads to unbiased output bits.

TABLE VI
SHANNON ENTROPY (SE) OF DIFFERENT SAMPLING METHODS (GARO)

| GARO_CTR $[x^1, x^2, \ldots, x^9, x^{10}]$ | SE D-FF sampling | SE T-FF sampling | SE State sampling |
|---|---|---|---|
| [1, 1, 0, 0, 0, 1, 0, 0, 1, 0] | 0.97273 | 0.67013 | 0.99828 |
| [1, 1, 0, 0, 1, 1, 0, 0, 0, 0] | 0.70914 | 0.38322 | 0.93948 |
| [0, 1, 1, 1, 1, 1, 1, 1, 1, 0] | 0.99755 | 0.99718 | 0.99982 |
| [0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0] | 0.99674 | 0.99709 | 0.99998 |
| [0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0] | 0.99803 | 0.99892 | 0.99986 |

Experiments have been conducted for all remaining suitable feedback polynomials complying with the defined criteria for all supported GARO lengths. Again the statistical tests on randomness using NIST RNG test suite have been carried out with the parameter settings stated in [11]. It turned out that again, only the proposed state sampling method could generate a random output bitstream which passes all the statistical tests. As a further outcome for the target FPGA a minimal GARO length of 13 is necessary to produce random numbers with good statistical properties.

## V. CONCLUSION AND FUTURE WORK

The assessment of fully-constrained FIRO and GARO noise sources revealed that there exists a relationship between the number of different occurring samples and the amount of contributing XOR connections of the feedback polynomial. Furthermore maximising the number of contributing XOR taps may sustain a chaotic oscillation and minimise the probability of switching to a periodic behaviour. For both FIROs and GAROs of different lengths the recommended amount of XOR taps and the number of fixed point free configurations have been derived. The proposed state sampling method utilises the whole internal state to generate the random output bit, which also leads to an unbiased bit stream for large enough FIRO/GARO lengths. Provided that the parameters (length, control polynomial, stabilisation time and sampling time) are chosen properly a strong noise source may be described in FPGA logic which does not necessarily require (complex) cryptographic post-processing. In the next steps full TRNG designs with start-up test, online tests and tot-test should be evaluated. The tests should utilise the raw information about the individual rings of the design instead of the state sampling output bits. One promising approach would be to evaluate both, the Shannon Entropies of D-type flip-flop output sampling method and T-type flip-flop toggling sampling method to identify a total failure of the noise source.

## REFERENCES


[1] Corrigan-Gibbs H., et al., *Ensuring High-Quality Randomness in Cryptographic Key Generation*, ACM Conference on Computer and Communications Security (CCS), 2013

[2] Fouque P., Tibouchi M., *Close to Uniform Prime Number Generation With Fewer Random Bits*, International Colloquium on Automata, Languages, and Programming, 2014

[3] Diffie W., Hellman M., *New Directions in Cryptography*, IEEE Transactions on Information Theory, 1976

[4] Badra M., et al., *Random Values, Nonce and Challenges: Semantic Meaning versus Opaque and Strings of Data*, IEEE 70th Vehicular Technology Conference, 2009

[5] Sunar B., et al., *A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks*, IEEE Transactions on Computers Volume 56 Issue 1 , 2007

[6] Schellekens D., et al., *FPGA Vendor Agnostic True Random Number Generator*, International Conference on Field Programmable Logic and Applications, 2006

[7] Dichtl M., Golić J., *High-Speed True Random Number Generation with Logic Gates Only*, CHES - Cryptographic Hardware and Embedded Systems, 2007

[8] Wold K., et al., *Analysis and Enhancement of Random Number Generator in FPGA Based on Oscillator Rings*, International Journal of Reconfigurable Computing, 2009

[9] Golić J., *New Methods for Digital Generation and Postprocessing of Random Data*, IEEE Transactions on Computers Volume 55 Issue 10, 2006

[10] Dichtl M., *Fibonacci Ring Oscillators as True Random Number Generators - A Security Risk*, Cryptology ePrint Archive, Report 2015/270, 2015

[11] Killmann, W., Schindler, W., *A proposal for: Functional classes for random number generators*, Bundesamt fr Sicherheit in der Informationstechnik (BSI), 2011