RANDOM NUMBER GENERATION ON RECONFIGURABLE RING OSCILLATOR

Kaiky M., Ivaniuk A.
Department of Informatics, Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus
E-mail: kaikymykhailo@gmail.com, ivaniuk@bsuir.by

This work is devoted to the study of a reconfigurable ring generator based on two-input XOR elements used to generate true random numbers. The paper examines a system for recording generator frequency oscillations and patterns of changes in oscillation frequencies at its outputs depending on the given generator configuration and the temperature of the FPGA chip. An approach to generating truly random numbers using a counter of the leading edges of the generated signal is considered.

Introduction

According to the NIST SP 800-90 [1] group of standards, sources of truly random numbers must be built on the basis of a physical noise generator, followed by digitization and processing of the random signal, converting it into sequences of random numbers. The most commonly used source of such noise is usually inverter-based ring oscillators.

I. Structure of reconfigurable ring oscillator

The work [2] proposes the structure of a ring oscillator based on N two-input logical XOR gates (fig. 1). Inputs C are generator configuration inputs, EN is a control input, and when its level is active, the generator can begin to oscillate (depending on the configuration). The proposed generator design begins to oscillate only when the Hamming weight of the vector C is odd, and the oscillation frequency depends on the number of units and their position in the configuration. The gates were implemented on the FPGA element base of Xilinx (Zynq-7000 family) and are LUT2 elements.

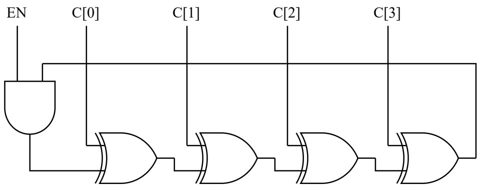

Figure 1 – Reconfigurable ring oscillator

II. Measuring oscillations frequencies

The oscillator frequencies are measured using two counters - a window counter tmw_{cnt}, a counter of the leading edges of generator oscillations clk_{cnt}. For the developed generator, the frequencies of its operation were measured on various configurations (fig. 2). Each configuration was measured 1000 times to obtain the average oscillation frequency. Measurements were carried out on a ring oscillator with 8 XOR elements, corresponding to 128 different configurations and on a window of 2 microseconds ($tmw_{cnt} = 100000$ at a system frequency of 50 MHz).

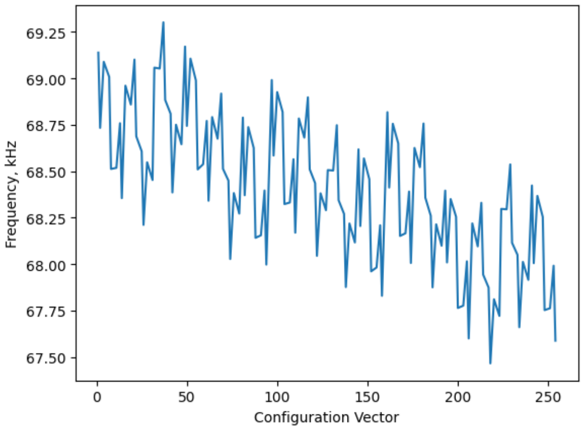

Figure 2 – Generator oscillation mean frequency depending on configuration

As can be seen from the figure, the frequency dependence tends to decrease the oscillation frequency with increasing configuration value. This is due to the number of toggled XOR elements in the generator. For greater clarity, we present the dependence of oscillation frequencies on the count of "ones" in the configuration vector (table 1). Also, clear patterns are visible, they are associated with combinations of switchable elements XOR.

Table 1 – Dependence of oscillation frequencies

F, [kHz]	Count of ones in configuration			
	1	3	5	7
f_{min}	68.506	67.764	67.466	67.588
f_{mean}	68.848	68.555	68.253	67.953
f_{max}	69.138	69.301	68.989	68.290

III. Reasoning for choosing the size of the measurement time window

In the experiment described above, the window size was 2 microseconds; this value was not chosen by chance. In the experiment described above, to determine the window size, generator was run 10 times with windows of sizes: $10^0, 10^1, 10^2, ..., 10^9$ toggle the tmw_{cnt}. As a result, we obtain the following dependence of the number of decimal places on the window size: $1, 1, 2, 2, 4, 5, 6, 7, 8, 9$.

IV. Frequency counter as a random number source

In addition to its main purpose, the oscillation frequency counter can also be used as a post-processing circuit for random sequences. To investigate this possibility, each configuration was fed to the generator 10,000 times. The figure 3 shows the distribution of numbers for 8 of 128 generator configurations, as you can see – they are shifted relative to each other and have different shapes.

