КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.959
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
доктор технічних наук, професор,
професор кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0000-0003-0690-2657
olena.a.niemkova@lpnu.ua

ПРАКТИЧНА СХЕМА ГІБРИДНОГО ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ АУДІОЕНТРОПІЇ ТА НЕЛІНІЙНИХ БУЛЕВИХ ФУНКЦІЙ

Анотація. У статті вирішено актуальну задачу генерації криптостійких псевдовипадкових послідовностей (ПВП) для забезпечення кібербезпеки сучасних цифрових систем. Генератори ПВП відіграють ключову роль у формуванні ключів шифрування, ініціалізаційних векторів, одноразових токенів автентифікації та інших критичних параметрів криптографічних протоколів. Недостатня криптостійкість таких генераторів може призвести до компрометації надійних протоколів, що підкреслює необхідність розробки нових методів, які долають обмеження традиційних детерміністичних підходів. Серед цих обмежень – передбачуваність послідовностей у разі розкриття внутрішнього стану, обмежена ентропія початкових значень, вразливість до статистичних атак та відсутність справжньої випадковості, що знижує ефективність у криптографічних застосуваннях. У статті запропоновано і реалізовано практичну схему побудови гібридного генератора псевдовипадкових послідовностей, що поєднує аудіоентропію та нелінійні булеві функції в алгебраїчній нормальній формі (АНФ). Архітектура базується на динамічному синтезі вихідних послідовностей модифікованих генераторів Джиффі за допомогою АНФ-функцій з високою нелінійністю, які генеруються випадково. Аудіоентропія, отримана з природного шуму мікрофона, використовується для ініціалізації початкових станів генераторів, що підвищує непередбачуваність послідовностей. Базою архітектури слугує модифікований генератор Джиффі з гнучкими параметрами регістрів зсуву (довжини 47, 53 та 59 бітів), фіксованими зворотними зв'язками на основі характеристичних поліномів із простими числами та статичними конфігураціями вихідної функції. Особливий акцент зроблено на використанні алгебраїчної нормальної форми (АНФ) булевих функцій, які дозволяють ефективно аналізувати та оптимізувати властивості нелінійності, кореляційної стійкості та складності криптоаналізу. Запропонована гібридна архітектура поєднує фізичні джерела ентропії з ефективними алгоритмами псевдовипадкової генерації, досягаючи балансу між непередбачуваністю та продуктивністю. Це актуально для вбудованих пристроїв та систем Інтернету речей (IoT), де обмежені обчислювальні ресурси, відсутні класичні джерела ентропії, а також існують вимоги до енергоефективності та реального часу. Проведене комплексне тестування за допомогою NIST SP 800-22 підтвердило високу статистичну якість згенерованих послідовностей: для 7 конфігурацій (нелінійність 24–224) воно показало 100% успіх.

Ключові слова: генератор псевдовипадкових послідовностей; булеві функції; нелінійність; аудіоентропія; генератор Джиффі; криптографічна стійкість; NIST STS; кібербезпека.

ВСТУП

У сучасному цифровому середовищі генератори псевдовипадкових послідовностей (ГПВП) відіграють ключову роль у забезпеченні криптографічної стійкості та інформаційної безпеки. Вони застосовуються для формування ключів, ініціалізаційних векторів, одноразових токенів автентифікації та інших параметрів, які визначають надійність криптографічних протоколів. Недостатня криптостійкість генератора може призвести до компрометації навіть найбільш статистично стійких алгоритмів. Водночас традиційні детерміністичні підходи характеризуються низкою обмежень, серед яких передбачуваність у разі розкриття внутрішнього стану, обмежена ентропія початкових значень, схильність до статистичних атак та відсутність справжньої випадковості. Це знижує їхню ефективність у криптографічних застосуваннях і створює потребу у нових методах генерації.

Алгебраїчна нормальна форма (АНФ) функцій становить особливий інтерес для криптографічних застосувань, оскільки дає змогу ефективно досліджувати їхні властивості не лінійності, кореляційної стійкості та складності аналізу. Булеві функції представляються у вигляді поліномів над полем GF(2), що дозволяє контролювати та максимізувати криптографічні характеристики генератора. Ключовими перевагами булевих функцій є висока нелінійність, оптимальний баланс між одиницями та нулями у вихідних послідовностях, складна кореляційна структура, а також можливість динамічної адаптації коефіцієнтів функції для підвищення непередбачуваності. Використання булевих функцій у гібридних архітектурах генераторів забезпечує додатковий рівень криптографічної стійкості, оскільки навіть часткове розкриття внутрішнього стану не дозволяє зловмиснику легко передбачити майбутні значення послідовності.

Постановка проблеми. Актуальним напрямом є використання гібридних архітектур, що поєднують фізичні джерела ентропії з ефективними алгоритмами псевдовипадкової генерації. Такий підхід забезпечує необхідний баланс між непередбачуваністю та продуктивністю, дозволяючи підтримувати якість випадкових послідовностей навіть за умов тривалого функціонування систем. Однак особливі труднощі виникають у сфері вбудованих пристроїв та Інтернету речей, де обмежені обчислювальні ресурси, відсутність класичних джерел ентропії, вимоги до енергоефективності та робота в реальному часі значно ускладнюють використання традиційних рішень.

У цьому контексті особливого значення набувають дослідження нових підходів, здатних поєднувати високу криптографічну стійкість із ресурсною оптимальністю. Запропонована в роботі гібридна архітектура, що базується на використанні аудіоентропії та динамічних АНФ-функцій, спрямована на подолання наявних обмежень і створення більш надійного механізму генерації псевдовипадкових послідовностей для сучасних застосувань.

