International Journal of 3D Printing Technologies and Dijital Industry
Uluslararası 3B Yazici Teknolojileri ve Dijital Endüstri Dergisi

RESEARCH OF PERIODIC PROPERTIES OF PSEUDO-ACCIDENTAL NUMBERS GENERATORS, BASED ON THE USE OF EXCESS BLOCK CODES

Roman Korolev [a]*, Serhii YEVSEIEV[b]

[a] Ivan Kozhedub Kharkiv University of Air Force, UKRAINE
[b] Simon Kuznets Kharkiv National University of Economics, UKRAINE

*Corresponding Author: korolevrv01@ukr.net

(**Received:** 20.04.2019**; Revised:** 21.05.2019**; Accepted:** 02.07.2019**)**

ABSTRACT

The development of computational technology and the growing needs of Internet resources are putting forward new demands on the quality of service for users of global and local computational networks based on Ethernet technologies. The main criteria for the quality of network user service are reliability and security. To ensure reliability, as a rule, methods based on jam resistant coding or protocols with decision-making feedback are used. For security, cryptographic protocols for symmetric and asymmetric cryptography, hashing algorithms and digital signatures are used. Random number generators occupy a special place among the mechanisms that ensure the reliability and security. This work discusses the methods of forming sequences of pseudo-random numbers (SPRN), the stability of which is based on the theoretical complexity problem of syndromic decoding. Periodic properties of generators are investigated, it is determined that the formed sequences do not have a maximum period.

Keywords: Random number generators, maximum period, security, jam resistant coding.

1. STATEMENT OF THE PROBLEM IN GENERAL FORM AND ANALYSIS OF THE LITERATURE

In work [1], statistical security studies of the most common SPRN generators were conducted: a generator based on the SHA-1 algorithm [3,5], a linear congruential generator [2, 5], a generator RC4 [5], a quadratic congruent generator [2], a generator based on the DES algorithm, generator based on the 3-DES algorithm [4], Blum-Blum-Shub generator [2, 4, 5], the US national AES encryption algorithm (FIPS-197) in the counter mode [8], provably stable generator based on the problem of syndromic decoding [10] (Generator Provably as Secure as Syndrome Decoding – (GPSSD)) [9]. Studies have shown that the considered generators have high rates of statistical security. The highest results were shown by the GPSSD generator a provably secure SPRN generator, the stability of which is substantiated by the theoretical complexity problem of syndromic decoding.

Thus, based on the experimental results obtained in [1], it can be affirmed that GPSSD is the most promising in terms of statistical safety. In addition to the largest number of tests that were conducted according to the NIST STS methodology [7], this generator belongs to a group of algorithms to which the concept of “Provable Security”, studied in detail in [6], can be applied. Practically, it means that the problem of cryptanalysis (calculating the secret key) of the SPRN generator can be reduced to one of the well-known theoretical complexity problems, for example, factorization, discrete logarithmation, etc. At the same time, the problem of estimating the efficiency of the GPSSD generator by other security indicators remains unstudied (period length of the formed sequences, structural secrecy, etc.). The purpose of this article is to study the periodic properties of the GPSSD generator, an assessment of the lengths of the periods formed by the SPRN.

2. STRUCTURE AND FEATURES OF THE GPSSD METHOD IMPLEMENTATION

The method of forming SPRN based on redundant codes was first proposed in [9]. It is based on the formation of the SPRN fragment according to the syndromic sequence of the redundant block code, which in turn is formed by the recurrent rule as a function of the secret key. The stability of the GPSSD generator is based on reducing the task of finding the secret key to solving the problem of syndromic decoding. The structural diagram of the GPSSD method is shown in Figure 1.

