# Analysis and synthesis of codes of generators in Quartus II

1st Vasyl Kychak
*Faculty of Infocommunications, Radioelectronics and Nanosystems*
*Vinnytsia National Technical University*
Vinnytsia, Ukraine
vvkychak@gmail.com

2nd Volodymyr Tromsuk
*Cycling commission radio engineering*
*Vinnitsa Technical College*
Vinnytsia, Ukraine
2013tvd@gmail.com
orcid: 0000-0001-5022-8159

3rd Serhii Tsyrulnyk
*Cycling commission radio engineering*
*Vinnitsa Technical College*
Vinnytsia, Ukraine
sovmsvom@gmail.com

4th Artem Metelitsa
*Cycling commission radio engineering*
*Vinnitsa Technical College*
Vinnytsia, Ukraine
artemmetelicha@gmail.com

5th Yaroslav Borodai
*Cycling commission radio engineering*
*Vinnitsa Technical College*
Vinnytsia, Ukraine
bortamu@mail.ru

6th Vasyl Tkachuk
*Cycling commission radio engineering*
*Vinnitsa Technical College*
Vinnytsia, Ukraine
tkachuk333@mail.ru

***Abstra t* — This work is devoted to the design and modeling of code sequence generators as the basic elements of noise immunity and cryptographic systems. The paper considers the construction of reversible generators of code sequences, which, although having a lower rate of operation, have a much higher noise immunity. Designing and developing such generators facilitates special software such as Quartus 2. This program allows you to obtain a code sequence generator, time charts and performance analysis.**

***Keywords* — *Code sequence generator (CSG), boolean function, Carnot map, shift register, Quartus II.***

## I. Introduction

Code sequence generators are most often used in information technology, as the basic elements of the diagnostics of communication systems, statistical simulation, and design, as well as in solving mathematical problems. CSG occupy a prominent place in modern information security systems. Particularly important roles in this important area are generators of pseudorandom binary sequences that used as the basic elements of streaming data protection algorithms, as well as for generating keys for symmetric algorithms and pseudorandom binary rows of authentication protocols for remote users of integrated computer and telecommunication systems [1-4]. The basis of another component of modern information security systems – symmetric data encryption algorithms – are generators of pseudorandom boolean functions and systems of functions that have specific properties. In modern conditions, increasing the productivity of computing systems and the ability to combine a large number of computers to violate data protection, the problem is an adequate increase in the reliability of information security, including the means based on the use of CSG.

The protective functions of code sequences and Boolean transformations are theoretically determined by the fundamental impossibility of analytically solving the system of nonlinear equations. This property of such transformations underlies the use of binary sequences and boolean functions in modern information security algorithms. Therefore, the level of data tampering with code sequences depends on the nonlinearity of the boolean transformations that are used when generating such sequences. Therefore, an important reserve for the enhancement of a wide range of information security means is to improve the structure of the generation of sequences in the direction of increasing the nonlinearity of the boolean transformations they use [5-9].

The growth of the speed of computing systems and the speed of digital data transmission in telecommunication networks creates more stringent requirements for the performance of information security devices, including the basis of which is the use of CSG: they must provide the implementation of the formation of elements of the sequence in the rate of data transmission [4].

Thus, at the present stage of the development of the technology of information protection in systems and networks, the problem of developing ways to increase the efficiency of generating code binary sequences becomes more relevant.

## II. The purpose and objectives of the study

The aim of the work is to increase the efficiency of the application, to protect the information in telecommunication systems, code binary sequences by improving the hardware of their generation and improving their characteristics, which determine the ability to counteract unauthorized access to data and protection against interference.

The main objectives of the study in accordance with the stated goal are as follows:

1. To construct the main switching graph of the reverse CSG.

2. Using the Carnot diagram, obtain the reverse oscillation of the right-side shift (SRSI) and left-side shift (SLSI) excitation.

