ISSN 2411-3816 (Print)
СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА
MODERN SPECIAL TECHNICS
DOI (Issue): https: //doi.org/10.36486/mst2411–3816.2020.1(60)
Issue 1(60) 2020

УДК 004.421.5

Максимович Володимир Миколайович,
доктор технічних наук, професор,
НУ "Львівська політехніка", м. Львів, Україна,
ORCID ID 0000-0001-8435-4129
Шабатура Марія Миколаївна,
кандидат технічних наук, доцент,
НУ "Львівська політехніка", м. Львів, Україна,
ORCID ID 0000-0003-0814-1855
Малогловець Андрій Сергійович,
аспірант,
НУ "Львівська політехніка", м. Львів, Україна,
ORCID ID 0000-0002-0490-7174

ДОСЛІДЖЕННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК МОДИФІКОВАНОГО АЛГОРИТМУ BBS

Генератор Блюм-Блюм-Шуба, BBS, належить до надійних генераторів, криптостійкість якого ґрунтується на складності вирішення задачі факторизації – розкладення числа на прості множники.

У роботі досліджено характеристики запропонованого авторами модифікованого алгоритму BBS, зокрема, період повторення та статистичні характеристик вихідної послідовності залежно від параметрів генератора. Дослідження проводилися з використанням тестів NIST і порівнянj із класичним алгоритмом BBS.

Для класичного та модифікованого алгоритмів BBS за допомогою тестів NIST були побудовані статистичні портрети для згенерованих послідовностей, які свідчать про покращання статистичних характеристик модифікованого алгоритму BBS.

Ключові слова: *псевдовипадкова послідовність; генератори псевдовипадкових послідовностей; одностороння функція; генератор Блюма-Блюма-Шуба.*

Генератор Блюм-Блюм-Шуба, BBS, относится к надежным генераторам, криптостойкость которого основывается на сложности решения задачи факторизации – разложения числа на простые множители.

В работе исследованы характеристики предложенного авторами модифицированного алгоритма BBS, в частности, период повторения и статистические характеристики выходной последовательности в зависимости от параметров генератора. Исследования проводились с использованием тестов NIST и в сравнении с классическим алгоритмом BBS.

Для классического и модифицированного алгоритмов BBS, с помощью тестов NIST, были построены статистические портреты для сгенерированных последо-

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2020.1(60).3

вательностей, которые свидетельствуют об улучшении статистических характеристик модифицированного алгоритма BBS.

Ключевые слова: *псевдослучайная последовательность; генераторы псевдослучайных последовательностей; односторонняя функция; генератор Блюма-Блюма-Шуба.*

Генератор BBS (Blum, Blum, Shub), названий на честь своїх авторів Леонора Блюма, Мануела Блюма і Майкла Шуба. Він належить до класу надійних генераторів, криптостійкість якого ґрунтується на складності вирішення задачі факторизації – розкладу числа на прості множники [1–4]. Класичний алгоритм BBS генератора дає змогу формувати на його основі різні модифікації з метою покращання його характеристик [5–7]. Аналіз наявних робіт [8–11], спрямованих на такі модифікації, свідчить про недостатність уваги можливості врахування в алгоритмі не лише поточних значень згенерованих чисел, але й їх попередніх значень.

Метою роботи є дослідження модифікованого алгоритму BBS генератора, зокрема, дослідження періодів повторення його вихідної послідовності чисел і дослідження статистичних характеристик з використанням тестів NIST.

Класичний алгоритм BBS

Модель класичного алгоритму BBS базується на формулі [1]

$$x_{n+1} = x_n^{\,2} \bmod M, \tag{1}$$

де x_n і x_{n+1} – поточне і наступне значення чисел, M – ключ, який є результатом добутку двох чисел Блюма, p і q:

$$M = p \cdot q\ . \tag{2}$$

Числа Блюма – це непарні прості числа, для яких виконуються умови [2]:

$$p \equiv 3(mod4),\ \ q \equiv 3(mod4). \tag{3}$$

Період повторення послідовності збільшується при зменшенні результату виконання операції пошуку найбільшого спільного дільника (НСД) для функцій Ейлера від p та q [2, 6]:

$$НСД(\varphi(p-1),\varphi(q-1))\,. \tag{4}$$

На кожному кроці алгоритму вихідні дані (вихідна бітова послідовність) отримуються з чисел x_n шляхом взяття або біта парності, або одного чи кількох найменш значущих біт.

Оскільки у формулі (1) використовується операція знаходження остачі від цілочисельного ділення, то на кожному кроці вхідний параметр і результат ітерації лежать у діапазонах:

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2020.1(60).3

$$x_n \in [0, M), \quad (5)$$

$$x_{n+1} \in [0, M). \quad (6)$$

Оскільки значення ключа M не змінюється при ітераціях, формулу (1) можна представити у вигляді:

$$x_{n+1} = f(x_n). \quad (7)$$

Значення періоду повторення вихідної послідовності класичного алгоритму лежать в діапазоні:

$$P \in [1, M - 1). \quad (8)$$

Модифікований алгоритм BBS

Для покращання характеристик класичного алгоритму BBS було запропоновано узагальнену модель модифікації, яка базується на формулі (7) із додаванням параметрів a і b:

$$x_{n+1} = f(x_n, a, b). \quad (9)$$

Параметр a умовно названий мажорним, оскільки він за конкретизованих модифікацій має більший вплив на результат ітерацій, ніж параметр b.

