UDC УДК 004.056.55:519.246 **doi:** https://doi.org/10.20998/3083-6298.2026.01.05

Khazail Rzayev[1], Shayasta Hasanova[1], Olha Korol[2], Iryna Aksonova[2], Illia Bukatych[2]

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

STATISTICAL ANALYSIS OF CRYPTOGRAPHIC STRENGTH OF SHA-3 COMPETITION FINALISTS USING NIST SP 800-22 METHODOLOGY

Abstract. Topicality. In today's conditions of rapid development of information technologies and the growth of the number of cyber threats, ensuring the cryptographic stability of hash functions is one of the key tasks of information security. The reliability of hash algorithms directly affects data protection, digital signature, authentication and information integrity. The evaluation of candidates for the competition for the selection of the standard hash algorithm SHA-3, organized by the National Institute of Standards and Technology (NIST), in order to increase the level of cryptographic security after the identification of vulnerabilities in previous algorithms of the SHA family, is of particular relevance. **The subject of the study** is the statistical properties of cryptographic hash algorithms. – finalists of the third round of the SHA-3 competition, as well as other candidates of the final stage. **The purpose of the article** is to conduct a comprehensive statistical assessment of the security of the specified algorithms using the NIST SP 800-22 test package, which is recommended for checking the randomness of bit sequences. **Results obtained.** During the study, samples of the initial bit sequences were generated for each algorithm and tested according to a set of statistical criteria. The results obtained indicate that not all finalists of the third round of the competition demonstrated full compliance with the requirements of statistical randomness. Only the Blake and Grøstl algorithms successfully passed the entire set of NIST SP 800-22 tests without detecting statistically significant deviations. **Conclusion.** Statistical testing is an important tool for the initial assessment of the cryptographic stability of hash functions. The results obtained confirm the high level of statistical reliability of the Blake and Grøstl algorithms and demonstrate the feasibility of using a comprehensive approach to the analysis of the security of candidate cryptographic standards.

Keywords: cryptographic hash function; SHA-3; statistical testing; NIST SP 800-22; cryptographic strength.

Introduction

Problem relevance. One of the key areas of development of modern cryptography is the improvement of methods for ensuring the integrity and authenticity of information in the conditions of increasing data volumes, distributed computing and the constant complication of cyber threats. A special place among such methods is occupied by cryptographic checksums, which allow to detect message modification, data forgery and unauthorized interference in information flows.

Modern mechanisms for forming cryptographic checksums are divided into two main classes:

methods based on symmetric cryptographic transformations – message authentication codes (MACs), which use a shared secret key to verify integrity and authenticity;

methods based on one-way transformations (hash functions) – are used in digital signature schemes, where a fixed-length hash of the message is first calculated, after which it is signed using asymmetric cryptographic algorithms. [1,2]

A hash function maps a message of arbitrary length into a fixed-size bit string, called the hash or message digest. Requirements for cryptographic hash functions include one-way, collision-resistance, spoofing resistance, and statistical indistinguishableness of the original data from a random sequence. [3-5]

From the perspective of the theory of secret systems, a potentially stable cryptographic system is considered to be one in which the statistical characteristics of the output data (cryptograms or hash values) do not depend on the properties of the plaintext. In other words, the results of the transformation should be as close as possible to perfectly random sequences. Any statistical dependence between the input and output data can be used by cryptanalysts to construct attacks.

In this regard, a scientific and practical problem arises: assessing the statistical stability of cryptographic checksums and hash functions using modern randomness testing methods. Even if an algorithm theoretically meets all the mathematical security requirements, in practice its operation may not be completely "perfectly random". In a real practical situation, minor regularities or deviations may appear, which in some cases can create potential weaknesses.

The relevance of studying these issues is due to [3,4]:

the transition to new cryptographic standards (in particular, the SHA-3 family),

the increase in security requirements in cloud, mobile, and IoT environments,

the need to ensure cryptographic stability in the context of the development of post-quantum computing.

