Наносистеми, наноматеріали, нанотехнології
Nanosistemi, Nanomateriali, Nanotehnologii
2026, т. 24, № 1, сс. 53–64
https://doi.org/10.15407/nnn.24.01.0053

PACS numbers: 03.67.-a, 03.67.Dd, 05.40.Ca, 07.05.Tp, 89.20.Bb, 89.20.Ff, 89.70.Cf

Розробка пристрою для одержання високої ентропії з фотонного шуму у криптографічних застосуваннях

Т. О. Горелікова

Запорізький національний університет,
вул. Університетська, 66,
69011 Запоріжжя, Україна

Робота стосується розробки прототипу квантового ґенератора випадкових чисел, що долає фундаментальні обмеження традиційних методів. На відміну від псевдовипадкових ґенераторів, які покладаються на обчислювальну складність, і класичних апаратних ґенераторів, схильних до зовнішніх впливів, запропонований пристрій базується на онтологічній природі випадковости мікросвіту. Джерелом ентропії є дробовий шум, що виникає внаслідок дискретної природи проходження зарядів у фотодетекторі. Такий підхід ґарантує непередбачуваність, що є основою для формування стійких криптографічних ключів і цифрових підписів. Представлений пристрій є комплексним апаратно-програмним рішенням. Ця розробка пропонує ефективне та надійне джерело ентропії для інтеґрації у сучасні системи безпеки, забезпечуючи стійкість до атак, які використовують слабкість ґенераторів випадкових чисел.

The work is concerned with the development of a prototype of a quantum random-number generator that overcomes the fundamental limitations of traditional methods. Unlike pseudo-random generators, which rely on computational complexity, and classical hardware generators, which are susceptible to external influences, the proposed device is based on the ontological nature of the randomness of the microworld. The source of entropy is fractional noise that arises from the discrete nature of the passage of charges inside the photodetector. This approach guarantees unpredictability, which is the basis for the formation of stable cryptographic keys and digital signatures. The presented device is a comprehensive hardware–software solution. This development offers an efficient and reliable source of entropy for integration into modern security systems, ensuring resistance to attacks, which exploit the weakness of random-number generators.

Ключові слова: квантовий ґенератор випадкових чисел, істинна ентропія, дробовий шум, криптографічна стійкість, фон Нейманів алґоритм,

апаратний захист інформації, системи безпеки.

Key words: quantum random-number generator, true entropy, fractional noise, cryptographic stability, von Neumann algorithm, hardware information protection, security systems.

(Отримано 2 жовтня 2025 р.)

1. ВСТУП

У сучасному цифровому світі забезпечення надійної інформаційної безпеки є одним з найбільш актуальних завдань. Зростання обсягів даних і популярности блокчейн-платформ створюють нові виклики для захисту від несанкціонованого доступу, шахрайства та кібератак. Одним з фундаментальних елементів безпечних інформаційних систем виступає ґенерація випадкових чисел, адже саме від їхньої якости залежить стійкість криптографічних алґоритмів, які, у свою чергу, є основою сучасних засобів захисту даних [1, 2].

Випадковість є необхідною для формування криптографічних ключів, одноразових паролів, цифрових підписів, а також для процедур автентифікації та верифікації. Будь-яке відхилення від істинної випадковости може мати катастрофічні наслідки. Доведено, що слабкі ґенератори випадкових чисел ставали причиною численних компрометацій криптосистем:

— компрометація RSA-ключів у чипах Infineon (2017) (через слабкий ГВЧ, що використовувався в чипах, дослідники змогли відновити приватні ключі RSA на основі відкритих);
— вразливість Debian OpenSSL (2008) (помилка в коді призвела до того, що для ґенерації ключів використовувалися передбачувані значення, що зробило їх легко зламуваними);
— компрометація Bitcoin-гаманців на Android (2013) (деякі додатки для криптовалют використовували слабкий ГВЧ, що дало змогу зловмисникам передбачити приватні ключі та викрасти кошти);
— вразливість PHP (2007) (слабка ентропія в ґенераторі випадкових чисел PHP робила сеансові ідентифікатори передбачуваними, що давало змогу викрадати сеанси користувачів на вебсайтах) [3].

Саме тому питання джерела випадковости не є другорядним; воно має першорядне значення у контексті побудови захищених систем.

