https://doi.org/10.31891/2219-9365-2025-82-12
УДК 004.3, 004.421.5, 004.056.5

ОСТАПЕЦЬ Денис
Український державний університет науки і технологій
https://orcid.org/0000-0003-1778-7770
e-mail: odaua@i.ua
ОПРЯТНИЙ Артур
Український державний університет науки і технологій
https://orcid.org/0000-0001-7145-9677
e-mail: artur.opriatnyi@icloud.com

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВИКОРИСТАННЯ ОКРЕМИХ ДАТЧИКІВ МОБІЛЬНИХ ПРИСТРОЇВ У ЯКОСТІ ДЖЕРЕЛА ЕНТРОПІЇ ГЕНЕРАТОРА ВИПАДКОВИХ ЧИСЕЛ

В роботі розглядається дослідження можливості застосування датчиків акселерометру, гіроскопу та магнітометру мобільних пристроїв в якості джерел ентропії для використання в апаратних генераторах випадкових чисел. Сформульовано вимоги та проведено порівняний аналіз можливих датчиків мобільних пристроїв, обґрунтовано вибір датчиків для подальшого дослідження. Розроблено спеціальний програмно-апаратний комплекс на базі смартфону та персонального комп'ютеру для отримання даних з датчиків акселерометру, гіроскопу та магнітометру та їх подальшої обробки. Розглянуто варіанти використання від 1 до 32 молодших біт даних з кожної з трьох координат, отриманих з датчиків та їх поєднання операціями конкатенації, додавання та додавання за модулем два. Проведено експериментальне дослідження різних способів використання даних, отриманих з вибраних датчиків мобільного пристрою для генерування випадкових чисел, зроблено оцінку їх ефективності. Показано, що запропонований підхід дозволить суттєво підвищити швидкість генерування випадкових чисел.

Ключові слова: випадкові числа, джерело ентропії, датчик, мобільний пристрій, акселерометр, гіроскоп, магнітометр, тести NIST.

OSTAPETS Denys, OPRIATNYI Artur
Ukrainian State University of Science and Technologies

RESEARCH OF THE POSSIBILITY OF USING SEPARATE MOBILE DEVICE SENSORS AS A SOURCE OF ENTROPY FOR A RANDOM NUMBER GENERATOR

This paper explores the potential of utilizing the accelerometer, gyroscope, and magnetometer sensors embedded in modern mobile devices as novel entropy sources for hardware-based random number generators (RNGs). The study begins by defining the fundamental requirements for effective entropy sources, followed by a detailed comparative analysis of available mobile device sensors. Based on this analysis, specific sensors were selected for further investigation due to their responsiveness, accessibility, and variability in data output. A specialized software-hardware complex was developed, comprising a smartphone for data acquisition and a personal computer for processing and analysis. This system enables the extraction of raw sensor data and supports experimentation with different bit-level manipulations.

The research examines the use of between 1 to 32 least significant bits (LSBs) from each axis (X, Y, Z) of the selected sensors. Various methods for combining these bits—such as simple concatenation, arithmetic summation, and modulo two addition (XOR)—are implemented and analyzed. Experimental evaluations focus on the statistical quality of the generated random numbers, their compliance with standard randomness criteria, and the throughput of generation.

The findings indicate that sensor data from mobile devices can serve as viable entropy sources, significantly enhancing the performance and speed of hardware RNGs. This approach not only leverages readily available consumer technology but also offers a scalable and cost-effective solution for secure and efficient random number generation in various applications, including cryptographic systems, simulations, and secure communications.

Keywords: random numbers, source of entropy, sensor, mobile device, accelerometer, gyroscope, magnetometer, NIST tests.

