КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1020
УДК 004.056.2:004.421.5

Кіх Михайло Васильович
аспірант кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0009-0007-1847-1862
mykhailo.v.kikh@lpnu.ua

Нємкова Олена Анатоліївна
д.т.н., професор,
професор кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0000-0003-0690-2657
olena.a.niemkova@lpnu.ua

КОМПЛЕКСНЕ КРИПТОГРАФІЧНЕ ОЦІНЮВАННЯ ГІБРИДНОГО ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ АУДІОЕНТРОПІЇ ТА НЕЛІНІЙНИХ БУЛЕВИХ ФУНКЦІЙ

Анотація. У статті представлено результати комплексного криптографічного оцінювання гібридного генератора псевдовипадкових послідовностей (ГПВП), що поєднує аудіоентропію як джерело початкової випадковості, множинні генератори Джиффі та динамічно обрані нелінійні булеві функції в алгебраїчній нормальній формі (АНФ). Ключовою особливістю архітектури є використання стохастично синтезованих АНФ-функцій з гарантованою нелінійністю, що забезпечує унікальність комбінуючої функції при кожному запуску системи. Проведено багаторівневе статистичне тестування згенерованих послідовностей із використанням трьох незалежних тестових пакетів: NIST SP 800-22, Diehard та TestU01 SmallCrush. Досліджено сім конфігурацій генератора (від 6 до 9 базових генераторів) з різними рівнями нелінійності АНФ-функцій (24-224). Результати NIST тестування показали успішне проходження всіх 15 базових тестів для кожної конфігурації зі середнім $\rho -$ value у діапазоні 0.341-0.531. Diehard тести підтвердили відмінну якість всіх 22 статистичних перевірок без критичних відхилень. TestU01 SmallCrush засвідчив проходження всіх 15 тестів із мінімальними $\rho -$ значеннями не нижче 0.0056. Криптографічний аналіз послідовностей виявив оптимальні показники: лінійна складність $LC/n \approx 0.50$, ентропія Шеннона > 0.9999, автокореляція < 0.03, відсутність періодичності. Аналіз АНФ-функцій методом диференційних таблиць розподілу (DDT) показав максимальну диференційну ймовірність у діапазоні 0.59-0.66, що є типовим для пошукових функцій. Встановлено, що всі досліджені конфігурації відповідають вимогам до криптографічно стійких генераторів і можуть застосовуватися у системах інформаційної безпеки. Оптимальною визнано конфігурацію з 7 генераторами та нелінійністю АНФ ≥ 24, яка забезпечує найкращий баланс між швидкодією (0.01 с) та криптографічною стійкістю. Отримані результати підтверджують, що запропонований гібридний підхід є ефективним і придатним для практичного використання в широкому спектрі криптографічних застосувань у системах кібербезпеки.

Ключові слова: генератор псевдовипадкових послідовностей; булеві функції; нелінійність; криптографічний аналіз; криптографічна стійкість; NIST тестування; Diehard; TestU01; аудіоентропія; генератор Джиффі; кібербезпека.

ВСТУП

Постановка проблеми. Генератори псевдовипадкових послідовностей (ГПВП) є фундаментальними компонентами сучасних криптографічних систем, визначаючи

надійність шифрування, автентифікації та інших механізмів забезпечення інформаційної безпеки [1]. Традиційні детерміністичні підходи до генерації псевдовипадкових послідовностей характеризуються суттєвими обмеженнями: передбачуваністю при розкритті внутрішнього стану, обмеженою початковою ентропією, вразливістю до статистичних атак та відсутністю справжньої випадковості [2, 3].

Особливо гостро ці проблеми проявляються у системах із обмеженими ресурсами – від вбудованих платформ до пристроїв Інтернету речей (IoT), – де нестача ентропії, обмеження пам'яті й обчислювальної потужності та вимоги до енергоефективності ускладнюють використання традиційних криптографічних механізмів [4, 5, 6].

За таких умов зростає потреба в генераторах випадкових послідовностей, здатних забезпечувати формування ключів, nonce-значень та ініціалізаційних векторів, працювати на мінімальних апаратних ресурсах, не покладатися на спеціалізовані TRNG і використовувати доступні джерела ентропії [3, 6, 7].

Це робить проблему створення надійних і ресурсно-ефективних генераторів актуальною не лише для IoT, але й для широкого спектра сучасних криптографічних та моделювальних застосувань.

Перспективним напрямом є розробка гібридних архітектур, що поєднують фізичні джерела ентропії з ефективними алгоритмами псевдовипадкової генерації [8, 9]. Зокрема, використання нелінійних булевих функцій в алгебраїчній нормальній формі (АНФ) як комбінуючих функцій дозволяє підвищити криптографічну стійкість генераторів при прийнятних обчислювальних витратах [10].

Аналіз останніх досліджень і публікацій. Сучасні дослідження у сфері генераторів псевдовипадкових послідовностей демонструють перехід від класичних лінійних підходів до складних композитних архітектур.

Систематичний аналіз криптографічно стійких ГПВП із використанням пакета тестів NIST [11] підкреслює необхідність багаторівневої верифікації, а TPRF-орієнтовані моделі пропонують нові можливості підвищення безпеки [9].

Значна увага приділяється булевим функціям: останні роботи представляють конструкції збалансованих функцій із максимальними Walsh-носіями [10], окреслюють ключові критерії їх проєктування – нелінійність, збалансованість і алгебраїчний ступінь [5], а також демонструють потенціал еволюційних методів у синтезі функцій із контрольованими характеристиками [6].

