

Synthesis and simulation of digital pseudo-random impulse sequence generator based on PLIC FPGA Xilinx using CAD Vivado 2016.2 and development of acoustic noise generator scheme for the protection of information

A Zaurbek, N A Seilova, D Z Dzhuruntaev*

Kazakh National Technical Research University named after K.I. Satpayev, Almaty, Kazakhstan

**Corresponding author's e-mail: juruntaev@rambler.ru*

Received 27 February 2017, www.cmnt.lv

Abstract

In this work with the help of CAD Vivado 2016.2 system and Verilog hardware description language there were synthesized, simulated and built temporary digital pseudo-random impulse sequence generator diagrams based on CAD of FPGA families of the Xilinx company and eight-rate shift LFSR register, which can be used in cryptography to create a stream encryption algorithms. On the basis of a digital pseudo-random impulse sequence generator and active low-pass filter of the second order of Sallen - Key there was constructed an electric diagram of the acoustic noise generator that provides protection against wiretapping by using embedded devices, telephone conversations, laser wiretapping system and unauthorized dictaphone recording of confidential voice information by creating a masking vibration noise.

Keywords:

computer-aided design, hardware description languages, programmable logic integrated circuits, synthesizing, simulation, circuit simulation, pseudo-random impulse sequence

1 Introduction

Programmable logic integrated circuits (PLIC) are one the fastest growing and promising elements of the digital circuitry. Today's widely used at present micro schemes of the programmable logic PLIC are the crystals on which there are hundreds of thousands or more of simple logic elements and triggers that allow to obtain the layout (prototype) of the digital device of almost any complexity.

Programmable logic integrated circuits provided to create quickly digital devices with an internal structure, defined by the user, that is, rapid conversion of one configuration of the digital circuit to another. In other words, the change of the principal electric scheme of the digital device in a PLIC crystal is performed by reprogramming. As a result, the cycle of creation of complex digital devices, including the development of multiprocessor systems and parallel processing systems with large amounts of data accumulation, is greatly reduced that reduces the cost of the whole project [1-4].

The most widespread in this area have PLIC with the FPGA type architecture (field-programmable gate array). PLIC FPGA advantage is their ability to provide not only high speed of processing, but also continuous processing and stable speed.

Integrated Circuits of a special purpose ASIC (abbreviation from English - Application-specific integrated circuit) run faster PLIC FPGA, but are not used to protect information systems. ASIC are programmed during manufacturing and have no possibility of reprogramming.

PLIC with FPGA architecture provides the broadest functional possibilities and the largest number of hardware resources, therefore, have the greatest interest in the

development of digital devices. PLIC micro schemes are widely used in digital signal processing system, as well as in information protection issues, in particular, for generating a pseudo-random impulse (numbers) sequence.

The need of a digital pseudo-random number generator usage occurs in many problems. Digital hardware random number generators are used for static testing and in cryptography, where they are used to create cryptographic keys for the encrypted data [1, 2].

Considering the above, the task of digital devices developing, including digital circuit of the pseudo-random impulse sequence generator based on PLIC with FPGA architecture, is relevant and has practical interest for the information security.

For effective use of PLIC FPGA micro schemes there is a need to know and understand the different approaches and aspects of the synthesis and simulation of digital device circuits that is almost impossible without the use of computer-aided design. The most commonly used are special tools of CAD Vivado of the Xilinx company, PLIC FPGA manufacturer [5, 6]. The process of digital devices designing in CAD Vivado includes the following steps: the creation of modules of an initial description of the designed device, the project synthesis and implementation on the basis of PLIC of FPGA families of the Xilinx company and simulation of digital devices.

Nowadays, for the creation of digital devices within a reasonable terms and with a high quality based on the PLIC micro schemes, containing hundreds of thousands or millions of logic gates, there are used effectively Vivado 2016.2 CAD and hardware description language such as Verilog or VHDL [5-7]. High-level languages VHDL, Verilog and Verilog System in CAD Vivado are used for

modeling and for creation of the synthesizable descriptions. Vivado important property is the ability to control the entire development cycle using Tcl scripting language, which is the basis of the new format of the description of design constraints xdc (Xilinx Design Constraints). Xdc format has, in comparison with the ucf format, previously used, more flexible description of design constraints, which facilitate the construction of scalable projects.

The aim of this work is to create a project using CAD Vivado 2016.2, associated with the description of the designed device on a high-level Verilog language, synthesis, simulation, with the temporary work diagrams construction and with the diagram implementation of digital generator

pseudo-random impulse sequence based on PLIC of FPGA families from Xilinx company and eight-rate linear feedback shift register, as well as the development of an electrical circuit of the noise generator, which creates an acoustic and vibro-acoustic noise to protect speech information.