Традиційно у цифрових системах використовуються псевдовипадкові ґенератори чисел (PRNG). Їхня робота базується на детермінованих алґоритмах, які з початкового значення (seed) обчис-

люють послідовності чисел, що виглядають випадковими. Популярними є алґоритми на основі лінійних конґруентних методів, зсувних реґістрів або криптографічних примітивів (наприклад, AES або SHA в режимі ґенератора). Перевагою PRNG є висока швидкодія, проте головним недоліком залишається їхня передбачуваність: знаючи початкове значення або внутрішній стан, зловмисник може відтворити всю послідовність [4].

Для підвищення рівня безпеки застосовуються криптографічно стійкі ґенератори (CSPRNG), які ускладнюють відновлення початкових умов навіть за відомої частини вихідної послідовности. Втім, їхня безпека завжди спирається на припущення про обчислювальну складність певних математичних задач. Тобто стійкість CSPRNG відносна: за умови відкриття нових алґоритмів чи розвитку швидкости обчислень такі ґенератори виявляються вразливими [5].

Іншою категорією є апаратні ґенератори випадкових чисел (HRNG), які використовують фізичні процеси як джерело ентропії. Найчастіше це — тепловий шум у резисторах, коливання електронних схем або хаотичні зміни в електромагнетних середовищах. Незважаючи на більш високу якість у порівнянні з PRNG, ці методи не позбавлені проблем:

— фізичні процеси можуть піддаватися зовнішньому впливу (наприклад, температурних змін або електромагнетних наведень);
— шумові процеси іноді мають латентні закономірності, що понижує рівень ентропії;
— складно формально довести істинну випадковість одержаних послідовностей.

Таким чином, обидва підходи, як псевдовипадкові, так і апаратні класичні ґенератори, мають істотні обмеження. У контексті високонавантажених криптографічних систем, де ціна помилки є надзвичайно високою, цього виявляється недостатньо [6].

2. КВАНТОВІ ПРОЦЕСИ ЯК ПРИРОДНЄ ДЖЕРЕЛО ВИПАДКОВОСТИ

На противагу класичним методам, квантові ґенератори випадкових чисел (QRNG) базуються на фундаментальних законах квантової механіки, які мають ймовірнісну природу. Випадковість тут не є наслідком складности чи неповноти розуміння, а виступає онтологічною характеристикою мікросвіту. Прикладами квантових процесів, що застосовуються у QRNG, є:

— фотонна поляризація: вибір напрямку поляризації окремого фотона є непередбачуваним;
— квантове тунелювання: час ймовірного переходу електрона через бар’єр не можна визначити наперед;

— дробовий шум (shot noise), який виникає внаслідок того, що носії заряду (фотони чи електрони) надходять у детектор у випадкові моменти часу;

— спонтанне випромінювання в лазерах: момент емісії фотона має квантово-ймовірнісну природу.

На відміну від теплового чи електронного шуму, ці процеси принципово не піддаються класичному передбаченню. Вони є реалізацією базових постулатів квантової теорії, і жоден алґоритм чи модель не дають змогу реконструювати їх наперед. Саме тому QRNG забезпечують істинну випадковість [7].

Вибір QRNG як базового джерела випадкових чисел у даній роботі зумовлений багатьма об'єктивними причинами. У PRNG випадковість лише емулюється, а в HRNG вона може бути спотворена шумом або зовнішніми чинниками. У QRNG випадковість ґарантована самою природою квантових явищ. Ґенерація значень на основі QRNG виключає ризик слабких значень, які виникають за недостатньої ентропії. Це критично важливо під час використання алґоритмів еліптичних кривих, де навіть невелика втрата випадковости може призвести до повного компрометування системи. На відміну від класичних джерел, QRNG не потребує статистичного моделювання для підтвердження випадковости: її ґарантують закони квантової механіки [8].

3. ПРИНЦИПИ РОБОТИ КВАНТОВОГО ҐЕНЕРАТОРА ВИПАДКОВИХ ЧИСЕЛ

Метод випадкового вибору учасників і контрольних точок базується на комбінації криптографії еліптичних кривих і ґенерації істинно випадкових чисел. QRNG у цьому контексті виступає не допоміжним, а визначальним елементом:

— він забезпечує непередбачуваність вибору учасників, що унеможливлює маніпуляції з боку окремих вузлів;

— ґарантує рівномірність розподілу під час вибору блоків, запобігаючи концентрації контролю;

— створює базу для формування ключів і підписів, стійких щодо атак на рівні як класичних, так і потенційних квантових комп'ютерів.