Аналіз останніх досліджень та публікацій. Дослідження у сфері генерації псевдовипадкових послідовностей демонструють перехід від класичних лінійних методів, таких як конгруентні генератори та регістри зсуву, до криптографічно стійких систем, що поєднують різні підходи [1] – [3]. Ключове значення мають булеві функції, які визначають властивості потокових і блокових шифрів. Їх криптографічна якість оцінюється за показниками збалансованості, нелінійності, кореляційної імунності, алгебраїчної стійкості та ступеня [4] – [6]. Нещодавні роботи (2023–2024 рр.) представили нові конструкції збалансованих булевих функцій із максимально можливими Walsh-носіями, а також застосування еволюційних

алгоритмів для синтезу функцій з оптимальною нелінійністю та контрольованим алгебраїчним ступенем [7] – [9].

У розвитку генераторів все більшого значення набувають комбінаторні підходи, зокрема клітинні автомати з нелінійними правилами, що забезпечують додаткову стійкість до атак [10], [11]. Перспективними виявились і методи багатовимірної оптимізації, які дозволяють долати обмеження класичних ГПВП [12], а також нейромережеві моделі, здатні генерувати послідовності з властивостями, придатними для криптографії, комунікацій і захисту даних [13]. Водночас залишається критичною проблема верифікації – дослідження 2022–2023 років наголошують на важливості застосування стандартних пакетів тестів, зокрема NIST SP 800-22, у поєднанні з криптографічно стійкими примітивами для оцінки якості генераторів [14], [15].

Попри значний прогрес, в літературі залишаються нерозв'язаними кілька завдань: інтеграція природних джерел ентропії з детерміністичними алгоритмами у реальному часі, розробка динамічних АНФ-функцій, здатних змінюватися під час роботи, створення ефективних рішень для ресурсно-обмежених систем, а також проєктування гібридних архітектур, які поєднують множинні генератори з адаптивними нелінійними механізмами. Запропоноване дослідження спрямоване на подолання цих обмежень шляхом інтеграції аудіоентропії, стохастичного синтезу АНФ-функцій та побудови практичної гібридної архітектури.

Мета статті. Мета статті полягає в розробці та обґрунтуванні практичної гібридної архітектури генератора псевдовипадкових послідовностей на основі аудіоентропії, модифікованого генератора Джиффі та динамічних нелінійних булевих функцій в алгебраїчній нормальній формі, з метою підвищення криптографічної стійкості та статистичної якості послідовностей, підтвердженої тестами NIST SP 800-22.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Загальна архітектура системи. Блок схема гібридного генератора зображена на рисунку 1. Опис компонентів системи поданий у таблиці 1.

Таблиця 1

Основні компоненти архітектури

Компонент	Функція	Параметри	Вихід
Аудіовхід	Збір природної ентропії	48 кГц, 16 біт, 2 канали	Цифрові семпли
Екстракція бітів	Перетворення в біти	XOR 3 сусідніх молодших бітів	Бітова послідовність
Тести якості	Верифікація ентропії	Розширене тестування	Прийняття/ відхилення
Генерація сідів	Формування початкових станів	159 біт × n генераторів	Масив сідів
Генератори Джиффі	ГПВП	Три поліноми із степенями – 59, 53, 47	*n* паралельних потоків
Пошук АНФ	Синтез комбінуючої функції	Стохастичний алгоритм	Оптимальна АНФ
АНФ комбінування	Нелінійне змішування	$f(x_1, x_2, \dots x_n) = \oplus\, a_i \prod_{j \in s_j} x_j$	Фінальна послідовність

де $a_j \in \{0,1\}$, а множина S_j визначає набір змінних у мономі.