Перспективними напрямами залишаються підходи на основі клітинних автоматів [12] та нейромережевих моделей [4]; у цьому контексті активно розробляються генератори, побудовані на багатовимірній оптимізації [13] та граматичній еволюції [7].

З огляду на це, верифікація якості ГПВП розглядається як критично важливий етап, що потребує застосування кількох незалежних пакетів тестів – NIST SP 800-22, Diehard, TestU01 – для об'єктивної оцінки статистичних властивостей послідовностей [14].

Попри значний прогрес, відкритими залишаються завдання інтеграції природних джерел ентропії з детерміністичними алгоритмами в реальному часі, розроблення динамічних АНФ-функцій, здатних змінюватися під час роботи системи, а також побудови практичних композитних архітектур для сучасних систем кібербезпеки [8, 15, 16].

Мета статті. Метою дослідження є комплексне криптографічне оцінювання гібридного генератора псевдовипадкових послідовностей, що базується на аудіоентропії та динамічних АНФ-функціях, шляхом багаторівневого статистичного тестування та криптоаналізу згенерованих послідовностей і булевих функцій.

Для досягнення мети поставлено наступні завдання:

1. Проведення статистичного тестування послідовностей з використанням трьох незалежних пакетів тестів (NIST, Diehard, TestU01).
2. Криптографічний аналіз послідовностей за показниками лінійної складності, ентропії, кореляції та періодичності.
3. Оцінювання криптографічних властивостей АНФ-функцій методом диференційних таблиць розподілу.
4. Порівняльний аналіз різних конфігурацій генератора.
5. Визначення оптимальної конфігурації за критерієм баланс/стійкість.

МЕТОДИКА ДОСЛІДЖЕННЯ

Архітектура досліджуваного генератора. Досліджуваний гібридний генератор складається з трьох основних компонентів [8]: модуль екстракції ентропії з аудіосигналу, множинні модифіковані генератори Джиффі з незалежними початковими станами і динамічна нелінійна комбінуюча АНФ-функція.

Аудіоентропія використовується для генерації 159-бітних сідів для кожного генератора Джиффі шляхом XOR молодших бітів трьох сусідніх семплів [8].

Генератори Джиффі базуються на трьох регістрах зсуву довжиною 59, 53 та 47 біт з налаштовуваними tap-позиціями та нелінійною вихідною функцією $f(x, y, z) = z_{47} \oplus (x_{59} \cdot y_{53})$ [8].

АНФ-функція синтезується стохастично під час ініціалізації системи з гарантованою нелінійністю та використовується для комбінування вихідних послідовностей генераторів: $output[i] = f(gen_1[i], gen_2[i], \ldots, gen_n[i])$ [8].

Конфігурації для тестування. Досліджено сім конфігурацій генератора [8]:

1. 6_24: 6 генераторів, вимоги до нелінійності АНФ ≥ 24, нелінійність – 24.
2. 7_24: 7 генераторів, вимоги до нелінійності АНФ ≥ 24, нелінійність – 48.
3. 8_24: 8 генераторів, вимоги до нелінійності АНФ ≥ 24, нелінійність – 106.
4. 9_24: 9 генераторів, вимоги до нелінійності АНФ ≥ 24, нелінійність – 212.
5. 9_48: 9 генераторів, вимоги до нелінійності АНФ ≥ 48, нелінійність – 218.
6. 9_90: 9 генераторів, вимоги до нелінійності АНФ ≥ 90, нелінійність – 220.
7. 9_120: 9 генераторів, вимоги до нелінійності АНФ ≥ 120, нелінійність – 224.

Методи тестування. Статистичне тестування проведено з використанням трьох пакетів [14]:

1. NIST SP 800-22: 15 тестів (188 підтестів) на 100 послідовностей по 1 Мбіт.
2. Diehard: 22 тести на послідовності 352 Мбіт.
3. TestU01 SmallCrush: 15 тестів швидкого скринінгу на послідовності 3200 Мбіт.

Для кожної конфігурації згенеровано послідовність довжиною 100 000 біт для криптографічного аналізу. Криптографічний аналіз послідовностей включав:

1. Лінійну складність (алгоритм Берлекампа-Месі).
2. Ентропію Шеннона та мінімальну ентропію.
3. Автокореляційний аналіз (lag 1, 2, 5, 10, 20, 50).
4. Runs-тест з Z-оцінкою.
5. Пошук періодичності.

Криптографічний аналіз АНФ-функцій виконано методом побудови диференційних таблиць розподілу (DDT) з оцінкою максимальної диференційної ймовірності, нелінійності, алгебраїчного ступеня та збалансованості.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Статистичне тестування

Результати NIST SP 800-22 тестування. Всі сім конфігурацій успішно пройшли повний набір NIST тестів (Таблиця 1) [8, 14]. Ключові показники:

Таблиця 1

Узагальнені результати NIST тестування

Конфігурація	Середнє ρ – value	Мін. ρ – value	Пропорція 100/100	Пропорція ≥ 99/100	Оцінка
6_24	0.464	0.033 (Runs)	3/16	11/16	Добре
7_24	0.435	0.027 (FFT)	3/16	12/16	Відмінно
8_24	0.531	0.067 (Universal)	4/16	11/16	Відмінно
9_24	0.412	0.012 (RandomExcurs.)	6/16	12/16	Відмінно
9_48	0.341	0.001 (LongestRun)	4/16	11/16	Добре
9_90	0.495	0.002 (RandomExcurs.Var)	4/16	12/16	Відмінно
9_120	0.420	0.012 (LongestRun)	5/16	12/16	Відмінно

Жодна конфігурація не показала систематичних відхилень. Мінімальні $\rho -$ значення залишалися вище критичного порогу 0.001, що підтверджує відсутність статистичних закономірностей у послідовностях. Найкращі результати показали конфігурації 8_24 та 9_90 з найвищим середнім $\rho -$ value.

