UDC 004.056.2: 519.682
DOI: https://doi.org/10.17721/ISTS.2025.10.30-36

Irada RAHIMOVA[1], PhD (Engin.)
ORCID ID: 0009-0006-1969-9976
e-mail: ika1402@icloud.com

Abdul oglu Abbasquliyev EYYUB[1], PhD Student
ORCID ID: 0009-0003-7714-5494
e-mail: formemaybe23@yahoo.com

Yelyzaveta SEVRIUKOVA[2], PhD (Econ.)
ORCID ID: 0000-0002-0757-490X
e-mail: elizavetasevryukova@ukr.net

Tetiana LAPTIEVA[2], PhD (Engin.)
ORCID ID: 0000-0002-5223-9078
e-mail: tetiana1986@ukr.net

[1]Azerbaijan Technical University, Baku, Azerbaijan
[2]National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

EXPERIMENTAL EVALUATION OF THE EFFICIENCY OF CRYPTOGRAPHIC GENERATORS OF PSEUDO-RANDOM NUMBERS

Background. *In the digital era, ensuring information security requires reliable cryptographic primitives. A critical component of modern cryptographic systems is the generator of pseudo-random numbers (PRNG), which underpins key generation, digital signatures, initialization vectors, and other security mechanisms. The security of the entire system often depends on the unpredictability and statistical quality of the generated sequences. This study aims to conduct an experimental evaluation of the efficiency of various cryptographic PRNGs with respect to three criteria: statistical randomness, cryptographic resistance, and computational performance.*

Methods. *A comparative experimental analysis of multiple classes of cryptographic pseudo-random number generators was conducted. The study examined generators based on linear feedback shift registers (LFSRs), congruential methods, stream and block ciphers (e.g., RC4, AES, GOST 28147-89), and one-way functions (e.g., BBS, RSA, Micali–Schnorr). Evaluation criteria included statistical properties (via NIST SP 800-22 tests), resistance to cryptanalysis, and computational efficiency measured in processor operations per output bit.*

Results. *The experimental results demonstrate that generators based on block and stream ciphers (e.g., AES, GOST 28147-89) offer the best balance between cryptographic strength and performance. In contrast, generators based on one-way functions (e.g., BBS, RSA) provide provable security but suffer from low speed and suboptimal period length. Simple generators such as LFSRs and linear congruential generators exhibit high speed and good statistical properties but lack cryptographic resistance, making them unsuitable for direct use in security-critical applications.*

Conclusions. *The choice of a pseudo-random number generator must be guided by the specific requirements of the target application—balancing security, speed, and implementation constraints. For general-purpose cryptographic systems, cipher-based generators are recommended. For high-assurance environments where provable security outweighs performance concerns, number-theoretic generators may be appropriate. Future work should focus on hybrid designs, post-quantum readiness, and integration with hardware entropy sources to enhance robustness in resource-constrained and critical infrastructure settings..*

Keywords*: pseudo-random number generators (PRNGs), cryptographic security, statistical randomness, block ciphers, stream ciphers, one-way functions, cryptographic resistance*

Background

The rapid development of information technologies and the wide spread of automated data processing systems have caused a sharp increase in the volume of transmitted and stored information. This, in turn, made it necessary to increase the level of its protection against unauthorized access and cyberattacks. In modern conditions, information security is the most important factor in the stable functioning of critical infrastructures, financial systems, government services and commercial organizations. One of the key elements ensuring data protection are cryptographic methods, the basis of which is the generation of random numbers necessary for the formation of encryption keys, digital signatures, initialization vectors and other important parameters.

Generators of pseudo-random numbers (PRNs) are hardware and software tools designed to generate sequences of numbers that have certain statistical properties that are close to truly random. However, unlike physical sources of randomness, pseudo-random sequences are formed by deterministic algorithms, which makes it important to ensure their unpredictability and resistance to cryptographic analysis. The use of vulnerable or predictable generators can lead to serious security threats, including the compromise of keys and the complete breaking of the cryptographic system. For example, the vulnerability in the Dual_EC_DRBG algorithm confirms that the insufficient stability of the generator can jeopardize the protection of even widely used standards.

Today, there are many different approaches to building pseudo-random number generators. Among them, one can distinguish generators based on shift registers with linear and nonlinear feedback, congruent generators, solutions based on block and stream ciphers, as well as designs using one-way functions. Each of these types has its advantages and disadvantages: some provide high speed of operation, but have low cryptographic strength, others, on the contrary, guarantee a high level of protection, but require significant computing resources.

