УДК 004.312.056.55

# ОЦІНКА ЕНТРОПІЇ ТА ФРАКТАЛЬНИХ ВЛАСТИВОСТЕЙ ПСЕВДОВИПАДКОВИХ ГЕНЕРАТОРІВ ЧИСЕЛ ДЛЯ ШИФРУВАННЯ

Львов Р.А.
e-mail: rostyslav.lvov@nure.ua
Науковий керівник – к. ф.-м. н., доц. Онищенко А.А.
Харківський національний університет радіоелектроніки, каф. Фізики
м. Харків, Україна

This work is devoted to the evaluation of pseudorandom number generators in the field of cryptography, in particular their entropy and fractal properties. The study proposed a hybrid generation algorithm that combines a linear congruent method with material sources of microcontroller randomness - ADC thermal noise and uninitialized SRAM memory states. Shannon entropy and minimal entropy were used to estimate the unpredictability coefficient. Fractal analysis, in particular the calculation of the Hearst indicator, is given special attention to identify hidden patterns in the data structure. The hybrid algorithm was compared with its base models using the NIST SP 800-22 test suite for statistical validation. The results obtained suggest that the combination of physical noise and the linear congruent method provides a balanced approach to safety and computational speed. This approach is effective for microcontrollers, which are weak and provide a reliable basis for secure data transmission in IoT networks.

Стрімкий розвиток цифровізації у всіх сферах людської діяльності сприяє масовому впровадженню Інтернету речей (IoT), бездротових сенсорних мереж та смарт-систем. Всі вони потребують безпеки, яка критично залежить від надійності генераторів випадкових чисел (ГВЧ), що, в свою чергу, є базою для формування криптографічних ключів. Складність проявляється в тому, що апаратні генератори справжніх випадкових чисел (ГВЧ) використовують джерела ентропії у вигляді складних та непередбачуваних природних явищ (наприклад, тепловий шум, квантові ефекти або використання фонового випромінювання лічильника Гейгера). Ці варіанти є надто комплексними та дорогими для застосування у промислових масштабах. Це спричиняє гостру необхідність у пошуку доступніших джерел ентропії, які можна було б раціонально використовувати на будь-яких мікроконтролерах. Вирішенням цієї ситуації є створення гібридних детермінованих генераторів (ДГВП), які користуються легкими математичними алгоритмами (зокрема, лінійним конгруентним методом), а початкове значення для відліку («зерно») можна отримати із доступних фізичних процесів самого мікроконтролера, таких як шум аналого-цифрового перетворювача (АЦП) та станів неініціліазованої оперативної пам’яті (SRAM). Для того, щоб перевірити криптографічну стійкість даних генераторів недостатньо лише теоретичних припущень

необхідне складне оцінювання рівня їхньої непередбачуваності та схованих закономірностей з використанням мір ентропії, фрактального аналізу та стандартизованих наборів статистичних тестів.

Для практичної реалізації гібридного генератора (на прикладі мікроконтролера ATmega328p) початкове значення формується з двох незалежних джерел. Першим джерелом є тепловий шум непідключених контактів аналого-цифрового перетворювача (АЦП). Оскільки найбільше ентропії містять саме молодші біти зчитаного значення, для їх виділення застосовується побітова маска (наприклад, 0b00000011). Після цього біти циклічно накопичуються у буфер. Другим джерелом «зерна» є стан неініціалізованої оперативної пам'яті (SRAM). Після подачі живлення вона заповнюється особливим випадковим чином. Тому отримані з обох джерел буфери ентропії перемішуються за допомогою логічної операції XOR ($\oplus$). Таким чином, утворюється надійне криптографічне початкове значення («зерно»).

Отримана апаратна ентропія слугує як початковий стан ($X_0$) для програмного розширення ключа за допомогою лінійного конгруентного методу (LCG). Обчислення наступних псевдовипадкових чисел $X_{n+1}$ здійснюється за рекурентною формулою

$$X_{n+1} = (aX_n + c)\ mod\ m, \tag{1}$$

де m – модуль $(m > 0)$, a – множник $(0 < a < m)$, c – приріст $(0 \le c < m)$.

Використання отриманого «зерна» усуває головний недолік цього методу – детерміновану передбачуваність.

Для математичного обґрунтування передбачуваності знегерованої цим алгоритмом послідовності застосовується ентропія Шеннона. Даний показник вказує середню кількість інформації на один біт та дозволяє виявляти відхилення від рівномірного розподілу нулів та одиниць.

Для бінарної послідовності ентропія Шеннона обчислюється за формулою виду

$$H = -\sum_{i=1}^{n} p_i p_i. \tag{2}$$

Але висока ентропія не виключає прихованих структурних повторень, тому додатково застосовується фрактальний аналіз де $p_i$ – ймовірність появи відповідного символу (тобто 0 або 1). За ідеальних умов генератор повинен наближатися до значення $H \approx 1$, що буде показником високої інформаційної складності.

Проте для справжньої криптографії критичною є мінімальна ентропія, що визначає стійкість ключа до вгадування, в найгіршому, для захисту, сценарії, та тестування NIST SP 800-22.

Формула мінімальної ентропії:

$$H_\infty = -(p_i)\,. \tag{3}$$

Для цього методу бінарна послідовність перетворюється на траєкторію «випадкового блукання» (random walk) за певним правилом

$$X_i = 2\varepsilon_i - 1, \quad (4)$$

де формуються накопичені суми виду

$$S_k = \sum X_i. \quad (5)$$

Обчислений для цієї траєкторії фрактальний показник Херста $H \approx 0{,}5$ саме доводить відсутність довгострокової пам'яті. Остаточна перевірка випадковості блукання та відсутності прихованих закономірностей здійснюється набором із 15 тестів NIST SP 800-22.

Послідовність визнається криптостійкою, якщо для кожного з перерахованих тестів обчислене $P - value \geq 0.01$, що підтверджує ймовірність її істинної випадковості на рівні 99 %.

Список використаних джерел:

1. Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J., Vo S., Bassham L. E. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Gaithersburg : NIST, 2010. 131 p. (NIST Special Publication 800-22 Rev. 1a).

URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf (дата звернення: 03.03.2026).

2. O. V. Lazorenko, A. A. Onishchenko, I. A. Taranova, M. A. Udovenko. Peculiarities of Hurst exponent estimation for natural physical processes // Journal of V. N. Karazìn Kharkiv National University. Series Physics. Iss. 40, 2024, 7–14. https://doi.org/10.26565/2222-5617-2023-40-01

3. Zolfaghari B., Bibak K., Koshiba T. The Odyssey of Entropy: Cryptography // Entropy. 2022. Vol. 24, No. 2. Art. 266. URL: https://doi.org/10.3390/e24020266 (дата звернення: 03.03.2026).

4. Черненко С. О., Остроухов О. В. Метод оцінювання ентропії псевдовипадкових послідовностей на основі фрактального аналізу. Захист інформації. 2023. Т. 25, № 4. С. 191–203.

5. Гайдур Г. І., Остроухов В. В. Аналіз властивостей генераторів псевдовипадкових чисел для систем критичного призначення. Системи обробки інформації. 2024. Вип. 1 (141). С. 141–152.