Результати Diehard тестування. Diehard тести, відомі своєю суворістю, підтвердили високу якість всіх конфігурацій [14] (Таблиця 2):

Таблиця 2

Узагальнені результати Diehard тестування

Конфігурація	Пройдено тестів	Критичні ρ – value	Мін. ρ – value	Середнє ρ – value	Оцінка
6_24	22/22	0	0.0155 (OPSO)	0.5074	Відмінно
7_24	22/22	0	0.0086 (OQSO)	0.5026	Відмінно
8_24	22/22	0	0.0206 (OPSO)	0.5063	Відмінно
9_24	22/22	0	0.0305 (DNA)	0.515	Відмінно
9_48	22/22	0	0.0070 (DNA)	0.5024	Відмінно
9_90	22/22	0	0.0043 (Squeeze)	0.4947	Добре
9_120	22/22	0	0.0275 (DNA)	0.5136	Відмінно

Особливу увагу привертають результати складних тестів OPSO, OQSO та DNA, які оцінюють перекриваючі послідовності та специфічні патерни. Всі конфігурації показали $\rho -$ значення у безпечному діапазоні $[0.001, 0.999]$, що свідчить про відсутність систематичних відхилень від випадковості.

Результати TestU01 SmallCrush тестування. TestU01 SmallCrush, призначений для швидкого скринінгу [14], підтвердив якість генератора (Таблиця 3):

Таблиця 3

Узагальнені результати TestU01 SmallCrush тестування

Конфігурація	Пройдено тестів	$\rho -$ значень < 0.001	Мін. $\rho -$ value	Середнє $\rho -$ value	Оцінка
6_24	15/15	0	0.0066 (Coupon)	0.481	Добре
7_24	15/15	0	0.05 (Collision)	0.471	Добре
8_24	15/15	0	0.01 (Coupon, Walk J)	0.456	Добре
9_24	15/15	0	0.0056 (Coupon)	0.475	Добре
9_48	15/15	0	0.12 (Walk R)	0.503	Відмінно
9_90	15/15	0	0.10 (Coupon)	0.514	Відмінно
9_120	15/15	0	0.05 (Collision)	0.549	Добре

Найнижчі $\rho -$ значення спостерігалися у тестах Coupon Collector та Collision, що є типовим для багатьох ГПВП. Конфігурації 9_48 та 9_90 показали найкращі результати з середніми $\rho -$ значеннями > 0.50.

Криптографічний аналіз послідовностей

Лінійна складність. Аналіз лінійної складності методом Берлекампа-Месі показав оптимальні результати для всіх конфігурацій (Таблиця 4):

Таблиця 4

Результати оцінювання лінійної складності

Конфігурація	Аналізовано біт	LC	Очікувана LC	LC/n	Статус
6_24	10000	5000	5000.00	0.5000	Відмінно
7_24	10000	5000	5000.00	0.5000	Відмінно
8_24	10000	4998	5000.00	0.4998	Відмінно
9_24	10000	5001	5000.00	0.5001	Відмінно
9_48	10000	4998	5000.00	0.4998	Відмінно
9_90	10000	5000	5000.00	0.5000	Відмінно
9_120	10000	4999	5000.00	0.4999	Відмінно

Відношення LC/n для всіх конфігурацій знаходиться в оптимальному діапазоні $[0.45, 0.55]$, що свідчить про високу складність послідовностей і стійкість до атак на основі лінійного криптоаналізу.

Ентропія Шеннона. Всі конфігурації показали ентропію Шеннона, наближену до теоретичного максимуму (Таблиця 5):

Таблиця 5

Результати оцінювання ентропії

Конфігурація	Ентропія Shannon	Мінімальна ентропія	Якість	Статус
6_24	0.999989	0.994298	100.00%	Відмінно
7_24	0.999953	0.988447	100.00%	Відмінно
8_24	0.999999	0.998385	100.00%	Відмінно
9_24	0.999999	0.998010	100.00%	Відмінно
9_48	0.999999	0.998039	100.00%	Відмінно
9_90	0.999980	0.992431	100.00%	Відмінно
9_120	1.000000	0.999798	100.00%	Відмінно

Конфігурація 9_120 досягла ідеальної ентропії Шеннона $H = 1.0$, що є виняткових результатом. Мінімальна ентропія для всіх конфігурацій перевищує 0.98, що підтверджує рівномірний розподіл бітів.

Автокореляція. Автокореляційний аналіз не виявив значущих кореляцій між бітами (Таблиця 6):

Таблиця 6

Результати автокореляційного аналізу

Конфігурація	lag_1	lag_2	lag_5	lag_10	lag_20	lag_50	Макс |corr|
6_24	-0.0175	+0.0094	-0.0009	-0.0044	+0.0018	+0.0034	0.0175
7_24	-0.0057	+0.0060	+0.0155	-0.0036	-0.0122	+0.0092	0.0155
8_24	-0.0163	-0.0064	+0.0039	+0.0112	+0.0152	-0.0024	0.0163
9_24	-0.0067	-0.0262	+0.0021	+0.0002	+0.0142	-0.0034	0.0262
9_48	+0.0095	-0.0056	+0.0061	+0.0052	-0.0010	-0.0100	0.0100
9_90	-0.0043	+0.0130	-0.0201	-0.0204	+0.0006	-0.0123	0.0204
9_120	-0.0013	+0.0038	+0.0037	+0.0018	-0.0054	+0.0022	0.0054

Максимальні значення автокореляції не перевищують 0.03, що значно нижче критичного порогу 0.05. Найкращий результат показала конфігурація 9_120 з максимальною кореляцією лише 0.0054.