2 Synthesis and simulation of digital pseudo-random impulse sequence circuits

In order to achieve the aims of the work there is launched CAD Vivado 2016.2 by the shortcut on your desktop. Opens the start screen of CAD Vivado 2016.2 Quick Start (Figure 1).



FIGURE 1 CAD Vivado 2016.2 Quick Start

As can be seen, on the Quick Start screen there can be created a new project, opened an existing one and you can familiarize with ready examples of projects or documentation CAD Vivado 2016.2.

In order to create a new project on the Quick Start screen select the command Create New Project and open the Project Name window (Figure 2).

In the Project Name field enter the name of the project, and in the Project location field specify the directory of location of the project, where it will be stored.

Thus, in the Project location field you can see the path to the previously created folder on the desktop.

Open the Project Type window and select the type of the RTL (Register Transfer Level) Project to create a project on the level of register exchanges using hardware description languages, for example, Verilog. Register transfer level (RTL) - a way of describing the operation (behavior) of synchronous digital circuits on the register level, logic signals and logic operations on the signals.

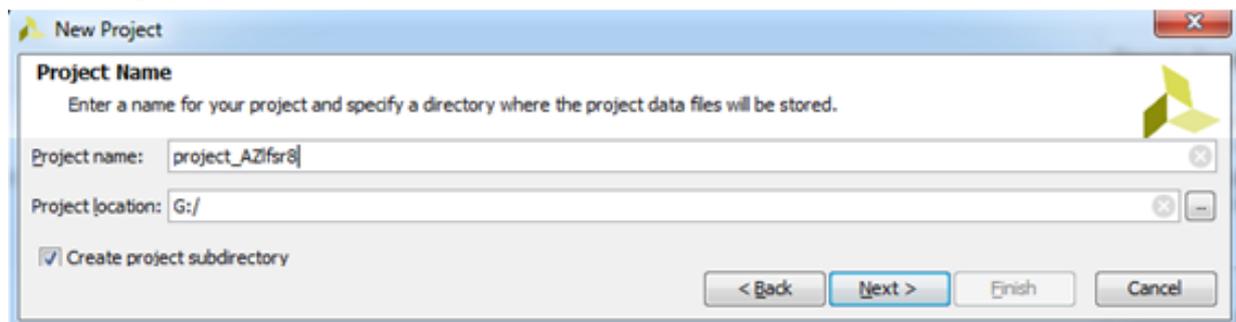


FIGURE 2 Project Name window for new project creation

Circuit or description entering of the designed device can be carried out by various methods, including circuit design.

In this work in order to describe the projected devices we use high-level Verilog language. Open the Add Sources window and then with the help of Create File button open a Create Source File panel (Figure 3).

In the File type field select Verilog, in the File Name field specify the name AZregoc8 file, and in the File location field specify the path where the file is stored.

Next, using a USB cable, connect BASYS 3 DIGILENT board to the computer.

In the FPGA folder select Basys3_Master.xdc file that allows you to add pre-defined rules and restrictions. Specify the location of the Basys3_Master.xdc file. Open the Default Part window (Figure 4).

