DOI: 10.58254/viti.8.2025.22.280

УДК 004.056.5

д-р техн. наук, професор Чевардін В. Є. ORCID 0000-0002-1070-4568 (ВІТІ ім. Героїв Крут)
Прийма О. О. ORCID 0009-0008-6991-1773 (ВІТІ ім. Героїв Крут)

РЕЗУЛЬТАТИ АНАЛІЗУ СТІЙКОСТІ ТА ОБЧИСЛЮВАЛЬНОЇ ШВИДКОДІЇ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ВЛАСТИВОСТЕЙ

У статті представлено результати комплексного дослідження криптографічних властивостей та обчислювальної ефективності детермінованих генераторів псевдовипадкових послідовностей (DRBG), стандартизованих NIST SP 800-90A Rev.1. Проведено порівняльний аналіз алгоритмів CTR_DRBG, HASH_DRBG, HMAC_DRBG та Dual_EC_DRBG з використанням різних криптографічних примітивів: блокового шифру AES-256, хеш-функцій SHA-256/SHA-512 та еліптичних кривих P-256/P-384.

Досліджено залежність продуктивності генераторів від типу базового криптографічного примітива шляхом вимірювання кількісних показників cycles per byte (cpb) на 64-бітній архітектурі. Верифіковано статистичні властивості згенерованих послідовностей за допомогою тестового набору NIST SP 800-22 Rev.1a. Встановлено, що CTR_DRBG на основі AES-256 та HMAC_DRBG із SHA-256 забезпечують оптимальне співвідношення між криптографічною стійкістю та швидкодією, демонструючи найвищу продуктивність серед досліджених реалізацій.

Показано, що Dual_EC_DRBG, побудований на операціях скалярного множення точок еліптичних кривих, характеризується найвищою обчислювальною складністю внаслідок арифметики у групі точок еліптичної кривої, проте демонструє граничну статистичну якість вихідних послідовностей. Обґрунтовано перспективність застосування еліптичних криптопримітивів у контексті побудови постквантово-стійких генераторів.

Результати дослідження формують методологічну основу для обґрунтованого вибору типу DRBG відповідно до вимог конкретного криптографічного застосування з урахуванням обмежень на обчислювальні ресурси та рівень безпеки. Отримані дані можуть бути використані для оптимізації протоколів генерації ключового матеріалу, розробки систем електронного підпису та автентифікації, а також проєктування криптографічних механізмів, сумісних із міжнародними стандартами безпеки.

Ключові слова: *детерміновані генератори псевдовипадкових бітів, DRBG, криптографічна стійкість, обчислювальна складність, еліптичні криві, блокові шифри, хеш-функції, статистичне тестування, постквантова криптографія.*

V. Chevardin, O. Pryma. Results of the Analysis of Cryptographic Resilience and Computational Performance of Pseudorandom Generators

The paper presents the results of a comprehensive study of the cryptographic properties and computational efficiency of deterministic random bit generators (DRBG) standardized in NIST SP 800-90A Rev.1. A comparative analysis of the CTR_DRBG, HASH_DRBG, HMAC_DRBG, and Dual_EC_DRBG algorithms was conducted using various cryptographic primitives, including the AES-256 block cipher, SHA-256/SHA-512 hash functions, and elliptic curves P-256 and P-384.

The dependence of generator performance on the type of underlying cryptographic primitive was investigated by measuring the quantitative indicator cycles per byte (cpb) on a 64-bit architecture. The statistical properties of the generated sequences were verified using the NIST SP 800-22 Rev.1a test suite. It was established that CTR_DRBG based on AES-256 and HMAC_DRBG using SHA-256 provide an optimal balance between cryptographic strength and computational speed, demonstrating the highest performance among the studied implementations.

Dual_EC_DRBG, based on scalar point multiplication over elliptic curves, exhibits the highest computational complexity due to the arithmetic of elliptic-curve point groups but achieves the highest statistical quality of output sequences. The study substantiates the prospects of using elliptic-curve cryptographic primitives for the design of post-quantum-resistant random bit generators.

The results form a methodological basis for the reasoned selection of DRBG types according to specific cryptographic application requirements, considering computational constraints and security levels. The findings can be used to optimize key-generation protocols, design electronic signature and authentication systems, and develop cryptographic mechanisms compliant with international security standards.

Keywords: *deterministic random bit generators, DRBG, cryptographic strength, computational complexity, elliptic curves, block ciphers, hash functions, statistical testing, post-quantum cryptography.*

Постановка проблеми та актуальність дослідження

Поява квантових комп'ютерів викликала реальну потребу в підвищенні стійкості існуючих криптопримітивів, які використовуються в системах електронно-цифрового підпису, системах та комплексах автентифікації та розмежування доступу, генерації загальних секретних ключів для шифрування та автентифікації даних. Паралельно була розпочата компанія щодо розробки нових криптопримітивів, які використовують інші математичні апарати для побудови криптографічних операцій. Особливу увагу вчені завжди приділяли розробці стійких алгоритмів генерації криптографічних ключів, що обґрунтовано їх значенням для протоколів та алгоритмів шифрування даних, інкапсуляції криптографічних ключів. За останнє десятиріччя було прийнято декілька національних стандартів NIST в якості базових та загально визначених алгоритмів генерації псевдовипадкових послідовностей для створення криптографічних ключів, а саме сімейства алгоритмів, які в якості криптопримітивів використовують блокові симетричні схеми шифрування, алгоритми гешування даних, перетворення точок еліптичної кривої над простими полями та їх розширення. Поява нових алгоритмів завжди викликає нові ризики щодо появи невідомих раніше уразливостей, які можуть бути виявлені з часом. Це, в свою чергу, уповільнює впровадження нових алгоритмів в існуючі інформаційні системи для криптографічного захисту інформації, тому власники інформаційних систем іноді схиляються до використання існуючих криптографічних систем з деякими удосконаленнями за рахунок збільшення параметрів криптографічної стійкості, за що платою є незначні зниження швидкодії алгоритмів, які компенсуються підвищенням потужності обчислювальних засобів.

Таким чином, підвищення швидкодії криптографічних генераторів псевдовипадкових послідовностей (ГПВП), оцінка їх псевдовипадкових властивостей та криптографічної стійкості є актуальним науковим напрямом важливим для забезпечення стійкості існуючих криптосистем до нових загроз викликаних появою та збільшенням потужності квантових комп'ютерів. У цієї роботі наведено порівняння основних класів генераторів із короткими характеристиками та оцінками стійкості та обчислювальної швидкодії.

Аналіз останніх публікацій та наукових результатів

Сьогодні існує багато розроблених як генераторів випадкових послідовностей (random bit generator – RBG) так і генераторів псевдовипадкових послідовностей (deterministic random bit generator – DRBG), які створені для використання в різноманітних протоколах, але як правило, мають схожий математичний апарат для побудови криптографічних систем шифрування, гешування та інших криптопримітивів. Останніми результатами, досягнутими в цьому напрямку є використання стандартизованих криптографічних алгоритмів для побудови криптографічно стійких генераторів DRBG. Розглянемо існуючі класи ГПВП, рекомендовані різними джерелами та стандартами, які були досліджені за останнє десятиріччя.

У роботі [1] розроблено нові моделі безпеки для генераторів псевдовипадкових чисел із вхідною ентропією. Основним результатом є побудова seedless-генераторів, що не потребують початкового випадкового зерна (ентропійного значення seed), але залишаються стійкими до компрометації внутрішнього стану генератора та впливу на джерела ентропії. Криптографічна стійкість ГПВП досягається за рахунок використання криптографічних хеш-функцій SHA-2, SHA-3 та HMAC, що забезпечують за думкою автора як обчислювальну, так і теоретичну стійкість.

У роботі [2] формалізовано визначення сім'ї 12-раундових функцій Keccak, відомих як TurboSHAKE, для використання в постквантових криптографічних схемах. Показано, що скорочення кількості раундів не погіршує стійкість алгоритму, а забезпечує вищу продуктивність і сумісність із існуючими реалізаціями Keccak/XOF, що стало можливим завдяки оптимізації структури примітива, запозиченого з Kangaroo Twelve.