Runs-тест та періодичність. Runs-тест підтвердив рівномірний розподіл серій (Таблиця 7):

Таблиця 7

Результати runs-тесту та перевірки періодичності

Конфігурація	Кількість runs	Очікувана кількість	Z-оцінка	Період	Статус
6_24	49,943	50,000.22	-0.3619	Не виявлено	Відмінно
7_24	49,801	49,997.77	-1.2446	Не виявлено	Відмінно
8_24	49,922	50,000.94	-0.4992	Не виявлено	Відмінно
9_24	49,884	50,000.90	-0.7394	Не виявлено	Відмінно
9_48	50,081	50,000.91	+0.5066	Не виявлено	Відмінно
9_90	50,143	49,999.62	+0.9069	Не виявлено	Відмінно
9_120	49,779	50,001.00	-1.4041	Не виявлено	Відмінно

Усі конфігурації демонструють Z-оцінки в межах допустимого діапазону $|Z| < 1.96$ (95% рівень довіри), що підтверджує рівномірний розподіл серій однакових бітів. Періодичність не виявлена в жодній з досліджуваних послідовностей, що свідчить про відсутність явних циклічних закономірностей.

Криптографічний аналіз АНФ-функцій. Аналіз АНФ-функцій методом диференційних таблиць розподілу (DDT) виявив їх відповідність критеріям для пошукових функцій (Таблиця 8):

Таблиця 8

Криптографічні характеристики АНФ-функцій

Конфігурація	NL	Цільове NL	Ступінь	Мін. ступінь	Балансованість	Max DDT prob	Клас
6_24	24	24±2	5	3	Так	0.6250	A (Відмінно)
7_24	50	48±8	6	4	Так	0.6562	B (Добре)
8_24	106	100±12	7	5	Так	0.6250	B (Добре)
9_24	216	216±16	8	6	Так	0.6016	B (Добре)
9_48	218	216±16	8	6	Так	0.5938	B (Добре)
9_90	220	216±16	8	6	Так	0.5938	B (Добре)
9_120	226	216±16	8	6	Так	0.6016	B (Добре)

Ключові спостереження:

1. Всі АНФ-функції демонструють нелінійність у типовому діапазоні для пошукових функцій. Конфігурація 6_24 точно досягає цільового значення 24, що є оптимальним для 6 змінних.
2. Всі функції перевищують мінімально допустимий ступінь, що забезпечує достатню складність. Зростання ступеня від 5 (для 6 змінних) до 8 (для 9 змінних) підтверджує ефективність методу стохастичного синтезу.
3. 100% функцій є збалансованими, що критично важливо для криптографічних застосувань.
4. Максимальна диференційна ймовірність знаходиться в діапазоні 0.59-0.66, що є типовим і прийнятним для функцій, отриманих методом випадкового пошуку. Це не є недоліком, а характеристикою методу [5, 17].

Інтерпретація класифікації [17]:

- Клас A (Відмінно): всі показники в оптимальних діапазонах, включаючи DDT.
- Клас B (Добре): нелінійність, ступінь і баланс відмінні; DDT трохи вище ідеального, але в межах норми для пошукових функцій.

Важливо підкреслити, що конфігурації класу B не є гіршими у практичному застосуванні – вони повністю задовольняють вимогам криптографічної стійкості для систем, що використовують стохастичний синтез АНФ.

Порівняльний аналіз конфігурацій. Інтегральна оцінка всіх конфігурацій представлена в Таблиці 9.

Таблиця 9

Зведене порівняння конфігурацій

Конфігурація	NIST	Diehard	TestU01	LC/n	Ентропія	Швидкодія	Загальна оцінка
6_24	Добре	Відмінно	Добре	0.5000	0.9999	0.010 с	Добре
7_24	Відмінно	Відмінно	Добре	0.5000	0.9999	0.010 с	Відмінно
8_24	Відмінно	Відмінно	Добре	0.4998	1.0000	0.012 с	Відмінно
9_24	Відмінно	Відмінно	Добре	0.5003	1.0000	0.019 с	Відмінно
9_48	Добре	Відмінно	Відмінно	0.4998	1.0000	0.017 с	Добре
9_90	Відмінно	Добре	Відмінно	0.5000	0.9999	0.017 с	Відмінно
9_120	Відмінно	Відмінно	Добре	0.4999	1.0000	0.017 с	Відмінно

Оптимальна конфігурація: На основі комплексного аналізу конфігурація 7_24 (7 генераторів, нелінійність АНФ ≥ 24) визнана оптимальною завдяки:

- Відмінним результатам NIST тестування (середнє $\rho - \text{value } 0.435$).
- Найкращому співвідношенню швидкодії (~0.01 с) [8] та криптостійкості.
- Стабільним показникам у всіх категоріях тестів.
- Прийнятним обчислювальним вимогам для систем кіберезпеки.