Вибір на користь квантового ґенератора випадкових чисел є свідомою відмовою від псевдовипадкових і класичних апаратних методів, які не відповідають сучасним вимогам щодо криптографічної безпеки. Використання QRNG уможливлює підняти рівень захищености системи на якісно новий щабель, забезпечуючи непередбачуваність і стійкість до будь-яких відомих типів атак.

Запропонований розроблений пристрій базується на використанні квантових джерел випадковости, що забезпечує якісно ви-

щий рівень непередбачуваности у порівнянні з класичними ґенераторами псевдовипадкових чисел. В основі роботи покладено явище дробового шуму (shot noise), яке виникає внаслідок дискретної природи фотонів та електронів. За падіння світлового потоку на фотодетектор процес реєстрації фотонів описується Пуассоновим розподілом, де ймовірність спостереження k фотонів за певний проміжок часу задається формулою

$$P(k;\lambda) = \lambda^k e^{-\lambda}/k!, \tag{1}$$

де λ — середня інтенсивність фотонного потоку.

У струмі, що виникає в результаті такого процесу, спостерігається шумова складова з квантовою природою, спектральна густина якої описується рівнянням

$$S_I(f) = 2qI, \tag{2}$$

де q — заряд електрона, а I — середній фотострум. Саме ця непередбачувана складова і стає основним джерелом ентропії у даному пристрої. Для того, щоб оцінити якість одержаних випадкових послідовностей, використовується Шеннонова ентропія, яка визначається як

$$H(x) = -\sum_{i=1}^{n} p_i \log_2 p_i, \tag{3}$$

де p_i — ймовірність появи відповідного символу. Ідеальний випадковий ґенератор забезпечує максимальне значення ентропії, близьке до одного біта на кожний зґенерований біт [9].

Однак фізичні джерела випадковости, зокрема фотодетектори, можуть демонструвати статистичні перекоси у бік ґенерації більшої кількости нулів чи одиниць. Для усунення цієї проблеми у пристрої був реалізований фон Нейманів алґоритм. Його суть полягає у тому, що вхідна послідовність розбивається на пари бітів, після чого відкидаються комбінації «00» і «11», тоді як «01» інтерпретується як нуль, а «10» як одиниця. Завдяки цьому зберігається лише рівноймовірна інформація, а перекіс джерела усувається. Формально процедура описується таким чином:

$$f(b_1, b_2) = \begin{cases} \varnothing, & b_1 = b_2, \\ 0, & (b_1, b_2) = (0,1), \\ 1, & (b_1, b_2) = (1,0). \end{cases} \tag{4}$$

Таким чином, навіть якщо первинний фотонний шум містить структурні відхилення, вихідна послідовність після оброблення за фон Неймановим алґоритмом набуває властивостей рівномір-

ного випадкового розподілу [10].

Розроблений ґенератор випадкових чисел базується на використанні фотонного шуму як джерела ентропії та його подальшому підсиленні за допомогою малошумних аналогових каскадів. Для практичної реалізації ґенератора було використано мікроконтролер ESP32, який виконує функції дискретизації аналогового сиґналу фотодіоди за допомогою вбудованого АЦП, його попереднього оброблення та подальшої цифрової трансформації. Зібрані біти послідовности подаються на програмну реалізацію фон Нейманового алґоритму для підвищення рівня ентропії. Такий підхід уможливлює одержати послідовності, що відповідають криптографічним вимогам до випадковости й успішно проходять перевірку за статистичними тестами стандарту NIST SP 800-22.