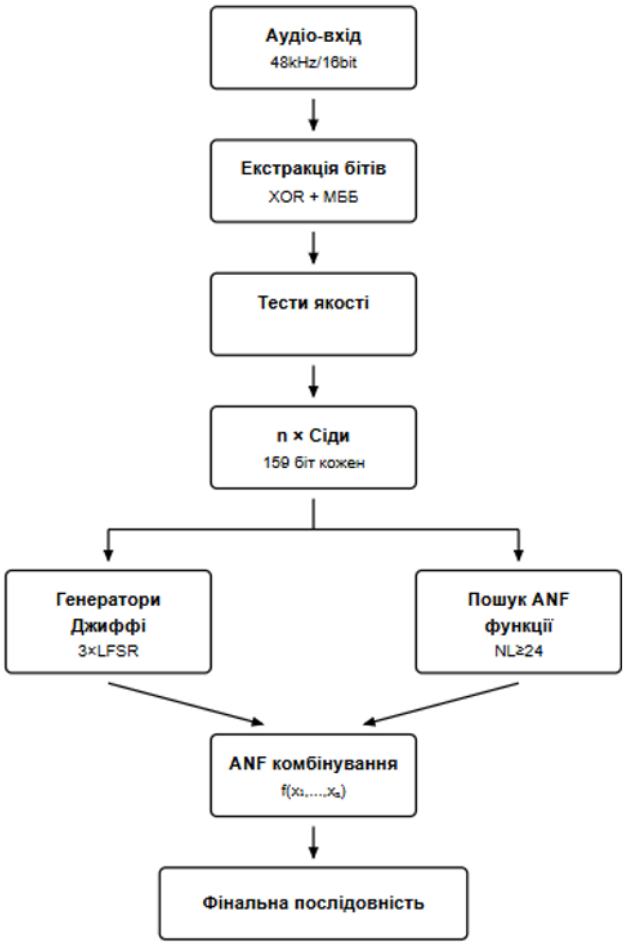


Рис. 1. Блок схема гібридного генератора

Екстракція ентропії з аудіосигналу. Аудіосигнал, отриманий із мікрофона в заданій області частоти, містить природний шум, який включає кілька компонентів. По-перше, це квантовий шум, що відбувається в процесі аналогово-цифрового перетворення (АЦП). По-друге, акустичні флуктуації, спричинені навколишнім середовищем. По-третє, електромагнітні наводки, такі як радіочастотні перешкоди, промислові шуми та атмосферні впливи. У порівнянні з іншими джерелами ентропії, таким як системний час, рухи миші чи натискання клавіатури, аудіошум вирізняється найбільшою якістю ентропії, швидкістю збору даних і незалежністю від дій користувача.

Параметри запису: 0.1 сек, 48 кГц, 2 канали, 16 біт → 9.6 тис. семплів (153 600 байтів). Використовується XOR молодших бітів трьох сусідніх семплів:

$$bit[i]=(sample[i]\&1)\oplus(sample[i+1]\&1)\oplus(sample[i+2]\&1)$$

Переваги пропонованого підходу полягають у використанні молодших бітів, які є найбільш зашумленими, що сприяє підвищенню якості псевдовипадкових послідовностей. По-перше, молодші біти мають найвищий рівень шуму, що робить їх ідеальними для генерації випадкових даних. По-друге, операція XOR забезпечує

вирівнювання розподілу, що сприяє рівномірності вихідної послідовності. По-третє, алгоритм вирізняється простотою реалізації, що дозволяє ефективно використовувати його навіть на мікроконтролерах із обмеженими обчислювальними ресурсами. Алгоритм вилучення ентропії з аудіосигналу представлений на рисунку 2.

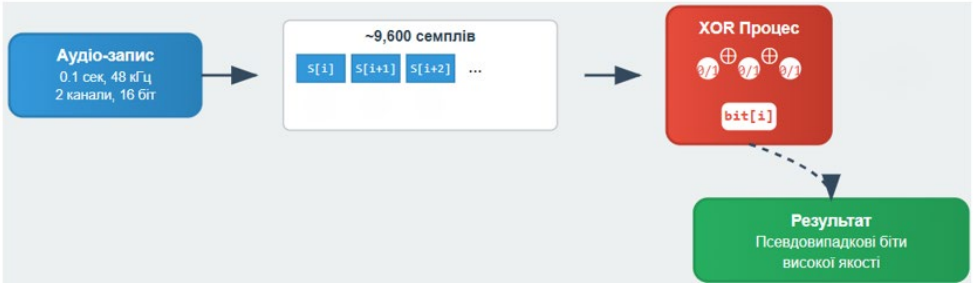


Рис. 2. Алгоритм екстракції ентропії з аудіосигналу

Математичний аналіз підтверджує стабільність цього методу навіть за умов відхилень ймовірності бітів, що робить його надійним для практичного застосування.

Для оцінювання статистичної якості згенерованих послідовностей було використано комплексний підхід, що включає аналіз ентропії, рівномірності розподілу, серій та автокореляційних характеристик. Приклади результатів розширеного тестування для 6-ти аудіозаписів тривалістю 0.1 сек кожний представлені у таблиці 2.

Таблиця 2

Результати розширеного тестування для 6 аудіозаписів

№	Рівномірність розподілу “0” і “1” (p-value>0.01)	Ентропія Шеннона (≥0,98)	Відносна різниця між кількістю “0” і “1” (%)	Тест серій на розподіленість бітів (p-value>0.01)	Автокореляція (<0.1)
1	0.583282	1.0000	0.79	0.9046	0.0024
2	0.544286	0.9999	0.88	0.8810	0.0026
3	0.049600	0.9994	2.83	0.7932	0.0024
4	0.750782	1.0000	0.46	0.8162	0.0023
5	0.664940	1.0000	0.63	0.1116	0.0028
6	0.506632	0.9999	0.96	0.0843	0.0028

Архітектура генераторів Джиффі. Серед відомих потокових генераторів псевдовипадкових послідовностей генератор Джиффі займає особливе місце завдяки вдалій комбінації високої статистичної якості та відносної простоти реалізації. Його основними перевагами є довгий період (для стандартних параметрів період становить приблизно 2^{159}, що практично унеможливлює повторення послідовності в реальних умовах використання), нелінійна вихідна функція (завдяки використанню булевої комбінації вихідних бітів кількох регістрів досягається висока стійкість проти методів відновлення внутрішнього стану), стійкість до лінійних атак (використання кількох

незалежних регістрів зсуву унеможливлює застосування простих методів лінійного криптоаналізу) та відносна простота реалізації (у порівнянні з іншими сучасними генераторами, архітектура Джиффі не вимагає складних арифметичних операцій, що робить його придатним для реалізації у вбудованих системах). Таким чином, генератор Джиффі було обрано як базовий для розробки системи множинних генераторів із можливістю модифікації структури під конкретні потреби.

Було застосовано варіант генератора Джиффі із фіксованими параметрами: довжини регістрів зсуву – 47, 53 та 59 біти; зафіксовані зворотні зв'язки у вигляді характеристичних поліномів; статичні конфігурації вихідної функції.