3. Check the reverse code sequence generator for self-esteem.

4. Build a complete switching graph of code sequence generator.

5. Simulation of the work of the designed code sequence generator in Quartus II.

6. Determination of ways to improve software and hardware implementation of the code sequence generator.

Methods of research are based on the theory of boolean functions, combinatorics, computer simulation.

## III. Designing a reverse CSG

The design of any CSG begins with the definition of its destination and creature polynomial. We design a reverse oscillator generator based on the creature polynomial $x^5 + x^4 + x^2 + x^1 + 1$. Such a generator will produce the same code sequence, both when shifting to the left, and when shifting to the right with high speed.

At the next stage, it is necessary to determine with a bit of a reversible shift register. The bit size of the register should be such that code combinations do not repeat. For a given polynomial, the minimum bitness of the reversible shift register, in which the code combinations without repetitions are provided, will be n = 6. The corresponding code sequence, in the decimal system, for the polynomial considered, will look like 27, 55, 46, 29, 59, 54 and 45.

Based on the resulting code sequence, we will construct a switching graph of the GCP, which shown in Fig. 1

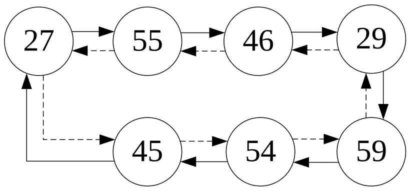
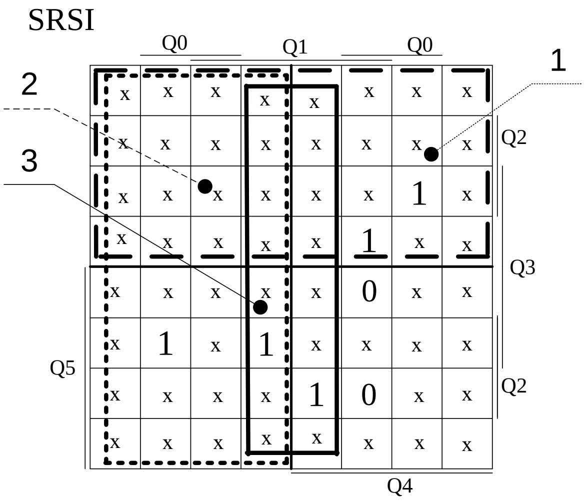


Fig. 1. Switching graph of CSG

The next step is to get the excitation function of the shift register [7-8]. To do this, fill out the Carnot map, for the excitation function of the SRSI shift register, as shown in Fig. 2



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| x | x | x | x | x | x | x | x |
| x | x | x | x | x | x | x | x |
| x | x | x | x | x | x | 1 | x |
| x | x | x | x | x | 1 | x | x |
| x | x | x | x | x | 0 | x | x |
| x | 1 | x | 1 | x | x | x | x |
| x | x | x | x | 1 | 0 | x | x |
| x | x | x | x | x | x | x | x |

Fig. 2. Carnot Map for SRSI Offset Excitation Function

To obtain the excitation function of the shift register, you must insert the numbers of the main switching graph (Fig. 1) into the Carnot card, as shown in Fig. 2. The numbers are entered so that if before the number, which is entered in the Carnot diagram is a pair number, then in the cell under the corresponding number is put 0, if the number is odd – 1. Next, you must circle the maximum number of units and unidentified states *x* multiple, where m = 0, 1, ..., 6.

We write the equation for the SRSI (the code shift to the right) excitation function and rewrite this equation in the basis of the I-NOT.

$$SRSI = \bar{Q}_5 + \bar{Q}_4 + Q_1\bar{Q}_0 = \overline{\overline{\overline{Q_5 Q_4} + Q_1\bar{Q}_0}} = \overline{Q_5 Q_4 \overline{\bar{Q}_0 Q_1}}. \qquad (1)$$

To obtain the inverse of the excitation of the SLSI (the code shift to the right) shift reversal register, it is necessary to replace the variables: changing the younger digits of the older and vice versa.