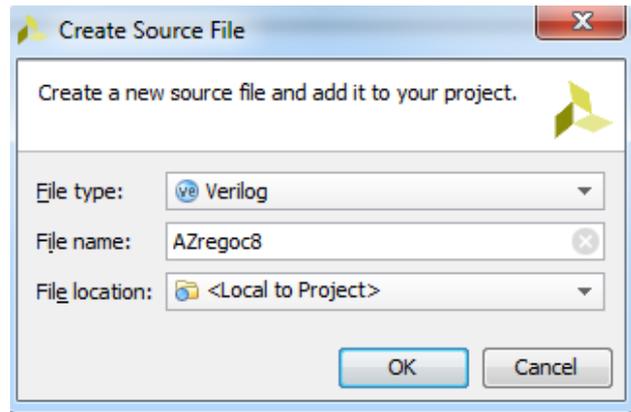


FIGURE 3 Create Source File panel

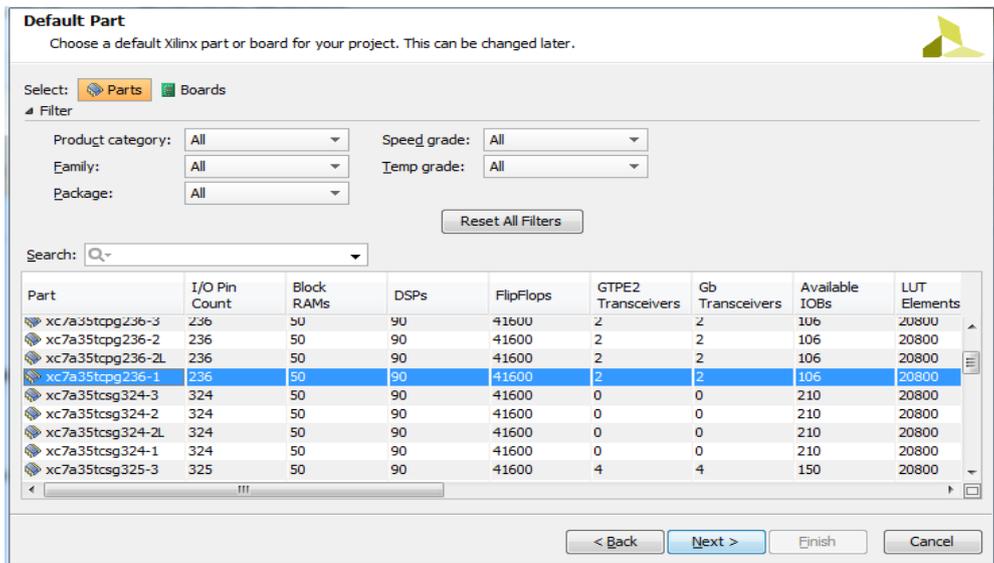


FIGURE 4 Default Part window

From the table Part, which lists the various micro schemes models of the BASYS DIGILENT board, choose xc7a35tcbg236-1 model and enter it in the Search field for the project implementation.

The window New Project Summary opens, click on the Finish button. In the Define Module window in the Port

Name field specify the names of the input and output ports in accordance with the scheme or program on Verilog language of the designed digital pseudo-random impulse sequence generator on the basis of eight-rate shift register LFSR with synchronous pulse clk, rst reset signal, enable permission signal and output signals reg [7: 0] Q (Figure 5).

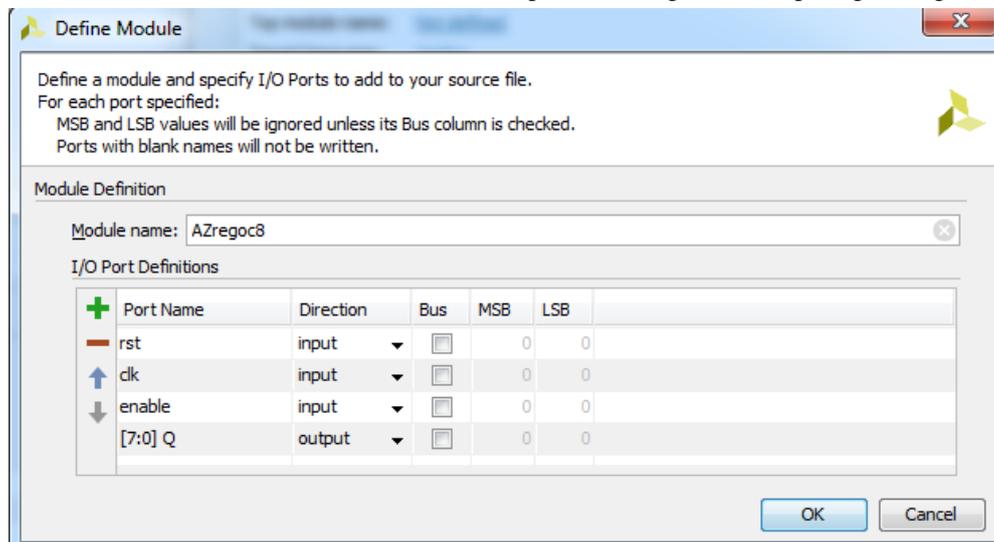


FIGURE 5 Define Modules window

Open the Project Manager window (Director - Project Manager). In this window open the Restrictions folder and select the file Basys3_Master.xdc in the folder constrs_1 (Figure 6). Open it with the Open Selected Source Files.

From the set of signals description Basys3_Master.xdc, which also shows the results of the BASYS 3 DIGILENT board, select and activate the input and output signals needed for our project. Basys3_Master.xdc file contains information for the development environment how the logical inputs and outputs AZregoc8 of the main module are connected with the location (LOC) of the physical legs of FPGA micro schemes, which are referred as PIN W5, PIN V17, PIN V14, etc. On

the Figure 7 there is shown a stripped-down version of Basys3_Master.xdc file for this board.