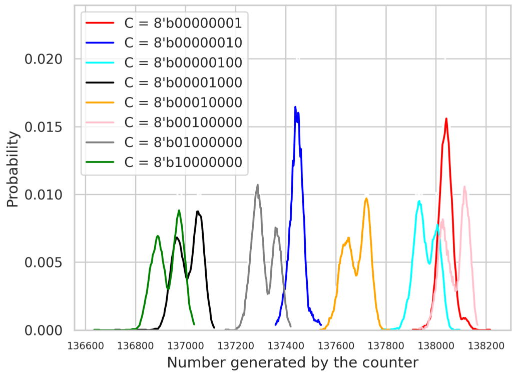

Figure 3 – Probability of numbers generated by the counter

Bias is the result of the special behavior of the counter as a post-processing circuit. Since the size of the measurement window is a fixed number, some of the higher digits of the counter will not change their value, while the lower ones, on the contrary, will make noise. This hypothesis is confirmed by calculating the probability of the appearance of one and zero in the digits of this counter (fig. 4).

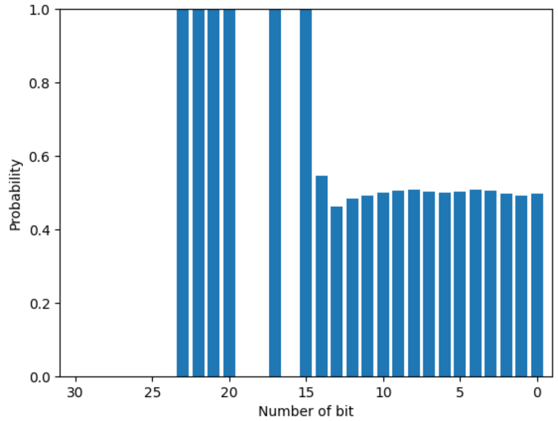

Figure 4 – Probability ones on clock counter

As can be seen from the figure 4, the highest 15 digits are stable and do not change their value depending on the experiment. The high stability of the most significant digits determines the generation of numbers in a given range (fig. 4). Introduce the value K - the number of unstable (oscillating) bits in the vector of frequency counter values. Then $K = 15$. Minor 15 - strives for the probability of occurrence of "ones" to be 0.5, which allows you to use data bits to generate truly random sequences.

V. Ring oscillator temperature measurement

As world practice has shown, the oscillation frequency of a ring oscillator strongly and linearly depends on the temperature of the chip. To conduct an experiment on measuring the oscillation frequencies of the proposed reconfigurable generator, its configuration was fixed $tmw_{cnt} = 100000$, $C = 8'h1$. The temperature was changed using a temperature chamber (TestEquity Model 155) in the range from -15 to +115 degrees Celsius. The dependence of the generator oscillation frequency on temperature is shown in the figure 5. As can be seen from the figure, when the operating temperature range of the microcircuit is exceeded, the K value undergoes a change.

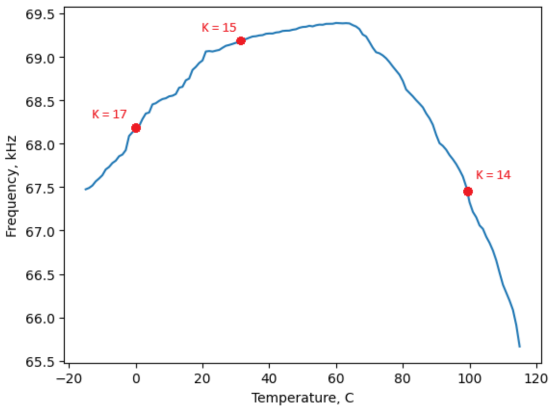

Figure 5 – Generator oscillation frequency depending on temperature

VI. Conclusion

When considering the structure of a reconfigurable ring oscillator, it is possible to limit the frequency-controlled oscillations and regulate their circuits by the configuration supplied to the operating inputs of the oscillator. The dependences of the generator oscillation frequency on a given configuration and temperature have been studied. The possibility of using a rising edge counter as a post-processing circuit for random bits is considered. It has been proven that the low-order bits of a frequency counter tend to have a uniform distribution of zeros and ones, which allows them to be used as true random number generators. The behavior of the edge counter in conjunction with a ring oscillator changes depending on the temperature of the microcircuit.

1. NIST Special Publication, NIST SP 800-90, Recommendation for Random Bit Generation – NIST. [Electronic resource] – Mode of access: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-90r.pdf. – Date of access: 01.10.2023.
2. Yarmolik V.N., Ivaniuk A.A., Shynkevich N.N. Physically unclonable functions with controlled propagation delay. Informatics. 2022;19(1):32-49. (In Russ.) https://doi.org/10.37661/1816-0301-2021-19-1-32-49