Одним із можливих варіантів реалізації узагальненої моделі (9) є модифікований алгоритм:

$$x_{n+1} = (x_n^{\,2} + a + b) \bmod M. \quad (10)$$

У цій роботі розглядається варіант алгоритму (10) за умови:

$$a_2 = x_{n-1} \text{ і } b = 0, \quad (11)$$

де x_{n-1} – попереднє значення ітераційного циклу.

Отже, у цьому разі модифікований алгоритм BBS описується рівнянням [12]:

$$x_{n+1} = (x_n^{\,2} + x_{n-1}) \bmod M. \quad (12)$$

Дослідження і порівняльний аналіз періодів повторення класичного і модифікованого алгоритмів BBS генераторів

Для дослідження періодів повторення були вибрані шість ключів (значень M) із найменшим значенням НСД, відповідно до формули (4), довжиною від 5 до 10 бітів, які задовольняють умови (3), та які подані у таблиці 1.

Таблиця 1

Ключі *M* для генератора BBS

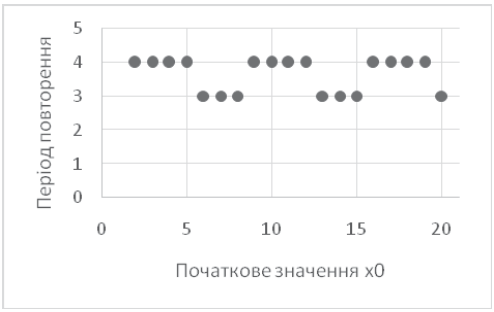
№	Число Блюма		Довжина ключа *M*, біт	Значення ключа *M*	Значення НСД ключа *M*
	p	*q*			
1	3	7	5	21	1
2	3	11	6	33	1
3	3	23	7	69	1
4	3	43	8	129	1
5	3	103	9	309	1
6	3	179	10	537	1

При визначенні періоду здійснювався перебір усіх можливих початкових значень $x_i - x_0$ із діапазону

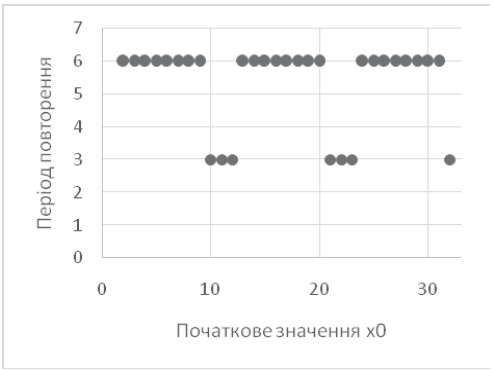
$$x_0 \in [2, M-1]. \tag{13}$$

При визначенні періоду повторення модифікованого алгоритму BBS (12) бралися до уваги як поточні, так і попередні значення згенерованої послідовності.

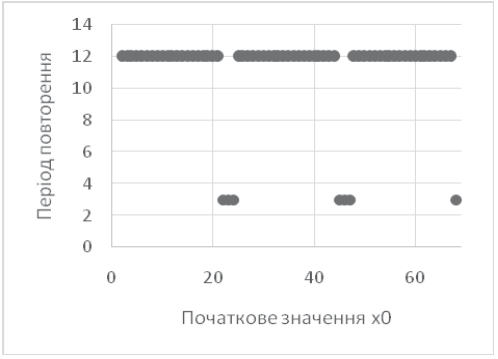
Залежності періоду повторення від початкових значень для класичного алгоритму BBS наведено на рис. 1, а для модифікованого – на рис. 2.