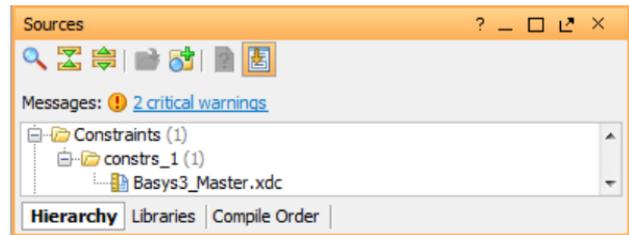


FIGURE 6 Project Manager window

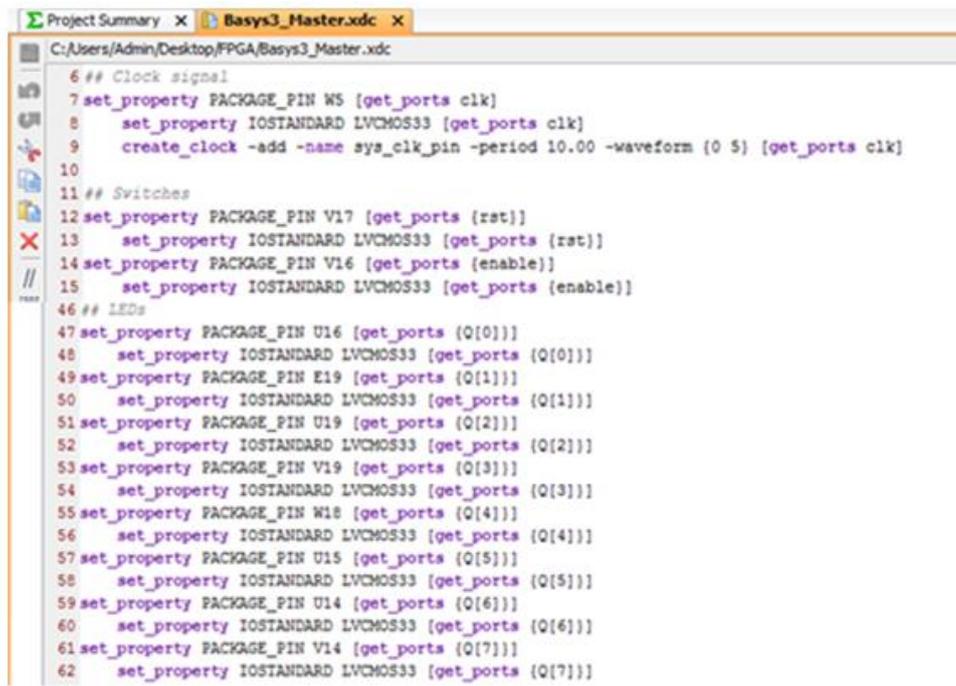


FIGURE 7 Basis3_Master.xdc file screenshot

Close Basys3_Master.xdc file. Next, in the Desing Sources folder open AZregoc8.v file and in the file add the pre-composed code text of the program on a high-level Verilog language in this file, which describes the operation of the digital generator pseudo-random impulse sequence diagram based on the eight-rate shift register LFSR. Close

AZregoc8.v file. Below, on the Figure 8 there is a screenshots of AZregoc8.v file. Close AZregoc8.v file. So the project is created. Next, using the Project Settings and the bit sequence Bitstream - bin_file, carry out the project setting. In order to open the synthesized circuit in Synthesis folder click on the Run Synthesis command.

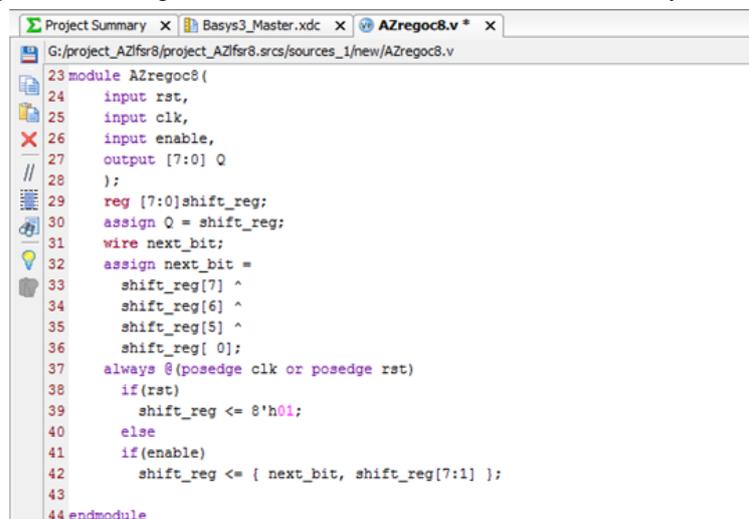


FIGURE 8 AZregoc8.v program screenshot

After the synthesis using the command Open Synthesized Design get a diagram of a digital pseudo-random impulse sequence generator based on the eight-rate shift register with the feedback LFSR, described on a high-level Verilog language (Figure 9).

In order to obtain a digital pseudo-random impulse

sequence generator circuit based on RTL - register transfer level run the Open Elaborated Design command. In the Schematic window appears abstract diagram of a digital pseudo-random impulse sequence generator based on eight-rate LFSR register with inputs clk, rst, enable, and outputs Q [7: 0] (Figure 10).