Стаття надійшла до редакції / Received 16.04.2025
Прийнята до друку / Accepted 11.05.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Випадкові числа використовуються в багатьох сферах науки та техніки. Багато існуючих алгоритмів не можуть забезпечити високу якість та непередбачуваність генерованих послідовностей псевдовипадкових чисел. Основними недоліками апаратних засобів генерування послідовностей дійсно випадкових чисел є їх більш висока вартість та більш низька швидкість роботи. Для розробки генератора дійсно випадкових чисел важливе використання якісного джерела ентропії [1].

Джерело ентропії – це фізичне джерело інформації, дані з якого або здаються випадковим, або стають випадковими після застосування певного процесу фільтрації/дистиляції [2]. В представленій роботі

пропонується в якості джерела ентропії використовувати датчики мобільних пристроїв, що дозволить зменшити вартість генератора та підвищити швидкість його роботи.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою робити є дослідження ефективності застосування датчиків акселерометру, гіроскопу та магнітометру мобільних пристроїв в якості джерел ентропії для використання в генераторах випадкових чисел. В роботі, відповідно до мети, поставлені такі задачі: порівняний аналіз можливих датчиків мобільних пристроїв, обґрунтування та вибір датчиків для подальшого дослідження; розробка спеціалізованого програмно-апаратного комплексу для отримання даних з вибраних датчиків мобільного пристрою та їх обробки; експериментальне дослідження різних способів використання даних, отриманих з вибраних датчиків мобільного пристрою в якості джерела ентропії та вибір найбільш ефективних.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У роботі розглядаються датчики смартфона у якості джерела ентропії.

Датчики – це пристрої, які використовуються в мобільних пристроях для виявлення різних аспектів навколишнього середовища [3]. Зараз існує достатньо багато датчиків, доступних в смартфонах, які вбудовані та допомагають функціонувати смартфону. Здебільшого ці датчики створені для проведення оцінки досвіду користувачів. Генератор випадкових чисел, який використовує датчики сучасного мобільного пристрою, здатний створювати високоякісні послідовності випадкових бітів [4]. Використання датчиків мобільних пристроїв, пристроїв IoT та вбудованих систем у якості джерел ентропії також розглядається в роботах [5 – 9].

На думку авторів, при виборі джерела ентропії для розробки генератора випадкових чисел на базі мобільного пристрою слід врахувати наступні вимоги:

- Чутливість датчика.
- Наявність датчика у більшості мобільних пристроїв.
- Швидкість оцифрування даних.
- Кількість отриманих біт за одне вимірювання.

Акселерометр, гіроскоп та магнітометр наявні майже у всіх сучасних смартфонах, є досить чутливими, а також дають можливість отримання найбільшої кількості біт тому, що фіксують зміни у трьох координатах. Інші датчики, такі як датчик освітлення та барометр фіксують лише одне значення. Тому саме акселерометр, гіроскоп та магнітометр було обрано в якості джерел ентропії для дослідження якості згенерованих випадкових послідовностей.

Для виконання досліджень розроблено спеціальний програмно-апаратний комплекс за допомогою якого можна отримувати дані з вибраних датчиків мобільного пристрою. Апаратна частина комплексу складається з комп'ютера MacBook Pro M3 та смартфона IPhone 14, обмін між якими реалізовано за протоколом TCP. Комп'ютер виконує роль сервера, його програмне забезпечення розроблене на мові Go [10] в середовищі JetBrains Goland [11]. Програмне забезпечення для мобільного пристрою розроблене на мові Dart [12] з використанням фреймворку Flutter [13] в середовищі Android Studio [14]. Приклади наборів даних, які можна отримати з використовуваних в роботі датчиків, наведено на рис. 1-3, відповідно.

```
x: 0.18052459716796876, y: 8.894503784179689, z: 4.1393421936035155
x: 0.19609222412109376, y: 8.922645263671875, z: 4.088597717285157
x: 0.16196319580078125, y: 8.918154602050782, z: 4.108955383300781
x: 0.17124389648437502, y: 8.890462188720704, z: 4.144281921386719
x: 0.22408401489257815, y: 8.895850982666015, z: 4.151167602539063
```