The purpose of this study is to conduct a comparative analysis and experimental assessment of various types of cryptographic generators of pseudorandom numbers according to three main criteria: the quality of the generated sequences, resistance to

© Rahimova Irada, Eyyub Abdul oglu Abbasquliyev, Sevriukova Yelyzaveta, Laptieva Tetiana, 2025

ISSN 2707-1758

cryptanalysis, and productivity. As part of the research, it is assumed that the most effective solutions will be identified, which will provide a balance between security and speed of work and can be recommended for use in modern cryptographic systems.

The obtained results have practical significance and can be used in the design and modernization of information protection systems, as well as in the selection of optimal algorithms for the generation of random numbers for specific tasks.

Statement of the problem. In the context of rapidly growing data volumes and expanding digital services, ensuring reliable information protection has become a top priority. The increasing number of cyber threats, advances in cryptanalysis, and the emergence of new computing paradigms—including quantum computing—pose additional challenges to security systems. PRNGs are a cornerstone of cryptographic protection, as they directly influence the generation of encryption keys, one-time passwords, digital signatures, and other critical parameters. The quality of a PRNG directly affects the resilience of the entire cryptographic system.

Insufficient robustness or predictability of PRNGs can lead to key compromise, loss of data confidentiality, and successful adversarial attacks. Moreover, key characteristics of PRNGs include not only cryptographic strength but also performance—especially in real-time systems and high-throughput environments. In practice, many solutions optimize for only one aspect: either high resistance with low speed or high performance with inadequate security.

The absence of a comprehensive evaluation framework for PRNG effectiveness complicates the selection of optimal solutions for specific information security requirements. Therefore, there is a clear need for a comparative analysis of existing PRNG approaches to identify their strengths and weaknesses and to formulate evidence-based recommendations for their deployment in contemporary cryptographic systems.

Analysis of the latest research and publications. Modern research in the field of generating random numbers and cryptographic algorithms emphasizes the need to create reliable and unpredictable GIS to ensure information security. Back in 1986, the author (Blum, 1986) laid the mathematical foundations of simple, but cryptographically stable GIS based on the complexity of the decomposition of large numbers. Research by M. Blum and S. Mykala (Micali, & Sidney, 1995; Rukhin, & Soto, 2001) showed the possibility of generating strong cryptographic sequences of bits, which became the foundation for modern encryption standards.

An important place among the studies is the assessment of the statistical properties of the HPS. So, in the work of A. Rukhin, and J. Soto (Rukhin, & Soto, 2001) proposed a set of standard tests that allow evaluating the quality of random sequences, which became the basis for cryptographic applications. R. Korolev (Korolev, 2009 Kuznetsov, 2007). investigated the statistical security and periodic properties of algorithms, including RC4, revealing potential vulnerabilities of stream ciphers and emphasizing the need for their constant analysis.

The development of random number generation methods is closely related to the improvement of cryptographic designs. Thus, in the works of S. Micali (Micali, & Sidney, 1995) methods of generation and joint use of pseudo-random functions for key management systems are proposed, and P. Morawiecki and J. Pieprzyk (Morawiecki, & Pieprzyk, 2013). considered parallel constructions of authenticated encryption based on a duplex scheme, which provides increased speed and security of data processing. Standards establish proven approaches to the generation of random numbers and cryptographically stable symmetric encryption algorithms.

Thus, the analysis of the presented publications shows that modern cryptography is based on a combination of theoretical models of the GPSCH, verification of their statistical reliability and the introduction of effective encryption designs (Prokushev, Ponomarenko, & Ponomarenko, 2021). This makes it possible to provide a high degree of information protection in various applications and forms the basis for further research in the field of cryptographic security.

The purpose of this article is to study modern approaches to the development and analysis of GPSCH used in cryptographic systems. Special attention is paid to the assessment of their statistical properties, cryptographic strength and compliance with international standards. Within the framework of the study, existing generation algorithms are considered, their strengths and weaknesses are identified, and methods of increasing the reliability and safety of HPS are analyzed to ensure effective information protection in modern conditions.

Methods

A comparative experimental analysis of multiple classes of cryptographic pseudo-random number generators was conducted. The study examined generators based on linear feedback shift registers (LFSRs), congruential methods, stream and block ciphers (e.g., RC4, AES, GOST 28147-89), and one-way functions (e.g., BBS, RSA, Micali–Schnorr). Evaluation criteria included statistical properties (via NIST SP 800-22 tests), resistance to cryptanalysis, and computational efficiency measured in processor operations per output bit.