У нашій модифікації збережено основну ідею трьох взаємодіючих регістрів (таблиця 3). Фінальна комбінація бітів обчислюється за допомогою булевої функції:

$$f(x, y, z) = z_{47} \oplus (x_{59} \cdot y_{53})$$

де x_{59}, y_{53}, z_{47} – старші біти відповідних регістрів.

Таблиця 3

Конфігурації генераторів Джиффі

Параметр	Регістр X	Регістр Y	Регістр Z
Довжина	59	53	47
Тар-позиції	[0, 19, 31, 43, 59]	[0, 17, 29, 41, 53]	[0, 13, 23, 37, 47]
Поліном	$x^{59} + x^{43} + x^{31} + x^{19} + 1$	$x^{53} + x^{41} + x^{29} + x^{17} + 1$	$x^{47} + x^{37} + x^{23} + x^{13} + 1$

Усі показники степенів вибраних поліномів були взяті з множини простих чисел. Застосування таких поліномів забезпечує успішне проходження генератором Джиффі тестів NIST.

Щоб уникнути збігу послідовностей при використанні кількох генераторів одночасно, застосовується механізм унікалізації початкових станів. Кожен генератор отримує незалежний 159-бітний сід, який завантажується в три реєстри. Сіди формуються на основі різних часових інтервалів аудіопотоку, що значно знижує рівень ентропії. У таблиці 4 наведено приклад початкових значень трьох регістрів шести генераторів Джиффі у шістнадцятковій системі числення.

Таблиця 4

Початкові стани 6 генераторів

№	X-регістр	Y-регістр	Z-регістр	Джерело сіда
1	0x26A6CCA18DA0660	0xF42870236211A	0x4E30B6FA84D1	Audio_1[0:159]
2	0x579BA105C77FEC0	0x13D6F8DA62673B	0x79346CCA6F2B	Audio_2[127:286]
3	0x21478880E92EB20	0x102417244E5961	0x834520803FD	Audio_3[89:248]
4	0x79819D68A610A00	0x1DE59017A89CCC	0x64720116A307	Audio_4[203:362]
5	0x4BD0CDE29314DC0	0x1397B2AAF57E3F	0x6A0653B3B270	Audio_5[45:204]
6	0xEC69F4B6C83328	0x1C4C68CB776501	0x60C12A09080B	Audio_6[167:326]

Синтез та інтеграція динамічних АНФ функцій у гібридний генератор. Алгебраїчна нормальна форма – це представлення булевої функції у вигляді суми по модулю 2 мономів змінних:

$$f(x_1, x_2, \dots, x_n) = \bigoplus_i a_i \prod_{j \in S_j} x_j,$$

де $a_i \in \{0,1\}$, а множина S_j визначає набір змінних у мономі.

Основна перевага АНФ – можливість перевірки нелінійності комбінуючої функції, що підвищує стійкість до кореляційних атак і робить вихідну послідовність менш передбачуваною.

У більшості класичних генераторів використовується фіксована функція перетворення, відома противнику. У нашій роботі АНФ-функція визначається динамічно, тобто генерується під час запуску системи на основі стохастичного пошуку. Це забезпечує унікальність вихідної функції для кожного запуску, ускладнення атак на структуру генератора та можливість підбору функцій з високою нелінійністю (наприклад, ≥ 24 для 6-ти генераторів).

Стохастичний пошук виконується в кілька етапів:

1. Генерація збалансованої таблиці істинності.
2. Перетворення Мебіуса для отримання АНФ.
3. Обчислення нелінійності за допомогою швидкого перетворення Волша–Адамара (ШПВА).
4. Відбір функцій, які задовольняють критеріям збалансованості, нелінійності та алгебраїчного ступеня.

У ході експериментів було обчислено конкретні АНФ-функції з різним рівнем нелінійності. Пошук відбувався шляхом перебору комбінацій вихідних послідовностей від декількох генераторів Джиффі та подальшого аналізу отриманих функцій. Для кожного експерименту встановлювалася кількість генераторів (6, 7, 8 і 9), вимоги до нелінійності (≥24, ≥48, ≥90, ≥120), а також фіксувалися середній, мінімальний та максимальний час пошуку функцій (за 100 повторів) відповідно для кожного варіанту. На основі отриманих результатів було сформовано таблицю 5 для аналізу продуктивності при пошуку АНФ функції.

Таблиця 5

Аналіз продуктивності при пошуку АНФ функції

№	Кількість вхідних змінних (кількість генераторів Джиффі)	Вимоги до нелінійність	Середній час пошуку, сек	Мінімальний час пошуку, сек	Максимальний час пошуку, сек
1	6	≥24	0.0102	0.0000	0.0343
2	7	≥24	0.0100	0.0027	0.0896
3	8	≥24	0.0120	0.0033	0.1195
4	9	≥24	0.0185	0.0028	0.1415
5	9	≥48	0.0174	0.0040	0.1462

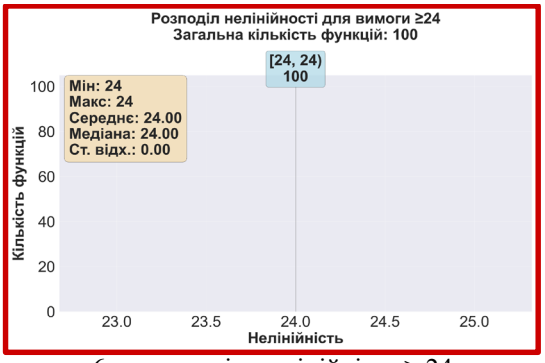
6	9	≥90	0.0165	0.0051	0.1230
7	9	≥120	0.0168	0.0061	0.1338