У структурі пристрою можна виділити три функціональні блоки: сенсорний, підсилювальний та обчислювальний. Сенсорну частину представлено фотодетектором, що працює в умовах слабкого освітлення або під впливом деякого джерела світла. Як базовий варіянт, застосовується фотодіода BPW34 у режимі зворотнього зміщення; проте для підвищення рівня шуму може бути використана лавинна фотодіода (APD), що працює у режимі пробою. Через неї тече дуже малий струм, настільки малий, що його неможливо сприйняти безпосередньо без посилення; тому у схему пристрою також додано підсилювач. Цей струм — непостійний; він складається з окремих перенесень заряду, що хаотично виникають. Електрони в напівпровіднику не рухаються як безперервний потік, а перестрибують випадково, підкоряючись ймовірнісній природі квантових процесів. Це і є дробовий шум — флюктуації (випадкові коливання), які виникають саме через дискретність електричного заряду, які неможливо передбачити або змоделювати, тому що вони відбуваються в квантовому масштабі, поза рамками класичної причинности.

Фотодіода у цій системі виконує роль не просто давача світла, а квантового джерела ентропії. Вона створює сиґнал, який абсолютно не піддається розрахунку, навіть якщо точно відомі всі параметри схеми, напруги, температури, рівня освітлення. Для підкреслення незалежности від зовнішніх чинників фотодіоду розташовано у світлонепроникній коробці. Фотодіода ґенерує темновий струм (dark current) навіть у повній темряві. Це пов’язане з тепловими коливаннями та квантовими ефектами у матеріялі, тому що сам факт проходження кожного окремого електрона крізь потенціяльний бар’єр — це процес ймовірнісний. Жодна програма, ніякий суперкомп’ютер не може заздалегідь зазначити, коли проскочить наступний електрон, і саме в цьому полягає фундаментальна непередбачуваність [11].

Джерелом світла може виступати світлодіода з низьким рівнем

власних шумів, розташована у світлонепроникному корпусі разом із фотодіодою для формування стабільного шумового каналу.

Аналоговий каскад реалізовано на операційному підсилювачі малошумного типу (наприклад MOPA2340UA). Схему побудовано за конфіґурацією неінвертувального підсилювача з великим коефіцієнтом підсилення, що забезпечує реєстрацію навіть незначних флюктуацій фотоструму. Резистор зворотнього зв'язку номіналом у 100 кОм визначає величину підсилення, тоді як паралельно ввімкнений конденсатор у 100 нФ виконує функцію обмеження високочастотної складової.

Вихід підсилювального каскаду подається на аналоговий вхід ESP32 (наприклад GPIO34), де сиґнал оцифровується вбудованим АЦП. Подальше оброблення передбачає застосування алґоритму за фон Нейманом, що усуває можливі статистичні перекоси у послідовності бітів.

Представлений різновид розробленого ґенератора випадкових чисел складається з трьох незалежних пар фотоелементів (фотодіод із відповідною підсилювальною обв'язкою), кожна з яких формує власний канал шумового сиґналу. Така архітектура дає змогу зменшити вплив локальних флюктуацій і підвищити стійкість системи: навіть якщо один канал тимчасово дає занижений рівень шуму, два інші залишаються активними, забезпечуючи ентропію. Для стабільности роботи додатково використовується допоміжна світлодіода, що створює контрольований рівень освітлення фотодіод і мінімізує ризик повної втрати сиґналу через зовнішні перешкоди. Електричну схему пристрою представлено на рис. 1.

Аналогові сиґнали з кожної пари фотоелементів надходять на входи ESP32, де перетворюються в цифровий вигляд за допомогою вбудованого АЦП. Подальше програмне оброблення передбачає поєднання даних трьох каналів у єдиний результат. Для цього використовується процедура з вибірковим застосуванням медіянного значення, яка пригнічує одиничні викиди, а також операції XOR, що забезпечують непередбачуваність вибору. Таким чином, кінцевий сиґнал містить як фізичну ентропію фотонного шуму, так і математично посилену випадковість. На рисунку 2 представлено зображення макетної плати готового прототипу пристрою, де розміщено усі описані вище компоненти.

У демонстраційному варіянті пристрою передбачено використання невеликого OLED-дисплея, який дає змогу у реальному часі виводити випадкове значення. Така функція має, насамперед, демонстраційний характер: вона дає можливість наочно показувати зміну випадкових величин і контролювати працездатність системи під час експериментів чи публічних презентацій.

