# Examination of optimal settings for a Gollman generator

Yuriy Kostiv[1], Maria Mandrona[1,2], Volodymyr Maksymovych[1], Oleh Harasymchuk[3], Yuriy Malynovskiy[4]

[1]Chair of Security of Information Technologies, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 12, E-mail: yura.kostiv@gmail.com

[2]Department of Information Security Management, Lviv State University of Life Safety, UKRAINE, Lviv, Kleparivska street 35. E-mail: mandrona27@gmail.com

[3]Academic Chair of Data Protection, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 12, E-mail: garasymchuk@ukr.net

[4]Theoretical and Applied Economycs Department, Lviv Polytechnic National University, 12 Bandery street, Lviv, UKRAINE

***Abstract – The article provides the reader with the results of an examination of a Gollman generator with a fixed number of basic m-sequence generators and different values of degrees of their polynomial. The examination was conducted using NIST statistical tests. The results obtained thereby allow to optimise the settings of the generator with specified output pulse sequence settings.***

Key words – pseudorandom generator, protection of information, pseudorandom numbers, statistic characteristics.

## I. Introduction

As computer and measuring equipment undergoes rapid development with implementation of innovative technologies, random and pseudorandom sequence generators widen the scope of their application, and therefore new requirements arise with regard to their design and the methodology to be applied in the assessment of their quality.

Determining the quality and operation reliability of random and pseudorandom sequence generators is a task of paramount importance

The purpose of the present research work is to examine the quality of a Gollman generator by way of changing its settings — specifically, by altering the value of the degree of the generative polynomial — and to use a set of NIST STS statistical tests in order to determine which settings are optimal for the generator.

## II. Results and Discussion

A Gollman generator is comprised of several consecutively connected m-sequence (shift registers) generators whereby the timing of each one of such constituent generators is regulated by its respectively preceding generator (Fig.1) [1, 2]. The output of a Gollman generator thus corresponds to the output of its last constituent m-sequence generator.

Conceptually, the present variety of generators is relatively simple in its design and may be used to generate pseudorandom sequences with long periods, linear complexities and satisfactory statistical properties.

In the present research work, in order to generate pseudorandom sequences, we are going to use five Gollman generators constructed on the basis of three M-sequence generators with their generative polynomials provided in Table 1.

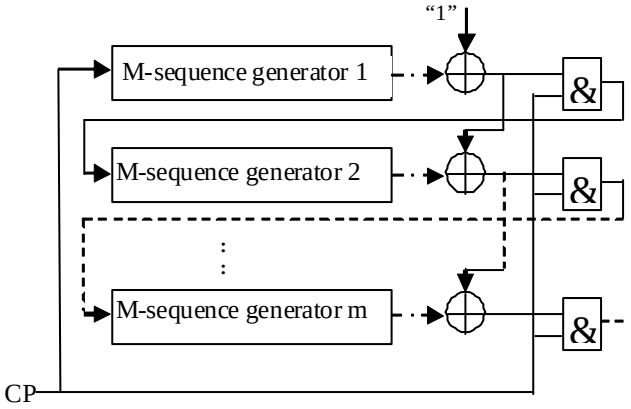


Fig. 1. Line chart of a Gollman generator

TABLE 1

GOLLMAN GENERATORS EXAMINED IN THE PRESENT RESEARCH WORK

| Number of the examined PRSG | Gollman generator functioning equation |
|---|---|
| **1** | $\Phi(x) = 1 \oplus x^6 + x^7$ |
| **2** | $\Phi(x) = 1 \oplus x^{12} + x^{17}$ |
| **3** | $\Phi(x) = 1 \oplus x^{18} + x^{25}$ |
| **4** | $\Phi(x) = 1 \oplus x^{18} + x^{31}$ |
| **5** | $\Phi(x) = 1 \oplus x^{42} + x^{47}$ |

Assessment of the generator's quality is conducted using a package of NIST STS statistical tests [4, 5]. As of now, no results of such an assessment of the Gollman generator can be found in presently available scientific literature. Therefore, we have used the Delphi programing language to design simulation models of such a generator. These simulation models allow us to determine output sequences depending on changes being made in the settings.

A set of NIST STS tests includes 15 statistical tests designed to corroborate the hypothesis of randomness of binary sequences of random length generated by PRSG [3].

Therefore, as a result of tests applied to a binary sequence, the vector of values of probabilities is formed: $P=\{P_1,P_2 \ldots P_{188}\}$.

The tests were conducted with the significance level of $\alpha = 0{,}01$ — as recommended by the NIST developers. The statistical portraits of generators are depicted as a matrix, size 1000×188 which is comprised of 188,000 values of corresponding probabilities.

Using the methodology [5], we have determined the limits of the confidence range; if the result of the conducted test falls within the 0.999439 – 0.0980561 range, then we conclude that the test has been successful; if the result is outside the above range, then the test has been unsuccessful. All figures display the confidence range in red dashed lines.