Thus, there is a need for a comprehensive statistical analysis of cryptographic transformations using standardized test packages (e.g., NIST SP 800-22), which allow assessing the degree of randomness of the generated bit sequences and their compliance with the theoretical requirements of cryptographic stability.

Therefore, the problem statement consists in studying the statistical properties of modern cryptographic checksums and hash functions and determining the level of their compliance with information security criteria based on experimental testing. [6]

Literature review. The issue of developing a new cryptographic hash function standard became particularly urgent after the practical demonstration of cryptographic matches for SHA-1 and the gradual decline in confidence in its cryptographic strength. Further research showed that the structural similarity between SHA-2 and SHA-1 could potentially create long-term security risks, despite the absence of practical attacks of a similar scale at that time. In this regard, in 2007, the National Institute of Standards and Technology (NIST) announced an open international competition for the development of a new hashing standard - SHA-3. The competition aimed to create algorithms with increased resistance to known attacks and universal application [7].

NIST's main requirements for candidates included:

support for fixed hash lengths (224, 256, 384, and 512 bits) to ensure a high level of cryptographic security and avoid vulnerabilities associated with short output values [7];

a unified internal structure of algorithms for all output sizes, which ensures uniformity of implementation and minimizes the risk of errors in practical application [8-10];

the ability to integrate into HMAC schemes and other cryptographic protocols while maintaining a given level of stability [2,6].

The competition documents also discussed the idea of parameterizing algorithms (e.g., changing the number of rounds to balance security and performance), although the possibility of including such parameterization in the final standard was questioned [7].

The first round of the competition collected 51 candidate hash functions. In subsequent rounds, the selection was based on cryptanalysis and performance evaluation, which is consistent with the review works of contemporary researchers that consider the evolution of cryptographic standards and the principles of their selection [1,8-11].

In modern research, significant attention is paid to statistical testing of cryptographic transformations. Although formal cryptographic robustness is proven within the framework of mathematical models, empirical analysis of randomness allows us to reveal hidden statistical dependencies between input and output data. In particular, studies show that even cryptographically robust designs can exhibit deviations from individual spectral analysis tests or series tests with an insufficient number of rounds or simplified implementations. [6,12].

There is also growing attention to the use of machine learning methods to detect statistical patterns that may be hidden from traditional tests; such approaches offer new ways to analyze cryptographic algorithms in different ranges of parameters [12].

Much attention is paid to the practical implementation of hash functions on modern platforms: in IoT environments, on mobile devices, and in hardware implementations. This is important because hardware optimizations can change the behavior of the statistical properties of algorithms in unpredictable ways that require separate evaluation [3-5].

Thus, the literature review confirms that a comprehensive assessment of cryptographic stability includes not only formal mathematical analysis, but also statistical studies, testing of implementations, performance comparisons, and adaptation to new hardware requirements.

The purpose of this article is to study the statistical evaluation of the security algorithms of the candidates submitted to the competition for the selection of the standard hash algorithm SHA-3 using the NIST SP 800-22 test suite, which is recommended for checking the randomness of bit sequences.

1. Conducting testing and interpreting statistical indicators

Despite the completion of the SHA-3 algorithm standardization process, the issue of comparative analysis of the competition finalists has not lost its relevance. A comprehensive assessment of cryptographic stability today involves not only formal proof of resistance to collisions or attacks on the prototype, but also experimental verification of the statistical characteristics of the output sequences. It is statistical analysis that allows us to identify potential dependencies or deviations from ideal randomness that may not manifest themselves within the framework of classical theoretical models.

Despite the official adoption of SHA-3 as a standard, the study of other finalists in the competition retains scientific significance. Comparison of alternative algorithmic designs allows us to assess their entropy properties, the degree of structural independence of the output data from the input parameters, as well as the level of practical implementation security in different computing environments. This approach contributes to the formation of well-founded conclusions about the feasibility of using certain algorithms in specialized or highly loaded systems.