У роботі [3] запропоновано нову конструкцію детермінованого генератора псевдовипадкових бітів (XDRBG), що ґрунтується на використанні будь-якої функції з

розширюваним виходом (XOF). Основним результатом є доведення формальної стійкості в ідеальній моделі XOF із щільними межами стійкості та демонстрацією квантової стійкості. Безпечність досягнуто завдяки універсальній конструкції, що поєднує алгоритми SHAKE128, SHAKE256 і ASCON-XOF та забезпечує як високу швидкодію, так і стійкість до компрометації внутрішнього стану генератору ПВП.

У роботі [4] наведено результати аналізу стійкості генератора DRBG, що базується на перестановках, запропонованого Coretti та іншими авторами на конференції CRYPTO 2019. Зокрема, авторами було доведено, що конструкція генераторів цього класу, заснована на "губковій" (sponge) схемі. Цей алгоритм отримав назву Sponge-DRBG. У роботі показано, що ця конструкція є стійкою до криптографічних атак. Авторам вдалося покращити теоретичну межу безпеки DRBG, що базується на перестановках, із рівня $O(min\{2^{c/3}, 2^{\lambda/2}\})$ до $O(min\{2^{c/2}, 2^{\lambda/2}\})$, тобто до максимально можливої (так званої *birthday-bound*) границі стійкості. Завдяки аналізу губкової структури (sponge construction) запропоновано новий генератор POSDRBG з підвищеною швидкістю генерації (output rate = 1) без втрати безпеки. Підвищення досягнуто за рахунок оптимізації параметрів ємності (c) та мінімальної ентропії (λ).

У роботі [5] запропоновано новий тип генератора псевдовипадкових бітів, побудований на асиметричних числових системах (ANS), які традиційно використовуються у стисненні даних. Автори показали статистичну схожість вихідних послідовностей з істинно випадковими для великих параметрів R на основі NIST STS тестів. Також автори показали, що після застосування Keccak-перетворень і ротаційних операцій вихідні дані також успішно проходять тести NIST STS. На думку авторів, отримані результати засвідчили формальну криптографічну стійкість при великих R та евристичну стійкість при менших значеннях, включно із заявленою квантовою стійкістю конструкції.

Таким чином, аналіз останніх робіт підтверджує основні напрями вдосконалення існуючих схем генерації ПВП, а саме це оцінка та підвищення криптографічної стійкості генераторів DRBG за рахунок використання більш стійких криптоперетворень як до існуючих методів криптоаналізу, так і для методів квантового криптоаналізу. Також, дослідження сучасних і перспективних алгоритмів генерації ПВП, пов'язано з швидкими оцінками потенційних властивостей вихідних послідовностей генераторів ПВП із використанням методик оцінки статистичної безпеки NIST STS. Далі у статті представлено власні дослідження існуючих та перспективних схем генерації ПВП з оцінкою криптографічної та статистичної безпеки.

Дослідження та оцінка параметрів стійкості та статистичної властивостей

Лінійні ГПВП (LCG, MCG)

Прості у реалізації та швидкі в роботі, проте вони не забезпечують криптографічної стійкості, що робить їх непридатними для захисту інформації. Основне призначення таких генераторів – це симуляції, статистичне моделювання та інші задачі, де не потрібна криптографічна захищеність.

Прикладами лінійних генераторів є LCG, MCG, XORShift, Mersenne Twister, PCG та WELL512a, серед яких найкращі показники швидкодії демонструє PCG зі значенням 1.5-4 cpb. Водночас криптографічна стійкість PCG залишається досить низькою та оцінюється приблизно на рівні $2^{30} - 2^{40}$, що підтверджує непридатність цього класу генераторів для криптографічних застосувань.

ГПВП на основі регістрів зсуву (LFSR/NLFSR)

Генератори цього типу формуються на основі регістрів зсуву з лінійними (LFSR) або нелінійними (NLFSR) зворотними зв'язками між бітами регістра. Завдяки високій обчислювальній ефективності та можливості апаратної реалізації, вони знайшли широке застосування у потокових шифрах, що забезпечують захист даних у режимі реального часу.

До найпоширеніших представників цього класу належать LFSR, NLFSR, Combined LFSR, Geffe, Shrinking та Stop-and-Go генератори. Серед них базовий LFSR характеризується найвищою швидкодією – приблизно 1–3 cycles per byte (cpb). Криптографічна стійкість генераторів, побудованих на основі регістрів зсуву, зазвичай оцінюється в межах $2^{50} - 2^{70}$, що робить їх прийнятними для окремих прикладних завдань, хоча вони поступаються сучасним криптографічним стандартам за рівнем безпеки.

Комбіновані ГПВП

Створюються шляхом поєднання кількох різних алгоритмів або методів генерації, що дозволяє значно підвищити як криптографічну стійкість, так і період послідовності порівняно з простими генераторами. Такий підхід компенсує недоліки окремих алгоритмів і забезпечує кращі статистичні властивості вихідної послідовності.

До найвідоміших представників комбінованих генераторів належать Xoshiro256**, Xoroshiro, WELL1024 та Hybrid Taus, серед яких найкращі показники швидкодії демонструє Xoshiro256** зі значенням 1–3 cpb. Криптографічна стійкість комбінованих генераторів оцінюється приблизно на рівні $2^{60} - 2^{80}$, що робить їх придатними для широкого спектра застосувань, включаючи наукові обчислення та деякі криптографічні задачі середнього рівня безпеки.

Криптографічні ГПВП (DRBG)

DRBG є фундаментальним компонентом сучасних систем криптографічного захисту інформації. Призначення DRBG полягає у формуванні бітових послідовностей, статистичні властивості яких наближені до істинно випадкових, але отримані детермінованим способом із використанням криптографічних перетворень. Забезпечення якісної псевдовипадковості є ключовою передумовою надійності криптографічних протоколів, систем шифрування, автентифікації, цифрових підписів та керування сесіями [6].

На відміну від класичних генераторів псевдовипадкових чисел, криптографічні DRBG мають підвищені вимоги до стійкості до передбачуваності, стійкості до відтворення попередніх станів генератору та стійкості до криптоаналітичних атак на алгоритм генерації внутрішнього стану генератору. Ці три показника визначають властивість таких алгоритмів, що навіть за умови розкриття частини внутрішнього стану або попередніх вихідних даних зловмисник не може обчислити наступні елементи послідовності [7].

Сучасні реалізації криптографічних DRBG ґрунтуються на використанні криптографічних примітивів із доведеною односторонністю, зокрема блочних шифрів, хеш-функцій, потокових шифрів та інших криптопримітивів. Це дозволяє пов'язати рівень криптографічної стійкості генератора із криптографічною стійкістю базового алгоритму. Найпоширенішими прикладами таких реалізацій є CTR-DRBG, HMAC-DRBG, SHAKE256 та Fortuna, які застосовують різні механізми оновлення початкового стану (reseed) та генерації внутрішнього стану DRBG.

Одним із найбільш ефективних та стандартизованих DRBG є CTR-DRBG (Counter-mode Deterministic Random Bit Generator), описаний у документі NIST SP 800-90A Rev. 1 [8]. Принцип його роботи базується на алгоритмі блочного шифрування у режимі лічильника (Counter Mode), що забезпечує високий рівень розсіювання, відсутність внутрішньої кореляції між блоками, криптографічну стійкість і непередбачуваність вихідних даних.

Прикладами генераторів ПВП на основі блокових, потокових схем шифрування та шгеш-функцій є: ChaCha20, AES-CTR-DRBG, HMAC-DRBG, SHAKE256, Fortuna, з яких за показниками швидкодії кращим є ChaCha20, а саме значення швидкодії для нього складає 3–12 cpb, при цьому значення його криптографічної стійкості складає $\geq 2^{128}$.

Квантові генератори (QRNG)

QRNG формують випадковість із фізичних квантових процесів, таких як фотонна емісія, квантові флуктуації вакууму або розпад радіоактивних ізотопів. Вважається, що сьогодні це найвищий рівень непередбачуваності, але використання цих генераторів для потокового

шифрування або для генерації спільних криптографічних ключів є складною задачею, що обмежує їх сферу застосування в криптографічних алгоритмах.

Прикладами генераторів ПВП на основі фізичних квантових процесів є генератори: ID Quantique QRNG, Toshiba QRNG, Quantis, Quside QRNG, з яких за показниками швидкодії кращим є ID Quantique QRNG, а саме значення швидкодії для нього складає 10–100 cpb, при цьому, значення його криптографічної стійкості неможливо оцінити класично. Завдяки квантовій природі випадковості, QRNG забезпечують теоретично абсолютну непередбачуваність, проте їхнє практичне впровадження стримується високою вартістю обладнання, складністю інтеграції та обмеженою швидкістю генерації порівняно з програмними рішеннями.