Results

Generators pseudo-random sequences – technical a device intended for production sequences of pseudorandom numbers satisfying certain statistical properties. Conducted studies showed that generators pseudo-random sequences of their kind use possible will divide into two many classes: crypto-resistant and cryptographic vulnerable (Fig. 1) (Milevskyi et al., 2024).

Cryptographically vulnerable GPSPs have the same properties as crypto-resistant ones, but they have one drawback – they are low cryptographic stability, which leads to impossibility their of use in cryptographic systems protection information, their used in empirical tests, or as "building blocks" in development crypto-resistant GPSP. Let's consider more in detail given higher generators and conduct them comparative research (Bobok et al., 2025).

Generators pseudo-random sequences based on registers shift. Registers shift with linear reverse coupling (LFSR, Linear Feedback Shift Register) is generating devices pseudo-random sequence bits based on linear functions from the previous ones composed They are widely used in various areas, where required generation random or quasi-random sequences. They are divided into registers shift with linear reverse connection and non-linear reverse connection. Register shift consists of from two parts: register displacements and functions reverse connections:

- main positive qualities of GPSP on the registers shift are;
- high quick action (quantity operations per bit formable sequence);
- effective hardware and software implementation;

ISSN 2707-1758

- good statistical properties;
- maximum period formable pseudorandom sequence Pl_{max}.

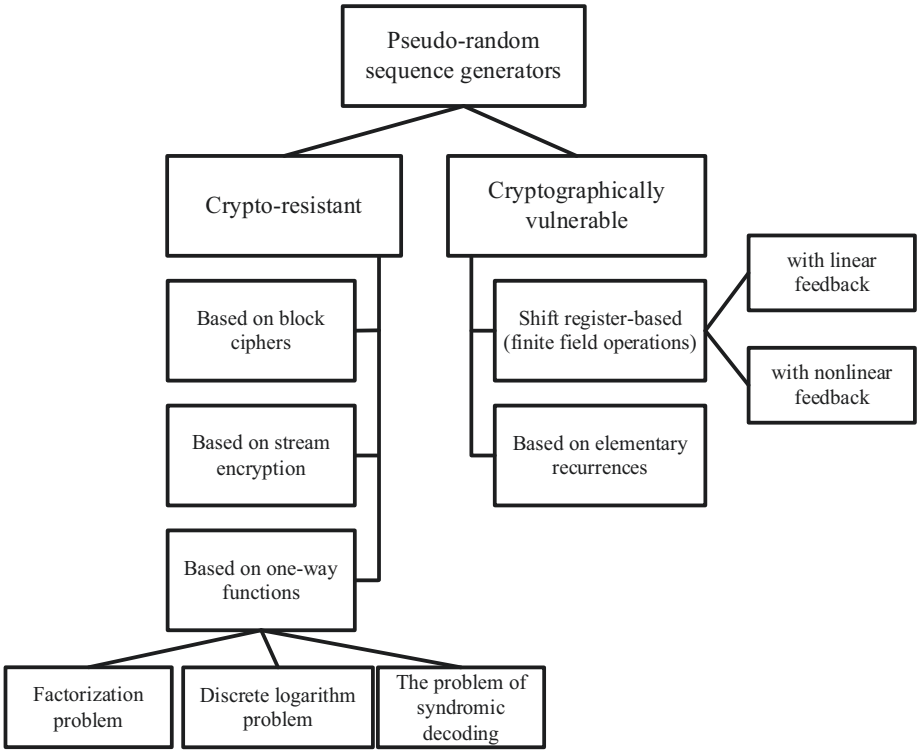


Fig. 1. Classification generators pseudo-random sequences

Main disadvantage these generators is their low cryptographic endurance In works it is shown that cryptanalysis must be intercepted$2l$ elements pseudorandom sequences to completely reveal function reverse connections.

Widely used class non-crypto-resistant generators are congruent generators. Let $x_0, a, c \in V_N$ – arbitrary fixed elements, then it is customary to say, that sequence $x_1, x_2 \dots x_n \in V_N$ is generated linear congruent generator with parameters $x_0, a, c \in V_N$, if this sequence satisfies recurrent ratio:

$$x_i = (ax_{i-1} + c) \, mod \quad N, \quad i = 1,2,\dots \tag{1}$$

Parameter$x_0 \in V_N$ is called initial value, parameter $a \neq 0$ – multiplier, c –increment N - field power. In case $c = 0$ ratios determines *multiplicative congruent generator*, and in case $c \neq 0$ – linear congruent generator. The period of such generators does not exceed N, if $x_0, a, c \in V_N$ selected correctly, then the period will be will be the maximum equal $N - 1$

Main advantages of congruent generators are recognized: speed formations pseudorandom number (due to the small amount operations), effective software and hardware realization, maximum period forming sequences. However, main the deficiency expressed in them predictability does not allow to use them in the system cryptographic protection information.