In view of this, this study provides for a statistical test of the stability of candidate algorithms that participated in the competition for the selection of the SHA-3 standard, using the NIST SP 800-22 test suite recommended by NIST. The use of this set of tests ensures the uniformity of the approach and the possibility of correct comparison of the results obtained with previous studies.

The following testing parameters were selected for experimental analysis:

test sequence length $n = 10^6$ bits;

number of test sequences $m = 100$;

level of significance $\alpha = 0,01$;

amount of test sample 10^8 bits.

The selected parameters meet the recommendations for ensuring sufficient representativeness of the results and allow us to assess not only the passing of individual tests, but also the consistency of indicators at the level of the sample population.

The value of $\alpha = 0,001$, says that out of 1000 random sequences that are tested, failed to test only one. In the P-value $\geq 0,001$ is considered as a random sequence with a level of confidence of 99,9%.

The value of $\alpha = 0,01$, says that of 100 random sequences would not have gone only one test. In the P-

value ≥ 0,01 is considered as a random sequence with a level of confidence of 99%.

The value of α = 0,05, says that of 100 random sequences would not have gone only five tests. In the P-value ≥ 0,05 is considered as a random sequence with 95% confidence level.

This technique allows us to estimate the statistical security, based on 16 tests with 189 known cryptanalytic attacks, with a certain probability. The technique is to examine the algorithm-candidate as a pseudo-random sequence generator and evaluation of statistical dependence between the input (information subject to cryptographic protection during transmission) and output (cryptogram) sequences of data. Cryptanalytic attack is realized (indicates the possibility of finding a statistical relationship between input and output sequences, which allows a cryptanalyst to find the input information), if the probability assessment of its passage by the algorithm-candidate is below 0,96.

In order to obtain the necessary sequence of hash for the package NIST STS a software package, that simulates all the algorithms of applicants passed the second round, has been developed. In writing the program used the materials provided for the contest. We put the test results of hashing algorithms in Table 1.

Table 1 – **Test results for HASH algorithms**

Name of the algorithm	The number of tests in which the testing was 99% of the sequences	The number of tests in which the testing was 96% of the sequences	The number of tests in which the probability value of P ≤ 0,01	The number of tests in which the probability value of P ≤ 0,001	The number of tests in which the probability value of P ≤ 0,05	Permissible value share of the test for a sample of 100 equals binary sequences	Permissible value share of the test for a sample size (n) sequence to test binary Random-Excursion equals
Blake	130	189	2	0	10	0,960150	0,952091 (62)
BMW	144	188	2	0	7		0,952688 (64)
CubeHash	137	189	2	1	9		0,951139 (59)
ECHO	139	189	2	0	13		0,954323 (70)
Fugue	142	188	0	0	4		0,954323 (70)
Grøstl	140	189	4	0	8		0,951781 (61)
Hamsi	134	187	1	0	11		0,953533 (67)
JH	129	187	3	0	14		0,952393 (63)
Keccak	134	187	5	1	10		0,952091 (62)
Luffa	129	189	3	0	10		0,951781 (61)
Shabal	123	188	0	0	9		0,949751 (55)
SHAvite3	135	187	1	0	15		0,950806 (58)
SIMD	131	188	3	0	8		0,950112 (56)
Skein	137	188	1	0	9		0,951464 (60)

The analysis of the results presented in Table 1 allows us to draw a generalized conclusion regarding the level of statistical stability of the SHA-3 candidate algorithms tested according to the NIST SP 800-22 methodology.

Most algorithms demonstrated a high percentage of test passes (96–99% of sequences), which indicates the general compliance of their output bit sequences with the requirements of statistical randomness. The value of the allowable proportion of successful test passes for a sample of 100 sequences is within the recommended threshold values (about 0,95), which confirms the correctness of the applied evaluation methodology.