Принципи побудови DRBG

Формування криптографічно стійких псевдовипадкових послідовностей базується на моделі детермінованої генерації, у якій випадковість вихідних даних забезпечується не фізичними джерелами ентропії (наприклад шуми діодів, зміни повітряної турбулентності та інші джерела ентропії), а криптографічною складністю відновлення внутрішнього стану генератора [9].

Згідно з визначенням [8], криптографічно стійкий DRBG можна подати у вигляді відображення $G: \{0,1\}^s \to \{0,1\}^n$, яке, отримавши початковий стан генератора (seed), сформований на основі ентропійних вхідних даних (entropy input), породжує послідовність довжиною $n \gg s$ біт, статистичні властивості якої не відрізняються від властивостей істинно випадкової послідовності.

Архітектура DRBG включає три основні фази [8]:

● Ініціалізація генератора (Instantiate) – це процес встановлення початкового внутрішнього стану генератора псевдовипадкових чисел. Результатом ініціалізації є встановлення параметрів внутрішнього стану, який визначається впорядкованою парою $S = (K, V)$, де K – симетричний ключ блочного шифру, а V – внутрішній лічильник, що керує послідовністю блоків.

● Оновлення стану генератора (Reseed) – це процес періодичного відновлення внутрішнього стану генератора з метою підвищення ентропії та запобігання втраті криптографічної стійкості. Під час оновлення до поточного стану вводяться нові ентропійні дані, а також, за потреби, додаткові параметри. У результаті формується нова пара (K, V), що замінює попередні значення ключа та лічильника. Процедура гарантує неможливість відтворення попередніх вихідних даних навіть за умови часткової компрометації стану.

● Генерація вихідних даних (Generate) – це процес формування вихідних бітів шляхом криптографічного перетворення поточного стану генератора. Для CTR_DRBG це відбувається через блочне шифрування лічильника V під ключем Key у режимі лічильника (CTR) $Output_i = E_K(V + i)$. Після завершення генерації виконується оновлення параметрів K та V, що запобігає повторному використанню стану та підтримує криптографічну стійкість генератора.

Криптографічно стійкий DRBG повинен задовольняти властивостям безпеки [8]:

● Стійкість до передбачення (prediction resistance) – компрометація поточного внутрішнього стану не повинна давати змоги передбачити майбутні вихідні біти.

● Стійкість до відновлення попередніх виходів (backtracking resistance) – компрометація поточного стану не дозволяє відновити дані, згенеровані раніше.

● Стійкість до продовження компрометації стану (state compromise extension resistance) – властивість, за якої компрометація внутрішнього стану генератора не впливає на подальші вихідні дані: після виконання оновлення стану генератора нові вихідні послідовності залишаються криптографічно незалежними від попередніх.

Оцінка показників обчислювальної швидкодії та криптографічної стійкості криптопримітивів реалізованих в структурах DRBG

Реалізації CTR-DRBG відрізняються вибором симетричного блочного шифру, який визначає як рівень стійкості, так і експлуатаційні характеристики (швидкодію, можливість паралельної обробки тощо). У цьому розділі систематизовано властивості реалізацій на основі DES, 3DES та AES у контексті вимог NIST SP 800-90A Rev.1 [8] і супутніх рекомендацій [14; 15].

Введемо показники для оцінки обчислювальної швидкодії та криптографічної стійкості DRBG:

- Cycles per byte (cpb) – це одиниця виміру складності, яка показує, скільки тактів процесор в середньому витрачає на обробку одного байта даних. Для більш кращого сприйняття переваги в швидкодії алгоритму та порівняльного аналізу продуктивності алгоритмів будемо використовувати обернену величину (1/cpb).
- Cycles per block – це одиниця виміру складності, яка показує, скільки тактів процесор в середньому витрачає на обробку одного блоку даних.
- Криптографічна стійкість (security strength) – ймовірність визначення закону формування ПВП (тобто прогнозування будь-яких бітів ПВП без знання секретного параметра seed) за рахунок визначення секретних параметрів генератора або зламу шифру. Криптографічну стійкість прийнято поєднувати також з обсягом обчислювальних витрат, які необхідно витратити для зламу криптографічного перетворення, на основі якого побудований генератор ПВП. Згідно з [8], необхідний об'єм роботи для відтворення закону формування ПВП з довжиною вхідного seed 112, 128, 192, 256 біт складе $2^{112}, 2^{192}, 2^{256}$ операцій відповідно. Є доведена та обчислювальна криптостійкість.

Під час порівняння криптографічних алгоритмів часто використовують їх здатність до розпаралелювання, тобто можливість одночасного опрацювання декількох блоків даних алгоритму як окремих потоків даних, що дає можливість отримувати перевагу над іншими алгоритмами в швидкодії.

У таблиці 1 наведено порівняння продуктивності CTR-DRBG із різними блочними шифрами. Показник cycles per byte (cpb) використовується як умовна міра швидкодії на архітектурі x86-64.

Таблиця 1

Порівняння CTR-DRBG на різних алгоритмах шифрування

Алгоритм	Блок (біт)	Раунди	Cycles / byte (cpb)	Cycles / block	Оцінка швидкодії (1/cpb)	Криптостійкість (2^exp)
AES -128	128	10	12–15	~1500–1900	0.08–0.066	$\approx 2^{128}$
AES-192	128	12	15–18	~1900–2300	0.066–0.055	$\approx 2^{192}$
AES-256	128	14	18–22	~2300–2800	0.055–0.045	$\approx 2^{256}$
AES-NI	128	10	1.0–1.5	~150–200	≈ 1	$\approx 2^{128}$
DES	64	16	70–90	~560–720	0.014–0.011	$\approx 2^{56}$
TDES	64	48	200–250	~1600–2000	0.005–0.004	$\approx 2^{112}$
EC P-256	240	2 операції	~5000–6000	$\sim 1.2 \times 10^6$	~0.00017–0.0002	$\approx 2^{128}$
EC P-384	368	2 операції	~10 000–12 000	$\sim 2.8 \times 10^6$	~0.00008–0.0001	$\approx 2^{192}$

Примітка. Для Dual_EC_DRBG кожна ітерація виконує дві еліптичні операції множення точки над базовими точками P та Q.

Як видно з таблиці 1, AES залишається найбільш ефективним варіантом для побудови CTR-DRBG. У сучасних процесорах підтримка інструкцій AES-NI знижує час генерації до 1–1.5 циклів на байт, що робить CTR-DRBG одним із найшвидших генераторів в своєму класі, який забезпечує криптографічну стійкість визначену стандартом NIST. Але слід зауважити, що з теоретичної точки зору цей клас не володіє доказовою стійкістю, а має лише обчислювальну стійкість. Доведення криптографічної стійкості генераторів CTR-DRBG базується на зведені задачі зламу DRBG до задачі зламу блокового ширу, який в свою чергу оцінюється тестуванням статистичних властивостей, а ні математичним доведенням границь розподілу. В довгострокової перспективі це означає, що у разі зниження стійкості цього шифру або появі нового методу криптоаналізу під загрозу підпадають всі побудовані на його основі криптоалгоритми. Для усунення цього недоліку виникає потреба в розробці нового криптопримітиву, як це було в ситуації з алгоритмом DES. В алгоритмі AES, на відміну від DES, розробники вже намагалися деякі перетворення зробити доказово стійкими.

У зв'язку з цим, в NIST SP 800-90A була зроблена спроба отримати доказово стійку схему генерації ПВП на основі перетворень в групі точок еліптичної кривої, для якої, нажаль, з часом були знайдені недоліки [12]. Враховуючи, що процес знаходження уразливостей в математичних конструкціях є повільним, іноді це займає роки, на практиці для оперативної оцінки уразливостей алгоритмів DRBG використовують одну з методик тестування статистичних властивостей (статистичної безпеки): DIEHARD, CRYPT-S, RIPE, NIST STS. Як правило, перевага віддається стандартизованій методиці NIST STS [13-14].

