УДК 681.324.067

С.В. ПОПЕРЕШНЯК
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ІНТЕГРАЦІЯ ФІЗИЧНИХ СЕНСОРІВ У ГЕНЕРАЦІЮ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

У статті представлено підхід до побудови генератора псевдовипадкових чисел на основі фізичних сенсорів, який є перспективним напрямом для забезпечення надійності та безпеки в різних галузях, як-от криптографія, Інтернет речей, ігрова індустрія та кіберфізичні системи. Сенсори різних типів, зокрема датчики температури, звуку, світла, гіроскопи та магнітометри, демонструють високу надійність як джерела ентропії завдяки природним флуктуаціям та непередбачуваним характеристикам, які вони реєструють. Фізичні явища, що вимірюються цими датчиками, генерують значний рівень непередбачуваності, що є критичним для побудови надійних генераторів псевдовипадкових чисел, стійких до передбачуваності. У роботі детально описано процес цифрової обробки сигналів від сенсорів, який містить кілька етапів: фільтрацію шумів, нормалізацію сигналів, квантування та бінаризацію для отримання випадкових бітів. Фільтрація шумів забезпечує усунення небажаних перешкод, нормалізація дає змогу привести сигнали до єдиного масштабу, а квантування та бінаризація забезпечують конвертацію аналогових сигналів у дискретну форму, придатну для генерації псевдовипадкових чисел. Такий підхід гарантує високу якість випадкових бітів, що підтверджується результатами криптографічних і статистичних тестів, які були проведені для оцінки випадковості та стійкості до передбачуваності отриманих чисел. Результати дослідження показали, що генератори на основі фізичних сенсорів можуть ефективно забезпечувати високий рівень випадковості, достатній для застосувань, що вимагають високої безпеки. Зокрема, підхід може бути корисним у криптографії для генерації ключів шифрування, у системах IoT для захисту конфіденційності даних, у кіберфізичних системах для забезпечення надійної роботи, а також в ігровій індустрії для створення непередбачуваних ігрових сценаріїв. У статті також наведено практичні рекомендації щодо вибору сенсорів залежно від умов використання та вимог до обладнання. Наприклад, для мобільних пристроїв можуть бути ефективними датчики руху (гіроскопи, акселерометри), тоді як для стаціонарних систем доречно використовувати датчики температури або звуку. Ураховано також аспекти інтеграції сенсорних генераторів у різноманітні системи, зокрема способи їх поєднання з наявними інфраструктурами та вимоги до апаратного забезпечення. Отже, розглянутий підхід до побудови генератора псевдовипадкових чисел на основі фізичних сенсорів є перспективним напрямом, який може суттєво підвищити надійність і безпеку сучасних систем. Запропоновані методи обробки сигналів і рекомендації щодо вибору сенсорів сприяють ефективному впровадженню генераторів у різних сферах, забезпечуючи високий рівень ентропії та захист від можливих атак.

Ключові слова: ентропія, генератор псевдовипадкових чисел, Інтернет речей, математична модель, сенсори, цифрова обробка даних.

S.V. POPERESHNYAK
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

INTEGRATION OF PHYSICAL SENSORS IN THE GENERATION OF PSEUDO-RANDOM NUMBERS

The paper presents an approach to building a pseudo-random number generator (PRNG) based on physical sensors, which is a promising direction for ensuring reliability and security in various fields such as cryptography, Internet of Things (IoT), gaming industry, and cyber-physical systems. Sensors of various types, including temperature, sound, light, gyroscopes, and magnetometers, show high reliability as sources of entropy due to the natural fluctuations and unpredictable characteristics they register. The physical phenomena measured by these sensors generate a significant level of unpredictability, which is critical for building reliable, predictability-resistant pseudo-random number generators. The work describes in detail the process of digital processing of signals from sensors, which includes several stages: noise filtering, signal normalization, quantization and binarization to obtain random bits. Noise filtering ensures the elimination of unwanted interference, normalization allows you to bring signals to a single scale, and quantization and binarization ensure the conversion of analog signals into a discrete form suitable for generating pseudorandom numbers. This approach guarantees the high quality of random bits, which is confirmed by the results of cryptographic and statistical tests that were conducted to assess the randomness and predictability of the received numbers. The research results showed that generators based on physical sensors can effectively provide a high degree of randomness sufficient for applications requiring high security. In particular, the approach can be useful in cryptography to generate encryption

https://doi.org/10.32782/mathematical-modelling/2024-7-2-16

keys, in IoT systems to protect data privacy, in cyber-physical systems to ensure reliable operation, and in the gaming industry to create unpredictable game scenarios. The article also provides practical recommendations for the selection of sensors depending on the conditions of use and equipment requirements. For example, motion sensors (gyroscopes, accelerometers) can be effective for mobile devices, while for stationary systems it is appropriate to use temperature or sound sensors. Aspects of integrating sensor generators into various systems are also considered, including how they can be combined with existing infrastructures and hardware requirements. Thus, the considered approach to building a generator of pseudo-random numbers based on physical sensors is a promising direction that can significantly increase the reliability and security of modern systems. The proposed methods of signal processing and recommendations for the selection of sensors contribute to the effective implementation of generators in various fields, ensuring a high level of entropy and protection against possible attacks.