At the same time, a more detailed analysis of the P-value indicators shows the presence of individual statistically significant deviations. For a number of algorithms, cases were recorded where the value $P \leq 0{,}01$ or even $P \leq 0{,}001$, which indicates potential deviations from the random hypothesis in certain tests. In particular, the BMW, Fugue, Hamsi, JH, Keccak, Shabal, SHAvite3, SIMD and Skein algorithms failed some of the tests (the numbers of which are given in parentheses), which formally means non-compliance with certain criteria for statistical stability.

Of particular note is the fact that even the SHA-3 algorithm (based on Keccak), which was chosen as the winner of the competition, demonstrated the presence of individual tests with marginal P-values. However, the number of such deviations does not exceed the permissible statistical limits, which allows us to consider them random within the accepted level of significance.

The most stable results were demonstrated by the Blake, Fugue and partly Grøstl algorithms, which are characterized by a minimum number of critical deviations and high values of the fraction of successful test passing. This indicates their good entropy properties and proximity to the model of a perfectly random sequence.

Thus, the statistical testing conducted confirms that:

most of the finalists of the SHA-3 competition provide a high level of statistical randomness;

individual algorithms have local deviations that may require additional cryptanalytic analysis;

the test results do not indicate critical vulnerabilities, but demonstrate the feasibility of a comprehensive assessment that combines theoretical cryptanalysis and statistical experimental research.

Thus, statistical analysis according to the NIST SP 800-22 method is an effective tool for initial verification of cryptographic stability and allows for a reasonable comparison of alternative hash function designs.

2. Statistical portrait of the software implementation of the finalist algorithms

NIST has announced the finalists for the SHA-3 hash algorithm: BLAKE (Jean-Philippe Aumasson), Grøstl (Lars Ramkilde Knudsen), JH (Hongjun Wu), Keccak (Joan Demen), and Skein (Bruce Schneier). The jury noted that these five projects implemented some of the new ideas that have emerged in recent years, including the construction of HAIFA (Blake) and the sponge hash (Keccak), which are alternatives to the classic MD construction. [8]

According to the report received after processing, statistical profiles of the software implementations of the finalist algorithms were constructed for testing hash sequences with the NIST STS package. The statistical portrait is a diagram of the probability of passing statistical tests. In Fig. 1-5 shows a statistical portrait of the software implementation of the finalist algorithms for selecting the standard SHA-3 hash algorithm.

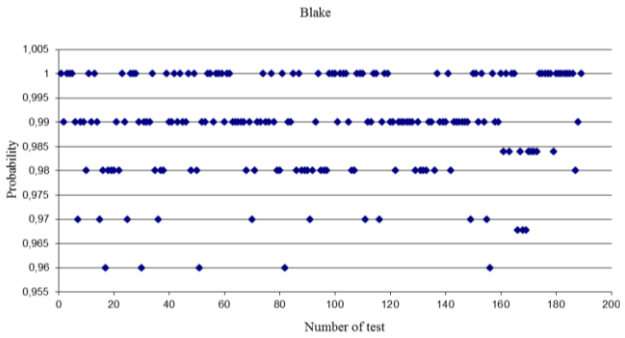
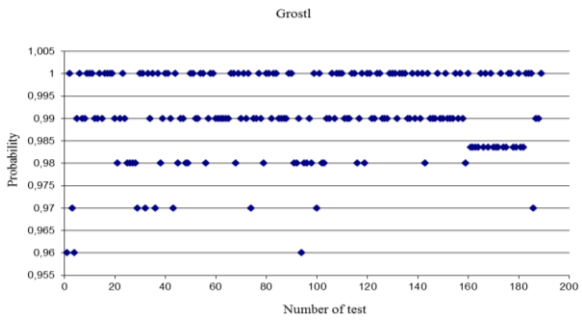


Fig. 1. Statistical portrait of the software implementation of the algorithm candidate Blake



The constructed statistical portraits of the software implementations of the SHA-3 competition finalist algorithms reflect the distribution of probabilities of passing the NIST SP 800-22 (NIST STS) tests and allow us to visually assess the level of their statistical stability.