Оцінка статистичних властивостей DRBG пакетом NIST Statistical Test Suite v2.1.2

Оцінювання статистичних властивостей псевдовипадкових послідовностей, згенерованих генераторами DRBG, виконано за допомогою пакета NIST Statistical Test Suite v2.1.2, який реалізує 15 базових статистичних тестів, визначених стандартом NIST SP 800-22. Для кожного алгоритму було згенеровано 100 незалежних бінарних послідовностей довжиною 1 000 000 біт. Перевірку проводили при рівні значущості $\alpha = 0.01$. Відповідно до вимог NIST, мінімальний рівень проходження тестів становить не менше 96 % для основних тестів і від 49 % до 69 % для тестів Random Excursions та Random Excursions Variant, залежно від кількості доступних траєкторій. Кожна згенерована послідовність оцінювалася за критерієм p-value, що дозволяє визначити статистичну відповідність розподілу бітів гіпотезі справжньої випадковості. Проходження тесту фіксувалося за умови p-value $\geq \alpha$, що свідчить про відсутність статистично значущих відхилень від рівномірного розподілу.

На діаграмах (рис. 1–10) по горизонтальній осі подано індекси тестів (Test Index), а по вертикальній – кількість послідовностей, що успішно пройшли тестування (Proportion of Passing Sequences).

Експериментальні дослідження проводилися на апаратній платформі Apple MacBook Pro (16-inch, 2021) з такими параметрами:

- процесор: Apple M1 Pro;
- оперативна пам'ять: 16 ГБ;
- операційна система: macOS Tahoe версії 26.1.

Сумарний та середній час генерації для кожного генератора наведено в таблиці 2.

Таблиця 2

Час генерації псевдовипадкових послідовностей для різних реалізацій DRBG-алгоритмів

Генератор	Загальний час генерації 100 послідовностей	Середній час генерації 1 послідовності
CTR_DRBG (DES)	13.837 с	0.138 с
CTR_DRBG (TDES)	40.304 с	0.403 с
CTR_DRBG (AES-256)	5.227 с	0.052 с
HASH_DRBG (SHA-1)	0.596 с	0.006 с

Генератор	Загальний час генерації 100 послідовностей	Середній час генерації 1 послідовності
HASH_DRBG (SHA-256)	0.384 с	0.004 с
HASH_DRBG (SHA-512)	0.227 с	0.002 с
HMAC_DRBG (SHA-1)	2.827 с	0.028 с
HMAC_DRBG (SHA-256)	1.712 с	0.017 с
HMAC_DRBG (SHA-512)	0.932 с	0.009 с
Dual_EC_DRBG (P-256)	20 хв 36 с	12.37 с
Dual_EC_DRBG (P-384)	35 хв 2 с	21.02 с

Отримані результати свідчать, що Dual_EC_DRBG характеризується найбільшою обчислювальною складністю через еліптичні операції, тоді як HASH_DRBG на основі SHA512 демонструє найвищу швидкодію. CTR-DRBG (AES256) та HMAC-DRBG (SHA256) забезпечують оптимальний баланс між продуктивністю та криптографічною стійкістю, що робить їх доцільними для практичного застосування у сучасних безпекових системах.

Для оцінки продуктивності генерації псевдовипадкових послідовностей було проведено порівняльний аналіз різних реалізацій алгоритмів DRBG. Вимірювання виконувалися на 64-бітній архітектурі з використанням метрики cycles per byte (cpb), що дозволило кількісно оцінити обчислювальні витрати кожного алгоритму. У таблиці 3 наведено показники швидкодії. Дані дозволяють порівняти ефективність симетричних (CTR_DRBG, HASH_DRBG, HMAC_DRBG) та еліптичних (Dual_EC_DRBG) підходів.

Таблиця 3

Оцінка продуктивності генераторів псевдовипадкових послідовностей (DRBG)

Генератор	Cycles / byte (cpb)	Оцінка швидкодії (1/cpb)
CTR_DRBG (DES)	70–90	0.014–0.011
CTR_DRBG (TDES)	200–250	0.005–0.004
CTR_DRBG (AES-256)	18–22	0.055–0.045
HASH_DRBG (SHA-1)	~22–28	~0.045–0.036
HASH_DRBG (SHA-256)	~12–16	~0.083–0.063
HASH_DRBG (SHA-512)	~9–11	~0.11–0.09
HMAC_DRBG (SHA-1)	~80–100	~0.012–0.010
HMAC_DRBG (SHA-256)	~60–70	~0.017–0.014
HMAC_DRBG (SHA-512)	~45–55	~0.022–0.018
Dual_EC_DRBG (P-256)	5 000–6 000	0.00020–0.00017
Dual_EC_DRBG (P-384)	10 000–12 000	0.00010–0.00008

За даними проведеного аналізу бачимо, що генератори на основі симетричних алгоритмів мають значно вищу швидкодію завдяки меншій обчислювальній складності. Натомість, реалізації Dual_EC_DRBG на еліптичних кривих, забезпечують вищу криптостійкість, проте мають найменшу продуктивність через складність операцій множення точок на кривій.

Результати тестування CTR_DRBG

Результати проведеного статистичного тестування показали, що генератор CTR-DRBG на основі DES успішно пройшов усі базові тести пакета NIST STS, а p-значення перебували в межах 0.05–0.96.

Незначне зниження спостерігалося лише в тесті Non-Overlapping Template, проте пропорція проходження залишалася в межах норми. Це підтверджує коректність формування послідовностей, однак через обмежену довжину ключа (56 біт) алгоритм DES не відповідає сучасним вимогам криптографічної стійкості і може використовуватись лише для демонстраційних цілей, що підтверджує недосконаліть цього алгоритму.

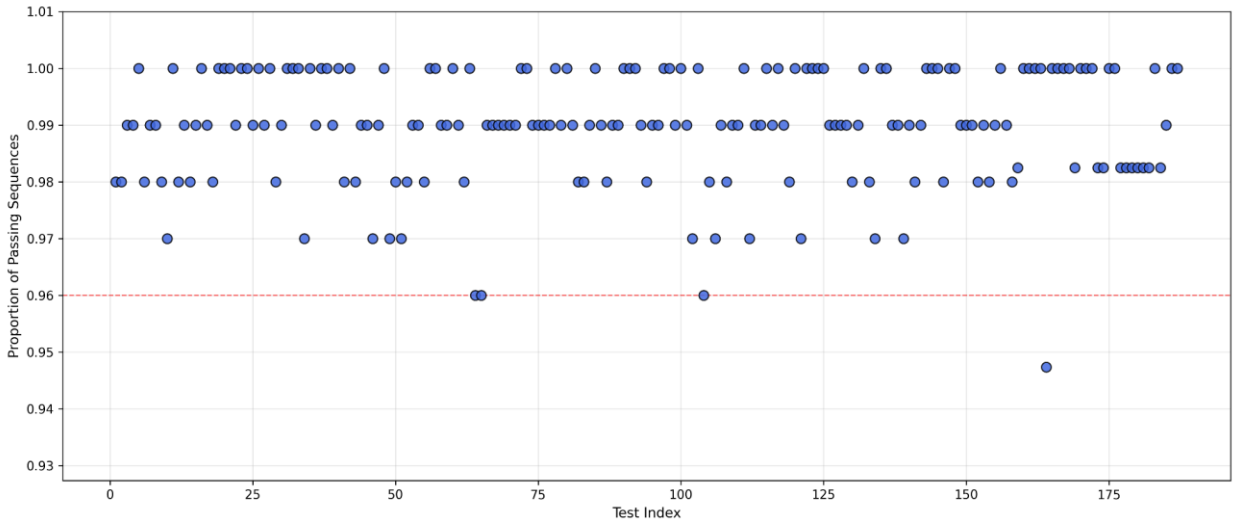

Рис. 1. Результати статистичного оцінювання генератора CTR_DRBG (на основі DES) за допомогою NIST Statistical Test Suite v2.1.2

Тестування CTR-DRBG, реалізованого з використанням Triple DES (TDES), показало рівномірний розподіл p-значень у межах 0.1–0.95. Тести Frequency, Runs, Cumulative Sums і FFT засвідчили стабільність, а для Random Excursions та Random Excursions Variant зафіксовано проходження понад 70 з 73 послідовностей, що перевищує мінімально допустимий поріг. Генератор формує статистично якісні послідовності, однак поступається за швидкодією через потрійне шифрування і має схожі на DES недоліки щодо криптографічної стійкості.