Key words: entropy, pseudorandom number generator, Internet of Things, mathematical model, sensors, digital data processing.

Постановка проблеми

У сучасному світі псевдовипадкові числа відіграють ключову роль у багатьох сферах, включно з криптографією, комп'ютерним моделюванням, статистичними методами та ігровою індустрією. Однак традиційні алгоритмічні генератори псевдовипадкових чисел мають певні обмеження, зокрема повторюваність та передбачуваність, що може стати серйозною проблемою для додатків, які вимагають високого рівня безпеки та ентропії [1; 2].

З огляду на це, виникає нагальна потреба створити більш надійні джерела ентропії. Одним із перспективних підходів є використання датчиків для генерації псевдовипадкових чисел, які можуть використовувати природні випадкові флуктуації фізичних процесів [3; 4]. Датчики, що вимірюють температуру, шум, рух, освітлення та інші параметри навколишнього середовища, забезпечують високий рівень ентропії, що робить їх привабливими для побудови апаратних генераторів псевдовипадкових чисел.

Стаття, присвячена одному з методів побудови генератора псевдовипадкових чисел на основі датчиків, є актуальною з кількох причин:

1. Зростання потреби в безпеці. З кожним роком зростають вимоги до криптографічної безпеки в мережах та інформаційних системах. Використання надійних генераторів випадкових чисел є критичним для захисту даних.
2. Проблеми передбачуваності традиційних алгоритмів. Алгоритмічні генератори (ПВЧ) мають обмежену ентропію, що робить їх вразливими до атак. Фізичні процеси, які використовують датчики, мають значно більший потенціал для непередбачуваності.
3. Розвиток апаратних рішень. З удосконаленням апаратного забезпечення, зокрема вбудованих систем та інтернету речей (IoT), зростає потреба в компактних і надійних генераторах псевдовипадкових чисел, що можна інтегрувати в пристрої з обмеженими ресурсами.
4. Інновації в науково-технічному прогресі. Використання датчиків для генерації псевдовипадкових чисел створює нові можливості для наукових досліджень і розробки нових технологічних рішень у різних галузях, як-от телекомунікації, автоматика, комп'ютерні науки та інші.

Отже, ця стаття сприяє розвитку методів генерації надійних псевдовипадкових чисел на основі апаратного забезпечення, пропонуючи інноваційний підхід до розв'язання проблеми передбачуваності й повторюваності чисел, що генеруються традиційними алгоритмами.

Постановка завдання

Генерація псевдовипадкових чисел є важливим складником багатьох сучасних систем, включно з криптографією, комп'ютерним моделюванням, ігровою індустрією та науковими дослідженнями. Традиційні алгоритмічні генератори псевдовипадкових чисел мають певні обмеження, пов'язані з їх передбачуваністю та низьким рівнем ентропії, що може бути критичним у випадках, коли потрібно забезпечити високу криптографічну безпеку [5; 6]. Постає питання про пошук альтернативних підходів, які б допомагали підвищити непередбачуваність

https://doi.org/10.32782/mathematical-modelling/2024-7-2-16

і випадковість чисел. Одним із таких перспективних методів є використання датчиків для генерації псевдовипадкових чисел на основі фізичних процесів. Однак залишається відкритою проблема розробки математичної моделі та технічних рішень для ефективної реалізації цього підходу.

Мета дослідження

Мета статті – розробити альтернативні шляхи до побудови генератора псевдовипадкових чисел на основі датчиків, що використовують випадкові фізичні явища для забезпечення високого рівня ентропії і непередбачуваності. У статті розглядаються методи вимірювання фізичних процесів, аналіз їх випадковості, математична обробка даних для отримання бітів випадкової послідовності та оцінка якості отриманих псевдовипадкових чисел.

Завдання статті

1. Аналіз джерел ентропії, доступних через датчики. Огляд можливих типів датчиків (температури, акустичних, світлових тощо), які можуть бути використані для генерації випадкових сигналів.

2. Розробка математичної моделі генерації псевдовипадкових чисел на основі вимірювань датчиків. Вивчення процесів нормалізації даних, квантування та обробки сигналів для перетворення фізичних вимірювань у послідовність бітів.

3. Реалізація цифрової обробки даних для забезпечення випадковості. Визначення методів фільтрації шумів, зменшення впливу детермінованих компонентів та побудова процесу отримання бітів.

4. Оцінка якості отриманих псевдовипадкових чисел. Проведення тестів на випадковість, як-от криптографічні та статистичні тести, для перевірки надійності та непередбачуваності генератора.

5. Розробка рекомендацій щодо практичної реалізації генератора на основі датчиків. Обговорення апаратних вимог та потенційних сценаріїв застосування таких генераторів у різних галузях.