Analysis of Fig. 1-5 shows that the Blake and Grøstl algorithms demonstrate the most uniform distribution of P-values in the permissible intervals, without pronounced failures in individual tests. Their statistical profiles are characterized by a high proportion of successful test passes and the absence of systematic deviations, which indicates good entropy properties and the absence of noticeable structural dependencies in the generated bit sequences.

The statistical portrait of the JH algorithm demonstrates minor fluctuations in indicators within

Fig. 2. Statistical portrait of the software implementation of the algorithm candidate Grøstl

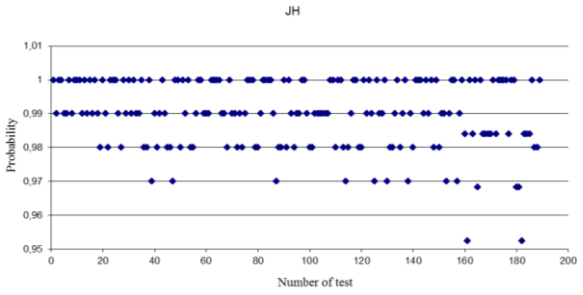


Fig. 3. Statistical portrait of the software implementation of the algorithm candidate JH

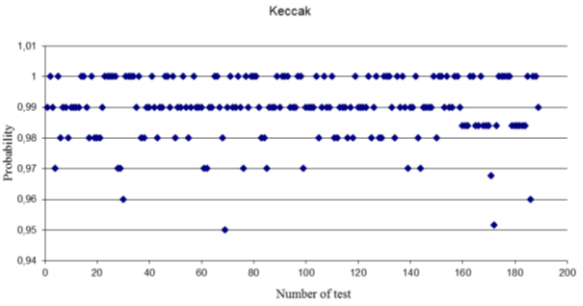


Fig. 4. Statistical portrait of the software implementation of the algorithm candidate Keccak

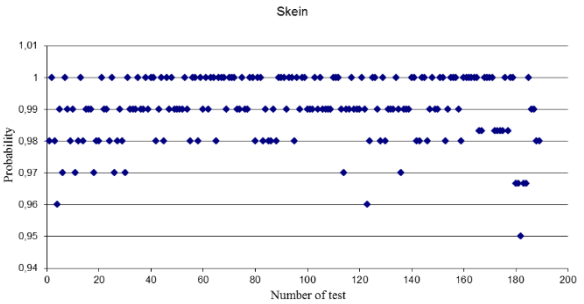


Fig. 5. Statistical portrait of the software implementation of the algorithm candidate Skein

individual tests, which is consistent with the results of the table analysis. Although the overall level of compliance with the randomness requirements remains high, the presence of individual P-value decreases may indicate local features of the internal structure of transformations.

For the Keccak algorithm (standardized as SHA-3), the statistical portrait also demonstrates stable results with minor deviations in individual tests. The distribution of probability values is quite uniform, which confirms the compliance of the algorithm with the criteria of statistical randomness within the accepted level of significance. The identified individual deviations are not systemic in nature and do not exceed the permissible statistical limits.

Skein algorithm is characterized by more noticeable fluctuations in the diagram, which is consistent with the results of testing, where individual tests were not performed. Although the overall structure of the profile

does not indicate critical instability, there is a greater variability of the indicators compared to Blake and Grøstl.

Summarizing the results of the analysis of statistical portraits, the following conclusions can be drawn:

all the studied algorithms generally demonstrate a high level of compliance with the requirements of statistical randomness;

the most stable profiles are those of Blake and Grøstl, which confirms their high entropy and the absence of systematic statistical anomalies;

Keccak demonstrates balanced characteristics, which is consistent with its further standardization;

JH and Skein have individual deviations that may require additional cryptanalytic or implementation analysis.

