

ДОСЛІДЖЕННЯ ФІЗИЧНИХ ДЖЕРЕЛ ЕНТРОПІЇ ДЛЯ АПАРАТНОЇ ГЕНЕРАЦІЇ ТА АНАЛІЗУ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Вінницький національний технічний університет

Анотація:

У доповіді досліджується фізична природа джерел ентропії, що застосовуються для побудови апаратних генераторів істинно випадкових чисел (ГІВЧ). Проаналізовано термодинамічні флуктуації електронів (тепловий шум резистора) та апаратні мікрошуми електронних компонентів як фундаментальний базис для формування абсолютно непередбачуваних послідовностей. Здійснено порівняння генераторів, побудованих на стохастичних фізичних процесах, із математичними моделями імітації випадковості (адитивні генератори Фібоначчі).

Ключові слова: тепловий шум, фізична ентропія, апаратний генератор випадкових чисел, ГІВЧ, флуктуації, статистичні тести.

Abstract:

The report investigates the physical nature of entropy sources used to build hardware true random number generators (TRNG). The thermodynamic fluctuations of electrons (resistor thermal noise) and hardware micro-noises of electronic components are analyzed as a fundamental basis for forming absolutely unpredictable sequences. A comparison is made between generators based on stochastic physical processes and mathematical models simulating randomness (additive Fibonacci generators).

Keywords: thermal noise, physical entropy, hardware random number generator, TRNG, fluctuations, statistical tests.

Вступ

Створення масивів випадкових даних є критично важливим завданням для сучасних методів моделювання фізичних систем, статистичного аналізу та криптографії. Фундаментальна проблема генерування таких даних полягає у тому, що класичні обчислювальні системи працюють за принципом строгого детермінізму. Будь-який математичний алгоритм здатен генерувати лише псевдовипадкові числа (ГПВЧ), які є періодичними і повністю залежать від початкового стану системи. Справжня, абсолютна випадковість у макроскопічному світі не може бути обчислена — вона може бути лише виміряна з реальних стохастичних фізичних процесів.

Отримання істинно випадкових чисел (ГІВЧ) вимагає наявності апаратного джерела ентропії, базою для якого виступають квантові ефекти або термодинамічні явища. Класичним прикладом такого явища є тепловий шум (шум Джонсона-Найквіста), спричинений хаотичним тепловим рухом носіїв заряду в провіднику. Окрім того, як макроскопічні джерела ентропії можуть використовуватися електромагнітні наведення, шуми підсилювачів та аналого-цифрових перетворювачів (АЦП), зокрема інтегрованих в аудіоадаптери. Дослідження цих фізичних флуктуацій, методів їх дискретизації та статистичної перевірки на рівномірність розподілу є актуальною науково-технічною задачею.

Мета роботи полягає у дослідженні фізичної природи джерел ентропії та порівняльному аналізі апаратних і алгоритмічних методів генерації випадкових послідовностей для сучасних інформаційних систем.

Результати дослідження

Фундаментальною проблемою стохастичного моделювання та захисту інформації є отримання істинно випадкових даних. Будь-яка детермінована обчислювальна система здатна генерувати лише псевдовипадкові числа, які математично імітують хаос. Наприклад, класичні адитивні генератори

Фібоначчі забезпечують високу швидкість формування цифрового шуму, але через свою рекурентну алгоритмічну природу вони залишаються періодичними та вразливими [2]. Тому для досягнення абсолютної непередбачуваності на практиці необхідно використовувати макроскопічні термодинамічні процеси або мікрошуми електронних компонентів [1].

Найбільш надійним та фізично обґрунтованим джерелом абсолютної ентропії є тепловий шум (шум Джонсона-Найквіста). Цей тип білого шуму виникає внаслідок хаотичного, броунівського руху носіїв заряду (електронів) у провіднику і є невід'ємною властивістю будь-якого резистивного елемента, незалежно від наявності зовнішнього джерела живлення. Згідно з фундаментальними законами статистичної термодинаміки, середньоквадратичне значення напруги теплового шуму визначається формулою [3]:

$$U_n = \sqrt{4k_B T R \Delta f} \quad (1)$$

де: k_B — стала Больцмана; T — абсолютна температура провідника у кельвінах; R — електричний опір провідника; Δf — смуга пропускання вимірювальної системи.

Використання цього фізичного явища дозволяє створювати апаратні генератори істинно випадкових чисел (ГІВЧ). Оскільки тепловий шум має рівномірну спектральну щільність потужності в широкому діапазоні частот, його оцифрування за допомогою аналого-цифрових перетворювачів (АЦП), зокрема тих, що вбудовані у стандартні аудіоадаптери, дозволяє отримувати масиви випадкових бітів. Поведінку такої системи принципово неможливо відтворити жодними математичними алгоритмами, що робить її ідеальною основою для генерації криптографічних ключів [1].