Було проведено аналіз розподілу значень нелінійності перших 100 отриманих АНФ-функцій, які мали нелінійність не менше ніж 24. Побудовано гістограми, де по осі X відкладено інтервали значень нелінійності, а по осі Y – кількість функцій, що потрапили до відповідного інтервалу. У результаті сформовано 7 гістограм, кожна з яких відповідає окремому експерименту. Кількість інтервалів було зафіксовано на рівні 9. Межі інтервалів визначалися на основі мінімального та максимального значення нелінійності, отриманого серед усіх 7 експериментів. Підсумкові результати узагальнено у таблиці 6 та проілюстровано на рисунку 3.

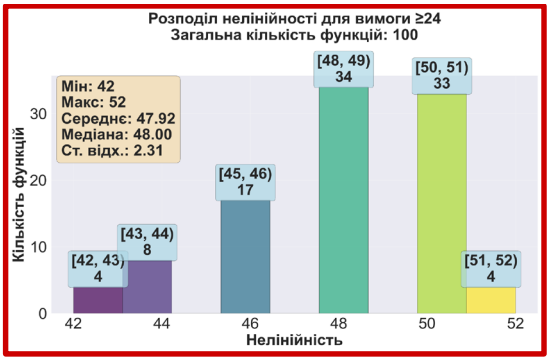
Таблиця 6

Розподіл нелінійностей отриманих АНФ-функцій

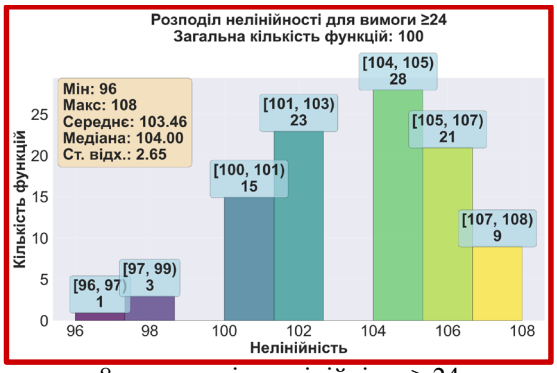
№	Кількість вхідних змінних (кількість генераторів Джиффі)	Вимоги до нелінійності	Мінімальна нелінійність	Максимальна нелінійність
1	6	≥24	24	24
2	7	≥24	42	52
3	8	≥24	96	108
4	9	≥24	208	226
5	9	≥48	204	226
6	9	≥90	206	226
7	9	≥120	210	226