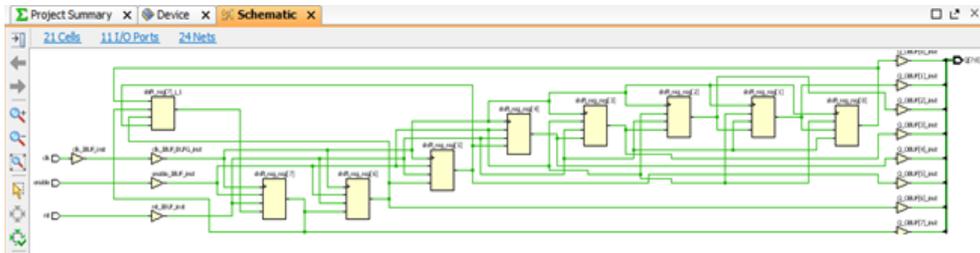


FIGURE 9 Screenshot of the digital pseudo-random impulse sequence generator based on the register LFSR

3 Construction of the temporary diagrams of the digital pseudo-random impulse sequence generator circuit operation

One of the major stages in the digital devices development based on PLIC is the simulation of the developed devices. In order to perform a behavioral simulation of the digital pseudo-random impulse sequence generator circuit based on the

LFSR register run the Run Behavioral Simulation command. There will be opened Behavioral Simulation panel.

In the Objects or Untitled 1 window indicate the necessary parameters of the circuit simulation, the desired value of the clock impulses clk, rst reset signal and the enable signal of the digital pseudo-random impulse sequence generator circuit based on eight-rate shift register LFSR.

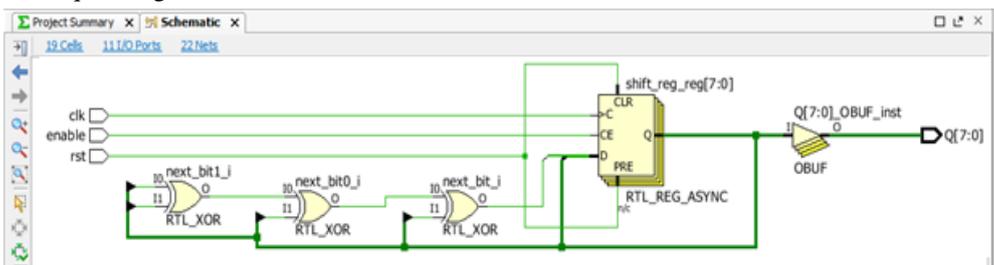


FIGURE 10 Screenshot of the the digital pseudo-random impulse sequence generator abstract circuit based on the LFSR register

At the beginning with the help of the Force Constant command make the shift register LFSR reset to "0". To construct a temporary operation diagrams of the digital pseudo-random impulse sequence generator based on the LFSR register select Force Clock command and indicate the threshold of the signal operation and the threshold of the trip signals.

Next, specify the time values for the beginning and completion of the register operation. Select the duration of the clock impulses clk. Specify the fill coefficient (the ratio of the impulse duration to the interval between impulses). Run the digital pseudo-random impulse sequence generator

circuit based on the LFSR register whose content according to each clock impulse clk is shifted to the right, and the new calculated bit slides into the shift register LFSR to the left.

The calculation of the new bit is made by the operation OR (XOR). The calculation of the new value of the shift register LFSR occurs in the line shift_reg <= {next_bit, shift_reg[7: 1]}. The next shifted bit next_bit is calculated by the assignment operation: assign next_bit = ... (see Figure 8).

Figure 11 shows the temporary diagrams of the digital pseudo-random impulse sequence generator based on eight-rate shift register LFSR.

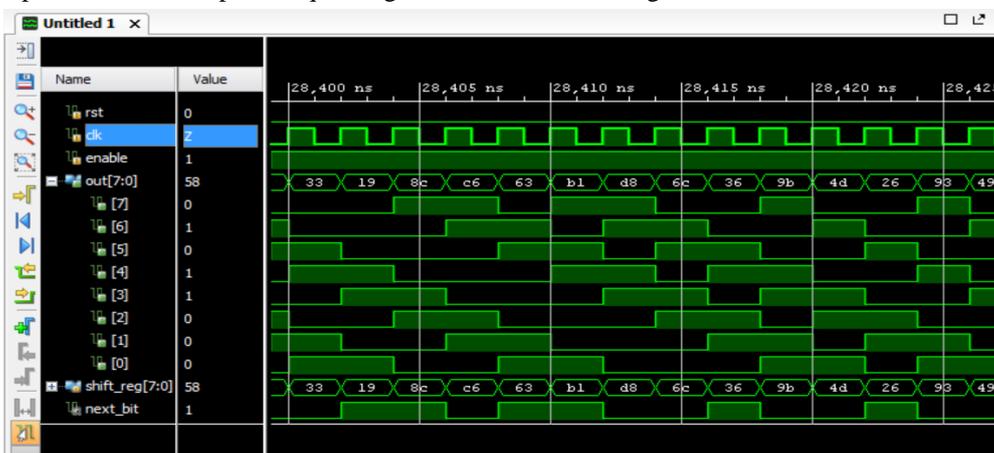


FIGURE 11 Screenshot of the digital pseudo-random impulse sequence generator based on eight-rate shift register LFSR temporary operation diagrams