Examples generators based on current ciphers are recognized stream cipher with variable with a key length of RC4, the WAKE algorithm.

RC4 (Rivest Cipher 4, Ron's Code) – developed stream cipher by Ronald Rivest in 1987. The RC4 cipher was used in some widespread standards and protocols such as WEP, WPA and TLS (until 2015).

Main advantages stream encryption algorithm RC4 are recognized high speed enough work small the size of the key. RC4 is enough vulnerable, if are not used randomly or linked keys, one key stream used twice. These factors, as well as way can be used make the cryptosystem dangerous, vulnerable.

Main positive the quality of GPSP, built on the basis of current ciphers, appears high speed conversion, compatible so at speed receipts incoming information Thus, it is ensured formation of PSP in a real time scale.

Next class crypto-resistant generators GPSP built on block ciphers.

Currently time developed large quantity block ciphers, many from which are national or departmental standards. The biggest popularity acquired such block ciphers as DES, AES, GOST 28147-89. They are studied by many cryptographers have not lost their relevance even now. The work of such ciphers is applied to a block of open multiple text mathematical transformations Multiplicity applications leads to the fact that resulting transformation it turns out cryptographically more complicated than the conversion itself.

One of representatives of block -symmetric cipher working in the gamma mode is GOST 28147-89.

One of regimes work GOST 28147-89 was the gamma mode, the structural diagram of which is presented in fig. 2.

Open data are divided into blocks of 64 bits each and encrypted in the gamma mode by the way household addition modulo 2 in the adder CM_5 with gamma cipher, which is generated in blocks of 64 bits. Initial filling drives N_1 and N_2 (synchronization S) are encrypted in simple mode replacements in the key memorable a 256-bit key is written to the device. In drives N_1 and N_2 64-bit binary is entered sequence S = (S_1, S_2, ..., S_{64}), which serves initial filling for the next one generation of M blocks gamma cipher 64-bit open block encryption algorithm data in idle mode replacements includes 32 cycles.

ISSN 2707-1758

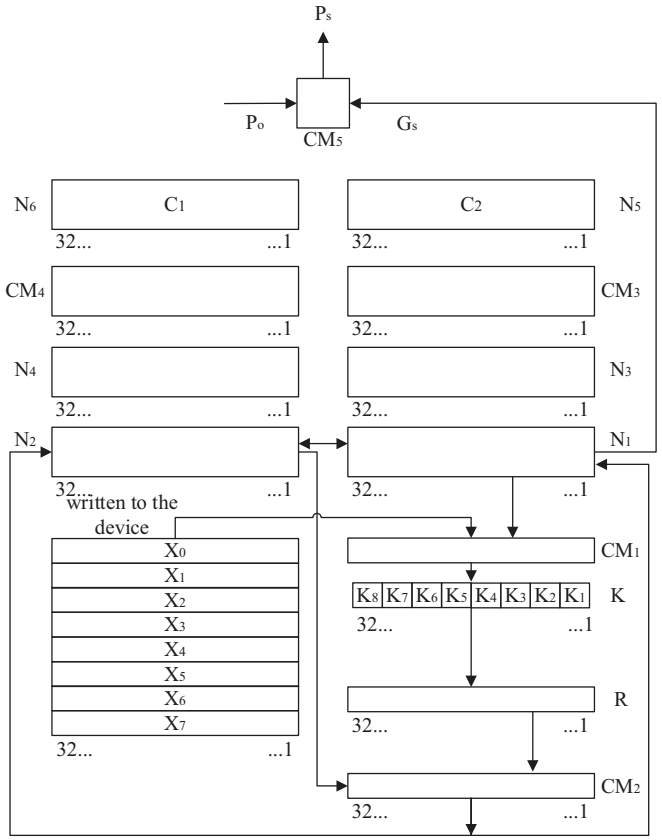


Fig. 2. GAMMIROW mode GOST 28147-89

The first cycle contains content storage unit N_1 is added modulo 2^{32} in the adder CM_1 with content storage X_0, at the same time data in N_1 are preserved. The resulting result passes through the substitution block K, then what the transformed vector enters the register R, where is being done cyclical a shift of 11 positions in the direction of senior ranks. Result shift everyday is added modulo 2 in the adder.