Разом із тим, наявність дисплея не є обов'язковою умовою для

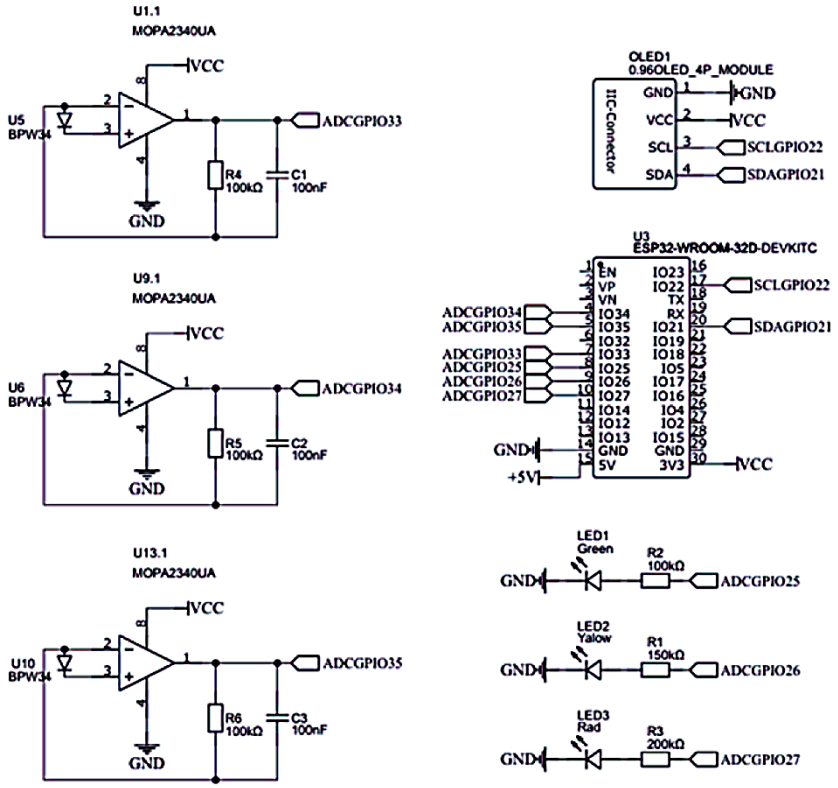

Рис. 1. Електрична схема розробленого прототипу квантового ґенератора випадкових чисел.[1]

роботи ґенератора. У практичних застосуваннях випадкові послідовності можуть безпосередньо передаватися через інтерфейс Serial (UART/USB) або ж передаватися по бездротових каналах (Wi-Fi, Bluetooth) на інші пристрої, зокрема на персональний комп'ютер, сервер або вбудовану систему, де вони будуть використані для криптографічних або статистичних задач. Такий підхід робить систему гнучкою: вона може виступати як автономний демонстраційний модуль із візуалізацією, так і як повноцінне джерело ентропії для інтеґрації у складніші апаратно-програмні комплекси. Демонстраційний варіянт пристрою представлено на фотографії (рис. 3).

4. ЕКСПЕРИМЕНТАЛЬНІ РЕЗУЛЬТАТИ Й ОЦІНКА ЕНТРОПІЇ

Для оцінки якости зґенерованих випадкових чисел було проведено статистичну аналізу вибірки з 2500 значень у діяпазоні від

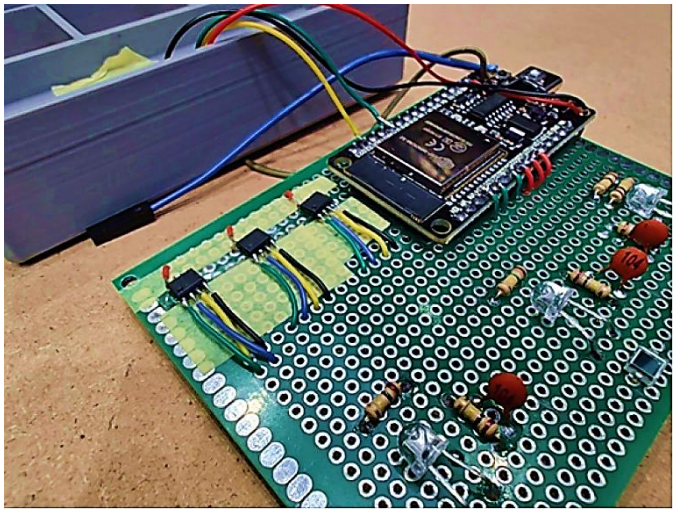

Рис. 2. Фотографія розпаяної макетної плати прототипу квантового ґенератора випадкових чисел.[2]