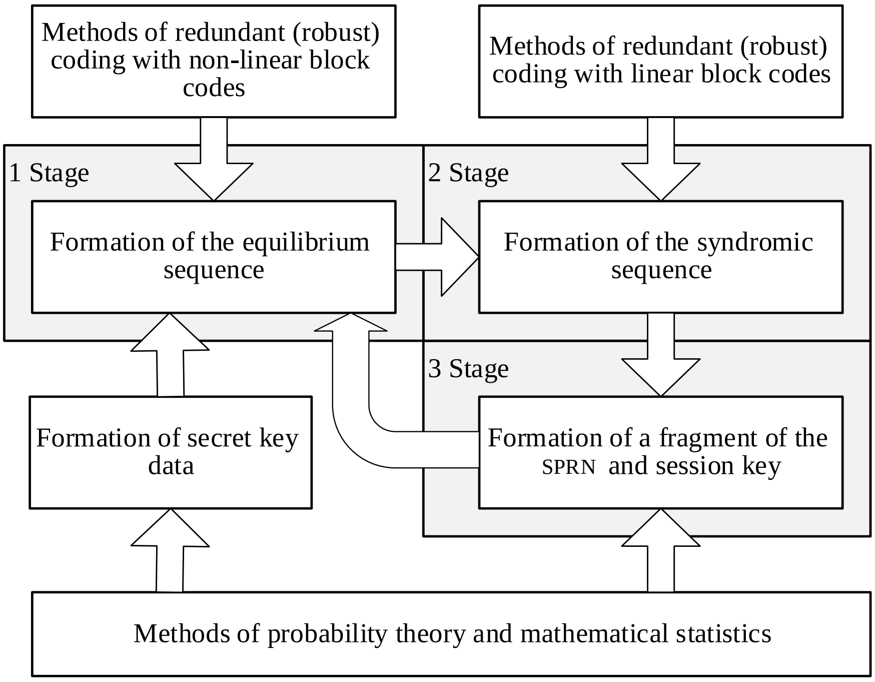
Methods of redundant (robust) coding with non-linear block codes
Methods of redundant (robust) coding with linear block codes
1 Stage
2 Stage
Formation of the equilibrium sequence
Formation of the syndromic sequence
3 Stage
Formation of secret key data
Formation of a fragment of the SPRN and session key
Methods of probability theory and mathematical statistics

Figure 1. Structural diagram of the GPSSD method.

At the first stage, using the methods of redundant (jam resistant) coding by nonlinear block codes, the equilibrium premises are formed according to the entered key sequence, corresponding to the entered secret key data. At the second stage, using the methods of redundant (jam resistant) coding by linear block codes, the syndromic sequences are formed according to the formed equilibrium premises. At the third and final stage, a fragment of the SPRN and a session key are used for the generated syndrome sequences using the methods of probability theory and mathematical statistics, which are used in further iterative generator procedures at the input of the first stage of the method. In [9], it was proposed to use the simplest division of the formed syndromic sequence into two parts: the first is used in further iterative procedures as a session key, the second is taken as the result of forming the SPRN fragment.

The process of forming SPRN using GPSSD is formalized by a combination of the following analytical relations:

- at the first stage, secret key data is entered

$$K_i = (K_{i_0} \quad K_{i_1} \quad \cdots \quad K_{i_{m-1}}), K_i \in K \subseteq GF^M(q), K_{i_j} \in GF(q) \qquad (1)$$

For the given feedback sequence

$$S *_{K_i} = \left(S *_{K_{i_0}} \quad S *_{K_{i_1}} \quad \cdots \quad S *_{K_{i_{m-1}}}\right), S *_{K_i} \in S *_K \subseteq GF^M(q), S *_{K_{i_j}} \in GF(q) \qquad (2)$$

(in the first round $S *_{K_i} = K_i)$) using equation

$$S *_{K_i} = \sum_{j=0}^{n-1} \left(\begin{matrix} j \\ C *_{K_{i_j}} \end{matrix} \right) \qquad (3)$$

establishing an equilibrium coding rule, i.e. converting a session key sequence into a binomial code sequence, an equilibrium sequence is formed

$C*_{K_i} = \begin{pmatrix} C*_{K_{i_0}} & C*_{K_{i_1}} & \cdots & C*_{K_{i_{n-1}}} \end{pmatrix}, \quad C*_{K_i} \in C*_K \subseteq GF^n(q), \quad C*_{K_{i_j}} \in GF(q), \quad w\left(C*_{K_i}\right) = w$
(4)

- at the third stage of the formed equilibrium sequence and the check H matrix of the redundant linear block (n, k, d) code using equation
  $S_{K_i} = C*_{K_i} \cdot H^T$ (5)

the syndromic sequence of the linear block code is formed, $r = n - k$:

$$S_{K_i} = \begin{pmatrix} S_{K_{i_0}} & S_{K_{i_1}} & \cdots & S_{K_{i_{r-1}}} \end{pmatrix}, S_{K_i} \in S_K \subseteq GF^r(q), S_{K_{i_j}} \in GF(q) \quad (6)$$

- at the fourth stage, a fragment of the SPRN and a feedback sequence are formed by the formed syndrome sequence by reducing the elements

$$S*_{K_i} = \begin{pmatrix} S*_{K_{i_0}} & S*_{K_{i_1}} & \cdots & S*_{K_{i_{m-1}}} \end{pmatrix}, S*_{K_i} \in S*_K \subseteq GF^M(q), S*_{K_{i_j}} \in GF(q)$$
(7)

used in the next cycle (round) of the first stage of the proposed method.