CM_2 with 32-bit content storage N_2. Result from CM_2 is written in N_1, and before contents N_1 is transferred to N_2. After encryption data from N_1 and N_2 are written to 32-bit drives N_3 and N_4: the contents of N_1 – in N_3, and N_2 – in N_4.

The content of N4 is added modulo $(2^{32}–1)$ in adder CM_4 with the 32-bit constant C_1 from drive N_6, the result is recorded in N_4. The contents of N_3 are summed modulo 2^{32} in adder CM_3 with a 32-bit constant C_2 from drive N_5, the result is recorded in N_3. Next The content of N_3 is transferred to N_1, and N_4 to N_2, while data in N_3 and N_4 are saved. The contents of N_1 and N_2 are encrypted in simple mode replacements Final filling N_1 and N_2 later encryption forms the first 64-bit gamma block cipher, which everyday is added modulo 2 in the CM_5 adder with the first 64-bit open block data in this scheme the substitution block K consisting of of 8 static blocks replacements.

In the table 1 are presented results conducted research speed block ciphers DES, AES, GOST-28147, which can to be used as a GPVP.

Table 1

Rating speed famous block ciphers

Block ciphers	DES	AES	GOST 28147-89
Quantity operations processor on the block formed sequence	81/56	40/32	192/64
Length period	2^{56}	2^{128}	2^{256}

Main positive qualities of GPCP built on the basis of block ciphers are:

- resistance to various types of cryptanalysis;
- good statistical properties formable pseudorandom sequence.

To the main disadvantages of block encryption possible to attribute:

- insensitivity crypto schemes to fall out or insert an integer number of blocks;
- existence problems the last block is incomplete length.

To the main the advantages of GOST 28147-89 are possible to attribute:

- the futility of an all-out attack;
- simplicity both with hardware and software implementation and highly effective speed modern encryption computers.

One of the directions in development crypto-resistant generators there is methods based on unilateral functions.

ISSN 2707-1758

The most important one-sided the function used in the construction of the GPCP is factorization whole numbers The widely known GPCP based on this problem, is the *BBS* generator, proposed in 1986 by Lenore Blum, Manuel Blum, and Michael Shub. Calculation of PVP in the *BBS generator* is described expression:

$$x_n = x_{n-1}^2 \, mod \quad N, \tag{2}$$

where $N = pq$ product two big simple $p$and$q$ which can to be both are comparable to 3 modulo 4 (this guarantees that each the quadratic remainder has one square the root which also is quadratic remainder) and the largest general divider $\phi(\phi(p-1), \phi(q-1))$ must to be small.

At every step of the algorithm original data are coming out from taking either the parity bit or one least significant bit. Mainly the advantage of GPSP BBS is that it is available x_n optional calculate everything $n-1$ previous numbers, necessary just know the basics the state of the generator, that is $x_0$and numbers p, q, and any element The sequence of PSP is described expression:

$$x_n = x_0^{2^n \, mod((p-1)(q-1))} \, mod \quad N. \tag{3}$$

Next representatives of GPSP based on use one-sided functions are recognized generators Micali–Schnorr and RSA. Their stability is based on a theoretically complex calculation problem discrete of logarit hms. Everyone element pseudorandom sequence in the Micali–Schnorr generator is described by the expression:

$$x_n = x_{n-1}^e \, mod \quad N. \tag{4}$$

Exit of this GPVP is available r beat pseudorandom sequences, quantity which is calculated by the formula:

$$r = [\lg(pq)] + 1 - \left\lfloor (\lg(pq) + 1)(1 - \frac{2}{e}) \right\rfloor, \tag{5}$$

where $e \in \begin{cases} 1 < e\ (p-1)(q-1) \\ NOD(e,(p-1)(q-1) = 1\ , p, q \text{ – prime numbers.} \\ 80e \le [\lg(pq)] + 1 \end{cases}$

In the RSA GPSP, each element sequence is described expression (5), but unlike the Micali–Schnorr generator on the way out arrives least significant beat Conducted studies showed that main shortcomings of the solution – based GPSP unilateral functions are:

- low speed formations pseudo-random sequences compared to GPSP based on other principles of formation; REF _Ref201077085 \r \h * MERGEFORMAT;
- impossibility to provide formation sequences of the maximum period.