Отже, у статті викладено концепцію побудови генератора псевдовипадкових чисел на основі фізичних явищ, що вимірюються датчиками, з використанням методів математичної обробки та оцінки випадковості отриманих чисел.

Аналіз останніх досліджень та публікацій

Інтеграція фізичних сенсорів у генерацію псевдовипадкових чисел є активно досліджуваною темою, особливо в контексті мобільних та IoT-пристроїв. Сенсори, як-от акселерометри, гіроскопи, мікрофони та камери, можуть забезпечувати джерела ентропії, використовуючи випадкові фізичні явища для генерації справжніх випадкових чисел. Це особливо важливо для криптографічних додатків, де необхідні надійні джерела випадковості.

Дослідження показують, що різні типи сенсорів мають різні рівні ентропії [6; 7]. Наприклад, акселерометри демонструють достатню кількість ентропії навіть за відсутності руху, тоді як сенсори з високою інерційністю, як-от барометричні датчики, мають нижчий рівень ентропії. Крім того, методи поєднання даних з кількох сенсорів, як-от гіроскоп й акселерометр, дають змогу покращити якість випадкових чисел завдяки використанню їх комбінації для отримання додаткової ентропії.

Сучасні підходи до генерації випадкових чисел на основі сенсорів також передбачають використання методів фільтрації та обробки даних, наприклад, застосування технік згортки або бітового XOR, щоб покращити якість результатів. Наприклад, у дослідженнях для дронів ураховували відмінності в даних сенсорів залежно від стану пристрою (у польоті чи на землі), що допомагало оптимізувати генерацію випадкових чисел [3].

https://doi.org/10.32782/mathematical-modelling/2024-7-2-16

Загалом, використання фізичних сенсорів для генерації випадкових чисел продовжує розвиватися, забезпечуючи потенціал для більш надійних криптографічних систем та покращення безпеки мобільних і вбудованих пристроїв.

Виклад основного матеріалу дослідження

І. Аналіз джерел ентропії, доступних через датчики

Ентропія в контексті генерації псевдовипадкових чисел означає кількість інформації або випадковості, яку можна отримати з фізичного процесу. Датчики можуть вимірювати різні фізичні величини, які за своєю природою містять значний рівень випадковості. Ці величини можуть бути використані як джерела ентропії для генерації випадкових сигналів [8–10]. Нижче наведено огляд найбільш поширених типів датчиків, які можуть бути використані для цього завдання.

1. Температурні датчики

Температурні датчики вимірюють температуру навколишнього середовища або певних компонентів. Хоча зміни температури часто відбуваються поступово, на мікрорівні температура може флуктуювати через зовнішні фактори, які є випадковими.

Джерело ентропії:

• теплові флуктуації: Зміни температури, викликані як внутрішніми процесами (наприклад, робота пристрою), так і зовнішніми умовами (атмосферні впливи), можуть мати випадкову компоненту;

• тепловий шум (джонсонівський шум): Він виникає через випадкові рухи заряджених частинок у провідниках. Цей вид шуму може бути використаний для генерації випадкових бітів.

Переваги:

• простота використання;

• довговічність і стабільність у різних середовищах.

Недоліки:

• низька частота флуктуацій у макроскопічних умовах;

• потрібна додаткова обробка для отримання стабільних випадкових бітів.

2. Акустичні датчики (мікрофони)

Акустичні датчики використовують для вимірювання звукових коливань у повітрі або рідинах. Звукові хвилі містять значний рівень шуму, який можна використовувати як джерело ентропії.

Джерело ентропії:

• акустичний шум: у навколишньому середовищі завжди наявні звукові коливання, які важко передбачити. Наприклад, у фоновому шумі можуть бути присутні шум вітру, руху людей, робота пристроїв тощо;

• когерентність сигналу: можна виявити дрібні випадкові коливання навіть у відносно тихому середовищі.

Переваги:

• постійний доступ до непередбачуваних коливань;

• висока частота змін сигналу.

Недоліки:

• можливі проблеми зі стабільністю в дуже тихих умовах;

• залежність від рівня навколишнього шуму.

3. Світлові датчики (фотодіоди, фототранзистори)

Світлові датчики використовують для вимірювання рівня освітленості. Випадкові коливання в інтенсивності світла, навіть у стабільному середовищі, можуть бути джерелом ентропії.

https://doi.org/10.32782/mathematical-modelling/2024-7-2-16

Джерело ентропії:

• квантові коливання інтенсивності світла: світло, що сприймається датчиком, має випадкові квантові коливання через природу фотонів, особливо в низькоінтенсивних умовах (темрява або дуже слабке освітлення);

• зовнішні фактори: зміни в освітленні через природні фактори, як-от рух хмар, зміна куту сонячних променів або інші випадкові процеси, що змінюють рівень освітленості.

Переваги:

• висока частота флуктуацій у змінних середовищах;

• доступність фотодіодів та інших світлових сенсорів.