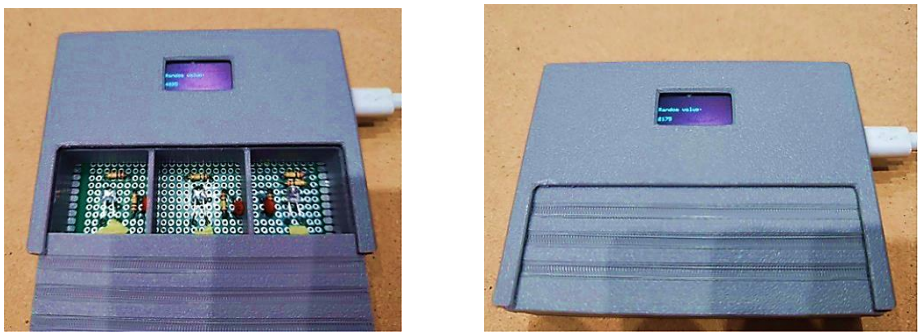

Рис. 3. Зовнішній вигляд готового демонстраційного прототипу квантового ґенератора випадкових чисел.[3]

101 до 9988. Усі числа виявилися унікальними, повтори відсутні, що свідчить про високий рівень різноманітности та відсутність очевидних артефактів у ґенерації. Середнє значення склало 4879,02, медіяна — 4619,5, а стандартний відхил — 2740,6, що добре узгоджується з очікуванням рівномірного розподілу.

Для перевірки рівномірности було виконано χ''-тест із розбиттям вибірки на десять рівних інтервалів. Одержане значення $\chi'' = 5{,}68$ із 9 ступенями свободи відповідає p-значенню приблизно у 0,77, що значно перевищує традиційний рівень значущости у 0,05. Таким чином, гіпотеза про рівномірний розподіл не відхиляється і можна стверджувати, що числа охоплюють увесь діяпа-

зон без концентрації у вузьких зонах.

Додатково було розраховано Шеннонову ентропію, яка склала $H \approx 7{,}97$ біт/символ, що є майже максимально можливим значенням для множини з 2500 рівноймовірних унікальних елементів. Це підтверджує високу ступінь невизначености та випадковости вибірки.

На рівні бітових послідовностей проведені тести на серійність, автокореляцію та стиснення не виявили статистично значимих відхилів.

Було проведено додаткові експерименти для незалежної вибірки, що дало змогу підтвердити стійкість одержаних результатів:

χ''-тест рівномірності (10 інтервалів від 1 до 9999): $\chi'' = 10{,}24$, $p = 0{,}3314$; значення $p > 0.05$ означає відсутність значних відхилів від рівномірного розподілу;

тест Колмогорова–Смирнова (нормування на [0, 1]): $KS = 0{,}070$, $p = 0{,}1663$; тест останньої цифри (χ'' для 0–9): $\chi'' = 5{,}36$, $p = 0{,}8019$;

цифри розподілені рівномірно, відсутнє упередження на рівні молодших розрядів; автокореляція (лаги 1–20): значення коливаються навколо нуля, істотних залежностей не виявлено.

Одержані результати свідчать, що вибірка пройшла ключові статистичні тести на випадковість. Серйозних закономірностей чи упереджень не виявлено. Це підтверджує, що розроблений ґенератор може використовуватися як надійне джерело ентропії для криптографічних задач та інших систем, де потрібна висока якість випадкових чисел.

5. ВИСНОВОК

У описаному пристрої поєднано фізичну непередбачуваність квантового шуму з математично обґрунтованими методами усунення перекосів і криптографічними механізмами постоброблення. Завдяки цьому досягається високий рівень ентропії за помірних апаратних витратах, що робить реалізацію на ESP32 ефективною як для наукових експериментів, так і для практичного використання у системах безпеки, блокчейн-технологіях чи Інтернеті речей.