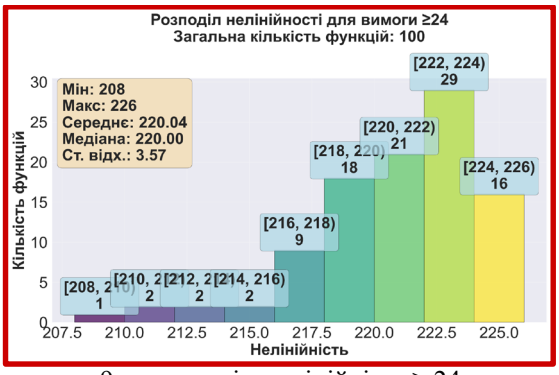
6 генераторів, нелінійність ≥ 24



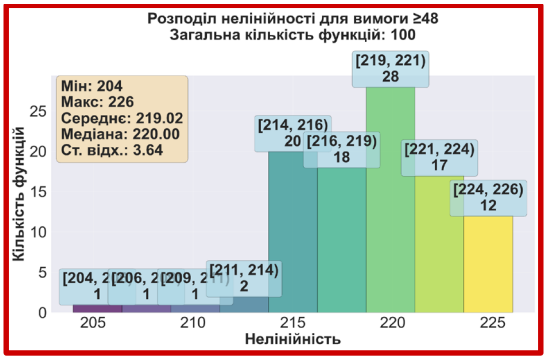
7 генераторів, нелінійність ≥ 24



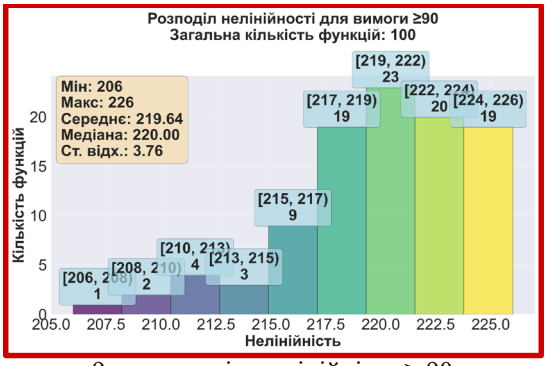
8 генераторів, нелінійність ≥ 24



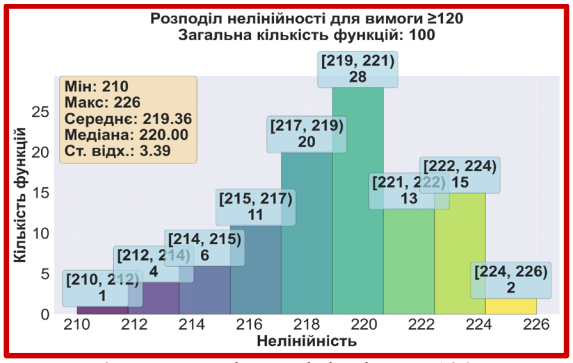
9 генераторів, нелінійність ≥ 24



9 генераторів, нелінійність ≥ 48



9 генераторів, нелінійність ≥ 90



9 генераторів, нелінійність ≥ 120

Рис. 3. Розподіл нелінійностей для різних вимог і кількості генераторів

У випадках, коли критичним фактором є швидкодія, доцільним є використання 6 змінних із нелінійністю ≥24; у свою чергу, для максимальної безпеки, коли час не є визначальним параметром, ефективним є застосування 9 змінних із нелінійністю ≥48. Загалом усі досліджені варіанти можна вважати практично прийнятними, оскільки навіть найповільніший режим не перевищує 0.05 с. Важливо підкреслити, що збільшення нелінійності понад 24 для дев'яти змінних не дає істотних переваг у швидкодії. Таким чином, система демонструє відмінну продуктивність і може бути рекомендована до практичного застосування у будь-якій із протестованих конфігурацій.

Після того як знайдена підходяща функція, вона використовується для комбінування виходів n генераторів Джиффі.

На кожному такті формується вектор вхідних бітів:

$$X_i = (gen_1[i], gen_2[i], \dots, gen_n[i]),$$

який подається на АНФ-функцію, що формує фінальний вихідний біт:

$$output[i] = f(X_i).$$

Схема комбінування:

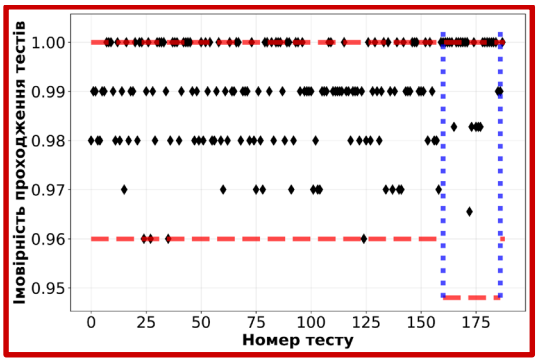
$$gen_1, gen_2, \dots, gen_n \rightarrow f(x_1, \dots, x_n) \rightarrow output$$

Гібридний підхід до генерації псевдовипадкових послідовностей має низку значних переваг. Кожен запуск використовує нову функцію комбінування, що забезпечує унікальність вихідних даних. Застосування алгебраїчної нормальної форми гарантує високу нелінійність, що робить послідовність криптографічно стійкою до атак. Поєднання аудіо-ентропії, множинних генераторів Джиффі та динамічної АНФ створює гібридну архітектуру, яка об'єднує переваги генераторів випадкових послідовностей (ГВП) і генераторів псевдовипадкових послідовностей (ГПВП), забезпечуючи високу якість і безпеку.

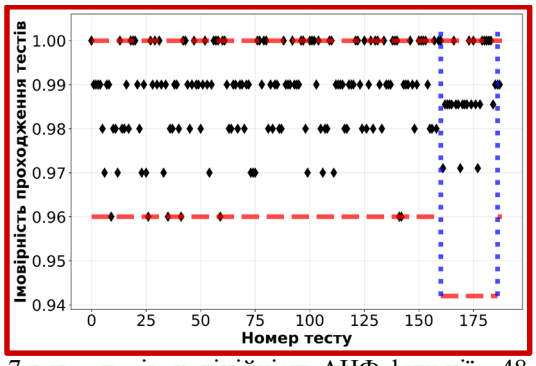
NIST STS тестування комбінованих послідовностей. За допомогою набору статистичних тестів NIST було проведено аналіз семи комбінованих послідовностей послідовностей: 6 генераторів, нелінійність АНФ функції 24 ; 7 генераторів, нелінійність АНФ функції 48; 8 генераторів, нелінійність АНФ функції 106; 9 генераторів, нелінійність АНФ функції 220; 9 генераторів, нелінійність АНФ функції 218; 9 генераторів, нелінійність АНФ функції 212; 9 генераторів, нелінійність АНФ функції 220.

Результати тестування представлені на рис. 4 у вигляді статистичних портретів. На горизонтальній вісі зображено номер тесту NIST, а на вертикальній вісі – ймовірність успішного проходження тесту. Тест вважається успішно пройденим, якщо ймовірність потрапляє в інтервал від 0,98 до 1 (для тестів [160, 186] нижній поріг 0,977); в іншому випадку тест вважається не пройденим. Межі довірчого інтервалу відзначені червоними лініями для кращого візуального сприйняття.

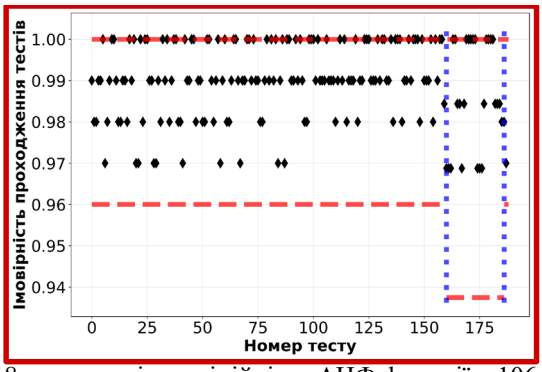
Усі сім варіантів гібридного генератора псевдовипадкових послідовностей успішно пройшли 15 статистичних тестів NIST SP 800-22, що підтверджує високу статистичну якість послідовностей. Тести оцінювали: збалансованість нулів і одиниць (Frequency, BlockFrequency), кумулятивне відхилення (CumulativeSums), довжину серій (Runs, LongestRun), лінійну незалежність (Rank), періодичність (FFT), частоту шаблонів (NonOverlappingTemplate, OverlappingTemplate), стисливість (Universal), регулярність підпослідовностей (ApproximateEntropy), випадкові блукання (RandomExcursions, RandomExcursionsVariant), частоти перекриваючих блоків (Serial) та лінійну складність (LinearComplexity).