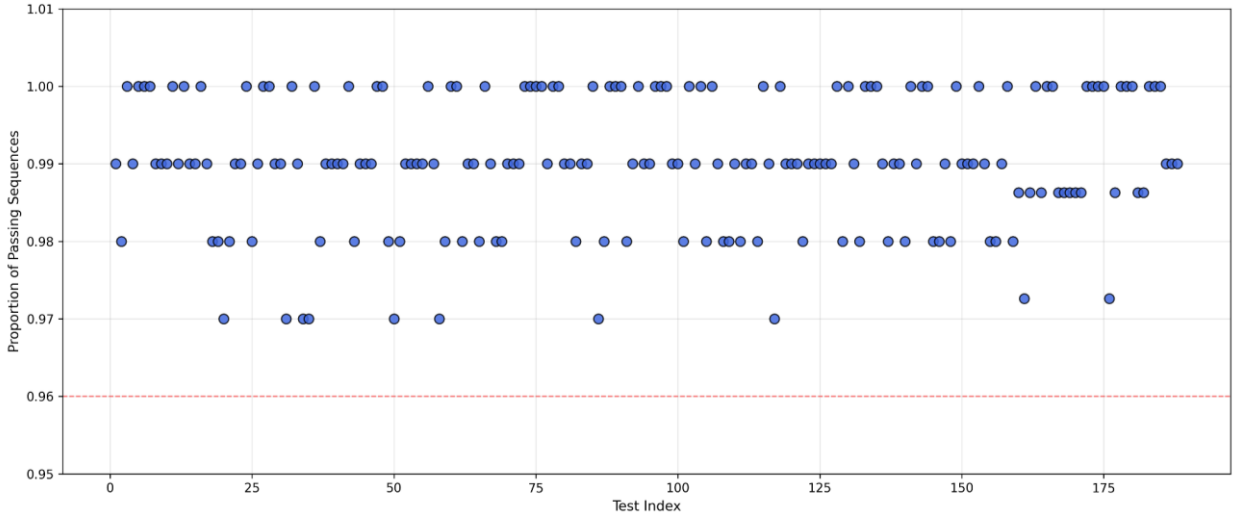

Рис. 2. Результати статистичного оцінювання генератора CTR_DRBG (на основі TDES) за допомогою NIST Statistical Test Suite v2.1.2

Перевагою є підвищена стійкість ($\approx 2^{112}$), за рахунок лише збільшення довжини ключової послідовності, а недоліком – зниження швидкодії через потрійне шифрування.

CTR-DRBG, побудований на основі AES-256, продемонстрував найкращі результати серед усіх реалізацій. Усі статистичні тести пройдено зі 100 % успішністю, *p*-значення рівномірно розподілені в межах 0.17–0.97. Тести Approximate Entropy, Serial і Linear Complexity не виявили відхилень, що підтверджує високу ентропію й однорідність згенерованих послідовностей. Це відповідає вимогам стандартів NIST SP 800-22 та NIST SP 800-90A Rev. 1.

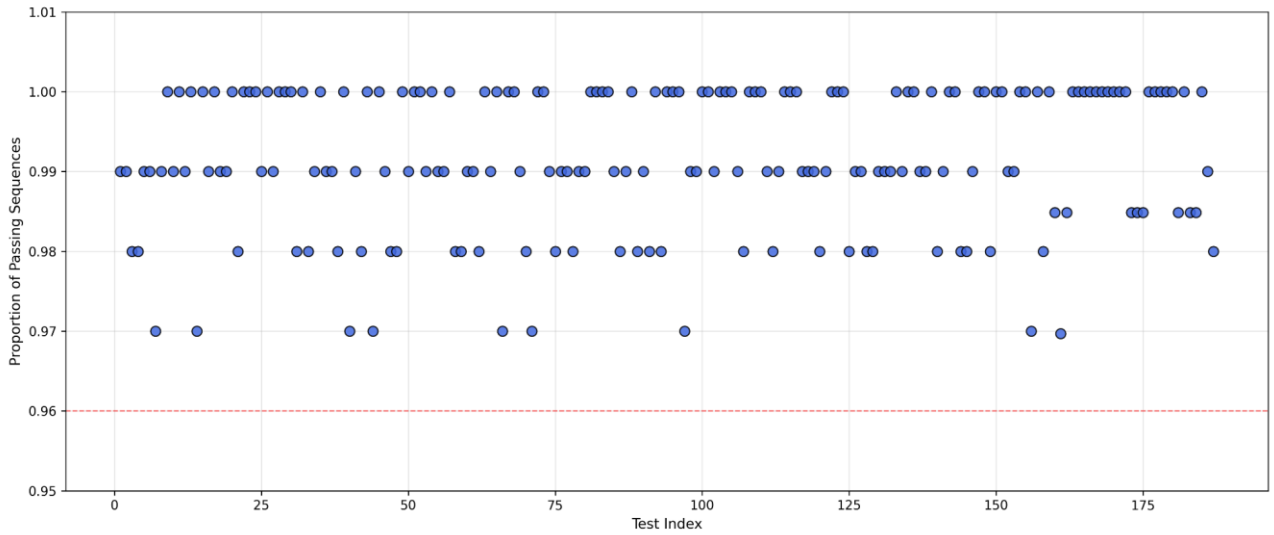

Рис. 3. Результати статистичного оцінювання генератора CTR_DRBG (на основі AES) за допомогою NIST Statistical Test Suite v2.1.2

Алгоритм забезпечує максимальну ентропію, рівномірність вихідних даних і найвищу криптографічну стійкість ($\sim 2^{256}$).

Узагальнені результати свідчать, що всі досліджувані реалізації CTR-DRBG – на основі DES, TDES та AES – формують статистично випадкові послідовності, які відповідають критеріям NIST SP 800-22. Найкращі показники продемонстрував CTR-DRBG(AES) зі стандарту NIST SP 800-90A Rev. 1, який поєднує високу швидкодію, максимальну ентропію та криптографічну стійкість, тоді як реалізації на базі DES і TDES є менш ефективними та не відповідають сучасним вимогам практичної безпеки.

Результати тестування HASH_DRBG

Результати статистичного тестування показали, що генератор HASH_DRBG, реалізований на основі SHA-1, формує послідовності з рівномірним розподілом p-значень і високою пропорцією проходження базових тестів пакета NIST STS. Це підтверджує відсутність статистично значущих відхилень та випадковість згенерованих даних (рис. 4).

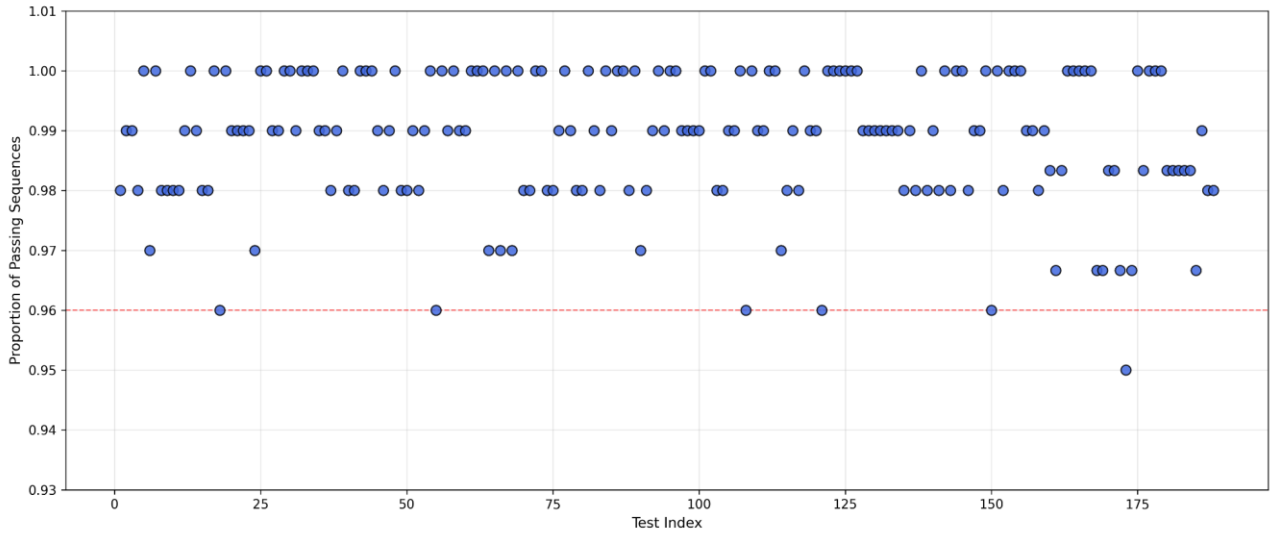

Рис. 4. Результати статистичного оцінювання генератора HASH_DRBG (на основі SHA1) за допомогою NIST Statistical Test Suite v2.1.2

Алгоритм забезпечує, в цілому, задовільні статистичні властивості, однак використання SHA1 на сьогодні не забезпечує достатній рівень стійкості до колізій геш-функцій, в зв’язку з чим рекомендовано до використання алгоритми не гірше за SHA256.

