УДК 004.3, 004.421.5, 004.056.5

Остапець Д. О., к.т.н., доцент
Панін Д. В., магістрант
Пірогов Д. А., магістрант
Український державний університет науки і технологій

ОГЛЯД ДЖЕРЕЛ ЕНТРОПІЇ ДЛЯ ГЕНЕРУВАННЯ ВИПАДКОВИХ ЧИСЕЛ

Генерування випадкових послідовностей чисел виступає ключовим інструментарієм в сучасних інформаційних технологіях, що інтегруються в різноманітні галузі. За допомогою випадкових чисел реалізується велика кількість задач, таких як тестування алгоритмів і систем, імітаційне моделювання, задачі чисельного аналізу, захисту інформації, криптографії та багато інших. При цьому дуже важливо використовувати якісні генератори випадкових чисел, оскільки від цього залежить якість розв'язуваних задач.

Відомо два основних підходи отримання випадкової послідовності чисел: генерування псевдовипадкових чисел (pseudorandom numbers, PRN) за допомогою спеціальних алгоритмів або таблиць та використання спеціальних апаратних пристроїв, що генерують істинні випадкові числа (true random numbers, TRN) [1].

Псевдовипадкові послідовності чисел, на відміну від істинно випадкових послідовностей, генеруються за допомогою детермінованих алгоритмів на основі заданого початкового значення (зерно, seed). Це зумовлює повну відтворюваність результату при ідентичних параметрах ініціалізації та наявність певного періоду циклічності [2]. Натомість функціонування генераторів істинно випадкових чисел (TRNG) базується на апаратній оцифровці стохастичних фізичних процесів (шумів), отриманих з джерел ентропії [3]. Отримане значення надалі використовується або як випадкова число, або як зерно для ініціалізації інших генераторів [1].

Джерело ентропії – це фізичне джерело інформації, вихідний сигнал якого або виглядає випадковим, або стає випадковим після застосування процесу «відіблювання». Відбілюванням називають процес перетворення необроблених даних з неповною ентропією на дані зі 100% ентропією на біт [4]. Джерела ентропії TRNG поділяються на дві категорії: фізичні джерела та нефізичні джерела [5].

Високий рівень природної ентропії забезпечується спектром фізичних явищ, що продукують випадкові сигнали: від мікроскопічних квантових та теплових шумів до макроскопічних процесів, таких як

атмосферні завади та ядерний розпад [1]. Для практичної реалізації TRNG на основі природних явищ необхідне обладнання (АЦП, підсилювачі, детектори), яке перетворює аналоговий шум у бітову послідовність, придатну для ініціалізації генератора.

Нефізичні джерела шуму використовують дані API, дані оперативної пам'яті, системний час або дані натискання клавіатури, руху миші, для генерації випадковості [3] або дані з акселерометра, гіроскопа та магнітометра [6] або дані з вбудованих камер девайсів, камер відеозапису [4]. Такі джерела простіші у впровадженні, адже вимагають виключно програмних засобів для трансформації системних даних у послідовність бітів. Недолік залежності цих джерел від зовнішньої активності усувається поєднанням даних із декількох джерел ентропії.

Список використаних джерел

1. D. Ostapets, V. Dziuba, P. Ivin, Hardware random numbers generator based on microcontroller. *MATEC Web of Conferences 390*, 04002. 2024. URL: https://doi.org/10.1051/matecconf/202439004002.

2. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST SP 800-90A Rev. 1. URL: http://dx.doi.org/10.6028/NIST.SP.800-90Ar1.

3. Turan M. S., Barker E., Kelsey J., McKay K. A., Baish M. L., Boyle M. Recommendation for the Entropy Sources Used for Random Bit Generation. NIST SP 800-90B. URL: https://doi.org/10.6028/NIST.SP.800-90B.

4. Hughes J. P., Gupta Y. “The Collector”: A Gigabit True Random Number Generator Using Image Sensor Noise. URL: https://wrach2019.lip6.fr/WRACH_2019_paper_2.pdf.

5. NA Lv, Chen T., Ma Y. Analysis on Entropy Sources based on Smartphone Sensors. *In 2020 the 10th International Conference on Communication and Network Security (ICCNS 2020*), Tokyo, November 27-29, Japan, 2020. 11 p. URL: https://doi.org/10.1145/3442520.3442528.

6. Остапець Д., Опрятний А. Дослідження можливості використання окремих датчиків мобільних пристроїв у якості джерела ентропії генератора випадкових чисел. *Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах»*. 2025. 82(2). С. 88–92. URL: https://doi.org/10.31891/2219-9365-2025-82-12.