Недоліки:

• у контрольованому середовищі з постійним освітленням ентропія може бути низькою;

• потрібно мати змінне джерело світла для отримання достатньої кількості випадкових змін.

4. Гіроскопи та акселерометри

Ці датчики використовують для вимірювання орієнтації та руху пристрою. Вони дуже чутливі до найменших змін руху, навіть якщо пристрій перебуває в умовах відносного спокою.

Джерело ентропії:

• мікрофлуктуації руху: гіроскопи й акселерометри можуть реєструвати дрібні рухи або вібрації, викликані випадковими процесами, наприклад, мікровібраціями навколишнього середовища або вібраціями внутрішніх компонентів;

• непередбачувані коливання: ці датчики можуть вловлювати непомітні для ока мікрорухи, спричинені, наприклад, зміною положення або випадковими коливаннями.

Переваги:

• висока чутливість до коливань;

• швидке реагування на зміни.

Недоліки:

• у стаціонарних системах, де немає руху, ентропія може бути обмеженою;

• може вимагати високої частоти опитування для ефективного використання ентропії.

5. Магнітні датчики (магнітометри)

Магнітометри вимірюють зміни в магнітному полі навколо пристрою. Навіть в умовах відсутності видимих змін магнітного поля можуть виникати випадкові коливання, викликані мікрофлуктуаціями в середовищі.

Джерело ентропії:

• зміни магнітного поля: випадкові зміни магнітного поля можуть бути спричинені рухом магнітних об’єктів, електричними потоками або геофізичними факторами;

• квантові коливання: у певних умовах, магнітометри можуть вловлювати квантові флуктуації магнітних полів.

Переваги:

• відсутність необхідності в безпосередньому фізичному контакті або зміні положення датчика;

• постійне наявність флуктуацій у магнітному полі.

Недоліки:

• чутливість до електромагнітних перешкод;

• можлива стабільність магнітного поля в контрольованих умовах.

6. Електрохімічні датчики

Ці датчики вимірюють хімічні зміни в середовищі, наприклад рівень вологості або концентрацію певних хімічних речовин.

https://doi.org/10.32782/mathematical-modelling/2024-7-2-16

Джерело ентропії:

• випадкові хімічні реакції: у багатьох середовищах, навіть у стабільних умовах, можуть відбуватися випадкові зміни хімічного складу або концентрації;

• флуктуації вологості або газів: випадкові зміни в складі повітря або вологість можуть впливати на показники електрохімічних датчиків.

Переваги:

• висока чутливість до змін у хімічному середовищі;

• використання в спеціальних умовах (наприклад, у хімічних лабораторіях або середовищах з контрольованою атмосферою).

Недоліки:

• повільна реакція в стабільних умовах;

• залежність від зовнішніх чинників.

Датчики різних типів можуть бути використані як джерела ентропії для генерації випадкових чисел, однак їх ефективність залежить від характеру вимірюваних фізичних процесів і середовища, у якому вони функціонують. Залежно від цільової системи можна використовувати один або кілька датчиків для покращення випадковості генератора:

• температурні та світлові датчики підходять для систем із повільними змінами середовища;

• акустичні датчики та гіроскопи підходять для середовищ із високою динамікою або рухом;

• магнітні датчики та електрохімічні сенсори можуть використовуватися в специфічних середовищах або для вимірювання особливих явищ.

Різноманітність доступних датчиків дає змогу гнучко налаштовувати генератори псевдовипадкових чисел під конкретні умови або вимоги системи.

II. Реалізація цифрової обробки даних для забезпечення випадковості

Для реалізації цифрової обробки даних з метою генерації псевдовипадкових чисел на основі показників датчиків необхідно забезпечити:

1. Фільтрацію шумів.
2. Зменшення впливу детермінованих компонентів.
3. Побудову процесу квантування для отримання бітів.

Розглянемо основні етапи обробки даних (рис. 1).

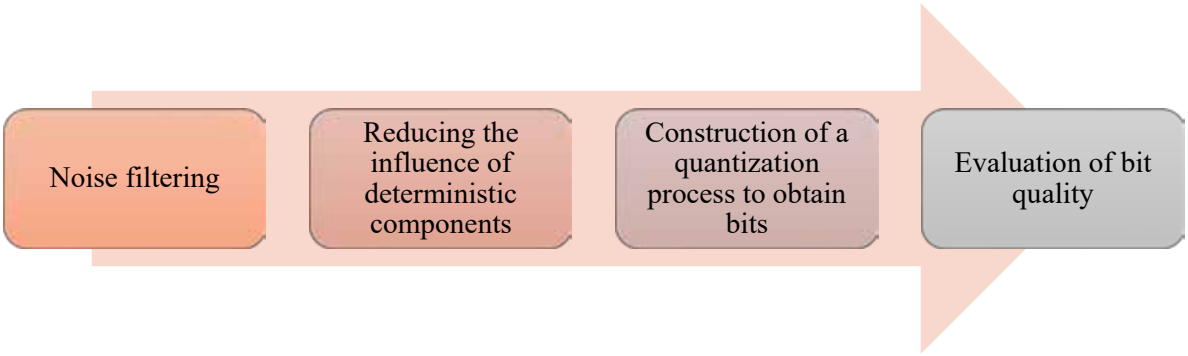

Рис. 1. Етапи обробки даних

1. Фільтрація шумів

Датчики реального світу вимірюють сигнали, що містять як корисний сигнал, так і випадкові шуми. Для виокремлення випадкової компоненти сигналу використовується фільтрація. Один із найпоширеніших підходів для фільтрації шуму – використання високочастотних фільтрів (наприклад, фільтри низьких частот), які дають змогу відсіяти довгострокові коливання (детерміновану компоненту).