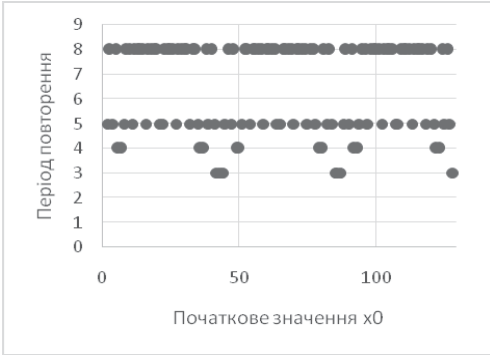
M = 21



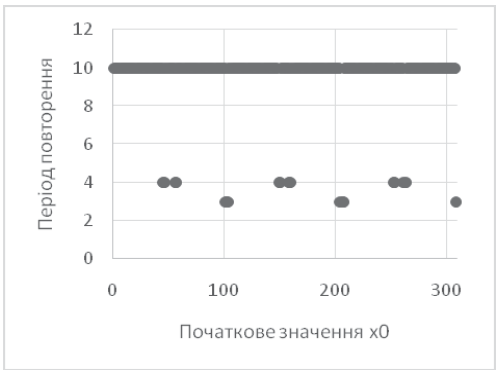
M = 33

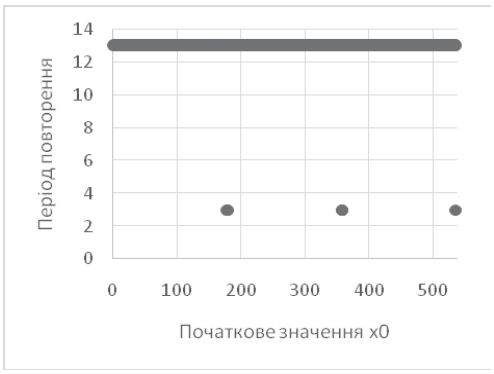


M = 69



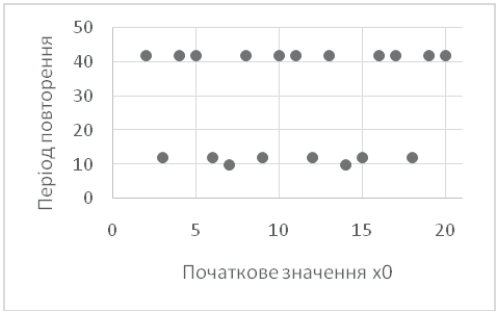
M = 129

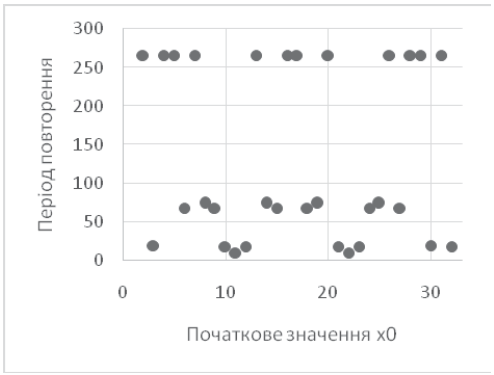




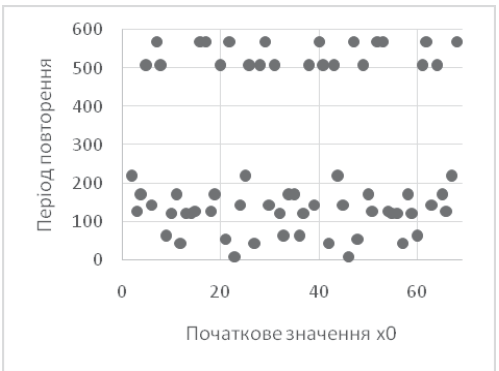
$M = 309$ $M = 537$

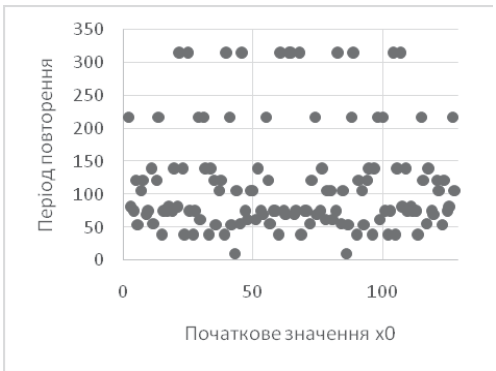
Рис. 1. Значення періоду повторення від початкових значень для класичного алгоритму BBS



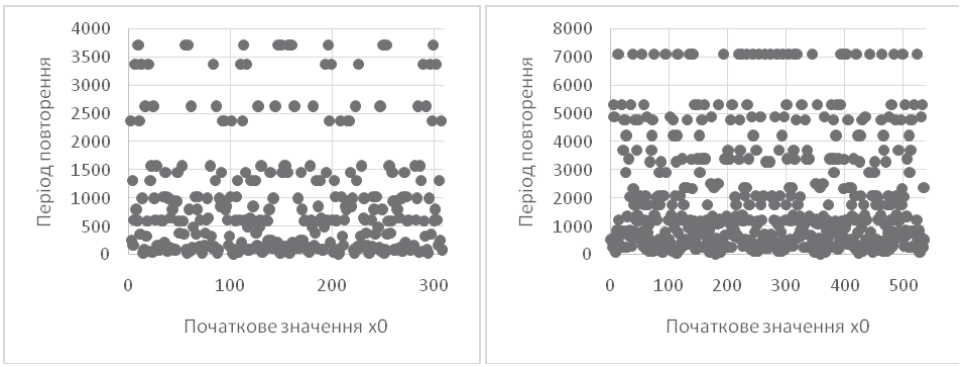


$M = 21$ $M = 33$





$M = 69$ $M = 129$



M = 309 M = 537

Рис. 2. Значення періоду повторення від початкових значень для модифікованого алгоритму BBS

Результати, представлені на рис. 1 і 2, ілюструють той факт, що період повторення вихідної послідовності чисел модифікованого алгоритму BBS значно збільшився порівняно із класичним алгоритмом BBS.