In the table 2 presents correspondence of key lengths to asymmetric and symmetric encryption algorithms.

Table 2

Compliance length keys asymmetric and symmetric encryption algorithms

Length for symmetrical algorithm	Length for asymmetrical algorithm
56 bits	384 bits
80 bits	768 bits
112 bits	1792 bits
128 bits	2304 bits

How follows from given in the table 2 data for formation of the period of PSP 2^{128}battles necessary to produce mathematical operations with dimensional numbers not less than 2304 bits, which in turn leads to significant use computational resources processor.

In the table 3 are presented results conducted research speed formation of one bit of provably stable PSP generators RSA, BBS, Micali–Schnorr for various degrees resistance.

Table 3

Rating speed provable-resistant GPSP

Proveably durable generators	Length period		
	2^{128}	2^{256}	2^{512}
Foundation degrees	2304 bits	14210 bits	81304 bits
RSA	1153656/1	265651872/1	49261255313/1
BBS	57456/1	2180945/1	71038737/1
Micali–Schnorr	561/1	28860/1	1307947/1

Main the advantage of GPSP based on the solution unilateral functions, is available mathematical provability difficulties cryptanalysis. The main ones disadvantages of such generators is computational complexity, and formation of PSP with period significantly less than the maximum.

For construction based on cryptographic schemes registers shift with inverses connections two methods are used generating pseudorandom sequences. The first method – use several in parallel working registers shifting and combining their exit any function complications. Such generators are called combined (Fig. 3).

Another alternative is generation pseudorandom sequence how nonlinear output functions the only one register shift, such a generator is called filter-generator (Fig. 4).

Generators built on this principle have maximum period $2^n - 1$ (where n quantity cells memory register shift). Mainly the disadvantage of such GPSP is complexity finding functions complications $f(x)$.

ISSN 2707-1758

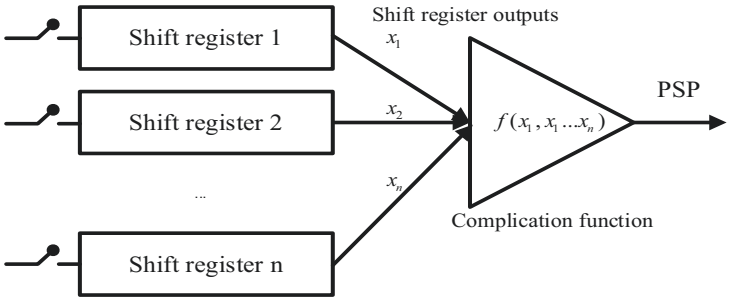


Fig. 3. Combined generator of pseudo-random numbers

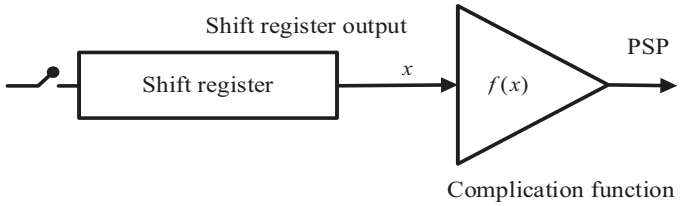


Fig. 4. Filter-generator

Discussion and conclusions

Conducted the study made it possible to comprehensively analyze existing approaches to the construction and application of the HPPSC with consideration their statistical characteristics, cryptographic durability and performance. received the results showed that the choice of a specific type of generator must be made be based on the specifics of informational tasks systems and requirements level protection.

Simple congruent generators and classic LFSR provide high speed formations sequences and ease of implementation, however their low cryptographic endurance does their unsuitable for direct use in protection systems information. They are can to be used as auxiliary tools during construction more difficult crypto-resistant structures.

Generators based on block and stream ciphers, such as AES, GOST 28147-89 and RC4, demonstrated optimal balance between safety and speed, that does their most suitable for a wide range of practical applications cryptographic applications. At the same time necessary to consider features realizations, including key management and reuse prevention key flows, that directly affects reliability systems.

Generators using one-sided functions (RSA, BBS, etc.), provide tall level protection at the expense of mathematically provable durability However, their application is limited scenarios, where priority is maximum security, and performance does not play key role, for example, in state and military information systems, as well as in infrastructures critical significance.

Prospects subsequent research associated with perfection existing methods generation random numbers and development new approaches that will be taken into account modern challenges (development quantum calculated and appearance more difficult methods cryptanalysis). Important direction is creation hybrid generators that will be to unite high cryptographic resistance with high at speed processing data.