https://doi.org/10.32782/mathematical-modelling/2024-7-2-16

Розглянемо способи фільтрації шумів:

• медіанний фільтр: застосовують для зменшення пікових шумів у сигналів. Він працює, обчислюючи медіану певної кількості значень у ковзному вікні розміру *n*.

Припустимо, у нас є сигнал $x(t)$, що зчитується з датчика:

$$x_{\text{filtered}}(t) = \text{median}\left(x(t-n),...,x(t+n)\right). \tag{1}$$

Цей метод дає змогу зменшити вплив аномальних значень або викидів, зберігаючи основні коливання;

• ковзне середнє: ще один спосіб згладити сигнал – обчислення середнього значення в ковзному вікні розміру w:

$$x_{\text{smooth}}(t) = \frac{1}{w}\sum_{i=t-w/2}^{t+w/2} x(i). \tag{2}$$

Така фільтрація дає змогу згладити сигнал, зменшивши вплив короткочасних флуктуацій.

2. Зменшення впливу детермінованих компонентів

Щоб виокремити дійсно випадкову частину сигналу, необхідно зменшити або повністю усунути детерміновані компоненти. Це можна зробити кількома способами:

• віднімання середнього значення: якщо детермінована компонента має стабільний тренд, її можна усунути, віднявши середнє значення сигналу:

$$x_{\text{detrended}}(t) = x(t) - \bar{x}, \tag{3}$$

де $\bar{x}$ – середнє значення сигналу за певний період часу.

• Фур'є-аналіз: Для виявлення регулярних компонент сигналу, що повторюються з певною частотою, можна застосувати **перетворення Фур'є**. Після визначення основних гармонік (детермінованих частот) можна видалити їх зі спектра, залишивши лише високочастотні флуктуації (випадковий шум).

Перетворення Фур'є для сигналу $x(t)$:

$$X(f) = \int_{-\infty}^{\infty} x(t)e^{-2\pi ift}dt. \tag{4}$$

Після перетворення сигнал можна обробляти шляхом видалення низькочастотних гармонік, що відповідають регулярним коливанням, і виконати зворотне перетворення для отримання чистого випадкового сигналу.

3. Процес отримання бітів

Після обробки сигналу необхідно перетворити його на послідовність бітів, які використовуватимуть для генерації випадкових чисел.

Алгоритм квантування:

• нормалізація сигналу: спочатку сигнал нормалізується до діапазону від 0 до 1. Припустимо, що значення сигналу перебувають у межах від $x_{\min}$ до x_{max}:

$$x_{norm}(t) = \frac{x(t) - x_{\min}}{x_{max} - x_{\min}} \tag{5}$$

https://doi.org/10.32782/mathematical-modelling/2024-7-2-16

• бінаризація сигналу: після нормалізації можна квантувати сигнал для отримання бітів. Для цього можна використовувати порогове значення, наприклад 0.5:

$$b(t)=\begin{cases}1, if\ x_{norm}(t)\geq 0.5\\ 0, if\ x_{norm}(t)<0.5\end{cases}. \tag{6}$$

Отримані біти можна зібрати в послідовність та використовувати як випадкові числа. Для побудови багаторозрядних чисел можна комбінувати кілька бітів у групи по k бітів:

$$R=\sum_{i=0}^{k-1} b(t+1)\cdot 2^i. \tag{7}$$

Це дасть змогу отримати псевдовипадкове число в діапазоні від 0 до 2^k-1.

4. Оцінка якості бітів

Після генерації бітів важливо перевірити їх на випадковість за допомогою таких методів:

• Тест Фріса (для аналізу рівномірності розподілу).

• Тест серій (для перевірки відсутності регулярних шаблонів у послідовності).

• Тест на довжину блоків нулів й одиниць (щоб перевірити, чи відсутні довгі послідовності з однакових бітів).

Реалізація цифрової обробки даних для генерації випадкових чисел із сигналів датчиків містить кілька етапів:

1. Фільтрація шумів для видалення детермінованих компонент.
2. Зменшення впливу регулярних компонент шляхом віднімання середнього або використання Фур'є-аналізу.
3. Нормалізація та бінаризація сигналу для отримання послідовності випадкових бітів.
4. Перевірка якості бітів за допомогою тестів на випадковість.