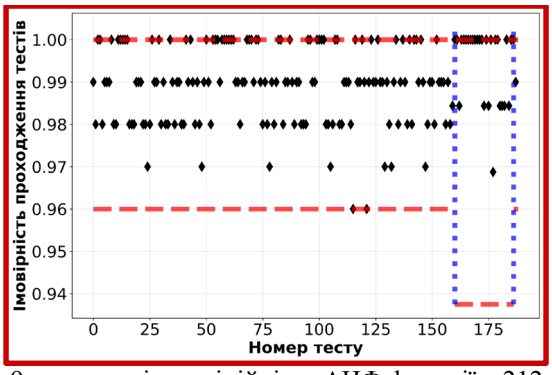
6 генераторів, нелінійність АНФ функції – 24



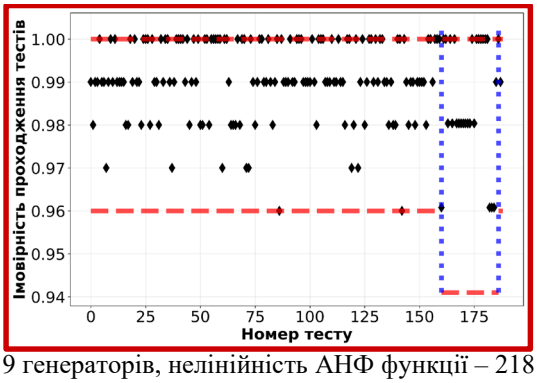
7 генераторів, нелінійність АНФ функції – 48



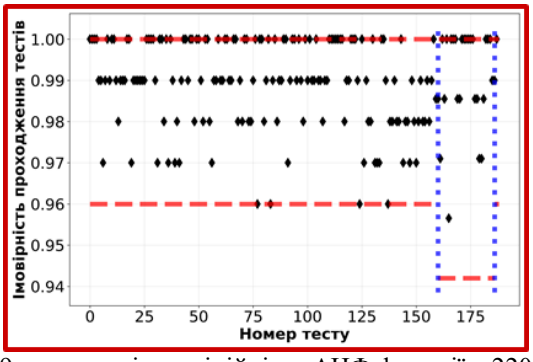
8 генераторів, нелінійність АНФ функції – 106



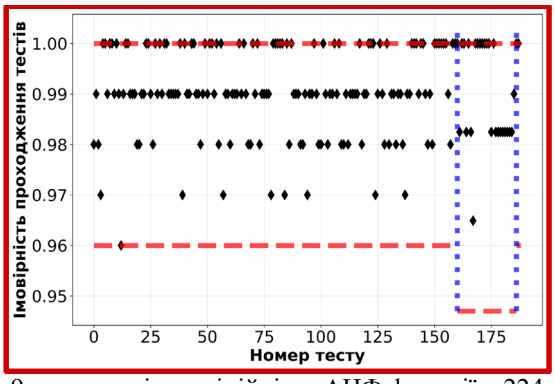
9 генераторів, нелінійність АНФ функції – 212



9 генераторів, нелінійність АНФ функції – 218



9 генераторів, нелінійність АНФ функції – 220



9 генераторів, нелінійність АНФ функції – 224

Рис. 4. Результати тестування 7 комбінованих послідовностей

Кожен варіант відповідав вимогам усіх тестів, демонструючи відсутність статистичних дефектів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Запропонована гібридна архітектура генератора псевдовипадкових послідовностей, що поєднує аудіоентропію, модифікований генератор Джиффі та динамічні АНФ-функції, продемонструвала високу статистичну якість. Усі протестовані конфігурації (з 6–9 генераторами та нелінійністю АНФ-функцій від 24 до 224) успішно пройшли 188 тестів NIST SP 800-22, що підтверджує хороші статистичні характеристики згенерованих послідовностей. Використання аудіоентропії забезпечує стабільне джерело високоякісної ентропії. Застосування синтезу випадкових АНФ-функцій дозволяє досягти високої нелінійності, а гнучка конфігурація регістрів зсуву підвищує адаптивність системи.

Експериментальний аналіз показав, що конфігурація з 6 змінними та нелінійністю ≥24 є оптимальною для систем, де критичною є швидкодія, тоді як конфігурація з 9 змінними та нелінійністю ≥48 забезпечує вищий рівень нелінійності. Час генерації АНФ-функцій у всіх випадках не перевищує 0.05 сек, що робить систему придатною для роботи в реальному часі.

Перспективи подальших досліджень у цій галузі охоплюють кілька ключових напрямів. Планується оптимізація алгоритмів випадкового пошуку АНФ-функцій, щоб підвищити швидкість генерації без втрати нелінійності. Передбачається інтеграція додаткових джерел ентропії для покращення якості початкових станів генераторів. Розглядається можливість застосування нейромережевих моделей для синтезу АНФ-функцій із заданими характеристиками. Також планується розроблення методів адаптивної зміни структури генератора в реальному часі, що сприятиме підвищенню стійкості до потенційних атак. Нарешті, буде проведено аналіз криптографічної стійкості, який включатиме оцінку стійкості до лінійного, диференціального криптоаналізу та інших специфічних атак.