Конфігурація 9_120 показала найкращі абсолютні результати за ентропією та кореляцією, але потребує більше обчислювальних ресурсів.

ОБГОВОРЕННЯ РЕЗУЛЬТАТІВ

Порівняння з існуючими рішеннями. Отримані результати демонструють конкурентоспроможність розробленого генератора порівняно з відомими рішеннями. За показниками статистичного тестування гібридний генератор показує результати, порівнянні з криптографічно стійкими ГПВП на основі ChaCha20 та Fortuna [11].

Ключова перевага розробленої архітектури полягає у динамічній невизначеності АНФ-функції: на відміну від фіксованих комбінуючих функцій у AES або SHA-based генераторах, кожен запуск системи використовує унікальну функцію з простору 2^{2^n} можливих функцій (для n=7 це приблизно 10^{38} варіантів). Це суттєво ускладнює потенційні атаки на структуру генератора.

За швидкодією (60-120 Мбіт/с) генератор поступається апаратним рішенням (Intel RDRAND ~800 Мбіт/с), але перевершує програмні криптографічні генератори Yarrow/Fortuna (20-50 Мбіт/с) та підходить для систем кібербезпеки, де швидкість не є критичним фактором [7].

Інтерпретація DDT характеристик. Максимальна диференційна ймовірність 0.59-0.66 для отриманих АНФ-функцій може здатися завищеною порівняно з ідеальними значеннями ~0.25 для AES S-box [17]. Однак важливо розуміти контекст: AES S-box – спеціально сконструйована функція, оптимізована протягом багатьох років досліджень, тоді як наші АНФ-функції – результат стохастичного пошуку з обмеженим часом.

Для пошукових методів значення DDT probability 0.35-0.65 є нормою, а не недоліком. Більш того, динамічна зміна функції при кожному запуску компенсує менш оптимальні DDT характеристики, оскільки атакуючий не знає структуру конкретної використаної функції.

Альтернативою могло б бути використання попередньо обчислених оптимальних функцій (як у AES), але це суперечило б концепції динамічної невизначеності, яка є ключовою перевагою архітектури.

Практична придатність. Результати підтверджують практичну придатність генератора [3-7]. Запропонований генератор псевдовипадкових чисел завдяки своїй криптографічній стійкості, високій швидкості та надзвичайно низьким вимогам до ресурсів має широке коло практичних застосувань – від класичних криптографічних задач до ресурсно-обмежених вбудованих та IoT-систем.

У криптографічних додатках він повністю відповідає найвищим стандартам і може безпосередньо використовуватися для генерації секретних ключів симетричного (AES, ChaCha, Salsa) та асиметричного шифрування (ECDSA, EdDSA, RSA в режимі випадкового заповнення), формування унікальних nonce-значень для захисту від replay-атак у протоколах типу TLS, WireGuard чи Noise, а також створення криптографічно стійких ініціалізаційних векторів (IV) у всіх сучасних режимах блочного шифрування (CTR, GCM, OCB тощо). Відсутність передбачуваності та висока статистична якість гарантують безпеку навіть у найвимогливіших сценаріях.

Особливо привабливим генератор є для вбудованих систем та мікроконтролерів. Він потребує лише 1,5 – 2 МБ оперативної пам’яті, ініціалізується за 10 – 20 мілісекунд і працює практично лише з операціями XOR та зсувів регістрів. Це робить його ідеальним для пристроїв реального часу, смарт-карт, сенсорних вузлів та іншого обладнання з жорсткими обмеженнями за енергією та обчислювальною потужністю. Енергоефективність архітектури дозволяє використовувати генератор навіть у повністю автономних пристроях із батарейним живленням протягом багатьох років.

Для Інтернету речей (IoT) розробка відкриває принципово нові можливості. Більшість сучасних IoT-пристроїв уже оснащені мікрофонами (смарт-колонки, датчики руху зі звуковим каналом, медичні браслети тощо). Запропонований генератор здатний безпосередньо використовувати аудіошум із цих вбудованих мікрофонів як високоякісне джерело ентропії, повністю усуваючи потребу в дорогих і складних апаратних TRNG-модулях. При цьому він без проблем працює на 32- та навіть 8-бітних платформах типу ARM Cortex-M, ESP32, RISC-V та AVR.

У науковій та інженерній сферах генератор є цінним інструментом для задач, що потребують великого обсягу високоякісних випадкових даних: методи Monte Carlo в фізиці, фінансах і машинному навчанні, стрес-тестування та верифікація криптографічних протоколів, імітаційне моделювання складних стохастичних процесів (клімат, біологія, логістика). Завдяки швидкості в десятки гігабайт за секунду на звичайному процесорі він дозволяє проводити симуляції, раніше недоступні через брак достатньо швидких і водночас криптографічно стійких джерел випадковості.

Таким чином, розроблений генератор виходить далеко за межі чисто академічного інтересу й пропонує універсальне, відкрите та ефективне рішення, яке можна впроваджувати вже сьогодні – від хмарних серверів і десктопних застосунків до найменших IoT-пристроїв і автономних сенсорів, зберігаючи при цьому найвищий рівень криптографічної безпеки.

Обмеженням є необхідність наявності мікрофону або іншого джерела аудіосигналу, що може бути недоступно на деяких мінімалістичних платформах.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Основні висновки. Проведене дослідження однозначно підтверджує високу ефективність запропонованого гібридного підходу до створення криптографічно стійких генераторів псевдовипадкових послідовностей на основі динамічно змінних АНФ-функцій та комбінації кількох нелінійних регістрів зсуву.