Ці методи дають змогу отримувати псевдовипадкові числа, використовуючи фізичні властивості сигналів датчиків, що значно підвищує їх непередбачуваність, як порівняти з традиційними алгоритмічними генераторами.

ІІІ. Загальна математична модель

Нехай $S(t)$ – це сигнал з датчика в момент часу t, тоді модель ГПВЧ може бути описана рівнянням:

$$R(t)=H\left(Q\left(\frac{S(t)-\min(S)}{\max(S)-\min(S)}\right)\right), \tag{8}$$

де:

• H – функція хешування або постобробки,

• $Q(x)$ – квантувальна функція, яка перетворює значення на бінарні біти.

Переваги:

1. Генерація числа базується на фізичних процесах, тому важко передбачити отримані результати.
2. Можливість використання різних типів датчиків для підвищення ентропії.

Недоліки:

1. Вимірювання можуть бути чутливими до зовнішніх умов або калібрування обладнання.
2. Потрібна додаткова обробка для отримання високоякісних псевдовипадкових чисел.

Отже, побудова генератора псевдовипадкових чисел на основі датчиків вимагає поєднання фізичних вимірів з математичною обробкою сигналу для отримання непередбачуваних значень.

https://doi.org/10.32782/mathematical-modelling/2024-7-2-16

IV. Розробка рекомендацій щодо практичної реалізації генератора псевдовипадкових чисел на основі датчиків

Для успішної реалізації генератора псевдовипадкових чисел (далі – ГПВЧ) на основі датчиків необхідно враховувати кілька апаратних вимог, що забезпечать стабільну роботу й достатню ентропію генерації випадкових чисел.

1. Вибір датчиків

Основні типи датчиків, які можуть використовувати для генерації випадкових чисел, містять:

• температурні датчики: вимірюють флуктуації температури на мікрорівні, особливо в чутливих умовах (наприклад, у системах охолодження);

• акустичні датчики: використовують мікрофони або інші пристрої для захоплення шумів у середовищі;

• світлові датчики: вимірюють зміни в освітленні або інфрачервоному спектрі, що може варіюватися навіть у контрольованих умовах;

• гіроскопи та акселерометри: можуть вимірювати невеликі коливання або рухи пристрою, що важко передбачити.

2. Продуктивність і частота збору даних

ГПВЧ на основі датчиків вимагає досить високої частоти збору даних для забезпечення стабільного потоку випадкових чисел. Типова частота опитування датчиків може варіюватися від кількох сотень герц до кількох кілогерц залежно від точності й характеристик сигналу:

• для датчиків з низькою частотою збору даних (наприклад, температурні датчики) можливо використовувати фільтрацію і накопичення даних для отримання достатньої ентропії;

• для високочастотних датчиків (акустичні або гіроскопи) можна використовувати більш прямий потік даних з мінімальною обробкою.

3. Процесорна потужність

Оскільки сигнал із датчиків часто потребує обробки (фільтрація шумів, нормалізація, бінаризація), необхідна обчислювальна потужність. Генератор може бути реалізований як:

• убудована система на мікроконтролері: для пристроїв з обмеженими ресурсами (наприклад, IoT), де енергоспоживання має бути мінімальним;

• апаратне забезпечення в серверах або безпекових модулях: тут може бути використано потужніший процесор для обробки великих обсягів даних з датчиків у режимі реального часу.

4. Енергоспоживання

ГПВЧ на основі датчиків може бути критичним у системах з обмеженим енергоспоживанням, як-от мобільні або IoT-пристрої. Рекомендації:

• використовувати датчики з низьким споживанням енергії;

• налаштувати частоту опитування датчиків відповідно до потреб конкретного додатка (зменшення частоти збору даних у випадках, коли висока ентропія не є критичною).

Для побудови генератора з високим рівнем непередбачуваності необхідно реалізувати ефективні методи обробки сигналів:

• фільтрація сигналів: застосування медіанних фільтрів або фільтрів низьких частот для видалення регулярних компонент (флуктуацій навколишнього середовища);

• квантування та бінаризація: нормалізація даних з датчиків та їх перетворення в бінарні послідовності через порогове значення;

• застосування хешування або криптографічних алгоритмів для додаткового покращення якості випадкових чисел і їх безпеки.

Розглянемо деякі потенційні сценарії застосування генераторів на основі датчиків.

1. Криптографія та безпека. Найважливіший сценарій застосування таких генераторів – це криптографія. Використання ГПВЧ на основі датчиків дає змогу значно підвищити надійність і стійкість систем безпеки за рахунок генерації більш непередбачуваних ключів:

https://doi.org/10.32782/mathematical-modelling/2024-7-2-16

• генерація криптографічних ключів для шифрування даних;

• захист від атак на псевдовипадковість: фізична природа датчиків дає змогу захиститися від передбачуваних алгоритмічних схем.