Рис. 1. Приклад набору даних акселерометра

```
x: 0.015908125787973404, y: -0.01739310473203659, z: 0.0044205812737345695
x: 0.009982593357563019, y: 0.011665711179375648, z: -0.0038836877793073654
x: -0.009955162182450294, y: -0.00221947836689651, z: 0.0022389194928109646
x: -0.015503591857850552, y: 0.007370031904429197, z: 0.002139317337423563
x: 0.00538464542478323, y: -0.0001536643976578489, z: 0.0004396878939587623
```

Рис. 2. Приклад набору даних гіроскопа

```
x: -128.0546875, y: 84.324462890625, z: -340.8043212890625
x: -127.80438232421875, y: 84.328369140625, z: -341.1653747558594
x: -128.00497436523438, y: 84.37646484375, z: -341.11334228515625
x: -128.17967224121094, y: 84.19140625, z: -341.33990478515625
x: -128.07577514648438, y: 84.26268005371094, z: -341.1424255371094
```

Рис. 3. Приклад набору даних магнітометра

Дані було отримано з мобільного пристрою в нерухомому стані. Як видно з рисунків, дані з датчиків мають деяку флуктуацію. Автори очікують, що чутливість даних датчиків дасть змогу використовувати їх у якості джерела ентропії для генератора випадкових чисел.

Оскільки акселерометр, гіроскоп та магнітометр вимірюють значення у трьох координатах (x, y, z), то для генерації наступних бітів послідовності авторами пропонується виконувати такі операції:

- Конкатенація молодших біт трьох координат.
- Отримання молодших біт суми трьох координат.
- Отримання молодших біт результату операції XOR трьох координат.

Для кожної з операцій пропонується отримати 1, 2, 4, 8, 16 та 32 біти. Приклади виконання обраних операцій зображені на рис. 4.

```
DEC representation:                  HEX representation:
x: 0.11960128784179688               x: 3f4a80487c2b452e
y: 8.937314758300781                 y: 4021DFE7b851eb85
z: 3.9953416442871097                z: 400ff67ae147ae2

conc 4       1110    sum 4        1110    xor 4       1110
least bits   0101    least bits   0101    least bits  0101
             0010                 0010                0010
-----------------    -----------------    ----------------
     111001010010                 0101                1001
```

Рис. 4. Приклади виконання операцій конкатенації, додавання та додавання за модулем два чотирьох молодших біт

В результаті аналізу отриманих даних з датчиків гіроскопу та магнітометру зроблено висновок, що в цьому випадку доцільно використовувати не молодші біти значень координат, а виконати їх арифметичний зсув на 32 біта вправо, оскільки молодша половина біт у цих датчиків майже завжди складалась виключно з нулів.

Таким чином, в роботі прийнято рішення провести серію експериментів з отримання випадкових чисел за зазначеними вище принципами та визначити їх ефективність. Для проведення експериментів отримано 10000 значень з кожного з трьох датчиків.

Під час отримання кожного значення датчику, всі три координати конвертувались у цілі числа, що представляли собою бітову послідовність координат по стандарту IEEE 754 [15].

Усі згенеровані послідовності перевірено набором тестів NIST [2]. Результати тестів представлені у табл. 1 – 3 для кожного з датчиків.

Тести в табл. 1 – 3 пронумеровано за їх порядком у кейсі NIST [2]:

- Тест №1 – Frequency (Monobit) Test.
- Тест №2 – Frequency Test within a Block.
- Тест №3 – Runs Test.
- Тест №4 – Test for the Longest Run of Ones in a Block.
- Тест №5 – Binary Matrix Rank Test.
- Тест №6 – Discrete Fourier Transform (Spectral) Test.
- Тест №7 – Non-overlapping Template Matching Test.
- Тест №11 – Serial Test.
- Тест №12 – Approximate Entropy Test.
- Тест №13 – Cumulative Sums (Cusum) Test.