Тестування HASH_DRBG на основі SHA-256 показало рівномірний розподіл p-значень і пропорцію проходження, що відповідає вимогам стандарту NIST SP 800-22. Усі тести отримали задовільні статистичні властивості без відхилень, що свідчить про придатність алгоритму для практичного використання у криптографічних системах (рис. 5).

Переваги – достатня статистична безпека генератора, достатня криптографічна стійкість без явних недоліків.

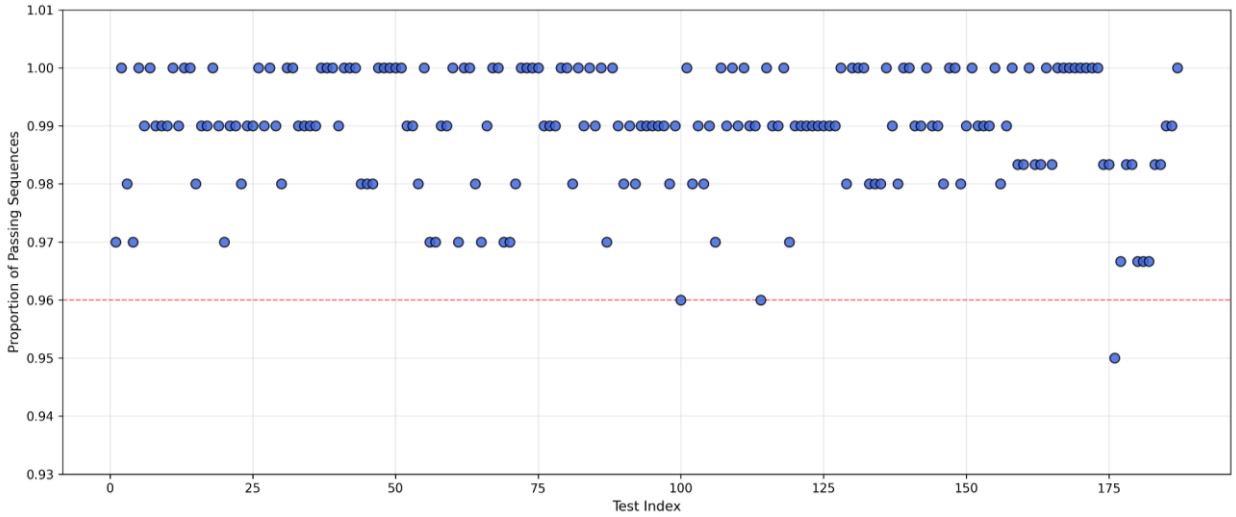

Рис. 5. Результати статистичного оцінювання генератора HASH_DRBG (на основі SHA256) за допомогою NIST Statistical Test Suite v2.1.2

Для HASH_DRBG на основі SHA512 отримано найвищій рівень статистичної безпеки серед усіх протестованих реалізацій: *p*-значення розподілені рівномірно в межах допустимих значень, а частка успішного проходження тестів перевищує мінімальні пороги (0.96 для 100 зразків і 0.49 для 52 зразків). Це підтверджує повну відповідність послідовностей критеріям випадковості та непередбачуваності (рис. 6).

Алгоритм демонструє максимальну статистичну безпеку і криптографічну стійкість, проте має підвищені обчислювальні витрати порівняно з SHA256.

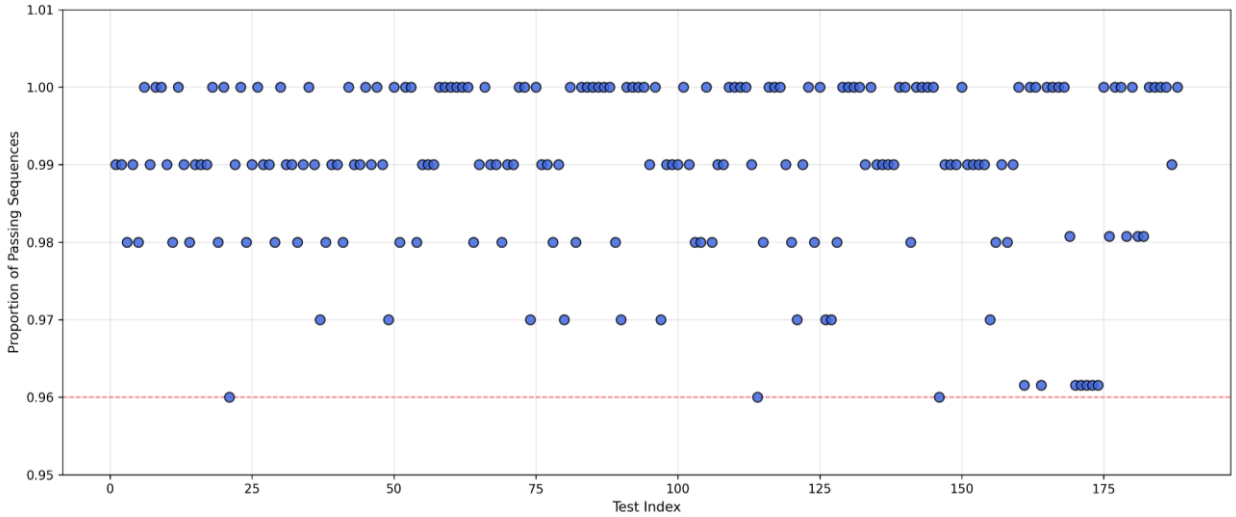

Рис. 6. Результати статистичного оцінювання генератора HASH_DRBG (на основі SHA512) за допомогою NIST Statistical Test Suite v2.1.2.

Узагальнюючи результати, наведені на рисунках 4–6, можна зробити висновок, що всі протестовані реалізації HASH_DRBG забезпечують статистично випадкові, рівномірні та непередбачувані послідовності, які відповідають вимогам стандартів NIST SP 800-22 та NIST SP 800-90A Rev. 1. Найкращий баланс між швидкодією та рівнем стійкості продемонстрував HASH_DRBG(SHA-256), тоді як SHA-512 характеризується максимальною стійкістю, а SHA1 поступається через застарілий алгоритм гешування.

Результати тестування HMAC_DRBG

Результати узагальненого тестування показано на рисунку 7, де подано перевірку рівномірності p-значень та частки послідовностей, що успішно пройшли кожен із тестів. Отримані значення розподілені в межах допустимого інтервалу [0;1] без ознак систематичних відхилень, а пропорції проходження перевищують мінімальні пороги, визначені методикою NIST STS. Це свідчить про відсутність статистичних аномалій у згенерованих даних.