Через неможливість перебору всіх початкових значень x_0 для великих значень ключа M наступні дослідження проводилися для окремих обраних значень M, наведених в табл. 2, і фіксованих значеннях x_0, наведених в табл. 3.

Таблиця 2

Ключі *M* для генератора BBS

№	Число Блюма		Довжина ключа *M*, біт	Значення ключа *M*	Значення НСД
	p	*q*			
1	3	5471	15	16413	1
2	3	10939	16	32817	1
3	3	21851	17	65553	1
4	3	43691	18	131073	1
5	3	87383	19	262149	1

Таблиця 3

Ключі *M* і початкові значення для генератора BBS

№	Значення ключа *M*	Значення періоду повторення для відповідного початкового значення x_0							
		Класичний BBS				Модифікований BBS			
		2	$\sqrt{M}/2$	$\sqrt{M}$	$M/2$	2	$\sqrt{M}/2$	$\sqrt{M}$	$M/2$
1	16413	548	548	548	548	93210	30314	16330	19018
2	32817	913	1824	913	913	5354	137786	71738	12834
3	65553	222	222	222	222	284122	67594	27522	563946
4	131073	10	18	18	10	909546	239946	160834	128586
5	262149	36	36	36	36	193786	2115898	1745322	415194

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2020.1(60).3
Issue 1(60) 2020 http://suchasnaspetstehnika.com/

З таблиці 3 видно, що тенденція до збільшення періоду повторення для модифікованого генератора BBS зберігається для ключів більшої довжини.

Дослідження та порівняльний аналіз статистичних характеристик класичного і модифікованого алгоритмів BBS генераторів

Для аналізу статистичних характеристик класичного алгоритму BBS та його модифікацій були використані статистичні тести NIST 2.1.2 – пакет із 15 статистичних тестів розроблений Лабораторією інформаційних технологій, що є головною дослідницькою організацією Національного інституту стандартів і технологій (NIST) [13]. Їх метою є визначення міри випадковості двійкових послідовностей, сформованих генераторами псевдовипадкових чисел. Ці тести засновані на різних статистичних властивостях, притаманних лише випадковим послідовностям.

Для дослідження статистичних характеристик були вибрані ключі з найменшим значенням НСД, відповідно до виразу (4), довжиною від 26 до 34 бітів, які задовольняють умови (3) та які подані у таблиці 4. Початкове значення для кожного ключа розраховувалося за формулою:

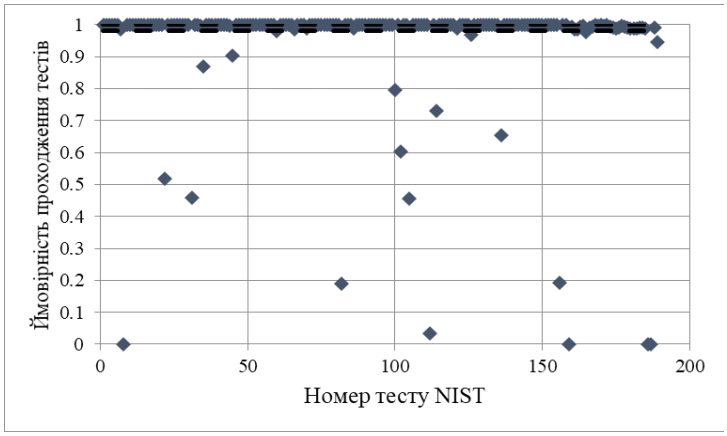
$$x_0 = \sqrt{M}/2. \qquad (14)$$

Таблиця 4

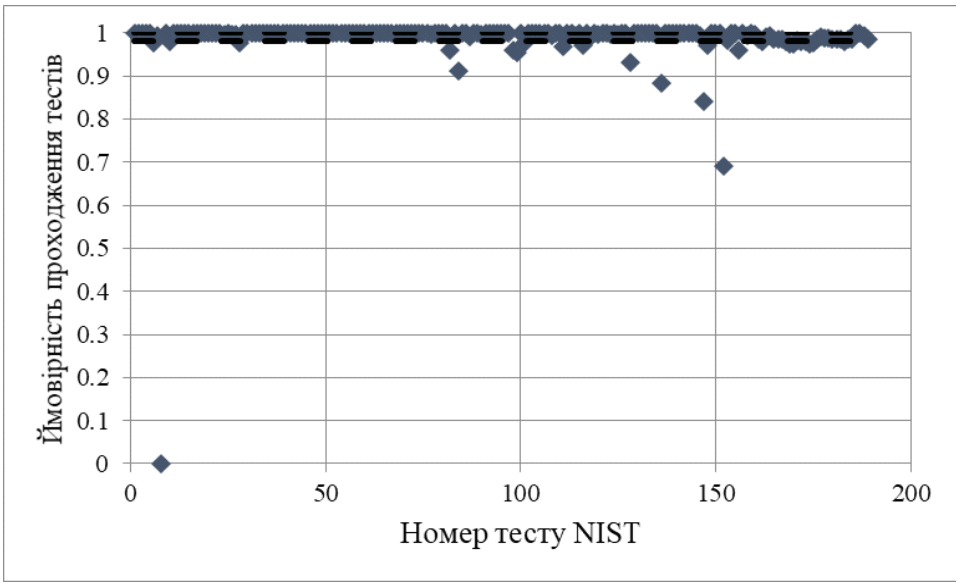
Ключі *M* для генератора BBS

№	Число Блюма		Довжина ключа *M*, біт	Значення ключа *M*	Значення НСД
	p	*q*			
1	5011	6719	26	33668909	2
2	21419	24407	30	595994533	2
3	45707	188159	34	8600183413	2

Результати аналізу статистичних характеристик подано у вигляді статистичних портретів на рис. 3–5 (варіанти № 1–3 відповідно), де на рис. *а* наведено портрети класичних генераторів BBS, а модифіковані версії цих генераторів – на рис. *б*.



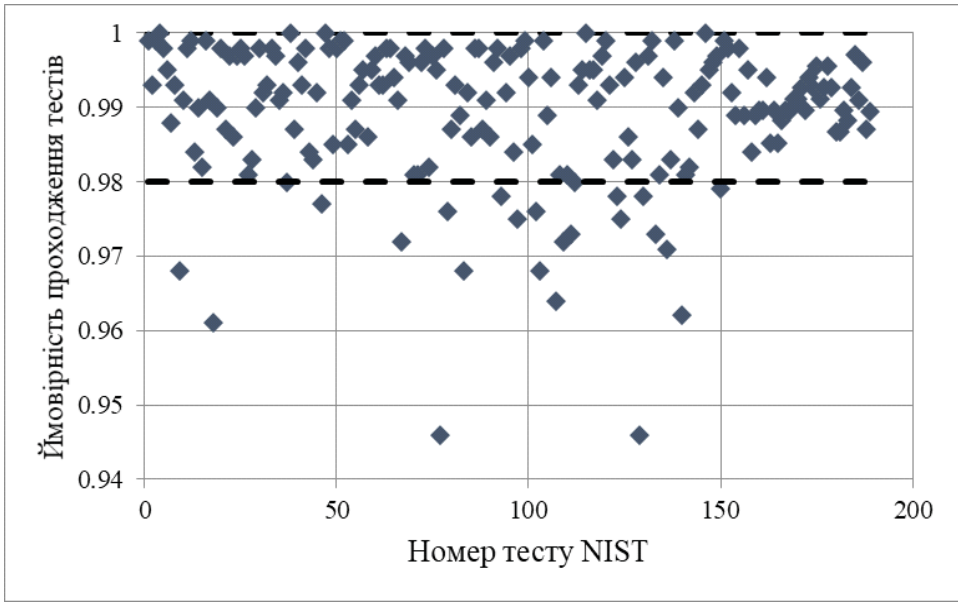
а



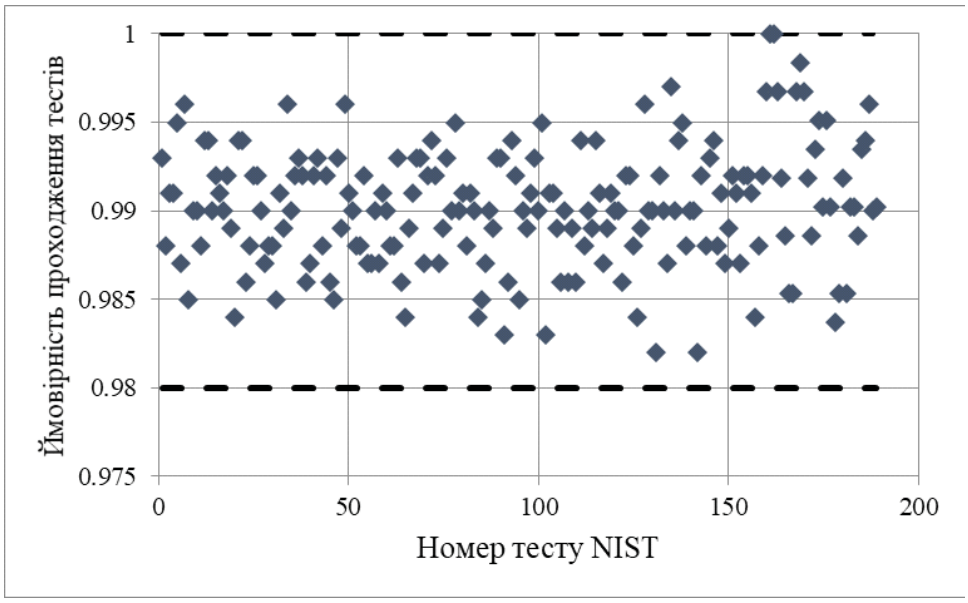
б

Рис. 3. Статистичні портрети генераторів – варіант № 1

Як видно з рис. 3, генератори не відповідають вимогам випадковості, оскільки значення проходження тестів знаходяться поза межами довірчого інтервалу. Проте модифікація генератора призводить до покращання статистичних характеристик.