Тести 8, 9, 10, 14 та 15 було виключено з результатів, оскільки згенерована випадкова послідовності не відповідає вимогам довжини даних тестів.

Таблиця 1.

Результати тестів NIST для послідовностей, згенерованих за допомогою акселерометра

Операція	Кількість біт	Тести NIST									
		№1	№2	№3	№4	№5	№6	№7	№11	№12	№13
conc x,y,z	1	+	+	+	+	+	+	+	+	-	+
conc x,y,z	2	+	+	+	+	+	+	+	+	-	+
conc x,y,z	4	+	+	+	+	+	+	-	+	-	+
conc x,y,z	8	+	+	+	-	+	+	-	-	-	+
conc x,y,z	16	-	+	-	-	-	-	+	-	-	-
conc x,y,z	32	-	-	+	-	-	-	+	-	-	-
x+y+z	1	-	-	-	-	+	-	-	-	-	-
x+y+z	2	-	-	-	-	+	-	-	-	-	-
x+y+z	4	-	-	-	-	+	+	+	+	-	-
x+y+z	8	-	+	-	-	+	+	-	-	-	-
x+y+z	16	-	-	-	-	-	-	+	-	-	-
x+y+z	32	-	-	-	-	-	-	+	-	-	-
x^y^z	1	+	+	+	+	+	+	+	+	+	+
x^y^z	2	+	+	+	+	+	+	+	+	+	+
x^y^z	4	+	+	+	+	+	+	+	+	+	+
x^y^z	8	+	+	+	+	+	+	+	+	-	+
x^y^z	16	+	+	+	+	+	+	+	-	-	+
x^y^z	32	+	+	+	-	-	-	+	-	-	+

Таблиця 2.

Результати тестів NIST для послідовностей, згенерованих за допомогою гіроскопа

Операція	Кількість біт	Тести NIST									
		№1	№2	№3	№4	№5	№6	№7	№11	№12	№13
conc x,y,z	1	+	+	+	+	+	+	+	+	+	+
conc x,y,z	2	+	+	+	+	+	+	+	+	+	+
conc x,y,z	4	+	+	+	+	+	+	+	+	+	+
conc x,y,z	8	+	+	+	+	+	+	+	+	+	+
conc x,y,z	16	+	+	+	+	+	+	+	+	-	+
conc x,y,z	32	-	-	-	-	-	-	+	-	-	-
x+y+z	1	+	+	+	+	+	+	+	+	+	+
x+y+z	2	+	+	+	+	+	+	+	+	+	+
x+y+z	4	+	+	+	+	+	+	+	+	-	+
x+y+z	8	+	+	+	+	+	+	+	+	+	+
x+y+z	16	+	+	+	+	+	+	+	+	-	+
x+y+z	32	-	-	-	-	-	-	+	-	-	-
x^y^z	1	+	+	+	+	+	+	+	+	+	+
x^y^z	2	+	+	+	+	+	+	+	+	-	+
x^y^z	4	+	+	+	+	+	+	+	+	+	+
x^y^z	8	+	+	+	+	+	+	+	+	-	+
x^y^z	16	+	+	+	+	+	+	+	+	+	+
x^y^z	32	-	-	-	-	-	-	+	-	-	-

Таблиця 3.