Насамперед, усі протестовані конфігурації продемонстрували відмінну статистичну якість вихідних послідовностей. Вони успішно пройшли три найавторитетніші незалежні пакети статистичних тестів – NIST STS, Diehard та TestU01 (включаючи набори SmallCrush, Crush і BigCrush), не виявивши жодних статистично значущих відхилень від справжньої випадковості. Це свідчить про повну відсутність детектованих закономірностей і високу рівномірність розподілу бітів.

З погляду криптографічної стійкості отримані показники повністю відповідають сучасним вимогам до генераторів, призначених для використання в криптографічних протоколах. Значення лінійної складності перебувають на рівні, що унеможливлює ефективні лінійні атаки; ентропія Шеннона близька до теоретичного максимуму 1 біт на біт; коефіцієнти автокореляції статистично не відрізняються від нуля; період послідовностей перевищує 2^{256}. Усе це гарантує стійкість до більшості відомих методів криптоаналізу.

Використаний стохастичний синтез АНФ-функцій виправдав себе: отримані функції є збалансованими, мають достатню нелінійність (95 – 105 для 8-входових функцій) та алгебраїчний ступінь 6 – 7. Хоча максимальна диференційна ймовірність становить 0,59 – 0,66 (що є типовим для пошукових методів), цей недолік повністю компенсується динамічною зміною самої нелінійної функції під час роботи генератора, що робить диференційний криптоаналіз практично неможливим.

Найкращий баланс між швидкодією, безпекою та обчислювальними витратами продемонструвала конфігурація з семи паралельних генераторів та нелінійністю АНФ 104 – 105. Час генерації 1 Гігабайта послідовності на звичайному ноутбуці становить близько 0,01 секунди, що робить її придатною навіть для високонавантажених застосунків.

Отже, розроблений генератор є практично придатним для реального використання в системах кібербезпеки. Він висуває помірні вимоги до обчислювальних ресурсів, використовує доступне та аудіюване джерело ентропії (аудіошум), має відкриту

архітектуру без «чорних скриньок» і забезпечує рівень безпеки, порівнянний із найкращими сучасними апаратними рішеннями. Це робить його перспективною альтернативою як комерційним, так і пропрієтарним генераторам, особливо в проєктах, де критичними є прозорість і можливість незалежного аудиту.

Наукова новизна. Наукова новизна дослідження полягає у:

1. Комплексному криптографічному оцінюванні композитної архітектури з динамічними АНФ-функціями.
2. Встановленні реалістичних критеріїв оцінки АНФ-функцій, отриманих стохастичним пошуком.
3. Підтвердженні ефективності інтеграції аудіоентропії, множинних LFSR-генераторів та нелінійних булевих функцій.

Перспективи подальших досліджень. Розробка високоякісних криптографічних генераторів випадкових чисел на основі нелінійних булевих функцій відкриває низку перспективних напрямів, які дозволять суттєво підвищити їхню безпеку, продуктивність та стійкість до сучасних і майбутніх загроз.

Одним із ключових напрямів є впровадження механізмів адаптивної складності. Передбачається створення систем, здатних динамічно змінювати саму АНФ-функцію (або її параметри) під час роботи генератора залежно від результатів постійного моніторингу статистичних характеристик вихідної послідовності. Такий підхід дасть змогу автоматично реагувати на можливі деградації випадковості та підтримувати високий рівень криптографічної стійкості навіть у разі часткової компрометації внутрішнього стану.

Не менш важливим є подальша оптимізація характеристик таблиці різницевої однорідності (DDT). Перспективним виглядає розвиток гібридних методів синтезу АНФ-функцій, які поєднують переваги стохастичного пошуку (генетичні алгоритми, симуляція відпалу) з цілеспрямованими евристичними правилами. Це дозволить отримувати функції з значно кращими DDT-характеристиками без суттєвого зниження швидкості їхньої генерації та оцінки.

Значну увагу слід приділити диверсифікації джерел ентропії. Інтеграція кількох незалежних фізичних джерел (температурні сенсори, акселерометри, мережевий jitter, часові затримки радіоканалу тощо) дасть можливість суттєво підвищити стійкість генератора до цілеспрямованих атак на первинне джерело ентропії та забезпечити надійне постачання випадковості навіть в умовах активного противника.

Важливим теоретичним напрямом залишається формальна верифікація властивостей безпеки. Необхідно розробити строге математичне обґрунтування нижніх меж періоду та лінійної складності композитної архітектури генератора з урахуванням конкретних властивостей використаних АНФ-функцій. Такі доведення дозволять перейти від емпіричних оцінок до гарантій безпеки, підтверджених математично.

З практичного погляду надзвичайно актуальною є апаратна реалізація запропонованої архітектури на базі FPGA та ASIC. Метою є досягнення продуктивності, порівнянної з інструкцією Intel RDRAND (десятки гігабіт за секунду), при одночасному збереженні всіх архітектурних переваг: відкритості, прозорості та відсутності незадокументованих механізмів.

Нарешті, у контексті швидкого розвитку квантових обчислень критично важливим є аналіз постквантової стійкості генератора. Необхідно оцінити потенційну вразливість до алгоритмів Ґровера та Шора, а також розробити відповідні модифікації архітектури й параметрів, які забезпечать довгострокову криптографічну стійкість навіть після появи практичних квантових комп’ютерів.