Thus, visual analysis of statistical portraits confirms the results of tabular evaluation and indicates the feasibility of using graphical representation as an additional tool for comprehensive assessment of cryptographic stability of hash algorithms.

Discussion of results

The results of statistical testing of the SHA-3 competition finalists using the NIST SP 800-22 methodology allowed for an in-depth analysis of their cryptographic properties from the standpoint of empirical assessment of randomness. It is worth emphasizing that statistical tests are not direct evidence of cryptographic robustness in the classical sense (resistance to collisions, attacks on the prototype, etc.), but they play an important role as an indicator of the presence of hidden structural dependencies in the output bit sequences.

The results of the study showed that most of the finalist algorithms demonstrated general compliance with the randomness requirements at a significance level of $\alpha = 0{,}01$. This indicates a sufficiently high level of entropy and effective mixing of input data in the transformation process. At the same time, for some algorithms, individual statistically significant deviations were recorded within certain tests, which may indicate local features of their internal structure or the specifics of the software implementation.

Of particular note is the fact that only the Blake and Grøstl algorithms demonstrated full compliance with all tests without exceeding the threshold values. This may indicate a more balanced architecture of their round transformations, the absence of noticeable correlations between the bits of the original sequence, and high quality of diffusion. This result is consistent with their reputation as cryptographically strong designs among the finalists of the competition.

For other candidates, including the algorithm standardized as SHA-3, the recorded single deviations are not systematic and remain within the limits of statistically acceptable fluctuations. Given the large number of tests performed, the appearance of individual P-values below the threshold level may be due to random factors. However, such results emphasize the need for a comprehensive approach to evaluation, i.e. a combination of mathematical cryptanalysis, statistical testing, and analysis of practical implementations.

When discussing the obtained data, one should also take into account the influence of the sample size (10^8 bits) and the number of test sequences ($m = 100$). The selected parameters ensure the representativeness of the results, however, when changing the length of the sequences or the implementation conditions (hardware/software optimization), the statistical indicators may vary. This opens up prospects for further research aimed at analyzing the scalability of statistical properties and their sensitivity to algorithm parameters.

Thus, the results confirm that statistical analysis is a necessary component of a comprehensive assessment of cryptographic stability. It allows not only to compare alternative algorithmic designs with each other, but also to identify potential directions for optimization and in-depth cryptanalytic research.

Conclusions

Thus, the study of the statistical properties of the SHA-3 competition finalists using the NIST SP 800-22 methodology allowed for a comprehensive empirical assessment of the level of their cryptographic stability from the perspective of the randomness of the initial bit sequences.

The results obtained confirmed that the Blake and Grøstl algorithms demonstrate a high level of statistical reliability and do not reveal significant deviations from the randomness hypothesis at a given significance level. This is consistent with their resistance to known cryptanalytic attacks and indicates a high-quality implementation of the diffusion and nonlinear data mixing mechanisms in the internal structure of the algorithms.

However, for the finalist algorithms JH, Keccak, and Skein, some statistically significant deviations were recorded within some tests. Although these deviations do not directly indicate the presence of practical vulnerabilities, they may indicate potential structural features that require additional cryptanalytic analysis. The presence of such deviations could theoretically reduce the margin of cryptographic strength of the algorithm under specialized or adaptive attacks.

Thus, the results of the work confirm the feasibility of using statistical testing as a tool for the initial and comparative evaluation of hash functions. Statistical analysis does not replace a rigorous mathematical proof of stability, but allows us to identify hidden patterns and assess the quality of algorithm implementation in practical conditions.

A promising direction for further research is:

analysis of the collision stability of the finalists of the SHA-3 competition using both theoretical models and experimental methods;

research of stability to attacks on the first and second prototype;

evaluation of the behavior of algorithms when changing parameters (number of rounds, implementation options);

expansion of statistical analysis using additional test packages and increased data samples;

analysis of the impact of hardware optimization and implementation features on statistical characteristics.