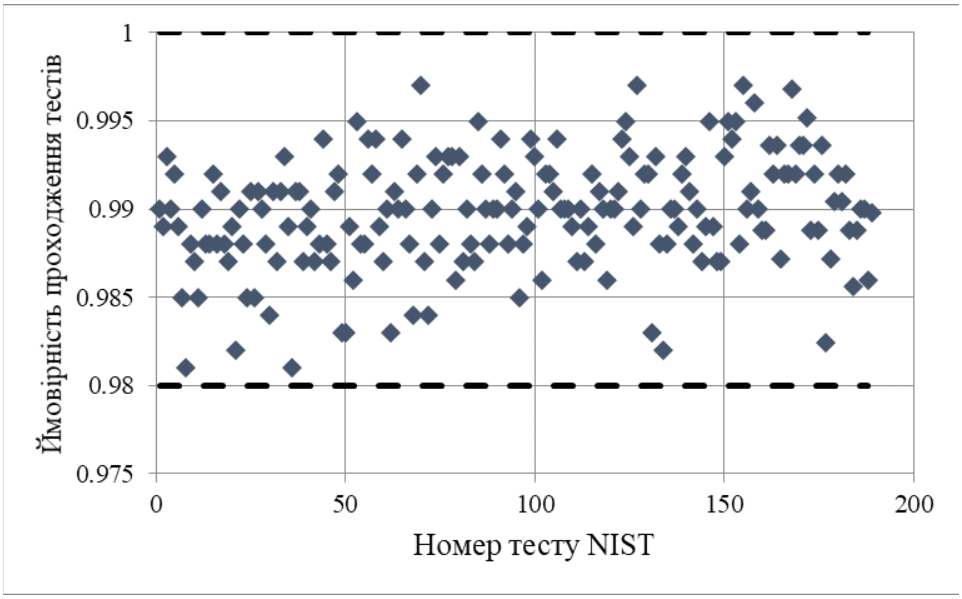
а



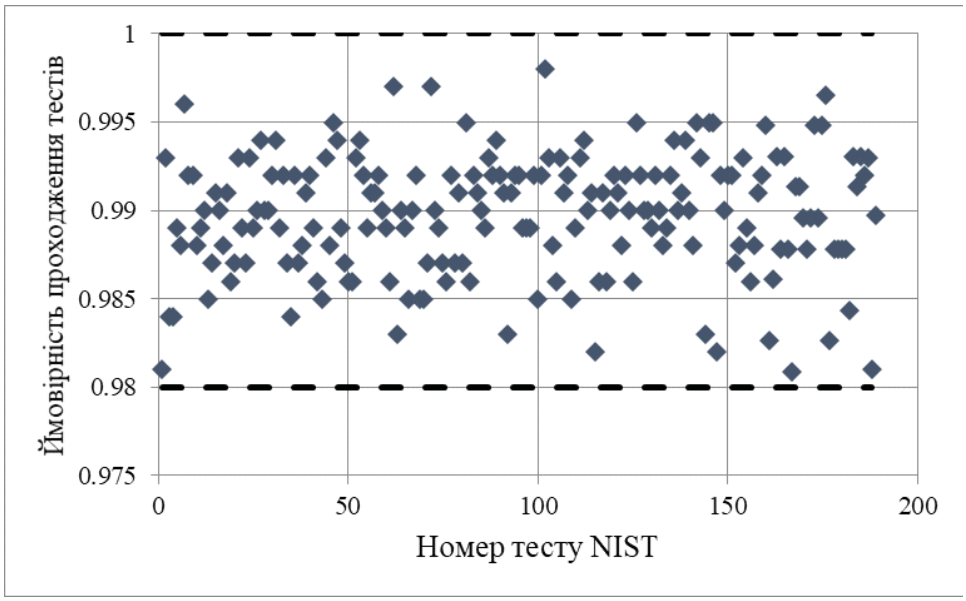
б

Рис. 4. Статистичні портрети генераторів – варіант № 2

Із статистичного портрета рис. 4 *б* видно, що модифікований генератор (варіант № 2) пройшов усі тести NIST, що свідчить про його статистичну безпеку, на відміну від класичного варіанту побудови генератора.



а



б

Рис. 5. Статистичні портрети генераторів – варіант № 3

Аналіз статистичних портретів, наведених на рис. 3, 4 та 5, свідчить по істотне покращання статистичних характеристик модифікованого BBS генератора у порівнянні із класичним його варіантом.