Для практичного використання термодинамічних флуктуацій у цифрових системах необхідно вирішити проблему узгодження масштабів. Оскільки напруга теплового шуму має порядок мікрівольт, її безпосереднє зчитування логічними елементами є неможливим. Фізична реалізація апаратного генератора вимагає наявності прецизійного операційного підсилювача, який збільшує амплітуду стохастичного сигналу до макроскопічних значень, після чого безперервний аналоговий сигнал подається на вхід аналого-цифрового перетворювача (АЦП) [3].

Процес дискретизації та квантування безперервного фізичного шуму неминуче вносить у систему додаткову апаратну похибку, відому як шум квантування. Цей шум виникає через округлення миттєвих значень напруги до найближчого дозволеного дискретного рівня. Згідно з теорією обробки сигналів, за умови рівномірного розподілу похибки в межах одного кроку квантування, дисперсія (потужність) шуму квантування визначається формулою [1]:

$$\sigma_q^2 = \frac{(\Delta U)^2}{12} \quad (2)$$

де: σ_q^2 — дисперсія шуму квантування; ΔU — крок квантування АЦП (різниця напруг між сусідніми дискретними рівнями).

Щоб квантування не знищило природну ентропію фізичного джерела, необхідно дотримуватися суворої фізичної умови: ефективна амплітуда теплового шуму після підсилення має значно перевищувати крок квантування ΔU . Завдяки виконанню цієї умови багаторозрядні АЦП, якими оснащуються стандартні аудіоадаптери комп'ютерних систем, здатні фіксувати найменші флуктуації напруги на відкритих входах. Це дозволяє використовувати звичайну звукову карту як повноцінний апаратний генератор істинно випадкових чисел без необхідності конструювання додаткових електронних плат [1, 3].

На противагу складним фізичним процесам підсилення та дискретизації, алгоритмічні генератори не потребують взаємодії з аналоговим світом і працюють виключно в дискретному математичному просторі. Наприклад, адитивні генератори Фібоначчі формують нові числа шляхом застосування операції додавання по модулю до попередньо збережених станів регістру. Відсутність теплових шумів, проблем із квантуванням та впливу зовнішніх електромагнітних завад робить такі генератори абсолютно стабільними, проте ця ж стабільність повністю позбавляє їх фізичної ентропії, перетворюючи згенерований цифровий шум на детерміновану і передбачувану послідовність [2].

Для підтвердження якості згенерованого цифрового шуму необхідно дослідити його статистичні характеристики. З точки зору статистичної радіофізики, миттєві значення напруги теплового шуму, що генерується резистивними елементами, підпорядковуються нормальному (гаусівському) закону розподілу ймовірностей. Це зумовлено тим, що результуючий макроскопічний сигнал є сумою величезної кількості незалежних мікроскопічних імпульсів, випромінюваних окремими електронами під час їх теплового руху. Відповідно до центральної граничної теореми, густина ймовірності розподілу амплітуд такої шумової напруги описується фундаментальною формулою [3]:

$$w(U) = \frac{1}{\sigma_U \sqrt{2\pi}} \exp\left(-\frac{U^2}{2\sigma_U^2}\right) \quad (3)$$

де: $w(U)$ — густина ймовірності миттєвого значення напруги U ; σ_U — середньоквадратичне відхилення напруги шуму (ефективна амплітуда); π — математична константа.

Фізична природа цього розподілу гарантує, що поява будь-якого конкретного значення напруги на вході аналого-цифрового перетворювача є принципово непередбачуваною в часі. Однак після оцифрування отриманий масив бітів може містити апаратні зміщення (наприклад, незначне домінування нулів або одиниць через температурний дрейф аудіоадаптера). Для усунення цих артефактів та вирівнювання ймовірностей до ідеального рівномірного розподілу застосовуються спеціальні алгоритми декореляції (відбілювання). На відміну від апаратних джерел, алгоритмічні системи, такі як адитивні генератори Фібоначчі, формують рівномірний розподіл суто математичними методами. Вони генерують числа, що є результатами рекурентних обчислень, а тому їхня випадковість є лише ілюзією, яка легко розкривається при аналізі фазового простору станів [2].

Об'єктивним критерієм оцінки ступеня хаотичності як істинно випадкових, так і псевдовипадкових послідовностей є їх перевірка за допомогою спеціалізованих пакетів статистичних тестів. Найбільш авторитетним стандартом у цій галузі є набір тестів NIST STS (National Institute of Standards and Technology Statistical Test Suite). Цей комплекс містить строгі математичні перевірки на частоту появи бітів, спектральний аналіз (Фур'є), перевірку на наявність шаблонів та лінійну складність. Хоча якісно налаштовані алгоритмічні генератори Фібоначчі здатні успішно проходити більшість тестів NIST, вони залишаються вразливими до криптоаналізу через періодичність свого алгоритму. Водночас цифрові послідовності, згенеровані на основі посиленого теплового шуму та належним чином оцифровані, демонструють ідеальні статистичні показники та абсолютну криптографічну стійкість [1, 3].