For the implementation of the digital pseudo-random impulse sequence generator circuit based on the shift register LFSR (for the programming of PLIC) activate Run Implementation command on FPGA BASYS 3 DIGILENT board and run the Program and Debug Generate Bitstream. If the board is connected by the USB cable to a computer, the lights on the board start to blink in accordance with the impulses generated by the digital pseudo-random impulse generator based on the shift register LFSR (Figure 12). Therefore, the shift register LFSR with the feedback operates as the digital pseudo-random impulse generator with pseudo-random intervals between them.

With the help of CAD Vivado and Verilog language there have been created various digital devices projects (decoder, multiplexer, D-trigger, adder, register, digital counter, etc.), related to the creation of the xc7a35tcpg236-1 micro scheme describing modules of the Basys 3family, with the synthesis, simulation and project implementation on the basis of PLIC of the FPGA families from Xilinx company.

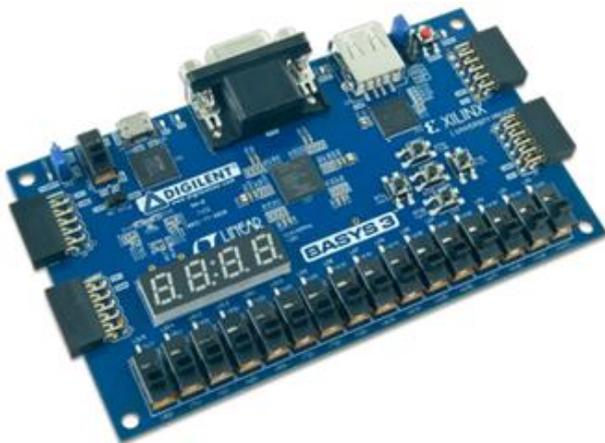


FIGURE 12 PLIC FPGA BASYS 3 DIGILENT board

The frequency of the generated impulse sequence of the shift register LFSR with the feedback allow to use it as a digital counter. A digital counter based on such generator

has a simplified feedback circuit, unlike ordinary binary counters, and therefore, can operate at high clock frequencies. However, you must make sure that such a digital counter is never entered in the zero state. For this purpose there is an enable signal in the register. Unlike conventional digital counter, shift register LFSR with the feedback moves from one state to another not in a binary count, that allows to use it to generate a test signal for error detecting in logic circuits. Digital pseudo-random impulse sequence generator based on shift register LFSR is used very often for stream ciphers in cryptography. Large random numbers generated from the sequence bits of the digital generator based on shift register LFSR are strongly correlated and sometimes not even random at all. However, digital generators based on the shift register LFSR can be used to create basic cryptographic algorithms [9, 10]. It should be noted that the digital pseudo-random impulse sequence generator synthesized using CAD Vivado 2016.2, can be used to generate masking vibration noise.

4 Development of the acoustic noise generator scheme

Noise vibrations are created for protection from illegal removal of confidential acoustic (speech) information. For wiretapping and unauthorized recording of voice information attackers can use a variety of technical means: wiretapping devices, laser wiretapping system, stethoscopes, voice recorders, and others.

In order to mask speech signals there is proposed noise generator electrical scheme, which creates an acoustic and vibro-acoustic noise (Figure 13). The structure of the acoustic noise generator includes a digital pseudo-random impulse sequence generator, built on the basis of eight-rate shift register with the feedback on the triggers of the D-type, multivibrator which generates the clock impulses, logic elements (LE) "OR" (XOR) and "NOT" by which the feedback is carried out, active filter of the low frequencies of the second order at the operational amplifier (OA) and piezoceramic transducer ZQ.

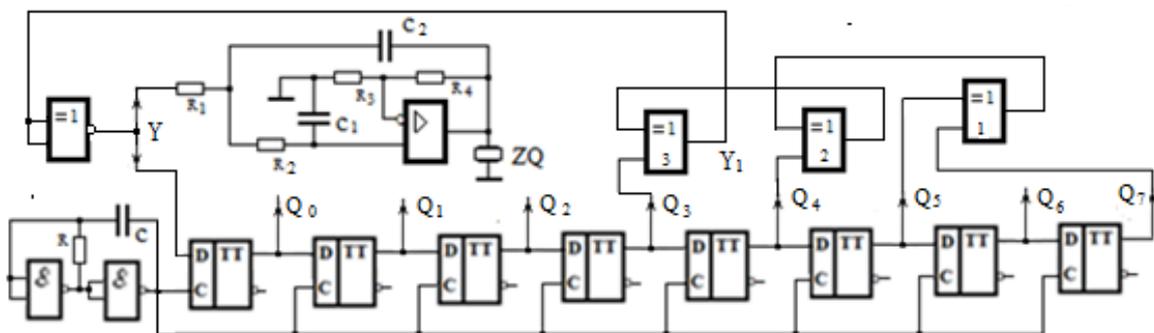


FIGURE 13 Digital pseudo-random impulse sequence generator and acoustic noise electrical scheme