2. Інтернет речей (IoT). ГПВЧ на основі датчиків може бути інтегрований в IoT-пристрої, де важлива стійкість до зламу й забезпечення унікальності комунікаційних сесій:

• автентифікація пристроїв через криптографічні алгоритми, що використовують випадкові числа для генерації унікальних токенів;

• шифрування переданих даних для захисту конфіденційності в мережах IoT.

3. Ігрова індустрія. В ігрових додатках випадковість відіграє ключову роль у забезпеченні чесності гри та створенні непередбачуваного досвіду для користувачів. ГПВЧ на основі датчиків може використовуватися для:

• генерації випадкових подій або чисел в ігрових процесах (наприклад, в азартних іграх, симуляціях або генерації ігрових карт);

• захисту від маніпуляцій з боку гравців через використання складних фізичних процесів для генерації непередбачуваних чисел.

4. Системи моделювання й прогнозування. Генератори на основі датчиків можуть використовувати в наукових дослідженнях, де необхідна висока якість випадкових чисел:

• моделювання фізичних процесів: у середовищах, де важлива точність випадкових параметрів, наприклад, у симуляціях квантових систем або кліматичних умов;

• фінансові моделі: для випадкових змін ринку або прогнозування волатильності.

5. Кіберфізичні системи. ГПВЧ на основі датчиків може бути інтегрований у кіберфізичні системи (CPS), які поєднують фізичні компоненти і обчислювальні процеси. Приклади:

• контроль за безпекою в системах енергозабезпечення або автоматизації виробництва, де випадкові числа потрібні для забезпечення захисту від зломів або саботажу.

Перед практичною реалізацією ГПВЧ на основі датчиків необхідно провести ретельне тестування на випадковість і стійкість до атак (наприклад, [11; 12]):

• використання наборів тестів NIST для перевірки криптографічної стійкості;

• проведення статистичних тестів для оцінки рівномірності та ентропії випадкових чисел;

• сертифікація за стандартами криптографічної безпеки, щоб забезпечити відповідність міжнародним стандартам, наприклад, FIPS 140-2.

Генератори псевдовипадкових чисел на основі датчиків створюють нові можливості для застосувань, де необхідна висока непередбачуваність і надійність. Для успішної реалізації таких генераторів потрібно забезпечити правильний вибір датчиків, оптимальну обробку сигналів, низьке енергоспоживання, а також ретельне тестування та сертифікацію.

Висновки

У статті розглянуто один із перспективних шляхів побудови генератора псевдовипадкових чисел на основі фізичних сенсорів. Датчики різних типів, як-от датчики температури, звуку, світла, гіроскопи та магнітометри, були визнані надійними джерелами ентропії через їхні природні флуктуації та непередбачувані характеристики. Фізичні явища, виміряні цими датчиками, забезпечують високий рівень непередбачуваності, необхідний для побудови надійних псевдовипадкових чисел.

Розроблено метод цифрової обробки сигналів від датчиків, що містить фільтрацію шумів, нормалізацію, квантування та бінаризацію для отримання випадкових бітів. Оцінка якості отриманих чисел за допомогою криптографічних і статистичних тестів показала, що генератори на основі датчиків можуть успішно забезпечувати високий рівень випадковості й стійкості до передбачуваності.

Практичні рекомендації містять вибір відповідного типу датчика на основі конкретних умов застосування та вимог до обладнання. Генератори цього типу можуть бути ефективно

https://doi.org/10.32782/mathematical-modelling/2024-7-2-16

застосовані в галузях, де потрібна висока безпека, включно з криптографією, Інтернетом речей (IoT), ігровою індустрією та кіберфізичними системами.

Тому генерація псевдовипадкових чисел на основі фізичних датчиків є перспективним напрямом для створення надійних і безпечних генераторів, які можна інтегрувати в різноманітні системи для забезпечення високої ентропії та захисту від можливих атак.