$$Q_0Q_1Q_2Q_3Q_4Q_5$$
$$Q_5Q_4Q_3Q_2Q_1Q_0$$

Thus, the excitation function of the SLSI shift register (left shift combination) will look like:

$$SLSI = \bar{Q}_0 + \bar{Q}_1 + Q_4\bar{Q}_5 = \overline{\overline{\overline{Q_0 Q_1} + Q_4\bar{Q}_5}} = \overline{Q_0 Q_1 \overline{\bar{Q}_5 Q_4}}. \qquad (2)$$

Based on the excitation functions (1) and (2), we construct a functional scheme of the GCP, which depicted in Fig. 3. To construct such a circuit, it is necessary to use an eight-digit reversible shift register of RG, six single-bit MUX multiplexers, two inverters, and four I-NOT elements.

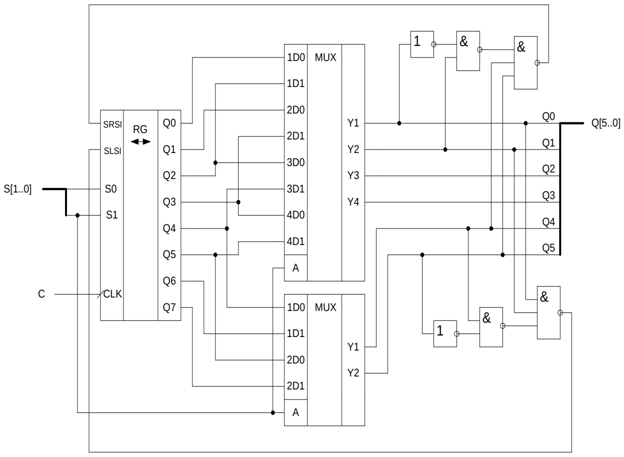


Fig. 3. Functional scheme of the CSG

The resulting functional scheme (Fig. 3) will act as a reversible CSG, but before that, it is necessary to test it for self-esteem. If the CSG will not be self-sustaining, then under the influence of external barriers, it can exit the main and work further in the parasitic cycle [9].

## IV. Check CSG for self esteem

Verification GCP, as a rule, carry out after receiving the function of excitation, but in this case, it is advisable to do this after the construction of the scheme. This allows us to see what rather scheme the implementation of the developed reversible CSG will have. Verification CSG to self-esteem performed by the formula:

$$N^+ = \begin{cases} 2N + x_N, & N < 2^{n-1}, \\ 2\left(N - 2^{n-1}\right) + x_N, & N \geq 2^{n-1}, \end{cases} \qquad (3)$$

$N^+$ – the decimal number of the test cycle; $N$ – decimal number from the test cycle; $n$ – CSG bit size; $x_N$ – can acquire the values 0 or 1, depending on the determined cell state in the Carnot diagram.

Using formula (3), all the states of the reversible CSG are checked, which do not belong to the main switching graph (Fig. 1). In order to test for self-esteem, you need to build a complete switch graph. To do this, we take any state outside of the working cycle, and by formula (3) we define the next state, but we now substitute the values of $x_N$ from the term diagram: for those codes which, according to the minimization performed, are units of units, $x_N = 1$. This means that it is necessary to check the numbers from 0 to 63 ($2^6 = 64$ combinations), except for the numbers belonging to the main switching graph. The calculations are quite cumbersome, so we will not bring them into this work.

Consequently, it is clear from the verification that the designed CSG is self-sustaining since we do not have parasitic cycles. According to the conducted self-esteem test and the conclusions are drawn, we will construct a complete switching graph of the reverse CSG, which depicted in Fig. 4.

## V. Design CSG in Graphic Editor Quartus II

To test the performance of a designed reversing CSG it is necessary to modify it. This can be done easily in Quartus II. To do this, you need to create a project in which to create a graphics file, where will be constructed scheme CSG (Fig. 5) and vector waveform file (Fig. 6), where the timing diagrams CSG will receive.

The construction of a reversing GCP scheme is complicated by the fact that it is necessary to set the control signals S [1..0] correctly, which determine which side of the assigned code combination (exercises or left) will move. At S = 01, the shift will be provided to the right, and at S = 10 – to the left.