Thus, as the conducted studies have shown, at each round of transformations using the methods of nonlinear (equilibrium) and linear coding, a fragment of the PSAP is formed, as a selection (truncation) of the syndromic sequence of a linear block code. The remaining part of the syndromic sequence goes to the first stage of the next round of transformations.

3. RESEARCH METHODOLOGY AND THE MAIN RESULTS OBTAINED

To carry out studies of the periodic properties of the GPSSD generator, a software model has been developed that implements the process of generating PAPs using redundant block data. A binary code with parameters (64,24,16) was used as input data. The corresponding length of the secret key was a bit, the length of the syndromic sequence of bits, the length of the session key of a bit, the length of the FPCHP fragment formed at each iteration *40 – 24 = 16* bits. The expected length of the period.

During the research, the GPSSD generator was tested on a full set of non-zero key data (total tests). In each test, the length of the period L was estimated. As a result of the experiment, the distribution of the number of sequences N over the lengths of the periods *L*, shown in Figure 2, was calculated.

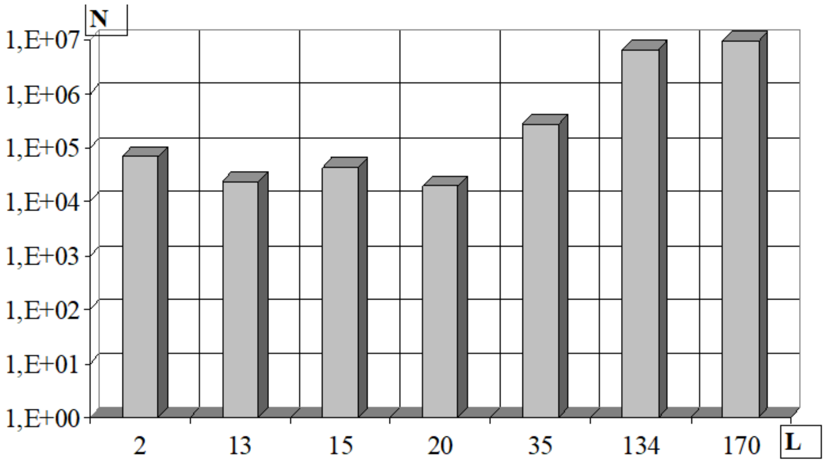

Figure 2. Distribution of the number of sequences by period length.

As follows from the figure. 2 data, the GPSSD generator forms sequences with a small period length *L = 2 – 170.* The largest number of sequences *(> 97%)* have a period of 134 or 170. At the same time, some sequences have an extremely short period *(L = 2–35)*. The analysis shows that the largest period of sequences, which allows you to create a GPSSD generator with the specified parameters, is $L = 170$, which is five orders of magnitude less than the maximum. Thus, it can be stated that a provably stable GPSSD generator with improved performance in statistical security [1] and speed [9] does not ensure the formation of sequences of the maximum period.

4. CONCLUSIONS

Studies have shown that a provably stable GPSSD generator, built using redundant block codes and having improved statistical security and speed indicators, does not ensure the formation of maximum period sequences, its periodic properties are unsatisfactory, which can cause the manifestation of effective cryptographic attacks.

A promising direction for further research is the development of an improved method based on redundant block codes, which, in addition to high rates of statistical security and speed, will allow the formation of sequences of a maximum period.

REFERENCES

1. Kuznetsov, A., Korolev, V., “Investigation of the statistical safety of pseudorandom number generators”, System processing information “HUPS”, Vol. 3, Issue 70, Pages 79-82, 2008.

2. Ivanov, M., “Theory, application and quality assessment of pseudo-random sequence generators”, p 240, 2003.

3. Popovsky, V., “Information security in telecommunication systems”, Kharkiv National University of Radio Electronics, Company Smith Company, p238, 2006..

4. Blum, L., “A Simple Unpredictable Pseudo-Random Number Generator”, Siam Journal on Computing, Vol. 15, Issue 2, Pages 364-386, 1986.

5. Schneier, B., “Applied cryptography. Protocols, algorithms, source texts in the C language”, Publishing house TRIUMPH, p819, 2002.

6. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, v. 0.15 (beta), Springer-Verlag, p829, 2004.

7. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22. Technology Administration U.S. Department of Commerce, Washington: National Institute of Standards and Technology, p164, 2000.

8. National Institute of Standards and Technology, “FIPS-197: Advanced Encryption Standard” [Articles in English], http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf , Accesed November 12, 2001.

9. Fisher, J. and Stern, J., “An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding”, EUROCRYPT’96 Proceeding, LNCS 1070, Pages 245 – 255, 1996.

10. McWilliams, F.J. and Sloan, N.J.A, “The theory of error correction codes”, Communication, p744, 1979.