Список використаної літератури

1. Rastoceanu F., Rughiniş R., Tranca D.-C. Lightweight cryptographic secure random number generator for IoT devices. *Proceedings of the 24th International Conference on Control Systems and Computer Science (CSCS)*, Bucharest, Romania, 2023. P. 180–185. doi: 10.1109/CSCS59211.2023.00036.
2. Parisot Bento L. M. S., Machado R. C. S. Testing and selecting lightweight pseudo-random number generators for IoT devices. *Proceedings of the IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT),* Rome, Italy, 2021. P. 715–720, doi: 10.1109/MetroInd4.0IoT51437.2021.9488454.
3. Cho S.-M., Hong E., Seo S.-H. Random Number Generator Using Sensors for Drone. *IEEE Access*, 2020. vol. 8, P. 30343–30354. doi: 10.1109/ACCESS.2020.2972958.
4. Jindal P., Singh B. RC4 Encryption-A Literature Survey. *Procedia Computer Science.* 2015. 46, P. 697–705.
5. Ruhillo. Using Smartphone Sensors to Generate Cryptographic Keys. *International Journal of Innovative Technology and Exploring Engineering*. 2020. 9, P. 1025–1029. doi: 10.35940/ijitee.C8994.029420.
6. Cotrina G., Peinado A., Ortiz A. Gaussian Pseudorandom Number Generator Based on Cyclic Rotations of Linear Feedback Shift Registers. *Sensors.* 2020. 20(7). 2103. doi:10.3390/s20072103.
7. Zia U., McCartney M., Scotney B. A novel pseudo-random number generator for IoT based on a coupled map lattice system using the generalised symmetric map. *SN Applied Sciences.* 2022. 4, p. 48. doi:10.1007/s42452-021-04919-4.
8. Florin R., Rughinis R., Ciocîrlan S.-D., Enache M. Sensor-Based Entropy Source Analysis and Validation for Use in IoT Environments, Electronics. 2021. doi:10.1173.10.3390/electronics10101173.
9. Hong S., Chang L. Sensor-Based Random Number Generator Seeding. *Access IEEE*. 2015. 3. P. 562–568.
10. Lv N., Chen T., Ma Y. Analysis on Entropy Sources based on Smartphone. *Sensors*. 2020. P. 21–31. doi:10.1145/3442520.3442528.
11. Popereshnyak S. Technique of the testing of pseudorandom sequences, *International Journal of Computing*. 2020. 19(3). P. 387–398. doi:10.47839/ijc.19.3.1888.
12. Masol V., Popereshnyak S. Joint Distribution of Some Statistics of Random Bit Sequences. *Cybernetics and Systems Analysis*. 2021. 57(1). P. 139–145. doi.org/10.1007/s10559-021-00337-x.

References

1. Rastoceanu, F., Rughiniş, R., & Tranca, D.-C. (2023). Lightweight cryptographic secure random number generator for IoT devices. *Proceedings of the 24th International Conference on Control Systems and Computer Science (CSCS)*, Bucharest, Romania. 180–185. doi: 10.1109/CSCS59211.2023.00036 [in English].
2. Parisot, Bento, L. M. S., & Machado, R. C. S. (2021). Testing and selecting lightweight pseudo-random number generators for IoT devices. *Proceedings of the IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT),* Rome, Italy. 715–720, doi: 10.1109/MetroInd4.0IoT51437.2021.9488454 [in English].

https://doi.org/10.32782/mathematical-modelling/2024-7-2-16

3. Cho, S.-M., Hong, E., & Seo, S.-H. (2020). Random Number Generator Using Sensors for Drone. *IEEE Access*. 8, 30343–30354. doi: 10.1109/ACCESS.2020.2972958 [in English].
4. Jindal, P., & Singh, B. (2015). RC4 Encryption-A Literature Survey. *Procedia Computer Science.* 46, 697–705 [in English].
5. Ruhillo. (2020). Using Smartphone Sensors to Generate Cryptographic Keys. *International Journal of Innovative Technology and Exploring Engineering*. 9, 1025–1029. doi: 10.35940/ijitee.C8994.029420 [in English].
6. Cotrina, G., Peinado, A., & Ortiz, A. (2020). Gaussian Pseudorandom Number Generator Based on Cyclic Rotations of Linear Feedback Shift Registers. *Sensors.* 20(7). 2103. doi: 10.3390/s20072103 [in English].
7. Zia, U., McCartney, M., & Scotney, B. (2022). A novel pseudo-random number generator for IoT based on a coupled map lattice system using the generalised symmetric map. *SN Applied Sciences.* 4, 48. doi: 10.1007/s42452-021-04919-4 [in English].
8. Florin, R., Rughinis, R., Ciocîrlan, S.-D., & Enache, M. (2021). Sensor-Based Entropy Source Analysis and Validation for Use in IoT Environments, Electronics. doi: 10.1173.10.3390/electronics10101173 [in English].
9. Hong, S., & Chang, L. (2015). Sensor-Based Random Number Generator Seeding. *Access IEEE*. 3, 562–568 [in English].
10. Lv, N., Chen, T., & Ma. Y. (2020). Analysis on Entropy Sources based on Smartphone. *Sensors*, 21–31. doi:10.1145/3442520.3442528 [in English].
11. Popereshnyak, S. (2020). Technique of the testing of pseudorandom sequences, *International Journal of Computing*. 19(3), 387–398. doi:10.47839/ijc.19.3.1888 [in English].
12. Masol, V., & Popereshnyak, S. (2021). Joint Distribution of Some Statistics of Random Bit Sequences. *Cybernetics and Systems Analysis*. 57(1), 139–145. doi.org/10.1007/s10559-021-00337-x [in English].

Поперешняк Світлана Володимирівна – к.ф.-м.н., доцент кафедри інформатики та програмної інженерії Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». E-mail: spopereshnayk@gmail.com, ORCID: 0000-0002-0531-9809.

Popereshnyak Svitlana Volodymyrivna – Candidate of Physical and Mathematical Sciences, Associate Professor at the Department of Informatics and Software of the National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”. E-mail: spopereshnayk@gmail.com, ORCID: 0000-0002-0531-9809.

https://doi.org/10.32782/mathematical-modelling/2024-7-2-16