Also promising is research algorithms, optimized for work in conditions limited computational resources (for example, in IoT devices), and study opportunities integration generators with hardware sources entropy to increase reliability system as a whole. In the long term perspective special attention must to be given development standards for new- generation cryptographic GPS systems, which will be able to provide protection given in the conditions post-quantum cryptography. This will allow create a reliable basis for building modern protection systems information, capable to resist future cyber threats (Barabash et al., 2023; Jensen, 2006; Gorbenko, & Ganzya, 2014; Starr, 1984; Yang et al., 2017, Berry, 1987).

Authors' contribution: Irada Rahimova – led the overall research design and methodology; conducted theoretical analysis of block cipher–based pseudo-random number generators (e.g., GOST 28147-89); and provided scientific supervision from the Azerbaijani team; Abdul oglu Abbasquliyev – performed experimental evaluations and computational testing of generator performance; collected and processed empirical data (e.g., speed metrics for DES, AES, GOST, BBS); and supported the comparative analysis and tabulation of results; Yelyzaveta Sevriukova – analyzed practical applicability of generators in real-world domains such as finance, government, and critical infrastructure; assessed cost–benefit trade-offs of security versus performance; and contributed to conclusions regarding deployment in strategic sectors; Tetiana Laptieva – conducted in-depth cryptographic analysis of generator security (e.g., LFSR, RC4, RSA, BBS); reviewed vulnerabilities and resistance to cryptanalysis (including cases like Dual_EC_DRBG); and formulated recommendations aligned with international standards (NIST, FIPS) and post-quantum readiness.

Sources of funding. This study did not receive any grant from a funding institution in the public, commercial, or non-commercial sectors.

References

Barabash, O., Sobchuk, V., Musienko, A., Laptiev, O., Bohomia, V., & Kopytko, S. (2023). System Analysis and Method of Ensuring Functional Sustainability of the Information System of a Critical Infrastructure Object. In: System Analysis and Artificial Intelligence. Studies in Computational Intelligence, 1107, 177–192. Springer, Cham. https://doi.org/10.1007/978-3-031-37450-0_11

Berry, J. (1987). Fundamental operations in computer-assisted map analysis. International Journal of Geographical Information Systems, 1, 119–136.

Blum, L. (1986). Simple Unpredictable Pseudo-Random Number Generator. SIAM Journal on Computing, 15(2), 364–386.

ISSN 2707-1758

Blum, M., & Micali, S. (1984). How to generate cryptographically strong sequences of pseudo-random bits. SIAM Journal on Computing, 13(4), 850–864.
Bobok, I. I., Kobozieva, A. A., Laptiev, O. A., Savchenko, V. A., Salii, A. G., & Kurtseitov, T. L. (2025). Method for Estimating the Bandwidth Capacity of a Steganographic Communication Channel. Problems of the Regional Energetics, 2, issue 66, 92–104. http://doi.org/10.52254/1857-0070.2025.2-66.08
Gorbenko, Y., & Ganzya, R. (2014). Analysis of the stability of popular cryptosystems against quantum cryptanalysis based on Grover's algorithm. Information protection, 16(2), 106–112.
Jensen, J. (2006). Remote Sensing and GIS Integration: Theories, Methods, and Applications. Geocarto International, 21(2), 5–16.
Korolev, R. V. (2009). Study of periodic properties of the RC4 stream encryption algorithm. Collection of scientific papers of the Kharkiv Air Force University, 4, 86–89. http://nbuv.gov.ua/UJRN/ZKhUPS_2009_4_22
Kuznetsov, A. (2007). Investigation of the statistical safety of generators of pseudorandom numbers. Systems Processing Information, 3(70), 79–82.
Micali, S., & Sidney, R. (1995). A simple method for generating and sharing pseudorandom functions, with applications to Clipper-like key escrow systems. Advances in Cryptology – CRYPTO'95 (LNCS 963), 185–196.
Milevskyi, S., Korol, O., Hryshchuk, O., Laptieva, T., & Yevseiev, S. (2024). Crypto-code constructions on LDPC codes properties assessment. Ukrainian Scientific Journal of Information Security, 30(2), 313–323. https://doi.org/10.18372/2225-5036.30.19244
Morawiecki, P., & Pieprzyk, J. (2013). Parallel authenticated encryption with the duplex construction. Cryptology ePrint Archive, Report 658.
Prokushev, Y., Ponomarenko, S., & Ponomarenko, S. (2021). Modeling the processes of designing information security systems in state information systems. Computational Nanotechnology, 8(1), 26–37.
Rukhin, A., & Soto, J. (2001). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800–22. https://www.researchgate.net/publication/235090427_A_Statistical_Test_Suite_for_Random_and_Pseudorandom_Number_Generators_for_Cryptographic_Applications
Starr, J. L. (1984). Geographic information systems: a question to ask before it's too late. Machine Processing of Remotely Sensed Data with Special Emphasis on Thematic Mapper Data and Geographic Information Systems, 194–199.
Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and Cloud Computing: Innovation Opportunities and Challenges for GIS. Computers, Environment and Urban Systems, 61, 93–102.