The study confirmed the high level of statistical stability of the Blake and Grøstl algorithms, and also demonstrated the need for further comprehensive analysis of other finalists of the SHA-3 competition in order to better understand their cryptographic potential and safety margin.

This work was supported by the Azerbaijan Science Foundation- Grant № AEF-MGC-2025-1(54)-20/04/1-M-04.

References

1. Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T. et al. (2022), "NIST IR 8413 Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process", *National Institute of Standards and Technology,* https://doi.org/10.6028/NIST.IR.8413
2. Turan, M. S., Barker, E., Kelsey, J., McKay, K. A., Baish, M. L. and Boyle, M. (2018), "NIST Special Publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation", *National Institute of Standards and Technology,* https://doi.org/10.6028/NIST.SP.800-90B
3. Khan, M., Kozyri, E., Johansen, D., and Dagenborg, H. (2025), "Survey of Lightweight Hardware-Based Hash Functions for Security in Constrained IoT Devices", *IEEE Access*, Vol. 13, DOI: 10.1109/ACCESS.2025.3611280
4. Kuznetsov, O., Peliukh, O., Poluyanenko, N., Bohucharskyi, S., and Kolovanova, I. (2023), "Comparative Analysis of Cryptographic Hash Functions in Blockchain Systems", *CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems. CEUR Workshop Proceedings,* https://ceur-ws.org/Vol-3550/paper7.pdf
5. Sharma, S. (2024), "A Comprehensive Study of Cryptographic Hash Functions", *Defence Materials & Stores Research & Development Establishment (DRDO),* https://www.researchgate.net/publication/381639930_A_Comprehensive_Study_of_Cryptographic_Hash_Functions
6. Paul, R., Dey, H., Ghosh, R. and Chakrabarti, A. (2016), "NIST Statistical Test Suite", *arXiv:1609.01389v1 [stat.AP],* https://www.academia.edu/81793392/NIST_Statistical_Test_Suite
7. FIPS 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. (2015), *National Institute of Standards and Technology. Gaithersburg, MD, USA,* http://dx.doi.org/10.6028/NIST.FIPS.202
8. Alshaikhli, I. F., Alahmad, M. A. and Munthir, K. (2012), "Comparison and Analysis Study of SHA-3 Finalists", *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT),* DOI: 10.1109/ACSAT.2012.64
9. Regenscheid, A., Perlner, R., Chang, S., Kelsey, J., Nandi, M. and Paul, S. (2009), "Status Report on the First Round of the SHA-3 Cryptographic Hash Algorithm Competition", *National Institute of Standards and Technology,* https://nvlpubs.nist.gov/nistpubs/legacy/ir/nistir7620.pdf
10. Gaffud San Jose, C. C. (2019), "Comparative and Security Performance Analysis of SHA-3", Journal of Advanced Research in Dynamical and Control Systems, Vol. 11, DOI:10.5373/JARDCS/V11SP11/20193121
11. Yesina, M., Ostrianska, Y. and Gorbenko, I. (2022), "Status report on the third round of the NIST post-quantum cryptography standardization process", *Radiotekhnika*, Vol. *3*(210), pp. 75–86, https://doi.org/10.30837/rt.2022.3.210.05
12. Foreman, C., Yeung, R. and Curchod, F. J. (2024), "Statistical testing of random number generators and their improvement using randomness extraction", *arXiv:2403.18716v1 [cs.CR]*, https://arxiv.org/html/2403.18716v1

Received (Надійшла) 24.02.2026
Accepted for publication (Прийнята до друку) 20.03.2026

Відомості про авторів/ About the Authors

Рзаєв Хазаїл Нураддін огли – доктор технічних наук, професор, кафедра комп'ютерних технологій, Азербайджанський технічний університет, Баку, Азербайджанська Республіка;
Khazail Rzayev - Doctor of technical sciences, Professor, Department of Computer Technology, Azerbaijan Technical University, Baku, Azerbaijan;
e-mail: xezail.rzayev@aztu.edu.az; ORCID Author ID: https://orcid.org/0000-0001-9272-4302;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57204042636.