Запропонована схема має потенціал для практичного застосування в системах кібербезпеки, зокрема для створення псевдовипадкових послідовностей, придатних для захисту даних і комунікаційних протоколів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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
2. 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
3. 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
4. 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
5. 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
6. 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

7. 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
8. 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(3), 18. https://doi.org/10.1007/s44443-025-00007-4
9. 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
10. NIST Special Publication 800-22. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications." National Institute of Standards and Technology, 2010. https://csrc.nist.gov/ publications/detail/sp/800-22/rev-1a/final
11. Zurc, I. "HANDBOOK of APPLIED CRYPTOGRAPHY" . CRC Press, 1996. https://www.academia.edu/33795500/HANDBOOK_of_APPLIED_CRYPTOGRAPHY
12. Seberry, J., Zhang, X. M., & Zheng, Y. L. (1995). Nonlinearity and Propagation Characteristics of Balanced Boolean Functions. Information and Computation, 119(1), 1–13. https://doi.org/10.1006/inco.1995.1073
13. Carlet, C. "Boolean Functions for Cryptography and Error Correcting Codes." In: Crama, Y., Hammer, P. (eds) Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge University Press, 2010. https://www.researchgate.net/publication/228720083_Boolean_Functions_for_Cryptography_and_Error_Correcting_Codes
14. Ferguson, N., Schneier, B., & Schneier, B. (2003). Practical cryptography. Wiley.
15. Cusick, T. W., & Stănică, P. (2009). Cryptographic Boolean functions and applications (1st edition). Academic Press.

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

PRACTICAL SCHEME OF A HYBRID GENERATOR OF PSEUDORANDOMS BASED ON AUDIOENTROPY AND NONLINEAR BOOLEAN FUNCTIONS

Abstract. The article solves the urgent problem of generating crypto-resistant pseudorandom sequences (PRS) to ensure the cybersecurity of modern digital systems. PRS generators play a key role in the formation of encryption keys, initialization vectors, one-time authentication tokens, and other critical parameters of cryptographic protocols. Insufficient crypto-resistance of such generators can lead to the compromise of reliable protocols, which emphasizes the need to develop new methods that overcome the limitations of traditional deterministic approaches. Among these limitations are the predictability of sequences in the event of disclosure of the internal state, limited entropy of initial values, vulnerability to statistical attacks, and the absence of true randomness, which reduces efficiency in cryptographic applications. The article proposes and implements a practical scheme for constructing a hybrid pseudorandom sequence generator that combines audio entropy and nonlinear Boolean functions in algebraic normal form (ANF). The architecture is based on the dynamic synthesis of output sequences of modified Jiffy generators using ANF functions with high nonlinearity, which are generated randomly. Audio entropy obtained from natural microphone noise is used to initialize the initial states of the generators, which increases the unpredictability of the sequences. The architecture is based on a modified Jiffy generator with flexible shift register parameters (lengths of 47, 53 and 59 bits), fixed feedbacks based on characteristic polynomials with prime numbers and static configurations of the output function. Special emphasis is placed on the use of algebraic normal form (ANF) of Boolean functions, which allows for effective analysis and optimization of the properties of nonlinearity, correlation stability and cryptanalysis complexity. The proposed hybrid architecture combines physical sources of entropy with efficient pseudorandom generation algorithms, achieving a balance between unpredictability and performance. This is relevant for embedded devices and Internet of Things (IoT) systems, where computing resources are limited, classical sources of entropy are absent, and there are requirements for energy efficiency and real-time. Comprehensive testing using NIST SP 800-22 confirmed the high statistical quality of the generated sequences: for 7 configurations (nonlinearity 24–224) it showed 100% success.

Keywords: pseudorandom sequence generator; Boolean functions; nonlinearity; audio entropy; Jiffy generator; cryptographic strength; NIST STS; cybersecurity.

REFERENCES

1. 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
2. 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
3. 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
4. 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

5. 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
6. 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
7. 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
8. 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(3), 18. https://doi.org/10.1007/s44443-025-00007-4
9. 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
10. NIST Special Publication 800-22. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications." National Institute of Standards and Technology, 2010. https://csrc.nist.gov/ publications/detail/sp/800-22/rev-1a/final
11. Zurc, I. "HANDBOOK of APPLIED CRYPTOGRAPHY" . CRC Press, 1996. https://www.academia.edu/33795500/HANDBOOK_of_APPLIED_CRYPTOGRAPHY
12. Seberry, J., Zhang, X. M., & Zheng, Y. L. (1995). Nonlinearity and Propagation Characteristics of Balanced Boolean Functions. Information and Computation, 119(1), 1–13. https://doi.org/10.1006/inco.1995.1073
13. Carlet, C. "Boolean Functions for Cryptography and Error Correcting Codes." In: Crama, Y., Hammer, P. (eds) Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge University Press, 2010. https://www.researchgate.net/publication/228720083_Boolean_Functions_for_Cryptography_and_Error_Correcting_Codes
14. Ferguson, N., Schneier, B., & Schneier, B. (2003). Practical cryptography. Wiley.
15. Cusick, T. W., & Stănică, P. (2009). Cryptographic Boolean functions and applications (1st edition). Academic Press.