Отримано редакцією журналу / Received: 14.11.25
Прорецензовано / Revised: 17.11.25
Схвалено до друку / Accepted: 22.11.25

Ірада РАГІМОВА[1], канд. техн. наук
ORCID ID: 0009-0006-1969-9976
e-mail: ika1402@icloud.com

Абдул огли Аббасгулієв ЕЮБ[1], асп.
ORCID ID: 0009-0003-7714-5494
e-mail: formemaybe23@yahoo.com

Єлизавета СЄВРЮКОВА[2], канд. екон. наук
ORCID ID: 0000-0002-0757-490X
e-mail: elizavetasevryukova@ukr.net

Тетяна ЛАПТЄВА[2], канд. техн. наук
ORCID ID: 0000-0002-5223-9078
e-mail: tetiana1986@ukr.net

[1]Азербайджанський технічний університет, Баку, Азербайджан
[2]Національний технічний університет "Харківський політехнічний інститут", Харків, Україна

ЕКСПЕРИМЕНТАЛЬНЕ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ КРИПТОГРАФІЧНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Вступ. ***У цифрову епоху забезпечення інформаційної безпеки вимагає надійних криптографічних примітивів. Ключовим компонентом сучасних криптосистем є генератор псевдовипадкових чисел (ГПВЧ), який лежить в основі генерації ключів, цифрових підписів, векторів ініціалізації та інших механізмів безпеки. Стійкість усієї системи часто залежить від непередбачуваності та статистичної якості генерованих послідовностей. Мета цього дослідження – експериментально оцінити ефективність різних криптографічних ГПВЧ за трьома критеріями: статистична випадковість, криптостійкість та обчислювальна продуктивність.***

Методи. ***Проведено порівняльний експериментальний аналіз різних класів криптографічних генераторів псевдовипадкових чисел. Досліджено генератори на основі регістрів зсуву з лінійним зворотним зв'язком (LFSR), конгруентні методи, потокові та блокові шифри (напр., RC4, AES, ГОСТ 28147-89), а також односторонні функції (напр., BBS, RSA, Мікалі–Шнорр). Критерії оцінювання включали статистичні властивості (за допомогою тестів NIST SP 800-22), стійкість до криптоаналізу й обчислювальну ефективність, виміряну кількістю операцій процесора на один вихідний біт.***

Результати. ***Експериментальні результати показали, що генератори на основі блокових і потокових шифрів (напр., AES, ГОСТ 28147-89) забезпечують найкращий баланс між криптостійкістю та продуктивністю. Навпаки, генератори на основі односторонніх функцій (напр., BBS, RSA) мають доведену стійкість, але страждають від низької швидкості та недостатньої довжини періоду. Прості генератори, такі як LFSR і лінійні конгруентні генератори, характеризуються високою швидкістю та гарними статистичними властивостями, проте не мають криптостійкості, що робить їх непридатними для безпосереднього використання в застосунках із високими вимогами до безпеки.***

Висновки. ***Вибір генератора псевдовипадкових чисел має ґрунтуватися на конкретних вимогах цільового застосунку – з урахуванням балансу між безпекою, швидкістю й обмеженнями реалізації. Для загальних криптографічних систем рекомендовано використовувати генератори на основі шифрів. У середовищах із підвищеними вимогами до доведеної стійкості, де продуктивність є вторинною, можуть застосовуватися теоретико-числові генератори. Подальші дослідження слід спрямувати на гібридні архітектури, готовність до постквантової епохи й інтеграцію з апаратними джерелами ентропії для підвищення надійності в умовах обмежених ресурсів та критично важливих інфраструктур.***

Ключові слова: ***генератори псевдовипадкових чисел, криптографічна безпека, статистична випадковість, блокові шифри, потокові шифри, односторонні функції, криптостійкість.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

ISSN 2707-1758