Класичний алгоритм BBS має прийнятний статистичний портрет, починаючи з ключа довжиною 34 біт (рис. 5 а). Модифікований алгоритм BBS має прийнятний статистичний портрет, починаючи з ключа довжиною 30 біт (рис. 4 б). Модифікований алгоритм BBS дозволяє отримати прийнятні статистичні портрети з меншим розміром ключового значення та зменшує необхідні системні ресурси для генерації псевдовипадкової послідовності. При цьому складність обчислень модифікації значно нижча, ніж складність обчислень одного кроку у класичних алгоритмах BBS.

Аналіз періодів повторення і статистичних характеристик модифікованого BBS генератора доводить його перевагу за цими параметрами над класичним BBS генератором.

Подальші дослідження за цим напрямом можуть бути спрямовані на:

– визначення множини значень ключів M і множини початкових значень x_0, для модифікованого алгоритму BBS, при яких статистичні характеристики генератора є гарантовано задовільними;

– пошук інших ефективних модифікацій алгоритму BBS на основі узагальненої моделі $x_{n+1} = \left(x_n^{\,2} + a + b\right) mod\, M.$

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2020.1(60).3
Issue 1(60) 2020 http://suchasnaspetstehnika.com/

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *L. Blum, M. Blum, and M. Shub,* "Comparison of two pseudo-random number generators," in R.L. Rivest, A. Sherman, and D. Chaum, editors, Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques CRYPTO'82, New York, Plenum Press, 1983, pp. 61–78.

2. *P. Junod,* "Cryptographic secure pseudo-random bits generation: the Blum-Blum-Shub generator," August 1999 Applications URL: http://crypto.junod.info/bbs.pdf (дата звернення: 05.11.2019).

3. *Divyanjali, V. Pareek,* "An overview of cryptographically secure pseudorandom number generators and BBS" IJCA Proceedings of the International Conference on Advances in Computer Engineering and Applications ICACEA, vol. 2, issue 3, pp. 19–28, March 2014.

4. *A. Sidorenko and B. Schoenmakers,* "Concrete security of the Blum-Blum-Shub pseudorandom generator," Cryptography and Coding, Lecture Notes on Computer Science, Springer, vol. 3796, pp. 355–375, Nov. 2005.

5. *K. Gawande, M. Mundle,* "Various implementations of Blum Blum Shub pseudo-random sequence generator," 1999 Applications. URL: https://pdfs.semanticscholar.org/5ddc/47b658a204ae76d00aec929b1a5b7fbbfaa6.pdf (дата звернення: 05.11.2019).

6. *L. Blum, M. Blum and M. Shub,* "A simple unpredictable pseudorandom number generator", SIAM Journal on Computing, vol. 15, issue 2, pp. 364–383, 1986.

7. *S. Gurpreet, G. Gurjot,* "DNA and Blum Blum Shub Random Number Generator Based Security Key Generation Algorithm", International Journal of Security and its Applications, vol. 11, pp. 1–10, April 2017.

8. *B. Shrestha,* Multiprime Blum-Blum-Shub Pseudorandom Number Generator, PhD thesis, September 2016 Applications. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/1030047.pdf (дата звернення: 05.11.2019).

9. *V. Kapur, S. Teja,* "Two level image encryption using pseudo random number generators" International Journal of Computer Applications, vol. 115, issue 12, pp. 1–4, 2015.

10. *B. Anssa, M. Khaled, G. Lakhdar,* "Implementation of Blum Blum Shub generator for message encryption", Proceedings of the International Conference on Control, Engineering and Information Technology (CEIT'14), Tunisia, vol. 6, pp. 118–123, 2014.

11. *P.P. Lopez, E.S. Millan,* "Cryptographically secure pseudorandom bit generator for RFID tags", Proceedings of the International Conference for Internet Technology and Secured Trans., London, 8–11, Nov 2010, pp. 1–6.

12. *Малогловець А.С., Максимович В.М.* Методи покращення статистичних характеристик криптостійких генераторів BBS псевдовипадкових чисел і бітових послідовностей. Матеріали VI Міжнародної конференції "Захист інформації і безпека інформаційних систем", Львів, 1 червня 2017 р. С. 73–74.

13. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications URL: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf (дата звернення: 05.11.2019).

REFERENCES

1. *L. Blum, M. Blum, and M. Shub* (1983) "Comparison of Two Pseudo-Random Number Generators," in R.L. Rivest, A. Sherman, and D. Chaum, editors, Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques CRYPTO'82, New York, Plenum Press, pp. 61–78 [in English].

2. *P. Junod* (1999) "Cryptographic secure pseudo-random bits generation: the Blum-Blum-Shub generator", August 1999 Applications. URL : http://crypto.junod.info/bbs.pdf (Date of Application: 05.11.2019) [in English].

3. *Divyanjali, V. Pareek* (2014) "An overview of cryptographically secure pseudorandom number generators and BBS", IJCA Proceedings of the International Conference on Advances in Computer Engineering and Applications ICACEA, vol. 2, issue 3, pp. 19–28, March 2014 [in English].

4. *A. Sidorenko and B. Schoenmakers,* "Concrete security of the Blum-Blum-Shub pseudorandom generator," Cryptography and Coding, Lecture Notes on Computer Science, Springer, vol. 3796, pp. 355–375, Nov. 2005 [in English].