Гасанова Шаяста Фархад кизи – старший викладач, кафедра комп'ютерних технологій, Азербайджанський технічний університет, Баку, Азербайджанська Республіка;
Shayasta Hasanova - Head teacher at the Department of "Computer Technologies", Azerbaijan Technical University, Baku, Azerbaijan;
e-mail: xezail.rzayev@aztu.edu.az; ORCID Author ID: https://orcid.org/0009-0003-4801-2270.

Король Ольга Григорівна – кандидат технічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Olha Korol – Candidate of Technical Sciences, Associate Professor, Associate Professor of Cyber Security Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: Olha.Korol@khpi.edu.ua; ORCID Author ID: https://orcid.org/0000-0002-8733-9984;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57190437459.

Аксьонова Ірина Вікторівна – кандидат економічних наук, доцент, старший дослідник, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;

Iryna Aksonova – Candidate of Economic Science, Associate Professor, Senior researcher, Associate Professor of Cyber Security Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: ivaksyonova@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-2605-0455;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57206727489.

Букатич Ілля Вадимович – аспірант кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Illia Bukatych – PhD student of Cyber Security Department, National Technical University "Kharkiv polytechnic institute", Kharkiv, Ukraine;
e-mail: illia.bukatych@gmail.com; ORCID Author ID: https://orcid.org/0009-0007-4695-073X;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=59490108100.

СТАТИСТИЧНИЙ АНАЛІЗ КРИПТОГРАФІЧНОЇ СТІЙКОСТІ ФІНАЛІСТІВ КОНКУРСУ SHA-3 ЗА МЕТОДОЛОГІЄЮ NIST SP 800-22

Х. Н. Рзаєв, Ш. Ф. Гасанова, О. Г. Король, І. В. Аксьонова, І. В. Букатич

Анотація. Актуальність. У сучасних умовах швидкого розвитку інформаційних технологій та зростання кількості кіберзагроз забезпечення криптографічної стійкості хеш-функцій є одним із ключових завдань інформаційної безпеки. Надійність хеш-алгоритмів безпосередньо впливає на захист даних, цифровий підпис, автентифікацію та цілісність інформації. Особливу актуальність має оцінювання кандидатів на конкурс з вибору стандартного хеш-алгоритму SHA-3, організований Національним інститутом стандартів і технологій (NIST) з метою підвищення рівня криптографічної безпеки після виявлення вразливостей у попередніх алгоритмах сімейства SHA. **Предметом дослідження** є статистичні властивості криптографічних хеш-алгоритмів – фіналістів третього раунду конкурсу SHA-3, а також інших кандидатів фінального етапу. **Метою статті** є проведення комплексної статистичної оцінки безпеки зазначених алгоритмів за допомогою тестового пакета NIST SP 800-22, який рекомендований для перевірки випадковості бітових послідовностей. **Отримані результати.** Під час дослідження для кожного алгоритму були згенеровані вибірки початкових бітових послідовностей та протестовані за набором статистичних критеріїв. Отримані результати свідчать про те, що не всі фіналісти третього туру конкурсу продемонстрували повну відповідність вимогам статистичної випадковості. Лише алгоритми Blake та Grøstl успішно пройшли весь набір тестів NIST SP 800-22 без виявлення статистично значущих відхилень. **Висновок.** Статистичне тестування є важливим інструментом для початкової оцінки криптографічної стійкості хеш-функцій. Отримані результати підтверджують високий рівень статистичної надійності алгоритмів Blake та Grøstl й демонструють доцільність використання комплексного підходу до аналізу безпеки кандидатів на криптографічні стандарти.

Ключові слова: криптографічна хеш-функція; SHA-3; статистичне тестування; NIST SP 800-22; криптографічна стійкість.