Timing diagrams show that the reversible CSG works according to the main switching graph (Fig. 1) and does not

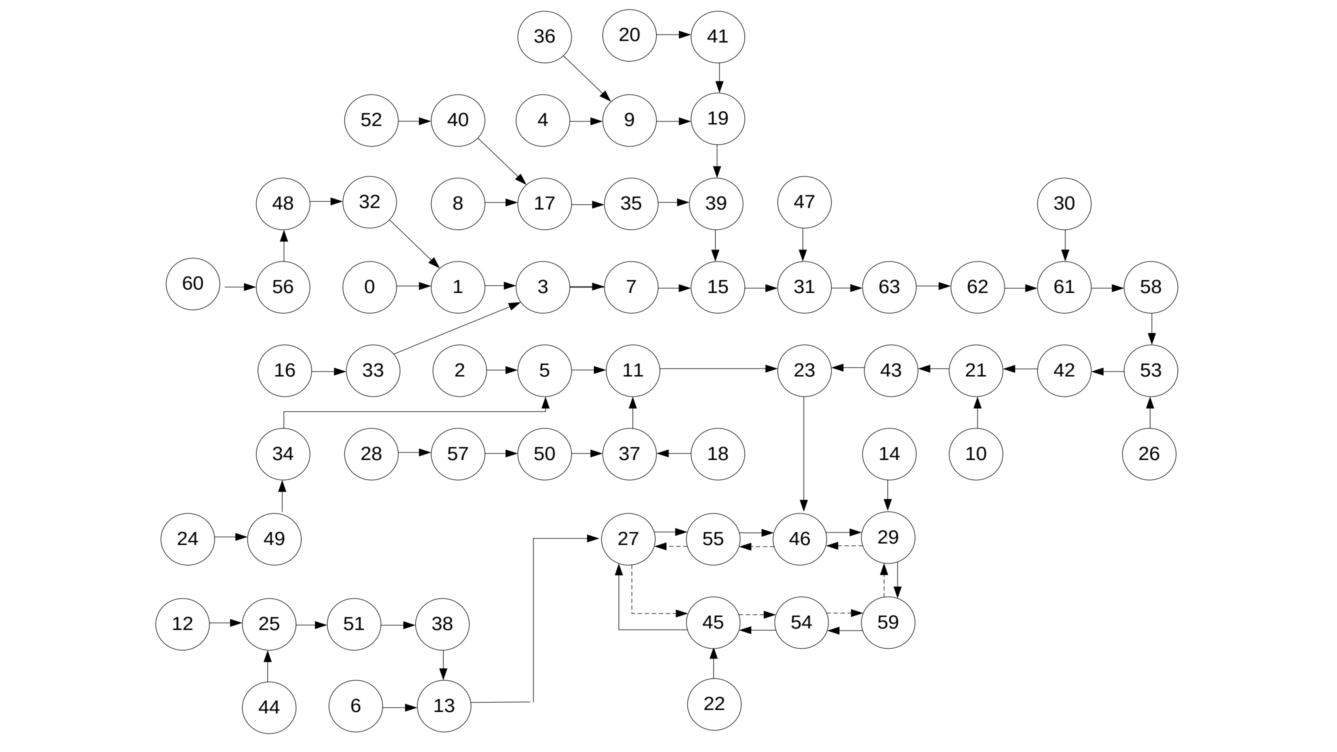


Fig. 4. Full switching graph of reverse CSG

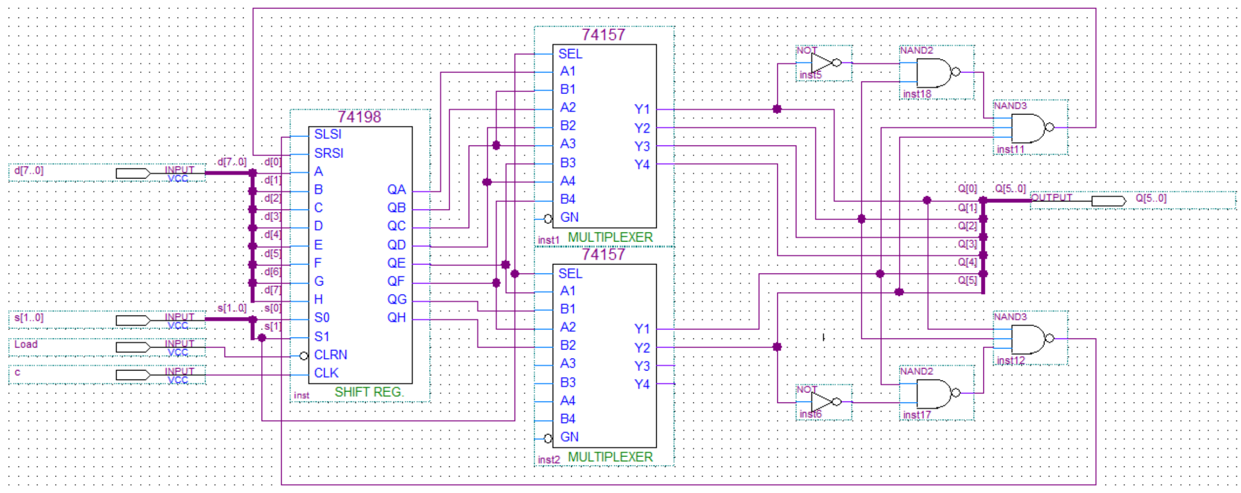