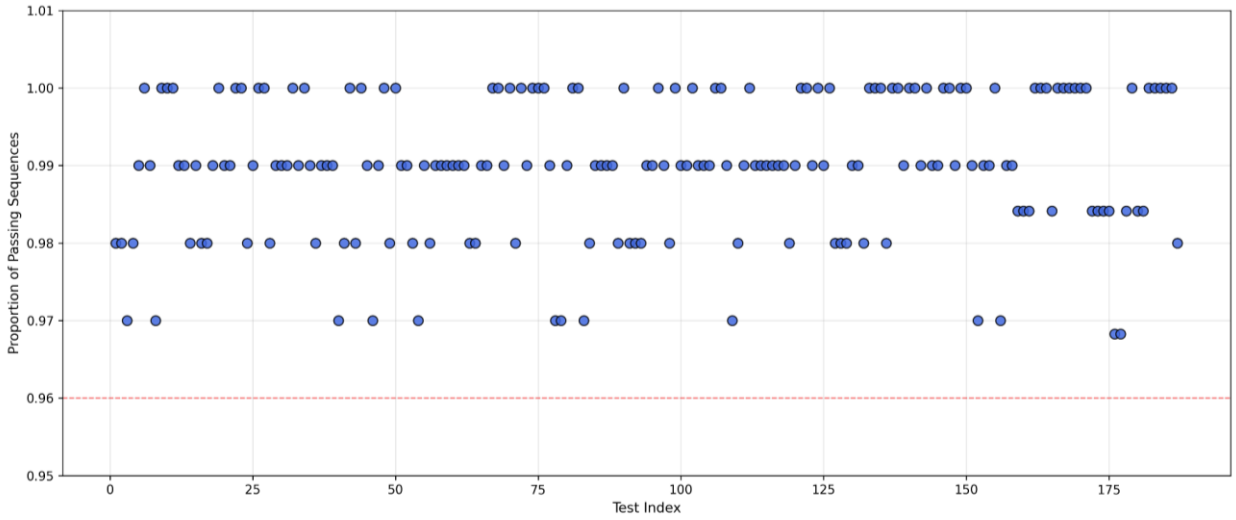

Рис. 7. Результати статистичного оцінювання генератора HMAC_DRBG (на основі SHA1) за допомогою NIST Statistical Test Suite v2.1.2

Отримано рівномірний розподіл *p*-значень і повне проходження тестів; недолік – використання застарілої хеш-функції SHA1.

Згідно з результатами тестування, представленими на рисунку 8, реалізація HMAC DRBG на основі SHA256 демонструє аналогічно високу статистичну якість: *p*-значення рівномірно розподілені, усі тести пройдено успішно, а пропорції проходження відповідають вимогам стандарту NIST SP 800-22. Це підтверджує надійність генерації псевдовипадкових послідовностей для криптографічних систем, що потребують високої ентропії та передбачуваної стійкості.

Алгоритм забезпечує високу ентропію та рівномірність вихідних даних; рекомендований для практичного застосування.

На основі результатів, наведених на рисунках 7–8, можна зробити висновок, що обидві реалізації HMAC_DRBG – на базі SHA-1 та SHA-256 – формують статистично випадкові та рівномірно розподілені послідовності, які відповідають критеріям випадковості, визначеним стандартом NIST SP 800-22. При цьому SHA256 забезпечує вищу криптографічну стійкість і є більш доцільним для сучасних систем криптографічного захисту інформації.

Результати тестування Dual_EC_DRBG

Статистичне оцінювання генератора Dual_EC_DRBG, реалізованого на еліптичних кривих P-256 та P-384, показало відповідність вимогам стандарту NIST SP 800-22. Для реалізації на кривій P-256 усі основні тести пакета NIST STS успішно пройдено: p-значення розподілені рівномірно в межах 0.004–0.98, а частка проходження перевищує мінімально

допустимий поріг (96 % для 100 послідовностей). Незначні відхилення спостерігались у тестах Non-Overlapping Template, однак вони не вплинули на загальну оцінку випадковості (рис. 9).

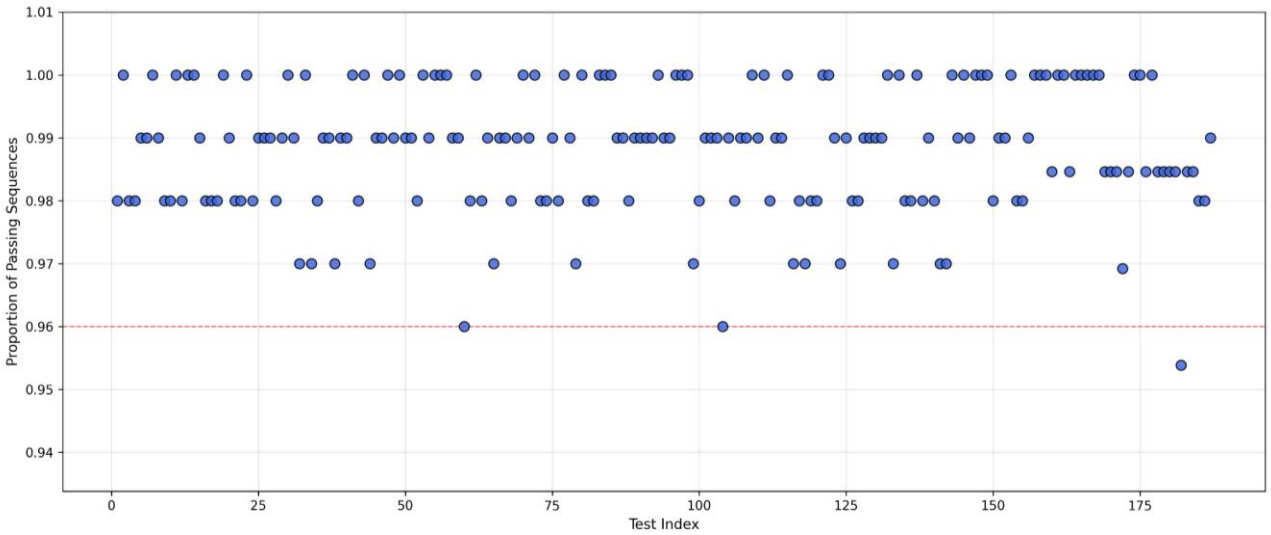

Рис. 8. Результати статистичного оцінювання генератора HMAC DRBG (на основі SHA256) за допомогою NIST Statistical Test Suite v2.1.2

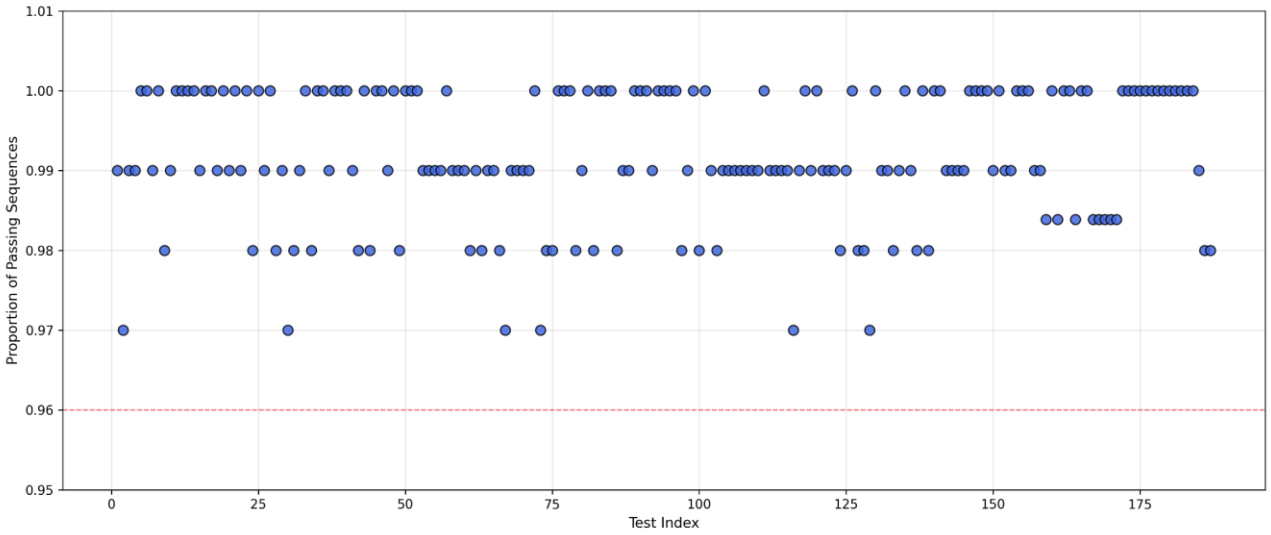

Рис. 9. Результати статистичного оцінювання генератора Dual_EC_DRBG (256 біт) за допомогою NIST Statistical Test Suite v2.1.2

Перевагою генератора є висока статистична якість та відсутність систематичних аномалій, а недоліком – значна обчислювальна складність процесу генерації.

Для реалізації на кривій P-384 отримано аналогічно високі показники випадковості: *p*-значення рівномірно розподілені в діапазоні 0.004–0.99, усі базові тести пройдено з часткою успіху понад 97 %. Додаткові тести Random Excursions та Random Excursions Variant підтвердили відсутність статистично значущих відхилень, що засвідчує правильність роботи генератора (рис. 10).