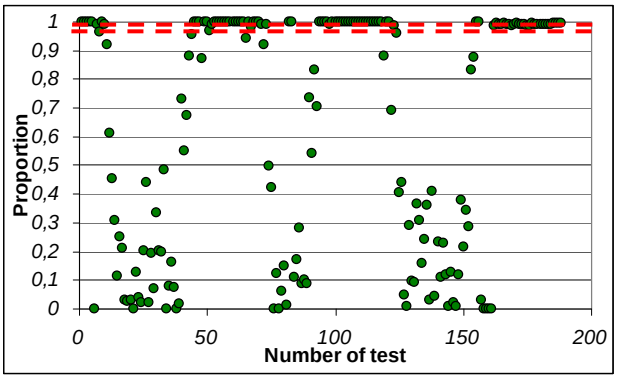


Fig. 2. Statistical portrait of the Generator No. 1

As the Figure 2 shows, the Generator No. 1 has bad statistical characteristics. Almost all of the test results are outside the confidence range.

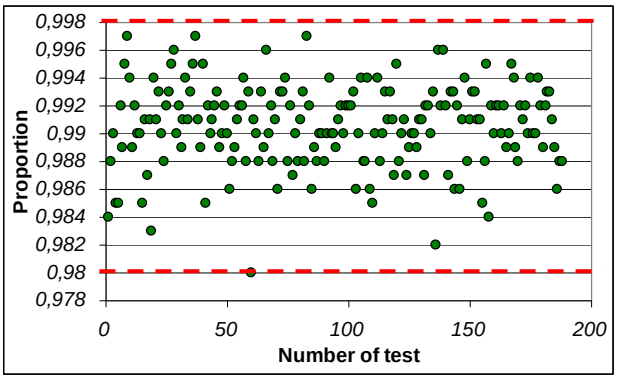


Fig.3 Statistical portrait of the Generator No. 3

The characteristics of the generator shown at Figure 3 have substantially improved since all of the tests have been passed here with only one of the results being outside the confidence range.

A detailed report on the assessment of Gollman generators is provided in Table 2, wherein it is stated which tests specifically have and which have not been passed successfully.

TABLE 2

RESULTS OF TESTS APPLIED TO GOLLMAN GENERATORS

| № | Statistical Test | No. Generators | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 1. | Frequency (Monobit) Test | - | + | + | + | + |
| 2. | Frequency Test within a Block | - | + | + | + | + |
| 3. | Cumulative Sums (Cusum) Test | - | + | + | + | + |
| 4. | Runs Test | - | + | + | + | + |
| 5. | Test for the Longest Run of Ones in a Block | - | + | + | + | + |
| 6. | Binary Matrix Rank Test | - | + | + | + | + |
| 7. | Discrete Fourier Transform (Specral) Test | - | + | + | + | + |
| 8. | Non-Overlapping Template Matching Test | - | - | + | + | + |
| 9. | Overlapping Template Matching Test | - | + | + | + | + |
| 10. | Maurer's "Universal Statistical" Test | - | + | + | + | + |
| 11. | Approximate Entropy Test | - | + | + | + | + |
| 12. | Serial Test | - | + | + | + | + |
| 13. | Linear Complexity Test | - | + | + | + | + |
| 14. | Random Excursions Test | - | + | + | + | + |
| 15. | Random Excursions Variant Test | - | + | + | + | + |

As one can see from the figures and the Table 2, the results of tests starting from Generator No. 3 are positive.

## Conclusion

The examination has shown that an increase of the degree of the generative polynomial leads to an improvement in the generator's quality.

The results of the testing of five Gollman generators have shown that the first generator with a generative polynomial of the 7th degree has not passed all of the tests. This indicates that the sequence contains repetitive sections located close to each other — which in turn indicates that there is a deviation from the random character of the examined sequence. The second generator has not passed three tests only, which means it cannot be used in cryptography but can be used as an element of a more complex cryptographic system. Other generators — that is, No. 3, 4, 5 — have passed all the tests successfully. This means that these generators have good prospects of future application in the information protection systems. The results received thereby allow to optimise the settings in the process of construction of a high-quality generator of random sequences.

## References

[1] M. A. Ivanov and I. V. Chugunkov Ed., Teorija, primenenie i ocenka kachestva generatorov psevdo-sluchajnyh posledovatel'nostej [Theory, application, and quality assessnent of pseudorandom sequence generators]. Moscow: KUDITS-OBRAZ Publ., 2003.

[2] O. I. Harasymchuk and V. M. Maksymovych, "Heneratory puassonivskoho impulsnoho potoku na osnovi heneratoriv M-poslidovnostei" ["Poisson Pulse Sequence Generators based on m-sequence generators"], Visnyk NU "Lvivska politekhnika" "Kompiuterni nauky ta informatsiini tekhnolohii" – Herald of the Lviv National Polytechnic University "Computer Sciences and Information technologies", no. 521, pp. 17-23, 2004.

[3] O. I. Harasymchuk and V. M. Maksymovych, "Heneratory psevdovypadkovykh chysel, yikh zastosuvannia, klasyfikatsiia, osnovni metody pobudovy i otsinka yakosti" ["Pseudorandom number generators, their application, classification, principal methods of construction and assessment of quality"], Naukovyi zhurnal "Zakhyst informatsii" – Journal "Information Protection", no. 3, pp. 29-36, 2002

[4] NIST SP 800-22. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Crypto-graphic Applications", csrc.nist.gov. [Online]. Available:http://csrc.nist.gov/publications/nistpubs//SP800-22rev1a.pdf [Accessed: April. 2010].

[5] I.D. Horbenko and Iu.I. Horbenko Ed., Prykladna kryptolohiia: Teoriia. Praktyka. Zastosuvannia: monohrafiia [Applied cryptology: Theory. Practice. Application: a monograph]. – Kharkiv: Publishing House «Fort», 2012.