Consider the operation principle of pseudo-random impulse sequence generator circuit on the basis of the shift register with the feedback. Zero state of the shift register with the feedback when the triggers of all bits are at logic 0 state (output trigger signals $Q_0 = Q_1 = \dots = Q_7 = 0$) is not working. In other words, the output code 000 ... 0 is a disabled state, as it blocks the operation of the digital pseudo-random sequence generator. In the shift register there should be entered something other than zero, otherwise the shift register will remain at zero and the zeros

will run around in the shift register.

Feedback is carried out from the trigger outputs of the 7th-, 5th-, 4th- and 3-rd register bit through the two-input logic elements "OR» (XOR – addition according to the module 2). To exclude the zero forbidden state of the shift register at the output of the last LE-3 XOR there is used an inverter (NOT logic element). Due to the use of the inverter the forbidden state of the digital generator will be a 1111 ... 1 code (instead of the code 000 ... 0), which in this case is eliminated by the initial resetting of the shift register to zero

at power-on signal R_a (shift register reset signal to zero is not indicated in the diagram). The generator produces a pseudo-random sequence of eight-bit codes from all register triggers, as well as pseudo-random sequence of zeros and ones from the output of any of the register triggers.

At zero register state at the logic element LE-3 "OR" output there will be a logic 0 signal ($Y_1 = 0$), and the output of the LE "NOT" - logic 1 ($Y = 1$) and the unit signal arrives to the trigger input of the zero bit of the shift register.

In order to obtain the first clock impulse of the multivibrator the feedback signal $Y = 1$ from the output of the digital generator is recorded to the trigger of the zero register bit and at the same time the register content is shifted by one bit to the right. At the same time the register content is as follows: $Q_0 = 1, Q_1 = Q_2 = Q_3 = Q_4 = Q_5 = Q_6 = Q_7 = 0$ that corresponds to the number 1. The feedback signal is $Y = 1$. Therefore, after the second clock impulse to the zero bit trigger the signal of a logic 1 is recorded, and the register content is shifted right again by one bit and the register will have a number 3 ($Q_0 = Q_1 = 1, Q_2 = Q_3 = Q_4 = Q_5 = Q_6 = Q_7 = 0$).

The feedback signal Y will still be equal to 1 ($Y = 1$). This 1- signal is recorded to the trigger of the zero bit after the third clock impulse and after register content shift will have number 7. After next multivibrator clock impulses the bit triggers state and the register content (register number) will vary pseudo-randomly, that means - generated sequence of numbers (impulses) will be pseudo-random before $2^8 - 1$ impulse.

In general, at n -bit shift register there can be generated m - code sequences of pseudo-random impulses where $m = 2^n - 1$. The pseudo-random code numbers (impulses) sequence differs from a true random interval, but within a period has no differences from the truly random.

Pseudo-random code numbers sequence corresponding to $m = 2^n - 1$ can be removed from any trigger output of shift register any bit as the same sequence comes with temporary shift from the trigger output of each bit. At a relatively large n value a pseudo-random sequence is virtually identical to the random sequence.

It should be noted also that acoustic noise generated by a digital pseudo-random impulse sequence generator, also provides protection against wiretapping by using embedded devices and dictaphone recording in the office of the head of the organization or the negotiations conducted in specially designated rooms for this purpose.

The digital output of the shift register, generating a maximum length sequence, can be converted into white noise with limited band by using a low frequency filter whose cutoff frequency is considerably lower than register clock frequency. The useful range of the noise generated by a digital pseudo-random sequence generator extends from the low frequency border, reverse to the repetition period, to high frequency border equal to about 20% of the clock frequency (at this frequency the noise power per hertz falls by 0.6 dB) [5]. In order to use a part of the spectrum, much closer to the clock speed, it is advisable to apply filters with a steeper cut, such as Butterworth, Chebyshev or Sallen - Key filters.

In this work, in order to create acoustic noise to the output of a digital pseudo-random impulse sequence generator there is connected the active low-pass filter (LPF) of a Sallen - Key second-order on the basis of the operational

amplifier, a load of which is a piezoceramic transducer ZQ (Figure 13). In the Sallen-Key scheme the capacitors C_1 and C_2 are selected with the same capacity. Resistors R_1 and R_2 are selected with the same resistance. Typically, the minimum capacity is selected. Such capacitors have a maximum stability in characteristics. Then, define the resistance value of R_1 and R_2 :

$$R_1 = R_2 = 1/2\pi f_p C,$$

where $C = C_1 = C_2$, f_p - pole frequency.