Fig. 5. Implementation of a reversible CSG in Quartus II

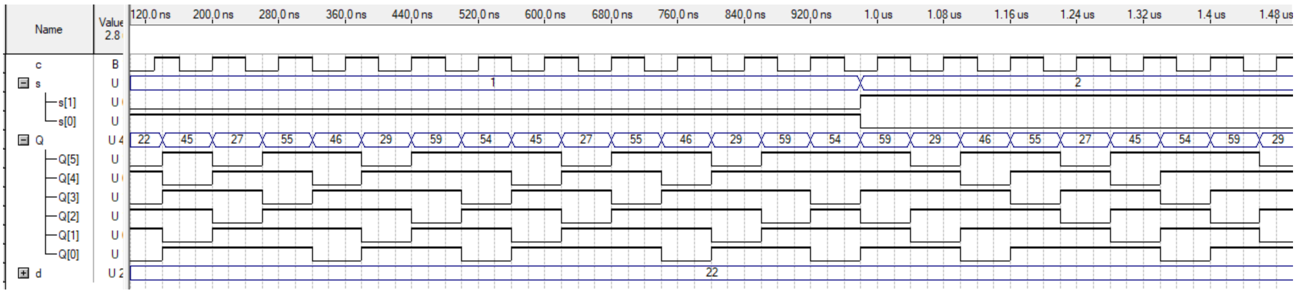
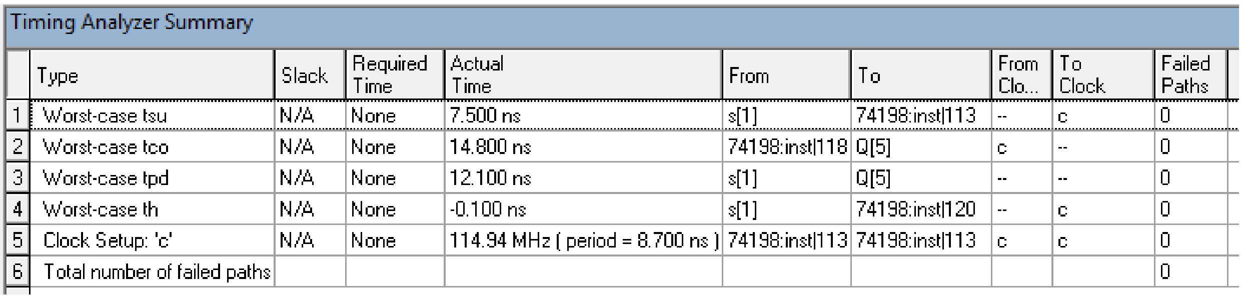


Fig. 6. Time charts of the reverse CSG

go beyond its limit, neither when it is offset to the right (S = 01) nor with the shift to the left (S = 10).