Підсумовуючи фізичні та алгоритмічні аспекти генерації випадкових величин, варто наголосити на фундаментальній різниці їхньої природи. Апаратні генератори спираються на незвідну складність макроскопічного світу, де термодинамічні процеси, на кшталт теплового руху електронів, є принципово незворотними. Це означає, що зовнішній спостерігач, навіть маючи повний доступ до структурної схеми пристрою та знаючи поточну температуру середовища, ніколи не зможе розрахувати наступний згенерований біт. Саме ця фізична незалежність макроскопічних флуктуацій від початкових умов системи робить ГПВЧ єдиним надійним джерелом ентропії для криптографічних апаратів критичного призначення [3].

З іншого боку, алгоритмічні моделі, такі як адитивні генератори Фібоначчі, залишаються незамінними у сфері імітаційного моделювання фізичних процесів. У задачах комп'ютерної фізики, де вимагається точна відтворюваність результатів експерименту (наприклад, при моделюванні методом Монте-Карло), строга детермінованість ГПВЧ стає їхньою головною перевагою. Проте використання таких математичних конструкцій для захисту інформації вимагає постійного контролю їхньої криптостійкості за допомогою розширених статистичних батарей, оскільки фазовий простір станів будь-якого комп'ютерного алгоритму є скінченним і циклічним [2].

Практична реалізація сучасних систем генерації цифрового хаосу вимагає синергії прикладної фізики та інформаційних технологій. Інженерний підхід дозволяє використовувати вже наявні в комп'ютерних системах апаратні компоненти, такі як звукові карти зі вбудованими високоточними АЦП, для фіксації мікроскопічних наведень та теплових шумів. Завдяки правильному програмному обробленню та декореляції оцифрованого аналогового сигналу, такі доступні рішення здатні забезпечити рівень ентропії, що повністю відповідає найсуворішим міжнародним стандартам статистичної безпеки (зокрема NIST STS) без необхідності конструювання спеціалізованих

лабораторних установок [1].

Висновки

Проведене дослідження підтверджує фундаментальну перевагу апаратних джерел ентропії над математичними алгоритмами у задачах, що вимагають абсолютної інформаційної безпеки. Використання макроскопічних термодинамічних процесів, зокрема теплового шуму резистивних елементів із подальшою дискретизацією через АЦП, дозволяє генерувати істинно випадкові послідовності (ГІВЧ). Їхня криптографічна стійкість базується на фізичній незворотності та принциповій непередбачуваності квантових і теплових флуктуацій.

Водночас алгоритмічні системи, зокрема адитивні генератори Фібоначчі, залишаються ефективним інструментом для задач імітаційного моделювання в прикладній фізиці завдяки високій швидкості генерації та математичній детермінованості. Проте їх застосування вимагає обов'язкової верифікації за допомогою стандартизованих статистичних тестів, таких як NIST STS. Таким чином, вибір методу генерації цифрового шуму має здійснюватися на основі фізичної природи поставленого завдання: алгоритмічні ГІВЧ доцільні для відтворюваних експериментів, тоді як фізичні ГІВЧ є єдиним надійним рішенням для криптографії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Randomus Anomalous. Генератор випадкових чисел з апаратним джерелом ентропії : технічна документація / програмний проект. – 2018. – 20 с.
2. Ісаков О. В. Порівняльний аналіз цифрових шумів, згенерованих адитивними генераторами Фібоначчі / О. В. Ісаков, С. С. Войтусік // Український журнал інформаційних технологій. – 2023. – Т. 5, № 1. – С. 67–76.
3. Блощинський Б. В. Способи реалізації генераторів істинно випадкових послідовностей : магістерська дисертація : 123 «Комп'ютерна інженерія» / Б. В. Блощинський. – Київ : КПІ ім. Ігоря Сікорського, 2022. – 96 с.

Мовчан Іван Сергійович, студент групи ЗПІ-25Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м.Вінниця, e-mail: ivanmovchan08@gmail.com.

Науковий керівник: **Володимир Валерійович Мартинюк** – доцент кафедри загальної фізики Вінницький національний технічний університет, м.Вінниця, e-mail: martynyuk.v.v@vntu.edu.ua

Movchan Ivan Serhiiovich, student of group ЗPI-25B, Faculty of Information Technology and Computer Engineering. ivanmovchan08@gmail.com.

Academic supervisor: **Volodymyr Valeriiovych Martyniuk** — Associate Professor of the Department of General Physics, Vinnytsia National Technical University, Vinnytsia, e-mail: martynyuk.v.v@vntu.edu.ua