The pole resonance frequency is determined according to the following formula:

$$f_p = 1/\sqrt{R_1 R_2 C_1 C_2}.$$

Resistors R_3 and R_4 in the Sallen-Key scheme determine the voltage gain in the same way as in a conventional inverting amplifier circuit.

In the scheme of the active RC filter the amplifier is covered by both negative and positive feedbacks. Positive feedback depth ratio is determined by resistors R_1 and R_2 or capacitors C_1 and C_2 . The operational amplifier operates according to the non-inverting amplifier circuit.

Active LPF, cutoff frequency of which is small in comparison with the frequency of the multivibrator clock impulses, converts digital noise (pseudo-random impulse sequence) to the analog.

Digital noise is a temporary random process, similar by its properties to the physical noise process and therefore is called "pseudo-random process".

5 Conclusion

In conclusion, it should be noted, that in this work with the help of CAD Vivado 2016.2 system and Verilog hardware description language there was synthesized, simulated and built temporary digital pseudo-random impulse sequence generator operation circuits based on PLIC of the FPGA families of the Xilinx company, which can be used in cryptography to create stream encryption algorithms.

On the basis of the digital pseudo-random impulse generator and active low-pass filter of the Sallen - Key second order, the load which is a piezoceramic transducer ZQ, there was built a electrical circuit of the acoustic noise generator which by creating a masking vibration noise provides protection against wiretapping by using embedded devices, laser wiretapping system and unauthorized dictaphone recording of confidential voice information.

In future it is expected to improve the cryptographic strength of the generated sequences with relatively large periods, linear complexity and good statistical properties through improvement of the digital pseudo-random impulse sequence generator based on the use of shift registers LFSR with different clocking (with a complicated clocking scheme).

This work relates to the field of information security for the creation of cryptographic keys for encrypted data transfer, and can also be used in systems of confidential speech information protection (for example, for protection of negotiations in the office of the head or in a room specially designated for this purpose) by means of an acoustic noising at the audio signals frequencies.

References

- [1] Harris D, Harris S 2013 *Digital circuit design and computer architecture* Second edition. Morgan Kaufman Publishing House, English Edition 1619 p.
- [2] Tarasov I. E., Pevtsov E F 2012 *Programmable logic circuits and their application in circuit design: Textbook* M.: MSTU MIREA 184 p.
- [3] Zotov V Y 2003 *Design of digital devices based on PLIC of the Xilinx company in CAD WebPACK ISE* M.: Hotline-Telecom 624 p.
- [4] Amosov V V 2007 *Circuitry and design tools of digital devices* BHV-Petersburg 542 p.
- [5] *VIVADO - a new development tool of Inline Group* plis.ru/docum/sredstvarazbotki_i_ip/vivado_- novoe sredstvo razrabotki
- [6] *The new version of CAD Vivado Design Suite 2016.1* www.komponenta.ru/about / news / novaya-versiya-sapr-vivado-design-suite
- [7] Polyakov A K 2003 *VHDL and VERILOG languages in the design of digital equipment* M.: SOLON-Press 320 p.
- [8] *The shift register with linear feedback* <https://ru.wikipedia.org/wiki>
- [9] Kuznetsov V M 2011 *Pseudo-random sequences generator on digital delay elements. Abstract of dissertation for the degree of Doctor of Technical Sciences* Kazan: KAI
- [10] Sizonenko A B 2012 Multichannel digital sound source based on the recurrence shift register *Journal "Special equipment and communication"* 3

AUTHORS	
	<p>Zaurbek Aizhan</p> <p>Current position, grades: student of group ВТнПО-13 п (5b070400) – (Computing engineering and software -13 Russian) Kazakh National Research Technical University to the name K.I. Satpayev, 4-course.</p> <p>Publications: More than 7 publications</p>
	<p>Nurgul Seilova</p> <p>Current position, grades: Head of department Information Security</p> <p>University studies: candidate of technical Sciences</p> <p>Scientific interest: network technologies, Information Security</p> <p>Publications: More than 30 publications</p> <p>Experience: 15 years of teaching experience and 3 years in managerial positions</p>
	<p>Juruntaev Joldas</p> <p>Current position, grades: Associated professor of department of Informative safety</p> <p>University studies: doctor of technical Sciences</p> <p>Scientific interest: Synthesis and design of digital devices on basis Programmable logic integrated circuits FPGA with the use automatic projection system Vivado 2016.2; technical equipments of defence of acoustic (speech) information; author of two textbooks circuit "Technology" on Russian and Kazakh the languages produced on permission of Department of Education and Science of Republics of Kazakhstan.</p> <p>Publications: more than 60 scientific reasons, more than 50 Teaching developments.</p> <p>Experience: 50 years of teaching experience.</p>