Продемонстрований прототип квантового ґенератора випадкових чисел успішно вирішує актуальну проблему забезпечення криптографічних систем джерелом істинної випадковости, яке є невразливим до класичних методів злому чи обчислювального прогнозування. Створений пристрій є значним кроком вперед, оскільки він свідомо відходить від застарілих псевдовипадкових і класичних апаратних ґенераторів, чия стійкість є лише відносною. Натомість, у роботі інтеґровано фундаментальне квантове

явище, — шум на напівпровідниковому переході, — в архітектуру, що забезпечує непередбачуваність на атомарному рівні. Апаратне рішення поєднує багаторазове фізичне джерело ентропії (три незалежні канали фотодетекторів) із спеціялізованими аналоговими каскадами. Ця багатоканальна архітектура у поєднанні з програмною корекцією, що використовує методи усунення перекосів, дала змогу досягти максимальної якости вихідної послідовности.

Експериментальні дослідження підтвердили, що ґенератор виробляє послідовності, які відповідають вимогам щодо якости випадкових чисел. Це робить розроблений пристрій джерелом ентропії для важливих застосувань, включаючи формування ключів у блокчейн-технологіях, механізми автентифікації, а також інші системи, де ціна помилки є надзвичайно високою. Таким чином, реалізація прототипу квантового ґенератора випадкових чисел на базі ESP32 демонструє ефективний шлях щодо побудови захищених і стійких щодо майбутніх атак апаратно-програмних комплексів.

ЦИТОВАНА ЛІТЕРАТУРА–REFERENCES

1. T. O. Horelikova and S. V. Choporov, *Int. J. Comput. Appl. Math. Comput. Sci.*, **2024**: 54 (2024); https://doi.org/10.1007/ijcams.2024.54
2. T. O. Horelikova, *Proc. All-Ukrainian Sci.-Pract. Conf. Students, Postgraduates and Young Scientists 'Existential Challenges of Education, Science, Security and Health in Modern Conditions: Research by Young Scientists' (December 12, 2024, Odesa)*, **41**, p. 89 (in Ukrainian).
3. L.-Y. Deng, N. Kumar, H. H.-S. Lu, and C.-C. Yang, *Random Number Generators for Computer Simulation and Cyber Security: Design, Search, Theory, and Application* (Cham: Springer: 2025); https://doi.org/10.1007/978-3-031-76722-7
4. J.-P. Aumasson, *Serious Cryptography* (San Francisco: No Starch Press: 2024).
5. T. Lugrin, *Random Number Generator. Trends in Data Protection and Encryption Technologies* (Eds. V. Mulder, A. Mermoud, V. Lenders, and B. Tellenbach) (Cham: Springer: 2023), p. 31; https://doi.org/10.1007/978-3-031-33386-6_7
6. H. Ravichandran, D. Sen, A. Wali, T. F. Schranghamer, N. Trainor, B. Ray, and S. Das, *ACS Nano*, **17**, No. 17: 16817 (2023); https://doi.org/10.1021/acsnano.3c03581
7. D. Johnston, *Random Number Generators—Principles and Practices: A Guide for Engineers and Programmers* (Berlin: Walter de Gruyter: 2018); https://doi.org/10.1515/9781501506062
8. C. Kollmitzer, S. Schauer, S. Rass, and B. Rainer, *Quantum Random Number Generation: Theory and Practice* (Cham: Springer: 2020); https://doi.org/10.1007/978-3-319-72596-3
9. M. Orszag, *Quantum Optics: Including Noise Reduction, Trapped Ions,*

Quantum Trajectories, and Decoherence (Cham: Springer: 2024); https://doi.org/10.1007/978-3-031-54853-6
10. Douglas Cenzer and Christopher P. Porter, *Computability*, **12**, No. 1: 1 (2023); https://doi.org/10.3233/COM-210343
11. *Quantum Probability and Randomness* (Eds. A. Khrennikov and K. Svozil) (Basel: MDPI Books: 2019); https://doi.org/10.3390/books978-3-03897-715-5

Zaporizhzhya National University,
66 Universytetska Str.,
UA-69011 Zaporizhzhia, Ukraine

[1] **Fig. 1.** Electrical diagram of the developed prototype of the quantum random-number generator prototype.
[2] **Fig. 2.** Photograph of the unsoldered breadboard of the prototype of the quantum random-number generator prototype.
[3] **Fig. 3.** Appearance of the finished prototype of the quantum random-number generator.