Результати тестів NIST для послідовностей, згенерованих за допомогою магнітометра

Операція	Кількість біт	Тести NIST									
		№1	№2	№3	№4	№5	№6	№7	№11	№12	№13
conc x,y,z	1	+	+	+	+	+	+	+	+	-	+
conc x,y,z	2	+	+	+	+	+	+	+	+	+	+
conc x,y,z	4	+	+	+	+	+	+	+	+	+	+
conc x,y,z	8	+	+	+	+	+	+	-	+	-	+
conc x,y,z	16	-	-	-	-	+	-	+	+	-	-
conc x,y,z	32	-	-	-	-	-	-	+	-	-	-
x+y+z	1	+	+	+	+	+	+	+	+	+	+
x+y+z	2	+	+	+	+	+	+	+	+	+	+
x+y+z	4	+	+	+	+	+	+	+	+	+	+
x+y+z	8	+	+	+	+	+	+	+	+	+	+
x+y+z	16	-	-	-	+	-	-	+	-	-	-
x+y+z	32	-	-	-	-	-	-	+	-	-	-
x^y^z	1	+	+	+	+	+	+	+	+	-	+
x^y^z	2	+	+	+	+	+	+	+	+	-	+
x^y^z	4	+	+	+	+	+	+	+	+	-	+
x^y^z	8	+	+	+	+	+	+	+	+	+	+
x^y^z	16	-	-	-	-	+	+	+	+	-	-
x^y^z	32	-	-	-	+	-	-	+	-	-	-

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

В основному, при побудові апаратних генераторів випадкових чисел, за одне звернення до джерела шумового сигналу (джерела ентропії) або після його оцифровування, отримують лише один біт генерованого випадкового числа. В таких випадках використовується або молодший біт двійкового коду оцифрованого значення шумового сигналу, або двійкова ознака його порівняння з деякім пороговим значенням.

Як видно з даних таблиць 1 – 3, найбільш ефективними способами отримання випадкових чисел виявились:

- для акселерометра – операція XOR для 4 молодших біт;
- для гіроскопа – операція XOR для 16 молодших біт;
- для магнітометра – операція додавання та XOR для 8 молодших біт.

Таким чином, запропонований підхід дозволить суттєво підвищити швидкість генерування випадкових чисел в порівнянні з класичним підходом.

В подальшому, окремого дослідження потребують більш довгі послідовності біт, що згенеровані за запропонованим підходом.

References

1. D. Ostapets, V. Dziuba, P. Ivin, Hardware random numbers generator based on microcontroller, MATEC Web of Conferences 390, 04002 (2024). doi: 10.1051/matecconf/202439004002.
2. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf.
3. Sensors Overview. URL: https://developer.android.com/develop/sensors-and-location/sensors/sensors_overview.
4. Introduction to Randomness and Random Numbers. URL: https://www.random.org/randomness/.
5. C. Hennebert, H. Hossayni, C. Lauradoux, Entropy harvesting from physical sensors, Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks (2013) 149–154. doi:10.1145/2462096.2462122.
6. J. Voris, N. Saxena, T. Halevi, Accelerometers and Randomness: Perfect Together, Fourth ACM Conference on Wireless Network Security (2011) 115–126. doi: 10.1145/1998412.1998433.
7. A. Suciu, D. Lebu, K. Marton, Unpredictable Random Number Generator Based on Mobile Sensors, IEEE International Conference on Intelligent Computer Communication and Processing (2011). doi: 10.1109/ICCP.2011.6047913.
8. M. P. Pawlowski, A. Jara, M. Ogorzalek, A. J. Jara, Harvesting Entropy for Random Number Generation for Internet of Things Constrained Devices Using On-Board Sensors (2015) doi: 10.3390/s151026838.
9. S.M. Cho, E. Hong, S.H. Seo, Random Number Generator Using Sensors for Drone, IEEE Access (2020) doi: 10.1109/ACCESS.2020.2972958.
10. Build simple, secure, scalable systems with Go. URL: https://go.dev.
11. Goland – Go Productive. URL: https://www.jetbrains.com/go/.
12. Paint your UI to life. URL: https://dart.dev.
13. Build for any screen. URL: https://flutter.dev.
14. Android Studio. URL: https://developer.android.com/studio.
15. IEEE Standard for Binary Floating-Point Arithmetic (IEEE Std 754-1985). URL: https://www.ime.unicamp.br/~biloti/download/ieee_754-1985.pdf.