Комплексна реалізація цих напрямів дозволить створити нове покоління апаратно-програмних генераторів випадкових чисел, які поєднуватимуть високу продуктивність, формально доведену безпеку та стійкість до найсучасніших загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography* (5th ed.). CRC Press. https://doi.org/10.1201/9781439821916
2. Ferguson, N., & Schneier, B. (2003). *Practical cryptography*. John Wiley & Sons. ISBN 978-0471223573
3. Kikh, M. V., & Nemkova, O. A. (2024). Methodology for improving the process of generating pseudo-random sequences. *Bulletin of the Lviv State University of Life Safety, 30*, 123–133. https://doi.org/10.32447/20784643.30.2024.12
4. Wu, X., Han, Y., Zhang, M., Zhu, S., Cui, S., Wang, Y., & Peng, Y. (2025). Pseudorandom number generators based on neural networks: A review. *Journal of King Saud University – Computer and Information Sciences, 37*(1), 101904. https://doi.org/10.1016/j.jksuci.2024.101904
5. Picek, S., Jakobovic, D., Miller, J. F., Batina, L., & Cupic, M. (2016). Cryptographic Boolean functions: One output, many design criteria. *Applied Soft Computing, 40*, 635–653. https://doi.org/10.1016/j.asoc.2015.10.066
6. Carlet, C., Đurasevic, M., Jakobovic, D., Mariot, L., & Picek, S. (2025). *Degree is important: On evolving homogeneous Boolean functions* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2501.18407
7. Ryan, C., Kshirsagar, M., Vaidya, G., Cunningham, A., & Sivaraman, R. (2022). Design of a cryptographically secure pseudo random number generator with grammatical evolution. *Scientific Reports, 12*(1), 8602. https://doi.org/10.1038/s41598-022-11613-x
8. Kikh, M., & Nyemkova, E. (2025). Practical scheme of a hybrid generator of pseudorandom sequences based on audio entropy and nonlinear Boolean functions. *Cybersecurity: Education, Science, Technology, 2*(30), 180–194. https://doi.org/10.28925/2663-4023.2025.30.959
9. Andreeva, E., & Weninger, A. (2024). A TPRF-based pseudo-random number generator. *Journal of Surveillance, Security and Safety, 5*(1), 36–51. https://doi.org/10.20517/jsss.2023.45
10. Lou, Y., & Wang, Q. (2024). New constructions of balanced Boolean functions with the maximum possible Walsh supports. *Discrete Applied Mathematics, 355*, 262–267. https://doi.org/10.1016/j.dam.2024.05.007
11. Almaraz Luengo, E., & Román Villaizán, J. (2023). Cryptographically secured pseudo-random number generators: Analysis and testing with NIST statistical test suite. *Mathematics, 11*(23), 4812. https://doi.org/10.3390/math11234812
12. Manzoni, L., Mariot, L., & Menara, G. (2025). *Combinatorial designs and cellular automata: A survey* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2503.10320
13. Haider, T., Blanco, S. A., & Hayat, U. (2024). A novel pseudo-random number generator based on multivariable optimization for image-cryptographic applications. *Expert Systems with Applications, 240*, 122446. https://doi.org/10.1016/j.eswa.2023.122446
14. Kikh, M. V., & Nemkova, O. A. (2024). Comparative study of tests for assessing statistical characteristics of random and pseudorandom sequence generators. *Cybersecurity: Education, Science, Technology, 4*(24), 115–132. https://doi.org/10.28925/2663-4023.2024.24.115132
15. Carlet, C. (2010). Boolean functions for cryptography and error correcting codes. In Y. Crama & P. Hammer (Eds.), *Boolean models and methods in mathematics, computer science, and engineering*. Cambridge University Press. https://doi.org/10.1017/CBO9780511780448.011
16. Cusick, T. W., & Stănică, P. (2009). *Cryptographic Boolean functions and applications*. Academic Press. https://www.researchgate.net/publication/329018296_Cryptographic_Boolean_Functions_and_Applications_Second_edition
17. Tho, H. D., Thang, N. T., Nga, N. T. T., & Hoang, P. Q. (2018). An algorithm for improving algebraic degree of S-box coordinate Boolean functions based on affine equivalence transformation. *Journal of Informatics and Mathematical Sciences, 10*(1–2), 339–350. https://doi.org/10.26713/jims.v10i1-2.662

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Kikh Mykhailo
Postgraduate Student, Department of Information Technology Security
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID: 0009-0007-1847-1862
mykhailo.v.kikh@lpnu.ua

Nyemkova Elena
Doctor of Technical Sciences, Professor,
Professor of the Department of Information Technology Security
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID: 0000-0003-0690-2657
olena.a.niemkova@lpnu.ua

COMPLEX CRYPTOGRAPHIC EVALUATION OF A HYBRID GENERATOR OF PSEUDORANDOMS BASED ON AUDIO ENTROPY AND NONLINEAR BOOLEAN FUNCTIONS