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2020.1(60).3

5. *K. Gawande, M. Mundle,* "Various implementations of Blum Blum Shub pseudo-random sequence generator", 1999 Applications. URL: https://pdfs.semanticscholar.org/5ddc/47b658a204ae76d00aec929b1a5b7fbbfaa6.pdf (Date of Application: 05.11.2019) [in English].

6. *L. Blum, M. Blum and M. Shub,* "A simple unpredictable pseudorandom number generator", SIAM Journal on Computing, vol. 15, issue 2, pp. 364–383, 1986 [in English].

7. *Gurpreet, S., Gurjot, G.* "DNA and Blum Blum Shub Random Number Generator Based Security Key Generation Algorithm", International Journal of Security and its Applications, vol. 11, pp. 1–10, April 2017 [in English].

8. *Shrestha, B.* Multiprime Blum-Blum-Shub Pseudorandom Number Generator, PhD thesis, September 2016 Applications. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/1030047.pdf (Date of Application: 05.11.2019) [in English].

9. *Kapur, V., Teja, S.* (2015) "Two level image encryption using pseudo random number generators," International Journal of Computer Applications, vol. 115, issue 12, pp. 1–4 [in English].

10. *Anssa, B., Khaled, M., Lakhdar, G.* (2014) "Implementation of Blum Blum Shub generator for message encryption," Proceedings of the International Conference on Control, Engineering and Information Technology (CEIT'14), Tunisia, vol. 6, pp. 118–123 [in English].

11. *Lopez, P.P., Millan, E.S.* (2010) "Cryptographically secure pseudorandom bit generator for RFID tags," Proceedings of the International Conference for Internet Technology and Secured Trans, London, 8–11 Nov., pp. 1–6 [in English].

12. *Malohlovets, A.S., Maksymovych, V.M.* (2017) Metody pokrashchennya statystychnykh kharakterystyk kryptostiykykh heneratoriv BBS psevdovypadkovykh chysel i bitovykh poslidovnostey. "Methods for the Improvement of the Statistical Characteristics of Crypto-Stable BBS Pseudorandom Numbers and Bit Sequences": Proceedings of the VI International Conference "Information Protection and Security of Information Systems", Lviv, June 1, 73–74 [in Ukrainian].

13. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. URL: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf. (Date of Application: 05.11.2019) [in English].

UDC 004.421.5

Maksymovych Volodymyr, Doct. Sci. (Engineering), Prof., LPNU, Lviv, Ukraine,
ORCID ID 0000-0001-8435-4129
Shabatura Mariia,
Cand. Sci. (Engineering), Assoc. Prof.,
LPNU, Lviv, Ukraine,
ORCID ID 0000-0003-0814-1855
Malohlovets Andrii,
Postgraduate Student,
LPNU, Lviv, Ukraine,
ORCID ID 0000-0002-0490-7174

STUDY OF STATISTICAL CHARACTERISTICS OF THE MODIFIED BBS ALGORITHM

Blum-Blum-Shub generator, BBS, which is cryptographically secure pseudorandom number generator, refers to reliable generators whose crypto-stability is based on the complexity of solving the problem of factorization – decomposition of numbers into simple multiples.

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2020.1(60).3
Issue 1(60) 2020 http://suchasnaspetstehnika.com/

The paper investigates the characteristics of the modified BBS algorithm proposed by the authors, in particular, the repetition period and the statistical characteristics of the output sequence, depending on the parameters of the generator. The studies were performed using NIST tests and compared to the classical BBS algorithm.

It was established that the repetition period of the classical BBS algorithm is quite small in comparison to the size of a key, for very small keys it may be up to 20 %, but with key size increasing it significantly decreases, and maximum value of the repetition period is 6 % from key value. The values of the repetition period for classical BBS algorithm may vary only in several values. The modified BBS algorithm, which is based on a unified modification model, showed a significant increase of the repetition period in comparison to the classical BBS algorithm, the values of the repetition period may be up to 13 times higher that key value, along with a variation of its values. This behavior persists with the size of the key.

For the classic and modified BBS algorithms, statistical portraits were constructed for generated pseudorandom bit sequences, which testify to the improved statistical characteristics of the modified BBS algorithm. Classical BBS algorithm has acceptable statistical portrait starting from 34 bits key and the key has the lowest result for greatest common divisor between previous values for two prime numbers, on which the key was created. In compare to previous statement, modified BBS algorithm has acceptable statistical portrait starting from 30 bits key. Modified BBS algorithm allows to get acceptable statistical portraits with lower size of key value and decreases required system resources for generating pseudorandom sequence, also computation complexity of modification significantly lower than computation complexity of single step in classic BBS algorithms.

Keywords: pseudorandom sequence; pseudorandom sequence generators; one-way functions; Blum-Blum-Shub generators.

Отримано 26.11.2019
Рецензент д.т.н., проф. Рибальський О.В.