A timed analysis showed that the developed reversible CSG has a high performance and is resistant to external impediments. Results of time analysis are shown in Fig. 7.



Timing Analyzer Summary

| | Type | Slack | Required Time | Actual Time | From | To | From Clo... | To Clock | Failed Paths |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Worst-case tsu | N/A | None | 7.500 ns | s[1] | 74198:inst\|113 | -- | c | 0 |
| 2 | Worst-case tco | N/A | None | 14.800 ns | 74198:inst\|118 | Q[5] | c | -- | 0 |
| 3 | Worst-case tpd | N/A | None | 12.100 ns | s[1] | Q[5] | -- | -- | 0 |
| 4 | Worst-case th | N/A | None | -0.100 ns | s[1] | 74198:inst\|120 | -- | c | 0 |
| 5 | Clock Setup: 'c' | N/A | None | 114.94 MHz ( period = 8.700 ns ) | 74198:inst\|113 | 74198:inst\|113 | c | c | 0 |
| 6 | Total number of failed paths | | | | | | | | 0 |

Fig. 7. Timing Analyzer Summary

## CONCLUSIONS

The method of designing n-bit shifting registers with a nonlinear feedback function for generating pseudorandom binary sequences with a repetition period of $2^n$ and high characteristics of complexity and nonlinearity is developed on the basis of the creature polynomial. Completed verification of GCP to self-esteem. Modeling of reversing CSG in Quartus II is carried out. Simulation confirms the performance of a designed reversible CSG.

## REFERENCES

[1] V. Kychak, V. Tromsyuk "Initial data processing algorithms of bit error rate testers" // Modern problems of radio engineering, telecommunications and computer science (TCSET'2016) : materials of Proceedings of the International Conference. Lviv: Lviv Polytechnic, 2016. P. 566–568

[2] V. Kychak, V. Tromsyuk "Sorting Method of Relative Positions of Synchroimpulses by Frequency of their Occurrence" // Journal of Automation and Information Sciences. New York. Begell House. Volume 48, Issue 10, 2016, Pages 49-56.

[3] Jian Ren, "Design of Long Period Pseudo-Random Sequences from the Addition of m-Sequences over Fp ", EURASIP Journal onWireless Communications and Networking 2004:1, 2004 Hindawi Publishing Corporation ,pp 12-18.

[4] V. Kychak, V. Tromsyuk "Assessment method of parameters and characteristics of bit errors" // Journal of Automation and Information Sciences. New York. Begell House. Volume 49, Issue 5, 2017, Pages 59-71.

[5] E. Dashofy, "Supporting stakeholder-driven, multi-view software architecture modeling," Ph.D. dissertation, UCI, 2007.

[6] V. Kychak, V. Tromsyuk "Calculation of parameters of errors in radioelectronic and telecommunication systems". Vinnytsia. VNTU. 2017. P. 76-77.

[7] Fisher Jean-Dernard. An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding / Jean-Dernard Fisher, Stern Jacques // EUROCRYPT'96 Proceeding, LNCS 1070. – P. 245-255.

[8] G. Bortnik, M. Vasylkivskyj "Phase jitter estimation in radio channels of telecommunication systems" / Modern Problems of Radio Engineering, Telecommunications and Computer Science – Proceedings of the 11th International Conference, TCSET'2012. – 2012. – P. 307.

[9] Mitić D. Calculating The Required Number of Bits In The Function of Confidence Level and Error Probability Estimation / D. Mitić, A. Lebl, Z. Markov // Serbian Journal of Electrical Engineering. – 2012. – Vol. 9, №. 3 – P. 361-375.