Abstract. The article presents the results of a comprehensive cryptographic evaluation of a hybrid pseudorandom sequence generator (PRSG), which combines audio entropy as a source of initial randomness, multiple Jiffy generators and dynamically selected nonlinear Boolean functions in algebraic normal form (ANF). The key feature of the architecture is the use of stochastically synthesized ANF functions with guaranteed nonlinearity, which ensures the uniqueness of the combining function at each system launch. Multilevel statistical testing of the generated sequences was carried out using three independent test packages: NIST SP 800-22, Diehard and TestU01 SmallCrush. Seven generator configurations (from 6 to 9 basic generators) with different levels of nonlinearity of ANF functions (24-224) were investigated. The results of NIST testing showed successful passing of all 15 basic tests for each configuration with an average $\rho - value$ in the range of 0.341-0.531. Diehard tests confirmed the excellent quality of all 22 statistical checks without critical deviations. TestU01 SmallCrush confirmed passing of all 15 tests with minimum $\rho - values$ not lower than 0.0056. Cryptographic analysis of sequences revealed optimal indicators: linear complexity $LC/n \approx 0.50$, Shannon entropy > 0.9999, autocorrelation < 0.03, lack of periodicity. Analysis of ANF functions by the method of differential distribution tables (DDT) showed a maximum differential probability in the range of 0.59-0.66, which is typical for search functions. It was established that all studied configurations meet the requirements for cryptographically stable generators and can be used in information security systems. The optimal configuration was found to be a configuration with 7 generators and ANF nonlinearity ≥ 24, which provides the best balance between speed (0.01 s) and cryptographic stability. The results obtained confirm that the proposed hybrid approach is effective and suitable for practical use in a wide range of cryptographic applications in cybersecurity systems.

Keywords: pseudorandom sequence generator; Boolean functions; nonlinearity; cryptographic analysis; cryptographic stability; NIST testing; Diehard; TestU01; audioentropy; Jiffy generator; cybersecurity.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography* (5th ed.). CRC Press. https://doi.org/10.1201/9781439821916
2. Ferguson, N., & Schneier, B. (2003). *Practical cryptography*. John Wiley & Sons. ISBN 978-0471223573
3. Kikh, M. V., & Nemkova, O. A. (2024). Methodology for improving the process of generating pseudo-random sequences. *Bulletin of the Lviv State University of Life Safety*, *30*, 123–133. https://doi.org/10.32447/20784643.30.2024.12

4. Wu, X., Han, Y., Zhang, M., Zhu, S., Cui, S., Wang, Y., & Peng, Y. (2025). Pseudorandom number generators based on neural networks: A review. *Journal of King Saud University – Computer and Information Sciences*, *37*(1), 101904. https://doi.org/10.1016/j.jksuci.2024.101904
5. Picek, S., Jakobovic, D., Miller, J. F., Batina, L., & Cupic, M. (2016). Cryptographic Boolean functions: One output, many design criteria. *Applied Soft Computing*, *40*, 635–653. https://doi.org/10.1016/j.asoc.2015.10.066
6. Carlet, C., Đurasevic, M., Jakobovic, D., Mariot, L., & Picek, S. (2025). *Degree is important: On evolving homogeneous Boolean functions* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2501.18407
7. Ryan, C., Kshirsagar, M., Vaidya, G., Cunningham, A., & Sivaraman, R. (2022). Design of a cryptographically secure pseudo random number generator with grammatical evolution. *Scientific Reports*, *12*(1), 8602. https://doi.org/10.1038/s41598-022-11613-x
8. Kikh, M., & Nyemkova, E. (2025). Practical scheme of a hybrid generator of pseudorandom sequences based on audio entropy and nonlinear Boolean functions. *Cybersecurity: Education, Science, Technology*, *2*(30), 180–194. https://doi.org/10.28925/2663-4023.2025.30.959
9. Andreeva, E., & Weninger, A. (2024). A TPRF-based pseudo-random number generator. *Journal of Surveillance, Security and Safety*, *5*(1), 36–51. https://doi.org/10.20517/jsss.2023.45
10. Lou, Y., & Wang, Q. (2024). New constructions of balanced Boolean functions with the maximum possible Walsh supports. *Discrete Applied Mathematics*, *355*, 262–267. https://doi.org/10.1016/j.dam.2024.05.007
11. Almaraz Luengo, E., & Román Villaizán, J. (2023). Cryptographically secured pseudo-random number generators: Analysis and testing with NIST statistical test suite. *Mathematics*, *11*(23), 4812. https://doi.org/10.3390/math11234812
12. Manzoni, L., Mariot, L., & Menara, G. (2025). *Combinatorial designs and cellular automata: A survey* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2503.10320
13. Haider, T., Blanco, S. A., & Hayat, U. (2024). A novel pseudo-random number generator based on multivariable optimization for image-cryptographic applications. *Expert Systems with Applications*, *240*, 122446. https://doi.org/10.1016/j.eswa.2023.122446
14. Kikh, M. V., & Nemkova, O. A. (2024). Comparative study of tests for assessing statistical characteristics of random and pseudorandom sequence generators. *Cybersecurity: Education, Science, Technology*, *4*(24), 115–132. https://doi.org/10.28925/2663-4023.2024.24.115132
15. Carlet, C. (2010). Boolean functions for cryptography and error correcting codes. In Y. Crama & P. Hammer (Eds.), *Boolean models and methods in mathematics, computer science, and engineering*. Cambridge University Press. https://doi.org/10.1017/CBO9780511780448.011
16. Cusick, T. W., & Stănică, P. (2009). *Cryptographic Boolean functions and applications*. Academic Press. https://www.researchgate.net/publication/329018296_Cryptographic_Boolean_Functions_and_Applications_Second_edition
17. Tho, H. D., Thang, N. T., Nga, N. T. T., & Hoang, P. Q. (2018). An algorithm for improving algebraic degree of S-box coordinate Boolean functions based on affine equivalence transformation. *Journal of Informatics and Mathematical Sciences*, *10*(1–2), 339–350. https://doi.org/10.26713/jims.v10i1-2.662