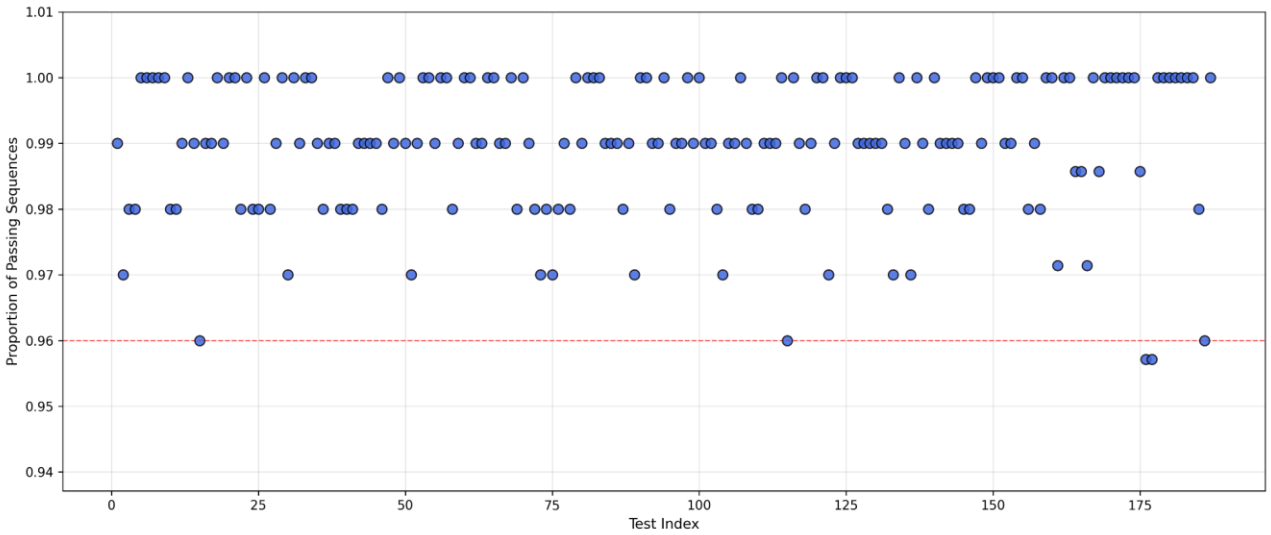

Рис. 10. Результати статистичного оцінювання генератора Dual_EC_DRBG (384 біт) за допомогою NIST Statistical Test Suite v2.1.2

Генератор характеризується рівномірним розподілом, високою ентропією та стабільністю результатів, однак має низьку швидкодію й значні часові витрати через обчислення на еліптичних кривих.

Узагальнюючи, Dual_EC_DRBG демонструє найвищу статистичну якість серед протестованих генераторів, проте має найнижчу продуктивність, що обмежує його практичне застосування у високошвидкісних системах.

Висновки

Таким чином, оцінки статистичної безпеки отримані для таких генераторів ПВП як CTR_DRBG (AES), CTR_DRBG (DES), CTR_DRBG (TDES), HASH_DRBG (SHA256), HASH_DRBG (SHA384), HASH_DRBG (SHA512), HMAC_DRBG (SHA1), HMAC_DRBG (SHA-256), Dual_EC_DRBG (P-256), Dual_EC_DRBG (P-384) показали перевагу генераторів ПВП на основі перетворень в групі точок еліптичної кривої, а саме генератор на основі еліптичних кривих Dual_EC_DRBG (256 біт) дозволив отримати псевдовипадкові послідовності 97 % яких пройшли всі тести NIST STS. Однак цей клас генераторів програє за швидкодією класу CTR_DRBG. Так, для генерації 10^8 бітів генератор Dual_EC_DRBG (P-256) витрачає 49.46 [c], Dual_EC_DRBG (P-384) – 84.09 [c], порівняно з CTR_DRBG (AES-256) – 5.227 [c] та HASH_DRBG (SHA-256) – 0.384 [c] відповідно.

Серед усіх генераторів ПВП, що досліджувалися, найкращій за швидкодією виявився лінійний генератор псевдовипадвоких властивостей PCG з показником 0.25–0.67 [1/cpb] та LFSR з показником 0.5 [1/cpb], але стійкість цього класу генераторів не задовольняє вимоги стандарту NIST SP 800-90A і не може використовуватися для захисту конфіденційної інформації. Найкращу оцінку обчислювальної швидкодії генераторів DRBG в класі генераторів CTR_DRBG отримав генератор CTR_DRBG(AES128) з показником 0.08–0.066 [1/cpb], але слід зауважити щодо цей тип генераторів на основі блокових шифрів не забезпечує доведену криптографічну стійкість, як це дозволяють зробити алгоритми на основі факторизації цілих чисел, дискретного логарифмування в простому полі, в групі точок еліптичної кривої або в ізогеніях еліптичної кривої.

Таким чином, процес вибору генераторів DRBG для реальних криптографічних додатків є складним та потребуючим комплексного підходу до вибору між максимальною криптографічною стійкістю та порівняльною якістю криптографічних послуг за причиною невеликої швидкодії криптоперетворень та якісними криптографічними послугами з відносно невеликим рівнем криптографічної стійкості генераторів ПВП.

Рішенням цього протиріччя є наступні наукові дослідження, а саме розробка нових методів генерації ПВП стійких до квантового криптоаналізу до повного переходу на постквантові криптосистеми, які планується впроваджувати в різноманітні сучасні технології такі як блокчейн, смартміcто, системи з використанням штучного інтелекту та інші системи, що потребують конфіденційності та автентичності даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. S. Coretti, Y. Dodis, H. Karthikeyan, and S. Tessaro. Seedless fruit is the sweetest: Random number generation, revisited. In Annual International Cryptology Conference, pages 205–234. Springer, 2019.

2. G. Bertoni, J. Daemen, S. Hoffert, M. Peeters, G. Van Assche, R. Van Keer, and B. Viguier. TurboSHAKE. Cryptology ePrint Archive, 2023.

3. John Kelsey, Stefan Lucks, Stephan Müller. XDRBG: A Proposed Deterministic Random Bit Generator Based on Any XOF. March 1, 2024

4. Woohyuk Chung, Seongha Hwang, Hwigyeom Kim, Jooyoung Lee. Enhancing Provable Security and Efficiency of Permutation-based DRBGs. Korea Advanced Institute of Science and Technology. A major revision of an IACR publication in CRYPTO 2025.

5. Josef Pieprzyk, Marcin Pawłowski, Paweł Morawiecki, Arash Mahboubi, Jarek Duda & Seyit. Pseudorandom bit generation with asymmetric numeral systems. International Journal of Information Security. Volume 24, article number 82, (2025).

6. Kelsey J., Ferguson N. Cryptographic Random Number Generation: Design, Implementation, and Evaluation // IEEE Security & Privacy. 2005. Vol. 3(2). P. 28–38.

7. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators (NIST SP 800-90A Rev. 1). Gaithersburg: NIST, 2015.

8. Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. Hoboken: Wiley, 2010.

9. Shannon C. E. A Mathematical Theory of Communication // Bell System Technical Journal. 1948. Vol. 27. P. 379–423, 623–656.

10. Eastlake D., Schiller J., Crocker S. Randomness Requirements for Security. RFC 4086, IETF, June 2005.

11. National Institute of Standards and Technology. FIPS PUB 140-3: Security Requirements for Cryptographic Modules. Gaithersburg: NIST, 2019.

12. Daniel R. L. Brown & Kristian Gjøsteen. A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator. Advances in Cryptology - CRYPTO 2007. P. 466–481.

13. Rukhin A. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (SP 800-22 rev.1a). NIST, 2010.

14. BSI. TR-02102-1: Cryptographic Mechanisms – Recommendations and Key Lengths. Bonn: Federal Office for Information Security (BSI), 2023.

15. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. New York: John Wiley & Sons, 1996. 784 p.

16. Чевардін В. Є. Методи побудови генераторів псевдовипадкових послідовностей на основі ізоморфних перетворень еліптичних кривих : дисертація доктора технічних наук : 05.13.21 – Системи захисту інформації / Чевардін Владислав Євгенійович ; Харків. нац. ун-т ім. В. Н. Каразіна. Харків, 2017. 340 с. Державний реєстр № 0518U000308.